Neusoft

东软 NetEye 防火墙软件 V3.2.4
命令参考手册

V4.00-R2101

东软联系信息

网站：http://www.neusoft.com

电子信箱：neteyeservice@neusoft.com

服务电话：4006-556789

目录

前言

本手册介绍了 NetEye 的安装和使用信息。 NetEye 的安装和维护需要由有经验的技术人员或者东软指定的服务提供商来进行。

前言包括以下信息：

手册结构

本手册由以下章节和附录构成：

- 前言介绍了命令的相关信息和使用 NetEye 前的准备工作。
- 第 1 章，系统维护命令到第 17 章，高可用性命令按功能模块列出了所有的章节，各章节内的命令按字母顺序排列。
- 术语表 介绍了通过命令行配置和管理 NetEye 过程中所使用的一些常用术语。
- 索引 按字母顺序列出了所有命令的链接，其中命令后面的 “*” 符号表示该命令的配置信息可被同步。

手册约定

介绍本手册的约定内容，包括注意事项以及命令行约定等。

注意事项

提示
需要关注的信息或建议。

命令行约定

本节定义了本手册中出现的命令行元素。管理员会在命令行中遇到下面一个或多个元素。

表 1 命令行约定

约定	描述信息
斜体	**1.** 命令行参数采用*斜体*表示，参数表示命令中必须赋予实际值的部分： **show alert-config** *alert_name* 例如显示名称为 test 的报警策略信息： **show alert-config test** **2.** 命令行参数对大小写敏感，例如： **show alert-config test** 和 **show alert-config TEST**两条命令分别显示名称为test 和 TEST 的报警策略信息。
粗体	**粗体**表示章节标题或命令行关键字。 命令行关键字对大小写不敏感，例如： **show system info**和**SHOW SYSTEM INFO**均显示系统的基本信息。
尖括号	尖括号括起来的部分表示参数的取值范围。 例如： • WORD<1-32> 表示指定参数的取值范围为 1-32 个字节。 • INTEGER<1-60> 表示指定参数的取值范围为 1-60 之间的整数。
方括号	用方括号括起来的部分表示可选参数。 **clear cam-table** [**vlan** *vlan_id*] 例如： **clear cam-table vlan 1**
竖线 (|)	竖线分隔的元素互不包含，只选一个。 **arp timeout** {**default |** *timeout_value*} 为下面命令中的互斥元素赋值： **arp timeout default** 或 **arp timeout 200**
(‘ . , ; + * - /)	标点符号或数学符号属文字符号，管理员需要按照系统的要求正确输入。
WORD	字符格式 “WORD”，由字母、数字、下划线组成，且不能以下划线开头，多个字符格式的参数可以用英文逗号隔开。
INTEGER	数字格式 “INTEGER”，取值范围只能是正整数。

表 1 命令行约定 (续)

约定	描述信息
NUMBER	数字列表，以 “,” 分隔，每项可以是单独的数字也可以是以 “-” 连接的数字范围。
LIMIT	端口号范围。 例如：23-45。
x.x.x.x	IPv4 地址格式 “x.x.x.x”，每个点分隔开的数值选取范围是 0-255。
A.B.C.D/M	IP 地址与掩码长度。 例如：10.3.1.0/24。
IPV4RANGE	IP 地址范围，格式为 “x.x.x.x-x.x.x.x”。
IPV4LIST	IP 地址列表，以 “,” 分隔，每项可以是单独的 IP 地址，也可以是 IP 地址范围。
MACLIST	MAC 地址列表，以 “,” 分隔，每项可以是单独的 MAC 地址也可以是 MAC 地址范围。
LINE	备注信息字符串，最大长度限制为 255 个字符。取值范围不允许输入英文的单引号、双引号、大于号、小于号、反斜线 （\）、 &。
HH:HH:HH:HH:HH:HH	MAC 地址 “HH:HH:HH:HH:HH:HH”，取值范围是 00:00:00:00:00:00-FF:FF:FF:FF:FF:FF。
YYYY-MM-DD	日期格式 “YYYY-MM-DD”，取值范围是 1970-01-01 至 2037-12-31。
HH:MM:SS	表示小时、分钟和秒，取值范围是 00:00:00-23:59:59。

表 2 常用命令集

命令原型	命令解释
end	退出当前配置模式，返回到普通配置模式。
exit	退出当前配置模式，返回到上一级配置模式。
list	列出当前配置模式下的所有命令。
configure mode	进入全局配置模式。
configure mode override	强制进入全局配置模式。
lock	锁住终端。

连接方式

管理员可以使用 Console、 Telnet 和 SSH 方式登录到 NetEye，进行 CLI 配置。

- **Console**

  Console 是 NetEye 设备的控制台接口。管理主机可以通过其接口登录到命令行来管理 NetEye。在管理主机上必须安装终端软件，如：Windows 系统的超级终端程序，Linux 系统的 Minicom 程序。

终端软件的配置如下：

- 波特率—9600
- 数据位—8
- 奇偶校验位—无
- 停止位—1

- **Telnet**

  Telnet 协议是 Internet 远程登录服务的标准协议。管理主机可以通过 Telnet 可用链接登录到命令行来管理 NetEye。

  使用 Telnet 协议远程管理 NetEye 需要同时满足下列条件：

  - 管理主机上需要安装 Telnet 客户端软件
  - 保持网络畅通，并且管理主机与 NetEye 可以进行 TCP 互联
  - NetEye 需要配置相应的 Telnet 服务

- **SSH**

  SSH(Secure Shell) 协议是建立在应用层和传输层基础上的安全协议。管理主机可以通过 SSH 可用链接登录到命令行来管理 NetEye。

  使用 SSH 协议远程管理 NetEye 需要同时满足下列条件：

  - 管理主机上需要安装 SSHv1 或者 SSHv2 客户端软件
  - 保持网络畅通，并且管理主机与 NetEye 可以进行 TCP 互联
  - NetEye 需要配置相应的 SSH 服务

配置模式

配置模式是管理员与 NetEye 之间进行命令行配置的交互窗口。

- **普通配置模式**

登录到 NetEye 后，所在的模式即为普通配置模式。在该模式中，可以对某一策略或者设备的相关信息进行查看和操作。例如：可以查看 NetEye 的系统信息、拷贝技术支持文件等。

普通配置模式的提示符：

```
NetEye@root>
```

- **全局配置模式**

登录到 NetEye 后，在普通配置模式下，可通过 **configure mode** 命令进入全局配置模式。在该模式下，可以对 NetEye 的策略、设备的资源等进行配置。例如：VLAN 和虚拟系统 （Vsys）的划分、主机名 （Hostname）的更改，以及对策略的添加或删除等操作。

进入全局配置模式：

```
NetEye@root>configure mode
NetEye@root-system]
```

- **VLAN 配置模式**

在全局配置模式下，可以输入 **vlan** *vlan_id* 命令进入到 VLAN 配置模式。

进入 VLAN 配置模式：

```
NetEye@root-system]vlan 1
NetEye@root-system-vlan1]
```

- **接口配置模式**

接口配置模式包括 Ethernet 接口、 Channel 接口、 VPN 隧道接口、冗余接口、虚拟接口、环回接口和 PPPoE 接口配置模式。

在全局配置模式下，可以输入 **interface ethernet** *interface_id* 命令进入到 Ethernet 接口配置模式。

进入 Ethernet 接口配置模式：

```
NetEye@root-system]interface ethernet 1
NetEye@root-system-if-eth1]
```

提示

通过 CLI 指定一个接口可以输入后缀，如：1 或 s2p3 ；也可以输入接口的全称，如：eth1 或 eth-s2p3。

在全局配置模式下，可以输入 **channel** *channel_id* 命令进入到 Channel 接口配置模式。

进入 Channel 接口配置模式：

```
NetEye@root-system]channel 1
NetEye@root-system-if-ch1]
```

在全局配置模式下，可以输入 **tunnel** *tunnel_id* 命令进入到 VPN 隧道接口配置模式。

进入 VPN 隧道接口配置模式：

```
NetEye@root-system]tunnel 11
NetEye@root-system-tunnel11]
```

在全局配置模式下，可以输入 **rint** *rint_id* 命令进入到冗余接口配置模式。

进入冗余接口配置模式：

```
NetEye@root-system]rint 1
NetEye@root-system-rint1]
```

在全局配置模式下，可以输入 **veth** *veth_id* 命令进入到虚拟接口配置模式。

进入虚拟接口配置模式：

```
NetEye@root-system]veth 1
NetEye@root-system-veth1]
```

在全局配置模式下，可以输入 **loopback** *lo_id* 命令进入到环回接口配置模式。

进入环回接口配置模式：

```
NetEye@root-system]loopback 1
NetEye@root-system-lo1]
```

在全局配置模式下，可以输入 **pppoe** *pppoe_id* 命令进入到 PPPoE 接口配置模式。

进入 PPPoE 接口配置模式：

```
NetEye@root-system]pppoe 1
NetEye@root-system-pppoe1]
```

- **虚拟网络配置模式**

在全局配置模式下，可以输入 **vnet** *vnet_id* 命令进入到虚拟网络配置模式。

进入虚拟网络配置模式：

```
NetEye@root-system]vnet 1
NetEye@root-system-vnet1]
```

- **虚拟路由器配置模式**

在全局配置模式下，可以输入 **virtual route** *vrid* 命令进入到虚拟路由器配置模式。

进入虚拟路由器配置模式：

```
NetEye@root-system]virtual route 1
NetEye@root-system-vr1]
```

- **虚拟路由器探测组配置模式**

在全局配置模式下，可以输入 **detect group** *group_id* 命令进入到虚拟路由器探测组配置模式。

进入虚拟路由器探测组配置模式：

```
NetEye@root-system]detect group 1
NetEye@root-system-dg1]
```

- **集群配置模式**

在全局配置模式下，可以输入 **cluster** 命令进入到集群配置模式。

进入集群配置模式：

```
NetEye@root-system]cluster
NetEye@root-system-cluster]
```

- **策略路由配置模式**

在全局配置模式下，可以输入 **policy route** *policy_name* 命令进入到策略路由配置模式。

进入策略路由配置模式：

```
NetEye@root-system]policy route test
NetEye@root-system-routepolicy-test]
```

- **OSPF 配置模式**

OSPF 配置模式包括 OSPF 普通配置模式、 OSPF 全局配置模式和 OSPF 路由配置模式。必须在全局配置模式输入 **ospf enable** 命令开启 OSPF 功能后，才可以进入 OSPF 的各配置模式。

在全局配置模式下，可以输入 **zebos ospf** 命令进入到 OSPF 普通配置模式。

进入 OSPF 普通配置模式：

```
NetEye@root-system]ospf enable
NetEye@root-system]zebos ospf
neteye-ospfd#
```

在 OSPF 普通配置模式下，可以输入 **configure terminal** 命令进入到 OSPF 全局配置模式。

进入 OSPF 全局配置模式：

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#
```

在 OSPF 全局配置模式下，可以输入 **router ospf** *process_id* 命令进入到 OSPF 路由配置模式。

进入 OSPF 路由配置模式：

```
neteye-ospfd(config)#router ospf 1
neteye-ospfd(config-router)#
```

在 OSPF 全局配置模式下，可以输入 **interface** *interface_name* 命令进入到 OSPF 接口配置模式。

进入 OSPF 接口配置模式：

```
neteye-ospfd(config)#interface eth1
neteye-ospfd(config-if)#
```

- **RIP 配置模式**

RIP 配置模式包括 RIP 普通配置模式、 RIP 全局配置模式和 RIP 路由配置模式。必须在全局配置模式输入 **rip enable** 命令开启 RIP 功能后，才可以进入 RIP 的各配置模式。

在全局配置模式下，可以输入 **zebos rip** 命令进入到 RIP 普通配置模式。

进入 RIP 普通配置模式：

```
NetEye@root-system]rip enable
NetEye@root-system]zebos rip
neteye-ripd#
```

在 RIP 普通配置模式下，可以输入 **configure terminal** 命令进入到 RIP 全局配置模式。

进入 RIP 全局配置模式：

```
neteye-ripd#configure terminal
neteye-ripd(config)#
```

在 RIP 全局配置模式下，可以输入 **router rip** 命令进入到 RIP 路由配置模式。

进入 RIP 路由配置模式：

```
neteye-ripd(config)#router rip
neteye-ripd(config-router)#
```

在 RIP 全局配置模式下，可以输入 **interface** *interface_name* 命令进入到 RIP 接口配置模式。

进入 RIP 接口配置模式：

```
neteye-ripd(config)#interface eth1
neteye-ripd(config-if)#
```

- **BGP 配置模式**

BGP 配置模式包括 BGP 普通配置模式、 BGP 全局配置模式和 BGP 路由配置模式。

必须在全局配置模式输入 **bgp enable** 命令开启 BGP 功能后，才可以进入 BGP 的各配置模式。

在全局配置模式下，可以输入 **zebos bgp** 命令进入到 BGP 普通配置模式。

进入 BGP 普通配置模式：

```
NetEye@root-system]bgp enable
NetEye@root-system]zebos bgp
neteye-bgpd#
```

在 BGP 普通配置模式下，可以输入 **configure terminal** 命令进入到 BGP 全局配置模式。

进入 BGP 全局配置模式：

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#
```

在 BGP 全局配置模式下，可以输入 **router bgp** *as_number* 命令进入到 BGP 路由配置模式。

进入 BGP 路由配置模式：

```
neteye-bgpd(config)#router bgp 1
neteye-bgpd(config-router)#
```

- **路由选项配置模式**

在全局配置模式下，可以输入 **zebos nsm** 命令，再输入 **configure terminal** 命令进入到路由选项配置模式。

进入路由选项配置模式：

```
NetEye@root-system] zebos nsm
neteye-nsm# configure terminal
```

```
neteye-nsm(config)#
```

- **VPN 配置模式**

在全局配置模式下，可以输入 **vpn** 命令进入到 VPN 配置模式。

进入 VPN 配置模式：

```
NetEye@root-system]vpn
NetEye@root-system-vpn]
```

- **Vsys 配置模式**

在全局配置模式下，可以输入 **vsys** *vsys_id* 命令进入到 Vsys 配置模式。

进入 Vsys 配置模式：

```
NetEye@root-system]vsys 1
NetEye@root-system-vsys1]
```

- **用户权限表配置模式**

在全局配置模式下，可以输入 **permission tables** *table_name* 命令进入到用户权限表配置模式。

进入用户权限表配置模式：

```
NetEye@root-system]permission tables test
NetEye@root-system-permissiontable-test]
```

- **Profile 配置模式**

在全局配置模式下，可以输入 **profile mode** *profile_name* 命令进入到 Profile 配置模式。

进入 Profile 配置模式：

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]
```

管理级别

NetEye 的管理员按照操作权限范围可分为五种角色：

- 根管理员 （Root Administrator）
- 根系统管理员 （Administrator）
- 根系统审计员 （Auditor）
- Vsys 管理员 （Vsys Administrator）
- Vsys 审计员 （Vsys Auditor ）

命令结构

本手册命令构成有三种情况：一是由单独的关键字组成；二是关键字与关键字的组合；三是关键字与参数的组合。

范例 1: 关键字 **halt**

范例 2: 关键字组合 **show system info**

范例 3: 关键字与参数组合 **`hostname`** *`name`*

特性说明

NetEye 具有缩写、提示以及 Tab 键命令补齐的特性，这些特性可以方便管理员操作。

- **缩写特性**

NetEye 的所有命令都具有缩写输入的特性，以简化复杂命令的输入工作。

例如：

命令的完整格式：**`configure mode`**

命令的缩写格式：**`con mo`**

- **提示特性**

NetEye 的所有命令都具有 “？”提示的特性，以方便指导管理员进行命令配置。管理员可以输入 “？”来显示当前模式下的所有命令列表，或者在命令配置的过程中，输入 “？”来显示当前命令的补齐说明。

- **Tab 键命令补齐**

NetEye 的所有命令都具有 Tab 键命令补齐的特性。管理员在输入命令关键字时可以引用 Tab 键，如果只有唯一条件可以匹配，则补齐当前命令；如果不是唯一条件匹配，则显示所有与当前关键字相似的列表，以备管理员补充输入。

相关文档

除了本手册，管理员还可获得产品附带的以下文档：

- *东软 NetEye 防火墙快速向导*
- *东软 NetEye 防火墙软件 V3.2.4 用户使用指南*
- *东软 NetEye 安全集中管理平台 V1.1 用户使用指南*

1 系统维护命令

主机名

hostname

使用 **hostname** 命令修改系统的主机名称。

命令

hostname *name*

语法

name	主机名称，格式为 WORD<1-24>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 修改系统主机名称为 NetEye。

```
NetEye@root-system]hostname NetEye
```

相关命令

命令名称	描述信息
show hostname	显示系统的主机名称。

show hostname

使用 **show hostname** 命令显示系统的主机名称。

命令

show hostname

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示系统的主机名称。

```
NetEye@root>show hostname
```

【返回结果】

```
  Hostname is NetEye
```

相关命令

命令名称	描述信息
hostname	修改系统主机名称。

License

license download

使用 **license download** 命令下载 License。

命令

license download to {**tftp** *ip_tftp trait_name* | **sftp** *ip_sftp* **username** *user_name* **password** *passwd trait_name* | **x**/**zmodem** *trait_name*}

语法

tftp	简单文件传输协议，表示下载 License 到 TFTP 服务器。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
trait_name	License 特征名，格式为 WORD<1-128>。
sftp	安全文件传输协议，表示下载 License 到 SFTP 服务器。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-64>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-64>。
x/zmodem	异步文件传输协议， Xmodem 或 Zmodem 由系统自动选择。表示通过 x/zmodem 协议下载 License。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V				

模式

该命令在全局配置模式下使用。

范例

范例 1. 下载特征名为 F_SCM 的 License 到 TFTP 服务器 192.168.1.100。

```
NetEye@root-system]license download to tftp 192.168.1.100 F_SCM
```

范例 2. 下载特征名为 F_SCM 的 License 到 SFTP 服务器 192.168.1.126， SFTP 服务器的用户名、密码均为 mike。

```
NetEye@root-system]license download to sftp 192.168.1.126 username mike
password mike F_SCM
```

相关命令

命令名称	描述信息
license import	上载 License 文件。
license word import	上载 License 字符串。

license import

使用 **license import** 命令上载 License 文件。

命令

license import from {**tftp** *ip_tftp file_name* | **sftp** *ip_sftp* **username** *user_name* **password** *passwd file_name* | **x/zmodem**}

语法

tftp	简单文件传输协议，表示从 TFTP 服务器上载 License 文件。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
file_name	License 文件名，格式为 WORD<1-128>。
sftp	安全文件传输协议，表示从 SFTP 服务器上载 License 文件。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-64>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-64>。
x/zmodem	异步文件传输协议， Xmodem 或 Zmodem 由系统自动选择。表示通过 x/zmodem 协议上载 License 文件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V				

模式

该命令在全局配置模式下使用。

范例

范例 1. 从 TFTP 服务器 192.168.1.100 上载 F_SCM.dat 文件到 NetEye。

```
NetEye@root-system]license import from tftp 192.168.1.100 F_SCM.dat
```

范例 2. 从 SFTP 服务器 192.168.1.126 上载 F_SCM.dat 文件到 NetEye， SFTP 服务器的用户名、密码均为 mike。

```
NetEye@root-system]license import from sftp 192.168.1.126 username mike
password mike F_SCM.dat
```

相关命令

命令名称	描述信息
license download	下载 License。
show license	显示 NetEye 的 License 信息。
unset license word	删除 License。

license word import

使用 **license word import** 命令上载 License 字符串。

命令

license word import *string*

语法

string	License 字符串的内容，格式为 LINE。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V				

模式

该命令在全局配置模式下使用。

范例

范例 . 上载 License 字符串。

```
NetEye@root-system]license word import TRAIT FW-VPN-IPS-IPSUP-AS-ASOL-
AV-AVUP-UF-UFOL neusoft perpetual SN=0090FB229F33-5200-1.0
FUNC=#F_FW:C=2000000;V=8;R=80000;U=50000##F_VPN:T=15000;TI=1000;HL=16;
SA=30000##F_IPS##F_IPSUP:ET=20100618##F_AS##F_ASOL:ET=20100618##F_AV##
F_AVUP:ET=20100618##F_UF##F_UFOL:ET=20100618# SIGN=C3A6F036C4C47C42
```

相关命令

命令名称	描述信息
license download	下载 License。
show license	显示 NetEye 的 License 信息。
unset license word	删除 License。

show license

使用 **show license** 命令显示 NetEye 的 License 信息。

命令

show license

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V			

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 NetEye 的 License 信息。

```
NetEye@root>show license
```

【返回结果】

```
License list


       TRAIT FW-VPN-IPS-IPSUP-AS-ASOL-AV-AVUP-UF-UFOL neusoft perpetual
SN=0090FB229F33-5200-1.0
FUNC=#F_FW:C=2000000;V=8;R=80000;U=50000##F_VPN:T=15000;TI=1000;HL=16;S
A=30000##F_IPS##F_IPSUP:ET=20100618##F_AS##F_ASOL:ET=20100618##F_AV##F_
AVUP:ET=20100618##F_UF##F_UFOL:ET=20100618# SIGN=C3A6F036C4C47C42
```

相关命令

命令名称	描述信息
license import	上载 License 文件。
license word import	上载 License 字符串。
unset license word	删除 License。

unset license word

使用 **unset license word** 命令删除 License。

命令

unset license word *trait_name*

语法

trait_name	License 特征名，格式为 WORD<1-128>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V				

模式

该命令在全局配置模式下使用。

范例

范例 . 删除特征名为 F_SCM 的 License。

```
NetEye@root-system]unset license word F_SCM
```

相关命令

命令名称	描述信息
license import	上载 License 文件。
license word import	上载 License 字符串。
show license	显示 NetEye 的 License 信息。

系统时间

ntp authentication enable, disable

使用 **ntp authentication enable, disable** 命令启用或禁用 NTP 认证。

命令

ntp authentication {**enable** | **disable**}

语法

enable | **disable**	• enable— 启用 NTP 认证 • disable— 禁用 NTP 认证 缺省设置为 disable

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令可以在全局配置模式下使用。

ntp auto-syn

使用 **ntp auto-syn** 命令设置自动校时的周期。配置成功后， NetEye 将按照设定的周期自动同步其系统时间。

命令

ntp auto-syn {**month** *month_interval* **day** *day time* | **day** *day_interval time* | **hour** *hour_interval* | **min** *min_interval*}

语法

month_interval	月份间隔值，格式为 INTEGER<1-12>。
day	日期，格式为 INTEGER<1-28>。
time	时间，格式为 HH:MM。
day_interval	日期间隔值，格式为 INTEGER<1-28>。
hour_interval	小时间隔值，格式为 INTEGER<1-23>。
min_interval	分钟间隔值，格式为 INTEGER<1-59>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令可以在全局配置模式下使用。

范例

范例 . 配置自动校时日期为 10 号，每隔 5 个月自动校时一次，并指定具体时间为 12:30。

```
NetEye@root-system]ntp auto-syn month 5 day 10 12:30
```

相关命令

命令名称	描述信息
ntp auto-syn enable, disable	启用或禁用自动校时功能。

ntp auto-syn adjust

使用 **ntp auto-syn adjust** 命令设置 NTP 校时的最大时间误差。配置成功后，如果 NTP 服务器上的时间与本地的时间误差超过该值，则 NetEye 将拒绝同步操作。

命令

ntp auto-syn adjust *max_interval*

语法

max_interval	NTP 校时的最大时间误差，单位为秒，格式为 INTEGER<0-3600>。 缺省值为 3

说明

1. 该命令只对自动校时起作用。
2. 当最大时间误差设置为 0 时，自动校时将不受最大时间误差的限制。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令可以在全局配置模式下使用。

范例

范例 . 设置 NTP 校时的最大时间误差为 360 秒。

```
NetEye@root-system]ntp auto-syn adjust 360
```

ntp auto-syn enable, disable

使用 **ntp auto-syn enable, disable** 命令启用或禁用自动校时功能。

命令

ntp auto-syn {**enable** | **disable**}

语法

enable | **disable**	• enable— 启用自动校时功能 • disable— 禁用自动校时功能 缺省设置为 disable

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令可以在全局配置模式下使用。

相关命令

命令名称	描述信息
ntp auto-syn	设置自动校时的周期。

ntp server

使用 **ntp server** 命令配置 NTP 服务器。配置成功后， NetEye 可以使用该服务器校对其系统时间。

命令

ntp server {**server1** | **server2** | **server3**} {*ip_address* | *domain_name*} [**key_id** *id_num* **key** *password*]

语法

server1	**server2**	**server3**	• sever1— NTP 服务器，其优先级最高。 • sever2— NTP 服务器，其优先级介于 sever1 和 sever3 之间。 • sever3— NTP 服务器，其优先级最低。
ip_address	NTP 服务器的 IP 地址，格式为 x.x.x.x。 地址范围为 1.0.0.0-223.255.255.255。
domain_name	NTP 服务器的域名，格式为 WORD<1-255>。
id_num	密钥 ID，格式为 INTEGER<1-65535>。
password	认证密码，格式为 WORD<1-32>。

说明

不指定 **key_id** *id_num* **key** *password*，表示配置不需要认证的 NTP 服务器。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令可以在全局配置模式下使用。

范例

范例 . 配置需要认证的 NTP 服务器 server2，其 IP 地址为 192.168.1.125，密钥 ID 为 255，认证密码为 newpass。

```
NetEye@root-system]ntp server server2 192.168.1.125 key_id 255 key
newpass
```

相关命令

命令名称	描述信息
unset ntp server	删除指定的 NTP 服务器。

ntp synchronize

使用 **ntp synchronize** 命令对 NetEye 进行立即校时。

命令

ntp synchronize

说明

立即校时不受最大时间误差的限制。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令可以在全局配置模式下使用。

show current timezone

使用 **show current timezone** 命令显示 NetEye 的当前时区以及夏令时的状态。

命令

show current timezone

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 NetEye 的当前时区以及夏令时的状态。

```
NetEye@root> show current timezone
```

【返回结果】

```
current timezone is:392 -> (GMT+08:00) China/Shanghai (Beijing)
```

show system time

使用 **show system time** 命令显示系统的当前时间。

命令

show system time

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

说明

Auditor、 Vsys administrator 和 Vsys Auditor 管理员也可以使用 **show system time** 命令。

模式

该命令在普通配置模式下使用。

范例

范例 . 显示系统时间信息。

```
NetEye@root>show system time
```

【返回结果】

```
Current time: 2008-11-20 17:00:05
Last Synchronization time: 0000-00-00 00:00:00
Last Synchronization method: not set
Auth: false
Primary Server:
Backup Server1:
Backup Server2:
Auto update time : false
```

show timezone

使用 **show timezone** 命令显示 NetEye 当前可以设置的所有时区以及该时区的 ID 号。

命令

show timezone

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 NetEye 当前可以设置的所有时区以及该时区的 ID 号。

```
NetEye@root>show timezone
```

【返回结果】

```
TimeZoneID ->  Description

0 -> (GMT-11:00) Westen Samoa/Apia
1 -> (GMT-11:00) USA/Midway
2 -> (GMT-11:00) Independent State of Samoa/Samoa
3 -> (GMT-11:00) East Samoa/Pago Pago
4 -> (GMT-11:00) Niue
5 -> (GMT-10:00) USA/Adak
6 -> (GMT-10:00) USA/Honolulu
7 -> (GMT-10:00) USA/Atka
8 -> (GMT-10:00) Tahiti/Tahiti
9 -> (GMT-10:00) Tokelau/Fakaofo
10 -> (GMT-10:00) Johnston
11 -> (GMT-10:00) Rarotonga
12 -> (GMT-10:00) USA/Aleutian
13 -> (GMT-10:00) USA/Hawaii
14 -> (GMT-09:00) USA/Anchorage
15 -> (GMT-09:00) USA/Juneau
```

```
16 -> (GMT-09:00) USA/Yakutat
17 -> (GMT-09:00) USA/Nome
18 -> (GMT-09:00) Polynesia/Gambier
19 -> (GMT-09:00) USA/Alaska
20 -> (GMT-08:00) Mexico/Tijuana
......
433 -> (GMT+11:00) Kosrae
434 -> (GMT+11:00) Ponape
435 -> (GMT+11:00) Guadalcanal
436 -> (GMT+12:00) McMurdo
437 -> (GMT+12:00) South Pole
438 -> (GMT+12:00) Russia/Kamchatka
439 -> (GMT+12:00) Russia(Siberian)/Anadyr
440 -> (GMT+12:00) TUVALU/Funafuti
441 -> (GMT+12:00) New Zealand/Auckland
442 -> (GMT+12:00) Kwajalein
443 -> (GMT+12:00) Nauru
444 -> (GMT+12:00) Wake
445 -> (GMT+12:00) Majuro
446 -> (GMT+12:00) Tarawa
447 -> (GMT+12:00) Wallis
448 -> (GMT+12:00) Fiji
449 -> (GMT+13:00) Enderbury
450 -> (GMT+13:00) Tongatapu
451 -> (GMT+14:00) Kiribati/Kiritimati
```

time

使用 **time** 命令设置系统的当前时间。

命令

time *date time*

语法

date	日期，格式为 YYYY-MM-DD。
time	时间，格式为 HH:MM:SS。

说明

NetEye 系统允许设置的时间范围是 1970 年 1 月 1 日 -2037 年 12 月 31 日。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令可以在全局配置模式下使用。

相关命令

命令名称	描述信息
show system time	显示系统的当前时间。

timezone

使用 **timezone** 命令设置 NetEye 系统时区。

命令

timezone *timezone_id*

语法

timezone_id	时区的 ID 号，格式为 INTEGER<0-451>。 缺省值为 392

说明

当用户修改时区后，需要保存当前配置，并重新启动 NetEye 系统，否则将会使日志时间不同步。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 设置 NetEye 的时区为 Singapore，其时区号为 390。

```
NetEye@root-system]timezone 390
```

相关命令

命令名称	描述信息
show current timezone	显示 NetEye 的当前时区以及夏令时的状态。

timezone dst off

使用 **timezone dst off** 命令关闭夏令时。

命令

timezone dst off

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
timezone dst on default	启用缺省设置的夏令时。

timezone dst on default

使用 **timezone dst on default** 命令启用缺省设置的夏令时。

命令

timezone dst on default

说明

NetEye 所在的地区必须有规定好的夏令时法，该命令才能生效。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
timezone dst off	关闭夏令时。

timezone dst on manual day-day

使用 **timezone dst on manual day-day** 命令手动设置夏令时。开始和结束时间均为日期。

命令

timezone dst on manual day-day *start_date start_time end_date end_time dstoff_time* [*start_year*]

语法

start_date	开始日期，格式为 MM-DD。
start_time	开始时间，格式为 HH:MM。
end_date	结束日期，格式为 MM-DD。
dstoff_time	时间偏移量，格式为 HH:MM。例如：10：00，表示时间偏移量为 10 小时。
end_time	结束时间，格式为 HH:MM。
start_year	生效起始年份，格式为 YYYY。

说明

1. 不指定 *start_year* 参数，表示每年都生效。
2. 当用户修改夏令时后，需要保存当前配置，并重新启动 NetEye，否则将会使日志时间不同步。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 手动设置夏令时，有效期为从 2010 年开始，每年的 8 月 1 日 8:00 至 10 月 31 日 17:30，时间偏移量为 1 小时。

```
NetEye@root-system]timezone dst on manual day-day 08-01 08:00 10-31
17:30 01:00 2010
```

timezone dst on manual day-week

使用 **timezone dst on manual day-week** 命令手动设置夏令时。开始时间为日期，结束时间为星期。

命令

timezone dst on manual day-week *start_date start_time end_month end_week end_day end_time dstoff_time* [*start_year*]

语法

start_date	开始日期，格式为 MM-DD。
start_time	开始时间，格式为 HH:MM。
end_month	结束月份，格式为 INTEGER<1-12>。
end_week	结束周号，格式为 INTEGER<1-5>。
end_day	结束日期，格式为 <Mon | Tue | Wed | Thu | Fri | Sat | Sun>。
dstoff_time	时间偏移量，格式为 HH:MM。例如：10：00，表示时间偏移量为 10 小时。
end_time	结束时间，格式为 HH:MM。
start_year	生效起始年份，格式为 YYYY。

说明

1. 不指定 *start_year* 参数，表示每年都生效。
2. 当用户修改夏令时后，需要保存当前配置，并重新启动 NetEye，否则将会使日志时间不同步。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 手动设置夏令时，有效期为每年 3 月 1 日的 12:00 至每年 8 月第一个星期日的 12:00，时间偏移量为 1 小时。

```
NetEye@root-system]timezone dst on manual day-week 03-01 12:00 8 1 Sun
12:00 01:00
```

timezone dst on manual week-day

使用 **timezone dst on manual week-day** 命令手动设置夏令时。开始时间为星期，结束时间为日期。

命令

timezone dst on manual week-day *start_month start_week start_day start_time end_date end_time dstoff_time* [*start_year*]

语法

start_month	开始月份，格式为 INTEGER<1-12>。
start_week	开始周号，格式为 INTEGER<1-5>。
start_day	开始日期，格式为 <Mon | Tue | Wed | Thu | Fri | Sat | Sun>。
start_time	开始时间，格式为 HH:MM。
end_date	结束日期，格式为 MM-DD。
end_time	结束时间，格式为 HH:MM。
dstoff_time	时间偏移量，格式为 HH:MM。例如：10：00，表示时间偏移量为 10 小时。
start_year	生效起始年份，格式为 YYYY。

说明

1. 不指定 *start_year* 参数，表示每年都生效。
2. 当用户修改夏令时后，需要保存当前配置，并重新启动 NetEye，否则将会使日志时间不同步。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 手动设置夏令时，有效期为从 2009 年开始，每年 1 月第 2 个星期三的 8:00 至每年 6 月 30 日的 17:30，时间偏移量为 1 小时。

```
NetEye@root-system]timezone dst on manual week-day 1 2 Wed 08:00 06-30
17:30 01:00 2009
```

timezone dst on manual week-week

使用 **timezone dst on manual week-week** 命令手动设置夏令时。开始和结束的时间均为星期。

命令

timezone dst on manual week-week *start_month start_week start_day start_time end_month end_week end_day end_time dstoff_time* [*start_year*]

语法

start_month	开始月份，格式为 INTEGER<1-12>。
start_week	开始周号，格式为 INTEGER<1-5>。
start_day	开始日期，格式为 <Mon | Tue | Wed | Thu | Fri | Sat | Sun>。
start_time	开始时间，格式为 HH:MM。
end_month	结束月份，格式为 INTEGER<1-12>。
end_week	结束周号，格式为 INTEGER<1-5>。
end_day	结束日期，格式为 <Mon | Tue | Wed | Thu | Fri | Sat | Sun>。
end_time	结束时间，格式为 HH:MM。
dstoff_time	时间偏移量，格式为 HH:MM。例如：10：00，表示时间偏移量为 10 小时。
start_year	生效起始年份，格式为 YYYY。

说明

1. 不指定 *start_year* 参数，表示每年都生效。
2. 当用户修改夏令时后，需要保存当前配置，并重新启动 NetEye，否则将会使日志时间不同步。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 手动设置夏令时，有效期为每年 7 月第 1 个星期一的 00:00 至每年 10 月第 4 个星期日的 22:00，时间偏移量为 1 小时。

```
NetEye@root-system]timezone dst on manual week-week 7 1 Mon 00:00 10 4
Sun 22:00 01:00
```

unset ntp server

使用 **unset ntp server** 命令删除指定的 NTP 服务器。

命令

unset ntp server {**server1** | **server2** | **server3**}

语法

server1	**server2**	**server3**	• sever1— 主服务器，其优先级最高。 • sever2— 备份服务器 1，其优先级介于 sever1 和 sever3 之间。 • sever3— 备份服务器 2，其优先级最低。

说明

如果启用 NTP 自动校时，则主 NTP 服务器不能被删除。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令可以在全局配置模式下使用。

相关命令

命令名称	描述信息
ntp server	配置 NTP 服务器。

语言设置

language

使用 **language** 命令设置 NetEye 系统语言，缺省设置为简体中文。

命令

language {**Chinese** | **English**}

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show language	显示 NetEye 系统语言设置。

show language

使用 **show language** 命令显示 NetEye 系统语言设置。

命令

show language

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 NetEye 系统使用的语言。

```
NetEye@root> show language
```

【返回结果】

```
  Firewall Language: Chinese
```

相关命令

命令名称	描述信息
language	设置 NetEye 系统语言。

报警配置

alert-config local-syslog

使用 **alert-config local-syslog** 命令修改本地 SYSLOG 报警策略。系统缺省设置为记录安全等级为 Emergency、 Alert、 Critical 和 Error，模块类型为 Manage、Session、 FW、 VPN 和 IPS 的事件信息。

命令

alert-config local-syslog internal level {**any** | **none** | *secure_level*} **type** {*type_name* | **any** | **none**}

语法

level	表示设置事件的安全等级。
any | none	• any— 表示设置所有安全等级 • none— 表示不设置安全等级
secure_level	事件的安全等级列表，如 Alert、 Error （参见表 3，“事件安全等级列表”）。格式为 WORD<1-128>。
type_name	模块类型列表，如 FW、 VPN （参见表 4，“模块类型列表”）。格式为 WORD<1-128>。
any | none	• any— 表示设置所有模块的类型 • none— 表示不设置模块的类型

表 3 事件安全等级列表

事件等级	等级说明
Emergency	检测到 SYN 攻击， Tear Drop 攻击或者 Ping of Death 攻击时发出的消息。
Alert	根据当前的情形需要立即做出响应的事件，比如 NetEye 受到攻击，或者 license 过期等。
Critical	影响设备功能的关键条件信息，比如高可用性 （HA）状态的改变。
Error	可能影响到设备功能的错误条件信息，比如在防病毒扫描或者与 SSH 服务器通信中的失败信息。
Warning	可能影响到设备功能的警告条件信息，比如链接邮件服务器失败或者认证失败、超时和成功。
Notification	普通事件的通告，包括由管理员初始的配置的改变。
Information	关于系统操作的通用信息。

表 3 事件安全等级列表 (续)

事件等级	等级说明
Debugging	用于 debug 目的的详细信息。

表 4 模块类型列表

模块名称	模块说明
Manage	管理事件。
Session	访问事件 （连接信息）。
FW	防火墙相关功能产生的事件。
VPN	VPN 相关功能产生的事件。
IPS	防攻击部分产生的攻击事件。
Anti-Virus	防病毒事件。
Anti-Spam	反垃圾邮件事件。
URL-Filter	URL 过滤事件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 修改本地 SYSLOG 报警策略。当出现 Critical 和 Error 报警事件时，将事件发送给本地 SYSLOG 服务器。

```
NetEye@root-system]alert-config local-syslog internal level
Critical,Error type any
```

相关命令

命令名称	描述信息
show alert-config local-syslog	显示本地 SYSLOG 报警策略。

alert-config mail

使用 **alert-config mail** 命令添加邮件报警策略。配置成功后， NetEye 以邮件形式将事件发送给指定的接收者。

命令

alert-config mail *alert_name* **server** {*ip_address* | *domain_name*} *port* **sender** *sender* [**user** *account_name* **password** {**simple | cipher**} *passwd*] **subscriber** *mail1,mail2…* **interval** *sent_cycle* **level** {**any** | **none** | *secure_level*} **type** {*type_name* | **any** | **none**}

语法

alert_name	策略名称，格式为 WORD<1-15>。
ip_address	SMTP 服务器的 IP 地址，格式为 x.x.x.x。
domain_name	SMTP 服务器的域名，格式为 WORD<1-255>。
port	SMTP 服务器的端口，格式为 INTEGER<1-65535>。
sender	发送者邮件地址，格式为 WORD<3-255>。
account_name	登录 SMTP 服务器的用户名称，格式为 WORD<1-255>。
simple	表示设置的口令为明文，即用户输入的口令未经过加密处理。
cipher	表示设置的口令为密文，即用户输入的口令是经过加密算法处理过的。
passwd	登录 SMTP 服务器的用户口令，格式为 WORD<1-255>。
mail	接收者的邮件地址列表，格式为 WORD<3-255>。多个接收者之间用逗号分隔，最多可设置 10 个。
interval	表示设置报警邮件的发送周期。
sent_cycle	周期值，以秒为单位，格式为 INTEGER<1-3600>。
level	表示设置事件的安全等级。
any | none	• any— 表示设置所有安全等级 • none— 表示不设置安全等级
secure_level	事件的安全等级列表，如 Alert、 Error （参见表 3，“事件安全等级列表”）。格式为 WORD<1-128>。
type_name	模块类型列表，如 FW、 VPN （参见表 4，“模块类型列表”）。格式为 WORD<1-128>。
any | none	• any— 表示设置所有模块的类型 • none— 表示不设置模块的类型

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加邮件报警策略 test，当出现 Warning 和 Debugging 报警事件时， NetEye 会通过 smtp.163.com 服务器将事件发送给 test1@163.com 和 test2@163.com，发送者为 test@163.com。

```
NetEye@root-system]alert-config mail test server smtp.163.com 25 sender
test@163.com subscriber test1@163.com,test2@163.com interval 60 level
Warning,Debugging type none
```

相关命令

命令名称	描述信息
show alert-config mail	显示邮件报警策略。
unset alert-config mail	删除邮件报警策略。

alert-config snmp-trap

使用 **alert-config snmp-trap** 命令添加 SNMP Trap 报警策略。配置成功后，NetEye 将事件发送给指定的 SNMP 管理端。

命令

alert-config snmp-trap *alert_name* {**v1** *address_list* [**v2c** *address_list*] **level** {**any** | **none** | *secure_level*} **type** {*type_name* | **any** | **none**} | **v2c** *address_list* [**v1** *address_list*] **level** {**any** | **none** | *secure_level*} **type** {*type_name* | **any** | **none**}}

语法

alert_name	策略名称，格式为 WORD<1-15>。
**v1	v2c**	• v1— 版本 1，表示使用 v1 版本格式发送事件 • v2c— 版本 2，表示使用 v2c 版本格式发送事件
address_list	SNMP 管理端 IP 地址列表，格式为 IPV4LIST<1-100>，每个 SNMP 管理端 IP 地址的第一个八位字节不能大于 223。
level	表示设置事件的安全等级。
**any	none**	• any— 表示设置所有安全等级 • none— 表示不设置安全等级
secure_level	事件的安全等级列表，如 Alert、 Error （参见表 3，“事件安全等级列表”）。格式为 WORD<1-128>。
type_name	模块类型列表，如 FW、 VPN （参见表 4，“模块类型列表”）。格式为 WORD<1-128>。
**any	none**	• any— 表示设置所有模块的类型 • none— 表示不设置模块的类型

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 添加 SNMP Trap 报警策略 (要求为 v1 版本)。当出现 Emergency 和 Alert 报警事件时， NetEye 将以 V1 版本的格式发送给 SNMP 管理端 192.168.1.101。

```
NetEye@root-system]alert-config snmp-trap test v1 192.168.1.101 level
Alert,Emergency type any
```

范例 2. 添加 SNMP Trap 报警策略 (要求 v1 和 v2c 版本)。当出现 Emergency 和 Alert 报警事件时， NetEye 将以 v1 版本的格式发送给 SNMP 管理端 192.168.1.199，以 v2c 版本的格式发送给 SNMP 管理端 192.168.1.111。

```
NetEye@root-system]alert-config snmp-trap test v1 192.168.1.199 v2c
192.168.1.111 level Alert,Emergency type none
```

相关命令

命令名称	描述信息
show alert-config snmp-trap	显示 SNMP Trap 报警策略。
unset alert-config snmp-trap	删除 SNMP Trap 报警策略。

alert-config syslog

使用 **alert-config syslog** 命令添加 SYSLOG 报警策略。配置成功后， NetEye 将事件发送给指定的 SYSLOG 服务器。

命令

alert-config syslog *alert_name* **server** *ip_address port* **level** {**any** | **none** | *secure_level*} **type** {*type_name* | **any** | **none**} [**complete** | **simplified**]

语法

alert_name	策略名称，格式为 WORD<1-15>。
ip_address	SYSLOG 服务器的 IP 地址，格式为 x.x.x.x，第一个八位字节不能大于 223。
port	SYSLOG 服务器的端口，格式为 INTEGER<1-65535>。
level	表示设置事件的安全等级。
any | none	• any— 表示设置所有安全等级 • none— 表示不设置安全等级
secure_level	事件的安全等级列表，如 Alert、 Error （参见表 3，“事件安全等级列表”）。格式为 WORD<1-128>。
type_name	模块类型列表，如 FW、 VPN （参见表 4，“模块类型列表”）。格式为 WORD<1-128>。
any | none	• any— 表示设置所有模块的类型 • none— 表示不设置模块的类型
complete | simplified	事件输出格式。 • complete— 表示将整条事件完整地输出。 • simplified— 表示将整条事件精简地输出。

说明

当使用 **alert-config syslog** 命令时，关键字 “**complete | simplified**”的详细输出格式请见如下说明：

1. **complete** 的格式：
2. <pri>MMM dd hh:mm:ss HostName:Vsysname ver-lid-mid-evid Level Mod username rep=xx | Message
3. 注释：<pri>月份 日期 时间 主机名:Vsys名称 事件库版本-语言标识-模块id-事件id 安全等级 模块名称 用户名称 rep= 重复次数 | 事件内容

【举例】<165>Nov 18 14:52:41 NetEye:root 01-02-019-0003 Notice Manage Anonymous rep=1 | User root logged in via web from 10.2.1.119.

4. **simplified** 的格式：

5. <pri>MMM dd hh:mm:ss HostName:Vsysname ver-lid-mid-evid Level Mod
6. 注释：<pri>月份 日期 时间 主机名:Vsys名称 事件库版本-语言标识-模块id-事件id 安全等级 模块名称

【举例】<165>Nov 18 14:52:41 NetEye:root 01-02-019-0003 Notice Manage

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加 SYSLOG 报警策略 (要求为完整输出格式)。当出现 Critical 和 Error 报警事件时， NetEye 将以完整输出的格式发送给 SYSLOG 服务器 192.168.1.102。

```
NetEye@root-system]alert-config syslog test server 192.168.1.102 300
level Critical,Error type none complete
```

相关命令

命令名称	描述信息
show alert-config syslog	显示 SYSLOG 报警策略。
unset alert-config syslog	删除 SYSLOG 报警策略。

alert-config terminal-print

使用 **alert-config terminal-print** 命令修改设置终端打印报警策略。

命令

alert-config terminal-print terminal level {**any** | **none** | *secure_level*} **type** {*type_name* | **any** | **none**}

语法

level	表示设置事件的安全等级。
any | none	• any— 表示设置所有安全等级 • none— 表示不设置安全等级
secure_level	事件的安全等级列表，如 Alert、 Error （参见表 3，“事件安全等级列表”）。格式为 WORD<1-128>。
type_name	模块类型列表，如 FW、 VPN （参见表 4，“模块类型列表”）。格式为 WORD<1-128>。
any | none	• any— 表示设置所有模块的类型 • none— 表示不设置模块的类型

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 修改终端打印报警策略，将 Critical 和 Error 报警事件和任意类型模块的日志信息输出到终端。

```
NetEye@root-system]alert-config terminal-print terminal level
Critical,Error type any
```

相关命令

命令名称	描述信息
show alert-config terminal-print	显示终端打印报警策略。

show alert-config

使用 **show alert-config** 命令显示所有的报警策略。

命令

show alert-config

说明

在返回结果中，用 “0”代表不记录该等级或模块的事件，“1”代表记录该等级或模块的事件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有的报警策略。

```
NetEye@root>show alert-config
```

【返回结果】

```
Alert configuration info:
Type     Name    emerg alert critic err  warn  noti  info  debug
man  ses  fw  vpn  ips  vir  spa  fil
[Local Syslog] internal   1     1     1     1     0     0     0
0     1    1    1   1    1    0    0    0
[Term Print]  terminal   0     0     0     0     0     0     0
0     0    0    0   0    0    0    0    0
```

相关命令

命令名称	描述信息
show alert-config local-syslog	显示本地 SYSLOG 报警策略。
show alert-config mail	显示邮件报警策略。
show alert-config snmp-trap	显示 SNMP Trap 报警策略。

命令名称	描述信息
show alert-config syslog	显示 SYSLOG 报警策略。

show alert-config local-syslog

使用 **show alert-config local-syslog** 命令显示本地 SYSLOG 报警策略。

命令

show alert-config local-syslog

说明

在返回结果中，用 “0”代表不记录该等级或模块的事件，“1”代表记录该等级或模块的事件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示本地的 SYSLOG 报警策略。

```
NetEye@root>show alert-config local-syslog
```

【返回结果】

```
Alert configuration info:
Type     Name    emerg alert critic err  warn  noti  info  debug
man  ses  fw  vpn  ips  vir  spa  fil
[Local Syslog] internal   1     1     1     1     0     0     0
0     1    1    1   1    1    0    0    0
```

相关命令

命令名称	描述信息
alert-config local-syslog	修改本地 SYSLOG 报警策略。

show alert-config mail

使用 **show alert-config mail** 命令显示邮件报警策略。

命令

show alert-config mail [*alert_name*]

语法

alert_name	策略名称，格式为 WORD<1-15>。

说明

1. 如果不指定 *alert_name* 参数，则显示所有的邮件报警策略。
2. 在返回结果中，用 “0”代表不记录该等级或模块的事件，“1”代表记录该等级或模块的事件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有的邮件报警策略。

```
NetEye@root>show alert-config mail
```

【返回结果】

```
Alert configuration info:
Type            Name        emerg  alert critic  err  warn  noti
info  debug  man   ses   fw   vpn   ips   vir  spa  fil
[SMTP]          email1        0     0     0     0     0     0
0     0     0     0     0     0     0    0    0    0
```

相关命令

命令名称	描述信息
alert-config mail	添加邮件报警策略。

命令名称	描述信息
unset alert-config mail	删除邮件报警策略。

show alert-config snmp-trap

使用 **show alert-config snmp-trap** 命令显示 SNMP Trap 报警策略。

命令

show alert-config snmp-trap [*alert_name*]

语法

alert_name	策略名称，格式为 WORD<1-15>。

说明

1. 如果不指定 *alert_name* 参数，则显示所有的 SNMP Trap 报警策略。
2. 在返回结果中，用 “0”代表不记录该等级或模块的事件，“1”代表记录该等级或模块的事件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有的 SNMP Trap 报警策略。

```
NetEye@root>show alert-config snmp-trap
```

【返回结果】

```
Alert configuration info:
Type            Name        emerg  alert critic  err  warn  noti  info
debug  man   ses   fw   vpn   ips   vir   spa   fil
[SNMP Trap]      snmp1          0     0     0     0     0     0     0
0     0     0     0     0     0     0     0     0
```

相关命令

命令名称	描述信息
alert-config snmp-trap	添加 SNMP Trap 报警策略。

命令名称	描述信息
unset alert-config snmp-trap	删除 SNMP Trap 报警策略。

show alert-config syslog

使用 **show alert-config syslog** 命令显示 SYSLOG 报警策略。

命令

show alert-config syslog [*alert_name*]

语法

alert_name	策略名称，格式为 WORD<1-15>。

说明

1. 如果不指定 *alert_name* 参数，则显示所有的 SYSLOG 报警策略。
2. 在返回结果中，用 “0”代表不记录该等级或模块的事件，“1”代表记录该等级或模块的事件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有的 SYSLOG 报警策略。

```
NetEye@root>show alert-config syslog
```

【返回结果】

```
Alert configuration info:
Type            Name        emerg  alert critic  err  warn  noti  info
debug  man   ses   fw   vpn   ips   vir   spa   fil
[Syslog]        aa            1     1     1     1     1     1     1
1     1     1     1     1     1    1     1     1
```

相关命令

命令名称	描述信息
alert-config syslog	添加 SYSLOG 报警策略。

命令名称	描述信息
unset alert-config syslog	删除 SYSLOG 报警策略。

show alert-config terminal-print

使用 **show alert-config terminal-print** 命令显示终端打印报警策略。

命令

show alert-config terminal-print

说明

在返回结果中，用 “0”代表不记录该等级或模块的事件，“1”代表记录该等级或模块的事件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示终端打印报警策略。

```
NetEye@root>show alert-config terminal-print
```

【返回结果】

```
Alert configuration info:
Type            Name        emerg  alert critic  err  warn  noti  info
debug  man   ses   fw   vpn   ips   vir  spa   fil
[Term Print]    terminal        0     0     0     0     0     0     0
0     0     0     0     0     0    0    0     0
```

相关命令

命令名称	描述信息
alert-config terminal-print	修改终端打印报警策略。

unset alert-config

使用 **unset alert-config** 命令删除指定的报警策略。

命令

unset alert-config *alert_name*

语法

alert_name	策略名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除报警策略 test。

```
NetEye@root-system]unset alert-config test
```

相关命令

命令名称	描述信息
unset alert-config mail	删除邮件报警策略。
unset alert-config snmp-trap	删除 SNMP Trap 报警策略。
unset alert-config syslog	删除 SYSLOG 报警策略。

unset alert-config mail

使用 **unset alert-config mail** 命令删除所有的邮件报警策略。

命令

unset alert-config mail

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除所有的邮件报警策略。

```
NetEye@root-system]unset alert-config mail
```

相关命令

命令名称	描述信息
alert-config mail	添加邮件报警策略。
show alert-config mail	显示邮件报警策略。

unset alert-config snmp-trap

使用 **unset alert-config snmp-trap** 命令删除所有的 SNMP Trap 报警策略。

命令

unset alert-config snmp-trap

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除所有的 SNMP Trap 报警策略。

```
NetEye@root-system]unset alert-config snmp-trap
```

相关命令

命令名称	描述信息
alert-config snmp-trap	添加 SNMP Trap 报警策略。
show alert-config snmp-trap	显示 SNMP Trap 报警策略。

unset alert-config syslog

使用 **unset alert-config syslog** 命令删除所有的 SYSLOG 报警策略。

命令

unset alert-config syslog

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除所有的 SYSLOG 报警策略。

```
NetEye@root-system]unset alert-config syslog
```

相关命令

命令名称	描述信息
alert-config syslog	添加 SYSLOG 报警策略。
show alert-config syslog	显示 SYSLOG 报警策略。

系统日志

copy log

使用 **copy log** 命令导出系统中指定的备份日志文件。

命令

copy log *file_name* **to** {**tftp** *ip_tftp* | **x/zmodem** | **sftp** *ip_sftp* **username** *user_name* **password** *passwd*}

语法

file_name	文件名称，格式为 WORD<1-32>。
tftp	简单文件传输协议，表示导出日志到 TFTP 服务器。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
x/zmodem	异步文件传输协议， Xmodem 或 Zmodem 由系统自动选择。表示使用 x/zmodem 协议导出日志。
sftp	安全文件传输协议，表示导出日志到 SFTP 服务器。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-64>。
passwd	登录 SFTP 服务器的用户口令，格式为 WORD<1-64>。

说明

NetEye 将新产生的日志记录在临时文件 messages 中。临时文件具有固定的大小，当临时文件写满后，NetEye 自动将其存储到备份文件中。备份日志文件名的格式为 messages.Y （Y 为文件创建的日期）。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 1. 导出备份日志文件 **messages.20071231** 到 TFTP 服务器 192.168.1.100。

```
NetEye@root>copy log messages.20071231 to tftp 192.168.1.100
```

范例 2. 导出备份日志文件 **messages.20071231** 到 SFTP 服务器 192.168.1.25， SFTP 服务器的用户名、密码均为 mike。

```
NetEye@root>copy log messages.20071231 to sftp 192.168.1.25 username
mike password mike
```

copy log to

使用 **copy log to** 命令将指定的备份日志文件从一种存储介质拷贝到另一种存储介质。

命令

copy log {**cf** | **hd**} *file_name* **to** {**cf** | **hd**}

语法

file_name	文件名称，格式为 WORD<1-32>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 将 CF 卡中的备份日志文件 **messages.20071231** 拷贝到硬盘。

```
NetEye@root>copy log cf messages.20071231 to hd
```

delete log

使用 **delete log** 命令删除存储介质中指定的备份日志文件。

命令

delete log {**cf** | **hd**} *file_name*

语法

file_name	文件名称，格式为 WORD<1-32>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除硬盘中的备份日志文件 messages.200712311212。

```
NetEye@root-system]delete log hd messages.200712311212
```

delete log all

使用 **delete log all** 命令删除所有的日志文件。

命令

delete log all

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show log	显示存储介质中所有的日志文件。

delete log time

使用 **delete log time** 命令删除指定时间范围的备份日志文件。

命令

delete log time *start_date start_time end_date end_time*

语法

start_date	起始日期，格式为 YYYY-MM-DD。
start_time	起始时间，格式为 HH:MM。
end_date	终止日期，格式为 YYYY-MM-DD。
end_time	终止时间，格式为 HH:MM。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除 2009 年 1 月 1 日 13 时至 2009 年 1 月 15 日 15 时的备份日志文件。

```
NetEye@root-system]delete log time 2009-01-01 13:00 2009-01-15 15:00
```

相关命令

命令名称	描述信息
show log file	显示指定时间范围的备份日志文件。

logging media

使用 **logging media** 命令显示当前存储介质列表。

命令

logging media

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在全局配置模式下使用。

范例

范例 . 显示当前存储介质列表。

```
NetEye@root-system]logging media
```

【返回结果】

```
*****Current Media List*****
Hard Disk existing
*****Current Storage Log Media*****
Hard Disk is storing syslog now
```

相关命令

命令名称	描述信息
logging media switch to	切换记录日志的存储介质。

logging media switch to

使用 **logging media switch to** 命令切换记录日志的存储介质。

命令

logging media switch to {**CF** | **HD**}

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V	V		

模式

该命令在全局配置模式下使用。

范例

范例 . 切换记录日志的存储介质为 CF 卡。

```
NetEye@root-system]logging media switch to CF
```

相关命令

命令名称	描述信息
logging media	显示当前存储介质列表。

logging policy

使用 **logging policy** 命令设置日志存储策略。

命令

logging policy {**stop** | **delete**}

说明

1. 选择 **stop** 关键字，表示当存储介质已满时， NetEye 将停止记录日志，对于接收到的日志将直接丢弃。
2. 选择 **delete** 关键字，表示当存储介质已满时，NetEye 将按照日志产生的时间，覆盖产生时间最早的日志文件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置日志存储策略，指定日志存储方式为 stop。

```
NetEye@root-system]logging policy stop
```

show log

使用 **show log** 命令显示存储介质中所有的日志文件。

命令

show log {**cf** | **hd**}

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 CF 卡中的日志信息。

```
NetEye@root>show log cf
```

【返回结果】

```
messages
```

相关命令

命令名称	描述信息
delete log all	删除所有的日志文件。

show log file

使用 **show log file** 命令显示指定时间范围的备份日志文件。

命令

show log file *start_date start_time end_date end_time*

语法

start_date	起始日期，格式为 YYYY-MM-DD。
start_time	起始时间，格式为 HH:MM。
end_date	终止日期，格式为 YYYY-MM-DD。
end_time	终止时间，格式为 HH:MM。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 2007 年 12 月 20 日 8 点至 2007 年 12 月 28 日 9 点 50 分的备份日志文件。

```
NetEye@root>show log file 2007-12-20 8:00 2007-12-28 9:50
```

【返回结果】

```
messages.20071227
```

相关命令

命令名称	描述信息
delete log time	删除指定时间范围的备份日志文件。

show log query

使用 **show log query** 命令显示日志信息。

命令

show log query level {**all** | *secure_level*} **type** {**all** | *type_name*} {**null** | *includefile*} {**0** | **1**} [*keyword*]

语法

secure_level	事件的安全等级列表，如 Alert、 Error （参见表 3，“事件安全等级列表”）。格式为 WORD<1-128>。
type_name	模块类型列表，如 FW、 VPN （参见表 4，“模块类型列表”）。格式为 WORD<1-128>。
includefile	备份日志文件名称，格式为 WORD<1-32>。 **null** 表示不选择任何备份文件。
0	**1**	• 0— 表示关键字大小写敏感 • 1— 表示关键字大小写不敏感
keyword	关键字，表示只显示包含该关键字的日志信息，格式为 WORD<1-100>，不支持中文。

说明

1. 该命令只能显示当前管理员登录的 Vsys 下的日志。
2. 可以选择一个或多个日志级别，例如：all 或 Alert 或 Alert|Error 等。
3. 可以选择一个或多个日志模块类型，例如：all 或 FW 或 FW|VPN 等。
4. 由于中英文日志统一存储在 messages 临时文件中，所以管理员进行中英文切换后看到的日志不是完全显示中文或英文。但是如果管理员切换到某种语言，那么该时刻起所有日志将会以该语言显示。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 Alert 和 Error 安全等级、所有模块的日志信息。

```
NetEye@root>show log query level Alert|Error type all null 0
```

【返回结果】

```
<161>Nov 19 15:12:33 NetEye:root 01-02-019-0004 Alert Manage Anonymous
rep=1 | User  mike logged in failed via web from 10.2.1.119.
<161>Nov 19 17:29:26 NetEye:root 01-02-087-0001 Alert Session attack
rep=1 | Identify the packet with potential attacks: protocol 17, from
10.2.1.81:2425[1] to 10.2.1.128:2425[any] in vsys 0, detected by
SESSION_FLOOD_DETECTOR.
<161>Nov 20 10:23:44 NetEye:root 01-02-019-0004 Alert Manage Anonymous
rep=1 | User  s logged in failed via web from 10.2.1.16.
```

show storage-media state

使用 **show storage-media state** 命令显示移动存储介质的状态。

命令

show storage-media state

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示移动存储介质的状态。

```
NetEye@root>show storage-media state
```

【返回结果】

```
% Storage media already mounted
```

相关命令

命令名称	描述信息
storage media	挂载或卸载移动存储介质。
storage media format	格式化移动存储介质。

storage media

使用 **storage media** 命令挂载或卸载移动存储介质。

命令

storage media HD {**mount** | **unmount**}

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在普通配置模式下使用。

范例

范例 . 卸载硬盘。

```
NetEye@root>storage media HD unmount
```

相关命令

命令名称	描述信息
show storage-media state	显示移动存储介质的状态。

storage media format

使用 **storage media format** 命令格式化移动存储介质。

命令

storage media HD format

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在普通配置模式下使用。

范例

范例 . 格式化硬盘。

```
NetEye@root>storage media HD format
```

相关命令

命令名称	描述信息
show storage-media state	显示移动存储介质的状态。

SNMP 配置

show snmp

使用 **show snmp** 显示 SNMP 的相关信息。

命令

show snmp {**daemon | location | contact**}

语法

daemon | location | contact	• daemon— 表示是否开启了 SNMP 服务。 • location— SNMP 位置信息，用于表示 NetEye 的地点。 • contact— SNMP 联系信息，用于表示管理 NetEye 相关人员的标识及联系方法。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 查看 NetEye 是否开启了 SNMP 服务。

```
NetEye@root>show snmp daemon
```

【返回结果】

```
The SNMP daemon is on
```

show snmp community

使用 **show snmp community** 命令显示指定权限的团体名。

命令

show snmp community {**read-only** | **read-write**}

语法

community	表示团体名。
read-only | read-write	• read-only— 表示团体名权限为 “只读” • read-write— 表示团体名权限为 “可写”

说明

当团体名为只读权限时，表示允许管理站以只读的方式访问 NetEye ；当团体名为读写权限时，表示允许管理站以读写的方式访问 NetEye。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 显示权限为 “只读”的团体名。

```
NetEye@root>show snmp community read-only
```

【返回结果】

```
The SNMP read-only community is green
```

相关命令

命令名称	描述信息
snmp community read-only,read-write	添加指定权限的团体名。
unset snmp community	删除指定权限的团体名。

show snmp usm user

使用 **show snmp usm user** 命令显示 SNMPv3 用户信息。

命令

show snmp usm user [*user_name*]

语法

usm	表示 SNMPv3 中对传输的报文进行加密和解密的模型。
user_name	SNMPv3 用户名称，格式为 WORD<1-63>。

说明

如果不指定具体的 *user_name* 参数，将显示全部 SNMPv3 用户信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 显示全部 SNMPv3 用户信息。

```
NetEye@root>show snmp usm user
```

【返回结果】

```
UserNames            SecurityLevel AuthPro PrivPro Read-Write
Jone                 authPriv      MD5     DES     read-only
Tom                  authNoPriv    MD5             read-write
```

相关命令

命令名称	描述信息
snmp usm user authNoPriv	添加安全等级为只认证不加密的 SNMPv3 用户。

命令名称	描述信息
snmp usm user authPriv	添加安全等级为认证加密的 SNMPv3 用户。
unset snmp usm user	删除 SNMPv3 用户。

snmp community read-only, read-write

使用 **snmp community read-only, read-write** 命令添加指定权限的团体名。

命令

snmp community *community_name* {**read-only** | **read-write**}

语法

community_name	SNMP 的团体名名称，格式为 WORD<1-128>。
read-only	**read-write**	• read-only— 表示团体名权限为 “只读” • read-write— 表示团体名权限为 “可写”

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 添加权限为 “只读”的团体名 Andy。

```
NetEye@root-system]snmp community Andy read-only
```

相关命令

命令名称	描述信息
show snmp community	显示指定权限的团体名。
unset snmp community	删除指定权限的团体名。

snmp contact

使用 **snmp contact** 命令设置 SNMP 联系信息。

命令

snmp contact *contact_string*

语法

contact_string	SNMP 联系信息，格式为 WORD<1-128>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 添加 SNMP 联系信息为 John_12345678。

```
NetEye@root-system] snmp contact John_12345678
```

相关命令

命令名称	描述信息
snmp location	设置 SNMP 位置信息。

snmp daemon on, off

使用 **snmp daemon on, off** 命令开启或者关闭 SNMP 服务。

命令

snmp daemon {**on** | **off**}

语法

on	**off**	• on— 表示开启 SNMP 服务 • off— 表示关闭 SNMP 服务 缺省设置为 off

说明

如果关闭了 SNMP 服务，表示 NetEye 不响应任何 SNMP 请求，管理员也不能查看或修改任何 SNMP 相关属性 （用户、团体名、位置信息和联系信息）。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 开启 SNMP 服务。

```
NetEye@root-system]snmp daemon on
```

snmp location

使用 **snmp location** 命令添加 SNMP 位置信息。

命令

snmp location *location_string*

语法

location_string	SNMP 位置信息，格式为 WORD<1-128>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 添加 SNMP 位置信息为 122-machine04。

```
NetEye@root-system]snmp location 122-machine04
```

相关命令

命令名称	描述信息
snmp contact	设置 SNMP 联系信息。

snmp usm user authNoPriv

使用 **snmp usm user authNoPriv** 命令添加安全等级为只认证不加密的 SNMPv3 用户。

命令

snmp usm user *user_name* **seclvl authNoPriv authpro MD5 authpassphrase** *authpassphrase_string* {**read-only** | **read-write**}

语法

usm	表示 SNMPv3 中对传输的报文进行加密和解密的模型。
user_name	SNMPv3 用户名称，格式为 WORD<1-63>。
seclvl	表示为用户设定安全级级别。
authNoPriv	表示用户的安全等级为只认证不加密。
authpro MD5	表示认证的时候使用 MD5 加密算法。
authpassphrase	表示设置认证密钥。
authpassphrase_string	认证密钥，格式为 WORD<8-128>。
read-only | read-write	• read-only— 表示用户权限为 “只读” • read-write—表示用户权限为 “可写”

说明

1. 在 NetEye 系统中，最多可以创建 5 个 SNMPv3 用户（包括加密和不加密的 SNMPv3 用户）。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 添加一个安全等级为只认证不加密的只读权限的 SNMPv3 用户 hello，该用户的认证密钥为 niumeng126 。

```
NetEye@root-system]snmp usm user hello seclvl authNoPriv authpro MD5
authpassphrase niumeng126 read-only
```

相关命令

命令名称	描述信息
show snmp usm user	显示 SNMPv3 用户信息。
unset snmp usm user	删除 SNMPv3 用户。

snmp usm user authPriv

使用 **snmp usm user authPriv** 命令添加安全等级为认证加密的 SNMPv3 用户。

命令

snmp usm user *user_name* **seclvl authPriv authpro MD5 authpassphrase** *authpassphrase_string* **privpro DES privpassphrase** *privpassphrase_string* {**read-only** | **read-write**}

语法

usm	表示 SNMPv3 中对传输的报文进行加密和解密的模型。
user_name	SNMPv3 用户名称，格式为 WORD<1-63>。
seclvl	表示为用户设定安全级级别。
authPriv	表示用户的安全等级为认证加密。
authpro MD5	表示认证的时候使用 MD5 加密算法。
authpassphrase	设置认证密钥。
authpassphrase_string	认证密钥，格式为 WORD<8-128>。
privpro DES	表示传输的时候使用 DES 加密算法。
privpassphrase	设置加密密钥。
privpassphrase_string	加密密钥，格式为 WORD<8-128>。
read-only | read-write	• read-only— 表示用户权限为 “只读” • read-write— 表示用户权限为 “可写”

说明

1. 在 NetEye 系统中，最多可以创建 5 个 SNMPv3 用户（包括加密和不加密的 SNMPv3 用户）。
2. SNMPv3 用户的默认加密类型为 DES，用户不可设置。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 添加一个安全等级为认证加密的只读权限的 SNMPv3 用户 hello，该用户的认证密钥为 niumeng126 ， 加密密钥为 vlantine3351。

```
NetEye@root-system]snmp usm user hello seclvl authPriv authpro MD5
authpassphrase niumeng126 privpro DES privpassphrase vlantine3351 read-
only
```

相关命令

命令名称	描述信息
show snmp usm user	显示 SNMPv3 用户信息。
unset snmp usm user	删除 SNMPv3 用户。

unset snmp community

使用 **unset snmp community** 命令删除指定权限的团体名。

命令

unset snmp community {**read-only** | **read-write**}

语法

read-only | read-write	• read-only— 表示团体名权限为 “只读” • read-write— 表示团体名权限为 “可写”

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 删除权限为 “只读”的团体名。

```
NetEye@root-system]unset snmp community read-only
```

相关命令

命令名称	描述信息
show snmp community	显示指定权限的团体名。
snmp community read-only,read-write	添加指定权限的团体名。

unset snmp usm user

使用 **unset snmp usm user** 命令删除 SNMPv3 用户。

命令

unset snmp usm user [*user_name*]

语法

usm	表示 SNMPv3 中对传输的报文进行加密和解密的模型。
user_name	SNMPv3 用户名称，格式为 WORD<1-63>。

说明

如果不指定具体的 *user_name* 参数，将删除全部 SNMPv3 用户。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 删除全部 SNMPv3 用户。

```
NetEye@root-system]unset snmp usm user
```

相关命令

命令名称	描述信息
show snmp usm user	显示 SNMPv3 用户信息。
snmp usm user authNoPriv	添加安全等级为只认证不加密的 SNMPv3 用户。
snmp usm user authPriv	添加安全等级为认证加密的 SNMPv3 用户。

系统升级

copy patch

使用 **copy patch** 命令在 CF 卡或硬盘间复制增强升级包。

命令

copy patch {**cf** | **hd**} *file_name* {**cf** | **hd**}

语法

file_name	升级包文件的名称，格式为 WORD<1-128>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 在 CF 卡和硬盘间复制增强升级包 patch1。

```
NetEye@root-system]copy patch cf patch1 hd
```

delete package internal

使用 **delete package internal** 命令删除本地存储的升级包，包括安装升级包和增强升级包。

命令

delete package internal *file_name*

语法

file_name	升级包文件的名称，格式为 WORD<1-128>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 删除本地存储的安装升级包 NetEye_FW_4_1_build_18040。

```
NetEye@root-system]delete package internal NetEye_FW_4_1_build_18040
```

相关命令

命令名称	描述信息
package upgrade	安装 NetEye 的升级包，包括安装升级包和增强升级包。
show package internal	显示本地存储的升级包，包括安装升级包和增强升级包。

delete patch

使用 **delete patch** 命令删除增强升级包。

命令

delete patch [**cf** | **hd**] *file_name*

语法

file_name	升级包文件的名称，格式为 WORD<1-128>。

说明

如果不指定 **cf** 或 **hd** 关键字，则表示删除已安装的增强升级包。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 删除 CF 卡上的增强升级包 patch1。

```
NetEye@root-system]delete patch cf patch1
```

相关命令

命令名称	描述信息
package upgrade	安装 NetEye 的升级包，包括安装升级包和增强升级包。
patch enable,disable	启用或禁用增强升级包。
show patch	显示 NetEye 的增强升级包信息。

delete system

使用 **delete system** 命令删除非启用状态的安装升级包。

命令

delete system *file_name*

语法

file_name	升级包文件的名称，格式为 WORD<1-128>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 删除名称为 NetEye_FW_4_1_build_18040 的安装升级包。

```
NetEye@root-system]delete system NetEye_FW_4_1_build_18040
```

相关命令

命令名称	描述信息
package upgrade	安装 NetEye 的升级包，包括安装升级包和增强升级包。
show system-list	显示 NetEye 系统列表。
system switch	切换安装升级包，进入该版本对应的系统。

package upgrade

使用 **package upgrade** 命令安装 NetEye 的升级包，包括安装升级包和增强升级包。

命令

package upgrade from {**tftp** *ip_tftp file_name* | **x/zmodem** | **sftp** *ip_sftp* **username** *user_name* **password** *passwd file_name* | **internal** *file_name*}

语法

tftp	简单文件传输协议，表示通过 TFTP 服务器安装升级包。
ip_tftp	tftp 服务器的 IP 地址，格式为 x.x.x.x。
file_name	升级包文件名，格式为 WORD<1-128>。
x/zmodem	异步文件传输协议， Xmodem 或 Zmodem 由系统自动选择。表示使用 x/zmodem 协议安装升级包。
sftp	安全文件传输协议，表示通过 SFTP 服务器安装升级包。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-64>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-64>。
internal	表示通过 NetEye 本地安装升级包。

说明

1. 升级包的大小不能超过 128M 字节。
2. 当管理员安装升级包时， NetEye 对该升级包的格式进行校验，只有格式正确的升级包才能被安装。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 1. 安装 TFTP 服务器 192.168.1.188 上的升级包 NetEye_FW_4_1_build_19033.install.nes。

```
NetEye@root-system]package upgrade from tftp 192.168.1.188
NetEye_FW_4_1_build_19033.install.nes
```

范例 2. 安装 SFTP 服务器 192.168.1.100 上的升级包 NetEye_FW_4_1_build_19033.install.nes， SFTP 服务器的用户名、密码均为 mike。

```
NetEye@root-system]package upgrade from sftp 192.168.1.100 username
mike password mike NetEye_FW_4_1_build_19033.install.nes
```

相关命令

命令名称	描述信息
delete system	删除非启用状态的安装升级包。
patch enable,disable	启用或禁用增强升级包。
show patch	显示 NetEye 的增强升级包信息。
show system-list	显示 NetEye 系统列表。
system switch	切换安装升级包，进入该版本对应的系统。

patch enable, disable

使用 **patch enable, disable** 命令启用或禁用增强升级包。

命令

patch {**enable** | **disable**} [*file_name*]

语法

enable | **disable**	• enable— 启用增强升级包 • disable— 禁用增强升级包
file_name	升级包文件名，格式为 WORD<1-128>。

说明

如果不指定 *file_name* 参数，则表示启用或禁用所有的增强升级包。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 1. 启用文件名称为 file2 的增强升级包。

```
NetEye@root-system]patch enable file2
```

范例 2. 禁用所有的增强升级包。

```
NetEye@root-system]patch disable
```

相关命令

命令名称	描述信息
delete patch	删除增强升级包。
package upgrade	安装 NetEye 的升级包，包括安装升级包和增强升级包。
show patch	显示 NetEye 的增强升级包信息。

show package internal

使用 **show package internal** 命令显示本地存储的增强升级包。

命令

show package internal

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V			

模式

该命令在普通配置模式下使用。

范例

范例 . 显示本地存储的增强升级包。

```
NetEye@root>show package internal
```

【返回结果】

```
patch1.tgz patch2.tgz
```

相关命令

命令名称	描述信息
delete package internal	删除本地存储的升级包，包括安装升级包和增强升级包。
package upgrade	安装 NetEye 的升级包，包括安装升级包和增强升级包。

show patch

使用 **show patch** 命令显示 NetEye 的增强升级包信息。

命令

show patch

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V			

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 NetEye 的增强升级包信息。

```
NetEye@root>show patch
```

【返回结果】

```
1
     name: patch1
 producer: Neusoft

   enable: no
     desc: test


Total: 1
```

相关命令

命令名称	描述信息
delete patch	删除增强升级包。
package upgrade	安装 NetEye 的升级包，包括安装升级包和增强升级包。
patch enable, disable	启用或禁用增强升级包。

show patch cf, hd

使用 **show patch cf, hd** 命令显示 CF 卡或硬盘上的增强升级包。

命令

show patch {**cf** | **hd**}

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V			

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 CF 卡的增强升级包。

```
NetEye@root>show patch cf
```

【返回结果】

```
patch1
```

相关命令

命令名称	描述信息
delete patch	删除增强升级包。
package upgrade	安装 NetEye 的升级包，包括安装升级包、增强升级包和固件升级包。
patch enable, disable	启用或禁用增强升级包。

show system-list

使用 **show system-list** 命令显示 NetEye 系统列表。

命令

show system-list

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V			

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 NetEye 系统列表。

```
NetEye@root>show system-list
```

【返回结果】

```
NetEye_FW_4_1_build_100005
NetEye_FW_4_1_build_19058 (running)
```

相关命令

命令名称	描述信息
delete system	删除非启用状态的安装升级包。
package upgrade	安装 NetEye 的升级包，包括安装升级包和增强升级包。
system switch	切换安装升级包，进入该版本对应的系统。

system switch

使用 **system switch** 命令切换安装升级包，进入该版本对应的系统。

命令

system switch *file_name*

语法

file_name	升级包文件的名称，格式为 WORD<1-128>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 切换安装升级包，进入 NetEye_FW_4_1_build_19058 版本对应的系统。

```
NetEye@root-system]system switch NetEye_FW_4_1_build_19058
```

相关命令

命令名称	描述信息
delete system	删除非启用状态的安装升级包。
package upgrade	安装 NetEye 的升级包，包括安装升级包和增强升级包。
show system-list	显示 NetEye 系统列表。

技术支持

copy technical-support file

使用 **copy technical-support file** 命令下载技术支持文件。

命令

copy technical-support file *file_name* {**tftp** *ip_tftp* | **x/zmodem | sftp** *ip_sftp* **username** *user_name* **password** *passwd*}

语法

file_name	文件名称，格式为 WORD<1-128>。
tftp	简单文件传输协议，表示下载技术支持文件到 TFTP 服务器上。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
x/zmodem	异步文件传输协议， Xmodem 或 Zmodem 由系统自动选择。表示使用 x/zmodem 协议下载技术支持文件。
sftp	安全文件传输协议，表示下载技术支持文件到 SFTP 服务器上。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-64>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-64>。

说明

下载技术支持文件时，需要指定该文件的扩展名 .tgz。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V			

模式

该命令在普通配置模式下使用。

范例

范例 1. 下载技术支持文件 file1.tgz 到 TFTP 服务器 192.168.1.100 上。

```
NetEye@root>copy technical-support file file1.tgz tftp 192.168.1.100
```

范例 2. 下载技术支持文件 file2.tgz 到 SFTP 服务器 192.168.1.126 上， SFTP 服务器的用户名、密码均为 mike。

```
NetEye@root>copy technical-support file file2.tgz sftp 192.168.1.126
username mike password mike
```

delete technical-support

使用 **delete technical-support** 命令删除技术支持文件。

命令

delete technical-support file *file_name*

语法

file_name	文件名称，格式为 WORD<1-128>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 删除技术支持文件 file1.tgz。

```
NetEye@root-system]delete technical-support file file1.tgz
```

相关命令

命令名称	描述信息
show technical-support	显示技术支持文件列表。
technical-support	创建技术支持文件。

show technical-support

使用 **show technical-support** 命令显示技术支持文件列表。

命令

show technical-support

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V			

模式

该命令在普通配置模式下使用。

范例

范例 . 显示技术支持文件列表。

```
NetEye@root>show technical-support
```

【返回结果】

```
file1.tgz

Total: 1
```

相关命令

命令名称	描述信息
delete technical-support	删除技术支持文件。
technical-support	创建技术支持文件。

technical-support

使用 **technical-support** 命令创建技术支持文件。创建成功后，该文件的默认扩展名为 .tgz。

命令

technical-support *file_name*

语法

file_name	文件名称，格式为 WORD<1-124>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 创建技术支持文件 file1。

```
NetEye@root-system]technical-support file1
```

相关命令

命令名称	描述信息
delete technical-support	删除技术支持文件。
show technical-support	显示技术支持文件列表。

备份和恢复

backup

使用 **backup** 命令备份 NetEye 系统的配置文件。

命令

backup [**entire-unit**] *file_name*

语法

file_name	备份文件名称，格式为 WORD<1-128>。

说明

1. 如果指定 **entire-unit** 关键字，表示备份 NetEye 整机配置文件，此时只有根系统管理员拥有该命令的操作权限；否则，表示备份 NetEye Root 或 Vsys 配置文件，此时根系统管理员和 Vsys 管理员均拥有该命令的操作权限。
2. 根系统中，最多可以存在 5 个整机配置备份文件与 5 个根系统配置备份文件；其他 Vsys 中，最多可以存在 5 个 Vsys 配置备份文件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 备份 NetEye 整机配置文件，备份文件名为 file。

```
NetEye@root-system]backup entire-unit file
```

相关命令

命令名称	描述信息
delete backup	删除 NetEye 的备份文件。
show backup	显示 NetEye 的备份文件。

copy backup

使用 **copy backup** 命令下载 NetEye 的备份文件。

命令

copy backup [**entire-unit**] *file_name* **to** {**x/zmodem** | **tftp** *ip_tftp file_name* | **sftp** *ip_sftp* **username** *user_name* **password** *passwd file_name*}

语法

file_name	文件名称，格式为 WORD<1-128>。
x/zmodem	异步文件传输协议， xmodem 或 zmodem 由系统自动选择。表示使用 x/zmodem 协议下载 NetEye 的备份文件。
tftp	简单文件传输协议，表示将 NetEye 的备份文件下载到 TFTP 服务器。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
sftp	安全文件传输协议，表示将 NetEye 的备份文件下载到 SFTP 服务器。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-64>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-64>。

说明

如果指定 **entire-unit** 关键字，表示下载 NetEye 整机配置备份文件，此时只有根系统管理员拥有该命令的操作权限；否则，表示下载 NetEye Root 或 Vsys 配置备份文件，此时根系统管理员和 Vsys 管理员均拥有该命令的操作权限。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 使用根系统管理员登录 NetEye，下载 NetEye Root 配置备份文件 file1 到 TFTP 服务器 192.168.1.150，保存文件名为 file2。

```
NetEye@root-system]copy backup file1 to tftp 192.168.1.150 file2
```

范例 2. 使用根系统管理员登录 NetEye，下载 NetEye Root 配置备份文件 file1 到 SFTP 服务器 192.168.1.152，保存文件名为 file2， SFTP 服务器的用户名、密码均为 mike。

```
NetEye@root-system]copy backup file1 to sftp 192.168.1.152 username
mike password mike file2
```

相关命令

命令名称	描述信息
restore from	通过远端设备上的备份文件恢复 NetEye。

copy backup internal

使用 **copy backup internal** 命令将 NetEte 本地的备份文件复制到同一存储介质中。

命令

copy backup [**entire-unit**] **internal** *file_name* **to internal** *file_name*

语法

internal	本地存储介质。
file_name	文件名称，格式为 WORD<1-128>。

说明

1. 如果指定 **entire-unit** 关键字，表示复制 NetEye 整机配置备份文件，此时只有根系统管理员拥有该命令的操作权限；否则，表示复制 NetEye Root 或 Vsys 的配置备份文件，此时根系统管理员和 Vsys 管理员均拥有该命令的操作权限。
2. 当根系统中已存在 5 个整机配置备份文件与 5 个根系统配置备份文件时，复制备份文件到本地存储介质操作将失败；当其他 Vsys 中已存在 5 个 Vsys 配置备份文件时，复制备份文件到本地存储介质操作将失败。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 复制 NetEye 的整机配置备份文件 file1 到本地存储介质中，保存文件名为 file2。

```
NetEye@root-system]copy backup entire-unit internal file1 to internal
file2
```

相关命令

命令名称	描述信息
restore from internal	通过本地备份文件恢复 NetEye。

delete backup

使用 **delete backup** 命令删除 NetEye 的备份文件。

命令

delete backup [**entire-unit**] **internal** *file_name*

语法

internal	本地存储介质。
file_name	备份文件名称，格式为 WORD<1-128>。

说明

如果指定 **entire-unit** 关键字，表示删除 NetEye 整机配置备份文件，此时只有根系统管理员拥有该命令的操作权限；否则，表示删除 Root 或 Vsys 的配置备份文件，此时根系统管理员和 Vsys 管理员均拥有该命令的操作权限。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除本地存储介质中的 NetEye 整机配置备份文件 file1。

```
NetEye@root-system]delete backup entire-unit internal file1
```

相关命令

命令名称	描述信息
backup	备份 NetEye 的配置文件。
show backup	显示 NetEye 的备份文件。

restore from

使用 **restore from** 命令通过远端设备上的备份文件恢复 NetEye。

命令

restore from {**x/zmodem** | **tftp** *ip_tftp file_name* | **sftp** *ip_sftp* **username** *user_name* **password** *passwd file_name*}

语法

x/zmodem	异步文件传输协议，xmodem 或 zmodem 由系统自动选择。表示使用 x/zmodem 协议，通过管理员工作站上的备份文件远程恢复 NetEye。
tftp	简单文件传输协议，表示使用 TFTP 服务器上的备份文件恢复 NetEye。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
file_name	备份文件名称，格式为 WORD<1-128>。
sftp	安全文件传输协议，表示使用 SFTP 服务器上的备份文件恢复 NetEye。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-64>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-64>。

说明

1. 恢复根系统的配置时，需要重启 NetEye。
2. 恢复其它 Vsys 系统的配置时，不需要重启 NetEye。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 通过 IP 地址为 192.168.1.220 的 TFTP 服务器上的备份文件 file1 恢复 NetEye。

```
NetEye@root-system]restore from tftp 192.168.1.220 file1
```

范例 2. 通过 IP 地址为 192.168.1.56 的 SFTP 服务器上的备份文件 file1 恢复 NetEye，SFTP 服务器的用户名、密码均为 mike。

```
NetEye@root-system]restore from sftp 192.168.1.56 username mike
password mike file1
```

相关命令

命令名称	描述信息
copy backup	下载 NetEye 的备份文件。

restore from internal

使用 **restore from internal** 命令通过 NetEye 本地的备份文件来恢复 NetEye。

命令

restore from internal [**entire-unit**] *file_name*

语法

file_name	备份文件名称，格式为 WORD<1-128>。

说明

1. 如果指定 **entire-unit** 关键字，表示通过整机配置备份文件恢复 NetEye，此时只有根系统管理员拥有该命令的操作权限；否则，表示通过 Root 或 Vsys 的配置备份文件恢复 NetEye，此时根系统管理员和 Vsys 管理员均拥有该命令的操作权限。
2. 恢复根系统的配置时，需要重启 NetEye。
3. 恢复其它 Vsys 系统的配置时，不需要重启 NetEye。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 通过 NetEye 本地的整机配置备份文件 file1 恢复 NetEye。

```
NetEye@root-system]restore from internal entire-unit file1
```

相关命令

命令名称	描述信息
copy backup internal	将 NetEye 本地的备份文件复制到同一存储介质中。

show backup

使用 **show backup** 命令显示 NetEye 的备份文件。

命令

show backup [**entire-unit**]

说明

如果指定 **entire-unit** 关键字，显示 NetEye 的整机配置备份文件，此时只有根系统管理员拥有该命令的操作权限；否则，显示 Root 或 Vsys 的配置备份文件，此时根系统管理员和 Vsys 管理员均拥有该命令的操作权限。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 NetEye 的整机配置备份文件。

```
NetEye@root>show backup entire-unit
```

【返回结果】

```
global_bak.tgz
```

相关命令

命令名称	描述信息
backup	备份 NetEye 的配置文件。
delete backup	删除 NetEye 的备份文件。

恢复出厂设置

reset

使用 **reset** 命令恢复 NetEye 的配置信息为出厂设置。

命令

reset

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在普通配置模式下使用。

范例

范例 . 恢复 NetEye 的配置信息为出厂设置。

```
NetEye@root>reset
```

重启和关闭

halt

使用 **halt** 命令关闭 NetEye。

命令

halt

说明

如果执行 **halt** 命令，没有保存的设置将丢失。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V			

模式

该命令在普通配置模式下使用。

范例

范例 . 关闭 NetEye。

```
NetEye@root>halt
```

reboot

使用 **reboot** 命令重启 NetEye。

命令

reboot

说明

如果执行 **reboot** 命令，没有保存的信息将丢失。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V			

模式

该命令在普通配置模式下使用。

范例

范例 . 重启 NetEye。

```
NetEye@root>reboot
```

SCM 服务器配置

scm server on, off

使用 **scm server on, off** 命令启用或者禁用 SCM 服务器。

命令

scm server {**on | off**}

语法

on | off	• on— 启用 SCM 服务器 • off— 禁用 SCM 服务器

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 启用 SCM 服务器。

```
NetEye@root-system]scm server on
```

相关命令

命令名称	描述信息
show scm server state	查看 SCM 服务器状态。

show scm server state

使用 **show scm server state** 命令查看 SCM 服务器状态。

命令

show scm server state

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 查看 SCM 服务器状态。

```
NetEye@root>show scm server state
```

【返回结果】

```
Scm server state : off
```

相关命令

命令名称	描述信息
scm server on, off	启用或者禁用 SCM 服务器。

user SCMAdmin password

使用 **user SCMAdmin password** 命令修改 SCM 管理员的密码。

命令

user SCMAdmin password

说明

SCM 管理员的密码缺省为 neteye。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 修改 SCM 管理员的密码为 abcd。

```
NetEye@root-system]user SCMAdmin password
Password(6-127):
Repeat Password(6-127):
```

SCM 客户端配置

scm client key

使用 **scm client key** 命令设置 SCM 服务器和被管理 NetEye 之间认证的 key 值。

命令

scm client key {**simple** *passwd_s* | **cipher** *passwd_c*}

语法

simple	表示设置的口令为明文，即管理员输入的口令未经过加密处理。
passwd_s	明文口令，格式为 WORD<1-127>。
cipher	表示设置的口令为密文，即管理员输入的口令是经过加密算法处理过的。
passwd_c	密文口令，格式为 WORD<1-38>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置 SCM 服务器和被管理 NetEye 之间认证的 key 值为 abcdef。

```
NetEye@root-system]scm client key simple abcdef
```

scm management allow

使用 **`scm management allow`** 允许 SCM Server 连接被管理 NetEye。

命令

scm management allow

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
scm management deny	拒绝 SCM Server 连接被管理 NetEye。

scm management deny

使用 **scm management deny** 拒绝 SCM Server 连接被管理 NetEye。

命令

scm management deny

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
scm management allow	允许 SCM Server 连接被管理 NetEye。

show scm management state

使用 **show scm management state** 命令查看是否允许 SCM Server 连接被管理 NetEye。

命令

show scm management state

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看是否允许 SCM Server 连接被管理 NetEye。

```
NetEye@root>show scm management state
```

【返回结果】

```
scm management state: on
```

相关命令

命令名称	描述信息
scm management allow	允许 SCM Server 连接被管理 NetEye。
scm management deny	拒绝 SCM Server 连接被管理 NetEye。

系统状态

show assetinfo

使用 **show assetinfo** 命令显示 NetEye 的资产信息。

命令

show assetinfo

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 NetEye 的资产信息。

```
NetEye@root>show assetinfo
```

【返回结果】

```
Hardware

Chassis Serial Number :      0090FB229F33
CPU Model :                  Intel(R) Pentium(R) Dual  CPU  E2160  @
1.80GHz
CPU Manufacture :            GenuineIntel
CPU freq :                   1800175000
Memory :                     2048 MB
Disk 0 Model :               TRANSCEND
Disk 0 Capacity :            1018 MB
Disk 1 Model :               Not Installed
Disk 1 Capacity :            0 MB
Platform :                   5200
BIOS Vendor :               Phoenix Technologies6.00 PG
BIOS Version :               6.00 PG
```

```
BIOS Data :                  01/13/2009
Motherboard Revision :
Motherboard Model :


Operating System

Product Model :              5200
Build :                      BUILD200080
Software Version :           4.2
```

show system info, state

使用 **show system info, state** 命令显示系统信息。

命令

show system {**info** | **state** }

语法

info | **state**	• info— 表示显示系统的基本信息 • state— 表示显示系统的状态信息

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 显示系统基本信息。

```
NetEye@root> show system info
```

【返回结果】

```
Product Name:           NISG
Model:                  5200
Software Name:          Neusoft NetEye NISG
Build:                  BUILD200080
Release Time:           2010-01-18 18:57:27
Software Version:       4.2
Installation type:      disk-less
Serial Number:          0090FB229F33
Current Time:           2010-01-19 14:46:39
System Uptime:          0 day 5 hours 00 min
Physical Memory:        2048 MB
Basic MAC:              00:90:FB:22:9F:33
```

show system resource-utilization

使用 **show system resource-utilization** 命令显示系统资源利用率。

命令

show system resource-utilization

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 显示系统资源利用率信息。

```
NetEye@root>show system resource-utilization
```

【返回结果】

```
Resource Utilization:

Vsys  Maximum Resource Limit  Policy Utilization  Session Utilization
NAT Utilization
root       100%                 0.0%                0.0%
0.0%
Vsys1      50%                  0.0%                0.0%
0.0%
Vsys2      80%                  0.0%                0.0%
0.0%
```

配置文件

copy config internal

使用 **copy config internal** 命令导出 NetEye 的配置文件。

命令

copy config internal *file_name* **to** {**tftp** *ip_tftp* | **x/zmodem | sftp** *ip_sftp* **username** *user_name* **password** *passwd*}

语法

file_name	文件名称，格式为 WORD<1-128>。
tftp	简单文件传输协议，表示导出配置文件到 TFTP 服务器。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
x/zmodem	异步文件传输协议， xmodem 或 zmodem 由系统自动选择。表示使用 x/zmodem 协议导出配置文件。
sftp	安全文件传输协议，表示导出配置文件到 SFTP 服务器。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-64>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-64>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 使用 x/zmodem 协议导出配置文件 file1。

```
NetEye@root-system]copy config internal file1 to x/zmodem
```

范例 2. 导出配置文件 file2 到 SFTP 服务器 192.168.1.100， SFTP 服务器的用户名、密码均为 mike。

```
NetEye@root-system]copy config internal file2 to sftp 192.168.1.100
username mike password mike
```

相关命令

命令名称	描述信息
import config from	通过外部服务器导入 NetEye 的配置文件。
import config from x/zmodem	通过 x/zmodem 协议导入 NetEye 的配置文件。

copy config internal to active

使用 **copy config internal to active** 命令将指定的配置文件设置为 NetEye 系统的启动文件。配置成功后，当启动 NetEye 时，自动运行该文件。

命令

copy config internal *file_name* **to active**

语法

file_name	文件名称，格式为 WORD<1-128>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置配置文件 file1 为 NetEye 系统的启动文件。

```
NetEye@root-system]copy config internal file1 to active
```

copy config to

使用 **copy config to** 命令将指定的配置文件复制到指定的存储介质。

命令

copy config {**hd** | **cf**} *pre_file_name* **to** {**hd** | **cf**} *post_file_name*

语法

pre_file_name	原文件名称，格式为 WORD<1-128>。
post_file_name	修改后的文件名称，格式为 WORD<1-128>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 复制 CF 卡中的配置文件 file1 到硬盘中，并将其命名为 file2。

```
NetEye@root-system]copy config cf file1 to hd file2
```

相关命令

命令名称	描述信息
delete config	删除存储介质上指定的配置文件。
show config cf, hd	显示存储介质上的配置文件。

delete config

使用 **delete config** 命令删除存储介质上指定的配置文件。

命令

delete config {**hd** | **cf**} *file_name*

语法

file_name	文件名称，格式为 WORD<1-128>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除 CF 卡上的配置文件 file1。

```
NetEye@root-system]delete config cf file1
```

相关命令

命令名称	描述信息
copy config to	将指定的配置文件复制到指定的存储介质。
show config cf, hd	显示存储介质上的配置文件。

import config from

使用 **import config from** 命令通过外部服务器导入 NetEye 的配置文件。

命令

import config *file_name* **from** {**tftp** *ip_tftp* | **sftp** *ip_sftp* **username** *user_name* **password** *passwd*}

语法

file_name	文件名称，格式为 WORD<1-128>。
tftp	简单文件传输协议，表示从 TFTP 服务器导入配置文件。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
sftp	安全文件传输协议，表示从 SFTP 服务器导入配置文件。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-64>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-64>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 通过 TFTP 服务器 192.168.1.123 导入配置文件 file1。

```
NetEye@root-system]import config file1 from tftp 192.168.1.123
```

范例 2. 通过 SFTP 服务器 192.168.1.100 导入配置文件 file2， SFTP 服务器的用户名、密码均为 mike。

```
NetEye@root-system]import config file2 from sftp 192.168.1.100 username
mike password mike
```

相关命令

命令名称	描述信息
copy config internal	导出 NetEye 的配置文件。

import config from x/zmodem

使用 **import config from x/zmodem** 命令通过 x/zmodem 协议导入 NetEye 的配置文件。

命令

import config from x/zmodem

语法

x/zmodem	异步文件传输协议， xmodem 或 zmodem 由系统自动选择。表示通过 x/zmodem 协议导入配置文件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 通过 x/zmodem 协议导入配置文件。

```
NetEye@root-system]import config from x/zmodem
```

相关命令

命令名称	描述信息
copy config internal	导出 NetEye 的配置文件。

load config

使用 **load config** 命令加载指定的配置文件。

命令

load config internal *file_name*

语法

internal	本地存储介质。
file_name	文件名称，格式为 WORD<1-128>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 加载本地存储介质上的配置文件 file1。

```
NetEye@root-system]load config internal file1
```

save config

使用 **save config** 命令保存 NetEye 系统当前的配置信息。

命令

save config [*file_name*]

语法

file_name	文件名称，格式为 WORD<1-128>。

说明

指定 *file_name* 参数，表示将系统当前的配置保存到指定的文件中；不指定 *file_name* 参数，表示将系统当前的配置保存到默认的文件中。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V		V	

模式

该命令在普通配置模式下使用。

范例

范例 . 保存系统当前的配置信息到默认的文件中。

```
NetEye@root>save config
```

show config

使用 **show config** 命令显示 NetEye 系统的配置信息。

命令

show config [*file_name*]

语法

file_name	文件名称，格式为 WORD<1-128>。

说明

如果不指定 *file_name* 参数，则显示所有的配置文件，否则，显示指定文件的配置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 NetEye 系统所有的配置文件。

```
NetEye@root>show config
```

【返回结果】

```
ne_def.cfg    *
```

show config default

使用 **show config default** 命令显示默认的 NetEye 配置信息。

命令

show config default

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示默认的 NetEye 配置信息。

```
NetEye@root>show config default
```

【返回结果】

```
#
user test administrator password cipher
098f6bcd4621d37356cade4e832627b4f65e5b
user a administrator password cipher
4124bc0a9335c27f5f086f24ba207a4912070c
password cipher 0c23a8bf29a191f10b8aee814737e2a6ec510c
#
 hostname NetEye
 banner vty Neusoft NetEye
 banner console Neusoft NetEye
 console timeout 10
 vty timeout 10
#
language English
#
interface ethernet s4p1
 working-type layer3-interface
 speed auto duplex auto
 auto advertise on
 flow control off
```

```
#
interface ethernet s4p2
 speed auto duplex auto
 auto advertise on
 flow control off
#
interface ethernet s4p3
 speed auto duplex auto
 auto advertise on
 flow control off
#
interface ethernet s4p4
 speed auto duplex auto
 auto advertise on
 flow control off
#
interface ethernet s4p1
 ip address 10.3.1.212 255.255.255.0
 mac address 00:A0:8E:A6:E7:B0
 dvmrp metric 1
 dvmrp ttl 1
 dvmrp disable
--More--
```

show config hd, cf

使用 **show config hd, cf** 命令显示存储介质上的 NetEye 配置文件。

命令

show config {**hd** | **cf**}

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示硬盘上的 NetEye 配置文件。

```
NetEye@root>show config hd
```

【返回结果】

```
ne_def.cfg
```

相关命令

命令名称	描述信息
copy config to	将指定的配置文件复制到指定的存储介质。
delete config	删除存储介质上指定的配置文件。

show current-config

使用 **show current-config** 命令显示 NetEye 系统当前正在运行的配置信息。

命令

show current-config

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 NetEye 系统当前正在运行的配置信息。

```
NetEye@root>show current-config
```

【返回结果】

```
Build running configuration...

Current configuration is : 2507 bytes

#
user test administrator password cipher
098f6bcd4621d37356cade4e832627b4f65e5b
user a administrator password cipher
4124bc0a9335c27f5f086f24ba207a4912070c
password cipher 0c23a8bf29a191f10b8aee814737e2a6ec510c
#
 hostname NetEye
 banner vty Neusoft NetEye
 banner console Neusoft NetEye
 console timeout 10
 vty timeout 10
#
language Chinese
#
```

```
channel 1
#
interface ethernet s4p1
 working-type layer3-interface
 speed auto duplex auto
 auto advertise on
 flow control off
#
interface ethernet s4p2
 speed auto duplex auto
 auto advertise on
 flow control off
#
interface ethernet s4p3
 speed auto duplex auto
 auto advertise on
 flow control off
#
interface ethernet s4p4
 speed auto duplex auto
 auto advertise on
 flow control off
#
vlan 1
 mac address 00:00:00:00:00:00
 dvmrp metric 1
 dvmrp ttl 1
 dvmrp disable
#
interface ethernet s4p1
 ip address 10.3.1.212 255.255.255.0
 mac address 00:A0:8E:A6:E7:B0
 dvmrp metric 1
 dvmrp ttl 1
 dvmrp disable
--More--
```

脚本文件

delete script internal

使用 **delete script internal** 命令删除系统内指定的配置脚本文件。

命令

delete script internal *file_name*

语法

file_name	文件名称，格式为 WORD<1-128>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除系统内的配置脚本文件 test。

```
NetEye@root-system]delete script internal test
```

相关命令

命令名称	描述信息
show script internal	显示系统内的配置脚本文件。

load script internal

使用 **load script internal** 命令运行加载系统内指定的配置脚本文件。

命令

load script internal *file_name*

语法

file_name	文件名称，格式为 WORD<1-128>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 运行加载系统内的配置脚本文件 test。

```
NetEye@root-system]load script internal test
```

相关命令

命令名称	描述信息
show script internal	显示系统内的配置脚本文件。

show script internal

使用 **show script internal** 命令显示系统内的配置脚本文件。

命令

show script internal [*file_name*]

语法

file_name	文件名称，格式为 WORD<1-128>。

说明

如果不指定 *file_name* 参数，则显示系统内所有的脚本文件列表。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示系统内所有的脚本文件列表。

```
NetEye@root>show script internal
```

相关命令

命令名称	描述信息
delete script internal	删除系统内指定的配置脚本文件。
load script internal	运行加载系统内指定的配置脚本文件。

2 调试命令

debug clear

使用 **debug clear** 命令来关闭监听并且恢复所有条件为默认值。

命令

debug clear

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

相关命令

命令名称	描述信息
debug match	设置监听条件。
debug stop	停止监听。

debug dump byte

使用 **debug dump byte** 命令来设置输出包字节标记。

命令

debug dump byte {**all** | **off** | *num*}

语法

all | **off** | *num*	• all— 输出全部包字节 • off— 不输出字节 • *num*— 每个包输出的最多字节数，格式为 INTEGER<1-65535>

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

相关命令

命令名称	描述信息
debug dump hook	设置监听数据包的位置。
debug dump session	设置输出会话标记。

debug dump complex

使用 **debug dump complex** 命令来设置输出详细包头信息的标记。

命令

debug dump complex {**on** | **off**}

语法

on	**off**	• on— 详细解析包头，包括接口，数据链路层，网络层，传输层 • off— 简单包头信息，只用一行打印概要信息

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

相关命令

命令名称	描述信息
debug dump hook	设置监听数据包的位置。
debug dump session	设置输出会话标记。

debug dump hook

使用 **debug dump hook** 命令来设置监听数据包的位置。

命令

debug dump hook {**input** | **output** | **error** | **input_output** | **input_error** | **output_error** | **all** | **clear** | **dnat** | **snat** | **route** | **policy**}

语法

input | **output** | **error** | **input_output** | **input_error** | **output_error** | **all** | **clear** | **dnat** | **snat** | **route** | **policy**	• input—NetEye 接受的原始数据包 • output—NetEye 成功发送的数据包 • error—处理过程中出错的数据包 • input_output —NetEye 接受的原始数据包和成功发送的数据包 • input_error—NetEye 接受的原始数据包和处理过程中出错的数据包 • output_error—NetEye 成功发送的数据包和处理过程中出错的数据包 • all—所有的数据包 • clear—清除 dump 标志 • dnat—NetEye 处理 dnat 的数据包 • snat—NetEye 处理 snat 的数据包 • route—NetEye 处理 route 的数据包 • policy—NetEye 处理 policy 的数据包

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

相关命令

命令名称	描述信息
debug dump byte	设置输出包的字节标记。
debug dump session	设置输出会话标记。

debug dump session

使用 **debug dump session** 命令来设置输出会话标记。

命令

debug dump session {**on** | **off**}

语法

on | **off**	• on— 开启输出会话 • off— 禁用输出会话

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

相关命令

命令名称	描述信息
debug dump byte	设置输出包的字节标记。
debug dump hook	设置监听数据包的位置。

debug file download

使用 **debug file download** 命令下载已经存在的 Debug 文件。

命令

debug file download *file_name* {**tftp** *ip_tftp file_name* | **x/zmodem | sftp** *ip_sftp* **username** *user_name* **password** *passwd file_name*}

语法

download	下载 Debug 文件。
file_name	文件名称，格式为 WORD<1-64>。
tftp	简单文件传输协议，表示下载 Debug 文件到 TFTP 服务器上。
ip_tftp	tftp 服务器的 IP 地址，格式为 x.x.x.x。
x/zmodem	异步文件传输协议。表示使用 x/zmodem 协议下载文件。
sftp	安全文件传输协议，表示下载 Debug 文件到 SFTP 服务器上。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-64>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-64>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 1. 下载 Debug 文件 file1 到 TFTP 服务器 192.168.1.25，保存文件名为 file2。

```
NetEye@root>debug file download file1 tftp 192.168.1.25 file2
```

范例 2. 下载 Debug 文件 file1 到 SFTP 服务器 192.168.1.100，保存文件名为 file2， SFTP 服务器的用户名、密码均为 mike。

```
NetEye@root>debug file download file1 sftp 192.168.1.100 username mike
password mike file2
```

debug file remove

使用 **debug file remove** 命令删除已经存在的 Debug 文件。

命令

debug file remove *file_name*

语法

remove	删除 Debug 文件。
file_name	文件名称，格式为 WORD<1-64>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

debug match

使用 **debug match** 命令设置监听条件。缺省设置为监听全部数据包。

命令

debug match {**ip** {*source_ipaddress* | **any**} {*destination_ipaddress* | **any**} | **protocol** {*num* | **tcp** | **udp** | **icmp** | **arp** | **any**} | **port** {*source_port* | **any**} {*destination_port* | **any**} | **input** {**any** | **ethernet** *ethernet_id* [**vlan** *vlan_num*] | **channel** *channel_id* [**vlan** *vlan_num*] | **vlan** *vlan_num* | **local** | {**rint** | **veth** | **pppoe**} *interface_id*} | **output** {**any** | **ethernet** *ethernet_id* [**vlan** *vlan_num*] | **channel** *channel_id* [**vlan** *vlan_num*] | **vlan** *vlan_num* | **local** | {**rint** | **veth** | **pppoe**} *interface_id*} | **mac** {*source_macaddress* | **any**} {*destination_macaddress* | **any**} | **bidir** {**on** | **off**}}

语法

source_ipaddress	源 IP 地址，格式为 x.x.x.x。 **any** 代表任何 IP 地址。
destination_ipaddress	目的 IP 地址，格式为 x.x.x.x。 **any** 代表任何 IP 地址。
num	协议号，格式为 INTEGER<1-255>。
source_port	源端口号，格式为 INTEGER<1-65535>。 **any** 代表任何端口。
destination_port	目的端口号，格式为 INTEGER<1-65535>。 **any** 代表任何端口。
input	设置接收接口条件。 **any** 代表任意接收接口。
ethernet_id	以太网接口 ID，格式为 WORD<1-6>。
vlan_num	VLAN 号，格式为 INTEGER<1-1023>。
channel_id	通道号，格式为 INTEGER<0-7>。
local	设置为本地接收接口。
rint | **veth** | **pppoe**	• rint— 冗余接口 • veth— 虚拟接口 • pppoe—pppoe 接口
interface_id	接口标识。 1. 如果设置为 **rint** 类型， interface_id 的格式为 INTEGER<1-4>。 2. 如果设置为 **veth** 类型， interface_id 的格式为 WORD<1-1023>。 3. 如果设置为 **pppoe** 类型， interface_id 的格式为 INTEGER<0-7>。
output	设置发送接口条件。
source_macaddress	源 MAC 地址，格式为 HH:HH:HH:HH:HH:HH。 **any** 代表任意 MAC 地址。

destination_macaddress	目的 MAC 地址，格式为 HH:HH:HH:HH:HH:HH。 **any** 代表任意 MAC 地址。
bidir	设置双向查询标记。
on | **off**	• on— 启用双向监听功能 • off— 禁用双向监听功能 缺省设置为 off

说明

如果输入的 *num* 参数小于 256，则匹配数据包 IP 包头的 protocol 字段；如果输入的 *num* 参数大于 255，则匹配数据包以太 （ether）头中的 protocol 字段。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 监听由源 IP 192.168.1.100 至目的 IP 10.1.2.100 的数据包。

```
NetEye@root>debug match ip 192.168.1.100 10.1.2.100
```

相关命令

命令名称	描述信息
debug clear	关闭 debug 并恢复所有条件为默认值。
debug start	开始监听数据包。
debug stop	停止监听。

debug qos

使用 **debug qos** 命令显示当前 Vsys 的入口或出口 QoS 信息。

命令

debug qos {**ingress** | **egress**}

语法

ingress | **egress**	• ingress— 表示入口 QoS 信息 • egress— 表示出口 QoS 信息

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看根系统的出口 QoS 信息

```
NetEye@root>debug qos egress
```

【返回结果】

```
 vsys = 0 on dev = imq0:
 class htb 1:7000 parent 1:ffff rate 8000bit ceil 176000bit burst 1610b/8 mpu
0b overhead 0b cburst 1819b/8 mpu 0b overhead 0b level 6
 Sent 600827 bytes 947 pkt (dropped 0, overlimits 0 requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0
 lended: 0 borrowed: 736 giants: 0
 tokens: 1554000 ctokens: 80182
```

debug qos egress

使用 **debug qos egress** 命令显示接口的出口 QoS 信息。

命令

debug qos egress {**ethernet** *interface_id* | **channel** *channel_id* | **vlan** *vlan_id* | **rint** *rint_id* | **veth** *veth_id* | **pppoe** *pppoe_id* | **tunnel** *tunnel_id*}

语法

interface_id	以太网接口 ID，格式为 WORD<1-6>。
channel_id	Channel 接口 ID，格式为 INTEGER<0-7>。
vlan_id	VLAN 接口 ID，格式为 INTEGER<1-1023>。
rint_id	冗余接口 ID，格式为 INTEGER<1-4>。
veth_id	虚拟接口 ID，格式为 INTEGER<1-1023>。
pppoe_id	PPPoE 接口 ID，格式为 INTEGER<0-7>。
tunnel_id	Tunnel 接口 ID，格式为 INTEGER<1-4095>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看接口 vlan1 的出口 QoS 信息。

```
NetEye@root>debug qos egress vlan 1
```

【返回结果】

```
 l3_ifname = vlan1 on dev = imq0:
 class htb 1:2 parent 1:7000 leaf 2: prio 4 quantum 30000 rate 2400Kbit ceil
8000Kbit burst 4599b/8 mpu 0b overhead 0b cburst 11600b/8 mpu 0b overhead 0b
level 0
 Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0
 lended: 0 borrowed: 0 giants: 0
```

```
tokens: 15333 ctokens: 11600
```

debug qos egress rulename

使用 **debug qos egress rulename** 命令显示指定 QoS 规则的出口 QoS 信息。

命令

debug qos egress rulename *rule_name*

语法

rule_name	QoS 规则名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看 QoS 规则 rule1 的出口 QoS 信息 。

```
NetEye@root>debug qos egress rulename rule1
```

【返回结果】

```
 vsys = 0, profile_id = 126 on dev = imq1:
 class htb 1:7e parent 1:ffff leaf 7e: prio 7 quantum 200000 rate 64000Kbit
ceil 8000Mbit burst 81600b/8 mpu 0b overhead 0b cburst 10001000b/8 mpu 0b
overhead 0b level 0
 Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0
 lended: 0 borrowed: 0 giants: 0
 tokens: 10200 ctokens: 10001
```

debug qos ingress

使用 **debug qos ingress** 命令显示接口的入口 QoS 信息。

命令

debug qos ingress {**ethernet** *interface_id* [**vlan** *vlan_id*] | **channel** *channel_id* [**vlan** *vlan_id*] | **vlan** *vlan_id* | **rint** *rint_id* [**vlan** *vlan_id*] | **veth** *veth_id* | **pppoe** *pppoe_id* | **tunnel** *tunnel_id*}

语法

interface_id	以太网接口 ID，格式为 WORD<1-6>。
vlan_id	VLAN 接口 ID，格式为 INTEGER<1-1023>。
channel_id	Channel 接口 ID，格式为 INTEGER<0-7>。
rint_id	冗余接口 ID，格式为 INTEGER<1-4>。
veth_id	虚拟接口 ID，格式为 INTEGER<1-1023>。
pppoe_id	PPPoE 接口 ID，格式为 INTEGER<0-7>。
tunnel_id	Tunnel 接口 ID，格式为 INTEGER<1-4095>。

说明

如果指定 **vlan** *vlan_id* 可选项，则表示显示 Trunk 模式下以太网接口、 Channel 接口或冗余接口的入口 QoS 信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看接口 vlan2 入口 QoS 信息。

```
NetEye@root>debug qos ingress vlan 2
```

【返回结果】

```
 l3_ifname = vlan2 on dev = imq_in:
 class htb 1:3 parent 1:7000 rate 16000Kbit ceil 80000Kbit burst 21600b/8 mpu
0b overhead 0b cburst 101600b/8 mpu 0b overhead 0b level 5
```

```
Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
rate 0bit 0pps backlog 0b 0p requeues 0
lended: 0 borrowed: 0 giants: 0
tokens: 10800 ctokens: 10160
```

debug start

使用 **debug start** 命令来开始监听数据包。

命令

debug start *time* [*file_name*]

语法

time	监听数据包的时间，单位为秒，格式为 INTEGER<3-14400>。
file_name	输出文件名称，格式为 WORD<1-64>。

说明

如果指定 *file_name* 参数，则会将 debug 信息同时写到相应的文件中。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

相关命令

命令名称	描述信息
debug clear	关闭 debug 并恢复所有条件为默认值。
debug stop	停止监听。

debug stop

使用 **debug stop** 命令来停止监听。

命令

debug stop

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

相关命令

命令名称	描述信息
debug clear	关闭 debug 并恢复所有条件为默认值。
debug start	开始监听数据包。

debug vpn ipsec

使用 **debug vpn ipsec** 命令打印 IPSec debug 信息。

命令

debug vpn ipsec *timeout*

语法

timeout	超时时间，格式为 INTEGER<3-14400>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 打印 IPSec debug 信息，指定超时时间为 100 秒。

```
NetEye@root>debug vpn ipsec 100
```

debug vpn isakmp

使用 **debug vpn isakmp** 命令打印不同级别的 ISAKMP debug 信息。

命令

debug vpn isakmp [**tunnel** *tunnel_name*] {**error** | **basic** | **detail**}

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
error | basic | detail	隧道信息类型。 • error— 错误信息 • basic— 协商状态信息 • detail— 详细信息

说明

如果不指定 *tunnel_name* 参数，则打印所有隧道指定级别的 debug 信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 打印隧道 test 的详细信息。

```
NetEye@root>debug vpn isakmp tunnel test detail
```

相关命令

命令名称	描述信息
unset debug vpn isakmp	关闭打印不同级别 ISAKMP debug 信息。

debug vpn l2tp

使用 **debug vpn l2tp** 命令打印隧道的 L2TP 信息。

命令

debug vpn l2tp

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

相关命令

命令名称	描述信息
unset debug vpn l2tp	关闭打印隧道的 L2TP 信息。

ping

使用 **ping** 命令检查 NetEye 与目的设备是否连通。

命令

ping {*url* | *ip_address*} [*num*]

语法

url	域名，格式为 WORD<1-128>。
ip_address	IP 地址，格式为 x.x.x.x。
num	可选项，发送 ping 包的数量，格式为 INTEGER<1-999999>，缺省值为 4。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 发送 10 个 ping 包来检查 NetEye 与域名为 test.com 的设备是否连通。

```
NetEye@root>ping test.com 10
```

show debug

使用 **show debug** 命令来显示当前监听条件和 Debug 文件。

命令

show debug

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示当前监听条件和 Debug 文件。

```
NetEye@root>show debug
```

【返回结果】

```
Debug Vsys : 0
 Interface : any ---> any
        IP : any ---> any
  Protocol : any
      Port : any ---> any
       Mac : any ---> any
     Bidir : off
      Dump : simple packet
      Hook : none
     Watch : OFF
0 debug file(s)
```

相关命令

命令名称	描述信息
debug dump byte	设置输出包的字节标记。
debug dump hook	设置监听数据包的位置。

命令名称	描述信息
debug dump session	设置输出会话标记。
debug match	设置监听条件。
debug start	开始监听数据包。

show debug vpn

使用 **show debug vpn** 命令显示当前或所有终端的 VPN debug 配置信息。

命令

show debug vpn [**all-tty**]

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

说明

如果选择 **all-tty** 关键字，表示显示所有终端的 debug 配置信息。否则，表示显示当前终端的 debug 配置信息。

模式

该命令在普通配置模式下使用。

范例

范例 . 显示当前终端的 VPN debug 配置信息。

```
NetEye@root>show debug vpn
```

【返回结果】

```
debug setting:
  error debug is on
  tunnel name [test]
   basic debug is on
```

traceroute

使用 **traceroute** 命令检测 NetEye 到目的地之间数据包所经过的路径。

命令

traceroute *ip_address*

语法

ip_address	目的 IP 地址，格式为 x.x.x.x。

说明

traceroute 命令不但可检测网络是否连通，还可查找到在数据包的传输路径中出现问题的地方。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 检测 NetEye 发出的数据包到达 IP 地址为 202.96.13.137 的设备所经过的路径。

```
NetEye@root>traceroute 202.96.13.137
```

unset debug vpn

使用 **unset debug vpn** 命令关闭打印当前或所有终端的 VPN debug 信息。

命令

unset debug vpn [**all-tty**]

说明

如果指定 **all-tty** 关键字，则关闭打印所有终端的 debug 信息。否则，关闭打印当前终端的 debug 信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

unset debug vpn isakmp

使用 **unset debug vpn isakmp** 命令关闭打印不同级别的 ISAKMP debug 信息。

命令

unset debug vpn isakmp [**tunnel** *tunnel_name*]

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。

说明

如果不指定 *tunnel_name* 参数，则关闭打印所有隧道不同级别的 debug 信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

相关命令

命令名称	描述信息
debug vpn isakmp	打印不同级别的 ISAKMP debug 信息。

unset debug vpn l2tp

使用 **unset debug vpn l2tp** 命令关闭打印隧道的 L2TP 信息。

命令

unset debug vpn l2tp

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

相关命令

命令名称	描述信息
debug vpn l2tp	打印隧道的 L2TP 信息。

3 网络配置命令

接口

acname

使用 **acname** 命令设置 AC 名称。

命令

acname *ac_name*

语法

ac_name	AC 名称，格式为 WORD<1-64>。

说明

AC 名称通常是 ADSL Modem 的商标型号或序列号，由 ISP 负责提供，一般情况下不用配置。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 PPPoE 接口配置模式下使用。

相关命令

命令名称	描述信息
unset acname	删除 AC 名称。

active on, off

使用 **active on, off** 命令启用或禁用 PPPoE 接口。

命令

active {**on** | **off**}

语法

on | **off**	• on— 启用 PPPoE 接口 • off— 禁用 PPPoE 接口 缺省设置为 off

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 PPPoE 接口配置模式下使用。

范例

范例 . 启用 PPPoE 接口 ppp0。

```
NetEye@root-system]pppoe 0
NetEye@root-system-pppoe0]active on
```

bind gateway

使用 **bind gateway** 命令添加网关隧道绑定策略。

命令

bind gateway *ip_address* {**tunnel** *tunnel_name* | **tunnelgroup** *tunnelgroup_name*}

语法

ip_address	网关 IP 地址，格式为 x.x.x.x。
tunnel | **tunnelgroup**	• tunnel—VPN 隧道 • tunnelgroup—VPN 隧道组
tunnel_name	VPN 隧道名称，格式为 WORD<1-15>。
tunnelgroup_name	VPN 隧道组名称，格式为 WORD<1-127>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 VPN 隧道接口配置模式下使用。

范例

范例 . 在 Tunnel1 接口上添加网关隧道绑定策略，网关 IP 地址为 192.168.1.111， VPN 隧道为 vpntunnel1。

```
NetEye@root-system]tunnel 1
NetEye@root-system-tunnel1]bind gateway 192.168.1.111 tunnel vpntunnel1
```

相关命令

命令名称	描述信息
show GTB	显示网关隧道绑定信息。
unset bind gateway	删除指定的网关隧道绑定策略。
unset GTB	删除所有网关隧道绑定策略。

channel

使用 **channel** 命令创建以太网通道或者进入指定的以太网通道配置模式。

命令

channel *channel_id*

语法

channel_id	以太网通道 ID，格式为 INTEGER<0-7>。

说明

如果指定 *channel_id* 的以太网通道不存在，则创建一个以 *channel_id* 命名的以太网通道，并进入该以太网通道配置模式。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 创建以太网通道 ch1。

```
NetEye@root-system]channel 1
```

相关命令

命令名称	描述信息
unset channel	删除指定的以太网通道。

default mac

使用 **default mac** 命令获取以太网接口、以太网通道、 VLAN 或冗余接口的默认 MAC 地址。

命令

default mac

说明

以太网接口、以太网通道和冗余接口的模式为三层时，对应接口的 MAC 地址才可以被修改。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Ethernet 接口配置模式、以太网通道配置模式、冗余接口配置模式或 VLAN 配置模式下使用。

相关命令

命令名称	描述信息
mac address	修改接口 MAC 地址。

description

使用 **description** 命令添加、修改或删除接口的备注信息。

命令

description [*string*]

语法

string	备注信息，格式为 LINE。

说明

1. 如果指定 *string* 参数，则表示添加或修改描述信息，否则表示删除描述信息。
2. 如果以太网接口、以太网通道、冗余接口、虚拟接口为二层接口，则只有 Administrator 可执行该命令。
3. 如果以太网接口、以太网通道、冗余接口、虚拟接口为三层或三层共享接口，则 Administrator 和 Vsys Administrator 均可执行该命令。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在接口配置模式或 VLAN 配置模式下使用。

范例

范例 . 添加以太网接口 eth1 的备注信息为 name eth1。

```
NetEye@root-system]interface ethernet 1
NetEye@root-system-if-eth1]description name eth1
```

dhcp client

使用 **dhcp client** 命令在三层接口上启用 DHCP （动态主机配置协议）客户端。配置成功后，此接口会通过 DHCP 服务器自动获得动态 IP 地址。

命令

dhcp client [**webauth**]

语法

webauth	表示获得的地址为 WebAuth 地址。

说明

1. 此处三层接口包括以太网接口、以太网通道、VLAN 接口、冗余接口、虚拟接口，其中在虚拟接口上启用 DHCP 客户端时，关键字 **webauth** 不可选。
2. NetEye 可以同时充当 DHCP 客户端、DHCP 中继代理服务器或 DHCP 服务器，但是一个三层接口只能配置一种角色。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Ethernet 接口配置模式、 Channel 接口配置模式、冗余接口配置模式、虚拟接口配置模式或 VLAN 配置模式下使用。

相关命令

命令名称	描述信息
dhcp update ip address	重新获得动态 IP 地址。
show dhcp interface	显示 DHCP 接口配置信息。
unset dhcp client	删除 DHCP 客户端的设置。

dhcp update ip address

使用 **dhcp update ip address** 命令重新获得动态 IP 地址。

命令

dhcp update ip address

说明

只有接口作为 DHCP 客户端时，管理员才可以通过此命令重新获得动态 IP 地址。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Ethernet 接口配置模式、 Channel 接口配置模式、冗余接口配置模式、虚拟接口配置模式或 VLAN 配置模式下使用。

相关命令

命令名称	描述信息
dhcp client	在三层接口上启用 DHCP 客户端。
unset dhcp client	删除 DHCP 客户端的设置。

flow control on, off

使用 **flow control on, off** 命令启用或禁用对以太网接口的流量控制。

命令

flow control {**on** | **off**}

语法

on | **off**	• on— 启用流量控制功能 • off— 禁用流量控制功能 缺省设置为 off

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 Ethernet 接口配置模式下使用。

范例

范例 . 启用以太网接口 eth1 的流控制状态。

```
NetEye@root-system]interface ethernet 1
NetEye@root-system-if-eth1]flow control on
```

hold ethernet

使用 **hold ethernet** 命令设置隶属于以太网通道的二层以太网接口。

命令

hold ethernet *interface_id*

语法

interface_id	以太网接口 ID 或名称，格式为 WORD<1-64>。

说明

1. 加入到以太网通道的二层以太网接口，必须未被划分到任何 VLAN 或虚拟系统，且未被使用。
2. 一个以太网通道最多只能添加 4 个以太网接口。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 Channel 接口配置模式下使用。

范例

范例 . 设置二层以太网接口 eth1 隶属于以太网通道 ch0。

```
NetEye@root-system]channel 0
NetEye@root-system-if-ch0]hold ethernet 1
```

相关命令

命令名称	描述信息
unset hold ethernet	删除隶属于以太网通道的二层以太网接口。

hold ethernet primary secondary

使用 **hold ethernet primary secondary** 命令设置冗余接口的主备物理接口。

命令

hold ethernet primary *interface_id* **secondary** *interface_id*

语法

primary	主物理接口。
secondary	备用物理接口。
interface_id	以太网接口 ID 或名称，格式为 WORD<1-10>。

说明

主备物理接口不能是同一物理接口。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在冗余接口配置模式下使用。

范例

范例 . 设置冗余接口 rint1 的主备物理接口，主接口为 eth1，备用接口为 eth2。

```
NetEye@root-system]rint 1
NetEye@root-system-rint1]hold ethernet primary eth1 secondary eth2
```

相关命令

命令名称	描述信息
unset ethernet	删除冗余接口的主备接口。

hold ethernet, channel, rint, veth

使用 **hold ethernet, channel, rint, veth** 命令设置隶属于 VLAN 的二层接口。

命令

hold {**ethernet** *interface_id* | **channel** *channel_id_list* | **rint** *rint_id_list* | **veth** *veth_id_list*}

语法

interface_id	以太网接口 ID 或名称，格式为 WORD<1-64>。
channel_id_list	以太网通道 ID 列表，格式为 WORD<1-64>。
rint_id_list	冗余接口 ID 列表，格式为 WORD<1-64>。
veth_id_list	虚拟接口 ID 列表，格式为 WORD<1-64>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 VLAN 配置模式下使用。

范例

范例 . 设置以太网接口 eth2 隶属于 VLAN1。

```
NetEye@root-system]vlan 1
NetEye@root-system-vlan1]hold ethernet 2
```

相关命令

命令名称	描述信息
unset hold ethernet, channel, rint, veth	删除隶属于 VLAN 的二层接口。

hold ethernet, rint

使用 **hold ethernet, rint** 命令设置隶属于 PPPoE 接口的二层以太网接口或二层冗余接口。

命令

hold {**ethernet** *interface_id* | **rint** *rint_id*}

语法

interface_id	以太网接口 ID 或名称，格式为 WORD<1-10>。
rint_id	冗余接口 ID，格式为 INTEGER<1-4>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 PPPoE 接口配置模式下使用。

范例

范例 . 设置以太网接口 eth2 隶属于 PPPoE 接口 ppp1。

```
NetEye@root-system]pppoe 1
NetEye@root-system-pppoe1]hold ethernet 2
```

相关命令

命令名称	描述信息
unset hold ethernet, rint	删除隶属于 PPPoE 接口的二层以太网接口或二层冗余接口。

interface ethernet

使用 **interface ethernet** 命令进入指定的以太网接口配置模式。

命令

interface ethernet *interface_id*

语法

interface_id	以太网接口 ID 或名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 进入以太网接口 eth1 的配置模式。

```
NetEye@root-system]interface ethernet 1
```

ip address

使用 **ip address** 命令添加三层共享接口或者三层接口的 IP 地址。

命令

ip address *ip_address netmask* [**webauth**] [**secondary**]

语法

ip_address	IP 地址，格式为 x.x.x.x。
netmask	子网掩码，格式为 x.x.x.x。
webauth	表示添加的地址为 WebAuth 地址。
secondary	设置从 IP 地址。

说明

1. 如果选择 **secondary** 关键字，表示添加设备的从 IP 地址；如果不选择 **secondary** 关键字，表示将添加设备的主 IP 地址。添加从 IP 地址时，该设备必须指定主 IP 地址。
2. 一个接口，最多可被添加 32 个 IP 地址。
3. 当添加 VPN 隧道接口和虚拟接口的 IP 地址时，关键字 **webauth** 不可选。
4. 当添加 Loopback 接口的 IP 地址时，关键字 **webauth** 和 **secondary** 不可选。
5. 当添加 PPPoE 接口的 IP 地址时，仅能输入参数 *ip_address*。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在接口配置模式或 VLAN 配置模式下使用。

范例

范例 1. 为 eth1 添加主 IP 地址 192.168.1.111，相应的子网掩码 255.255.255.0，并将该 IP 地址设置为 WebAuth 地址。

```
NetEye@root-system]interface ethernet 1
NetEye@root-system-if-eth1]ip address 192.168.1.111 255.255.255.0 webauth
```

范例 2. 为 tunnel1 添加从 IP 地址 192.168.1.23，相应的子网掩码 255.255.255.0。

```
NetEye@root-system]tunnel 1
```

```
NetEye@root-system-tunnel1]ip address 192.168.1.23 255.255.255.0
secondary
```

相关命令

命令名称	描述信息
unset ip address	删除共享接口或三层接口的 IP 地址。

loopback

使用 **loopback** 命令创建环回接口或者进入指定的环回接口配置模式。

命令

loopback *lo_id*

语法

lo_id	环回接口 ID，格式为 INTEGER<1-1023>。

说明

如果指定 *lo_id* 的环回接口不存在，则创建一个以 *lo_id* 命名的环回接口，并进入该环回接口配置模式。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 创建环回接口 lo1。

```
NetEye@root-system]loopback 1
```

相关命令

命令名称	描述信息
unset loopback	删除指定的环回接口。

mac address

使用 **mac address** 命令修改以太网接口、以太网通道、 VLAN 或冗余接口的 MAC 地址。

命令

mac address *mac_address*

语法

mac_address	设备的 MAC 地址，格式为 HH:HH:HH:HH:HH:HH。

说明

以太网接口、以太网通道和冗余接口的模式为三层时，对应接口的 MAC 地址才可以被修改。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Ethernet 接口配置模式、以太网通道配置模式、冗余接口配置模式或 VLAN 配置模式下使用。

范例

范例 . 修改以太网接口 eth1 的 MAC 地址为 00:76:6c:61:00:01。

```
NetEye@root-system]interface ethernet 1
NetEye@root-system-if-eth1]mac address 00:76:6c:61:00:01
```

相关命令

命令名称	描述信息
default mac	获取接口的默认 MAC 地址。

mode

使用 **mode** 命令配置拨号方式。

命令

mode {**auto** | **ondemand**} [**attempts** {*num* | **default**} [**interval** {*interval_time* | **default**}] | **interval** {*interval_time* | **default**} [**attempts** {*num* | **default**}]]

语法

auto	**ondemand**	• auto—自动拨号 • ondemand— 按需拨号 缺省设置为 auto
num	重拨次数，格式为 INTEGER<0-999>。 **default**，缺省值为 0，表示不限制重拨次数。
interval_time	重拨时间间隔，单位为秒，格式为 INTEGER<5-600>。 **default** 表示缺省值为 60 秒。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 PPPoE 接口配置模式下使用。

范例

范例 . 在 ppp0 接口上配置按需拨号方式，重拨次数为 4，重拨时间间隔为 100 秒。

```
NetEye@root-system]pppoe 0
NetEye@root-system-pppoe0]mode ondemand attempts 4 interval 100
```

相关命令

命令名称	描述信息
unset mode	恢复默认拨号配置。

mode ondemand idle

使用 **mode ondemand idle** 命令配置拨号闲置时间，在这个时间内如果没有数据传输，会自动断开拨号连接。

命令

mode ondemand idle {*idle_time*| **default**}

语法

idle_time	闲置间隔，单位为分钟，格式为 INTEGER<0-120>。 **default**，缺省值为 0，表示永远不断开连接。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 PPPoE 接口配置模式下使用。

范例

范例 . 在 ppp0 接口上配置按需拨号的闲置时间为 100 秒。

```
NetEye@root-system]pppoe 0
NetEye@root-system-pppoe0]mode ondemand idle 100
```

相关命令

命令名称	描述信息
unset mode	恢复默认拨号配置。

monitor

使用 **monitor** 命令设置冗余接口的探测方式。

命令

monitor type {**icmp** | **arp**} **interval** *interval_time* **threshold** *num* **ip address** *ip_address*

语法

icmp | **arp**	探测类型。 • icmp—ICMP Ping 方式 • arp— ARP Ping 方式
interval_time	探测间隔，单位为秒，格式为 INTEGER<3-60>。缺省值为 3 秒。
num	探测重试次数，格式为 INTEGER<1-10>。缺省值为 3，表示不限制重试次数。
ip_address	IP 地址，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在冗余接口配置模式下使用。

范例

范例 . 在冗余接口 rint1 上配置探测方式，探测类型为 ARP Ping 方式，探测重试次数为 4，探测间隔为 10 秒， IP 地址为 192.168.1.123。

```
NetEye@root-system]rint 1
NetEye@root-system-rint1]monitor type arp interval 10 threshold 4 ip address 192.168.1.123
```

相关命令

命令名称	描述信息
unset monitor	删除冗余接口的探测方式。

mtu

使用 **mtu** 命令修改三层接口的最大传输单元。

命令

mtu {**default** | *mtu_num*}

语法

default	缺省设置。
mtu_num	最大传输单元。三层接口 （除 Loopback 接口）的 MTU 的格式为 INTEGER<68-1500>， Loopback 接口的 MTU 的格式为 INTEGER<68-65535>。

说明

VPN 隧道接口的 MTU 的缺省值为 1424， Loopback 接口的 MTU 的缺省值为 16436，其他接口的 MTU 的缺省值为 1500。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在接口配置模式 （除虚拟接口配置模式和 PPPoE 接口配置模式）或 VLAN 配置模式下使用。

范例

范例 . 设置三层以太网接口 eth1 的最大传输单元为 1000 bytes。

```
NetEye@root-system]interface ethernet 1
NetEye@root-system-if-eth1]mtu 1000
```

overwrite-default-gateway

使用 **overwrite-default-gateway** 命令覆盖系统默认网关。配置成功后，将从 ISP 获取的 IP 地址作为默认网关。

命令

overwrite-default-gateway

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 PPPoE 接口配置模式下使用。

相关命令

命令名称	描述信息
unset overwrite-default-gateway	禁用覆盖系统默认网关。

overwrite-dns

使用 **overwrite-dns** 命令覆盖系统 DNS。配置成功后，将从 ISP 获取的 DNS 作为默认 DNS。

命令

overwrite-dns

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 PPPoE 接口配置模式下使用。

相关命令

命令名称	描述信息
unset overwrite-dns	禁用覆盖系统 DNS。

port access vlan

使用 **port access vlan** 命令设置二层接口隶属于指定的 VLAN。

命令

port access vlan *vlan_id*

语法

vlan_id	VLAN ID，格式为 INTEGER<1-1023>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 Ethernet 接口配置模式、 Channel 接口配置模式、冗余接口配置模式或虚拟接口配置模式下使用。

范例

范例 . 设置工作模式为 Access 的以太网通道 ch0 隶属于 VLAN1。

```
NetEye@root-system]channel 0
NetEye@root-system-if-ch0]port access vlan 1
```

相关命令

命令名称	描述信息
unset port access vlan	删除二层接口所隶属的 VLAN。

port mode

使用 **port mode** 命令设置二层接口 （除虚拟接口）的工作模式。

命令

port mode {**access** | **trunk**}

语法

access | **trunk**	• access—Access 工作模式，不支持 802.1Q 协议，指定的二层接口只能被划分到一个 VLAN 中。 • trunk— Trunk 工作模式，支持 802.1Q 协议，指定的二层接口被设置为 Trunk 端口，允许多个 VLAN 的数据通过该接口。 缺省设置为 access

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 Ethernet 接口配置模式、 Channel 接口配置模式或冗余接口配置模式下使用。

范例

范例 . 设置以太网接口 eth1 的工作模式为 access。

```
NetEye@root-system]interface ethernet 1
NetEye@root-system-if-eth1]port mode access
```

port trunk allowed vlan

使用 **port trunk allowed vlan** 命令设置指定 Trunk 端口所允许的 VLAN。配置成功后，对允许的 VLAN 中的数据进行 802.1Q 封装。

命令

port trunk allowed vlan *vlan_id_list*

语法

vlan_id_list	VLAN ID 列表，格式为 NUMBER， 1-1023 表示所有存在的 VLAN。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 Ethernet 接口配置模式、 Channel 接口配置模式或冗余接口配置模式下使用。

范例

范例 . 设置 Trunk 端口 ch0 允许所有存在的 VLAN。

```
NetEye@root-system]channel 0
NetEye@root-system-if-ch0]port trunk allowed vlan 1-1023
```

相关命令

命令名称	描述信息
unset port trunk allowed vlan	删除指定 Trunk 端口所允许的 VLAN。

port trunk native vlan

使用 **port trunk native vlan** 命令设置指定 Trunk 端口所允许的 Native VLAN。配置成功后，不对该 VLAN 中的数据进行 802.1Q 封装。

命令

port trunk native vlan *vlan_id*

语法

vlan_id	VLAN ID，格式为 INTEGER<1-1023>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 Ethernet 接口配置模式、 Channel 接口配置模式或冗余接口配置模式下使用。

范例

范例 . 设置 Trunk 端口 ch0 所允许的 Native VLAN 为 VLAN2。

```
NetEye@root-system]channel 0
NetEye@root-system-ch0]port trunk native vlan 2
```

相关命令

命令名称	描述信息
unset port trunk native	删除指定 Trunk 端口所允许的 Native VLAN。

pppoe

使用 **pppoe** 命令创建 PPPoE 接口或者进入指定的 PPPoE 接口配置模式。

命令

pppoe *pppoe_id*

语法

pppoe_id	PPPoE ID，格式为 INTEGER<0-7>。

说明

如果指定 *pppoe_id* 的 PPPoE 接口不存在，则创建一个以 *pppoe_id* 命名的 PPPoE 接口，并进入该 PPPoE 接口配置模式。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 创建 PPPoE 接口 ppp1。

```
NetEye@root-system]pppoe 1
```

相关命令

命令名称	描述信息
unset pppoe	删除指定的 PPPoE 接口。

rint

使用 **rint** 命令创建冗余接口或者进入指定的冗余接口配置模式。

命令

rint *rint_id*

语法

rint_id	冗余接口 ID，格式为 INTEGER<1-4>。

说明

如果指定 *rint_id* 的冗余接口不存在，则创建一个以 *rint_id* 命名的冗余接口，并进入该冗余接口配置模式。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 创建冗余接口 rint1。

```
NetEye@root-system]rint 1
```

相关命令

命令名称	描述信息
unset rint	删除指定的冗余接口。

servicename

使用 **servicename** 命令设置服务名称。

命令

servicename *service_name*

语法

service_name	服务名称，格式为 WORD<1-16>。

说明

服务名称通常是 ISP 的名称或者时 ISP 提供的服务名称，由 ISP 负责提供，一般情况下不用配置。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 PPPoE 接口配置模式下使用。

相关命令

命令名称	描述信息
unset servicename	删除服务名称。

sflow disable

使用 **sflow disable** 命令禁用三层接口的 sFlow 功能。

命令

sflow disable

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在接口配置模式或 VLAN 配置模式下使用。

相关命令

命令名称	描述信息
sflow enable	启用三层接口的 sFlow 功能。

sflow enable

使用 **sflow enable** 命令启用三层接口的 sFlow 功能。

命令

sflow enable instance *instance_name* **direction** {**inbound** | **outbound** | **eitherbound**}

语法

instance_name	实例名称，格式为 WORD<1-15>。
inbound | **outbound** | **eitherbound**	抽样数据来源。 • inbound— 流入数据 • outbound— 流出数据 • eitherbound— 流入和流出数据

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在接口配置模式或 VLAN 配置模式下使用。

范例

范例 . 启用接口 eth1 的 sFlow 功能，并选择实例 Ntars，数据抽样来源为 inbound。

```
NetEye@root-system]interface ethernet 1
NetEye@root-system-if-eth1]sflow enable instance Ntars direction inbound
```

相关命令

命令名称	描述信息
sflow disable	禁用三层接口的 sFlow 功能。

show GTB

使用 **show GTB** 命令显示网关隧道绑定信息。

命令

show interface tunnel *tunnel_id* **GTB**

语法

tunnel_id	VPN 隧道接口 ID，格式为 INTEGER<1-4095>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 VPN 隧道接口 tunnel2 的网关隧道绑定信息。

```
NetEye@root>show interface tunnel 2 GTB
```

【返回结果】

```
IP Address      | Tunnel Name
10.3.1.1        | tunnelgroup1
192.168.1.1     | vpntunnel
```

相关命令

命令名称	描述信息
bind gateway	添加网关隧道绑定策略。
unset bind gateway	删除指定的网关隧道绑定策略。
unset GTB	删除所有网关隧道绑定策略。

show interface

使用 **show interface** 命令查看所有接口的相关信息。

命令

show interface [**brief**]

语法

brief	表示简明信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有接口的简明信息。

```
NetEye@root>show interface brief
```

【返回结果】

```
Name      Active    IP Address          MAC               Held Interface
MTU       Vsys
vlan1     off                           00:00:00:00:00:21   ch0~
1500      vsys1
vlan2     off                           00:00:00:00:00:22
1500      vsys1
vlan3     on                        00:00:00:00:00:23                 1500
root
eth0      on        10.3.1.63/24        00:0C:29:A2:51:B9
1500      root
eth2      on                        00:0C:29:A2:51:CD                 1500
root


Name      Active    IP Address          MAC               Held Interface
MTU       Vsys
ppp2      on
vsys1
```

```
ppp0      on
root

Name      Active    IP Address          MTU       Vsys
tunnel2   on                            1424      root

Name      Active    Mode                Ethlist   Vlan List
rint1     on        Layer2 Access

Name      Active    Mode                Vlan List
veth1               Layer2

Name      Active    Status    Speed     Duplex    Mode                Vlan List
eth0      on        up                            Layer3
eth2      on        up                            Layer3
eth1      on        up                             Layer2 Access       vlan1
```

相关命令

命令名称	描述信息
show interface channel	显示以太网通道信息。
show interface ethernet	显示以太网接口信息。
show interface loopback	显示环回接口信息。
show interface rint	显示冗余接口信息。
show interface tunnel	显示 VPN 隧道接口信息。
show interface veth	显示虚拟接口信息。
show interface vlan	显示 VLAN 信息。

show interface channel

使用 **show interface channel** 命令显示以太网通道信息。

命令

show interface channel [*channel_id* | **brief**]

语法

channel_id	以太网通道 ID，格式为 INTEGER<0-7>。
brief	表示简明信息。

说明

1. 如果不指定 *channel_id* 参数，则显示所有的以太网通道信息。
2. 如果省略 **brief** 关键字，则显示以太网通道的详细信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有以太网通道简明信息。

```
NetEye@root>show interface channel brief
```

【返回结果】

```
Name      Active    Mode               Ethlist            Vlan List
ch0       on        Layer2 Access                         vlan1
ch2       on        Layer3             eth2


Name      Active    IP Address         MAC              Held Interface
MTU       Vsys
ch2       on        10.2.1.1/24        00:63:68:6E:00:1A   eth2
1500      root
```

相关命令

命令名称	描述信息
show interface	显示所有接口信息。

show interface ethernet

使用 **show interface ethernet** 命令显示以太网接口信息。

命令

show interface ethernet [*interface_id* | **brief**]

语法

interface_id	以太网接口 ID，格式为 WORD<1-10>。
brief	表示简明信息。

说明

1. 如果不指定 *interface_id* 参数，则显示所有的以太网接口信息。
2. 如果省略 **brief** 关键字，则显示以太网接口的详细信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有以太网接口的简明信息。

NetEye@root>**show interface ethernet brief**

【返回结果】

```
Name      Active    Status    Speed     Duplex    Mode              Vlan
List
eth0      on        up                          Layer3
eth1      on        up                          Layer2 Access
eth2      on        up                          Layer2 Access

Name      Active    IP Address        MAC             Held Interface
MTU       Vsys
```

```
eth0      on       10.3.1.63/24       00:0C:29:A2:51:B9
1500       root
```

相关命令

命令名称	描述信息
show interface	显示所有接口信息。

show interface loopback

使用 **show interface loopback** 命令显示环回接口信息。

命令

show interface loopback [*lo_id* | **brief**]

语法

lo_id	环回接口 ID，格式为 WORD<1-1024>。
brief	表示简明信息。

说明

1. 如果不指定 *lo_id* 参数，则显示所有的环回接口信息。
2. 如果省略 **brief** 关键字，则显示环回接口的详细信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示虚拟系统 vsys1 的环回接口的详细信息。

NetEye@vsys1>**show interface loopback**

【返回结果】

```
lo1 is on
  RefCount: 0
  MTU: 16436 bytes
  Internet address is
        0.0.0.0/255.255.255.255
  Description:
```

```
lo2 is on
RefCount: 0
MTU: 16436 bytes
Internet address is
      10.3.1.1/255.255.255.0
Description:
```

相关命令

命令名称	描述信息
show interface	显示所有接口信息。

show interface pppoe

使用 **show interface pppoe** 命令显示 PPPoE 接口信息。

命令

show interface pppoe [*pppoe_id* | **brief**]

语法

pppoe_id	PPPoE 接口 ID，格式为 WORD<0-7>。
brief	表示简明信息。

说明

1. 如果不指定 *pppoe_id* 参数，则显示所有的 PPPoE 接口信息。
2. 如果省略 **brief** 关键字，则显示 PPPoE 接口的详细信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有 PPPoE 接口的简明信息。

NetEye@root>**show interface pppoe brief**

【返回结果】

```
Name      Active    IP Address        MAC               Held Interface
MTU        Vsys

ppp0      on                          -
-          root

ppp2      on                          -
-          vsys1
```

相关命令

命令名称	描述信息
show interface	显示所有接口信息。

show interface rint

使用 **show interface rint** 命令显示冗余接口信息。

命令

show interface rint [*rint_id* | **brief**]

语法

rint_id	冗余接口 ID，格式为 WORD<1-4>。
brief	表示简明信息。

说明

1. 如果不指定 *rint_id* 参数，则显示所有的冗余接口信息。
2. 如果省略 **brief** 关键字，则显示冗余接口的详细信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有冗余接口的简明信息。

NetEye@root>**show interface rint brief**

【返回结果】

```
Name      Active    Mode               Ethlist            Vlan List
rint1     on        Layer2 Access
rint2     on        Layer3             eth1~

Name      Active    IP Address         MAC               Held Interface
MTU       Vsys
rint2     on       11.3.1.3/24        00:63:68:6e:00:02   eth1~
1500       root
```

相关命令

命令名称	描述信息
show interface	显示所有接口信息。

show interface tunnel

使用 **show interface tunnel** 命令显示虚拟专用网 （VPN）隧道接口信息。

命令

show interface tunnel [*tunnel_id* | **brief**]

语法

tunnel_id	VPN 隧道接口 ID，格式为 INTEGER<1-4095>。
brief	表示简明信息。

说明

1. 如果不指定 *tunnel_id* 参数，则显示所有的 VPN 隧道接口信息。
2. 如果省略 **brief** 关键字，则显示 VPN 隧道接口的详细信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有 VPN 隧道接口简明信息。

```
NetEye@root> show interface tunnel brief
```

【返回结果】

```
Name      Active    VSYS  MTU     IP Address
tunnel2   on        0   1424
```

相关命令

命令名称	描述信息
show interface	显示所有接口信息。

show interface veth

使用 **show interface veth** 命令显示虚拟接口信息。

命令

show interface veth [*veth_id* | **brief**]

语法

veth_id	虚拟接口 ID，格式为 WORD<1-1023>。
brief	表示简明信息。

说明

1. 如果不指定 *veth_id* 参数，则显示所有的虚拟接口信息。
2. 如果省略 **brief** 关键字，则显示虚拟接口的详细信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有虚拟接口的简明信息。

NetEye@root>**show interface veth brief**

【返回结果】

```
Name      Active    IP Address         MAC            MTU      Virtual Network
Vsys
veth1     On       11.1.1.2/24      00:63:68:6E:00:21   1500     vnet1
root
veth2     On                        00:63:68:6E:00:22   1500     vnet1
vsys1
veth3     On                        00:63:68:6E:00:23   1500     vnet2
vsys2
veth5     On                        00:63:68:6E:00:25   1500     vnet3
vsys2
```

```
veth6    On                    00:63:68:6E:00:26   1500     vnet3
vsys1

Name      Active    Mode               Virtual Network     Vlan List
veth1     On        Layer3             vnet1
veth2     On        Layer3             vnet1
veth3     On        Layer3             vnet2
veth5     On        Layer3             vnet3
veth6     On        Layer3             vnet3
veth7     On        Layer2 Access
```

相关命令

命令名称	描述信息
show interface	显示所有接口信息。

show interface vlan

使用 **show interface vlan** 命令显示 VLAN 信息。

命令

show interface vlan [*vlan_id* | **brief**]

语法

vlan_id	VLAN ID，格式为 INTEGER<1-1023>。
brief	表示简明信息。

说明

1. 如果不指定 *vlan_id* 参数，则显示所有 VLAN 的信息。
2. 如果省略 **brief** 关键字，则显示 VLAN 的详细信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有 VLAN 的简明信息。

```
NetEye@root>show interface vlan brief
```

【返回结果】

```
Name       Active  IP Address        MAC             Held Interfaces MTU
Vsys
vlan1      on                   00:63:68:6E:00:19  ch1             1500
root
vlan2      on                   00:A0:8E:A6:E7:B3  eth-s4p4        1500
root
```

相关命令

命令名称	描述信息
show interface	显示所有接口信息。

shutdown

使用 **shutdown** 命令禁用接口。配置成功后，该接口不能进行数据收发。

命令

shutdown

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在接口配置模式 （除 PPPoE 接口配置模式）或 VLAN 配置模式下使用。

范例

范例 . 禁用以太网接口 eth1。

```
NetEye@root-system]interface ethernet 1
NetEye@root-system-if-eth1]shutdown
```

相关命令

命令名称	描述信息
unset shutdown	启用接口。

speed duplex

使用 **speed duplex** 命令设置以太网接口的连接速度和双工模式。

命令

speed {**10** | **100** | **1000** | **auto**} **duplex** {**half** | **full** | **auto**}

语法

10 | **100** | **1000** | **auto**	• 10— 表示连接速度为 10 Mbit/s • 100— 表示连接速度为 100 Mbit/s • 1000— 表示连接速度为 1000 Mbit/s • auto— 表示连接速度由自动协商确定
half | **full** | **auto**	• half— 半双工 • full— 全双工 • auto— 双工模式由自动协商确定

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 Ethernet 接口配置模式下使用。

范例

范例 . 设置以太网接口 eth1 的双工模式为全双工，连接速度为 1000 Mbit/s。

```
NetEye@root-system]interface ethernet 1
NetEye@root-system-if-eth1]speed 1000 duplex full
```

switch

使用 **switch** 命令进行冗余接口的主备切换。

命令

switch

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在冗余接口配置模式下使用。

tunnel

使用 **tunnel** 命令创建 VPN 隧道接口或进入指定的 VPN 隧道接口配置模式。

命令

tunnel *tunnel_id*

语法

tunnel_id	隧道接口 ID，格式为 INTEGER<1-4095>。

说明

如果指定 *tunnel_id* 的 VPN 隧道接口不存在，则创建一个以 *tunnel_id* 命名的 VPN 隧道接口，并进入该 VPN 隧道接口配置模式。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 进入 VPN 隧道接口 tunnel22 的配置模式。

```
NetEye@root-system]tunnel 22
```

相关命令

命令名称	描述信息
unset tunnel	删除指定的 VPN 隧道接口。

Unnumbered

使用 **Unnumbered** 命令借用其他三层接口的 IP 地址。

命令

Unnumbered *l3_interface_name*

语法

l3_interface_name	三层接口名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 隧道接口配置模式下使用。

范例

范例 .VPN 隧道接口 tunnel1 借用三层接口 eth2 的 IP 地址。

```
NetEye@root-system]tunnel 1
NetEye@root-system-tunnel1]Unnumbered eth2
```

相关命令

命令名称	描述信息
unset Unnumbered	删除借用其他三层接口的 IP 地址。

unset acname

使用 **unset acname** 命令删除 AC 名称。

命令

unset acname

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 PPPoE 接口配置模式下使用。

相关命令

命令名称	描述信息
acname	设置 AC 名称。

unset bind gateway

使用 **unset bind gateway** 命令删除指定的网关隧道绑定策略。

命令

unset bind gateway *ip_address*

语法

ip_address	网关 IP 地址，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 隧道接口配置模式下使用。

范例

范例 . 删除网关隧道绑定策略中 IP 地址为 192.168.1.111 的表项。

```
NetEye@root-system]tunnel 1
NetEye@root-system-tunnel1]unset bind gateway 192.168.1.111
```

相关命令

命令名称	描述信息
bind gateway	添加网关隧道绑定策略。
show GTB	显示网关隧道绑定信息。
unset GTB	删除所有网关隧道绑定策略。

unset channel

使用 **unset channel** 命令删除指定的以太网通道。

命令

unset channel *channel_id*

语法

channel_id	以太网通道 ID，格式为 INTEGER<0-7>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 删除以太网通道 ch1。

```
NetEye@root-system]unset channel 1
```

相关命令

命令名称	描述信息
channel	创建以太网通道或进入以太网通道配置模式。

unset dhcp client

使用 **unset dhcp client** 命令删除 DHCP 客户端的设置。

命令

unset dhcp client

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Ethernet 接口配置模式、 Channel 接口配置模式、冗余接口配置模式、虚拟接口配置模式或 VLAN 配置模式下使用。

相关命令

命令名称	描述信息
dhcp client	在三层接口上启用 DHCP 客户端。
dhcp update ip address	重新获得动态 IP 地址。
show dhcp interface	显示 DHCP 接口配置信息。

unset ethernet

使用 **unset ethernet** 命令删除冗余接口的主备接口。

命令

unset ethernet

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在冗余接口配置模式下使用。

相关命令

命令名称	描述信息
hold ethernet primary secondary	设置主备物理接口。

unset GTB

使用 **unset GTB** 命令删除所有网关隧道绑定策略。

命令

unset GTB

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 VPN 隧道接口配置模式下使用。

相关命令

命令名称	描述信息
bind gateway	添加网关隧道绑定策略。
unset bind gateway	删除指定的网关隧道绑定策略。
unset GTB	删除所有网关隧道绑定策略。

unset hold ethernet

使用 **unset hold ethernet** 命令删除隶属于以太网通道的二层以太网接口。

命令

unset hold ethernet *interface_id*

语法

interface_id	以太网接口 ID 或名称，格式为 WORD<1-64>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 Channel 配置模式下使用。

范例

范例 . 删除隶属于以太网通道 ch0 的二层以太网接口 eth1。

```
NetEye@root-system]channel 0
NetEye@root-system-if-ch0]unset hold ethernet 1
```

相关命令

命令名称	描述信息
hold ethernet	设置隶属于以太网通道的二层以太网接口。

unset hold ethernet, channel, rint, veth

使用 **unset hold ethernet,channel, rint, veth** 命令删除隶属于 VLAN 的二层接口。

命令

unset hold {**ethernet** *interface_id* | **channel** *channel_id_list* | **rint** *rint_id_list* | **veth** *veth_id_list*}

语法

interface_id	以太网接口 ID 或名称，格式为 WORD<1-64>。
channel_id_list	以太网通道 ID 列表，格式为 WORD<1-64>。
rint_id_list	冗余接口 ID 列表，格式为 WORD<1-64>。
veth_id_list	虚拟接口 ID 列表，格式为 WORD<1-64>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 VLAN 配置模式下使用。

范例

范例 . 删除隶属于 VLAN1 的以太网通道 ch0 和 ch2。

```
NetEye@root-system]vlan 1
NetEye@root-system-vlan1]unset hold channel 0,2
```

相关命令

命令名称	描述信息
hold ethernet, channel, rint, veth	设置隶属于 VLAN 的二层接口。

unset hold ethernet, rint

使用 **unset hold ethernet, rint** 命令删除隶属于 PPPoE 接口的二层物理接口或二层冗余接口。

命令

unset hold {**ethernet** *interface_id* | **rint** *rint_id*}

语法

interface_id	以太网接口 ID 或名称，格式为 WORD<1-10>。
rint_id	冗余接口 ID，格式为 INTEGER<1-4>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 PPPoE 接口配置模式下使用。

范例

范例 . 删除隶属于 PPPoE 接口 ppp1 的二层物理接口 eth2。

```
NetEye@root-system]pppoe 1
NetEye@root-system-pppoe1]unset hold ethernet 2
```

相关命令

命令名称	描述信息
hold ethernet, rint	指定隶属于 PPPoE 的二层物理接口或二层冗余接口。

unset ip address

使用 **unset ip address** 命令删除三层共享接口或者三层接口的 IP 地址。

命令

unset ip address [*ip_address netmask*]

语法

ip_address	IP 地址，格式为 x.x.x.x。
netmask	子网掩码，格式为 x.x.x.x。

说明

1. 如果不指定 *ip_address* 及 *netmask* 参数，将删除所有的 IP 地址。
2. Loopback 接口的 IP 地址不能被删除。
3. PPPoE 接口只能使用 **unset ip address** 命令。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在接口配置模式或 VLAN 配置模式下使用。

范例

范例 . 删除共享以太网接口 eth1 的地址为 192.168.1.111，相应的子网掩码为 255.255.255.0 的 IP 地址。

```
NetEye@root-system]interface ethernet 1
NetEye@root-system-if-eth1]unset ip address 192.168.1.111 255.255.255.0
```

相关命令

命令名称	描述信息
ip address	添加三层共享接口或者三层接口的 IP 地址。

unset loopback

使用 **unset loopback** 命令删除指定的环回接口。

命令

unset loopback *lo_id*

语法

lo_id	环回接口 ID，格式为 INTEGER<1-1023>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
loopback	创建以太网通道或进入以太网通道配置模式。

unset mode

使用 **mode** 命令删除拨号方式配置，恢复默认设置。

命令

unset mode

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 PPPoE 接口配置模式下使用。

相关命令

命令名称	描述信息
mode	配置拨号方式。

unset monitor

使用 **unset monitor** 命令删除冗余接口的探测方式。

命令

unset monitor type {**icmp** | **arp**} **ip address** *ip_address*

语法

icmp | **arp**	探测类型。 • icmp—ICMP Ping 方式 • arp— ARP Ping 方式
ip_address	IP 地址，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在冗余接口配置模式下使用。

范例

范例 . 删除冗余接口 rint1 上配置的探测方式，探测类型为 ARP Ping 方式， IP 地址为 192.168.1.123。

```
NetEye@root-system]rint 1
NetEye@root-system-rint1]unset monitor type arp ip address 192.168.1.123
```

相关命令

命令名称	描述信息
monitor	设置冗余接口的探测方式。

unset overwrite-default-gateway

使用 **unset overwrite-default-gateway** 命令禁用覆盖系统默认网关。

命令

unset overwrite-default-gateway

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 PPPoE 接口配置模式下使用。

相关命令

命令名称	描述信息
overwrite-default-gateway	覆盖系统默认网关。

unset overwrite-dns

使用 **usnet overwrite-dns** 命令禁用覆盖系统 DNS。

命令

unset overwrite-dns

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 PPPoE 接口配置模式下使用。

相关命令

命令名称	描述信息
overwrite-dns	覆盖系统 DNS。

unset port access vlan

使用 **unset port access vlan** 命令删除二层接口所隶属的 VLAN。

命令

unset port access vlan

语法

access	二层接口的 Access 工作模式。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 Ethernet 接口配置模式、 Channel 接口配置模式、冗余接口配置模式或虚拟接口配置模式下使用。

相关命令

命令名称	描述信息
port accesss vlan	设置二层接口隶属于指定 VLAN。

unset port trunk allowed vlan

使用 **unset port trunk allowed vlan** 命令删除指定 Trunk 端口所允许的 VLAN。

命令

unset port trunk allowed vlan *vlan_id_list*

语法

trunk	二层接口的 Trunk 工作模式。
vlan_id_list	VLAN ID 列表，格式为 NUMBER， 1-1023 表示所有存在的 VLAN。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 Ethernet 接口配置模式、 Channel 接口配置模式或冗余接口配置模式下使用。

范例

范例 . 删除 Trunk 端口 eth1 所允许的所有 VLAN。

```
NetEye@root-system]interface ethernet 1
NetEye@root-system-if-eth1]unset port trunk allowed vlan 1-1023
```

相关命令

命令名称	描述信息
port trunk allowed vlan	设置指定 Trunk 端口所允许的 VLAN。

unset port trunk native

使用 **unset port trunk native** 命令删除指定 Trunk 端口所允许的 Native VLAN。

命令

unset port trunk native

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 Ethernet 接口配置模式、 Channel 接口配置模式或冗余接口配置模式下使用。

范例

范例 . 删除 Trunk 端口 eth1 所允许的 Native VLAN。

```
NetEye@root-system]interface ethernet 1
NetEye@root-system-if-eth1]unset port trunk native
```

相关命令

命令名称	描述信息
port trunk native vlan	设置指定 Trunk 端口所允许的 Native VLAN。

unset pppoe

使用 **unset pppoe** 命令删除指定的 PPPoE 接口。

命令

unset pppoe *pppoe_id*

语法

pppoe_id	PPPoE ID，格式为 INTEGER<0-7>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 删除 PPPoE 接口 ppp1。

```
NetEye@root-system]unset pppoe 1
```

相关命令

命令名称	描述信息
pppoe	创建 PPPoE 接口或进入指定的 PPPoE 接口配置模式。

unset rint

使用 **unset rint** 命令删除指定的冗余接口。

命令

unset rint *rint_id*

语法

rint_id	冗余接口 ID，格式为 INTEGER<1-4>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 删除冗余接口 rint1。

```
NetEye@root-system]usnet rint 1
```

相关命令

命令名称	描述信息
rint	创建冗余接口或进入冗余接口配置模式。

unset servicename

使用 **unset servicename** 命令删除服务名称。

命令

unset servicename

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 PPPoE 接口配置模式下使用。

相关命令

命令名称	描述信息
servicename	设置服务名称。

unset shutdown

使用 **unset shutdown** 命令启用接口。

命令

unset shutdown

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在接口配置模式 （除 PPPoE 接口配置模式）或 VLAN 配置模式下使用。

范例

范例 . 启用以太网接口 eth1。

```
NetEye@root-system]interface ethernet 1
NetEye@root-system-if-eth1]unset shutdown
```

相关命令

命令名称	描述信息
shutdown	禁用接口。

unset tunnel

使用 **unset tunnel** 命令删除指定的 VPN 隧道接口。

命令

unset tunnel *tunnel_id*

语法

tunnel_id	隧道 ID，格式为 INTEGER<1-4095>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除 VPN 隧道接口 tunnel6。

```
NetEye@root-system]unset tunnel 6
```

相关命令

命令名称	描述信息
tunnel	创建 VPN 隧道接口或进入指定的 VPN 隧道接口配置模式。

unset Unnumbered

使用 **unset Unnumbered** 命令删除借用其他三层接口的 IP 地址。

命令

unset Unnumbered

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 隧道接口配置模式下使用。

范例

范例 . 删除 VPN 隧道接口 tunnel1 借用的 IP 地址。

```
NetEye@root-system]tunnel 1
NetEye@root-system-tunnel1]unset Unnumbered
```

相关命令

命令名称	描述信息
Unnumbered	借用其他三层接口的 IP 地址。

unset user

使用 **usnet user** 命令删除拨号用户。

命令

unset user

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 PPPoE 接口配置模式下使用。

相关命令

命令名称	描述信息
username	配置拨号用户。

unset veth

使用 **unset veth** 命令删除指定的虚拟接口。

命令

unset veth *veth_id*

语法

veth_id	虚拟接口 ID，格式为 INTEGER<1-1023>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 删除虚拟接口 veth1。

```
NetEye@root-system]unset veth 1
```

相关命令

命令名称	描述信息
veth	创建虚拟接口或进入指定的虚拟接口配置模式。

unset vlan

使用 **unset vlan** 命令删除指定的 VLAN。

命令

unset vlan *vlan_id*

语法

vlan_id	VLAN ID，格式为 INTEGER<1-1023>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 删除 VLAN50。

```
NetEye@root-system]unset vlan 50
```

相关命令

命令名称	描述信息
vlan	创建 VLAN 或进入指定的 VLAN 配置模式。

unset webauth

使用 **unset webauth** 命令禁用 PPPoE 接口 WebAuth 认证。

命令

unset webauth

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 PPPoE 接口配置模式下使用。

相关命令

命令名称	描述信息
webauth	启用 PPPoE 接口 WebAuth 认证。

username

使用 **username** 命令配置拨号用户。

命令

username *user_name* **password** *passwd*

语法

user_name	用户名称，格式为 WORD<1-64>。
passwd	密码，格式为 WORD<1-64>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 PPPoE 接口配置模式下使用。

范例

范例 . 在 ppp0 接口上配置拨号用户，用户名称为 test，密码为 123456。

```
NetEye@root-system]pppoe 0
NetEye@root-system-pppoe0]username test password 123456
```

相关命令

命令名称	描述信息
unset user	删除拨号用户。

veth

使用 **veth** 命令创建虚拟接口或进入指定的虚拟接口配置模式。

命令

veth *veth_id*

语法

veth_id	虚拟接口 ID，格式为 INTEGER<1-1023>。

说明

如果指定 *veth_id* 的虚拟接口不存在，则创建一个以 *veth_id* 命名的虚拟接口，并进入该虚拟接口配置模式。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 创建虚拟接口 veth1。

```
NetEye@root-system]veth 1
```

相关命令

命令名称	描述信息
unset veth	删除指定的虚拟接口。

vlan

使用 **vlan** 命令创建 VLAN 或进入指定的 VLAN 配置模式。

命令

vlan *vlan_id*

语法

vlan_id	VLAN ID，格式为 INTEGER<1-1023>。

说明

如果指定 *vlan_id* 的 VLAN 不存在，则创建一个以 *vlan_id* 命名的 VLAN，并进入该 VLAN 配置模式。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 进入 VLAN2 的配置模式。

```
NetEye@root-system]vlan 2
```

相关命令

命令名称	描述信息
unset vlan	删除指定的 VLAN。

wait-time

使用 **wait-time** 命令设置冗余接口的故障恢复等待时间。

命令

wait-time *wait_time*

语法

wait_time	等待时间，单位为秒，格式为 INTEGER<3-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在冗余接口配置模式下使用。

范例

范例 . 设置冗余接口 rint1 的故障恢复等待时间为 4。

```
NetEye@root-system]rint 1
NetEye@root-system-rint1]wait-time 4
```

webauth

使用 **webauth** 命令启用 PPPoE 接口 WebAuth 认证。

命令

webauth

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 PPPoE 接口配置模式下使用。

相关命令

命令名称	描述信息
unset webauth	禁用 PPPoE 接口 WebAuth 认证。

working-type

使用 **working-type** 命令设置二层接口的模式。

命令

working-type {**layer2-interface** | **layer3-interface** | **layer3-shared-interface**}

语法

layer2-interface | **layer3-interface** | **layer3-shared-interface**	• layer2-interface— 二层模式 • layer3-interface— 三层模式 • layer3-shared-interface— 三层共享模式

说明

虚拟接口不能设置为三层共享模式。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 Ethernet 接口配置模式、 Channel 接口配置模式、冗余接口配置模式或虚拟接口配置模式下使用。

范例

范例 . 设置以太网接口 eth1 为二层接口。

```
NetEye@root-system]interface ethernet 1
NetEye@root-system-if-eth1]working-type layer2-interface
```

接口 Bypass

bypass

使用 **bypass** 命令配置网卡对的 Bypass 功能。

命令

bypass *nic_name1 nic_name2* {**watchdog** | **poweroff**} {**enable** | **disable**}

语法

nic_name1	物理网卡名 1，格式为 WORD<1-15>。
nic_name2	物理网卡名 2，格式为 WORD<1-15>。该名称不能和物理网卡名 1 相同。
watchdog	**poweroff**	指进入 Bypass 模式的两种情况： • watchdog—指软件故障 • poweroff—指断电
enable	**disable**	enable— 启用 Bypass 功能 disable— 禁用 Bypass 功能

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 启用网卡对 eth1 和 eth2 的 Bypass 功能，当出现软件故障时进入 Bypass 模式。

```
NetEye@root-system]bypass eth1 eth2 watchdog enable
```

相关命令

命令名称	描述信息
show bypass	查看 Bypass 功能的配置状态。

show bypass

使用 **show bypass** 命令查看 Bypass 功能的配置状态。

命令

show bypass

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看 Bypass 功能的配置状态。

```
NetEye@root> show bypass
```

相关命令

命令名称	描述信息
bypass	配置网卡对的 Bypass 功能。

ARP

arp

使用 **arp** 命令在指定接口上添加静态或代理 ARP （地址解析协议）表项。

命令

arp [**proxy**] {**vlan | ethernet | channel | rint | veth**} *interface_id ip_address mac_address*

语法

proxy	可选关键字，表示添加 ARP 代理类型的表项。
vlan | **ethernet** | **channel** | **rint** | **veth**	• vlan—VLAN 接口 • ethernet— 以太网接口 • channel— 以太网通道 • rint— 冗余接口 • veth— 虚拟接口
interface_id	接口标识。 1. 如果设置为 **vlan** 类型， *interface_id* 的格式为 INTEGER<1-1023>。 2. 如果设置为 **ethernet** 类型， *interface_id* 的格式为 WORD<1-10>。 3. 如果设置为 **channel** 类型， *interface_id* 的格式为 INTEGER<0-7>。 4. 如果设置为 **rint** 类型， *interface_id* 的格式为 INTEGER<1-4>。 5. 如果设置为 **veth** 类型， *interface_id* 的格式为 INTEGER<1-1023>。
ip_address	IP 地址，格式为 x.x.x.x。
mac_address	MAC 地址，格式为 HH:HH:HH:HH:HH:HH。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 在 VLAN1 下添加静态 ARP 表项，指定 IP 地址为 192.168.1.100， MAC 地址为 00:00:00:00:22:33。

```
NetEye@root-system]arp vlan 1 192.168.1.100 00:00:00:00:22:33
```

相关命令

命令名称	描述信息
show arp proxy	显示代理 ARP 表项。
show arp static	显示静态 ARP 表项。
unset arp proxy	删除代理 ARP 表项。
unset arp static	删除静态 ARP 表项。
unset arp static vlan, ethernet, channel, rint, veth	删除指定接口中的静态 ARP 表项。

arp timeout

使用 **arp timeout** 命令在指定接口上设置动态 ARP 表项的超时值。

命令

arp {**vlan | ethernet | channel | rint | veth**} *interface_id* **timeout** {*timeout_value* | **default**}

语法

vlan | **ethernet** | **channel** | **rint** | **veth**	• vlan—VLAN 接口 • ethernet— 以太网接口 • channel— 以太网通道 • rint— 冗余接口 • veth— 虚拟接口
interface_id	接口标识。 1. 如果设置为 **vlan** 类型， *interface_id* 的格式为 INTEGER<1-1023>。 2. 如果设置为 **ethernet** 类型， *interface_id* 的格式为 WORD<1-6>。 3. 如果设置为 **channel** 类型， *interface_id* 的格式为 INTEGER<0-7>。 4. 如果设置为 **rint** 类型， *interface_id* 的格式为 INTEGER<1-4>。 5. 如果设置为 **veth** 类型， *interface_id* 的格式为 INTEGER<1-1023>。
timeout	表示动态 ARP 表条目的超时时间。
timeout_value	超时时间值，单位为秒，格式为 INTEGER<3-30000>。
default	缺省值为 14400 秒。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 在 VLAN1 下设置 ARP 表项为默认超时值。

```
NetEye@root-system]arp vlan 1 timeout default
```

相关命令

命令名称	描述信息
show arp timeout	显示所有接口的 ARP 表项超时值。

show arp

使用 **show arp** 命令显示当前系统所有的 ARP 表项。

命令

show arp [{**vlan** | **ethernet** | **channel** | **rint** | **veth**} *interface_id*]

语法

vlan | **ethernet** | **channel** | **rint** | **veth**	• vlan—VLAN 接口 • ethernet— 以太网接口 • channel— 以太网通道 • rint— 冗余接口 • veth— 虚拟接口
interface_id	接口标识。 1. 如果设置为 **vlan** 类型， *interface_id* 的格式为 INTEGER<1-1023>。 2. 如果设置为 **ethernet** 类型， *interface_id* 的格式为 WORD<1-6>。 3. 如果设置为 **channel** 类型， *interface_id* 的格式为 INTEGER<0-7>。 4. 如果设置为 **rint** 类型， *interface_id* 的格式为 INTEGER<1-4>。 5. 如果设置为 **veth** 类型， *interface_id* 的格式为 INTEGER<1-1023>。

说明

如果只输入 **show arp** 命令，表示显示所有 ARP 表项；否则，表示显示指定接口中的 ARP 表项。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 VLAN1 下的 ARP 表项。

```
NetEye@root>show arp vlan 1
```

【返回结果】

```
IP Address Hardware Address   Type     State   Living_time (s) Interface
40.1.1.30  00:16:35:74:16:B8 dynamic REACHABLE   16              Vlan1
```

相关命令

命令名称	描述信息
arp	添加静态或代理 ARP 表项。
unset arp static	删除静态 ARP 表项。
unset arp static vlan, ethernet, channel, rint, veth	删除指定接口中的静态 ARP 表项。

show arp dynamic

使用 **show arp dynamic** 命令显示动态 ARP 表项。

命令

show arp dynamic

语法

dynamic	动态 ARP 表项。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 当前系统下的动态 ARP 表项。

```
NetEye@root>show arp dynamic
```

【返回结果】

```
IP Address  Hardware Address    Type      State     Living_time (s)
Interface
10.3.1.130  00:1B:78:B7:71:6D   dynamic  REACHABLE     6
eth1
10.3.1.159  00:08:74:D9:9C:94   dynamic  REACHABLE     31
eth1
10.3.1.239  00:1B:78:B5:08:5A   dynamic  REACHABLE     3322
eth1
10.3.1.1    FE:FD:0D:00:CB:74   dynamic  REACHABLE     787
eth1
```

相关命令

命令名称	描述信息
unset arp dynamic	删除动态 ARP 表项。
unset arp dynamic vlan, ethernet, channel, rint, veth	删除指定接口中的动态 ARP 表项。

show arp proxy

使用 **show arp proxy** 命令显示代理 ARP 表项。

命令

show arp proxy

语法

proxy	代理 ARP 表项。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 当前系统下的代理 ARP 表项。

```
NetEye@root>show arp proxy
```

【返回结果】

```
IP Address  Hardware Address    Type     State   Living_time (s)
Interface
10.3.1.212  00:A0:8E:A6:E7:B0   proxy      -         -              eth-
s4p1
10.1.1.1    00:A0:8E:A6:E7:B1   proxy      -         -              vlan1
```

相关命令

命令名称	描述信息
arp	添加静态或代理 ARP 表项。
unset arp proxy	删除所有代理 ARP 表项。

show arp static

使用 **show arp static** 命令显示静态 ARP 表项。

命令

show arp static

语法

static	静态 ARP 表项。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 当前系统下的静态 ARP 表项。

```
NetEye@root>show arp static
```

【返回结果】

```
IP Address    Hardware Address    Type    State  Living_time (s)
Interface
10.3.1.13     00:18:78:B7:71:6D   static    -        -            vlan1
```

相关命令

命令名称	描述信息
arp	添加静态或代理 ARP 表项。
unset arp static	删除静态 ARP 表项。
unset arp static vlan, ethernet, channel, rint, veth	删除指定接口中的静态 ARP 表项。

show arp timeout

使用 **show arp timeout** 命令显示所有接口的 ARP 表项的超时值。

命令

show arp timeout

语法

timeout	表示动态 ARP 表项的超时值。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 所有接口的 ARP 表项超时值。

```
NetEye@root>show arp timeout
```

【返回结果】

```
Vlan1      14400 s
Vlan2      14400 s
Vlan10     14400 s
```

相关命令

命令名称	描述信息
arp timeout	设置动态 ARP 表项的超时值。

unset arp dynamic

使用 **unset arp dynamic** 命令删除动态 ARP 表项。

命令

unset arp dynamic [*ip_address*]

语法

dynamic	动态 ARP 表项。
ip_address	IP 地址。格式为 x.x.x.x。

说明

如果不指定 *ip_address* 参数，则删除所有的动态 ARP 表项。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除所有动态 ARP 表项。

```
NetEye@root-system]unset arp dynamic
```

相关命令

命令名称	描述信息
arp	添加静态或代理 ARP 表项。
show arp dynamic	显示动态 ARP 表项。
unset arp dynamic vlan , ethernet, channel, rint, veth	删除指定接口中的动态 ARP 表项。

unset arp dynamic vlan, ethernet, channel, rint, veth

使用 **unset arp dynamic vlan, ethernet, channel, rint, veth** 命令删除指定接口中的动态 ARP 表项。

命令

unset arp dynamic {**vlan** | **ethernet** | **channel** | **rint** | **veth**} *interface_id*

语法

dynamic	动态 ARP 表项。
vlan | **ethernet** | **channel** | **rint** | **veth**	• vlan—VLAN 接口 • ethernet— 以太网接口 • channel— 以太网通道 • rint— 冗余接口 • veth— 虚拟接口
interface_id	接口标识。 1. 如果设置为 **vlan** 类型， *interface_id* 的格式为 INTEGER<1-1023>。 2. 如果设置为 **ethernet** 类型， *interface_id* 的格式为 WORD<1-6>。 3. 如果设置为 **channel** 类型， *interface_id* 的格式为 INTEGER<0-7>。 4. 如果设置为 **rint** 类型， *interface_id* 的格式为 INTEGER<1-4>。 5. 如果设置为 **veth** 类型， *interface_id* 的格式为 INTEGER<1-1023>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除 VLAN1 接口中的动态 ARP 表项。

```
NetEye@root-system]unset arp dynamic vlan 1
```

相关命令

命令名称	描述信息
arp	添加静态或代理 ARP 表项。
show arp dynamic	显示动态 ARP 表项。

unset arp proxy

使用 **unset arp proxy** 命令删除代理 ARP 表项。

命令

unset arp proxy [*ip_address*]

语法

proxy	代理 ARP 表项。
ip_address	IP 地址。格式为 x.x.x.x。

说明

如果不指定 *ip_address* 参数，则删除所有的代理 ARP 表项。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除所有代理 ARP 表项。

```
NetEye@root-system]unset arp proxy
```

相关命令

命令名称	描述信息
arp	添加静态或代理 ARP 表项。
show arp proxy	显示代理 ARP 表项。

unset arp proxy vlan, ethernet, channel, rint, veth

使用 **unset arp dynamic vlan, ethernet, channel, rint, veth** 命令删除指定接口中的代理 ARP 表项。

命令

unset arp proxy {**vlan** | **ethernet** | **channel** | **rint** | **veth**} *interface_id*

语法

proxy	代理 ARP 表项。
vlan | **ethernet** | **channel** | **rint** | **veth**	• vlan—VLAN 接口 • ethernet— 以太网接口 • channel— 以太网通道 • rint— 冗余接口 • veth— 虚拟接口
interface_id	接口标识。 1. 如果设置为 **vlan** 类型， *interface_id* 的格式为 INTEGER<1-1023>。 2. 如果设置为 **ethernet** 类型， *interface_id* 的格式为 WORD<1-6>。 3. 如果设置为 **channel** 类型， *interface_id* 的格式为 INTEGER<0-7>。 **4.** 如果设置为 **rint** 类型， *interface_id* 的格式为 INTEGER<1-4>。 **5.** 如果设置为 **veth** 类型， *interface_id* 的格式为 INTEGER<1-1023>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除 VLAN1 接口中的代理 ARP 表项。

```
NetEye@root-system]unset arp proxy vlan 1
```

相关命令

命令名称	描述信息
arp	添加静态或代理 ARP 表项。
show arp proxy	显示代理 ARP 表项。

unset arp static

使用 **unset arp static** 命令删除静态 ARP 表项。

命令

unset arp static [*ip_address*]

语法

static	静态 ARP 表项。
ip_address	IP 地址。格式为 x.x.x.x。

说明

如果不指定 *ip_address* 参数，则删除所有的静态 ARP 表项。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除所有静态 ARP 表项。

```
NetEye@root-system]unset arp static
```

相关命令

命令名称	描述信息
arp	添加静态或代理 ARP 表项。
show arp static	显示静态 ARP 表项。
unset arp static vlan, ethernet, channel, rint, veth	删除指定接口中的动态 ARP 表项。

unset arp static vlan, ethernet, channel, rint, veth

使用 **unset arp static channel, ethernet, vlan, rint, veth** 命令删除指定接口中的静态 ARP 表项。

命令

unset arp static {**vlan** | **ethernet** | **channel** | **rint** | **veth**} *interface_id*

语法

static	静态 ARP 表项。
vlan | **ethernet** | **channel** | **rint** | **veth**	• vlan—VLAN 接口 • ethernet— 以太网接口 • channel— 以太网通道 • rint— 冗余接口 • veth— 虚拟接口
interface_id	接口标识。 1. 如果设置为 **vlan** 类型， *interface_id* 的格式为 INTEGER<1-1023>。 2. 如果设置为 **ethernet** 类型， *interface_id* 的格式为 WORD<1-6>。 3. 如果设置为 **channel** 类型， *interface_id* 的格式为 INTEGER<0-7>。 4. 如果设置为 **rint** 类型， *interface_id* 的格式为 INTEGER<1-4>。 5. 如果设置为 **veth** 类型， *interface_id* 的格式为 INTEGER<1-1023>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除 VLAN1 接口中的静态 ARP 表项。

```
NetEye@root-system]unset arp static vlan 1
```

相关命令

命令名称	描述信息
arp	添加静态或代理 ARP 表项。
show arp static	显示静态 ARP 表项。

CAM

cam-table

使用 **cam-table** 命令为指定接口中的 CAM 表添加静态条目。配置成功后， NetEye 通过匹配数据包的目的 MAC 地址和 CAM 表的 MAC 地址，找到对应的二层接口发送数据包。

命令

cam-table vlan *interface_id* {**channel** | **ethernet | rint | veth**} *interface_id mac_address*

语法

interface_id	接口标识，格式为 INTEGER<1-1023>。
channel | **ethernet**	• channel— 以太网通道 • ethernet— 以太网接口 • rint — 冗余接口 • veth— 虚拟接口
interface_id	接口标识。格式为 WORD<1-10>。
mac_address	MAC 地址，格式为 HH:HH:HH:HH:HH:HH。

说明

此处提到的二层接口的工作模式为 Access 模式。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 为 VLAN1 下的 CAM 表添加静态条目，指定目的 MAC 地址为 00:00:00:00:22:33，对应转发接口为 **ethernet** 1。

```
NetEye@root-system]cam-table vlan 1 ethernet 1 00:00:00:00:22:33
```

相关命令

命令名称	描述信息
show cam-table	显示 CAM 表信息。
unset cam-table static	删除指定接口的 CAM 表的静态条目。

cam-table timeout

使用 **cam-table timeout** 命令设置 CAM 表动态条目的超时时间。系统缺省默认值为 300 秒。

命令

cam-table timeout [**vlan** *interface_id*] {*timeout_value* | **default**}

语法

interface_id	接口标识，格式为 INTEGER<1-1023>。
timeout_value	超时时间值，以秒为单位。格式为 INTEGER<10-30000>。
default	缺省值为 300 秒。

说明

1. 如果不指定 **vlan** *interface_id* 参数，则表示设置所有接口的 CAM 表动态条目的超时时间。
2. 动态条目超时后会被自动删除；静态条目不会因为超时而被删除，但可以手动删除。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置 VLAN1 下 CAM 表的动态条目超时时间为 5000 秒。

```
NetEye@root-system]cam-table timeout vlan 1 5000
```

相关命令

命令名称	描述信息
show cam-table timeout	显示所有接口的 CAM 表的动态条目超时时间。

show cam-table

使用 **show cam-table** 命令显示 CAM 表信息。

命令

show cam-table [**vlan** *interface_id*]

语法

vlan	VLAN 接口。
interface_id	接口标识，格式为 INTEGER<1-1023>。

说明

如果不指定 **vlan** *interface_id* 参数，则显示所有接口的 CAM 表信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有接口的 CAM 表信息。

```
NetEye@root>show cam-table
```

【返回结果】

```
Dynamic Address Count:                     2
Static Address (User-defined) Count:       1
System Self Address Count:                 1
Multicast Address Count:                   1
Total MAC addresses:                       5
Maximum MAC addresses:                 16384

Non-static Address Table:
```

```
Destination Address  Address Type  Layer3 inf  Destination Port  Timeout
(s)
-------------------------------------------------------------------------
----
0019.bb60.005f       dynamic        vlan1        eth1          4860
001b.78b6.1f9a       dynamic        vlan1        eth1          4250
00a0.8ea6.e883       static         vlan1         ch1           -
0063.686e.0019       self           vlan1       vlan1           -
-------------------------------------------------------------------------
----
0100.5e05.150a       multicast      vlan1      eth-s4p3         -
```

相关命令

命令名称	描述信息
cam-table	为指定接口中的 CAM 表添加静态条目。

show cam-table timeout

使用 **show cam-table timeout** 命令显示所有接口的 CAM 表的动态条目超时时间。

命令

show cam-table timeout

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有接口的 CAM 表的动态条目超时时间。

```
NetEye@root>show cam-table timeout
```

【返回结果】

```
vlan5      5000 s
Vlan10     4860 s
```

相关命令

命令名称	描述信息
cam-table timeout	设置 CAM 表动态条目的超时时间。

unset cam-table dynamic

使用 **unset cam-table dynamic** 命令删除 CAM 表的动态条目。

命令

unset cam-table dynamic [**vlan** *interface_id*]

语法

interface_id	接口标识，格式为 INTEGER<1-1023>。

说明

如果不指定 **vlan** *interface_id* 参数，则表示删除所有接口的 CAM 表的动态条目。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除所有接口的 CAM 表的动态条目。

```
NetEye@root-system]unset cam-table dynamic
```

相关命令

命令名称	描述信息
cam-table	为指定接口中的 CAM 表添加静态条目。
show cam-table	显示 CAM 表信息。

unset cam-table static

使用 **unset cam-table static** 命令删除指定接口的 CAM 表的静态条目。

命令

unset cam-table static vlan *interface_id* [*mac_address*]

语法

interface_id	表示以太网通道或接口标识。格式为 INTEGER<1-1023>。
mac_address	MAC 地址，格式为 HH:HH:HH:HH:HH:HH。

说明

如果不指定 *mac_address* 参数，则表示删除指定接口的 CAM 表的所有静态条目。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除 VLAN1 下 CAM 表的所有静态条目。

```
NetEye@root-system]unset cam-table static vlan 1
```

相关命令

命令名称	描述信息
cam-table	为指定接口中的 CAM 表添加静态条目。
show cam-table	显示 CAM 表信息。

虚拟网络

hold veth

使用 **hold veth** 命令将虚拟接口划入到虚拟网络。

命令

hold veth *veth_id*

语法

veth_id	虚拟接口 ID，格式为 INTEGER<1-1023>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在虚拟网络配置模式下使用。

范例

范例 . 将虚拟接口 1 划入到虚拟网络 1 中。

```
NetEye@root-system]vnet 1
NetEye@root-system-vnet1]hold veth 1
```

相关命令

命令名称	描述信息
unhold veth	将虚拟接口从虚拟网络中划出。

show vnet

使用 **show vnet** 命令显示虚拟网络信息。

命令

show vnet [*vnet_id* | **brief**]

语法

vnet_id	虚拟网络 ID，格式为 INTEGER<1-255>。
brief	显示简明信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在普通配置模式下使用。

范例

范例 . 显示虚拟网络 1 的信息。

```
NetEye@root>show vnet 1
```

【返回结果】

```
NetEye@root> show vnet 1
v-network       counts  v-eth
(("vnet1",      "2",    ("veth1","veth2")))
```

unhold veth

使用 **unhold veth** 命令将虚拟接口从虚拟网络中划出。

命令

unhold veth *veth_id*

语法

veth_id	虚拟接口 ID，格式为 INTEGER<1-1023>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在虚拟网络配置模式下使用。

范例

范例 . 将虚拟接口 1 从虚拟网络 1 中划出。

```
NetEye@root-system]vnet 1
NetEye@root-system-vnet1]unhold veth 1
```

相关命令

命令名称	描述信息
hold veth	将虚拟接口划入到虚拟网络。

unset vnet

使用 **unset vnet** 命令删除指定的虚拟网络。

命令

unset vnet *vnet_id*

语法

vnet_id	虚拟网络 ID，格式为 INTEGER<1-255>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 删除虚拟网络 1。

```
NetEye@root-system]unset vnet 1
```

相关命令

命令名称	描述信息
vnet	创建虚拟网络或者进入指定虚拟网络配置模式。

vnet

使用 **vnet** 命令创建虚拟网络或者进入指定虚拟网络配置模式。

命令

vnet *vnet_id*

语法

vnet_id	虚拟网络 ID，格式为 INTEGER<1-255>。

说明

如果指定 *vnet_id* 的虚拟网络不存在，则创建一个以 *vnet_id* 为标识的虚拟网络，并进入该虚拟网络配置模式。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 创建虚拟网络 1。

```
NetEye@root-system]vnet 1
```

相关命令

命令名称	描述信息
unset vnet	删除指定的虚拟网络。

sFlow

sflow agent ip

使用 **sflow agent ip** 命令设置代理 IP 地址。

命令

sflow agent ip *ip_address*

语法

ip_address	IP 地址，格式为 x.x.x.x。 缺省值为 127.0.0.1。

说明

sFlow 代理在 NetEye 系统内是唯一的，负责统一收集每一个 sFlow 实例提交的 Flow 信息，并发送给指定的收集器。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 设置代理 IP 地址为 192.168.1.100。

```
NetEye@root-system]sflow agent ip 192.168.1.100
```

相关命令

命令名称	描述信息
show sflow	显示 sFlow 信息。

sflow instance

使用 **sflow instance** 命令添加 sFlow 实例。

命令

sflow instance *instance_name* **collector** *ip_address collector_port* **rate** *rate_num* **interval** *interval_num* **maxheader** *maxheader_num* **maxdatagram** *maxdatagram_num* **comment** [*string*]

语法

instance_name	sFlow 实例名称，格式为 WORD<1-15>。
ip_address	Flow 信息收集器的 IP 地址，格式为 x.x.x.x。
collector_port	Flow 信息收集器的端口，格式为 INTEGER<1-65535>。 缺省值为 6343。
rate_num	Flow 信息抽样率，格式为 INTEGER<1-1048576>。 缺省值为 65536。
interval_num	间隔时间，格式为 INTEGER<5-100>。 缺省值为 20。
maxheader_num	发送的每个原始数据包的最大长度，格式为 INTEGER<20-3000>。 缺省值为 128。
maxdatagram_num	发送 sFlow 数据包的最大长度，格式为 INTEGER<100-3000>。 缺省值为 1400。
string	备注信息，格式为 LINE。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 添加 sFlow 实例，实例名称为 test， Flow 信息收集器的 IP 地址为 192.168.2.100 端口为 6555， Flow 信息的采样率为 65535，统计的时间间隔为 30 秒，最大发送数据包大小为 256 字节， Flow 报文的长度为 1500。

```
NetEye@root-system]sflow instance test collector 192.168.2.100 6555
rate 65535 interval 30 maxheader 256 maxdatagram 1500 comment
```

相关命令

命令名称	描述信息
show sflow	显示 sFlow 实例的配置信息。
unset sflow instance	删除指定 sFlow 实例。

sflow source

使用 **sflow source** 命令设置 sFlow 数据包的源 IP 地址接口。

命令

sflow source *source_name*

语法

source_name	接口名称，格式为 WORD<1-10>。当输入 Auto 时，表示自动获取接口的 IP 地址。

说明

1. NetEye 根系统内每一个三层接口（三层以太网接口、三层 Channel 接口、三层冗余接口、三层虚拟接口、三层共享接口、 VLAN 接口、 Tunnel 接口、 Loopback 接口和 PPPoE 接口）都可以独立设置是否启用 sFlow 功能，对于启用 sFlow 功能的接口可以选择使用的 sFlow 实例，根据选定的 sFlow 实例中的配置，抽样并发送 Flow 信息到收集器。
2. 当管理员指定数据包源IP地址为自动获取或者设置的接口不存在时，数据包的源IP地址将使用发送数据包接口的 IP 地址。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 设置 sFlow 数据包源 IP 地址接口为自动获取。

```
NetEye@root-system]sflow source Auto
```

相关命令

命令名称	描述信息
show sflow	显示 sFlow 配置信息。

show sflow

使用 **show sflow** 命令显示 sFlow 的配置信息。

命令

show sflow

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 sFlow 的配置信息。

```
NetEye@root>show sflow
```

【返回结果】

```
sFlow Agent Configuration
Source IP:  Auto
Agent  IP:  127.0.0.1
sFlow Version: V5
-------------------------------------------------
sFlow Instance List(Total:1)
Name            Collector       Rate    Interval    HeaderSize  DataSize   Used by   Comment
test          192.168.2.100:634365536   20        128       1400      lo2      sFlow instance
```

相关命令

命令名称	描述信息
sflow agent ip	设置代理 IP。

show sflow instance

使用 **show sflow instance** 命令显示 sFlow 实例的配置信息。

命令

show sflow instance *instance_name*

语法

instance_name	sFlow 实例名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示名称为 test 的 sFlow 实例的配置信息。

```
NetEye@root>show sflow instance test
```

【返回结果】

```
Name Collector       Rate Interval HeaderSize  DataSize Used by Comment
test 1.1.11.1:6555   65535   30          256         1500
```

相关命令

命令名称	描述信息
sflow instance	添加 sFlow 实例。

unset sflow instance

使用 **unset sflow instance** 命令删除指定 sFlow 实例。

命令

unset sflow instance *instance_name*

语法

instance_name	sFlow 实例名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 删除名称为 test 的 sFlow 实例。

```
NetEye@root-system]unset sflow instance test
```

相关命令

命令名称	描述信息
sflow instance	添加 sFlow 实例。
show sflow instance	显示 sFlow 实例的配置信息。

安全域

show zone

使用 **show zone** 命令显示安全域的信息。

命令

show zone [*zone_name*]

语法

zone_name	安全域名称，格式为 WORD<1-15>。

说明

不指定 *zone_name* 参数，表示显示所有安全域的信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示安全域 zoneA 的信息。

```
NetEye@root>show zone zoneA
```

【返回结果】

```
Name : zoneA
Refcount: 2
Number  : 1
Policy: Vpn
Description: tihs is a Zone.
Interface: tunnel1
```

相关命令

命令名称	描述信息
unset zone	删除安全域。
zone	创建安全域。

unset zone

使用 **unset zone** 命令删除安全域。

命令

unset zone [*zone_name*]

语法

zone_name	安全域名称，格式为 WORD<1-15>。

说明

不指定 *zone_name* 参数，表示删除所有安全域。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除安全域 zoneA。

```
NetEye@root-system]unset zone zoneA
```

相关命令

命令名称	描述信息
show zone	显示安全域。
zone	创建安全域。
zone description	设置安全域的描述信息。

unset zone based-layer2

使用 **unset zone based-layer2** 命令删除安全域中的二层接口。

命令

unset zone *zone_name* **based-layer2** *interface_name*

语法

zone_name	安全域名称，格式为 WORD<1-15>。
l2_interface_name	二层接口名称，格式为 WORD<1-100>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除安全域 zoneB 中的二层接口 eth1。

```
NetEye@root-system]unset zone zoneB based-layer2 eth1
```

相关命令

命令名称	描述信息
zone based-layer2	在安全域中添加二层接口。

unset zone based-layer3

使用 **unset zone based-layer3** 命令删除安全域中的三层接口。

命令

unset zone *zone_name* **based-layer3** *interface_name*

语法

zone_name	安全域名称，格式为 WORD<1-15>。
interface_name	三层接口名称，格式为 WORD<1-100>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除安全域 zoneA 中的三层接口 VLAN1。

```
NetEye@root-system]unset zone zoneA based-layer3 vlan1
```

相关命令

命令名称	描述信息
zone bsaed-layer3	在安全域中添加三层接口。

zone

使用 **zone** 命令创建安全域。

命令

zone *zone_name*

语法

zone_name	安全域名称，格式为 WORD<1-15>。

说明

每个 Vsys 下最多可以创建 30 个安全域。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 创建安全域 zoneA。

```
NetEye@root-system]zone zoneA
```

相关命令

命令名称	描述信息
show zone	显示安全域信息。
unset zone	删除安全域。
zone description	设置安全域的描述信息。

zone based-layer2

使用 **zone based-layer2** 命令配置基于二层接口的安全域。

命令

zone *zone_name* **based-layer2 vlan** *vlan_id* [*l2_interface_name*]

语法

zone_name	安全域名称，格式为 WORD<1-15>。
vlan_id	VLAN 标识，格式为 INTEGER<1-1023>。
l2_interface_name	二层接口名称，格式为 WORD<1-100>。

说明

1. 如果指定的二层接口属于不同 VLAN，则不能被划入相同的安全域。
2. 三层接口和二层接口不能划入相同的安全域。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 配置基于二层接口的安全域，添加二层接口 eth1 到安全域 zoneA 中，该接口属于 VLAN 3。

```
NetEye@root-system]zone zoneA based-layer2 vlan 3 eth1
```

相关命令

命令名称	描述信息
unset zone based-layer2	删除安全域中的二层接口。

zone based-layer3

使用 **zone based-layer3** 命令配置基于三层接口的安全域。

命令

zone *zone_name* **based-layer3** *l3_interface_name*

语法

zone_name	安全域名称，格式为 WORD<1-15>。
l3_interface_name	三层接口名称，格式为 WORD<1-100>。

说明

1. VLAN 可以作为一个整体和其他三层接口共同成为一个安全域，此时 VLAN 内部不能再划分安全域。
2. 三层接口和二层接口不能划入相同的安全域。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 配置基于三层接口的安全域，添加三层接口 VLAN1 到安全域 zoneB 中。

```
NetEye@root-system]zone zoneB based-layer3 vlan1
```

相关命令

命令名称	描述信息
unset zone based-layer3	删除安全域中的三层接口。

zone description

使用 **zone description** 命令设置安全域的描述信息。

命令

zone *zone_name* **description** [*string*]

语法

string	描述信息，格式为 LINE。
zone_name	安全域名称，格式为 WORD<1-15>。

说明

如果不指定 *string* 参数，表示设置安全域的描述信息为空。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置安全域 zoneA 的描述信息为 infomationA。

```
NetEye@root-system]zone zoneA description infomationA
```

相关命令

命令名称	描述信息
unset zone	删除安全域。
zone	添加安全域。

QoS

qos enable, disable

使用 **qos enable, disable** 命令启用或禁用 QoS 功能。

命令

qos {**enable** | **disable**}

语法

enable | **disable**	• enable— 启用 QoS 功能 • disable— 禁用 QoS 功能 缺省设置为 disable

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 启用 QoS 功能。

```
NetEye@root-system]qos enable
```

相关命令

命令名称	描述信息
show qos state	显示 QoS 功能的状态。

qos interface

使用 **qos interface** 命令设置指定接口的带宽限制。

命令

qos interface {**ingress** | **egress**} {**gbw** *g_bandwidth* [**mbw** *m_bandwidth*] | **mbw** *m_bandwidth*} **prio** *pri*

语法

ingress | **egress**	• ingress— 表示入口带宽限制 • egress— 表示出口带宽限制
g_bandwidth	保证带宽，单位为 Kbps，格式为 INTEGER<1-6000000>。
m_bandwidth	最大带宽，单位为 Kbps，格式为 INTEGER<1-6000000>。
pri	接口获取剩余带宽的优先级，格式为 INTEGER<1-7>。

说明

1. 要使接口的带宽限制生效，必须启用 QoS 功能。
2. 如果不指定 **gbw** *g_bandwidth* 参数，则表示不对接口的流量保留任何的带宽，该接口允许的数据连接只能使用剩余带宽。
3. 如果不指定 **mbw** *m_bandwidth* 参数，则表示接口的流量将不受最大带宽约束，尽最大能力使用系统可用的带宽资源。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在接口配置模式 （除环回接口配置模式）或 VLAN 配置模式下使用。

范例

范例 . 设置 VLAN1 的出口带宽限制，其保证带宽为 600，最大带宽为 10000，获取剩余带宽的优先级为 2。

```
NetEye@root-system]vlan 1
NetEye@root-system-vlan1]qos interface egress gbw 600 mbw 10000 prio 2
```

相关命令

命令名称	描述信息
show qos state interface	显示接口带宽限制的配置信息。
unset qos interface	删除指定接口的带宽限制。

qos rule

使用 **qos rule** 命令添加 QoS 规则。

命令

qos rule *rule_name* {**gbw** *g_bandwidth* [**mbw** *m_bandwidth*] | **mbw** *m_bandwidth*} **prio** *pri* [**dscp** *dscp_value*]

语法

rule_name	QoS 规则名称，格式为 WORD<1-15>。
g_bandwidth	保证带宽，单位为 Kbps，格式为 INTEGER<1-6000000>。
m_bandwidth	最大带宽，单位为 Kbps，格式为 INTEGER<1-6000000>。
pri	QoS 规则获取剩余带宽的优先级，格式为 INTEGER<1-7>。
dscp_value	DSCP 值，格式为 INTEGER<0-63>。

说明

1. 要使 QoS 规则生效，必须启用 QoS 功能。
2. 如果不指定 **gbw** *g_bandwidth* 参数，则表示不对 QoS 规则的流量保留任何的带宽，该 QoS 规则允许的数据连接只能使用剩余带宽。
3. 如果不指定 **mbw** *m_bandwidth* 参数，则表示 QoS 规则的流量将不受最大带宽约束，尽最大能力使用系统可用的带宽资源。
4. 如果指定 DSCP 值，可用于区分不同数据包，帮助下游服务器区分优先级。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加 QoS 规则名称为 test，其保证带宽为 30000，最大带宽为 80000，优先级为 1。

```
NetEye@root-system]qos rule test gbw 30000 mbw 80000 prio 1
```

相关命令

命令名称	描述信息
show qos rule	显示 QoS 规则的配置信息。
unset qos rule	删除指定的 QoS 规则。

qos vsys

使用 **qos vsys** 命令设置指定 Vsys 的带宽限制。

命令

qos vsys {**ingress** | **egress**} {**gbw** *g_bandwidth* [**mbw** *m_bandwidth*] | **mbw** *m_bandwidth*} **prio** *pri*

语法

ingress | **egress**	• ingress— 表示入口带宽限制 • egress— 表示出口带宽限制
g_bandwidth	保证带宽，单位为 Kbps，格式为 INTEGER<1-6000000>。
m_bandwidth	最大带宽，单位为 Kbps，格式为 INTEGER<1-6000000>。
pri	Vsys 获取剩余带宽的优先级，格式为 INTEGER<1-7>。

说明

1. 要使 Vsys 的带宽限制生效，必须启用 QoS 功能。
2. 如果不指定 **gbw** *g_bandwidth* 参数，则表示不对 Vsys 的流量保留任何的带宽，该 Vsys 允许的数据连接只能使用剩余带宽。
3. 如果不指定 **mbw** *m_bandwidth* 参数，则表示 Vsys 的流量将不受最大带宽约束，尽最大能力使用系统可用的带宽资源。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 Vsys 配置模式下使用。

范例

范例 . 设置虚拟系统 vsys1 的出口带宽限制，其保证带宽为 600，最大带宽为 10000，获取剩余带宽的优先级为 2。

```
NetEye@root-system]vsys 1
NetEye@root-system-vsys1]qos vsys egress gbw 600 mbw 10000 prio 2
```

相关命令

命令名称	描述信息
show qos state vsys	显示 Vsys 带宽限制的配置信息。
unset qos vsys	删除指定 Vsys 的带宽限制。

show qos rule

使用 **show qos rule** 显示 QoS 规则的配置信息。

命令

show qos rule [*rule_name*]

语法

rule_name	QoS 规则名称，格式为 WORD<1-15>。

说明

如果不指定 *rule_name* 参数，则显示所有 QoS 规则的配置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看规则名称为 test 的 QoS 配置信息。

```
NetEye@root>show qos rule test
```

【返回结果】

```
Name            Guaranteed Bandwidth    Maximum Bandwidth    Priority    DSCP
test            30000                   80000                1           1
```

show qos state

使用 **show qos state** 显示 QoS 功能的状态。

命令

show qos state

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 查看 QoS 功能的状态。

```
NetEye@root>show qos state
```

【返回结果】

```
Qos Enable.
```

show qos state interface

使用 **show qos state interface** 显示接口带宽限制的配置信息。

命令

show qos state interface

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看接口带宽限制的配置信息。

```
NetEye@root>show qos state interface
```

【返回结果】

```
Interface       QoS   Ingress>>MB    GB       Priority    Egress>>MB     GB
Priority
eth0            off
vlan1            on    1000          300      4           1000           300
4
vlan2            on    10000         2000     4           10000          2000
4
```

show qos state vsys

使用 **show qos state vsys** 显示 Vsys 带宽限制的配置信息。

命令

show qos state vsys

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 查看 Vsys 带宽限制的配置信息。

```
NetEye@root>show qos state vsys
```

【返回结果】

```
Interface    QoS    Ingress>>MB    GB    Priority    Egress>>MB    GB    Priority
root          off
vsys1         on     80000        10000  7          80000       10000  7
```

unset qos interface

使用 **unset qos interface** 命令删除指定接口的带宽限制。

命令

unset qos interface [**ingress** | **egress**]

语法

ingress | **egress**	• ingress— 表示入口带宽限制 • egress— 表示出口带宽限制

说明

如果不指定 **ingress** 或 **egress** 关键字，则表示删除入口和出口带宽限制，且禁用该接口的带宽限制。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在接口配置模式 （除环回接口配置模式）或 VLAN 配置模式下使用。

范例

范例 . 禁用 VLAN1 的带宽限制。

```
NetEye@root-system]vlan 1
NetEye@root-system-vlan1]unset qos interface
```

相关命令

命令名称	描述信息
show qos state interface	显示接口带宽限制的配置信息。
qos interface	设置接口的带宽限制。

unset qos rule

使用 **unset qos rule** 命令删除指定的 QoS 规则。

命令

unset qos rule *rule_name*

语法

rule_name	QoS 规则名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除规则名称为 test 的 QoS 规则。

```
NetEye@root-system]unset qos rule test
```

相关命令

命令名称	描述信息
show qos rule	显示 QoS 规则的配置信息。
qos rule	添加 QoS 规则。

unset qos vsys

使用 **unset qos vsys** 命令删除指定 Vsys 的带宽限制。

命令

unset qos vsys [**ingress** | **egress**]

语法

ingress | **egress**	• ingress— 表示入口带宽限制 • egress— 表示出口带宽限制

说明

如果不指定 **ingress** 或 **egress** 关键字，则表示删除入口和出口带宽限制，且禁用该 Vsys 的带宽限制。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 Vsys 配置模式下使用。

范例

范例 . 禁用虚拟系统 vsys1 的带宽限制。

```
NetEye@root-system]vsys 1
NetEye@root-system-vsys1]unset qos vsys
```

相关命令

命令名称	描述信息
show qos state vsys	显示 Vsys 带宽限制的配置信息。
qos vsys	设置 Vsys 的带宽限制。

DHCP

dhcp interface none

使用 **dhcp interface none** 命令取消指定接口的 DHCP 属性。

命令

dhcp interface *interface_name* **none**

语法

interface_name	接口名称，格式为 WORD<1-15>。
none	表示取消接口的属性。

说明

1. 本命令不能用于取消 DHCP 客户端。
2. 对于三层接口可以设置为 DHCP 客户端、DHCP 中继代理服务器、DHCP 服务器或取消 DHCP 属性，但是这四种操作是互斥的。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 取消接口 VLAN1 的 DHCP 配置。

```
NetEye@root-system]dhcp interface vlan1 none
```

相关命令

命令名称	描述信息
show dhcp interface	显示 DHCP 接口配置信息。

dhcp interface relay

使用 **dhcp interface relay** 命令设置指定接口的 DHCP 中继代理服务器。

命令

dhcp interface *interface_name* **relay** *ip_address* {**primary** | **secondary** | **tertiary** | **quartus**}

语法

interface_name	接口名称，格式为 WORD<1-15>。
ip_address	DHCP 中继代理服务器的 IP 地址，格式为 x.x.x.x。
primary	表示所配置的 IP 地址为第一个 IP 地址。
secondary	表示所配置的 IP 地址为第二个 IP 地址。
tertiary	表示所配置的 IP 地址为第三个 IP 地址。
quartus	表示所配置的 IP 地址为第四个 IP 地址。

说明

1. 如果接口上没有配置合法的 IP 地址，则不能开启 DHCP 中继代理。
2. 对于三层接口可以设置为 DHCP 客户端、DHCP 中继代理服务器、DHCP 服务器或取消 DHCP 属性，但是这四种操作是互斥的。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置接口 tunnel1 的 DHCP 中继代理服务器的主 IP 地址为 192.168.1.130。

```
NetEye@root-system]dhcp interface tunnel1 relay 192.168.1.130 primary
```

相关命令

命令名称	描述信息
show dhcp interface	显示 DHCP 接口配置信息。
unset dhcp interface relay	删除指定接口的 DHCP 中继代理服务器。

dhcp interface relay change-gateway

使用 **dhcp interface relay change-gateway** 命令设置接口的 DHCP 中继代理是否更新网关。

命令

dhcp interface *interface_name* **relay change-gateway** {**enable** | **disable**}

语法

interface_name	接口名称，格式为 WORD<1-15>。
enable | disable	• enable— 表示更新网关 • disable— 表示不更新网关

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置接口 VLAN1 的 DHCP 中继代理更新网关。

```
NetEye@root-system]dhcp interface vlan1 relay change-gateway enable
```

dhcp interface server

使用 **dhcp interface server** 命令设置指定接口的 DHCP 服务器模式。

命令

dhcp interface *interface_name* **server** {**auto** | **enable** | **disable**}

语法

interface_name	接口名称，格式为 WORD<1-15>。
auto | enable | disable	NetEye 为每个三层接口启用 DHCP 服务器后提供的三种工作模式。 • auto— 自动模式 • enable— 启用模式 • disable— 禁用模式

说明

对于三层接口可以设置为 DHCP 客户端、 DHCP 中继代理服务器、 DHCP 服务器或取消 DHCP 属性，但是这四种操作是互斥的。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置接口 tunnel1 的 DHCP 服务器的工作模式为启用。

```
NetEye@root-system]dhcp interface tunnel1 server enable
```

相关命令

命令名称	描述信息
show dhcp interface	显示 DHCP 接口配置信息。

dhcp subnet

使用 **dhcp subnet** 命令添加 DHCP 作用域。

命令

dhcp subnet *subnet_name ip_address mask_length*

语法

subnet_name	作用域名称，格式为 WORD<1-15>。
ip_address	子网 IP 地址，格式为 x.x.x.x。
mask_length	子网掩码的长度，格式为 INTEGER<1-31>。

说明

每个作用域的子网允许出现包含，但是同一个 vsys 内的所有地址池都不能交叉。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加作用域 sub1，指定子网地址为 10.1.1.0，掩码长度为 24。

```
NetEye@root-system]dhcp subnet sub1 10.1.1.0 24
```

相关命令

命令名称	描述信息
show dhcp server subnet	显示 DHCP 作用域配置信息。
unset dhcp subnet	删除 DHCP 作用域。

dhcp subnet domain

使用 **dhcp subnet domain** 命令设置指定作用域的域名。

命令

dhcp subnet *subnet_name* **domain** *domain_name*

语法

subnet_name	作用域名称，格式为 WORD<1-15>。
domain_name	域名，格式为 WORD<1-255>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置作用域 sub2 的域名为 www.test.com。

```
NetEye@root-system]dhcp subnet sub2 domain www.test.com
```

相关命令

命令名称	描述信息
unset dhcp subnet domain	删除指定作用域的域名。

dhcp subnet dynamic

使用 **dhcp subnet dynamic** 命令为指定的作用域添加动态地址列表。

命令

dhcp subnet *subnet_name* **dynamic** *ip_address_list*

语法

subne_name	作用域名称，格式为 WORD<1-15>。
ip_address_list	IP 地址列表，格式为 IPV4LIST<1-8>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 为作用域 sub1 添加动态地址列表。

```
NetEye@root-system]dhcp subnet sub1 dynamic 192.168.1.152-192.168.1.173
```

相关命令

命令名称	描述信息
unset dhcp subnet dynamic	删除指定作用域的动态地址列表。

dhcp subnet gateway, wins, dns, smtp, pop3, news, nis

使用 **dhcp subnet gateway, wins, dns, smtp, pop3, news, nis** 命令设置指定作用域的特定服务的 IP 地址。例如，设置 DNS 的 IP 就是给客户端分配地址的时候将 DNS 的 IP 也一起告诉客户端，客户端就可以使用此 DNS 服务器。

命令

dhcp subnet *subnet_name* {**gateway** | **wins** | **wins2**| **dns** | **dns2**| **dns3** | **smtp** | **pop3** | **news** | **nis**} *ip_address*

语法

subnet_name	作用域名称，格式为 WORD<1-15>。
gateway | **wins** | **wins2**| **dns** | **dns2**| **dns3** | **smtp** | **pop3** | **news** | **nis**	允许分配给该作用域的主机的特殊服务。 • gateway— 网关 • wins—WINS 服务器 • wins2— 副 WINS 服务器 • dns— DNS 服务器 • dns2— 副 DNS 服务器 • dns3— 第三 DNS 服务器 • smtp— SMTP 服务器 • pop3 — POP3 服务器 • news— NEWS 服务器 • nis— 网络信息服务器
ip_address	IP 地址，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置作用域 sub2 的 DNS 的 IP 地址 192.168.1.130。

```
NetEye@root-system]dhcp subnet sub2 dns 192.168.1.130
```

相关命令

命令名称	描述信息
unset dhcp subnet gateway, wins, dns, smtp, pop3, news, nis	删除指定作用域的特定服务的 IP 地址。

dhcp subnet lease

使用 **dhcp subnet lease** 命令设置指定作用域的租期。默认设置为 1440 分钟。

命令

dhcp subnet *subnet_name* **lease** {**unlimited** | *lease_time*}

语法

subnet_name	作用域名称，格式为 WORD<1-15>。
lease	表示租期。
unlimited	表示不限制租期。
lease_time	租期时间，单位为 “分钟”，格式为 INTEGER<1-1440000>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置作用域 sub1 的租期为 14400 分钟。

```
NetEye@root-system]dhcp subnet sub1 lease 14400
```

dhcp subnet nistag

使用 **dhcp subnet nistag** 命令设置指定作用域的网络信息服务器的标签。

命令

dhcp subnet *subnet_name* **nistag** *tag*

语法

subnet_name	作用域名称，格式为 WORD<1-15>。
tag	标签信息，格式为 LINE。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置作用域 sub1 的网络信息服务器的标签为 This is sub1。

```
NetEye@root-system]dhcp subnet sub1 nistag This is sub1
```

相关命令

命令名称	描述信息
unset dhcp subnet nistag	删除指定作用域的网络信息服务器的标签。

dhcp subnet reserve

使用 **dhcp subnet reserve** 命令设置指定作用域的保留地址。

命令

dhcp subnet *subnet_name* **reserve** *ip_address mac_address*

语法

subnet_name	作用域名称，格式为 WORD<1-15>。
ip_address	IP 地址，格式为 x.x.x.x。
mac_address	MAC 地址，格式为 HH:HH:HH:HH:HH:HH。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置作用域 sub1 的保留 IP 地址为 192.168.1.130， MAC 地址为 FF:44:12:00:FF:74。

```
NetEye@root-system]dhcp subnet sub1 reserve 192.168.1.130
ff:44:12:00:ff:74
```

相关命令

命令名称	描述信息
unset dhcp subnet reserve	删除指定作用域的特定保留地址。

show dhcp interface

使用 **show dhcp interface** 命令显示 DHCP 接口配置信息。

命令

show dhcp interface [*interface_name*]

语法

interface_name	接口名称，格式为 WORD<1-15>。

说明

如果不指定 *interface_name* 参数，表示显示所有 DHCP 接口配置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有 DHCP 接口配置信息。

```
NetEye@root>show dhcp interface
```

【返回结果】

```
Interface       Type    Server type Relay address
eth-s4p1        Server  auto
tunnel1         Relay               192.168.1.130
vlan1           Client
```

show dhcp server ip-binding

使用 **show dhcp server ip-binding** 命令显示 DHCP 服务器的 IP 地址绑定状态。

命令

show dhcp server ip-binding [**subnet** *subnet_name*]

语法

subnet	表示显示指定作用域的 DHCP 服务器 IP 地址绑定状态。
subnet_name	作用域名称，格式为 WORD<1-15>。

说明

如果不指定 **subnet** *subnet_name* 参数，表示显示所有作用域的 DHCP 服务器的 IP 地址绑定状态。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 DHCP 服务器的 IP 地址绑定状态。

```
NetEye@root>show dhcp server ip-binding
```

【返回结果】

```
DHCP Subnet Interface  IP Address     MAC Address      End Time
          Lease Time(minute)   Type
sub1        vlan1     222.222.222.6   00:50:04:BD:3C:32 2008-01-09
09:44:37    1440               Dynamic
sub1        vlan1     222.222.222.9   00:1B:78:B6:1F:73 2008-01-09
09:41:46    1440               Dynamic
```

show dhcp server subnet

使用 **show dhcp server subnet** 命令显示 DHCP 作用域的配置信息。

命令

show dhcp server subnet [*subnet_name*]

语法

subnet_name	作用域名称，格式为 WORD<1-15>。

说明

如果不指定 *subnet_name* 参数，表示显示所有 DHCP 作用域的配置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 sub1 作用域的配置信息。

```
NetEye@root>show dhcp server subnet sub1
```

【返回结果】

```
Subnet: sub1 192.168.1.0/24
Lease: unlimited

Advanced setting
  Gateway:                  Wins:                  Wins2:
      Dns:                  Dns2:                   Dns3:
     News:                  Pop3:                   Smtp:
  Net Info Server:
  Net Info Server Tag: This is sub1
  Domain Name:
```

```
Dynamic IP Address                  | Reserved IP Address
192.168.1.100    192.168.1.123      | 192.168.1.120    FF:44:12:00:FF:74
192.168.1.124                       |
```

相关命令

命令名称	描述信息
dhcp subnet	添加 DHCP 作用域。
unset dhcp subnet	删除 DHCP 作用域。

unset dhcp interface relay

使用 **unset dhcp interface relay** 命令删除指定接口的 DHCP 中继代理服务器。

命令

unset dhcp interface *interface_name* **relay** {**primary** | **secondary** | **tertiary** | **quartus**}

语法

interface_name	接口名称，格式为 WORD<1-15>。
primary	表示删除的 IP 地址为第一个 IP 地址。
secondary	表示删除的 IP 地址为第二个 IP 地址。
tertiary	表示删除的 IP 地址为第三个 IP 地址。
quartus	表示删除的 IP 地址为第四个 IP 地址。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除接口 VLAN1 的 DHCP 中继代理服务器的主 IP 地址。

```
NetEye@root-system]unset dhcp interface vlan1 relay primary
```

相关命令

命令名称	描述信息
dhcp interface relay	设置指定接口的 DHCP 中继代理服务器。
show dhcp interface	显示 DHCP 接口配置信息。

unset dhcp subnet

使用 **unset dhcp subnet** 命令删除 DHCP 作用域。

命令

unset dhcp subnet [*subnet_name*]

语法

subnet_name	作用域名称，格式为 WORD<1-15>。

说明

如果不指定 *subnet_name* 参数，表示删除所有 DHCP 作用域；否则，表示删除指定的 DHCP 作用域。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除作用域 sub1。

```
NetEye@root-system]unset dhcp subnet sub1
```

相关命令

命令名称	描述信息
dhcp subnet	添加 DHCP 作用域。
show dhcp server subnet	显示 DHCP 作用域配置信息。

unset dhcp subnet domain

使用 **unset dhcp subnet domain** 命令删除指定作用域的域名。

命令

unset dhcp subnet *subnet_name* **domain**

语法

subnet_name	作用域名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
dhcp subnet domain	设置指定作用域的域名。

unset dhcp subnet dynamic

使用 **unset dhcp subnet dynamic** 命令删除指定作用域的动态地址列表。

命令

unset dhcp subnet *subnet_name* **dynamic** *start_ip_address*

语法

subnet_name	作用域名称，格式为 WORD<1-15>。
start_ip_address	起始 IP 地址，格式为 x.x.x.x。

说明

删除指定作用域的动态地址列表时，只需指定起始 IP 地址即可。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除作用域 sub1 的动态地址列表，指定起始 IP 地址为 192.168.1.152。

```
NetEye@root-system]unset dhcp subnet sub1 dynamic 192.168.1.152
```

相关命令

命令名称	描述信息
dhcp subnet dynamic	为指定的作用域添加动态地址列表。

unset dhcp subnet gateway, wins, dns, smtp, pop3, news, nis

使用 **unset dhcp subnet gateway, wins, dns, smtp, pop3, news, nis** 命令删除指定作用域的特定服务的 IP 地址。

命令

unset dhcp subnet *subnet_name* {**gateway** | **wins** | **wins2**| **dns** | **dns2**| **dns3** | **smtp** | **pop3** | **news** | **nis**}

语法

subnet_name	作用域名称，格式为 WORD<1-15>。
gateway	**wins**	**wins2**| **dns**	**dns2**| **dns3**	**smtp**	**pop3**	**news**	**nis**	允许分配给该作用域的主机的特殊服务。 • gateway— 网关 • wins—WINS 服务器 • wins2— 副 WINS 服务器 • dns— DNS 服务器 • dns2— 副 DNS 服务器 • dns3— 第三 DNS 服务器 • smtp— SMTP 服务器 • pop3 — POP3 服务器 • news— NEWS 服务器 • nis— 网络信息服务器

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
dhcp subnet gateway, wins, dns, smtp, pop3, news, nis	设置指定作用域的特定服务的 IP 地址。

unset dhcp subnet nistag

使用 **unset dhcp subnet nistag** 命令删除指定作用域的网络信息服务器的标签。

命令

unset dhcp subnet *subnet_name* **nistag**

语法

subnet_name	作用域名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
dhcp subnet nistag	设置指定作用域的网络信息服务器的标签。

unset dhcp subnet reserve

使用 **unset dhcp subnet reserve** 命令删除指定作用域的特定保留地址。

命令

unset dhcp subnet *subnet_name* **reserve** {*ip_address* | *mac_address*}

语法

subnet_name	作用域名称，格式为 WORD<1-15>。
ip_address	IP 地址，格式为 x.x.x.x。
mac_address	MAC 地址，格式为 HH:HH:HH:HH:HH:HH。

说明

1. 如果指定 *ip_address* 参数，表示删除指定作用域的特定 IP 地址的保留地址。
2. 如果指定 *mac_address* 参数，表示删除指定作用域的特定 MAC 地址的保留地址。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除作用域 sub2 的 IP 地址为 192.168.1.152 的保留地址。

```
NetEye@root-system]unset dhcp subnet sub2 reserve 192.168.1.152
```

相关命令

命令名称	描述信息
dhcp subnet reserve	设置指定作用域的保留地址。

DNS

dns cache

使用 **dns cache** 命令添加静态 DNS 缓存，静态 DNS 缓存可以加快客户端请求的回应速度。

命令

dns cache *domain_name ip_address* **input-interface** {**any** | *interface_name*}

语法

domain_name	域名，格式为 WORD<1-255>。
ip_address	IP 地址，格式为 x.x.x.x。
input-interface	数据入口三层接口。
interface_name	接口名称，格式为 WORD<1-16>。 **any** 表示任意接口。

说明

1. 当内网用户做 DNS 查询时，首先查找静态缓存中的记录。
2. 对于同一个域名，可以有多个对应的 IP 地址。
3. 静态缓存共支持 2048 个条目，每条静态缓存信息可以配置 64 条 IP 地址。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加域名为 www.test.com 的静态 DNS 缓存，对应的 IP 地址为 192.168.1.130 和 192.168.1.150，入口接口为 any。

```
NetEye@root-system]dns cache www.test.com 192.168.1.130 input-interface
any
NetEye@root-system]dns cache www.test.com 192.168.1.150 input-interface
any
```

相关命令

命令名称	描述信息
show dns cache	显示 DNS 缓存信息。
unset dns cache static	删除静态 DNS 缓存。

dns cache-state

使用 **dns cache-state** 命令启用或禁用 DNS 静态缓存。

命令

dns cache-state {**on** | **off**}

语法

on | off	• on— 启用 DNS 静态缓存 • off— 禁用 DNS 静态缓存

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show dns cache-state	显示 DNS 静态缓存状态。

dns host

使用 **dns host** 命令配置 NetEye 域名服务器。配置成功后， NetEye 将使用所配置的域名服务器来解析域名。

命令

dns host *server_ip* {**primary** | **secondary** | **tertiary**}

语法

server_ip	DNS 服务器 IP 地址，格式为 x.x.x.x。 地址范围为 1.0.0.0-223.255.255.255。
primary	表示所配置的 DNS 服务器为首选 DNS 服务器。
secondary	表示所配置的 DNS 服务器为次选 DNS 服务器。
tertiary	表示所配置的 DNS 服务器为第三位备选 DNS 服务器。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show dns host	显示 DNS 服务器配置。
unset dns host	删除域名服务器配置。

dns server-select

使用 **dns server-select** 命令添加 DNS 代理服务器。DNS 代理功能主要起一个代理中继的作用， DNS 请求的数据包首先送到 NetEye，然后 NetEye 来作为客户端向 DNS 服务器查询，然后将查询结果返回给用户，同时缓存该记录。

命令

dns server-select *domain_name* **output-interface** {**any** | *interface_name*} **primary** *server_ip* [**secondary** *server_ip* [**tertiary** *server_ip*]]

语法

domian_name	域名，格式为 WORD<1-255>。
output-interface	表示 DNS 请求的发送接口。
interface_name	接口名称，格式为 WORD<1-16>。 **any** 表示任意接口。
primary	表示所配置的 DNS 服务器为首选 DNS 服务器。
server_ip	DNS 服务器 IP 地址，格式为 x.x.x.x。
secondary	表示所配置的 DNS 服务器为次选 DNS 服务器。
tertiary	表示所配置的 DNS 服务器为第三位备选 DNS 服务器。

说明

本命令中提到的接口指的是可路由的接口， HA 接口除外。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 添加 DNS 代理服务器，域名为 www.test.com，使 DNS 请求可以从任意接口发出去，首选服务器为 192.168.1.130，次选服务器为 192.168.1.150。

```
NetEye@root-system]dns server-select www.test.com output-interface any
primary 192.168.1.130 secondary 192.168.1.150
```

范例 2. 添加 DNS 代理服务器，域名为 *，使 DNS 请求可以从任意接口发出去，首选服务器为 192.168.1.134，次选服务器为 192.168.1.154。

```
NetEye@root-system]dns server-select * output-interface any primary
192.168.1.134 secondary 192.168.1.154
```

相关命令

命令名称	描述信息
show dns server-select	显示 DNS 代理配置信息。
unset dns server-select	删除 DNS 代理服务器。

show dns cache

使用 **show dns cache** 命令显示 DNS 缓存信息。 DNS 缓存是记录 IP 地址与域名的对应关系的列表，包括动态缓存和静态缓存。

命令

show dns cache [*domain_name* | **dynamic** | **static**]

语法

domain_name	域名，格式为 WORD<1-255>。
dynamic	表示显示动态缓存信息。
static	表示显示静态缓存信息。

说明

1. 如果只输入 **show dns cache** 命令，而不选择可选参数或关键字，则表示显示所有 DNS 缓存信息。
2. 如果指定 *domain_name* 参数，表示显示指定域名的 DNS 缓存信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示域名为 com.cn 的 DNS 缓存信息。

```
NetEye@root>show dns cache com.cn
```

【返回结果】

```
  Domain Name: com.cn
  Type: Static
  Host Addresses and Input-Interfaces:
    192.168.1.130    Any
    192.168.1.150    Any
```

相关命令

命令名称	描述信息
dns cache	添加静态 DNS 缓存。
unset dns cache dynamic	删除动态 DNS 缓存。
unset dns cache static	删除静态 DNS 缓存。

show dns cache-state

使用 **show dns cache-state** 命令显示 DNS 静态缓存状态。

命令

show dns cache-state

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 DNS 静态缓存状态。

```
NetEye@root>show dns cache-state
```

【返回结果】

```
DNS cache state: off
```

相关命令

命令名称	描述信息
dns cache-state	启用或禁用 DNS 静态缓存。

show dns host

使用 **show dns host** 命令显示 DNS 服务器配置信息。

命令

show dns host

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 DNS 配置信息。

```
NetEye@root>show dns host
```

【返回结果】

```
DNS list
    Primary: 10.3.1.212
    Secondary:
    Tertiary :
```

相关命令

命令名称	描述信息
dns host	配置 NetEye 域名服务器。
unset dns host	删除域名服务器配置。

show dns server-select

使用 **show dns server-select** 命令显示 DNS 代理配置信息。

命令

show dns server-select [*domain_name*]

语法

domain_name	域名，格式为 WORD<1-255>。

说明

如果不指定 *domain_name* 参数，表示显示所有的 DNS 代理配置信息。否则，表示显示指定域名的 DNS 代理配置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有 DNS 代理配置信息。

```
NetEye@root>show dns server-select
```

【返回结果】

```
Domain-Name                    Interface DNS-Servers
www.test.com                    any       192.168.1.130
com.cn                         any       192.168.1.150
```

相关命令

命令名称	描述信息
dns server-select	添加 DNS 代理服务器。
unset dns server-select	删除 DNS 代理服务器。

unset dns cache dynamic

使用 **unset dns cache dynamic** 命令删除动态 DNS 缓存。

命令

unset dns cache dynamic [*domain_name*]

语法

domain_name	域名，格式为 WORD<1-255>。

说明

如果不指定 *domain_name* 参数，表示删除所有的动态 DNS 缓存。否则，表示删除指定域名的动态 DNS 缓存。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show dns cache	显示 DNS 缓存信息。

unset dns cache static

使用 **unset dns cache static** 命令删除静态 DNS 缓存。

命令

unset dns cache static [*domain_name*]

语法

domain_name	域名，格式为 WORD<1-255>。

说明

如果不指定 *domain_name* 参数，表示删除所有的静态 DNS 缓存。否则，表示删除指定域名的静态 DNS 缓存。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
dns cache	添加静态 DNS 缓存。
show dns cache	显示 DNS 缓存信息。

unset dns host

使用 **unset dns host** 命令删除 DNS 服务器配置。

命令

unset dns host {**primary** | **secondary** | **tertiary** | **all**}

语法

primary	表示删除的 DNS 服务器为首选 DNS 服务器。
secondary	表示删除的 DNS 服务器为次选 DNS 服务器。
tertiary	表示删除的 DNS 服务器为第三位备选 DNS 服务器。
all	表示删除所有 DNS 服务器。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
dns host	配置 NetEye 域名服务器。
show dns host	显示 DNS 服务器配置信息。

unset dns server-select

使用 **unset dns server-select** 命令删除 DNS 代理服务器。

命令

unset dns server-select [*domain_name*]

语法

domain_name	域名，格式为 WORD<1-255>。

说明

如果不指定 *domain_name* 参数，表示删除所有的 DNS 代理服务器。否则，表示删除指定域名的 DNS 代理服务器。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
dns serrver-select	添加 DNS 代理服务器。
show dns server-select	显示 DNS 代理配置信息。

4 服务配置命令

访问设置

banner

使用 **banner** 命令设置或者修改 NetEye 的 Banner 信息。

命令

banner {**console** | **vty**} *string*

语法

string	Banner 信息，格式为 LINE。
vty	虚拟端口，支持的协议包括 Telnet 和 SSH 方式。通过 Telnet 和 SSH 方式登录 NetEye 后，显示相同的 Banner 信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置以 Console 方式登录到 NetEye 显示的 Banner 信息为：HELLO。

```
NetEye@root-system]banner console HELLO
```

相关命令

命令名称	描述信息
show banner	显示 NetEye 的 Banner 信息。

console timeout

使用 **`console timeout`** 命令配置 Console 超时时间。配置成功后，通过 Console 方式登录到 NetEye，如果系统处于空闲状态的时间超过设置的超时时间，管理员终端会自动退出登录界面。

命令

console timeout *time*

语法

time	超时时间，单位为分钟，“0”表示永不超时，默认值为 10 分钟。格式为 INTEGER<0-120>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

service

使用 **service** 命令启用或禁用指定的访问控制项。

命令

service {telnet | web | ping | ssh | scm-console} {on | off}

语法

telnet	Telnet 服务，表示可以通过 Telnet 方式登录到命令行来管理 NetEye。
web	Web 服务，表示可以通过 Web 界面来管理 NetEye。
ssh	SSH 服务，表示可以通过 SSH 方式登录到命令行来管理 NetEye。
ping	Ping 服务，表示可以使用 Ping 命令验证与 NetEye 的连接是否保持畅通。
scm-console	SCM 服务，表示可以通过 SCM Console 登录 NetEye。
on | off	• on— 启用服务 • off— 禁用服务

说明

Telnet、 Ping 以及 SCM 服务默认为 off，其他服务默认为 on。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 禁用 Telnet 服务。

```
NetEye@root-system]service telnet off
```

service allow zone

使用 **service allow zone** 命令为指定的访问控制项添加访问控制策略。配置成功后，管理员可以根据指定访问控制项的访问控制策略登录到 NetEye。

命令

service {**telnet** | **web** | **ssh** | **ping** | **scm-console**} **allow zone** {*zone_name* | **any**} *start_ip* [*end_ip*]

语法

telnet	Telnet 服务，表示可以通过 Telnet 方式登录到命令行来管理 NetEye。
web	Web 服务，表示可以通过 Web 界面来管理 NetEye。
ssh	SSH 服务，表示可以通过 SSH 方式登录到命令行来管理 NetEye。
ping	Ping 服务，表示可以使用 Ping 命令验证与 NetEye 的连接是否保持畅通。
scm-console	SCM 服务，表示可以通过 SCM Console 登录 NetEye。
zone	安全域。
zone_name	安全域名称，格式为 WORD<1-15>。 **any** 表示任意安全域。
start_ip	起始 IP 地址，格式为 x.x.x.x。
end_ip	终止 IP 地址，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 指定 IP 地址为 192.168.1.128 的设备通过 Telnet 方式访问 NetEye。

```
NetEye@root-system]service telnet allow zone any 192.168.1.128
```

相关命令

命令名称	描述信息
show service	显示访问控制项的配置信息。
unset service	删除指定访问控制项的访问控制策略。

service root-net-login enable, disable

使用 **service root-net-login enable, disable** 命令修改根管理员远程访问控制状态。

命令

service root-net-login {**enable** | **disable**}

语法

root-net-login	设置根管理员远程访问控制状态。
enable | **disable**	• enable— 允许根管理员远程访问 NetEye • disable— 禁止根管理员远程访问 NetEye 缺省设置为 enable

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 允许根管理员远程访问 NetEye。

```
NetEye@root-system]service root-net-login enable
```

相关命令

命令名称	描述信息
show root-net-login	显示根管理员远程访问控制状态信息。

service telnet, ssh, web port

使用 **service telnet, ssh, web port** 命令修改指定访问控制项的端口号。

命令

service {**telnet** | **ssh** | **web**} **port** *num*

语法

telnet | **ssh** | **web**	• telnet— Telnet 服务 缺省设置为 23 • ssh— SSH 服务 缺省设置为 22 • web— Web 服务 缺省设置为 443
num	服务器端口号，格式为 INTEGER<1-65535>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 修改 Web 访问控制项的端口号为 500。

```
NetEye@root-system]service web port 500
```

相关命令

命令名称	描述信息
show service port	显示访问控制项的端口号。

show banner

使用 **show banner** 命令显示 NetEye 的 Banner 信息。

命令

show banner

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 NetEye 的 Banner 信息。

```
NetEye@root>show banner
```

【返回结果】

```
Console: Neusoft NetEye
Telnet/Ssh: Neusoft NetEye
```

相关命令

命令名称	描述信息
banner	设置或者修改 NetEye 的 Banner 信息。

show root-net-login

使用 **show root-net-login** 显示根管理员远程访问控制状态信息。

命令

show root-net-login

语法

root-net-login	设置根管理员远程访问控制状态。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 显示根管理员远程访问控制状态信息。

```
NetEye@root>show root-net-login
```

【返回结果】

```
root net login: enable
```

相关命令

命令名称	描述信息
service root-net-login enable, disable	修改根管理员远程访问控制状态。

show service

使用 **show service** 命令显示访问控制项的配置信息。

命令

show service [**telnet** | **web** | **ssh** | **ping** | **scm-console**]

语法

telnet	Telnet 服务，表示可以通过 Telnet 方式登录到命令行来管理 NetEye。
web	Web 服务，表示可以通过 Web 界面来管理 NetEye。
ssh	SSH 服务，表示可以通过 SSH 方式登录到命令行来管理 NetEye。
ping	Ping 服务，表示可以使用 Ping 命令验证与 NetEye 的连接是否保持畅通。
scm-console	SCM 服务，表示可以通过 SCM Console 登录 NetEye。

说明

如果不指定 telnet、 web、 ssh、 ping 和 scm-console 中任一关键字，表示显示所有服务的配置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 Telnet 服务的配置信息。

```
NetEye@root>show service telnet
```

【返回结果】

```
Telnet service:
  Allow Access:Yes      Auth:local
  Access:allow Any              0.0.0.0-255.255.255.255
```

show service port

使用 **show service port** 命令显示访问控制项的端口号。其中访问控制项包括：Telnet， WEB 和 SSH。

命令

show service port

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示访问控制项的端口号信息。

```
NetEye@root>show service port
```

【返回结果】

```
Telnet port: 23
   SSH port: 22
   Web port: 443
```

相关命令

命令名称	描述信息
service telnet, ssh, web port	修改指定访问控制项的端口号。

unset service

使用 **unset service** 命令删除指定访问控制项的访问控制策略。

命令

unset service {**telnet** | **web** | **ssh** | **ping** | **scm-console**} [**allow zone** {*zone_name* | **any**} *start_ip* [*end_ip*]]

语法

telnet	Telnet 服务，表示可以通过 Telnet 方式登录到命令行来管理 NetEye。
web	Web 服务，表示可以通过 Web 界面来管理 NetEye。
ssh	SSH 服务，表示可以通过 SSH 方式登录到命令行来管理 NetEye。
ping	Ping 服务，表示可以使用 Ping 命令验证与 NetEye 的连接是否保持畅通。
scm-console	SCM 服务，表示可以通过 SCM Console 登录 NetEye。
zone	安全域。
zone_name	安全域名称，格式为 WORD<1-15>。 **any** 表示任意安全域。
start_ip	起始 IP 地址，格式为 x.x.x.x。
end_ip	终止 IP 地址，格式为 x.x.x.x。

说明

如果不指定 **allow zone** 关键字及其后面的参数，则表示删除指定访问控制项的所有访问控制策略。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在全局配置模式下使用。

范例

范例 . 限定 IP 地址为 192.168.1.128 的设备不可以通过 Telnet 方式访问 NetEye。

```
NetEye@root-system]unset service Telnet allow zone any 192.168.1.128
```

相关命令

命令名称	描述信息
service allow zone	为指定的访问控制项添加访问控制策略。
show service	显示访问控制项的配置信息。

vty timeout

使用 **vty timeout** 命令配置 Telnet 和 SSH 超时时间。配置成功后，通过 Telnet 或 SSH 方式登录到 NetEye，如果系统处于空闲状态的时间超过设置的超时时间，管理员终端会自动退出登录界面。

命令

vty timeout *time*

语法

vty	虚拟终端连接，包含 SSH 和 Telnet。
time	超时时间，以分钟为单位，“0”表示永不超时，默认值为 10 分钟。格式为 INTEGER<0-120>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

Web 配置

web generate ssl-certificate request

使用 **web generate ssl-certificate request** 命令生成证书请求及对应的密钥。配置成功后，回显证书请求和密钥内容，供管理员保存和使用。

命令

web generate ssl-certificate request key-bits *key_length* **country** *country_name* **state-or-province** *state_name* **locality** {**none** | *locality_name*} **organization** *organization_name* **organizational-unit** {**none** | *unit_name*} **common-name** *common_name* **email-address** {**none** | *email_address*} **passphrase** {**none** | *password*}

语法

generate	生成证书请求及对应的密钥。
ssl-certificate	SSL 认证证书。
request	表示证书请求。
key_length	密钥长度。单位：位 （bit），可选长度为 512， 768， 1024。
country_name	国家名称，格式为 WORD<2-2>。
state_name	州或省份名称，格式为 WORD<1-127>。
locality_name	城市名称，格式为 WORD<1-127>。
organization_name	公司名称，格式为 WORD<1-64>。
unit_name	部门名称，格式为 WORD<1-64>。
common_name	公共域名，格式为 WORD<1-64>。
email_address	邮件地址，格式为 WORD<3-40>。
password	*password* 表示密钥口令，格式为 WORD<4-256>。 **none** 表示不对密钥进行加密。

说明

1. 密钥长度值越大，相应的解密、加密时间越长。
2. 密钥默认采用 RSA 非对称算法。如果指定 *password* 参数，表示使用对称加密算法 3DES 对私钥进行加密保护。

3. 国家名称的格式取值范围为数字和字母。州或省份名称、城市名称、公司名称、部门名称、公共域名和邮件地址的格式取值范围为数字、字母和特殊字符 （不包含 "、'、 <、 >、 &、 \、 /、 !、 ‘、 $ 和 #）。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 生成密钥长度为 1024 位，密钥保护口令为 test，国家为 CN(China)，省份为 Liaoning，城市为 Shenyang，公司为 NTC，公共域名为 www.NTC.com，邮件地址为 stone@NTC.com 的证书请求及密钥文件。

```
NetEye@root-system]web generate ssl-certificate request key-bits 1024
country CN state-or-province Liaoning locality Shenyang organization
NTC organizational-unit none common-name www.NTC.com email-address
stone@NTC.com passphrase test
```

相关命令

命令名称	描述信息
web install ssl-certificate	上载 SSL 证书。

web generate ssl-certificate self-signed

使用 **web generate ssl-certificate self-signed** 命令生成自签名证书及对应的密钥。配置成功后，回显证书和密钥内容，供管理员保存和使用。

命令

web generate ssl-certificate self-signed certificate *certificate_name* **key** *key_name* **key-bits** *key_length* **country** *country_name* **state-or-province** *state_name* **locality** {**none** | *locality_name*} **organization** *organization_name* **organizational-unit** {**none** | *unit_name*} **common-name** *common_name* **email-address** {**none** | *email_address*} **passphrase** {**none** | *password*}

语法

generate	生成自签名证书及对应的密钥。
ssl-certificate	SSL 认证证书。
self-signed	表示自签名证书。
certificate_name	证书文件名，格式为 WORD<1-127>。
key_name	密钥文件名，格式为 WORD<1-127>。
key_length	密钥长度。单位：位 （bit），可选长度为 512， 768， 1024。
country_name	国家名称，格式为 WORD<2-2>。
state_name	州或省份名称，格式为 WORD<1-127>。
locality_name	城市名称，格式为 WORD<1-127>。
organization_name	公司名称，格式为 WORD<1-64>。
unit_name	部门名称，格式为 WORD<1-64>。
common_name	公共域名，格式为 WORD<1-64>。
email_address	邮件地址，格式为 WORD<3-40>。
password	*password* 表示密钥口令，格式为 WORD<4-256>。 **none** 表示不对密钥进行加密。

说明

1. 密钥长度值越大，相应的解密、加密时间越长。
2. 密钥默认采用 RSA 非对称算法。如果指定 *password* 参数，表示使用对称加密算法 3DES 对私钥进行加密保护。
3. 证书文件名和密钥文件名不可以相同。

4. 国家名称的格式取值范围为数字和字母。州或省份名称、城市名称、公司名称、部门名称、公共域名和邮件地址的格式取值范围为数字、字母和特殊字符 （不包含 "、'、 <、 >、 &、 \、 /、 !、 ‘、 $ 和 #）。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 生成证书文件名为 test.crt，密钥文件名为 test.key，密钥长度为 1024 位，密钥保护口令为 test，国家为 CN(China)，省份为 Liaoning，城市为 Shenyang，公司为 NTC，公共域名为 www.NTC.com，邮件地址为 stone@NTC.com 的自签名证书及密钥文件。

```
NetEye@root-system]web generate ssl-certificate self-signed certificate
test.crt key test.key key-bits 1024 country CN state-or-province
Liaoning locality Shenyang organization NTC organizational-unit none
common-name www.NTC.com email-address stone@NTC.com passphrase test
```

相关命令

命令名称	描述信息
web install ssl-certificate	上载 SSL 证书。

web install ssl-certificate

使用 **web install ssl-certificate** 命令上载 SSL 证书和密钥。配置成功后，可以重启 HTTPS 服务，使用新证书对 HTTPS 服务器进行验证。

命令

web install ssl-certificate from {**tftp** *ip_tftp* **certificate** *certificate_name* **key** *key_name* **| x/zmodem | sftp** *ip_sftp* **username** *user_name* **password** *passwd* **certificate** *certificate_name* **key** *key_name*} **passphrase** {**none** | *password*}

web install ssl-certificate self-signed certificate *certificate_name* **key** *key_name* **passphrase** {**none** | *password*}

语法

ssl-certificate	SSL 认证证书。
tftp	简单文件传输协议，表示从 TFTP 服务器导入 SSL 证书和密钥。
ip_tftp	TFTP 服务器 IP 地址，格式为 x.x.x.x。
x/zmodem	异步文件传输协议， Xmodem 或 Zmodem 由系统自动选择。表示使用 x/zmodem 协议导入 SSL 证书和密钥。
sftp	安全文件传输协议，表示从 SFTP 服务器导入 SSL 证书和密钥。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-64>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-64>。
certificate_name	证书文件名，格式为 WORD<1-127>。
key_name	密钥文件名，格式为 WORD<1-127>。
none | *password*	*password* 表示密钥口令，格式为 WORD<4-256>。 **none** 表示不对密钥进行加密。
self-signed	表示自签名证书。

说明

1. 自签名证书生成后直接部署在 NetEye 中，所有不必进行上载。
2. 证书文件名和密钥文件名不可以相同。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 1. 使用密钥保护口令 test，从 TFTP 服务器 192.168.1.111 导入本地证书 server.crt 和密钥 server.key 到 NetEye。

```
NetEye@root-system]web install ssl-certificate from tftp 192.168.1.111
certificate test.crt key test.key passphrase test
```

范例 2. 使用密钥保护口令 test，从 SFTP 服务器 192.168.1.100 导入本地证书 server.crt 和密钥 server.key 到 NetEye， SFTP 服务器的用户名、密码均为 mike。

```
NetEye@root-system]web install ssl-certificate from sftp 192.168.1.100
username mike password mike certificate test.crt key test.key
passphrase test
```

范例 3. 使用密钥保护口令 test，上载自签名证书 test.crt 及其相应密钥 test.key。

```
NetEye@root-system]web install ssl-certificate self-signed certificate
test.crt key test.key passphrase test
```

相关命令

命令名称	描述信息
web generate ssl-certificate self-signed	生成证书。
web generate ssl-certificate request	生成证书请求。

SSH

import ssh authkeys

使用 **`import ssh authkeys`** 命令导入 SSHv2 或 SSHv1 版本公钥。

命令

import ssh authkeys {**v1 rsa** | **v2** {**rsa** | **dsa**}} **from** {**tftp** *ip_tftp file_name* | **x/zmodem | sftp** *ip_sftp* **username** *user_name* **password** *passwd sftp_file_name*}

语法

authkeys	认证密钥。
v1	**v2**	NetEye 支持的 SSH 协议版本。 • v1— 版本 1 • v2— 版本 2
rsa	**dsa**	非对称加密算法。 • rsa—RSA 算法，既能用于数据加密也能用于数字签名 • dsa—DSA 算法，只能用于数字签名
tftp	简单文件传输协议，表示从 TFTP 服务器导入公钥。
ip_tftp	TFTP 服务器 IP 地址，格式为 x.x.x.x。
file_name	公钥文件名，格式为 WORD<1-128>。
x/zmodem	异步文件传输协议， Xmodem 或 Zmodem 由系统自动选择。表示使用 x/zmodem 协议导入公钥。
sftp	安全文件传输协议，表示从 SFTP 服务器导入公钥。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-64>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-64>。
sftp_file_name	通过 sftp 上载的公钥文件的路径及文件名，格式为 WORD<1-256>。

说明

1. 导入的公钥可以是OpenSSH或SSH2格式。如果是SSH2格式，会对其进行自动格式转换，将其转换为 OpenSSH 格式。
2. 公钥默认的文件名扩展名是 .pub。
3. 如果用 **x/zmodem** 导入，会弹出对话框让管理员指定文件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在全局配置模式下使用。

范例

范例 1. 从 TFTP 服务器 192.168.1.100 导入 SSHv2 版本的 RSA 公钥，公钥文件名为 test.pub。

```
NetEye@root-system]import ssh authkeys v2 rsa from tftp 192.168.1.100 test.pub
```

范例 2. 从 SFTP 服务器 192.168.1.25 导入 SSHv1 版本的 RSA 公钥，公钥文件名为 test.pub， SFTP 服务器的用户名、密码均为 mike。

```
NetEye@root-system]import ssh authkeys v1 rsa from sftp 192.168.1.25 username mike password mike test.pub
```

show ssh hostkey

使用 **show ssh hostkey** 命令显示 SSHv2 或 SSHv1 主机密钥信息。

命令

show ssh hostkey {**v1 rsa** | **v2** {**rsa** | **dsa**} [**ssh2-format**]}

语法

hostkey	主机密钥。
v1	**v2**	NetEye 支持的 SSH 协议版本。 • v1— 版本 1 • v2— 版本 2
rsa	**dsa**	非对称加密算法。 • rsa—RSA 算法，既能用于数据加密也能用于数字签名 • dsa—DSA 算法，只能用于数字签名
ssh2-format	SSH2 格式，表示以 SSH2 格式显示密钥内容。

说明

1. 选择RSAv1主机密钥，可以显示其密钥长度、指数和模；选择RSAv2或DSAv2主机密钥，可以 OpenSSH 和 SSH2 两种格式显示其内容。
2. 如果指定 **ssh2-format** 关键字，表示把密钥内容从OpenSSH格式转换成SSH2格式，然后以 SSH2 格式显示密钥内容；如果不指定 **ssh2-format** 关键字，表示以 OpenSSH 格式显示密钥内容。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 SSH2 格式的 SSHv2 的 DSA 主机密钥信息。

```
NetEye@root>show ssh hostkey v2 dsa ssh2-format
```

【返回结果】

```
---- BEGIN SSH2 PUBLIC KEY ----
```

```
Comment: "DSA key converted from OpenSSH format"
AAAAB3NzaC1kc3MAAACBAJTH1/sKCLJijfCkPr1zzxzyNQJfKss9my/zsi6MFEZTzF9MqV
WpaOe6hrYUcERzrAy6+J7kEoe53R+9j+84SLozClwcj652523FSXWsozTE2VJsKlfCI/4g
2VRmv+7d1b+BL0+u5/EClyaMr7Yfd8yQvbezKqD+3ZMiiAHpCK09AAAAFQClDyCMVZAhd+
6Y9TpzKgoZXqmopwAAAIArq2cYc3P6+aads/oH9VDJiC3hZrbvLJahVA2/pbMsBRppqwyr
5Iz483V/7SrCWNB/LTmSDSerY42/9Smifx6oL03W8r8/KXKSuma+Z8WiceIS56X3dBEs2i
BNxqcBUU8owDzVLAMKbyQmn0eTwqMZhERLK1V6H6Pn6i+xLKU0/gAAAIBSkJjorkK772gn
JCKV5nGuacxAR+vNvbv84USO0KWA0PG7mNLq6jNf3wEF+m5YqowR5GiU5em1OIMjoy9Wwa
OnNGHk2l35PuffN0+h96K5SNWhF7EMebmK5zauUhIFOUZRwQbHO1DzW9sW+8Bvly/9ZZYX
vPNjRrcGTcY4G/vhIA==
---- END SSH2 PUBLIC KEY ----
```

相关命令

命令名称	描述信息
ssh hostkey	更新主机密钥。

show ssh server authentication

使用 **show ssh server authentication** 命令显示 SSH 服务对认证方式的支持情况。

命令

show ssh server authentication {**pubkey** | **passwd** | **rsa**}

语法

pubkey | **passwd** | **rsa**	• pubkey—Pubkey 认证方式，仅在 SSH v2 下有效 • passwd—Password 认证方式 • rsa—RSA 认证方式，仅在 SSHv1 下有效

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 SSH 服务对 Pubkey 认证方式的支持情况。

```
NetEye@root>show ssh server authentication pubkey
```

【返回结果】

```
PubkeyAuthentication yes
```

相关命令

命令名称	描述信息
ssh server authentication	设置认证方式。

show ssh server ciphers

使用 **show ssh server ciphers** 命令显示 SSH 加密算法。

命令

show ssh server ciphers

语法

ciphers	表示加密算法。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 SSH 服务支持的加密算法。

```
NetEye@root>show ssh server ciphers
```

【返回结果】

```
Ciphers 3des-cbc,blowfish-cbc,arcfour,cast128-cbc,aes128-cbc,aes192-
cbc,aes256-cbc
```

相关命令

命令名称	描述信息
ssh server ciphers	设置 SSH 加密算法。

show ssh server key-regeneration-time

使用 **show ssh server key-regeneration-time** 命令显示生成服务器密钥的时间间隔值。

命令

show ssh server key-regeneration-time

语法

key-regeneration-time	表示生成服务器密钥的时间间隔值。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 显示生成服务器密钥的时间间隔值。

```
NetEye@root>show ssh server key-regeneration-time
```

【返回结果】

```
KeyRegenerationInterval 3600
```

相关命令

命令名称	描述信息
ssh server key-regeneration-time	设置生成服务器密钥的时间间隔值。

show ssh server login-grace-time

使用 **show ssh server login-grace-time** 命令显示宽限登录时间。

关于宽限登录时间，表示 SSH 服务器等待完成认证的时间限制值。

命令

show ssh server login-grace-time

语法

login-grace-time	表示宽限登录时间。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 SSH 服务支持的宽限登录时间。

```
NetEye@root>show ssh server login-grace-time
```

【返回结果】

```
LoginGraceTime 600
```

相关命令

命令名称	描述信息
ssh server login-grace-time	设置宽限登录时间。

show ssh server protocol

使用 **show ssh server protocol** 命令显示 SSH 服务支持的协议版本信息。

命令

show ssh server protocol

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 SSH 服务支持的协议版本信息。

```
NetEye@root>show ssh server protocol
```

【返回结果】

```
Protocol 2,1
```

相关命令

命令名称	描述信息
ssh server protocol	设置 SSH 服务支持的协议版本。

show ssh server server-key-bits

使用 **show ssh server server-key-bits** 命令显示服务器密钥的长度信息。

命令

show ssh server server-key-bits

语法

server-key-bits	表示服务器密钥长度。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 显示服务器密钥的长度信息。

```
NetEye@root>show ssh server server-key-bits
```

【返回结果】

```
ServerKeyBits 768
```

相关命令

命令名称	描述信息
ssh server server-key-bits	设置服务器密钥的长度。

ssh hostkey

使用 **ssh hostkey** 命令更新 SSHv1 或 SSHv2 主机密钥。

命令

ssh hostkey {**v1 rsa** | **v2** {**rsa** | **dsa**}} *key_length*

语法

hostkey	主机密钥。
v1	**v2**	NetEye 支持的 SSH 协议版本。 • v1—版本 1 • v2—版本 2
rsa	**dsa**	非对称加密算法。 • rsa—RSA 算法，既能用于数据加密也能用于数字签名 • dsa—DSA 算法，只能用于数字签名
key_length	密钥长度。单位：位（bit），可选长度为 512，640，768，896，1024。

说明

1. 更新主机密钥允许选择主机密钥长度和加密算法及其支持的协议版本。
2. 主机密钥长度值越大，安全性越高，所以推荐使用 1024bits。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 更新 SSHv1 主机密钥，设置主机密钥长度为 1024bits。

```
NetEye@root-system]ssh hostkey v1 rsa 1024
```

相关命令

命令名称	描述信息
show ssh hostkey	显示主机密钥信息。

ssh server authentication

使用 **ssh server authentication** 命令设置 SSH 服务的认证方式。

命令

ssh server authentication {pubkey | passwd | rsa} {on | off}

语法

pubkey | passwd | rsa	• pubkey— 公共密钥 （Pubkey）认证方式，仅在 SSHv2 下有效 • passwd— 用户名密码 （Password）认证方式 • rsa—RSA 认证方式，仅在 SSHv1 下有效
on | off	• on— 支持认证方式 • off— 不支持认证方式

说明

1. Password认证方式允许输入用户名和密码进行验证，Pubkey认证和RSA认证允许通过用户名和用户认证公钥进行验证。
2. 出于安全性考虑，最好选择支持 Pubkey 和 RSA 认证。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 设置 SSH 服务支持 Pubkey 认证方式。

```
NetEye@root-system]ssh server authentication pubkey on
```

相关命令

命令名称	描述信息
show ssh server authentication	显示 SSH 服务对认证方式的支持情况。

ssh server ciphers

使用 **ssh server ciphers** 命令设置 SSH 加密算法。

命令

ssh server ciphers *algorithm_name*

语法

ciphers	表示加密算法。
algorithm_name	算法名称，格式为 WORD<1-128>。该选项为加密算法与加密模式的组合，具体选项有 3des-cbc， blowfish-cbc， arcfour，cast128-cbc， aes128-cbc， aes192-cbc， aes256-cbc。

说明

关于加密模式，目前 NetEye 只采用加密分组链接 （CBC）模式。

提示

该命令只可以设置 SSHv2 的加密算法，但对 SSHv1 无效。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 设置 SSH 服务支持的加密算法为 3des-cbc。

```
NetEye@root-system]ssh server ciphers 3des-cbc
```

相关命令

命令名称	描述信息
show ssh server ciphers	显示 SSH 加密算法。

ssh server key-regeneration-time

使用 **ssh server key-regeneration-time** 命令设置生成服务器密钥的时间间隔值。系统缺省的默认值为 3600 秒。

命令

ssh server key-regeneration-time *interval_time*

语法

key-regeneration-time	表示生成服务器密钥的时间间隔值。
interval_time	时间间隔值。单位为秒，格式为 INTEGER<0-65535>。设置为 0 表示不再重新生成服务器密钥。

说明

服务器密钥仅在 SSHv1 下有效。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 设置生成服务器密钥的时间间隔值为 5000 秒。

```
NetEye@root-system]ssh server key-regeneration-time 5000
```

相关命令

命令名称	描述信息
show ssh server key-regeneration-time	显示生成服务器密钥的时间间隔值。

ssh server login-grace-time

使用 **ssh server login-grace-time** 命令设置宽限登录时间 , 系统缺省的默认值为 600 秒。

关于宽限登录时间，表示 SSH 服务器等待管理员完成认证的时间限制值。

命令

ssh server login-grace-time *grace_time*

语法

login-grace-time	表示宽限登录时间。
grace_time	宽限登录时间。单位为秒，格式为 INTEGER<0-65535>。设置为 0 表示没有时间限制。

说明

如果发出 SSH 连接请求后，在宽限登录时间内没有完成认证和登录，则自动断开此次 SSH 连接。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 设置 SSH 宽限登录时间为 1000 秒。

```
NetEye@root-system]ssh server login-grace-time 1000
```

相关命令

命令名称	描述信息
show ssh server login-grace-time	显示宽限登录时间。

ssh server protocol

使用 **ssh server protocol** 命令设置 SSH 服务支持的协议版本。

命令

ssh server protocol {**v1** | **v2** | **all**}

语法

v1	**v2**	**all**	NetEye 支持的 SSH 协议版本。 • v1— 版本 1 • v2— 版本 2 • all— 版本 1 和版本 2 缺省设置为 all

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 设置 SSH 服务支持协议 v1 版本。

```
NetEye@root-system]ssh server protocol v1
```

相关命令

命令名称	描述信息
show ssh server protocol	显示 SSH 服务支持的协议版本。

ssh server server-key-bits

使用 **ssh server server-key-bits** 命令设置服务器密钥的长度。系统缺省的默认值为 768bits。

命令

ssh server server-key-bits *key_length*

语法

server-key-bits	表示服务器密钥长度。
key_length	密钥长度。单位：位（bit），可选长度为 512，640，768，896，1024。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 设置服务器密钥的长度为 512bits。

```
NetEye@root-system]ssh server server-key-bits 512
```

相关命令

命令名称	描述信息
show ssh server server-key-bits	显示服务器密钥的长度信息。

5 对象命令

object description

使用 **object description** 命令添加指定对象的描述信息。

命令

object {**ipaddr** | **service** | **mac** | **protocol**} *object_name* **description** *string*

语法

object_name	对象名称，格式为 WORD<1-63>。
string	备注信息，格式为 LINE。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 为 IP 地址对象 test 添加描述信息：**This is ipaddr object**。

```
NetEye@root-system]object ipaddr test description This is ipaddr object
```

相关命令

命令名称	描述信息
object group description	添加指定对象组的描述信息。

object group

使用 **object group** 命令添加指定类型的对象组。

命令

object group *group_name* **type** {**ipaddr** | **service** | **mac** | **protocol**} [*object_list*]

语法

group_name	对象组名称，格式为 WORD<1-63>。
object_list	对象名称列表，格式为 WORD<1-1300>。

说明

如果不指定 *object_list* 参数，则添加空的对象组。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 添加一个空的服务对象组 test1。

```
NetEye@root-system]object group test1 type service
```

范例 2. 添加一个服务对象组 test2，其成员为服务对象 test3 和 test4。

```
NetEye@root-system]object group test2 type service test3,test4
```

相关命令

命令名称	描述信息
unset object	删除指定对象组的成员。

object group description

使用 **object group description** 命令添加指定对象组的描述信息。

命令

object group *group_name* **description** *string*

语法

group_name	对象组名称，格式为 WORD<1-63>。
string	备注信息，格式为 LINE。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 为对象组 test 添加描述信息：**This is object group。**

```
NetEye@root-system]object group test description This is object group
```

相关命令

命令名称	描述信息
object description	添加指定对象的描述信息。

object ipaddr

使用 **object ipaddr** 命令添加 IP 地址对象。

命令

object ipaddr *object_name* {*ip_address_list* | **subnet** *subnet_address subnet_mask*}

语法

object_name	对象名称，格式为 WORD<1-63>。
ip_address_list	IP 地址列表，格式为 IPV4LIST<1-32>。
subnet_address	子网 IP 地址，格式为 x.x.x.x。
subnet_mask	子网掩码，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加一个 IP 地址对象 test，其成员为 192.168.1.106 和 192.168.1.218。

```
NetEye@root-system]object ipaddr test 192.168.1.106,192.168.1.218
```

相关命令

命令名称	描述信息
unset object ipaddr	删除指定 IP 地址对象的成员。

object mac

使用 **object mac** 命令添加 MAC 地址对象。

命令

object mac *object_name maclist*

语法

object_name	对象名称，格式为 WORD<1-63>。
maclist	MAC 地址列表，格式为 MACLIST<1-32>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加一个 MAC 地址对象 test，其成员为 55:55:55:55:55:55 和 66:66:66:66:66:66。

```
NetEye@root-system]object mac test 55:55:55:55:55:55,66:66:66:66:66:66
```

相关命令

命令名称	描述信息
unset object mac	删除指定 MAC 地址对象的成员。

object protocol

使用 **object protocol** 命令添加协议对象。

命令

object protocol *object_name protocol_num*

语法

object_name	对象名称，格式为 WORD<1-63>。
protocol_num	协议号或协议号范围，格式为 NUMBER<1-65535>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加一个协议对象 test，其成员为 37 （数据报传送协议， DDP）。

```
NetEye@root-system]object protocol test 37
```

相关命令

命令名称	描述信息
unset object protocol	删除指定协议对象的成员。

object service

使用 **object service** 命令添加服务对象。

命令

object service *object_name* {{**tcp** | **udp**} {*src_port* | *srcport_range*} {*dst_port* | *dstport_ range*} | **icmp** {*icmp_type* | *icmp_list* | **any**} | **other** *protocol_num*}

语法

object_name	对象名称，格式为 WORD<1-63>。
src_port	源端口，格式为 INTEGER<1-65535>。
srcport_range	源端口范围，格式为 LIMIT。
dst_port	目的端口，格式为 INTEGER<1-65535>。
dstport_range	目的端口范围，格式为 LIMIT。
icmp_type	ICMP 协议类型，可以设置为： ECHO_and_ECHOREPLY； DEST_UNREACH； SOURCE_QUENCH； REDIRECT； ROUTER_ADVERTISEMENT； ROUTER_SOLICITATION； TIME_EXCEEDED； PARAMETERPROB； TIMESTAMP_and_TIMESTAMPREPLY； INFO_REQUEST_and_INFO_REPLY； ADDRESS_and_ADDRESSREPLY。 **any** 表示上述协议类型中的任意一种。
icmp_list	ICMP 的协议类型列表，格式为 WORD<1-256>。列表可以为下述协议类型的任意组合： ECHO_and_ECHOREPLY； INFO_REQUEST_and_INFO_REPLY； TIMESTAMP_and_TIMESTAMPREPLY； ADDRESS_and_ADDRESSREPLY； ROUTER_ADVERTISEMENT； ROUTER_SOLICITATION； DEST_UNREACH； SOURCE_QUENCH； REDIRECT； TIME_EXCEEDED； PARAMETERPROB。

other	除 TCP、 UDP 和 ICMP 之外的协议。
protocol_num	协议号或协议号范围，格式为 NUMBER<1-255>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 添加一个服务对象 test1，其成员的协议类型为 TCP，源端口号为 11，目的端口号为 12。

```
NetEye@root-system]object service test1 tcp 11 12
```

范例 2. 添加一个服务对象 test2，其成员的协议类型为 DDP （数据报传送协议，其对应的协议号为 37）。

```
NetEye@root-system]object service test2 other 37
```

相关命令

命令名称	描述信息
unset object service	删除指定服务对象的成员。

show object

使用 show **object** 命令显示指定类型对象的配置信息。

命令

show object {**ipaddr** | **service** | **mac** | **protocol**} [*object_name*]

语法

object_name	对象名称，格式为 WORD<1-63>。

说明

如果不指定 *object_name* 参数，则显示指定类型的所有对象的配置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 IP 地址对象 test 的配置信息。

```
NetEye@root>show object ipaddr test
```

【返回结果】

```
  Name: test
  Ip Address:
        Start Ip          End Ip            Mask
        192.168.1.11      192.168.1.128     -
  Comment:
        test
```

相关命令

命令名称	描述信息
show object group	显示对象组的配置信息。

show object group

使用 show **object group** 命令显示对象组的配置信息。

命令

show object group [*group_name*]

语法

group_name	对象组名称，格式为 WORD<1-63>。

说明

如果不指定 *group_name* 参数，则显示所有对象组的配置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有对象组的配置信息。

```
NetEye@root>show object group
```

【返回结果】

```
Name           Type          Objects
OBJG           IP Address    test
new            IP Address    test,test1
servicegroup   Service
```

相关命令

命令名称	描述信息
show object	显示指定类型对象的配置信息。

unset object

使用 **unset object** 命令删除指定对象组的成员。

命令

unset object group *group_name object_list*

语法

group_name	对象组名称，格式为 WORD<1-63>。
object_list	对象名称列表，格式为 WORD<1-1300>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除对象组 test1 的成员 test2 和 test3。

```
NetEye@root-system]unset object group test1 test2,test3
```

相关命令

命令名称	描述信息
object group	添加指定类型的对象组。

unset object group

使用 **unset object group** 命令删除对象组。

命令

unset object group [*group_name*]

语法

group_name	对象组名称，格式为 WORD<1-63>。

说明

如果不指定 *group_name* 参数，则删除所有的对象组。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除所有的对象组。

```
NetEye@root-system]unset object group
```

相关命令

命令名称	描述信息
unset object ipaddr, service, mac, protocol	删除指定类型的对象。

unset object ipaddr

使用 **unset object ipaddr** 命令删除指定 IP 地址对象的成员。

命令

unset object ipaddr *object_name* {*ip_address_list* | **subnet** *subnet_address subnet_mask*}

语法

object_name	对象名称，格式为 WORD<1-63>。
ip_address_list	IP 地址列表，格式为 IPV4LIST<1-32>。
subnet_address	子网 IP 地址，格式为 x.x.x.x。
subnet_mask	子网掩码，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除 IP 地址对象 test 的成员 192.168.1.106 和 192.168.1.224。

```
NetEye@root-system]unset object ipaddr test 192.168.1.106,192.168.1.224
```

相关命令

命令名称	描述信息
object ipaddr	添加 IP 地址对象。

unset object ipaddr, service, mac, protocol

使用 **unset object ipaddr, service, mac, protocol** 命令删除指定类型的对象。

命令

unset object {**ipaddr** | **service** | **mac** | **protocol**} [*object_name*]

语法

object_name	对象名称，格式为 WORD<1-63>。

说明

如果不指定 *object_name* 参数，则删除指定类型的所有对象。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除所有的 MAC 地址对象。

```
NetEye@root-system]unset object mac
```

相关命令

命令名称	描述信息
unset object group	删除对象组。

unset object mac

使用 **unset object mac** 命令删除指定 MAC 地址对象的成员。

命令

unset object mac *object_name maclist*

语法

object_name	对象名称，格式为 WORD<1-63>。
maclist	MAC 地址列表，格式为 MACLIST<1-32>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除 MAC 地址对象 test 的成员 55:55:55:55:55:55 和 66:66:66:66:66:66。

```
NetEye@root-system]unset object mac test
55:55:55:55:55:55,66:66:66:66:66:66
```

相关命令

命令名称	描述信息
object mac	添加 MAC 地址对象。

unset object protocol

使用 **unset object protocol** 命令删除指定协议对象的成员。

命令

unset object protocol *object_name protocol_num*

语法

object_name	对象名称，格式为 WORD<1-63>。
protocol_num	协议号或协议号范围，格式为 NUMBER<1-255>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除协议对象 test 的成员 37。

```
NetEye@root-system]unset object protocol test 37
```

相关命令

命令名称	描述信息
object protocol	添加协议对象。

unset object service

使用 **unset object service** 命令删除指定服务对象的成员。

命令

unset object service *object_name* {{**tcp | udp**} {*src_port* | *srcport_range*} {*dst_port* | *dstport_range*} | **icmp** {*icmp_type* | *icmp_list* | **any**} | **other** *protocol_num*}

语法

object_name	对象名称，格式为 WORD<1-63>。
src_port	源端口，格式为 INTEGER<1-65535>。
srcport_range	源端口范围，格式为 LIMIT。
dst_port	目的端口，格式为 INTEGER<1-65535>。
dstport_range	目的端口范围，格式为 LIMIT。
icmp_type	ICMP 协议类型，可以设置为： ECHO_and_ECHOREPLY； DEST_UNREACH； SOURCE_QUENCH； REDIRECT； ROUTER_ADVERTISEMENT； ROUTER_SOLICITATION； TIME_EXCEEDED； PARAMETERPROB； TIMESTAMP_and_TIMESTAMPREPLY； INFO_REQUEST_and_INFO_REPLY； ADDRESS_and_ADDRESSREPLY。 **any** 表示上述协议类型中的任意一种。
icmp_list	ICMP 的协议类型列表，格式为 WORD<1-256>。列表可以为下述协议类型的任意组合： ECHO_and_ECHOREPLY； INFO_REQUEST_and_INFO_REPLY； TIMESTAMP_and_TIMESTAMPREPLY； ADDRESS_and_ADDRESSREPLY； ROUTER_ADVERTISEMENT； ROUTER_SOLICITATION； DEST_UNREACH； SOURCE_QUENCH； REDIRECT； TIME_EXCEEDED； PARAMETERPROB。

other	除 TCP、 UDP 和 ICMP 之外的协议。
protocol_num	协议号或协议号范围，格式为 NUMBER<1-255>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除服务对象 test 的成员 DDP。

```
NetEye@root-system]unset object service test other 37
```

相关命令

命令名称	描述信息
object service	添加服务对象。

6 用户命令

管理用户

password

使用 **password** 命令修改管理员的口令。

命令

password {*user_name* | **simple** | **cipher** *passwd*}

语法

user_name	用户名，格式为 WORD<1-56>。
simple	表示设置的口令为明文，即管理员输入的口令未经过加密处理。
cipher	表示设置的口令为密文，即管理员输入的口令是经过加密算法处理过的。
passwd	口令，格式为 WORD<1-38>。

提示

含有关键字 **cipher** 的 **password** 命令主要用于 NetEye 在系统恢复时使用，不建议管理员使用该命令

说明

在 **password** *user_name* 命令中需要注意：

1. 根管理员可以修改根系统管理员的口令，并且修改口令时，不需要提供旧口令。
2. 根系统管理员可以修改根系统审计员和 Vsys 管理员的口令，并且修改口令时，不需要提供旧口令。
3. Vsys 管理员可以修改自己的 Vsys 审计员的口令，并且修改口令时，不需要提供旧口令。

在 **password** {**simple** | **cipher** *passwd*} 命令中，需要注意：

1. 该命令表示修改当前管理员的密码。
2. 使用含有关键字 **simple** 的命令时，系统会提示管理员输入旧密码。如果密码正确，系统会提示管理员输入新密码并确认新密码；反之，终止修改密码的操作。
3. 只有以根管理员登录时，才可以使用含有关键字 **cipher** 的命令。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在全局配置模式下使用。

范例

范例 1. 根管理员登录 NetEye 后，修改根系统管理员 test 的密码。

```
NetEye@root-system]password test
Password(6-128):
Repeat Password(6-128):
```

范例 2. 修改当前管理员的密码。

```
NetEye@root-system]password simple
Old password(6-128):
New password(6-128):
Repeat password(6-128):
```

show line

使用 **show line** 命令显示当前所有登录管理员的信息。

命令

show line

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示当前所有登录管理员的信息。

```
NetEye@root>show line
```

【返回结果】

```
User    UserType        From         LoginType
test    Administrator   10.3.1.122   Telnet
test    Administrator   10.3.1.211   Telnet
test    Administrator   10.3.1.128   Telnet
test    Administrator   10.3.1.121   Telnet
test    Administrator   10.3.1.129   Telnet
test    Administrator   10.3.1.156   Web
test    Administrator   10.3.1.211   Web
root    Root            10.3.1.155   Web
test    Administrator   10.3.1.156   Web
```

show user administrator

使用 **show user administrator** 命令显示 NetEye 管理员信息。

命令

show user administrator [*user_name*]

语法

user_name	用户名，格式为 WORD<1-56>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

说明

1. 如果当前登录管理员为根管理员，则可以查看根系统管理员信息。如果当前登录管理员为根系统管理员，则可以查看管理员本身、根系统审计员和 Vsys 管理员的信息。如果当前登录管理员为 Vsys 管理员，则可以查看该 Vsys 的 Vsys 审计员的信息。
2. 如果不指定 *user_name* 参数，则显示当前登录角色可查看的所有管理员信息。

模式

该命令在普通配置模式下使用。

范例

范例 . 根管理员登录 NetEye 后，查看所有的根系统管理员的信息。

```
NetEye@root>show user administrator
```

【返回结果】

```
   User name  Logintype           Authtype Vsys name  Privilege
    test       web,telnet,ssh,scm   Local    root       Administrator
```

相关命令

命令名称	描述信息
unset user administrator	删除指定的管理员。
user administrator	添加 NetEye 管理员。

unset user administrator

使用 **unset user administrator** 命令删除 NetEye 管理员。

命令

unset user administrator *user_name*

语法

user_name	用户名，格式为 WORD<1-56>。

说明

1. 根管理员可以删除根系统管理员。
2. 根系统管理员可以删除根系统审计员和 Vsys 管理员。
3. Vsys 管理员可以删除本 Vsys 的 Vsys 审计员。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show user administrator	显示 NetEye 管理员信息。
user administrator	添加 NetEye 管理员。

unset user administrator allowed-vsys

使用 **unset user administrator allowed-vsys** 命令将指定的 Vsys 管理员从特定的 Vsys 中删除。

命令

unset user administrator *user_name* **allowed-vsys** *vsys_name*

语法

user_name	用户名，格式为 WORD<1-56>。
vsys_name	虚拟系统名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令可以全局配置模式下使用。

相关命令

命令名称	描述信息
user allowed-vsys	将指定的 Vsys 管理员添加至特定的 Vsys。

unset user administrator auditor

使用 **unset user administrator auditor** 命令删除所有根系统审计员。

命令

unset user administrator auditor

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show user administrator	显示 NetEye 管理员信息。
user administrator	添加 NetEye 管理员。

unset user administrator logintype

使用 **unset user administrator logintype** 命令删除管理员的登录类型。

命令

unset user administrator *user_name* **logintype** *login_type*

语法

user_name	用户名，格式为 WORD<1-56>。
login_type	登录类型，格式为 WORD<3-18>。可以设置的登录类型为： Web； Telnet； SSH； SCM。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除管理员 test 的 web 以及 scm 登录方式。

```
NetEye@root-system]unset user administrator test logintype web,scm
```

相关命令

命令名称	描述信息
user administrator logintype	添加管理员的登录类型。

unset user administrator vsys-auditor

使用 **unset user administrator vsys-auditor** 命令删除当前 Vsys 的所有 Vsys 审计员。

命令

unset user administrator vsys-auditor

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
			V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show user administrator	显示 NetEye 管理员信息。
user administrator	添加 NetEye 管理员。

user administrator

使用 **user administrator** 命令添加 NetEye 管理员。

命令

user administrator *user_name* {**administrator** | **auditor** | **vsys-administrator vsys** *vsys_name_list* | **vsys-auditor**} **authtype** {**local** [**logintype** *login_type*] **password** {**simple** [**description** *string*] | **cipher** *passwd*} | **external** [**logintype** *login_type*] [**description** *string*]}

语法

user_name	用户名，格式为 WORD<1-56>。
administrator	添加根系统管理员。
auditor	添加根系统审计员。
vsys-administrator	添加 vsys 管理员。
vsys_name_list	虚拟系统名称列表，格式为 WORD<1-100>。
vsys_auditor	添加 vsys 审计员。
authtype	认证类型，包括 local 和 external。 • local— 表示添加本地认证的管理员 • external— 表示添加远程认证的管理员
login_type	登录类型，格式为 WORD<3-18>。可以设置的登录类型为： Web； Telnet； SSH； SCM。
simple	表示设置的口令为明文，即管理员输入的口令未经过加密处理。
string	备注信息，格式为 LINE。
cipher	表示设置的口令为密文，即管理员输入的口令是经过加密算法处理过的。
passwd	加密后的口令，格式为 WORD<1-38>。

提示

含有关键字 **cipher** 的 **user** 命令主要用于 NetEye 在系统恢复时使用，不建议管理员使用该命令。

说明

1. 根系统管理员只能由根管理员添加。
2. 根系统审计员只能由根系统管理员添加。

3. Vsys 管理员只能由根系统管理员添加。
4. Vsys 审计员只能由该 Vsys 的 Vsys 管理员添加。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V		V	

提示
根据添加管理员角色的不同，权限也有所不同，请详见说明。

模式

该命令在全局配置模式下使用。

范例

范例 . 根系统管理员登录到 NetEye 后，为根系统添加名称为 test 的根系统本地审计员。

```
NetEye@root-system]user administrator test auditor authtype local
password simple
Password(6-128):
Repeat Password(6-128):
```

相关命令

命令名称	描述信息
show user administrator	显示 NetEye 管理员信息。
unset user administrator	删除指定的管理员。

user administrator allowed-vsys

使用 **user administrator allowed-vsys** 命令将指定的 Vsys 管理员添加至特定的 Vsys。

命令

user administrator *user_name* **allowed-vsys** *vsys_name*

语法

user_name	用户名，格式为 WORD<1-56>。
vsys_name	虚拟系统名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令可以全局配置模式下使用。

相关命令

命令名称	描述信息
unset user administrator allowed-vsys	将指定的 Vsys 管理员从特定的 Vsys 中删除。

user administrator description

使用 **user administrator description** 命令设置管理员的描述信息。

命令

user administrator *user_name* **description** [*string*]

语法

user_name	用户名，格式为 WORD<1-56>。
string	描述信息字符串，格式为 LINE。

说明

如果不指定 *string* 参数，表示设置管理员的描述信息为空。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 为管理员 test 添加描述信息：This is administrator，然后修改描述信息为：This is an Administrator。

```
NetEye@root-system]user administrator test description This is
administrator
NetEye@root-system]user administrator test description This is an
Administrator
```

user administrator logintype

使用 **user administrator logintype** 命令添加管理员的登录类型。

命令

user administrator *user_name* **logintype** *login_type*

语法

user_name	用户名，格式为 WORD<1-56>。
login_type	登录类型，格式为 WORD<3-18>。可以设置的登录类型为： Web； Telnet； SSH； SCM。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 为管理员 test 添加 web 登录方式。

```
NetEye@root-system]user administrator test logintype web
```

相关命令

命令名称	描述信息
unset adminstrator logintype	删除管理员的登录类型。

网络用户

copy authuser file

使用 **copy authuser file** 命令导出网络用户文件。

命令

copy authuser file *file_name* **to** {**tftp** *ip_tftp* | **sftp** *ip_sftp* **username** *user_name* **password** *passwd* | **x**/**zmodem**}

语法

file_name	文件名称，格式为 WORD<1-63>。
tftp	简单文件传输协议，表示导出网络用户文件到 TFTP 服务器上。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
sftp	安全文件传输协议，表示导出网络用户文件到 SFTP 服务器上。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-64>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-64>。
x/zmodem	异步文件传输协议， Xmodem 或 Zmodem 由系统自动选择。表示使用 x/zmodem 协议导出网络用户文件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 导出网络用户文件 file1 到 SFTP 服务器 192.168.1.100，SFTP 服务器的用户名和密码均为 test。

```
NetEye@root-system]copy authuser file file1 to sftp 192.168.1.100
username test password test
```

相关命令

命令名称	描述信息
import authuser file	导入网络用户文件。

create authuser file

使用 **create authuser file** 命令创建网络用户文件。

命令

create authuser file *file_name*

语法

file_name	文件名称，格式为 WORD<1-63>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
delete authuser file	删除网络用户文件。
show user authuser file	查看网络用户文件列表。

delete authuser file

使用 **delete authuser file** 命令删除网络用户文件。

命令

delete authuser file [*file_name*]

语法

file_name	文件名称，格式为 WORD<1-63>。

说明

如果不指定 *file_name* 参数，则删除所有的网络用户文件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
create authuser file	创建网络用户文件。
show user authuser file	查看网络用户文件列表。

import authuser file

使用 **import authuser file** 命令导入网络用户文件。

命令

import authuser file from {**tftp** *ip_tftp file_name* | **sftp** *ip_sftp* **username** *user_name* **password** *passwd* **filename** *file_name* | **x**/**zmodem**}

语法

tftp	简单文件传输协议，表示从 TFTP 服务器导入指定的网络用户文件。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
file_name	文件名称，格式为 WORD<1-63>。
sftp	安全文件传输协议，表示从 SFTP 服务器导入指定的网络用户文件。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-64>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-64>。
x/zmodem	异步文件传输协议， Xmodem 或 Zmodem 由系统自动选择。表示使用 X/Zmodem 协议导入指定的网络用户文件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 从 TFTP 服务器 192.168.1.125 导入网络用户文件 test。

```
NetEye@root-system]import authuser file from tftp 192.168.1.125 test
```

show user authuser

使用 **show user authuser** 命令显示网络用户的相关信息。

命令

show user authuser [*user_name*]

语法

user_name	用户名称，格式为 WORD<1-63>。

说明

如果不指定 *user_name* 参数，则显示所有网络用户的相关信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有网络用户的相关信息。

```
NetEye@root>show user authuser
```

【返回结果】

```
Users     Authentication Type  Login Type  Timeout  Permission Table
State
  test      Local                -           300      default
enable
  mike      Local                WebAuth     300      test
enable
```

相关命令

命令名称	描述信息
unset user authuser	删除网络用户。
user authuser authtype	添加网络用户。

show user authuser default configuration

使用 **show user authuser default configuration** 命令显示外部网络用户的默认配置。

命令

show user authuser default configuration

说明

外部网络用户表示非 NetEye 上创建的、由 Radius 服务器进行认证的用户。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示网络用户的默认配置。

```
NetEye@root>show user authuser default configuration
```

【返回结果】

```
Default Configuration
        Authentication Type:  Remote
        Timeout:  300
        Permission Table:  default
        Login Type:  WebAuth, VPN
```

相关命令

命令名称	描述信息
unset user authuser default configuration	删除外部网络用户的默认角色。
user authuser default configuration auth	将外部网络用户的默认角色设置为 WebAuth。
user authuser default configuration multipoint	设置外部网络用户默认是否可以进行多点登录。

命令名称	描述信息
user authuser default configuration permission-table	设置外部网络用户的默认权限表。
user authuser default configuration timeout	设置外部网络用户的默认超时时间。
user authuser default configuration vpn	将外部网络用户的默认角色设置为 VPN。

show user authuser file

使用 **show user authuser file** 命令查看网络用户文件列表。

命令

show user authuser file

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看网络用户文件信息。

```
NetEye@root>show user authuser file
```

【返回结果】

```
test.u  test1.u test2.u
```

相关命令

命令名称	描述信息
create authuser file	创建网络用户文件。
delete authuser file	删除网络用户文件。

show webauth online

使用 **show webauth online** 命令显示在线的 WebAuth 用户信息。

命令

show webauth online

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示在线的 WebAuth 用户信息。

```
NetEye@root>show webauth online
```

【返回结果】

```
User name Ip Address  onlineTime   realTimeTraffic  traffic   idleTime
test      10.2.1.119  00:00:09     0                0         289
```

unset user authuser

使用 **unset user authuser** 命令删除网络用户。

命令

unset user authuser [*user_name*]

语法

user_name	用户名称，格式为 WORD<1-63>。

说明

如果不指定 *user_name* 参数，则删除所有的网络用户。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除网络用户 test。

```
NetEye@root-system]unset user authuser test
```

相关命令

命令名称	描述信息
show user authuser	显示网络用户的相关信息。
user authuser authtype	添加网络用户。

unset user authuser vpn, auth

使用 **unset user authuser vpn, auth** 命令删除指定网络用户的角色。

命令

unset user authuser *user_name* {**vpn** | **auth**}

语法

user_name	用户名称，格式为 WORD<1-63>。
vpn | **auth**	• vpn—VPN 用户 • auth—WebAuth 用户

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除网络用户 test 的 WebAuth 角色。

```
NetEye@root-system]unset user authuser test auth
```

相关命令

命令名称	描述信息
user authuser auth	为指定的网络用户添加 WebAuth 角色。
user authuser vpn ike-id fqdn, user-fqdn, asn1-dn, key-id	为指定的网络用户添加 VPN 角色，指定其 IKE ID 类型为 fqdn， user-fqdn， asn1-dn 或 key-id。
user authuser vpn ike-id ipv4-address	为指定的网络用户添加 VPN 角色，指定其 IKE ID 类型为 ipv4-address。

unset user authuser default configuration

使用 **unset user authuser default configuration** 命令删除外部网络用户的默认角色。

命令

unset user authuser default configuration {**vpn** | **auth**}

说明

外部网络用户表示非 NetEye 上创建的、由 Radius 服务器进行认证的用户。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除网络用户的默认 vpn 角色。

```
NetEye@root-system]unset user authuser default configuration vpn
```

相关命令

命令名称	描述信息
show user authuser default configuration	显示外部网络用户的默认配置。
user authuser default configuration auth	将外部网络用户的默认角色设置为 WebAuth。
user authuser default configuration multipoint	设置外部网络用户默认是否可以进行多点登录。
user authuser default configuration permission-table	设置外部网络用户的默认权限表。
user authuser default configuration timeout	设置外部网络用户的默认超时时间。
user authuser default configuration vpn	将外部网络用户的默认角色设置为 VPN。

user authuser auth

使用 **user authuser auth** 命令为指定的网络用户添加 WebAuth 角色。

命令

user authuser *user_name* **auth**

语法

user_name	用户名称，格式为 WORD<1-63>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 为网络用户 test 添加 WebAuth 角色。

```
NetEye@root-system]user authuser test auth
```

相关命令

命令名称	描述信息
unset user authuser vpn, auth	删除指定网络用户的角色。
user authuser vpn ike-id fqdn, user-fqdn, asn1-dn, key-id	为指定的网络用户添加 VPN 角色，指定其 IKE ID 类型为 fqdn， user-fqdn， asn1-dn 或 key-id。
user authuser vpn ike-id ipv4-address	为指定的网络用户添加 VPN 角色，指定其 IKE ID 类型为 ipv4-address。

user authuser authtype

使用 **user authuser authtype** 命令添加网络用户。

命令

user authuser *user_name* **authtype** {**local** [**password** *passwd*] | **external**} {**enable | disable**}

语法

user_name	用户名称，格式为 WORD<1-63>。
authtype	认证类型，包括 local 和 external。 • local— 表示添加本地认证的用户 • external— 表示添加外部认证的用户
passwd	口令，格式为 WORD<1-38>。
enable | **disable**	• enable— 启用添加的网络用户 • disable— 禁用添加的网络用户

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 添加本地认证网络用户 test，设置口令并启用该用户。

```
NetEye@root-system]user authuser test authtype local password abcdef enable
```

范例 2. 添加远程认证网络用户 test 并启用该用户。

```
NetEye@root-system]user authuser test authtype external enable
```

相关命令

命令名称	描述信息
show user authuser	显示网络用户的相关信息。
unset user authuser	删除网络用户。

user authuser default configuration auth

使用 **user authuser default configuration auth** 命令将外部网络用户的默认角色设置为 WebAuth。

命令

user authuser default configuration auth

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

说明

外部网络用户表示非 NetEye 上创建的、由 Radius 服务器进行认证的用户。

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show user authuser default configuration	显示外部网络用户的默认配置。
unset user authuser default configuration	删除外部网络用户的默认角色。
user authuser default configuration multipoint	设置外部网络用户默认是否可以进行多点登录。
user authuser default configuration permission-table	设置外部网络用户的默认权限表。
user authuser default configuration timeout	设置外部网络用户的默认超时时间。
user authuser default configuration vpn	将外部网络用户的默认角色设置为 VPN。

user authuser default configuration multipoint

使用 **user authuser default configuration multipoint** 命令设置外部网络用户默认是否可以进行多点登录。

命令

user authuser default configuration {**vpn | auth**} **multipoint** {**enable | disable**}

语法

vpn | auth	• vpn—VPN 用户 • auth—WebAuth 用户
enable | disable	• enable— 表示外部网络用户的默认属性为多点登录 • disable— 表示外部网络用户的默认属性为单点登录

说明

1. 外部网络用户表示非 NetEye 上创建的、由 Radius 服务器进行认证的用户。
2. 多个用户使用指定用户名称，在不同地点、不同终端，可以建立多条连接。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show user authuser default configuration	显示外部网络用户的默认配置。
unset user authuser default configuration	删除外部网络用户的默认角色。
user authuser default configuration auth	将外部网络用户的默认角色设置为 WebAuth。
user authuser default configuration permission-table	设置外部网络用户的默认权限表。

命令名称	描述信息
user authuser default configuration timeout	设置外部网络用户的默认超时时间。
user authuser default configuration vpn	将外部网络用户的默认角色设置为 VPN。

user authuser default configuration permission-table

使用 **user authuser default configuration permission-table** 命令设置外部网络用户的默认权限表。

命令

user authuser default configuration permission-table *table_name*

语法

table_name	权限表名称，格式为 WORD<1-16>。

说明

外部网络用户表示非 NetEye 上创建的、由 Radius 服务器进行认证的用户。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置外部网络用户的默认权限表为 table_test。

```
NetEye@root-system]user authuser default configuration permission-table
table_test
```

相关命令

命令名称	描述信息
show user authuser default configuration	显示外部网络用户的默认配置。
unset user authuser default configuration	删除外部网络用户的默认角色。
user authuser default configuration auth	将外部网络用户的默认角色设置为 WebAuth。
user authuser default configuration multipoint	设置外部网络用户默认是否可以进行多点登录。

命令名称	描述信息
user authuser default configuration timeout	设置外部网络用户的默认超时时间。
user authuser default configuration vpn	将外部网络用户的默认角色设置为 VPN。

user authuser default configuration timeout

使用 **user authuser default configuration timeout** 命令设置外部网络用户的默认超时时间。

命令

user authuser default configuration timeout *time*

语法

time	超时时间，单位为秒，“0”表示永不超时，默认值为 300 秒。格式为 INTEGER<0-3600>。

说明

外部网络用户表示非 NetEye 上创建的、由 Radius 服务器进行认证的用户。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置外部网络用户的默认超时时间为 500 秒。

```
NetEye@root-system]user authuser default configuration timeout 500
```

相关命令

命令名称	描述信息
show user authuser default configuration	显示外部网络用户的默认配置。
unset user authuser default configuration	删除外部网络用户的默认角色。
user authuser default configuration auth	将外部网络用户的默认角色设置为 WebAuth。
user authuser default configuration multipoint	设置外部网络用户默认是否可以进行多点登录。

命令名称	描述信息
user authuser default configuration permission-table	设置外部网络用户的默认权限表。
user authuser default configuration vpn	将外部网络用户的默认角色设置为 VPN。

user authuser default configuration vpn

使用 **user authuser default configuration vpn** 命令将外部网络用户的默认角色设置为 VPN。

命令

user authuser default configuration vpn [**assigned-ip** {**none** | *ip_address* | *ippool_name*} **dns1** {*dns1_ip_address* | **none**} **dns2** {*dns2_ip_address* | **none**} **wins1** {*wins1_ip_address* | **none**} **wins2** {*wins2_ip_address* | **none**}]

语法

none | *ip_address* | *ippool_name*	• none—NetEye 不为 VPN 用户分配私有 IP 地址，VPN 用户使用公网 IP 与 VPN 网关后的子网进行通讯 • ip_address—NetEye 为 VPN 用户分配固定的私有 IP 地址，格式为 x.x.x.x • ippool_name— 地址池名称，格式为 WORD<1-63>。表示 NetEye 为 VPN 用户分配的私有 IP 地址是从指定的 IP 地址池中动态获取
dns1_ip_address	主要 DNS 服务器 IP 地址，格式为 x.x.x.x。
dns2_ip_address	备用 DNS 服务器 IP 地址，格式为 x.x.x.x。
wins1_ip_address	主要 WINS 服务器 IP 地址，格式为 x.x.x.x。
wins2_ip_address	备用 WINS 服务器 IP 地址，格式为 x.x.x.x。

说明

外部网络用户表示非 NetEye 上创建的、由 Radius 服务器进行认证的用户。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置外部网络用户的默认 VPN 角色，用户 IP 地址为动态分配， DNS 服务器 IP 地址为 192.168.1.22， WINS 服务器 IP 地址为 192.168.1.156。

```
NetEye@root-system]user authuser default configuration vpn assigned-ip
none dns1 192.168.1.22 dns2 none wins1 192.168.1.156 wins2 none
```

相关命令

命令名称	描述信息
show user authuser default configuration	显示外部网络用户的默认配置。
unset user authuser default configuration	删除外部网络用户的默认角色。
user authuser default configuration auth	将外部网络用户的默认角色设置为WebAuth。
user authuser default configuration multipoint	设置外部网络用户默认是否可以进行多点登录。
user authuser default configuration permission-table	设置外部网络用户的默认权限表。
user authuser default configuration timeout	设置外部网络用户的默认超时时间。

user authuser enable, disable

使用 **user authuser enable, disable** 命令启用或禁用指定的网络用户。

命令

user authuser *user_name* {**enable | disable**}

语法

user_name	用户名称，格式为 WORD<1-63>。
**enable	disable**	• enable— 启用指定的网络用户 • disable— 禁用指定的网络用户

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 禁用网络用户 test。

```
NetEye@root-system]user authuser test disable
```

相关命令

命令名称	描述信息
show user authuser	显示网络用户的相关信息。

user authuser multipoint

使用 **user authuser multipoint** 命令设置指定的网络用户是否可以进行多点登录。

命令

user authuser *user_name* {**vpn | auth**} **multipoint** {**enable | disable**}

语法

user_name	用户名称，格式为 WORD<1-63>。
vpn | auth	• vpn—VPN 用户 • auth—WebAuth 用户
enable | disable	• enable— 表示指定的网络用户可以多点登录 • disable— 表示指定的网络用户不可以进行多点登录

说明

多个用户使用指定用户名称，在不同地点、不同终端，可以建立多条连接。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

user authuser password

使用 **user authuser password** 命令修改指定网络用户的口令。

命令

user authuser *user_name* **password**

语法

user_name	用户名称，格式为 WORD<1-63>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 修改网络用户 test 的口令。

```
NetEye@root-system]user authuser test password
Password(1-128):
Repeat Password(1-128):
```

user authuser permission-table

使用 **user authuser permission-table** 命令修改指定网络用户的权限表。

命令

user authuser *user_name* **permission-table** *table_name*

语法

user_name	用户名称，格式为 WORD<1-63>。
table_name	权限表名称，格式为 WORD<1-16>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 修改网络用户 test 的权限表为 table_test。

```
NetEye@root-system]user authuser test permission-table table_test
```

user authuser timeout

使用 **user authuser timeout** 命令修改指定网络用户的超时时间。

命令

user authuser *user_name* **timeout** *time*

语法

user_name	用户名称，格式为 WORD<1-63>。
time	超时时间，单位为秒，“0”表示永不超时，默认值为 300 秒。格式为 INTEGER<0-3600>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 修改网络用户 test 的超时时间为 1000 秒。

```
NetEye@root-system]user authuser test timeout 1000
```

user authuser vpn ike-id fqdn, user-fqdn, asn1-dn, key-id

使用 **user authuser vpn ike-id fqdn, user-fqdn, asn1-dn, key-id** 命令为指定的网络用户添加 VPN 角色，指定其 IKE ID 类型为 fqdn， user-fqdn， asn1-dn 或 key-id。

命令

user authuser *user_name* **vpn ike-id** {**fqdn** | **user-fqdn** | **asn1-dn** | **key-id**} *ike* [**type** {**xauth** | **l2tp**} **assigned-ip** {**none** | *ip_address* | *ippool_name*} [**dns1** *dns1_ip_address* [**dns2** *dns2_ip_address*]] [**wins1** *wins1_ip_address* [**wins2** *wins2_ip_address*]]]

语法

user_name	用户名称，格式为 WORD<1-63>。
fqdn | **user-fqdn** | **asn1-dn** | **key-id**	• fqdn— 表示将 *ike* 参数设置为域名 • user-fqdn— 表示将 *ike* 参数设置为电子邮件地址 • asn1-dn— 表示将 *ike* 参数设置为固定的格式。例如 C=CN，ST=Guangdong， L=Guangzhou， O=abcd， OU=Security，CN=test， emailAddress=test@abcd.com。其中 C 代表国家，ST 代表省份， L 代表城市，O 代表公司， OU 代表部门， CN 代表用户名， emailAddress 代表用户的邮件地址 • key-id— 表示将 *ike* 参数设置为字符串
ike	VPN 用户的 IKE ID，格式为 WORD<1-1023>。
xauth | **l2tp**	• xauth— 可扩展认证 • l2tp— 第二层隧道协议
none | *ip_address* | *ippool_name*	• none—NetEye 不为 VPN 用户分配私有 IP 地址，VPN 用户使用公网 IP 与 VPN 网关后的子网进行通讯 • ip_address—NetEye 为 VPN 用户分配固定的私有 IP 地址，格式为 x.x.x.x • ippool_name— 地址池名称，格式为 WORD<1-63>。表示 NetEye 为 VPN 用户分配的私有 IP 地址是从指定的 IP 地址池中动态获取
dns1_ip_address	主要 DNS 服务器 IP 地址，格式为 x.x.x.x。
dns2_ip_address	备用 DNS 服务器 IP 地址，格式为 x.x.x.x。
wins1_ip_address	主要 WINS 服务器 IP 地址，格式为 x.x.x.x。
wins2_ip_address	备用 WINS 服务器 IP 地址，格式为 x.x.x.x。

说明

DNS 服务器 IP 地址和 WINS 服务器 IP 地址最多可分别指定两个。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 为网络用户 test 添加 VPN 角色，指定其 IKE ID 类型为 user-fqdn，认证类型为 xauth， DNS 服务器 IP 地址为 192.168.1.120， WINS 服务器 IP 地址为 192.168.1.160。

```
NetEye@root-system]user authuser test vpn ike-id user-fqdn
test@abcd.com type xauth assigned-ip none dns1 192.168.1.120 wins1
192.168.1.160
```

相关命令

命令名称	描述信息
unset user authuser vpn, auth	删除指定网络用户的角色。
user authuser auth	为指定的网络用户添加 WebAuth 角色。
user authuser vpn ike-id ipv4-address	为指定的网络用户添加 VPN 角色。

user authuser vpn ike-id ipv4-address

使用 **user authuser vpn ike-id ipv4-address** 命令为指定的网络用户添加 VPN 角色，指定其 IKE ID 类型为 ipv4-address。

命令

user authuser *user_name* **vpn ike-id ipv4-address** *ipv4* [**type** {**xauth** | **l2tp**} **assigned-ip** {**none** | *ip_address* | *ippool_name*} [**dns1** *dns1_ip_address* [**dns2** *dns2_ip_address*]] [**wins1** *wins1_ip_address* [**wins2** *wins2_ip_address*]]]

语法

user_name	用户名称，格式为 WORD<1-63>。
ipv4	VPN 用户的 IKE ID，格式为 x.x.x.x。
xauth | **l2tp**	• xauth— 可扩展认证 • l2tp— 第二层隧道协议
none | *ip_address* | *ippool_name*	• none—NetEye 不为 VPN 用户分配私有 IP 地址，VPN 用户使用公网 IP 与 VPN 网关后的子网进行通讯 • ip_address—NetEye 为 VPN 用户分配固定的私有 IP 地址，格式为 x.x.x.x • ippool_name— 地址池名称，格式为 WORD<1-63>。表示 NetEye 为 VPN 用户分配的私有 IP 地址是从指定的 IP 地址池中动态获取
dns1_ip_address	主要 DNS 服务器 IP 地址，格式为 x.x.x.x。
dns2_ip_address	备用 DNS 服务器 IP 地址，格式为 x.x.x.x。
wins1_ip_address	主要 WINS 服务器 IP 地址，格式为 zx.x.x.x。
wins2_ip_address	备用 WINS 服务器 IP 地址，格式为 x.x.x.x。

说明

DNS 服务器 IP 地址和 WINS 服务器 IP 地址最多可分别指定两个。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 为网络用户 test 添加 VPN 角色，指定其 IKE ID 类型为 ipv4-address，认证类型为 xauth， DNS 服务器 IP 地址为 192.168.1.128， WINS 服务器 IP 地址为 192.168.1.165。

```
NetEye@root-system]user authuser test vpn ike-id ipv4-address
192.168.1.25 type xauth assigned-ip none dns1 192.168.1.128 wins1
192.168.1.165
```

相关命令

命令名称	描述信息
unset user authuser vpn, auth	删除指定网络用户的角色。
user authuser auth	为指定的网络用户添加 WebAuth 角色。
user authuser vpn ike-id fqdn, user-fqdn,asn1-dn,key-id	为指定的网络用户添加 VPN 角色。

webauth user offline

使用 **webauth user offline** 命令强制在线的 WebAuth 用户下线。

命令

webauth user offline [**ip** *ip_address*]

语法

ip_address	IP 地址，格式为 x.x.x.x。

说明

如果不指定 **ip** *ip_address* 参数，则强制所有在线的 WebAuth 用户下线。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 强制所有在线的 WebAuth 用户下线。

```
NetEye@root-system]webauth user offline
```

权限表

permission tables

使用 **permission tables** 命令添加用户权限表或进入指定的用户权限表配置模式。

命令

permission tables *table_name*

语法

table_name	用户权限表名称，格式为 WORD<1-15>。

说明

如果指定 *table_name* 的用户权限表不存在，则创建一个以 *table_name* 命名的用户权限表，并进入该用户权限表配置模式。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 进入指定的用户权限表配置模式 test。

```
NetEye@root-system]permission tables test
```

相关命令

命令名称	描述信息
show permission association	显示用户权限表的相关信息。
unset permission tables	删除用户权限表。

policy

使用 **policy** 命令添加用户权限表策略。配置成功后，可以通过权限表为用户分配不同的网络权限策略。

命令

policy *policy_name* {*szone* | **any**} {*src_iplist* | **any** | **object** *ipaddr_object_name* | **group** *ipaddr_group_name*} {*dzone* | **any**} {*dst_ iplist* | **any** | **object** *ipaddr_object_name* | **group** *ipaddr_group_name*} {**any** | **icmp** {*icmp_type* | *icmp_list* | **any**} | {**tcp** | **udp**} {*src_port* | *srcport_range*} {*dst_port* | *dstport_ range*} | **other** *protocol_num* | **protocol-object** *protocol_object_name* | **protocol-group** *protocol_group_name*} {**permit** | **deny**} {**enable** | **disable**} [*pri*]

语法

policy_name	用户权限表策略名称，格式为 WORD<1-15>。
szone	源安全域名称，格式为 WORD<1-15>。 **any** 表示任意安全域。
src_iplist	源 IP 地址列表，格式为 IPV4LIST<1-32>。 **any** 表示任意 IP 地址。
ipaddr_object_name	IP 地址对象名称，格式为 WORD<1-63>。
ipaddr_group_name	IP 地址对象组名称，格式为 WORD<1-63>。
dzone	目的安全域名称，格式为 WORD<1-15>。 **any** 表示任意安全域。
dst_iplist	目的 IP 地址列表，格式为 IPV4LIST<1-32>。 **any** 代表任意 IP 地址。
icmp_type	ICMP 协议类型，可以设置为： ECHO_and_ECHOREPLY； DEST_UNREACH； SOURCE_QUENCH； REDIRECT； ROUTER_ADVERTISEMENT； ROUTER_SOLICITATION； TIME_EXCEEDED； PARAMETERPROB； TIMESTAMP_and_TIMESTAMPREPLY； INFO_REQUEST_and_INFO_REPLY； ADDRESS_and_ADDRESSREPLY 。 **any** 表示上述协议类型中的任意一种。

icmp_list	ICMP 的协议类型列表，格式为 WORD<1-256>。列表可以为下述协议类型的任意组合： ECHO_and_ECHOREPLY； INFO_REQUEST_and_INFO_REPLY； TIMESTAMP_and_TIMESTAMPREPLY； ADDRESS_and_ADDRESSREPLY； ROUTER_ADVERTISEMENT； ROUTER_SOLICITATION； DEST_UNREACH； SOURCE_QUENCH； REDIRECT； TIME_EXCEEDED； PARAMETERPROB。
src_port	源端口，格式为 INTEGER<1-65535>。
srcport_range	源端口范围，格式为 LIMIT。
dst_port	目的端口，格式为 INTEGER<1-65535>。
dstport_range	目的端口范围，格式为 LIMIT。
other	除 TCP、 UDP 和 ICMP 之外的协议。
protocol_num	协议号或协议号范围，格式为 NUMBER<1-255>。
protocol_object_name	协议对象名称，格式为 WORD<1-63>。
protocol_group_name	协议对象组名称，格式为 WORD<1-63>。
permit | **deny**	• permit— 允许匹配该用户权限表策略的数据包通过 NetEye • deny— 拒绝匹配该用户权限表策略的数据包通过 NetEye
enable | **disable**	• enable— 启用该用户权限表策略 • disable— 禁用该用户权限表策略
pri	用户权限表策略的优先级，格式为 INTEGER<1-80000>。

说明

1. 如果*pri*设置为1，表示将该用户权限表策略添加到所有策略的前面；如果*pri*省略，表示将该用户权限表策略添加到所有策略的后面。
2. 当在一条策略中指定多个 ICMP 类型时，可用逗号隔开，并且不能重复。
3. 如果选择 **other** 关键字，则指定的协议号和协议号范围不包括 TCP、UDP 和 ICMP，不允许单独设置 1、 6 和 17。例如指定协议号范围是 3-10，实际的协议号范围为 3-5，7-10。
4. 当在一条策略中指定多个其它协议时，协议号范围不能重叠。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在用户权限表配置模式下使用。

范例

范例 1. 为用户权限表 table test 添加用户权限表策略 test1，其优先级为 12，不指定任何传输层协议，状态为启用。配置成功后，允许源安全域为 zone1、目的安全域为 zone2 的 IP 数据包通过 NetEye。

```
NetEye@root-system]permission tables test
NetEye@root-system-permissiontable-test]policy test1 zone1 any zone2 any any permit enable 12
```

范例 2. 为用户权限表 table test 添加用户权限表策略 test2，其优先级为空，传输层协议为 ICMP， ICMP 协议类型为 ADDRESS_and_ADDRESSREPLY、TIMESTAMP_and_TIMESTAMPREPLY，状态为禁用。配置成功后，拒绝源安全域为 zone1、目的安全域为 zone2、目的 IP 地址范围在 192.168.1.100-192.168.1.122 的 IP 数据包通过 NetEye。

```
NetEye@root-system]permission tables test
NetEye@root-system-permissiontable-test]policy test2 zone1 any zone2 192.168.1.100-192.168.1.122 icmp ADDRESS_and_ADDRESSREPLY, TIMESTAMP_and_TIMESTAMPREPLY deny disable
```

相关命令

命令名称	描述信息
policy enable, disable	启用或禁用指定的用户权限表策略。
show permission	显示指定用户权限表中用户权限表策略的相关信息。
unset policy	删除用户权限表策略。

policy enable, disable

使用 **policy enable, disable** 命令启用或禁用指定的用户权限表策略。

命令

policy *policy_name* {**enable** | **disable**}

语法

policy_name	用户权限表策略名称，格式为 WORD<1-15>。
enable | **disable**	• enable— 启用指定的用户权限表策略 • disable— 禁用指定的用户权限表策略

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在用户权限表配置模式下使用。

相关命令

命令名称	描述信息
policy	添加用户权限表策略。
show permission	显示指定用户权限表中用户权限表策略的相关信息。
unset policy	删除用户权限表策略。

policy number

使用 **policy number** 命令修改指定用户权限表策略的优先级。

命令

policy *policy_name* **number** *pri*

语法

policy_name	用户权限表策略名称，格式为 WORD<1-15>。
pri	用户权限表策略优先级，格式为 INTEGER<1-80000>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在用户权限表配置模式下使用。

范例

范例 . 在指定的用户权限表配置模式 table test 中，设置用户权限表策略 test 的优先级为 5。

```
NetEye@root-system]permission tables test
NetEye@root-system-permissiontable-test]policy test number 5
```

相关命令

命令名称	描述信息
policy	添加用户权限表策略。
show permission	显示指定用户权限表中用户权限表策略的相关信息。
unset policy	删除用户权限表策略。

policy permit, deny

使用 **policy permit, deny** 命令修改指定用户权限表策略的访问控制方式。

命令

policy *policy_name* {**permit** | **deny**}

语法

policy_name	用户权限表策略名称，格式为 WORD<1-15>。
permit	**deny**	• permit— 允许匹配该用户权限表策略的数据包通过 NetEye • deny— 拒绝匹配该用户权限表策略的数据包通过 NetEye

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在用户权限表配置模式下使用。

范例

范例 . 在指定的用户权限表配置模式 table test 中，允许符合用户权限表策略 test 的数据包通过 NetEye。

```
NetEye@root-system]permission tables test
NetEye@root-system-permissiontable-test]policy test permit
```

相关命令

命令名称	描述信息
policy	添加用户权限表策略。
show permission	显示指定用户权限表中用户权限表策略的相关信息。
unset policy	删除用户权限表策略。

policy protocol

使用 **policy protocol** 命令为指定的用户权限表策略添加自定义服务。

命令

policy *policy_name* **protocol** {**icmp** {*icmp_type* | *icmp_list* | **any**} | **other** *protocol_num* | {**tcp** | **udp**} {*src_port* | *srcport_range*} {*dst_port* | *dstport_ range*} | **protocol-object** *object_name* | **protocol-group** *group_name*}

语法

policy_name	用户权限表策略名称，格式为 WORD<1-15>。
icmp_type	ICMP 协议类型，可以设置为： ECHO_and_ECHOREPLY； DEST_UNREACH； SOURCE_QUENCH； REDIRECT； ROUTER_ADVERTISEMENT； ROUTER_SOLICITATION； TIME_EXCEEDED； PARAMETERPROB； TIMESTAMP_and_TIMESTAMPREPLY； INFO_REQUEST_and_INFO_REPLY； ADDRESS_and_ADDRESSREPLY 。 **any** 表示上述协议类型中的任意一种。
icmp_list	ICMP 的协议类型列表，格式为 WORD<1-256>。列表可以为下述协议类型的任意组合： ECHO_and_ECHOREPLY； INFO_REQUEST_and_INFO_REPLY； TIMESTAMP_and_TIMESTAMPREPLY； ADDRESS_and_ADDRESSREPLY； ROUTER_ADVERTISEMENT； ROUTER_SOLICITATION； DEST_UNREACH； SOURCE_QUENCH； REDIRECT； TIME_EXCEEDED； PARAMETERPROB。
other	除 TCP、 UDP 和 ICMP 之外的协议。
protocol_num	协议号或协议号范围，格式为 NUMBER<1-255>。
src_port	源端口，格式为 INTEGER<1-65535>。
srcport_range	源端口范围，格式为 LIMIT。

dst_port	目的端口，格式为 INTEGER<1-65535>。
dstport_range	目的端口范围，格式为 LIMIT。
object_name	协议对象名称，格式为 WORD<1-63>。
group_name	协议对象组名称，格式为 WORD<1-63>。

说明

如果选择 **other** 关键字，则指定的协议号和协议号范围不包括 TCP、 UDP 和 ICMP，不允许单独设置 1、 6 和 17。例如指定协议号范围是 3-10，实际的协议号范围为 3-5，7-10。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在用户权限表配置模式下使用。

范例

范例 1. 在指定的用户权限表配置模式 table test 中，为用户权限表策略 test 添加 ICMP 协议，不指定 ICMP 协议类型。

```
NetEye@root-system]permission tables test
NetEye@root-system-permissiontable-test]policy test protocol icmp any
```

范例 2. 在指定的用户权限表配置模式 table test 中，为用户权限表策略 test1 添加 TCP 协议，源端口号为 5，目的端口号为 63。

```
NetEye@root-system]permission tables test
NetEye@root-system-permissiontable-test]policy test1 protocol tcp 5 63
```

相关命令

命令名称	描述信息
policy	添加用户权限表策略。
show permission	显示指定用户权限表中用户权限表策略的相关信息。
unset policy	删除用户权限表策略。

policy sourceip, desip

使用 **policy sourceip, desip** 命令为指定的用户权限表策略添加源 IP 或目的 IP 地址。

命令

policy *policy_name* {**sourceip** | **desip**} {**object** *ipaddr_object_name* | **group** *ipaddr_group_name* | **address** *ip_list* | *ip_address* **netmask** *ip_mask*}

语法

policy_name	用户权限表策略名称，格式为 WORD<1-15>。
sourceip | **desip**	• sourceip— 表示添加源 IP 地址 • desip— 表示添加目的 IP 地址
ipaddr_object_name	IP 地址对象名称，格式为 WORD<1-63>。
ipaddr_group_name	IP 地址对象组名称，格式为 WORD<1-63>。
ip_list	源 / 目的 IP 地址列表，格式为 IPV4LIST<1-32>。
ip_address	源 / 目的 IP 地址，格式为 x.x.x.x。
ip_mask	源 / 目的 IP 地址的子网掩码，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在用户权限表配置模式下使用。

范例

范例 1. 在指定的用户权限表配置模式 table test 中，为用户权限表策略 test1 添加源 IP 地址，引用 IP 地址对象 OBJ。

```
NetEye@root-system]permission tables test
NetEye@root-system-permissiontable-test]policy test1 sourceip object OBJ
```

范例 2. 在指定的用户权限表配置模式 table test 中，为用户权限表策略 test2 添加源 IP 地址 192.168.1.112 及其子网掩码 255.255.255.0。

```
NetEye@root-system]permission tables test
```

```
NetEye@root-system-permissiontable-test]policy test2 sourceip
192.168.1.112 netmask 255.255.255.0
```

相关命令

命令名称	描述信息
show permission	显示指定用户权限表中用户权限表策略的相关信息。

show permission

使用 **show permission** 命令显示指定用户权限表中用户权限表策略的相关信息。

命令

show permission *table_name* [**policy** *policy_name*]

语法

table_name	用户权限表名称，格式为 WORD<1-15>。
policy_name	用户权限表策略名称，格式为 WORD<1-15>。

说明

如果不指定 **policy** *policy_name* 参数，则显示指定用户权限表中所有用户权限表策略的相关信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示用户权限表 table test 中，用户权限表策略 test 的相关信息。

```
NetEye@root>show permission table test policy test
```

【返回结果】

```
Name: test
  State: enable
  Action: permit

  From: Any
  To: Any
  Source IP Address:
    Any
  Destination IP Address:
```

```
    Any
  Services:
    Protocol  Port/Type
    ICMP           Any
```

相关命令

命令名称	描述信息
policy	添加用户权限表策略。
policy enable, disable	启用或禁用指定的用户权限表策略。
unset policy	删除用户权限表策略。

show permission association

使用 **show permission association** 命令显示用户权限表的相关信息。

命令

show permission association [*table_name*]

语法

table_name	用户权限表名称，格式为 WORD<1-15>。

说明

如果不指定 *table_name* 参数，则显示所有用户权限表的相关信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有用户权限表的相关信息。

```
NetEye@root>show permission association
```

【返回结果】

```
Permission Table Name:
               default
UserName:
               user-default
               test
Permission Table Name:
               table test
UserName:
Permission Table Name:
               test
UserName:
```

```
                mike
Permission Table Name:
                test1
UserName:
```

相关命令

命令名称	描述信息
permission tables	添加用户权限表或进入指定的用户权限表配置模式。
unset permission tables	删除用户权限表。

unset permission tables

使用 unset **permission tables** 命令删除用户权限表。

命令

unset permission tables [*table_name*]

语法

table_name	用户权限表名称，格式为 WORD<1-15>。

说明

如果不指定 *table_name* 参数，则删除所有的用户权限表。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除所有的用户权限表。

```
NetEye@root-system]unset permission tables
```

相关命令

命令名称	描述信息
permission tables	添加用户权限表或进入指定的用户权限表配置模式。
show permission association	显示用户权限表的相关信息。

unset policy

使用 unset policy 命令删除用户权限表策略。

命令

unset policy [*policy_name*]

语法

policy_name	用户权限表策略名称，格式为 WORD<1-15>。

说明

如果指定 *policy_name* 参数，则表示删除指定的用户权限表策略。否则表示删除用户权限表中的所有策略。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在用户权限表配置模式下使用。

范例

范例 . 在指定的用户权限表配置模式 table test 中，删除所有的用户权限表策略。

```
NetEye@root-system]permission tables test
NetEye@root-system-permissiontable-test]unset policy
```

相关命令

命令名称	描述信息
policy	添加用户权限表策略。
policy enable, disable	启用或禁用指定的用户权限表策略。
show permission	显示指定用户权限表中用户权限表策略的相关信息。

7 认证和计费命令

认证配置

server account

使用 **server account** 命令设置计费服务器。

命令

server account *server_name*

语法

server_name	计费服务器名称，格式为 WORD<1-32>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show server account	显示计费服务器信息。
unset server account	删除计费服务器。

server authentication

使用 **server authentication** 命令设置认证服务器。

命令

server authentication type {**administrator** | **scm** | **authuser**} *server_name*

语法

server_name	认证服务器名称，格式为 WORD<1-32>。
administrator | **scm** | **authuser**	• administrator— 表示设置管理员的认证服务器 • scm— 表示设置 SCM 管理员的认证服务器 • authuser— 表示设置网络用户的认证服务器

说明

1. 如果输入的 *server_name* 参数为 local，则表示进行本地认证。
2. 仅有 Administrator 可以设置 SCM 管理员的认证服务器。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
server authentication local	设置管理员的本地认证服务器。
show server authentication	显示认证服务器信息。

server authentication local

使用 **server authentication local** 命令设置管理员的本地认证服务器。

命令

server authentication type administrator local

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V				

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
server authentication	设置认证服务器。
show server authentication	显示认证服务器信息。

show server account

使用 **show server account** 命令显示计费服务器信息。

命令

show server account

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示计费服务器信息。

```
NetEye@root>show server account
```

【返回结果】

```
Accounting Server for User: test
```

相关命令

命令名称	描述信息
server account	设置计费服务器。
unset server account	删除计费服务器。

show server authentication

使用 **show server authentication** 命令显示认证服务器信息。

命令

show server authentication

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示认证服务器信息。

```
NetEye@root>show server authentication
```

【返回结果】

```
Authentication Server for Administrator: Local
Authentication Server for User: Local
Authentication Server for SCM User: Local
```

相关命令

命令名称	描述信息
server authentication	设置认证服务器。

unset server account

使用 **unset server account** 命令删除计费服务器。

命令

unset server account

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
server account	设置计费服务器。
show server account	显示计费服务器信息。

WebAuth 配置

show webauth access-port

使用 **show webauth access-port** 命令查看 WebAuth 认证的访问端口。

命令

show webauth access-port

说明

WebAuth 认证的缺省访问端口为 80。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看 WebAuth 认证的访问端口。

```
NetEye@root>show webauth access-port
```

【返回结果】

```
webauth access port:
   80
```

相关命令

命令名称	描述信息
unset webauth access-port	删除 WebAuth 认证的访问端口。
webauth access-port	添加 WebAuth 认证的访问端口。

show webauth banner

使用 **show webauth banner** 命令查看 WebAuth 用户登录成功或失败后的回显信息。

命令

show webauth banner

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看 WebAuth 用户登录成功或失败后的回显信息。

```
NetEye@root>show webauth banner
```

【返回结果】

```
Success: Congratulations, you have successfully logged in!
Fail: Sorry, your login failed.
```

相关命令

命令名称	描述信息
webauth banner success, fail	设置 WebAuth 用户登录成功或失败后的回显信息。

show webauth auth-port

使用 **show webauth auth-port** 命令查看 WebAuth 认证的通信端口。

命令

show webauth auth-port

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看 WebAuth 认证的通信端口。

```
NetEye@root> show webauth auth-port
```

【返回结果】

```
Webauth port: 4325
```

相关命令

命令名称	描述信息
webauth auth-port	修改 WebAuth 认证的通信端口。

unset webauth access-port

使用 **unset webauth access-port** 命令删除 WebAuth 认证的访问端口。

命令

unset webauth access-port [*access_port_num*]

语法

access_port_num	WebAuth 认证的访问端口号，格式为 INTEGER<1-65535>。

说明

如果不指定 *access_port_num* 参数，则表示删除所有 WebAuth 认证的访问端口。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除所有 WebAuth 认证的访问端口。

```
NetEye@root-system]unset webauth access-port
```

相关命令

命令名称	描述信息
show webauth access-port	查看 WebAuth 认证的访问端口。
webauth access-port	添加 WebAuth 认证的访问端口。

webauth access-port

使用 **webauth access-port** 命令添加 WebAuth 认证的访问端口。

命令

webauth access-port *access_port_num*

语法

access_port_num	WebAuth 认证的访问端口号，格式为 INTEGER<1-65535>。

说明

1. 每个 Vsys 最多存在 8 个 WebAuth 认证的访问端口。
2. 如果用户未添加其他 WebAuth 认证的访问端口，则默认对 80 端口的 HTTP 请求进行 WebAuth 认证。此时，用户仅需在浏览器的地址栏中输入指定的 URL 即可，如 http://www.neusoft.com。
3. 如果用户已添加其他 WebAuth 认证的访问端口，则可以对已添加端口的 HTTP 请求进行 WebAuth 认证。此时，用户可以在浏览器的地址栏中输入指定的 URL: 已添加的访问端口号即可，如 http://www.neusoft.com:8080。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加 WebAuth 认证的访问端口 8080。

```
NetEye@root-system]webauth access-port 8080
```

相关命令

命令名称	描述信息
show webauth access-port	查看 WebAuth 认证的访问端口。
unset webauth access-port	删除 WebAuth 认证的访问端口。

webauth auth-port

使用 **webauth auth-port** 命令修改 WebAuth 认证的通信端口。

命令

webauth auth-port *port_num*

语法

port_num	WebAuth 认证的通信端口号，格式为 INTEGER<1-65535>。

说明

WebAuth 认证的通信端口缺省为 4325。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 修改 WebAuth 认证的通信端口为 666。

```
NetEye@root-system]webauth auth-port 666
```

相关命令

命令名称	描述信息
show webauth auth-port	查看 WebAuth 认证的通信端口。

webauth banner success, fail

使用 **webauth banner success, fail** 命令设置 WebAuth 用户登录成功或失败后的回显信息。

命令

webauth banner {**success | fail**} *string*

语法

string	NetEye 系统回显给 WebAuth 用户的信息，格式为 LINE。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置 WebAuth 用户登录成功后的回显信息为 hello。

```
NetEye@root-system]webauth banner success hello
```

相关命令

命令名称	描述信息
show webauth banner	查看 WebAuth 用户登录成功或失败后的回显信息。

RADIUS 服务器

radius server

使用 **radius server** 命令添加一个 RADIUS 服务器。

命令

radius server *server_name* **ip** *ip_address* [**secondaryIP** *secondaryip_address*] **port** *port_number* [**key** *key*]

语法

server_name	RADIUS 服务器名称，格式为 WORD<1-32>。
ip_address	服务器 IP 地址，格式为 x.x.x.x。
secondaryIP	服务器的备用 IP 地址，当主 IP 地址无应答时，启用备用 IP 地址。
secondaryip_address	服务器的备用 IP 地址，格式为 x.x.x.x。
port_number	服务器端口号，格式为 INTEGER<1-65535>。
key	RADIUS 服务器与 NetEye 协商的共享密钥，格式为 WORD<6-64>。

说明

如果选择 **secondaryIP**，则表示为 RADIUS 服务器添加备用 IP 地址；如果选择 **key**，则表示为 RADIUS 服务器添加密钥信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例：添加 RADIUS 服务器 test1， IP 地址为 2.0.0.1，备用 IP 地址为 2.0.0.2，端口为 81。

```
NetEye@root-system]radius server test1 ip 2.0.0.1 secondaryIP 2.0.0.2
port 81
```

相关命令

命令名称	描述信息
show radius server	显示所有的 RADIUS 服务器信息。
unset radius server	删除 RADIUS 服务器。

show radius server

使用 **show radius server** 命令显示所有的 RADIUS 服务器信息。

命令

show radius server

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有的 RADIUS 服务器信息。

```
NetEye@root>show radius server
```

【返回结果】

```
 Radius server list:

    Name        IP              StandIPAdd       Port        State
    test        10.2.1.110      10.2.1.119       22
```

相关命令

命令名称	描述信息
radius server	添加 RADIUS 服务器。
unset radius server	删除 RADIUS 服务器。

unset radius server

使用 **unset radius server** 命令删除 RADIUS 服务器。

命令

unset radius server [*server_name*]

语法

server_name	RADIUS 服务器名称，格式为 WORD<1-32>。

说明

如果不指定 *server_name* 参数，表示删除所有的 RADIUS 服务器。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
radius server	添加 RADIUS 服务器。
show radius server	显示所有的 RADIUS 服务器信息。

8 路由命令

静态路由

matching

使用 **matching** 命令为策略路由添加策略条件。配置成功后，如果数据包满足该策略路由所有的策略条件，则进入此策略路由的路由表查找相匹配的路由。

命令

matching {**sip** {*start_ipaddress* [*end_ipaddress*] | *ipaddr_object_name* | *ipaddr_group_name* | *ip_addr* **mask** *mask_length*} | **protocol** {**icmp** {*icmp_type* | **any**} | {**tcp** | **udp**} *start_port* [*end_port*] | **other** *start_typenum* [*end_typenum*] | *protocol_object_name* | *protocol_group_name*} | **tos** *tos_type* | **input-interface** *interface_name*}

语法

start_ipaddress	源 IP 地址的起始地址，格式为 x.x.x.x。
end_ipaddress	源 IP 地址的终止地址，格式为 x.x.x.x。
ipaddr_object_name	IP 地址对象名称，格式为 WORD<1-15>。
ipaddr_group_name	IP 地址对象组名称，格式为 WORD<1-15>。
ip_addr	源 IP 地址，格式为 x.x.x.x。
mask_length	掩码长度，格式为 INTEGER<1-32>。

icmp_type	ICMP 协议类型，设置个数为 1，可以设置为： ECHO_and_ECHOREPLY； DEST_UNREACH； SOURCE_QUENCH； REDIRECT； ROUTER_ADVERTISEMENT； ROUTER_SOLICITATION； TIME_EXCEEDED； PARAMETERPROB； TIMESTAMP_and_TIMESTAMPREPLY； INFO_REQUEST_and_INFO_REPLY； ADDRESS_and_ADDRESSREPLY。 **any** 表示上述协议类型中的任意一种类型。
start_port	起始端口，格式为 INTEGER<1-65535>。
end_port	终止端口，格式为 INTEGER<1-65535>。
start_typenum	起始协议号，格式为 INTEGER<1-255>。
end_typenum	终止协议号，格式为 INTEGER<1-255>。
protocol_object_name	协议对象名称，格式为 WORD<1-15>。
protocol_group_name	协议对象组名称，格式为 WORD<1-15>。
tos	表示设置 TOS （TOS 是指 IP 数据包包头中的服务类型字段）的服务类型。
tos_type	服务类型，格式为 INTEGER<0-15>。 0 表示：不要求任何服务。 1 表示：D 比特，要求更低的时延； 2 表示：T 比特，要求更高的吞吐量； 4 表示：R 比特，要求更高的可靠性； 8 表示：C 比特，要求选择代价更小的路由。
input-interface	入口三层接口。
interface_name	三层接口名称，格式为 WORD<1-16>。

说明

源 IP 地址的起始地址和终止地址之间的 IP 地址数量不能超过 100 个。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在策略路由配置模式下使用。

范例

范例 . 为策略路由 test 添加策略条件。当源 IP 地址为 192.168.1.100 的数据包从 VLAN1 进入 NetEye 进行路由匹配时，如果该数据包的包头为 PARAMETERPROB 类型的 ICMP 协议以及包头的 TOS 服务为要求更高的吞吐量，则进入 test 的路由表查找路由。

```
NetEye@root-system]policy route test
NetEye@root-system-routepolicy-test]matching sip 192.168.1.100
NetEye@root-system-routepolicy-test]matching input-interface vlan1
NetEye@root-system-routepolicy-test]matching protocol icmp
PARAMETERPROB
NetEye@root-system-routepolicy-test]matching tos 2
```

相关命令

命令名称	描述信息
policy route	添加策略路由。
unset matching	删除策略条件。

policy route

使用 **policy route** 命令添加策略路由。配置成功后，可以为该策略路由添加策略条件并为该策略路由的路由表添加静态路由。

命令

policy route *policy_name* [**number** *pri*]

语法

policy_name	策略路由名称，格式为 WORD<1-15>。
pri	*pri* 关键字为可选项，表示策略的优先级，缺省设置为 1。格式为 INTEGER<1-80000>。

说明

如果 *pri* 设置为 1，表示将该策略路由添加到所有策略路由的前面；如果 *pri* 省略，表示将该策略路由添加到所有策略路由的后面。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加名称为 test 的策略路由，其优先级为 2。

```
NetEye@root-system]policy route test number 2
```

相关命令

命令名称	描述信息
policy route enable, disable	启用或者禁用策略路由。
show policy route	显示策略路由配置信息。
unset policy route	删除策略路由。

policy route enable, disable

使用 **policy route enable, disable** 命令启用或者禁用策略路由。

命令

policy route *policy_name* {**enable** | **disable**}

语法

policy_name	策略路由名称，格式为 WORD<1-15>。
enable | disable	• enable— 启用策略路由 • disable— 禁用策略路由 缺省设置为 enable

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 禁用策略路由 test。

```
NetEye@root-system]policy route test disable
```

相关命令

命令名称	描述信息
policy route	添加策略路由。
show policy route	显示策略路由配置信息。
unset policy route	删除策略路由。

route

使用 **route** 命令为缺省路由表和策略路由的路由表添加静态路由。配置成功后，与该静态路由相匹配的数据包发送到该静态路由指定的设备。

命令

route {**default** | *ip_address netmask*} {**interface** *interface_name* [**gateway** *nexthop*] | **gateway** *nexthop* [**interface** *interface_name*]} [*metric*]

语法

default	默认路由，表示目的 IP 地址和子网掩码均为 0.0.0.0。
ip_address	目的 IP 地址，格式为 x.x.x.x。
netmask	子网掩码，格式为 x.x.x.x。
interface_name	三层接口名称，格式为 WORD<1-16>。
nexthop	下一跳 IP 地址，格式为 x.x.x.x。
metric	路由度量值，格式为 INTEGER<1-255>，缺省值为 1。

说明

1. 在全局配置模式下只能为缺省路由表添加静态路由。如果为缺省路由表添加默认路由，其目的地址和子网掩码只能设置为 0.0.0.0。
2. 在策略路由配置模式下只能为策略路由的路由表添加静态路由。
3. 如果有多条路由可以匹配，那么最小路由度量值的路由优先选取。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在策略路由配置模式和全局配置模式下使用。

范例

范例 1. 在全局配置模式下为缺省路由表添加静态路由。当一个数据包要达到 202.118.1.82，会通过 VLAN2 接口发送到 192.168.1.101 后，再进行转发。

```
NetEye@root-system]route 202.118.1.82 255.255.255.255 interface vlan2
gateway 192.168.1.101
```

范例 2. 在策略路由配置模式下，为 test 策略路由添加一条静态路由，指定其路由度量值为 3。当一个数据包要到达 202.118.1.23，会通过 VLAN1 接口发送到 192.168.1.102 后，再进行转发。

```
NetEye@root-system]policy route test
NetEye@root-system-routepolicy-test]route 202.118.1.23 255.255.255.255
gateway 192.168.1.102 interface vlan1 3
```

相关命令

命令名称	描述信息
policy route	添加策略路由。
show route	显示缺省路由表中路由的配置信息。
unset route	删除路由表中的静态路由。

route load-balancing

使用 **route load-balancing** 命令为缺省路由表和策略路由的路由表添加具有负载均衡功能的静态路由。配置成功后，与该静态路由相匹配的数据包发送到该静态路由指定的设备。

命令

route {**default** | *ip_address netmask*} **load-balancing** {{**gateway** *nexthop* | **interface** *interface_name* **gateway** *nexthop*} *weight* [**ip-track** {**arpping** *track_address* | **ping** *track_address* | **tcpping** *track_address* **port** *track_port*} *track_cycle track_time*] | **interface** *interface_name weight*} [*metric*]

语法

default	默认路由，表示目的 IP 地址和子网掩码均为 0.0.0.0。
ip_address	目的 IP 地址，格式为 x.x.x.x。
netmask	子网掩码，格式为 x.x.x.x。
interface_name	三层接口名称，格式为 WORD<1-16>。
nexthop	下一跳 IP 地址，格式为 x.x.x.x。
ip-track	表示设置链路探测。
tcpping | arpping | ping	• tcpping—TCP ping 方式 • arpping—ARP ping 方式 • ping—ICMP ping 方式
track_port	探测端口，格式为 INTEGER<1-65535>。
track_cycle	探测周期，格式为 INTEGER<1-30000>。
track_time	探测时间，格式为 INTEGER<1-999>。
weight	权重，格式为 INTEGER<1-255>，缺省值为 1。
metric	路由度量值，格式为 INTEGER<1-255>，缺省值为 1。

说明

1. 在全局配置模式下只能为缺省路由表添加具有负载均衡功能的静态路由。如果为缺省路由表添加默认路由，其目的地址和子网掩码只能设置为 0.0.0.0。
2. 在策略路由配置模式下只能为策略路由的路由表添加具有负载均衡功能的静态路由。
3. 如果有多条路由可以匹配，那么最小路由度量值的路由优先选取。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在策略路由配置模式和全局配置模式下使用。

范例

范例 1. 在全局配置模式下，为缺省路由表添加具有负载均衡功能的静态路由。当一个数据包要达到 202.118.1.18，会通过 VLAN2 接口发送到 192.168.1.101 后，再进行转发。

```
NetEye@root-system]route 202.118.1.18 255.255.255.255 load-balancing interface vlan2 gateway 192.168.1.101 2
```

范例 2. 在策略路由配置模式下，为策略路由 test 添加一条具有负载均衡功能的静态路由。当一个数据包要到达 202.118.1.24，会通过 VLAN1 接口发送到 192.168.1.102 后，再进行转发。

```
NetEye@root-system]policy route test
NetEye@root-system-routepolicy-test]route 202.118.1.24 255.255.255.255 load-balancing gateway 192.168.1.102 interface vlan1 2 3
```

相关命令

命令名称	描述信息
policy route	添加策略路由。
show route	显示缺省路由表中路由的配置信息。
unset route	删除路由表中的静态路由。
unset route load-balancing	删除具有负载均衡功能的静态路由。

show policy route

使用 **show policy route** 命令显示策略路由配置信息。

命令

show policy route [*policy_name*]

语法

policy_name	策略路由名称，格式为 WORD<1-15>。

说明

如果指定 *policy_name* 参数，则显示该策略路由的详细信息；如果不指定 *policy_name* 参数，则显示所有的策略路由的简单信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示策略路由 test 的配置信息。

```
NetEye@root>show policy route test
```

【返回结果】

```
Route-policy:
  Policy Name: test
  Input-Interface: Any
  Tos: Any
  State: enable
IP list:
              Any
Protocol list:

Routing table:
```

```
Type Destination        Interface Gateway         Metric Weight Lb  IP-
Track
S    10.1.1.0/24        vlan2                     25             No
```

相关命令

命令名称	描述信息
policy route	添加策略路由。
policy route enable, disable	启用或者禁用策略路由。
unset policy route	删除策略路由。

show route

使用 **show route** 命令显示缺省路由表中所有的路由配置信息。

命令

show route

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例：显示缺省路由表中所有的路由配置信息。

```
NetEye@root>show route
```

【返回结果】

```
Routing table:
Type Destination        Interface Gateway         Metric Weight Lb  IP-
Track

C    10.3.1.0/24        eth-s4p1
S    default                      10.3.1.1        1             No
```

相关命令

命令名称	描述信息
policy route	添加策略路由。
route	为缺省路由表和策略路由的路由表添加静态路由。
route load-balancing	添加具有负载均衡功能的静态路由。

unset matching

使用 **unset matching** 命令删除策略路由的策略条件。

命令

unset matching [**sip** [*start_ipaddress* [*end_ipaddress*] | *ipaddr_object_name* | *ipaddr_group_name* | *ip_addr* **mask** *mask_length*] | **protocol** {**icmp** | **tcp** | **udp** | **other** | *protocol_object_name* | *protocol_group_name*} | **tos** | **input-interface**]

语法

start_ipaddress	源 IP 地址的起始地址，格式为 x.x.x.x。
end_ipaddress	源 IP 地址的终止地址，格式为 x.x.x.x。
ipaddr_object_name	IP 地址对象名称，格式为 WORD<1-63>。
ipaddr_group_name	IP 地址对象组名称，格式为 WORD<1-63>。
ip_addr	源 IP 地址，格式为 x.x.x.x。
mask_length	掩码长度，格式为 INTEGER<1-32>。
protocol_object_name	协议对象名称，格式为 WORD<1-63>。
protocol_group_name	协议对象组名称，格式为 WORD<1-63>。
tos	表示设置 TOS （TOS 是指 IP 数据包包头中的服务类型字段）的服务类型。

说明

1. 如果不指定任何参数，即命令为 **unset matching**，表示删除策略路由的所有策略条件。
2. 如果仅使用命令 **unset matching sip**，表示删除策略路由的所有源 IP 条件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在策略路由配置模式下使用。

范例

范例 . 删除策略路由 test 的策略条件。

```
NetEye@root-system]policy route test
NetEye@root-system-routepolicy-test]unset matching sip 192.168.1.100
192.168.1.150
NetEye@root-system-routepolicy-test]unset matching input-interface
NetEye@root-system-routepolicy-test]unset matching protocol icmp
NetEye@root-system-routepolicy-test]unset matching tos
```

相关命令

命令名称	描述信息
policy route	添加策略路由。
matching	为策略路由添加策略条件。

unset policy route

使用 **unset matching** 命令删除策略路由。

命令

unset policy route [*policy_name*]

语法

policy_name	策略路由名称，格式为 WORD<1-15>。

说明

如果不指定 *policy_name* 参数，则删除所有的策略路由。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除策略路由名称为 test 的策略路由。

```
NetEye@root-system]unset policy route test
```

相关命令

命令名称	描述信息
policy route	添加策略路由。
policy route enable, disable	启用或者禁用策略路由。
show policy route	显示策略路由配置信息。

unset route

使用 **unset route** 命令删除静态路由。

命令

unset route {**default** | *ip_address netmask*} [**interface** *interface_name* [**gateway** *nexthop*] | **gateway** *nexthop* [**interface** *interface_name*]]

语法

default	默认路由，表示目的 IP 地址和子网掩码均为 0.0.0.0。
ip_address	目的 IP 地址，格式为 x.x.x.x。
netmask	子网掩码，格式为 x.x.x.x。
interface_name	三层接口名称，格式为 WORD<1-16>。
nexthop	下一跳 IP 地址，格式为 x.x.x.x。

说明

1. 在全局配置模式下，删除的路由为缺省路由表中的静态路由。如果不指定任何参数，即命令为 **unset route**，表示删除缺省路由表中所有的静态路由，包括具有负载均衡功能的静态路由。
2. 在策略路由配置模式下，删除的路由为策略路由的路由表中的静态路由。如果不指定任何参数，即命令为 **unset route**，表示删除策略路由的路由表中所有的静态路由，包括具有负载均衡功能的静态路由。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在策略路由配置模式和全局配置模式下使用。

范例

范例 . 在策略路由配置模式下，删除策略路由 test 的路由表中目的地址为 192.168.1.112 的静态路由。

```
NetEye@root-system]policy route test
NetEye@root-system-routepolicy-test]unset route 192.168.1.112
255.255.255.255
```

相关命令

命令名称	描述信息
policy route	添加策略路由。
route	为缺省路由表和策略路由的路由表添加静态路由。
show route	显示缺省路由表中路由的配置信息。
unset route load-balancing	删除具有负载均衡功能的静态路由。

unset route load-balancing

使用 **unset route load-balancing** 命令删除缺省路由表和策略路由的路由表中具有负载均衡功能的静态路由。

命令

unset route {**default** | *ip_address netmask*} **load-balancing** {**gateway** *nexthop* | **interface** *interface_name* [**gateway** *nexthop*]} *weight*

语法

default	默认路由，表示目的 IP 地址和子网掩码均为 0.0.0.0。
ip_address	目的 IP 地址，格式为 x.x.x.x。
netmask	子网掩码，格式为 x.x.x.x。
interface_name	三层接口名称，格式为 WORD<1-16>。
nexthop	下一跳地址，格式为 x.x.x.x。
weight	权重，格式为 INTEGER<1-255>，缺省值为 1。

说明

1. 在全局配置模式下，删除的路由为缺省路由表中具有负载均衡功能的静态路由。
2. 在策略路由配置模式下，删除的路由为该策略路由的路由表中具有负载均衡功能的静态路由。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在策略路由配置模式和全局配置模式下使用。

范例

范例 . 在策略路由配置模式下，删除策略路由 test 的路由表中从 VLAN1 发送出去的目的地址为 192.168.1.111 的具有负载均衡功能的静态路由。

```
NetEye@root-system]policy route test
NetEye@root-system-routepolicy-test]unset route 192.168.1.111
255.255.255.255 load-balancing interface vlan1 3
```

相关命令

命令名称	描述信息
policy route	添加策略路由。
route load-balancing	添加具有负载均衡功能的静态路由。
show route	显示缺省路由表中路由的配置信息。

多播路由

dvmrp route

使用 **dvmrp route** 命令为多播路由表添加静态多播路由。配置成功后， NetEye 可以使用所配置的静态路由，在三层接口间转发多播信息流。

命令

dvmrp route *multicast_source_ipaddress group_address* **input** *interface_name* **forwarding** *interface_namelist* [**threshold** *threshold_value*]

语法

multicast_source_ipaddress	源 IP 地址，格式为 x.x.x.x。
group_address	组 IP 地址，格式为 x.x.x.x。
input	表示多播转发的入口三层接口。
interface_name	入口三层接口 ，格式为 WORD<1-16>。
forwarding	表示多播转发的出口三层接口。
interface_namelist	出口三层接口列表，格式为 WORD<1-224>。
threshold_value	生存时间，格式为 INTEGER<1-254>，缺省值为 1。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 为多播路由表添加静态多播路由。当源 IP 地址为 192.168.1.2 到组 IP 地址为 224.1.11.1 的数据包从接口 eth-s4p1 到达 NetEye 时，将从 vlan1 接口转发出去，该多播包的生存时间为 1。

```
NetEye@root-system]dvmrp route 192.168.1.2 224.1.11.1 input eth-s4p1
forwarding vlan1 threshold 1
```

相关命令

命令名称	描述信息
show dvmrp route	显示 DVMRP 的路由信息。
unset dvmrp route	删除 DVMRP 多播路由表中的多播路由。

show dvmrp route

使用 **show dvmrp route** 命令显示 **DVMRP**（距离矢量多播路由协议）的路由信息。

命令

show dvmrp route

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 DVMRP 的路由信息。

```
NetEye@root>show dvmrp route
```

【返回结果】

```
DVMRP route table:

 Source      Group     Input Interface   Forwarding Interfaces  Threshold
192.168.1.2 224.1.11.1     eth-s4p1             vlan1                1
```

相关命令

命令名称	描述信息
dvmrp route	添加静态多播路由信息。

unset dvmrp route

使用 **unset dvmrp route** 命令删除 **DVMRP**（距离矢量多播路由协议）多播路由表中的多播路由。

命令

unset dvmrp route [*multicast_source_ipaddress group_address* **input** *interface_name*]

语法

multicast_source_ipaddress	源 IP 地址，格式为 x.x.x.x。
group_address	组 IP 地址，格式为 x.x.x.x。
input	表示多播转发的入口三层接口。
interface_name	入口三层接口名称，格式为 WORD<1-16>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除 DVMRP 多播路由表中入口接口为 VLAN100、源 IP 地址为 192.168.1.100、组 IP 地址为 224.3.3.3 的多播路由。

```
NetEye@root-system]unset dvmrp route 192.168.1.100 224.3.3.3 input
vlan100
```

相关命令

命令名称	描述信息
dvmrp route	为多播路由表添加静态多播路由。
show dvmrp route	显示 DVMRP 的路由信息。

OSPF

area authentication

使用 **area authentication** 命令在 OSPF 区域中启用认证功能。

使用 **no** 关键字取消该设置。

命令

area *area_id* **authentication** [**message-digest**]

no area *area_id* **authentication**

语法

area_id	区域 ID，格式为 INTEGER<0-4294967295> 或 x.x.x.x。
message-digest	表示在指定的 OSPF 区域启用 MD5 认证。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

说明

配置成功后，此区域中发出的所有的 OSPF 数据包中将带有认证信息。

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#area 1 authentication
```

area default-cost

使用 **area default-cost** 命令为发送到末梢或 NSSA 区域的汇聚缺省路由设置 Metric 值。

使用 **no** 关键字取消该设置。

命令

area *area_id* **default-cost** *metric_value*

no area *area_id* **default-cost**

语法

area_id	区域 ID，格式为 INTEGER<0-4294967295> 或 x.x.x.x。
metric_value	Metric 值，格式为 INTEGER<0-16777215>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#area 1 default-cost 10
```

相关命令

命令名称	描述信息
area nssa	指定一个区域的类型为 NSSA。
area stub	指定一个区域为 STUB 区域。

area nssa

使用 **area nssa** 命令指定一个区域的类型为 NSSA。

使用 **no** 关键字取消该设置。

命令

area *area_id* **nssa** [**default-information-originate** [**metric** *metric_value*] [**metric-type** {**1** | **2**}]] [**no-redistribution**] [**no-summary**] [**translator-role** {**always** | **candidate** | **never**}]

no area *area_id* **nssa** [**default-information-originate**] [**no-redistribution**] [**no-summary**] [**translator-role**]

语法

area_id	区域 ID，格式为 INTEGER<0-4294967295> 或 x.x.x.x。
default-information-originate	在 OSPF ABR 或 OSPF ASBR 中产生一个能够进入 NSSA 的缺省路由。在 ABR 上配置该命令时无需定义缺省路由；如果在 ASBR 上配置该命令，则需要配置缺省路由。
metric_value	进入 NSSA 的缺省路由的 Metric 值，格式为 INTEGER<0-16777214>。
1 | 2	进入 NSSA 的缺省路由的 Metric 类型。
no-redistribution	不将额外路由重发布到 NSSA 内。
no-summary	不导入汇总路由 （过滤类型 3 的 LSA）。
translator-role	指定 NSSA 的传输模式，是否对 Tpye7 LSA 进行转换。
always | candidate | never	• always — 一直进行 NSSA-LSA 到 Type-5 LSA 转换 • candidate— 被选中时进行 NSSA-LSA 到 Type-5 LSA 转换 • never— 从不进行 NSSA-LSA 到 Type-5 LSA 转换

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
```

```
neteye-ospfd(config-router)#area 1 nssa
neteye-ospfd(config-router)#area 3 nssa translator-role candidate
no-redistribution default-information-originate metric 34 metric-type 2
```

相关命令

命令名称	描述信息
area default-cost	为发送到末梢或 NSSA 区域的汇聚缺省路由设置 Metric 值。

area range

使用 **area range** 命令在 ABR 上设置路由汇总。

使用 **no** 关键字取消该设置。

命令

[**no**] **area** *area_id* **range** *ip_prefix* [**advertise** | **not-advertise**]

语法

area_id	区域 ID，格式为 INTEGER<0-4294967295> 或 x.x.x.x。
ip_prefix	IP 地址范围，格式为 A.B.C.D/M。
advertise | **not-advertise**	• advertise — 发布该 ABR • not-advertise— 不发布该 ABR

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#area 1 range 192.16.0.0/24
```

area stub

使用 **area stub** 命令指定一个区域为 STUB 区域。

使用 **no** 关键字取消该设置。

命令

[**no**] **area** *area_id* **stub** [**no-summary**]

语法

area_id	区域 ID，格式为 INTEGER<0-4294967295> 或 x.x.x.x。
no-summary	不发布该 ABR。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#area 1 stub
```

area virtual-link

使用 **area virtual-link** 命令在区域上建立到骨干区域的虚链路。

使用 **no** 关键字取消该设置。

命令

area *area_id* **virtual-link** *neighbor_ip* [[**authentication** [**message-digest** | **null**]] [**dead-interval** *dead_interval*] [**hello-interval** *hello_interval*] [**retransmit-interval** *retransmit_interval*] [**transmit-delay** *transmit_delay*] [**message-digest-key** *key_id* **md5** *msg_key* | **authentication-key** *auth_key*]]

no area *area_id* **virtual-link** *neighbor_ip* [**authentication**] [**dead-interval**] [**hello-interval**] [**retransmit-interval**] [**transmit-delay**] [**message-digest-key** *key_id*] [**authentication-key**]

语法

area_id	区域 ID，格式为 INTEGER<0-4294967295> 或 x.x.x.x。
neighbor_ip	虚链路邻居 IP 地址，格式为 X.X.X.X。
message-digest | **null**	• message-digest — 启用虚链路 MD5 认证 • null— 不进行认证 • 如果不指定 message-digest 或 null 关键字，则表示启用虚链路明文认证
dead_interval	虚链路邻居的失效时间，单位为秒，格式为 INTEGER<1-65535>。当在此时间内没有收到链路邻居的 Hello 数据包，即认为链路邻居失效。 缺省值为 40
hello_interval	发送 Hello 数据包的时间间隔，单位为秒，格式为 INTEGER<1-65535>。 缺省值为 10
retransmit_interval	设置在没有得到虚链路邻居确认的情况下，重传 OSPF 数据包的等待时间。单位为秒，格式为 INTEGER<1-3600>。 缺省值为 5
transmit_delay	设置在接口上转发 LSA 升级包所使用的时间，单位为秒，格式为 INTEGER<1-3600>。 缺省值为 1
message-digest-key	设置虚链路的 MD5 认证密钥值。
key_id	密钥 ID，格式为 INTEGER<1-255>。
msg_key	密钥值，格式为 WORD<16-16>。
authentication-key	设置虚链路的明文认证密钥值。
auth_key	密钥值，格式为 WORD<8-8>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#area 1 virtual-link 10.10.11.50 hello 5
dead 10
```

相关命令

命令名称	描述信息
area default-cost	为发送到末梢或 NSSA 区域的汇聚缺省路由设置 Metric 值。

auto-cost reference bandwidth

使用 **auto-cost reference bandwidth** 命令设置参考带宽值。

使用 **no** 关键字取消该设置。

命令

auto-cost reference-bandwidth *reference_bandwidth*

no auto-cost reference-bandwidth

语法

reference_bandwidth	参考带宽值，格式为 INTEGER<0-4294967>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#auto-cost reference-bandwidth 50
```

clear ip ospf process

使用 **clear ip ospf process** 命令清除并重启 OSPF 路由进程。

命令

clear ip ospf [*process_id*] **process**

语法

process_id	路由进程 ID，格式为 INTEGER<1-8>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

说明

如果不指定 *process_id* 参数，则清除并重启所有运行的 OSPF 进程。

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#clear ip ospf process
```

compatible rfc1583

使用 **compatible rfc1583** 命令兼容 rfc 1583。

使用 **no** 关键字取消该设置。

命令

[**no**] **compatible rfc1583**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

说明

OSPF 默认兼容 rfc 2328。

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#compatible rfc1583
```

debug ospf events

使用 **debug ospf events** 命令设置 OSPF 事件的 debug 功能。
使用 **no** 关键字取消该设置。

命令

[**no**] **debug ospf events** [**abr**] [**asbr**] [**lsa**] [**nssa**] [**os**] [**router**] [**vlink**]

语法

area_id	区域 ID，格式为 INTEGER<0-4294967295> 或 x.x.x.x。
no-summary	ABR 不向 stub 区域中发布链路汇聚广播。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

说明

如果不指定任何 debug 选项，则设置所有选项的 debug 功能。

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#no debug ospf event abr
neteye-ospfd#debug ospf event asbr
neteye-ospfd#debug ospf event lsa
neteye-ospfd#no debug ospf event nssa
neteye-ospfd#debug ospf event os
neteye-ospfd#debug ospf event router
neteye-ospfd#debug ospf event vlink
```

debug ospf ifsm

使用 **debug ospf ifsm** 命令设置接口有限状态机 （IFSM）的 debug 功能。
使用 **no** 关键字取消该设置。

命令

[**no**] **debug ospf ifsm** [**status**] [**events**] [**timers**]

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

说明

如果不指定任何 debug 选项，则设置所有选项的 debug 功能。

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#no debug ospf ifsm events
neteye-ospfd#debug ospf ifsm status
neteye-ospfd#debug ospf ifsm timers
```

debug ospf lsa

使用 **debug ospf lsa** 命令设置链路状态广播 （LSA）的 debug 功能。
使用 **no** 关键字取消该设置。

命令

[**no**] **debug ospf lsa** [**flooding**] [**generate**] [**install**] [**maxage**] [**refresh**]

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

说明

如果不指定任何 debug 选项，则设置所有选项的 debug 功能。

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#no debug ospf lsa refresh
neteye-ospfd#debug ospf lsa flooding
neteye-ospfd#debug ospf lsa install
neteye-ospfd#debug ospf lsa maxage
neteye-ospfd#debug ospf lsa generate
```

debug ospf nfsm

使用 **debug ospf nfsm** 命令设置邻居有限状态机 （NFSM）的 debug 功能。
使用 **no** 关键字取消该设置。

命令

[**no**] **debug ospf nfsm** [**events**] [**status**] [**timers**]

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

说明

如果不指定任何 debug 选项，则设置所有选项的 debug 功能。

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#debug ospf nfsm events
neteye-ospfd#no debug ospf nfsm timers
```

debug ospf nsm

使用 **debug ospf nsm** 命令设置网络服务单元（NSM）的 debug 功能。
使用 **no** 关键字取消该设置。

命令

[**no**] **debug ospf nsm** [**interface**] [**redistribute**]

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

说明

如果不指定任何 debug 选项，则设置所有选项的 debug 功能。

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#debug ospf nsm interface
neteye-ospfd#no debug ospf nsm redistribute
```

debug ospf packet

使用 **debug ospf packet** 命令设置 OSPF 数据包的 debug 功能。

使用 **no** 关键字取消该设置。

命令

[**no**] **debug ospf packet** [**dd**] [**detail**] [**hello**] [**ls-ack**] [**ls-request**] [**ls-update**] [**recv**] [**send**]

语法

dd	数据库描述的 debug 信息。
detail	详细的 debug 信息。
hello	Hello 包的 debug 信息。
ls-ack	链路状态确认的 debug 信息。
ls-request	链路状态请求的 debug 信息。
ls-update	链路状态升级的 debug 信息。
recv	接收数据包的 debug 信息。
send	发送数据包的 debug 信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

说明

如果不指定任何 debug 选项，则设置所有选项的 debug 功能。

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#debug ospf packet detail
neteye-ospfd#debug ospf packet dd send detail
neteye-ospfd#no debug ospf packet ls-request recv detail
```

debug ospf route

使用 **debug ospf route** 命令设置路由计算相关的 debug 功能。

使用 **no** 关键字取消该设置。

命令

[**no**] **debug ospf route** [**ase**] [**ia**] [**install**] [**spf**]

语法

ase	外部路由计算的 debug 信息。
ia	区域内路由计算的 debug 信息。
install	路由安装的 debug 信息。
spf	最短路径优先计算的 debug 信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

说明

如果不指定任何 debug 选项，则设置所有选项的 debug 功能。

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#debug ospf route
neteye-ospfd#no debug ospf route ia
neteye-ospfd#debug ospf route install
```

default-information originate

使用 **default-information originate** 命令向 OSPF 域中引入一条外部缺省路由。

使用 **no** 关键字取消该设置。

命令

default-information originate [**always**] [**metric** *metric_value*] [**metric-type** {**1** | **2**}] [**route-map** *route_map_name*]

no default-information originate [**always**] [**metric**] [**metric-type**] [**route-map**]

语法

always	无论本地路由表中是否存在缺省路由都向外广播。
metric_value	外部缺省路由 metric 值，格式为 INTEGER<0-16777214>。
1 | **2**	外部缺省路由 metric 类型。
route_map_name	Route Map 名称，格式为 WORD。只有满足 Route Map 条件，才引入外部缺省路由。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#default-information originate always metric 23 metric-type 2 route-map myinf
```

default-metric

使用 **default-metric** 命令设置 OSPF 路由协议的缺省 Metric 值。

使用 **no** 关键字取消该设置。

命令

default-metric *metric_value*

no default-metric

语法

metric_value	缺省 Metric 值，格式为 INTEGER<0-16777214>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#default-metric 100
```

相关命令

命令名称	描述信息
redistribute	向 OSPF 区域中引入其他协议的路由。

distance

使用 **distance** 命令设置指定路由类型的 OSPF 路由管理距离。

使用 **no** 关键字取消该设置。

命令

distance {*ospf_admin_distance* | **ospf** {**external** *external_admin_distance* | **inter-area** *inter_area_admin_distance* | **intra-area** *intra_area_admin_distance*}}

no distance {*ospf_admin_distance* | **ospf**}

语法

ospf_admin_distance	OSPF 管理距离，格式为 INTEGER<1-255>。
external_admin_distance	OSPF 外部管理距离，格式为 INTEGER<1-255>。
inter_area_admin_distance	OSPF 区域间管理距离，格式为 INTEGER<1-255>。
intra_area_admin_distance	OSPF 区域内管理距离，格式为 INTEGER<1-255>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#distance ospf inter-area 20
```

distribute-list

使用 **distribute-list** 命令过滤网络路由。

使用 **no** 关键字取消该设置。

命令

[**no**] **distribute-list** *access_list_name* {**in** | **out** {**bgp** | **connected** | **rip** | **static** | **ospf** [*process_id*]}}

语法

access_list_name	访问列表名称，格式为 WORD。
in	阻止从 OSPF 学到的路由放置到 IP 路由表中。即使 OSPF 路由被阻止放置到 IP 路由选择表中，该条路由仍然被保存在 OSPF 数据库中，并且会被广播到 OSPF 邻居路由器。
out	阻止从其他路由进程重发布到 OSPF 的路由放置到 OSPF 数据库。
process_id	路由进程 ID，格式为 INTEGER<1-8>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#distribute-list list1 out bgp
```

相关命令

命令名称	描述信息
redistribute	向 OSPF 区域中引入其他协议的路由。

ip ospf authentication

使用 **ip ospf authentication** 命令设置发送和接收 OSPF 数据包所使用的认证方法。

使用 **no** 关键字取消该设置。

命令

ip ospf [*interface_id*] **authentication** [**message-digest** | **null**]

no ip ospf [*interface_id*] **authentication**

语法

interface_id	接口 IP 地址，格式为 x.x.x.x。
message-digest | **null**	• message-digest — MD5 认证 • null— 不进行认证

说明

如果不指定 **message-digest** 或 **null** 关键字，则表示发送和接收 OSPF 数据包使用明文认证。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 接口配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#interface eth1
neteye-ospfd(config-if)#ip ospf authentication null
```

相关命令

命令名称	描述信息
area authentication	在 OSPF 区域中启用认证功能。
ip ospf authentication-key	设置 OSPF 使用的认证密码。
ip ospf message-digest-key	设置用于 OSPF 认证的 MD5 密钥。

ip ospf authentication-key

使用 **ip ospf authentication-key** 命令设置 OSPF 使用的认证密码。配置成功后，一个域中的所有路由器将使用相同的认证密码。

使用 **no** 关键字取消该设置。

命令

ip ospf [*interface_id*] **authentication-key** *password*

no ip ospf [*interface_id*] **authentication-key**

语法

interface_id	接口 IP 地址，格式为 x.x.x.x。
password	认证密码，格式为 LINE。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 接口配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#network 10.10.10.0 0.0.0.255 area 0
neteye-ospfd(config-router)#area 0 authentication
neteye-ospfd(config-router)#exit
neteye-ospfd# interface eth1
neteye-ospfd(config-if)# ip ospf authentication-key test
```

相关命令

命令名称	描述信息
area authentication	在 OSPF 区域中启用认证功能。
ip ospf authentication	设置指定发送和接收 OSPF 数据包所使用的认证方法。

ip ospf cost

使用 **ip ospf cost** 命令设置路由器 LSA 中的链路状态 metric 值。
使用 **no** 关键字取消该设置。

命令

ip ospf [*interface_id*] **cost** *metric_value*

no ip ospf [*interface_id*] **cost**

语法

interface_id	接口 IP 地址，格式为 x.x.x.x。
metric_value	metric 值，格式为 INTEGER<1-65535>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 接口配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#interface eth1
neteye-ospfd(config-if)#ip ospf cost 10
```

相关命令

命令名称	描述信息
auto-cost reference bandwidth	设置参考带宽值。
show ip ospf interface	显示 OSPF 接口信息。

ip ospf database-filter

使用 **ip ospf database-filter** 命令阻止 LSA 在当前接口上泛洪。

使用 **no** 关键字取消该设置。

命令

[**no**] **ip ospf** [*interface_id*] **database-filter all out**

语法

interface_id	接口 IP 地址，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 接口配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#interface eth1
neteye-ospfd(config-if)#ip ospf database-filter all out
```

ip ospf dead-interval

使用 **ip ospf dead-interval** 命令设置邻居死亡定时器。配置成功后，如果在此时间内没有收到邻居的 hello 数据包，则认为邻居死亡。

使用 **no** 关键字取消该设置。

命令

ip ospf [*interface_id*] **dead-interval** *dead_interval*

no ip ospf [*interface_id*] **dead-interval**

语法

interface_id	接口 IP 地址，格式为 x.x.x.x。
dead_interval	死亡定时器值，单位为秒，格式为 INTEGER<1-65535>。 缺省值为 40

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 接口配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#interface eth1
neteye-ospfd(config-if)#ip ospf dead-interval 10
```

相关命令

命令名称	描述信息
ip ospf hello-interval	设置发送 hello 数据包的时间间隔。
show ip ospf interface	显示 OSPF 接口信息。

ip ospf disable all

使用 **ip ospf disable all** 命令在指定接口上关闭对 OSPF 数据包的处理。使用 **no** 关键字取消该设置。

命令

[**no**] **ip ospf disable all**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 接口配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#interface eth1
neteye-ospfd(config-if)#ip ospf disable all
```

ip ospf hello-interval

使用 **ip ospf hello-interval** 命令设置发送 hello 数据包的时间间隔。

使用 **no** 关键字取消该设置。

命令

ip ospf [*interface_id*] **hello-interval** *hello_interval*

no ip ospf [*interface_id*] **hello-interval**

语法

interface_id	接口 IP 地址，格式为 x.x.x.x。
hello_interval	时间间隔，单位为秒，格式为 INTEGER<1-65535>。 缺省值为 10

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 接口配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#interface eth1
neteye-ospfd(config-if)#ip ospf hello-interval 3
```

相关命令

命令名称	描述信息
ip ospf dead-interval	设置邻居死亡定时器。
show ip ospf interface	显示 OSPF 接口信息。

ip ospf message-digest-key

使用 **ip ospf message-digest-key** 命令设置用于 OSPF 认证的 MD5 密钥。使用 **no** 关键字取消该设置。

命令

ip ospf [*interface_id*] **message-digest-key** *key_id* **md5** *key*

no ip ospf [*interface_id*] **message-digest-key** *key_id*

语法

interface_id	接口 IP 地址，格式为 x.x.x.x。
key_id	密钥 ID，格式为 INTEGER<1-255>。
key	密钥值，格式为 LINE。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 接口配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#interface eth1
neteye-ospfd(config-if)#ip ospf authentication message-digest
neteye-ospfd(config-if)#ip ospf message-digest-key 1 md5 yourpass
```

相关命令

命令名称	描述信息
ip ospf dead-interval	设置邻居死亡定时器。
show ip ospf interface	显示 OSPF 接口信息。

ip ospf mtu

使用 **ip ospf mtu** 命令设置 OSPF 的 MTU 值。

使用 **no** 关键字取消该设置。

命令

ip ospf mtu *mtu_num*

no ip ospf mtu

语法

mtu_num	最大传输单元，格式为 INTEGER<576-65535>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 接口配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#interface eth1
neteye-ospfd(config-if)#ip ospf mtu 1480
```

ip ospf priority

使用 **ip ospf priority** 命令设置路由器的优先级，用以指定 OSPF 网络中的 DR。使用 **no** 关键字取消该设置。

命令

ip ospf [*interface_id*] **priority** *priority*

no ip ospf [*interface_id*] **priority**

语法

interface_id	接口 IP 地址，格式为 x.x.x.x。
priority	优先级，格式为 INTEGER<0-255>。 缺省值为 1

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 接口配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#interface eth1
neteye-ospfd(config-if)#ip ospf priority 3
```

ip ospf retransmit-interval

使用 **ip ospf retransmit-interval** 命令设置指定接口邻接方的链路状态广播（LSA）重传时间间隔。

使用 **no** 关键字取消该设置。

命令

ip ospf [*interface_id*] **retransmit-interval** *retransmit_interval*

no ip ospf [*interface_id*] **retransmit-interval**

语法

interface_id	接口 IP 地址，格式为 x.x.x.x。
retransmit_interval	时间间隔，单位为秒，格式为 INTEGER<1-65535>。 缺省值为 5

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 接口配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#interface eth1
neteye-ospfd(config-if)#ip ospf retransmit-interval 6
```

ip ospf transmit-delay

使用 **ip ospf transmit-delay** 命令设置传送 LSA 数据包的时间延迟。

使用 **no** 关键字取消该设置。

命令

ip ospf [*interface_id*] **transmit-delay** *delay*

no ip ospf [*interface_id*] **transmit-delay**

语法

interface_id	接口 IP 地址，格式为 x.x.x.x。
delay	时间延迟，单位为秒，格式为 INTEGER<1-65535>。 缺省值为 1

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 接口配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#interface eth1
neteye-ospfd(config-if)#ip ospf transmit-delay 3
```

max-concurrent-dd

使用 **max-concurrent-dd** 命令设置可同时处理的最多 DD(数据库描述符) 数。

命令

max-concurrent-dd *dd_processes_num*

语法

dd_processes_num	DD 进程数，格式为 INTEGER<1-65535>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#max-concurrent-dd 4
```

network area

使用 **network area** 命令设置启用 OSPF 的接口，以及该接口所在的 OSPF 区域。使用 **no** 关键字取消该设置。

命令

[**no**] **network** {*ip_address wildcard_mask* | *ip_prefix*} **area** *area_id*

语法

ip_address	IP 地址，格式为 X.X.X.X。
wildcard_mask	反向掩码，格式为 X.X.X.X。
ip_prefix	IP 地址范围，格式为 A.B.C.D/M。
area_id	区域 ID，格式为 INTEGER<0-4294967295> 或 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#network 10.0.0.0 0.255.255.255 area 3
```

ospf enable, disable

使用 **ospf enable, disable** 命令启用或禁用 OSPF 功能。

命令

ospf {**enable** | **disable**}

语法

enable	**disable**	• enable— 启用 OSPF 功能 • disable— 禁用 OSPF 功能

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show ospf state	显示是否启用了 OSPF 功能。

overflow database

使用 **overflow database** 命令设置当前 OSPF 实例可支持的最多 LSA 数。使用 **no** 关键字设置没有最大 LSA 数限制。

命令

overflow database *max_lsas_num* {**hard** | **soft**}

语法

max_lsas_num	最大 LSA 数，格式为 INTEGER<0-4294967294>。
hard | **soft**	• hard— 如果 LSA 数超出限定值，将关闭。 • soft— 如果 LSA 数超出限定值，将发出警告信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#overflow database 5 hard
```

overflow database external

使用 **overflow database external** 命令设置外部数据库的大小、及路由器等待结束溢出状态的时间。

使用 **no** 关键字取消该设置。

命令

overflow database external *max_lsas_num recover_time*

语法

max_lsas_num	最大 LSA 数，格式为 INTEGER<0-2147483647>。在 AS 内所有路由器此参数的设置必须相同。
recover_time	路由器等待结束溢出状态的时间，格式为 INTEGER<0-65535>。如果此参数设置为 0，则只有在运行了明确的管理员命令后，路由器才能结束溢出状态。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#overflow database external 5 3
```

passive-interface

使用 **passive-interface** 命令设置在指定的接口上禁止发送 hello 数据包。

命令

passive-interface *interface_name* [*ip_address*]

语法

interface_name	接口名称，格式为 WORD<3-15>。
ip_address	接口 IP 地址，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 接口配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#passive-interface eth1
```

redistribute

使用 **redistribute** 命令向 OSPF 区域中引入其他协议的路由。
使用 **no** 关键字取消该设置。

命令

redistribute {**bgp** | **rip** | **connected** | **static**} [**metric** *metric_value*] [**metric-type** {**1** | **2**}] [**route-map** *route_map_name*] [**tag** *tag*]

no redistribute {**bgp** | **rip** | **connected** | **static**} [**metric**] [**metric-type**] [**route-map**] [**tag**]

语法

bgp	表示引入 BGP 路由。
rip	表示引入 RIP 路由。
connected	表示引入直连路由。
static	表示引入静态路由。
metric_value	外部 metric 值，格式为 INTEGER<0-16777214>。
1 | **2**	外部 metric 类型。
route_map_name	Route Map 名称，格式为 WORD。表示根据 Route Map 向 OSPF 区域中引入其他协议中的路由。
tag	外部路由标记，格式为 INTEGER<0-4294967295>。表示根据路由标签向 OSPF 区域中引入其他协议中的路由。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#redistribute bgp metric 12
```

redistribute ospf

使用 **redistribute ospf** 命令重发布指定的 OSPF 进程到另一个 OSPF 进程中，或通过设置 metric 值、 Route Map、路由标记有选择的将特定的 OSPF 进程重发布到另一个 OSPF 进程中。

使用 **no** 关键字取消该设置。

命令

redistribute ospf *process_id* [**metric** *metric_value*] [**metric-type** {**1** | **2**}] [**route-map** *route_map_name*] [**tag** *tag*]

no redistribute ospf *process_id* [**metric**] [**metric-type**] [**route-map**] [**tag**]

语法

process_id	路由进程 ID，格式为 INTEGER<1-8>。
metric_value	外部 metric 值，格式为 INTEGER<0-16777214>。
1 | 2	外部 metric 类型。
route_map_name	Route Map 名称，格式为 WORD。
tag	外部路由标记，格式为 INTEGER<0-4294967295>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 1
neteye-ospfd(config-router)#redistribute ospf 2 metric 10 metric-type 1
route-map rmp1 tag 3
```

router ospf

使用 **router ospf** 命令进入到 OSPF 路由配置模式。
使用 **no** 关键字删除指定的路由进程。

命令

[**no**] **router ospf** *process_id*

语法

process_id	路由进程 ID，格式为 INTEGER<1-8>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 全局配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#
```

router-id

使用 **router-id** 命令为 OSPF 进程设置路由器标识。
使用 **no** 关键字取消该设置。

命令

router-id *ip_address*

no router-id [*ip_address*]

语法

ip_address	路由器标识，格式为 X.X.X.X。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#router-id 10.10.10.60
```

相关命令

命令名称	描述信息
show ip ospf	显示 OSPF 路由进程信息。

show debugging ospf

使用 **show debugging ospf** 命令显示 OSPF 的 debug 选项。

命令

show debugging ospf

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#show debugging ospf
```

【返回结果】

```
OSPF packet Link State Update debugging is on
OSPF all events debugging is on
te mo
2002/05/09 14:08:11 OSPF: RECV[LS-Upd]: From 10.10.10.70 via
eth0:10.10.10.50
(10.10.10.10 -> 224.0.0.5)
2002/05/09 14:08:11 OSPF: LSA[10.10.10.10:10.10.10.70]:
instance(0x8139cd0) created
with Link State Update
2002/05/09 14:08:11 OSPF: RECV[LS-Upd]: From 10.10.10.70 via
eth0:10.10.10.50
(10.10.10.10 -> 224.0.0.5)
2002/05/09 14:12:33 OSPF: SEND[LS-Upd]: Begin send queue
2002/05/09 14:12:33 OSPF: SEND[LS-Upd]: # of LSAs 1, destination
224.0.0.5
2002/05/09 14:12:33 OSPF: SEND[LS-Upd]: End send queue
2002/05/09 14:12:33 OSPF: SEND[LS-Upd]: To 224.0.0.5 via
eth0:10.10.10.50
```

show ip ospf

使用 **show ip ospf** 命令显示 OSPF 路由进程信息。

命令

show ip ospf [*process_id*]

语法

process_id	OSPF 进程 ID，格式为 INTEGER<1-8>。

说明

如果不指定 *process_id* 参数，则显示所有 OSPF 路由进程信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#show ip ospf
```

【返回结果】

```
Routing Process "ospf 1" with ID 10.10.11.60
Process uptime is 46 minutes
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
This router is an ASBR (injecting external routing information)
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Refresh timer 10 secs
Number of external LSA 1. Checksum Sum 0xBC1E
Number of non-default external LSA 1
External LSA database is unlimited.
Number of areas attached to this router: 1
```

```
Area 0 (BACKBONE)
Number of interfaces in this area is 1(1)
Number of fully adjacent neighbors in this area is 1
Area has no authentication
SPF algorithm last executed 00:46:27.935 ago
SPF algorithm executed 2 times
Number of LSA 5. Checksum Sum 0x026a20
Routing Process "ospf 100" with ID 10.10.11.146
Process uptime is 0 minute
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Refresh timer 10 secs
Number of external LSA 0. Checksum Sum 0x0
Number of non-default external LSA 0
External LSA database is unlimited.
Number of areas attached to this router: 1
Area 1
Number of interfaces in this area is 1(1)
Number of fully adjacent neighbors in this area is 0
Number of fully adjacent virtual neighbors through this area is 0
Area has no authentication
SPF algorithm executed 0 times
Number of LSA 1. Checksum Sum 0x00e3e2
```

show ip ospf border-routers

使用 **show ip ospf border-routers** 命令显示 OSPF 路由进程的 ABR 和 ASBR 信息。

命令

show ip ospf [*process_id*] **border-routers**

语法

process_id	OSPF 进程 ID，格式为 INTEGER<1-8>。

说明

如果不指定 *process_id* 参数，则显示所有 OSPF 路由进程的 ABR 和 ASBR 信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#show ip ospf border-routers
```

【返回结果】

```
OSPF process 1 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 10.15.0.1 [10] via 10.10.0.1, eth0, ASBR, Area 0.0.0.0
i 172.16.10.1 [10] via 10.10.11.50, eth1, ABR, ASBR, Area 0.0.0.0
```

show ip ospf database

使用 **show ip ospf database** 命令显示 OSPF 路由进程的数据库摘要信息。

命令

show ip ospf [*process_id*] **database** [**self-originate | max-age | adv-router** *ip_address*]

语法

process_id	OSPF 进程 ID，格式为 INTEGER<1-8>。
**self-originate	max-age	adv-router**	• self-originate — 只显示自身产生的 LSA。 • max-age— 显示 MaxAge 列表中的 LSA 信息。此列表维护达到最大生存时间 （3600 秒）的数据库中所有 LSA 信息。 • adv-router— 显示指定路由器的 LSA。
ip_address	发布路由器地址，格式为 X.X.X.X。

说明

如果不指定 *process_id* 参数，则显示所有 OSPF 路由进程的数据库摘要信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#show ip ospf database
```

【返回结果】

```
OSPF Router process 1 with ID (10.10.11.60)
Router Link States (Area 0.0.0.1)
Link ID ADV Router Age Seq# CkSum Link count
10.10.11.60 10.10.11.60 32 0x80000002 0x472b 1
OSPF Router process 100 with ID (10.10.11.60)
Router Link States (Area 0.0.0.0)
Link ID ADV Router Age Seq# CkSum Link count
10.10.11.60 10.10.11.60 219 0x80000001 0x4f5d 0
```

show ip ospf database asbr-summary

使用 **show ip ospf database asbr-summary** 命令显示 ASBR 汇总 LSA 信息。

命令

show ip ospf [*process_id*] **database asbr-summary** [*link_state_id*] [**adv-router** *ip_address* | **self-originate**]

语法

process_id	OSPF 进程 ID，格式为 INTEGER<1-8>。
link_state_id	链路状态 ID，格式为 X.X.X.X。
adv-router	显示指定路由器的 LSA。
ip_address	发布路由器地址，格式为 X.X.X.X。
self-originate	只显示自身产生的 LSA。

说明

如果不指定 *process_id* 参数，则显示所有 OSPF 路由进程的 ASBR 汇总 LSA 信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#show ip ospf database asbr-summary
```

show ip ospf database external

使用 **show ip ospf database external** 命令显示外部 LSA 信息。

命令

show ip ospf [*process_id*] **databaseexternal** [*link_state_id*] [**adv-router** *ip_address*| **self-originate**]

语法

process_id	OSPF 进程 ID，格式为 INTEGER<1-8>。
link_state_id	链路状态 ID，格式为 X.X.X.X。
adv-router	显示指定路由器的 LSA。
ip_address	发布路由器地址，格式为 X.X.X.X。
self-originate	只显示自身产生的 LSA。

说明

如果不指定 *process_id* 参数，则显示所有 OSPF 路由进程的外部 LSA 信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#show ip ospf database external self-originate
```

【返回结果】

```
OSPF Router process 100 with ID (10.10.11.50)
AS External Link States
LS age: 298
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 10.10.100.0 (External Network Number)
```

```
Advertising Router: 10.10.11.50
LS Seq Number: 80000001
Checksum: 0x7033
Length: 36
Network Mask: /24
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 20
Forward Address: 10.10.11.50
External Route Tag: 0
```

show ip ospf database network

使用 **show ip ospf database network** 命令显示网络 LSA 信息。

命令

show ip ospf [*process_id*] **database network** [*link_state_id*] [**adv-router** *ip_address*| **self-originate**]

语法

process_id	OSPF 进程 ID，格式为 INTEGER<1-8>。
link_state_id	链路状态 ID，格式为 X.X.X.X。
adv-router	显示指定路由器的 LSA。
ip_address	发布路由器地址，格式为 X.X.X.X。
self-originate	只显示自身产生的 LSA。

说明

如果不指定 *process_id* 参数，则显示所有 OSPF 路由进程的网络 LSA 信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#show ip ospf database network
```

【返回结果】

```
OSPF Router process 200 with ID (192.30.30.2)
Net Link States (Area 0.0.0.0)
LS age: 1175
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: network-LSA
Link State ID: 192.10.10.9 (address of Designated Router)
```

```
Advertising Router: 192.30.30.3
LS Seq Number: 80000002
Checksum: 0xdfb1
Length: 32
Network Mask: /24
Attached Router: 192.20.20.1
Attached Router: 192.30.30.3
LS age: 1327
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: network-LSA
Link State ID: 192.20.20.2 (address of Designated Router)
Advertising Router: 192.20.20.2
LS Seq Number: 8000000d
Checksum: 0xbce6
Length: 32
Network Mask: /24
Attached Router: 192.20.20.1
Attached Router: 192.20.20.2
LS age: 1278
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: network-LSA
Link State ID: 192.30.30.3 (address of Designated Router)
Advertising Router: 192.30.30.3
Advertising Router: 192.30.30.3
LS Seq Number: 80000001
Checksum: 0x0556
Length: 32
Network Mask: /24
Attached Router: 192.30.30.2
Attached Router: 192.30.30.3
LS age: 1436
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: network-LSA
Link State ID: 192.40.40.2 (address of Designated Router)
Advertising Router: 192.20.20.2
--More--
```

show ip ospf database nssa-external

使用 **show ip ospf database nssa-external** 命令显示 NSSA 外部 LSA 信息。

命令

show ip ospf [*process_id*] **database nssa-external** [*link_state_id*] [**adv-router** *ip_address*| **self-originate**]

语法

process_id	OSPF 进程 ID，格式为 INTEGER<1-8>。
link_state_id	链路状态 ID，格式为 X.X.X.X。
adv-router	显示指定路由器的 LSA。
ip_address	发布路由器地址，格式为 X.X.X.X。
self-originate	只显示自身产生的 LSA。

说明

如果不指定 *process_id* 参数，则显示所有 OSPF 路由进程的 NSSA 外部 LSA 信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#show ip ospf database nssa-external adv-router 10.10.11.50
```

【返回结果】

```
OSPF Router process 100 with ID (10.10.11.50)
NSSA-external Link States (Area 0.0.0.0)
NSSA-external Link States (Area 0.0.0.1 [NSSA])
LS age: 78
Options: 0x0 (*|-|-|-|-|-|-|-)
LS Type: AS-NSSA-LSA
```

```
Link State ID: 0.0.0.0 (External Network Number For NSSA)
Advertising Router: 10.10.11.50
LS Seq Number: 80000001
Checksum: 0xc9b6
Length: 36
Network Mask: /0
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 1
NSSA: Forward Address: 0.0.0.0
--More--
OSPF Router process 100 with ID (10.10.11.50)
NSSA-external Link States (Area 0.0.0.0)
NSSA-external Link States (Area 0.0.0.1 [NSSA])
LS age: 78
Options: 0x0 (*|-|-|-|-|-|-|-)
LS Type: AS-NSSA-LSA
Link State ID: 0.0.0.0 (External Network Number For NSSA)
Advertising Router: 10.10.11.50
LS Seq Number: 80000001
Checksum: 0xc9b6
Length: 36
Network Mask: /0
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 1
NSSA: Forward Address: 0.0.0.0
External Route Tag: 0
NSSA-external Link States (Area 0.0.0.1 [NSSA])
```

show ip ospf database router

使用 **show ip ospf database router** 命令显示路由器 LSA 信息。

命令

show ip ospf [*process_id*] **database router** [*link_state_id*] [**adv-router** *ip_address*| **self-originate**]

语法

process_id	OSPF 进程 ID，格式为 INTEGER<1-8>。
link_state_id	链路状态 ID，格式为 X.X.X.X。
adv-router	显示指定路由器的 LSA。
ip_address	发布路由器地址，格式为 X.X.X.X。
self-originate	只显示自身产生的 LSA。

说明

如果不指定 *process_id* 参数，则显示所有 OSPF 路由进程的路由器 LSA 信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#show ip ospf database router 10.10.11.50
```

【返回结果】

```
OSPF Router process 100 with ID (10.10.11.50)
Router Link States (Area 0.0.0.0)
LS age: 878
Options: 0x2 (*|-|-|-|-|-|E|-)
Flags: 0x3 : ABR ASBR
LS Type: router-LSA
```

```
Link State ID: 10.10.11.50
Advertising Router: 10.10.11.50
LS Seq Number: 80000004
Checksum: 0xe39e
Length: 36
Number of Links: 1
Link connected to: Stub Network
(Link ID) Network/subnet number: 10.10.10.0
(Link Data) Network Mask: 255.255.255.0
Number of TOS metrics: 0
TOS 0 Metric: 10
Router Link States (Area 0.0.0.1)
LS age: 877
Options: 0x2 (*|-|-|-|-|-|E|-)
Flags: 0x3 : ABR ASBR
LS Type: router-LSA
Link State ID: 10.10.11.50
Advertising Router: 10.10.11.50
LS Seq Number: 80000003
Checksum: 0xee93
Length: 36
Number of Links: 1
Link connected to: Stub Network
(Link ID) Network/subnet number: 10.10.11.0
(Link Data) Network Mask: 255.255.255.0
Number of TOS metrics: 0
TOS 0 Metric: 10
```

show ip ospf database summary

使用 **show ip ospf database summary** 命令显示汇总 LSA 信息。

命令

show ip ospf [*process_id*] **database summary** [*link_state_id*] [**adv-router** *ip_address*| **self-originate**]

语法

process_id	OSPF 进程 ID，格式为 INTEGER<1-8>。
link_state_id	链路状态 ID，格式为 X.X.X.X。
adv-router	显示指定路由器的 LSA。
ip_address	发布路由器地址，格式为 X.X.X.X。
self-originate	只显示自身产生的 LSA。

说明

如果不指定 *process_id* 参数，则显示所有 OSPF 路由进程的汇总 LSA 信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#show ip ospf database summary 10.10.10.0
```

【返回结果】

```
OSPF Router process 100 with ID (10.10.11.50)
Summary Link States (Area 0.0.0.0)
Summary Link States (Area 0.0.0.1)
LS age: 1124
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: summary-LSA
```

```
Link State ID: 10.10.10.0 (summary Network Number)
Advertising Router: 10.10.11.50
LS Seq Number: 80000001
Checksum: 0x41a2
Length: 28
Network Mask: /24
TOS: 0 Metric: 10
```

show ip ospf interface

使用 **show ip ospf interface** 命令显示 OSPF 接口信息。

命令

show ip ospf interface *interface_name*

语法

interface_name	接口名称，格式为 WORD<3-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#show ip ospf interface eth1
```

【返回结果】

```
eth1 is up, line protocol is up
Internet Address 1.1.1.1/24, Area 0.0.0.0, MTU 1500
Process ID 0, Router ID 33.33.33.33, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State Waiting, Priority 1, TE Metric 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Neighbor Count is 0, Adjacent neighbor count is 0
Crypt Sequence Number is 1106347721
Hello received 0 sent 1, DD received 0 sent 0
LS-Req received 0 sent 0, LS-Upd received 0 sent 0
LS-Ack received 0 sent 0, Discarded 0
```

show ip ospf neighbor

使用 **show ip ospf neighbor** 命令显示 OSPF 邻居信息。

命令

show ip ospf [*process_id*] **neighbor** [**all** | **detail** [**all**] | **interface** *ip_address* | *neighbor_id* [**detail**]]

语法

process_id	OSPF 进程 ID，格式为 INTEGER<1-8>。
all	包括 down 状态的邻居。
ip_address	接口 IP 地址，格式为 X.X.X.X。
neighbor_id	邻居 ID，格式为 X.X.X.X。
detail	显示 OSPF 邻居的详细信息。

说明

如果不指定 *process_id* 参数，则显示所有 OSPF 路由进程的邻居信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#show ip ospf 8 neighbor
```

【返回结果】

```
OSPF process 8:
Neighbor ID Pri State Dead Time Address Interface
10.10.11.50 1 Full/Backup 00:00:31 10.10.11.50 eth1
```

show ip ospf route

使用 **show ip ospf route** 命令显示 OSPF 路由表信息。

命令

show ip ospf [*process_id*] **route**

语法

process_id	OSPF 进程 ID，格式为 INTEGER<1-8>。

说明

如果不指定 *process_id* 参数，则显示所有 OSPF 路由进程的路由表信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#show ip ospf route
```

【返回结果】

```
OSPF process 1:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
O 10.10.0.0/24 [10] is directly connected, eth0, Area 0.0.0.0
O 10.10.11.0/24 [10] is directly connected, eth1, Area 0.0.0.0
O 10.10.11.100/32 [10] is directly connected, lo, Area 0.0.0.0
E2 10.15.0.0/24 [10/50] via 10.10.0.1, eth0
IA 172.16.10.0/24 [30] via 10.10.11.50, eth1, Area 0.0.0.0
E2 192.168.0.0/16 [10/20] via 10.10.11.50, eth1
```

show ip ospf virtual-links

使用 **show ip ospf virtual-links** 命令显示 OSPF 虚链路信息。

命令

show ip ospf [*process_id*] **virtual-links**

语法

process_id	OSPF 进程 ID，格式为 INTEGER<1-8>。

说明

如果不指定 *process_id* 参数，则显示所有 OSPF 路由进程的虚链路信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#show ip ospf virtual-links
```

【返回结果】

```
Virtual Link VLINK0 to router 10.10.0.9 is up
Transit area 0.0.0.1 via interface eth0
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Adjacency state Full
Virtual Link VLINK1 to router 10.10.0.123 is down
Transit area 0.0.0.1 via interface *
Transmit Delay is 1 sec, State Down,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in inactive
Adjacency state Down
```

show ip protocols

使用 **show ip protocols** 命令显示 OSPF 进程参数和统计数据。

命令

show ip protocols

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 普通配置模式下使用。

范例

```
neteye-ospfd#show ip protocols
```

【返回结果】

```
Routing Protocol is "ospf 8"
Invalid after 0 seconds, hold down 0, flushed after 0
Outgoing update filter list for all interfaces is
Incoming update filter list for all interfaces is
Routing for Networks:
192.30.30.0/24
192.40.40.0/24
Routing Information Sources:
Gateway Distance Last Update
Distance: (default is 110)
Address Mask Distance List
```

show ospf state

使用 **show ospf state** 命令显示是否启用了 OSPF 功能。

命令

show ospf state

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在普通配置模式下使用。

范例

范例 . 显示是否启用了 OSPF 功能。

```
NetEye@root>show ospf state
```

【返回结果】

```
OSPF is On
```

相关命令

命令名称	描述信息
ospf enable, disable	启用或禁用 OSPF 功能。

summary-address

使用 **summary-address** 命令根据指定的地址范围对路由进行汇总或抑制。

命令

summary-address *ip_prefix* [**not-advertise** | **tag** *tag_value*]

语法

ip_prefix	IP 地址范围，格式为 A.B.C.D/M。
not-advertise	表示抑制外部路由。
tag_value	标记值，格式为 INTEGER<0-4294967295>。 缺省值为 0

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#summary-address 172.16.0.0/16 tag 3
```

timers spf exp

使用 **timers spf exp** 命令使用指数后退延迟设置路由计时器。

使用 **no** 关键字取消该设置。

命令

timers spf exp *min_hold_time max_hold_time*

no timers spf exp

语法

min_hold_time	设置接收改变和启动 SPF 计算之间的最小延迟时间，单位为毫秒，格式为 INTEGER<0-2147483647>。 缺省值为 5
max_hold_time	设置接收改变和启动 SPF 计算之间的最大延迟时间，单位为秒，格式为 INTEGER<0-2147483647>。 缺省值为 10

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 OSPF 路由配置模式下使用。

范例

```
neteye-ospfd#configure terminal
neteye-ospfd(config)#router ospf 8
neteye-ospfd(config-router)#timers spf exp 5 10
```

RIP

cisco-metric-behavior

使用 **cisco-metric-behavior** 命令启用或禁用与 Cisco 一致的 Metric 更新功能。

命令

cisco-metric-behavior {**enable** | **disable**}

no cisco-metric-behavior

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 路由配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#router rip
neteye-ripd(config-router)#cisco-metric-behavior enable
```

clear ip rip route

使用 **clear ip rip route** 命令从 RIP 路由表中删除指定路由协议的路由条目。

命令

clear ip rip route {*ip_prefix* | **static** | **connected** | **rip** | **ospf** | **bgp** | **all**}

语法

ip_prefix	IP 地址范围，格式为 A.B.C.D/M。表示从 RIP 路由表中删除与此目的地址精确匹配的路由条目。
static	表示从 RIP 路由表中删除静态路由条目。
connected	表示从 RIP 路由表中删除直连路由条目。
rip	表示从 RIP 路由表中删除 RIP 路由条目。
ospf	表示从 RIP 路由表中删除 OSPF 路由条目。
bgp	表示从 RIP 路由表中删除 BGP 路由条目。
all	表示从 RIP 路由表中删除所有路由条目。

说明

指定 all 关键字表示删除 RIP 路由表中的所有信息。如果要保留 RIP 网络，则需使用 **redistribute connected** 命令将 RIP 网络设置成直连路由。指定 rip 关键字可删除从邻居学到的 RIP 路由并使 RIP 网络处于非活动状态。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 普通配置模式下使用。

范例

```
neteye-ripd#clear ip rip route 10.0.0.0/8
neteye-ripd#clear ip rip route ospf
```

debug rip events, nsm, packet

使用 **debug rip events, nsm, packet** 命令显示 RIP 事件、RIP 数据包和 RIP NSM 的 Debug 信息。

使用 **no** 关键字取消该设置。

命令

[**no**] **debug rip** {**events** | **nsm** | **packet** {**recv** | **send**} [**detail**]}

语法

events	显示 RIP 事件的 Debug 信息。
nsm	显示 RIP 数据包和 RIP NSM 的 Debug 信息。
packet {**recv**	**send**}	• packet recv — 显示接收数据包的 Debug 信息 • packet send — 显示发送数据包的 Debug 信息
detail	显示发送或接收数据包的详细信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 普通配置模式下使用。

范例

```
neteye-ripd#debug rip packet
```

相关命令

命令名称	描述信息
show debugging rip	显示 RIP 的 Debug 配置信息。

default-information originate

使用 **default-information originate** 命令向 RIP 路由进程中添加一条缺省路由。

使用 **no** 关键字取消该设置。

命令

[**no**] **default-information originate**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 路由配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#router rip
neteye-ripd(config-router)#default-information originate
```

default-metric

使用 **default-metric** 命令设置重发布进入 RIP 路由进程的外部路由缺省 Metric 值。使用 **no** 关键字取消该设置。

命令

default-metric *metric*

no default-metric

语法

metric	Metric 值，格式为 INTEGER<1-16>。

说明

将本条命令与 **redistribute** 命令一起使用使所有重发布的路由的路由协议都使用指定的 Metric 值。缺省 Metric 值对于重发布具有非兼容 Metric 值的路由是非常有用的。协议之间的 Metric 值是不同的，所以不能够直接进行对比。缺省 Metric 值提供了对比的标准。所有重发布的路由都会使用缺省 Metric 值。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 路由配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#router rip
neteye-ripd(config-router)#default-metric 10
```

distance

使用 **distance** 命令设置 RIP 路由的管理距离。
使用 **no** 关键字取消该设置。

命令

[**no**] **distance** *distance_value* [*prefix_list* [*access_list*]]

语法

distance_value	管理距离，格式为 INTEGER<1-255>。 缺省值为 120
prefix_list	前缀列表名称，格式为 WORD。
access_list	访问列表名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 路由配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#router rip
neteye-ripd(config-router)#distance 8 10.0.0.0/8 mylist
```

distribute-list

使用 **distribute-list** 命令根据访问列表或前缀列表过滤流入或流出路由更新信息。使用 **no** 关键字取消该设置。

命令

[**no**] **distribute-list** {*access_list* | **prefix** *prefix_list*} {**in** | **out**} [*interface_name*]

语法

access_list	访问列表名称，格式为 WORD。
prefix_list	前缀列表名称，格式为 WORD。
in | **out**	• in — 过滤流入的路由更新信息 • out — 过滤流出的路由更新信息
interface_name	接口名称，格式为 WORD<3-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 路由配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#router rip
neteye-ripd(config-router)#distribute-list prefix myfilter in eth1
```

ip rip authentication mode

使用 **ip rip authentication mode** 命令为 RIP 版本 2 数据包指定认证方式。使用 **no** 关键字取消该设置。

命令

ip rip authentication mode {**md5** | **text**}

no ip rip authentication mode

语法

md5 | **text**	• md5 — 使用 MD5 密钥认证算法 • text — 指定认证方式为明文或使用简单用户口令认证

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 接口配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#interface eth1
neteye-ripd(config-if)#ip rip authentication mode md5
```

相关命令

命令名称	描述信息
ip rip authentication string	为认证密钥指定一个字符串或密码。

ip rip authentication string

使用 **ip rip authentication string** 命令为认证密钥指定一个字符串或密码。使用 **no** 关键字取消该设置。

命令

ip rip authentication string *line*

no ip rip authentication string

语法

line	认证密钥字符串或密码，格式为 LINE。

说明

使用该命令可为指定接口上的单个密钥设置密码。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 接口配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#interface eth1
neteye-ripd(config-if)#ip rip authentication string guest
```

相关命令

命令名称	描述信息
ip rip authentication mode	为 RIP 版本 2 数据包指定认证方式。

ip rip receive version

使用 **ip rip receive version** 命令在设置接口上接收指定版本类型的 RIP 数据包，并覆盖 **version** 命令所进行的设置。

使用 **no** 关键字取消该设置。

命令

ip rip receive version {**1** | **2**}

no ip rip receive version

语法

1	**2**	• 1 — 表示在指定接口上接收 RIP 版本 1 的数据包 • 2 — 表示在指定接口上接收 RIP 版本 2 的数据包 缺省设置为 2

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 接口配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#interface eth1
neteye-ripd(config-if)#ip rip receive version 2
```

相关命令

命令名称	描述信息
version	指定一个全局 RIP 版本。

ip rip receive-packet

使用 **ip rip receive-packet** 命令为接口配置接收 RIP 数据包功能。
使用 **no** 关键字取消该设置。

命令

[**no**] **ip rip receive-packet**

说明

缺省状态为启用接收数据包功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 接口配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#interface eth1
neteye-ripd(config-if)#ip rip receive-packet
```

相关命令

命令名称	描述信息
ip rip send-packet	为接口配置发送 RIP 数据包功能。

ip rip send version

使用 **ip rip send version** 命令设置在接口上发送指定版本类型的 RIP 数据包。使用 **no** 关键字取消该设置。

命令

ip rip send version {**1** | **2**}

no ip rip send version

语法

1	**2**	• 1 — 表示在指定接口上发送 RIP 版本 1 的数据包 • 2 — 表示在指定接口上发送 RIP 版本 2 的数据包 缺省设置为 2

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 接口配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#interface eth1
neteye-ripd(config-if)#ip rip send version 2
```

相关命令

命令名称	描述信息
version	指定一个全局 RIP 版本。

ip rip send version 1-compatible

使用 **ip rip send version 1-compatible** 命令允许 RIP 版本 2 的接口发送兼容 RIP 版本 1 的数据包，此时 RIP 数据包将使用广播方式代替多播。

使用 **no** 关键字取消该设置。

命令

[**no**] **ip rip send version 1-compatible**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 接口配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#interface eth1
neteye-ripd(config-if)#ip rip send version 1-compatible
```

ip rip send-packet

使用 **ip rip send-packet** 命令为接口配置发送 RIP 数据包功能。
使用 **no** 关键字取消该设置。

命令

[**no**] **ip rip send-packet**

说明

缺省状态为启用发送数据包功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 接口配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#interface eth1
neteye-ripd(config-if)#ip rip send-packet
```

相关命令

命令名称	描述信息
ip rip receive-packet	为接口配置接收 RIP 数据包功能。

ip rip split-horizon

使用 **ip rip split-horizon** 命令启用接口水平分割功能。缺省为启用毒性水平分割。

使用 **no** 关键字取消该设置。

命令

[**no**] **ip rip split-horizon** [**poisoned**]

语法

poisoned	进行带毒性逆转的水平分割。

说明

使用该命令可避免将路由更新中包含的从同一网关学到的路由再发回到该网关，并可避免将路由更新中包含的从同一邻接方学到的路由发回到该邻接方。如果指定了 poisoned 关键字，则路由更新信息中可包含上述提到的两种路由，但是要把他们的度量值设为无限大。因此通告这些路由不可达。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 接口配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#interface eth1
neteye-ripd(config-if)#ip rip split-horizon poisoned
```

neighbor

使用 **neighbor** 命令指定 RIP 邻居路由器。
使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** *ip_address*

语法

ip_address	邻居路由器 IP 地址，格式为 X.X.X.X。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 路由配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#router rip
neteye-ripd(config-router)#neighbor 1.1.1.1
```

相关命令

命令名称	描述信息
passive-interface	在指定的接口上禁止广播 RIP 数据包。

network

使用 **network** 命令指定一个运行 RIP 的网络。
使用 **no** 关键字取消该设置。

命令

[**no**] **network** {*ip_prefix* | *interface_name*}

语法

ip_prefix	IP 地址范围，格式为 A.B.C.D/M。
interface_name	接口名称，格式为 WORD<3-15>。

说明

使用该命令指定一个接收 RIP 路由更新信息的网络。如果不指定该网络，网络内的接口将无法获知任何 RIP 路由更新信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 路由配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#router rip
neteye-ripd(config-router)#network 10.0.0.0/8
neteye-ripd(config-router)#network eth1
```

相关命令

命令名称	描述信息
clear ip rip	从 RIP 路由表中删除指定路由协议的路由条目。
show ip rip	显示 RIP 路由表。

offset-list

使用 **offset-list** 命令设置当从接口上发送或接收路由更新时，向匹配指定访问列表的路由条目添加 Metric 值。

使用 **no** 关键字取消该设置。

命令

[**no**] **offset-list** *access_list* {**in | out**} *metric* [*interface_name*]

语法

access_list	访问列表名称，格式为 WORD。
in | out	• in — 表示访问列表将会被流入的发布路由 Metric 值所使用 • out — 表示访问列表将会被流出的发布路由 Metric 值所使用
metric	Metric 值，格式为 INTEGER<1-16>。
interface_name	接口名称，格式为 WORD<3-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 路由配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#router rip
neteye-ripd(config-router)#offset-list accesslist1 in 5 eth1
```

passive-interface

使用 **passive-interface** 命令在指定的接口上禁止广播 RIP 数据包。
使用 **no** 关键字取消该设置。

命令

[**no**] **passive-interface** *interface_name*

语法

interface_name	接口名称，格式为 WORD<3-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 路由配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#router rip
neteye-ripd(config-router)#passive-interface eth1
```

redistribute

使用 **redistribute** 命令将其他协议的路由重发布到 RIP 路由进程中。
使用 **no** 关键字取消该设置。

命令

[**no**] **redistribute** {**connected** | **static** | **ospf** | **bgp**} [[**metric** *metric*] **route-map** *route_map*]

语法

connected | **static** | **ospf** | **bgp**	• connected — 重发布直连路由 • static — 重发布静态路由 • ospf — 重发布 OSPF 路由 • bgp — 重发布 BGP 路由
metric	Metric 值，格式为 INTEGER<1-16>。
route_map_name	Route Map 名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 路由配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#router rip
neteye-ripd(config-router)#redistribute connected route-map ipi
```

rip enable, disable

使用 **rip enable, disable** 命令启用或禁用 RIP 功能。

命令

rip {**enable** | **disable**}

语法

enable	**disable**	• enable— 启用 RIP 功能 • disable— 禁用 RIP 功能

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show rip state	显示是否启用了 RIP 功能。

route

使用 **route** 命令添加静态 RIP 路由。
使用 **no** 关键字取消该设置。

命令

[**no**] **route** *ip_prefix*

语法

ip_prefix	IP 地址范围，格式为 A.B.C.D/M。

说明

使用该命令添加一条静态 RIP 路由。该命令主要用来调试目的，而不适用于内核路由表。如果添加了一条 RIP 路由，则会在 RIP 路由表中校验此路由。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 路由配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#router rip
neteye-ripd(config-router)#route 1.2.3.4/8
```

相关命令

命令名称	描述信息
clear ip rip	从 RIP 路由表中删除指定路由协议的路由条目。
show ip rip	显示 RIP 路由表。

router rip

使用 **router rip** 命令创建 RIP 路由进程并进入 RIP 路由配置模式。
使用 **no** 关键字取消该设置。

命令

[**no**] **router rip**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 全局配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#router rip
neteye-ripd(config-router)#
```

相关命令

命令名称	描述信息
network	指定一个运行 RIP 的网络。
version	指定一个全局 RIP 版本。

show debugging rip

使用 **show debugging rip** 命令显示 RIP 的 Debug 配置信息。

命令

show debugging rip

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 普通配置模式下使用。

范例

```
neteye-ripd#show debugging rip
```

【返回结果】

```
RIP debugging status:
  RIP event debugging is on
  RIP packet detail debugging is on
```

相关命令

命令名称	描述信息
debug rip events, nsm, packet	显示 RIP 事件、 RIP 数据包和 RIP NSM 的 Debug 信息。

show ip protocols rip

使用 **show ip protocols rip** 命令显示 RIP 进程参数和统计信息。

命令

show ip protocols rip

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 普通配置模式下使用。

范例

```
neteye-ripd#show ip protocols rip
```

【返回结果】

```
Routing Protocol is "rip"
Sending updates every 30 seconds with +/-50%, next due in 12 seconds
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
Default redistribution metric is 1
Redistributing: connected static
Default version control: send version 2, receive version 2
Interface Send Recv Key-chain
eth0 2 2
Routing for Networks:
10.10.0.0/24
Routing Information Sources:
Gateway BadPackets BadRoutes Distance Last Update
Distance: (default is 120
```

show ip rip

使用 **show ip rip** 命令显示 RIP 路由表。

命令

show ip rip

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 普通配置模式下使用。

范例

```
neteye-ripd#show ip rip
```

【返回结果】

```
Codes: R - RIP, C - Connected, S - Static, O - OSPF, I - IS-IS,
B - BGP
Network Next Hop Metric From If Time
K 0.0.0.0/0 10.0.1.1 16 eth1 01:58
C 10.0.1.0/24 1 eth1
S 10.10.10.0/24 1 eth0
C 10.10.11.0/24 1 eth0
S 192.168.101.0/24 1 eth0
R 192.192.192.0/24 1 --
```

相关命令

命令名称	描述信息
clear ip rip	从 RIP 路由表中删除指定路由协议的路由条目。
network	指定一个运行 RIP 的网络。
route	添加静态 RIP 路由。

show ip rip database

使用 **show ip rip database** 命令显示 RIP 数据库信息。

命令

show ip rip database

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 普通配置模式下使用。

范例

```
neteye-ripd#show ip rip database
```

【返回结果】

```
Codes: R - RIP, C - Connected, S - Static, O - OSPF, I - IS-IS,
B - BGP
Network Next Hop Metric From If Time
K 0.0.0.0/0 10.0.1.1 16 eth1 01:58
C 10.0.1.0/24 1 eth1
S 10.10.10.0/24 1 eth0
C 10.10.11.0/24 1 eth0
S 192.168.101.0/24 1 eth0
R 192.192.192.0/24 1 --
```

show ip rip interface

使用 **show ip rip interface** 命令显示 RIP 接口信息。可以通过指定接口名称来查看某一特定的接口信息。

命令

show ip rip interface [*interface_name*]

语法

interface_name	接口名称，格式为 WORD<3-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 普通配置模式下使用。

范例

```
neteye-ripd#show ip rip interface
```

【返回结果】

```
lo is up, line protocol is up
RIP is not enabled on this interface
eth0 is up, line protocol is up
RIP is not enabled on this interface
eth1 is down, line protocol is down
RIP is not enabled on this interface
eth2 is up, line protocol is up
Routing Protocol: RIP
Receive RIP packets
Send RIPv1 Compatible
Passive interface: Disabled
Split horizon: Enabled with Poisoned Reversed
IP interface address:
10.10.1.1/24
```

```
10.10.2.1/24
```

show rip state

使用 **show rip state** 命令显示是否启用了 RIP 功能。

命令

show rip state

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在普通配置模式下使用。

范例

范例 . 显示是否启用了 RIP 功能。

```
NetEye@root>show rip state
```

【返回结果】

```
RIP is Off
```

相关命令

命令名称	描述信息
rip enable, disable	启用或禁用 RIP 功能。

timers

使用 **timers** 命令调整路由网络定时器。

使用 **no** 关键字取消该设置。

命令

timers basic *update timeout garbage*

no timers basic

语法

update	路由表的更新时间间隔值，单位为秒，格式为 INTEGER<5-2147483647>。 缺省值为 30
timeout	路由信息的超时时间，单位为秒，格式为 INTEGER<5-2147483647>。如果在指定的超时时间内没有收到路由更新信息，则通知路由无效。 缺省值为 180
garbage	垃圾收集的间隔值，单位为秒，格式为 INTEGER<5-2147483647>。 缺省值为 120

说明

使用该命令调整 RIP 定时参数。每隔 30 秒，各邻接方将会收到包含完整路由表格的更新信息。如果超过指定的超时时间，路由将会无效。但是，该无效路由将会在路由表中保留一小段时间，这样可确保各邻接方收到路由已被丢弃的信息。如果超过垃圾参数规定的超时时间，该路由最终将会从路由表格中删除。如果达到指定的垃圾时间，该路由将会随所有的路由更新信息发送出去。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 路由配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#router rip
neteye-ripd(config-router)#timers basic 30 180 120
```

version

使用 **version** 命令指定一个全局 RIP 版本。

使用 **no** 关键字取消该设置。

命令

[**no**] **version** {**1** | **2**}

语法

1 | 2	• 1 — 指定 RIP 版本 1 • 2 — 指定 RIP 版本 2 缺省设置为 2

说明

RIP 协议可应用于版本 1 和版本 2 模式。版本 2 较版本 1 具有更多特性，特别体现在认证方面。如果设置了一种 RIP 版本，那么对应版本类型的数据包将通过所有启用 RIP 协议的接口来收发。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 RIP 路由配置模式下使用。

范例

```
neteye-ripd#configure terminal
neteye-ripd(config)#router rip
neteye-ripd(config-router)#version 1
```

相关命令

命令名称	描述信息
ip rip receive version	在设置接口上接收指定版本类型的 RIP 数据包，并覆盖 **version** 命令所进行的设置。
ip rip send version	设置在接口上发送指定版本类型的 RIP 数据包。

BGP

aggregate-address

使用 **aggregate-address** 命令设置 BGP 路由汇总。

使用 **no** 关键字取消该设置。

命令

[**no**] **aggregate-address** *ip_prefix* [**summary-only**] [**as-set**]

语法

ip_prefix	IP 地址范围，格式为 A.B.C.D/M。
summary-only	表示保留汇总路由，过滤掉详细路由。
as-set	表示生成自治系统集。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#aggregate-address 10.0.0.0/8 summary-only
as-set
```

auto-summary

使用 **auto-summary** 命令设置 BGP speaker 自动向它的对端发送路由汇总。

使用 **no** 关键字取消该设置。

命令

[**no**] **auto-summary**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#auto-summary
```

bgp aggregate-nexthop-check

使用 **bgp aggregate-nexthop-check** 命令设置当进行 BGP 路由汇总时，对下一跳进行检查。

使用 **no** 关键字取消该设置。

命令

[**no**] **bgp aggregate-nexthop-check**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 全局配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#bgp aggregate-nexthop-check
```

bgp always-compare-med

使用 **bgp always-compare-med** 命令允许 BGP 比较来自不同自治系统路由的 MED 状态。

使用 **no** 关键字取消该设置。

命令

[**no**] **bgp always-compare-med**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp always-compare-med
```

相关命令

命令名称	描述信息
bgp bestpath as-path ignore	设置当决定最佳路径时，忽略自治系统路径信息。
bgp bestpath compare-routerid	允许比较同一 eBGP 路径的路由器 ID。
bgp bestpath med	允许比较 MED 属性。
bgp deterministic-med	设置 BGP 使用邻居的 AS 和 MED 分类路径，以保证任何时刻都使用相同的方法分类路径。

bgp bestpath as-path ignore

使用 **bgp bestpath as-path ignore** 命令设置当决定最佳路径时，忽略自治系统路径信息。

使用 **no** 关键字取消该设置。

命令

[no] bgp bestpath as-path ignore

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp bestpath as-path ignore
```

相关命令

命令名称	描述信息
bgp always-compare-med	允许 BGP 比较来自不同自治系统路由的 MED 状态值。
bgp bestpath med	允许比较 MED 属性。
bgp bestpath compare-routerid	允许比较同一 eBGP 路径的路由器 ID。

bgp bestpath compare-confed-aspath

使用 **bgp bestpath compare-confed-aspath** 命令设置允许比较联邦自治系统路径长度。

使用 **no** 关键字取消该设置。

命令

[**no**] **bgp bestpath compare-confed-aspath**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp bestpath compare-confed-aspath
```

相关命令

命令名称	描述信息
bgp bestpath as-path ignore	设置当决定最佳路径时，忽略自治系统路径信息。

bgp bestpath compare-routerid

使用 **bgp bestpath compare-routerid** 命令允许比较同一 eBGP 路径的路由器 ID。

使用 **no** 关键字取消该设置。

命令

[**no**] **bgp bestpath compare-routerid**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

说明

缺省情况下，当 BGP 从 eBGP 对端接收到相同的 eBGP 路径时，选择接收到的第一条路由作为最佳路径。

模式

该命令在 BGP 路由配置模式下使用。

范例

```
eteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp bestpath compare-routerid
```

相关命令

命令名称	描述信息
show ip bgp	显示 BGP 网络信息。
show ip bgp neighbors	显示 BGP 邻居 TCP 连接的详细信息。

bgp bestpath med

使用 **bgp bestpath med** 命令允许比较 MED 属性。

命令

bgp bestpath med confed [**missing-as-worst**]

bgp bestpath med missing-as-worst [**confed**]

语法

confed	表示在联邦路径中比较 MED。
missing-as-worst	表示不将缺失 MED 作为选择标准。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp bestpath med missing-as-worst
```

相关命令

命令名称	描述信息
bgp always-compare-med	允许 BGP 比较来自不同自治系统路由的 MED 状态。
bgp bestpath as-path ignore	设置当决定最佳路径时，忽略自治系统路径信息。
bgp deterministic-med	设置 BGP 使用邻居的 AS 和 MED 分类路径，以保证任何时刻都使用相同的方法分类路径。

bgp bestpath med remove-recv-med

使用 **bgp bestpath med remove-recv-med** 命令删除所有入向路由的 MED。使用 **no** 关键字取消该设置。

命令

[no] bgp bestpath med remove-recv-med

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp bestpath med remove-recv-med
```

bgp bestpath med remove-send-med

使用 **bgp bestpath med remove-send-med** 命令删除所有出向路由的 MED。使用 **no** 关键字取消该设置。

命令

[**no**] **bgp bestpath med remove-send-med**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp bestpath med remove-send-med
```

bgp client-to-client reflection

使用 **bgp client-to-client reflection** 命令保存从 BGP 路由反射器发送至客户端的路由反射信息。

使用 **no** 关键字取消该设置。

命令

[**no**] **bgp client-to-client reflection**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#no bgp client-to-client reflection
```

相关命令

命令名称	描述信息
bgp cluster-id	设置 BGP 路由反射器的集群 ID。
neighbor route-reflector-client	将 NetEye 设置为一个 BGP 路由反射器，并将指定的邻居配置为它的客户端。
show ip bgp	显示 BGP 网络信息。

bgp cluster-id

使用 **bgp cluster-id** 命令设置 BGP 路由反射器的集群 ID。

使用 **no** 关键字取消该设置。

命令

bgp cluster-id *cluster_id*

no cluster-id

语法

cluster_id	路由反射器的集群 ID，格式为 X.X.X.X 或 INTEGER<1-4294967295>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp cluster-id 1.1.1.1
```

相关命令

命令名称	描述信息
bgp client-to-client reflection	保存从 BGP 路由反射器发送至客户端的路由反射信息。
neighbor route-reflector-client	将 NetEye 设置为一个 BGP 路由反射器，并将指定的邻居配置为它的客户端。
show ip bgp	显示 BGP 网络信息。

bgp confederation identifier

使用 **bgp confederation identifier** 命令建立 BGP 联邦，并指定联邦自治系统号。

使用 **no** 关键字取消该设置。

命令

bgp confederation identifier *as_number*

no bgp confederation identifier

语法

as_number	自治系统号，格式为 INTEGER<1-65535>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp confederation identifier 1
```

相关命令

命令名称	描述信息
bgp confederation peers	设置属于联邦的子自治系统号。

bgp confederation peers

使用 **bgp confederation peers** 命令设置属于联邦的子自治系统号。

使用 **no** 关键字取消该设置。

命令

bgp confederation peers *as_number*

no bgp confederation peers

语法

as_number	自治系统号，格式为 INTEGER<1-65535>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp confederation peers 1234
```

相关命令

命令名称	描述信息
bgp confederation identifier	建立 BGP 联邦，并指定联邦自治系统号。

bgp config-type

使用 **bgp config-type** 命令设置 BGP 配置类型。

命令

bgp config-type {**standard | zebos**}

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 全局配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#bgp config-type standard
```

bgp dampening

使用 **bgp dampening** 命令设置 BGP 抑制参数，用以防止路由频繁抖动。

使用 **no** 关键字取消该设置。

命令

[**no**] **bgp dampening** [*reachtime* [*reuse suppress maxsuppress* [*unreachtime*]]| **route-map** *route_map_name*]

语法

reachtime	可达性半衰期，单位为分钟，格式为 INTEGER<1-45>。表示惩罚值减少到当前值的一半所经历的时间。 缺省值为 15
reuse	重用极限值，格式为 INTEGER<1-20000>。当一条被抑制路由的惩罚值损失到重用极限值之下，该路由将不再受到抑制。 缺省值为 750
suppress	抑制极限值，格式为 INTEGER<1-20000>。当一条路由的惩罚值超过所设置的抑制极限值，该路由就会受到抑制。 缺省值为 2000
maxsuppress	最大抑制时间，单位为分钟，格式为 INTEGER<1-255>。被抑制路由的最大抑制时间。 缺省值为 60
unreachtime	惩罚值的不可达性半衰期，单位为分钟，格式为 INTEGER<1-45>。
route_map_name	Route Map 名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp dampening 20 800 2500 80 25
```

bgp default local-preference

使用 **bgp default local-preference** 命令设置 BGP 默认本地优先级。

使用 **no** 关键字取消该设置。

命令

bgp default local-preference *local_preference*

no bgp default local-preference [*local_preference*]

语法

local_preference	本地优先级，格式为 INTEGER<0-4294967295>。 缺省值为 100

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp default local-preference 2345555
```

bgp deterministic-med

使用 **bgp deterministic-med** 命令设置 BGP 使用邻居的 AS 和 MED 分类路径，以保证任何时刻都使用相同的方法分类路径。

使用 **no** 关键字取消该设置。

命令

[**no**] **bgp deterministic-med**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

说明

如果不指定任何 debug 选项，则开启所有选项的 debug 功能。

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp deterministic-med
```

相关命令

命令名称	描述信息
show ip bgp	显示 BGP 网络信息。
show ip bgp neighbors	显示 BGP 邻居 TCP 连接的详细信息。

bgp enable, disable

使用 **bgp enable, disable** 命令启用或禁用 BGP 功能。

命令

bgp {**enable** | **disable**}

语法

enable | **disable**	• enable— 启用 BGP 功能 • disable— 禁用 BGP 功能

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show bgp state	显示是否启用了 BGP 功能。

bgp enforce-first-as

使用 **bgp enforce-first-as** 命令强制设定发送 BGP 更新的 BGP 邻居的自治系统号必须是自治系统路径列表的第一个，如果不是，这条路由会被禁止。

使用 **no** 关键字取消该设置。

命令

[**no**] **bgp enforce-first-as**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp enforce-first-as
```

bgp extended-asn-cap

使用 **bgp extended-asn-cap** 命令配置一个 BGP 路由器具有发送 4 字节 ASN 能力。使用 **no** 关键字取消该设置。

命令

[**no**] **bgp extended-asn-cap**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 全局配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)# bgp extended-asn-cap
```

bgp fast-external-failover

使用 **bgp fast-external-failover** 命令设置当 BGP 连接使用的接口失效后，立即重置 BGP 连接。

使用 **no** 关键字取消该设置。

命令

[**no**] **bgp fast-external-failover**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp fast-external-failover
```

bgp graceful-restart

使用 **bgp graceful-restart** 命令启用 BGP 优雅重启功能。

使用 **no** 关键字取消该设置。

命令

bgp graceful-restart [**restart-time** *restart_time* | **stalepath-time** *stalepath_time*]

no bgp graceful-restart [**restart-time | stalepath-time**]

语法

restart_time	邻居重启所需的最大时间，单位为秒，格式为 INTEGER<1-3600>。 缺省值为 120
stalepath_time	从重启中的邻居收到的路径信息的保存时间，单位为秒，格式为 INTEGER<1-3600>。 缺省值为 360

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp graceful-restart restart-time 150
```

bgp log-neighbor-changes

使用 **bgp log-neighbor-changes** 命令启用对 BGP 邻居状态改变情况的记录。

使用 **no** 关键字取消该设置。

命令

[**no**] **bgp log-neighbor-changes**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

说明

被记录的事件包括：接收到的 BGP 通知、接收到的错误的 BGP 更新、用户重置请求、对等体超时、对等体关闭会话、接口抖动、路由器 ID 的改变、邻居的删除、加入到对等体组中的成员、管理员人为关闭、远程自治系统的改变、路由反射器客户端配置的修改。

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp log-neighbor-changes
```

bgp multiple-instance

使用 **bgp multiple-instance** 命令启用 BGP 多实例支持。

使用 **no** 关键字取消该设置。

命令

[**no**] **bgp multiple-instance**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 全局配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#bgp multiple-instance
```

bgp rfc1771-path-select

使用 **bgp rfc1771-path-select** 命令兼容 RFC1771 的路径选择方式。

使用 **no** 关键字取消该设置。

命令

[**no**] **bgp rfc1771-path-select**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 全局配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#bgp rfc1771-path-select
```

bgp rfc1771-strict

使用 **bgp rfc1771-strict** 命令严格支持 RFC1771。

使用 **no** 关键字取消该设置。

命令

[no] bgp rfc1771-strict

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 全局配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#bgp rfc1771-strict
```

bgp router-id

使用 **bgp router-id** 命令设置路由器 ID。

使用 **no** 关键字取消该设置。

命令

bgp router-id *router_id*

no bgp router-id [*router_id*]

语法

router_id	路由器 ID，格式为 X.X.X.X。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

说明

如果 loopback 接口已被配置，则路由器 ID 为 loopback 接口的 IP 地址，否则路由器 ID 为最大的 IP 地址。

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp router-id 1.1.2.3
```

bgp scan-time

使用 **bgp scan-time** 命令设置 BGP 路由进行下一跳扫描的时间间隔。

使用 **no** 关键字取消该设置。

命令

bgp scan-time *time*

no bgp scan-time [*time*]

语法

time	时间间隔，单位为秒，格式为 INTEGER<0-60>。 缺省值为 60

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

说明

如果将 *time* 参数设置为 0，则表示禁用下一跳扫描。

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp scan-time 10
```

bgp update-delay

使用 **bgp update-delay** 命令为支持优雅重启功能的路由器设置更新延迟时间。使用 **no** 关键字取消该设置。

命令

bgp update-delay *delay_value*

no bgp update-delay [*delay_value*]

语法

delay_value	更新延迟时间，单位为秒，格式为 INTEGER<1-3600>。 缺省值为 120

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#bgp update-delay 345
```

clear ip bgp *

使用 **clear ip bgp *** 命令重置所有对端的 BGP 连接。

命令

clear ip bgp * [in [prefix-filter] | out | soft [in | out]]

语法

in | out	• in— 表示入方向发布路由将被清除 • out— 表示出方向发布路由将被清除
prefix-filter	表示过滤 ORF 前缀列表，并对入向路由重新进行软配置。
soft [in | out]	• soft — 表示入方向和出方向发布路由都将被软清除 • soft in— 表示入方向发布路由将被软清除 • soft out— 表示出方向发布路由将被软清除

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#clear ip bgp * soft in
```

clear ip bgp

使用 **clear ip bgp** 命令重置指定对端的 BGP 连接。

命令

clear ip bgp {*ip_address* | *as_number*} [**in** [**prefix-filter**] | **out** | **soft** [**in** | **out**]]

语法

ip_address	IP 地址，格式为 X.X.X.X。表示指定 IP 地址的 BGP 路由将被清除。
as_number	自治系统号，格式为 INTEGER<1-4294967295>。
in | out	• in— 表示入方向发布路由将被清除 • out— 表示出方向发布路由将被清除
prefix-filter	表示过滤 ORF 前缀列表，并对入向路由重新进行软配置。
soft [**in | out**]	• soft — 表示入方向和出方向发布路由都将被软清除 • soft in— 表示入方向发布路由将被软清除 • soft out— 表示出方向发布路由将被软清除

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#clear ip bgp 10.10.0.12 soft
neteye-bgpd#clear ip bgp 100
```

clear ip bgp dampening

使用 **clear ip bgp dampening** 命令重置 BGP 路由抑制信息。

命令

clear ip bgp dampening [*ip_address* | *ip_prefix*]

语法

ip_address	IP 地址，格式为 X.X.X.X。
ip_prefix	IP 地址范围，格式为 A.B.C.D/M。

说明

如果不指定 *ip_address* 和 *ip_prefix* 参数，则重置所有 BGP 路由抑制信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#clear ip bgp dampening 10.10.0.121
```

clear ip bgp external

使用 **clear ip bgp external** 命令重置所有外部对等体的 BGP 连接。

命令

clear ip bgp external [**in** [**prefix-filter**] | **out** | **soft** [**in** | **out**]]

语法

in | out	• in— 表示入方向发布路由将被清除 • out— 表示出方向发布路由将被清除
prefix-filter	表示过滤 ORF 前缀列表，并对入向路由重新进行软配置。
soft [**in | out**]	• soft — 表示入方向和出方向发布路由都将被软清除 • soft in— 表示入方向发布路由将被软清除 • soft out— 表示出方向发布路由将被软清除

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#clear ip bgp external out
```

clear ip bgp flap-statistics

使用 **clear ip bgp flap-statistics** 命令清除地址族中包含的所有前缀的抖动次数及历史持续时间。

命令

clear ip bgp flap-statistics [*ip_address* | *ip_prefix*]

语法

ip_address	IP 地址，格式为 X.X.X.X。
ip_prefix	IP 地址范围，格式为 A.B.C.D/M。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#clear ip bgp flap-statistics 10.10.0.121
```

clear ip bgp peer-group

使用 **clear ip bgp peer-group** 命令重置对等体组中所有成员的 BGP 连接。

命令

clear ip bgp peer-group *group_name* [**in** [**prefix-filter**] | **out** | **soft** [**in** | **out**]]

语法

group_name	对等体组名称，格式为 WORD。
in | out	• in— 表示入方向发布路由将被清除 • out— 表示出方向发布路由将被清除
prefix-filter	表示过滤 ORF 前缀列表，并对入向路由重新进行软配置。
soft [**in | out**]	• soft — 表示入方向和出方向发布路由都将被软清除 • soft in— 表示入方向发布路由将被软清除 • soft out— 表示出方向发布路由将被软清除

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#clear ip bgp peer-group Peer1 out
```

clear ip bgp view

使用 **clear ip bgp view** 命令重置一个指定 BGP 实例的 BGP 连接。

命令

clear ip bgp view *view_name* ***** [**in** [**prefix-filter**] | **soft** [**in** | **out**]]

语法

view_name	view 名称，格式为 WORD。
in	表示入方向发布路由将被清除
prefix-filter	表示过滤 ORF 前缀列表，并对入向路由重新进行软配置。
soft [**in**	**out**]	• soft — 表示入方向和出方向发布路由都将被软清除 • soft in— 表示入方向发布路由将被软清除 • soft out— 表示出方向发布路由将被软清除

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#clear ip bgp view I4 * in prefix-filter
```

debug bgp

使用 **debug bgp** 命令开启 BGP 的 debug 功能。

使用 **no** 关键字取消该设置。

命令

[**no**] **debug bgp** [**all** | **dampening** | **events** | **filters** | **fsm** | **keepalives** | **mpls** | **nsm** | **update** [**in** | **out**]]

语法

all	指定 BGP 所有 debug 选项。
dampening	指定 BGP 抑制 debug。
events	指定 BGP 事件 debug。
filters	指定 BGP 过滤 debug。
fsm	指定 BGP 有限状态机 debug。
keepalives	指定 BGP keepalive debug。
mpls	指定 BGP 多协议标签交换 debug。
nsm	指定 BGP 网络服务单元 debug。
update [**in** | **out**]	• update —指定 BGP 入向和出向更新 debug • update in—指定 BGP 入向更新 debug • update out—指定 BGP 出向更新 debug

说明

如果不指定任何 debug 选项，则开启 BGP 的普通 debug 功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#debug bgp
neteye-bgpd#debug bgp events
```

distance

使用 **distance** 命令设置管理距离。

使用 **no** 关键字取消该设置。

命令

[**no**] **distance** {*admin_distance ip_prefix* [*access_list_name*] | **bgp** *external_admin_distance internal_admin_distance local_admin_distance*}

语法

admin_distance	BGP 管理距离，格式为 INTEGER<1-255>。
ip_prefix	IP 地址范围，格式为 A.B.C.D/M。
access_list_name	访问列表名称，格式为 WORD。
external_admin_distance	BGP 外部管理距离，格式为 INTEGER<1-255>。 缺省值为 20
internal_admin_distance	BGP 内部管理距离，格式为 INTEGER<1-255>。 缺省值为 200
local_admin_distance	BGP 本地管理距离，格式为 INTEGER<1-255>。 缺省值为 200

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#distance 34 10.10.0.0/24 mylist
```

ip as-path access-list

使用 **ip as-path access-list** 命令设置自治系统路径访问列表。

使用 **no** 关键字取消该设置。

命令

[**no**] **ip as-path access-list** *list_name* {**deny | permit**} *line*

语法

list_name	访问列表名称，格式为 WORD。
deny | permit	• deny —拒绝访问 • permit—允许访问
line	匹配自治系统路径的正则表达式。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 全局配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#ip as-path access-list mylist deny ^65535$
```

ip community-list

使用 **ip community-list** 命令设置团体列表条目。

使用 **no** 关键字取消该设置。

命令

[no] ip community-list *list_name* {**deny | permit**} [**AS:VAL | internet | local-AS | no-advertise | no-export**]

语法

list_name	团体列表名称，格式为 WORD。
**deny	permit**	• deny —拒绝访问 • permit—允许访问
**AS:VAL	internet	local-AS	no-advertise	no-export**	• AS:VAL —指定团体号的有效值 • internet —指定的路由不被发布到 internet • local-AS —指定的路由不被发布到外部 BGP 对等体 • no-advertise —指定的路由不被发布到其他 BGP 对等体 • no-export —指定的路由不被发布到自治系统边界外

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 全局配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#
```

ip community-list expanded

使用 **ip community-list expanded** 命令设置扩展团体列表条目。

使用 **no** 关键字取消该设置。

命令

[**no**] **ip community-list** {**expanded** *list_name*| *list_num*} {**deny | permit**} *line*

语法

list_name	扩展团体列表名称，格式为 WORD。
list_num	扩展团体列表编号，格式为 INTEGER<100-199>。
deny | permit	• deny —拒绝访问 • permit—允许访问
line	匹配扩展团体的正则表达式。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 全局配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#ip community-list expanded mylist deny ^65535$
```

ip community-list standard

使用 **ip community-list standard** 命令设置标准团体列表条目。

使用 **no** 关键字取消该设置。

命令

[no] ip community-list {standard *list_name*| *list_num*} {**deny | permit**} [**AS:VAL | internet | local-AS | no-advertise | no-export**]

语法

list_name	标准团体列表名称，格式为 WORD。
list_num	标准团体列表编号，格式为 INTEGER<1-99>。
**deny	permit**	• deny —拒绝访问 • permit—允许访问
**AS:VAL	internet	local-AS	no-advertise	no-export**	• AS:VAL —指定团体号的有效值 • internet —指定的路由不被发布到 internet • local-AS —指定的路由不被发布到外部 BGP 对等体 • no-advertise —指定的路由不被发布到其他 BGP 对等体 • no-export —指定的路由不被发布到自治系统边界外

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 全局配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#ip community-list standard mylist deny ^65535$
```

ip extcommunity-list expanded

使用 **ip extcommunity-list expanded** 命令创建扩展的扩展团体列表。

使用 **no** 关键字取消该设置。

命令

ip extcommunity-list {**expanded** *list_name* | *list_num*} {**deny** | **permit**} *line*

no ip extcommunity-list {**expanded** *list_name* | *list_num*} [{**deny** | **permit**} *line*]

语法

list_name	扩展的扩展团体列表名称，格式为 WORD。
list_num	扩展的扩展团体列表编号，格式为 INTEGER<100-199>。
deny | permit	• deny —拒绝访问 • permit—允许访问
line	匹配扩展团体的正则表达式。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 全局配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#ip extcommunity-list expanded CLIST permit .*
```

ip extcommunity-list standard

使用 **ip extcommunity-list standard** 命令创建标准的扩展团体列表。

使用 **no** 关键字取消该设置。

命令

ip extcommunity-list {**standard** *list_name* **|** *list_num*} {**deny** | **permit**} **AA:NN**

no ip extcommunity-list {**standard** *list_name* **|** *list_num*} [{**deny** | **permit**} **AA:NN**]

语法

list_name	标准的扩展团体列表名称，格式为 WORD。
list_num	标准的扩展团体列表编号，格式为 INTEGER<1-99>。
deny | permit	• deny —拒绝访问 • permit—允许访问
AA:NN	指定团体号的有效值。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 全局配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#ip extcommunity-list standard CLIST permit 7645:70
```

neighbor

使用 **neighbor** 命令添加一个对等体组。
使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** *group_name* **peer-group**

语法

group_name	对等体组名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor group1 peer-group
```

相关命令

命令名称	描述信息
neighbor peer-group	向对等体组中添加一个邻居。

neighbor activate

使用 **neighbor activate** 命令启用指定 AF 路由和邻居路由的交换。
使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **activate**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 1.2.3.4 activate
```

相关命令

命令名称	描述信息
neighbor remote-as	与 BGP 邻居建立一条 iBGP 或 eBGP 的 TCP 连接。

neighbor advertisement-interval

使用 **neighbor advertisement-interval** 命令设置发送 BGP 路由更新的最小时间间隔。

使用 **no** 关键字取消该设置。

命令

neighbor {*neighbor_id* | *group_name*} **advertisement-interval** *time_interval*

no neighbor {*neighbor_id* | *group_name*} **advertisement-interval** [*time_interval*]

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。
time_interval	时间间隔，单位为秒，格式为 INTEGER<0-600>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.0.3 advertisement-interval 45
```

neighbor attribute-unchanged

使用 **neighbor attribute-unchanged** 命令将无变化的 BGP 属性发布给指定的邻居。

使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **attribute-unchanged** [**as-path**] [**next-hop**] [**med**]

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。
as-path	表示将无变化的自治系统路径属性发布给指定的邻居。
next-hop	表示将无变化的下一跳属性发布给指定的邻居。
med	表示将无变化的 MED 属性发布给指定的邻居。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.0.75 attribute-unchanged
as-path med
```

neighbor capability dynamic

使用 **neighbor capability dynamic** 命令允许 BGP speaker 以无中断方式向对端发布或撤销地址族能力。

使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **capability dynamic**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.10.1 capability dynamic
```

neighbor capability graceful-restart

使用 **neighbor capability graceful-restart** 命令向邻居发布 NetEye 具有优雅重启的功能。

命令

neighbor {*neighbor_id* | *group_name*} **capability graceful-restart**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.10.50 capability graceful-restart
```

相关命令

命令名称	描述信息
bgp graceful-restart	启用 BGP 优雅重启功能。

neighbor capability orf prefix-list

使用 **neighbor capability orf prefix-list** 命令向邻居发布 NetEye 具有外向路由过滤 （ORF）功能。

使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **capability orf prefix-list** {**receive** | **send** | **both**}

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。
receive | **send** | **both**	• receive—表示本地路由器能够从对端接收 ORF 条目。 • send—表示本地路由器能够发送 ORF 条目到对端。 • both—表示本地路由器即能发送 ORF 条目到对端，又能从对端接收 ORF 条目。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.0.5 capability orf
prefix-list both
```

neighbor capability route-refresh

使用 **neighbor capability route-refresh** 命令向邻居发布 NetEye 具有路由刷新功能。

使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **capability route-refresh**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.10.1 capability route-refresh
```

neighbor collide-established

使用 **neighbor collide-established** 命令向邻居发布 NetEye 具有 BGP 连接冲突解决机制。

使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **collide-established**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 3.3.3.3 collide-established
```

neighbor connection-retry-time

使用 **neighbor connection-retry-time** 命令设置指定邻居的连接重试时间。使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **connection-retry-time** *retry_time*

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。
retry_time	连接重试时间，单位为秒，格式为 INTEGER<1-65535>。 缺省值为 120

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.10.10 connection-retry-time
125
```

neighbor default-originate

使用 **neighbor default-originate** 命令允许 BGP 本地路由向邻居发送默认路由 0.0.0.0。

使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **default-originate** [**route-map** *route_map_name*]

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。
route_map_name	Route Map 名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.10.1 default-originate
route-map myroute
```

neighbor description

使用 **neighbor description** 命令添加 BGP 邻居的备注信息。
使用 **no** 关键字取消该设置。

命令

neighbor {*neighbor_id* | *group_name*} **description** *string*

no neighbor {*neighbor_id* | *group_name*} **description** [*string*]

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。
string	备注信息，格式为 LINE。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 1.2.3.4 description Backup router for sales
```

neighbor disallow-infinite-holdtime

使用 **neighbor disallow-infinite-holdtime** 命令禁止配置无限的协商时间。使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** *neighbor_id* **disallow-infinite-holdtime**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.11.4.26 disallow-infinite-holdtime
```

neighbor distribute-list

使用 **neighbor distribute-list** 命令过滤指定 BGP 邻居的路由更新。
使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **distribute-list** *access_list_name* {**in** | **out**}

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。
access_list_name	IP 访问列表名称，格式为 WORD。
in | **out**	• in—表示入向发布路由将被过滤 • out—表示出向发布路由将被过滤

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 1.2.3.4 distribute-list mylist out
```

neighbor dont-capability-negotiate

使用 **neighbor dont-capability-negotiate** 命令禁止与指定的 BGP 邻居进行 BGP 协商。

使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **dont-capability-negotiate**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.0.34 dont-capability-negotiate
```

neighbor ebgp-multihop

使用 **neighbor ebgp-multihop** 命令接受并尝试对在间接网络的外部对端进行ＢＧＰ连接。

使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **ebgp-multihop** [*count*]

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。
count	最大跳数，格式为 INTEGER<1-255>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.10.34 remote-as 20
neteye-bgpd(config-router)#neighbor 10.10.10.34 ebgp-multihop 5
```

neighbor enforce-multihop

使用 **neighbor enforce-multihop** 命令强制 eBGP 邻居进行多跳。
使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **enforce-multihop**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.10.34 remote-as 20
neteye-bgpd(config-router)#neighbor 10.10.10.34 enforce-multihop
```

neighbor filter-list

使用 **neighbor filter-list** 命令过滤指定 BGP 邻居的路由更新。
使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **filter-list** *access_list_name* {**in** | **out**}

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。
access_list_name	自治系统路径访问列表名称，格式为 WORD。
in | **out**	• in—表示入向发布路由将被过滤 • out—表示出向发布路由将被过滤

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.0.34 filter-list mylist out
```

neighbor maximum-prefix

使用 **neighbor maximum-prefix** 命令限制从指定的 BGP 邻居获得前缀的数目。使用 **no** 关键字取消该设置。

命令

neighbor {*neighbor_id* | *group_name*} **maximum-prefix** *max_prefix* [*threshold*] [**warning-only**]

no neighbor {*neighbor_id* | *group_name*} **maximum-prefix** [*max_prefix* [**warning-only**]]

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。
max_prefix	最大前缀的数量，格式为 INTEGER<1-4294967295>。
threshold	阈值，格式为 INTEGER<1-100>。
warning-only	表示当超出限制时，只发送一条警告信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.0.72 maximum-prefix 1244
warning-only
```

neighbor next-hop-self

使用 **neighbor next-hop-self** 命令允许 NetEye 改变发送给 iBGP 对等体的下一跳信息，把下一跳信息设置为与这个邻居进行通信的接口的 IP 地址。

使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **next-hop-self**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.0.72 remote-as 100
neteye-bgpd(config-router)#neighbor 10.10.0.72 next-hop-self
```

neighbor override-capability

使用 **neighbor override-capability** 命令覆盖与 BGP 邻居进行 BGP 协商的结果。

使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **override-capability**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.10.10 override-capability
```

neighbor passive

使用 **neighbor passive** 命令设置一个 BGP 邻居为 passive 模式。
使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **passive**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.10.10 passive
```

neighbor peer-group

使用 **neighbor peer-group** 命令向对等体组中添加一个邻居。
使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** *neighbor_id* **peer-group** *group_name*

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor group1 peer-group
neteye-bgpd(config-router)#neighbor 10.10.0.63 peer-group group1
```

相关命令

命令名称	描述信息
neighbor	添加一个对等体组。

neighbor prefix-list

使用 **neighbor prefix-list** 命令设置通过前缀列表向邻居发布路由更新。使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **prefix-list** *list_name* {**in** | **out**}

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。
list_name	列表名称，格式为 WORD。
in | **out**	• in—表示入向发布路由将被过滤 • out—表示出向发布路由将被过滤

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.10.10 prefix-list list1 in
```

neighbor remote-as

使用 **neighbor remote-as** 命令与 BGP 邻居建立一条 iBGP 或 eBGP 的 TCP 连接。使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **remote-as** *as_number*

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。
as_number	邻居的自治系统号，格式为 INTEGER<1-65535>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.0.73 remote-as 345
```

neighbor remove-private-AS

使用 **neighbor remove-private-AS** 命令从出站更新中移除私有自治系统号。

使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **remove-private-AS**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。

说明

私有自治系统号范围为 64512-65535。私有自治系统号不发布到网络中。此命令只应用于 eBGP 对等体。只有当更新中只有私有自治域号时， BGP 才会移除他们；如果更新中即有私有自治域号，又有公共自治域号，则系统认为配置错误。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.0.63 remove-private-AS
```

neighbor restart-time

使用 **neighbor restart-time** 命令设置指定 BGP 邻居的重启时间，此命令会覆盖 **bgp graceful-restart** 命令的设置。

使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **restart-time** *time*

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。
time	重启时间，单位为秒，格式为 INTEGER<1-3600>。 缺省值为 120

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 3.3.3.3 restart-time 45
```

相关命令

命令名称	描述信息
bgp graceful-restart	启用 BGP 优雅重启功能。

neighbor route-map

使用 **neighbor route-map** 命令在入向或出向路由上应用 Route Map。
使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **route-map** *route_map_name* {**in** | **out**}

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。
route_map_name	Route Map 名称，格式为 WORD。
in	**out**	• in—表示 Route Map 应用于入向发布 • out—表示 Route Map 应用于出向发布

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.10.10 route-map rmap2 in
```

neighbor route-reflector-client

使用 **neighbor route-reflector-client** 命令将 NetEye 设置为一个 BGP 路由反射器，并将指定的邻居配置为它的客户端。

使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **route-reflector-client**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.0.72 route-reflector-client
```

neighbor send-community

使用 **neighbor send-community** 命令将团体属性发布给指定的 BGP 邻居。
使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **send-community** [**both** | **extended** | **standard**]

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。
both | **extended** | **standard**	• both—发布标准和扩展团体属性 • extended—发布扩展团体属性 • standard—发布标准土体属性

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.0.72 send-community
```

neighbor shutdown

使用 **neighbor shutdown** 命令禁用指定的 BGP 邻居。
使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **shutdown**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.0.72 shutdown
```

neighbor soft-reconfiguration inbound

使用 **neighbor soft-reconfiguration inbound** 命令开始存储更新，而不必考虑所应用的路由策略。

使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **soft-reconfiguration inbound**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。

说明

使用该命令存储入向软配置的更新信息。软配置可以用来代替 BGP 路由刷新能力。使用该命令启用本地存储介质来储存所有接收到的路由信息及路由属性信息。这要求有更大的内存。当对一个邻接方进行了软重置 （入向），则会根据入向策略对本地存储的路由信息进行重新处理。但是与 BGP 邻接方的连接不会受到影响。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.10.10 soft-reconfiguration inbound
```

neighbor strict-capability-match

使用 **neighbor strict-capability-match** 命令设置如果能力值和对等体不完全匹配时，则断开 BGP 连接。

使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **strict-capability-match**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.10.10 strict-capability-match
```

neighbor timers

使用 **neighbor timers** 命令设置指定 BGP 邻居的定时器。
使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **timers** {**connect** *connect_timer* | *keepalive_interval holdtime*}

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。
connect_timer	connect 定时器，单位为秒，格式为 INTEGER<0-65535>。
keepalive_interval	存活时间，单位为秒，格式为 INTEGER<0-65535>。表示隔多久向邻居发送存活信息。 缺省值为 60
holdtime	保持时间，单位为秒，格式为 INTEGER<0-65535>。表示多久没有收到邻居的存活信息，就宣布这个邻居已经死掉了。 缺省值为 180

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.10.10 timers 60 120
neteye-bgpd(config-router)#neighbor 10.10.10.10 timers connect 10
```

neighbor transparent-as

使用 **neighbor transparent-as** 命令设置不向自治系统路径中添加自身的自治域号，即使邻居是一个 eBGP 对等体。

命令

neighbor {*neighbor_id* | *group_name*} **transparent-as**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.10.10 transparent-as
```

neighbor transparent-nexthop

使用 **neighbor transparent-nexthop** 命令设置保持路由的下一跳值，即使邻居是一个 eBGP 对等体。

命令

neighbor {*neighbor_id* | *group_name*} **transparent-nexthop**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.10.10 transparent-nexthop
```

neighbor unsuppress-map

使用 **neighbor unsuppress-map** 命令向指定的邻居有选择地泄漏更加详细的路由信息。

使用 **no** 关键字取消该设置。

命令

[**no**] **neighbor** {*neighbor_id* | *group_name*} **unsuppress-map** *route_map_name*

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。
route_map_name	Route Map 名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.0.73 unsuppress-map mymap
```

neighbor update-source

使用 **neighbor update-source** 命令设置 iBGP 会话 TCP 连接使用的可选接口。使用 **no** 关键字取消该设置。

命令

neighbor {*neighbor_id* | *group_name*} **update-source** *interface_name*

no neighbor {*neighbor_id* | *group_name*} **update-source**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。
interface_name	接口名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.0.72 update-source myif
```

neighbor version

使用 **neighbor version** 命令禁用 NetEye 的版本协商能力，并且强制将邻居的 BGP 版本指定为 4。

使用 **no** 关键字取消该设置。

命令

neighbor {*neighbor_id* | *group_name*} **version 4**

no neighbor {*neighbor_id* | *group_name*} **version**

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.10.10 version 4
```

neighbor weight

使用 **neighbor weight** 命令设置指定邻居的默认权重值。
使用 **no** 关键字取消该设置。

命令

neighbor {*neighbor_id* | *group_name*} **weight** *weight_value*

no neighbor {*neighbor_id* | *group_name*} **weight** [*weight_value*]

语法

neighbor_id	BGP 邻居 ID，格式为 X.X.X.X。
group_name	对等体组名称，格式为 WORD。
weight_value	权重值，格式为 INTEGER<0-65535>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#neighbor 10.10.10.10 weight 60
```

network

使用 **network** 命令指定被 BGP 路由进程发布的网络。
使用 **no** 关键字取消该设置。

命令

[**no**] **network** {*ip_address* | *ip_prefix*} [**route-map** *route_map_name*]

语法

ip_address	IP 地址，格式为 X.X.X.X。
ip_prefix	IP 地址范围，格式为 A.B.C.D/M。
route_map_name	Route Map 名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#network 1.2.3.0
```

network backdoor

使用 **network backdoor** 命令设置 BGP 路由进程发布的网络。使用 **backdoor** 关键字来指定一条通向 BGP 边界路由器的后门路由，此路由器能够提供网络的更详细的信息。

使用 **no** 关键字取消该设置。

命令

[**no**] **network** {*ip_address* | *ip_prefix*} **backdoor**

语法

ip_address	IP 地址，格式为 X.X.X.X。
ip_prefix	IP 地址范围，格式为 A.B.C.D/M。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#network 3.3.3.0/24 backdoor
```

network route-map

使用 **network route-map** 命令修改网络中的 BGP 属性。使用 **backdoor** 关键字来指定一条 BGP 后门路由。

使用 **no** 关键字取消该设置。

命令

[**no**] **network** {*ip_address* | *ip_prefix*} **route-map** *route_map_name* [**backdoor**]

语法

ip_address	IP 地址，格式为 X.X.X.X。
ip_prefix	IP 地址范围，格式为 A.B.C.D/M。
route_map_name	Route Map 名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#network 172.16.1.0/24 route-map ipi
```

network synchronization

使用 **network synchronization** 在将指定的静态网络前缀被 BGP RIB 引用之前，确保这些前缀是本地的或具有 IGP 可达性。

使用 **no** 关键字取消该设置。

命令

[**no**] **network synchronization**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#network synchronization
```

redistribute

使用 **redistribute** 命令将其他路由协议中的路由条目重发布到 BGP 路由进程中。使用 **no** 关键字取消该设置。

命令

[**no**] **redistribute** {**ospf** | **rip** | **connected** | **static**} [**route-map** *route_map_name*]

语法

route_map_name	Route Map 名称，格式为 WORD。 Route Map 决定具体重发布哪些路由。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#redistribute ospf route-map rmap1
```

restart bgp graceful

使用 **restart bgp graceful** 命令使用优雅重启方式重启 BGP speaker。

命令

restart bgp graceful

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#restart bgp graceful
```

router bgp

使用 **router bgp** 命令添加 BGP 路由进程并进入到 BGP 路由配置模式。
使用 **no** 关键字取消该设置。

命令

[**no**] **router bgp** *as_number* [**view** *view_name*]

语法

as_number	自治系统号，格式为 INTEGER<1-4294967295>。
view_name	view 名称，格式为 WORD。

说明

如果要指定 *view_name* 参数，则必须先执行 **bgp multiple-instance** 启用 BGP 多实例支持。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 全局配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100 view 1
neteye-bgpd(config-router)#
```

show bgp state

使用 **show bgp state** 命令显示是否启用了 BGP 功能。

命令

show bgp state

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在普通配置模式下使用。

范例

范例 . 显示是否启用了 BGP 功能。

```
NetEye@root>show bgp state
```

【返回结果】

```
BGP is On
```

相关命令

命令名称	描述信息
bgp enable, disable	启用或禁用 BGP 功能。

show debugging bgp

使用 **show debugging bgp** 命令显示 BGP debug 选项设置。

命令

show debugging bgp

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show debugging bgp
```

【返回结果】

```
BGP debugging status:
BGP debugging is on
BGP events debugging is on
BGP updates debugging is on
BGP fsm debugging is on
```

show ip bgp

使用 **show ip bgp** 命令显示 BGP 网络信息。

命令

show ip bgp [*ip_address* | *ip_prefix*]

语法

ip_address	IP 地址，格式为 X.X.X.X。
ip_prefix	IP 地址范围，格式为 A.B.C.D/M。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp
```

【返回结果】

```
BGP table version is 7, local router ID is 80.80.80.80
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
S>i10.70.0.0/24 192.10.23.67 0 100 0 ?
S>i30.30.30.30/32 192.10.23.67 0 100 0 ?
S>i63.63.63.1/32 192.10.23.67 0 100 0 ?
S>i67.67.67.67/32 192.10.23.67 0 100 0 ?
S>i172.22.10.0/24 192.10.23.67 0 100 0 ?
S>i192.10.21.0 192.10.23.67 0 100 0 ?
S>i192.10.23.0 192.10.23.67 0 100 0 ?
Total number of prefixes 7
```

show ip bgp attribute-info

使用 **show ip bgp attribute-info** 命令显示内部属性 hash 信息。

命令

show ip bgp attribute-info

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp attribute-info
```

【返回结果】

```
attr[1] nexthop 0.0.0.0
attr[1] nexthop 10.10.10.10
attr[1] nexthop 10.10.10.50
```

show ip bgp cidr-only

使用 **show ip bgp cidr-only** 命令显示所有非自然掩码的路由。

命令

show ip bgp cidr-only

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp cidr-only
```

【返回结果】

```
BGP table version is 0, local router ID is 10.10.10.50
Status codes: s suppressed, d damped, h history, p stale, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
*> 3.3.3.0/24 10.10.10.10 0 11 i
*> 6.6.6.0/24 0.0.0.0 32768 i
Total number of prefixes 2
```

show ip bgp community

使用 **show ip bgp community** 命令显示匹配团体属性的路由。

命令

show ip bgp community [*number*] [**local-AS**] [**no-advertise**] [**no-export**] [**exact-match**]

语法

number	团体号，格式为 AA:NN，其中 AA 表示自治系统编号， NN 表示分配给团体的编号。
local-AS	不向外发布本地 AS。
no-advertise	不向对等端发布路由信息。
no-export	不导出到下一个 AS。
exact-match	显示团体的精确匹配。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp community local-AS exact-match
```

show ip bgp community-info

使用 **show ip bgp community-info** 显示所有 BGP 团体信息。

命令

show ip bgp community-info

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp community-info
```

show ip bgp community-list

使用 **show ip bgp community-list** 命令显示匹配团体列表的路由。

命令

show ip bgp community-list *list_name* [**exact-match**]

语法

list_name	团体列表名称，格式为 WORD。
exact-match	显示精确匹配指定团体的路由。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp community-list mylist exact-match
```

show ip bgp dampening

使用 **show ip bgp dampening** 命令显示路由抖动的详细信息。

命令

show ip bgp dampening {**dampened | flap-statistics | parameters**}

语法

dampened	显示因惩罚受抑制的路径。
flap-statistics	显示路由抖动统计。
parameters	显示惩罚参数配置的详细信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp dampening parameters
```

【返回结果】

```
dampening 15 750 2000 60 15
Reachability Half-Life time : 15 min
Reuse penalty : 750
Suppress penalty : 2000
Max suppress time : 60 min
Un-reachability Half-Life time : 15 min
Max penalty (ceil) : 11999
Min penalty (floor) : 375
```

show ip bgp filter-list

使用 **show ip bgp filter-list** 命令显示匹配过滤列表的路由。

命令

show ip bgp filter-list *list_name*

语法

list_name	访问列表名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp filter-list mylist
```

show ip bgp inconsistent-as

使用 **show ip bgp inconsistent-as** 命令显示起始于不稳定自治系统路径的路由。

命令

show ip bgp inconsistent-as

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp inconsistent-as
```

show ip bgp neighbors

使用 **show ip bgp neighbors** 命令显示 BGP 邻居 TCP 连接的详细信息。

命令

show ip bgp neighbors [*neighbors_id* [**advertised-routes | received prefix-filter | received-routes | routes**]]

语法

neighbors_id	邻居 ID，格式为 X.X.X.X。
advertised-routes	显示发布到 BGP 邻居的路由。
received prefix-filter	显示前缀列表过滤。
received-routes	显示从邻居接收到的路由。
routes	显示所有从邻居学习到的路由。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp neighbors
```

【返回结果】

```
BGP neighbor is 192.10.23.67, remote AS 1, local AS 1, internal link
BGP version 4, remote router ID 172.22.10.10
BGP state = Established, up for 00:00:22
Last read 00:00:22, hold time is 240, keepalive interval is 60 seconds
Neighbor capabilities:
Route refresh: advertised and received (old and new)
Address family IPv4 Unicast: advertised and received
Received 3 messages, 0 notifications, 0 in queue
Sent 3 messages, 0 notifications, 0 in queue
```

```
Route refresh request: received 0, sent 0
Minimum time between advertisement runs is 5 seconds
For address family: IPv4 Unicast
BGP table version 1, neighbor version 1
Index 1, Offset 0, Mask 0x2
AF-dependant capabilities:
Graceful restart: advertised, received
Community attribute sent to this neighbor (both)
0 accepted prefixes
0 announced prefixes
Connections established 1; dropped 0
Graceful-restart Status:
Remote restart-time is 120 sec
Local host: 192.10.23.80, Local port: 33837
Foreign host: 192.10.23.67, Foreign port: 179
Nexthop: 192.10.23.80
Nexthop global: 1111::80
Nexthop local: fe80::203:47ff:fe97:bb79
BGP connection: non shared network
```

show ip bgp neighbors connection-retrytime

使用 **show ip bgp neighbors connection-retrytime** 命令显示与邻居建立会话的连接重试时间。

命令

show ip bgp neighbors *neighbors_id* **connection-retrytime**

语法

neighbors_id	邻居 ID，格式为 X.X.X.X。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp neighbors 10.11.4.26 connection-retrytime
```

show ip bgp neighbors hold-time

使用 **show ip bgp neighbors hold-time** 命令显示与邻居建立会话的保持时间。

命令

show ip bgp neighbors *neighbors_id* **hold-time**

语法

neighbors_id	邻居 ID，格式为 X.X.X.X。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp neighbors 10.11.4.26 hold-time
```

show ip bgp neighbors keepalive

使用 **show ip bgp neighbors keepalive** 命令显示发送给指定邻居的 keepalive 消息的数目。

命令

show ip bgp neighbors *neighbors_id* **keepalive**

语法

neighbors_id	邻居 ID，格式为 X.X.X.X。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp neighbors 10.11.4.26 keepalive
```

show ip bgp neighbors keepalive-interval

使用 **show ip bgp neighbors keepalive-interval** 命令显示与邻居建立会话的发送 keepalive 消息的时间间隔。

命令

show ip bgp neighbors *neighbors_id* **keepalive-interval**

语法

neighbors_id	邻居 ID，格式为 X.X.X.X。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp neighbors 10.11.4.26 keepalive-interval
```

show ip bgp neighbors notification

使用 **show ip bgp neighbors notification** 命令显示发送给指定邻居的通知消息的数目。

命令

show ip bgp neighbors *neighbors_id* **notification**

语法

neighbors_id	邻居 ID，格式为 X.X.X.X。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp neighbors 10.11.4.26 notification
```

show ip bgp neighbors open

使用 **show ip bgp neighbors open** 命令显示发送给指定邻居的打开消息的数目。

命令

show ip bgp neighbors *neighbors_id* **open**

语法

neighbors_id	邻居 ID，格式为 X.X.X.X。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp neighbors 10.11.4.26 open
```

show ip bgp neighbors rcvd-msgs

使用 **show ip bgp neighbors rcvd-msgs** 命令显示邻居收到消息的数目。

命令

show ip bgp neighbors *neighbors_id* **rcvd-msgs**

语法

neighbors_id	邻居 ID，格式为 X.X.X.X。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp neighbors 10.11.4.26 rcvd-msgs
```

show ip bgp neighbors sent-msgs

使用 **show ip bgp neighbors sent-msgs** 命令显示发送给指定邻居的消息的数目。

命令

show ip bgp neighbors *neighbors_id* **sent-msgs**

语法

neighbors_id	邻居 ID，格式为 X.X.X.X。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp neighbors 10.11.4.26 sent-msgs
```

show ip bgp neighbors update

使用 **show ip bgp neighbors update** 命令显示发送给指定邻居的更新消息的数目。

命令

show ip bgp neighbors *neighbors_id* **update**

语法

neighbors_id	邻居 ID，格式为 X.X.X.X。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp neighbors 10.11.4.26 update
```

show ip bgp paths

使用 **show ip bgp paths** 命令显示 BGP 路径信息。

命令

show ip bgp paths

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp paths
```

show ip bgp prefix-list

使用 **show ip bgp prefix-list** 命令显示匹配前缀列表的路由。

命令

show ip bgp prefix-list *list_name*

语法

list_name	列表名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp prefix-list mylist
```

show ip bgp quote-regexp

使用 **show ip bgp quote-regexp** 命令显示匹配被引用的自治系统路径的路由。

命令

show ip bgp quote-regexp *regular_expression*

语法

regular_expression	表示匹配自治系统路径的有规律的表达式，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd# show ip bgp quote-regexp "IPI"
```

show ip bgp regexp

使用 **show ip bgp regexp** 命令显示匹配自治系统路径的路由。

命令

show ip bgp regexp *regular_expression*

语法

regular_expression	表示匹配自治系统路径的有规律的表达式，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp regexp myexpression
```

show ip bgp route-map

使用 **show ip bgp route-map** 命令显示匹配指定 Route Map 的路由。

命令

show ip bgp route-map *route_map_name*

语法

route_map_name	Route Map 名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp route-map IPI
```

show ip bgp scan

使用 **show ip bgp scan** 命令显示 BGP 扫描状态。

命令

show ip bgp scan

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp scan
```

【返回结果】

```
BGP scan is running
BGP scan interval is 60
BGP instance : AS is 11,DEFAULT
Current BGP nexthop cache:
BGP connected route:
10.10.10.0/24
10.10.11.0/24
```

show ip bgp summary

使用 **show ip bgp summary** 命令显示 BGP 邻居状态的一个汇总。

命令

show ip bgp summary

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp summary
```

【返回结果】

```
BGP router identifier 10.10.15.50, local AS number 65000
1 BGP AS-PATH entries
0 BGP community entries
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/
PfxRcd10.10.9.50 4 65000 460 595 0 0 0 00:17:48 3
10.10.14.51 4 100 9
```

show ip bgp view

使用 **show ip bgp view** 命令显示指定实例的邻居信息。

命令

show ip bgp view *view_name* [*ip_address* | *ip_prefix*]

语法

view_name	view 名称，格式为 WORD。
ip_address	IP 地址，格式为 X.X.X.X。
ip_prefix	IP 地址范围，格式为 A.B.C.D/M。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp view I2
```

【返回结果】

```
BGP table version is 0, local router ID is 10.10.10.50
Status codes: s suppressed, d damped, h history, p stale, * valid, >
best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
*>i100.156.70.0/24 10.10.10.52 0 0 i
*>i100.156.71.0/24 10.10.10.52 0 0 i
*>i100.156.72.0/24 10.10.10.52 0 0 i
*>i100.156.73.0/24 10.10.10.52 0 0 i
*>i100.156.74.0/24 10.10.10.52 0 0 i
Total number of prefixes 5
```

show ip bgp view neighbors

使用 **show ip bgp view neighbors** 命令显示指定实例的邻居信息。

命令

show ip bgp view *view_name* **neighbors** [*ip_address*]

语法

view_name	view 名称，格式为 WORD。
ip_address	IP 地址，格式为 X.X.X.X。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp view I2 neighbors
```

【返回结果】

```
BGP neighbor is 10.10.10.52, remote AS 10, local AS 10, internal link
BGP version 4, remote router ID 10.10.10.52
BGP state = Established, up for 00:03:22
Last read 00:00:13, hold time is 90, keepalive interval is 30 seconds
Neighbor capabilities:
Route refresh: advertised
Address family IPv4 Unicast: advertised
Received 8 messages, 0 notifications, 0 in queue
Sent 8 messages, 0 notifications, 0 in queue
Route refresh request: received 0, sent 0
Minimum time between advertisement runs is 5 seconds
For address family: IPv4 Unicast
Community attribute sent to this neighbor (both)
```

```
5 accepted prefixes
0 announced prefixes
Connections established 1; dropped 0
Local host: 10.10.10.50, Local port: 179
Foreign host: 10.10.10.52, Foreign port: 36950
Nexthop: 10.10.10.50
Nexthop global: fe80::280:c8ff:feb9:d268
Nexthop local: ::
BGP connection: non shared network
Read thread: on Write thread: off
```

show ip bgp view summary

使用 **show ip bgp view summary** 命令显示指定实例的邻居的汇总数据。

命令

show ip bgp view *view_name* **summary**

语法

view_name	view 名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip bgp view I2 summary
```

【返回结果】

```
BGP router identifier 10.10.10.50, local AS number 10
1 BGP AS-PATH entries
0 BGP community entries
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.10.52 4 10 1 2 0 0 0 00:00:07 5
Total number of neighbors 1
```

show ip extcommunity-list

使用 **show ip extcommunity-list** 命令显示扩展团体列表配置。

命令

show ip extcommunity-list [*list_name* | *list_num*]

语法

list_name	扩展团体列表名称，格式为 WORD。
list_num	扩展团体列表编号，格式为 INTEGER<1-199>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip extcommunity-list 33
```

show ip protocols

使用 **show ip protocols** 命令显示 BGP 进程参数和统计。

命令

show ip protocols

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 普通配置模式下使用。

范例

```
neteye-bgpd#show ip protocols
```

【返回结果】

```
Routing Protocol is "bgp 100"
Sending updates every 30 seconds with +/-50%, next due in 12 seconds
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
Default redistribution metric is 1
Redistributing: connected static
Default version control: send version 2, receive version 2
Interface Send Recv Key-chain
eth0 2 2
Routing for Networks:
10.10.0.0/24
Routing Information Sources:
Gateway BadPackets BadRoutes Distance Last Update
Distance: (default is 120
```

synchronization

使用 **synchronization** 命令设置当 NetEye 从 iBGP 邻居学习到路由后，只有这些路由在 IGP 中可达， BGP 才会发布这些路由。

使用 **no** 关键字取消该设置。

命令

[**no**] **synchronization**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#synchronization
```

timers

使用 **timers** 命令设置 BGP 的存活时间和保持时间值。
使用 **no** 关键字取消该设置。

命令

timers bgp *keepalive_interval holdtime*

[**no**] **timers bgp** [*keepalive_interval holdtime*]

语法

keepalive_interval	存活时间，单位为秒，格式为 INTEGER<0-65535>。表示隔多久向邻居发送存活信息。 缺省值为 30
holdtime	保持时间，单位为秒，格式为 INTEGER<0-65535>。表示多久没有收到邻居的存活信息，就宣布这个邻居已经死掉了。 缺省值为 90

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 BGP 路由配置模式下使用。

范例

```
neteye-bgpd#configure terminal
neteye-bgpd(config)#router bgp 100
neteye-bgpd(config-router)#timers bgp 40 120
```

路由选项

access-list

使用 **access-list** 命令创建访问列表。

使用 **unset** 关键字取消该设置。

命令

[**unset**] **access-list** *list_name* {**deny** | **permit**} **ip** {*source_address mask_length* | **any**} [**exact-match**]

语法

list_name	访问列表名称，格式为 WORD。
deny | **permit**	• deny— 指定拒绝的路由 • permit— 指定允许的路由
source_address	源 IP 地址，格式为 X.X.X.X。
mask_length	掩码长度，格式为 INTEGER<0-32>。 **any** 表示任意的 IP 地址。
exact-match	表示进行精确匹配。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]access-list test deny ip 2.2.2.3 24
```

相关命令

命令名称	描述信息
show access-list	显示访问列表。

access-list remark

使用 **access-list remark** 命令设置访问列表的备注信息。

使用 **unset** 关键字取消该设置。

命令

[**unset**] **access-list** *list_name* **remark** *string*

语法

list_name	访问列表名称，格式为 WORD。
string	备注信息，格式为 LINE。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show access-list	显示访问列表。

distance static

使用 **distance static** 命令设置静态路由的管理距离。

使用 **no** 关键字取消该设置。

命令

distance static *static_admin_distance*

no distance static

语法

static_admin_distance	静态管理距离，格式为 INTEGER<1-255>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在路由选项配置模式下使用。

maximum-paths

使用 **maximum-paths** 命令启用多路径支持，并设置在 FIB （转发信息库）中可建立的最大路径数。

使用 **no** 关键字取消该设置。

命令

maximum-paths *numbers*

no maximum-paths [*numbers*]

语法

numbers	在 FIB 中可建立的最大路径数，格式为 INTEGER<1-8>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在路由选项配置模式下使用。

范例

```
NetEye@root-system] zebos nsm
neteye-nsm#configure terminal
neteye-nsm(config)#maximum-paths 5
```

prefix-list

使用 **prefix-list** 命令创建前缀列表。

使用 **unset** 关键字取消该设置。

命令

[**unset**] **prefix-list** *list_name* {**deny | permit**} {*ip_address mask_length* [**le** *max_pre_length* **ge** *min_pre _length*] | **any**}

语法

list_name	前缀列表名称，格式为 WORD。
deny	**permit**	• deny— 指定拒绝的路由 • permit— 指定允许的路由
ip_address	IP 地址，格式为 X.X.X.X。
mask_length	掩码长度，格式为 INTEGER<0-32>。
max_pre_length	最大前缀长度，格式为 INTEGER<0-32>。
min_pre _length	最小前缀长度，格式为 INTEGER<0-32>。
any	表示匹配任意前缀。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]prefix-list test deny 10.0.0.0 8 le 22 ge 14
```

相关命令

命令名称	描述信息
show prefix-list	显示前缀列表信息。

prefix-list description

使用 **prefix-list description** 命令设置前缀列表的描述信息。

使用 **unset** 关键字取消该设置。

命令

[**unset**] **prefix-list** *list_name* **description** *string*

语法

list_name	前缀列表名称，格式为 WORD。
string	描述信息，格式为 LINE。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]prefix-list test description This is prefix-list
test
```

prefix-list sequence-number

使用 **prefix-list sequence-number** 命令设置在前缀列表中显示序号。

使用 **unset** 关键字取消该设置。

命令

[**unset**] **prefix-list sequence-number**

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]prefix-list sequence-number
```

route-map

使用 **route-map** 命令创建 Route Map 条目。

使用 **unset** 关键字取消该设置。

命令

route-map *route_map_name* {**deny | permit**} *sequence*

unset route-map *route_map_name* [{**deny | permit**} *sequence*]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10
```

相关命令

命令名称	描述信息
show route-map	显示 Route Map 的配置信息。

route-map match as-path

使用 **route-map match as-path** 命令设置 Route Map 匹配的自治系统路径。

使用 **unset** 关键字取消该设置。

命令

route-map *route_map_name* {**deny | permit**} *sequence* **match as-path** *as_path*

unset route-map *route_map_name* {**deny | permit**} *sequence* **match as-path** [*as_path*]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
as_path	自治系统路径访问列表名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 match as-path myaccesslist
```

route-map match community, extcommunity

使用 **route-map match community, extcommunity** 命令设置 Route Map 匹配的团体名列表。

使用 **unset** 关键字取消该设置。

命令

[**unset**] **route-map** *route_map_name* {**deny | permit**} *sequence* **match** {**community | extcommunity**} *community_list* [**exact-match**]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | permit	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
community | extcommunity	• community— 表示匹配 BGP 团体名列表 • extcommunity— 表示匹配 BGP 扩展团体名列表
community_list	团体名列表名称，格式为 WORD。
exact-match	表示精确匹配团体名列表。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 match extcommunity
community-list1 exact-match
```

route-map match interface

使用 **route-map match interface** 命令设置 Route Map 匹配的接口。

使用 **unset** 关键字取消该设置。

命令

route-map *route_map_name* {**deny | permit**} *sequence* **match interface** *interface_name*

unset route-map *route_map_name* {**deny | permit**} *sequence* **match interface** [*interface_name*]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
interface_name	接口名称，格式为 WORD<1-16>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 match interface eth1
```

route-map match ip

使用 **route-map match ip** 命令设置 Route Map 匹配的 IP 地址。

使用 **unset** 关键字取消该设置。

命令

route-map *route_map_name* {**deny | permit**} *sequence* **match ip** {**address** | **next-hop**} {*access_list* | **prefix-list** *prefix_list*}

unset route-map *route_map_name* {**deny | permit**} *sequence* **match ip** {**address** | **next-hop**} [*access_list* | **prefix-list** [*prefix_list*]]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
address | **next-hop**	• address— 表示匹配 IP 地址 • next-hop— 表示匹配下一跳 IP 地址
access_list	IP 访问列表名称，格式为 WORD。
prefix_list	IP 前缀列表名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 match ip address
myaccesslist
```

route-map match metric

使用 **route-map match metric** 命令设置 Route Map 匹配的 Metric。

使用 **unset** 关键字取消该设置。

命令

route-map *route_map_name* {**deny | permit**} *sequence* **match metric** *metric_value*

unset route-map *route_map_name* {**deny | permit**} *sequence* **match metric** [*metric_value*]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
metric_value	Metric 值，格式为 INTEGER<0-4294967295>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 match metric 56253
```

route-map match origin

使用 **route-map match origin** 命令设置 Route Map 匹配的路由来源。

使用 **unset** 关键字取消该设置。

命令

route-map *route_map_name* {**deny | permit**} *sequence* **match origin** {**egp | igp | incomplete**}

unset route-map *route_map_name* {**deny | permit**} *sequence* **match origin** [**egp | igp | incomplete**]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | permit	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
egp | igp | incomplete	• egp— 表示来自于 EGP 的路由 • igp— 表示来自于 IGP 的路由 • incomplete— 表示不确定来源的路由

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 match origin incomplete
```

route-map match route-type external

使用 **route-map match route-type external** 命令设置 Route Map 匹配的外部路由类型。

使用 **unset** 关键字取消该设置。

命令

route-map *route_map_name* {**deny | permit**} *sequence* **match route-type external** {**type-1** | **type-2**}

unset route-map *route_map_name* {**deny | permit**} *sequence* **match route-type external** [**type-1** | **type-2**]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
type-1 | **type-2**	• **type-1—** 路由类型 1，表示代价值是这条路由的外部代价加上到达自治系统边界路由器的代价之和。 • **type-2—** 路由类型 1，表示代价值只计算自治系统的外部代价，不计算到达本自治系统边界的路径代价。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 match route-type external
type-1
```

route-map match tag

使用 **route-map match tag** 命令设置 Route Map 匹配的标记。

使用 **unset** 关键字取消该设置。

命令

route-map *route_map_name* {**deny | permit**} *sequence* **match tag** *tag_value*

unset route-map *route_map_name* {**deny | permit**} *sequence* **match tag** [*tag_value*]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
tag_value	标记值，格式为 INTEGER<0-4294967295>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 match tag 100
```

route-map set aggregator

使用 **route-map set aggregator** 命令修改匹配 Route Map 路由的自治系统号。

使用 **unset** 关键字取消该设置。

命令

route-map *route_map_name* {**deny | permit**} *sequence* **set aggregator as** *as_number ip_address*

unset *route_map_name* {**deny | permit**} *sequence* **set aggregator as** [*as_number ip_address*]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
as_number	汇聚器的自治系统号，格式为 INTEGER<1-4294967295>。
ip_address	汇聚器的 IP 地址，格式为 X.X.X.X。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 set aggregator as 43
10.10.0.3
```

route-map set as-path

使用 **route-map set as-path** 命令修改匹配 Route Map 路由的自治系统路径。

使用 **unset** 关键字取消该设置。

命令

route-map *route_map_name* {**deny | permit**} *sequence* **set as-path prepend** *as_number*

unset route-map *route_map_name* {**deny | permit**} *sequence* **set as-path prepend** [*as_number*]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
as_number	自治系统号，格式为 INTEGER<1-4294967295>。

说明

在此处添加的自治系统号，将被添加到原有自治系统路径的后面。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 set as-path prepend 10
```

route-map set atomic-aggregate

使用 **route-map set aggregator** 命令设置匹配 Route Map 的路由进行自动汇总。使用 **unset** 关键字取消该设置。

命令

[**unset**] **route-map** *route_map_name* {**deny | permit**} *sequence* **set atomic-aggregater**

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 set atomic-aggregater
```

route-map set comm-list delete

使用 **route-map set comm-list delete** 命令删除匹配 Route Map 路由的指定团体名属性。

使用 **unset** 关键字取消该设置。

命令

[**unset**] **route-map** *route_map_name* {**deny | permit**} *sequence* **set comm-list** *community_list* **delete**

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
community_list	团体名列表名称，格式为 WORD。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 set comm-list
community-list1 delete
```

route-map set community

使用 **route-map set community** 命令设置匹配 Route Map 路由的指定团体属性。使用 **unset** 关键字取消该设置。

命令

[**unset**] **route-map** *route_map_name* {**deny | permit**} *sequence* **set community** {*community_number* | **internet** | **local-AS** | **no-advertise** | **no-export**} [**additive**]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
community_number	团体号，格式为 INTEGER<1-65535> 或 AA:NN，其中 AA 表示自治系统编号， NN 表示分配给团体的编号。
internet	指定 Internet。
local-AS	只在本地自治系统内部进行发送。
no-advertise	不发送路由通告到 eBGP 对等体。
no-export	不发送路由通告到任何对等体。
additive	以增量方式添加到已存在的团体属性中。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 set community no-export
additive
```

route-map set community none

使用 **route-map set community none** 命令设置匹配 Route Map 路由无团体属性。使用 **unset** 关键字取消该设置。

命令

[**unset**] **route-map** *route_map_name* {**deny | permit**} *sequence* **set community none**

语法

route_map_name	Route Map 名称，格式为 WORD。
**deny	permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 set community none
```

route-map set dampening

使用 **route-map set dampening** 命令设置匹配 Route Map 路由的抖动惩罚属性。

使用 **unset** 关键字取消该设置。

命令

[**unset**] **route-map** *route_map_name* {**deny | permit**} *sequence* **set dampening** [*reach_time* [*reuse_threshold suppress_threshold max_suppression_time* [*unreach_time*]]]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
reach_time	可达半衰期，格式为 INTEGER<1-45>。
reuse_threshold	重用阈值，格式为 INTEGER<1-20000>。
suppress_threshold	抑制阈值，格式为 INTEGER<1-20000>。
max_suppression_time	最大抑制时间，格式为 INTEGER<1-255>。
unreach_time	不可达半衰期，格式为 INTEGER<1-45>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 set dampening 20 333 534 30
```

route-map set ip next-hop

使用 **route-map set ip next-hop** 命令设置匹配 Route Map 路由的下一跳 IP 地址。使用 **unset** 关键字取消该设置。

命令

route-map *route_map_name* {**deny | permit**} *sequence* **set ip next-hop** *ip_address*

unset route-map *route_map_name* {**deny | permit**} *sequence* **set ip next-hop** [*ip_address*]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
ip_address	下一跳 IP 地址，格式为 X.X.X.X。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 set ip next-hop 10.10.0.67
```

route-map set local-preference

使用 **route-map set local-preference** 命令设置匹配 Route Map 路由的本地 BGP 优先级。

使用 **unset** 关键字取消该设置。

命令

route-map *route_map_name* {**deny | permit**} *sequence* **set local-preference** *preference_value*

[**unset**] **route-map** *route_map_name* {**deny | permit**} *sequence* **set local-preference** [*preference_value*]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
preference_value	优先级，格式为 INTEGER<0-4294967295>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 set local-preference 25
```

route-map set metric

使用 **route-map set metric** 命令设置匹配 Route Map 路由的 metric 值。

使用 **unset** 关键字取消该设置。

命令

route-map *route_map_name* {**deny | permit**} *sequence* **set metric** {*metric_value* | **add** *add_metric_value* | **subtract** *subtract_metric_value*}

unset route-map *route_map_name* {**deny | permit**} *sequence* **set metric** [*metric_value* | **add** [*add_metric_value*] | **subtract** [*subtract_metric_value*]]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
metric_value	表示设置路由的 metric 值，格式为 INTEGER<0-4294967295>。
add_metric_value	表示在原有路由 metric 的增加值，格式为 INTEGER<0-4294967295>。
subtract_metric_value	表示在原有路由 metric 的减少值，格式为 INTEGER<0-4294967295>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 set metric add 60
```

route-map set metric-type

使用 **route-map set metric-type** 命令设置匹配 Route Map 路由的 metric 类型。使用 **unset** 关键字取消该设置。

命令

route-map *route_map_name* {**deny | permit**} *sequence* **set metric-type** {**type-1** | **type-2**}

unset route-map *route_map_name* {**deny | permit**} *sequence* **set metric-type** [**type-1** | **type-2**]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
type-1 | **type-2**	• type-1— 设置为外部类型 1 • type-2— 设置为外部类型 2

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 set metric-type type-1
```

route-map set origin

使用 **route-map set origin** 命令设置匹配 Route Map 路由的来源。

使用 **unset** 关键字取消该设置。

命令

route-map *route_map_name* {**deny | permit**} *sequence* **set origin** {**egp** | **igp**| **incomplete**}

unset route-map *route_map_name* {**deny | permit**} *sequence* **set origin** [**egp** | **igp**| **incomplete**]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
egp | **igp** | **incomplete**	• egp— 表示来自于 EGP 的路由 • igp— 表示来自于 IGP 的路由 • incomplete— 表示不确定来源的路由

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 set origin egp
```

route-map set originator-id

使用 **route-map set originator-id** 命令设置匹配 Route Map 路由的源 ID 属性。使用 **unset** 关键字取消该设置。

命令

route-map *route_map_name* {**deny | permit**} *sequence* **set originator-id** *ip_address*

unset route-map *route_map_name* {**deny | permit**} *sequence* **set originator-id** [*ip_address*]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
ip_address	指定的源 IP 地址，格式为 X.X.X.X。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 set originator-id
10.10.1.67
```

route-map set tag

使用 **route-map set tag** 命令设置匹配 Route Map 路由的标记值。

使用 **unset** 关键字取消该设置。

命令

route-map *route_map_name* {**deny | permit**} *sequence* **set tag** *tag_value*

unset route-map *route_map_name* {**deny | permit**} *sequence* **set tag** [*tag_value*]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
tag_value	标记值，格式为 INTEGER<0-4294967295>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 set tag 6
```

route-map set weight

使用 **route-map set weight** 命令设置匹配 Route Map 路由的权重值。

使用 **unset** 关键字取消该设置。

命令

route-map *route_map_name* {**deny | permit**} *sequence* **set weight** *weight_value*

[**unset**] **route-map** *route_map_name* {**deny | permit**} *sequence* **set weight** [*weight_value*]

语法

route_map_name	Route Map 名称，格式为 WORD。
deny | **permit**	• deny— 指定动作为拒绝 • permit— 指定动作为允许
sequence	序号，格式为 INTEGER<1-65535>。
weight_value	权重值，格式为 INTEGER<0-4294967295>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

```
NetEye@root-system]route-map test permit 10 set weight 60
```

show access-list

使用 **show access-list** 命令显示访问列表信息。

命令

show access-list

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在普通配置模式下使用。

范例

```
NetEye@root>show access-list
```

【返回结果】

```
ZebOS IP access list test
    permit 10.3.3.0/24 exact-match
ZebOS IP access list test1
    deny   10.4.4.0/24
```

相关命令

命令名称	描述信息
access-list	创建访问列表。

show prefix-list

使用 **show prefix-list** 命令显示前缀列表信息。

命令

show prefix-list [**summary** | **detail**] [*list_name*]

语法

summary | **detail**	• summary— 表示显示前缀列表的概要信息 • detail— 表示显示前缀列表的详细信息
list_name	前缀列表名称，格式为 WORD。

说明

如果不指定 *list_name* 参数，则显示所有前缀列表的配置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在普通配置模式下使用。

范例

```
NetEye@root>show prefix-list detail test
```

【返回结果】

```
ip prefix-list test:
   count: 1, range entries: 0, sequences: 5 - 5
   seq 5 deny 10.0.0.0/8 ge 14 le 22 (hit count: 0, refcount: 0)
```

相关命令

命令名称	描述信息
prefix-list	创建前缀列表。

show route-map

使用 **show route-map** 命令显示 Route Map 的配置信息。

命令

show route-map [*route_map_name*]

语法

route_map_name	Route Map 名称，格式为 WORD。

说明

如果不指定 *route_map_name* 参数，则显示所有 Route Map 的配置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在普通配置模式下使用。

范例

```
NetEye@root>show route-map test
```

【返回结果】

```
route-map test, permit, sequence 2
  Match clauses:
  Set clauses:
route-map test, permit, sequence 10
  Match clauses:
    extcommunity community-list1 exact-match
    as-path myaccesslist
    ip address myaccesslist
    route-type external type-1
  Set clauses:
    aggregator as 43 10.10.0.3
```

相关命令

命令名称	描述信息
route-map	创建 Route Map 条目。

9 地址转换命令

地址映射

policy mip

使用 **policy mip** 命令添加静态地址映射策略。配置成功后， NetEye 将根据静态地址映射策略，在数据包经过 NetEye 的时候转换其 IP 地址。

命令

policy mip *policy_name before_trans_ipaddress after_trans_ipaddress* [**domain** *domain_name*] {**enable** | **disable**} [*pri*]

语法

policy_name	策略名称，格式为 WORD<1-15>。
before_trans_ipaddress	转换前的 IP 地址，格式为 x.x.x.x。
after_trans_ipaddress	转换后的 IP 地址，格式为 x.x.x.x。
domain_name	域名，格式为 WORD<1-63>。
enable | **disable**	• enable— 启用静态地址映射策略 • disable— 禁用静态地址映射策略
pri	静态地址映射策略的序号，格式为 INTEGER<1-80000>。

说明

1. 如果指定 *domain_name* 参数，则表示 dnat 的转换前地址对应了该域名。
2. 如果*pri*设置为1，表示将该静态地址映射策略添加到所有策略的前面；如果*pri*省略，表示该静态地址映射策略添加到所有策略的后面。
3. NetEye 内部网络发起的数据包经过 NetEye 时，通过匹配静态地址映射策略转换数据包的源 IP 地址； NetEye 外部发起点的数据包经过 NetEye 时，通过匹配静态地址映射策略转换数据包的目的 IP 地址。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加静态地址映射策略 test。当从 NetEye 内部网络发起的数据包经过 NetEye 后，数据包的源 IP 地址 10.3.1.23 会转换为 202.107.117.11。

```
NetEye@root-system]policy mip test 10.3.1.23 202.107.117.11 enable 2
```

相关命令

命令名称	描述信息
policy mip enable, disable	启用或者禁用静态地址映射策略。
policy mip matching	为静态地址映射策略添加策略条件。
policy mip number	改变静态地址映射策略的序号。
show policy mip	显示静态地址映射策略的配置信息。
unset policy mip	删除静态地址映射策略。

policy mip enable, disable

使用 **policy mip enable, disable** 命令启用或者禁用静态地址映射策略。

命令

policy mip *policy_name* {**enable** | **disable**}

语法

policy_name	策略名称，格式为 WORD<1-15>。
enable	**disable**	• enable— 启用静态地址映射策略。 • disable— 禁用静态地址映射策略。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
policy mip	添加静态地址映射策略。

policy mip matching

使用 **policy mip matching** 命令为静态地址映射策略添加策略条件。配置成功后，如果数据包满足该静态地址映射策略所有的策略条件，则使用该策略进行静态地址映射。

命令

policy mip *policy_name* **matching** {**dip** {*start_ipaddress* [*end_ipaddress*] | **object** *ipaddr_object_name* | **group** *ipaddr_group_name* | **netmask** *ip_address net_mask*} | **protocol** {**icmp** {*icmp_type* | *icmp_list* | **any**} | {**tcp** | **udp**} **port** *start_port* [*end_port*] | **other** *start_typenum* [*end_typenum*] | **object** *protocol_object_name* | **group** *protocol_group_name*} | {**input-interface | output-interface**} *interface_name*}

语法

policy_name	策略名称，格式为 WORD<1-15>。
dip	目的 IP 地址。
start_ipaddress	起始 IP 地址，格式为 x.x.x.x。
end_ipaddress	终止 IP 地址，格式为 x.x.x.x。
ipaddr_object_name	IP 地址对象名称，格式为 WORD<1-63>。
ipaddr_group_name	IP 地址对象组名称，格式为 WORD<1-63>。
ip_address	IP 地址，格式为 x.x.x.x。
net_mask	子网掩码，格式为 x.x.x.x。
icmp_type	ICMP 协议类型，可以设置为： ECHO_and_ECHOREPLY； DEST_UNREACH； SOURCE_QUENCH； REDIRECT； ROUTER_ADVERTISEMENT； ROUTER_SOLICITATION； TIME_EXCEEDED； PARAMETERPROB。 TIMESTAMP_and_TIMESTAMPREPLY； INFO_REQUEST_and_INFO_REPLY； ADDRESS_and_ADDRESSREPLY。 **any** 表示上述协议类型中的任意一种类型。

icmp_list	ICMP 协议类型列表，格式为 WORD<1-256>。列表可以为下述协议类型的任意组合： ECHO_and_ECHOREPLY， DEST_UNREACH， SOURCE_QUENCH， REDIRECT， ROUTER_ADVERTISEMENT， ROUTER_SOLICITATION， TIME_EXCEEDED， PARAMETERPROB， TIMESTAMP_and_TIMESTAMPREPLY， INFO_REQUEST_and_INFO_REPLY， ADDRESS_and_ADDRESSREPLY。
start_port	源端口的起始端口，格式为 INTEGER<1-65535>。
end_port	源端口的终止端口，格式为 INTEGER<1-65535>。
start_typenum	起始协议号，格式为 INTEGER<1-255>。
end_typenum	终止协议号，格式为 INTEGER<1-255>。
protocol_object_name	协议对象名称，格式为 WORD<1-63>。
protocol_group_name	协议对象组名称，格式为 WORD<1-63>。
input-interface	入口三层接口。
output-interface	出口三层接口。
interface_name	三层接口名称，格式为 WORD<1-16>。

说明

1. 最多可以设置 32 组含有协议类型的策略条件。

2. IP 地址范围列表不能超过 32 个。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 为静态地址映射 test 添加策略条件，设置目的 IP 地址范围为 192.168.1.0/24。

```
NetEye@root-system]policy mip test matching dip netmask 192.168.1.0
255.255.255.0
```

范例 2. 为静态地址映射 test 添加策略条件，设置出口为 vlan2。

NetEye@root-system]**policy mip test matching output-interface vlan2**

范例 3. 为静态地址映射 test 添加策略条件，设置目的 IP 地址引用 IP 地址对象 OBJ。

NetEye@root-system]**policy mip test matching dip object OBJ**

相关命令

命令名称	描述信息
policy mip	添加静态地址映射策略。
show policy mip	显示静态地址映射策略的配置信息。
unset policy mip	删除静态地址映射策略。
unset policy mip matching	删除静态地址映射策略的策略条件。

policy mip number

使用 **policy mip number** 命令更改静态地址映射策略的序号。

命令

policy mip *policy_name* **number** *pri*

语法

policy_name	策略名称，格式为 WORD<1-15>。
pri	表示静态地址映射策略的序号，格式为 INTEGER<1-80000>。

说明

如果 *pri* 设置为 1，表示将该目的地址转换策略添加到所有策略的前面。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
policy mip	添加静态地址映射策略。
show policy mip	显示静态地址映射策略的配置信息。
unset policy mip	删除静态地址映射策略。

show policy mip

使用 **show policy mip** 命令显示静态地址映射策略的配置信息。

命令

show policy mip [*policy_name*]

语法

policy_name	策略名称，格式为 WORD<1-15>。

说明

如果不指定 *policy_name* 参数，则显示所有静态地址映射策略的配置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示静态地址映射策略 test 的配置信息。

```
NetEye@root>show policy mip test
```

【返回结果】

```
MIP rule list:
  Policy Name: test State: enable
  In-Interface: Any
  Out-Interface: Any
  Domain Name:
  Before_Trans_IP:
    10.3.1.23
  Before_Trans_List_Obj:
  Before_Trans_List_ObjGrp:
  Before_Trans_List_Netmask:
```

```
  Any
After_Trans_IP:
  202.107.117.11
After_Trans_List_Obj:
After_Trans_List_ObjGrp:
After_Trans_List_Netmask:
  Any
Matching_IP_List:
  Any
Matching_IP_List_Obj:
Matching_IP_List_ObjGrp:
Matching_IP_List_Netmask:
  Any
Matching_Protocol_List:
  Any
Matching_Protocol_List_Obj:
  Any
Matching_Protocol_List_ObjGrp:
  Any
```

相关命令

命令名称	描述信息
policy mip	添加静态地址映射策略。
policy mip matching	为静态地址映射策略添加策略条件。

unset policy mip

使用 **unset policy mip** 命令删除静态地址映射策略。

命令

unset policy mip [*policy_name*]

语法

policy_name	策略名称，格式为 WORD<1-15>。

说明

如果不指定 *policy_name* 参数，则删除所有静态地址映射策略。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
policy mip	添加静态地址映射策略。
show policy mip	显示静态地址映射策略的条件。

unset policy mip matching

使用 **unset policy mip matching** 命令删除静态地址映射策略的策略条件。

命令

unset policy mip *policy_name* **matching** {**all | dip | protocol** [**icmp | tcp | udp | other | group | object**] | **input-interface | output-interface**}

语法

policy_name	策略名称，格式为 WORD<1-15>。
dip	目的 IP 地址。
input-interface	入口三层接口。
output-interface	出口三层接口。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除静态地址映射策略 test 的策略条件。

```
NetEye@root-system]unset policy mip test matching dip
NetEye@root-system]unset policy mip test matching
input-interface
```

相关命令

命令名称	描述信息
policy mip	添加静态地址映射策略。
policy mip matching	添加静态地址映射策略的策略条件。
show policy mip	显示静态地址映射策略的信息。
unset policy mip	删除静态地址映射策略。

源地址转换

policy snat

使用 **policy snat** 命令添加源地址转换策略。配置成功后， NetEye 将根据该策略，在数据包经过 NetEye 的时候转换其源 IP 地址。

命令

policy snat *policy_name* {**iplist** *before_trans_iprange_list* | **netmask** *before_trans_ip_address before_trans_net_mask* | **object** *object_name* | **group** *group_name*} {**interface** *interface_name* | **iplist** *after_trans_iprange_list* | **netmask** *after_trans_ip_address after_trans_net_mask*} {**holdtime** *time* | **napt**} {**enable** | **disable**} [*pri*]

语法

policy_name	策略名称，格式为 WORD<1-15>。
before_trans_iprange_list	转换前的源 IP 地址列表，格式为 IPV4LIST<1-32>。
before_trans_ip_address	转换前 IP 地址，格式为 x.x.x.x。
before_trans_net_mask	转换前子网掩码，格式为 x.x.x.x。
object_name	IP 地址对象名称，格式为 WORD<1-63>。
group_name	IP 地址组名称，格式为 WORD<1-63>。
interface	表示添加基于 NetEye 接口作为转换后地址的源地址转换策略。
interface_name	接口名称，格式为 WORD<1-16>。
after_trans_iprange_list	转换后的源 IP 地址列表，格式为 IPV4LIST<1-8>。
after_trans_ip_address	转换后 IP 地址，格式为 x.x.x.x。
after_trans_net_mask	转换后子网掩码，格式为 x.x.x.x。
time	NAT 映射关系的保留时间，单位是秒，格式为 INTEGER<30-99999999>。
napt	表示允许进行源端口转换。
enable | **disable**	• enable— 启用源地址转换策略。 • disable— 禁用源地址转换策略。
pri	*pri* 为可选项，表示源地址转换策略的序号，格式为 INTEGER<1-80000>。

说明

1. 如果 *pri* 设置为 1，表示将该源地址转换策略添加到所有策略的前面；如果 *pri* 省略，表示该源地址转换策略添加到所有策略的后面。
2. NAT 映射关系的保留时间是指转换为该地址的所有会话都断开后，该地址的保留时间。如果在设置的时间内没有转换到该地址的会话，则释放该地址。
3. 在同一个 Vsys 下的源地址转换策略中，如果有多条策略指定了相同或者重叠的 *after_trans_iprange_list*，那么这些策略都必须进行端口转换，或者都不进行端口转换。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加源地址转换策略 test。当来自于 192.168.1.1-192.168.1.254 的数据包进入 NetEye 后，其源 IP 地址会被转换为 202.104.112.1，映射关系的保留时间为 200 秒。

```
NetEye@root-system]policy snat test iplist
192.168.1.1-192.168.1.254 iplist 202.104.112.1 holdtime 200 enable 2
```

相关命令

命令名称	描述信息
policy snat enable, disable	启用或者禁用源地址转换策略。
policy snat matching	为源地址转换策略添加策略条件。
policy snat number	改变源地址转换策略的序号。
show policy snat	显示源地址转换策略的配置信息。
unset policy snat	删除源地址转换策略。

policy snat append

使用 **policy snat append** 命令为源地址转换策略追加 IP 地址。

命令

policy snat *policy_name* **append** {**after**{**ip** *start_ip* [*end_ip*] | **netmask** *ip_address net_mask*} | **before** {**object** *ipaddr_object_name* | **group** *ipaddr_group_name* | **ip** *start_ip* [*end_ip*] | **netmask** *ip_address net_mask*}}

语法

policy_name	策略名称，格式为 WORD<1-15>。
start_ip	起始 IP 地址，格式为 x.x.x.x。
end_ip	终止 IP 地址，格式为 x.x.x.x。
ipaddr_object_name	IP 地址对象名称，格式为 WORD<1-63>。
ipaddr_group_name	IP 地址对象组名称，格式为 WORD<1-63>。
ip_address	IP 地址，格式为 x.x.x.x。
net_mask	子网掩码，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 为源地址转换策略 test 追加转换前 IP 地址，引用 IP 地址对象 OBJ。

```
NetEye@root-system]policy snat test append before object OBJ
```

范例 2. 为源地址转换策略 test 追加转换后 IP 地址 192.168.1.100 及其子网掩码 255.255.255.0。

```
NetEye@root-system]policy snat test append after netmask 192.168.1.100
255.255.255.0
```

相关命令

命令名称	描述信息
policy snat	添加源地址转换策略。
policy snat enable, disable	启用或者禁用源地址转换策略。
unset policy snat	删除源地址转换策略。

policy snat enable, disable

使用 **policy snat enable, disable** 命令启用或者禁用源地址转换策略。

命令

policy snat *policy_name* {**enable** | **disable**}

语法

policy_name	策略名称，格式为 WORD<1-15>。
enable | **disable**	• enable— 启用源地址转换策略。 • disable— 禁用源地址转换策略。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
policy snat	添加源地址转换策略。

policy snat matching

使用 **policy snat matching** 命令为源地址转换策略添加策略条件。配置成功后，如果数据包满足该策略所有的策略条件，则转换源 IP 地址。

命令

policy snat *policy_name* **matching** {**dip** {*start_ipaddress* [*end_ipaddress*] | **object** *ipaddr_object_name* | **group** *ipaddr_group_name* | **netmask** *ip_address net_mask*} | **protocol** {**icmp** {*icmp_type* | *icmp_list* | **any**} | {**tcp** | **udp**} **port** *start_port* [*end_port*] | **other** *start_typenum* [*end_typenum*] | **object** *protocol_object_name* | **group** *protocol_group_name*} | {**input-interface | output-interface**} *interface_name*}

语法

policy_name	策略名称，格式为 WORD<1-15>。
dip	目的 IP 地址。
start_ipaddress	起始 IP 地址，格式为 x.x.x.x。
end_ipaddress	终止 IP 地址，格式为 x.x.x.x。
ipaddr_object_name	IP 地址对象名称，格式为 WORD<1-63>。
ipaddr_group_name	IP 地址对象组名称，格式为 WORD<1-63>。
ip_address	IP 地址，格式为 x.x.x.x。
net_mask	子网掩码，格式为 x.x.x.x。
icmp_type	ICMP 协议类型，可以设置为： ECHO_and_ECHOREPLY； DEST_UNREACH； SOURCE_QUENCH； REDIRECT； ROUTER_ADVERTISEMENT； ROUTER_SOLICITATION； TIME_EXCEEDED； PARAMETERPROB。 TIMESTAMP_and_TIMESTAMPREPLY； INFO_REQUEST_and_INFO_REPLY； ADDRESS_and_ADDRESSREPLY 。 **any** 表示上述协议类型中的任意一种类型。

icmp_list	ICMP 协议类型列表，格式为 WORD<1-256>。列表可以为下述协议类型的任意组合： ECHO_and_ECHOREPLY， DEST_UNREACH， SOURCE_QUENCH， REDIRECT， ROUTER_ADVERTISEMENT， ROUTER_SOLICITATION， TIME_EXCEEDED， PARAMETERPROB， TIMESTAMP_and_TIMESTAMPREPLY， INFO_REQUEST_and_INFO_REPLY， ADDRESS_and_ADDRESSREPLY。
start_port	源端口的起始端口，格式为 INTEGER<1-65535>。
end_port	源端口的终止端口，格式为 INTEGER<1-65535>。
start_typenum	起始协议号，格式为 INTEGER<1-255>。
end_typenum	终止协议号，格式为 INTEGER<1-255>。
protocol_object_name	协议对象名称，格式为 WORD<1-63>。
protocol_group_name	协议对象组名称，格式为 WORD<1-63>。
input-interface	入口三层接口。
output-interface	出口三层接口。
interface_name	三层接口名称，格式为 WORD<1-16>。

说明

1. IP 地址范围列表不能超过 32 个。

2. 最多可以设置 32 组含有协议类型的策略条件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 为源地址转换策略 test 添加策略条件，设置目的 IP 地址范围为 192.168.1.100-192.168.1.122。

```
NetEye@root-system]policy snat test matching dip 192.168.1.100
192.168.1.122
```

范例 2. 为源地址转换策略 test 添加策略条件，设置入口为 vlan1。

```
NetEye@root-system]policy snat test matching input-interface vlan1
```

范例 3. 为源地址转换策略 test 添加策略条件，设置目的 IP 地址引用 IP 地址对象 OBJ。

```
NetEye@root-system]policy snat test matching object OBJ
```

相关命令

命令名称	描述信息
policy snat	添加源地址转换策略。
show policy snat	显示源地址转换策略的配置信息。
unset policy snat	删除源地址转换策略。
unset policy snat matching	删除源地址转换策略的策略条件。

policy snat number

使用 **policy snat number** 命令更改源地址转换策略的序号。

命令

policy snat *policy_name* **number** *pri*

语法

policy_name	策略名称，格式为 WORD<1-15>。
pri	表示源地址转换策略的序号，格式为 INTEGER<1-80000>。

说明

如果 *pri* 设置为 1，表示将该目的地址转换策略添加到所有策略的前面。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
policy snat	添加源地址转换策略。
show policy snat	显示源地址转换策略的配置信息。
unset policy snat	删除源地址转换策略。

show policy snat

使用 **show policy snat** 命令显示源地址转换策略的配置信息。

命令

show policy snat [*policy_name*]

语法

policy_name	策略名称，格式为 WORD<1-15>。

说明

如果不指定 *policy_name* 参数，则显示所有源地址转换策略的配置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式。

范例

范例 . 显示源地址转换策略 stest 的配置信息。

```
NetEye@root>show policy snat test
```

【返回结果】

```
Snat rule list:
  Policy Name: test State: enable Port-Trans: false
  In-Interface: Any
  Out-Interface: Any
  Before_Trans_List:
    192.168.1.1-192.168.1.254
  Before_Trans_List_Obj:
  Before_Trans_List_ObjGrp:
  Before_Trans_List_Netmask:
    Any
```

```
After_Trans_List:
  202.104.112.1
After_Trans_List_Obj:
After_Trans_List_ObjGrp:
After_Trans_List_Netmask:
  Any
Matching_IP_List:
  Any
Matching_IP_List_Obj:
Matching_IP_List_ObjGrp:
Matching_IP_List_Netmask:
  Any
Matching_Protocol_List:
  Any
Matching_Protocol_List_Obj:
  Any
Matching_Protocol_List_ObjGrp:
  Any
Hold time: 200
```

相关命令

命令名称	描述信息
policy snat	添加源地址转换策略。
policy snat matching	为源地址转换策略添加策略条件。

unset policy snat

使用 **unset policy snat** 命令删除源地址转换策略。

命令

unset policy snat [*policy_name*]

语法

policy_name	策略名称，格式为 WORD<1-15>。

说明

如果不指定 *policy_name* 参数，则删除所有源地址转换策略。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
policy snat	添加源地址转换策略。
show policy snat	显示源地址转换策略的配置信息。

unset policy snat matching

使用 **unset policy snat matching** 命令删除源地址转换策略的策略条件。

命令

unset policy snat *policy_name* **matching** {**all | dip** | **protocol** [**icmp** | **tcp** | **udp** | **other | group | object**] | **input-interface | output-interface**}

语法

policy_name	策略名称，格式为 WORD<1-15>。
dip	目的 IP 地址。
input-interface	入口三层接口。
output-interface	出口三层接口。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除源地址转换策略 test 的策略条件。

```
NetEye@root-system]unset policy snat test matching dip
NetEye@root-system]unset policy snat test matching
input-interface
```

相关命令

命令名称	描述信息
policy snat	添加源地址转换策略。
policy snat matching	添加源地址转换策略的策略条件。
show policy snat	显示源地址转换策略的配置信息。
unset policy snat	删除源地址转换策略。

目的地址转换

policy dnat

使用 **policy dnat** 命令添加目的地址转换策略。配置成功后， NetEye 将根据该策略，在数据包经过 NetEye 的时候改变其目的 IP 地址。

命令

policy dnat *policy_name before_trans_ipaddress* [**domain** *domain_name*] {*after_trans_ipaddress* | {**tcp** | **udp** | **other**} *before_trans_port after_trans_ipaddress after_trans_port*} {**enable** | **disable**} [*pri*]

语法

policy_name	策略名称，格式为 WORD<1-15>。
before_trans_ipaddress	转换前目的 IP 地址，格式为 x.x.x.x。
domain_name	域名，格式为 WORD<1-63>。
before_trans_port	转换前端口，格式为 INTEGER<1-65535>。
after_trans_ipaddress	转换后目的 IP 地址，格式为 x.x.x.x。
after_trans_port	转换后端口，格式为 INTEGER<1-65535>。
enable | **disable**	• enable— 启用目的地址转换策略。 • disable— 禁用目的地址转换策略。
pri	*pri* 为可选项，表示目的地址转换策略的序号，格式为 INTEGER<1-80000>。

说明

1. 如果*pri*设置为1，表示将该目的地址转换策略添加到所有策略的前面；如果*pri*省略，表示该目的地址转换策略添加到所有策略的后面。
2. 如果指定 *domain_name* 参数，则表示 dnat 的转换前地址对应了该域名。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加目的地址转换策略 test。当目的地址为 192.168.1.101 的数据包从 80 端口进入 NetEye 时，其目的地址和端口分别转换为 192.168.2.106 和 8080。

```
NetEye@root-system]policy dnat test 192.168.1.101 tcp 80 192.168.2.106
8080 enable 2
```

相关命令

命令名称	描述信息
policy dnat enable, disable	启用或者禁用目的地址转换策略。
policy dnat load-balancing	添加具有负载均衡功能的目的地址转换策略。
policy dnat number	设置目的地址转换策略的序号。
show policy dnat	显示目的地址转换策略的配置信息。
unset policy dnat	删除目的地址转换策略。

policy dnat enable, disable

使用 **policy dnat enable, disable** 命令启用或者禁用目的地址转换策略。

命令

policy dnat *policy_name* {**enable** | **disable**}

语法

policy_name	策略名称，格式为 WORD<1-15>。
enable | **disable**	• enable— 启用目的地址转换策略。 • disable— 禁用目的地址转换策略。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
policy dnat	添加目的地址转换策略。
policy dnat load-balancing	添加具有负载均衡功能的目的地址转换策略。

policy dnat load-balancing

使用 **policy dnat load-balancing** 命令添加具有负载均衡功能的目的地址转换策略。配置成功后， NetEye 将根据目的地址转换策略，在数据包经过 NetEye 的时候改变其目的 IP 地址。

命令

policy dnat *policy_name* **load-balancing** *before_trans_ipaddress* [**domain** *domain_name*] {**tcp** | **udp | other**} *before_trans_port after_trans_ip after_trans_port weight* [**ip-track** {**arpping | ping | tcpping port** *track_port*} *track_interval track_ time*] {**enable** | **disable**} [*pri*]

语法

policy_name	策略名称，格式为 WORD<1-15>。
before_trans_ipaddress	转换前的目的 IP 地址，格式为 x.x.x.x。
domain_name	域名，格式为 WORD<1-63>。
before_trans_port	转换前端口，格式为 INTEGER<1-65535>。
after_trans_ip	转换后的目的 IP 地址，格式为 x.x.x.x。
after_trans_port	转换后的端口，格式为 INTEGER<1-65535>。
weight	度量值，格式为 INTEGER<1-255>。
ip-track	表示设置链路探测。
arpping | ping | tcpping	• arpping—ARP ping 方式 • ping—ICMP ping 方式 • tcpping—TCP ping 方式
track_port	探测端口，格式为 INTEGER<1-65535>。
track_interval	探测周期，格式为 INTEGER<1-30000>。
track_time	探测次数，格式为 INTEGER<1-999>。
enable | disable	• enable— 启用目的地址转换策略。 • disable— 禁用目的地址转换策略。
pri	*pri* 为可选项，表示目的地址转换策略的序号，格式为 INTEGER<1-80000>。

说明

1. 如果*pri*设置为1，表示将该目的地址转换策略添加到所有策略的前面；如果*pri*省略，表示该目的地址转换策略添加到所有策略的后面。
2. 如果指定 *domain_name* 参数，则表示 dnat 的转换前地址对应了该域名。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加具有负载均衡功能的目的地址转换策略 test。当目的地址为 192.168.1.100 的数据包从 80 端口进入 NetEye 时，其目的地址转换为 192.168.2.10、 192.168.2.20，端口号转换为 8080，并使用 Ping 方式探测转换后的目的 IP 地址是否有效。

```
NetEye@root-system] policy dnat test load-balancing 192.168.1.100 tcp
80 192.168.2.10 8080 2 ip-track ping 3 5 enable
```

```
NetEye@root-system] policy dnat test matching load-balancing
192.168.2.20 8080 3 ip-track ping 3 5
```

相关命令

命令名称	描述信息
policy dnat	添加目的地址转换策略。
policy dnat enable, disable	启用或者禁用目的地址转换策略。
policy dnat matching	为目的地址转换策略添加策略条件。
policy dnat number	设置目的地址转换策略的序号。
show policy dnat	显示目的地址转换策略的配置信息。
unset policy dnat	删除目的地址转换策略。

policy dnat matching

使用 **policy dnat matching** 命令为目的地址转换策略添加策略条件。配置成功后，如果数据包满足该策略所有的策略条件，则使用该策略转换其目的 IP 地址。

命令

policy dnat *policy_name* **matching** {**sip** {*start_ipaddress* [*end_ipaddress*] | **object** *ipaddr_object_name* | **group** *ipaddr_group_name* | **netmask** *ip_address net_mask*} | **input-interface** *interface_name* | **load-balancing** *after_trans_ip after_trans_port weight* [**ip-track** {**arpping | ping | tcpping port** *track_port*} *track_interval track_time*]}

语法

policy_name	策略名称，格式为 WORD<1-15>。
sip	源 IP 地址。
start_ipaddress	起始 IP 地址，格式为 x.x.x.x。
end_ipaddress	终止 IP 地址，格式为 x.x.x.x。
ipaddr_object_name	IP 地址对象名称，格式为 WORD<1-63>。
ipaddr_group_name	IP 地址对象组名称，格式为 WORD<1-63>。
ip_address	IP 地址，格式为 x.x.x.x。
net_mask	子网掩码，格式为 x.x.x.x。
input-interface	入口三层接口。
interface_name	三层接口名称，格式为 WORD<1-16>。
after_trans_ip	转换后的目的 IP 地址，格式为 x.x.x.x。
after_trans_port	转换后的端口，格式为 INTEGER<1-65535>。
weight	度量值，格式为 INTEGER<1-255>。
ip-track	表示设置链路探测。
arpping | ping | tcpping	• arpping—ARP ping 方式 • ping—ICMP ping 方式 • tcpping—TCP ping 方式
track_port	探测端口，格式为 INTEGER<1-65535>。
track_interval	探测周期，格式为 INTEGER<1-30000>。
track_time	探测次数，格式为 INTEGER<1-999>。

说明

IP 地址范围列表不能超过 32 个。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 为目的地址转换策略 test 添加策略条件，设置源 IP 地址为 192.168.1.100。

```
NetEye@root-system]policy dnat test matching sip 192.168.1.100
```

范例 2. 为目的地址转换策略 test 添加策略条件，设置入口为 vlan1。

```
NetEye@root-system]policy dnat test matching input-interface vlan1
```

范例 3. 为目的地址转换策略 test 添加策略条件，设置源 IP 地址引用 IP 地址对象 OBJ。

```
NetEye@root-system]policy dnat test matching sip object OBJ
```

相关命令

命令名称	描述信息
policy dnat	添加目的地址转换策略。
show policy dnat	显示目的地址转换策略的配置信息。
unset policy dnat	删除目的地址转换策略。
unset policy dnat matching	删除目的地址转换策略的策略条件。

policy dnat number

使用 **policy dnat number** 命令更改目的地址转换策略的序号。

命令

policy dnat *policy_name* **number** *pri*

语法

policy_name	策略名称，格式为 WORD<1-15>。
pri	*pri* 为可选项，表示目的地址转换策略的序号，格式为 INTEGER<1-80000>。

说明

如果 *pri* 设置为 1，表示将该目的地址转换策略添加到所有策略的前面；如果 *pri* 省略，表示该目的地址转换策略添加到所有策略的后面。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
policy dnat	添加目的地址转换策略。
show policy dnat	显示目的地址转换策略的配置信息。
unset policy dnat	删除目的地址转换策略。

show policy dnat

使用 **show policy dnat** 命令显示目的地址转换策略的配置信息。

命令

show policy dnat [*policy_name*]

语法

policy_name	策略名称，格式为 WORD<1-15>。

说明

如果不指定 *policy_name* 参数，则显示所有目的地址转换策略的配置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式。

范例

范例 . 显示目的地址转换策略 test 的配置信息。

```
NetEye@root>show policy dnat test
```

【返回结果】

```
Dnat rule list:
  Policy Name: test                State: disable  Load_Balancing: no
Napt: true
  In-Interface: Any
  Protocol: tcp
  Before_Trans_Ip:
    IP               Port   Domain-Name
    6.0.0.0          5      77
  After_Trans_Ip_List:
    IP               Port   Metric Detect  Port   Interval  Failure
    8.0.0.0          7
  Matching_IP_List:
```

```
  Any
Matching_IP_List_Obj:
Matching_IP_List_ObjGrp:
Matching_IP_List_Netmask:
  Any
```

相关命令

命令名称	描述信息
policy dnat	添加目的地址转换策略。
policy dnat matching	为目的地址转换策略添加策略条件。

unset policy dnat

使用 **unset policy dnat** 命令删除目的地址转换策略。

命令

unset policy dnat [*policy_name*]

语法

policy_name	策略名称，格式为 WORD<1-15>。

说明

如果不指定 *policy_name* 参数，则删除所有目的地址转换策略。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
policy dnat	添加目的地址转换策略。
show policy dnat	显示目的地址转换策略的配置信息。

unset policy dnat matching

使用 **unset policy dnat matching** 命令删除目的地址转换策略的策略条件。

命令

unset policy dnat *policy_name* **matching** {**all | sip | input-interface**}

语法

policy_name	策略名称，格式为 WORD<1-15>。
sip	源 IP 地址。
input-interface	入口三层接口。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除目的地址转换策略 test 的策略条件。

```
NetEye@root-system]unset policy dnat test matching sip
NetEye@root-system]unset policy dnat test matching
input-interface
```

相关命令

命令名称	描述信息
policy dnat	添加目的地址转换策略。
policy dnat matching	添加目的地址转换策略的策略条件。
show policy dnat	显示目的地址转换策略的配置信息。
unset policy dnat	删除目的地址转换策略。

10 会话命令

clear session

使用 **clear session** 命令删除当前系统的会话。

命令

clear session [**num** *sessionnum* | {*szone* | **any**} {*dzone* | **any**} {*sip* | *siprange* | **any**} {*dip* | *diprange* | **any**} **protocol** {{**tcp** | **udp**} [{*sport* | *sport_range* | **any**} {*dport* | *dport_range* | **any**}] | **icmp** [*icmp_type*] | **other** [*num*] | **any**}]

语法

sessionnum	会话号，格式为 WORD<1-8>。
szone	源安全域，格式为 WORD<1-15>。 **any** 代表任何源安全域。
dzone	目的安全域，格式为 WORD<1-15>。 **any** 代表任何目的安全域。
sip	源 IP 地址，格式为 x.x.x.x。
siprange	源 IP 地址范围，格式为 IPV4RANGE。 **any** 代表任何源 IP 地址。
dip	目的 IP 地址，格式为 x.x.x.x。
diprange	目的 IP 地址范围，格式为 IPV4RANGE。 **any** 代表任何目的 IP 地址。
sport	源端口，格式为 INTEGER<1-65535>。 **any** 代表任何源端口。
sport_range	源端口的范围，格式为 LIMIT。
dport	目的端口，格式为 INTEGER<1-65535>。 **any** 代表任何目的端口。
dport_range	目的端口的范围，格式为 LIMIT。

icmp_type	ICMP 协议类型，设置个数为 1，可以设置为： ECHO_and_ECHOREPLY； TIMESTAMP_and_TIMESTAMPREPLY； INFO_REQUEST_and_INFO_REPLY； ADDRESS_and_ADDRESSREPLY； DEST_UNREACH； PARAMETERPROB； REDIRECT； ROUTER_ADVERTISEMENT； SOURCE_QUENCH； TIME_EXCEEDED； ROUTER_SOLICITATION。
num	协议号，格式为 INTEGER<1-255>。

说明

如果不指定任何参数，则删除当前系统所有的会话。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在普通配置模式下使用。

范例

范例 . 删除当前系统的源 IP 地址为 192.168.2.100、目的 IP 地址为 192.168.1.100 的会话。

```
NetEye@root> clear session any any 192.168.2.100 192.168.1.100 protocol tcp
```

相关命令

命令名称	描述信息
show session	显示当前系统的会话表。
show session count	显示当前系统的会话数目。

show session

使用 **show session** 命令显示当前系统的会话表。

命令

show session [{*szone* | **any**} {*dzone* | **any**} {*sip* | *siprange* | **any**} {*dip* | *diprange* | **any**} **protocol** {**tcp** [{*sport* | *sport_range* | **any**} {*dport* | *dport_range* | **any**} {*tcp_state* | **any**}] | **udp** [{*sport* | *sport_range* | **any**} {*dport* | *dport_range* | **any**} {*udp_state* | **any**}] | **icmp** [*icmp_type*] | **other** [*num*] | **any**}]

语法

szone	源安全域，格式为 WORD<1-15>。 **any** 代表任何源安全域。
dzone	目的安全域，格式为 WORD<1-15>。 **any** 代表任何目的安全域。
sip	源 IP 地址，格式为 x.x.x.x。
siprange	源 IP 地址范围，格式为 IPV4RANGE。 **any** 代表任何源 IP 地址。
dip	目的 IP 地址，格式为 x.x.x.x。
diprange	目的 IP 地址范围，格式为 IPV4RANGE。 **any** 代表任何目的 IP 地址。
sport	源端口，格式为 INTEGER<1-65535>。 **any** 代表任何源端口。
sport_range	源端口的范围，格式为 LIMIT。
dport	目的端口，格式为 INTEGER<1-65535>。 **any** 代表任何目的端口。
dport_range	目的端口的范围，格式为 LIMIT。
tcp_state	TCP 会话状态，设置个数为 1，可以设置为： ESTED； FIN； CLOSED； SYN； SYN_SENT； SYN_ACKED。 **any** 代表任意一种状态。
udp_state	UDP 会话状态，设置个数为 1，可以设置为： ESTED。 **any** 代表任意一种状态。

icmp_type	ICMP 协议类型，设置个数为 1，可以设置为： ECHO_and_ECHOREPLY； TIMESTAMP_and_TIMESTAMPREPLY； INFO_REQUEST_and_INFO_REPLY； ADDRESS_and_ADDRESSREPLY； DEST_UNREACH； PARAMETERPROB； REDIRECT； ROUTER_ADVERTISEMENT； SOURCE_QUENCH； TIME_EXCEEDED； ROUTER_SOLICITATION。
num	协议号，格式为 INTEGER<1-255>。

说明

如果不指定任何参数，则显示当前会话表中所有的信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示当前系统的会话表。

```
NetEye@root> show session
```

【返回结果】

```
9BCE8694 : (null) -> (null)                    state: ESTED
           10.3.1.44:0->239.255.255.250:0, protocol:2
           est-time  D2009/12/17T15:37:53  last-time  0d0h8m45s
           10.3.1.44:0 <- 239.255.255.250:0
           Next Hop: 0.0.0.0
9BCF8208 : (null) -> (null)                    state: ESTED
           10.3.1.23:2361->10.3.1.52:22, protocol:tcp
           est-time  D2009/12/17T15:46:32  last-time  0d0h0m6s
```

```
            10.3.1.23:2361 <- 10.3.1.52:22
            Next Hop: 0.0.0.0
9BCEC818 : (null) -> (null)                  state: INIT
            10.3.1.28:137->10.3.1.255:137, protocol:udp
            est-time  D2009/12/17T15:46:36  last-time  0d0h0m2s
            10.3.1.28:137 <- 10.3.1.255:137
            Next Hop: 0.0.0.0
9BD25C64 : (null) -> (null)                  state: ESTED
            10.3.1.11:0->224.0.0.22:0, protocol:2
            est-time  D2009/12/17T15:41:49  last-time  0d0h4m49s
            10.3.1.11:0 <- 224.0.0.22:0
            Next Hop: 0.0.0.0
9BCE3044 : (null) -> (null)                  state: SYN_SENT
            192.168.255.254:50113->10.3.1.63:443, protocol:tcp
            est-time  D2009/12/17T15:45:03  last-time  0d0h1m35s
            192.168.255.254:50113 <- 10.3.1.63:443
            Next Hop: 0.0.0.0
9BDCCB20 : (null) -> (null)                  state: ESTED
            10.3.1.222:0->224.0.0.251:0, protocol:2
            est-time  D2009/12/17T10:04:40  last-time  0d5h41m58s
            10.3.1.222:0 <- 224.0.0.251:0
            Next Hop: 0.0.0.0
9BD0534C : (null) -> (null)                  state: ESTED
            10.3.1.44:0->224.0.0.252:0, protocol:2
            est-time  D2009/12/17T14:12:34  last-time  0d1h34m4s
            10.3.1.44:0 <- 224.0.0.252:0
            Next Hop: 0.0.0.0
9BCE8208 : (null) -> (null)                  state: SYN_SENT
            192.168.255.254:50110->10.3.1.63:443, protocol:tcp
            est-time  D2009/12/17T15:45:00  last-time  0d0h1m38s
            192.168.255.254:50110 <- 10.3.1.63:443
```

相关命令

命令名称	描述信息
clear session	删除当前系统的会话。
show session count	显示当前系统的会话数目。

show session count

使用 **show session count** 命令显示当前系统的会话数目。

命令

show session count [{*szone* | **any**} {*dzone* | **any**} {*sip* | *siprange* | **any**} {*dip* | *diprange* | **any**} **protocol** {**tcp** {*sport* | *sport_range* | **any**} {*dport* | *dport_range* | **any**} {*tcp_state* | **any**} | **udp** {*sport* | *sport_range* | **any**} {*dport* | *dport_range* | **any**} {*udp_state* | **any**} | **icmp** {*icmp_type*| **any**} | **other** {*num* | **any**}}]

语法

szone	源安全域，格式为 WORD<1-15>。 **any** 代表任何源安全域。
dzone	目的安全域，格式为 WORD<1-15>。 **any** 代表任何目的安全域。
sip	源 IP 地址，格式为 x.x.x.x。
siprange	源 IP 地址范围，格式为 IPV4RANGE。 **any** 代表任何源 IP 地址。
dip	目的 IP 地址，格式为 x.x.x.x。
diprange	目的 IP 地址范围，格式为 IPV4RANGE。 **any** 代表任何目的 IP 地址。
sport	源端口，格式为 INTEGER<1-65535>。 **any** 代表任何源端口。
sport_range	源端口的范围，格式为 LIMIT。
dport	目的端口，格式为 INTEGER<1-65535>。 **any** 代表任何目的端口。
dport_range	目的端口的范围，格式为 LIMIT。
tcp_state	TCP 会话状态，设置个数为 1，可以设置为： ESTED； FIN； CLOSED； SYN； SYN_SENT； SYN_ACKED。 **any** 代表任意一种状态。
udp_state	UDP 会话状态，设置个数为 1，可以设置为： ESTED。 **any** 代表任意一种状态。

icmp_type	ICMP 协议类型，设置个数为 1，可以设置为： ECHO_and_ECHOREPLY； TIMESTAMP_and_TIMESTAMPREPLY； INFO_REQUEST_and_INFO_REPLY； ADDRESS_and_ADDRESSREPLY； DEST_UNREACH； PARAMETERPROB； REDIRECT； ROUTER_ADVERTISEMENT； SOURCE_QUENCH； TIME_EXCEEDED； ROUTER_SOLICITATION。 **any** 代表任意一种类型。
num	协议号，格式为 INTEGER<1-255>。 **any** 代表任意协议号。

说明

如果不指定任何参数，则显示当前系统中所有的会话数目。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示当前系统的源 IP 地址为 192.168.2.2、目的 IP 地址为 192.168.2.5 的 TCP 会话数目。

```
NetEye@root> show session count any any 192.168.2.2 192.168.2.5 protocol tcp any any any
```

【返回结果】

```
Total: 1 session(s)
```

相关命令

命令名称	描述信息
clear session	删除当前系统的会话。
show session	显示当前系统的会话表。

11 策略命令

黑名单

blacklist

使用 **blacklist** 命令添加黑名单条目。配置成功后， NetEye 将对指定源安全域内特定源 IP 地址或源 MAC 地址的流量进行阻断。

命令

blacklist zone {*src_zone_name* | **any**} {**ip** *src_ip_address* **mask** *net_mask* | **mac** *src_mac_address* } [**timeout** *time*]

语法

src_zone_name	源安全域名称，格式为 WORD<1-15>。 any 表示任意源安全域。
src_ip_address	源 IP 地址，格式为 x.x.x.x。
net_mask	子网掩码，格式为 x.x.x.x。
src_mac_address	源 MAC 地址，格式为 HH:HH:HH:HH:HH:HH。
time	黑名单有效时间，单位为秒，格式为 INTEGER<3-99999999>。

说明

如果不指定 *time* 参数，则表示黑名单永久生效。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加一条未指定源安全域的 IP 地址黑名单条目， IP 地址为 192.168.101.1，子网掩码为 255.255.255.255，有效时间为 5000 秒。

```
NetEye@root-system]blacklisk zone any ip 192.168.1.101 mask
255.255.255.255 timeout 5000
```

相关命令

命令名称	描述信息
show blacklist	显示所有的黑名单条目。
unset blacklist	删除所有的黑名单条目。
unset blacklist zone	删除指定地址类型的黑名单条目。

blacklist export

使用 **blacklist export** 命令导出黑名单。

命令

blacklist export {**zmodem** | **tftp** *ip_tftp file_name* | **sftp** *ip_sftp user_name passwd file_name*}

语法

zmodem	异步文件传输协议，表示使用 zmodem 协议导出黑名单。
tftp	简单文件传输协议，表示将黑名单导出到 TFTP 服务器。
ip_tftp	TFTP 服务器 IP 地址，格式为 x.x.x.x。
file_name	文件名称，格式为 WORD<1-100>。
sftp	安全文件传输协议 ，表示将黑名单导出到 SFTP 服务器。
ip_sftp	SFTP 服务器 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-100>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-100>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 将黑名单导出到 TFTP 服务器，保存文件名为 file1。 TFTP 服务器地址为 192.168.1.100。

```
NetEye@root-system]blacklist export tftp 192.168.1.100 file1
```

范例 2. 将黑名单导出到 SFTP 服务器，保存文件名为 file2。 SFTP 服务器地址为 192.168.1.200，用户名、密码均为 ralph。

```
NetEye@root-system]blacklist export sftp 192.168.1.200 ralph ralph
file2
```

相关命令

命令名称	描述信息
blacklist import	导入黑名单。

blacklist import

使用 **blacklist import** 命令导入黑名单。

命令

blacklist import {**zmodem** | **tftp** *ip_tftp file_name* | **sftp** *ip_sftp user_name passwd file_name*}

语法

zmodem	异步文件传输协议，表示使用 zmodem 协议导入黑名单。
tftp	简单文件传输协议，表示通过 TFTP 服务器导入黑名单。
ip_tftp	TFTP 服务器 IP 地址，格式为 x.x.x.x。
file_name	文件名称，格式为 WORD<1-100>。
sftp	安全文件传输协议，表示通过 SFTP 服务器导入黑名单。
ip_sftp	SFTP 服务器 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-100>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-100>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 通过 TFTP 服务器 192.168.1.100 导入文件名为 file1 的黑名单。

```
NetEye@root-system]blacklist import  tftp 192.168.1.100 file1
```

范例 2. 通过 SFTP 服务器 192.168.1.200 导入文件名为 file2 的黑名单， SFTP 服务器的用户名、密码均为 ralph。

```
NetEye@root-system]blacklist import  sftp 192.168.1.200 ralph ralph
file2
```

相关命令

命令名称	描述信息
blacklist export	导出黑名单。

show blacklist

使用 **show blacklist** 命令显示所有的黑名单条目。

命令

show blacklist

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有的黑名单条目。

```
NetEye@root>show blacklist
```

【返回结果】

```
NO.    Type  IP/MAC              Zone            Valid Time(s)  Packets
Dropped  Bytes Dropped
1      IP    10.20.20.0/24       aa                        0
0
2      IP    10.21.21.0/24       aa                        0
0
3      IP    10.20.28.0/24       aa                        0
0
4      MAC   10:ff:ff:ff:ff:ff    Any                       0
0
```

相关命令

命令名称	描述信息
blacklist	添加黑名单条目。
unset blacklist	删除所有的黑名单条目。
unset blacklist zone	删除指定地址类型的黑名单条目。

unset blacklist

使用 **unset blacklist** 命令删除所有的黑名单条目。

命令

unset blacklist

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除所有的黑名单条目。

```
NetEye@root-system]unset blacklist
```

相关命令

命令名称	描述信息
blacklist	添加黑名单条目。
show blacklist	显示所有的黑名单条目。
unset blacklist zone	删除指定地址类型的黑名单条目。

unset blacklist zone

使用 **unset blacklist zone** 命令删除指定地址类型的黑名单条目。

命令

unset blacklist zone {*src_zone_name* | **any** } {**ip** *src_ip_address* **mask** *net_mask* | **mac** *src_mac_address*}

语法

src_zone_name	源安全域名称，格式为 WORD<1-15>。 **any** 表示任意源安全域。
src_ip_address	源 IP 地址，格式为 x.x.x.x。
net_mask	子网掩码，格式为 x.x.x.x。
src_mac_address	源 MAC 地址，格式为 HH:HH:HH:HH:HH:HH。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除一条未指定源安全域的 IP 地址黑名单条目， IP 地址为 192.168.101.1，子网掩码为 255.255.255.255。

```
NetEye@root-system]unset blacklist zone any ip 192.168.101.1 mask
255.255.255.255
```

相关命令

命令名称	描述信息
blacklist	添加黑名单条目。
show blacklist	显示所有的黑名单条目。
unset blacklist	删除所有的黑名单条目。

访问策略

policy access

使用 **policy access** 命令来添加访问策略。配置成功后， NetEye 可以通过匹配该策略，允许或者拒绝 IP 数据包通过 NetEye。

命令

policy access *policy_name* {*szone* | **any**} {*src_iplist* | **any** | **object** *ipaddr_object_name* | **group** *ipaddr_group_name*} {*dzone* | **any**} {*dst_ iplist* | **any** | **object** *ipaddr_object_name* | **group** *ipaddr_group_name* | **DomainName** *domain_name*} {**any** | **icmp** {*icmp_type* | *icmp_list* | **any**} | {**tcp** | **udp**} {*src_port* | *srcport_range*} {*dst_port* | *dstport_ range*} | **other** *protocol_num* | **protocol-object** *protocol_object_name* | **protocol-group** *protocol_group_name*} {**permit** | **deny**} {**enable** | **disable**} [*pri*]

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
szone	源安全域名称，格式为 WORD<1-15>。 **any** 表示任意安全域。
src_iplist	源 IP 地址列表，格式为 IPV4LIST<1-32>。 **any** 表示任意 IP 地址。
ipaddr_object_name	IP 地址对象名称，格式为 WORD<1-63>。
ipaddr_group_name	IP 地址对象组名称，格式为 WORD<1-63>。
dzone	目的安全域名称，格式为 WORD<1-15>。 **any** 表示任意安全域。
dst_iplist	目的 IP 地址列表，格式为 IPV4LIST<1-32>。 **any** 代表任意 IP 地址。
domain_name	域名，格式为 WORD<1-63>。
icmp_type	ICMP 协议类型，可以设置为： ECHO_and_ECHOREPLY ； DEST_UNREACH ； SOURCE_QUENCH ； REDIRECT ； ROUTER_ADVERTISEMENT ； ROUTER_SOLICITATION ； TIME_EXCEEDED ； PARAMETERPROB ； TIMESTAMP_and_TIMESTAMPREPLY ； INFO_REQUEST_and_INFO_REPLY ； ADDRESS_and_ADDRESSREPLY 。 **any** 表示上述协议类型中的任意一种。

icmp_list	ICMP 的协议类型列表，格式为 WORD<1-256>。列表可以为下述协议类型的任意组合： ECHO_and_ECHOREPLY； INFO_REQUEST_and_INFO_REPLY； TIMESTAMP_and_TIMESTAMPREPLY； ADDRESS_and_ADDRESSREPLY； ROUTER_ADVERTISEMENT； ROUTER_SOLICITATION； DEST_UNREACH； SOURCE_QUENCH； REDIRECT； TIME_EXCEEDED； PARAMETERPROB。
src_port	源端口，格式为 INTEGER<1-65535>。
srcport_range	源端口范围，格式为 LIMIT。
dst_port	目的端口，格式为 INTEGER<1-65535>。
dstport_range	目的端口范围，格式为 LIMIT。
other	除 TCP、 UDP 和 ICMP 之外的协议。
protocol_num	协议号或协议号范围，格式为 NUMBER<1-255>。
protocol_object_name	协议对象名称，格式为 WORD<1-63>。
protocol_group_name	协议对象组名称，格式为 WORD<1-63>。
permit | **deny**	• permit— 允许匹配该访问策略的数据包通过 NetEye • deny— 拒绝匹配该访问策略的数据包通过 NetEye
enable | **disable**	• enable— 启用该访问策略 • disable— 禁用该访问策略
pri	访问策略的优先级，格式为 INTEGER<1-80000>。

说明

1. 如果*pri*设置为1，表示将该访问策略添加到所有策略的前面；如果*pri*省略，表示将该访问策略添加到所有策略的后面。
2. 当在一条策略中指定多个 ICMP 类型时，可用逗号隔开，并且不能重复。
3. 如果选择 **other** 关键字，则指定的协议号和协议号范围不包括 TCP、UDP 和 ICMP，不允许单独设置 1、 6 和 17。例如指定协议号范围是 3-10，实际的协议号范围为 3-5，7-10。
4. 当在一条策略中指定多个其它协议时，协议号范围不能重叠。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 添加访问策略 test1，其优先级为 12，不指定任何传输层协议，状态为启用。配置成功后，允许源安全域为 zone1、目的安全域为 zone2 的 IP 数据包通过 NetEye。

```
NetEye@root-system]policy access test1 zone1 any zone2 any any permit
enable 12
```

范例 2. 添加访问策略 test2，其优先级为空，传输层协议为 ICMP， ICMP 协议类型为 ADDRESS_and_ADDRESSREPLY、 TIMESTAMP_and_TIMESTAMPREPLY，状态为禁用。配置成功后，拒绝源安全域为 zone1、目的安全域为 zone2、目的 IP 地址范围在 192.168.1.100-192.168.1.122 的 IP 数据包通过 NetEye。

```
NetEye@root-system]policy access test2 zone1 any zone2 192.168.1.100-
192.168.1.122 icmp ADDRESS_and_ADDRESSREPLY,
TIMESTAMP_and_TIMESTAMPREPLY deny disable
```

范例 3. 添加访问策略 test3，其优先级为 25，协议为 UDP，状态为启用。配置成功后，允许源安全域为 zone1、源 IP 地址范围在 192.168.1.156-192.168.1.178、目的安全域为 zone2、目的 IP 地址范围在 192.168.1.120-192.168.1.130、源端口范围为 80-92、目的端口范围为 22-45 的 IP 数据包通过 NetEye。

```
NetEye@root-system]policy access test3 zone1 192.168.1.156-
192.168.1.178 zone2 192.168.1.120-192.168.1.130 udp 80-92 22-45 permit
enable 25
```

相关命令

命令名称	描述信息
policy access enable, disable	启用或禁用指定的访问策略。
show policy access	显示访问策略的配置信息。
unset policy access	删除访问策略。

policy access auth

使用 **policy access auth** 命令设置指定访问策略的访问控制。

命令

policy access *policy_name* **auth** {**true** | **false**}

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
auth	匹配该访问策略的数据包需要进行用户认证。
true	**false**	• true— 进行认证 • false— 不进行认证

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show policy access	显示访问策略的配置信息。

policy access dns-proxy

使用 **policy access dns-proxy** 命令启用或禁用匹配指定访问策略数据包的 DNS 代理。

命令

policy access *policy_name* **dns-proxy** {**enable** | **disable**}

语法

policy_name	访问策略名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show policy access	显示访问策略的配置信息。

policy access dynamic-port

使用 **policy access dynamic-port** 命令开启或关闭访问策略中指定服务的动态端口。

命令

policy access *policy_name* **dynamic-port** {**FTP** | **TFTP** | **SIP** | **H.323** | **RTSP** | **Tuxedo** | **Oracle**} {**enable** | **disable**}

语法

policy_name	访问策略名称，格式为 WORD<1-15>。

说明

只有开启访问策略的动态端口后，才能开启指定服务的动态端口。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 开启访问策略 test 中 TFTP 服务的动态端口。

```
NetEye@root-system]policy access test dynamic-port TFTP enable
```

相关命令

命令名称	描述信息
policy access dynamic-port enable, disable	开启或关闭指定访问策略的动态端口打开功能。
policy access dynamic-port protocol mode	设置访问策略中指定服务的端口模式。

policy access dynamic-port enable, disable

使用 **policy access dynamic-port enable, disable** 命令开启或关闭指定访问策略的动态端口打开功能。

命令

policy access *policy_name* **dynamic-port** {**enable** | **disable**}

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
enable | **disable**	• enable—开启动态端口 • disable—关闭动态端口 缺省设置为 enable

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 开启访问策略 test 的动态端口。

```
NetEye@root-system]policy access test dynamic-port enable
```

相关命令

命令名称	描述信息
policy access dynamic-port protocol	设置访问策略中指定服务的动态端口。
policy access dynamic-port protocol mode	设置访问策略中指定服务的端口模式。

policy access dynamic-port protocol

使用 **policy access dynamic-port protocol** 命令设置访问策略中指定服务的动态端口。配置成功后，指定服务的动态端口流量将被 NetEye 转发。

命令

policy access *policy_name* **dynamic-port** {{**FTP** | **RTSP** | **Tuxedo** | **Oracle**} **protocol TCP** | {**TFTP** | **SIP**} **protocol UDP** | **H.323 protocol** {**TCP** | **UDP**}} *port_num_list*

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
port_num_list	端口号列表，格式为 NUMBER<1-10>。

说明

1. 只有开启指定访问策略的动态端口，并将服务的端口模式设置为手动模式后，才能设置该服务的动态端口。
2. 如果要添加多个端口号，需要使用逗号分隔服务端口号。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置访问策略 test 中 tftp 服务的动态端口为 2000 和 3000。

```
NetEye@root-system]policy access test dynamic-port TFTP protocol UDP
2000,3000
```

相关命令

命令名称	描述信息
policy access dynamic-port enable, disable	开启或关闭指定访问策略的动态端口打开功能。
policy access dynamic-port protocol mode	设置访问策略中指定服务的端口模式。

policy access dynamic-port protocol mode

使用 **policy access dynamic-port protocol mode** 命令设置访问策略中指定服务的端口模式。

命令

policy access *policy_name* **dynamic-port** {{**FTP** | **RTSP** | **Oracle**} **protocol TCP** | {**TFTP** | **SIP**} **protocol UDP** | **H.323 protocol** {**TCP** | **UDP**}}**mode** {**auto** | **port**}

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
auto	**port**	• auto—自动模式，表示允许指定服务的所有流量通过。 • port—手动模式，表示允许指定服务的特定端口流量通过。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置访问策略 test 中 tftp 服务的端口模式为自动模式。

```
NetEye@root-system]policy access test dynamic-port TFTP protocol UDP mode auto
```

相关命令

命令名称	描述信息
policy access dynamic-port enable, disable	开启或关闭指定访问策略的动态端口打开功能。

policy access enable, disable

使用 **policy access enable, disable** 命令启用或禁用指定的访问策略。

命令

policy access *policy_name* {**enable** | **disable**}

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
enable | **disable**	• enable— 启用指定的访问策略 • disable— 禁用指定的访问策略

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
policy access	添加访问策略。
show policy access	显示访问策略的配置信息。
unset policy access	删除访问策略。

policy access im-p2p

使用 **policy access im-p2p** 命令启用或禁用对指定 IM-P2P 流量的阻断功能。

命令

policy access *policy_name* **im-p2p** {**QQ** | **BitTorrent** | **DC** | **eMule** | **Gnutella** | **KaZaA** | **ICQ** | **IRC** | **MSNMessenger** | **Yahoo!Messenger**} {**enable** | **disable**}

语法

policy_name	访问策略名称，格式为 WORD<1-15>。

说明

只有启用访问策略中阻断 IM-P2P 流量功能后，才能启用对指定 IM-P2P 流量的阻断功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 启用对访问策略 test 中 ICQ 流量的阻断功能。

```
NetEye@root-system]policy access test im-p2p ICQ enable
```

相关命令

命令名称	描述信息
policy access im-p2p enable, disable	启用或禁用指定访问策略的阻断 IM-P2P 流量功能。
policy access im-p2p protocol	设置阻断访问策略中指定 IM-P2P 服务的特定端口流量。

policy access im-p2p enable, disable

使用 **policy access im-p2p enable, disable** 命令启用或禁用指定访问策略的阻断 IM-P2P 流量功能。

命令

policy access *policy_name* **im-p2p** {**enable** | **disable**}

语法

policy_name	访问策略名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 启用访问策略 test 的阻断 IM-P2P 流量功能。

```
NetEye@root-system]policy access test im-p2p enable
```

相关命令

命令名称	描述信息
policy access im-p2p	启用或禁用对指定 IM-P2P 流量的阻断功能。
policy access im-p2p protocol	设置阻断访问策略中指定 IM-P2P 服务的特定端口流量。

policy access im-p2p protocol

使用 **policy access im-p2p protocol** 命令设置阻断访问策略中指定 IM-P2P 服务的特定端口流量。

命令

policy access *policy_name* **im-p2p** {{**QQ** | **BitTorrent** | **DC** | **eMule** | **Gnutella** | **KaZaA**} **protocol** {**TCP** | **UDP**} | {**ICQ** | **IRC** | **MSNMessenger** | **Yahoo!Messenger**} **protocol TCP**} *port_num_list*

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
port_num_list	端口号列表，格式为 NUMBER<1-10>。

说明

1. 只有启用指定访问策略的阻断 IM-P2P 流量功能，并将指定 IM-P2P 服务的端口模式设置为手动模式后，才能设置阻断该 IM-P2P 服务的特定端口流量。
2. 如果要添加多个端口号，需要使用逗号分隔服务端口号。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置阻断访问策略 test 中 ICQ 服务端口号为 8000 的流量。

```
NetEye@root-system]policy access test im-p2p ICQ protocol TCP 8000
```

相关命令

命令名称	描述信息
policy access im-p2p enable, disable	启用或禁用指定访问策略的阻断 IM-P2P 流量功能。
policy access im-p2p	启用或禁用对指定 IM-P2P 流量的阻断功能。

policy access im-p2p protocol mode

使用 **policy access im-p2p protocol mode** 命令设置访问策略中指定 IM-P2P 服务的端口模式。

命令

policy access *policy_name* **im-p2p** {{**QQ** | **BitTorrent** | **DC** | **eMule** | **Gnutella** | **KaZaA**} **protocol** {**TCP** | **UDP**} | {**ICQ** | **IRC** | **MSNMessenger** | **Yahoo!Messenger**} **protocol TCP**} **mode** {**auto** | **port**}

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
auto	**port**	• auto—自动模式，表示阻断指定 IM-P2P 服务的所有流量。 • port—手动模式，表示阻断指定 IM-P2P 服务的特定端口流量。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置访问策略 test 中 ICQ 服务的端口模式为手动模式。

```
NetEye@root-system]policy access test im-p2p ICQ protocol TCP mode port
```

相关命令

命令名称	描述信息
policy access im-p2p enable, disable	启用或禁用指定访问策略的阻断 IM-P2P 流量功能。
policy access im-p2p	启用或禁用对指定 IM-P2P 流量的阻断功能。

policy access log on, off

使用 **policy access log on, off** 命令为指定的访问策略设置日志记录开关。

命令

policy access *policy_name* **log** {**on** | **off**}

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
on | **off**	• on— 访问策略的日志开关，当有新建会话的数据包匹配到此策略时，发送数据包事件信息到 NetEye 的日志系统 • off— 关闭访问策略的日志开关，当有新建会话的数据包匹配此策略时，不发送数据包事件信息到 NetEye 系统 缺省值为 off

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置访问策略 test 的日志记录为开启状态。

```
NetEye@root-system]policy access test log on
```

policy access nat-linkage

使用 **policy access nat-linkage** 命令启用或禁用匹配指定访问策略数据包的 NAT 与 DNS 联动。

命令

policy access *policy_name* **nat-linkage** {**enable** | **disable**}

语法

policy_name	访问策略名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show policy access	显示访问策略的配置信息。

policy access number

使用 **policy access number** 命令修改指定的访问策略的优先级。配置成功后，可以改变 IP 数据包匹配该策略的先后顺序。

命令

policy access *policy_name* **number** *pri*

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
pri	访问策略优先级，格式为 INTEGER<1-80000>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置访问策略 test 的优先级为 5。

```
NetEye@root-system]policy access test number 5
```

相关命令

命令名称	描述信息
policy access	添加访问策略访问策略。
show policy access	显示访问策略访问策略的配置信息。
unset policy access	删除访问策略访问策略。

policy access permit, deny

使用 **policy access permit, deny** 命令允许或拒绝匹配访问策略的数据包。

命令

policy access *policy_name* {**permit** | **deny**}

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
permit	**deny**	• permit— 允许符合指定访问策略的数据包通过 NetEye • deny—拒绝符合指定访问策略的数据包通过 NetEye

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 允许匹配访问策略 test 的数据包通过 NetEye。

```
NetEye@root-system]policy access test permit
```

相关命令

命令名称	描述信息
policy access	添加访问策略。
show policy access	显示访问策略的配置信息。
unset policy access	删除访问策略。

policy access protocol

使用 **policy access protocol** 命令向指定的访问策略中添加服务。

命令

policy access *policy_name* **protocol** {**icmp** {*icmp_type* | *icmp_list* | **any**} | **other** *protocol_num* | {**tcp | udp**} {*src_port* | *srcport_range*} {*dst_port* | *dstport_ range*} | **protocol-object** *object_name* | **protocol-group** *group_name*}

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
icmp_type	ICMP 协议类型，可以设置为： ECHO_and_ECHOREPLY； DEST_UNREACH； SOURCE_QUENCH； REDIRECT； ROUTER_ADVERTISEMENT； ROUTER_SOLICITATION； TIME_EXCEEDED； PARAMETERPROB； TIMESTAMP_and_TIMESTAMPREPLY； INFO_REQUEST_and_INFO_REPLY； ADDRESS_and_ADDRESSREPLY 。 **any** 表示上述协议类型中的任意一种。
icmp_list	ICMP 的协议类型列表，格式为 WORD<1-256>。列表可以为下述协议类型的任意组合： ECHO_and_ECHOREPLY； INFO_REQUEST_and_INFO_REPLY； TIMESTAMP_and_TIMESTAMPREPLY； ADDRESS_and_ADDRESSREPLY； ROUTER_ADVERTISEMENT； ROUTER_SOLICITATION； DEST_UNREACH； SOURCE_QUENCH； REDIRECT； TIME_EXCEEDED； PARAMETERPROB。
other	除 TCP、 UDP 和 ICMP 之外的协议。
protocol_num	协议号或协议号范围，格式为 NUMBER<1-255>。
src_port	源端口，格式为 INTEGER<1-65535>。
srcport_range	源端口范围，格式为 LIMIT。

dst_port	目的端口，格式为 INTEGER<1-65535>。
dstport_range	目的端口范围，格式为 LIMIT。
object_name	协议对象名称，格式为 WORD<1-63>。
group_name	协议对象组名称，格式为 WORD<1-63>。

说明

如果选择 **other** 关键字，则指定的协议号和协议号范围不包括 TCP、 UDP 和 ICMP，不允许单独设置 1、 6 和 17。例如指定协议号范围是 3-10，实际的协议号范围为 3-5， 7-10。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 在访问策略 test1 中添加 ICMP 协议，不指定 ICMP 协议类型。

```
NetEye@root-system]policy access test1 protocol icmp any
```

范例 2. 在访问策略 test2 中添加 TCP 协议，源端口号为 5，目的端口号为 63。

```
NetEye@root-system]policy access test2 protocol tcp 5 63
```

相关命令

命令名称	描述信息
policy access	添加访问策略。
show policy access	显示访问策略的配置信息。
unset policy access	删除访问策略。

policy access qos

使用 **policy access qos** 命令设置指定访问策略的 QoS 规则。

命令

policy access *policy_name* **qos** *qos_name*

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
qos_name	QoS 规则名称，格式为 WORD<1-64>。

说明

只有启用访问策略的 QoS 功能后，管理员才能修改指定访问策略的 QoS 规则。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 修改访问策略 test 的 QoS 规则为 qos_rule。

```
NetEye@root-system]policy access test qos qos_rule
```

相关命令

命令名称	描述信息
policy access bandwidth	启用或禁用指定访问策略的 QoS 功能。
unset policy access qos	删除指定访问策略的 QoS 规则。

policy access schedule

使用 **policy access schedule** 命令设置指定访问策略的有效期。配置成功后，该策略仅在有效时间内处于可用状态。

命令

policy access *policy_name* **schedule start-week** *start_weekday* **end-week** *end_weekday time_range*

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
start_weekday	以星期为单位的访问策略的开始日期，格式为 INTEGER<1-7>。 1 Monday 2 Tuesday 3 Wednesday 4 Thursday 5 Friday 6 Saturday 7 Sunday
end_weekday	以星期为单位的访问策略的终止日期，格式为 INTEGER<1-7>。 1 Monday 2 Tuesday 3 Wednesday 4 Thursday 5 Friday 6 Saturday 7 Sunday
time_range	访问策略的有效时间段，格式为 <HH:MM:SS-HH:MM:SS>。

说明

1. 如果访问策略不设置生效时间，则认为该策略在任何时间都有效。
2. 当访问策略设置多个有效时间段时，各个时间段之间用逗号隔开。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置访问策略 test 的有效期为周一至周五的 8:30:00-17:30:00。

```
NetEye@root-system]policy access test schedule start-week 1 end-week 5
8:30:00-17:30:00
```

相关命令

命令名称	描述信息
policy access timeout	设置指定的访问策略的会话超时时间。
unset policy access timeout, schedule	删除指定的访问策略的高级设置。

policy access sourceip, desip

使用 **policy access sourceip, desip** 命令为指定的访问策略添加源 IP 或目的 IP 地址。

命令

policy access *policy_name* {**sourceip** {**object** *ipaddr_object_name* | **group** *ipaddr_group_name* | **address** *ip_list* | *ip_address* **netmask** *ip_mask*} | **desip** {**object** *ipaddr_object_name* | **group** *ipaddr_group_name* | **DomainName** *domain_name* | **address** *ip_list* | *ip_address* **netmask** *ip_mask*}}

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
sourceip | **desip**	• sourceip— 表示添加源 IP 地址 • desip— 表示添加目的 IP 地址
ipaddr_object_name	IP 地址对象名称，格式为 WORD<1-63>。
ipaddr_group_name	IP 地址对象组名称，格式为 WORD<1-63>。
domain_name	域名，格式为 WORD<1-63>。
ip_list	源 / 目的 IP 地址列表，格式为 IPV4LIST<1-32>。
ip_address	源 / 目的 IP 地址，格式为 x.x.x.x。
ip_mask	源 / 目的 IP 地址的子网掩码，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 为访问策略 test1 添加源 IP 地址，引用 IP 地址对象 OBJ。

```
NetEye@root-system]policy access test1 sourceip object OBJ
```

范例 2. 为访问策略 test2 添加源 IP 地址 192.168.1.112 及其子网掩码 255.255.255.0。

```
NetEye@root-system]policy access test2 sourceip 192.168.1.112 netmask
255.255.255.0
```

相关命令

命令名称	描述信息
show policy access	显示访问策略的配置信息。

policy access ssl

使用 **policy access ssl** 命令在访问策略启用阻断非标准 SSL 端口上的 SSL 隧道流量功能的情况下，是否允许 TCP 端口上的指定类型流量。

命令

policy access *policy_name* **ssl** {**POP3S** | **SMTPS** | **IMAPS** | **LDAPS**} {**enable** | **disable**}

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
POP3S | **SMTPS** | **IMAPS** | **LDAPS**	• POP3S—TCP 995 端口上的 POP3S 流量 • SMTPS—TCP 465 端口上的 SMTPS 流量 • IMAPS—TCP 993 端口上的 IMAPS 流量 • LDAPS—TCP 636 端口上的 LDAPS 流量
enable | **disable**	• enable—启用指定的选项 • disable—禁用指定的选项

说明

要允许 TCP 端口上的指定类型流量，必须先启用阻断非标准 SSL 端口上的 SSL 隧道流量功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 在访问策略 test 启用阻断非标准 SSL 端口上的 SSL 隧道流量功能的情况下，允许 TCP 995 端口上的 POP3S 流量。

```
NetEye@root-system] policy access test ssl POP3S enable
```

相关命令

命令名称	描述信息
policy access ssl enable, disable	启用或禁用阻断非标准 SSL 端口上的 SSL 隧道流量功能。
show policy access	显示访问策略的配置信息。

policy access ssl enable, disable

使用 **policy access ssl enable, disable** 命令启用或禁用阻断非标准 SSL 端口上的 SSL 隧道流量功能。

命令

policy access *policy_name* **ssl** {**enable** | **disable**}

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
enable | **disable**	• enable—启用阻断非标准 SSL 端口上的 SSL 隧道流量功能 • disable—禁用阻断非标准 SSL 端口上的 SSL 隧道流量功能 缺省设置为 disable

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
policy access ssl	在访问策略启用阻断非标准 SSL 端口上的 SSL 隧道流量功能的情况下，允许 TCP 端口上的指定类型流量。
show policy access	显示访问策略的配置信息。

policy access timeout

使用 **policy access timeout** 命令设置指定的访问策略的会话超时时间。

命令

policy access *policy_name* **timeout** {**tcp** {**syn** | **fin** | **ested** | **close**} | **udp** | **icmp**} *exceed_time*

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
syn | **fin** | **ested** | **close**	• syn—表示设置 TCP 会话 SYN 状态的超时时间 缺省值为 300 秒 • fin—表示设置 TCP 会话 FIN 状态的超时时间 缺省值为 600 秒 • ested—表示设置 TCP 会话 ESTED 状态的超时时间 缺省值为 3600 秒 • close—表示设置 TCP 会话 CLOSE 状态的超时时间 缺省值为 10 秒
udp	表示设置 UDP 会话的超时时间。 缺省值为 300 秒
icmp	表示设置 ICMP 会话的超时时间。 缺省值为 3 秒
exceed_time	超时时间，格式为 INTEGER<1-99999999>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 设置访问策略 test1 的 TCP 会话 SYN 状态超时时间为 15000 秒。

```
NetEye@root-system]policy access test1 timeout tcp syn 15000
```

范例 2. 设置访问策略 test2 的 ICMP 会话超时时间为 300 秒。

```
NetEye@root-system]policy access test2 timeout icmp 300
```

相关命令

命令名称	描述信息
policy access schedule	设置指定访问策略的有效期。
unset policy access timeout, schedule	删除指定的访问策略的高级设置。

policy access tunnel

使用 **policy access tunnel** 命令设置当数据包匹配到动作为允许的访问策略后，将被转发到的 VPN 隧道或隧道组。

命令

policy access *policy_name* **tunnel** {*tunnel_name* | *tunnel_group_name*}

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
tunnel_name	VPN 隧道名称，格式为 WORD<1-15>。
tunnel_group_name	隧道组名称，格式为 WORD<1-127>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 当数据包匹配到动作为允许的访问策略 test 后，其将被 VPN 隧道 tunnel1 转发。

```
NetEye@root-system]policy access test tunnel tunnel1
```

show policy access

使用 **show policy access** 命令显示访问策略的配置信息。

命令

show policy access [*policy_name*]

语法

policy_name	访问策略名称，格式为 WORD<1-15>。

说明

如果不指定 *policy_name* 参数，则显示所有访问策略的配置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示访问策略 test 的配置信息。

```
NetEye@root>show policy access test
```

【返回结果】

```
Name: test
  State: disable
  Action: permit
  Auth: on
  DNS Proxy: on
  DNS NAT: off
  QoS Rule: test
  Logging: on
  Tunnel:
```

```
From: Any
To: Any

Source IP Address:
  IPMask        10.3.3.0/24

Destination IP Address:
  IPMask        10.4.4.0/24

Services:
  Any

Timeout:
  ICMP       2
  UDP        300
  TCP_SYN    300
  TCP_FIN    3
  TCP_ESTED 3600
  TCP_CLOSE  5

Schedule:
  -
```

相关命令

命令名称	描述信息
policy access	添加访问策略。
policy access enable, disable	启用或禁用指定的访问策略。
unset policy access	删除访问策略。

unset policy access

使用 **unset policy access** 命令删除访问策略。

命令

unset policy access [*policy_name*]

语法

policy_name	访问策略名称，格式为 WORD<1-15>。

说明

如果不指定 *policy_name* 参数，则删除所有的访问策略。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
policy access	添加访问策略。
policy access enable, disable	启用或禁用指定的访问策略。
show policy access	显示访问策略的配置信息。

unset policy access timeout, schedule, tunnel

使用 **unset policy access timeout, schedule, tunnel** 命令删除指定的访问策略的高级设置。

命令

unset policy access *policy_name* {**timeout** | **schedule** | **tunnel**}

语法

policy_name	访问策略名称，格式为 WORD<1-15>。
timeout | **schedule** | **tunnel**	• timeout—删除指定的访问策略的超时设置 • schedule—删除指定的访问策略的有效期设置 • tunnel—删除指定访问策略与 VPN 隧道或隧道组的绑定

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除访问策略 test 的有效期设置。

```
NetEye@root-system]unset policy access test schedule
```

相关命令

命令名称	描述信息
policy access schedule	设置指定访问策略的有效期。
policy access timeout	设置指定的访问策略的会话超时时间。
policy access tunnel	设置当数据包匹配到动作为允许的访问策略后，将被转发到的 VPN 隧道或隧道组。

unset policy access qos

使用 **unset policy access qos** 命令删除指定访问策略的 QoS 规则。

命令

unset policy access *policy_name* **qos**

语法

policy_name	访问策略名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除访问策略 test 的 QoS 规则。

```
NetEye@root-system]unset policy access test qos
```

相关命令

命令名称	描述信息
policy access qos	设置指定访问策略的 QoS 规则。

多播策略

policy multicast

使用 **policy multicast** 命令添加多播策略。配置成功后， NetEye 可以通过匹配多播策略，允许或者拒绝多播数据信息流通过 NetEye。

命令

policy multicast *policy_name* {*szone* | **any**} {*source_iplist* | **any**} {*group_iplist* | **any**} **allowedzone** {*dzone_list* | **any**} {**enable** | **disable**} [*pri*]

语法

policy_name	多播策略名称，格式为 WORD<1-15>。
szone	源安全域名称，格式为 WORD<1-15>。 **any** 代表任何安全域。
source_iplist	源 IP 地址列表，格式为 IPV4LIST<1-32>。 **any** 代表的范围为 0.0.0.0-223.255.255.255。
group_iplist	组 IP 地址列表，格式为 IPV4LIST<1-32>。 **any** 代表的范围为 224.0.0.0-239.255.255.255。
allowedzone	表示多播策略的目的安全域。
dzone_list	目的安全域名称列表，格式为 WORD<1-255>。
enable | **disable**	• enable— 启用添加的多播策略 • disable— 禁用添加的多播策略
pri	*pri* 为可选项，表示策略优先级，格式为 INTEGER<1-80000>。

说明

1. 如果 *pri* 设置为 1，表示将该多播策略添加到所有策略的前面；如果 *pri* 省略，表示将该多播策略添加到所有策略的后面。
2. 在默认情况下，不允许多播数据信息流通过 NetEye。如果要允许多播数据信息流通过 NetEye，必须配置多播策略。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加多播策略 test，其优先级为 1。配置成功后，当 IP 地址范围在 0.0.0.0-255.255.255.255 的多播数据流从安全域 SzoneA 进入 NetEye，要发送到 IP 地址范围在 224.0.0.0-239.255.255.255 的设备上 ， 允许通过安全域 DzoneA 和 DzoneB 发送到目的设备。

```
NetEye@root-system]policy multicast test SzoneA any any allowedzone
DzoneA,DzoneB enable 1
```

相关命令

命令名称	描述信息
policy multicast allowedzone	为多播策略追加目的安全域。
policy multicast enable, disable	启用或者禁用多播策略。
policy multicast number	更改多播策略的优先级。
show policy multicast	显示多播策略。
unset policy multicast	删除多播策略。

policy multicast allowedgip

使用 **policy multicast allowedgip** 命令为多播策略追加组 IP 地址。

命令

policy multicast *policy_name* **allowedgip** *group_iplist*

语法

policy_name	多播策略名称，格式为 WORD<1-15>。
allowedgip	表示多播策略的组 IP 地址。
group_iplist	组 IP 地址列表，格式为 IPV4LIST<1-32>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 为多播策略 test 追加组 IP 地址 232.1.1.1。

```
NetEye@root-system]policy multicast test allowedgip 232.1.1.1
```

相关命令

命令名称	描述信息
policy multicast allowedsip	为多播策略追加源 IP 地址。
policy multicast allowedmask	为多播策略追加源 / 组 IP 地址及其子网掩码。

policy multicast allowedmask

使用 **policy multicast allowedmask** 命令为多播策略追加源 / 组 IP 地址及其子网掩码。

命令

policy multicast *policy_name* **allowedmask** {**Sip | Gip**} **subnet** *subnet_address subnet_mask*

语法

policy_name	多播策略名称，格式为 WORD<1-15>。
allowedmask	表示多播策略的源 / 组 IP 地址及其子网掩码。
subnet_address	多播策略的源 / 组 IP 地址，格式为 x.x.x.x。
subnet_mask	源 / 组 IP 地址的子网掩码，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 为多播策略 test 追加源 IP 地址 10.1.1.2 及其子网掩码 255.255.255.255。

```
NetEye@root-system]policy multicast test allowedmask Sip subnet
10.1.1.2 255.255.255.255
```

相关命令

命令名称	描述信息
policy multicast allowedsip	为多播策略追加源 IP 地址。
policy multicast allowedgip	为多播策略追加组 IP 地址。

policy multicast allowedsip

使用 **policy multicast allowedsip** 命令为多播策略追加源 IP 地址。

命令

policy multicast *policy_name* **allowedsip** *source_iplist*

语法

policy_name	多播策略名称，格式为 WORD<1-15>。
allowedsip	表示多播策略的源 IP 地址。
source_iplist	源 IP 地址列表，格式为 IPV4LIST<1-32>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 为多播策略 test 追加源 IP 地址 10.1.1.2。

```
NetEye@root-system]policy multicast test allowedsip 10.1.1.2
```

相关命令

命令名称	描述信息
policy multicast allowedgip	为多播策略追加组 IP 地址。
policy multicast allowedmask	为多播策略追加源 / 组 IP 地址及其子网掩码。

policy multicast allowedzone

使用 **policy multicast allowedzone** 命令为多播策略追加目的安全域。

命令

policy multicast *policy_name* **allowedzone** *dzone*

语法

policy_name	多播策略名称，格式为 WORD<1-15>。
allowedzone	表示多播策略的目的安全域。
dzone	目的安全域名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 为 test 多播策略追加目的安全域 ZoneA。

```
NetEye@root-system]policy multicast test allowedzone ZoneA
```

相关命令

命令名称	描述信息
policy multicast	添加多播策略。
show policy multicast	显示多播策略。
unset policy multicast	删除多播策略。

policy multicast enable, disable

使用 **policy multicast enable, disable** 命令启用或禁用指定的多播策略。

命令

policy multicast *policy_name* {**enable** | **disable**}

语法

policy_name	多播策略名称，格式为 WORD<1-15>。
enable | **disable**	• enable— 启用指定的多播策略 • disable— 禁用指定的多播策略

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
policy multicast	添加多播策略。
show policy multicast	显示多播策略。
unset policy multicast	删除多播策略。

policy multicast number

使用 **policy multicast number** 命令更改多播策略的优先级。优先级的数值越小代表其级别越高。在进行多播策略匹配时，优先匹配级别高的策略。

命令

policy multicast *policy_name* **number** *pri*

语法

policy_name	多播策略名称，格式为 WORD<1-15>。
pri	表示策略的优先级，格式为 INTEGER<1-80000>。

说明

如果 *pri* 设置为 1，表示将该多播策略添加到所有策略的前面。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 更改 test 多播策略的优先级为 3。

```
NetEye@root-system]policy multicast test number 3
```

相关命令

命令名称	描述信息
policy multicast	添加多播策略。
show policy multicast	显示多播策略。
unset policy multicast	删除多播策略。

policy multicast qos

使用 **policy multicast qos** 命令设置多播策略的 QoS 规则。

命令

policy multicast *policy_name* **qos** *qos_name*

语法

policy_name	多播策略名称，格式为 WORD<1-15>。
qos_name	QoS 规则名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置多播策略 test 的 QoS 规则， QoS 规则名称为 rule。

```
NetEye@root-system]policy multicast test qos rule
```

show policy multicast

使用 **show policy multicast** 命令显示多播策略。

命令

show policy multicast [*policy_name*]

语法

policy_name	多播策略名称，格式为 WORD<1-15>。

说明

如果不指定 *policy_name*，则显示所有的多播策略。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示名称为 test 的多播策略。

```
NetEye@root>show policy multicast test
```

【返回结果】

```
Multicast security policy test:
  SZone: Any
  State: enable
  Sip List:
      Any
  Gip List:
      Any
  AllowedZone:
      Any
```

相关命令

命令名称	描述信息
policy multicast	添加多播策略。
unset policy multicast	删除多播策略。

unset policy multicast

使用 **unset policy multicast** 命令删除多播策略。

命令

unset policy multicast [*policy_name*]

语法

policy_name	多播策略名称，格式为 WORD<1-15>。

说明

如果不指定 *policy_name*，则删除所有多播策略。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除名称为 test 的多播策略。

```
NetEye@root-system]unset policy multicast test
```

相关命令

命令名称	描述信息
policy multicast	添加多播策略。
show policy multicast	显示多播策略。

unset policy multicast allowedzone

使用 **unset policy multicast allowedzone** 命令删除多播策略的安全域。

命令

unset policy multicast *policy_name* **allowedzone** *dzone*

语法

policy_name	多播策略名称，格式为 WORD<1-15>。
allowedzone	表示多播策略的目的安全域。
dzone	目的安全域名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除 test 多播策略的目的安全域 ZoneA。

```
NetEye@root-system]unset policy multicast test allowedzone ZoneA
```

相关命令

命令名称	描述信息
policy multicast allowedzone	为多播策略追加安全域。
policy multicast	添加多播策略。
show policy multicast	显示多播策略。
unset policy multicast	删除多播策略。

unset policy multicast qos

使用 **unset policy multicast qos** 命令禁用多播策略的 QoS 规则。

命令

unset policy multicast *policy_name* **qos**

语法

policy_name	多播策略名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 禁用多播策略 test 的 QoS 规则。

```
NetEye@root-system] unset policy multicast test qos
```

会话策略

policy session

使用 **policy session** 命令添加指定协议类型的会话限制策略。配置成功后，如果符合此策略的会话数达到了指定的阈值，则不允许再建立新的会话。

命令

policy session *policy_name* {*src_zone* | **any**} {*dst_zone* | **any**} {**sourceip** *sip_list* | **object** {*ipaddr_object_name* | *ipaddr_group_name* | **any**}} {**desip** *dip_list* | **object** {*ipaddr_object_name* | *ipaddr_group_name* | **any**}} {**any** | **icmp** {*icmp_type* | **any**} | **other** {*protocol_num* | *protocol_range* | **any**} | {**tcp | udp**} {*port_num* | *port_range* | **any**}} *threshold_value* **type** {**srcip** | **dstip** | **policy**} {**enable** | **disable**} {**alert** [**drop**] | **drop** [**alert**]}

语法

policy_name	策略名称，格式为 WORD<1-15>。
src_zone	源安全域名称，格式为 WORD<1-15>。 **any** 代表任意安全域。
dst_zone	目的安全域名称，格式为 WORD<1-15>。 **any** 代表任意安全域。
sip_list	源 IP 地址列表，格式为 IPV4LIST。 **any** 代表任意 IP 地址。
ipaddr_object_name	IP 地址对象名称，格式为 WORD<1-63>。
ipaddr_group_name	IP 地址对象组名称，格式为 WORD<1-63>。
dip_list	目的 IP 地址列表，格式为 IPV4LIST。 **any** 代表任意 IP 地址。
icmp_type	ICMP 的协议类型，设置个数为 1，可以设置为： ECHO_and_ECHOREPLY； INFO_REQUEST_and_INFO_REPLY； TIMESTAMP_and_TIMESTAMPREPLY； ADDRESS_and_ADDRESSREPLY； **any** 代表上述协议类型中任意一种。
other	除 TCP、 UDP 和 ICMP 之外的协议。
protocol_num	other 类型协议的协议号，格式为 INTEGER<1-255>。 **any** 代表任意协议号。
protocol_range	other 类型协议的协议号范围，格式为 LIMIT。
port_num	端口号，格式为 INTEGER<1-65535>。 **any** 代表任意端口号。
port_range	端口号范围，格式为 LIMIT。

threshold_value	阈值，表示并发会话的最大数目，格式为 INTEGER <1-99999999>。
srcip | **dstip** | **policy**	• srcip— 限制来自相同源 IP 地址的并发会话数目 • dstip— 限制来自相同目的 IP 地址的并发会话数目 • policy— 同时限制来自相同源 IP 地址和目的 IP 地址的并发会话数目
enable | **disable**	• enable— 启用该策略 • disable— 禁用该策略
alert | **drop**	• alert— 发送报警事件 • drop— 丢弃攻击数据包

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加协议类型为 DDP （数据报传送协议，其对应的协议号为 37）的会话限制策略 test，如果源安全域 szone 中源 IP 地址列表为 192.168.1.126-192.168.1.134 和目的安全域 dzone 中目的 IP 地址为 192.168.1.154-192.168.1.188 的会话数超过 50000000，则不允许再建立新的会话，并发送报警事件。

```
NetEye@root-system]policy session test szone dzone sourceip
192.168.1.126-192.168.1.134 desip 192.168.1.154-192.168.1.188 other 37
50000000 type policy enable alert
```

相关命令

命令名称	描述信息
show policy session	查看会话限制策略。

policy session alloweddipaddress, alloweddipobject

使用 **policy session alloweddipaddress, alloweddipobject** 命令为会话限制策略追加目的 IP 地址。

命令

policy session *policy_name* {**alloweddipaddress** *dip_list* | **alloweddipobject** {*ipaddr_object_name* | *ipaddr_group_name*}}

语法

policy_name	策略名称，格式为 WORD<1-15>。
dip_list	目的 IP 地址列表，格式为 IPV4LIST<1-32>。
ipaddr_object_name	IP 地址对象名称，格式为 WORD<1-63>。
ipaddr_group_name	IP 地址对象组名称，格式为 WORD<1-63>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 为会话限制策略 test 追加目的 IP 地址，引用 IP 地址对象 OBJ。

```
NetEye@root-system] policy session test alloweddipobject OBJ
```

相关命令

命令名称	描述信息
policy session allowedsipaddress, allowedsipobject	为会话限制策略追加源 IP 地址。
policy session allowedmask	为会话限制策略追加源 / 目的 IP 地址及其子网掩码。

policy session allowedmask

使用 **policy session allowedmask** 命令为会话限制策略追加源 / 目的 IP 地址及其子网掩码。

命令

policy session *policy_name* **allowedmask** {**Sip | Dip**} **subnet** *subnet_address subnet_mask*

语法

policy_name	策略名称，格式为 WORD<1-15>。
subnet_address	源 / 目的 IP 地址，格式为 x.x.x.x。
subnet_mask	源 / 目的 IP 地址的子网掩码，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 为会话限制策略 test 追加源 IP 地址 10.1.1.2 及其子网掩码 255.255.255.255。

```
NetEye@root-system]policy session test allowedmask Sip subnet 10.1.1.2
255.255.255.255
```

相关命令

命令名称	描述信息
policy session alloweddipaddress, alloweddipobject	为会话限制策略追加目的 IP 地址。
policy session allowedsipaddress, allowedsipobject	为会话限制策略追加源 IP 地址。

policy session allowedsipaddress, allowedsipobject

使用 **policy session allowedsipaddress, allowedsipobject** 命令为会话限制策略追加源 IP 地址。

命令

policy session *policy_name* {**allowedsipaddress** *sip_list* | **allowedsipobject** {*ipaddr_object_name* | *ipaddr_group_name*}}

语法

policy_name	策略名称，格式为 WORD<1-15>。
sip_list	源 IP 地址列表，格式为 IPV4LIST<1-32>。
ipaddr_object_name	IP 地址对象名称，格式为 WORD<1-63>。
ipaddr_group_name	IP 地址对象组名称，格式为 WORD<1-63>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 为会话限制策略 test 追加源 IP 地址 10.1.1.2。

```
NetEye@root-system]policy session test allowedsipaddress 10.1.1.2
```

相关命令

命令名称	描述信息
policy session alloweddipaddress, alloweddipobject	为会话限制策略追加目的 IP 地址。
policy session allowedmask	为会话限制策略追加源 / 目的 IP 地址及其子网掩码。

policy session enable, disable

使用 **policy session enable, disable** 命令启用或者禁用指定的会话限制策略。

命令

policy session *policy_name* {**enable** | **disable**}

语法

policy_name	策略名称，格式为 WORD<1-15>。
enable | **disable**	• enable— 启用指定的策略 • disable— 禁用指定的策略

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 禁用会话限制策略 test。

```
NetEye@root-system]policy session test disable
```

相关命令

命令名称	描述信息
show policy session	查看会话限制策略。

policy session protocol

使用 **policy session protocol** 命令为指定的会话限制策略追加特定类型的协议。

命令

policy session *policy_name* **protocol** {**icmp** {*icmp_type* | **any**} | **other** {*protocol_num* | *protocol_range*} | {**tcp | udp**} {*port_num* | *port_range*}}

语法

policy_name	策略名称，格式为 WORD<1-15>。
icmp_type	ICMP 的协议类型，设置个数为 1，可以设置为： ECHO_and_ECHOREPLY； INFO_REQUEST_and_INFO_REPLY； TIMESTAMP_and_TIMESTAMPREPLY； ADDRESS_and_ADDRESSREPLY； **any** 代表上述协议类型中任意一种。
other	除 TCP、 UDP 和 ICMP 之外的协议。
protocol_num	other 类型协议的协议号，格式为 INTEGER<1-255>。
protocol_range	other 类型协议的协议号范围，格式为 LIMIT。
port_num	端口号，格式为 INTEGER<1-65535>。
port_range	端口号范围，格式为 LIMIT。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 为会话限制策略 test 追加 DDP 协议，其协议号为 37。

```
NetEye@root-system]policy session test protocol other 37
```

相关命令

命令名称	描述信息
show policy session	查看会话限制策略。

show policy session

使用 **show policy session** 命令查看会话限制策略。

命令

show policy session [*policy_name*]

语法

policy_name	策略名称，格式为 WORD<1-15>。

说明

如果不指定 *policy_name* 参数，则显示所有的会话限制策略。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有的会话限制策略。

```
NetEye@root>show policy session
```

【返回结果】

```
Session-limit policy :
Name            Szone  Dzone  Sip            Dip            Services
Type    Thres  Action  State
test              Any    Any    192.168.1.126-~   192.168.1.154-~
other:37    Policy  5000~  Alert   Enable
```

相关命令

命令名称	描述信息
policy session	添加指定协议类型的会话限制策略。

unset policy session

使用 **unset policy session** 命令删除会话限制策略。

命令

unset policy session [*policy_name*]

语法

policy_name	策略名称，格式为 WORD<1-15>。

说明

如果不指定 *policy_name* 参数，则删除所有的会话限制策略。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除会话限制策略 test。

```
NetEye@root-system]unset policy session test
```

相关命令

命令名称	描述信息
show policy session	查看会话限制策略。

unset policy session protocol

使用 **unset policy session protocol** 命令将指定会话限制策略的协议类型设置为任意类型。

命令

unset policy session *policy_name* **protocol**

语法

policy_name	策略名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 将会话限制策略 test 的协议类型设置为任意类型。

```
NetEye@root-system]unset policy session test protocol
```

相关命令

命令名称	描述信息
show policy session	查看会话限制策略。

安全策略

policy security

使用 **policy security** 命令来添加安全策略。配置成功后， NetEye 可以通过匹配该策略，对 IP 数据包进行深度检测。

命令

policy security *policy_name* {**any** | *szone*} {**any** | **Obj** {*ipaddr_object_name* | *ipaddr_group_name*} | **Rang** *sip_ list* | **sub** *source_ipaddress net_mask*} {**any** | *dzone*} {**any** | **Obj** {*ipaddr_object_name* | *ipaddr_group_name*} | **Rang** *dip_ list* | **sub** *destination_ipaddress net_mask*} {**Default** | *profile_name*} [*pri*]

语法

policy_name	安全策略名称，格式为 WORD<1-15>。
szone	源安全域名称，格式为 WORD<1-15>。 **any** 表示任意安全域。
ipaddr_object_name	IP 地址对象名称，格式为 WORD<1-63>。
ipaddr_group_name	IP 地址对象组名称，格式为 WORD<1-63>。
sip_list	源 IP 地址列表，格式为 IPV4LIST<1-32>。 **any** 表示任意 IP 地址。
source_ipaddress	源 IP 地址，格式为 x.x.x.x。
net_mask	子网掩码，格式为 x.x.x.x。
dzone	目的安全域名称，格式为 WORD<1-15>。 **any** 表示任意安全域。
dip_list	目的 IP 地址列表，格式为 IPV4LIST<1-32>。 **any** 表示任意 IP 地址。
destination_ipaddress	目的 IP 地址，格式为 x.x.x.x。
Default	系统默认的防护配置名称。
profile_name	防护配置名称，格式为 WORD<1-10>。
pri	安全策略的优先级，格式为 INTEGER<1-79999>。

说明

如果 *pri* 设置为 1，表示将该安全策略添加到所有策略的前面；如果 *pri* 省略，表示将该安全策略添加到所有策略的后面。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加安全策略 test，允许源安全域为 zone1、源 IP 地址为 192.168.1.0、子网掩码为 255.255.255.0、目的安全域为 zone2、目的 IP 地址为任意，启用系统默认的防护配置。配置成功后，匹配条件的 IP 数据包可以通过 NetEye。

```
NetEye@root-system]policy security test zone1 sub 192.168.1.0
255.255.255.0  zone2 any Default
```

相关命令

命令名称	描述信息
policy security enable, disable	启用或禁用指定的安全策略。
show policy security	显示安全策略的状态信息。
unset policy security	删除安全策略。

policy security enable, disable

使用 **policy security enable, disable** 命令启用或禁用指定的安全策略。

命令

policy security *policy_name* {**enable** | **disable**}

语法

policy_name	安全策略名称，格式为 WORD<1-15>。
enable | **disable**	• enable— 启用指定的安全策略 • disable— 禁用指定的安全策略

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 启用安全策略 test。

```
NetEye@root-system]policy security test enable
```

相关命令

命令名称	描述信息
policy security	添加安全策略。
show policy security	显示安全策略的状态信息。
unset policy security	删除安全策略。

policy security Obj, Rang, sub

使用 **policy security Obj, Rang, sub** 命令修改指定安全策略的 IP 地址。

命令

policy security *policy_name* {**Source** | **Destination**} {**Obj** {*ipaddr_object_name* | *ipaddr_group_name*} | **Rang** *iplist* | **sub** *ipaddress net_mask*}

语法

policy_name	安全策略名称，格式为 WORD<1-15>。
ipaddr_object_name	IP 地址对象名称，格式为 WORD<1-63>。
ipaddr_group_name	IP 地址对象组名称，格式为 WORD<1-63>。
iplist	IP 地址列表，格式为 IPV4LIST<1-32>。
ipaddress	IP 地址，格式为 x.x.x.x。
net_mask	子网掩码，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 修改安全策略 test 的源 IP 地址，修改后的源 IP 地址为 192.168.1.0，子网掩码为 255.255.255.0。

```
NetEye@root-system] policy security test Source sub 192.168.1.0
255.255.255.0
```

相关命令

命令名称	描述信息
policy security number	修改指定安全策略的优先级。
policy security profile	修改指定安全策略引用的防护配置策略。
policy security zone	修改指定安全策略的安全域。

policy security number

使用 **policy security number** 命令修改指定安全策略的优先级。配置成功后，可以改变 IP 数据包匹配该策略的先后顺序。

命令

policy security *policy_name* **number** *pri*

语法

policy_name	安全策略名称，格式为 WORD<1-15>。
pri	安全策略优先级，格式为 INTEGER<1-79999>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置安全策略 test 的优先级为 5。

```
NetEye@root-system]policy security test number 5
```

相关命令

命令名称	描述信息
policy security Obj, Rang, sub	修改指定安全策略的 IP 地址。
policy security profile	修改指定安全策略引用的防护配置策略。
policy security zone	修改指定安全策略的安全域。

policy security profile

使用 **policy security profile** 命令修改指定安全策略引用的防护配置。

命令

policy security *policy_name* **profile** {**Default** | *profile_name*}

语法

policy_name	安全策略名称，格式为 WORD<1-15>。
default	系统默认的防护配置。
profile_name	防护配置名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 将安全策略 test 引用的防护配置修改为 profile1。

```
NetEye@root-system]policy security test profile profile1
```

相关命令

命令名称	描述信息
policy security Obj, Rang, sub	修改指定安全策略的 IP 地址。
policy security number	修改指定安全策略的优先级。
policy security zone	修改指定安全策略的安全域。

policy security service AUTO

使用 **policy security service AUTO** 命令设置服务的识别方式为自动识别。

命令

policy security *policy_name* **service** {{**http | smtp | pop3 | imap | ftp | telnet | msn | nntp | x11 | oracle | mysql | pop2 | mssql | finger**} **TCP |** {**dns** | **sip** | **tftp**} **UDP |** {**snmp** | **netbios** | **smb** | **wins** | **sunrpc** | **dcerpc**} {**TCP** | **UDP**}} **AUTO**

语法

policy_name	安全策略名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 在安全策略 test 中设置 http 服务的识别方式为自动识别。

```
NetEye@root-system]policy security test service http TCP AUTO
```

相关命令

命令名称	描述信息
policy security service enable, disable	设置安全策略中所要检测的服务。
policy security service PORT	设置服务为端口识别并设置端口号。
show policy security service	显示指定安全策略的服务状态。

policy security service enable, disable

使用 **policy security service enable, disable** 命令设置安全策略中所要检测的服务。

命令

policy security *policy_name* **service** {**http | smtp | pop3 | imap | ftp | telnet | msn | nntp | x11 | oracle | mysql | pop2 | mssql | finger | dns** | **sip** | **tftp** | **snmp** | **netbios** | **smb** | **wins** | **sunrpc** | **dcerpc**} {**enable** | **disable**}

语法

policy_name	安全策略名称，格式为 WORD<1-15>。
enable	**disable**	• enable— 检测指定的服务 • disable— 不检测指定的服务

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置在安全策略 test 中检测 http 服务。

```
NetEye@root-system]policy security test service http enable
```

相关命令

命令名称	描述信息
policy security service AUTO	设置服务的识别方式为自动识别。
policy security service PORT	设置服务为端口识别并设置端口号。
show policy security service	显示指定安全策略的服务状态。

policy security service PORT

使用 **policy security service port** 命令设置服务为端口识别并设置端口号。

命令

policy security *policy_name* **service** {{**http | smtp | pop3 | imap | ftp | telnet | msn | nntp | x11 | oracle | mysql | pop2 | mssql | finger**} **TCP** | {**dns** | **sip** | **tftp**} **UDP** | {**snmp** | **netbios** | **smb** | **wins** | **sunrpc** | **dcerpc**} {**TCP** | **UDP**}} **PORT** *num*

语法

policy_name	安全策略名称，格式为 WORD<1-15>。
num	服务器端口号，格式为 NUMBER<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置安全策略 test 的 http 服务为端口识别，端口号为 8080。

```
NetEye@root-system]policy security test service http TCP PORT 8080
```

相关命令

命令名称	描述信息
policy security service AUTO	设置服务的识别方式为自动识别。
policy security service enable, disable	启用或禁用指定安全策略包含的服务。
show policy security service	显示指定安全策略的服务状态。

policy security service update_state enable, disable

使用 **policy security service update_state enable, disable** 命令设置是否默认选择最新更新的服务。

命令

policy security *policy_name* **service update_state** {**enable** | **disable**}

语法

policy_name	安全策略名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置安全策略 test 默认选择最新的更新服务。

```
NetEye@root-system] policy security test service update_state enable
```

相关命令

命令名称	描述信息
show policy security service update_state	显示是否默认选择最新更新的服务。

policy secrity zone

使用 **policy security zone** 命令修改指定安全策略的安全域。

命令

policy security *policy_name* {**Source | Destination**} **zone** *zone_name*

语法

policy_name	安全策略名称，格式为 WORD<1-15>。
zone_name	安全域名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 修改安全策略 test 的源安全域为 zone1。

```
NetEye@root-system] policy security test Source zone zone1
```

相关命令

命令名称	描述信息
policy security Obj, Rang, sub	修改指定安全策略的 IP 地址。
policy security number	修改指定安全策略的优先级。
policy security profile	修改指定安全策略引用的多套策略。

show policy security

使用 **show policy security** 命令显示安全策略的状态信息。

命令

show policy security [*policy_name*]

语法

policy_name	安全策略名称，格式为 WORD<1-15>。

说明

如果不指定 *policy_name* 参数，则显示所有安全策略的状态信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示安全策略 test 的状态信息。

```
NetEye@root>show policy security test
```

【返回结果】

```
Name: test
  State: enable
  Action: permit
  Auth: off
  Logging: off
  Tunnel:

  From: Any
  To: Any

  Source IP Address:
```

```
  ObjectIPAddr  test

Destination IP Address:
  GroupIPAddr   new

Services:
  Protocol Port/Type
  ICMP          Any

Timeout:
  -
Schedule:
  -
```

相关命令

命令名称	描述信息
policy security	添加安全策略。
policy security enable, disable	启用或禁用指定的安全策略。
unset policy security	删除安全策略。

show policy security service

使用 **show policy security service** 命令显示指定安全策略的服务状态。

命令

show policy security *policy_name* **service**

语法

policy_name	安全策略名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示安全策略 test 的服务状态。

```
NetEye@root>show policy security test service
```

【返回结果】

```
index    enable      service       type       flag      port
    1     Disable          dns        UDP       PORT        53
    2     Disable         http        TCP       PORT        80
    3     Disable         smtp        TCP       PORT        25
    4     Disable         pop3        TCP       PORT       110
    5     Disable         imap        TCP       PORT       143
    6     Disable          ftp        TCP       PORT        21
    7     Disable          sip        UDP       PORT      5060
    8     Disable         tftp        UDP       PORT        69
    9     Disable       oracle        TCP       PORT      1521
   10     Disable       telnet        TCP       PORT        23
   11     Disable          msn        TCP       PORT      1863
   12     Disable         snmp        TCP       PORT   161,162
   13     Disable         snmp        UDP       PORT   161,162
```

```
14      Disable    netbios        TCP       PORT        139
15      Disable    netbios        UDP       PORT    137,138
16      Disable       nntp        TCP       PORT        119
17      Disable        smb        TCP       PORT    139,445
18      Disable        smb        UDP       PORT        138
19      Disable        x11        TCP       PORT       6000
20      Disable       wins        TCP       PORT         42
21      Disable       wins        UDP       PORT         42
22      Disable      mysql        TCP       PORT       3306
23      Disable       pop2        TCP       PORT        109
24      Disable     sunrpc        TCP       PORT        111
25      Disable     sunrpc        UDP       PORT        111
26      Disable      mssql        TCP       PORT       1433
27      Disable     finger        TCP       PORT         79
28      Disable     dcerpc        TCP       PORT        135
29      Disable     dcerpc        UDP       PORT        135
```

相关命令

命令名称	描述信息
policy security service auto	设置服务的识别方式为自动识别。
policy security service enable, disable	设置安全策略中所要检测的服务。
policy security service port	设置服务为端口识别并设置端口号。

show policy security service update_state

使用 **show policy security service update_state** 命令显示是否默认选择最新更新的服务。

命令

show policy security *policy_name* **service update_state**

语法

policy_name	安全策略名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示安全策略 test 是否默认选择最新更新的服务。

```
NetEye@root> show policy security test service update_state
```

【返回结果】

```
Policy Name : test
Service update State : Enable
```

相关命令

命令名称	描述信息
policy security service update_state enable, disable	设置是否默认选择最新更新的服务。

unset policy security

使用 **unset policy security** 命令删除安全策略。

命令

unset policy security [*policy_name*]

语法

policy_name	策略名称，格式为 WORD<1-15>。

说明

如果不指定 *policy_name* 参数，则删除所有的安全策略。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除安全策略 test。

```
NetEye@root-system]unset policy security test
```

相关命令

命令名称	描述信息
policy security	添加安全策略。
policy security enable, disable	启用或禁用指定的安全策略。
show policy security	显示安全策略的状态信息。

缺省策略

policy default inter-zone

使用 **policy default inter-zone** 命令修改域间的默认策略动作。配置成功后，将允许或拒绝两个安全域之间的所有 IP 或非 IP 数据包的转发。

命令

policy default inter-zone {**access** | **non-ip-filter**} {**permit** | **deny**}

语法

inter-zone	表示域间，即两个安全域之间。
access | non-ip-filter	• access— 访问策略 • non-ip-filter— 非 IP 包过滤策略
permit | deny	• permit— 允许符合该策略的数据包通过 NetEye • deny— 拒绝符合该策略的数据包通过 NetEye 缺省设置为 deny

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 修改域间的默认非 IP 包过滤策略动作为允许。

```
NetEye@root-system]policy default inter-zone non-ip-filter permit
```

相关命令

命令名称	描述信息
policy default intra-zone	修改域内的默认策略动作。
show policy default	显示默认策略的相关信息。

policy default intra-zone

使用 **policy default intra-zone** 命令修改域内的默认策略动作。配置成功后，将允许或拒绝同一安全域内的所有 IP 和非 IP 数据包的转发。

命令

policy default intra-zone *zone_name* {**permit** | **deny**}

语法

intra-zone	表示域内，即在一个安全域中。
zone_name	安全域名称，格式为 WORD<1-15>。
permit | deny	• permit— 允许符合该策略的数据包通过 NetEye • deny— 拒绝符合该策略的数据包通过 NetEye 缺省设置为 permit

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 修改 zone1 域内的默认策略动作为拒绝。

```
NetEye@root-system]policy default intra-zone zone1 deny
```

相关命令

命令名称	描述信息
policy default inter-zone	修改域间的默认策略动作。
show policy default	显示默认策略的相关信息。

show policy default

使用 **show policy default** 命令显示默认策略的相关信息。

命令

show policy default

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示默认策略的相关信息。

```
NetEye@root>show policy default
```

【返回结果】

```
Default Inter-Zone Policies
  Policy Type             Action
  Access Policies     Deny
  Non-IP Packet Filtering Deny

Default Intra-Zone Policies
  Zone            Action
  1234            Permit
```

相关命令

命令名称	描述信息
policy default inter-zone	修改域间的默认策略动作。
policy default intra-zone	修改域内的默认策略动作。

show timeout

使用 **show timeout** 命令显示 ICMP、 UDP 和 TCP 会话的超时时间。

命令

show timeout [ICMP | UDP | TCP {CLOSE | ESTED | FIN | SYN}]

语法

**CLOSE	ESTED	FIN	SYN**	• CLOSE—TCP会话CLOSE状态的超时时间，CLOSE标志表示没有连接 • ESTED—TCP 会话 ESTED 状态的超时时间，EST 标志表示连接已建立，数据传送在进行 • FIN —TCP 会话 FIN 状态的超时时间， FIN 标志表示终止连接 • SYN—TCP会话SYN状态的超时时间，SYN标志表示在连接建立时对序号进行同步

说明

如果命令为 **show timeout** 形式，表示显示所有会话的超时时间设置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有会话的超时时间的设置信息。

```
NetEye@root>show timeout
```

【返回结果】

```
Default Session Timeouts
  States      Timeout value (in seconds)
  ICMP        2
  TCP_SYN     300
  TCP_FIN     3
  TCP_ESTED   3600
```

```
TCP_CLOSE   5
UDP         300
```

相关命令

命令名称	描述信息
timeout	设置 ICMP、 UDP 和 TCP 会话的超时时间。
timeout reset	恢复会话的超时时间为缺省值。

timeout

使用 **timeout** 命令设置 ICMP、 UDP 和 TCP 会话的超时时间。配置成功后，如果会话处于空闲状态的时间超过超时时间，在会话表中清除超时的连接。

命令

timeout {**ICMP** | **UDP** | **TCP** {**CLOSE** | **ESTED** | **FIN** | **SYN**}} *time*

语法

CLOSE | **ESTED** | **FIN** | **SYN**	• CLOSE—TCP会话CLOSE状态的超时时间，CLOSE标志表示没有连接 • ESTED—TCP 会话 ESTED 状态的超时时间，EST 标志表示连接已建立，数据传送在进行 • FIN —TCP 会话 FIN 状态的超时时间， FIN 标志表示终止连接 • SYN—TCP会话SYN状态的超时时间，SYN标志表示在连接建立时对序号进行同步
time	超时时间，单位为秒，格式为 INTEGER<1-99999999>。 ICMP 会话的超时时间的缺省值为 3 秒； UDP 会话的超时时间的缺省值为 300 秒； TCP 会话 SYN 状态的超时时间的缺省值为 300 秒； TCP 会话 FIN 状态的超时时间的缺省值为 600 秒； TCP 会话 ESTED 状态的超时时间的缺省值为 3600 秒； TCP 会话 CLOSE 状态的超时时间的缺省值为 10 秒。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置 TCP 会话 SYN 状态的超时时间为 400 秒。

```
NetEye@root-system]timeout TCP SYN 400
```

相关命令

命令名称	描述信息
show timeout	显示 ICMP、 UDP 和 TCP 会话的超时时间。
timeout reset	恢复会话的超时时间为缺省值。

timeout reset

使用 **timeout reset** 命令恢复会话的超时时间为缺省值。

命令

timeout reset

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show timeout	显示 ICMP、 UDP 和 TCP 会话的超时时间。

非 IP 包过滤

policy non-ip-filter

使用 **policy non-ip-filter** 命令添加非 IP 包过滤策略。

命令

policy non-ip-filter *policy_name* {*src_zone* | **any**} {*dst_zone* | **any**} {*smac_list* | **any** | **object** *mac_object_name* | **objectgroup** *mac_group_name*} {*dmac_list* | **any** | **object** *mac_object_name* | **objectgroup** *mac_group_name*} **protocol** {*numlist* | **any | object** *protocol_object_name* | **objectgroup** *protocol_group_name*} {**permit** | **deny**} {**enable** | **disable**} [*pri*]

语法

policy_name	策略名称，格式为 WORD<1-15>。
src_zone	源安全域名称，格式为 WORD<1-15>。 **any** 代表任意安全域。
dst_zone	目的安全域名称，格式为 WORD<1-15>。 **any** 代表任意安全域。
smac_list	源 MAC 地址列表，格式为 MACLIST<1-32>。 **any** 代表任意 MAC 地址列表。
mac_object_name	MAC 地址对象名称，格式为 WORD<1-63>。
mac_group_name	MAC 地址对象组名称，格式为 WORD<1-63>。
dmac_list	目的 MAC 地址列表，格式为 MACLIST<1-32>。 **any** 代表任意 MAC 地址列表。
numlist	协议列表，格式为 NUMBER<1-32>。 **any** 代表任意协议。
protocol_object_name	协议对象名称，格式为 WORD<1-63>。
protocol_group_name	协议对象组名称，格式为 WORD<1-63>。
permit | **deny**	• permit— 允许符合该策略的非 IP 数据包通过 NetEye • deny— 禁止符合该策略的非 IP 数据包通过 NetEye
enable | **disable**	• enable— 启用非 IP 包过滤策略 • disable— 禁用非 IP 包过滤策略
pri	策略的优先级，格式为 INTEGER<1-80000>，其中 “1”为最高优先级。

说明

如果不指定 *pri* 参数，则策略的优先级将被自动赋值为当前策略最低优先级加 1。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 添加非 IP 包过滤策略 test，其优先级为 1，协议为 6，状态为启用。配置成功后，拒绝由源安全域 zone1 至目的安全域 zone2 的非 IP 数据包通过 NetEye。

```
NetEye@root-system]policy non-ip-filter test zone1 zone2 any any
protocol 6 deny enable 1
```

范例 2. 添加非 IP 包过滤策略 test，其优先级为 5，引用协议对象 OBJ，状态为启用。配置成功后，允许由源安全域 zone1 至目的安全域 zone2 的非 IP 数据包通过 NetEye。

```
NetEye@root-system]policy non-ip-filter test zone1 zone2 any any
protocol object OBJ permit enable 5
```

相关命令

命令名称	描述信息
show policy non-ip-filter	显示非 IP 包过滤策略的相关信息。
unset policy non-ip-filter	删除非 IP 包过滤策略。

policy non-ip-filter enable, disable

使用 **policy non-ip-filter enable, disable** 命令启用或者禁用指定的非 IP 包过滤策略。

命令

policy non-ip-filter *policy_name* {**enable** | **disable**}

语法

policy_name	策略名称，格式为 WORD<1-15>。
enable | **disable**	• enable— 启用非 IP 包过滤策略 • disable— 禁用非 IP 包过滤策略

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 启用非 IP 包过滤策略 test。

```
NetEye@root-system]policy non-ip-filter test enable
```

相关命令

命令名称	描述信息
policy non-ip-filter permit, deny	设置非 IP 包过滤策略的行为。

policy non-ip-filter number

使用 **policy non-ip-filter number** 命令设置指定非 IP 包过滤策略的优先级。设置成功后，可以改变非 IP 数据包匹配此策略的先后顺序。

命令

policy non-ip-filter *policy_name* **number** *pri*

语法

policy_name	策略名称，格式为 WORD<1-15>。
number	表示为非 IP 包过滤策略设置优先级。
pri	策略的优先级，格式为 INTEGER<1-80000>，其中 “1” 为最高优先级。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置非 IP 包过滤策略 test 的优先级为 50。

```
NetEye@root-system]policy non-ip-filter test number 50
```

policy non-ip-filter permit, deny

使用 **policy non-ip-filter permit, deny** 设置指定非 IP 包过滤策略的行为。

命令

policy non-ip-filter *policy_name* {**permit** | **deny**}

语法

policy_name	策略名称，格式为 WORD<1-15>。
permit | **deny**	• permit— 允许符合该策略的非 IP 数据包通过 NetEye • deny— 禁止符合该策略的非 IP 数据包通过 NetEye

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 拒绝符合 test 策略的非 IP 数据包通过 NetEye。

```
NetEye@root-system]policy non-ip-filter test deny
```

相关命令

命令名称	描述信息
policy non-ip-filter enable, disable	启用或者禁用指定的非 IP 包过滤策略。

policy non-ip-filter protocol

使用 **policy non-ip-filter protocol** 命令为指定的非 IP 包过滤策略追加协议。

命令

policy non-ip-filter *policy_name* **protocol** {*numlist* | **object** *protocol_object_name* | **objectgroup** *protocol_group_name*}

语法

policy_name	策略名称，格式为 WORD<1-15>。
numlist	协议列表，格式为 NUMBER<1-32>。
protocol_object_name	协议对象名称，格式为 WORD<1-63>。
protocol_group_name	协议对象组名称，格式为 WORD<1-63>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 为非 IP 包过滤策略 test 追加协议 1， 2-5。

```
NetEye@root-system]policy non-ip-filter test protocol 1,2-5
```

范例 2. 为非 IP 包过滤策略 test 追加协议，引用协议对象 OBJ。

```
NetEye@root-system]policy non-ip-filter test protocol object OBJ
```

policy non-ip-filter schedule

使用 **policy non-ip-filter schedule** 命令为指定的非 IP 包过滤策略设置生效时间。设置成功后，该策略仅在生效时间内处于可用的状态。

命令

policy non-ip-filter *policy_name* **schedule start-week** *start_weekday* **end-week** *end_weekday time_scope*

语法

policy_name	策略名称，格式为 WORD<1-15>。
schedule	表示设定非 IP 包过滤策略的生效时间。
start-week	表示为非 IP 包过滤策略设定起始日期。
start_weekday	以星期为单位的非 IP 包过滤策略的起始日期，格式为 INTEGER<1-7>。
end-week	表示为非 IP 包过滤策略设定终止日期。
end_weekday	以星期为单位的非 IP 包过滤策略的终止日期，格式为 INTEGER<1-7>。
time_scope	时间范围，格式为 <HH:MM:SS-HH:MM:SS><1-8>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置非 IP 包过滤策略 test 的生效时间为每周一至每周三的 8:00:00-17:30:00。

```
NetEye@root-system]policy non-ip-filter test schedule start-week 1 end-week 3 8:00:00-17:30:00
```

相关命令

命令名称	描述信息
unset policy non-ip-filter schedule	删除指定非 IP 包过滤策略的生效时间。

policy non-ip-filter smac, dmac

使用 **policy non-ip-filter smac, dmac** 命令为指定的非 IP 包过滤策略追加 MAC 地址。

命令

policy non-ip-filter *policy_name* {**smac | dmac**} {*mac_list* | **object** *mac_object_name* | **objectgroup** *mac_group_name*}

语法

policy_name	策略名称，格式为 WORD<1-15>。
mac_list	MAC 地址列表，格式为 MACLIST<1-32>。
mac_object_name	MAC 地址对象名称，格式为 WORD<1-63>。
mac_group_name	MAC 地址对象组名称，格式为 WORD<1-63>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 为非 IP 包过滤策略 test 追加源 MAC 地址 22:22:22:22:22:22， 22:22:22:22:22:23。

```
NetEye@root-system]policy non-ip-filter test smac
22:22:22:22:22:22,22:22:22:22:22:23
```

范例 2. 为非 IP 包过滤策略 test 追加源 MAC 地址，引用 MAC 地址对象 OBJ。

```
NetEye@root-system]policy non-ip-filter test smac object OBJ
```

show policy non-ip-filter

使用 **show policy non-ip-filter** 命令显示非 IP 包过滤策略的相关信息。

命令

show policy non-ip-filter [*policy_name*]

语法

policy_name	策略名称，格式为 WORD<1-15>。

说明

如果不指定 *policy_name* 参数，则显示所有的非 IP 包过滤策略信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示非 IP 包过滤策略 test 的相关信息。

```
NetEye@root>show policy non-ip-filter test
```

【返回结果】

```
NonIp_Packet-filter rule:

  Name: test   State: enable  Action: permit
    From: Any
    To: Any
  Source MAC Address:
  Any
  Destination MAC Address:
  Any
  Protocols:
  Any
  Schedule:
```

```
Week:  -  -
```

相关命令

命令名称	描述信息
poilcy non-ip-filter	添加非 IP 包过滤策略。
unset policy non-ip-filter	删除非 IP 包过滤策略。

unset policy non-ip-filter

使用 **unset policy non-ip-filter** 命令删除非 IP 包过滤策略。

命令

unset policy non-ip-filter [*policy_name*]

语法

policy_name	策略名称，格式为 WORD<1-15>。

说明

如果不指定 *policy_name* 参数，则删除所有的非 IP 包过滤策略。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除非 IP 包过滤策略 test。

```
NetEye@root-system]unset policy non-ip-filter test
```

相关命令

命令名称	描述信息
poilcy non-ip-filter	添加非 IP 包过滤策略。
show policy non-ip-filter	显示非 IP 包过滤策略的相关信息。

unset policy non-ip-filter schedule

使用 **unset policy non-ip-filter schedule** 命令删除指定非 IP 包过滤策略的生效时间。配置成功后，非 IP 包过滤策略在任意时间都处于可用的状态。

命令

unset policy non-ip-filter *policy_name* **schedule**

语法

policy_name	策略名称，格式为 WORD<1-15>。
schedule	表示非 IP 包过滤策略的生效时间。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除非 IP 包过滤策略 test 的生效时间。

```
NetEye@root-system]unset policy non-ip-filter test schedule
```

相关命令

命令名称	描述信息
policy non-ip-filter schedule	为指定的非 IP 包过滤策略设置生效时间。

IP-MAC 绑定

policy ip-mac

使用 **policy ip-mac** 命令添加 IP-MAC 地址绑定策略。

命令

policy ip-mac *policy_name* {*ip_list* | **object** *ipaddr_object_name* | **objectgroup** *ipaddr_group_name*} *mac_address* {**enable | disable**}

语法

policy_name	策略名称，格式为 WORD<1-15>。
ip_list	IP 地址列表，格式为 IPV4LIST<1-32>。
ipaddr_object_name	IP 地址对象名称，格式为 WORD<1-63>。
ipaddr_group_name	IP 地址对象组名称，格式为 WORD<1-63>。
mac_address	MAC 地址，格式为 HH:HH:HH:HH:HH:HH。
enable | **disable**	• enable—启用所添加的 IP-MAC 地址绑定策略 • disable—禁用所添加的 IP-MAC 地址绑定策略

说明

设置多个 IP 地址对应一个 MAC 地址时，可以在一条策略或多条策略中指定。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 添加 IP 地址引用 IP 地址对象 OBJ， MAC 地址为 00:BF:36:2F:B0:9A 的 IP-MAC 地址绑定策略 test1，其状态为启用。

```
NetEye@root-system]policy ip-mac test1 object OBJ 00:BF:36:2F:B0:9A
enable
```

范例 2. 添加 IP 地址列表为 192.168.1.155-192.168.1.165， MAC 地址为 0C:9F:D3:66:1E:DB 的 IP-MAC 地址绑定策略 test2，其状态为禁用。

```
NetEye@root-system]policy ip-mac test2 192.168.1.155-192.168.1.165
0C:9F:D3:66:1E:DB disable
```

相关命令

命令名称	描述信息
policy ip-mac enable, disable	启用或禁用指定的 IP-MAC 地址绑定策略。
show policy ip-mac	显示 IP-MAC 地址绑定策略。
unset policy ip-mac	删除 IP-MAC 地址绑定策略。

policy ip-mac enable, disable

使用 **policy ip-mac enable, disable** 命令启用或禁用指定的 IP-MAC 地址绑定策略。

命令

policy ip-mac *policy_name* {**enable** | **disable**}

语法

policy_name	策略名称，格式为 WORD<1-15>。
enable | **disable**	• enable—启用所添加的 IP-MAC 地址绑定策略 • disable—禁用所添加的 IP-MAC 地址绑定策略

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 启用 IP-MAC 地址绑定策略 test1。

```
NetEye@root-system]policy ip-mac test1 enable
```

相关命令

命令名称	描述信息
policy ip-mac	添加 IP-MAC 地址绑定策略。
show policy ip-mac	显示 IP-MAC 地址绑定策略。
unset policy ip-mac	删除 IP-MAC 地址绑定策略。

policy ip-mac pursue

使用 **policy ip-mac pursue** 命令为指定的 IP-MAC 地址绑定策略追加 IP 地址。

命令

policy ip-mac pursue *policy_name* {*ip_list* | **object** *ipaddr_object_name* | **objectgroup** *ipaddr_group_name* | **subnet** *ip_address ip_mask*}

语法

policy_name	策略名称，格式为 WORD<1-15>。
ip_list	IP 地址列表，格式为 IPV4LIST<1-32>。
ipaddr_object_name	IP 地址对象名称，格式为 WORD<1-63>。
ipaddr_group_name	IP 地址对象组名称，格式为 WORD<1-63>。
ip_address	IP 地址，格式为 x.x.x.x。
ip_mask	子网掩码，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 为 IP-MAC 地址绑定策略 test1 追加 IP 地址 192.168.1.225。

```
NetEye@root-system]policy ip-mac pursue test1 192.168.1.225
```

范例 2. 为 IP-MAC 地址绑定策略 test2 追加 IP 地址，引用 IP 地址对象 OBJ。

```
NetEye@root-system]policy ip-mac pursue test2 object OBJ
```

范例 3. 为 IP-MAC 地址绑定策略 test3 追加 IP 地址 192.168.1.56 及其子网掩码 255.255.255.255。

```
NetEye@root-system]policy ip-mac pursue test3 subnet 192.168.1.56
255.255.255.255
```

相关命令

命令名称	描述信息
show policy ip-mac	显示 IP-MAC 地址绑定策略。

show policy ip-mac

使用 **show policy ip-mac** 命令显示 IP-MAC 地址绑定策略。

命令

show policy ip-mac [*policy_name*]

语法

policy_name	策略名称，格式为 WORD<1-15>。

说明

如果不指定 *policy_name* 参数，则表示显示所有的地址绑定策略。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示策略名称为 test 的 IP-MAC 地址绑定策略。

```
NetEye@root>show policy ip-mac test
```

【返回结果】

```
  Name: test
  State: enable
  IP Address List:
    192.168.1.100
  Mac Address:
    22:33:44:55:11:2f
```

相关命令

命令名称	描述信息
policy ip-mac	添加 IP-MAC 地址绑定策略。
policy ip-mac enable, disable	启用或禁用指定的 IP-MAC 地址绑定策略。
unset policy ip-mac	删除 IP-MAC 地址绑定策略。

unset policy ip-mac

使用 **unset policy ip-mac** 命令删除 IP-MAC 地址绑定策略。

命令

unset policy ip-mac [*policy_name*]

语法

policy_name	策略名称，格式为 WORD<1-15>。

说明

如果不指定 *policy_name* 参数，则表示删除所有的地址绑定策略。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除策略名称为 test 的 IP-MAC 地址绑定策略。

```
NetEye@root-system]unset policy ip-mac test
```

相关命令

命令名称	描述信息
policy ip-mac	添加 IP-MAC 地址绑定策略。
policy ip-mac enable, disable	启用或禁用指定的 IP-MAC 地址绑定策略。
show policy ip-mac	显示 IP-MAC 地址绑定策略。

信任地址

policy zone-binding

使用 **policy zone-binding** 命令设置安全域绑定的类型。

命令

policy zone-binding *zone_name* {**zone-ip** | **zone-mac**}

语法

zone_name	安全域名称，格式为 WORD<1-15>。
zone-ip	绑定类型，表示安全域和 IP 地址绑定。
zone-mac	绑定类型，表示安全域和 MAC 地址绑定。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置安全域 test 的绑定类型为安全域和 IP 地址绑定。

```
NetEye@root-system]policy zone-binding test zone-ip
```

相关命令

命令名称	描述信息
show policy zone-binding	显示安全域绑定策略。
unset policy zone-binding	删除安全域内所有指定类型的绑定策略。

policy zone-binding zone-ip

使用 **policy zone-binding zone-ip** 命令添加指定的安全域和 IP 地址绑定策略。配置成功后，指定的安全域只能允许或拒绝指定的 IP 地址的数据包通过 NetEye。

命令

policy zone-binding *zone_name* **zone-ip** {**permit-address** | **refuse-address**} *start_ipaddr* [*end_ipaddr*]

语法

zone_name	安全域名称，格式为 WORD<1-15>。
start_ipaddr	起始 IP 地址，格式为 x.x.x.x。
end_ipaddr	终止 IP 地址，格式为 x.x.x.x。

说明

绑定 IP 和拒绝 IP 每项最多可以设置 80000 条。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加安全域 test 和 IP 地址 192.168.1.130-192.168.1.150 的绑定策略，允许符合该策略的数据包通过 NetEye。

```
NetEye@root-system]policy zone-binding test zone-ip permit-address
192.168.1.130 192.168.1.150
```

相关命令

命令名称	描述信息
unset policy zone-binding zone-ip	删除指定的安全域和 IP 地址绑定策略。
show policy zone-binding	显示安全域绑定策略。

policy zone-binding zone-mac

使用 **policy zone-binding zone-mac** 命令添加指定的安全域和 MAC 地址绑定策略。配置成功后，指定的安全域只能允许或拒绝指定的 MAC 地址的数据包通过 NetEye。

命令

policy zone-binding *zone_name* **zone-mac** {**permit-address** | **refuse-address**} *start_mac* [*end_mac*]

语法

zone_name	安全域名称，格式为 WORD<1-15>。
start_mac	起始 MAC 地址，格式为 HH:HH:HH:HH:HH:HH。
end_mac	终止 MAC 地址，格式为 HH:HH:HH:HH:HH:HH。

说明

绑定 MAC 地址和拒绝 MAC 地址每项最多可以设置 80000 条。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加安全域 test 和 MAC 地址的绑定策略，允许 MAC 地址范围 B0:30:EB:77:E8:55-B0:30:EB:77:E8: 96 的数据包通过 NetEye。

```
NetEye@root-system]policy zone-binding test zone-mac permit-address B0:30:EB:77:E8:55 B0:30:EB:77:E8:96
```

相关命令

命令名称	描述信息
show policy zone-binding	显示安全域绑定策略。
unset policy zone-binding zone-mac	删除指定的安全域和 MAC 地址的绑定策略。

show policy zone-binding

使用 **show policy zone-binding** 命令显示安全域绑定策略。

命令

show policy zone-binding [*zone_name*]

语法

zone_name	安全域名称，格式为 WORD<1-15>。

说明

不指定 *zone_name* 参数，表示显示所有安全域绑定策略。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示安全域 zoneA 的安全域绑定策略。

```
NetEye@root>show policy zone-binding zoneA
```

【返回结果】

```
Zone is zoneA
Bind type is Zone-MAC binding
Permit MAC Address List:
       32:57:FA:C3:22:51 - 32:57:FA:C3:23:00
Refuse MAC Address List:
       63:35:2D:86:EF:95 - 63:35:2D:86:EF:A0
```

相关命令

命令名称	描述信息
policy zone-binding zone-ip	添加指定的安全域和 IP 地址绑定的策略。
policy zone-binding zone-mac	添加指定的安全域和 MAC 地址绑定的策略。

命令名称	描述信息
unset policy zone-binding zone-ip	删除指定的安全域和 IP 地址的绑定策略。
unset policy zone-binding zone-mac	删除指定的安全域和 MAC 地址的绑定策略。

unset policy zone-binding

使用 **unset policy zone-binding** 命令删除安全域内所有指定类型的绑定策略。

命令

unset policy zone-binding *zone_name* {**zone-ip** | **zone-mac**}

语法

zone_name	安全域名称，格式为 WORD<1-15>。
zone-ip	绑定类型，表示安全域和 IP 地址绑定。
zone-mac	绑定类型，表示安全域和 MAC 地址绑定。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除安全域 test 中所有的 IP 地址绑定策略。

```
NetEye@root-system]unset policy zone-binding test zone-ip
```

相关命令

命令名称	描述信息
show policy zone-binding	显示安全域绑定策略。

unset policy zone-binding zone-ip

使用 **unset policy zone-binding zone-ip** 命令删除指定的安全域和 IP 地址绑定策略。

命令

unset policy zone-binding *zone_name* **zone-ip** {**permit-address** | **refuse-address**} *start_ipaddr* [*end_ipaddr*]

语法

zone_name	安全域名称，格式为 WORD<1-15>。
start_ipaddr	起始 IP 地址，格式为 x.x.x.x，范围是 IPV4LIST<1-32>。
end_ipaddr	终止 IP 地址，格式为 x.x.x.x，范围是 IPV4LIST<1-32>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除安全域 test 和 IP 地址 192.168.1.130-192.168.1.150 的绑定策略。

```
NetEye@root-system]unset policy zone-binding test zone-ip permit-address 192.168.1.130 192.168.1.150
```

相关命令

命令名称	描述信息
policy zone-binding zone-ip	添加指定的安全域和 IP 地址绑定策略。
show policy zone-binding	显示安全域绑定策略。

unset policy zone-binding zone-mac

使用 **unset policy zone-binding zone-mac** 命令删除指定的安全域和 MAC 地址绑定策略。

命令

unset policy zone-binding *zone_name* **zone-mac** {**permit-address** | **refuse-address**} *start_mac* [*end_mac*]

语法

zone_name	安全域名称，格式为 WORD<1-15>。
start_mac	起始 MAC 地址，格式为 HH:HH:HH:HH:HH:HH。
end_mac	终止 MAC 地址，格式为 HH:HH:HH:HH:HH:HH。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除安全域 test 和 MAC 地址的绑定策略。

```
NetEye@root-system]unset policy zone-binding test zone-mac permit-address B0:30:EB:77:E8:55 B0:30:EB:77:E8:96
```

相关命令

命令名称	描述信息
policy zone-binding zone-mac	添加指定的安全域和 MAC 地址绑定策略。
show policy zone-binding	显示安全域绑定策略。

12 多播命令

DVMRP

dvmrp cache-lifetime

使用 **dvmrp cache-lifetime** 命令设置 **DVMRP** （距离矢量多播路由协议）路由的缓存时间，其缺省值为 300 秒。

命令

dvmrp cache-lifetime *time*

语法

time	路由缓存时间，单位为 “秒”，格式为 INTEGER<60-7200>。

说明

设置的 DVMRP 路由的缓存时间必须是 5 的倍数。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
dvmrp enable, disable	启用或者禁用虚拟系统的距离矢量多播路由协议。
dvmrp on, off	启用或者禁用三层接口的距离矢量多播路由协议。
show dvmrp state	显示 DVMRP （距离矢量多播路由协议）的路由状态信息。

dvmrp enable, disable

使用 **dvmrp enable, disable** 命令启用或者禁用虚拟系统的距离矢量多播路由协议。

命令

dvmrp {**enable** | **disable**}

语法

enable | **disable**	• enable— 启用虚拟系统的距离矢量多播路由协议 • disable— 禁用虚拟系统口的距离矢量多播路由协议 缺省设置为 disable

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令可以全局配置模式下使用。

相关命令

命令名称	描述信息
show dvmrp state	显示 DVMRP （距离矢量多播路由协议）的路由状态信息。

dvmrp metric

使用 **dvmrp metric** 命令修改三层接口的 **DVMRP** （距离矢量多播路由协议）度量值。

命令

dvmrp metric {*metric* | **default**}

语法

metric | **default**	• *metric*—DVMRP 度量值，格式为 INTEGER<1-32>。 • default—表示缺省值，其值为 1。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VLAN 配置模式、 Ethernet 接口配置模式、 Channel 接口配置模式或冗余接口配置模式下使用。

相关命令

命令名称	描述信息
dvmrp on, off	启用或者禁用三层接口的距离矢量多播路由协议。
show dvmrp state	显示 DVMRP （距离矢量多播路由协议）的路由状态信息。

dvmrp on, off

使用 **dvmrp on, off** 命令启用或者禁用三层接口的距离矢量多播路由协议。

命令

dvmrp {**on** | **off**}

语法

on	**off**	• on— 启用三层接口的距离矢量多播路由协议 • off— 禁用三层接口的距离矢量多播路由协议 缺省设置为 off

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VLAN 配置模式、 Ethernet 接口配置模式、 Channel 接口配置模式或冗余接口配置模式下使用。

相关命令

命令名称	描述信息
show dvmrp state	显示 DVMRP （距离矢量多播路由协议）的路由状态信息。

dvmrp pim

使用 **dvmrp pim** 命令设置 **DVMRP** （距离矢量多播路由协议）是否兼容 PIM 协议。

命令

dvmrp pim {**enable** | **disable**}

语法

enable | **disable**	• enable—DVMRP 协议兼容 PIM 协议 • disable—DVMRP 协议不兼容 PIM 协议 缺省设置为 disable

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
dvmrp on, off	启用或者禁用虚拟系统和三层接口的距离矢量多播路由协议。
show dvmrp state	显示 DVMRP （距离矢量多播路由协议）的路由状态信息。

dvmrp prune-lifetime

使用 **dvmrp prune-lifetime** 命令设置 Prune 存活时间，其缺省值为 7200 秒。

命令

dvmrp prune-lifetime *time*

语法

time	Prune 存活时间，单位为 “秒”，格式为 INTEGER<120-7200>。

说明

设置的 Prune 存活时间必须是 5 的倍数。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
dvmrp on, off	启用或者禁用虚拟系统和三层接口的距离矢量多播路由协议。
show dvmrp state	显示 DVMRP （距离矢量多播路由协议）的路由状态信息。

dvmrp threshold

使用 **dvmrp threshold** 命令设置三层接口的阈值。

命令

dvmrp threshold {*threshold_value* | **default**}

语法

threshold_value	• *threshold_value*—阈值，格式为 INTEGER<1-255>。 • default—表示缺省值，其值为 1。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VLAN 配置模式、 Ethernet 接口配置模式、 Channel 接口配置模式或冗余接口配置模式下使用。

相关命令

命令名称	描述信息
dvmrp on, off	启用或者禁用三层接口的距离矢量多播路由协议。
show dvmrp state	显示 DVMRP （距离矢量多播路由协议）的路由状态信息。

show dvmrp interface, neighbor, timer

使用 **show dvmrp interface, neighbor, timer** 命令显示 DVMRP 相关的监控信息。

命令

show dvmrp {**interface** | **neighbor** | **timer**}

语法

interface | **neighbor** | **timer**	• interface— 显示 DVMRP 的接口信息 • neighbor— 显示 DVMRP 的相邻信息 • timer— 显示 DVMRP 的定时器信息

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 DVMRP 的定时器信息。

```
NetEye@root>show dvmrp timer
```

【返回结果】

```
DVMRP Timers List:

Timer                                          Information
Next neighbor igmp time(seconds)               0
Next neighbor probe due in(seconds)            0
Cache entry average lifetime(seconds)          300
Prune entry average lifetime(seconds)          7200
```

show dvmrp neighbor-routes

使用 **show dvmrp neighbor-routes** 命令显示邻居路由表的信息。

命令

show dvmrp neighbor-routes

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示邻居路由表的信息。

```
NetEye@root>show dvmrp neighbor-routes
```

show dvmrp state

使用 **show dvmrp state** 命令显示 **DVMRP**（距离矢量多播路由协议）的路由状态信息。

命令

show dvmrp state

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 DVMRP 的状态信息。

```
NetEye@root>show dvmrp state
```

【返回结果】

```
Dvmrp State: disable

Pim state: off

Cache lifetime: 300

Prune lifetime: 7200

Layer 3 interface list
Interface Name   State Metric   Threshold
vlan1023         on    1        1
eth1             on    1        1
vlan1            off   1        1
```

相关命令

命令名称	描述信息
dvmrp on, off	启用或者禁用三层接口的距离矢量多播路由协议。

IGMP Snooping

igmp-snooping

使用 **igmp-snooping** 命令打开或者关闭 VLAN 接口的 IGMP 侦听功能。启动成功后，Neteye 开始侦听 VLAN 内的组播流量。

命令

igmp-snooping {**on** | **off**}

语法

on | **off**	• on— 打开 VLAN 接口的 IGMP 侦听功能 • off— 关闭 VLAN 接口的 IGMP 侦听功能 缺省设置为 off

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VLAN 配置模式下使用。

相关命令

命令名称	描述信息
show igmp-snooping state	显示 IGMP Snooping 的状态。

igmp-snooping interface-flags

使用 **igmp-snooping interface-flags** 命令设置 VLAN 包含的二层接口的路由标识。

命令

igmp-snooping interface-flags {**ethernet** | **channel** | **redundant** | **veth**} *interface_num* {**negotiate** | **multicast- router** | **host**}

语法

interface_num	以太网接口标识。 1. 如果设置为 ethernet 接口类型， *interface_num* 的格式为 WORD<1-10>。 2. 如果设置为 channel 接口类型， *interface_num* 的格式为 INTEGER<0-7>。 3. 如果设置为 redundant 接口类型， *interface_num* 的格式为 INTEGER<1-4>。 4. 如果设置为 veth 接口类型， *interface_num* 的格式为 INTEGER<1-1023>。
negotiate | multicast-router | host	路由接口标志。 • negotiate— 自动识别类型 • multicast-router— 路由器类型 • host— 主机类型

说明

网络类型的缺省设置为 **negotiate**。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VLAN 配置模式下使用。

igmp-snooping version

使用 **igmp-snooping version** 命令设置二层接口的 IGMP Snooping 协议的版本。

命令

igmp-snooping version {**ethernet** | **channel** | **redundant** | **weth**} *interface_num* {**v1** | **v2** | **auto**}

语法

interface_num	以太网接口标识。 1. 如果设置为 ethernet 接口类型， *interface_num* 的格式为 WORD<1-10>。 2. 如果设置为 channel 接口类型， *interface_num* 的格式为 INTEGER<0-7>。 3. 如果设置为 redundant 接口类型， *interface_num* 的格式为 INTEGER<1-4>。 4. 如果设置为 veth 接口类型， *interface_num* 的格式为 INTEGER<1-1023>。
v1 | v2 | auto	IGMP Snooping 协议的版本，缺省设置为 auto。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VLAN 配置模式下使用。

范例

范例 . 设置二层接口 ethernet2 使用 v1 版本的 IGMP Snooping 协议。

```
NetEye@root-system]vlan 1
NetEye@root-system-vlan1]igmp-snooping version ethernet 2 v1
```

multicast cam-table

使用 **multicast cam-table** 命令为 VLAN 添加多播转发表。配置成功后， NetEye 可以在 VLAN 接口内，使用多播转发表的信息转发信息流。

命令

multicast cam-table *group_address interface_list*

语法

group_address	多播组 IP 地址，格式为 x.x.x.x。
interface_list	VLAN 包含的二层接口列表，格式为 WORD<1-1024>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VLAN 配置模式下使用。

范例

范例 . 为 VLAN1 添加多播转发表。当要向多播组 224.2.1.2 转发信息流时，通过 VLAN1 的二层接口 eth2 和 eth3 转发出去。

```
NetEye@root-system]vlan 1
NetEye@root-system-vlan1]multicast cam-table 224.2.1.2 eth2,eth3
```

相关命令

命令名称	描述信息
unset multicast cam-table	删除 VLAN 的多播转发表。

show igmp-snooping state

使用 **show igmp-snooping state** 命令显示 IGMP Snooping 的状态。

命令

show igmp-snooping state [**vlan** *vlan_num*]

语法

vlan_num	VLAN 的接口标识，格式为 INTEGER<1-1023>。

说明

如果不指定 VLAN，则显示当前虚拟系统所有接口的 IGMP-SNOOPING 状态。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 VLAN1 的 IGMP-SNOOPING 的状态。

```
NetEye@root>show igmp-snooping state vlan 1
```

【返回结果】

```
vlan1, State: off
  Include port
    eth-s4p2, interface_flags is negotiate, version is auto
  Multicast CAM table
    Gip               Port
```

相关命令

命令名称	描述信息
igmp-snooping	启用或者禁用 VLAN 接口的 IGMP 侦听功能。

unset multicast cam-table

使用 **unset multicast cam-table** 命令删除 VLAN 的多播转发表。

命令

unset multicast cam-table [*group_address*]

语法

group_address	多播组 IP 地址，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VLAN 配置模式下使用。

范例

范例 . 删除 VLAN1 的多播组 IP 地址为 224.3.3.3 的多播转发表。

```
NetEye@root-system]vlan 1
NetEye@root-system-vlan1]unset multicast cam-table 224.3.3.3
```

相关命令

命令名称	描述信息
multicast cam-table	为 VLAN 添加多播转发表。

13 虚拟专用网命令

VPN 用户组和 IP 地址池

group

使用 **group** 命令添加 VPN 用户组。

命令

group *group_name*

语法

group_name	用户组名称，格式为 WORD<1-63>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

相关命令

命令名称	描述信息
unset group	删除 VPN 用户组。

group external

使用 **group external** 命令设置指定的用户组是否包含外部 VPN 用户。

命令

group *group_name* **external** {**xauth | l2tp | no**}

语法

group_name	用户组名称，格式为 WORD<1-63>。
**xauth	l2tp	no**	• xauth—设置指定的用户组包含外部 xauth 用户 • l2tp— 设置指定的用户组包含外部 l2tp 用户 • no— 设置指定的用户组不包含外部 VPN 用户

说明

外部 VPN 用户表示非 NetEye 上创建的、由 Radius 服务器进行认证的用户。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

group user

使用 **group user** 命令添加 VPN 用户到用户组中。

命令

group *group_name* **user** *user_list*

语法

group_name	用户组名称，格式为 WORD<1-63>。
user_list	VPN 用户列表，格式为 WORD<1-1300>。

说明

1. 一个用户不可重复添加到多个用户组中。

2. 如果用户组不存在，则同时添加用户组。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 添加 VPN 用户 user1 和 user2 到用户组 test 中。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]group test user user1,user2
```

相关命令

命令名称	描述信息
unset group user	从用户组中删除 VPN 用户。

ippool

使用 **ippool** 命令添加 VPN 用户地址池或向已存在的地址池中添加 IP 地址。

命令

ippool *ippool_name* {*ip_address* | *ip_range*}

语法

ippool_name	地址池名称，格式为 WORD<1-63>。
ip_address	IP 地址，格式为 x.x.x.x。
ip_range	IP 地址范围，格式为 IPV4RANGE。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 添加 VPN 用户地址池 test，指定其地址范围为 192.168.1.100-192.168.1.150。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]ippool test 192.168.1.100-192.168.1.150
```

相关命令

命令名称	描述信息
unset ippool	删除 VPN 用户地址池。

show vpn group

使用 **show vpn group** 命令显示本地认证用户组信息。

命令

show vpn group [*group_name*]

语法

group_name	用户组名称，格式为 WORD<1-63>。

说明

如果不指定 *group_name* 参数，则显示所有本地认证用户组信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示本地认证用户组 test 的信息。

```
NetEye@root>show vpn group test
```

【返回结果】

```
Group Name  : test
State    : no use
Inlude Users:
              user1
```

相关命令

命令名称	描述信息
group	添加 VPN 用户组。

show vpn ippool

使用 **show vpn ippool** 命令显示地址池信息。

命令

show vpn ippool [*ippool_name*]

语法

ippool_name	地址池名称，格式为 WORD<1-63>。

说明

如果不指定 *ippool_name* 参数，则显示所有地址池信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示地址池的信息。

```
NetEye@root>show vpn ippool
```

【返回结果】

```
  IPPoolName                    StartIP            EndIP
State
  p1                          10.3.1.15          10.3.1.75          no
use
```

unset group

使用 **unset group** 命令删除 VPN 用户组。

命令

unset group [*group_name*]

语法

group_name	用户组名称，格式为 WORD<1-63>。

说明

1. 如果不指定 *group_name* 参数，则删除所有的 VPN 用户组。
2. 如果用户组正在使用，则禁止删除。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 删除 VPN 用户组 test。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]unset group test
```

相关命令

命令名称	描述信息
group	添加 VPN 用户组。

unset group user

使用 **unset group user** 命令从用户组中删除 VPN 用户。

命令

unset group *group_name* **user** [*user_list*]

语法

group_name	用户组名称，格式为 WORD<1-63>。
user_list	VPN 用户列表，格式为 WORD<1-1300>。

说明

1. 如果不指定 *user_list* 参数，则从用户组中删除所有的 VPN 用户。
2. 如果用户组正在使用，则禁止从用户组中删除用户。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 删除用户组 test 中的 VPN 用户 user1 和 user2。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]unset group test user user1,user2
```

相关命令

命令名称	描述信息
group user	添加 VPN 用户到用户组中。

unset ippool

使用 **unset ippool** 命令删除 VPN 用户地址池。

命令

unset ippool [*ippool_name*]

语法

ippool_name	地址池名称，格式为 WORD<1-63>。

说明

1. 如果不指定 *ippool_name* 参数，则删除所有的地址池。
2. 如果地址池正在使用，则禁止删除。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

相关命令

命令名称	描述信息
ippool	添加 VPN 用户地址池或向已存在的地址池中添加 IP 地址。

证书

ca certificate checkmethod

使用 **ca certificate checkmethod** 命令设置 CA 证书的有效性检查方法，包括使用 OCSP、证书吊销列表或不对证书有效性进行检查。

命令

ca *file_name* **certificate checkmethod** {{**ocsp url** *url* | **crl**} [**strictcheck**] | **none**}

语法

file_name	CA 证书名称，格式为 WORD<1-127>。
ocsp	在线证书状态协议。NetEye 做为 OCSP 客户端，向 OCSP 服务器发出请求， OCSP 服务器验证证书是否有效。
url	OCSP 服务器地址，格式为 WORD<1-1023>。
crl	证书吊销列表。 NetEye 通过检查 CRL，验证证书是否有效。
strictcheck	证书状态严格检查。
none	表示不对证书进行有效性检查。

说明

1. 当无法连接到 OCSP 服务器或 OCSP 服务器返回的证书状态信息为未知时，如果启用证书状态严格检查，则 NetEye 认为证书失效；如果禁用证书状态严格检查，则 NetEye 认为证书有效。
2. 当没有任何 CRL 被上载到 NetEye 时，如果启用证书状态严格检查，则 NetEye 认为证书失效；如果禁用证书状态严格检查，则 NetEye 认为证书有效。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 设置通过 OCSP 检查 CA 证书 test 的有效性，并对证书状态进行严格检查。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]ca test.cer certificate checkmethod ocsp url
http://www.test.com strictcheck
```

ca scep

使用 **ca scep** 命令设置指定 CA 证书的 SCEP 服务。

命令

ca *file_name* **scep url** {**none** | *url*}

ca *file_name* **scep ident** {**none** | *ca_identity*}

ca *file_name* **scep challenge** {**none** | *challenge*}

ca *file_name* **scep polling** {**enable interval** *send_interval* **count** *time* | **disable**}

ca *file_name* **scep url** {**none** | *url*} **ident** {**none** | *ca_identity*} **challenge** {**none** | *challenge*} **polling** {**enable interval** *send_interval* **count** *time* | **disable**}

语法

file_name	CA 证书名称，格式为 WORD<1-127>。
scep	简单证书注册协议。
url	CA 服务器地址，格式为 WORD<1-1023>。
ca_identity	CA 证书标识，格式为 WORD<1-255>。
challenge	挑战码，格式为 WORD<1-127>。用于 CA 服务器对证书请求者进行身份验证。
send_interval	轮询时间间隔，单位为分钟，格式为 INTEGER<1-600>。表示多长时间向 CA 服务器发送一次查询消息。
time	轮询次数，格式为 INTEGER<1-1000>。表示向 CA 服务器发送的轮询次数。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 1. 设置 CA 证书 ca1 的 SCEP 服务，指定其轮询时间间隔为 120 分钟，轮询次数为 50 次。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]ca ca1 scep polling enable interval 120 count 50
```

范例 2. 设置 CA 证书 ca2 的 SCEP 服务，指定其 CA 服务器地址为 www.test.com，挑战码为 abcdef，轮询时间间隔为 60 分钟，轮询次数为 20 次。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]ca ca2 scep url http://www.test.com ident no
challenge abcdef  polling enable interval 60 count 20
```

相关命令

命令名称	描述信息
show certificate caserver	查看指定 CA 服务器的配置信息。

delete vpn certificate

使用 **delete vpn certificate** 命令删除本地证书、 CA 证书或证书吊销列表。

命令

delete vpn certificate {**local** | **ca** | **crl**} [*file_name*]

语法

local | **ca** | **crl**	• local— 本地证书 • ca—CA 证书 • crl— 证书吊销列表
file_name	文件名称，格式为 WORD<1-127>。

说明

1. 证书文件的扩展名一般为 .cer，而证书吊销列表的扩展名一般为 .crl。为了便于管理和区分，建议指定其对应的扩展名。
2. 如果不指定 *file_name* 参数，则表示删除指定的整个类别证书。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 删除本地证书 test。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]delete vpn certificate local test.cer
```

相关命令

命令名称	描述信息
show certificate	查看本地证书、 CA 证书或证书吊销列表。
show certificate request	查看指定的证书请求文件。

delete vpn certificate req

使用 **delete vpn certificate req** 命令删除证书请求文件。

命令

delete vpn certificate req [*request_name*]

语法

request_name	证书请求文件名称，格式为 WORD<1-127>。

说明

如果不指定 *file_name* 参数，则删除所有的证书请求文件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例 . 删除证书请求文件 test。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]delete vpn certificate req test
```

相关命令

命令名称	描述信息
show certificate request	查看指定的证书请求文件。

enroll request

使用 **enroll request** 命令将证书请求文件发送给 CA 进行签发。

命令

enroll request *request_name* **ca** *server_name* **url** *url* **ident** {**none** | *ca_identity*} **challenge** {**none** | *challenge*} **polling** {**enable interval** *send_interval* **count** *time* | **disable**} [**renew** {**days** | **hours** | **minutes**} *num*]

语法

request_name	证书请求文件名称，格式为 WORD<1-127>。
server_name	CA 服务器名称，格式为 WORD<1-127>。
url	CA 服务器地址，格式为 WORD<1-1023>。
ca_identity	CA 证书标识，格式为 WORD<1-255>。
challenge	挑战码，格式为 WORD<1-127>。用于 CA 服务器对证书请求者进行身份验证。
send_interval	轮询时间间隔，单位为分钟，格式为 INTEGER<1-600>。表示多长时间向 CA 服务器发送一次查询消息。
time	轮询次数，格式为 INTEGER<1-1000>。表示向 CA 服务器发送的轮询次数。
renew	自动更新证书。
num	设置证书更新时间，格式为 INTEGER<1-86400>。例如关键字设置为 **days**， *num* 设置为 5，则证书将在到期前 5 天进行自动更新。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 向 CA 服务器发送证书自动注册请求，设置挑战码为 abc123，轮询时间间隔为 120 分钟，轮询次数为 50 次，启用证书自动更新，在证书到期前 5 天自动更新证书。

```
NetEye@root-system]vpn
```

```
NetEye@root-system-vpn]enroll request test ca caserver1 url
www.test.com ident ca1 challenge abc123 polling enable interval 120
count 50 renew days 5
```

相关命令

命令名称	描述信息
enroll request accept-ca-certificate	接受或拒绝 CA 证书指纹。
generate certificate-request	生成证书请求文件。

enroll request accept-ca-certificate

使用 **enroll request accept-ca-certificate** 命令接受或拒绝 CA 证书指纹。

命令

enroll request *request_name* **accept-ca-certificate** {**accept** | **cancel**}

语法

request_name	证书请求文件名称，格式为 WORD<1-127>。
accept | **cancel**	• accept— 接受证书指纹 • cancel— 拒绝证书指纹

说明

当第一次向某个 CA 服务器发送证书注册请求时，在命令行界面会打印 CA 证书指纹信息，此时一定要联系 CA，确认证书的合法性。如果接受 CA 证书指纹，则继续进行本地证书的注册，否则终止本次证书注册过程。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

相关命令

命令名称	描述信息
enroll request	将证书请求文件发送给 CA 进行签发。

generate certificate-request

使用 **generate certificate-request** 命令生成证书请求文件，请求信息将发送给 CA 用来签发证书。

命令

generate certificate-request *request_name* **country** {**none** | *country_name*} **state-or-province** {**none** | *state_name*} **locality** {**none** | *locality_name*} **organization** {**none** | *organization_name*} **organizational-unit** {**none** | *unit_name*} **common-name** {**none** | *common_name*} **ip-address** {**none** | *ip_address*} **email-address** {**none** | *email*} **dns** {**none** | *fqdn_name*} {**rsa** | **dsa**} {**768** | **1024** | **1536** | **2048**} [*password*]

语法

request_name	证书请求文件名称，格式为 WORD<1-127>。
country_name	国家名称，格式为 WORD<2-2>。
state_name	州或省份名称，格式为 WORD<1-127>。
locality_name	城市名称，格式为 WORD<1-127>。
organization_name	公司名称，格式为 WORD<1-127>。
unit_name	部门名称，格式为 WORD<1-127>。
common_name	公共名，格式为 WORD<1-127>。
ip_address	IP 地址，格式为 X.X.X.X。
email	邮件地址，格式为 WORD<3-63>。
fqdn_name	完全合格域名，格式为 WORD<1-255>。
rsa | **dsa**	非对称加密算法。 • rsa—RSA 算法，既能用于数据加密也能用于数字签名 • dsa—DSA 算法，只能用于数字签名
768 | **1024** | **1536** | **2048**	密钥对长度。密钥越长，越安全，但加密和解密的速度越慢。
password	本地私钥的加密口令，格式为 WORD<4-127>。

说明

1. 国家、州或省份、城市、公司、部门、公共名、 IP 地址、邮件地址以及完全合格域名不可以同时设置为 **none**。
2. 国家名称的格式取值范围为数字和字母。州或省份名称、城市名称、公司名称、部门名称、公共域名和邮件地址的格式取值范围为数字、字母和特殊字符 （不包含 "、'、 <、 >、 &、 \、 /、 !、 ‘、 $ 和 #）。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 为 Neusoft 公司网络部的用户 Jim 生成证书请求文件 test，当 CA 签发证书后，管理员将其发送至 Jim@neteye.com。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]generate certificate-request test country CN state-or-province ln locality sy organization Neusoft organizational-unit network common-name www.test.com ip-address none email-address Jim@neteye.com dns none rsa 1024
```

相关命令

命令名称	描述信息
enroll request	将证书请求文件发送给 CA 进行签发。

import vpn certificate

使用 **import vpn certificate** 命令导入本地证书或 CA 证书。

命令

import vpn certificate {**local** | **ca**} **from** {**tftp** *ip_tftp file_name* | **sftp** *ip_sftp* **username** *user_name* **password** *passwd sftp_file_name* | **x**/**zmodem**} [*mod_file_name*]

语法

local | **ca**	• local— 本地证书 • ca—CA 证书
tftp	简单文件传输协议，表示从 TFTP 服务器导入指定的本地证书或 CA 证书。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
file_name	文件名称，格式为 WORD<1-127>。
sftp	安全文件传输协议，表示从 SFTP 服务器导入指定的本地证书或 CA 证书。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-64>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-64>。
sftp_file_name	证书文件在 SFTP 服务器中的路径以及文件名，格式为 WORD<1-256>。。
x/zmodem	异步文件传输协议， Xmodem 或 Zmodem 由系统自动选择。表示使用 X/Zmodem 协议导入指定的本地证书或 CA 证书。
mod_file_name	修改后文件名称，格式为 WORD<1-127>。

说明

证书文件的扩展名一般为 .cer，为了便于管理和区分，建议指定其对应的扩展名。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 从 TFTP 服务器 192.168.1.125 导入本地证书 test，并将证书名称改为 test1 存储到 NetEye 上。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]import vpn certificate local from tftp
192.168.1.125 test.cer test1.cer
```

import vpn certificate crl

使用 **import vpn certificate crl** 命令导入证书吊销列表。

命令

import vpn certificate crl from {**tftp** *ip_tftp file_name* | **sftp** *ip_sftp* **username** *user_name* **password** *passwd sftp_file_name* | **x**/**zmodem**}

语法

crl	证书吊销列表。
tftp	简单文件传输协议，表示从 TFTP 服务器导入指定的证书吊销列表。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
file_name	文件名称，格式为 WORD<1-127>。
sftp	安全文件传输协议，表示从 SFTP 服务器导入指定的证书吊销列表。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-64>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-64>。
sftp_file_name	证书吊销列表在 SFTP 服务器中的路径以及文件名。
x/zmodem	异步文件传输协议， Xmodem 或 Zmodem 由系统自动选择。表示使用 X/Zmodem 协议导入指定的证书吊销列表。

说明

证书吊销列表的扩展名一般为 .crl。为了便于管理和区分，建议指定其对应的扩展名。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 以 X/Zmodem 方式导入证书吊销列表。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]import vpn certificate crl from x/zmodem
```

show certificate

使用 **show certificate** 命令查看本地证书、 CA 证书或证书吊销列表。

命令

show certificate {**local** | **ca** | **crl**} [*file_name*]

语法

local | **ca** | **crl**	• local— 本地证书 • ca—CA 证书 • crl— 证书吊销列表
file_name	文件名称，格式为 WORD<1-127>。

说明

1. 如果不指定 *file_name* 参数，则显示所有的本地证书、 CA 证书或证书吊销列表。
2. 证书文件的扩展名一般为 .cer，而证书吊销列表的扩展名一般为 .crl。为了便于管理和区分，建议指定其对应的扩展名。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看所有的 CA 证书。

```
NetEye@root>show certificate ca
```

【返回结果】

```
************************************************************
  Name: ca.crt.pem
  Issuer:
        C=US, O=neteye, OU=security, CN=Jim, emailAddress=Jim@neteye.com

  Subject:
        C=US, O=neteye, OU=security, CN=Jim, emailAddress=Jim@neteye.com
```

```
End time:     2010:01:19:13:59:08

  State:        Valid
```

相关命令

命令名称	描述信息
delete vpn certificate	删除本地证书、 CA 证书或证书吊销列表。

show certificate caserver

使用 **show certificate caserver** 命令查看指定 CA 服务器的配置信息。

命令

show certificate caserver *server_name*

语法

server_name	CA 服务器名称，格式为 WORD<1-127>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看 CA 服务器 test 的配置信息。

```
NetEye@root>show certificate caserver test
```

【返回结果】

```
CertName:     ca1
 Subject:      C=cn, ST=ln, L=shenyang, O=neusoft, OU=security,
CN=lihongguang,
emailAddress=li.hg@neusoft.com

 OCSP Configuration
 Check Method: crl
 Best Effort:  no
 OCSP URL:

 SCEP Configuration
 CA/RA URL:    https://www.test.com
 CA ident:
 Challenge:    abcdefg
 Polling: Enable
       Interval:  10 Minutes
       Number:  5
```

相关命令

命令名称	描述信息
ca scep	设置指定 CA 证书的 SCEP 服务。

show certificate request

使用 **show certificate request** 命令查看指定的证书请求文件。

命令

show certificate request *request_name*

语法

request_name	证书请求文件名称，格式为 WORD<1-127>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看证书请求文件 test。

```
NetEye@root>show certificate request test
```

【返回结果】

```
CertName:     test1
  Version:      0
  Pubkeyalg:    rsaEncryption
  Status:       Keypair
  Subject:      C=cn, ST=liaoning, L=shenyang, O=neusoft, OU=security

  Choose CA:
  CA/RA URL:
  CA ident:
  Challenge:
  Polling:      Disable
  Renew:        Disable

  Pubkey:       3081 8902 8181 00b9 f515 8adb f8dd 6aec 9c31 abc8 78bb 6b7e 9e71
bc48 bab2 124c 5708 a9d6 507a d82d cdf7 b491 7205 8d3a 9717 ddc7 8ca6 0abb 24a9
4b61 f7a8 a171 1fc9 caf0 e9e5 3b1d e289 cc41 5e60 2636 2663 9d84 d676 7832 b338
b15c 2568 9a36 ee73 1657 36de 8f8d e628 c688 b1f4 1a84 058e 9114 8bb2 fbad 5f06
8f01 9e05 f45c 2170 f724 ceca fd02 0301 0001
```

相关命令

命令名称	描述信息
delete vpn certificate req	删除证书请求文件。

VPN 隧道

bind tunnel tunnel-interface

使用 **bind tunnel tunnel-interface** 命令在指定的 VPN 隧道上绑定隧道接口。

命令

bind tunnel *tunnel_name* **tunnel-interface** *interface_id*

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
interface_id	隧道接口 ID，格式为 INTEGER<1-4095>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 在 VPN 隧道 test 上绑定隧道接口 10。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]bind tunnel test tunnel-interface 10
```

相关命令

命令名称	描述信息
unset bind tunnel tunnel-interface	在指定的 VPN 隧道上解除隧道接口。

show tunnel

使用 **show tunnel** 命令来显示指定的 VPN 隧道信息。

命令

show tunnel *tunnel_name*

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 VPN 隧道 test 的信息。

```
NetEye@root>show tunnel test
```

【返回结果】

```
Basic information:

  Name: test State: disable
  Outgoing Interface: eth0   Ip: Any
  Remote Peer: Dynamic ip
  Peer: -
  Authentication Method: Preshared key
    Preshared Key: <******>
  Phase1:
    Proposal: g2-3des-sha1,g2-3des-md5,g2-aes128-sha1,g2-aes128-md5
    Lifetime: 86400 s
  Phase2:
    Proposal: g2-esp-aes128-md5,g2-esp-aes128-sha1,g2-esp-3des-md5,g2-
esp-3des-sha1
    Lifetime: 28800 s
  Local IKE ID: -
  Remote IKE ID: -
  TunInter: Tunnel1
```

```
xauth/l2tp: -

Add Time: 2008-03-26 14:33:03
Status:  Close
In Packets: 0
Out Packets: 0
```

show tunnels

使用 **show tunnels** 命令来显示所有自动密钥或手动密钥隧道信息。

命令

show tunnels {**auto** | **manual**}

语法

auto | **manual**	• auto— 表示显示所有自动密钥信息 • manual— 表示显示所有手动密钥隧道信息

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有自动密钥隧道信息。

```
NetEye@root>show tunnels auto
```

【返回结果】

```
Auto tunnel list: (total: 1)

Name  RemotePeer Peer  Auth TunInter  Enable Status  In Packets Out
Packets
kkk   Dynamic ip -     PSK  Tunnel1   yes    Close   0          0
```

show vpn-accel

使用 **show vpn-accel** 命令来显示加密卡状态。

命令

show vpn-accel

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 显示加密卡状态。

```
NetEye@root>show vpn-accel
```

【返回结果】

```
vpn-accel state is disable
```

tunnel certificate

使用 **tunnel certificate** 命令设置自动密钥隧道为证书认证方式，并设置证书。

命令

tunnel *tunnel_name* **certificate** *local_cert_name* {*remote_cert_name* | **any**}

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
local_cert_name	本端证书名称，格式为 WORD<1-127>。
remote_cert_name	对端 CA 证书名称，格式为 WORD<1-127>。 **any** 表示已上载到 NetEye 上的任意 CA 证书。

说明

指定的证书必须都已经上载到 NetEye 上。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 设置已存在的自动密钥隧道 test 为证书认证方式。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnel test certificate cert1 any
```

tunnel dialup certificate

使用 **tunnel dialup certificate** 命令添加远程用户或用户组到 VPN 网关的证书认证自动隧道。配置成功后，数据可通过此隧道安全传输。

命令

tunnel *tunnel_name* **dialup** {**user** {*user_name* | **none**} | **group** *group_name*} **interface** *interface_name* {*local_ip_address* | **any**} **certificate** *local_cert_name* {*remote_cert_name* | **any**} [**local-subnet** *local_subnet_address local_subnet_mask*] {**enable** | **disable**}

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
user_name	远程用户名称，格式为 WORD<1-63>。 **none** 表示不指定用户。
group_name	用户组名称，格式为 WORD<1-63>。
interface_name	出口设备名称，需设置为三层接口，格式为 WORD<3-10>。
local_ip_address	本端 IP 地址，格式为 x.x.x.x。 **any** 表示任意 IP 地址。
local_cert_name	本端证书名称，格式为 WORD<1-127>。
remote_cert_name	对端 CA 证书名称，格式为 WORD<1-127>。 **any** 表示已上载到 NetEye 上的任意 CA 证书。
local_subnet_address	本端子网 IP 地址，格式为 x.x.x.x。
local_subnet_mask	本端子网掩码，格式为 x.x.x.x。
enable | **disable**	• enable— 表示启用隧道 • disable— 表示禁用隧道

说明

指定的证书必须都已经上载到 NetEye 上。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 启用远程用户 user1 到 VPN 网关的证书认证自动密钥隧道 test。指定其出口设备为 vlan10，本端 IP 地址为 192.168.1.120，本端证书名称是 cert1。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnel test dialup user user1 interface vlan10
192.168.1.120 certificate cert1 any enable
```

相关命令

命令名称	描述信息
tunnel dialup preshared-key	添加远程用户或用户组到 VPN 网关的预共享密钥认证自动隧道。

tunnel dialup preshared-key

使用 **tunnel dialup preshared-key** 命令添加远程用户或用户组到 VPN 网关的预共享密钥认证自动隧道。配置成功后，数据可通过此隧道安全传输。

命令

tunnel *tunnel_name* **dialup** {**user** {*user_name* | **none**} | **group** *group_name*} **interface** *interface_name* {*local_ip_address* | **any**} **preshared-key** *key* [**local-subnet** *local_subnet_address local_subnet_mask*] {**enable** | **disable**}

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
user_name	远程用户名称，格式为 WORD<1-63>。 **none** 表示不指定用户。
group_name	用户组名称，格式为 WORD<1-63>。
interface_name	出口设备名称，需设置为三层接口，格式为 WORD<3-10>。
local_ip_address	本端 IP 地址，格式为 x.x.x.x。 **any** 表示任意 IP 地址。
key	预共享密钥，格式为 WORD<1-127>。
local_subnet_address	本端子网 IP 地址，格式为 x.x.x.x。
local_subnet_mask	本端子网掩码，格式为 x.x.x.x。
enable | **disable**	• enable— 表示启用隧道 • disable— 表示禁用隧道

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 启用远程用户 user1 到 VPN 网关的预共享密钥认证自动隧道 test。指定其出口设备为 vlan10，预共享密钥为 abcde。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnel test dialup user user1 interface vlan10
192.168.1.100 preshared-key abcde enable
```

相关命令

命令名称	描述信息
tunnel dialup certificate	添加远程用户或用户组到 VPN 网关的证书认证自动隧道。

tunnel enable, disable

使用 **tunnel enable, disable** 命令启用或禁用指定的 VPN 隧道。

命令

tunnel *tunnel_name* {**enable** | **disable**}

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
enable | **disable**	• enable— 表示启用指定的 VPN 隧道 • disable— 表示禁用指定的 VPN 隧道

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

相关命令

命令名称	描述信息
unset tunnel	删除 VPN 隧道。

tunnel gateway certificate

使用 **tunnel gateway certificate** 命令添加网关到网关的证书认证自动隧道。配置成功后，数据可通过此隧道安全传输。

命令

tunnel *tunnel_name* **gateway** {*remote_ip_address* | *remote_domain_name*} **interface** *interface_name* {*local_ip_address* | **any**} **certificate** *local_cert_name* {*remote_cert_name* | **any**} [**local-subnet** *local_subnet_address local_subnet_mask* **remote-subnet** *remote_subnet_address remote_subnet_mask*] {**enable** | **disable**} [**permanent**]

tunnel *tunnel_name* **gateway any interface** *interface_name* {*local_ip_address* | **any**} **certificate** *local_cert_name* {*remote_cert_name* | **any**} [**local-subnet** *local_subnet_address local_subnet_mask* **remote-subnet** *remote_subnet_address remote_subnet_mask*] {**enable** | **disable**}

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
remote_ip_address	对端 IP 地址，格式为 x.x.x.x。
any	表示地址是动态分配的，无需指定。
remote_domain_name	对端域名，格式为 WORD<1-255>。
interface_name	出口接口名称，需设置为三层接口，格式为 WORD<3-10>。
local_ip_address	本端 IP 地址，格式为 x.x.x.x。 **any** 表示任意 IP 地址。
local_cert_name	本端证书名称，格式为 WORD<1-127>。
remote_cert_name	对端 CA 证书名称，格式为 WORD<1-127>。 **any** 表示已上载到 NetEye 上的任意 CA 证书。
local_subnet_address	本端子网 IP 地址，格式为 x.x.x.x。
local_subnet_mask	本端子网掩码，格式为 x.x.x.x。
remote_subnet_address	对端子网 IP 地址，格式为 x.x.x.x。
remote_subnet_mask	对端子网掩码，格式为 x.x.x.x。
enable | **disable**	• enable— 表示启用隧道 • disable— 表示禁用隧道
permanent	隧道类型，表示永久隧道。

说明

1. 指定的证书必须都已经上载到 NetEye 上。
2. 如果对端信息设置为 IP 地址或域名时，可以选择隧道的类型，隧道类型包括普通隧道和永久隧道。
3. 如果选择了 **permanent** 参数，则表示永久隧道；永久隧道会在启用后主动发起协商，即使协商失败也会不断的发起协商，直到协商成功为止。
4. 如果没有选择 **permanent** 参数，则表示普通隧道；普通隧道不会在启用后主动发起协商，仅当有数据要通过隧道时发起协商；普通隧道可以被动接受对端发起的协商。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 启用网关到网关的证书认证自动隧道 test。指定其出口为 vlan10，本端 IP 地址为 192.168.1.120，本端证书名称为 cert1。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnel test gateway any interface vlan10
192.168.1.120 certificate cert1 any enable
```

相关命令

命令名称	描述信息
tunnel gateway preshared-key	添加网关到网关的预共享密钥认证自动隧道。

tunnel gateway preshared-key

使用 **tunnel gateway preshared-key** 命令添加网关到网关的预共享密钥认证自动隧道。配置成功后，数据可通过隧道安全传输。

命令

tunnel *tunnel_name* **gateway** {*remote_ip_address* | *remote_domain_name*} **interface** *interface_name* {*local_ip_address* | **any**} **preshared-key** *key* [**local-subnet** *local_subnet_address local_subnet_mask* **remote-subnet** *remote_subnet_address remote_subnet_mask*] {**enable** | **disable**} [**permanent**]

tunnel *tunnel_name* **gateway any interface** *interface_name* {*local_ip_address* | **any**} **preshared-key** *key* [**local-subnet** *local_subnet_address local_subnet_mask* **remote-subnet** *remote_subnet_address remote_subnet_mask*] {**enable** | **disable**}

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
remote_ip_address	对端 IP 地址，格式为 x.x.x.x。
any	表示地址是动态分配的，无需指定。
remote_domain_name	对端域名，格式为 WORD<1-255>。
interface_name	出口接口名称，需设置为三层接口，格式为 WORD<3-10>。
local_ip_address	本端 IP 地址，格式为 x.x.x.x。 **any** 表示任意 IP 地址。
key	预共享密钥，格式为 WORD<1-127>。
local_subnet_address	本端子网 IP 地址，格式为 x.x.x.x。
local_subnet_mask	本端子网掩码，格式为 x.x.x.x。
remote_subnet_address	对端子网 IP 地址，格式为 x.x.x.x。
remote_subnet_mask	对端子网掩码，格式为 x.x.x.x。
enable | **disable**	• enable— 表示启用隧道 • disable— 表示禁用隧道
permanent	隧道类型，表示永久隧道。

说明

1. 如果对端信息设置为 IP 地址或域名时，可以选择隧道的类型，隧道类型包括普通隧道和永久隧道。
2. 如果选择了 **permanent** 参数，则表示永久隧道；永久隧道会在启用后主动发起协商，即使协商失败也会不断的发起协商，直到协商成功为止。

3. 如果没有选择 **permanent** 参数，则表示普通隧道；普通隧道不会在启用后主动发起协商，仅当有数据要通过隧道时发起协商；普通隧道可以被动接受对端发起的协商。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 启用网关到网关的预共享密钥认证自动隧道 test。指定其对端 IP 地址为 192.168.1.175，出口为 vlan10，本端 IP 地址为 192.168.1.120，预共享密钥为 abcde。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnel test gateway 192.168.1.175 interface vlan10 192.168.1.120 preshared-key abcde enable
```

相关命令

命令名称	描述信息
tunnel gateway certificate	添加网关到网关的证书认证自动隧道。

tunnel ike

使用 **tunnel ike** 命令配置自动密钥隧道本端或对端的 IKE ID。

命令

tunnel *tunnel_name* **ike** {**peer-id | local-id**} {**ipv4-address** *ip_address* | {**fqdn** | **user-fqdn** | **asn1-dn** | **key-id**} *ike*}

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
ip_address	IP 地址，格式为 x.x.x.x。
fqdn	**user-fqdn**	**asn1-dn**	**key-id**	• fqdn— 表示将 *ike* 参数设置为域名 • user-fqdn— 表示将 *ike* 参数设置为电子邮件地址 • asn1-dn— 表示将 *ike* 参数设置为固定的格式。例如 C=CN，ST=Guangdong， L=Guangzhou， O=ABC， OU=Security，CN=test，emailAddress=test@test.com。其中 C 代表国家，ST 代表省份， L 代表城市， O 代表公司， OU 代表部门， CN 代表用户名， emailAddress 代表用户的邮件地址 • key-id— 表示将 *ike* 参数设置为字符串
ike	隧道本端或对端的 IKE ID，格式为 WORD<1-1023>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 1. 配置自动密钥隧道 test1 本端的 IKE ID。指定其类型为 **fqdn**， IKE ID 为 www.test.com。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnel test1 ike local-id fqdn www.test.com
```

范例 2. 配置自动密钥隧道 test2 对端的 IKE ID。指定其类型为 **ipv4-address**， IKE ID 为 192.168.1.115。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnel test2 ike peer-id ipv4-address
192.168.1.115
```

tunnel ike dpd

使用 **tunnel ike dpd** 命令配置自动密钥隧道的 DPD 属性。

命令

tunnel *tunnel_name* **ike dpd** *interval retry*

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
dpd	对方失效探测。表示隧道两端的 VPN 网关通过发送 keepalive 报文来探测对端的状态。
interval	**dpd** 时间间隔，单位为秒。格式为 INTEGER<1-3600>。 缺省值为 30
retry	**dpd** 重复连接次数，格式为 INTEGER<2-32767>。 缺省值为 4

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 配置自动密钥隧道 test 的 DPD 属性。指定其 DPD 时间间隔为 25， DPD 重复连接次数为 5。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnel test ike dpd 25 5
```

相关命令

命令名称	描述信息
tunnel ike dpd disable	禁用自动密钥隧道的 DPD 功能。

tunnel ike dpd disable

使用 **tunnel ike dpd disable** 命令禁用自动密钥隧道的 DPD 功能。

命令

tunnel *tunnel_name* **ike dpd disable**

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
dpd	对方失效探测。表示隧道两端的 VPN 网关通过发送 keepalive 报文来探测对端的状态。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

相关命令

命令名称	描述信息
tunnel ike dpd	配置自动密钥隧道的 DPD 属性。

tunnel ike lifetime

使用 **tunnel ike lifetime** 命令设置第一阶段或第二阶段 sa 的生存时间。

命令

tunnel *tunnel_name* **ike** {**phase1 | phase2**} **lifetime** *time*

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
time	生存时间，单位为秒，格式为 INTERGER<180-2147483647>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 设置第一阶段 sa 的生存时间为 2000 秒。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnel test ike phase1 lifetime 2000
```

tunnel ike phase1 default

使用 **tunnel ike phase1 default** 命令修改自动密钥隧道协商的第一阶段属性为默认状态。

命令

tunnel *tunnel_name* **ike phase1 default**

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。

说明

1. 默认状态的提议集为 g2-3des-sha1， g2-3des-md5， g2-aes128-sha1， g2-aes128-md5。
2. 默认状态的协商模式为主模式。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

相关命令

命令名称	描述信息
tunnel ike phase1	配置自动密钥隧道协商的第一阶段属性。

tunnel ike phase1 mode

使用 **tunnel ike phase1** 命令配置自动密钥隧道协商的第一阶段属性。

命令

tunnel *tunnel_name* **ike phase1** {**proposal** {*custom_proposal* | **default**} | **mode** {**main** | **aggressive**}}

分别配置各个属性。

tunnel *tunnel_name* **ike phase1 proposal** {*custom_proposal* | **default**} **mode** {**main** | **aggressive**}

同时配置全部属性。

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
custom_proposal | **default**	• *custom_proposal*— 第一阶段的提议集。可选择 g1-3des-md5，g1-3des-sha1， g1-aes128-md5， g1-aes128-sha1， g2-3des-sha1，g2-3des-md5，g2-aes128-sha1，g2-aes128-md5，g2-aes192-md5，g2-aes192-sha1，g2-aes256-md5，g2-aes256-sha1， g5-3des-md5，g5-3des-sha1， g5-aes256-md5， g5-aes256-sha1 • default— 默认的提议集。表示自动密钥隧道第一阶段的四个提议集为 g2-3des-sha1， g2-3des-md5， g2-aes128-sha1， g2-aes128-md5
main | **aggressive**	• main — 表示协商模式为主模式 • aggressive— 表示协商模式为进取模式 缺省值为 main

说明

自动密钥隧道第一阶段可选择 1-4 个提议集，并用逗号隔开。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 配置自动密钥隧道 test 协商第一阶段的提议集为默认的提议集，模式为主模式。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnel test ike phase1 proposal default mode
main
```

相关命令

命令名称	描述信息
tunnel ike phase1 default	修改自动密钥隧道协商的第一阶段属性为默认状态。

tunnel ike phase2 default

使用 **tunnel ike phase2 default** 命令修改自动密钥隧道协商的第二阶段属性为默认状态。

命令

tunnel *tunnel_name* **ike phase2 default**

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。

说明

1. 默认状态的提议集为 g2-esp-aes128-md5， g2-esp-aes128-sha1， g2-esp-3des-md5， g2-esp-3des-sha1。
2. 默认状态隧道的模式为隧道模式。
3. 默认状态启用回放攻击保护。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

相关命令

命令名称	描述信息
tunnel ike phase2	配置自动密钥隧道协商的第二阶段属性。

tunnel ike phase2 mode

使用 **tunnel ike phase2** 命令配置自动密钥隧道协商的第二阶段属性。

命令

tunnel *tunnel_name* **ike phase2** {**proposal** {*custom_proposal* | **default**} | **mode** {**tunnel** | **transport**} | **replay** {**on** | **off**}}

分别配置各个属性。

tunnel *tunnel_name* **ike phase2 proposal** {*custom_proposal* **default**} **mode** {**tunnel** | **transport**} **replay** {**on** | **off**}

同时配置全部属性。

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
custom_proposal | **default**	• *custom_proposal*— 第二阶段提议集，可选择 nopfs-esp-3des-md5， nopfs-esp-3des-sha1， nopfs-esp-aes128-md5， nopfs-esp-aes128-sha1， g1-esp-3des-sha1， g1-esp-aes128-md5，g5-esp-3des-md5， g5-esp-3des-sha1， g5-esp-aes128-md5，g5-esp-aes128-sha1， g2-ah-md5，g2-ah-sha1，g2-esp-aes128-md5， g2-esp-aes128-sha1， g2-esp-3des-md5，g2-esp-3des-sha1， g2-esp-aes192-md5， g2-esp-aes192-sha1，g2-esp-aes256-md5， g2-esp-aes256-sha1， g2-ah-md5-esp-3des，g2-ah-sha1-esp-3des，g2-ah-md5-esp-aes128，g2-ah-sha1-esp-aes128 • default— 默认的提议集，表示自动密钥隧道的第二阶段四个提议集为 g2-esp-aes128-md5， g2-esp-aes128-sha1， g2-esp-3des-md5， g2-esp-3des-sha1
tunnel | transport	• tunnel— 表示隧道的模式为隧道模式 • transport— 表示隧道的模式为传输模式 缺省值为 tunnel
on | off	• on— 表示启用回放攻击保护 • off— 表示禁用回放攻击保护 缺省值为 on

说明

1. 自动密钥隧道第二阶段可选择 1-4 个提议集，并用逗号隔开。
2. 回放攻击是指攻击者截获合法的 IPSec 报文，向该报文的目的地址发送大量该报文的副本，对 VPN 网关进行 DoS 攻击。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 配置自动密钥隧道 test 协商第二阶段的提议集为默认的提议集，隧道的模式为传输模式，启用回放攻击保护。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnel test ike phase2 proposal default mode transport replay on
```

相关命令

命令名称	描述信息
tunnel ike phase2 default	修改自动密钥隧道协商的第二阶段属性为默认状态。

tunnel interface

使用 **tunnel interface** 命令设置自动密钥隧道本端出口和本端 IP 地址。

命令

tunnel *tunnel_name* **interface** *interface_name* {*local_ip_address* | **any**}

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
interface_name	出口接口名称，格式为 WORD<3-10>。
local_ip_address	本端 IP 地址，格式为 x.x.x.x。 **any** 表示任意 IP 地址。

说明

本命令中提到的接口是不包括隧道和以太网接口的三层接口。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 设置自动密钥隧道 test 的出口为 vlan1，本端 IP 为 any。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnel test interface vlan1 any
```

tunnel local-subnet, remote-subnet

使用 **tunnel local-subnet, remote-subnet** 命令设置自动密钥隧道本端或对端子网。

命令

tunnel *tunnel_name* {**local-subnet | remote-subnet**} {*subnet_address subnet_mask* | **any**}

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
subnet_address	子网 IP 地址，格式为 x.x.x.x。
subnet_mask	子网掩码，格式为 x.x.x.x。
any	表示任意子网。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 设置自动密钥隧道 test 的本端子网，其 IP 地址为 192.168.1.0，子网掩码为 255.255.255.0。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnel test local-subnet 192.168.1.0
255.255.255.0
```

相关命令

命令名称	描述信息
unset tunnel local-subnet, remote-subnet	删除自动密钥隧道的本端子网或对端子网。

tunnel manual gateway

使用 **tunnel manual gateway** 命令添加网关到网关的手动密钥隧道。

命令

tunnel *tunnel_name* **manual gateway remote-ip** *remote_ip_address* **local-ip** *local_ip_address* **ah** *ah_local_spi ah_remote_spi* **auth** {**hmac-md5 | hmac-sha1**} **key** *ah_auth_key* **mode** {**tunnel | transport**} {**enable | disable**}

使用 ah 协议的手动密钥隧道。

tunnel *tunnel_name* **manual gateway remote-ip** *remote_ip_address* **local-ip** *local_ip_address* **esp** *esp_local_spi esp_remote_spi* {**auth** {**hmac-md5 | hmac-sha1**} **key** *esp_auth_key* | **encrypt** {**3des | aes128 | aes192 | aes256**} **key** *esp_enc_key*} **mode** {**tunnel | transport**} {**enable | disable**}

使用 esp 协议的手动密钥隧道。指定 esp 认证或 esp 加密。

tunnel *tunnel_name* **manual gateway remote-ip** *remote_ip_address* **local-ip** *local_ip_address* **esp** *esp_local_spi esp_remote_spi* **auth** {**hmac-md5 | hmac-sha1**} **key** *esp_auth_key* **encrypt** {**3des | aes128 | aes192 | aes256**} **key** *esp_enc_key* **mode** {**tunnel | transport**} {**enable | disable**}

使用 esp 协议的手动密钥隧道。同时指定 esp 认证和 esp 加密。

tunnel *tunnel_name* **manual gateway remote-ip** *remote_ip_address* **local-ip** *local_ip_address* **ah-esp ah** *ah_local_spi ah_remote_spi* **auth** {**hmac-md5 | hmac-sha1**} **key** *ah_auth_key* **esp** *esp_local_spi esp_remote_spi* {**auth** {**hmac-md5 | hmac-sha1**} **key** *esp_auth_key* | **encrypt** {**3des | aes128 | aes192 | aes256**} **key** *esp_enc_key*} **mode** {**tunnel | transport**} {**enable | disable**}

使用 ah 协议和 esp 协议的手动密钥隧道。指定 esp 认证或 esp 加密。

tunnel *tunnel_name* **manual gateway remote-ip** *remote_ip_address* **local-ip** *local_ip_address* **ah-esp ah** *ah_local_spi ah_remote_spi* **auth** {**hmac-md5 | hmac-sha1**} **key** *ah_auth_key* **esp** *esp_local_spi esp_remote_spi* **auth** {**hmac-md5 | hmac-sha1**} **key** *esp_auth_key* **encrypt** {**3des | aes128 | aes192 | aes256**} **key** *esp_enc_key* **mode** {**tunnel | transport**} {**enable | disable**}

使用 ah 协议和 esp 协议的手动密钥隧道。同时指定 esp 认证和 esp 加密。

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
remote_ip_address	对端 IP 地址，格式为 x.x.x.x。
local_ip_address	本端 IP 地址，格式为 x.x.x.x。

ah	认证头协议。
esp	封装安全载荷协议。
ah_remote_spi	AH 协议对端安全参数索引，格式为 WORD<8-8>。
ah_local_spi	AH 协议本端安全参数索引，格式为 WORD<8-8>。
hmac	带密钥的散列消息认证码。
md5	消息摘要算法 5。
sha1	安全散列算法 1。
hmac-md5 | hmac-sha1	• hmac-md5— 表示使用 md5 算法的 hmac。 • hmac-sha1— 表示使用 sha1 算法的 hmac。
ah_auth_key	AH 协议认证密钥。格式 WORD<1-66>。 当认证算法选择 hmac-md5 时，认证密钥为 32 位十六进制数；当认证算法选择 hmac-sha1 时，认证密钥为 40 位十六进制数。
tunnel | transport	• tunnel— 表示隧道的模式为隧道模式 • transport— 表示隧道的模式为传输模式 缺省值为 tunnel
enable | disable	• enable— 表示启用隧道 • disable— 表示禁用隧道
esp_remote_spi	ESP 协议对端安全参数索引，格式为 WORD<8-8>。
esp_local_spi	ESP 协议本端安全参数索引，格式为 WORD<8-8>。
esp_auth_key	ESP 协议认证密钥。格式 WORD<1-66>，以十六进制数形式输入。 当认证算法选择 hmac-md5 时，认证密钥为 32 位十六进制数；当认证算法选择 hmac-sha1 时，认证密钥为 40 位十六进制数。
3des | aes128 | aes192 | aes256	• 3des— 表示三倍数据加密标准。一种对称密码算法，用来对传输的数据进行加密和解密 • aes128— 表示 128 位密钥的高级加密标准 • aes192— 表示 192 位密钥的高级加密标准 • aes256— 表示 256 位密钥的高级加密标准
esp_enc_key	ESP 协议加密密钥。格式 WORD<1-66>，以十六进制数形式输入。 当加密算法选择 3des 时，加密密钥为 48 位十六进制数；当加密算法选择 aes128 时，加密密钥为 32 位十六进制数；当加密算法选择 aes192 时，加密密钥为 48 位十六进制数；当加密算法选择 aes256 时，加密密钥为 64 位十六进制数。

提示

安全索引参数为 8 位十六进制数，取值范围为 00000100-2fffffff。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 添加网关到网关的手动密钥隧道 test，指定其对端 IP 地址为 192.168.1.115，本端 IP 地址为 192.168.1.180， AH 协议本端安全参数索引为 11111111， AH 协议对端安全参数索引为 22222222，认证算法为 hmac-md5，认证密钥为 abcdeabcdeabcdeaabcdeabcdeabcdea，隧道的模式为隧道模式。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnel test manual gateway remote-ip 192.168.1.115 local-ip 192.168.1.180 ah 11111111 22222222 auth hmac-md5 key abcdeabcdeabcdeaabcdeabcdeabcdea mode tunnel enable
```

相关命令

命令名称	描述信息
unset tunnel	删除 VPN 隧道。

tunnel nat-traversal auto enable, disable

使用 **tunnel nat-traversal auto enable, disable** 命令启用或禁用自动密钥隧道的 NAT 穿越功能。

命令

tunnel *tunnel_name* **nat-traversal auto** {**enable** [*interval*] | **disable**}

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
interval	发送 NAT keepalive 数据报文的时间间隔，单位为秒，格式为 INTEGER<1-3600>。
enable | **disable**	• enable— 表示启用自动密钥隧道的 NAT 穿越功能 • disable— 表示禁用自动密钥隧道的 NAT 穿越功能

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

相关命令

命令名称	描述信息
tunnel nat-traversal manual enable, disable	启用或禁用手动密钥隧道的 NAT 穿越功能。

tunnel nat-traversal manual enable, disable

使用 **tunnel nat-traversal manual enable, disable** 命令启用或禁用手动密钥隧道的 NAT 穿越功能。

命令

tunnel *tunnel_name* **nat-traversal manual** {**enable** | **disable**}

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
enable | **disable**	• enable— 表示启用手动密钥隧道的 NAT 穿越功能 • disable— 表示禁用手动密钥隧道的 NAT 穿越功能

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

相关命令

命令名称	描述信息
tunnel nat-traversal auto enable, disable	启用或禁用自动密钥隧道的 NAT 穿越功能。

tunnel permanent

使用 **tunnel permanent** 命令设置自动密钥隧道类型为永久或普通。

命令

tunnel *tunnel_name* **permanent** {**on** | **off**}

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
permanent	隧道类型，表示永久隧道。
on	**off**	• on— 表示永久隧道 • off— 表示普通隧道

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 设置自动密钥隧道 test 为永久隧道。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnel test permanent on
```

tunnel preshared-key

使用 **tunnel preshared-key** 命令设置自动密钥隧道为预共享密钥认证方式，并设置预共享密钥。

命令

tunnel *tunnel_name* **preshared-key** *key*

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
key	预共享密钥，格式为 WORD<1-127>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 设置自动密钥隧道 test 为预共享密钥认证方式，预共享密钥为 abcdef。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnel test preshared-key abcdef
```

tunnel remote

使用 **tunnel remote** 命令设置自动密钥隧道对端的 IP 地址。

命令

tunnel *tunnel_name* **remote** {*remote_ip_address* | *remote_domain_name*}

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
remote_ip_address	对端 IP 地址，格式为 x.x.x.x。
remote_domain_name	对端域名，格式为 WORD<1-255>。

说明

本命令只能用于对端类型为静态 IP 地址类型的自动密钥隧道。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 设置自动密钥隧道 test 对端的 IP 为 192.168.1.125。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnel test remote 192.168.1.125
```

tunnel remote user, group

使用 **tunnel remote user, group** 命令设置自动密钥隧道对端的用户或用户组。

命令

tunnel *tunnel_name* **remote** {**user** {*user_name* | **none**} | **group** *group_name*}

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
user_name	用户名称，格式为 WORD<1-63>。 **none** 表示不指定用户。
group_name	用户组名称，格式为 WORD<1-63>。

说明

本命令只能用于对端类型为拨号用户或用户组的自动密钥隧道。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 设置自动密钥隧道 test 的对端的用户为 user1。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnel test remote user user1
```

tunnel xauth enable, disable

使用 **`tunnel xauth enable, disable`** 命令启用或禁用自动密钥隧道的 xauth 功能。

命令

tunnel *tunnel_name* **xauth** {**enable** | **disable**}

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
xauth	可扩展认证。表示在隧道协商阶段对远程用户进行 xauth 认证。需要用户提供其用户名和密码。
enable | **disable**	• enable—表示启用自动密钥隧道的 xauth 功能 • disable—表示禁用自动密钥隧道的 xauth 功能

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

unset bind tunnel tunnel-interface

使用 **unset bind tunnel tunnel-interface** 命令在指定的 VPN 隧道上解除隧道接口。

命令

unset bind tunnel *tunnel_name* **tunnel-interface** *interface_id*

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
interface_id	隧道接口 ID。格式为 INTEGER<1-4095>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

相关命令

命令名称	描述信息
bind tunnel tunnel-interface	在指定的隧道上绑定隧道接口。

unset tunnel

使用 **`unset tunnel`** 命令删除 VPN 隧道。

命令

unset tunnel [*tunnel_name*]

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。

说明

1. 如果隧道被策略引用，则禁止删除。
2. 如果不指定 *tunnel_name* 参数，则表示删除所有的 VPN 隧道。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

相关命令

命令名称	描述信息
unset tunnels auto, manual	删除所有自动或手动 VPN 隧道。

unset tunnel local-subnet, remote-subnet

使用 **unset tunnel local-subnet, remote-subnet** 命令删除自动密钥隧道的本端子网或对端子网。

命令

unset tunnel *tunnel_name* {**local-subnet** | **remote-subnet**} *subnet_address subnet_mask*

语法

tunnel_name	隧道名称，格式为 WORD<1-15>。
subnet_address	子网 IP 地址，格式为 x.x.x.x。
subnet_mask	子网掩码，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 删除自动密钥隧道 test 的对端子网 10.3.3.0/24，使 10.3.3.0/24 网段的主机不能与本端子网进行通信。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]unset tunnel test remote-subnet 10.3.3.0
255.255.255.0
```

相关命令

命令名称	描述信息
tunnel local-subnet, remote-subnet	设置自动密钥隧道本端或对端子网。

unset tunnels auto, manual

使用 **unset tunnels auto, manual** 命令删除所有自动或手动的密钥隧道。

命令

unset tunnels {**auto** | **manual**}

语法

auto | **manual**	• auto—表示删除所有自动密钥隧道 • manual—表示删除所有手动密钥隧道

说明

如果隧道被策略引用，则禁止删除。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

相关命令

命令名称	描述信息
unset tunnel	删除 VPN 隧道。

vpn-accel on, off

使用 **vpn-accel on, off** 命令启用或禁用 VPN 硬件加密卡。

命令

vpn-accel {**on** | **off**}

语法

on | off	• on—表示启用 VPN 硬件加密卡 • off—表示禁用 VPN 硬件加密卡

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 VPN 配置模式下使用。

隧道组

bind tunnelgroup tunnel-interface

使用 **bind tunnelgroup tunnel-interface** 命令在指定的隧道组上绑定隧道接口。

命令

bind tunnelgroup *group_name* **tunnel-interface** *interface_id*

语法

group_name	隧道组名称，格式为 WORD<1-127>。
interface_id	隧道接口 ID，格式为 INTEGER<1-4095>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 模式下使用。

范例

范例 . 在隧道组 test 上绑定隧道接口 10。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]bind tunnelgroup test tunnel-interface 10
```

相关命令

命令名称	描述信息
unset bind tunnelgroup tunnel-interface	在指定的隧道组上解除绑定隧道接口。

show tunnelgroup

使用 **show tunnelgroup** 命令查看指定的隧道组配置信息。

命令

show tunnelgroup *group_name*

语法

group_name	隧道组名称，格式为 WORD<1-127>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看隧道组 test 的配置信息。

```
NetEye@root>show tunnelgroup test
```

【返回结果】

```
GroupName                  tunnel_id       Priority  TunnelState
TunnelInterface  Enable
test                  tunnel1       0       unusable      tunnel4
enable
                   tunnel2       1       unusable
```

相关命令

命令名称	描述信息
show tunnelgroups	查看所有的隧道组配置信息。

show tunnelgroups

使用 **show tunnelgroups** 命令查看所有的隧道组配置信息。

命令

show tunnelgroups

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示隧道组的配置信息。

```
NetEye@root>show tunnelgroups
```

【返回结果】

```
VPN tunnelgroup list: (total: 2)

GroupName                  tunnel_id       Priority  TunnelState
TunnelInterface  Enable
test                  tunnel1       0       unusable      tunnel4
enable
                   tunnel2       1       unusable
test1                   -             -        -
enable
```

相关命令

命令名称	描述信息
show tunnelgroup	查看指定的隧道组配置信息。

tunnelgroup

使用 **tunnelgroup** 命令添加隧道组。

命令

tunnelgroup *group_name* {**enable | disable**}

语法

group_name	隧道组名称，格式为 WORD<1-127>。
**enable	disable**	• enable— 启用隧道组 • disable— 禁用隧道组

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 模式下使用。

范例

范例 . 添加并启用隧道组 test。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnelgroup test enable
```

相关命令

命令名称	描述信息
tunnelgroup tunnel	向隧道组中添加隧道成员。

tunnelgroup tunnel

使用 **tunnelgroup tunnel** 命令向指定的隧道组中添加隧道成员。

命令

tunnelgroup *group_name* **tunnel** *tunnel_name* **priority** *pri*

语法

group_name	隧道组名称，格式为 WORD<1-127>。
tunnel_name	隧道名称，格式为 WORD<1-15>。
pri	隧道在隧道组中的优先级。数字越大，优先级越高。

说明

1. 隧道组中的隧道成员必须为网关到网关的自动密钥隧道。
2. 一个隧道组最多包含 16 条成员隧道。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 模式下使用。

范例

范例 . 向隧道组 test 中添加隧道成员 tunnel1，并指定隧道 tunnel1 的优先级为 20。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]tunnelgroup test tunnel tunnel1 priority 20
```

相关命令

命令名称	描述信息
tunnelgroup	添加隧道组。
unset tunnelgroup tunnel	删除指定隧道组中的隧道成员。

unset bind tunnelgroup tunnel-interface

使用 **unset bind tunnelgroup tunnel-interface** 命令在指定的隧道组上解除绑定隧道接口。

命令

unset bind tunnelgroup *group_name* **tunnel-interface** *interface_id*

语法

group_name	隧道组名称，格式为 WORD<1-127>。
interface_id	隧道接口 ID，格式为 INTEGER<1-4095>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 在隧道组 test 上解除绑定隧道接口 10。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]unset bind tunnelgroup test tunnel-interface 10
```

相关命令

命令名称	描述信息
bind tunnelgroup tunnel-interface	在指定的隧道组上绑定隧道接口。

unset tunnelgroup

使用 **unset tunnelgroup** 命令删除指定的隧道组。

命令

unset tunnelgroup *group_name*

语法

group_name	隧道组名称，格式为 WORD<1-127>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

相关命令

命令名称	描述信息
unset tunnelgroups	删除所有的隧道组。

unset tunnelgroup tunnel

使用 **unset tunnelgroup tunnel** 命令删除指定隧道组中的隧道成员。

命令

unset tunnelgroup *group_name* {**tunnel** *tunnel_name* | **tunnels**}

语法

group_name	隧道组名称，格式为 WORD<1-127>。
tunnel_name	隧道名称，格式为 WORD<1-15>。
tunnels	表示删除隧道组中的所有隧道成员。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

范例

范例 . 删除隧道组 test 中的隧道成员 tunnel1。

```
NetEye@root-system]vpn
NetEye@root-system-vpn]unset tunnelgroup test tunnel tunnel1
```

相关命令

命令名称	描述信息
tunnelgroup	添加隧道组。
tunnelgroup tunnel	向隧道组中添加隧道成员。

unset tunnelgroups

使用 **unset tunnelgroups** 命令删除所有的隧道组。

命令

unset tunnelgroups

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 VPN 配置模式下使用。

相关命令

命令名称	描述信息
unset tunnelgroup	删除指定的隧道组。

14 攻击防御命令

attack-defense

使用 **attack-defense** 命令在指定安全域内设置特定攻击类型的防御。配置成功后，当受到特定类型的攻击时，可以发送报警事件或者丢弃攻击数据包。

命令

attack-defense *zone_name attack_type* **active** {**on** {**alert** [**drop**] | **drop** [**alert**]} | **off** [**alert** [**drop**] | **drop** [**alert**]]}

语法

zone_name	安全域名称，格式为 WORD<1-15>。
attack_type	攻击类型，设置个数为 1，可以设置为： icmp-flood； tcp-syn-flood； udp-flood； tcp-rst-scan； winnuke； land； smurf； tcp-fin-scan； tcp-xmas-scan； tcp-null-scan； tcp-syn-port-scan； ip-address-sweep； spoofed-reset-protection； small-pmtu； ip-record-route-option； ip-timestamp-option； ip-loose-source-option； ip-strict-source-option； ip-traceroute-option； other-ip-options； icmp-iss-pinger； icmp-l3retriever-ping； icmp-nemesis-echo； icmp-ping-nmap； icmp-icmpenum； icmp-redirect-host； icmp-redirect-net； icmp-superscan-echo； icmp-traceroute-ipopts； icmp-webtrends； icmp-source-quench； icmp-broadscan-smurf； icmp-ping-speedera； icmp-tjpingpro； icmp-ping-whatsupgold； icmp-ping-cyberKit； icmp-ping-sniffer-pro/netxray； icmp-admin-prohibited； icmp-destination-Host-admin-prohibited； icmp-destination-network-admin-prohibited； icmp-digital-island； icmp-path-mtu-dos。
on | **off**	• on— 启用特定攻击类型的防御 • off— 禁用特定攻击类型的防御
alert | **drop**	• alert— 发送报警事件 • drop— 丢弃攻击数据包

说明

1. 攻击防御是在添加安全域时自动添加的，特定的攻击类型有其对应的缺省动作。

2. active 为 off 时，可以不指定动作，此时使用特定攻击类型的缺省动作。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 在安全域 test 内设置 TCP SYN 端口扫描防御。当受到 TCP SYN 端口扫描时，发送报警事件并丢弃攻击数据包。

```
NetEye@root-system]attack-defense test tcp-syn-port-scan active on
alert drop
```

相关命令

命令名称	描述信息
show attack-defense	查看指定安全域内攻击防御的各项设置。

attack-defense tcp-syn-cookie

使用 **attack-defense tcp-syn-cookie** 命令在指定安全域内启用或者禁用 SYN Cookie 防御。启用该功能后，进行 SYN 代理功能，屏蔽非法的 SYN 连接请求。

命令

attack-defense *zone_name* **tcp-syn-cookie active** {**on** | **off**}

语法

zone_name	安全域名称，格式为 WORD<1-15>。
on | **off**	• on— 启用 SYN Cookie 防御 • off— 禁用 SYN Cookie 防御

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 在安全域 test 内启用 SYN Cookie 防御。

```
NetEye@root-system]attack-defense test tcp-syn-cookie active on
```

相关命令

命令名称	描述信息
show attack-defense	查看指定安全域内攻击防御的各项设置。
attack-defense	在指定安全域内设置特定攻击类型的防御。

attack-defense spoofed-reset

使用 **attack-defense spoofed-reset** 命令设置 TCP 逃避控制的伪造 TCP 重置保护的阈值。

命令

attack-defense *zone_name* **spoofed-reset** {**RST** *threshold_value* [**Period** *threshold_value* [**Block** *threshold_value*] | **Block** *threshold_value* [**Period** *threshold_value*]] | **Period** *threshold_value* [**RST** *threshold_value* [**Block** *threshold_value*] | **Block** *threshold_value* [**RST** *threshold_value*]] | **Block** *threshold_value* [**Period** *threshold_value* [**RST** *threshold_value*] | **RST** *threshold_value* [**Period** *threshold_value*]]}

语法

zone_name	安全域名称，格式为 WORD<1-15>。
RST	表示设置最多允许通过的 RST 数据包的个数，缺省值为 5。
Period	表示设置 RST 数据包通过的时间范围，缺省值为 15 秒。
Block	表示设置阻断 RST 数据包的时间周期，缺省值为 120 秒。
threshold_value	阈值，该值可以是数据包的个数，也可以是单位时间值，格式为 INTEGER<2-10000>。

说明

1. NetEye 管理员可以同时设置多个 TCP 逃避控制的伪造 TCP 重置保护的阈值。
2. 只有在规定的时间，通过指定的 RST 数据包个数时，才能触发 RST 数据包的阻断。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 在安全域 test 内，设置 RST 数据包的阻断周期为 150 秒。

```
NetEye@root-system]attack-defense test spoofed-reset Block 150
```

相关命令

命令名称	描述信息
show attack-defense	查看指定安全域内攻击防御的各项设置。
attack-defense	在指定安全域内设置特定攻击类型的防御。
attack-defense tcp-syn-cookie	在指定安全域内启用或者禁用 SYN Cookie 防御。

attack-defense small-pmtu

使用 **attack-defense small-pmtu** 命令设置 TCP 逃避控制的最小 MTU 值，防止 Small PMTU 形式的带宽攻击发生。

命令

attack-defense *zone_name* **small-pmtu parameter** *threshold_value*

语法

zone_name	安全域名称，格式为 WORD<1-15>。
threshold_value	最小 MTU 值，格式为 INTEGER<68-512>，缺省值为 350。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 在安全域 test 内，设置最小 MTU 值为 400。

```
NetEye@root-system]attack-defense test small-pmtu parameter 400
```

相关命令

命令名称	描述信息
show attack-defense	查看指定安全域内攻击防御的各项设置。
attack-defense	在指定安全域内设置特定攻击类型的防御。
attack-defense tcp-syn-cookie	在指定安全域内启用或者禁用 SYN Cookie 防御。

attack-defense threshold

使用 **attack-defense threshold** 命令在指定安全域内设置 icmp-flood、 tcp-syn-flood、 udp-flood、 ip-address-sweep 或 tcp-syn-port-scan 防御的阈值。

命令

attack-defense *zone_name* {{**icmp-flood** | **tcp-syn-flood** | **udp-flood**} **threshold** *threshold_flood* | **ip-address-sweep threshold** *threshold_sweep* | **tcp-syn-port-scan threshold** *threshold_scan*}

语法

zone_name	安全域名称，格式为 WORD<1-15>。
threshold	阈值，该值可以是数据包的个数，也可以是单位时间值。
threshold_flood	每秒允许通过的数据包个数，单位为个 / 秒，格式为 INTEGER <1-1000000>， icmp-flood 阈值缺省为 10000， tcp-syn-flood 阈值缺省为 100000， udp-flood 阈值缺省为 100000。
threshold_sweep	IP 地址扫描检测的时间间隔，单位为毫秒，该时间间隔必须为 100 毫秒的倍数，格式为 INTEGER<100-10000>，缺省值为 100。
threshold_scan	TCP SYN 端口扫描检测的时间间隔，单位为秒，格式为 INTEGER<1-7200>，缺省值为 1。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 在安全域 test 内设置 udp-flood 防御的阈值为 2000。

```
NetEye@root-system]attack-defense test udp-flood threshold 2000
```

相关命令

命令名称	描述信息
show attack-defense	查看指定安全域内攻击防御的各项设置。

show attack-defense

使用 **show attack-defense** 命令查看指定安全域内攻击防御的各项设置。

命令

show attack-defense *zone_name* [**dos-defense** | **reconnaissance-defense** | **ip-options** | **tcp-evasion-control** | **icmp-attack-defense**]

语法

zone_name	安全域名称，格式为 WORD<1-15>。
dos-defense | **reconnaissance-defense** | **ip-options** | **tcp-evasion-control** | **icmp-attack-defense**	• dos-defense—拒绝服务攻击防御 • reconnaissance-defense—攻击探测防御 • ip-options—IP 选项数据包攻击 • tcp-evasion-control—TCP 逃避控制 • icmp-attack-defense—ICMP 攻击防御

说明

如果不指定 **dos-defense**、 **reconnaissance-defense**、 **ip-options**、 **tcp-evasion-control** 或 **icmp-attack-defense** 关键字，则查看指定安全域内所有攻击防御的各项设置。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看安全域 test 内拒绝服务攻击防御的各项设置。

```
NetEye@root>show attack-defense test dos-defense
```

【返回结果】

```
Attack Defense Configuration:
Zone: test

DoS Defense
Name                            Active  Threshold       Action
ICMP Flood                      Off     10000           Alert Drop
```

```
TCP SYN Flood                  Off     100000          Alert Drop
UDP Flood                      Off     100000          Alert Drop
TCP RST Scan                   Off
WinNuke                        On                      Alert Drop
LAND                           On                      Alert Drop
Smurf                          On                      Alert Drop
TCP SYN Cookie                 Off
Ping of Death                  On                      Drop
Teardrop                       On                      Drop
```

15 深度检测命令

规则更新

show update configure information

使用 **show update configure information** 命令显示当前规则库更新方式。

命令

show update configure information

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示当前规则库更新方式。

```
NetEye@root> show update configure information
```

【返回结果】

```
Update mode: Internet
Server URL: nts.neusoft.com/autoupdate
Rule base: ips,av
Schedule: disable
```

show update rulebase

使用 **show update rulebase** 命令显示规则库的当前状态。

命令

show update rulebase

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

说明

管理员可以对 NetEye 的防病毒和攻击签名规则库进行更新。

模式

该命令在普通配置模式下使用。

范例

范例 . 显示规则库的当前状态。

```
NetEye@root> show update rulebase
```

【返回结果】

```
Software Name: Neusoft NetEye NISG
Software Version: 4.2-BUILD10043

Rule Base  Rule Version Engine Version Last Update        Service State
HTTP       1.0.0        1.0            2009-10-27 18:51:05 Valid to 2010-05-06
UTC
DNS        1.0.0        1.0            2009-10-27 18:52:36 Valid to 2010-05-06
UTC
FTP        1.0.0        1.0            2009-10-27 18:53:24 Valid to 2010-05-06
UTC
IMAP       1.0.0        1.0            2009-10-27 18:54:05 Valid to 2010-05-06
UTC
Oracle     1.0.0        1.0            2009-10-27 18:56:03 Valid to 2010-05-06
UTC
Others     1.0.0        1.0            2009-10-27 18:57:05 Valid to 2010-05-06
UTC
```

```
POP3        1.0.0        1.0            2009-10-27 18:58:56 Valid to 2010-05-06
UTC
SIP         1.0.0        1.0            2009-10-27 19:00:02 Valid to 2010-05-06
UTC
SMTP        1.0.0        1.0            2009-10-27 19:08:03 Valid to 2010-05-06
UTC
Telnet      1.0.0        1.0            2009-10-27 19:10:48 Valid to 2010-05-06
UTC
Tftp        1.0.0        1.0            2009-10-27 19:11:05 Valid to 2010-05-06
UTC
Backdoor    1.0.0        1.0            2009-10-27 19:15:38 Valid to 2010-05-06
UTC
Anti-Virus 1.0.0         1.0            2009-10-27 12:18:51 Valid to 2010-05-06
UTC
```

update rulebase auto immediately

使用 **update rulebase auto immediately** 命令立即进行规则库自动更新。

命令

update rulebase auto immediately

说明

要自动更新规则库，必须先设置规则库的更新方式 （即 SCM 服务器或互联网），并指定规则库自动更新的服务器地址。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
update rulebase auto item	设置规则库自动更新的内容选项。
update rulebase auto schedule	设置规则库自动更新周期。
update rulebase auto schedule start, stop	开启或关闭规则库自动更新计划。
update rulebase auto server	设置规则库自动更新的服务器地址。
update rulebase auto type	设置规则库自动更新的方式。

update rulebase auto item

使用 **update rulebase auto item** 命令设置规则库自动更新的内容选项。

命令

update rulebase auto item (attack-signature | av | all)

语法

attack-signature | av | all	• attack-signature—攻击签名规则库 • av— 防病毒规则库 • all— 攻击签名和防病毒规则库

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
update rulebase auto immediately	立即进行规则库自动更新。
update rulebase auto schedule	设置规则库自动更新周期。
update rulebase auto schedule start, stop	开启或关闭规则库自动更新计划。
update rulebase auto server	设置规则库自动更新的服务器地址。
update rulebase auto type	设置规则库自动更新的方式。

update rulebase auto schedule

使用 **update rulebase auto schedule** 命令设置规则库自动更新周期。

命令

update rulebase auto schedule {**monthly** *day time* | **weekly** *weekday time* | **daily** *time* | **interval** *hour_interval*}

语法

monthly	每月中某一天的固定时刻进行规则库更新。
day	日期，格式为 WORD<1-28>。
time	时间，格式为 HH:MM。
weekly	每周中某一天的固定时刻进行规则库更新。
weekday	星期，格式为 INTEGER<1-7>。
daily	每天的固定时刻进行规则库更新。
interval	每隔 N 小时进行规则库更新。
hour_interval	小时间隔，格式为 INTEGER<1-24>。

说明

1. 要自动更新规则库，必须先设置规则库的更新方式 （即 SCM 服务器或互联网），并指定规则库自动更新的服务器地址。
2. 要设置规则库自动更新周期，必须先开启规则库自动更新计划。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 设置每月的 23 号 9 时进行规则库更新。

```
NetEye@root-system]update rulebase auto schedule monthly 23 9:00
```

相关命令

命令名称	描述信息
update rulebase auto immediately	立即进行规则库自动更新。
update rulebase auto item	设置规则库自动更新的内容选项。
update rulebase auto schedule start, stop	开启或关闭规则库自动更新计划。
update rulebase auto server	设置规则库自动更新的服务器地址。
update rulebase auto type	设置规则库自动更新的方式。

update rulebase auto schedule start, stop

使用 **update rulebase auto schedule start, stop** 命令开启或关闭规则库自动更新计划。

命令

update rulebase auto schedule {start | stop}

语法

start | stop	• start—开启规则库自动更新计划 • stop— 关闭规则库自动更新计划

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
update rulebase auto immediately	立即进行规则库自动更新。
update rulebase auto item	设置规则库自动更新的内容选项。
update rulebase auto schedule	设置规则库自动更新周期。
update rulebase auto server	设置规则库自动更新的服务器地址。
update rulebase auto type	设置规则库自动更新的方式。

update rulebase auto server

使用 **update rulebase auto server** 命令设置规则库自动更新的服务器地址。

命令

update rulebase auto server {*ip_address* | *domain_name*}

语法

ip_address	IP 地址，格式为 X.X.X.X。
domain_name	域名，格式为 WORD<1-255>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 设置规则库自动更新的服务器地址为 10.3.1.23。

```
NetEye@root-system]update rulebase auto server 10.3.1.23
```

相关命令

命令名称	描述信息
update rulebase auto immediately	立即进行规则库自动更新。
update rulebase auto item	设置规则库自动更新的内容选项。
update rulebase auto schedule	设置规则库自动更新周期。
update rulebase auto schedule start, stop	开启或关闭规则库自动更新计划。
update rulebase auto type	设置规则库自动更新的方式。

update rulebase auto type

使用 **update rulebase auto type** 命令设置规则库自动更新的方式。

命令

update rulebase auto type {internet | scm}

语法

internet | scm	• internet—通过互联网进行规则库自动更新 • scm— 通过 SCM 服务器进行规则库自动更新

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
update rulebase auto immediately	立即进行规则库自动更新。
update rulebase auto item	设置规则库自动更新的内容选项。
update rulebase auto schedule	设置规则库自动更新周期。
update rulebase auto schedule start, stop	开启或关闭规则库自动更新计划。
update rulebase auto server	设置规则库自动更新的服务器地址。

update rulebase manu

使用 **update rulebase manu** 命令上载规则库升级包。

命令

update rulebase manu from {**tftp** *ip_tftp file_name* | **sftp** *ip_sftp* **user** *user_name* **password** *passwd file_name* | **x/zmodem**}

语法

tftp	简单文件传输协议，表示通过 TFTP 服务器上载规则库升级包。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
file_name	升级包名称，格式为 WORD<1-128>。
sftp	安全文件传输协议，表示通过 SFTP 服务器上载规则库升级包。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-64>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-64>。
x/zmodem	异步文件传输协议， Xmodem 或 Zmodem 由系统自动选择。表示通过 X/Zmodem 协议上载规则库升级包。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 通过 TFTP 服务器 10.3.1.23 上载规则库升级包 test。

```
NetEye@root-system]update rulebase manu from tftp 10.3.1.23 test
```

防病毒

av engine internal, external

使用 **av engine internal, external** 命令设置防病毒策略，包括内部防病毒与外部防病毒。

命令

av engine {**internal** | **external**}

语法

internal | **external**	• internal — 启用集成于 NetEye 的防病毒引擎 • external — 启用外部防病毒引擎 缺省设置为 internal

说明

内部防病毒支持对 HTTP、 FTP、 SMTP、 POP3 和 IMAP 的病毒检测；外部防病毒支持对 HTTP 的病毒检测。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

av internal file oversize

使用 **av internal file oversize** 命令设置当待扫描文件的大小超出内部防病毒引擎扫描范围时，防病毒引擎采取的处理动作。

命令

av internal file oversize {**block** | **pass**}

语法

block | **pass**	• block — 阻断文件 • pass — 放行文件 缺省设置为 block

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
av internal file scan-limit	设置内部防病毒引擎对文件大小的限制。
av internal file type block, pass,scan	设置内部防病毒引擎针对特定类型文件所采取的动作。
av internal file unrecognized	设置当内部防病毒引擎对文件类型无法识别时所采取的动作。

av internal file scan-limit

使用 **av internal file scan-limit** 命令设置内部防病毒引擎对文件大小的限制。当待扫描的文件大小超出扫描范围时，防病毒引擎将不再对文件进行扫描，直接采取阻断或放行的处理动作。

命令

av internal file scan-limit *file_size*

语法

file_size	文件大小限制，单位为 MB，格式为 INTEGER<1-256>。 缺省值为 20

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
av internal file oversize	设置当待扫描文件的大小超出内部防病毒引擎扫描范围时，防病毒引擎采取的处理动作。
av internal file signature enable, disable	启用或禁用基于文件特征识别文件类型。
av internal file type block, pass,scan	设置内部防病毒引擎针对特定类型文件所采取的动作。
av internal file unrecognized	设置当内部防病毒引擎对文件类型无法识别时所采取的动作。

av internal file signature enable, disable

使用 **av internal file signature enable, disable** 命令启用或禁用基于文件特征来识别文件类型。

命令

av internal file signature {**enable** | **disable**}

语法

enable	**disable**	• enable — 启用基于文件特征来识别文件类型 • disable— 禁用基于文件特征来识别文件类型

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
av internal file type block, pass,scan	设置内部防病毒引擎针对特定类型文件所采取的动作。

av internal file type block, pass, scan

使用 **av internal file type block, pass, scan** 命令设置内部防病毒引擎针对特定类型文件所采取的处理动作。

命令

av internal file type *file_type* {**block** | **pass** | **scan**}

语法

file_type	文件类型，格式为 WORD<1-15>。
block | **pass** | **scan**	• block — 阻断文件 • pass — 放行文件 • scan — 扫描文件

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 设置针对 .gif 类型的文件，内部防病毒引擎不对其进行扫描，直接采取放行的处理动作。

```
NetEye@root-system]av internal file type gif pass
```

相关命令

命令名称	描述信息
av internal file oversize block, pass	设置当待扫描文件的大小超出内部防病毒引擎扫描范围时，防病毒引擎采取的处理动作。
av internal file scan-limit	设置内部防病毒引擎对文件大小的限制。
av internal file unrecognized	设置当内部防病毒引擎对文件类型无法识别时所采取的动作。

av internal file unrecognized

使用 **av internal file unrecognized** 命令设置当内部防病毒引擎对待扫描文件类型无法识别时，所采取的处理动作。

命令

av internal file unrecognized {**block** | **pass** | **scan**}

语法

block | **pass** | **scan**	• block — 阻断文件 • pass — 放行文件 • scan — 扫描文件 缺省设置为 scan

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
av internal file oversize	设置当待扫描文件的大小超出内部防病毒引擎扫描范围时，防病毒引擎采取的处理动作。
av internal file scan-limit	设置内部防病毒引擎对文件大小的限制。
av internal file type block, pass,scan	设置内部防病毒引擎针对特定类型文件所采取的动作。

av internal scan continue-download

使用 **av internal scan continue-download** 命令针对不同类型服务，启用或禁用持续下载功能。

命令

av internal scan continue-download service {http | ftp | smtp | pop3 | imap} {enable | disable}

语法

enable | disable	• enable — 启用持续下载功能 • disable — 禁用持续下载功能

说明

持续下载是指当客户端下载文件时，为了避免病毒扫描时数据传输阻塞引起连接超时，NetEye 将该文件已下载的一部分传给客户端。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 启用 FTP 服务的持续下载功能。

```
NetEye@root-system]av internal scan continue-download service ftp
enable
```

av internal scan initialize-fail

使用 **av internal scan initialize-fail** 命令设置当内部防病毒引擎初始化失败时，对待扫描文件采取的处理动作。

命令

av internal scan initialize-fail {**block** | **pass**}

语法

block	**pass**	• block — 阻断文件 • pass — 放行文件 缺省设置为 block

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
av internal scan overload-or-scan-fails	设置当内部防病毒引擎由于过载或扫描失败时，对待扫描文件采取的处理动作。
av internal scan virus-detect	设置当内部防病毒引擎检测到病毒时，对病毒文件采取的处理动作。

av internal scan overload-or-scan-fails

使用 **av internal scan overload-or-scan-fails** 命令设置当内部防病毒引擎由于过载或扫描失败时，对待扫描文件采取的处理动作。

命令

av internal scan overload-or-scan-fails {block | pass}

语法

block | pass	• block — 阻断文件 • pass — 放行文件 缺省设置为 block

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
av internal scan initialize-fail	设置当内部防病毒引擎初始化失败时，对待扫描文件采取的处理动作。
av internal scan virus-detect	设置当内部防病毒引擎检测到病毒时，对病毒文件采取的处理动作。

av internal scan virus-detect

使用 **av internal scan virus-detect** 命令设置当内部防病毒引擎检测到病毒时，对病毒文件采取的处理动作。

命令

av internal scan virus-detect {block | pass}

语法

block | pass	• block — 阻断病毒文件 • pass — 放行病毒文件 缺省设置为 block

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
av internal scan initialize-fail	设置当内部防病毒引擎初始化失败时，对待扫描文件采取的处理动作。
av internal scan overload-or-scan-fails	设置当内部防病毒引擎由于过载或扫描失败时，对待扫描文件采取的处理动作。

icap_server

使用 **icap server** 命令设置外部防病毒服务器。

命令

icap_server {*ip_address* | *domain_name*} *port* {**request** *request_application* [**response** *response_application*] | **response** *response_application* [**request** *request_application*]}

语法

ip_address	外部防病毒服务器 IP 地址，格式为 X.X.X.X。
domain_name	外部防病毒服务器域名，格式为 WORD<8-255>。
port	外部防病毒服务器端口号，格式为 INTEGER<1-65535>。
request_application	请求服务程序，格式为 WORD<1-64>。
response_application	应答服务程序，格式为 WORD<1-64>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 设置外部防病毒服务器，指定其 IP 地址为 10.3.1.23，端口号为 5555。

```
NetEye@root-system]icap_server 10.3.1.23 5555 requset /av/reqmod
```

相关命令

命令名称	描述信息
show icap_server configure information	查看外部防病毒服务器设置。

icap_server action

使用 **icap server action** 命令设置当外部防病毒服务器不可达时，对待扫描文件的处理动作。

命令

icap_server action {block | pass}

语法

block | pass	• block — 阻断待扫描文件 • pass — 放行待扫描文件

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show icap_server configure information	查看外部防病毒服务器设置。

show av engine

使用 **show av engine** 命令查看防病毒引擎配置。

命令

show av engine

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看防病毒引擎配置。

```
NetEye@root>show av engine
```

【返回结果】

```
Internal: On
External: off
```

show av internal file-setting

使用 **show av internal file-setting** 命令查看内部防病毒引擎针对文件的扫描设置。

命令

show av internal file-setting

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看内部防病毒引擎针对文件的扫描设置。

```
NetEye@root>show av internal file-setting
```

【返回结果】

```
Max File Size To Scan: 20 MBytes
When File Oversizes: block
--------------------------------
When File Type Unrecognized: scan
File type signatures (magic numbers) examming: enable

File Type Description                                Action
7z        7z archive data                             pass
Z         UNIX Compressed Archive File                block
ace       ACE compressed archive                      scan
afx       AFX compressed file data                    pass
arc       LH ARC old version                          pass
arj       arj archive data                            pass
avi       Audio Video Interleave File                 pass
bat       MS-DOS batch file text                      pass
bh        BlackHole Archive Format File               scan
bmp       PC bitmap data                              pass
bz2       bzip2 compressed data                       block
```

cab	Microsoft Cabinet file	scan
chm	MS Windows HtmlHelp Data	pass
class	compiled Java class data	block
csf	Photoshop Color Settings	pass
dat	Data	pass
dll	MS Windos PE	block
dmf	MS-Windows special zipped file	pass
emf	Windows Enhanced Metafile image	pass
eps	DOS EPS Binary File	scan
exe	MS-DOS executable	scan
flash	interactive animations on the web	block
gif	Graphics Interchange Format	block
gzip	gzip compressed data	scan
hlp	MS Windows Help Data	scan
html	HTML document text	block
ico	Icon for ms-windows	block
jp2	JPEG 2000 image data	pass
jpg	JPEG image data	pass
js	JavaScript Source Code	block
lzh	Compressed Archive File	scan
lzo	lzop compressed data	pass
m4a	MPEG-4 Audio Layer	block
mp2	MPEG ADTS, layer 2	pass
mp3	MP3 file with ID3 version2	block
mpa	MPEG ADTS, layer 1	pass
mpeg	MPEG-4 LOAS	scan
mpg	JVT NAL sequence	pass
office	Microsoft Office Document	pass
ogg	Ogg Vorbis Codec Compressed Multimedia File	block
pcx	PCX image data	pass
pdf	pdf document	scan
pdg	Chaoxing Digital Library files	pass
perl	perl script text executable	pass
php	PHP Script	block
png	PNG image data	pass
postscript	postscript document text	block
psd	Photoshop Format	block
qt	Apple QuickTime	pass

rar	Rar archive data	block
reg	Windows registery file	block
rm	RealMedia Streaming Media	pass
rpm	LINUX Package file	pass
rtf	Rich Text Format data	pass
sct	Foxpro Screen	block
shar	shell archive text	block
sig	PGP sig	block
sqx	SQX Archiver Compressed Archive	block
tar	Tape Archive File	pass
tif	TIFF image data	scan
wma	WMA Real Media File	block
wmf	ms-windows metafont	block
xml	XML document text	block
zip	Zip archive data	pass
zoo	Zoo archive data	pass

show av internal scan-setting

使用 **show av internal scan-setting** 命令查看内部防病毒引擎处理动作的设置。

命令

show av internal scan-setting

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看内部防病毒引擎处理动作的设置。

```
NetEye@root>show av internal scan-setting
```

【返回结果】

```
When Virus Detect: block
When Engine Overload: block
When Engine Fail: block
Continue Download       Status
http                    enable
ftp                     enable
smtp                    enable
pop3                    enable
imap                    enable
```

show icap_server configure information

使用 **show icap_server configure information** 命令查看外部防病毒服务器设置。

命令

show icap_server configure information

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 查看外部防病毒服务器设置。

```
NetEye@root>show icap_server configure imformation
```

【返回结果】

```
ICAP service is on
Host:10.3.1.23
Port:44
Program
  Request:/av/reqmod
  Response:aaa
When the server cannot be reached:Block
```

相关命令

命令名称	描述信息
icap_server	设置外部防病毒服务器。

show monitor anti-virus

使用 **show monitor anti-virus** 命令显示 AV 的监控信息。

命令

show monitor anti-virus

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 AV 的监控信息。

```
NetEye@root>show monitor anti-virus
```

反垃圾邮件

as allow-list, block-list export ip

使用 **as allow-list, block-list export ip** 命令导出 IP 允许列表或 IP 阻断列表。

命令

as {**allow-list | block-list**} **export** {**tftp ip** *ip_tftp file_name* | **sftp ip** *ip_sftp user_name passwd file_name* | **zmodem ip**}

语法

tftp	简单文件传输协议，表示导出 IP 允许列表或 IP 阻断列表到 TFTP 服务器上。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
file_name	文件名称，格式为 WORD<1-100>。
sftp	安全文件传输协议，表示导出 IP 允许列表或 IP 阻断列表到 SFTP 服务器上。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-100>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-100>。
zmodem	异步文件传输协议。表示使用 Zmodem 协议导出 IP 允许列表或 IP 阻断列表。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 导出 IP 允许列表 test 到 TFTP 服务器 192.168.1.125。

```
NetEye@root-system]as allow-list export tftp ip 192.168.1.125 test
```

相关命令

命令名称	描述信息
as allow-list, block-list import ip	导入 IP 允许列表或 IP 阻断列表。

as allow-list, block-list export sender

使用 **as allow-list, block-list export sender** 命令导出发件人允许列表或发件人阻断列表。

命令

as {**allow-list | block-list**} **export** {**tftp sender** *ip_tftp file_name* | **sftp sender** *ip_sftp user_name passwd file_name* | **zmodem sender**}

语法

tftp	简单文件传输协议，表示导出发件人允许列表或发件人阻断列表到 TFTP 服务器上。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
file_name	文件名称，格式为 WORD<1-100>。
sftp	安全文件传输协议，表示导出发件人允许列表或发件人阻断列表到 SFTP 服务器上。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-100>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-100>。
zmodem	异步文件传输协议。表示使用 Zmodem 协议导出发件人允许列表或发件人阻断列表。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 导入发件人允许列表 list1 到 SFTP 服务器 192.168.1.125， SFTP 服务器的用户名和密码均为 test。

```
NetEye@root-system]as allow-list export sftp sender 192.168.1.125  test
test list1
```

相关命令

命令名称	描述信息
as allow-list, block-list import sender	导入发件人允许列表或发件人阻断列表。

as allow-list, block-list import ip

使用 **as allow-list, block-list import ip** 命令导入 IP 允许列表或 IP 阻断列表。

命令

as {**allow-list | block-list**} **import** {**tftp ip** *ip_tftp file_name* | **sftp ip** *ip_sftp user_name passwd file_name* | **zmodem ip**}

语法

tftp	简单文件传输协议，表示从 TFTP 服务器导入 IP 允许列表或 IP 阻断列表。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
file_name	文件名称，格式为 WORD<1-100>。
sftp	安全文件传输协议，表示从 SFTP 服务器导入 IP 允许列表或 IP 阻断列表。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-100>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-100>。
zmodem	异步文件传输协议。表示使用 Zmodem 协议导入 IP 允许列表或 IP 阻断列表。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 从 TFTP 服务器 192.168.1.125 导入 IP 允许列表 test。

```
NetEye@root-system]as allow-list import tftp ip 192.168.1.125 test
```

相关命令

命令名称	描述信息
as allow-list, block-list export ip	导出 IP 允许列表或 IP 阻断列表。

as allow-list, block-list import sender

使用 **as allow-list, block-list import sender** 命令导入发件人允许列表或发件人阻断列表。

命令

as {**allow-list | block-list**} **import** {**tftp sender** *ip_tftp file_name* | **sftp sender** *ip_sftp user_name passwd file_name* | **zmodem sender**}

语法

tftp	简单文件传输协议，表示从 TFTP 服务器导入发件人允许列表或发件人阻断列表。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
file_name	文件名称，格式为 WORD<1-100>。
sftp	安全文件传输协议，表示从 SFTP 服务器导入发件人允许列表或发件人阻断列表。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-100>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-100>。
zmodem	异步文件传输协议。表示使用 Zmodem 协议导入发件人允许列表或发件人阻断列表。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 从 SFTP 服务器 192.168.1.125 导入发件人允许列表 list1， SFTP 服务器的用户名和密码均为 test。

```
NetEye@root-system]as allow-list import sftp sender 192.168.1.125  test
test list1
```

相关命令

命令名称	描述信息
as allow-list, block-list export sender	导出发件人允许列表或发件人阻断列表。

as allow-list, block-list ip

使用 **as allow-list, block-list ip** 命令配置 IP 允许列表或 IP 阻断列表。

命令

as {**allow-list** | **block-list**} **ip** *ip_address* {**enable** | **disable**}

语法

ip_address	IP 地址，格式为 x.x.x.x。
enable	**disable**	• enable — 启用该 IP 地址条目 • disable — 禁用该 IP 地址条目

说明

1. 如果列表中不存在与输入的参数匹配的条目，则表示添加；如果存在匹配的条目，则表示修改相应条目的状态。
2. 发件人的IP地址首先与IP允许列表进行匹配，再与IP阻断列表进行匹配。如果与IP允许列表某 IP 地址条目相一致，则直接转发邮件；如果与 IP 阻断列表某 IP 地址条目相一致，则直接阻断该连接。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 向 IP 阻断列表中添加 IP 地址条目 202.118.34.57。

```
NetEye@root-system]as block-list ip 202.118.34.57 enable
```

相关命令

命令名称	描述信息
show as allow-list, block-list ip	显示 IP 允许列表或 IP 阻断列表中的 IP 地址条目。
unset as allow-list, block-list ip	删除 IP 允许列表或 IP 阻断列表中的 IP 地址条目。

as allow-list, block-list sender

使用 **as allow-list, block-list sender** 命令配置发件人允许列表或发件人阻断列表。

命令

as {**allow-list** | **block-list**} **sender** *email* {**enable** | **disable**}

语法

email	邮件地址允许的字符，如只输入域名或完整的邮件地址。格式为 WORD<1-255>。
enable | **disable**	• enable — 启用该邮件地址条目 • disable — 禁用该邮件地址条目

说明

1. 如果列表中不存在与输入的参数匹配的条目，则表示添加；如果存在匹配的条目，则表示修改相应条目的状态。
2. 发件人邮件地址首先与允许列表进行匹配，再与阻断列表进行匹配。如果与发件人允许列表某邮件地址条目相一致，则直接转发邮件；如果与发件人阻断列表某邮件地址条目相一致，则直接阻断该连接。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 向发件人阻断列表中添加邮件地址条目 test.com。

```
NetEye@root-system]as block-list sender test.com enable
```

相关命令

命令名称	描述信息
show as allow-list, block-list sender	显示发件人允许列表或发件人阻断列表中的邮件地址条目。
unset as allow-list, block-list sender	删除发件人允许列表或发件人阻断列表中的邮件地址条目。

as scan overload

使用 **as scan overload** 命令设置当防垃圾邮件引擎过载或扫描失败时，对待扫描邮件的处理动作。

命令

as scan overload {**block** | **pass**}

语法

block | **pass**	• block — 阻断邮件 • pass — 转发邮件

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show as scan-setting	显示垃圾邮件扫描设置。

as scan spam-detect

使用 **as scan spam-detect** 命令设置当防垃圾邮件引擎检测到垃圾邮件时，对邮件采取的处理动作。

命令

as scan spam-detect {block | pass | tag}

语法

block | pass | tag	• block — 阻断垃圾邮件 • pass — 转发垃圾邮件 • tag — 标记并转发垃圾邮件

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show as scan-setting	显示垃圾邮件扫描设置。

as scan timeout

使用 **as scan timeout** 命令设置当防垃圾邮件引擎响应超时时，对待扫描邮件的处理动作。

命令

as scan timeout {**block** | **pass**}

语法

block	**pass**	• block — 阻断邮件 • pass — 转发邮件

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show as scan-setting	显示垃圾邮件扫描设置。

as spam-word

使用 **as spam-word** 命令向垃圾邮件关键字列表中添加关键字条目。

命令

as spam-word *string* **location** {**subject** | **body** | **both**} **score** *score_value* {**enable** | **disable**}

语法

string	关键字条目，格式为 WORD<2-48>。
subject | **body** | **both**	• subject — 表示关键字应用于标题过滤 • body — 表示关键字应用于正文过滤 • both — 表示关键字应用于标题和正文过滤
score_vlaue	分值，格式为 INTEGER<1-100>。
enable | **disable**	• enable — 启用该关键字条目 • disable — 禁用该关键字条目

说明

分值指对邮件的标题和正文进行关键字检测时，每检查到一次与关键字相符的字符串时所加的分值，当分值总和超出分数阈值时，则按照垃圾邮件进行处理。关于分数阈值的设置，请参见 **as spam-word score** 命令。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 向垃圾邮件关键字列表中添加关键字条目 @test.com，指定其应用于标题过滤，分值设置为 15，并启用该关键字条目。

```
NetEye@root-system]as spam-word @test.com location subject score 15
enable
```

相关命令

命令名称	描述信息
as spam-word enable, disable	启用或禁用垃圾邮件关键字列表中指定的关键字条目。
show as spam-word	显示垃圾邮件关键字列表的配置信息。
unset as spam-word	删除垃圾邮件关键字列表中的关键字条目。

as spam-word action

使用 **as spam-word action** 命令设置当邮件标题或正文中检测到用户自定义关键字的分值总和超出分数阈值时，对邮件采取的处理动作。

命令

as spam-word action {block | pass | tag}

语法

block | pass | tag	• block — 阻断邮件 • pass — 转发邮件 • tag — 标记并转发邮件

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

as spam-word enable, disable

使用 **as spam-word enable, disable** 命令启用或禁用垃圾邮件关键字列表中指定的关键字条目。

命令

as spam-word *string* {**enable** | **disable**}

语法

string	关键字条目，格式为 WORD<2-48>。
enable | **disable**	• enable — 启用指定的关键字条目 • disable — 禁用指定的关键字条目

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
as spam-word	向垃圾邮件关键字列表中添加关键字条目。
show as spam-word	显示垃圾邮件关键字列表的配置信息。
unset as spam-word	删除垃圾邮件关键字列表中的关键字条目。

as spam-word export

使用 **as spam-word export** 命令导出垃圾邮件关键字列表。

命令

as spam-word export {**tftp** *ip_tftp file_name* | **sftp** *ip_sftp user_name passwd file_name* | **zmodem**}

语法

tftp	简单文件传输协议，表示导出垃圾邮件关键字列表到 TFTP 服务器上。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
file_name	文件名称，格式为 WORD<1-100>。
sftp	安全文件传输协议，表示导出垃圾邮件关键字列表到 SFTP 服务器上。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-100>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-100>。
zmodem	异步文件传输协议。表示使用 Zmodem 协议导出垃圾邮件关键字列表。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 使用 Zmodem 协议导出垃圾邮件关键字列表。

```
NetEye@root-system]as spam-word export zmodem
```

相关命令

命令名称	描述信息
as spam-word import	导入垃圾邮件关键字列表。

as spam-word import

使用 **as spam-word import** 命令导入垃圾邮件关键字列表。

命令

as spam-word import {**tftp** *ip_tftp file_name* | **sftp** *ip_sftp user_name passwd file_name* | **zmodem**}

语法

tftp	简单文件传输协议，表示从 TFTP 服务器导入 垃圾邮件关键字列表。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
file_name	文件名称，格式为 WORD<1-100>。
sftp	安全文件传输协议，表示从 SFTP 服务器导入垃圾邮件关键字列表。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-100>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-100>。
zmodem	异步文件传输协议。表示使用 Zmodem 协议导入垃圾邮件关键字列表。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 使用 Zmodem 协议导入垃圾邮件关键字列表。

```
NetEye@root-system]as spam-word import zmodem
```

相关命令

命令名称	描述信息
as spam-word export	导出垃圾邮件关键字列表。

as spam-word score

使用 **as spam-word score** 命令设置垃圾邮件关键字列表的分数阈值。

命令

as spam-word score *score_value*

语法

score_value	分数阈值，格式为 INTEGER<100-1000>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置垃圾邮件关键字列表的分数阈值为 800。

```
NetEye@root-system]as spam-word score 800
```

show as allow-list, block-list ip

使用 **show as allow-list, block-list ip** 命令显示 IP 允许列表或 IP 阻断列表中的 IP 地址条目。

命令

show as {**allow-list** | **block-list**} **ip** [*ip_address*]

语法

ip_address	IP 地址，格式为 x.x.x.x。

说明

如果不指定 *ip_address* 参数，则显示 IP 允许列表或 IP 阻断列表中的所有 IP 地址条目。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 IP 允许列表中所有的 IP 地址条目。

```
NetEye@root>show as allow-list ip
```

【返回结果】

```
IP Address          State
10.3.1.23           Enable
10.10.1.12          Enable
```

相关命令

命令名称	描述信息
as allow-list, block-list ip	配置 IP 允许列表或 IP 阻断列表
unset as allow-list, block-list ip	删除 IP 允许列表或 IP 阻断列表中的 IP 地址条目。

show as allow-list, block-list sender

使用 **show as allow-list, block-list sender** 命令显示发件人允许列表或发件人阻断列表中的邮件地址条目。

命令

show as {**allow-list** | **block-list**} **sender** [*email*]

语法

email	邮件地址允许的字符，如只输入域名或完整的邮件地址。格式为 WORD<1-255>。

说明

如果不指定 *email* 参数，则显示发件人允许列表或发件人阻断列表中所有的邮件地址条目。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示发件人阻断列表中所有的邮件地址条目。

```
NetEye@root>show as block-list sender
```

【返回结果】

```
Email                                                    State
test.com                                                 Enable
buy.com                                                  Enable
```

相关命令

命令名称	描述信息
as allow-list, block-list sender	配置发件人允许列表或发件人阻断列表
unset as allow-list, block-list sender	删除发件人允许列表或发件人阻断列表中的邮件地址条目。

show as scan-setting

使用 **show as scan-setting** 命令显示防垃圾邮件引擎处理动作的设置。

命令

show as scan-setting

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示防垃圾邮件引擎处理动作的设置。

```
NetEye@root>show as scan-setting
```

【返回结果】

```
When Spam Detect:Block
When Engine Timeout:Block
When Engine Overload:Block
```

相关命令

命令名称	描述信息
as scan overload	设置当防垃圾邮件引擎过载或扫描失败时，对待扫描邮件的处理动作。
as scan spam-detect	设置当防垃圾邮件引擎检测到垃圾邮件时，对邮件采取的处理动作。
as scan timeout	设置当防垃圾邮件引擎响应超时时，对待扫描邮件的处理动作。

show as spam-word

使用 **show as spam-word** 命令显示垃圾邮件关键字列表的配置信息。

命令

show as spam-word [*string*]

语法

string	垃圾邮件关键字条目，格式为 WORD<1-48>。

说明

如果不指定 *string* 参数，则显示所有垃圾邮件关键字条目的配置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示所有垃圾邮件关键字条目的配置信息。

```
NetEye@root>show as spam-word
```

【返回结果】

```
Score Threshold : 100
When Spam Word Detect : Tag

Word                                                    Location
Score          State
购物
Subject,Body        10              Enable
体育
Subject             10              Enable
休闲
Body                10              Enable
```

相关命令

命令名称	描述信息
as spam-word	向垃圾邮件关键字列表中添加关键字条目。
as spam-word enable, disable	启用或禁用垃圾邮件关键字列表中指定的关键字条目。
unset as spam-word	删除垃圾邮件关键字列表中的关键字条目。

show monitor anti-spam

使用 **show monitor anti-spam** 命令显示 AS 的监控信息。

命令

show monitor anti-spam

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 AS 的监控信息。

```
NetEye@root>show monitor anti-spam
```

unset as

使用 **unset as** 命令删除反垃圾邮件的所有配置信息。

命令

unset as

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

unset as allow-list, block-list ip

使用 **unset as allow-list, block-list ip** 命令删除 IP 允许列表或 IP 阻断列表中的 IP 地址条目。

命令

unset as {**allow-list** | **block-list**} **ip** *ip_address*

语法

ip_address	IP 地址，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
as allow-list, block-list ip	配置 IP 允许列表或 IP 阻断列表。
show as allow-list, block-list ip	显示 IP 允许列表或 IP 阻断列表中的 IP 地址条目。

unset as allow-list, block-list sender

使用 **unset as allow-list, block-list sender** 命令删除发件人允许列表或发件人阻断列表中的邮件地址条目。

命令

unset as {**allow-list | block-list**} **sender** *email*

语法

email	邮件地址允许的字符，如只输入域名或完整的邮件地址。格式为 WORD<1-255>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
as allow-list, block-list sender	配置发件人允许列表或发件人阻断列表。
show as allow-list, block-list sender	显示发件人允许列表或发件人阻断列表中的邮件地址条目。

unset as spam-word

使用 **unset as spam-word** 命令删除垃圾邮件关键字列表中的关键字条目。

命令

unset as spam-word *string*

语法

string	垃圾邮件关键字条目，格式为 WORD<2-48>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
as spam-word	向垃圾邮件关键字列表中添加关键字条目。
as spam-word enable, disable	启用或禁用垃圾邮件关键字列表中指定的关键字条目。
show as spam-word	显示垃圾邮件关键字列表的配置信息。

URL 过滤

copy url-bwls

使用 **copy url-bwls** 命令导出指定 URL 黑 / 白名单。

命令

copy url-bwls *bwl_name* **to** {**tftp** *ip_tftp* | **zmodem** | **sftp** *ip_sftp* **username** *user_name* **password** *passwd remote_path*}

语法

bwl_name	URL 黑 / 白名单名称，格式为 WORD<1-15>。
tftp	简单文件传输协议，表示将 指定 URL 黑 / 白名单导出到 TFTP 服务器。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
zmodem	异步文件传输协议，表示使用 zmodem 协议导出指定 URL 黑 / 白名单。
sftp	安全文件传输协议 ，表示将 指定 URL 黑 / 白名单导出到 SFTP 服务器。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-64>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-64>。
remote_path	存放 URL 黑 / 白名单的路径，格式为 WORD<1-256>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 使用 zmodem 协议导出 URL 白名单 whitelist1。

```
NetEye@root-system]copy url-bwls whitelist1 to zmodem
```

范例 2. 将 URL 黑名单 blacklist2 导出到 TFTP 服务器 192.168.1.152 。

```
NetEye@root-system]copy url-bwls blacklist2 to tftp 192.168.1.152
```

相关命令

命令名称	描述信息
import url-bwls	导入 URL 黑 / 白名单。

import url-bwls

使用 **import url-bwls** 命令导 入 URL 黑 / 白名单。

命令

import url-bwls {**whitelist** | **blacklist**} **from** {**tftp** *ip_tftp file_name* | **zmodem** | **sftp** *ip_sftp* **username** *user_name* **password** *passwd sftp_file_name*}

语法

tftp	简单文件传输协议，表示从 TFTP 服务器导入 URL 黑 / 白名单。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
file_name	文件名称，格式为 WORD<1-256>。
zmodem	异步文件传输协议，表示使用 zmodem 协议导 入 URL 黑 / 白名单。
sftp	安全文件传输协议 ，表示从 SFTP 服务器导入 URL 黑 / 白名单。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-64>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-64>。
sftp_file_name	URL 黑 / 白名单在 SFTP 服务器中的路径以及文件名，格式为 WORD<1-256>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 从 TFTP 服务器 192.168.122.20 导入 URL 白名单 file1。

```
NetEye@root-system]import url-bwls whitelist from tftp 192.168.122.20
file1
```

范例 2. 从 SFTP 服务器 192.168.158.28 导入 URL 黑名单 file2， SFTP 服务器的用户名、密码均为 mike。

```
NetEye@root-system]import url-bwls blacklist from sftp 192.168.158.28
username mike password mike file2
```

相关命令

命令名称	描述信息
copy url-bwls	导出指定 URL 黑 / 白名单。

show url-bwls

使用 **show url-bwls** 命令显示 URL 黑 / 白名单。

命令

show url-bwls [*bwl_name*]

语法

bwl_name	URL 黑 / 白名单名称，格式为 WORD<1-15>。

说明

如果不指定 *bwl_name* 参数，则显示所有 URL 黑 / 白名单；否则显示指定的 URL 黑白名单。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 URL 白名单 whitelist1。

```
NetEye@root>show url-bwls whitelist1
```

【返回结果】

```
Name: whitelist1
Comment: this is a whitelist
Type: Whitelist
------------------------------------------------------------------
----------------
---------------
URL List: www.test.com
```

相关命令

命令名称	描述信息
unset url-bwls	删除 指定的 URL 黑 / 白名单或指定 URL 黑 / 白名单中的特定 URL。
url-bwls whitelist, blacklist	添加 URL 黑 / 白名单或修改 指定 URL 黑 / 白名单的类型。

show url-filter scan

使用 **show url-filter scan** 命令显示 URL 过滤引擎扫描失败时的动作。

命令

show url-filter scan

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 URL 过滤引擎扫描失败时的动作。

```
NetEye@root>show url-filter sacn
```

【返回结果】

```
When the URL filtering engine fails: Allow
```

相关命令

命令名称	描述信息
url-filter scan fail	设置 URL 过滤引擎扫描失败时的动作。

unset url-bwls

使用 **unset url-bwls** 命令删除 指定的 URL 黑 / 白名单或指定 URL 黑 / 白名单中的特定 URL。

命令

unset url-bwls *bwls_name* [**url** *url_name*]

语法

bwl_name	URL 黑 / 白名单名称，格式为 WORD<1-15>。
url_name	URL，格式为 WORD<6-256>。

说明

如果不指定 *url_name* 参数，表示删除指定的 URL 黑 / 白名单 。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除 URL 白名单 whitelist1 中的 www.test.com。

```
NetEye@root-system]unset url-bwls whitelist1 url www.test.com
```

相关命令

命令名称	描述信息
show url-bwls	显示 URL 黑 / 白名单。
url-bwls whitelist, blacklist	添加 指定 URL 黑 / 白名单或修改 指定 URL 黑 / 白名单的类型。

url-bwls description

使用 **url-bwls description** 命令添加或修改指定 URL 黑 / 白名单的备注信息。

命令

url-bwls *bwl_name* **description** *string*

语法

bwl_name	URL 黑 / 白名单名称，格式为 WORD<1-15>。
string	备注信息，格式为 WORD<1-256>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加 URL 白名单 whitelist1 的备注信息 this is a whitelist。

```
NetEye@root-system]url-bwls whitelist1 description this is a whitelist
```

url-bwls url

使用 **url-bwls url** 命令为指定的 URL 黑 / 白名单添加 URL 。

命令

url-bwls *bwl_name* **url** *url_name*

语法

bwl_name	URL 黑 / 白名单名称，格式为 WORD<1-15>。
url_name	URL，格式为 WORD<6-256>。

说明

每个 URL 黑 / 白名单最多可添加 100 个 URL。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加 URL 白名单 whitelist2 的 URL 地址 www.test1.com

```
NetEye@root-system]url-bwls whitelist2 url www.test1.com
```

相关命令

命令名称	描述信息
url bwls description	添加或修改指定 URL 黑 / 白名单的备注信息。

url-bwls whitelist, blacklist

使用 **url-bwls whitelist, blacklist** 命令添加指定 URL 黑 / 白名单或修改指定 URL 黑 / 白名单的类型。

命令

url-bwls *bwl_name* {**whitelist** | **blacklist**}

语法

bwl_name	URL 黑 / 白名单名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在普通全局配置模式下使用。

范例

范例 . 将 URL 白名单 whitelist2 的类型改为黑名单。

```
NetEye@root>url-bwls whitelist2 blacklist
```

相关命令

命令名称	描述信息
show url-bwls	显示 URL 黑 / 白名单。
unset url-bwls	删除 指定 URL 黑 / 白名单或指定 URL 黑 / 白名单中的特定 URL。

url-filter scan fail

使用 **`url-filter scan fail`** 命令设置 URL 过滤引擎扫描失败时的动作。

命令

url-filter scan fail {**block** | **allow**}

语法

block | **allow**	• block—阻断 URL • allow—放行 URL

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在普通全局配置模式下使用。

相关命令

命令名称	描述信息
show url-filter scan	显示 URL 过滤引擎扫描失败时的动作。

攻击签名

attack signatures on, off

使用 **attack signatures on, off** 命令启用或禁用指定 profile 的攻击签名检测。

命令

attack signatures {**on** | **off**}

语法

on	**off**	• on— 启用攻击签名检测 • off— 禁用攻击签名检测

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

ruleset

使用 **ruleset** 命令创建自定义攻击签名规则集。

命令

ruleset *rule_set_name* [*string*]

语法

rule_set_name	规则集名称，格式为 WORD<1-64>。
string	备注信息，格式为 LINE。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
unset ruleset	命令删除指定的自定义规则集。

ruleset pre-defined enable, disable

使用 **ruleset pre-defined enable, disable** 命令启用或禁用 profile 中的指定预定义规则集。

命令

ruleset pre-defined *rule_set_name* {**enable | disable**}

语法

rule_set_name	规则集名称，格式为 WORD<1-64>。
**enable	disable**	• enable— 启用规则集 • disable— 禁用规则集

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

相关命令

命令名称	描述信息
ruleset user-defined	启用 profile 中指定的自定义规则集。

ruleset user-defined

使用 **ruleset user-defined** 命令启用 profile 中指定的自定义规则集。

命令

ruleset user-defined *rule_set_name*

语法

rule_set_name	规则集名称，格式为 WORD<1-64>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

相关命令

命令名称	描述信息
ruleset pre-defined enable, disable	启用或禁用 profile 中的指定预定义规则集。

ruleset user-defined, pre-defined

使用 **ruleset user-defined, pre-defined** 命令设置指定 profile 应用的规则集类型。

命令

ruleset {**user-defined** | **pre-defined**}

语法

user-defined | pre-defined	• user-defined— 表示应用自定义规则集 • pre-defined— 表示应用预定义规则集

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

ruleset vulnerabilities action

使用 **ruleset vulnerabilities action** 命令设置规则集中指定规则的动作。

命令

ruleset *rule_set_name* **vulnerabilities** *vulnerabilities_id* **action** {**allow | block**}

语法

rule_set_name	规则集名称，格式为 WORD<1-64>。
vulnerabilities_id	漏洞 ID，格式为 INTEGER<0-999999999>。
allow | block	• allow— 表示匹配规则的数据流量将被放行 • block— 表示匹配规则的数据流量将被阻断

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
ruleset vulnerabilities enable, disable	启用或禁用规则集中指定的规则。

ruleset vulnerabilities enable, disable

使用 **ruleset vulnerabilities enable, disable** 命令启用或禁用规则集中指定的规则。

命令

ruleset *rule_set_name* **vulnerabilities** *vulnerabilities_id* {**enable | disable**}

语法

rule_set_name	规则集名称，格式为 WORD<1-64>。
vulnerabilities_id	漏洞 ID，格式为 INTEGER<0-999999999>。
enable | disable	• enable— 表示启用规则 • disable— 表示禁用规则

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
ruleset vulnerabilities action	设置规则集中指定规则的动作。

ruleset vulnerabilities log

使用 **ruleset vulnerabilities log** 命令开启或关闭规则集中指定规则的记录日志功能。

命令

ruleset *rule_set_name* **vulnerabilities** *vulnerabilities_id* **log** {**on** | **off**}

语法

rule_set_name	规则集名称，格式为 WORD<1-64>。
vulnerabilities_id	漏洞 ID，格式为 INTEGER<0-999999999>。
on	**off**	• on— 表示开启记录日志 • off— 表示关闭记录日志

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
ruleset vulnerabilities enable, disable	启用或禁用规则集中指定的规则。

show profile attack signature

使用 **show profile attack signature** 命令显示指定 profile 的规则集信息。

命令

show profile *profile_name* **attack signature**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通模式下使用。

范例

范例 . 显示 profile test 的规则集信息。

```
NetEye@root>show profile test attack signature
```

【返回结果】

```
Attack Signatures Detection:off
Rule Sets: pre-defined rule sets is enable
------------------------------------------------------------------------
-------------
Name                          Type           Entries        Enable
Comment
Mail                          Pre-Defined     72             no
Mail vulnerability sets
Ftp                           Pre-Defined     91             no
Ftp vulnerability sets
Web                           Pre-Defined     714            no
Web vulnerability sets
Database                      Pre-Defined     31             no
Database vulnerability sets
```

```
WindowsNetwork                Pre-Defined    34            no
Windows Network vulnerability sets
ruleset1             Customed    1232       no
```

show ruleset

使用 **show ruleset** 命令显示规则集信息。

命令

show ruleset [*rule_set_name*]

语法

rule_set_name	规则集名称，格式为 WORD<1-64>。

说明

如果不指定 *rule_set_name* 参数，则显示所有的规则集信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通模式下使用。

范例

范例 . 显示所有的规则集信息。

```
NetEye@root>show ruleset
```

【返回结果】

```
Name                          Type            Entries         Comment
Mail                          Pre-Defined     72              Mail
vulnerability sets
Ftp                           Pre-Defined     91              Ftp
vulnerability sets
Web                           Pre-Defined     714             Web
vulnerability sets
Database                      Pre-Defined     31              Database
vulnerability sets
WindowsNetwork                Pre-Defined     34              Windows
Network vulnerability sets
ruleset1                      Customed        1232
```

unset ruleset

使用 **unset ruleset** 命令删除自定义规则集。

命令

unset ruleset [*rule_set_name*]

语法

rule_set_name	规则集名称，格式为 WORD<1-64>。

说明

如果不指定 *rule_set_name* 参数，则表示删除所有自定义规则集。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
ruleset	创建自定义攻击签名规则集。

通知消息

import notification http url_block

使用 **import notification http url_block** 命令设置当 NetEye 根据 URL 过滤规则阻断 URL 时，通过 Web 页面发送给客户端的响应信息。

命令

import notification {**tftp http url_block host** *ip_tftp* **filename** *file_name* | **sftp http url_block host** *ip_sftp* **user** *user_name* **password** *passwd* **filename** *file_name* | **zmodem http url_block**}

语法

tftp	简单文件传输协议，表示从 TFTP 服务器导入响应信息文件。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
file_name	文件名称，格式为 WORD<1-100>。
sftp	安全文件传输协议，表示从 SFTP 服务器导入响应信息文件。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-100>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-100>。
zmodem	异步文件传输协议，表示使用 Zmodem 协议导入响应信息文件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 从 TFTP 服务器 10.3.1.23 导入响应信息文件 test。

```
NetEye@root-system]import notification tftp http url_block host
10.3.1.23 filename test
```

相关命令

命令名称	描述信息
show notification message http url_block	显示当 NetEye 根据 URL 过滤规则阻断 URL 时，通过 Web 页面发送给客户端的响应信息。

import notification mail attach_strip

使用 **import notification mail attach_strip** 命令设置当邮件附件被剥离时的提示信息。

命令

import notification {**tftp mail attach_strip host** *ip_tftp* **filename** *file_name* | **sftp mail attach_strip host** *ip_sftp* **user** *user_name* **password** *passwd* **filename** *file_name* | **zmodem mail attach_strip**}

语法

tftp	简单文件传输协议，表示从 TFTP 服务器导入提示信息文件。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
file_name	文件名称，格式为 WORD<1-100>。
sftp	安全文件传输协议，表示从 SFTP 服务器导入提示信息文件。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-100>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-100>。
zmodem	异步文件传输协议，表示使用 Zmodem 协议导入提示信息文件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 从 SFTP 服务器 10.3.1.23 导入提示信息文件 file1，SFTP 服务器的用户名和密码均为 test。

```
NetEye@root-system]import notification sftp mail attach_strip host
10.3.1.23 user test password test filename file1
```

相关命令

命令名称	描述信息
show notification message mail attach_strip	显示当邮件附件被剥离时的提示信息。

import notification mail field_strip

使用 **import notification mail field_strip** 命令设置当邮件字段被剥离时的提示信息。

命令

import notification {**tftp mail field_strip host** *ip_tftp* **filename** *file_name* | **sftp mail field_strip host** *ip_sftp* **user** *user_name* **password** *passwd* **filename** *file_name* | **zmodem mail field_strip**}

语法

tftp	简单文件传输协议，表示从 TFTP 服务器导入提示信息文件。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
file_name	文件名称，格式为 WORD<1-100>。
sftp	安全文件传输协议，表示从 SFTP 服务器导入提示信息文件。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-100>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-100>。
zmodem	异步文件传输协议，表示使用 Zmodem 协议导入提示信息文件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 通过 Zmodem 协议导入当邮件字段被剥离时指定的提示信息文件。

```
NetEye@root-system]import notification zmodem mail field_strip
```

相关命令

命令名称	描述信息
show notification message mail field_strip	显示当邮件字段被剥离时的提示信息。

import notification mail virus_found

使用 **import notification mail virus_found** 命令设置当邮件附件被病毒感染时的提示信息。

命令

import notification {**tftp mail virus_found host** *ip_tftp* **filename** *file_name* | **sftp mail virus_found host** *ip_sftp* **user** *user_name* **password** *passwd* **filename** *file_name* | **zmodem mail virus_found**}

语法

tftp	简单文件传输协议，表示从 TFTP 服务器导入提示信息文件。
ip_tftp	TFTP 服务器的 IP 地址，格式为 x.x.x.x。
file_name	文件名称，格式为 WORD<1-100>。
sftp	安全文件传输协议，表示从 SFTP 服务器导入提示信息文件。
ip_sftp	SFTP 服务器的 IP 地址，格式为 x.x.x.x。
user_name	登录 SFTP 服务器的用户名，格式为 WORD<1-100>。
passwd	登录 SFTP 服务器的密码，格式为 WORD<1-100>。
zmodem	异步文件传输协议，表示使用 Zmodem 协议导入提示信息文件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
show notification message mail virus_found	显示当邮件附件被病毒感染时的提示信息。

show notification message http url_block

使用 **show notification message http url_block** 命令显示当 NetEye 根据 URL 过滤规则阻断 URL 时，通过 Web 页面发送给客户端的响应信息。

命令

show notification message http url_block

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示当 NetEye 根据 URL 过滤规则阻断 URL 时，通过 Web 页面发送给客户端的响应信息。

```
NetEye@root>show notification message http url_block
```

【返回结果】

```
The following messages will be sent to the client as a response Web page
Notification Messages :
The URL is blocked due to URL filtering rules.
```

相关命令

命令名称	描述信息
import notification http url_block	设置当 NetEye 根据 URL 过滤规则阻断 URL 时，通过 Web 页面发送给客户端的响应信息。

show notification message mail attach_strip

使用 **show notification message mail attach_strip** 命令显示当邮件附件被剥离时的提示信息。

命令

show notification message mail attach_strip

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示当邮件附件被剥离时的提示信息。

```
NetEye@root>show notification message mail attach_strip
```

【返回结果】

```
The following messages will be replaced in the attachment or body of the
Email
Notification Messages :
        << The attachment of this e-mail has been stripped. >>
```

相关命令

命令名称	描述信息
import notification mail attach_strip	设置当邮件附件被剥离时的提示信息。

show notification message mail field_strip

使用 **show notification message mail field_strip** 命令显示当邮件字段被剥离时的提示信息。

命令

show notification message mail field_strip

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示当邮件字段被剥离时的提示信息。

```
NetEye@root>show notification message mail field_strip
```

【返回结果】

```
The following messages will be replaced in the attachment or body of the
Email
Notification Messages :
        <<  One or more MIME parts of this e-mail have been stripped.  >>
```

相关命令

命令名称	描述信息
import notification mail field_strip	设置当邮件字段被剥离时的提示信息。

show notification message mail virus_found

使用 **show notification message mail virus_found** 命令显示当邮件附件被病毒感染时的提示信息。

命令

show notification message mail virus_found

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示当邮件附件被病毒感染时的提示信息。

```
NetEye@root>show notification message mail virus_found
```

【返回结果】

```
The following messages will be replaced in the attachment or body of the
Email
Notification Messages :
        << Virus is found in the attachment of this e-mail, and the
attachment has been stripped. >>
```

相关命令

命令名称	描述信息
import notification mail virus_found	设置当邮件附件被病毒感染时的提示信息。

防护配置

profile mode

使用 **profile mode** 命令创建并进入指定的 Profile 配置模式。

命令

profile mode *profile_name*

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 创建并进入指定的 Profile 配置模式 test。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]
```

相关命令

命令名称	描述信息
show profile	显示所有或指定的 profile 配置信息。
unset profile	删除 profile。

profile name

使用 **profile name** 命令添加指定 profile 的描述信息。

命令

profile name *profile_name string*

语法

profile_name	profile 名称，格式为 WORD<1-10>。
string	备注信息，格式为 LINE。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

show profile

使用 **show profile** 命令显示 profile 的配置信息。

命令

show profile [*profile_name* **used_by**]

语法

profile_name	profile 名称，格式为 WORD<1-10>。

说明

如果不指定 *profile_name* 参数，则显示所有 profile 的配置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的配置信息。

```
NetEye@root>show profile test used_by
```

【返回结果】

```
| Index  | Profile Name |  Used By Policy  |   Policy  Type   |
|    1   |       test   |          policy1 |  Security Policy |
```

相关命令

命令名称	描述信息
profile mode	创建并进入指定的 Profile 配置模式。
unset profile	删除 profile。

unset profile

使用 **unset profile** 命令删除 profile。

命令

unset profile [*profile_name*]

语法

profile_name	profile 名称，格式为 WORD<1-10>。

说明

如果不指定 *profile_name* 参数，则表示删除所有 profile。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

相关命令

命令名称	描述信息
profile mode	创建并进入指定的 Profile 配置模式。
show profile	显示所有或指定的 profile 配置信息。

Web 检测

http anti-virus enable, disable

使用 **http anti-virus enable, disable** 命令启用或禁用 HTTP 流量病毒扫描功能。

命令

http anti-virus {**enable** | **disable**}

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用 HTTP 流量病毒扫描功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http anti-virus enable
```

相关命令

命令名称	描述信息
show profile http anti-virus	显示指定 profile 的 HTTP 流量病毒扫描状态。

http directory action

使用 **http directory action** 命令设置目录列表检测的动作。

命令

http directory action {**block** | **allow**}

语法

block | **allow**	• block— 阻断，表示断开服务器与客户端之间的连接。 • allow— 放行，表示不对数据通讯做任何处理，连接正常。

说明

要设置目录列表检测的动作，必须先启用目录列表检测功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置目录列表检测的动作为放行。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http directory action allow
```

相关命令

命令名称	描述信息
show profile http directory	显示指定 profile 的目录列表检测的配置信息。

http directory level

使用 **`http directory level`** 命令设置目录列表检测的等级。

命令

http directory level {**high** | **medium** | **low**}

语法

high | **medium** | **low**	• high— 代表检测所有 HTTP 应答。当 HTTP 页面上有父目录的链接，且关键字为 “Parent Directory”，则丢弃该应答。 • medium— 代表检测所有 HTTP 应答。当被要求的目录出现在 HTML 页面的标题中或 HTTP 页面有父目录链接时，应答将被丢弃。 • low— 代表只检测应答中包含以 “/” 和 “\” 结尾的 URL。当被要求的目录出现在 HTTP 页面的标题中或 HTTP 页面有父目录链接时，应答将被丢弃。

说明

要设置目录列表检测的等级，必须先启用目录列表检测功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置目录列表检测的等级为 medium。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http directory level medium
```

相关命令

命令名称	描述信息
show profile http directory	显示指定 profile 的目录列表检测的配置信息。

http error-concealment response

使用 **http error-concealment response** 命令启用或禁用隐藏指定错误代码的应答信息。

命令

http error-concealment response {**enable** | **disable**} *string*

语法

string	表示错误代码。如果要输入多个错误代码，可以用 “,” 分隔。

说明

要启用或禁用隐藏指定错误代码的应答信息，必须先启用隐藏错误信息功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用隐藏错误代码 414 和 417 的应答信息。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http error-concealment response enable 414,417
```

相关命令

命令名称	描述信息
show profile http error-concealment	显示指定 profile 的隐藏错误代码的配置信息。

http header-filtering

使用 **http header-filtering** 命令配置首部过滤。

命令

http header-filtering *app_name header_name value_name* {**enable** | **disable**}

语法

app_name	应用程序名称，格式为 WORD<1-64>。不能输入空白字符。
header_name	首部名称，格式为 WORD<1-32>。
value_name	首部值，格式为 WORD<1-32>。
enable | **disable**	当 NetEye 检测到匹配的应用程序名称、首部名称和首部值时的处理动作。 • enable— 阻断，表示断开服务器与客户端之间的连接。 • disable— 放行，表示不对数据通讯做任何处理，连接正常。

说明

1. 如果首部过滤列表中不存在与输入的参数匹配的条目，则表示添加；如果存在匹配的条目，则表示修改相应条目的处理动作。
2. 要配置首部过滤，必须先启用首部过滤功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 1. 为 profile test 添加首部过滤内容，其应用程序为 Skype，首部为 User-Agent，首部值为 Skype，并阻断该内容。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http header-filtering Skype User-Agent Skype enable
```

范例 2. 为 profile test 修改应用程序为 Skype，首部为 User-Agent，首部值为 Skype 的首部过滤内容的处理动作为放行。

```
NetEye@root-system]profile mode test
```

```
NetEye@root-system-pro-test]http header-filtering Skype User-Agent
Skype disable
```

相关命令

命令名称	描述信息
show profile http header-filtering, word-filtering	显示指定 profile 的页面过滤的配置信息。
unset http header-filtering	删除指定首部过滤内容。

http header-filtering, word-filtering enable, disable

使用 **http header-filtering, word-filtering enable, disable** 命令启用或禁用页面过滤的相关功能。

命令

http {**header-filtering** | **word-filtering**} {**enable** | **disable**}

语法

header-filtering | word-filtering	• header-filtering— 表示首部过滤 • word-filtering— 表示关键字过滤

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用关键字过滤功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http word-filtering enable
```

相关命令

命令名称	描述信息
show profile http header-filtering, word-filtering	显示指定 profile 的页面过滤的配置信息。

http header-filtering, word-filtering log

使用 **http header-filtering, word-filtering log** 命令开启或关闭页面过滤功能选项的产生日志功能。

命令

http {**header-filtering** | **word-filtering**} **log** {**on** | **off**}

语法

header-filtering | word-filtering	• header-filtering— 表示首部过滤 • word-filtering— 表示关键字过滤

说明

要开启或关闭指定选项的产生日志功能，必须先启用相应选项功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启关键字过滤的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http word-filtering log on
```

相关命令

命令名称	描述信息
show profile http header-filtering, word-filtering	显示指定 profile 的页面过滤的配置信息。

http header-substitution

使用 **http header-substitution** 命令配置首部置换。

命令

http header-substitution *header_name value_name* {**Delete** | **Substitute** *substitute_value*} {**enable** | **disable**}

语法

header_name	首部名称，格式为 WORD<1-32>。
value_name	首部值，格式为 WORD<1-32>。
Delete | **Substitute**	首部置换动作。 • Delete— 删除首部信息 • Substitute— 用首部替换值替换首部值
substitute_value	首部替换值，格式为 WORD<1-32>。
enable | **disable**	• enable— 启用首部置换功能 • disable— 禁用首部置换功能

说明

1. 如果首部置换列表中不存在与输入的参数匹配的条目，则表示添加；如果存在匹配的条目，则表示修改相应条目的状态。
2. 要配置首部置换，必须先启用首部置换功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 1. 为 profile test 添加首部置换内容，其首部为 Server，首部值为 Microsoft，动作为删除，并启用该内容。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http header-substitution Server Microsoft
Delete enable
```

范例 2. 为 profile test 修改首部为 Server，首部值为 Microsoft，动作为删除的首部置换内容的状态为禁用。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http header-substitution Server Microsoft
Delete disable
```

相关命令

命令名称	描述信息
show profile http header-substitution	显示指定 profile 的首部置换的配置信息。
unset http header-substitution	删除指定首部置换内容。

http header-substitution, error-concealment, directory enable, disable

使用 **http header-substitution, error-concealment, directory enable, disable** 命令启用或禁用防止信息泄露的相关功能。

命令

http {**header-substitution** | **error-concealment** | **directory**} {**enable** | **disable**}

语法

header-substitution | error-concealment | directory	• header-substitution— 表示首部置换 • error-concealment— 表示隐藏错误信息 • directory— 表示目录列表检测

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用目录列表检测功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http directory enable
```

相关命令

命令名称	描述信息
show profile http directory	显示指定 profile 的目录列表检测的配置信息。
show profile http error-concealment	显示指定 profile 的隐藏错误代码的配置信息。
show profile http header-substitution	显示指定 profile 的首部置换的配置信息。

http header-substitution, error-concealment, directory log

使用 **http header-substitution, error-concealment, directory log** 命令开启或关闭防止信息泄露功能选项的产生日志功能。

命令

http {**header-substitution** | **error-concealment** | **directory**} **log** {**on** | **off**}

语法

header-substitution | error-concealment | directory	• header-substitution— 表示首部置换 • error-concealment— 表示隐藏错误信息 • directory— 表示目录列表检测

说明

要开启或关闭指定选项的产生日志功能，必须先启用相应选项功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启隐藏错误信息的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http error-concealment log on
```

相关命令

命令名称	描述信息
show profile http directory	显示指定 profile 的目录列表检测的配置信息。
show profile http error-concealment	显示指定 profile 的隐藏错误代码的配置信息。
show profile http header-substitution	显示指定 profile 的首部置换的配置信息。

http injection Command level

使用 **`http injection Command level`** 命令设置命令注入攻击防御的等级。

命令

http injection Command level {**high** | **medium** | **low**}

语法

high | **medium** | **low**	• high— 代表阻断在 URL 的 path 部分和 Form 字段中含 Distinct Shell 命令的连接。 • medium— 代表阻断在 URL 的 path 部分和 Form 字段中含有 Non-distinct Shell 命令的连接，或在整个 URL 和 Form 字段中含有 Distinct Shell 命令的连接。 • low— 代表阻断在整个 URL 和 Form 字段中含有 Distinct Shell 命令以及 Non-distinct Shell 命令的连接。

说明

要设置命令注入攻击防御的等级，必须先启用命令注入攻击防御功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置命令注入攻击防御的等级为 medium。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http injection Command level medium
```

相关命令

命令名称	描述信息
show profile http injection	显示指定 profile 的注入攻击防御的配置信息。

http injection Cross-Site level

使用 **http injection Cross-Site level** 命令设置跨站脚本攻击防御的等级。

命令

http injection Cross-Site level {**high** | **medium** | **low**}

语法

high | **medium** | **low**	• high— 代表阻断含有 HTML 标签或 HTML 标签的其他显示方式（如：&gt, &#60）的 HTTP 请求。 • medium— 代表阻断含有 HTML 标签 HTTP 请求。 • low— 代表阻断含有脚本命令的 HTTP 请求。

说明

要设置跨站脚本攻击防御的等级，必须先启用跨站脚本攻击防御功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置跨站脚本攻击防御的等级为 medium。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http injection Cross-Site level medium
```

相关命令

命令名称	描述信息
show profile http injection	显示指定 profile 的注入攻击防御的配置信息。

http injection Cross-Site, LDAP

使用 **http injection Cross-Site, LDAP** 命令配置跨站脚本攻击防御或 LDAP 注入攻击防御的内容。

命令

http injection {**Cross-Site** | **LDAP**} **command** *defense_command* {**enable** | **disable**}

语法

Cross-Site | LDAP	• Cross-Site— 表示跨站脚本攻击防御 • LDAP— 表示 LDAP 注入攻击防御
defense_command	脚本命令或 LDAP 注入名称，格式为 WORD<1-32>。不允许输入“<”，“>”，“&”和空格。
enable | disable	当 NetEye 检测到匹配的脚本命令或 LDAP 注入名称时的处理动作。 • enable— 阻断，表示断开服务器与客户端之间的连接。 • disable— 放行，表示不对数据通讯做任何处理，连接正常。

说明

1. 如果脚本命令列表或 LDAP 注入名称列表中不存在与输入的参数匹配的条目，则表示添加；如果存在匹配的条目，则表示修改相应条目的处理动作。
2. 要设置攻击防御的内容，必须先启用相应的攻击防御功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 1. 为 profile test 添加脚本命令为 .cookie 的跨站脚本攻击内容，并阻断该脚本命令。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http injection Cross-Site command .cookie enable
```

范例 2. 为 profile test 修改脚本命令为 .cookie 的跨站脚本攻击内容的处理动作为放行。

```
NetEye@root-system]profile mode test
```

```
NetEye@root-system-pro-test]http injection Cross-Site command .cookie
disable
```

相关命令

命令名称	描述信息
show profile http injection	显示指定 profile 的注入攻击防御的配置信息。
unset http injection Cross-Site, LDAP	删除跨站脚本攻击防御或 LDAP 注入攻击防御的内容 .
unset http injection defense	删除全部注入攻击防御内容。

http injection enable, disable

使用 **`http injection enable, disable`** 命令启用或禁用注入攻击防御功能。**命令**

http injection {**Cross-Site** | **LDAP** | **SQL** | **Command**} {**enable** | **disable**}

语法

Cross-Site | LDAP | SQL | Command	• Cross-Site— 表示跨站脚本攻击防御 • LDAP— 表示 LDAP 注入攻击防御 • SQL— 表示 SQL 注入攻击防御 • Command— 表示命令注入攻击防御

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用 SQL 注入攻击防御。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http injection SQL enable
```

相关命令

命令名称	描述信息
show profile http injection	显示指定 profile 的注入攻击防御的配置信息。

http injection LDAP level

使用 **http injection LDAP level** 命令设置 LDAP 注入攻击防御的等级。

命令

http injection LDAP level {**high** | **medium** | **low**}

语法

high | **medium** | **low**	• high— 代表阻断在 URL 的 path 部分和 Form 字段中含 Filter Injection 定义的关键字的连接。 • medium— 代表阻断在 URL 的 path 部分和 Form 字段中含有段中含 Filter Injection 定义的关键字和 DN Injection 定义的关键字的连接。 • low— 代表阻断在整个 URL 和 Form 字段中含有 Filter Injection 定义的关键字和 DN Injection 定义的关键字的连接。

说明

要设置 LDAP 注入攻击防御的等级，必须先启用 LDAP 注入攻击防御功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置 LDAP 注入攻击防御的等级为 medium。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http injection LDAP level medium
```

相关命令

命令名称	描述信息
show profile http injection	显示指定 profile 的注入攻击防御的配置信息。

http injection log

使用 **http injection log** 命令开启或关闭注入攻击防御功能选项的产生日志功能。

命令

http injection {Cross-Site | LDAP | SQL | Command} log {on | off}

语法

Cross-Site | LDAP | SQL | Command	• Cross-Site— 表示跨站脚本攻击防御 • LDAP— 表示 LDAP 注入攻击防御 • SQL— 表示 SQL 注入攻击防御 • Command— 表示命令注入攻击防御

说明

要开启或关闭指定选项的产生日志功能，必须先启用相应选项功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启 SQL 注入攻击防御的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http injection SQL log on
```

相关命令

命令名称	描述信息
show profile http injection	显示指定 profile 的注入攻击防御的配置信息。

http injection SQL level

使用 **http injection SQL level** 命令设置 SQL 注入攻击防御的等级。

命令

http injection SQL level {**high** | **medium** | **low**}

语法

high | **medium** | **low**	• high— 代表阻断在 URL 的 path 部分和 Form 字段中含 Distinct SQL 命令的连接。 • medium— 代表阻断在 URL 的 path 部分和 Form 字段中含有 Non-distinct SQL 命令的连接，或在整个 URL 和 Form 字段中含有 Distinct SQL 命令的连接。 • low— 代表阻断在整个 URL 和 Form 字段中含有 Distinct SQL 命令以及 Non-distinct SQL 命令的连接。

说明

要设置 SQL 注入攻击防御的等级，必须先启用 SQL 注入攻击防御功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置 SQL 注入攻击防御的等级为 medium。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http injection SQL level medium
```

相关命令

命令名称	描述信息
show profile http injection	显示指定 profile 的注入攻击防御的配置信息。

http injection SQL, Command

使用 **http injection SQL, Command** 命令配置 SQL 注入或命令注入攻击防御的内容。

命令

http injection {**SQL** | **Command**} **command** {**Distinct** | **Non-Distinct**} *defense_command* {**enable** | **disable**}

语法

**SQL	Command**	• SQL— 表示 SQL 注入攻击防御 • Command— 表示命令注入攻击防御
Distinct	**Non-Distinct**	• Distinct— 表示 Distinct SQL 或 Shell 命令 • Non-Distonct— 表示 Non-Distinct SQL 或 Shell 命令
defense_command	注入攻击防御命令，格式为 WORD<1-120>。不允许输入 “<”，“>”，“&”和空格。
**enable	disable**	当 NetEye 检测到匹配的注入攻击防御命令时的处理动作。 • enable— 阻断，表示断开服务器与客户端之间的连接。 • disable— 放行，表示不对数据通讯做任何处理，连接正常。

说明

1. 如果 SQL 注入列表或命令注入名称列表中不存在与输入的参数匹配的条目，则表示添加；如果存在匹配的条目，则表示修改相应条目的处理动作。
2. 要设置攻击防御的内容，必须先启用相应的攻击防御功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 1. 为 profile test 添加 Distinct SQL 命令为 bigint 的 SQL 注入攻击防御内容，并阻断该命令。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http injection SQL command Distinct bigint enable
```

范例 2. 为 profile test 修改 Distinct SQL 命令为 bigint 的 SQL 注入攻击防御内容的处理动作为放行。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http injection SQL command Distinst bigint disable
```

相关命令

命令名称	描述信息
show profile http injection	显示指定 profile 的注入攻击防御的配置信息。
unset http injection defense	删除全部注入攻击防御内容。
unset http injection SQL, Command	删除 SQL 注入或命令注入攻击防御的内容。

http protocol-anomaly action

使用 **http protocol-anomaly action** 命令设置 HTTP 协议异常检测相关功能的动作。

命令

http protocol-anomaly {**method** | **url** | **version** | **reason-phrase** | **status-code** | **header**| **non-standard traffic**} **action** {**block** | **allow**}

语法

method |url | version | reason-phrase | status-code | header | non-standard traffic	• method— 表示请求方法 • url— 表示请求 URL • version— 表示 HTTP 版本 • reason-phrase— 表示状态短语 • status-code— 表示状态码 • header— 表示首部 • non-standard traffic— 表示检测非标准端口 （非 80 端口）上的 HTTP 流量
block | allow	• block— 阻断，表示断开服务器与客户端之间的连接。 • allow— 放行，表示不对数据通讯做任何处理，连接正常。

说明

1. 除了 **non-standard traffic** 是检测非标准端口上的 HTTP 流量外，其他选项都是检测格式和长度异常。
2. 要设置非标准端口上的 HTTP 流量检测的动作，必须先启用非标准端口上的 HTTP 流量检测功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置请求方法的格式和长度异常检测的动作为放行。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http protocol-anomaly method action allow
```

相关命令

命令名称	描述信息
show profile http protocol-anomaly	显示指定 profile 的 HTTP 协议异常检测的配置信息。

http protocol-anomaly log

使用 **http protocol-anomaly log** 命令开启或关闭 HTTP 协议异常检测的产生日志功能。

命令

http protocol-anomaly {**method** | **url** | **version** | **reason-phrase** | **status-code** | **header**| **non-standard traffic**} **log** {**on** | **off**}

语法

method |url | version | reason-phrase | status-code | header | non-standard traffic	• method— 表示请求方法 • url— 表示请求 URL • version— 表示 HTTP 版本 • reason-phrase— 表示状态短语 • status-code— 表示状态码 • header— 表示首部 • non-standard traffic— 表示检测非标准端口 （非 80 端口）上的 HTTP 流量

说明

1. 除了 **non-standard traffic** 是检测非标准端口上的 HTTP 流量外，其他选项都是检测格式和长度异常。
2. 要开启或关闭非标准端口上的 HTTP 流量检测的产生日志功能，必须先启用非标准端口上的 HTTP 流量检测功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启请求方法的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http protocol-anomaly method log on
```

相关命令

命令名称	描述信息
show profile http protocol-anomaly	显示指定 profile 的 HTTP 协议异常检测的配置信息。

http protocol-anomaly non-standard traffic

使用 **http protocol-anomaly non-standard traffic** 命令启用或禁用非标准端口上的 HTTP 流量检测的功能。

命令

http protocol-anomaly non-standard traffic {**enable** | **disable**}

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用非标准端口上的 HTTP 流量检测的功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http protocol-anomaly non-standard traffic enable
```

相关命令

命令名称	描述信息
show profile http protocol-anomaly	显示指定 profile 的 HTTP 协议异常检测的配置信息。

http protocol-restriction

使用 **http protocol-restriction** 命令启用或禁用特定首部长度或阻断请求方式检测功能。

命令

http protocol-restriction {**specific-header** | **block-request**} {**enable** | **disable**}

语法

specific-header | block-request	• specific-header— 表示检测特定首部长度 • block-request— 表示阻断请求方式

说明

要启用或禁用指定选项功能，必须先启用 HTTP 协议限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用 HTTP 协议限制的检测特定首部长度功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http protocol-restriction specific-header enable
```

相关命令

命令名称	描述信息
show profile http protocol-restriction	显示指定 profile 的 HTTP 协议限制的配置信息。

http protocol-restriction block-request methods

使用 **http protocol-restriction block-request methods** 命令设置 HTTP 协议允许或阻断的请求方式。

命令

http protocol-restriction block-request methods {**blocked** | **allowed**} *sting*

语法

blocked | **allowed**	• blocked— 阻断，表示断开服务器与客户端之间的连接。 • allowed— 允许，表示不对数据通讯做任何处理，连接正常。
string	请求方式名称。如果要输入多个请求名称，可以用以 “,” 分隔。

说明

要设置允许或阻断的请求方式，必须先启用 HTTP 协议限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置 HTTP 协议允许的请求方式为 GET 和 POST。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http protocol-restriction block-request
methods allowed GET,POST
```

相关命令

命令名称	描述信息
show profile http protocol-restriction	显示指定 profile 的 HTTP 协议限制的配置信息。

http protocol-restriction enable, disable

使用 **http protocol-restriction enable, disable** 命令启用或禁用 HTTP 协议限制功能。

命令

http protocol-restriction {**enable** | **disable**}

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用 HTTP 协议限制功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http protocol-restriction enable
```

相关命令

命令名称	描述信息
show profile http protocol-restriction	显示指定 profile 的 HTTP 协议限制的配置信息。

http protocol-restriction level

使用 **http protocol-restriction level** 命令设置 HTTP 协议限制的等级。

命令

http protocol-restriction level {**high** | **medium** | **low** | **custom**}

说明

1. 系统为管理员提供了高、中、低三个级别的保护配置，推荐级别为 “中”。管理员也可以自定义保护配置。
2. 要设置 HTTP 协议限制的等级，必须先启用 HTTP 协议限制功能。
3. 在进行 HTTP 协议限制时，首先需要选择协议限制等级，然后通过其他协议限制命令对相应等级的保护配置信息进行设置。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置 HTTP 协议限制级别为中。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http protocol-restriction level medium
```

相关命令

命令名称	描述信息
show profile http protocol-restriction	显示指定 profile 的 HTTP 协议限制的配置信息。

http protocol-restriction log

使用 **http protocol-restriction log** 命令开启或关闭特定首部长度或阻断请求方式检测功能的产生日志功能。

命令

http protocol-restriction {**specific-header** | **block-request**} **log** {**on** | **off**}

语法

specific-header | block-request	• specific-header— 表示检测特定首部长度 • block-request— 表示阻断请求方式

说明

要开启或关闭指定选项的产生日志功能，必须先启用 HTTP 协议限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启特定首部长度检测功能的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http protocol-restriction specific-header log on
```

相关命令

命令名称	描述信息
show profile http protocol-restriction	显示指定 profile 的 HTTP 协议限制的配置信息。

http protocol-restriction max

使用 **http protocol-restriction max** 命令设置长度限制和最大首部数限制。

命令

http protocol-restriction max {**header-number** | **header-length** | **request-body** | **url-length**} *number_value*

语法

header-number | header-length | request-body | url-length	• header-number— 表示首部数 • header-length— 表示首部长度 • request-body— 表示请求正文长度 • url-length— 表示 URL 长度
number_value	• 最大首部数，格式为 INTEGER<1-1024>。 • 最大首部长度或最大 URL 长度，单位为字节，格式为 INTEGER<1-2048>。 • 最大请求正文长度，单位为字节，格式为 INTEGER<1-65535>。

说明

要设置指定选项，必须先启用相应选项功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置最大首部数限制为 300。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http protocol-restriction max header-number 300
```

相关命令

命令名称	描述信息
show profile http protocol-restriction	显示指定 profile 的 HTTP 协议限制的配置信息。

http protocol-restriction max action

使用 **http protocol-restriction max action** 命令设置长度限制和最大首部数的动作。

命令

http protocol-restriction max {**header-number** | **header-length** | **request-body** | **url-length**} **action** {**block** | **allow**}

语法

header-number | header-length | request-body | url-length	• header-number— 表示首部数 • header-length— 表示首部长度 • request-body— 表示请求正文长度 • url-length— 表示 URL 长度
block | allow	• block— 阻断，表示断开服务器与客户端之间的连接。 • allow— 放行，表示不对数据通讯做任何处理，连接正常。

说明

要设置指定选项的动作，必须先启用相应选项功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置最大首部数的动作为放行。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http protocol-restriction max header-number action allow
```

相关命令

命令名称	描述信息
show profile http protocol-restriction	显示指定 profile 的 HTTP 协议限制的配置信息。

http protocol-restriction max enable, disable

使用 **http protocol-restriction max enable, disable** 命令启用或禁用长度限制和最大首部数限制功能。

命令

http protocol-restriction max {**header-number** | **header-length** | **request-body** | **url-length**} {**enable** | **disable**}

语法

header-number | header-length | request-body | url-length	• header-number— 表示首部数 • header-length— 表示首部长度 • request-body— 表示请求正文长度 • url-length— 表示 URL 长度

说明

要启用或禁用指定选项，必须先启用 HTTP 协议限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用最大首部数限制功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http protocol-restriction max header-number enable
```

相关命令

命令名称	描述信息
show profile http protocol-restriction	显示指定 profile 的 HTTP 协议限制的配置信息。

http protocol-restriction max log

使用 **http protocol-restriction max log** 命令开启或关闭长度限制和最大首部数限制的产生日志功能。

命令

http protocol-restriction max {**header-number** | **header-length** | **request-body** | **url-length**} **log** {**on** | **off**}

语法

header-number | header-length | request-body | url-length	• header-number— 表示首部数 • header-length— 表示首部长度 • request-body— 表示请求正文长度 • url-length— 表示 URL 长度

说明

要开启或关闭指定选项的产生日志功能，必须先启用相应选项功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启最大首部数限制的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http protocol-restriction max header-number log on
```

相关命令

命令名称	描述信息
show profile http protocol-restriction	显示指定 profile 的 HTTP 协议限制的配置信息。

http protocol-restriction non-ascii

使用 **http protocol-restriction non-ascii** 命令启用或禁用非 ASCII 码字符限制功能。

命令

http protocol-restriction non-ascii {**header** | **form**} {**enable** | **disable**}

语法

header| form	• header— 表示非 ASCII 码首部 • form— 表示 Form 字段的非 ASCII 码字符
enable | disable	当 NetEye 检测到匹配的非 ASCII 码字符时的处理动作。 • enable— 阻断，表示断开服务器与客户端之间的连接。 • disable— 放行，表示不对数据通讯做任何处理，连接正常。

说明

1. 如果启用阻断Form字段的非ASCII码字符限制，会导致无法上传二进制文件，可能影响部分功能正常应用。
2. 要启用或禁用非 ASCII 码字符限制功能，必须先启用 HTTP 协议限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用阻断非 ASCII 码首部功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http protocol-restriction non-ascii header enable
```

相关命令

命令名称	描述信息
show profile http protocol-restriction	显示指定 profile 的 HTTP 协议限制的配置信息。

http protocol-restriction non-ascii log

使用 **http protocol-restriction non-ascii log** 命令开启或关闭非 ASCII 码字符限制的产生日志功能。

命令

http protocol-restriction non-ascii {**header** | **form**} **log** {**on** | **off**}

语法

header | form	• header— 表示非 ASCII 码首部 • form— 表示 Form 字段的非 ASCII 码字符

说明

要开启或关闭产生日志功能，必须先启用非 ASCII 码字符限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启阻断非 ASCII 码首部功能的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http protocol-restriction non-ascii header log on
```

相关命令

命令名称	描述信息
show profile http protocol-restriction	显示指定 profile 的 HTTP 协议限制的配置信息。

http protocol-restriction specific-header

使用 **http protocol-restriction specific-header** 命令配置特定首部长度限制功能。

命令

http protocol-restriction specific-header *header_name max_length* {**enable** | **disable**}

语法

header_name	首部名称，格式为 WORD<1-32>。
max_length	最大长度，格式为 INTEGER<1-2048>。
enable | disable	• enable— 启用特定首部长度限制功能 • disable— 禁用特定首部长度限制功能

说明

1. 如果特定首部长度列表中不存在与输入的参数匹配的条目，则表示添加；如果存在匹配的条目，则表示修改相应条目的状态。
2. 要配置特定首部长度限制功能，必须先启用特定首部长度检测功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 1. 为 profile test 添加特定首部长度内容，其首部名称为 Host，最大长度为 2100，并启用该内容。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http protocol-restriction specific-header Host 2100 enable
```

范例 2. 为 profile test 修改首部名称为 Host，最大长度为 2100 的特定首部长度内容的状态为禁用。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http protocol-restriction specific-header Host 2100 disable
```

相关命令

命令名称	描述信息
show profile http protocol-restriction	显示指定 profile 的 HTTP 协议限制的配置信息。
unset http protocol-restriction specific-header	删除 HTTP 协议限制的特定首部长度内容。

http url-filter

使用 **http url-filter** 命令为指定的 profile 设置特定 URL 分类的处理动作。

命令

http url-filter url-category *category_id* {**allow** | **block**} {**enable** | **disable**}

语法

category_id	分类 ID 号，格式为 NUMBER<1- 256>。

说明

只有在启用指定 profile 的 URL 分类后，才能设置特定 URL 分类的处理动作。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 将 profile test 的 URL 分类 1-10 的处理动作设置为允许。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http url-filter category enable
NetEye@root-system-pro-test]http url-filter url-category 1-10 allow
enable
```

相关命令

命令名称	描述信息
http url-filter category	启用或禁用 URL 分类。
show profile http url-filter	显示全部 HTTP 协议 URL 分类信息。

http url-filter blacklist, whitelist

使用 **http url-filter blacklist, whitelist** 命令配置 URL 黑 / 白名单名称。

命令

http url-filter {**blacklist** | **whitelist**} *bwls_name*

语法

bwls_name	黑 / 白名单名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 配置 URL 黑名单为 blacklist1。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http url-filter blacklist blacklist1
```

相关命令

命令名称	描述信息
show profile http url-filter	显示全部 HTTP 协议 URL 的分类信息。

http url-filter category

使用 **http url-filter category** 命令启用或禁用指定 profile 的 URL 分类。

命令

http url-filter category {**enable** | **disable**}

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 启用 profile test 的 URL 分类。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http url-filter category enable
```

相关命令

命令名称	描述信息
http url-filter unknown-category	配置未知 URL 分类的处理动作。
http url-filter	为指定的 profile 设置特定 URL 分类的处理动作。
show profile http url-filter	显示全部 HTTP 协议 URL 的分类信息。

http url-filter unknown-category

使用 **http url-filter unknown-category** 命令为指定的 profile 配置未知 URL 分类的处理动作。

命令

http url-filter unknown-category {**allow** | **block**}

说明

只有在启用指定 profile 的 URL 分类后，才能为指定的 profile 配置未知 URL 分类的处理动作。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 将 profile test 的未知 URL 分类的处理动作设置为允许。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http url-filter unknown-category allow
```

相关命令

命令名称	描述信息
http url-filter category	启用或禁用 URL 分类。
show profile http url-filter	显示全部 HTTP 协议 URL 的分类信息。

http word-filtering

使用 **http word-filtering** 命令配置关键字过滤内容。

命令

http word-filtering *keyword score_value* {**enable** | **disable**}

语法

keyword	关键字，格式为 WORD<1-32>。
score_value	分值，格式为 INTEGER<1-100>。
enable | disable	• enable— 对关键字进行匹配 • disable— 对关键字不进行匹配

说明

1. 如果关键字列表中不存在与输入的参数匹配的条目，则表示添加；如果存在匹配的条目，则表示修改相应条目的状态。
2. 要配置关键字过滤内容，必须先启用关键字过滤功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 1. 为 profile test 添加关键字过滤内容，其关键字为 SecureN，分值为 10，并 enable 该内容。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http word-filtering SecureN 10 enable
```

范例 2. 为 profile test 修改关键字为 SecureN，分值为 10 的关键字过滤内容的状态为 disable。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http word-filtering SecureN 10 disable
```

相关命令

命令名称	描述信息
show profile http header-filtering, word-filtering	显示指定 profile 的页面过滤的配置信息。
unset http word-filtering	删除指定关键字过滤内容。

http word-filtering action

使用 **http word-filtering action** 命令设置关键字过滤的动作。

命令

http word-filtering action {**block** | **pass**}

语法

block | **pass**	当 Web 页面上的关键字总分值超过分数阈值时采取的动作。 • block— 阻断，表示断开服务器与客户端之间的连接。 • pass— 放行，表示不对数据通讯做任何处理，连接正常。

说明

要设置关键字过滤的动作，必须先启用关键字过滤功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置关键字过滤的动作为放行。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http word-filtering action pass
```

相关命令

命令名称	描述信息
show profile http header-filtering, word-filtering	显示指定 profile 的页面过滤的配置信息。

http word-filtering threshold

使用 **http word-filtering threshold** 命令设置关键字过滤的分数阈值。

命令

http word-filtering threshold *score_threshold_value*

语法

score_threshold_value	分数阈值，格式为 INTEGER<100-1000>。缺省值为 1000。

说明

要设置关键字过滤的分数阈值，必须先启用关键字过滤功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置关键字过滤的分数阈值为 400。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]http word-filtering threshold 400
```

相关命令

命令名称	描述信息
show profile http header-filtering, word-filtering	显示指定 profile 的页面过滤的配置信息。

show profile http anti-virus

使用 **show profile http anti-virus** 命令显示指定 profile 的 HTTP 流量病毒扫描状态。

命令

show profile *profile_name* **http anti-virus**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的 HTTP 流量病毒扫描状态。

```
NetEye@root>show profile test http anti-virus
```

【返回结果】

```
Scan Virus on HTTP traffic : disable
```

相关命令

命令名称	描述信息
http anti-virus enable, disable	启用或禁用 HTTP 流量病毒扫描功能。

show profile http directory

使用 **show profile http directory** 命令显示指定 profile 的目录列表检测的配置信息。

命令

show profile *profile_name* **http directory**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的目录列表检测的配置信息。

```
NetEye@root>show profile test http directory
```

【返回结果】

```
Directory Listing Detection     Level       Action        Log
disable                         Low         Block         off
```

相关命令

命令名称	描述信息
http directory action	设置目录列表检测的动作。
http directory level	设置目录列表检测的等级。
http header-substitution, error-concealment, directory enable, disable	启用或禁用防止信息泄露的相关功能。
http header-substitution, error-concealment, directory log	开启或关闭防止信息泄露功能选项的产生日志功能。

show profile http error-concealment

使用 **show profile http error-concealment** 命令显示指定 profile 的隐藏错误代码的配置信息。

命令

show profile *profile_name* **http error-concealment**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的隐藏错误代码的配置信息。

```
NetEye@root>show profile test http error-concealment
```

【返回结果】

```
Error Concealment : enable
Log : on
------------------------------------------------------------------------------
Conceal Response Errors:

Concealed   Error Code   Description
disable     400          Bad Request
disable     401          Unauthorized
disable     402          Payment Required
disable     403          Forbidden
disable     404          Not Found
disable     405          Method Not Allowed
disable     406          Not Acceptable
disable     407          Proxy Authentication Required
disable     408          Request Timeout
```

```
disable     409          Conflict
disable     410          Gone
disable     411          Length Required
disable     412          Precondition Failed
enable      413          Request Entity Too Large
enable      414          Request-URI Too Long
enable      415          Unsupported Media Type
enable      416          Requested Range Not Satisfiable
enable      417          Expectation Failed
disable     422          Unprocessable Entity
disable     423          Locked
disable     424          Method Failure
disable     425          Insufficient Space on Resource
enable      500          Internal Server Error
enable      501          Not Implemented
enable      502          Bad Gateway
enable      503          Service Unavailable
disable     504          Gateway Timeout
disable     505          HTTP Version Not Supported
disable     506          Loop Detected,Variant Also Varies,Partiall Update Not
Implemented,Redirection Failed
disable     507          Insufficient Storage
disable     510          Not Extended
```

相关命令

命令名称	描述信息
http error-concealment response	启用或禁用隐藏指定错误代码的应答信息。
http header-substitution, error-concealment, directory enable, disable	启用或禁用防止信息泄露的相关功能。
http header-substitution, error-concealment, directory log	开启或关闭防止信息泄露功能选项的产生日志功能。

show profile http header-filtering, word-filtering

使用 **show profile http header-filtering, word-filtering** 命令显示指定 profile 的页面过滤的配置信息。

命令

show profile *profile_name* **http** {**header-filtering** | **word-filtering**}

语法

profile_name	profile 名称，格式为 WORD<1-10>。
header-filtering | word-filtering	• header-filtering— 表示显示首部过滤的配置信息 • word-filtering— 表示显示关键字过滤配置信息

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的关键字过滤的配置信息。

```
NetEye@root>show profile test http word-filtering
```

【返回结果】

```
Word Substitution : enable
Score Threshold : 1000
When total score of words in a web page exceeds Score Threshold : block the
page
Log : on
------------------------------------------------------------------------
blocked  Word                                Score
enable   SecureN                             50
enable   search\.info                        10
```

相关命令

命令名称	描述信息
http header-filtering	配置首部过滤。
http header-filtering, word-filtering enable, disable	启用或禁用页面过滤的相关功能。
http header-filtering, word-filtering log	开启或关闭页面过滤功能选项的产生日志功能。
http word-filtering	配置关键字过滤内容。
http word-filtering action	设置关键字过滤的动作。
http word-filtering threshold	设置关键字过滤的分数阈值。
unset http header-filtering	删除指定首部过滤内容。
unset http word-filtering	删除关键字过滤内容。

show profile http header-substitution

使用 **show profile http header-substitution** 命令显示指定 profile 的首部置换的配置信息。

命令

show profile *profile_name* **http header-substitution**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 首部置换的配置信息。

```
NetEye@root>show profile test http header-substitution
```

【返回结果】

```
Header Substitution : disable
Log : off
------------------------------------------------------------------------------
---------------
state     header                              value
action
enable    Server                              .*IIS.*
Substitute with 'IIS'
enable    Server                              .*Apache.*
Substitute with 'Apache'
```

相关命令

命令名称	描述信息
http header-substitution	配置首部过滤。
http header-substitution, error-concealment, directory enable, disable	启用或禁用防止信息泄露的相关功能。
http header-substitution, error-concealment, directory log	开启或关闭防止信息泄露功能选项的产生日志功能。
unset http header-substitution	删除指定首部置换内容。

show profile http injection

使用 **show profile http injection** 命令显示指定 profile 的注入攻击防御的配置信息。

命令

show profile *profile_name* **http injection** {**defense** | **Cross-Site** | **LDAP** | **SQL** | **Command**}

语法

profile_name	profile 名称，格式为 WORD<1-10>。
defense | Cross-Site | LDAP | SQL | Command	• defense— 表示显示注入攻击防御总体信息 • Cross-Site— 表示显示跨站脚本攻击防御的配置信息 • LDAP— 表示显示 LDAP 注入攻击防御的配置信息 • SQL— 表示显示 SQL 注入攻击防御的配置信息 • Command— 表示显示命令注入攻击防御的配置信息

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的 LDAP 注入攻击防御的配置信息。

```
NetEye@root>show profile test http injection LDAP
```

【返回结果】

```
Name:   LDAP Injection
Enable: Disable
Level:  Medium
Log:    On
------------------------------------------------------------------------
Enable    Command              | Enable    Command              | Enable
Command
Disable   c                 | Disable   cn                | Disable   dc
Disable   l                 | Disable   o                 | Disable   ou
Disable   st                     | Disable   street              | Disable   uid
```

相关命令

命令名称	描述信息
http injection Command level	设置命令注入攻击防御的等级。
http injection Cross-Site level	设置跨站脚本攻击防御的等级。
http injection Cross-Site, LDAP	配置跨站脚本攻击防御或 LDAP 注入攻击防御的内容。
http injection enable, disable	启用或禁用注入攻击防御功能。
http injection LDAP level	设置 LDAP 注入攻击防御的等级。
http injection log	开启或关闭注入攻击防御功能选项的产生日志功能。
http injection SQL level	设置 SQL 注入攻击防御的等级。
http injection SQL, Command	配置 SQL 注入或命令注入攻击防御的内容。
unset http injection Cross-Site, LDAP	删除跨站脚本攻击防御或 LDAP 注入攻击防御的内容。
unset http injection defense	删除全部注入攻击防御内容。
unset http injection SQL, Command	删除 SQL 注入或命令注入攻击防御的内容。

show profile http protocol-anomaly

使用 **show profile http protocol-anomaly** 命令显示指定 profile 的 HTTP 协议异常检测的配置信息。

命令

show profile *profile_name* **http protocol-anomaly**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的 HTTP 协议异常检测的配置信息。

```
NetEye@root>show profile test http protocol-anomaly
```

【返回结果】

```
state      name                                    Action    log
  --       Methods                                 Allow     on
  --       Request-URIs                            Allow     on
  --       HTTP-Version                            Allow     on
  --       Reason-Phrase                           Allow     on
  --       Status-Code                             Allow     on
  --       Headers                                 Allow     on
disable    Inspect HTTP traffic on non-standard ports  Allow     on
```

相关命令

命令名称	描述信息
http protocol-anomaly action	设置 HTTP 协议异常检测相关功能的动作。

命令名称	描述信息
http protocol-anomaly log	开启或 关闭 HTTP 协议异常检测的产生日志功能。
hhttp protocol-anomaly non-standard traffic	启用或禁用非标准端口上的 HTTP 流量检测的功能。

show profile http protocol-restriction

使用 **show profile http protocol-restriction** 命令显示指定 profile 的 HTTP 协议限制的配置信息。

命令

show profile *profile_name* **http protocol-restriction** [**block-request methods | level | specific-header**]

语法

profile_name	profile 名称，格式为 WORD<1-10>。
block-request methods | level | specific-header	• block-request methods— 表示显示 HTTP 协议限制允许和阻断的请求方式 • level— 表示显示 HTTP 协议限制的等级 • specific-header— 表示显示 HTTP 协议限制的特定首部长度过滤配置信息

说明

如果仅指定 **protocol-restriction** 关键字，则表示显示 HTTP 协议限制 （除了允许 / 阻断的请求方式和特定首部长度过滤）的配置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的 HTTP 协议限制等级。

```
NetEye@root>show profile test http protocol-restriction level
```

【返回结果】

```
Profilename is test current level: Medium
```

相关命令

命令名称	描述信息
http protocol-restriction	启用或禁用特定首部长度或阻断请求方式检测功能。
http protocol-restriction block-request methods	设置 HTTP 协议允许或阻断的请求方式。
http protocol-restriction enable, disable	启用或禁用 HTTP 协议限制功能。
http protocol-restriction level	设置 HTTP 协议限制的等级。
http protocol-restriction log	开启或关闭特定首部长度或阻断请求方式检测功能的产生日志功能。
http protocol-restriction max	设置长度限制和最大首部数限制。
http protocol-restriction max action	设置长度限制和最大首部数的动作。
http protocol-restriction max enable, disable	启用或禁用长度限制和最大首部数限制功能。
http protocol-restriction max log	开启或关闭长度限制和最大首部数限制的产生日志功能。
http protocol-restriction non-ascii	启用或禁用非 ASCII 字符限制功能。
http protocol-restriction non-ascii log	开启或关闭非 ASCII 字符限制的产生日志功能。
http protocol-restriction specific-header	配置特定首部长度限制功能。
unset http protocol-restriction specific-header	删除 HTTP 协议限制的特定首部长度内容。

show profile http url-filter

使用 **show profile http url-filter** 命令显示指定 profile 的全部 HTTP 协议 URL 的配置信息，包括 URL 黑 / 白名单、 URL 分类、 URL 未知分类的默认处理动作信息。

命令

show profile *profile_name* **http url-filter**

语法

profile_name	防护配置名称，格式为 WORD<1-10>。

说明

URL 分类含义如表 5 所示：

表 5 URL 分类含义

URL 分类 ID 号	名称	含义
1	广告	提供广告图片或其他广告内容文件 （如标题广告和弹出式广告）的网站。
2	烟酒	推销烟酒相关产品或服务的网站。
3	匿名技术	为用户登录其他网站提供匿名登录服务的网站或代理，无论是为了绕过 Web 过滤还是其他原因。
4	艺术	此类网站提供艺术相关内容或有关艺术的组织机构，如剧院、博物馆、展览馆、舞蹈公司、摄影机构，以及数码图像资源等。
5	商业	提供公司网址等相关商业信息的网站。此类网站为各种规模的公司完成其日常商业活动提供信息、服务或产品。
6	运输	提供机动车辆，如汽车、摩托车、船只、卡车、旅行车等相关信息的网站，包括制造商网站、经销商网站、审查网、报价信息网、在线交易网、爱好者俱乐部等。
7	聊天	通过聊天服务或聊天室提供基于 Web 的实时信息交换的网站。
8	论坛和新闻组	以新闻组、论坛、留言板方式共享信息的网站。

表 5 URL 分类含义 (续)

URL 分类 ID 号	名称	含义
9	被入侵网站	已经被入侵的网站，包括易受某种高风险攻击入侵的网站。此类网站通常是为了在用户不知情的情况下安装一些恶意程序。
10	电脑科技	此类网站提供电脑、软件、硬件、 IT、外围设备和电脑服务相关信息，如产品评价、讨论和 IT 新闻。
11	犯罪	此类网站为违法犯罪行为或反侦查提供建议，如教授谋杀、制造炸弹、开锁的方法，提供非法操纵电子设备、非法访问计算机系统或数据库、网络诈骗及非法发布软件等相关信息。
12	约会或交友	提供有关约会、交友等人际关系方面信息的网站，包括婚介、在线约会、配偶介绍等。
13	下载	包含可下载软件的网站，可以是共享软件、免费软件或收费软件，包括点对点下载网站。
14	教育	由各类教育机构或学校 （包括远程教育）主办的网站，包括一般性教育资源和参考资源，如词典、百科全书、在线课程、教学辅助工具和讨论指南。
15	娱乐	有关电视、电影、音乐、视频 （包括视频点播）的网站，例如节目指南、名人站点和娱乐新闻。
16	金融	有关银行、金融、支付或投资的网站，包括银行、经纪服务、网上股票交易、股票行情、资金管理、保险公司、信贷联盟、信用卡公司等。
17	赌博	此类网站提供在线赌博、彩票、赌场及博彩机构相关信息。
18	游戏	有关电脑游戏或其他游戏的网站，提供游戏制作者、如何获取作弊代码等相关信息。包括所有发布游戏相关信息的网站。
19	政府	由政府机构、部门或代办处创办和维护的网站，包括公安部门、消防部门、税务局、突发事件服务部门、民事防护部门、反恐组织、军队和医院。

表 5 URL 分类含义 (续)

URL 分类 ID 号	名称	含义
20	仇恨和偏执	此类网站宣扬政治至上，鼓动基于种族、宗教、性别、年龄、残疾、性取向或国籍而压迫人民或少数群体。
21	医疗保健	有关医疗保健和健美的网站，包括提供医学流程、处方药等相关信息。
22	非法药品	提供以下信息的网站：购买、制造、使用非法药物或娱乐毒品及辅助用具、滥用处方药和其他合成药物。
23	求职	包含职位列表、职业信息、空缺职位搜索辅助信息 （如简历制作、面试技巧等）、职业介绍所、猎头公司。
24	流媒体技术和下载	传输流内容的网站，包括网络电台、网络电视、 MP3，提供实时播放媒体或压缩媒体文件下载服务的网站；还包括影迷网以及由音乐人、乐队或唱片公司运行的官方网站。
25	新闻	包含新闻和即时事件的网站，如新闻报纸、新闻专线服务、个性化新闻服务、广播网和杂志。
26	非营利机构和非政府组织	致力于俱乐部、团体、联盟和非营利性组织的网站，许多此类团体是为了教育或慈善目的。
27	裸体照	包含全裸或半裸图片的网站，但并不一定完全跟性有关。包括广告或销售女士内衣或泳衣的网站。
28	个人网站	有关个人或由个人主办的网站，包括商业网站上的个人网站。
29	网络钓鱼或诈骗	用于迷惑或欺诈之目的 （如钓鱼）的网站，例如窃取金融信息或其他用户帐号信息。此类网站通常伪装成合法网站，以诱导用户输入自己的身份认证信息。
30	政治	宣扬政治党派、鼓吹政治主张，或提供有关政治党派、利益团体、选举、立法或游说的网站，也包括从法律角度提供信息或建议的网站。
31	色情	包含明显色情内容的网站，包括成人用品（如成人玩具、光盘和视频）、成人服务（如视频通讯、伴游服务和钢管舞俱乐部）、色情故事以及对性行为的文字描述。

表 5 URL 分类含义 (续)

URL 分类 ID 号	名称	含义
32	房地产	有关商用或住宅房产服务的网站，包括租赁、购买、出售、融资房屋或办公室等。
33	宗教	有关信仰、人类精神信仰和宗教信仰的网站，包括基督教、犹太教、清真寺以及其他敬拜场所的网站。
34	酒店餐饮	列举、评论、推销或宣传食品、就餐或外卖服务的网站，包括提供食谱、烹调指南、食品饮料和酒水推销的网站。
35	搜索引擎和门户网站	支持 Web、新闻组、图像、目录和其他在线内容搜索的网站，包括门户网站和目录网站 （如白页和黄页）。
36	购物	提供网上购物、商品目录、网上预定、商品拍卖、分类广告的网站，不包括购买其他分类的商品或服务，如健康和医药类。
37	社交	为各类主题 （如友谊、约会或各种专业话题）的网上社区提供社交平台的网站。
38	垃圾网站	通过垃圾邮件技术来进行宣传的网站。
39	体育	有关体育团队、球迷俱乐部、比分情况、体育新闻的网站，包括职业或娱乐方面的所有体育信息。
40	恶意软件	此类网站在用户电脑上安装恶意软件，其目的是使得第三方能监控用户系统或未经用户许可修改用户系统。
41	翻译软件	将网页或短语从一种语言翻译为另一种语言的网站。此类网站可被用于绕过某个过滤系统的过滤。
42	旅游	提供旅游相关信息或在线预定旅游服务（如机票、住宿、汽车租赁）的网站，包括地区或城市信息网站。
43	暴力	包含描述或宣传攻击人类、动物或组织机构的图像或文字的网站，带有一种阴森恐怖色彩的网站，如对血迹斑斑的恐怖画面或禽兽般残暴行为的恐怖描写。
44	武器	描写、出售或评论枪支武器的网站，包括用于运动目的的枪支设备。
45	Web 邮箱	使用户能够通过 Web 访问邮箱账号、收发电子邮件的网站。

表 5 URL 分类含义 (续)

URL 分类 ID 号	名称	含义
46	通用网站	未明确划分为任何类别的网站，如空白页。
47	休闲娱乐	有关娱乐活动和兴趣爱好的网站，包括动物园、公共娱乐中心、游泳池、游乐园和兴趣爱好 （如园艺、文学、美术工艺、家居装饰、家庭、家人等）。
48	僵尸网	使用 bots 或 zombies （僵尸病毒）的网站，包括指挥和控制网站。
49	邪教	关于非传统宗教行为的网站。此类被称为“邪教”的宗教行为被认为是错误的、异端的、极端的、强迫的，其成员通常由一位魅力型领袖来领导。
50	时尚美容	关于时尚、珠宝、魅力、美容、造型、化妆品以及相关产品或服务的网站，包括产品评论、对比、一般消费者信息。
51	电子贺卡	允许人们收发贺卡和明信片的网站。
52	黑客技术	怂恿非法访问专属计算机系统或给出相关信息的网站，其目的在于窃取信息、欺诈、制造病毒或用于窃取数字信息的其他非法活动。
53	非法软件	此类网站非法发布软件或受版权保护的资料，如电影或音乐、软件破解版、非法序列号、非法 License 密钥生成器。
54	镜像共享	处理数码照片与图像、在线相册和数码照片转换的网站。
55	信息安全	提供有关数据保护的合法信息的网站，包括最新发现的网络漏洞以及如何阻断相应的漏洞攻击。
56	即时通信网站	使用户可以登录使用即时通信服务的网站，如 ICQ、 AOL、 IRC、 MSN、 Jabber、 Yahoo! Messenger 等。
57	网络错误	不能成功解析为 IP 地址的网站。
58	停放域名	未激活的网站，通常留待以后使用。此类网站通常不包含自身内容，只是显示“正在筹建”、“购买此域名”等消息或广告。

表 5 URL 分类含义 (续)

URL 分类 ID 号	名称	含义
59	点对点	使用户能够不依赖于中间服务器而直接交换文件的网站。
60	私有 IP 地址	使用 RFC 1918 中定义的私有 IP 地址的网站。此类网站的 IP 地址在自身企业网内部是唯一的，但与其他企业网地址可能存在冲突，所以这些网站一般不需要访问其他企业网的主机 （或只是有限的访问）
61	考试作弊	鼓励不道德行为的网站，如提供考试答案、作文、研究论文、学期论文等作弊或剽窃行为。
62	性教育	有关性教育的网站，包含以下主题：对性伴侣的尊重、堕胎、同性恋的生活方式、避孕用品、性传播疾病、怀孕。
63	低俗网站	提供令人不快或低俗内容的网站，如低俗笑话或亵渎的语言。
64	虐童图片	此类网站描写或讨论受到性虐待或其他虐待行为的儿童。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的全部 HTTP 协议 URL 的分类信息。

```
NetEye@root>show profile test http url-filter
```

【返回结果】

```
% URL Whitelist: None
URL Blacklist: None
URL Categorization: Enable
Default action for URLs of unknown categories: Block
```

```
------------------------------------------------------------------
----------------

-------------------------------

ID Category              Action Enable  | ID Category
Action Enable

1 Advertisements & Pop-Ups   Block Disable | 33 Religion
Block  Disable

2  Alcohol & Tobacco          Block  Disable |  34  Restaurants
& Dining    Block  Disable

3   Anonymizers                  Block  Disable |  35  Search
Engines &Portals Block  Disable

4  Arts                  Block  Disable |  36  Shopping
Block  Disable

5   Business                     Block  Disable |  37  Social
Networking       Block  Disable

6  Transportation          Block  Disable |  38  Spam Sites
Block  Disable

7  Chat                  Block  Disable |  39  Sports
Block  Disable

8  Forums & Newsgroups      Block  Disable |  40  Malware
Block  Disable

9  Compromised           Block  Disable |  41  Translators
Block  Disable

10 Computers & Technology    Block  Disable |  42  Travel
Block  Disable

11 Criminal Activity       Block  Disable |  43  Violence
Block  Disable

12 Dating & Personals       Block  Disable |  44  Weapons
Block  Disable

13  Download Sites               Block  Disable |  45  Web-based
Email         Block  Disable

14 Education              Block  Disable |  46  General
Block  Disable

15  Entertainment               Block  Disable |  47  Leisure &
Recreation    Block  Disable

16 Finance               Block  Disable |  48  Botnets
Block  Disable

17 Gambling              Block  Disable |  49  Cults
Block  Disable
```

```
18 Games                          Block Disable | 50 Fashion &
Beauty        Block Disable
19 Government                     Block Disable | 51 Greeting
cards          Block Disable
20 Hate & Intolerance       Block Disable | 52 Hacking
Block Disable
21 Health & Medicine              Block Disable | 53 Illegal
Software        Block Disable
22 Illegal Drug                   Block Disable | 54 Image
Sharing          Block Disable
23 Job Search                  Block Disable | 55 Information
Security    Block Disable
24 Streaming Media & Downloads  Block Disable | 56 Instant
Messaging       Block Disable
25 News                           Block Disable | 57 Network
Errors          Block Disable
26 Non-profits & NGOs             Block Disable | 58 Parked
Domains          Block Disable
27 Nudity                         Block Disable | 59 Peer-to-
Peer            Block Disable
28 Personal Sites              Block Disable | 60 Private IP
Addresses    Block Disable
29 Phishing & Fraud               Block Disable | 61 School
Cheating         Block Disable
30 Politics                       Block Disable | 62 Sex
Education           Block Disable
31 Pornography/Sexually ExplicitBlock Disable | 63 Tasteless
Block Disable
32 Real Estate                 Block Disable | 64 Child Abuse
Imags       Block Disable
```

相关命令

命令名称	描述信息
http url-filter	为指定的 profile 设置特定 URL 分类的处理动作。
http url-filter blacklist, whitelist	配置 URL 黑 / 白名单名称。
http url-filter category	启用或禁用指定 profile 的 URL 分类。
http url-filter unknown-category	配置未知 URL 分类的处理动作。

unset http header-filtering

使用 **unset http header-filtering** 命令删除指定首部过滤内容。

命令

unset http header-filtering *app_name header_name value_name*

语法

app_name	应用程序名称，格式为 WORD<1-64>。不能输入空白字符。
header_name	首部名称，格式为 WORD<1-32>。
value_name	首部值，格式为 WORD<1-32>。

说明

要删除首部过滤内容，必须先启用首部过滤功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 删除应用程序为 Skype，首部为 User-Agent，首部值为 Skype 的首部过滤内容。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]unset http header-filtering Skype User-Agent Skype
```

相关命令

命令名称	描述信息
http header-filtering	配置首部过滤。
show profile http header-filtering, word-filtering	显示指定 profile 的页面过滤的配置信息。

unset http header-substitution

使用 **unset http header-substitution** 命令删除指定首部置换内容。

命令

unset http header-substitution *header_name value_name*

语法

header_name	首部名称，格式为 WORD<1-32>。
value_name	首部值，格式为 WORD<1-32>。

说明

要删除首部置换内容，必须先启用首部置换功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 删除首部为 Server，首部值为 Microsoft 的首部置换内容。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]unset http header-substitution Server Microsoft
```

相关命令

命令名称	描述信息
http header-substitution	配置首部置换。
show profile http header-substitution	显示指定 profile 的首部置换的配置信息。

unset http injection Cross-Site, LDAP

使用 **unset http injection Cross-Site, LDAP** 命令删除跨站脚本攻击防御或 LDAP 注入攻击防御的内容。

命令

unset http injection {**Cross-Site** | **LDAP**} **command** [*defense_command*]

语法

Cross-Site | LDAP	• Cross-Site— 表示跨站脚本攻击防御 • LDAP— 表示 LDAP 注入攻击防御
defense_command	脚本命令或 LDAP 注入名称，格式为 WORD<1-32>。不允许输入“<”，“>”，“&”和空格。

说明

1. 如果不指定 *defense_command* 参数，则表示删除所有跨站脚本攻击防御或 LDAP 注入攻击防御的内容。
2. 要删除注入攻击防御内容，必须先启用相应的注入攻击防御功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 删除脚本命令为 .cookie 的跨站脚本攻击内容。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]unset http injection Cross-Site command
.cookie
```

相关命令

命令名称	描述信息
http injection Cross-Site, LDAP	配置跨站脚本攻击防御或 LDAP 注入攻击防御的内容。
show profile http injection	显示指定 profile 的注入防御攻击的配置信息。
unset http injection defense	删除全部注入攻击防御内容。

unset http injection defense

使用 **unset http injection defense** 命令删除全部注入攻击防御内容。

命令

unset http injection defense command

说明

1. 该命令主要用于在 HA 同步之前清空当前配置。
2. 要删除注入攻击防御内容，必须先启用相应的注入攻击防御功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 删除全部注入攻击防御内容。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]unset http injection defense command
```

相关命令

命令名称	描述信息
http injection Cross-Site, LDAP	配置跨站脚本攻击防御或 LDAP 注入攻击防御的内容。
http injection SQL, Command	配置 SQL 注入或命令注入攻击防御的内容。
show profile http injection	显示指定 profile 的注入防御攻击的配置信息。
unset http injection Cross-Site, LDAP	删除跨站脚本攻击防御或 LDAP 注入攻击防御的内容。
unset http injection SQL, Command	删除 SQL 注入或命令注入攻击防御的内容。

unset http injection SQL, Command

使用 **unset http injection SQL, Command** 命令删除 SQL 注入或命令注入攻击防御的内容。

命令

unset http injection {**SQL** | **Command**} **command** {**Distinct** | **Non-Distinct**} [*defense_command*]

语法

SQL | Command	• SQL— 表示 SQL 注入攻击防御 • Command— 表示命令注入攻击防御
Distinct | **Non-Distinct**	• Distinct— 表示 Distinct SQL 或 Shell 命令 • Non-Distonct— 表示 Non-Distinct SQL 或 Shell 命令
defense_command	脚本命令或 LDAP 注入名称，格式为 WORD<1-120>。不允许输入“<”，“>”，“&”和空格。

说明

1. 如果不指定 *defense_command* 参数，则表示删除所有 SQL 注入或命令注入攻击防御的内容。
2. 要删除注入攻击防御内容，必须先启用相应的注入攻击防御功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 删除 Distinct SQL 命令为 bigint 的 SQL 注入攻击防御内容。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]unset http injection SQL command Distinct
bigint
```

相关命令

命令名称	描述信息
http injection SQL, Command	配置 SQL 注入或命令注入攻击防御的内容。
show profile http injection	显示指定 profile 的注入攻击防御的配置信息。
unset http injection defense	删除全部注入攻击防御内容。

unset http protocol-restriction specific-header

使用 **unset http protocol-restriction specific-header** 命令删除特定首部长度内容。

命令

unset http protocol-restriction specific-header *header_name*

语法

header_name	首部名称，格式为 WORD<1-32>。

说明

要删除特定首部长度内容，必须先启用特定首部长度检测功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 删除首部名称为 Host 的特定首部长度内容。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]unset http protocol-restriction specific-header Host
```

相关命令

命令名称	描述信息
http protocol-restriction specific-header	配置特定首部长度限制功能。
show profile http protocol-restriction	显示指定 profile 的 HTTP 协议限制的配置信息。

unset http word-filtering

使用 **unset http word-filtering** 命令删除指定关键字过滤内容。

命令

unset http word-filtering *keyword*

语法

keyword	关键字，格式为 WORD<1-32>。

说明

要删除关键字过滤内容，必须先启用关键字过滤功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 删除关键字为 SecureN 的关键字过滤内容。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]unset http word-filtering SecureN
```

相关命令

命令名称	描述信息
http word-filtering	配置关键字过滤内容。
show profile http header-filtering, word-filtering	显示指定 profile 的页面过滤的配置信息。

邮件检测

imap protocol-restriction max

使用 **imap protocol-restriction max** 命令设置 IMAP 协议限制相关功能的最大值。

命令

imap protocol-restriction max {**command-length** | **command** | **noop-command** | **parameter** | **response** | **tag** | **unknown-command**} *number_value*

语法

command-length | **command** | **noop-command** | **parameter** | **response** | **tag** | **unknown-command**	• command-length— 表示最大命令长度 • command— 表示最多命令次数 • noop-command— 表示最多 NOOP 命令次数 • parameter— 表示最大参数长度 • response— 表示最大应答长度 • tag— 表示最大 Tag 长度 • unknowm-command— 表示最多未知命令次数
number_value	• 最大命令长度值，单位为字节，格式为 INTEGER<1-2048>。 • 最多命令次数值，格式为 INTEGER<1-256>。 • 最多 NOOP 命令次数值，格式为 INTEGER<1-128>。 • 最大参数长度值，单位为字节，格式为 INTEGER<1-1024>。 • 最大应答长度值，单位为字节，格式为 INTEGER<1-4096>。 • 最大 Tag 长度值，单位为字节，格式为 INTEGER<1-512>。 • 最多未知命令次数值，格式为 INTEGER<1-128>。

说明

要设置 IMAP 协议限制相关功能的最大值，必须先启用相应功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置 IMAP 协议限制的最多命令次数值为 128。

```
NetEye@root-system]profile mode test
```

```
NetEye@root-system-pro-test]imap protocol-restriction max command 128
```

相关命令

命令名称	描述信息
protocol-restriction enable, disable	启用或禁用邮件协议限制功能。
protocol-restriction max enable, disable	启用或禁用邮件协议限制的相关功能。
show profile protocol-restriction	显示指定 profile 的邮件协议限制的相关信息。

mail anti-spam enable, disable

使用 **mail anti-spam enable, disable** 命令启用或禁用反垃圾邮件扫描功能。

命令

mail anti-spam {**pop3** | **smtp**} {**enable** | **disable**}

语法

pop3 | smtp	• pop3— 邮局协议，用于接收邮件。 • smtp— 简单邮件传输协议，用于发送邮件。

说明

POP3 是基于内容的反垃圾邮件检测， SMTP 是基于 IP 信誉和内容的反垃圾邮件检测。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用 POP3 协议的反垃圾邮件扫描功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]mail anti-spam pop3 enable
```

相关命令

命令名称	描述信息
show profile mail anti-spam	显示指定 profile 的反垃圾邮件功能状态。

mail anti-virus enable, disable

使用 **mail anti-virus enable, disable** 命令启用或禁用邮件协议的防病毒功能。

命令

mail anti-virus {**pop3** | **imap** | **smtp**} {**enable** | **disable**}

语法

pop3 | imap | smtp	• pop3— 邮局协议，用于接收邮件。 • imap— 因特网信息访问协议，用于接收邮件。 • smtp— 简单邮件传输协议，用于发送邮件。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用 POP3 协议的防病毒功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]mail anti-virus pop3 enable
```

相关命令

命令名称	描述信息
show profile mail anti-virus	显示指定 profile 的邮件协议防病毒功能状态。

mail information-disclosure substitute

使用 **mail information-disclosure substitute** 命令替换邮件服务器信息。

命令

mail information-disclosure substitute {**pop3-banner** | **imap-banner** | **smtp-banner**} *string*

语法

pop3-banner | imap-banner | smtp-banner	• pop3-banner—POP3 服务器信息 • imap-banner—IMAP 服务器信息 • smtp-banner—SMTP 服务器信息
string	自定义信息，格式为 LINE。

说明

要替换邮件服务器信息，必须先启用邮件服务器信息替换功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 替换 POP3 服务器信息为 Mail Server Ready。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]mail information-disclosure substitute pop3-banner Mail Server Ready
```

相关命令

命令名称	描述信息
mail information-disclosure substitute enable, disable	启用或禁用邮件服务器信息替换功能。
show profile mail information-disclosure	显示指定 profile 的邮件服务器信息替换功能的相关信息。

mail information-disclosure substitute enable, disable

使用 **mail information-disclosure substitute enable, disable** 命令启用或禁用邮件服务器信息替换功能。

命令

mail information-disclosure substitute {**pop3-banner** | **imap-banner** | **smtp-banner**} {**enable** | **disable**}

语法

pop3-banner | imap-banner | smtp-banner	• pop3-banner—POP3 服务器信息 • imap-banner—IMAP 服务器信息 • smtp-banner—SMTP 服务器信息

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用 POP3 服务器信息替换功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]mail information-disclosure substitute pop3-banner enable
```

相关命令

命令名称	描述信息
mail information-disclosure substitute	替换邮件服务器信息。
show profile mail information-disclosure	显示指定 profile 的邮件服务器信息替换功能的相关信息。

mail size

使用 **mail size** 命令设置邮件大小上限。

命令

mail size *mail_size*

语法

mail_size	邮件大小上限，单位为 MB，格式为 INTEGER<1-100>。缺省值为 10MB。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置邮件大小上限为 20。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]mail size 20
```

相关命令

命令名称	描述信息
show profile mail size_limit	显示指定 profile 的邮件大小上限。

protocol-anomaly action

使用 **protocol-anomaly action** 命令设置邮件协议异常检测相关功能的动作。

命令

{**pop3** | **imap** | **smtp**} **protocol-anomaly** {**length** | **sequence** | **format** | **mime** | **traffic**} **action** {**block** | **allow** | **reject** | **detail**}

语法

**pop3	imap	smtp**	• pop3— 邮局协议，标准端口号为 110。 • imap— 因特网信息访问协议，标准端口号为 143。 • smtp— 简单邮件传输协议，标准端口号为 25。
**length	sequence	format	mime	traffic**	• length— 表示检测命令和应答长度异常 • sequence— 表示检测命令顺序异常 • format— 表示检测命令和应答格式异常 • mime— 表示检测 MIME 格式和长度异常 • traffic— 表示探测非标准端口上的邮件协议流量
**block	allow	reject	detail**	检测到协议异常时采取的动作。 • block— 阻断，表示断开服务器与客户端之间的连接。 • allow— 放行，表示允许数据包通过。 • reject— 拒绝，表示丢弃异常数据包，并通知客户端。 • detail— 表示根据检测命令和应答格式异常的详细设置采取动作。

说明

1. 仅有检测命令和应答长度异常、检测命令顺序异常时才能够设置 reject 动作。
2. 要设置非标准端口上的邮件协议流量探测的动作，必须先启用非标准端口上的邮件协议流量探测功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置 POP3 协议的命令顺序异常检测的动作为放行。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]pop3 protocol-anomaly sequence action allow
```

相关命令

命令名称	描述信息
protocol-anomaly format detail action	设置邮件协议命令和请求格式异常检测的动作。
protocol-anomaly format detail response action	设置邮件协议应答格式异常检测的动作。
protocol-anomaly traffic enable, disable	启用或禁用非标准端口上的邮件协议流量检测功能。
show profile protocol-anomaly	显示指定 profile 的邮件协议异常检测的相关信息。

protocol-anomaly format detail action

使用 **protocol-anomaly format detail action** 命令设置邮件协议命令和请求格式异常检测的动作。

命令

{**pop3** | **imap** | **smtp**} **protocol-anomaly format detail action** {**block** | **allow** | **reject**} *string*

语法

block | **allow** | **reject**	检测到协议异常时采取的动作。 • block— 阻断，表示断开服务器与客户端之间的连接。 • allow— 放行，表示允许数据包通过。 • reject— 拒绝，表示丢弃异常数据包，并通知客户端。
string	命令，格式为 LINE。

说明

如果要输入多个命令，可以用空格分隔。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置 POP3 协议的 USER 和 PASS 命令和请求格式异常检测的动作为放行。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]pop3 protocol-anomaly format detail action allow USER PASS
```

相关命令

命令名称	描述信息
protocol-anomaly action	设置邮件协议异常检测相关功能的动作。

命令名称	描述信息
protocol-anomaly format detail response action	设置邮件协议应答格式异常检测的动作。
show profile protocol-anomaly detail	显示指定 profile 的邮件协议格式异常检测的详细信息。

protocol-anomaly format detail response action

使用 **protocol-anomaly format detail response action** 命令设置邮件协议应答格式异常检测的动作。

命令

{**pop3** | **imap** | **smtp**} **protocol-anomaly format detail response action** {**block** | **allow**}

语法

block | **allow**	检测到协议异常时采取的动作。 • block— 阻断，表示断开服务器与客户端之间的连接。 • allow— 放行，表示允许数据包通过。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置 POP3 协议的应答格式异常检测的动作为阻断。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]pop3 protocol-anomaly format detail response action block
```

相关命令

命令名称	描述信息
protocol-anomaly action	设置邮件协议异常检测相关功能的动作。
protocol-anomaly format detail action	设置邮件协议命令和请求格式异常检测的动作。
show profile protocol-anomaly detail	显示指定 profile 的邮件协议格式异常检测的详细信息。

protocol-anomaly log

使用 **protocol-anomaly log** 命令开启或关闭邮件协议异常检测相关功能的产生日志功能。

命令

{**pop3** | **imap** | **smtp**} **protocol-anomaly** {**length** | **sequence** | **format** | **mime** | **traffic**} **log** {**on** | **off**}

语法

length | **sequence** | **format** | **mime** | **traffic**	• length— 表示检测命令和应答长度异常 • sequence— 表示检测命令顺序异常 • format— 表示检测命令和应答格式异常 • mime— 表示检测 MIME 格式和长度异常 • traffic— 表示探测非标准端口上的邮件协议流量

说明

要开启或关闭非标准端口上的邮件协议流量探测的产生日志功能，必须先启用非标准端口上的邮件协议流量探测功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启 POP3 协议检测命令顺序异常的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]pop3 protocol-anomaly sequence log on
```

相关命令

命令名称	描述信息
protocol-anomaly traffic enable, disable	启用或禁用非标准端口上的邮件协议流量检测功能。
show profile protocol-anomaly	显示指定 profile 的邮件协议异常检测的相关信息。

protocol-anomaly traffic enable, disable

使用 **protocol-anomaly traffic enable, disable** 命令启用或禁用非标准端口上的邮件协议流量探测功能。

命令

{**pop3** | **imap** | **smtp**} **protocol-anomaly traffic** {**enable** | **disable**}

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用非标准端口上的 POP3 流量探测功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]pop3 protocol-anomaly traffic enable
```

相关命令

命令名称	描述信息
protocol-anomaly action	设置邮件协议异常检测相关功能的动作。
protocol-anomaly log	开启或关闭邮件协议异常检测相关功能的产生日志功能。
show profile protocol-anomaly	显示指定 profile 的邮件协议异常检测的相关信息。

protocol-restriction block

使用 **protocol-restriction block** 命令设置阻断或允许的命令。

命令

{**pop3** | **imap** | **smtp**} **protocol-restriction block command** {**blocked** | **allowed**} *string*

语法

blocked | **allowed**	检测到协议异常时采取的动作。 • blocked— 阻断，表示断开服务器与客户端之间的连接。 • allowed— 允许，表示允许数据包通过。
string	命令，格式为 LINE。

说明

1. 如果要输入多个命令，可以用空格分隔。
2. 要设置阻断或允许的命令，必须先启用已知命令阻断功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置 POP3 协议阻断的命令为 NOOP。

```
NetEye@root-system-pro-test]pop3 protocol-restriction block command
blocked NOOP
```

相关命令

命令名称	描述信息
protocol-restriction block enable, disable	启用或禁用命令阻断功能。
protocol-restriction enable, disable	启用或禁用邮件协议限制功能。
show profile protocol-restriction block	显示指定 profile 的命令阻断功能的相关信息。

protocol-restriction block enable, disable

使用 **protocol-restriction block enable, disable** 命令启用或禁用命令阻断功能。

命令

{**pop3** | **imap** | **smtp**} **protocol-restriction block** {**unknown-command** | **command**} {**enable** | **disable**}

语法

unknown-command	**command**	• unknown-command— 表示阻断未知命令 • command— 表示阻断已知命令

说明

要启用或禁用命令阻断功能，必须先启用相应的邮件协议限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用 POP3 协议的未知命令阻断功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]pop3 protocol-restriction block unknown-command enable
```

相关命令

命令名称	描述信息
protocol-restriction block	设置邮件协议阻断或允许的命令。
protocol-restriction block log	开启或关闭命令阻断功能的产生日志功能。
protocol-restriction enable, disable	启用或禁用邮件协议限制功能。
show profile protocol-restriction block	显示指定 profile 的命令阻断功能的相关信息。

protocol-restriction block log

使用 **protocol-restriction block log** 命令开启或关闭命令阻断功能的产生日志功能。

命令

{**pop3** | **imap** | **smtp**} **protocol-restriction block** {**unknown-command** | **command**} **log** {**on** | **off**}

语法

unkmown-command | **command**	• unknown-command— 表示阻断未知命令 • command— 表示阻断已知命令

说明

要开启或关闭产生日志功能，必须先启用相应的命令阻断功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启 POP3 协议的未知命令阻断功能的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]pop3 protocol-restriction block unknown-command log on
```

相关命令

命令名称	描述信息
protocol-restriction block enable, disable	启用或禁用命令阻断功能。
protocol-restriction enable, disable	启用或禁用邮件协议限制功能。
show profile protocol-restriction block	显示指定 profile 的命令阻断功能的相关信息。

protocol-restriction enable, disable

使用 **protocol-restriction enable, disable** 命令启用或禁用邮件协议限制功能。

命令

{**pop3** | **imap** | **smtp**} **protocol-restriction** {**enable** | **disable**}

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用 POP3 协议限制功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]pop3 protocol-restriction enable
```

相关命令

命令名称	描述信息
show profile protocol-restriction	显示指定 profile 的邮件协议限制的相关信息。

protocol-restriction level

使用 **protocol-restriction level** 命令设置邮件协议限制的等级。

命令

{**pop3** | **imap** | **smtp**} **protocol-restriction level** {**high** | **medium** | **low** | **custom**}

说明

系统为管理员提供了高、中、低三个级别的保护配置，推荐级别为 “中”。防火墙管理员也可以自定义保护配置。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为防护配置 test 设置 POP3 协议限制等级为中。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]pop3 protocol-restriction level medium
```

相关命令

命令名称	描述信息
protocol-restriction enable, disable	启用或禁用邮件协议限制功能。
show profile protocol-restriction level	显示指定 profile 的邮件协议限制的等级。

protocol-restriction max

使用 **protocol-restriction max** 命令设置 POP3 或 SMTP 协议限制相关功能的最大值。

命令

{**pop3** | **smtp**} **protocol-restriction max** {**command-length** | **command** | **noop-command** | **parameter** | **response** | **unknown-command**} *number_value*

语法

command-length | **command** | **noop-command** | **parameter** | **response** | **unknown-command**	• command-length— 表示最大命令长度 • command— 表示最多命令次数 • noop-command— 表示最多 NOOP 命令次数 • parameter— 表示最大参数长度 • response— 表示最大应答长度 • unknowm-command— 表示最多未知命令次数
number_value	• 最大命令长度值，单位为字节，格式为 INTEGER<1-1024>。 • 最多命令次数值，格式为 INTEGER<1-256>。 • 最多 NOOP 命令次数值，格式为 INTEGER<1-128>。 • 最大参数长度值，单位为字节，格式为 INTEGER<1-512>。 • 最大应答长度值，单位为字节，格式为 INTEGER<1-2048>。 • 最多未知命令次数值，格式为 INTEGER<1-128>。

说明

要设置 POP3 或 SMTP 协议限制相关功能的最大值，必须先启用相应功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置 POP3 协议限制的最多命令次数值为 128。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]pop3 protocol-restriction max command 128
```

相关命令

命令名称	描述信息
protocol-restriction enable, disable	启用或禁用邮件协议限制功能。
protocol-restriction max enable, disable	启用或禁用邮件协议限制的相关功能。
show profile protocol-restriction	显示指定 profile 的邮件协议限制的相关信息。

protocol-restriction max action

使用 **protocol-restriction max action** 命令设置邮件协议限制相关功能的动作。

命令

{**pop3** | **imap** | **smtp**} **protocol-restriction max** {**command-length** | **command** | **noop-command** | **parameter** | **response** | **tag** | **unknown-command**} **action** {**block** | **allow** | **reject**}

语法

command-length | **command** | **noop-command** | **parameter** | **response** | **tag** | **unknown-command**	• command-length— 表示最大命令长度 • command— 表示最多命令次数 • noop-command— 表示最多 NOOP 命令次数 • parameter— 表示最大参数长度 • response— 表示最大应答长度 • tag— 表示最大 Tag 长度 (仅适用于 IMAP 协议) • unknowm-command— 表示最多未知命令次数
block | **allow** | **reject**	• block— 阻断，表示断开服务器与客户端之间的连接。 • allow— 放行，表示允许数据包通过。 • reject— 拒绝，表示丢弃异常数据包，并通知客户端。

说明

1. 仅有检测到最大命令长度、最大参数长度和最大Tag长度超出限制时才能够设置reject动作。
2. 要设置邮件协议限制相关功能的动作，必须先启用相应功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置 POP3 协议限制的最多命令次数的动作为放行。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]pop3 protocol-restriction max command action allow
```

相关命令

命令名称	描述信息
protocol-restriction enable, disable	启用或禁用邮件协议限制功能。
protocol-restriction max enable, disable	启用或禁用邮件协议限制的相关功能。
show profile protocol-restriction	显示指定 profile 的邮件协议限制的相关信息。

protocol-restriction max enable, disable

使用 **protocol-restriction max enable, disable** 命令启用或禁用邮件协议限制的相关功能。

命令

{**pop3** | **imap** | **smtp**} **protocol-restriction max** {**command-length** | **command** | **noop-command** | **parameter** | **response** | **tag** | **unknown-command**} {**enable** | **disable**}

语法

command-length | **command** | **noop-command** | **parameter** | **response** | **tag** | **unknown-command**	• command-length— 表示最大命令长度 • command— 表示最多命令次数 • noop-command— 表示最多 NOOP 命令次数 • parameter— 表示最大参数长度 • response— 表示最大应答长度 • tag— 表示最大 Tag 长度 (仅适用于 IMAP 协议) • unknowm-command— 表示最多未知命令次数

说明

要启用或禁用邮件协议限制的相关功能，必须先启用邮件协议限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用 POP3 协议限制的最多命令次数功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]pop3 protocol-restriction max command enable
```

相关命令

命令名称	描述信息
protocol-restriction enable, disable	启用或禁用邮件协议限制功能。
show profile protocol-restriction	显示指定 profile 的邮件协议限制的相关信息。

protocol-restriction max log

使用 **protocol-restriction max log** 命令开启或关闭邮件协议限制相关功能的产生日志功能。

命令

{**pop3** | **imap** | **smtp**} **protocol-restriction max** {**command-length** | **command** | **noop-command** | **parameter** | **response** | **tag** | **unknown-command**} **log** {**on** | **off**}

语法

command-length | **command** | **noop-command** | **parameter** | **response** | **tag** | **unknown-command**	• command-length— 表示最大命令长度 • command— 表示最多命令次数 • noop-command— 表示最多 NOOP 命令次数 • parameter— 表示最大参数长度 • response— 表示最大应答长度 • tag— 表示最大 Tag 长度 (仅适用于 IMAP 协议) • unknowm-command— 表示最多未知命令次数

说明

要开启或关闭产生日志功能，必须先启用相应功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启 POP3 协议限制的最多命令次数的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]pop3 protocol-restriction max command log on
```

相关命令

命令名称	描述信息
protocol-restriction enable, disable	启用或禁用邮件协议限制功能。

命令名称	描述信息
protocol-restriction max enable, disable	启用或禁用邮件协议限制的相关功能。
show profile protocol-restriction	显示指定 profile 的邮件协议限制的相关信息。

protocol-restriction user-defined

使用 **protocol-restriction user-defined** 命令设置用户自定义命令。

命令

{**pop3** | **imap** | **smtp**} **protocol-restriction allow user-defined command** *command_name* {**enable** | **disable**}

语法

command_name	• POP3 用户和 SMTP 用户自定义命令名称，格式为 WORD<4-8>。 • IMAP 用户自定义命令名称，格式为 WORD<4-16>。
enable | **disable**	• enable— 表示放行用户自定义命令 • disable— 表示阻断用户自定义命令

说明

1. 如果自定义列表中不存在与输入的参数匹配的条目，则表示添加；如果存在匹配的条目，则表示修改相应条目的状态。
2. 要设置用户自定义命令，必须先启用相应的用户自定义命令功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 1. 为 profile test 添加 POP3 用户自定义命令 RLOG，并放行该命令。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]pop3 protocol-restriction allow
user-defined command RLOG enable
```

范例 2. 为 profile test 修改 POP3 用户自定义命令 RLOG 的动作为阻断。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]pop3 protocol-restriction allow
user-defined command RLOG disable
```

相关命令

命令名称	描述信息
protocol-restriction user-defined enable, disable	启用或禁用用户自定义命令功能。
show profile protocol-restriction user-defined	显示指定 profile 的用户自定义命令的相关信息。
unset protocol-restriction user-defined	删除指定用户自定义命令。

protocol-restriction user-defined enable, disable

使用 **protocol-restriction user-defined enable, disable** 命令启用或禁用用户自定义命令功能。

命令

{**pop3** | **imap** | **smtp**} **protocol-restriction allow user-defined** {**enable** | **disable**}

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用 POP3 用户自定义命令功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]pop3 protocol-restriction allow user-defined enable
```

相关命令

命令名称	描述信息
show profile protocol-restriction user-defined	显示指定 profile 的用户自定义命令的相关信息。

protocol-restriction user-defined log

使用 **protocol-restriction user-defined log** 命令开启或关闭用户自定义命令的产生日志功能。

命令

{**pop3** | **imap** | **smtp**} **protocol-restriction allow user-defined log** {**on** | **off**}

说明

要开启或关闭产生日志功能，必须先启用相应的用户自定义命令功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启 POP3 用户自定义命令的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]pop3 protocol-restriction allow user-defined log on
```

相关命令

命令名称	描述信息
protocol-restriction user-defined enable, disable	启用或禁用用户自定义命令功能。
show profile protocol-restriction user-defined	显示指定 profile 的用户自定义命令的相关信息。

show profile mail anti-spam

使用 **show profile mail anti-spam** 命令显示指定 profile 的反垃圾邮件功能状态。

命令

show profile *profile_name* **mail anti-spam**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 邮件协议的反垃圾邮件功能状态。

```
NetEye@root>show profile test mail anti-spam
```

【返回结果】

```
smtp:enable
pop3:enable
```

相关命令

命令名称	描述信息
mail anti-spam enable, disable	启用或禁用反垃圾邮件扫描功能。

show profile mail anti-virus

使用 **show profile mail anti-virus** 命令显示指定 profile 的邮件协议防病毒功能状态。

命令

show profile *profile_name* **mail anti-virus**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的邮件协议防病毒功能状态。

```
NetEye@root>show profile test mail anti-virus
```

【返回结果】

```
smtp:enable
pop3:enable
imap:enable
```

相关命令

命令名称	描述信息
mail anti-virus enable, disable	启用或禁用邮件协议的防病毒功能。

show profile mail information-disclosure

使用 **show profile mail information-disclosure** 命令显示指定 profile 的邮件服务器信息替换功能的相关信息。

命令

show profile *profile_name* **mail information-disclosure**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 邮件服务器信息替换功能的相关信息。

```
NetEye@root>show profile test mail information-disclosure
```

【返回结果】

```
state     name                                  message
enable    Substitute SMTP Server Banner with    Mail Server Ready...
enable    Substitute POP3 Server Banner with    Mail Server Ready...
enable    Substitute IMAP Server Banner with    Mail Server Ready...
```

相关命令

命令名称	描述信息
mail information-disclosure substitue	替换邮件服务器信息。
mail information-disclosure substitue enable, disable	启用或禁用邮件服务器信息替换功能。

show profile mail size_limit

使用 **show profile mail size_limit** 命令显示指定 profile 的邮件大小上限。

命令

show profile *profile_name* **mail size_limit**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的邮件大小上限。

```
NetEye@root>show profile test mail size_limit
```

【返回结果】

```
Mail Size Limit
Mail Size :   4 (MB)
```

相关命令

命令名称	描述信息
mail size	设置邮件大小上限。

show profile protocol-anomaly

使用 **show profile protocol-anomaly** 命令显示指定 profile 的邮件协议异常检测的相关信息。

命令

show profile *profile_name* {**pop3** | **imap** | **smtp**} **protocol-anomaly**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的 POP3 协议异常检测的相关信息。

```
NetEye@root>show profile test pop3 protocol-anomaly
```

【返回结果】

```
state    name                                                Action
log
   --    Inspect command and response format anomaly          Accept Detail
Config on
   --    Inspect command and response length anomaly          Reject
on
   --    Inspect command sequence anomaly                    Reject
on
   --    Inspect MIME format and length anomaly               Allow
on
disable  Detect POP3 traffic on non-standard (non-110) ports  Block
on
```

相关命令

命令名称	描述信息
protocol-anomaly action	设置邮件协议异常检测相关功能的动作。
protocol-anomaly format detail action	设置邮件协议命令和请求格式异常检测的动作。
protocol-anomaly format detail response action	设置邮件协议应答格式异常检测的动作。
protocol-anomaly log	开启或关闭邮件协议异常检测相关功能的产生日志功能。
protocol-anomaly traffic enable, disable	启用或禁用非标准端口上的邮件协议流量探测功能。
show profile protocol-anomaly detail	显示邮件协议格式异常检测的详细信息。

show profile protocol-anomaly detail

使用 **show profile protocol-anomaly detail** 命令显示指定 profile 的邮件协议格式异常检测的详细信息。

命令

show profile *profile_name* {**pop3** | **imap** | **smtp**} **protocol-anomaly inspect format detail**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的 POP3 协议格式异常检测的详细信息。

```
NetEye@root>show profile test pop3 protocol-anomaly inspect format
detail
```

【返回结果】

```
Response        block
------------------------
USER            Reject
PASS            Block
STAT            Reject
UIDL            Reject
LIST            Reject
RETR            Reject
TOP             Reject
DELE            Reject
RSET            Reject
NOOP            Reject
QUIT            Allow
APOP            Reject
```

```
CAPA            Reject
AUTH            Block
STLS            Reject
XTND            Reject
RESPONSE        Block
```

相关命令

命令名称	描述信息
protocol-anomaly format detail action	设置邮件协议命令和请求格式异常检测的动作。
protocol-anomaly format detail response action	设置邮件协议应答格式异常检测的动作。
show profile protocol-anomaly	显示邮件协议异常检测的相关信息。

show profile protocol-restriction

使用 **show profile protocol-restriction** 命令显示指定 profile 的邮件协议限制的相关信息。

命令

show profile *profile_name* {**pop3** | **imap** | **smtp**} **protocol-restriction**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的 SMTP 协议限制的相关信息。

```
NetEye@root>show profile test smtp protocol-restriction
```

【返回结果】

```
Protocol Restriction : enable
Level: Medium
------------------------------------------------------------------------------
state     name                    length(bytes)   Action   log
enable    MAX Command Length      256             Reject   on
enable    MAX Parameter Length    256             Reject   on
enable    MAX Response Length     512             Block    on
enable    MAX NOOP Commands       10              Block    on
disable   MAX Commands            128             Block    on
enable    MAX Unknown Commands    10              Block    on

SMTP Add "Received" header when forwarding : enable                    Log :
on
SMTP Strip MIME parts with mutiple "Content-Type" headers : enable       Log :
on
```

```
SMTP Strip MIME parts with mutiple "Encoding" headers : enable          Log :
on
SMTP Strip MIME parts with unknown "Encoding" headers : disable         Log :
on
SMTP Strip all of the email attachments : disable                       Log :
on
SMTP Strip all of the fragmented email messages : disable               Log :
on
SMTP Block message with recipient without domain name : enable          Log :
on
```

相关命令

命令名称	描述信息
protocol-restriction enable, disable	启用或禁用邮件协议限制功能。
protocol-restriction level	设置邮件协议限制的等级。
protocol-restriction max	设置邮件协议限制相关功能的最大值。
protocol-restriction max action	设置邮件协议限制相关功能的动作。
protocol-restriction max enable, disable	启用或禁用邮件协议限制的相关功能。
protocol-restriction max log	启用或禁用邮件协议限制相关功能的产生日志功能。
smtp protocol-restriction block recipient enable, disable	启用或禁用 SMTP 协议阻断收件人没有域名的邮件功能。
smtp protocol-restriction block recipient log	启用或禁用 SMTP 协议阻断收件人没有域名的邮件功能的产生日志功能。
smtp protocol-restriction received enable, disable	启用或禁用 SMTP 协议转发时添加 Received 头字段功能。
smtp protocol-restriction received log	启用或禁用 SMTP 协议转发时添加 Received 头字段功能的产生日志功能。
smtp protocol-restriction strip enable, disable	启用或禁用 SMTP 协议剥离所有邮件附件或所有分片邮件功能。
smtp protocol-restriction strip log	启用或禁用 SMTP 协议剥离所有邮件附件或所有分片邮件功能的产生日志功能。
smtp protocol-restriction strip multiple enable, disable	启用或禁用 SMTP 协议剥离带有多个 Content-Type 头字段或 Encoding 头字段的 MIME 字段功能。

命令名称	描述信息
smtp protocol-restriction strip multiple log	启用或禁用 SMTP 协议剥离带有多个 Content-Type 头字段或 Encoding 头字段的 MIME 字段功能的产生日志功能。
smtp protocol-restriction strip unknown enable, disable	启用或禁用 SMTP 协议剥离带有未知 Encoding 头字段的 MIME 字段功能。
smtp protocol-restriction strip unknown log	启用或禁用 SMTP 协议剥离带有未知 Encoding 头字段的 MIME 字段功能的产生日志功能。

show profile protocol-restriction block

使用 **show profile protocol-restriction block** 命令显示指定 profile 的命令阻断功能的相关信息。

命令

show profile *profile_name* {**pop3** | **imap** | **smtp**} **protocol-restriction block command**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的 POP3 协议命令阻断功能的相关信息。

```
NetEye@root>show profile test pop3 protocol-restriction block command
```

【返回结果】

```
POP3 Block Unknown Commands : disable       Log : on
POP3 Block Commands : enable                Log : on
-------------------------------------------------------------
--Allowed Commands------
USER
PASS
STAT
UIDL
LIST
RETR
TOP
DELE
RSET
QUIT
APOP
```

```
CAPA
AUTH
STLS
XTND
------------------------
--Blocked Commands------
NOOP
```

相关命令

命令名称	描述信息
protocol-restriction block	设置阻断或允许的命令。
protocol-restriction block enable, disable	启用或禁用命令阻断功能。
protocol-restriction block log	开启或关闭命令阻断功能的产生日志功能。
protocol-restriction enable, disable	启用或禁用邮件协议限制功能。

show profile protocol-restriction level

使用 **show profile protocol-restriction level** 命令显示指定 profile 的邮件协议限制等级。

命令

show profile *profile_name* {**pop3** | **imap** | **smtp**} **protocol-restriction level**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的 POP3 协议限制等级。

```
NetEye@root>show profile test pop3 protocol-restriction level
```

【返回结果】

```
Profilename is test current level: Medium
```

相关命令

命令名称	描述信息
protocol-restriction enable, disable	启用或禁用邮件协议限制功能。
protocol-restriction level	设置邮件协议限制的等级。

show profile protocol-restriction user-defined

使用 **show profile protocol-restriction user-defined** 命令显示指定 profile 的用户自定义命令的相关信息。

命令

show profile *profile_name* {**pop3** | **imap** | **smtp**} **protocol-restriction allow user-defined command**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的 POP3 用户自定义命令的相关信息。

```
NetEye@root>show profile test pop3 protocol-restriction allow
user-defined command
```

【返回结果】

```
User-Defined Commands : enable
Log : on
-----------------------------------
State     Command
enable    XAUTH
disable   XLOGIN
enable    RLOG
```

相关命令

命令名称	描述信息
protocol-restriction user-defined	配置用户自定义命令。
protocol-restriction user-defined enable, disable	启用或禁用用户自定义命令功能。
protocol-restriction user-defined log	开启或关闭用户自定义命令的产生日志功能。
unset protocol-restriction user-defined	删除指定用户自定义命令。

smtp protocol-restriction block recipient enable, disable

使用 **smtp protocol-restriction block recipient enable, disable** 命令启用或禁用 SMTP 协议阻断收件人没有域名的邮件功能。

命令

smtp protocol-restriction block recipient {**enable** | **disable**}

说明

要启用或禁用该功能，必须先启用 SMTP 邮件协议限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用 SMTP 协议阻断收件人没有域名的邮件功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]smtp protocol-restriction block recipient enable
```

相关命令

命令名称	描述信息
show profile protocol-restriction	显示指定 profile 的邮件协议限制的相关信息。
smtp protocol-restriction block recipient log	开启或关闭 SMTP 协议阻断收件人没有域名的邮件功能的产生日志功能。

smtp protocol-restriction block recipient log

使用 **smtp protocol-restriction block recipient log** 命令开启或关闭 SMTP 协议阻断收件人没有域名的邮件的产生日志功能。

命令

smtp protocol-restriction block recipient log {**on** | **off**}

说明

要开启或关闭产生日志功能，必须先启用相应功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启 SMTP 协议阻断收件人没有域名的邮件的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]smtp protocol-restriction block recipient log on
```

相关命令

命令名称	描述信息
show profile protocol-restriction	显示指定 profile 的邮件协议限制的相关信息。
smtp protocol-restriction block recipient enable, disable	启用或禁用 SMTP 协议阻断收件人没有域名的邮件功能。

smtp protocol-restriction received enable, disable

使用 **smtp protocol-restriction received enable, disable** 命令启用或禁用 SMTP 协议转发时添加 Received 头字段的功能。

命令

smtp protocol-restriction received {**enable** | **disable**}

说明

要启用或禁用该功能，必须先启用 SMTP 邮件协议限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用 SMTP 协议转发时添加 Received 头字段的功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]smtp protocol-restriction received enable
```

相关命令

命令名称	描述信息
show profile protocol-restriction	显示指定 profile 的邮件协议限制的相关信息。
smtp protocol-restriction received log	开启或关闭 SMTP 协议转发时添加 Received 头字段功能的产生日志功能。

smtp protocol-restriction received log

使用 **smtp protocol-restriction received log** 命令开启或关闭 SMTP 协议转发时添加 Received 头字段的产生日志功能。

命令

smtp protocol-restriction received log {**on** | **off**}

说明

要开启或关闭产生日志功能，必须先启用相应功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启 SMTP 协议转发时添加 Received 头字段的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]smtp protocol-restriction received log on
```

相关命令

命令名称	描述信息
show profile protocol-restriction	显示指定 profile 的邮件协议限制的相关信息。
smtp protocol-restriction received enable, disable	启用或禁用 SMTP 协议转发时添加 Received 头字段的功能。

smtp protocol-restriction strip enable, disable

使用 **smtp protocol-restriction strip enable, disable** 命令启用或禁用 SMTP 协议剥离所有邮件附件或所有分片邮件的功能。

命令

smtp protocol-restriction strip {**attachment** | **fragment**} {**enable** | **disable**}

语法

attachment | fragment	• attachment— 表示邮件附件 • fragment— 表示分片邮件

说明

要启用或禁用指定功能，必须先启用 SMTP 邮件协议限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用 SMTP 协议剥离所有邮件附件的功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]smtp protocol-restriction strip attachment enable
```

相关命令

命令名称	描述信息
show profile protocol-restriction	显示指定 profile 的邮件协议限制的相关信息。
smtp protocol-restriction strip log	开启或关闭 SMTP 协议剥离所有邮件附件或所有分片邮件功能的产生日志功能。

smtp protocol-restriction strip log

使用 **smtp protocol-restriction strip log** 命令开启或关闭 SMTP 协议剥离所有邮件附件或所有分片邮件功能的产生日志功能。

命令

smtp protocol-restriction strip {**attachment** | **fragment**} **log** {**on** | **off**}

语法

attachment | fragment	• attachment— 表示邮件附件 • fragment— 表示分片邮件

说明

要开启或关闭产生日志功能，必须先启用相应功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启 SMTP 协议剥离所有邮件附件功能的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]smtp protocol-restriction strip attachment log on
```

相关命令

命令名称	描述信息
show profile protocol-restriction	显示指定 profile 的邮件协议限制的相关信息。
smtp protocol-restriction strip enable, disable	启用或禁用 SMTP 协议剥离所有邮件附件或所有分片邮件的功能。

smtp protocol-restriction strip multiple enable, disable

使用 **smtp protocol-restriction strip multiple enable, disable** 命令启用或禁用 SMTP 协议剥离带有多个 Content-Type 头字段或 Encoding 头字段的 MIME 字段功能。

命令

smtp protocol-restriction strip multiple {**content-type** | **encoding**} {**enable** | **disable**}

语法

content-type | encoding	• content-type— 表示 Content-Type 头字段的 MIME 字段 • encoding— 表示 Encoding 头字段的 MIME 字段

说明

要启用或禁用指定功能，必须先启用 SMTP 邮件协议限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用 SMTP 协议剥离带有多个 Encoding 头字段的 MIME 字段功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]smtp protocol-restriction strip multiple encoding enable
```

相关命令

命令名称	描述信息
show profile protocol-restriction	显示指定 profile 的邮件协议限制的相关信息。
smtp protocol-restriction strip multiple log	开启或关闭 SMTP 协议剥离带有多个 Content-Type 头字段或 Encoding 头字段的 MIME 字段功能的产生日志功能。

smtp protocol-restriction strip multiple log

使用 **smtp protocol-restriction strip multiple log** 命令开启或关闭 SMTP 协议剥离带有多个 Content-Type 头字段或 Encoding 头字段的 MIME 字段的产生日志功能。

命令

smtp protocol-restriction strip multiple {**content-type** | **encoding**} **log** {**on** | **off**}

语法

content-type | encoding	• content-type— 表示 Content-Type 头字段的 MIME 字段 • encoding— 表示 Encoding 头字段的 MIME 字段

说明

要开启或关闭产生日志功能，必须先启用相应功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启 SMTP 协议剥离带有多个 Encoding 头字段的 MIME 字段的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]smtp protocol-restriction strip multiple encoding log on
```

相关命令

命令名称	描述信息
show profile protocol-restriction	显示指定 profile 的邮件协议限制的相关信息。
smtp protocol-restriction strip multiple enable, disable	启用或禁用 SMTP 协议剥离带有多个 Content-Type 头字段或 Encoding 头字段的 MIME 字段的功能。

smtp protocol-restriction strip unknown enable, disable

使用 **smtp protocol-restriction strip unknown enable, disable** 命令启用或禁用 SMTP 协议剥离带有未知 Encoding 头字段的 MIME 字段功能。

命令

smtp protocol-restriction strip unknown encoding {**enable** | **disable**}

说明

要启用或禁用该功能，必须先启用 SMTP 邮件协议限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用 SMTP 协议剥离带有未知 Encoding 头字段的 MIME 字段功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]smtp protocol-restriction strip unknown encoding enable
```

相关命令

命令名称	描述信息
show profile protocol-restriction	显示指定 profile 的邮件协议限制的相关信息。
smtp protocol-restriction strip unknown log	开启或关闭 SMTP 剥离带有未知 Encoding 头字段的 MIME 字段功能的产生日志功能。

smtp protocol-restriction strip unknown log

使用 **smtp protocol-restriction strip unknown log** 命令开启或关闭 SMTP 协议剥离带有未知 Encoding 头字段的 MIME 字段功能的产生日志功能。

命令

smtp protocol-restriction strip unknown encoding log {on | off}

说明

要开启或关闭产生日志功能，必须先启用相应功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启 SMTP 协议剥离带有未知 Encoding 头字段的 MIME 字段功能的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]smtp protocol-restriction strip unknown encoding log on
```

相关命令

命令名称	描述信息
show profile protocol-restriction	显示指定 profile 的邮件协议限制的相关信息。
smtp protocol-restriction strip unknown enable, disable	启用或禁用 SMTP 协议剥离带有未知 Encoding 头字段的 MIME 字段的功能。

unset protocol-restriction user-defined

使用 **unset protocol-restriction user-defined** 命令删除指定用户自定义命令。

命令

unset {**pop3** | **imap** | **smtp**} **protocol-restriction allow user-defined command** *command_name*

语法

command_name	• POP3 用户和 SMTP 用户自定义命令名称，格式为 WORD<4-8>。 • IMAP 用户自定义命令名称，格式为 WORD<4-16>。

说明

要删除用户自定义命令，必须先启用相应的用户自定义命令功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 删除 POP3 用户自定义命令 RLOG。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]unset pop3 protocol-restriction allow user-defined command RLOG
```

相关命令

命令名称	描述信息
protocol-restriction user-defined	配置用户自定义命令。
protocol-restriction user-defined enable, disable	启用或禁用用户自定义命令功能。
show profile protocol-restriction user-defined	显示指定 profile 的用户自定义命令的相关信息。

FTP 检测

ftp virus-scan enable, disable

使用 **ftp virus-scan enable, disable** 命令启用或禁用 FTP 流量病毒扫描。

命令

ftp virus-scan {**enable** | **disable**}

语法

enable | **disable**	• enable— 启用 FTP 流量病毒扫描 • disable— 禁用 FTP 流量病毒扫描

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在 Profile 配置模式下使用。

相关命令

命令名称	描述信息
show profile ftp	显示指定 profile 的 FTP 流量病毒扫描设置。

show profile ftp

使用 **show profile ftp** 命令显示指定 profile 的 FTP 流量病毒扫描设置。

命令

show profile *profile_name* **ftp**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的 FTP 流量病毒扫描设置。

```
NetEye@root>show profile test ftp
```

【返回结果】

```
Scan Virus : Enable
```

相关命令

命令名称	描述信息
ftp virus-scan enable, disable	启用或禁用 FTP 流量病毒扫描。

DNS 检测

dns cache_defense enable, disable

使用 **dns cache_defense enable, disable** 命令启用或禁用缓存中毒防御功能。

命令

dns cache_defense {**enable** | **disable**}

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用缓存中毒防御功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns cache_defense enable
```

相关命令

命令名称	描述信息
show profile dns cache_defense	显示指定 profile 的缓存中毒防御功能的相关信息。

dns cache_defense dns_scrambling enable, disable

使用 **dns cache_defense dns_scrambling enable, disable** 命令启用或禁用 DNS 不规则化的相关功能。

命令

dns cache_defense dns_scrambling [id |proxy] {enable | disable}

语法

**id	proxy**	• id— 表示 ID 不规则化 • proxy— 表示应用到嵌入式 DNS 代理

说明

1. 如果不指定 **id** 或 **proxy** 关键字，则表示启用或禁用 DNS 不规则化功能。
2. 要启用或禁用 DNS 不规则化功能，必须先启用缓存中毒防御功能。
3. 只有启用 DNS 不规则化功能后，才能启用或禁用 ID 不规则化以及应用到嵌入式 DNS 代理功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用 ID 不规则化功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns cache_defense dns_scrambling id enable
```

相关命令

命令名称	描述信息
show profile dns cache_defense	显示指定 profile 的缓存中毒防御功能的相关信息。

dns cache_defense drop enable, disable

使用 **dns cache_defense drop enable, disable** 命令启用或禁用外部请求限制的相关功能。

命令

dns cache_defense drop [**proxy** | *zone_name*] {**enable** | **disable**}

语法

proxy	表示应用到嵌入式 DNS 代理。
zone_name	安全域名称，格式为 WORD<1-15>。

说明

1. 如果不指定 **proxy** 关键字或 *zone_name* 参数，则表示启用或禁用外部请求限制功能。
2. 如果指定 *zone_name* 参数，则表示启用或禁用外部请求安全域。
3. 要启用或禁用外部请求限制功能，必须先启用缓存中毒防御功能。
4. 只有启用外部请求限制功能后，才能启用或禁用外部请求安全域以及应用到嵌入式 DNS 代理功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用外部请求安全域 zone1。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns cache_defense drop zone1 enable
```

相关命令

命令名称	描述信息
show profile dns cache_defense	显示指定 profile 的缓存中毒防御功能的相关信息。
show profile dns cache_defense drop zones	显示指定 profile 的外部请求安全域的相关信息。

dns cache_defense logging

使用 **dns cache_defense logging** 命令开启或关闭缓存中毒防御功能选项的产生日志功能。

命令

dns cache_defense {**dns_scrambling** | **drop** | **mismatched_replies**} **logging** {**on** | **off**}

语法

dns_scrambling | **drop** | **mismatched_replies**	• dns_scrambling— 表示 DNS 不规则化 • drop— 表示外部请求限制 • mismatched_replies— 表示常不匹配的应答检测

说明

要开启或关闭指定选项的产生日志功能，必须先启用相应选项功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启 DNS 不规则化的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns cache_defense dns_scrambling logging on
```

相关命令

命令名称	描述信息
show profile dns cache_defense	显示指定 profile 的缓存中毒防御功能的相关信息。

dns cache_defense mismatched_replies

使用 **dns cache_defense mismatched_replies** 命令设置常不匹配的应答检测功能的相关参数。

命令

dns cache_defense mismatched_replies {**Interval** *interval_time* | **max_number** *replies_num*}

语法

interval_time	时间间隔值。单位为秒，格式为 INTEGER<1-60>。缺省值为 5 秒。
replies_num	最大不匹配应答数。单位为次，格式为 INTEGER<1-65535>。缺省值为 50 次。

说明

要设置常不匹配的应答检测功能的相关参数，必须先启用常不匹配的应答检测功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置常不匹配的应答检测功能的最大不匹配应答数为 500 次。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns cache_defense mismatched_replies
max_number 500
```

相关命令

命令名称	描述信息
show profile dns cache_defense	显示指定 profile 的缓存中毒防御功能的相关信息。

dns cache_defense mismatched_replies enable, disable

使用 **dns cache_defense mismatched_replies enable, disable** 命令启用或禁用常不匹配的应答检测功能。

命令

dns cache_defense mismatched_replies {**enable** | **disable**}

说明

要启用或禁用常不匹配的应答检测功能，必须先启用缓存中毒防御功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用常不匹配的应答检测功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns cache_defense mismatched_replies enable
```

相关命令

命令名称	描述信息
show profile dns cache_defense	显示指定 profile 的缓存中毒防御功能的相关信息。

dns cache_defense select dns server

使用 **dns cache_defense select dns server** 命令启用或禁用进行缓存中毒防御的 DNS 服务器。

命令

dns cache_defense {**dns_scrambling** | **drop**} **select dns server** *server_name* {**enable** | **disable**}

语法

dns_scrambling | drop	• dns_scrambling— 表示 DNS 不规则化 • drop— 表示外部请求限制
server_name	DNS 服务器名称，格式为 WORD<1-15>。

说明

1. 只有选择了 DNS 服务器，设置的 DNS 不规则化功能和外部请求限制功能才能生效。
2. 要启用或禁用进行缓存中毒防御的 DNS 服务器，必须先启用相应的功能，包括 DNS 不规则化和外部请求限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用进行外部请求限制功能的 DNS 服务器 server1。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns cache_defense drop select dns server server1 enable
```

相关命令

命令名称	描述信息
show profile dns cache_defense select dns server	显示指定 profile 的进行缓存中毒防御的 DNS 服务器。

dns domain

使用 **dns domain** 命令配置域名黑名单条目。

命令

dns domain *domain_name* {**enable** | **disable**}

语法

domain_name	域名，格式为 WORD<1-255>。域名只能由英文字母、数字、连字符和点组成。
enable | **disable**	当 NetEye 检测到匹配的条目时的处理动作。 • enable— 阻断，表示断开服务器与客户端之间的连接。 • disable— 放行，表示不对数据通讯做任何处理，连接正常。

说明

1. 如果域名列表中不存在输入的域名，则表示添加；如果域名列表中存在输入的域名，则表示修改相应条目的处理动作。
2. 要配置域名黑名单条目，必须先启用域名黑名单功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 1. 为 profile test 添加域名为 sina.com 的域名黑名单条目，并阻断该条目。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns domain sina.com enable
```

范例 2. 为 profile test 修改域名黑名单的域名为 sina.com 的处理动作为放行。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns domain sina.com disable
```

相关命令

命令名称	描述信息
show profile dns domain	显示指定 profile 的域名黑名单的相关信息。
unset dns domain	删除指定域名黑名单条目。

dns domain enable, disable

使用 **dns domain enable, disable** 命令启用或禁用域名黑名单功能。

命令

dns domain {**enable** | **disable**}

语法

enable | **disable**	• enable— 启用域名黑名单 • disable— 禁用域名黑名单

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用域名黑名单功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns domain enable
```

相关命令

命令名称	描述信息
show profile dns domain	显示指定 profile 的域名黑名单的相关信息。

dns domain fuzzy

使用 **dns domain fuzzy** 命令启用或禁用指定域名黑名单条目的模糊匹配功能。

命令

dns domain *domain_name* **fuzzy** {**on** | **off**}

语法

domain_name	域名，格式为 WORD<1-255>。域名只能由英文字母、数字、连字符和点组成。

说明

要启用或禁用指定域名黑名单条目的模糊匹配功能，必须先启用该域名黑名单条目。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用域名黑名单中域名 sina.com 的模糊匹配功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns domain sina.com fuzzy on
```

相关命令

命令名称	描述信息
show profile dns domain	显示指定 profile 的域名黑名单的相关信息。

dns domain logging

使用 **dns domain logging** 命令开启或关闭域名黑名单的产生日志功能。

命令

dns domain logging {**on** | **off**}

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启域名黑名单的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns domain logging on
```

相关命令

命令名称	描述信息
show profile dns domain	显示指定 profile 的域名黑名单的相关信息。

dns protocol-anomaly action

使用 **dns protocol-anomaly action** 命令设置 DNS 协议异常检测相关功能的动作。

命令

dns protocol-anomaly [**traffic**] **action** {**block** | **allow**}

语法

traffic	表示检测非标准端口（非 53 端口）上的 DNS 流量。
block	**allow**	• block— 阻断，表示断开服务器与客户端之间的连接。 • allow— 放行，表示不对数据通讯做任何处理，连接正常。

说明

1. 如果不指定 **traffic** 关键字，表示检测格式和长度异常。
2. 要设置非标准端口上的 DNS 流量检测的动作，必须先启用非标准端口上的 DNS 流量检测功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置检测格式和长度异常的动作为放行。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns protocol-anomaly action allow
```

相关命令

命令名称	描述信息
show profile dns protocol-anomaly	显示指定 profile 的 DNS 协议异常检测的相关信息。

dns protocol-anomaly logging

使用 **dns protocol-anomaly logging** 命令开启或关闭 DNS 协议异常检测的产生日志功能。

命令

dns protocol-anomaly [**traffic**] **logging** {**on** | **off**}

语法

traffic	表示检测非标准端口（非 53 端口）上的 DNS 流量。

说明

1. 如果不指定 **traffic** 关键字，表示启用或禁用检测格式和长度异常的产生日志功能。
2. 要开启或关闭非标准端口上的 DNS 流量检测的产生日志功能，必须先启用非标准端口上的 DNS 流量检测功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启非标准端口上的 DNS 流量检测的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns protocol-anomaly traffic logging on
```

相关命令

命令名称	描述信息
show profile dns protocol-anomaly	显示指定 profile 的 DNS 协议异常检测的相关信息。

dns protocol-anomaly traffic

使用 **dns protocol-anomaly traffic** 命令启用或禁用非标准端口上的 DNS 流量检测功能。

命令

dns protocol-anomaly traffic {**enable** | **disable**}

语法

traffic	表示检测非标准端口（非 53 端口）上的 DNS 流量。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用非标准端口上的 DNS 流量检测功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns protocol-anomaly traffic enable
```

相关命令

命令名称	描述信息
show profile dns protocol-anomaly	显示指定 profile 的 DNS 协议异常检测的相关信息。

dns protocol-restriction

使用 **dns protocol-restriction** 命令添加 DNS 协议限制的授权 IP 地址。配置成功后，除了授权 IP 地址外，阻断 DNS 区域传输。

命令

dns protocol-restriction {**IP mask** *ip_address netmask* | **IP range** *ip_address_list* | **Object** *object_name*}

语法

ip_address	IP 地址，格式为 x.x.x.x。
netmask	子网掩码，格式为 x.x.x.x。
ip_address_list	IP 地址列表，格式为 IPV4LIST<1-32>。
object_name	IP 地址对象名称，格式为 WORD<1-63>。

说明

要添加 DNS 协议限制的授权 IP 地址，必须先启用区域传输限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 添加 DNS 协议限制的授权 IP 地址，地址对象为 ipobject1。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns protocol-restriction Object ipobject1
```

相关命令

命令名称	描述信息
show profile dns protocol-restriction	显示指定 profile 的 DNS 协议限制的相关信息。
unset dns protocol-restriction	删除 DNS 协议限制的授权 IP 地址。

dns protocol-restriction enable, disable

使用 **dns protocol-restriction enable, disable** 命令启用或禁用 DNS 协议限制功能。

命令

dns protocol-restriction {**enable** | **disable**}

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用 DNS 协议限制功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns protocol-restriction enable
```

相关命令

命令名称	描述信息
show profile dns protocol-restriction	显示指定 profile 的 DNS 协议限制的相关信息。

dns protocol-restriction logging

使用 **dns protocol-restriction logging** 命令开启或关闭 DNS 协议限制功能选项的产生日志功能。

命令

dns protocol-restriction {**resource** | **transfer**} **logging** {**on** | **off**}

语法

resource | **transfer**	• resource— 表示 UDP 资源记录数限制 • transfer— 表示区域传输限制

说明

要启用或禁用指定选项的产生日志功能，必须先启用相应选项功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启 UDP 资源记录数限制的产生日志功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns protocol-restriction resource logging on
```

相关命令

命令名称	描述信息
show profile dns protocol-restriction	显示指定 profileDNS 协议限制的相关信息。

dns protocol-restriction resource max

使用 **dns protocol-restriction resource max** 命令设置 UDP 资源相关的最大资源记录数。

命令

dns protocol-restriction resource max {**additional** | **answer** | **authority**} *num*

语法

additonal |answer | authority	• additional— 表示附加记录数 • answer— 表示回答记录数 • authority— 表示授权记录数
num	最大记录数，格式为 INTEGER<1-10>。

说明

要设置 UDP 资源相关的最大资源记录数，必须先启用相应的最大资源记录数限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置 UDP 资源的最大回答记录数为 4。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns protocol-restriction resource max answer 4
```

相关命令

命令名称	描述信息
show profile dns protocol-restriction	显示指定 profile 的 DNS 协议限制的相关信息。

dns protocol-restriction resource max action

使用 **dns protocol-restriction resource max action** 命令设置 UDP 资源相关的最大资源记录数限制的动作。

命令

dns protocol-restriction resource max {**additional** | **answer** | **authority**} **action** {**block** | **allow**}

语法

additonal |answer | authority	• additional— 表示附加记录数 • answer— 表示回答记录数 • authority— 表示授权记录数
block | allow	当检测到超过最大资源记录数时所采取的动作。 • block— 阻断，表示断开服务器与客户端之间的连接。 • allow—放行，表示不对数据通讯做任何处理，连接正常。

说明

要设置 UDP 资源相关的最大资源记录数限制的动作，必须先启用相应的最大资源记录数限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置 UDP 资源的最大回答记录数限制的动作为阻断。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns protocol-restriction resource max answer action block
```

相关命令

命令名称	描述信息
show profile dns protocol-restriction	显示指定 profile 的 DNS 协议限制的相关信息。

dns protocol-restriction resource max enable, disable

使用 **dns protocol-restriction resource max enable, disable** 命令启用或禁用 UDP 资源相关的的最大资源记录数限制功能。

命令

dns protocol-restriction resource max {**additional** | **answer** | **authority**} {**enable** | **disable**}

语法

additonal |answer | authority	• additional— 表示附加记录数 • answer— 表示回答记录数 • authority— 表示授权记录数

说明

要启用或禁用 UDP 资源相关的最大资源记录数限制功能，必须先启用 UDP 资源记录数限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用 UDP 资源的最大回答记录数限制功能。

```
NetEye@root-system]profile mode test

NetEye@root-system-pro-test]dns protocol-restriction resource max
answer enable
```

相关命令

命令名称	描述信息
show profile dns protocol-restriction	显示指定 profile 的 DNS 协议限制的相关信息。

dns protocol-restriction resource, transfer enable, disable

使用 **dns protocol-restriction resource, transfer enable, disable** 命令启用或禁用 UDP 资源记录数限制功能或区域传输限制功能。

命令

dns protocol-restriction {**resource** | **transfer**} {**enable** | **disable**}

语法

resource	**transfer**	• resource— 表示 UDP 资源记录数限制 • transfer— 表示区域传输限制

说明

要启用或禁用 UDP 资源记录数限制功能以及区域传输限制功能，必须先启用 DNS 协议限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用区域传输限制功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]dns protocol-restriction transfer enable
```

相关命令

命令名称	描述信息
show profile dns protocol-restriction	显示指定 profile 的 DNS 协议限制的相关信息。

dns server

使用 **dns server** 命令添加 DNS 服务器。

命令

dns server *server_name ip_address*

语法

server_name	DNS 服务器名称，格式为 WORD<1-15>。
ip_address	DNS 服务器的 IP 地址，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加 DNS 服务器 server1，服务器的 IP 地址为 10.4.6.2。

```
NetEye@root-system]dns server server1 10.4.6.2
```

相关命令

命令名称	描述信息
show dns server	显示 DNS 服务器列表。
unset dns server	删除 DNS 服务器。

dns server comments

使用 **dns server comments** 命令设置指定 DNS 服务器的备注信息。

命令

dns server *server_name* **comments** [*string*]

语法

server_name	DNS 服务器名称，格式为 WORD<1-15>。
string	备注信息，格式为 LINE。

说明

如果不指定 *string* 参数，则表示删除指定 DNS 服务器的备注信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 设置 DNS 服务器 server1 的备注信息为 This is a dns server。

```
NetEye@root-system]dns server server1 comments This is a dns server
```

相关命令

命令名称	描述信息
dns server	添加 DNS 服务器。
show dns server	显示 DNS 服务器列表。
unset dns server	删除 DNS 服务器。

dns server enable, disable

使用 **dns server enable, disable** 命令设置指定 DNS 服务器的授权地址。

命令

dns server *server_name* {**domain** *domain_name* | **IP mask** *ip_address netmask* | **IP range** *ip_address_list*} {**enable** | **disable**}

语法

server_name	DNS 服务器名称，格式为 WORD<1-15>。
domain_name	域名，格式为 WORD<1-255>。
ip_address	IP 地址，格式为 x.x.x.x。
netmask	子网掩码，格式为 x.x.x.x。
ip_address_list	IP 地址列表，格式为 IPV4LIST<1-32>。
enable | **disable**	• enable— 放行，表示不对数据通讯做任何处理，连接正常。 • disable— 阻断，表示断开服务器与客户端之间的连接。

说明

如果授权列表中不存在输入的授权域名或授权 IP 地址，则表示添加；如果授权列表中存在输入的授权域名或授权 IP 地址，则表示修改相应条目的状态。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 1. 为 DNS 服务器 server1 添加域名为 sina.com 的授权域名，并启用该域名。

```
NetEye@root-system]dns server server1 domain sina.com enable
```

范例 2. 为 DNS 服务器 server1 修改授权域名为 sina.com 的状态为禁用。

```
NetEye@root-system]dns server server1 domain sina.com disable
```

相关命令

命令名称	描述信息
dns server	添加 DNS 服务器。
dns server IP address	修改指定 DNS 服务器的 IP 地址。
show dns server	显示 DNS 服务器列表。
unset dns server	删除 DNS 服务器。
unset dns server domain, IP	删除指定 DNS 服务器的相关配置。

dns server IP address

使用 **dns server IP address** 命令修改指定 DNS 服务器的 IP 地址。

命令

dns server *server_name* **IP address** *ip_address*

语法

server_name	DNS 服务器名称，格式为 WORD<1-15>。
ip_address	IP 地址，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 修改 DNS 服务器 server1 的 IP 地址，地址为 10.4.3.2。

```
NetEye@root-system]dns server server1 IP address 10.4.3.2
```

相关命令

命令名称	描述信息
dns server	添加 DNS 服务器。
show dns server	显示 DNS 服务器列表。
unset dns server	删除 DNS 服务器。

show dns server

使用 **show dns server** 命令显示 DNS 服务器列表。

命令

show dns server [*server_name* {**domain** | **IP**}]

语法

server_name	DNS 服务器名称，格式为 WORD<1-15>。
domain | **IP**	• domain— 表示显示授权域名 • IP— 表示显示授权 IP 地址

说明

如果指定 *server_name* 参数，表示显示指定 DNS 服务器的授权域名或授权 IP 地址。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 DNS 服务器列表。

```
NetEye@root>show dns server
```

【返回结果】

```
Name                IP Address      Comments
a                   1.1.1.1
```

相关命令

命令名称	描述信息
dns server	添加 DNS 服务器。
dns server comments	设置指定 DNS 服务器的备注信息。
dns server enable, disable	设置指定 DNS 服务器的授权地址。
dns server IP address	修改 DNS 服务器的 IP 地址。

命令名称	描述信息
unset dns server	删除 DNS 服务器。
unset dns server domain, IP	删除指定 DNS 服务器的相关配置。

show profile dns cache_defense

使用 **show profile dns cache_defense** 命令显示指定 profile 的缓存中毒防御功能的相关信息。

命令

show profile *profile_name* **dns cache_defense**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的缓存中毒防御功能的相关信息。

```
NetEye@root>show profile test dns cache_defense
```

【返回结果】

```
Enable DNS Scrambling                   State:enable        Logging:on
       Enable ID Scrambling             State:enable
       Apply to the embedded DNS proxy  State:enable

Drop Inbound Requests                   State:enable        Logging:on
       Apply to the embedded DNS proxy  State:enable

Detect Frequent Mismatched Replies      State:enable        Logging:on
       MAX Number of Mismatched Replies:50
       Within an Interval of:           5 Seconds
```

相关命令

命令名称	描述信息
dns cache_defense enable, disable	启用或禁用缓存中毒防御功能。
dns cache_defense dns_scrambling enable, disable	启用或禁用 DNS 不规则化的相关功能。
dns cache_defense drop enable, disable	启用或禁用外部请求限制的相关功能。
dns cache_defense logging	开启或关闭缓存中毒防御功能选项的产生日志功能。
dns cache_defense mismatched_replies	设置常不匹配的应答检测功能的相关参数。
dns cache_defense mismatched_replies enable, disable	启用或禁用常不匹配的应答检测功能。

show profile dns cache_defense drop zones

使用 **show profile dns cache_defense drop zones** 命令显示指定 profile 的外部请求安全域的相关信息。

命令

show profile *profile_name* **dns cache_defense drop zones**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的外部请求安全域的相关信息。

```
NetEye@root>show profile test dns cache_defense drop zones
```

【返回结果】

```
Selecte   Zone
Disable   zone2
Enable    zone1
```

相关命令

命令名称	描述信息
dns cache_defense enable, disable	启用或禁用缓存中毒防御功能。
dns cache_defense drop enable, disable	启用或禁用外部请求限制的相关功能。

show profile dns cache_defense select dns server

使用 **show profile dns cache_defense select dns server** 命令显示指定 profile 的进行缓存中毒防御的 DNS 服务器。

命令

show profile *profile_name* **dns cache_defense** {**dns_scrambling** | **drop**} **select dns server**

语法

profile_name	profile 名称，格式为 WORD<1-10>。
dns_scrambling | drop	• dns_scrambling— 表示 DNS 不规则化 • drop— 表示外部请求限制

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的进行外部请求限制功能的 DNS 服务器。

```
NetEye@root>show profile test dns cache_defense drop select dns server
```

【返回结果】

```
Profile: test
Selecte      DNS Servers
Enable       server1
Disable      server2
```

相关命令

命令名称	描述信息
dns cache_defense enable, disable	启用或禁用缓存中毒防御功能。
dns cache_defense dns_scrambling enable, disable	启用或禁用 DNS 不规则化的相关功能。

命令名称	描述信息
dns cache_defense drop enable, disable	启用或禁用外部请求限制的相关功能。
dns cache_defense select dns server	启用或禁用进行缓存中毒防御的 DNS 服务器。

show profile dns domain

使用 **show profile dns domain** 命令显示指定 profile 的域名黑名单的相关信息。

命令

show profile *profile_name* **dns domain**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的域名黑名单的相关信息。

```
NetEye@root>show profile test dns domain
```

【返回结果】

```
Domain Blacklist State: Enable
Logging: on
State    Fuzzy Matching  Domain Name
Enable   off             sina.com
Enable   on              blog
```

相关命令

命令名称	描述信息
dns domain	配置域名黑名单条目。
dns domain enable, disable	启用或禁用域名黑名单功能。
dns domain fuzzy	启用或禁用指定域名黑名单条目的模糊匹配功能。
dns domain logging	开启或关闭域名黑名单的产生日志功能。
unset dns domain	删除指定域名黑名单条目。

show profile dns protocol-anomaly

使用 **show profile dns protocol-anomaly** 命令显示指定 profile 的 DNS 协议异常检测的相关信息。

命令

show profile *profile_name* **dns protocol-anomaly**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的 DNS 协议异常检测的相关信息。

```
NetEye@root>show profile test dns protocol-anomaly
```

【返回结果】

```
Profile: test
       Detect format and length anomalies.                  Action: Allow
Logging: on
Enable  Detect DNS traffic on non-standard (non-53) ports:     Action: Allow
Logging: on
```

相关命令

命令名称	描述信息
dns protocol-anomaly action	设置 DNS 协议异常检测相关功能的动作。
dns protocol-anomaly logging	开启或关闭 DNS 协议异常检测的产生日志功能。
dns protocol-anomaly traffic	启用或禁用非标准端口上的 DNS 流量检测功能。

show profile dns protocol-restriction

使用 **show profile dns protocol-restriction** 命令显示指定 profile 的 DNS 协议限制的相关信息。

命令

show profile *profile_name* **dns protocol-restriction** [**resource** | **transfer**]

语法

profile_name	profile 名称，格式为 WORD<1-10>。
resource | transfer	• resource— 表示 UDP 资源记录数限制 • transfer— 表示区域传输限制

说明

如果不指定 **resource** 或 **transfer** 关键字，则表示显示 DNS 协议限制的所有相关信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的 UDP 资源记录数的相关信息。

```
NetEye@root>show profile test dns protocol-restriction resource
```

【返回结果】

```
State     Name                              Number  Action
Enable    MAX Number of Answer Records      4       Allow
Enable    MAX Number of Authority Records   4       Allow
Enable    MAX Number of Additional Records  4       Allow
```

相关命令

命令名称	描述信息
dns protocol-restriction	添加 DNS 协议限制的授权 IP 地址。
dns protocol-restriction enable, disable	启用或禁用 DNS 协议限制功能。

命令名称	描述信息
dns protocol-restriction logging	开启或关闭 DNS 协议限制功能选项的产生日志功能。
dns protocol-restriction resource max	设置 UDP 资源相关的最大资源记录数。
dns protocol-restriction resource max action	设置 TCP 资源相关的最大资源记录数限制的动作。
dns protocol-restriction resource max enable, disable	启用或禁用 UDP 资源相关的最大资源记录数限制功能。
dns protocol-restriction resource, transfer enable, disable	启用或禁用 UDP 资源记录数限制功能或区域传输限制功能。
show profile dns protocol-restriction	显示指定 profile 的 DNS 协议限制的相关信息。
unset dns protocol-restriction	删除 DNS 协议限制的授权 IP 地址。

unset dns domain

使用 **unset dns domain** 命令删除指定域名黑名单条目。

命令

unset dns domain *domain_name*

语法

domain_name	域名，格式为 WORD<1-255>。

说明

要删除域名黑名单的条目，必须先启用域名黑名单功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 删除 profile test 的域名为 blog 的域名黑名单条目。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]unset dns domain blog
```

相关命令

命令名称	描述信息
dns domain	配置域名黑名单条目。
show profile dns domain	显示指定 profile 的域名黑名单的相关信息。

unset dns protocol-restriction

使用 **unset dns protocol-restriction** 命令删除 DNS 协议限制的授权 IP 地址。

命令

unset dns protocol-restriction {**IP mask** *ip_address netmask* | **IP range** *ip_address_list*| **Object** *object_name*}

语法

ip_address	授权 IP 地址，格式为 x.x.x.x。
netmask	子网掩码，格式为 x.x.x.x。
ip_address_list	IP 地址列表，格式为 IPV4LIST<1-32>。
object_name	IP 地址对象名称，格式为 WORD<1-63>。

说明

要删除 DNS 协议限制的授权 IP 地址，必须先启用 DNS 协议限制功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 删除 profile test 的 DNS 协议限制的 IP 地址对象 ipobject1。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]unset dns protocol-restriction Object ipobject1
```

相关命令

命令名称	描述信息
dns protocol-restriction	添加 DNS 协议限制的授权 IP 地址。
show profile dns protocol-restriction	显示指定 profile 的 DNS 协议限制的相关信息。

unset dns server

使用 **unset dns server** 命令删除 DNS 服务器。

命令

unset dns server [*server_name*]

语法

server_name	DNS 服务器名称，格式为 WORD<1-15>。

说明

如果不指定 *server_name* 参数，则表示删除所有 DNS 服务器。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除 DNS 服务器 server1。

```
NetEye@root-system]unset dns server server1
```

相关命令

命令名称	描述信息
dns server	添加 DNS 服务器。
show dns server	显示 DNS 服务器列表。
unset dns server domain, IP	删除指定 DNS 服务器的相关配置。

unset dns server domain, IP

使用 **unset dns server domain, IP** 命令删除指定 DNS 服务器的相关配置。

命令

unset dns server *server_name* {**domain** *domain_name* | **IP mask** *ip_address netmask* | **IP range** *ip_address_list*}

语法

server_name	DNS 服务器名称，格式为 WORD<1-15>。
domain_name	授权域名，格式为 WORD<1-255>。
ip_address	授权 IP 地址，格式为 x.x.x.x。
netmask	子网掩码，格式为 x.x.x.x。
ip_address_list	IP 地址列表，格式为 IPV4LIST<1-32>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除 DNS 服务器 server1 的域名 sina.com。

```
NetEye@root-system]unset dns server server1 domain sina.com
```

相关命令

命令名称	描述信息
dns server	添加 DNS 服务器。
show dns server	显示 DNS 服务器列表。
unset dns server	删除 DNS 服务器。

Telnet 检测

show profile telnet command-filtering terminals

使用 **show profile telnet command-filtering terminals** 命令显示指定 profile 的终端 Telnet 流量检测状态。

命令

show profile *profile_name* **telnet command-filtering terminals**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的终端 Telnet 流量检测状态。

```
NetEye@root>show profile test telnet command-filtering terminals
```

【返回结果】

```
Terminals:
 Command Filtering: Disable
 ANSI: Disable
 XTERM: Enable
 VT100: Disable
 VT52: Disable
```

相关命令

命令名称	描述信息
telnet command-filtering terminal	开启或关闭指定终端的 Telnet 流量检测功能。

show profile telnet command-filtering user-defined

使用 **show profile telnet command-filtering user-defined** 命令显示指定 profile 的用户自定义命令阻断配置信息。

命令

show profile *profile_name* **telnet command-filtering user-defined**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的用户自定义命令阻断配置信息。

```
NetEye@root>show profile test telnet command-filtering user-defined
```

【返回结果】

```
Block User Defined Commands:
Log: On
 ---------------------------------
State       Command
Disable
Enable       ping
```

相关命令

命令名称	描述信息
telnet command-filtering user-defined	设置用户自定义命令。
unset telnet command-filtering user-defined	删除用户自定义命令。

telnet command-filtering on, off

使用 **telnet command-filtering on, off** 命令开启或关闭 Telnet 命令过滤功能。

命令

telnet command-filtering {**on** | **off**}

语法

on | **off**	• on—开启 Telnet 命令过滤功能 • off—关闭 Telnet 命令过滤功能 缺省设置为 off

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启 telnet 命令过滤功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]telnet command-filtering on
```

相关命令

命令名称	描述信息
show profile telnet command-filtering user-defined	显示指定 profile 的用户自定义命令阻断配置信息。

telnet command-filtering terminal

使用 **telnet command-filtering terminal** 命令开启或关闭指定终端的 Telnet 流量监测功能。

命令

telnet command-filtering terminal {**ANSI** | **XTERM** | **VT100** | **VT52**} {**on** | **off**}

语法

on | **off**	• on—开启指定终端的 Telnet 流量监测功能 • off—关闭指定终端的 Telnet 流量监测功能 缺省值为 off

说明

要开启或关闭指定终端的 Telnet 流量检测功能，必须先开启 Telnet 命令过滤功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启 Xterm 终端的 Telnet 流量检测功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]telnet command-filtering terminal XTERM on
```

相关命令

命令名称	描述信息
show profile telnet command-filtering terminals	显示指定 profile 的终端 Telnet 流量检测状态。

telnet command-filtering user-defined

使用 **telnet command-filtering user-defined** 命令设置用户自定义命令。

命令

telnet command-filtering user-defined *command* {**enable** | **disable**}

语法

command	用户自定义命令，格式为 WORD<1-64>。
enable | **disable**	• enable—启用阻断功能 • disable—禁用阻断功能

说明

1. 要添加用户自定义命令，必须先开启 Telnet 命令过滤功能。
2. 如果列表中不存在与输入的参数匹配的条目，则表示添加；如果存在匹配的条目，则表示修改相应条目的状态。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 添加用户自定义命令 Ping，并阻断该自定义命令。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]telnet command-filtering user-defined ping enable
```

相关命令

命令名称	描述信息
show profile telnet command-filtering user-defined	显示指定 profile 的用户自定义命令阻断配置信息。
unset telnet command-filtering user-defined	删除用户自定义命令。

telnet command-filtering user-defined log

使用 **telnet command-filtering user-defined log** 命令开启或关闭阻断用户自定义命令的日志记录功能。

命令

telnet command-filtering user-defined log {**on** | **off**}

语法

on | **off**	• on—开启日志记录功能 • off—关闭日志记录功能 缺省值为 off

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 开启阻断用户自定义命令的日志记录功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]telnet command-filtering user-defined log on
```

相关命令

命令名称	描述信息
show profile telnet command-filtering user-defined	显示指定 profile 的用户自定义命令阻断配置信息。

unset telnet command-filtering user-defined

使用 **unset telnet command-filtering user-defined** 命令删除用户自定义命令。

命令

unset telnet command-filtering user-defined *command*

语法

command	用户自定义命令，格式为 WORD<1-64>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 删除用户自定义命令 ping。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]unset telnet command-filtering user-defined ping
```

相关命令

命令名称	描述信息
show profile telnet command-filtering user-defined	显示指定 profile 的用户自定义命令阻断配置信息。
telnet command-filtering user-defined	设置用户自定义命令。

MSN Messenger 检测

msn block

使用 **msn block** 命令启用或禁用 MSN Messenger 特定功能的应用限制。

命令

msn block {**file-transfer** | **application-share** | **white-board** | **remote-assistant** | **video** | **audio** | **windows-live-advanced-setting**} {**enable** | **disable**}

语法

file-transfer | **application-share** | **white-board** | **remote-assistant** | **video** | **audio** | **windows-live-advanced-setting**	• file-transfer—表示 MSN Messenger 的文件传输功能 • application-share—表示 MSN Messenger 的应用共享功能 • white-board—表示 MSN Messenger 的白板功能 • remote-assistant—表示 MSN Messenger 的远程协助功能 • video—表示 MSN Messenger 的视频功能 • audio—表示 MSN Messenger 的音频功能 • windows-live-advanced-setting—表示MSN Live Messenger的视频、音频和文件传输功能
enable | **disable**	• enable—启用 MSN Messenger 特定功能的应用限制 • disable—禁用 MSN Messenger 特定功能的应用限制 缺省设置为 enable

说明

要启用或禁用 MSN Messenger 特定功能的应用限制，必须先启用 MSN Messenger 的流量检测功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 禁用 MSN Messenger 的文件传输限制。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]msn block file-transfer disable
```

相关命令

命令名称	描述信息
show profile msn	显示指定 profile 的 MSN Messenger 应用限制配置信息。

msn inspect enable, disable

使用 **msn inspect enable, disable** 命令启用或禁用 MSN Messenger 的流量检测功能。

命令

msn inspect {**enable** | **disable**}

语法

enable | **disable**	• enable—启用 MSN Messenger 的流量检测功能 • disable—禁用 MSN Messenger 的流量检测功能 缺省设置为 enable

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 禁用 MSN Messenger 的流量检测功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]msn inspect disable
```

相关命令

命令名称	描述信息
show profile msn	显示指定 profile 的 MSN Messenger 应用限制配置信息。

msn inspect log

使用 **msn inspect log** 命令开启或关闭 MSN Messenger 的日志记录功能。

命令

msn inspect log {**on** | **off**}

语法

on | **off**	• on—开启 MSN Messenger 的日志记录功能 • off—关闭 MSN Messenger 的日志记录功能 缺省设置为 on

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 关闭 MSN Messenger 的日志记录功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]msn inspect log off
```

相关命令

命令名称	描述信息
show profile msn	显示指定 profile 的 MSN Messenger 应用限制配置信息。

show profile msn

使用 **show profile msn** 显示指定 profile 的 MSN Messenger 应用限制配置信息。

命令

show profile *profile_name* **msn**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的 MSN Messenger 应用限制配置信息。

```
NetEye@root>show profile test msn
```

【返回结果】

```
Inspect MSN Messenger traffic : Enable
Log : On
Block file transfer : Enable
Block application sharing : Enable
Block white board : Enable
Block remote assistant : Enable
Block vedio : Enable
Block audio : Enable
Block vedio,audio and file transfer of MSN Live Messengers : Enable
```

相关命令

命令名称	描述信息
msn block	启用或禁用 MSN Messenger 特定功能的应用限制。
msn inspect enable, disable	启用或禁用 MSN Messenger 的流量检测功能。
msn inspect log	开启或关闭 MSN Messenger 的日志记录功能。

TCP 检测

show profile tcp

使用 **show profile tcp** 命令显示指定 profile 的 TCP 协议限制配置信息。

命令

show profile *profile_name* **tcp**

语法

profile_name	profile 名称，格式为 WORD<1-10>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示 profile test 的 TCP 协议限制配置信息。

```
NetEye@root>show profile test tcp
```

【返回结果】

```
Protocol Restriction:  Disable
----------------------------------
Verify TCP sequence numbers: Disable        Log: Off
Track on all out of state packets.
Verify TCP Checksums: Enable        Log: On
Pass  packets with invalid checksum.
```

相关命令

命令名称	描述信息
tcp checksum	启用或禁用带有非法校验和的数据包的探测功能。
tcp sequence track	设置 TCP 序列号检验功能。

tcp checksum

使用 **tcp checksum** 命令启用或禁用带有非法校验和的数据包的探测功能。

命令

tcp checksum log {**on** | **off**}

语法

on | **off**	• on—启用带有非法校验和的数据包的探测功能 • off—禁用带有非法校验和的数据包的探测功能 缺设置为 off

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 启用带有非法校验和的数据包的探测功能。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]tcp checksum log on
```

相关命令

命令名称	描述信息
show profile tcp	显示指定 profile 的 TCP 协议限制配置信息。

tcp sequence track

使用 **tcp sequence track** 命令设置 TCP 序列号检验功能。

命令

tcp sequence track {**none** | **all** | **anomalous** | **suspicious**}

语法

none | **all** | **anomalous** | **suspicious**	• none—指不对数据包进行检验。 • all—指对所有数据包进行不符合连接状态探测。 • anomalous—指对异常数据包进行不符合连接状态探测。 • suspicious—指对可疑数据包进行不符合连接状态探测。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在 Profile 配置模式下使用。

范例

范例 . 为 profile test 设置 TCP 序列号检验功能，探测所有不符合连接状态的数据包。

```
NetEye@root-system]profile mode test
NetEye@root-system-pro-test]tcp sequence track all
```

相关命令

命令名称	描述信息
show profile tcp	显示指定 profile 的 TCP 协议限制配置信息。

16 虚拟系统命令

description

使用 **description** 命令为虚拟系统 （Vsys）设置描述信息。

命令

description [*string*]

语法

string	备注信息，格式为 LINE。

说明

如果不指定 *string* 参数，表示设置虚拟系统的描述信息为空。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 Vsys 配置模式下使用。

范例

范例 . 为虚拟系统 vsys2 设置备注信息为：hello,this is vsys2!

```
NetEye@root-system]vsys 2
NetEye@root-system-vsys2]description hello,this is vsys2!
```

hold vlan, channel, ethernet, rint, veth, pppoe

使用 **hold vlan, channel, ethernet, rint, veth, pppoe** 命令将指定的三层接口添加到虚拟系统中。

命令

hold {**vlan** *vlan_id* | **channel** *channel_id* | **ethernet** *ethernet_id* | **rint** *redundant_id* | **veth** *vethernet_id* | **pppoe** *pppoe_id*}

语法

vlan_id	VLAN ID 列表，格式为 NUMBER。
channel_id	以太网通道 ID 列表，格式为 NUMBER。
ethernet_id	以太网接口 ID 或名称，格式为 WORD<1-10>。 例如：1 或 eth1。
redundant_id	冗余接口 ID 列表，格式为 NUMBER。
vethernet_id	虚拟接口 ID 列表，格式为 NUMBER。
pppoe_id	PPPoE 接口 ID 列表，格式为 NUMBER。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 Vsys 配置模式下使用。

范例

范例 . 添加接口 vlan2， vlan3， vlan5 到 vlan10， rint1 到虚拟系统 vsys1。

```
NetEye@root-system]vsys 1
NetEye@root-system-vsys1]hold vlan 2,3,5-10
NetEye@root-system-vsys1]hold rint 1
```

相关命令

命令名称	描述信息
unset hold vlan, channel, ethernet, rint, veth, pppoe	从虚拟系统中删除指定的三层接口。

manage-ip-address

使用 **manage-ip-address** 命令为虚拟系统在指定的三层接口上配置管理 IP 地址。

命令

manage-ip-address *ip_address netmask* {**vlan** *vlan_id* | **channel** *channel_id* | **ethernet** *ethernet_id* | **redundant** *redundant_id* | **vethernet** *vethernet_id* | **pppoe** *pppoe_id*}

语法

ip_address	IP 地址，格式为 x.x.x.x。
netmask	子网掩码，格式为 x.x.x.x。
vlan_id	VLAN ID，格式为 INTEGER<1-1023>。
channel_id	以太网通道 ID，格式为 INTEGER<0-7>。
ethernet_id	以太网接口 ID 或名称，格式为 WORD<1-10>。
redundant_id	冗余接口 ID，格式为 INTEGER<1-4>。
vethernet_id	虚拟接口 ID，格式为 INTEGER<1-1023>。
pppoe_id	PPPoE 接口 ID，格式为 INTEGER<0-7>。

说明

每个虚拟系统只能添加一个管理 IP 地址，且添加后不能删除，只能修改。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 Vsys 配置模式下使用。

范例

范例 . 为虚拟系统 vsys1 在 vlan1 接口上配置管理 IP 地址为 192.168.1.111 及子网掩码 255.255.255.0。

```
NetEye@root-system]vsys 1
NetEye@root-system-vsys1]manage-ip-address 192.168.1.111 255.255.255.0
vlan 1
```

show vsys

使用 **show vsys** 命令显示虚拟系统的相关信息。

命令

show vsys [*vsys_id* | **root**]

语法

vsys_id	Vsys 标识，格式为 INTEGER<1-255>。
root	根 Vsys。

说明

如果不指定 *vsys_id* 参数和 **root** 关键字，将显示所有虚拟系统的信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V			

模式

该命令在普通配置模式下使用。

范例

范例 . 显示虚拟系统 vsys1 的相关所有信息。

```
NetEye@root>show vsys 1
```

【返回结果】

```
Vsys vsys1 is enable,3% resource occupy
MaxLinkNumber: 30000
Description:
```

switch vsys

使用 **switch vsys** 命令切换虚拟系统。

命令

switch vsys *vsys_name*

语法

vsys_name	Vsys 名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在普通配置模式下使用。

范例

范例 . 切换到虚拟系统 vsys1。

```
NetEye@root>switch vsys vsys1
```

unset hold vlan, channel, ethernet, rint, veth, pppoe

使用 **unset hold vlan, channel, ethernet, rint, veth, pppoe** 命令从虚拟系统中删除指定的三层接口。

命令

unset hold {**ethernet** *ethernet_id* | **channel** *channel_id* | **vlan** *vlan_id* | **rint** *redundant_id* | **veth** *vethernet_id* | **pppoe** *pppoe_id*}

语法

vlan_id	VLAN ID 列表，格式为 NUMBER。
channel_id	以太网通道 ID 列表，格式为 NUMBER。
ethernet_id	以太网接口 ID 或名称，格式为 WORD<1-10>。 例如：1 或 eth1。
redundant_id	冗余接口 ID 列表，格式为 NUMBER。
vethernet_id	虚拟接口 ID 列表，格式为 NUMBER。
pppoe_id	PPPoE 接口 ID 列表，格式为 NUMBER。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在 Vsys 配置模式下使用。

范例

范例 . 将 vlan2， vlan3， vlan5 到 vlan10， rint1 从虚拟系统 vsys1 中删除。

```
NetEye@root-system]vsys 1
NetEye@root-system-vsys1]unset hold vlan 2,3,5-10
NetEye@root-system-vsys1]unset hold rint 1
```

相关命令

命令名称	描述信息
hold vlan, channel, ethernet, rint, veth, pppoe	将指定的三层接口添加到虚拟系统中。

unset vsys

使用 **unset vsys** 命令删除一个已存在的虚拟系统。

命令

unset vsys *vsys_id*

语法

vsys_id	Vsys 标识，格式为 INTEGER<1-255>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 删除虚拟系统 vsys1。

```
NetEye@root-system]vsys 1
NetEye@root-system]unset vsys 1
```

相关命令

命令名称	描述信息
vsys	进入 Vsys 配置模式。
vsys resource-limit	添加一个 Vsys 并为其分配最大资源百分比。

vsys

使用 **vsys** 命令进入指定 Vsys 配置模式。

命令

vsys {*vsys_id* | **root**}

语法

vsys_id	Vsys 标识，格式为 INTEGER<1-255>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 进入虚拟系统 vsys1 配置模式。

```
NetEye@root-system]vsys 1
```

相关命令

命令名称	描述信息
unset vsys	删除一个 Vsys。
vsys resource-limit	添加一个 Vsys 并为其分配最大资源百分比。

vsys enable, disable

使用 **vsys enable, disable** 命令启用或者禁用指定虚拟系统。

命令

vsys *vsys_id* {**enable** | **disable**}

语法

vsys_id	Vsys 标识，格式为 INTEGER<1-255>。
enable | **disable**	• enable— 启用指定虚拟系统 • disable— 禁用指定虚拟系统 缺省值为 enable

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 启用虚拟系统 vsys1。

```
NetEye@root-system]vsys 1 enable
```

vsys resource-limit

使用 **vsys resource-limit** 命令添加一个虚拟系统并为其分配最大资源百分比。

命令

vsys *vsys_id* **resource-limit** *num*

语法

vsys_id	Vsys 标识，格式为 INTEGER<1-255>。
resource-limit	为 Vsys 分配最大资源。
num	Vsys 最大资源百分比，格式为 INTEGER<1-100>。

说明

1. 当指定的 Vsys 已经存在时，该命令会修改 Vsys 的最大资源百分比。
2. 添加的 Vsys 缺省状态为 “启用”。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 创建虚拟系统 vsys1 并为其分配最大 50% 的系统资源。

```
NetEye@root-system]vsys 1 resource-limit 50
```

相关命令

命令名称	描述信息
unset vsys	删除一个 Vsys。
vsys	进入 Vsys 配置模式。

17 高可用性命令

虚拟路由器

auth enable, disable

使用 **auth enable, disable** 命令启用或禁用同一 VRRP 组内虚拟路由器成员间的认证。

命令

auth {**enable password** *auth_key* | **disable**}

语法

enable | disable	• enable— 启用认证 • disable— 禁用认证 缺省设置为 disable
auth_key	认证密钥，格式为 WORD<1-8>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器配置模式下使用。

范例

范例 . 启用虚拟路由器认证，并设置认证密钥为 abcdef。

```
NetEye@root-system]virtual router 1
NetEye@root-system-vr1]auth enable password abcdef
```

相关命令

命令名称	描述信息
show virtual-router	显示虚拟路由器的配置信息。

backup ip

使用 **backup ip** 命令添加虚拟路由器的备份 IP 地址。

命令

backup ip address *ip_address* **mask** *netmask*

语法

ip_address	IP 地址，格式为 x.x.x.x。
netmask	子网掩码，格式为 x.x.x.x。

说明

同一 VRRP 组内各虚拟路由器成员的备份 IP 地址必须一致。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器配置模式下使用。

范例

范例 . 添加虚拟路由器 vr1 的备份 IP 地址 10.3.1.23。

```
NetEye@root-system]virtual router 1
NetEye@root-system-vr1]backup ip address 10.3.1.23 mask 255.255.255.255
```

相关命令

命令名称	描述信息
show virtual-router	显示虚拟路由器的配置信息。
unset backup ip	删除虚拟路由器的备份 IP 地址。

description

使用 **description** 命令设置虚拟路由器的备注信息。

命令

description [*string*]

语法

string	备注信息，格式为 LINE。

说明

如果指定 *string* 参数，则表示添加或修改备注信息，否则表示删除备注信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器配置模式下使用。

范例

范例 . 设置虚拟路由器 vr1 的备注信息为 This is virtual router 1。

```
NetEye@root-system]virtual router 1
NetEye@root-system-vr1]description This is virtual router 1
```

相关命令

命令名称	描述信息
show virtual-router	显示虚拟路由器的配置信息。

election interface

使用 **election interface** 命令设置虚拟路由器的选举接口 （即通信接口）。

命令

election interface *interface_name*

语法

interface_name	接口名称，格式为 WORD<1-15>。

说明

具有三层属性的接口，包括三层接口、 Vlan 接口、三层共享接口和三层 Channel 接口可以作为虚拟路由器的选举接口使用。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器配置模式下使用。

范例

范例 . 设置虚拟路由器 vr1 的选举接口为 eth1。

```
NetEye@root-system]virtual router 1
NetEye@root-system-vr1]election interface eth1
```

相关命令

命令名称	描述信息
show virtual-router	显示虚拟路由器的配置信息。
unset election interface	删除虚拟路由器的选举接口。

interval

使用 **interval** 命令设置 VRRP 组内主虚拟路由器向备份虚拟路由器发送报文的通告周期。

命令

interval *interval_value*

语法

interval _value	通告周期，单位为秒，格式为 INTEGER<1-60>。 缺省值为 1

说明

1. 同一个 VRRP 组内各虚拟路由器的通告周期必须一致。
2. 如果虚拟路由器加入到某一虚拟路由器探测组中，则其通告周期属性将被虚拟路由器探测组的通告周期属性所替换。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器配置模式下使用。

范例

范例 . 设置 VRRP 组内主虚拟路由器向备份虚拟路由器发送报文的通告周期为 3 秒。

```
NetEye@root-system]virtual router 1
NetEye@root-system-vr1]interval 3
```

相关命令

命令名称	描述信息
show virtual-router	显示虚拟路由器的配置信息。

ip-track

使用 **ip-track** 命令设置虚拟路由器的 IP 探测。

命令

ip-track type {**tcp-ping interface** *interface_name* **ip** *track_address* **port** *track_port* | {**arp-ping** | **ping**} **interface** *interface_name* **ip** *track_address*} **interval** *interval_value* **threshold** *threshold_value* **weight** *weight_value*

语法

tcp-ping | **arp-ping** | **ping**	• tcp-ping—TCP ping 方式 • arp-ping—ARP ping 方式 • ping—ICMP ping 方式
interface_name	接口名称，格式为 WORD<1-15>。
track_address	探测 IP 地址，格式为 x.x.x.x。
track_port	探测端口，格式为 INTEGER<1-65535>。
interval_value	探测周期，单位为秒，格式为 INTEGER<1-60>。
threshold_value	探测重试次数，格式为 INTEGER<1-999>。
weight_value	权重，格式为 INTEGER<1-254>。

说明

1. 如果探测 IP 地址不可达，则虚拟路由器的优先级将被减去权重值。
2. 如果虚拟路由器加入到某一虚拟路由器探测组中，则其 IP 探测属性将被虚拟路由器探测组的 IP 探测属性所替换。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器配置模式下使用。

范例

范例 . 在虚拟路由器 vr1 中，设置 ICMP ping 探测方式，从接口 eth0 探测 IP 地址 202.107.117.18 是否可达，同时设置探测周期为 5 秒，探测重试次数为 20，权重为 5。

```
NetEye@root-system]virtual router 1
```

```
NetEye@root-system-vrl]ip-track type ping interface eth0 ip
202.107.117.18 interval 5 threshold 20 weight 5
```

相关命令

命令名称	描述信息
unset ip-track	删除虚拟路由器的 IP 探测方式。

priority

使用 **priority** 命令设置虚拟路由器在 VRRP 组内的优先级。

命令

priority *pri*

语法

pri	优先级，格式为 INTEGER<1-254>。 缺省值为 100

说明

1. 如果虚拟路由器加入到某一虚拟路由器探测组中，则其优先级属性将被虚拟路由器探测组的优先级属性所替换。
2. 如果虚拟路由器选举接口的 IP 地址是 VRRP 组备份的 IP 地址，则该虚拟路由器在 VRRP 组内的优先级为 255，且不可被编辑。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器配置模式下使用。

范例

范例 . 设置虚拟路由器 vr1 的优先级为 120。

```
NetEye@root-system]virtual router 1
NetEye@root-system-vr1]priority 120
```

相关命令

命令名称	描述信息
show virtual-router	显示虚拟路由器的配置信息。

preempt enable, disable

使用 **preempt enable, disable** 命令启用或禁用虚拟路由器的抢占模式。

命令

preempt {**enable** | **disable**}

语法

enable | disable	• enable—启用抢占模式 • disable—禁用抢占模式 缺省设置为 enable

说明

1. 只有开启抢占模式，当 VRRP 组内备份虚拟路由器的优先级大于当前主虚拟路由器时，才会发生主备切换，否则不发生切换。
2. 如果虚拟路由器加入到某一虚拟路由器探测组中，则其抢占模式属性将被虚拟路由器探测组的抢占模式属性所替换。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器配置模式下使用。

范例

范例 . 启用虚拟路由器 vr1 的抢占模式。

```
NetEye@root-system]virtual router 1
NetEye@root-system-vr1]preempt enable
```

相关命令

命令名称	描述信息
show virtual-router	显示虚拟路由器的配置信息。

show virtual-router event-track

使用 **show virtual-router event-track** 命令显示事件探测配置信息。

命令

show virtual-router event-track

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示事件探测配置信息。

```
NetEye@root> show virtual-router event-track
```

【返回结果】

```
Disk Failure : Enable
```

show virtual-router

使用 **show virtual-router** 命令显示虚拟路由器的配置信息。

命令

show virtual-router {all | *vrid***}**

语法

vrid	虚拟路由器 ID，格式为 INTEGER<1-254>。 **all** 表示显示所有虚拟路由器的配置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示虚拟路由器 vr1 的配置信息。

```
NetEye@root>show virtual-router 1
```

【返回结果】

```
VRID:           1
Enable:         on
Interface:      eth1
Interval:       1
Preempt:        Enable
Authentication: 0
Backup ip:
State:          backup
Detection Group:        1
Config Priority:        100
Election Priority:      100
Description:
```

```
Type      Interface IP                  Port      Interval  Threshold
Weight
Ping      eth1      10.3.1.23           -         30        5         20
```

unset backup ip

使用 **unset backup ip** 命令删除虚拟路由器的备份 IP 地址。

命令

unset backup ip address *ip_address*

语法

ip_address	IP 地址，格式为 x.x.x.x。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器配置模式下使用。

范例

范例 . 删除虚拟路由器 vr1 的备份 IP 地址 10.3.1.23。

```
NetEye@root-system]virtual router 1
NetEye@root-system-vr1]unset backup ip address 10.3.1.23
```

相关命令

命令名称	描述信息
backup ip	添加虚拟路由器的备份 IP 地址。
show virtual-router	显示虚拟路由器的配置信息。

unset election interface

使用 **unset election interface** 命令删除虚拟路由器的选举接口。

命令

unset election interface *interface_name*

语法

interface_name	接口名称，格式为 WORD<1-15>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器配置模式下使用。

范例

范例 . 删除虚拟路由器 vr1 的选举接口 eth1。

```
NetEye@root-system]virtual router 1
NetEye@root-system-vr1]unset election interface eth1
```

相关命令

命令名称	描述信息
election interface	设置虚拟路由器的选举接口。
show virtual-router	显示虚拟路由器的配置信息。

unset virtual router event-track disk-failure

使用 **unset virtual router event-track disk-failure** 命令禁用磁盘异常事件探测。

命令

unset virtual router event-track disk-failure

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 禁用磁盘异常事件探测。

```
NetEye@root-system] unset virtual router event-track disk-failure
```

相关命令

命令名称	描述信息
virtual router event-track disk-failure	启用磁盘异常事件探测。
show virtual-router event-track	显示事件探测配置信息。

unset ip-track

使用 **unset ip-track** 命令删除虚拟路由器的 IP 探测方式。

命令

unset ip-track type {**tcp-ping interface** *interface_name* **ip** *track_address* **port** *track_port* | {**arp-ping** | **ping**} **interface** *interface_name* **ip** *track_address*}

语法

tcp-ping | **arp-ping** | **ping**	• tcp-ping—TCP ping 方式 • arp-ping—ARP ping 方式 • ping—ICMP ping 方式
interface_name	接口名称，格式为 WORD<1-15>。
track_address	探测 IP 地址，格式为 x.x.x.x。
track_port	探测端口，格式为 INTEGER<1-65535>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器配置模式下使用。

范例

范例 . 删除虚拟路由器 vr1 对 202.107.117.11 通过 ICMP ping 方式的 IP 探测。

```
NetEye@root-system]virtual router 1
NetEye@root-system-vr1]unset ip-track type ping interface eth1 ip
202.107.117.11
```

相关命令

命令名称	描述信息
ip-track	设置虚拟路由器的 IP 探测。

unset virtual router

使用 **unset virtual router** 命令删除指定的虚拟路由器。

命令

unset virtual router *vrid*

语法

vrid	虚拟路由器 ID，格式为 INTEGER<1-255>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除虚拟路由器 vr1。

```
NetEye@root-system]unset virtual router 1
```

相关命令

命令名称	描述信息
show virtual-router	显示虚拟路由器的配置信息。
virtual router	添加虚拟路由器并进入到虚拟路由器配置模式。

virtual router

使用 **virtual router** 命令添加虚拟路由器并进入到虚拟路由器配置模式。

命令

virtual router *vrid*

语法

vrid	虚拟路由器 ID，格式为 INTEGER<1-255>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 添加虚拟路由器 vr1。

```
NetEye@root-system]virtual router 1
NetEye@root-system-vr1]
```

相关命令

命令名称	描述信息
show virtual-router	显示虚拟路由器的配置信息。
unset virtual router	删除指定的虚拟路由器。

virtual router event-track disk-failure

使用 **virtual router event-track disk-failure** 命令启用磁盘异常事件探测。

命令

virtual router event-track disk-failure

说明

当 NetEye 启用磁盘异常事件探测后，如果探测到磁盘出现故障，则会触发一次故障切换。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在全局配置模式下使用。

范例

范例 . 启用磁盘异常事件探测。

```
NetEye@root-system] virtual router event-track disk-failure
```

相关命令

命令名称	描述信息
show virtual-router event-track	显示事件探测配置信息。
unset virtual router event-track disk-failure	禁用磁盘异常事件探测。

virtual-router enable, disable

使用 **virtual-router enable, disable** 命令启用或禁用虚拟路由器。

命令

virtual−router {**enable** | **disable**}

语法

enable | disable	• enable—启用虚拟路由器 • disable—禁用虚拟路由器 缺省设置为 enable

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器配置模式下使用。

相关命令

命令名称	描述信息
show virtual-router	显示虚拟路由器的配置信息。

虚拟路由器探测组

description

使用 **description** 命令设置虚拟路由器探测组的备注信息。

命令

description [*string*]

语法

string	备注信息，格式为 LINE。

说明

如果指定 *string* 参数，则表示添加或修改备注信息，否则表示删除备注信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器探测组配置模式下使用。

范例

范例 . 删除虚拟路由器探测组 dg1 的备注信息。

```
NetEye@root-system]detection group 1
NetEye@root-system-dg1]description
```

相关命令

命令名称	描述信息
show detection-group	显示虚拟路由器探测组的配置信息。

detection group

使用 **detection group** 命令创建虚拟路由器探测组，并进入到虚拟路由器探测组配置模式。

命令

detection group *group_id*

语法

group_id	虚拟路由器探测组 ID，格式为 INTEGER<1-255>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 创建虚拟路由器探测组 dg1。

```
NetEye@root-system]detection group 1
NetEye@root-system-dg1]
```

相关命令

命令名称	描述信息
show detection-group	显示虚拟路由器探测组的配置信息。
unset detection group	删除指定的虚拟路由器探测组。

hold virtual-router

使用 **hold virtual-router** 命令设置虚拟路由器探测组成员。

命令

hold virtual-router *vrid* **weight** *weight_value*

语法

vrid	虚拟路由器 ID，格式为 INTEGER<1-254>。
weight_value	权重，格式为 INTEGER<1-254>。

说明

如果虚拟路由器探测组中不存在与输入的 *vrid* 参数匹配的虚拟路由器，则表示添加；如果存在匹配的虚拟路由器，则表示修改该虚拟路由器的权重。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器探测组配置模式下使用。

范例

范例 . 向虚拟路由器探测组 dg1 中添加虚拟路由器成员 vr1。

```
NetEye@root-system]detection group 1
NetEye@root-system-dg1]hold virtual-router 1 weight 25
```

相关命令

命令名称	描述信息
show detection-group	显示虚拟路由器探测组的配置信息。
unset hold virtual-router	从虚拟路由器探测组中删除指定的虚拟路由器成员。

interval

使用 **interval** 命令设置虚拟路由器探测组的通告周期。

命令

interval *interval_value*

语法

interval _value	通告周期，单位为秒，格式为 INTEGER<1-60>。 缺省值为 1

说明

同一个 VRRP 组内各虚拟路由器的通告周期必须一致。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器探测组配置模式下使用。

范例

范例 . 设置虚拟路由器探测组 dg1 的通告周期为 3 秒。

```
NetEye@root-system]detection group 1
NetEye@root-system-dg1]interval 3
```

相关命令

命令名称	描述信息
show detection-group	显示虚拟路由器探测组的配置信息。

ip-track

使用 **ip-track** 命令设置虚拟路由器探测组的 IP 探测。

命令

ip-track type {**tcp-ping interface** *interface_name* **ip** *track_address* **port** *track_port* | {**arp-ping** | **ping**} **interface** *interface_name* **ip** *track_address*} **interval** *interval_value* **threshold** *threshold_value* **weight** *weight_value*

语法

tcp-ping | **arp-ping** | **ping**	• tcp-ping—TCP ping 方式 • arp-ping—ARP ping 方式 • ping—ICMP ping 方式
interface_name	接口名称，格式为 WORD<1-15>。
track_address	探测 IP 地址，格式为 x.x.x.x。
track_port	探测端口，格式为 INTEGER<1-65535>。
interval_value	探测周期，单位为秒，格式为 INTEGER<1-60>。
threshold_value	探测重试次数，格式为 INTEGER<1-999>。
weight_value	权重，格式为 INTEGER<1-254>。

说明

如果探测 IP 地址不可达，则虚拟路由器探测组的优先级将被减去权重值。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器探测组配置模式下使用。

范例

范例 . 在虚拟路由探测组 dg1 中，设置 TCP ping 探测方式 , 从接口 eth1 探测 IP 地址 202.107.117.20、端口为 80 的地址是否可达，同时设置探测周期为 3 秒，探测重试次数为 10，权重为 25。

```
NetEye@root-system]detection group 1
NetEye@root-system-dg1]ip-track type tcp-ping interface eth1 ip
202.107.117.20 port 80 interval 3 threshold 10 weight 25
```

相关命令

命令名称	描述信息
unset ip-track	删除虚拟路由器探测组的 IP 探测方式。

priority

使用 **priority** 命令设置虚拟路由器探测组的优先级。

命令

priority *pri*

语法

pri	优先级，格式为 INTEGER<1-254>。 缺省值为 100

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器探测组配置模式下使用。

范例

范例 . 设置虚拟路由器探测组 dg1 的优先级为 120。

```
NetEye@root-system]detection group 1
NetEye@root-system-dg1]priority 120
```

相关命令

命令名称	描述信息
show detection-group	显示虚拟路由器探测组的配置信息。

preempt enable, disable

使用 **preempt enable, disable** 命令启用或禁用虚拟路由器探测组的抢占模式。

命令

preempt {**enable** | **disable**}

语法

enable | disable	• enable—启用抢占模式 • disable—禁用抢占模式 缺省设置为 enable

说明

只有启用抢占模式，当 VRRP 组内备份虚拟路由器的优先级大于当前主虚拟路由器时，才会发生主备切换，否则不发生切换。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器探测组配置模式下使用。

范例

范例 . 禁用虚拟路由器探测组 dg1 的抢占模式。

```
NetEye@root-system]detection group 1
NetEye@root-system-dg1]preempt disable
```

相关命令

命令名称	描述信息
show detection-group	显示虚拟路由器探测组的配置信息。

show detection-group

使用 **show detection-group** 命令显示虚拟路由器探测组的配置信息。

命令

show detection-group {**all** | *group_id*}

语法

group_id	虚拟路由器探测组 ID，格式为 INTEGER<1-255>。 **all** 表示显示所有虚拟路由器探测组的配置信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V	V	V

模式

该命令在普通配置模式下使用。

范例

范例 . 显示虚拟路由器探测组 dg1 的配置信息。

```
NetEye@root>show detection-group 1
```

【返回结果】

```
vsys:           0
GID:            1
Priority:       100
Interval:       1
Preempt:        Enable
Group Member:   1
Config Priority:        100
Election Priority:      100
Description:

Type      Interface IP                  Port      Interval  Threshold
Weight
ARP Ping  eth3     10.5.5.5          -       5        5        5
```

```
NetEye@root> show detection-group 1
vsys:           0
GID:            1
Priority:       1
Interval:       5
Preempt:        Enable
Group Member:   1
Config Priority:        1
Election Priority:      1
Description:    This is detection-group1.

Type      Interface IP                  Port      Interval  Threshold
Weight
ARP Ping  eth3      10.5.5.5            -         5         5         5
```

unset detection group

使用 **unset detection group** 命令删除指定的虚拟路由器探测组。

命令

unset detection group *group_id*

语法

group_id	虚拟路由器探测组 ID，格式为 INTEGER<1-255>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在全局配置模式下使用。

范例

范例 . 删除虚拟路由器探测组 dg1。

```
NetEye@root-system]unset detection group 1
```

相关命令

命令名称	描述信息
detection group	创建虚拟路由器探测组。
show detection-group	显示虚拟路由器探测组的配置信息。

unset hold virtual-router

使用 **unset hold virtual-router** 命令从虚拟路由器探测组中删除指定的虚拟路由器成员。

命令

unset hold virtual-router *vrid*

语法

vrid	虚拟路由器 ID，格式为 INTEGER<1-255>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器探测组配置模式下使用。

范例

范例 . 从虚拟路由器探测组 dg1 中删除虚拟路由器 vr1。

```
NetEye@root-system]detection group 1
NetEye@root-system-dg1]unset hold virtual-router 1
```

相关命令

命令名称	描述信息
hold virtual-router	设置虚拟路由器探测组成员。
show detection-group	显示虚拟路由器探测组的配置信息。

unset ip-track

使用 **unset ip-track** 命令删除虚拟路由器探测组的 IP 探测方式。

命令

unset ip-track type {**tcp-ping interface** *interface_name* **ip** *track_address* **port** *track_port* | {**arp-ping** | **ping**} **interface** *interface_name* **ip** *track_address*}

语法

tcp-ping | **arp-ping** | **ping**	• tcp-ping—TCP ping 方式 • arp-ping—ARP ping 方式 • ping—ICMP ping 方式
interface_name	接口名称，格式为 WORD<1-15>。
track_address	探测 IP 地址，格式为 x.x.x.x。
track_port	探测端口，格式为 INTEGER<1-65535>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V		V	

模式

该命令在虚拟路由器探测组配置模式下使用。

范例

范例 . 删除虚拟路由器探测组 dg1 对 202.107.117.11 通过 ICMP ping 方式的 IP 探测。

```
NetEye@root-system]detection group 1
NetEye@root-system-dg1]unset ip-track type ping interface eth1 ip
202.107.117.11
```

相关命令

命令名称	描述信息
ip-track	设置虚拟路由器探测组的 IP 探测。

集群

auth enable, disable

使用 **auth enable, disable** 命令启用或禁用集群内设备间的认证。

命令

auth {**enable password** *auth_key* | **disable**}

语法

enable | disable	• enable— 启用认证 • disable— 禁用认证 缺省设置为 disable
auth_key	认证密钥，格式为 WORD<1-8>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

范例

范例 . 启用集群认证，并设置认证密钥为 abcdef。

```
NetEye@root-system]cluster
NetEye@root-system-cluster]auth enable password abcdef
```

相关命令

命令名称	描述信息
show cluster	显示集群配置信息。

clusterid

使用 **clusterid** 命令将 NetEye 设备加入到指定的集群中。

命令

clusterid *cluster_id*

语法

cluster_id	集群 ID，格式为 INTEGER<1-63>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

范例

范例 . 将 NetEye 设备加入到集群 1 中。

```
NetEye@root-system]cluster
NetEye@root-system-cluster]clusterid 1
```

相关命令

命令名称	描述信息
show cluster	显示集群配置信息。
unset clusterid	将 NetEye 设备从集群中删除。

config check

使用 **config check** 命令比较同一集群内设备间的配置信息是否相同。

命令

config check

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

范例

范例 . 比较同一集群内设备间的配置信息是否相同。

```
NetEye@root-system]cluster
NetEye@root-system-cluster]config check
```

config sync

使用 **config sync** 命令进行配置信息立即同步。配置成功后，所有配置信息将会立即同步到对端 NetEye。

命令

config sync

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

config sync auto enable, disable

使用 **config sync auto enable, disable** 命令启用或禁用自动同步配置信息功能。

命令

config sync auto {**enable** | **disable**}

语法

enable | disable	• enable— 启用自动同步配置信息功能 • disable— 禁用自动同步配置信息功能 缺省设置为 disable

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

范例

范例 . 启用自动同步配置信息功能。

```
NetEye@root-system]cluster
NetEye@root-system-cluster]config sync auto enable
```

相关命令

命令名称	描述信息
show cluster	显示集群配置信息。

encrypt enable, disable

使用 **encrypt enable, disable** 命令启用或禁用同一集群内设备间的同步信息加密功能。

命令

encrypt {**enable password** *enc_key* | **disable**}

语法

enable | disable	• enable— 启用加密 • disable— 禁用加密 缺省设置为 disable
enc_key	加密密钥，格式为 WORD<1-8>。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

范例

范例 . 启用同一集群内设备间的同步信息加密，并设置加密密钥为 abcdef。

```
NetEye@root-system]cluster
NetEye@root-system-cluster]encrypt enable password abcdef
```

相关命令

命令名称	描述信息
show cluster	显示集群配置信息。

local ip address

使用 **local ip address** 命令设置集群设备本端同步接口的 IP 地址。

命令

local ip address *ip_address* **mask** *netmask*

语法

ip_address	IP 地址，格式为 x.x.x.x。
netmask	子网掩码，格式为 x.x.x.x。

说明

1. 必须保证集群设备本 / 对端同步接口的 IP 地址处于可达状态。
2. 在设置 IP 地址前，需要首先选取本端同步接口。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

范例

范例 . 设置集群设备本端同步接口的 IP 地址为 10.3.1.23/24。

```
NetEye@root-system]cluster
NetEye@root-system-cluster]local ip address 10.3.1.23 mask
255.255.255.0
```

相关命令

命令名称	描述信息
local interface	设置集群设备本端的同步接口。
show cluster	显示集群配置信息。

local interface

使用 **local interface** 命令设置集群设备本端的同步接口。

命令

local interface *interface_name*

语法

interface_name	接口名称，格式为 WORD<1-15>。

说明

1. 具有二层属性的接口，包括二层物理接口或二层 Channel 接口可以作为集群设备的同步接口使用。
2. 如果某个接口被作为同步接口使用，则其不能再进行它用。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

范例

范例 . 设置集群设备本端的同步接口为 ch1。

```
NetEye@root-system]cluster
NetEye@root-system-cluster]local interface ch1
```

相关命令

命令名称	描述信息
show cluster	显示集群配置信息。
local ip address	设置集群设备本端同步接口的 IP 地址。

peer ip address

使用 **peer ip address** 命令设置集群设备对端同步接口的 IP 地址。

命令

peer ip address *ip_address*

语法

ip_address	IP 地址，格式为 x.x.x.x。

说明

必须保证集群设备本 / 对端同步接口的 IP 地址处于可达状态。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

范例

范例 . 设置集群设备对端同步接口的 IP 地址为 10.3.1.28。

```
NetEye@root-system]cluster
NetEye@root-system-cluster]peer ip address 10.3.1.28
```

相关命令

命令名称	描述信息
show cluster	显示集群配置信息。

rti session

使用 **rti session** 命令添加要进行同步的自定义会话信息。配置成功后，添加的会话信息将被同步到对端 NetEye。

命令

rti session {{**tcp** | **udp**} {*port_num* | *port_range*} | **other** {*protocol_num* | *protocol_range*}}

语法

port_num	端口号，格式为 INTEGER<1-65535>。
port_range	端口号范围，格式为 LIMIT。
other	除 TCP 和 UDP 之外的协议。
protocol_num	other 类型协议的协议号，格式为 INTEGER<1-255>。
protocol_range	other 类型协议的协议号范围，格式为 LIMIT。

说明

如果要添加自定义会话信息，则需要首先启用自动同步运行信息功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

范例

范例 . 对 TCP 协议 23 端口的会话进行同步。

```
NetEye@root-system-cluster]rti session tcp 23
```

相关命令

命令名称	描述信息
rti session default	设置同步默认的会话信息。
rti sync enable, disable	启用或禁用自动同步运行信息功能。

命令名称	描述信息
show cluster	显示集群配置信息。
unset rti session	删除要进行同步的自定义会话信息。

rti session default

使用 **rti session default** 命令设置同步默认的会话信息。

命令

rti session default

说明

1. 如果要同步默认的会话信息，则需要首先启用自动同步运行信息功能。
2. 如果同步默认的会话信息，则包括会话、VPN SA 和 DHCP 分配的 IP 等将被同步到对端 NetEye，并且自定义会话信息将失效。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

相关命令

命令名称	描述信息
rti session	添加要进行同步的自定义会话信息。
rti sync enable, disable	启用或禁用自动同步运行信息功能。
show cluster	显示集群配置信息。

rti sync enable, disable

使用 **rti sync enable, disable** 命令启用或禁用自动同步运行信息功能。

命令

rti sync {**enable** | **disable**}

语法

enable | disable	• enable— 启用自动同步运行信息 • disable— 禁用自动同步运行信息 缺省值为 disable

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

范例

范例 . 启用自动同步运行信息功能。

```
NetEye@root-system]cluster
NetEye@root-system-cluster]rti sync enable
```

相关命令

命令名称	描述信息
show cluster	显示集群配置信息。

show cluster

使用 **show cluster** 命令显示集群配置信息。

命令

show cluster

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
V	V	V		

模式

该命令在普通配置模式下使用。

范例

范例 . 显示集群配置信息。

```
NetEye@root>show cluster
```

【返回结果】

```
Basic Information
Clusterid: 1
Interface device: Ch0
Local sync address: 2.1.1.1
Mask: 24
Remote sync address: 192.168.1.1

Mirror Information
Mirror status: Inactive
Encrypt: Off
Authentication: Off
Auto sync configuration: On

Runtime Information
Session information: Default
Auto sync runtime information: On
```

```
System Time Information
Time sync: Off
Benchmark: Off
Daily: Off
Time: 00:00
When boot: Off
When modified: Off
```

time benchmark

使用 **time benchmark** 命令设置当前 NetEye 是否为系统时间同步基准。

命令

time benchmark {**on** | **off**}

语法

on | **off**	• on— 设置当前 NetEye 为时间同步基准 • off— 设置当前 NetEye 不为时间同步基准 缺省设置为 off

说明

1. 如果要设置时间同步基准 NetEye，则需要首先启用自动同步系统时间功能。
2. 在指定集群中只能有一台 NetEye 作为基准，如果 NetEye 所属的集群已经设置了时间同步基准，则返回给管理员一个错误信息。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

范例

范例 . 将当前 NetEye 设置为系统时间同步基准。

```
NetEye@root-system]cluster
NetEye@root-system-cluster]time benchmark on
```

相关命令

命令名称	描述信息
show cluster	显示集群配置信息。
time sync enable, disable	启用或禁用自动同步系统时间功能。

time boot on, off

使用 **time boot on, off** 命令设置当 NetEye 启动时，是否立即同步系统时间。

命令

time boot {**on** | **off**}

语法

on | off	• on—当 NetEye 启动时，立即同步系统时间。 • off—当 NetEye 启动时，不进行系统时间同步。 缺省设置为 off

说明

如果要进行该设置，则需要首先启用自动同步系统时间功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

范例

范例 . 当 NetEye 启动时，立即同步系统时间。

```
NetEye@root-system]cluster
NetEye@root-system-cluster]time boot on
```

相关命令

命令名称	描述信息
show cluster	显示集群配置信息。
time sync enable, disable	启用或禁用自动同步系统时间功能。

time daily

使用 **time daily** 命令设置每日同步系统时间。

命令

time daily {*time_sync* | **off**}

语法

time_sync	同步时间，格式为 HH:MM。 **off** 表示不进行每日同步。 缺省值为 00:00。

说明

如果要设置每日同步系统时间，则需要首先启用自动同步系统时间功能。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

范例

范例 . 设置集群 NetEye 每日同步时间为上午 8 时。

```
NetEye@root-system]cluster
NetEye@root-system-cluster]time daily 08:00
```

相关命令

命令名称	描述信息
show cluster	显示集群配置信息。
time sync enable, disable	启用或禁用自动同步系统时间功能。

time modified on, off

使用 **time modified on, off** 命令设置当 NetEye 系统时间被更改时，是否立即同步系统时间。

命令

time modified {**on** | **off**}

语法

on | off	• on—当 NetEye 系统时间被更改时，立即同步系统时间。 • off—当 NetEye 系统时间被更改时，不进行系统时间同步。 缺省设置为 off

说明

1. 如果要进行该设置，则需要首先启用自动同步系统时间功能。
2. 当集群内 NetEye 系统时间被更改后，立即将修改后的系统时间同步到对端，即使对端是时间同步基准，也进行立即同步。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

范例

范例 . 设置当 NetEye 系统时间被更改时，立即同步系统时间。

```
NetEye@root-system]cluster
NetEye@root-system-cluster]time modified on
```

相关命令

命令名称	描述信息
show cluster	显示集群配置信息。
time sync enable, disable	启用或禁用自动同步系统时间功能。

time sync enable, disable

使用 **time sync enable, disable** 命令启用或禁用自动同步系统时间功能。

命令

time sync {**enable** | **disable**}

语法

**enable	disable**	• enable—启用自动同步系统时间 • disable—禁用自动同步系统时间 缺省设置为 off

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

范例

范例 . 启用自动同步系统时间功能。

```
NetEye@root-system]cluster
NetEye@root-system-cluster]time sync enable
```

相关命令

命令名称	描述信息
show cluster	显示集群配置信息。

unset clusterid

使用 **unset clusterid** 命令将 NetEye 设备从集群中删除。

命令

unset clusterid

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

相关命令

命令名称	描述信息
clusterid	将 NetEye 设备加入到指定的集群中。
show cluster	显示集群配置信息。

unset local interface

使用 **unset local interface** 命令删除集群设备的本端同步接口。

命令

unset local interface

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

相关命令

命令名称	描述信息
local interface	设置集群设备本端的同步接口。
show cluster	显示集群配置信息。

unset rti session

使用 **unset rti session** 命令删除要进行同步的自定义会话信息。

命令

unset rti session {{**tcp** | **udp**} {*port_num* | *port_range*} | **other** {*protocol_num* | *protocol_range*}}

语法

port_num	端口号，格式为 INTEGER<1-65535>。
port_range	端口号范围，格式为 LIMIT。
other	除 TCP 和 UDP 之外的协议。
protocol_num	other 类型协议的协议号，格式为 INTEGER<1-255>。
protocol_range	other 类型协议的协议号范围，格式为 LIMIT。

权限

Root Administrator	Administrator	Auditor	Vsys Administrator	Vsys Auditor
	V			

模式

该命令在集群配置模式下使用。

范例

范例 . 删除对 TCP 协议 23 端口的会话同步。

```
NetEye@root-system]cluster
NetEye@root-system-cluster]unset rti session tcp 23
```

相关命令

命令名称	描述信息
rti session	添加要进行同步的自定义会话信息。
show cluster	显示集群配置信息。

术语表

A

ABR — Area Border Router，区域边界路由器。在 OSPF 中，连接到多个区域接口的路由器叫做区域边界路由器。

AES — Advanced Encryption Standard，高级加密标准。用来加密和认证信息。

AH — Authentication Header，认证头协议。用于验证 IP 数据包的真实性和完整性的方法。

ARP — Address Resolution Protocol，地址解析协议。用来映射一个硬件地址或 MAC 地址到一个 IP 地址。

B

BGP — Border Gateway Protocol，边界网关协议。 BGP 在 TCP/IP 网络中进行区域间路由。 BGP 是一种外部网关协议，它在多个自治系统间或域间进行路由，并与其他 BGP 系统交换路由和访问信息。

C

CA — Certificate Authority，证书权威机构。用来负责签发和吊销证书的第三方机构。

CLI — Command Line Interface，命令行接口。基于命令行方式管理 NetEye 的一种服务接口。

CRL — Certificate Revocation List，证书吊销列表。

D

DES — Data Encryption Standard，数据加密标准。

DER — Distinguished Encoding Rules，高级编码规则。

DHCP — Dynamic Host Configuration Protocol，动态主机配置协议。通过 DHCP 功能，可以为网络内的主机动态指定 IP 地址。

DNAT — Destination Network Address Translation，目的网络地址转换。用于在外部网络中定义一系列的合法地址，采用动态分配的方法映射到内部网络。

DNS — Domain Name System，域名系统。用于将域名转换为对应的 IP 地址。

DoS — Denial of Service，拒绝服务。拒绝服务是一种网络攻击，主要目的是使网络中的服务不可用。

DSA — Digital Signature Algorithm，数字签名算法。非对称密码算法，它可以产生一个数字签名，而存在形式为一对大数。

DVMRP — Distance Vector Multicast Routing Protocol，距离矢量多播路由协议。是一种互联网路由协议，为互联网络的主机组提供了一种面向无连接信息组播的有效机制。

E

EGP — Exterior Gateway Protocol，外部网关协议。 EGP 的主要作用是在不同的自治系统内的相邻网关之间传递网络可达性信息，此协议现已基本被 BGP 协议所代替。

ESP — Encapsulating Security Payload，封装安全载荷协议。由 AH 扩展而来，它的工作方式是将整个 IP 数据包，包括报头和有效载荷一起压缩，装入一个新的数据包，并为它生成一个新的 IP 报头。

F

FQDN — Fully Qualifiled Domain Name，完全合格域名。

FTP — File Transfer Protocol，文件传输协议。文件传输协议是 TCP/IP 协议族的一部分，主要用于在主机间传输文件。

H

H.323 — H.323 是使不同的设备间能够通信的一个标准化协议。 H.323 定义了一组共同的编译码器，呼叫建立和协商程序，及基本的数据传输方法。

HTTPS — Secure Hypertext Transfer Protocol，安全超文本传输协议。 HTTP 的一种 SSL 加密版本。

I

ICMP — Internet Control Message Protocol，互联网控制消息协议。网络层协议，主要用于在主机与路由器之间传递控制信息，包括报告错误、交换受限控制和状态信息等。

IGMP — Internet Group Management Protocol，组管理协议。用于 IP 主机向任意一个直接相邻的路由器报告他们的组成员情况。

IKE — Internet Key Exchange，互联网密钥交换协议。用于交换和管理在 VPN 中使用的加密密钥。

IMAP — Internet Message Access Protocol，因特网信息访问协议。用于访问存储在邮件服务器系统内的电子邮件和电子公告板信息。

IP — Internet Protocol，网际协议。

L

L2TP — Layer 2 Tunneling Protocol，第二层隧道协议。

M

MAC — Media Access Control，介质访问控制子层协议。该协议位于 OSI 七层协议中数据链路层的下半部分，主要负责控制与物理层连接的物理介质。

MTU — Maximum Transmission Unit，最大传输单元。是指一种通信协议的某一层上面所能通过的最大数据报大小。

N

NAT — Network Address Translation，网络地址转换。是一种把内部私有网络地址（IP 地址）翻译成合法网络 IP 地址的技术。其目的之一是解决 IPv4 地址不足问题；其二可隐藏报文原始地址。

NSSA — Not-so-stubby-area。 RFC1587 中对此特性进行了描述。它是对当前 stub 区域特性非专属性的扩展。该特性允许外部路由以有限的方式进入 stub 区域。

NTP — Network Time Protocol，网络时间协议。一种通过向时间服务器发送请求来校对主机时间的协议。

O

OCSP — Online Certificate Status Protocol，在线证书状态协议。检查证书是否有效。

OSPF — Open Shortest Path First，最短路径优先。最短路径优先是 IP 网络的一种路由协议。由于 OSPF 对网络带宽的高效利用及其在拓扑变化之后迅速收敛的特点而在大型网络中得以迅速发展。

p

PIM — Protocol Independent Multicast，独立多播协议。PIM 可利用各种单播路由协议建立的单播路由表完成 RPF 检查功能。

POP — Post Office Protocol，邮局协议。客户端邮件应用程序使用该协议从邮件服务器上恢复邮件。

Q

QoS — Quality of Service，服务质量。传输系统的一个执行措施，反应了它的传输质量和服务的可用性。

R

RA — Registration Authority，注册审批机构。是 CA 的一个授权代理，负责证书的注册和发放 CRL。

RADIUS — Remote Authentication Dial In User Service，远程拨入用户认证服务。一种分布式的客户端 / 服务器系统，用来对访问进行验证，拒绝未经授权的访问。

RFC — Request for Comments，请求注解。 RFC 文档定义了因特网中通信所需的协议和标准。 RFC 由因特网工程任务组 (IETF) 发展并发行的。

RIP — Routing Information Protocol，路由信息协议。它是因特网中最常见的 IGP。RIP 使用跳数作为路由度量值。

Root Vsys — 根虚拟系统，又称为 Root 系统，是系统缺省的 Vsys，在它的基础上可以划分出其他 Vsys。通常又把它称为 Vsys0 或者物理 NetEye。

RSA — 一种基于陷门（Trapdoor）功能概念的加密算法，适用于公共密钥加密和数字签名。

S

SCEP — Simple Certificate Enrollment Protocol，简单证书注册协议。是一种从证书管理机构申请和获得证书的方法 (也称作注册)。

SNAT — Source Network Address Translation，源网络地址转换。用于将内部网络中的每个主机永久映射成外部网络中的某个合法的地址。

SNMP — Simple Network Management Protocol，简单网络管理协议。一种广泛使用的应用于管理网络设备的通信协议。

SSH — Secure Shell Protocol，安全外壳协议。是一种为远程登录会话和其他网络服务提供安全性的协议，利用 SSH 协议可以有效防止远程管理过程中的信息泄露。

SSL — Secure Scoket Layer，安全套接子层。位于应用层和 TCP/IP 之间，提供透明加密的数据通信。

T

TCP — Transmission Control Protocol，传输控制协议。是一种面向连接的、可靠的、基于字节流的运输层通信协议。

Telnet — 远程登录协议。基于 rfc854、rfc855。是 TCP / IP 网络（例如 Internet）的登录和仿真程序。主要功能是允许管理员登录进入远程主机系统。

TFTP — Trivial File Transfer Protocol，简单文件传输协议。用于在客户机与服务器之间进行简单的文件传输。

U

UDP — User Datagram Protocol，用户数据报协议。是 ISO 参考模型中一种无连接的传输层协议，提供面向事务的简单不可靠信息传送服务。

URL — Uniform Resource Locator，统一资源定位符。使用浏览器访问超文本文档及其他服务的一种标准化的寻址方案。

V

VRRP — Virtual Router Redundancy Protocol，虚拟路由器冗余协议。

VLAN — Virtual Local Area Network，虚拟局域网。是指在交换局域网的基础上，采用网络管理软件构建的可跨越不同网段、不同网络的端到端的逻辑网络。

VPN — Virtual Private Network，虚拟专用网络。可通过加密的通讯协议，在连接在 Internet 上的位于不同位置的两个或多个企业内部网之间建立一条专有的通讯线路。

Vsys — 虚拟系统。将物理 NetEye 在逻辑上虚拟为多个 NetEye 的实现方式，其中每个虚拟出来的部分都有各自独立的安全控制策略。

X

XAUTH — Extended Authentication，可扩展认证。

Xmodem — 一种使用拨号调制解调器的个人计算机通信中广泛使用的异步文件运输协议。以 128 字节块的形式传输数据，并且每个块都使用一个校验和过程来进行错误检测。

Z

Zmodem — Xmodem 文件传输协议的一种增强形式，不仅能传输更大的数据，而且错误率更小。

索引

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Z