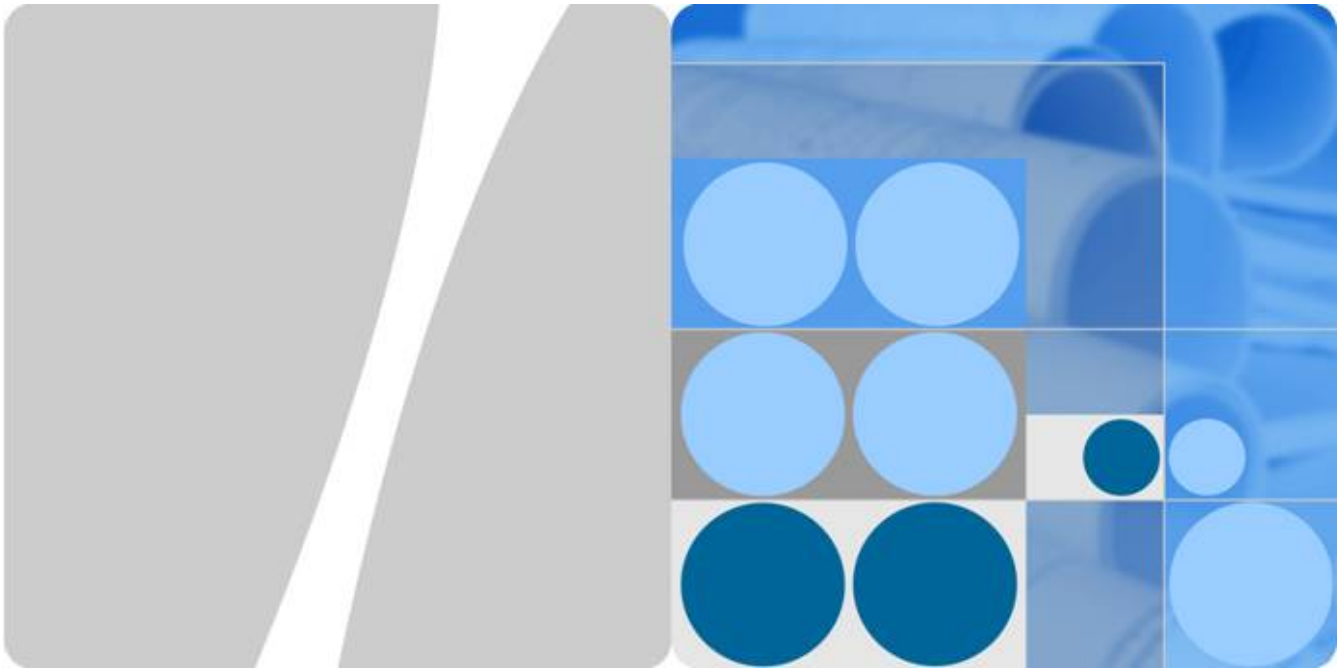


Quidway Eudemon 8080E/8160E 防火墙
V100R003

配置指南 系统管理分册

文档版本 04
发布日期 2011-01-05

华为技术有限公司

HUAWEI

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 0755-28560000 4008302118

客户服务传真： 0755-28560111

前 言

读者对象

本文档介绍了如何配置 Eudemon 8080E/8160E 的文件系统、信息中心、NTP、SNMP、RMON 和 RMON2，远程抓包，以及系统的升级和维护。

本文档提供了 Eudemon 8080E/8160E 的配置方法。

本文档主要适用于以下工程师：

- 技术支持工程师
- 维护工程师
- 网络工程师
- 网络管理员
- 网络维护工程师

目 录

插图目录

表格目录

1 配置文件系统

关于本章

通过配置文件系统，管理存储设备中的目录和文件。

1.1 文件系统简介
文件系统是指存储设备中的目录和文件。

1.2 管理目录
通过管理目录，实现对目录的各种操作。

1.3 管理文件
通过管理文件，实现对文件的各种操作。

1.4 运行批处理文件
通过运行批处理文件，可以逐条执行批处理文件中的命令行。

1.5 配置文件系统提示方式
通过配置文件系统提示方式，可以选择对文件系统进行操作的提示方式。

1.6 配置举例
介绍文件系统的配置举例。

1.1 文件系统简介

文件系统是指存储设备中的目录和文件。

目录是一种将整个文件集合进行组织的机制，是文件的逻辑上的容器。

文件是系统的存储信息，文件系统是对信息进行管理的一种机制。

1.2 管理目录

通过管理目录，实现对目录的各种操作。

1.2.1 查看当前工作目录

通过查看当前工作目录，可以了解用户当前工作的本地目录。

操作步骤

步骤 1 在用户视图下执行命令 **pwd**，显示当前的工作目录。

----结束

1.2.2 改变当前目录

通过改变当前目录，可以修改用户当前工作的本地目录。

操作步骤

步骤 1 在用户视图下执行命令 **cd** { *directory* | **cfcard:** }，改变当前目录。

----结束

1.2.3 显示目录或文件信息

通过显示目录或文件信息，可以查看存储设备中所有文件、指定文件或目录的信息。

操作步骤

步骤 1 在用户视图下执行命令 **dir** [**/all**] [*filename* | **cfcard:**]，显示目录或文件信息。

----结束

1.2.4 创建目录

通过创建目录，可以在指定存储设备指定目录下创建目录。

操作步骤

步骤 1 在用户视图下执行命令 **mkdir** { *directory* | **cfcard:** }，创建目录。

----结束

1.2.5 删除目录

通过删除目录，可以删除指定存储设备指定目录下的空目录。

操作步骤

步骤 1 在用户视图下执行命令 **rmdir** { *directory* | **cfcard:** }，删除目录。

----结束

1.3 管理文件

通过管理文件，实现对文件的各种操作。

1.3.1 显示文件的内容

通过显示文件的内容，可以了解指定文件的内容。

操作步骤

步骤 1 在用户视图下执行命令 **more** *filename offset*，显示文件的内容。

----结束

1.3.2 拷贝文件

通过拷贝文件，可以实现在同一存储设备内或不同存储设备间复制文件。

操作步骤

步骤 1 在用户视图下执行命令 **copy** [**cfcard:**/] *source-filename* [**cfcard:**/] *destination-filename*，拷贝文件。

----结束

1.3.3 移动文件

通过移动文件，可以实现在同一存储设备内或不同存储设备间剪切文件。

操作步骤

步骤 1 在用户视图下执行命令 **move** [**cfcard:**/] *source-filename* [**cfcard:**/] *destination-filename*，移动文件。

----结束

1.3.4 重新命名文件

通过重新命名文件，可以根据需要修改文件名。

操作步骤

步骤 1 在用户视图下执行命令 **rename** [**cfcard:**/] *source-filename* [**cfcard:**/] *destination-filename*，重新命名文件。

----结束

1.3.5 删除文件

通过删除文件，可以将文件放在回收站目录中或彻底删除文件。

背景信息

删除文件时，如果选择彻底删除文件，删除的文件将不可恢复。

操作步骤

步骤 1 在用户视图下执行命令 **delete** [**/unreserved**] { *filename* | **cfcard:** }，删除文件。

----结束

1.3.6 彻底删除回收站中的文件

通过彻底删除回收站中的文件，可以将存放在回收站目录中的文件彻底删除。

背景信息

通过该操作删除文件后，将不可恢复。

操作步骤

步骤 1 在用户视图下执行命令 **reset recycle-bin** [*filename* | **cfcard:**]，彻底删除回收站中的文件。

说明

执行命令 **reset recycle-bin**，可删除回收站中的所有文件。

----结束

1.3.7 恢复删除文件

通过恢复删除文件，可以恢复存放在回收站目录中的文件。

背景信息

删除文件时，如果选择彻底删除文件，删除的文件将不可恢复。

操作步骤

步骤 1 在用户视图下执行命令 **undelete** { *filename* | **cfcard:** }，恢复删除文件。

----结束

1.4 运行批处理文件

通过运行批处理文件，可以逐条执行批处理文件中的命令行。

前提条件

在客户端编辑的批处理文件，已经上传到当前设备上。

背景信息

说明

批处理文件的扩展名为“.bat”。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **execute** *filename*，执行批处理文件中的命令行。

----结束

1.5 配置文件系统提示方式

通过配置文件系统提示方式，可以选择对文件系统进行操作的提示方式。

背景信息

可对文件系统配置以下提示方式：

- 配置文件系统提示方式为 **alert**，对可能会导致数据丢失或破坏的用户操作（比如删除文件操作）进行提示，经用户确认后执行该操作。
- 配置文件系统提示方式为 **quiet**，对用户操作不进行提示。

缺省情况下，文件系统为 **alert** 提示方式。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **file prompt** { **alert** | **quiet** }，配置文件系统的提示方式。

----结束

1.6 配置举例

介绍文件系统的配置举例。

组网需求

用户成功登录 Eudemon 后，对 Eudemon 文件系统进行配置，拷贝文件到指定目录下。

背景信息

文件在存储设备中的路径一定要正确，如果不指定目标文件名，则目标文件名默认为源文件名，即目标文件和源文件同名。

数据规划

文件系统配置举例数据规划如表 1-1 所示。

表 1-1 文件系统配置举例数据规划

项目	数据	备注
源文件名和文件路径	cfcard:/private-data.txt	-
目标文件名和文件路径	cfcard:/test/private-data.txt	-

操作步骤

步骤 1 显示当前目录下的文件信息。

```
<Eudemon> dir
Directory of cfcard:/

   0   -rw-        53  Jul 28 2008 18:43:02   private-data.txt
   1   -rw-     16309  Apr 21 2008 17:46:48   paf.txt
   2   -rw-      6906  Apr 21 2008 17:46:48   license.txt
   3   -rw-         0  Apr 18 2008 17:35:12   patchnpstate.dat
   4   -rw-     16309  Apr 18 2008 17:07:08   paf.txt.bak
   5   -rw-      1109  Apr 21 2008 16:53:30   vrpcfg.zip
   6   -rw-  86088080  Jul 23 2008 16:47:28   e8000ev100r002c01.cc
   7   -rw-       867  Jul 28 2008 17:26:38   infotest.zip
   8   drw-         -  Jul 28 2008 18:52:58   test
   9   drw-         -  Jul 26 2008 11:49:30   test1

506880 KB total (261008 KB free)
```

步骤 2 拷贝文件 private-data.txt 从 cfcard:/到 cfcard:/test/。

```
<Eudemon> copy cfcard:/private-data.txt cfcard:/test/private-data.txt
Copy cfcard:/private-data.txt to cfcard:/test/private-data.txt?[Y/N]:y
100%  complete
Info:Copied file cfcard:/private-data.txt to cfcard:/test/private-data.txt...Done
```

----结束

结果验证

显示当前目录下的文件信息，可以看到文件已经被拷贝至指定目录下。

```
<Eudemon> cd cfcard:/test
<Eudemon> dir
Directory of cfcard:/test/

   0   drw-         -  Jul 26 2008 14:53:22   test.txt
   1   -rw-         0  Jul 26 2008 16:50:56   patchnpstate.dat
   2   -rw-        53  Jul 28 2008 18:52:58   private-data.txt

506880 KB total (261008 KB free)
```

2 配置日志/告警/调试信息的输出

关于本章

通过配置信息中心，用户能够有效地监控网络运行情况和诊断网络故障。

2.1 简介
介绍日志和信息中心的概念。

2.2 配置二进制日志
通过配置二进制日志信息输出，可以向日志主机输出二进制日志。

2.3 配置 Syslog 日志信息输出
通过配置日志信息输出，可以通过信息中心输出 Syslog 日志信息。

2.4 配置告警信息输出
通过配置告警信息输出，可以通过信息中心输出告警信息。

2.5 配置调试信息输出
通过配置调试信息输出，可以通过信息中心输出调试信息。

2.6 清除信息中心统计数据
信息中心统计数据清除后，将无法恢复。

2.7 清除日志缓冲区信息
清除日志缓冲区信息，以释放日志缓冲区的空间。

2.8 清除告警缓冲区信息
清除告警缓冲区信息，以释放告警缓冲区的空间。

2.9 配置举例
介绍信息中心的配置举例。

2.1 简介

介绍日志和信息中心的概念。

2.1.1 日志
介绍日志的种类及其输出原理。

2.1.2 信息中心
信息中心是 Eudemon 的信息枢纽，能够接收系统各模块的日志、调试和告警信息，并能对信息进行分类和筛选。

2.1.1 日志

介绍日志的种类及其输出原理。

日志种类划分

Eudemon 能够将系统消息或包过滤的动作存入缓冲区或定向发送到日志主机上。通过对日志内容的分析和归档，管理员能够检查网络中违背安全策略的行为、网络攻击的类型等信息，实时的日志记录还可以用来检测正在进行的入侵。

Eudemon 能够输出以下几种日志信息：

- 会话信息日志（包括 ASPF 等）
- 攻击防范日志
- 黑名单日志

说明

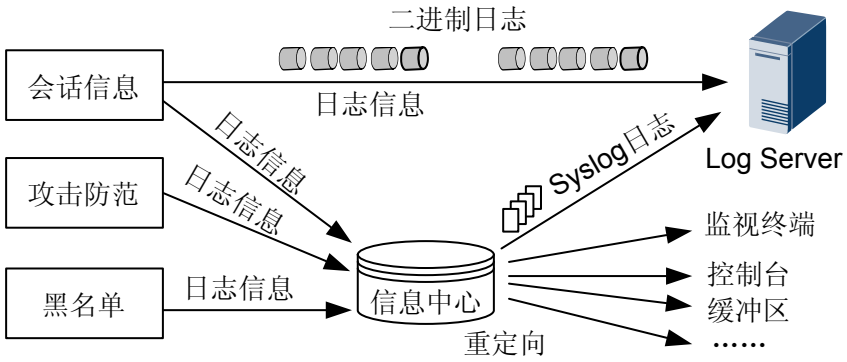
Eudemon 输出攻击防范日志时，对于 Eudemon 本身发出的报文所触发的攻击日志，日志中的“Receive Interface”字段不会显示具体信息。“Receive Interface”字段表示收到攻击报文的接口。

对于上述这些日志，根据日志输出方式的不同可以分为二进制日志、Syslog 日志。

日志输出原理

日志种类和日志输出方式之间的对应关系如图 2-1 所示。

图 2-1 日志输出原理示意图



在 Eudemon 中，攻击防范、黑名单产生的日志信息量小，因此采用 SysLog 方式以文本格式进行输出。这些日志信息必须通过信息中心模块进行日志管理和输出重定向，或者显示在终端屏幕上，或将 SysLog 日志发送给日志主机进行存储和分析。

相反，会话产生的日志信息量很大，因此对于这种类型的流提供了一种“二进制”输出方式，直接输出到日志主机以便对日志进行存储和分析，无需信息中心模块的参与。相比较而言，二进制日志的传输效率高于 Syslog 日志。

2.1.2 信息中心

信息中心是 Eudemon 的信息枢纽，能够接收系统各模块的日志、调试和告警信息，并能对信息进行分类和筛选。

信息的分类

信息中心可以接收和处理 3 类信息：

- 日志信息（log 类）

  例如：
  ```
  2009-04-29 11:28:54 Eudemon %%01SHELL/5/CMDRECORD(l): ....:vt1 ....:
  128.18.196.3 ....:** ......:public ....:info-center loghost 128.18.196.3 facility local4
  language chinese.
  ```

- 调试信息（debug 类）

  例如：
  ```
  *0.18800833 Eudemon IP/8/debug_case:
  Receiving, interface = GigabitEthernet2/0/13, version = 4, headlen = 20, tos = 0 , pktlen =
  40, pktid = 29348, offset = 0, ttl = 128, protocol = 6, checksum = 65330, s = 128.18.196.3, d
  = 128.18.196.208
  prompt: Receiving IP packet from GigabitEthernet2/0/13
  ```

- 告警信息（trap 类）

  例如：
  ```
  #2009-04-27 05:57:58 Eudemon ENTMIB/5/TRAP:1.3.6.1.2.1.47.2.0.1 Entity MIB chan
  ```

信息的严重等级

根据信息的严重等级或紧急程度，信息分为 8 个等级，信息越严重，其严重等级值越小，如表 2-1 所示。

根据严重等级过滤信息时，仅输出严重等级值小于或等于所配置的严重等级阈值的信息，即输出所配置级别和比所配置级别更严重的信息。例如，当配置严重等级阈值为 6 时，仅输出严重等级值为 0 ～ 6 的信息。

表 2-1 信息严重等级的定义

显示值	严重等级	描述
0	Emergency	设备致命的异常，系统已经无法恢复正常，必须重启设备。如程序异常导致设备重启，内存在使用过程中被检测出错误等。
1	Alert	设备重大的异常，需要立即采取措施。如设备内存占用率达到极限等。

显示值	严重等级	描述
2	Critical	设备较大的异常，需要采取措施进行处理或原因分析。如设备内存占用率超过告警线，温度超过低温告警线，检测出错误的消息（消息是由本设备内部生成）等。
3	Error	错误的操作或设备的异常流程，不会影响后续业务，但是需要关注和原因分析。如用户输入错误命令，用户密码错误等。
4	Warning	设备的异常运转，可能引起业务故障的流程，需要引起注意。如用户关闭路由进程，检测出错误协议报文等。
5	Notice	用于设备正常运转的关键操作信息。如用户对接口的**shutdown** 命令等。
6	Informational	用于设备正常运转的一般性操作信息。如用户使用**display** 命令等。
7	Debugging	设备正常运转的一般性信息，用户无需关注。

信息中心的工作过程

信息中心的工作过程如下：

1. 接收各模块输出的日志信息（log）、告警信息（trap）和调试信息（debug）。
2. 根据用户的设置，将不同严重等级的信息输出到不同的信息通道。
3. 根据信息通道和输出方向的关联，将信息输出到不同方向。

信息通道和输出方向

信息中心支持 10 个通道。缺省情况下，通道 0 ～ 5、9 有缺省通道名，与 7 个输出方向分别关联。具体如表 2-2 所示。

表 2-2 信息通道和输出方向

通道号	缺省通道名	输出方向	描述
0	console	console	本地控制台，可以接收日志、告警、调试信息。
1	monitor	monitor	VTY 终端，可以接收日志、告警、调试信息。方便远程维护。
2	loghost	loghost	日志主机，可以接收日志、告警、调试信息。信息在日志主机上以文件形式保存，供随时查看。

通道号	缺省通道名	输出方向	描述
3	trapbuffer	trapbuffer	SNMP（Simple Network Management Protocol） trap 信息缓冲区，可以接收 SNMP trap 告警信息。在 Eudemon 内部分配，用于记录信息。
4	logbuffer	logbuffer	日志缓冲区，可以接收日志信息。在 Eudemon 内部分配，用于记录信息。
5	snmpagent	snmpagent	SNMP Agent，可以接收 SNMP trap 告警信息。
6	channel6	未指定	保留
7	channel7		
8	channel8		
9	channel9	logfile	日志文件，可以接收日志、告警、调试信息。在 Eudemon 的存储设备上以文件形式保存。

日志信息的输出格式

日志信息的输出格式为：<Integer>TimeStamp HostName %%ddXYZ/Serverity/Brief(L):-Slot=k﹣XXX;Description。

日志信息各字段的详细说明如**表 2-3** 所示。

表 2-3 日志信息输出格式说明

字段	字段含义	说明
<Integer>	前导符	在向日志主机发送的时候添加前导符，在设备本机保存的日志不保存前导符。 Integer=*local-number**8+*severity*。其中，*local-number* 表示日志主机记录工具的编号，主要用于在日志主机端标志不同的日志来源，查找、过滤对应日志源的日志。在配置日志主机相关参数时可以设置 *local-number*，参数取值为 local0 ～ local7，对应的十进制数值为 16 ～ 23，缺省取值为 local7。*severity*（信息级别）的取值范围为 0 ～ 7，信息级别具体含义如**表 2-1** 所示。

字段	字段含义	说明
TimeStamp	时间戳，信息输出的时间	时间戳有以下格式可供选择: ● boot 型 相对时间类型。调试信息缺省采用 boot 型时间戳。 ● date 型 系统时间类型。告警信息和日志信息缺省采用 date 型时间戳。 ● short-date 型 与 date 型的唯一区别是，short-date 型时间戳不含年份。 ● format-date 型 另一种时间格式。按照年、月、日、时、分、秒的格式显示：YYYY-MM-DD hh:mm:ss ● none 型 信息中不包含时间戳。
HostName	设备本机的主机名	缺省是“Eudemon”。
%%	华为公司的标识	标识该日志是由华为公司的产品输出的。
dd	版本号	用来标识该日志格式的版本。
XYZ	模块名	向信息中心输出信息的模块名称。
Serverity	日志的级别	表示日志信息的级别。
Brief	简要描述	日志信息的简要描述。
(L)	信息的类别	● l：日志信息 ● T：告警信息 ● d：debugging 信息 ● D：诊断日志信息
-Slot=k－XXX	定位信息	根据日志产生模块的不同，日志信息中有可能不包括此部分信息。 Slot：表示发送定位信息的槽位号。此部分信息前后各有一个空格。
Description	描述信息	各个模块向信息中心输出的信息的具体内容。由各个模块在每次输出时填充，详细描述该日志的具体内容。

告警信息的输出格式

告警信息的输出格式为：TimeStamp HostName ModuleName/Serverity/Brief:Description。

告警信息各字段的详细说明如**表 2-4** 所示。

表 2-4 告警信息输出格式说明

字段	字段含义	说明
TimeStamp	时间戳，信息输出的时间	时间戳有以下格式可供选择： ● boot 型 相对时间类型。调试信息缺省采用 boot 型时间戳。 ● date 型 系统时间类型。告警信息和日志信息缺省采用 date 型时间戳。 ● short-date 型 与 date 型的唯一区别是，short-date 型时间戳不含年份。 ● none 型 信息中不包含时间戳。
HostName	设备本机的主机名	缺省是“Eudemon”。
ModuleName	模块名	用来表示产生告警的模块名。
Serverity	严重级别	具体如**表 2-1** 所示。
Brief	简要描述	告警信息的简要描述。
Description	描述信息	告警信息的描述信息。

调试信息的输出格式

调试信息的输出格式与所调试模块有关，此处不再赘述。

2.2 配置二进制日志

通过配置二进制日志信息输出，可以向日志主机输出二进制日志。

背景信息

二进制日志实时向日志主机输出，因此需要配置日志主机。Eudemon 最多支持配置 16 个日志主机，实现日志主机的负载分担功能。

如果配置了多个日志主机，缺省情况下，Eudemon 发送二进制日志时，会根据配置的日志主机 ID，依次向 1 ～ 16 号的日志主机循环发送。

用户可以根据需要配置日志并发功能，开启日志并发功能后，每一条日志向所有的日志主机都发送。

说明

日志主机为 Secoway eLog 日志管理系统，关于 eLog 的详细介绍请参见相应的产品手册。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall session log-type binary host** *host-id ip-address port*，配置接收二进制日志的日志主机。

步骤 3 执行命令 **firewall session log-type binary source** *ip-address port*，配置发送二进制日志时使用的源 IP 地址和端口。

步骤 4 （可选）执行命令 **firewall session log-type binary send-type concurrent**，配置日志并发功能。

步骤 5 执行命令 **firewall interzone** [**vpn instance** *vpn-instance-name*] *zone-name1 zone-name2*，进入安全域间视图。

步骤 6 执行命令 **session log enable acl-number** *acl-number* {**inbound** | **outbound**}，开启域间二进制日志功能。

在安全域间可以根据基本 ACL 或高级 ACL 来设置记录二进制日志的条件，同时可以针对出方向和入方向分别配置。

----结束

2.3 配置 Syslog 日志信息输出

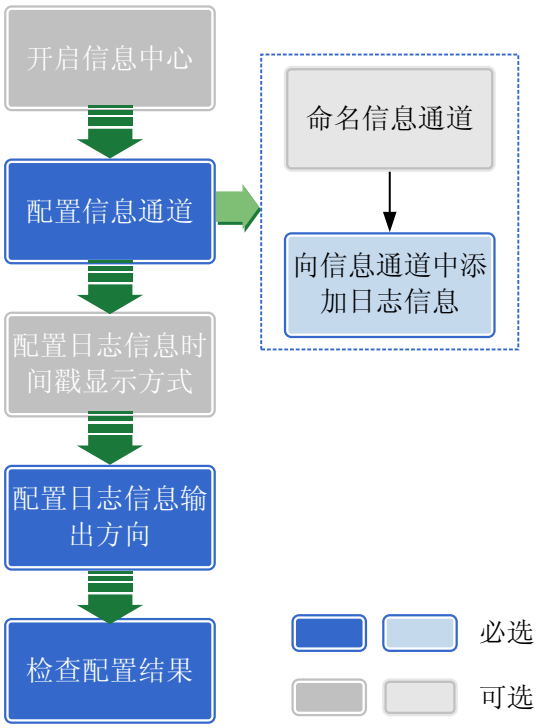
通过配置日志信息输出，可以通过信息中心输出 Syslog 日志信息。

2.3.1 配置流程

介绍日志信息输出的配置流程。

日志信息输出的配置流程如**图 2-2** 所示。

图 2-2 日志信息输出的配置流程图



2.3.2 开启信息中心

通过开启信息中心，可以使信息中心处于工作状态。

背景信息

说明

缺省情况下，信息中心处于工作状态。在信息中心开启时，由于需要对信息进行分类并输出，特别是在处理信息较多时，对系统性能有一定的影响。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center enable**，开启信息中心功能。

----结束

2.3.3 配置信息通道

通过配置信息通道，可以命名信息通道，并向信息通道中添加日志信息。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center channel** *channel-number* **name** *channel-name*，将编号为 *channel-number* 的信息通道命名为 *channel-name*。

信息中心支持 10 个通道，其中通道 0 ～ 5、9 有缺省通道名，如表 2-2 所示。

步骤 3 执行命令 **info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } **log** { **state** { **off** | **on** } | **level** *severity* } *，向信息通道中添加日志信息，并配置输出日志信息的严重等级阈值。

----结束

2.3.4 配置日志信息时间戳显示方式

通过配置日志信息时间戳显示方式，可以配置日志信息输出时间的显示方式。

背景信息

该配置为可选配置。

缺省情况下，日志信息的时间戳格式为 date。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center timestamp log** { **boot** | **date** | **none** | { **short-date** | **format-date** } [**precision-time** { **tenth-second** | **millisecond** }] }，配置日志信息时间戳显示方式。

----结束

2.3.5 配置日志信息输出方向

通过配置日志信息输出方向，可以根据实际需要选择日志信息的输出通道。

背景信息

信息中心可以在每个输出方向通过配置命令指定所需要的通道，所有信息经过指定通道的过滤，发送到相应的输出方向（共有 7 个方向）。

说明

- 需要开启信息中心，设置才会生效。
- 二进制日志不能通过主控板的千兆以太网口发送。

操作步骤

- 配置向控制台输出信息。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. 执行命令 **info-center console channel** { *channel-number* | *channel-name* }，配置向本地控制台输出信息。
  3. 执行命令 **quit**，退回到用户视图。
  4. 执行命令 **terminal monitor**，打开终端显示信息功能。
  5. 执行命令 **terminal logging**，打开终端显示日志信息功能。
- 配置向 Telnet 终端输出信息。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。

2. 执行命令 **info-center monitor channel** { *channel-number* | *channel-name* }，配置向 Telnet 终端输出信息。
3. 执行命令 **quit**，退回到用户视图。
4. 执行命令 **terminal monitor**，打开终端显示信息功能。
5. 执行命令 **terminal logging**，打开终端显示日志信息功能。

- 配置向日志主机输出信息。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. 执行命令 **info-center loghost** *ip-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | **language** { **chinese** | **english** }] *，配置向日志主机输出信息，并设置输出信息的信息通道以及其它参数。

     系统最多可设置 8 个日志主机。
  3. （可选）执行命令 **info-center loghost source** *interface-type interface-number*，配置向日志主机输出信息的源接口。

     使用此配置，可以将发向日志主机的信息的源地址设置为某一接口的 IP 地址，从而使日志主机能够通过源地址判断信息的来源，进行信息的归类管理。
- 配置向日志缓冲区输出信息。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. 执行命令 **info-center logbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*] *，配置向日志缓冲区输出信息，并设置日志缓冲区的大小。

     在信息中心开启后，缺省情况从 channel4 向日志缓冲区输出信息，日志缓冲区的大小为 512。
- 配置向日志文件输出信息。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. 执行命令 **info-center logfile channel** { *channel-number* | *channel-name* }，配置向日志文件输出信息。

----结束

2.3.6 配置攻击防范日志输出时间

配置系统定时输出攻击防范日志的时间间隔。

背景信息

二进制日志实时向日志主机输出，黑名单日志实时向信息中心输出，都无需配置日志输出时间。只有攻击防范日志可以配置日志输出时间。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall defend log-time** *time*，配置攻击防范日志的输出时间。

日志输出时间的单位为秒。缺省情况下，攻击防范日志输出时间为 30 秒。

----结束

2.3.7 检查配置结果

配置日志信息输出结束后，需要检查配置的正确性。

检查日志信息输出配置结果的相关操作如**表 2-5** 所示。

表 2-5 检查日志信息输出的配置结果

操作	命令
显示信息通道的内容	**display channel** [*channel-number* | *channel-name*]
显示信息中心记录的信息	**display info-center** [**statistics**]
显示日志缓冲区记录的信息	**display logbuffer** [**size** *size-value* | **level** *severity* | **slot** *slot-number*] * [| [**exclude** | **include**] *string*]
	display logbuffer summary [**level** *severity* | **slot** *slot-number*] *
显示攻击防范日志输出时间间隔	**display firewall logtime defend**

2.4 配置告警信息输出

通过配置告警信息输出，可以通过信息中心输出告警信息。

2.4.1 配置流程
介绍告警信息输出的配置流程。

2.4.2 开启信息中心
通过开启信息中心，可以使信息中心处于工作状态。

2.4.3 配置信息通道
通过配置信息通道，可以命名信息通道，并向信息通道中添加告警信息。

2.4.4 配置告警信息时间戳显示方式
通过配置告警信息时间戳显示方式，可以配置告警信息输出时间的显示方式。

2.4.5 配置告警信息输出方向
通过配置告警信息输出方向，可以根据实际需要选择告警信息的输出通道。

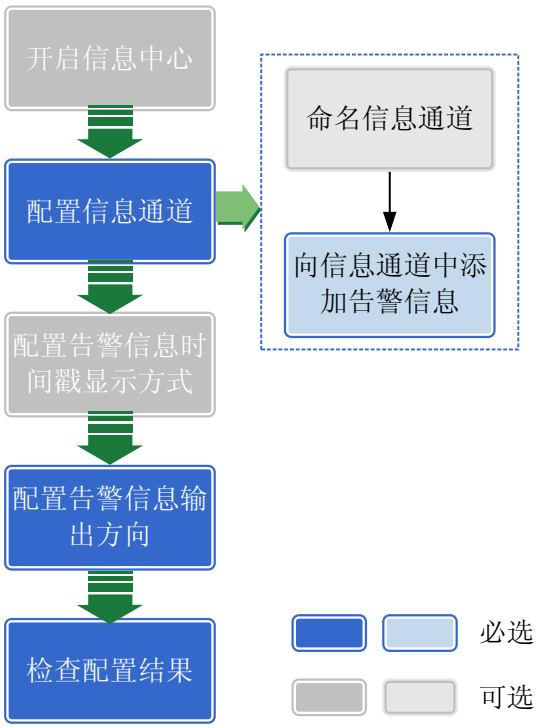
2.4.6 检查配置结果
配置告警信息输出结束后，需要检查配置的正确性。

2.4.1 配置流程

介绍告警信息输出的配置流程。

告警信息输出的配置流程如**图 2-3** 所示。

图 2-3 告警信息输出的配置流程图



2.4.2 开启信息中心

通过开启信息中心，可以使信息中心处于工作状态。

背景信息

说明

缺省情况下，信息中心处于工作状态。在信息中心开启时，由于需要对信息进行分类并输出，特别是在处理信息较多时，对系统性能有一定的影响。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center enable**，开启信息中心功能。

----结束

2.4.3 配置信息通道

通过配置信息通道，可以命名信息通道，并向信息通道中添加告警信息。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center channel** *channel-number* **name** *channel-name*，将编号为 *channel-number* 的信息通道命名为 *channel-name*。

信息中心支持 10 个通道，其中通道 0 ～ 5、9 有缺省通道名，如表 2-2 所示。

步骤 3 执行命令 **info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } **trap** { **state** { **off** | **on** } | **level** *severity* } *，向信息通道中添加告警信息，并配置输出告警信息的严重等级阈值。

----结束

2.4.4 配置告警信息时间戳显示方式

通过配置告警信息时间戳显示方式，可以配置告警信息输出时间的显示方式。

背景信息

该配置为可选配置。

缺省情况下，告警信息的时间戳格式为 date。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center timestamp trap** { **boot** | **date** | **none** | **short-date** }，配置告警信息时间戳显示方式。

----结束

2.4.5 配置告警信息输出方向

通过配置告警信息输出方向，可以根据实际需要选择告警信息的输出通道。

背景信息

信息中心可以在每个输出方向通过配置命令指定所需要的通道，所有信息经过指定通道的过滤，发送到相应的输出方向（共有 7 个方向）。

说明

需要开启信息中心，设置才会生效。

操作步骤

- 配置向控制台输出信息。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. 执行命令 **info-center console channel** { *channel-number* | *channel-name* }，配置向本地控制台输出信息。
  3. 执行命令 **quit**，退回到用户视图。
  4. 执行命令 **terminal monitor**，打开终端显示信息功能。
  5. 执行命令 **terminal trapping**，打开终端显示告警信息功能。
- 配置向 Telnet 终端输出信息。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. 执行命令 **info-center monitor channel** { *channel-number* | *channel-name* }，配置向 Telnet 终端输出信息。

3. 执行命令 **quit**，退回到用户视图。
4. 执行命令 **terminal monitor**，打开终端显示信息功能。
5. 执行命令 **terminal trapping**，打开终端显示告警信息功能

- 配置向告警缓冲区输出信息。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. 执行命令 **info-center trapbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*] *，配置向告警缓冲区输出信息，并设置告警缓冲区的大小。

     在信息中心开启后，缺省情况从 channel3 向告警缓冲区输出信息，告警缓冲区的大小为 256。
- 配置向 SNMP 输出信息。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. 执行命令 **info-center snmp channel** { *channel-number* | *channel-name* }，配置向 SNMP 输出信息。
  3. 执行命令 **snmp-agent**，启动 SNMP 代理功能。
- 配置向日志主机输出信息。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. 执行命令 **info-center loghost** *ip-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | **language** { **chinese** | **english** }] *，配置向日志主机输出信息，并设置输出信息的信息通道以及其它参数。

     系统最多可设置 8 个日志主机。
  3. （可选）执行命令 **info-center loghost source** *interface-type interface-number*，配置向日志主机输出信息的源接口。

     使用此配置，可以将发向日志主机的信息的源地址设置为某一接口的 IP 地址，从而使日志主机能够通过源地址判断信息的来源，进行信息的归类管理。
- 配置向日志文件输出信息。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. 执行命令 **info-center logfile channel** { *channel-number* | *channel-name* }，配置向日志文件输出信息。

----结束

2.4.6 检查配置结果

配置告警信息输出结束后，需要检查配置的正确性。

检查告警信息输出配置结果的相关操作如表 2-6 所示。

表 2-6 检查告警信息输出的配置结果

操作	命令
显示信息通道的内容	**display channel** [*channel-number* | *channel-name*]
显示信息中心记录的信息	**display info-center** [**statistics**]
显示告警缓冲区记录的信息	**display trapbuffer** [**size** *size-value*]

2.5 配置调试信息输出

通过配置调试信息输出，可以通过信息中心输出调试信息。

2.5.1 配置流程
介绍调试信息输出的配置流程。

2.5.2 开启信息中心
通过开启信息中心，可以使信息中心处于工作状态。

2.5.3 配置信息通道
通过配置信息通道，可以命名信息通道，并向信息通道中添加调试信息。

2.5.4 配置调试信息时间戳显示方式
通过配置调试信息时间戳显示方式，可以配置调试信息输出时间的显示方式。

2.5.5 配置调试信息输出方向
通过配置告警信息输出方向，可以根据实际需要选择告警信息的输出通道。

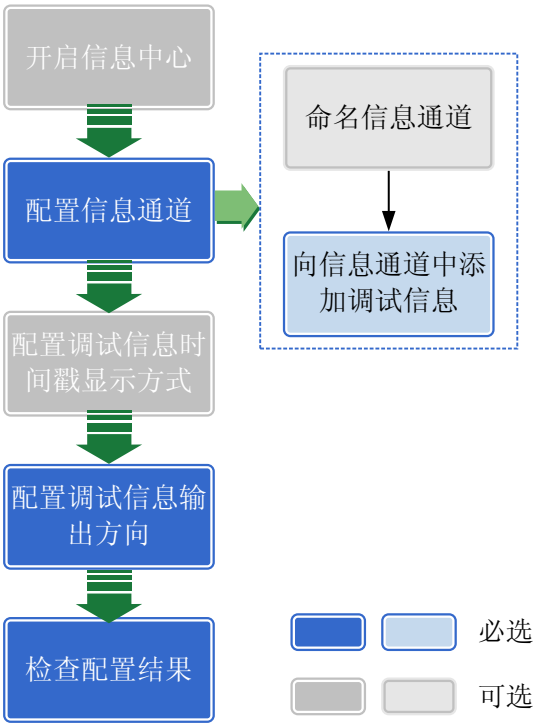
2.5.6 检查配置结果
配置调试信息输出结束后，需要检查配置的正确性。

2.5.1 配置流程

介绍调试信息输出的配置流程。

调试信息输出的配置流程如图 2-4 所示。

图 2-4 调试信息输出的配置流程图



2.5.2 开启信息中心

通过开启信息中心，可以使信息中心处于工作状态。

背景信息

说明

缺省情况下，信息中心处于工作状态。在信息中心开启时，由于需要对信息进行分类并输出，特别是在处理信息较多时，对系统性能有一定的影响。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center enable**，开启信息中心功能。

----结束

2.5.3 配置信息通道

通过配置信息通道，可以命名信息通道，并向信息通道中添加调试信息。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center channel** *channel-number* **name** *channel-name*，将编号为 *channel-number* 的信息通道命名为 *channel-name*。

信息中心支持 10 个通道，其中通道 0 ～ 5、9 有缺省通道名，如表 2-2 所示。

步骤 3 执行命令 **info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } **debug** { **state** { **off** | **on** } | **level** *severity* } *，向信息通道中添加调试信息，并配置输出调试信息的严重等级阈值。

----结束

2.5.4 配置调试信息时间戳显示方式

通过配置调试信息时间戳显示方式，可以配置调试信息输出时间的显示方式。

背景信息

该配置为可选配置。

缺省情况下，调试信息的时间戳格式为 boot。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center timestamp debugging** { **boot** | **date** | **none** | **short-date** }，配置调试信息时间戳显示方式。

----结束

2.5.5 配置调试信息输出方向

通过配置告警信息输出方向，可以根据实际需要选择告警信息的输出通道。

背景信息

信息中心可以在每个输出方向通过配置命令指定所需要的通道，所有信息经过指定通道的过滤，发送到相应的输出方向（共有 7 个方向）。

说明

需要开启信息中心，设置才会生效。

操作步骤

- 配置向控制台输出信息。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. 执行命令 **info-center console channel** { *channel-number* | *channel-name* }，配置向本地控制台输出信息。
  3. 执行命令 **quit**，退回到用户视图。
  4. 执行命令 **terminal monitor**，打开终端显示信息功能。
  5. 执行命令 **terminal debugging**，打开终端显示调试信息功能。
- 配置向 Telnet 终端输出信息。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. 执行命令 **info-center monitor channel** { *channel-number* | *channel-name* }，配置向 Telnet 终端输出信息。
  3. 执行命令 **quit**，退回到用户视图。
  4. 执行命令 **terminal monitor**，打开终端显示信息功能。
  5. 执行命令 **terminal debugging**，打开终端显示调试信息功能。
- 配置向日志主机输出信息。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. 执行命令 **info-center loghost** *ip-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | **language** { **chinese** | **english** }] *，配置向日志主机输出信息，并设置输出信息的信息通道以及其它参数。

     系统最多可设置 8 个日志主机。
  3. （可选）执行命令 **info-center loghost source** *interface-type interface-number*，配置向日志主机输出信息的源接口。

     使用此配置，可以将发向日志主机的信息的源地址设置为某一接口的 IP 地址，从而使日志主机能够通过源地址判断信息的来源，进行信息的归类管理。
- 配置向日志文件输出信息。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. 执行命令 **info-center logfile channel** { *channel-number* | *channel-name* }，配置向日志文件输出信息。

----结束

2.5.6 检查配置结果

配置调试信息输出结束后，需要检查配置的正确性。

检查调试信息输出配置结果的相关操作如表 2-7 所示。

表 2-7 检查调试信息输出的配置结果

操作	命令
显示信息通道的内容	**display channel** [*channel-number* | *channel-name*]
显示信息中心记录的信息	**display info-center** [**statistics**]

2.6 清除信息中心统计数据

信息中心统计数据清除后，将无法恢复。

背景信息

注意

清除信息中心的统计信息后，以前的统计信息将无法恢复，请务必仔细确认。

操作步骤

步骤 1 在用户视图下执行 **reset info-center statistics**，清除信息中心统计数据。

----结束

2.7 清除日志缓冲区信息

清除日志缓冲区信息，以释放日志缓冲区的空间。

操作步骤

步骤 1 在用户视图下执行命令 **reset logbuffer**，清除日志缓冲区信息。

----结束

2.8 清除告警缓冲区信息

清除告警缓冲区信息，以释放告警缓冲区的空间。

操作步骤

步骤 1 在用户视图下执行命令 **reset trapbuffer**，清除告警缓冲区信息。

----结束

2.9 配置举例

介绍信息中心的配置举例。

2.9.1 向日志主机输出二进制日志信息举例

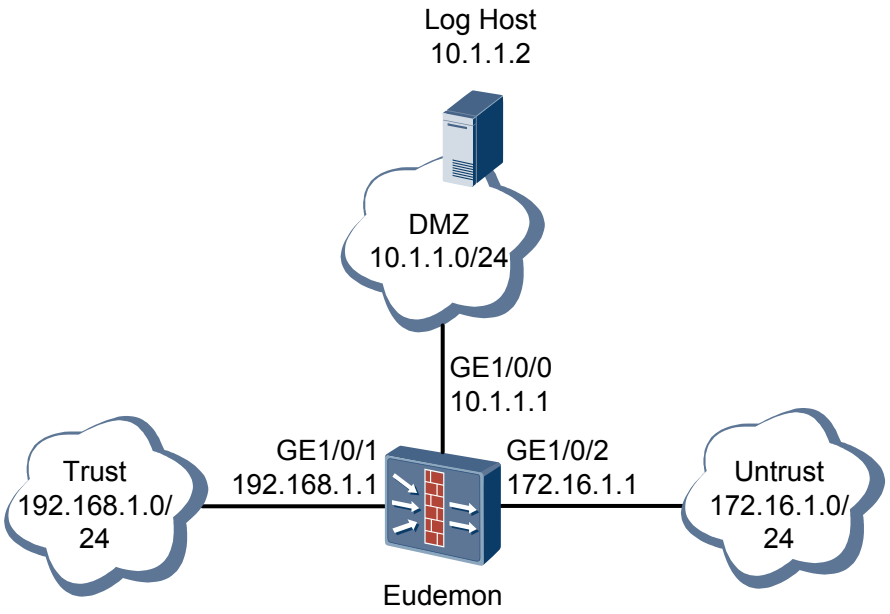
介绍向日志主机输出二进制日志信息的配置举例。

组网需求

如图 2-5 所示，某公司内部网络通过 Eudemon 进行连接，网络环境描述如下：

- Trust 区域通过接口 GigabitEthernet 1/0/1 与 Eudemon 连接。
- Untrust 区域通过接口 GigabitEthernet 1/0/2 与 Eudemon 连接。
- Log 服务器属于 DMZ 区域，通过接口 GigabitEthernet 1/0/0 与 Eudemon 连接。

图 2-5 配置向日志主机输出二进制日志信息组网图



要求配置二进制日志功能，将从 Trust 区域到 Untrust 区域的会话日志输出至 Log Server，供管理员分析。

配置思路

1. 根据网络规划为 Eudemon 分配接口，并将接口加入相应的安全区域。
2. 创建 ACL，并配置 ACL 规则。
3. 配置 Log Server 的 IP 地址和端口号，并在域间配置二进制日志功能。

数据准备

为完成此配置例，需准备如下的数据：

- Eudemon 各接口的 IP 地址。
- Log Server 的 IP 地址和端口号。
- Eudemon 与 Log Server 通讯的 IP 地址和端口号。

操作步骤

步骤 1 完成 Eudemon 的基本配置。

配置接口 GigabitEthernet 1/0/1 的 IP 地址。

```
<Eudemon> system-view
[Eudemon] interface GigabitEthernet 1/0/1
[Eudemon-GigabitEthernet1/0/1] ip address 192.168.1.1 24
[Eudemon-GigabitEthernet1/0/1] quit
```

配置接口 GigabitEthernet 1/0/2 的 IP 地址。

```
[Eudemon] interface GigabitEthernet 1/0/2
[Eudemon-GigabitEthernet1/0/2] ip address 172.16.1.1 24
[Eudemon-GigabitEthernet1/0/2] quit
```

配置接口 GigabitEthernet 1/0/0 的 IP 地址。

```
[Eudemon] interface GigabitEthernet 1/0/0
[Eudemon-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Eudemon-GigabitEthernet1/0/0] quit
```

将接口 GigabitEthernet 1/0/1 加入 Trust 区域。

```
[Eudemon] firewall zone trust
[Eudemon-zone-trust] add interface GigabitEthernet 1/0/1
[Eudemon-zone-trust] quit
```

将接口 GigabitEthernet 1/0/2 加入 Untrust 区域。

```
[Eudemon] firewall zone untrust
[Eudemon-zone-untrust] add interface GigabitEthernet 1/0/2
[Eudemon-zone-untrust] quit
```

将接口 GigabitEthernet 1/0/0 加入 DMZ 区域。

```
[Eudemon] firewall zone dmz
[Eudemon-zone-dmz] add interface GigabitEthernet 1/0/0
[Eudemon-zone-dmz] quit
```

创建高级 ACL 3000，配置源地址为 192.168.1.0/24、目的地址为 172.16.1.0/24 的规则。

```
[Eudemon] acl 3000
[Eudemon-acl-adv-3000] rule permit ip source 192.168.1.0 0.0.0.255 destination 172.16.1.0 0.0.0.255
[Eudemon-acl-adv-3000] quit
```

在 Trust 和 Untrust 域间配置包过滤。

```
[Eudemon] firewall interzone trust untrust
[Eudemon-interzone-trust-untrust] packet-filter 3000 outbound
[Eudemon-interzone-trust-untrust] quit
```

创建高级 ACL 3001，配置目的地址为 10.1.1.0/24 的规则。

```
[Eudemon] acl 3001
[Eudemon-acl-adv-3001] rule permit ip destination 10.1.1.0 0.0.0.255
[Eudemon-acl-adv-3001] quit
```

在 Local 和 DMZ 域间配置包过滤。

```
[Eudemon] firewall interzone local dmz
[Eudemon-interzone-local-dmz] packet-filter 3001 outbound
[Eudemon-interzone-local-dmz] quit
```

步骤 2 配置二进制日志功能。

创建基本 ACL 2000。

```
[Eudemon] acl 2000
[Eudemon-acl-basic-2000] rule permit
[Eudemon-acl-basic-2000] quit
```

在 Trust 和 Untrust 域间配置二进制日志功能。

```
[Eudemon] firewall interzone trust untrust
[Eudemon-interzone-trust-untrust] session log enable acl-number 2000 outbound
[Eudemon-interzone-trust-untrust] quit
```

配置二进制日志输出至 Log Server。

说明

Log Server 的配置请参考相关文档，本配置举例假设 Log Server 的 IP 地址为 10.1.1.2，端口号为 9002。

```
[Eudemon] firewall session log-type binary host 10.1.1.2 9002 source 10.1.1.1 9001
```

----结束

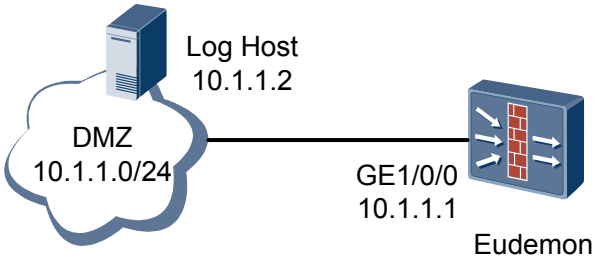
2.9.2 向日志主机输出 Syslog 日志信息举例

介绍向日志主机输出 Syslog 日志的配置举例。

组网需求

如图 2-6 所示，要求向日志主机输出 PPP 模块和 IP 模块的日志信息，Log 服务器属于 DMZ 区域，通过接口 GigabitEthernet 1/0/0 与 Eudemon 连接。需要在 Eudemon 侧和日志主机侧分别配置。

图 2-6 配置向日志主机输出 Syslog 日志信息组网图



数据准备

向日志主机输出 Syslog 日志信息举例的数据规划如表 2-8 所示。

表 2-8 向日志主机输出 Syslog 日志信息举例的数据规划

项目	数据	备注
日志主机的 IP 地址	10.1.1.2	-
信息通道名	loghost	-
允许日志输出的模块	PPP、IP	-
信息级别	informational	-
日志信息输出语言	英文	-
（可选）发送日志信息的源接口	GigabitEthernet 1/0/0	-

操作步骤

步骤 1 完成 Eudemon 的基本配置。

配置接口 GigabitEthernet 1/0/0 的 IP 地址。

```
<Eudemon> system-view
[Eudemon] interface GigabitEthernet 1/0/0
[Eudemon-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Eudemon-GigabitEthernet1/0/0] quit
```

将接口 GigabitEthernet 1/0/0 加入 DMZ 区域。

```
[Eudemon] firewall zone dmz
[Eudemon-zone-dmz] add interface GigabitEthernet 1/0/0
[Eudemon-zone-dmz] quit
```

创建高级 ACL 3001，配置目的地址为 10.1.1.0/24 的规则。

```
[Eudemon] acl 3001
[Eudemon-acl-adv-3001] rule permit ip destination 10.1.1.0 0.0.0.255
[Eudemon-acl-adv-3001] quit
```

在 Local 和 DMZ 域间配置包过滤。

```
[Eudemon] firewall interzone local dmz
[Eudemon-interzone-local-dmz] packet-filter 3001 outbound
[Eudemon-interzone-local-dmz] quit
```

步骤 2 配置 Eudemon 的信息中心。

开启信息中心功能。

```
[Eudemon] info-center enable
```

将 IP 地址为 10.1.1.2 的主机用作日志主机，日志主机记录工具为 Local4，输出语言为英文。

[Eudemon] info-center loghost 10.1.1.2 facility local4 language english

允许输出信息的模块为 PPP，设置严重等级阈值为 informational。

[Eudemon] info-center source ppp channel loghost log level informational

允许输出信息的模块为 IP，设置严重等级阈值为 informational。

[Eudemon] info-center source ip channel loghost log level informational

（可选）配置发送日志信息的源接口。

[Eudemon] info-center loghost source GigabitEthernet 1/0/0

步骤 3 日志主机侧配置。

日志主机上也要进行相应设置以完成上述功能。具体配置请参见日志主机的相关文档。

----结束

2.9.3 向控制台输出调试信息举例

介绍向控制台输出调试信息的配置举例。

组网需求

如图 2-7 所示，要求配置向控制台输出 IP 模块的调试信息。

图 2-7 配置向控制台输出调试信息组网图

数据规划

向控制台输出调试信息配置举例的数据规划如表 2-9 所示。

表 2-9 向控制台输出调试信息配置举例的数据规划

项目	数据	备注
信息通道名	console	-
允许信息输出的模块	ip	-
信息级别	debugging	-

操作步骤

步骤 1 开启信息中心。

进入系统视图。

<Eudemon> **system-view**

开启信息中心。

[Eudemon] **info-center enable**

步骤 2 配置信息的输出方向及输出内容。

配置向本地控制台输出信息。

[Eudemon] **info-center console channel console**

允许 IP 模块的日志输出，严重等级限制为 emergencies ～ debugging。

[Eudemon] **info-center source ip channel console debug level debugging**

退回用户视图。

[Eudemon] **quit**

步骤 3 配置信息显示。

打开终端显示信息功能。

<Eudemon> **terminal monitor**

打开终端显示调试信息功能。

<Eudemon> **terminal debugging**

打开 IP 模块的调试开关。

<Eudemon> **debugging ip packet**

----结束

结果验证

查看配置的通道信息。

```
<Eudemon> display channel console
channel number:0, channel name:console
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      notification  Y      (null)        Y      (null)
1000000  IP       Y      notification  Y      (null)        Y      (null)
```

3 配置 NTP

关于本章

通过配置 NTP（Network Time Protocol），可以使网络中的设备时钟保持一致。

3.1 NTP 简介

NTP 用来同步网络中分布式时间服务器和客户端之间的 UTC（Universal Time Coordinated）时间，使网络中的设备提供基于统一时间的应用成为可能。

NTP 属于应用层协议，基于 UDP 传输，使用的端口号为 123。

时间服务器和客户端是相对的。提供时间标准的设备为时间服务器，接收时间服务的设备为时间客户端。运行 NTP 的设备通过交换 NTP 报文，既可以作为时间客户端同步其他时钟源，又可以作为时间服务器被时间客户端同步。

应用环境

NTP 主要应用于需要网络中所有主机或设备时钟保持一致的场合，比如：

- 网络管理

  对不同设备采集来的日志信息、调试信息进行分析时，需要时间依据。
- 定时重启设备

  为了保证网络中的所有设备定时重启，要求所有设备的时钟保持一致。
- 多系统协同处理事件

  为保证正确的执行顺序，多个系统必须参考同一时钟。
- 在备份服务器和客户机之间进行增量备份

  要求备份服务器和所有客户端之间的时钟同步。

优点

管理员手工修改网络设备的系统时钟不但工作量巨大，而且不能保证时钟的精确性。NTP 可以快速高精度地实现网络中设备的时钟同步，具有以下优点：

- 采用分层（Stratum）的方法来定义时钟的准确性，可以迅速同步网络中各台设备的时间。

  NTP 主时钟的层数设定后，与该主时钟进行时钟同步的设备的层数递增。
- 支持访问控制和 MD5（Message Digest 5）验证。
- 支持采用单播、组播或广播方式发送协议报文。

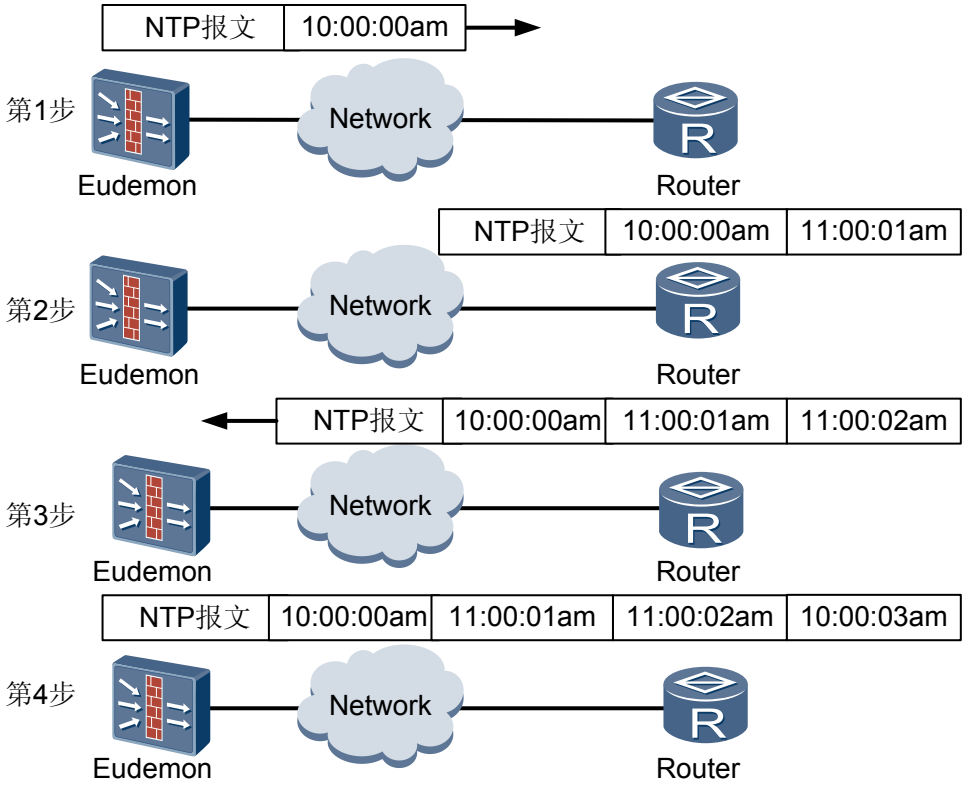
工作原理

NTP 基本工作原理如图 3-1 所示。Eudemon 和 Router 都有自己独立的系统时钟，需要通过 NTP 实现各自系统时钟的自动同步。

为便于理解，先作如下假设：

- 在 Eudemon 和 Router 的系统时钟同步之前，Eudemon 的时钟设定为 10:00:00am，Router 的时钟设定为 11:00:00am。
- 以 Router 作为 NTP 时间服务器，即 Eudemon 主动与 Router 的时钟进行同步。
- 数据包在 Eudemon 和 Router 之间单向传输所需要的时间为 1 秒。

图 3-1 NTP 基本工作原理图



系统时钟同步的过程如下。

1. Eudemon 发送一个 NTP 消息包给 Router，该消息包带有它离开 Eudemon 时的时间戳，该时间戳为 10:00:00am(T1)。
2. 当此 NTP 消息包到达 Router 时，Router 加上自己的时间戳，该时间戳为 11:00:01am (T2)。
3. 当此 NTP 消息包离开 Router 时，Router 再加上自己的时间戳，该时间戳为 11:00:02am(T3)。
4. 当 Eudemon 接收到该响应消息包时，加上一个新的时间戳，该时间戳为 10:00:03am (T4)。

   至此，Eudemon 已经拥有足够的信息来计算两个重要的参数：

   - NTP 消息来回一个周期的时延 Delay=(T4-T1)-(T3-T2)。
   - Eudemon 相对 Router 的时间差 Offset=((T2-T1)+(T3-T4))/2。

   Eudemon 根据这些信息设定自己的时钟，使之与 Router 的时钟同步。

说明

开启 NTP 功能后，运行 NTP 的设备实现时钟同步需要的时间根据网络环境不同而不同。

3.2 配置 NTP 基本功能

通过配置 NTP 基本功能，满足不同情况下的网络时钟同步需求。

3.2.1 配置 NTP 服务器/客户端模式

配置 NTP 服务器/客户端模式下的 NTP 基本功能。

背景信息

本地 Eudemon 作为客户端，工作在 NTP 服务器/客户端模式下。

操作步骤

- 配置 NTP 客户端。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. （可选）执行命令 **ntp-service source-interface** *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]，指定本地发送 NTP 报文的源接口。
  3. 执行命令 **ntp-service unicast-server** *ip-address* [**authentication-keyid** *key-id* | **preference** | **source-interface** *interface-type interface-number* | **version** *number* | **vpn-instance** *vpn-instance-name*] *，指定 NTP 单播服务器。

     当执行命令 **ntp-service source-interface** *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]指定了本地发送 NTP 报文的源接口，又在该步骤中使用参数 **source-interface** 指定了源接口，则优先使用该步骤中指定的源接口。

     ip-address 指定的远程服务器作为本地的时间服务器，是一个主机地址，不能是广播、组播地址。

     说明

     指定单播 NTP 服务器后，本地 Eudemon 自动工作在客户端模式。服务器端除配置 NTP 主时钟外，不需要专门配置。
- （可选）在作为客户端的 Eudemon 上，配置 NTP 服务器的源接口。

1. 在用户视图下执行命令 **system-view**，进入系统视图。
2. 执行命令 **ntp-service source-interface** *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]，指定本地发送 NTP 报文的源接口。

   通常情况下，只需要在客户端指定 NTP 服务器的 IP 地址，客户端和服务器端使用该 NTP 服务器 IP 地址交换 NTP 报文。

   如果在服务器端指定了发送 NTP 报文的源接口，则客户端配置的服务器 IP 地址必须与这个源接口的 IP 地址相同。否则，客户端将无法正确处理服务器发来的 NTP 报文，导致不能同步时钟。

----结束

3.2.2 配置 NTP 对等体模式

配置 NTP 对等体模式下的 NTP 基本功能。

背景信息

本地 Eudemon 作为主动对等体（symmetric active），工作在对等体模式下。

说明

指定了 NTP 对等体后，本地 Eudemon 自动工作在主动对等体模式。被动对等体不需要专门配置。

操作步骤

- 配置 NTP 主动对等体。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. （可选）执行命令 **ntp-service source-interface** *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]，指定本地发送 NTP 报文的源接口。
  3. 执行命令 **ntp-service unicast-peer** *ip-address* [**authentication-keyid** *key-id* | **preference** | **source-interface** *interface-type interface-number* | **version** *number* | **vpn-instance** *vpn-instance-name*] *，指定 NTP 对等体。

     当执行命令 **ntp-service source-interface** *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]指定了本地发送 NTP 报文的源接口，又在该步骤中指定 NTP 对等体时，使用参数 **source-interface** 指定了源接口，则优先使用该步骤中指定的源接口。

     ip-address 指定的远程服务器作为本地的对等体，是一个主机地址，不能是广播、组播地址或参考时钟的 IP 地址。
- （可选）在作为主动对等体的 Eudemon 上，配置 NTP 被动对等体的源接口。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. （可选）执行命令 **ntp-service source-interface** *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]，指定本地发送 NTP 报文的源接口。

     通常情况下，只需要在主动对等体端指定被动对等体的 IP 地址，对等体之间使用此 IP 地址交换 NTP 报文。

     如果在被动对等体端指定了发送 NTP 报文的源接口，则主动对等体端配置的对等体 IP 地址必须与这个源接口的 IP 地址相同，否则，主动对等体将无法正确处理被动对等体发来的 NTP 响应报文。

----结束

3.2.3 配置 NTP 广播模式

配置 NTP 广播模式下的 NTP 基本功能。

操作步骤

- 配置 NTP 广播服务器。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图，即指定发送 NTP 广播包的接口。
  3. 执行命令 **ntp-service broadcast-server** [**authentication-keyid** *key-id* | **version** *number*] *，配置本地 Eudemon 作为 NTP 广播服务器。

     配置完成后，本地 Eudemon 作为广播服务器从指定接口周期性地向广播地址 255.255.255.255 发送时钟同步报文。

     说明

     该配置只能在同一局域网中使用。
- 配置 NTP 广播客户端。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. （可选）执行命令 **ntp-service max-dynamic-sessions** *number*，配置本地允许建立的动态会话数目。

     该配置不影响已经建立的 NTP 会话。当会话数达到或超过允许的最大数目时，不能再建立新的会话。

     缺省情况下，最多允许建立 100 个 NTP 动态会话。
  3. 执行命令 **interface** *interface-type interface-number*，进入接口视图，即指定接收 NTP 广播包的接口。
  4. 执行命令 **ntp-service broadcast-client**，配置本地 Eudemon 作为 NTP 广播客户端。

     配置完成后，本地 Eudemon 作为 NTP 广播客户端，从指定接口侦听服务器发来的 NTP 广播消息包，并对本地时钟同步。

----结束

3.2.4 配置 NTP 组播模式

配置 NTP 组播模式的 NTP 基本功能。

操作步骤

- 配置 NTP 组播服务器。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图，即指定发送 NTP 组播包的接口。
  3. 执行命令 **ntp-service multicast-server** [*ip-address*] [**authentication-keyid** *key-id* | **ttl** *ttl-number* | **version** *number*] *，配置 NTP 组播服务器。

配置完成后，本地 Eudemon 作为组播服务器，从指定接口周期性向组播目的地址 224.0.1.1 发送时钟同步报文。

- 配置 NTP 组播客户端。
  1. 在用户视图下执行命令 **system-view**，进入系统视图。
  2. （可选）执行命令 **ntp-service max-dynamic-sessions** *number*，配置本地允许建立的动态会话数目。

     该配置不影响已经建立的 NTP 会话。当会话数达到或超过允许的最大数目时，不能再建立新的会话。

     缺省情况下，最多允许建立 100 个 NTP 动态会话。
  3. 执行命令 **interface** *interface-type interface-number*，进入接口视图，即指定接收 NTP 组播包的接口。
  4. 执行命令 **ntp-service multicast-client** [*ip-address*]，配置本地 Eudemon 为 NTP 组播客户端。

     配置完成后，本地 Eudemon 作为 NTP 组播客户端，从指定接口侦听服务器发来的 NTP 组播消息包，并对本地时钟同步。

----结束

3.2.5 配置 NTP 主时钟

当使用 Eudemon 提供 NTP 主时钟时，则需要在作为服务器的 Eudemon 上进行该配置。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ntp-service refclock-master** [*ip-address*] [*stratum*]，配置 NTP 主时钟。

ip-address 指本地参考时钟的 IP 地址 127.127.t.u，其中 t 的取值为 1，表示本地参考时钟。u 的取值范围为 0 ～ 3，表示 NTP 的进程号。

当不指定 IP 地址时，默认设置本地时钟 127.127.1.0 为 NTP 主时钟。

----结束

3.2.6 禁止接口接收 NTP 消息

当需要禁止本地 Eudemon 上的某个接口接收 NTP 消息时，则进行该配置。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **ntp-service in-interface disable**，禁止接口接收 NTP 消息。

----结束

3.2.7 配置 NTP 的访问控制权限

NTP 访问控制权限是一种最小限度的安全措施，更安全的方法是配置 NTP 验证。

前提条件

已配置 ACL。

背景信息

Eudemon 提供 4 个等级的访问限制，当 1 个 NTP 访问请求到达本地时，按照最小访问限制到最大访问限制依次匹配，以第 1 个匹配的为准，匹配顺序如下：

- peer（最小访问限制）

  可以对本地 NTP 服务进行时间请求和控制查询，本地时钟也可以同步到远程服务器。
- server

  可以对本地 NTP 服务进行时间请求和控制查询，但本地时钟不会同步到远程服务器。
- synchronization

  只允许对本地 NTP 服务进行时间请求。
- query（最大访问限制）

  只允许对本地 NTP 服务进行控制查询。

可根据实际需求决定在哪台设备上配置 NTP 访问控制权限。具体描述如表 3-1 所示。

表 3-1 配置 NTP 访问控制权限

NTP 工作模式	限制的 NTP 请求类型	进行配置的设备
NTP 服务器/客户端模式	限制客户端同步到服务器端	客户端
	限制服务器端处理客户端的同步时间请求	服务器
NTP 对等体模式	限制两端相互同步	主动对等体端
	限制被动对等体端处理时间请求	被动对等体端
NTP 组播模式	限制客户端同步到服务器端	NTP 组播客户端
NTP 广播模式	限制客户端同步到服务器端	NTP 广播客户端

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ntp-service access** { **peer** | **query** | **server** | **synchronization** } *acl-number*，配置访问本地 Eudemon NTP 服务的控制权限。

----结束

3.2.8 检查配置结果

配置 NTP 基本功能结束后，需要检查配置的正确性。

检查 NTP 基本功能配置结果的相关操作如表 3-2 所示。

表 3-2 检查 NTP 基本功能的配置结果

操作	命令
显示 NTP 服务的状态信息	**display ntp-service status**
显示 NTP 服务维护的 sessions 状态	**display ntp-service sessions** [**verbose**]
显示从本地设备回溯到参考时钟源的各个 NTP 时间服务器的简要信息	**display ntp-service trace**

3.3 配置 NTP 验证功能

在一些对安全性要求较高的网络中，可开启 NTP 协议的验证功能。

3.3.1 启用 NTP 验证

配置 NTP 验证功能时，必须首先启用 NTP 验证。

背景信息

配置 NTP 验证功能可以分为配置客户端的 NTP 验证和配置服务器端的 NTP 验证两个部分。对于 NTP 对等体模式来说，主动对等体相当于客户端，被动对等体相当于服务器端。

在配置 NTP 验证功能时，请注意以下几点：

- NTP 客户端和服务器端都需要启用 NTP 验证功能，否则不能进行有效验证。
- NTP 客户端与服务器端必须配置相同的验证密钥，并声明该密钥可信，否则无法通过验证。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ntp-service authentication enable**，启用 NTP 验证功能。

步骤 3 执行命令 **ntp-service authentication-keyid** *key-id* **authentication-mode md5** *password*，配置 NTP 验证密钥。

步骤 4 执行命令 **ntp-service reliable authentication-keyid** *number*，声明可信的密钥。

----结束

3.3.2 配置 NTP 服务器/客户端模式的验证

在客户端上配置 NTP 服务器/客户端模式的 NTP 验证功能。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ntp-service unicast-server** *ip-address* [**authentication-keyid** *key-id* | **preference** | **source-interface** *interface-type interface-number* | **version** *number* | **vpn-instance** *vpn-instance-name*] *，配置与指定 NTP 服务器同步时钟时使用的密钥 ID。

----结束

3.3.3 配置 NTP 对等体模式的验证

在主动对等体端配置 NTP 对等体模式的 NTP 验证功能。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ntp-service unicast-peer** *ip-address* [**authentication-keyid** *key-id* | **preference** | **source-interface** *interface-type interface-number* | **version** *number* | **vpn-instance** *vpn-instance-name*] *，配置与指定 NTP 对等体同步时钟时使用的密钥 ID。

----结束

3.3.4 配置 NTP 广播模式的验证

在服务器端配置 NTP 广播模式的 NTP 验证功能。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图，即指定发送 NTP 广播包的接口。

步骤 3 执行命令 **ntp-service broadcast-server** [**authentication-keyid** *key-id* | **version** *number*] *，配置本地 Eudemon 作为 NTP 广播服务器时使用的密钥 ID。

客户端的配置与不带验证时相同，具体请参见 **3.2.3 配置 NTP 广播模式**中的相关配置。

----结束

3.3.5 配置 NTP 组播模式的验证

在服务器端配置 NTP 组播模式的 NTP 验证功能。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图，即指定发送 NTP 组播包的接口。

步骤 3 执行命令 **ntp-service multicast-server** [*ip-address*] [**authentication-keyid** *key-id* | **ttl** *ttl-number* | **version** *number*] *，配置本地 Eudemon 作为 NTP 组播服务器时使用的密钥 ID。

客户端的配置与不带验证时相同，具体请参见 **3.2.4 配置 NTP 组播模式**中的相关配置。

----结束

3.3.6 检查配置结果

配置 NTP 验证功能结束后，需要检查配置的正确性。

检查 NTP 验证功能配置结果的相关操作如**表 3-3** 所示。

表 3-3 检查 NTP 验证功能的配置结果

操作	命令
显示 NTP 服务的状态信息	**display ntp-service status**
显示 NTP 服务维护的 sessions 状态	**display ntp-service sessions** [**verbose**]

3.4 调试 NTP

在出现 NTP 运行故障时，请在用户视图下执行 debugging 命令对 NTP 进行调试，查看调试信息，定位故障并分析故障原因。

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

有关 **debugging** 命令的解释请参见《*Quidway Eudemon 8080E/8160E Debugging 参考*》。

操作步骤

步骤 1 在用户视图下执行命令 **terminal monitor**，打开终端显示信息功能。

步骤 2 执行命令 **terminal debugging**，打开终端显示调试信息功能。

步骤 3 执行命令 **debugging ntp-service** { **access** | **adjustment** | **all** | **authentication** | **event** | **filter** | **packet** | **parameter** | **refclock** | **selection** | **synchronization** | **validity** }，打开 NTP 调试开关。

----结束

3.5 配置举例

介绍 NTP 的配置举例。

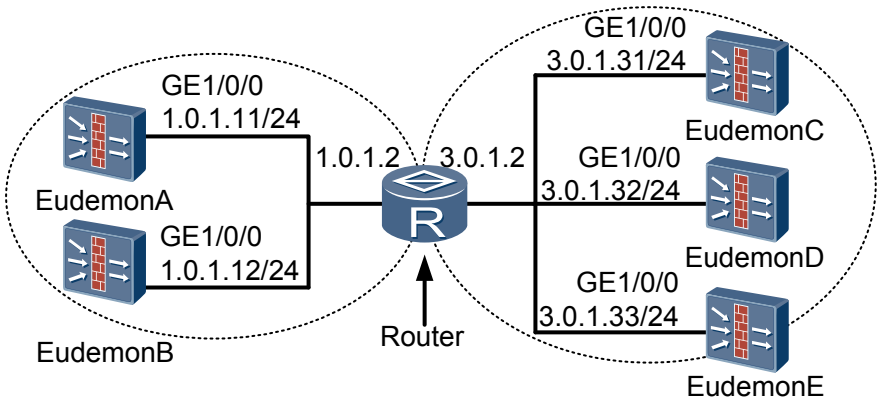
3.5.1 配置 NTP 服务器/客户端模式举例

介绍 NTP 服务器/客户端模式的配置举例。

组网需求

如图 3-2 所示，EudemonA 设置本地时钟作为 NTP 主时钟，层数为 2。EudemonB 以 EudemonA 作为时间服务器，EudemonB 将自己设为客户端模式，EudemonA 自动成为服务器模式。配置完成后 EudemonA 和 EudemonB 完成时钟同步。

图 3-2 NTP 典型配置组网图



数据规划

NTP 服务器/客户端模式配置举例数据规划如表 3-4 所示。

表 3-4 NTP 服务器/客户端模式配置举例数据规划

项目	数据	备注
时间服务器的 IP 地址	1.0.1.11/24	-
NTP 主时钟的层数	2	-

操作步骤

步骤 1 配置 EudemonA 和 EudemonB 的接口 IP 地址，并配置路由可达。具体过程略。

步骤 2 配置 EudemonA 将本地时钟作为 NTP 主时钟。

进入系统视图。

```
<EudemonA> system-view
```

设置本地设备时钟作为 NTP 主时钟，为其他设备提供同步时间，stratum 为 2。

```
[EudemonA] ntp-service refclock-master 2
```

步骤 3 配置 EudemonB。

同步前查看 EudemonB 的 NTP 状态为 unsynchronized。

```
<EudemonB> display ntp-service status
clock status: unsynchronized
clock stratum: 16
reference clock ID: none
nominal frequence: 99.8562 Hz
actual frequence: 99.8562 Hz
clock precision: 2^7
clock offset: 0.0000 ms
root delay: 0.00 ms
root dispersion: 0.00 ms
peer dispersion: 0.00 ms
reference time: 00:00:00.000 UTC Jan 1 1900 (00000000.00000000)
```

进入系统视图。

```
<EudemonB> system-view
```

设置 EudemonA 作为时间服务器。

```
[EudemonB] ntp-service unicast-server 1.0.1.11
```

----结束

结果验证

1. 查看 EudemonB 的 NTP 状态为 synchronized。

```
<EudemonB> display ntp-service status
clock status: synchronized
```

```
clock stratum: 3
reference clock ID: 1.0.1.11
nominal frequence: 250.0000 Hz
actual frequence: 249.9992 Hz
clock precision: 2^19
clock offset: 0.66 ms
root delay: 27.47 ms
root dispersion: 208.39 ms
peer dispersion: 9.63 ms
reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

此时 EudemonB 已经与 EudemonA 同步，层数比 EudemonA 大 1，为 3。

2. 查看 EudemonB 的 NTP 会话信息，EudemonB 与 EudemonA 建立了连接。

```
<EudemonB> display ntp-service sessions
      source      reference    stra reach poll  now offset delay disper
**************************************************************************
[12345]1.0.1.11     LOCAL(0)     2    1     64    6   0.0    16.5  0.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured,
      6 vpn-instance
```

3.5.2 配置 NTP 对等体模式举例

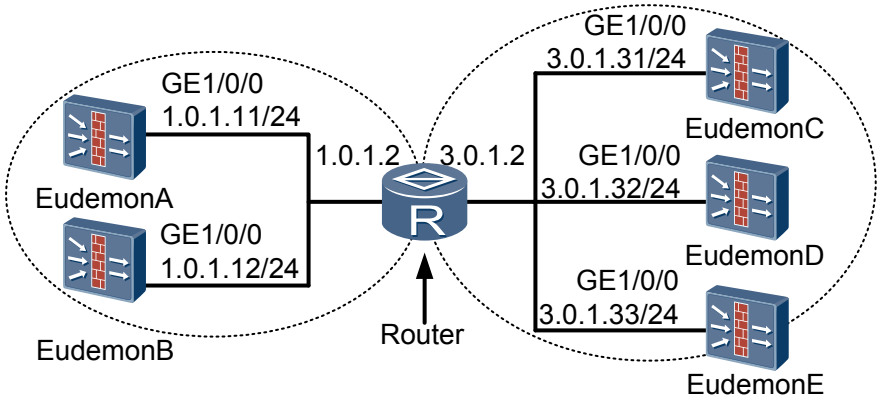
介绍 NTP 对等体模式的配置举例。

组网需求

如图 3-3 所示，EudemonC 本地时钟作为 NTP 主时钟，层数为 2。EudemonD 以 EudemonC 作为时间服务器，将 EudemonC 设为 Server 模式、EudemonD 为 Client 模式。同时，EudemonE 将 EudemonD 设为对等体，EudemonE 为主动对等体模式，EudemonD 为被动对等体模式。

配置完成后，EudemonC 向 EudemonD 提供时钟源，EudemonE 主动向 EudemonD 时钟同步，EudemonC、EudemonD、EudemonE 完成时钟同步。

图 3-3 NTP 典型配置组网图



数据规划

NTP 对等体模式配置举例数据规划如表 3-5 所示。

表 3-5 NTP 对等体模式配置举例数据规划

项目	数据	备注
EudemonC 接口 GigabitEthernet 1/0/0 的 IP 地址。	3.0.1.31/24	-
EudemonD 接口 GigabitEthernet 1/0/0 的 IP 地址。	3.0.1.32/24	-
NTP 主时钟的层数	2	-

操作步骤

步骤 1 配置各 Eudemon 的 IP 地址，具体操作略。

步骤 2 配置 EudemonC 作为 NTP 主时钟。

进入系统视图。

```
<EudemonC> system-view
```

设置本地设备时钟作为 NTP 主时钟，为其他设备提供同步时间，层数为 2。

```
[EudemonC] ntp-service refclock-master 2
```

步骤 3 配置 EudemonD。

进入系统视图。

```
<EudemonD> system-view
```

设置 EudemonC 为时间服务器。

```
[EudemonD] ntp-service unicast-server 3.0.1.31
```

退出系统视图。

```
[EudemonD] quit
```

步骤 4 配置 EudemonE。

进入系统视图。

```
<EudemonE> system-view
```

设置本地时钟作为 NTP 主时钟，层数为 1。

```
[EudemonE] ntp-service refclock-master 1
```

本地时钟同步后，设置 EudemonD 为对等体。

```
[EudemonE] ntp-service unicast-peer 3.0.1.32
```

----结束

结果验证

以上配置将 EudemonD 和 EudemonE 配置为对等体，EudemonE 处于主动对等体模式，EudemonD 处于被动对等体模式，由于 EudemonE 的层数为 1，而 EudemonD 的层数为 2，所以 EudemonD 向 EudemonE 同步。

1. 查看 EudemonD 的 NTP 状态。

```
<EudemonD> display ntp-service status
clock status: synchronized
clock stratum: 2
reference clock ID: 3.0.1.31
nominal frequence: 250.0000 Hz
actual frequence: 249.9992 Hz
clock precision: 2^19
clock offset: 0.66 ms
root delay: 27.47 ms
root dispersion: 208.39 ms
peer dispersion: 9.63 ms
reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

此时 EudemonD 已经与 EudemonE 同步。

2. 查看 EudemonD 的 NTP 会话信息，EudemonD 与 EudemonE 建立了连接。

```
<EudemonD> display ntp-service sessions
      source    reference       stra reach poll  now offset delay disper
********************************************************************************
[12345]3.0.1.31   LOCAL(0)         2   377   64    1   199.53 26.1  9.7
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured,
      6 vpn-instance
```

3.5.3 配置 NTP 广播模式举例

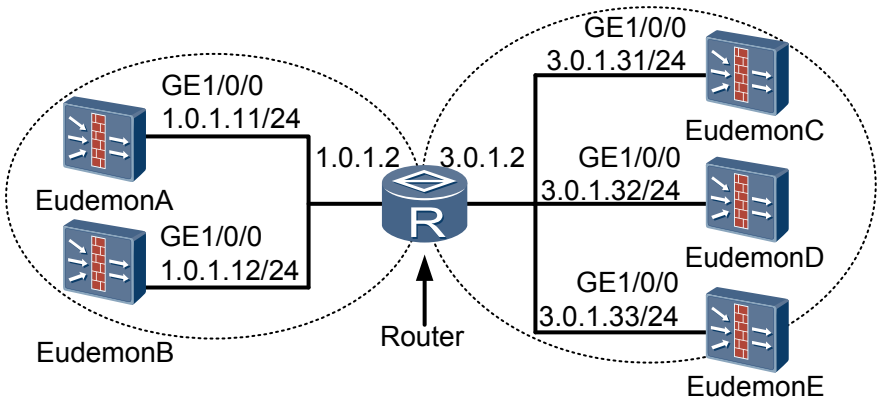
介绍 NTP 广播模式的配置举例。

组网需求

如图 3-4 所示，EudemonC 设置本地时钟作为 NTP 主时钟，层数为 2，并从接口 GigabitEthernet 1/0/0 向外发送广播消息包，设置 EudemonD 和 EudemonA 分别从各自的接口 GigabitEthernet 1/0/0 监听广播消息。

由于 EudemonA 和 EudemonC 不在同一个网段，所以收不到 EudemonC 发出的广播包；而 EudemonD 和 EudemonC 在同一个网段，所以 EudemonD 能够收到 EudemonC 发出的广播包，完成与 EudemonC 的时钟同步。

图 3-4 NTP 典型配置组网图



数据规划

NTP 广播模式配置举例数据规划如表 3-6 所示。

表 3-6 NTP 广播模式配置举例数据规划

项目	数据	备注
EudemonA 接口 GigabitEthernet 1/0/0 的 IP 地址	1.0.1.311/24	-
EudemonC 接口 GigabitEthernet 1/0/0 的 IP 地址	3.0.1.31/24	-
EudemonD 接口 GigabitEthernet 1/0/0 的 IP 地址	3.0.1.32/24	-
NTP 主时钟的层数	2	-

操作步骤

步骤 1 配置 EudemonC。

进入系统视图。

```
<EudemonC> system-view
```

设置本地时钟作为 NTP 主时钟，层数为 2。

```
[EudemonC] ntp-service refclock-master 2
```

进入接口视图。

```
[EudemonC] interface GigabitEthernet 1/0/0
```

在接口视图下设置为广播服务器。

```
[EudemonC-GigabitEthernet1/0/0] ntp-service broadcast-server
```

步骤 2 配置 EudemonD。

进入系统视图。

```
<EudemonD> system-view
```

进入接口视图。

```
[EudemonD] interface GigabitEthernet 1/0/0
```

在接口视图下设置为广播客户端。

```
[EudemonD-GigabitEthernet1/0/0] ntp-service broadcast-client
```

退出接口视图。

```
[EudemonD-GigabitEthernet1/0/0] quit
```

退出系统视图。

```
[EudemonD] quit
```

步骤 3 配置 EudemonA。

进入系统视图。

```
<EudemonA> system-view
```

进入接口视图。

```
[EudemonA] interface GigabitEthernet 1/0/0
```

在接口视图下设置为广播客户端。

```
[EudemonA-GigabitEthernet1/0/0] ntp-service broadcast-client
```

----结束

结果验证

以上配置将 EudemonD 和 EudemonA 配置为从接口 GigabitEthernet 1/0/0 监听广播消息，而 EudemonC 从接口 GigabitEthernet 1/0/0 发送广播消息包，由于 EudemonA 与 EudemonC 不在相同的网段，所以接收不到 EudemonC 发出的广播包，而 EudemonD 接收到 EudemonC 发出的广播包后与其同步。

1. 查看 EudemonD 的 NTP 状态。

```
<EudemonD> display ntp-service status
clock status: synchronized
clock stratum: 3
reference clock ID: 3.0.1.31
nominal frequence: 250.0000 Hz
actual frequence: 249.9992 Hz
clock precision: 2^19
offset: 0.66 ms
root delay: 27.47 ms
root dispersion: 208.39 ms
peer dispersion: 9.63 ms
reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

此时 EudemonD 已经与 EudemonC 同步，层数比 EudemonC 大 1，为 3。

2. 查看 EudemonD 的 NTP 会话信息，可以看到 EudemonD 与 EudemonC 建立了连接。

```
<EudemonD> display ntp-service sessions
        source          reference       stra reach poll  now offset delay disper
**********************************************************************************
[12345]3.0.1.31       LOCAL(0)          3  377    64     1   199.53  0.0      9.7
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured,
       6 vpn-instance
```

3.5.4 配置 NTP 组播模式举例

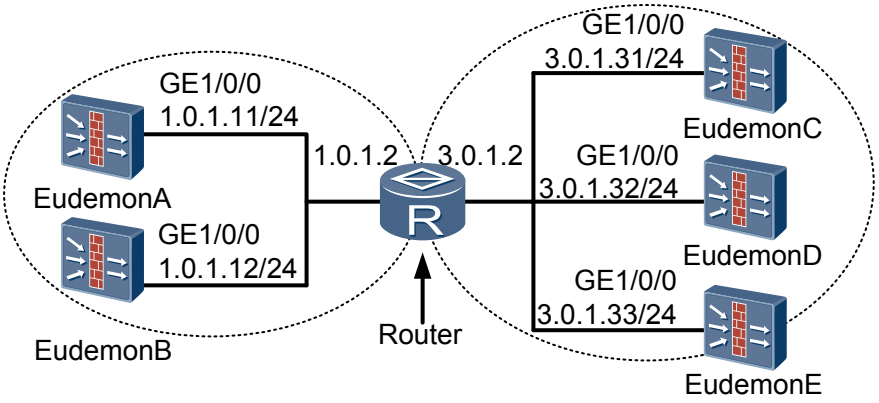
介绍 NTP 组播模式的配置举例。

组网需求

如图 3-5 所示，EudemonC 设置本地时钟作为 NTP 主时钟，层数为 2，并从接口 GigabitEthernet 1/0/0 向外发送组播消息包，设置 EudemonD 和 EudemonA 分别从各自的接口 GigabitEthernet 1/0/0 监听组播消息。

由于 EudemonA 和 EudemonC 不在同一个网段，所以收不到 EudemonC 发出的组播包；而 EudemonD 和 EudemonC 在同一个网段，所以 EudemonD 能够收到 EudemonC 发出的组播包，完成与 EudemonC 的时钟同步。

图 3-5 NTP 典型配置组网图



数据规划

NTP 组播模式配置举例数据规划如表 3-7 所示。

表 3-7 NTP 组播模式配置举例数据规划

项目	数据	备注
EudemonA 接口 GigabitEthernet 1/0/0 的 IP 地址	1.0.1.311/24	-
EudemonC 接口 GigabitEthernet 1/0/0 的 IP 地址	3.0.1.31/24	-
EudemonD 接口 GigabitEthernet 1/0/0 的 IP 地址	3.0.1.32/24	-
NTP 主时钟的层数	2	-

操作步骤

步骤 1 配置 EudemonC。

进入系统视图。

```
<EudemonC> system-view
```

设置本地时钟作为 NTP 主时钟，层数为 2。

```
[EudemonC] ntp-service refclock-master 2
```

进入接口视图。

```
[EudemonC] interface GigabitEthernet 1/0/0
```

设置 EudemonC 为组播服务器。

```
[EudemonC-GigabitEthernet1/0/0] ntp-service multicast-server
```

步骤 2 配置 EudemonD。

进入系统视图。

```
<EudemonD> system-view
```

进入接口视图。

```
[EudemonD] interface GigabitEthernet 1/0/0
```

设置 EudemonD 为组播客户端。

```
[EudemonD-GigabitEthernet1/0/0] ntp-service multicast-client
```

退出接口视图。

```
[EudemonD-GigabitEthernet1/0/0] quit
```

退出系统视图。

```
[EudemonD] quit
```

步骤 3 配置 EudemonA。

进入系统视图。

```
<EudemonA> system-view
```

进入接口视图。

```
[EudemonA] interface GigabitEthernet 1/0/0
```

设置 EudemonA 为组播客户端。

```
[EudemonA-GigabitEthernet1/0/0] ntp-service multicast-client
```

----结束

结果验证

以上配置将 EudemonD 和 EudemonA 配置为从接口 GigabitEthernet 1/0/0 监听组播消息，而 EudemonC 从接口 GigabitEthernet 1/0/0 发送组播消息包，由于 EudemonA 与 EudemonC 不在相同的网段，所以接收不到 EudemonC 发出的组播包，而 EudemonD 接收到 EudemonC 发出的组播包后与其同步。

1. 查看 EudemonD 的 NTP 状态。

```
<EudemonD> display ntp-service status
clock status: synchronized
clock stratum: 3
reference clock ID: 3.0.1.31
nominal frequence: 250.0000 Hz
actual frequence: 249.9992 Hz
clock precision: 2^19
clock offset: 0.66 ms
root delay: 27.47 ms
root dispersion: 208.39 ms
peer dispersion: 9.63 ms
reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

此时 EudemonD 已经与 EudemonC 同步，层数比 EudemonC 大 1，为 3。

2. 查看 EudemonD 的 NTP 会话信息，可以看到 EudemonD 与 EudemonC 建立了连接。

```
<EudemonD> display ntp-service sessions
      source          reference       stra reach poll  now offset delay disper
********************************************************************************
[12345]3.0.1.31       LOCAL(0)          3   377    64     1   199.53  26.1    9.7
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured,
      6 vpn-instance
```

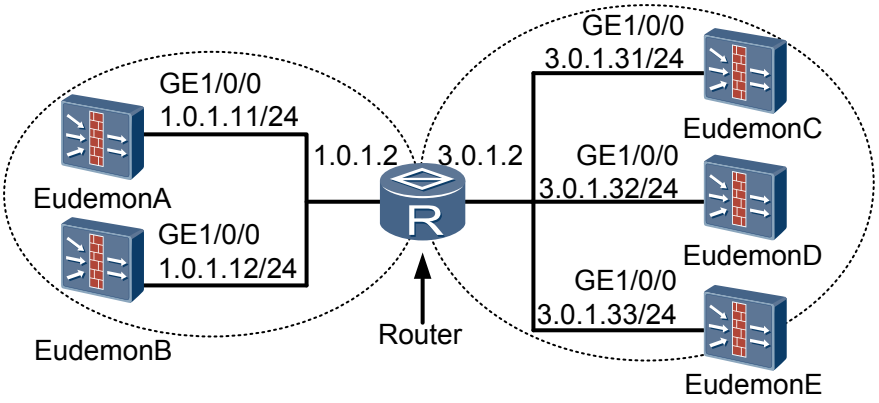
3.5.5 配置带验证的 NTP 服务器/客户端模式举例

介绍带验证的 NTP 服务器/客户端模式的配置举例。

组网需求

如图 3-6 所示，EudemonA 设置本地时钟作为 NTP 主时钟，层数为 2，EudemonB 以 EudemonA 作为时间服务器，同时两端配置 NTP 验证。

图 3-6 NTP 典型配置组网图



数据规划

带验证的 NTP 服务器/客户端模式配置举例数据规划如表 3-8 所示。

表 3-8 带验证的 NTP 服务器/客户端模式配置举例数据规划

项目	数据	备注
NTP 主时钟的层数	2	-
密钥 ID	42	-
密码	aNiceKey	-

操作步骤

步骤 1 配置 EudemonA。

进入系统视图。

```
<EudemonA> system-view
```

设置本地时钟作为 NTP 主时钟，层数为 2。

```
[EudemonA] ntp-service refclock-master 2
```

启动 NTP 身份验证功能。

```
[EudemonA] ntp-service authentication enable
```

设置 MD5 身份验证密钥，密钥 ID 号为 42，密钥为 aNiceKey。

```
[EudemonA] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

指定密钥是可信的。

```
[EudemonA] ntp-service reliable authentication-keyid 42
```

步骤 2 配置 EudemonB。

进入系统视图。

```
<EudemonB> system-view
```

将 EudemonA 作为时间服务器并指定验证 ID。

```
[EudemonB] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

启动 NTP 身份验证功能。

```
[EudemonB] ntp-service authentication enable
```

设置 MD5 身份验证密钥，密钥 ID 号为 42，密钥为 aNiceKey。

```
[EudemonB] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

指定密钥是可信的。

```
[EudemonB] ntp-service reliable authentication-keyid 42
```

退出系统视图。

```
[EudemonB] quit
```

----结束

结果验证

EudemonB 可以向 EudemonA 同步，同步后查看 EudemonB 的 NTP 状态。

```
<EudemonB> display ntp-service status
clock status: synchronized
clock stratum: 3
reference clock ID: 1.0.1.11
nominal frequence: 250.0000 Hz
actual frequence: 249.9992 Hz
clock precision: 2^19
clock offset: 0.66 ms
root delay: 27.47 ms
root dispersion: 208.39 ms
peer dispersion: 9.63 ms
reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

此时 EudemonB 已经与 EudemonA 同步，层数比 EudemonA 大 1，为 3。

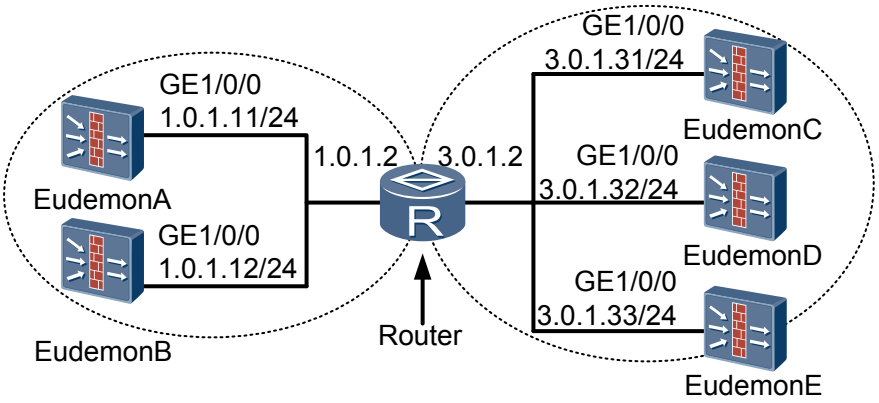
3.5.6 配置带验证的 NTP 广播模式举例

介绍带验证的 NTP 广播模式的配置举例。

组网需求

如图 3-7 所示，EudemonC 设置本地时钟作为 NTP 主时钟，层数为 3，并从接口 GigabitEthernet 1/0/0 向外发送广播消息包，设置 EudemonD 从接口 GigabitEthernet 1/0/0 监听广播消息，同时两端配置 NTP 验证。

图 3-7 NTP 典型配置组网图



数据规划

带验证的 NTP 广播模式配置举例数据规划如表 3-9 所示。

表 3-9 带验证的 NTP 广播模式配置举例数据规划

项目	数据	备注
NTP 主时钟的层数	3	-
密钥 ID	88	-
密码	123456	-

操作步骤

步骤 1 配置 EudemonC。

进入系统视图。

```
<EudemonC> system-view
```

设置本地时钟作为 NTP 主时钟，层数为 3。

```
[EudemonC] ntp-service refclock-master 3
```

启动 NTP 身份验证功能。

```
[EudemonC] ntp-service authentication enable
```

设置 MD5 身份验证密钥，密钥 ID 号为 88，密钥为 123456。

```
[EudemonC] ntp-service authentication-keyid 88 authentication-mode md5 123456
```

指定密钥是可信的。

```
[EudemonC] ntp-service reliable authentication-keyid 88
```

进入接口视图。

```
[EudemonC] interface GigabitEthernet 1/0/0
```

设置本 Eudemon 为 NTP 广播服务器并指定验证 ID。

```
[EudemonC-GigabitEthernet1/0/0] ntp-service broadcast-server authentication-id 88
```

步骤 2 配置 EudemonD。

进入系统视图。

```
<EudemonD> system-view
```

启动 NTP 身份验证功能。

```
[EudemonD] ntp-service authentication enable
```

设置 MD5 身份验证密钥，密钥 ID 号为 88，密钥为 123456。

```
[EudemonD] ntp-service authentication-keyid 88 authentication-mode md5 123456
```

指定密钥是可信的。

```
[EudemonD] ntp-service reliable authentication-keyid 88
```

进入接口视图。

```
[EudemonD] interface GigabitEthernet 1/0/0
```

设置本 Eudemon 为 NTP 广播客户端。

```
[EudemonD-GigabitEthernet1/0/0] ntp-service broadcast-client
```

退出接口视图。

```
[EudemonD-GigabitEthernet1/0/0] quit
```

退出系统视图。

```
[EudemonD] quit
```

----结束

结果验证

以上配置将 EudemonD 配置为从接口 GigabitEthernet 1/0/0 监听广播消息，而 EudemonC 从接口 GigabitEthernet 1/0/0 发送广播消息包，EudemonD 接收到 EudemonC 发出的广播包后与其同步。

查看 EudemonD 的 NTP 状态。

```
<EudemonD> display ntp-service status
clock status: synchronized
clock stratum: 4
reference clock ID: 3.0.1.31
nominal frequency: 250.0000 Hz
```

```
actual frequency: 249.9992 Hz
clock precision: 2^19
clock offset: 198.7425 ms
root delay : 27.47 ms
root disper: 208.39 ms
peer disper: 9.63 ms
reference time: 17:03:32.022 UTC Sep 6 2003(BF422AE4.05AEA86C)
```

此时 EudemonD 已经与 EudemonC 同步，层数比 EudemonC 大 1，为 4。

4 配置 SNMP

关于本章

通过配置 SNMP，可以检查设备性能，收集网络状态信息，并且对设备进行管理。

4.1 简介
介绍 SNMP 的基本概念、报文格式、工作机制，以及 MIB 的概念和设备支持的 MIB 种类。

4.2 配置 SNMP
配置 SNMP 功能后，网管系统可以对设备进行访问和管理。

4.3 配置 Trap 功能
Trap 是未经请求被管理设备主动向 NMS 发送的信息，用于报告紧急的重要事件。被管理设备必须配置 Trap 功能后才会主动发送这些信息。

4.4 配置接口索引固定功能
在需要使用接口索引作为计费的依据，要求接口的索引值必须固定的应用环境中，可以配置接口索引固定功能。

4.5 维护 SNMP
在 SNMP 运行出现故障时，可在用户视图下执行 **debugging** 命令进行调试，查看调试信息，定位故障并分析故障原因。

4.6 配置举例
介绍 SNMP 的配置举例。

4.1 简介

介绍 SNMP 的基本概念、报文格式、工作机制，以及 MIB 的概念和设备支持的 MIB 种类。

4.1.1 SNMP 概述

介绍 SNMP 的基本概念。

简单网络管理协议 SNMP（Simple Network Management Protocol）是规定 NMS（Network Management System）和 Agent 之间传递管理信息的应用层协议。

SNMP 具有以下特点：

- 查看网络状况进行网络管理。

  网络管理员能够对网络上的任何节点检索信息，进行修改，寻找故障，完成故障诊断，容量规划和生成报告。
- 使用 UDP（User Datagram Protocol）传输协议，受到许多产品的广泛支持。
- 采用轮询机制，按照一定的时间间隔收集数据，获得有关设备和网络性能的情况，有助于排除故障。

4.1.2 SNMP 报文

介绍 SNMP 的报文种类和报文格式。

类型

SNMP 定义了 5 种报文类型用于进行 SNMP 操作，具体报文类型如**表 4-1** 所示。

表 4-1 SNMP 报文类型

类型	说明
GetRequest	包含 NMS 希望从 Agent 的 MIB（Management Information Base）中读取值的一个或多个变量列表。
GetNextRequest	提供了一种连续读一个 MIB 的多个变量的方法。
SetRequest	用于设置一个或多个变量的值。

类型	说明
GetResponse	用于发送对上述三种请求报文的响应报文。
Trap	允许被管对象主动发送某些不经请求的信息，用于报告重要事件。

格式

SNMP 报文格式如图 4-1 所示。

图 4-1 SNMP 报文格式

与 SNMP 定义的 5 种报文类型相对应，其中的协议数据单元 PDU（Protocol Data Unit）也有以下五种：

- GetRequest-PDU
- GetNextRequest-PDU
- GetResponse-PDU
- SetRequest-PDU
- Trap-PDU

4.1.3 SNMP 工作机制

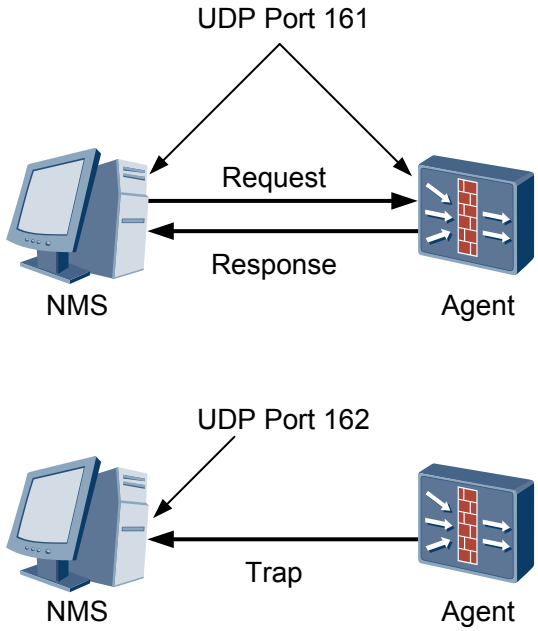
介绍 SNMP 的工作机制。

结构

SNMP 的结构如图 4-2 所示，分为 NMS 和 Agent 两部分：

- NMS 是运行客户端程序的工作站，实现以下功能。
  - 向网络设备发送各种 Request 报文。
  - 接收来自被管理设备的 Response 报文及 Trap 报文，并显示结果。
- Agent 是驻留在被管理设备上的一个进程，实现以下功能。
  - 接收、处理来自网管站的 Request 报文。
  - 根据报文类型对管理变量进行 Read 或 Write 操作，并生成 Response 报文，返回给 NMS。
  - 根据各协议模块对触发条件的定义，在达到触发条件后，如进入、退出系统视图设备重新启动等，相应的模块通过 Agent 主动向 NMS 发送 Trap 报文，报告所发生的事件。

图 4-2 SNMP 结构示意图

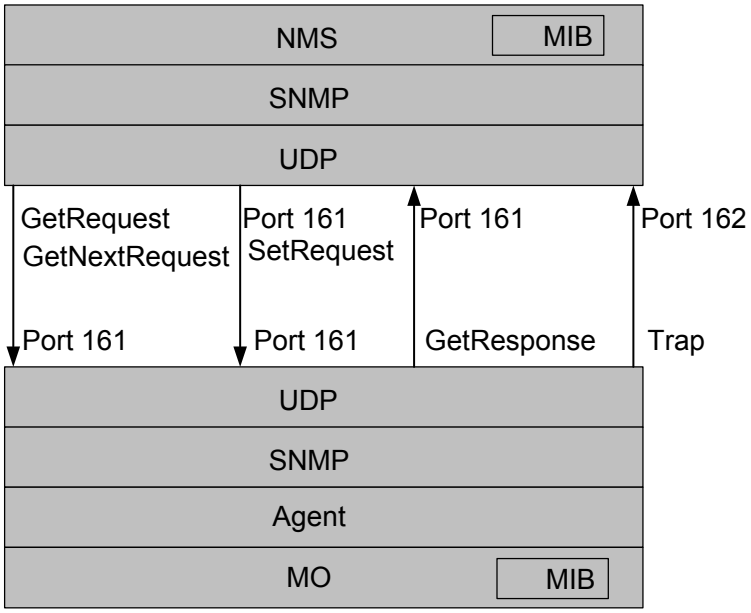


运行过程

SNMP 协议运行过程如下。

1. NMS 向被管理设备发送各种请求报文。每个 SNMP 报文被封装成一个 UDP 数据报文发送出去。
2. 驻留在被管理设备上的 Agent 从设备的 161 端口接收来自 NMS 的 UDP 请求报文，经解码、团体名认证，分析得到管理变量在 MIB（Management Information Base）中对应的节点，从相应的模块中得到管理变量的值，再形成响应报文，编码发送回 NMS。
3. NMS 从 161 端口得到 UDP 响应报文后（Trap 报文从第 162 号端口接收），再经同样的处理，最终显示出结果。如图 4-3 所示。

图 4-3 SNMP 协议运行过程



4.1.4 MIB

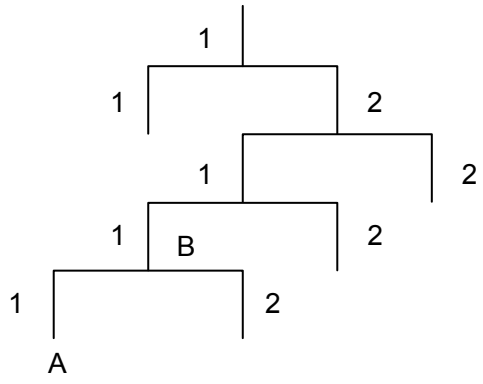
介绍 MIB 的概念。

结构

为了在 SNMP 报文中唯一标识设备中的管理变量，SNMP 通过 MIB（Management Information Base）来识别管理对象。

MIB 是树层次结构如图 4-4 所示，它是监控的网络设备标准变量的集合，它能够唯一确定管理对象。例如，图 4-4 中管理对象 B 可以用一串数字 { 1.2.1.1 } 唯一确定。

图 4-4 MIB 树结构



Eudemon 支持的 MIB

目前 Eudemon 的 SNMP Agent 支持 SNMP v3，兼容 SNMP v1、SNMP v2c，其支持的 MIB 如表 4-2 所示。

表 4-2 系统支持的 MIB

MIB 属性	MIB 内容	所遵循的标准或规格说明
公有 MIB	基于 TCP/IP 网络设备的 MIB II	RFC 1213
	RIP-2 MIB	RFC 1724
	以太网 MIB	RFC 2665，RFC 2668
	PPP MIB	RFC 1471，RFC 1473
	OSPF MIB	RFC 1253
	IF MIB	RFC 1573
	SNMPV2 MIB	RFC 1907
	Framework MIB	RFC 2571
	Usm MIB	RFC 2573
	Mpd MIB	RFC 2572
	Vacm MIB	RFC 2275
	Target MIB	RFC 2273
	Notification MIB	RFC 2273
	RADIUS MIB	RFC 2618，RFC 2620
私有 MIB	性能告警 MIB	-
	设备面板 MIB	-
	设备资源 MIB	-
	QoS	-
	配置管理 MIB	-
	系统管理 MIB	-

4.2 配置 SNMP

配置 SNMP 功能后，网管系统可以对设备进行访问和管理。

4.2.1 配置基本 SNMP Agent 功能
介绍开启 SNMP Agent 功能、配置管理员联络方法、配置设备位置以及配置本地 SNMP 实体引擎 ID 的过程。

4.2.2 配置团体名
介绍团体名的配置过程，以及基于 ACL 和 MIB 视图进行访问控制。

4.2.3 配置 SNMP 组和用户
介绍 SNMP 组和用户的配置过程，以及通过配置相应的访问控制列表，允许指定组的内的用户可以对设备进行管理，同时通过认证和加密实现安全性。

4.2.1 配置基本 SNMP Agent 功能

介绍开启 SNMP Agent 功能、配置管理员联络方法、配置设备位置以及配置本地 SNMP 实体引擎 ID 的过程。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent**，启动 SNMP Agent 服务。

步骤 3 执行命令 **snmp-agent sys-info version** { { **v1** | **v2c** | **v3** } * | **all** }，配置 SNMP 协议的版本。

步骤 4 （可选）执行命令 **snmp-agent sys-info contact** *syscontact*，配置管理员联络方法。

步骤 5 （可选）执行命令 **snmp-agent sys-info location** *syslocation*，配置设备位置。

步骤 6 执行命令 **snmp-agent local-engineid** *engineid*，配置本地 SNMP 实体的引擎 ID。

Engineid（十六进制数字串）缺省为公司的企业号+设备信息。设备信息可以是 IP 地址、MAC（Medium Access Control）地址或自己定义的十六进制数字串。

对于 SNMP Agent v3，启动 SNMP Agent 服务后，系统会自动配置本地 SNMP 实体引擎 ID 和 SNMP 协议版本。

----结束

4.2.2 配置团体名

介绍团体名的配置过程，以及基于 ACL 和 MIB 视图进行访问控制。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent community** { **read** | **write** } *community-name* [**acl** *acl-number* | **mib-view** *view-name*] *，设置团体名及访问权限。

----结束

4.2.3 配置 SNMP 组和用户

介绍 SNMP 组和用户的配置过程，以及通过配置相应的访问控制列表，允许指定组的内的用户可以对设备进行管理，同时通过认证和加密实现安全性。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]，配置 SNMP v3 组。

步骤 3 执行命令 **snmp-agent usm-user v3** *user-name group-name* [**authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode des56** *priv-password*]] [**acl** *acl-number*]，为 SNMP v3 组添加一个新用户。

----结束

4.2.4 配置 MIB 视图信息

介绍 MIB 视图信息的配置过程，可以基于 MIB 视图进行访问控制。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent mib-view** { **included** | **excluded** } *view-name oid-tree*，配置 MIB 视图信息。

----结束

4.2.5 配置 SNMP 报文的最大尺寸

通过加大 SNMP 报文的最大传输单元的尺寸，来解决网管端查询设备端状态信息时，只能得到部分的信息的情况。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent packet max-size** *byte-count*，配置 Agent 接收/发送的 SNMP 消息包的最大值。

----结束

4.2.6 检查配置结果

配置 SNMP 功能结束后，需要检查配置的正确性。

检查 SNMP Agent 配置结果的相关操作如**表 4-3** 所示。

表 4-3 检查 SNMP Agent 配置结果

操作	命令
显示 SNMP 报文统计信息	**display snmp-agent statistics**
显示当前设备的引擎 ID	**display snmp-agent** { **local-engineid** | **remote-engineid** }

操作	命令
显示 Eudemon 上的组名、安全模式、各种视图的状态以及各组存储方式的信息	**display snmp-agent group** [*group-name*]
显示组用户名表中所有 SNMP v3 用户名称的信息	**display snmp-agent usm-user** [**engineid** *engine-id* | **username** *user-name* | **group** *group-name*] *
显示当前配置的团体名	**display snmp-agent community** [**read** | **write**]
显示当前配置的 MIB 视图	**display snmp-agent mib-view** [**exclude** | **include** | **viewname** *view-name*]
显示系统维护联络信息字符串	**display snmp-agent sys-info contact**
显示系统位置字符串	**display snmp-agent sys-info location**
显示 SNMP 的版本信息	**display snmp-agent sys-info version**

4.3 配置 Trap 功能

Trap 是未经请求被管理设备主动向 NMS 发送的信息，用于报告紧急的重要事件。被管理设备必须配置 Trap 功能后才会主动发送这些信息。

4.3.1 配置 Trap 报文发送功能

开启 Trap 报文发送功能后，设备将会主动向网管系统发送 Trap 信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent trap enable** [*trap-type* [*trap-list*]]，配置 Trap 报文发送功能。

此命令中如果不带参数，表示允许发送所有模块的所有类型的 Trap 报文。

----结束

4.3.2 配置 Trap 目标主机

设置 Trap 目标主机的 IP 地址，接受设备发送的 Trap 信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent target-host trap address udp-domain** *ip-address* [**udp-port** *port-number*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]，设置 Trap 主机。

----结束

4.3.3 配置 Trap 报文的源接口

设备端配置的 Trap 报文的源接口和网管端配置的设备发送报文的接口需要一致，否则会引起网管端无法接受 Trap 报文的情况。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent trap source** *interface-type interface-number*，指定发送 Trap 报文的源接口。

----结束

4.3.4 配置 Trap 报文的队列长度

在设备发送 Trap 信息比较频繁时，可以将 Trap 队列长度调大，减少告警丢失的发生。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent trap queue-size** *size*，设置 Trap 报文的队列长度。

----结束

4.3.5 配置 Trap 报文的保存时间

在设备发送 Trap 信息比较频繁时，可以减少报文的保存时间。

背景信息

应根据实际需要配置 Trap 报文的保存时间，超过保存时间的 Trap 报文都将被丢弃。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent trap life** *seconds*，配置 Trap 报文的保存时间。

----结束

4.3.6 配置 Trap 报文的会话告警阈值

当设备的会话数达到告警阈值时，设备将向网管发送 Trap 报文。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent session trap threshold** *threshold-value*，配置 Trap 报文的会话告警阈值。

----结束

操作结果

任意视图下执行命令 **display snmp-agent session trap threshold** ，可以查看当前所配置的 CPU 会话告警阈值。

4.4 配置接口索引固定功能

在需要使用接口索引作为计费的依据，要求接口的索引值必须固定的应用环境中，可以配置接口索引固定功能。

4.4.1 开启接口索引固定功能

介绍开启接口索引固定功能的过程。

背景信息

说明

在插拔接口板或系统重启前，必须使用 **save** 命令保存当前接口索引的映像文件，否则可能会引起接口索引改变。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ifindex constant**，开启接口索引固定功能。

----结束

4.4.2 配置索引固定的接口最大数量

介绍设置索引固定的接口最大数量的过程。

背景信息

为了保证接口索引文件不超过预期的大小，可以设置索引固定的接口最大数量。设置该最大数量后，可以防止接口索引文件因为系统运行，频繁增删接口变得很大，占用过多的系统资源。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **set constant-ifindex max-number** *number*，设置索引固定的接口最大数量。

----结束

4.4.3 配置子接口索引的内存分配模式

介绍设置子接口索引的内存分配模式的过程。

背景信息

当新建子接口时，系统会在内存中按照特定的方式生成子接口的索引映像文件。为了适应不同的情况，可以按照以下情况设置子接口索引的内存分配模式：

- 松散模式
  子接口编号不连续时选用。
- 紧凑模式
  子接口编号连续时选用。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **set constant-ifindex subinterface** { **dense-mode** | **sparse-mode** }，配置子接口索引的内存分配模式。

----结束

4.4.4 检查配置结果

配置接口索引固定功能结束后，需要检查配置的正确性。

检查接口索引配置结果的相关操作如表 4-4 所示。

表 4-4 检查接口索引配置结果

操作	命令
显示接口索引固定的状态和配置信息	**display constant-ifindex configuration**

4.5 维护 SNMP

在 SNMP 运行出现故障时，可在用户视图下执行 **debugging** 命令进行调试，查看调试信息，定位故障并分析故障原因。

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭所有调试开关。

有关 **debugging** 命令的解释请参见《*Quidway Eudemon 8080E/8160E 命令参考*》。

SNMP 维护相关命令如表 4-5 所示。

表 4-5 SNMP 维护命令

操作	命令
打开 SNMP 调试开关	**debugging snmp-agent** { **header** | **packet** | **process** | **trap** }

4.6 配置举例

介绍 SNMP 的配置举例。

组网需求

如图 4-5 所示，要求网管工作站（NMS）与 Eudemon 通过 IP 网络相连，网管工作站 IP 地址为 129.102.149.23，Eudemon 以太网口 IP 地址为 129.102.0.1。

图 4-5 配置 SNMP 组网图

配置思路

首先在 Eudemon 上启动 SNMP Agent，配置 SNMP 版本，设备团体名和访问权限，设置管理员联系方法、Eudemon 物理位置和主机名，配置 Trap 功能。最后配置网管理工作站。

数据准备

为完成此配置例，需准备如下的数据：

- SNMP 版本
- 团体名及权限
- 管理员信息

操作步骤

步骤 1 配置 Eudemon。

进入系统视图。

```
<Eudemon> system-view
```

启动 SNMP Agent，配置版本为 SNMP V1。

```
[Eudemon] snmp-agent sys-info version v1
```

设置团体名为 public，并且允许使用该团体名进行只读访问。

```
[Eudemon] snmp-agent community read public
```

设置团体名为 private，并且允许使用该团体名进行只写访问。

```
[Eudemon] snmp-agent community write private
```

设置管理员联系方法、Eudemon 物理位置和主机名。

```
[Eudemon] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Eudemon] snmp-agent sys-info location telephone-closet,3rd-floor
[Eudemon] sysname sysadm
```

使能 Trap 功能。

```
[sysadm] snmp-agent trap enable
```

允许向 129.102.149.23 发送 SNMP Trap 报文，使用团体名 public。

```
[sysadm] snmp-agent target-host trap address udp-domain 129.102.149.23 params securityname public
```

步骤 2 配置 NMS。

请参考所使用 NMS 的相关文档。

----结束

5 配置 RMON 和 RMON2

关于本章

通过配置 ROMAN 和 ROMAN2，实现对网络中的数据流量进行监控和统计。

5.1 RMON 和 RMON2 简介

RMON 主要实现对一个网段或者整个网络中的数据流量的监视功能，RMON2 则是 RMON 的简单扩充。

概述

远程监控 RMON（Remote Monitoring）是目前应用相当广泛的网络管理标准之一，是 Internet 工程任务组 IETF（Internet Engineering Task Force）定义的一种管理信息库 MIB（Management Information Base），是对 MIB II 标准最重要的增强。

采用 RMON 能够减少 NMS（Network Management System）同 Agent 间的通讯流量，主动有效地监控管理网络。

RMON 原理

说明

目前 Eudemon 只能对网络设备的千兆以太网接口和百兆以太网接口进行监控和统计。

RMON 完全基于简单网络管理协议 SNMP（Simple Network Management Protocol）体系结构，与现存的 SNMP 框架相兼容，包括网管系统 NMS 和运行在各网络设备上的 Agent 两部分：

- NMS

  从 Agent 获取管理信息并控制网络资源。
- Agent

  对网络中的各种流量信息进行跟踪统计。如某段时间内某网段上的报文总数，或发往某台主机的正确报文总数等。

RMON 允许有多个 NMS，可用以下两种方法收集数据：

- 专用 RMON Probe（探测仪）

  NMS 直接从 RMON Probe 获取管理信息并控制网络资源。该方式能够获取 RMON MIB 的全部信息。
- RMON Agent 嵌入网络设备

  将 RMON Agent 直接嵌入网络设备中，使之成为带 RMON Probe 功能的网络设备。该方式受设备资源限制，一般不能获取 RMON MIB 的所有数据，大多数只收集四个组（告警、事件、历史和统计）的信息。

Eudemon 为节约系统资源，每个 RMON Agent 中表格的表项都有自己的生存时间。生存时间指当行状态为有效状态 Valid 时，此行可以存在的时间。如果某行一直处于 invalid 状态，其生存时间将递减，当生存时间为零时，此行被删除。各表项的容量和最大生存时间如表 5-1 所示。

表 5-1 RMON Agent 各表的生存时间

表名称	表项容量	最大生存时间（s）
统计表	100	600
历史控制表	100	600

表名称	表项容量	最大生存时间（s）
告警表	60	6000
事件表	60	600
日志表	600	-
扩展告警表	50	6000

说明

日志表没有最大生存时间，日志事件行对应的日志最多可以为 10 条，超过 10 条将循环覆盖。

Eudemon RMON 的实现

Eudemon 将 RMON Agent 模块直接嵌入网络设备中，与其它模块形成一个完整的系统。

Eudemon 支持 RFC 2819 规定的统计、历史、告警和事件四个组以及华为公司规定的私有扩展告警组（Performance-MIB）：

- 统计组

  统计组统计以下监控子网的基本信息，它包含一个以太网统计表（etherStatsTable）。

  - 网段的流量
  - 各种类型包的分布
  - 各种类型错误帧数
  - 碰撞次数等

  说明

  RMON 统计结果与 **display interface** 的结果不完全一致，两者虽然都是从底层获取数据，但 RMON 搜集的信息更全面。

- 历史组

  历史组定期地收集网络状态统计信息并存储起来，以便后续的处理。它包含以下两个表。

  - 历史控制表（historyControlTable）

    主要设置采样间隔时间等控制信息。

  - 以太网历史表（etherHistoryTable）

    提供网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。历史控制表中的每一控制项在以太网历史表中最多可以有 10 条对应的历史数据，超过指定条数后循环覆盖。

- 告警组

  告警组针对告警变量（可以是本地 MIB 的任意对象）预先定义一组阈值，如果采样数据在相应的方向上越过阈值（不管是初次还是再次越过），监视器就记录日志或者把告警发往网管站。告警组包括一个告警表（alarmTable）。

- 事件组

  事件组提供关于 RMON Agent 所产生的所有事件的表。当 RMON Agent 发生某事件时，Eudemon 记录该事件的日志或发送 Trap 到网管站。

事件组主要实现 Log、Trap 以及 Log-Trap 三种事件输出，每个日志事件行对应的日志最多可以为 10 条，超过 10 条将循环覆盖。

事件组包括事件表（eventTable）和日志表（logTable）。

- 扩展告警组

  扩展告警组在 RFC 2819 基础上增加了可以用表达式来设定告警对象和告警生存时间的功能。它包括一个扩展告警表（prialarmTable）。

RMON2 简介

RMON2 是 RMON MIB 规范的一部分，是原始 RMON 的简单扩充，添加了一些新的组。最初 RMON 只是监视 MAC 层的协议流量，扩展到 RMON2 后可以监视 MAC 层以上的协议流量。这里的 MAC 层指数据链路层，RMON 和 RMON2 都是针对于以太网链路的监控。

RMON2 从 OSI（Open Systems Interconnection）模型第 3 层到第 7 层对数据包进行解码。它有两个重要的含义：

- RMON2 Agent 能基于网络层协议和地址来监视流量，能够看到与之相连的外部 LAN（Local Area Network）网段，查看通过 Eudemon 进入 LAN 的流量。
- RMON2 Agent 可以对应用程序流量解码和监视（例如 E-mail、FTP 和 WWW 协议），能够记录进出特定应用程序的流量。

在 Eudemon 的实现中，目前 RMON2 只支持两个 MIB 组：protocolDir 和 nlHost。其中 nlHost 只支持网络层主机组，不支持应用层主机组，即不实现主机控制表中对应用层主机组的控制部分和 alHostTable 表，因此在协议目录组中只能设置 IP 协议，设置其它协议是无效的。

5.2 配置 RMON

通过配置 RMON，对某一网段的网络状况进行监控和流量统计。

5.2.1 开启 RMON 统计功能
在需要进行流量统计的接口上开启 RMON 统计功能，否则 RMON 统计表和历史表采集的统计值为零。

5.2.2 配置统计表
在需要进行流量统计的接口上配置统计表。

5.2.3 配置历史控制表
在需要进行流量统计的接口上配置历史控制表。

5.2.4 配置事件表
在需要进行监控的设备上配置事件表。

5.2.5 配置告警表
在需要进行监控的设备上配置告警表。

5.2.6 配置扩展告警表
在被监控的设备上配置扩展告警表。

5.2.7 检查配置结果
配置 RMON 结束后，需要检查配置的正确性。

5.2.1 开启 RMON 统计功能

在需要进行流量统计的接口上开启 RMON 统计功能，否则 RMON 统计表和历史表采集的统计值为零。

前提条件

- 配置接口的参数。
- 配置 SNMP 基本功能。

背景信息

RMON 功能可以根据实际需要选择以下启动方式：

- 预先启动。
- 在怀疑某个接口所连接的子网的流量有异常时启动。

RMON 功能推荐的启动方法如下：

- 预先配置好统计表。
- 对流量有异常的端口配置两条历史控制策略。
- 对某项指标或某几项指标有怀疑时进行告警配置。

说明

RMON 只能提供一些流量统计和异常等信息，并不能防止这些异常情况；要消除异常情况需要通过其它管理手段。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface GigabitEthernet** *interface-number*，进入接口视图。

步骤 3 执行命令 **rmon-statistics enable**，开启接口的 RMON 统计功能。

----结束

5.2.2 配置统计表

在需要进行流量统计的接口上配置统计表。

背景信息

用户在监控接口的统计信息时，需要为相应的接口在统计表中创建一行，给出接口的 OID（Object Identifier）、行的索引和行的状态。此后，用户可以用读取本行的方式获取最新的统计数据。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface gigabitethernet** *interface-number*，进入接口视图。

步骤 3 执行命令 **rmon statistics** *entry-number* [**owner** *text-string*]，配置统计表。

----结束

5.2.3 配置历史控制表

在需要进行流量统计的接口上配置历史控制表。

背景信息

历史数据管理功能可以设定对某个接口进行采样、保存数量和采样参数（时间间隔），定期对指定的端口进行数据采集并将采集到的信息保存到历史表中以备查看。

RMON 规范建议每个被监视的接口要有两个历史控制条目以上：一个历史控制条目设置为 30 秒取样一次，使监视器能够探测流量模式的突变；另一个历史控制条目设置为 30 分钟取样一次，监视接口的稳定状态行为。短周期取样使监视器能够探测到流量模式的突变，长周期取样则监视接口的稳定状态行为。

说明

- 为了减少 RMON 对系统性能的影响，历史表的采样间隔应在 10 秒以上，且不要对同一端口配置过多的历史控制表项和告警表项。
- Eudemon 为每个历史控制条目最多保留 10 条最近的记录。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface GigabitEthernet** *interface-number*，进入接口视图。

步骤 3 执行命令 **rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *owner-name*]，配置历史控制表。

----结束

5.2.4 配置事件表

在需要进行监控的设备上配置事件表。

背景信息

RMON 事件管理在事件表的指定行添加事件，并定义事件的处理方式：

- log
  只发送日志。
- log-trap
  发送日志同时也向 NMS 发送 Trap 消息。
- none
  标记为没有事件发生。
- trap
  只向 NMS 发送 Trap 消息。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rmon event** *entry-number* [**description** *string*] { **log** | **log-trap** *object* | **none** | **trap** *object* } [**owner** *owner-name*]，配置事件表。

----结束

5.2.5 配置告警表

在需要进行监控的设备上配置告警表。

背景信息

RMON 告警管理可以按照指定的采样间隔对指定的告警变量（用此变量的 OID 指定）进行监视，当被监视数据的值越过定义的阈值时会产生告警事件。事件通常会记录在设备的日志表中，或向 NMS 发送 Trap。

如果告警上限和下限所对应事件（event-entry1、event-entry2）在事件表中均没有配置，即使达到了告警条件也不会产生告警（此时告警记录的状态为 undercreation，不是有效状态 valid）。只要事件表中配置了上限和下限其中一个事件，符合条件便会触发相应的告警（告警记录的状态为 valid）。

如果告警变量设置错误，例如设置成一个不存在的 OID，告警记录的状态也为 undercreation，不会正常告警。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rmon alarm** *entry-number alarm-OID sampling-time* { **absolute** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *owner-name*]，配置告警表。

----结束

5.2.6 配置扩展告警表

在被监控的设备上配置扩展告警表。

背景信息

在 RFC 2819 的告警表基础上，RMON 扩展告警管理增加了用表达式设定告警对象的功能，并且可以限定扩展告警行的总生存时间。

扩展告警表比告警表多了以下几项：

- 告警变量的表达式字符串
  可以是若干简单告警变量 OID 组成的四则表达式（＋，－，*，/和小括号）。
- 扩展告警行的描述字符串
- 扩展告警状态周期
  必须大于采样间隔，单位为秒。

- 扩展告警状态类型

  包括两种类型：永远（Forever）和限定时间（cycle）。对于 cycle 类型，当经过了扩展告警状态周期指定时间后，不再产生告警并且 cycle 类型扩展告警表的此表行被删除。

如果告警上限和下限所对应事件（event-entry1、event-entry2）在事件表中均没有配置，即使达到了告警条件也不会产生告警（此时告警记录的状态为 undercreation，不是有效状态 valid）。只要事件表中配置了上限和下限其中一个事件，符合条件便会触发相应的告警（告警记录的状态为 valid）。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rmon prialarm** *entry-number prialarm-formula description-string sampling-interval* { **absolute** | **changeratio** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **entrytype** { **cycle** *entry-period* | **forever** } [**owner** *text-string*]，配置扩展告警表。

----结束

5.2.7 检查配置结果

配置 RMON 结束后，需要检查配置的正确性。

检查 RMON 配置结果的相关操作如表 5-2 所示。

表 5-2 检查 RMON 配置结果

操作	命令
显示 RMON 统计消息	**display rmon statistics** [**GigabitEthernet** *interface-number*]
显示 RMON 历史信息	**display rmon history** [**Gigabitethernet** *interface-number*]
显示 RMON 告警信息	**display rmon alarm** [*entry-number*]
显示 RMON 事件	**display rmon event** [*entry-number*]
显示 RMON 事件日志	**display rmon eventlog** [*entry-number*]
显示 RMON 扩展告警表	**display rmon prialarm** [*entry-number*]

5.3 配置 RMON2

通过配置 ROMAN2，可以对网络上某一接口进行流量监控，分析所有进出该接口的数据流向，并分别统计每台主机流经该接口的数据。

5.3.1 配置主机控制表
在被监控的设备上配置主机控制表。

5.3.2 配置协议目录表

在被监控的设备配置协议目录表。

5.3.3 检查配置结果
配置 RMON2 结束后，需要检查配置的正确性。

5.3.1 配置主机控制表

在被监控的设备上配置主机控制表。

前提条件

配置以太网接口的参数。

背景信息

对某一个接口进行流量统计，必须创建该接口的主机控制表条目。

索引用来判断是创建一个条目还是对已存在的条目进行修改。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rmon2 hlhostcontroltable index** *ctrl-index* [**datasource interface** *interface-type interface-num*] [**maxentry** *maxentry-value*] [**owner** *owner-name*] [**status** { **active** | **inactive** }]，配置主机控制表。

进行该配置时需注意：

- 创建条目时必须配置参数 **datasource interface**（即 hlHostControlDataSource）。每个接口在主机控制表中只能创建一行条目，不能重复创建。
- 当设置 hlHostControlStatus 的值为 **inactive** 时，会自动删除主机表中所有与其相关的条目。
- 当 hlHostControlStatus 的值为 **active** 时，不能修改 hlHostControlDataSource 和 hlHostControlNlMaxDesiredEntries（主机表的最大条目数）的值。
- 当 hlHostControlDataSource 对应的接口状态为 Down 时，如果 hlHostControlStatus 的值是 **active**，则会自动转换为 **notinservice**，在命令行下显示为 Plug-out 状态，在 NMS 上看到的状态为 notinservice。此时该行不允许用户修改，只能被删除。当接口状态变为 UP 时，主机控制表的状态又将恢复为 **active**。
- 当某行中 hlHostControlDataSource 对应的接口被删除时，该行也被删除。

----结束

5.3.2 配置协议目录表

在被监控的设备配置协议目录表。

前提条件

配置以太网接口的参数。

背景信息

目前 RMON2 只支持以太网口的 IP 协议包的流量统计，一种协议占一个条目，所以这个表目前最多只有一行。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rmon2 protocoldirtable protocoldirid** *protocol-id* **parameter** *parameter-value* [**descr** *description-string*] [**host** { **notsupported** | **supportedon** | **supportedoff** }] [**owner** *owner-name*] [**status** { **active** | **inactive** }]，配置协议目录表。

进行该配置时需注意：

- 当创建一个条目或将一个条目的状态（protocolDirStatus）设置为 **active** 时，必须同时设置 **parameter**（相当于 protocolDirDescr）和 **host**（相当于 protocolDirHostConfig）参数。
- 当 protocolDirStatus 设为 **active** 时，不能修改 protocolDirDescr 中的值。如果这时对象 protocolDirHostConfig 的值为 **notsupported** 时，也不能被修改为其他值，如果为非 **notsupported**，则可以在 **supportedon** 和 **supportedoff** 之间切换。当 protocolDirHostConfig 的值从 **supportedon** 变成 **supportedoff** 时，将删除主机控制表中对应的条目。
- 当 protocolDirStatus 设置为 **inactive** 时，将删除主机控制表中的相关条目。

----结束

5.3.3 检查配置结果

配置 RMON2 结束后，需要检查配置的正确性。

检查 RMON2 配置结果的相关操作如表 5-3 所示。

表 5-3 检查 RMON2 配置结果

操作	命令
显示协议目录表信息	**display rmon2 protocoldirtable**
显示主机控制表信息	**display rmon2 hlhostcontroltable** [**index** *ctrl-index*]
显示主机表信息	**display rmon2 nlhosttable** [**hostcontrolindex** *ctrl-index*] [**timemark** *time-value*] [**protocoldirlocalindex** *protocol-local-index*] [**hostaddress** *ip-address*]

5.4 调试 RMON 和 RMON2

在 ROMAN 和 ROMAN2 出现运行故障时，请在用户视图下执行 **debugging** 命令对 ROMAN 和 ROMAN2 进行调试，查看调试信息，定位故障并分析故障原因。

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

有关 **debugging** 命令的解释请参见《*Quidway Eudemon 8080E/8160E Debugging 参考*》。

操作步骤

步骤 1 在用户视图下执行命令 **terminal monitor**，打开终端显示信息功能。

步骤 2 执行命令 **terminal debugging**，打开终端显示调试信息功能。

步骤 3 调试 ROMAN 和 ROMAN2。

- 执行命令 **debugging rmon**，打开 RMON 调试开关。
- 执行命令 **debugging rmon2**，打开 RMON2 调试开关。

----结束

5.5 配置举例

介绍 RMON 和 RMON2 的配置举例。

5.5.1 配置 RMON 举例

介绍 RMON 的配置举例。

组网需求

如**图 5-1** 所示，要求对千兆以太网接口 GigabitEthernet 1/0/0 连接的 LAN 进行以下监控：

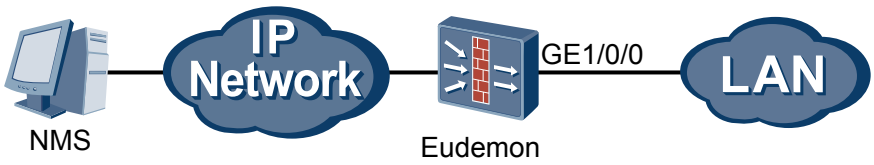
- 统计

  有关流量和各种类型包数量的实时和历史统计信息。
- 告警监控

  对此接口流量的字节数设置告警监控。当每分钟的流量超过设定值时，记录日志。
- Trap 发送

  监控此子网的广播和组播信息流量，对该子网的组播和广播总数进行告警设置，当超过设定值时，主动向 NMS 上报告警信息。

图 5-1 配置 RMON 组网图



数据规划

RMON 配置举例数据规划如表 5-4 所示。

表 5-4 RMON 配置举例数据规划

项目	数据	备注
信息采样时间间隔	30 秒钟	-
触发事件 1 阈值	最大阈值为 1000、最小阈值为 10	-
触发事件 2 阈值	最大阈值为 1000、最小阈值为 0	-

操作步骤

步骤 1 配置路由器和网管端路由可达（略）。

步骤 2 配置统计功能。

使能 RMON 接口统计功能。

```
<Eudemon> system-view
[Eudemon] interface GigabitEthernet 1/0/0
[Eudemon-GigabitEthernet1/0/0] rmon-statistics enable
```

配置统计表。

```
[Eudemon-GigabitEthernet1/0/0] rmon statistics 1 owner Test300
```

步骤 3 配置历史控制表。

设置 RMON 对子网中的流量信息进行采样，采样间隔为 30 秒钟，并保存最近 10 次数据。

```
<Eudemon> system-view
[Eudemon] interface GigabitEthernet 1/0/0
[Eudemon-GigabitEthernet1/0/0] rmon history 1 buckets 10 interval 30 owner Test300
```

退出接口视图。

```
[Eudemon-GigabitEthernet1/0/0] quit
```

退出系统视图。

```
[Eudemon] quit
```

步骤 4 配置事件表。

设置 RMON 的 1 号事件处理方式为记录日志。

```
<Eudemon> system-view
[Eudemon] rmon event 1 log owner Test300
```

设置 2 号事件处理方式为向网管站发送 Trap 消息。

```
[Eudemon] rmon event 2 description forUseofPrialarm trap public owner Test300
[Eudemon] quit
```

步骤 5 配置告警表。

设置采样间隔时间和触发事件 1 的阈值。

```
<Eudemon> system-view
[Eudemon] rmon alarm 1 1.3.6.1.2.1.2.2.1.10.402653698 30 delta rising-threshold 10000 1 falling-threshold 10 1 owner Test300
```

退出系统视图。

```
[Eudemon] quit
```

步骤 6 配置扩展告警表。

设置 RMON 对统计表中广播和组播总数每 30 秒钟进行一次采样，当采样的变化值高于最大阈值 1000 或低于最小阈值 0 时触发事件 2，向网管站发送 Trap 信息。

```
<Eudemon> system-view
[Eudemon] rmon prialarm 1 .1.3.6.1.2.1.16.1.1.1.6.1+.1.3.6.1.2.1.16.1.1.1.7.1 sumofbroadandmulti 30 delta rising-threshold 1000 2 falling-threshold 0 2 entrytype forever owner Test300
[Eudemon] quit
```

如果所设置的扩展告警变量超过预定范围后，网管站可以接受到告警 Trap 信息。

----结束

结果验证

1. 查看统计功能配置效果，可以随时查看子网的数据流量信息。

```
<Eudemon> display rmon statistics GigabitEthernet 1/0/0
Statistics entry 1 owned by Test300 is VALID.
  Interface : GigabitEthernet1/0/0<ifEntry.402653698>
  Received  :
  octets              :142915224 , packets          :1749151
  broadcast packets   :11603     , multicast packets:756252
  undersized packets  :0         , oversized packets:0
  fragments packets   :0         , jabbers packets  :0
  CRC alignment errors:0         , collisions       :0
  Dropped packet (insufficient resources):1795
  Packets received according to length (octets):
  64     :150183    ,  65-127  :150183    ,  128-255  :1383
  256-511:3698      ,  512-1023:0         ,  1024-1518:0
```

2. 查看历史控制表配置效果。命令行方式只会显示最后一次采样记录，如果要查看所有历史记录，需要使用特定网管站软件。

```
<Eudemon> display rmon history GigabitEthernet 1/0/0
History control entry 1 owned by Test300 is VALID,
  Samples Interface     :GigabitEthernet1/0/0<ifEntry.402653698>
Sampling interval    :30(sec) with 10 buckets max.
Lastest Sampling time    :0days 00h:19m:43s
  Latest sampled values:
  Dropevents    :0    , octets                  :645
  Packets       :7    , broadcast packets       :7
  multicast packets:0    , CRC alignment errors     :0
  undersize packets:6    , oversize packets         :0
```

```
  fragments        :0    , jabbers                 :0
  collisions    :0    , utilization             :0
```

3. 查看事件表配置结果。

```
<Eudemon> display rmon event
Event table 1 owned by Test300 is VALID.
Description: null.
  Will cause log  when triggered, last triggered at 0days 00h:24m:10s.
Event table 2 owned by Test300 is VALID.
Description: forUseofPrialarm.
  Will cause snmp-trap when triggered, last triggered at 0days 00h:26m:10s.
```

4. 查看告警信息。

```
<Eudemon> display rmon alarm 1
Alarm table 1 owned by Test300 is VALID.
Samples  delta value : 1.3.6.1.2.1.2.2.1.10.402653698<ifInOctets. 402653698>
Sampling interval         : 30(sec)
Rising threshold          : 10000(linked with event 1)
Falling threshold         : 10(linked with event 1)
When startup enables      : risingOrFallingAlarm
Latest value              : 1975
```

5. 查看扩展告警表信息。

```
<Eudemon> display rmon prialarm 1
Prialarm table 1 owned by Test300 is VALID.
  Samples delta value: .1.3.6.1.2.1.16.1.1.1.6.1+.1.3.6.1.2.1.16.1.1.1.7.1
  Sampling interval         : 30(sec)
  Rising threshold          : 1000(linked with event 2)
  Falling threshold         : 0(linked with event 2)
  When startup enables      : risingOrFallingAlarm
  This entry will exist     : forever.
  Latest value              : 16
```

6. 查看事件日志信息。

```
<Eudemon> display rmon eventlog
Event table 1 owned by Test300 is VALID.
  Generates eventLog 1.1 at 0days 00h:39m:30s.
  Description: The 1.3.6.1.2.1.2.2.1.10.402653698 defined in alarm table 1, uprise 10000 with
alarm value 10192. Alarm sample type is delta.
```

5.5.2 配置 RMON2 举例

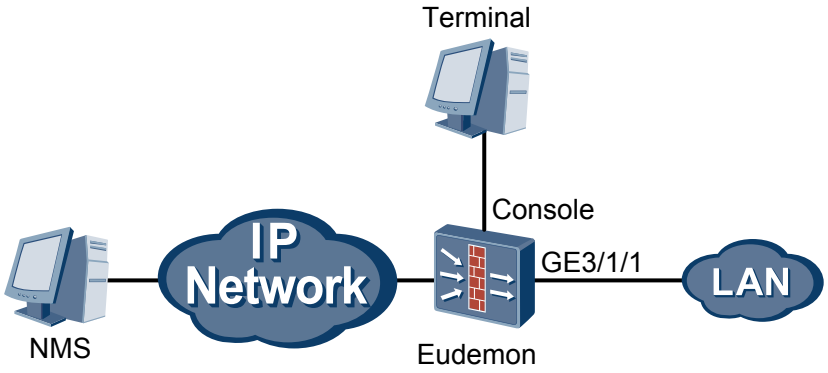
介绍 RMON2 的配置举例。

组网需求

如图 5-2 所示，要求通过配置 RMON2，对 Eudemon 的 GigabitEthernet3/1/1 接口进行 IP 协议包的流量统计。

RMON2 的监视过程可以通过 SNMP 网管工作站进行远程监视，也可以通过命令行配置方式进行流量监视。此例主要是通过命令行配置来进行流量监视。

图 5-2 配置 RMON2 组网图



数据规划

RMON2 配置举例数据规划如表 5-5 所示。

表 5-5 RMON2 配置举例数据规划

项目	数据	备注
主机控制表索引	123	-
主机表最大表项	100	-
协议 ID	8.0.0.0.1.0.0.8.0	-

操作步骤

步骤 1 配置主机控制表。

设置索引为 123，并将主机表的最大条目数设为 100。

```
<Eudemon> system-view
[Eudemon] rmon2 hlhostcontroltable index 123 datasource interface gigabitethernet 3/1/1 maxentry 100
owner china status active
```

步骤 2 配置协议目录表。

协议 ID 目前只支持 8.0.0.0.1.0.0.8.0，parameter 只支持 2.0.0，host 的值设置为 suppurtedon（即对该协议进行流量统计）。

```
[Eudemon] rmon2 protocoldirtable protocoldirid 8.0.0.0.1.0.0.8.0 parameter 2.0.0 descr IP host
supportedon owner china status active
```

----结束

结果验证

1. 查看整个主机表的信息。

```
<Eudemon> display rmon2 nlhosttable hostcontrolindex 123
Abbreviation:
HIdx - hlHostControlIndex
```

```
PIdx - ProtocolDirLocalIndex
Addr - nlHostAddress
InPkts - nlHostInPkts
OutPkts - nlHostOutPkts
InOctes - nlHostInOctets
OutOctes - nlHostOutOctets
OutMac - nlHostOutMacNonUnicastPkts
ChgTm - nlHostTimeMark
CrtTm - nlHostCreateTime
HIdx  PIdx Addr           InPkts     OutPkts    InOctes    OutOctes   OutMac     ChgTm
CrtTm
123   1     10.110.99.2          0              78              0                 10046
78          81489      40859
123   1       10.110.99.255         78             0              10046           0
0           81489      40859
```

2. 指定 IP 地址来查看特定主机的流量。

```
<Eudemon> display rmon2 nlhosttable hostcontrolindex 123 hostaddress 10.110.99.2
Abbreviation:
HIdx - hlHostControlIndex
PIdx - ProtocolDirLocalIndex
Addr - nlHostAddress
InPkts - nlHostInPkts
OutPkts - nlHostOutPkts
InOctes - nlHostInOctets
OutOctes - nlHostOutOctets
OutMac - nlHostOutMacNonUnicastPkts
ChgTm - nlHostTimeMark
CrtTm - nlHostCreateTime
HIdx  PIdx Addr           InPkts     OutPkts    InOctes    OutOctes   OutMac     ChgTm
CrtTm
123   1        10.110.99.2     0          78                 0              10046
78          81489      40859
```

3. 设置时间过滤器的值，只查看符合过滤条件的条目。

```
<Eudemon> display rmon2 nlhosttable hostcontrolindex 123 timemark 1000 hostaddress
10.110.99.2
Abbreviation:
HIdx - hlHostControlIndex
PIdx - ProtocolDirLocalIndex
Addr - nlHostAddress
InPkts - nlHostInPkts
OutPkts - nlHostOutPkts
InOctes - nlHostInOctets
OutOctes - nlHostOutOctets
OutMac - nlHostOutMacNonUnicastPkts
ChgTm - nlHostTimeMark
CrtTm - nlHostCreateTime
HIdx  PIdx Addr           InPkts     OutPkts    InOctes    OutOctes   OutMac     ChgTm
CrtTm
123   1        10.110.99.2     0          78                 0              10046
78          81489      40859
```

4. 查看主机控制表信息，可以看到该接口上的增加主机条目数、删除的主机条目数和主机表的最大条目数。

```
<Eudemon> display rmon2 hlhostcontroltable
Abbreviation:
index - hlhostcontrolindex
datasource - hlhostcontroldatasource
droppedfrm - hlhostcontrolnldroppedframes
inserts - hlhostcontrolnlinserts
Deletes - hlHostControlNlDeletes
maxentries - hlhostcontrolnlmaxdesiredentries
owner - hlhostcontrolowner
status - hlhostcontrolstatus
index datasource              droppedfrm inserts    Deletes    maxentries owner
status
123   GigabitEthernet3/1/1          0          19         0          100     China active
```

6 配置远程抓包

关于本章

通过配置远程抓包，可以将抓取到的报文发送到主机上进行报文分析。

6.1 简介
介绍远程抓包的基本原理和工作方式。

6.2 配置远程抓包
介绍配置远程抓包的过程。

6.3 配置基于满足 ACL 的丢包抓包远程抓包举例
介绍远程抓包的配置举例

6.1 简介

介绍远程抓包的基本原理和工作方式。

远程抓包功能是将经过 Eudemon 的报文复制保存到内存中，然后通过一定的命令将报文发送到特定的主机进行解析。

实际应用中，该功能主要用于分析并定位网络问题。一般通过一台可以 Telnet 到 Eudemon 的主机进行配置，配置后完成抓包，再将抓取到的报文发送到主机上进行报文分析。

6.2 配置远程抓包

介绍配置远程抓包的过程。

6.2.1 配置基于 ACL 抓包

介绍基于 ACL 抓包的配置过程。

数据准备

为完成该配置，需准备如下的数据：

- ACL 的编号和规则。
- 抓包抽样比。
- 最大抓包个数。

背景信息

Eudemon 支持基于 ACL 的抓包，便于用户进行攻击取证。

说明
配置基于 ACL 的抓包功能时，不能在设备上使用编号为 3999 的 ACL。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall packet-capture mode acl enable**,开启基于 ACL 的抓包功能。

步骤 3 执行命令 **firewall packet-capture acl** *acl-number*,应用 ACL 规则。

acl-number 为高级 ACL 的编号，取值范围为 3000 ～ 3999。

步骤 4 执行命令 **firewall packet-capture mode acl sample-rate** *sample-rate*，配置抓包抽样比。

sample-rate 的取值范围为 1 ～ 100，缺省值为 1:1。

说明
抓包 ACL 只能配置一个。

步骤 5 执行命令 **firewall packet-capture mode acl max-count** *max-count*，配置 ACL 抓包个数限制。

max-count 的取值范围为 1 ～ 10000，缺省值为 100。

配置抓包个数限制后，如果已经抓到报文的个数等于 *max-count* 的值，则停止抓包。用户可以通过再次执行 **firewall packet-capture mode acl enable** 命令重新进行抓包。

步骤 6 执行命令 **firewall packet-capture log-local-ip** *ip-address*,配置抓包的本地 IP 地址。

步骤 7 执行命令 **firewall packet-capture log-server-ip** *ip-address*,配置抓包的远端服务器的 IP 地址。

----结束

6.2.2 配置基于丢包抓包

介绍丢包抓包的配置过程。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall packet-capture mode drop enable**,开启基于丢包抓包功能。

步骤 3 执行命令 **firewall packet-capture mode drop sample-rate** *sample-rate*，配置丢包采样率。

sample-rate 的取值范围为 1 ～ 100，缺省值为 1:1。

步骤 4 执行命令 **firewall packet-capture mode drop max-count** *max-count*，配置丢包的采样最大值。

max-count 的取值范围为 1 ～ 10000，缺省值为 100。

步骤 5 执行命令 **firewall packet-capture log-local-ip** *ip-address*,配置抓包的本地 IP 地址。

步骤 6 执行命令 **firewall packet-capture log-server-ip** *ip-address*,配置抓包的远端服务器的 IP 地址。

----结束

6.2.3 配置基于满足 ACL 的丢包抓包

介绍基于 ACL 的丢包抓包的配置过程。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall packet-capture mode acl enable**,开启基于 ACL 的抓包功能。

步骤 3 执行命令 **firewall packet-capture mode drop enable**,开启基于丢包抓包功能。

步骤 4 执行命令 **firewall packet-capture acl** *acl number*,配置丢包抓包的 acl 组号，并在组中添加需要过滤的 rule 规则。

步骤 5 执行命令 **firewall packet-capture mode acl sample-rate** *sample-rate*，配置基于 ACL 的抓包采样率。

sample-rate 的取值范围为 1 ～ 100，缺省值为 1:1。

步骤 6 执行命令 **firewall packet-capture mode drop sample-rate** *sample-rate*，配置丢包抓包采样率。

sample-rate 的取值范围为 1 ～ 100，缺省值为 1:1。

步骤 7 执行命令 **firewall packet-capture mode acl max-count** *max-count*，配置基于 ACL 的抓包采样最大值。

max-count 的取值范围为 1 ～ 10000，缺省值为 100。

步骤 8 执行命令 **firewall packet-capture mode drop max-count** *max-count*，配置丢包抓包的采样最大值。

max-count 的取值范围为 1 ～ 10000，缺省值为 100。

步骤 9 执行命令 **firewall packet-capture log-local-ip** *ip-address*,配置抓包的本地 IP 地址。

步骤 10 执行命令 **firewall packet-capture log-server-ip** *ip-address*,配置抓包的远端服务器的 IP 地址。

----结束

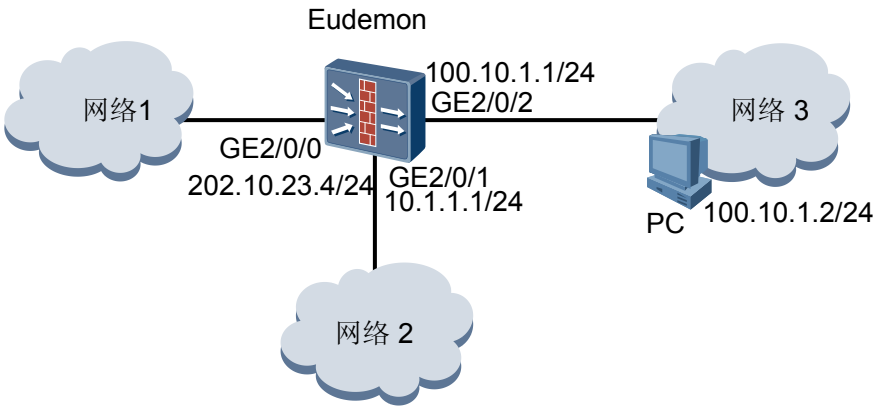
6.3 配置基于满足 ACL 的丢包抓包远程抓包举例

介绍远程抓包的配置举例

组网需求

如图 6-1 所示，Eudemon 的 GigabitEthernet2/0/0 接口和网络 1 相连，GigabitEthernet2/0/1 接口和网络 2 相连，GigabitEthernet2/0/2 接口和网络 3 相连，三个接口上均有一定的数据流量通过。可以从 PC 机 Telnet 到 Eudemon。现在需要在 PC 上 Telnet 到 Eudemon 对 GigabitEthernet2/0/0、GigabitEthernet2/0/1 和 GigabitEthernet2/0/2 接口进行抓包配置，并将抓取的报文发送到 PC 进行分析。在 PC 上启动 FirewallPacketyzer.exe 报文接收软件。

图 6-1 远程抓包配置组网图



配置思路

采用如下思路配置远程抓包：

- 1.在 PC 上启动 FirewallPacketyzer.exe 报文接收软件。
- 2.在 Eudemon 上通过配置抓包命令行配置抓包参数，发送抓取到的报文到 PC。

操作步骤

步骤 1 开启基于 ACL 丢包抓包功能。

进入系统视图。

```
<Eudemon> system-view
```

对丢包中的某些满足条件的报文抓取就需要配置丢包 acl，匹配满足条件的报文，抓报模式要同时配置 acl 和 drop。

```
[Eudemon] firewall packet-capture mode acl enable
[Eudemon] firewall packet-capture mode drop enable
```

步骤 2 配置 ACL 规则。

创建高级 ACL 3001 的规则。

```
[Eudemon] acl 3001
[Eudemon-acl-adv-3001] rule permit ip
Eudemon-acl-adv-3001] quit
```

说明

此处 ACL 规则表示所有流经需抓包接口的 IP 报文都会被抓取。实际应用时请根据具体情况精确配置 ACL 规则。

应用 ACL 规则。

```
[Eudemon] firewall packet-capture acl 3001
```

步骤 3 分别配置 acl 和 drop 的抓包个数限制。

```
[Eudemon] firewall packet-capture mode acl max-count 10000
[Eudemon] firewall packet-capture mode drop max-count 10000
```

说明

配置抓包个数限制后，如果已经抓到报文的个数等于 10000 的值，则停止抓包。用户可以通过再次执行 **firewall packet-capture mode acl enable** 命令重新进行抓包。

步骤 4 配置抓包抽样比。

```
[Eudemon] firewall packet-capture mode acl sample rate 1
```

步骤 5 配置丢包抽样比。

```
[Eudemon] firewall packet-capture mode drop sample-rate 1
```

步骤 6 配置抓包的本地 IP 地址。

```
[Eudemon] firewall packet-capture log-local-ip 192.1.1.1
```

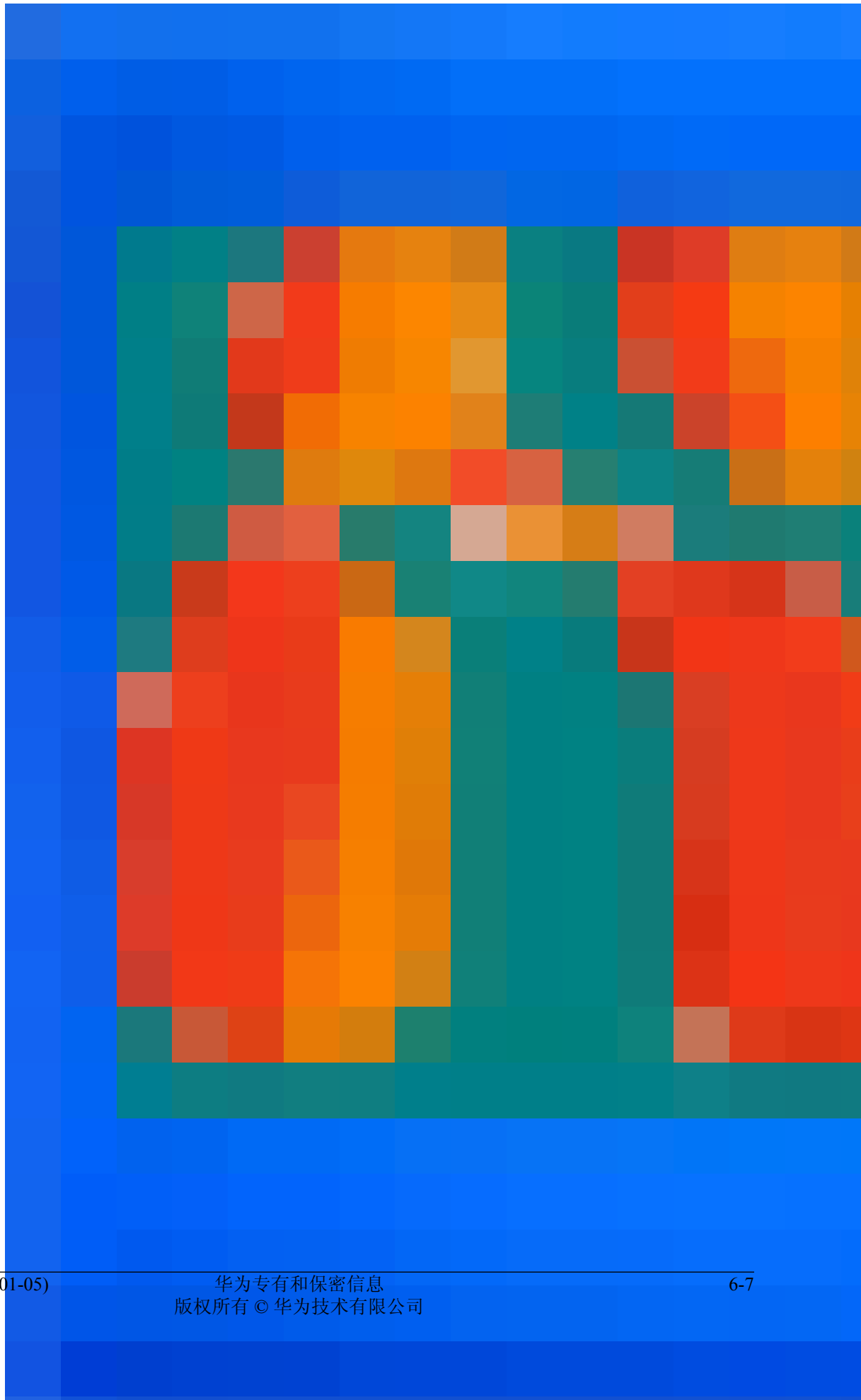
步骤 7 配置抓包的远端服务器的 IP 地址。

```
[Eudemon] firewall packet-capture log-server-ip 202.10.23.4
```

步骤 8 在 PC 上进行如下配置。

在 PC 上启动 FirewallPacketyer.exe 报文接收软件。（界面图如图 6-2 所示。）

图 6-2 FirewallPacketyer.exe 报文接收软件界面图



单击“Start”启动接收报文，单击“Stop”停止接收报文；生成的.cap 文件将被保存在“Save Path”指定的目录下面；“Local Port”默认为 9110，这里设置的端口必须和 Eudemon 侧设置的目的主机端口一致。

----结束

7 升级和维护

关于本章

升级和维护包括配置 License 授权、升级软件、安装和卸载补丁。

7.1 通过命令行方式升级软件
通过命令行方式升级软件，实现对系统的升级。

7.2 通过 CF 卡方式升级软件
通过 CF 卡方式升级软件，实现对系统的升级。

7.3 安装和卸载补丁
通过安装和卸载补丁，实现对补丁文件的管理。

7.4 配置 License
通过配置 License 授权，实现动态控制 Eudemon 的部分功能。

7.5 维护调试

7.6 复位系统或单板

7.7 配置电子标签功能

7.1 通过命令行方式升级软件

通过命令行方式升级软件，实现对系统的升级。

7.1.1 简介

软件升级即升级设备的系统软件。

当 Eudemon 系统软件版本不符合现有的工作需求，且有新版本的系统软件时，即可进行软件升级。

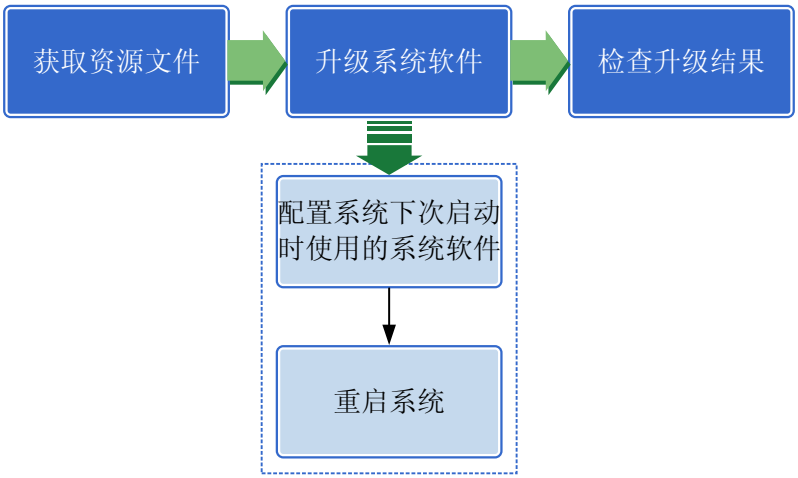
在设备正常运行的状态下，用户通过 Console 口、Telnet 或 SSH 方式登录设备，在命令行环境下将版本软件传送至设备的 CF 卡 1 中，并指定设备下一次启动时使用的版本软件，然后重新启动设备。

7.1.2 配置流程

介绍通过命令行方式升级系统软件的流程。

命令行方式升级的流程如图 7-1 所示。

图 7-1 命令行方式升级流程图



7.1.3 获取系统软件

获取资源文件到设备上之后，才能进行软件升级。

前提条件

- Eudemon 上电，且启动正常。
- Eudemon 与 PC 通信正常。

背景信息

说明

下文所描述的各种客户端、服务器程序由用户自己购买、安装，Eudemon 不附带此软件。

操作步骤

- 通过 TFTP 方式。

  Eudemon 作为 TFTP 客户端从 TFTP 服务器上获得系统软件。这种情况下，不要求 TFTP 服务器和 Eudemon 在同一个网段，只要保证二者之间路由可达即可。

  在 TFTP 主机上运行 TFTP 服务器程序，并把需要上传的系统软件放到相应的 TFTP 工作目录下。在用户视图下，执行命令 **get** *remote-filename* [*local-filename*]下载系统软件到 Eudemon 的相应目录下，具体操作请参见*《Quidway Eudemon 8080E/8160E 配置指南 基础配置分册》*。
- 通过 FTP 方式。
  - Eudemon 作为 FTP 客户端。

    这种情况下，不要求 FTP 服务器和 Eudemon 在同一个网段，只要保证二者之间路由可达即可。

    在 FTP 主机上运行 FTP 服务器程序，并把需要下载的系统软件放到相应的 FTP 的工作目录下，在用户视图下，执行命令 **get** *remote-filename* [*local-filename*] 下载系统软件到 Eudemon 的相应目录下，具体操作请参见*《Quidway Eudemon 8080E/8160E 配置指南 基础配置分册》*。
  - Eudemon 作为 FTP 服务器。

    这种情况下，不要求 FTP 客户端和 Eudemon 在同一个网段，只要保证二者之间路由可达即可。

    在 Eudemon 上启动 FTP 服务器，具体操作请参见*《Quidway Eudemon 8080E/8160E 配置指南 基础配置分册》*。通过 FTP 客户端登录到 Eudemon 后，把系统软件上传到 Eudemon 相应的目录下。
- 通过 Xmodem 方式。

  具体操作请参见*《Quidway Eudemon 8080E/8160E 配置指南 基础配置分册》*。

----结束

7.1.4 升级系统软件

通过命令行方式升级系统软件，实现系统的升级。

前提条件

系统软件必须存放在 **cfcard:** 的根目录下。

操作步骤

步骤 1 在用户视图下执行命令 **startup system-software** *sys-filename* [**slave-board**]，配置系统下次启动时使用的系统软件。

步骤 2 （可选）执行命令 **startup saved-configuration** *cfg-filename*，配置系统下次启动时使用的配置文件。

步骤 3 执行命令 **reboot**，重新启动 Eudemon。

----结束

7.1.5 检查升级结果

检查系统升级是否成功。

检查软件升级配置结果的相关操作如**表 7-1** 所示。

表 7-1 检查软件升级配置结果

操作	命令
显示本次及下次启动相关的系统软件、配置文件名	**display startup**
显示系统当前使用的版本信息	**display version**

7.2 通过 CF 卡方式升级软件

通过 CF 卡方式升级软件，实现对系统的升级。

7.2.1 简介

将 CF 卡插入主控板前面板上的 CF 卡 2 槽位，可实现设备自动升级。

将版本软件拷贝到 CF 卡中，然后将 CF 卡插入到主控板上的 CF 卡 2 槽位中，重新启动设备。设备重启时，会自动将 CF 卡 2 中的版本软件拷贝到 CF 卡 1 中，并使用新的版本软件启动。

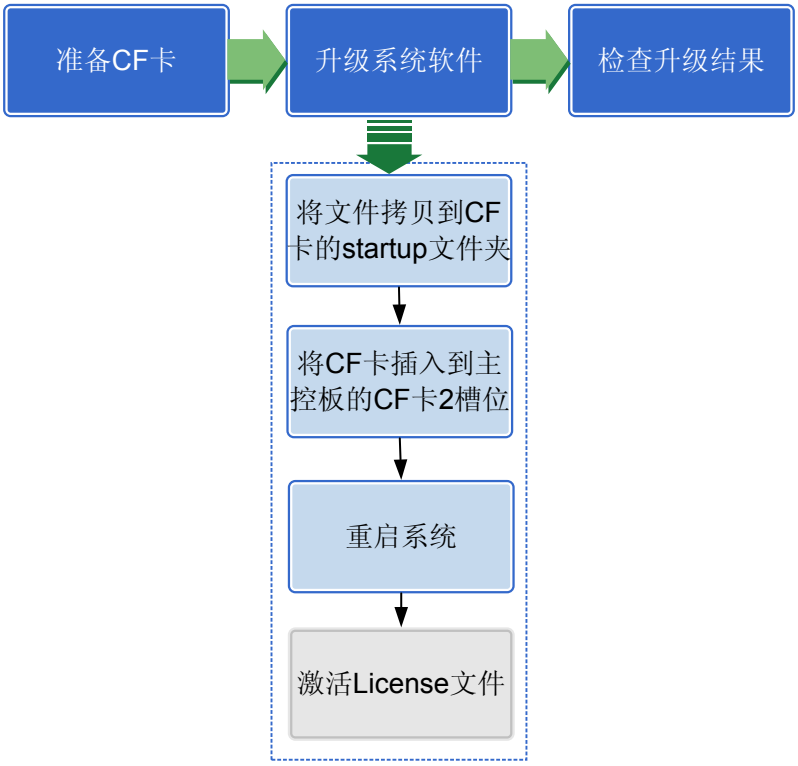
使用 CF 卡升级软件操作过程简单，不需要网络环境的支持，对业务影响小。

7.2.2 配置流程

介绍通过 CF 卡方式升级系统软件的流程。

CF 卡方式升级的流程如图 7-2 所示。

图 7-2 CF 卡方式升级流程图



7.2.3 升级系统软件

通过 CF 卡方式升级系统软件，实现系统的升级。

前提条件

请联系技术支持工程师，获取装有新版本系统软件的 CF 卡。

操作步骤

步骤 1 将文件拷贝到 CF 卡的 startup 文件夹。

升级所需文件必须放到 CF 卡根目录下的 startup 文件夹下，对文件的命名有如下要求：

- 系统程序必须以.cc 为后缀名，并且只能存放一个；不能修改 paf.txt 和 license.txt 文件的名称。
- License 文件必须以.dat 为后缀名，并且只能存放一个。
- 配置文件的名称中必须包含 vrpcfg 关键字，必须以.cfg 或.zip 为后缀名，并且只能存放一个。如果需要拷贝配置文件，建议命名为 vrpcfg.cfg 或者 vrpcfg.zip。

由于一块 CF 卡只能用于一个主控板升级一次，因为如果两块主控板都在位，需要准备两块 CF 卡。

步骤 2 将 CF 卡插入到主控板 CF 卡 2 槽位。

步骤 3 在用户视图下使用 reboot 命令重新启动 Eudemon。

执行 reboot 命令后，设备将会显示两次提示信息，询问用户是否继续，请用户输入**y** 继续重启操作。

设备重启时，会自动查找 CF 卡 2 中 startup 文件夹，将 startup 文件夹中的文件复制到 CF 卡 1 中，然后使用新的版本软件启动。

说明

设备启动耗时受待复制文件的大小、当前的硬件配置以及配置文件影响。单板越多，单板注册的时间就越长；配置越多，需要恢复配置的时间就越长。

步骤 4 （可选）设备重启完成后，在系统视图下使用 license file 命令激活 License 文件。

```
<Eudemon> system-view
[Eudemon] license file license.dat
```

----结束

7.2.4 检查升级结果

检查系统升级是否成功。

检查软件升级配置结果的相关操作如表 7-2 所示。

表 7-2 检查软件升级配置结果

操作	命令
显示本次及下次启动相关的系统软件、配置文件名	**display startup**
显示系统当前使用的版本信息	**display version**

7.3 安装和卸载补丁

通过安装和卸载补丁，实现对补丁文件的管理。

7.3.1 补丁安装和卸载简介
补丁用于解决系统软件的少量且急需解决的问题。

7.3.2 配置流程
介绍补丁的安装和卸载流程。

7.3.3 安装补丁
通过安装补丁，可以在不中断系统运行的情况下，使用补丁程序对系统软件进行升级。

7.3.4 卸载补丁
通过卸载补丁，可以去激活或者删除补丁。

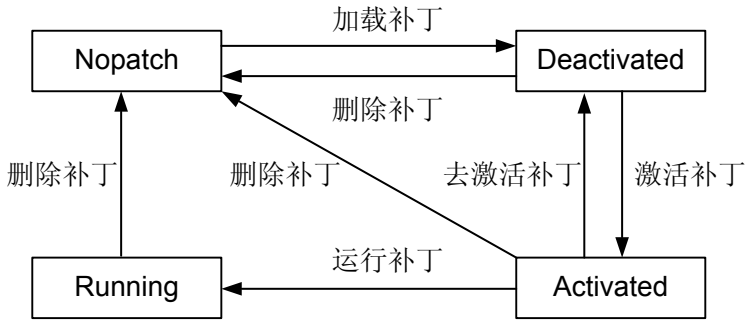
7.3.1 补丁安装和卸载简介

补丁用于解决系统软件的少量且急需解决的问题。

补丁是一种与 Eudemon 系统软件兼容的软件，补丁文件的扩展名是“.pat”。

Eudemon 提供了在线安装补丁功能，可以在不中断系统运行的情况下，使用补丁程序对系统软件进行升级。补丁程序有三种状态：激活（Activated）、去激活（Deactivated）、运行（Running）。状态之间转换关系如图 7-3 所示。

图 7-3 补丁程序转换关系

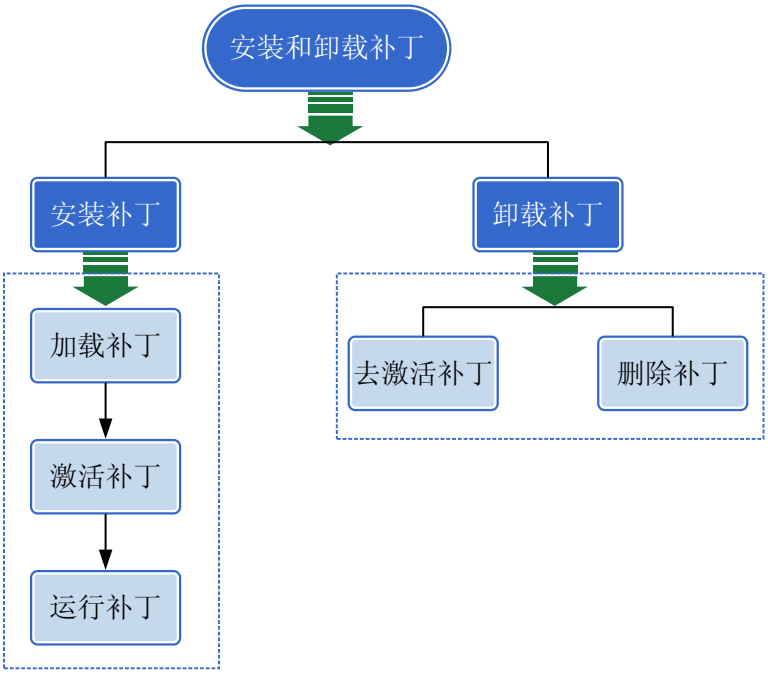


7.3.2 配置流程

介绍补丁的安装和卸载流程。

补丁安装和卸载的流程如图 7-4 所示。

图 7-4 补丁安装和卸载流程图



7.3.3 安装补丁

通过安装补丁，可以在不中断系统运行的情况下，使用补丁程序对系统软件进行升级。

前提条件

- 上传补丁软件到设备。

  具体操作类似于上传系统软件到设备，请参见 7.1.3 获取系统软件。
- 需要安装的补丁文件名必须为 patch.pat，且必须存放在 **cfcard:** 的根目录下。

背景信息

如果补丁文件没有被删除，单板复位后，激活状态的补丁将恢复为去激活状态，只有运行状态的补丁会继续生效。

操作步骤

步骤 1 在用户视图下执行命令 **patch load** [**allpatch** | **slave** | **slot** *slot number* [**slavecpu**]]，加载补丁。

加载补丁时，系统会自动对该补丁进行校验，以验证该补丁和主机版本的校验和是否一致，如果不一致，补丁将加载失败。

步骤 2 执行命令 **patch active** { **allpatch** | *patch number* [**slave** | **slot** *slot number* [**slavecpu**]] }，激活处于去激活状态的补丁。

激活补丁时注意事项如下：

- 如果补丁不存在，系统将提示补丁不存在。
- 激活补丁时，如果处于去激活状态的补丁不存在，系统将提示补丁激活失败。

步骤 3 执行命令 **patch run** { **allpatch** | *patch number* [**slave** | **slot** *slot number* [**slavecpu**]] }，运行处于激活状态的补丁。

运行补丁时注意事项如下：

- 如果补丁不存在，系统将提示补丁不存在。
- 运行补丁时，如果处于激活状态的补丁不存在，系统将提示补丁运行失败。

----结束

后续处理

执行命令 **display patch-information** [**allpatch** | **slave** | **slot** *slot number* [**slavecpu**]]，显示补丁信息。

7.3.4 卸载补丁

通过卸载补丁，可以去激活或者删除补丁。

操作步骤

- 执行命令 **patch deactive** { **allpatch** | *patch number* [**slave** | **slot** *slot number* [**slavecpu**]] }，去激活补丁。

  去激活补丁时注意事项如下：

  - 如果补丁不存在，系统将提示补丁不存在。

- 去激活补丁时，如果补丁处于运行状态，系统将提示补丁去激活失败。
- 如果补丁处于激活状态时，则可以去激活。

- 执行命令 **patch delete** { **allpatch** | *patch number* [**slave** | **slot** *slot number* [**slavecpu**]] }，删除补丁。

  当系统不再需要补丁程序的时候，可以删除补丁。

  删除补丁时注意事项如下：

  - 不管补丁处于什么状态，都将被删除。
  - 补丁删除后不可恢复，如果需要该补丁则必须重新加载。

----结束

后续处理

执行命令 **display patch-information** [**allpatch** | **slave** | **slot** *slot number* [**slavecpu**]]，显示补丁信息。

7.4 配置 License

通过配置 License 授权，实现动态控制 Eudemon 的部分功能。

7.4.1 License 简介

介绍 License 控制的配置项，以及如何申请 License。

可通过购买 License 获得以下 Eudemon 的功能和处理性能：

- 虚拟防火墙功能

  未加载 License 情况下，Eudemon 支持创建 1 个虚拟防火墙。
- IPsec 功能

  未加载 License 情况下，Eudemon 不支持 IPSec 功能，并且相关命令行不可见。
- GTP 功能

  未加载 License 情况下，Eudemon 不支持 GTP 功能，并且相关命令行不可见。
- IPS 功能

  未加载 License 情况下，Eudemon 不支持 IPS 升级服务。

需要收集以下信息，以进行 License 的申请：

- 合同编号（Contract No.）

  从随设备附带的 License 授权证书上获得。
- License 授权码 LAC（License Authorization Code）

  从随设备附带的 License 授权证书上获得。

- 设备序列号 ESN（Equipment Serial Number）

  登录到设备后在任意视图下执行 **display license** 命令获得。

说明

如果为多台设备申请 License，请确保每台设备的 LAC 与 ESN 一一对应。

请登录 http://license.huawei.com，使用以上信息申请 License。华为技术支持工程师会尽快处理，并将 License 尽快发送给您。

7.4.2 配置 License 授权

介绍了加载 License 的方法。

前提条件

上传 License 文件到设备。

具体操作类似于上传系统软件到设备，请参见 7.1.3 获取系统软件。

操作步骤

步骤 1 在用户视图下执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **license file** *license-file* ，激活指定的 License 文件。

只有当 License 文件与设备的 ESN（Equipment Serial Number）编号完全匹配时，才能成功激活 License 文件。执行命令 **display license** 可查看设备的 ESN 编号。

当需要激活新的 License 文件时，必须先通过 **undo license file** 命令取消已经激活的 license 文件。

----结束

后续处理

执行命令 **display license**，查看当前 License 的信息。

7.5 维护调试

7.5.1 维护调试

当设备出现故障时，可以使用系统提供的以下测试和调试命令判断系统和网络运行情况。

Ping

主要用于检查网络连接是否正常及主机是否可达。

Tracert

用于测试数据包从发送主机到目的地所经过的网关，它主要用于检查网络连接是否正常，以及分析网络什么位置发生了故障。

Tracert 的执行过程就是记录每一个 ICMP（Internet Control Message Protocol） TTL（Time-to-Live）超时消息的源地址，以提供一个 IP 数据包到达目的地所经历的路径，具体过程如下。

1. 发送一份 TTL 字段为 1 的 IP 数据包给目的主机，第一跳路由器将 TTL 值减去 1，丢弃该数据包，并发回一个 ICMP 超时信息，可以得到第一跳路由器的地址。
2. 然后重新发送一份 TTL 字段为 2 的 IP 数据包给目的主机，同样第二跳路由器发回一个 ICMP 超时信息，可以得到第二跳路由器的地址。
3. 这个过程不断进行，直到该数据包到达目的地。

Debugging

系统的命令行接口提供了种类丰富的调试功能，对于 Eudemon 所支持的各种协议和功能，基本上都提供了相应的调试功能，可以帮助用户对错误进行诊断和定位。

通过以下两种方法完成对调试信息输出的控制和过滤：

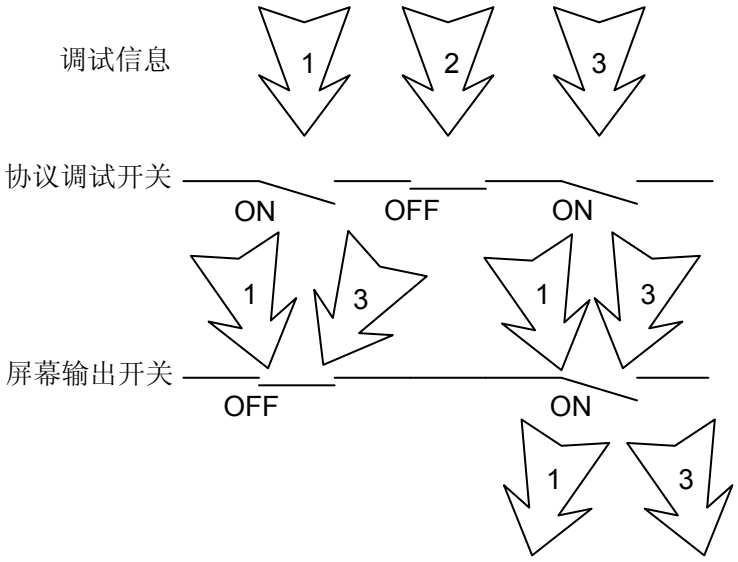
- 调试信息输出的开关控制

  调试信息的输出可以由以下两个开关控制。

  - 协议调试开关，控制是否输出某协议的调试信息。
  - 屏幕输出开关，控制是否在某个用户屏幕上输出调试信息。

  二者关系如图 7-5 所示。

图 7-5 调试信息输出示意图



- 正则表达式

  在输出的信息比较多时，可以使用正则表达式过滤显示输出的内容。

  正则表达式是一种可用于模式匹配和替换的工具，在使用时，用户需要根据一定的规则构建匹配模式，然后将匹配模式与目标对象进行匹配。最简单的正则表达式不包含任何有特殊含义的字符，例如，可以规定一个正则表达式 hello，它只匹配字符串“hello”。

  为帮助用户灵活地构建匹配模式，正则表达式提供了一些具有特殊含义的专用字符，也称为“元字符”（metacharacter），用来规定其它字符在目标对象中的出现模式。元字符描述如表 7-3 所示。

  表 7-3 元字符描述

元字符	含义
\	转义字符
.	匹配除“\n”之外任何单个字符，包括空格
*	之前的字符在目标对象中出现 0 次或连续多次
+	之前的字符在目标对象中出现 1 次或连续多次
|	竖线左边和右边的字符为“或”的关系
^	之后的字符必须出现在目标对象的开始
$	之前的字符必须出现在目标对象的结束
[xyz]	匹配方括号内列出的任意字符
[^xyz]	匹配除了方括号内列出的字符外的任意字符（^号在字符前）
[a-z]	匹配指定范围内的任意字符
[^a-z]	匹配不在指定范围内的任意字符
{ n }	n 是一个非负整数，匹配连续出现的确定 n 次
{ n, }	n 是一个非负整数，匹配连续出现的至少 n 次
{ n,m }	m 和 n 均为非负整数，n<=m。匹配连续出现的次数为 n ～ m 次。使用时注意，逗号与 n 和 m 之间不能有空格

  例如：“^ip”表示匹配以字符串“ip”开始的目标对象；“ip$”表示匹配以字符串“ip”结束的目标对象。

7.5.2 Ping

背景信息

ping 命令可用于测试网络连接性故障。根据 Ping 测试输出的报文响应时间，还可以判断网络线路质量。如果网络速度较慢，执行 Ping 测试时可适当加大等待响应报文的超时时间。

操作步骤

步骤 1 执行命令 **ping** [**ip**] [**-a** *source-ip-address* | **-c** *count* | **-d** | **-f** | **-h** *ttl-value* | **-i** *interface-type interface-number* | **-m** *time* | **-n** | **-p** *pattern* | **-q** | **-r** | **-s** *packetsize* | **-t** *timeout* | **-tos** *tos-value* | **-v** | **-vpn-instance** *vpn-instance-name*] * *host*，测试网络连接是否正常。

各选项及参数意义请参见《*Quidway Eudemon 8080E/8160E 防火墙 命令参考*》。

命令执行结果输出包括：

- 每一个 **ping** 报文的响应情况

  如果到超时仍没有收到响应报文，则输出 `Request time out`，否则显示响应报文中数据字节数、报文序号、TTL 和响应时间等。

- **ping** 后的统计信息

  包括发送报文数、接收报文数、未响应报文百分比和响应时间的最小、最大和平均值。

----结束

7.5.3 Tracert

操作步骤

步骤 1 执行命令 **tracert** [**-a** *source-ip-address* | **-f** *first-TTL* | **-m** *max-TTL* | **-p** *port* | **-q** *nqueries* | **-vpn-instance** *vpn-instance-name* | **-w** *timeout*] * *host*，跟踪路由，测试故障发生的位置。

各选项及参数意义请参见《*Quidway Eudemon 8080E/8160E 防火墙 命令参考*》。

----结束

7.5.4 Debugging

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

操作步骤

步骤 1 执行命令 **debugging** *module-name* [*debug-option1*] [*debug-option2*]，打开调试开关。

说明

对于部分调试开关，*debug-option* 可以包含 **acl** *acl-number*，即根据 ACL 策略调试所需要的报文，例如 **debugging ip packet acl** *acl-number*。

有关 **debugging** 命令的解释请参见《*Quidway Eudemon 8080E/8160E 防火墙 命令参考*》。

----结束

7.6 复位系统或单板

7.6.1 简介

注意

在 Eudemon 工作不正常时，尽量排除故障，不要轻易复位系统或单板，以免对业务造成影响。

复位系统

当发生下列情况时，Eudemon 可能需要复位：

- 系统升级。
- 加载主机程序。
- 工作不正常。

复位时，Eudemon 将按用户已设定的下次启动配置文件重新启动。复位系统有以下两种类型：

- 立即复位系统

  通过命令或者断电复位系统。
- 定时复位系统

  为了方便用户选择系统复位的时间，Eudemon 提供了系统定时复位功能。用户可以按照以下两种方式，选择系统复位的时间。
  - 指定具体复位时间，例如指定 Eudemon 在凌晨 2 点 30 分自动复位。
  - 指定复位延迟时间，例如指定 Eudemon 在延迟 3 小时后自动复位。

复位单板

当发生下列情况时，需要复位单板：

- 加载新的配置数据。
- 单板工作不正常。

7.6.2 立即复位系统

注意

在 Eudemon 工作不正常时，尽量排除故障，不要轻易复位系统，以免对业务造成影响。

命令方式复位系统

在用户视图下执行命令 **reboot**，立即复位系统。

断电方式复位系统

注意

无特殊情况请不要使用该方法。

先将 Eudemon 断电，3 分钟后给 Eudemon 重新上电，从而复位 Eudemon 系统。

7.6.3 定时复位系统

背景信息

注意

系统定时复位应该选择业务流量较小的时间进行，以免由于大量业务中断，造成较大损失。

操作步骤

步骤 1 执行命令 **schedule reboot** { **at** *exact-time* | **delay** *interval* }，定时复位系统。

----结束

7.6.4 立即复位单板

背景信息

注意

- 系统复位时全部单板同时复位。
- 在单板工作不正常时，尽量排除故障，不要轻易复位单板，以免对业务造成影响。

操作步骤

步骤 1 执行命令 **reset slot** *slot-number*，立即复位单板。

----结束

7.6.5 检查配置结果

检查复位配置结果的相关操作如**表 7-4** 所示。

表 7-4 检查复位配置结果

操作	命令
查看当前设备 reboot 终端服务的参数设置	**display schedule reboot**

7.7 配置电子标签功能

7.7.1 电子标签简介

电子标签用来实现查询或者备份设备实体的制造信息。支持分级的功能，即可以查询、备份设备上所有单板的制造信息或者指定槽位单板的制造信息。

电子标签可以备份在 FTP 服务器上或者设备的 CF 卡上。

7.7.2 查询电子标签

操作步骤

步骤 1 执行命令 **display elabel** [*slot-number*]，查询电子标签。

----结束

7.7.3 备份电子标签

操作步骤

- 执行命令 **backup elabel** *filename* [*slot-number*]，将电子标签备份到 CF 卡上。
- 执行命令 **backup elabel ftp** *host filename username password* [*slot-number*]，将电子标签备份到 FTP 服务器上。

----结束