H3C IPS 入侵防御系统

配置指导

杭州华三通信技术有限公司
http://www.h3c.com.cn

资料版本：20100913-C-1.07

H3C、  、Aolynk、  、H^{3}Care、  、TOP G、  、IRF、NetPilot、Neocean、NeoVTL、SecPro、SecPoint、SecEngine、SecPath、Comware、Secware、Storware、NQA、VVG、V^{2}G、V^{n}G、PSPT、XGbus、N-Bus、TiGem、InnoVision、HUASAN、华三均为杭州华三通信技术有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。H3C 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，H3C 尽全力在本手册中提供准确的信息，但是 H3C 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前 言

H3C IPS 入侵防御系统配置指导介绍了 IPS 入侵防御系统的各种特性及其配置方法，包含原理简介、配置任务描述和配置举例。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1.命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... } *	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...] *	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入 1～n 次。
#	由“#”号开始的行表示为注释行。

2.图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3.各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4.图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表 IPS 入侵防御系统。
	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。

产品配套资料

H3C IPS 入侵防御系统的配套资料可以通过各系列产品的资料导航来查阅：

产品	资料导航
T200 系列盒式 IPS	H3C T200 系列入侵防御系统 资料导航
T1000 系列盒式 IPS	H3C T1000 系列入侵防御系统 资料导航
T5000 系列盒式 IPS	H3C T5000-S3 入侵防御系统 资料导航
SecBlade 系列 IPS 插卡	H3C SecBlade IPS插卡 资料导航

资料获取方式

您可以通过H3C网站（www.h3c.com.cn）获取最新的产品资料：

H3C 网站与产品资料相关的主要栏目介绍如下：

- [服务支持/文档中心]：可以获取硬件安装类、软件升级类、配置类或维护类等产品资料。
- [产品技术]：可以获取产品介绍和技术介绍的文档，包括产品相关介绍、技术介绍、技术白皮书等。
- [解决方案]：可以获取解决方案类资料。
- [服务支持/软件下载]：可以获取与软件版本配套的资料。

技术支持

用户支持邮箱：customer_service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

网址：http://www.h3c.com.cn

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 常用网络应用配置

1.1 常用网络应用配置

1.1.1 Ping 操作

在日常的系统维护中，用户可以使用 **ping** 命令来检查当前网络的连接情况。通过使用 **ping** 命令，用户可以检查指定地址的设备是否可达，测试网络连接是否出现故障。

ping 命令的执行过程为：

(1) 源设备向目的设备发送 ICMP 回显请求（ECHO-REQUEST）报文；

(2) 如果网络工作正常，则目的设备在接收到该报文后，向源设备回应 ICMP 回显应答（ECHO-REPLY）报文；

(3) 如果网络工作异常，源设备将显示目的地址不可达或超时等提示信息；

(4) 源设备上显示相关统计信息。

ping 命令输出信息分为以下几种情况：

- **ping** 命令的执行对象是目的设备的 IP 地址；
- 目的设备对每个 ICMP 回显请求报文的响应，如果在超时时间内没有收到响应报文，则输出提示信息和 Ping 过程报文的统计信息；如果在超时时间内收到响应报文，则输出响应报文的字节数、报文序号、TTL（Time To Live，生存时间）、响应时间和 Ping 过程报文的统计信息。

Ping 过程报文的统计信息包括发送报文个数、接收到响应报文个数、未响应报文数百分比、响应时间的最小值、平均值和最大值。

表1-1 在设备上执行 Ping 操作

操作	命令	说明
检查 IP 网络中的指定地址是否可达	**ping** [**-Q** *tos* | **-R** | **-b** | **-c** *count* | **-f** | **-i** *interval* | **-n** | **-p** *pad* | **-q** | **-s** *packet-size* | **-t** *ttl* | **-v** | **-w** *timeout*] *ip-address*	可选 网络层协议为 IPv4 时使用 可在用户视图或系统视图下执行

说明

如果网络传输速度较慢，用户在配置 **ping** 命令的超时时间参数**-w** 时，可以适当增大超时时间。

表1-2 禁止设备管理口发送 ICMP 回显应答报文

操作	命令	说明
禁止设备管理口发送 ICMP 回显应答报文，使其他网络设备无法 Ping 通设备管理口	**network icmp echo-reply disable**	必选 缺省情况下，设备管理口可以发送 ICMP 回显应答报文

1.1.2 Telnet 服务

设备支持 Telnet 协议，当设备启动了 Telnet 服务后，用户可以通过 Telnet 方式登录到设备上，对设备进行远程管理和维护。

表1-3 Telnet 服务配置

操作	命令	说明
启动 Telnet 服务	**telnet service enable**	必选 缺省情况下，Telnet 服务处于关闭状态

说明

- 通过 Telnet 方式登录设备使用的密码与通过 Console 口登录的密码相同。
- 通过 Telnet 和 SSH 方式同时登录设备的用户总数不能超过 7。

1.1.3 SSH 服务

设备支持 SSH 协议，当设备启动了 SSH 服务后，用户可以通过 SSH 方式登录到设备上，对设备进行远程管理和维护。

表1-4 SSH 服务配置

操作	命令	说明
启动 SSH 服务	**ssh service enable**	必选 缺省情况下，SSH 服务处于关闭状态

说明

- 通过 SSH 方式登录设备使用的用户名和密码都是“sshadmin”。
- 通过 Telnet 和 SSH 方式同时登录设备的用户总数不能超过 7。

目 录

1 接口管理配置

1.1 简介

根据功能的不同，设备上有两种以太网接口：

- 管理口。该类以太网接口供管理设备使用，不具备业务处理能力，可以方便用户对设备进行配置和管理，并且不占用设备业务接口。
- 业务口。该类以太网接口具备业务处理能力，可以处理和转发各种业务数据。

1.2 接口管理配置

1.2.1 以太网接口配置

设置以太网接口的双工模式时存在三种情况：

- 当希望接口在发送数据包的同时可以接收数据包，可以将接口设置为全双工（**full**）属性。
- 当希望接口同一时刻只能发送数据包或接收数据包时，可以将接口设置为半双工（**half**）属性。
- 当设置接口为自协商（**auto**）状态时，接口的双工状态由本接口和对端接口自动协商而定。

设置以太网接口的速率时，当设置接口速率为自协商（**auto**）状态时，接口的速率由本接口和对端接口双方自动协商而定。

表1-1 以太网接口基本配置

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-name*	-
设置管理口的 IP 地址	**ip address** *ip-address* { *mask* | *mask-length* }	可选 缺省情况下，管理口的 IP 地址为 192.168.1.1
设置以太网接口的双工模式	**duplex** { **auto** | **full** | **half** }	可选 缺省情况下，接口的双工模式为 **auto**（自协商）状态 需要注意的是，万兆以太网接口只支持 **full** 参数；Combo 光口不支持配置 **half** 参数；千兆以太网接口在速率为 1000Mbps 时不支持 **half** 参数
设置以太网接口的速率	**speed** { **10** | **100** | **1000** | **10000** | **auto** }	可选 缺省情况下，以太网接口的速率为 **auto**（自协商）状态 需要注意的是，万兆以太网接口的速率只能为 **10000**；Combo 光口不支持配置此命令；命令中各参数的支持情况与接口板的型号有关，请以实际情况为准
关闭以太网接口	**shutdown**	可选 缺省情况下，接口处于开启状态 如果想开启接口，可以使用 **undo shutdown** 命令

1.2.2 Combo 接口配置

Combo 接口是指设备面板上的两个以太网接口（通常一个是光口一个是电口），而在设备内部只有一个转发接口。Combo 电口与其对应的光口在逻辑上是光电复用的，用户可根据实际组网情况选择其中的一个使用，但两者不能同时工作，当激活其中的一个接口时，另一个接口就自动处于禁用状态。

表1-2 配置 Combo 接口的状态

操作	命令	说明
进入系统视图	**system-view**	-
进入 Combo 接口视图	**interface** *interface-name*	-
激活指定的 Combo 接口	**combo enable** { **copper** | **fiber** }	可选 缺省情况下，电口处于激活状态

1.2.3 接口显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后接口的运行情况，通过查看显示信息验证配置的效果。

表1-3 接口显示和维护

操作	命令
显示指定接口当前的运行状态和相关信息	**display interface** [*interface-name*]

目 录

1 静态路由配置

1.1 简介

一台设备可以由多个管理站进行管理。设备可以将检测到的异常和网络攻击的情况上报到管理站，管理员可以在管理站上远程管理设备，也可以在不同的管理站上接收并分析设备产生的日志，从而有效地预测和规避网络安全威胁。

路由管理模块提供了对设备到各管理站的路由信息的管理。通过手工配置静态路由，在设备上建立一张路由表，表中每条路由项都指明了要到达某个管理站需经过的下一跳。

缺省路由是在设备没有找到匹配的路由表入口项时才使用的路由。在配置静态路由时，如果指定的目的 IP 地址和子网掩码均为 0.0.0.0，则表示配置了一条缺省路由。

1.2 配置静态路由

1.2.1 配置准备

在配置静态路由之前，需完成以下任务：

- 配置相关接口的物理参数
- 配置相关接口的链路层属性
- 配置相关接口的 IP 地址

1.2.2 配置静态路由

表1-1 配置静态路由

操作	命令	说明
进入系统视图	**system-view**	-
配置到达目的管理站的静态路由	**ip route-static** *dest-addr mask geteway-addr*	必选

说明

- 在使用 **ip route-static** 配置静态路由时，如果将目的地址与子网掩码配置为全零（0.0.0.0），则表示配置的是缺省路由。
- 网关地址不能为本地接口 IP 地址，否则静态路由不会生效。

1.2.3 静态路由显示和维护

在完成上述配置后，在系统视图下执行 **display** 命令查看静态路由的信息。

表1-2 静态路由显示和维护

操作	命令
查看静态路由的信息	**display ip route-static**

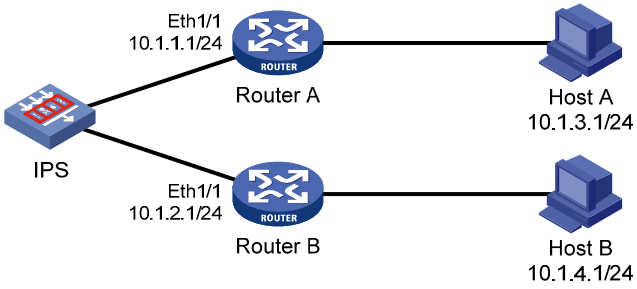
1.3 静态路由典型配置举例

1. 组网需求

IPS 设备分别通过 Router A 和 Router B 与管理站主机 Host A 和 Host B 相连。在 IPS 上配置静态路由，使其可以与 Host A 和 Host B 通信。

2. 组网图

图1-1 静态路由配置组网图



3. 配置步骤

配置到 Host A 的静态路由。

```
<Sysname> system-view
[Sysname] ip route-static 10.1.3.1 255.255.255.0 10.1.1.1
```

配置到 Host B 的静态路由。

```
[Sysname] ip route-static 10.1.4.1 255.255.255.0 10.1.2.1
```

4. 验证配置结果

使用 **ping** 命令验证 Host A 是否可达。

```
[Sysname] ping 10.1.3.1
PING 10.1.3.1 (10.1.3.1) 56(84) bytes of data.
64 bytes from 10.1.3.1: icmp_seq=1 ttl=128 time=0.864 ms
64 bytes from 10.1.3.1: icmp_seq=2 ttl=128 time=0.183 ms
64 bytes from 10.1.3.1: icmp_seq=3 ttl=128 time=0.851 ms
64 bytes from 10.1.3.1: icmp_seq=4 ttl=128 time=0.180 ms

--- 10.1.3.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.180/0.519/0.864/0.338 ms, pipe 2
```

使用 **ping** 命令验证 Host B 是否可达。

```
[Sysname] ping 10.1.4.1
PING 10.1.4.1 (10.1.4.1) 56(84) bytes of data.
64 bytes from 10.1.4.1: icmp_seq=1 ttl=128 time=0.949 ms
64 bytes from 10.1.4.1: icmp_seq=2 ttl=128 time=0.169 ms
64 bytes from 10.1.4.1: icmp_seq=3 ttl=128 time=0.840 ms
```

```
64 bytes from 10.1.4.1: icmp_seq=4 ttl=128 time=0.173 ms

--- 10.1.4.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.169/0.532/0.949/0.364 ms, pipe 2
```

目 录

1 设备管理配置

1.1 设备管理简介

通过设备管理功能，用户能够查看设备当前的工作状态，配置设备运行的相关参数，实现对设备的日常维护和管理。

目前的设备管理主要提供重启设备、指定设备下次启动时采用的启动文件和配置 CPU 和主板的温度告警阈值等功能。

1.2 设备管理配置

1.2.1 配置设备重启

当设备运行出现故障时，用户可以根据实际情况，通过重启设备来排除故障。该操作等效于给设备断电后又上电启动，主要用于远程维护时，可以直接重启设备，而不需要到设备所在地进行硬件重启。

表1-1 配置设备重启

操作	命令	说明
进入系统视图	**system-view**	-
重新启动整个系统	**reboot**	必选

注意

重新启动会导致业务中断，请谨慎使用。

1.2.2 指定设备启动文件

启动文件是用于引导、启动设备的应用程序文件。当存储介质中有多个启动文件时，用户可以通过以下命令，指定设备下次启动时所采用的文件。主用启动文件用于引导、启动设备；备用启动文件只用于异常情况下，主用启动文件不可用时，引导、启动设备。

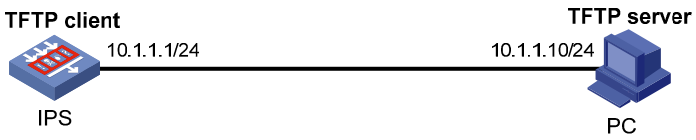
表1-2 指定设备启动文件

操作	命令	说明
指定设备启动文件	**boot-loader file** *file-name* { **backup** | **main** }	必选 该命令可在用户视图下执行，也可在系统视图下执行

1.2.3 从 TFTP 服务器下载文件

当设备作为 TFTP 客户端时，可以通过以下命令从 TFTP 服务器下载设备启动文件到本地设备。

图1-1 从 TFTP 服务器下载文件组网图



使用 TFTP 之前，网络管理员需要配置好 TFTP 客户端和服务器的 IP 地址，并且确保客户端和服务器之间的路由可达。

表1-3 从 TFTP 服务器下载文件

操作	命令	说明
进入系统视图	**system-view**	-
从 TFTP 服务器下载文件	**bootimage upgrade tftp** *ip-address* **get** *filename*	必选

注意

- 设备仅支持同时存放 3 个软件版本。如果采用命令行的方式下载软件版本，下载前，无论设备是否已经存放了 3 个软件版本，当下载的软件版本与现有软件版本同名，系统将直接覆盖原有同名的版本文件；如果下载前，设备已经存放了 3 个软件版本，并且下载的软件版本与现有软件版本不同名，下载将失败，同时系统还会提示“Up to three software images can be supported.”即，设备的软件版本数已经达到最大值 3，不可以再下载不同名的版本文件了。
- 待下载的文件必须是合法的启动文件，否则无法进行下载。
- 如果设备的剩余存储空间不足，请删除原有的应用程序后再进行下载。

1.2.4 配置 CPU 和主板的温度告警阈值

通过以下配置任务，用户可以设置 CPU 和主板的温度告警阈值。当 CPU 或主板的温度超出用户设定的阈值时，设备系统会发出告警信号，便于用户及时进行处理。

表1-4 配置单板的温度告警阈值

操作	命令	说明
进入系统视图	**system-view**	-
配置 CPU 和主板的温度告警阈值	**temperature-limit** { **board** | **cpu** } *lower-value upper-value*	可选 缺省情况下，主板或 CPU 上的温度告警下限值为 10 摄氏度，上限值为 80 摄氏度

1.2.5 设备管理显示和维护

在完成上述配置后，在用户视图或者系统视图下执行 **display** 命令可以显示配置后设备的运行情况，通过查看显示信息验证配置的效果。

表1-5 设备管理显示和维护

操作	命令
显示启动文件信息	**display boot-loader**
显示 CPU 占用率的统计信息	**display cpu-usage**
显示设备上的 CF 卡信息、硬盘信息和制造信息	**display device** [**cf-card** | **harddisk** [*harddisk-num*] | **manuinfo**]
显示设备的温度信息	**display environment** [**cpu**]
显示设备内置风扇的工作状态	**display fan** [*fan-id*]
显示设备内存的使用状况	**display memory**
显示设备电源的状况	**display power** [*power-id*]

1.3 设备管理典型配置举例

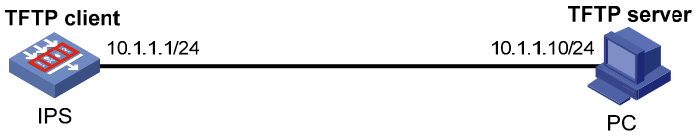
1.3.1 设备升级配置举例

1. 组网需求

- IPS 设备作为 TFTP 客户端，PC 作为 TFTP 服务器。
- IPS 设备管理口的 IP 地址为 10.1.1.1/24，PC 的 IP 地址为 10.1.1.10/24。
- IPS 设备通过 TFTP 协议从 TFTP 服务器上下载启动文件。

2. 组网图

图1-2 配置设备升级组网图



3. 配置步骤

(1) 配置 PC（TFTP 服务器）。在 PC 上启动 TFTP 服务器，配置 TFTP 工作目录，并将要下载到 IPS 设备的启动文件放到工作目录下。（具体配置步骤略）

(2) 配置 IPS 设备（TFTP 客户端）。

进入系统视图。

```
<Sysname> system-view
```

从 TFTP 服务器下载启动文件 bzImage。

```
[Sysname] bootimage upgrade tftp 10.1.1.10 get bzImage
```

指定 bzImage 为系统下次启动时的主用启动文件。

```
[Sysname] boot-loader file bzImage main
```

重启 IPS 设备，实现 IPS 设备启动文件的升级。

```
[Sysname] reboot
Current configuration may be lost in next startup if you continue.Are you sure?
(Y/N) [N]: y
```

目 录

1 系统基本配置

1.1 系统基本配置

1.1.1 进入或退出系统视图

当用户登录到设备后，会自动进入用户视图，此时屏幕显示的提示符是：<*设备名*>。要进入或退出系统视图，用户可以进行如下的操作。

表1-1 进入或退出系统视图

操作	命令	说明
进入系统视图	**system-view**	-
从系统视图返回到用户视图	**quit**	-

说明

使用 **quit** 命令，可以从当前视图返回上一层视图。如果用户需要从任意的非用户视图返回到用户视图，可以执行 **return** 命令，也可以直接按组合键<Ctrl+Z>完成。

1.1.2 配置设备名称

用户可以使用 **sysname** 命令用来设置设备的名称。设备的名称对应于命令行接口的提示符，如设备的名称为 Sysname，则用户视图的提示符为<Sysname>。

表1-2 配置设备名称

操作	命令	说明
进入系统视图	**system-view**	-
设置设备名称	**sysname** *sysname*	可选 缺省情况下，设备名称与设备型号有关，请以设备的实际情况为准

1.1.3 配置系统时间

1. 系统时间配置

为了保证与其它设备协调工作，用户需要将系统时间配置准确。

表1-3 配置系统时间

操作	命令	说明
配置时间和日期	**clock datetime** *HH:MM:SS YYYY/MM/DD*	可选 该命令在用户视图下执行

操作	命令	说明
配置系统所在的时区	**clock timezone** { **gmt** | **gmt+1** | **gmt+10** | **gmt+11** | **gmt+12** | **gmt+2** | **gmt+3** | **gmt+4** | **gmt+5** | **gmt+6** | **gmt+7** | **gmt+8** | **gmt+9** | **gmt-1** | **gmt-10** | **gmt-11** | **gmt-12** | **gmt-2** | **gmt-3** | **gmt-4** | **gmt-5** | **gmt-6** | **gmt-7** | **gmt-8** | **gmt-9** }	可选 该命令在用户视图下执行 缺省情况下，本地时区为东八时区，即 GMT+8

2. 系统时间的显示

系统时间是系统信息时间戳显示的时间，该时间与**display clock**命令显示的时间相同。该时间由**clock datetime**和**clock timezone**命令联合决定。如果以上两条命令都不配置，则**display clock**命令显示的为原系统时间。如果把两条以上命令任意组合进行配置，配置后的系统时间请参见 表1-4。表中配置列各参数的含义为：

- 1：表示执行 **clock datetime** 命令配置了时间 *HH:MM:SS*；
- 2：表示执行 **clock timezone** 命令配置了时区参数，时间偏移量为 *n*（-9～+9）；
- [1]：表示 **clock datetime** 命令是可选配置，可执行也可不执行。
- 表中举例默认原系统时间为 2005/1/1 1:00:00。

表1-4 系统时间配置和显示关系表

配置	**display clock** 显示的时间	举例
1	*HH:MM:SS*	配置：clock datetime 1:0:0 2007/1/1 显示：Mon Jan 1 01:00:00 2007 GMT+8
2	原系统时间+“*n*”	配置：clock timezone gmt+1 显示：Sat Jan 1 02:00:00 2005 GMT+1
1、2	“*HH:MM:SS*”+“*n*”	配置：clock datetime 2:0:0 2007/2/2 和 clock timezone gmt+1 显示：Fri Feb 2 03:00:00 2007 GMT+1
[1]、2、1	*HH:MM:SS*	配置：clock timezone gmt+1 和 clock datetime 3:0:0 2007/3/3 显示：Sat Mar 3 03:00:00 2007 GMT+1

1.1.4 配置用户连接的超时时间

用户可以使用 **idle-timeout** 命令来设置用户连接的超时时间。如果在超时时间段内设备和用户之间没有消息交互，设备就会自动断开用户连接。

表1-5 配置用户连接的超时时间

操作	命令	说明
进入系统视图	**system-view**	-
配置用户连接的超时时间	**idle-timeout** *minutes* [*seconds*]	可选 缺省情况下，用户连接的超时时间为 5 分钟

1.1.5 配置用户登录密码

用户可以使用 **password** 命令来设置 Console 口和 Telnet 用户登录设备的密码；还可以使用 **reset web-admin-user-password** 命令将 Web 用户 admin 的密码恢复到缺省情况“admin”。

表1-6 配置用户登录密码

操作	命令	说明
进入系统视图	**system-view**	-
配置用户登录密码	**password**	可选 缺省情况下，用户登录密码为“H3C”
恢复 Web 用户 admin 的初始密码	**reset web-admin-user-password**	可选 缺省情况下，Web 用户 admin 的密码为“admin”

说明

- 缺省情况下，设备存在用户名为“admin”、密码为“admin”的 Web 用户。
- 若 admin 用户已被删除，则执行 **reset web-admin-user-password** 命令无效。

1.1.6 收集诊断信息

通过 **collect diag_info** 命令可以将系统产生的调试信息生成一个名为“h3c.debug”的文件，并上传到指定的 TFTP 服务器上保存。当设备发生故障时，用户可以将生成的文件发给设备维护人员，以便定位故障。

表1-7 收集诊断信息

操作	命令	说明
进入系统视图	**system-view**	-
收集诊断信息	**collect diag_info** *ip-address*	必选

说明

收集诊断信息之前，需要配置好 TFTP 服务器的 IP 地址，并确保设备和 TFTP 服务器之间路由可达。

1.1.7 系统基本配置显示和维护

在完成上述配置后，执行 **display** 命令可以查看系统相应的配置信息和运行信息。

表1-8 系统基本配置显示和维护

操作	命令
在用户视图下，显示系统版本信息	**display version**

操作	命令
在用户视图下，显示系统当前的时间和日期	**display clock**
在系统视图下，显示用户连接的超时时间	**display idle-timeout**

1.2 命令行特性

1.2.1 命令行简介

命令行接口是设备与用户之间的交互界面。通过命令行接口，用户可以输入命令对设备进行配置，并可以通过查看输出的信息确认配置结果，方便用户配置和管理设备。

为提高设备的可管理性和可操作性，命令行接口还提供了如下的特性：

- 用户随时可以键入“?”以获得在线帮助；
- 提供种类丰富、内容详尽的调试信息，帮助用户诊断、定位网络故障；
- 提供命令历史记录功能，用户可以方便地查看曾经执行过的命令，并再次执行；
- 支持不完整关键字输入，用户只需键入唯一标识关键字的部分字符即可正确识别、执行该关键字。比如命令 **display interface**，用户在执行该命令时，只需输入“**dis int**”。

1.2.2 命令行在线帮助

命令行接口提供如下几种在线帮助：

- 完全帮助
- 部分帮助

通过上述各种在线帮助能够获取到帮助信息，分别描述如下：

(1) 在任意视图下，使用 **help** 命令来显示命令行使用的帮助信息。

表1-9 显示命令行使用的帮助信息

操作	命令	说明
显示命令行使用的帮助信息	**help**	可选 该命令在任意视图下执行

(2) 在任意视图下，使用 **list** 命令来显示该视图下所有可以使用的命令。

表1-10 显示当前视图下所有可以使用的命令

操作	命令	说明
显示当前视图下所有可以使用的命令	**list**	可选 该命令在任意视图下执行

(3) 在任意视图下，键入“?”获取该视图下所有的命令及其简单描述。

```
<Sysname>
  boot-loader         Boot configuration
  clock               Clock configuration
  display             Display configuration
  help                Description of the interactive help system
```

```
  list               Display command list
  ping               Ping function
  quit               Return to previous view
  return             Return to user view
  system-view        Enter the system view
  temperature-limit  Temperature limit configuration
  terminal           Terminal configuration
  undo               Negate a command or set its default(s)
<Sysname>
```

说明

键入的“?”在界面上不显示。

(4) 键入一条命令，后接以空格分隔的“?”，如果该位置为关键字，则列出全部关键字及其简单描述。

```
<Sysname>display
  boot-loader      Display boot loader information
  clock            Clock configuration
  cpu-usage        CPU information
  device           Display device information
  environment      Display environment information
  fan              Display fan status
  history-command  The historical command list
  interface        Interface configuration
  memory           Display memory information
  power            Display power status
  version          System version
<Sysname>display
```

(5) 键入一条命令，后接以空格分隔的“?”，如果该位置为参数，则列出有关的参数描述。

```
<Sysname>system-view
[Sysname]idle-timeout
  <1-1440>  Timeouts value, the range is [1-1440] minute(s)
[Sysname]idle-timeout 100
  <0-59>  Timeouts value, the range is [0-59] second(s)
  <cr>
[Sysname]idle-timeout 100
```

<cr>表示该位置无参数，在紧接着的下一个命令行该命令被复述，直接键入回车即可执行。

(6) 键入一个字符串，其后紧接“?”，列出以该字符串开头的所有命令。

```
<Sysname>te
  temperature-limit  Temperature limit configuration
  terminal           Terminal configuration
<Sysname>te
```

(7) 键入一条命令，后接一个字符串紧接“?”，列出命令以该字符串开头的所有关键字。

```
<Sysname> display de
  device  Display device information
<Sysname>display de
```

(8) 键入命令的某个关键字的前几个字母，按下<Tab>键，如果以输入字母开头的关键字唯一，则可以显示出完整的关键字；如果不唯一，则将显示所有匹配的关键字。

```
<Sysname>bo
<Sysname>boot-loader
<Sysname>boot-loader file

<Sysname>t
<Sysname>te
temperature-limit    terminal
<Sysname>te
```

1.2.3 命令行的 undo 格式

在命令前加 **undo** 关键字，即为命令的 undo 形式。几乎每条配置命令都有对应的 undo 形式，**undo** 命令一般用来恢复缺省情况、禁用某个功能或者删除某项设置。例如，**sysname** 命令用来设置设备的名称；**undo sysname** 用来恢复设备名称为缺省值。

1.2.4 命令行编辑功能

命令行接口提供了基本的命令编辑功能，支持多行编辑，如 表 1-11所示。

表1-11 编辑功能表

按键	功能
普通按键	若编辑缓冲区未满，则插入到当前光标位置，并向右移动光标
<Backspace>	删除光标位置的前一个字符，光标前移
<Ctrl+A>	将光标移动到当前行的开头
<Ctrl+B>或左光标键←	将光标向左移动一个字符
<Ctrl+C>	停止当前正在执行的功能
<Ctrl+D>	删除当前光标所在位置的字符
<Ctrl+E>	将光标移动到当前行的末尾
<Ctrl+F>或右光标键→	光标向右移动一个字符
<Ctrl+H>	删除光标左侧的一个字符
<Ctrl+K>	终止呼出的连接
<Ctrl+N>或下光标键↓	显示历史命令缓冲区中的后一条命令
<Ctrl+P>或上光标键↑	显示历史命令缓冲区中的前一条命令
<Ctrl+V>	粘贴剪贴板的内容
<Ctrl+W>	删除光标左侧连续字符串内的所有字符
<Ctrl+Z>	退回到用户视图
<Esc+B>	将光标移动到左侧连续字符串的首字符处
<Esc+D>	删除光标所在位置及其右侧连续字符串内的所有字符
<Esc+F>	将光标向右移到下一个连续字符串之前

按键	功能
<Tab>键	输入不完整的关键字后按下<Tab>键，系统自动执行部分帮助，具体说明参见“1.2.2 命令行在线帮助”

说明

使用<Esc+B>、<Esc+D>和<Esc+F>组合键时，不能将<Caps Lock>键打开；其他组合键不受影响。

1.2.5 命令行显示

当显示信息较多时，系统会自动将信息分屏显示。通常情况下，一屏最多可以显示 25 行信息，用户也可以使用 **terminal rows** 命令设置用户界面下一屏显示的行数。

表1-12 配置一屏显示的行数

操作	命令	说明
配置一屏可以显示的信息的行数	**terminal rows** *rows*	可选 该命令在用户视图下执行 缺省情况下，一屏可以显示的信息行数为 25

注意

显示终端实际一屏可显示的行数由终端的规格决定。比如通过 **terminal rows** 命令配置一屏可显示 40 行信息，但显示终端的规格为 24 行，当暂停显示按空格键时，设备发送给显示终端的信息为 1～40 行，但当前屏幕显示的是第 18～40 行的信息，前面的 17 行信息需要通过<Page Up>/<Page Down>键来翻看。

命令行接口还提供了这样的显示特性：在一次显示信息超过一屏时，提供了暂停功能，这时用户可以有三种选择，如 表 1-13所示。

表1-13 显示功能表

按键或命令	功能
暂停显示时键入空格键	继续显示下一屏信息
暂停显示时键入回车键	继续显示下一行信息
暂停显示时键入<Ctrl+C>	停止显示和命令执行
<Ctrl+E>	将光标移动到当前行的末尾
<PageUp>	显示上一页信息
<PageDown>	显示下一页信息

1.2.6 命令行的历史记录功能

命令行接口将用户最近使用的历史命令自动保存，用户可以随时调用保存的历史命令，并重复执行。命令行接口为每个用户保存 20 条历史命令。操作如 表 1-14所示。

表1-14 访问历史命令

操作	命令或按键	结果
显示历史命令	**display history-command**	显示用户输入的有效历史命令
访问上一条历史命令	上光标键↑或<Ctrl+P>	如果还有更早的历史命令，则取出上一条历史命令
访问下一条历史命令	下光标键↓或<Ctrl+N>	如果还有更晚的历史命令，则取出下一条历史命令

说明

用光标键对历史命令进行访问，在 Windows 200X 及 XP 的 Terminal 和 Telnet 下都是有效的，但对于 Windows 9X 超级终端，↑、↓光标键会无效，这是由于 Windows 9X 的超级终端对这两个键作了不同解释所致，这时可以用组合键<Ctrl+P>和<Ctrl+N>来代替↑、↓光标键达到同样目的。

目 录

1 加密 P2P 识别

1.1 加密 P2P 识别简介

随着 P2P（Peer to Peer，对等网络）技术的不断发展和广泛应用，P2P 数据流量在网络流量中所占的比重越来越大，这不仅对网络带宽资源造成了浪费，还对其他业务的正常运行造成了严重影响。通过带宽管理模块，设备可以对 P2P 流量进行识别和控制，但是无法识别加密的 P2P 流量。需要启用加密 P2P 识别功能，设备才能对加密的 P2P 流量进行识别。

加密 P2P 识别有长度序列识别、模糊识别和精确识别三种方式：

- 加密 P2P 长度序列识别：首先根据 P2P 软件的明文特征识别出运行 P2P 软件的主机，再对这些主机之间交互的流量的长度序列特征进行分析，识别出加密 P2P 流量。此方式的识别效率较高，很少发生误报。
- 加密 P2P 模糊识别：利用 P2P 系统的逻辑网络直径较大以及每个节点都具有客户端、服务器双重角色的特点，通过网络直径计算和节点角色分析的方法对加密 P2P 流量进行模糊的识别。此方式的识别效率最高，但误报率也最高。
- 加密 P2P 精确识别：通过 P2P 协议特征分析和 Peer 节点识别的方法对加密 P2P 流量进行精确的识别。此方式的识别效率最低，但不会发生误报。

长度序列识别、模糊识别和精确识别这三种加密 P2P 识别方式可以同时启用，其优先级从高到低依次为：模糊识别、精确识别、长度序列识别。

1.2 配置加密 P2P 识别

1.2.1 启用加密 P2P 识别

配置启用加密 P2P 识别功能。

表1-1 配置启用加密 P2P 识别功能

操作	命令	说明
进入系统视图	**system-view**	-
启用加密 P2P 识别功能	**p2p** { **length-serial** | **original** | **precise** } **enable**	必选 缺省情况下，未启用加密 P2P 识别功能

1.2.2 加密 P2P 识别显示和维护

在完成上述配置后，在系统视图下执行 **display** 命令可以显示加密 P2P 识别功能的启用状态。当加密 P2P 精确识别功能启用时，还会显示当前的 UDP 和 TCP 协商节点数量。

表1-2 加密 P2P 识别显示和维护

操作	命令
显示加密 P2P 识别功能的启用状态	**display p2p**

目 录

附录 A 缩略语表

[#](#) [P](#) [T](#)

缩略语	英语解释	中文解释
P		**Return**
P2P	Peer to Peer	对等网络
T		**Return**
TTL	Time To Live	生存时间