

第2篇 H3C 网络设备操作入门

第7章 路由器、交换机及其操作系统介绍

第8章 命令行操作基础

第9章 网络设备文件管理

第10章 网络设备基本调试

第7章 路由器、交换机及其操作系统介绍

构建各种规模的企业网络的主要设备是路由器 (router) 和交换机 (switch)。传统意义上，路由器是利用第三层 IP 地址信息进行报文转发的互联设备，交换机是利用第二层 MAC 地址信息进行数据帧交换的互联设备。本章将对路由器和交换机的上述区别和其它特点进行描述分析。(在本书中，如无特殊说明，“路由器”均指 IP 路由器，“交换机”均指以太网交换机)

H3C 公司提供全系列路由器、交换机及其它网络设备。本章在描述路由器和交换机的一般通用概念后，将向学员简单介绍 H3C 的路由器和交换机产品系列。

控制路由器和交换机工作的核心软件是网络设备的操作系统。H3C 网络设备使用的操作系统软件是 H3C Comware。本章将说明 H3C Comware 的概念、作用与特点。

7.1 本章目标

课程目标

● 学习完本课程，您应该能够：

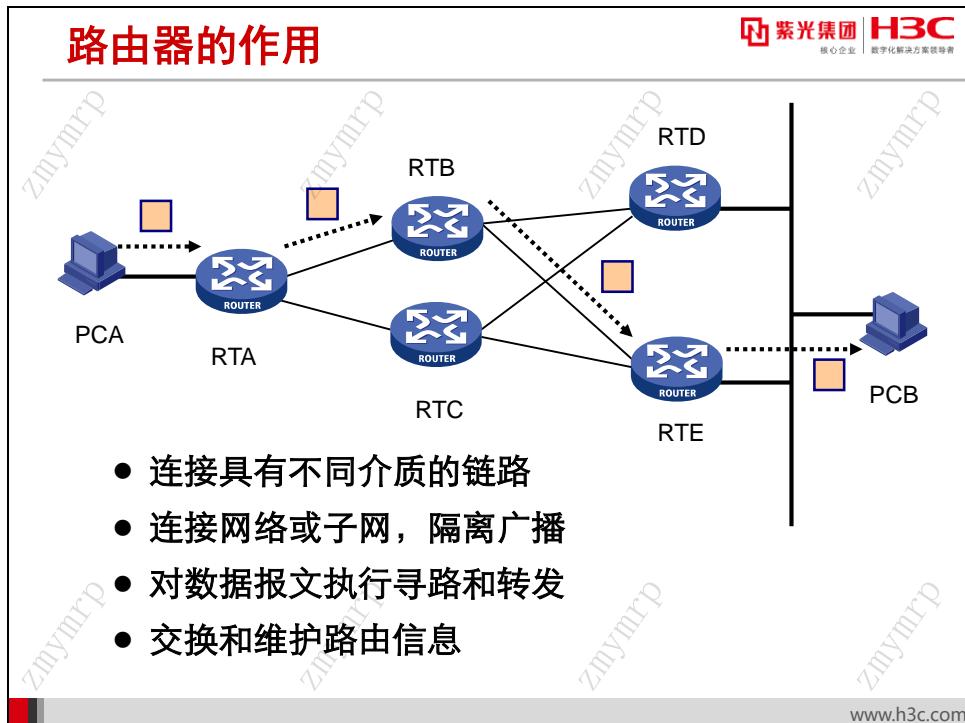
- 了解路由器、交换机的基本概念
- 初步了解H3C路由器和交换机的组成
- 掌握H3C网络设备操作系统

Comware的作用与特点



7.2 路由器与交换机的作用与特点

7.2.1 路由器的作用与特点



作为网络互联的一种关键设备，路由器是伴随着 Internet 和网络行业发展起来的。正如其名字的寓意一样，这种设备最重要的功能是在网络中对 IP 报文寻找一条合适的路径进行“路由”，也就是向合适的方向转发。它的实质是完成了 TCP/IP 协议族中 IP 层提供的无连接、尽力而为的数据报文传送服务。

在上图中，PCA 和 PCB 分别处于两个网段当中，因此，PCA 和 PCB 的通信必须依靠路由器这类网络中转设备来进行。先来考察 PCA 向 PCB 发送报文时，沿途经过的路由器的作用。

首先，PCA 会对 IP 报文的目的地址进行判断，对需要到达其他网段的报文，一律交给其默认网关进行转发，在本例中 PCA 的默认网关设置为 RTA。RTA 为了完成转发任务，会检查 IP 报文的目的地址，找到与自身维护的路由转发信息相匹配的项目，从而知道应该将报文从哪个接口转发给哪个下一跳路由器。在这个例子中，假设 RTA 通过路由转发将报文发送给了 RTB。类似地，RTB 经过路由查找将报文发送给 RTE。因为 RTE 通过 IP 报文的目的地址判断 PCB 处于其直连网络上，所以将报文直接发送给 PCB。（以上是对路由器进行 IP 报文转发过程和原理的大致描述，在后续的模块中，我们还将进一步学习路由信息和转发过程的细节。）

在上图中，路由器之间的连接可以是同样的链路类型，也可以是完全不同的链路类型。比如，对于 RTD 来讲，它的一侧使用时分复用的串行链路，而另外一侧使用共享介质同时与 RTE 和 PCB 连接。因此，路由器的第二个重要作用就是用来连接“异质”的网络。

最后，路由器进行报文转发依赖自身所拥有的路由转发信息，这些信息可以手工配置，但更常见的情况是路由器之间自动地进行路由信息的交换，以适应网络动态变化和扩展的要求，因此，路由器的另一个重要作用是交互路由等控制信息并进行最优路径的计算。

路由器的特点



紫光集团 | H3C
核心企业 | 数字化解决方案领导者

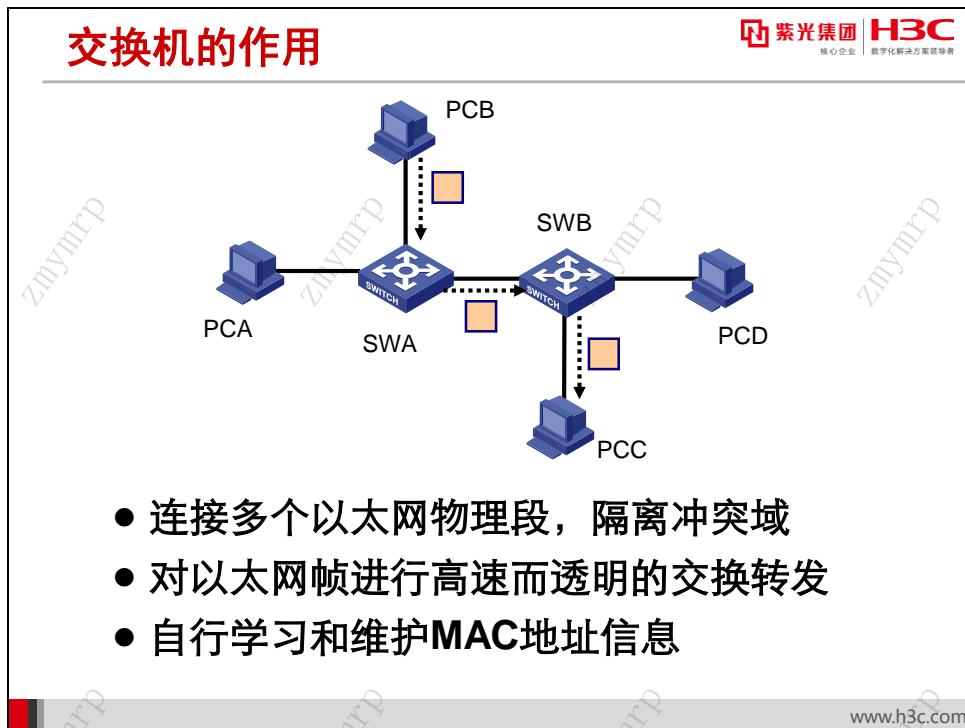
- 主要工作在OSI模型的物理层、数据链路层和网络层
- 根据网络层信息进行路由转发
- 提供丰富的接口类型
- 支持丰富的链路层协议
- 支持多种路由协议

www.h3c.com

了解了路由器的作用，对路由器的特点就比较容易理解：

- 按照 ISO/OSI 参考模型，路由器主要工作在物理层、数据链路层和网络层。当然，为了实现一些管理功能，比如路由器本身也可以作为 FTP 的服务器端，因此路由器也要实现传输层和应用层的某些功能。但从作为网络互联设备的角度讲，提供物理层、数据链路层和网络层的功能是路由器的基本特点；
- 路由器的接口类型比较丰富，因此可以用来连接不同介质的“异质”网络。比照第一个特点，也可以看出，路由器因此要支持较为丰富的物理层和链路层的协议和标准；
- 如在上面的例子看到，路由器要依靠路由转发信息对 IP 报文进行转发。这是 IP 层也是路由器的核心功能；
- 为了形成路由表和转发表，路由器要交互路由等协议控制信息。

7.2.2 交换机的作用与特点



如上图所示，PCA、PCB、PCC、PCD 和交换机 SWA、SWB 处于同一个局域网中，因此，SWA 和 SWB 的核心作用是利用桥接和交换将局域网进行扩展。

从数据转发机制上看，交换机与路由器的作用也有不同。假设 PCB 要和 PCC 进行通信，由于两者处于同一个网络，PCB 首先要根据 PCC 的二层地址（即 MAC 地址）信息，将信息封装成以太网帧，并通过自身的网络接口发出，于是 SWA 将收到此帧。与路由器不同，SWA 不是依靠第三层 IP 目的地地址，而是第二层的 MAC 地址来决定如何转发报文。SWA 在 MAC 地址表中查找与报文目的 MAC 地址匹配的表项，从而知道应该将报文从与 SWB 相连的端口转发出去；如果没有匹配的项目，报文将广播到除收到报文的入端口外的所有其他端口。SWB 也会执行同样的操作，直到把报文交给 PCC。

不难发现，在整个发送过程中，PCB 并不需要了解 SWA 的存在，而 SWA 同样不需要了解 SWB 的存在，因此这种交换过程是透明的。

交换机的特点



紫光集团 H3C

核心企业 数字化解决方案领导者

- 主要工作在OSI模型的物理层、数据链路层
- 提供以太网间的透明桥接和交换
- 依据链路层的MAC地址，将以太网数据帧在端口间进行转发

www.h3c.com

至此，从交换机的作用和转发报文过程看，我们可以将传统以太网交换机的特点归纳如下：

- 它主要工作在 OSI 模型的物理层、数据链路层，不依靠三层地址和路由信息；
- 传统交换机提供以太局域网间的桥接和交换，而不必连接不同种类的网络；
- 交换机上的数据交换依靠 MAC 地址映射表，这个表是交换机自行学习到的，而不需要相互交换目的地的位置信息。

7.2.3 交换机和路由器的发展趋势

路由器与交换机的发展趋势

紫光集团 H3C
核心企业 数字化解决方案领导者

- 路由和交换的融合
- 多业务功能的融合

www.h3c.com

路由器和交换机的发展趋势体现在两个融合上。

首先，路由器和交换机在功能上逐渐走向融合。路由主要体现在第三层（IP）互联的功能，而交换特指以太网数据链路层的交换。现在，越来越多的路由器开始提供二层以太网交换模块与功能；交换机也不仅仅提供二层交换的基本功能，而增加了路由等三层功能。如今，路由器和交换机依然是网络互联主要和关键的设备，交换和路由的融合扩展了这两种设备的应用范围，增加了设备使用的灵活性。

其次是多业务功能的融合。在网络应用的驱动下，安全、语音、无线等业务功能逐步被集成到路由器和交换机中。使得传统的路由交换设备不仅仅完成网络互联功能，还可以提供一定的增值业务功能。同时，这方面的特征还体现在设备厂商开放一定的接口，以促成厂商间在网络设备上实现一定程度的集成。

路由器和交换机有多种分类方法。比如，传统上根据设备的功能和性能分为高端、中端和低端路由器或交换机。也可以根据设备所在的网络位置，分为核心、汇聚、接入路由器或交换机。另外，其他的一些分类和命名方法——如多业务路由器或交换机——则从另一个角度展示了路由器和交换机的用途和发展趋势。

7.3 H3C 路由器和交换机介绍

7.3.1 H3C 系列路由器



H3C CR16K 是 H3C 自主研发的核心路由器，采用业界先进的 CLOS 交换架构，整机交换容量高达 54.42Tbps，采用 Comware V7 网络操作系统，提供丰富的业务特性和强大的自愈功能，主要应用在运营商 IP 骨干网、数据中心骨干互联节点以及各种行业大型 IP 网络的核心和汇聚位置。

对于大型企业网络的核心和骨干层，H3C 提供 SR8800 系列路由器，该系列路由器采用了分布式的高性能网络处理器（NP）硬件转发技术和 Crossbar 无阻塞交换技术，保障了高处理性能。作为核心路由器，SR8800 提供双路由交换主控板，可支持 12 个业务板插槽，可支持万兆（10G）业务板。SR8800 同时融合了以太网交换机的特性，提供了常用二层功能，是典型的路由交换一体化设备。

SR6600 系列产品是 H3C 基于高端路由器平台自主研发的业务承载路由器。采用了全业务分布式处理架构，业务全部内置无需另外购置业务板卡，同时具备弹性可扩展业务处理能力，并采用自主研发的集路由转发与业务处理于一体的 Apollo 硬件芯片内核，实现高性能业务线速转发。SR6600 创新的以 IRF2 技术为基础，实现了广域网汇聚虚拟化，在降低运维、管理成本的同时，大幅提高网络可靠性。

MSR (Multiple Services Router) 多业务开放路由器是 H3C 专门面向行业分支机构和大中型企业而推出的新一代网络产品。包括 MSR56、MSR36 和 MSR26 等系列。MSR 路由器能够提供更智能的业务调度管理机制，支持业务模块化的松耦合，并能实现进程和补丁的动态加

载。硬件上，MSR 采用高性能多核 CPU 处理器及无阻塞交换架构，极大提升多业务并发处理能。

MSR 路由器另外一个显著的特点是采用了 OAA (Open Application Architecture) 开放应用体系架构，产品提供了一个公开软硬件接口及标准规范的开放平台，任何厂商与合作伙伴均可以基于此平台开发更为深层智能的网络应用功能。

此外，H3C 还提供 ER 系列模块化路由器，作为大型网络的汇聚或接入路由器以及小型网络的核心设备。

注意：

不同型号路由器的体系结构、安装、操作和配置等均可能有所差别。本课程基于 MSR36 系列路由器进行讲解，并以其作为实验操作的练习设备。如果读者所采用的设备型号与本书不同，可参考所用设备的相关手册。



上图显示了 H3C MSR36-40 路由器的直观图。MSR36-40 是一种模块化的路由器，前面板主要包括配置口 (Console) 和 CF 卡插槽以及多种类型的接口模块插槽。前面板还配置了系统指示灯、接口指示灯、CF 卡指示灯，以辅助用户对系统运行状态进行监控和判断。

MSR36-40 不仅支持多种可插拔的业务扩展模块，后面板上的电源模块也可以根据业务的需要进行灵活配置，并支持热插拔。

MSR36 系列路由器提供对通用模块 SIC（智能接口卡）和 HMIM（多功能接口模块）接口卡的支持，每个接口模块的大小、接口类型和数目也各不相同，用户可以根据实际情况进行灵活配置。

7.3.2 H3C 系列交换机



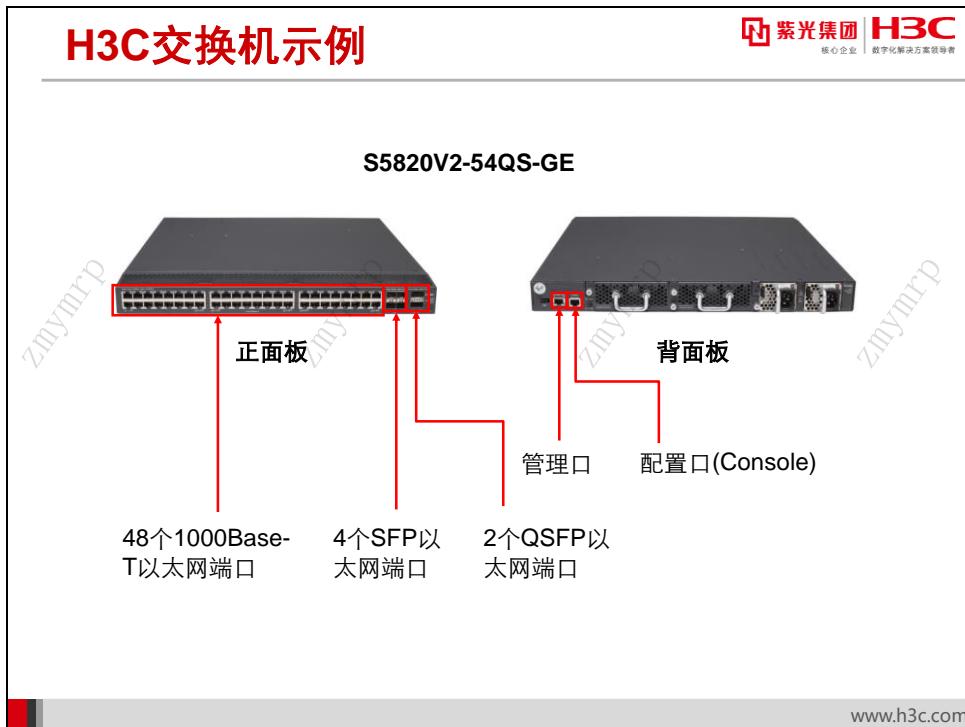
H3C 的 S12500 系列核心路由交换机，提供大容量、高性能的 L2/L3 转发服务，并集成了安全特性。H3C 高端交换机还包括 S10500、S9500E、S7500E 系列。

H3C 中低端交换机系列产品类型较多，包括 S5830、S5820、S5800V2、S5800、S5500-EI/SI、S5120-HI/EI/SI、S3600V2-EI/SI、S3100V2 系列等等。

本课程选用的 S5820V2 交换机系列产品是 H3C 基于全新软硬件平台开发的支持 IPv4/IPv6 双栈的路由交换机设备。根据提供接口与类型的不同又可分为 S5820V2-52Q、S5820V2-52QF、S5820V2-54QS-GE 等。

注意：

不同型号交换机的体系结构、安装、操作和配置等均可能有所差别。本课程基于 S5820V2 交换机进行讲解，并以其作为实验操作的练习设备。如果读者所采用的设备型号与本书不同，可参考所用设备的相关手册。



上图所示为 H3C S5820V2 系列交换机。与路由器类似，交换机也提供 **Console** 口进行设备参数的配置。

对各型号交换机的进一步命名主要根据交换机提供的以太端口数目、接口类型等。如 S5820V2-54QS-GE 交换机提供了 48 个 10M/100M/1000M 自适应以太端口、4 个 SPF 类型的 GE/10GE 以太端口，还提供了 2 个 QSFP 类型的 10GE/40GE 以太端口。

7.4 H3C 网络设备操作系统 Comware

Comware 的作用

 紫光集团 | H3C
核心企业 | 数字化解决方案领导者

- Comware 是设备运行的网络操作系统，H3C 产品的核心软件平台
- 对硬件驱动和底层操作系统进行屏蔽与封装
- 集成了丰富的链路层协议、以太网交换、IP 路由及转发、安全等功能模块
- 制定了软硬件接口标准规范，对第三方厂商提供开放平台与接口

H3C 网络设备的操作系统的名字是 Comware，它经历了从多产品多平台向统一平台发展和变革的过程。Comware 的含义是网络设备共用的核心软件平台。就像计算机的操作系统控制 PC 的作用一样，Comware 负责整个硬件和软件系统的正常运行，并为用户提供了管理设备的接口和界面。

类似于 OSI 和 TCP/IP 协议栈的分层思想，Comware 也是采用模块化的方法构建的。一方面，Comware 对硬件驱动和底层系统进行了封装，为上层各个模块提供了统一的编程接口。另外一方面，对于上层实现分为链路层、IP 转发、路由、安全等功能模块，以便于协议功能的实现和扩展。

最后，Comware 也制定了内部软硬件接口标准和规范，对第三方厂商提供了开放平台与接口。

注意：

不同版本的 Comware 软件的操作和命令等均可能有所差别。本课程基于 Comware V7 版本进行讲解。如果读者所采用的版本与本书不同，可参考所用版本的相关手册。

Comware的特点



- 支持IPv4及IPv6多协议
- 支持多核CPU
- 路由和交换功能融合
- 高可靠性和弹性扩展
- 灵活的裁减和定制功能

www.h3c.com

Comware 的特点可以归纳如下：

- 支持 IPv4 和 IPv6 双协议栈。IPv6 是下一代的 IP 标准及技术，可以解决 IPv4 地址缺乏等相关重要问题；
- 支持多核 CPU，增强网络设备的处理能力；
- 同时提供路由和交换功能。作为网络设备的操作系统平台，可以同时被路由器和交换机所共用；
- Comware 注重了系统的高可靠性和弹性扩展功能，提供了 IRF (Intelligent Resilient Framework, 智能弹性架构) 特性；
- Comware 采取组件化设计并提供开放接口，便于软件的灵活裁减和定制，因此具有良好的伸缩性和可移植性。

7.5 本章总结

本章总结

- 路由器是利用三层IP地址信息进行报文转发的互联设备
- 交换机是利用二层MAC信息进行数据帧交换的互联设备
- 路由器、交换机的运行依赖的软件核心是网络设备的操作系统
- **H3C Comware**软件平台是H3C IP网络设备的核心软件平台

第8章 命令行操作基础

H3C Comware 采用基于命令行的用户接口 (Command Line Interface, CLI) 进行管理和操作。用户可以通过 Console、AUX、Telnet 和 SSH 等多种方法连接到网络设备。为了提高网络配置的安全性和可管理性, H3C Comware 采用了配置权限的分级控制方法。H3C Comware 还提供了友好的操作界面和灵活而丰富的配置命令, 以便用户更好地使用网络设备, 本章将介绍一些常用的命令行特性和操作配置命令。

8.1 本章目标

课程目标

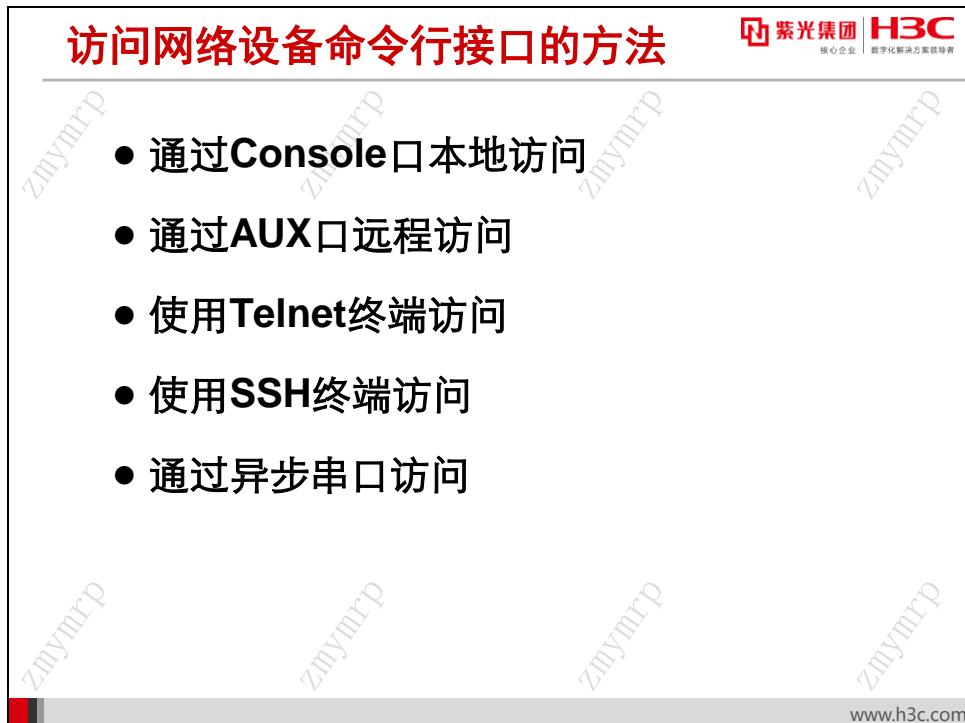
● 学习完本课程, 您应该能够:

- 掌握配置网络设备的基本方法
- 掌握分级命令行的使用方法
- 掌握网络设备的常用配置命令



8.2 访问网络设备的命令行接口

8.2.1 连接到命令行接口的方法

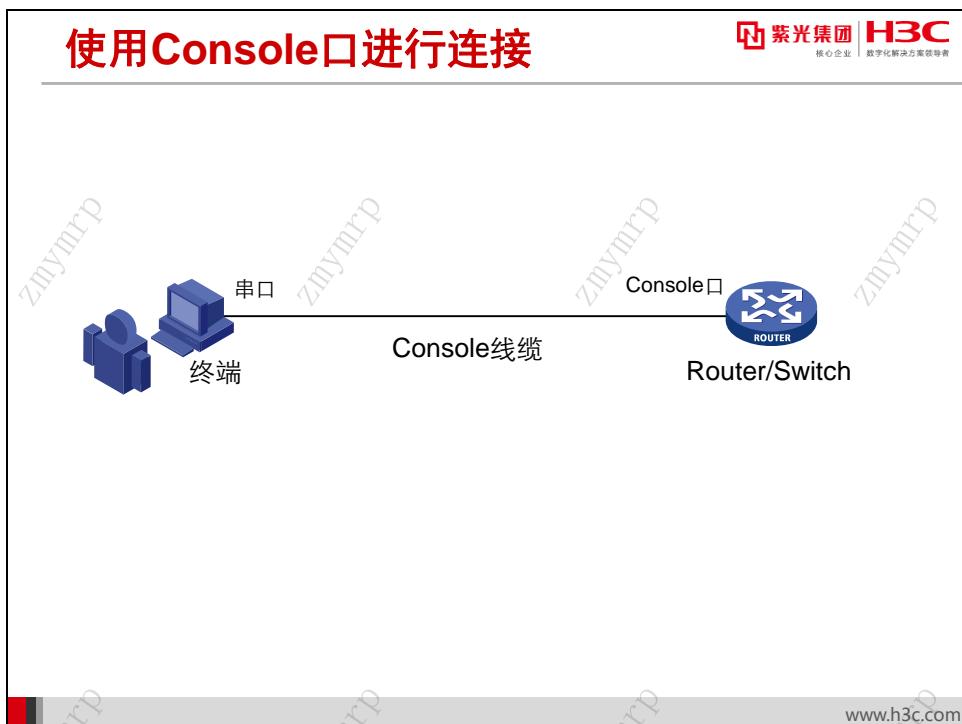


为了通过命令行接口（Command Line Interface, CLI）对设备进行管理和操作，必须使用基于字符的终端或远程登录方式连接到网络设备。H3C 网络设备提供了访问 CLI 的多种方法：

- 通过 **Console** 口本地访问
- 通过 **AUX** 口远程访问
- 使用 **Telnet** 终端访问
- 使用 **SSH** 终端访问
- 通过异步串口访问

下面将详细介绍前四种访问方式。第五种方式并不常用，本书不做详细讲解。

8.2.2 通过 Console 进行连接

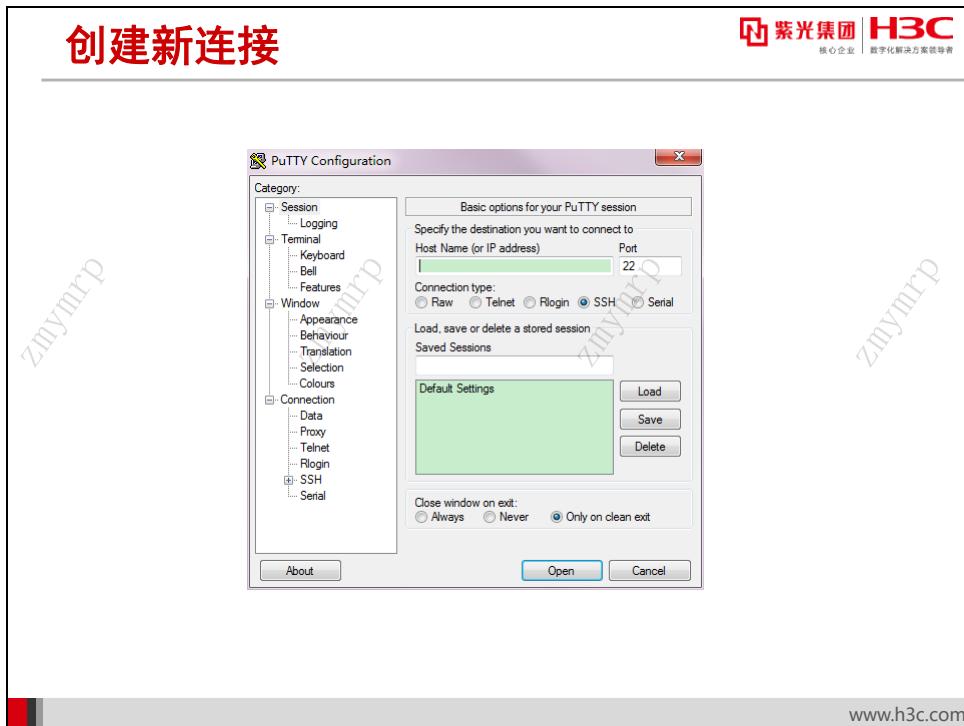


用终端登录到网络设备的 **Console** 端口（控制台端口）就是一种最基本的连接方式。路由器和交换机都提供一个 **Console** 口，端口类型为 **EIA/TIA-232 DCE**。用户需要把一台字符终端的串行接口通过专用的 **Console** 线缆连接到网络设备的 **Console** 口上，然后通过终端访问 **CLI**。

Console 线的一端为 **RJ45** 接头，用于连接路由器或交换机的 **Console** 口，另一端为 **DB9** 接头，用于与终端的串口相连。由于 **Console** 线缆的长度和传输距离是有限的，这种方法只适用于本地操作。

Console 口连接是最基本的连接方式，也是对设备进行初始配置时最常用的方式。路由器和交换机的 **Console** 口用户默认拥有最大权限，可以执行一切操作和配置。

在实际应用时，通常会用运行终端仿真程序的计算机替代终端。下面以使用 **Windows 7** 操作系统的个人计算机为例讲解连接方法。



首先，需要在计算机上安装终端仿真软件 PuTTY，以便后续通过该软件登录设备，对设备进行配置。



打开软件后，在连接方式【Connection type】处选择串口【Serial】，串口线需根据实际连接情况选择，本例中使用串口 COM4。波特率使用默认的 9600 即可。

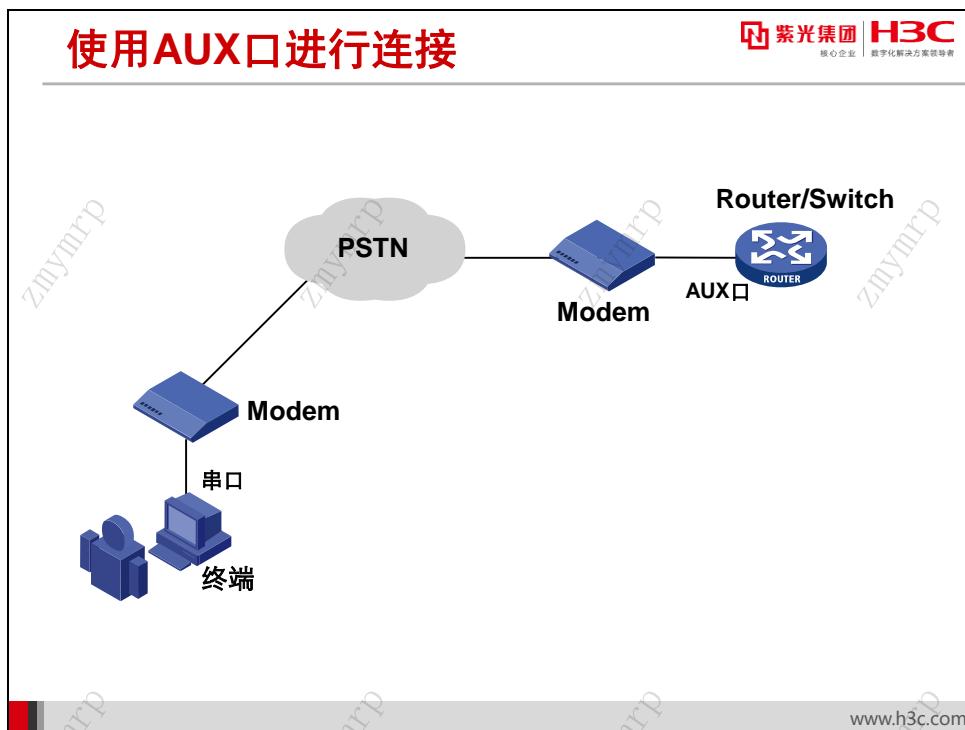
注意：

大部分 H3C 网络设备的默认波特率为 9600，但有些设备可能采用其他的默认波特率，具体操作时可参考网络设备的相关手册。



设置好通讯参数后，直接点击【Open】，就可进入到如上图的设备配置界面了。

8.2.3 使用 AUX 口进行连接

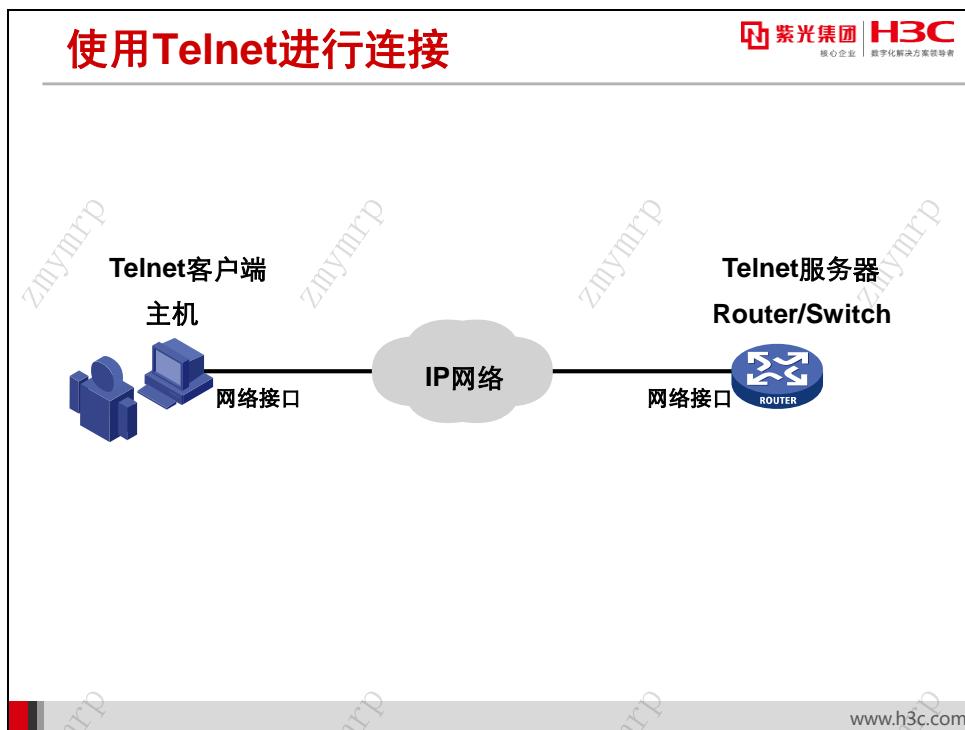


网络设备提供的 AUX 端口 (Auxiliary port, 辅助端口) 通常用于对设备进行远程操作和配置，端口类型为 EIA/TIA-232 DTE。在这种配置环境中，用户字符终端通过 PSTN (公共交换电话网络) 建立拨号连接，接入到网络设备的 AUX 口上。当然，为了建立这个连接，用户终端和网络设备双方都需要一台 Modem (调制解调器)。其中网络设备的 AUX 口通过 AUX 电缆连接到 Modem，终端则用串口通过 Modem 线缆连接到 Modem。

在实际应用时，同样经常用运行终端仿真程序的计算机替代终端。

AUX 口配置虽然不是一种常用的方法，但在 IP 网络中断时，可以满足远程操作设备的需求。本教材中对此不再进行详细介绍。

8.2.4 使用 Telnet 进行连接



Telnet 是基于 TCP 的用于主机或终端之间远程连接并进行数据交互的协议。它遵循客户机/服务器的操作模型，使用户的本地计算机能够与远程计算机连接，成为远程主机的一个终端，从而允许用户登录到远程主机系统进行操作。

网络设备可以作为 Telnet 服务器，为用户提供远程登录服务。在这种连接模式下，用户通过一台作为 Telnet 客户端的计算机直接对网络设备发起 Telnet 登录，登录成功后即可对设备进行操作配置。

使用 Telnet 方式有一些先决条件。首先，客户端与网络设备（服务器）之间必须具备 IP 可达性，这意味着网络设备和客户端必须配置了 IP 地址，并且其中间网络必须具备正确的路由。第二，出于安全性考虑，网络设备必须配置一定的 Telnet 验证信息，包括用户名、口令等等；另外，中间网络还必须允许 TCP 和 Telnet 协议报文通过，而不能禁止之。

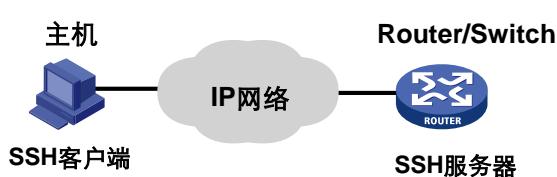
当然，网络设备也可以作为 Telnet 客户端登录到其他网络设备上。

8.2.5 通过 SSH 进行连接

SSH介绍



- **SSH (Secure Shell, 安全外壳) 在无安全保证的网络上提供安全的远程登录等服务**
- **由传输协议、验证协议和连接协议三部分组成**
- **使用TCP端口22**
- **提供Password和Publickey两种验证方式**



www.h3c.com

使用 Telnet 远程配置网络设备时，所有的信息都是以明文的方式在网络上传输的。为了提高交互数据的安全性，可以使用 **SSH (Secure Shell, 安全外壳)** 终端进行配置。用户通过一个不能保证安全的网络环境远程登录到设备时，SSH 特性可以提供安全保障和强大的验证功能，以保护设备不受诸如 IP 地址欺诈、明文密码截取等攻击。

SSH 技术标准由传输协议、验证协议和连接协议三个部分组成，并且也是基于 TCP 实现的，使用 TCP 端口号 22。如同 Telnet 一样，一台网络设备可以接受多个 SSH 客户端的连接。

网络设备还支持作为 SSH 客户端的功能，允许用户与支持 SSH 服务器的设备建立 SSH 连接，用户从而可以从本地设备通过 SSH 登录到远程设备上。

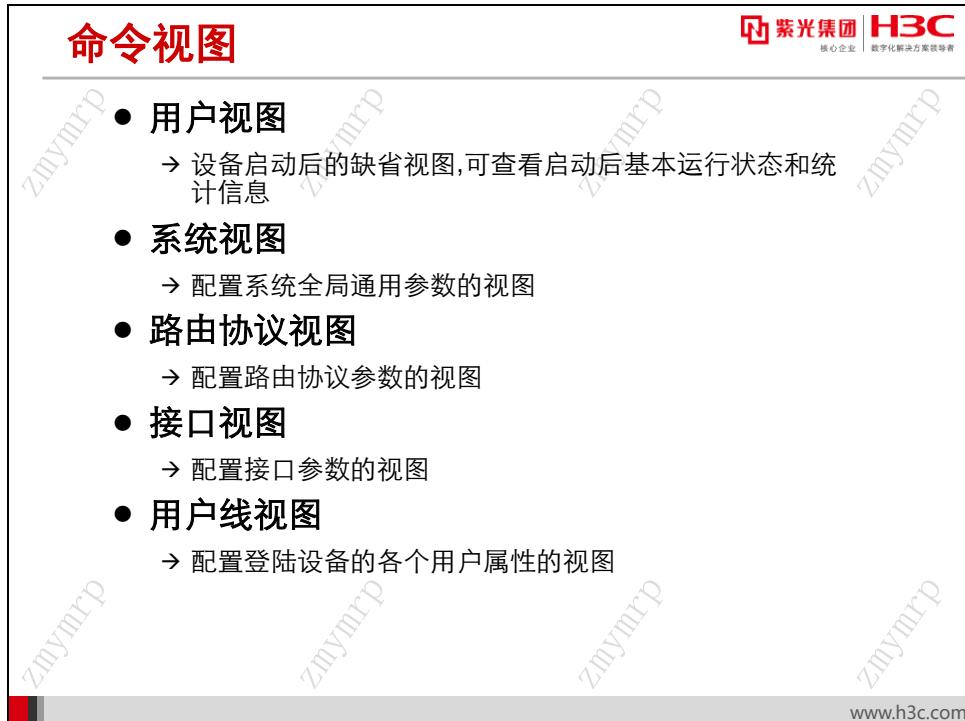
SSH 提供两种验证方法：

- **Password 验证：**客户端向服务器发出 **password** 验证请求，将用户名和密码加密后发送给服务器；服务器将该信息解密后得到用户名和密码的明文，与设备上保存的用户名和密码进行比较，并返回验证成功或失败的消息。在这种方式下，传输的数据会被加密，但是客户端无法了解要连接的服务器是否真正的服务器。
- **Publickey 验证：**用户需要创建一对密钥，并将公共密钥保存在服务器端。客户端发送 RSA 验证请求和自己的公钥模数给服务器端；服务器进行合法性检查，如果不合法，则直接发送失败消息，否则产生一个 32 字节的随机数，按 **MSB (Most Significant Bit, 最高位)** 优先排列成一个 **MP (多精度)** 型整数，并用客户端的公钥加密后向客户端发起一个验证挑战；客户端收到挑战消息后用自己的私钥解密得到 **MP** 型整数，用它和会话 **ID** (密钥和算法协商阶段生成的中间产物) 生成消息摘要 **MD5** 值，把这

个 16 字节的 MD5 值加密后发送给服务器；服务器接收后还原出 MD5 值并与它自己计算出的 MD5 值相比较，如果相同，验证成功，发送成功消息；否则失败，发送失败消息。

8.3 命令行使用入门

8.3.1 命令视图



命令视图是 Comware 命令行接口对用户的一种呈现方式。用户登录到命令行接口后总会处于某种视图之中。当用户处于某个视图中时, 就只能执行该视图所允许的特定命令和操作, 只能配置该视图限定范围内的特定参数, 只能查看该视图限定范围内允许查看的数据。

命令行接口提供多种命令视图, 比较常见的命令视图类型包括:

- 用户视图**

网络设备启动后的缺省视图, 在该视图下可以查看启动后设备基本运行状态和统计信息。

- 系统视图**

这是配置系统全局通用参数的视图, 可以在用户视图下使用 `system-view` 命令进入该视图。

- 路由协议视图**

在后续的章节中, 我们会学习路由和路由协议, 路由协议的大部分参数是在路由协议视图下进行配置的。比如 `OSPF` 协议视图、`RIP` 协议视图等。在系统视图下, 使用路由协议启动命令可以进入到相应的路由协议视图。

- 接口视图**

配置接口参数的视图称为接口视图。在该视图下可以配置接口相关的物理属性、链路层特性及 IP 地址等重要参数。使用 `interface` 并指定接口类型及接口编号可以进入相应的接口视图。

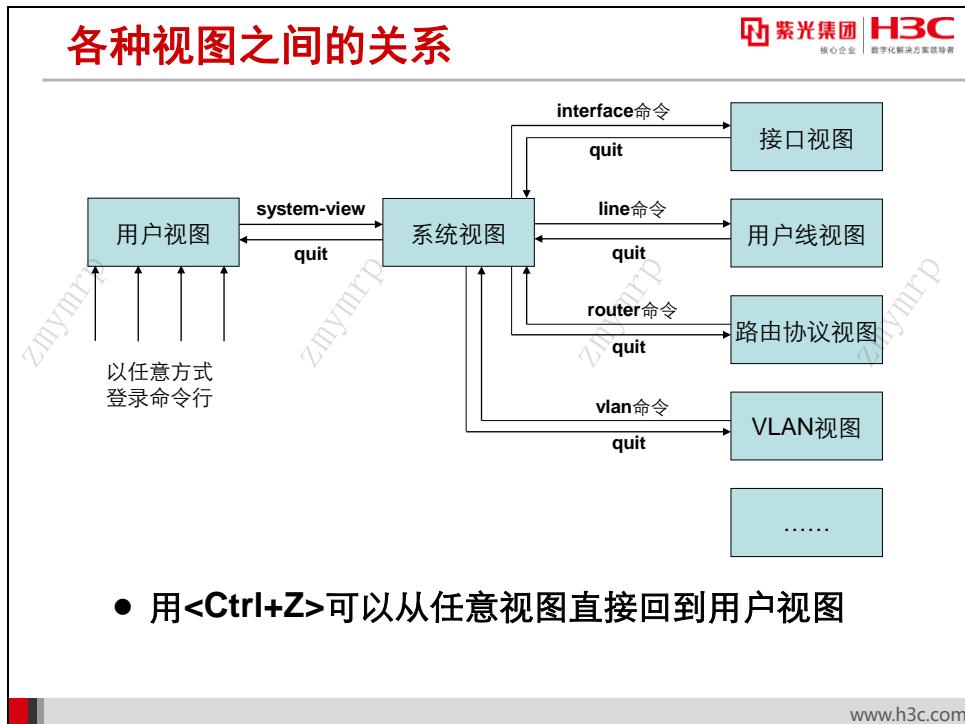
- 用户线视图

用户线视图（**line view**）是系统提供的一种视图，主要用来管理工作在流方式下的异步接口。通过在用户线视图下的各种操作，可以达到统一管理各种用户配置的目的。

与设备的配置方法相对应，用户线视图分为以下四种：

- **Console** 用户线视图：此视图用于配置 **Console** 用户线相关参数。通过 **Console** 口登录的用户使用 **Console** 用户线。
- **AUX** 用户线视图：此视图用于配置 **AUX** 用户线相关参数。通过 **AUX** 口登录的用户使用 **AUX** 用户线。
- **TTY**（**True Type Terminal**，实体类型终端）用户线视图：此视图用于配置 **TTY** 用户线相关参数。以终端通过异步串口连接网络设备的登录用户使用 **TTY** 用户线。这是一种不常用的登录方法，本书不做详细讲解。
- **VTY**（**Virtual Type Terminal**，虚拟类型终端）用户线视图：此视图用于配置 **VTY** 用户线相关参数。通过 **VTY** 方式登录的用户使用此用户线。**VTY** 是一种逻辑终端线，用于对设备进行 **Telnet** 或 **SSH** 访问。目前每台设备最多支持 64 个 **VTY** 用户同时访问。

每一个用户线的特定参数配置，都在相应的用户线视图下执行。例如要配置 **Console** 用户线的验证方式，首先需要在系统视图下执行命令 **line class console** 进入用户线视图，然后在此视图下用 **authentication-mode** 命令进行配置。而如果要配置 **Telnet** 用户线的验证方式，则可以通过 **line vty 0 63** 命令一次性配置 64 个用户的验证方式。



视图具备层次化结构，要进入某个视图，可能必须首先进入另一个视图。例如，要进入接口视图，必须首先进入系统视图。退出时则按照相反的次序。例如用 `quit` 命令退出接口视图后，随即回到系统视图。

要进入某个视图，需要使用相应的特定命令。而要从当前视图返回上一层视图，使用 `quit` 命令。如果要从任意的非用户视图立即返回到用户视图，可以执行 `return` 命令，也可以直接按组合键`<Ctrl+Z>`。

使用命令视图

紫光集团 | H3C
核心企业 | 数字化解决方案领导者

```
*****
* Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
*****
```

```
Line aux0 is available.
```

```
Press ENTER to get started.
<H3C>%Oct 13 09:16:14:706 2013 H3C SHELL/5/SHELL_LOGIN: TTY logged in from aux0.

<H3C>system-view
System View: return to User View with Ctrl+Z.
[H3C]interface GigabitEthernet 0/0
[H3C-GigabitEthernet0/0]description to_MyPC
[H3C-GigabitEthernet0/0]ip add 192.168.0.1 255.255.255.0
[H3C-GigabitEthernet0/0]quit
[H3C]user-interface vty 0 63
[H3C-line-vty0-63]authentication-mode scheme
```

www.h3c.com

上图显示了使用命令视图的一个实例。在该例中，按回车键后，即进入用户视图，输入 **system-view** 命令后，进入了系统视图。在系统视图下，输入 **interface GigabitEthernet 0/0** 命令即进入 **GigabitEthernet 0/0** 的接口视图。在该接口下，用 **description** 命令对接口用途进行描述，用 **ip address** 命令为该接口配置了 IP 地址，然后用 **quit** 命令退回到系统视图。最后用 **line vty 0 63** 进入了 VTY 用户视图下，为 VTY 登录指定了验证方法。

8.3.2 命令行类型

命令类型



- **读类型**
 - 用于显示系统配置信息和维护信息，如显示命令 display、显示文件信息的命令dir
- **写类型**
 - 用于对系统进行配置，如使能信息中心功能的命令info-center enable、配置调试信息开关的命令debugging
- **执行类型**
 - 用于执行特定的功能，如ping命令、与FTP服务器建立连接的命令ftp

www.h3c.com

Comware 系统的命令行是控制用户权限的最小单元。根据命令作用的不同，将命令分为以下三类：

- **读类型**：用于显示系统配置信息和维护信息，如显示命令 display、显示文件信息的命令 dir；
- **写类型**：用于对系统进行配置，如使能信息中心功能的命令 info-center enable、配置调试信息开关的命令 debugging；
- **执行类型**：用于执行特定的功能，如 ping 命令、与 FTP 服务器建立连接的命令 ftp。

用户角色

用户角色	用户权限
network-admin	可操作系统所有的功能和资源
network-operator	可执行系统所有的功能和资源相关的display命令 (display history-command all除外)
level-n ($n = 0\sim 15$)	level-0 ~ level-14可以由管理员为其配置权限 其中level-0、level-1和level-9有缺省用户权限 level-15的用户权限和network-admin相同，管理员无法对其进行配置

www.h3c.com

系统预定义了多种用户角色，部分角色拥有缺省的用户权限。如果系统预定义的用户角色无法满足权限管理的需求，管理员还可以自定义已有用户角色或是创建新的角色，来实现更精细化的权限控制。

8.3.3 命令行帮助特性

命令行帮助特性



```

<H3C>?
User view commands:
  archive          Archive configuration
  backup           Backup the startup configuration file to a TFTP server
  boot-loader      Software image file management
  bootrom          Update/read/backup/restore bootrom
  cd               Change current directory
  clock             Specify the system clock
  copy              Copy a file
  debugging         Enable system debugging functions
  delete            Delete a file
  diagnostic-logfile Diagnostic log file configuration
  dialer            Specify Dial-on-Demand Routing(DDR) configuration
  information
  dir               Display files and directories on the storage media
  display           Display current system information
  exception         Exception information configuration
  firmware          Firmware update
  fixdisk           Check and repair a storage medium
  format            Format a storage medium
  ---- More ----

```

```

[H3C]interface Vlan-interface ?
  <1-4094>  Vlan-interface interface number
[H3C]interface Vlan-interface 1 ?
  <cr>

```

www.h3c.com

命令行接口提供方便易用的在线帮助手段，便于用户使用：

- 键入<?>获取该视图下所有的命令及其简单描述；
- 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；如果该位置为参数，则列出有关的参数描述；

命令行帮助特性（续）



```
<H3C>di?  
  diagnostic-logfile  
  dialer  
  dir  
  display  
  
<H3C>dis?  
  display  
  
<H3C>dis  
<H3C>display v?  
  version  
  version-update-record  
  vlan  
  vlan-group  
  voice  
  vrrp  
  
<H3C>display ver?  
  version  
  version-update-record
```

此处按下`<Tab>`键可以补全命令

www.h3c.com

- 字符串后紧接`<?>`，列出以该字符串开头的所有命令；
- 命令后接一字符串紧接`<?>`，列出命令以该字符串开头的所有关键字；
- 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，反复按下`<Tab>`键，则可以循环显示出所有以输入字母开头的关键字。

8.3.4 错误提示信息

错误提示信息



```

[H3C]di
^
% Ambiguous command found at '^' position.

[H3C]dispaly
^
% Wrong parameter found at '^' position.

[H3C]display
^
% Incomplete command found at '^' position.

[H3C]display interface GigabitEthernet 0/0 0
^
% Too many parameters found at '^' position.

[H3C]display interface GigabitEthernet 0/0/0
^
% Wrong parameter found at '^' position.

[H3C]

```

www.h3c.com

用户键入的命令如果通过语法检查则正确执行，否则向用户报告错误信息。常见错误提示信息如下表：

英文错误信息	错误原因
Unrecognized command	命令无法解析
Incomplete command	参数输入不完整
Ambiguous command found at '^' position	以输入的字母开头的命令不唯一，无法识别
Too many parameters	输入参数过多
Wrong parameter	输入参数错误

8.3.5 命令行历史记录功能

命令行历史记录功能

● 查看历史命令记录

```
<H3C>display history-command
```

● 翻阅和调出历史记录中的某一条命令

- 用<↑>或<Ctrl+P>快捷键调出上一条历史命令
- 用<↓>或<Ctrl+N>快捷键调出下一条历史命令

www.h3c.com

命令行接口将用户最近使用过的命令自动保存在历史命令缓冲区中，用户可以通过 `display history-command` 显示这些命令，也可以随时查看或调用保存的历史命令，并编辑或执行。缺省情况下，每个用户的历史命令缓冲区的容量都是 10，即命令行接口为每个用户保存 10 条历史命令，可以在用户线视图下通过 `history-command max-size size-value` 命令来设置用户线历史命令缓冲区的容量。

用户可以调出历史命令重新执行或进行编辑。用上光标键<↑>或<Ctrl+P>，如果缓冲区中还有比当前命令更早的历史命令，则取出之；用下光标键<↓>或<Ctrl+N>，如果缓冲区中还有比当前命令更晚的历史命令，则取出之。

8.3.6 命令行编辑功能

命令行编辑功能	
按键	功能
普通字符键	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
<←>或<Ctrl+B>	光标向左移动一个字符位置
<→>或<Ctrl+F>	光标向右移动一个字符位置
<Ctrl+A>	将光标移动到当前行的开头
<Ctrl+E>	将光标移动到当前行的末尾
<Ctrl+D>	删除当前光标所在位置的字符
<Ctrl+W>	删除光标左侧连续字符串内的所有字符
<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+B>	将光标移动到左侧连续字符串的首字符处
<Esc+F>	将光标向右移到下一个连续字符串之前
<Ctrl+X>	删除光标左侧所有的字符
<Ctrl+Y>	删除光标右侧所有的字符

www.h3c.com

命令行接口提供了基本的命令编辑功能，主要的编辑按键如表所示。

8.3.7 分页显示

分页显示



```

<H3C>display interface
Aux0
Current state: UP
Description: Aux0 Interface
Bandwidth: 9kbps
Internet protocol processing: disabled
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Physical layer: asynchronous, Baudrate: 9600 bps
Phy-mru: 1700
Last 300 seconds input rate: 0.00 bytes/sec, 0 bits/sec, 0.00 packets/sec
Last 300 seconds output rate: 0.00 bytes/sec, 0 bits/sec, 0.00 packets/sec
Input:
  0 packets, 0 bytes
  0 broadcasts, 0 multicasts
  0 errors, 0 runts, 0 giants
  0 CRC, 0 align errors, 0 overruns
  0 aborts, 0 no buffers, 0 frame errors
---- More ----

```

本页未显示完
还有下一页

- <Space>: 继续显示下一屏信息
- <Enter>: 继续显示下一行信息
- <Ctrl+C> : 停止显示和命令执行

www.h3c.com

命令行接口提供了分页显示特性。在一次显示信息超过一屏时，会暂时停止继续显示，这时用户可以有三种选择：

- 按<Space>键：继续显示下一屏信息
- 按<Enter>键：继续显示下一行信息
- 按<Ctrl+C>键：停止显示和命令执行

8.4 常用命令

8.4.1 常用设备管理命令

常用设备管理命令

- 配置设备名称

```
[H3C] sysname ?
TEXT Host name (1 to 64 characters)
```

- 配置系统时间

```
<H3C> clock datetime ?
TIME Specify the time (hh:mm:ss)
```

- 显示系统时间

```
<H3C> display clock
```

- 配置欢迎/提示信息

```
[H3C] header ?
incoming      Specify the banner of the terminal line
legal         Specify the legal banner
login          Specify the login authentication banner
motd          Specify the banner of today
shell          Specify the session banner
```

www.h3c.com

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，如果设备的名称为 **RTA**，则用户视图的提示符为<RTA>。

为了保证与其他设备协调工作，用户可以用 **display clock** 查看当前系统时间，用 **clock datetime** 命令设置系统时间。

欢迎信息是用户在连接到设备、进行登录验证以及开始交互配置时系统显示的一段提示信息。管理员可以根据需要，设置相应的提示信息。

系统支持的欢迎信息包括：

- **shell** 欢迎信息，也称 **session** 条幅。进入控制台会话时显示；
- 用户接口欢迎信息，也称 **incoming** 条幅。主要用于 **TTY Modem** 激活用户接口时显示；
- 登录欢迎信息，也称 **login** 条幅。主要用于配置密码验证和 **scheme** 验证时显示；
- **MOTD** 欢迎信息。在启动验证前显示，该特性的支持情况与设备的型号有关，请以设备的实际情况为准；
- 授权欢迎信息，也称 **legal** 条幅。系统在用户登录前会给出一些版权或者授权信息，然后显示 **legal** 条幅，并等待用户确认是否继续进行验证或者登录。如果用户输入 **Y**

或者直接按<Enter>键，则进入验证或登录过程；如果输入 N，则退出验证或登录过程。Y 和 N 不区分大小写。

8.4.2 常用信息查看命令

常用信息查看命令

紫光集团 | **H3C**
 核心企业 | 数字化解决方案领导者

- 查看版本信息
<H3C> display version
- 查看当前配置
<H3C> display current-configuration
- 显示接口信息
<H3C> display interface
- 显示接口IP状态与配置信息
<H3C> display ip interface brief
- 显示系统运行统计信息
<H3C> display diagnostic-information

通过 **display version** 命令可以查看网络设备使用的操作系统版本号等信息。通过 **display current-configuration** 命令可以查看设备当前运行的配置。

为了查看设备的接口信息，可以使用 **display interface** 命令。该命令将显示设备所有接口的类型、编号、物理层状态、数据链路层协议、IP 地址、接口报文收发统计等全面信息。如果只想查看接口 IP 状态等简要信息，也可以使用 **display ip interface brief** 命令。

因为各个功能模块都有其对应的信息显示命令，所以一般情况下，要查看各个功能模块的运行信息，用户需要逐条运行相应的 **display** 命令。为便于一次性收集更多信息，方便日常维护或问题定位，用户可以在任意视图下执行 **display diagnostic-information** 命令，显示系统当前各个主要功能模块运行的统计信息。

8.5 配置远程登录

在对服务器端路由器进行远程登录前，必须要对设备进行配置。第一次对设备做配置时，必须通过 Console 口进行本地配置。本节讲解 Telnet 和 SSH 远程登录路由器的基本配置。交换机的相关配置非常近似。

8.5.1 通过 Telnet 登录路由器的配置

路由器Telnet服务配置命令



 紫光集团 | H3C
 核心企业 | 数字化解决方案提供者

- 配置与网络相连端口的IP地址

```
[H3C-GigabitEthernet0/0] ip address ip-address
{ mask | mask-length }
```

- 使能Telnet服务器端功能

```
[H3C] telnet server enable
```

- 进入vty用户界面视图，设置验证方式

```
[H3C] line vty first-num2 [ last-num2 ]
[H3C-line-vty0-63] authentication-mode { none |
password | scheme }
```

www.h3c.com

上图以及随后的几张图演示了采用密码验证方案时，在网络设备上配置 Telnet 服务器的命令：

- 配置至少一个 IP 地址，以便提供 IP 连通性；
- 启动 Telnet 服务器；
- 进入 VTY 用户界面视图。VTY 的编号为 0~63，第一个登录的远程用户为 VTY 0，第二个为 VTY 1，依次类推。此处可以选择要配置的 VTY 编号。

为 VTY 用户界面视图配置验证方式。这里有三种方式可以选择。关键字 **none** 表示不验证；**password** 表示使用单纯的密码验证方法，登录时只需要输入密码；**scheme** 表示使用用户名/密码验证方法，登录时须输入用户名及其密码。

路由器Telnet服务配置命令（续）

● 设置登录密码和用户级别

```
[H3C-line-vty0-63] set authentication password { hash  
| simple } password  
[H3C-line-vty0-63] user-role role-name
```

● 创建用户、配置密码、设置服务类型、 设置用户级别

```
[H3C] local-user username  
[H3C-luser-manage-xxx] password { hash | simple }  
password  
[H3C-luser-manage-xxx] service-type telnet  
[H3C-luser-manage-xxx] authorization-attribute user-  
role role-name
```

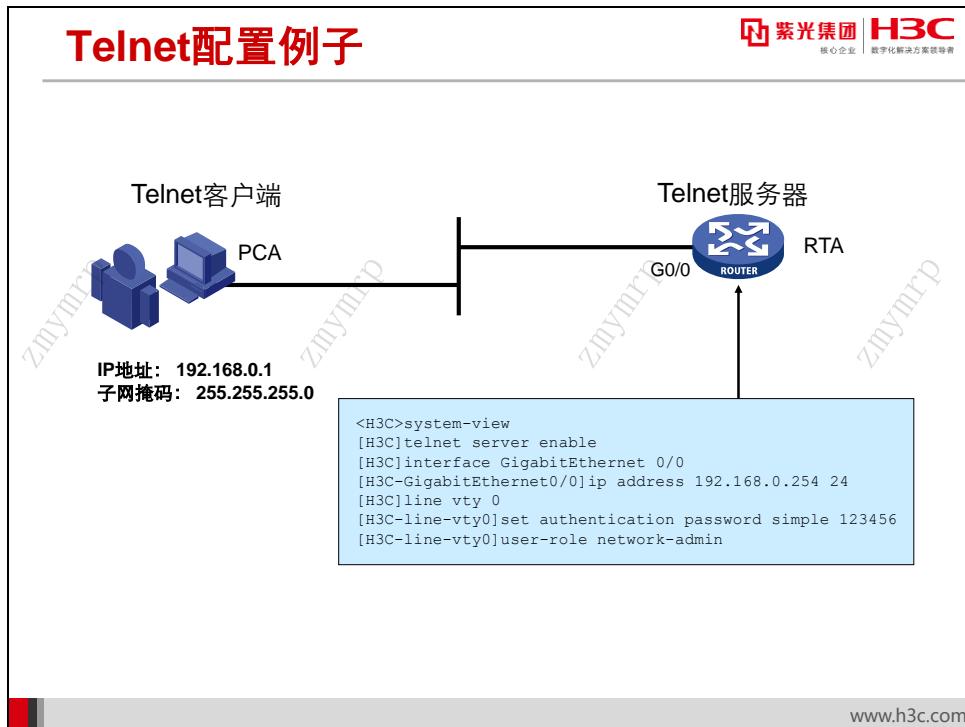
www.h3c.com

- 如果选择了 **password** 验证方法，则须配置一个验证密码，并可以在用户界面视图下配置通过本用户界面登录后的用户级别。

如果选择了 **scheme** 验证方法，则系统默认采用本地用户数据库中的用户信息进行验证，因此须配置本地用户名、密码、用户角色等信息，用户服务类型选择为 **telnet**，供远程登录验证使用。

注意：

当本地用户的用户角色与其登录时所用用户线中的用户角色不同时，系统优先采用前者作为登录后的实际用户角色。



一个客户端通过 Telnet 连接路由器的配置例子如图所示。本例假设客户端主机 PCA 与路由器 RTA 直接通过以太网相连，用户角色要求设置为 **network-admin**。按图示命令配置好路由器 RTA，并对 PCA 配置 IP 地址和子网掩码，启动 Telnet 客户端，即可登录 RTA 的命令行了。

注意：

Telnet 连接依赖于 IP 可达性。如果客户端与服务器端不处于同一网段，还需要正确地配置 IP 路由。IP 路由的配置非本章内容，请参考本书相关章节。

用Telnet登录

紫光集团 | **H3C**
核心企业 | 数字化解决方案提供者



```
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation. 保留所有权利。
C:\Users\Chen>telnet 192.168.0.254

*****
* Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent,
* no decompiling or reverse-engineering shall be allowed. *
*****
Password: <H3C>
```

输入密码

www.h3c.com

在 PCA 的 Telnet 终端软件上键入路由器的 IP 地址，与路由器建立连接，在提示输入密码时，正确输入事先配置好的密码 123456，即可通过验证，并出现命令行提示符<H3C>，随后就可以对路由器进行操作了。

如果登录过程中提示“**All user interfaces are used, please try later!**”，说明系统允许登录的 Telnet 用户数已经达到上限，请待其他用户释放以后再连接。

注意：

更改当前用户的角色后，需要退出并重新登录，修改后的用户角色才会生效。

8.5.2 通过 SSH 登录路由器的配置

路由器SSH服务配置命令

● 使能SSH服务器功能

[H3C] ssh server enable

● 配置SSH客户端登录时的用户界面

[H3C-line-vty0-63] authentication-mode scheme
[H3C-line-vty0-63] protocol inbound ssh

● 配置SSH用户

[H3C] local-user *username*
[H3C-luser-manage-xxx] password { hash | simple }
password
[H3C-luser-manage-xxx] service-type ssh
[H3C-luser-manage-xxx] authorization-attribute user-role *role-name*

www.h3c.com

上图给出了采用密码验证方案时，在网络设备上配置 SSH 服务器的命令：

- 启动 SSH 服务器；
- 配置用户界面，使其支持 SSH 远程登录协议，配置结果将在下次登录请求时生效；
- 为服务器配置 SSH 本地用户，供远程登录验证使用。

当然，在网络设备上仍然必须配置至少一个 IP 地址，以便提供 IP 连通性。

路由器SSH服务配置命令（续）



核心企业 | 数字化解决方案领导者

● 生成RSA密钥

```
[H3C] public-key local create rsa
```

● 导出RSA密钥

```
[H3C] public-key local export public rsa ssh2
```

● 销毁RSA密钥

```
[H3C] public-key local destroy rsa
```

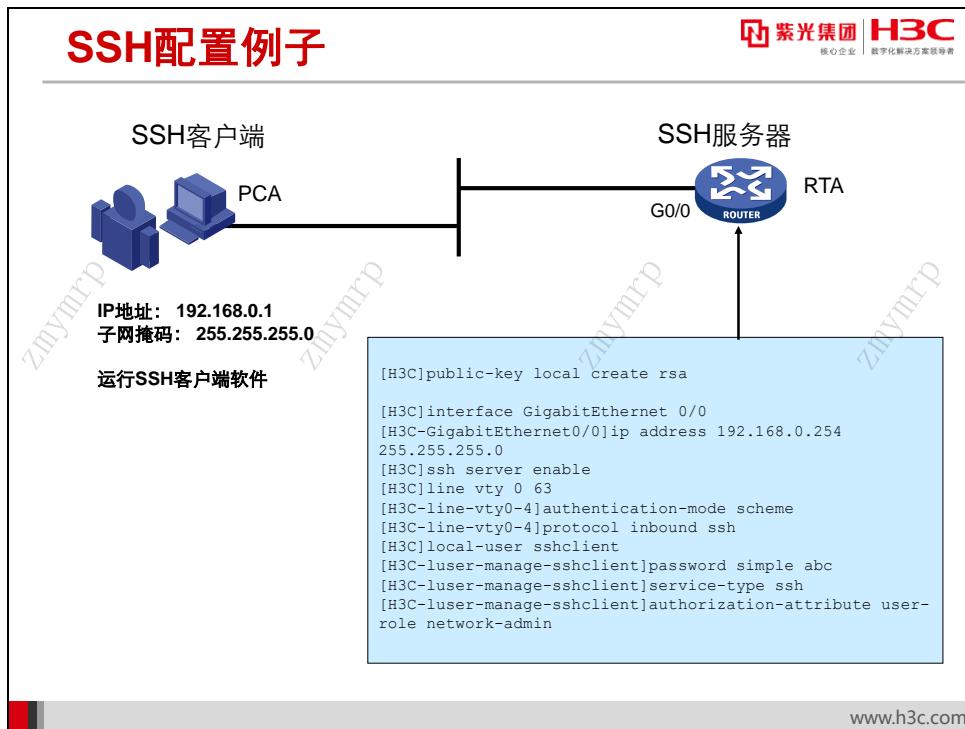
www.h3c.com

为了完成 SSH 验证和会话，需要利用主机密钥对等参数，生成会话密钥和会话 ID。上图显示了生成主机密钥对的命令。服务器密钥和主机密钥的最小长度为 512 位，最大长度为 2048 位。在 SSH2 中，有的客户端要求服务器端生成的密钥长度必须大于或等于 768 位。生成密钥对时，如果已经有了 RSA 密钥对，系统则提示是否替换原有密钥。

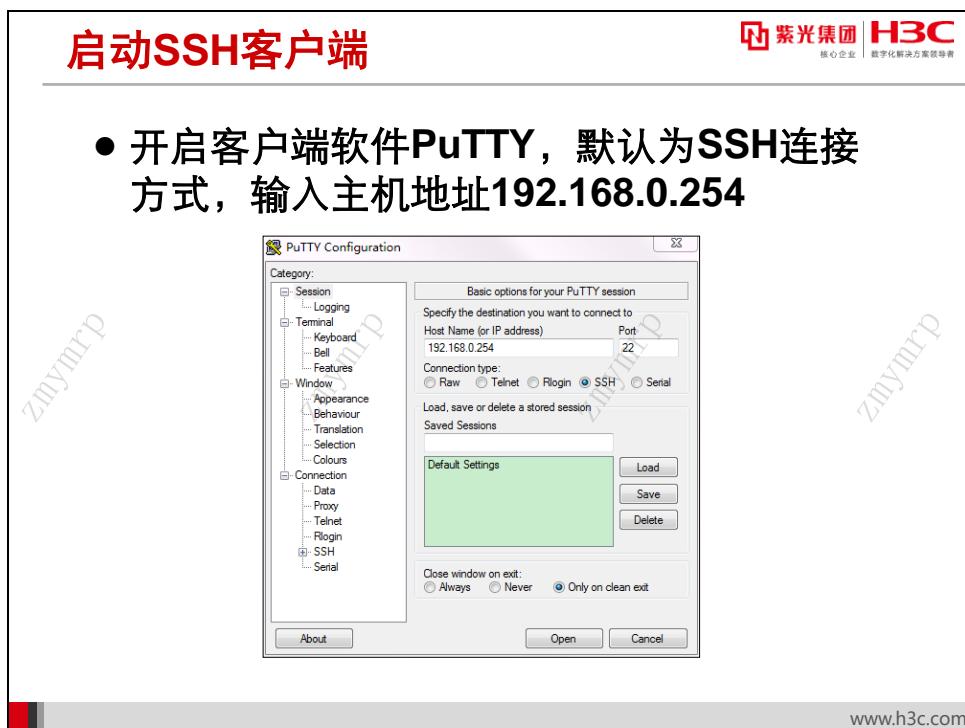
对于已经生成的 RSA 密钥对，可以根据指定格式在屏幕上显示 RSA 主机公钥或导出 RSA 主机公钥到指定文件，从而为在远端配置 RSA 主机公钥作准备。也可以手工销毁当前的密钥对。

注意：

SSH 连接依赖于 IP 可达性。如果客户端与服务器端不处于同一网段，还需要正确地配置 IP 路由。IP 路由的配置非本章内容，请参考本书相关章节。



配置 SSH 服务器，首先在上面生成本地非对称密钥对，然后开启 SSH 服务。
在用户线视图下开启用户认证，并设置该用户线支持的协议为 SSH。
最后创建本地用户，配置服务类型为 SSH，并授权用户角色为网络管理员。



SSH客户端软件有很多，本节以客户端软件PuTTY为例，说明SSH客户端的配置方法。

SSH客户端要与服务器建立连接，需要做如下基本配置：

- 指定服务器IP地址；
- 选择远程连接协议为SSH。通常客户端可以支持多种远程连接协议，如Telnet、Rlogin、SSH等。要建立SSH连接，必须选择远程连接协议为SSH；
- 选择SSH版本。由于设备目前支持的版本是SSH服务器2.0版本，客户端可以选择2.0或2.0以下版本。

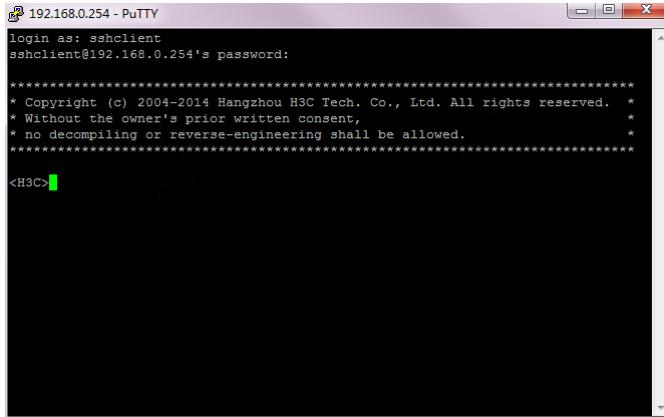
终端参数配置好后，点击【Open】，可发起与服务器端（网络设备）的连接，并弹出下图所示的对话框。



输入预先设置的用户名和密码，即可进入命令行界面。

登录网络设备（续）

紫光集团 **H3C**
核心企业 | 数字化解决方案领导者



```
192.168.0.254 - PuTTY
login as: sshclient
sshclient@192.168.0.254's password:

*****
* Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent,                                *
* no decompiling or reverse-engineering shall be allowed.                  *
*****
```

<H3C>

www.h3c.com

输入密码后回车，即可正常登陆设备。上图为设备登陆后的显示页面。

8.6 本章总结

本章总结

- 支持Console口本地配置、AUX口本地或远程配置、Telnet或SSH本地或远程配置
- 命令行提供多种命令视图
- 系统命令行采用分级保护方式，命令类型可分为读类型、写类型、执行类型3种类型

第9章 网络设备文件管理

设备以文件系统的方式对保存在设备存储介质中的文件（如操作系统文件、配置文件等）进行管理。本章将介绍 H3C 网络设备文件系统的操作命令。

配置文件是用来保存用户对设备所进行的配置，记录用户的配置信息的文本格式文件。本章介绍了如何对配置文件进行管理维护。

同时本章将介绍 BootROM 和操作系统软件的升级方法及使用 FTP 和 TFTP 加载系统文件的操作。

9.1 本章目标

课程目标

学习完本课程，您应该能够：

- 了解H3C网络设备文件系统的作用与操作方法
- 掌握配置文件保存、擦除、备份与恢复的操作方法
- 掌握网络设备软件的升级等操作方法
- 掌握用FTP和TFTP传输系统文件的方法



9.2 网络设备文件系统介绍

9.2.1 什么是网络设备文件系统

网络设备的文件系统



紫光集团 | H3C
核心企业 | 数字化解决方案领导者

- 设备以文件的方式对运行所需的数据进行存储
- 网络设备通过文件系统管理这些文件
- 主要文件
 - 启动软件包
 - 配置文件
 - 日志文件

Z
n
y
m
r
p

www.h3c.com

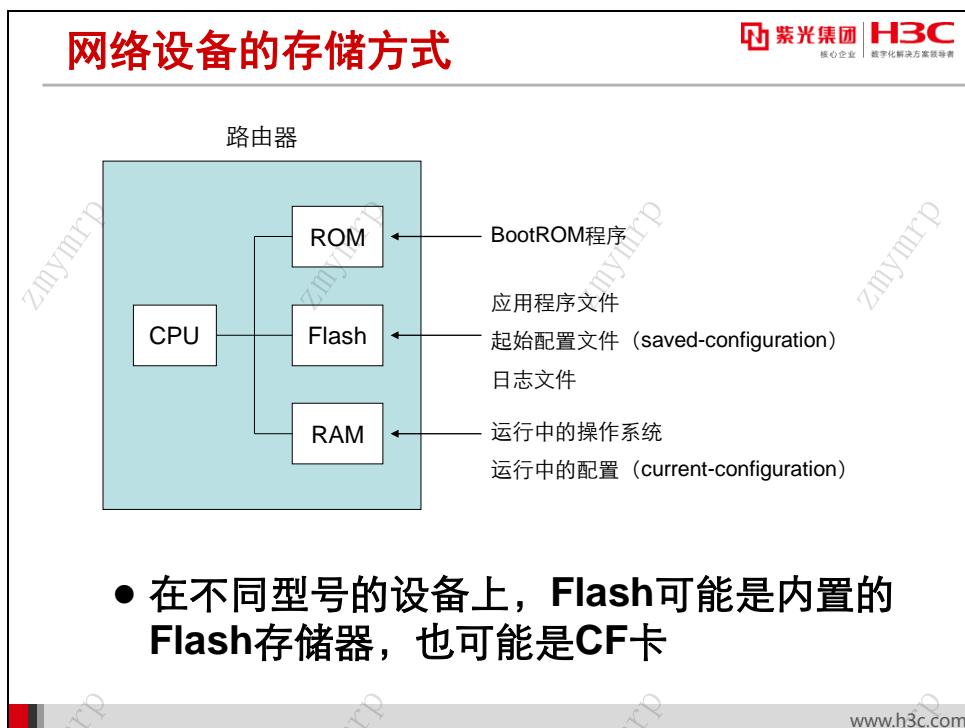
网络设备启动时需要一些基本的程序和数据，运行中也会产生一些重要数据，这些数据都以文件的方式保存在存储器中，以便调用和管理。

网络设备通过文件系统对这些文件进行管理和控制，并为用户提供了操作和管理文件系统的工具。

在文件系统中保存的文件类型主要包括：

- 启动软件包：Comware 操作系统用于引导设备启动的程序文件，设备必须具有 Boot 包和 System 包才能正常运行。启动软件包有 BIN 文件和 IPE 文件两种发布形式；
- 配置文件：系统将用户对设备的所有配置以命令的方式保存成文本文件，称为配置文件，这种文件的扩展名为.cfg；
- 日志文件：系统在运行中产生的文本日志可以存储在文本格式的日志文件中，称为日志文件。

9.2.2 网络设备的存储方式



网络设备上具有三种存储介质：

- ROM (read-only memory, 只读存储器)：用于存储 BootROM 程序。BootROM 程序是一个微缩的引导程序，主要任务是查找应用程序文件并引导到操作系统，在应用程序文件或配置文件出现故障时提供一种恢复手段；
- Flash 存储器（快闪存储器）：用于存储应用程序文件、保存的配置文件和运行中产生的日志文件等。默认情况下，网络设备从 Flash 存储器读取应用程序文件和配置文件进行引导。Flash 存储器的形式是多样的，根据设备型号的不同，可能是 CF (Compact Flash) 卡、内置 Flash 存储器等；
- RAM (random-access memory, 随机访问存储器)：只用于系统运行中的随机存储，例如存储当前运行的 Comware 系统程序和运行中的当前配置等。系统关闭或重启后其信息会丢失。

9.2.3 文件系统的操作

文件系统的操作



- **目录操作**
 - 创建/删除目录、显示当前工作目录以及显示指定目录下的文件或目录的信息等
- **文件操作**
 - 删除文件、恢复删除的文件、彻底删除文件、显示文件的内容、重命名文件、拷贝文件、移动文件、显示指定文件的信息等
- **存储设备操作**
 - 恢复存储设备的空间、格式化存储设备等
- **设置文件系统的提示方式**

www.h3c.com

文件系统的功能主要包括目录的创建和删除、文件的拷贝和显示等。

默认情况下，对于有可能导致数据丢失的命令（比如删除文件、覆盖文件等命令），文件系统将提示用户进行确认。

根据操作对象的不同，可以把文件系统操作分为以下几类：

● 目录操作：

目录操作包括创建/删除目录、显示当前工作目录以及显示指定目录下的文件或目录的信息等。可以使用下面的命令来进行相应的目录操作。请在用户视图下进行下列操作。

操作	命令	说明
创建目录	mkdir directory	可选
删除目录	rmdir directory	可选
显示当前的工作路径	pwd	可选
显示目录或文件信息	dir [/all] [file-url]	可选
改变当前目录	cd directory	可选

● 文件操作：

文件操作包括删除文件、恢复删除的文件、彻底删除文件、显示文件的内容、重命名文件、拷贝文件、移动文件、显示指定的文件的信息等。可以使用下面的命令来进行相应的文件操作。

操作	命令	说明
删除文件	delete [/unreserved] file-url	可选
恢复删除文件	undelete file-url	可选

操作	命令	说明
彻底删除回收站中的文件	reset recycle-bin [<i>file-uri</i>] [/force]	可选
显示文件的内容	more <i>file-uri</i>	可选 目前只支持显示文本文件
重命名文件	rename <i>fileurl-source</i> <i>fileurl-dest</i>	可选
拷贝文件	copy <i>fileurl-source</i> <i>fileurl-dest</i>	可选
移动文件	move <i>fileurl-source</i> <i>fileurl-dest</i>	可选
显示目录或文件信息	dir [/all] [<i>file-uri</i>]	可选

● 存储设备操作:

由于异常操作等原因，存储设备的某些空间可能不可用。用户可以通过 **fixdisk** 命令来恢复存储设备的空间，也可以通过 **format** 命令来格式化指定的存储设备。

操作	命令	说明
恢复存储设备的空间	fixdisk <i>device</i>	可选
格式化存储设备	format <i>device</i>	可选

注意:

格式化操作将导致存储设备上的所有文件丢失，并且不可恢复；尤其需要注意的是，格式化 Flash，将丢失全部应用程序文件和配置文件。

对于可以支持热插拔的存储设备（如 CF 卡、USB 存储器等），可以在用户视图下用 **mount** 和 **umount** 命令挂载和卸载该存储设备。卸载存储设备是逻辑上让存储设备处于非连接状态，此时用户可以安全地拔出存储设备；挂载存储设备是让卸载的存储设备重新处于连接状态。

操作	命令	说明
挂载存储设备	mount <i>device-name</i>	可选 缺省情况下，存储设备插入时已经处于连接状态，不需要再挂载
卸载存储设备	umount <i>device-name</i>	可选

注意:

在拔出处于挂载状态的存储设备前，请先执行卸载操作，以免损坏存储设备。

在执行挂载或卸载操作过程中，禁止对单板或存储设备进行插拔或倒换操作；在进行文件操作过程中也禁止对存储设备进行插拔或倒换操作。否则，可能会引起文件系统的损坏。

● 设置文件系统操作的提示方式:

用户可以通过命令修改当前文件系统的提示方式。文件系统支持 **alert** 和 **quiet** 两种提示方式。在 **alert** 方式下，当用户对文件进行有危险性的操作时，系统会跟用户进行交互确认。在 **quiet** 方式下，用户对文件进行任何操作，系统均不作提示。该方式可能会导致一些因粗心而发生的、不可恢复的、对系统造成破坏的操作发生。

操作	命令	说明
设置文件系统的提示方式	file prompt { alert quiet }	可选 缺省情况下，文件系统的提示方式为 alert

9.3 文件的管理

9.3.1 配置文件介绍

配置文件介绍



紫光集团 | H3C
核心企业 | 数字化解决方案领导者

- **起始配置与当前配置**
- **配置文件是以文本格式保存的命令，默
认配置并不出现在配置文件中**
- **配置文件的选择顺序**
 - 如果用户指定了启动配置文件，且配置文件存在，
则以启动配置文件进行初始化
 - 如果用户指定的启动配置文件不存在，则以空配
置进行初始化

www.h3c.com

配置文件是指以文本格式保存设备配置命令的文件。配置文件记录用户的配置信息，通过配置文件，用户可以非常方便地了解这些配置信息。

设备启动时，会根据读取的配置文件进行初始化工作，该配置称为起始配置（**saved-configuration**）。如果设备中没有配置文件，则系统在启动过程中使用缺省参数进行初始化。与起始配置相对应，系统运行时采用的配置称为当前配置（**current-configuration**）。当前配置实际上是启动时的起始配置和启动后用户对设备执行的增量配置的叠加。用户对设备执行当前配置存放在设备的临时存储器中，设备重启之后会丢失。

配置文件为一个文本文件，其中以文本格式保存了非默认的配置命令。配置文件中命令的组织以命令视图为基本框架，同一命令视图的命令组织在一起，形成一节，节与节之间通常用空行或注释行隔开（以#开始的为注释行，空行或注释行可以是一行或多行）。整个文件以 **return** 结束。

网络设备可以保存多个配置文件。系统启动时优先选择用户指定的启动配置文件，如果没有指定任何启动配置文件，则以空配置启动。

注意：

大部分 H3C 网络设备支持配置文件的 main/backup 属性，使得设备上可以同时存在主用、备用两种属性的配置文件。当主用配置文件损坏或丢失时，可以用备用配置文件来启动或配置设备。该特性的细节超出本书范围，读者可参考相关手册。

9.3.2 配置文件的管理

配置文件的操作



核心企业 | 数字化解决方案提供者

- 保存配置
`<H3C> save`
- 擦除配置
`<H3C> reset saved-configuration`
- 设置下次启动的配置文件
`<H3C> startup saved-configuration filename`
- 备份/恢复下次启动配置文件
`<H3C> backup startup-configuration to tftp-server [dest-filename]`
`<H3C> restore startup-configuration from tftp-server src-filename`

www.h3c.com

用户通过命令行可以修改设备的当前配置，而且这些配置是暂存于 RAM 中的，设备一旦重启或断电就立即丢失。如果要使当前配置在系统下次重启时继续生效，在重启设备前，请使用 **save** 命令将当前配置保存到配置文件中。

用户通过命令可以擦除设备中的配置文件。配置文件被擦除后，设备下次上电时，系统将采用缺省的配置参数进行初始化。

Backup/Restore 特性主要实现通过命令行对设备下次启动配置文件进行备份和恢复的功能。设备与服务器之间使用 **TFTP** 协议进行数据的传输，其中 **Backup** 特性用于将设备下次启动配置文件备份至 **TFTP** 服务器上；而 **Restore** 特性用于将 **TFTP** 服务器上保存的配置文件下载到设备并设置为下次启动配置文件。在后续的小节中我们将进一步学习如何使用 **TFTP** 服务。

配置文件的显示与维护



- 查看保存的配置文件

```
<H3C> display saved-configuration
```

- 查看系统启动配置文件

```
<H3C> display startup
```

- 查看当前生效的配置

```
<H3C> display current-configuration
```

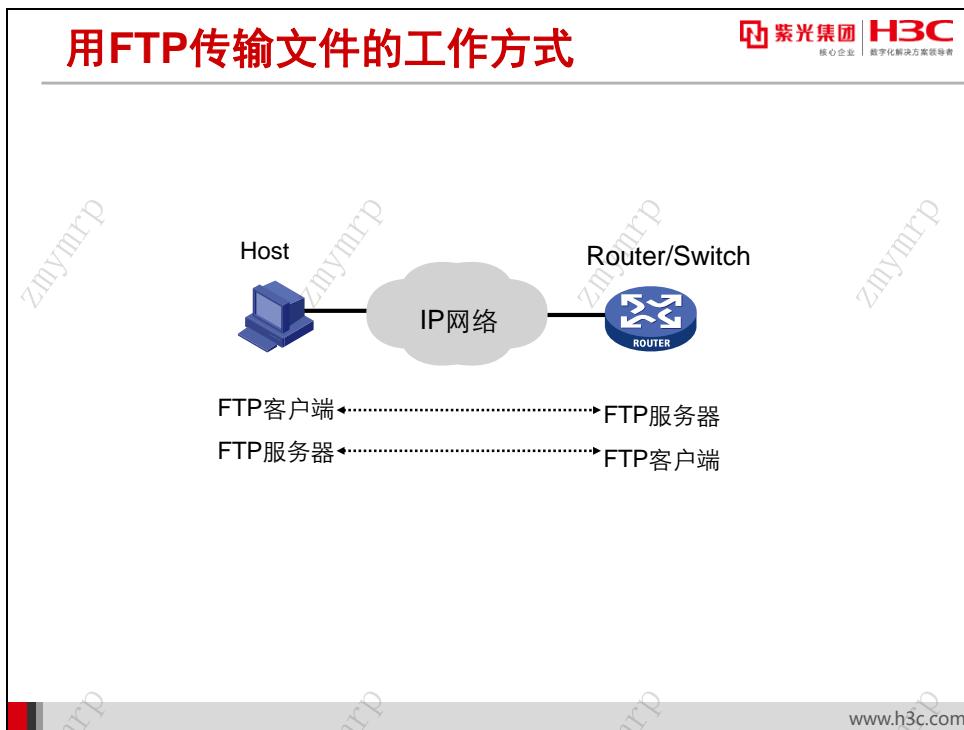
- 查看当前视图下生效的配置

```
[H3C-line-vty0-63] display this
```

www.h3c.com

在任意视图下执行 **display saved-configuration** 命令显示保存的配置文件的内容，**display current-configuration** 命令显示当前生效的配置信息，**display startup** 显示了系统当前和下次启动时使用的配置文件。另外，在任意视图下执行 **display this** 命令，可以显示当前生效的与该视图相关的配置信息。

9.3.3 使用 FTP 传输文件



可以用 **FTP** (File Transfer Protocol, 文件传输协议) 来进行网络设备文件的传输。

网络设备的 **FTP** 实现支持两种方式：

- 设备作为 **FTP** 客户端：用户在设备的命令行终端上执行 **ftp** 命令，建立设备与远程 **FTP** 服务器的连接，下载远程 **FTP** 服务器上的文件，或上传本地文件；
- 设备作为 **FTP** 服务器：用户在其他主机上运行 **FTP** 客户端程序，登录到设备上进行文件上传和下载操作。在用户登录前，网络管理员需要事先在网络设备上配置好 **FTP** 服务器的相关参数。

配置设备的FTP服务



核心企业 | 数字化解决方案领导者

● 使能FTP服务器功能

```
[H3C] ftp server enable
```

● 创建用户

```
[H3C] local-user username
```

● 设置服务类型及登录密码

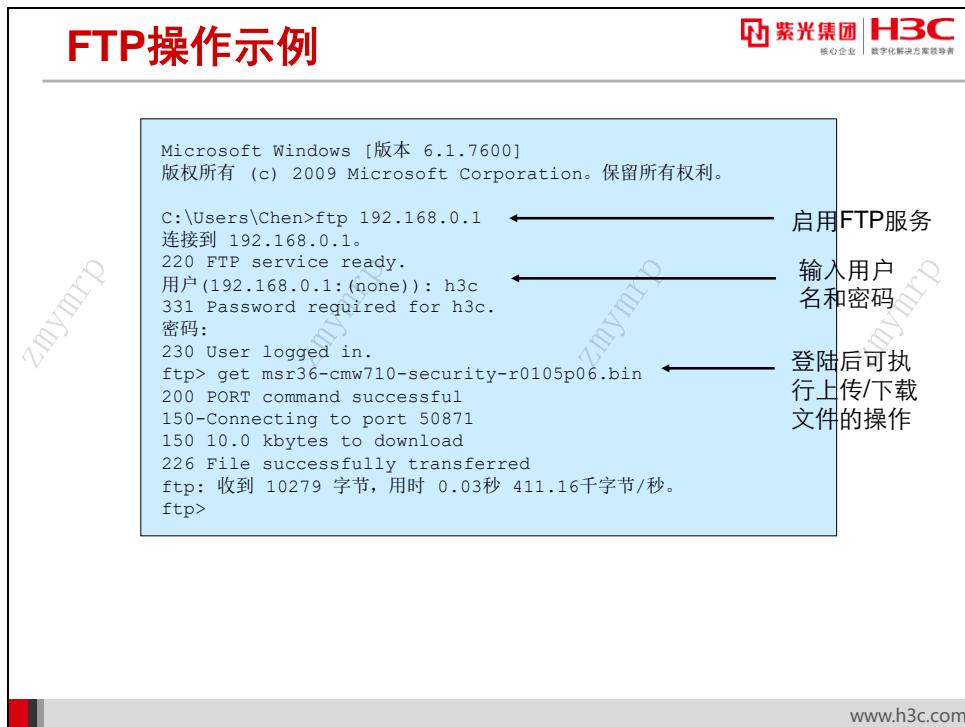
```
[H3C-luser-manage-xxx] service-type ftp
[H3C-luser-manage-xxx] password { hash | simple } password
```

www.h3c.com

设备作为FTP服务器时，需要进行如下配置：

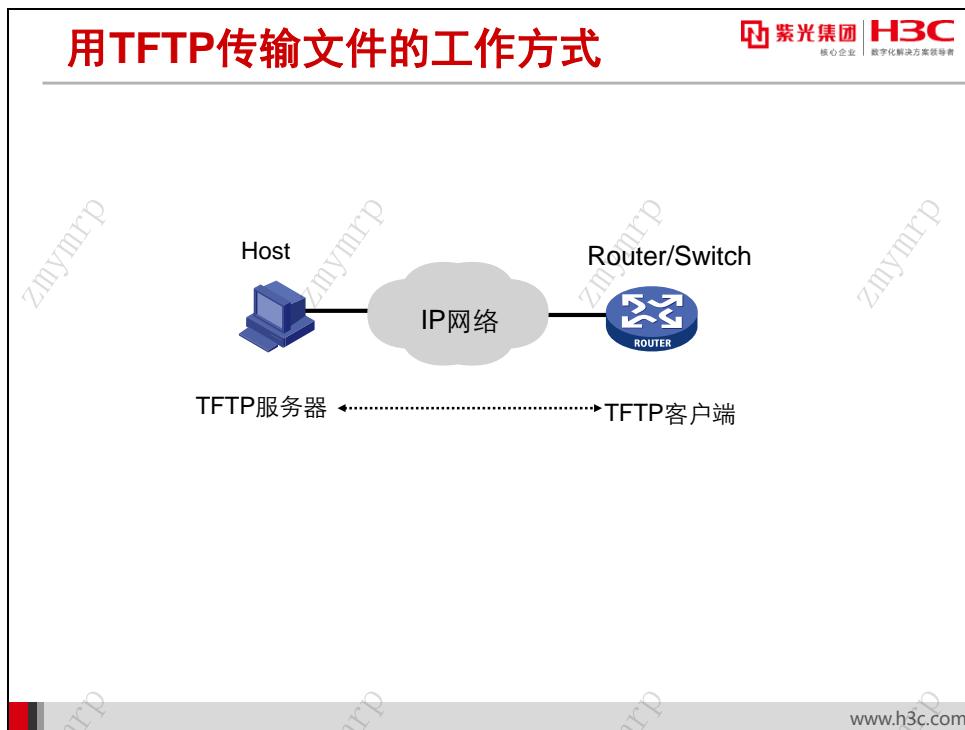
设备	操作	说明
网络设备 (FTP服务器)	启动FTP服务器功能	缺省情况下，系统关闭FTP服务器功能 可以通过display ftp-server命令查看 设备上FTP服务器功能的配置信息
	配置FTP服务器的验证和授权	配置FTP用户的用户名、密码、授权的工作目录
	配置FTP服务器的运行参数	配置FTP连接的超时时间
主机(FTP客户端)	使用FTP客户端程序登录设备	-

在网络设备上配置好相应FTP服务后，就可以在FTP客户端主机上登录网络设备。验证通过后，就可执行文件上传和下载操作了。



上图显示了在 PC 机上执行 FTP 命令从作为 FTP 服务器的路由器下载启动软件包的实例。在本例中，PC 机从路由器下载了启动软件包 `msr36-cmw710-security-r0105p06.bin`。这是一种常用的设备配置和维护手段。

9.3.4 使用 TFTP 传输文件



TFTP (Trivial File Transfer Protocol, 简单文件传输协议) 也是用于在远端服务器和本地主机之间传输文件的，相对于 FTP，TFTP 没有复杂的交互存取接口和认证控制，适用于客户端和服务端之间不需要复杂交互的环境。TFTP 协议的运行基于 UDP 协议，因此只适用于相对可靠的网络介质上。

TFTP 协议传输是由客户端发起的。当需要下载文件时，由客户端向 TFTP 服务器发送读请求包，然后从服务器接收数据，并向服务器发送确认；当需要上传文件时，由客户端向 TFTP 服务器发送写请求包，然后向服务器发送数据，并接收服务器的确认。TFTP 传输文件有两种模式：一种是二进制模式，用于传输程序文件；另一种是 ASCII 码模式，用于传输文本文件。

网络设备可以作为 TFTP 客户端，从 TFTP 服务器上传或下载文件。

在设备上使用TFTP服务



```
<H3C> tftp tftp-server { get | put | sget } source-
filename [ destination-filename ] [ source { interface
interface-type interface-number | ip source-ip-
address } ]
```

- 在执行上传/下载操作时，到TFTP服务器的可达路由可能有多条，用户可以配置客户端TFTP报文的源地址
- 当设备作为TFTP客户端时，可以把本设备的文件上传到TFTP服务器，还可以从TFTP服务器下载文件到本地设备
- 下载分为普通下载和安全下载两种

www.h3c.com

设备作为TFTP客户端时，需要进行如下配置：

设备	操作	说明
网络设备 (TFTP客户端)	<ul style="list-style-type: none"> 配置设备接口的IP地址，使其和TFTP服务器的IP地址在同一网段 可以直接使用TFTP命令登录远端的TFTP服务器上传或下载文件 	TFTP适用于客户端和服务器之间不需要复杂交互的环境。请保证设备和TFTP服务器之间路由可达
主机(TFTP服务器)	启动TFTP服务器，并作了TFTP工作目录的配置	-

在执行上传/下载操作时，到TFTP服务器的可达路由可能有多条，用户可以配置客户端TFTP报文的源地址。

当设备作为TFTP客户端时，可以使用 **put** 关键字把本设备的文件上传到TFTP服务器，还可以使用 **get** 关键字从TFTP服务器下载文件到本地设备。

tftp sget 命令用来在安全模式下，将文件从TFTP服务器的指定文件下载并保存到本地设备。在这种模式下，设备将获取的远端文件先保存到内存中，等用户文件全部接收完毕，才将它写到Flash中。这样如果系统文件下载失败，原有的系统文件不会被覆盖，设备仍能启动。这种方法安全系数较高，但需要较大的内存空间。

TFTP 操作示例

紫光集团 **H3C**
核心企业 | 数字化解决方案领导者

```
<H3C>tftp 192.168.0.10 get config.cfg
config.txt already exists. Overwrite it? [Y/N]:Y
Press CTRL+C to abort.
% Total    % Received % Xferd  Average Speed   Time   Time   Current
          Dload  Upload   Total   Spent   Left  Speed
100  3124  100  3124     0      0  65729      0  --:--:--  --:--:-- 254k
```

www.h3c.com

上图显示了在网络设备上执行 TFTP 命令从 TFTP 服务器上下载配置文件的实例。在本例中，网络设备从 TFTP 服务器上下载了配置文件 config.cfg。这也是一种常用的设备配置和维护手段。

9.3.5 指定启动文件

指定下次启动加载的应用程序文件

● 指定下次启动加载的应用程序文件

```
<H3C> boot-loader file file-url
```

● 显示下次启动加载的应用程序文件

```
<H3C> display boot-loader
```

www.h3c.com

启动文件是设备启动时选用的应用程序文件。当存储介质中有多个应用程序文件时，用户可以通过 **boot-loader** 命令，指定设备下次启动时所采用的启动文件。这实际上为系统进行操作系统软件升级提供了一个便利的途径，也就是说，若需要进行操作系统升级时，只需要将新的应用程序文件上载到设备中，并将其指定为启动文件，重新启动设备，即可由系统自行完成操作系统的升级。因为旧的应用程序文件仍然存在，所以能很容易地恢复到此前的系统版本。

通过 **display boot-loader** 命令可以查看系统当前和下次启动使用的启动文件。

9.3.6 重启设备

重启设备

紫光集团 H3C
核心企业 数字化解决方案领导者

- 重启系统

<H3C> reboot

- 开启设备定时重启功能，并指定重启的具体时间

<H3C> schedule reboot at *hh:mm* [*date*]

- 开启设备定时重启功能，并指定重启的等待时延

<H3C> schedule reboot delay { *hh:mm* | *mm* }

- 显示设备的重启时间

<H3C> display schedule reboot

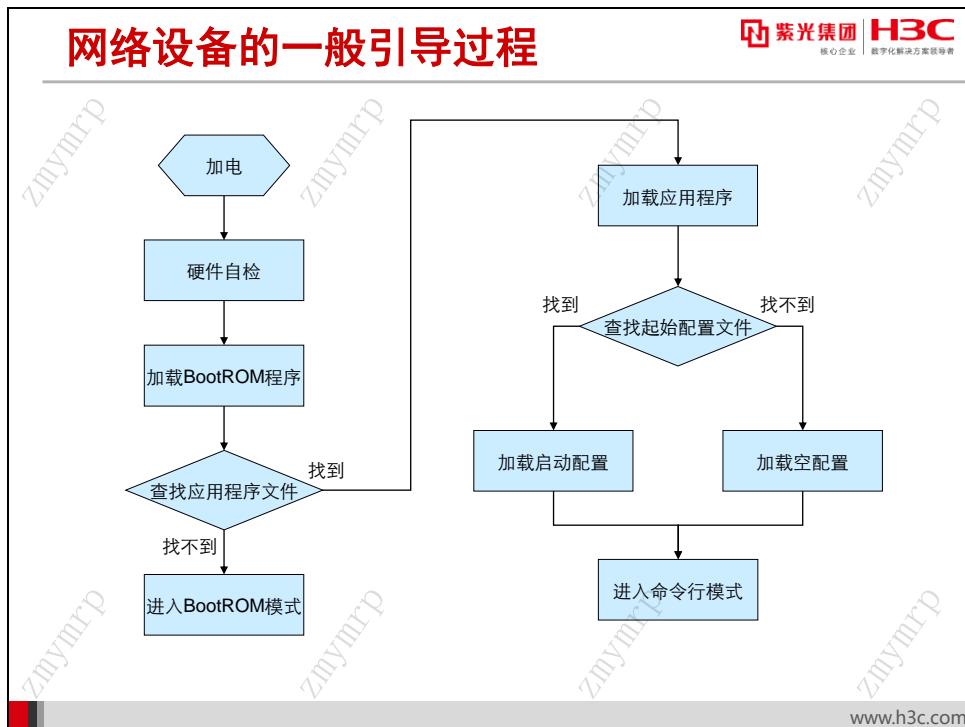
www.h3c.com

当指定了新的启动文件操作系统软件或者执行了 BootROM 升级之后，需要重启设备完成系统软件的升级。

用户可以用 **reboot** 命令使设备立即重启；也可以通过 **schedule** 命令设置一个时刻，让设备定时自动重启，或设置一个时延，让设备经过指定时间后自动重启。

9.4 网络设备软件维护基础

9.4.1 网络设备的一般引导过程



虽然网络设备的启动过程根据设备型号、软件版本等各自有所不同，但基本上都要经历硬件自检、BootROM 软件引导、Comware 系统初始化等几个阶段。之后，操作系统将接管设备的控制，完成大部分业务功能。

如流程图所示，路由器加电后，首先进行硬件的自检，紧接着是 BootROM 的启动过程。BootROM 是存放在主板 ROM 中的一段程序，可以将它类比为个人计算机 CMOS 中的基本输入输出系统（BIOS），在设备的操作系统真正运行前负责系统的引导，并维护系统的一些底层参数。接下来，在 BootROM 程序的引导下，设备开始查找 Comware 应用程序文件，找到后即将其解压缩并加载运行。随后，Comware 将读取并复原设备的配置文件。整个系统启动后，用户就可进入命令行界面进行相关操作了。

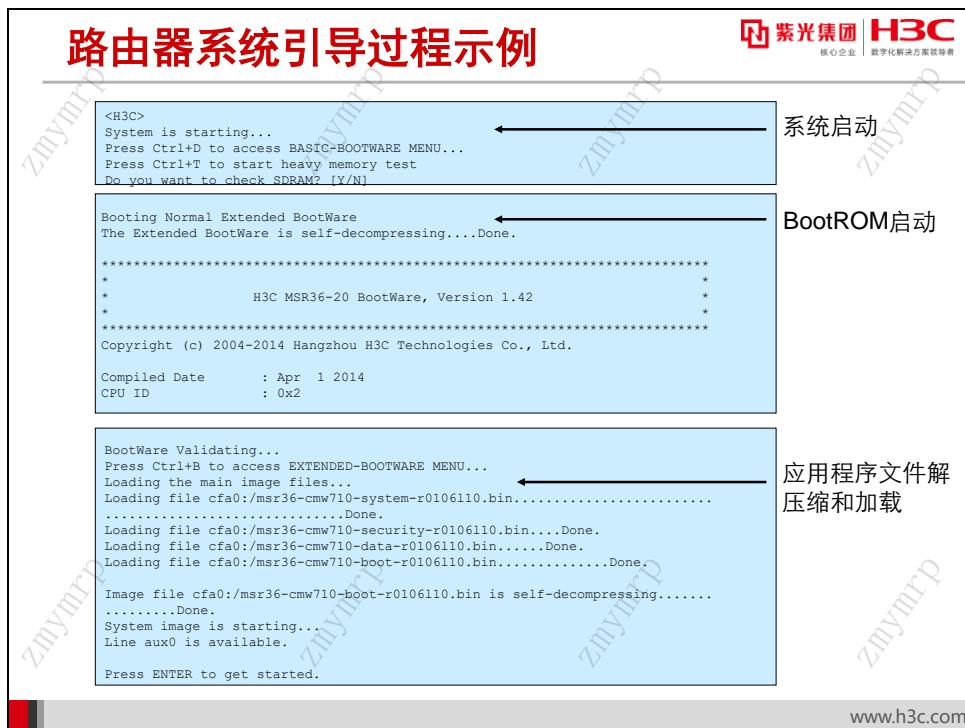
如果 BootROM 程序无法找到 Comware 应用程序文件，或 Comware 应用程序文件发生损坏，则系统进入 BootROM 模式，管理员可根据 BootROM 菜单进行修复操作。管理员也可以强制中断启动过程，进入 BootROM 模式。

网络设备可以保存多个配置文件。系统启动时优先选择用户指定的启动配置文件，如果没有指定任何启动配置文件，则以空配置启动。

注意：

正如支持多配置文件一样，出于安全考虑，网络设备也支持多映像功能。系统可以同时保存多个启动软件包，启动软件包可以分为主程序文件、备份程序文件和安全程序文件，系统亦将以此顺序选择这三个文件来启动路由器。

此功能的细节超出本书范围，读者可自行参考相关手册。



图例显示了路由器的典型启动信息输出。在本例子中，BootROM 的版本为 1.42。在 BootROM 启动末段，根据提示键入<Ctrl+B>，系统将中断引导，进入 BootROM 模式；否则，系统将进入程序解压过程。

注意：

必须在出现“Press Ctrl+B to access EXTENDED-BOOTWARE MENU...”提示的 6 秒钟之内键入<Ctrl+B>，系统方能进入 BootROM 菜单，否则系统将进入程序解压过程。若程序进入解压过程后再希望进入 BootROM 菜单，则需要重新启动路由器。

交换机的启动过程与路由器启动过程大体一致，本书不再图示。

9.4.2 网络设备的一般性软件维护方法

网络设备软件维护的一般性方法



- 在命令行模式中采用**TFTP/FTP**上传/下载应用程序及配置文件，实现应用程序升级
- 在**BootROM**模式中通过以太口采用**TFTP/FTP**完成应用程序软件升级
- 在**BootROM**模式中通过**Console**口采用**XModem**协议完成**BootROM**及应用程序的升级

H3C 网络设备提供了丰富而灵活的软件维护方法：

- 在命令行模式中采用 **TFTP/FTP** 来上传/下载应用程序或配置文件，实现应用程序升级或配置管理；
- 在 **BootROM** 模式中通过以太口采用 **TFTP/FTP** 完成应用程序软件升级；
- 在 **BootROM** 模式中通过 **Console** 口采用 **XModem** 协议完成 **BootROM** 及应用程序的升级。

在常规情况下，设备可以正常引导到命令行模式，而管理员希望对操作系统软件进行升级或备份，或者希望快速导入导出配置文件。此时可以直接在命令行模式中采用 **TFTP/FTP** 方式进行文件的上传/下载，这是比较方便的一种方式。

在某些情况下，设备无法引导到命令行模式，只能进入 **BootROM** 模式，而管理员希望对操作系统软件进行恢复或升级。此时可以在 **BootROM** 模式中利用 **BootROM** 菜单提供的操作功能，采用 **TFTP/FTP** 方式上传应用程序文件，使设备能够正常启动并引导到命令行模式。在这种模式下，必须将 **TFTP/FTP** 服务器连接到设备的特定以太端口上。

在上述情况下，如果无法实现 **TFTP/FTP** 服务器与设备的网络连接（例如端口损坏或无服务器软件），则可以在 **BootROM** 模式中通过 **Console** 口采用 **XModem** 协议完成 **BootROM** 及应用程序的升级，使设备能够正常启动并引导到命令行模式。

注意：

错误的 BootROM、配置文件和应用程序文件管理操作可能导致设备无法启动。只有理解了 BootROM 相关选项或参数作用，并且在确有必要的情况下才可进行相关操作。

9.5 本章总结

本章总结

- 设备对存储介质中的文件以文件系统的方式管理
- 文件系统操作包括目录操作、文件操作、介质操作等
- 配置文件包括起始配置和当前配置
- 通过指定启动文件可以进行操作系统软件升级
- 可用FTP和TFTP远程加载配置文件、操作系统软件和BootROM等系统文件

第10章 网络设备基本调试

网络按照初始目标组建配置完成后，首要的任务是检查网络的连通性。网络的连通性是指一台主机或设备上的一个 IP 地址到另一台主机或设备上的一个 IP 地址的可达性。本章将介绍检测网络连通性的常用命令。

为了达到网络连通性，单个网络设备及网络设备之间同时还运行各种协议或交互相关控制信息。有时，为了定位这些协议或模块是否正常运行，需要使用调试工具。本章对如何使用调试工具以及如何控制调试信息的输出和显示也进行了介绍。

10.1 本章目标

课程目标

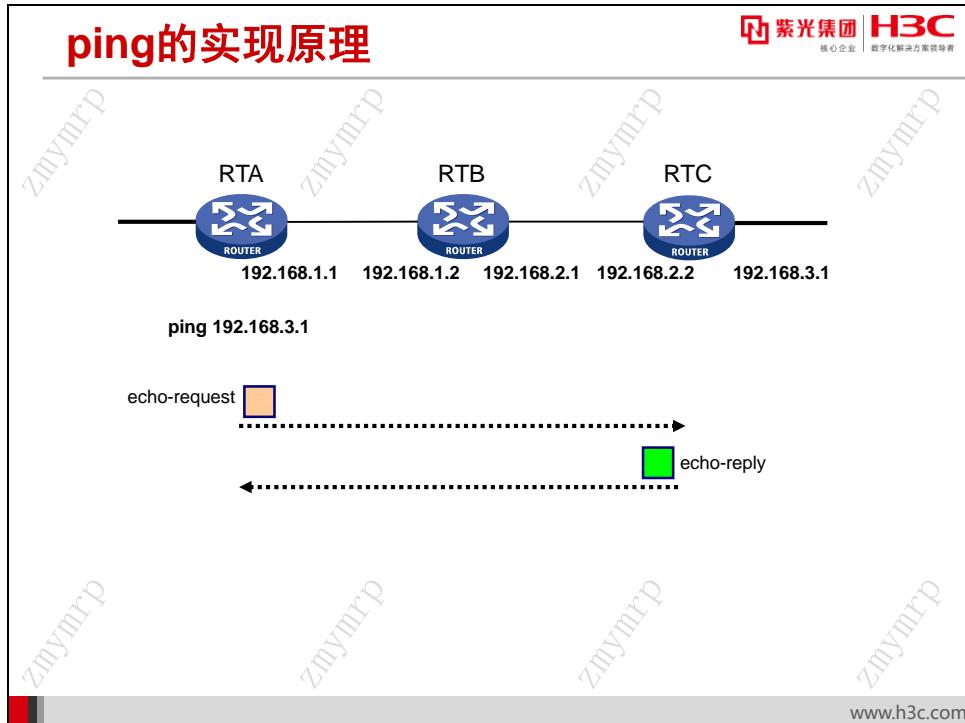
学习完本课程，您应该能够：

- 掌握用ping、tracert命令检查系统连通性
- 掌握使用debug等命令进行网络系统基本调试的方法



10.2 网络连通性测试

10.2.1 使用 ping 测试网络连通性



ping 实际上是基于 ICMP 协议开发的应用程序，它是在计算机的各种操作系统或网络设备上广泛使用的检测网络连通性的常用工具。通过使用 ping 命令，用户可以检查指定地址的主机或设备是否可达，测试网络连接是否出现故障。

ICMP 定义了不同类型的协议报文，ping 主要使用了其中 Echo Request（回波请求）和 Echo Reply（回波响应）两种报文。如图所示，在 RTA 命令行界面输入 ping 192.168.3.1 命令，源设备 RTA 向目的设备 RTC 发送 ICMP Echo Request 报文；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 Echo Reply 报文（如本例）；如果网络工作异常，源设备 RTA 将显示目的地址不可达或超时等提示信息。通过这个交互过程，源设备 RTA 即可知道目的设备的 IP 层相关状态。

ping命令的输出

紫光集团 **H3C**
核心企业 | 数字化解决方案领导者

```
[RTA]ping 192.168.3.1
Ping 192.168.3.1 (192.168.3.1): 56 data bytes, press CTRL-C to break
56 bytes from 192.168.3.1: icmp_seq=0 ttl=64 time=1.824 ms
56 bytes from 192.168.3.1: icmp_seq=1 ttl=64 time=1.591 ms
56 bytes from 192.168.3.1: icmp_seq=2 ttl=64 time=1.204 ms
56 bytes from 192.168.3.1: icmp_seq=3 ttl=64 time=1.402 ms
56 bytes from 192.168.3.1: icmp_seq=4 ttl=64 time=0.919 ms

--- Ping statistics for 192.168.3.1 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.919/1.388/1.824/0.312 ms
[RTA]Oct 17 07:45:09:111 2013 RTA PING/6/PING_STATISTICS: Ping
statistics for 192.168.3.1: 5 packets transmitted, 5 packets received,
0.0% packet loss, round-trip min/avg/max/std-dev =
0.919/1.388/1.824/0.312 ms.
```

www.h3c.com

上图演示了 ping 命令的实际输出结果。

在本例中, RTA 在超时时间内收到了目的设备 RTC 对每个 ICMP Echo Request 报文的响应, 因此 RTA 上输出了响应报文的字节数、报文序号、TTL (Time To Live, 生存时间)、响应时间。

在图中最后的几行中, 输出了 ping 过程报文的统计信息, 主要包括发送报文个数、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。

使用 ping 命令

```

<H3C>ping ?
  -a          Specify the source IP address
  -c          Specify the number of echo requests
  -f          Specify packets not to be fragmented
  -h          Specify the TTL value
  -i          Specify an outgoing interface
  -m          Specify the interval for sending echo requests
  -n          Numeric output only. No attempt will be made to lookup host
             addresses for symbolic names
  -p          No more than 8 "pad" hexadecimal characters to fill out the
             sent packet. For example, -p f2 will fill the sent packet
             with 000000f2 repeatedly
  -q          Display only summary
  -r          Record route. Include the RECORD_ROUTE option in the
             ECHO_REQUEST packets and display the route
  -s          Specify the payload length
  -t          Specify the wait time for each reply
  -topology   Specify a topology
  -tos        Specify the TOS value
  -v          Display the received ICMP packets other than ECHO-RESPONSE
             packets
  -vpn-instance  STRING<1-253>  Specify a VPN instance
  ip          IP information
  ipv6        IPv6 information

```

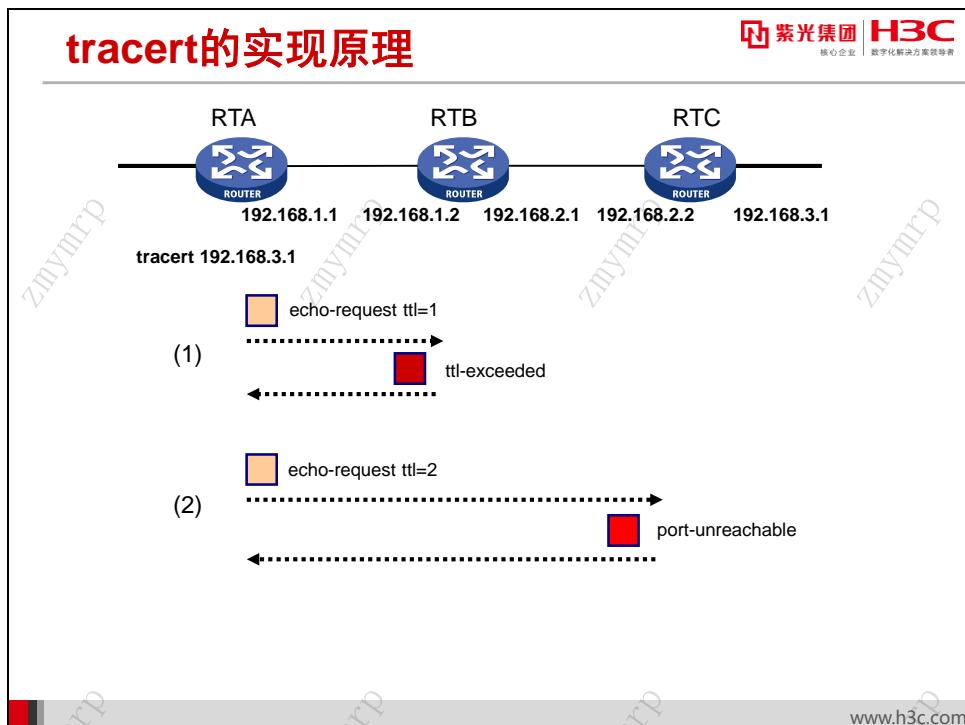
www.h3c.com

ping 命令提供了丰富的可选参数, 说明如下:

- **-a source-ip:** 指定 ICMP Echo Request 报文中的源 IP 地址;
- **-c count:** 指定发送 ICMP Echo Request 报文的数目, 取值范围为 1~4294967295, 默认值为 5;
- **-f:** 将长度大于接口 MTU 的报文直接丢弃, 即不允许对发送的 ICMP Echo Request 报文进行分片;
- **-h ttl:** 指定 ICMP Echo Request 报文中的 TTL 值, 取值范围为 1~255, 默认值为 255;
- **-i interface-type interface-number:** 指定发送报文的接口的类型和编号;
- **-m interval:** 指定发送 ICMP Echo Request 报文的时间间隔, 取值范围为 1~65535, 单位为毫秒, 默认值为 200 毫秒。如果在 timeout 时间内收到目的主机的响应报文, 则下次 ICMP Echo Request 报文的发送时间间隔为报文的实际响应时间与 interval 之和; 如果在 timeout 时间内没有收到目的主机的响应报文, 则下次 ICMP Echo Request 报文的发送时间间隔为 timeout 与 interval 之和;
- **-n:** 不进行域名解析。默认情况下, 系统将对 hostname 进行域名解析;
- **-p pad:** 指定 ICMP Echo Request 报文 “PAD” 字段的填充值, 为 1~8 位的 16 进制数。比如, 若将 pad 设置为 0xff, 则 “PAD” 字段将被全部填充为 0x000000ff, 以便发送报文的总长度达到设备要求值。默认情况下, 填充的字节从 0x01 开始, 逐渐递增, 直到 0xff, 然后又从 0x01 开始循环填充;

- **-q**: 只显示统计信息。默认情况下，系统将显示包括统计信息在内的全部信息；
- **-r**: 记录路由。默认情况下，系统不记录路由；
- **-s packet-size**: 指定发送的 ICMP Echo Request 报文的长度（不包括 IP 和 ICMP 报文头），取值范围为 20~8100，单位为字节，默认值为 56 字节；
- **-t timeout**: 指定 ICMP Echo Reply 报文的超时时间，取值范围为 0~65535，单位为毫秒，默认值为 2000 毫秒；
- **-tos tos**: 指定 ICMP Echo Request 报文中的 ToS（Type of Service，服务类型）域的值，取值范围为 0~255，默认值为 0；
- **-v**: 显示接收到的非 Echo Reply 的 ICMP 报文。默认情况下，系统不显示非 Echo Reply 的 ICMP 报文。

10.2.2 使用 tracert 检测网络连通性



通过使用 **tracert** 命令，用户可以查看报文从源设备传送到目的设备所经过的路由器。当网络出现故障时，用户可以使用该命令分析出现故障的网络节点。

本图演示了在 RTA 上执行 **tracert 192.168.3.1** 命令的工作过程：

- 1) 源设备 RTA 对目的设备的某个较大的端口发送一个 TTL 为 1 的 UDP 报文；
- 2) 由于网络设备处理 IP 报文中的 TTL 值时，将其逐跳递减，因此，该报文到达第一跳 RTB 后，TTL 将变为 0，RTB 于是回应一个 TTL 超时的 ICMP 报文，该报文中含有第一跳的 IP 地址，这样源设备就得到了第一跳路由器 RTB 的地址；

- 3) 源设备重新发送一个 TTL 为 2 的报文给目的设备;
- 4) TTL 为 2 的 ICMP 报文首先传递给 RTB, TTL 递减为 1, 该 ICMP 报文到达 RTC 后, TTL 将递减为 0, 由于 RTC 是 ICMP 的目的地, RTC 将回应给 RTA 一个端口不可达的 ICMP 消息, RTA 收到该消息后, 将会知道已经跟踪到了目的地, 因此, 将停止向外发送报文;
- 5) 如果 RTC 距离 RTA 有多跳, 以上过程将不断进行, 直到最终到达目的设备, 源设备就得到了从它到目的设备所经过的所有路由器的地址。

tracert命令的输出

紫光集团 H3C
核心企业 | 数字化解决方案领导者

```
[RTA]tracert 192.168.3.1
traceroute to 192.168.3.1 (192.168.3.1), 30 hops at most, 52 bytes each packet,
press CTRL_C to break
 1  192.168.1.2 (192.168.1.2)  0.691 ms  0.497 ms  0.491 ms
 2  192.168.3.1 (192.168.3.1)  0.996 ms  0.896 ms  0.902 ms
```

```
*Oct 17 09:17:11:996 2013 RTA IPFW/7/IPFW_PACKET:
Sending, interface = GigabitEthernet0/0, version = 4, headlen = 20, tos = 0,
pktlen = 52, pktid = 33516, offset = 0, ttl = 1, protocol = 17,
checksum = 45434, s = 192.168.1.1, d = 192.168.3.1
prompt: Sending the packet from local at GigabitEthernet0/0.

*Oct 17 09:17:11:996 2013 RTA IPFW/7/IPFW_PACKET:
Receiving, interface = GigabitEthernet0/0, version = 4, headlen = 20, tos = 0,
pktlen = 80, pktid = 32, offset = 0, ttl = 255, protocol = 1,
checksum = 14393, s = 192.168.1.2, d = 192.168.1.1
prompt: Receiving IP packet.

*Oct 17 09:17:11:997 2013 RTA SOCKET/7/ICMP:
Time(s):1382001431  ICMP Input:
ICMP Packet: src = 192.168.1.2, dst = 192.168.1.1
              type = 11, code = 0 (ttl-exceeded)
Original IP: src = 192.168.1.1, dst = 192.168.3.1
proto = 17, first 8 bytes = 82EC829A 00200000
```

www.h3c.com

本图的上半部分显示了 RTA 执行 **tracert** 命令后的输出, 对于每个 TTL 递增的报文, RTA 都要重复发三次, 因此输出结果中显示了每一跳接收响应的时延。最后一跳是跟踪的目的地。

本图的下半部分显示了 RTA 执行 **tracert** 命令后的调试信息 (后面的小节中将详细讲解如何获得调试信息), 调试信息显示了中间跳路由器和最后目的跳路由器对 RTA 的不同响应方法。

使用tracert命令

```

<H3C>tracert ?
-a          Specify the source IP address used by TRACERT
-f          Specify the TTL value for the first packet
-m          Specify the maximum TTL value
-p          Specify the destination UDP port number
-q          Specify the number of probe packets sent each time
-t          Set the Type of Service (ToS) value
-topology   Specify a topology
-vpn-instance Specify a VPN instance
-w          Set the timeout to wait for each reply
STRING<1-253> IP address or hostname of the destination device
ipv6        IPv6 information
  
```

www.h3c.com

tracert 命令使用的可选参数含义如下：

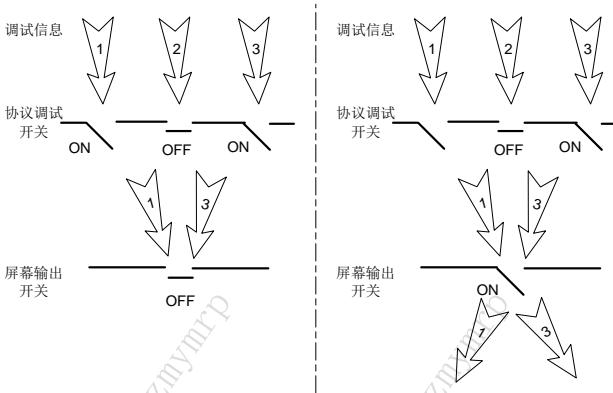
- **-a source-ip:** 指明 **tracert** 报文的源 IP 地址。该地址必须是设备上已配置的合法 IP 地址。不指定该参数时，**tracert** 报文的源 IP 地址是该报文出接口的主 IP 地址；
- **-f first-ttl:** 指定一个初始 TTL，即第一个报文所允许的跳数。取值范围为 1~255，且小于或等于最大 TTL，默认值为 1；
- **-m max-ttl:** 指定一个最大 TTL，即一个报文所允许的最大跳数。取值范围为 1~255，且大于或等于初始 TTL，默认值为 30；
- **-p port:** 指明目的设备的 UDP 端口号，取值范围为 1~65535，默认值为 33434。用户一般不需要更改此选项；
- **-q packet-num:** 指明每次发送的探测报文个数，取值范围为 1~65535，默认值为 3；
- **-t tos:** 指定 **Tracert** 报文中 ToS 域的值，取值范围为 0~255，默认值为 0；
- **-vpn-instance vpn-instance-name:** 指定目的设备所属的 VPN；
- **-w timeout:** 指定探测报文的响应报文的超时时间，取值范围是 1~65535，单位为毫秒，默认值为 5000 毫秒；
- **host:** 目的设备的 IP 地址或主机名（主机名是长度为 1~253 的字符串）。

10.3 系统调试

10.3.1 系统调试概述

系统调试介绍

- 对网络设备所支持的绝大部分协议和功能，系统都提供了相应的调试功能，帮助用户对错误进行诊断和定位
- 调试信息的输出由两个开关控制




H3C
核心企业 | 数字化解决方案领导者

www.h3c.com

对于设备所支持的各种协议和特性，系统基本上都提供了相应的调试功能，帮助用户对错误进行诊断和定位。

调试信息的输出可以由两个开关控制：

- 协议调试开关：也称为模块调试开关，控制是否输出某协议模块的调试信息；
- 屏幕输出开关：控制是否在某个用户屏幕上显示调试信息。

协议调试开关和屏幕输出开关的关系如图所示。用户只有将两个开关都打开，调试信息才会在终端显示出来。

10.3.2 系统调试操作

系统调试的操作



- 开启控制台对系统信息的监视功能
<H3C> terminal monitor
- 打开调试信息的屏幕输出开关
<H3C> terminal debugging
- 打开模块调试开关
<H3C> debugging module-name
- 显示调试开关
<H3C> display debugging

www.h3c.com

terminal debugging 命令的作用是打开调试信息的屏幕输出开关，以控制是否在某个用户屏幕上显示调试信息。

debugging 命令用于打开协议调试开关。因此，该命令后面要指定相关的协议模块名称，如 ATM、ARP。当然模块名称可能不只一个参数，比如关心 IP 层如何处理报文时，可以使用 **debugging ip packet** 命令。

terminal monitor 命令用于开启控制台对系统信息的监视功能。调试信息属于系统信息的一种，因此，这是一个更高一级的开关命令，只不过该命令在需要观察调试信息时候是可选的，因为默认情况下，控制台的监视功能就处于开启状态。

最后，通过 **display debugging** 命令可以查看系统当前哪些协议调试信息开关是打开的。

10.3.3 调试信息输出示例

调试信息输出的例子

紫光集团 H3C
核心企业 数字化解决方案领导者

```

<RTA>ping -c 1 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.2: icmp_seq=0 ttl=64 time=1.802 ms

--- Ping statistics for 192.168.1.2 ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.802/1.802/1.802/0.000 ms

<RTA>*Oct 17 08:28:50:880 2013 RTA IPFW/7/IPFW_PACKET:
Sending, interface = GigabitEthernet0/0, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 79, offset = 0, ttl = 255, protocol = 1,
checksum = 14342, s = 192.168.1.1, d = 192.168.1.2
prompt: Sending the packet from local at GigabitEthernet0/0.

*Oct 17 08:28:50:882 2013 RTA IPFW/7/IPFW_PACKET:
Receiving, interface = GigabitEthernet0/0, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 3446, offset = 0, ttl = 64, protocol = 1,
checksum = 59871, s = 192.168.1.2, d = 192.168.1.1
prompt: Receiving IP packet.

*Oct 17 08:28:50:882 2013 RTA IPFW/7/IPFW_PACKET:
Delivering, interface = GigabitEthernet0/0, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 3446, offset = 0, ttl = 64, protocol = 1,
checksum = 59871, s = 192.168.1.2, d = 192.168.1.1
prompt: IP packet is delivering up.

%Oct 17 08:28:50:886 2013 RTA PING/6/PING_STATISTICS: Ping statistics for
192.168.1.2: 1 packets transmitted, 1 packets received, 0.0% packet loss, round-
trip min/avg/max/std-dev = 1.802/1.802/1.802/0.000 ms.

```

www.h3c.com

这里是一个为了观察 **ping** 命令执行过程，打开 **debug ip packet** 协议调试开关的例子。该例显示了当 RTA 发出一个 ICMP ECHO-REQUEST 报文和收到一个 ICMP ECHO-REPLY 报文时，IP 协议层处理的详细过程。

该例中，执行 **ping** 命令时使用了**-c** 参数，因此只发出一个 ICMP 请求回应报文。“Oct 17 08:28:50:880 2013 RTA IPFW/7/IPFW_PACKET:”为屏幕打出的系统信息，提示以下将是调试信息的输出，并且说明了调试信息的输出时间，及相关的模块名 **IPFW**——IP 转发模块。

调试信息分为三个段落。第一段说明了承载该 ICMP 报文的 IP 报头实际内容，包括报文长度、报文 ID、偏移量、协议号、源地址和目的地址等。经过查找路由表/转发表，该 ICMP 报文将从本地的 **GigabitEthernet0/0** 转发出去。第二段说明 RTA 从 **GigabitEthernet0/0** 收到了一个报文，和第一段类似，RTA 打印出了该报文 IP 头的相关内容。可以看出，这个报文就是对刚刚发出的 ICMP 回声请求报文的应答。最后一段与第二段描述的是同一个报文，由于 RTA 就是此报文的目的地，它要被递交给本地 IP 转发层的上层进行处理。

在图中最后的几列中显示了 **ping** 过程报文的统计信息，主要包括：发送了一个报文，接收到一个响应报文，由于没有未响应报文，因此丢包率是 0%，此次 **ping** 响应时间的最小值、平均值和最大值都是 1.802 毫秒（因为只进行了一次 ICMP 请求和应答）。

10.4 本章总结

本章总结

- **ping**使用ICMP回显请求与应答检测网络连通性
- **tracert**使用TTL超时机制检测网络连通性
- 调试信息的输出由协议开关和屏幕开关两个开关控制