甲信三层以太网交换机基础配置

配置指南(CLI)

(Rel_01)

北京甲信技术有限公司（以下简称“甲信”）为客户提供全方位的技术支持和服务。直接向甲信购买产品的用户，如果在使用过程中有任何问题，可与甲信各地办事处或用户服务中心联系，也可直接与公司总部联系。

读者如有任何关于甲信产品的问题，或者有意进一步了解公司其他相关产品，可通过下列方式与我们联系：

公司网址：　　www.jiaxinnet.com.cn

技术支持邮箱：　jxhelp@bjjx.cc

技术支持热线：　400-179-1180

公司总部地址：　北京市海淀区丹棱 SOHO 7 层 728 室

邮政编码:　　100080

声　明

目录

1 基础配置

本章介绍交换机设备的基础配置信息及配置过程，并提供相关的配置案例。

- 登录设备
- 加载与升级
- 时间管理
- 接口管理

1.1 登录设备

1.1.1 简介

登录交换机设备进行配置和管理，可以采用 CLI（Command-Line Interface，命令行界面）方式、Web 方式。

交换机命令行方式下有多种配置方式：

- Console 方式：第一次配置时必须采用 Console 方式，甲信设备支持 RJ45、M12、Micro USB 和 Mini-USB 类型的 Console 口。
- Telnet 方式：设备默认 IP 地址为 192.168.0.1。如需修改 IP 地址，需要先通过 Console 方式登录，在设备上配置 IP 地址，以及设置用户名和密码，再使用新 IP 地址进行远程 Telnet 配置。
- SSH 方式：在通过 SSH 登录设备之前，需要先通过 Console 接口登录设备并启动 SSH 服务。

当需要在 Web 方式下配置时，也必须先通过命令行方式，配置 VLAN 接口 IP 地址，然后才可以通过 NView NNM 网管平台对设备进行配置。

1.1.2 通过 Console 口登录设备

说明

- 设备均支持 RJ45 类型的 Console 口。
- 设备使用黑色线序 Console 线缆，如不确定，请查看该设备系列对应的《用户手册》或《产品描述》手册，或咨询我司技术人员。
- 以下均以 RJ45 类型 Console 口为例进行说明。

简介

Console 口是网络设备用来与运行终端仿真程序的 PC 进行连接的常用接口，用户可以借助此接口对本地设备进行配置和管理。这种管理方式不需借助网络进行通信，所以被称为带外（out-of-band）管理方式，在网络运行异常的情况下，用户也可以通过 Console 口对设备进行配置和管理。

在以下两种情况中，只能通过 Console 口登录设备进行配置：

- 设备第一次加电启动
- 无法通过 Telnet 方式登录设备

缺省配置

设备上 Console 口的缺省配置如下。

功能	缺省值
传输速率	115200
流控方式	无流控
验证方式	不验证
停止位	1
数据位	8

通过 Console 口登录

当用户希望通过 PC 连接 Console 口登录设备时，首先需要通过配置线缆将设备的 Console 口和 PC 的 RS-232 串口相连，如图 1-1 所示，然后在 PC 上运行终端仿真程序，如微软公司的 Windows XP 操作系统自带的“超级终端”程序，将通信参数如图 1-2 配置，完成后即可登录设备。

图 1-1 通过 PC 连接 Console 口登录设备的组网示意图

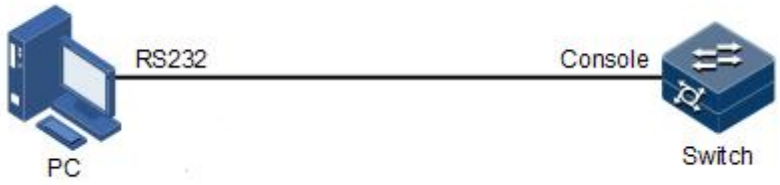


图 1-2 “超级终端”中的通信参数配置示意图

说明

初始情况下串口波特率为 115200。

配置 Console 口波特率

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure** JX(config)#**line console** JX(config-line-console)#**baudrate { 115200 | 9600 }**	修改串口登录波特率。

配置 Console 密码和认证方式

请在设备上进行以下配置。

步骤	配置	说明
1	JX#configure JX(config)#line console password	设置串口密码。
2	JX(config)#line console JX(config-line-console)#login authentication { local | password | none}	设置串口认证方式 local：用户名密码 password：串口密码 none：不认证

检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#show line console information	查看串口波特率配置信息。

1.1.3 通过 Telnet 登录设备

简介

说明

初始情况下，设备缺省管理 IP 地址为 192.168.0.1，子网掩码为 255.255.255.0。如需修改设备 IP 地址，用户可以通过 Console 口登录设备，并对设备进行配置。设备的缺省用户名和密码均为 JX。Telnet 连接状态下输错 3 次密码自动断开连接。

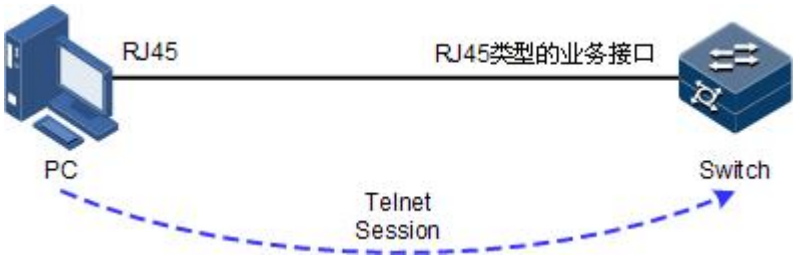
Telnet 提供了一种通过 PC 远程登录设备的方式。用户可以先通过 PC 登录到一台网络设备，然后再通过 Telnet 方式远程登录到联网的其他网络设备，而不需要为每一台网络设备都连接一台 PC。

有 SNMP 接口的设备，需使用 SNMP 接口进行 telnet 登录。无 SNMP 接口的设备，可以使用任意接口进入管理 VLAN 进行 telnet 登录。

交换机设备提供的 Telnet 服务包括：

- Telnet Server：用户在 PC 上运行 Telnet 客户端程序登录到设备，对设备进行配置管理。如下图所示，交换机此时提供的是 Telnet Server 服务。

图 1-3 交换机作为 Telnet Server 设备的组网示意图

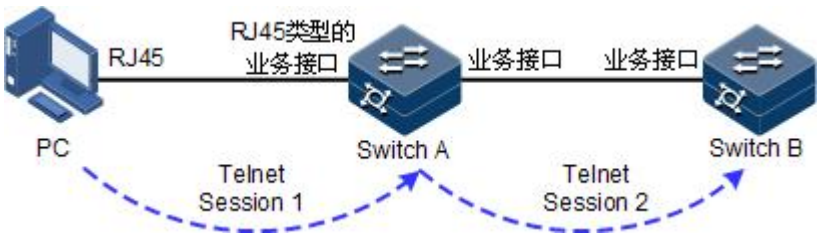


说明

设备支持 Telnet 最大用户数为 10 个。

- Telnet Client：用户在 PC 上通过终端仿真程序或 Telnet 客户端程序建立与设备的连接后，再通过 telnet 命令登录到其它设备，对其进行配置管理。如下图所示，Switch A 此时既作为 Telnet Server，也同时提供 Telnet Client 服务。

图 1-4 交换机设备作为 Telnet Client 设备的组网示意图



缺省配置

设备上 Telnet 服务器功能的缺省配置如下。

功能	缺省值
Telnet 服务器功能状态	使能
Telnet 服务器监听端口号	23
使能 Telnet 服务器功能的接口	所有接口
最大 Telnet 连接数	10

说明

通过 Telnet 配置设备时，建议不要频繁修改设备的 IP 地址。修改 IP 地址可能导致当前 Telnet 连接断开，需根据新的 IP 地址重新建立 Telnet 连接。

配置 Telnet 服务器

在通过 Telnet 登录设备之前，用户需要通过 Console 接口登录设备并启动 Telnet 服务，请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface vlan** *vlan-id* JX(config)#**interface ge 1/0/1**	进入 VLAN 接口或带外接口配置模式，以下使用进入 VLAN 接口为例。
3	JX(config-vlan*)#**ip address** *ip-address* [*ip-mask*] [**sub**] JX(config-vlan*)#**ipv6 address** *ipv6-address/prefix-length* [**eui-64**] JX(config-vlan*)#**exit**	配置设备 IP 地址。
4	JX(config)#**telnet server start**	开启设备 Telnet Server 功能。
5	JX(config)#**telnet server stop**	断开指定的 Telnet 连接。
6	JX(config)#**telnet-ipv6 server start**	开启设备 IPv6 Telnet Server 功能。
7	JX(config)#**telnet-ipv6 server stop**	断开指定的 IPv6 Telnet 连接。

配置 Telnet 服务器端口号

Telnet 缺省端口号为 23，可进行以下配置修改端口号。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**telnet server port** {*port-number* | **default**}	修改 Telnet IPv4 服务端口号。
3	JX(config)#**telnet-ipv6 server start**	开启设备 IPv6 Telnet Server 功能。
4	JX(config)#**telnet-ipv6 server port** {*port-number* | **default**}	修改 Telnet IPv6 服务端口号。

配置 Telnet 客户端

请在作为 Telnet Client 的设备上进行以下配置。

步骤	配置	说明
1	JX#**telnet** *ipv4-address* [**-p** *port-id* | **-s** *source-ipv4-address*] JX#**telnet-ipv6** *ipv6-address* [**-p** *port-id* | **-s** *source-ipv6-address*]*	以 Telnet 方式登录其他设备。

检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show running-config**	查看 Telnet Server 的配置情况。

1.1.4 通过 SSH 登录设备

简介

Telnet 缺少安全的认证方式，而且传输过程采用 TCP（Transmission Control Protocol，传输控制协议）进行明文传输，存在很大的安全隐患。单纯提供 Telnet 服务容易招致 DoS（Deny of Service，拒绝服务）、主机 IP 地址欺骗、路由欺骗等恶意攻击。

传统的 Telnet 和 FTP（File Transfer Protocol，文件传输协议）通过明文传送密码和数据的方式，已经慢慢不被用户所接受。SSH 是一个网络安全协议，通过对网络数据的加密，可以有效防止远程管理过程中的信息泄露问题，在网络环境中为远程登录和其他网络服务提供了更高的安全性。

SSH 通过 TCP 进行数据交互，它在 TCP 之上构建了一个安全的通道。另外，SSH 服务除了支持标准端口 22 以外，还支持其他服务端口，以防止设备受到来自网络的非法攻击。

在通过 SSH 登录设备之前，用户需要通过 Console 接口登录设备并启动 SSH 服务。

设备支持基于密码和公钥两种认证方式。

- 基于密码认证方式：与登录设备认证使用同一数据库。SSH 客户端只需输入用户名和密码，就可以登录到远程 SSHv2 服务器。所有传输的数据都会被加密，但是可能会有其他服务器伪冒真正的服务器，无法避免伪冒服务器攻击。
- 基于公钥认证方式：SSHv2 客户端除需要输入用户名和密码外，还需要依靠密钥进行认证。登录前在 SSHv2 客户端创建一对密钥，包括主机公钥和主机私钥，并将公钥存入 SSHv2 服务器。登录认证过程和传输的数据都会被加密，避免了伪冒服务器攻击。

缺省配置

设备上 SSH 登录设备的缺省配置如下。

功能	缺省值
SSH 服务器功能状态	禁止
本地 SSH 密钥对长度	512bit
密钥重协商周期	0h
SSH 采用的认证方式	password
SSH 认证超时时间	600s
SSH 侦听端口号	22
SSH 会话功能状态	禁用
SSH 协议版本	v2
SSH 安全算法模式	禁止

配置 SSH 服务器

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**ssh server start**	开启设备 IPv4 SSH Server 功能
3	JX(config)#**ssh server stop**	关闭设备 IPv4 SSH Server 功能
2	JX(config)#**ssh-ipv6 server start**	开启设备 IPv6 SSH Server 功能
3	JX(config)#**ssh-ipv6 server stop**	关闭设备 IPv6 SSH Server 功能

检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show ssh config**	查看 SSH 配置信息。

1.1.5 通过 Web 登录设备

简介

为了方便用户对设备进行配置和维护，设备支持 Web 网管功能。用户可以利用 Web 网管在图形界面下直观的管理和配置设备。

Web 网管支持以下两种文本传输协议：

- HTTP（Hypertext Transfer Protocol，超文本传输协议）：用来在网络上传递 Web 页面信息。在设备上使能 HTTP 服务功能后，用户就可以通过 HTTP 协议登录设备，并利用 Web 界面访问、控制设备。
- HTTPS（Secure Hypertext Transfer Protocol，安全的超文本传输协议）：利用 SSL（Secure Sockets Layer，安全套接层）协议保证合法客户端可以安全访问设备。客户端与设备之间交互的数据需要经过加密，保证了数据传输的安全性和完整性，从而实现对设备的安全管理。

配置 Web 网管功能后，远程用户可以通过 Web 浏览器登录设备并对其进行管理。如果禁止 Web 网管功能，则断开所有已经建立的 HTTP 连接。

缺省配置

设备上 Web 网管的缺省配置如下。

功能	缺省值
HTTP 功能状态	使能

配置 Web 网管功能

请在设备上进行以下配置。

步骤	配置	说明
1	`JX#configure`	进入全局配置模式。
2	`JX(config)#http server { start | stop }`	使能 HTTP 功能，使用 **stop** 格式禁止该功能。
3	`JX(config)#https server { start | stop }`	使能 HTTPS 功能，使用 **stop** 格式禁止该功能。

检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	`JX#show running-config`	查看设备配置信息。

1.1.6 管理登录用户

简介

第一次启动交换机设备时，用户只要将 PC 通过 Console 接口与设备连接，在超级终端中输入初始的用户名和密码，即可以登录设备并对其进行配置。

说明

初始情况下，设备的用户名为 JX，密码为 JX。

如果为设备的业务接口配置了 IP 地址，在没有任何权限控制的情况下，任意远端用户都可以通过 Telnet 方式登录设备，或者通过与设备建立 PPP（Point to Point Protocol，点对点协议）连接来访问网络，这显然对设备和网络都是不安全的。为此需要为设备创建用户并设置密码和权限，对登录用户进行管理。

缺省配置

设备上用户管理的缺省配置如下。

功能	缺省值
本地用户信息	• 用户名：JX • 密码：JX • 用户权限：15
新建用户权限	15
新建用户激活状态	**active**
新建用户服务类型	console、telnet、ssh、ftp、http
密码复杂度	**3**
密码复杂度	**3**
用户名复杂度	**1**
用户名最大长度	**64**
密码最大长度	**64**
缺省支持特殊字符	**`~!@#$%^&*()_-+={}[]\:;'<>",./**

配置本地用户管理

请在设备上进行以下配置。

步骤	配置	说明
1	JX(config)#**username** *user-name* **password** { **cipher** | **reversible-cipher** | **plain** } *password* **group** { **administrators** | **operators** | **users** | **guests** } [**domain** [**telnet** | **ssh** | **http** | **ftp** | **console** | **default** | **all**]]	创建或修改登录用户的用户名和密文形式密码。
2	JX(config)#**username** *user-name* **domain** [**telnet** | **ssh** | **http** | **ftp** | **console** | **default** | **all**]*	修改用户组域。
3	JX(config)#**username** *user-name* **group** { **administrators** | **operators** | **users** | **guests** }	修改用户组。
4	JX(config)#**user password-complex** { *complex* | **default** }	配置用户密码复杂度。
4	JX(config)#**user password-length** { *length* | **default** }	配置用户密码最小长度。
5	JX(config)#**user name-complex** { *complex* | **default** }	配置用户名复杂度，默认值为 1。
6	JX(config)#**user name-length** { *length* | **default** }	配置用户名长度，默认值为 1。
7	JX(config)#**username** *user-name* { **login-lock** | **manual-lock** | **unlock** } [**reauth-interval** { *interval* | **default** } | **fail-count** { *count* | **default**]*	配置用户锁定类型为 登录锁定（login-lock）时可以配置登录失败次数和重认证间隔。
8	JX#**show user name** *user-name*	查看配置用户的信息
9	JX#**user special-characters** *CHARLIST*	配置用户名称和用户密码可包含的特殊字符

说明

- 除缺省用户外，设备最多可再创建 30 个本地用户。
- 用户启用登录锁定（login-lock）时可配置最大登录失败次数和重认证间隔，默认失败次数上限是 3 次，重认证时间间隔为 10s。当登录失败达上限并且在静默时间内设备处于登录锁定，此时无法登录。超过静默时间，解除锁定，也可通过 unlock 手动解除锁定。
- 用户启动手工锁定（manual-lock）将会一直锁定，不受失败次数和重认证间隔限制。可通过 unlock 手动解除锁定

1.1.7 用户密码恢复

简介

当用户忘记设备登录用户密码时，用户只要将 PC 通过 Console 接口与设备连接，在超级终端中进入临时密码视图，获取临时密码序列号，可通过临时密码序列号生成临时密码。临时密码校验成功登录设备后，需要用户再次修改本地用户的密码。

说明

密码恢复操作只能在 Console 终端进行。在登录界面输入快捷键“CTRL+P”进入临时密码视图。

临时密码恢复功能缺省开启状态。

配置临时密码恢复

请在设备上进行以下配置。

步骤	配置	说明
1	快捷键 CTRL+P	在 Console 登录界面键入快捷键
2	JX(key)#**get temporary-password-serial**	获取临时密码序列号
3	JX(key)#**check temporary-password** *password*	校验临时密码
4	JX(config)#**temporary-password** { enable | disable }	开启关闭临时密码恢复功能。

1.1.8 终端属性设置

简介

用户可以设置 Console，Telnet，SSH 终端的超时时间，屏幕逐页滚动控制，终端颜色，大小写敏感，交互模式等终端属性。

配置终端属性

请在设备上进行以下配置。

步骤	配置	说明
1	JX(config)#**terminal length** { 0 | *length* | default }	设置屏幕逐页滚动的条数。 0：不逐页滚动，直接全部输出 缺省逐页滚动为 24 行
2	JX(config)#**terminal timeout** { 0 | *timeout* }	设置终端超时时间。 0：终端不超时 缺省超时时间 10 分钟
3	JX(config)#**terminal monitor** JX(config)#**no terminal monitor**	开启关闭终端信息监控
4	JX(config)#**terminal mmi-mode** { enable | disable }	开启关闭设备人机交互模式。
5	JX(config)#**case-sensitive** { enable | disable }	开启关闭输入大小写字母敏感功能

1.1.9 Bootrom 密码设置

简介

用户可以设置 bootrom 密码。

配置终端属性

请在设备上进行以下配置。

步骤	配置	说明
1	JX(config)#**bootrom password** *PASSWORD*	设置 bootrom 密码，密码字符串
2	JX(config)#**no bootrom password**	清除 bootrom 密码
3	JX(config)#**show bootrom password**	查看 bootrom 密码

1.2 加载与升级

1.2.1 简介

加载

传统的配置文件加载方式为串口加载，该方式加载速度慢、耗时长、不具备远程加载功能，导致操作很不方便。为了解决这些问题，引入了 FTP 加载方式、TFTP 加载方式等。

设备提供多种方法用于确定设备在 TFTP/FTP 服务器上的配置文件名称，比如手动输入、使用 DHCP 客户端获取、使用默认的配置文件名。除此之外，用户还可以指定某种配置文件命名规则，根据规则使用设备自身的属性（例如设备型号、MAC 地址、软件版本号）确定与指定设备对应的配置文件名称。

升级

当需要为设备增加新特性、优化原有功能或解决当前软件版本的 BUG 时，可以对设备进行升级。

设备支持以下升级方式：

- 命令行升级方式

1.2.2 通过 TFTP 命令行升级方式升级系统软件

在通过命令行升级方式升级系统软件前，需要首先搭建 TFTP 环境，PC 作为 TFTP 服务器，交换机设备作为客户端，基本要求如下：

- 将 TFTP 服务器网口和交换机接口用网线连接，交换机设备默认 IP 地址为 192.168.0.1。
- 配置 TFTP 服务器端，确保服务器处于可用状态。
- 配置 TFTP 服务器的 IP 地址，使之与设备的 IP 地址处于同一网段，使设备可以访问服务器。

通过命令行升级方式升级系统软件的步骤如下：

步骤	配置	说明
1	JX#{**tftp | tftp-ipv6 } get** {*ipv4-address | ipv6-address* } *remote-file-name* [**localfile** *local-file-name*]	通过 TFTP 协议下载系统启动软件。支持 IPv6 地址。
2	JX#**upgrade os [localfile** *local-file-name*]	升级系统软件。
3	JX#**reboot**	重新启动设备。

1.2.3 通过 FTP 命令行升级方式升级系统软件

在通过命令行升级方式升级系统软件前，需要首先搭建 FTP 环境，PC 作为 FTP 服务器，交换机设备作为客户端，基本要求如下：

- 将 FTP 服务器网口和交换机接口用网线连接，交换机设备默认 IP 地址为 192.168.0.1。
- 配置 FTP 服务器端，确保服务器处于可用状态。
- 配置 FTP 服务器的 IP 地址，使之与设备的 IP 地址处于同一网段，使设备可以访问服务器。

通过命令行升级方式升级系统软件的步骤如下：

步骤	配置	说明
1	JX#{**ftp | ftp-ipv6 } get** {*ipv4-address | ipv6-address* } *user-name user-password remote-file-name* [**localfile** *local-file-name*]	通过 FTP 协议下载系统启动软件。支持 IPv6 地址。
2	JX#**upgrade os [localfile** *local-file-name*]	升级系统软件。
3	JX#**reboot**	重新启动设备。

1.2.4 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show startup-config**	查看设备启动时加载的配置信息。
2	JX#**show running-config**	查看设备的当前配置信息。
3	JX#**show version**	查看系统的版本信息。

1.2.5 指定系统启动镜像

指定启动镜像为主或备镜像，请在设备上执行以下命令。

序号	检查项	说明
1	JX#**boot os {main | backup}**	指定系统启动镜像为主或备镜像，设置完成后下一次启动生效。仅设备支持双镜像时可选择，缺省系统从主镜像启动。

1.2.6 检查系统版本信息

查看系统版本信息，请在设备上执行以下命令查看结果。

序号	检查项	说明
1	JX#show os-package	查看系统版本信息，包括主备镜像版本信息、版本大小、编译时间等。

1.3 时间管理

1.3.1 简介

随着互联网在社会各个方面的发展和延伸，网络上多种涉及时间的应用，如网上实时交易、分布性的网络计算和处理、交通航班航路管理、数据库管理等，都需要精确、可靠的时间。

为了保证设备系统时间的精准，设备提供了完善的时间管理功能,，包括手动配置系统时间和时区、手动配置夏令时、NTP 功能以及 SNTP 功能。

时间和时区

通常情况下设备时间配置为设备所在地的实时时间，将时区配置为以格林尼治标准时间为基础的所在地时区（如中国北京在格林尼治为基准的东八区，即配置为+08:00）。

设备支持“年月日时分秒”的时间显示和时区偏移显示，可手动配置设备的时间和时区。

夏令时

夏令时（DST，Daylight Saving Time）是一种为节约资源而人为规定地方时间的制度。一般在夏季人为将时间调整提前一小时，可以使人早起早睡以减少照明量。但各个国家对夏令时的具体规定不同，所以在配置夏令时前需要考虑当地的具体情况。

设备支持配置夏令时开始的时间和结束的时间，以及调整时间的偏移量。

NTP

NTP（Network Time Protocol，网络时间协议）是用于互联网中时间同步的标准互联网协议，用于快速使网络内所有具有时钟的设备进行时钟同步。NTP 基于 UDP 进行传输，使用的端口号是 123，保证较高的精度（误差在 10ms 左右）。

NTP 基本原理如下图所示，时钟同步的工作过程如下：

步骤 1 Switch A 发送一个 NTP 消息包给 Switch B，该消息包带有离开 Switch A 时的时间戳，该时间戳为 10:00:00am，记为 t1。

步骤 2 当此 NTP 消息包到达 Switch B 时，Switch B 加上自己的时间戳，该时间戳为 11:00:01am，记为 t2。

步骤 3 当此 NTP 消息包离开 Switch B 时，Switch B 再加上自己的时间戳，该时间戳为 11:00:02am，记为 t3。

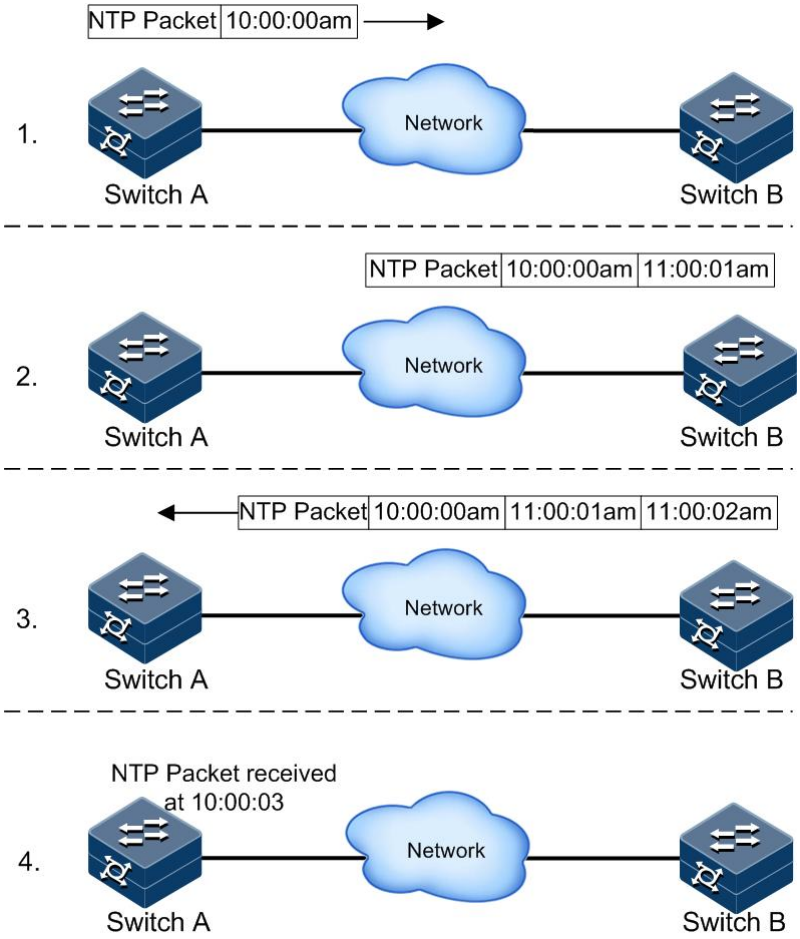
步骤 4 当 Switch A 接收到该响应消息包时，加上一个新的时间戳，该时间戳为 10:00:03am，记为 t4。

至此，Switch A 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)。
- Switch A 和 Switch B 之间的时间差：Offset=((t2-t1)+(t3-t4))/2。

Switch A 根据这些信息来设定自己的时钟，实现与 Switch B 的时钟同步。

图 1-5 NTP 基本原理



NTP 支持多种工作模式进行时间同步：

- 服务器/客户端模式

在服务器/客户端模式中，客户端向不同的服务器发送时钟同步报文。服务器收到报文后会发送应答报文。客户端收到应答报文后，进行时钟过滤和选择，并同步到优选的服务器。

在该模式下，客户端仅能同步服务器的时间，而服务器无法同步客户端的时间。设备不能既作为客户端又作为服务器。

- 对等体模式

在对等体模式中，配置对等体的设备可以向层级高的设备或者服务器进行对时。

已配置 NTP 服务器的设备不能再配置对等体。

SNTP

SNTP（Simple Network Time Protocol，简单网络时间协议）将设备系统时间同步为格林尼治时间，然后根据系统时区的设置来转化成本地时间。当 SNTP 客户端与服务器不在同一地区时，SNTP 客户端同步的时间为格林威治时间，然后根据系统时区的设置来转化成本地时间。

SNTP 客户端获取时间有两种方式，即主动发送请求报文和被动监听报文，通过不同模式实现：

- 单播模式：SNTP 客户端主动发送请求报文。指定设备的 SNTP 单播服务器地址后，设备将每隔 10s 尝试一次从 SNTP 服务器获取时钟信息，并且每次从 SNTP 服务器获取时钟信息的最大超时时间为 3 秒。
- 组播或广播模式：SNTP 客户端被动监听报文。
  - 配置 SNTP 客户端为组播模式后，设备将时刻监听组播地址 224.0.1.1，从 SNTP 组播服务器获取时钟信息，并且每次从 SNTP 获取时钟信息的最大超时时间为服务器发送周期的 1.5 倍。
  - 配置 SNTP 客户端为广播模式后，设备将时刻监听广播地址 255.255.255.255，从 SNTP 广播服务器获取时钟信息，并且每次从 SNTP 获取时钟信息的最大超时时间为服务器发送周期的 1.5 倍。

1.3.2 配置准备

场景

配置设备的系统时间，保证系统时间的精准。

- 无论何时，手动配置时间和时区立即生效。
- 开启 NTP 或 SNTP 功能，经过同步周期后，设备同步到的时间会实时刷新，覆盖当前系统时间。
- NTP 功能与 SNTP 功能互斥，不能同时配置。

前提

无

NTP

设备上 NTP 的缺省配置如下。

功能	缺省值
设备是否作为 NTP 主时钟	否
全局 NTP 服务器	无
全局 NTP 对等体	无
参考时钟源	0.0.0.0
身份验证功能	关闭
身份验证密钥 ID	无
可信密钥	无

SNTP

设备上 SNTP 的缺省配置如下。

功能	缺省值
SNTP 服务器地址	无

1.3.3 配置 NTP

配置 NTP 基本功能

请在设备上进行以下配置。

注意

NTP 功能和 SNTP 功能互斥，二者不能同时使用。

步骤	配置	说明
1	`JX#configure`	进入全局配置模式。
2	`JX(config)#ntp client update-interval { interval | default }`	配置 ntp client 通告时间 interval：通告间隔时间 范围 4-17 秒 缺省为 6 秒
3	`JX(config)#ntp server broadcast-interval { interval | default }`	配置 ntp server 通告时间 interval：通告间隔时间 范围 4-17 秒 缺省为 6 秒

步骤	配置	说明
4	JX(config)#**ntp master**	指定为主时钟
5	JX(config)#**ntp stratum** *value*	配置系统时钟的层数 value：层数 范围 1-15 缺省为 16
6	JX(config)#**ntp unicast-peer** *peer-ipv4* { **version** *version-id* | **authentication-keyid** *key-value* | **vpn** *vpn-name* | **port** *port-id* }	配置指定 ipv4 对等体 peer-ipv4：对等体 ipv4 地址 version-id：ntp 版本号 key-value：使用的认证索引 vpn-name：vpn 名称 port-id：使用的 udp 端口号
7	JX(config)#**ntp unicast-server** sserver-*ipv4* { **version** *version-id* | **authentication-keyid** *key-value* | **vpn** *vpn-name* | **port** *port-id* }	配置指定 ipv4 服务器 server-ipv4：服务器 ipv4 地址 version-id：ntp 版本号 key-value：使用的认证索引 vpn-name：vpn 名称 port-id：使用的 udp 端口号

说明

如果设备被配置为 NTP 参考时钟源，则无法配置 NTP 服务器或 NTP 对等体；反之亦然，如果配置了 NTP 服务器或对等体，则无法将设备配置为 NTP 参考时钟源。

配置 NTP 身份验证功能

在对安全性要求较高的网络中，使用 NTP 协议时需要进行身份验证。NTP 客户端使能身份验证功能后只与通过验证的服务器进行同步，保证了网络的安全性。NTP 客户端只有使能了身份验证功能才会对服务器进行验证，若未使能身份验证功能，即使服务器携带密钥信息，客户端也不会进行验证，直接与服务器进行时间同步。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**ntp authentication** { **enable** | **disable** }	（可选）ntp 认证全局使能 enable：使能 diabale：去使能。

步骤	配置	说明
3	JX(config)#**ntp authentication-keyid** *key-value* **md5 key** { **cipher** | **plain** } *string*	（可选）添加 ntp 验证密钥 key-value：密钥索引值 cipher：密文 plain：明文 STRING：密钥字符串
4	JX(config)#**ntp trusted-keyid** *key-value* **enable**	（可选）指定已创建的密钥是可信的 key-value：密钥索引值

1.3.4 配置 SNTP

配置 SNTP 客户端功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config-sntp)#**sntp client update-interval** <4-17>	配置 sntp client 通告时间。
3	JX(config-sntp)#**sntp server broadcast-interval** <4-17>	配置 sntp server 通告时间
4	JX(config-sntp)#**sntp authentication** { **enable** | **disable** }	SNTP 认证全局使能
5	JX(config-sntp)#**sntp authentication-keyid** <1-4294967295> **md5 key string**	添加 SNTP 验证密钥
6	JX(config-sntp)#**sntp master**	指定为主时钟
7	JX(config-sntp } **sntp stratum <1-15>**	配置系统时钟的层数
8	JX(config-sntp)#**sntp trusted-keyid** <1-4294967295>	指定已创建的密钥是可信的
9	JX(config-sntp)#**sntp unicast-peer** { **A.B.C.D** } JX(config-sntp)#**sntp unicast-peer** { **A.B.C.D** } **version** { **3** | **4** } JX(config-sntp)#**sntp unicast-peer** { **A.B.C.D** } **version** { **3** | **4** } **authentication-keyid** <1-4294967295> JX(config-sntp)#**sntp unicast-peer** { **A.B.C.D** } **authentication-keyid** <1-4294967295>	为设备指定 IPv4 对等体

步骤	配置	说明
10	JX(config-sntp)# **sntp unicast-server { A.B.C.D }** JX(config-sntp)#**sntp unicast-server { A.B.C.D } version { 3 | 4 }** JX(config-sntp)#**sntp unicast-server { A.B.C.D } version { 3 | 4 } authentication-keyid** <1-4294967295> JX(config-sntp)#**sntp unicast-server { A.B.C.D } authentication-keyid** <1-4294967295>	为设备指定单播 IPv4 SNTP 服务器

1.3.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show ntp information**	显示 ntp 本地信息
2	JX#**show ntp peer**	显示 ntp 对端信息
3	JX#**show ntp key**	显示 ntp 密钥信息
4	JX#**show ntp session**	显示 ntp 会话信息
5	JX#**show sntp**	显示 sntp 全局配置
6	JX#**show sntp service**	显示 sntp 业务配置
7	JX#**show sntp service verbose**	显示 sntp 业务详细配置

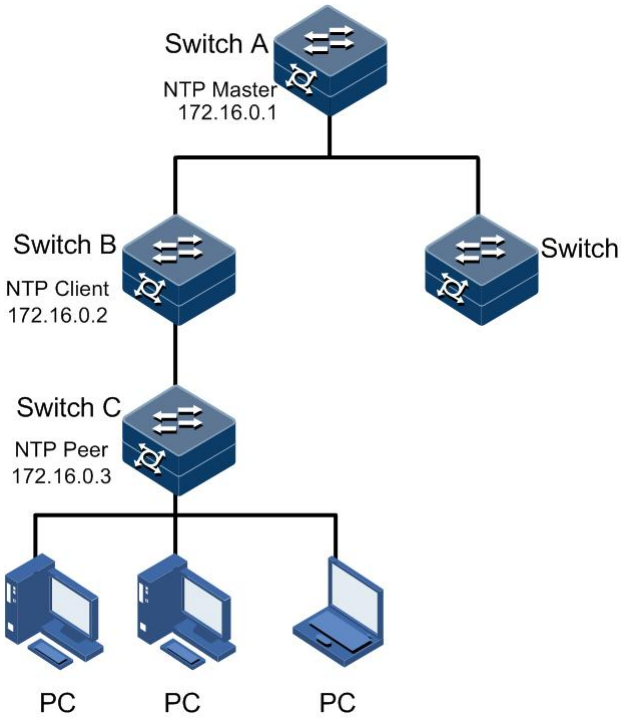
1.3.6 配置 NTP 功能示例

组网需求

某公司搭建稳定的时钟同步系统，使公司内部设备保持系统时间的一致和精准。基本规划为：

- Switch A 作为时钟同步系统的主时钟。
- Switch B 作为时钟同步系统的客户端，需设置上层的 Switch A 为 NTP 服务器。
- 设置 Switch C 为 Switch B 的 NTP 对等体，接收 Switch B 发出的下行同步数据流。

图 1-6 NTP 组网示意图



配置步骤

步骤 1 配置 Switch A。

```
JX#hostname SwitchA
SwitchA#config
SwitchA(config)#ntp
SwitchA(config-ntp)#master
SwitchA(config-ntp)#ntp stratum 2
```

步骤 2 配置 Switch B。

```
JX#hostname SwitchB
SwitchB#config
SwitchB(config)#ntp
SwitchB(config-ntp)#ntp unicast-server 172.16.0.1
SwitchB(config-ntp)#ntp unicast-peer 172.16.0.3
SwitchB(config-ntp)#ntp stratum 3
```

步骤 3 配置 Switch C

```
JX#hostname SwitchC
SwitchC#config
SwitchC(config)#ntp
SwitchC(config-ntp)#ntp unicast-peer 172.16.0.2
SwitchC(config-ntp)#ntp stratum 4
```

检查结果

- 查看 Switch A。

通过 **show ntp** 查看 Switch A 配置是否正确。

```
SwitchA#show ntp
```

- 查看 Switch B。

通过 **show ntp** 查看 Switch B 配置是否正确。

```
SwitchB#show ntp
```

通过 **show ntp service** 查看 Switch B 的 NTP 会话信息。

```
SwitchB#show ntp service
```

- 查看 Switch C。

通过 **show ntp** 查看 Switch C 配置是否正确。

```
JX#show ntp
```

通过 **show ntp service** 查看 Switch C 的 NTP 会话信息。

```
JX#show ntp service
```

1.4 接口管理

1.4.1 简介

以太网接口

以太网以其高度灵活、相对简单、易于实现的特点，成为重要的局域网组网技术。以太网接口分为：以太网电接口和以太网光接口。

交换机设备支持以太网电接口和以太网光接口。

- 自协商功能

自动协商的主要功能就是使物理链路两端的设备通过交互信息自动选择同样的工作参数。自动协商的内容主要包括双工模式、运行速率等参数。一旦协商通过，链路两端的设备就锁定在同样的双工模式和运行速率。

- 连接线缆

一般以太网标准网线分为直通线 MDI（Medium Dependent Interface）和交叉线 MDI-X（Medium Dependent Interface cross-over）两种。MDI 提供终端到网络中继设备的物理和电路连接。MDI-X 提供同种设备（终端到终端）的连接。主机和路由器的接口类型为 MDI，集线器和交换机的端口类型为 MDI-X。一般情况下，异类设备互连用直通线，同类设备互连用交叉线。自适应连接则无需考虑直通线或交叉线。

设备以太网线连接支持自适应 MDI/MDI-X。

VLAN 接口

VLAN 接口是一种逻辑接口，用于实现 VLAN 间的三层互通。每个 VLAN 对应一个 VLAN 接口，在为 VLAN 接口配置了 IP 地址后，该接口即可作

为本 VLAN 内网络设备的网关，实现跨网段的报文进行基于 IP 地址的三层转发。

LoopBack 接口

LoopBack 接口是一种逻辑虚拟接口，由于该接口物理层状态和链路层协议始终处于 Up 状态，稳定性强，因此可以配置 IP 地址，并常用于动态路由协议中，作为设备的 Router ID。

NULL 接口

NULL 接口是一种逻辑虚拟接口，永远处于 Up 状态，但不能转发报文，也不能配置 IP 地址和链路层协议。NULL 接口可以对报文进行过滤，将不需要的网络流量发送到 NULL 接口，免去配置 ACL 的复杂操作。例如，在路由协议中指定到达某一网段的下一跳为 NULL 接口，则任何发送到该网段的网络数据报文都会被丢弃。

1.4.2 接口的缺省配置

设备上物理层接口的缺省配置如下。

功能	缺省值
接口的双工模式	自协商
接口的速率	自协商
接口速率统计功能状态	打开
接口的流控功能状态	禁止
接口状态	打开

1.4.3 配置接口基本属性

当互连的两个设备的接口属性，如 MTU（Maximum Transfered Unit，最大传输单元）、双工模式、速率等参数不一致时，会造成设备间无法正常通信，此时需要调整接口的属性使两端设备互相匹配。

以太网物理层分为半双工、全双工和自协商三种工作模式。

- 半双工在任意时刻只能接收或发送报文。
- 全双工在任意时刻可以同时接收和发送报文。
- 自协商是指链路两端的设备通过交互信息自动选择双工模式，一旦协商通过，两端的设备就使用同样的双工模式进行报文传输。

请在设备上进行以下配置。

步骤	配置	说明
1	`JX#config`	进入全局配置模式。

步骤	配置	说明
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/1)#**description** *string*	配置接口的描述信息
4	JX(config-ge-1/0/1)#**mtu** *max-frame-length*	配置接口的最大传输单元
5	JX(config-ge-1/0/1)#**negotiation auto { enable | disable }**	配置接口自协商功能使能或关闭
6	JX(config-ge-1/0/1)#**duplex { full | half | default}**	配置接口的双工模式。 需要先去使能接口自协商
7	JX(config-ge-1/0/1)#**speed { 10 | 100 | 1000 | default}**	配置接口的速率。 对于光接口而言，接口的速率还取决于光模块的规格。
8	JX(config-ge-1/0/1)#**transceiver type { 1000BASE-T | 1000BASE-X | 100GBASE-COPPER | 100GBASE-FIBER | 10GBASE-COPPER | 10GBASE-FIBER }**	配置 SFP 接口连接模式。
9	JX(config-ge-1/0/1)#**port up-hold-time** *delay-time-value*	配置端口状态变化为 UP 时延迟处理时间
10	JX(config-ge-1/0/1)#**port down-hold-time** *delay-time-value*	配置端口状态变化为 DOWN 时延迟处理时间。

1.4.4 配置接口信息统计功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**flow-statistic interval** *time-value*	配置全局接口信息统计周期。 缺省对所有接口生效，具体接口可以配置相应命令覆盖全局
3	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
4	JX(config-ge-1/0/1)#**port flow-statistic interval** *time-value*	配置接口信息统计周期。 该配置覆盖全局的接口信息统计周期配置
5	JX(config-ge-1/0/1)#**reset statistics**	清除接口的统计信息。

1.4.5 配置接口流控功能

IEEE802.3x 是全双工以太网数据链路层的流量控制方法。当客户端向服务器发出请求后，自身系统或网络产生拥塞时，客户端会向服务器发出 PAUSE 帧，以延缓服务器向客户端的数据传输。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/1)#**flow-control { enable| disable }**	配置接口流控功能使能或关闭
4	JX#**show interface** *interface-type interface-number*	查询接口详细信息，查看流控功能使能状态。

1.4.6 配置接口打开或关闭

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式/VLAN 接口配置模式/链路聚合接口配置模式。
3	JX(config-ge-1/0/1)#**shutdown**	关闭当前接口。 可以使用 **no shutdown** 命令再次打开接口。

1.4.7 配置接口允许通过的 tagged 报文类型

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式/链路聚合接口配置模式。
3	JX(config-ge-1/0/1)#**accept-frame-type { all | only-tagged }**	all：配置接口 tagged 和 untagged 报文通过。 only-tagged:配置接口只允许 tagged 报文通过。 缺省是 all。

1.4.8 配置管理报文优先级

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式
3	JX(config-vlanif-*)#**packet-priority 8021p** *value*	配置报文优先级。
4	JX(config-vlanif-*)#**no packet-priority 8021p**	恢复报文缺省优先级

1.4.9 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show interface**	查看接口列表概要信息。
2	JX#**show interface verbose**	查看接口列表详细信息。
3	JX#**show interface** *interface-type interface-number*	查看具体接口的详细信息
4	JX#**show interface** [*interface-type interface-number*] **config**	查看接口配置信息。