.doc in alpha 豆丁

特别说明

此资料来自豆丁网(http://www.docin.com/)

您现在所看到的文档是使用**下载器**所生成的文档

此文档的原件位于

http://www.docin.com/p-1333347.html

感谢您的支持

抱米花

http://blog.sina.com.cn/lotusbaob

.doc in alpha 豆丁

1 VLAN 基本原理

虚拟局域网(Virtual LAN)是由一组连接在交换机上的终端计算机和连接交换机的干道(Trunk)构成的。VLAN 通常对应于单个网络或者子网，具有物理 LAN 一样的属性。从应用的角度看，VLAN 中的终端计算机一般具有相同的需求，它们又可能在地理位置上是分散的，但相互之间就像连接在同一条线路上一样。

在配置上，可以把不同交换机连接的计算机划到同一 VLAN 中，也可以把同一交换机端口上的计算机划分到不同的 VLAN 中。借助于 VLAN，可以控制广播域的大小，并把通信限制在 VLAN 的范围内。

1.1 VLAN 的基本原理

交换机的端口可以运行在接入方式(Access Mode)或干道模式(Trunk Mode)，对应端口所连接的链路分别被叫做接入链路和 Trunk 链路。

接入模式的端口(接入端口——Access Port)用于连接终端设备，如客户机和服务器等，这种端口仅属于一个 VLAN。接入链路上传输的是普通的以太帧。干道(Trunks)是一条点到点链路，用于连接两台交换机，一台交换机和路由器或者服务器(需要特殊的适配卡)，负责在同一个 Trunk 链路上传输多个 VLAN 的通信(采用复用方式)。连接 Trunk 链路的交换机端口通常是交换机上具有最大带宽的端口。Trunk 链路是多个 VLAN 的公用通道，采用 Trunk 链路可以把 VLAN 扩展到整个网络的范围。

要在 Trunk 链路中传输多个 VLAN 的通信，就需要能区分帧所属的 VLAN，这可以通过专门的协议对帧进行封装，或者在帧中加入标记(Tag)来实现。ISL 是一种专用协议，支持 Cisco 设备之间的 Trunk 链路。而 IEEE 802.1Q 是一种标准协议，可以支持不同厂商设备的 Trunk 链路。

VLAN 的工作原理

在图(P116)中，端口 A 和端口 B 是接入端口，同属于一个 VLAN(VLAN 200)，它们不能接收来自其它 VLAN 的帧。交换机 Y 接收到端口 A 发往端口 B 的帧时，不会对帧进行 Trunking 协议封装，而直接把其转发到端口 B。

图中的端口 C 是 VLAN 200 的一个成员。端口 A 发往端口 C 的帧是按下列方式处理的：

- 交换机 Y 接收端口 A 的帧，通过端口号与 VLAN 的关联识别出是发往 VLAN 200 的通信；
- 交换机 Y 用标识为 VLAN 200 的 ISL 对帧进行封装，然后通过 Trunk 链路把此帧发送到中间交换机；
- 中间交换机重复上述步骤，直到帧最后抵达交换机 Z；
- 交换机 Z 对 Trunking 协议帧进行拆封，去除 ISL 头，并转发到端口 C。

1.2 VLAN 的技术特点

什么是 VLAN

灵活性

安全性

广播控制

提高带宽利用率

减少延迟

1.3 不同的 Trunking 技术

Trunking 技术有多种，分别是交换机间链路 ISL(Inter-Switch Link)、IEEE 802.1Q、IEEE 802.10 和 ATM LANE(LAN 仿真)。ISL 是 Cisco 专用的封装协议(Cisco IOS 11.1 版本开始支持)，用于交换机之间的 Trunking。这种协议在帧的前面增加了 26 字节的头部，在帧的末尾增加了 4 字节的 CRC 校验码。之中技术支持快速以太网和吉比特以台网。IEEE 802.1Q 采用帧标记(Frame Tagging)或者内部标记(Internal Tagging)的方式，也就是通过插在帧头的 VLAN 标识标明 VLAN。IEEE 802.10 提供了使用 FDDI 帧传输 VLAN 信息的方法。它把 VLAN 信息写在 802.10 帧的安全联盟标识符(SAID-Security Association Identifier)中，支持跨越 FDDI 骨干传输 VLAN 信息。ATM LANE 标准是一项 ATM 论坛标准，用于在 ATM 网络中支持 VLAN。

1．交换机间链路

ISL 协议在以太帧的前面增加了 26 字节的 ISL 头部，在以太帧的最后增加了 4 字节的 CRC 校验码。ISL header 中包含 10 比特的 VLAN ID。

26B ISL header	DA	SA	T/L	DATA	FCS	4B CRC

26 字节的 ISL 头部如下：

40	4	4	48	16	24	24	15	1	16	16	可变长度	32
DA	Type	User	SA	LEN	SNAP/LLC	HSA	VLAN ID	BPDU/CDP	Index	保留	被封装的帧	FCS(CRC)

各字段的说明如下：

标志	说明
DA	组播地址：0x01-00-0c-00-00，向接收交换机说明这是一个 ISL 封装的帧
Type	标明数据帧的类型，0000-以太网，0001-令牌环，0010-FDDI，0011-ATM
User	其值通常为 0。可以在特殊情况下用于令牌环传输
SA	发送帧的交换机的 802.3 MAC 地址
LEN	标识用户数据和 ISL 帧头的总长度(从 DA 到 ISL 的 CRC 字段)
SNAP/LLC	固定值 0XAA-AA-03
HAS	复制的 ISL SA 字段的高位部分
VLAN ID	标识用户帧所属的 VLAN 号(只用了 10 比特)
BPDU/CDP	为 1 时表示接收交换机应立刻对此帧进行检查(因为是生成树、ISL、VTP 或 CDP 数据)
Index	标识数据帧来自源交换机的哪个端口
保留	令牌环和 FDDI 帧中的特殊信息(如访问控制字段 AC、帧复制字段 FC)用此字段传输。对以太网，此字段值为 0
被封装的帧	原始的用户帧，包括原始帧中的 FCS
FCS(CRC)	ISL 帧的 CRC 校验码，不会取代用户帧的 FCS

可以使用 show port capabilities 命令查看交换机和路由器支持何种 Trunking。

2. IEEE 802.1Q

IEEE 802.1Q 标准的名称是虚拟桥接局域网标准(Standard for Virtual Bridged Local-Area Network)。该标准支持不同厂家的 VLAN 复用一个网段。

该标准采用的是内部标记机制，即在数据帧中插入 4 字节的标记，并重新计算帧校验序列。

IEEE 802.1Q 帧的格式如下：

					802.1Q 标记(4B)					
PRE	SF	DA	SA	TPI	P	C	VI	L/T	DATA	FCS
					802.1p(3b)					

各字段含义如下：

标志	说明
PRE	前导码，用于同步
SF	起始定界符，标志帧的开始
DA	目的 802.3 MAC 地址
SA	源 802.3 MAC 地址
TPI	标记协议标识符(2B)，以太网为 0x8100(802.3ab 格式)
P	802.1p 优先级，从 0 到 7(7 的优先级最高)
C	规范形式标记符(1b)，说明 MAC 地址是否用规范形式表示。以太网为 0
VI	VLAN 标识符(12b)，表示帧所属的 VLAN 号(取值范围从 0~4095)
L/T	标准的以太帧字段
DATA	用户数据(不超过 1500B)
FCS	帧校验序列

802.1p 依赖 802.1Q 标记机制进行 2 层通信的优先级划分。1998 年通过的 802.3ab 标准把普通的 802.3 帧的最大长度扩展为 1522B，以便容纳附加的 VLAN 标记头部。

3. IEEE 802.10

多个 VLAN 可以复用支持 IEEE 802.10 协议的 FDDI 骨干。支持 802.10 的 FDDI 接口根据 VLAN 标识有选择地对帧进行转发。VLAN 标识是用户可配置的 4 字节 IEEE 802.10 安全联盟标识(SAID)，用于标识帧所属的 VLAN。

4. ATM LANE(LAN 仿真)

LANE 协议使得可以在 ATM 网络上仿真 LAN，也就是使 ATM 所连接的设备可以按以太网或者令牌环网的方式运行。

LANE 定义了一个供网络层协议使用的接口，并且与现有的 LAN 保持一致。数据通过 ATM 网络传输时，会被封装成适当的 LAN MAC 格式。

仿真局域网(ELAN-Emulated LAN)是一个在交换机上实现的逻辑结构，支持 LANE 网络内一组主机之间的 2 层通信。同一个 ATM 网络中可以运行一个或多个 ELAN。然而，ELAN 之间是相互独立的，不同的 ELAN 内的用户不能直接通信。与 VLAN 一样，ELAN 之间只能通过 3 层

设备通信。

由于 ELAN 提供了类似 VLAN 的通信机制，可以看作是一个广播域。这使得可以在使用不同 VLAN 复用技术(ISL、802.10 等)的 2 层交换机上进行 ELAN 到 VLAN 的映射。支持 3 层的设备也可以把 IP 子网映射为 ELAN，并在 ELAN 之间进行路由选择。

LANE 不仿真特定 LAN 的接入方式(CSMA/CD 或 Token Ring)，也使得不需要对高层协议进行任何修改就可以在 ATM 网络中运行。由于 LANE 向网络层驱动程序提供和现有的 MAC 协议相同的服务接口，网络层驱动程序也不需要做修改。

但是，需要在 ATM 交换机、路由器或者 ATM 客户机上部署专用的下层软件——LAN 仿真客户端 LEC(LAN Emulation Client)。这个客户端软件能够与被叫做 LAN 仿真服务器 LES(LAN Emulation Server)的中央控制点进行通信。一个广播未知服务器 BUS(Broadcast and Unknown Server)作为中央点分发广播和组播信息。LAN 仿真配置服务器 LECS(LAN Emulation Configuration Server)中保存了关于 LEC 和其所属的 ELAN 的数据库(LECS 和 BUS 必须在同一台设备上)。

1.4 VLAN Trunking 协议

VLAN 干道协议 VTP(VLAN Trunking Protocol)是 Cisco 的专用协议。利用 VTP 可以提高管理效率，使得不需要在每台交换机上配置相同的 VLAN 信息；VTP 提供的映射方案可以实现以太网 VLAN 到 ATM LANE ELAN 或 FDDI 802.10 VLAN 的映射，使通信流跨越混合介质骨干进行传输。

1. VTP 的基本机制

VTP 是 2 层协议，该协议可以管理 VLAN 的增加、删除和重命名，实现 VLAN 配置的一致性，减少配置错误。可以用 VTP 管理网络中的 VLAN1~VLAN1005(VTP 不支持 Catalyst 6000 上的 VLAN 1025~VLAN 4094)。利用 VTP，可以集中在一台交换机上对配置进行变更，变更的结果会自动传送到网络中的所有其它交换机(这些交换机必须处于同一个域)。

- VTP 通过发送组播(MAC 地址为 01-00-0c-cc-cc-cc)消息(Messages)进行工作。
- VTP 通告(Advertisements)只通过 Trunk 端口传送。
- VTP 消息(Messages)在 VLAN1 中传送；因此，VLAN1 不能从 Trunk 中去除。即使使用“在 Trunk 上停用 VLAN1(VLAN1 disable on trunk)”功能把 VLAN1 从 Trunk 上修剪掉(例如，命令 clear trunk 2/1 1 可以在 Trunk 端口 2/1 上停用 VLAN1)，也只是阻断该 Trunk 上的用户数据，控制协议数据(DTP、Pagp、CDP、VTP 等)仍可以传送。使用修剪功能，可以避免把 VLAN 扩展到整个园区网络，使 STP 环路限制在 VLAN1 的范围。
- 只有在经过 DTP 自动协商且启动了 Trunk 时，VTP 信息才可以在 802.1Trunk 上传送。

VTP 域内的各交换机定期地在每个 Trunk 上利用保留的 VTP 组播地址发送通告。邻接的交换机接收通告，并根据需要更新自己的 VTP 和 VLAN 配置。

2. VTP 域

VTP 域(VTP Domain)也叫做 VLAN 管理域(VLAN Management Domain)，由一个以上通过 Trunk 连接且共享 VTP 域名的交换机组成。

一台交换机只能属于一个 VTP 域。缺省情况下，交换机处于 VTP 服务器模式，不属于任何管理域。交换机通过 Trunk 链路收到关于域的通告，或者在交换机上配置 VLAN 管理域之后，交换机才会属于一个 VLAN 域。而且，只有在指定或者交换机自学习到管理域的名称后，才能在

VTP 服务器上创建或者更改 VLAN。

每个 VTP 设备都会记录自己的 VTP 配置修改编号。32 位的 VTP 配置修改编号标识 VTP 配置的修改版本，其取值范围为 0~4294947295。每修改一次，配置修改编号就加 1；当达到 4294947295 时再修改配置，VTP 配置修改编号将再次从 0 开始循环。VTP 数据包包含发送设备的 VTP 配置修改编号。接收设备通过 VTP 配置修改编号判断接收到的信息是否比当前的信息更新。

在 VTP 服务器上发生的 VTP 配置变更，会被传播到 VTP 域内的所有交换机。VTP 通告在在所有的 Trunk 链路上传播，包括 ISL、IEEE 802.1Q、IEEE 802.10 和 ATM LANE。交换机在 Trunk 链路上收到 VTP 通告，就会继承管理域的名称和 VTP 配置修改编号。通告中的管理域名称与当前的名称不同，或者配置修改编号版本低，交换机会忽略这样的通告。

VTP 信息会在 VLAN 管理域内保持。要使用 VTP，就必须为每台交换机指定 VTP 域名。

为了保证 VTP 域的连通性，VTP 域的必须同时满足下列要求。

- 域内的所有交换机必须使用相同的域名(不管是通过配置还是自学习方式)
- VTP 域内的所有交换机连接成树形结构
- 所有的交换机必须启动 Trunking

3. 交换机的 VTP 工作模式

交换机可以工作在服务器模式、客户机模式、透明模式或关闭模式。

(1) 服务器(Server)模式

VTP 服务器维护着 VTP 域内所有 VLAN 的完整列表。在 VTP 服务器模式下，可以创建、修改和删除 VLAN，为整个 VTP 域指定其它的配置参数(如 VTP 版本和 VTP 修剪等)。VTP 服务器会把自己的 VLAN 配置通告给相同 VTP 域内的其它交换机，并利用从 Trunk 链路上收到的通告实现与其它交换机之间 VLAN 配置的同步。VTP 信息存储在 NVRAM(非易失随机存取存储器)中。所有 Cisco 交换机的缺省模式是服务器模式。

(2) 客户机(Client)模式

VTP 客户机中也维持着 VTP 域内所有 VLAN 的列表。但是，这些信息没有存放在 NVRAM 中。VTP 客户机与 VTP 服务器工作方式相同，但不支持创建、修改和删除 VLAN；任何更改都是通过 VTP 服务器通告实现的。

(3) 透明(Transparent)模式

透明模式的交换机不会加入 VTP，不会通告自己的 VLAN 配置，也不会根据接收到的通告同步自己的 VLAN 配置。但是，透明模式的交换机会在 Trunk 端口上转发接收到的 VTP 通告。在透明模式的交换机上配置 VLAN，其配置信息只在本地有效(保存在 NVRAM 中)。

(4) 关闭(Off)模式

VTP Off 模式与 VTP 透明模式类似，但交换机不转发 VTP 通告。

不同的 VTP 模式如何处理 VTP 信息见下表。

功能	服务器	客户机	透明
提供 VTP 信息	Yes	Yes	No
监听 VTP 信息	Yes	Yes	No
创建 VLAN	Yes	No	Yes(仅本地有效)
记住 VLAN	Yes	No	Yes(仅本地有效)

表中的“提供 VTP 信息”是指在所有的 Trunk 上发送 VTP 信息，“监听 VTP 信息”指监听 MAC 地址为 01-00-0c-cc-cc-cc 的组播帧并处理 VTP 更新。

服务器和客户机在发送和监听 VTP 消息方面没有差别，区别仅在于，不能在客户机上直接配置 VLAN，并且在重新启动后，客户机不能记住 VLAN 信息(没有写入 NVRAM)。

透明模式的交换机不参加到 VTP 中，此类交换机只通过所有的 Trunk 转发所有的 VTP 消息，而不做其它处理。

4．VTP 通告

VTP 通告负责在 VTP 域的各成员之间传送 VTP 信息。

(1) VTP 通告(Advertisements)的内容

周期性的 VTP 通告(Advertisements)会使用组播地址(01-00-0c-cc-cc-cc)通过 Trunk 端口发送。该通告包含下列配置信息。

- VLAN ID(ISL 和 802.1Q)
- 仿真 LAN 名称(ATM LANE)
- 802.10 SAID 值(FDDI)
- VTP 域名
- VTP 配置修改编号
- VLAN 配置，包括 MTU
- 帧格式

(2) 发送 VTP 消息时，以太网帧各字段的取值

VTP 消息封装在 ISL 帧或者 IEEE 802.1Q 帧内。发送 VTP 消息时，以太网帧各字段的取值如下：

- DA 取组播地址：01-00-0c-cc-cc-cc
- LLC 中的 DSAP 和 SSAP 取值都为 0xAA
- 子网访问协议 SNAP(Subnetwork Access Protocol)头部中的组织惟一标识 OUI(Oaganizationnal Unique Identifier)取值为 00-00-0c(表示是 Cisco)
- SNAP 头部中的以太网类型为 2003

(3) ISL VTP 数据包

ISL 和 802.1Q 协议都可以封装 VTP 消息。下面给出的是 ISL 封装。

ISL 头部	以太网头部	LLC 头部	SNAP 头部	VTP 头部	VTP 消息	CRC
26B	14B	3B	3B	变长		

VTP 头部的格式取决于 VTP 消息的类型，但是，所有数据包头部都包含下列字段

- VTP 协议版本：1 或 2
- VTP 消息类型
- 管理域长度
- 管理域名称

(4) VTP 消息类型

- 汇总通告(Summary Advertisements)

该消息用于向邻接的交换机广播目前的 VTP 域名和配置修改编号(缺省时每 5 分钟发送一次)。汇总通告的格式如下。

VTP 版本	消息类型	后续通告数	管理域名长度

管理域名(不足 32 字节用 0 填充)
配置修改编号
更新者标识
更新时间戳(12 字节)
MD5 摘要(16 字节)

VTP 版本：1 或 2

消息类型：0x01，标识汇总通告

后续通告数：跟随在汇总通告后的子网通告个数，取值范围为 0~255(0 表示没有子网通告)

管理域名长度：VTP 域名的长度

管理域名：VTP 域名

更新者标识：最近发生配置修改编号变化的交换机的 IP 地址

更新时间戳：最近发生配置修改编号变化的日期和时间

MD5 摘要：VTP 头部和 VTP 口令的哈希函数值

MD5 原理——

MD5 是 1991 年由 Ronald Rivest 构造的一种单向的哈希函数，RFC 1321 给出了其详细的算法。

哈希函数从文本中取出字节片，把其转换为 128 比特的数字串。这个数字串叫做哈希值或消息摘要(Message Digest),可以用来标识特定的文本。哈希值是由文本串产生的数字，其数据量比文本自身要小的多。哈希函数的算法使得不同文本产生相同函数值的可能性非常少。

发送者使用单向哈希函数，根据数据文本和发送者的密码产生 128 比特的消息摘要，随同数据一起发送。接收者根据同一数据文本和自己的密码重新计算哈希值。如果帧中的消息摘要与接收者的计算得到的消息摘要不一致，就认为收发双方的密码不匹配，数据面临安全威胁。

- 子网通告(Subset Advertisements)

在 VTP 服务器上增加、删除或者修改了 VLAN，就会引起配置修改编号增加，导致交换机首先发送一个汇总通告，然后发送一个或多个子网通告。而挂起、激活某个 VLAN，改变 VLAN 的名称或者 MTU，会触发子网通告。子网通告中包含 VLAN 列表和相应 VLAN 的信息。如果 VLAN 较多，可能需要发送多个子网通告。

子网通告的格式如下。

VTP 版本	消息类型	序号	管理域名长度
管理域名(不足 32 字节用 0 填充)			
配置修改编号			
VLAN 信息 1			
VLAN 信息 2			
……			
VLAN 信息 n			

消息类型：0x02，标识子网通告

序号：该子网通告在本次子网通告序列中的编号，取值从 1 开始

VLAN 信息：子网通告列出了各个 VLAN(包括缺省 VLAN)的下列信息

VLAN 活动状态——活动(Active)或者挂起(Suspended)
VLAN 类型——以太网，令牌环，FDDI 或其它类型
VLAN 名长度
ISL VLAN-ID
MTU
802.10 索引——SAID(通过 FDDI Trunk 时使用)
VLAN 名称

- 通告请求(Advertisement Requests)

在下列情况下，交换机会发出通告请求：

交换机重新启动时
VTP 域名变更时
交换机收到了比自己的配置修改编号高的汇总通告时

收到通告请求，VTP 设备就会发送汇总通告，然后发送一个或多个子网通告
通告请求的格式如下：

VTP 版本	消息类型	Rsvd	管理域名长度
管理域名(不足 32 字节用 0 填充)			
起始值			

消息类型：0x03，标识通告请求
Rsvd：保留，通常为 0
起始值：当该值为 n 时，是要求重传从 n 开始的子网通告

- VTP 加入消息(VTP Join Messages)——资料缺

5. VTP 修剪

VTP 确保了 VTP 域内的交换机可以了解所有的 VLAN 配置，但 VLAN 中的所有组播、广播和目的地址未知的单播会在此广播域内的所有端口(包括 Trunk 端口)进行洪泛。VTP 修剪功能可以动态地去除这些不必要的 VLAN 通信——未知地址单播和广播洪泛。

1.5 生成树协议 STP(Spanning Tree Protocol)

STP 协议是 2 层协议，其作用是通过一种专用的算法发现网络中交换机之间的物理环路，并构建一个逻辑的树形拓扑结构。

通过环路可以提供冗余，提高可靠性，但如果配置不当，就会引起网络灾难。

1.5.1 STP 机制的引入

一、广播环路

网络中存在物理环路(网桥/交换机之间的环路)，2 层广播帧(MAC 地址为 FF-FF-FF-FF-FF-FF)会在物理环路上形成广播环路，形成广播风暴。

网桥环路比路由环路的危害更严重。因为 IP 分组中存在一个 TTL 字段，路由器转发分组时将使 TTL 值逐步减小，最终会丢弃 TTL=0 的分组。而以太网帧中并没有 TTL 字段，使得广播帧无法撤消。

二、网桥表受损

目的站点不存在(可能关闭、故障或根本就不存在)的单播帧会引起网桥表受损，从而导致洪泛转发。

1.5.2 生成树算法

STP 中的生成树算法要用到网桥 ID(BID—Bridge ID)、路径开销(Path Cost)和端口 ID(Port ID)3个参数。

一、生成树算法锁使用的参数

1. 网桥 ID

BID 是由网桥优先级和 MAC 地址字段构成的一个序偶。网桥优先级(Bridge Priority)用于衡量网桥在生成树算法中的优先权(值越小，优先级越高)。BID 中的 MAC 地址是网桥中的 MAC 地址中的一个。生成树算法会对 BID 进行比较：BID 越小，优先级越高。

设(s,t)和(u,v)是两个 BID，其中 s、u 是网桥优先级，t、v 是 MAC 地址。在对 BID 进行比较时，遵循下列原则：

仅当 s<u 或(s=u 并且 t<v)时，有(s,t)<(u,v)。

字段	网桥优先级	MAC 地址
长度	2B	6B
缺省值	32768(取值范围 0~65535)	

2. 路径开销

路径开销是对网桥之间接近程度的度量，其值是两个网桥之间的路径上的所有链路开销的总和。路径开销使用的不是跳数(Hop Count)。

IEEE 802.1D 对路径开销的最初定义是 1000 Mbps 除以链路的带宽。例如，10 BASE T 链路的开销是 100(1000/10)，快速以太链路的开销是 10(1000/100)。

因为开销是用整形数存放的，而 10 Gbps 链路开销但是 0.1(1000/10000)，是一个无效值。因此，IEEE 对路径开销重新进行了定义，如下表所示。

带宽	STP 开销
4 Mbps	250
10 Mbps	100
16 Mbps	62
45 Mbps	39
100 Mbps	19
155 Mbps	14
622 Mbps	6
1 Gbps	4
10 Gbps	2

Catalyst 4000 和 6000 系列交换机支持大于等于 10 Gbp 带宽，对链路开销进行了重新定义，可以进行配置。

3. 端口 ID

端口 ID 是由端口优先级和端口编号两部分构成的一个序偶。其中，要求一个模块上的端口编号必须是连续的，不同模块之间则无此要求；而且，端口编号不一定从 0 开始。生成树算法会对端口 ID 进行比较：端口 ID 越小，优先级越高。比较方法与 BID 的比较方法是一样的。

字段	端口优先级(Port Priority)	端口编号(Port Number)
长度	8 bits(CatOS 为 6 bits)	8 bits(CatOS 为 10 bits)
缺省值	128(CatOS 为 32)	端口可达 256 个(CatOS 为 1024 个)

二、STP 原理

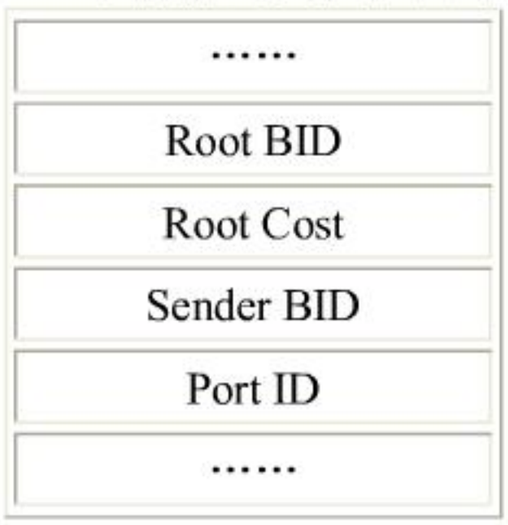
网桥使用网桥协议数据单元 BPDU(Bridge Protocol Data Unit)传递生成树信息。网络初始化时，所有网桥都向网络中泛洪 BPDU。网桥启动后，所有端口都会每隔 2 秒(缺省的 Hello Time)发送一个 BPDU。如果端口收到其它网桥的 BPDU 比自己保存的 BPDU 更好，就会停止发送 BPDU。如果连续 20 秒(缺省的 Max Age 值)没有收到其它网桥的更好的 BPDU，本地端口就会继续发送 BPDU。

通过 STP 信息交换，经历选举根桥、选举根端口和选举指定端口几个步骤，会在存在物理环路的整个网络或 VLAN 中生成一个无环的树形拓扑结构。在网络运行过程中，如果拓扑发生变化，会经历相同的步骤生成新的无环的树形拓扑结构，保证网络正常工作。

在此过程中，需要选举一个网桥成为根桥(Root Bridge)，作为网络的中心。其它网桥则根据到根桥的路径开销选举根端口(Root Port)，确定一组指定端口(Designated Port)。最后构建一个逻辑上无环的树形拓扑，根桥是树干，无环的活动路径作为向外辐射的树枝。在稳定状态的网络中，BPDU 从根桥出发，沿着树枝链路向各个网段传输。

1．选举根桥

根桥由网络中 BID 最小的交换机担任。各个网桥是通过交换 BPDU 获知 BID 的(BPDU 不传输用户数据)。该帧在网桥之间传播，包括所有的交换机和用作桥接的路由器。



网桥每隔 2 秒产生一个 BPDU，在该 BPDU 的 Root BID 字段中填写它所认为的根桥的 BID，在 Sender BID 字段中填写自己的 BID。最初状态，在交换机了解到其它更好的 Root BID 之前，将在 Root BID 字段填写自己的 BID，宣告自己是根桥。

根桥的选举过程——P162 图

2．选举根端口

根端口的选举过程——P163 图

3．选举指定端口

指定端口的确定过程——P164 图

4．STP 状态

STP 状态及其转换——P167 图

5．STP 中的定时器

定时器	缺省值	主要用途
Hello Time	2s	根桥产生并发送配置 BPDU 的时间间隔
Forward Delay	15s	“监听”和“学习”状态的持续时间
Max Age	20s	网桥存储 BPDU 的时间

配置(Configuration)BPDU 和拓扑变更通知(TCN——Topology Change Notification)BPDU。Configuration BPDU 控制初始的 STP 收敛过程，TCN BPDU 负责在拓扑结构的变化时——

802.1D 标准的 HelloTime 控制根桥产生并发送配置 BPDU 的时间间隔。每个端口都会保存所接收到的最佳 BPDU。在此过程中，网桥保存的每 2 秒一个的连续 BPDU 流。如果发送最佳 BPDU 的网桥出现故障，将导致 Max Age 定时器超时，此非根网桥就会停止周期性地发送 BPDU。此时，网桥会把保存的 BPDU 作废，并开始寻找新的根端口。

6．拓扑变更时生成新的树形拓扑

在 STP 稳定工作的过程中，如果网络拓扑发生了变化，需要 30~50 秒(20(Max Age)+15(Listening)+15(Learning))的时间才能收敛在一个新的拓扑结构上。

网络拓扑的变化会触发网桥产生一个拓扑变更通知 BPDU(TCN BPDU)，并发送给根桥——TCN BPDU 在到达根桥的路径上传输，由指定网桥的从根端口和指定端口转发。TCN BPDU 通过 BPDU 中 1 字节的 Type 字段标识(其值为 0x80)。网桥会一直发送 TCN BPDU，直到收到指定网桥的“拓扑变更响应 BPDU(TCA BPDU——Topology Change Acknowledgment BPDU)”。

1.5.3 加快 STP 收敛的技术

一、配置 STP 定时器

二、PortFast

三、UpLinkFast

四、BackboneFast

1.5.4 以太通道(EtherChannel)

以太通道技术是 Cisco 的专有技术。该技术通过把多条物理链路聚集成一条逻辑链路，可以把网络主干的速度提高到 160 Gbps(全双工)。通道中的某一链路出现故障时，以太通道能继续运行；在故障恢复时，该链路会再加入到以太通道中(此即“弹性”的概念)。这样，就可以在交换机、路由器和服务器之间提供高速的容错链路。

以太通道有 4 种形式，分别是标准以太通道(用于兼容以前的技术)、快速以太通道(FEC—

FastEtherChannel)、吉比特以太通道(GEC—Gigabit EtherChannel)和 10G 以太通道(10-Gigabit EtherChannel)。

以太通道可以把 2~8 个链路聚集在一起，使通道的速率接近 1Tbps。使用单模光纤时，在 50km 的范围内，通道速率可以达到 16 Tbps。这样的通道既可以用作接入通道，也可以用作 Trunk 链路。

以太通道的特点：

1. 对网络应用是透明的——不要求网络应用做任何改变
2. 负载均衡——单播、组播和广播负载都可以由通道内的链路之间分担
3. “弹性”和快速收敛——通道具有“弹性”；链路故障时重新分配负载的时间小于 1 秒

一、帧分配

二、PAgP 和 LACP

1.6 VLAN 之间的路由

VLAN 可以控制广播域的大小，并把通信限制在 VLAN 的范围内。但是，如果没有外部路由器或者内部的路由处理器，不同 VLAN 中的设备之间就无法通信。VLAN 之间的通信需要路由选择，可以配置一个或多个路由处理器或路由器实现 VLAN 之间的路由选择。

路由器的功能就是实现网络之间的通信。路由器可以防止广播的传播，所使用的转发算法比交换机的转发算法更具有智能，可以有效地利用带宽。路由器还支持源和目的之间的冗余路径，并能选择最优路径，有助于实现不同路径之间的负载均衡。此外，在组播通信中，路由器也发挥着关键的作用。

路由处理器是一组可以提供路由选择功能的硬件组件，包括 RSM、RSFC、MSM 和 MSFC，它们以电路板卡的形式出现，可以插在交换机中。路由处理器是 3 层网络设备的主系统处理器，负责管理路由表和缓存，发送和接收路由信息，在网络之间进行路由选择。“路由处理器(Route Processor)”一般指的是带主系统处理器的交换模块，其功能与路由器是相同的。因此，我们统称为路由器。

1.6.1 园区网中路由器的作用

在交换式网络中，路由器支持 VLAN 之间的通信。在园区网络中，路由器支持到服务区块(DMZ?)的 VLAN 访问，也支持对广域网直接或间接的访问。

一、分隔广播域

VLAN 把通信限制在一个广播域内，而广播域对应着一个 3 层的子网。因此，如果没有路由器的介入，VLAN 之间就无法进行通信。从相反的角度讲，路由器把不同的广播分隔开了。

二、实现主机的跨 VLAN 通信

不同的子网用路由器连接，会引起终端计算机如何跨越多个局域网段与其它子网中用户通信的问题。终端计算机不需要处理路由表，但它除了必须知道接收方的 IP 地址外，还必须进行配置，使自己知道默认路由器(即缺省网关)的 IP 地址。

网络设备的缺省路由器 IP 地址取决于该网络设备所处的子网。每个 VLAN 在路由器有自己的缺省网关。类似地，配置 VLAN 之间的路由选择时，标准的配置过程是在交换机上配置 IP 缺省网关，指向路由器中为“管理 VLAN”配置的 IP 地址。这样，就启动了通过“管理 VLAN”到园区网中其它设备的连接。

三、实现跨 VLAN 边界的多 VLAN 通信

当网络中的 VLAN 比较多时，就必须决定为每个 VLAN 分配一个单独的路由器接口，还是使用 VLAN Trunking 把多个 VLAN 指定到一个路由器接口。

可以设置路由器的一个接口专门为一个 VLAN 服务。这种方案的不足之处，是需要大量的路由器接口。而有些 VLAN 之间也不一定需要经常进行 VLAN 之间的路由选择，会产生路由器接口不能充分利用的情况。

另一种方案是采用 Trunking 技术，在一条 ISL 或者 IEEE 802.1Q Trunk 链路上承载多个 VLAN 的通信。

四、汇聚层的作用

汇聚层可以为不同的通信(例如组播和广播)提供边界，VLAN 也终止于汇聚层。对于 3 层核心，一般不使用 VLAN。

汇聚层一般由由较高端的交换机或带有 3 层模块的交换机组成。由于具备 3 层功能，汇聚层就成为接入层与核心层之间的分界点。

五、外部路由器

VLAN 之间的路由选择可以通过一台路由器和一台交换机实现。在这种配置中，各 VLAN 与该交换机相连，该交换机再与路由器连接。路由器和该交换机之间通过 Trunk 链路连接。

使用 Trunk 链路的优点是可以减少所需要的路由器和交换机端口数量，也可以减少配置的复杂性。其缺点也是明显的：

- 每个 VLAN 的带宽可能不足(各 VLAN 共享 Trunk 链路的带宽)；
- 在路由器上可能产生额外的开销(处理 Trunking 协议的封装等)；
- 低版本的 Cisco IOS 在 ISL 接口上支持的功能有限(仅支持 IP 和 IPX，不支持热备份路由器协议 HSRP)

六、内部路由处理器(带路由模块的交换机)

最新的汇聚层交换机的趋势是把路由处理器与交换模块集成在一起，交换机的背板(交换机内部使用的高速交换通道)提供交换引擎与路由处理器之间的通信路径。

交换机内部的路由处理器使用的数据流与外部路由器与交换机配合工作时的数据流类似，其区别在于，交换机背板上是用 Trunk 连接交换机和路由处理器的。这样做的技术优点在于：

- 速度(比外部 Trunk 速率高，性能更好)；
- 集成性(路由处理和交换过程紧密集成、提供 2 与 3 层之间的智能通信)

1.6.2 VLAN 间路由选择的配置

一、

二、

三、

1.7 地址转换

1.7.1 网络地址转换概述

一、内部地址与外部地址

IPv4 使用 32 比特的 IP 地址，整个地址空间大约包含 40 亿个单独的 IP 地址。表面看来地址空间特别大，实际上，地址空间已面临枯竭的威胁。一种解决办法是使用更高版本的 TCP/IPv6 协议(其 IP 地址使用 128 比特编码)；另一种方案是使用保留公共地址空间的 RFC 1918。RFC 1918 为专用网络设置了保留的地址空间，这个地址空间用做专用网络的内部地址。ISP 通常在其路由器上进行配置，拒绝转发内部地址用户的流量。因此，不能使用内部地址访问 Internet 网络，内部地址也不能被 Internet 所访问。

1．内部地址的设置

Internet 地址授权委员会设置的专用地址空间如下：

网络类型	内部地址范围	CIDR 前缀
A	10.0.0.0~10.255.255.255(16777214 个)	10.0.0.0/8
B	172.16.0.0~172.31.255.255(1048574 个)	172.16.0.0/12
C	192.168.0.0~192.168.255.255(65534 个)	192.168.0.0/16

上述地址空间是专用地址空间，只能在内部网络中使用(不同的内部网络之间可以重复)，无法与公共网络连接并实现路由。当内部网络要与 Internet 互连时，必须进行地址转换。也就是把不惟一的内部地址转换为全球惟一的全局地址，使内部网络节点可以访问 Internet。

被转换的内部节点地址叫做内部地址(本地地址)，转换后的地址叫做外部地址(全局地址)。这种转换不仅支持内部网络与 Internet 网络的互连，也为内部网络提供了一种附加的保护功能。

2．内部和外部地址的类型

有两种不同类的内部地址和两种不同类的外部地址。参见(3-P270 图)。

内部局部地址——内部网络中分配给一般计算机的 IP 地址，一般是 RFC 1918 规定的保留地址

内部全局地址——外部网络可看到的内部计算机的 IP 地址(全局地址)，一般由 ISP 提供

外部局部地址——外部网络表现在内部网络的 IP 地址(从 RFC 1918 地址空间中分配)——？？

外部全局地址——外部网络主机配置的 IP 地址

二、网络地址转换 NAT(Network Address Translation)的类型

根据转换的方式，NAT 的类型划分为下列两种。

1．动态地址转换

把很多的本地地址转换为一个全局地址或数量有限的一组全局地址，也就是建立很多个内部地址与一个全局地址的映射关系，或者是建立很多个内部地址与一组全局地址的映射关系。因为在建立向外的连接时，转换协议选择第一个可用的全局地址进行分配并使用，因此，这种转换叫做动态地址转换(在连接期间，保持该全局地址)。

动态地址转换又进一步分为网络地址转换 NAT(Network Address Translation)和端口地址转换 PAT(Port Address Translation)。

网络地址转换把多个本地地址映射到一个全局地址池中；端口地址转换则把多个本地地址映射到一个全局地址。只所以叫做端口地址转换，是因为防火墙或路由器使用转换成的单一源地址，而并不改变源端口，以允许多个连接使用单一的全局地址。因为受可用端口数的限制(总共 65536 个，而其中 1024 个已经作为知名端口使用)，PAT 大约可以支持 64000 个内部节点。因为需要使

用源端口和目的端口，因而，一些应用不使用 PAT。

2．静态地址转换

对于静态地址转换，允许本地地址到全局地址按一比一的比例进行转换。即使是内部网络，Web 服务器和 E-mail 服务器一般都必须有静态地址(更实际的做法是直接使用全局地址)。

1.7.2 网络地址转换 NAT

NAT 支持把大量的本地地址转换为数量有限的一组全局地址。这种技术可以对外部网络隐藏内部网络地址的配置，实现一定的安全性。

图(2-P55)展示了NAT的转换原理——内部网络所有节点的地址被映射到一个全局地址池中。

严格地讲，NAT 执行的是一个对 IP 包头中的目的 IP 地址、源 IP 地址或两个地址同时进行替换的过程。通过这种方式，把包头中所使用的内部地址转换为全局地址的进程。因此，就可以不必为内部网络的每个用户分配全局的 IP 地址。

替换过程是由路由器使用 NAT 软件或硬件实现的。执行 NAT 功能的设备叫做 NAT 逻辑单元，它可以是路由器、Windows 计算机或其它设备系统。

一般情况下，实现 NAT 功能的设备在一个存根域(Stub Domain)的边界上运行。所谓存根域，也就是一个与外界有单一连接的网络。

NAT 进程检查内部网络来的 IP 包，用一个全局 IP 地址替换本地源 IP 地址，并在 NAT 转换表中记录这个转换。

当外部主机发送应答的时候，NAT 路由器接收该应答包。通过检查当前网络地址转换表的方式，把外来包的目的 IP 地址替换为原来的内部 IP 地址。

在 Cisco 路由器的缺省情况下，动态 NAT 表目保留 23 小时。

1.7.3 端口地址转换 PAT(NAT 过载)

为了使用少量的地址服务于大量的内部计算机，必须使用端口地址转换(也叫做地址过载—Address Overloading)。所谓地址过载，就是 NAT 路由器通过在转换表中映射 TCP 和 UDP 端口号实现不同的连接，使几百个保留的内部地址能够使用同一个全局地址访问 Internet。

图(2-P56)展示了 PAT 转换的原理——本地转换为单一的全局地址。

与 NAT 不同，PAT 要定义的是一个全局地址，而不是一组全局地址。

1.7.4 静态地址转换

静态地址转换把一个单一的本地地址转换为一个单一的全局地址，具有静态的一一对应关系。这意味着每个内部局部地址要求一个内部全局地址。静态映射关系一直保存在 NAT 表中，除非管理者予以删除。

图(2-P57)展示了静态地址转换的应用。

一般情况下，应该允许外部主机和 DNS 系统使用全局地址访问使用保留(私用)地址的 Web 服务器。

5 基于 IOS 设备的 VLAN 设计和配置

5.1 VLAN 的设计

VLAN 设计在网络设计阶段进行，需要考虑的问题包括：

在 VLAN 之间共享资源；

负载均衡；

冗余链路；

逻辑地址；

如何用 VLAN 对网络进行分段。

5.2 设备选择

5.3 VLAN 配置

Console——Hyper Terminal

局域网——Telnet

Modem——

1．进入交换机和改变配置模式

模式	进入方式	提示符	退出方式
用户模式	启动会话	Switch>	Logout 或 quit
特权模式	用户模式：enable	Switch#	Exit 或 disable
VLAN 配置	特权模式：vlan database	Switch(vlan)#	回特权模式：Exit
全局模式	特权模式：config	Switch(config)#	回特权模式：Exit、end、Ctrl+Z
接口配置模式	全局模式：interface	Switch(config-if)#	回全局模式：Exit；特权：end、Ctrl+Z
连接配置模式	全局模式：line vty/line console	Switch(config-line)#	回全局模式：Exit；特权：end、Ctrl+Z

2．命令行处理和编辑(含帮助、历史等操作)

3．保存和清除配置

4．口令配置

5．配置名称、联系任和位置

6．装载映像到 FLASH

7．配置基于端口的 VLAN

8．配置 VMPS 和动态端口

9．配置以太网 Trunk

10．配置 VTP

(1) 配置 VTP 服务器

(2) 配置 VTP 客户机

(3) 配置 VTP 透明模式

(4) 配置 VTP 版本

(5) 配置 VTP 口令

(6) 监控 VTP

(7) 配置 VTP 修剪

12．STP 配置

5.4 VLAN 之间路由选择配置

在开始进行 VLAN 之间路由选择配置之前，必须在交换机上定义 VLAN。

5.5 NAT 配置

本节介绍 NAT 配置的基本命令，包括动态 NAT 配置、PAT 配置、静态 NAT 配置和查看 NAT 配置的命令和应用实例。

5.5.1 (基于路由器的)基本命令介绍

一、动态 NAT 配置命令

1．定义地址池

Router(config)#Ip Nat Pool name start_ip end_ip [Netmask netmask | Prefix_length prefix_length]

2．定义被转换的地址

通常使用全局命令 Access-list 创建一个访问列表，指定路由器应该转换的源地址范围

Router(config)#Access-List access_list_name Permit source [source_wildcard]　　或

3．使用 Ip Nat Inside Source List 命令创建基于源地址的动态转换

Router(config-if)#Ip Nat Inside Source List access_list_number Pool name

4．接口配置命令

使用下列接口配置命令在路由器上至少配置一个接口作为内部接口：

Router(config-if)#Ip Nat Inside

使用下列命令把一个接口配置为外部接口：

Router(config-if)#Ip Nat Outside

二、PAT 配置命令

下列命令中的关键词 OVERLOAD 用于配置端口转换：

Router(config)#IP NAT INSIDE SOURCE LIST access_list_number POOL name OVERLOAD

三、静态 NAT 配置命令

下列命令用于实现内部局部地址和内部全局地址的转换：

Router(config)#IP NAT INSIDE SOURCE STATIC local_ip global_ip

配置静态映射关系之后，必须指定内部接口和外部接口。

三、检查 NAT 配置的命令

1. SHOW IP NAT TRANSLATION VERBOSE
2. SHOW IP NAT STATISTICS
3. DEBUG IP NAT
4. CLEAR IP NAT TRANSLATION [*|INSIDE|OUTSIDE]——谨用！

5.5.2 应用实例

一、动态 NAT 配置

动态 NAT 配置方案见 3-P272 图。

1. 定义 NAT 地址池

Router(config)#IP NAT POOL mynatpool 171.70.2.1　171.70.2.254 NETMASK 255.255.255.0

2. 定义访问列表

Router(config)#ACCESS-LIST　24　PERMIT　10.1.1.0　0.0.0.255

Router(config)#IP NAT INSIDE SOURCE LIST 24　POOL　mynatpool

3. 配置 NAT 接口

Router(config)#INTERFACE bri0

Router(config-if)#IP NAT OUTSIDE

Router(config-if)#INTERFACE e0

Router(config-if)# IP NAT INSIDE

4. 查看 NAT 设置

Router#SHOW IP NAT TRANSLATION

5. 改变表目保留时间

Router(config)#IP NAT TRANSLATION TIMEOUT seconds

二、PAT 配置

配置方案见 3-P274 图。

Router(config)#IP NAT POOL mypatpool　171.70.2.1　171.70.2.30　NETMASK 255.255.255.0

Router(config)#ACCESS-LIST 24 PERMIT 10.1.1.0　0.0.0.255

Router(config)#IP NAT INSIDE SOURCE LIST 24 POOL mypatpool OVERLOAD

Router(config)#INTERFACE SERIAL　0

Router(config-if)#IP NAT OUTSIDE

Router(config-if)#INTERFACE ETHERNET 0

Router(config-if)#IP NAT INSIDE

三、静态 NAT 配置

配置方案见 3-P273 图。

Router(config)#IP NAT INSIDE SOURCE STATIC 10.1.1.7　172.70.2.10

Router(config)#INTERFACE bri0

```
Router(config-if)#IP NAT OUTSIDE
Router(config-if)#INTERFACE e0
Router(config-if)#IP NAT INSIDE
```

5.5 远程访问配置

6 路由器及路由原理

6.1 路由器的基本结构

6.1.1 路由器的作用

路由器执行网络之间的路由选择功能，可以通过路由器把不同的网络连接起来，实现不同网络之间的信息传输。

物理链路——物理通道？

不同网络——协议转换？

选择路由——路径选择？

6.1.2 路由器的组成

路由器是一种专用计算机系统，由路由器背板、CPU、各种不同类型和用途的存储器、连接不同网络的接口和操作系统等组成。根据需要，可以在路由器背板(主板)上插入相关的功能模块，提供连接相关技术网络的支持。

一、CPU

CPU 是路由器的核心部件，用于执行路由选择算法，实现路由过滤和网络管理等功能。有些路由算法(例如 OSPF)要进行大量的计算，因此，路由器的性能在很大程度上取决于 CPU 的性能。

不同的路由器使用的 CPU 不完全相同。大多数的 Cisco 路由器采用的是 Motorola 的 CPU(68000 系列)或 Orion 的 RISC CPU(R4700)。如果需要，可以查看路由器 CPU 的类型(用 show version 命令)。

二、存储器

路由器中具有不同类型的存储器，用于存放不同类型的程序或数据。

1. 主存储器

主存储器用于存储路由表、地址解析协议(ARP)缓存数据和运行中程序的代码。路由器操作系统要占用很多的存储器空间。为了保证系统的正常运行，提高系统的性能，应配备足够容量的主存储器。

主存储器一般是 DRAM 存储器，在路由器断电的情况下，其中存储的信息就会消失。

2. 非易失性存储器 NVRAM

NVRAM 中存放的是路由器配置文件。网络建设好之后，系统的配置一般不会改变，其配置文件需要在系统运行期间长期保存。即使断电，也要求配置信息不丢失，以便恢复供电后继续运行。NVRAM 存储器具有这种特性，断电时其中的信息也不会丢失。这并不是说 NVRAM 中的内容不可改变。网络管理员可以在线改变网络的配置，并重新写回 NVRAM 中。

3. 只读存储器 ROM

有些路由器需要 ROM 类存储器保存提供基本功能的操作系统。这类存储器还可以存储上电诊断程序和 ROM 监控程序(用于执行系统诊断、硬件初始化、启动操作系统、恢复密码、改变配置寄存器的值、下载操作系统镜像文件等)。由于是只读存储器，其中的信息不能改变，因此，对 ROM 中代码进行升级的惟一是用另一片 ROM 芯片进行替换。

4. 启动 Flash

即使断电，Flash 存储器的信息也不会丢失。与 ROM 的一个区别是，Flash 支持对其中的文件进行改写或删除。因此，新出的路由器一般不使用 ROM 存储器，而是把诊断程序和 ROM 监控程序保存在“启动 Flash”存储器中。

5. Flash 存储器

Flash 存储器一般用来保存路由器操作系统的镜像文件。

Flash 存储器可以是内部的，也可以是外部的。外部 Flash 一般以 PCMCIA(个人计算机存储卡国际协会)卡的形式插在路由器的插槽中。如果容量允许，Flash 存储器中可以存储多个文件，可以用配置命令指定路由器启动过程中加载的镜像文件。

6. 配置寄存器

配置寄存器是一个 16 位的虚拟寄存器。该寄存器用于指定路由器启动的次序、中断参数和控制台(console)波特率。

下表给出的是配置寄存器的一个具体值：0x2102，其中第一行是各位的序号。

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0

下表给出的是配置寄存器各位的含义。

寄存器位	16 进制值	功能描述
0~3		设置路由器的启动特性： 0000——停留在引导提示符下 0001——从 EPROM 中获得启动镜像文件 0002~1111——选择缺省的网络启动文件名
4	-	未使用
5	-	未使用
6	0x0040	忽略 NVRAM 中的配置信息，可用于恢复密码
7	0x0080	起用 OEM 位
8	0x0100	屏蔽暂停键(若未设置，会进入引导监控模式)
9	-	未使用
10	0x0400	全 0 的地址是 IP 广播地址
11~12	0x0800~ 0x1800	Console 速率： [12/11] 16 进制值 波特率 00 0x0000 9600 01 0x0800 4800 10 0x1000 1200 11 0x1800 2400
13	0x2000	启动失败时，使用 ROM 的镜像文件进行启动
14	0x4000	IP 广播具有网络编号
15	0x8000	启用诊断信息，忽略 NVRAM 的内容

三、路由器背板

四、网络接口

五、其它模块

六、路由器操作系统

6.2 VLAN 的设计

6.2.1 应用实例

一、CPU

二、存储器

三、接口及其类型

四、工作状态(?)

6.2.2 应用实例

一、CPU

二、存储器

三、接口及其类型

四、工作状态(?)

6.3 VLAN 的设计

一、CPU

二、存储器

三、接口及其类型

四、工作状态(?)

6.3.1 应用实例

一、CPU

二、存储器

三、接口及其类型

四、工作状态(?)

6.3.2 应用实例

一、CPU

二、存储器

三、接口及其类型

四、工作状态(?)

6.4 VLAN 的设计

一、CPU

二、存储器

三、接口及其类型

四、工作状态(?)

6.4.1 应用实例

一、CPU

二、存储器

三、接口及其类型

四、工作状态(?)

6.4.2 应用实例

一、CPU

二、存储器

三、接口及其类型

四、工作状态(?)

7 (基于 IOS 的)路由器配置

7.1 路由器的工作模式

路由器具有各种不同的工作模式。其中“用户执行模式”具有的权限最少；配置模式的权限最大，可以对配置进行修改。为了保证网络的安全性，对不同模式可以设置不同的密码和口令。只有回答的密码和口令正确时，才可以进入相映的工作模式。对于新路由器或配置文件被删除的路由器，最初始的设置可以通过“初始对话模式”进行设置。

下面将分别介绍路由器各种不同工作模式的特点和进入方式。

7.1.1 初始对话配置模式

如果路由器是新的，或者路由器中的配置文件被删除，启动时，路由器就会提示用户是否进入系统配置对话模式。

首先，路由器显示下列提示：

Would you like to enter the initial configuration dialog?[yes/no]:**yes**

可以回答“no”，不进入初始对话配置模式，而使系统进入后面介绍的“用户执行模式”。

假设回答“yes”，系统将进入初始对话配置模式。下面介绍的是初始对话配置模式的操作步骤和内容。

回答“yes”后，系统会提示是否进入基本管理设置：

Would you like to enter basic management setup?[yes/no]:**yes**

回答“yes”(黑体字表示用户输入，下同)，系统会要求回答路由器主机名：

Enter host name [router]:**router**

回答当前路由器主机名(可以自己定义)“router”后，系统接着提问特权模式密码：

Enter enable secret:**cisco**

回答密码“ciasco”(为避免忘记，这里的所有密码和口令均回答“cisco”。实际配置时用户应根据自己的情况回答)，系统接着提问特权模式口令：

Enter enable password:**cisco**

回答口令“ciasco”，系统接着提问虚拟终端口令：

Enter virtual terminal password:**cisco**

回答口令“ciasco”，系统接着提问是否配置简单网络管理协议：

Configure SNMP Network Management?[yes]**n**

回答口令“n”后，系统显示当前接口汇总信息。然后提出下列问题：

Enter interface name used to connect to

the management network from the above interface summary:**ethernet0**

回答口令“ethernet0”后，系统接着询问该接口的 IP 地址和子网掩码：

IP address for this interface:**10.1.1.1**

Subnet mask for this interface[255.0.0.0]:**255.255.255.0**

接着，系统将显示配置的结果信息。最后显示下列选项，询问是否保存配置信息：

[0] Go to the IOS command prompt without saving this config.

[1] Return back to the setup without saving this config.

[2] Save this configuration to nvram and exit.

Enter your selection[2]:**2**

在此选择“2”，保存配置信息后退出。

一般情况下，新路由器会询问是否进入初始对话配置模式。以后启动路由器时，会直接进入“用户执行模式”。在进入不同工作模式时，路由器会询问相应的密码和口令，对用户身份进行验证。在密码和口令正确时，才会进入相应的工作模式。

7.1.2 常用的工作模式

不同的工作模式具有不同的操作权限，用户执行模式仅可以查看系统的基本信息，特权执行模式可以查看路由器的配置信息，配置模式则可以对配置进行修改。

一、用户执行模式

在成功加载完整的 IOS 之后，路由器首先进入“用户执行模式”。该模式的提示符如下：

router>

其中，“router”是路由器的主机名(Host name)。

在用户执行模式下，可以显示系统信息，执行基本的测试操作，改变终端设置。但是，不允许查看配置文件，不允许更改信息，不允许使用 debug 命令。要查看这些信息，必须进入“特权执行模式”。

二、特权执行模式

特权执行模式也叫做 enable 模式。在用户执行模式中，执行“enable”命令就可以进入特权执行模式。进入特权执行模式后，系统提示符如下：

router#

在特权模式下，可以显示路由器设置和状态信息。在该模式的基础上，可以进入配置模式，对路由器进行配置。

三、配置模式

1．基本配置模式

在特权模式中执行“configure terminal”命令，就可以进入基本配置模式，其提示符如下：

router(config)#

在该模式下，可以对路由器、路由器接口和 console 接口进行配置。配置对象不同，可以执行的命令也就不同。可以把配置模式进一步划分为接口配置模式、路由协议配置模式等。下面分别进行介绍。

2．接口配置模式

用下列命令进入接口配置模式：

router(config)#**interface ethernet 0**

router(config-if)#

其中，router(config-if)#是接口配置模式的提示符。

3．路由协议配置模式

可以用下列不同的命令进入路由协议配置模式：

router(config)#**router rip**

router(config-router)#**exit**

router(config)#**router eigrp 100**

router(config-router)#

其中，router(config-router)#是路由协议配置模式的提示符。

4．线路配置模式

可以用下列不同的命令进入线路配置模式，对 console 和虚拟类型终端(vty)进行配置。

router(config)#**line con 0**

router(config-line)#**exit**

router(config)#**line vty 2**

router(config-line)#

其中，router(config-line)#是线路配置模式的提示符。

5．映射配置模式

用下列命令可以进入映射配置模式：

router(config)#**route-map ccie**

router(config-route-map)#

其中，router(config-route-map)#是映射配置模式的提示符。

不同模式下的具体配置命令将在后面逐步介绍。

7.1.3 其它工作模式

一、ROM 监控模式

启动时，若没有加载任何 IOS 镜像文件，路由器就进入“ROM 监控模式”。监控模式的提示符如下：

rommon>

或

>

二、启动模式

如果“启动 Flash”中含有具备最小 IOS 功能的启动程序，路由器就进入“启动模式”。启动模式的提示符如下：

router(boot)>

在启动模式下，路由器的自举程序不会加载整个 IOS 镜像文件。因此，仅允许查看配置信息，路由器处于没有路由选择功能的工作状态。需要时，可以使用 TFTP 协议配置一个缺省网关，以加载 IOS 镜像文件。

7.2 路由器的基本操作

7.2.1 路由器的访问方式

路由器上一般配置有不同的端口，例如 console 端口、以太网(ethernet)端口和辅助(AUX)端口等。因此，我们可以通过 console 电缆直接把计算机连接到路由器的 console 端口，使用 Windows 中的“超级终端(Hyper Terminal)”对路由器进行配置；可以利用 ethernet 端口把路由器连接到网络中，把网络中的计算机作为操作平台，使用 Telnet 或 SNMP 对路由器进行配置；还可以使用路由器的辅助端口和 Modem，对路由器进行远程配置。

下面分别介绍路由器的各种不同访问方式。

一、控制台访问方式

这种访问方式是通过路由器的 console 端口与路由器连接，对路由器进行配置。根据与路由器相连接的设备的不同，console 方式方式又进一步分为 Hyper Terminal 和反向 Telnet 方式。

1．Hyper Terminal 访问方式

利用随路由器一起提供的console专用电缆，可以把计算机直接连接到路由器的console端口。硬件连接好之后，启动计算机。然后启动“开始”/“附件”/“通信”中的“超级终端”，就可以建立计算机与路由器的连接，开始对路由器进行配置。

在建立连接的过程中，需要输入连接的名称，并对终端软件进行如下设置：

9600 bps；

无奇偶校验位；

8 个数据位；

1 个停止位；

无数据流控制。

在这种方式中，首先需要使用下列命令对控制台进行配置：

line con 0

password 口令

login

2．反向 Telnet 访问方式

具备异步接口的路由器可以充当终端服务器，并通过异步通信线路与需要进行配置的路由器的 console 端口相连接。使用 Telnet 对终端服务器进行访问，对路由器的访问则是使用反向 Telnet 进行的。

要实现反向 Telnet，需要在终端服务器上配置一个回送 IP 地址。假设回送 IP 地址是 20.1.1.1，就可以使用下列命令访问指定的路由器。

telnet 20.1.1.1 2001　　；访问用第一条异步线路连接到的路由器

telnet 20.1.1.1 2002　　；访问用第二条异步线路连接到的路由器

二、局域网访问方式

在这种访问方式中，路由器与一个局域网络连接在一起，网络中的计算机使用 Telnet 或 SNMP 访问和配置路由器。

1．Telnet 访问方式

Telnet 方式也就是虚拟终端方式。在这种方式中，首先需要使用下列命令对线路进行配置：

line vty 0 4

password 口令

longin

2．SNMP 访问方式

要用一台 SNMP 服务器访问路由器，首先需要对 SNMP 读和读写通信字符串进行配置。下面的命令设置只读字符串为“ccie-read”：

router(config)#snmp community ccie-read ro

下面的命令把读写字符串设置为“ccie-write”：

router(config)#snmp community ccie-write wr

在路由器上可以为网络管理服务器设置 SNMP 断点。使用下列命令，可以把所有断点发送到通信字符串为“ccie-trap”的 SNMP 服务器(IP 地址为 20.1.1.1)：

router(config)#snmp host 20.1.1.1 ccie-trap

三、辅助端口访问方式

辅助端口通常连接 Modem，支持对路由器的远程访问。在这种方式中，首先需要做如下的配置：

line aux 0
password 口令
login
transport input all
modem autoconfigure discovery
exec-timeout 30 0

7.2.2 密码设置与恢复

可以为控制台(console)、辅助端口(aux)和虚拟终端线路(vty)访问设置密码，防止对路由器的非法访问，保证网络的安全。

login 命令告诉路由器，只有输入正确的密码才能进入对路由器的访问。而 password 命令则用于密码的设置。

一、密码设置

1. 控制台密码的设置

控制台密码是用 line console 0 命令设置的。下面给出的是配置的操作步骤。

router(config)#line console 0
router(config-line)#login
router(config-line)#password 口令

2. 辅助端口密码的设置

辅助端口密码是用 line aux 0 命令设置的。下面给出的是配置的操作步骤。

router(config)#line aux 0
router(config-line)#login
router(config-line)#password 口令

3. 终端线路密码的设置

多数路由器具有 5 条终端线路，分别是线路 0、1、2、3 和 4。这些终端线路的密码是用 line vty 0 4 命令设置的。下面给出的是配置的操作步骤。

router(config)#line vty 0 4
router(config-line)#login
router(config-line)#password 口令

4. 特权执行模式密码的设置

特权执行模式的密码可以使用 enable password 命令或者 enable secret 设置。区别在于，系统会对用 enable secret 命令设置的密码进行加密，具有更强的安全性。如果两条命令都使用，enable secret 命令会覆盖 enable password 命令。

(1) 使用 enable password 命令设置
命令格式：enable password 口令
(2) 使用 enable secret 命令设置
命令格式：enable secret 口令

二、密码恢复

1. RISC 处理器的路由器的密码恢复

2. 非 RISC 处理器的路由器的密码恢复

7.2.3 TFTP 与配置文件管理

一、TFTP

使用 TFTP 协议，可以在路由器之间传送 IOS 镜像文件和配置文件。

1．传输配置文件

使用 write network 或 copy running-config tftp 命令都可以把配置文件拷贝到指定的 TFTP 服务器。在命令的执行过程中，需要指定 TFTP 服务器的 IP 地址和配置文件名。而 configure network 和 copy tftp running-config 命令则执行相反的功能，用于把 TFTP 服务器中的配置文件拷贝到 RAM 存储器中。

下面给出的是 copy tftp running-config 命令的执行过程。

router#**copy tftp running-config**

address or name of remote host[]?**1.1.1.1**

source filename[]?**router-config1**

destination filename[running-config]?

2．传输 IOS 镜像文件

copy flash tftp 命令可以把 IOS 镜像文件拷贝到指定的 TFTP 服务器，而 copy tftp flash 命令则执行相反的功能，用于把 IOS 镜像文件从 TFTP 服务器拷贝拷贝到 flash 系统中。

下面给出的是 copy flash tftp 和 copy tftp flash 命令的执行过程。

router#**copy flash tftp**

source filename[]?**mc3810**

address or name of remote host[]?**1.1.1.1**

destination filename[mc3810]?

router#**copy tftp flash**

address or name of remote host[]?**1.1.1.1**

source filename[]?**mc3810**

destination filename[mc3810]?

二、配置文件管理

路由器的配置信息可以存储在 NVRAM、DRAM、终端或某台 TFTP 服务器中。启动的时候，系统会使用 NVRAM 中的配置信息进行配置。启动成功后，配置信息将存放在 DRAM 中。用户可以通过不同的方式查看路由器的配置信息。

下表给出的是对配置文件进行管理的命令。

配置文件管理命令	功能
Write terminal Show running-config	在显示器上显示配置信息
Configure termnal	进入配置模式，以便对配置进行修改、更新

Configure memery Copy startup-config running-config	把 NVRAM 中的配置信息拷贝到活动存储器中，使其立刻生效
Write memery Copy running-config startup-config	把正在运行的配置信息拷贝到 NVRAM 中
Copy tftp running-config Configure network	把配置文件从 TFTP 服务器拷贝到活动存储器
Copy running-config tftp Write network	把正在运行的配置信息拷贝到某 TFTP 服务器
Write erase	删除 NVRAM 中的配置文件
Show configuration Show startup-config	在显示器上显示 NVRAM 中的启动配置文件

7.2.4 常用的 CLI 命令：show 与 debug 命令

一、show 命令

在用户执行模式和特权执行模式，可以使用 show 命令显示路由选择协议、接口和系统的状态信息。

Show 命令很复杂，具有很多可选的关键字和参数。这里只对 show 命令的选项作概要性介绍，用户可以在实际环境中通过反复练习，熟悉该命令的不同使用方法。

1． show 命令常用的选项

执行 show ?命令可以查询 show 命令的关键字和参数选项。

Router#**show ?**

下表给出了执行上述 show ?命令列出的常用选项。

选项	英文说明	含义
Access-list	List access lists	显示访问列表信息
Accounting	Accounting data for active sessions	显示当前会话及统计信息
Flash:	Display information about flash:file system	显示 flash 文件系统的信息
Frame-relay	Frame-relay information	显示帧中继信息
Interfaces	Interface status and configuration	显示路由器接口信息
Ip	IP information	显示 IP 信息
Logging	Show the contents of logging buffers	显示日志信息
Running-config	Current operating configuration	显示运行配置信息
spanning-tree	Spanning tree topology	显示生成树信息
Standby	Hot standby protocol information	显示热？？？协议信息
Startup-config	Contents of startup configuration	显示启动配置信息

2． Show ip 命令常用的选项

Show ip 命令是最常用的一个命令。可以用 show ip ?命令显示该命令选项关键字。

Router#**show ip ?**

下表给出了执行上述 show ip ?命令列出的常用选项。

选项	英文说明	含义
Arp	IP ARP table	显示 IP ARP 表的信息
Bgp	BGP information	显示 BGP 表的信息
Eigrp	IP-EIGRP show commands	IP-EIGRP 显示命令
interface	IP interface status and configuration	显示接口状态和配置信息
Ospf	OSPF information	显示 OSPF 信息
Pim	PIM information	显示 PIM 信息
Policy	Policy routing	显示策略路由信息
protocol	IP routing protocol process parameters and statistics	显示路由协议参数和统计信息
Rip	IP RIP show commands	IP RIP 显示命令
Route	IP routing table	显示 IP 路由表

3． Show ip interface brief 命令

可以用 show ip interface brief 命令查看 IP 接口的汇总信息，包括接口信息、配置的 IP 地址以及接口和协议的工作状态。下面给出的是该命令执行时的显示情况。

Router#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0	136.5.20.5	YES	manual	up	up
FR-ATM20	unassigned	YES	unset	administratively down	down
Lookback0	unassigned	YES	unset	up	up
Serial0	unassigned	YES	unset	administratively down	down
Serial0	136.5.21.6	YES	manual	up	up

4． Show version 命令

这个命令可以显示启动 IOS 的版本，系统正常运行的时间，RAM、Flash 和 NVRAM 的容量，路由器 CPU 的类型，接口状态，配置寄存器的设置以及系统上电的方式(加电启动、重新启动或者是出现错误)。该命令的执行情况，读者可以自己执行、查看。

二、debug 命令

debug 命令只能在特权执行模式中执行。通过 Telnet 访问路由器时，需要执行 Terminal monitor 命令，以便把执行 debug 命令时的信息显示在自己的屏幕上(console 方式则不需要)。

1．Debug 命令的常用选项

下表给出的是执行上述 debug ?命令列出的常用选项。

选项	英文说明	含义
Aaa	AAA Authentication,Authorization and Account	认证、授权和统计
Access-expression	Boolean access expression	布尔型访问表达式
All	Enable all debugging	启动所有 debug 项目
Alps	ALPS debug information	ALPSA 调试信息
Arp	IP ARP and HP Probe transactions	ARP 和 HP Probe 事务

2．路由选择协议调试命令

下表给出的是用于 OSPF、EIGRP 和 RIP 协议的 debug 命令。

命令	功能
OSPF 命令	
Debug ip ospf adj	列出 OSPF 的相邻关系信息
Debug ip ospf events	列出 OSPF 的事件信息
Debug ip ospf packet	列出 OSPF 的数据包信息
Debug ip ospf spf	列出 OSPF 最短路径优先算法的信息
Debug ip ospf tree	列出 OSPF 数据库树的信息
EIGRP 命令	
Debug ip eigrp neighbors	列出 EIGRP 相邻路由器的信息
Debug ip eigrp packets	列出 EIGRP 的数据包信息
Debug ip eigrp transmit	列出 EIGRP 传输事件的信息
RIP 命令	
Debug ip rip database	列出 RIP 数据库事件的信息
Debug ip rip events	列出 RIP 协议事件的信息
Debug ip rip trigger	列出 RIP 触发数据包事件的信息

另外，使用 show debug 命令可以查看系统中已经启动的调试选项。

7.3 路由器接口的配置

7.3.1 以太接口的配置

所有的以太网(ethernet)接口都基于 IEEE 802.3 标准。快速以太网(Fast Ethernet)基于 IEEE 802.3u 标准，而吉比特以太网(Gigabit Ethernet)则基于 IEEE 802.3z 标准。

一、基本命令

1． 选择以太网封装(可选)

命令格式：**encapsulation [arpa|sap|snap]**

以太网帧的封装格式可以是 arpa(ARPA Ethernet 版本 2.0，为默认封装)、sap(SAP IEEE 802.3)或者用于 IEEE 802.2 介质的 snap(SNAP)。

2. 选择介质类型(可选)

命令格式：**media-type [aui|10baset|mii|100basex]**

3. 指定接口速度——只用于快速以太网

命令格式：**speed [10|100|auto]**

4. 指定双工模式——适用于快速以太网和吉比特以太网

命令格式：**deplex [full|half|auto]**

默认为 half。

5. 配置快速以太网通道(可选)

(1) 把接口分配到一个通道

命令格式：**channel-group** group

至多可以有 4 个快速以太网接口捆绑在一个共同的组中。被捆绑的接口不能再配置 IP 层地址。所有的 3 层通信量分布在组内的各个接口上，非 3 层的通信量则通过组内的第一条链路传输。

(2) 给通道分配 IP 地址

命令格式：**interface port-channel** group

可以把捆绑作为一个整体分配 IP 地址或者桥接组。端口通道(port channel)充当路由接口而不是单个的物理接口。

二、配置实例

配置 1 个以太网接口(e 0/1)、一个吉比特以太网接口(g 5/0/0)和 2 个快速以太网接口(fa 2/3 和 fa 2/4)。

具体要求如下：

e 0/1：IP 地址为 10.1.1.1，子网掩码为 255.255.255.0；

g 5/0/0：IP 地址为 10.1.3.1，子网掩码为 255.255.255.0，全双工；

fa 2/3 和 fa 2/4：接口速度和工作模式(full/half/auto)为 auto，2 个接口无 IP 地址，把它们配置为一个以太网通道 1，该通道的 IP 地址为 10.1.2.1，掩码为 255.255.255.0。

配置命令如下：

```
interface ethernet 0/1
        ip address 10.1.1.1 255.255.255.0

interface fastethernet 2/3
        speed auto
        duplex auto
        channel-group 1
        no ip address

interface fastethernet 2/4
        speed auto
        duplex auto
        channel-group 1
        no ip address
```

```
interface port-channel 1
        ip address 10.1.2.1 255.255.255.0

interface gigabitethernet 5/0/0
        ip address 10.1.3.1 255.255.255.0
        duplex full
```

7.3.2 VLAN 接口的配置

路由器上的 VLAN 接口是虚拟接口，但被当作独立的物理接口。该虚拟接口可以包含子接口，以支持特定的 VLAN。

一、基本命令

1. 定义 VLAN 的子接口

命令格式：**interface fastethernet** mod/num.subinterface

interface gigabitehernet mod/slot.subinterface

2. 配置 Trunking 封装

命令格式：**encapsulation [isl|dot1q]** vlan [native]

封装可以是 ISL 或 IEEE 802.1Q。在使用 dot1q 的情况下，可以用关键字 native 把子接口 VLAN 配置为 natrive VLAN。

二、配置实例

配置目标：

使用一个吉比特以太网接口聚集 IEEE 802.1Q 的 VLAN：子接口 17 用于 VLAN 17，子接口 26 用于 VLAN 26(子接口号可以任意设置，且不要求和 VLAN 号一致)。

配置命令如下：

```
interface gigabitethernet 9/0/0.17
        description VLAN 17 to Accounting Dept
        encapsulation dot1q 17 native
        ip address 192.168.88.1 255.255.255.0

interface gigabitethernet 9/0/0.26
        description VLAN 26 to Engineering Dept
        encapsulation dot1q 26
        ip address 192.168.100.1 255.255.255.0
```

7.3.3 Frame-Relay 接口的配置

一、命令

二、命令

7.3.4 Serial 接口的配置

一、命令

二、命令

7.4 路由协议的配置

7.4.1 RIP 协议的配置

一、命令

二、命令

7.4.2 OSPF 协议的配置

一、命令

二、命令

7.4.3 EIGRP 协议的配置

一、命令

二、命令

参考资料：

1. CCNP 思科网络技术学院教程(第七学期)多层交换 Cisco System 公司等 韦新 译 人民邮电出版社 2003 年 7 月
2. CCSP Cisco 安全 PIX 防火墙认证考试指南 Greg Bastien 等 卢泽新 等译 人民邮电出版社 2003 年 10 月
3. CCNP 思科网络技术学院教程(第六学期)远程接入 Cisco System 公司等 张伟 等译 人民邮电出版社 2003 年 10 月
4. CCIE 路由与交换认证考试指南 A.Anthony Bruno 卓林 等译 人民邮电出版社 2003 年 6 月
5.