



CCNA/CCNP/CCIE 案例实战手册

交换部分



目录

前言	5
案例一 深刻理解 VLAN、TRUNK 和 VTP 协议	6
案例二 最简单路由转发拓扑——单臂路由	10
案例三 使用 TELNET/SSH 去管理远程设备	12
案例四 为交换机灌 IOS 和密码恢复	14
案例五 交换网络核心技术——生成树原理	16
案例六 深刻理解生成树协议的工作方式	18
案例七 利用生成树的特性保护根交换机	20
案例八 利用 ETHERCHANNEL (EC) 增加链路带宽和冗余性	22
案例九 【综合实验】实现不丢包转发——MSTP+HSRP	24
案例十 堆叠的好处——简化网络管理及增加设备性能	28
案例十一 在网络设备上提供 DHCP 服务	31
案例十二 在企业网中跨网段部署 DHCP 的方式	33
案例十三 在企业网中部署 AAA 服务器	38
案例十四 【综合实验】通过 AAA 验证后，自动获取 IP 并上网	45
案例十五 使用端口安全——加强企业接入层交换机安全性	47
案例十六 利用 RSPAN 监控企业异常网络流量	50
案例十七 利用 QOS 保障企业重要数据流量通信	53
案例十八 理解组播路由协议的原理和用法	59
案例十九 【综合实验】组播在视频直播中的应用	63

前言

这一套文档我不敢保证后面不会有来者，但可以保证绝对前无古人，任何人只要把这两个文档里面 80% 的东西掌握了，你不需要考任何认证，因为这些实验和理论都是 CCNA/CCNP/CCIE 考试的精华内容，不管是建设横跨国家之间的大型网络项目，还是小到几百人的公司网络，所使用的技术都不会超出这个范围，并且结合真实项目需求和部署案例加以讲解，里面每个实验都涉及案例拓扑、关键知识点、实战需求、配置命令详解和排错思路 5 大部分，适合不同基础的用户学习，如果你是一个菜鸟，就从关键知识点开始看，然后根据实战需求的步骤做实验；如果你是一个大侠，你可以看案例拓扑和实战需求，然后搭拓扑做实验；如果你是一个工程师这个手册也可以当作一本命令手册，因为里面涉及到各种常用技术的命令配置规范，不管怎样，这个文档适合所有人，因为我们的编写目的就是出一本能让人看的懂并且学得会的技术文档；

以我多年实施项目的经验来看，路由是一个网络的上层建筑，而要保证上层建筑的稳固，你必须保证底层建筑的扎实和牢靠，而交换就是一个网络的地基，网络界有一句名言：“学好路由能让你升值和加薪，而学好交换则能保住你的工作不丢”。这句话的含义也许现在你不懂，但等你以后工作了，慢慢体会这句话的深层含义吧。

目标

解救正走在考证路上迷茫的广大 Cisco 学员，你们是这个国家未来信息网络的栋梁，如果你们不能找一个正确的学习方向，那么中国未来的信息高速公路的建设也是暗淡的，只有你们的素质提高了，我们才能更好的享受信息给我们带来的便利。这套手册的目标是帮助你把网络的核心——路由和交换的基础理论学扎实，只有路由和交换学扎实了，你才能在它的基础上添砖加瓦，安全、无线、语音和负载均衡等等无不都需要路由的畅通。

版本

这是本套文档的测试版本，后续结合还会陆续更新更多的内容，此为交换部分，参考了众多书籍和项目案例，自认为交换文档，目前的技术涵盖已经很全了，但还有一些具体的技术，里面没有收录，因此 Combat-Lab 会考虑再出一个技术方案的文档，这个文档是各个厂商项目流行的技术的应用，例如：Cisco 的 VSS 虚拟交换机的部署、FWSM 模块的部署等等，我们的技术收录不会局限于考试大纲，只要是目前企业在用的，客户需要的技术，我们都会争取收录进来，因此也希望广大网友多多为我们募集好的技术，我们会再加把劲，把更多的好技术收录进来；

案例一 深刻理解 VLAN、Trunk 和 VTP 协议

案例
拓
扑

图1

图2

图3

关
键
知
识
点

冲突域： 一个网段属于一个冲突域，例如：每个 Hub 都属于一个冲突域，而 Switch 的每个端口都属于冲突域；

广播域： 一个子网属于一个广播域，逻辑上一个 LAN 组成一个广播域，物理上一个交换机构成一个广播域；

划分 VLAN 的优势：

- 1. 缩小广播域
- 2. 安全性
- 3. 扩展性，不受地域限制

Native VLAN： 默认情况下，交换机所有接口默认都在 Native VLAN 中，vlan 1 是 Native VLAN，无法删除，非 Native VLAN 的流量在 Trunk 中传输数据时要被添加 Vlan 标记，但是 Native VLAN 在 Trunk 中传输数据时是不进行标记的。

VLAN 号范围：

VLAN 范围	范围	用途	通过 VTP 扩散
0,4095	保留	仅限系统使用，用户不能查看和使用这些 vlan	—
1	正常	Cisco 默认 VLAN，用户可以使用该 VLAN，但不能删除它	是
2 ~ 1001	正常	用于以太网的 VLAN，用户可以创建、使用和删除这些 VLAN	是
1002 ~ 1005	正常	用于 FDDI 和令牌环的 Cisco 默认 VLAN，用户不能删除	是
1006 ~ 1024	保留	仅限系统使用，用户不能查看和使用这些 vlan	—

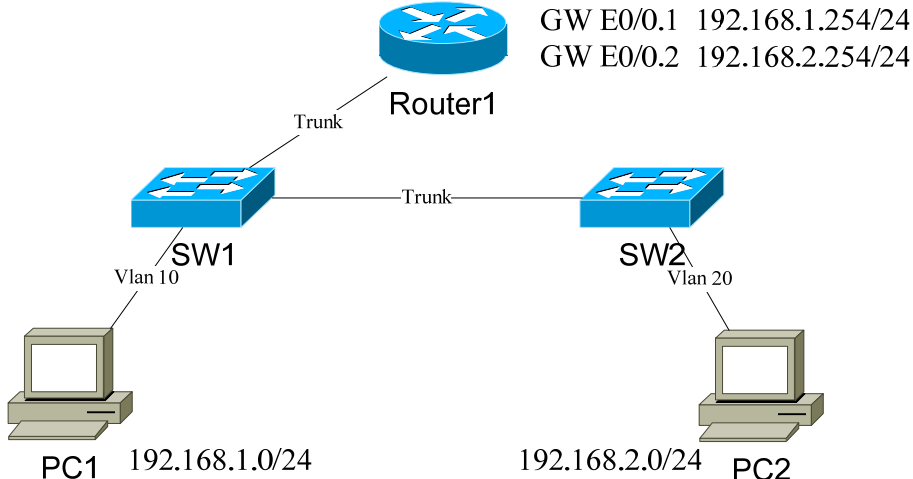
	1025 ~ 4096	扩展	仅用于以太网 VLAN	
Cisco 交换机 VLAN 支持矩阵				
交换机类型	VLAN 的最大数量		VLAN ID 范围	
Catalyst 2950	250		1 ~ 1005	
Catalyst 2960	255		1 ~ 4094	
Catalyst 2970/3550/3560	1005		1 ~ 4094	
Catalyst 4000/4500/6500	4094		1 ~ 4094	
链路聚集协议：				
ISL：Cisco 私用的 Trunk 封装协议，不修改原始帧的基础上，裹上 ISL 的报头和报尾（30 byte）；				
IEEE 802.1Q：在原始帧的源 MAC 和长度之间插入一个 Tag 字段（4 byte），并重新计算 FCS 校验；				
理解 Dynamic Trunk Protocol（DTP）：				
接入（Access）：强制将接口永久配置为非 Trunk 链路；				
干道（Trunk）：强制将接口永久配置为 Trunk 链路				
非协商（Nonegotiate）：将接口永久配置 Trunk 链路，并且禁止接口产生 DTP 帧；				
动态期望（Dynamic Desirable）：使接口主动尝试将链路转换为 Trunk 链路；				
动态自动（Dynamic Auto）：使接口愿意将链路转换为 Trunk 链路；				
	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	连接受限
Access	Access	Access	连接受限	Access
VLAN 链路聚集协议（VTP）：用于在交换机之间同步 VLAN 的相关信息，默认情况下，Cisco 交换机每 5 秒通过管理 VLAN 以二层组播数据帧的形式传输一次 VTP 通告，下面是 VTP 的三种模式；				
1.Server mode：可以创建、修改和删除 VLAN，转发 VTP 通告，同步 VLAN 并保存到 NVRAM 中；				
2.Client mode：不能创建、修改和删除 VLAN，转发 VTP 通告，同步 VLAN 但不保存到 NVRAM 中；				
3.Transparent mode：只在本地创建、修改和删除 VLAN，转发 VTP 通告，不同步但保存到 NVRAM；				
重要：只有管理域名和密码匹配才能同步 VLAN 信息，没修改一次 VLAN 信息，VTP 的配置修订号都会自动加 1，如果交换机上的配置修订号低，将被高版本的 VTP 通告消息覆盖；				
实战需求	实战目的：测试相同 vlan，不同网段主机是否能够通信；不同 vlan，相同网段又是否能够通信			
	需求一：图 1 中，将 PC1 和 PC2 连接交换机的端口都划入 vlan 10，配置 PC1 地址为 192.168.1.10，配置 PC2 地址为 192.168.2.10，掩码都是 24 位，不配置默认网关，开启抓包软件 wireshark 看是否能够抓到流量，并测试是否能够 ping 通，为什么？			
	需求二：PC1 和 PC2 分别将对方的 IP 地址设置为网关，再次互 ping，同时查看抓包信息，分析整个通信过程，是否能够 ping 通，为什么？			
	需求三：图 2 中，将连接 PC1 的接口划入 vlan 10，配置地址为 192.168.1.10；将连接 PC2 的端口划入 vlan 20，配置地址为 192.168.1.11，测试是否能够 ping 通，抓报分析，为什么？			
	需求四：将两个交换机使用 Trunk 连接起来，SW1 是 vtp server 模式，SW2 是 vtp client 模式，管理域名都是 CCNP，在 SW1 上创建 vlan 10/20/30/40/50，查看 SW2 是否能够自动学习到这些 VLAN；			
配	VLAN 配置规则（旧配置——3620 等路由器上）：			
	vlan database		进入 VLAN 配置模式	

置
命
令
详
解

vlan [1 ~ 1005] name [名称]	配置 vlan 和名称
apply	退出并应用配置
VLAN 配置规则（新配置——2950/3560 等交换机上）:	
vlan [1 ~ 1005]	配置 VLAN
name [名称]	配置 vlan 名称
int f0/x	进入接口
switchport mode access	配置为 access 模式
switchport access vlan [1 ~ 1005]	将接口划入指定 VLAN 中
Trunk 配置规则（2950 上）:	
int f0/x	进入接口
switchport mode trunk	将接口强制配置为 trunk 模式
switchport mode dynamic auto/ desirable	将接口配置为动态协商模式
Trunk 配置规则（3550/3560 上）:	
int f0/x	进入接口
switchport trunk encapsulation dot1q	使用 802.1Q 封装该接口，必须先打
switchport mode trunk	将接口配置为 Trunk
switchport trunk allowed vlan [1 ~ 1024]	指定允许哪些 VLAN 通过
switchport trunk native vlan [vlan ID]	指定 native vlan
VTP 配置规则:	
vtp mode [模式]	配置 VTP 的模式，默认是 server
vtp domain [域名]	配置 VTP 的管理域名，匹配才能同步
vtp password [密码]	配置 VTP 的密码，可选
vtp version [1/2]	配置 VTP 的版本，可选，默认为 1
验证命令:	
show vlan	查看 VLAN 信息
show interface vlan [VLAN ID]	查看具体某个 VLAN 的详细信息
show interface f0/x switchport	查看交换接口的详细配置信息
show interfaces trunk module 0	查看设备上所有端口的 Trunk 状态
show interfaces status	查看每个接口状态、双工和速率
show interface summary	查看接口包转发状态
show vtp status	查看 VTP 协议状态
show ip interface brief	查看设备的所有接口信息
show mac-address-table	查看交换机的 MAC 地址转发表
show arp	查看交换机 ARP 表项
重要命令: 默认情况下，交换机的 vlan 文件不是保存在 config.text 中，因此在清除启动配置后，还可以看见 vlan 信息，cisco 交换机是将 VLAN 信息保存在 Flash 中的的 vlan.dat 中，只有将该文件删除，vlan 信息才能彻底删掉；	


	<div>show flash:使用 show 命令查看是否有 vlan.dat 文件</div> <div>delete flash:vlan.dat使用 delete 命令删除 vlan.dat 文件</div>
排错思路	<div>1. 相同 vlan，不同网段之间的 PC，只有在互指网关的情况下，才可以通信，这是因为在不指定网关的情况下，PC 如果要去另一个网段，它不知道应该把这个包给谁，因为目的主机和它不是一个网段，因此 PC 不会产生任何二层和三层流量，直接报错 (PING: 传输失败。General failure.)；例如 PC1 如要使用 192.168.1.10 的地址 ping 通 192.168.2.10 的地址，在不指定网关的情况下，通过子网掩码，PC1 获悉 192.168.2.10 是另一个子网的地址，windows 将之间返回：传输错误的提示，不会产生任何流量；</div> <div>2. 互指网关后，PC1 会直接发送 arp 广播在所有属于 vlan 10 的端口中寻找 192.168.2.10，因为 PC2 也在 vlan 10 中，所以会收到改广播，收到 arp 广播后，PC2 一看与自己的地址相同，就会给 PC1 回一个包，这样两台不同网段的主机就 ping 通了。</div>

案例二 最简单的路由转发拓扑——单臂路由

案例拓扑	 <p>Router1</p> <p>GW E0/0.1 192.168.1.254/24 GW E0/0.2 192.168.2.254/24</p> <p>Trunk</p> <p>SW1</p> <p>Vlan 10</p> <p>PC1 192.168.1.0/24</p> <p>Trunk</p> <p>SW2</p> <p>Vlan 20</p> <p>192.168.2.0/24 PC2</p>
关键知识点	<p>二层转发方式：</p> <ol style="list-style-type: none"> 直通式（Cut Through）：一旦检测到数据包的目的 MAC 地址，即刻查表并作出转发决策，实现交换功能。该方式由于不需要存储，所以转发延迟非常小，但由于不等接收到完整的数据就转发，无法进行错误校验，由于没有缓存，不同速率之间的端口无法通信； 存储转发（Store and Forward）：接收完整的数据包，并进行错误校验，在保证没有错误的情况下，再作出转发决策，该方式时延大，但可以在不同速率之间的端口之间通信，是目前主流交换机通常采用的转发方式； 碎片转发（Fragment Free）：检查数据包的长度，如果小于 64 字节，说明是假包，则丢弃该包；如果大于 64 字节，则转发该包，这种方式也不提供错误校验； <p>三层转发方式：</p> <ol style="list-style-type: none"> 进程交换（Process Switching）：路由器将去掉数据帧的二层报头，然后在路由表中查找每个数据包的三层目的地址，然后用修改后的二层头部封装数据帧，并将其从接口发送出去，这些操作都是由 CPU 处理的，该方式非常消耗 CPU，不推荐使用； 快速交换（Fast Switching）：查看首个数据包的 IP 前缀，再查询路由表之后，将会在快速交换缓存中为这个 IP 前缀创建一个表项，之后再进入的数据包，不会再查表，直接根据缓存中的数据转发； Cisco 快速转发（Cisco Express Forwarding）：启用 CEF 后，路由器将使用 CPU 计算出的表信息（如：路由表和 ARP 表）来创建基于硬件的数据表，这种表就是转发信息库（FIB）和邻接关系表，设备会根据这些表对所有的数据帧（包括第一个数据帧）执行基于硬件的转发决策； <p>CEF 支持以下两种交换方式：</p> <ol style="list-style-type: none"> 集中式转发：由三层引擎做出路由和交换决策，所有数据包都要通过交换矩阵进入中央引擎，因此它的硬件交换性能取决于中央交换引擎和交换矩阵； 分布式转发：中央交换引擎会将 FIB 表和邻接关系表的副本放在各接口或线卡中，因此各个线卡或模块可以独立做出转发决策，而无需中央交换引擎的帮助，数据帧通过交换矩阵直接在端口之间传输，因此，系统性能为所有转发引擎之和；
实	<p>实战目的：理解单臂路由，使用 Router1 来使 PC1 和 PC2 两个不同网段的主机可以通信；</p>

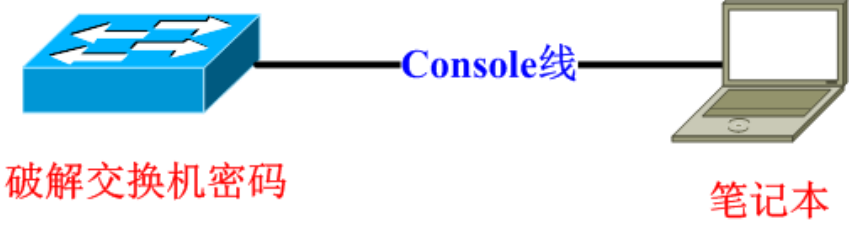
战 需 求	<p>需求一：SW1 有 vlan 10 和 20，配置协议使 SW2 能够学习到这两个 vlan</p> <p>需求二：将 PC1 和 PC2 配置到不同网段和 VLAN 中；</p> <p>需求三：为了使 PC1 能够 ping 通 PC2，需要增加一台 Router1，在不同的网段之间做路由，Router1 与 SW1 相连的接口需要起子接口，PC1 和 PC2 的网关都是子接口的 IP 地址；</p> <p>需求四：为了能够在链路上承载不同的 vlan 的数据包，SW1 和 SW2、SW1 和 Router1 之间的链路都需要配置为干道（Trunk）协议；</p>
配 置 命 令 详 解	<p>子接口配置规则：</p> <pre>interface f0/x</pre> <p>进入物理接口</p> <pre>no shutdown</pre> <p>打开接口</p> <pre>interface f0/x.[1 ~ 410000]</pre> <p>进入子接口</p> <pre>encapsulation dot1Q [vlan ID]</pre> <p>将子接口封装到指定的 vlan 中</p> <pre>ip address [网络地址] [子网掩码]</pre> <p>为子接口配置 IP 地址</p> <p>验证命令：</p> <pre>show ip route</pre> <p>查看 IP 路由表</p>
排 错 思 路	<ol style="list-style-type: none"> 1. 如 SW2 无法学习到 SW1 的 vlan，查看 sw1 和 sw2 之间的链路是否配置为 trunk，查看命令： sh interfaces f0/1 switchport; 2. 如 PC1 或 PC2 无法 ping 通自己的网关，也请检查 sw1 和 sw2 之间的链路是否起 trunk，还要检查 sw1 与 Router1 之间的链路是否起 trunk，并且检查 Router1 子接口是否封装了正确的 vlan，还要检查子接口的物理接口是否 no shutdown; 3. 如 PC1 和 PC2 都分别 ping 通了自己的网关和对方的网关，但互 ping 不同，请确认对方 PC 已经关闭了防火墙功能；

案例三 使用 Telnet/SSH 去管理远程设备

案例拓扑	<div style="text-align: center;"> <p>配置 Telnet/SSH</p>  <p>192.168.1.1</p> <p>192.168.1.10</p> <p>管理客户端</p> </div>
关键知识点	<p>远程登录的需求：很多情况下，你也许不能在设备前使用 console 线来管理，这时就需要通过 telnet 或 SSH 访问其 CLI 远程管理它，为了能够远程访问，必须首先设置虚拟类型终端（VTY）；</p> <p>1.Telnet：基于 TCP 协议，端口号 23，是一组提供远程登录方法的程序，所有传输的信息（包括用户名和密码）都是明文的；</p> <p>2.SSH：基于 TCP 协议，端口号 22，使用 RSA 算法对所有传输的信息（包括用户名和密码）进行加密，另一个优点是其传输的数据是经过压缩的，所以可以加快传输的速度，目前 SSH 存在两种版本（版本 1 和版本 2），版本 1 有一些加密算法存在漏洞，并且已经被破解，攻击者可以插入数据，版本 2 修复了这些漏洞，并且版本 2 可以兼容版本 1；</p>
实战需求	<p>实战目的：配置 sw1，使之能够通过 telnet/SSH 访问，并且限制只有 PC1 的 IP 地址才能够管理</p> <p>需求一：首先确保管理客户端能够 ping 通交换机；</p> <p>需求二：先在交换机上配置 telnet，并配置密码，使 PC 能够通过 telnet 去管理交换机；</p> <p>需求三：在交换机上配置，使客户端需要输入用户和密码才能访问到设备；</p> <p>需求四：配置 ACL，并在 vty 中调用，限制只有某个 IP 地址可以访问该设备；</p> <p>需求五：在设备上启用 SSH 协议，并配置客户端通过 SSH 访问并管理设备；</p>
配置命令详解	<p>控制台（Console）密码配置规则：</p> <pre>line console 0</pre> <p style="text-align: right;">进入控制台管理接口</p> <pre>password [密码]</pre> <p style="text-align: right;">配置控制台密码</p> <pre>login</pre> <p style="text-align: right;">开启登录</p> <p>Telnet 配置规则（只需密码）：</p> <pre>interface vlan [1 ~ 1005]</pre> <p style="text-align: right;">进入 SVI 接口</p> <pre>ip address [网络地址] [子网掩码]</pre> <p style="text-align: right;">为 SVI 接口配置 IP</p> <pre>line vty 0 4</pre> <p style="text-align: right;">进入 VTY 接口配置模式</p> <pre>password [密码]</pre> <p style="text-align: right;">配置只使用密码登录</p> <pre>login</pre> <p style="text-align: right;">打开远程登录，必须敲</p> <p>Telnet 配置规则（需要用户名和密码）：</p> <pre>username [用户名] password [密码]</pre> <p style="text-align: right;">配置本地用户名和密码</p>

	<p>line vty 0 4 login local access-class [ACL 号] in access-list [100 ~ 199] permit ip host [网络地址] any</p> <p>SSH 配置规则：</p> <p>ip domain-name [域名] crypto key generate rsa ip ssh version [1/2] line vty 0 4 login local transport input ssh transport output telnet</p> <p>重要：Cisco 交换机必须配置特权密码，否则 telnet 用户无法进入特权模式；</p> <p>验证命令： show line</p>	<p>进入 VTY 接口配置模式 配置登录时，使用本地用户名和密码进行验证 入方向调用 ACL 配置 ACL，允许指定的 IP 访问该设备 *必须使用扩展 ACL</p> <p>配置域名，要使用 ssh 必须配置该命令 生成密钥 配置 SSH 的版本号 进入 VTY 接口配置模式 配置登录时，使用本地用户名和密码进行验证 允许 ssh 访问进入 允许用 telnet 去访问其他设备</p> <p>查看 VTY 线路状态</p>
排 错 思 路	<p>1. 如 PC1 无法 ping 通交换机的 SVI 接口，首先确保交换机连接 PC1 的接口是否已经划入了 SVI 所属于的 vlan，还有 SVI 接口是否 no shutdown，查看命令：show run</p> <p>2. 如 PC 返回远程登录被拒绝，请确保 vty 接口下有 login，查看命令：show run</p> <p>3. 如可以登录用户模式，但无法进如特权模式，请确保已经配置了特权模式密码</p> <p>4. 如已经配置了 ACL 调用，但无法限制登录 IP，请确保 ACL 的目的地址是 any</p>	

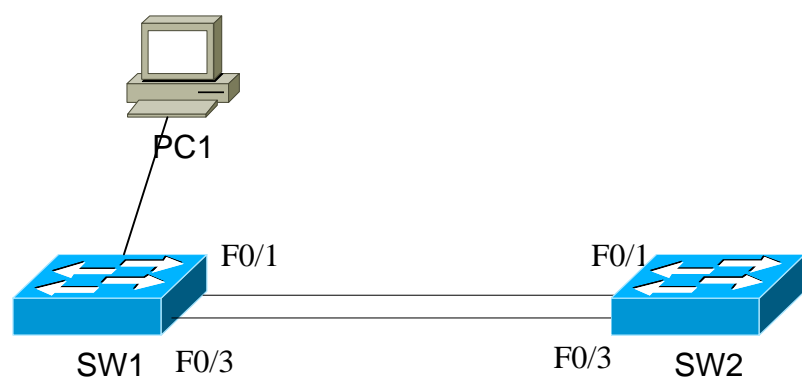
案例四 为交换机灌 IOS 和密码恢复

案例拓扑	<p style="color: red; text-align: center;">丢失IOS的交换机</p>  <p style="color: red; text-align: center;">破解交换机密码</p> <p style="color: red; text-align: center;">笔记本</p>
关键知识点	<p style="color: red;">路由器和交换机在 xmodem 中灌 IOS 的不同点：</p> <p>1.路由器：在 rommon 模式中，你所灌的 IOS 不是传输到路由器的 Flash 中，而是传输到了路由器的 RAM 中，也就是内存中，所有当你通过 Console 上传完 IOS 之后，还需要通过 IP 地址，在把这个 IOS 传输一遍，这个时候是传到路由器的 Flash 中；</p> <p>2.交换机：在 rommon 模式中，你所灌的 IOS 是直接传输到交换机的 Flash 中，因此不需要像路由器那样再灌一遍；</p> <p style="color: red;">路由器和交换机在密码恢复时的不同点：</p> <p>1.路由器：通过修改配置寄存器，可以让路由器启动的时候选择加载或者不加载配置文件，从而达到破解密码的目的；</p> <p>2.交换机：交换机没有配置寄存器的概念，如果想破解密码，必须进入到 rommon 模式下，将交换机的配置文件“config.text”改名，使之无法加载默认的配置文​​件，从而达到破解密码的目的；</p>
实战需求	<p style="color: red;">实战目的：</p> <p>需求一：按照配置步骤，先为交换机灌 IOS；</p> <p>需求二：按照配置步骤，然后为交换机做密码恢复；</p>
配置命令详解	<p>交换机灌 IOS 步骤：</p> <ol style="list-style-type: none"> 1.按住 mode，进入 xmodem 模式 2.输入 flash_init，初始化 Flash 3. dir flash：查看是否完成初始化，是否有 IOS 文件 4. copy xmodem: flash:[/IOS 文件名] 系统出现 C 这个字母后，开始传文件 5.在 SecureCRT 的“传输文件”中选择“send xmodem”，选择要发送 IOS，点击 OK 6.时间比较长，完成后，直接 boot，加载 IOS 文件 <p>交换机密码恢复步骤：</p> <ol style="list-style-type: none"> 1.启动过程中，按交换机面板上的 mode 键 2.看到“switch:”提示符后，输入 flash_init，初始化 flash

	<p>3.通过命令“show flash:”查看文件，看是否有“config.text”这个文件</p> <p>4.使用命令“rename flash:config.text flash:config.old”重命名这个文件</p> <p>5.boot 命令，重启交换机，进入特权模式，再使用上面的命令将文件名修改回来</p> <p>6.执行命令“copy flash:config.text system:running-config”恢复原始配置</p> <p>7.进入全局模式，通过命令“enable password”修改口令</p> <p>8.write 命令，保存配置</p>
排 错 思 路	

案例五 交换网络核心技术——生成树原理

案
例
拓
扑



关
键
知
识
点

什么是 STP： 一种在交换网络中，逻辑上切断一条链路，以避免产生二层环路的一种手段；
常见的 STP 协议：

- 1.CST: 协议号 802.1d，只维护一个 STP 实例，而不管交换机上有多少个 VLAN；
- 2.PVST+: Cisco 私用协议，基于 CST，但会为每个 VLAN 维护一个实例，增加了一些特性；
- 3.RSTP: 协议号 802.1w，只维护一个 STP 实例，但收敛速度加快；
- 4.MSTP: 协议号 802.1s，基于 RSTP，可以将多 VLAN 映射到一个实例中，还支持一些特性；

工作方式： STP 会强制一些端口进入备份状态，使其不会侦听、转发或泛洪数据帧。总的效果是最后只有一条路径能够通向一个网段；如果网络中通往任何一个网段的连通性出现了问题，STP 就会自动激活先前的非活动路径来重建连接（前提是存在冗余路径）；

网桥标识符（BID）的组成： 如下图所示，BID 由下面三部分组成：

Bridge ID - 8 Bytes

Bridge Priority

MAC Address

2 bytes6 bytes

Bridge ID - 8 Bytes

Bridge Priority

Extend System ID

MAC Address

4 bits12 bits48 bits

1.Bridge Priority（网桥优先级）：默认是 32768，取值范围是 0 ~ 65535，每 4096 倍数增长；

2.Extend System ID: 这个值就是 VLAN 号，它会和 Bridge Priority 叠加组成 BID 的第一部分，例如: Bridge Priority 是 32768，VLAN 号是 1，那么 BID 第一部分的值就是 32769；

3.MAC Address: 取设备的 MAC 地址；

端口角色	描述
根端口	这一类端口存在于非根网桥上，它是交换机端口去往根桥的最佳路径。根端口会将数据流转发给根桥，每个网桥上只会有一个根端口；
指定端口	这一类端口即存在于根网桥上，也存在于非根网桥上，对于根网桥来说，所有的端口都将会成为指定端口。对于非根网桥来说，指定端口是需要与交换机之间收发数据帧的端口，每个网段中只能有一个指定端口；
非指定端口	既不是根端口，也不是指定端口的所有其他端口，都将成为非指定端口，非指定端口只能接收，但不能转发数据帧（因为被逻辑上阻塞了）

STP 4 种端口状态：

- 1.Blocking（阻塞状态）
- 2.Listening（侦听状态）

	<p>3.Learning（学习状态）</p> <p>4.Forwarding（转发状态）</p> <p>STP 选举过程：</p> <p>1.选 1 个根网桥：每个 VLAN 或实例中只能有一个根网桥，网桥 ID 最小的将成为根桥，在根桥上所有端口都会成为指定端口，指定端口可以发送和接收流量，还可以发送和接收 BPDU；</p> <p>2.在所有非根桥上选举根端口：STP 将在每个非根网桥上选举 1 个根端口，该端口所连接的路径一定是该网桥到根桥开销最低的路径，选举根端口次序是：cost > 对端 BID > 对端接口 ID；</p> <p>3.在每个网段上选举指定端口：STP 会为每个网段选举一个指定端口，从它到达根网桥的路径开销最低，每个网段只能有一个指定端口，选举次序是：cost > 对端 BID > 对端接口 ID；</p> <p>4.所有其他端口都会被堵塞（B）</p>
实 战 需 求	<p>实战目的：观察认识生成树协议（STP）——最简单的生成树拓扑</p> <p>需求一：SW1 和 SW2 关闭 VLAN 1 的生成树协议，连接一台 PC 并产生一些广播包，观察交换机 CPU 利用率变化情况；</p> <p>需求二：SW1 和 SW2 开启生成树协议，让交换机自动选举根桥（Root Bridge）、根端口（Root Port）、指定端口（Designated Port）、阻塞端口（Blocked Port）；</p> <p>需求三：观察哪一个交换机是根桥，为什么</p> <p>需求四：观察根交换机上的端口都是什么端口</p> <p>需求五：观察与根交换机端口相连的对端交换机端口是什么角色</p> <p>需求六：为什么非根桥上有一个端口被 Block</p>
配 置 命 令 详 解	<p>STP 配置规则：</p> <p>no spanning-tree vlan [vlan ID] 在交换机上关闭 STP 协议</p> <p>show processes cpu 查看交换机 CPU 利用率</p> <p>spanning-tree vlan [vlan ID] priority [0-61440] 改变交换机优先级</p> <p>show spanning-tree 查看网桥优先级（BID），端口角色等</p>
排 错 思 路	1.

案例六 深刻理解生成树协议的工作方式

案例
拓
扑

图 1

图 2

图 3

关
键
知
识
点

以太网二层链路开销：

链路速度	开销（修订的 IEEE 规范）	开销（早先的 IEEE 规范）
10Gbit/s（万兆）	2	1
1G bit/s（千兆）	4	1
100 Mbit/s（百兆）	19	10
10 Mbit/s（十兆）	100	100

RSTP 端口角色：

1. 丢弃（discarding）
2. 学习（Learning）
3. 转发（Forwarding）

RSTP 端口状态：

1. 根端口
2. 指定端口
3. 替代端口（Alternate）
4. 备份端口（Backup）

MSTP 工作机制：

实

实战目的：观察认识生成树协议（STP）——最简单的生成树拓扑

案例七 利用生成树的特性保护根交换机

案例拓扑

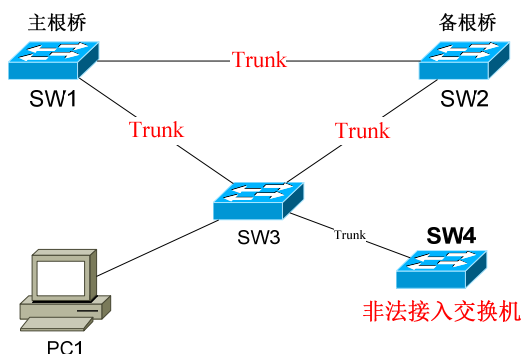


图 1

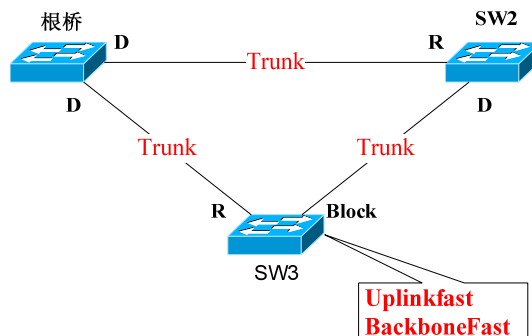
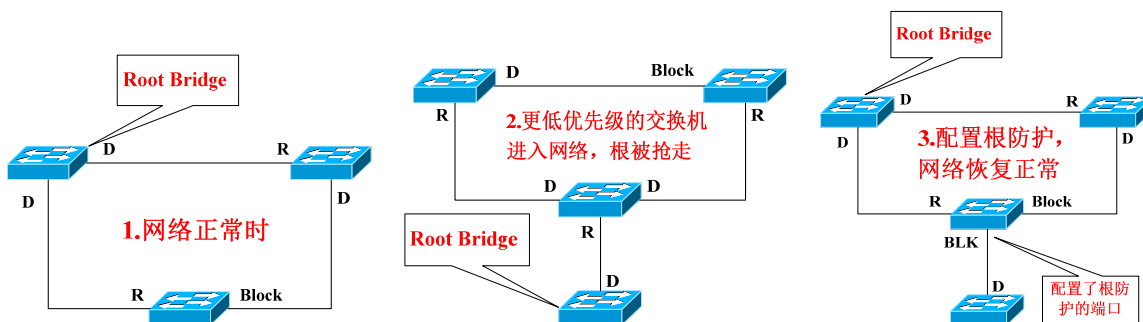


图 2

关键点

生成树的增强特性：

- 1.Portfast**：启用该命令后的端口，将跳过 STP 的 Block、Listening、Learning 的过程，直接进入 Forwarding 状态，只适用于接入层直接连接 PC 的端口，加快收敛时间；
- 2.BPDU Guard (BPDU 防护)**：配置为该模式的端口将不能接收 BPDU 包，一旦收到端口将变为 err-disable 状态，配置在接入层，防止接入非法的交换机，从而抢根；
- 3.BPDU Filter (BPDU 过滤)**：防止交换机在启用了 Portfast 特性的接口上接收和发送 BPDU；
- 4.Root Guard (根防护)**：启用该命令的端口，一旦收到比当前根桥更优的 BPDU 包，将会把这个接口 STP 状态置为 BKN，直到不再收到该类型的 BPDU 包为止，一般配置在接入层；



- 5.环路防护**：启用该命令的端口，在指定时间内，没有收到 BPDU 包后，交换机将把 Block 端口置为“不一致环路”状态，从而防止二层环路发生；
- 6.UDLD (单向链路检测)**：启用该命令后的端口，交换机会定期向邻居发送 UDLD 协议数据包，并且期望收到回应，如果指定之间没有收到，就认为该链路为单向链路，并且将端口关闭；
- 7.UplinkFast**：启用该命令的端口，可以加速选举一个新的根端口，根端口将立即进入转发状态，而不需要经历侦听和学习状态；
- 8.BackboneFast**：当非根桥阻塞端口收到一个劣质的 BPDU 是，将加速该端口从 Block 状态转换为 Forwarding 状态的速度，并且告诉发送劣质 BPDU 包的交换机一个更好的 BPDU；

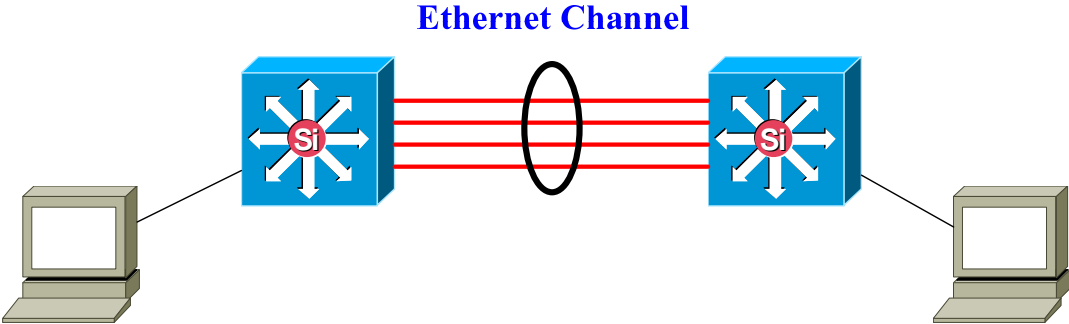
生成树协议的比较：

协议	标准	所需资源	收敛速度	支持特性	实例范围	备注
CST	802.1d	低	50 秒	否	所有 VLAN	已淘汰
PVST+	Cisco	高	50 秒	是	每 VLAN	默认启用
RSTP	802.1w	中	1 秒	否	所有 VLAN	
MSTP	802.1s	中高	1 秒	是	依照实例数量	

实战

实战目的：深入理解 STP 的 Portfast、BPDUGuard、BPDUfilter、RootGuard

案例八 利用 EtherChannel (EC) 增加链路带宽和冗余性

案例拓扑													
关键点	<p>EC 的功能：可以通过将多条物理链路捆绑成为一条逻辑链路的来增加带宽和提供线路冗余；</p> <p>EC 的优点：</p> <ol style="list-style-type: none"> 1.增加带宽：最多可以将 8 个物理接口捆绑为一个逻辑接口，将链路带宽增加 8 倍； 2.实现冗余：由于所有的链路会被看成一条逻辑连接，因此其中某一条物理链路断开并不会给拓扑带来任何的变化，于是 STP 也就没必要重新计算，只要交换机之间还有一条链路是正常的，那么 EC 就会照常工作，尽管的总吞吐量会降低； 3.避免二层环路：EC 能够屏蔽 STP 协议，使 STP 认为这是一条物理线路； 4.负载分担：在同一个 EC 的几条链路上可以实现基于源和目 IP、MAC 或端口的负载分担； <p>重要：EC 不支持捆绑 10M 口；</p> <p>配置相同：EC 既可以捆绑 Trunk，也可以捆绑 Access，但必须保证两端的模式是一样的；</p> <p>支持的协议：</p> <ol style="list-style-type: none"> 1.PAgP：端口汇聚协议是 cisco 私有的协议，PAgP 数据包每 30 秒发送一次； 2.LACP：该协议是 IEEE 标准协议，工作方式与 PAgP 类似； <p>PAgP 和 LACP 的模式：</p> <table border="1" data-bbox="252 1294 1417 1556"> <thead> <tr> <th>模式</th><th>描述</th></tr> </thead> <tbody> <tr> <td>Auto</td><td>在这种模式下，接口会对 PAgP 数据包作出响应，但不主动发起协商；</td></tr> <tr> <td>Desirable</td><td>这种模式下，接口主动发送 PAgP 数据包来主动与其他接口进行协商；</td></tr> <tr> <td>on</td><td>这种模式不使用 PAgP 或 LACP，而强制端口与邻居形成 Etherchannel；</td></tr> <tr> <td>Passive</td><td>被动协商模式，接口对 LACP 数据包作出响应，但不主动发起协商；</td></tr> <tr> <td>Active</td><td>主动协商模式，接口主动发送 LACP 数据包与其他端口进行协商；</td></tr> </tbody> </table> <p>EtherChannel 负责分担：可以配置 EC 根据数据包来自不同的源（MAC、IP、Port）的信息，来作出选择，将数据包从不同的接口转发出去，负责分担可以基于下面这些关键字：</p> <ol style="list-style-type: none"> 1.src-mac：基于源 MAC 地址 2.dst-mac：基于目的 MAC 地址 3.src-dst-mac：基于源和目的 MAC 地址 4.src-ip：基于源 IP 地址 5.dst-ip：基于目的 IP 地址 6.src-dst-ip：基于源和目的 IP 地址 7.src-port：基于源端口 8.dst-port：基于目的端口 9.src-dst-port：基于源和目的端口 	模式	描述	Auto	在这种模式下，接口会对 PAgP 数据包作出响应，但不主动发起协商；	Desirable	这种模式下，接口主动发送 PAgP 数据包来主动与其他接口进行协商；	on	这种模式不使用 PAgP 或 LACP，而强制端口与邻居形成 Etherchannel；	Passive	被动协商模式，接口对 LACP 数据包作出响应，但不主动发起协商；	Active	主动协商模式，接口主动发送 LACP 数据包与其他端口进行协商；
模式	描述												
Auto	在这种模式下，接口会对 PAgP 数据包作出响应，但不主动发起协商；												
Desirable	这种模式下，接口主动发送 PAgP 数据包来主动与其他接口进行协商；												
on	这种模式不使用 PAgP 或 LACP，而强制端口与邻居形成 Etherchannel；												
Passive	被动协商模式，接口对 LACP 数据包作出响应，但不主动发起协商；												
Active	主动协商模式，接口主动发送 LACP 数据包与其他端口进行协商；												
实	<p>实战目的：四个端口逻辑上捆绑成一个 EC，两端主机之间互 ping，依次拔线验证不丢包；</p>												

案例九 【综合实验】实现不丢包转发——MSTP+HSRP

案例
拓
扑

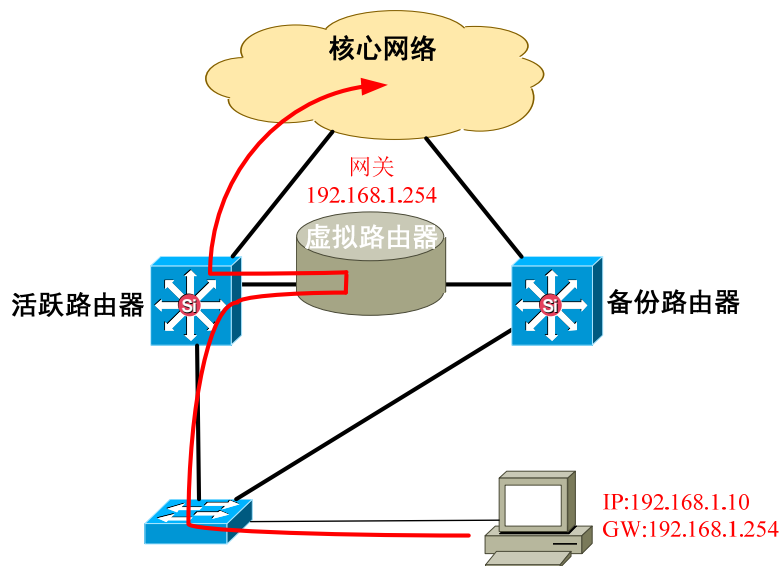
关
键
知
识
点

使用 FHRP 的目的：通常终端设备中配置了默认网关 IP 地址，如果默认网关 IP 地址所属的路由器发生故障，那么本地设备就无法向外网发送数据包了，即使目前网络中有冗余的路由器可以充当该网段的默认网关，也没有任何方法能够使终端设备获得新默认网关的 IP 地址；因此网关对于终端主机的重要性不言而喻，所以你需要确保网关的健壮性和最高的可用性，配置首跳冗余协议（FHRP），例如：HSRP 和 VRRP 是一种好的解决方案；

HSRP 和 VRRP 对比：

HSRP	VRRP
Cisco 私有协议	IEEE 标准协议
最多支持 255 个组	最多支持 255 个组
1 个活跃路由器、1 个备份路由器、若干候选路由器	1 个活跃路由器、若干备份路由器
虚拟 IP 地址与真实 IP 地址不能相同	虚拟 IP 地址与真实 IP 地址可以相同
使用 224.0.0.2 发送 Hello 数据包	使用 224.0.0.18 发送 Hello 数据包
默认计时器：Hello 时间 3 秒，保持时间 10 秒	默认小于 HSRP
可以追踪接口或对象	只能追踪对象
支持认证	支持认证

工作原理：通过让一台路由器充当活跃的网关路由器，而另一台或多台其他路由器则处于备用模式，一旦活跃路由器失效，备用路由器马上就接管它的角色成为活跃路由器，对于局域网中的主机来说它们就是一个虚拟路由器，如下图，两台或多台路由器可以通过共享一个 IP 地址和 MAC 地址，共同维护一个虚拟路由器，因此它可以提供网关的冗余性，且无需在终端设备上进入任何额外的配置；



通信原理：管理员需要把虚拟路由器的 IP 地址配置为该网段主机的默认网关，当主机要把数据帧发往默认网关时，主机会用 ARP 来解析网关 IP 地址所对应的 MAC 地址。ARP 解析会返回虚拟路由器的 MAC 地址。发往虚拟路由器 MAC 地址的数据帧，会由虚拟路由器组中活跃的物理路由器进行处理。而转发流量的过程是对终端主机来说是透明的。

切换过程：活跃和备份路由器之间默认每 3 秒钟使用组播地址 224.0.0.2 UDP 1985 端口交换一次 Hello 消息，组中所有路由器都需要建立 L2 层邻接关系，以此来知晓各自的状态；

情况 1：一旦活跃路由器的链路发生故障（不是路由器之间的链路），活跃路由器就会自动降级，并用 Hello 消息告知备份路由器，备份路由器一旦发现自己的优先级比活跃路由器高，马上就会成为活跃路由器，充当转发路由器的角色；

情况 2：一旦活跃路由器的链路发生故障（路由器之间的链路），备份路由器就不会再收到活跃路由器发出的 Hello 消息，备用路由器就会成为活跃路由器，充当转发路由器的角色；

HSRP 中路由器的角色：

1.虚拟路由器：终端主机上网关 IP 和 MAC 地址的绑定，虚拟路由器并不处理数据帧，一个组只能有一个虚拟路由器；

2.活跃路由器：活跃路由器负责处理所有发送到虚拟路由器地址的数据帧，并将它转发到目的网络，一个组只能有一个活跃路由器；

3.备用路由器：周期性监听 Hello 消息，当活跃路由器发生故障或者自动降级，这时备份路由器就会接替活跃路由器的角色，一个组只能有一个备用路由器；

4.其他路由器：始终保持监听状态（Listen State），当活跃和备用路由器都发生故障，组中其他路由器将会竞争成为活跃或备份路由器，一个组其他路由器可以有多台；

HSRP 中路由器的五种状态：

1.初始（Initial）：未运行 HSRP 时的状态；

2.监听（Listen）：知道虚拟 IP 地址，但既不是活跃路由器，也不是备份路由器，但它会监听 Hello 消息；

3.宣告（Speak）：发送周期性 Hello 消息，参与活跃和备份路由器竞选

4.备用（Standby）：是下一个活跃路由器的候选者，，周期性发送 Hello 消息；

5.活跃（Active）：负责转发虚拟路由器的流量，周期性发送 Hello 消息；

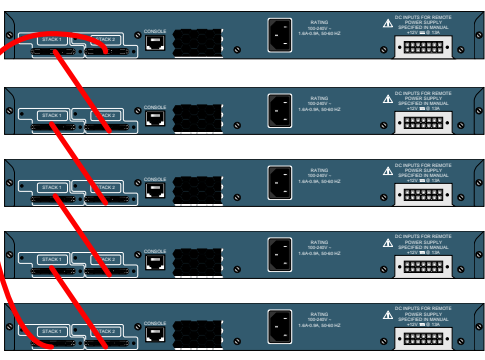
重要 1：当在网络中配置 STP 和 HSRP 时，确保活跃路由器与相应 VLAN 的根网桥相同，否则将会导致次优路径；

HSRP 优先级：具有最高优先级的路由器将成为活跃路由器，如相同则选择拥有最高 IP 地址的；

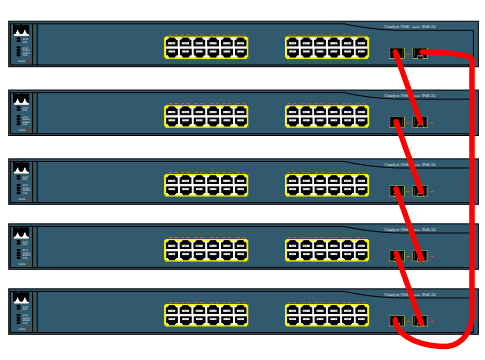
排 错 思 路	<ol style="list-style-type: none">1. 首先排二层错误，查看核心上 STP 端口状态是否正确，主核心和备核心上不能有端口被 Block，否则一定是出现抢根现象，请确保接入层交换机的优先级比主核心和备核心都要低；2. 查看接入层交换机端口状态是否正确，如有问题，请确保接入层的 MST 实例、名字和主用核心一致；3. 如 HSRP 无法完成同步，请确保两个 SVI 接口下面的 HSRP 虚地址一样；4. 如 HSRP 无法自动切换，请确保准对某个 vlan 的主 HSRP 的优先级比备用 HSRP 大 10；5. 如 HSRP 无法自动切换，请确保已经配置了跟踪端口；6. 如 PC 能够 ping 通自己的网关，但无法互相 ping 通，请确保能够 ping 到对方的网关，如不通，请确保在 3560 上已经开启了 ip routing（默认关闭路由功能）；
------------------	---

案例十 堆叠的好处——简化网络管理及增加设备性能

案例拓展



Cisco 3750 堆叠方式



H3C 3600 堆叠方式

关键点

级联的定义：是使用双绞线通过交换机的某个端口与其它交换机相连的，由于它的简单，所有级联可以在任何网络设备厂家的交换机之间完成；优点是：增加网络的连接距离，而缺点则是管理麻烦，容易产生链路瓶颈的问题；

堆叠的定义：是使用专用的堆叠端口和堆叠线缆，将交换机之间的背板连接起来的，它是一种建立在芯片级上的连接，堆叠只有在自己厂家的设备之间，且此设备必须具有堆叠功能才可实现，多台交换机堆叠在一起，从逻辑上来说，它们属于同一个设备，连接到任何一台设备上，都可以管理所有设备；

支持设备堆叠的主流厂家：

主流厂家	Cisco	H3C
支持型号	Catalyst 3750	S3600/5600
堆叠数量	9 台	8 台
堆叠总带宽	32 或 64G	4G

Cisco 堆叠注意事项：



3750 采用的是背板堆叠的方式，所以它是真堆叠，机器本身有堆叠口需专门的堆叠线可以达到 32G 带宽。交换机堆叠后，从逻辑上来说，它们属于同一个设备。这样，如果你想对这几台交换机进行设置，只要连接到任何一台设备上，就可看到堆叠中的其他交换机。

- 1.设备 IOS 版本、系统名称必须相同
- 2.Cisco 允许在不同型号的 3750 交换机之间做堆叠
- 2.堆叠时有主从关系，先开 Master 交换机，再开 Slave 交换机
- 3.堆叠使用后面板专用的 Stack 模块和堆叠线缆
- 4.信号灯变黄后，表示堆叠成功

H3C 堆叠注意事项：

S3600/5600 采用现有的光口做堆叠，所以它是假堆叠，堆叠线既可以采用专用的 H3C 专用堆叠线缆，也可以使用普通的光纤，采用堆叠组的概念，每个交换机有两个堆叠组，同时只能有一个堆叠组运行，堆叠成功后，将多台设备，逻辑上融合成为一台，在任何设备上，都能看到全部设备的配置，并且只有一个 IP；

- 1.设备 VRF 版本、设备名称和配置必须一致
- 2.堆叠 SFP 模块使用现有的光口
- 3.使用专用的 SFP 堆叠线缆
- 4.堆叠端口需要成对使用，即 1 和 2 一组，3 和 4 一组
- 5.所有设备同一时刻只能有一个堆叠组运行

	<p>6.当堆叠端口灯从绿色变为黄色，代表堆叠成功</p> <p>7. H3C 与 Quidway 品牌的交换机不能混合堆叠，SI 与 EI 系列设备也无法混合堆叠</p>
实战需求	<p>实战目的：配置 H3C 交换机，将 3 台交换机堆叠起来，方便管理和维护；</p> <p>需求一：使用 H3C 专用堆叠线缆，将 3 台交换机的背板连接起来，实现增加交换容量、增加端口数量、方便管理和维护的目的；</p> <p>需求二：所有堆叠端口最终变为黄色，标志堆叠成功，插入任何一台交换机的 console 口，都能管理所有三台交换机的配置；</p>
配置命令详解	<p>Cisco 堆叠配置规则：</p> <p>情况 1：如叠设备型号相同，只需按上图将交换机堆叠起来即可，不需要任何配置</p> <p>1.设备按照上图连接，方法为 master 的 stack1 接口连接到 slave 的 stack2 接口上；</p> <p>2.开 master，不作任何的配置，等完全启动后，开 slave 的机器，不作任何的配置</p> <p>3.堆叠信号灯变黄后，表示堆叠成功</p> <p>情况 2：如叠设备型号不相同，除了要按照上图连接设备之外，还需要做如下的配置</p>  <p>1.统一所有设备的 IOS 版本；</p> <p>2.指定要堆叠设备的型号</p> <p>3.指定堆叠的优先级</p> <p>以上图 3 台交换机为例型号分别为，WS-C3750G-24TS、WS-C3750G-24TS、WS-C3750G-48TS 交换机 1 做为主交换 配置如下：</p> <pre>switch 1 provision ws-c3750g-24ts</pre> <p>指定设备型号</p> <pre>switch 1 priority 15</pre> <p>指定设备优先级</p> <pre>switch 2 provision ws-c3750g-24ts</pre> <pre>switch 2 priority 14</pre> <pre>switch 3 provision ws-c3750g-48ts</pre> <pre>switch 3 priority 13</pre> <pre>copy running-config startup-config</pre> <p>（保存配置在这里不要用 wr）</p> <p>其他交换机做为从交换，不需要任何配置，先启动主，再启动其他从交换机，就可以了；</p> <p>H3C 堆叠配置规则：</p> <p>H3C 堆叠在堆叠时，即使型号一样，也需要一些配置命令，配置方法如下：</p>  <p>1.指定所要堆叠的端口号</p> <p>2.指定交换机序号（槽位号）可选</p> <p>以上图 3 台交换机为例：</p> <p>交换机 1 配置： fabric-port g1/1/1 enable</p> <p>指定堆叠端口号 g1/1/1</p> <p>fabric-port g1/1/2 enable</p> <p>指定堆叠端口号 g1/1/2</p> <p>交换机 2 配置： fabric-port g1/1/1 enable</p> <p>fabric-port g1/1/2 enable</p>

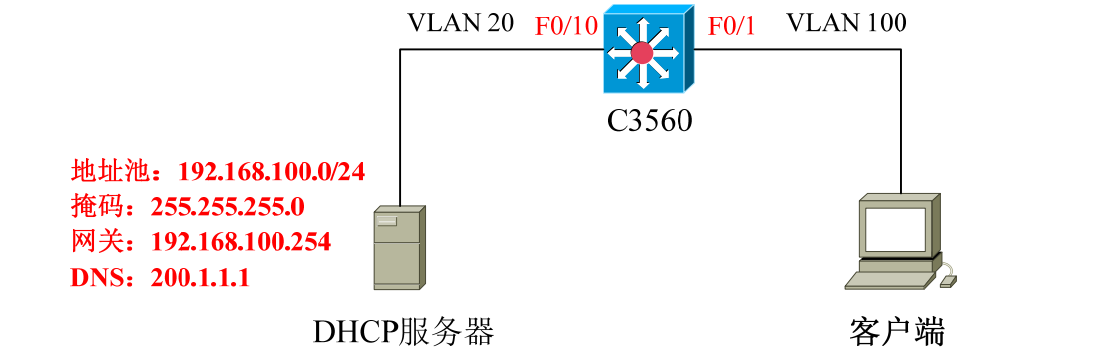
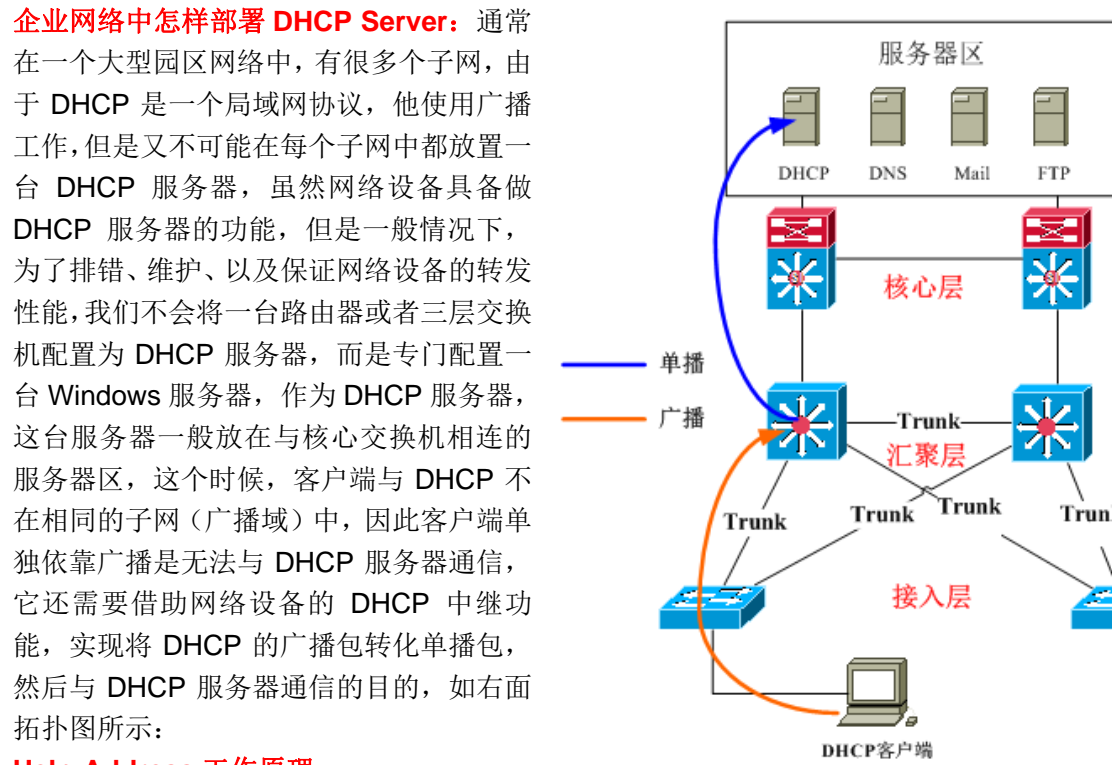
	<div>change unit-id 1 to 2指定交换机序号为 2</div> <div>交换机 3 配置：fabric-port g1/1/1 enable</div> <div> fabric-port g1/1/2 enable</div> <div> change unit-id 1 to 3指定交换机序号为 3</div> <div>PS1：交换机名称一定要一样</div> <div>PS2：如不指定交换机序号，交换机会自己协商并计算一个唯一的序号</div> <div>查看命令：</div> <div>show platform stack-manager all显示所有交换堆叠的信息</div> <div>show switch显示堆叠交换机的汇总信息</div> <div>show switch 1显示一号交换机的信息</div> <div>show switch detail显示堆叠成员明细的信息</div> <div>show switch neighbors显示堆叠邻居的完整信息</div> <div>show switch stack-ports显示堆叠交换机的完整端口信息</div>
排 错 思 路	<div>1. 如交换机始终无法完成同步，确保你所要堆叠的所有交换机名字都一样；</div> <div>2. H3C 交换机堆叠规则是，一个交换机只能起一个堆叠组，1、2 口为一个堆叠组，3、4 口为一个堆叠组；</div>

案例十一 在网络设备上提供 DHCP 服务

案例拓扑	<div><div><div><div><div>VLAN 100: 192.168.100.254</div><div>地址池: 192.168.100.0/24</div><div>掩码: 255.255.255.0</div><div>网关: 192.168.100.254</div><div>DNS: 200.1.1.1</div></div><div><div>VLAN 200: 192.168.200.254</div><div>地址池: 192.168.200.0/24</div><div>掩码: 255.255.255.0</div><div>网关: 192.168.200.254</div><div>DNS: 200.1.1.1</div></div></div><div><div><div><div><div></div><div>DHCP</div></div><div><div>VLAN 100</div><div>VLAN 200</div></div></div><div><div><div>PC1</div><div>PC2</div></div></div></div></div></div></div>
关键点	<div><p>什么是 DHCP（动态主机配置协议）：是一个局域网的网络协议，使用 UDP 协议工作，主要有两个用途：1.给内部网络主机自动分配 IP 地址。2.对内网主机的 IP 地址做集中管理。DHCP 分两部分，一个是服务器端，而另一个是客户端，所有的 IP 网络数据都由 DHCP 服务器集中管理，并负责处理客户端的 DHCP 请求，客户端除了会从服务器获得的 IP 地址外，还将从服务器获得默认网关（Gateway）、掩码（netmask）和 DNS 地址等信息，而在客户端上面，除了将 DHCP 选项打勾之外，无需做任何的配置。DHCP 提供如下三种 IP 主机分配方式：</p><p>1.手动分配：管理员为某些特定主机绑定固定 IP 地址，且永远不会过期</p><p>2.自动分配：一旦客户端从 DHCP 服务器租用到一个 IP 地址之后，就永远使用这个地址；</p><p>3.动态分配：当客户端获取到一个 IP 地址后，并非永久的使用该地址，只要租约到期，就要释放这个地址，当然它有优先续约权；</p><p>DHCP 工作原理：</p><p>1.DHCP Discover（寻找 Server）：当客户端首次登录网络时，它会向网络发出一个 DHCP Discover 的封包，如下图第一步，由于客户端不知道自己属于哪一个网络，所以封包的源地址会为 0.0.0.0，而目的地址则为 255.255.255.255，然后向网络进行广播。默认情况下，Discover 封包的等待时间为 1 秒，若得不到响应的情况下，客户端一共有四 Discover 广播（包括第一次在内），除了第一次会等待 1 秒之外，其余三次的等待时间分别是 9、13、16 秒。</p><p>2.DHCP Offer（提供 IP 地址租约）：当 DHCP 服务器在端口（UDP 67）上监听到客户端发出的 Discover 广播后，它会从那些还没有租出的地址范围内，选择最前面的空置 IP，连同其它 TCP/IP 信息，响应给客户端一个 Offer 的封包。由于客户端在开始的时候还没有 IP 地址，所以在其 Discover 封包内会带有其 MAC 地址信息，并且有一个 XID 编号来辨别该封包，DHCP 服务器响应的 Offer 封包会根据这些资料传递给要求租约的客户。</p><div><div><div><div><div>① DHCP Discover</div><div>DHCP Offer ②</div><div>③ DHCP Request</div><div>DHCP ACK ④</div></div><div><div><div>客户端</div><div>DHCP服务器</div></div></div></div></div><p>3.DHCP Request（接受 IP 地址租约）：如果收到多个 Offer，客户端通常会选最先抵达的那个，并且会向网络发送一个 Request 广播封包，告诉所有 DHCP 服务器它将接受哪一台服务器提供</p></div></div>

	<p>的 IP 地址。同时，客户端还会向网络发送一个 ARP 封包，查询网络上有没有其它机器使用该 IP 地址；如果发现该 IP 已经被占用，客户端则会送出一个 Declient 封包给 DHCP 服务器，拒绝接受其 offer，并重新发送 Discover 信息。事实上，主动权永远在客户端这边。</p> <p>4.DHCP ACK (租约确认)：当 DHCP 服务器接收到客户端的 Request 之后，会向客户端发出一个 ACK 响应，以确认 IP 租约的正式生效，也就结束了一个完整的 DHCP 工作过程。</p> <p>注意：一旦 DHCP 客户端从服务器那里取得 DHCP 租约之后，除非其租约已经失效，否则就无需再发送 DHCP Discover 信息了，而会直接使用已经租用到的 IP 地址向 DHCP 服务器发出 DHCP Request 信息，如果没问题，将直接回应 DHCP ACK 来确认。如果该地址已经失效或已经被其它机器使用了，服务器则会响应一个 DHCP NACK 封包给客户端，要求其重新执行 DHCP Discover。</p>																
实战需求	实战目的： 配置交换机能够实现 DHCP 功能，为 PC1 和 PC2 分配地址；																
	<p>需求一：如上图拓扑，将交换机配置为 DHCP 服务器，下发 IP 地址、网关、DNS 等信息；</p> <p>需求二：使用三层交换机起两个 SVI 接口，将 PC1 和 PC2 端口划入相应的 VLAN 中；</p> <p>需求三：按照拓扑图的信息，配置 DHCP 地址池，为 PC1 分配 192.168.100.0/24 网段的地址，为 PC2 分配 192.168.200.0/24 网段的地址；</p>																
配置命令详解	<p>DHCP 配置规则：</p> <table border="0"> <tr> <td>ip dhcp pool [名字]</td><td>定义地址池</td></tr> <tr> <td>network [网段] [掩码]</td><td>定义地址池的网段</td></tr> <tr> <td>default-router [默认网关]</td><td>定义网关地址</td></tr> <tr> <td>dns-server [域名服务器]</td><td>定义 DNS 服务器</td></tr> <tr> <td>lease [地址租用时间]</td><td>定义租用时间</td></tr> <tr> <td>ip dhcp excluded-address [排除地址]</td><td>定义排除地址</td></tr> </table> <p>查看命令：</p> <table border="0"> <tr> <td>sh ip dhcp pool</td><td>查看地址池信息</td></tr> <tr> <td>sh ip dhcp binding</td><td>查看地址绑定信息</td></tr> </table>	ip dhcp pool [名字]	定义地址池	network [网段] [掩码]	定义地址池的网段	default-router [默认网关]	定义网关地址	dns-server [域名服务器]	定义 DNS 服务器	lease [地址租用时间]	定义租用时间	ip dhcp excluded-address [排除地址]	定义排除地址	sh ip dhcp pool	查看地址池信息	sh ip dhcp binding	查看地址绑定信息
ip dhcp pool [名字]	定义地址池																
network [网段] [掩码]	定义地址池的网段																
default-router [默认网关]	定义网关地址																
dns-server [域名服务器]	定义 DNS 服务器																
lease [地址租用时间]	定义租用时间																
ip dhcp excluded-address [排除地址]	定义排除地址																
sh ip dhcp pool	查看地址池信息																
sh ip dhcp binding	查看地址绑定信息																
排错思路	<p>1. 如无法下发地址，请确保有匹配的 SVI 接口地址；</p> <p>1. 如无法下发地址，请确保连接 PC 的端口，已经划分到正确的 vlan 中，查看命令：sh vlan</p>																

案例十二 在企业网中跨网段部署 DHCP 的方式

案例 拓 扑	 <p>地址池：192.168.100.0/24 掩码：255.255.255.0 网关：192.168.100.254 DNS：200.1.1.1</p> <p>DHCP服务器</p> <p>客户端</p>
关 键 知 识 点	<p>企业网络中怎样部署 DHCP Server：通常在一个大型园区网络中，有很多个子网，由于 DHCP 是一个局域网协议，他使用广播工作，但是又不可能在每个子网中都放置一台 DHCP 服务器，虽然网络设备具备做 DHCP 服务器的功能，但是一般情况下，为了排错、维护、以及保证网络设备的转发性能，我们不会将一台路由器或者三层交换机配置为 DHCP 服务器，而是专门配置一台 Windows 服务器，作为 DHCP 服务器，这台服务器一般放在与核心交换机相连的服务器区，这个时候，客户端与 DHCP 不在相同的子网（广播域）中，因此客户端单独依靠广播是无法与 DHCP 服务器通信，它还需要借助网络设备的 DHCP 中继功能，实现将 DHCP 的广播包转化单播包，然后与 DHCP 服务器通信的目的，如右面拓扑图所示：</p> <p>Help-Address 工作原理：</p> <p>要现实广播转单播，我们需要借助于网络设备的 Helper-Address 功能，由于 DHCP Discover 是以广播方式进行的，其情形只能在同一网络之内进行，因此路由器是不会将广播传送出去的。因此这种情形下 DHCP Discover 是永远没办法抵达位于另一网段 DHCP 服务器的，当然也不会发生 Offer 及其它动作了。要解决这个问题，我们可以让网络设备来接管客户的 DHCP 请求，然后将此请求使用单播方式传递给真正的 DHCP 服务器，然后再将服务器的回复传递给客户。</p> 
实 战 需 求	<p>实战目的：配置交换机的帮助地址功能，验证广播转单播的功能，使 PC1 能够获取 IP 地址</p> <p>需求一：在三层交换机上起两个 SVI 接口，开启路由功能；</p> <p>需求二：分别将 PC1 和 DHCP 服务器划入不同的 vlan 中；</p> <p>需求三：配置 DHCP 服务器，使之能够为 PC1 分配 192.168.200.0/24 的地址段；</p> <p>需求四：在交换机上的 SVI 接口启用 helper-address，目的地址是 DHCP 地址；</p>

配置命令详解

交换机 Help-Address 配置规则：

Interface f0/x

ip helper-address [DHCP 服务器地址]

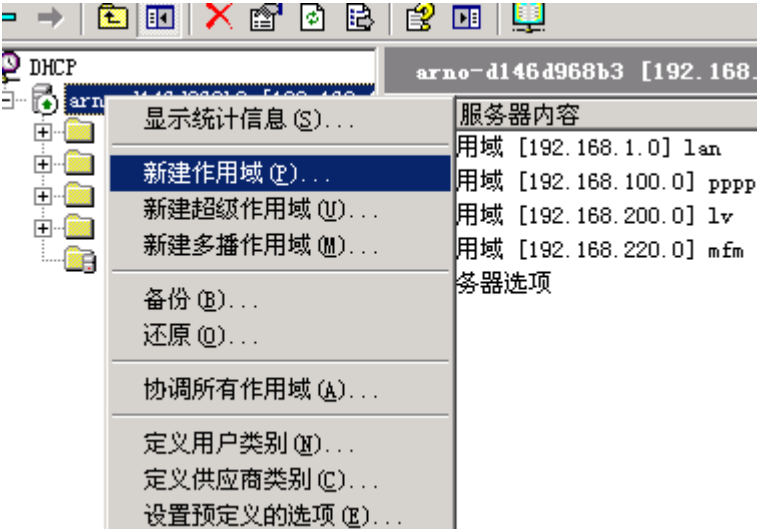
在接口下配置 helper-address，指定 DHCP Server

Windows 2003 DHCP 配置：

1. 首先确保你的 windows 2000/2003 server 已经安装了 DHCP 功能，如果没有，请在添加删除中开启；
2. 在控制面板中的管理工具里面，打开 DHCP，如下图：



3. 右键单击，新建作用域



4. 下一步，名称“任意”，地址范围：指定你所有要分配的地址空间；

新建作用域向导

IP 地址范围

您通过确定一组连续的 IP 地址来定义作用域地址范围。

输入此作用域分配的地址范围。

起始 IP 地址 (S):

192.168.100.1

结束 IP 地址 (E):

192.168.100.253

子网掩码定义 IP 地址的多少位用作网络/子网 ID，多少位用作主机 ID。您可以用长度或 IP 地址来指定子网掩码。

长度 (L):

24

子网掩码 (U):

255.255.255.0

5. 下一步，添加排除地址：指定该地址段中，你不想分配的地址，完成后添加（可选）；

新建作用域向导

添加排除

排除是指服务器不分配的地址或地址范围。

键入您想要排除的 IP 地址范围。如果您想排除一个单独的地址，则“起始 IP 地址”键入地址。

起始 IP 地址 (S):

结束 IP 地址 (E):

添加 (A)

排除的地址范围 (C):

192.168.101.33 到 192.168.101.34

删除 (D)

6. 下一步，配置 DHCP 选项：指定默认网关和 DNS；

新建作用域向导

配置 DHCP 选项

您必须配置最常用的 DHCP 选项之后，客户端才可以使用作用域。

当客户端获得一个地址时，它也被指定了 DHCP 选项，例如路由器（默认的 IP 地址，DNS 服务器，和此作用域的 WINS 设置。

您选择的设置应用于此作用域，这些设置将覆盖此服务器的“服务器选项”文件夹中的设置。

您想现在为此作用域配置 DHCP 选项吗？

- ☒ 是，我想现在配置这些选项 (Y)
- ☐ 否，我想稍后配置这些选项 (N)

7. 下一步，指定为 PC 分配的默认网关，一般是你交换机的 SVI 接口地址，完成后添加；

新建作用域向导

路由器 (默认网关)

您可为指定此作用域要分配的路由器或默认网关。

要添加客户端使用的路由器的 IP 地址，请在下面输入地址。

IP 地址 (I):

| . . .

添加 (A)

192.168.101.254

删除 (R)

上移 (U)

下移 (D)

8. 下一步，指定为 PC 分配的 DNS 地址，完成后添加；

新建作用域向导

域名称和 DNS 服务器

域名系统 (DNS) 映射并转换网络上的客户端计算机使用的域名称。

您可以指定网络上的客户端计算机用来进行 DNS 名称解析时使用的父域。

父域 (P):

要配置作用域客户端使用网络上的 DNS 服务器，请输入那些服务器的 IP 地址。

服务器名 (S):

解析 (R)

IP 地址 (I):

| . . .

202.192.168.1

添加 (A)

删除 (R)

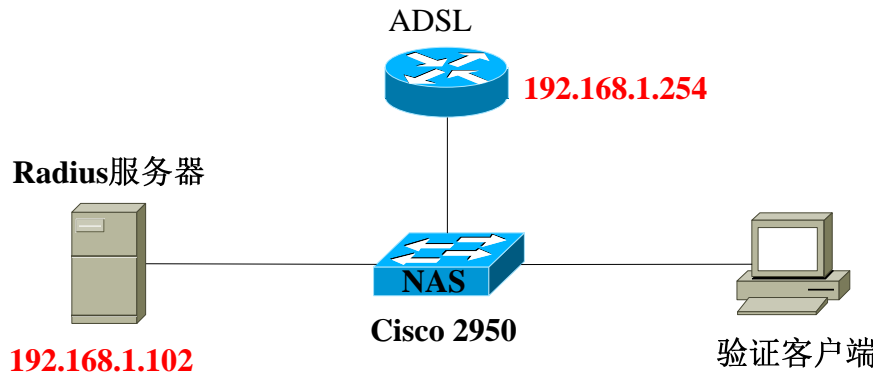
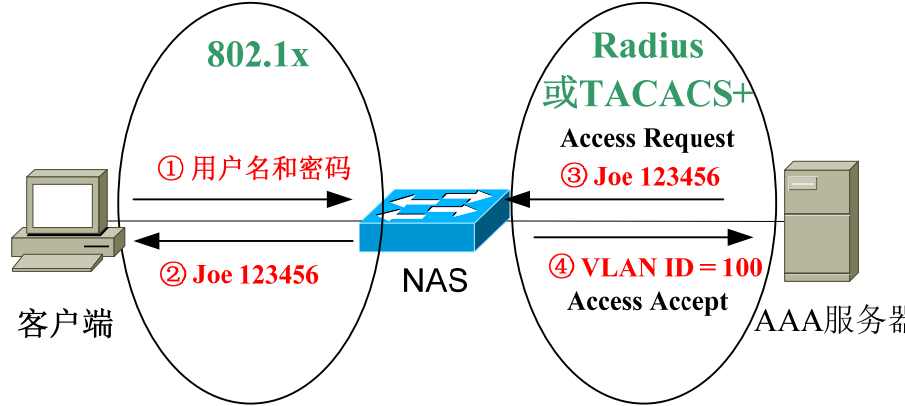
上移 (U)

下移 (D)

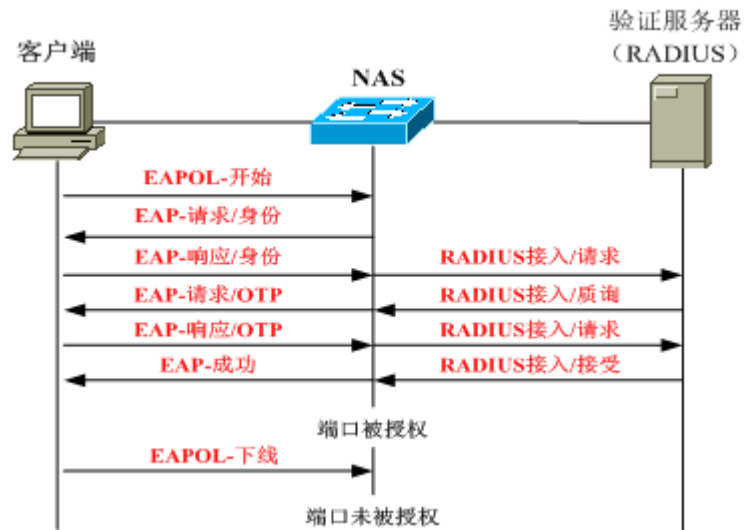
9. WINS 服务器不用配置，下一步激活该作用域；

排 错 思 路	<ol style="list-style-type: none">1. 首先确保手动为 PC 配备地址后，PC 可以 ping 通 DHCP，如无法 ping 通，请确保三层交换机已开启了 ip routing 功能；2. 如无法下发地址，请确保 SVI 接口上已经配置了 helper-address，并且地址是 DHCP 地址；
------------------	--

案例十三 在企业网中部署 AAA 服务器

案例拓扑	
关键点	<p>什么是 AAA： 定义了如何在网络设备上配置基于安全的访问控制框架，AAA 是一个体系结构框架，用来指导管理员以统一的方式配置三种独立的安全功能：</p> <ul style="list-style-type: none">1.Authentication（认证）： 在用户访问网络和网络服务前确认用户的身份，用户需要提供诸如用户名、密码和指纹等信息来提交给服务器进行审核；2.Authorization（授权）： 基于一个中央数据库，来授予用户能够访问资源的级别，分配给用户能够拥有的权限，并且限制用户能够做什么事，不能够做什么事；3.Accounting（审计）： 记录用户登陆后，所做的一切行为，登陆的起始时间，执行过的命令，通信的数据包数和字节数； <p>为什么使用 AAA： 网络运行 AAA 认证，能让管理员集中管理网络设备，控制他们的权限，监控他们的行为，但在网络中实施 AAA 认证，还有如下的考虑：</p> <ul style="list-style-type: none">1.内网安全： 提高内网通信的安全性，防止未授权的用户访问内网；2.终端数量： 接入网络的用户增多，管理员需要为每个用户分配合适的访问权限；3.网络管理： 内网使用终端的人员变动频繁，将极大的增加网络管理员的工作量；4.审计信息： 用户对内网的一些关键性设备和资料的操作，需要做记录和审核。  <p>什么是 NAS（Network Access Server）： NAS 就是网络访问服务器的简称，它可以是一台交换机也可以是路由器，它负责将用户提交的验证信息转发给 AAA 服务器，再负责将 AAA 的服务器的回复信息，转发给用户，它承担着中间人的角色（如上图所示），因此交换机需要一些协议才能支持上面两种角色的转换，下面是这两种协议的介绍：</p> <ul style="list-style-type: none">1.IEEE 802.1x： 它是客户端与 NAS 之间的一种认证协议，客户端需要支持 802.1x 功能，才能与 NAS 进行通信，在客户端没有通过认证之前，交换机将只接受认证身份认证协议（EAPOL）的流量通过（如右图所示），认证成功以后，才会接收其他的流量；

2.RADIUS: 它是 AAA 服务器与 NAS 之间的一种通信协议,NAS 使用 Radius 协议将用户的验证信息转发给 AAA 服务器,服务器也会使用 Radius 协议将一些配置信息传递给 NAS, NAS 根据这些配置信息对客户端的访问权限作出控制,如右图所示:



两大 AAA 通信协议:

1.Radius: IETF 标准协议, 目前使用最为广泛。

2.TACACS+: Cisco 私有协议, 很少使用;

	TACACS+	Radius
端口号	TCP:49	UDP: 旧端口 authen/author 1645 accout 1646 新端口 authen/author 1812 accout 1813
CPU 及内存消耗	多	少
加密方式	加密整个包	只加密密码部分
标准	Cisco 私有协议	IETF 标准协议

企业网 AAA 常见部署拓扑:

为了保障 AAA 服务器的独立性和安全性,在企业网中, AAA 服务器一般放置在服务器区,在 AAA 服务器上安装有支持 Radius 协议的认证软件,例如: Cisco ACS;

接入服务器作为 NAS, 需要配置管理 IP, 并且与 AAA 服务器进行通信, 管理员需要在 AAA 服务器上需要把 NAS 设备的 IP 地址加入到列表中, 以授权这台设备与自己通信的权利;

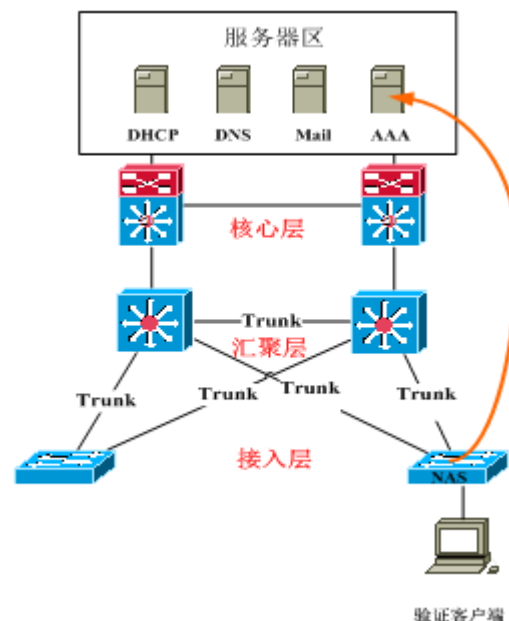
网络设备做 AAA 认证的注意事项:

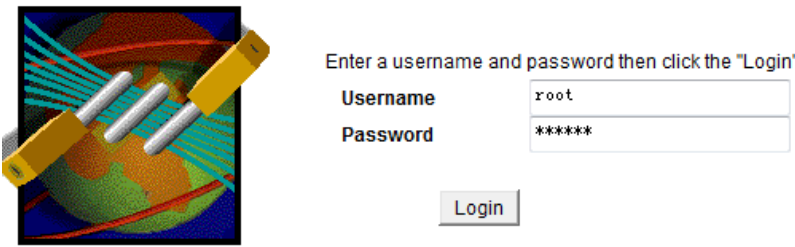
- 1.本地配置: 验证没问题后, 再存盘
- 2.telnet 配置: 先保留一个 session 在里面, 另一个 session 用来测试, 以便回退。

AAA 服务器运行条件:

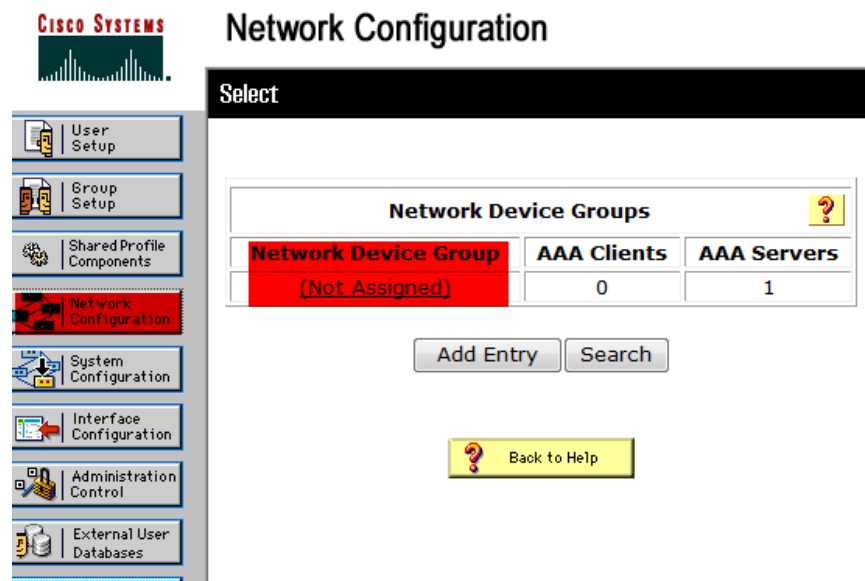
- 1.Windows 2000 Server 或 2003 Server 版本
- 2.安全 Java 运行环境

Cisco 安全访问控制服务器 (ACS): ACS 是 Cisco 的一套软件, 它可以基于 Radius 和 Tacacs+ 对客户端进行认证、授权和审计;

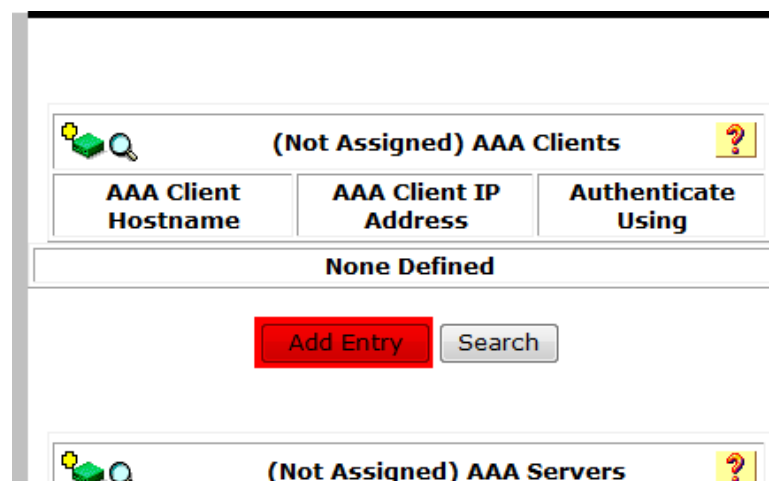


<p>实 战 需 求</p>	<p>实战目的：配置 AAA 服务器，使认证成功用户，能够正常访问网络；</p> <p>需求一：配置连接用户 PC 的交换机成为 NAS，启用 AAA 认证功能，并且在接口启用 802.1x 功能，用户 PC 上启用 802.1x 认证功能，能够接收交换机的认证信息；</p> <p>需求二：在一台 Windows 2003 服务器上安全 Cisco ACS，配置它成为网络中的 Radius 服务器，并按照下面的配置规则，配置 NAS 地址、建立用户和授权用户通过认证后，所能分配到的 VLAN ID；</p> <p>注意：因为实验网络都串联在公司局域网中，默认是 VLAN 1，所以在下发 VLAN 时 VLAN ID 一定要是 1，否则用户获取不到 IP；</p>
<p>配 置 命 令 详 解</p>	<p>接入交换机（NAS）配置规则：</p> <pre> aaa new-model aaa authentication dot1x default group radius aaa authorization network default group radius dot1x system-auth-control dot1x guest-vlan supplication radius-server host [服务器 IP] key [密码] interface f0/x switchport mode access dot1x port-control auto dot1x guest-vlan [VLAN ID] dot1x auth-fail vlan [VLAN ID] test aaa group radius [用户名] [密码] </pre> <p>全局启用 AAA 认证功能</p> <p>dot1x 使用 radius 服务器来认证</p> <p>使用 radius 服务器来做网络授权</p> <p>全局启用 dot1x 功能</p> <p>启用 guest-vlan 功能</p> <p>配置 AAA 服务器 IP 地址和连接密码</p> <p>接口模式为 access，必须先打</p> <p>接口启用 802.1x 验证功能</p> <p>配置 guest-vlan</p> <p>配置认证失败的 vlan</p> <p>特权下测试 AAA 服务器连通性 没命令但可以打</p> <p>Cisco ACS 配置规则：</p> <p>1. 使用用户名和密码登录 ACS，本实验室地址为：http://192.168.1.102:2002</p> <p>should see a Username and Password field. If you cannot see t. enable Java support in your browser.</p> <div data-bbox="287 1568 1085 1814">  </div> <p>2. 选择左侧的 Network Configuration（网络配置），然后点击右侧的 Network Device Group 中</p>

的 Not Assigned, 进入 AAA 设备组中;



3. 在 AAA Clients 中, 点击添加 Add Entry



4. AAA Client Hostname: 任意

AAA Client IP Address: 是指你连接用户 PC, 做认证的交换机的管理 IP 地址, 一定要匹配

Key: 连接 AAA 服务器的密码, 这个密码要与交换机上 radius-server 命令后面的一致

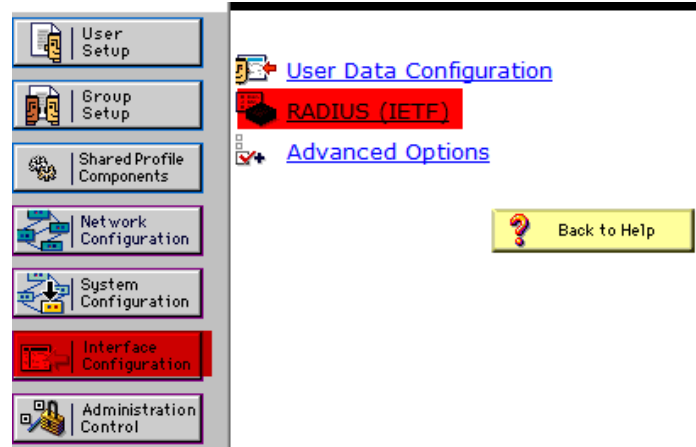
Authenticate Using: 认证方式, 使用 RADIUS (IETF)

最后点击 Submit+Apply, 保存并应用该配置

Add AAA Client

AAA Client Hostname	<input type="text" value="test123"/>
AAA Client IP Address	<input type="text" value="192.168.1.x"/>
Key	<input type="text" value="test123"/>
Network Device Group	<input type="text" value="(Not Assigned)"/>
Authenticate Using	<input type="text" value="RADIUS (IETF)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	

5. 选择左侧的 Interface Configuration（接口配置），然后点击右侧的 RADIUS（IETF）；



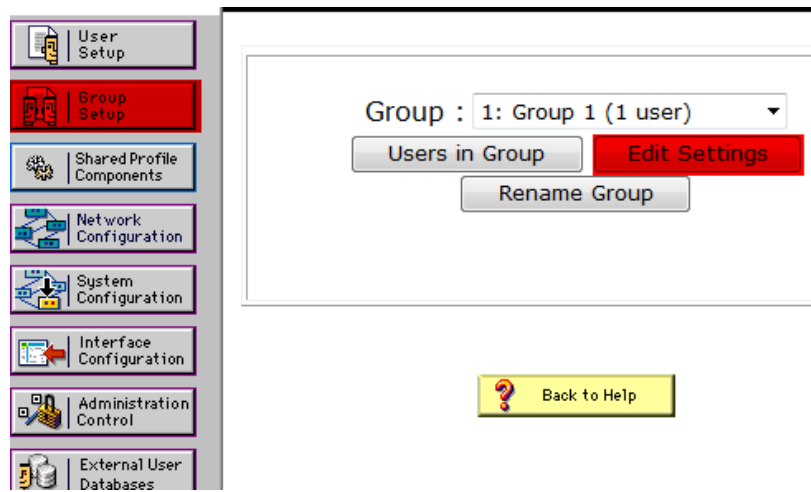
6. 进入 RADIUS（IETF），勾选 064、065、081；

- ☐ ☒ [064] Tunnel-Type
- ☐ ☒ [065] Tunnel-Medium-Type
- ☐ ☐ [066] Tunnel-Client-Endpoint
- ☐ ☐ [067] Tunnel-Server-Endpoint
- ☐ ☐ [069] Tunnel-Password
- ☐ ☐ [071] ARAP-Features
- ☐ ☐ [072] ARAP-Zone-Access
- ☐ ☐ [078] Configuration-Token
- ☐ ☒ [081] Tunnel-Private-Group-ID

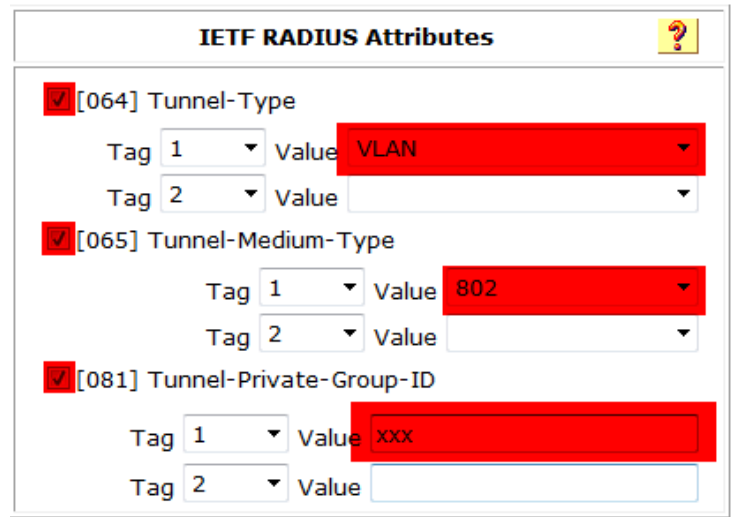
7. 选择左侧的 User Setup (用户设置), 在右侧 User 中输入你要建立的用户名, 然后点击 Add;

8. 在 Password Authentication 下面, 输入密码, 并且选择你要加入的组, 然后点击 submit;

9. 选择左侧的 Group Setup (组设置), 选择你刚刚加入的组, 点击 Edit Settings, 修改组设置;



10. 将滚动条拉到最后, 勾选 064, value 是 vlan, 勾选 065, value 是 802, 勾选 081, value 是你所要下发的 vlan 号, 例如你的 IP 地址属于 vlan 100, 那就输入 100;



排
错
思
路

1. 首先确保你的 NAS 交换机能够 ping 通 AAA 服务器;
2. 如验证无法通过, 请确保你的 ACS 上的 AAA 客户端的地址和密码与你的交换机匹配;
3. 如连接 PC 后, 无法弹出验证窗口, 请确保端口已经开启了 802.1x 验证功能;

案例十四 【综合实验】通过 AAA 验证后，自动获取 IP 并上网

案例
拓扑

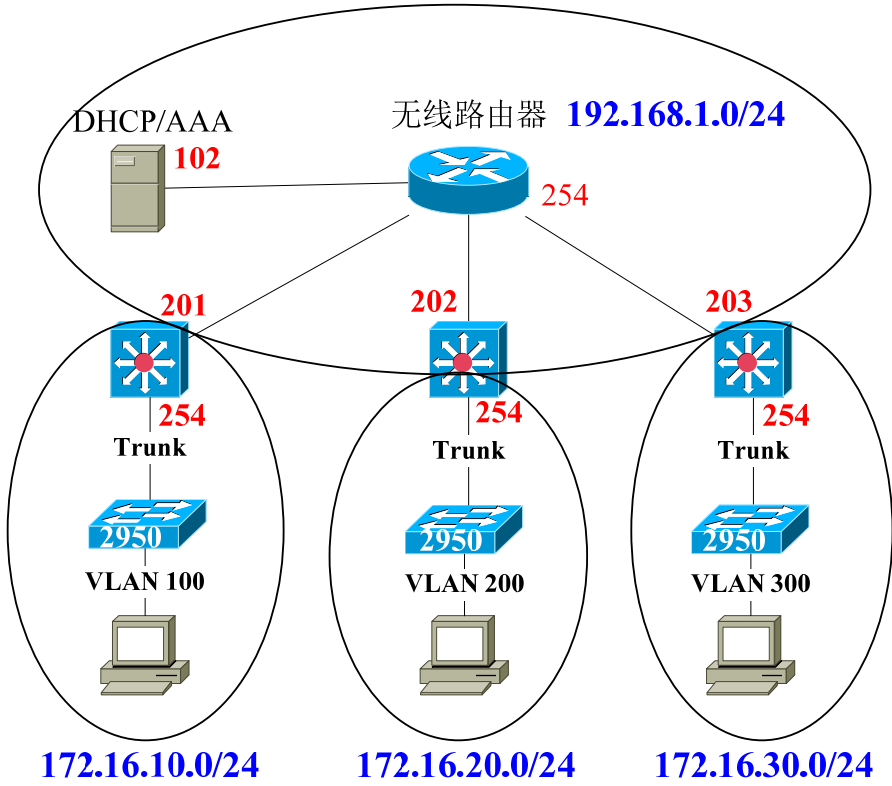


图 1

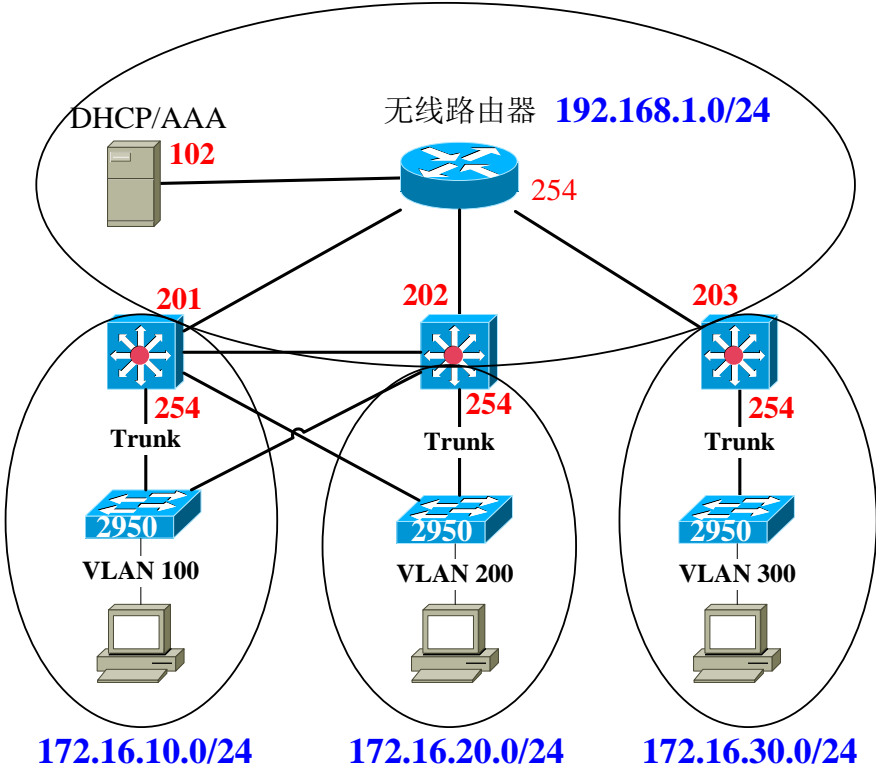


图 2

<p>实 战 需 求</p>	<p>实战目的：对用户接入网络的 PC 进行验证，为通过验证的用户分配 IP 地址，使用户可以上网；</p> <p>需求一：如图 1 所示，实验室内网出口是一台无线路由器，它的地址是 192.168.1.254，它是整个内网的网关，并且有一台 DHCP/AAA 服务器连接在上面，地址是 192.168.1.102；</p> <p>使用 ACS，分别对三个不同网段用户的接入 PC 进行验证；</p> <p>需求二：本次实验要求三个用户通过认证后，分别获取 DHCP 服务器上不同网段的 IP 地址，VLAN 100 获取 172.16.10.0/24 网段的 IP，依次类推，如拓扑所示；</p> <p>需求三：由于在客户和无线路由器之间有两个网段，因此需要用的三层路由，这里我们使用 3560 作为网络的核心，三台 3560 VLAN 1 的地址分别是 192.168.1.201/202/203，使用 2950 作为接入交换机；</p> <p>需求四：如图 2 所示，选出两台 3560 和两台 2950，实现双上联的冗余拓扑结构，利用 MSTP+HSRP 技术使接入层在有一条链路断开的情况下，ping 外网时，实现无丢包转发；</p> <p>注意：本次实验涉及二层交换、三层交换、默认路由、MSTP、HSRP、AAA 配置、DHCP 中继、DHCP 和 AAA 服务器的配置，涉及到的技术点非常多，请仔细、仔细、再仔细，多用验证命令查看；</p>
<p>配 置 命 令 详 解</p>	<p>配置思路：</p> <ol style="list-style-type: none"> 1. 首先为你的三层交换机起两个 SVI，一个是与 DHCP 位于同一个网段，如上图，地址规范：201/202/203；一个是你所连接的用户网段，vlan 100/200/300，开启 ip routing，并配置一条到网关（ADSL）的默认路由； 2. 然后将 3560 与 2950 之间链路配置为 Trunk，以保证能传输不同 vlan 的流量； 3. 在 ADSL 上准对 vlan 100/200/300 配置 3 条返回流量的默认路由； 4. 在你的 NAS（2950）上配置一个管理 IP 地址，并确保能够 ping 通 AAA 服务器； 5. 配置你的 NAS（2950）使之能够对用户 PC 进行验证； 6. 配置你的 AAA 服务器：建立用户，配置 AAA 客户端； 7. 配置 DHCP 服务器，并在 3560 的连接用户的 SVI 接口配置 helper-address
<p>排 错 思 路</p>	<ol style="list-style-type: none"> 1. 如无法 ping 通网关和 DHCP 服务器，请确保 3560 上有一条默认路由指向出口网关（ADSL 的地址）； 2. 如能够 ping 通网关，但无法上网，请确保 ADSL 有准对三个网段的回包路由； 3. 如 ACS 上没有认证信息，首先确保你的 NAS（2950 交换机）能够 ping 通 ACS 服务器； 4. 如 ACS 上没有认证信息，请确保 ACS 上的 AAA 客户端参数配置正确； 5. 如无法 ping 通 DHCP，请确保三层交换机上开启 ip routing 功能； 6. 如无法下发地址，请确保三层交换机上 SVI 接口开启 helper-address 功能

案例十五 使用端口安全—加强企业接入层交换机安全性

案例拓扑

DHCP Server

GW:192.168.1.254

攻击者

合法用户

关键知识点

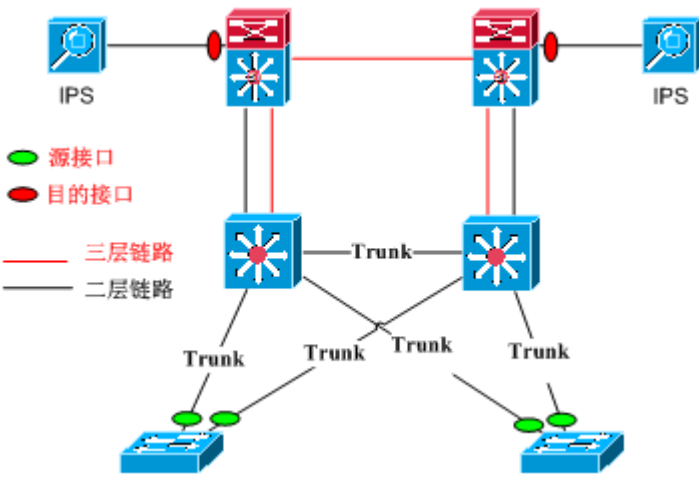
二层攻击分类及防御方法：

攻击方法	描述	防御方法
MAC 层攻击		
MAC 地址泛洪	具有唯一且无效源 MAC 地址的数据帧向交换机泛洪,消耗完交换机的 CAM 表空间后,从而阻止合法主机的 MAC 地址添加到 CAM 表中,使得交换机将使用广播来转发所有单播帧;	端口安全
VLAN 攻击		
VLAN 跳转	通过改变 Trunk 链路中封装数据包的 VLAN ID, 攻击设备可以发送或接收不同 VLAN 中的数据包, 而绕过三层安全性机制	加强 Trunk 的配置和未使用端口的协商状态
欺骗攻击		
DHCP 欺骗	攻击设备可以在短时间内消耗完 DHCP 服务器上可用地址空间, 或者使用中间人攻击, 把自己伪装成 DHCP 服务器	DHCP 侦听
生成树欺骗	攻击设备伪装成 STP 拓扑中的根网桥, 从而成为网络中的二层转发核心, 配合使用 SPAN, 可以监听网络中所有通信流量	主动配置主用和备用根设备 启用根防护、BPDU 防护、BPDU 过滤等特性
MAC 欺骗	攻击设备伪装成当前 CAM 表中合法设备的 MAC 地址, 使交换机把去往合法设备的数据帧转发到攻击设备上;	端口安全
ARP 欺骗	攻击设备故意为合法主机伪造 ARP 应答。攻击设备的 MAC 地址就会成为该合法网络设备所发出的数据帧的二层目的地址	动态 ARP 监测、端口安全
交换机设备攻击		
CDP 修改	截获 CDP 发送的明文信息, 获悉网络拓扑和设备信息;	端口上禁用 CDP

	<div>show ip dhcp snooping</div> <div>查看 DHCP 侦听配置</div>
排 错 思 路	<div>1. 如即是绑定了错误的 MAC 地址，还可以 ping 通网关，请确保端口安全功能已经打开；</div>

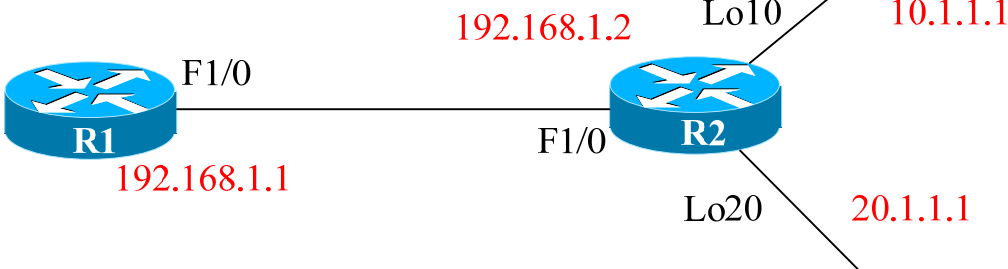
案例十六 利用 RSPAN 监控企业异常网络流量

<p>案例 拓 扑</p>	<div><div><p>图 1</p></div><div><p>图 2</p></div></div>
<p>关 键 知 识 点</p>	<p>SPAN (Switched Port Analyzer, 交换端口分析器) 是什么：SPAN 是一种监控网络流量的方法，它将源端口或特定 VLAN 的流量复制到一个目的端口进行分析。SPAN 不会影响源端口或 VLAN 的网络流量交换传输影响；</p> <ul style="list-style-type: none">➢ 可以指定 SPAN 监控源端口上出方向 (tx)、入方向 (rx) 和双向 (Both) 流量所有的帧；➢ 接口一旦被配置为目的端口，他将不再接收和发送除 SPAN 外的任何流量；➢ SPAN 的目的接口不参与任何 VLAN 的生成树选举；➢ 你可以将 Trunk 端口配置成 SPAN 的目的端口，从而发送多个 VLAN 的封装流量；➢ 一个 EtherChannel 组可配置为 SPAN 的源端口，但不能配置为目的端口➢ Cisco 2950 只能配置 1 个 SPAN 会话，而 3560、4500 和 6500 都可以配置两组 SPAN 会话； <p>SPAN 所能监控到的网络流量，包括：</p> <ul style="list-style-type: none">■ 组播或网桥协议数据单元 (BPDU) 帧；■ Cisco 设备发现协议 (CDP) 帧■ VLAN 中继协议 (VTP) 帧■ 动态中继协议 (DTP) 帧■ 生成树协议 (STP) 帧■ 端口聚合协议 (PAgP) 帧 <p>理解 RSPAN (Remote SPAN, 远程 SPAN) 的用处：类似于 SPAN，但它支持监控不同交换机上的源端口、源 VLAN 和目的端口，从而有助于跨越网络远程监控多台交换机的通信流量；</p> <p>工作原理：接入层交换机配置 RSPAN 的源是连接 PC 的接口，配置 RSPAN 的目的是 Remote VLAN，由于接入层和汇聚层之间跑 Trunk，因此它可以承载 Remote VLAN 的流量，数据在到达核心层交换机后，配置 SPAN 的源为 Remote VLAN，配置 SPAN 的目的为连接了网络分析仪的端口；</p> <div></div> <p>RSPAN 的一些特性：</p> <ul style="list-style-type: none">■ 安装增强版本 (EI) 的 IOS 镜像■ 不能监控 BPDU 包■ RSPAN VLAN 只能承载 RSPAN 的流量■ 管理 VLAN (本征 VLAN) 不要配置成 Remote VLAN

	<p>■ RSPAN 源端口和目的端口必须位于不同的设备</p> <p>企业网 RSPAN 部署方式：</p> <p>通常企业网中部署 RSPAN 时，不需要监控 Access 层交换机的所有接口，而只需要监控 Access 上联的 Trunk 接口，然后再将流量镜像到 Remote VLAN。为了避免二层环路，因此汇聚层与核心层一般是三层链路，但这样就无法传递 Remote VLAN 的数据了，因此我们需要在汇聚层与核心层之间跳一根线，让它专门承载 Remote VLAN 的数据，汇聚层交换机不需要做任何配置；在核心层 RSPAN 的源是 Remote VLAN，目的是连接 IDS/IPS 或者安装有抓包软件 PC 的接口；</p> 
<p>实战需求</p>	<p>实战目的：配置 Switch_1，使 PC2 能够监听到 PC1 所有的通信流量</p> <p>需求一：见图 1，先不配置 SPAN，PC1 ping 自己的网关，PC2 开启抓包软件，看是否有 PC1 的流量。</p> <p>需求二：在交换机上配置 SPAN，PC2 再看是否能抓取到 PC1 的通信流量；</p> <p>需求二：见图 2，配置 RSPAN，使位于 SW2 上的监听者能够抓取到位于 SW1 上服务器的通信流量；</p>
<p>配置命令详解</p>	<p>本地 SPAN 配置规则：Cisco</p> <p>monitor session [组号] source interface [接口] rx tx both 配置被监听端口及流量方向</p> <p>monitor session [组号] destination interface [接口] 配置监听端口，连接分析仪</p> <p>RSPAN 配置规则：</p> <p>1) 源配置</p> <p>vlan [VLAN ID]</p> <p>remote-vlan 指定该 VLAN 是 Remote VLAN</p> <p>monitor session [组号] source interface [接口] rx tx both 配置被监听端口及流量方向</p> <p>monitor session [组号] destination remote vlan [VLAN ID] reflector-port</p> <p>2) 目的配置</p> <p>vlan [VLAN ID]</p> <p>remote-vlan 指定该 VLAN 是 Remote VLAN</p> <p>monitor session 1 source remote vlan [VLAN ID] 配置源为 Remote VLAN</p> <p>monitor session [组号] destination interface [接口] 配置监听端口，连接分析仪</p> <p>本地 SPAN 配置规则：H3C</p> <p>mirroring-group 1 local</p> <p>mirroring-group 1 mirroring-port e1/0/47 both 配置被监听端口</p> <p>mirroring-group 1 monitor-port e1/0/48 配置监听端口</p>

排 错 思 路	<ol style="list-style-type: none">1. 组号码一定要一致；2. Cisco 交换机，被配置为监听端口的端口状态是 mirroring，该端口无法通信，而 H3C 交换机不存在此问题，还是可以通信；
------------------	--

案例十七 利用 QoS 保障企业重要数据流量通信

案例拓扑	 <pre> graph LR R1((R1)) --- F1/0 --- R2((R2)) R1 --- IP1[192.168.1.1] R2 --- IP2[192.168.1.2] R2 --- Lo10[Lo10] R2 --- Lo20[Lo20] Lo10 --- IP3[10.1.1.1] Lo20 --- IP4[20.1.1.1] </pre>
关键点	<p>三种 QoS 模型：</p> <ol style="list-style-type: none"> 1.尽力而为服务模型（Best-Effort Service）：设备尽最大努力传输数据，数据传输之前，不需要得到许可，有多少传多少，任何数据都不能得到保证，延迟也无法预计，这种服务模型采用先进先出（FIFO）队列，它没有实施任何 QoS，网络设备，默认情况下都工作在这种模型下； 2.集成服务模型（IntServ）：又称为硬 QoS，在发送数据之前，必须先向网络申请带宽，这种情况下，数据传输不会有任何延迟。但如果在没有向网络申请带宽的情况下传输数据，那么它的流量只能得到尽力而为的服务。申请带宽时，所用到的协议为 RSVP，由于传输之前必须申请贷款，因此需要耗费一些时间，在现有的网络中，集成服务模型的 QoS 通常并不被采用； 3.区分服务模型（DiffServ）：又称为软 QoS，在该模型下网络将对不同的数据提供不同的服务，因此，所有数据都将被分成不同的类别，并且指定不同的优先级，在网络发生拥塞时，网络总是先传输高优先级的数据，放弃或者推迟传输低优先级的数据，但是在网络没有拥塞时，所有数据全部正常传输。现在的网络中，实施 QoS 时通常采用这种服务模型。 <p>重要：在园区网中实施 QoS 时，大多数交换机都只支持 DiffServ，而不是 IntServ</p> <p>什么是端到端 QoS（End-to-End QoS）：数据包从源到目的路径中所有设备都为某类数据执行相同的 QoS 策略，那么这样的 QoS 就被称为端到端 QoS。</p> <p>什么是流（Flow）：当数据包的源 IP，目的 IP，协议，端口号和会话的 socket 全部相同时，这样的数据被认为是同一个流（flow），同一个流，通常应该得到相同的 QoS 服务；</p> <p>令牌桶算法：当流量到达一个实施了 QoS 的接口后，需要查看令牌桶中是否有令牌，1 个令牌允许接口发送或接收 1bit 的数据，当接口通过 1bit 数据后，同时也要从桶中移除 1 个令牌，当桶中没有令牌的时候，任何流量都会被视为超过额定带宽而丢弃；令牌桶中的令牌不仅仅可以被移除，同样也可以往里添加，为了保证接口随时有数据能够通过，就必须不停地往桶里加令牌，由此可见，往桶里加令牌的数量和速度，就决定了数据通过接口的速度。</p> <ul style="list-style-type: none"> ➤ CIR（承诺信息速率）：控制往令牌桶里加令牌的数量以控制接口的带宽，这个速率就是 CIR，例如，设置用户的带宽为 1000 bit 每秒，那只要保证每秒钟往桶里添加 1000 个令牌即可； ➤ Bc（Burst size）：同一秒钟令牌可以一次性添加完，也可以分几次添加，每次添加令牌的数量被称为 Bc，如果 Bc 只是 CIR 的一半，那么很明显每秒钟就需要往桶里加两次令牌； ➤ Tc（Time interval）：表示多久该往桶里加一次令牌，而这个时间并不能手工设置，因为这个时间可以靠 CIR 和 Bc 的关系计算得到，$Bc/CIR=Tc$； <p>例子：如果 CIR 是 8000，Bc 是 4000，那就是每秒加两次，Tc 就是 $4000/8000=0.5$，也就是 0.5 秒，即 500 ms。</p> <p>1.单桶双速：只存在一个令牌桶，并且流量只会出现两种结果，即符合 CIR 或超出 CIR，上一秒钟没有用完的令牌，会全部清空，下一秒钟再重新加入令牌；</p>

例子：第 1 秒，加入 8000 令牌，用户使用 5000 后，剩余 3000 被清空

第 2 秒，加入 8000 令牌，用户使用 6000 后，剩余 2000 被清空

第 3 秒，加入 8000 令牌，用户使用 8000 后，没有剩余

第 4 秒，加入 8000 令牌，用户使用 7000 后，剩余 1000 被清空

2.假双桶三速：使用两个令牌桶，一个真桶，一个假桶，用户每秒的可用带宽，总是两个桶的令牌之和，第一个桶的令牌机制和单桶双速算法没有任何区别，关键在于第二个桶。第二个桶的令牌不能直接加入，只有当前一秒钟结束后，第一个桶中存在剩余令牌时，这些剩余令牌就可以从第一个桶中被转移到第二个桶中。但并不是第一个桶所有未用令牌都可以放入第二个桶，**Burst Excess (Be)** 限定了第二个桶令牌的数量；由此可见，**Be** 是不可能超过 **CIR** 的，因为第一个桶每秒的所有令牌就是 **CIR**，即使所有令牌全部被移到第二个桶，**Be** 最多也只能等于 **CIR** 而不能超过。而 **Be** 和 **Bc** 却毫无关系。需要注意的是，在每二秒结束时，如果用户没有将第二个桶的令牌用完，那么第二个桶的令牌也是要全部被清除的，第二个桶中的令牌，总是来自于上一秒第一个桶没用完的令牌。由于使用了两个桶，所以用户的流量也会出现三种结果：

小于或等于 **CIR**（也就是符合 **CIR**）（conform）

大于 **CIR** 并小于或等于 **CIR** 与 **Be** 之和（也就是符合两个桶令牌之和）（exceed）

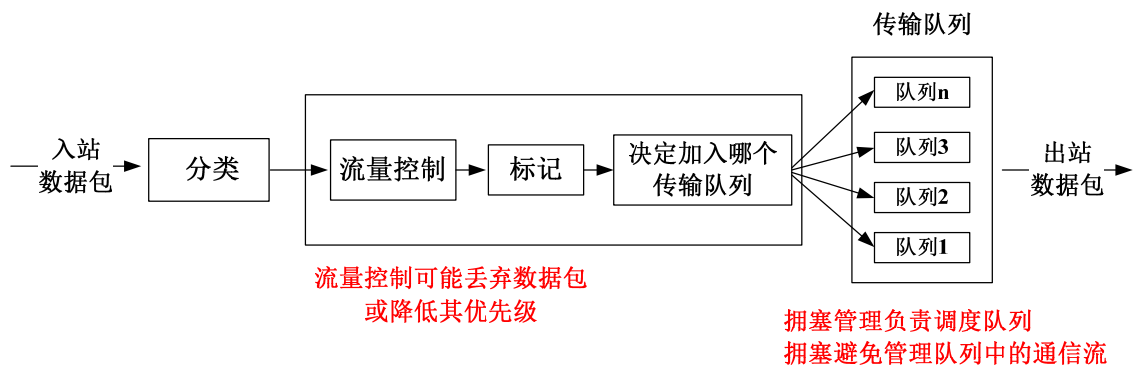
超过 **CIR** 与 **Be** 之和（也就是超过两个桶令牌之和）（violate）

例子：将 **CIR** 设置为 8000bit，**Be** 设置为 2000，每一秒都会往第一个桶里加 8000 个令牌，每一秒结束后，所有第一个桶未使用完的令牌将放入 2000 个到第二个桶；

	第 1 个桶令牌数	消耗令牌数	第 2 个桶令牌数	用户可用带宽总数
第 1 秒	8000	6000	0	8000
第 2 秒	8000	7000	2000	10000
第 3 秒	8000	5000	1000	9000
第 4 秒	8000	9000	2000	10000
第 5 秒	8000	8000	0	8000
第 6 秒	8000	6000	0	8000
第 7 秒	8000	10000	2000	10000

3.真双桶三速：同样使用两个令牌桶，然而这两个桶是相互独立的，并不会将第一个桶未用的令牌放入第二个桶。第一个桶与以往的算法相同，也就是每秒都有 **CIR** 的数量，而第二个桶可以直接设置为 **CIR+Be** 之和，称为 **PIR**，也就是说第二个桶总是比第一个桶要大，用户的流量总是以第二个桶的大小传输，而不用像假双桶三速中的令牌桶算法时，需要在上一秒钟以低于 **CIR** 的速度传输。当用户的数据通过接口时，总是先检查第二个桶的最大速率，即 **PIR**，如果超出则采取动作，如果未超出，再检查是否符合第一个桶的 **CIR**，如果超出 **CIR**，则采取相应动作，如果未超过，则正常传输。

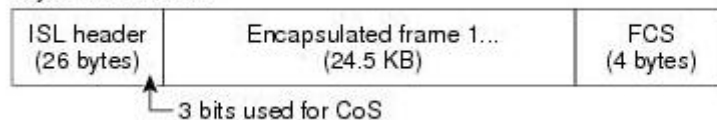
QoS 的四大组件：在实施 QoS 时，需要不同的组件之间相互组合，才能设计出完整的 QoS 策略，而每个组件中，都会有相应的 QoS 技术提供支持，以下是 QoS 四个组件：



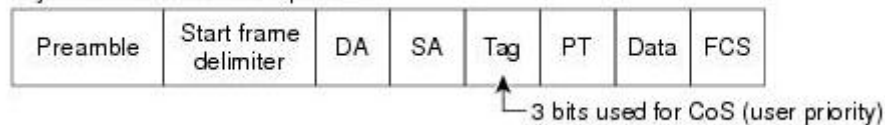
1.分类和标记:

- 一层特征: 物理接口、子接口、PVC
- 二层特征: MAC 地址、802.1Q 的 COS 位、VLAN 标示、帧中继可丢弃 (DE) 位

Layer 2 ISL Frame

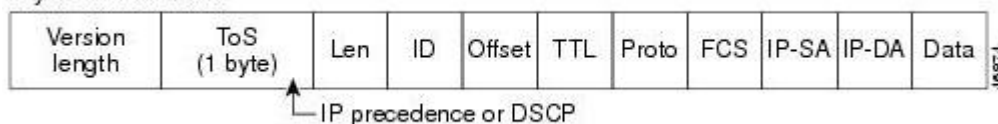


Layer 2 802.1Q and 802.1p Frame



- 三层特征: IP Precedence (IP 优先级)、DiffServ 代码 (DSCP)、源 IP 和目的 IP

Layer 3 IPv4 Packet



- 四层以上特征: TCP 或 UDP 端口号、URL

2.管制和整形:

- 管制 (Policing): 如果流量超过额定带宽, 处理方式为直接丢弃;
- 整形 (Shaping): 如果流量超过额定带宽, 将流量缓存到内存中, 等待下一秒再传输;

下面是一些管制和整形的工具:

Committed access rate (CAR)——承诺访问速率, 管制工具

Generic Traffic Shaping (GTS)——通用流量整形, 整形工具

Frame Relay Traffic Shaping (FRTS) ——帧中继流量整形, 整形工具

Class-Based Shaping——基于类的流量整形, 整形工具

3.拥塞管理: 规定在网络发生拥塞后, 使用队列技术来传输数据的优先顺序, 它需要依赖已经做好的分类和标记, 只有在发生拥塞后, 这些队列机制才会生效, 一个接口只能使用一种队列技术, 下面是目前存在的队列技术:

- **FIFO queuing (先进先出队列):** 接口没有启用 QoS 时候的默认队列;
- **Priority queuing (PQ):** 它被称为优先级队列, 是因为在发生拥塞时, 该队列只传优先级最高的数据, 只有当优先级最高的数据全部传完之后, 才会传次优先级的数据。

- **Custom queuing (CQ):** 它里面中有 1—16 共 16 个队列，每个队列可以分别指定同一时间点可以传输数据包的总数，第 1 个队列传完了，再传第 2 个，依次类推；
- **Weighted Fair Queuing (WFQ):** 它是基于 Weight 的公平队列，根据数据包的 IP 优先级来分配带宽，优先级高，带宽就多，优先级低，带宽就少，所谓公平，就是所有的数据包在任何时刻都可以分到带宽，WFQ 在给数据包分配带宽时，是基于流 (flow) 来分配的；
- **Class-Based WFQ (CBWFQ):** 它是基于 WFQ 的，并且对 WFQ 做了一些改进，它可以为某些特定的流量分配指定的带宽。例如 A、B、C、D、E 共 5 个人分 100 斤大米，在使用 WFQ 时，是根据 A、B、C、D、E 这五个人的优先级，将 100 斤大米公平地分给五个人的，但如果使用 CBWFQ，就可以规定将 80 斤大米按优先级只分配给 A、B、C 三个人，而再将 20 斤大米按优先级分配给 D、E 两个人，因此在使用 WFQ 时，是所有人分配所有的大米，而使用 CBWFQ 时，是不同人群，分配不同数量的大米；
- **Low Latency Queuing (LLQ):** 语音或视频数据在通信时，需要一直保持足够的带宽，否则就会受到影响，LLQ 的低延迟队列正是针对延迟和抖动较敏感的语音或视频流量设计的，它为特定的流量划分特定的带宽，划给特定流量的带宽是绝对能够保证的，LLQ 队列中的流量能够优先传送，即使超过了额定带宽，只要不发生拥塞，就可以正常传输，否则丢弃；
- **IP RTP Priority:** 该队列只为对延迟要求较高的实时数据（语音和视频或 UDP 目标端口号为 16384 至 32767）保证带宽，受 RTP 保护的数据流，可以在任何流量之前优先传递，RTP 优先于 LLQ 传送，RTP 只支持串口和帧中继 PVC；

4.拥塞避免: 在发生拥塞后，再去做管理，无异于亡羊补牢，因此，在拥塞没有发生前，提前利用一些技术，避免拥塞的发生，才是一个好的方案，下面是一些拥塞避免的技术；

- **Tail Drop:** 尾丢弃是接口的默认行为，发生拥塞时，优先丢弃最后到达的数据；
- **WRED:** 工作机制与 WFQ 有相同之处，它也是依靠流量的优先级来分配相应的丢弃几率，它将根据数据包的 DSCP 或 IP 优先级高低来丢弃数据包，默认使用 IP 优先级，只能与 WFQ 或 CBWFQ 一起使用；
- **WRED-ECN:** 该技术允许设备，在即将发生拥塞时，发送 ECN（明确拥塞通告）告知数据源降低发送速度，该功能必须开启 WRED，并且需要配合 WFQ 或 CBWFQ 一起使用；
- **Frame Relay DE 位:** 在 Frame Relay 网络中，数据包中标有 DE 字段，如果为 1，表示数据包不重要，如果为 0，表示重要，发生拥塞前，将先丢为 1 的数据，默认所有数据都为 0；

MQC 模型:

1.定义流量:

```
access-list 1 permit 10.1.1.1 0.0.0.0
```

用 ACL 匹配源主机 10.1.1.1 发出的数据

```
class-map match-all ccie
```

创建 class-map，

```
match access-group 1
```

调用 ACL 的数据

注意：关键字 match-all 指定匹配所有条件，match-any，则任一条满足即可，默认为 match-all，名为 class-default 的 class-map，表示匹配所有数据。

2.设置策略:

```
policy-map cisco
```

创建一个 policy-map 策略

```
class ccie
```

调用 class-map 匹配到的数据

```
drop
```

设置丢弃策略

注意：一个 policy-map 里面可以调用多个 class-map，如果调用 class-default，那么表示之前没有匹配到的流量，全部都会被 class-default 所匹配。

3.应用策略

```
interface f0/0
```

进入接口

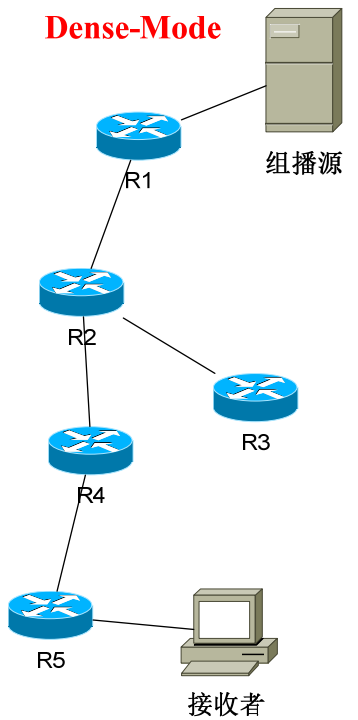
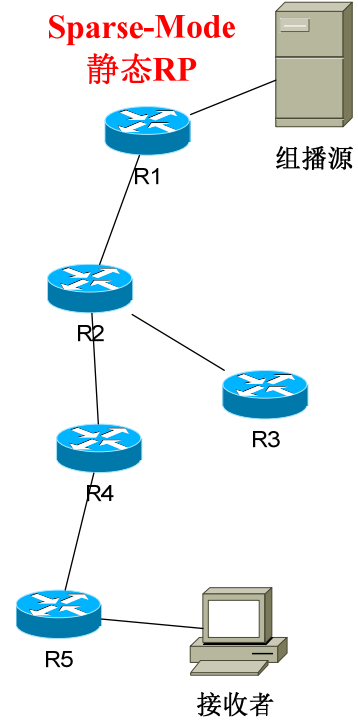
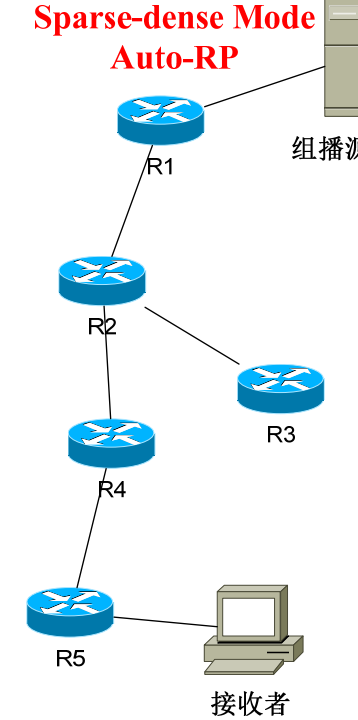
```
service-policy output cisco
```

在出方向调用策略

实 战 需 求	<p>实战目的：</p> <p>需求一： R2 身后有两个网段，10.1.1.1 和 20.1.1.1，配置 R1，对于到目标网络 10.1.1.0/24 的流量，管制到 8000bit/s，每秒钟添加 4 次令牌，合规动作为传递，违规动作即丢弃包，在 R1 上 ping 去往 10.1.1.1 的流量，发现丢包，ping 20.1.1.1，正常通过；</p> <p>需求二： R2 身后有两个网段，10.1.1.1 和 20.1.1.1，配置 R1，对于到目标网络 10.1.1.0/24 的流量，整形到 8000bit/s，每秒钟添加 4 次令牌，在 R1 上 ping 去往 10.1.1.1 的流量，发现不丢包了，但 ping 包速度很慢，ping 20.1.1.1，速度正常；</p> <p>需求三： 在 R1 上配置到 10.1.1.1 的流量，保证带宽为 10M，去往 20.1.1.1 的流量，保证带宽为 20M，其他所有流量使用剩余的带宽，由于拥塞管理，只有在发生拥塞时才能验证，因此实验室环境只能通过 show 命令查看配置，无法验证；</p> <p>需求四： 在 R1 上配置到 10.1.1.1 的流量，保证带宽为 50M，并使用 WRED 算法，提前预知拥塞发生，并随机丢弃包，由于拥塞避免只有在即将发生拥塞时才能生效，因此实验室环境只能通过 show 命令查看配置，无法验证；</p>
配 置 命 令 详 解	<p>QoS 配置规则：</p> <p>1) 配置管制</p> <pre>access-list [ACL 号] permit ip any [网络号] [反掩码]</pre> <p>配置要抓取的地址</p> <pre>class-map [名字]</pre> <p>配置一个 class-map</p> <pre>match access-group [ACL 号]</pre> <p>调用所配置的 ACL</p> <pre>policy-map [名字]</pre> <p>配置一个 Policy-map</p> <pre>class [名字]</pre> <p>调用所配置的 class-map</p> <pre>police cir [承诺信息速率] bc [令牌速率] be [突发速率] conform-action [动作] exceed-action [动作]</pre> <p>配置 CIR、Bc、Be 及合规动作和违规动作</p> <pre>int s0/0</pre> <pre>service-policy output input [名字]</pre> <p>接口调用策略</p> <p>2) 配置整形</p> <pre>access-list [ACL 号] permit ip any [网络号] [反掩码]</pre> <p>配置要抓取的地址</p> <pre>class-map [名字]</pre> <p>配置一个 class-map</p> <pre>match access-group [ACL 号]</pre> <p>调用所配置的 ACL</p> <pre>policy-map [名字]</pre> <p>配置一个 Policy-map</p> <pre>class [名字]</pre> <p>调用所配置的 class-map</p> <pre>shape average [承诺信息速率] [令牌速率] [突发速率]</pre> <p>配置 CIR、Bc、Be</p> <pre>int s0/0</pre> <pre>service-policy output input [名字]</pre> <p>接口调用策略</p> <p>3) 配置拥塞管理——CBWFQ</p> <pre>access-list [ACL 号] permit ip any [网络号] [反掩码]</pre> <p>配置要抓取的地址</p> <pre>class-map [名字]</pre> <p>配置一个 class-map</p> <pre>match access-group [ACL 号]</pre> <p>调用所配置的 ACL</p> <pre>policy-map [名字]</pre> <p>配置一个 Policy-map</p>

	<div>class [名字] bandwidth [带宽] int s0/0 service-policy output [名字] sh int f0/x 注意：CBWFQ 只能应用在接口 out 方向</div> <div>4) 配置拥塞避免——WRED Interface f1/x random-detect random-detect dscp-based sh queueing random-detect</div> <div>5) 配置拥塞避免——基于 CBWFQ 的 WRED policy-map [名字] class class-default bandwidth [带宽] random-detect int f0/x service-policy output [名字]</div>	<div>调用所配置的 class-map 指定分配的带宽</div> <div>接口调用策略 无法做实验验证，通过命令看队列是否是 CBWFQ</div> <div>开启 WRED，默认基于 IP 优先级 开启基于 DSCP 的 WRED 查看队列</div> <div>配置一个 policy-map 指定一个默认类 为这个类指定一个带宽 为这个队列启用 WRED</div> <div>接口调用策略</div>
排 错 思 路		

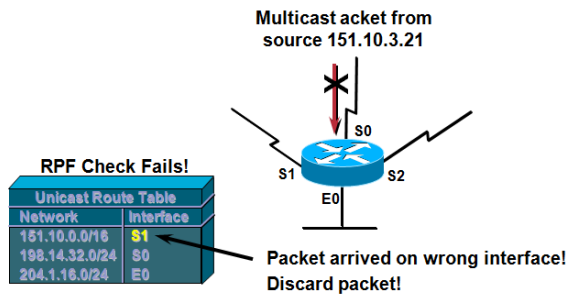
案例十八 理解组播路由协议的原理和用法

<p>案例拓扑</p>	<div><div><p>Dense-Mode</p><p>图 1</p></div><div><p>Sparse-Mode 静态RP</p><p>图 2</p></div><div><p>Sparse-dense Mode Auto-RP</p><p>图 3</p></div></div>
<p>关键点</p>	<p>组播的三个组成部分：</p> <ol style="list-style-type: none">1.组播地址：能被组播识别的地址集，例如：239.1.1.1；2.组成员机制：主机加入和退出组的机制，例如：IGMPv1、IGMPv2、IGMPv3；3.组播路由协议：路由器有效传送组播到各个网络的组成员，且不会过度消耗网络资源的路由协议，例如：BSR 和 Auto-RP 协议； <p>组播地址取值范围： D 类地址：224.0.0.0——239.255.255.255。</p> <p>组管理机制： IGMP 可以使用查询和报告来发现组成员；</p> <p>组播路由协议： 要让路由器生成一张功能完全的组播路由表，就需要在路由器之间运行一种协议，这种协议可以让组播源和目的之间的路由表生成单播表一样地生成组播表，最后路由器根据这张组播路由表来完成组播的转发。</p> <p>组播树： 组播的发送者通常面临着要将数据发向多个接收者，而要保证组播的出口信息，要保证接收者能够正常收到组播，就必须让路由器知道自己该将组播从什么接口发出去，只有这样让路由器之间协同工作，都能够记住组播的出口，最终在发送者与接收者之间形成一条连线，这样才能完成组播的转发。当多个网络存在接收者时，那么这样的连线就会有多条，组播发送者到接收者之间的这些转发线路，被称为组播转发树，而组播发送者就好比是组播树的树根，组播总是从根发向接收者。要完成从发送者到接收者之间的组播转发，组播树上的路由器都应该记住组播的出口，每台中间路由器都记住出口之后，最终便形成了组播树，而要记住组播的出口信息，这就是组播路由表的工作。</p> <p>(S, G)源树： 一个发送者，对应一个 S,G，例如：组地址为 224.1.1.1，发送为 10.1.1.1 和 10.2.2.2，那么在组播路由表里就要建立两个表项：(10.1.1.1,224.1.1.1) 和 (10.2.2.2,224.1.1.1)，以此类推，在密集模式中的源树将记录组播源接口（RPF 检查）和转发接口（组播接收者），其他所有运行组播协议，但没有接收者的接口都将被修剪（Prune）；</p>

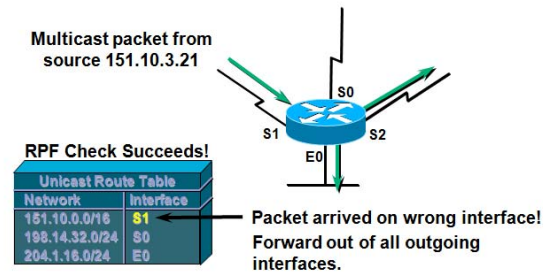
(*, G) 共享树：多个发送者对应一个*,G, 例如：组地址为 224.1.1.1, 发送为 10.1.1.1 和 10.2.2.2, 那么在组播路由表里就要建立一个表项：(*,224.1.1.1), 在稀疏模式中的共享树将记录组播源接口 (RPF 检查) 和转发接口 (组播接收者), 而不记录其他不相关的接口; 稀疏模式中, 组播用户到 RP 用源树, 组播源到 RP 用共享树

RPF 检查：组播路由器在收到组播数据后, 都要对数据进行 RPF 检测, 只有从源的方向发来的数据才能被转发, 从其它接口过来的数据被认为是无效的, 下图是 RPF 检查失败和成功的例子;

• RPF Check Fails

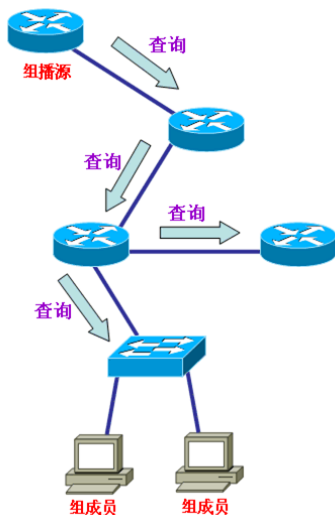


• RPF Check Succeeds



PIM 协议的模式：

Dense-Mode (密集模式)：采用的方法为路由器主动向网络查询是否有接收者, 组播源会向所有

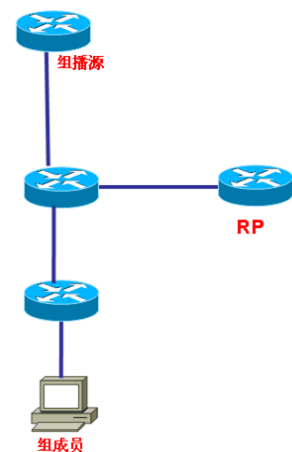


PIM 邻居发出查询, 查询数据包中包含组的地址, 下一跳 PIM 邻居还会继续向它的邻居发出查询数据包, 这些查询数据包会在所有 PIM 邻居之间传递。如果查询数据包发向一个连接了组成员的网络, 这时路由器收到组成员的报告之后, 就会向自己上一跳邻居 (RPF 接口方向的邻居) 发送加入组的消息, 以宣布自己要接收组播, 从而将组播转发到组成员。在这些过程中, 如果某些 PIM 路由器根本没有与组成员相连, 那么它将会向自己的上一跳邻居发送剪除消息, 以宣布自己不需要接收组播, 最终组播从源发出后, 只会沿着组播树被发到连接了组成员的网络, 而其它不相关的网络是不会有组播流量的。

组播发送源将数据发给组播路由器, 然后路由器依照组播路由表朝着接收者的方向转发, 这样的路径, 是依靠单播路由表计算出来的最短路径, 也就是说从发送者到接收者之间的路径, 总是最短的;

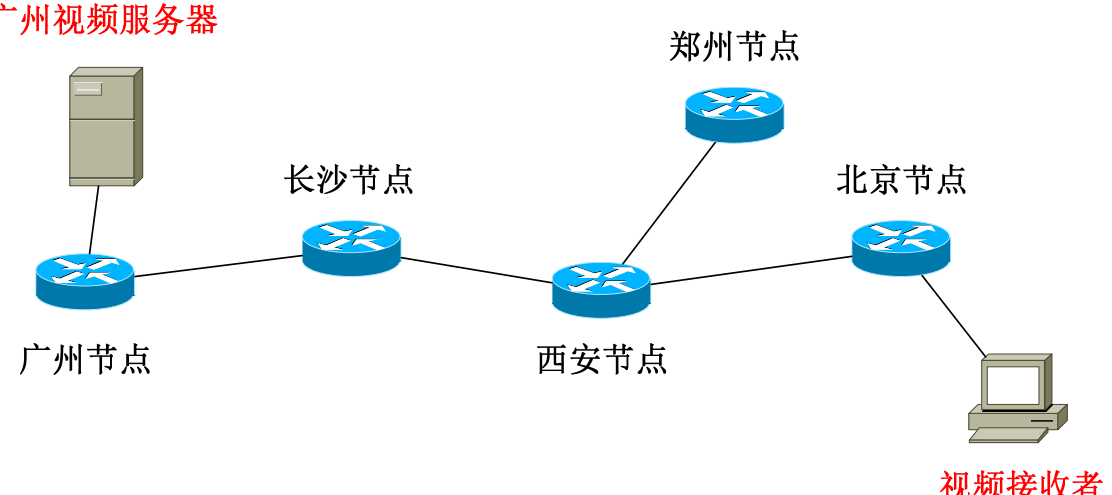
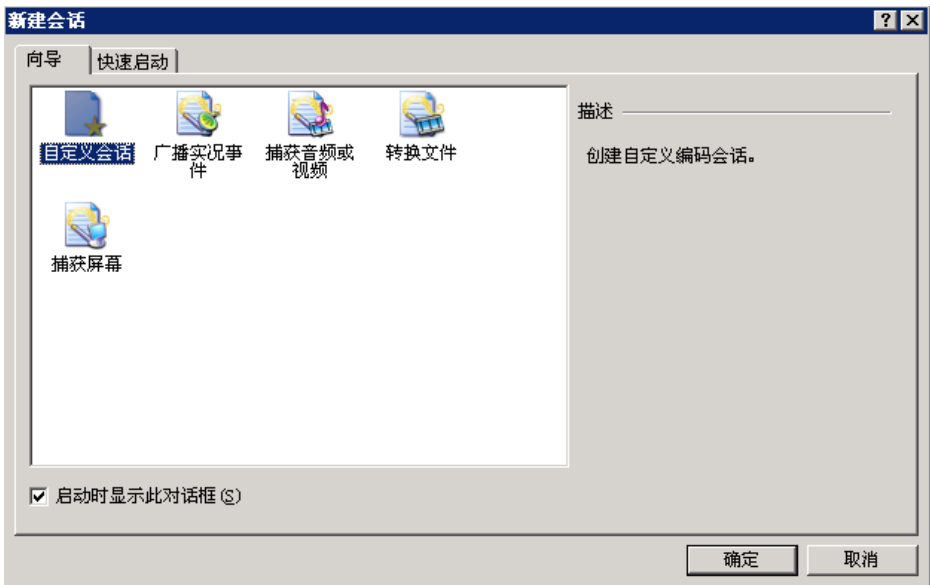
Sparse-Mode (稀疏模式)：由于记录组播信息采用(*, G)的方式, 而并不关心组播源地址, 因此造成路由器不知道组播发送者的 IP 地址是什么, 也就无法完成 RPF 反向路径检测。在这种情况下, PIM-SM 在网络中选出一个组播会聚点, 即 RP, RP 就是组播网络的核心, 发送者统一将组播数据发送到 RP, 然后 RP 再将数据发到接收者, 也就是说接收者收到的数据, 都是由 RP 转发过来的, 路由器也就认为 RP 的地址, 就是组播源的 IP 地址。

在建立组播树时, PIM-SM 并不会让路由器发送查询数据包去查询组成员, 而组成员的发现是靠组成员自己主动向路由器发送报告数据包, 当一台路由器从接口上收到组成员的报告之后, 就会向自己的上一跳邻居发送加入消息, 以通告自己需要接收组播, 直到组播源收到加入消息为止, 通过这样的方式, 就可以建立组播源到组成员之间的组播树。

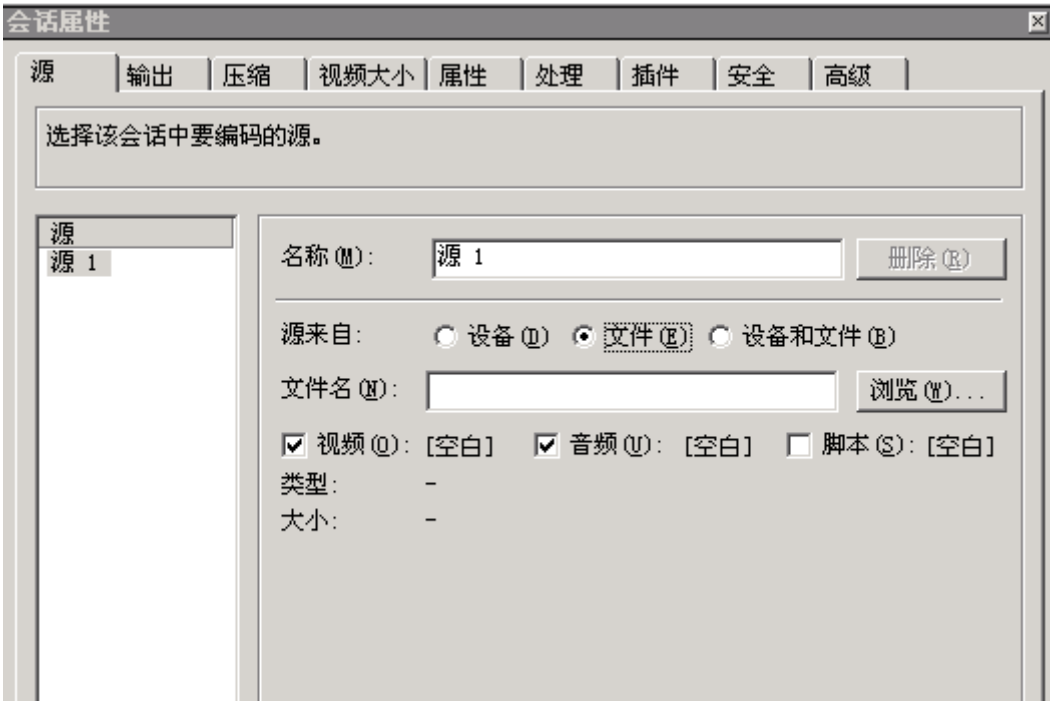


	<div>ip pim send-rp-announce [接口] scope [跳数] group-list [ACL 号]</div> <div>使用指定接口宣告自己是某个组的候选 RP</div> <div>ip pim send-rp-discovery [接口] scope [跳数]</div> <div>使用指定接口宣告自己是 RP 映射代理</div> <div>查看命令：</div> <div>sh ip mroute</div> <div>查看组播路由表</div> <div>sh ip pim rp</div> <div>查看组和 RP 对应关系</div>
排 错 思 路	

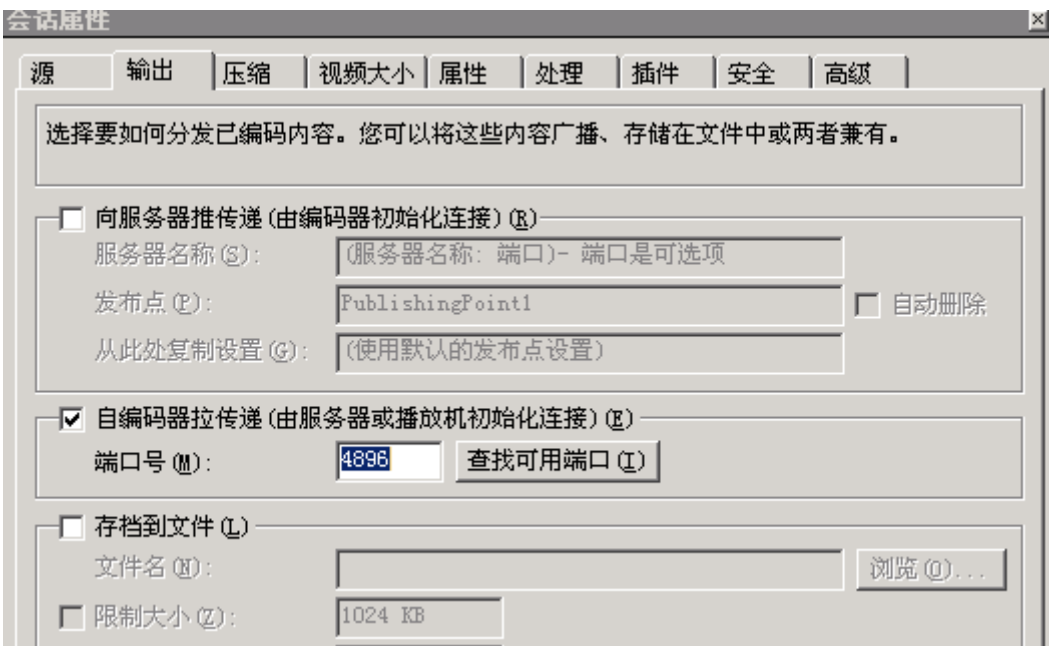
案例十九 【综合实验】组播在视频直播中的应用

案例拓扑	<p>广州视频服务器</p>  <p>郑州节点</p> <p>长沙节点</p> <p>广州节点</p> <p>西安节点</p> <p>北京节点</p> <p>视频接收者</p>
实战需求	<p>实验目的：配置组播协议，使北京接受者能够通过组播收看到的广州视频服务器发布的视频；</p> <p>题外话：真实广域网几乎是不会运行组播的，因为这需要节点上每台运营商的路由器都开启组播功能，这个不现实，也不可能；这个实验只是为了让你明白组播的原理和应用场景；</p> <p>需求一：某公司在广州有一台视频服务器，用于内部培训视频的播放，配置路由器和视频服务器，使北京的用户只需要在浏览器中输入一个地址，就能收看到视频服务器正在播放的视频；</p> <p>需求二：全网跑 OSPF，所有路由器全局启用组播功能，节点上所有的接口启用组播稀疏密集模式，配置西安节点既是组 x.x.x.x 的 C-RP，也是 MA 映射代理；</p> <p>需求三：在广州的视频服务器上配置 Windows Media Services 和 Windows Media 编码器（配置步骤参考下面的配置规则）；</p>
配置命令详解	<p>视频服务器配置规则：</p> <ol style="list-style-type: none">通过添加删除程序，在 Windows 2003 上安装 Windows Media Services 服务下载并安装 Windows Media 编码器运行 Windows Media 编码器，新建自定义会话，并点击确定 

4. 源来自 中选择文件，在浏览中选择你要发布的视频文件



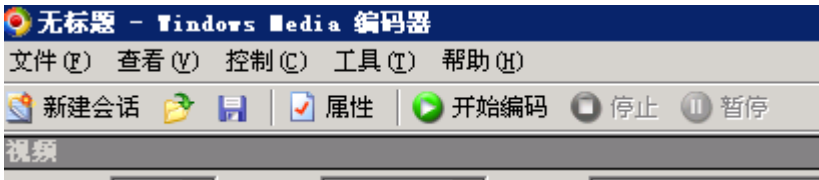
5. 输出中选择可用端口号，不能和你现有的端口重复，一般让他自己查找就行



6. 压缩中选择你要呈现视频窗口的大小和码率，其他默认不变，点击应用



7. 点击开始编码，Windows Media 编码器方面设置就完成了



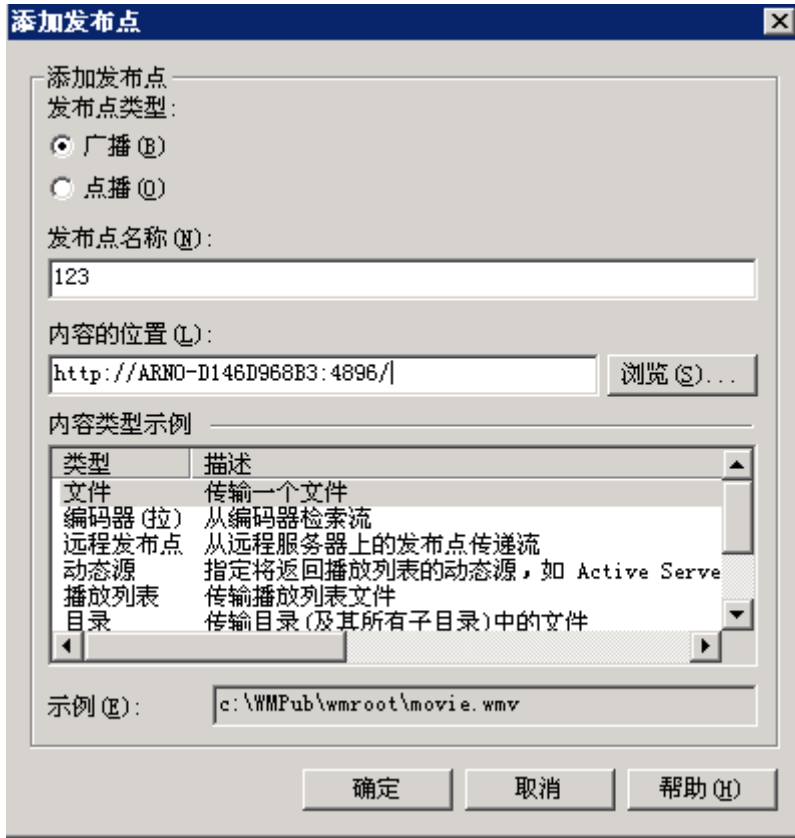
8. 在连接中，将 <http://ARNO-D146D968B3:4896/> 这个地址 copy 下来，后面要使用



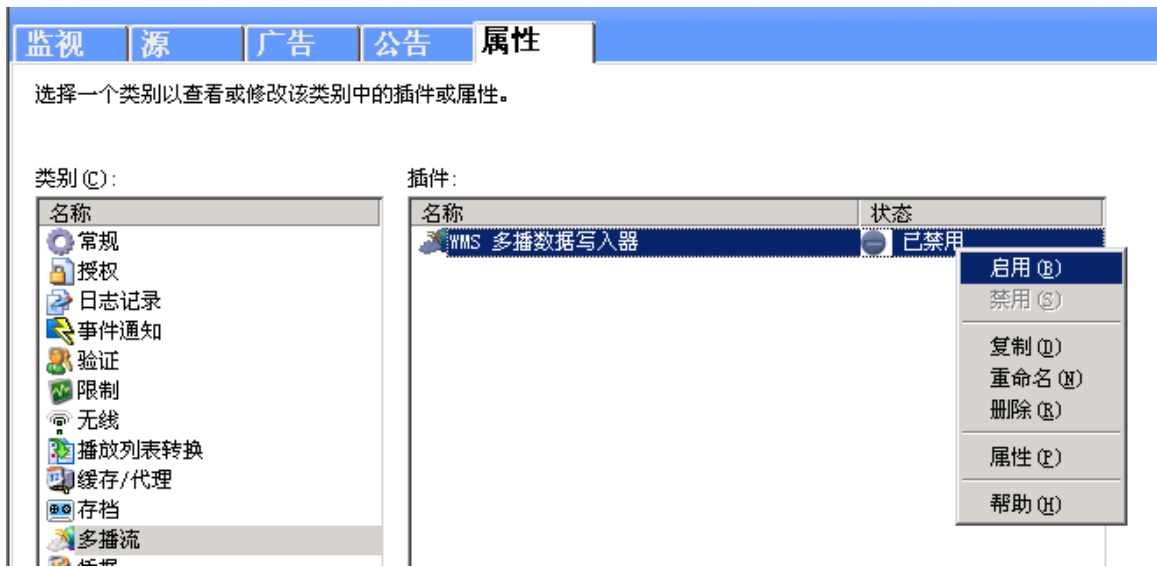
9. 在 Windows Media Services 中右键点击发布点，选择“添加发布点（高级）”



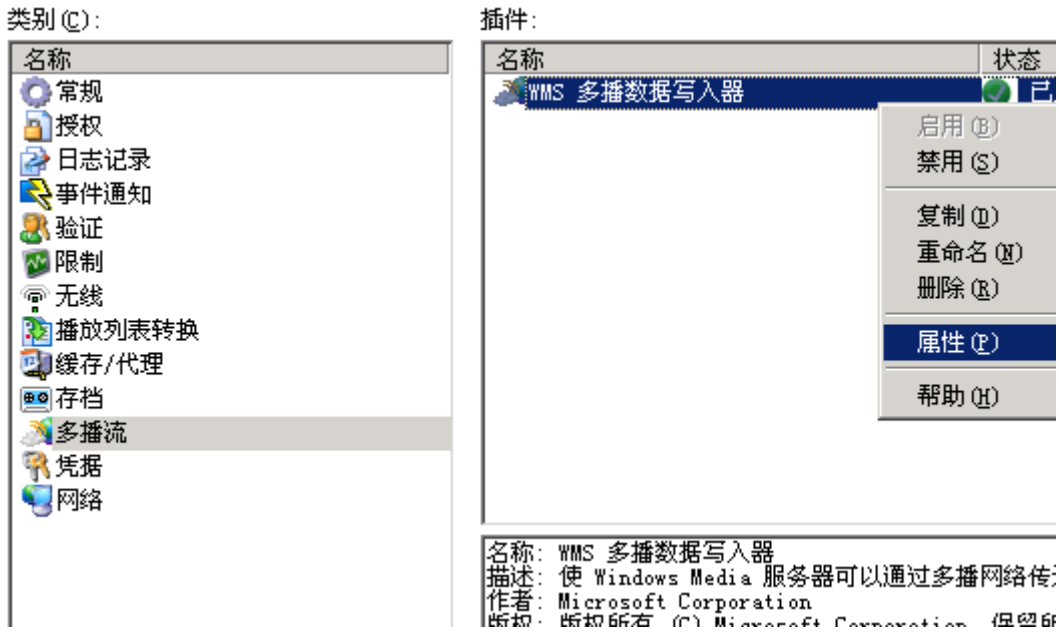
10. 选择“广播”发布，填写发布点名称，在内容的位置中，将刚才 copy 的地址填进去，然后确定



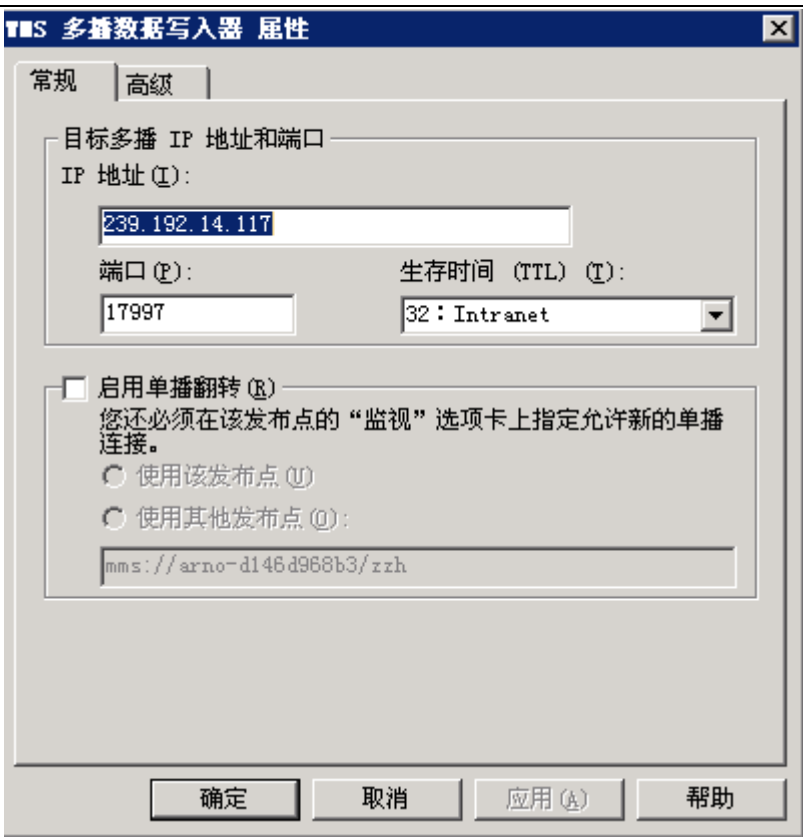
11. 右边内容框中选择“属性”，选择“多播流”，右键单击 WMS 多播数据写入器，选择启用



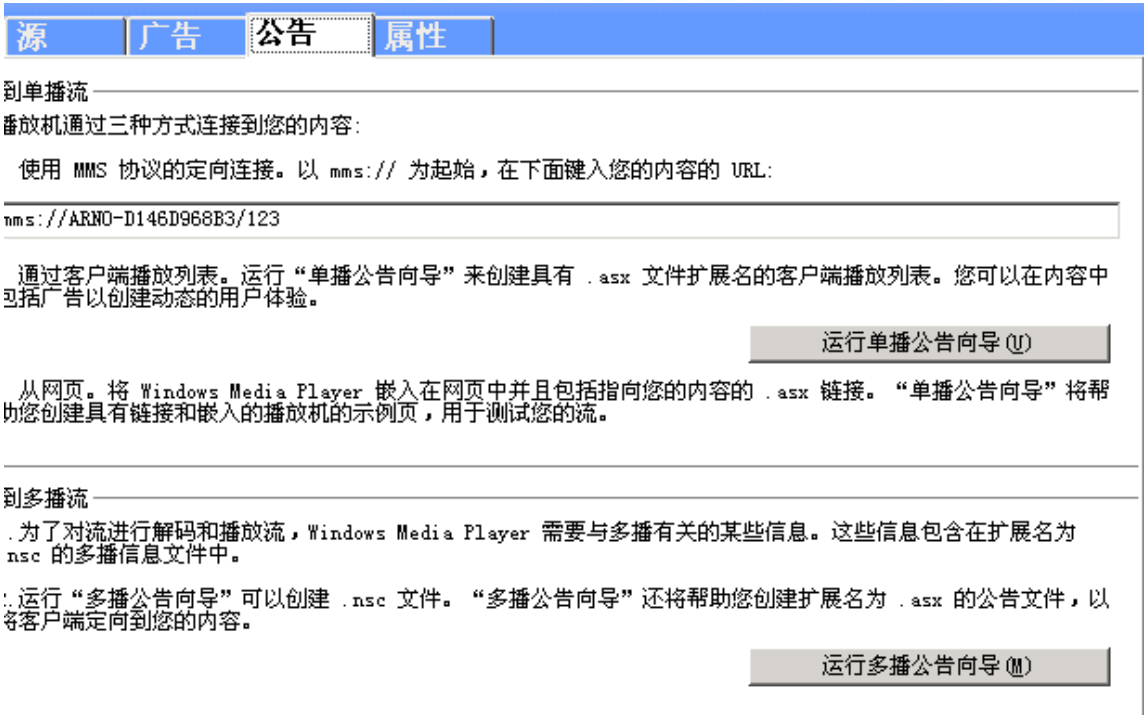
12. 启用之后，再选择属性



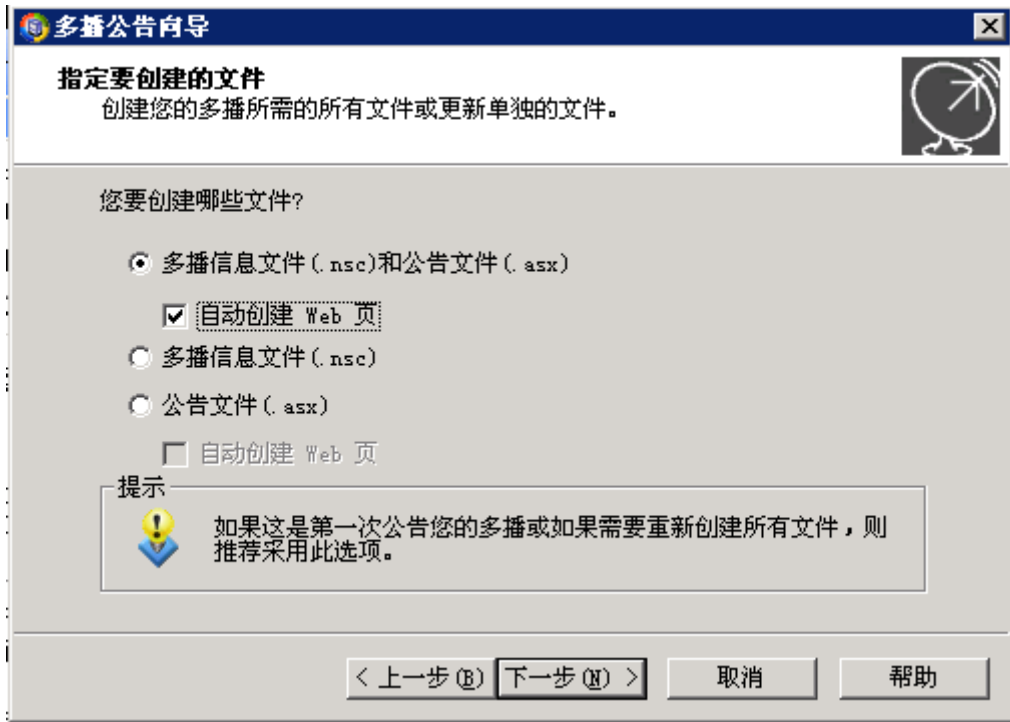
13. 出现“WMS 多播数据写入器”属性，把下面这个组播地址记录下来，这个地址就是在配置 ip igmp join-group 需要配置的地址；



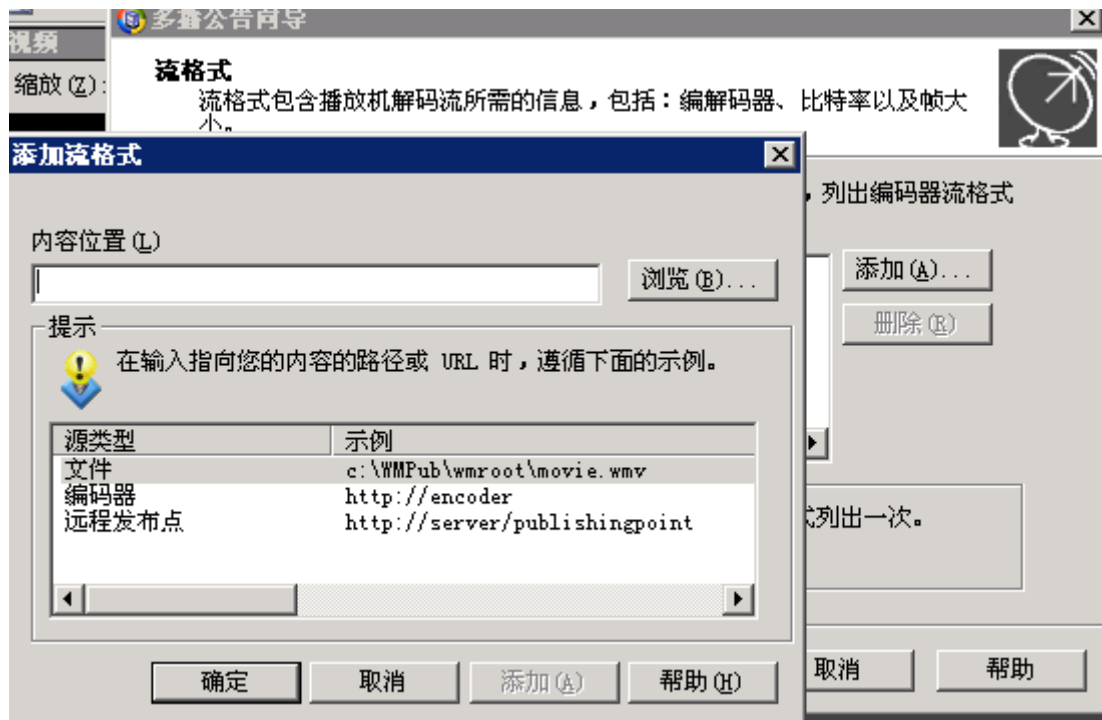
14. 切换至“公告”选项卡，选择“运行多播公告向导”



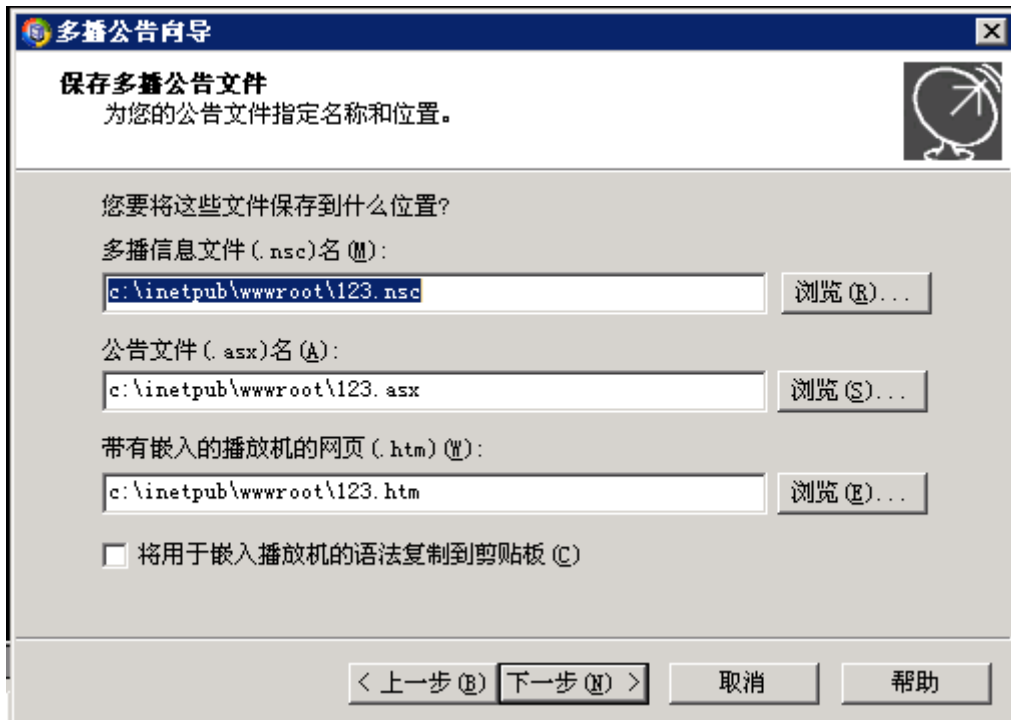
15. 点击下一步，选择第一项“多播信息文件和公告文件”并勾选自动创建 web 页



16. 下一步进入添加内容页，点击添加，将最初 copy 的网址填进去



17. 下一步，都是默认选项，直到看到该页面，该位置是你 IIS 发布网页的位置，需要用浏览器可以访问到，IIS 的配置这里不再说明。



18. 这里要将里面计算机名称改为你视频服务器的 IP 地址



19. 之后都是默认下一步，直到完成配置。



在北京的客户 PC 的浏览器中输入该地址 <http://192.168.1.102/123.htm>，就可以通过组播看到广州视频服务器发布的视频了

排
错
思
路

1. 首先，确保你能够 ping 通广州那台视频服务器的 IP 地址，然后再确保能够 ping 视频服务器的组播地址；
2. 如果 ping 不通 IP 地址，检查路由，如果 ping 不通组播地址，检查组播 RP 映射表项；
3. 路由器靠近视频服务器那一端的端口加组地址要和多播流里面的发布的地址一致