

# H3C Debug 信息详解

——基础常识



杭州华三通信技术有限公司保留一切权利

地址：杭州市高新技术产业开发区之江科技工业园六和路 310 号 H3C 公司

邮编：310053

TEL：0571—86760000

FAX：0571—86760001

# 目 录

1.	两种以太网帧格式及其封装.....	12
2.	<b>IP 首部 20 字节</b> .....	13
3.	<b>TCP 首部 20 字节</b> .....	13
4.	<b>UDP 首部 8 字节</b> .....	13
5.	<b>VLAN 格式</b> .....	14
6.	<b>PPP 格式和 PPPoE 格式</b> .....	15
	PPP 格式.....	15
	PPPoE 格式.....	16
7.	<b>ICMP 报文结构</b> .....	18
8.	<b>IGMP 报文格式</b> .....	19
9.	<b>MPLS 封装报文的结构</b> .....	20
10.	<b>ARP 报文结构</b> .....	20
11.	<b>HDLC 帧格式</b> .....	21
12.	交换机环路检测报文格式.....	22
13.	光模块都是左端为发，右端为收。.....	22
14.	百兆光模块没有波长为 <b>850</b> 的，只有 <b>1310</b> 和 <b>1550</b> 。.....	23
15.	光纤知识简介.....	23
16.	交换机端口处理.....	25
17.	交换机端口速率与双工的说明.....	26
18.	<b>DCD、DTR、DSR、RTS 及 CTS</b> 等五个状态指示代表含义.....	26
19.	<b>BOOTROM 密码破解</b> .....	26
20.	串口线缆.....	27
21.	<b>IP 地址分类和私有 IP</b> .....	27
22.	<b>TCP/IP 常用端口号</b> .....	28
23.	<b>IEEE 802 标准：定义了系列局域网标准</b> .....	28
24.	<b>MAC 地址全为 1 为广播地址；第一字节的最后一个 BIT 为 1 是多播地址。</b> .....	29
25.	路由协议及其发现路由的优先级.....	29
26.	最佳路由选取原则.....	29
27.	路由协议的分类.....	29
28.	各路由协议在 <b>TCP/IP</b> 协议栈中的对应关系.....	30
29.	<b>IP 报文转发过程</b> .....	30
30.	<b>AS 同一机构管理，统一的选路策略的一些路由器。1—65411 为注册的因特网编号，65412—65535 为专用网络编号（不允许出现在公网上）。</b> .....	32
31.	各协议对应协议号.....	32
32.	交换机中端口自协商优先级（由高到低）： <b>100BASE-TX 全双工、100BASE-T4、100BASE-TX、10BASE-T 全双工、10BASE-T</b> .....	32
33.	交换机中的两种流量控制.....	32
34.	组播基于 <b>UDP</b> .....	33
35.	常用预留组播 <b>IP 地址</b> .....	35

36.	常用预留组播 MAC 地址.....	35
37.	MODEM 指示灯含义.....	36
38.	OSPF 报文头 192BITS.....	37
39.	OSPF 有五种报文类型.....	37
40.	OSPF 的 LSA 类型.....	37
41.	OSPF 邻居状态.....	38
42.	OSPF 网络拓扑类型.....	38
43.	OSPF 路由分级管理.....	39
44.	OSPF 根据网络的需求将区域划分为以下几种类型：.....	40
45.	OSPF 为什么是无环的.....	41
46.	OSPF 选路：经过骨干区域的和经过非骨干区域的路径选择.....	41
47.	OSPF 规定，只有从相同的区域学习到的路由才能形成等价路由。.....	41
48.	一台路由器是否为 ABR，取决于其在骨干区是否有 FULL 的邻居。.....	41
49.	OSPF 的缺省路由.....	41
50.	同一区域内的 OSPF 进程号应一致。.....	42
51.	OSPF 多进程与 OSPF 多实例的区别.....	42
52.	OSPF 的路由过滤分两种方式.....	42
53.	两种设定 DR 优先级的命令说明.....	42
54.	在 OSPF 中使用路由策略引入路由时，应使用基本 ACL。.....	43
55.	BGP 协议消息类型.....	43
56.	BGP 状态机.....	44
57.	BGP 选路策略.....	44
58.	BGP 传递路由的策略.....	44
59.	BGP 属性目前 16 种可扩展到 256 种，分为必遵、可选、过渡、非过渡。.....	45
60.	BGP 通告默认路由的三个步骤.....	45
61.	BGP 路由处理过程：接受路由—实施策略—路由聚合—选路—加入路由表—发布。.....	45
62.	BGP 报文比 OSPF 报文少一个的原因。.....	45
63.	BGP 中反射与联盟的比较.....	46
64.	LP 与 MED 属性的比较.....	46
65.	BGP 普通团体属性 4 字节长，扩展团体属性 8 字节长。.....	46
66.	路由引入时使用 ROUTING POLICY 过滤，路由发布和接收时用 IP PREFIX 和 ACL.....	46
67.	ISDN 简介.....	46
68.	ISDN 的用户-网络接口规范.....	47
69.	Q931 消息格式.....	48
70.	用户端与网络段交互的信息类型.....	48
71.	BRI 接口有两种类型，P2MP 接口和 P2P 接口.....	49
72.	PRI 接口为点对点接口，所以 TEI 值为 0。.....	50
73.	ISDN 网络侧功能支持情况.....	50
74.	中低端路由器产品分三个系列.....	50
75.	WEB 网管功能支持的机型.....	54
76.	高端 NE 路由器产品介绍.....	54
77.	NE20 对 NAT、GRE、L2TP、IPSEC 功能支持情况的说明.....	56
78.	NE40/NE80 对 NAT、GRE、L2TP、IPSEC 功能支持情况的说明.....	56

79.	<b>MSR 产品介绍</b> .....	56
80.	<b>交换机产品概述</b> .....	57
81.	<b>路由器上的精确匹配与交换机上的精确匹配的区别是：交换机上的精确匹配要求 ARP 表项中有精确的目的主机 IP 地址；而路由器上只要找到最长匹配的网段地址即可，无需主机 IP。（S3526 和 S3526E 支持精确匹配）</b> .....	61
82.	<b>中低端交换机 ACL 生效规则</b> .....	61
83.	<b>X.25 协议参考模型</b> .....	61
84.	<b>X.25 协议为两台通信的 DTE 之间建立的连接被称为虚电路，这种“电路”只在逻辑上存在。</b> .....	62
85.	<b>LAPB 协议简介</b> .....	62
86.	<b>XOT 简介</b> .....	62
87.	<b>X2T 简介</b> .....	63
88.	<b>PAD 是一种类似于 TELNET 的应用，可以从一端通过 X121 地址建立到另一端的 PAD 连接进行配置等操作。</b> .....	64
89.	<b>X.25 虚电路范围</b> .....	64
90.	<b>“虚电路”和“逻辑信道”</b> .....	66
91.	<b>帧中继网络用户接口上最多可支持 1024 条虚电路，其中用户可用的 DLCI 范围是 16~1007（帧中继 LMI 协议占用 DLCI 为 0 和 1023 的 PVC）。</b> .....	66
92.	<b>FR 在用户面上仅完成物理层和链路层的功能，在链路层完成统计复用、帧透明传输和错误检测，但是不提供错误后重传操作。</b> .....	67
93.	<b>帧中继默认的网络类型是 NBMA（NONBROADCAST MULTIACCESS）非广播多点可达</b> .....	67
94.	<b>帧中继的带宽管理</b> .....	68
95.	<b>DTE 与 DCE 的区分</b> .....	68
96.	<b>ARP、RARP、INARP 协议比较</b> .....	68
97.	<b>帧中继中的点对点接口和点对多点接口的区别</b> .....	68
98.	<b>目前 H3C 路由器只支持永久虚电路方式。</b> .....	69
99.	<b>ATM（ASYNCHRONOUS TRANSFER MODE）简介</b> .....	69
100.	<b>ATM 的虚链路</b> .....	70
101.	<b>VPI/VCI</b> .....	70
102.	<b>ATM 信元的转发</b> .....	71
103.	<b>ATM 的网络接口</b> .....	72
104.	<b>ATM 层次功能与工作过程</b> .....	73
105.	<b>之所以通过网上邻居和共享文件看到对方 PC，是因为基于 UDP 的广播，但只能在同一 VLAN 内“看到”，不同 VLAN 无法看到对方，但可通过输入 IP 地址进行访问。若想“看到”跨 VLAN 的 PC 需配置 UDPHelper 指定该跨 VLAN 的 PC 的 IP 地址。</b> .....	74
106.	<b>IPoEoA 应用需配置 VE 接口模板（VE 口—&gt;ATM 接口），PPPoA 需配置 VT 模板（VT 口—&gt;ATM 接口），PPPoEoA 需配置 VE 和 VT（VT 口—&gt;VE 口—&gt;ATM 口）。</b> .....	74
107.	<b>PPP 的验证</b> .....	77
108.	<b>PPP 运行流程</b> .....	78
109.	<b>MP 的配置主要有两种方式</b> .....	80
110.	<b>PPP 的 PAP 和 CHAP 认证中，单项验证时在主验证方的接口视图下配置认证方式，</b>	

从认证方只需配置用户名和密码；双向验证时两端接口视图下都需配置认证方式。	81
111. 路由器升级注意事项	81
112. CMS 问题单升级研发时问题单提交类型有 4 种	81
113. E1/T1 各接口说明	81
114. 中低端路由器的 E1 板卡和串口板卡可以跨板进行 PPP 捆绑	88
115. 中低端路由器串口对 CRC 校验的支持情况	88
116. 中低端路由器对于 E1 模块，配置接口自环命令 LOOPBACK 时，系统会强制修改接口时钟为 MASTER；如果使用直通头将收发两个 BNC 短接进行物理自环时，需要手动将时钟设置成 MASTER 模式，否则可能导致物理层无法 UP。	88
117. 中低端路由器 E1 与 E1VI 接口阻抗的异同	88
118. 网络攻击的主要方式：窃听报文、IP 地址欺骗、源路由攻击、端口扫描、DoS 拒绝服务、应用层攻击	89
119. RMON 共九组，常用的端口统计、历史、告警、事件 4 组。	89
120. 交换机端口自协商使用物理芯片来完成，不需要专用的数据报文。发送 16BIT 的报文，整个报文按 16MS 间隔重复。	89
121. 基于流的交换，第一个报文经过三层处理，其他的进行 2 次转发。包交换，每个包都要进行三层检查。	89
122. 交换机属于 MDIX 设备，PC 为 MDI 设备。物理芯片实现。	89
123. 802.1D 生成树协议	89
124. STP 报文格式如下：	90
125. RSTP 报文格式	91
126. MSTP 报文格式	91
127. 当拓扑发生变化时，STP 是否产生 TCN BPDU 取决于以下两条标准。	93
128. 对于 STP，一共有 3 个计时器影响着端口状态以及网络的收敛。	93
129. STP 端口的几种状态：	93
130. STP 拓扑变化后的 BPDU 发送处理过程	94
131. 快速生成树改进：	95
132. STP 与 RSTP 区别	95
133. 传统 STP 的问题——STP 和 RSTP 都是基于端口与 VLAN 无关的协议。	95
134. STP、RSTP 和 MSTP 的比较	95
135. STP、RSTP 和 MSTP 间 BPDU 报文的区别	96
136. 当对一个端口进行配置时，环路保护功能、ROOT 保护功能和设置边缘端口三个配置项中，同一时刻只能有一个配置项生效。	96
137. MSTP 在工程中使用的规范	97
138. STP PATH COST 的三个标准	99
139. 中低端路由器 1.74 版本中 DISPLAY BASE-INFORMATION 命令中没有 LOGBUFFER 的信息，也没有 DISPLAY LOGBUFFER 命令，可通过 DISPLAY INFO-CENTER LOGBUFFER 命令查看缓冲区中的调试和日志信息。	100
140. 路由器 CMW3.4 版本下基于 MAC 的 ACL 需在桥接模式实现；CMW1.74 版本下无此限制。CMW1.74 版本下 FIREWALL 缺省是 ENABLE 的；CMW3.4 版本下 FIREWALL 需手工 ENABLE。CMW1.74 版本下 ACL 默认是深度优先匹配；CMW3.4 版本下 ACL 默认是配置顺序匹配。	100
141. 交换机与路由器的 ACL 比较	100

142.	传统路由器的处理流程.....	101
143.	三层交换机进行数据包交换的过程。.....	103
144.	二层交换的一般流程如下：.....	104
145.	<b>MAC</b> 表项地址学习规则.....	105
146.	目前路由器实现机制是先找路由器表，再查找 <b>NAT SESSION</b> 表项； <b>NAT SERVER</b> 表项与 <b>NAT</b> 变换的 <b>SESSION</b> 表项不同，它是全局使能的表项。进行 <b>NAT</b> 变换时即使 <b>FIREWALL DISABLE</b> 也没关系，但用到包过滤则必须 <b>ENABLE</b> 。.....	105
147.	<b>PORTAL</b> 特性规格参数：.....	105
148.	原 <b>65</b> 系列交换机支持 <b>SALIENCE I、II、III</b> 交换引擎； <b>H3C 75</b> 系列只支持 <b>SALIENCE III</b> 交换引擎；而 <b>OEM</b> 给 <b>3COM</b> 的 <b>7700</b> 系列交换机支持 <b>SALIENCE I、II</b> 交换引擎， <b>7750</b> 系列交换机只支持 <b>SALIENCE III</b> 交换引擎。.....	105
149.	低端交换机有 <b>3</b> 个 <b>MAC</b> 地址，不同于路由器，在路由器上每个接口都有 <b>MAC</b> 地址。.....	105
150.	报文在转发过程中，如果是二层转发则源、目的 <b>MAC</b> 地址不会改变；如果是三层转发，那么源、目的 <b>MAC</b> 地址会改变（源 <b>MAC</b> 为当前转发接口的 <b>MAC</b> ，目的 <b>MAC</b> 为下一跳目的的 <b>MAC</b> ），在这个过程中源、目的的 <b>IP</b> 地址是不会改变的，无论是二层转发还是三层转发。.....	106
151.	二层与三层的区别是：三层对 <b>IP</b> 报文进行处理和转发；对报文的检测属于二层范畴。上 <b>CPU</b> 处理的报文并不能说明就是三层处理，只要是协议报文都会上 <b>CPU</b> 进行处理，二层协议如 <b>STP</b> ， <b>GVRP</b> 都会上 <b>CPU</b> 进行处理。.....	106
152.	在 <b>NAT SERVER</b> 配置中，如果内外网想通过域名访问，方法如下.....	106
153.	配置 <b>PVLAN (ISOLATE-USER-VLAN)</b> 的注意事项——节约 <b>VLAN ID</b> .....	106
154.	配置 <b>SUPER VLAN</b> 的注意事项——节约 <b>IP</b> 地址.....	107
155.	当作 <b>MP</b> 捆绑时，在虚接口启用 <b>OSPF</b> ， <b>VIRTUAL-TEMPLATE</b> 默认 <b>OSPF</b> 网络类型为 <b>NBMA</b> ，因此必须手工制定邻居。.....	107
156.	配置 <b>QOS</b> 时提示带宽不够的解决办法.....	107
157.	<b>SSH</b> 是基于 <b>TCP</b> 的连接。.....	107
158.	<b>AR18-2X</b> 做 <b>DDNS</b> 时当本地公网地址改变时，不能自动更新。.....	107
159.	一个交换机 <b>A</b> 端口下连另一台交换机 <b>B</b> ，该交换机 <b>A</b> 端口的 <b>MAC</b> 表项会学习到交换机 <b>B</b> 所学到的所有 <b>PC</b> 的 <b>MAC</b> ；如果将其中的一台 <b>PC</b> 的 <b>MAC</b> 绑定到其他端口，则该 <b>PC</b> 无法正常通信。.....	107
160.	路由器在发出 <b>ARP</b> 请求后，就会生成一个 <b>ARP</b> 表项，其中 <b>MAC</b> 地址为 <b>0</b> ，当收到应答后，会用收到的 <b>MAC</b> 地址更新表项，但如果没有收到的话该表项会一直保存（直到一段时间后老化）。.....	107
161.	如果在一个接口上同时配置了包过滤和 <b>NAT</b> ，发送数据包的时候先进行包过滤，然后进行 <b>NAT</b> ；接收数据包的时候先进行 <b>NAT</b> ，然后进行包过滤。.....	109
162.	<b>800</b> 问题分为咨询、配置和故障三类。根据问题单处理的不同阶段，将该问题的处理状态从原来所处处理状态变更为“处理中”、“研发处理中”、“已有解决方案”、“处于观察中”、“一般关闭”五种状态之一。.....	109
163.	<b>ARP</b> 表项与 <b>MAC</b> 表项内容.....	109
164.	我们的路由器现在不支持 <b>FTP</b> 的被动模式，如果出现在外网无法访问内网映射出去的 <b>FTP</b> 服务器，需要将其“使用被动模式”的选项去掉。.....	109
165.	我们的 <b>VRP</b> 和 <b>CMW</b> 使用的是同一个版本文件，只是在启动的时候获取主板上的逻辑信息来判读是 <b>QUIDWAY</b> 还是 <b>H3C</b> 品牌，对应显示不同的版本信息。.....	109

166.	<b>3COM</b> 设备的 <b>3C</b> 编码与设备对应关系.....	109
167.	两台交换机做 <b>VRRP</b> 的说明.....	110
168.	<b>3COM</b> 交换机与其他厂商交换机互连说明。.....	110
169.	目前 <b>DMC</b> 功能对于大部分常用网络设备都可以识别，如果遇到部分无法识别的设备，请采用如下方法尝试：.....	110
170.	<b>AR18</b> 系列路由器的 <b>WEB</b> 网管功能需上传 <b>HTTP.ZIP</b> 的文件包（不能使用 <b>XMODEM</b> 方式）；而防火墙无需上传该文件包，因为它是随主机软件一同上传到设备上去的。.....	110
171.	查看并解决 <b>ARP</b> 欺骗病毒的方法.....	110
172.	我们的路由器缺省允许 <b>SSH</b> 登录，但是又没有配置其他 <b>SSH</b> 参数。 当有试图使用 <b>SSH</b> 方式登陆的时候就发现开始连接，然后断开的 <b>LOG</b> 信息。可以使用下面的命令解决这个问题，即禁止 <b>SSH</b> 登录。.....	111
173.	<b>AR18</b> 系列路由器的以太网启子接口后无法 <b>PING</b> 通子接口 <b>IP</b> 地址，只有连接上交换机并映射 <b>VLAN</b> 后，才可以 <b>PING</b> 通自身设置的 <b>IP</b> 地址。.....	111
174.	中低端交换机的 <b>COMBO</b> 复用口需先 <b>SHUTDOWN</b> 电口，光口才能 <b>UP</b> （如有必要需 <b>UNDO SHUTDOWN</b> 光口，如 <b>S5500</b> ）。.....	112
175.	<b>AR18-22S-8</b> 和 <b>AR18-23S-1</b> 在配置 <b>IPSEC</b> 时，本身使用的就是硬件加密卡，无需配置命令 “ <b>IPSEC CARD-PROPOSAL</b> ”（也没有该命令）。.....	112
176.	<b>IKE</b> 是 <b>UDP</b> 上的应用层协议，是 <b>IPSEC</b> 的信令协议。.....	112
177.	配置 <b>IPSEC</b> 时若使用接口上的 <b>SUB</b> 地址建立隧道，必须配置 “ <b>LOCAL-ADDRESS</b> 从 <b>IP</b> ”。.....	112
178.	在 <b>GRE OVERIPSEC WITH OSPF</b> 的应用中， <b>GRE</b> 的作用是： <b>IPSEC</b> 没有逻辑或物理接口， <b>OSPF</b> 需要接口做路由，只能通过 <b>GRE</b> 进行封装。.....	112
179.	在进行 <b>L2TP</b> 的配置中，当内网通过外网口进行 <b>NAT</b> 变换时，无需在 <b>NAT</b> 变换的 <b>ACL</b> 中 <b>DENY</b> 掉 <b>L2TP</b> 的数据流，因为数据是将 <b>VT</b> 模板接口作为访问的下一跳，而 <b>NAT</b> 变换是应用在物理接口上的，实际不会对 <b>L2TP</b> 的流量产生影响。.....	112
180.	配置 <b>IPSEC</b> 野蛮模式时，中心与分支的私网网段应在不同网段，因为若是相同网段的报文 <b>PC</b> 不会将其送到内网网关。此外，当存在多个分支时，应配置多个 <b>PEER</b> ，之后匹配相同模板名不同节点号进行区分（新版本）或使用不同的模板（老版本建议使用该方式）。其他 <b>VPN</b> 技术各私网 <b>IP</b> 也应该在不同网段。.....	112
181.	<b>IPSEC</b> 主模式和野蛮模式的区别.....	112
182.	<b>DVPN</b> 隧道的建立基于 <b>UDP</b> 端口 <b>9010</b> 。.....	113
183.	<b>AR18-2X</b> 对配置的要求非常高，可能因为少敲了几个命令行就导致掉线的。.....	113
184.	对 <b>Qos</b> 队列的理解。.....	113
185.	<b>MSR(8048)</b> 路由器 <b>COMWARE</b> 软件基本版( <b>BI</b> )与标准版( <b>SI</b> )相关说明.....	114
186.	只有 <b>GRE</b> 支持封装组播报文。.....	116
187.	<b>H3C AR28</b> 系列路由器与 <b>QUIDWAY AR28</b> 系列路由器是两个不同品牌的路由器，虽然功能特性一致，但硬件构成和软件逻辑有一些区别。.....	116
188.	当用户需要现场支持、返修时，我们把客户信息反馈给热线和备件让她们给客户回电，不要让客户多次拨打 <b>800</b> 电话！！.....	117
189.	<b>VRP1.74</b> 版本配置的 <b>SUB</b> 地址不能与主 <b>IP</b> 同网段； <b>VRP3.4</b> 主从 <b>IP</b> 可同网段。.....	117
190.	低端路由器上只有两个物理串口，但执行 <b>DISP CUR</b> 后却显示有 <b>S0</b> ， <b>S1</b> 和 <b>S2</b> 三个串口.....	117
191.	中低端路由器对于 <b>CF</b> 卡的支持.....	117

192.	<b>8040(AR28、AR46 路由器)和 8043(AR18 路由器)均不支持 802.1x 认证；8048(MSR 系列路由器)交换板支持该功能</b> .....	118
193.	所有的 <b>SA</b> 模块和设备自带的串口都支持异步模式，并可以通过命令进行修改，只有 <b>R2620/R2621</b> 的串口比较特殊：只支持同步模式。.....	118
194.	<b>AR</b> 系列路由器与 <b>MSR</b> 系列路由器 <b>TELNET-SERVER</b> 功能实现的区别.....	118
195.	<b>AR18-2X</b> 如何关闭掉 <b>WWW</b> 管理服务.....	118
196.	<b>AR18</b> 系列路由器如何在 <b>BOOTROM</b> 菜单下看配置文件.....	118
197.	什么是 <b>MSCA</b> 和 <b>MPUF</b> .....	118
198.	<b>VPM</b> 和 <b>VCPM</b> 的作用是什么.....	118
199.	<b>NE</b> 系列路由器 <b>V5</b> 版本的 <b>PAF</b> 和 <b>LICENSE</b> 文件说明.....	119
200.	如何查看设备的 <b>CPU</b> 占用率.....	119
201.	<b>FE</b> 单板的芯片型号区分.....	119
202.	<b>BOM</b> 编码信息.....	119
203.	板卡的高度有 <b>0.5U</b> 、 <b>1U</b> .....	120
204.	关于 <b>SIC</b> 卡以太网接口模块的使用.....	120
205.	<b>AR46</b> 上 <b>ERPU</b> 与 <b>RPU</b> 主控板的区别.....	120
206.	中低端路由器板卡使用注意事项.....	121
207.	关于硬件流控和软件流控.....	121
208.	<b>ISDN</b> 非常有用的命令.....	122
209.	中低端路由器 <b>TCP MSS</b> 的实现原理.....	122
210.	<b>NAT SERVER</b> 映射比路由器本地服务优先.....	123
211.	<b>S3900</b> 和 <b>S5600</b> 设备在 <b>BOOTROM</b> 中选择跳过配置启动后，会在每次启动后都跳过配置，要想解决需再次进入 <b>BOOTROM</b> 菜单选择该选项后输入“ <b>No</b> ”。.....	123
212.	<b>ARP</b> 静态绑定的三种方式.....	124
213.	<b>AR28/AR46</b> 系列路由器 <b>FCM</b> 单板在线升级.....	124
214.	<b>AR18</b> 系列路由器对于 <b>ARP</b> 欺骗病毒的防治命令说明.....	124
215.	交换机防 <b>ARP</b> 攻击命令说明.....	124
216.	交换机上的 <b>DHCP-SNOOPING</b> 和 <b>DHCP RELAY</b> 不能同时启用。.....	125
217.	对于 <b>ARP SPOOF</b> 病毒所进行攻击的说明.....	125
218.	免费 <b>ARP</b> 报文发送的目的有两个.....	125
219.	<b>ARP</b> 工作原理.....	125
220.	使用 <b>ROUTE-POLICY</b> 将路由进行路由过滤时应注意.....	126
221.	<b>H3C</b> 无线全系列产品.....	126
222.	<b>NAT</b> 变换使用的 <b>ACL</b> 可以是高级访问控制列表， <b>RULE</b> 的配置可以精确指定到端口。.....	127
223.	判断 <b>AR</b> 系列路由器串口是否损坏的方法.....	127
224.	线速转发指标计算方法.....	127
225.	交换机中广播风暴抑制比的说明.....	128
226.	<b>V/R/B/D</b> 版本号说明.....	128
227.	交换机有三种转发方式，目前我们的交换机使用的是存储转发方式。.....	128
228.	支持 <b>VLAN</b> 的交换机有两种 <b>MAC</b> 地址学习方式分别是 <b>IVL</b> 和 <b>SVL</b> 。.....	129
229.	三层交换机与路由器在转发操作上的主要区别在于其实现的方式：.....	130
230.	三层交换技术的发展.....	130
231.	<b>IRF</b> 基础.....	131



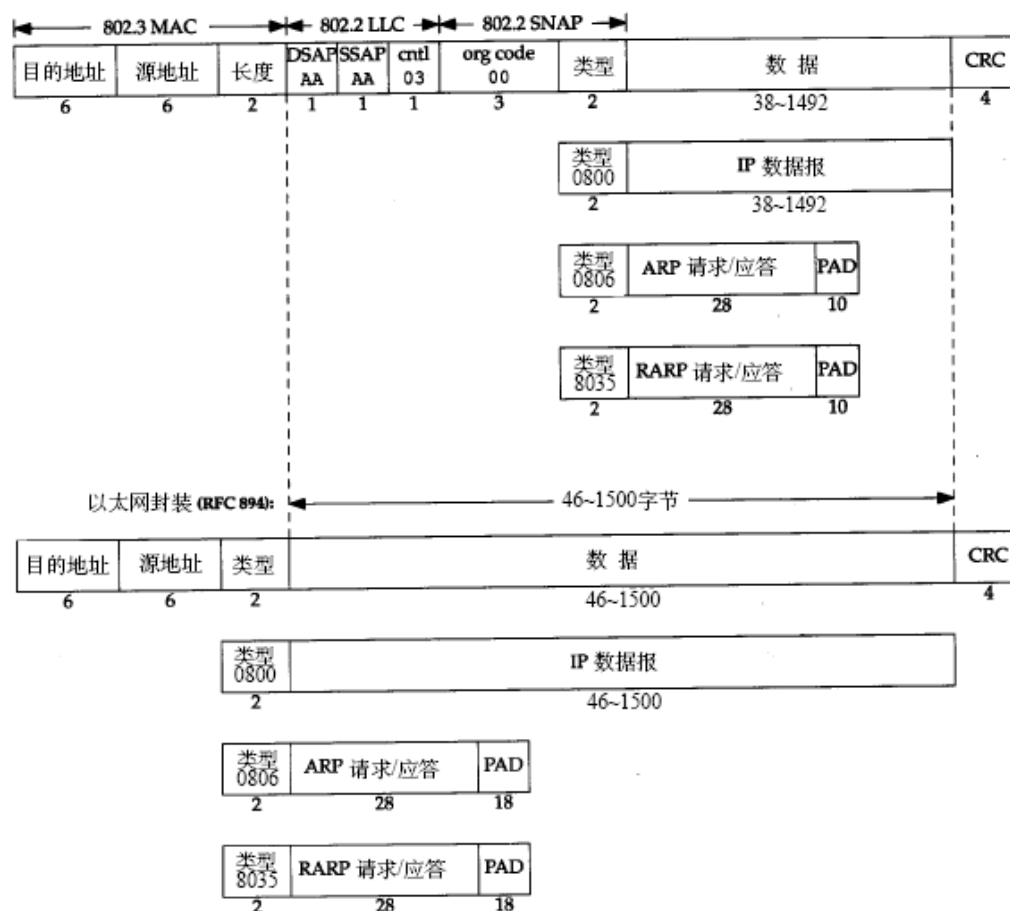
232.	备件知识.....	131
233.	中低端路由器 <b>B03</b> 版本 <b>TELNET VPN-INSTANCE</b> 时必须指定源地址或者源端口，否则 <b>TELNET</b> 不能连接。而其它版本无需指定源地址或原端口。.....	133
234.	路由的核心功能主要包括数据报文转发和路由处理两方面。.....	133
235.	<b>GVRP</b> 注册和注销状态维护原理.....	133
236.	<b>TELNET</b> 用户登陆规则.....	136
237.	路由器接口错帧统计说明.....	137
238.	交换机接口错误帧统计说明.....	137
239.	以太网交换机中， <b>AUX</b> 口和 <b>CONSOLE</b> 口是同一个口，所以用户界面类型中只有 <b>AUX</b> 口用户界面类型。.....	139
240.	<b>VLAN-VPN</b> 原理介绍.....	139
241.	端口汇聚分为手工汇聚、动态 <b>LACP</b> 汇聚和静态 <b>LACP</b> 汇聚。（推荐使用静态汇聚）.....	140
242.	<b>VOICE VLAN</b> 功能介绍.....	142
243.	交换机中 <b>ARP</b> 表项检查功能指不学习 <b>MAC</b> 地址为组播 <b>MAC</b> 的 <b>ARP</b> 表项，默认使能。.....	144
244.	二层设备的 <b>MAC</b> 地址学习都是通过源 <b>MAC</b> 地址学习来进行的。.....	144
245.	“ <b>RESOURCE ERRORS</b> ” 是 <b>AR46 RPU</b> 接口下特有的统计错误类型，一般是由 <b>CPU</b> 高、端口队列溢出造成的。通过升级路由器版本解决。.....	144
246.	路由器和交换机的优先级说明.....	144
247.	<b>H3C</b> 交换机启动后将有 5 个缺省的 <b>OUI</b> 地址.....	145
248.	交换机 <b>IP</b> 、 <b>MAC</b> 和端口绑定说明.....	145
249.	交换机 <b>AM IP-POOL</b> 功能说明（只限制三层访问，无法对端口下的二层访问进行限制）。.....	146
250.	当以太网接口启用 <b>DOT1X</b> 认证后，只有将该接口配置为基于端口的认证方法后，才可以使用 <b>DOT1X GUEST-VLAN</b> 的配置。.....	146
251.	<b>PCA</b> 无法 <b>PING</b> 通 <b>PCB</b> 但可以通过 <b>FTP</b> 的方式进行访问，但 <b>PCB</b> 可以 <b>PING</b> 通 <b>PCA</b> ，原因有可能是在 <b>PCB</b> 上的防火墙（ <b>WINDOWS XP</b> 系统）配置中的“例外”选项卡中，将“文件和打印机共享”排除在例外允许访问之外。.....	146
252.	交换机作集中式 <b>MAC</b> 认证时， <b>MAC</b> 地址作为用户名密码时 <b>MAC</b> 地址间应去掉“—”。.....	146
253.	纯二层组播不用“ <b>MULTICAST ROUTING-ENABLE</b> ”；未知组播丢弃如果不配置查询器不能开启，如果不开启查询器只开启未知组播丢弃功能，会导致纯二层网络中所有组播都是未知组播而被丢弃。.....	147
254.	<b>VRP</b> 和 <b>COMWARE</b> 不是操作系统，是基于操作系统之上的应用平台。.....	147
255.	<b>SNMP</b> 网管服务器发送消息查询设备采用轮询方式，报文是基于 <b>UDP</b> 的 <b>161</b> 端口；设备主动发送自身消息给 <b>SNMP</b> 网管服务器基于 <b>UDP</b> 的 <b>162</b> 端口，该报文为 <b>TRAP</b> 报文。.....	147
256.	<b>RADIUS</b> 本地认证配置在路由器和交换机上的区别.....	147
257.	静态路由只有在物理层 <b>DOWN</b> 的情况下，才会被路由表删除，即使配置 <b>DETECT-GROUP</b> 侦测，也不能删除物理 <b>UP</b> 、但协议层 <b>DOWN</b> 的静态路由。.....	147
258.	在一个 <b>2FXS</b> 卡上接两个电话，在该路由器上配置两个 <b>POTS</b> 实体，即可实现通话。.....	147
259.	当出现 <b>PING</b> 对端地址只有第一个报文能通时，多于接口快转功能的开启有关。.....	147

260.	在路由器 VRP 1.74 版本配置子接口时，应先映射 VLAN 再配置 IP 地址。.....	147
261.	备件服务应确保 5 方面准确无误.....	147
262.	在 TUNNEL 口上应用 Qos 的 LR、CBQ 等时，需关闭接口快转功能。.....	148
263.	在 SAE 接口上配置工作在“异步模式“后，系统视图下才会出现“USER- INTERFACE TTY”。.....	148
264.	中低端交换机与 SOHO 产品易混淆产品列表.....	148
265.	配置 RADIUS 认证时，只有在 RADIUS SCHEME 中配置服务类型为 EXPAND 或 HUAWEI，才能实现 SERVER 下发用户级别。.....	148
266.	交换机端口链路汇聚（或聚合）都是基于流的负载分担（没有命令进行更改）， 只有使用手工链路聚合时，端口数量在加减过程中才不会产生丢包；如果一端设 备配置端口汇聚另一端不配置，则会产生丢包。.....	149
267.	交换机和路由器进入隐含命令模式都需在 SYSTEM 视图下输入“_”。.....	149
268.	配置镜像时，交换机上只能配置一个监控端口。.....	149
269.	配置交换机接口 OSPF 的 COST 值时，只能在虚接口下配置，物理接口下没有该命 令“OSPF COST”。.....	149
270.	H3C 品牌的交换机可以通过命令查看设备序列号，路由器不成。.....	149
271.	3Com 与 H3C 设备的 OEM 关系.....	149
272.	RADIUS 和 HWTACACS 的 SCHEME 可以同时使用，在 DOMAIN 的配置中进行区分， 两者的区别如下：.....	150
273.	在路由器上应用策略路由时，更改下一跳的地址只要路由可达即可（不能是缺省 路由）；在交换机上更改的下一跳地址必须是直连的下一跳地址。.....	150
274.	802.1x 的工作机制.....	150
275.	802.1X 的 EAPOL 报文格式.....	151
276.	802.1X 的 EAP 报文格式.....	152
277.	802.1x 的认证过程.....	153
278.	802.1x 的定时器.....	154
279.	802.1X 的认证触发方式.....	155
280.	802.1X 配置注意事项.....	155
281.	AR28、46 加密卡的区别.....	156
282.	低端交换机使用 DISPLAY ACL 无法看到 RULE 的匹配关系，只能使用流量统计功 能。.....	156
283.	交换机端口上出现大量的 CRC 统计错误，可能原因是链路问题或两端端口协商问 题。.....	156
284.	在交换机上使用“DISPLAY ARP”命令显示出的统计含义。.....	156
285.	VRRP 的虚拟路由器的 IP 地址必须和备份组中成员交换机使用的真实 IP 地址在同 一网段。.....	157
286.	交换机中“DISPLAY IP STATISTIC”和“DISPLAY INTERFACE”两个命令的区别。.....	157
287.	交换机中使用“AM USER-BIND”命令不可以替代“ARP 入侵检测”功能。.....	159
288.	交换机入端口流量大于出端口带宽时，交换芯片检测到自身 BUFFER 不足，因此在 入端口就丢弃报文。如果是二层报文可使用流量统计进行观察，上 CPU 的报文使用 DISPLAY IP STATISTICS 进行观察。.....	159
289.	确认用户从 DHCP SERVER 获取的 IP 地址和用户主机的 MAC 地址的对应关系有两 种方式。.....	159
290.	修改交换机 MSTP 的端口 COST 值时，应修改根端口的 PATHCOST。.....	160

291.	使用 V5 平台的交换机进行 WEB 网管时无需上传相关的管理压缩文件，只需在交换机上设置 IP、TELNET 用户名即可。	160
292.	交换机中，当报文写道 Cos 和 DSCP 值时，以 Cos 为发送标准；每个 IP 报文都带着固定的 DSCP 值，一般全部为 0。	160
293.	更改交换机 MAC 地址的方法。	160
294.	交换机中只有 S56、S51 有 COMBO 口的概念，S39、S36 系列交换机后面的 SFP 模块没有 COMBO 口的概念。即只有所有口都是千兆口时才会有 COMBO 口。	161
295.	S39、S36 交换机以前存在带有上下箭头的接口用来进行堆叠，不带箭头的接口不能进行堆叠，现在升级到最新版本后，所有 SFP 接口都可进行堆叠，但要成对使用，即使用 1、2 口或 3、4 口，不能使用 1、3 口或 2、4 口。	161
296.	V5 版本的本地账号通过 DISPLAY CURRENT 是无法显示的。	161
297.	对于路由器来说 VRP1.74 版本的地址池是在系统视图下配置，到了 V3、V5 都要求在 DOMAIN SYSTEM 下进行配置。	161
298.	VLAN 模式是 SVL 的交换机，使用“DISPLAY MAC-ADDRESS”命令显示内容中，VLANID 项显示为 N/A。	161
299.	交换机中的端口配置了“MAC-ADDRESS MAX-MAC-COUNT 0”命令后，由于该端口 MAC 表项为空，所有到达该端口的报文都会被丢弃而不会在 VLAN 内广播。	161
300.	交换机中支持“IGMP-SNOOPING GROUP-POLICY”功能有两个前提条件。	161
301.	使用 V5 平台的交换机在配置 ACL 时的注意事项。	161
302.	H3C 交换机支持 JUMBO 帧最大长度为 9216 字节。	162
303.	在 V5 平台交换机上应用用户自定义流模板时应关闭如下功能：	163
304.	哑终端占用网络带宽得计算方法。	163
305.	交换机中 QinQ 技术内层标签类型为 0x8100；外层标签类型为 0x9100。	164
306.	SSL VPN——SECURE SOCKET LAYER VPN 是基于 TCP 建立的，从 1.0 到 3.0，但现在很少使用，将其取而代之的是 TLS VPN（1.0）。	164
307.	交换机中 S39/36 堆叠后跨 UNIT 进行端口隔离不生效，而 S56 设备可以实现。	164
308.	在进行 RIP 和 OSPF 的路由配置时，对于 NBMA 的网络类型必须手工指定邻居（使用“PEER”命令）。	164
309.	在低端交换机中，从 IP 电话发送到交换机的数据被划分到 VOICE VLAN 后，Cos 和 DSCP 的优先级都会改变，Cos 变为 6，DSCP 被设置为 46。如果通过 QoS 的重标记功能再次改变该 VOICE VLAN 的数据流，可能由于 ACL 冲突无法实现。	165
310.	在低端交换机 V5 平台配置 RADIUS 认证（含 DOT1X）时，在 DOMAIN 视图下必须认证授权都配置且使用方案应一样，计费的配置可选。	165
311.	IP 地址冲突在 IPV4 上都是靠 ARP 报文的发送来检测的，所以要想检测并报告必须是和自己的 IP 地址冲突才会上报。两个 PC 的地址冲突和交换机根本没有关系，交换机也无法判断，所以不会上报 TRAP 信息。	165
312.	低端交换机中 S39SI 与 EI 设备无法进行堆叠。	165
313.	低端交换机中配置远程镜像时，源端口不能镜像双向报文，即只能配置“INBOUND”或“OUTBOUND”方向。	165
314.	S36/56 交换机上 MODE 切换按钮的说明	165
315.	交换机 Qos 优先级理解	165
316.	VRRP 虚 IP 地址对应的 MAC 地址说明	166
317.	在低端交换机同一端口上下发二层和三层 ACL 时，按照各交换机下发顺序生效，并不是二层优先。	167

318.	集群式堆叠数设备，前面板的码管只会显示交换机的角色，不会向 <b>IRF</b> 那样显示设备的 <b>UNIT</b> 号，此外也不能想 <b>IRF</b> 堆叠那样，从一台 <b>UNIT</b> 上看到所有的配置信息。.....	167
319.	无法通过 <b>TELNET VRRP</b> 组的虚 <b>IP</b> 方式登录交换机和路由器。.....	168
320.	千兆 <b>SFP</b> 电口模块是否支持 <b>10/100/1000</b> 的速率配置，取决于所插设备。如 <b>S56</b> 支持配置 <b>10/100/1000</b> ，而 <b>S36</b> 设备不支持。.....	168
321.	支持 <b>MCE</b> 功能的交换机在配置时，应先配置“ <b>SWITCH-MODE MCE</b> ”命令，并按提示重启设备，之后使用“ <b>DISPLAY SWITCH-MODE</b> ”命令查看设备是否工作在 <b>MCE</b> 模式，如果是才可以开始配置，否则会提示“ <b>VPN-TABLE IS FULL</b> ”。.....	168
322.	在交换机上，策略路由就是指指的是流量的重定向。低端交换机只有 <b>V5</b> 平台产品支持。.....	168
323.	<b>S36</b> 和 <b>56</b> 不支持 <b>WEB</b> 页面登录的 <b>TACACS</b> 认证，只支持 <b>LOCAL USER</b> 和 <b>TELNET</b> 用户认证。.....	168
324.	<b>PC</b> 发送的报文如果目的 <b>MAC</b> 地址填充为零或与交换机上的网关不在同一网段，那么交换机无法学习到其 <b>ARP</b> 表项。.....	168
325.	配置后不保存设备配置信息，重启后就会出现无法加入堆叠体的现象。.....	168

## 1. 两种以太网帧格式及其封装



注:

8863

Discovery Stage ———应用于 PPPoE

8864

PPP Session Stage ———应用于 PPPoE

9001

交换机环路检测协议

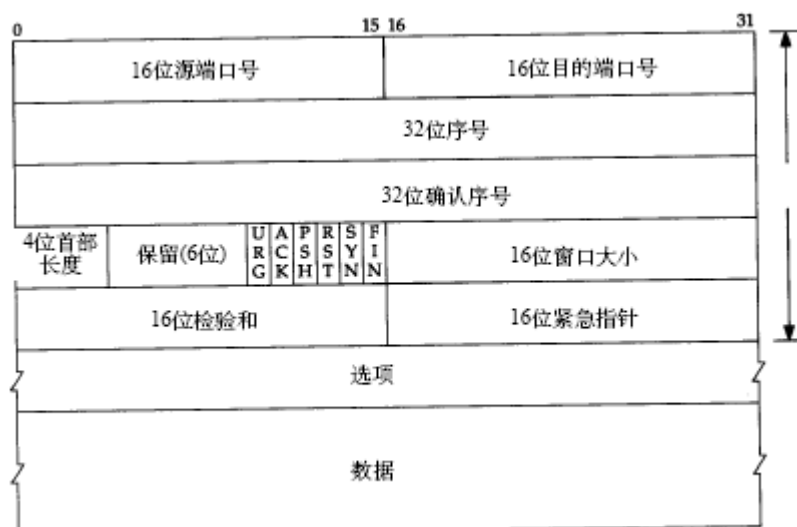
8847/8848

MPLS 单播/组播报文

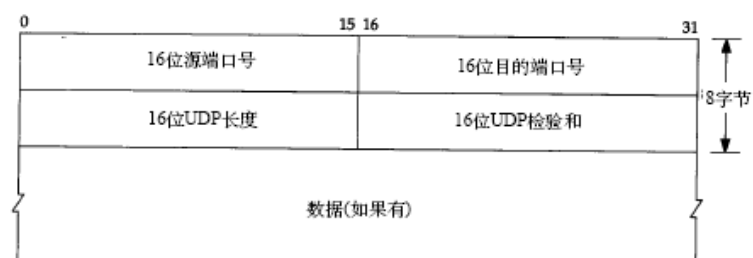
## 2. IP 首部 20 字节



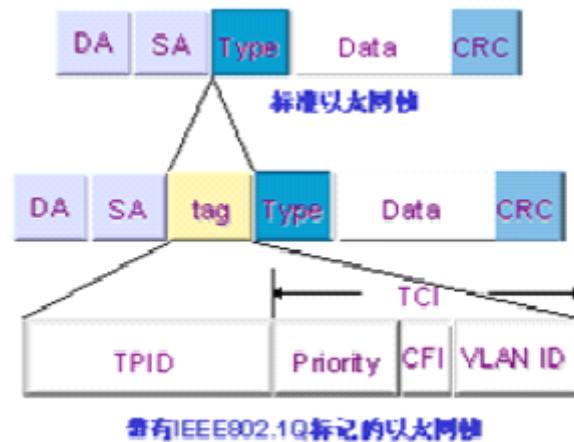
## 3. TCP 首部 20 字节



## 4. UDP 首部 8 字节



## 5. VLAN 格式



TPID (Tag Protocol Identifier) 是 IEEE 定义的新的类型, 表明这是一个加了 802.1Q 标签的帧。TPID 包含了一个固定的值 0x8100。

TCI 是包含的是帧的控制信息, 它包含了下面的一些元素:

**Priority:** 这 3 位指明帧的优先级。一共有 8 种优先级, 0—7。IEEE 802.1Q 标准使用这三位信息。

**Canonical Format Indicator( CFI ):** CFI 值为 0 说明是规范格式, 1 为非规范格式。它被用在令牌环/源路由 FDDI 介质访问方法中来指示封装帧中所带地址的比特次序信息。

**VLAN Identified( VLAN ID ):** 这是一个 12 位的域, 指明 VLAN 的 ID, 一共 4096 个, 每个支持 802.1Q 协议的交换机发送出来的数据包都会包含这个域, 以指明自己属于哪一个 VLAN。

### vlan 的分类:

- (1) 基于端口的 vlan;
- (2) 基于 mac 地址的 vlan;
- (3) 基于协议的 vlan;
- (4) 基于子网的 vlan。

## 6. PPP 格式和 PPPoE 格式

### PPP 格式

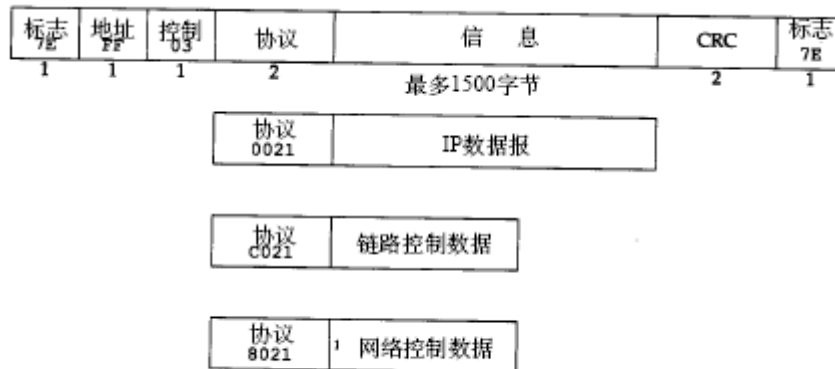
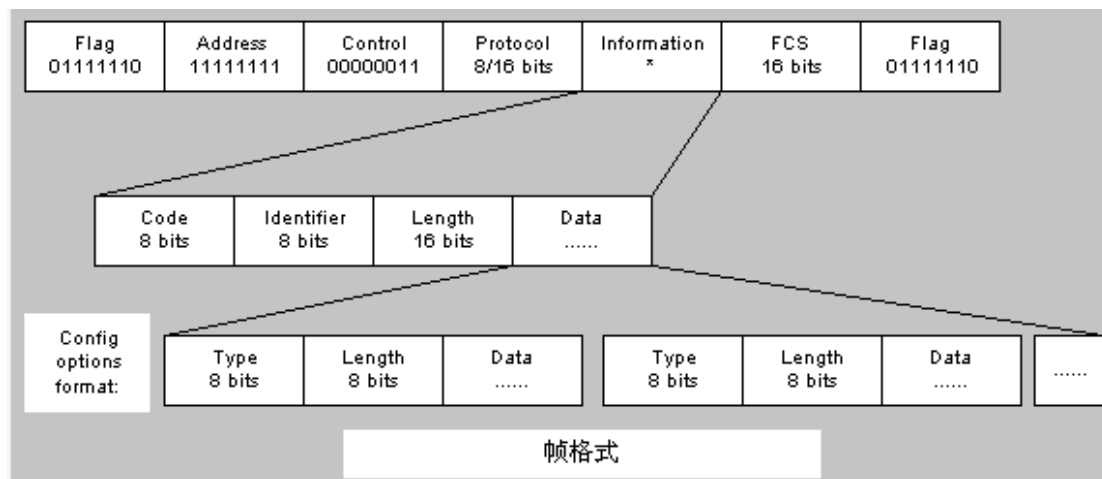


图2-3 PPP数据帧的格式



**注：**Code 域表明了此报文为哪种 PPP 协商报文。Identifier 域标志协商包文的唯一性，用于进行协商报文的识别与匹配。Length 域为此协商报文长度（包含 Code 及 Identifier 域）。Data 域所包含的为协商报文内容。Type 为协商选项类型，其后的 Length 为此协商选项长度（包含 Type 域），紧接着的 Data 域为协商选项具体内容（这里叫做 value，描述起来更方便些）。

<b>0021</b>	<b>Internet Protocol——IP</b>
<b>C021</b>	<b>Link Control Protocol——LCP</b>
<b>8021</b>	<b>Internet Protocol Control Protocol——IPCP</b>
<b>C023</b>	<b>Password Authentication Protocol——PAP</b>
<b>C223</b>	<b>Challenge Handshake Authentication Protocol——CHAP</b>
<b>C227</b>	<b>PPP EAP</b>
<b>8281</b>	<b>MPLS CP</b>

其他如下：

常用 protocol 代码：

0021	Internet Protocol
002b	Novell IPX



002d	Van Jacobson Compressed TCP/IP
002f	Van Jacobson Uncompressed TCP/IP
8021	Internet Protocol Control Protocol
802b	Novell IPX Control Protocol
8031	Bridging NC
C021	Link Control Protocol
C023	Password Authentication Protocol
C223	Challenge Handshake Authentication Protocol

常用 code 值:

0x01	Configure-Request
0x02	Configure-Ack
0x03	Configure-Nak
0x04	Configure-Reject
0x05	Terminate-Request
0x06	Terminate-Ack
0x07	Code-Reject
0x08	Protocol-Reject
0x09	Echo-Request
0x10	Echo-Reply
0x11	Discard-Request
0x12	RESERVED

常用协商 type 值:

0x01	Maximum-Receive-Unit
0x02	Async-Control-Character-Map
0x03	Authentication-Protocol
0x04	Quality-Protocol
0x05	Magic-Number
0x06	RESERVED
0x07	Protocol-Field-Compression
0x08	Address-and-Control-Field-Compression

## PPPoE 格式

以太网的帧格式如图所示:

DESTINATION -ADDR 6 octets	SOURCE-ADDR 6 octets	ETHER-TYPE 2 octets	payload	CHECKSUM
----------------------------------	-------------------------	------------------------	---------	----------

**Ether-Type** 域在发现阶段为 0x8863，在 PPP 会话阶段为 0x8864。

在 payload 中封装的 PPPoE 数据包格式如图所示:

VER 4 bits	TYPE 4 bits	CODE 8 bits	SESSION_ID 16 bits
LENGTH      2 octets			payload      2 octets

其中，VER 和 TYPE 的值在 PPPoE 的不同阶段不变，都为 0x1。CODE 域为 8 比特长，在发现阶段有以下几种 CODE 值：

CODE	包类型
0x09	PADI
0x07	PADO
0x19	PADR
0x65	PADS
0xa7	PADT

PPPoE 有两个不同的阶段：发现阶段和 PPP 会话阶段。

### (1) 发现阶段

与 PPP 建立的端对端的关系不同，发现阶段建立的是一种客户服务器的关系。通过发现阶段，一个主机（客户端）可以发现一个接入集中器（服务器端）。由于网络的拓扑结构，一个主机可以和多个接入集中器相联系，发现阶段允许主机先找到所有的接入集中器，然后从中挑选一个与之通信。发现阶段顺利结束后，主机和接入集中器都可以得到它们在以太网上建立点到点连接时所需要的信息，**即用来唯一定义一个会话的两个因素：对端的以太网地址和会话标识。**

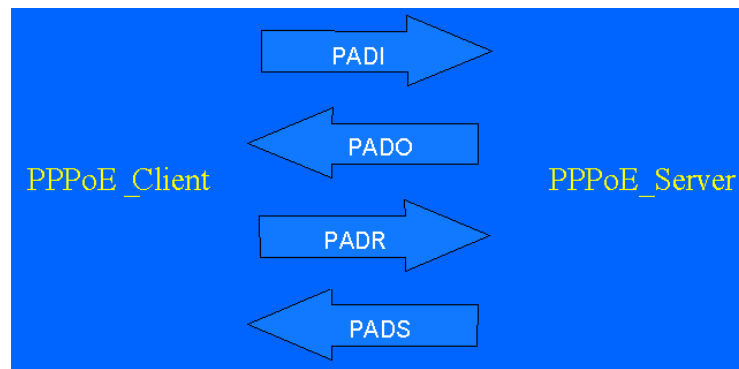
发现阶段可以分为四个步骤：

**第一步：**主机在本以太网内**广播一个 PADI 包**，在此包中包含主机想要得到的服务类型信息。

**第二步：**以太网内的所有接入集中器在收到这个初始化包后，将其中请求的服务与自己能提供的服务进行比较，其中可以为此主机提供此服务的接入集中器**发回 PADO 包**，不能提供此服务的集中器不能发 PADO 包。

**第三步：**主机可能收到多个集中器的 PADO 包，主机通过 PADO 的内容，依据一定的条件从发回 PADO 包的可提供服务的接入集中器中挑选一个，并向它发回一个会话请求包 **PADR（非广播）**，在这个包中再次包含所想得到的服务的信息。

**第四步：**被选定的接入集在收到会话请求包 PADR 后，就开始准备进入 PPP 会话阶段。它会产生一个会话标识以唯一的标识它和主机的这段 PPPoE 会话。并把这个特定的会话标识包含在会话确认包 **PADS** 中**发回给主机**，如果没有错误发生就进入到 PPP 会话阶段，而主机在收到会话确认包后如果没有错误发生也进入到 PPP 会话阶段。



## (2) PPP 会话阶段

一旦 PPPoE 的会话阶段开始后，主机和接入集中器之间就依据 PPP 协议传送 PPP 数据，进行 PPP 的各项协商和数据传输。在这一阶段传输的数据包中必须包含在发现阶段确定的会话标识并保持不变。正常情况下，会话阶段的结束是由 PPP 协议控制完成的，但在 PPPoE 中定义了一个 PADI 包用来结束会话，主机或者接入集中器可以在 PPP 会话开始后的任何时候通过发送这个数据包来结束会话。

对于在 PPP 会话阶段进行的一系列协商中的 LCP 协商，PPPoE 有如下的要求：

- ①、建议使用魔术字选项
- ②、建议不使用协议字段压缩选项 (Protocol Field Compression PFC)
- ③、任何一端都不能请求以下选项：

Field Check Sequence (FCS) Alternatives

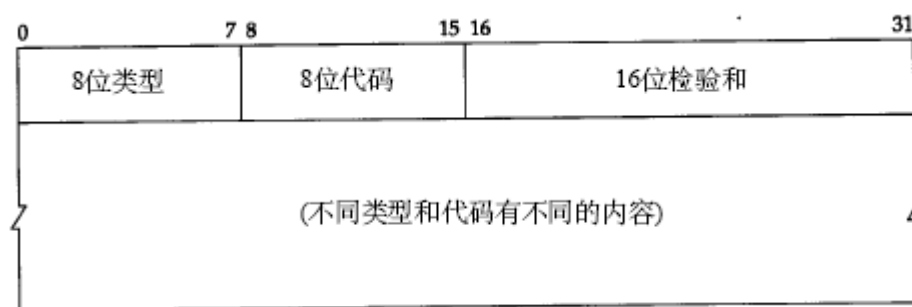
Address-and-Control-Field-Compression (ACFC)

Asynchronous-Control-Character-Map (ACCM)

如果发出了这些请求则必须被拒绝。

- ④、Maximum-Receive-Unit (MRU) 选项协商不能超过 1492 字节。

## 7. ICMP 报文结构

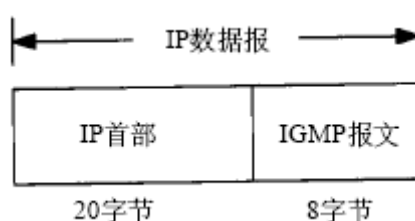


ICMP 报文类型如下：

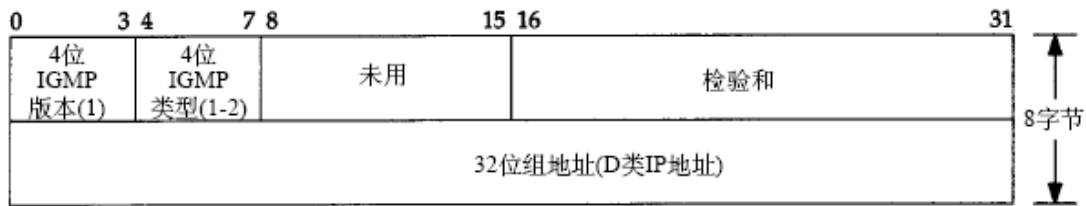
类 型	代 码	描 述	查 询	差 错
0	0	回显应答(Ping应答, 第7章)	•	
3		目的不可达:		
	0	网络不可达 (9.3节)		•
	1	主机不可达 (9.3节)		•
	2	协议不可达		•
	3	端口不可达 (6.5节)		•
	4	需要进行分片但设置了不分片比特 (11.6节)		•
	5	源站选路失败 (8.5节)		•
	6	目的网络不认识		•
	7	目的主机不认识		•
	8	源主机被隔离 (作废不用)		•
	9	目的网络被强制禁止		•
	10	目的主机被强制禁止		•
	11	由于服务类型 TOS, 网络不可达 (9.3节)		•
	12	由于服务类型 TOS, 主机不可达 (9.3节)		•
	13	由于过滤, 通信被强制禁止		•
	14	主机越权		•
	15	优先权中止生效		•
4	0	源端被关闭 (基本流控制, 11.11节)		•
5		重定向 (9.5节):		•
	0	对网络重定向		•
	1	对主机重定向		•
	2	对服务类型和网络重定向		•
	3	对服务类型和主机重定向		•
8	0	请求回显 (Ping请求, 第7章)	•	
9	0	路由器通告 (9.6节)	•	
10	0	路由器请求 (9.6节)	•	
11		超时:		
	0	传输期间生存时间为0 (Traceroute, 第8章)		•
	1	在数据报组装期间生存时间为0 (11.5节)		•
12		参数问题:		
	0	坏的IP首部 (包括各种差错)		•
	1	缺少必需的选项		•
13	0	时间戳请求 (6.4节)	•	
14	0	时间戳应答 (6.4节)	•	
15	0	信息请求 (作废不用)	•	
16	0	信息应答 (作废不用)	•	
17	0	地址掩码请求 (6.3节)	•	
18	0	地址掩码应答 (6.3节)	•	

## 8. IGMP 报文格式

正如 **ICMP** 一样, **IGMP** 也被当作 **IP** 层的一部分。IGMP 报文通过 IP 数据报进行传输。**IGMP** 有固定的报文长度 (8 字节), 没有可选数据。IGMP 报文封装在 IP 数据报中, IGMP 报文通过 IP 首部中协议字段值为 2 来指明。



**IGMP v1** 报文如下:



这是版本为 1 的 IGMP。IGMP 类型为 1 说明是由多播路由器发出的查询报文，为 2 说明是主机发出的报告报文。校验和的计算和 ICMP 协议相同。组地址为 D 类 IP 地址。在查询报文中组地址设置为 0，在报告报文中组地址为要参加的组地址。

IGMP v2 报文如下：



## 9. MPLS 封装报文的结构

(1) MPLS 封装的 ICMP 报头长度计算如下：

二层报文头 + IP 头 + ICMP 头 + 外网标签 + 内网标签 + 数据  
(eth 14 字节, PPP 5 字节) (20 字节) (8 字节) (4 字节) (4 字节)

(2) MPLS 倒数第二跳没有外网标签；

(3) 如果出现 MPLS 链路所连 PC 无法 ping 通大包的现象，建议配置如下命令：

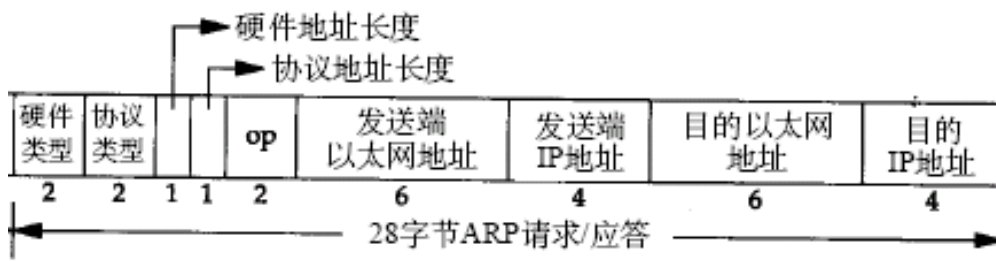
在 MPLS 视图下配置 [Router-mpls] mtu label-including

该命令的作用是设置出接口在进行 MTU 计算时将 MPLS 标签长度计算在内。

注：

报文长度计算时不计算以太网的前导码，也不计算 CRC 长度。

## 10. ARP 报文结构



说明如下：

硬件类型字段表示硬件地址的类型。它的值为 1 即表示以太网地址。协议类型字段表示要映射的协议地址类型。它的值为 0x0800 即表示 IP 地址。它的值与



协议字段目前有以下几种类型：

CHDLC\_PROTOCOL\_KEEPALIVE      0x8035  
CHDLC\_PROTOCOL\_IP              0x0800  
CHDLC\_PROTOCOL\_IPX             0x8137

当携带上层数据包时，帧中的数据字段内就是上层的数据，当此帧是 KeepAlive 帧时，数据区的格式：

type	par1	par2	rel	time0	time1
32	32	32	16	16	16

其中 par1, par2 分别为本端和对端的 keepalive 序列号，time0, time1 分别为系统启动时间到发送此 KeepAlive 的时间间隔的高位和低位，rel 暂时没用到。

type 有以下几种：

CHDLC\_PACKET\_ADDRESS\_REQUEST    0  
CHDLC\_PACKET\_ADDRESS\_REPLY      1  
CHDLC\_PACKET\_KEEPALIVE\_REQUEST  2

举例：

Serial0 (O) Len 22

8f 00 80 35 00 00 00 02 00 00 00 0b 00 00 00 01  
ff ff 00 00 00 00

Serial0

HDLC O: len 22, addr 0x8f, protocol KEEPALIVE, type KEEPALIVE\_REQ,  
myseq 12, mineseen 1, yourseen 0, line UP

## 12. 交换机环路检测报文格式

说明如下：环路检测报文是设备的端口上发送一种特殊的报文，通过检测该报文是否能够从发送出去的端口送回来，来确定这个端口上是否存在环路情况。环路检测是一个持续的过程，也就是说，在设备上需要每隔一定时间间隔进行一次检测，来确定各个端口上是否存在环路，以及上次发现存在环路的端口上环回是否已经消失等情况。

## 13. 光模块都是左端为发，右端为收。

1000\_BASE\_SX\_SFP：IEEE802.3 以太网标准中定义的 1000BASE-SX 采用多模

短波激光器(Short Wavelength Laser),因此 **1000\_BASE\_SX\_SFP** 是一个多模 SFP 光模块, 连接多模光模块必须使用多模光纤。

1000BASE\_BASE\_LX\_SFP: IEEE802.3 以太网标准中定义的 1000BASE-LX 采用单模长波激光器(Long Wavelength Laser), 连接单模光模块可使用单模光纤或多模光纤, 但用多模光纤传输距离近。

14. 百兆光模块没有波长为 850 的, 只有 1310 和 1550。

## 15. 光纤知识简介

以太网交换机常用的光模块有 SFP, GBIC, XFP, XENPAK。它们的英文全称, 中文名不常用, 可以简单了解下

**SFP**: Small Form-factor Pluggable transceiver , 小封装可插拔收发器

**GBIC** : GigaBit Interface Converter, 千兆以太网接口转换器

**XFP**: 10-Gigabit small Form-factor Pluggable transceiver 万兆以太网接口小封装可插拔收发器

**XENPAK**: 10 Gigabit EtherNet Transceiver PAcKage 万兆以太网接口收发器集合封装

参数含义:

- (1) 850nm 1310nm 1550nm: 光波波长
- (2) 100Mbps 1000Mbps: 传输速率
- (3) 10km 30km 70km: 链路长度
- (4) SX LX: 激光器类型(短波 长波)
- (5) SM MM: 工作模式(单模 多模)

光纤连接器:

光纤连接器由光纤和光纤两端的插头组成, 插头由插针和外围的锁紧结构组成。根据不同的锁紧机制, 光纤连接器可以分为 FC 型、SC 型、LC 型、ST 型和 MTRJ 型。

(1) FC 连接器采用螺纹锁紧机构, 是发明较早、使用最多的一种光纤活动连接器。

(2) SC 是一种矩形的接头, 由 NTT 研制, 不用螺纹连接, 可直接插拔, 与 FC 连接器相比具有操作空间小, 使用方便。低端以太网产品非常常见。

(3) LC 是由 LUCENT 开发的一种 Mini 型的 SC 连接器, 具有更小的体积, 已广泛在系统中使用, 是今后光纤活动连接器发展的一个方向。低端以太网产品非常常见。

(4) ST 连接器是由 AT&T 公司开发的, 用卡口式锁紧机构, 主要参数指标与 FC 和 SC 连接器相当, 但在公司应用并不普遍, 通常都用在多模器件连接, 与其它厂家设备对接时使用较多。

(5) MTRJ 的插针是塑料的, 通过钢针定位, 随着插拔次数的增加, 各配合面会发生磨损, 长期稳定性不如陶瓷插针连接器。

光纤知识:

光纤是传输光波的导体。光纤从光传输的模式来分可分为单模光纤和多模光纤。

(1) 在单模光纤中光传输只有一种基模模式, 也就是说光线只沿光纤的内芯进行传输。由



于完全避免了模式射散使得单模光纤的传输频带很宽因而适用于高速，长距离的光纤通讯。

(2) 在多模光纤中光传输有多个模式，由于色散或像差，这种光纤的传输性能较差，频带窄，传输速率较小，距离较短。

### 光纤的特性参数：

(1) 光纤的结构预制的石英光纤棒拉制而成，通信用的多模光纤和单模光纤的外径都为 125  $\mu\text{m}$ 。

(2) 纤体分为两个区域：纤芯(Core)和包层(Cladding layer)。单模光纤纤芯直径为 8~10  $\mu\text{m}$ ，多模光纤纤芯径有两种标准规格，芯径分别为 62.5  $\mu\text{m}$ （美国标准）和 50  $\mu\text{m}$ （欧洲标准）。

(3) 我们在用户资料<安装手册>中经常看到对接口光纤规格有这样的描述：62.5  $\mu\text{m}$ /125  $\mu\text{m}$  多模光纤，其中 62.5  $\mu\text{m}$  就是指光纤的芯径，125  $\mu\text{m}$  就是指光纤的外径。

(4) 单模光纤使用的光波长为 1310nm 或 1550 nm。

多模光纤使用的光波长多为 850 nm。

从颜色上可以区分单模光纤和多模光纤。单模光纤外体为黄色，多模光纤外体为橘红色。

**百兆光口自协商：**百兆光口不具有自协商的功能，没有自协商的概念。百兆光口可以工作在百兆全双工也可以工作在百兆半双工，但通常都默认为百兆全双工而不使用百兆半双工。

**千兆光口自协商：**千兆光口可以工作在强制和自协商两种模式。802.3 规范中千兆光口只支持 1000M 速率，支持全双工（Full）和半双工（Half）两种双工模式。自协商和强制最根本的区别就是两者在建立物理链路时发送的码流不同，自协商模式发送的是/C/码，也就是配置（Configuration）码流，而强制模式发送的是/I/码，也就是 idle 码流。

### 千兆光口自协商过程：

(1) 两端都设置为自协商模式

双方互相发送/C/码流，如果连续接收到 3 个相同的/C/码且接收到的码流和本端工作方式相匹配，则返回给对方一个带有 Ack 应答的/C/码，对端接收到 Ack 信息后，认为两者可以互通，设置端口为 UP 状态

(2) 一端设置为自协商，一端设置为强制

自协商端发送/C/码流，强制端发送/I/码流，强制端无法给对端提供本端的协商信息，也无法给对端返回 Ack 应答，故自协商端 DOWN。但是强制端本身可以识别/C/码，认为对端是与自己相匹配的端口，所以直接设置本端端口为 UP 状态

(3) 两端均设置为强制模式

双方互相发送/I/码流，一端接收到/I/码流后，认为对端是与自己相匹配的端口，直接设置本端端口为 UP 状态

### 注：

(1) 可见光部分波长范围是：390-760（毫微米），大于 760nm 部分是红外光，小于 390nm 部分是紫外光。光纤中应用的是：850nm，1310nm，1550nm 三种。

(2) 光纤裸纤一般分为三层：中心高折射率玻璃（芯径一般为 50 或 62.5nm），中间为低折射率硅玻璃包层（直径一般为 125nm），最外是加强用的树脂涂层。

(3) 多模光纤：中心玻璃芯教粗（50 或 62.5nm），可传多种模式的光。

单模光纤：中心玻璃芯教细（芯径一般为 9 或 10nm），只能传一种模式的光。

(4) 常用光纤规格：

单模：8/125nm，9/125nm，10/125nm

多模： 50/125nm 欧洲标准

62.5/125nm 美国标准

工业，医疗和低速网络：100/140nm，200/230nm

塑料：98/1000nm 用于汽车控制

(5) 缺省情况下，百兆、千兆和万兆以太网光端口均工作在全双工模式下，不需用户对其进行配置。百兆、千兆和万兆以太网光端口的速率不需用户进行设置。

## 16. 交换机端口处理

端口类型	对接收报文的处理		发送报文时的处理
	当接收到的报文不带 Tag 时	当接收到的报文带有 Tag 时	
Access 端口	接收该报文，并为报文添加缺省 VLAN 的 Tag	当 VLAN ID 与缺省 VLAN ID 相同时：接收该报文 当 VLAN ID 与缺省 VLAN ID 不同时：丢弃该报文	由于 VLAN ID 就是缺省 VLAN ID，不用设置，去掉 Tag 后发送
Trunk 端口	VLAN 的 Tag	当 VLAN ID 与缺省 VLAN ID 相同时：接收该报文 当 VLAN ID 与缺省 VLAN ID 不同时，但 VLAN ID 是该端口允许通过的 VLAN ID 时：接收该报文	当 VLAN ID 与缺省 VLAN ID 相同时：去掉 Tag，发送该报文 当 VLAN ID 与缺省 VLAN ID 不同时：保持原有 Tag，发送该报文
Hybrid 端口		当 VLAN ID 与缺省 VLAN ID 不同时，且 VLAN ID 是该端口不允许通过的 VLAN ID 时：丢弃该报文	当 VLAN ID 与缺省 VLAN ID 相同时：去掉 Tag，发送该报文（此为系统默认情况） 当 VLAN ID 与缺省 VLAN ID 不同时，可以通过命令 <code>port hybrid vlan vlan-id-list { tagged   untagged }</code> 配置该端口是否带有 Tag，发送该报文

## 17. 交换机端口速率与双工的说明

**100M 电口**支持 10M，100M 和 Auto 的速率模式，Half，Full 和 Auto 的双工

模式。

**100M 光口**只能工作在 100M Full 模式下。

**1000M 光口**只能工作在 1000M 或 Auto 速率模式,Full 或 Auto 双工模式。(注意: 保证与对方端口工作模式相同, 否则可能出现 link up 但是不能互通的现象)

**1000M 电口**支持 10M, 100M, 1000M 和 Auto 的速率模式, Full 和 Auto 双工模式。

另外, 1000Base-T 以太网端口也可以工作在 Half 模式下, 但当速率设置为 1000M 后, 双工属性只可以设置为 Full 或 Auto。

## 18. DCD、DTR、DSR、RTS 及 CTS 等五个状态指示代表含义

DCD ( Data Carrier Detect 数据载波检测)

DTR (Data Terminal Ready, 数据终端准备好)

DSR (Data Set Ready 数据准备好)

RTS ( Request To Send 请求发送)

CTS (Clear To Send 清除发送)

在这五个控制信号中, **DTR和RTS是DTE设备** (数据终端设备, 在实际应用中就是路由器) 发出的, **DSR、CTS和DCD是DCE设备** (数据电路终结设备, 在实际中就是各种基带MODEM) 发出的。

这五个控制信号的协商机制如下:

1) 在路由器的串口没有配置流控命令的情况下, **只要一上电, DTR和RTS就会被置成有效 (即只要一加电这两个状态就UP, 不管串口有没有接电缆)**, 当路由器检测到对端送过来的DSR、CTS和DCD三个信号时, 串口的物理状态就上报UP (任何一个物理信号无效都不会报UP, 或者说, 这三个信号中只要有一个为DOWN, 路由器串口的物理状态就处于DOWN的状态)。

另外, 如果在路由器的串口上配置了**NO DETECT DSR-DTR**命令, DTE侧 (路由器) 就不会检测对端是否送过来DSR和CTS信号, 只要检测到DCD信号, 物理层就报UP。

2) 如果在路由器的串口上配置了流控命令 (具体命令为 flowcontrol auto), RTS 和 CTS 两个信号就会用于流量控制 (路由器串口和基带 Modem 之间的数据发送、接收流控)。当出现数据处理不及时的情况, 这两个控制信号就可能处于 DOWN 的状态。

## 19. Bootrom 密码破解

**R、AR18、AR28 系列路由器** Bootrom 超级密码是 **WhiteLily2970013** (注意: 区分大小写)。

**AR46 系列路由器** Bootrom 超级密码在 B02 版本以前都是 **8060bsp**, 从 B02 开始后超级密码变为 **supperman**。

## 20. 串口线缆

### V.24 规程:

DB50 (路由器端) --DB25 (外接网络端)

DB28 (路由器端) --DB25 (外接网络端)

V.24 电缆接口分 DCE 和 DTE 两侧,分别对应数据电路端接设备(网络侧)和数据终端设备(用户侧)。对应的 DCE 侧为插座(25 孔),DTE 侧为插头(25 针)。通信的双方相对而言,路由器属于 DTE 侧设备,各种 Modem、ISDN 终端适配器等则属于 DCE 设备。

可工作在同步和异步两种方式下:

**异步工作方式下最高传输速率是 115200bps**

**同步方式下最高传输速率是 64000bps**

在路由器上使用的 V.24 规程电缆有:

WAN——广域网电缆

AUX——备份口电缆

8ASY——8 异步串口电

CONSOLE——控制台接口电缆

### V.35 规程:

DB50 (路由器端) --DB34 (外接网络端)

DB28 (路由器端) --DB34 (外接网络端)

V.35 电缆的接口特性严格遵照 EIA/TIA-V.35 标准。路由器端为 DB50 接头,外接网络端为 34 针接头,也分 DCE 和 DTE 两种,对应的 DCE 侧为插座(34 孔),DTE 侧为插头(34 针)。

**V.35 电缆一般只用于同步方式传输数据**,此方式下,与使用 V.24 电缆相同,路由器总是处在 DTE 侧。**V.35 电缆工作在同步方式下的最大传输速率是: 2048000 bps。**

## 21. IP 地址分类和私有 IP

A 类(0 开头): 0~127

B 类(10 开头): 128~191

C 类(110 开头): 192~223

D 类(1110 开头): 224~239 (多播地址)

E 类(11110 开头): 240~255 (留待后用)

### 私有 IP:

A 类中: 10.0.0.0~10.255.255.255

B 类中: 172.16.0.0~172.31.255.255

C 类中: 192.168.0.0~192.168.255.255

## 22. TCP/IP 常用端口号

1~1023: 知名端口号 (低于 255 为公共应用; 255~1023 为各个公司特殊应用)

1024~5000: 临时端口号

5000 以上: 为其它服务器预留

### TCP (协议号 6):

DNS——53  
HTTP——80  
FTP——20 (数据) /21 (控制)  
Telnet——23  
SMTP——25  
TACACS——49  
BGP——179

### UDP (协议号 17):

DNS——53  
TFTP——69  
SNMP——161  
BootP——67 (Server) /68 (Client)  
L2tp——1701  
RIP——520  
协议无关多播 PIM——103  
Radius——1812 (认证) /1813 (计费)  
NetBIOS-NS (NetBIOS Name Server)——137  
NetBIOS-DS (NetBIOS Datagram Server)——138

## 23. IEEE 802 标准: 定义了系列局域网标准

### 802.1: 基本局域网问题

802.1d——透明桥接协议  
802.1q——VLAN 标准  
802.1v——802.1q 的补充, 基于端口和协议的 vlan 标准  
802.1p——Qos 优先级 Tos  
802.1x——基于端口的认证标准

### 802.2: 定义 LLC 子层

### 802.3: 以太网标准

802.3ad: LACP 链路聚合控制协议  
802.3b: 双绞线上千兆以太网规范  
802.3u: 百兆快速以太网  
802.3z: 千兆以太网

### 802.4: 令牌总线网

### 802.5: 令牌环网

24. **MAC 地址全为 1 为广播地址；第一字节的最后一个 bit 为 1 是多播地址。**

25. **路由协议及其发现路由的优先级**

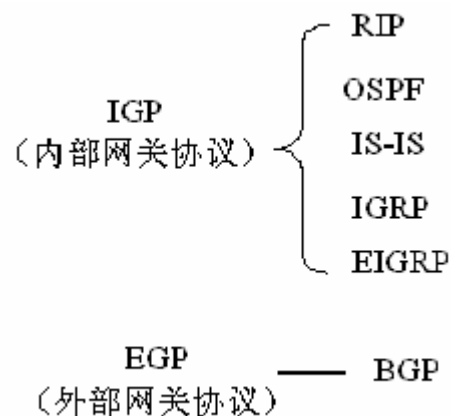
路由协议或路由种类	相应路由的优先级
DIRECT	0
OSPF	10
IS-IS	15
STATIC	60
RIP	100
OSPF ASE	150
OSPF NSSA	150
IBGP	256
EBGP	256
UNKNOWN	255

26. **最佳路由选取原则**

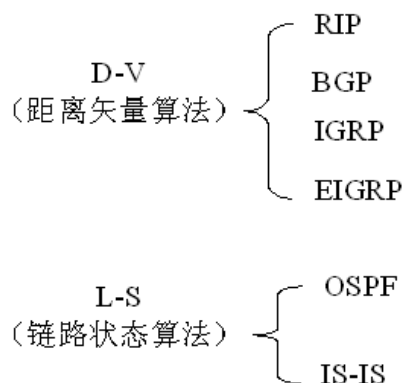
最佳路由的选取原则是“精确匹配”，即使优先级低，只要匹配到最精确就可作为最佳路由。例如，静态路由优先级低于 OSPF，但静态路由可精确到主机，而 OSPF 只精确到网段，则该静态路由为最佳路由。

27. **路由协议的分类**

(1) 按应用范围区分：

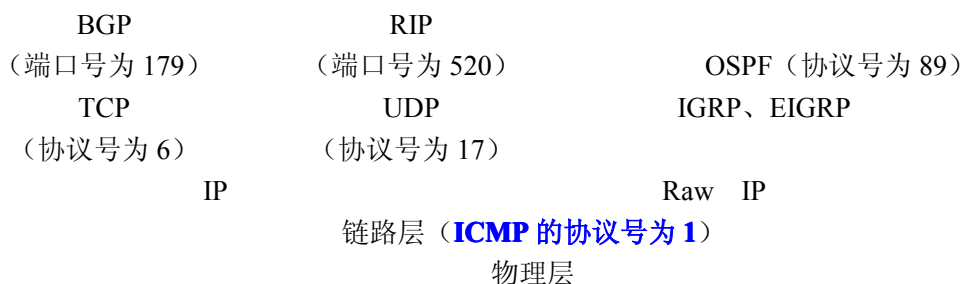


(2) 按寻径算法区分：

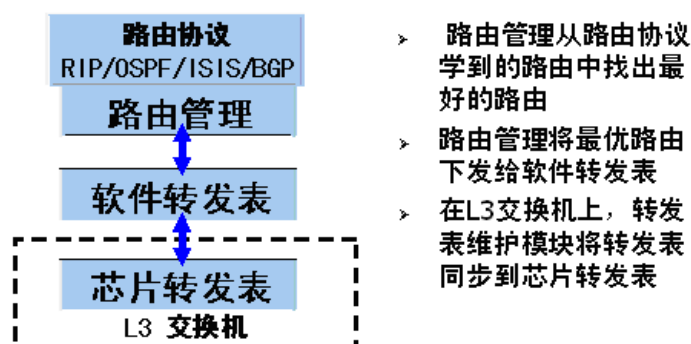


**注：**D-V 算法直接传送各路由器的路由表信息，每个 Router 都不了解整个网络的拓扑（L-S 算法则不同），它们只知道与自己直连的网络情况和从邻居得到的路由更新信息。

## 28. 各路由协议在 TCP/IP 协议栈中的对应关系



## 29. IP 报文转发过程



在我们的系统中，报文转发时查找的是转发表。对路由器来说，是软件转发表，而对于三层交换机来说是芯片转发表。

需要澄清两个概念：**转发表 FIB** (Forwarding Information Base) 和路由表 (Route Table)。转发表是 IP 层真正用来控制数据包发送的，IP 发送报文时通过查询转发表决定下一跳；而路由表是路由管理模块用来统一管理、收集上层寻径协议找回的各种路由信息，**路由管理根据特定策略从路由表中选中评价较好的路由（称为选中路由 Active Route）来修改转发表**。比如 RIP 和 OSPF 都学到了一条到同一网段的路由，但下一跳却不同，路由管理会根据协议的优先级优先将 OSPF 学到

的路由下发给转发表。

与转发表项相关的网络诊断命令：

- > **dis fib x.x.x.x**  
显示转发表
- > **dis ip routing-table x.x.x.x**  
显示路由表
- > **dis ip fast-forwarding cache x.x.x.x**  
显示快转表
- > **undo ip fast-forwarding**  
在接口模式下关掉接口的快转

检查快转表和FIB 表是否一致，快转表的错误导致错误转发

- > **dis cpu**  
显示当前CPU使用率
- > **dis cpu history**  
显示CPU 的历史使用率
- > **dis memory**  
显示系统可用内存
- > **dis memory limit**  
显示内存告警门限
- > **dis task （仅用于隐藏模式下）**  
显示系统内各个任务占用CPU的时间
- > 察看接口统计中的错误计数

### IP 报文转发过程总结如下：

（1）主机在发送之前，**先使用自身的子网掩码与目的地之相与**，看目的 IP 是否和自己是同一网段

（2）如果 gateway 是他自己（PC 将和自己同网段的 gateway 设为自己本身），他认为这样的转发属于二层转发，于是把剩下的事情交给链路层去做，然后链路层查缓存里的 ARP 表里有没有，有就直接送 2 层转发（查 MAC 表）

（3）如果 ARP 表里没有，那么就进入 ARP 过程，请求目的 IP 的 MAC 地址

（4）如果目的 IP 的 Gateway 不是他自己，则认为和自己不是同一网段，就进行 3 层查找，也就是说找路由表，找到最长匹配的项。（一般要是找不到的话，默认网关就是最匹配的）。**如果是 PC 会直接交给链路层查找 Gateway 的 MAC 地址转发**，如果没有，则发送 ARP 请求网关 MAC 地址，然后发送，到此报文发送完毕。

（5）如果是在路由器上，还可能进行递归查询，如果下一跳地址非直连网段，



进行递归查询，找下一跳的路由。

(6) 反复递归查询后，如果没找到下一跳为直连网段的路由，那么不可达。

(7) 如果找到匹配的路由，且下一跳为自己的直连网段，那么将进入 ARP 过程，请求下一跳的 MAC 地址，按照下一跳 MAC 地址传送数据。

(8) 到达下一跳后反复上面的过程。

(9) 如果所找到的路由的下一跳为本地环回口，也就是自己的 IP，那么后面的操作就可以看作和 step 2 的过程一样了

30. **AS 同一机构管理，统一的选路策略的一些路由器。1—65411 为注册的因特网编号，65412—65535 为专用网络编号（不允许出现在公网上）。**

31. **各协议对应协议号**

ICMP	1
IGMP	2
TCP	6
UDP	17
GRE	47
ESP	50
AH	51
OSPF	89
VRRP	112

32. **交换机中端口自协商优先级（由高到低）：100BASE-TX 全双工、100BASE-T4、100BASE-TX、10BASE-T 全双工、10BASE-T**

33. **交换机中的两种流量控制**

(1) 半双工采用后推压力（backpressure）技术实现，流量控制。

例如，如果一台高速 100Mbps 服务器通过交换机将数据发送给一个 10Mbps 的客户机，该交换机将尽可能多地缓冲其帧，一旦交换机的缓冲器装满，它就通知服务器停止发送。

有两种方法可以达到这一目的：交换机可以强行制造一次与服务器的冲突，使得服务器退避；或者，交换机通过插入一次“载波检测”使得服务器的端口保持繁忙，这样就能使服务器感觉到好象开关要发送数据一样。利用这两种方法，服

务器都会在一定时间内停止发送，从而允许交换机去处理积聚在它的缓冲器中的数据。

(2) 全双工流控遵行 802.3x 标准，采用 64 字节“PAUSE” MAC 帧。该帧采用一个保留的组播地址 **01-80-c2-00-00-01**，将它发送给正在发送的站，发送站接收到该帧后，就会暂停或停止发送。**PAUSE 帧利用了一个保留的组播地址，它不会被网桥和交换机所转发，这样，PAUSE 帧不会产生附加信息量。**

**PAUSE 功能的应用场合：**

- 一对终端（简单的两点网络）
- 一个交换机和一个终端
- 交换机和交换机之间的链路

**PAUSE 功能不解决下列问题：**

- 稳定状态的网络拥塞
- 端到端流量控制
- 比简单“停一启”更复杂的机制

- ①、加电时，服务器 NIC 和开关检查它们是否都具有全双工能力，并将发送方式调整为全双工。
- ②、自动协商脉冲也会告诉这两个设备，它们都具有全双工能力。
- ③、服务器利用它的发送通道（也是交换机的接收通道）开始发送。
- ④、交换机接收帧，并转发到 10Mbps 客户机，但速度慢得多。
- ⑤、当交换机的内部缓冲器快装满时，它就通过其发送通道（服务器的接收通道）开始将 PAUSE 帧发送到服务器 NIC，从而停止服务器的发送。
- ⑥、交换机将其缓冲器中的数据传送到较慢的客户机，直到其内部缓冲器可以再次接收数据为止。
- ⑦、一旦缓冲器腾空，交换机就停止发送 PAUSE 帧，服务器就重新开始发送。

## **34. 组播基于 UDP**

(1) 组成员关系协议为

主机与路由器间包括 IGMP。

组播路由协议为路由器与路由器之间包括域内组播路由协议和域间组播路

由协议。

①、域内组播密集型 DVMRP、PIM-DM、MOSPF。

②、域内组播稀疏性 CBT、PIM-SM。

③、域间组播：MSDP、MBGP 组播扩展。

(2) 组播地址 224.0.0.0 到 239.255.255.255。保留组播 224.0.0.0 到 224.0.0.255；本地管理组地址 239.0.0.0 到 239.255.255.255；用户组播地址 224.0.1.0 到 238.255.255.255。

(3) 组播 mac 前三位 01-00-5e，后面 2 进制为 “0” +IP 地址后 23 位。

(4) 二层组播协议，IGMP snooping、HGMP、HMVR、RGMP、GMRP 等。常用的为 IGMP snooping。

(5) IGMP 消息有：0x11 组播组查询、0x16 版本二组播组查询报告 0x17 表示离开组播组、0x12 表示版本 1 组播组报告。

(6) PIM-DM 转发路径是**有源树 (SPT)**，其中的“源”就是实际组播源；PIM-SM 转发路径是**共享树 (RPT)**，其中的 ROOT 指的是 RP，**PIM-SM 域中必须至少配置一个候选 BSR、一个候选 RP**，可选配置静态 RP，它的作用是通过 BSR 动态计算的 RP 失效后，静态 RP 起作用。

(7) 组播报文的转发基于 RFP（逆向路径转发）机制，必须依靠单播路由表或者单独提供给组播使用的单播路由表（如 MBGP 组播路由表）。

(8) **组播实现中，组播路由表分三个层次**：每个组播路由协议有一个协议自身的组播路由表；各个组播路由协议的组播路由信息经过综合形成组播核心路由表；组播核心路由表与组播转发表保持一致，而组播转发表真正控制着组播数据包的转发。组播转发表主要用于调试，一般情况下，用户只需查看组播核心路由表获得需要的信息。

(9) PIM-SM 在域内的候选 BSR 中选举出一个主 BSR（一个网络内部只能有一个主 BSR），该选举出的主 BSR 负责收集候选 RP 发来的信息，并把它们广播出去。各候选 RP 之间没有主次之分，所有的组播路由器收到主 BSR 通告的候选 RP 消息后，根据相同的算法计算出与某一组播组对应的 RP。如果由于某种原因使由 BSR 机制选举产生的动态 RP 失效，则可以通过配置静态 RP 来指定。静态 RP 作为动态 RP 的备份，可以提高网络的健壮性，增强组播网络的运营管理能力。

如果配置的静态 RP 地址是本机某个状态为 UP 的接口地址,本机就作为静态 RP。作为静态 RP 的接口不必使能 PIM 协议。在 BSR 机制选举产生的 RP 有效时,静态 RP 不起作用。

(10) 组播地址中没有网络段地址的概念,即 239.1.1.0 也可以作为一个组播地址。

### 35. 常用预留组播 IP 地址

D 类地址范围	含义
224.0.0.0	基准地址 (保留)
224.0.0.1	所有主机的地址
224.0.0.2	所有组播路由器的地址
224.0.0.3	不分配
224.0.0.4	DVMRP 路由器
224.0.0.5	OSPF 路由器
224.0.0.6	OSPF DR
224.0.0.7	ST 路由器
224.0.0.8	ST 主机
224.0.0.9	RIP-2 路由器
224.0.0.10	IGRP 路由器
224.0.0.11	活动代理
224.0.0.12	DHCP 服务器/中继代理
224.0.0.13	所有 PIM 路由器
224.0.0.14	RSVP 封装
224.0.0.15	所有 CBT 路由器
224.0.0.16	指定 SBM
224.0.0.17	所有 SBMS
224.0.0.18	VRRP
.....	.....

### 36. 常用预留组播 MAC 地址

STP 报文 (DMAC = 0180C2000000)

Dot1X 报文 (DMAC = 0180C2000003)

GVRP 报文 (DMAC = 0180C2000021)

GMRP 报文 (DMAC = 0180C2000020)

PIM 报文 (DMAC = 01005E00000D)

### 37. MODEM 指示灯含义

(1) POWER (电源指示灯): 此灯亮表示 MODEM 已接通电源。

(2) DSR (调制解调器准备好指示灯): DSR 指示灯表示 MODEM 对 DSR 信号的操作情况。

正常情况下 DSR 亮表示 MODEM 已联到电话线上,并做好接受信号的准备.如果 DSR 信号设置为强制高时,则 MODEM 一加电,DSR 灯便亮,并保持到断电.当 MODEM 设置为 CTS/DSR 硬件数据流量控制方式时,DSR 指示灯便反映数据传输过程中数据流动与停止的情况。

(3) TXD (发送数据指示灯): 当 MODEM 发送数据时, 此灯亮, 它表示 MODEM 发送数据的情况。

(4) RXD (接收数据指示灯): 当 MODEM 接收数据时, 该指示灯亮。

(5) DTR (计算机准备好指示灯): DTR 指示灯反映着与 MODEM 相连的计算机 DTR 信号的操作情况。正常情况下 DTR 指示灯亮, 表示 MODEM 允许应答与呼叫, DTR 灯灭表示 MODEM 与电话线联接解除, 并禁止应答与呼叫。如果 DTR 被设置为强制高时, 则只要 MODEM 一加电, DTR 指示灯立即亮, 并保持到断电。

(6) CD (载波检测指示灯): 该指示灯表示 MODEM 对载波信号的操作情况。CD 设置为随实际变化时, MODEM 在联机过程中, 一旦检测到远方 MODEM 发来的有效载波, CD 指示灯亮。如果 CD 设置为强制高时, 则 MODEM 一加电, CD 指示灯立即亮, 并保持到断电。

(7) RI (振铃指示灯): 当 MODEM 检测到来自远方的 MODEM 的振铃时, RI 指示灯便亮。

(8) CTS (清除发送指示灯): CTS 指示灯亮表示 MODEM 对 CTS 信号的操作情况。在正常情况下 CTS 指示灯亮时, 表示 MODEM 已经做好和计算机交换数据的准备工作, 允许计算机开始发送数据。如果 CTS 被设置为强制高时, 则 MODEM 一加电, CTS 灯立即亮, 并一直维持到断电。

(9) MR (MODEM READY/调制解调器准备好了) 上电初始化完毕后, MR 灯亮, 表明 MODEM 核心电路正常。

(10) TR (TERMINAL READY/终端准备好了) 当 TR 指示灯亮时, 表明与 MODEM 相连的终端、计算机等 DTE 设备已经作好准备, 允许 MODEM 应答呼叫, 对于已经连接上的 MODEM, 若 TR 指示灯灭了, 那么就会断开 MODEM 的连接。TR 指示灯实际上反映了串口上 DTR 电路的状态

(11) SD (SEND DATA/发送数据) 在发送数据是, 这个指示灯会亮。

RD (RECEIVE DATA/接收数据) 在接收数据时, 这个指示灯会亮

(12) AA (AUTOMATISM ANSWER/自动应答) 当 MODEM 设置成自动应答时, AA 灯会亮, 而且在检测到一个振铃时, 就会闪烁。

(13) OH (OVERHEAD/摘机提示) 当 MODEM 摘机时, OH 灯就会亮, 也就是当 MODEM 拨号、联机或应答情况下。当 MODEM 以脉冲拨号时, OH 指示灯会亮。

(14) HS (HIGH SPEED/高速状态) 当 MODEM 的连接速率在 2400bps 以上时, HS 指示灯才会亮。

### 38. OSPF 报文头 192bits

### 39. OSPF 有五种报文类型

#### (1) Hello 报文:

发现及维护邻居关系，定时通报，选举 DR 和 BDR。

#### (2) DD 报文:

通告本端的 LSA，描述本地 LSDB 的情况（数据库同步时发送的 LSA 的摘要，即 LSA 的 HEAD）。

#### (3) LSR 报文:

缺少的 LSA 的摘要，即向对端请求自己没有的 LSA。

#### (4) LSU 报文:

回应对端请求，向其发送**所需要的 LSA 的全部内容**。

#### (5) LSACK 报文:

用于收到 LSU 之后，进行确认。

### 40. OSPF 的 LSA 类型

#### (1) 五类基本的 LSA:

在 RFC2328 中定义了五类 LSA，描述如下：

1 ①、Router-LSAs (Type-1): **由每个路由器生成**，描述本路由器运行 OSPF 的接口状态。

1 ②、Network-LSAs (Type-2): **由广播网络和 NBMA 网络的 DR 生成**，描述本网段的链路状态，只在 DR 所处区域内传播。

1 ③、Network Summary-LSAs (Type-3): **由区域边界路由器 ABR 生成**，描述本区域内的每一条 OSPF 路由，包括其目的地址、掩码、花费值等信息。其传递范围是 ABR 中除了该 LSA 生成区域之外的其它区域。

1 ④、ASBR Summary LSAs (Type-4): **由区域边界路由器 ABR 生成**，描述去往本区域内部的自治系统边界路由器 ASBR 的路由（主机路由）。

⑤、AS-external-LSAs (Type-5): **由自治系统边界路由器 ASBR 生成**，描述到达其它 AS 的路由，传播到整个 AS（Stub 区域除外）。AS 的缺省路由也可以用 AS-external-LSAs 来描述。

#### (2) 第七类 LSA

在 RFC1587 (OSPF NSSA Option) 中增加了一类新的 LSA: NSSA LSAs，也称为 Type-7 LSAs，它做为 NSSA 区域内的路由器引入外部路由时使用。

Type-7 LSAs 与 Type-5 LSAs 主要有以下两点区别：

1 ①、Type-7 LSAs 在 NSSA 区域 (Not-So-Stubby Area) 内产生和发布；但 NSSA 区域内不会产生或发布 Type-5 LSAs。

1 ②、Type-7 LSAs 只能在一个 NSSA 内发布，当到达区域边界路由器 ABR 时，**由 ABR 将 Type-7 LSAs 转换成 Type-5 LSAs 再发布（并同时更改 LSA 的发布者 为 ABR）**，不直接发布到其它区域或骨干区域。

#### (3) Opaque LSAs

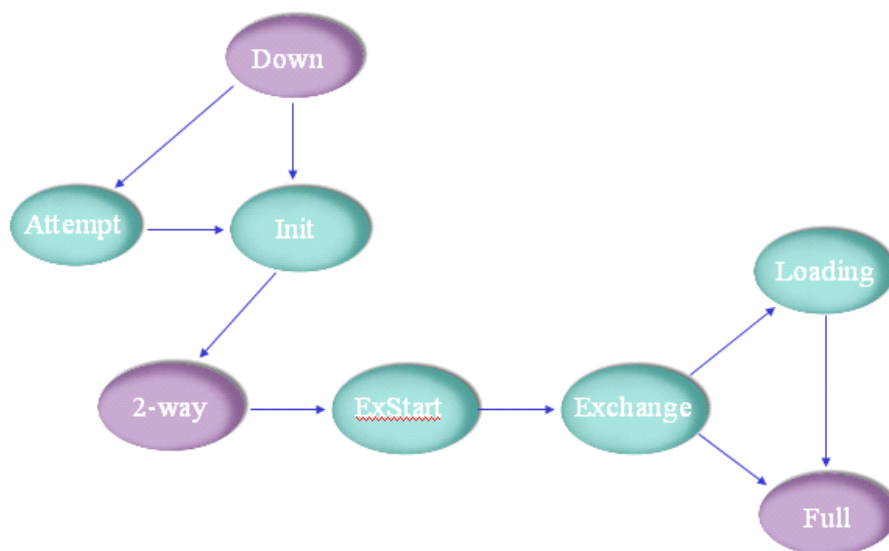
为了使 OSPF 能够支持更多新的业务应用，在 RFC2370 (The OSPF Opaque

LSA) 中定义了用于对 OSPF 进行扩展的 Opaque LSAs。

Opaque LSAs 包含三种类型的 LSA, 不同类型的 LSA 扩散范围不同:

- 1 ①、Type-9: 扩散范围为 link-local, 可以认为只在某一个接口所在的网段扩散, 不会发布到本地网段或本地子网以外。
- 1 ②、Type-10: 扩散范围为 area-local, 即, 只在本区域以内扩散。
- 1 ③、Type-11: 与 Type-5 LSAs 具有相同的扩散范围, 可以在除 STUB 区域和 NSSA 区域之外的整个自治系统内部扩散。

#### 41. OSPF 邻居状态



说明如下:

- (1) Down 过去 dead-interval 时间未收到邻居发来的 Hello 报文
- (2) Attempt NBMA 网络时出现, 定时向手工指定的邻居发送 Hello 报文。
- (3) init 本端已收到邻居发来的 Hello 报文, 但其中没有我端的 router id, 即邻居未受到我的 hello 报文。
- (4) 2-Way 双方都收到了 Hello 报文。若两端均为 DRother 的话即会停留在这个状态。
- (5) Exstart 互相交换 DD 报文 (只包含标志位, 无实际内容), 建立主从关系。
- (6) Exchange 双方用 DD 报文表述 LSDB, 互相交换。
- (7) Loading 发送 LSR。
- (8) Full 对端的 LSA 本端均有, 两端建立邻接关系。

#### 42. Ospf 网络拓扑类型

- (1) 只有本路由器 (stub networks)
- (2) 通过点对点网络与一台路由器连接 (point to point, 如 PPP、LAPB)  
**点到点**: hello 10, dead 40, 以 224.0.0.5 发送协议报文。接口状态为 point-to-point
- (3) 通过广播或 NBMA 的网络与多台路由器连接 (broadcast/NBMA), **NBMA 是全连**

通的

①、广播（如 Ethernet）：hello 10, dead 40, 以 224.0.0.5, 224.0.0.6 发送协议报文（224.0.0.5 所有 OSPF 路由器, 224.0.0.6 DR）。接口状态类型：DR, BDR, DROTHER

②、NBMA（如 HDLC、X.25、FR 和 ATM）：hello 30, dead 120, 单播发送协议报文。接口状态类型：DR, BDR, DROTHER（对于接口类型为 NBMA 的网络，由于无法通过广播 Hello 报文的形式发现相邻路由器，必须手工为其指定相邻路由器的 IP 地址，并说明该相邻路由器是否有选举权。）

（4）通过点到多点网络与多台路由器相连（point to multipoint, 由 NBMA 修改而来）

点到多点（由其它的网络类型强制更改）：hello 30, dead 120, 以 224.0.0.5 发送协议报文。接口状态为 point-to-point

注：

### （1）NBMA 和点到多点的区别

- ①、NBMA 全互连，点到多点不需要全互连
- ②、在 NBMA 上选举 DR, BDR, 点到多点不需要
- ③、NBMA 是一种缺省的网络类型，点到多点不是
- ④、NBMA 用单播发送协议报文，需要手工配置邻居，点到多点既可以用单播发送又可以用多播发送。

### （2）DR 选举原则

OSPF 协议定义了 DR，所有路由器都只将信息发送给 DR，由 DR 将网络链路状态广播出去，除 DR/BDR 外的路由器（称为 DR Other）之间将不再建立邻居关系，也不再交换任何路由信息。

选举规则如下：

- ①、优先级最大的路由器，若优先级相等，则选 router id 最大的路由器
- ②、新加入的路由器暂时不参加选举，如果已经有 DR 存在，即使本路由器优先级高，也承认现有的 DR
- ③、DR 不一定是优先级最大的路由器；DR 是某个网段的概念是针对路由器接口而言；在广播和 NBMA 网络中才选举 DR, BDR（它们的值为接口的 IP）。

## 43. OSPF 路由分级管理

外部路由类型 1：到外部路由的花费=本路由器到相应 ASBR 的花费+ASBR 到该目的地址的花费

外部路由类型 2：到外部路由花费=ASBR 到该目的地址的花费

区域内路由》区域间路由》外部路由类型 1》外部路由类型 2》NSSA 类型 1》

NSSA 类型 2

前两种的 cost 为 10，后两种为 150



#### 44. OSPF 根据网络的需求将区域划分为以下几种类型:

##### (1) 普通区域 (1、2、3、4、5)

当区域被缺省定义时,它被认为是普通区域。普通区域可以是标准区域或骨干区域。标准区域是最通用的区域,它携带区域内路由,区域间路由和外部路由。骨干区域是连接所有其它 OSPF 区域的中央区域。

##### (2) STUB 区域 (1、2、3)

STUB 区域是一个不允许 AS 外部 LSA 在其内部泛洪的区域。STUB 区域只可以携带区域内路由和区域间路由。在这些区域中路由器的 OSPF 数据库和路由表规模以及路由信息传递的数量都会大大减少,为了保证到自治系统外的路由依旧可达,由该区域的 ABR 生成一条缺省路由 0.0.0.0 传播到区域内, **所有到自治系统外部的路由都必须通过 ABR 才能到达。**

##### (3) 完全 STUB 区域 (1、2)

完全 STUB 区域是区域中最受限的形式,它不仅不允许携带外部路由,甚至连区域间路由也不允许携带,只可以携带区域内路由。在这些区域中路由器的 OSPF 数据库和路由表规模以及路由信息传递的数量都会大大减少,为了保证到区域外的路由依旧可达,由该区域的 ABR 生成一条缺省路由 0.0.0.0 传播到区域内, **所有到该区域外部的路由都必须通过 ABR 才能到达。**

##### (4) NSSA 区域 (1、2、3、7)

NSSA 区域允许一些外部路由通告到 OSPF 自主系统内部,而同时保留自主系统的区域部分的 STUB 区域的特征。假设一个 STUB 区域中的路由器连了一个运行其他路由进程的自治系统,现在这台路由器就变成了 ASBR,所以这个区域就不能再称为 STUB 区域了。然而如有把这个区域配置成一个 NSSA 区域,ASBR 会产生 NSSA 外部 LSA(类型 7),可以泛洪到整个 NSSA 区域。这些 7 类 LSA 在 NSSA ABR 上会转换成 5 类 LSA 并且泛洪到整个 OSPF 域中。

##### (5) 完全 NSSA 区域 (1、2、7)

和 NSSA 区域相似,完全 NSSA 区域允许一些外部路由通告到 OSPF 自主系统内部,而同时保留自主系统区域部分的完全 STUB 区域的特征。该区域的 ASBR 会产生 NSSA 外部 LSA(类型 7)在其区域内部泛洪并通过该区域的 ABR 转换成 5 类 LSA 在整个 OSPF 域泛洪。同时,该区域的 ABR 也会产生一条缺省路由 0.0.0.0 传播到区域内,所有域间路由都必须通过 ABR 才能到达。

**注:**

##### ①、STUB 域

不传播外部路由 (TYPE 5),由 ABR 生成一条缺省路由传播到区域。

只有一个 ABR 或有多个 ABR 但是这些 ABR 之间没有虚连接的区域为 STUB。

骨干域不能为 STUB,虚连接不能穿过 STUB。

STUB 内的所有路由器都要配置为该属性。

STUB 不能存在 ASBR。

##### ②、NSSA 区域

自治系统外部路由不能引入到 NSSA 区域中,但是区域内的外部路由可以在 NSSA 中传播并发送到区域之外。

区域内的路由器需要支持该属性,区域外的路由器不用,由 ABR 把 LSA TYPE 7 转化为 LSA TYPE 5。

##### ③、完全 Stub 区域 (Totally Stubby Area)

指那些不接收第三、四、五类 LSA（ABR 生成的包含缺省路由的第三类 LSA 除外）的区域，在这些区域中，没有去往自治系统以外和自治系统内区域间的路由

④、完全 NSSA 区域和 NSSA 区域不同的是，它不允许携带区域间路由。

#### 45. OSPF 为什么是无环的

每一条 LSA 都标记了生成者；

采用 SPF 算法，生成一棵树，根到叶子是单向不可回复的路径；

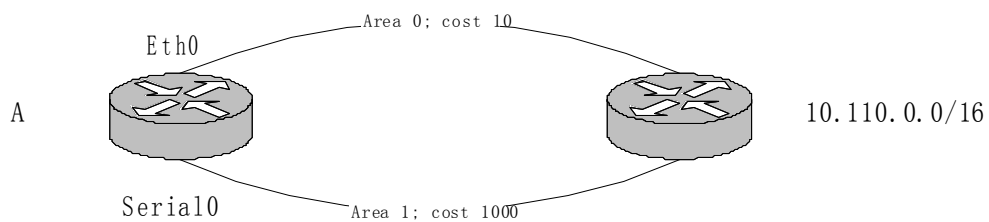
路由变化时重新运行 SPF 算法

划分骨干区域

不能保证引入的外部路由没有环路

#### 46. OSPF 选路：经过骨干区域的和经过非骨干区域的路径选择

如果对于某一外部目标网络有经过骨干区域的和经过非骨干区域的区域内路径，应该优选哪条路由？



如上图，从A路由到外部网络10.110.0.0/16的路由有两条，一条走骨干区域，cost为10；另一条走非骨干区域，cost 1000。

OSPF优选的路由应当为Serial0，按照RFC2328 Section 16.4.1，对外部网络OSPF优选非骨干区域的路径，目的是减轻骨干区域的负载。

#### 47. OSPF 规定，只有从相同的区域学习到的路由才能形成等价路由。

#### 48. 一台路由器是否为 ABR，取决于其在骨干区是否有 FULL 的邻居。

#### 49. OSPF 的缺省路由

OSPF 中不能通过 import route 命令引入缺省路由，而是通过命令进行发布。  
各区域的缺省路由产生的方式如下：

##### （1）普通区域：手工配置

产生的缺省路由不仅在本区域内泛洪，还泛洪到整个 OSPF 域中。

##### （2）Stub 区域：ABR 自动产生 3 类缺省路由

只泛洪到整个 Stub 区域。

### (3) 完全 Stub 区域: ABR 自动产生 3 类缺省路由

只泛洪到整个完全 Stub 区域。

### (4) NSSA 区域

在 NSSA ABR 上需手工配置, 从而产生 7 类缺省路由, 只泛洪到整个 NSSA 区域。

在 NSSA ASBR 上需手工配置, 产生 7 类缺省路由, 但前提是已经存在一条缺省路由, 只泛洪到整个 NSSA 区域。

### (5) 完全 NSSA 区域: ABR 自动产生 3 类缺省路由

只泛洪到整个 NSSA 区域。

## 50. 同一区域内的 OSPF 进程号应一致。

## 51. OSPF 多进程与 OSPF 多实例的区别

- (1) 每一个 OSPF 实例与一个 VPN-instance 相对应, 拥有自己独立的接口和路由表。
- (2) 多个 OSPF 进程共享一个路由表, 只不过对于其各自接口发布各自的网段路由。

## 52. OSPF 的路由过滤分两种方式

(1) 过滤路由表: filter-policy import (OSPF)

(2) 对 LSA 的过滤: filter-policy export

import route

abr-summary not-advertise (OSPF)

abr-summary not-advertise (area)

filter-policy import (area) /export (area)

## 53. 两种设定 DR 优先级的命令说明

接口视图下 **ospf dr-priority 优先值**: 用来进行实际中 DR 的选举。

OSPF 视图下 **peer IP 地址 dr-priority 优先值**: 用来表示邻居是否有选举权。

#### 54. 在 OSPF 中使用路由策略引入路由时，应使用基本 ACL。

路由的引入只涉及到目的网段，将所要引入的网段作为 source 写入 ACL 中。

#### 55. BGP 协议消息类型

BGP 协议机的运行是通过消息驱动的，其消息共可分为四类：

##### (1) open message

它是连接建立后发送的第一个消息，它用于建立 BGP 对等体间的连接关系。

##### (2) update message

它是 BGP 系统中最重要信息，用于在对等体之间交换路由信息，它最多由三部分构成：不可达路由(unreachable)、路径属性(path attributes)、网络可达性信息 NLRI (network layer reach/reachable information)。

##### (3) notification message

它是错误通告消息。当检测到差错时，发送该报文关闭 peer 连接。

##### (4) keep-alive message

它是用于检测连接有效性的消息。当收到 open 报文后向对端回应，peer 间周期性发送，保持连接。

**注：**

①、BGP 的报文比 OSPF 的少一个，在于 BGP 基于 TCP 协议，该协议完成了 ACK 的功能，而 OSPF 基于 IP，所以需要 LACK 报文完成确认功能。

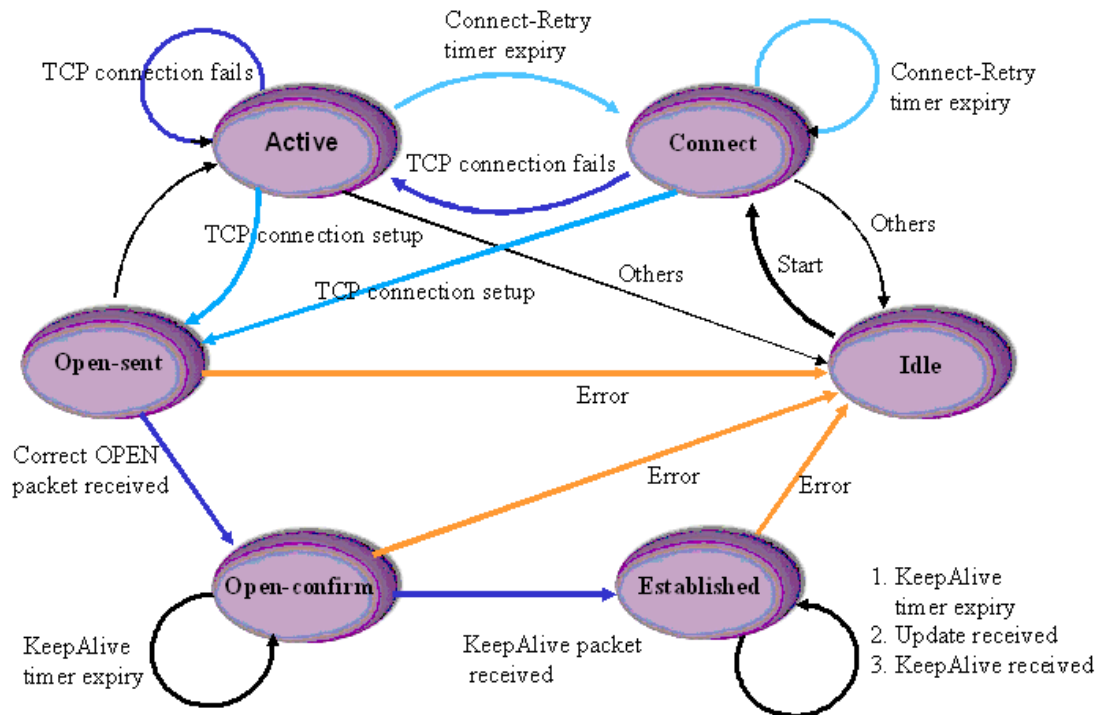
②、Update 报文一次只能通告一个路由，但可以携带多个属性。当一次通告多条路由的话，只能携带相同的属性。Update 可以同时列出多个被撤销的路由。

③、缺省情况，keepalive 60s 一发。

④、Notification 的 errorcode 含义如下：

错误代码	1	2	3	4	5	6
错误类型	消息头错	OPEN消息错	UPDATE消息错	保持时间超时	状态机错	退出

## 56. BGP 状态机



说明如下：

BGP 开始 Idle 状态，BGP 一旦 start 则进入 Connect 状态，接着建立 TCP 连接，如果不成功则进入 Active 状态，成功就进入 Open-sent 状态，Open-sent 状态收到一个正确的 open 报文就进入 Open-confirm 状态，当收到 keepalive 报文，就会建立 BGP 连接，进入 Established 状态。

## 57. BGP 选路策略

- (1) 首先丢弃下一跳(next-hop)不可达的路由
- (2) 优选最大权重(weight)的路由(Cisco 独有)
- (3) 优选最高本地优先级(local-preference)的路由
- (4) 优选本路由器始发的路由
- (5) 优选经过 AS(AS-path) 最少的路由
- (6) 优选起点类型(origin)最低的路由
- (7) 优选 MED 值最低的路由
- (8) 优选从 EBGp 学来的路由
- (9) 优选 AS 内部最短的路径可到达的路由
- (10) 优选 BGP ID 最低的路由器发布的路由

## 58. BGP 传递路由的策略

- (1) 多条路由选最优的给自己；

- (2) 只将自己使用的路由通告给对等体;
- (3) 从 EBGP 获得的路由会通告给所有 BGP peer, 从 IBGP 获得的路由不通告给 IBGP peer, 看同步情况决定是否通告给 EBGP peer。( 我们的路由器默认都是非同步的)。

59. **BGP 属性目前 16 种可扩展到 256 种, 分为必遵、可选、过渡、非过渡。**

**Origin 属性** 标识路由的来源, 0—IGP 聚合和注入路由、1—EGP EGP 得到、3—incomplete 其他方式 从其他 IGP 引入的

**AS-path 属性** 达到某个目的地址所经过的所有 AS 号码序列。宣告时把新经过的 AS 号码放在最前。

**NexT Hop 属性** 必遵属性 当对等体不知道路由时, 须将下一条属性改为本地

**Local-preference 属性** 可选 帮助 AS 内的路由器选择到 AS 区域外的较好的出口, 本地优先级属性只在 AS 内部, IBGP peer 间交换。

**MED 属性** 向外部指示进入某个具有多入口的 AS 的优先路径。选 MED 小的。

**Community 属性** (no-export 不通告到联盟 / AS 外部; no-advertise 不通告给任何 BGP Peer; local-AS 不通告给任何 EBGP; Internet 通告所有路由器 )

60. **BGP 通告默认路由的三个步骤**

创建默认静态路由 (ip route 0.0.0.0 0.0.0.0 xx.xx.xx.xx)

在 BGP 中引入静态路由 (import static)

通告默认路由 (default-route imported)

注: 如果该默认路由是通过 IGP (如 OSPF) 学来的, 需要在 BGP 中 import 该 IGP。

61. **BGP 路由处理过程: 接受路由—实施策略—路由聚合—选路—加入路由表—发布。**

62. **BGP 报文比 OSPF 报文少一个的原因。**

BGP 比 OSPF 少一个确认报文, 原因在于 BGP 基于 TCP, 确认消息由 TCP 协议完成, 而 OSPF 基于 IP, 只能由 OSPF 自身完成确认。

### 63. BGP 中反射与联盟的比较

- (1) 都是为解决大规模网络中 IBGP 必须全连接所造成的负担问题。
- (2) 反射对客户来说是透明的，对路由器是否支持反射没有要求；而联盟中所有路由器都必须支持联盟。
- (3) 反射要求反射器之间仍然是全连接，而联盟间不要求是全连接。

### 64. LP 与 MED 属性的比较

- (1) LP 是 AS 内部控制流量如何出 AS，而 MED 是控制流量怎样进入 AS。
- (2) LP 只在 AS 内部有效，在通过外部对等体通告路由的时候，LP 被过滤掉；而 MED 只在外部对等体关系中有效，在内部对等体之间通告路由时被忽略。
- (3) LP 值越大，优先级越高；MED 值越小，优先级越高。

### 65. BGP 普通团体属性 4 字节长，扩展团体属性 8 字节长。

### 66. 路由引入时使用 routing policy 过滤，路由发布和接收时用 ip prefix 和 ACL

### 67. ISDN 简介

ISDN 为用户提供一组有限的标准多用途用户—网络接口，ITU-T 的 I.412 建议中为用户—网络接口规定了两种接口结构：

基本速率接口(BRI)：B 信道的速率是 64 kbit/s，D 信道的速率是 16 kbit/s  
带宽为 2B+D，最高 144kbps。

基群速率接口(PRI)：B 信道的速率是 64 kbit/s，D 信道的速率是 64 kbit/s  
带宽为 30B+D（欧标，中国），最高 2.048Mbps；  
23B+D（美标，日本），最高 1.544Mbps。

其中：

- (1) B 信道为用户信道，用来传送语音、数据等用户信息，传送速率是 64 kbit/s。
- (2) D 信道为控制信道，它传送公共信道信令，这些信令用来控制同一接口的 B

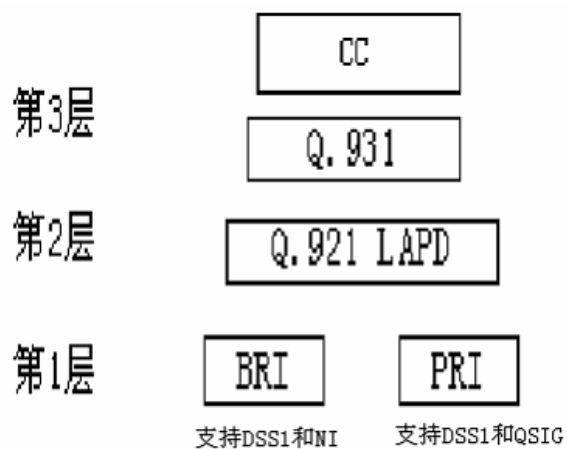
信道上的呼叫。

ITU-T Q. 921 是 D 信道的数据链路层协议，它定义了用户到网络接口上第 2 层实体间经 D 信道交换信息的规则，同时支持第 3 层实体的接入。

ITU-T Q. 931 是 D 信道的网络层协议，它提供了在通信应用实体间建立、保持和终结网络连接的方法。

呼叫控制(call control, 即 CC)是对 Q. 931 进一步的封装, Q. 931 把由网络侧传递过来的消息转发给 CC, 由 CC 和高层应用（比如 DCC）进行信息转换。

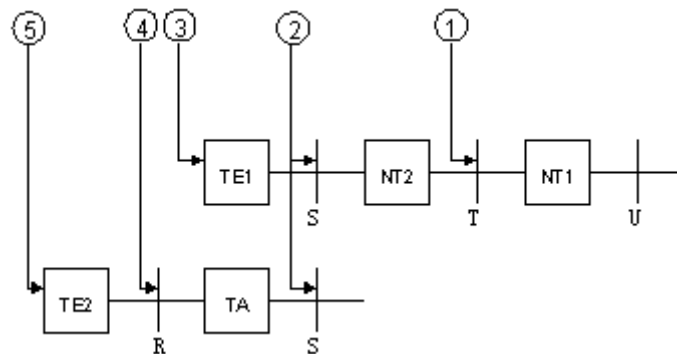
D 信道协议栈如下：



**注：**BRI/BSV 接口支持 NI 和 DSS1 协议，但只支持 BSV 接口的网络侧；PRI 接口支持 DSS1 和 QSIG 协议，支持两者的网络侧。

## 68. ISDN 的用户-网络接口规范

在 ITU-T I. 411 建议中，根据功能群（用户接入 ISDN 所需的一组功能）、参考点（用来区分功能群的概念上的点）的概念，提出了 ISDN 用户-网络接口的参考配置。



说明如下：



功能群分为：

网络终端 1（NT1）：主要实现了 OSI 第一层的功能，包含用户线传输功能、环路测试和 D 信道竞争等。

网络终端 2（NT2）：又称为智能网络终端，包含了 OSI 的 1~3 层。

1 类终端设备（TE1）：又称为 ISDN 标准终端，是符合 ISDN 接口标准的用户设备（如数字话机等）。

2 类终端设备（TE2）：又称为非 ISDN 标准终端设备，是不符合 ISDN 接口标准的用户设备。

终端适配器（TA）：完成适配功能，使 TE2 接入 ISDN 标准接口。

参考点包括：

R 参考点：位于非 ISDN 设备和 TA 之间。

S 参考点：位于用户终端和 NT2 之间。

T 参考点：位于 NT1 和 NT2 之间。

U 参考点：位于 NT1 设备和线路终端设备之间。

69. Q931 消息格式

Q931 消息由协议标识符 0x08、CR 值的长度、CR 值、消息类型和信息单元 (IE) 组成。

其中：不同的 Q931 消息中，携带的信息单元不同。对于一个特定的消息，可以参考 Q931 协议查看，可以携带的信息，必须携带的信息单元。

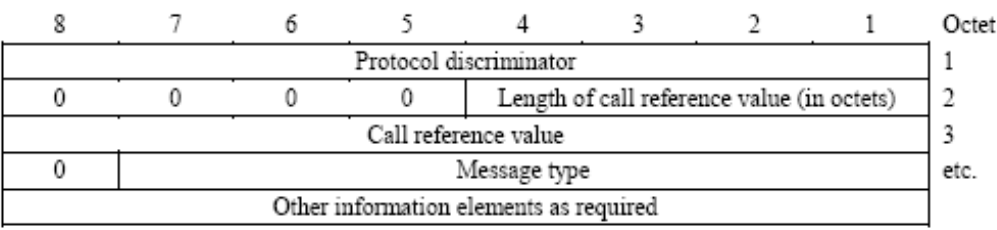


Figure 4-1/Q.931 – General message organization example

70. 用户端与网络段交互的信息类型

用户侧	网络侧	说明
方向 →	方向 ←	
Setup		包括拨号号码，拨号类型。例如：语音拨号。

	Setup acknowledge	呼叫确认，通道预留。
	Calling proceeding	呼叫处理中。
	Alerting	振铃。说明对端已经振铃，同时用户侧受到该信号后产生振铃声。该时刻用户侧到 PTO 侧的 B 信道连接已经建立。
	Connect	远端的用户响应，B 信道建立。
Connect Ack		连接确认。
Disconnect		用户端挂断，发送 Normal Clearing 的信息。
	Release	释放 B 通道连接。
Release complete		释放确认。

#### 说明：

整体发号方式和重叠发号方式的区别在于在 ISDN 建立呼叫过程中，对被叫号码的处理上：

<1>如果在 SETUP 消息里面携带了完整的被叫号码，并且携带了 Send complete 信息单元，那么就是整体发号方式。

<2>如果在 SETUP 消息里面没有完全携带被叫号码，那么就是重叠发号方式，就会给用户侧发送 SETUP ACK 消息，表明网络侧认为号码不全，同时告诉用户侧将后续的被叫号码通过 INFORMATION 消息发送给网络侧。

## 71. BRI 接口有两种类型，P2MP 接口和 P2P 接口

**BRI 接口默认接口类型为 P2MP**，表示点对多点。P2MP 接口为了区分不同的对端，在使用 BRI 接口之前，会进行 TEI 值的协商，**通过不同的 TEI 值来区分不同的终端。**

而 **P2P** 的 BRI 接口，表示点对点类型。只有一个对端连接设备，**使用的 TEI 值为 0，这个和 PRI 接口很相似。**

通常情况下，**PBX 和路由器的 BRI 的默认接口类型为 P2MP 接口**。如果和 P2P BRI 接口对接，就应该在接口模式下配置 **isdn link-mode p2p** 命令将接口配置为 P2P 接口。

#### 注意：

- (1) 路由器 **BRI** 接口的类型必须和对端的接口类型一致，否则协商不成功。
- (2) **Q921** 协议支持一个 **BRI** 接口接 **8** 个终端设备。**display** 显示信息中的 **Link Layer** 表示链路层，**Link Layer 1~8** 表示链路层 **1~8** 个连接的情况。

(3)但由于 **BRI** 接口只有 **2 个 B 通道**,所以同时最多可以有两个设备使用,**Q921** 层通过 **TEI** 进行区分不同的终端。

(4) 路由器使用的 **TEI** 值是通过向 **PBX** 申请得到。

(5) **Link Layer 1** 到 **Link Layer 8** 分别表示这 **8 个 Q921** 链路层连接的状态信息。

72. **PRI 接口为点对点接口, 所以 TEI 值为 0。**

## 73. **ISDN 网络侧功能支持情况**

(1) PRI 接口的 DSS1 和 QSIG 协议支持 ISDN 网络侧功能。

(2) BSV 接口运行 DSS1 协议的时候, 支持 ISDN 网络侧功能。

(3) BRI 接口不支持 ISDN 网络侧功能。

**注:**

(1) BSV 接口卡只支持语音方式应用, 不支持 BRI 数据方式应用, 这和 ISDN BRI 接口卡是有区别的。

(2) 激活与去激活

BSV 无论作用户侧还是网络侧, 其典型物理特性为: 激活和去激活机制。**该特性是 ISDN BRI 接口所特有的。**所谓去激活是指使已进入工作状态的系统转入休止状态。在休止状态下, 除少数控制电路外, 其余电路都将停止供电, 以降低功耗和延长系统的使用寿命。与之相对, 激活就是使处于休止状态的系统转入工作状态, 全系统加电, 再使之运转起来。需要特别强调的是: BSV 只有在网络侧模式下才能主动发起去激活请求来解除线路激活状态。BSV 作用户侧使用时, 无权主动发起去激活请求, 只能被动地解除激活状态。

## 74. **中低端路由器产品分三个系列**

分别是 8040 的 R 系列路由器 (只有 Quidway 品牌), 8040 的 AR28/46 系列路由器 (分 H3C 和 Quidway 两个品牌), 8043 的 AR18 系列路由器 (分 H3C 和 Quidway 两个品牌), 其中 **AR18 系列产品较多, 概述如下:**

1、V2R7 (AR18-1x, 除 AR18-10) —— 无 H3C 品牌 **VRP1.74**

AR18-12、AR18-13、AR18-15、AR18-16、AR18-18

2、V1R1 (AR18-20、20S、30、31、32、33、34、35、33E、34E)

H3C 品牌机型包括: AR18-33、AR18-34、AR18-33E、AR18-34E

3、V1R2 (AR1821A、30E、31E、21B、32E、35E) —— 6 款产品都存在 Quiday 和 H3C

两个品牌

4、V1R3（AR18-22-24）——该款产品存在 Quiday 和 H3C 两个品牌

5、V1R5（AR18-10）——无 H3C 品牌

6、V1R7（AR18-21、22、23-1、22-8、22S-8、23S-1）——6 款产品都存在 Quiday 和 H3C 两个品牌

7、V6R1（AR18-63-1）——无 Quidway 品牌

#### **R 系列路由器介绍：**

##### **1、R160x Series VRP1.44-0007**

R1602

R1603

R1604

##### **2、R25xx Series VRP1.44-0007**

R2501

R2509

R2511

##### **3、R4001 Series VRP1.44-0007**

R4001

##### **4、R25xxE Series VRP1.44-0007**

R2501E

R2509E

R2511E

##### **5、R4001E Series VRP1.44-0007**

R4001E

##### **6、R263x Series VRP1.66-0005**

R2630

R2631

##### **7、R36xx Series VRP1.66-0005**

R3640

R3680

##### **8、R161x Series VRP1.74-0118 Don't support VRP3.30**

R1612

R1613

R1614

R1615

##### **9、R1760 Series VRP1.74 Don't support VRP3.30**

R1760

##### **10、R261x Series VRP1.74 Don't support VRP3.30**

R2610

R2611

**11、R262x Series VRP1.74 Don't support VRP3.30**

R2620

R2621

**12、R263xE Series VRP1.74 Don't support VRP3.30**

R2630E

R2631E

**13、R36xxE Series VRP1.74 Don't support VRP3.30**

R3640E

R3680E

R3680E-RPS

**AR28、46 设备介绍:**

AR28-09B **VRP1.74**

AR28-09

AR28-10

AR28-11

AR28-12

AR28-13

AR28-14

AR28-30

AR28-31

AR28-40

AR28-80

AR46-20

AR46-40

AR46-80

**注:**

(1) 路由器 E 系列与不带 E 系列之间的区别在于 E 增强型在硬件配置方面比不带 E 强，其他应用无太大差别。

(2) R4001E 与其他低端主要区别有一个 cE1/PRI 接口。

(3) 低端路由器唯一只有 R1760 具有模块化（低端产品的价格中端产品的功能）R1760 模块化插槽分为 2 个 Sic 卡插槽 1 个 MIM 大插槽（与中端路由器模块插槽同，可通用）

(4) 中端路由器 R.\*. 系列，第三个数字可代表支持最大模块 MIM 槽数  
例如 R2620 有 2 个 MIM 槽 R3680 有 8 个 MIM 槽。

(5) R2600 系列第四位数字为以太口数量，例 R2620 有 1 个 10/100M 以太口 R2621 有 2 个 10/100M 以太口。

(6) 低端路由器 R1600 系列 R2500 系列 R4001 系列 R1760 系列；中端路由器 R2600 系列 R3600 系列。

**(7) AR18 系列路由器产品特点:**

①、AR18-20、20S、21:

三层口: Ethernet1/0、Ethernet2/0

二层口: Ethernet1/1—Ethernet1/4

②、AR18-21A:

三层口: Ethernet1/0、Ethernet3/0、Atm2/0

二层口: Ethernet1/1—Ethernet1/4

③、AR18-22:

三层口: Ethernet1/0、Ethernet2/0、Ethernet3/0

二层口: Ethernet1/1—Ethernet1/4

④、AR18-22-8:

三层口: Ethernet1/0、Ethernet2/0、Ethernet3/0

二层口: Ethernet1/1—Ethernet1/8

⑤、AR18-22-24:

三层口: Ethernet1/0、Ethernet2/0、Ethernet3/0

二层口: Ethernet3/1—Ethernet3/24

⑥、AR18-23-1:

三层口: Ethernet1/0—Ethernet4/0

⑦、AR18-63-1:

三层口: GigabitEthernet1/0—GigabitEthernet4/0

(8) R1603 BRI 接口的类型是 S/T; R1604 BRI 接口的类型是 U 口。具体用哪款路由器根据电信方提供的 BRI 接口的类型。

R1603 /R1604 还具有 2 个模拟电话口 POTS,可接两部电话或传真。

(9) R1602 与 R1603/1604 主要区别在

R1602 无 BRI 接口和 POTS 口,有 2 个同异步口。

R1603/1604 同异步口只有 1 个,各有 1 个 BRI 口和 2 个模拟电话口 POTS。

(10) R2501E 与 R2509E/R2511E 之间主要区别在 R2509E/R2511E 多 8 异步串口且 R2509E 1 个, R2511E 2 个。

(11) R3600 系列为全模块化体系设计。

(12) AR18 系列路由器,有些接口是通过 PCI 总线连接到 CPU,有些接口是直连 CPU 的,直连 CPU 的接口在处理速度会更快。一般建议流量大的接口就使用直连 CPU 的接口。流量在 30M 以下,使用哪个接口都可以,如果是 30M 以上可以使用直连 CPU 的接口,在 NAT 双出口时,如果在北方地区(南方地区),由于访问网通(电信)的流量会大些,建议使用直连 CPU 的接口。流量在 100M 以下,使用 AR18-63 的那个接口无所谓,高于 100M,建议使用直连 CPU 的接口。

AR18-21: 4 个 LAN 口和 WAN 口都是直连到 CPU;

AR18-22: 4 个 LAN 口和 WAN 0 口直连 CPU, WAN 1 接口通过 PCI 总线连接 CPU;

AR18-22-8/22S-8: 8 个 LAN 通过交换芯片连接到 CPU,都可以做到线速转发, WAN 0 口直连 CPU, WAN 1 口通过 PCI 总线连接 CPU;

AR18-23-1/23S-1: WAN 0 和 WAN 1 通过 PCI 总线连接 CPU, WAN 2 和 WAN 3 直连 CPU;

AR18-63-1: WAN 0 和 WAN 1 接口直连 CPU, WAN 2 和 WAN 3 通过 PCI 总线连接 CPU;

AR18-22-24: WAN 0 和 WAN 1 接口都是通过 PCI 总线连接到 CPU 的。

**注: 直连 CPU 的接口,可以支持自适应 MDI/MIX, 4 个 LAN 口 / 8 个 LAN 口也支持。**

(13) AR18 系列路由器 CPU 规格:

AR18-22-24 200MHz

AR18-21/22 266MHz

AR18-22-8/22S-8    AR18-23-1/23S-1    400MHz  
AR18-63-1    800MHz

## 75. WEB 网管功能支持的机型

(1) 目前 H3C AR18 系列路由器中，支持 WEB 网管功能的机型包括：

路由器型号
AR18-33E/34E
AR 18-30E/31E/32E/35E/21A/21B
AR 1822-24
AR 18-21/ AR 18-22/ AR 18-23-1/ AR 18-22-8/ AR 18-22S-8/ AR 18-23S-1

(2) 目前 Quidway AR18 系列路由器中，支持 WEB 网管功能的机型包括：

路由器型号
AR18-30/33E/34E
AR 18-30E/31E/32E/35E/21A/21B
AR 1822-24
AR 18-21/ AR 18-22/ AR 18-23-1/ AR 18-22-8/ AR 18-22S-8/ AR 18-23S-1

## 76. 高端 NE 路由器产品介绍

(1) 8090：最高端，10G 平台，主控板上带 CF 卡，分布式转发。

含三款设备：NE5000E、NE80E 和 NE40E。

①、NE5000E：应用于安全，但销售清单中已经去除。

②、NE80E 和 NE40E：应用于企业网，主要使用 V5 版本（不同于 MSR 的 V5 版本，license 的控制相对简单），分两种 license：

IPv6 enable 和 IPv6 diable

(2) 8011：是维护与销售的重点，2.5G 平台，主控板上后加 CF 卡，分布式转发。

含三款设备：NE80、NE40 和 S8016

①、NE80：双主控，16 个槽位，采用机框式结构；硬盘更新为增强型硬盘；增加 CF 卡。

②、NE40：分三种，即 2 槽（单主控）、4 槽（双主控）和 8 槽（双主控）。如下业务需小卡单板支持（只有 V5 版本支持）：GRE、L2tp、NatStream、Nat 和 Nat-Pt。

③、S8016（外形酷似 NE80）：将 NE80 改装为高端交换机，用 NP 转发，在 05 年被 85 替代，现在已经停产。

### **注：软件版本的说明**

①、NE40，主力 VRP3.1 版本，分支 1：23XX，分支 2：25XX，25XX 非常特殊。

②、V5，VRP5.3，全是靠 license 控制，V3 升级到 V5 升级中注意一定要保证 paf 与 license 文件一致。第二注意一定要将 license 放到正确的位置上。

### **(3) 8070:**

①、NE20（分 2、4 和 8 槽，为单主控，集中式转发，通过 CPU 和 NP 配合完成；靠 flash 存储）和 NE20E（双主控）

这两款都是集中转发，版本分为

V3（不维护了）

V5，又分 5.1（过渡版本）和 5.3（发货版本）；V5 版本支持 IPv6、TE 等，且 5.3 版本支持 NE20E。

此外 NE20 板卡分为

高速卡：通过 NP 转发（1、2、4 为高速槽位）

低速卡：通过 CPU 软件转发（3、5、6、7、8 为低速槽位）

②、NE16E、NE08E 和 NE05

a. 采用 cpu 转发

b. 是我们自己的

c. 业务槽位依次分别为 12 个，6 个，4 个

软件版本：主力发货 VRP3.1，可收费升级到 V5.3，5.3 支持 VIU8 的转发板，100M 可达到限速。

### **注：**

（1）高端路由器硬件结构由总装机箱，路由交换单元（RSU）高可靠控制单元版（HAU）系统监控单元（ALUA）通用接口单元（VIU）组成 及模块和软件组成。

（2）路由交换单元包括前处理板（RT-NE-RSUB(256M) RT-NE-RSUC(512M)）与路由扩展单元 RT-NERSEU 组成。



(3) 通用接口处理单元包括通用接口前处理板 (RT-NE-VIUB) 通用接口扩展单元 (RT-NE-VIEU)。

(4) NE40 支持 3 跳等值静态路由。

(5) NE20/NE20E 支持 ATM 子接口重定向；

8011 不支持 ATM 子接口重定向；

8090 不支持 ATM 子接口重定向。

## **77. NE20 对 NAT、GRE、L2TP、IPSEC 功能支持情况的说明**

在 VRP5.10 上 NE20 支持 NAT、GRE、L2TP 功能，但不支持 IPsec 功能；

在 VRP5.30 上 NE20/NE20E 都支持 NAT、GRE、L2TP，但不支持 IPsec 功能；

这些都是软件特性不需要特殊单板。

## **78. NE40/NE80 对 NAT、GRE、L2TP、IPSEC 功能支持情况的说明**

在 VRP3.10 上 NE40/NE80 支持 NAT 且需要专用的 NAT 板，但不支持 GRE、L2TP 和 IPsec 功能；

在 VRP5.30 版本上 NE40/NE80 支持 NAT、GRE、L2TP，并且必须使用专用 NAT、GRE、L2TP 隧道板，但暂不支持 IPsec 功能。

## **79. MSR 产品介绍**

**V1R1:** MSR20—20/21 MSR20—40 (H3C 品牌)

AR19—61/62 AR29—01 (Quidway 品牌)

**V2R1:** MSR30—20/40/60 (H3C 品牌)

AR29—21/41/61 (Quidway 品牌)

**V3R1B01:** MSR50—40/60 (H3C 品牌)

AR49—45/65 (Quidway 品牌)

**V3R1B02:** 3Com 机型 OSR37—20/40

57—01/20/40/60

67—40/60

部分 OAP 单板

**V3R1B03:** MSR30—16 (即 MSR30—20 的低成本版本)

**V3R2B01:** MSR30—11 (用于金融)

XMIM (扩展 MIM 板卡)

**V3R2B02:** ICT20—10（以太网上行），ICT20—15（海外版的 ADSL 上行）

WIFI 扣卡

**V3R2B03:** ICT20—11（串口上行），ICT20—12（E1/T1 上行），ICT20—13（DSL 上行），

**V5R1B01:** ASM（防毒卡），NAM（网络访问模块）

**V5R1B02:** WAAM（广域网性能优化模块），VCM（语音融合模块），EADM（迷你 EAD 模块）

**V5R1B03:** MSM（媒体交换模块）

**V3R3:** 转发 2Mpps

## 80. 交换机产品概述

**早期产品:** S2403/2403F（Web 页面式管理，支持 MultiVlan 和 HGMP）

二者外观没有太大差别，主要差别是 S2403F 可以支持 100M 光接口。

**第一代产品:**

S3026: 二层交换机，只支持 32 个 VLAN。

S3526: 三层交换机，路由查找方式为精确匹配，而非最长匹配。

**相同血缘的产品有 S3026FS/FM，S3526FS/FM:** 分别继承了 S3026 和 S3526 的所有软件特点，只是提供了更多的光接口，以满足不同场合的应用需求。（其中 F 代表百兆，S 和 M 分别代表单模和多模）

**为了缓解由于 S2403/S2403F 交换机的停产后**，市场上相同层次的设备短缺，推出了 **S2000 系列交换机，主要型号包括:** S2008、S2016、S2403H 和 S2026。同时，对于那些成本预算低，管理要求低的用户，推出了 **S2000B 系列交换机，主要型号包括** S2008B、S2016B 和 S2026B。20008B、2016B 支持 PoE 供电。

**第一批使用 Broadcom 芯片的交换机:**

代表就是 S3026E 和 S3526E，逐步替代 S3026 和 S3526。在 S3026E 和 S3526E 的基础上，2002 年上半年伊始，又相继诞生了 S3026EFS/FM 和 S3526EFS/FM。并于 2002 年年中至 2003 年上半年，相继开发出了 S3050C、S3026C、S3026G、S3026T 以及 S3026C-PWR 等多款使用 Broadcom 芯片的二、三层交换机

**全千兆二层交换机主打设备（使用 Broadcom 芯片）:**

S5012G——12 个千兆电口和 4 个 Combo GBIC 口；

S5012T-12/10GBC——10 个 GBIC、2 个千兆电口以及 2 个 Combo 千兆电口；  
S5024G-24/20TP 具有 20 个千兆电口及 4 个 GBIC 口。

### 使用 Marvell 芯片的交换机：

S3528G（24 个百兆口+4 个 GBIC 口）、S3528P（24 个百兆口+4 个 SFP 口）；  
S3552G（48 个百兆口+4 个 GBIC 口）、S3552P（48 个百兆口+4 个 SFP 口），  
S3552F 以及 S3552F-HI（F 表示扩展槽）。

### 2004 年下半年，推出了一系列以 SI 结尾的交换机（使用 Broadcom 芯片）：

内部称之为 2050 系列，包括 S2026C-SI、S2026Z-SI 和 S3026C-SI、S3026G-SI、  
S3026S-SI。

原有的 S2000 系列交换机（S2008、S2016、S2026）也日益面临停产，相继  
推出了 S2000C 系列交换机（S2008C、S2016C、S2026C），以及 S2000-EI 系列交  
换机（S2008-EI、S2016-EI、S2403H-EI）。

S2000C 系列交换机被包装成 S2100-SI 系列交换机， S2000-EI 系列交换机  
被包装成 S2100-EI 系列以及 E2000 系列交换机，以供其他 OEM 厂商使用或在教  
育网中进行使用。

**S2100-SI 系列包括：**S2108-SI、S2116-SI 和 S2126-SI。S2100-SI 系列各产品  
外形及性能特性，均与 S2000C 系列中端口数相同的交换机一致；

**S2100-EI 系列包括：**S2108-EI、S2116-EI 和 S2126-EI。

**E2000 系列包括：**E008-FE、E017-FE 和 E026-FE。S2100-EI 系列和 E2000 系列  
各产品外形及性能特性，均与 S2000-EI 系列中端口数相同的交换机一致。

### H3C 公司成立后（使用 Broadcom 芯片）：

加入 IRF 特性，也就是 3com 交换机所支持的 XRN 特性。而该时期设计开发  
的产品，在内部被称作 **F1（S5600 系列）和 Monza（S3900 系列）**。

**S3900 系列分为 S3900-SI 和 S3900-EI 两个系列，各自包装成 S3600-SI 和 S3600-  
EI 系列。**

### 进入 2006 年后的交换机：

基于 V3 平台开发的 **S3100 系列**，**S5100-EI 系列**，**S5100-SI 系列**， 基于 V5 平  
台开发的具备 IPV4/IPV6 双协议栈的 **S3610 系列**， **S5510 系列**， **S5500-SI/EI**  
**系列**，以及单独为教育网包装的 **E 系列**交换机等。

平台类型	设备型号
V3平台 (IPv4业务, IPv6管理)	S3100
	S5100-SI
	S5100-EI
V5平台 (IPv4/IPv6双协议栈)	S3610
	S5510
	S5500-SI
	S5500-EI

芯片类型	设备型号
Broadcom	S3100
	S5500-SI
	S5500-EI
Marvell	S5100-SI
	S5100-EI
	S3610
	S5510

**S3100 系列：桌面接入；**

S3100-SI 系列替代 S2000EI 成为新一代的主打接入交换机，C 系列为扩展模块可更换，T 系列为固定千兆电口。

**S5100 系列：处理海量数据的能力；**

**S5510 系列：核心交换机。**

P 系列为 4 个千兆 SFP 接口（Combo），F 系列为 4 个千兆电口（Combo）。

**S3610 系列：**

P 系列为 4 个千兆 SFP 接口（Combo），F 系列为 4 个千兆电口（Combo），TP 系列为 2 个千兆电口+2 个千兆 SFP 接口。

**E 系列对应关系：**

S3928-TP-SI/S3952—————E328/E352（三层交换机）

S3126C—————E126（二层交换机）

S3952 裁减特性—————E152（二层交换机）

S3026/S3026-SI/ S3026T—————E026/E026-SI/ E026T（二层交换机）

S3050C—————E050（二层交换机）

E328—————H3C S3600-28TP-SI

E352—————H3C S3600-52P-SI

E126—————H3C S3100-26C-SI

E126A—————H3C S3100-26TP-EI

E152—————H3C-3100-52P

注：

- (1) S3026 支持 100 /1000M 光纤模块
- (2) S3526 只支持 1000M 光纤模块
- (3) S3026FS/FM S3526FS/FM 模块支持百兆千兆
- (4) 低端 S2008/S2016 的 LS-FSIU LANSWITCH 百兆单模光口板 LS-FMIU LANSWITCH 百兆多模光口板。与中端的同型号不通用（记住）
- (5) **S3526 系列以上是路由交换机（2，3 层）S3026 向下都是 2 层交换机**
- (6) S3026 提供 12 个固定百兆以太网口 S3526 提供 24 个固定百兆以太网口
- (7) S3026FM/FS S3526FS/FM 提供固定 12 个百兆光纤接口
- (8) S5516 全模块化 4 个千兆 GE 插槽,每个模块为 4 端口千兆
- (9) S3000 系列交换机模块 6 端口的百兆(电，多，单)模块交换机接口类型为 MTRJ 型
- (10) S5516 4 端口千兆(单，多)光纤模块为交换机接口类型为 LC 型
- (11) S5516 千兆短波光纤模块是 多模模块
- (12) S5516 千兆长波光纤模块是 单模模块
- (13) **S3500 系列交换机中，S3552G、S3552P、S3228G、S3528P、S3552F 不支持 isolateuser-vlan 的配置。**
- (14) **S2000B、S2000C 和 S2100-SI 不支持配置管理 IP，无法实现 SNMP 管理。**
- (15) H3C 如下交换机支持关闭 VLAN 特性
  - S2000 系列交换机中的 S2016-EI，2403H-EI
  - S3000 系列交换机中的 S3026，S3026C
  - S3500 系列交换机中的 S3526E，S3526C
- (16) **S3924P-SI 只有 24 个百兆电口，无 SFP 模块，虽然后面带个“P”。**
- (17) **S3900 和 S5600 设备堆叠插上线即可，无需配置。**
- (18) **SFP 接口既可以插入 SFP 光模块，也可以插入电口模块。**

81. 路由器上的精确匹配与交换机上的精确匹配的区别是：交换机上的精确匹配要求 ARP 表项中有精确的目的主机 IP 地址；而路由器上只要找到最长匹配的网段地址即可，无需主机 IP。（S3526 和 S3526E 支持精确匹配）

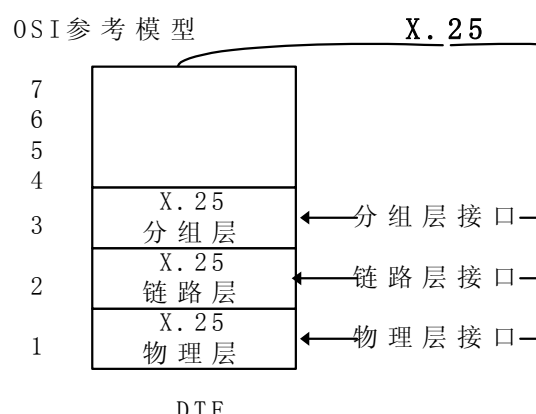
## 82. 中低端交换机 ACL 生效规则

大部分交换机支持的 ACL 匹配规则为后下发先生效，如 S3900 和 S5600 系列、S3000 系列（S3050C），在 H3C 系列中，S3600 和 S5600 支持的也是后下发先生效。

还有一部分设备支持的 ACL 匹配规则是先下发先生效，如 S3528/S3552、S5100 系列、S5500-SI、和 S5516。

此外，S3526 支持的 ACL 匹配顺序是深度优先，最小地址范围的 rule 先生效。

## 83. X.25 协议参考模型



X.25 协议按照 OSI 参考模型的结构，定义了从物理层到分组层一共三层的内容。

(1) X.25 第三层（分组层）规程描述了分组层所使用分组的格式和两个三层实体之间进行分组交换的规程；

(2) X.25 第二层（链路层）规程也叫做平衡型链路接入规程（LAPB, Link Access Procedure, Balanced），LAPB 定义了 DTE 与 DCE 之间交互的帧的格式和规程；

(3) X.25 第一层（物理层）则定义了 DTE 与 DCE 之间进行连接时的一些物理电气特性。

84. **X.25 协议为两台通信的 DTE 之间建立的连接被称为虚电路，这种“电路”只在逻辑上存在。**

一旦在一对 DTE 之间建立一条虚电路，这条虚电路便被赋予一个唯一的虚电路号，当其中的一台 DTE 要向另一台 DTE 发送一个分组时，它便给这个分组标上号（虚电路号）交给 DCE 设备，DCE 就是根据分组所携带的这个号来决定如何在交换网内部交换这个数据分组，使其正确到达目的地。X.25 第二层（LAPB）在 DTE/DCE 之间建立的一条链路被 X.25 第 3 层复用，最终呈现给用户的是可以使用的若干条虚电路。

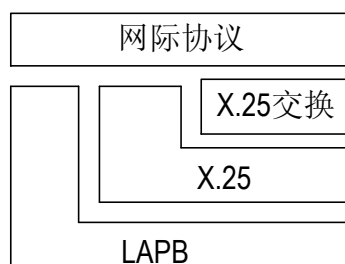
SVC 是在有数据传输要求时，由 X.25 经过呼叫临时建立的；PVC 是手工配置的，不论是否有数据传输要求而总是存在的。

85. **LAPB 协议简介**

国际标准规定的 X.25 链路层协议 LAPB，采用了高级数据链路控制规程（HDLC）的帧结构，并且是它的一个子集。它通过置异步平衡方式（SABM）命令要求建立链路。建立链路时只需要由两个站中的任意一个站发送 SABM 命令，另一站发送 UA 响应即可以完成双向链路的建立。

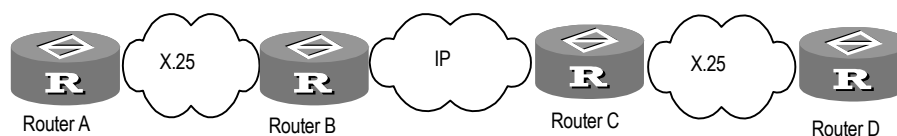
虽然 LAPB 是作为 X.25 的第二层被定义的，但是，作为独立的链路层协议，它可以直接承载非 X.25 的上层协议进行数据传输。

Quidway 系列路由器可以设置串口的链路层协议为 LAPB，进行简单的本地数据传输；同时，Quidway 系列路由器的 X.25 还具备交换功能，也就是说，可以将路由器当作一台小型 X.25 分组交换机使用，保护用户在 X.25 之上的投资。下图描述了 LAPB、X.25、X.25 交换三者之间的关系：



86. **XOT 简介**

**XOT (X.25 Over TCP)** 是一种把 X.25 报文承载在 TCP 上，实现两个 X.25 网通过 IP 网来互联的协议。实际应用环境如下图所示：



### **XOT 的实现原理（以 SVC 为例）：**

如上图所示，QuidwayA 有数据传输时，首先发送一个呼叫请求分组建立虚电路；QuidwayB 收到此呼叫分组后，经判断是 XOT 应用，于是首先与 QuidwayC 建立一条 TCP 连接，然后把 X.25 呼叫分组报文贴上 XOT 报文头封装在 TCP 里传输到 QuidwayC；QuidwayC 去掉 TCP 和 XOT 报文头后，通过 X.25 本地交换把呼叫请求分组传递给 QuidwayD；QuidwayD 收到呼叫请求分组后应答呼叫确认，直到链路完全建立，进入数据传输状态。建立并应用 TCP 连接的整个过程对 QuidwayA 和 QuidwayD 来说是透明的，它们并不关心也无法关心此时是通过 IP 网还是 X.25 网来转发数据的。

## **87. X2T 简介**

X2T(X.25 to TCP switch)技术能够将 X.25 网络和 IP 网络连接起来，从而使 X.25 主机和 IP 主机可以互相访问。

对于 X.25 主机来说，IP 主机有一个 X.121 地址相对应。当路由器收到 X.25 呼叫请求分组时，它会检查分组中的目的 X.121 地址。根据此地址，路由器在配置的 X2T 路由表中进行查找。如果发现了匹配的路由，路由器会与 X2T 路由中相应的目的 IP 地址的主机建立一条 TCP 连接。TCP 连接建立后，路由器从 X.25 报文里提取纯数据通过 TCP 连接发送到 IP 主机侧。

对于 IP 主机来说，要访问 X.25 主机，只需通过路由器 IP 网络侧接口的 IP 地址即可。当路由器收到 TCP 连接建立请求时，它会检查 TCP 连接的目的 IP 地址和 TCP 端口号。根据此地址，路由器在配置的 X2T 路由表中进行查找。发现了匹配的路由后，如果 X25 主机和路由器之间通过 SVC 连接，路由器会与 X2T 路由中相应的目的 X.121 地址的主机建立一条 X.25 虚电路，虚电路建立后，路由器从 TCP 报文里提取纯数据通过 X.25 虚电路发送到 X.25 主机侧；如果 X25 主机和路由器之间通过 PVC 连接，则路由器直接将数据通过配置的 X.25 PVC 发送到 X.25 主机侧。



88. **PAD 是一种类似于 telnet 的应用，可以从一端通过 X121 地址建立到另一端的 PAD 连接进行配置等操作。**

## 89. **X.25 虚电路范围**

X.25 协议可以将 DTE/DCE 之间的一条实际的物理链路复用，建立多条在逻辑上存在的虚连接，这种虚连接称为虚电路（VC, Virtual Circuit）或逻辑信道（LC, Logic Channel）。**X.25 可以建立的虚连接最多可达 4095 条，编号从 1~4095**，这个可以用来区分每一条虚电路（或逻辑信道）的编号称为逻辑信道号（LCI, Logic Channel Identifier）或虚电路号（VCN, Virtual Circuit Number）。

X.25 协议中很重要的一部分内容就是如何管理这一共 4095 条虚电路。所有的虚电路号被划分成四个区域，这四个区域分别是（按编号的升序排列）：

- 1 A-永久虚电路区间
- 1 B-单向呼入信道区间
- 1 C-双向信道区间
- 1 D-单向呼出信道区间

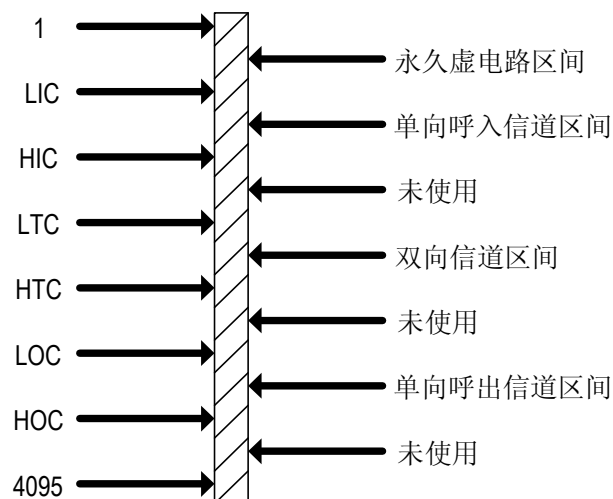
通过 X.25 呼叫建立的虚电路，其编号一定在 B、C、D 三者其一之中，也只能在三者其一之中；而设置的永久虚电路则只能在区间 A 中。

那么，这些信道是如何被分配的呢？根据《ITU-T 建议 X.25》，X.25 在发起呼叫时，采用如下的空闲信道分配策略：

- 1 只有 DCE 可以使用“单向呼入信道区间”中的信道发起呼叫；
- 1 只有 DTE 可以使用“单向呼出信道区间”中的信道发起呼叫；
- 1 DCE，DTE 均可使用“双向信道区间”中的信道发起呼叫；
- 1 DCE 总使用最低的可使用的逻辑信道；
- 1 DTE 总使用最高的可使用的逻辑信道。

有了以上这一套策略，就可以避免通信的某一侧独占所有的信道，并且将呼叫碰撞发生的可能性降低到了最小。

X.25 协议使用六个参数来界定这四个区域，如下图所示：



六个参数意义请参见下表：

参数	意义
LIC	Lowest Incoming-only Channel 最低单向呼入信道号
HIC	Highest Incoming-only Channel 最高单向呼入信道号
LTC	Lowest Two-way Channel 最低双向信道号
HTC	Highest Two-way Channel 最高双向信道号
LOC	Lowest Outgoing-only Channel 最低单向呼出信道号
HOC	Highest Outgoing-only Channel 最高单向呼出信道号

每一个区间（永久虚电路区间除外）被两个参数定义，可以称其为该区间的上限和下限；每个参数均可在 1 到 4095 之间（包括 1 和 4095）取值，但是，只有同时满足如下条件的配置才被认为是正确的配置：

- ①、严格升序，即  $1 \leq lic \leq hic < ltc \leq htc < loc \leq hoc \leq 4095$ ；
- ②、若某个区间的上、下限其中之一为 0，那么另一个也必须为 0（上、下限均为 0 表示该区间被禁止使用）。

最后，还有以下几点需要注意：

- ①、在一个物理连接的两侧（即 DTE、DCE 之间），X.25 的这六个参数必须保证对应相等，否则，很有可能导致因规程无法正常进行而数据传输失败；

②、配置的过程中，在保证升序的前提下，一定要注意各参数的缺省情况，根据实际情况进行判断，完成参数的正确设置；

③、因为 X.25 规程需要 DTE、DCE 具有同样的虚电路范围参数，所以新的正确配置在 X.25 协议已经协商通的状态下是不能立即生效的，需要执行 shutdown 与 undo shutdown 命令。

90. “虚电路”和“逻辑信道”

虚电路指的是端到端的一条逻辑通路（即主叫 DTE 和被叫 DTE 之间），逻辑信道指的是直接连接的两台设备之间的逻辑通路（或许是 DTE 与 DCE 之间，或许是两台分组交换机的端口之间）；而**一条虚电路是由若干段逻辑信道拼接而成，并且每一段逻辑信道具有独立的编号。**

91. 帧中继网络用户接口上最多可支持 1024 条虚电路，其中用户可用的 DLCI 范围是 16~1007（帧中继 LMI 协议占用 DLCI 为 0 和 1023 的 PVC）。

由于帧中继虚电路是面向连接的，本地不同的 DLCI 连接到不同的对端设备，因此我们可以认为本地 DLCI 就是对端设备的“帧中继地址”。

DLCI（数据链路连接标识，Data Link Connection Identifier 的首字母缩写）只在本地接口和与之直接相连的对端接口有效，不具有全局有效性，即**在帧中继网络中，不同的物理接口上相同的 DLCI 并不表示是同一个虚连接。**

标志      地址      信息      FCS      标志

DLCI	C/R	EA	DLCI	FECN	BECN	DE	EA
6位	1位	1位	4位	1位	1位	1位	1位

C/R：命令/响应

C/R 位允许上层识别帧是命令还是响应。帧中继协议不用。

EA：扩展地址

EA 位表明当前字节是否是地址的最后一个字节。

FECN：前向显式拥塞通知

前向显式拥塞通知位可以由所经过路径中任何一个交换机来设置，用来表示在帧传输的方向上出现了拥塞。它通知目标站点发生了拥塞。

BECD: 后向显式拥塞通知

后向显式拥塞通知位用于表示在帧传输相反的方向上出现了拥塞。它通知发送方发生拥塞。

DE: 丢弃资格

DE 位指明帧的优先级。在紧急情况下, 交换机可能需要抛弃一些帧来缓和瓶颈并防止网络由于过载而崩溃。当 DE 被设为 1 时, 这个比特通知网络只要当前流中有其他优先级为 0 的帧存在, 就不要丢弃这个帧。该位可由帧的发送方设置, 或由网络中任何一个交换机设置。

DLCI: 数据链路连接标识符

第一个字节的前 6 个比特构成 DLCI 的第一部分。DLCI 的第二部分使用第二个字节的前 4 个比特。这些比特是标准所定义的 10 比特数据链路连接标识符的一部分。

**注:** 类似与 HDLC 的帧。实际上, 标志、FCS 和信息字段是相同的。然而没有控制字段。地址字段定义了 DLCI, 并有几个比特用于拥塞控制及通信量。

FR 在用户面上仅完成物理层和链路层的功能, 在链路层完成统计复用、帧透明传输和错误检测, 但是不提供错误后重传操作。

**92. FR 在用户面上仅完成物理层和链路层的功能, 在链路层完成统计复用、帧透明传输和错误检测, 但是不提供错误后重传操作。**

帧中继网提供了用户设备 (如路由器, 桥, 主机等) 之间进行数据通信的能力, 用户设备被称作数据终端设备 (即 DTE); 为用户设备提供接入的设备, 属于网络设备, 被称为数据通信设备 (即 DCE)。DTE 和 DCE 之间的接口被称为用户——网络接口 (即 UNI); 网络与网络之间的接口被称为网间网接口 (即 NNI)。

**93. 帧中继默认的网络类型是 NBMA (Nonbroadcast Multiaccess) 非广播多点可达**

也就是说虽然帧中继网络中的各个节点之间相互连通, 但是和以太网不同的是这种网络不支持广播, 如果某个节点得到路由信息, 它需要复制多条然后通过 PVC 一条一条发送到相连的多个节点。

在配置 FR 或 X. 25 时, 当上层承载的协议或数据报文需要进行广播时, 必须在配置 map 时加上 broadcast 属性 (如配置 ospf 时)。

## 94. 帧中继的带宽管理

帧中继网络为每个帧中继用户分配三个带宽控制参数：**Bc、Be和CIR**。同时，每隔Tc时间间隔对虚电路上的数据流量进行监视和控制。CIR是网络与用户约定的用户信息传送速率，即承诺信息速率。如果用户以小于等于CIR的速率传送信息，应保证这部分信息的传送。Bc是网络允许用户以CIR速率在Tc时间间隔传送的数据量，即 $Tc = Bc/CIR$ 。Be是网络允许用户在Tc时间间隔内传送的超过Bc的数据量。

网络对每条虚电路进行带宽控制，采用如下策略。

在Tc内：当用户数据传送量  $\leq Bc$  时，继续传送收到的帧；

当用户数据传送量  $> Bc$  但  $\leq Bc+Be$  时，将Be范围内传送的帧的DE比特置“1”，若网络未发生严重拥塞，则继续传送，否则将这些帧丢弃；  
当Tc内用户数据传送量  $> Bc+Be$  时，将超过范围的帧丢弃。

## 95. DTE 与 DCE 的区分

数据链路层不同于物理层。物理层的DTE与DCE是由电缆来决定的。一旦插上电缆，就自动决定了这台设备是DTE还是DCE。而数据链路层的DTE与DCE则看是否为数据终端设备。**帧中继中的DTE与DCE是链路层的概念。**

## 96. ARP、RARP、INARP 协议比较

协议类型	已知参数	返回参数	备注
ARP	目的协议地址	目的链路层地址	广播请求，单播应答
RARP	源链路层地址	源协议地址	一般需要RARP服务器，广播请求
INARP	目的链路层地址	目的协议地址	本地DLCI相当于目的链路层地址，单播请求，单播应答(设备间通过固定的永久虚电路连接)

## 97. 帧中继中的点对点接口和点对多点接口的区别

无论点到点接口还是点到多点的子接口，都是在实际物理接口上承载的逻辑接口。**它们本质的区别在于点到点类型只能与一条PVC相关，点到多点类型可以与多个PVC相关。**因此，点到点接口是不必也不能配置3层地址与PVC

的映射关系的，转发时完全通过三层路由来决定封装 DLCI 号。对于点到多点接口，往往需要配置地址映射，当然，如果双方都支持反向地址解析，地址映射的配置对于点对多点子接口也是可选的。

基于上面的说明，要配置一个 NBMA 网络，对于中心点的路由器，只能使用点到多点的子接口，因为，不能创建多个点到点的子接口，然后给它们指定相同网段的三层地址。

## 98. 目前 H3C 路由器只支持永久虚电路方式。

## 99. ATM（Asynchronous Transfer Mode）简介

ATM 是异步传输模式的简称，是以信元为基本单位进行信息传输、复接和交换的。ATM 信元具有 53 字节的固定长度，其中 5 个字节构成信元头部，主要用作路由信息和优先级信息，其余 48 个字节是有效载荷。

ATM 是面向连接的交换，每条虚电路（Virtual Circuit，VC）用虚路径标识符（Virtual Path Identifier，VPI）和虚通道标识符（Virtual Channel Identifier，VCI）来标识。一个 VPI/VCI 值对只在 ATM 节点之间的一段链路上有局部意义。它在 ATM 节点上被翻译。当一个连接被释放时，与此相关的 VPI/VCI 值对也被释放，它被放回资源表，供其它连接使用。

ATM 基本协议框架分为 3 个平面，即用户平面、控制平面和管理平面。

（1）用户平面和控制平面又各分为 4 层，即物理层、ATM 层、ATM 适配层和高层。

（2）管理平面又分为层次管理和平面管理。其中前者负责各平面中各层的管理，具有与其它平面相对应的层次结构；后者负责系统的管理和各平面之间的通信。

（3）控制平面主要利用信令协议来完成连接的建立和拆除。

各平面与各层的关系请见下图：

ATM 适配层 (ATM Adaption Layer, AAL) 是高层协议与 ATM 层间的接口, 它负责转接 ATM 层与高层协议之间的信息。目前, 已经提出 4 种类型的 AAL: AAL1、AAL2、AAL3/4 和 AAL5, 每一种类型分别支持 ATM 网中某些特征业务。大多数 ATM 设备制造商现在生产的产品普遍采用 AAL5 来支持数据通信业务。

## 100. ATM 的虚链路

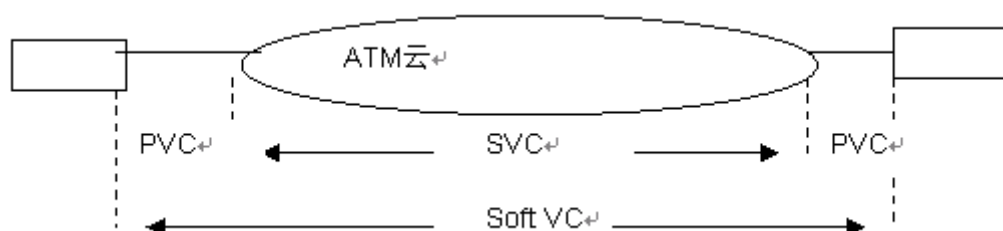
有三种, 分别是 PVC (永久虚电路)、交换虚电路 (SVC) 和 Soft VC。

1) PVC 是通过管理员静态配置的, 是 VPC/VCI 的永久的集合, 一旦连接就不能释放。

2) SVC 的虚电路不是永久连接的, 是通过设备利用行令 PVC 传递的命令, 在 ATM 设备中动态的建立的。

3) Soft VC 是 ATM 云是基于 SVC 的, 而外围是通过 PVC 方式接入的 ATM 云中。

如图所示:

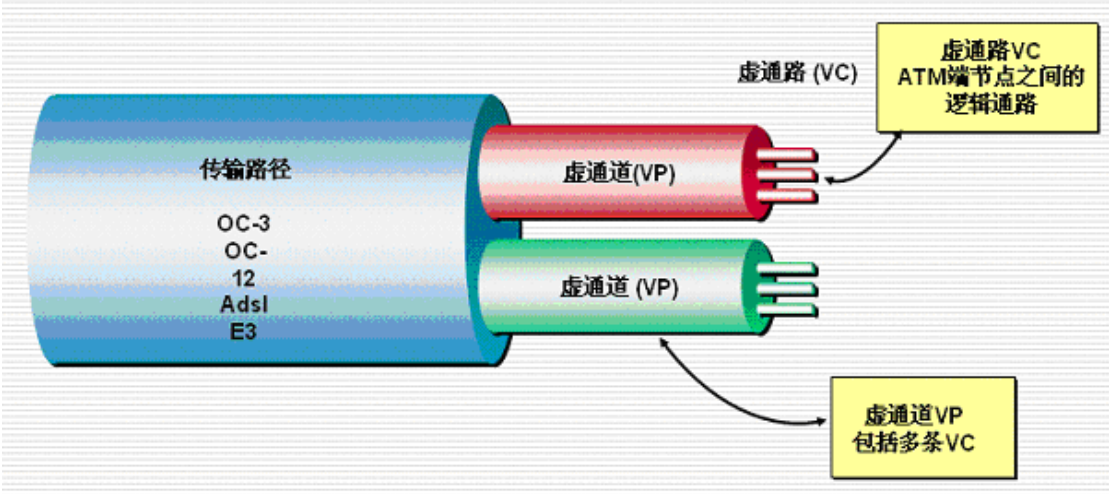


## 101. VPI/VCI

在 ATM 中, 使用一对 VPI/VCI 的组合来标识一条逻辑连接。同样, VPI/VCI 的值也是在本地接口才有意义。

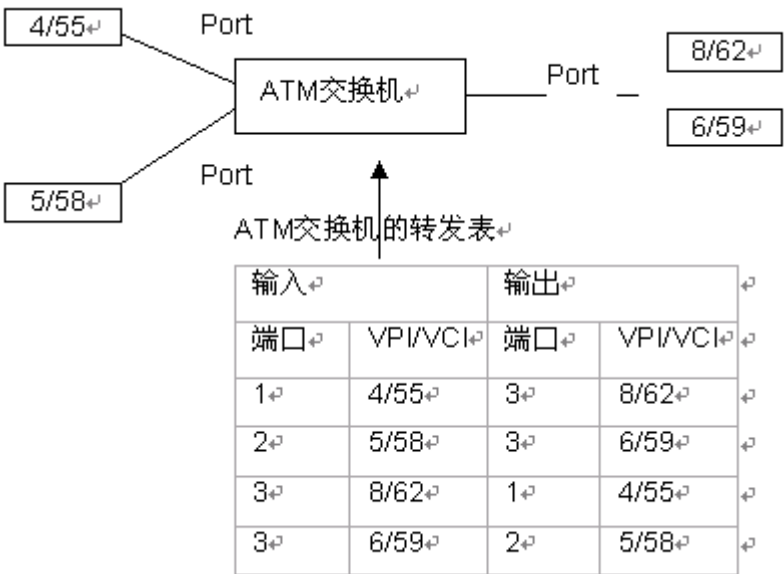
VPI（虚通道标识符）用于标识虚电路连接的虚通道号，而 VCI（虚电路标识符）用于标识虚通道中的虚电路号。一个虚电路连接（VCC）包含了多个 VP，一个虚通道（VP）又包含了多个虚电路（VC）。两者的组合构成了连接标识符。

为什么要分为 VP、VC 两级通道呢。这是因为随着网络的不断扩大，可以在主干网络上只进行 VP 的交换，减少转发表项和系统的资源。



## 102. ATM 信元的转发

ATM 信元中地址指的是 VPI/VCI（虚拟通路标识/虚电路标识），类似于 IP 地址。该 VPI/VCI 的号码应当有网络管理员定义或动态的由 ATM 交换机生成。信元的转发也是通过按照交换机内部的转发表来完成，如下图。



图中的转发表将 4/55 同 8/62 相关联，如第一行表示所有从 VPI/VCI 为 4/55



发到交换机的信元都会将信元头的 VPI/VCI 修改为 8/62 同 3 端口发送出去。相当与在 4/55 同 8/62 间、5/58 同 6/59 间建立了转发电路。

### 103. ATM 的网络接口

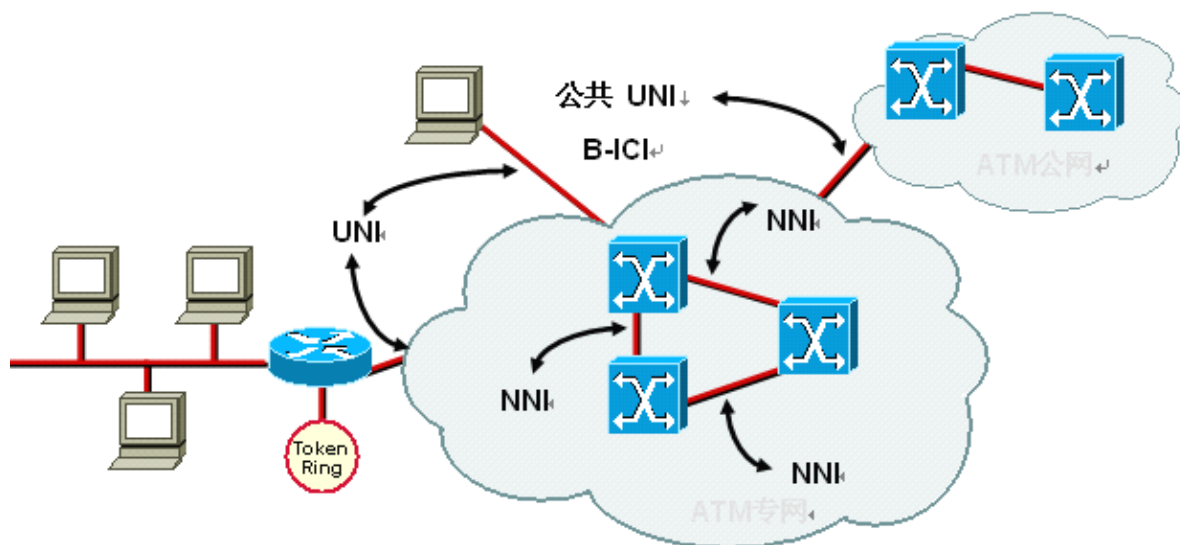
ATM接口主要分四种类型：用户网络接口接口（UNI）、NNI接口（NNI）、B—ICI接口、ATM网络互连接口。

（1）UNI（用户网络接口）定义的是外围设备与ATM交换机之间的接口。有两种类型的UNI：**公用UNI和专用UNI**。两种UNI的基本不同点是：专用UNI是使外围设备与专用网交换机相互连接的协议，而公用UNI是使外围设备与公用网交换机相互连接的协议。**两者最大的不同是在于SVC的编址方式上。专用UNI为NSAP（网络层服务接入点），而公用UNI为E.164。**

（2）NNI定义的是网络间的接口，专用NNI和公用NNI两者都涉及到交换机和交换机的内部互联，包括路由和信令方面。**PNNI是在专用ATM云内使用，而公用NNI由一个ATM服务提供商使用。**

（3）B—ICI（BISDN内部载波接口）提供对多个ATM服务提供商的内部连接。B—ICI与NNI紧密相连。

（4）AINI（ATM网络互连接口）使专用和公用网络实现了互联。AINI是另一种能实现专用对公用网络连通性的方式。是建立在PNNI信令之上。定义AINI的目的就是为了使两种网络互连更容易，



### ATM 接口总结

专用 ATM 网络	专用 ATM 网络	公用 ATM 网络	外围设备
公用 ATM 网络	IISP、PNNI	公用 UNI、AINI	专用 UNI
	公用 UNI、AINI	PNNI、B-ICI、	公用 UNI
		AINI	
外围设备	专用 UNI	公用 UNI	N/A

### 104. ATM 层次功能与工作过程

高层

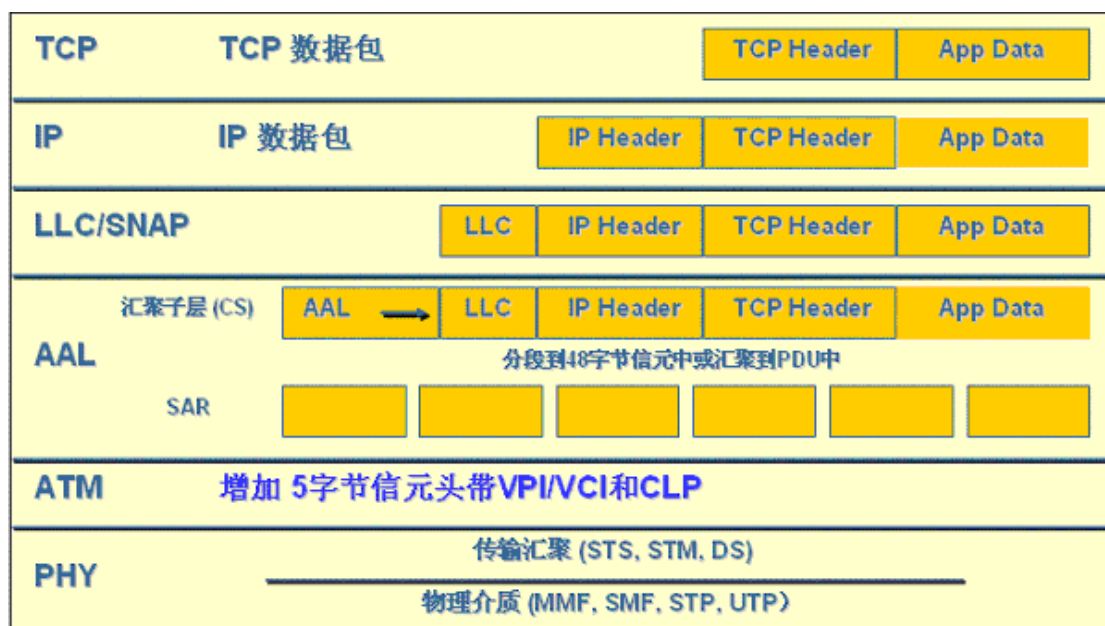
层  
管  
理

会聚子层  
分段和重组子层  
信头产生/校验  
信元 VPI/VCI 翻译  
信元复用和分路  
一般流量控制  
HEC 产生/校验  
信元定界和速率退耦  
传输帧的适配  
传输帧的产生和恢复  
比特定时（时钟恢复）  
线路编码  
物理介质

CS  
SAR  
  
ATM  
  
TC  
  
PMD

AAL  
  
  
  
  
  
物理层

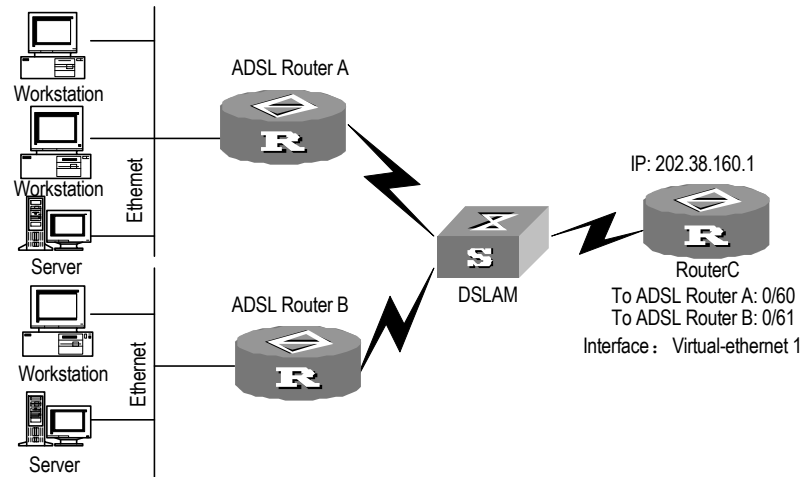
一个 IP 报文在整个 ATM 协议栈中传播的封装过程，解封装过程正好相反。



105. 之所以通过网上邻居和共享文件看到对方 **PC**, 是因为基于 **UDP** 的广播, 但只能在同一 **VLAN** 内 “看到”, 不同 **VLAN** 无法看到对方, 但可通过输入 **IP** 地址进行访问。若想“看到”跨 **vlan** 的 **pc** 需配置 **udphelper** 指定该跨 **vlan** 的 **pc** 的 **IP** 地址。

106. **IPoEoA** 应用需配置 **VE** 接口模板 (**VE** 口→**ATM** 接口), **PPPoA** 需配置 **VT** 模板 (**VT** 口→**ATM** 接口), **PPPoEoA** 需配置 **VE** 和 **VT** (**VT** 口→**VE** 口→**ATM** 口)。

(1) **IPoEoA** 的方式, 需要将 **IP** 报文封装在以太帧内, 再封装为 **ATM** 信元传输。所以需要在路由器之间有 **IP** 接口和以太网地址信息。可以通过建立虚拟逻辑以太网接口 (**VE**), 在将 **VE** 映射到 **ATM** 的 **PVC** 上的方式来实现。



### 报文转发步骤:

由 workstation 来 Ping 路由器 C

IPOE 报文发送到路由器 A, A 根据目的 IP 查找路由表(查看命令: `display ip routing-table`), 下一跳接口为 VE。

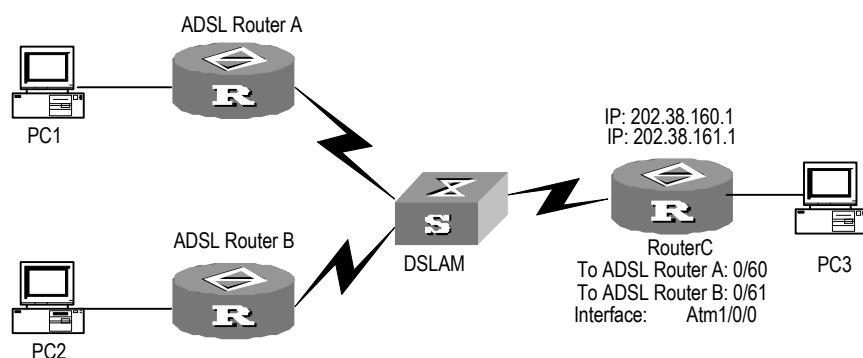
路由器通过 VE 映射 ATM 的 PVC(查看命令: `display atm map-info`), 将以太网报文封装到 ATM 信元内发送到 DSLAM, 报文结构为 IPOEOA

DSLAM 将信元转发到路由器 C 上

路由器收到 IPOEOA 报文后, 在 ATM 接口解封为 IPOE 报文转发给 VE。

由路由器 C 返回的 ICMP echo 报文处理方式同上类似。完成 PING 的过程。

(2) PPPoA 的方式是通过 PPP 的报文封装在 ATM 内在 ATM 网络上传输。原理同 IPOEOA 类似, 因为 PPP 的建议需要认证等相关操作, 所以通过建立一逻辑接口虚拟模板 (VT) 的方式来满足。



### 报文转发步骤:

当在路由器 A 上设置好 VT, 并在 ATM 建立到 VT 的映射后, 路由器 A 就会向路由器 C 发出 PPP 建立的请求, 并通过在路由器 C 上的认证。然后路由器 C 会向

路由器 A 通过 IPCP 方式分配一个 IP 地址。完成 PPP 的建立的操作过程

路由器 A 获得 IP 地址后，会在路由表内建立一条到达路由器 C 的路由（查看命令：display ip routing-table）。如果在路由器 A 上 Ping 路由器 C，路由器 A 首先会查路由表确定出接口为 VT。因为 VT 内链路封装格式为 PPP（查看命令：display interface Virtual-Template），所以将报文封装为 PPP 报文。

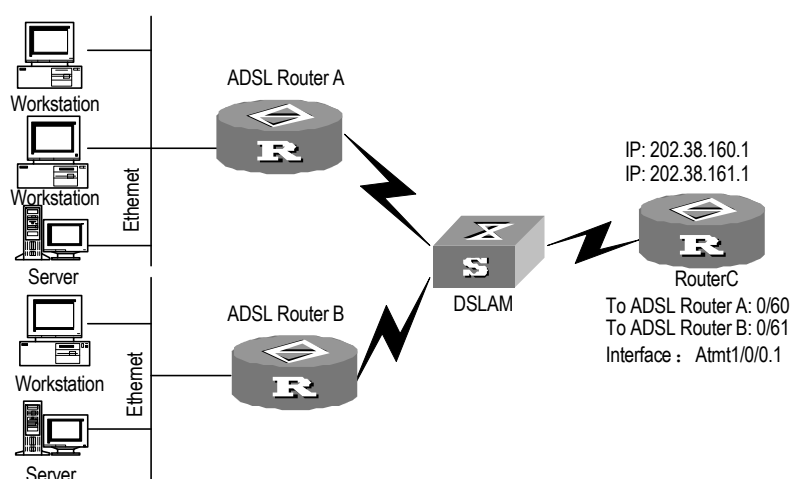
在根据 VT 所映射查找到相应的 ATM 接口（查看命令：disp atm map-info）。再将 PPP 报文封装到 ATM 信元内转发出去，也就是 PPPoA。

路由器 C 收到 DSLAM 转发的路由器 A 发出的信元，在 ATM 接口处解封装 PPPoA 为 PPP 报文，转到 VT 接口处理。

路由器 C 的 VT 接口再将 PPP 转为 IP 报文处理。

之后按照相反过程将应答报文发回给路由器 A，完成 Ping 的操作。

(3) PPPoEOA 的实现方法实际上就是在 VT 上实现 PPP 封装，在 VE 上实现将 PPP 封装成 PPPoE，在 ATM 接口上在封装为 PPPoEOA 的方式转发的过程。



### 报文转发步骤:

在 workstation 上 Ping 路由器 C。PC 发出的报文是 IPOE 报文。

路由器 A 收到后处理报文，根据目的 IP 查找路由表（查看命令：display ip routing-table），出接口为 VT，因为 VT 内封装格式为 PPP（查看命令：display interface Virtual-Template），所以将报文转为 PPP 封装。

在逻辑接口 VT 的关联查找根据 PPPoE 的 session，找到 VE。（查看命令：disp pppoe-client session summary 或 disp pppoe-server session summary）。因为在 VE 内封装格式为 PPPoE，所以根据 session 的源目的 MAC

将 PPP 报文封装为 PPPOE 报文。

再根据 VE 的关联的 ATM 接口（查看命令：disp atm map-info），将报文封装为 PPPOEOA 转发到 DSLAM。

DSLAM 将信元转发到路由器 C 上，ATM 接口去 PPPOEOA 封装为 PPPOE。在根据 VE 去封装为 PPP，在根据 VT 由路由器处理，发出响应报文。

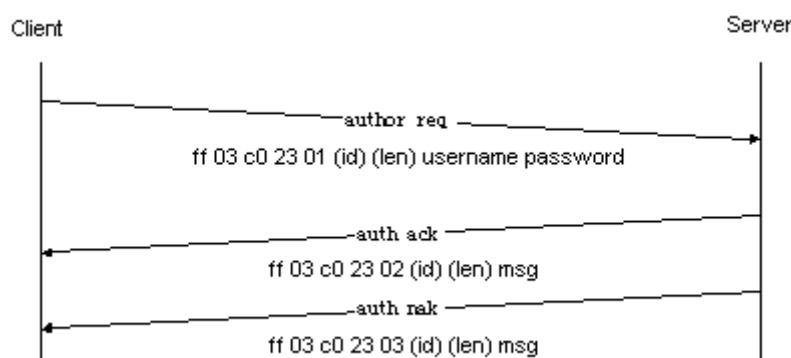
同样原理转发回路器 A，完成 Ping 的操作。

## 107. PPP 的验证

### （1）PAP 验证

**PAP 验证为两次握手验证，它在网络上采用明文方式传输用户名和口令。** PAP 验证的过程如下：

- 1 ①、被验证方发送用户名和口令到验证方；
- 1 ②、验证方根据本端用户表查看是否有此用户以及口令是否正确，然后返回不同的响应（Acknowledge or Not Acknowledge）。



### （2）CHAP 验证

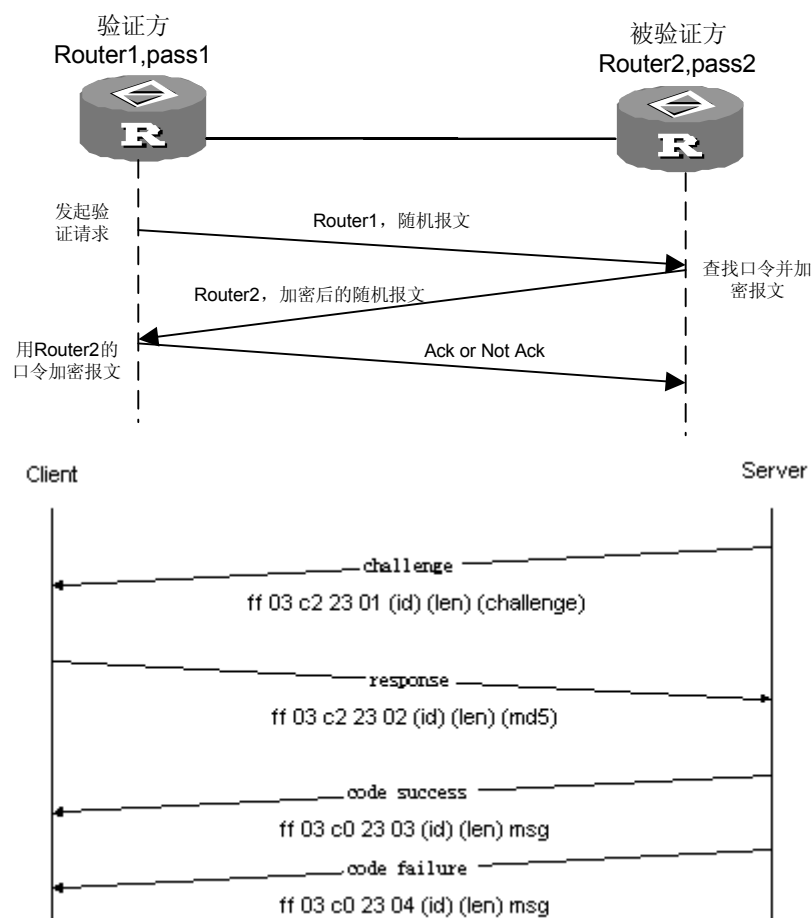
**CHAP 验证为三次握手验证，它只在网络上传输用户名，而用户口令并不在网络上传播。** CHAP 验证过程如下：

- 1 ①、验证方主动发起验证请求，向被验证方发送：  
一些随机产生的报文（Challenge）+ 验证方的用户名；
- 1 ②、被验证方接到验证方的验证请求后，被验证方根据此报文中验证方的用户名在 local-user 下和 ppp chap 下查找用户口令字。**若两者都存在，则 ppp chap password 配置的口令优先：**

如找到用户表中与验证方用户名相同的用户：  
 被验证方用户名+加密报文（此报文ID、local-user下的口令字和MD5算法）

如找到用户表中与验证方用户名相同的用户，检查本端接口上是否配置了ppp chap password命令，如果配置了该命令则：  
 被验证方用户名+加密报文（此报文ID、ppp chap下的口令字和MD5算法）

1 ③、验证方接收到该报文后，根据此报文中被验证方的用户名，在自己的本地用户数据库（local-user）中查找被验证方用户名对应的被验证方口令字，利用该口令和 MD5 算法对原随机报文加密，比较二者的密文，根据比较结果返回不同的响应（Acknowledge or Not Acknowledge）。



注：CHAP 验证时，两端密码一致则被验证端接口下只需定义用户名无需定义密码，即只需在系统视图下定义对端的 local-user。

## 108. PPP 运行流程

(1) 当物理层不可用时，链路处于 Dead 阶段，链路必须从这个阶段开始和结束。当物理层可用后，PPP 链路就会进入到 Establish 阶段。

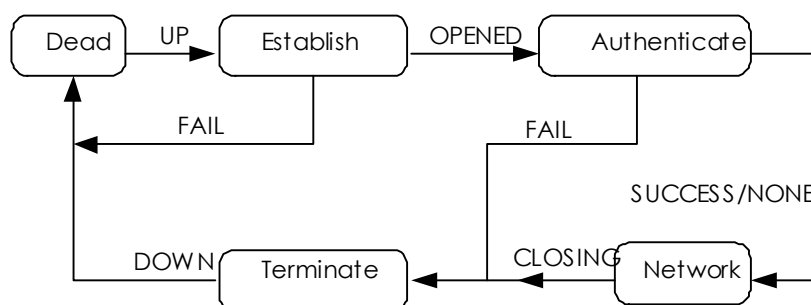
(2) 在 Establish 阶段 PPP 链路进行 LCP 协商，协商内容包括工作方式（是 SP 还是 MP）、验证方式和最大传输单元等。**LCP 在协商成功后进入 Opened 状态**，表示底层链路已经建立。

(3) 若未配置验证，则进入 Network 协商阶段(NCP)，此时 LCP 状态仍为 Opened，而 **NCP 状态从 Initial 转到 Request-sent**，进入第（5）步的流程；若配置了验证（远端验证本地或者本地验证远端）则进入 Authenticate 阶段，开始 CHAP 或 PAP 验证，进入第（4）步流程；

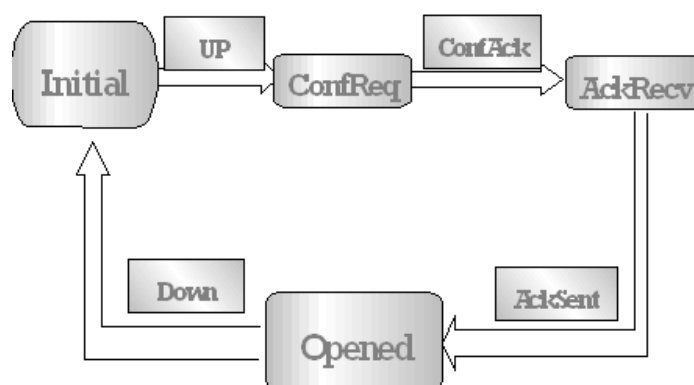
(4) 如果验证失败进入 Terminate 阶段，拆除链路，LCP 状态转为 Down；如果验证成功就进入 Network 协商阶段（NCP），此时 LCP 状态仍为 Opened，而 **NCP 状态从 Initial 转到 Request-sent**。

(5) NCP 协商支持 IPCP、IPXCP 协商，其中 IPCP 协商主要包括双方的 IP 地址。通过 NCP 协商来选择和配置网络层协议。只有选中的网络层协议配置成功后，该网络层协议才可通过这条链路发送报文了。

(6) PPP 链路将一直保持通信，直至有明确的 LCP 或 NCP 帧关闭这条链路，或发生了某些外部事件（例如，用户的干预）。



其状态转换过程为：





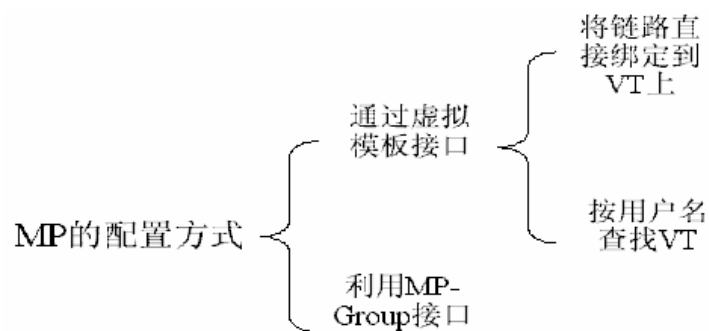
## 109. MP 的配置主要有两种方式

一种是通过虚拟模板接口（Virtual-Template），一种是利用 MP-Group 接口。  
采用虚拟模板接口配置 MP 时，又可以细分为两种情况：

①、将物理接口与虚拟模板接口直接关联：通过命令 `ppp mp virtual-template` 直接将链路绑定到指定的虚拟模板接口上，这时可以配置验证也可以不配置验证。如果不配置验证，系统将通过对端终端描述符捆绑出 MP 链路；如果配置了验证，系统将通过用户名和对端终端描述符捆绑出 MP 链路。

②、将用户名与虚拟模板接口关联：根据验证通过后的用户名查找相关联的虚拟模板接口，然后根据用户名和对端终端描述符捆绑出 MP 链路。这种方式**需要在要绑定的接口下配置 `ppp mp` 及双向验证（CHAP 或 PAP）**，否则链路协商不通。

如下图：



**这两种配置方式的区别主要是：**

1 ①、VT 可以与验证相结合，可以根据对端的用户名找到指定的虚拟模板接口，从而利用模板上的配置，创建相应的捆绑（Bundle），以对应一条 MP 链路。

1 由一个虚拟模板接口还可以派生出若干个捆绑（Bundle，系统中用 VT 通道来表示），每个捆绑对应一条 MP 链路。那么这样一来，从网络层看来，这若干条 MP 链路会形成一个点对多点的网络拓扑。从这个意义上讲，虚拟模板接口比 MP-GROUP 接口更加灵活。

1 为区分虚拟模板接口派生出的多个捆绑，需要指定捆绑方式，系统在虚拟模板接口视图下提供了命令 `ppp mp binding-mode` 来指定绑定方式，绑定方式有 authentication、both、descriptor 三种，缺省是 both。Authentication 是根据验证用户名捆绑，descriptor 是根据终端描述符捆绑（LCP 协商时，会协商出这个

选项值)，both 是要同时参考这两个值。

1 ②、MP-group 接口与虚拟模板接口相比则单纯许多，它是 MP 的专用接口，不能支持其他应用，也不能利用对端的用户名来指定捆绑，同时也不能派生多个捆绑。但正因为它的简单，导致了它的快速高效、配置简单、容易理解。

**110. PPP 的 pap 和 chap 认证中，单项验证时在主验证方的接口视图下配置认证方式，从认证方只需配置用户名和密码；双向验证时两端接口视图下都需配置认证方式。**

**111. 路由器升级注意事项**

(1) 1.74 注意关 PC 防火墙，配网关，路由器设为 aaa accounting optional；上传文件时

bin

put xxxx.bin system

(2) NE 的升级要设 ftp 目录。

**112. CMS 问题单升级研发时问题单提交类型有 4 种**

- (1) 第一次出现无解决方案
- (2) 技术问题
- (3) 新产品新版本老问题
- (4) 无解决方案重复出现的问题

**113. E1/T1 各接口说明**

目前，在数字通信系统中存在**两种时分复用系统**，一种是 ITU-T 推荐的 **E1 系统**，广泛应用于欧洲以及中国；一种是由 ANSI 推荐的 **T1 系统**，主要应用于北美和日本（日本采用的 J1，与 T1 基本相似，可以算作 T1 系统）。

### 第一部分 CE1/PRI 接口

(1) E1 工作方式（也称为非通道化工作方式）

它相当于一个不分时隙、数据带宽为 2Mbps 的接口，其逻辑特性与同步串口相同，支持 PPP、帧中继、LAPB 和 X.25 等数据链路层协议，支持 IP 和 IPX 等网

络协议。

(2) CE1/PRI 工作方式（也称为通道化工作方式）

当 CE1/PRI 接口使用 CE1/PRI 工作方式时，它在物理上分为 32 个时隙，对应编号为 0~31，其中 0 时隙用于传输同步信息。

对该接口有两种使用方法：CE1 接口和 PRI 接口。

①、当将接口作为 CE1 接口使用时，**可以将除 0 时隙外的全部时隙任意分成若干组（channel set），每组时隙捆绑以后，作为一个接口使用**，其逻辑特性与同步串口相同，支持 PPP、帧中继、LAPB 和 X.25 等数据链路层协议，支持 IP 和 IPX 等网络协议。

②、当将接口作为 PRI 接口使用时，时隙 16 被作为 D 信道来传输信令，因此，**只能从除 0 和 16 时隙以外的时隙中随意选出一组时隙作为 B 信道，将它们同 16 时隙一起，捆绑为一个 pri set，作为一个接口使用**，其逻辑特性与 ISDN PRI 接口相同，支持 PPP 数据链路层协议，支持 IP 和 IPX 等网络协议，可以配置 DCC 等参数。

### 配置方法总结：

- (1) 进入指定 CE1/PRI 接口：**controller e1 number**
- (2) 设置 CE1/PRI 接口匹配的传输线路长度：**cable { long | short }**

**long（缺省）**：表示接收器的衰减为-43db；

**short**：表示接收器的衰减为-10db。

- (3) 设置接口工作方式：

**using e1（工作在 E1 方式）**

或

**using ce1（工作在 CE1/PRI 方式，缺省）**

- (4) 若为 E1 方式，则直接进入系统自动创建的 Serial 接口：

**interface serial number:0**

若为 CE1 方式，则需要先指定为 channel-set 或 pri-set:

①、**channel-set set-number timeslot-list range**，系统会自动创建一个 Serial 接口 serial number:set-number。此接口的逻辑特性与同步串口相同。进入方式为：

**interface serial number:set-number**

②、**pri-set [ timeslot-list range ]**，系统会自动创建一个 Serial 接口 serial number:15。它在逻辑上等同于一个 ISDN PRI 接口。进入方式为：

**interface serial number:15**

**需要注意的是：**

①、对于 CE1/PRI 接口，只有利用命令 `using ce1` 使其工作在 CE1/PRI 方式时才可以被捆绑为 `channel set`。在一个 CE1/PRI 接口上可以捆绑出多达 31 个 `channel set`。

②、对于 CE1/PRI 接口，只有利用命令 `using ce1` 使其工作在 CE1/PRI 方式时，才可以被捆绑为 `pri set`。在将 CE1/PRI 接口捆绑为 `pri set` 时，如果不指定捆绑的时隙，则会将所有时隙捆绑起来，形成一个类似 30B+D 的 ISDN PRI 接口。如果捆绑的时隙只有一个 16 时隙，则会捆绑失败。**在一个 CE1/PRI 接口上同时只能捆绑出一个 `pri set`。**

③、CE1/PRI 接口工作在 CE1/PRI 方式下时，支持 `crc4` 和 `no-crc4`（缺省）两种帧格式。其中 `crc4` 帧格式支持对物理帧进行 4 比特的循环冗余校验，而 `no-crc4` 帧格式则不支持。

④、非成帧模式下，**CE1/PRI 接口相当于同步串口（这里称之为 E1 接口）**，没有“帧”的概念，因此不需要用 AIS 告警来进行帧同步，此时可以关闭 AIS 告警检测。但是，某些用户提出特殊需求——希望通过 AIS 告警快速感知对端 E1 接口的 UP/DOWN 的变化，此时需要将 AIS 告警检测开关打开。

**需要注意，非成帧模式下打开 AIS 告警检测开关会出现以下情况：**若此时对端的帧间填充符（也称为 idle 码）配置为 `0xff`（默认为 `0x7e`），最初会因为链路层协议没有 UP，数据量很小，链路上传送的都是帧间填充符 `0xff`，此时 E1 接口会收到大量的逻辑“1”，而 E1 接口的物理层芯片会误将这些填充符当作对方发来的 AIS 告警（AIS 告警也是大量的逻辑“1”），从而导致链路无法 UP。此时，必须将 AIS 告警检测开关关闭，链路方可以正常 UP。**只有 CE1/PRI 接口工作在非成帧模式（配置 `using e1` 命令）下，打开/关闭 AIS 告警开关命令才有效。成帧模式下，缺省已经打开 AIS 告警检测开关，进行帧同步检测，不能配置该命令。**

## 第二部分 E1-F 接口

E1-F 接口是指部分（Fractional）化 E1 接口，它是 CE1/PRI 接口的简化版本。在 E1 接入应用中，如果不需要划分出多个通道组（`channel set`）或不需要 ISDN PRI 功能，使用 CE1/PRI 接口就显得浪费。此时，可以利用 E1-F 接口来满足这些简单的 E1 接入需求。相对 CE1/PRI 接口而言，使用 E1-F 接口是一种低价位的 E1

接入方案。

与 CE1/PRI 接口相比，E1-F 接口的特点有：

(1) 工作在成帧方式时，**E1-F** 接口只能将时隙捆绑为一个通道组，而 CE1/PRI 接口可以将时隙任意分组，捆绑出多个通道组。

(2) **E1-F** 接口不支持 **PRI** 工作方式。

**E1-F 接口拥有两种工作方式：成帧方式和非成帧方式。E1-F 接口缺省工作在成帧方式。**

(1) 当 E1-F 接口工作于非成帧方式时，它相当于一个不分时隙、数据带宽为 2048kbps 的接口，其逻辑特性与同步串口相同，支持 PPP、HDLC、帧中继、LAPB 和 X.25 等数据链路层协议，支持 IP 和 IPX 等网络协议。

(2) 当 E1-F 接口工作于成帧方式时，它在物理上分为 32 个时隙，对应编号为 0~31。其中 0 时隙用于传输同步信息，**其余时隙可以被任意捆绑成一个通道组 (channel set)**，E1-F 接口的速率为  $n \times 64\text{kbps}$ ，其逻辑特性与同步串口相同，支持 PPP、帧中继、LAPB 和 X.25 等数据链路层协议，支持 IP 和 IPX 等网络协议。

### 配置方法总结：

(1) 与 CE1/PRI 接口不同，**E1-F** 接口没有 **Controller** 视图。系统将 E1-F 接口识别为一个同步串口，**进入 E1-F 接口的视图就是进入相应串口的视图**；E1-F 接口排列顺序与同步串口相同，它们与同步串口一起进行编号。

(2) 设置 E1-F 接口工作在非成帧方式：**fe1 unframed**

设置 E1-F 接口工作在成帧方式：**undo fe1 unframed (缺省)**

(3) 当 E1-F 接口工作在成帧方式时，可以对接口上的时隙进行捆绑：

**fe1 timeslot-list range**

### 在进入相应串口进行配置时，应注意：

①、缺省情况下，E1-F 接口对所有时隙进行捆绑。因为 E1-F 接口的 0 时隙被用于传输同步信息，所以，当对 E1-F 接口的时隙进行全部捆绑时，实际捆绑的时隙为 1~31 时隙。**与 CE1/PRI 接口不同的是，在 E1-F 接口上只能捆绑出一个通道组 (channel set)，捆绑出的通道组就对应当前的同步串口。**而在 CE1/PRI 接口上可以捆绑出多个通道组，并且每捆绑一个通道组，系统都会自动生成一个与

之相对应的同步串口。

②、E1-F 接口支持两种线路编解码格式：ami 格式和 hdb3（缺省）格式。

③、E1-F 接口工作在成帧方式时，支持 crc4 和 no-crc4（缺省）两种帧格式。其中 crc4 帧格式支持对物理帧进行 4 比特的循环冗余校验，而 no-crc4 帧格式则不支持。

### 第三部分 CT1/PRI 接口

T1 线路由 24 个多路复用信道组成，即一个 T1 基群帧 DS1 包含 24 个 DS0(64kbps)时隙，每个时隙有 8 个 bit 位，另外还有 1 bit 作帧同步位(framing bit)，故每个基群帧共  $24 \times 8 + 1 = 193\text{bit}$ 。由于每秒钟可以传送 8000 帧，故 DS1 的传送速率为  $193 \times 8\text{k} = 1.544\text{ Mbps}$ 。

CT1/PRI 接口**只能工作在通道化工作方式**，它有两种使用方法：

1 （1）当作为 CT1 接口使用时，**可以将全部时隙（时隙 1~24）任意地分成若干组**，每组时隙捆绑为一个 channel set。每组时隙捆绑后系统自动生成一个接口，其逻辑上等同于同步串口，支持 PPP、帧中继、LAPB 和 X.25 等数据链路层协议，支持 IP 和 IPX 等网络协议。

1 （2）当作为 PRI 接口使用时，由于**编号为 24 的时隙用作 D 信道传输信令**，因此只能从除 24 时隙以外的时隙中随意选出一组时隙作为 B 信道，**将它们同 24 时隙一起捆绑为一个 pri set，作为一个接口使用**，其逻辑特性等同于 ISDN PRI 口，支持 PPP 数据链路层协议，支持 IP 和 IPX 等网络协议，可以配置 DCC 等参数。

### 配置方法总结：

(1) 进入指定 CT1/PRI 接口：**controller t1 number**

(2) 设置 CT1/PRI 接口匹配的传输线路长度：

**cable long { 0db | -7.5db | -15db | -22.5db }**

**cable short { 133ft | 266ft | 399ft | 533ft | 655ft }**

**缺省为 long 0 db**

(3) 只能工作在通道化方式下，

**①、channel-set set-number timeslot-list range [ speed { 56k | 64k } ]**，系统会自动创建一个 Serial 接口 serial number:set-number。此接口的逻辑特性与同步串口

相同。进入方式为：

**interface serial number: set-number**

②、**pri-set [ timeslot-list range ]**，系统会自动创建一个 Serial 接口 serial number:23。它在逻辑上等同于一个 ISDN PRI 接口。进入方式为：

**interface serial number:23**

**在进入相应串口进行配置时，应注意：**

- ①、在一个 CT1/PRI 接口上可以捆绑出多达 24 个 channel set。
- ②、在将 CT1/PRI 接口捆绑为 pri set 时，24 时隙被用来当作 D 信道，其余时隙被用来当作 B 信道。如果不指定捆绑的时隙，则会将所有时隙捆绑起来，形成一个类似 23B+D 的 ISDN PRI 接口。如果捆绑的时隙只有一个 24 时隙，则会捆绑失败。在一个 CT1/PRI 接口上，同时只能捆绑出一个 pri set。
- ③、CT1/PRI 接口支持两种线路编解码格式：ami 格式和 b8zs（缺省）格式。
- ④、CT1/PRI 接口支持超帧（SF，Super Frame）和扩展超帧（ESF，extended Super Frame）两种帧格式。在超帧格式中，多个帧可以共享相同的帧同步信息和信令信息，从而可以有更多的有效位传送用户数据。实际应用中，需要对系统进行测试时，使用扩展超帧技术，可以使测试不影响正常业务的运行。CT1/PRI 接口的缺省帧格式为 ESF。
- ⑤、CT1/PRI 接口在配置为扩展超帧（ESF，extended Super Frame）格式时，其中的 FDL（Facility Data Link）位可用来传递报警信息、性能信息及环回码等，相关的规范包括 ANSI T1.403 和 AT&T TR 54016。
- ⑥、利用 bert 命令配置好测试模式，指定测试时间，开始测试后，可以查看接口状态中的 BERT 测试状态和测试结果。缺省情况下，CT1/PRI 接口不进行 BERT 测试。设置 CT1/PRI 接口进行线路位（Bit）错误率的测试命令如下：**bert pattern { 2^20| 2^15 } time minutes [ unframed ]**

#### **第四部分 T1-F 接口**

T1-F 接口是指部分（Fractional）化 T1 接口，它是 CT1/PRI 接口的简化版本。在 T1 接入应用中，如果不需要划分出多个通道组（channel set）或不需要 ISDN PRI 功能，使用 CT1/PRI 接口就显得浪费。此时，可以利用 T1-F 接口来满足这些简单的 T1 接入需求。相对 CT1/PRI 接口而言，使用 T1-F 接口是一种低价位的 T1



接入方案。

与 CT1/PRI 接口相比，T1-F 接口的特点有：

(1) 工作在成帧方式时，T1-F 接口只能将时隙捆绑为一个通道组，而 CT1/PRI 接口可以将时隙任意分组，捆绑出多个通道组。

(2) T1-F 接口不支持 PRI 工作方式。

**T1-F 接口只能工作在成帧工作方式**，它可以将全部时隙（时隙 1~24）任意地捆绑成一个组（channel set），T1-F 接口的速率为  $n \times 64\text{kbps}$  或  $n \times 56\text{kbps}$ ，其逻辑上等同于同步串口，支持 PPP、HDLC、帧中继、LAPB 和 X.25 等数据链路层协议，支持 IP 和 IPX 等网络协议。

### 配置方法总结：

(1) 与 CT1/PRI 接口不同，T1-F 接口没有 Controller 视图。系统将 T1-F 接口识别为一个同步串口，**进入 E1-F 接口的视图就是进入相应串口的视图**；T1-F 接口排列顺序与同步串口相同，它们与同步串口一起进行编号。

(2) 设置 T1-F 接口使用长距离传输线路 **ft1 cable long *decibel***

设置 T1-F 接口使用短距离传输线路 **ft1 cable short *length***

**缺省 T1-F 接口的传输线路衰减为 long 0db。**

(3) 对 T1-F 接口进行时隙捆绑

**ft1 timeslot-list *range* [ speed { 56k | 64k } ]**

### 在进入相应串口进行配置时，应注意：

①、与 CT1/PRI 接口不同的是，在 T1-F 接口上只能捆绑出一个通道组（channel set），捆绑出的通道组就对应当前的同步串口。而在 CT1/PRI 接口上，可以捆绑出多个通道组，并且每捆绑一个通道组，系统都会自动生成一个同步串口，与之相对应。缺省情况下，T1-F 接口对所有时隙进行捆绑。

②、当将 T1-F 接口绑定到 Virtual-template 下，若需要通过 ft1 timeslot-list 命令更改 T1-F 接口的时隙捆绑，请先将相应的 T1-F 接口 shutdown，然后再执行 ft1 timeslot-list 命令。需要注意的是链路两端的两个 T1-F 接口需要同时做上述的修改，然后对 T1-F 接口执行 undo shutdown 命令。否则执行命令 display interface virtual-template 时，显示的 virtual-template 口的波特率可能会不正确。

③、T1-F 接口支持两种线路编解码格式：ami 格式和 b8zs（缺省）格式。



④、FDL (Facility Data Link) 是 T1 的 ESF (Extended Super Frame, 扩展超帧) 帧格式中 4kbps 的一个带宽, 可以用来传递性能信息或者环回码之类。缺省情况下, FDL 为禁止状态。

⑤、利用 bert 命令配置好测试模式, 指定测试时间, 开始测试后, 可以查看接口状态中的 BERT 测试状态和测试结果。设置 T1-F 接口进行线路位 (Bit) 错误率的测试命令如下: `ft1 bert pattern { 2^20| 2^15 } time minutes [ unframed ]`

#### 114. 中低端路由器的 E1 板卡和串口板卡可以跨板进行 PPP 捆绑

#### 115. 中低端路由器串口对 CRC 校验的支持情况

(1) 对于 CE1 形成的串口、CE1 通道形成的串口、以及 CE1 通道时隙捆绑形成的串口, 都可以在相应的串口视图下配置它的 CRC 校验。可以配置 32 位、16 位及不校验, 缺省情况下串口使用 16 位 CRC 校验。

(2) 对于 CT1 模块、CT3 模块、CE3 模块及 POS 模块也支持上述 3 种校验方式。

(3) 对与 E1-F 模块形成的串口、同异步串口模块 (SA 与 SAE), 只支持 16 位的 CRC 校验且无命令可修改。

(4) CRC 校验配置一定要双方一致, 如果一端配置 CRC 校验, 一端不配置, 可能短时间内可以通信, 但长时间通信不能保证。

#### 116. 中低端路由器对于 E1 模块, 配置接口自环命令 **loopback** 时, 系统会强制修改接口时钟为 **master**; 如果使用直通头将收发两个 BNC 短接进行物理自环时, 需要手动将时钟设置成 **master** 模式, 否则可能导致物理层无法 UP。

#### 117. 中低端路由器 E1 与 E1VI 接口阻抗的异同

1E1/2E1/4E1/1E1-F/2E1-F/4E1-F 模块接口阻抗缺省为 75 欧姆, 设有内部拨码开关, 全 “ON” 时为 75 欧姆, 全 “OFF” 时为 120 欧姆。

E1VI 模块接口阻抗为 120 欧姆, 没有内部拨码开关, 线缆阻抗必须匹配, 即采用 120 欧姆的平衡双绞线电缆; 如果对端设备采用 75 欧姆的非平衡双绞线电缆, 则需要外加一个 75 欧姆-120 欧姆转换器, 以保证阻抗的连续性。

118. **网络攻击的主要方式：窃听报文、ip 地址欺骗、源路由攻击、端口扫描、DoS 拒绝服务、应用层攻击**

119. **RMON 共九组，常用的端口统计、历史、告警、事件 4 组。**

完全的 RMON 共有九组：1.统计 Statistics; 2.历史 History; 3.报警 Alarm; 4.主机统计数 Hosts; 5.主机统计最大值 Host Top N; 6.矩阵 Matrix; 7.过滤存储 Filter; 8.包捕获 Packet Capture; 9.事件 Event。一般的交换机至少支持 4 组（1，2，3，9 组）RMON。

120. **交换机端口自协商使用物理芯片来完成，不需要专用的数据报文。发送 16bit 的报文，整个报文按 16ms 间隔重复。**

121. **基于流的交换，第一个报文经过三层处理，其他的进行 2 次转发。包交换，每个包都要进行三层检查。**

122. **交换机属于 MDIX 设备，PC 为 MDI 设备。物理芯片实现。**

123. **802.1D 生成树协议**

802.1D 生成树协议，在网桥间传递一种特殊的配置信息 BPDU。功能：选择根桥、计算最短路径、选出指定网桥、选择个端口、选择包含在生成树上的端口。

BPDU 包括：根桥 ID、最小路径开销、指定网桥 ID、指定端口 ID。

（1）网桥 ID 用网桥优先级和 mac 地址组合来表示，桥优先级可以手工配置 0—61440（默认为 32768）。

（2）从本网桥到根桥的路径上所有经过端口的端口开销之和为“根路径开销”。

（3）端口 ID 由两部分组成：端口优先级+端口 Index，端口优先级可以手工配置 0—240（默认为 128）。

**注：**

**（1）BPDU 采用固定 mac 地址 01-80-c2-00-00-00 来作为目的地址。SAP 值 0x42。**

（2）根桥为网桥 ID 最小的那个。

（3）BPDU 优先级比较原则——4 者依次，最小的为优。

## 124. STP 报文格式如下：

配置 BPDU 在是一种“心跳”报文，只要端口上使能了 STP，则配置 BPDU 就会按照 Hello Timer 所规定的时间间隔发出。在初始化过程中，每个桥都主动发出配置 BPDU；但在网络拓扑稳定以后，只有根桥主动发送配置 BPDU，其他桥在收到上游传来的配置 BPDU 后，才触发发送自己的配置 BPDU。配置 BPDU 的长度至少要 35 个字节，而且如果当且仅当发送者 BID 或发送端口 PID 两个字段中至少有一个和本桥本接收端口不同，才会被处理，否则丢弃，这样避免了处理和本端口信息一致的 BPDU。



说明如下：

**DMA:** 目的 MAC 地址，配置消息的目的地址是一个固定的桥的组播地址（**0x0180c2000000**）

**SMA:** 源 MAC 地址，即发送该配置消息的桥 MAC 地址

**L/T:** 帧长

**LLC Header:** 配置消息固定的链路头

**Payload:** BPDU 数据

域	字节	说明
协议号	2	总是 0
版本	1	总是 0
类型	1	当前 BPDU 的类型 0 = 配置 BPDU, 0x80= TCN BPDU
标志	1	最低位 = TC（Topology Change, 拓扑变化）标志 最高位 = TCA（Topology Change Acknowledgment, 拓扑变化确认）标志
根桥 BID	8	当前根桥的 BID，由树根的优先级（0-65535，默认 32768）和 MAC 地址组合而成。
根路径开销	4	本端口累计到根桥的开销，实际由 PortPathCost 叠加而成，有两个标准——dot1d-1998，默认值为 100 和 dot1t，默认值为 200000。
发送者 BID	8	本交换机的 BID，由指定交换机的优先级和 MAC 地址组合而成。
发送端口 PID	2	发送该 BPDU 的端口 ID，由指定端口的优先级（0-256，默认 128）和端口编号组成。
Message Age	2	该 BPDU 的消息年龄

Max Age	2	消息老化年龄
Hello Time	2	发送两个相邻 BPDU 间的时间间隔
Forward Delay	2	控制 Listening 和 Learning 状态的持续时间

其中“标志”段格式如下：

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
TCA	保留未使用						TC

**TCN BPDU** 内容比较简单，只有“协议号、版本和类型”前 3 个字段。且类型字段为 **0x80**。TCA 位只有在回应 TCN BPDU 的“配置 BPDU”中置 1。

## 125. RSTP 报文格式

在 BPDU 的格式上，除了保证和 STP 格式基本一致之外，RSTP 作了一些小的变化。一个是在 Type 字段，配置 BPDU 类型不再是 0 而是 2，版本号也变成了 2。另一个变化是在 Flag 字段，把原来保留的中间 6 位使用起来。这样改变了的配置 BPDU 叫做 **RST BPDU**。

RST BPDU 的 Flag 字段格式：

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
TCA	Agreement	Forwarding	Learning	端口角色		Proposal	TC

端口角色 =

- 00 未知
- 01 根端口
- 10 Alternate / Backup
- 11 指定端口

## 126. MSTP 报文格式

无论是域内的 MST BPDU 还是域间的。其前 35 个字节和 RST BPDU 相同。从第 36 个字节开始是 MSTP 专有段。最后的 MSTI 配置信息字段由若干 MSTI 配置信息组连缀而成。

**MST BPDU 和 RST BPDU 相同的前 35 字节如下：**

长度	偏移	字段名
2	0	协议标识符
1	2	协议版本标识符
1	3	BPDU类型
1	4	CIST标志字段
8	5	CIST根桥
4	13	CIST外部路径开销
8	17	CIST每个域的根
2	25	CIST端口标识
2	27	Message Age
2	29	Max Age
2	31	Hello Time
2	33	Forward Delay
1	35	Version1 长度(0)

**MST 专有字段如下：**

长度	偏移	字段名
2	36	Version3 长度
51	38	MST 配置标识
4	89	IST 内部路径开销
8	93	CIST 桥 BID
1	101	CIST 剩余跳数
Version3 LEN	102	MSTI 配置信息

**MSTI 配置信息如下：**

长度	字段名
1	MSTI 标志
8	MSTI 域根
4	MSTI 内部路径开销
1	MSTI 桥优先级
1	MIST 端口优先级
1	MSTI 剩余跳数

**127. 当拓扑发生变化时，STP 是否产生 TCN BPDU 取决于以下两条标准。**

(1) 网桥至少有一个指定端口，并且某端口从其他状态（如 blocking、listening 或 learning）转到 forwarding 状态。

(2) 某端口由 forwarding、learning 状态转到 blocking 状态。

当以上两个条件满足其一时，STP 交换机就会发出 TCN BPDU 报文。

**128. 对于 STP，一共有 3 个计时器影响着端口状态以及网络的收敛。**

(1) **Hello Timer:** STP 交换机发送 BPDU 的时间间隔。当网络拓扑稳定之后，该计时器的修改只有在根桥修改才有效。根桥会在之后发出的 BPDU 中填充适当的字段以向其他非根桥传递该计时器修改信息。但当拓扑变化之后，TCN BPDU 的发送不受这个计时器的管理。

(2) **Forwarding Delay Timer:** 指一个端口 Listening 和 Learning 的各自时间，默认为 15 秒，即 Listening 状态持续 15 秒，随后 Learning 状态再持续 15 秒。这两个状态下的端口会处于 Blocking 状态（这里的 blocking 状态指的是不接收和转发数据报文），这是 STP 用于避免临时环路的关键。

(3) **Max Age 和 Message Age:**

端口保存的配置消息有一个生存期 Message Age 字段，并按时间递增；每当收到一个生存期更小的配置消息，则更新自己的配置消息；端口会根据接收到的 BPDU 存储所接收到的最好的四个信息（根桥 BID、累计根路径开销、发送者 BID 和发送端口 PID）。每次接收到合适的 BPDU，端口都会启动这个 Max Age 计时器。超过这个 Max Age 时间端口接收不到合适 BPDU，就会认为网络直径过大。这个时间默认为 20 秒。

**129. stp 端口的几种状态:**

(1) disabled 不收发任何报文。

(2) Blocking 不接收和发送数据，接受但不发送 bpdu，不进行地址学习。

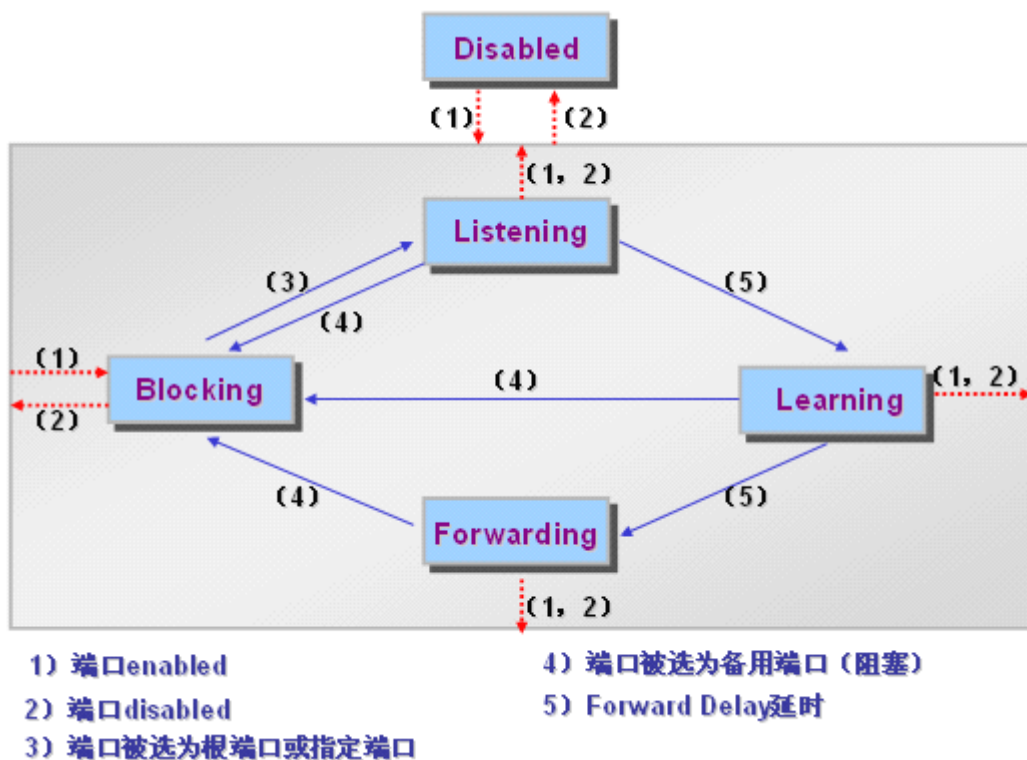
(3) Listening 不接收和发送数据，接受并发送 bpdu，不进行地址学习（根桥、根端口、指定端口就是在该状态内完成）。

(4) Learning 不接收或转发数据，接受并发送 bpdu，开始地址学习。

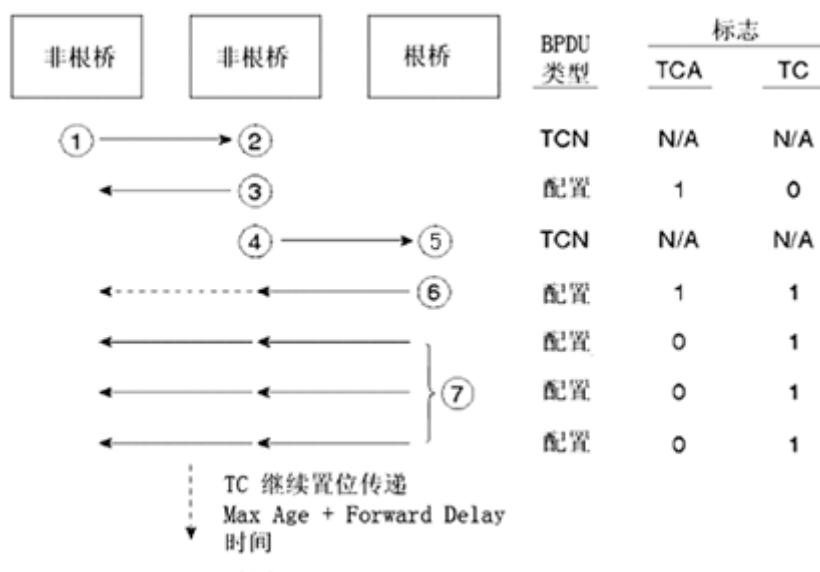
(5) Forwarding 接受并转发数据，接受并发送 bpdu，学习地址。

说明：端口处于 Listening 和 Learning 状态的时间是由 Forward Delay Timer 来统一控制的，这两个时间总是一样长的。

端口状态变化如下：



### 130. STP 拓扑变化后的 BPDU 发送处理过程



说明如下：

如果非根桥交换机的指定端口断掉，则交换机会立即通过根端口以一定速率发送 TCN BPDU 给上游交换机，上游交换机收到该 TCN BPDU 后会立刻向下游交换机回应 TCA BPDU(即把标志字段的 TCA 位置位的配置 BPDU)并继续向上游传递 TCN BPDU。下游交换机收到 TCA 消息的交换机会停止发送 TCN BPDU。如此不断的传递，直到传到根桥。然后，根桥将自己的 MAC 地址表老化时间改为 Forward Delay，并将 TCN 位置 1。其后会持续 Forward Delay+Max Age 长的时间内在发出的配置 BPDU 中把 TC 位置位。其下游任何交换机接收到根桥传递过来的 TC 置位的配置 BPDU 都会将自己的 MAC 地址表老化时间修改为 Forward Delay 那么长时间。

### 131. 快速生成树改进:

(1) 若旧的根端口已经阻塞，新的根端口连接网段的指定端口正好处于转发态，那新的根端口可无延时进入转发。

(2) 等待进入转发的指定非边缘接口向下游发送一个握手报文，下游若回应赞同，则此接口无延时进入转发。**握手必须在点对点链路中，会向下传递握手直到网络边缘。**

(3) 边缘接口无时延进入转发。

注：RSTP 也是单生成树实例，网络直径最好不要超过 7。

### 132. STP 与 RSTP 区别

- (1) 协议版本不同 (0 vs 2)
- (2) 端口状态转换方式不同 (5 种 vs 3 种)
- (3) 配置消息报文格式不同
- (4) 拓扑改变消息传播方式不同。

### 133. 传统 STP 的问题——STP 和 RSTP 都是基于端口与 VLAN 无关的协议。

Trunk 链路上实际上运行着多个 VLAN，所有 VLAN 共用一棵生成树；无法实现不同 VLAN 在多条 Trunk 链路上的负载均衡。

### 134. STP、RSTP 和 MSTP 的比较

(1) STP 的特性

形成一棵无环路的树：解决环路故障并实现冗余备份



(2) RSTP 的特性

①、形成一棵无环路的树：解决环路故障并实现冗余备份

②、快速收敛

根端口快速进入转发状态

采用握手机制实现端口的快速转发

设置边缘端口实现快速转发

(3) MSTP 的特性

①、形成一棵无环路的树：解决环路故障并实现冗余备份

②、快速收敛

③、形成多棵生成树实现负载均衡

不同 VLAN 的流量可以按照不同的路径进行转发

135. STP、RSTP 和 MSTP 间 BPDU 报文的区别

	Protocol version	BPDU type
STP (802.1d):	00	00 (配置 BPDU), 0x80 (TCN BPDU)
RSTP (802.1w)	02	02
MSTP (802.1s)	03	02

**注:** 在 STP 中有配置 BPDU 和 TCN BPDU (拓扑改变通知) 两种报文; RSTP 中有配置 BPDU 和 TC BPDU。

136. 当对一个端口进行配置时, 环路保护功能、Root 保护功能和设置边缘端口三个配置项中, 同一时刻只能有一个配置项生效。

(1) BPDU 保护 (经常和设置边缘端口共同使用) 功能: 在边缘交换机的系统视图下配置, 交换机上启动了 BPDU 保护功能以后, 如果边缘端口收到了 BPDU, 系统就将这些端口 shutdown, 同时通知网管。被 shutdown 的端口只能由网络管理人员恢复。

(2) 环路保护功能 (端口视图下配置): 环路保护对端口角色为 ROOT、ALTERNATE 的实例有效。但是, 参与 MSTP 计算的所有端口都可以配置环路保护, 环路保护对于指定端口没有影响。

(3) 根保护功能 (端口视图下配置): 对于设置了 Root 保护功能的端口, 端口角色只能保持为指定端口。一旦这种端口上收到了优先级高的配置消息, 即其将

被选择为非指定端口时,这些端口的状态将被设置为阻塞状态,不再转发报文(相当于将此端口相连的链路断开)。当在 2 倍 Forward Delay 时间内没有收到更优的配置消息时,端口会恢复原来的正常状态。

### 137. MSTP 在工程中使用的规范

- 1、**必须**将交换机连接客户端或者服务器(包括其他不会发出 BPDU 报文的网络终端或者网络设备)的端口,配置成为边缘端口,同时开启交换机的 BPDU 保护功能;或者直接关闭该端口的生成树协议。

配置方法如下:

```
[Quidway-Ethernet1/0/1]stp edged-port enable
```

```
[Quidway]stp bpdu-protection
```

或者:

```
[Quidway-Ethernet1/0/1]stp disable
```

- 2、为了避免端口由于各种错误而发生了端口角色改变,导致网络中产生环路,在交换机上参与生成树协议计算的端口上**必须**增加环路保护功能。

配置方法如下:

```
[Quidway-Ethernet1/0/1]stp loop-protection
```

- 3、根保护功能属于**可选**功能,所以在不确定根保护特性功能的情况下,不需要配置根保护功能。

由不同厂商设备 MSTP 网络互连形成的大网络,由于其他厂商用服人员、用户或其他相关人员的误配置,可能使原本指定为根桥的我司设备根桥角色被抢夺,导致全网的拓扑振荡。为了避免这种情况,如果网络规划中已经指定我司设备为根桥,则我司设备网络和其他厂商设备网络(我司设备的下游网络)边界上,在我司设备上和其他厂商设备互连的端口上,可以配置 Root 保护功能。当收到来自其他厂商设备网络的优先级更高的 BPDU 报文使,我司设备会丢弃该报文,并将端口临时阻塞,防止网络拓扑振荡。

配置方法如下:

```
[Quidway-Ethernet1/0/1]stp root-protection
```

- 4、为了避免交换机由于收到频繁的 TC/TCN 报文,而按照协议规定对 MAC 地址表项

及 ARP 地址表项进行频繁删除操作，继而出现设备 CPU 占用率增高、业务中断的故障，**必须**在交换机上增加 TC 报文保护功能的配置。

配置方法如下：

```
[Quidway]stp tc-protection enable
```

但可以根据实际配置决定 TC 报文保护的域值。当实例数增多时，TC 数量会增多。一般地，为了减少 CPU 负担，可以适当下调 TC 报文保护的域值；但如果要提高各实例流量切换的性能，可以适当上调 TC 报文保护的域值。缺省阈值为 6。

配置方法如下：

```
[Quidway]stp tc-protection threshold 6
```

- 5、为了在出现抢根时，可以打印出日志和告警信息，及时通知网络管理员。在指定 MSTP 网络根桥时，**强烈推荐**使用主根配置命令。

配置命令如下

```
[Quidway]stp instance instance-id root primary
```

- 6、为了避免由于上游交换机 CPU 负荷或者光纤单通网络故障情况对下游交换机 MSTP 计算造成影响，导致网络拓扑频繁振荡，**强烈推荐**在除根桥以外的下游交换机上增加超时因子的配置。

配置命令如下：

```
[Quidway]stp timer-factor 10
```

- 7、MSTP 和 RSTP 互连的网络，当 RSTP 设备做上游，为了实现 RSTP 设备端口状态的快速迁移。请在 MSTP 设备上和 RSTP 设备互连的端口增加 No-Agreement-Check 的配置。

配置命令如下：

```
[Quidway-Ethernet1/0/1]stp no-agreement-check
```

- 8、在和支持 IEEE802.1s 标准 MSTP 的 Cisco 或者其他厂商设备互连的网络中，为了实现多实例互通。请在我司 MSTP 设备的端口下增加强制标准报文的配置。

配置命令如下：

```
[Quidway-Ethernet1/0/1]stp compliance dot1s
```

上述使用规范总结于下表中：

特 性	要 求
MSTP 模式	建议不作修改
BPDU 保护	必须配置

环路保护功能	必须配置
根保护	可选配置
TC 报文保护	必须配置
主根	强烈推荐
超时因子	强烈推荐
No-Agreement-Check	RSTP 做上游时，必须配置
强制标准报文	和其他厂商设备互通时，必须配置

### 138. STP PATH COST 的三个标准

STP的path cost计算有下面三个标准：

**系统视图** **stp pathcost-standard { dot1d-1998 | dot1t | legacy }**

参数说明如下：**dot1d-1998**：IEEE 802.1D标准方法。

**dot1t**：IEEE 802.1t标准方法。

**legacy**：华为的私有计算方法

知道了 port cost，再查找下面的表就可以知道是哪种标准，如果没有匹配下面的表，那使用的就是华为私有的 legacy.

链 路 速率	双工状态		802.1D-1998	IEEE 802.1t	华 为 -3com 标 准
0	-		65535	200,000,000	200,000
10 Mbit/ s	Half-Duplex				
	Full-Duplex		100	2,000,000	2,000
	Aggregated Link	2	99	1,999,999	2,000
	Ports		95	1,000,000	1,800
	Aggregated Link	3	95	666,666	1,600
	Ports		95	500,000	1,400
100 Mbit/ s	Half-Duplex				
	Full-Duplex		19	200,000	200
	Aggregated Link	2	18	199,999	200
	Ports		15	100,000	180
	Aggregated Link	3	15	66,666	160
	Ports		15	50,000	140
	Aggregated Link	4			
	Ports				
	Half-Duplex				
	Full-Duplex				
	Aggregated Link	2			
	Ports				

链 路 速率	双工状态	802.1D-1998	IEEE 802.1t	华 为 -3com 标 准
1000 Mbit/ s	Full-Duplex			
	Aggregated Link 2	4	20,000	20
	Ports	3	10,000	18
	Aggregated Link 3	3	6,666	16
10 Gbit/ s	Ports	3	5,000	14
	Aggregated Link 4			
	Ports			
	Full-Duplex			
10 Gbit/ s	Aggregated Link 2	2	2,000	2
	Ports	1	1,000	1
	Aggregated Link 3	1	666	1
	Ports	1	500	1
10 Gbit/ s	Aggregated Link 4			
	Ports			
	Full-Duplex			
	Aggregated Link 2			

一般情况下，全双工状态下链路的路径开销值比半双工状态下略小一点。

在计算聚合链路路径开销值时，802.1D-1998 标准不考虑该聚合链路的链路数量。802.1T 标准则考虑聚合链路的链路数量，计算公式为

路径开销 = 200,000,000 / 链路速率

公式中，链路速率为聚合链路中处于非阻塞状态的端口速率之和，单位为 100Kbit/s。

139. 中低端路由器 1.74 版本中 **display base-information** 命令中没有 **logbuffer** 的信息，也没有 **display logbuffer** 命令，可通过 **display info-center logbuffer** 命令查看缓冲区中的调试和日志信息。

140. 路由器 CMW3.4 版本下基于 MAC 的 ACL 需在桥接模式实现；CMW1.74 版本下无此限制。CMW1.74 版本下 firewall 缺省是 enable 的；CMW3.4 版本下 firewall 需手工 enable。CMW1.74 版本下 ACL 默认是深度优先匹配；CMW3.4 版本下 ACL 默认是配置顺序匹配。

141. 交换机与路由器的 ACL 比较

#### (1) 交换机的 ACL

项目	数字取值范围
基于数字标识的基本访问控制列表	2000~2999

项目	数字取值范围
基于数字标识的高级访问控制列表	3000~3999
基于数字标识的二层访问控制列表	4000~4999
基于数字标识的用户自定义访问控制列表	5000~5999
一条访问控制列表可以定义的子规则	0~65534
交换机最多可以定义的子规则(所有访问控制列表的子规则之和)	—

### 需要注意的是：

如果 ACL 用于直接下发到硬件中对转发数据进行过滤和流分类，则用户定义的子规则匹配顺序将不起作用。如果 ACL 用于对由软件处理的报文进行过滤和流分类，用户指定的匹配顺序将会有效，并且用户一旦指定某一条访问控制列表子规则的匹配顺序，就不能再更改该顺序。在定义二层和用户自定义的访问控制列表时不能定义匹配顺序。

1 **缺省情况下**，访问控制列表中子规则的匹配顺序**为按用户配置顺序进行匹配**。

### (2) 路由器的 ACL

在 **VRP 3.4** 版本下：

- 1000~1999：基于接口的访问控制列表
- 2000~2999：基本的访问控制列表
- 3000~3999：高级的访问控制列表
- 4000~4999：基于 MAC 地址的访问控制列表。

在 **VRP 1.74** 版本下：

- 2000~2999：基本的 ACL
- 3000~3999：扩展的 ACL：
- 4000~4099：有关 MAC 地址的 ACL
- 4100~4199：以太网类型的 ACL。

## 142. 统路由器的处理流程

图中所示的主机 A 和 B 之间通过路由器进行的互连，其首次互通如下过程（以 A 向 C 发起 ping 请求为例），假定主机的 ARP 表和路由器中的 ARP 表项为空：

（1）A 检查报文的目的 IP 地址，发现和自己不在同一个网段，需要通过网关（这里为路由器）进行路由转发，查找网关的 MAC 地址表，没有发现网关的 MAC 地址；

（2）A---->路由器，发送 ARP 请求广播报文，请求网关的 MAC 地址，该报文直接发送给路由器；

（3）路由器---->A，发送 ARP 回应单播报文，目的 MAC 地址为主机 A，同时在路由器上形成关于主机 A 的 ARP 表项，A 收到 ARP 应答后，在 A 上形成了关于网关的 ARP 表项；

（4）A---->路由器 icmp request（目的 MAC 是路由器 Port1 的 MAC，源 MAC 是 A 的 MAC，目的 IP 是 C，源 IP 是 A）；

（5）路由器收到报文后，在路由表中根据报文的目的 IP 地址查找路由表项，然后根据 ARP 表来查找下一跳的 MAC 地址，此时没有发现 B 的 MAC，将此 ICMP 报文缓存下来。

（6）路由器---->B，发送 ARP 请求报文，源 MAC 为 Port2 的 MAC，目的 MAC 为广播地址；

（7）B--->路由器，发送 ARP 回应报文，路由器形成了关于主机 B 的 ARP 表项；

（8）路由器---->B，发送 icmp request（目的 MAC 是 B 的 MAC，源 MAC 是

路由器的 Port2 的 MAC，目的 IP 是 B，源 IP 是 A），同步骤（4）相比**报文的 MAC 头进行了重新的封装，而 IP 层以上的字段基本上不变**；

（9） B---->A，发送 icmp reply，这以后的处理同前面 icmp request 的过程基本相同，只是没有了 ARP 请求的部分。

传统路由器的 IP 报文的路由转发过程，对每个包都需要进行路由查找和转发处理的。

### 143. 三层交换机进行数据包交换的过程。

如图所示：交换机上划分了两个 VLAN，在 VLAN1，VLAN 2 上配置了路由接口用来实现 VLAN 1 和 VLAN 2 之间的互通，主机 A、B 在 VLAN1 内，主机 C 在 VLAN2 内。

#### ● A 和 B 之间的互通（以 A 向 B 发起 ping 请求为例）——**相同 VLAN**

- （1） A 检查报文的目的 IP 地址，发现和自己在同一网段；
- （2） A---->B ARP 请求报文，该报文在 VLAN1 内广播；
- （3） B---->A ARP 回应报文；
- （4） A---->B icmp request；
- （5） B---->A icmp reply；

#### ● A 和 C 之间的互通（以 A 向 C 发起 ping 请求为例）：——**不同 VLAN**

- （1） A 检查报文的目的 IP 地址，发现和自己在不在同一网段；
- （2） A---->switch（int vlan 1） ARP 请求报文，该报文在 VLAN1 内广播；
- （3） 网关---->A ARP 回应报文，此为单播报文，目的 MAC 地址为主机 A，同时生成了到 A 的硬件转发表项；
- （4） A---->switch icmp request（目的 MAC 是 int vlan 1 的 MAC，源 MAC 是



A 的 MAC，目的 IP 是 C，源 IP 是 A)；

(5) switch 收到报文后，根据报文的目的 MAC 判断出是三层的报文。检查报文的目的 IP 地址，发现是在自己的直连网段；

(6) switch (int vlan 2) ---->C ARP 请求报文，该报文在 VLAN2 内广播；

(7) C--->switch (int vlan 2) ARP 回应报文；同时生成到 C 了硬件转发表项。

(8) switch (int vlan 2) ---->C icmp request (目的 MAC 是 C 的 MAC，源 MAC 是 int vlan 2 的 MAC，目的 IP 是 C，源 IP 是 A)，同步骤 (4) 相比**报文的 MAC 头进行了重新的封装，而 IP 层以上的字段基本上不变**，封装完后进行转发；

(9) C---->A icmp reply，此时通过查找硬件转发表项，通过 ASIC 进行转发。后续到 A 和到 C 的报文，都是通过查找硬件转发表，通过 ASIC 进行转发。

以上的各步处理中，如果 ARP 表中已经有了相应的表项，则不会给对方发 ARP 请求报文。

以后，当再进行 A 与 C 之间数据包转发时，将用最终的目的站点的 MAC 地址封包，数据转发过程全部交给第二层交换处理，信息得以高速交换。其指导思想为：**一次路由，随后交换。而传统的路由器对每一个数据包都进行拆包、打包的操作，限制了系统的带宽。**

#### 144. 二层交换的一般流程如下：

(1) 当交换机从某个端口收到一个数据包，它先读取包头中的源 MAC 地址，这样它就知道源 MAC 地址的机器是连在哪个端口上的；

(2) 再读取包头中的目的 MAC 地址，并在地址表中查找相应的端口；

(3) 如表中有与这目的 MAC 地址对应的端口，把数据包直接发送到这端口上；

(4) 如表中找不到相应的端口则把数据包广播到所属 vlan 的所有端口上；当目的主机对源主机回应时，交换机又可以学习目的主机的 MAC 地址与哪个端口对应，在下次传送数据时就不再进行广播了。

不断的循环这个过程，对于全网的 MAC 地址信息都可以学习到，二层交换机就是这样建立和维护它自己的地址表。

注：

- (1) 广播报文：如果报文正确，则在 VLAN 内广播。
- (2) 多播报文：如果多播 MAC 未知，则在 VLAN 内广播。如果多播 MAC 已知，则根据 MAC 表项中端口列表转发。
- (3) 单播报文：如果单播 MAC 未知，则在 VLAN 内广播。如果单播 MAC 已知，则根据 MAC 表项中的内容处理（包括目的丢弃、源丢弃、正常转发等）。

#### 145. **MAC 表项地址学习规则**

如果报文的 SA+VLAN 组合在 MAC 表中被找到：

- (1) 报文入端口与 MAC 表项中端口一致，则跳过地址学习，但表项的 HIT 位被设置 1，使得表项在下一轮老化检查中可以继续保留。
- (2) 报文入端口与 MAC 表项中端口不一致，MAC 地址是静态的，则跳过地址学习，报文 copy 到 CPU。
- (3) 报文入端口与 MAC 表项中端口不一致，MAC 地址是动态的，则进行地址学习。

如果报文的 SA+VLAN 组合在 MAC 表中未找到，则进行地址学习。

#### 146. **目前路由器实现机制是先找路由器表，再查找 nat session 表项；nat server 表项与 nat 变换的 session 表项不同，它是全局使能的表项。进行 nat 变换时即使 firewall disable 也没关系，但用到包过滤则必须 enable。**

#### 147. **Portal 特性规格参数：**

AR28,512;  
RPU,1024;  
ERPU,2048

148. 原 65 系列交换机支持 **Salience I、II、III** 交换引擎；H3C 75 系列只支持 **Salience III** 交换引擎；而 OEM 给 3Com 的 7700 系列交换机支持 **Salience I、II** 交换引擎，7750 系列交换机只支持 **Salience III** 交换引擎。

149. 低端交换机有 3 个 **MAC** 地址，不同于路由器，在路由器上每个接口都有 **MAC** 地址。

在低端交换机上，有 3 个 **MAC** 地址：

- (1) **端口的 MAC**：各端口 **MAC** 地址相同。
- (2) **VLAN 虚接口的 MAC**：各虚接口 **MAC** 地址相同。
  - a) 如果是二层交换机，那么虚接口 **MAC**=端口 **MAC**；
  - b) 如果是三层交换机，那么虚接口 **MAC**=端口 **MAC**+1。
- (3) **CPU 的 MAC**：端口 **MAC**+2。

150. 报文在转发过程中，如果是二层转发则源、目的 **MAC** 地址不会改变；如果是三层转发，那么源、目的 **MAC** 地址会改变（源 **MAC** 为当前转发接口的 **MAC**，目的 **MAC** 为下一跳目的的 **MAC**），在这个过程中源、目的的 **IP** 地址是不会改变的，无论是二层转发还是三层转发。

151. 二层与三层的区别是：三层对 **IP** 报文进行处理和转发；对报文的检测属于二层范畴。上 **CPU** 处理的报文并不能说明就是三层处理，只要是协议报文都会上 **CPU** 进行处理，二层协议如 **STP**，**GVRP** 都会上 **CPU** 进行处理。

152. 在 **nat server** 配置中，如果内外网想通过域名访问，方法如下

(1) 内网通过域名访问的命令如下，前提是该域名在公网注册成功（需要注意的是公网 **IP** 地址不能用 **current-interface** 参数代替，目前只有 **nat server** 配置中有该参数）。

[H3C]nat dns-map www.h3c.com 公网 IP 地址 公网端口号

(2) 公网通过注册域名服务后（有的网站提供 **DDNS** 的服务），可以通过域名进

行访问。

**注：**一个公网 IP 地址通过不同端口号映射两个以上 web server 时，在外网访问不同 web server 时需使用端口号加以区别；在内网访问时由于 dns-map 命令有设置端口的参数，所以可以通过各自域名访问不同 web server。

### 153. 配置 PVLAN (isolate-user-vlan) 的注意事项——节约 VLAN ID

- (1) pvlan 不能跟 trunk 口同时配置；
- (2) 上行端口必须添加到 pvlan 中；
- (3) 实现机制：1 个 pvlan 和多个 secondary vlan 相对应，pvlan 包含所有相对应的 secondary vlan 中包含的端口和上行口（不能是 trunk 口），这样上层交换机只需识别下层交换机中的 pvlan 而不必关心 pvlan 中的 secondary vlan。
- (4) Isolate-user-VLAN 和 Secondary VLAN 中必须已经包含了端口。
- (5) Isolate-user-VLAN 中的所有端口都不是 802.1Q 的 trunk 端口，包括与其它交换机相连的 uplink 口。
- (6) 每个 port 的 PVID 就是它所属 Secondary VLAN 的 ID。
- (7) uplink 端口的 PVID 是 Isolate-user-VLAN 的 ID。

**注：**该功能再 S2000、S3026、S3526 上支持，以后的交换机都通过配置 hybrid 口来实现了。一个 Isolate-user-VLAN 对应一个 IP 子网，即同一个 Isolate-user-VLAN 中包含的所有 Secondary VLAN 处在同一个子网中。

### 154. 配置 Super VLAN 的注意事项——节约 IP 地址

支持 Super VLAN 功能的交换机允许在 Super VLAN 上配置一个 IP 地址，而其它 Sub VLAN 通过 ARP 代理借用 Super VLAN 的接口 IP 地址进行三层通信。

- (1) Super VLAN 中不能包含任何端口
- (2) Super VLAN 开启后，ARP proxy 自动开启
- (3) Super VLAN 开启后，对应 VLAN 接口的 ARP proxy 不能关闭
- (4) 建立映射前，Sub VLAN 必须已经包含了端口
- (5) 映射关系一旦建立，不能修改 Sub VLAN 的端口列表

### 155. 当作 MP 捆绑时，在虚接口启用 OSPF，virtual-template 默认 ospf 网络类型为 NBMA，因此必须手工制定邻居。

### 156. 配置 qos 时提示带宽不够的解决办法

- (1) 修改接口可用最大带宽：qos max-bandwidth
- (2) 设备接口可利用的带宽：qos reserved-bandwidth pct

157. **SSH 是基于 TCP 的连接。**
158. **AR18-2X 做 DDNS 时当本地公网地址改变时，不能自动更新。**
159. **一个交换机 A 端口下连另一台交换机 B，该交换机 A 端口的 MAC 表项会学习到交换机 B 所学到的所有 PC 的 MAC；如果将其中的一台 PC 的 MAC 绑定到其他端口，则该 PC 无法正常通信。**
160. **路由器在发出 arp 请求后，就会生成一个 arp 表项，其中 mac 地址为 0，当收到应答后，会用收到的 mac 地址更新表项，但如果没有收到的话该表项会一直保存（直到一段时间后老化）。**

一个正常的arp表项更新如下：（VRP1.74版本下）

ARP\_Resolve :mac address length is 0

ARP: **sending Arp Request**, interface = Ethernet2 :

00 01 08 00 06 04 00 01 00 e0 fc 20 1e 17 0a 99 5b 01 **00 00**  
**00 00 00 00 0a 99 5b 17**

ARP: **Received Arp Reply**, interface = Ethernet2 :

00 01 08 00 06 04 00 02 **00 12 3f 60 4f 8b 0a 99 5b 17** 00 e0  
fc 20 1e 17 0a 99 5b 01

Add or update arp cache:

Inet 10.153.91.23 00-12-3f-60-4f-8b Dynamic Ethernet2

dis arp

Interface	Address	MAC Address	Type
<b>Ethernet2</b>	<b>10.153.91.23</b>	<b>00-12-3f-60-4f-8b</b>	<b>Dynamic</b>
Ethernet2	10.153.91.27	00-11-43-c5-4e-ff	Dynamic
Ethernet2	10.153.91.39	00-05-5d-a0-47-4d	Dynamic
Ethernet2	10.153.91.64	00-11-43-c7-50-a2	Dynamic
Ethernet2	10.153.91.51	00-11-43-c5-2d-75	Dynamic
<b>Ethernet2</b>	<b>10.153.91.132</b>	<b>00-00-00-00-00-00</b>	<b>Dynamic</b>
Ethernet2	10.153.91.52	00-0c-76-0a-17-e5	Dynamic
Ethernet2	10.153.91.40	00-14-2a-9a-4a-82	Dynamic
Ethernet2	10.153.91.20	00-13-46-ec-6f-3c	Dynamic
Ethernet0	10.153.7.93	00-e0-fc-7a-c7-08	Dynamic

在arp表中存在的**Ethernet2 10.153.91.132 00-00-00-00-00-00 Dynamic**这条，路由器只发出去了arp请求，而没有收到应答

ARP\_Resolve :mac address length is 0

ARP: sending Arp Request, interface = Ethernet2 :

00 01 08 00 06 04 00 01 00 e0 fc 20 1e 17 0a 99 5b 01 00 00  
00 00 00 00 0a 99 5b 84

注：在3.4版本中情况类似，不过解析不成功的arp表项显示为incomplete

161. 如果在一个接口上同时配置了包过滤和 NAT，发送数据包的时候先进行包过滤，然后进行 NAT；接收数据包的时候先进行 NAT，然后进行包过滤。

162. 800 问题分为咨询、配置和故障三类。根据问题单处理的不同阶段，将该问题的处理状态从原来所处处理状态变更为“处理中”、“研发处理中”、“已有解决方案”、“处于观察中”、“一般关闭”五种状态之一。

### 163. ARP 表项与 MAC 表项内容

#### (1) ARP 表项

IP 地址	MAC 地址	所属 VLAN	接口	动态学习/静态配置
-------	--------	---------	----	-----------

#### (2) MAC 表项

目的 MAC	所属 VLAN	出接口	老化时间
--------	---------	-----	------

164. 我们的路由器现在不支持 FTP 的被动模式，如果出现在外网无法访问内网映射出去的 FTP 服务器，需要将其“使用被动模式”的选项去掉。

165. 我们的 VRP 和 CMW 使用的是同一个版本文件，只是在启动的时候获取主板上的逻辑信息来判读是 quidway 还是 H3C 品牌，对应显示不同的版本信息。

### 166. 3Com 设备的 3C 编码与设备对应关系

3C17 后为：

100 系列号	——4300 系列
200 系列号	——4400 系列（3C17206 为 S4400SE）
300 系列号	——4200 系列
400 系列号	——3800 系列
500 系列号	——3200 系列
700 系列号（700、701、702、706）	——4900 系列
（707、708、709）	——40x0 系列

3C16 后为： 400 系列号——Baseline 系列  
700 系列号——OfficeConnect 系列  
800 系列号——7700 系列  
900 系列号——3300 系列

## 167. 两台交换机做 VRRP 的说明

心跳线互连口指 switch1——switch2 两台起 vrrp 的交换机之间的互连端口，由于这条链路主要用来传输 vrrp 协议的相关数据，同步两台设备上的 vrrp 信息，故俗称心跳线。

这两台设备上的互连接口需要配置 trunk。

## 168. 3Com 交换机与其他厂商交换机互连说明。

H3C 或 Cisco 有 trunk 概念的交换机与 3Com 产品互连时，当 3Com 交换机级联口以 tagged 的形式存在于 VLAN2、3 而以 untagged 的形式存在于 VLAN1 时，如果对端 trunk 口 permit vlan all 且 pvid 为 1，那么两端的 VLAN1 可以相互通信，如果 pvid 为 2 或 3，那么 3Com 交换机 VLAN1 下所连 PC 就与对端的 VLAN2 或 3 通信了；当 3Com 级联口接收到没有 tag 标记的报文时，如果 3Com 交换机级联口以 untagged 的形式存在与某一 VLAN，那么 3Com 交换机就将该报文发送给该 VLAN，如果 3Com 交换机级联口都是以 tagged 的形式存在于各 VLAN，那么该没有 tag 标记的报文就被丢弃。

## 169. 目前 DMC 功能对于大部分常用网络设备都可以识别，如果遇到部分无法识别的设备，请采用如下方法尝试：

- (1) 在异步口下配置：undo detect dsr-dtr；
- (2) 将该接口 shutdown 后 undo shutdown。

## 170. AR18 系列路由器的 web 网管功能需上传 http.zip 的文件包（不能使用 XModem 方式）；而防火墙无需上传该文件包，因为它是随主机软件一同上传到设备上去的。

## 171. 查看并解决 arp 欺骗病毒的方法

- (1) 网络运行正常时，在 PC 上的 DOS 窗口下运行：arp -a，查看网关 IP 和 MAC 地址；
- (2) 在 DOS 窗口下使用“arp -s 网关 IP 网关 MAC ”命令进行地址绑定；或在 PC 不能上网时，运行“arp -d”命令删除现有 arp 对应关系进行更新。
- (3) 在路由器上进行 arp 的静态 IP 与 MAC 绑定（注意要整个网段全绑定），另外在配置接口发送免费 arp 报文。

172. 我们的路由器缺省允许 **SSH** 登录，但是又没有配置其他 **SSH** 参数。当有试图使用 **SSH** 方式登陆的时候就发现开始连接，然后断开的 **log** 信息。可以使用下面的命令解决这个问题，即禁止 **SSH** 登录。

```
protocol inbound { all | pad | ssh | telnet }
```

该命令缺省形式为 ALL，如不使用 SSH，则可选择需要的登录方式即可，如只用 telnet 为 protocol inbound telnet。

173. **AR18** 系列路由器的以太网启子接口后无法 **ping** 通子接口 IP 地址，只有连接上交换机并映射 **VLAN** 后，才可以 **ping** 通自身设置的 IP 地址。

二层交换机做 trunk 透传多个 vlan 信息，在 AR18-2X（支持划分 vlan 的设备）做子接口不通。

在 AR18-2X 连接交换机的二层接口上必须做 trunk，且要允许多个 vlan 通过，在配置时必须手动指定某些 vlan，不能允许所有 vlan。（如果允许所有 vlan，会只允许 vlan 1）



174. 中低端交换机的 **combo** 复用口需先 **shutdown** 电口，光口才能 **UP**（如有必要需 **undo shutdown** 光口，如 **S5500**）。
175. **AR18-22S-8** 和 **AR18-23S-1** 在配置 **IPSec** 时，本身使用的就是硬件加密卡，无需配置命令 “**ipsec card-proposal**”（也没有该命令）。
176. **IKE** 是 **UDP** 上的应用层协议，是 **IPSec** 的信令协议。
177. 配置 **IPSec** 时若使用接口上的 **sub** 地址建立隧道，必须配置 “**local-address** 从 **IP**”。
178. 在 **GRE overIPSec with OSPF** 的应用中，**GRE** 的作用是：**IPSec** 没有逻辑或物理接口，**OSPF** 需要接口做路由，只能通过 **GRE** 进行封装。
179. 在进行 **L2TP** 的配置中，当内网通过外网口进行 **nat** 变换时，无需在 **nat** 变换的 **acl** 中 **deny** 掉 **I2tp** 的数据流，因为数据是将 **VT** 模板接口作为访问的下一跳，而 **nat** 变换是应用在物理接口上的，实际不会对 **L2TP** 的流量产生影响。
180. 配置 **IPSec** 野蛮模式时，中心与分支的私网网段应在不同网段，因为若是相同网段的报文 **PC** 不会将其送到内网网关。此外，当存在多个分支时，应配置多个 **peer**，之后匹配相同模板名不同节点号进行区分（新版本）或使用不同的模板（老版本建议使用该方式）。其他 **VPN** 技术各私网 **IP** 也应该在不同网段。
181. **IPSec** 主模式和野蛮模式的区别
- （1）交换的消息：主模式 6 个，野蛮模式 3 个。
- （2）NAT 支持：
- ①、pre-shared key 认证：主模式不支持 NAT；野蛮模式支持 NAT。

②、证书认证：两种模式都支持 NAT

(3) 对等体标识：

①、主模式：只能采用 IP 识别。

②、可使用 IP 或 Name 方式。

(4) 协商能力：主模式>野蛮模式。

## 182. DVPN 隧道的建立基于 UDP 端口 9010。

## 183. AR18-2X 对配置的要求非常高，可能因为少敲了几个命令行就导致掉线的。



AR18-2X最新配置

## 184. 对 Qos 队列的理解。

每个主接口都只有一个队列，没有配置 qos 时的队列是 fifo，配置了以后就成了所配置的队列。本来即使创建了子接口，但是队列还是只有一个，即主接口的队列，所以在这种情况下各个子接口之间的带宽是可以互相抢占的；但是在子接口上配置嵌套策略以后，相当于另外创建了一个队列，在这种情况下，配置了嵌套策略的子接口就独占了这部分的带宽。

还有就是主接口和子接口配置 qos 的区别，是这样的，qos 从网络层次上来说可以分为3层：

(1) 3 层 qos，包括 car、gts。对 3 层的 qos 来说，主接口和子接口是分开实现的，也就是说互不相关，各管各的。

(2) 2 层 qos，包括各种队列。子接口上是没有直接实现 2 层 qos 的，如果要使用的话必须通过嵌套策略来实现，但是一般不建议这样做。如果配置嵌套策略的话，必须先在父策略中配置 lr，再在子策略中配置队列。配置嵌套策略以后，会在子接口上创建一个新的队列，该队列与原来主接口的队列是独立的，也就是说这部分的带宽是这个子接口独占的。它并没有接口带宽，只是做了个 LR。速度是靠 LR cir 的配置控制的。在主接口上能不能发出去是没有保证的。

(3) 3 层 QOS 是在 3 层和 2 层之间实现的。LR 也是 2 层的，是在 2 层和物理层之间实现的。就是已经打了链路层头后，再做 LR。我们一般不说一层 QOS。

如下，子接口不能直接配置队列和 lr：

[R1-Ethernet0/0/1.2]qos ?

apply Apply specific QoS policy on interface

car Apply CAR(Committed Access Rate) policy on interface

gts Apply GTS(Generic Traffic Shaping) policy on interface

```
[R1-Ethernet0/0/1.2]int e 0/0/1
```

```
[R1-Ethernet0/0/1]qos ?
```

apply	Apply specific QoS policy on interface
car	Apply CAR(Committed Access Rate) policy on interface
cq	Apply CQ(Custom Queuing) on interface
fifo	Apply FIFO(First In First Out) queuing on interface
gts	Apply GTS(Generic Traffic Shaping) policy on interface
lr	Apply LR(Line Rate) policy on physical interface
max-bandwidth	Set bandwidth for QoS calculation
pq	Apply PQ(Priority Queuing) on interface
reserved-bandwidth	Max reserved bandwidth of the interface for QoS
rtpq	Apply RTP(Realtime Transport Protocol) queuing on interface
wfq	Apply WFQ(Weighted Fair Queuing) on interface
wred	Apply WRED(Weighted Random Early Detect) on interface

```
[R1-Ethernet0/0/1]
```

## 185. **MSR(8048)路由器 Comware 软件基本版(BI)与标准版(SI)相关说明**

**SI 版本即标准版本**，具备产品手册、操作手册、命令手册提到的全系列功能，因此也称为主线版本，即 MSR 路由器原有版本在 CMW 5.20 B1203 之后统称为 SI 的版本。以 MSR30-20 为例，如下操作可以根据命令执行结果中的红粗字体判断当前使用的是否为 SI 版本：

```
<H3C>display version
```

```
H3C Comware Platform Software
```

```
Comware software, Version 5.20, Beta 1203, Standard
```

```
Copyright(c) 2004-2006 Hangzhou Huawei-3Com Technology Co., Ltd. All rights reserved.
```

```
H3C MSR20-40 uptime is 0 week, 0 day, 6 hours, 27 minutes
```

```
Last reboot 2007/01/08 10:00:02
```

```
System returned to ROM By Power-up.
```

**BI 版本则被称为分支版本**，在 CMW 5.20 B1203 后正式推出。还是以 MSR20-40 为例，如下操作可以根据命令执行结果中的红粗字体判断当前所使用版本是否为 BI 版本：

<H3C>display version

H3C Comware Platform Software

Comware software, Version 5.20, Beta 1203, Basic

Copyright(c) 2004-2006 Hangzhou Huawei-3Com Technology Co., Ltd. All rights reserved.

H3C MSR20-40 uptime is 0 week, 0 day, 0 hour, 8 minutes

Last reboot 2007/01/08 16:35:25

System returned to ROM By <Reboot> Command.

### SI、BI 版本功能的具体差异

BI 版本和 SI 版本相比，许多功能特性被裁减，下面一一列举 BI 版本不支持的功能：

- (1) 广域网——HDLC
- (2) 广域网——DLSW
- (3) 广域网——QSIG
- (4) 广域网——PPPoFR
- (5) 交换特性——LACP
- (6) 交换特性——GARP
- (7) 交换特性——GVRP
- (8) 交换特性——PoE (Power over Ethernet, 以太网供电)
- (9) IP——DHCP Relay
- (10) IP——UDP Helper
- (11) IP——DHCP Snoop
- (12) IP——IPv6 过渡技术 (包括 NATPT 和各种隧道技术)，BI 版本只支持 IPv6 基本功能如 ND 和静态路由协议
- (13) 路由协议——ISIS (包括 IPv4 和 IPv6, 整体裁减)
- (14) 路由协议——OSPFv3 (OSPF for IPv6)
- (15) 路由协议——RIPng (RIP for IPv6)
- (16) 路由协议——BGP4+ (BGP for IPv6)
- (17) 路由协议——IPv6 组播路由协议 (BI 版本支持 IPv4 组播路由协议)
- (18) 路由协议——IPX
- (19) MPLS——整体被裁，BI 版本整体不支持任何 MPLS 功能
- (20) 安全——MAC 认证
- (21) 安全——IKE
- (22) 安全——IPSec, BI 版本不支持任何 IPSec 功能
- (23) 安全——PAM (Port to Application Map, 端口与应用映射)
- (24) 安全——SSL (Secure Socket Layer, 安全套接字层)
- (25) 语音——整体被裁，BI 版本整体不支持任何语音功能
- (26) 系统管理——AutoConfig
- (27) 其他——BI 版本不需要进行 License 注册，而 SI 版本在 CMW 5.2 B1203P01 版本及后续版本是必须要进行 License 注册的，否则只有 1 个月的使用期限，由于 BI 版本不需注册，故没有这个限制。

**注：**未列在上述 27 条，而出现在产品手册、操作手册或命令手册的其余功能，BI 版本均支持。

### 如何进行 SI 版本 License 注册

以下以 MSR30-20 为例，

#### (1) 标准版 License 注册

使用正确的授权序列号注册，在用户视图下输入以下命令：

```
<H3C>license register XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
Register successfully!
```

**（注：**“XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX”为随设备一同购买的产品授权序列号，该授权序列号会随设备以信封的形式发送给客户）。

**注意：**如果不进行注册，该软件只能试用一个月，超过试用期后设备会每隔 30 分钟自动重启一次！

注册失败 3 次后的提示信息显示如下：

```
<H3C>license register XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
Failed to register three times, reboot the system to register again.
```

#### (2) 查看注册结果：

display license 命令显示信息

当软件未注册时， 显示信息如下：

```
<H3C>display license
The software has not been registered
```

当软件已注册时， 显示信息如下：

```
<H3C>display license
Software license information
-----
Serial Number: *****_*****_*****_*****_*****_*****_*****
Register Date: 2007-2-6 16:45:22
Trade Code   : 213130A15D0061000001
```

**注：**Serial Number 即为已经注册成功的授权序列号

### 186. 只有 GRE 支持封装组播报文。

### 187. H3C AR28 系列路由器与 Quidway AR28 系列路由器是两个不同品牌的 的路由器，虽然功能特性一致，但硬件构成和软件逻辑有一些区别。

比如 H3C AR28 的 BOOTROM 版本和 Quidway AR28 的则不通用，两个品牌路由器的 BOOTROM 版本和主机软件版本也是各自独立归档发布的，不要混用。

H3C AR28 系列路由器的配套 BOOTROM 版本为 9.18 及更高版本，配套主机软件版本为 H3C CMW3.40-0109P08 及更高版本。严禁使用 Quidway 品牌的 BOOTROM 9.17 及更低版本升级 H3C AR28 系列路由器，这样会导致升级后系统无法正常启动，甚至不能进入 BOOT 菜单。另外 H3C AR28 的 BOOTROM 芯片是焊接在主板上，不能通过芯片起拔器取

出，这点与 Quidway AR28 不同（Quidway AR28 的 BOOTROM 芯片是嵌入主板槽位上，可以取出烧片）。如果出现误升级 Quidway 配套的 BOOTROM 导致 H3C AR28 路由器系统无法启动，只能返修设备了。

需要强调的是，H3C AR28 与 Quidway AR28 的 BOOTROM 版本是分别归档的，请大家升级时一定注意版本配套关系，切记不要混用。另外由于 AR46 的 BOOTROM 随主机软件版本自动升级，因此不需区别 H3C 和 Quidway 品牌，只要保证主机软件版本配套即可。

**188. 当用户需要现场支持、返修时，我们把客户信息反馈给热线和备件让她们给客户回电，不要让客户多次拨打 800 电话！！**

**189. VRP1.74 版本配置的 sub 地址不能与主 IP 同网段；VRP3.4 主从 IP 可同网段。**

**190. 低端路由器上只有两个物理串口，但执行 disp cur 后却显示有 S0，S1 和 S2 三个串口**

之所以会出现这个现象，是因为有些低端路由器将 AUX 接口显示为一个串口，如 R2509 上只有串口 0、1，但执行 disp cur 后显示有串口 0、1、2，其中 Serial 2 口就是 AUX 接口。

**191. 中低端路由器对于 CF 卡的支持**

目前只有 AR46 ERPU 板有 CF 插槽

对于 MSR 产品，所有型号都有 CF 插槽，CF 卡作为必备的附件（版本和配置都放在 CF 卡中），所有的 20、30、50 都可以支持。

192. **8040(AR28、AR46 路由器)和 8043(AR18 路由器)均不支持 802.1x 认证；8048(MSR 系列路由器)交换板支持该功能**

193. **所有的 SA 模块和设备自带的串口都支持同异步模式，并可以通过命令进行修改，只有 R2620/R2621 的串口比较特殊：只支持同步模式。**

194. **AR 系列路由器与 MSR 系列路由器 telnet-server 功能实现的区别**

AR 系列路由器 telnet-server 服务缺省是使能的，并且同时允许多个用户进入系统视图配置，包括 console、telnet 登录等；

MSR 系列路由器 telnet-server 服务缺省是关闭的，需要配置 telnet-server enable（系统视图）使能；另外缺省情况下只允许一个用户在系统视图下进行配置，如果此时已有一个用户通过 console 口登录设备操作，那么其它用户就无法通过 telnet 登录操作了，可以使用命令 configure-user count 设置并发配置用户数，不同型号的设备支持的取值范围不同，请以设备的实际情况为准。

195. **AR18-2X 如何关闭掉 WWW 管理服务**

[Quidway]ip http shutdown

196. **AR18 系列路由器如何在 bootrom 菜单下看配置文件**

bootrom 菜单下 ctrl+p 可看配置文件。

197. **什么是 MSCA 和 MPUF**

MPUF 是 MSR50 系列的主控板，是一个完整的主机系统，MSCA 是 MSR50 系列的后主控板，主要用于提供 VPM、VCPM 和 ESM0、ESM1 扩展插槽。MSR50 只需要 MPUF 就可以正常启动，如果需要扩展内置 VPM、内置 VCPM 或者 SNDE/ANDE 等模块，必须购置 MSCA

198. **VPM 和 VCPM 的作用是什么**

VPM(Voice Processing Module)语音处理模块主要由 DSP 组成，其主要作用是进行语音数据的编解码处理、EC 回声消除、CNG 产生舒适噪音。

VCPM(Voice Co-Processing Module)语音协处理模块起桥梁作用，主要有：将 SIC 卡或 MIM/FIC 卡的 local bus 总线转换为 PCI 总线，进行 TDM 链路切换，提供分配 TDM 时钟源。

**注：**基于系统的结构，这两个模块在支持语音业务的时候需要同时配，相互协同工作完成语音业务(无论将要插在主板上还是插到语音模块上)。

## 199. NE 系列路由器 V5 版本的 paf 和 license 文件说明

NE 系列高端路由器从 V5 版本开始，新增 paf 和 license 两个文件，设备所使用的 paf&license 文件必须与软件版本配套才能正常工作。其中 paf 文件定义了产品能够支持的功能规格，而 license 文件则定义了用户可以使用的功能规格。通过这两个文件可以实现组件的功能裁剪以及对产品的功能进行规格性定制，例如：设备可支持的用户数量、路由数量等等。

对于 NE 系列高端路由器，paf 与 license 文件与软件版本一起打包发布，使用时必须将这两个文件传到设备的 flash 中，并确保两个文件的名字不发生改变。部分软件版本提供多套 paf 和 license 文件与之配合工作，例如：NE40 有 IPv6 Enable 和 IPv6 Disable 两套 paf&license 文件，对于没有使用 IPv6 业务的局点建议使用 IPv6 Disable 的 paf&license 文件；对于需要开通 IPv6 业务的局点则必须使用 IPv6 Enable 的 paf 和 license 文件。

## 200. 如何查看设备的 CPU 占用率

```
VRP1.4 (router-config)#h-b cpu
VRP1.6(router-config)#h-cpload
VRP 1.74:display process cpu 或 disp system cpu
VRP3.3:对于 VRP3.3 必需在隐含模式下打开 cpu 占用率检测开关
_h 进入隐含模式,set cpu-usage monitor 打开 cpu 占用率检测开关后 disp cpu
VRP3.4:display cpu
```

## 201. FE 单板的芯片型号区分

FE 单板有三种芯片 21143, 82559, 82551  
dis ver 中  
[SLOT 0] 2FE (Hardware)2.1, (Driver)2.0, (Cpld)0.0  
驱动为 1.x 的为 21143  
驱动为 2.x 的为 82559  
驱动为 3.x 的为 82551

## 202. BOM 编码信息

常见的条码有：

- 1、02 开头，长度为 16 位。如条码 023855103A000300。物料编码为：03023855，第 8～10 位“03A”表示 2003 年 10 月份生产发货。
- 2、03 开头，长度为 16 位。如条码 0340411024000542，物料编码为：03034041，第 8～10 位“024”表示 2002 年 4 月生产发货。
- 3、21 开头，长度为 20 位，如条码 210231A5060055000008，可以知道物料的编码为 0231A506。第 12～14 位“055”表示 2005 年 5 月份生产。000008 表示序号。



## 203. 板卡的高度有 0.5U、1U

目前大多数模块的高度是 1/2U，及 AR 28 系列产品上的 SIC 和 MIM 卡槽位的高度，但有部分 MIM 或 FIC 单板模块的高度是 1U，这样 AR 28 系列产品的一个 MIM 插槽就不能容纳这种单板，占 1U 高度的单板有：

模块编码	模块型号	备注
02311171	RT-E1VI	
02311486	RT-T1VI	
02311217	RT-12AM	原 16AS 模块占 1/2U 高度，只需一个 MIM 插槽
0231A347	RT-16LS	

对于 AR 46 路由器来说，其每一个 FIC 插槽就占 1U 高度，即一个 FIC 插槽可支持一块上述占 1U 高度的单板的安装。

目前 SIC 卡还没有占 1U 高度的。

## 204. 关于 SIC 卡以太网接口模块的使用

R2611 和 AR2811 不能用 RT-SIC-1FEA 和 RT-SIC-1ETH 模块

R2610 和 AR2810 只能选择一块 RT-SIC-1FEA 或 RT-SIC-1ETH 模块(且只能插在固定的 SIC 卡槽位，一般为两个 SIC 槽位中右侧编号小的槽位)

R1760 和 AR2809B 及 AR2809 只能选择一块 RT-SIC-1FEA 或 RT-SIC-1ETH 模块(且只能插在固定的 SIC 卡槽位，一般为两个 SIC 槽位中右侧编号小的槽位)

## 205. AR46 上 ERPU 与 RPU 主控板的区别

主控板主要完成协议处理、低速数据包转发、接口控制、故障检测等功能，是产品的核心部分。另外，主控板还提供硬件复位按钮 RESET。

ERPU 主控板相比于 RPU，多了一个 CF 卡(Compact Flash)，多了 3 个光电复用口(若作电口使用，则无法作为光口使用；反之亦然。)，内部增加了一个加密卡，提高了 IPSEC 的加密性能。

两者具体规格参数如下：

主控板(RPU)规格属性表

项目	属性
接口	2 个 10/100M 以太网口 1 个 AUX 口 1 个配置口
处理器	733MHz
Boot ROM	1024KB
SDRAM	缺省：256MB 最大：512MB
Flash	32MB

主控板(ERPU)规格属性表

项目	属性
固定接口	3 个 10/100/1000M 以太网口(提供光口和电口两种连接器) 1 个 AUX 口 1 个配置口 CF 卡插槽(CF 卡选配)
处理器	700MHz
Boot ROM	512KB
内存	512MB 或 1024MB
Flash	64MB

主控板(ERPU(H))规格属性表

项目	属性
固定接口	2 个 10/100/1000M 以太网电接口 1 个 10/100/1000M 以太网口(提供光口和电口两种连接器) 1 个 AUX 口 1 个配置口 CF 卡插槽(CF 卡选配)
处理器	700MHz
Boot ROM	512KB
NVRAM	512KB
DDR SDRAM	512MB
Flash	64MB

## 206. 中低端路由器板卡使用注意事项

AR 路由器: B02 版本(VRP3.4 001X)不支持 FCM 模块; B03(VRP3.4 010X)版本支持 FCM 模块, 且支持 AM 模块做 POS 接入。

VRP1.74 平台上使用的板卡绝大部分都能够直接拿到 VRP3.4 平台上来用, 但 RT-8LSA、RT-2S1B、RT-2ADSL 及 RT-2ADSL-I 除外。

SIC-1FEA 和 SIC-1ETH 两种小卡只能在 AR28-09/AR28-10/AR2809B/R1760/R2610 上使用, 并且只能选择使用一块, 插 SIC 插槽 0 槽位。AR28-11/R2611 不支持。

RT-4BSE 只能在 AR2830/31/40/80 上使用, 且是 B03 版本支持。

VRP1.74 0119P01 以前版本不支持 SIC-1SAE 小卡, VRP3.4 均支持 SIC-1SAE 小卡。

B03 版本支持 6/12AME 模块, B02 版本虽然识别这两种模块, 但 modem 不能正常响应。

## 207. 关于硬件流控和软件流控

当双方的速率不匹配时, 若速率慢的一方缓冲区已满, 则其可以启动流控, 通知速率快的一方停止发送; 待其处理完毕后, 再通知速率快的一方继续发送。

硬件流控: 双方通过硬件上的一些电平的变化进行流控功能, 一般是通过 CTS 和 RTS 信号。硬件流控的配置方式为 flowcontrol hardware

软件流控：当双方连接采用 3 线时，因 DSR/DTR/CTS/RTS 均没有连接，所以

(1) 要配置 `undo detect dsr-dtr`，该命令的作用是不检测 dsr/dtr 信号，而端口自动 up；否则，端口检测到 dsr/dtr 信号后才 up

(2) 要配置 `flowcontrol software`，即软件流控，软件流控是通过一些特殊字符进行流控的。当速率慢的一方缓冲区已满，则向对方发送 0x13 (ctrl-q)，通知速率快的一方停止发送；待其处理完毕后，再发送 0x11(ctrl-s)通知速率快的一方继续发送。还要注意的，若用户数据中有 0x11 或 0x13 则，配置软件流控后，则和流控字符冲突，造成这 2 个字符被当做流控字符，不会发给 unix,可能某些操作不能成功，此事可以打开调试开关，看是否有这 2 个字符，再和用户解释，0x11 和 0x13 是国际标准的流控字符。

## 208. ISDN 非常有用的命令

### (1) 中低端路由器采用 E1VI 模块，DSS1 信令与 PBX 对接不成功时，调试报文出现 **Invalid information element contents, Message not compatible with call state** 的解决办法

系统出现了兼容性问题。应观察 PBX 侧发来的 setup 消息和我司路由器发的 setup 消息中的 low\_l, h\_lay 信息。默认情况下，我司两个都会发！如果 PBX 省略了，就会出现兼容性问题，需要在我司路由器与 PBX 相连的接口上通过配置：**isdn ignore hlc** 或者 **isdn ignore llc** 解决。

### (2) 中低端路由器采用 E1VI，DSS1 信令与 PBX 对接，PBX 下连电话呼出时过 4s 就挂断，调试报文显示：**ISDN L3 timer T313 timeout** 问题的解决方法

对于 PBX 主动发起的连接，连接建立后我司路由器默认情况下会发送 Connect request, 过了 4s 没有收到 Connect ACK 就拆线。出现上述问题就在于 PBX 没有回送 Connect ACK, 解决方法是在与 PBX 相连的接口下配置：**isdn ignore connect-ack**。Isdn ignore connect-ack 命令用于配置路由器的 ISDN 协议在发送了 CONNECT request 消息之后无需等待 CONNECT ACK 消息，直接切换到 ACTIVE 状态，并开始数据和语音业务的通信。

### (3) 在被叫的 Bri 接口下配置

**isdn ignore callednum**（我们做为被叫端时不发送 SETUP\_ACK，解决部分 ISDN 交换机不识别 SETUP\_ACK 的问题）

**undo isdn waitconnectack**（命令用来设置路由器不等待 CONNECTACK 消息而直接进入 ACTIVE 状态，并开始数据和语音业务的通信，解决部分交换机不发送 CONNECTACK 的问题）

## 209. 中低端路由器 tcp mss 的实现原理

PC1(192.168.0.1)——Router——Internet——www server(238.135.1.1)

建立 tcp 连接的两端在三次握手时会协商 tcp mss 大小，具体如下：

pc1 发出 syn 报文，其中 option 选项填充的 mss 字段一般为 1460，同样 www server 收到 syn 报文后，会发送 syn+ack 报文应答，option 选项填充的 mss 字段也为 1460；协商双方会比较 syn 和 syn+ack 报文中 mss 字段大小，选择较小的 mss 作为发送 tcp 分片的大小。通过比较，协商双方的 tcp mss 都是 1460。

对于涉及 mpls l3vpn、pppoe+nat、ipsec、l2tp、gre 等组网，通常由于报文太大需要分片，一般可以通过设置 tcp mss 解决。

### 针对上例说明 tcp mss 如何实现

假设在路由器内网口配置 tcp mss 1200

路由器收到 www server 的 syn+ack 报文时会修改 option 选项中的 mss 字段为 1200, 然后再转发给 PC1, PC1 收到报文后认为对端的 tcp mss 为 1200, 这样 PC1 发送资料给 www server 时会以 1200 作为分片大小; 但路由器修改 tcp mss 为 1200 的操作 www server 是不知道的, 因此 www server 还会以 1460 作为分片大小发送报文。

假设再路由器外网口配置 tcp mss 1200

路由器收到 PC1 的 syn 报文时会修改 option 选项中的 mss 字段为 1200, 然后再转发给 www server, 同样 www server 发送资料给 PC1 时会以 1200 作为分片大小; 同样 PC1 不知道路由器修改 tcp mss 为 1200, 因为 PC1 还会以 1460 作为分片大小发送报文。

因此在实现双向大包传输时需要在内外网同时修改 tcp mss

综上所述: 在路由器接口上配置的 tcp mss 命令仅对出接口方向的 syn 报文和 syn+ack 报文有效, 对于入接口方向的 syn 和 syn+ack 报文无效。

## 210. nat server 映射比路由器本地服务优先

在公网口作 nat server 映射:

```
[eth1/1] nat server protocol tcp global 202.60.229.238 23 inside 192.168.2.10 telnet
```

因 nat server 映射比路由器本地服务优先, 公网口的 telnet 被映射到内网。

如果同时需要公网口 telnet 到路由器, 可以更换映射。

## 211. S3900 和 S5600 设备在 Bootrom 中选择跳过配置启动后, 会在每次启动后都跳过配置, 要想解决需再次进入 Bootrom 菜单选择该选项后输入 “No”。

如果选择了跳过配置启动, 会在启动过程中看到提示, 如下:

```
Starting at 0x80020000...
```

```
Initialize:
```

```
LSHILTSU..... OK!
```

```
SDRAM fast selftest..... OK!
```

```
Flash fast selftest..... OK!
```

```
CPLD selftest..... OK!
```

```
Switch chip selftest..... OK!
```

```
PHY selftest..... OK!
```

```
Please check leds.....FINISHED!
```

```
Startup configuration is skipped.
```

```
User interface aux1 is available.
```

```
Press ENTER to get started.
```

```
<H3C>
```

## 212. ARP 静态绑定的三种方式

(1) arp static: 需全网段绑定才能防治 ARP 病毒, 否则 PC 更改 IP 后, 路由器仍然可以动态学习到新的 ip 和 mac 映射关系, 该 pc 仍然可以上网。

(2) arp fixup: 该命令是将动态学习到的 arp 表项全部固化, 即变为静态 arp 表项不会老化。

(3) arp fixed ip mac: 该命令是将 mac 和 ip 进行一一对应, 并固化为静态 arp 表项。

注:

后两条命令与第一条命令的区别是无需全网绑定就可实现防治 ARP 病毒的功能。

## 213. AR28/AR46 系列路由器 FCM 单板在线升级

B04 版本和 B05 版本升级 FCM 的唯一区别之处, B04 版本下需要进入隐含模式, 而 B05 版本只需在系统视图下配置即可

## 214. AR18 系列路由器对于 ARP 欺骗病毒的防治命令说明

(1) ARP 静态绑定: 需全网段绑定才能防治 ARP 病毒, 否则 PC 更改 IP 后, 路由器仍然可以动态学习到新的 ip 和 mac 映射关系, 从而使该 pc 受到影响。

(2) 对于使用 “arp fixed ip-address mac-address” 命令添加的 IP 和 MAC 映射关系, 当收到 ARP 欺骗病毒攻击时, 通过查询已配置的固化表项, 不会受到病毒的影响; 对于新加入到网络中的 PC 通过动态 ARP 也是可以正常通信的, 但如果受到 ARP 欺骗病毒的攻击, 通信会受到影响, 解决的办法就是将该新加入 PC 的 ip 和 mac 进行固化。

(3) 使用 “arp fixup” 命令的作用是将当前动态学习到的 arp 和 mac 映射关系固化, 即转变为静态 ARP 表项, 那么转化后相关的主机不会受到病毒的影响; 对于新加入到网络中的 PC 通过动态 ARP 学习也是可以正常通信的, 但如果受到 ARP 欺骗病毒的攻击, 通信会受到影响, 解决的办法就是再运行一下该命令, 即将当前的动态表项继续固化。

## 215. 交换机防 ARP 攻击命令说明

### (1) DHCP Server 动态分配地址的典型配置

```
#
vlan 1
  arp detection enable
#
interface Vlan-interface1
  ip address 1.1.1.1 255.0.0.0
#
interface Ethernet1/0/3 （连接 DHCP Server 的接口）
  dhcp-snooping trust
  ip source static binding ip-address 1.1.1.10 mac-address 0000-0000-0002 （若想 ping 通 DHCP Server, 需绑定该 Server 的 IP 和 MAC） #
  dhcp-snooping
#
```

## (2) 手工指定 PC 的 IP 地址的典型配置

```
#
vlan 1
    arp detection enable
#
interface Vlan-interface1
    ip address 1.1.1.1 255.0.0.0
#
interface Ethernet1/0/1 (连接 PC 的接口)
    ip source static binding ip-address 1.1.1.2 mac-address 0000-0000-0002
#
dhcp-snooping
#
```

## (3) 注意事项

- ①、在“手工指定 IP 地址的典型配置”中，无需配置“dhcp-snooping trust”。
- ②、如果 DHCP Server 和 ARP 防攻击功能在同一台设备上开启，那么下连 PC 无法 ping 通接口地址池所在 VLAN 虚接口的 IP 地址，如果开启全局地址池，那么下连 PC 无法 ping 通该设备上和上层设备的虚接口 IP 地址。

## 216. 交换机上的 dhcp-snooping 和 dhcp relay 不能同时启用。

- (1) DHCP Relay 是三层的功能，DHCP Snooping 是二层的功能，DHCP Relay 对 DHCP 报文作三层转发，DHCP Snooping 对 DHCP 报文作二层透传，无法同时使用；
- (2) DHCP Relay 和 DHCP Snooping 对涉及对表项进行记录，同时提供给 1X 认证模块使用，两个功能同时使用，则 1X 功能也会混乱。

## 217. 对于 ARP Spoof 病毒所进行攻击的说明

PC1 要与 PC3 进行通信，它会发送 arp request 确认 PC3 的 mac 地址，当攻击者 PC2 先于 PC3 收到该 arp 请求报文后，它会以更快的速度和频率向 PC1 发送 arp 应答，虽然 PC3 也会给 PC1 回应 ARP 应答，但由于 PC2 的发送频率更快（毕竟是病毒，不快不勤的发送错包，达不到破坏的目的），所以 PC1 与 PC3 的通信现象是时通时断或根本无法通信。

## 218. 免费 arp 报文发送的目的有两个

- (1) 确认网络中身份，查看是否有与自己 IP 相冲突的地址；
- (2) 同时更新内网 PC 关于原有的 IP 与 MAC 映射关系。

## 219. ARP 工作原理

PC1 如果想要和 PC2 进行通信，那么 PC1 在将报文发送给 PC2 前，会把自己的 IP 地址与目的地的 IP 地址比较，主要是采用 PC 上所配置的子网掩码来确

定目的站是否与自己在同一子网内。若两个站点不在同一子网内，则 PC1 就会向"缺省网关"发出 ARP 报文，而"缺省网关"的 IP 地址已经在主机上进行设置了。这里我们假设两台 PC 都在同一子网内，通常 PC1 在发送一个 ip 包之前，它要到自己的 ARP 缓存表中寻找是否有目标主机的 IP 地址，如果找到了，也就知道了目标主机的 MAC 地址，然后直接发送；如果没有找到，那么 PC1 就会发送一个 ARP 广播包目标 MAC 地址是“FF.FF.FF.FF.FF.FF”，这表示向同一网段内的所有主机发出这样的询问：PC2 的 MAC 地址是什么？在这个广播报文的封装中，目的地的 MAC 地址段填充的是全“0”字符。当 PC2 收到这个广播报文后，它发现其中的目的 IP 地址与自己的 IP 地址一致，于是就以单播的形式发送 ARP 应答报文，意思就是说我就是 PC2，我的 MAC 地址是这个，我们从这个应答报文中填充的源 MAC 地址段可以看到，PC2 已经将自己的 MAC 封装进去了。PC1 一旦收到这个应答报文，就会将 PC2 的 IP 和 MAC 映射关系保存在 ARP 表项中。

我们可以概括出 ARP 的交互过程大致分为 3 步：

第一，PC1 broadcast a message “如果你是 PC2 的 IP 地址，则请你告诉我，你的 MAC 地址。”

第二，收到广播消息的主机，如果发现被请求的 IP 地址与本机的 IP 地址相同，则响应一个回答报文。

第三，收到广播消息的主机都更新关于发送广播消息的主机的 ARP 缓存。

## 220. 使用 route-policy 将路由进行路由过滤时应注意

```
route-policy 1 deny node 10
  if-match acl 3000
route-policy 1 permit node 20
```

由于我们需要过滤少数几条路由，因此 route-policy 的节点 10 为 deny，节点 20 为 permit（**如果没有配置节点 20，支配节点 10 那么其他路由都会被拒绝掉**）。

## 221. H3C 无线全系列产品



H3C无线全系列产品  
.wmf



222. **Nat 变换使用的 ACL 可以是高级访问控制列表,rule 的配置可以精确指定到端口。**

## 223. 判断 AR 系列路由器串口是否损坏的方法

前提条件：路由器能够正常启动；

步骤：在上电前在串口上连接一根 V35 电缆；DCE/DTE 均可（最好是 DCE，用万用表测试方便）；

上电后等待路由器正常启动完成；

将万用表打在直流电压档，然后黑色表笔连接 V35 电缆的 B 针（孔）；红色表笔连接 K 针（孔），测试 K 针的电压；

如果读数在-5V~-9v 那么这个串口肯定是没有损坏的；

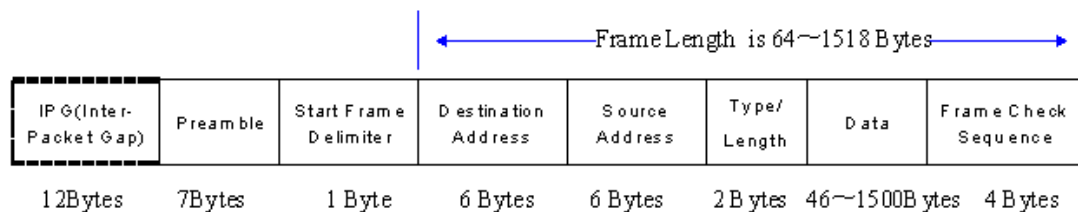
如果读数不在这个区间，那么极有可能是损坏的；

实验室验证了一把，测出的值在-7.4 左右，串口正常。

该实验方法适用于通过软件方法无法确认串口是否正常的情况下。

## 224. 线速转发指标计算方法

首先，我们要了解以太网帧结构，如下图所示。



根据 Ethernet 的 CSMA/CD 的工作原理，报文在发送之前，要先侦听一段时间，如果在这段时间内线路空闲，则可以发送。这段时间就是帧间隙(IPG Inter-Packet Gap)，通常为 96bit-time。接下来是以太网帧结构中的 8 个字节的前导码，其中 7 个字节(Preamble)为 AA(其二进制形式为 01010101)用于与接收端同步，第 8 个字节(StartFrame Delimiter)为 AB(帧定界符)，用于定界，标明从现在开始后面的内容真正的是以太网帧了。

因此，对于长度为 64 字节的以太网帧，其实际长度应该是

$$(7+1+64) \times 8 + 96 = 672 \text{ bit/ Packet}$$

以 100M 端口线速转发为例，100M 就是 1 秒钟 100M bits 的流量，一个 64 字节的以太网帧长度是 672bits，那么 1 秒钟有多少个 64 字节的以太网帧被转发呢？

$$100\text{M}/672 = 148810 \text{ pps (Packet Per Second)}$$



## 225. 交换机中广播风暴抑制比的说明

芯片提供按 PPS 方式按端口对广播报文（包括广播报文，未知单播和未知多播报文）进行限速，超过设定上限则丢弃。

百分比方式在设计上假定所有进入统计的报文都为 64 字节换算成 PPS 方式。比如，10% 限定，那么对于百兆端口为 10M 流量，对应 64 字节的报文（**包括前导码 8 字节**）为 14881 个。那么寄存器中的门限实际为限定 14881 个报文。

由于这种设计方式，导致百分比进行广播抑制不准确，越是长包越不准确。请采用 PPS 方式。

## 226. V/R/B/D 版本号说明

**V 版本**是用来区分一组市场定位不同或开发平台不兼容的主版本，以下两种情况必须形成新的 V 版本。

（1）产品市场定位的变化导致了产品特性的明显变化。

（2）变化的产品平台与原有平台不兼容。如 S3552V100R001 和 S3552V200R001，前者基于平台软件 PLAT R003，后者基于平台软件 COMWAREV300R001。

V 版本与硬件款型是相对应的，即不同的 V 版本产品不能相互升级。如 S3526（S3526V100R001）不能加载 S3526V200R001 软件。

**R 版本**是 V 版本的子版本，当有软件特性更新或新增单板时，形成新的 R 版本。

V 版本和 R 版本的区别在于 V 版本对应硬件差异（通常是交换芯片不同），而 R 版本只是软件特性上的不同。

**B 版本**是按 Build 划分的，一个 Build 就是一个可验证的模块。按照系统设计原则对耦合性小的模块进行划分，新增模块对原有系统的稳定性不会产生影响。

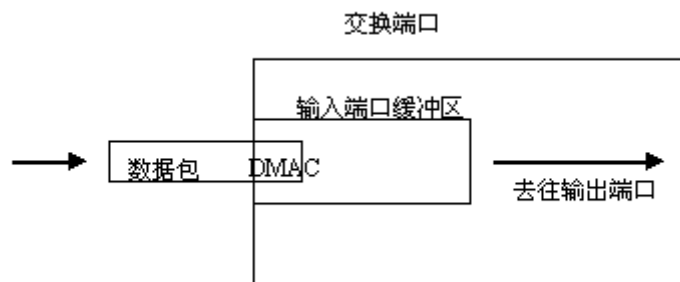
**D 版本**是按合入问题单滚动，后一个版本比前一个版本更稳定。一般情况下，D 版本间不允许有大特性的不同。

V/R/B/D 号是公司内部的版本号，研发人员接触的较多，而用服和市场人员反馈问题一般是用版本的流水号，如 Release 0010，版本流水号唯一对应内部的 V/R/B/D 号。

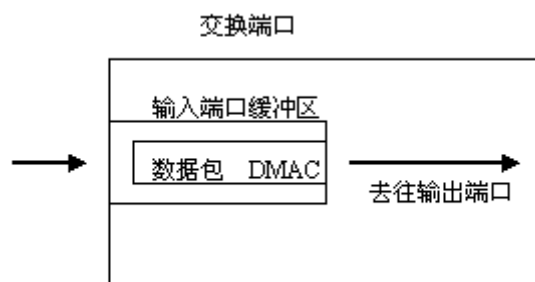
## 227. 交换机有三种转发方式，目前我们的交换机使用的是存储转发方式。

交换机有三种交换转发方式：Cut-through forwarding，Store and forwarding 和 Frag-free。交换机的交换方式决定了当设备收到一个数据帧的时候如何处理。

（1）Cut-through forwarding（直通转发，也翻译成短径转发）：交换机只读取数据帧的目的地址就开始转发。



(2) Store and forwarding (存储转发): 交换机复制整个数据帧到输入端口缓冲区后才进行转发。在数据帧转发之前, 交换机还要检查帧长度的合法性, 进行 CRC 校验, 检查到错误帧就丢弃。

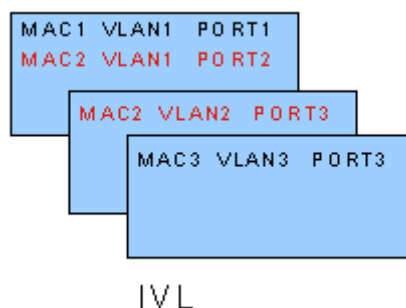


(3) Frag-free: 这种交换转发方式结合了直通转发和存储转发的优点, 交换机接收完数据帧的前 64 字节 (一个最短帧长度), 然后根据头信息查表转发。它是 Catalyst 1900 的默认转发模式。

交换机的转发方式影响了时延(Latency)大小。交换机延时是指从交换机接收到数据包到开始向目的端口复制数据包之间的时间间隔。对于采用直通交换方式的交换机机不管数据帧的整体大小, 而只根据目的地址来决定转发方向, 因此直通转发延时小, 有固定的时延值。但是这种转发方式不适合于高错误率的网络。对于存储转发方式的交换机, 时延和帧的长短有关。

## 228. 支持 VLAN 的交换机有两种 MAC 地址学习方式分别是 IVL 和 SVL。

IVL 模式是独享式的 MAC 地址学习模式, 各个 VLAN 内学习到的 MAC 地址为各个 VLAN 所有, 不会共享给其他 VLAN。我司多数交换机为这种 MAC 学习模式。



IVL

SVL 模式是共享式 MAC 地址学习模式, 某一个 VLAN 学习到的 MAC 会被其他所有 VLAN 共享使用, 我司 3026 系列交换机, 2050 系列交换机支持这种 MAC 学习模式。

MAC1	VLAN1	PORT1
MAC2	VLAN2	PORT2
MAC3	VLAN3	PORT3

## SVL

不同学习方式的交换机转发流程有所不同。

对于支持 IVL 的交换机，转发流程分以下几步：

- (1) 根据帧内 Tag Header 的 VLAN ID 查找 L2FDB 表，确定查找的范围；
- (2) 根据目的 MAC 查找出端口，图中应该从端口 2 转发出去；
- (3) 如果在 L2FDB 表中查找不到该目的 MAC，则该报文将通过广播的方式在该 VLAN 内所有端口转发；
- (4) 同时该以太网帧的源 MAC 将被学习到接收到报文的端口上，即端口 1（VLAN 2）；
- (5) L2FDB 表中的 MAC 地址通过老化机制更新；
- (6) 在转发的过程中，不会对帧的内容进行修改。

对于支持 SVL 的交换机，转发流程分以下几步：

- (1) 根据帧的目的 MAC 查 MAC 转发表(即 L2FDB)，查找相应的出端口。根据现有 L2FDB 表，报文应该从端口 2 发送出去；
- (2) 判断出端口的 VLAN ID 和报文 Tag Header 内的 VLAN ID 是否匹配，匹配则转发，不匹配则丢弃；
- (3) 如果在 L2FDB 表中查找不到该目的 MAC，则判断出端口的 VLAN ID 和报文 Tag Header 内的 VLAN ID 是否匹配，不匹配直接丢弃；匹配则在该 VLAN 内广播；
- (4) L2FDB 表中 MAC 地址通过老化机制来更新；
- (5) 在转发的过程中，不会对帧的内容进行修改。

## 229. 三层交换机与路由器在转发操作上的主要区别在于其实现的方式：

- (1) 三层交换机通过硬件实现查找和转发
- (2) 传统路由器通过微处理器上运行的软件实现查找和转发
- (3) 三层交换机的软件路由表与路由器一样，需要软件通过路由协议来建立和维护
- (4) 三层交换机相对于路由器来说在硬件中多了一个硬件路由表，该硬件路由表来源于软件路由表。

## 230. 三层交换技术的发展

- (1) 传统的三层路由技术通过软件查找路由表进行逐包转发。

传统三层路由技术对每个报文进行处理，并基于第三层地址信息转发报文。这一方法称为逐包转发。

- (2) 流交换通过硬件完成后续报文的快速转发，这个转发过程称为精确匹配，而且首报文转发仍然采用软件查找路由表实现转发。

根据数据流的首报文转发建立新的快速转发路径，同一数据流的后续报文按照此转发路

径进行转发的方法称之为流交换（FS）。

（3）最长匹配的三层交换技术，所有报文的转发都通过硬件的快速匹配完成转发。

## 231. IRF 基础

IRF 的含义就是智能弹性框架(Intelligent Resilient Framework)。多台设备互相连接起来形成一个“联合设备”(Fabric)。无论在管理还是在使用上，就成为了一个整体。

每台设备称作一个 Unit，多个 Unit 互联就组成了一个 Fabric。内部互连的端口就称为 Fabric Port，业务端口称为 User Port。

IRF 的三个重要方面：

（1）DDM（分布式设备管理）：

外界可以将整个 Fabric 看成一台整体设备进行管理，用户可以通过 CONSOLE、SNMP、TELNET、WEB 等多种方式来管理整个 Fabric。

（2）DRR（分布式弹性路由）：

Fabric 的多个设备在外界看来是一台单独的三层交换机。整个 Fabric 将作为一台设备进行路由功能和转发功能。在某一个设备发生故障时，路由协议和数据转发可以不中断。

（3）DLA（分布式链路聚合）：

支持跨设备的链路聚合，可以在设备之间进行链路的负载分担和互为备份。

**注：**

（1）多个 Unit 中有一个被选举成 Master Unit。只有 Master Unit 上的路由协议才向外发出报文，代表整个 Unit 和外部交换信息、建立邻居关系。

（2）只有 Master Unit 才会计算并下发三层转发表。

（3）Master 将向其他 Unit 上的路由协议备份足够的信息，以便在 Master Unit 故障时，其他 Unit 可以无缝的接手 Master 的工作。

（4）IPC/IUC：设备内的单板间通信成为 IPC，IRF 内的 Unit 间通信称为 IUC。

（5）HA/XHA：双主控设备之间的热备份称为 HA，IRF 内 Unit 间的热备份成为 XHA。

（6）PPRDT：协议报文重定向，使用类似 ACL 的方法将特性协议报文传送到特定的 Unit 上进行处理。

## 232. 备件知识

（1）非工作时间快速备件服务包括：7×24×2 到达、7×24×4 到达、7×8×ND 到达三种级别。

（2）RMA 系统面向客户包括三种类型：（认证与非认证）代理商、工程师和最终用户。对于最终用户只提供坏件先退的服务，尽量引导客户通过代理商申请备件。

（3）基本保修条款：提供免费 5×8×NBD 发出服务，DOA 期内提供新件更换，DOA 期外提供维修件更换。

普通产品：保修期 1 年。

SOHO 产品：路由器保修 1 年，交换机中 5000 系列、1026C 和 1016C 保修 1 年，其它交换机保修 3 年。

存储产品：保修 3 年。

(4) 保修起始时间：

最终用户：从用户购买之日起计算，需提供有效购买凭证。

代理商：从公司发货之日起 90 天开始计算。

(5) DOA 期：除了部分 SOHO 产品，其它产品的 DOA 期都是 30 天。

(6) DOA 期的判断：

最终用户：从用户购买之日起+DOA 期内，需提供有效购买凭证。

代理商：从公司发货之日起 90 天+DOA 期内。

(7) 返修设备的保修期：为原产品保修期或更换、维修件到货之日后 90 天内，**以较长者为准。**

(8) 3 个备件分拨中心 (DC)：深圳、杭州和北京。

3 个备件维修中心 (RC)：深圳、杭州和北京。

30 个区域备件中心 (LC)：28 个办事处+海口+银川。

6 个二级支持城市：宁波、青岛、厦门、拉萨和西宁。**负责总部要求的重大工程备件紧急支持，不直接面向普通客户，不对外宣传。**

(9) 判断设备是否超过维保，需结合 CBS、SPMS、CDIP 和三年维保记录一起查询确认。

(10) 保外设备的维修报价：

申请人	备件更换	原厂返修
代理商	目录价*15%	目录价*8%
最终用户	目录价*17%	目录价*10%

(11) 通过客户提供的条码、服务合同号和项目订单号查询设备是否属于非工作时间快速紧急需求。

(12) 有三种情况可以提供好件先行的服务

①、申请由认证代理商和工程师提交。

②、报修设备属于备件发货坏。

③、购买我司的服务产品。

(13) 判断 3Com 产品备件交付是否 3Com 支持还是 H3C 支持的方法：

①、根据 RMA 号码判断：J 开头的 RMA 由 3Com 支持；A 或 E 开头的 RMA 由 H3C 支持。

②、根据操作类型判断：OEM 好件先行/坏件先退由 3Com 支持；好件先行/坏件先退由 H3C 支持。

（14）坏件返回时限：收到好件后的 15 个工作日。

（15）3Com 产品普通 RMA 申请不需要返回附配件；DOA 申请必须同时返回所有附配件。

（16）良品和跟踪品的区别：

良品指的是全新件，跟踪品指的是维修件，就设备本身，公司对于跟踪品由严格的维修要求，区别在于：

跟踪品的外观不同于全新件，同时没有光盘、保修卡、说明书、挂耳等附配件；外包装上，跟踪品没有 IQPC 的封箱标签，同时发货标签上备注“SP”字样。

### 233. 中低端路由器 B03 版本 telnet vpn-instance 时必须指定源地址或者源端口，否则 telnet 不能连接。而其它版本无需指定源地址或原端口。

即使用如下命令：

```
telnet vpn-instance vpn1 192.168.2.2 source-ip 192.168.1.1
```

也可以在系统视图下配置 telnet source-interface XXX(绑定 VPN 的端口)来避免，但是之后不能 telnet 非 vpn 中的地址。

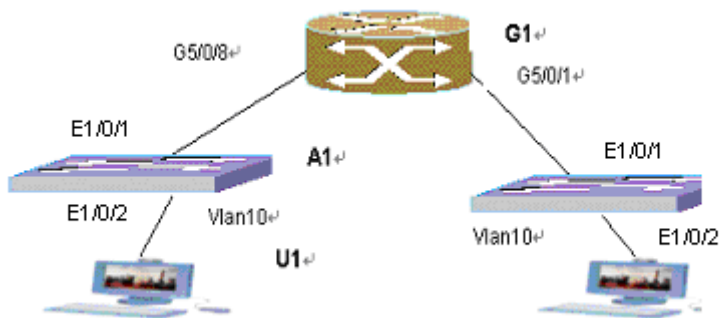
另外，telnet source-ip XXX 命令中的 IP 地址不能为绑定 VPN 的端口的 IP 地址，否则即使配置也不会生效，并且在配置文件中不会出现。

### 234. 路由的核心功能主要包括数据报文转发和路由处理两方面。

数据报文转发是路由器和第三层交换机最基本的功能，用来在子网间传送数据报文；路由处理子功能包括创建和维护路由表，完成这一功能需要启用路由协议如 RIP 或 OSPF 来发现和建立网络拓扑结构视图，形成路由表。

### 235. GVRP 注册和注销状态维护原理

VLAN 注册信息是 GVRP 的一个关键，该信息维护的两个主要手段就是“注册”+“注销”；另外为了避免异常，增加了“定时机制”来共同维护 VLAN 注册信息的状态机。



如上图 A1、A2 是接入层交换机，G1 是汇聚设备，各设备级连接口为 trunk 端口且容许所有 VLAN 通过。

### 声明+注册：

为了让 U1、U2 在 VLAN10 内二层互通，先在 A1 上创建 VLAN10 且将 E1/0/2 加入到 VLAN10 中，这个时候产生如下的自动动作：

- (1)因为 A1 设备的端口 E1/0/1 是容许所有 VLAN 通过的，而且 VLAN10 是本地静态创建的 VLAN，E1/0/1 自动加到 VLAN10 中，表示 A1 希望且实际容许从 E1/0/1 发送（/接收）VLAN10 的报文；
- (2)为了表达上述“希望”意愿，A1 设备向 G1 设备发送 GVRP 组播报文，这一过程就是所说的“声明”；
- (3)G1 设备从 G5/0/8 收到 A1 设备的“希望”意愿后，就在 G5/0/8“注册”VLAN10，注册的实际结果就是将端口 G5/0/8 加到 VLAN10 中，如果 G1 设备上还没有 VLAN10，就需要创建动态的 VLAN10；
- (4)既然创建了动态的 VLAN10，G1 设备就具备 VLAN10 的报文处理能力，而且 G5/0/1 是容许所有 VLAN 通过的，这就导致 G1 设备产生从 G5/0/1 发送（/接收）VLAN10 的报文“希望”意愿；
- (5)为了表达上述“希望”意愿，G1 设备向 A2 设备发送 GVRP 组播“声明”报文；

然后在 A2 上创建 VLAN10 且将 E1/0/2 加入到 VLAN10 中，上述的过程又反方向执行一次，产生如下的结果

- (1)A1、A2、G1 设备都创建了 VLAN10，具备 VLAN10 的报文处理能力；
- (2)图中的所有端口都具有希望发送（/接收）VLAN10 报文的意愿；
- (3) 图中的所有端口都实际容许发送（/接收）VLAN10 报文；



### 回收+注销:

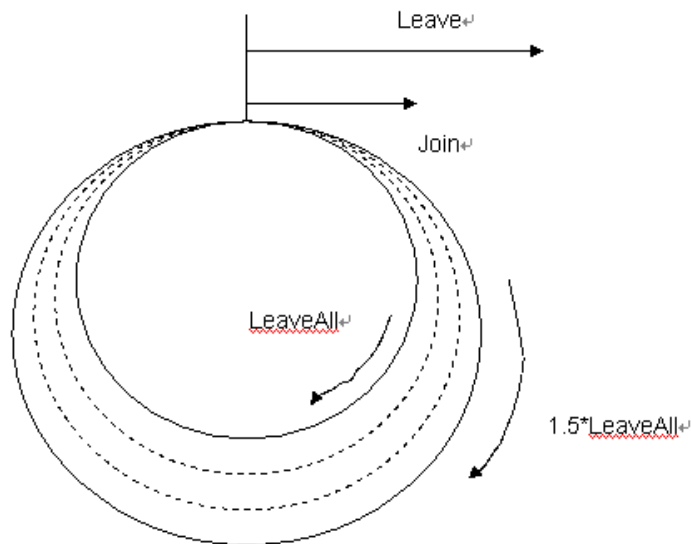
在 A1 上执行 E1/0/1 不容许 VLAN10 的命令,这个时候产生如下的自动动作:

- (1)这个命令表示 A1 不希望从 E0/1 发送 (/接收) VLAN10 的报文;
- (2)为了表达上述“不希望”意愿, A1 设备向 G1 设备发送 GVRP 组播报文, 这一过程就是所说的“回收”;
- (3) G1 设备从 G5/0/8 收到 A1 设备的“不希望”意愿后, 就在 G5/0/8 “注销” VLAN10, 注销的实际结果就是从 VLAN10 中将端口 G5/0/8 删除;
- (4) G1 设备上的所有动态 VLAN10 的端口检测有没有其他的端口属于动态 VLAN10, 如果除了自己没有其它端口属于动态 VLAN10, 就向本端口发送“不希望”意愿的“回收”; 本例中, 就会向 A2 设备发送回收;

同样的, 在 A2 上执行 E1/0/1 不容许 VLAN10 的命令, 将导致 G5/0/1 从 VLAN10 中删除, 而且没有任何端口属于 VLAN10, 就删除动态的 VLAN10。

### 定时机制:

正常情况下, 上述的四个机制是足够应用了。但是实际情况下, 各种报文在链路中传输的过程中会丢失, 或者由于链路故障以及设备故障, “回收”都来不及发出, 等等这些情况下会产生一些动态的垃圾配置。为了解决这一问题, GARP 设计了一个比较完善的定时机制。如下图:



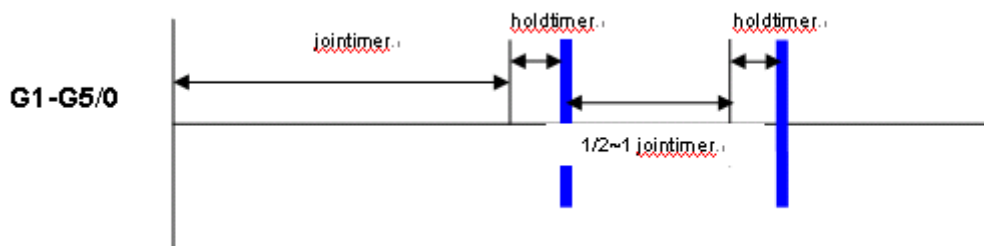
说明如下: GARP 协议使用 LeaveAll 定时器来实时更新维护的属性信息。一台启动了 GARP 应用协议的设备针对每个应用全局维护一个 LeaveAll 定时器, 该循环的 LeaveAll 定时器就好比一个驱动器, LeaveAll 定时器超时, 会从每



个启动了该应用协议的端口发送 LeaveAll 消息，同时在每个启动了该应用协议的端口上启动 Join 定时器和 Leave 定时器。

如图所示，LeaveAll 定时器就在(1~1.5)LeaveAll timer 的周长无限循环，每次到达超时点时就要启动 Join 定时器和 Leave 定时器。需要注意的是当收到其他设备的 LeaveAll 消息后，就会提前到达超时点。

LeaveAll 超时会启动 Join 定时器，Join 的超时会启动 Hold 定时器，Hold 定时器超时会试图发送 Join 消息，是否发送要看状态机的实际状态了。另外根据状态机的迁移来决定是否启动第二个 Join 定时器。



LeaveAll 超时同时会启动 Leave 定时器，Leave 定时器是分 4 个阶段实现的 LV--L3--L2--L1，每个阶段为 1/4Leave timer 长度，L1 超时就要注销对应的属性了，如果在 LV--L3--L2--L1 的过程中，重新收到了 JOIN “声明”，Leave 定时器就被中途作废，没有超时的机会了。

## 236. telnet 用户登陆规则

当一个用户 telnet 登陆，会从 vty0 到 vty4 查找第一个绑定了 telnet 协议的空闲 vty，如果找到以此 vty 登陆，无论是否成功，不会跨越这个 vty 到下一个 vty 进行认证。

如果此 vty 认证方式为 password 且没有设置 password 就会提示：  
Login password has not been set !

如果没有只绑定 telnet 协议的空闲 vty，会从 vty0 到 vty4 查找第一个绑定了 all 协议的空闲 vty，如果找到以此 vty 登陆，同样不会跨越这个 vty 到下一个 vty 进行认证。

如果此 vty 认证方式为 password 且没有设置 password 就会提示：  
Login password has not been set !

## 237. 路由器接口错帧统计说明

### (1) Input 接口统计:

packets: 接收报文个数;  
bytes: 接收字节数;  
broadcasts: 接收广播报文个数;  
multicasts: 接收组播报文个数;  
error: 接收错误总个数;  
runs: 超小包错误 (小于 2 字节)  
giants: 超大包错误 (大于 1700 字节)  
CRC: CRC 校验错误;  
align errors: 字节不对齐错误;  
overruns: 接收溢出错误;  
dribbles:  
aborts: 接收到异常序列错误;  
no buffer: 没有接收 buffer 错误;  
frame errors: 接收帧错误;

### (2) Output 接口统计:

packets: 发送报文个数;  
bytes: 发送字节数;  
error: 发送错误总个数;  
underruns: 芯片需要发送时, 但接口没有准备好待发送的数据; collisions:  
不涉及  
deferred: 不涉及

## 238. 交换机接口错误帧统计说明

以太网帧有两种格式Ethernet II和IEEE802.3。这两种帧格式的主要不同点在于前者定义的2字节的类型, 而后者定义的是2字节的长度。正常以太网帧数据段 (以太网帧目的MAC地址一直到末尾的校验和结束) 长度为64字节—1518字节,

其中正常长度帧的最后4个字节为帧校验序列(FCS)字段,该字段是用循环冗余校验(CRC)进行帧错误检测。(还有8字节的前导码)。

### (1) Input 接口统计:

交换机入端口报文转发之前会对帧长度的合法性以及CRC校验码进行检查,如果帧长度低于或超过合法长度,或者CRC出错,交换机对其直接丢弃并按错帧类型进行统计。

输入错帧类型	类型简述
Runts	无论是否有vlan tag,数据段小于64字节,而且没有CRC校验错误的帧
Giants	没有vlan tag,数据段大于1518字节,小于最大帧长度(Maximum Frame Length),而且没有CRC校验错误的帧。有vlan tag,数据段大于1522字节,小于最大帧长度,而且没有CRC校验错误的帧
Throttles	交换机察觉缓存或CPU过载,关闭接口接收器的情形称为Throttle。Throttle是cisco路由器上的一个概念,我们的交换机目前不具备这个功能,一般应该显示为不支持
CRC	帧长度在正常范围(不带tag,长度在64到1518之间,或带tag,长度在64到1522之间),而且CRC校验错,如果支持此项,则不支持奇偶校验错误项
Frame	不是整数字节,而是多1~7bit,因此不对齐,或乱序或空帧,而且CRC校验错误,但是不计入CRC错误
Overrun	由于接口输入速率超过接收方处理能力,导致丢包,由于我们的交换机一般是线速转发,这项一般应该为0,只有部分交换机对上传CPU或三层线速转发的帧有接口带宽限制,或是通过ACL实现的带宽限制,因此被丢弃的帧,计入此项
Aborts	除其他错误之外,产品认为有必要统计的错误,例如前导码异常的帧,计入此项
Ignored	由于接口内部buffer满,丢弃的帧,与由于主系统缓存空间缺乏,导致的丢弃帧不同。线速转发的帧,在多接口满带宽输入,单接口输出等情况下,由于输出接口的带宽不足,数据帧将内部缓存占满,导致从接口输入的帧在进入内部缓存之前被丢弃,以及进入内部缓存的帧超时无法输出,计入此项,上传到CPU的帧,由于CPU处理能力限制,toCPU的缓存满,导致被丢弃,也计入此项
Parity	奇偶校验错误帧。如果支持此项,则不支持CRC错误项

### (2) Output接口统计:

输出错帧类型	类型简述
Underruns	与Overrun相反,输出接口的缓存从输出队列中取以太网帧时没有帧。是一种非常罕见的硬件异常。有的交换机没有单独的接口输出缓存,与接口输出队列是同一块缓存
Buffer failures	内部缓存满,如果输出队列满,输出的以太网帧将在内部缓存中暂时存储,由于内部缓存满,导致帧丢弃。由于交换机对线速转发的数据帧发生的这种异常,认为只是到达内部缓存而没有到达出接口,是个输入帧,因此计入 Input Ignore

Aborts	d Error, 只有从CPU发出的帧, 由于内部缓存满, 导致帧丢弃, 计入此项 在半双工模式下, 由于冲突检测, 延迟发送超过15次的帧, 被丢弃, 计入此项。 除其他错误之外, 产品认为有必要统计的错误, 例如添加前导码异常的帧, 也计入此项
Deferred	半双工模式下, 由于检测到载波正在被声明, 当时没有发出的包, 延时一次, 计数加一
Collisions	半双工模式下, 在以太网帧数据部分的前64字节进入线路前, 由于检测到冲突, 当时没有发出的包
Late collisions	半双工模式下, 在以太网帧数据部分的前64字节进入线路后, 由于检测到冲突, 当时没有发出的包
Lost carrier	载波丢失, 一般适用于串行WAN接口, 发送过程中, 每丢失一个载波, 此计数加一, 对于交换机, 通常是由于线路中断造成
No carrier	无载波, 一般适用于串行WAN接口, 当试图发送帧时, 如果没有载波出现, 此计数加一, 对于交换机, 通常是由于线路中断造成

测试仪器构造错误帧验证待测设备在接收到错误或者异常的帧的时候, 是过滤出错误帧还是继续转发错误帧到目的地址

AST II错帧类型	类型简述
Oversize	不带vlan tag, 数据段长度大于1518字节, 没有CRC校验错误的帧
VLAN oversize	带vlan tag, 数据段长度大于1522字节, 没有CRC校验错误的帧
Undersize	无论是否有vlan tag, 数据段长度小于64字节, 没有CRC校验错误的帧
CRC	数据段长度在正常范围, CRC校验错误的帧
Dribble Bit	没有以一个字节边界结束, CRC校验正确的帧
Errors	
Alignment	没有以一个字节边界结束, CRC校验错误的帧
Errors	

Drop : 错包是丢包统计, 这种错包是由于流量大于 CPU 处理能力导致的报文丢失(drops)

239. 以太网交换机中, **AUX 口**和 **Console 口**是同一个口, 所以用户界面类型中只有 **AUX 口**用户界面类型。

## 240. VLAN-VPN 原理介绍

VLAN-VPN 是指将用户私网 VLAN Tag 封装在公网 VLAN Tag 中, 使报文带着两层 VLAN Tag 穿越运营商的骨干网络 (公网)。在公网中报文只根据外层 VLAN Tag (即公网 VLAN Tag) 传播, 用户的私网 VLAN Tag 被屏蔽。

携带双层 VLAN Tag 的报文结构如图所示:

DA (6B)	SA (6B)	ETYPE (2B)	Nested VLAN TAG (2B)	ETYPE (2B)	User VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500 B)	FCS (4B)
------------	------------	---------------	-------------------------	---------------	-----------------------	---------------	--------------------	-------------

如果某端口的 GVRP、GMRP、IRF、NTDP、STP 或 802.1x 协议中的任一个已经启动，则不允许用户开启端口的 VLAN-VPN 特性。

默认情况下，设备的 STP 和 NTDP 协议是开启的。需要在相应端口下应用 `stp disable` 命令和 `undo ntdp enable` 命令来关闭相应协议。

## 241. 端口汇聚分为手工汇聚、动态 LACP 汇聚和静态 LACP 汇聚。（推荐使用静态汇聚）

### 手工汇聚和静态 LACP 汇聚

手工汇聚和静态 LACP 汇聚都是人为配置的汇聚组，不允许系统自动添加或删除手工或静态汇聚端口。手工或静态汇聚组必须包含一个端口，当汇聚组只有一个端口时，只能通过删除汇聚组的方式将该端口从汇聚组中删除。

手工汇聚端口的 LACP 协议为关闭状态，禁止用户使能手工汇聚端口的 LACP 协议。

静态汇聚端口的 LACP 协议为使能状态，当一个静态汇聚组被删除时，其成员端口将形成一个或多个动态 LACP 汇聚，并保持 LACP 使能。禁止用户关闭静态汇聚端口的 LACP 协议。

在手工汇聚组和静态汇聚组中，端口可能处于两种状态：**Active** 和 **Inactive**。其中，只有 **Active** 状态的端口能够收发用户业务报文，而 **Inactive** 状态的端口不能收发用户业务报文。在一个汇聚组中，处于 **Active** 状态的端口中的最小端口是汇聚组的主端口，其他的作为成员端口。

(1) 在手工汇聚组中，系统按照以下原则设置端口处于 **Active** 或者 **Inactive** 状态：

1 系统按照端口全双工/高速率、全双工/低速率、半双工/高速率、半双工/低速率的优先次序，选择优先次序最高的端口处于 **Active** 状态，其他端口则处于 **Inactive** 状态。

1 端口因存在硬件限制（如不能跨板汇聚）无法汇聚在一起，而无法与处于 **Active** 状态的最小端口汇聚的端口将处于 **Inactive** 状态。

1 与处于 **Active** 状态的最小端口的速率、双工属性和链路状态不同的端口将处

于 Inactive 状态。

(2) 在静态汇聚组中,系统按照以下原则设置端口处于 Active 或者 Inactive 状态:

1 系统按照端口全双工/高速率、全双工/低速率、半双工/高速率、半双工/低速率的优先次序,选择优先次序最高的端口处于 Active 状态,其他端口则处于 Inactive 状态。

1 与处于 Active 状态的最小端口所连接的对端设备不同,或者连接的是同一个对端设备但端口在不同的汇聚组内的端口将处于 Inactive 状态。

1 端口因存在硬件限制(如不能跨板汇聚)无法汇聚在一起,而无法与处于 Active 状态的最小端口汇聚的端口将处于 Inactive 状态。

1 与处于 Active 状态的最小端口的基本配置不同的端口将处于 Inactive 状态。

由于设备所能支持的汇聚组中的最大端口数有限制,如果处于 Active 状态的端口数超过设备所能支持的汇聚组中的最大端口数,系统将按照端口号从小到大的顺序选择一些端口为 Selected 端口,其他则为 Unselected 端口。

Selected 端口和 Unselected 端口都能收发 LACP 协议,但是 Unselected 端口不能转发用户的业务报文。

### 动态 LACP 汇聚

动态 LACP 汇聚是一种系统自动创建/删除的汇聚,不允许用户增加或删除动态 LACP 汇聚中的成员端口。只有速率和双工属性相同、连接到同一个设备、有相同基本配置的端口才能被动态汇聚在一起。

动态汇聚中,端口的 LACP 协议处于使能状态。一个端口也可以创建动态汇聚,此时为单端口汇聚。

由于设备所能支持的汇聚组中的最大端口数有限制,如果当前的成员端口数量超过了最大端口数的限制,则本端系统和对端系统会进行协商,根据设备 ID 优的一端的端口 ID 的大小,来决定端口的状态。具体协商步骤如下:

(1) 比较设备 ID (系统优先级+系统 MAC 地址)。先比较系统优先级,如果相同再比较系统 MAC 地址。设备 ID 小的一端被认为优。

(2) 比较端口 ID (端口优先级+端口号)。对于设备 ID 优的一端的各个端口,首先比较端口优先级,如果优先级相同再比较端口号。端口 ID 小的端口为 Selected 端口,剩余端口为 Unselected 端口。

在一个汇聚组中，Selected 端口中的最小端口是汇聚组的主端口，其他端口作为成员端口。

**说明：**若成员端口数量未超过最大 Selected 端口数限制，则所有成员端口都是 Selected 端口。Selected 端口和 Unselected 端口都能收发 LACP 协议，但是 Unselected 端口不能转发用户的业务报文。

## 242. Voice Vlan 功能介绍

Voice VLAN 指为用户的语音数据流而专门划分的 VLAN。通过划分 Voice VLAN 并将连接语音设备的端口加入 Voice VLAN，可以为语音数据配置 QoS，提高语音流量的传输优先级，保证通话质量。

识别数据流是否是 IP Phone 数据流的依据是进入端口的流的源 MAC 地址，用户可以预先设置 OUI（Organizationally Unique Identifier）地址，也可以使用缺省的 OUI 地址来作为判断标准。

OUI（Organizationally Unique Identifier）是 MAC 地址的前 24 位，是 IEEE 为不同设备供应商分配的一个全球唯一的标识符。

OUI 地址	Mask	Description
0003-6b00-0000	ffff-ff00-0000	Cisco phone
000f-e200-0000	ffff-ff00-0000	H3C Aolynk phone
00d0-1e00-0000	ffff-ff00-0000	Pingtel phone
00e0-7500-0000	ffff-ff00-0000	Polycom phone
00e0-bb00-0000	ffff-ff00-0000	3Com phone

下面以常用的组网方案为例介绍 IP 电话获取 IP 地址的过程。

如图所示，IP 电话需要通过 DHCP 服务器和网络呼叫处理器配合，建立语音数据的发送路径。如图所示，IP 电话从上电开机到具备向外界传输语音数据的能力，需要经历以下三个步骤：

(1) IP 电话上电后，会发出 untag 的 DHCP 请求报文，报文中除包含请求自身 IP 的内容外，还会在 Option184 字段中包含四个特殊的请求信息。此报文将在接收端口缺省 VLAN 内进行广播，位于缺省 VLAN 内的 DHCP Server1 接收到该报文后，将回复给 IP 电话相应的信息：

①、如果 DHCP Server1 没有配置 Option 184 功能，则直接回应 IP 电话，告知为其分配的 IP 地址。该 IP 电话由于没有收到 Voice VLAN 信息，将只能发送 untag 报文，且在连接交换机的端口所在缺省 VLAN 内进行通信，因此接入端口的缺省 VLAN 就需要被手工设置为 Voice VLAN。（说明：在这种情况下，将跳过后面的步骤 2 和 3，IP 电话直接通过网关进行对外通信。）

②、如果 DHCP Server1 已经配置了 Option 184 功能，则向 IP 电话发送回应报文，在告知为其分配的 IP 地址以及网络呼叫处理器的 IP 地址和 Voice VLAN 的编号等信息。

(2) 如果 IP 电话通过 DHCP Server1 的回应报文获得了 Voice VLAN 信息，将放弃 DHCP Server1 分配的 IP 地址，重新构造 DHCP 请求报文，并为请求报文封装 Voice VLAN 的 Tag，向 Voice VLAN 中发送。工作在 Voice VLAN 中的 DHCP Server2 将为 IP 电话重新分配 IP 地址，并发送带 Tag 的回复报文。IP 电话收到后，即可发送带有 Voice VLAN Tag 的语音数据。此时，需要交换机上连接 IP 电话的端口允许 Voice VLAN 报文携带 Tag 通过。



(3) 在获取到 DHCP Server2 分配的 IP 地址之后，IP 电话将与 DHCP Server1 指定的网络呼叫处理器进行连接，下载软件，之后就可以正常进行通信了。

对于手工设置 IP 地址及 Voice VLAN 的 IP 电话，只需要保证设置的 Voice VLAN 编号与交换机保持一致，同时设置与网络呼叫处理器路由可达的 IP 地址即可。

**注意：**

(1) 只有当系统视图和端口视图下的 Voice VLAN 属性都打开时，Voice VLAN 功能才能正常运行。

(2) 如果用户的 IP 语音设备发出的是携带 VLAN Tag 的语音流，且接入的端口上开启了 802.1x 认证和 guest VLAN，为保证各功能的正常使用，请为 Voice VLAN、端口的缺省 VLAN 和 802.1x 的 guest VLAN 分配不同的 VLAN ID。

1 如果用户的 IP 语音设备发出的是不携带 VLAN Tag 的语音流，为实现 Voice VLAN 功能，只能将接入端口的缺省 VLAN 配置为 Voice VLAN，此时将不能实现 802.1x 认证功能。

**243. 交换机中 ARP 表项检查功能指不学习 MAC 地址为组播 MAC 的 ARP 表项，默认使能。**

**244. 二层设备的 MAC 地址学习都是通过源 MAC 地址学习来进行的。**

当端口收到一个未知源 MAC 地址的报文，会将这个 MAC 添加到接收端口上，以便后续以该 MAC 地址为目的的报文能够直接转发，即一次学习，多次转发。

**245. “resource errors” 是 AR46 RPU 接口下特有的统计错误类型，一般是由 cpu 高、端口队列溢出造成的。通过升级路由器版本解决。**

**246. 路由器和交换机的优先级说明**

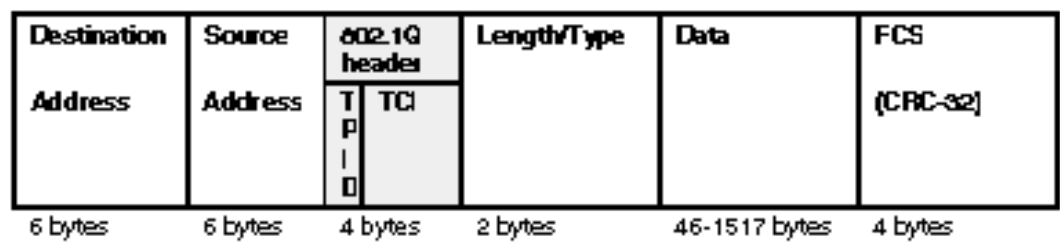
(1) IP 优先级、TOS 优先级和 DSCP 优先级

IP header 的 TOS 字段有 8 个 bit，其中前 3 个 bit 表示的就是 IP 优先级，取

值范围为 0~7；第 3~6 这 4 个 bit 表示的是 TOS 优先级，取值范围为 0~15；在 RFC2474 中，重新定义了 IP 报文头部的 TOS 域，称之为 DS 域，其中 DSCP 优先级用该域的前 6 位（0-5 位）表示，取值范围为 0~63，后 2 位（6、7 位）是保留位。

(2) 802.1p 优先级

802.1p 优先级位于二层报文头部，适用于不需要分析三层报头，而需要在二层环境下保证 QoS 的场合。



每一个支持 802.1Q 协议的主机，在发送数据包时，都在原来的以太网帧头中的源地址后增加了一个 4 字节的 802.1Q 标签头。

这 4 个字节的 802.1Q 标签头包含了 2 个字节的标签协议标识（TPID--Tag Protocol Identifier, 它的值是 8100), 和 2 个字节的标签控制信息(TCI--Tag Control Information)，TCI 字节中 Priority 字段就是 802.1p 优先级，它由 3 个 bit 组成，取值范围为 0~7。这 3 位指明帧的优先级。一共有 8 种优先级，主要用于当交换机阻塞时，优先发送哪个数据包。

247. H3C 交换机启动后将有 5 个缺省的 OUI 地址

- 00:0F:E2 H3C Aolynk phone
- 00:E0:BB 3com phone
- 00:03:6B Cisco phone
- 00:E0:75 Polycom phone
- 00:D0:1E Pingtel phone

248. 交换机 IP、MAC 和端口绑定说明

(1) H3C 3600/H3C S5600/S3900/S5600/S5100EI 系列产品只支持三者同时绑定;

(2) S3000 系列中 S3026EFGTC/S3026C-PWR/S3050C 支持三者同时绑定或任意两者的绑定；

(3) S3500 系列设备除了 S3526E/C 外都不支持上述三者或任意两者绑定；

(4) S5000 系列设备支持三者或任意两者绑定；

(5) H3C S5500-SI、S2000C/S2000-EI、S3100SI 系列设备不支持三者或任意两者的绑定。

**249. 交换机 am ip-pool 功能说明（只限制三层访问，无法对端口下的二层访问进行限制）。**

支持此功能的产品包括：

(1) H3C 3600、H3C 5600、H3C 5100、Quidway S3500；

(2) Quidway S3900、Quidway S5600 和 Quidway S5000 系列交换机。

**250. 当以太网接口启用 dot1x 认证后，只有将该接口配置为基于端口的认证方法后，才可以使用 dot1x guest-vlan 的配置。**

**251. PCA 无法 ping 通 PCB 但可以通过 ftp 的方式进行访问，但 PCB 可以 ping 通 PCA，原因有可能是在 PCB 上的防火墙（Windows XP 系统）配置中的“例外”选项卡中，将“文件和打印机共享”排除在例外允许访问之外。**

**252. 交换机作集中式 MAC 认证时，mac 地址作为用户名密码时 mac 地址间应去掉“—”。**

如下：

```
local-user 0015c50d1645
password simple 0015c50d1645
service-type lan-access
attribute ip 1.1.1.2 mac 0015-c50d-1645
```

253. 纯二层组播不用“**multicast routing-enable**”；未知组播丢弃如果不配置查询器不能开启，如果不开启查询器只开启未知组播丢弃功能，会导致纯二层网络中所有组播都是未知组播而被丢弃。

254. **VRP** 和 **Comware** 不是操作系统，是基于操作系统之上的应用平台。

255. **SNMP** 网管服务器发送消息查询设备采用轮询方式，报文是基于 **UDP** 的 **161** 端口；设备主动发送自身消息给 **SNMP** 网管服务器基于 **UDP** 的 **162** 端口，该报文为 **trap** 报文。

256. **Radius** 本地认证配置在路由器和交换机上的区别

在路由器上，必须手工配置命令“**local-server nas-ip 127.0.0.1**”；

在交换机上，该命令是默认配置。

257. 静态路由只有在物理层 **down** 的情况下，才会被路由表删除，即使配置 **detect-group** 侦测，也不能删除物理 **UP**、但协议层 **down** 的静态路由。

258. 在一个 **2FXS** 卡上接两个电话，在该路由器上配置两个 **POTS** 实体，即可实现通话。

259. 当出现 **ping** 对端地址只有第一个报文能通时，多于接口快转功能的开启有关。

260. 在路由器 **VRP 1.74** 版本配置子接口时，应先映射 **vlan** 再配置 **IP** 地址。

261. 备件服务应确保 **5** 方面准确无误

项目、地点、价格、质量和时间。

这里的准确无误指精确、正确、确切和明确。

262. 在 Tunnel 口上应用 Qos 的 LR、CBQ 等时，需关闭接口快转功能。

263. 在 SAE 接口上配置工作在“异步模式”后，系统视图下才会出现“user-interface tty”。

264. 中低端交换机与 SOHO 产品易混淆产品列表

E126	(LSW)	E126-SI	(SOHO)
QuidwayS2126-EI	(LSW)	S2126	(SOHO)
QuidwayS2126-SI	(LSW)	H3C S2126	(SOHO)
S2008C	(LSW)	S2008CP/CT	(SOHO)
S2008B	(LSW)	S5016P	(SOHO)
S5012G	(LSW)	S5024P	(SOHO)
S5012T	(LSW)		
S5024G	(LSW)		

265. 配置 Radius 认证时，只有在 radius scheme 中配置服务类型为 expand 或 huawei，才能实现 Server 下发用户级别。

如下：

```
radius scheme h3c
server-type extended
```

266. 交换机端口链路汇聚（或聚合）都是基于流的负载分担（没有命令进行更改），只有使用手工链路聚合时，端口数量在加减过程中才不会产生丢包；如果一端设备配置端口汇聚另一端不配置，则会产生丢包。

267. 交换机和路由器进入隐含命令模式都需在 **system** 视图下输入 “\_”。

268. 配置镜像时，交换机上只能配置一个监控端口。

269. 配置交换机接口 **OSPF** 的 **cost** 值时，只能在虚接口下配置，物理接口下没有该命令 “**ospf cost**”。

270. **H3C** 品牌的交换机可以通过命令查看设备序列号，路由器不成。

```
<H3C>display device manuinfo
```

```
DEVICE_NAME : 000000000011111111122222222222
```

```
DEVICE_SERIAL_NUMBER : a0000000000111111112222222223333333333
```

```
MAC_ADDRESS : 000F-E23E-F710
```

```
MANUFACTURING_DATE : 333
```

```
VENDOR_NAME : HUAWEI-3COM
```

**需要注意的是：**2006 年 10 月份发货的 H3C 品牌交换机可以通过该命令看到序列号。Quidway 品牌交换机都无法看到。

271. **3Com 与 H3C 设备的 OEM 关系**

**(1) 早期 oem 产品：**

3Com S5500G ————— H3C S56

3Com S5500 ————— H3C S39

3Com S4500 ————— 3Com S5500 ————— H3C S39

**(2) 目前新增产品：**

3Com S4500G ————— H3C S5500SI

3Com S4200G ————— H3C S5100EI

### (3) 将要新增产品:

3Com S4210 ———— H3C S3100TP-SI

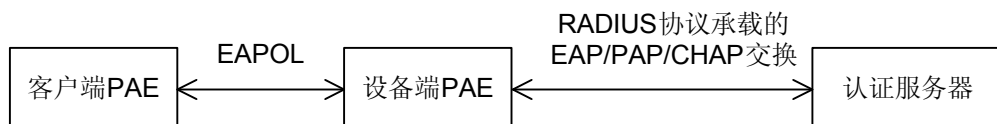
272. **Radius 和 HWTACACS 的 scheme 可以同时使用，在 domain 的配置中进行区分，两者的区别如下：**

<b>HWTACACS 协议</b>	<b>RADIUS 协议</b>
使用 TCP，网络传输更可靠	使用 UDP
除了标准的 HWTACACS 报文头，对报文主体全部进行加密	只是对验证报文中的密码字段进行加密
认证和授权分离，例如，可以用一个 TACACS 服务器进行认证，另外一个 TACACS 服务器进行授权	认证和授权一起处理
适于进行安全控制	适于进行计费
支持对路由器上的配置命令进行授权使用	不支持

273. **在路由器上应用策略路由时，更改下一跳的地址只要路由可达即可（不能是缺省路由）；在交换机上更改的下一跳地址必须是直连的下一跳地址。**

### 274. **802.1x 的工作机制**

IEEE 802.1x 认证系统利用 EAP（Extensible Authentication Protocol，可扩展认证协议）协议，作为在客户端和认证服务器之间交换认证信息的手段。



(1) 在客户端 PAE（相当于 PC 上安装的 802.1X 客户端）与设备端 PAE（相当于交换机）之间，EAP 协议报文使用 EAPOL 封装格式，直接承载于 LAN 环境中。

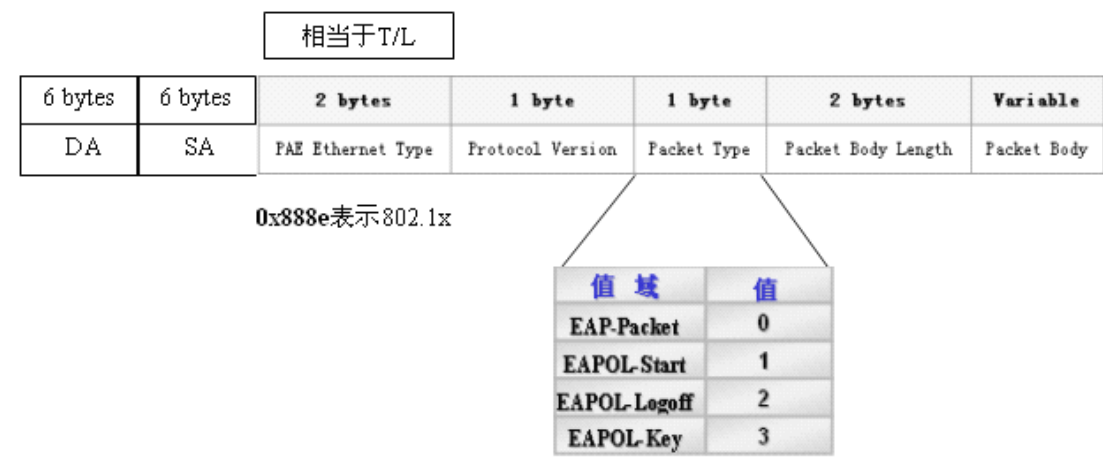
(2) 在设备端 PAE 与 RADIUS 服务器之间，EAP 协议报文可以使用 EAPoR 封

装格式（EAP over RADIUS），承载于 RADIUS 协议中；也可以由设备端 PAE 进行终结，而在设备端 PAE 与 RADIUS 服务器之间传送 PAP 协议报文或 CHAP 协议报文。

（3）当用户通过认证后，认证服务器会把用户的相关信息传递给设备端，设备端 PAE 根据 RADIUS 服务器的指示（Accept 或 Reject）决定受控端口的授权/非授权状态。

275. 802.1X 的 EAPOL 报文格式

EAPoL 报文封装在以太网帧中，如图所示：



说明如下：

**PAE Ethernet Type:** 表示协议类型，802.1x 分配的协议类型为 **0x888E**。

**Protocol Version:** 表示 EAPOL 帧的发送方所支持的协议版本号，入 0x01。

**Packet Type:**

**EAP-Packet**（值为 **00**），认证信息帧，用于承载认证信息；

**EAPOL-Start**（值为 **01**），认证发起帧；

**EAPOL-Logoff**（值为 **02**），退出请求帧；

**EAPOL-Key**（值为 **03**），密钥信息帧；

**EAPOL-Encapsulated-ASF-Alert**（值为 **04**），用于支持 ASF（Alerting Standards Forum）的 Alerting 消息。

**Packet Body Length:** 表示数据长度。如果为 0，则表示没有后面的数据域。

**Packet Body:** 根据不同的 Type 有不同的格式。

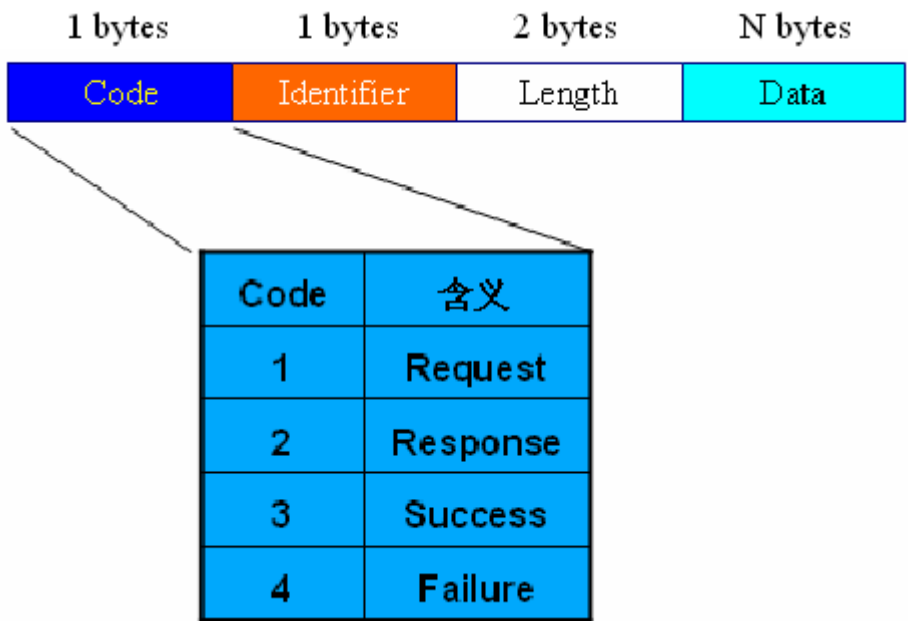
其中，EAPOL-Start，EAPOL-Logoff 和 EAPOL-Key 仅在客户端和设备端之



间存在；在设备端和认证服务器之间，EAP-Packet 报文重新封装承载于 RADIUS 协议上，以便穿越复杂的网络到达认证服务器；EAPOL-Encapsulated-ASF-Alert 封装与网管相关的信息，例如各种警告信息，由设备端终结。

276. 802.1X 的 EAP 报文格式

当 EAPOL 数据包格式 Type 域为 EAP-Packet 时，Packet Body 为 EAP 数据包结构，如下图所示。



说明如下：

**Code:** 指明 EAP 包的类型，一共有 4 种：Request，Response，Success，Failure。

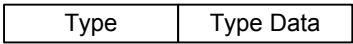
**Identifier:** 辅助进行 Response 和 Request 消息的匹配。

**Length:** EAP 包的长度，包含 Code、Identifier、Length 和 Data 的全部内容。

**Data:** 由 Code 决定。

Success 和 Failure 类型的包没有 Data 域，相应的 Length 域的值为 4。

EAP Request/Response 消息中的 Data 域由 Type 和 Type-data 两个域构成：



**Type:** 指出 EAP 的认证类型。其中，值为 1 时，代表 Identity，用来查询对方的身份；值为 4 时，代表 MD5-Challenge，类似于 PPP CHAP 协议，包含质询消息。

**Type Data:** Type Data 域的内容随不同类型的 Request 和 Response 而不同。

目前已经定义的 **Request/Response Type** 值为：

Type=1	Identity
Type=2	Notification
Type=3	Nak (Response only)
Type=4	MD5-Challenge
Type=5	One-Time Password (OTP)
Type=6	Generic Token Card

## 277. 802.1x 的认证过程

交换机支持 EAP 终结方式和 EAP 中继方式进行认证。

### (1) EAP 中继方式

这种方式是 IEEE 802.1x 标准规定的，将 EAP 协议承载在其他高层协议中，如 EAP over RADIUS，以便扩展认证协议报文穿越复杂的网络到达认证服务器。一般来说，EAP 中继方式需要 RADIUS 服务器支持 EAP 属性：**EAP-Message**（值为 79）和 **Message-Authenticator**（值为 80）。

**EAP 中继方式**有四种认证方法：

- ①、EAP-MD5：验证客户端的身份，RADIUS 服务器发送 MD5 加密字（EAP-Request/MD5 Challenge 报文）给客户端，客户端用该加密字对口令部分进行加密处理。
- ②、EAP-TLS（Transport Layer Security，传输层安全）：验证客户端和 RADIUS 服务器端双方的身份，通过 EAP-TLS 认证方法检查彼此的安全证书，保证双方的正确性，防止网络数据被盗窃。
- ③、EAP-TTLS：是对 EAP-TLS 的一种扩展。在 EAP TLS 中，实现对客户端和认证服务器的双向认证。EAP-TTLS 扩展了这种实现，它使用 TLS 建立起来的安全隧道传递信息。
- ④、PEAP（Protected Extensible Authentication Protocol，受保护的扩展认证协议）：首先创建和使用 TLS 安全通道来进行完整性保护，然后进行新的 EAP 协商，从而完成对客户端的身份验证。

说明：

由于 EAP 中继方式对报文的内容不做改动，如果要采用 PEAP、EAP-TLS、EAP-TTLS 或者 EAP-MD5 这四种认证方法之一，需要在客户端和 RADIUS 服务器上选择一致的认证方法，而在交换机上，只需要通过 `dot1x authentication-method eap` 命令启动 EAP 中继方式即可。

## （2）EAP 终结方式

这种方式将 EAP 报文在设备端终结并映射到 RADIUS 报文中，利用标准 RADIUS 协议完成认证和计费。

对于 EAP 终结方式，交换机与 RADIUS 服务器之间可以采用 PAP 或者 CHAP 认证方法。

EAP 终结方式与 EAP 中继方式的认证流程相比，不同之处在于用来对用户口令信息进行加密处理的随机加密字由交换机生成，之后交换机会把用户名、随机加密字和客户端加密后的口令信息一起送给 RADIUS 服务器，进行相关的认证处理。

## 278. 802.1x 的定时器

802.1x 认证过程中会启动多个定时器以控制接入用户、交换机以及 RADIUS 服务器之间进行合理、有序的交互。**802.1x 的定时器主要有以下几种：**

（1）**握手定时器（handshake-period）**：此定时器是在用户认证成功后启动的，交换机以此间隔为周期发送握手请求报文，以定期检测用户的在线情况。如果 **dot1x retry** 命令配置重试次数为 N，则如果交换机连续 N 次没有收到客户端的响应报文，就认为用户已经下线。

（2）**静默定时器（quiet-period）**：对用户认证失败以后，交换机需要静默一段时间（该时间由静默定时器设置）后，用户可以再重新发起认证，在静默期间，交换机不处理认证功能。

（3）**重认证超时定时器（reauth-period）**：在该定时器设置的时长内，交换机会发起 802.1X 重认证。

（4）**RADIUS 服务器超时定时器（server-timeout）**：若在该定时器设置的时长内，RADIUS 服务器未成功响应，交换机将重发认证请求报文。

(5) **客户端认证超时定时器 (supp-timeout)**: 当交换机向客户端发送了 Request/Challenge 请求报文后, 交换机启动此定时器, 若在该定时器设置的时长内, 设备端没有收到客户端的响应, 交换机将重发该报文。

(6) **传送超时定时器 (tx-period)**: 以下两种情况 Authenticator 设备启动 tx-period 定时器。其一是在客户端主动发起认证的情况下, 当交换机向客户端发送单播 Request/Identity 请求报文后, 交换机启动该定时器, 若在该定时器设置的时长内, 交换机没有收到客户端的响应, 则交换机将重发认证请求报文; 其二是为了对不支持主动发起认证的 802.1x 客户端进行认证, 交换机会在启动 802.1x 功能的端口不停地发送组播 Request/Identity 报文, 发送的间隔为 tx-period。

(7) **ver-period**: 客户端版本请求超时定时器。若在该定时器设置的时长内, Supplicant 设备未成功发送版本应答报文, 则 Authenticator 设备将重发版本请求报文。

## 279. 802.1X 的认证触发方式

(1) 标准 EAP 触发方式:

目的组播地址: **01-80-c2-00-00-03**, 客户端主动发 EAPOL-start 报文。仅有 **capol-start 为组播报文, 其他为单播**, 有线网中减少负载。认证报文全部为组播报文, 适应于无线。

(2) DHCP 触发方式:

采用 DHCP 报文作为触发设备对用户进行认证的条件, 只有 DHCP Discover 报文可以触发认证, 当前用户在线的情况下, 不触发认证。

(3) 华为专有触发方式:

有些通信设备不能透传上述多播报文, 采用广播触发认证方式。

(4) 支持客户端静态 IP 地址的触发方式:

设备每隔 N 秒 (默认情况下为 30 秒) 主动向客户端发起认证, 支持 Windows XP 在静态 IP 的情况下也能够进行认证。

## 280. 802.1X 配置注意事项

(1) 必须同时开启全局和端口的 802.1x 特性后, 802.1x 的配置才能生效。

(2) 对于非 H3C 客户端，由于不支持握手功能，在握手周期内交换机不会收到握手回应报文。因此需要将在线用户握手功能关闭，以防止错误地认为用户下线。

(3) 只有在端口认证方式下，交换机才可以支持 Guest VLAN 功能。一台交换机只能配置一个 Guest VLAN。

(4) 在使用 CAMS 作为认证服务器时，当要启用 802.1x 重认证时，不能在 domain 中配置 accounting none。而其他服务器无此限制。

## 281. AR28、46 加密卡的区别

(1) 应用在 AR2809B 上的加密卡是 NDEC（网络数据加密卡），它是 MIM 卡，可直接插在槽位上。

(2) 应用在 AR46 上的加密卡由两种：

①、FIC-HNDE（高性能网络数据加密卡），它是插在 AR46 的槽位上的。

②、ENDE（加密扣卡），它是安装在主控板上的，仅用于 AR46 的 ERPU 或 ERPU（H）的主控板上。

## 282. 低端交换机使用 display acl 无法看到 rule 的匹配关系，只能使用流量统计功能。

## 283. 交换机端口上出现大量的 CRC 统计错误，可能原因是链路问题或两端端口协商问题。

## 284. 在交换机上使用 “display arp” 命令显示出的统计含义。

Dump ARP Statistics Data:

All VIFs Static ARP Number: 576

VIF4 Dynamic ARP Number: 0

VIF3 Dynamic ARP Number: 0

VIF2 Dynamic ARP Number: 0

VIF1 Dynamic ARP Number: 0

Timer Entering Counter : 362876 定时器统计

In Blackbox Counter : 0 切换标志，这个目前应该是不会用到的

Failed Update Fdb Counter : 0 下发驱动失败统计

Resolving Failed Counter : 5933 解析失败统计

ARP Overflow Counter : 0 上溢出统计

ARP Underflow Counter : 82 下溢出统计  
 Last Error Code : 0 最后一次错误类型  
 ETHER Input Counter : 29005646 以太收包统计  
 ARP Input Counter : 28771495 ARP收包统计

Type: S-Static		D-Dynamic			
IP Address	MAC Address	VLAN ID	Port Name / AL ID	Aging	Type
192.168.1.2	00e0-a01c-d537	N/A	N/A	N/A	S
192.168.1.9	00e0-a01c-da11	N/A	N/A	N/A	S
192.168.1.31	00e0-a01c-cc85	N/A	N/A	N/A	S
192.168.1.8	00e0-a01c-db14	1	GigabitEthernet1/0/2	N/A	S
192.168.1.33	00e0-a01c-clf2	1	GigabitEthernet1/0/1	N/A	S
. . . . .					
192.168.3.15	00e0-a01c-cf60	3	GigabitEthernet1/0/23	N/A	S
192.168.3.253	00d0-6808-6269	3	GigabitEthernet1/0/19	N/A	S
--- 494 entries displayed. total number is 576 entries ---					

--- 494 entries displayed, total number is 576 entries ---

红色字体说明如下：前面的数量是 disp arp 操作时，显示在屏幕上的 arp 数量。total number 指的是实际物理芯片中统计的 arp 数量。后者反应实际 arp 数量。前者只反应显示出来的情况，这里就是客户实际配置的静态表项。比如 arp 刷新，导致 arp 顺序发生变化，导致 arp 显示的数量与实际统计数量不统一。还有可能是显示过程中，按任意键中断，也会导致 arp 显示的数量与实际统计数量不统一。通过 display arp 显示出来的表项，不一定就是用户的全部表项，要看 total number 的统计值。或者停止流量的情况下静态显示。动态显示的结果是不能确保准确的。

285. **VRRP 的虚拟路由器的 IP 地址必须和备份组中成员交换机使用的真实 IP 地址在同一网段。**

286. **交换机中“display ip statistic”和“display interface”两个命令的区别。**

display ip statistic 是平台的统计信息（是对上送 CPU 的报文的统计）；而 display interfaces 是驱动端的统计；display ip statistic 看到的都是上送了 CPU 的报文的统计信息，如果报文只做二层，就不会有相应的统计信息。

display interfaces 命令显示的内容中，只有 overrun 的统计报文会被丢弃。

display ip statistic 命令显示的内容如下：

**<H3C>dis ip statistics**

```

Input:  sum          16371575      local          8306108
        bad protocol  1239274      bad format     96
        bad checksum  22          bad options    0
Output: forwarding   6331927      local          8402681
        dropped       0          no route       122450
        compress fails 0
Fragment:input       0          output         0
        dropped       0
        fragmented    0          couldn't fragment 0
Reassembling:sum     0          timeouts      0

```

说明如下：

字段		描述
Input：	sum	输入报文总数
	Local	输入的目的地地址是本地的报文
	bad protocol	协议号错的报文数
	bad format	格式错误的报文数
	bad checksum	校验和错误的报文数
	bad options	选项错误的报文数
Output：	forwarding	转发的报文数
	local	本地发送报文数
	dropped	发送时丢弃的报文数
	no route	查不到路由的报文数
	compress fails	压缩失败的报文数
Fragment：	input	输入的分片数
	output	输出的分片数
	dropped	丢弃的分片数
	fragmented	成功分片的报文数
	couldn't fragment	不能分片的报文数
Reassembling：	sum	重组报文总数
	timeouts	超时的分片报文数

上述带“bad”的统计都会被丢弃；“no route”指查转发表失败，如果不走三层不会有统计。

各带“bad”的统计说明如下：

bad protocol：是发给本机的报文，未知的上层协议类型的统计；

bad checksum: IP 报文头进行校验和错误;

bad format : 是多项错误之和, 具体包括以下各项 ( pstIpStat->ips\_ulBadVers+pstIpStat->ips\_ulBadHLen+pstIpStat->ips\_ulBadLen+pstIpStat->ips\_ulTooShort+pstIpStat->ips\_ulTooSmall+pstIpStat->ips\_ulCantForward+pstIpStat->ips\_ulTTLExceed);

bad options: IP 报文选项错误。

**287. 交换机中使用“am user-bind”命令不可以替代“arp 入侵检测”功能。**

因为 am 命令用来检测 IP 报文中的 IP、MAC 和端口对应关系, 对于协议号为 0806 的 arp 报文无法进行检测。

**288. 交换机入端口流量大于出端口带宽时, 交换芯片检测到自身 buffer 不足, 因此在入端口就丢弃报文。如果是二层报文可使用流量统计进行观察, 上 cpu 的报文使用 display ip statistics 进行观察。**

**289. 确认用户从 DHCP Server 获取的 IP 地址和用户主机的 MAC 地址的对应关系有两种方式。**

(1) 三层交换机可以通过 DHCP Relay 记录用户的 IP 地址信息。

(2) 二层交换机可以通过 DHCP Snooping 功能监听 DHCP 广播报文, 记录用户的 IP 地址信息。



290. 修改交换机 **MSTP** 的端口 **cost** 值时，应修改根端口的 **pathcost**。
291. 使用 **V5** 平台的交换机进行 **web** 网管时无需上传相关的管理压缩文件，只需在交换机上设置 **IP**、**telnet** 用户名即可。
292. 交换机中，当报文写道 **Cos** 和 **DSCP** 值时，以 **Cos** 为发送标准；每个 **ip** 报文都带着固定的 **dscp** 值，一般全部为 **0**。
293. 更改交换机 **MAC** 地址的方法。

重启交换机，先按 **ctrl+B**，再 **ctrl+t**，然后回车，输入密码 **huawei-3com**，之后输入如下命令 “**test setmacaddr 00e0fc437421** ” 即可。

294. 交换机中只有 **S56、S51** 有 **Combo** 口的概念，**S39、S36** 系列交换机后面的 **SFP** 模块没有 **Combo** 口的概念。即只有所有口都是千兆口时才会有 **Combo** 口。
295. **S39、S36** 交换机以前存在带有上下箭头的接口用来进行堆叠，不带箭头的接口不能进行堆叠，现在升级到最新版本后，所有 **SFP** 接口都可进行堆叠，但要成对使用，即使用 **1、2** 口或 **3、4** 口，不能使用 **1、3** 口或 **2、4** 口。
296. **V5** 版本的本地账号通过 **display current** 是无法显示的。
297. 对于路由器来说 **VRP1.74** 版本的地址池是在系统视图下配置，到了 **V3、V5** 都要求在 **domain system** 下进行配置。
298. **VLAN** 模式是 **SVL** 的交换机，使用“**display mac-address**”命令显示内容中，**VlanID** 项显示为 **N/A**。
299. 交换机中的端口配置了“**mac-address max-mac-count 0**”命令后，由于该端口 **mac** 表项为空，所有到达该端口的报文都会被丢弃而不会在 **vlan** 内广播。
300. 交换机中支持“**igmp-snooping group-policy**”功能有两个前提条件。
- (1) 具有查询器（使能 **igmp** 或 **igmp-snooping querier**）；
  - (2) 至少有一个端口上不应用 **group-policy**，以便使 **igmp-snooping** 表项中始终有该组播组，而不会被交换机认为是未知组播。
301. 使用 **V5** 平台的交换机在配置 **ACL** 时的注意事项。
- (1) **ACL** 最终的匹配动作是 **permit** 还是 **deny**，不由 **ACL** 中 **rule** 的动作决定，而是由此 **ACL** 所对应的 **behavior** 的动作决定的。

(2) 对于既有 permit 又有 deny 要求的访问控制，必须规定两个 behavior，一个为 permit，一个为 deny。例如：

**acl number 2000**

```
rule 0 permit source 1.1.1.0 0.0.0.255
```

**acl number 2001**

```
rule 0 deny
```

**traffic classifier permit operator and**

```
if-match acl 2000
```

**traffic classifier deny operator and**

```
if-match acl 2001
```

**traffic behavior permit**

```
filter permit
```

**traffic behavior deny**

```
filter deny
```

**qos policy test**

```
classifier deny behavior deny
```

```
classifier permit behavior permit
```

**interface Ethernet1/0/4**

```
qos apply policy test inbound
```

(3) ACL 默认为匹配，如果没有设置 deny 动作，没有匹配 ACL 中定义的数据流也会转发出去。

## 302. H3C 交换机支持 Jumbo 帧最大长度为 9216 字节。

工程质量注意事项：

- (1) 按照扣分原则，见不到的内容默认合格。
- (2) 光纤在机柜外应走槽道或使用套管；电源线应与数据线各走一边，否则会对数据的传输造成影响。
- (3) 机壳接地与电源接地是两回事，若客户坚持，应签订工程备忘录。
- (4) 最新机柜型号为 N68。

- (5) 标签朝向应一致，且便于查看。
- (6) 软件标签应包括版本合配置信息。
- (7) 应注意我司合代理商是否进行了挂牌服务。
- (8) 接地线应黄绿线相间。

### 303. 在 V5 平台交换机上应用用户自定义流模板时应关闭如下功能：

```
[H3C]undo dot1x
[H3C]undo cluster en
[H3C]undo habp en
[[H3C]undo ndp en
[H3C]und ntdp en
[H3C]int e1/0/1
[H3C-Ethernet1/0/1]undo stp
[H3C-Ethernet1/0/1]undo ntdp en
[H3C-Ethernet1/0/1]undo ndp enable
[H3C-Ethernet1/0/1]flow-tem bbb
```

#### 注意：

- (1) 用户自定义 ACL 需要和扩展型用户自定义流模板配合使用。
- (2) 在端口上应用流模板时，请关闭如下功能：802.1x 功能、集群功能（NDP、NTDP、HABP、Cluster）、DHCP Snooping、端口隔离、MAC+IP 端口绑定、灵活 QinQ、Voice VLAN，否则流模板将不能成功应用。同时建议用户不要在端口上应用流模版后使能这些功能。

### 304. 哑终端占用网络带宽得计算方法。

在不使用加密得情况下，路由器异步口连接终端得波特率为 9600bps。

带宽的计算方法：

主要是异步转 TCP/IP 时需要增加 20 字节 IP 头和 20 字节 TCP 头，每个终端占用网络上行 IP 数据接口带宽为  $\text{baud} = \text{speed} + 40 \text{ 字节} \times 8\text{bit}$

其中，speed 小于 9600bps，则最大占用为  $\text{baud} = 9600 + 320 = 10\text{kbps}$

对于 2M 的线路，若没有其它数据业务，那么带 170~180 个终端是可以的。

若网络中还有其它业务并且终端较多时，应适当考虑增大带宽或作 Qos。

305. 交换机中 **QinQ** 技术内层标签类型为 **0x8100**; 外层标签类型为 **0x9100**。
306. **SSL VPN——Secure Socket Layer VPN** 是基于 **TCP** 建立的, 从 **1.0** 到 **3.0**, 但现在很少使用, 将其取而代之的是 **TLS VPN (1.0)**。
307. 交换机中 **S39/36** 堆叠后跨 **Unit** 进行端口隔离不生效, 而 **S56** 设备可以实现。
308. 在进行 **RIP** 和 **OSPF** 的路由配置时, 对于 **NBMA** 的网络类型必须手工指定邻居 (使用 “**peer**” 命令)。

通常情况下, **RIP** 使用广播或组播地址发送报文, 如果在不支持广播或组播报文的链路上运行 **RIP**, 则必须手工指定 **RIP** 的邻居; 需要注意的是, 当指定的邻居和本地路由器非直接连接, 则必须取消对更新报文的源地址进行检查。

**OSPF** 协议由于无法通过广播 **Hello** 报文的形式发现相邻路由器, 必须手工指定相邻路由器的 **IP** 地址, 以及该相邻路由器是否有选举权等。

309. 在低端交换机中，从 IP 电话发送到交换机的数据被划分到 **voice vlan** 后，**Cos** 和 **dscp** 的优先级都会改变，**cos** 变为 **6**，**dscp** 被设置为 **46**。如果通过 **qos** 的重标记功能再次改变该 **voice vlan** 的数据流，可能由于 **acl** 冲突无法实现。

310. 在低端交换机 **V5** 平台配置 **radius** 认证（含 **dot1x**）时，在 **domain** 视图下必须认证授权都配置且使用方案应一样，计费的配置可选。

311. **IP** 地址冲突在 **IPV4** 上都是靠 **ARP** 报文的发送来检测的，所以要想检测并报告必须是和自己的 **IP** 地址冲突才会上报。两个 **PC** 的地址冲突和交换机根本没有关系，交换机也无法判断，所以不会上报 **Trap** 信息。

312. 低端交换机中 **S39SI** 与 **EI** 设备无法进行堆叠。

313. 低端交换机中配置远程镜像时，源端口不能镜像双向报文，即只能配置“**inbound**”或“**outbound**”方向。

314. **S36/56** 交换机上 **Mode** 切换按钮的说明

按钮旁边的“端口模式切换指示灯”，

为绿色时——各端口灯的颜色表示当前端口速率；

为黄色时——各端口灯的颜色表示当前端口的工作模式（双工、半双工）；

为绿色闪烁时——PoE 模式下端口上电自检失败。

315. 交换机 **Qos** 优先级理解

（1）每个端口默认有 8 个队列，每个队列的优先级就是它们的队列号，数值大的优先级高，这个优先级叫做本地优先级。

（2）端口优先级指通过命令配置在端口上的优先级。默认情况下，对于接收的报文，交换机将使用报文接收端口的优先级替换报文的 **802.1p** 优先级，然后根据该优先级为报文分配本地优先级。此时用户可以配置端口的优先级。另外用户

也可指定交换机信任报文自身携带的优先级（即 `priority trust` 命令）。

（3）可以改变 802.1p 优先级和本地优先级的映射关系，从而改变 802.1p 优先级和输出队列之间的映射关系。

（4）个别产品（Marwell 芯片）支持 DSCP 直接映射到队列，但大多数（Broadcom 芯片）的产品都只支持 CoS 映射到队列；不过如果对方只有 DSCP 有效，我们可以采用 `remark` 的方式先做 DSCP 到 CoS 的映射。当报文中同时具有 `dscp` 和 `cos` 的优先级时，可以通过队列调度中的命令进行选择。

### 316. VRRP 虚 IP 地址对应的 MAC 地址说明

#### （1）配置虚拟路由器的 IP 地址：

虚拟路由器的 IP 地址可以是备份组所在网段中未被分配的 IP 地址，也可以是备份组中成员交换机的接口 IP 地址。

①、真实 IP 地址与虚拟路由器的 IP 地址相同的交换机被称为“IP 地址拥有者”。

②、一个备份组可以有多个虚 IP 地址；备份组中最后一个虚拟路由器的 IP 地址被删除后，这个备份组也将同时被删除，对这个备份组进行的所有配置都不再有效。

③、**虚拟路由器的 IP 地址必须和备份组中成员交换机使用的真实 IP 地址在同一网段**，如果配置了不在同网段的虚拟路由器的 IP 地址，该备份组会处于 VRRP 尚未配置的初始状态，此状态下，VRRP 不起作用。

④、如果用户将自己的主机 IP 地址配置为与备份组的虚拟路由器的 IP 地址相同的 IP 地址，则本网段的所有报文都发送到用户的主机，使本网段的数据不能被正确转发。

#### （2）配置虚拟路由器的 IP 和 MAC 地址之间的关系

1 可以由用户来设置 MAC 地址和虚拟 IP 地址的对应关系。用户可以根据需要将备份组的多个虚拟 IP 地址和一个虚拟 MAC 地址对应，也可以将对应关系设置为虚拟 IP 和交换机路由接口的实际 MAC 地址对应。缺省情况下，交换机采用备份组的虚拟 MAC 地址和虚拟 IP 地址对应。

**根据 RFC 协议，虚 MAC 地址格式如下：00-00-5E-00-01-{VRID}**

317. 在低端交换机同一端口上下发二层和三层 **acl** 时，按照各交换机下发顺序生效，并不是二层优先。

318. 集群式堆叠设备，前面板的码管只会显示交换机的角色，不会向 **IRF** 那样显示设备的 **Unit** 号，此外也不能想 **IRF** 堆叠那样，从一台 **Unit** 上看到所有的配置信息。

For Cluster Commander, it will display C.

For cluster Slave, it will display S.

For Candidate, it will display c.

For un-clustered unit, it will display 1.



319. 无法通过 **telnet VRRP** 组的虚 IP 方式登录交换机和路由器。
320. 千兆 **SFP** 电口模块是否支持 **10/100/1000** 的速率配置, 取决于所插设备。  
如 **S56** 支持配置 **10/100/1000**, 而 **S36** 设备不支持。
321. 支持 **MCE** 功能的交换机在配置时, 应先配置 “**switch-mode mce**” 命令, 并按提示重启设备, 之后使用 “**display switch-mode**” 命令查看设备是否工作在 **MCE** 模式, 如果是才可以开始配置, 否则会提示 “**VPN-Table is full**”。
322. 在交换机上, 策略路由就是指指的是流量的重定向。低端交换机只有 **V5** 平台产品支持。
323. **S36** 和 **56** 不支持 **web** 页面登录的 **tacacs** 认证, 只支持 **local user** 和 **telnet** 用户认证。
324. **PC** 发送的报文如果目的 **MAC** 地址填充为零或与交换机上的网关不在同一网段, 那么交换机无法学习到其 **arp** 表项。
325. 配置后不保存设备配置信息, 重启后就会出现无法加入堆叠体的现象。