

HCNE Exam Reference

Version: 2.00 Written by 杨 诚

本资料基于HCNE教材Issue 4.0

D001 网络基础

• **LAN的类型**: 以太网(Ethernet)、令牌总线网(Token Bus)、令牌环网(Token Ring)、FDDI(光纤分布式数据接口)。

WAN 的类型: 公共电话网(PSTN)、综合业务数字网(ISDN)、数字数据网(DDN)专线、X.25、帧中继(Frame Relay)、异步传输模式(ATM)。

WAN 的交换模式: 报文交换、分组交换。

• **LAN 的网络拓扑结构**: 总线型、星型、树型、环型、网型

WAN 的网络拓扑结构: 星型、树型、全网状/半网状

• **标准化组织及其标准**

ISO: OSI

IEEE: 802.x

ANSI: FDDI

EIA/TIA: RS232、CAT5、V.24、HSSI

ITU: X.25、FR

IAB

• **OSI 各层的功能**

应用层: 应用程序间通信

表示层: 提供数据格式转换、数据加密

会话层: 建立、维护、管理会话(会话控制、会话管理)

传输层: 建立和维护虚电路, 进行差错校验和流量控制。

网络层: 寻址和路由选择, 设备有路由器和三层交换机。

数据链路层: 定义了物理地址、网络拓扑、线缆规划、错误校验, 设备有交换机。

物理层: 比特流传输, 定义了机械、电气、功能、接口特性, 设备有中继器和集线器。

• **可路由协议**: IP、IPX

路由协议: RIP、OSPF、BGP 等

• **流量控制的三种方式**: 缓存技术、源抑制报文、窗口机制

D002 TCP/IP 协议与子网规划

• **TCP/IP 协议栈**: (没有定义 OSI 的表示层和会话层)

应用层	HTTP,FTP,TFTP,Telnet,PING...
传输层	TCP,UDP
网络层	IP,ICMP,IGMP,ARP,RARP
数据链路层	Ethernet,802.3,PPP,HDLC,FR...
物理层	接口和线缆

• **常用 TCP 端口号**: HTTP:80, FTP:20(数据)/21(命令), Telnet:23, SMTP:25, POP:110, DNS:53

常用 UDP 端口号: DNS:53, BootP:67(Server)/68(Client), TFTP:69, SNMP:161

• **TCP 报文格式** 协议号: 6

16 位源端口						16 位目的端口			
32 位序列号									
32 位确认号									
首部长度	保留(6 位)	URG	ACK	PSH	RST	SYN	FIN	16 位窗口大小	
16 位 TCP 校验和					16 位紧急指针				
选项									
数据									

UDP 报文格式 协议号: 17

16 位源端口	16 位目的端口
16 位 UDP 长度	16 位 UDP 校验和
数据	

- TCP 建立连接需要 3 次握手，拆除连接需要 4 次握手

IP 报文格式

版本	报文长度	服务类型	总长度	
标识符			标志	片偏移
生存时间 TTL	协议		报头校验和	
源 IP 地址				
目的 IP 地址				
IP 选项				

- **CIDR 无类域间路由**把路由表中的若干条路由汇聚为一条路由，减少了路由表的规模，提高了路由器的可扩展性。使用 CIDR 技术汇聚的网络地址的比特位必须是一致的。

D003 常见网络接口与线缆**以太网类型和接口**

10M 以太网	10Base-T 10Base2 10Base5
100M 以太网	100Base-TX 100Base-FX
1000M 以太网	1000Base-T 1000Base-F

哪些设备互联需使用交叉线(Cross)

主机-主机、路由器-路由器，主机-路由器、交换机普通口-交换机普通口、集线器级连口-交换机级连口

- **异步串口**分为：异步方式的同/异步串口(Serial)、专用异步串口。

异步串口可设为：专线方式、拨号方式。

同步串口可工作在 DTE 或 DCE 方式。可接 V.24/V.35 电缆。

V.24 规程主要特性

电缆接口：DB50(路由器端)-DB25(外接网络端)

异步工作方式下最高速率 115200bps，封装协议 PPP

同步工作方式下最高速率 64000bps，封装协议 PPP、HDLC、X.25、FR...

符合 V.24 规程的路由器接口有：WAN 接口(Serial)、AUX 接口、Console 口、八异步口串行口(8AS)

V.35 规程主要特性

电缆接口：DB50(路由器端)-DB34(外接网络端)

只工作在同步方式，最高速率 2048000bps

V.24 和 V.35 控制信号

DTR：数据终端准备好

DSR：数据准备好

DCD：数据载体检测

RTS：请求发送

CTS：清除发送

- **单模光纤**传输频带宽、传输容量大。传输距离 10 公里。

多模光纤传输性能较差。传输距离 550 米。

D004 以太网交换机基础及配置**802.3 线缆**

10Base5	粗同轴电缆	500m
10Base2	细同轴电缆	200m
10BaseT	双绞线	100m
10BaseF	光纤	2km

• 802.3 帧结构

PRE	SFD	DA	SA	LEN	LLC 控制信息	DATA	PAD	CRC
-----	-----	----	----	-----	----------	------	-----	-----

PRE: 先导字节

SFD: 帧开始标志

DA: 目的 MAC 地址

SA: 源 MAC 地址

LEN: LLC 帧长度

DATA: 数据字段

PAD: 填充字段

CRC: 校验字段

• 快速以太网标准 802.3u。

• 千兆以太网标准 802.3z、千兆以太网双绞线定义 802.3ab。

千兆以太网支持半双工和全双工自动协商, 可采用双绞线/单、多模光纤传输。在同一冲突域中不支持中继器互联, 不能与低速以太网协商速率。

• 冲突域: CSMA/CD 算法中每个站点所监听的网络范围。

局域网交换技术的核心设备是局域网交换机 LAN Switch, 其每一个端口都视作一个冲突域。

• LAN Switch 逻辑模型(P.4-12)

交换机在逻辑上分为: 数据转发逻辑、输入/输出接口。

- LAN Switch 转发逻辑: 负责把数据发到正确的地方

转发逻辑构成: 过滤/转发逻辑部分、学习逻辑、接口、MAC 地址表。

- 过滤/转发逻辑: 决定了对交换机所接收到的数据帧的处理方式。

- 学习逻辑: 动态维护 MAC 地址表。

- LAN Switch 输入输出接口: 用于连接其他设备, 并经过它们和其他设备通信。

接口分为: 接入接口、上行接口

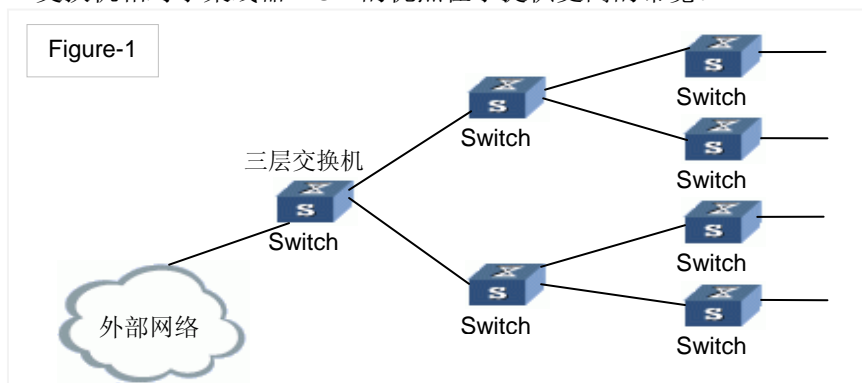
- 接入接口: 用于连接端系统(Client), 必须采用与端系统相同的技术。

- 上行接口: 用于连接其他交换机, 需要承载其他接口的流量总和, 应具有高性能。

• 现代局域网模型

三层交换机: 综合路由器和交换机功能的产品。

交换机相对于集线器 HUB 的优点在于提供更高的带宽。



VRP

交换机配置命令举例(大括号{}中的选项为单选项, 斜体字部分为参数值)

[Quidway]super password <i>password</i>	修改特权模式口令
[Quidway]sysname <i>switch_name</i>	命名交换机(或路由器)
[Quidway]interface <i>ethernet 0/1</i>	进入接口视图
[Quidway]quit	退出系统视图
[Quidway-Ethernet0/1]duplex {half full auto}	配置接口双工工作状态
[Quidway-Ethernet0/1]speed {10 100 auto}	配置接口速率
[Quidway-Ethernet0/1]flow-control	开启流控制
[Quidway-Ethernet0/1]mdi {across normal auto}	配置 MDI/MDIX 状态
[Quidway-Ethernet0/1]shutdown/undo shutdown	关闭/重启端口

• VLAN

VLAN 帧：IEEE 802.1Q 定义了 VLAN 帧，在标准以太网帧的 SA 后加入了一个 Tag Header，Tag Header 中的一个重要字段是 VLAN ID，标识了该帧所属的 VLAN。

划分 VLAN 目的：并非为了隔离各个网段，而是为了提高网络性能和安全性。

• 以太网交换机的三种接口工作方式：半双工、全双工、自动协商。

VRP VLAN 基本配置命令(以 Quidway S3026 为例)

[Quidway]vlan 3 创建并进入 VLAN 配置模式，缺省时系统将所有端口加入 VLAN 1，这个端口既不能被创建也不能被删除。

[Quidway]undo vlan 3 删除一个 VLAN

[Quidway-vlan3]port ethernet 0/1 to ethernet 0/4 给 VLAN 增加/删除以太网接口

[Quidway-Ethernet0/2]port access vlan 3 将本接口加入到指定 VLAN id

[Quidway-Ethernet0/2]port link-type {access|trunk|hybrid} 设置端口工作方式，access(缺省)不支持 802.1q 帧的传送，而 trunk 支持(用于 Switch 间互连)，hybrid 和 trunk 的区别在于 trunk 只允许缺省 VLAN 的报文发送时不打标签，而 hybrid 允许多个 VLAN 报文发送时不打标签。

[Quidway-Ethernet0/2]port trunk permit vlan {id|all} 设置允许 trunk 端口通过指定 VLAN 的数据帧，trunk 端口默认仅允许通过 VLAN 1 的数据帧。

[Quidway-Ethernet0/2]port trunk pvid vlan 3 设置 trunk 端口的 PVID，如果 trunk 端口上收到了非 802.1q 帧时，Switch 会给该帧加上 802.1q 标志，该标志字段中的 VLAN ID 即 PVID。

• 端口聚合：将多个端口聚合在一起，完成所有接入端口流量总和的传输，解决了上行链路的瓶颈问题。

VRP 端口聚合配置命令

[Quidway]link-aggregation ethernet 0/7 to ethernet 0/10 {ingress|both} 配置端口聚合

Port_num1 为端口聚合组的起始端口号，Port_num2 为终止端口号；

ingress 为接口入负荷分担方式，both 为接口出负荷分担方式。

[Quidway]undo link-aggregation {master_port_num|all} 清除端口聚合，master_port_num 为主接口，即聚合组中最小的以太网接口号，all 为所有聚合端口。

• STP(Spanning Tree 生成树协议,基于 802.1D 网桥协议)

STP 可以消除网络环路带来的广播风暴，其基本思想是以交换机为节点生成一个转发树(树没有环路)。

根桥：树的根为根桥交换机。

选择根桥的依据：1、优先级：优先级最高的被选作根桥(0-65535，数值越小优先级越高)

2、MAC 地址：若优先级相同，则选择 MAC 地址最小的。

VRP STP 基本配置命令

[Quidway]stp {enable|disable} 开启/关闭 STP 功能，默认关闭，开启后所有端口都参与 STP 计算。

[Quidway-Ethernet0/3]stp disable 关闭指定接口上的 STP 功能，如某些网络不存在环路可以关闭 STP。

D005 路由器基础及配置

• 路由器的作用：数据转发、路由(寻径)、备份、流量控制、子网速率适配、隔离网络、异种网络互连

• 路由表的内容：

目的网络地址	子网掩码	下一跳地址
--------	------	-------

• 配置路由器的 5 种方法：Console 口、远程拨号、Telnet、哑终端、FTP。

- Console 口配置简述：RJ45 头接在路由器的 Console 口上，RS232 头接在计算机的串口上。
配置“超级终端”，速率 9600bps、数据位 8 位、无校验、停止位 1、无流控。

• 升级路由器方法：通过 Console 口、通过 FTP/TFTP。(P.5-26)

• 破解路由器口令：1、重启路由器；

2、按下 Ctrl+B；

3、输入 Bootrom 口令(默认为空)；

4、在 Boot Menu 中选择 3: Clear application password；

5、最后选择 5: Exit and reboot。

VRP 路由器基本配置命令举例

[Quidway]sysname <i>router_name</i>	命名路由器(或交换机)
[Quidway]delete	删除 Flash ROM 中的配置
[Quidway]save	将配置写入 Flash ROM
[Quidway]interface <i>serial 0</i>	进入接口配置模式
[Quidway]quit	退出接口模式到系统视图
[Quidway]shutdown/undo shutdown	关闭/重启接口
[Quidway-Serial0]ip address <i>ip_address subnet_mask</i>	为接口配置 IP 地址和子网掩码
[Quidway]display version	显示 VRP 版本号
[Quidway]display current-configuration	显示系统运行配置信息
[Quidway]display interfaces	显示接口配置信息
[Quidway]display ip routing	显示路由表
[Quidway]ping <i>ip_address</i>	测试网络连通性
[Quidway]tracert <i>ip_address</i>	测试数据包从主机到目的地所经过的网关
[Quidway]debug all	打开所有调试信息
[Quidway]undo debug all	关闭所有调试信息
[Quidway]info-center enable	开启调试信息输出功能
[Quidway]info-center console debugging	将调试信息输出到 PC
[Quidway]info-center monitor debugging	将调试信息输出到 Telnet 终端或哑终端

D006 广域网协议原理及配置

• OSI 和 WAN 的对应关系

OSI 参考模型	WAN 技术
网络层	X.25
数据链路层	HDLC、PPP、X.25、LAPB、Frame Relay
物理层

• WAN 的主要连接技术：点对点（HDLC、PPP）、分组交换（X.25、Frame Relay、ATM）

• HDLC：运行于同步串行线路，属于链路层协议（如 DDN）。对于比特流实现透明传输，若出现边界标志字段 F 相同的情况可采用零比特填充法解决。

Keepalive 时延用于设置轮询间隔，默认为 10 秒，链路两端 Keepalive 必须相同。

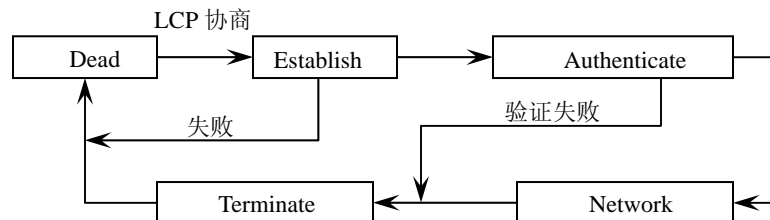
VRP HDLC 配置命令

[Quidway-Serial0]link-protocol hdlc	封装 HDLC 协议（同步接口）
[Quidway-Serial0]timer hold	设置 Keepalive 时延

• PPP/MP：物理层可以是同步或异步电路。

PPP 协议构成：网络层控制协议 NCP：IPCP、IPXCP。建立、配置、测试 PPP 数据链路连接
链路层控制协议 LCP。协商在链路上所传输的数据包的格式与类型。

扩展协议族(验证协议：PAP、CHAP)

PPP 协商流程：

PAP 验证：两次握手验证，口令以明文发送，被验证方发起验证请求。

CHAP 验证: 三次握手验证, 不发送口令, 主验证方发起验证请求。

MP(MultiLink PPP): 将多个 PPP 链路捆绑使用以增加带宽。首先要在 LCP 阶段协商是否使用 MP。

VRP PPP 配置命令

[Quidway-Serial0]link-protocol ppp 封装 PPP 协议
 [Quidway-Serial0]ppp authentication-mode {pap|chap} 设置验证类型
 [Quidway]local-user *username* password {simple|cipher} *password* 配置用户列表
 - PAP 验证配置:
 主验证方
 [Quidway]local-user *username* password {simple|cipher} *password* 配置用户列表
 [Quidway-Serial0]ppp authentication-mode pap
 被验证方
 [Quidway-Serial0]ppp pap local-user *username* password {simple|cipher} *password*
 - CHAP 验证配置:
 主验证方
 [Quidway]local-user *username* password {simple|cipher} *password* 配置被验证方用户列表
 [Quidway-Serial0]ppp chap host *hostname* 配置本地名称
 [Quidway-Serial0]ppp authentication-mode chap
 被验证方
 [Quidway]local-user *username* password {simple|cipher} *password* 配置主验证方用户列表
 [Quidway-Serial0]ppp chap user *username* 配置本地名称

VRP MP 配置命令

[Quidway-Serial0]ppp mp 封装 MP 协议
 [Quidway]ppp mp user *username* bind virtual-template *number* 建立用户与虚拟模板的对应关系
 [Quidway]interface virtual-template *number* 配置虚拟接口模板
 [Quidway]ppp mp max-bind *number* 设置虚拟模板最大绑定数(1-100)

- **X.25:** 是 DTE 与 DCE 之间的接口规程。X.25 协议分为分组层、数据链路层、物理层。
 X.25 数据链路层协议采用 LAPB (平衡型链路访问规程)。
 X.25 的封装格式: BFE、DDN、IETF、Cisco 兼容。
 X.25 虚电路有: PVC (永久虚电路)、SVC (交换式虚电路)。每接口最多配置 4095 条 VC。
 X.25 虚电路范围: $1 \leq LIC \leq HIC \leq LTC \leq HTC \leq LOC \leq HOC \leq 4095$

VRP X.25 配置命令

[Quidway-Serial0]link-protocol x25 封装 X.25 协议
 [Quidway-Serial0]x25 x121-address *x.121-address* 配置 X.121 地址
 [Quidway-Serial0]x25 map protocol *protocol-address* *x121-address* *x.121-address* 建立对端协议地址到对端 X.121 地址的映射, *protocol* 可以是 ip 或 ipx。
 [Quidway-Serial0]x25 pvc *pvc-number* protocol *protocol-address* *x121-address* *x.121-address* 建立 PVC
 [Quidway-Serial0]x25 vc-range {in-channel *hic lic*|bi-channel *htc ltc*|out-channel *hoc loc*} 配置虚电路范围
 [Quidway-Serial0]x25 packet-size *最大接收分组长度* *最大发送分组长度* 配置报文长度,缺省为 128
 [Quidway-Serial0]x25 window-size *最大接收分组长度* *最大发送分组长度* 配置窗口大小,缺省为 2
 [Quidway-Serial0]x25 modulo {8|128} 配置分组编号模数, 缺省为 8

帧中继: 在 X.25 基础上发展起来的快速分组交换技术。链路层协议为 LAPF。帧最大程度 1600bit。

DLCI 标识每一条虚电路, DLCI 只有本地意义, 不同物理接口上的 DLCI 可以相同。帧中继接口上最多支持 1024 条虚电路, 用户可用的 DLCI 范围是 16~1007。DLCI0 和 DLCI1023 为 LMI 专用。

LMI 协议用于建立和维护路由器和交换机间的连接。**三种 LMI 协议:** ITU-Q933a、ANSI、Cisco 兼容。

帧中继封装格式: IETF、Cisco 兼容。

带宽控制参数

CIR: 承诺信息速率; Bc: 承诺突发量; Be: 允许超过突发量; DE: 可丢弃标志; FECN: 前向拥塞指示; BECN: 后向拥塞指示。

当数据传送量 $\leq Bc$ 时, 正常传送;

当数据传送量 $\in (Bc, Bc+Be]$ 时, 将 Be 范围内的帧 DE 位置 1, 若发生拥塞则将其丢弃;

当数据传送量 $> Bc+Be$ 时, 将超过范围的帧丢弃;

当拥塞发生时, FECN 先被置位, 若继续拥塞, BECN 也被置位。

Inverse ARP: 用于求解每条虚电路的对端协议地址 IP 或 IPX(本地 DLCI 与对端协议地址的映射)。

帧中继的网络拓扑: 星型、部分网状、全网状。

NBMA: 帧中继的默认网络类型是 NBMA 非广播多点可达。帧中继不支持广播。

帧中继接口分为主接口和子接口。子接口分为点到点和点到多点, 子接口是逻辑接口。

VRP

帧中继配置命令

[Quidway-Serial0]link-protocol fr {mfr|ietf|nonstandard} 封装帧中继协议: IETF、Cisco 兼容

[Quidway-Serial0]fr interface-type {dte|dce|nni} 配置帧中继接口类型, NNI 为帧中继交换机之间的接口。若配为 DCE 或 NNI, 则须先使能 fr switching。

[Quidway-Serial0]fr lmi type {q933a|ansi|cisco-compatible} 配置 LMI 协议类型

[Quidway-Serial0]fr dlci dlci_number 配置一条本地虚电路号

[Quidway-Serial0]fr map {ip|ipx} protocol-address dlci dlci_number 建立本地 DLCI 到对端协议地址的映射

[Quidway-Serial0]fr inarp [ip|ipx] [dlci_number] 配置 Inverse ARP 动态映射

[Quidway]interface type number.subinterface_number 创建并进入子接口配置模式

D007 路由协议原理及配置

• **路由:** 指导 IP 数据包发送的路径信息。

• **路由表信息:**

Destination/Mask	Proto	Pref	Metric	Nexthop	Interface
目的地址/子网掩码	协议	优先级	花费	下一跳	接口

- Destination/Mask: 目的网络地址/子网掩码。目的地址“与”子网掩码=网络地址

- Protocol: 路由来源, 即路由如何生成的。

- Direct: 链路层协议发现的路由, 开销小、配置简单、无需人工维护。

- Static: 静态路由, 无开销, 配置简单, 需人工配置。

- RIP, OSPF: 动态路由, 开销大, 配置复杂, 无需人工维护。

- Preference: 优先级。高优先级路由协议发现的路由优先被加入路由表。优先级 0 表示直接路由(Direct)、10 表示 OSPF、60 表示静态路由(Static)、100 表示 RIP、255 表示任何来源不明的路由(Unknown)。数字越小优先级越高。

- Metric: 路由的花费表示达到目的地所花的代价, 花费值受到线路延迟、带宽、线路占有率、线路可信度、跳数、最大传输单元 MTU 的影响。静态路由的花费值为 0。不同路由协议的花费值不可比。

- Nexthop: 下一个路由器的接口地址。

- Interface: 输出接口, IP 包从该路由器的哪个接口转发, 如 Ethernet0、Serial0、Loopback0 等。

• **路由自环:** 从源路由器发出的报文经过几个转发后又回到源路由器。如:

[RouterA]ip route-static 20.0.0.0 8 10.0.0.2 [RouterB]ip route-static 20.0.0.0 8 10.0.0.1

• **缺省路由:** 当没有合适的路由时, 缺省路由才被使用, 目的网络地址和掩码均为 0.0.0.0。

VRP

静态路由配置命令

[Quidway]ip route-static destination_network_address subnet_mask
{interface_name|gateway_address} [preference preference_value] [reject|black_bone]

[命令说明] reject: 任何去往该目的地的报文均被丢弃, 通知源主机不可达。

black_bone: 任何去往该目的地的报文均被丢弃, 不通知源主机。

当只有下一跳的接口是 PPP 或 HDLC 接口才能写 *interface_name*, 如 Serial0, 否则只能写 *gateway_address*(下一跳地址)。

[命令举例] [Quidway]ip route-static 129.1.0.0 16 10.0.0.2

[Quidway]ip route-static 129.1.0.0 255.255.0.0 10.0.0.2

[Quidway]ip route-static 129.1.0.0 16 Serial2

[Quidway]ip route-static 0.0.0.0 0.0.0.0 10.0.0.2 配置缺省路由。

• 动态路由协议的底层协议

- RIP 协议基于 UDP 协议, 端口号 520。
- BGP 协议基于 TCP 协议。TCP 协议的端口号为 179。
- OSPF 协议封装在 IP 报文中, 协议号 89。

• 动态路由协议的分类

- 按作用范围划分: IGP(RIP, OSPF, IS-IS)、EGP(BGP)
- 按寻径算法划分: 距离矢量算法(RIP, BGP)、链路状态算法(OSPF, IS-IS)

• **路由发现:** 运行距离矢量路由协议的路由器从邻居路由器获得路由信息, 并将这些信息连同自己的路由信息再转发给其他邻居, 逐级传递以达到全网同步。

• 路由环路

产生原因: 网络故障可能引起路径与实际网络拓扑结构不一致而导致网络不能快速收敛。

环路补救方案: 定义最大值, RIP 协议定义最大跳数为 16, 大于 16 的跳数为网络不可达。

环路避免方案: 水平分割、路由中毒、抑制时间、触发更新

• RIP (端口号 520)

路由权: RIP 协议使用跳数来衡量到达目的地的距离。大于等于 16 的跳数表示网络不可达。在源和目的网间所要经过的最多路由器的数目为 15。

RIP 每 30 秒发送一次路由更新报文, 若 180 秒内没有收到对端更新报文, 则认为不可达, 其后 120 秒内没有收到就删除该条路由。

RIP 有 RIP-1 和 RIP-2。RIP-2 支持 VLSM 以及明文认证和 MD5 加密认证。

接口工作方式		报文传送方式
RIP-1 广播方式		RIP-1、RIP-2 广播报文
RIP-2	广播方式	RIP-1、RIP-2 广播报文
	组播方式	RIP-2 组播报文(组播地址 224.0.0.9)

缺省方式下, 接口运行 RIP-1 报文, 即只接收和发送 RIP-1 报文。

VRP RIP 协议配置命令

[Quidway]display rip	显示 RIP 配置信息
[Quidway]rip	启动并进入 RIP 配置模式
[Quidway-rip]network {network_number all}	在指定网络/所有网络上使能 RIP
[Quidway-rip]peer ip_address	配置报文的定点传送
[Quidway-Ethernet0]rip version {1 2 [bcast mcast]}	指定 RIP 版本及传送方式
[Quidway-Serial0]rip work	指定接口工作状态(同 rip input,rip output)
[Quidway-rip]summary	配置 RIP-2 路由聚合
[Quidway-Serial0]rip authentication simple password	配置 RIP-2 明文认证密码
[Quidway-Serial0]rip authentication md5 key-string string	配置 RIP-2 MD5 密文认证密码串
[Quidway-Serial0]rip authentication md5 type {nonstandard-compatible usual}	指定 MD5 类型
[Quidway]debugging rip packet	打开 RIP 调试开关
[Quidway]info-center console debugging	将调试信息输出到 PC

• OSPF (协议号 89)

Router ID: 运行 OSPF 的路由器必须有 Router ID。是一个 32bit 的整数。缺省 Router ID 为 Loopback 接口或当前接口的 IP 地址。Router ID 是全网唯一的。

OSPF 的五种报文: Hello、DD(Database Description)、LSR、LSU、LSAck

区域: OSPF 将自治系统 AS 划分为不同的区域,即在逻辑上将路由器划分为不同的组。用 Area ID 标识。

骨干区域(Backbone Area): Area 0, 用来解决路由自环问题。所有的区域必须和骨干区域相连,骨干区域自身也必须是连通的。

ABR: 区域边界路由器,区域边界上的路由器,属于不同的区域。

虚连接: 只在两台 ABR 之间穿过一个非骨干区域(转换区域)建立一条逻辑上的连接通道。

VRP

OSPF 配置命令

[Quidway]display ospf	显示路由器的 Router ID
[Quidway]router id <i>ip_address</i>	配置 Router ID
[Quidway]ospf enable	启用 OSPF 协议
[Quidway-Serial0]ospf enable area <i>area_id</i>	配置当前接口所属的 OSPF 区域

D008 访问控制列表和地址转换

- **IP 包的 5 元素 (访问控制列表的规则):** 协议号、源地址、目标地址、源端口号、目标端口号。
- **访问控制列表的应用场合:** 防火墙、QoS、DCC 触发拨号条件、地址转换 NAT、路由信息过滤。

- **访问控制列表的分类标识(acl-number):** 标准访问控制列表 1-99、扩展访问控制列表 100-199。

- 标准访问控制列表: 通过源地址来过滤数据包。如:

```
rule permit source 202.110.10.0 0.0.0.255
```

- 扩展访问控制列表: 通过协议号、源地址、目标地址、目标端口号等来过滤数据包。如:

```
rule deny tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0 0.0.0.255 destination-port equal ftp
```

- **访问控制列表的组合方法:** auto 表示深度优先,即地址范围小的规则优先考虑;config 表示按照配置的顺序。

VRP

访问控制列表配置命令

[Quidway]acl <i>acl-number</i> [match-order [config auto]]	配置列表序号及匹配规则
[Quidway-acl-1]rule {normal special} {permit deny} [source <i>source-address source-wildcard</i> any]	配置标准访问控制列表
[Quidway-acl-1]rule {normal special} {permit deny} {tcp udp} {source <i>source-address source-wildcard</i> any} [source-port <i>operator start-port [end-port]</i>] {destination <i>destination-address destination-wildcard</i> any} [destination-port <i>operator start-port [end-port]</i>] [logging]	配置扩展访问控制列表,oprator 的取值: equal、greater-than、less-than、not-equal、range。

[Quidway]firewall {enable|disable}

打开或关闭防火墙

[Quidway]firewall default {permit|deny}

配置防火墙默认过滤模式,默认 permit

[Quidway]display firewall

显示防火墙信息

[Quidway-Serial0]firewall packet-filter *acl-number* [inbound|outbound] 在接口上应用访问控制列表,并指明出入的方向

[Quidway]timerange {enable|disable}

打开或关闭防火墙时间段功能

[Quidway]settr *start-time end-time*

配置时间段范围,格式为 hh:mm

[Quidway]display isintr

显示当前时间是否在时间段内

[Quidway]display timerange

显示所配置的时间段

[Quidway]info-center enable

开启日志记录功能

[Quidway]info-center loghost *ip_address*

指定日志主机

- **NAT 提出的背景:** IP 地址日益短缺。

- **私有地址范围:** 10.0.0.0~10.255.255.255

172.16.0.0~172.31.255.255

192.168.0.0~192.168.255.255

- **配置 NAT 的两种方法:** Easy IP 直接使用接口的 IP 作为转换后的源地址;
使用地址池(地址必须是连续的)。
- **NAT 的缺点:** 1. 对于报文中含有有用地址信息的情况较难处理;
2. 不能处理 IP 报头加密的报文;
3. 由于隐藏了内部主机地址, 使网络调试变得复杂。

D009 DCC、ISDN 原理及配置

- **DCC 适用于:** PSTN、ISDN。
- **DCC 支持的网络拓扑:** 点到点、点到多点、多点到多点。
- **轮询 DCC:** 一个 Dialer 口可包含多个物理口, 但一个物理口同时只能属于一个 Dialer 口。同一个 Dialer Interface 的所有物理口成为一个 Dialer-group。

接口发出/收到呼叫配置

使能轮询 DCC: dialer enable-legacy/dialer enable-circular (ISDN 无需此命令)

点对点: dialer number 或 dialer route

点对多点: dialer route

- **共享 DCC:** 物理口的配置和逻辑口的配置分离开, 一个物理口同时可以属于多个逻辑口。共享 DCC 对 MP 的支持是通过流量控制来实现的。

DCC 特性参数

dialer timer idle *seconds*

设置链路空闲时间

dialer timer compete *seconds*

设置忙端口链路空闲时间

dialer timer enable *seconds*

设置链路断开后重拨时间

dialer timer wait-carrier *seconds*

设置端口数据发送最大等待时间

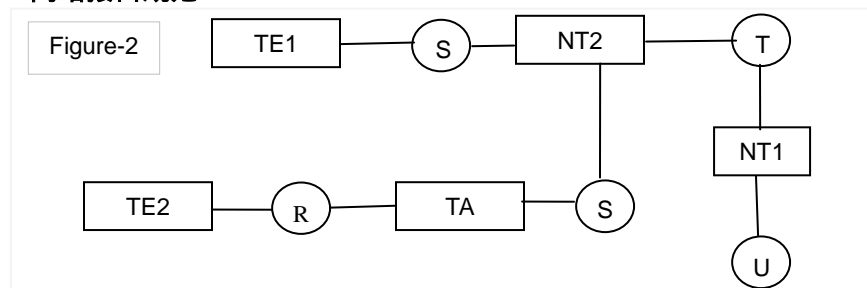
- **ISDN 接口 (B: 用户信道 D: 控制信道)**

ISDN BRI 提供 2B+D 信道, B 信道速率为 64Kbps, D 信道为 16Kbps, 共 144Kbps。

ISDN PRI 提供 30B+D 信道, B 信道速率为 64Kbps, D 信道为 64Kbps, 共 2Mbps。(欧洲)

ISDN PRI 提供 23B+D 信道, B 信道速率为 64Kbps, D 信道为 64Kbps, 共 1.5Mbps。(北美)

- **ISDN 协议模型构成:** 控制平面 C、用户平面 U、管理平面 M。C 和 U 不直接通信, 由 M 来协调管理。
- **ISDN 用户-网络接口规范**



NT1: 1 类网络终端。

NT2: 2 类网络终端, 又称智能网络终端。

TE1: 1 类终端设备, 又称 ISDN 标准终端。

TE2: 2 类终端设备, 又称非 ISDN 标准终端。

TA: 终端适配器。

ISDN 协议参数

设置数字入呼叫: isdn answer1 *被叫号码 子地址*

isdn answer2 *被叫号码 子地址*

设置模拟入呼叫: isdn pots answer1 *被叫号码 子地址*

isdn pots answer2 *被叫号码 子地址*

D010 备份中心原理及配置

- **主接口**：可以被备份的接口。可作主接口的有：物理接口及其子接口；逻辑通道：X.25 或 FR。拨号接口不能作主接口。
- **备份接口**：为其他接口做备份。可作备份接口的有：物理接口或虚拟接口模板上的逻辑通道。以太网口不能作为备份接口。

VRP

备份中心配置命令

- 备份接口为物理接口

[Quidway-Serail0]standby interface *interface_type interface_num* [*priority*] 指定物理接口为备份接口，*priority* 为优先级

[Quidway-Serail0]interface *interface_type interface_num* 进入指定的备份接口(物理)

- 备份接口为逻辑通道或 Dialer Route

[Quidway-Serail0]x25 map *protocol address x121-address x.121-address logic-channel logic-channel-number* 建立 X.25 与逻辑通道关联

[Quidway-Serail0]fr map *protocol address dlci dlci-address logic-channel logic-channel-number* 建立 FR 与逻辑通道关联

[Quidway-Serail0]dialer route *protocol next-hop-address dialer-string logic-channel logic-channel-num* 建立 Dialer Route 与逻辑通道关联

[Quidway-Serail0]logic-channel *logic-channel-number* 进入指定的备份接口(逻辑通道)

[Quidway-Serail0]standby **logic-channel** *logic-channel-num* [*priority*] 指定逻辑通道为备份接口

- 主备接口切换（主接口是物理接口）

[Quidway-Serail0]standby timer [*enable-delay|disable-delay*] 指定主备接口切换时延(0~65535)
enable-delay 为主→备切换时延，disable-delay 为备→主切换时延

- 主备接口切换（主接口是逻辑通道）

[Quidway-logic-channel-1]standby state-down *times* 设置判断逻辑通道是否 down 的尝试次数

[Quidway-logic-channel-1]standby state-up *seconds* 设置判断逻辑通道是否 up 的检查间隔秒数