网络实验考试复习-1

2017年12月3日 18:39

1、网络实验入门

(1) 在实验前，清空各个机器的配置：

```
<R1>: reset saved-configuration
<R1>: reboot
```

(2) tracert 命令返回 ** 的解决方法：

```
[R1]: ip ttl-expires enable
[R1]: ip unreachables enable
```

(3) 配置路由器接口 IP：

```
[R1]interface e0/0
[R1-Ethernet0/0]:ip address 192.168.2.1 24
```

(4) 配置PC机的IP、网关：

略。

(5) 配置 NAT 地址转换

i. 配置访问控制列表 (ACL)

```
[R1] acl basic 2001
[R1-acl-2001] rule 1 permit source 192.168.100.0 0.0.0.255
[R1-acl-2001] rule 2 permit source 10.0.0.0 0.255.255.255
[R1-acl-2001] rule 3 deny source any
```

ii. 配置地址池

```
[R1] nat address-group 1
[R1-address-group-1] address 192.168.5.120 192.168.5.124
```

iii. 配置NAT地址转换

```
[R1] interface e0/0
```

```
[R1-e0/0] nat outbound 2001 address-group 1
```

iv. 引入缺省路由

```
[R1]ip route-static 0.0.0.0 0.0.0.0 192.168.5.1 //缺省路由
```

(将缺省路由引入ospf的命令为:

```
[R1-ospf-1]default-route-advertise cost 100
```
)

(6) NAT 原理:

使用**网络地址**与**端口号**转换的 NAPT(Network Address and Port Translation) 技术，利用传输层的端口号，将多个内部专用 IP 地址映射为少数几个公网 IP 地址的技术。

网络实验考试复习-2

2017年12月3日 20:46

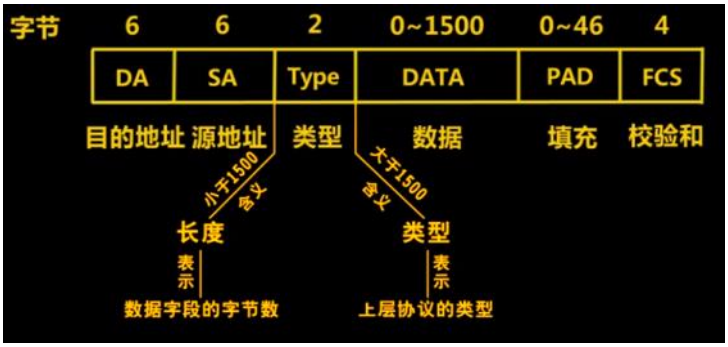
2、链路层和网络层实验

（1）以太网帧格式分析：

a．以太网帧格式：

1）EthernetII 无连接链路协议：

2）IEEE802.3 面向连接的链路协议：



b．截获IEEE802.3MAC帧的方法：

1）在IP协议配置中将 NetBIOS、IPX/SPX/NetBIOS协议打开

2）抓包 --> IEEE802.3MAC帧

3）其上为Logical-link Control协议，是一个面向连接的逻辑链路控制协议。

c．IP协议选择EthernetII无连接链路协议的原因：

IP的核心思想是简单，高效 --> 选择EthernetII无连接链路协议

（2）交换机MAC地址表和端口聚合：

a．交换机的逆向学习法：

当交换机收到一些数据以后，根据帧中的**源地址**来学习地址和端口的映射，并在MAC地址表中登记这种映射。转发时按MAC地址进行转发。

目的MAC地址	发送端口号
MAC1	E0/1
MAC2	E0/5
MAC3	E0/5
MAC4	E0/8

1）**清空交换机 MAC 地址表：**

```
[S1] dis mac   //查看MAC地址表(1:MAC地址、2:VLAN编号、3:这条信息是怎么得来的（学来的定期忘掉）、4:端口号、5:生命值(几秒内不被更新则忘记))
[S1] undo mac //清空MAC地址表
```

2）**如何证明MAC表是从源地址学习的：**

a）清空MAC地址表

b）断开主机B的连接后，使用主机 A ping 主机 B，并用抓包软件抓包

c）查看MAC地址表观察（学到了 A 没有学到 B）

b．广播风暴产生原因：

广播风暴产生的原因是网络中存在环路。

c．生成树协议：

1）**作用：**

a）通过线路检测，在**逻辑上**断开网络中的回路，防止产生广播风暴。

b）当线路出现故障时，断开的接口会被重新激活，恢复通信，起到**链路备份**的作用。

2）**启用/撤销生成树协议：**

```
[S1] stp enable //启动生成树协议
[S1] stp disable //撤销生成树协议
```

d．端口聚合：

1）**作用：**

a）线路之间**互相备份**。

b）可以充分利用**带宽**。

2）**配置端口聚合：**

```
[S1] interface bridge-aggregation 1
[S1-Bridge-Aggregation 1] link-aggregation mode dynamic
[S1-Ethernet 1/0/1] port link-aggregation group 1
[S1-Ethernet 1/0/2] port link-aggregation group 2
```

e. 清空交换机的MAC地址表：

```
[S1] undo mac-address
```

(3) VLAN的配置与分析：

a. 冲突域/广播域：

通过集线器(Hub)连起来的网络是一个冲突域。交换机工作在数据链路层，可以隔离冲突，被称为广播域。

b. VLAN 数据帧的传输：

VLAN 数据帧包含 Tag 域，但目前任何主机都不支持带有 tag 域的以太帧，因此，在交换机->主机的通信中，必须删除 Tag 域；在交换机->交换机的通信中，需要增加 tag 域。

当交换机接收到某数据帧时，根据数据帧中的 tag 域或接收端口的默认 Vlan ID 来判断该数据应当转发到哪些端口。

c. VLAN 端口分类：

1) access端口：（交换机->其他设备）

只能属于1个VLAN，从该端口发送的数据包是不带VLAN标签的，只能连接非交换机设备（主机、路由器、打印机等）

2) Trunk端口： （交换机->交换机）

可以属于多个VLAN，可以接受和发送带VLAN标签的保温，只能用于连接交换机和交换机之间。

3) Hybrid端口：（交换机->均可）

Access+Trunk，转发报文时，可以允许多个VLAN的报文不打标签，Trank只默认的可以不打。

d. VLAN 的配置：

```
[S1] vlan 2
[S1-vlan2] port e0/0
[S1-Ethernet0/0] port link-type trunk //配置端口类型
[S1-Ethernet0/0] port trunk permit vlan 2 to 3
                                    //配置Trunk 端口允许通过的Vlan
[S1-Ethernet0/0] port link-type hybrid //配置端口类型
```

```
[S1-Ethernet0/0] port hybrid pvid vlan 1 //指定端口的默认 Vlan
[S1-Ethernet0/0] port hybrid vlan 2 tagged
[S1-Ethernet0/0] port hybrid vlan 3 untagged
```

（4）PPP协议分析：

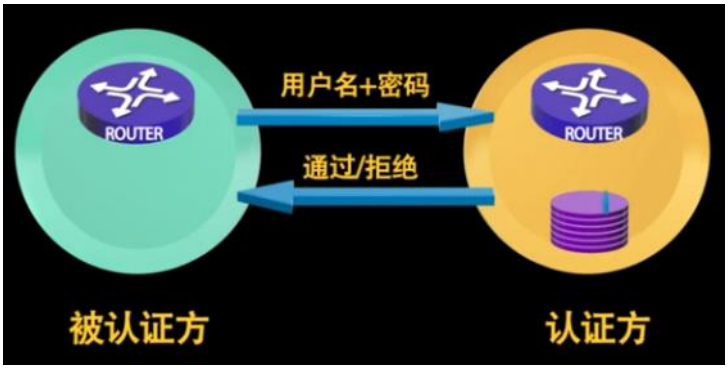
a．简介：

PPP协议是广泛使用的链路协议，**点对点**。

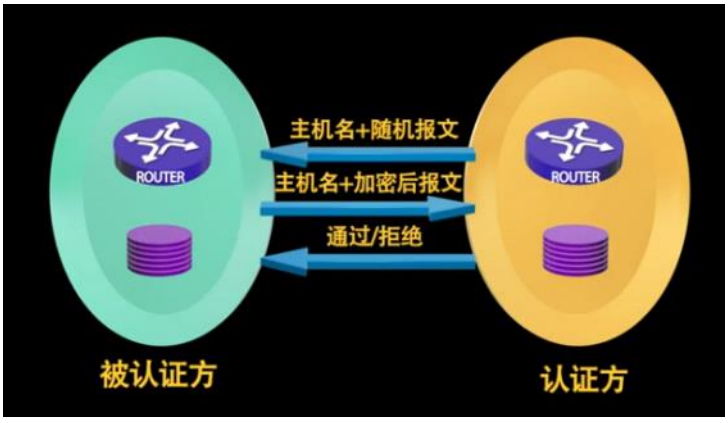
帧格式：

地址和控制可以进一步省略（点对点）

PAP认证：



CHAP认证：



b．配置PPP协议：

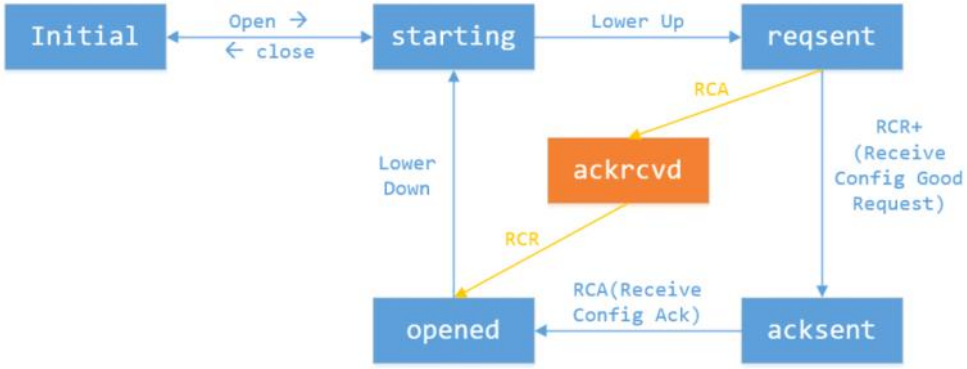
```
[R1] interface Serial 1/0
[R1-Serial1/0] link-protocol ppp //配置串口为ppp协议
```

[R1-Serial1/0] shutdown && undo shutdown //重启串口生效

<R1> debugging ppp all //打开 ppp 的 debug开关

<R1> terminal debugging //显示debug信息 --> 可以看到ppp报文

LCP协商状态转换图：



c．配置PAP认证：

[R1认证方]

[R1] local-user RTB class network -->为对方配置一个用户

[R1-luser-network-RTB] service-type ppp -->服务类型PPP

[R1-luser-network-RTB] password simple aaa -->设置密码aaa

[R1-S0/0] ppp suthentication pap -->授权R1作为认证方

[R2被认证方]

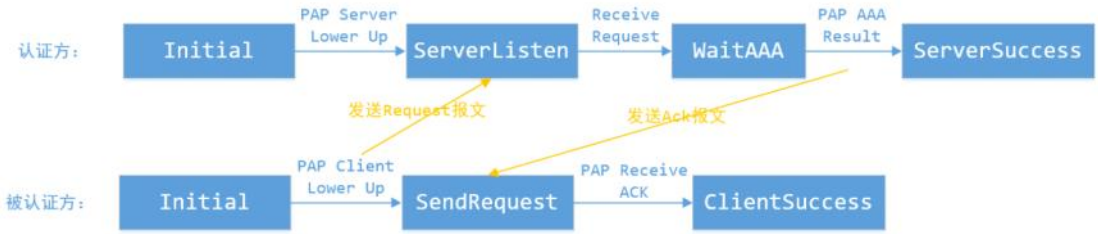
[R2-S0/0] ppp pap local-user RTB password simple aaa -->pap认证方式，通过用户RTB和密码aaa登陆

[R2-S0/0] shutdown && undo shutdown //重启端口，使配置生效。

[打开调试功能观察过程]

<R1>debugging ppp pap all

<R1>terminal debugging



a．配置CHAP认证：

```
[R1认证方]
[R1] local-user RTB class network    -->为对方配置一个用户
[R1-luser-network-RTB] service-type ppp  -->服务类型PPP
[R1-luser-network-RTB] password simple aaa   -->设置密码aaa
[R1-S0/0] ppp suthentication chap -->授权R1作为认证方
[R1-S0/0] ppp chap user RTA  -->  本方用户名RTA
```

```
[R2被认证方]
[R2] local-user RTA class network    -->为对方配置一个用户
[R2-luser-network-RTA] service-type ppp  -->服务类型PPP
[R2-luser-network-RTA] password simple aaa   -->设置密码aaa
[R2-S0/0]ppp chap user RTB  -->本方用户名RTB
[R2-S0/0] shutdown && undo shutdown  //重启端口，使配置生效。
```

[打开调试功能观察过程]

```
<R1>debugging ppp chap all
<R1>terminal debugging
```

网络实验考试复习-3

2017年12月3日 21:23

3、ospf协议实验

(1) OSPF路由协议概述

a. 区域(Area):

一个路由器的集合，相同的区域有着相同的拓扑结构。

b. OSPF基本配置:

```
[R1] router id 1.1.1.1
[R1] ospf
[R1-ospf-1] area 0
[R1-ospf-1-area-0.0.0.0]network 1.1.1.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 168.1.1.0 0.0.0.255
```

c. OSPF相关命令:

1) <R1> reset ospf all process //重启ospf进程
2) [R1] display ospf peer //查看邻居信息
3) [R1] display ospf brief(verbose) //查看概要信息
4) [R1] display ospf routing //显示ospf路由表信息
5) [R1] display ospf lsdb (router/network/summary/asbr/ase) //查看LSA信息

(2) OSPF 协议报文交互过程:

a. OSPF报文类型:

1) Hello报文:

周期性地发送给本路由器的邻居。

2) DD(Database Description Packet) 报文:

用来交换邻居路由器之间的链路信息。使用空DD报文确认主从关系。

3) LSR(Link State Request Packet)报文:

交换DD报文后，发送LSR报文请求所需的LSA。

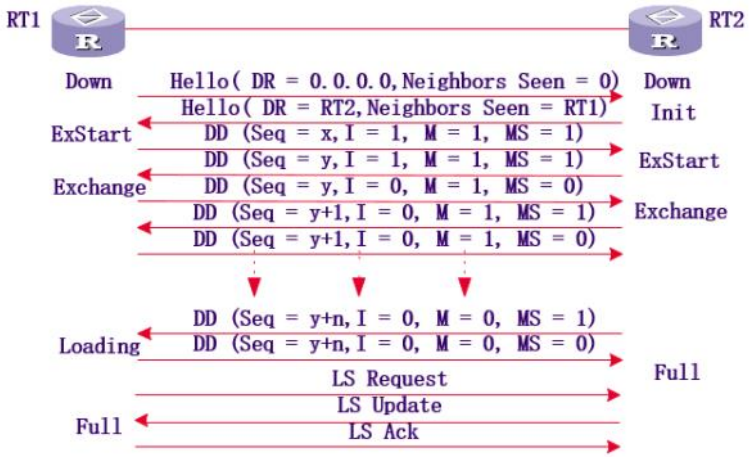
4）LSU(Link State Update)报文：

向LSR报文的发送者路由器发送LSA信息。

5）LSAck(Link State Acknowledgment)报文：

对接收到的LSU报文进行确认。

b．报文交互过程：



1）Hello 报文发现邻居

2）DD 报文(空) 进行主从关系协商

(I:是否是第一条DD，M:是否是最后一条DD，MS:是否是Master)

3）DD 报文交换

4）LSR请求

5）LSU更新

6）LSAck应答

(3) OSPF协议的链路状态描述：

a．OSPF的链路状态描述：

OSPF中，所有对路由器链路状态信息的描述都封装在**链路状态通告LSA报文**中发出。

b．OSPF的四种网络类型：

1）Stub net 网络类型：（末端网络）

Link id（网段）、data（掩码）、type（类型）、metric（花费）

2）PPP 网络类型：（点到点）

相连网段：Stub net 网络类型

相连路由：Router类型（router id、接口地址、类型、花费）

3）PTMP 网络类型：（点到多点）

相连网段：Stub net 网络类型

相连路由：Router类型

c．DR/BDR的选举过程：

DR用于传递消息。所有路由器都只将路由信息发送给 DR，再由 DR 将路由信息发送给本网段的其他路由器。BDR是备胎。

DR/BDR 一旦选举完成，除非故障，否则不会更换。

DR/BDR 的选举优先选择 Priority 高的，然后选 Router ID 大的。

d．LSA 类型：

1）第一类 LSA ： Router

描述**本路由器**运行OSPF的接口的连接状况、花费等信息。传递范围在所属区域内。（描述DRother到DR的连接）

2）第二类 LSA ： Network(Net)

DR 生成。描述网段内所有已经同其建立了邻接关系的路由器。传递范围在所属区域内。（描述网段内的路由器信息）

3）第三类 LSA ： Summary Network(SumNet)

ABR 生成。ABR 完成它所属区域中的区域内路由计算后，将本区域内的每一条OSPF路由封装发送到相邻区域。传递范围是除了第三类LSA生成的区域之外的其他区域。（描述网段内的OSPF路由信息）

4）第四类 LSA ： Asbr-Summary(SumASB)

ABR 生成。描述本区域内部到达 ASBR 的路由。传递范围为第四类LSA生成的区域之外的其他区域(描述到达ASBR的路由信息)

5）**第五类 LSA ： AS-External(ASE)**

ASBR 生成。描述道自治系统外部路由信息。传递范围为整个自治系统(除Stub区域)。

e．**路由器的类型**：

1）**IAR(Internal Area Router)：区域内路由器**

2）**ABR(Area Border Router)：区域边界路由器**

该路由器同时属于至少两个区域，且其中一个区域必须为area0

3）**BBR(BackBone Router)：骨干路由器**

至少有一个接口属于骨干区域area0，故所有ABR和area0内部路由器都是BBR。

4）**ASBR(AS Boundary Router)：自治系统边界路由器**

f．**骨干区域**：

即 area 0，要求其他所有的区域必须和骨干区域相连，并且骨干区域自身也必须是连通的。所有ABR将自身区域内路由信息收集完成后生成第三类LSA统一发送给骨干区域，再通过骨干区域将这些信息转发给其他非骨干区域。可以有效地**避免产生区域间路由回环**。

g．**配置回环**：

```
[S1] interface loop 1
[S1-LoopBack1] ip addr 4.4.4.4 255.255.255.255
```

h．**引入外部路由**：

```
[S1-ospf-1] import direct
[S1-ospf-1] import static
[S1-ospf-1] default-route-advertise cost 100
```

(4) OSPF协议路由的计算：

每台路由器使用 **SPF 算法**，**以自己为根节点**计算出一棵最短路径树。由这棵树便可得到到网络中各个节点的路由。

路由时优先选择区域内路由、区域间路由、自制系统Type1路由、自治系统Type2路由。

[为链路添加cost]

```
[S1-Vlan-interface2] ospf cost 200
[R1-Ethernet0/0] ospf cost 100
```

（5）其他：

```
[S2]ip route-static 192.168.0.0 255.255.0.0 202.112.2.1 pre 60
[R2-ospf] import-route static cost 200
```

网络实验考试复习-4

2017年12月3日 22:48

4、网络管理实验（SNMP网络管理协议）

（1）网络管理实验流程：

a. 启动 XP 桌面上的 Startup Quidview **Server** 软件。

b. 启动 XP 桌面上的 Startup Quidview **Client** 软件。

c. 用户名和密码填入admin && quidview。

d. 配置 SNMP 代理

```
[R1] snmp-agent
[R1] snmp-agent sys ver v1
[R1] snmp-agent com write private
[R1] snmp-agent com read public
[R1] snmp-agent trap enable
[R1] snmp-agent target-host trap  address udp-domain
192.168.2.10(网管站IP) params securityname public
```

e. 资源管理->自动发现，添加种子节点IP，自动发现网络拓扑。

f. 资源管理->添加设备，输入待发现的网络设备的 IP 地址和子网掩码。

（2）ASN.1 基本编码规则：

T字段(8位)：标识符

L字段(8位) ： V字段的长度

V字段：表示数据元素的值。

5、IPv6技术实验

（1）IPv6地址：

128比特。

a. 首选格式： 2001:0410:0000:0001:0000:0000:0000:45EF

b. 压缩格式： 2001:0410:0000:0001::45EF(只能压缩一次)

c. 内嵌Ipv4地址的IPv6地址：0:0:0:0:0:0:192.168.1.2

(2) IPv6地址的类型：

a. 单播地址：

1）特殊-**未指定地址**：0:0:0:0:0:0:0:0（相当于0:0:0:0）

2）特殊-**环回地址**：::1（相当于127.0.0.1）

b. 组播地址：

1）**FF01::1** ：本地接口范围内的所有节点。

2）**FF01::2** ：本地接口范围内的所有路由器。

3）**FF02::1** ：本地链路范围内的所有节点。

4）**FF02::2** ：本地链路范围内的所有路由器。

(3) IPv6实验配置：

```
[S1] ipv6 //打开 ipv6
[S1] interface vlan 2
[S2-vlan-interface2] ipv6 address 2001::1/64
[S2-vlan-interface2] undo ipv6 nd ra halt
                                    //打开nd协议的ra公告
[R1] ipv6 route-static 2001::64 2007::1 //配置静态路由

[R1] ospfv3 1
[R1-ospfv3-1] router-id 2.2.2.2
[R1-ospfv3-1] import-route direct
[R1] interface e0/0
[R1-Ethernet0/0] ospfv3 1 area 0 //此端口开启ospf并设置区域
为0
```

(4) netsh interface ipv6命令:

```
[cmd] netsh
[cmd] netsh > interface
[cmd] netsh interface > ipv6
[cmd] netsh interface ipv6 > show join  //显示加入的多播组
[cmd] netsh interface ipv6 > show address //显示当前IP地址
[cmd] netsh interface ipv6 > show route  //显示路由表项目
[cmd] netsh interface ipv6 > show neighbors interface=5
                                          //查看邻居
[cmd] netsh interface ipv6 > show destinationcache
                                          //查看目的缓存表
```

(5) 查看OSPFv3路由表:

```
Display ipv6 routing-table //查看ipv6路由表
Display ospfv3 lsdb //查看LSDB
```

Ping 命令:

```
Ping ipv6 2001::1
```

(6) on-link 和 off-link的不同:

On-link 是链路内的link过程，直接访问主机获取mac。而off-link是链路间的link过程，需要通过路由器获取mac。

(7) ND协议:

a. RS(路由器请求报文):

主机发出，希望路由器回复路由信息。Hop limit为255，防止有别的链路的RS来欺骗。ICMPv6 options包含发送者的MAC地址。目的地址是FF02::2

b. RA(路由器通告报文):

对 RS 报文的回复信息。路由器选项包括路由器的MAC地址、MTU、前缀信息等。目的地址是FF02::1。

c. NS(邻居请求报文):

用于**解析邻居的MAC地址** && **重复地址检测**(IP报文中源地址为0地址，并且ICMPv6中无选项字段)

d. NA(邻居公告报文):

R:路由器标记(1路由器 0主机)

S:请求标记（1对NS报文的响应 0主动发出的)

O:覆盖标记（1可用NA中目标MAC地址覆盖邻居缓存表 0只有在不知道的时候可以使用更新邻居缓存表)

(8) MLD组播侦听者发现协议:

a. 路由器发出 **组播侦听者查询报文** 查询本地组播成员。

b. 主机发出 **组播侦听者报告报文** 宣告自己加入的组播组。

c. 路由器接收到 报告报文后 添加相关表项。

d. 主机离开组播组时 发出 **组播侦听者完成报文。**

需要路由器进行处理，所以设置了 Hop-by-hop选项头，让路由器来进行处理。Hop limit为1，以使MLD报文限制在链路本地上。

(9) ospfv3协议:

a. 8类LSA: Link-LSAs

描述链路本地信息。

b. 9类LSA: Intra-Area-Prefix-LSAs

描述网络前缀。

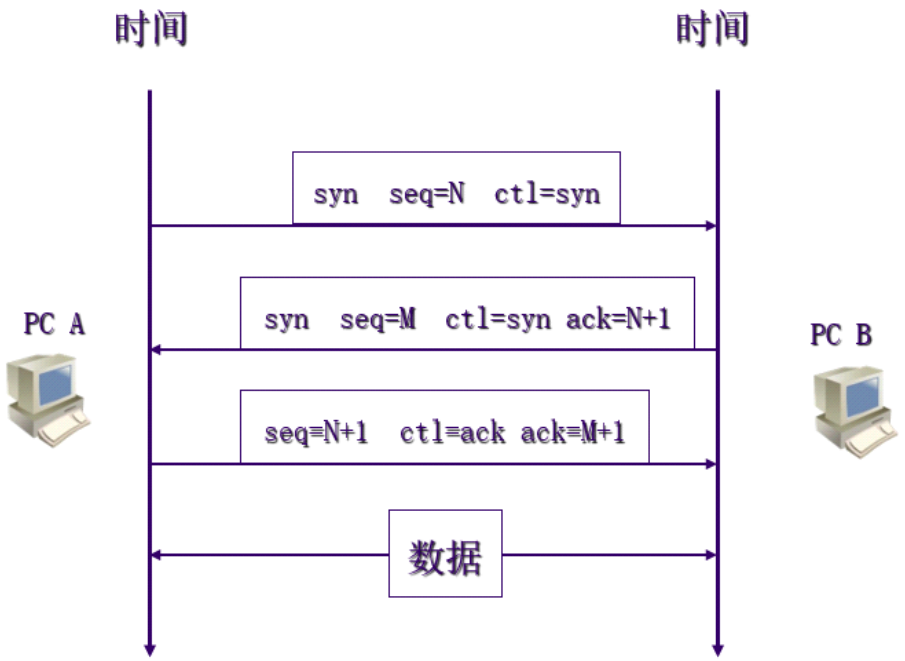
网络实验考试复习-5

2017年12月4日 0:45

7、传输层实验

（1）TCP协议基本分析

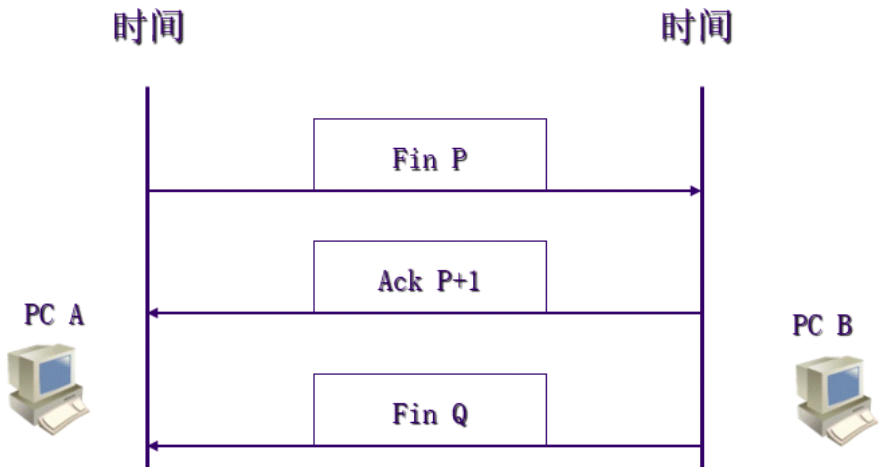
a．连接建立过程 - 三次握手：

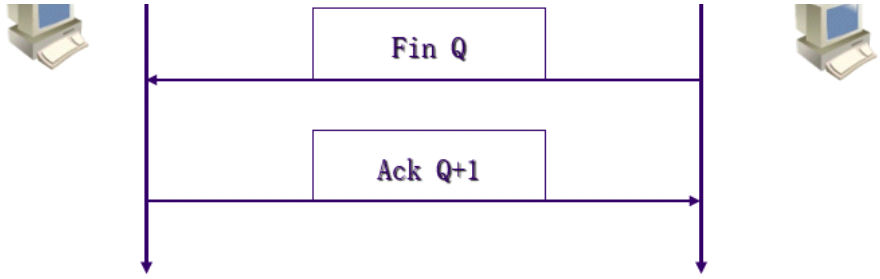


option字段的MSS =

MTU(1518)-帧头帧尾(18)-IP/TCP首部(40) = 1460

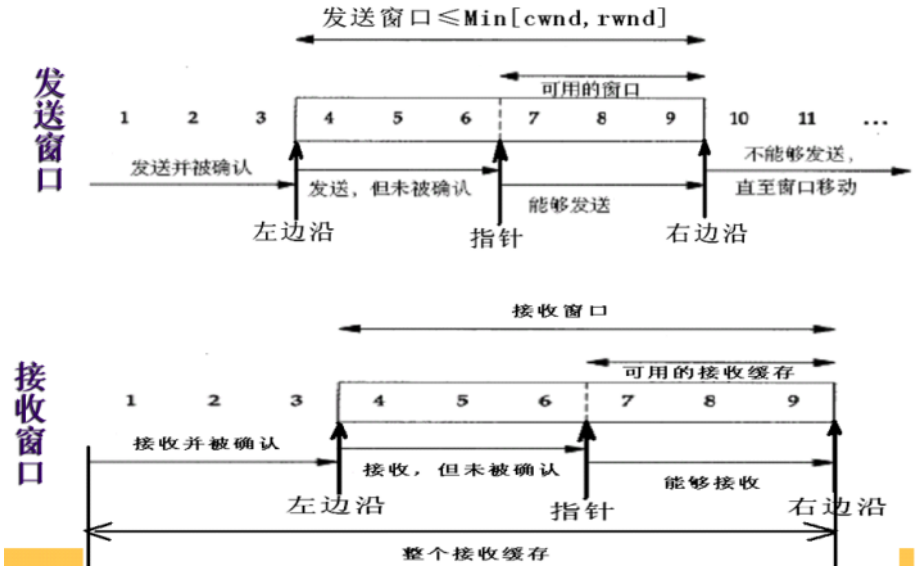
b．连接撤销 - 四次确认：





（2）拥塞控制机制

a．滑动窗口机制：



(5) ARP协议分析:

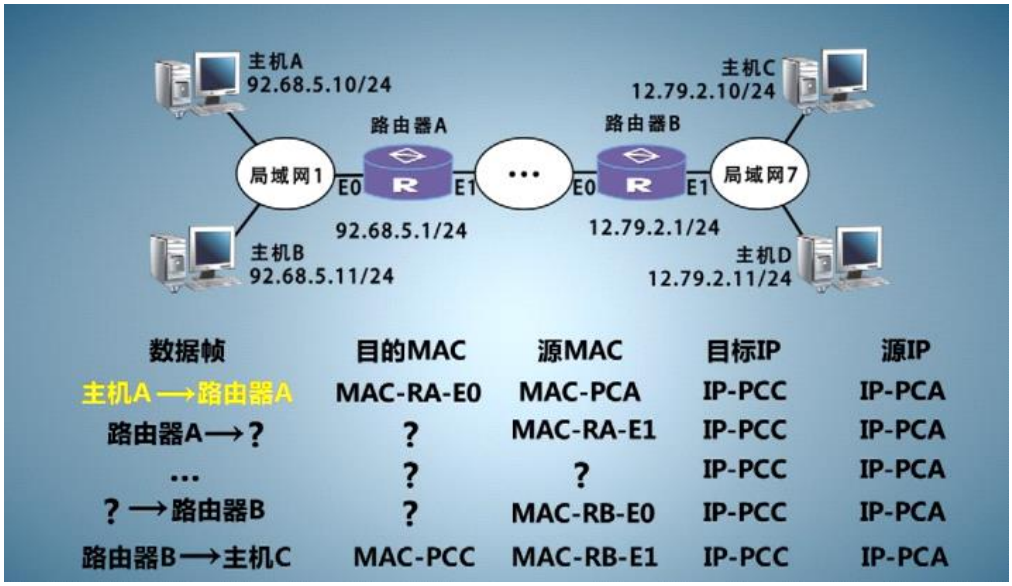
a. ARP协议:

APR是**地址解析协议**，用于将计算机的网络地址转化为物理地址(32位IP-->48位MAC)

解决同一局域网主机的**IP地址和MAC地址的映射**问题。

b. IP数据报格式:

c. 传输过程:



A-->B

A先查找自身的ARP缓存，如果有B的MAC地址则发送。未找到时:

i) A广播ARP请求包（我是A的IP&&MAC，谁知道IP为？？的MAC地址）。

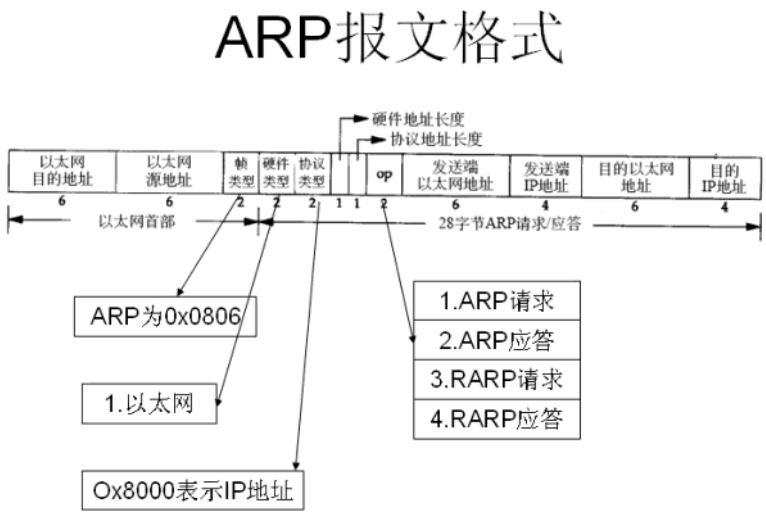
ii）同一网络内的所有主机都能收到，但只有对应IP地址的主机回应ARP。

iii）主机B将A的IP&&MAC存入缓存，并向主机A发送响应报文。

iv）A将B的IP&&MAC存入缓存。

请求报文广播，应答报文单播

d．报文格式：



e．查看PC机上的 ARP缓存表：

```
[cmd] arp -a //查看arp缓存表
[cmd] arp -d //清空arp缓存表
```

清空交换机 ARP 缓存：

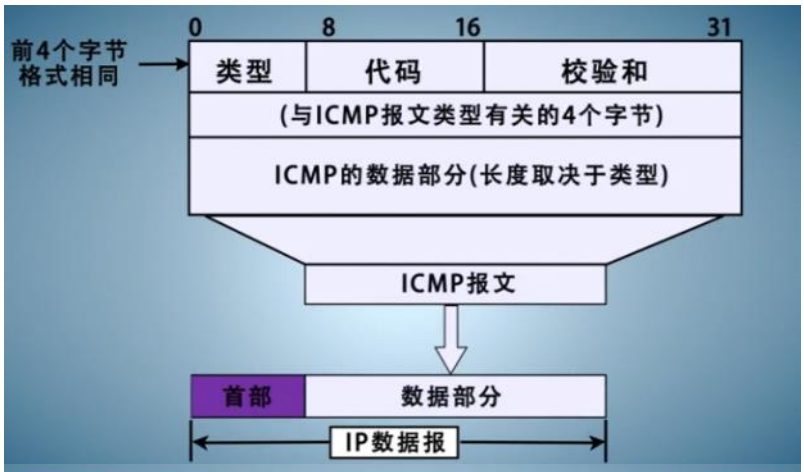
```
<S1> reset arp all
```

(6)ICMP协议分析：

a．ICMP协议：

允许路由器和主机报告差错情况，并用于调试。

b．不同ICMP有不同格式，但前4个字节格式相同。



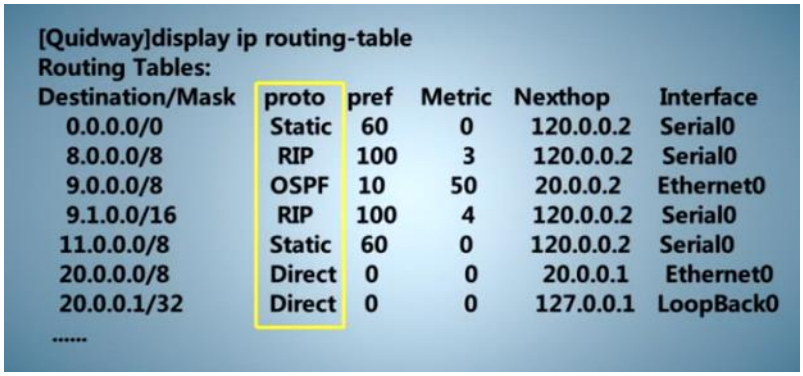
类型	ICMP报文功能	类型	ICMP报文功能
0	回送应答，构成常用的ping命令	13	时戳请求
3	信宿不可达	14	时戳应答
4	信源抑制，用于流控和拥塞控制	15	信息请求（已不用）
5	重定向（改变路由）	16	信息应答（已不用）
8	回送请求，构成常用的ping命令	17	地址掩码请求
11	数据报超时，超过分组生成周期	18	地址掩码应答
12	数据报参数错		

c．差错报告报文：

路由器无法将数据报发送到目的地时，只能丢弃，这时向发送端返回差错报告报文。

(7) IP协议分析：

a．路由表：



a）目的地址/掩码长度

b）发现该路由的路由协议（路由来源）-->静态路由（人工配置），RIP（动态），OSPF（动态），Direct（直连路由，链路层协议发现，本接口网段）

c）优先级(越小越高)

d）花费

e）路由的下一跳地址

f）端口，将从这个端口发出

b．最长匹配原则：

如9.1.1.8-->发送到9.1.0.0对应的120.0.0.2

c．查看路由表：

```
[S1] display ip routing-table
```

（8）静态路由和默认路由的配置：

```
[R1] ip route-static 0.0.0.0 0.0.0.0 192.168.5.1
[R1] ip route-static 192.168.2.0 255.255.255.0 192.168.1.1
```

(静态路由引入ospf : `[S1-ospf] import-route static`)

(默认路由引入ospf : `[R1-ospf-1] default-route-advertise cost 100`)