计算机网络课程第二次实验 ---- VLAN、路由配置与访问控制列表

2011年10月18日

1. **实验目的：**

本次实验主要目的是使学生掌握虚拟局域网的工作原理与基本配置命令；掌握路由器路由协议的配置方法与访问控制列表的配置。本实验将涉及计算机网络的物理层、数据链路层、网络层等不同层次相关内容。

1. **实验内容：**

本实验共包含以下三个子实验的内容：

1. 实验三 VLAN基础配置：掌握虚拟局域网的工作原理和基本配置命令。
2. 实验四 路由器及路由协议的配置：掌握路由器及常用路由协议的基本配置方法。
3. 实验五 访问控制列表配置：掌握交换机上配置访问控制列表的基本方法。
4. **实验设备：**

实验设备共分10组，每4人组成一组，每组的实验设备具体组成如下：

（1） 华为AR28-31路由器： 1台

（2） 华为S3500交换机： 1台

（3） 华为S2403-H交换机： 2台

（4） PC机： 4台

1. **实验要求：**

每位同学需独立完成实验三，实验四，实验五共三个子实验的内容。每完成一个子实验的内容请联系助教确认相关实验的结果。

为了确保在规定时间内正确完成相关实验，请各位同学在做实验之前一定要认真阅读相关资料，做好实验的准备工作。在实验过程中，请爱护实验室的各种设备。除必要的设备连接及设置外，不要随意改变实验室设备的位置及设备的其他设置。如有必要变动设备位置或修改设备的其他设置时，请和助教或指导老师事先联系。每次做完实验离开之前，请每位同学Shutdown自己使用的PC机，并关掉显示器。每组最后一个完成实验的同学请关掉本组的设备电源总开关。

**实验三 VLAN基础配置**

1. **实验目的：**

掌握虚拟局域网的工作原理、基本配置命令和配置注意事项。

1. **VLAN的基础知识**

VLAN（Virtual Local Area Network），是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段从而实现虚拟工作组的技术。IEEE于1999年颁布了用以标准化VLAN实现方案的IEEE 802.1Q协议标准草案。

VLAN技术允许网络管理者将一个物理的LAN逻辑地划分成不同的广播域（或称虚拟LAN，即VLAN），每一个VLAN都包含一组有着相同需求的计算机，由于VLAN是逻辑地而不是物理地划分，所以同一个VLAN内的各个计算机无须被放置在同一个物理空间里，即这些计算机不一定属于同一个物理LAN网段。

如在一个公司内部，相同的部门之间实现二层互通，不同的部门之间隔离，而这些部门是分散到不同的交换机上，这个时候就可以在各台交换机上将属于一个部门的端口划分到相同的vlan里，交换机之间互连的端口使用trunk属性，这样就可以实现vlan的交换机间互通；

* VLAN划分有四种方式：

1. 基于端口的划分：交换机的某些端口分属不同VLAN，连接在端口下的主机即属于相应的VLAN。优点是定义VLAN成员非常简单；但是如果VLAN用户离开原来的接入端口，连接到新端口，就必须重新指定新端口所属的VLAN号。
2. 基于MAC地址的划分：某个主机属于哪个VLAN只与它的MAC地址有关。优点是用户改变物理位置（接入端口）时，不用重新配置；但是初始的配置工作量很大。
3. 基于协议的划分：某个主机属于哪个VLAN只与它运行的网络协议有关（如IP协议和IPX协议）。这种方法实际应用中非常少，因为目前绝大多数是IP协议的主机，无法将广播域划分得更小。
4. 基于子网的划分：根据主机所有的IP地址所在的网络子网来划分广播域。优点是管理配置灵活，用户自由移动位置而不需要重新配置交换机或主机，但是为了判断用户的属性，必须检查每个数据包的网络层地址，将消耗交换机的不少资源；并且同一个端口可能存在多个VLAN用户，将导致广播报文的抑制效率下降。

综上所述，基于端口划分VLAN是最普遍使用的一种方法，也是目前所有交换机都支持的方法。有少量交换机支持基于MAC地址的VLAN划分。

1. **VLAN配置**

对VLAN进行配置时，首先应根据需求创建VLAN。

VLAN配置包括：

              开启/关闭设备VLAN特性

              创建/删除VLAN

              为VLAN指定以太网端口

              为VLAN指定描述字符

              对以太网端口进行VLAN相关设置

1. 开启/关闭设备VLAN特性

当交换机的VLAN特性被关闭后，交换机在报文交换的过程中将不再使用VLAN标记，从而失去了VLAN域的隔离功能。可以使用下面的命令来开启/关闭设备VLAN特性。

请在系统视图进行下列配置。

|  |  |
| --- | --- |
| 操作 | 命令 |
| 开启/关闭VLAN特性 | **vlan** { **enable | disable** } |

1. 创建/删除VLAN

可以使用下面的命令来创建/删除VLAN。创建VLAN时，如果该VLAN已存在，则直接进入该VLAN视图；如果该VLAN不存在，则此配置任务将首先创建VLAN，然后进入VLAN视图。

请在系统视图下进行下列配置。

|  |  |
| --- | --- |
| 操作 | 命令 |
| 创建VLAN并进入VLAN视图 | **vlan** *vlan\_id* |
| 删除已创建的VLAN | **undo vlan**{ *vlan\_id* [ **to** *vlan\_id* ] | **all** } |

需要注意的是，缺省VLAN1不能被删除。

1. 为VLAN指定描述字符

可以使用下面的命令来指定VLAN的描述字符。请在VLAN视图下进行下列配置。

| 操作 | 命令 |
| --- | --- |
| 为VLAN指定一个描述字符串 | **description** *string* |
| 恢复VLAN的描述字符串为缺省描述 | **undo description** |

缺省情况下，VLAN缺省描述字符串为该VLAN的VLAN ID，例如“VLAN 0001”

1. 为VLAN指定以太网端口

可以使用下面的命令为VLAN指定以太网端口。请在VLAN视图下进行下列配置。

|  |  |
| --- | --- |
| 操作 | 命令 |
| 为指定的VLAN增加以太网端口 | **port** *interface\_list* |
| 删除指定的VLAN的某些以太网端口 | **undo port** *interface\_list* |

缺省情况下，系统将所有端口都加入到一个缺省的VLAN中，该VLAN的ID为1。

需要注意的是，Trunk和Hybrid端口只能通过以太网端口视图下的**port**和**undo port**命令加入VLAN或从VLAN中删除，而不能通过本命令实现。

1. VLAN显示和调试

在完成上述配置后，在所有视图下执行display命令可以显示配置后VLAN的运行情况，通过查看显示信息验证配置的效果。

|  |  |
| --- | --- |
| 操作 | 命令 |
| 显示VLAN相关信息 | **display** **vlan** [ *vlan\_id* | **all** | **static** | **dynamic** ] |

1. 以太网端口VLAN相关设置
2. 把当前以太网端口加入到指定VLAN

请在以太网端口视图下执行下列相应命令。

* + 把当前Access 端口加入到指定VLAN

**port access vlan** *vlan\_id* （Access 端口只能加到1 个VLAN 中）

* + 将当前Hybrid 端口加入到指定VLAN

**port hybrid vlan** *vlan\_id\_list* { **tagged** |**untagged** } （可以加到多个VLAN 中）

* + 把当前Trunk 端口加入到指定VLAN

**port trunk permit vlan** { *vlan\_id\_list* |**all** } （可以加到多个VLAN 中）

* + 把当前Access端口从指定VLAN删除： **undo port access vlan**
  + 把当前Hybrid端口从指定VLAN中删除：**undo port hybrid vlan** *vlan\_id\_list*
  + 把当前Trunk端口从指定VLAN中删除：**undo port trunk permit vlan** { *vlan\_id\_list* | all }

1. 设置以太网端口缺省VLAN ID

Access 端口只属于1 个VLAN，所以它的缺省VLAN就是它所在的VLAN，不用设置。

Hybrid 端口和Trunk 端口属于多个VLAN，所以需要设置缺省VLAN ID。如果设置了端口的缺省VLAN ID，当端口接收到不带VLAN Tag 的报文后则将报文转发到属于缺省VLAN 的端口。当端口发送带有VLAN Tag 的报文时，如果该报文的VLAN ID 与端口缺省的VLAN ID 相同，则系统将去掉报文的VLAN Tag，然后再发送该报文。

* + 设置Hybrid端口的缺省VLAN ID：**port hybrid pvid vlan** *vlan\_id*
  + 设置Trunk端口的缺省VLAN ID：**port trunk pvid vlan** *vlan\_id*
  + 恢复Hybrid端口的缺省VLAN ID为缺省值：**undo port hybrid pvid**
  + 恢复Trunk端口的缺省VLAN ID为缺省值：**undo port trunk pvid**

1. VLAN配置实例
2. PVID配置实例
3. 组网需求

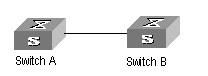
以太网交换机Switch A与对端交换机Switch B使用Trunk端口Ethernet0/16相连，本例将为该Trunk端口配置缺省的VLAN ID，验证port trunk pvid vlan命令的使用。port trunk pvid vlan的典型应用是当接收到没有标记的报文时，该Trunk端口将此报文发往缺省VLAN ID标识的VLAN。

Trunk属性是在交换机使用过程中经常用到的一种以太网端口链路类型，简单介绍一下经常用到的几种情况：

 如在一个公司内部，相同的部门之间实现二层互通，不同的部门之间隔离，而这些部门是分散到不同的交换机上，这个时候就可以在各台交换机上将属于一个部门的端口划分到相同的vlan里，交换机之间互连的端口使用trunk属性，这样就可以实现vlan的交换机间互通；

 在一个组网中，用户接入使用二层交换机，如果要实现这个二层交换机上的vlan之间三层互通，一般需要将这些vlan透传到一个三层设备，可以是三层交换机或者路由器，由这些三层设备实现用户三层的互通，这时就需要在二层交换机与三层设备互连的端口设置成trunk属性；

1. 组网图



1. 配置步骤

以下只列出了Switch A的配置，Switch B应作类似的配置：（以第一组第1位同学的设置为例）

<S2403H-1-1> system-view //进入系统视图，配置系统参数，出现[ ]符号

[S2403H-1-1] vlan 101 // 创建VLAN 101。同组成员间不重复即可。例如

同组4位同学分别使用101, 102, 103, 104等。

[S2403H-1-1-vlan101] quit

[S2403H-1-1] interface ethernet0/16 // 进入Ethernet0/16以太网端口视图。同组同学使用

的端口号不要重复即可。例如同组4位同学分别使

用e0/16, e0/17, e0/18, e0/19等。

[S2403H-1-1-Ethernet0/16] port link-type trunk // 配置端口Ethernet0/16为Trunk端口

[S2403H-1-1-Ethernet0/16] port trunk permit vlan 2 to 50 101 //允许2到50、101等VLAN通过。

[S2403H-1-1-Ethernet0/16] port trunk pvid vlan 101 // 配置端口Ethernet0/16的缺省VLAN ID为100。

[S2403H-1-1-Ethernet0/16] display interface e0/16 //可以看到端口为trunk端口，PVID为101

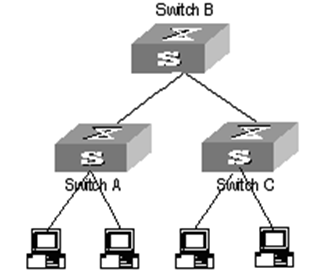
[S2403H-1-1-Ethernet0/16] quit

[S2403H-1-1] undo vlan 101 //删除VLAN101

1. VLAN组网配置实例
2. 组网需求：

下图中Switch B为S3500具有路由功能的三层交换机,Switch A和Switch C为S2403二层交换机。Switch A和Switch C通过ethernet0/25口连接至Switch B,用户主机接在Switch A和Switch C。

请在此网络拓扑之上，参照以上的说明，创建一个VLAN.



二层交换机上只能有一个Vlan配置IP地址，一般为管理vlan。我们创建的vlan虽然在二层上不能显示其interface,但我们可以通过ping测试它确实是存在的，而且也可实现内部通信。

1. 配置步骤
2. 在三层交换机上创建vlan,并为其分配IP地址：

先查看台式机IP地址和网关（下划线表示该数值需要根据组号或座位而改变）。 telnet 至用户网关，如：192.168.1.254 //1根据组号而改变

在系统视图下（system-view），

[S3500-1] vlan 101 //创建101号vlan，vlan号>100，个位数与台式机IP

地址末位相同

[S3500-1-vlan101] quit

[S3500-1] interface vlan-interface 101 //进入vlan101的接口视图

[S3500-1-Vlan-interface101] ip address 172.17.1.254 255.255.255.0

//为vlan101分配网段，如172.17.1.0 /24 ,可以从此网段中任选一地址作为网关地址，其余作为用户地址。

[S3500-1- Vlan-interface101] quit

注意： ①Vlan号 1- 4均已使用，请勿覆盖、删除。

②各人选取的网段不能相互重叠，也不能与已分配的网段重叠。因此，

组1 使用IP地址为 172.17.1~5.0 /24

组2 使用IP地址为 172.17.6~10.0 /24

组3 使用IP地址为 172.17.11~15.0 /24

组4 使用IP地址为 172.17.16~20.0 /24

组5 使用IP地址为 172.17.21~25.0 /24

组6 使用IP地址为 172.17.26~30.0 /24

组7 使用IP地址为 172.17.31~35.0 /24

组8 使用IP地址为 172.17.36~40.0 /24

组9 使用IP地址为 172.17.41~45.0 /24

组10 使用IP地址为 172.17.46~50.0 /24

1. 将三层交换机port加入新建的VLAN：

[s3500-1] interface ethernet0/11 //进入port视图，1与台式机IP地址末位相同

[S3500-1-Ethernet0/11] port link-type access //设置port为access模式

[S3500-1-Ethernet0/11] port access vlan 101 //将port划分到vlan101，

[S3500-1-Ethernet0/11] display vlan 101 //检查vlan IP地址和port划分状况

1. 将自己的网线插到三层交换机port11
2. 设置用户机器的ip地址和网关：

ip:172.17.1.1 //用户ip可在自己所配网段内任选

网关:172.17.1.254 //VLAN101的IP地址即为网关

掩码：255.255.255.0

1. 测试：

（1）使用ping命令在vlan间测试，也可ping至二层和三层的交换机。

Ping 172.17.1.254 网关是否通？

（2）在三层交换机上使用display interface Ethernet 0/11可以看到端口为access端口，PVID为101

1. 将用户机器的网线不是插在三层交换机上，而是插到二层交换机上，做如下配置：

检查三层交换机与二层交换机连接的端口是否设置为trunk端口，是否允许属于相应vlan 的信息通过（本实验室已配置），若不是，参照第8)步进行设置。

**[S3500-1] display interface Ethernet 0/23 //**三层交换机与下面一个二层交换机连接的端口

**[S3500-1] display interface Ethernet 0/22 //**三层交换机与上面一个二层交换机连接的端口

1. 在二层交换机上建vlan101并为其划分port:

telnet 172.16.11.3 //1 为组号，3 为机柜最下面的二层交换机IP地址末位数

[S2403H-1-2] vlan 101 //创建VLAN101

[S2403H-1-2-vlan101]quit

[S2403H-1-2] interface ethernet0/11 //进入port视图，port编号ethernet0/1至0/24，可从中任选,但组内同学使用的端口不能相互重叠。例如1选用PC机IP地址最末位，即同组4位同学分别使用e0/11, e0/12, e0/13, e0/14等。

[S2403H-1-2-Ethernet0/11] port link-type access //设置port为access模式

[S2403H-1-2-Ethernet0/11] port access vlan 101 //将port划分到vlan101

[S2403H-1-2-Ethernet0/11] quit

1. 配置二层交换机Ethernet0/25为Trunk端口，允许所有VLAN通过。（本实验室已配置）

如果没有配置为Trunk端口，则可以使用以下命令将Ethernet0/25设置为Trunk端口。

[S2403H-1-2] interface ethernet0/25

[S2403H-1-2-Ethernet0/25] port link-type trunk

[S2403H-1-2-Ethernet0/25] port trunk permit vlan all

[S2403H-1-2-Ethernet0/25] quit

1. 将自己的网线插到二层交换机port11(即Ethernet 0/11)，进行测试。

（1）使用ping命令在vlan间测试，也可ping至二层和三层的交换机。

Ping 172.17.1.254 网关是否通？

（2）在二层交换机上使用display interface Ethernet 0/11可以看到端口为access端口，PVID为101

1. [S2403H-1-2] undo vlan 101 //删除VLAN101

**注意：Vlan号 1- 4均已使用，请勿覆盖、删除。**

1. **思考：**如果完成第4步后，ping不通自己配置的网关，用什么办法再登录交换机进行检查和修改配置？
2. **实验要求**
3. 试验各种相关命令
4. 验证配置实例
5. 思考并解答相关思考问题

**实验四 路由器接口及路由协议的配置**

1. **实验目的：**

本实验的主要目的是使学生了解路由器的接口类型并掌握基本的路由器接口设置方法。同时掌握RIP及OSPF两种常用路由协议的配置方法。为后续网络设计及实现的相关实验做准备。

1. **路由器接口及其配置：**

在因特网中进行路由选择要使用路由器，路由器根据所收到的报文的目的地址选择一条合适的路由（通过某一网络），将报文传送到下一个路由器，路由中最后的路由器负责将报文送交目的主机。

1. **路由器接口**

路由器的接口即指路由器系统与网络中的其它设备交换数据并相互作用的部分，其功能就是完成路由器与其它网络设备的数据交换。

路由器一般支持物理接口和逻辑接口这两类接口。物理接口就是真实存在、有对应器件支持的接口，如以太网接口、同/异步串口等。物理接口又分为两种，一种是LAN（局域网）接口，主要是指以太网接口，路由器可以通过它与本地局域网中的网络设备交换数据；另一种是WAN（广域网）接口，包括同/异步串口、AUX接口、AM接口、CE1/PRI接口、ISDN BRI接口等，路由器可以通过它们与外部网络中的网络设备交换数据。

逻辑接口是指能够实现数据交换功能但物理上不存在、需要通过配置建立的接口，包括Dialer（拨号）接口、子接口、备份中心逻辑通道以及虚拟接口模板等。

以太网接口分为电接口和光接口两种，支持100-1000Mbit/s，本实验室的以太网接口为10-100Mbit/s的电接口。实验室的网络拓扑结构是：10台AR28-31各自通过以太网端口与AR46-40的十个以太网端口相连，10台AR28-31又用电缆在各自的同步串口间相连，形成环状。因此我们主要熟悉这两类端口。

1. **路由器接口配置方法**
2. 进入接口的视图：在系统视图下执行以下命令。

interface *type number*

1. 设置接口描述：

路由器的物理接口都有一个接口描述配置项，接口描述主要用来帮助识别接口的用途。请在接口视图下进行下列配置。

* 设置接口描述：description *interface-description*
* 恢复缺省的接口描述：undo description

1. 显示接口信息：

在所有视图下：display interface [*type number* ]

在进一步配置一个接口前需要对组网需求和组网图有一个完整详细的了解。具体配置一个接口至少需要完成以下几个工作：

1. 如果该接口是物理接口需要明确其连接情况接口工作方式及相关工作参数。
2. 如果该接口是广域网接口则需要配置链路层协议以及工作参数等。本项设置要与相连的对端接

口相适应。

1. 配置该接口的网络协议如IP 协议地址。
2. 配置通过该接口能达到的目的网络的静态路由或者配置动态路由协议在该接口上的工作参数。
3. 如果该接口支持拨号则需要配置DCC 工作参数以及对Modem 的管理等。

在接口视图下，需要配置的参数较多，本部分主要介绍物理接口所特有的一些参数的配置，同时，对逻辑接口的定义做简单介绍。有关链路层、网络层协议和参数的配置以及一些特殊功能的配置（如拨号等）本部分将不再赘述。

1. **以太网接口配置方法**

以太网接口配置包括：

1. 进入指定以太网接口的视图：在系统视图下执行以下命令。

**interface** *Ethernet number*

后续以太网接口有关的各种命令都必须在相应的接口视图下使用。

1. 设置网络协议地址：

设置接口的IP地址： **ip address** *ip-address mask* [ **sub** ]

取消接口的IP地址： **undo ip address** [ *ip-address mask* ] [ **sub** ]

1. 设置MTU:

MTU（Maximum Transmission Unit，最大传输单元）参数影响IP报文的分片与重组。

请在以太网接口视图下进行下列配置。

设置MTU: **mtu***size*

恢复MTU的缺省值: **undo mtu**

*size* 的值为46 - 1500byte。缺省的MTU为1500。

1. 选择以太网接口的工作速率：**speed { 10 | 100 | negotiation }**

恢复缺省的工作速率: **undo speed。**

缺省速率选择**negotiation**，即系统自动协商

1. 选择以太网接口的工作方式：**duplex { negotiation | full | half }** 缺省情况下为**negotiation** 方式，即系统自动协商。
2. 允许或禁止对内自环：

在对以太网接口作特殊功能测试时，有时需要将其设为对内自环。可以在以太网接口视图下进行下列配置，允许其对内自环。

允许对内自环：**loopback**

禁止对内自环：**undo loopback**

缺省为禁止对内自环。

1. 设置太网接口的流控方式：

设置千兆以太网流控： **flow-control**

恢复缺省设置：**undo flow-control**

缺省情况不启用流控。如本端启用流控，那么只有在对端也支持流控时才有效。

请进入接口视图进行参数配置，具体的配置命令可在接口视图下输入“？”获得帮助。**具体的配置本实验室已经设置好**，可以用“display interface ethernet”来查看。

1. **同步串口配置方法**

同步串口特性：

* 可以工作在DTE（Data Terminal Equipment）和DCE（Data Circuit-terminating Equipment）两种方式，一般情况下，同步串口作为DTE设备，接受DCE设备提供的时钟。
* 同步串口可以外接多种类型电缆，如V.24、V.35、X.21、RS449、RS530等。VRP可以自动检测同步串口外接电缆类型，并完成电气特性的选择，一般情况下，无需手工配置。
* 同步串口支持的链路层协议包括PPP、帧中继、LAPB和X.25等。
* 支持IP和IPX网络层协议。
* 可以通过执行**display interface serial**命令，查看同步串口的当前外接电缆类型以及工作方式（DTE/DCE）等信息。

同步串口的配置包括以下步骤：

1. 进入指定的同/异步串口的视图：在系统视图下运行 **interface serial** *interface-number*

后续同步串口参数设置命令均在同/异步串口视图下运行。

1. 设置同/异步串口工作在同步方式： **physical-mode sync**
2. 设置链路层协议： **link-protocol { fr | hdlc | lapb | ppp | sdlc | x25 }**

同步串口的链路层协议可以为PPP、LAPB、X.25、Frame Relay、HDLC、SDLC等。缺省选用PPP 链路层协议

1. 设置数字信号编码格式：

同步串口支持两种数字信号编码格式：NRZ（不归零）编码和NRZI（反向不归零）编码。缺省使用NRZ 编码格式。

使用NRZI 编码格式： **code nrzi**

使用NRZ编码格式：**undo code**

1. 设置波特率： **baudrate** *baudrate* 缺省波特率为64000bps

两个同步串口相连时，线路上的波特率由DCE侧决定。因此，当同步串口工作在DCE方式下，需要用**baudrate**命令设置接口波特率；如果作为DTE设备使用，则接口波特率通过协商从对端（DCE侧）获得。

1. 选择工作时钟： **clock** { dteclk1 | dteclk2 | dteclk3 | dteclk4 }

同步串口有两种工作方式：DTE（Data Terminal Equipment）和DCE（Data Circuit-terminating Equipment），不同的工作方式有不同的工作时钟选择。

1. 如果同步串口作为DCE设备，则需要向对端DTE设备提供时钟，此时需要选择DCEclk；
2. 如果同步串口作为DTE设备，则需要接受对端DCE设备提供的时钟，由于同步设备的接收和发送时钟是独立的，则DTE设备的接收时钟可以选择DCE设备的发送或接收时钟，DTE设备的发送时钟也可以选择DCE设备的发送或接收时钟，由此产生四种组合，即在DTE侧可以有四种时钟选择。

DCE 侧同步串口缺省时钟为dceclk，不需要配置；DTE 侧同步串口缺省时钟选择

为dteclk1

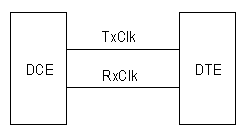


图4-1 同步串口时钟选择示意图

同步串口作为DTE侧的时钟选择方法：

|  |  |
| --- | --- |
| 选择方法 | 意义 |
| DTE1 | TxClk = TxClk, RxClk = RxClk |
| DTE2 | TxClk = TxClk, RxClk = TxClk |
| DTE3 | TxClk = RxClk, RxClk = TxClk |
| DTE4 | TxClk = RxClk, RxClk = RxClk |

TxClk为发送时钟，RxClk为接收时钟；“=”前为DTE侧时钟，“=”后为DCE侧时钟。

1. 配置MTU：

设置同步串口的MTU：**mtu** *size*

恢复MTU的缺省值：**undo** **mtu**

缺省MTU值为1500。

1. 配置keepalive报文发送周期：

串口会在每个keepalive周期向对端发送keepalive报文，用以检测链路状态是否正常。

请在串口视图下进行下列配置。缺省情况下，keepalive报文的发送周期为10秒。

设置keepalive报文发送周期：**timer hold** *seconds*

恢复keepalive报文发送周期缺省值：**undo timer hold**

1. **逻辑接口配置方法**

逻辑接口指能够实现数据交换功能但物理上不存在、需要通过配置建立的接口，包括Dialer（拨号）接口、子接口、LoopBack接口、NULL接口、备份中心逻辑通道以及虚拟模板接口等等。

由于时间等条件所限，本次实验不进行逻辑接口的设置练习，在此只对其进行简单介绍。

1. Dialer 接口：拨号接口。有同步串口、异步串口、ISDN BRI 接口和ISDN PRI 接口。
2. LoopBack接口：TCP/IP 协议规定127.0.0.0 网段的地址属于环回地址，包含这类地址的接口属于环回接口。华为系列路由器上定义了Loopback0 为环回接口，可以用来接收所有发送给本机的数据包。
3. Null 接口：是一种纯软件性质的逻辑接口，任何送到该接口的网络数据报文都会被丢弃。它永远处于Up状态，但不能转发数据包，也不能配置IP地址或配置其它链路层协议。
4. 子接口：在一个物理接口上配置出来的多个逻辑上的虚接口，这些虚接口共用物理接口的物理层参数又可以分别配置各自的链路层和网络层，为用户提供了很高的灵活性。
5. 虚拟接口模板（Virtual-Template）：是用于配置一个虚拟接口的模板，主要应用于VPN及MP等应用环境。在VPN 会话连接建立之后或将多个PPP 链路捆绑成MP 之后需要创建一个虚拟接口用于和对端交换数据，此时系统将按照用户的配置选择一个虚拟接口模板，根据该模板的配置参数动态地创建一个虚拟接口。
6. **路由协议的配置**

在因特网中进行路由选择要使用路由器，路由器根据所收到的报文的目的地址选择一条合适的路由（通过某一网络），将报文传送到下一个路由器，路由中最后的路由器负责将报文送交目的主机。

1. **路由表**

路由器转发分组的关键是路由表，每个路由器中都保存着一张路由表。表中每条路由项都指明分组到某子网或某主机应通过路由器的哪个物理端口发送，然后就可到达该路径的下一个路由器，或者不再经过别的路由器而传送到直接相连的网络中的目的主机。

那么，路由表表项是如何生成的呢？路由表生成的方法可分为两大类：手工静态配置和动态协议生成，对应地，路由协议可划分为：静态路由、动态路由协议两类。其中动态路由协议又包括TCP/IP协议栈的RIP（Routing Information Protocol，路由信息协议）、OSPF（Open Shortest Path First，开放式最短路由优先）协议、OSI参考模型的IS-IS（Intermediate System to Intermediate System）协议等。

1. 路由表中关键项：
2. 目的地址(Destination)：用来标识IP 包的目的地址或目的网络
3. 网络掩码(Mask)：与目的地址一起来标识目的主机或路由器所在的网段的地址。将目的地址和网络掩码“逻辑与”后可得到目的主机或路由器所在网段的地址。例如：目的地址为129.102.8.10，掩码为255.255.0.0的主机或路由器所在网段的地址为129.102.0.0。掩码由若干个连续“1”构成，既可以以点分十进制表示，也可以用掩码中连续“1”的个数来表示。
4. 输出接口(Interface)：说明IP 包将从该路由器哪个接口转发
5. 下一跳IP地址(Nexthop)：说明IP 包所经由的下一个路由器
6. 本条路由加入IP路由表的优先级(Priority)：针对同一目的地可能存在不同下一跳的若干条路由，这些不同的路由可能是由不同的路由协议发现的，也可以是手工配置的。优先级高（数值小）将成为当前的最优路由。
7. 路由协议(Protocol)：说明该条路由是由何种路由协议发现的。路由器支持对静态路由的配置，同时支持RIP、OSPF、IS-IS和BGP等一系列动态路由协议，另外路由器在运行过程中根据接口状态和用户配置，会自动获得一些直接路由。如果目的地的网络与路由器直接相连，则显示“DIRECT”；如果是手工设置的静态路由，则显示“STATIC”。
8. 开销(Cost)：说明本条路由的开销大小。
9. 路由的分类：
10. 根据路由的目的地不同可以划分为:

* 子网路由: 目的地为子网（子网掩码Mask小于32位）
* 主机路由: 目的地为主机（子网掩码Mask为32位）

1. 根据目的地与该路由器是否直接相连又可分为:

* 直接路由: 目的地所在网络与路由器直接相连
* 间接路由: 目的地所在网络与路由器不是直接相连

为了不使路由表过于庞大，可以设置一条缺省路由。凡遇到查找路由表失败后的数据包，就选择缺省路由转发。

1. 常用路由表显示命令：可在任何视图下执行下列命令。
2. 查看路由表摘要信息: **display ip routing-table**
3. 查看路由表详细信息: **display ip routing-table verbose**
4. 查看指定目的地址的路由: **display ip routing-table** *ip-address* [ *mask* ] [ **longer-match** ] [ verbose ]
5. 查看指定协议发现的路由: **display ip routing-table protocol** *protocol* [ **inactive** | **verbose** ]
6. 路由表实例

在任何视图下输入以下命令都可以查看路由表：**display ip routing-table**

下表为一路由器的路由表。

Destination/Mask Protocol Pre Cost Nexthop Interface

172.16.0.1/32 OSPF 10 1565 172.16.3.9 Serial2/0

172.16.4.10 Serial2/1

172.16.0.2/32 OSPF 10 1565 172.16.3.9 Serial2/0

172.16.4.10 Serial2/1

172.16.0.3/32 OSPF 10 1563 172.16.3.9 Serial2/0

172.16.0.4/32 DIRECT 0 0 127.0.0.1 InLoopBack0

172.16.0.5/32 OSPF 10 1563 172.16.4.10 Serial2/1

172.16.0.6/32 OSPF 10 1565 172.16.3.9 Serial2/0

172.16.4.10 Serial2/1

172.16.0.7/32 OSPF 10 1565 172.16.3.9 Serial2/0

172.16.4.10 Serial2/1

172.16.0.8/32 OSPF 10 1565 172.16.3.9 Serial2/0

172.16.4.10 Serial2/1

172.16.0.9/32 OSPF 10 1565 172.16.3.9 Serial2/0

172.16.4.10 Serial2/1

172.16.0.10/32 OSPF 10 1565 172.16.3.9 Serial2/0

172.16.3.8/30 DIRECT 0 0 172.16.3.10 Serial2/0

172.16.3.9/32 DIRECT 0 0 172.16.3.9 Serial2/0

172.16.3.10/32 DIRECT 0 0 127.0.0.1 InLoopBack0

172.16.4.4/30 DIRECT 0 0 172.16.4.5 Ethernet0/1

172.16.4.5/32 DIRECT 0 0 127.0.0.1 InLoopBack0

172.16.4.8/30 DIRECT 0 0 172.16.4.9 Serial2/1

172.16.4.9/32 DIRECT 0 0 127.0.0.1 InLoopBack0

172.16.4.10/32 DIRECT 0 0 172.16.4.10 Serial2/1

1. **路由的优先级**

到相同的目的地，不同的路由协议包括静态路由可能会发现不同的路由，但并非这些路由都是最优的。事实上在某一时刻到某一目的地的当前路由仅能由唯一的路由协议来决定。这样各路由协议包括静态路由都被赋予了一个优先级。

当存在多个路由信息源时具有较高优先级的路由协议发现的路由将成为当前有效路由。各种路由协议及其发现路由的缺省优先级数值越小，表明优先级越高，如表4-1所示。

表4-1 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 |
| STATIC | 60 |
| RIP | 100 |
| IBGP | 256 |
| EBGP | 256 |
| UNKNOWN | 255 |

其中0 表示直接连接的路由，255 表示任何来自不可信源端的路由。

除了直连路由DIRECT、 IBGP 及EBGP 外，各动态路由协议的优先级都可根据用户需求手工进行配置，另外每条静态路由的优先级都可以不相同。

1. **缺省路由的配置**

缺省路由是一种特殊的路由，可以通过静态路由配置，某些动态路由协议也可以生成缺省路由，如OSPF和IS-IS。

缺省路由是在没有找到匹配的路由时才使用的路由。即只有当没有合适的路由时，缺省路由才被使用。在路由表中，缺省路由以到网络0.0.0.0（掩码为0.0.0.0）的路由形式出现。如果报文的目的地址不能与任何路由相匹配，那么系统将使用缺省路由转发该报文。如果没有缺省路由且报文的目的地不在路由表中，那么该报文被丢弃，同时，向源端返回一个ICMP报文报告该目的地址或网络不可达。可通过命令**display ip routing-table**的输出查看是否设置了缺省路由。

在系统视图下，执行以下命令可以设置缺省路由。

**ip route-static** 0.0.0.0 { 0.0.0.0 | 0 } {**null** *null-interface-number* | *gateway-address* } [ **preference** *value* ][ **reject** | **blackhole** ]

删除缺省路由：

**undo ip route-static** 0.0.0.0 { 0.0.0.0 | 0 } [**null** *null-interface-number* | *gateway-address* ] [ **preference** *value* ]

1. **静态路由的配置**

静态路由（Static Routing）是一种特殊的路由，它是由网络管理员采用手工方法在路由器中配置而成。这种方法适合在规模较小、路由表也相对简单的网络中使用。它比较简单，容易实现；可以精确控制路由选择，改进网络的性能；减少路由器的开销，为重要的应用保证带宽。但对于大规模网络而言，如果网络结构发生改变或网络链路发生故障，用手工的方法配置及修改路由表，对管理员形成很大压力。

静态路由还有如下的属性：

* 可达路由，正常的路由都属于这种情况，即IP报文按照目的地标示的路由被送往下一跳，这是静态路由的一般用法。
* 目的地不可达的路由，当到某一目的地的静态路由具有“**reject**”属性时，任何去往该目的地的IP报文都将被丢弃，并且通知源主机目的地不可达。
* 目的地为黑洞的路由，当到某一目的地的静态路由具有“**blackhole**”属性时，任何去往该目的地的IP报文都将被丢弃，并且不通知源主机。

其中“**reject**”和“**blackhole**”属性一般用来控制本路由器可达目的地的范围，辅助网络故障的诊断。

1. 静态路由的配置命令：
2. 增加一条静态路由：在系统视图下输入以下命令。

**ip route-static** *ip-address* { *mask* | *mask-length* } { **null** *null-interface-number* | *gateway-address* } [ **preference** *value* ] [ **reject** | **blackhole** ]

在配置静态路由时如果不指定优先级，则缺省为命令**ip route-static default-preference**指定的值，该值缺省情况下为60。

1. 删除一条静态路由：在系统视图下输入以下命令。

**undo ip route-static***ip-address* { *mask* | *mask-length* }[ *interface-type* *interface-number* ] [ *nexthop-address* ] [ **preference** *value* ]

1. 设置静态路由的缺省优先级：在系统视图下输入以下命令。

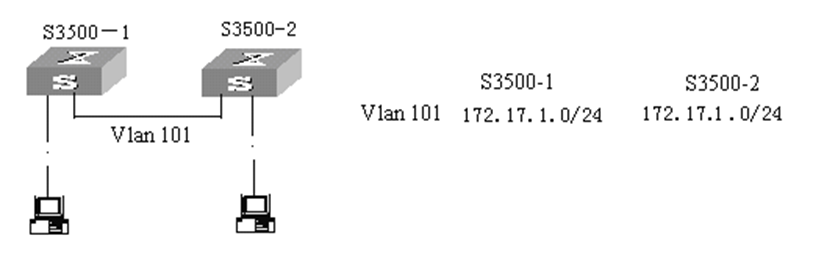
可以通过下列命令配置静态路由的缺省优先级。配置该命令改变缺省优先级的值后，随后配置的静态路由如果不指定其优先级，则其优先级为该命令配置的缺省优先级。

**ip route-static default-preference** *default-preference-value*

缺省情况下，*default-preference-value*的值为60。

1. 静态路由的配置举例：（以第1组与第2组之间的静态路由设置为例）
2. 组网图

要求：组1的1号机与组2的1号机合作配置静态路由。(其中带下划线的数字需根据组号变化。)



1. 配置步骤

a) 在S3500-1和S3500-2分别创建Vlan ，对应的ip如下：

**注意：同一交换机上选取的网段不能相互重叠，也不能与已分配的网段重叠。因此，**

组1与 组2协作 使用IP地址为 172.17.1~5.0 /24

组3与 组4协作 使用IP地址为 172.17.6~10.0 /24

组5与 组6协作 使用IP地址为 172.17.11~15.0 /24

组7与 组8协作 使用IP地址为 172.17.16~20.0 /24

组9与 组10协作 使用IP地址为 172.17.21~25.0 /24

登录到各组三层交换机（IP地址可以是用户的网关，下划线表示该数值需要根据组号或

座位而改变）

S3500-1：

system-view //进入系统视图

vlan 101 //创建101号vlan，个位数与台式机IP地址末位相同

quit

interface e0/11 //进入接口视图； 个位数与台式机IP地址末位相同

port access vlan 101 //将接口加入VLAN101

quit

interface vlan-interface 101 //进入 vlan接口视图

ip address 172.17.1.1 255.255.255.0 //建VLAN ip address

quit

S3500-2：

system-view //进入系统视图

vlan 101 //创建101号vlan，**与S3500-1相同**，个位数与台式机IP地址末位相同

quit

interface e0/11 //进入接口视图；个位数与台式机IP地址末位相同

port access vlan 101 //将接口加入VLAN101

quit

interface vlan-interface 101 //进入 vlan接口视图

ip address 172.17.1.2 255.255.255.0 //ip address与S3500-1的VLAN101在同网段，

但是IP地址不同。

quit //退出vlan interface视图

b) 用户机器的网线不要改动，用另外的网线将S3500-1和S3500-2 的e0/11连接，并将各组

S3500上连至AR28-31的连线拔掉。

测试：A 在交换机上能否互相ping通对方刚才所设的IP地址？如果成功，继续进行；

B 在PC机上能否互相ping通对方所设的IP地址？能否互相ping通对方用户的IP地

址？

c) 添加静态路由:

S3500－1：

系统视图下：ip route-static 192.168.2.0 24 172.17.1.2

S3500－2：

系统视图下：ip route-static 192.168.1.0 255.255.255.0 172.17.1.1

**参数解释：** 192.168.1.0为目标(对方)网段，255.255.255.0为网段掩码，

172.17.1.1 为下一跳IP，即对方所设的IP地址。

d) 测试：

* 用display ip routing-table 命令查看该静态路由是否已经生效
* 用display ip routing-table protocol static verbose 命令查看该静态路由详细信息
* ping 对方的网关通否？ping对方的主机通否

e) 思考：是否能ping通对方的交换机IP地址，如172.16.11.1? 172.16.12.1?

如果要ping通，该怎么加静态路由？

f) 删除静态路由: **undo ip route-static** *ip-address*

**注意**：

* 请严格按照分配的ip和port进行设置，以免发生冲突。
* 静态路由要添加对方交换机上的网段和接口地址。
* Vlan 1- 4均已使用，请勿覆盖。

1. **RIP协议配置**

RIP是Routing Information Protocol（路由信息协议）的简称。它是一种较为简单的内部网关协议（Interior Gateway Protocol，IGP），主要用于规模较小的网络中。由于RIP的实现较为简单，协议本身的开销对网络的性能影响比较小，并且在配置和维护管理方面也比OSPF或IS-IS容易，因此在实际组网中仍有广泛的应用。

RIP是一种基于距离矢量（Distance-Vector）算法的协议。距离矢量算法就是相邻的路由器之间互相交换整个路由表，并进行矢量的叠加，最后达到知道整个网络路由。管理比较简单，但是它的收敛速度慢，支持站点的数量有限，主要用于规模较小的网络中。它通过UDP报文进行路由信息的交换，每隔30秒向外发送一次更新报文。如果路由器经过180秒没有收到来自对端的路由更新报文，则将所有来自此路由器的路由信息标记为不可达，若在其后120秒内仍未收到更新报文，就将这些路由器从路由表中删除。

RIP使用跳数（Hop Count）来衡量到达目的网络的距离，称为路由权（Routing Cost）。在RIP中，路由器到与它直接相连网络的跳数为0，通过一个路由器可达的网络的跳数为1，其余依此类推。为限制收敛时间，RIP规定cost取值0～15之间的整数，大于或等于16的跳数被定义为无穷大，即目的网络或主机不可达。RIP协议有RIP1和RIP2两个版本，RIP2支持明文认证和MD5密文认证，并支持变长子网掩码等。

1. RIP的路由数据库

每个运行RIP的路由器管理一个路由数据库，该路由数据库包含了到网络所有可达目的网络的路由项，这些路由项包含下列信息：

* 目的地址：指主机或网络的地址。
* 下一跳地址：指为到达目的地，本路由器要经过的下一个路由器地址。
* 接口： 指转发报文的接口。
* 路由权值：指本路由器到达目的地的跳数，是一个0～15之间的整数。
* 路由时间：从路由项最后一次被修改到现在所经过的时间，路由项每次被修改时，路由时间重置为0。路由标记：区分路由为内部路由协议的路由还是引入外部路由协议的路由的标记。

具体的原理请参考教材。

1. RIP路由协议常用命令
2. 启动RIP： 在系统视图下执行相应命令。

* 启动RIP，进入RIP视图： rip
* 停止RIP协议的运行： undo rip

缺省情况下，不运行RIP。

1. 在指定网段使能RIP：

为了灵活地控制RIP工作，可以指定某些接口，将其所在的相应网段配置成RIP网络，使这些接口可收发RIP报文。请在RIP视图下进行下列配置。

* 在指定的网络接口上应用RIP：**network** *network-address*
* 在指定的网络接口上取消应用RIP：undo network*network-address*

1. 配置RIP的路由引入：

RIP允许用户将其它路由协议的路由信息引入到RIP路由表中，并可以设置引入时使用的缺省路由权。可引入到RIP中的路由类型包括：Direct、Static、OSPF、BGP和IS-IS。请在RIP视图下进行下列配置。

* 引入其它协议的路由：import-route *protocol* [ cost *value* ]

如果在引入路由时没有指定路由权，则使用缺省路由权，其缺省值为1。

* 取消对其它协议路由的引入：undo import-route *protocol*

1. 设置缺省路由权值：请在RIP视图下进行下列配置。

* 设定缺省路由权值：default cost *value*
* 恢复缺省路由权值：undo default cost

缺省的缺省路由权值为1。

1. 配置RIP优先级：

每一种路由协议都有自己的优先级，协议的优先级将影响路由策略采用哪种路由协议获取的路由作为最优路由。优先级的数值越大，其实际的优先级越低。可以手工设定RIP的优先级。请在RIP视图下进行下列配置。

* 设置RIP协议的优先级：preference *value*
* 将RIP协议的优先级恢复为缺省值：undo preference

缺省情况下，RIP的优先级为100。

1. RIP显示命令：

* 显示RIP的当前运行状态及配置信息：display rip
* 显示RIP的接口信息：display rip interface
* 显示RIP路由表：display rip routing

**[注：]** RIP协议还有很多其他命令，感兴趣的同学可以自己查看，在这里就不一一列举。

1. RIP配置举例：
2. 组网图：使用上面配置静态路由使用的组网图。
3. 配置步骤：
4. 建立vlan，请参见静态路由设置。
5. 配置RIP协议

S3500-1：在系统视图下，

rip //启用 rip，进入RIP视图

network 172.17.1.0 // 172.17.1.0 应用rip

network 192.168.1.0 // 192.168.1.0应用rip

preference 8 //提高rip优先权为8

S3500-2：在系统视图下，

rip //启用 rip

network 172.17.1.0 //172.17.1.0 应用rip

network 192.168.2.0 // 192.168.2.0应用rip

preference 8 //提高rip优先权为8

1. 测试：
   * 用display rip 命令查看该路由配置
   * 用display ip routing-table protocol rip verbose 命令查看该路由详细信息
   * ping 对方的网关通否？ping对方的主机通否？
2. 思考：是否能ping通对方的交换机IP地址，如172.16.11.2? 172.16.12.2?

如果要ping通，该怎么加network？

1. 取消应用RIP: **undo network** *network-address*
2. **注意**：

* 请严格按照分配的ip和port进行设置；或者两组同学讨论后确定不冲突的IP地址和端口。
* 如果刚才配置了静态路由，需要先删除。**undo ip route-static** *ip-address*
* RIP路由设置是添加本地交换机上的网段。
* Vlan 1- 4均已使用，请勿覆盖。本次实验需组间合作，请协调进行。

1. **OSPF路由协议配置**

OSPF（Open Shortest Path First，开放最短路由优先协议）是IETF 组织开发的一个基于链路状态的内部网关协议。详细介绍请参考教科书。在OSPF各项配置中，必须先启动OSPF、指定接口与区域号后，才能配置其它的功能特性，而配置与接口相关的功能特性不受OSPF是否开启的限制。需要注意的是，在关闭OSPF后，原来与OSPF相关的接口参数也同时失效。

1. 基本的OSPF 配置命令：
2. 配置Router ID：

一台路由器如果要运行OSPF协议，必须存在Router ID。路由器的ID是一个32比特无符号整数，采用IP地址形式，是一台路由器在自治系统中的唯一标识。路由器的ID可以手工配置，如果没有配置ID号，若系统当前配置了Loopback接口IP地址，则选择最后配置的Loopback接口的IP地址作为router id；若系统当前没有配置Loopback接口，则选取第一个配置并UP的物理接口的IP地址作为router id。手工配置路由器的ID时，必须保证自治系统中任意两台路由器的ID都不相同。一般建议选择loopback接口的IP地址作为本机ID号，因为该接口永远UP（除非手工shutdown）。请在系统视图下进行下列配置。

* 配置路由器的ID号：router id *router-id*
* 取消路由器的ID号：undo router id

1. 启动OSPF：请在系统视图下进行下列配置。

* 启动OSPF，进入OSPF视图：ospf
* 关闭OSPF路由协议进程：undo ospf

缺省情况下，不运行OSPF。

1. 进入OSPF区域视图：

OSPF协议将自治系统划分成不同的区域（Area），在逻辑上将路由器分为不同的组。在区域视图下可以进行区域相关配置。请在OSPF视图下进行下列配置。

* 进入OSPF区域视图：area *area-id*
* 删除指定的OSPF区域：undo area *area-id*

区域ID (area-id) 可以采用十进制整数或IP地址形式输入，但显示时使用IP地址形式。

1. 在指定网段开启OSPF：

在系统视图下使用ospf命令启动OSPF后，还必须指定在哪个网段上应用OSPF。请在OSPF区域视图下进行下列配置。

* 指定网段运行OSPF协议：network *ip-address wildcard-mask*
* 取消网段运行OSPF协议：undo network *ip-address wildcard-mask*

wildcard-mask为网络子网的反掩码。即如果网络子网掩码为255.255.255.0，则其反掩码(wildcard-mask) 即为：0.0.0.255。

1. 配置OSPF的路由引入：

路由器上各动态路由协议之间可以互相共享路由信息，由于OSPF的特性，其它的路由协议发现的路由总被当作自治系统外部的路由信息处理。可引入的路由包括direct、static、RIP、IS-IS与BGP，也可以引入其它进程的OSPF路由，并可以设置引入时的权值。请在OSPF视图下进行下列配置。

* 引入其它协议的路由信息：import-route *protocol* [ cost value ]
* 取消引入其它协议路由信息：undo import-route *protocol*

1. 配置OSPF的优先级：请在OSPF视图下进行下列配置。

* 配置OSPF协议在各路由协议之间的优先级：preference *preference*
* 恢复协议缺省优先级：undo preference

缺省情况下，OSPF协议的优先级为10；引入外部路由协议的优先级为150。

1. OSPF显示命令：

在完成上述配置后，在所有视图下执行display命令可以显示配置后OSPF的运行情况，用户可以通过查看显示信息验证配置的效果。

* 查看OSPF路由过程的信息：display ospf brief
* 查看OSPF路由表信息：display ospf routing
* 查看OSPF接口信息：display ospf interface
* 查看OSPF邻接点信息：display ospf peer
* 查看OSPF下一跳信息：display ospf nexthop

**本实验室已经配置OSPF路由协议。**

1. OSPF配置举例：
2. 组网图：使用上面的配置静态路由的组网图。
3. 配置过程：
4. 建立vlan，连线同上。
5. 启动并配置OSPF协议

S3500-1: 在系统视图下，

[S3500-1] router id 172.16.0.11 // 配置router id和loopback0地址一致，个位

数为组号，**本实验室已配置**

[S3500-1] ospf // 进入ospf路由视图

[S3500-1-ospf] area 0 // 进入区域0视图

[S3500-1-ospf-area-0.0.0.0] network 172.16.0.11 0.0.0.0 //接口loopback 0开启OSPF，

**本实验室已配置**

[S3500-1-ospf-area-0.0.0.0] network 172.17.1.0 0.0.0.255 // VLAN101开启OSPF

[S3500-1-ospf-area-0.0.0.0] quit //退出区域0视图

[S3500-1-ospf] import-route direct //向ospf中引入直连路由

S3500-2配置步骤与S3500-1类似。

1. 测试：
   * 用display ospf 命令查看该路由配置
   * 用display ip routing-table protocol ospf verbose 命令查看该路由详细信息
   * ping 对方的网关通否？ping对方的主机通否？
2. 查看设置结果：**display ospf interface**
3. **实验要求**
4. 按照要求对路由器端口进行相应配置。参考配置实例，分别进行静态路由、RIP及OSPF路由协议的配置。

**实验五 访问控制列表**

1. **实验目的：**

本实验的主要目的是学习在交换机上配置访问控制列表。

1. **访问控制列表基础知识**

为了过滤通过网络设备的数据包，需要配置一系列的匹配规则，以识别需要过滤的对象。在识别出特定的对象之后，网络设备才能根据预先设定的策略允许或禁止相应的数据包通过。访问控制列表（Access Control List，ACL）就是用来实现这些功能。

ACL通过一系列的匹配条件对数据包进行分类，这些条件可以是数据包的源地址、目的地址、端口号等。ACL应用在交换机全局或端口，交换机根据ACL中指定的条件来检测数据包，从而决定是转发还是丢弃该数据包。由ACL定义的数据包匹配规则，还可以在其它需要对流量进行区分的场合引用，如定义QoS中的流分类规则时。

一条访问控制规则可以由多条子规则组成。由于每一条子规则指定的数据包的范围大小有别，在匹配一个访问控制规则的时候就存在匹配顺序的问题。交换机中ACL可以直接下发到交换机的硬件中用于数据转发过程中的过滤和流分类。此时一条ACL中多个子规则的匹配顺序是由交换机的硬件决定的，用户即使在定义ACL时配置了匹配顺序也不起作用。对于本实验室的三层交换机S3526C而言，同一个ACL 配置了多个子规则时，硬件匹配顺序是后下发的子规则将会先匹配。交换机也使用ACL来对由软件处理的报文进行过滤和流分类。此时ACL子规则的匹配顺序有两种：config（指定匹配该规则时按用户的配置顺序）和auto（指定匹配该规则时系统自动排序，即按“深度优先”的顺序）。这种情况下用户可以在定义ACL的时候指定一条ACL中多个子规则的匹配顺序。用户一旦指定某一条访问控制列表的匹配顺序，就不能再更改该顺序。只有把该列表中所有的规则全部删除后，才能重新指定其匹配顺序。

在以太网交换机中，访问控制列表分为以下几类：

* 基于数字标识的基本访问控制列表。
* 基于名字标识的基本访问控制列表。
* 基于数字标识的高级访问控制列表。
* 基于名字标识的高级访问控制列表。
* 基于数字标识的二层访问控制列表。
* 基于名字标识的二层访问控制列表。

交换机上对各种访问控制列表的数目限制如下表5-1所示：

                                                                 表5-1 访问控制列表的数量限制

| 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 |
| 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 |
| 基于名字标识的基本访问控制列表 | － |
| 基于名字标识的高级访问控制列表 | － |
| 基于名字标识的二层访问控制列表 | － |
| 一条访问控制列表可以定义的子规则 | 0～127 |
| 交换机最多可以支持的子规则（所有访问控制列表的子规则之和） | － |

1. **ACL配置命令**

访问控制列表配置包括：

* 配置时间段
* 定义访问控制列表
* 激活访问控制列表

以上三个步骤最好依次进行，先配置时间段，然后定义访问控制列表（在其中会引用定义好的时间段），最后激活访问控制列表，使其生效。

1. **配置时间段**

 对时间段的配置有如下内容：配置每天的时分范围、周期范围和日期范围。配置日期范围采用的是年、月、日、时、分的形式，配置周期范围采用的是每周的周几的形式，配置每天的时分范围采用的是每天的几点、几分的形式。可以使用下面的命令来配置时间段。

* 创建时间段：

**time-range** *time-name* { *start-time* **to** *end-time* *days-of-the-week* [ **from** *start-time* *start-date* ] [ **to** *end-time* *end-date* ] | **from** *start-time* *start-date* [ **to** *end-time end-date* ] }

如果不配置起始时分和结束时分，时间段就是一天内所有的时间。如果不配置结束日期，时间段就是从配置生效之日起到系统可以表示的最大时间为止。

* 删除时间段：

**undo time-range** *time-name* [ *start-time* **to** *end-time* *days-of-the-week* [ **from** *start-time start-date* ] [ **to** *end-time end-date* ] | **from** *start-time start-date* [ **to** *end-time end-date* ] ]

1. **定义访问控制列表**
2. **定义基本访问控制列表**

基本访问控制列表只根据三层源IP制定规则,对数据包进行相应的分析处理。

1. 进入基本访问控制列表视图:在系统视图下输入以下命令。

**acl** { **number** *acl-number* |**name** *acl-name* **basic** }[ **match-order** { **config** | **auto** } ]

**basic**：表示基本访问控制列表。**config**：表示匹配访问列表的规则时按用户的配置顺序。**auto**：表示匹配访问列表的规则时按深度优先顺序。

1. 定义子规则：在基本访问控制列表视图下输入以下命令。

**rule** [ *rule-id* ] { **permit** | **deny** } [ **source** *source-addrwildcard* | **any** ] [ **fragment** ] [**time-range** *name*]

1. 删除访问控制列表的一个子规则：在基本访问控制列表视图下输入以下命令。

**undo rule** *rule-id* [ **source** ] [ **fragment** ] [ **time-range** ]

1. 删除访问控制列表，或者删除全部访问控制列表：在系统视图下输入以下命令。

**undo acl** { **number** *acl-number*| **name** *acl-name* |**all** }

基本访问控制列表的数字标识取值范围为2000 ~ 2999

一条访问控制列表可以定义的子规则 0 ~ 127

1. **定义高级访问控制列表**

高级访问控制列表根据源IP、目的IP、使用的TCP 或UDP 端口号、报文优先级等数据包的属性信息制定分类规则，对数据包进行相应的处理。高级访问控制列表支持对三种报文优先级的分析处理:TOS(Type Of Service)优先级,IP优先级和DSCP优先级。

1. 进入高级访问控制列表视图:在系统视图下输入以下命令。

**acl** { **number** *acl-number |* **name** *acl-name* **advanced** }[ **match-order** { **config** | **auto** } ]

1. 定义子规则：在高级访问控制列表视图下输入以下命令。

**rule** [ *rule-id* ] { **permit** | **deny** } *protocol* [ **source** *source-addr wildcard* | **any** ] [ **destination** *dest-addr wildcard* | **any** ][ **source-port** *operator port1* [ *port2* ] ] [ **destination-port** *operator port1* [ *port2* ] ] [ **icmp-type** *type code* ] [ **established** ][ [ **precedence** *precedence* | **tos** *tos* ]\* | **dscp** *dscp* ] [ **fragment** ] [ **time-range** *name* ]

1. 删除访问控制列表的一个子规则：在高级访问控制列表视图下输入以下命令。

**undo rule** *rule-id*[ **source** ] [ **destination** ] [ **source-port** ] [ **destination-port** ] [**icmp-type** ] [ **precedence** ] [ **tos** ] [ **dscp** ] [ **fragment** ]  [ **time-range** ]

1. 删除访问控制列表，或者删除全部访问控制列表：在高级访问控制列表视图下输入以下命令。**undo acl** { **number** *acl-number* **| name** *acl-name |* **all** }

高级访问控制列表的数字标识取值范围为3000~ 3999

**注意：**上面命令中的*port1 port2* 参数指的是各种高层应用使用的TCP 或者UDP 的端口号，对于部分常见的端口号可以用相应的助记符来代替其实际数字，如使用“bgp”来代替BGP 协议使用的TCP 端口号179。

**表5-2 常用IP 协议号**

|  |  |  |
| --- | --- | --- |
| 协议 | 协议号 | 全称 |
| IP | 0 | Internet Protocol |
| ICMP | 1 | Internet Protocol Message Protocol |
| IGMP | 2 | Internet Group Managemen |
| GGP | 3 | Gateway-Gateway Protocol |
| TCP | 6 | Transmission Control Protocol |
| EGP | 8 | Exterior Gateway Protocol |
| IGP | 9 | Interior Gateway Porotocl |
| PUP | 12 | PARC Universal Packet Protocol |
| UDP | 17 | User Datagram Protocol |
| HMP | 20 | Host Monitoring Protocol |
| XNS-IDP | 22 | Xerox NS IDP |
| RDP | 27 | Reliable Datagram Protocol |
| GRE | 47 | General Routing Encapsulation |
| ESP | 50 | Encap Security Payload |
| AH | 51 | Authentication Header |
| RVD | 66 | MIT Remote Virtual Disk |
| EIGRP | 88 | Enhandced Interior Gateway Routing Portocol |
| OSPF | 89 | Open Shortest Path First |

**表5-3 常用TCP/UDP 端口号**

|  |  |  |  |
| --- | --- | --- | --- |
| 服务 | 端口号 | 协议 | 描述 |
| Echo | 7 | tcp |  |
| Echo | 7 | udp |  |
| ftp-data | 20 | tcp | FTP, data |
| ftp | 21 | tcp | FTP. control |
| telnet | 23 | tcp |  |
| Smtp | 25 | tcp | Simple Mail Transfer Protocol |
| Time | 37 | tcp | timserver |
| Time | 37 | udp | timserver |
| nameserver | 42 | tcp | Host Name Server |
| nameserver | 42 | udp | Host Name Server |
| Domain | 53 | tcp | Domain Name Server |
| Domain | 53 | udp | Domain Name Server |
| Bootps | 67 | udp | Bootstrap Protocol Server |
| Bootpc | 68 | udp | Bootstrap Protocol Client |
| Tftp | 69 | udp | Trivial File Transfer |
| Gopher | 70 | tcp |  |
| Finger | 79 | tcp |  |
| http | 80 | tcp | World Wide Web |
| pop2 | 109 | tcp | Post Office Protocol-Version 2 |
| pop3 | 110 | tcp | Post Office Protocol-Version 3 |

1. **定义二层访问控制列表**

二层访问控制列表根据源MAC地址、源VLAN ID、二层协议类型、报文二层接收端口、报文二层转发端口、目的MAC地址等二层信息制定规则，对数据进行相应处理。

1. 进入二层访问控制列表视图:在系统视图下输入以下命令。

**acl** { **number** *acl-number |* **name** *acl-name* **link** }[ **match-order** { **config** | **auto** } ]

1. 定义子规则：在二层访问控制列表视图下输入以下命令。

**rule** [ *rule-id* ] { **permit** | **deny** } [ **ingress**  { *source-vlan-id*| *source-mac-addr* | **interface** { *interface-name* |*interface-type interface-num* } }\* | **any** } ] [ **egress**{ { *destination-vlan-id* | *dest-mac-addr |* **interface** { *interface-name* | *interface-type interface-num* } }\* |**any** } ] [ **time-range** *name* ]

1. 删除访问控制列表的一个子规则：在二层访问控制列表视图下输入以下命令。

**undo rule** *rule-id*

1. 删除访问控制列表，或者删除全部访问控制列表：在系统视图下输入以下命令。

**undo acl** { **number** *acl-number* **| name** *acl-name* |**all** }

二层访问控制列表的数字标识取值范围为4000~ 4999

1. **激活访问控制列表**

将访问控制列表定义好后，必须激活之后才能使之生效。本配置用来激活那些对交换机硬件转发的数据进行过滤或分类的访问控制列表。可以使用下面的命令来激活定义好的访问控制列表。

1. 激活访问控制列表：在系统视图下进行下列配置。

**packet-filter** { **ip-group** { *acl-number* | *acl-name* } [ **rule** *rule* ] | **link-group** { *acl-number* | *acl-name* } [ **rule** *rule* ] }

1. 取消激活访问控制列表: 在系统视图下进行下列配置。

**undo packet-filter** { **ip-group** { *acl-number* | *acl-name* } [ **rule** *rule* ] | **link-group** { *acl-number* | *acl-name* } [ **rule** *rule* ] }

1. **访问控制列表的显示**

在完成上述配置后，在所有视图下执行**display**命令都可以显示配置后访问控制列表的运行情况。用户可以通过查看显示信息验证配置的效果。在用户视图下执行**reset**命令可以将有关访问控制列表的统计信息清除。

1. 显示时间段状况：**display time-range**[ **all** | *name* ]
2. 显示访问控制列表的详细配置信息：display acl config { all | *acl-number* | *acl-name* }
3. 显示访问控制列表的下发应用信息：**display acl running-packet-filter all**
4. 清除访问控制列表的统计信息：**reset acl counter** { **all** | acl-number | acl-name }

**display acl config**命令显示的匹配信息是由交换机CPU处理的匹配信息。用户可以使用命令**display qos-global traffic-statistic**显示交换机转发数据的匹配信息。

1. **ACL配置实例**
2. 配置需求：

通过基本访问控制列表实现在每天8:00 -18:00 时间段内，对源IP 为10.1.1.1 主机发出报文的过滤。

1. 配置过程：(以第一组为例)
2. 定义时间段

[S3500-1] **time-range** T1 8:00 to 18:00 daily //定义8:00 至18:00 的周期时间段,命名为T1

1. 定义源IP 为10.1.1.1 的ACL

[S3500-1] acl name traffic-of-host basic // 进入基于名字的基本访问控制列表视图,

命名为traffic-of-host

[S3500-1-acl-basic-traffic-of-host] rule 1 deny source 10.1.1.1 0 time-range T1

// 定义源IP 为10.1.1.1 的访问规则

1. 激活ACL

[S3500-1] **packet-filter ip-group** traffic-of-host //将traffic-of-host 的ACL 激活

1. 单向访问控制列表的配置：

单向访问控制主要是针对有方向的数据包，例如ICMP，TCP报文等，而对于没有方向的UDP报文，交换机暂时无法进行控制，所以如果要实现单向访问控制就简单等同于对ICMP和TCP报文的控制。

单向访问控制列表只使用数据包的源地址来判断数据包，只能粗略地区别对待网内的用户群。配置访问控制列表时，如果源IP取自己或其他同学的IP地址，会使机器与交换机失去连接，无法恢复，因此要仔细设计实验。如下一个实验：（下划线表示该数值需要根据组号或座位而改变）：

1. Ping 自己的网关， 能通否？
2. telnet 至自己网关，如：192.168.3.254 //3根据组号而改变
3. 在系统视图下，

[S3500-3]**acl number** 3001 //配置高级访问控制规则, number > 3000,个位数与台式机

IP地址末位相同

1. [S3500-3-acl-3001]**rule 2 deny icmp source** 192.168.3.1 0 //拒绝ICMP报文。Source地址

改变为自己机器的IP

1. [S3500-3-acl-3001]
2. [S3500-3]**quit**
3. [S3500-3]**packet-filter ip-group** 3001 **rule** 2 //激活
4. 检测：

* 自己的机器仍旧与交换机连接着，但是不能ping通网关。
* 用同组其它同学的机器，在三层交换机(S3500-3)上执行以下命令：

[S3500-3] **display acl config** { **all** | *acl-number* | *acl-name* } // 显示访问控制列表的详细配置信息

* **display acl running-packet-filter all //**显示访问控制列表的下发应用信息

1. 删除：[S3500-3]**undo packet-filter ip-group** 3001

[S3500-3]**undo acl number** 3001

1. 思考：

* 若要阻止IP为192.168.3.1的主机访问目标地址172.16.11.10,该如何配置？
* 配置rule 2 命令行最后的0 表示什么意思？

1. **实验要求**

认真阅读实验相关内容，并按配置实例进行ACL配置练习。