《计算机网络系统》路由交换系列实验-2

VLAN（中继、路由)、动态路由与 ACL

设计编辑：张翔、张超魁

一、实验名称：VLAN（中继、路由)、动态路由与 ACL

二、实验学时：4 学时

三、实验目的

1. 掌握如何在交换机上划分基于端口的 VLAN、如何给 VLAN 内添加端口，理解跨交换机之间 VLAN 的特点以及掌握 VLAN 间路由的方法；
2. 理解路由器的工作原理，掌握路由器的基本操作以及简单的动态路由；
3. 通过对交换机的各种安全操作，提高网络安全意识。

四、实验原理

1. VLAN 与 VLAN 中继

网络性能对业务处理与用户体验有很大的影响。VLAN（Virtual Local Area Network，虚拟局域网）是一种可极大改善网络性能的技术。

(1) 切割以及扩展广播域

VLAN 能将大型广播域划分成较小的广播域。较小的广播域能够限制参与广播的设备数量，并允许将设备分成各个工作组。这使得管理者可以不依赖于主机的物理位置，而是以逻辑的方式分隔不同功能/用途/部门的主机，使之在数据链路层逻辑上相互隔离互通。

VLAN 同时也能扩展网络广播域，将过去以路由器为边界的广播域扩展成为以 VLAN 为边界的广播域。通过 VLAN 中继，在不使用路由器的情况下，可通过交换机构建按需定义广播边界的大型交换网络，并基于三层交换机实现不同 VLAN 之间的互联互通。

(2) 逻辑上独立的 IP 子网

VLAN 是一个逻辑上独立的 IP 子网。多个 IP 网络可以通过 VLAN 存在于同一个交换网络中。为了让同一个 VLAN 上的计算机能相互通信，每台计算机必须具有与该 VLAN 一致的 IP 地址和子网掩码。其中的交换机必须配置 VLAN，并且必须将位于 VLAN 中的每个端口分配给 VLAN。配置了单个 VLAN 的交换机端口称为接入端口。

注意，如果两台计算机只是在物理上连接到同一台交换机，并不表示它们能够通信。无论是否使用 VLAN，两个不同网络和子网上的设备必须通过路由器（第 3 层）才能通信。要将多个网络和子网组织到一个交换网络中，不一定要使用 VLAN，但是使用 VLAN 会更简单与方便。

(3) VLAN 与传统子网的比较

尽管一般 VLAN 与子网会通常是对应的，但它们工作在网络上不同的层中，并且解决的是不同的问题。VLAN 相当于把一台交换机变成了多台交换机，或者把多台交换机重新组合形成逻辑上的多台交换机，以分解广播域。每个 VLAN 被视为一个单独的局域网，且只能通过三层路由到达另一个 VLAN。而子网本质是一组 IP 地址，当目的 IP 地址与源 IP 地址不在同一子网中时，与 VLAN 一样，必须通过路由实现两个子网的互联互通。VLAN 是基于软件的，传统子网划分主要是基于硬件的（比如基于路由器的路由端口进行划分）。

(4) VLAN 中继与 802.1Q 协议

VLAN 和 VLAN 中继有着密不可分的联系。如果没有 VLAN 中继，现代交换 LAN 中的 VLAN 实际上没有任何用处。VLAN 中继是以太网交换机接口和另一个联网设备（如路由器或计算机）的以太网接口之间的点对点链路，负责在单个链路上传输多个 VLAN 的流量。VLAN 中继可让 VLAN 扩展到整个网络上。VLAN 中继不属于具体某个 VLAN，而是作为 VLAN 在交换机之间的管道。

VLAN 中继通过在以太网帧头部中打标记的方式实现，主要是通过在以太网帧头增加 802.1Q 字段，用以记录帧所属 VLAN，帮助交换机识别 VLAN 中继 Trunk 链路上传输的到底是哪个 VLAN 的帧。

2. VLAN 与 VLAN 中继配置应用

(1) VLAN 编号与配置存储

每一个 VLAN 都有一个 VLAN ID，一般也可以对 VLAN 进行命名。VLAN ID 的选择有两种范围：普通范围的 VLAN ID 是 1~1001，扩展范围的 VLAN ID 是 1006~4094。而 VLAN 1 和 VLAN 1002~1005 是保留 ID 号。在配置普通范围 VLAN 时，配置细节会自动存储在交换机闪存内一个名为 vlan.dat 的文件中，把运行配置文件的修改保存到启动配置文件。

(2) VLAN 创建命名与查看

IOS 命令向交换机添加 VLAN 的过程如下（在全局配置模式下）：

// 创建 ID 为<vlan_id>的 VLAN，之后 CLI 会切换到此 VLAN 的配置模式

S1(config)# vlan <vlan_id>

// 指定唯一的 VLAN 名称标识 VLAN（可选，默认名称为 VLAN 后面加若干个 0 再加上 VLAN 号，如 VLAN0001）

S1(config-vlan)# name <vlan_name>

// 返回特权执行模式，此时配置会保存在 vlan.dat 文件中，同时配置生效

S1(config-vlan)# end

在特权执行模式下使用 **show vlan** 可以看到当前设备的 VLAN 状态：

show vlan [brief|id <vlan-id>|name <vlan-name>|summary]

(3) 交换机接口 VLAN 模式

交换机接口的模式有以下三种：Access、Dynamic、Trunk：

- Access 型端口只能属于 1 个 VLAN，一般用于连接计算机的端口，连接 Access 接口链路通常称为 Access Link；
- Trunk 型的端口可以属于多个 VLAN，通过给以太网帧头打标记（tag）的方式支持接收和发送多个 VLAN 的数据，一般用于交换机之间连接的端口，即支持 VLAN 中继；
- Dynamic 型端口支持端口之间通过自动协商确认是采用 Access 型还是 Trunk 型。

- ✧ switchport mode dynamic desirable: 主动与对协商成为 Trunk 接口的可能性，如果邻居接口模式为 Trunk/desirable/auto 之一，则接口将变成 trunk 接口工作。如果不能 形成 trunk 模式，则工作在 access 模式。这种模式是现在交换机的默认模式。
- ✧ switchport mode dynamic auto: 只有邻居交换机主动与自己协商时才会变成 Trunk 接口，所以它是一种被动模式，当邻居接口为 Trunk/desirable 之一时，才会成为 Trunk。如果不能形成 trunk 模式，则工作在 access 模式。

(4) 指定 VLAN 的接口添加或删除

默认情况下所有接口都在 VLAN1 下，添加接口至单个指定 VLAN 的方法范例如下：

// 进入 f0/10 接口的配置模式

S1(config)# interface f0/10

//强制修改端口为接入模式。

S1(config-if)# switchport mode access

// 将接口添加到 VLAN 20 中，端口在 access 模式下允许 vlan 20 通过 S1(config-if)# switchport access vlan 20

S1(config-if)# end

删除 VLAN 成员资格需要在接口配置模式下使用 no switchport access vlan 命令：

S1(config)# interface f0/10

S1(config-if)# no switchport mode access

S1(config-if)# end

此时接口会被重新分配给 VLAN1。

(5) 删除已创建的 VLAN

删除 VLAN 需要在全局配置模式下使用命令 no vlan <vlan_id>。需要注意，删除 VLAN 不会将此 VLAN 下的接口转移到其他 VLAN 下。

(6) 配置 VLAN 中继（干线）接口

使用 switchport mode trunk 命令。在交换机端口上输入该命令，接口即更改为永久中继模式，并且端口会进入 DTP（Dynamic Trunking Protocol）协商，以将链路转换为中继链路

默认情况下中继接口允许所有 VLAN 通过，如果需要限制中继接口允许的 VLAN，则需在接口配置模式下使用命令 switchport trunk allowed vlan add <vlan_list>，删除这一限制可以在接口配置模式下使用命令 no switchport trunk allowed vlan。

将接口重置为静态接入模式可以在接口配置模式下使用命命令 switchport mode access。

3. VLAN 间路由

VLAN 和中继用于把 LAN 分段。用 VLAN 分段功能限定 LAN 中各广播域的范围，可提高整个网络的性能和安全。VLAN 间路由则可以使属于不同 VLAN 的设备进行通信。

VLAN 间路由有多种方式：

(1) 每个路由器的路由接口对应一独立 VLAN

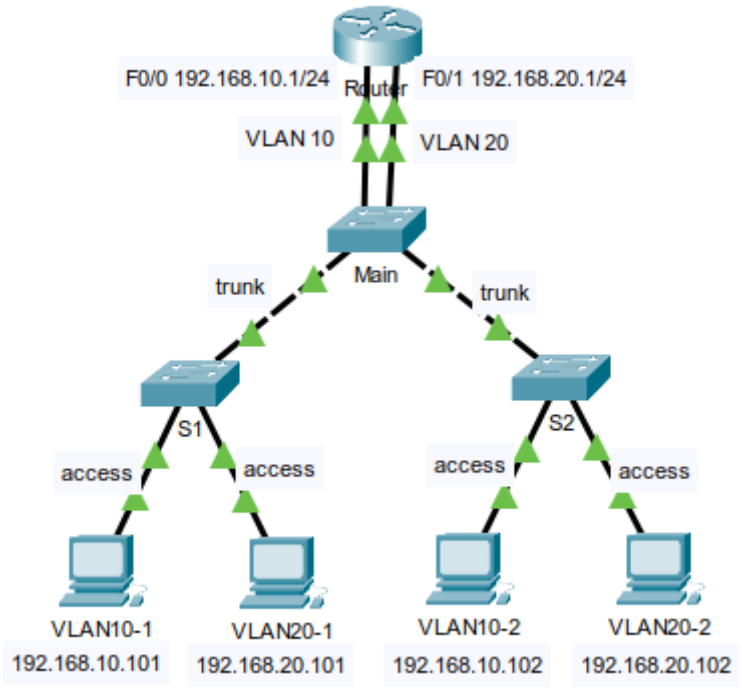

图 1 每个路由器接口对应一个 VLAN 的情形

这一拓扑在逻辑上与下图一致：

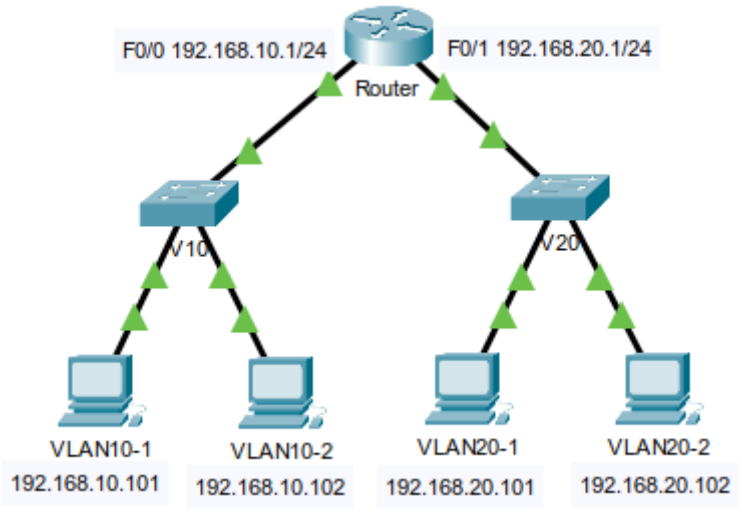

图 2 每个路由器接口对应一个 VLAN 的逻辑情形

(2) 单臂路由器（单路由器接口支持多 VLAN）

单臂路由器只需要一个接口就可完成所有的工作，下面主要介绍单臂路由器

的配置。

单臂路由器路由需使用虚拟子接口和中继链路。子接口是基于软件的虚拟接口，可分配到各物理接口。每个子接口配置有自己的 IP 地址、子网掩码和惟一的 VLAN 分配，使单个物理接口可同时属于多个逻辑网络。这种方法适用于在网络中有多个 VLAN 但只有少数路由器物理接口的 VLAN。

使用单臂路由器模式配置 VLAN 间路由时，路由器的物理接口必须与相邻交换机的中继链路相连接。针对网络上每个唯一的 VLAN/子网创建子接口。每个子接口都分配有所属子网的 IP 地址，并对与其交互的 VLAN 帧添加 VLAN 标记。这样，路由器可以在流量通过中继链路返回交换机时区分不同子接口的流量。

假设有如图 2 所示拓扑：

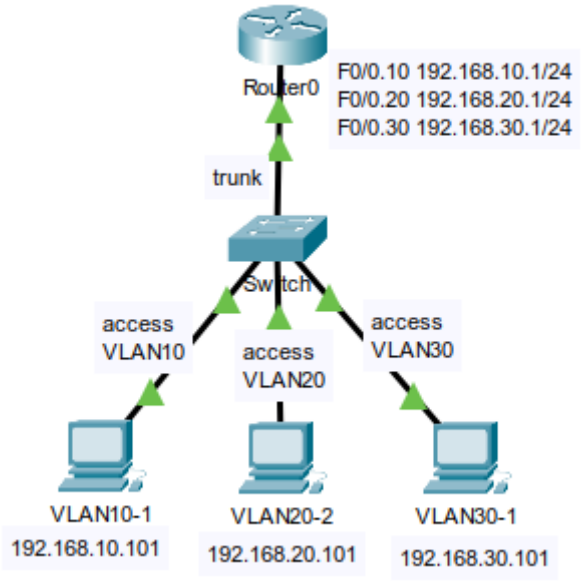

图 3 单臂路由器拓扑示例

这一拓扑在逻辑上与下图一致：

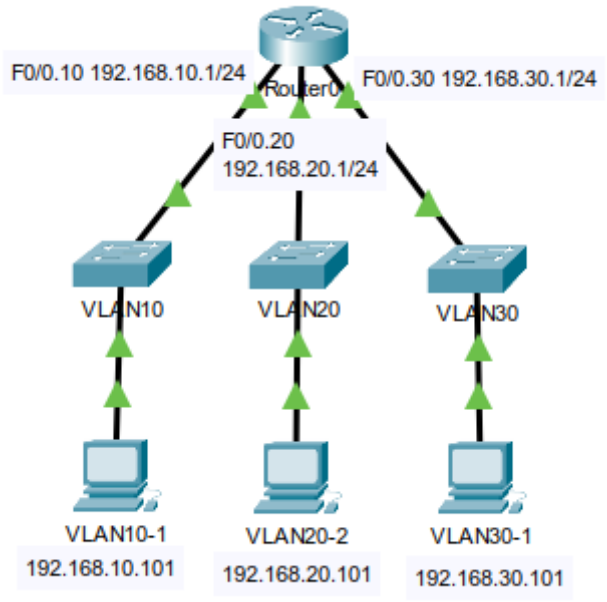

图 4 单臂路由器逻辑拓扑

假设已经划分号 VLAN 并分配相应的端口，首先需配置交换机与路由器之间的链路为 Trunk：

S1(config)# interface f0/4

S1(config-if)# switchport mode trunk

S1(config-if)# end

接下来配置路由器以实现 VLAN 间路由。不同于物理接口配置，全局配置模式下使用 interface <interface_id.subinterface_id>命令创建各个子接口。子接口创建后，在子接口配置模式下运行 encapsulation dot1q <vlan_id>命令分配 VLAN ID。然后运行 ip address <ip_address> <subnet_mask>子接口配置模式命令为该子接口分配 IP 地址：

R1(config)# interface f0/0.10

R1(config-subif)# encapsulation dot1q 10

R1(config-subif)# ip address 192.168.10.101 255.255.255.0

R1(config-subif)# interface f0/0.20

R1(config-subif)# encapsulation dot1q 20

R1(config-subif)# ip address 192.168.20.101 255.255.255.0

R1(config-subif)# interface f0/0.30

R1(config-subif)# encapsulation dot1q 30

R1(config-subif)# ip address 192.168.30.101 255.255.255.0

R1(config-subif)# interface f0/0

R1(config-if)# no shutdown

R1(config-if)# end

现在可以使用 show ip route 命令检查路由表，并在主机上使用 ping 命令测试网络。

(3) 三层交换机虚拟路由端口

三层交换机具有一定的路由功能，因此可以进行 VLAN 间路由。三层交换机的 VLAN 间路由实际上是通过 SVI（交换机虚拟接口（SVI:switch virtual interface））实现的，这种技术允许三层交换机在 VLAN 之间路由数据传输。三层交换机进行 VLAN 间数据传输的过程类似于路由器，SVI 类似于路由器接口。关于 SVI 更详细的信息，请参见实验原理**“5. SVI”**。

假设有如图 5 所示的拓扑：

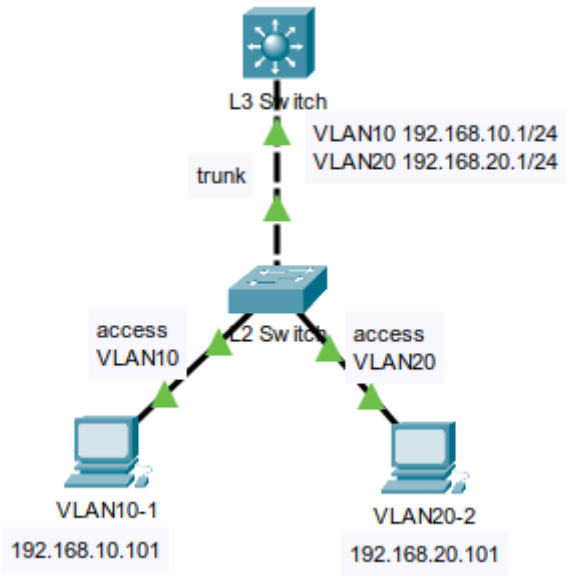

图 5 使用三层交换机进行 VLAN 间路由

首先配置三层交换机与二层交换机之间的链路为 Trunk，以及中继封装协议：

L2Switch(config)# interface fastEthernet 0/3

L2Switch(config-if)# switchport mode trunk

L3Switch(config)# interface fastEthernet 0/1

L3Switch(config-if)# switchport trunk encapsulation dot1q

```
L3Switch(config-if)# switchport mode trunk
```

之后创建 VLAN 并进入 VLAN 接口配置 IP 地址：

```
L3Switch(config)# vlan 10
L3Switch(config-vlan)# vlan 20
L3Switch(config-vlan)# exit
L3Switch(config)# interface vlan 10
L3Switch(config-if)# ip address 192.168.10.101 255.255.255.0
L3Switch(config-if)# no shutdown
L3Switch(config-if)# interface vlan 20
L3Switch(config-if)# ip address 192.168.20.101 255.255.255.0
L3Switch(config-if)# no shutdown
```

最后开启三层交换机的路由功能

```
L3Switch(config)# ip routing
```

现在可以使用 show ip route 命令检查路由表，并在主机上使用 ping 命令测试网络。

4. ACL

ACL（Access Control List，访问控制列表）可以用于禁止数据流通过，或只允许特定数据流通过（黑白名单）。ACL 类似于一个防火墙，ACL 是一系列 permit 或 deny 语句组成的顺序列表，它应用于地址或上层协议。在控制数据流进出网络方面，ACL 提供了一种功能强大的方法，可为所有被路由的网络协议配置 ACL。

ACL 是一个路由器配置脚本，它根据分组报头中的条件控制路由器允许还是拒绝分组。ACL 是最常用的 IOS 软件功能之一，它还可用于选择数据流类型，以便对其进行分析、转发或其他处理。每当分组经过有 ACL 的接口时，路由器将按从上到下的顺序以每次一行的方式检查 ACL，以查找与分组匹配的语句。ACL 使用允许或拒绝规则决定分组的命运，从而执行一条或多条安全策略。还可配置 ACL 来控制对网络或子网的访问。默认情况下，路由器没有配置任何 ACL，因此不会过滤数据流。

(1) 标准 ACL 与扩展 ACL

标准 ACL 只根据源 IP 地址过滤分组，而扩展 ACL 根据多种属性过滤 IP 分组，包括源和目标 IP 地址、源和目标 TCP/UDP 端口、协议类型（IP、ICMP、UDP、TCP 或协议号）。

ACL 命令在全局配置模式下创建。

下面是一个标准 ACL 命令，其允许来自网络 192.168.30.0/24 的所有数据流：

R1(config)# access-list 10 permit 192.168.30.0 0.0.0.255

由于末尾的隐式 deny any 语句，该 ACL 将拒绝其他所有数据流。

下面是一条扩展 ACL 命令，其允许从网络 192.168.30.0/30 发送任何主机的 80 端口数据流。

R1(config)# access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80

使用命令 show access-list 可以查看当前设置的 ACL。

(2) 编号 ACL 和命名 ACL

ACL 也可分为编号 ACL 和命名 ACL。编号 ACL 适用于在有较多类似数据流的小型网络中定义 ACL 类型。因为无法通过编号知晓 ACL 用途，所以当前更多使用名称来标识 ACL。

- 编号 ACL
  - ✧ 标准 IP ACL：1~99 和 1300~1999：；
  - ✧ 扩展 IP ACL：100~199 和 2000~2699：；
  - ✧ 其他协议：200~1299。
- 命名 ACL
  - ✧ 名称中可以包含字母数字字符；
  - ✧ 建议名称以大写字母书写；
  - ✧ 名称中不能包含空格或标点，而且必须以字母开头。

(3) 标准 ACL 配置

标准 ACL 完整语法如下：

R1(config)# access-list <access-list-number> <deny|permit|remark> <source>

[<source-wildcard>][1og]

- access-list number，ACL 编号，取值范围为 1~99 和 1300~1999（标准 ACL 编号）
- deny | permit，符合条件时拒绝丨符合条件时允许
- remark，在 IP 访问列表中添加备注，以提高列表的可读性
- source，发送分组的网络或主机的编号，指定 source 的方式有两种：
  - 使用 32 位的点分十进制格式；
  - 使用关键字 any 表示 source 和 source-wildcard 分别为 0.0.0.0 和 255.255.255.255
- source-wildcard（可选），应用于 source 的通配符，指定 source-wildcard 的方式有两种：
  - 使用 32 位的点分十进制格式，将要忽略的位设置为 1；
  - 使用关键字 any 表示 source 和 source-wildcard 分别为 0.0.0.0 和 255.255.255.255
  - **source-wildcard 中 bit 位为 1 时，对应的 IP 地址 bit 位通配（即 0 和 1 均匹配）**
- 1og（可选），将因分组匹配条目而生成的日志消息发送到控制台（使用命令 logging console 可指定要发送到控制台的消息级别）
  - 消息包含 ACL 号、分组被允许还是拒绝、源地址和分组数
  - 消息将在出现与条件匹配的第一个分组时生成，随后每 5 分钟生成一次，其中包含在过去的 5 分钟内被允许或拒绝的分组数

以下是若干范例：

拒绝来自 192.168.8.201 的所有数据流：

```
R1(config)# access-list 50 deny 192.168.8.201
```

接受来自 192.168.8.0/30 的所有数据流（隐含拒绝其他所有）：

```
R1(config)# access-list 60 permit 192.168.8.0 0.0.0.3
```

为 60 号 ACL 添加备注，每条备注不能超过 100 个字符：

```
R1(config)# access-list 60 remark This ACL is to control the outbound router traffic.
```

可以使用命令的 no 形式删除 ACL，如删除编号为 10 的 ACL：

```
R1(config)# no access-list 10
```

关于通配符，并不是只有末尾的内容才可以通配。例如：

```
access-list 60 permit 192.168.8.1 255.0.0.0
```

就可以匹配(0~255).168.8.1 的地址允许它们通过。这种情况很少见。

如果匹配某一网段的 IP，可以发现通配符是子网掩码的补码。

配置标准 ACL 后，可使用下面命令将其关联到接口（在接口配置模式下）：

R1(config-if)# ip access-group <access_list_num | access_list_name> <in | out>

要删除 ACL，首先在接口配置模式下执行命令 no ip access-group，然后在全局配置模式下执行命令 no access-list 将 ACL 删除。

使用 ACL 也可以控制 VTY 访问，这需要用到命令 access-class：

R1(config-line)# access-class <access_list_num | access_list_name> <in [vrf-also] | out>

命令 access-class 可用于限制进入和离开路由器终端虚拟线路（VTY）的 Telnet 会话。

过滤 Telnet 数据流通常被认为是一种扩展 IP ACL 功能，因为它过滤高层协议。然而，由于是使用命令 access-class 根据源地址过滤进出的 Telnet 会话，并将过滤应用于 VTY 线路，因此可使用标准 ACL 语句来控制 VTY 访问。

(4) 扩展 ACL 配置

扩展 ACL 除了增加更多匹配向，其基本于标准 ACL 没有区别（注意编号 ACL 的编号范围）。配置编号扩展命令语法如下：

access-list <access-list-number> <deny | permit | remark> <protocol> <source> <source-wildcard> [<operand> [<port port-number> | <name>]] [<destination> < destination-wildcard> [<operand> [<port port-number> | <name>]]] [established]

- access-list-number：使用 100~199 或 2000~2699 的编号标识访问列表
- protocol：常见的关键字包括 icmp、ip、tcp 和 udp。要与任何 Intemet pmoocol 协议（包括 ICMP、TCP 和 UDP）都匹配，可使用关键字 ip
- source/destination：分组源/目的的网络或主机的编号
- source-wildcard：用于源地址的通配符掩码
- operand：（可选）比较源/目标端口。可能的运算符包括 lt（小于）、gt（大于）、eq（等于）、neq（不等于）和 range（闭区间）。
- port-name|name：（可选）十进制的 TCP/UDP 端口号或名称。
- established：（可选）只适用于 TCP 协议，表明已建立连接。

(5) 命名 ACL 配置

命名 ACL 的配置与编号 ACL 有一些差异，其配置命令如下：

R1(config)# access-list <standard | extend> name

随后 CLI 进入标准命名 ACL 配置模式，可使用 permit 或 deny 语句创建一个或多个条件：

R1(config-std-nacl)# [sequence_num] <permit | deny | remark> <source> [<source-wildcard>][1og]

再随后使用命令 ip access-group 将命名 ACL 应用于端口：

R1(config-if)# access-group name <in | out>

5. SVI

SVI（Switch Virtual Interface，交换机虚拟端口）是交换机上的逻辑第三层接口（功能上等价于路由器的路由端口），配置 SVI 的目的包括：

- 为 VLAN 提供默认网关，允许流量在 VLAN 之间路由（主要用在三层交换机）；
- 提供 fallback bridging；
- 提供到交换机的第 3 层 IP 连接；
- 支持桥接配置和路由协议；

一个 SVI 代表一个由交换端口构成的 VLAN，以便于实现系统中路由和桥接的功能。SVI 接口即通常所谓的 VLAN 接口，不过它是虚拟的，用于连接整个 VLAN，所以其也经常被称为逻辑三层接口。一个 VLAN 仅可以有一个 SVI。

在交换机的管理 VLAN 上配置 IP 地址和子网掩码的步骤如下（假设 VLAN99 为管理 VLAN）：

```
// 进入 VLAN99 的接口配置模式
S1(config)# interface vlan 99
// 配置接口 IP 地址
S1(config-if)# ip address <ip_address> <netmask>
// 启动接口
S1(config-if)# no shutdown
S1(config-if)# end
```

之后就可以为这一 VLAN 分配端口了。

6. 交换机端口安全性配置

未提供端口安全性的交换机将允许攻击者连接到系统上未使用的已启用端口，并执行信息收集或攻击。配置端口安全性的一些方法如下：

使端口安全性的模式：

- 静态安全 MAC 地址：静态 MAC 地址是在接口配置模式下使用 switchport port-security mac-address <mac-address>命令手动配置的。以此方法配置的 MAC 地址存储在地址表中，并添加到交换机的运行配置中。
- 动态安全 MAC 地址：动态 MAC 地址是动态获取的，并且仅存储在地址表中。以此方式配置的 MAC 地址在交换机重新启动时将被移除。
- 粘滞安全 MAC 地址：可以将端口配置为动态获得 MAC 地址，然后将这

些 MAC 地址保存到运行配置中。

- 粘滞安全 MAC 的一些配置如下：
  - 当使用 switchport port-security mac-address sticky 接口配置命令在接口上启用粘滞获取时，接口将所有动态安全 MAC 地址（包括那些在启用粘滞获取之前动态获得的 MAC 地址）转换为粘滞安全 MAC 地址，并将所有粘滞安全 MAC 地址添加到运行配置。
  - 如果使用 no switchport port-security mac-address sticky 接口配置命令禁用粘滞获取，则粘滞安全 MAC 地址仍作为地址表的一部分，但是已从运行配置中移除。已经被删除的地址可以作为动态地址被重新配置和添加到地址表。
  - 如果使用 switchport port-security mac-address sticky <mac_address>接口配置命令配置粘滞安全 MAC 地址时，这些地址将添加到地址表和运行配置中。如果禁用端口安全性，则粘滞安全 MAC 地址仍保留在运行配置中。
  - 如果将粘滞安全 MAC 地址保存在配置文件中，则当交换机重新启动或者接口关闭时，接口不需要重新获取这些地址。如果不保存粘滞安全地址，则它们将丢失。如果粘滞获取被禁用，粘滞安全 MAC 地址则被转换为动态安全地址，并被从运行配置中删除。
  - 如果禁用粘滞获取并输入 switchport port-security mac-address sticky <mac-address>接口配置命令，则会出现错误消息，并且粘滞安全 MAC 地址不会添加到运行配置。

当出现以下任一情况时，会发生安全违规：

- 地址表中添加了最大数量的安全 MAC 地址，有工作站试图访问接口，而该工作站的 MAC 地址未出现在该地址表中。
- 在一安全接口上获取或配置的地址出现在同一个 VLAN 中的另一个安全接口上。

根据出现违规时要采取的操作，可以将接口配置为 3 种违规模式之一：

- 保护（protect）：当安全 MAC 地址的数量达到端口允许的限制时，带有未知源地址的数据包将被丢弃，直至移除足够数量的安全 MAC 地址或增加允许的最大地址数。不会得到发生安全违规的通知。
- 限制（restrict）：当安全 MAC 地址的数量达到端口允许的限制时，带有

未知源地址的数据包将被丢弃，直至您移除足够数量的安全 MAC 地址或增加允许的最大地址数。在此模式下，您会得到发生安全违规的通知。具体而言就是，将有 SNMP 陷阱发出、syslog 消息记入日志，以及违规计数器的计数增加。

- 关闭（shutdown）：在此模式下，端口安全违规将造成接口立即变为错误禁用（error-disabled）状态，并关闭端口 LED。该模式还会发送 SNMP 陷阱、将 syslog 消息记入日志，以及增加违规计数器的计数。当安全端口处于错误禁用状态时，先输入 shutdown 再输入 no shutdown 可使其脱离此状态。此模式为默认模式。

设置惩罚措施的命令如下：

Switch(config-if)# switchport port-security violation [protect|restrict|shutdown]

默认情况下，端口安全性在端口上禁用，安全 MAC 地址最大数量为 1，违规模式设置为关闭，粘滞地址获取选项为禁用。

启用端口安全性时，在端口配置模式下使用命令 switchport port-security 即可，需注意首先把接口设置为 access 模式，动态端口不可配置为安全端口。

设置最大允许的安全地址数量的命令为：switchport port-security maximum <num>

7. RIPv2

RIP（Routing Information Protocols，路由信息协议）是应用较早、使用较普遍的 IGP（Interior Gateway Protocol，内部网关协议），适用于小型同类网络，是典型的距离矢量（distance-vector）协议。其以跳数做为度量值，规定最大跳数为 15。其包含 3 种计时器：更新计时器、无效计时器、刷新计时器。它让每台路由器周期性地向每个相邻的邻居发送完整的路由表。路由表包括每个网络或子网的信息，以及与之相关的度量值。

(1) 启动和检验 RIPv2

启动 RIPv2 需要执行下面两条命令（没有第二条命令则启动 RIPv1）：

R1(config)# router rip
R1(config-router)#version 2

之后可在路由配置模式中使用命令 network <addr>指定网络，该命令的具体作用包括：

- 在属于某个指定网络的所有接口上启用 RIP；

- 相关接口则将开始发送和接收 RIP 更新，即在每 30s 一次的 RIP 路由更新中向其他路由器通告该指定网络。

(2) 被动接口（Passive Interface）

有些路由器含有一些不和其他路由器连接的接口，因此没有必要从这些接口向外发送路由更新。可以在 RIP 配置中使用 passive-interface 命令，不让该接口发送这些更新。

在 LAN 上发送不需要的更新会在以下 3 个方面对网络造成影响：

1) 带宽浪费在传输不必要的更新上。因为 RIP 更新是广播，所以交换机将向所有端口转发更新。
2) LAN 上的所有设备都必须逐层处理更新，直到传输层后接收设备才会丢弃更新。
3) 在广播网络上通告更新会带来严重的风险。RIP 更新可能会被数据包嗅探软件中途截取。路由更新可能会被修改并重新发回该路由器，从而导致路由表根据错误度量误导流量。

停止不需要的更新命令如下：

R1(config-router)# passive-interface <interface-type> <interface-number>

例如：passive-interface g0/0。请注意，子接口默认也会被广播。

所有的路由协议都支持 passtive-interface 命令。进行常规路由配置时，应在适当的时候使用 passive-interface 命令。

(3) 自动汇总（Auto-summary）

在路由表中路由越少就意味着能够更快地定位转发数据包的路由。汇总多条路由到一条就是我们所知道的路由汇或路由聚合。一些路由协议，比如 RIP，能够在某些路由器上自动的汇总。RIPv1（有类路由协议（分类 IP））是开启路由汇总且不能取消，RIPv2 作为无类路由协议（无类别域间路由）可以取消这一操作。

路由汇总（路由聚合）的优点是可以使接收和发送的路由更新更小，是路由之间的更新占用较少带宽，但其不支持不连续网络（将一个有类网络的两个或更多的子网通过另一个有类网络连接在一起的互连网络），因为有类路由协议的路由更新中不包含子网掩码。

在 RIPv2 中禁用自动汇总的命令为 no auto-summary。

(4) 默认路由与传播

默认路由是路由器用来在路由表中没有特定路由的情况下，表示所有路由的方法。默认路由经常用来访问非本地管理网络，比如 Internet。

要在 RIP 路由域中为所有其他网络提供 Intemet 连接，需要将默认静态路由通告给使用该动态路由协议的其他所有路由器。可以在路由器上配置静态默认路由，但这种方法没有扩展性

在 RIP 等许多路由协议中，可在路由器配置模式中使用命令 **default-information originate** 指定该路由器为默认信息来源，由该路由器在 RIP 更新中传播静态默认路由。

8. 监控日志管理

(1) 时间戳

要将系统配置为对调试消息或日志消息进行时间戳记，需使用全局配置命令 service timestamps。使用此命令的 no 形式禁用此服务：

service timestamps type [uptime]

service timestamps type datetime [msec] [localtime] [show-timezone]

- type：要加时间戳的消息类型：debug 或 log。
- uptime：（可选）自系统重新启动以来经历的时间。
- datetime：带日期和时间的时间戳。
- mesc：（可选）在日期和时间戳中包含毫秒。
- localtime：（可选）相对于本地时区的时间戳。
- show-timezone：（可选）在时间戳中包含时区名称。

(2) NTP 服务器

ntp server <ip-address | ipv6-address | dns-name> [key <key-id>] [maxpoll <max-poll>] [minpoll <min-poll>] [prefer] [use-vrf <vrf-name>]

指定 NTP 服务器的地址，与服务器建立关联，key 关键字可以配置与 NTP 服务器通信时要使用的密钥。key-id 参数的范围是 1 到 65535。使用 maxpoll 和 minpoll 关键字配置轮询对等方的最大和最小间隔。的范围内为最大轮询和分钟

轮询参数是从 4 到 16 秒，和默认值分别为 6 和 4。使用 prefer 的关键字，使这个服务器成为首选 NTP 服务器。使用 use-vrf 关键字将 NTP 服务器配置为通过指定的 VRF（虚拟路由转发（Virtual Routing Forwarding））进行通信。所述 vrf-name 参数可以是 default、management，或任何区分大小写字母数字字符串，最多 32 个字符。

如果路由设备通过 NTP 同步到外部时间源，并且您希望硬件时钟同步到 NTP 时间，请在全局配置模式下使用 ntp update-calendar 命令。

(3) 日志服务器

要在指定的主机名或 IPv4/IPv6 地址上配置远程 syslog 服务器，请使用 logging server 命令。要禁用远程系统日志服务器，请使用此命令的 no 形式，命令的基本形式如下：

logging server <host> [severity-level] [facility <facility>s| use-vrf {vrf_name | management}]

host 即远程系统日志服务器的主机名或 IPv4/IPv6 地址，severity-level 是应该在其中记录消息的所需严重性级别的编号。记录低于或低于指定级别的消息。facility 可以指定传出工具，vrf_name 指定要在远程服务器中使用的虚拟路由和转发（VRF）。该名称最多可以包含 32 个字母数字字符。management 指定管理 VRF。这是默认的 VRF。

登录后使用 logging trap 可以限制记录到 syslog 服务器的消息：

logging trap level

日志等级如下

0：紧急(Emergencies)
1：告警(Alerts)
2：严重的(Critical)
3：错误(Errors)
4：警告(Warnings)
5：通知(Notifications)
6：信息(Informational)
7：调试(Debugging)

五、实验内容

实验拓扑如图 6 所示：

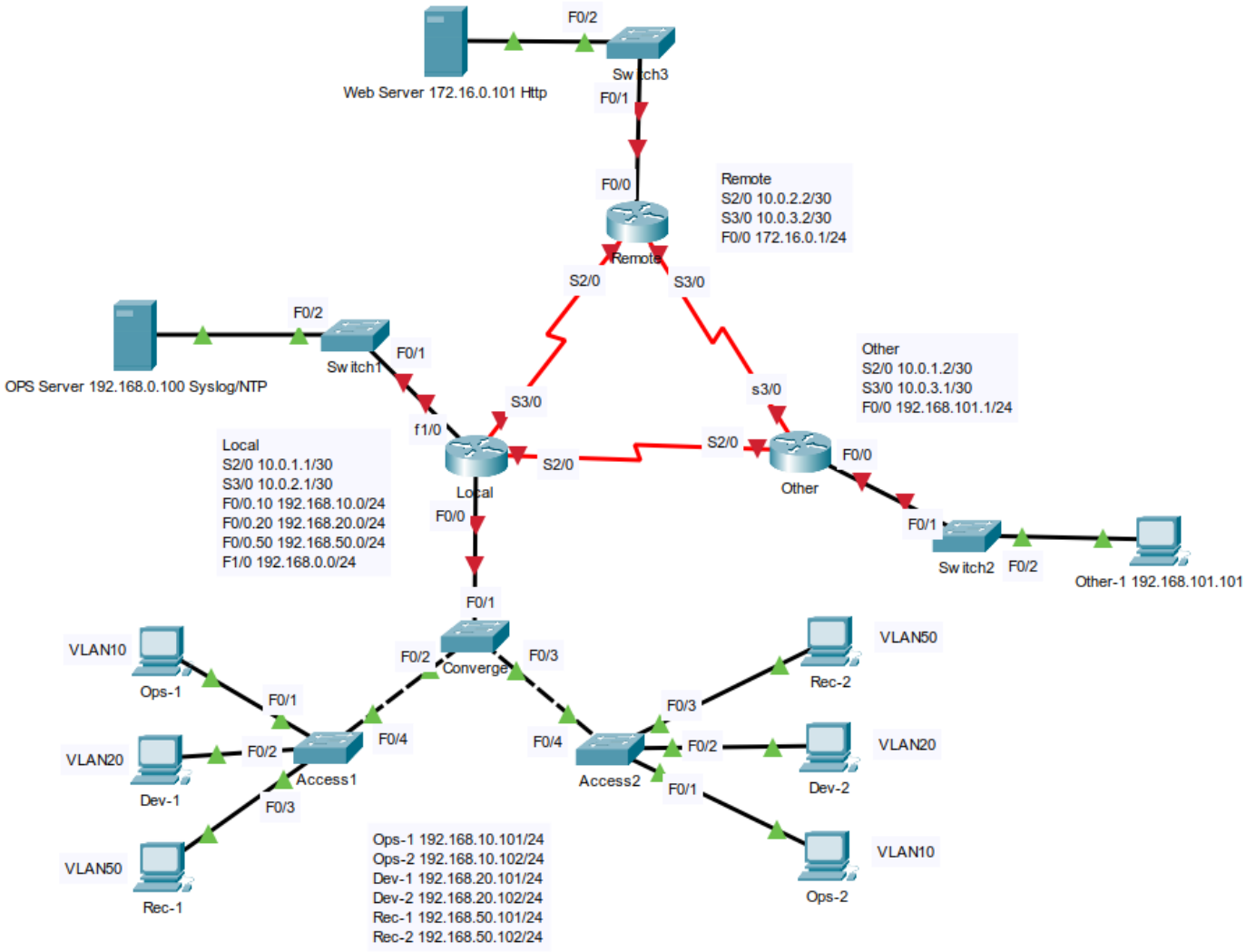

图 6 实验使用的拓扑

此实验要求执行基本的路由器配置任务，设定路由器接口和主机地址，并配置 VLAN、中继和 VLAN 之间路由。还要求配置 RIPv2，并使用 ACL 控制对路由器 VTY 线路的访问。

需要从终端连接到设备控制台来完成所有 IOS 设备配置。

Local 路由器：

基本设备配置

接口编址

VLAN 间路由

RIPv2 路由

对 VTY 的标准命名 ACL

带有 NTP 时间戳的 Syslog 日志记录

Remote、Other 路由器：

RIPv2 路由

Converge：

VLAN 和中继

接口管理

Access1：

VLAN 和中继

端口安全配置

接口管理

Access2：

VLAN 和中继

端口安全配置

接口管理

Access 中主机：

IP 地址、子网掩码、网关

地址表：

Device	**Interface**	**Network/Address**
Local	S2/0	10.0.1.1/30
	S3/0	10.0.2.1/30
	F0/0.10	192.168.10.0/24
	F0/0.20	192.168.20.0/24
	F0/0.50	192.168.50.0/24
	F1/0	192.168.0.0/24
Remote	S2/0	10.0.2.2/30
	S3/0	10.0.3.2/30
	F0/0	172.16.0.1/24
Other	S2/0	10.0.1.2/30

	S3/0	10.0.3.1/30
	F0/0	192.168.101.1/24
Converge	SVI	192.168.10.10
Access1	SVI	192.168.10.11
Access2	SVI	192.168.10.12
Ops-1	NIC	192.168.10.101/24
Ops-2	NIC	192.168.10.102/24
Dev-2	NIC	192.168.20.101/24
Dev-2	NIC	192.168.20.102/24
Rec-1	NIC	192.168.50.101/24
Rec-2	NIC	192.168.50.102/24
Other-1	NIC	192.168.101.101
Ops Server	NIC	192.168.0.100/24
Web Server	NIC	172.16.0.101/24

VLAN表：

VLAN	**Name**	**Network/Address**	**Port Assignments**
10	OPS (Management)	192.168.10.0/24	Converge: SVI; Access1: SVI, F0/1; Access2: SVI, F0/1
20	DEV	192.168.20.0/24	Access1: Fa0/2; Access2: F0/2
50	REC	192.168.50.0/24	Access1: Fa0/3; Access2: F0/3

六、实验器材

Packet Tracer

七、实验步骤

1. 在 Local 路由器上完成基本设置：

① 禁用 DNS 查找。

② 使用地址表中显示的名称配置设备。

③ 配置密码加密。

④ 指定特权执行模式密码的加密类型。

⑤ 配置 MOTD 标语以警告用户禁止未经授权的访问。

⑥ 配置控制台行，使路由器状态消息不会中断命令行输入。

⑦ 配置控制台访问密码以通过密码才能访问。

⑧ 将 VTY 端口配置为仅接受通过 SSH 的连接。配置值如下：

```
Domain Name: test.com
Local Username: admin
User Password: class
Modulus: 1024
Version: 2
```

2. Local 接口编址

使用地址表中给出的 IP 地址激活并配置主路由器的 S2/0、S3/0 和 F1/0 接口，并配置这些接口的描述。（F0/0 接口将在后面的步骤中进行配置）。

3. VLAN 和中继

根据 VLAN 表中的值，为交换机 Converge、Access1 和 Access2 配置 VLAN 以及 VLAN 中继。

(1) 在交换机中添加 VLAN。

(2) 按照 VLAN 表中的名称命名 VLAN。

(3) 将 Converge、Access1 和 Access2 交换机之间的链接配置为中继。将 Converge 和 Local 之间的链接配置为中继。所有中继接口都应静态配置为中继。

(4) 将相应的端口分配给 VLAN。

4. VLAN 间路由

使用地址表和 VLAN 表中的信息在 Local 路由器上对 VLAN 配置路由。

5. 访问控制列表（ACL）配置

配置满足以下要求的命名标准 ACL：

(1) 列表命名为 "block20"。

(2) 防止任何在 VLAN20 上的主机访问 Local 的 VTY 线路。

(3) 其他所有主机的通信都应允许。

(4) 该列表应包含两条语句。② 和 ③ 中的每个要求分别一条。

6. 交换机虚拟接口（SVI）配置

根据地址表和 VLAN 表中的信息，在 Converge、Access1 和 Access2 上配置交换机虚拟管理接口。所有主机都应该能访问这些交换机（即使不在同一个网络中）。

7. 交换机端口安全性配置

通过以下要求配置 Access 交换机来提高安全性。

(1) 禁用所有未使用的交换机端口;
(2) 在所有已连接主机的端口上激活端口安全功能;
(3) 最多仅允许两个 MAC 地址访问 Active 端口;
(4) 配置交换机端口以自动获知两个允许的 MAC 地址并在运行配置中记录;
(5) 配置交换机端口，使之在超过每个端口的最大地址数时，丢弃具有未知源地址的数据包，直到一定数量的 secure MAC 地址被删除而留出给新地址的空间为止。发生的违规不需要进行通知。

8. 动态路由 RIPv2

在 Local、Remote 和 Other 上配置 RIPv2 路由。

(1) 在 Local、Remote 和 Other 上配置 RIPv2，使所有网络均可访问。
(2) 配置所有 LAN 物理接口，以使 RIP 更新不会发送到 LAN。
(3) 确保使用支持无类别路由的 RIP 版本。
(4) 阻止 RIP 自动汇总网络。
(5) 配置 RIP 以自动将 Other 上已配置的默认路由发送到 Local 和 Remote。

9. 配置网络监控

在 Local 上配置 NTP 和 Syslog 服务。

(1) 激活日志（log）和调试（debug）的时间戳服务。
(2) 将 Local 配置为 NTP 客户端。NTP 服务器是 Ops Server，地址为 192.168.0.100。

(3) 配置系统日志以将调试（debugging）级别的消息发送到 Ops Server。

10. 配置主机地址

为连接到 Access 的主机配置地址，以便它们可以通过 IP 地址连接到互联网上的 Web Server 服务器。需要的信息在地址表中有提供。

七、实验步骤

1. 在 Local 路由器上完成基本设置：

① **禁用 DNS 查找。**

Router(config)#no ip domain-lookup

//为了避免输错命令后路由器查询域名系统长时间没有反应，在实验时首先使用该名利，禁用 DNS 查找。原因是对于系统不认识的命令它会把它当做一个域名去网上寻求域名解析，很费时间。

② **使用地址表中显示的名称配置设备。**

Router(config)#hostname Local

③ **配置密码加密。**

Local(config)#service password-encryption

!使用该命令对口令加密，防止将口令显示为明文。

④ **指定特权执行模式密码的加密类型。**

Local(config)#enable secret class

!设置访问特权执行模式的口令为 class，且该口令以加密方式保存（secret）。

⑤ **配置 MOTD 标语以警告用户禁止未经授权的访问。**

Local(config)#banner motd $users that unauthorized access is prohibited$

⑥ **配置控制台行，使路由器状态消息不会中断命令行输入。**

Local(config)#line console 0

Local(config-line)#logging synchronous

!设置同步输入，使路由器状态消息不会中断命令行输入。

⑦ 配置控制台访问密码以通过密码才能访问。

Local(config-line)#password cisco

!设置控制台的访问密码为 cisco

Local(config-line)#login

⑧ 将 VTY 端口配置为仅接受通过 SSH 的连接。配置值如下：

```
Domain Name: test.com
Local Username: admin
User Password: class
Modulus: 1024
Version: 2
```

Local(config)#ip domain-name test.com
//使用 ip domain-name 命令配置域名：test.com
Local(config)#username admin password class
//创建一个本地用户 admin，口令为：class
! SSH 配置
Local(config)#crypto key generate rsa
! 使用该命令生成 RSA 非对称密钥
How many bits in the modulus [512]: 1024 ！选择 1024 作为加密密钥强度
Local(config)#ip ssh version 2
!配置 SSH 的版本为 2
Local(config)#line vty 0 15
!进入线路 vty 配置模式，对序号为 0-15 的所有线路同时进行配置
Local(config-line)#transport input ssh
!让 VTY 接受 SSH 连接
Local(config-line)#login local
!根据本地数据库进行身份验证
Local(config-line)#exit

2. Local 接口编址

使用地址表中给出的 IP 地址激活并配置主路由器的 S2/0、S3/0 和 F1/0 接口，并配置这些接口的描述。（F0/0 接口将在后面的步骤中进行配置）。

! 广域网

Local(config)# interface serial 2/0

!进入接口 serial 2/0 的配置模式

Local(config-if)#clock rate 2000000

!设置串口的波特率，正常情况下，最大的波特率就是 2000000，设置该命令后，可能出现以下的错误提示，这个没有关系。

This command applies only to DCE interfaces

原因是：对于串行同步通信设备，需要同步时钟信号。因此在串行线缆两端的设备，一段将产生一个时钟信号，而另一段则被动的接收时钟信号。主动产生时钟信号的设备，称为 DCE（数据通信设备），而被动接收时钟信号的设备，称为 DTE（数据终端设备）。因此对于连接两台路由的串行电缆，一端是 DCE（把鼠标放置在串行线缆上，端口标号前有一个小时钟的那个），另外一段是 DTE（标号前没有小时钟的那个）。只能对 DCE 设备设置波特率。

Local(config-if)#ip address 10.0.1.1 255.255.255.252

!配置 serial 2/0 接口的 IP 地址和子网掩码

Local(config-if)#no shutdown

!激活端口

Local(config-if)# interface serial 3/0

!进入接口 serial 3/0 的配置模式

Local(config-if)#clock rate 2000000

!设置串口的波特率

Local(config-if)#ip address 10.0.2.1 255.255.255.252

!配置 serial 3/0 接口的 IP 地址和子网掩码

Local(config-if)#no shutdown

! 局域网

Local(config-if)# interface fastEthernet 1/0

Local(config-if)#ip address 192.168.0.1 255.255.255.0

Local(config-if)#no shutdown

=====以下为 Remote 路由器接口编址==========

Router(config)#int s2/0

Router(config-if)#clock rate 2000000

Router(config-if)#ip addr 10.0.2.2 255.255.255.252

```
Router(config-if)#no sh
Router(config-if)#int s3/0
Router(config-if)#clock rate 2000000
Router(config-if)#ip addr 10.0.3.2 255.255.255.252
Router(config-if)#no sh

Router(config-if)#int f0/0
Router(config-if)#ip addr 172.16.0.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#exit
=====以下为 Other 路由器接口编址==============
Router(config)#int s2/0
Router(config-if)#clock rate 2000000
Router(config-if)#ip addr 10.0.1.2 255.255.255.252
Router(config-if)#no sh
Router(config-if)#int s3/0
Router(config-if)#clock rate 2000000
Router(config-if)#ip addr 10.0.3.1 255.255.255.252
Router(config-if)#no sh

Router(config-if)#int f0/0
Router(config-if)#ip addr 192.168.101.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#exit
```

3. VLAN 和中继

根据 VLAN 表中的值，为交换机 Converge、Access1 和 Access2 配置 VLAN 以及 VLAN 中继。

(1) 在交换机中添加 VLAN。

(2) 按照 VLAN 表中的名称命名 VLAN。

！交换机 Converge 配置

```
Switch(config)#vlan 10
！配置 vlan 10，同时进入 vlan 10 的配置模式
Switch(config-vlan)#name OPS
！设置 vlan 10 的名称为 OPS
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name DEV
Switch(config-vlan)#vlan 50
Switch(config-vlan)#name REC
Switch(config-vlan)#exit
```

！交换机 Access1 配置

同上面交换机 Converge 配置

！交换机 Access2 配置

同上面交换机 Converge 配置

(3) 将 Converge、Access1 和 Access2 交换机之间的链接配置为中继。将 Converge 和 Local 之间的链接配置为中继。所有中继接口都应静态配置为中继。

！交换机 Converge 配置：交换机 Converge 一共有 3 个端口需要配置为 trunk 模式，分别是：f0/1、f0/2、f0/3

```
Switch(config)#interface fastEthernet 0/1
！进入交换机 Converge 端口 fastEthernet 0/1 的配置模式
Switch(config-if)#switchport mode trunk
！设置给端口为中继（trunk 干线）模式
Switch(config-if)#interface fastEthernet 0/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#interface fastEthernet 0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

！交换机 Access1 配置

```
Switch(config)#interface fastEthernet 0/4
！进入交换机 Access1 端口 fastEthernet 0/4 的配置模式
Switch(config-if)#switchport mode trunk
！设置给端口为中继（trunk 干线）模式
```

！交换机 Access2 配置

Switch(config)#interface fastEthernet 0/4
！进入交换机 Access2 端口 fastEthernet 0/4 的配置模式
Switch(config-if)#switchport mode trunk
！设置给端口为中继（trunk 干线）模式

(4) 将相应的端口分配给 VLAN。

！交换机 Converge 配置

！交换机 Converge 只使用 3 个 trunck 端口，其余端口未使用，因此不用分配。

！交换机 Access1 配置

！交换机 Access1 除 f0/4 用于连接 Converge 交换机（trunk 模式）外，还使用了 f0/1、f0/2、f0/3 一共 3 个端口，分别连接 VLAN10、VLAN10、VLAN10
Switch(config)#interface fastEthernet 0/1
！进入交换机 Access1 端口 fastEthernet 0/4 的配置模式
Switch(config-if)#switchport mode access
！设置该端口为 access 模式
Switch(config-if)#switchport access vlan 10
！使用 witchport access 名利，把该端口分配给 Vlan 10
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 50
Switch(config-if)#exit

！交换机 Access2 配置

配置同 Access1 交换机

4. VLAN 间路由

使用地址表和 VLAN 表中的信息在 Local 路由器上对 VLAN 配置路由。

Local(config)# interface fastEthernet 0/0.10
!进入 fastEthernet 0/0 接口的子接口配置模式，后面的.10，是子接口对应的 VLAN 的 ID 号。
Local(config-subif)#encapsulation dot1Q 10
！配置以太网子接口 vlan ID 为 10 的 VLAN，采用的封装格式为 802.1q
Local(config-subif)# ip address 192.168.10.1 255.255.255.0
！设置 fastEthernet 0/0 接口中，VLAN 10 对应的以太网子接口的 IP 地址。
Local(config-subif)# interface fastEthernet 0/0.20
！进入 fastEthernet 0/0.20 子接口的配置模式。
Local(config-subif)# encapsulation dot1Q 20

！配置以太网子接口 vlan ID 为 10 的 VLAN，采用的封装格式为 802.1q
Local(config-subif)#ip address 192.168.20.1 255.255.255.0
！设置 fastEthernet 0/0 接口中，VLAN 10 对应的以太网子接口的 IP 地址。
Local(config-subif)# interface fastEthernet 0/0.50
Local(config-subif)# encapsulation dot1Q 50
Local(config-subif)#ip address 192.168.50.1 255.255.255.0
Local(config-subif)# interface fastEthernet 0/0
！进入 fastEthernet 0/0 接口的配置模式
Local(config-if)#no shutdown
！激活端口
Local(config-if)#exit

5. 访问控制列表（ACL）配置

配置满足以下要求的命名标准 ACL：

(1) 列表命名为 "block20"。

(2) 防止任何在 VLAN20 上的主机访问 Local 的 VTY 线路。

(3) 其他所有主机的通信都应允许。

(4) 该列表应包含两条语句。② 和 ③ 中的每个要求分别一条。

Local(config)#ip access-list standard block20
！采用命名 ACL 配置方式，使用 ip access-list standard 命令创建一个名为 block20 的 ACL，并进入该标准命名 ACL 配置模式。
Local(config-std-nacl)#deny 192.168.20.0 0.0.0.255
！使用 deny 命令添加一项规则，禁止 VLAN20 上的主机访问。
Local(config-std-nacl)#permit any
！使用 permit 命令添加一项规则，允许所有主机访问。
Local(config-std-nacl)#exit
！退出标准命名 ACL 配置模式。
Local(config)#line vty 0 15
！进入 line vty 的配置模式，同时对 0-15 这几个线路进行配置。
Local(config-line)#access-class block20 in
！该刚才配置的名为 "block20"的 ACL 应用于所有的 vty 线路的输入(in)数据流的控制
Local(config-subif)#exit

注：大家可以发现：deny 192.168.20.0 0.0.0.255 和 permit any 两条规则有矛盾之处。这个时候，系统使用“深度优先”的原则，将规则按照精确度从高到底进行排序，系统按照精确度从高到低的顺序进行报文匹配。规则中定义的匹配项限制越严格，规则的精确度就越高，即优先级越高，那么该规则的编号就越小，系统越先匹配。例如，有一条规则的目的 IP 地址匹配项是一台主机地址 2.2.2.2/32，而另一条规则的目的 IP 地址匹配项是一个网段 2.2.2.0/24，前一条规则指定的地址范围更小，所以其精确度更高，系统会优先将报文与前一条规则进行匹配。因

此对于 deny 192.168.20.0 0.0.0.255 和 permit any 两条规则，系统将优先匹配 deny 192.168.20.0 0.0.0.255 规则，如果不能与之匹配，再和 permit any 匹配。

6. 交换机虚拟接口（SVI）配置

根据地址表和 VLAN 表中的信息，在 Converge、Access1 和 Access2 上配置交换机虚拟管理接口。所有主机都应该能访问这些交换机（即使不在同一个网络中）。

Converge、Access1 和 Access2 的 SVI 配置信息为：

Device	Interface	Network/Address
Converge	SVI	192.168.10.10
Access1	SVI	192.168.10.11
Access2	SVI	192.168.10.12

！交换机 Converge 配置

Switch(config)#interface vlan 10

！进入 vlan 10 的虚拟接口配置模式

Switch(config-if)#ip address 192.168.10.10 255.255.255.0

！设置 vlan 10 的虚拟接口 IP

Switch(config-if)#no shutdown

！激活 vlan 10 的虚拟接口

Switch(config-if)#exit

Switch(config)#ip default-gateway 192.168.10.1

！使用 ip default-gateway 命令设置缺省网关为：192.168.10.1

！注：由于交换机的 SVI 的 IP 的网络号为 192.168.10.0/24，因此网关需要和该 IP 具有相同的网络号。该网关 IP 为和该子网连接的路由器接口在 vlan 10 子接口的 IP。即 192.168.10.1。

！交换机 Access1 配置

Switch(config)#interface vlan 10

Switch(config-if)#ip address 192.168.10.11 255.255.255.0

Switch(config-if)#no shutdown

Switch(config-if)#exit

Switch(config)#ip default-gateway 192.168.10.1

！交换机 Access2 配置

Switch(config)#interface vlan 10

Switch(config-if)#ip address 192.168.10.12 255.255.255.0

Switch(config-if)#no shutdown

Switch(config-if)#exit

Switch(config)#ip default-gateway 192.168.10.1

7. 交换机端口安全性配置

通过以下要求配置 Access 交换机来提高安全性。

(1) 禁用所有未使用的交换机端口;

！对于 2 台 Access 交换机，都只使用 0/1-4 共 4 个端口，其余的 fastEthernet 0/5-24 和 gigabitEthernet 0/1-2 端口都没有使用。因此需要全部禁用

！交换机 Access1 配置

Switch(config)#interface range fastEthernet 0/5-24

！使用 interface range 命令同时对 fastEthernet 0/5-24 端口进行配置

Switch(config-if-range)#shutdown

！关闭所有的 20 个端口

Switch(config-if-range)#exit

Switch(config)#interface range gigabitEthernet 0/1-2

！使用 interface range 命令同时对 gigabitEthernet 0/1-2 端口进行配置

Switch(config-if-range)#shutdown

！关闭所有的 2 个端口

Switch(config-if-range)#exit

Switch(config)#

！交换机 Access2 配置

同交换机 Access1 配置

(2) 在所有已连接主机的端口上激活端口安全功能;

！交换机 Access1 配置

Switch(config)#interface range fastEthernet 0/1-3

！使用 interface range 命令同时对 fastEthernet 0/1-3 端口进行配置

Switch(config-if-range)#switchport port-security

！使用 switchport port-security 命令激活端口安全功能
Switch(config-if-range)#exit
！交换机 Access2 配置
同交换机 Access1 配置

(3) 最多仅允许两个 MAC 地址访问 Active 端口;

接口的 Port-Security 特性一旦激活后，默认的最大安全地址个数为 1，也就是说，只允许一个 MAC 作为安全地址接入该端口，而其余主机由于 mac 地址不匹配而无法通过该端口收发数据。

通过接口安全功能，能够限制接口（所连接的）的最大 MAC 数量，从而限制接入的主机用户；或者限定接口所连接的特定 MAC，从而实现接入用户的限制。

！交换机 Access1 配置
Switch(config)#interface range fastEthernet 0/1-3
！使用 interface range 命令同时对 fastEthernet 0/1-3 端口进行配置
Switch(config-if-range)#switchport port-security maximum 2
！最大允许的安全 MAC 地址数量为 2
Switch(config-if-range)#exit
！交换机 Access2 配置
同交换机 Access1 配置

(4) 配置交换机端口以自动获知两个允许的 MAC 地址并在运行配置中记录;

当设置了 Port-Security 接口的最大允许 MAC 的数量后，接口关联的安全地址表项可以通过如下方式获取：

- 在接口下使用 switchport port-security mac-address 来配置静态安全地址表项。
- 使用接口动态学习到的 MAC 来构成安全地址表项。
- 一部分静态配置，一部分动态学习。

！交换机 Access1 配置
Switch(config)#interface range fastEthernet 0/1-3
！使用 interface range 命令同时对 fastEthernet 0/1-3 端口进行配置
Switch(config-if-range)#switchport port-security mac-address sticky
！将动态安全地址配置为粘滞（sticky），这样自动获取的 mac 地址保存到运行配置中。
Switch(config-if-range)#exit
！交换机 Access2 配置
同交换机 Access1 配置

(5) 配置交换机端口，使之在超过每个端口的最大地址数时，丢弃具有未知源地址的数据包，直到一定数量的 secure MAC 地址被删除而留出给新地址的空间为止。发生的违规不需要进行通知。

！交换机 Access1 配置
Switch(config)#interface range fastEthernet 0/1-3
！使用 interface range 命令同时对 fastEthernet 0/1-3 端口进行配置
Switch(config-if-range)#switchport port-security violation protect

！设置端口的惩罚模式为 protect，
Switch(config-if-range)#exit 保护模式，安全 MAC 地址的数量达到端口允许的限制时，带有未知源地址的数据包将被丢弃，不会发生安全违规的通知。
！交换机 Access2 配置
同交换机 Access1 配置

8. 动态路由 RIPv2

在 Local、Remote 和 Other 上配置 RIPv2 路由。

(1) 在 Local、Remote 和 Other 上配置 RIPv2，使所有网络均可访问。

！路由器 Local 动态 rip 配置
Local(config)#route rip
！进入 rip 配置模式
Local(config-router)#version 2
！启动 RIPv2
Local(config-router)#network 10.0.1.0
！使用命令 network 命令，指明网络 10.0.1.0 所属的所有接口启用 RIP
Local(config-router)#network 10.0.2.0
！使用命令 network 命令，指明网络 10.0.2.0 所属的所有接口启用 RIP
Local(config-router)#network 192.168.10.0
Local(config-router)#network 192.168.20.0
Local(config-router)#network 192.168.50.0
Local(config-router)#network 192.168.0.0
Local(config-router)#exit

！路由器 Remote 动态 rip 配置
Router(config)#route rip
Router(config-router)#version 2
Router(config-router)#network 10.0.2.0
Router(config-router)#network 10.0.3.0
Router(config-router)#network 172.16.0.0
Router(config-router)#exit

！路由器 Other 动态 rip 配置
Router(config)#route rip
Router(config-router)#version 2
Router(config-router)#network 192.168.101.0
Router(config-router)#network 10.0.1.0
Router(config-router)#network 10.0.3.0
Router(config-router)#exit

(2) 配置所有 LAN 物理接口，以使 RIP 更新不会发送到 LAN。

！路由器 Local 动态 rip 配置
Local(config)#route rip
Local(config-router)#passive-interface f1/0
！禁止通过 interface f1/0 端口向与其相连接的网络转发路由更新消息。
Local(config-router)#passive-interface f0/0.10
！禁止通过 interface f1/0.20 子接口向与其相连接的网络转发路由更新消息。
Local(config-router)#passive-interface f0/0.20
Local(config-router)#passive-interface f0/0.50
Local(config-router)#passive-interface f0/0
Local(config-router)#exit
！路由器 Remote 动态 rip 配置
Router(config)#route rip
Router(config-router)#passive fastEthernet 0/0
Router(config-router)#end

！路由器 Other 动态 rip 配置
同路由器 Remote 配置

(3) 确保使用支持无类别路由的 RIP 版本。

注 RIPv2 就是支持无类别路由，前面已经设置过

(4) 阻止 RIP 自动汇总网络。

！路由器 Local 动态 rip 配置
Local(config)#route rip
！进入 rip 配置模式
Local(config-router)#no auto-summary
！禁用自动汇总网络

！路由器 Remote 动态 rip 配置
Router(config)#route rip
Router(config-router)#no auto-summary

！路由器 Other 动态 rip 配置
Router(config)#route rip
Router(config-router)#no auto-summary

(5) 配置 RIP 以自动将 Other 上已配置的默认路由发送到 Local 和 Remote。

！路由器 Other 动态 rip 配置
Router(config)#route rip
！进入 rip 配置模式
Router(config-router)#default-information originate

！使用命令 **default-information originate** 指定该路由器为默认信息来源，由该路由器在 RIP 更新中传播静态默认路由。

9. 配置网络监控

在 Local 上配置 NTP 和 Syslog 服务。

(1) 激活日志（log）和调试（debug）的时间戳服务。

Local(config)#service timestamps log datetime msec

！激活日志时间戳服务，使用带日期和时间的时间戳，且在日期和时间戳中包含毫秒。

Local(config)#service timestamps debug datetime msec

！激活调试时间戳服务，使用带日期和时间的时间戳，且在日期和时间戳中包含毫秒。

(2) 将 Local 配置为 NTP 客户端。NTP 服务器是 Ops Server，地址为 192.168.0.100。

Local(config)#ntp server 192.168.0.100

！ 指定 NTP 服务器的地址为 192.168.0.100

Local(config)#ntp update-calendar

！（可选）同步时钟

(3) 配置系统日志以将调试（debugging）级别的消息发送到 Ops Server。

Local(config)#logging 192.168.0.100

！ 配置日志服务器的地址为 192.168.0.100

Local(config)#logging trap debugging

！ 设置记录到日志系统的消息的基本为调试级别

10. 配置主机地址

为连接到 Access 的主机配置地址，以便它们可以通过 IP 地址连接到互联网上的 Web Server 服务器。需要的信息在地址表中有提供。

注：以下几台主机的网关统一为 192.168.10.1

Ops-1	NIC	192.168.10.101/24
Ops-2	NIC	192.168.10.102/24
Dev-2	NIC	192.168.20.101/24
Dev-2	NIC	192.168.20.102/24

Rec-1	NIC	192.168.50.101/24
Rec-2	NIC	192.168.50.102/24