《网络工程》

实验任务书

国防科学技术大学计算机学院

2024 年 11 月

目录

实验 1 制作网线

1. 实验目的

掌握制作 EIA/TIA 568B 标准制作直连线的方法；了解网线的内部结构。

2. 实验设备

- 网线钳
- 网线测试仪
- 双绞线若干
- RJ-45 水晶头若干

3. 实验原理

（1） 非屏蔽双绞线的内部结构

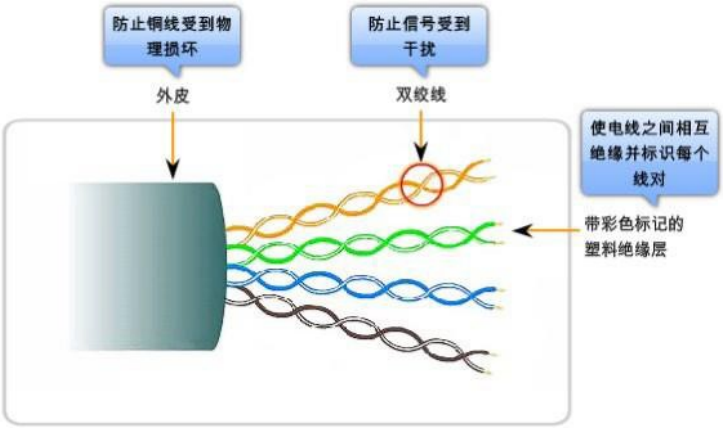


图 1 UTP 内部结构

Unshielded Twisted Paired 非屏蔽双绞线，简称 UTP。UTP 内部有四对不同颜色标记的双绞线，每对双绞线以固定间隔绞合在一起，绞合的作用是为抵消电脉冲传输过程中所形成的电磁场。外皮包裹着四对双绞线，防止内部铜线受到物理损伤。如图 1-1 所示。

（2） 非屏蔽双绞线与 RJ45 连接标准

EIA/TIA 制定的布线标准规定了不同颜色的 4 对双绞线与 RJ45 针脚连接。其中 EIA/TIA 568A 标准规定的线序为绿白、绿、橙白、蓝、蓝白、橙、棕白、棕，EIA/TIA 568B 标准规定的线序为橙白、橙、绿白、蓝、蓝白、绿、棕白、棕，如图 1-2 所示。国内普遍使用 EIA/TIA 568B 标准。

在 10Mb/s 和 100Mb/s 的以太网中只使用两对线，1、2 用于发送，3、6 用于接收。

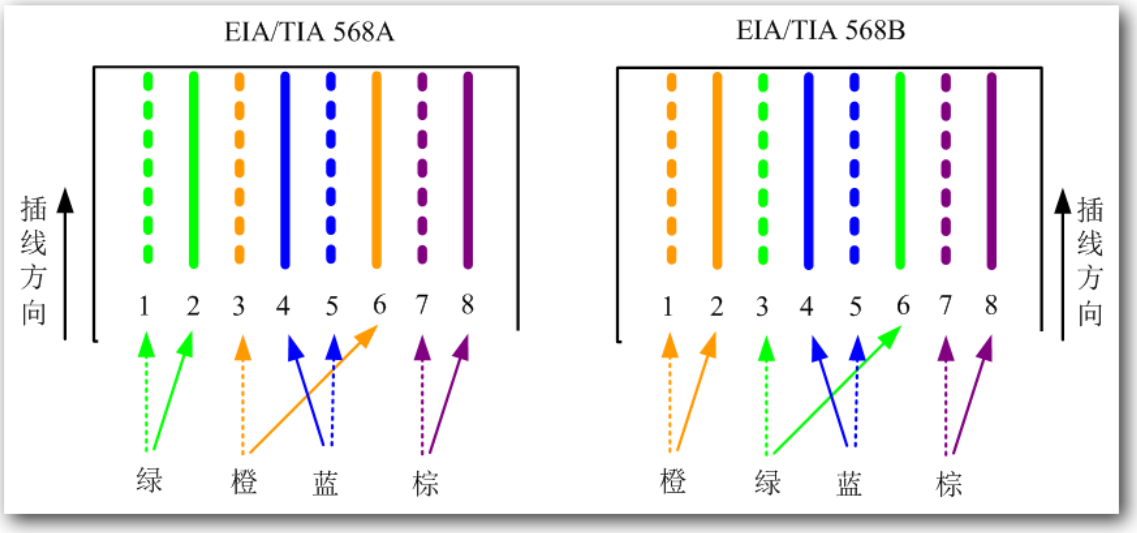


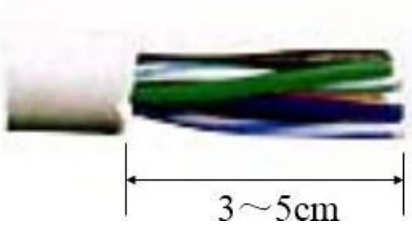
图 2 EIA/TIA 568A 和 EIA/TIA 568B 线序

4. 实验任务

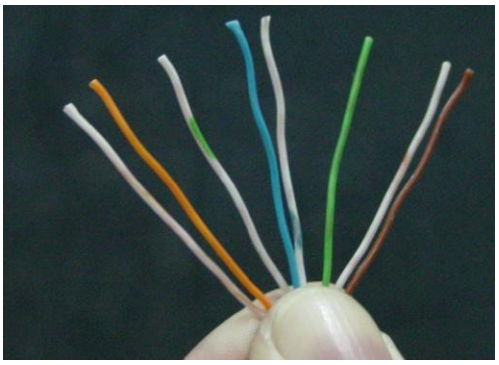
每人使用实验设备制作一根 1m 左右网线，使用测线仪测试网线各端口连通情况，并做好记录，使用自己制作的网线连接电脑与交换机，观察并记录连通情况。

5. 实验步骤

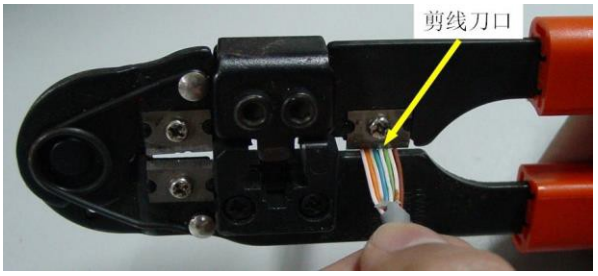
第一步：用网线钳前部剥线器剥除双绞线外皮 3～5 cm。

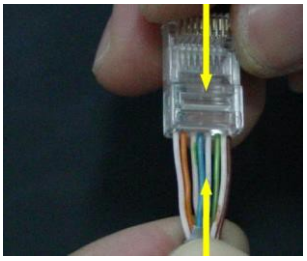


第二步：分离每一对线，将其弄直，将它们按白橙/橙/白绿/蓝/白蓝/绿/白棕/棕顺序排列。注意：绿色线应该跨越蓝色对线。

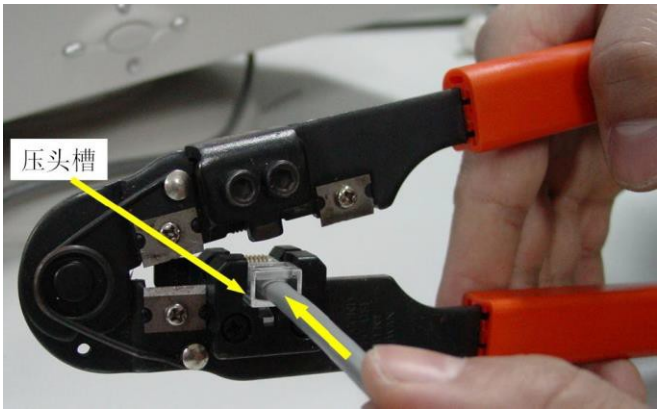


第三步：将上述网线钳剪齐，长度约为 14mm。再将双绞线的每一根线依序放入 RJ-45 接头的引脚内，第一只引脚内应该置放白橙色线，注意弹片端朝下 。





第四步：从水晶头正面目视每根双绞线已经放置正确并到达底部位置之后，可用网线钳用力压 RJ-45 接头，使水晶头内部的金属片恰好刺破双绞线的包皮与内部金属线良好接触。



第五步：重复第一步到第四步，再制作另一端的 RJ-45 接头。完成后的连接线两端的 RJ-45 接头，引脚和颜色完全一样。

选作内容：
参考上述步骤制作一根交叉线。

6. 实验测评

用网线测试仪检测该 RJ-45 接头的双绞线是否可用。测试仪由两部分组成。线

缆的两端接头分别插入测试仪的两部分中。线路两端的测试仪上的 LED 依次同时发光则说明线路正常；如果有某个或某些灯不亮或次序不对，则说明线路有问题。

如果接触不良，则需要尝试用网线钳用力压两端水晶头，使它们良好接触。

如果发现线序不对请将某端水晶头剪掉，重新按实验步骤，再制作一个 RJ-45 接头。

7. 思考题

1、如何检查双绞线的导通性？
2、直通线和交叉线的区别？
3、如果直连线两端线序发生了同样的错误，网线还能使用吗？

实验 2 交换机基础配置

1. 实验目的

理解 VLAN 的应用场景；
掌握 VLAN 的基本配置；
掌握 Accress、Trunk 接口的配置方法。

2. 实验设备

- 台式机
- 交换机
- 网线
- 配置线

3. 实验原理

VLAN技术

早期的局域网技术是基于总线型结构的。总线型拓扑结构是由一根单电缆连接着所有主机，这种局域网技术存在着冲突域问题，即所有用户都在一个冲突域中，那么同一时间内只有一台主机能发送消息，从任意设备发出的消息都会被其他所有主机接收到，用户可能收到大量不需要的报文；而且所有主机共享一条传输通道，任意主机之间都可以直接互相访问，无法控制信息的安全。为了避免冲突域，同时扩展传统局域网以接入更多计算机，可以在局域网中使用二层交换机。交换机能有效隔离冲突域，但是由于所有计算机仍处于同一个广播域，任意设备都能接收到所有报文，不但降低了网络的效率，而且降低了安全性，即广播域和信息安全问题依旧存在。为了能减少广播，提高局域网安全性，人们使用虚拟局域网即VLAN技术把一个物理的LAN在逻辑上划分成多个广播域。VLAN内的主机间可以直接通信，而VLAN间不能直接互通。这样，广播报文被限制在一个VLAN内，同时也提高了网络安全性。不同的VLAN使用不同的VLANID区分，VLANID的范围是0~4095，可配置的值为1~4094，0和4095为保留值。

华为交换机的接口模式

华为交换机的接口模式有三种：Access、Trunk和Hybrid。其中，Access、Trunk接口模式和Cisco交换机的接口模式一样，Hybrid接口是华为设备特有的接口模式，

Hybrid接口和Trunk接口的相同之处是都可以允许多个vlan的流量通过并打标签，不同之处在于Hybrid接口可以允许多个vlan的报文发送时不打vlan标签。

Access接口模式：Access接口必须加入某一vlan（这也是默认所有接口都属于vlan1的原因），对交换机而言，该接口只能允许一个vlan流量通行，且不打vlan标签，用于连接PC、服务器、路由器（非单臂路由）等设备。

Trunk接口模式：该接口默认允许所有vlan通行（用于承载多个vlan通行），且对每个vlan通过打不同标识加以区分，主要用于连接交换机等设备。

Hybrid接口模式：华为交换机接口默认为Hybrid模式（Cisco交换机默认为Access模式），既可以实现Access接口的功能，也可以实现Trunk接口的功能，可以在没有三层网络设备（路由器、三层交换机）的情况下实现跨vlan通信和访问控制（当然了，也有局限性，就是各个vlan中的IP地址都属于同一网段，否则，仍然需要通过三层网络设备来进行通信，）。相对于Access接口和Trunk接口具有更高的灵活性与可控性。

表 1 VLAN配置部分命令说明

操 作	命 令
操 作	命 令
创建VLAN	**vlan** *vlan-id* [**alias** *vlan-alias*]
删除VLAN	**undo vlan** *vlan-id* [**|all**]
VLAN视图下配置一个或一组端口属于某个VLAN	**port** interface-type { interface-num [**to** interface-num] } & <1-10>
接口视图下配置该端口属于某个VLAN	**port access vlan** *vlan-id*
指定端口类型：trunk, access, hybrid	**port** *link-type* { *trunk/access/hybrid}*
取消端口类型的设置	**undo port** *link-type* { *trunk/access/hybrid}*
设置Trunk端口可以通过的VLAN	**[undo] port trunk permit vlan** { {*vlan-id* [**to** *vlan-id*]}&<1-10> | **all** }
显示VLAN的信息	display vlan vlan-id [/all]
进入vlan 三层虚接口视图	interface vlan-interface *vlan-id*
配置静态路由	ip route-static <*ip_address*> *[* <*mask*> | <masklen>] interface_name> | <gateway_address> [preference <preference_value>] [reject |backhole]
显示路由信息	display ip routing-table

4. 实验内容

本实验模拟某公司网络场景。公司规模较大，员工200余名，内部网络是一个大的局域网。公司放置了多台接入交换机（如S1和S2）负责员工的网络接入。接入交换机之间通过汇聚交换机S3相连。公司通过划分VLAN来隔离广播域，由于员工

较多，相同部门的员工通过不同交换机接入。为了保证在不同交换机下相同部门的员工能互相通信，需要配置交换机之间链路为干道模式，以实现相同VLAN跨交换机通信。

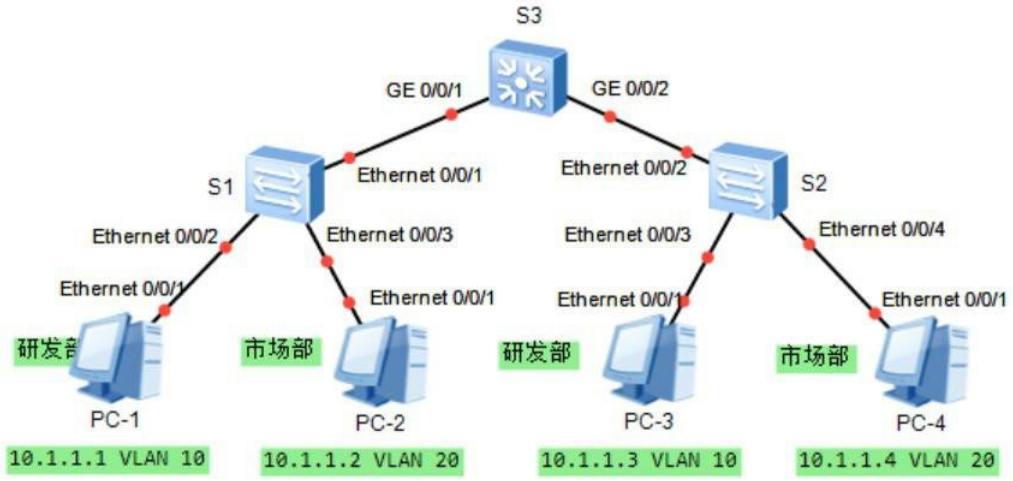
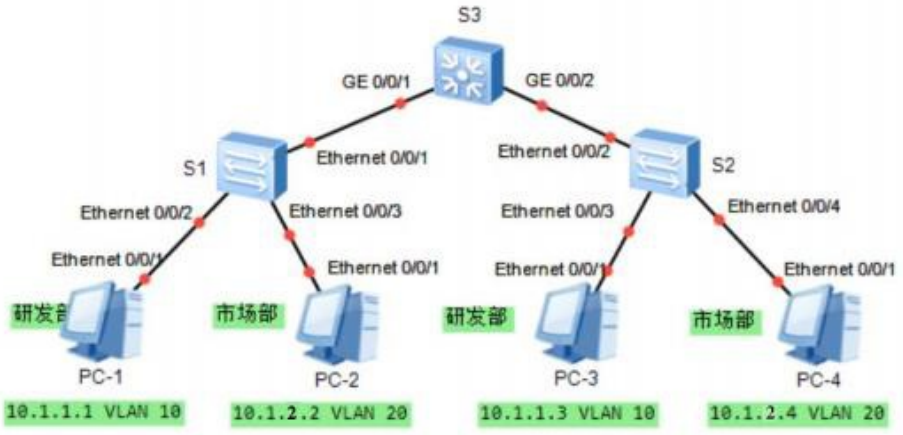


图 3 交换机基础配置拓扑图

5. 实验步骤

1) 根据图3完成网络连接。
2) 根据拓扑图中的IP地址（子网掩码：255.255.255.0）对PC进行网络配置，并使用ping命令检测并记录PC间的连通性。在没有完成划分VLAN之前各PC之间



都能互通（属于默认VLAN1）。如果此时网络不能连通，请检查PC上的防火墙、电脑管家等软件是否关闭；检查交换机上的端口是否属于VLAN1。

3) 公司内网需要通过VLAN的划分来隔离不同的部门，需要在3台交换机S1、S2、S3上分别创建VLAN10和VLAN20。配置完成后，可使用display vlan命令查看所

配置的VLAN信息，也可以使用display vlan summary命令查看所配置的VLAN简

要信息。

4) 研发部员工属于VLAN10，市场部员工属于VLAN20，在交换机上配置Access接口并划分到相应的VLAN，配置Trunk端口并允许所有VLAN通过。配置完成后，使用display port vlan命令检查VLAN和接口配置情况。请根据实际设备配置端口号。使用ping命令检测并记录PC间的连通性。

5) 在S1上配置VLANIF接口实现三层路由通信。在S1上创建对应VLAN10的VLANIF接口，配置IP地址为10.1.1.254/24。再创建对应VLAN20的VLANIF接口，配置IP地址为10.1.2.254/24。修改4台PC的相关网络配置。使用ping命令检测并记录PC间的连通性。

6. 实验评测

各部门之间能够正常通信。

7. 思考题

1) 步骤 2、4、5 中的网络连通性有何变化，造成这些变化的原因是什么？
2) 连接 PC 的交换机接口也可以配置成 Trunk 接口吗？为什么？
3) 如果使用 Hybrid 接口模式，应该如何配置？

实验 3 交换机生成树协议（STP）配置

1. 实验目的

理解 STP 的应用场景；
掌握 STP 的配置方法；
了解 STP 相关参数。

2. 实验设备

- 台式机
- 交换机
- 网线
- 配置线

3. 实验原理

为了提高网络通信的可靠性，有时需要在交换机之间连接多条物理链路（直接的或间接的），这将导致网络中存在环路，从而引起广播风暴。为了解决该问题，IEEE提出了生成树协议标准 IEEE802.1d（简称 STP）、快速生成树协议标准 IEEE802.1w（简称 RSTP）和多生成树协议标准 IEEE802.1s（简称 MSTP）。

STP 是用来避免数据链路层出现逻辑环路的协议，使用 BPDU 传递网络信息计算出一根无环的树状网络结构，并阻塞特定端口。在网络出现故障的时候，STP 能快速发现链路故障，并尽快找出另外一条路径进行数据传输。

交换机上运行的 STP 通过 BPDU 信息的交互，选举根交换机，然后每台非根交换机选择用来与根交换机通信的根端口，之后每个网段选择用来转发数据至根交换机的指定端口，最后剩余端口则被阻塞。

在 STP 工作过程中，通过根交换机的选举，根端口、指定端口的选举生成树，消除环路。可以通过各种命令来调整 STP 的参数，用以优化网络。例如，交换机优先级、端口优先级、端口代价值等。

STP 的收敛时间较长，即当主链路断开后需要经过较长的时间（分钟级）才能切换到备用链路上。RSTP 在 STP 的基础上增加了替换端口和备份端口角色，分别用做“根端口”和“指定端口”，当链路发生故障时，可在小于 1 秒的时间内直接切换到替换端口或备份端口上。

表 1 STP 配置部分命令说明

操 作	命 令	备注
开启/关闭设备RSTP	stp { enable | disable }	系统视图
配置交换机工作STP模式	stp mode { stp | rstp }	系统视图
配置交换机的BPDU 保护功能	stp bpdu-protection	系统视图
配置特定交换机的Bridge 优先级	stp priority *bridge-priority*	系统视图
指定交换机为生成树的根交换机	stp root primary	系统视图
指定交换机为生成树的备份根交换机	stp root secondary	系统视图
配置特定交换机的Forward Delay 时间	stp timer forward-delay *centiseconds*	系统视图
配置特定交换机的Hello Time 时间	stp timer hello *centiseconds*	系统视图
配置特定交换机的Max Age 时间	stp timer max-age *centiseconds*	系统视图
配置特定交换机的超时时间因子	stp timeout-factor *number*	系统视图
配置特定端口的Path Cost	stp cost *cost*	系统视图
在指定端口上开启RSTP	stp enable	系统视图
在指定端口上关闭RSTP	stp disable	系统视图
配置特定端口为边缘端口/非边缘端口	stp edged-port { enable | disable }	系统视图
配置交换机的环路保护功能	stp loop-protection	系统视图
配置特定端口的mCheck 变量	stp mcheck { primary | secondary	端口视图
配置特定端口是否与点对点链路相连	stp point-to-point { auto | force-false |force-true }	端口视图
配置特定端口的优先级	stp port priority *port-priority*	端口视图
配置交换机的Root 保护功能	stp root-protection	端口视图
配置特定端口的最大发送速率	stp transmit-limit *packetnum*	端口视图
显示本设备及当前端口的配置信息	display stp [interface *interface-list*]	显示和调式
打开或关闭 RSTP 的调试开关（收发报文、事件、错误等）	[undo] debugging stp { error | event | packet | all }	显示和调式
使能调试信息在终端输出	terminal debugging	显示和调式

4. 实验内容

某公司购置了 4 台交换机，组建网络。考虑到网络的可靠性，将 4 台交换机如图 2-1 所示拓扑搭建。由于默认情况下，交换机之间运行 STP 后，根交换机、根端口、指定端口的选择将基于交换机的 MAC 地址的大小，因此带来了不确定性，极可能由此产生隐患。公司网络规划，需要 S1 作为主根交换机，S2 作为 S1 的备份根交换机。同时对于 S4 交换机，E0/0/1 接口应该作为根端口。对于 S2 和 S3 之间的链路，应该保证 S2 的 E0/0/3 接口作为指定端口。同时在交换机 S3 上，存在两个接口 E0/0/10、E0/0/11 连接到测试 PC，测试 PC 经常上下线网络，需要将交换机 S3 与之相连的对应端口定义为边缘端口，避免测试电脑上下线对网络产生的影响。

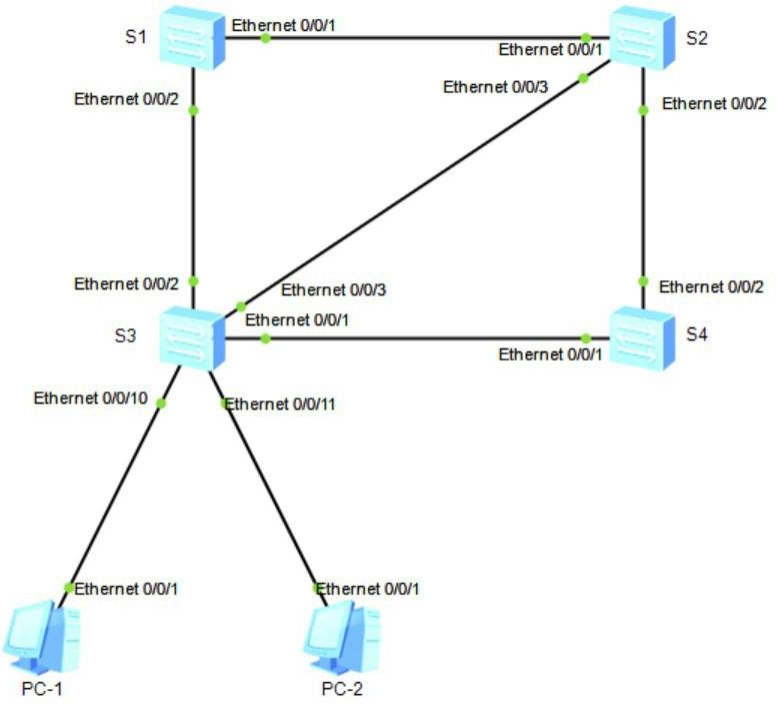


图 3 生成树协议拓扑图

5. 实验步骤

6) 根据图2-1完成网络连接。
7) 在交换机上启用并配置STP，配置完成后，默认情况下需要等待30s生成树重新计算的时间（15s Forward Delay加上15sLearning状态时间），再使用display stp命令查看S1的生成树状态。
8) 使用display stp brief命令查看S1、S2、S3、S4上生成树协议摘要信息，并截图完成思考题1-4。
9) 将 S1 配置为主根交换机，S2 为备份根交换机。将 S3 的 E0/0/10 和 E0/0/11 配置为边缘端口。配置完成后使用命令 display stp 查看 S1 和 S2 的状态信息。完成思考题 5。

6. 实验评测

断开 S2 和S3，S2 和S4 之间的链路，使用命令 display stp brief 查看四台交换机的状态信息。

7. 思考题

4) 哪台交换机是根桥？

5) 配置了生成树协议的交换机有几种端口状态，作用是什么？
6) 哪些端口处于转发状态，哪些端口处于丢弃状态？
7) 哪些端口角色为根端口（ROOT）？哪些端口角色为指定端口（DESI）？哪些端口角色为预备端口（ALTE）？
8) 画出生成树的逻辑拓扑，被阻塞的线路不要描述。

实验 4 路由重发布

1. 实验目的

- 理解路由重发布的应用场景
- 理解默认路由的应用场景
- 掌握RIP发布默认路由的配置
- 掌握OSPF发布默认路由的配置
- 了解路由引入时修改开销值的方法

2. 实验设备

- 台式机
- 路由器
- 网线
- 配置线

3. 实验原理

在大型的企业中，可能在同一网内使用到多种路由协议，为了实现多种路由协议的协同工作，路由器可以使用路由重分发（route redistribution）将其学习到的一种路由协议的路由通过另一种路由协议广播出去，这样网络的所有部分都可以连通了。 为了实现重分发，路由器必须同时运行多种路由协议，这样，每种路由协议才可以取路由表中的所有或部分其他协议的路由来进行广播。

不同的网络会根据自身的实际情况来选用路由协议。比如有些网络规模很小，为了管理简单，部署了RIP；而有些网络很复杂，可以部署OSPF。不同路由协议之间不能直接共享各自的路由信息，需要依靠配置路由重发布来实现。

不同的路由协议计算路由开销的依据是不同的，开销值的大小和范围都是不同的。OSPF的开销值基于带宽，而且值的范围很大，RIP的开销基于跳数，范围很小，所以当配置OSPF和RIP相互引入时一定要小心（在华为设备上，当引入OSPF路由至RIP时，如不指定Cost值，开销值将默认设为1。尽管如此，网络管理员还是应该手工配置开销值以反映网络的真实情况）。

默认路由是指目的地址和掩码都是0的路由条目。当路由器无精确匹配的路由时，就可以通过默认路由进行报文转发。

合理使用默认路由，可以在很大程度上减小本地路由表的大小，节约设备资源。默认路由可以在路由器上手工配置，也可以由路由协议自动发布。RIP和OSPF这两种路由协议都可以通过配置使路由器对协议邻居发布默认路由，并且可以设置该路由的度量值。

4. 实验内容

如下图所示，路由器R1分别连接两家公司网络，R1左侧公司A内部网络运行RIP协议，公司B内部网络运行OSPF协议。由于业务发展需要，两家公司人员需要能够互相通信，但是为了保护自身网络的私密性，双方都不愿意对方知道自己网络的明细路由。

通过配置路由协议以自动发布默认路由的方式来完成此需求。

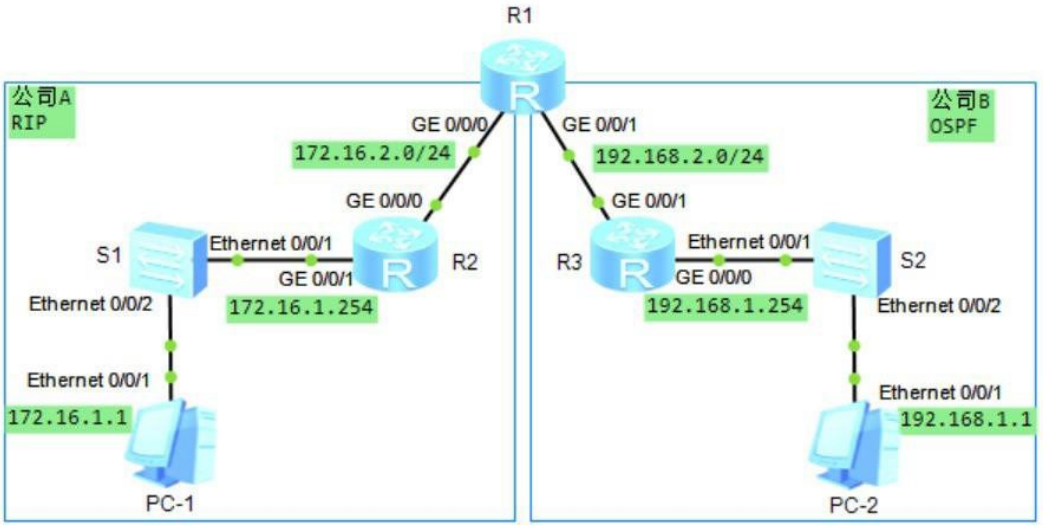


图 6 路由重发布拓扑图

5. 实验步骤

1) 规划并设计各设备IP地址并完成下表：

表3 IP地址表

设备名	接口	IP地址	子网掩码	网关
PC-1	N/A			
PC-2	N/A			
R1				N/A
				N/A

R2				N/A

				N/A
R3				N/A
				N/A

2) 据图3-2完成网络连接并配置主机IP。
3) 根据实验拓扑图配置路由协议，公司A内部运行RIP协议。在R1和R2上配置RIP，进程号为1，启用RIPv2版本、关闭自动汇总，通告各自接口所在网段，R1在RIP中仅通告GE0/0/0接口所在网段。公司B内部运行OSPF协议。在R1和R3上配置OSPF，使用进程号1，所有网段都属于区域0，R1在OSPF中仅通告GE0/0/1接口所在网段。查看R1、R2、R3上的路由表。回答思考题1。
4) 在R1的RIP进程中，使用default-route originate命令发布默认路由。配置完成后查看R2的路由表。在R1的OSPF进程中，使用default-route-advertise always命令发布默认路由。配置完成后查看R3的路由表。

6. 实验评测

PC-1 和 PC-2 之间能否正常通信。

7. 思考题

1) 根据步骤 3 中各台路由器上的路由表， 分析 PC-1 和 PC-2 能否正常通信？
2) 根据步骤 4 中各台路由器上的路由表， 分析 PC-1 和 PC-2 能否正常通信？
3) 在本实验的步骤 4 中， OSPF 发布默认路由时使用到了 default-route advertise always 命令，如果末尾不加 always 参数，会出现什么情况？如何解决？

实验 5 BFD应用与配置

1. 实验目的

- 能阐述BFD的工作原理
- 能根据需求设置有效的BFD

2. 实验设备

- 台式机
- 路由器
- 网线
- 配置线

3. 实验原理

我们知道网络中路由起着重要的作用，如果网络中链路不通时，如果路由表无法快速调整，那么网络将无法传输数据，造成极大的危害和损失。而我们前面所学的路由如静态路由，OSPF路由都存在这样的问题。因为静态路由没有检测机制，需要网络管理员人工检测；OSPF检测机制太慢，甚至达到30-40秒，才能发现链路故障后对路由表进行调整。以上两种情况在实际的工程中是无法忍受的。为此，我们引入BFD（Bidirectional Forwarding Detection，双向转发检测），BFD是一种基于RFC 5880标准的高速故障检测机制，两个系统建立BFD会话后，在它们之间的通道上周期性地发送BFD报文，如果一方在协商的检测时间内没有接收到BFD报文，则认为这条双向通道上发生了故障。上层协议通过BFD感知到链路故障后可以及时采取措施，进行故障恢复。BFD用于毫秒级的快速检测、监控网络中链路或者IP路由的转发连通状况。BFD提供了一个通用的、标准化的、介质无关、协议无关的快速故障检测机制。

为体会BFD的工作原理，掌握BFD的典型配置，我们在静态路由和OSPF两种路由协议的基础上进行BFD配置实验。注意以下几点

- 保证路由配置正确，链路可达；
- 在没有配置BFD的情况下观察链路断开后对路由表的影响，分别在PC上用tracert命令跟踪路由和在路由器上用display ip routing-table 命令刷新展示路由信息，这里需要两个同学配合；
- 配置BFD后观察链路断开后对路由表的影响，分别在PC上用tracert命令跟踪路由和在路由器上用display ip routing-table 命令刷新展示路由信息，这里需要两个同学配合；

4. 实验内容

A）静态路由与 BFD 联动实验

1. 为重点关注 BFD 配置，本实验在 eNSP 上进行；
2. 需配置两条路由，可以减少经过 LSW1 的条路由优先级，构成浮动路由；
3. 拓扑图参考图 7，没有配置 BFD 联动时，分别关闭 LSW1 的 GE0/0/0 接口和 AR3 的 GE0/0/1 接口，分别记录 AR1 和 AR2 上路由表变化情况，记录并分析解释产生这种现象的原因。

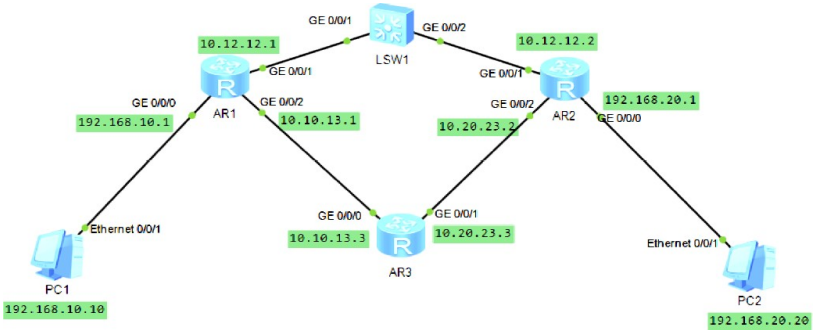


图7 静态路由拓扑图

4. 根据实际路由设置，配置合理的 BFD 联动，关闭 LSW1 的 GE0/0/0 接口，观察 AR1 上路由表变化情况，记录并分析解释产生这种现象的原因。

B）OSPF 路由与 BFD 联动实验

1. 本实验在真实设备上实验；
2. 拓扑图参考图 8，OSPF 可以配置为单域或多域形式；
3. 断开 LSW1 和 LSW2 的链路，在配置 BFD 联动前和配置 BFD 联动后分别观察 AR1 上的路由表变化。

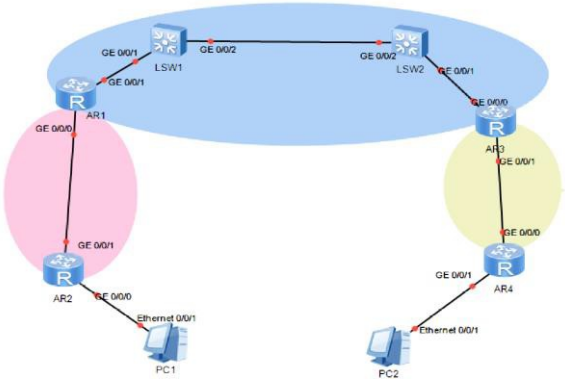


图8 OSPF路由拓扑图

5. 实验步骤

1、实验方案设计

a） IP 地址列表

b） 拓扑图

2、实验结果图表

a） 配置路由后的连通性截屏示意图、各个路由器路由表截屏示意图

b） 断开链路的相关接口列表

c） 断开链路后连通性截屏示意图、各个路由器路由表截屏示意图

d) 配置 BFD 联动的截屏示意图

e) 断开链路后连通性截屏示意图、各个路由器路由表截屏示意图

3、BFD 与静态路由、OSPF 联动实验结果分析

4、提交思考题答案

8. 实验评测

PC1 和 PC2 之间能否在链路断开后快速自动恢复正常通信。

9. 思考题

a) 创建BFD会话中本地标识符和远端标识符可以一样吗？

b) BFD与浮动路由联动前，图1中的PC1和PC2不能通信，是因为浮动路由机制不起作用了吗？如果不是，请说明原因。

c) 图7中AR1和AR2配置了BFD后，当链路恢复连通后，路由器会立刻启用优先级小的路由吗？分析下原因。

d) BFD配置成单臂回声模式时，是单跳还是多跳？请问如何配置？

实验 6 VRRP 配置

1. 实验目的

理解 VRRP 的应用场景；
掌握 VRRP 虚拟路由器的配置。

2. 实验设备

- 台式机
- 交换机
- 路由器
- 网线
- 配置线

3. 实验原理

随着 Internet 的发展，人们对网络可靠性的要求越来越高。对于用户来说，能够时刻与外部网络保持通信非常重要，但内部网络中的所有主机通常只能设置一个网关 1P 地址，通过该出口网关实现主机与外部网络的通信。若此时出口网关设备发生故障，主机与外部网络的通信就会中断，所以配置多个出口网关是提高网络可靠性的常用方法。为此，IETF 组织推出了 VRRP 协议，主机在多个出口网关的情况下，仅需配置一个虚拟网关 IP 地址作为出口网关即可，解决了局域网主机访问外部网络的可靠性问题。

VRRP (Virtual Router Redundancy Protocol)全称是虚拟路由器冗余协议，它是一种容错协议。该协议通过把几台路由设备联合组成一台虚拟的路由设备，该虚拟路由器在本地局域网拥有唯一的一个虚拟 1D 和虚拟 IP 地址。实际上，该虚拟路由器是由一个 Master 设备和若干 Backup 设备组成。正常情况下.业务全部由 Master 承担，所有用户端仅需设置此虚拟 IP 为网关地址。当 Master 出现故障时，Backup 接替工作，及时将业务切换到备份路由器，从而保持通信的连续性和可靠性。而用户端无需做任何配置更改,对故障无感知。

VRRP 的 Master 选举基于优先级，优先级取值范围是 0~255，默认情况下，配置优先级为 100。在接口上可以通过配置优先级的大小来手工选择 Master 设备。

4. 实验任务

本实验模拟企业网络场景。公司内员工所用电脑，如 PC-1、PC-2,通过交换机

LSW1 连接到公司网络，LSW1 连接到公司出口网关路由器。为了提高网络的可靠性，公司使用两台路由器 R2 与 R3 作为双出口连接到外网路由器 RI。RI、R2、R3 之间运行 OSPF 协议。在双网关的情况下，如果在 PC 上配置 R2 或 R3 的真实 IP 地址作为网关，当其中一台路由器故障时，就需要手动更改 PC 的网关 IP,若网络中有大量 PC 则需要耗费大量时间和人力去更改配置，且会带来一定时间的断网影响。为了能够使故障所造成的断网影响达到最小化，增强网络的可靠性，网络管理员在 R2 与 R3 之间部署 VRRP 协议，这样当任一网关发生故障时就能自动切换而无需更改 PC 的网关 IP 地址。

VRRP 基本配置的拓扑如下图所示：

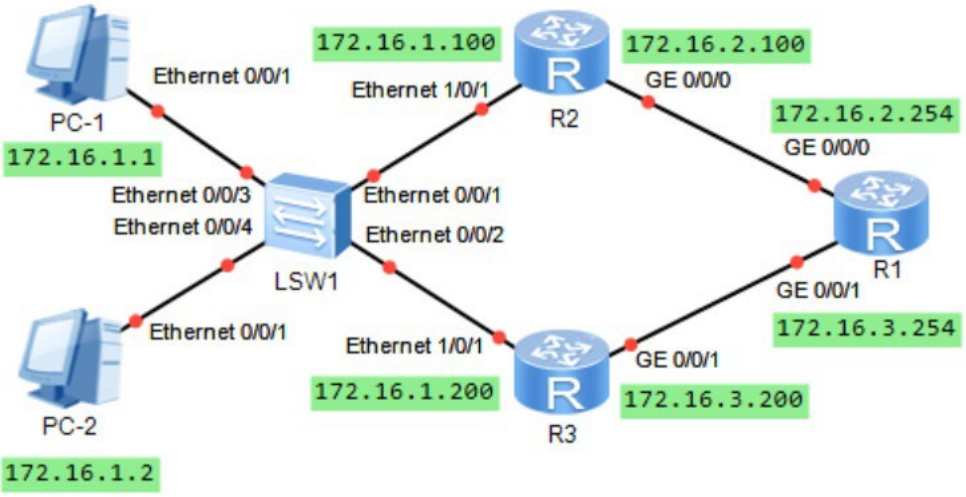


图 VRRP 基本配置拓扑

5. 实验步骤

1) 规划并设计各设备IP地址并完成下表：

表2 IP地址表

设备名	接口	IP地址	子网掩码	网关
PC-1	N/A			
PC-2	N/A			
R1				N/A
				N/A
				N/A
R2				N/A
				N/A
R3				N/A
				N/A

2) 据图3-1完成网络连接并配置IP地址，使用ping命令检查各直连链路的连通性。
3) 部署OSPF网络。在公司的出口网关路由器R2、R3和外网路由器R1上配置OSPF 协议，使用进程号1，且所有网段均通告进区域0中。配置完成后，使用disp ospf peer brief在R1上检查OSPF的邻居建立情况。
4) 现网络管理员想针对两台出口网关路由器实现备份，既正常情况下，只有主网关工作，当发生故障时自动切换到备份网关。通过配置VRRP协议可以实现此需求。在R2和R3上配置VRRP协议，使用vrrp vrid 1 virtual-ip命令创建VRRP备份组，指定R1和R2处于同一个VRRP备份组内，VRRP备份组号为1，配置虚拟IP 为172.16.1.254。注意虚拟IP地址必须和当前接口在同一网段。经过配置后，PC 将使用虚拟路由器IP作为默认网关。
5) 在VRRP协议中，优先级决定路由器在备份组中的角色，优先级高者成为Master。如果优先级相同，则比较IP地址。系统默认优先级为100。请配置R2、R2的VRRP 优先级，使R2为主网关，R3为备份网关。配置完成后，使用disp vrrp或者disp vrrp brief或者disp vrrp interface命令来查看并分析信息。

6. 实验评测

在 PC 上使用 tracert 命令测试访问公网时数据包的转发路径。

在PC 上使用ping XX -t 命令持续测试公网连通性，同时手动模拟网络出现故障， 比如将 LSW1 的接口关闭，观察 ping 数据包的变化，经过 3S 左右，使用 disp VRRP 查看 R3 的信息，分析变化。

再次在 PC 上使用 tracert 命令测试访问公网时数据包的转发路径。手动恢复故障，查看 R2、R3 上的 VRRP 工作状态。

7. 思考题

1、记录并分析不同情况下主备网关的变化？
2、如果主路由器发生故障，备份路由器通过什么机制检测？
3、交换机上是否也可以配置 VRRP？