

**计算机网络实验报告**

|  |  |
| --- | --- |
| **班级：** | 计试2201 |
| **学号：** | X |
| **姓名：** | XXX |
| **组号：** | G6 |

二〇二四年十月

目 录

[实验一 组网与接入认证 1](#_Toc146280482)

[实验二 VLAN的配置与协议分析 3](#_Toc146280483)

[实验三 ARP协议分析 5](#_Toc146280484)

[实验四 TCP协议分析 7](#_Toc146280485)

[实验五 应用层协议分析 9](#_Toc146280486)

[实验六 RIP协议分析 12](#_Toc146280487)

[实验七 OSPF路由协议分析 15](#_Toc146280488)

[实验八 防火墙与SSLVPN 17](#_Toc146280489)

[选做实验 19](#_Toc146280490)

实验一 组网与接入认证

实验名称：组网与接入认证 时间： 2024 年 10 月 30 日

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **班 级** | 计试2201 | | **学号** | X | | **姓 名** | X | |
| 组别 | G6 | | | | | **联系电话** | X | |
| 实验组网图  （设备编号、端口号、IP地址、  认证角色等） |  | | | | | | | |
| 组 网  实 验  结 果 | 1.网络连通测试结果：   |  |  |  |  | | --- | --- | --- | --- | |  |  | 所用命令 | 能否ping通 | | 同一网段中 | PC1 ping PC3 | ping 10.5.2.13 | 能 | | PC2 ping PC4 | ping 10.5.2.14 | 能 | | 不同网段中 | PC1 ping PC2 | ping 10.5.2.12 | 能 | | PC3 ping PC4 | ping 10.5.2.14 | 能 |   2.用show ip route查看R1的路由表，分析不同网段互通的原因？    因为两个不同网段通过路由器进行了直接连接。网关的作用是实现局域网的互联。 | | | | | | | |
| 认 证  实 验  结 果 | 3.按指导书完成接入认证，回答问题：  （1）认证终端为PC1，认证用户为 3 ，身份验证方法为 MD5-Challenge 。  （2）在交换机上启动802.1x认证后，认证终端没有回答认证质询前，认证终端PC与相同网段PC互通的测试命令及结果是：  不能ping通    （3）在交换机上启动802.1x认证后，认证终端完成认证质询后，认证终端PC与不同网段PC互通的测试命令及结果是：    能ping通    4.分析交换机及认证服务器在接入认证过程中的主要工作及步骤。  交换机的主要工作及步骤  初始状态：  交换机端口处于未授权状态，不允许任何流量通过，除了EAPOL（Extensible Authentication Protocol over LAN）帧。  检测设备连接：  交换机检测到终端设备（Supplicant）连接到端口，发送EAP-Request/Identity报文，要求终端设备发送身份信息。  接收身份信息：  终端设备回应EAP-Response/Identity报文，包含设备的身份信息（如用户名）。  转发身份信息：  交换机接收到EAP-Response/Identity报文后，将其封装成RADIUS Access-Request报文，转发给认证服务器。  处理认证服务器响应：  认证服务器根据身份信息验证用户，返回RADIUS Access-Accept或Access-Reject报文。  如果认证成功（Access-Accept），交换机端口切换到授权状态，允许正常网络流量通过。  如果认证失败（Access-Reject），交换机保持端口在未授权状态。  认证服务器（Authentication Server）的主要工作及步骤  接收认证请求：  认证服务器接收到交换机发送的RADIUS Access-Request报文，包含终端设备的身份信息。  验证身份信息：  认证服务器根据身份信息查询数据库，验证用户的身份和凭证（如用户名和密码）。  发送认证结果：  认证成功：认证服务器发送RADIUS Access-Accept报文给交换机，并可能包含授权属性（如VLAN ID、访问控制列表等）。  认证失败：认证服务器发送RADIUS Access-Reject报文给交换机，通知认证失败的原因。 | | | | | | | |
| 本人机位（图中标识） | | 2 | | | 同组人（只填一人） | | | X |
| 本人主要工作 | | 第一部分连线，ping测试，第二部分的服务器构建，为系统添加账户，配置交换机等。 | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |

实验二 VLAN的配置与协议分析

实验名称：VLAN的配置与协议分析 时间： 年 月 日 早□ 午□ 晚□

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **班 级** | **计试2201** | | **学号** | X | | **姓 名** | X | |
| 组别 | G6 | | | | | **联系电话** | X | |
| 实验组网图 | 【拓扑图中，请标明设备编号、端口号、vlan号、IP地址、掩码等】 | | | | | | | |
| 实 验  结 果 | 1．VLAN配置完成后，验证同一VLAN的两台计算机能否通信，不同VLAN之间的计算机能否通信，记录结果并解释原因（步骤3）。  同一vlan能通，不同vlan不通  原因是交换机为每个数据包都标记了VLAN号标签，当有数据包传到交换机处时，交换机只会将有相同 VLAN 号的报文转发到对应的主机，从而隔离了不同 VLAN。  2．步骤6（完成Trunk端口配置）完成后，测试同一VLAN和不同VLAN中计算机的互通情况，记录测试结果并解释原因。  同一vlan能通，不同vlan不通  因为我们为两个交换机的 E0/0/1 端口都配置成了 Trunk 模式，在该模式下端口可以属于多个VLAN，也可以接收和发送多个不同 VLAN 的报文。进入 Trunk 端口的数据帧，对于已经携带 tag域的数据，端口直接进行转发，而对于普通数据帧，端口用自己的缺省 VLAN ID 进行封装后再转发。这样就使得两个交换机能够传输属于不同 VLAN 的数据包，使得 PC1 和 PC3 虽然不在同一交换机下，但由于二者在同一 VLAN 中，他们依然可以相互通信。  3. 填写步骤7中的表格并解释原因（设置镜像端口后）。  表2-1 跨交换机VLAN实验（PC1 ping PC2）   |  |  |  | | --- | --- | --- | | 转发过程 | 802.1Q VLAN ID | 标记出现与否的原因分析 | | PC1 - S1 | Request报文：无 | 报文还未经过 S2 封装 802.1q 协议 | | Reply报文：无 | 监控主机新网卡过滤掉了 802.1q 协议 | | S1 - S2 | Request报文：2 | 报文经过 S2 封装后标记上了 VLAN 号  为 2 | | Reply报文：无 | 监控主机新网卡过滤掉了 802.1q 协议 | | S2 – PC2 | Request报文：无 | 监控主机新网卡过滤掉了 802.1q 协议 | | Reply报文：无 | 监控主机新网卡过滤掉了 802.1q 协议 |   当PC1通过交换机S1发送请求报文时，该报文最初不包含VLAN ID。在S1发送至S2的过程中，由于这个数据帧最初没有802.1Q VLAN标签，所以当它经过trunk端口时，会被自动打上该端口的默认VLAN ID，即PVID（Primary VLAN ID），这里是VLAN 2。接着，当S2通过其trunk端口接收到这个请求报文时，若发现报文的VLAN ID与端口的PVID匹配，它便会去除VLAN标签，并将报文转发给PC2。回复报文（reply）从PC2发回时，会遵循类似的路径和VLAN标记过程。  4. 完成实验步骤10后，填写表格，解释不同Vlan 间可以通信的原因？  表2-2 跨VLAN通信（PC2 ping PC4）   |  |  |  | | --- | --- | --- | | 转发过程 | 802.1Q VLAN ID | 标记出现与否的原因分析 | | PC2 -- S2 | Request报文：无 | 报文还未经过 S2 封装 802.1q 协议 | | Reply报文：无 | 监控主机新网卡过滤掉了 802.1q 协议 | | S1 -- S2 | Request报文：3 | 报文经过 S2 封装后标记上了 VLAN 号  为 3 | | Reply报文：无 | 监控主机新网卡过滤掉了 802.1q 协议 | | S2 -- PC4 | Request报文：无 | 监控主机新网卡过滤掉了 802.1q 协议 | | Reply报文：无 | 监控主机新网卡过滤掉了 802.1q 协议 |   trunk 类型的端口可以允许多个 VLAN 通过，比较将要发送报文的 VLAN 信息和端口的 PVID，如果不相等则直接发送。如果两者相等则剥离 VLAN 信息，再发送。 实验中没有设置 PVID 缺省值为 VLAN1。  Trunk 端口收到一个报文,判断是否有 VLAN 信息：如果有，则判断该 trunk 端口是否允许该VLAN 的数据进入：如果可以则转发，否则丢弃；在 trunk 端口出方向，比较将要发送报文的 VLAN信息和端口的 PVID，如果不相等则直接发送。如果两者相等则剥离 VLAN 信息，再发送。  在 trunk 端口设置中，将 trunk 端口加入到了 VLAN2 和 VLAN3 中，因此 trunk 端口允许携带VLAN2 和 VLAN3 的数据帧通过。PC3 向 PC4 发起了 ICMP 请求，携带 VLAN 信息为 VLAN3，与 VLAN1 不同所以直接转发，在 S1 处经过路由转发到 PC4；PC4 向 PC3 发起了 ICMP 应答，携带 VLAN 信息为 VLAN2，与 VLAN1 不同直接转发，经过 E0/0/1 截获的报文携带信息 VLAN2，经 S1 路由发送到 PC3。在 PC3 ping PC4 过程中发送四条报文，响应四条报文，都需要经过 E 0/0/1端口，都被 PC2 监听到，因此总共有八条报文。  互动讨论主题   1. 交换设备工作原理、端口类型和端口镜像工作原理；   1. 交换设备的工作原理:  - 交换机利用其内部的MAC地址表来记录连接到它的各个设备的MAC地址与对应的端口。  - 当交换机需要转发数据时，它会根据这个MAC地址表来确定正确的端口，以便将数据包发送到正确的目的地。  2. 端口类型:  - 交换机的端口主要分为两种：接入端口和汇聚（或称为trunk）端口。  - 接入端口通常用于连接单个设备，如计算机或打印机。  - 汇聚端口则用于连接不同交换机之间，允许多个VLAN的数据通过。  3. 端口镜像的工作原理:  - 端口镜像是一种监控技术，它创建特定端口（称为源端口）的数据流的精确复制。  - 这些数据包的副本随后被发送到另一个端口（称为监控端口），使得网络管理员可以分析这些数据流，进行故障诊断或网络监控。   1. Vlan的配置与工作原理。  VLAN配置概括 **创建VLAN**：在交换机中定义唯一的VLAN ID，用于区分网络中的虚拟局域网。  **端口分配**：将交换机端口分配到特定VLAN，连接设备成为该VLAN的一部分。  **配置Trunk端口**：用于在多个交换机间传输多个VLAN的数据，实现跨交换机的VLAN互通。  **Access与Hybrid端口**：  Access端口：允许特定VLAN的数据通过，连接终端设备。  Hybrid端口：支持多个VLAN数据，适用于复杂网络需求。 VLAN工作原理概括 **VLAN标签**：在以太网帧中加入VLAN ID和控制信息（IEEE 802.1Q标准）。  **帧传输**：802.1Q帧通过Trunk端口携带VLAN信息，交换机根据标签转发或丢弃帧。  **隔离与通信**：VLAN逻辑隔离不同网络段，提升安全性和效率，不同VLAN通信需经路由器或三层交换机。 | | | | | | | |
| 本人机位（图中标识） | | 2 | | | 同组人（只填一人） | | | X |
| 本人主要工作 | | 配合操作，VLAN划分与通信，Trunk端口配置，报文捕获分析等。 | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |

实验三 ARP协议分析

实验名称：ARP协议分析与欺骗防范 时间： 年 月 日 早□ 午□ 晚□

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 | 计试2201 | | 学号 | X | | 姓 名 | X | |
| 组别 | G6 | | | | | 联系电话 | X | |
| 使用设备组别  G1 G2  G3 G4  G5 G6  G7 G8  实验组网图  （标明设备编号、端口号、vlan号、IP地址） |  | | | | | | | |
| 实 验  结 果 | 1. 记录步骤4中“arp –a”的结果，写出其含义。     含义：在PCA ping PCB后，PCA的arp表中就有了PCB的地址   1. 观察同一网段的arp包格式，记录结果。  |  |  |  | | --- | --- | --- | | 字段 | 请求报文 | 应答报文 | | 以太网链路层Destination项 | Broadcast(ff:ff:ff:ff:ff:ff) | Sony\_e5:60:ae(f0:bf:97:e5:60:ae) | | 以太网链路层Source项 | Sony\_e5:60:ae(f0:bf:97:e5:60:ae) | Shanghai\_9c:2e:57(00:e0:0f:9c:2e:57) | | ARP报文发送者硬件地址 | Sony\_e5:60:ae(f0:bf:97:e5:60:ae) | Shanghai\_9c:2e:57(00:e0:0f:9c:2e:57) | | ARP报文发送者IP | 10.5.2.11 | 10.5.2.1 | | ARP报文目标硬件地址 | 00:00:00\_00:00:00 | Sony\_e5:60:ae(f0:bf:97:e5:60:ae) | | ARP报文目标IP | 10.5.2.1 | 10.5.2.11 |  1. 完成步骤7后，分析不同网段的ARP请求和响应报文，填写下表。  |  |  |  | | --- | --- | --- | | 字段 | 请求报文 | 应答报文 | | 以太网链路层Destination项 | Broadcast(ff:ff:ff:ff:ff:ff) | Sony\_e5:60:ae(f0:bf:97:e5:60:ae) | | 以太网链路层Source项 | Sony\_e5:60:ae(f0:bf:97:e5:60:ae) | Cisco\_26:a8:41(f4:7f:35:26:a8:41) | | ARP报文发送者硬件地址 | Sony\_e5:60:ae(f0:bf:97:e5:60:ae) | Cisco\_26:a8:41(f4:7f:35:26:a8:41) | | ARP报文发送者IP | 10.5.2.11 | 10.5.2.1 | | ARP报文目标硬件地址 | 00:00:00\_00:00:00 | Sony\_e5:60:ae(f0:bf:97:e5:60:ae) | | ARP报文目标IP | 10.5.2.11 | 10.5.2.11 |  1. 完成步骤4后，测试结果及原因是：   (1)不通，因为ip地址变化了  (2)通，因为fa0/1没有启用访问控制列表  (3)不通，因为mac地址变了  (4)不通，因为mac和ip都变了 | | | | | | | |
| 本人机位（图中标识） | | 2 | | | 同组人（只填一人） | | | X |
| 本人主要工作 | | 协助进行设备连接，交换机配置，arp报文捕获分析。 | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 收教师签名 | |  | | | 本实验成绩 | | |  |

实验四 TCP协议分析

实验名称：TCP协议分析 时间： 年 月 日 早□ 午□ 晚□

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 | 计试2201 | | 学号 | X | | 姓 名 | X | |
| 组别 | G6 | | | | | 联系电话 | X | |
| 实验组网图 |  | | | | | | | |
| 实 验  结 果 | 1. 分析截获的报文，记录TCP连接建立过程的三个报文和连接撤销过程的四个报文。   （1）TCP连接建立报文信息：  报文捕获计算机：   |  |  |  |  | | --- | --- | --- | --- | | 字段名称 | 第1条报文值及含义 | 第二条报文值及含义 | 第三条报文值及含义 | | 报文发出计算机 | 10.5.2.11 | 10.5.3.13 | 10.5.2.11 | | 捕获的报文序号 | 3 | 4 | 5 | | Sequence Number | 0 | 0 | 1 | | Acknowledgement Number | 0 | 1 | 1 | | ACK标志 | Not Set | Set | Set | | SYN标志 | Set | Set | Not Set |   （2）TCP连接撤销报文信息：  报文捕获计算机：   |  |  |  |  |  | | --- | --- | --- | --- | --- | | 字段名称 | 第一条报文值及含义 | 第二条报文值及含义 | 第三条报文值及含义 | 第四条报文值及含义 | | 报文发出计算机 | 10.5.2.11 | 10.5.3.13 | 10.5.2.11 | (无，只有三条) | | 捕获的报文序号 | 112 | 115 | 116 |  | | Sequence Number | 1 | 1 | 2 |  | | Acknowledgement Number | 1 | 2 | 2 |  | | ACK标志 | Set | Set | Set |  | | FIN标志 | Set | Set | Not Set |  |  1. 记录TCP数据传送阶段的前12个报文。  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | 报文序号 | 报文种类 (数据/确认) | 序号字段Seq Number | 确认号Ack Number | 数据长度 | 确认到哪条报文（填序号） | 窗口大小 | | 9 | PSH | 1 | 1 | 2000 | / | 65536 | | 10 | ACK | 1 | 2001 | 0 | 9 | 65536 | | 11 | PSH | 2001 | 1 | 2000 | / | 65536 | | 12 | ACK | 1 | 4001 | 0 | 11 | 65536 | | 13 | PSH | 4001 | 1 | 2000 | / | 65536 | | 14 | ACK | 1 | 6001 | 0 | 13 | 65536 | | 15 | PSH | 6001 | 1 | 2000 | / | 65536 | | 16 | ACK | 1 | 8001 | 0 | 15 | 65536 | | 17 | PSH | 8001 | 1 | 2000 | / | 65536 | | 18 | ACK | 1 | 10001 | 0 | 17 | 65536 | | 19 | PSH | 10001 | 1 | 2000 | / | 65536 | | 20 | ACK | 1 | 12001 | 0 | 19 | 65536 |  1. 如何确定那条捕获的报文已被确认？窗口值大小何时、何因由谁调整？   当收到ack报文，确认序号是上次已成功收到数据字节序号加 1时，上条报文已被确认  接收方用接收窗口大小控制发送方的发送窗口大小，再由发送窗口大小控制发送速率 | | | | | | | |
| 本人机位（图中标识） | | 2 | | | 同组人（只填一人） | | | X |
| 本人主要工作 | | 分析TCP报文协议 | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |

实验五 应用层协议分析

实验名称： 应用层协议分析 时间： 年 月 日 早□ 午□ 晚

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 | 计试2201 | | 学号 | X | | 姓 名 | X | |
| 组别 | G6 | | | | | 联系电话 | X | |
| 使用设备组别  G1 G2  G3 G4  G5 G6  G7 G8  实验组网图  （标明设备编号、端口号、vlan号、IP地址） |  | | | | | | | |
| 应用层协议分析 | 1. HTTP协议分析   （1）清空缓存后的ARP，DNS和HTTP协议分析  步骤1：在计算机终端上运行Wireshark截获所有的报文。  步骤2：清空ARP，DNS和HTTP浏览器的缓存：  浏览器缓存的清除以Chrome浏览器为例，地址栏中输入chrome://settings/，找到高级选项中的“隐私设置和安全性”，清除浏览数据。  执行“ipconfig /flushdns”清除本地DNS缓存。  执行“arp –d”命令清空arp缓存。  步骤3：在浏览器中分别访问几个网址，注意区分http和https（目前很多网站默认都是https，访问时需指定是 http 还是 https），如http://www.people.com.cn/， https://www.baidu.com， https://www.unb.br/。  步骤4：执行完之后，Wireshark停止报文截获，分析截获的报文。  观察分析几个协议的配合使用（ARP，DNS，HTTP等）；  注意访问的延迟情况，记录每个网址建立链接（三次握手）花费的时间；  特别分析HTTP的请求和应答报文格式，统计在一次网址的访问中，建立了几个连接，下载了几个对象（HTML，CSS，JS，图片等），有几次DNS解析，有没有Cookie等。  HTTPS的加密内容不好分析，可观察分析TLS加密传输的建立过程，传输端口等。  使用了50234-50236 共3个连接，取了接近两百个对象，有七十次左右DNS解析，无cookie  （2）带缓存的ARP，DNS和HTTP协议分析  照着1.7.1中的步骤1-4再次执行一遍，但不执行步骤2，观察缓存的使用和带来的好处（建立连接、下载对象、DNS解析等的数量）。  结合数据包分析缓存工作原理，分析cookie工作原理。  使用了50234-50236 共3个连接，取了13个对象，无DNS解析，有cookie  缓存工作原理：对于相同域名的请求，系统会优先从DNS缓存中获取IP地址，避免再次进行DNS解析，从而减少解析时间和减轻DNS服务器的负担。  （3）使用ncat工具访问HTTP服务（选做）  参考1.7.1中的步骤1-4和分析结果，在命令窗口执行ncat -C xxx.xxx.xxx.xxx 80，ncat连接上HTTP服务器后，根据协议输入合适的请求。其中xxx.xxx.xxx.xxx 为服务器地址。   1. FTP协议分析   （1）FTP协议的分析  步骤1：在远程的云服务器上开启ftp服务，并在云服务器控制台把21端口开放。在云服务器上运行报文截获工具（如Linux的tcpdump，Windows的Wireshark）截获FTP报文。  步骤2：在计算机终端上运行Wireshark截获报文，使用IE浏览器来访问该FTP服务器。比如在地址栏输入 <ftp://xxx.xxx.xxx.xxx/> 其中xxx.xxx.xxx.xxx 是该云服务器的IP地址。  步骤3：进入FTP服务器中的某个目录中，下载一个文件。结束后，停止报文截获。  分析该FTP的过程。注意对照服务器和客户端的一起分析，注意NAT的影响。观察是否使用了被动模式，如果是主动模式并且工具允许，使用被动模式再做一次下载，并分析。  如果FTP不能正常工作，请仔细抓包并分析原因。NAT穿越问题可能是原因之一。  （2）使用ncat工具来访问FTP服务  步骤1：提前把用到的FTP命令准备好（写在notepad++中）。  步骤2：在云服务器上运行报文截获工具准备截获FTP报文。在命令窗口执行ncat –C xxx.xxx.xxx.xxx 21，ncat连接上FTP服务器后，根据协议输入合适的命令。其中xxx.xxx.xxx.xxx 为云服务器地址。  步骤3：解析完毕后停止报文截获。把过程整理记录到报告中。  在ncat模拟FTP客户端的过程中，请查看服务器的文件列表，并下载一个不大的文本文件。过程中，必要时用netstat命令观察双方的（新开）端口监听情况。   1. 互动讨论主题   （1）HTTP协议的缓存，DNS的缓存；缓存对网络访问速度的影响。  （2）NAT对FTP传输的影响，比较HTTP与FTP的特点；   1. 进阶自设计   （1）用nmap的ncat来模拟https客户端，访问1-2个网站。  （2）在云服务器上搭建Apache2（或其他WEB服务器），并测试修改HTML或图片文件，看客户端能否及时访问到更新的内容。注意抓包分析。 | | | | | | | |
| 本人机位（图中标识） | | 2 | | | 同组人（只填一人） | | | X |
| 本人主要工作 | | 对HTTP协议进行分析 | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |

实验六 RIP协议分析

实验名称：RIP协议分析  时间： 年 月 日 早□ 午□ 晚□

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 | 计试2201 | | 学号 | X | | 姓 名 | X | |
| 组别 | G1 G2 G3 G4 G5 G6 G7 G8？ | | | | | 联系电话 | X | |
| 实验组网图 | 【可以手画拍照。拓扑图中，请标明设备编号、端口号、vlan号、IP地址、掩码等】 | | | | | | | |
| 实 验  结 果 | * 1. 步骤1之后在R1上ping各台PC，看能否ping通，分析路由表并写出原因。   不能  根据拓扑图和目前的网络设置，网络中的每个点都只能有两种路由：与自身直接连接产生的路由和在同一个子网的路由。因此，只能联通直接连接的点或同一子网下的点。  R1和四台PC机都不在同一个子网下，也没有直接连接。因此，R1路由表中只有直接连接S1与S2的路由，没有到PC机的路由。所以通过R1，只能ping通S1或S2，不能ping通四台PC机。   * 1. 步骤2之后在R1上ping各台PC，看能否ping通，分析路由表并写出原因。   能  添加静态路由后，R1通过S1，可以访问vlan7的网络了。因此，R1是可以ping通vlan下的PC1与PC2的；然而，依然不能访问vlan2，所以不能ping通PC3和PC4。       * 1. 步骤4之后。   2. 测试连通性（在R1上ping各台PC，看能否ping通），记录连通性结果，写出原因。   能  开启RIP协议后，R1与S1不断学习路由，直至稳定；而S2没有开启RIP协议，所以S2连通的路由不能分享给R1和S1。所以，R1所能连通的范围是R1、S1连通的范围，不包括S2连通的范围。所以，R1可以ping通PC1和PC2，而无法ping通PC3和PC4。   * 1. 查看路由填写下表。  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | 设备 | Destination/Mask | Protocol | Pref | Cost | Nexthop | Interface | | S1 | 10.5.3.0/24 | 直连 |  |  |  |  | | 10.5.4.0/24 | 直连 |  |  |  |  | | 10.5.5.0/24 | R-RIPv1,v2 | 120 | 2 | 10.5.4.2 | vlan4 | | 10.5.7.0/24 | 直连 |  |  |  |  | | R1 | 10.5.3.0/24 | R-RIPv1,v2 | 120 | 1 | 10.5.4.1 | Ethernet1/0[0] | | 10.5.4.0/24 | 直连 |  |  |  |  | | 10.5.7.0/24 | R-RIPv1,v2 | 120 | 1 | 10.5.4.1 | Ethernet1/0[0] |  * 1. 步骤5之后。   测试连通性（在PC1/PC2上pingPC3/PC4，看能否ping通），记录连通性结果，写出原因。查看PC1-PC4的路由连通路径。  PC1能ping通PC3     * 1. 步骤6之后。   测试PC2与PC3连通性，查看PC2-PC3的路由连通路径。  能连通  此时PC2上ping PC3需要经过VLAN7，VLAN4，VLAN5，VLAN2     * 1. 步骤9之后.   分析所截获的报文，理解所截获的请求报文和应答报文的含义，选择一对请求/应答报文，将各字段值填入下表：  RIP请求报文   |  |  |  |  |  | | --- | --- | --- | --- | --- | | 观察点： | | 字段 | 值 | 含义 | | IP | | 目的地址 | 224.0.0.9 | 这条报文的目的地址 | | UDP | | 端口号 | 520 | 使用的udp端口号 | | RIP | 头部 | 命令字段 | 1 | 这是一条请求报文 | | 版本号 | 2 | 使用的协议为RIPV2 | | 路由信息 | 地址族标识 | 0 | 没有给出目的地址 | | 网络地址 | \ |  | | 跳数 | 16 | 相当于不可达 |   RIP应答报文   |  |  |  |  |  | | --- | --- | --- | --- | --- | | 观察点： | | 字段 | 值 | 含义 | | IP | | 目的地址 | 224.0.0.9 | 这条报文的目的地址 | | UDP | | 端口号 | 520 | 使用的udp端口号 | | RIP | 头部 | 命令字段 | 2 | 这是一条回复报文 | | 版本号 | 2 | 使用的协议为RIPV2 | | 路由信息 | 地址族标识 | 2 | 目的地址是ipv4 | | 网络地址 | 10.5.4.0 10.5.3.0 10.5.7.0 | 路由的目的地址 | | 跳数 | 1 1 16 | 到达上述地址的跳数 |   互动讨论主题  1）解释名词术语：缺省路由、直连路由、静态路由与动态路由；  缺省路由是一种特殊类型的静态路由，通常用于指导数据包向未知目的地的传输。在缺省路由中，目的地址和子网掩码都设置为全零（0.0.0.0/0）。这意味着，如果路由器上没有更具体的路由可用，那么所有目的地未知的数据包都将被发送到缺省路由指定的下一跳地址。  直连路由指的是路由器接口直接连接的网络子网的路由。当路由器的某个接口配置有有效的IP地址，并且该接口启动时，路由器会自动在其路由表中添加一个直连路由。  静态路由是网络管理员手动配置的固定路由。它不会自动适应网络结构的变化，因为它不依赖于路由选择协议来更新。  动态路由依赖于路由选择协议来自动发现网络中的路由信息。这些路由会根据网络的变化动态调整。当网络拓扑发生变化时（例如，链接的添加、移除或改变），路由协议会自动更新路由信息。  2）RIP构建路由的条件与好处；  条件：网络规模小、路由器支持、RIP版本一致、路由器之间直连与邻居关系。  优点： 配置实现简单、开销较小、问题定位快、适用于网络规模小的环境。  3）理解RIP构建的路由表及其使用；  RIP 路由器通过周期性广播其路由表，与邻近路由器交换路由信息。每次广播包含目的网络、下一跳路由器和到达目的地的距离。接收路由信息的路由器使用距离向量算法更新其路由表，计算最优路径，并将更新后的信息继续传播。这个重复过程确保整个网络中的路由器保持最新的路由信息。  4）RIP报文如何构建路由表；  RIP 协议通过请求和响应报文在路由器之间交换路由信息。路由器启动时发送请求报文获取邻居的路由表信息，邻居通过响应报文提供目的网络、下一跳和距离等路由项。接收路由信息的路由器利用距离向量算法更新其路由表，并定期广播更新后的信息，确保整个网络的路由信息共享和同步。   1. RIP报文的启动与报文形成次序的关系。   路由器启动后会初始化配置和路由表，初始路由表仅包含直接连接的路由。随后，路由器发送 RIP 请求报文向邻居获取路由信息，并处理响应报文，利用距离向量算法更新路由表。通过定期交换 RIP 报文，路由器逐步完善路由表，构建全面的网络路径信息。 | | | | | | | |
| 本人机位（图中标识） | | 2 | | | 同组人（只填一人） | | | X |
| 本人主要工作 | | 分析连通性，报文和原理。 | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |

实验七 OSPF路由协议分析

实验名称：OSPF路由协议分析 时间： 年 月 日 早□ 午□ 晚□

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 | 计试2201 | | 学号 | X | | 姓 名 | X | |
| 组别 | G6 | | | | | 联系电话 | X | |
| 使用设备组别  G1 G2  G3 G4  G5 G6  G7 G8  实验组网图  （标明设备编号、端口号、vlan号、IP地址） |  | | | | | | | |
| 实 验  结 果 | * + 1. 针对自己截获的报文，写出其包含的ospf报文的的含义（每类挑选一条）；结合实验获得的报文，简要描述ospf协议邻居建立和数据库同步的过程。   1354：hello报文，用于发现及维持邻居关系  1360：DD报文，用于描述整个数据库，该数据包仅在 OSPF 初始化时发送。其主要作用是描述本地 LSDB 的 LSA 摘要信息，并通过交换 DD 报文来确定哪些 LSA 需要交换。  1365：LSR报文，用于向相邻的 OSPF 路由器请求部分或全部的数据，这种数据包是  在当路由器发现其数据已经过期时才发送的。  1366：LSU 报文，这是对 LSA 数据包的响应。LSU 报文包含了所请求 LSA 信息的具  体细节，当路由器收到 LSU 报文后，会以 flooding 的方式发送出去。  1370：LSAck 报文：是对 LSA 数据包的响应。路由器收到 LSU 报文后，都会以组播  地址 224.0.0.5 发送 LSAck 报文表示自己已经收到相应的 LSA 信息。  建立和同步的过程：先是路由器发送各自的hello报文，并发现邻居关系。之后发送各自的DD报文来描述自身数据库，以此初始化OSPF。当自身数据过期时，发送LSA请求更新自身数据。对LSA报文回答LSU，即回复要请求更新的消息。对LSU回答LSAck表示收到了LSA消息。 | | | | | | | |
|  | * + 1. 说明路由器R1、R2中产生的OSPF路由表项的含义？   图一的OSPF路由表项表示，为了到达目标地址1.1.1.1/32，路由器需要通过接口Async0/0向下一跳路由器10.5.1.1发送数据包。OSPF的管理距离为110，度量值为11。  图一的OSPF路由表项表示，为了到达目标地址2.2.2.2/32，路由器需要通过接口Async0/0向下一跳路由器10.5.1.2发送数据包。OSPF的管理距离为110，度量值为11。      OSPF分组中有一种链路状态广播Router-LSA，说明它各字段的含义与作用。   * + 1. 选择封装在OSPF分组中的任一种链路状态广播Router-LSA，说明各字段的涵义与作用。   LS Age=1:  表示LSA的年龄，以秒为单位。用于判断LSA是否过期。  Options:  描述路由器支持的OSPF特性。图中只支持需求电路功能。  LS Type:1  LSA的类型，对于Router-LSA，该字段的值为1。  Link State ID:2.2.2.2  发布此LSA的路由器的Router ID。  Advertising Router:2.2.2.2  发布此LSA的路由器的Router ID，与Link State ID相同。  LS Sequence Number:0x80000010  LSA的序列号，用于区分不同版本的LSA。序列号增加表示新的版本。  LS Checksum:0x8748  该LSA的校验和，用于数据完整性验证。  Length:48  该LSA的总长度，包括头部和内容。 | | | | | | | |
| 本人机位（图中标识） | | 2 | | | 同组人（只填一人） | | | X |
| 本人主要工作 | | 分析ospf协议，设置拦截报文，分析路径 | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |

实验八 防火墙与SSLVPN

实验名称：防火墙与SSLVPN实验 时间： 年 月 日 早□ 午□ 晚□

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 | 计试2201 | | 学号 | X | | 姓 名 | X | |
| 组别 | G6 | | | | | 联系电话 | X | |
| 使用设备组别  G1 G2  G3 G4  G5 G6  G7 G8  实验组网图  （标明设备编号、端口号、IP地址等） |  | | | | | | | |
| 实 验  结 果 | 1. 本组CISCO ASA5505中Vlan的划分、命名及端口分配方案是：   Vlan2:PC1,PC2  Vlan1:PC3,PC4  0端口分到VLAN2，其余在VLAN1   1. CISCO ASA5505内网DHCP服务器的IP范围是：   10.1.5.2-10.1.5.33   1. SSL VPN用户地址池的名称和地址范围是：   ssluser 10.10.10.1-10.10.10.10   1. 创建的SSL VPN用户名是：vpnuser1,vpnuser2 2. 所配置的防火墙测试方案及结果是：   外网 Web 模式能访问内部 Web 资源  外网客户端模式能访问内部 Web 资源     1. 分析步骤10完成捕获的报文，分析两台PC上报文的差别。   通过客户端连接 VPN，客户端会被分配一个 VPN 地址，即报文地址中的  10.10.10.1。客户端可以看到内网 PC 的 IP 地址，穿过防火墙直接地进行通信，因此，  在 PC1 抓包看到的目的地就是内网 PC 的 IP 地址 10.6.3.80，在内网 PC 上看到的来源  是 10.10.10.1，即外网 PC 所使用的 VPN 用户地址。 | | | | | | | |
| 本人机位（图中标识） | | 2 | | | 同组人（只填一人） | | | X |
| 本人主要工作 | | 协助SSLVPN，WEBVPN服务配置，抓包分析。 | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |

选做实验

实验名称： 时间： 年 月 日 早□ 午□ 晚□

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 |  | | 学号 |  | | 姓 名 |  | |
| 组别 |  | | | | | 联系电话 |  | |
| 实验组网图  （标明设备编号、端口号、IP地址等） |  | | | | | | | |
| 实验过程及结果 |  | | | | | | | |
| 本人机位（图中标识） | |  | | | 同组人（只填一人） | | |  |
| 本人主要工作 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |