

**计算机网络实验报告**

|  |  |
| --- | --- |
| **班级：** | 计算机越杰2101 |
| **学号：** | 2213611582 |
| **姓名：** | 段弘毅 |
| **组号：** | 第一组 |

二〇二三年九月

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：2023年 10月 24日 早□ 午□ 晚√

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **班 级** | **计算机越杰2101** | | **学号** | **2213611582** | | **姓 名** | **段弘毅** | |
| 组别 | G1 | | | | | **联系电话** | **18302968081** | |
| 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 | PCA ping PCB | Ping 10.1.2.12 | 能 | | PCC ping PCD | Ping 10.1.3.14 | 能 | | 不同网段中 | PCB ping PCC | Ping 10.1.3.123 | 能 | | PCD ping PCA | Ping 10.1.2.11 | 能 |     2.用show ip route查看R1的路由表，分析不同网段互通的原因？    如果路由器下的两个端口分别连接到两台交换机，那么这两台交换机之间可以互相通信。因此，每台交换机所在的网络段也能够相互连接 | | | | | | | |
| 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PCA，认证用户为 user1 ，身份验证方法为 密码:user1 。  （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：  ping 10.1.2.12 无法访问目标主机 请求超时  （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与相同网段PC互通的测试命令及结果是：  ping 10.1.2.12 正在Ping 10.1.2.12 具有65500字节的数据：来自10.1.2.12的回复：字节=65500时间=49ms TTL=50  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。  交换机的关键操作流程涉及：监测端口的当前状态，对未通过认证的端口进行处理，向认证服务器发送请求，等待并接收服务器的响应，进行认证过程中的交互质询，处理最终的认证结果，并保持认证状态的持续更新。  而认证服务器的核心工作步骤包括：接受来自交换机的认证请求，验证请求者的身份信息，通过质询步骤加强认证的安全性，核实认证凭证的有效性，制定最终的认证决策，并将该结果反馈给交换机，同时保持认证过程的连续性和稳定性。  **5.进阶自设计实验（选）写在新的一页中，要求详见实验指导书2.6节**  1）采用 Wireshark 软件捕获接入认证的报文，分析 802.1x 认证交互过程.    端口状态检查、认证请求、认证响应、认证质询、认证凭据传输、认证凭据验证、认证结果通知、重新认证和保持活动状态。 | | | | | | | |
| 本人机位（图中标识） | | 2-PC2 | | | 同组人（只填一人） | | | 姬天骄 |
| 本人主要工作 | | 我主要承担了第二部分关于802.1x认证服务器的一系列关键任务。这些任务不仅包括从头开始构建认证服务器的认证端点，而且还涉及到为系统添加新的用户账户，确保每个环节的功能都能正常运行。接着，我负责对认证服务器进行全面的测试，以验证其性能和稳定性，同时也配置了与认证服务器直接连接的认证交换机，确保网络设备之间的兼容性和高效通信。此外，我还进行了认证客户端的连接测试，这是为了验证客户端是否能够顺利地通过认证过程并成功接入网络。最后，作为整个项目的一部分，我使用Wireshark这一强大的网络分析工具来捕获和分析认证过程中客户端与服务器之间的数据传输，这帮助我们深入理解认证过程的内在机制，并确保数据传输的安全性和效率。 | | | | | | |
| 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：2023年10月31日 早□ 午□ 晚√

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **班 级** | **计算机越杰2101** | **学号** | **2213611582** | **姓 名** | **段弘毅** |
| 组别 | G1 | | | **联系电话** | **18302968081** |
| 实验组网图 | 交换机5650 1:Pc1->1口，2->2口，3->3口，4->4口 | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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）。  在同一个虚拟局域网（VLAN）内，两台计算机能够相互通信，但处于不同VLAN的计算机则无法进行通信。这是因为设置不同的VLAN本质上是在创建隔离的网络环境，每个独立的网络中的主机无法感知或直接与其他网络中的主机进行通信。        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。        主机在相同的虚拟局域网（VLAN）内可以互相进行ping操作，但如果它们位于不同的VLAN中，则不能实现此类通信。这种情况发生的原因是，在交换机之间设置了trunk端口，并且将这些端口分别配置为属于不同的VLAN。因此，虽然位于不同交换机上但属于同一VLAN的主机能够通过trunk端口互相通信，但不同VLAN的主机由于VLAN间的隔离原则，其数据包会被交换机拒绝转发，从而无法实现通信  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： | 没有 | | Reply报文： | 没有 | | S1 - S2 | Request报文： | 预期出现，为2 | | Reply报文： | 预期出现，为2 | | S2 – PC2 | Request报文： | 没有 | | Reply报文： | 没有 |   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： | 没有 | | Reply报文： | 没有 | | S1 -- S2 | Request报文： | 预期出现，为2 | | Reply报文： | 预期出现，为3 | | S2 -- PC4 | Request报文： | 没有 | | Reply报文： | 没有 |   这种通信实现的原因在于，交换机S1上配置了专门为VLAN 2和VLAN 3设置的网关。由于S1的trunk端口允许VLAN 2和VLAN 3之间的通信，不同VLAN中的设备发送的报文都会被导向S1。在S1上，报文通过配置的网关找到目标VLAN的地址，然后被转发到目标设备，从而实现了跨VLAN的通信。  **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的配置  1. 创建VLAN\*  在交换机上创建VLAN，涉及到定义一个或多个VLAN ID。每个VLAN都有一个独特的标识符，用于区分网络中的不同虚拟局域网。  2. 端口分配  将交换机的特定端口分配到创建的VLAN中。这意味着连接到这些端口的设备将成为VLAN网络的一部分。  3. 配置Trunk端口  Trunk端口用于在多个交换机之间传输多个VLAN的数据。通过在交换机间配置Trunk端口，可以实现不同交换机上相同VLAN内设备的互通。  4. Access和Hybrid端口  Access端口只允许特定VLAN的数据通过，通常用于连接终端用户设备。  Hybrid端口可以同时接收多个VLAN的数据，但通常有更复杂的配置，用于特定网络需求。  VLAN的工作原理  1. VLAN标签（VLAN Tag）  根据IEEE 802.1Q标准，在以太网帧中加入一个4字节的VLAN标签（Tag）。这个标签包括VLAN ID和其他控制信息。  2. IEEE 802.1Q数据帧  802.1Q标准定义了带有VLAN标签的数据帧格式。当一个数据帧从一个Trunk端口发送时，它包含了VLAN标签，使得接收端的交换机能够识别该数据帧属于哪个VLAN。  3. 数据帧的传输  当数据帧到达一个Trunk端口，交换机根据帧中的VLAN标签决定如何转发这个帧。如果接收端口是一个Access端口，且属于数据帧中标记的VLAN，则数据帧会被转发到该端口；如果不是，数据帧则会被丢弃。  4. 隔离和通信  VLAN技术允许网络管理员逻辑上隔离不同的网络段，即使它们物理上连接到同一个交换机。这种隔离增加了网络的安全性和效率，因为每个VLAN内的通信都被限制在该VLAN内部，不同VLAN之间的直接通信被阻止，除非通过路由器或层3交换机。 | | | |
| 本人机位（图中标识） | | 2-PC3 | 同组人（只填一人） | 姬天骄 |
| 本人主要工作 | | 主要负责配合操作，在VLAN划分与通信、Trunk端口配置、端口镜像的配置及报文的捕获与记录分析、VLAN间通信的设置与报文捕获分析时指导和讨论 | | |
| 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：2023年11月7日 早□ 午□ 晚√

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **班 级** | **计算机越杰2101** | | **学号** | **2213611582** | | **姓 名** | **段弘毅** | |
| 组别 | G1 | | | | | **联系电话** | **18302968081** | |
| 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。     图上所示的两段内容展示了PCA设备上的两个网络接口所对应的IP地址到MAC地址的映射关系。“arp -a”命令用于展示ARP（地址解析协议）缓存信息。这个ARP缓存实际上是一个用于存储IP地址与相应MAC地址配对的内存区域，基本上就像一个将IP地址映射到MAC地址的列表。每个列表项包含了网络中其他设备的IP地址及其相应的MAC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 | ff:ff:ff:ff:ff:ff | 00:e0:4c:01:90:95 | | 以太网链路层Source项 | 00:e0:4c:01:90:95 | 00:e0:4c:68:f3:0b | | ARP报文发送者硬件地址 | 00:e0:4c:01:90:95 | 00:e0:4c:68:f3:0b | | ARP报文发送者IP | 10.1.2.11 | 10.1.2.12 | | ARP报文目标硬件地址 | 00:00:00:00:00:00 | 00:e0:4c:01:90:95 | | ARP报文目标IP | 10.1.2.12 | 10.1.2.11 |  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 | ff:ff:ff:ff:ff:ff | 00:e0:4c:68:f3:0b | | 以太网链路层Source项 | 00:e0:4c:68:f3:0b | 44:ad:d9:67:01:42 | | ARP报文发送者硬件地址 | 00:e0:4c:68:f3:0b | 44:ad:d9:67:01:42 | | ARP报文发送者IP | 10.1.3.12 | 10.1.3.1 | | ARP报文目标硬件地址 | 00:00:00:00:00:00 | 00:e0:4c:68:f3:0b | | ARP报文目标IP | 10.1.3.1 | 10.1.3.12 |   当ARP（地址解析协议）缓存中不存在某个IP地址与MAC地址的对应关系时，若ARP请求的发送者和目标接收者位于不同的网络段，发送的ARP请求会定向到该网络段的网关。这里的ARP请求报文具有以下特点：  1. 目标MAC地址  在ARP请求报文中，目标MAC地址被设置为"00:00:00:00:00:00"，表示目的硬件地址尚未晓。  2. 广播地址  "ff:ff:ff:ff:ff:ff"用作目标地址，这是一个广播地址，意味着报文将被发送给同一局域网中的所有设备。  接下来，当ARP应答报文被发送时：  1. 路由器网关响应  ARP应答是由路由器网关发出的，它作为该网络段的网关设备，向请求方提供所需信息。  2. 源和目标地址  ARP应答报文的源地址是路由器的MAC地址和网关IP地址，而目标地址则是原ARP请求发送者（即PC）的MAC地址和IP地址  这个过程确保了不同网络段中设备之间的正确通信，即使在初次通信时没有缓存的IP到MAC地址映射。   1. 完成步骤4后，测试结果及原因是：           在Cisco 3560交换机上，应用访问控制列表（ACL）技术进行MAC与IP绑定意味着，通信的成功与否取决于是否在ACL中包含了相应的MAC和IP地址匹配。如果更改了PC的IP地址、更换接入网络的MAC地址，或同时更改IP和MAC地址，这些都会导致与ACL中的规则不符，从而阻断通信。相对地，如果在VLAN 2中新增一个未受限制的接口（如fa0/1），由于它不受ACL规则限制，因此不会影响到该接口的链接通信。   1. **进阶自设计实验（选）写在新的一页中，要求详见实验指导书。**   运行软件时之前，先扫描局域网的机器。    之后可以获得目标主机的IP地址。    之后用SniffLa监听整个网络任意机器之间的通讯，  这个过程的原理是通过ARP欺骗使局域网内的所有设备误以为攻击者的机器是网络网关，进而实现对整个网络的监听。在发动攻击后，攻击者会用抓包软件捕捉网络流量，从而可以看到数据包和流量统计数字不断增加。这样，攻击者就能够直接监控到特定目标机器的上网流量。 | | | | | | | |
| 本人机位（图中标识） | | 2-PC3 | | | 同组人（只填一人） | | | 姬天骄 |
| 本人主要工作 | | 本次实验  我协助进行了设备的连接，：交换机的配置，ARP报文的捕获记录与分析；  同时，我主要执行了交换机上MAC与IP绑定与WinArpAttacker进行监听目标主机流量的实验部分。 | | | | | | |
| 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：2023年11月14日 早□ 午□ 晚√

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **班 级** | **计算机越杰2101** | | **学号** | **2213611582** | | **姓 名** | **段弘毅** | |
| 组别 | G1 | | | | | **联系电话** | **18302968081** | |
| 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。 2. 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 | 10.1.3.14 | 10.1.2.12 | 10.1.3.14 | | 捕获的报文序号 | 45 | 48 | 49 | | Sequence Number | 0 | 0 | 1 | | Acknowledgement Number | 0 | 1 | 1 | | ACK标志 | 0 | 1 | 1 | | SYN标志 | 1 | 1 | 0 |  1. 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 | 10.1.3.14 | 10.1.2.12 | 10.1.2.12 | 10.1.3.14 | | 捕获的报文序号 | 976 | 977 | 978 | 979 | | Sequence Number | 341837 | 1 | 1 | 341838 | | Acknowledgement Number | 1 | 341838 | 341838 | 2 | | ACK标志 | 1 | 1 | 1 | 1 | | FIN标志 | 1 | 0 | 1 | 0 |  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 | | 50 | 数据 | 1 | 1 | 1460 | 49 | 65536 | | 51 | 数据 | 1461 | 1 | 540 | 50 | 65536 | | 52 | 确认 | 1 | 2001 | 0 | 51 | 65536 | | 53 | 数据 | 2001 | 1 | 1460 | 52 | 65536 | | 54 | 数据 | 3461 | 1 | 540 | 53 | 65536 | | 55 | 确认 | 1 | 4001 | 0 | 54 | 65536 | | 56 | 数据 | 4001 | 1 | 1460 | 55 | 65536 | | 57 | 数据 | 5461 | 1 | 540 | 56 | 65536 | | 58 | 确认 | 1 | 6001 | 0 | 57 | 65536 | | 59 | 数据 | 6001 | 1 | 1460 | 58 | 65536 | | 60 | 数据 | 7461 | 1 | 540 | 59 | 65536 | | 61 | 确认 | 1 | 8001 | 0 | 60 | 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？   在TCP协议中，通过确认号（ACK number）来验证哪些数据已经成功被接收。发送方发送数据后，接收方会回复一个确认号，该确认号是发送方数据的序列号加上数据的长度。如果发送方收到的确认号与这个计算结果相匹配，就可以确认该数据已被成功接收。在分析抓包数据时，查看每个TCP报文的确认号字段可以帮助确认哪些报文已经被接收。  窗口值的调整由发送方和接收方共同决定。接收方会根据自己的缓冲区大小和处理能力来调整窗口值，通过发送带有窗口通告字段（Window Advertisement）的报文告知发送方。当接收方缓冲区有空间接收更多数据时，它会增加窗口值。发送方则根据接收方的窗口通告来调整其发送数据量。如果接收方的窗口值为0，发送方将暂停数据发送，直到接收方窗口值大于0，此时发送方根据新的窗口值发送相应量的数据，以避免因数据过载引起网络拥堵。   1. 进阶自设计实验写在新的一页中（选），要求详见实验指导书。 | | | | | | | |
| 本人机位（图中标识） | | 2-PC3 | | | 同组人（只填一人） | | | 姬天骄 |
| 本人主要工作 | | 分析TCP报文的分析，设备初始化 | | | | | | |
| 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2023年11月21日 早□ 午□ 晚√

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **班 级** | **计算机越杰2101** | | **学号** | **2213611582** | | **姓 名** | **段弘毅** | |
| 组别 | G1 | | | | | **联系电话** | **18302968081** | |
| 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：在浏览器中访问3个网址，比如[www.xjtu.edu.cn](http://www.xjtu.edu.cn), [www.github.com](http://www.github.com), [www.unb.br](http://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。  在分析网络通信时，特别关注不同协议如何协同工作以及它们在处理访问请求时的延迟情况。重点观察HTTP协议下的请求和响应行为。在访问一个特定网站时，注意以下几点：网站访问过程中建立的连接数量、下载的资源类型数量（如HTML文件、CSS样式表、JavaScript文件、图片等）、进行的DNS查询次数、以及是否涉及Cookie的使用等。  （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。    （3）使用ncat工具访问HTTP服务  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. 互动讨论主题   HTTP协议的缓存，DNS的缓存；缓存对网络访问速度的影响。  HTTP缓存机制:  当客户端请求网页资源（如HTML、CSS、图片等）时，浏览器会首先检查本地缓存中是否已有该资源的副本。  HTTP缓存主要处理GET请求的响应。在初次请求资源时，服务器在响应头中发送资源的缓存参数。基于这些参数，浏览器在随后的请求中可能不需要再向服务器请求同一资源。  如果浏览器缓存中存在请求的资源副本，并且该副本仍然是最新的（根据缓存参数），浏览器会直接从缓存中加载资源，状态码为200。这被称为“强缓存”。  如果强缓存不适用，浏览器将发送请求至服务器，询问是否有更新。如果服务器确认当前缓存仍有效，返回304状态码，指示浏览器使用本地缓存。这被称为“协商缓存”。  DNS缓存的作用:  DNS缓存是对域名解析结果的本地存储。当域名第一次被解析后，解析结果会存储在本地，附带一个TTL值指示其有效期。  对于后续相同域名的请求，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。  这种缓存策略显著提高了网络访问速度，降低了网络延迟，减少了带宽使用，并提升了用户体验。  缓存的总体益处:  缓存机制减轻了服务器的负担，因为许多请求可以直接由客户端的缓存处理，无需额外的服务器资源。  它加快了网页的加载速度，因为从本地缓存加载资源比从服务器重新获取要快得多。  支持离线访问，用户可以在没有网络连接时浏览之前访问过的网页。  减少了网络流量消耗，这对于有数据使用限制的网络环境尤其重要。 | | | | | | | |
| 本人机位（图中标识） | | 2-PC3 | | | 同组人（只填一人） | | | 姬天骄 |
| 本人主要工作 | | 初始化，对HTTP协议的抓包 | | | | | | |
| 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：2023年 11月 28日 早□ 午□ 晚√

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **班 级** | **计算机越杰2101** | | **学号** | **2213611582** | | **姓 名** | **段弘毅** | |
| 组别 | G1 | | | | | **联系电话** | **18302968081** | |
| 实验组网图 |  | | | | | | | |
| 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。     由于路由器R1和PC1、PC2位于不同的网络段，且R1目前没有关于PC1和PC2所在网络段的路由信息，所以R1无法成功执行对PC1和PC2的ping操作。由于缺少必要的路由表项，R1无法确定到达这两台PC的路径   * 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。     由于R1已经通过静态路由配置得知了10.1.7.0网络段的路由信息，它能够识别并访问到PC1和PC2所在的网络。因此，R1现在可以成功地对PC1和PC2执行ping操作   * 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。     由于交换机S1中的三个虚拟局域网（VLAN）相关的路由信息已经通过动态路由信息协议（RIP）传递给了路由器R1，因此R1能够识别并访问到这些VLAN，使得它可以成功地对网络中的设备进行ping通信   * 1. 查看路由填写下表。  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | 设备 | Destination/Mask | Protocol | Pref | Cost | Nexthop | Interface | | S1 | 10.1.3.0/24 | D | 0 | 0 | Vlan3 | Vlan3 | | 10.1.4.0/24 | D | 0 | 0 | Vlan4 | Vlan4 | | 10.1.7.0/24 | D | 0 | 0 | Vlan7 | Vlan7 | | 127.0.0.0/8 | D | 0 | 0 | Loopback | Loopback | | R1 | 10.1.3.0/24 | R | 120 | 1 | 10.1.3.1 | E1/0 | | 10.1.4.0/24 | D | 0 | 0 | Vlan4 | E1/0 | | 10.1.7.0/24 | R | 120 | 1 | 10.1.4.1 | E1/1 |  * 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。    硬件问题造成PC3无法ping通    PC1&PC2可以ping通PC3&PC4，因为S1与S2之间通过网线直连，且两侧同属于vlan3。   * 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。       * 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 | 所有RIP2路由器 | | UDP | | 端口号 | 520 | 默认UDP协议端口号 | | RIP | 头部 | 命令字段 | 1 | Request | | 版本号 | 2 | RIP version2 | | 路由信息 | 地址族标识 | 0 | 解释网络地址时应遵循的协议族 | | 网络地址 | 0.0.0.0 |  | | 跳数 | 0 |  |   RIP应答报文   |  |  |  |  |  | | --- | --- | --- | --- | --- | | 观察点： | | 字段 | 值 | 含义 | | IP | | 目的地址 | 224.0.0.9 | 所有RIP2路由器 | | UDP | | 端口号 | 520 | 默认UDP协议端口号 | | RIP | 头部 | 命令字段 | 2 | Response | | 版本号 | 2 | RIP version2 | | 路由信息 | 地址族标识 | 2 | 解释网络地址时应遵循的协议族 | | 网络地址 | 10.1.7.0 | 该报文返回学习的地址 | | 跳数 | 4 | 经4跳可达Source |   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（Default Route）:  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。缺省路由常用于连接到互联网，作为内部网络向外部世界发送数据的最后出口。  直连路由:  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。这个路由指示路由器如何向直接连接的网络发送数据包。  静态路由:  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。静态路由适用于网络结构简单、稳定或不经常变化的情况，或者作为动态路由的补充。  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。动态路由适用于网络规模较大、经常变化的环境，因为它们减少了网络管理员的手动配置负担。  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路由表是通过路由器间不断交换路由信息来建立和更新的。RIP路由器会周期性地向其他路由器广播它所知的所有路由信息，包括目的网络的位置、到达那里的下一跳路由器以及到目的地的距离。收到这些信息的路由器会用距离向量算法来更新自己的路由表，计算出到每个目的地的最优路径，并把这些更新后的路由信息传递给邻近的路由器。这个过程不断重复，以此确保整个网络中的每个路由器都有最新的路由信息。  4）RIP报文如何构建路由表；  路由器利用RIP协议的报文互相交换路由信息。当一个路由器启动，它发送请求报文给它的邻居路由器，询问它们的路由表信息。收到这些请求的路由器会回复，通过响应报文发送它们的路由表信息给发起请求的路由器。这些响应报文包含了每个路由项的详细信息，例如目的网络、下一跳路由器和距离。  路由器接收到这些响应后，会根据所含的路由信息来更新自己的路由表，使用距离向量算法进行更新。随着RIP报文的定期交换，各个路由器逐渐共享并汇总彼此的路由信息，进而构建起网络的完整路由表。每个路由器会根据收到的信息以及自己的现有路由表来计算出到达各个目的地的最短路径，并将这些新的路由信息通过广播传递给邻近的路由器，确保整个网络的路由信息得到更新和维护。  5）RIP报文的启动与报文形成次序的关系。  路由器的启动阶段：一旦路由器启动，它首先进行初始化，这包括加载配置和分配IP地址。此时，路由器也会检查RIP协议是否已激活，并根据其配置进行设置。  初始化路由表：路由器启动后，它会建立起初始的路由表。一开始，这个路由表可能为空，或者仅包含与路由器直接连接的路由信息。由于尚未从其他路由器接收到RIP报文，路由器此时还不了解网络的其他部分。  发送RIP请求报文：路由器启动后，会向邻近的路由器发送RIP请求报文，以获取它们的路由信息。这一步骤是为了收集网络中其他路由器的信息，帮助构建一个全面的路由表。  处理收到的响应：在发出请求报文后，路由器等待并处理来自邻居路由器的RIP响应报文。收到响应后，路由器会解析其中包含的路由信息，并利用距离向量算法来更新其路由表。  构建完整的路由表：随着时间的推移，通过定期交换RIP报文，路由器逐步获取到网络中其他路由器的路由信息。这些信息被用来更新路由器的路由表，最终形成一个全面反映网络可达路径和距离信息的整路由表。 | | | | | | | |
| 本人机位（图中标识） | | 2-PC3 | | | 同组人（只填一人） | | | 姬天骄 |
| 本人主要工作 | | 分析连通性与报文 | | | | | | |
| 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：2023年12月5日 早□ 午□ 晚√

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **班 级** | **计算机越杰2101** | | **学号** | **2213611582** | | **姓 名** | **段弘毅** | |
| 组别 | G1 | | | | | **联系电话** | **18302968081** | |
| 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。     在OSPF协议的运作中，R1启动OSPF后开始周期性地发送Hello报文，以便与邻近的路由器建立邻居关系。当R2也开启OSPF并发出Hello报文时，R1和R2互相接收对方的Hello报文，进而开始相互交换数据库描述（DD）报文，分享彼此的链路状态信息。在这个过程中，初步两者都试图成为主路由器（Master）。  随后，通过一定的协商过程，确定两者中的一个为主路由器，另一个作为从路由器（Slave），继续交换DD报文以共享链路信息。如果任一路由器发现对方有自己尚未知晓的链路信息，它将发送链路状态请求（LSR）报文，请求获取详细的链路状态信息。接收到LSR报文的路由器响应以链路状态更新（LSU）报文，向请求方提供所需信息。最后，收到信息的路由器通过发送链路状态确认（LSAck）报文确认信息接收。  这一系列的报文交换完成后，两个路由器之间的邻居关系和数据库同步就顺利完成了。 | | | | | | | |
|  | * + 1. 说明路由器R1、R2中产生的OSPF路由表项的含义？     OSPF协议中包含三个关键的表项：OSPF邻居表、链路状态数据库（LSDB）表和OSPF路由表。  1. OSPF邻居表  在OSPF协议中，路由器首先需要建立邻居关系才能交换链路状态信息。这种邻居关系是通过互相发送Hello报文来建立的。  OSPF邻居表记录了与一个路由器相邻的其他OSPF路由器的信息和状态。  2. LSDB表  链路状态数据库（LSDB）存储了路由器自己生成的和从邻居路由器接收到的链路状态公告（LSA）信息。  这个表中的信息包括LSA的类型（Type）和发出LSA的路由器（AdvRouter）。  3. OSPF路由表  OSPF路由表与路由器的一般路由表是两个不同的概念。OSPF路由表包含了用于数据包转发决策的关键信息，如目的地（Destination）、路径成本（Cost）和下一跳（NextHop）等。  这些表项共同协作，使OSPF能够高效地管理和转发网络中的数据流量     * + 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 年龄”显示自LSA生成以来经过的时间，单位是秒。  - “选项”字段用于指定附加特性。  - “LS 类型”字段用于识别LSA的数据包类型。  - “链路状态ID”具有不同的含义，这取决于LS类型字段的值。  - “通告路由器”字段显示了生成该LSA的路由器的ID。  - 其余字段包括序列号、校验和和长度，分别用于保证LSA的一致性和完整性。  进阶自设计实验（选）写在新的一页中，要求详见实验指导书。  在这个网络中，DCR-2626和DCRS-5650运行着OSPF协议，用于实现动态路由选择。OSPF协议使用Dijkstra算法来计算最短路径，以确定数据包的最佳路由路径。  当DCR-2626和DCRS-5650之间建立OSPF邻居关系时，它们开始交换路由信息，并利用Dijkstra算法计算出整个网络的最短路径。每个路由器维护一个链路状态数据库，其中包含了网络的拓扑信息，包括连接到的网络和链路的成本。基于这些信息，每个路由器能够计算出到达目标网络的最短路径，并将这些信息添加到自己的路由表中。  当数据包需要从源网络发送到目标网络时，发送方路由器会查询自己的路由表，以确定数据包的下一跳路由器。这个下一跳路由器会继续查询自己的路由表，逐步将数据包转发到目标网络。这个过程保证了数据包沿着最短路径进行传输。  在此网络中，DCR-2626还配置了NAT协议，允许它将局域网内的私有IP地址映射为校园网的公共IP地址。这意味着当数据包从局域网发往校园网时，DCR-2626会对数据包进行源IP地址的转换，以确保数据包在离开局域网后具有合适的源地址。在数据包返回时，DCR-2626将目标IP地址还原为原始的源地址。  综上所述，OSPF协议利用Dijkstra算法实现最短路径计算，确保了数据包的有效路由。此外，NAT协议的配置使得局域网内的主机能够与外部网络通信，实现了局域网与广域网之间的互联。这些协议和算法共同构建了网络的高效通信和路由机制。 | | | | | | | |
| 本人机位（图中标识） | | 2-PC3 | | | 同组人（只填一人） | | | 姬天骄 |
| 本人主要工作 | | 设置拦截报文，分析OSPF协议，分析通路 | | | | | | |
| 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：2023年12月12日 早□ 午□ 晚√

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **班 级** | **计算机越杰2101** | | **学号** | **2213611582** | | **姓 名** | **段弘毅** | |
| 组别 | G1 | | | | | **联系电话** | **18302968081** | |
| 使用设备组别  G1  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：      1. CISCO ASA5505内网DHCP服务器的IP范围是：   10.1.3.2-10.1.3.33   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：   username vpnuser1 password vpnuser1  username vpnuser2 password vpnuser2   1. 所配置的防火墙测试方案及结果是：                1. 分析步骤10完成捕获的报文，分析两台PC上报文的差别。   Web模式：  PC机：    服务器端：  C:\Users\Administrator\Desktop\捕获1.PNG  在Web模式下，PC和服务器之间的数据传输涉及使用网关进行通信。服务器端通过TCP协议来传输和确认数据报文，而PC端则通过TLSv1协议来接收数据，并使用TCP协议进行报文确认  客户端模式：  PC机：    (exp)    (cisco)  服务器端：  C:\Users\Administrator\Desktop\捕获2.PNG  在客户端模式中，由于VPN配置的虚拟网卡的影响，防火墙将PC和服务器视为同一网络段的设备。因此，它们之间的数据报文直接通过TCP协议互相发送和接收，好像没有通过网关。然而，实际上PC机仍然通过其在exp物理网卡所指定的网关接收数据   1. 进阶自设计。   园网络环境中，计算机或移动设备通过校园内的DHCP服务器获取一个内部IP地址。设备与校园内的资源交流主要依赖交换机和路由器，通常不需要额外的加密或建立隧道。  WebVPN时，用户需要登录WebVPN服务以创建一个加密的隧道连接到校园网络。在这种情况下，访问校园资源的数据传输主要依赖HTTPS协议，确保在WebVPN客户端和服务器之间的数据是加密的。  SLVPN则在用户的计算机上创建一个虚拟网络接口，同样建立一个加密隧道到校园网络。它也使用HTTPS协议来保证数据传输的安全。与WebVPN相比，SSLVPN提供更广泛的远程访问选项，不仅限于通过Web浏览器访问。 | | | | | | | |
| 本人机位（图中标识） | | 2-PC3 | | | 同组人（只填一人） | | | 姬天骄 |
| 本人主要工作 | | 初始化、SSLVPN与WEBVPN服务的配置、web资源的访问抓包与分析。 | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |