计算机网络专题实验现场检查单1（共1页）

实验名称：组网与接入认证 时间：2024 年 5 月 10 日 早☑ 午□ 晚□

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 |  | | 学号 |  | | 姓 名 |  | |
| E-Mail |  | | | | | 联系电话 |  | |
| 使用设备组别  G1 G2  G3 G4  G5 G6  G7 G8  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 PC2 | ping 10.1.2.12 | 能 | | PC3 ping PC4 | ping 10.1.3.14 | 能 | | 不同网段中 | PC2 ping PC3 | ping 10.1.3.13 | 能 | | PC1 ping PC4 | ping 10.1.3.14 | 能 |   2. 用display ip routing-table查看R1的路由表，分析不同网段互通的原因？  在R1的路由表中，存在10.1.2.0/24和10.1.3.0/24的项。这意味着不同网段的交换机连到同一个路由器上，路由器会根据路由表转发信息，从而实现不同网段的互通。 | | | | | | | |
| 本人机位（图中标识） | | PC1 | | | 同组人（只填一人） | | |  |
| 本人主要工作 | | 配置PC1 | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |

计算机网络专题实验现场检查单2（共2页）

实验名称：VLAN的配置与协议分析 时间：2024 年 5月 10日 早☑ 午□ 晚□

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 |  | | 学号 |  | | 姓 名 |  | |
| E-Mail |  | | | | | 联系电话 |  | |
| 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．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中的计算机能够直接通信，因为它们处于同一广播域中。而不同VLAN之间的计算机在没有进行特定配置以实现VLAN间路由的情况下无法直接通信，这是由VLAN技术的隔离特性所决定的。  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。  完成Trunk端口配置后，同一VLAN内的计算机能够正常通信，因为它们处于相同的广播域中。Trunk端口允许来自多个VLAN的数据通过一个物理链接传输，确保了数据包在保持其VLAN标识的同时，能从一个交换机传输到另一个交换机。  对于不同VLAN的计算机，通常情况下，它们无法直接通信。这是因为不同VLAN分隔了广播域，  3. 填写步骤7中的表格并解释原因（设置镜像端口后）。   |  |  |  | | --- | --- | --- | | Ping发起： | Source: | Destination: | | 观查点 | 10.1.2.11 10.1.2.13 | |  |  |  |  |  | | --- | --- | --- | --- | | 转发过程（标明方向） | 报文类型（请求/响应） | VLAN标记（只填写观察到的） | 标记出现与否的原因 | | PCA — S1 | 请求 | 无 | 无法观察 | | S1 — S2 | 请求 | VLAN2 | 为了确保S2能理解数据包属于VLAN2，数据包保留VLAN2标记，镜像到PC2上得以观察 | | S2 — PCC | 请求 | 无 | VLAN标记已被剥去 |   4. 完成实验步骤10后，解释不同Vlan 间可以通信的原因？  通过在交换机S1上配置VLAN2和VLAN3的接口IP地址，并设置计算机的默认网关为它们各自VLAN的接口IP，实质上为两个VLAN之间提供了通信路径。这时，PCC和PCD之间的ping通信得以实现，是因为配置了交换机S1的Layer 3功能，将其作为两个VLAN间的路由器使用。这使得从PCC发出的ICMP请求通过其网关（VLAN2的接口IP），由S1路由到PCD所在的VLAN3，并通过PCD的网关（VLAN3的接口IP）回到PCD，完成了请求和响应的过程。 | | | | | | | |
| 本人机位（图中标识） | | PC1 | | | 同组人（只填一人） | | |  |
| 本人主要工作 | | 配置PC1 | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |

计算机网络专题实验现场检查单3（共2页）

实验名称：ARP协议分析与欺骗防范 时间：2024年 5月 17日 早☑ 午□ 晚□

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 |  | | 学号 |  | | 姓 名 |  | |
| E-Mail |  | | | | | 联系电话 |  | |
| 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。   接口：10.1.2.11--0x10  Internet地址 物理地址 类型  224.0.0.22 01-00-5e-00-00-16 静态  239.255.255.250 01-00-5e-7f-ff-fa 静态  接口：10.1.2.11--0x10 这是指示ARP请求发起的网络接口及其地址为10.1.2.11，0x10为该网络接口的标识。  Internet地址224.0.0.22 对应物理地址 01-00-5e-00-00-16 类型静态  Internet地址239.255.255.250 对应物理地址 01-00-5e-7f-ff-fa 类型静态   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 | f0:92:1c:de:4c:9a | | 以太网链路层Source项 | f0:92:1c:de:4c:9a | 2c:44:fd:39:71:be | | ARP报文发送者硬件地址 | f0:92:1c:de:4c:9a | 2c:44:fd:39:71:be | | 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 | f0:92:1c:de:4c:9a | | 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 | 74:46:a0:96:20:1e | | 以太网链路层Source项 | 74:46:a0:96:20:1e | 34:66:56:4c:82:0c | | ARP报文发送者硬件地址 | 74:46:a0:96:20:1e | 34:66:56:4c:82:0c | | 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 | 74:46:a0:96:20:1e | | ARP报文目标IP | 10.1.3.1 | 10.1.3.12 |  1. 完成3.10节步骤4后，测试结果及原因是：   接口：10.1.2.11--0x10  Internet地址 物理地址 类型  224.0.0.22 01-00-5e-00-00-16 静态  239.255.255.250 01-00-5e-7f-ff-fa 静态  这个步骤的测试结果显示网络中针对组多播通信的基本配置是保留的，但是清理了其它动态学习的ARP条目。这种做法可能是为了网络维护、确保网络的基本多播通信功能不受影响，同时去除动态学习但当时不需要的ARP条目，保持ARP缓存的清洁。 | | | | | | | |
| 本人机位（图中标识） | | PC1 | | | 同组人（只填一人） | | |  |
| 本人主要工作 | | 配置PC1 | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |

计算机网络专题实验现场检查单4（共2页）

实验名称：TCP协议分析 时间： 2024年 5月17 日 早□ 午☑ 晚□

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 |  | | 学号 |  | | 姓 名 |  | |
| E-Mail |  | | | | | 联系电话 |  | |
| 使用设备组别  G1 G2  G3 G4  G5 G6  G7 G8  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 | 10.1.2.11 | 10.1.3.12 | 10.1.2.11 | | 捕获的报文序号 | 821 | 822 | 823 | | Sequence Number | 0 | 0 | 1 | | Acknowledgement Number | 0 | 1 | 1 | | ACK标志 | 0 | 1 | 1 | | SYN标志 | 1 | 1 | 0 |   （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 | 10.1.2.11 | 10.1.3.12 | 10.1.3.12 | 10.1.2.11 | | 捕获的报文序号 | 3854 | 3855 | 3856 | 3857 | | Sequence Number | 835025 | 1 | 1 | 835026 | | Acknowledgement Number | 1 | 835026 | 835026 | 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 | | 7217 | 数据 | 1 | 1 | 1460 | 1461 | 513 | | 7218 | 数据 | 1461 | 1 | 1460 | 2921 | 513 | | 7219 | 数据 | 2921 | 1 | 1460 | 4381 | 513 | | 7220 | 确认 | 1 | 4381 | 0 | 1 | 8212 | | 7221 | 数据 | 4381 | 1 | 1460 | 5841 | 513 | | 7222 | 确认 | 1 | 5841 | 0 | 1 | 8212 | | 7223 | 数据 | 5841 | 1 | 1460 | 7301 | 513 | | 7224 | 数据 | 7301 | 1 | 1460 | 8761 | 513 | | 7225 | 确认 | 1 | 8761 | 0 | 1 | 8212 | | 7226 | 数据 | 8761 | 1 | 1460 | 10221 | 513 | | 7227 | 数据 | 10221 | 1 | 1460 | 11681 | 513 | | 7228 | 确认 | 1 | 11681 | 0 | 1 | 8212 |  * + - 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？   （1）要确认捕获的报文已被确认，可以在Wireshark中查找以下标志：  序列号：检查报文的序列号。如果序列号被确认，将看到序列号大于已确认序列号的后续数据包。  确认号：检查ACK报文中的确认号。如果确认号与报文的序列号匹配，则表示该报文已被确认。  （2）窗口大小调整：  接收端的窗口大小最初被设置为一个值（例如2000字节），并在SYN分组中被通告给发送端。  当接收端处理传入数据时，它发送具有更新的窗口大小的ACK数据包，指示有多少缓冲空间可供发送端发送更多数据。  发送端根据接收端的窗口大小调整其发送速率，确保其不会溢出接收端的缓冲区。 | | | | | | | |
| 本人机位（图中标识） | | PC1 | | | 同组人（只填一人） | | |  |
| 本人主要工作 | | 配置PC1 | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |

计算机网络专题实验现场检查单5（共2页）

实验名称： RIP协议分析 时间：2024 年 5月 24日 早☑ 午□ 晚

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 |  | | 学号 |  | | 姓 名 |  | |
| E-Mail |  | | | | | 联系电话 |  | |
| 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） |  | | | | | | | |
| RIP协议配置与启动实验结果 | 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R1配置了接口e1/0的地址为10.1.4.2/24，设备现已处于端口路由模式。此初始化配置只允许R1与直接相连的网络通信，这意味着只有连接在网络10.1.4.0/24上的PC才能被ping通。因为VLAN3，VLAN2和VLAN7的其他网络并未配置在R1上，所以在VLAN7上的PCA和PCB，以及在VLAN2上的PCC和PCD均不能被R1 ping通。  2. 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。  R1配置了静态路由到10.1.7.0/24网络，因此，R1现在可以ping通在VLAN7上的PCA和PCB。然而，由于不涉及到VLAN2，R1仍然无法ping通位于该子网的PCC和PCD。  3. 步骤4之后。  （1） 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。  那些未配置在RIP中的网络导致该拓扑中的PC仍然是不可达的。例如，如果10.1.7.0/24网络被正确加入RIP，并且R1的相应接口也配置在RIP中，那么在VLAN7的PCA和PCB是能够ping通的。然而，如果VLAN2和VLAN3的相关网络没有加入RIP进程或端口配置不正确，那么R1就无法ping通在这些VLAN上的PCC和PCD。  （2） 查看路由填写下表。   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | 设备 | Destination/Mask | Protocol | Pref | Cost | Nexthop | Interface | | R1 | 10.1.3.0/24 | RIP | 100 | 1 | 10.1.4.1 | GE0/2 | | 10.1.4.0/24 | Direct | 0 | 0 | 10.1.4.2 | GE0/2 | | 10.1.5.0/24 | Direct | 0 | 0 | 10.1.5.2 | GE0/1 | | 10.1.7.0/24 | RIP | 100 | 1 | 10.1.4.1 | GE0/2 | | 127.0.0.0/8 | Direct | 0 | 0 | 127.0.0.1 | InLoop0 |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | S1 | 10.1.3.0/24 | Direct | 0 | 0 | 10.1.3.1 | Vlan3 | | 10.1.4.0/24 | Direct | 0 | 0 | 10.1.4.1 | Vlan4 | | 10.1.5.0/24 | RIP | 100 | 1 | 10.1.4.2 | Vlan4 | | 10.1.7.0/24 | Direct | 0 | 0 | 10.1.7.1 | Vlan7 | | 127.0.0.0/8 | Direct | 0 | 0 | 127.0.0.1 | InLoop0 | | | | | | | | |
| RIP协议分析结果 | * + - 1. 完成7.8节步骤4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，将应答报文之一的各字段值填入下表：  |  |  |  |  |  | | --- | --- | --- | --- | --- | | 观察点： | | 字段 | 值 | 含义 | | IP | | 目的地址 | 224.0.0.9 | 组播方式发送路由 | | UDP | | 端口号 | 520 | UDP传输的端口号为520 | | RIP | 头部 | 命令字段 | 2 | RIP应答报文 | | 版本号 | 2 | RIP请求报文为RIPv2报文 | | 路由信息 | 地址族标识 | 2 | 表示IP协议簇 | | 网络地址 | 10.1.2.0  10.1.3.0  10.1.4.0  10.1.5.0 | 该路由的目的IP地址 | | 跳数 | 2/1/1/2 | 请求报文路由开销 | | | | | | | | |
| 本人机位（图中标识） | | PCA | | | 同组人（只填一人） | | |  |
| 本人主要工作 | | 配置PCA | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |

计算机网络专题实验现场检查单6（共2页）

实验名称OSPF路由协议分析 时间：2024 年 5月24日 早□ 午☑ 晚□

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 |  | | 学号 |  | | 姓 名 |  | |
| E-Mail |  | | | | | 联系电话 |  | |
| 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。  6-1  Hello报文：用于发现和维持邻居关系。每个Hello报文包含了发送者的路由器ID、区域ID、Hello和Dead间隔等信息。路由器通过定期发送Hello报文来宣告自身的存在。  Database Description (DBD)报文：在邻居关系建立过程的交换阶段使用，主要用于在相邻路由器之间交换数据库摘要信息，这些摘要信息描述了发送者的完整路由状态数据库的内容。  Link State Request (LSR)报文：当路由器在DBD交换中发现自己缺少某些LSA信息，或者认为某些LSA信息已经过时时，会发送LSR报文来请求发送完整的LSA信息。  Link State Update (LSU)报文：这种报文用于响应LSR报文，包含了被请求的一个或多个完整LSA记录。这允许路由器将自己的数据库更新为最新状态。  Link State Acknowledgment (LSAck)报文：用于确认收到LSU报文。  OSPF邻居建立过程包括：发送Hello报文以建立邻居关系，通过DBD交换了解彼此数据库摘要，通过LSR、LSU和LSAck报文进行数据库的详细交换和确认，最后达到Full邻居状态，这表示两个OSPF路由器间的数据库完全同步。  2. 说明路由器R1、R2中产生的OSPF路由表项的含义？  6-2  路由器R1和R2中产生的OSPF路由表项记录了通过OSPF协议学习到的网络路径信息：  目的网络地址：这是要发送到的网络或子网的IP地址。在OSPF环境中，这些地址是通过OSPF协议的交互动态学习到的。  子网掩码：与目的地址相对应的子网掩码，用于确定网络的大小和边界。  成本（Cost）：代表达到目的网络的路径成本，这是根据链路状态信息和算法（如Dijkstra算法）计算出的路径成本，反映了路径的质量。成本越低，表明该路径越优选。  下一跳地址：数据包在到达最终目的地之前，应发送到的下一个路由器或设备的IP地址。  出口接口：本地路由器上用于发送往目的网络数据包的物理或逻辑接口。这是确定数据包离开本地路由器，前往下一跳地址时应使用的接口。  路由类型：指明该条路由是如何获得的  3. 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。  6-3  Router-LSA包含了生成它的路由器的最新链路状态信息，也就是该路由器的接口和它们的状态以及与这些接口邻接的路由器的详细信息。Router-LSA的各个字段如下：  LS Age：该LSA自从上次刷新或者创建开始经过的时间。  Options：表示路由器的某些能力，如是否支持某些OSPF扩展。  LS Type：表示LSA的类型，在Router-LSA中，该值为1。  Link State ID：在Router-LSA中，此字段通常是生成LSA的路由器的ID。  Advertising Router：生成此LSA的路由器的ID。  LS Sequence Number：用来检测更新，这个序号每产生一个新的LSA就会递增。  LS Checksum：用于检查LSA内容在传输过程中是否被改变。  Length：整个LSA消息的长度。 | | | | | | | |
|  |
| 本人机位（图中标识） | | PCA | | | 同组人（只填一人） | | |  | |
| 本人主要工作 | | 配置PCA | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |

计算机网络专题实验现场检查单7（共1页）

实验名称：防火墙与SSLVPN实验 时间： 2024 年5 月 17 日 早□ 午☑ 晚□

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 |  | | 学号 |  | | 姓 名 |  | |
| E-Mail |  | | | | | 联系电话 |  | |
| 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. 创建的SSL VPN用户名是：user1 2. 分析完成捕获的报文，分析两台PC上报文的差别。   配置SSL VPN后，内网PC直接访问Web服务器的报文通常未加密，而外网PC通过VPN访问的报文是加密的，使用TLS v1.2协议，只有VPN服务器和客户端可以解密。内网访问显示直接的IP地址，外网访问则显示外网PC和VPN服务器的IP，真实目标IP被隐藏。SSL VPN提供加密隧道和用户认证，大大提高了通过不安全网络访问内网资源的安全性。 | | | | | | | |
| 本人机位（图中标识） | | ServerA | | | 同组人（只填一人） | | |  |
| 本人主要工作 | | 配置ServerA | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |