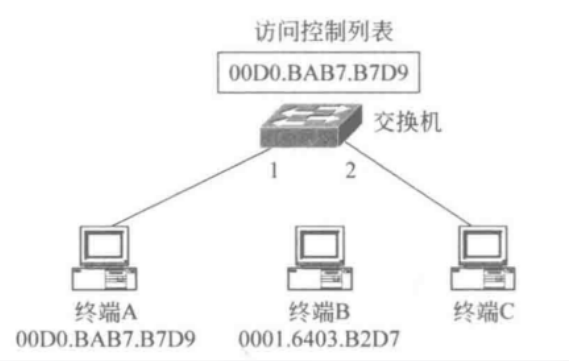

2024
计算机与网络安全综合实验
时间：2024年

本次实验任务——以太网安全实验

- 访问控制列表实验
- 安全端口实验
- 防DHCP欺骗攻击实验

访问控制列表实验



- 实验内容
- 交换机端口1的访问控制列表中静态配置终端A的MAC地址，交换机其它端口不启动安全功能，将终端C接入交换机端口2。
- 主要操作
  - 先将终端A接入交换机端口1，实现终端A与终端C之间的数据传输过程；
  - 再将终端B接入交换机端口1，进行终端B和终端C之间的数据传输过程，发现交换机端口1自动关闭。
  - 重新开启交换机端口1，再将终端A接入交换机端口1，实现终端A和终端C之间的数据传输过程。

访问控制列表实验

- 实验目的
  - 验证交换机端口静态配置访问控制列表的过程。
  - 验证访问控制列表控制终端接入的过程。
  - 验证关闭端口的重新开启过程。

访问控制列表

- 实验原理
  - 交换机端口1的访问控制列表中静态配置了终端A的MAC地址，因此当终端A接入交换机端口1且向交换机端口1发送MAC帧时，MAC帧的源MAC地址与访问控制列表中的MAC地址相同，交换机继续转发该MAC帧。
  - 当终端B接入交换机端口1且向交换机端口1发送MAC帧时，由于MAC帧的源MAC地址与访问控制列表中的MAC地址不同，因此交换机丢弃该MAC帧，并关闭交换机端口1。
  - 需要通过特殊的命令序列才能重新开启交换机端口1。

安全端口实验

- 将交换机端口1设置为安全端口，自动将先学习到的两个MAC地址添加到访问控制列表中。交换机其它端口不启动安全功能，将终端D接入交换机端口2。

安全端口实验

- 主要过程
  - 先将终端A的MAC地址接入交换机端口1，实现终端A和终端D之间的数据传输过程，此时终端A的MAC地址自动添加到访问控制列表中；
  - 然后将终端B接入交换机端口1，实现终端B和终端D之间的数据传输过程，此时终端B的MAC地址自动添加到访问控制列表中；
  - 再将终端C接入交换机端口1，进行终端C和终端D之间的数据传输过程，由于该MAC帧的源MAC地址不在访问控制列表中，且访问控制列表中的MAC地址数已经达到了最大MAC地址数2，交换机丢弃该MAC帧。

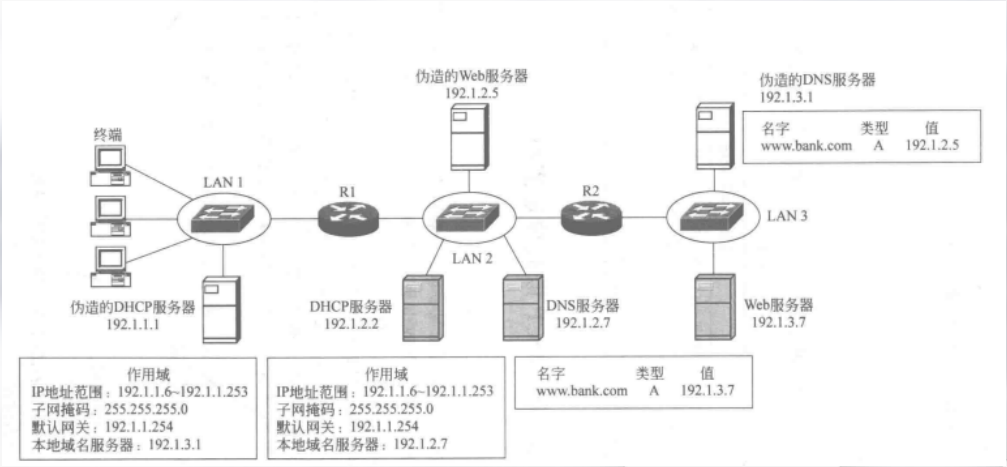
安全端口实验

- 实验目的
  - 验证交换机端口安全功能配置过程。
  - 验证访问控制列表自动添加MAC地址的过程。
  - 验证对违规接入终端采取的各种动作的含义。
  - 验证安全端口方式下的终端接入控制过程。

防DHCP欺骗攻击实验

– 如图所示是黑客实施钓鱼网站的常见手段。

- 黑客通过在网络中接入伪造的DHCP服务器、伪造的DNS服务器和伪造的Web服务器，使用户用正确的完全合格的域名www. bank.com访问黑客伪造的Web服务器。

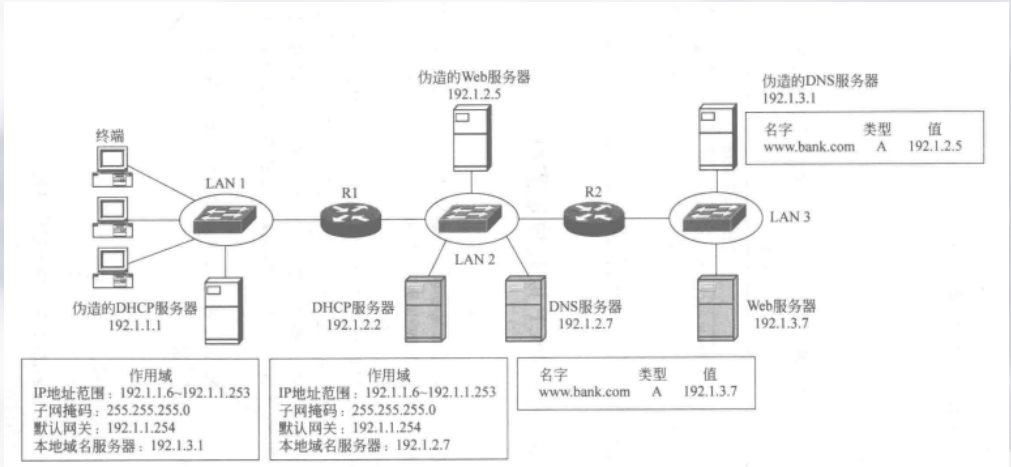


防DHCP欺骗攻击实验

钓鱼网站实施过程中，使用户用正确的完全合格的域名www.bank.com访问黑客伪造的Web服务器的关键是：

终端从伪造的DHCP服务器中获取网络信息。通过接入伪造的DHCP服务器使终端从伪造的DHCP服务器中获取网络信息的过程称为DHCP欺骗攻击。

因此，成功实施DHCP欺骗攻击是成功实施如图所示的钓鱼网站的基础。



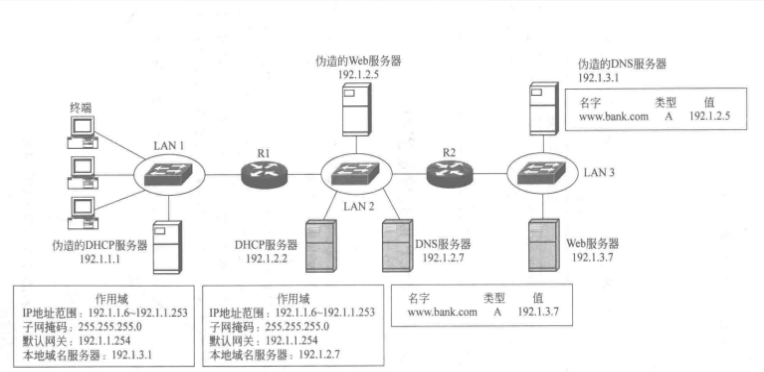
防DHCP欺骗攻击实验

- 在交换机中启动防DHCP欺骗攻击功能，在接入伪造的DHCP服务器的情况下，保证终端只从DHCP服务器获取网络信息。

防DHCP欺骗攻击实验

- 实验目的
  - 验证DHCP服务器配置过程。
  - 验证DNS服务器配置过程。
  - 验证终端用完全合格的域名访问Web服务器的过程。
  - 验证DHCP欺骗攻击过程。
  - 验证钓鱼网站实施过程。
  - 验证交换机防DHCP欺骗攻击功能的配置过程。

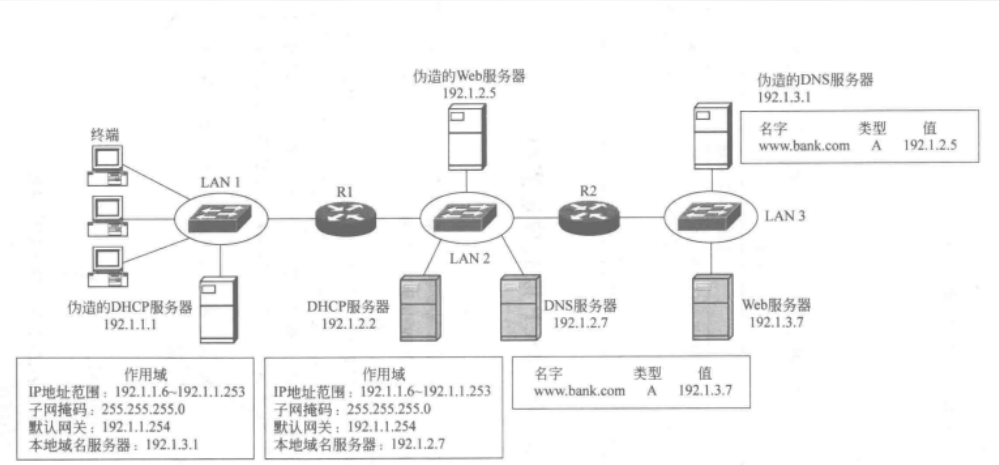
防DHCP欺骗攻击实验



- 终端通过DHCP自动获取的网络信息中包含本地域名服务器地址。
- 对于如图所示的网络应用系统，DHCP服务器中给出的本地域名服务器地址是192.1.2.7，地址为192.1.2.7的域名服务器中与完全合格的域名 www.bank.com绑定的Web服务器地址是192.1.3.7。因此，终端可以用完全合格的域名www.bank.com 访问Web服务器。

防DHCP欺骗攻击实验

- 一旦终端连接的网络中接入伪造的DHCP服务器，终端很可能从伪造的DHCP服务器获取网络信息，得到伪造的域名服务器的IP地址192.1.3.1，伪造的域名服务器中将完全合格的域名www.bank.com与伪造的Web服务器的IP地址192.1.2.5绑定在一起，导致终端用完全合格的域名www.bank.com访问伪造的 Web服务器。



防DHCP欺骗攻击实验

- 如果交换机启动防DHCP欺骗攻击的功能，只有连接在信任端口的DHCP服务器才能为终端提供自动配置网络信息的服务。
- 因此，对于如图所示的实施DHCP欺骗攻击的网络应用系统，连接终端的以太网中，如果只将连接路由器R1的交换机端口设置为信任端口，将其他交换机端口设置为非信任端口，则终端只能接收由路由器R1转发的DHCP消息，使终端只能获取DHCP服务器提供的网络信息。