第3讲
以太网安全技术

一、以太网交换机安全功能

消除与以太网相关的安全威胁应该从弥补协议缺陷和增强交换机安全功能两方面着手。

1）弥补协议缺陷是提出相应的安全协议。

2）增强交换机安全功能是通过在交换机中集成安全技术，使得以这样的交换机为核心设备构建的以太网具有抵御MAC表溢出、MAC地址欺骗、DHCP欺骗、ARP欺骗和生成树欺骗等攻击行为的安全功能。

一、以太网交换机安全功能

请大家讨论以下攻击原理及解决思路：

- MAC表溢出
- MAC地址欺骗
- DHCP欺骗
- ARP欺骗
- 生成树欺骗

一、以太网交换机安全功能

1. MAC表溢出攻击的解决思路

解决思路是限制每一个端口允许接收的源MAC地址不同的MAC帧的数量。

2. MAC地址欺骗攻击的解决思路

解决思路是由管理员确定每一个交换机端口连接的终端的MAC地址，每一个交换机端口只允许接收源MAC地址是该端口连接的终端的合法MAC地址的MAC帧。

一、以太网交换机安全功能

3．DHCP欺骗攻击的解决思路

解决思路是由管理员确定允许接收DHCP响应消息的交换机端口，交换机丢弃所有从其他端口接收到的DHCP响应消息。

4．ARP欺骗攻击的解决思路

解决思路是交换机中建立正确的MAC地址与IP地址之间的绑定关系，交换机能够检测ARP请求报文或响应报文中指定的MAC地址与IP地址之间绑定关系的正确性，丢弃所有指定错误的MAC地址与IP地址之间绑定关系的ARP请求报文或响应报文。

一、以太网交换机安全功能

5. 生成树欺骗攻击

解决思路是由管理员确定参与生成树建立过程的交换机端口，其他交换机端口一律丢弃接收到的BPDU。

二、以太网接入控制技术

1. 终端或用户标识符

交换机需要鉴别接入交换机端口的终端的身份，只允许授权接入以太网的终端通过该终端连接的交换机端口实现与连接在同一以太网上的其他终端或路由器之间的MAC帧传输过程。

用MAC地址作为终端身份标识信息。

用用户名和口令作为用户身份标识信息。

二、以太网接入控制技术

2．身份鉴别过程——访问控制列表

对于只允许授权终端接入以太网的接入控制过程，交换机需要建立访问控制列表，访问控制列表中给出允许接入以太网的终端的MAC地址。当交换机接收到MAC帧，当且仅当发送MAC帧的终端的MAC地址在访问控制列表中时，交换机才继续转发该MAC帧。否则，交换机将丢弃该MAC帧。

二、以太网接入控制技术

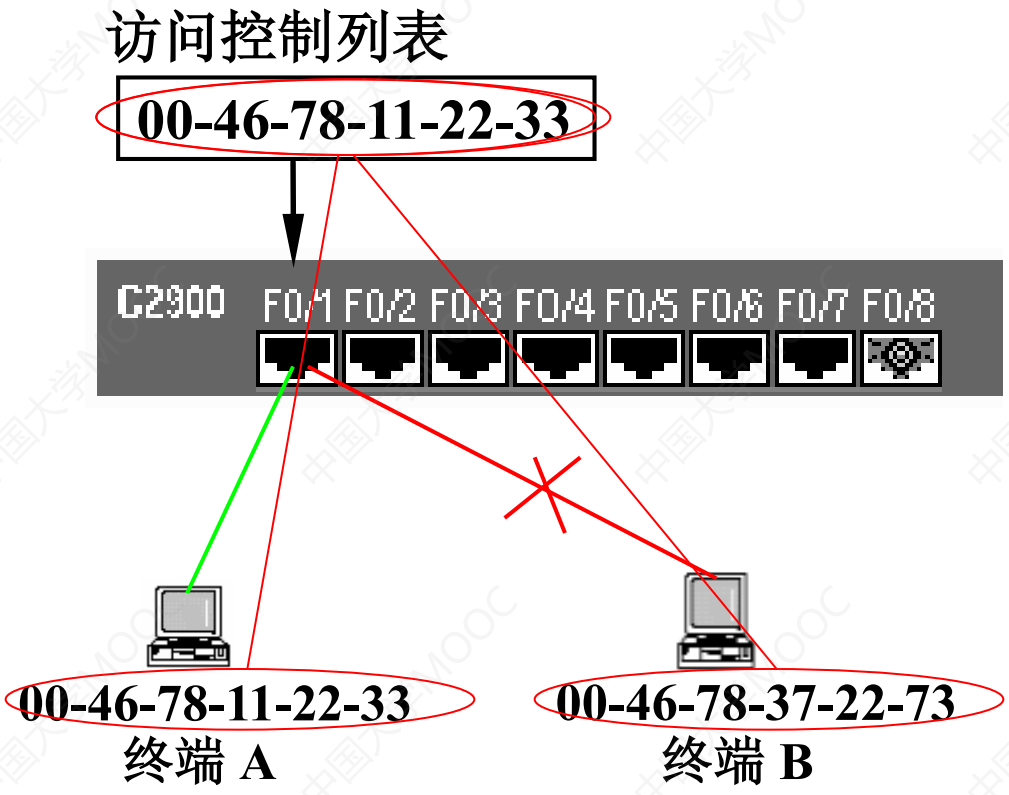
2．身份鉴别过程——访问控制列表

讨论访问控制列表配置方式：

1）静态

2）动态

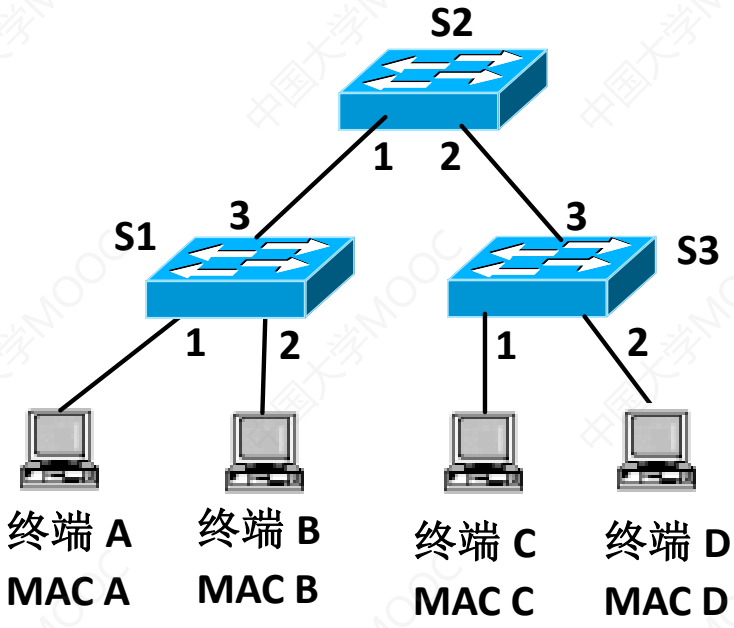
静态配置访问控制列表



访问控制列表

- 允许为交换机每一个端口配置访问控制列表，列表中给出允许接入的终端的MAC地址；
- 配置访问控制列表的端口只允许转发源MAC地址属于列表中MAC地址的MAC帧，因此对于接入端口，只允许物理连接MAC地址属于列表中MAC地址的终端。

静态配置访问控制列表



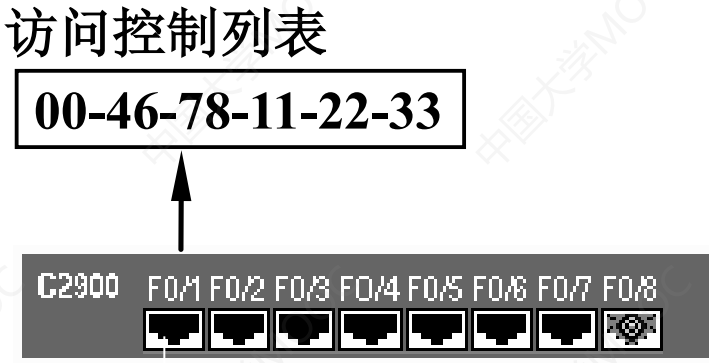
S1.1 访问控制列表	S1.2 访问控制列表	S3.1 访问控制列表	S3.2 访问控制列表
MAC A	MAC B	MAC C	MAC D

S1.3 访问控制列表	S2.1 访问控制列表	S2.2 访问控制列表	S3.3 访问控制列表
MAC C MAC D	MAC A MAC B	MAC C MAC D	MAC A MAC B

以太网有着如下安全要求：

- 保持如图所示的终端A、终端B、终端C和终端D与交换机端口之间的连接方式不变；
- 只允许终端A、终端B、终端C和终端D之间相互通信；
- 禁止其他终端接入以太网。

安全端口



- 安全端口是自动建立访问控制列表的机制；
- 允许为每一个交换机端口设置MAC地址数N，从端口学习到的前N个MAC地址作为访问控制列表的MAC地址；
- 不允许转发源地址是N个地址以外的MAC帧。

二、以太网接入控制技术

2. 身份鉴别过程——用户信息列表

对于只允许授权用户通过连接在以太网上的任意终端访问网络的接入控制过程，交换机需要建立授权用户信息列表，授权用户信息列表中给出授权用户的用户名和口令。用户访问网络前，必须提供用户身份标识信息，只允许用户身份标识信息在授权用户信息列表中的用户通过以太网访问网络。

控制用户访问网络过程通常与控制终端接入以太网过程相结合，交换机需要通过用户身份鉴别过程建立授权用户与终端MAC地址之间的绑定关系。

二、以太网接入控制技术

2．身份鉴别过程——用户信息列表

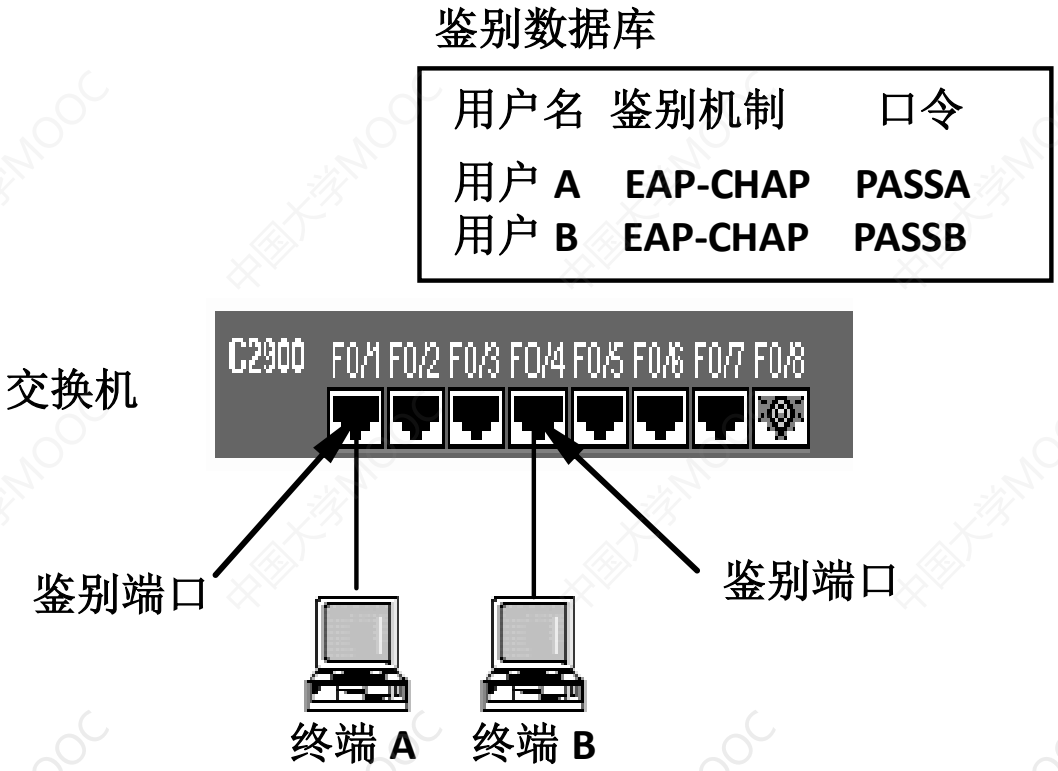
讨论访问用户信息列表配置方式：

1）本地

2）统一

802.1X接入控制过程

1．本地鉴别过程



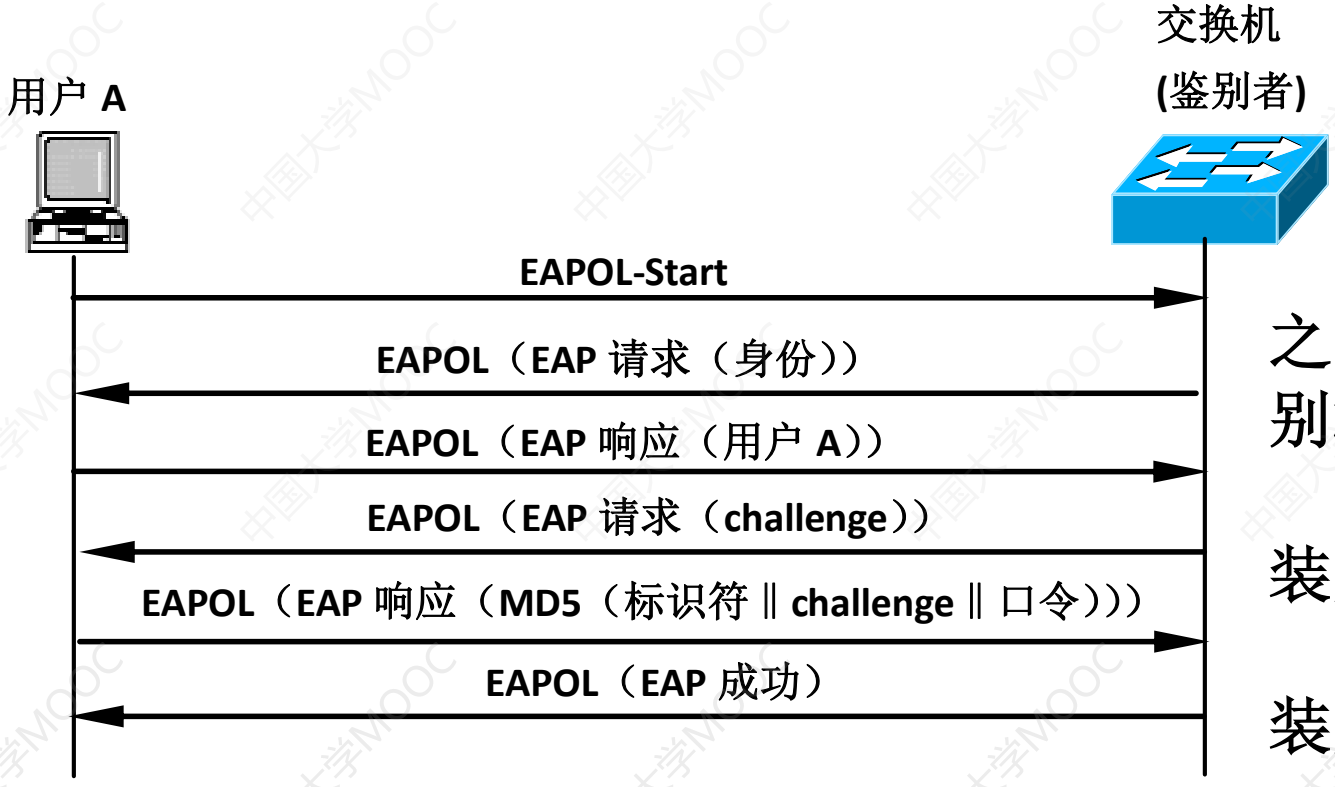
在终端连接的交换机中建立鉴别数据库，鉴别数据库中给出授权用户身份标识信息和鉴别机制。

802. 1X接入控制过程

1. 本地鉴别过程

鉴别数据库

用户名	鉴别机制	口令
用户 A	EAP-CHAP	PASSA
用户 B	EAP-CHAP	PASSB



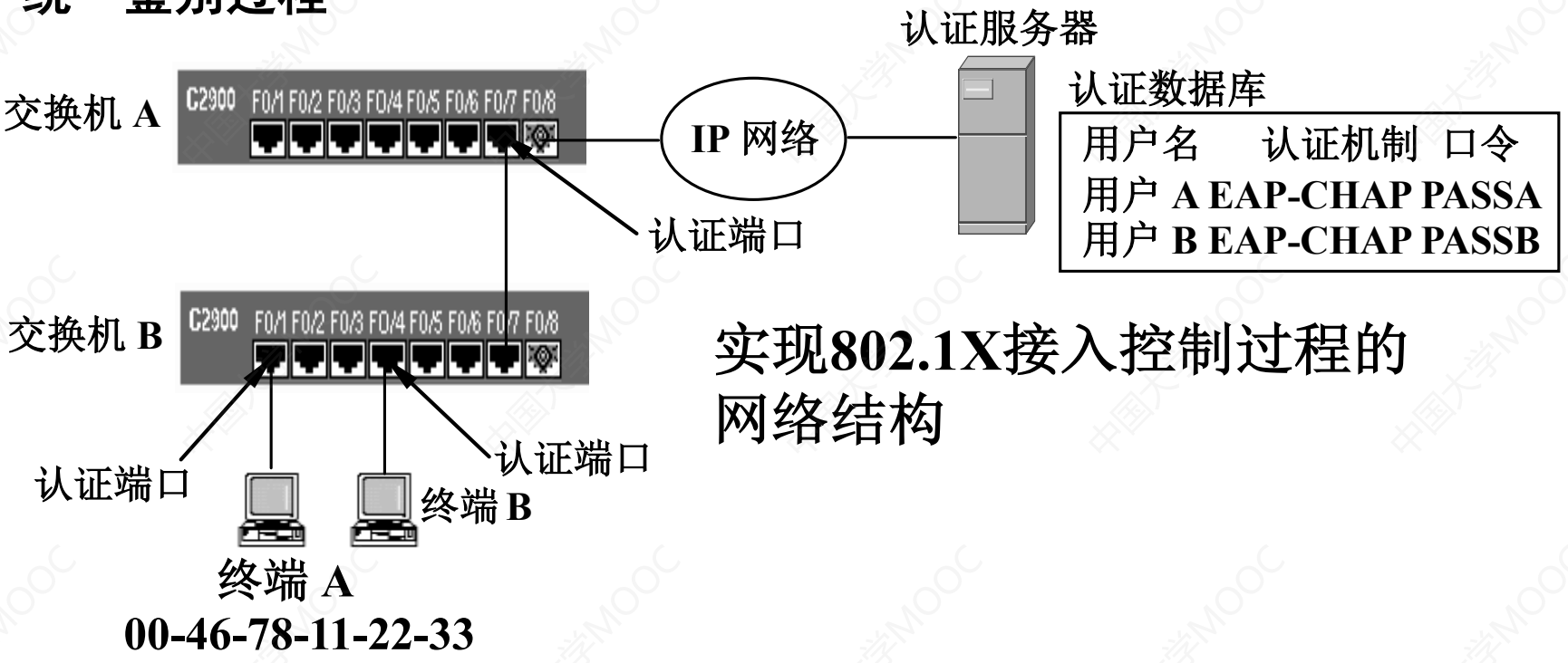
终端和交换机之间采用CHAP鉴别机制；

鉴别信息封装成EAP报文；

EAP报文封装成以太网帧。

802.1X接入控制过程

2. 统一鉴别过程

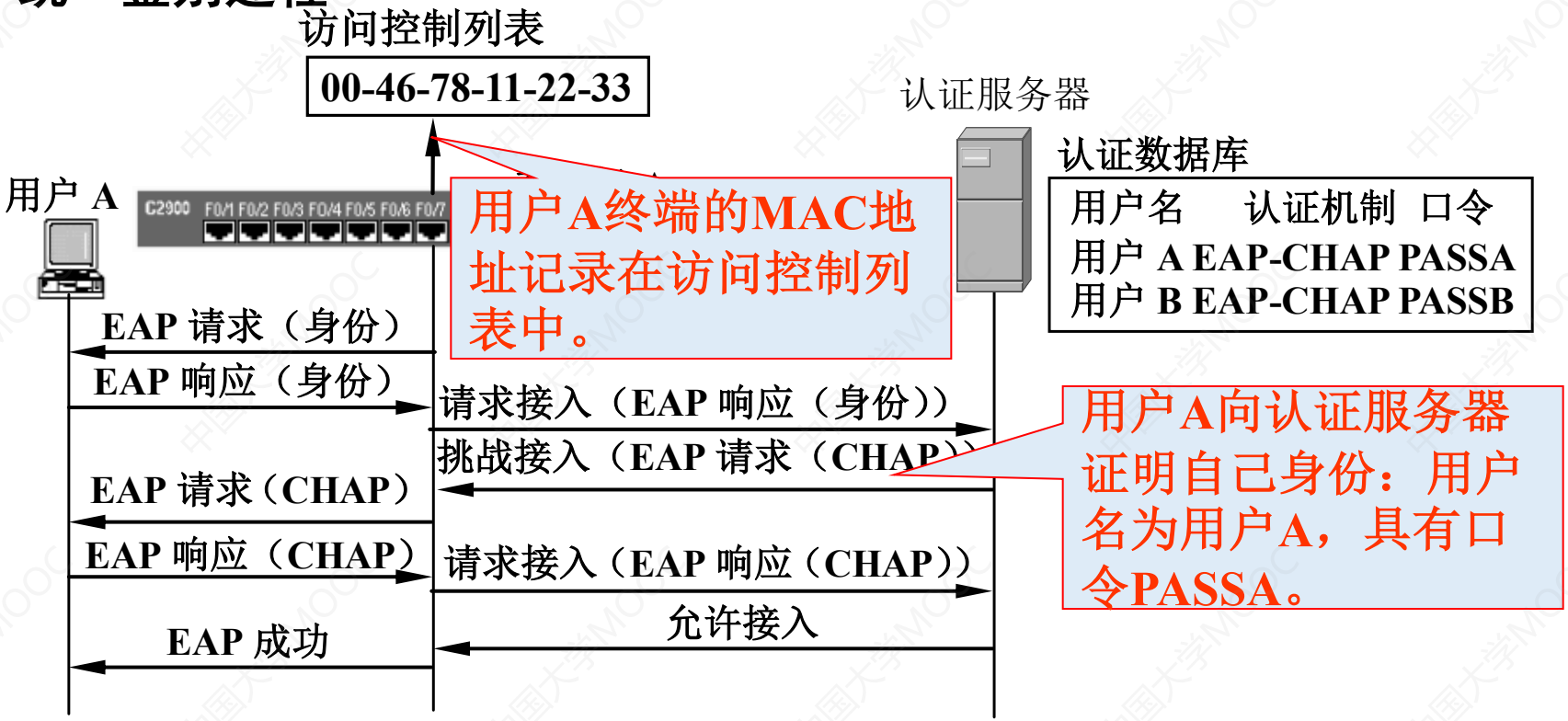


实现802.1X接入控制过程的网络结构

- 802.1X基于端口认证机制，一旦完成认证过程，端口就处于正常转发状态，这种方式适用于交换机B的认证端口，不适用交换机A的认证端口；
- 802.1X基于MAC地址认证机制是认证和访问控制列表的有机结合，一旦交换机通过对某个用户的身份认证，将该用户终端的MAC地址记录在访问控制列表的中，这种方式下，访问控制列表的中的MAC地址是动态的，随着用户接入增加，随着用户退出减少。

802.1X接入控制过程

2. 统一鉴别过程



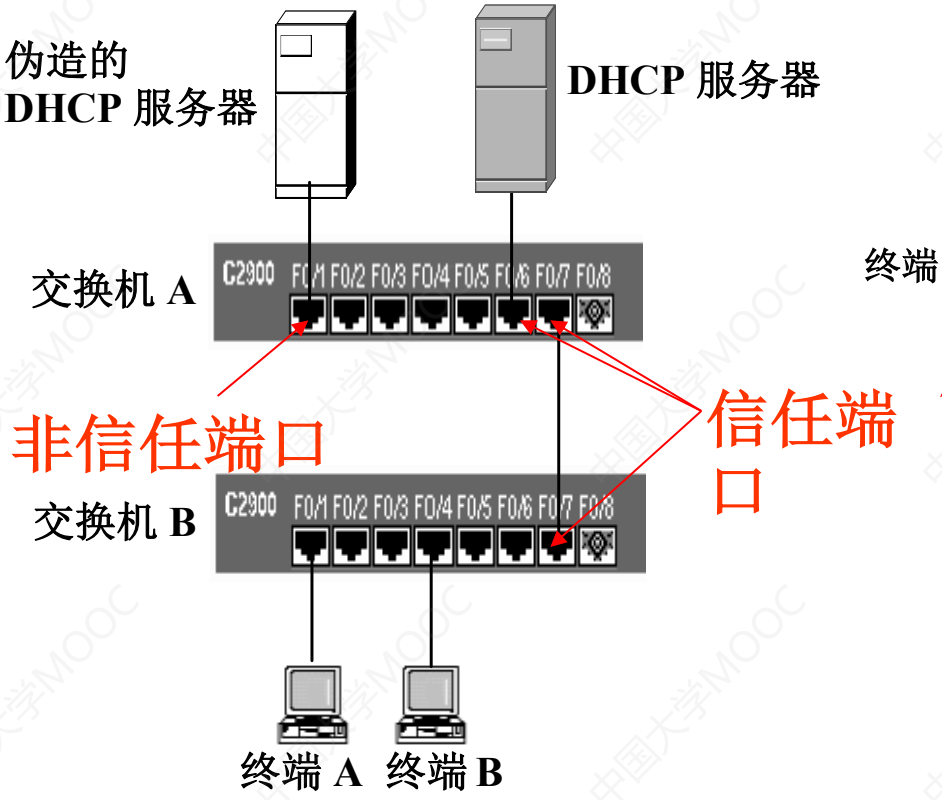
- 认证数据库表明：允许用户名为用户A，具有口令PASSA的用户接入以太网；
- 交换机A将端口7设置为认证端口，意味着必须根据认证数据库指定的认证机制：EAP-CHAP完成用户身份认证的用户终端的MAC地址才能记录在端口7的访问控制列表的中。

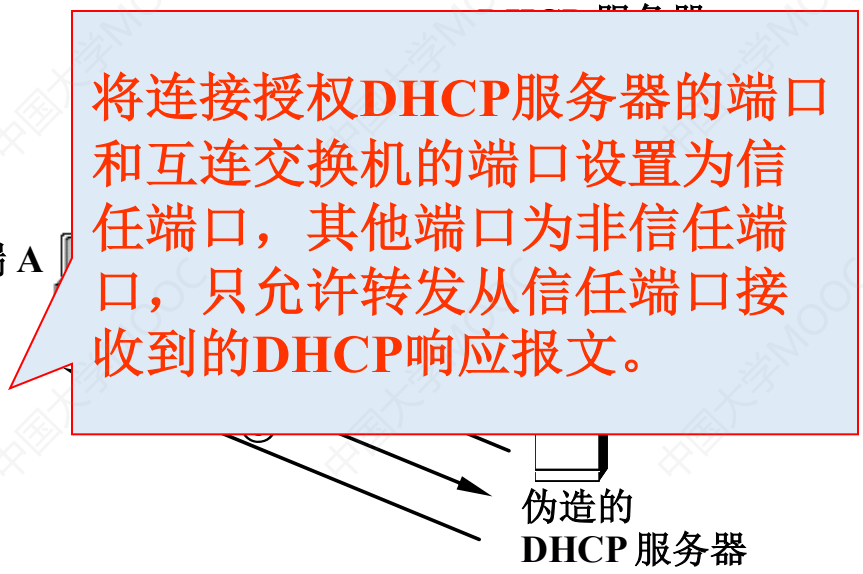
以太网接入控制过程可以解决以下问题：

一是由于每一个交换机端口只允许接收源MAC地址是访问控制列表中的MAC地址的MAC帧，限制了交换机接收到的源MAC地址不同的MAC帧的数量，防止交换机发生转发表（MAC表）溢出的情况，有效地防御了MAC表溢出攻击。

二是由于可以指定连接到每一个交换机端口的终端的MAC地址，因此，可以有效防御通过修改终端的MAC地址实施的MAC地址欺骗攻击。

信任端口与非信任端口

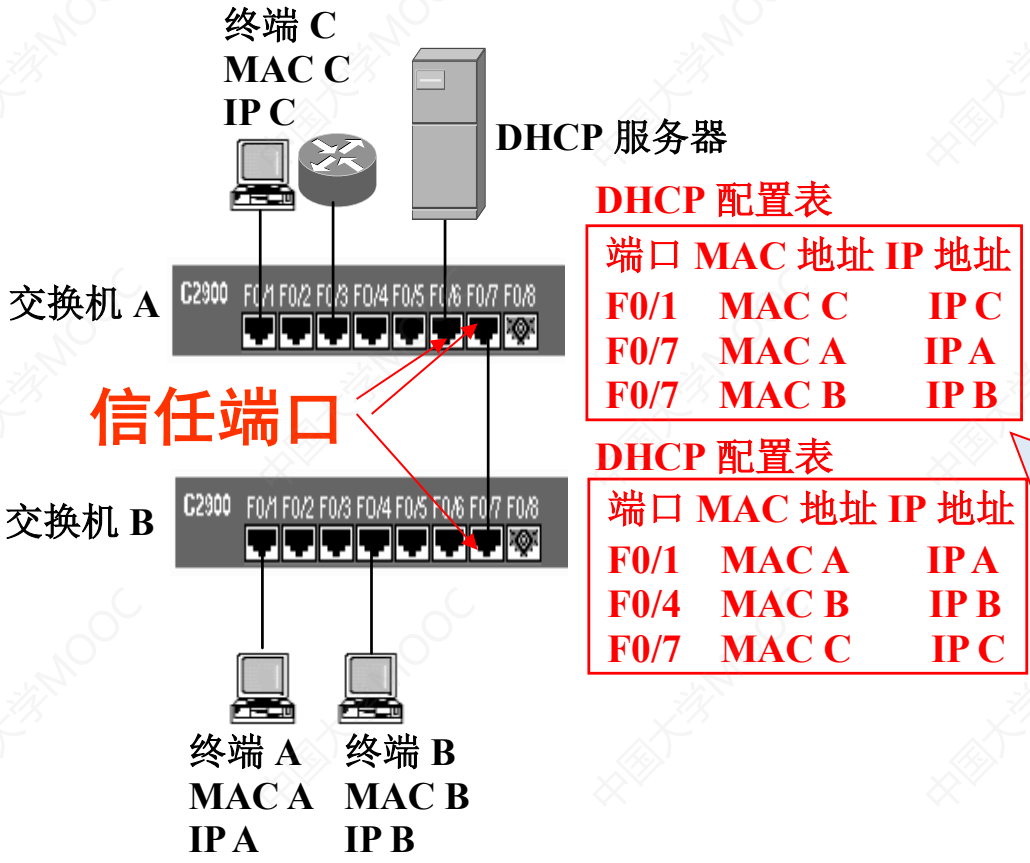




①：终端 A 发送的发现报文
②：伪造的 DHCP 服务器发送的应答报文
③：DHCP 服务器发送的应答报文
④：终端 A 发送的请求报文
⑤：伪造的 DHCP 服务器发送的确认报文

伪造的DHCP服务器为终端配置错误的网络信息，导致终端发送的数据都被转发到冒充默认网关的黑客终端。

DHCP侦听信息库



DHCP 配置表

端口	MAC 地址	IP 地址
F0/1	MAC C	IP C
F0/7	MAC A	IP A
F0/7	MAC B	IP B

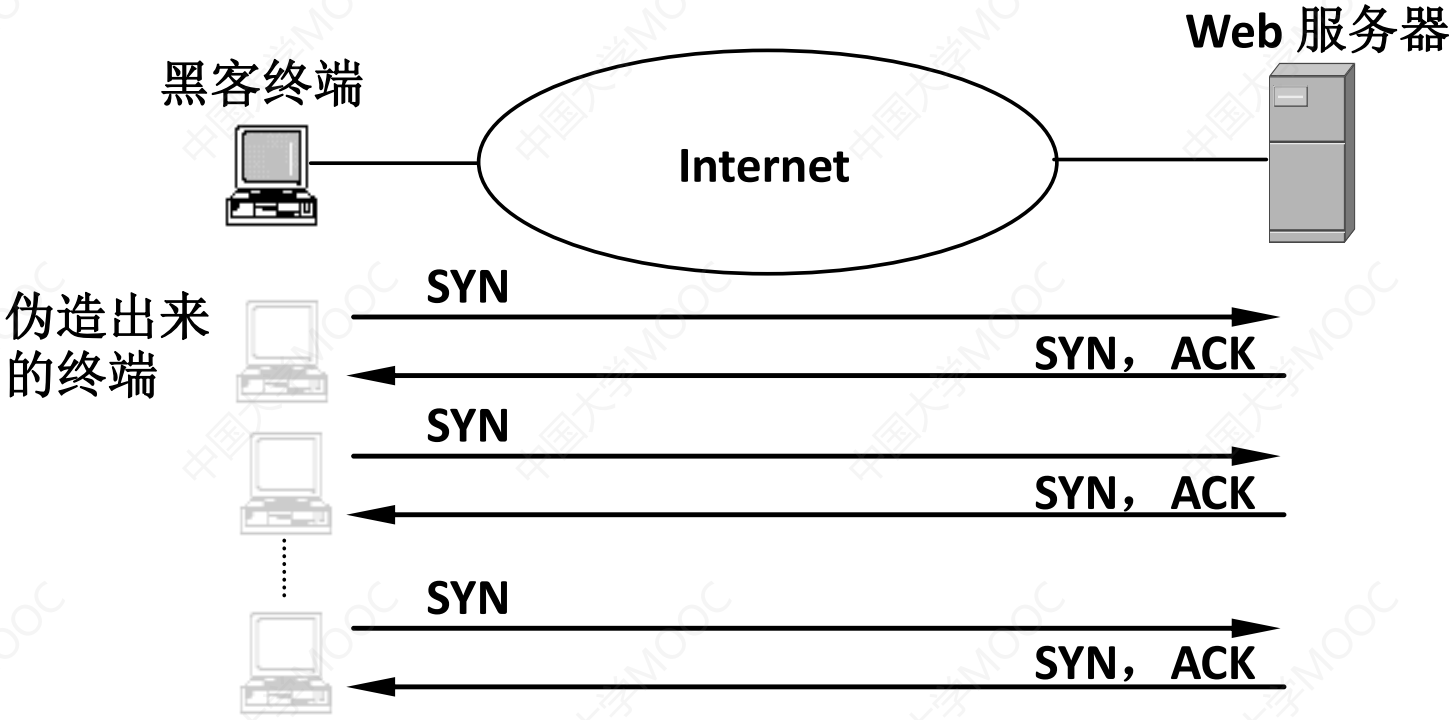
DHCP 配置表

端口	MAC 地址	IP 地址
F0/1	MAC A	IP A
F0/4	MAC B	IP B
F0/7	MAC C	IP C

解决方法基于终端配置通过DHCP服务器获得；
交换机侦听通过信任端口接收到的DHCP响应报文，并将响应报文中作为终端标识符的MAC地址和DHCP分配给终端的IP地址记录在DHCP配置表中；
一旦交换机接收到ARP报文，根据ARP报文中给出的IP地址和MAC地址对匹配DHCP配置表，如果找到匹配项，继续转发ARP报文，否则，丢弃ARP报文。

ARP欺骗攻击过程

终端B通过发送将终端A的IP地址和自己MAC地址绑定的ARP报文，在其他终端和路由器的ARP缓冲器中增添一项<IP A MAC B>，导致其他终端和路由器将目的IP地址为IP A的IP分组，全部封装成以MAC B为目的地址的MAC帧。



当交换机通过非信任端口接收到某个IP分组，用该IP分组的源IP地址和封装该IP分组的MAC帧的源MAC地址匹配交换机的DHCP侦听信息库，如果在侦听信息库中找不到与该MAC地址和IP地址对匹配的项，断定该IP地址是伪造的，交换机丢弃该IP分组。

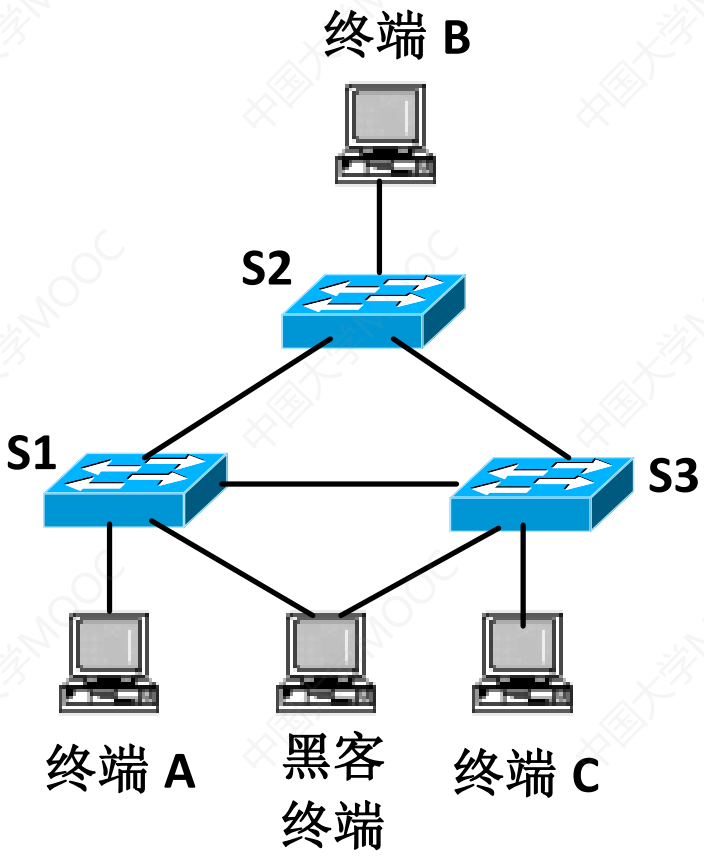
SYN泛洪攻击——针对服务器的DoS攻击

SYN泛洪攻击防御机制

实施SYN泛洪攻击的前提是伪造源IP地址，因此，最直接的防御SYN泛洪攻击的办法是，使网络具有阻止伪造源IP地址的IP分组继续传输的功能。

SYN泛洪攻击导致大量处于未完成状态的TCP连接，如果会话表只对处于完成状态的TCP连接分配连接项，SYN泛洪攻击将无法耗尽会话表中的连接项。

实施生成树欺骗攻击的条件



实施如图所示的生成树欺骗攻击过程需要满足以下两个条件:

1）交换机S1和交换机S3连接黑客终端的端口能够接收、处理和转发黑客终端发送的BPDU。

2）将黑客终端配置成优先级最高的交换机，以此生成BPDU，并将BPDU发送交换机S1和S3。

四、生成树欺骗攻击与防御机制

交换机中有两类端口，一类是实现交换机之间互连的端口，称为主干端口。另一类是直接连接终端的端口，称为接入端口。

交换机中的接入端口是不需要参与构建生成树过程的。因此，可以将交换机接入端口设置成不运行生成树协议的端口。一旦某个交换机端口不运行生成树协议，该端口不会发送、接收BPDU。

生成树欺骗攻击

生成树欺骗攻击防御机制

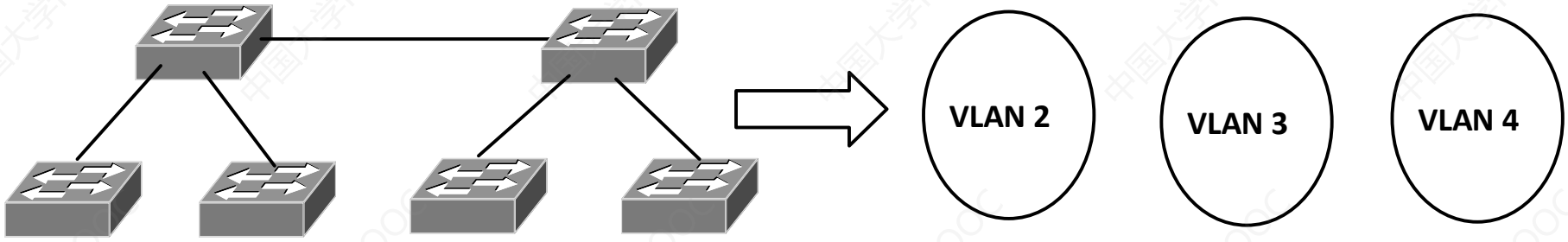
防御生成树欺骗攻击的前提是，不允许黑客终端参与网络生成树建立过程，即只在用于实现两个认证交换机之间互连的交换机端口启动生成树协议。

五、虚拟局域网

本讲主要内容

- 虚拟局域网降低攻击危害；
- 虚拟局域网安全应用实例。

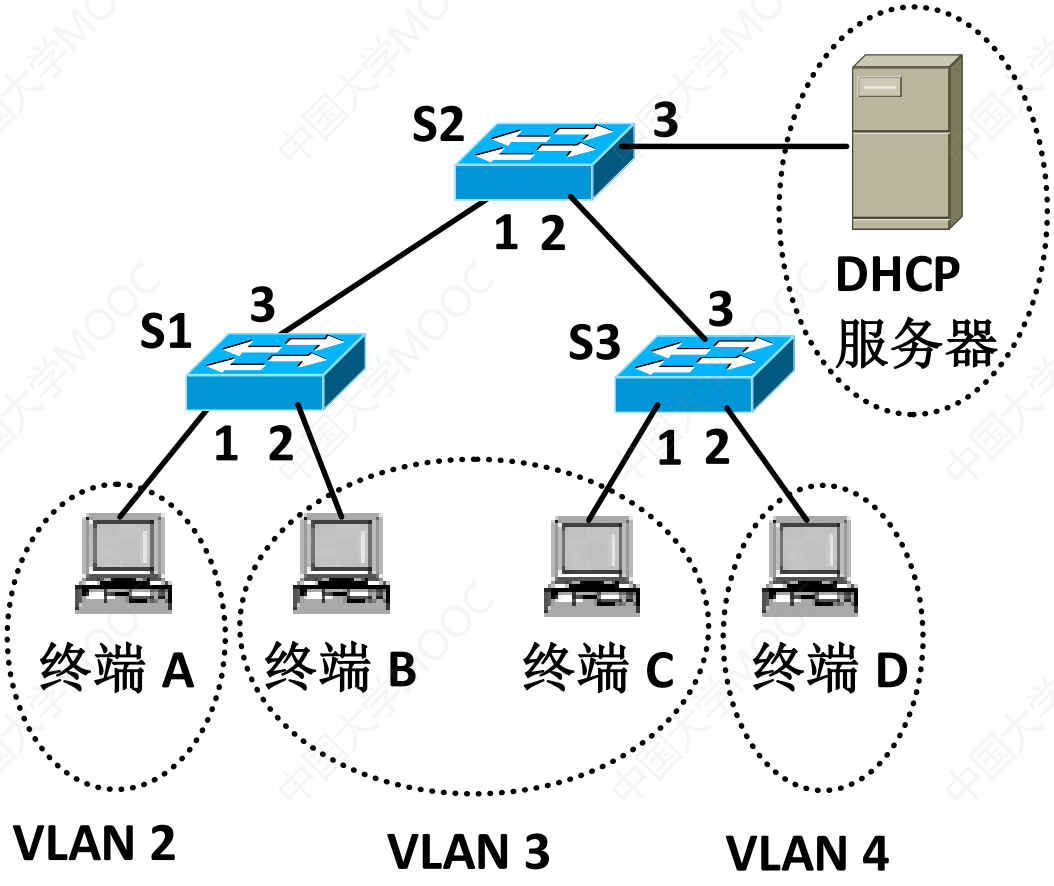
五、虚拟局域网



1. 虚拟局域网特性

虚拟局域网技术可以将一个物理以太网划分为多个逻辑上完全独立的虚拟局域网（VLAN），所有的广播帧只能在同一个VLAN内广播，无法扩散到其他的VLAN。

五、虚拟局域网



如果不划分VLAN，整个物理以太网属于同一个广播域， MAC表溢出攻击、MAC地址欺骗攻击、DHCP欺骗攻击、ARP欺骗攻击和生成树欺骗攻击等都是针对如图所示的物理以太网展开。

五、虚拟局域网

2. 虚拟局域网可以降低的危害

- 降低ARP欺骗攻击危害；
- 降低DHCP欺骗攻击危害；
- 降低MAC地址欺骗攻击危害；
- 降低MAC表溢出攻击危害；
- 降低生成树欺骗攻击危害。

五、虚拟局域网

VLAN划分增强以下安全性：

- 缩小广播域；
- 控制黑客终端接入某个VLAN；
- 控制VLAN间通信过程。