第2讲
网络攻击（下）

高梦州

内容安排

1. 网络攻击的定义与分类
2. 嗅探攻击
3. 截获攻击
4. 拒绝服务攻击
5. 欺骗攻击
6. 非法接入和登录
7. 小结

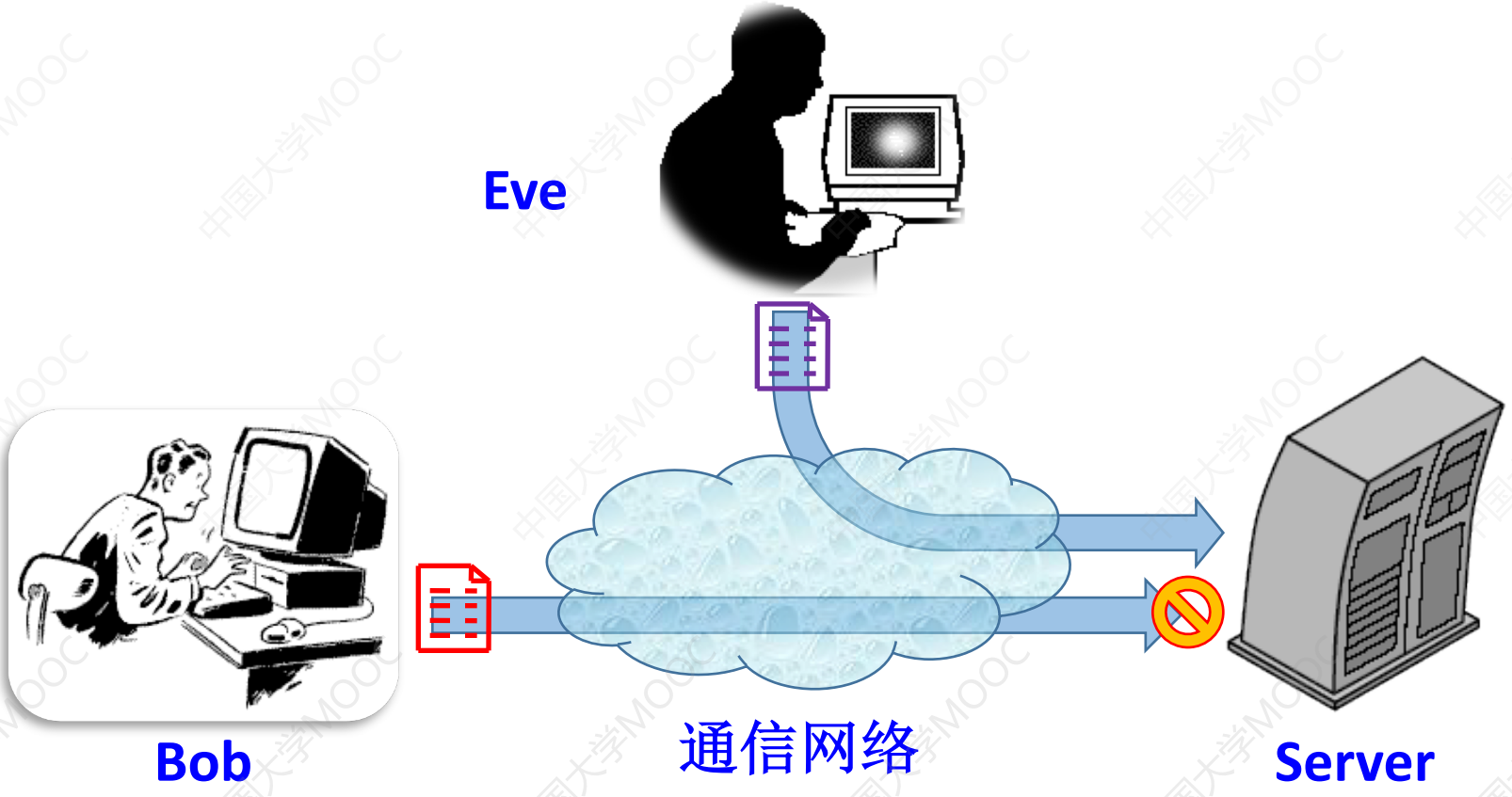
4 拒绝服务攻击

本部分主要内容

- SYN泛洪攻击；
- Smurf攻击；
- DDOS。

4 拒绝服务攻击

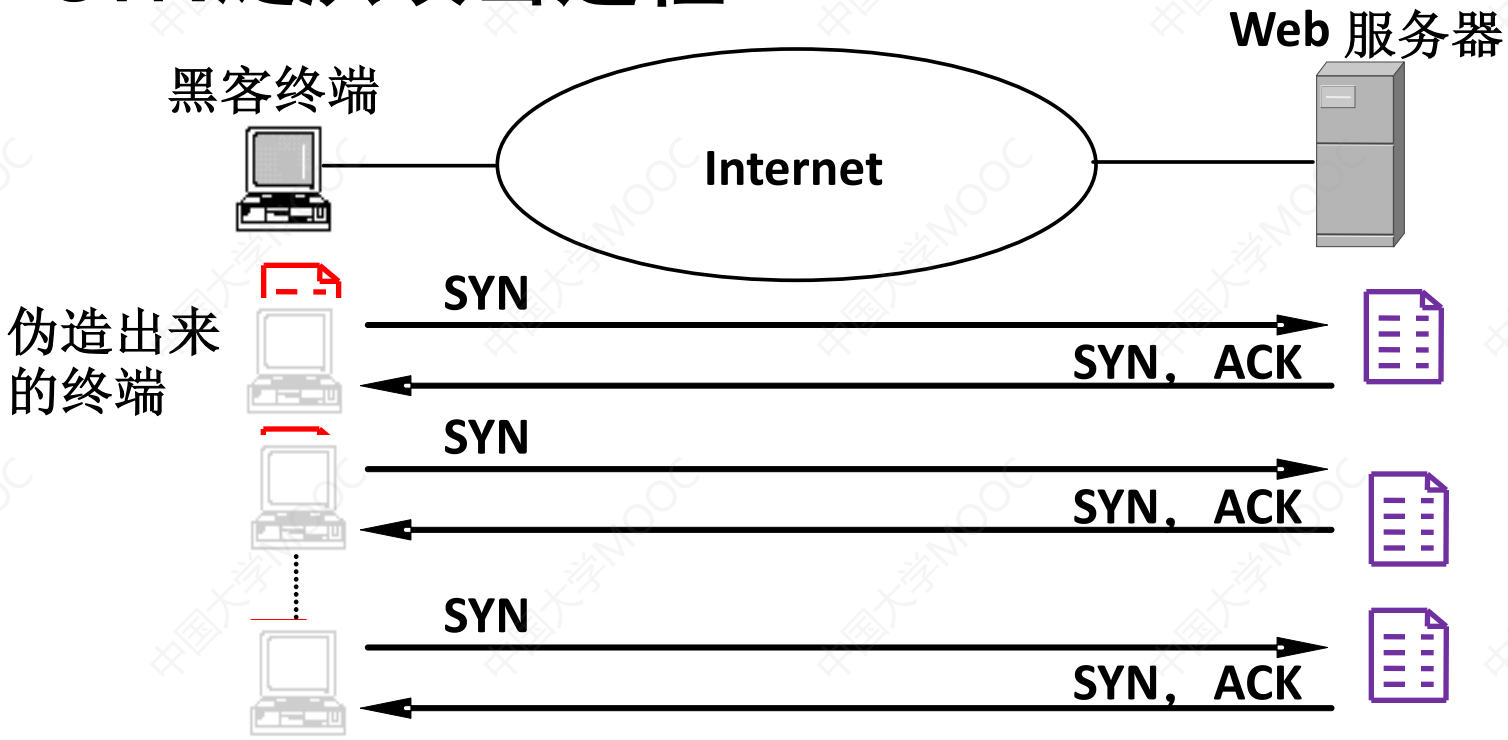
拒绝服务攻击（Denial of Service, DoS）攻击就是用某种方法耗尽网络设备、链路或服务器资源，使其不能正常提供服务的一种攻击手段。



4 拒绝服务攻击

4.1 SYN泛洪攻击——针对服务器的DoS攻击

- SYN泛洪攻击过程



通过大量未完成的TCP连接，快速耗尽Web服务器的会话表资源，使得正常的TCP连接无法建立。

4 拒绝服务攻击

4.1 SYN泛洪攻击——针对服务器的DoS攻击

- SYN泛洪攻击防御机制

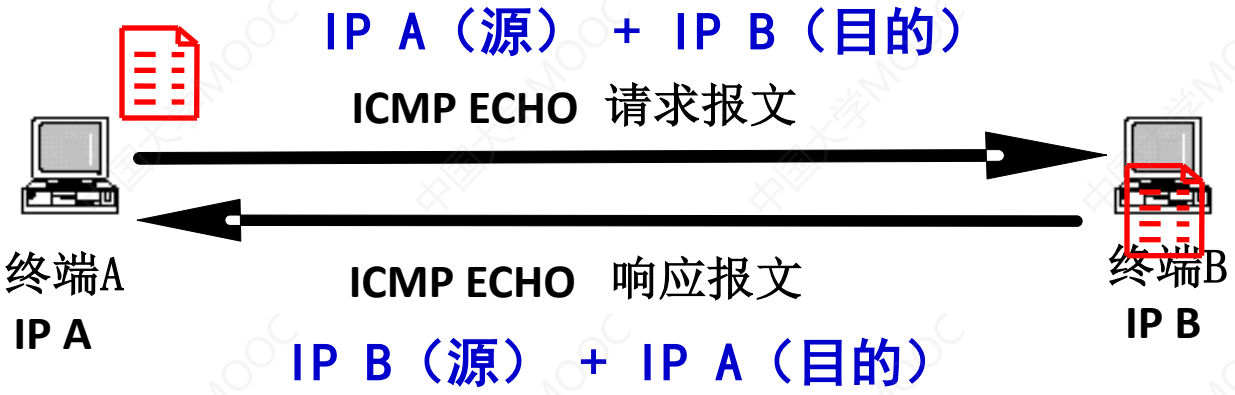
实施SYN泛洪攻击的前提是伪造源IP地址，因此，最直接的防御SYN泛洪攻击的办法是，使网络具有阻止伪造源IP地址的IP分组继续传输的功能。

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。

4 拒绝服务攻击

4.2 Smurf攻击——针对网络带宽的DoS攻击

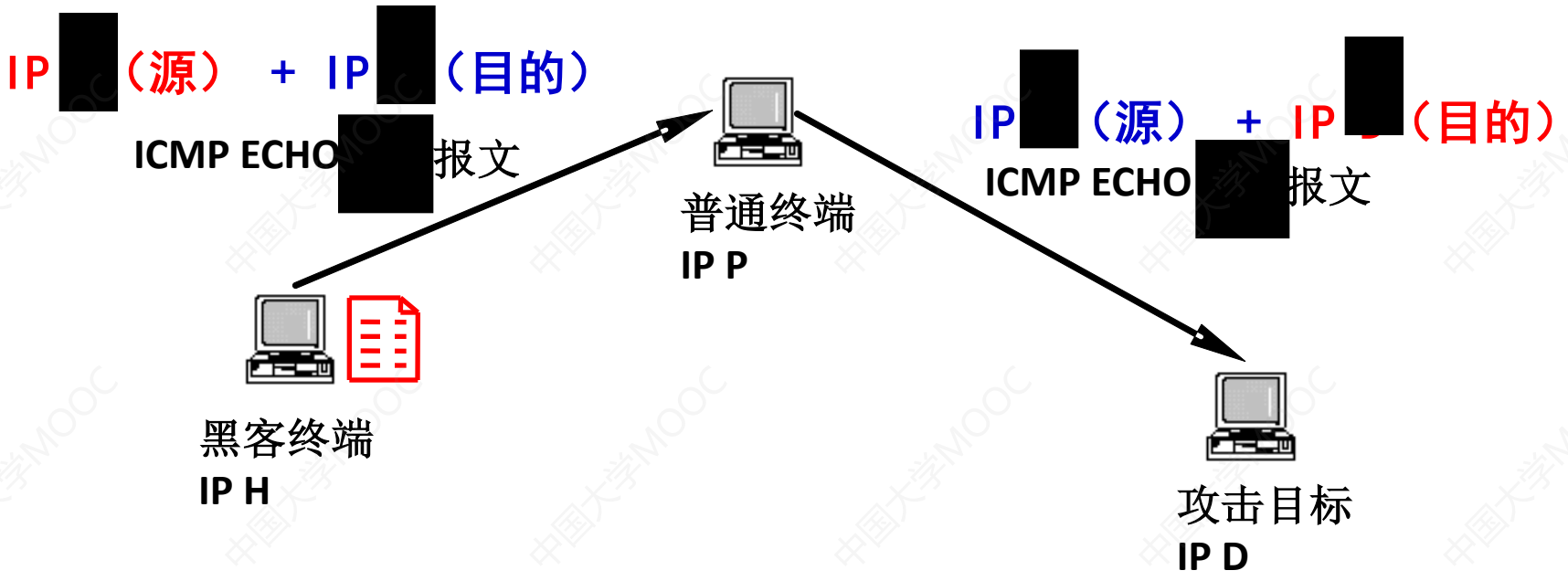
- ping过程



4 拒绝服务攻击

4.2 Smurf攻击——针对网络带宽的DoS攻击

- ping间接攻击过程

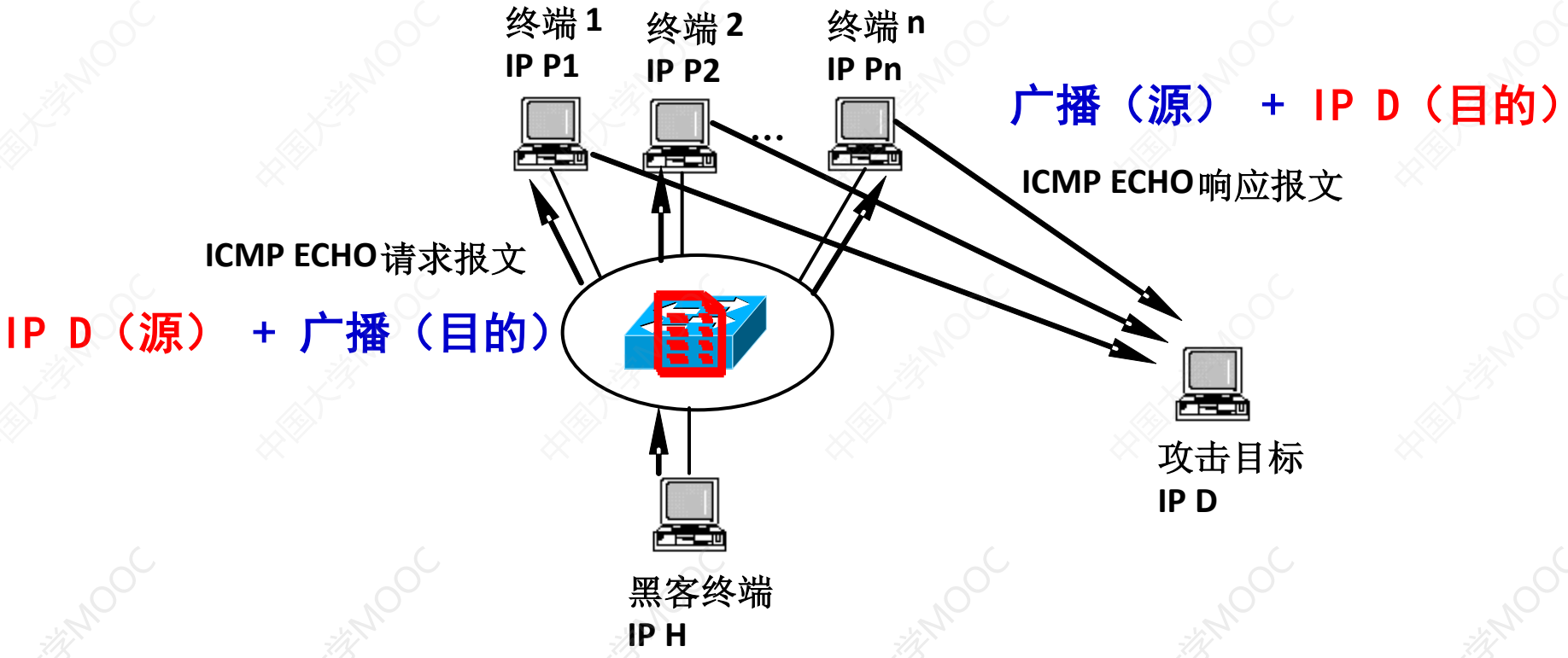


- 间接攻击过程使得黑客终端对攻击目标是透明的，导致攻击者很难直接追踪到黑客终端。

4 拒绝服务攻击

4.2 Smurf攻击——针对网络带宽的DoS攻击

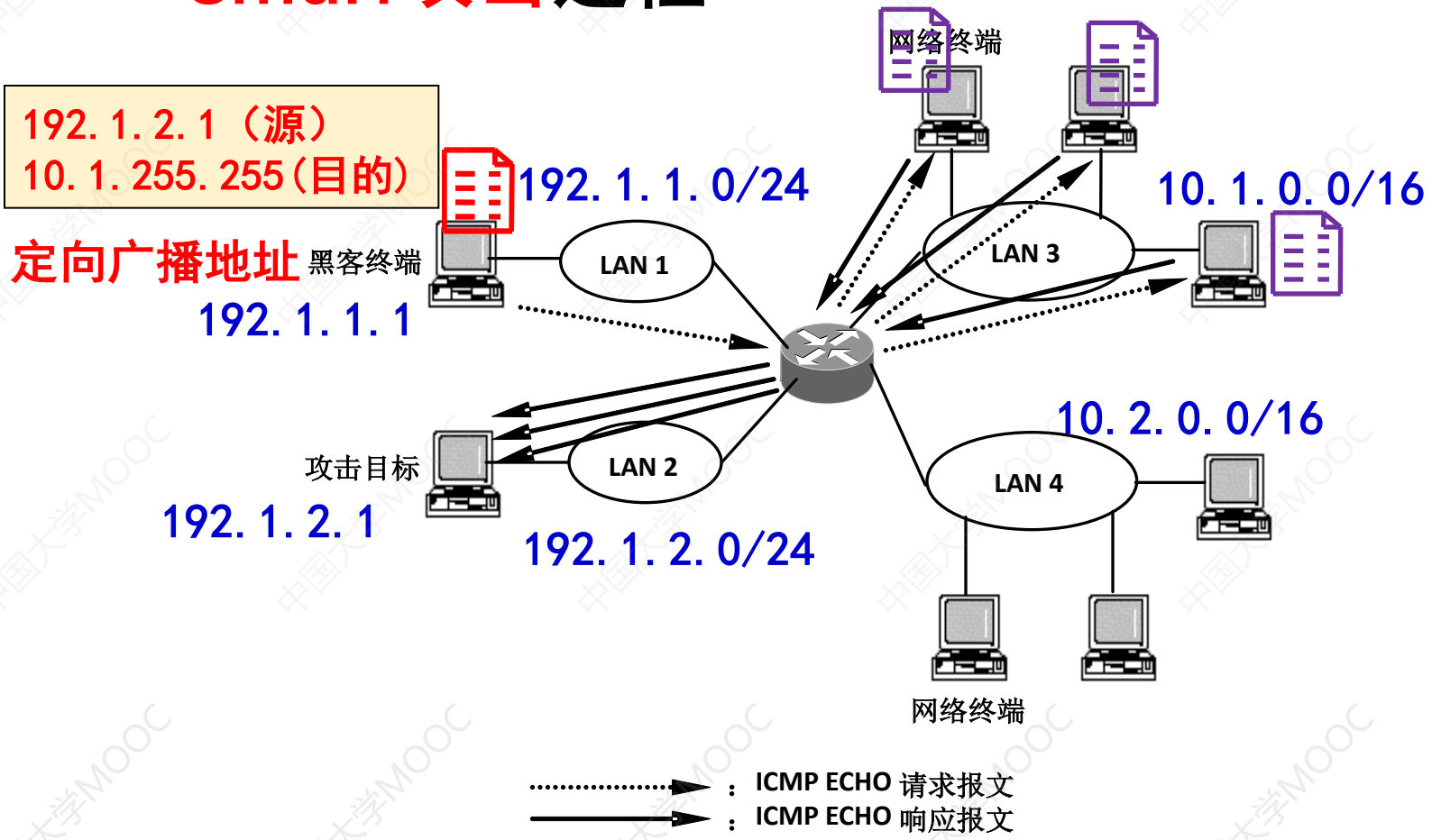
- ping放大攻击过程



4 拒绝服务攻击

4.2 Smurf攻击——针对网络带宽的DoS攻击

- Smurf攻击过程



4 拒绝服务攻击

4.2 Smurf攻击——针对网络带宽的DoS攻击

- Smurf攻击防御机制

➢使网络具有阻止伪造源IP地址的IP分组继续传输的功能；

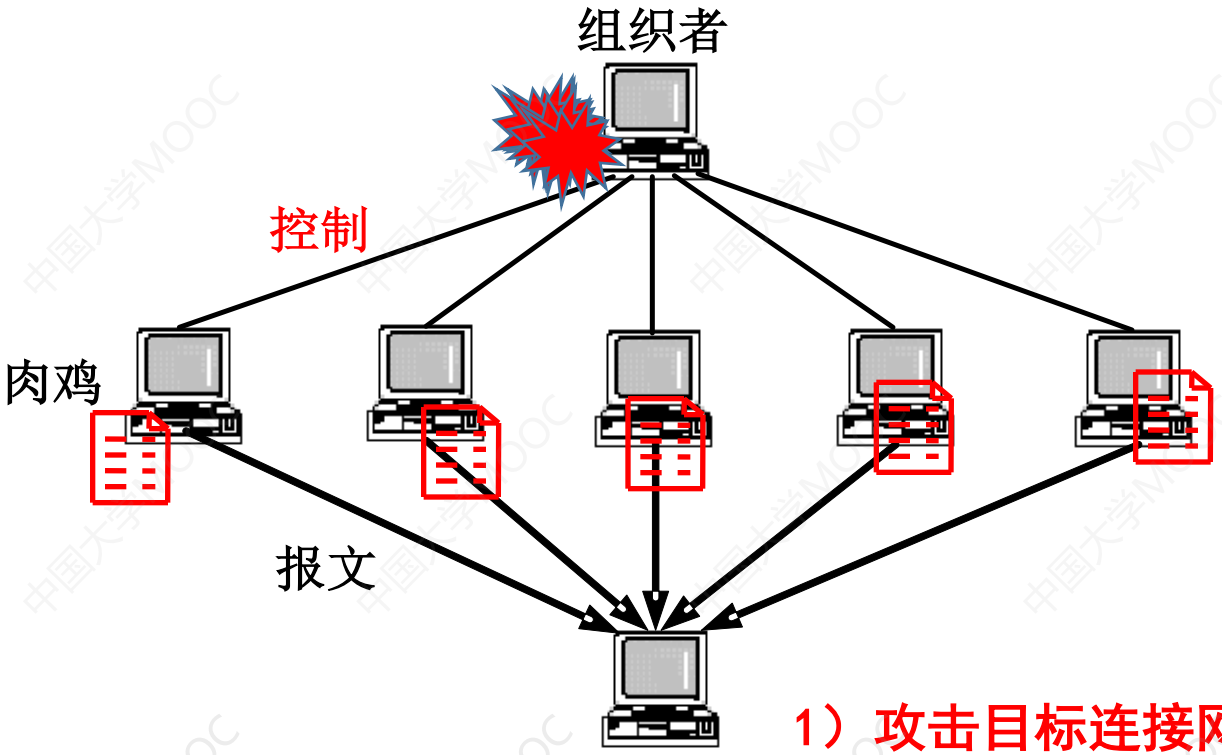
➢路由器阻止以直接广播地址为目的IP地址的IP分组继续转发；

➢主机系统拒绝响应ICMP ECHO请求报文。

4 拒绝服务攻击

4.3 DDoS攻击——针对处理器、网络带宽的DoS攻击

- 直接DDoS攻击



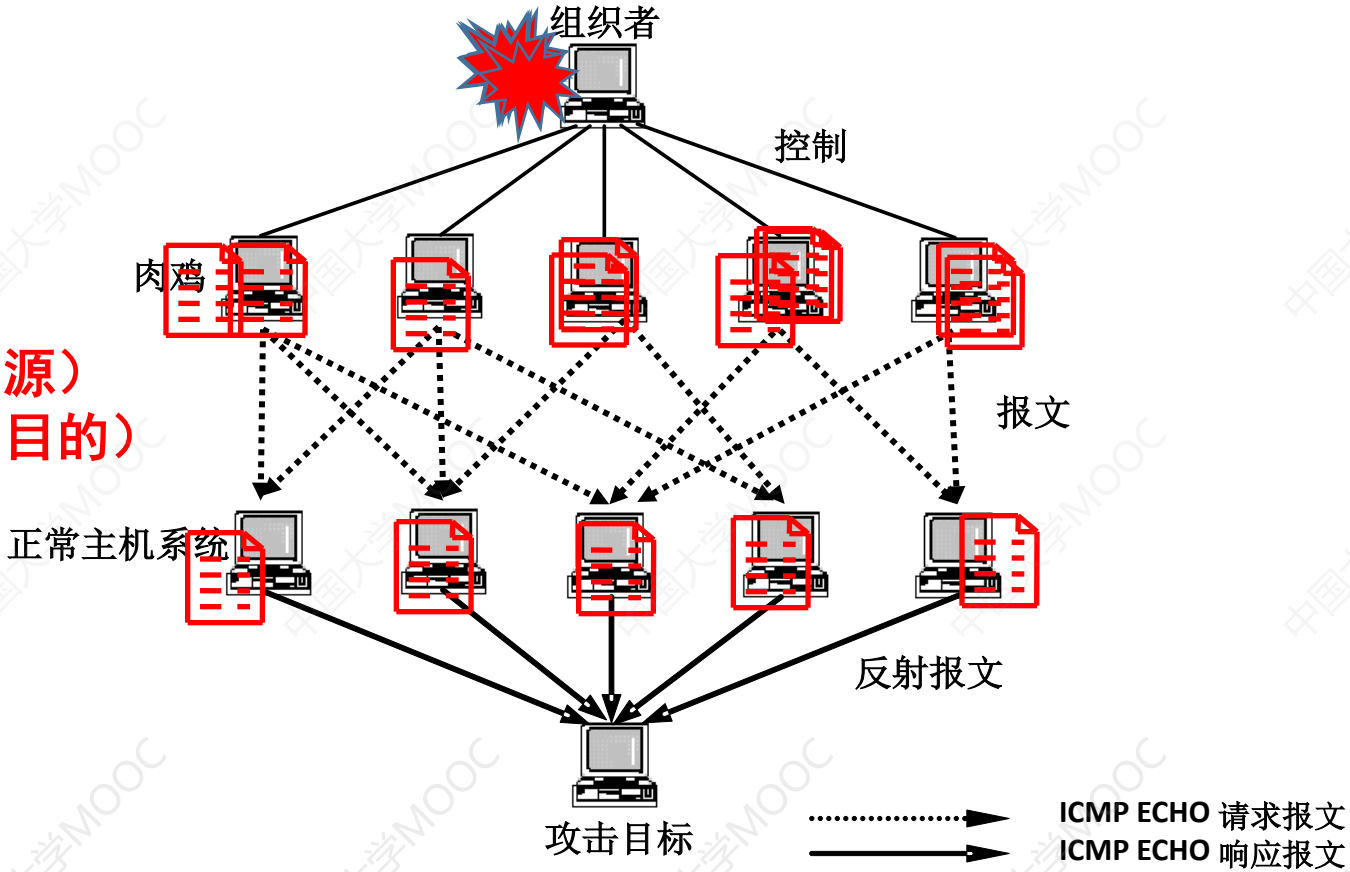
1）攻击目标连接网络的链接过载
2）攻击目标处理器资源耗尽

4 拒绝服务攻击

4.3 DDoS攻击——针对处理器、网络带宽的DoS攻击

- 间接DDoS攻击

攻击目标IP（源）
随机主机IP（目的）



4 拒绝服务攻击

4.3 DDoS攻击——针对处理器、网络带宽的DoS攻击

- DDoS攻击防御机制

一是需要尽可能地减少肉鸡，这就要求连接在互联网上的主机系统能够具备防御病毒和黑客入侵的能力。

二是使主机系统拒绝响应ICMP ECHO请求报文。

三是网络具有统计目的IP地址相同的ICMP ECHO响应报文，或ICMP差错报告报文数量的能力，如果网络中单位时间内经过的目的IP地址相同的ICMP ECHO响应报文，或ICMP差错报告报文的数量超过设定的阈值，网络能够丢弃部分ICMP ECHO响应报文，或ICMP差错报告报文。

内容安排

1. 网络攻击的定义与分类
2. 嗅探攻击
3. 截获攻击
4. 拒绝服务攻击
5. 欺骗攻击
6. 非法接入和登录
7. 小结

5 欺骗攻击

本部分主要内容

- 源IP地址欺骗攻击；
- 钓鱼网站。

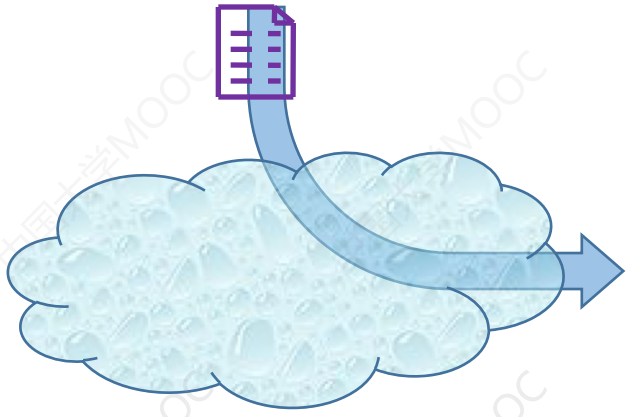
5 欺骗攻击

欺骗攻击就是用错误的信息误导网络数据传输过程和用户资源访问过程的攻击行为。

- 伪装Bob，欺骗Alice

Eve

Bob



通信网络

Alice

5 欺骗攻击

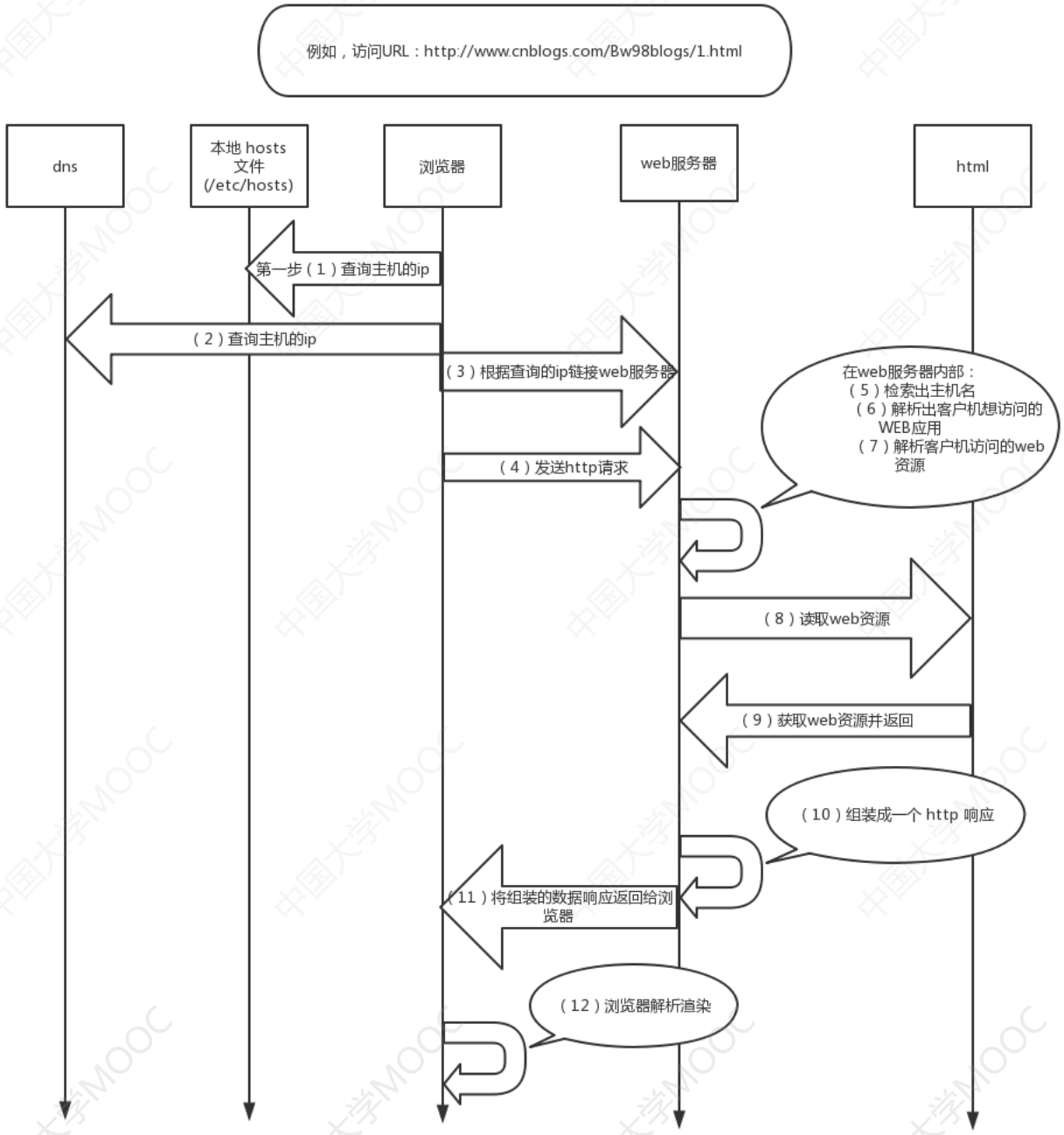
5.1 源IP地址欺骗攻击

■ 源IP地址欺骗攻击原理

源IP地址欺骗是指某个终端发送IP分组时，不是以该终端真实的IP地址作为源IP地址，而是用其它终端的IP地址，或者伪造一个本不存在的IP地址作为IP分组的源IP地址的行为。

■ 源IP地址欺骗攻击防御机制

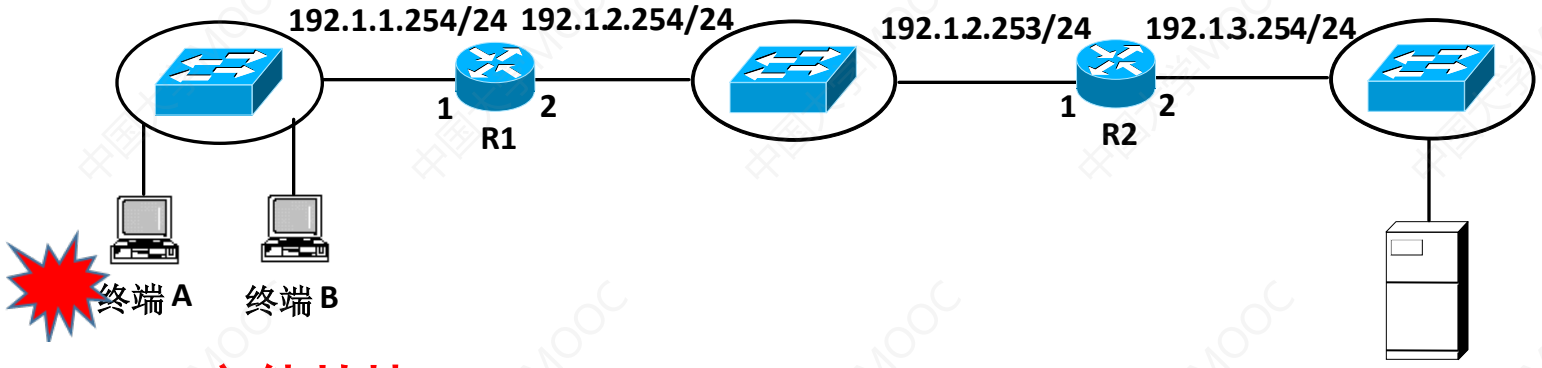
网络接收到某个IP分组时，首先判别该IP分组的源IP地址是否与发送该IP分组的终端的IP地址一致，如果不一致，终止该IP分组的转发过程。


例如，访问URL：http://www.cnblogs.com/Bw98blogs/1.html
dns
本地 hosts 文件 (/etc/hosts)
浏览器
web服务器
html
第一步（1）查询主机的ip
（2）查询主机的ip
（3）根据查询的ip链接web服务器
（4）发送http请求
在web服务器内部：
（5）检索出主机名
（6）解析出客户机想访问的WEB应用
（7）解析客户机访问的web资源
（8）读取web资源
（9）获取web资源并返回
（10）组装成一个 http 响应
（11）将组装的数据响应返回给浏览器
（12）浏览器解析渲染

5 欺骗攻击

5.2 钓鱼网站

- 终端入侵



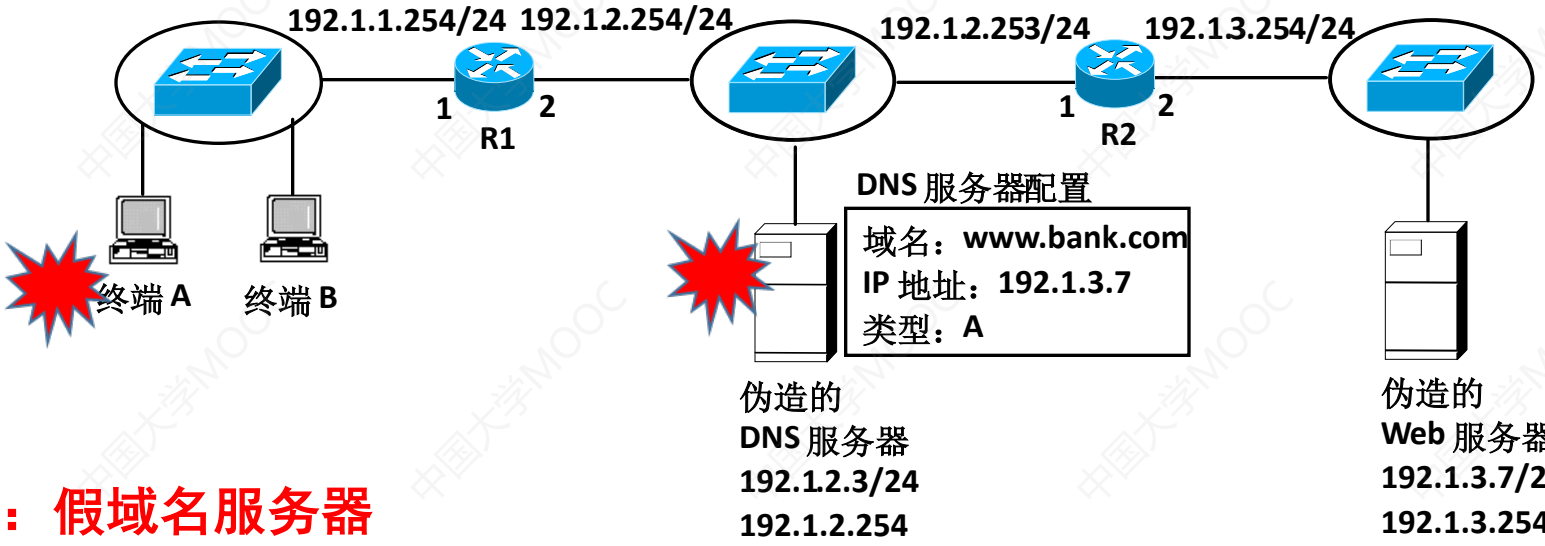
方法1：hosts文件劫持

将终端中的hosts文件中添加域名www.bank.com与IP地址192.1.3.7的绑定项

5 欺骗攻击

5.2 钓鱼网站

- 终端入侵



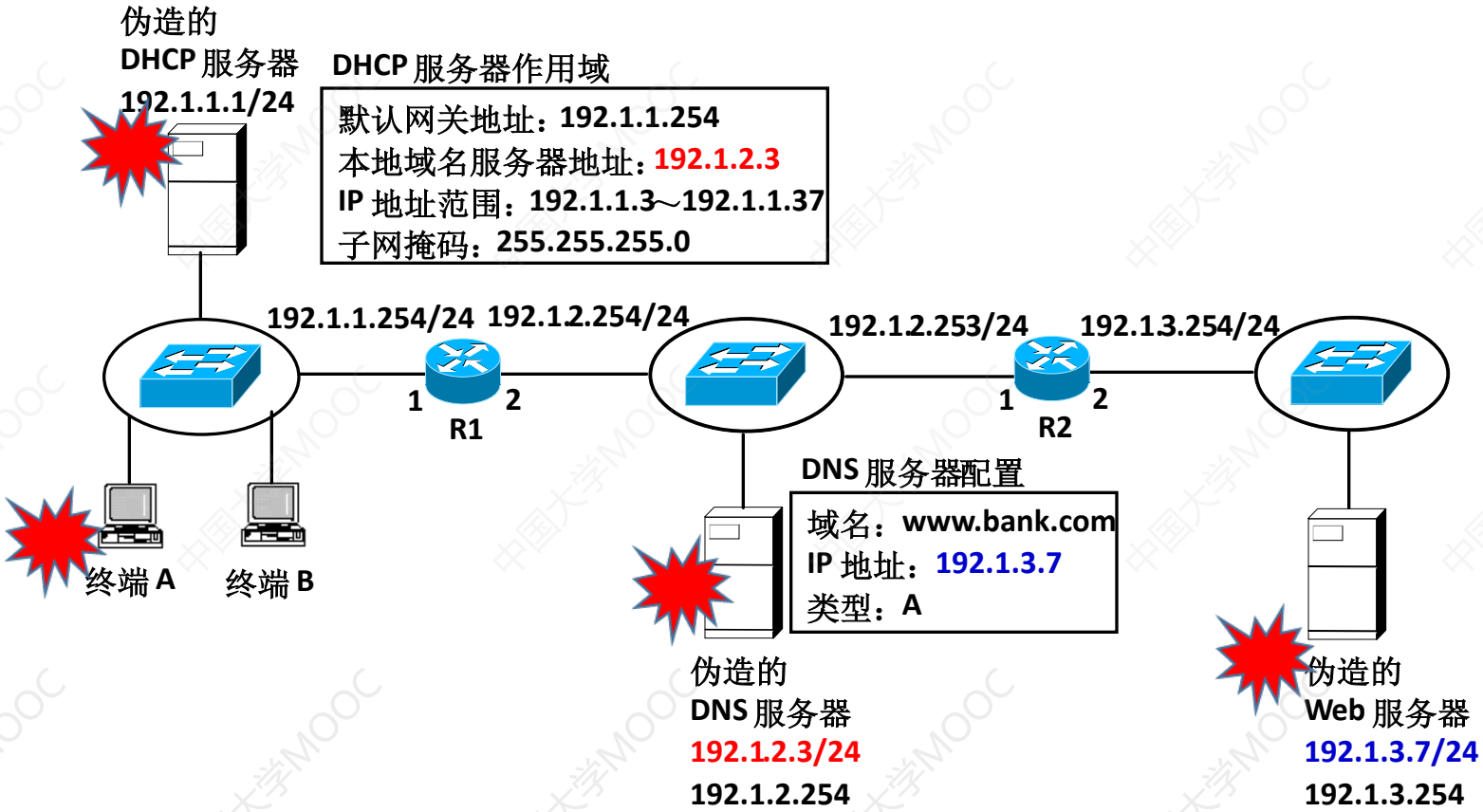
方法2：假域名服务器

将终端中配置的本地域名服务器地址改为假的域名服务器地址，在假的域名服务器中配置域名www.bank.com与IP地址192.1.3.7的绑定项

5 欺骗攻击

5.2 钓鱼网站

- 非终端入侵



5 欺骗攻击

5.2 钓鱼网站

- 钓鱼网站防御机制

一是主机具有防御黑客入侵的能力，黑客无法修改主机信息。

二是以太网交换机具有防止伪造的DHCP服务器接入的能力，只允许经过认证的DHCP服务器接入以太网。

三是终端具有鉴别Web服务器的能力，证实Web服务器身份后，才对Web服务器进行访问。

内容安排

1. 网络攻击的定义与分类
2. 嗅探攻击
3. 截获攻击
4. 拒绝服务攻击
5. 欺骗攻击
6. 非法接入和登录
7. 小结

6 非法接入和登录

本部分主要内容

- 非法接入无线局域网；
- 非法登录。

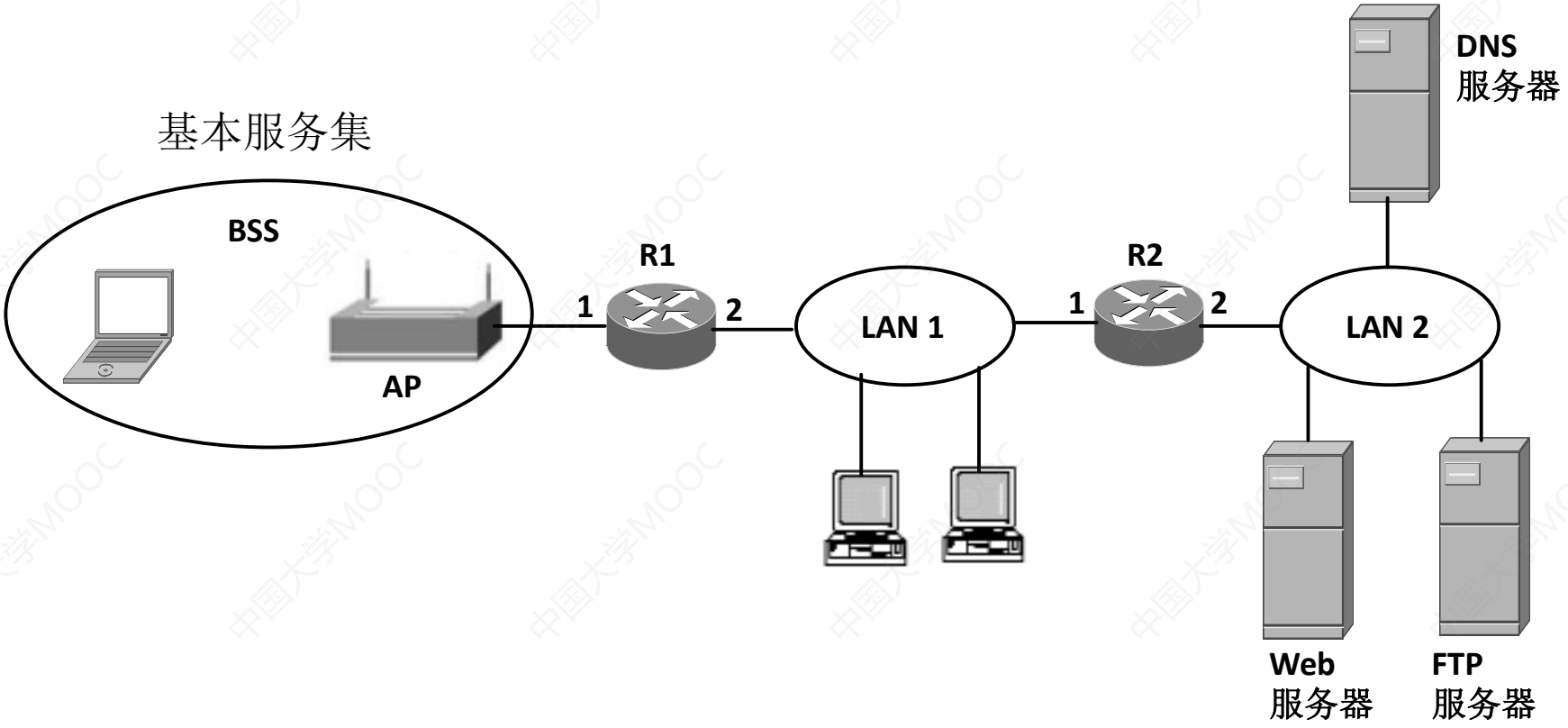
6 非法接入和登录

非法接入是指非授权**终端**与无线局域网中的接入点（Access Point，AP）之间建立关联的过程。

非法登录是指非授权**用户**远程登录网络设备和服务器，并对网络设备和服务器进行配置和管理的过程。

6 非法接入和登录

6.1 非法接入无线局域网



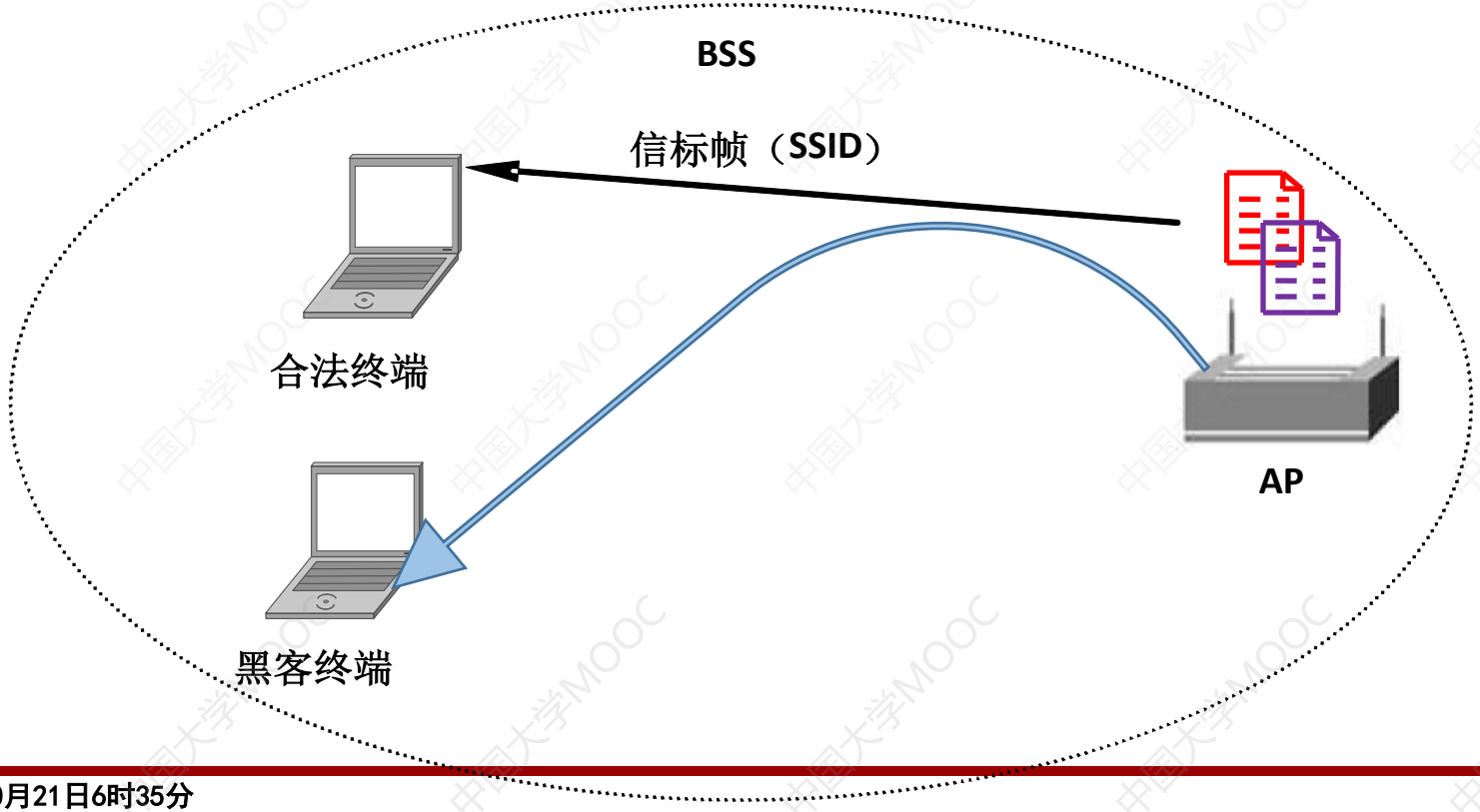
网络结构

6 非法接入和登录

6.1 非法接入无线局域网

- 获得SSID

黑客终端可以通过侦听信标帧或探测响应帧获得AP的SSID。

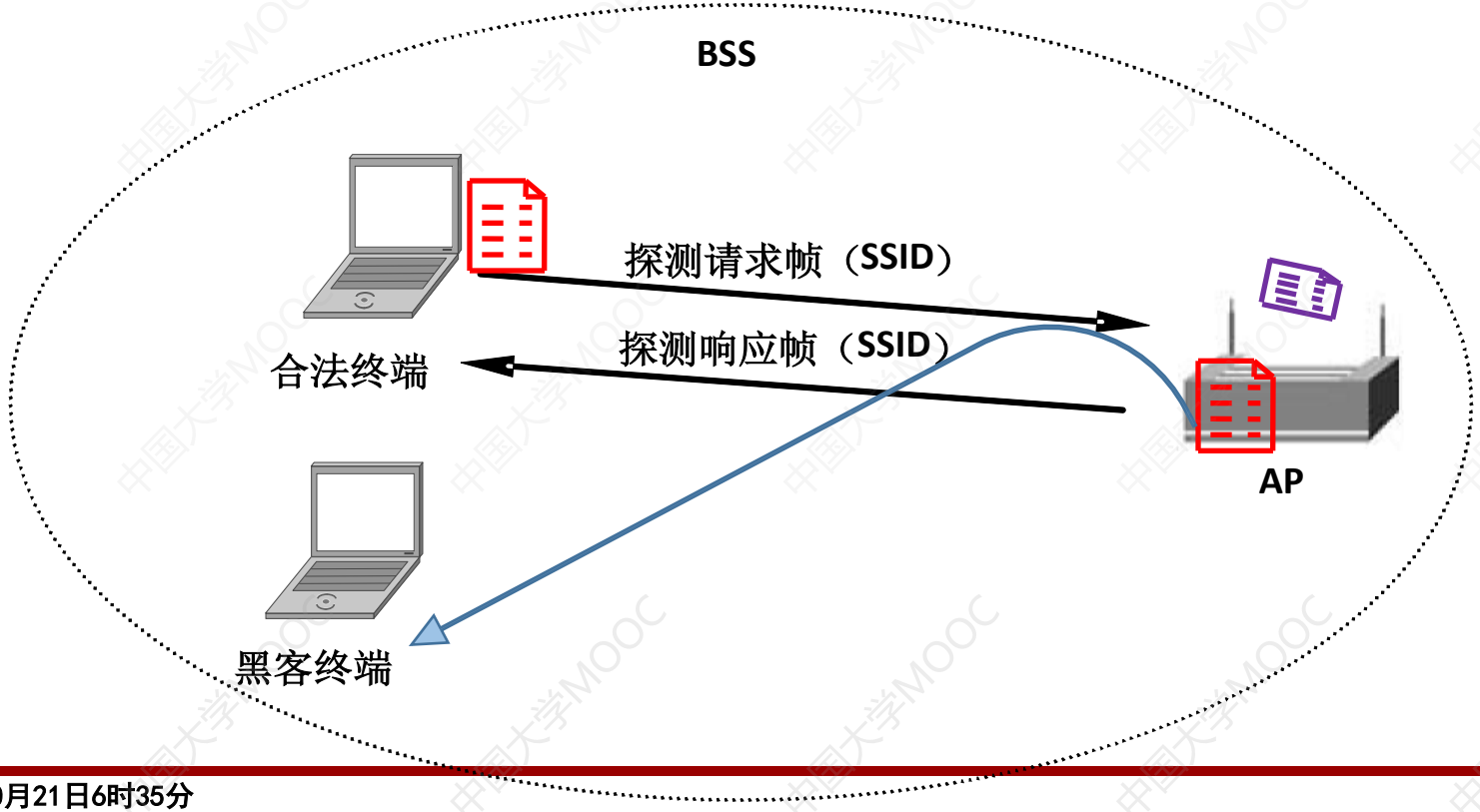


6 非法接入和登录

6.1 非法接入无线局域网

- 获得SSID

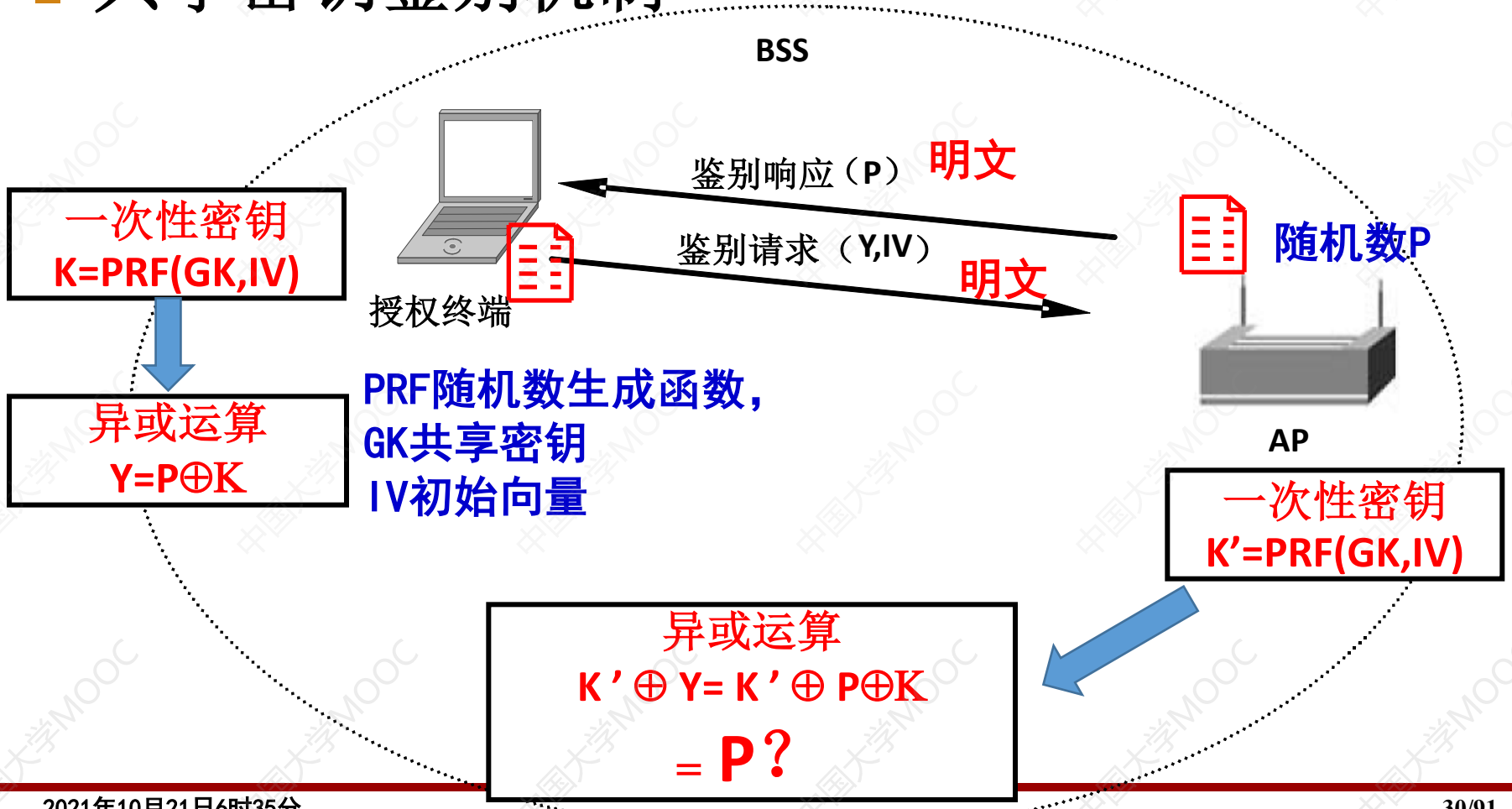
黑客终端可以通过侦听信标帧或探测响应帧获得AP的SSID。



6 非法接入和登录

6.1 非法接入无线局域网

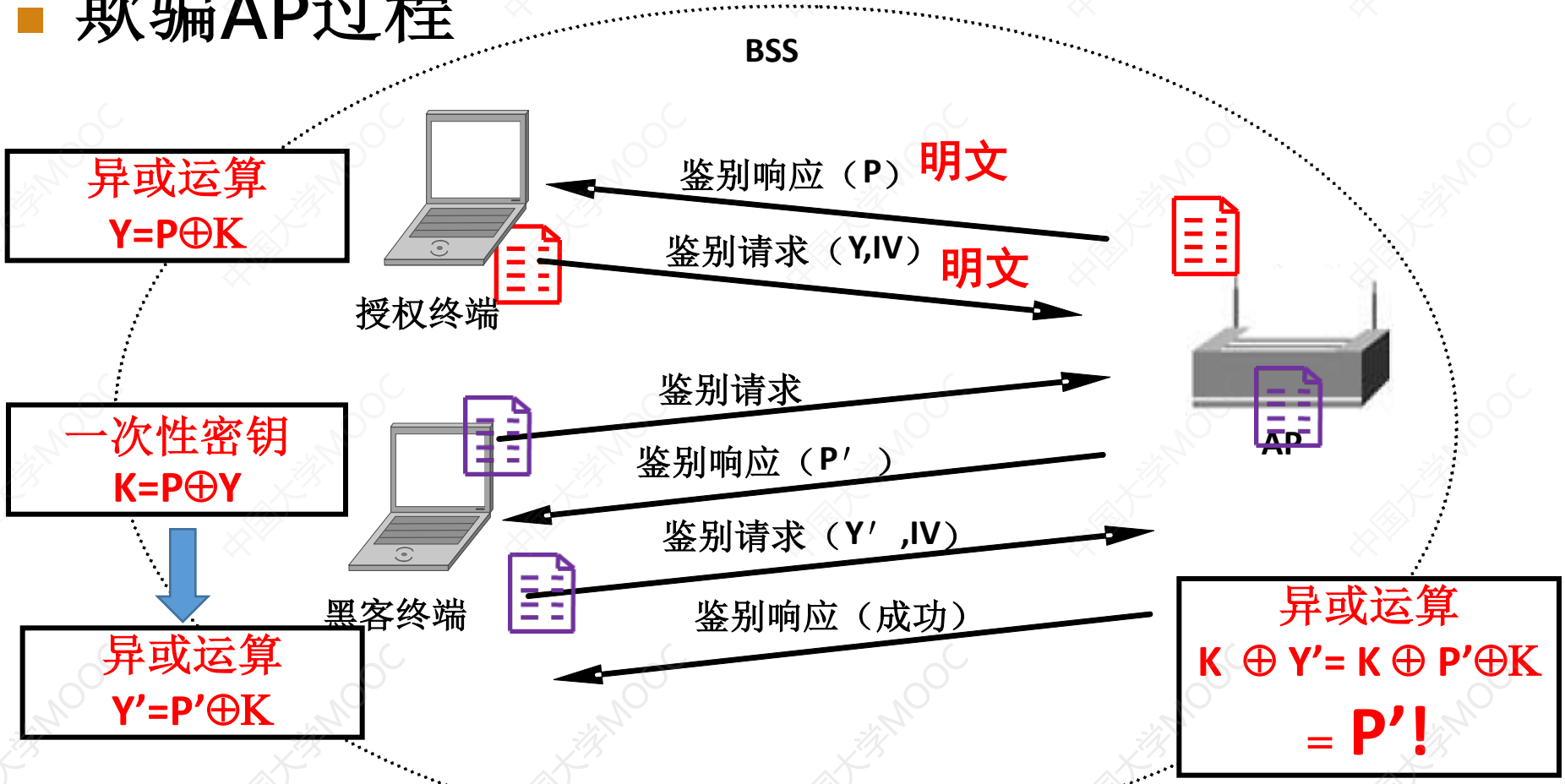
- 共享密钥鉴别机制



6 非法接入和登录

6.1 非法接入无线局域网

- 欺骗AP过程



6 非法接入和登录

6.1 非法接入无线局域网

- 非法接入防御机制

防御黑客终端非法接入的主要方法是，AP不用通过一次性密钥K异或随机数P生成的密文Y来证明授权终端拥有共享密钥GK。

6 非法接入和登录

6.2 非法登录

非法登录是指非授权用户远程登录网络设备和Web服务器，并对网络设备和Web服务器进行非法配置的攻击行为。

6 非法接入和登录

6.2 非法登录

- 非法登录过程

获取授权用户的用户名和口令

方法一：明码传输，直接截获

方法二：暴力破解口令

方法三：社会工程学推测口令

6 非法接入和登录

6.2 非法登录

- 非法登录防御机制

一是使得授权用户正常登录时，以密文方式向网络设备和Web服务器传输用户身份标识信息，如用户名和口令。
二是要求网络设备和Web服务器设置的口令必须具备一定长度，同时包含数字、大写字母、小写字母和特殊字符，使得黑客短时间内无法通过暴力破解来获得口令。

内容安排

1. 网络攻击的定义与分类
2. 嗅探攻击
3. 截获攻击
4. 拒绝服务攻击
5. 欺骗攻击
6. 非法接入和登录
7. 小结

7 小结

（1）主动攻击

- 篡改信息；
- 欺骗攻击；
- 拒绝服务攻击；
- 重放攻击。

7 小结

2. 被动攻击

- 嗅探信息；
- 非法访问；
- 数据流分析。