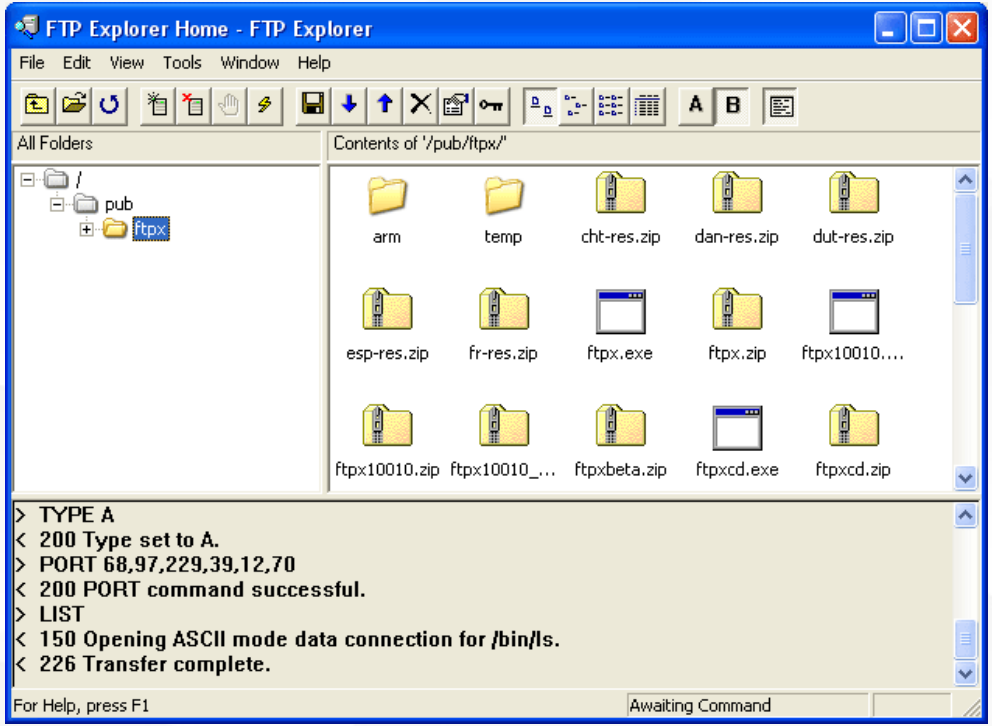
地址解析协议 ARP

(Address Resolution Protocol)

案例


FTP Explorer Home - FTP Explorer
File Edit View Tools Window Help
All Folders
Contents of '/pub/ftpx/'
/
pub
ftpx
arm
temp
cht-res.zip
dan-res.zip
dut-res.zip
esp-res.zip
fr-res.zip
ftpx.exe
ftpx.zip
ftpx10010....
ftpx10010.zip
ftpx10010_...
ftpxbeta.zip
ftpxcd.exe
ftpxcd.zip
> TYPE A
< 200 Type set to A.
> PORT 68,97,229,39,12,70
< 200 PORT command successful.
> LIST
< 150 Opening ASCII mode data connection for /bin/ls.
< 226 Transfer complete.
For Help, press F1
Awaiting Command

案例

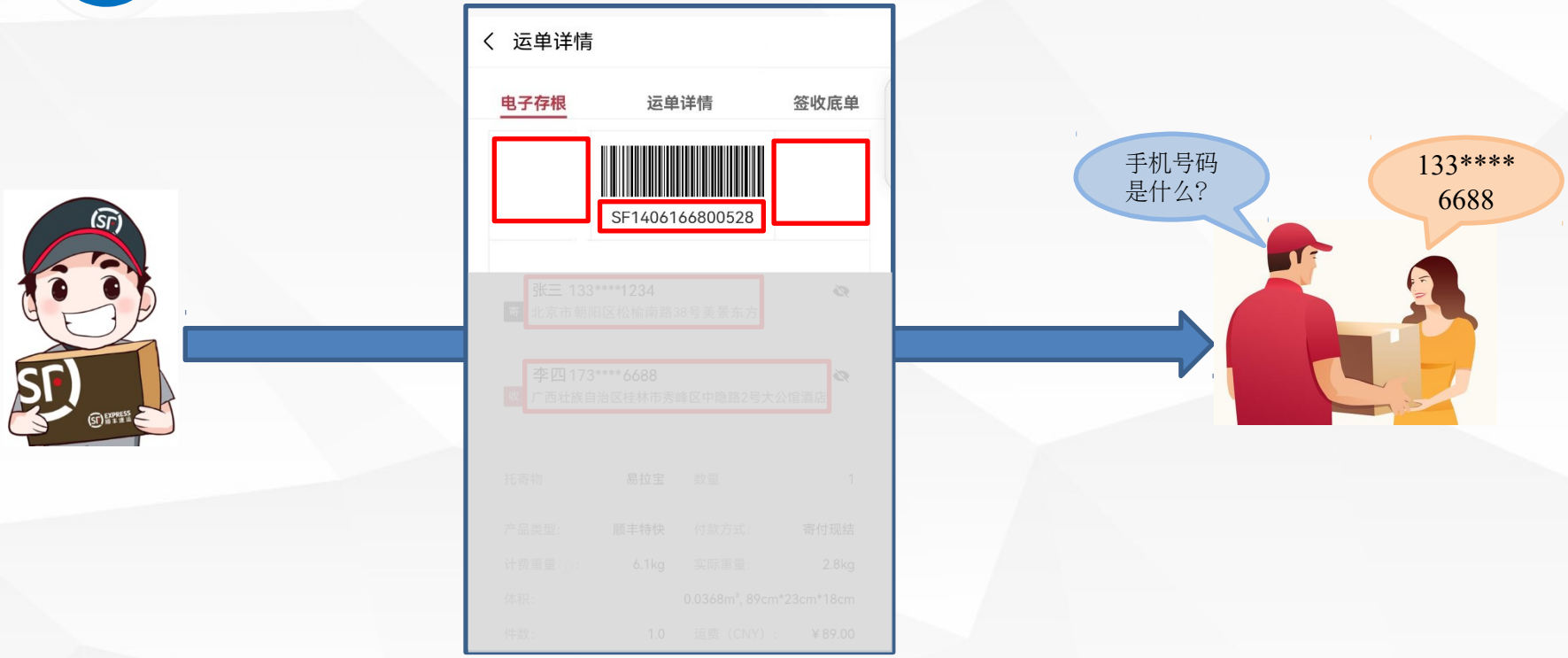

360流量防火墙
管理网速
保护网速
局域网防护
防蹭网
网络连接
测网速
遭受ARP攻击，已拦截
详情
已自动绑定网关
切换到手动绑定
局域网防护已开启，正在保护您的上网安全!
自动绑定网关
已开启
ARP主动防御
已开启
IP冲突拦截
已开启
局域网隐身
不会遭受局域网攻击，开启后将无法查看网络邻居，无法使用FTP、共享打印机等设备。
已开启
安全防护日志
ARP攻击包拦截数
40
IP冲突拦截
0
查看详细日志
白名单设置
可以将电脑中的程序添加入白名单中，局域网防护将不再拦截，让您在局域网内上网更安心。
设置白名单

ARP 协议原理

问题 1：在快递从揽收到交给收件人，经过了怎样的过程?

ARP 协议原理

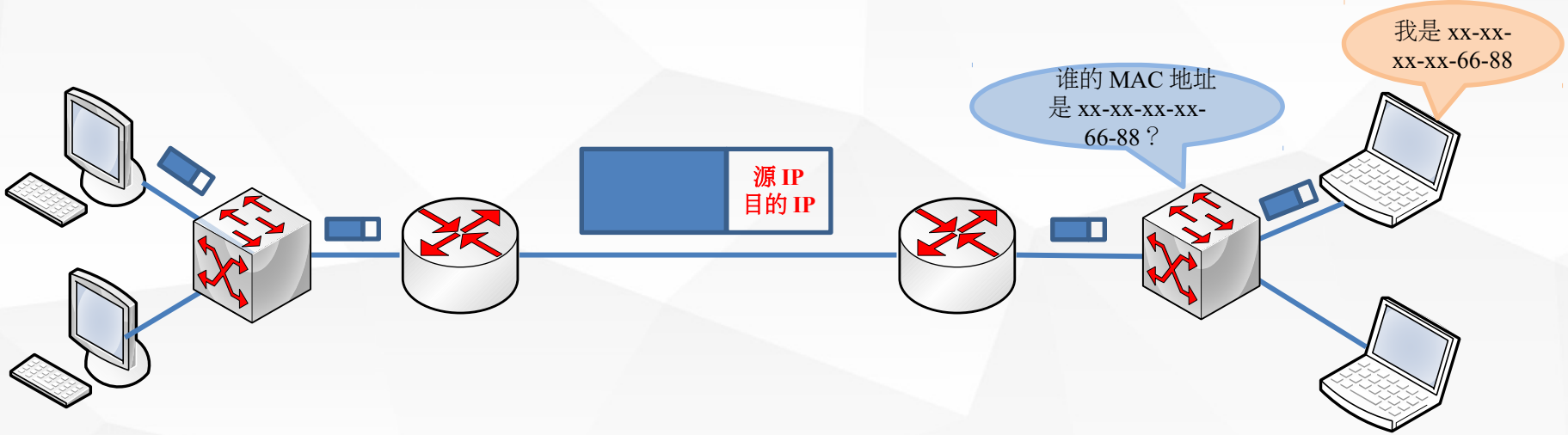
问题 2： 在快递运输过程中使用了哪些标识来保证快递能准确投递到收件人手中?



01

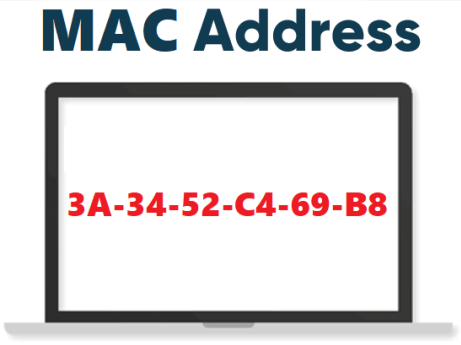
ARP 协议原理

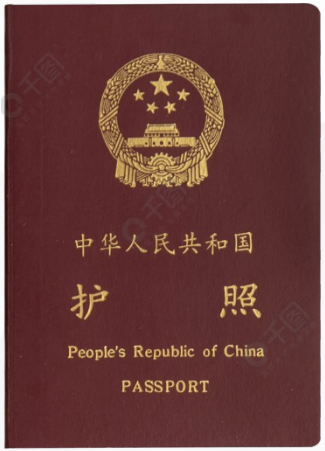
生活场景 VS 应用场景



ARP 协议原理

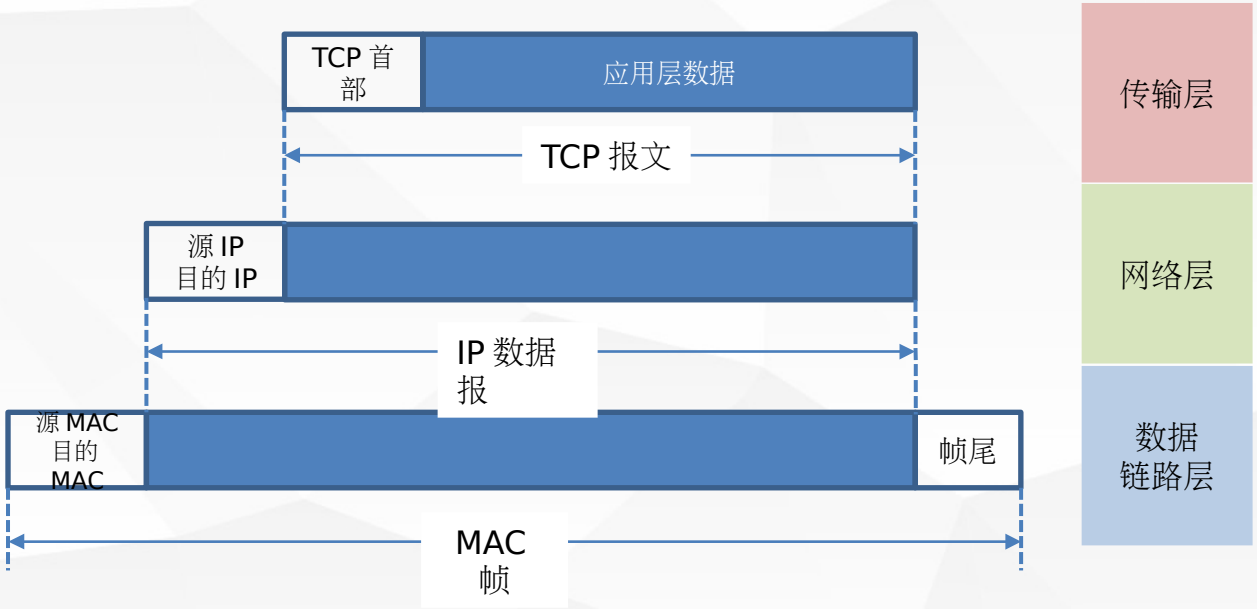
地址 VS 证件





ARP 协议原理

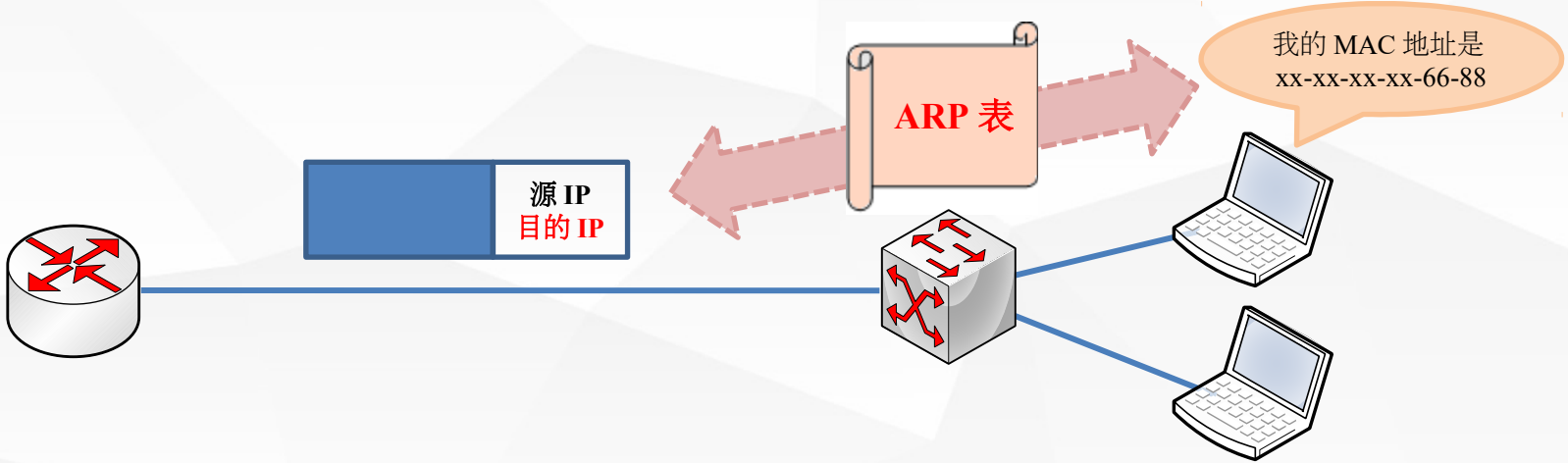
IP 地址 VS MAC 地址



01

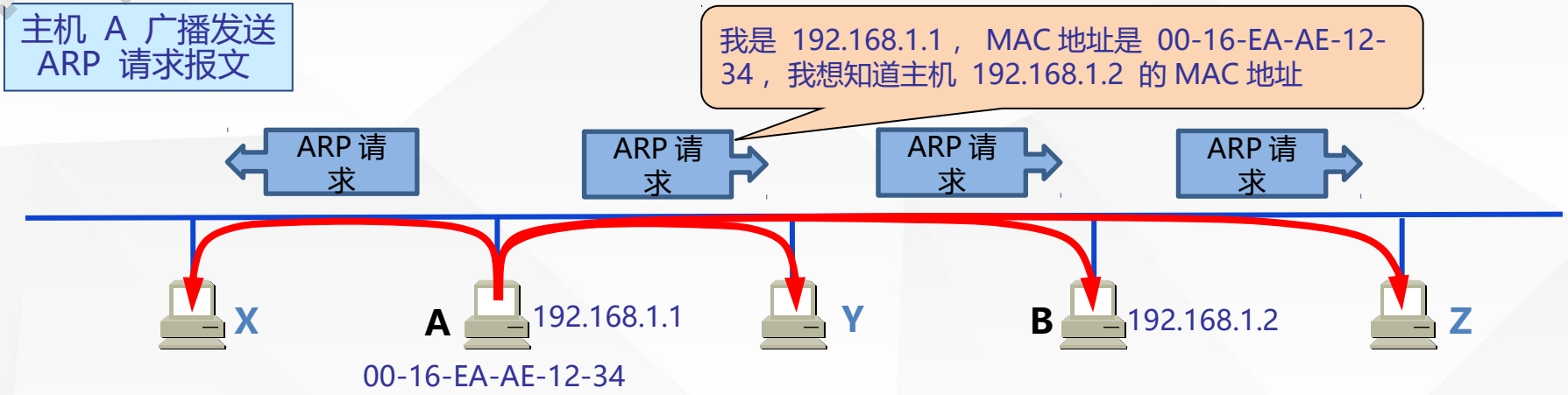
ARP 协议原理

生活场景 VS 应用场景

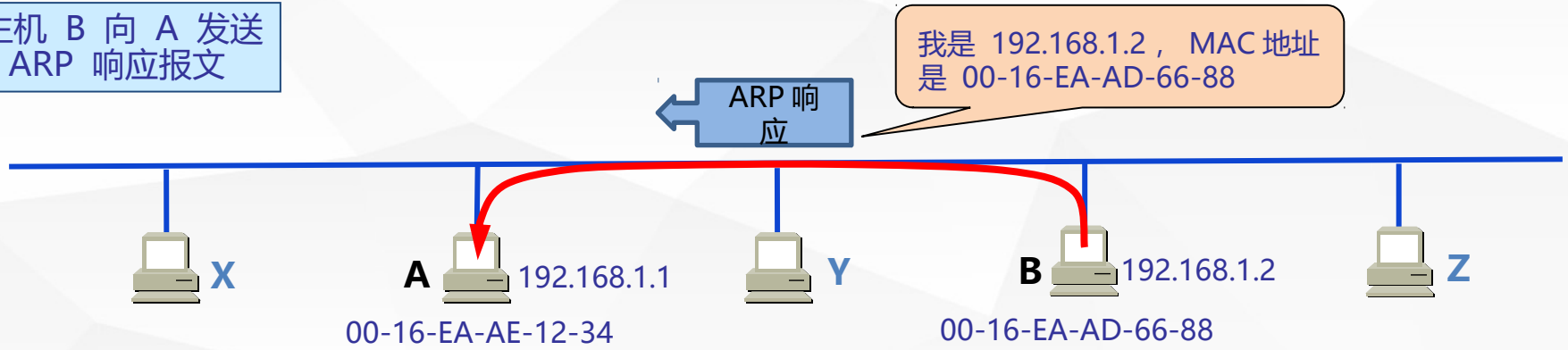


01 ARP 协议工作过程

主机 A 广播发送 ARP 请求报文



主机 B 向 A 发送 ARP 响应报文



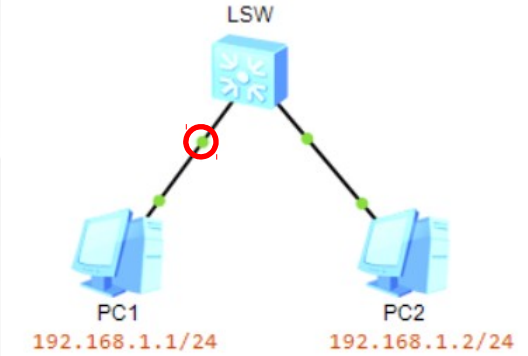
ARP 协议原理

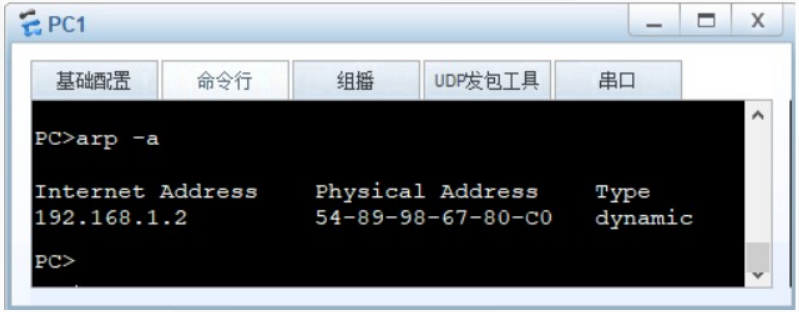
问题 3： 是否在每次通信前一定要运行 ARP 协议?

- 为使广播量最小， ARP 维护 IP 地址到 MAC 地址映射的缓存以便将来使用。 ARP 缓存是个用来储存 IP 地址和 MAC 地址的缓冲区，其本质就是一个 IP 地址与 MAC 地址的对应表，表中每一个条目分别记录了网络上其他主机的 IP 地址和对应的 MAC 地址。
- 当地址解析协议被询问一个 IP 地址节点的 MAC 地址时，先在 ARP 缓存中查看，若存在，就直接返回与之对应的 MAC 地址，若不存在，才发送 ARP 请求向局域网查询。
- ARP 缓存可以包含动态和静态项目。动态项目随时间推移自动添加和删除，每个动态 ARP 缓存项的潜在生命周期是 10 分钟。静态项目一直保留在缓存中，直到重新启

02

重点难点解析





No.	Time	Source	Destination	Protocol	Info
13	26.703000	HuaweiTe_af:1e:02	Spanning-tree-(for-	STP	MST. Root = 32768/0/4c:1f:cc:af:1e:02 Cost = 0 Port = 0x8001
14	26.703000	HuaweiTe_8d:64:45	Broadcast	ARP	Who has 192.168.1.2? Tell 192.168.1.1
15	26.750000	HuaweiTe_67:80:c0	HuaweiTe_8d:64:45	ARP	192.168.1.2 is at 54:89:98:67:80:c0
16	26.781000	192.168.1.1	192.168.1.2	ICMP	Echo (ping) request (id=0x46b6, seq(be/le)=1/256, ttl=128)
17	26.813000	192.168.1.2	192.168.1.1	ICMP	Echo (ping) reply (id=0x46b6, seq(be/le)=1/256, ttl=128)
18	27.844000	192.168.1.1	192.168.1.2	ICMP	Echo (ping) request (id=0x47b6, seq(be/le)=2/512, ttl=128)
19	27.891000	192.168.1.2	192.168.1.1	ICMP	Echo (ping) reply (id=0x47b6, seq(be/le)=2/512, ttl=128)
20	28.906000	192.168.1.1	192.168.1.2	ICMP	Echo (ping) request (id=0x48b6, seq(be/le)=3/768, ttl=128)
21	28.953000	192.168.1.2	192.168.1.1	ICMP	Echo (ping) reply (id=0x48b6, seq(be/le)=3/768, ttl=128)
22	28.969000	HuaweiTe_af:1e:02	Spanning-tree-(for-	STP	MST. Root = 32768/0/4c:1f:cc:af:1e:02 Cost = 0 Port = 0x8001
23	29.969000	192.168.1.1	192.168.1.2	ICMP	Echo (ping) request (id=0x49b6, seq(be/le)=4/1024, ttl=128)
24	30.016000	192.168.1.2	192.168.1.1	ICMP	Echo (ping) reply (id=0x49b6, seq(be/le)=4/1024, ttl=128)
25	31.031000	192.168.1.1	192.168.1.2	ICMP	Echo (ping) request (id=0x4ab6, seq(be/le)=5/1280, ttl=128)
26	31.078000	192.168.1.2	192.168.1.1	ICMP	Echo (ping) reply (id=0x4ab6, seq(be/le)=5/1280, ttl=128)
27	31.188000	HuaweiTe_af:1e:02	Spanning-tree-(for-	STP	MST. Root = 32768/0/4c:1f:cc:af:1e:02 Cost = 0 Port = 0x8001

请求报文

No.	Time	Source	Destination	Protocol	Info
13	26.703000	HuaweiTe_af:1e:02	Spanning-tree-(for-	STP	MST. Root = 32768/0/4c:1f:cc:af:1e:02 Cost = 0 Port = 0x8001
14	26.703000	HuaweiTe_8d:64:45	Broadcast	ARP	Who has 192.168.1.2? Tell 192.168.1.1
15	26.750000	HuaweiTe_67:80:c0	HuaweiTe_8d:64:45	ARP	192.168.1.2 is at 54:89:98:67:80:c0
16	26.781000	192.168.1.1	192.168.1.2	ICMP	Echo (ping) request (id=0x46b6, seq(be/le)=1/256, ttl=128)
17	26.813000	192.168.1.2	192.168.1.1	ICMP	Echo (ping) reply (id=0x46b6, seq(be/le)=1/256, ttl=128)
18	27.844000	192.168.1.1	192.168.1.2	ICMP	Echo (ping) request (id=0x47b6, seq(be/le)=2/512, ttl=128)
19	27.891000	192.168.1.2	192.168.1.1	ICMP	Echo (ping) reply (id=0x47b6, seq(be/le)=2/512, ttl=128)
20	28.906000	192.168.1.1	192.168.1.2	ICMP	Echo (ping) request (id=0x48b6, seq(be/le)=3/768, ttl=128)
21	28.953000	192.168.1.2	192.168.1.1	ICMP	Echo (ping) reply (id=0x48b6, seq(be/le)=3/768, ttl=128)

```
⊞ Frame 14: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: HuaweiTe_8d:64:45 (54:89:98:8d:64:45), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    [Is gratuitous: False]
    Sender MAC address: HuaweiTe_8d:64:45 (54:89:98:8d:64:45)
    Sender IP address: 192.168.1.1 (192.168.1.1)
    Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
    Target IP address: 192.168.1.2 (192.168.1.2)
```

响应报文

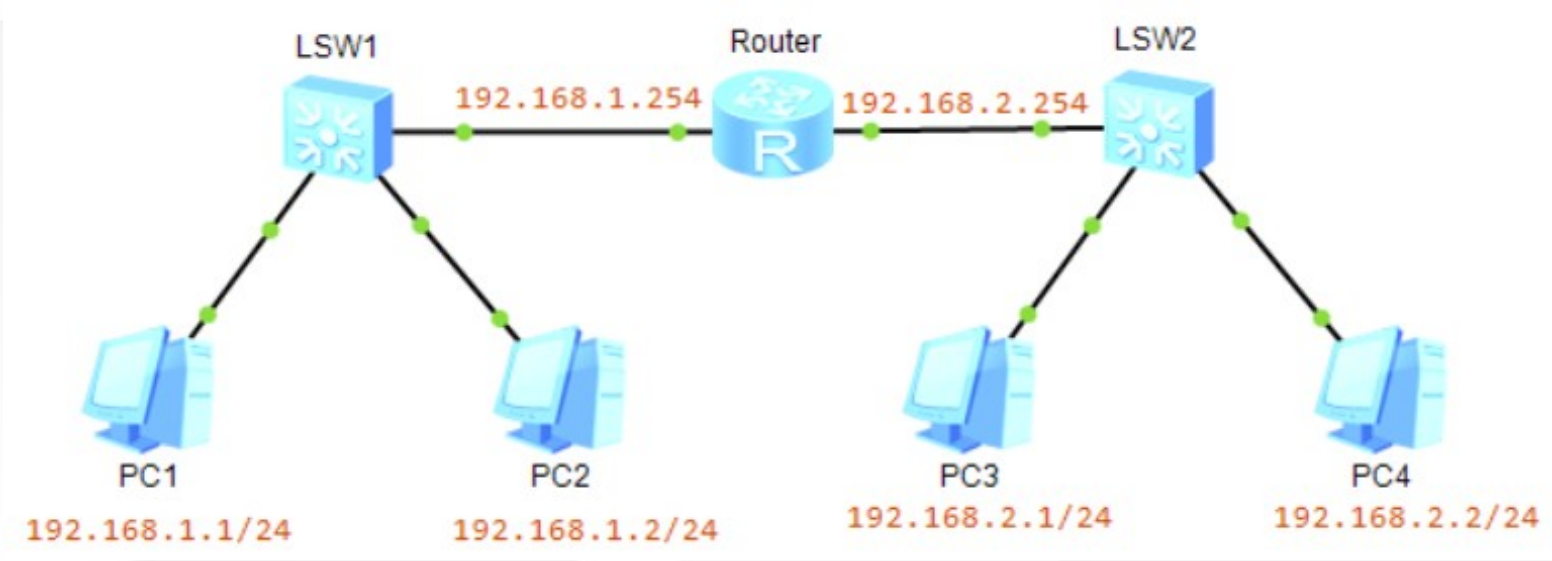
No.	Time	Source	Destination	Protocol	Info
13	26.703000	HuaweiTe_af:1e:02	Spanning-tree-(for-	STP	MST. Root = 32768/0/4c:1f:cc:af:1e:02 Cost = 0 Port = 0x8001
14	26.703000	HuaweiTe_8d:64:45	Broadcast	ARP	Who has 192.168.1.2? Tell 192.168.1.1
15	26.750000	HuaweiTe_67:80:c0	HuaweiTe_8d:64:45	ARP	192.168.1.2 is at 54:89:98:67:80:c0
16	26.781000	192.168.1.1	192.168.1.2	ICMP	Echo (ping) request (id=0x46b6, seq(be/le)=1/256, ttl=128)
17	26.813000	192.168.1.2	192.168.1.1	ICMP	Echo (ping) reply (id=0x46b6, seq(be/le)=1/256, ttl=128)
18	27.844000	192.168.1.1	192.168.1.2	ICMP	Echo (ping) request (id=0x47b6, seq(be/le)=2/512, ttl=128)
19	27.891000	192.168.1.2	192.168.1.1	ICMP	Echo (ping) reply (id=0x47b6, seq(be/le)=2/512, ttl=128)
20	28.906000	192.168.1.1	192.168.1.2	ICMP	Echo (ping) request (id=0x48b6, seq(be/le)=3/768, ttl=128)
21	28.953000	192.168.1.2	192.168.1.1	ICMP	Echo (ping) reply (id=0x48b6, seq(be/le)=3/768, ttl=128)

```
⊞ Frame 15: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: HuaweiTe_67:80:c0 (54:89:98:67:80:c0), Dst: HuaweiTe_8d:64:45 (54:89:98:8d:64:45)
⊟ Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    [Is gratuitous: False]
    Sender MAC address: HuaweiTe_67:80:c0 (54:89:98:67:80:c0)
    Sender IP address: 192.168.1.2 (192.168.1.2)
    Target MAC address: HuaweiTe_8d:64:45 (54:89:98:8d:64:45)
    Target IP address: 192.168.1.1 (192.168.1.1)
```

问题 4：对于跨网段的通信，ARP 协议如何运行?

02

重点难点解析


LSW1
Router
LSW2
192.168.1.254
192.168.2.254
PC1
192.168.1.1/24
PC2
192.168.1.2/24
PC3
192.168.2.1/24
PC4
192.168.2.2/24

03

应用拓展

问题 5：通过学习 ARP 协议的原理和工作过程，你觉得 ARP 协议是否存在漏洞?

03

应用拓展

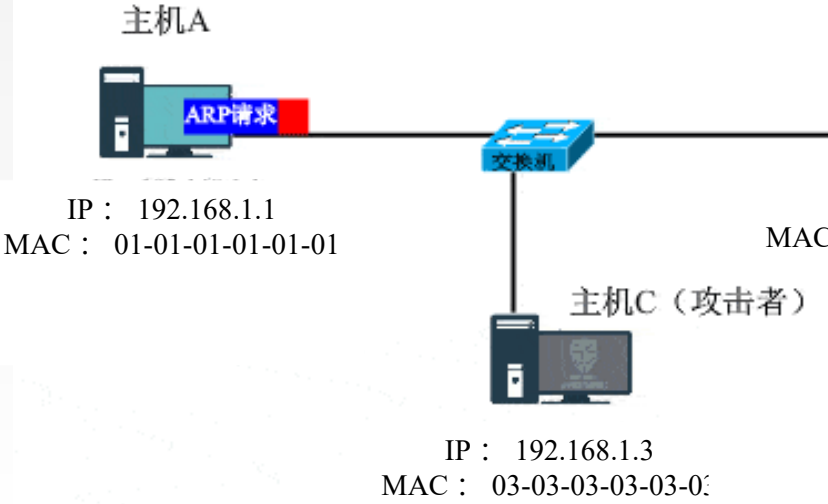
ARP 攻击分类

ARP 断网攻击

通知主机或路由器一系列错误的内网 MAC 地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在主机或路由器中，结果所有数据只能发送给错误的 MAC 地址，造成正常主机无法收到信息。

ARP 欺骗

建立虚假网关，使被欺骗主机向虚假网关发送数据，而不是通过正常的路由器途径上网。 ARP 欺骗可以导致目标计算机与网关通信失败，更会导致通信重定向，所有的数据都会通过攻击者的机器，因此存在极大的安全隐患。



主机 B ARP 映射表	
IP 地址	MAC 地址
192.168.1.1	01-01-01-01-01-01

主机 C ARP 映射表	
IP 地址	MAC 地址
192.168.1.1	01-01-01-01-01-01

IP： 192.168.1.1
MAC： 01-01-01-01-01-01

IP： 192.168.1.2
MAC： 02-02-02-02-02-02

IP： 192.168.1.3
MAC： 03-03-03-03-03-03

主机 A ARP 映射表

IP 地址	MAC 地址
192.168.1.2	02-02-02-02-02-02

主机 B ARP 映射表

IP 地址	MAC 地址
192.168.1.1	01-01-01-01-01-01

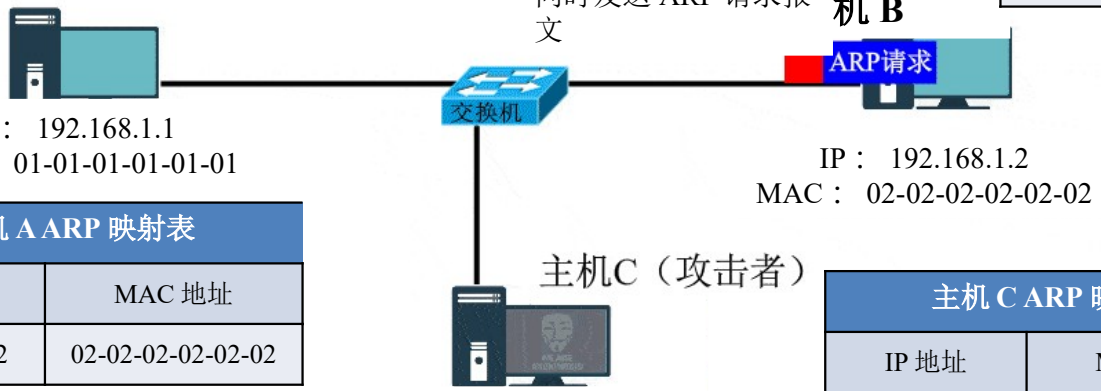
主机 C ARP 映射表

IP 地址	MAC 地址
192.168.1.1	01-01-01-01-01-01

03

应用拓展

信息收集



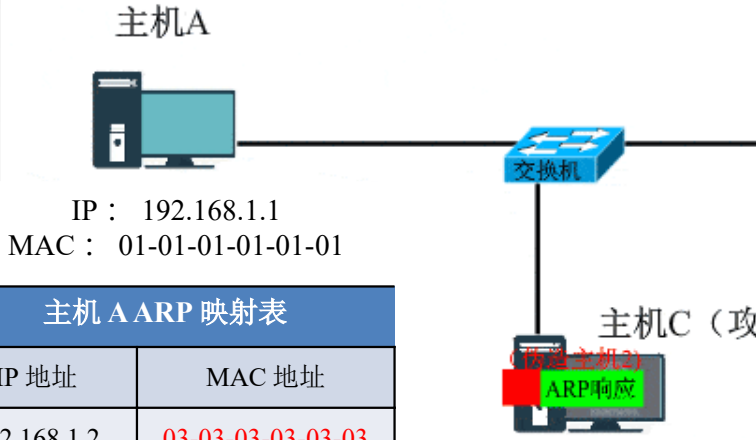
主机 B ARP 映射表	
IP 地址	MAC 地址
192.168.1.1	01-01-01-01-01-01

主机 A ARP 映射表	
IP 地址	MAC 地址
192.168.1.2	02-02-02-02-02-02

主机 C ARP 映射表	
IP 地址	MAC 地址
192.168.1.1	01-01-01-01-01-01
192.168.1.2	02-02-02-02-02-02

应用拓展

伪造 ARP 响应报文

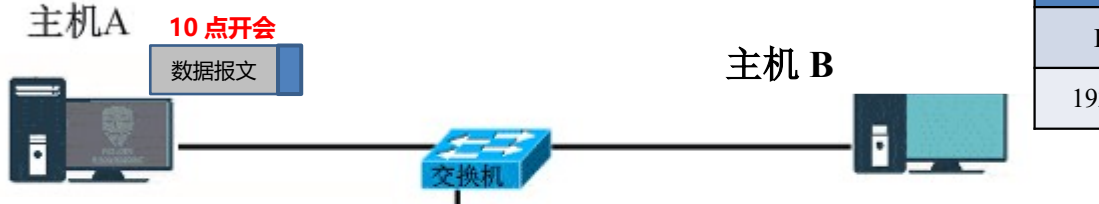


主机 B ARP 映射表	
IP 地址	MAC 地址
192.168.1.1	01-01-01-01-01-01

主机 A ARP 映射表	
IP 地址	MAC 地址
192.168.1.2	03-03-03-03-03-03

主机 C ARP 映射表	
IP 地址	MAC 地址
192.168.1.1	01-01-01-01-01-01
192.168.1.2	02-02-02-02-02-02

进行 ARP 欺骗



IP： 192.168.1.1
MAC： 01-01-01-01-01-01

IP： 192.168.1.2
MAC： 02-02-02-02-02-02

主机 C （攻击者）

10 点开会
数据报文

IP： 192.168.1.3
MAC： 03-03-03-03-03-03

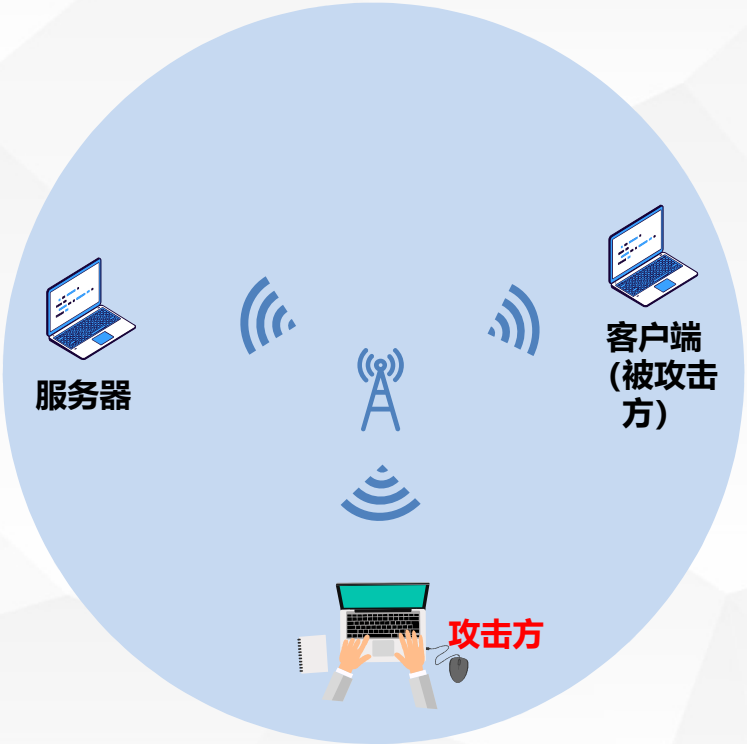
主机 A ARP 映射表	
IP 地址	MAC 地址
192.168.1.2	03-03-03-03-03-03

主机 B ARP 映射表	
IP 地址	MAC 地址
192.168.1.1	01-01-01-01-01-01

主机 C ARP 映射表	
IP 地址	MAC 地址
192.168.1.1	01-01-01-01-01-01
192.168.1.2	02-02-02-02-02-02

03

应用场景实战



03

应用场景实战

组员 1 任务

- 服务器
  - 创建 FTP 或 Web 站点
  - 设置 FTP 访问的账号密码
  - 设置 Web 登录的账号密码

组员 2 任务

- 客户端
  - 使用账号密码访问 FTP 或 Web
  - 查看 ARP 映射表
  - 抓包查看数据包的流向

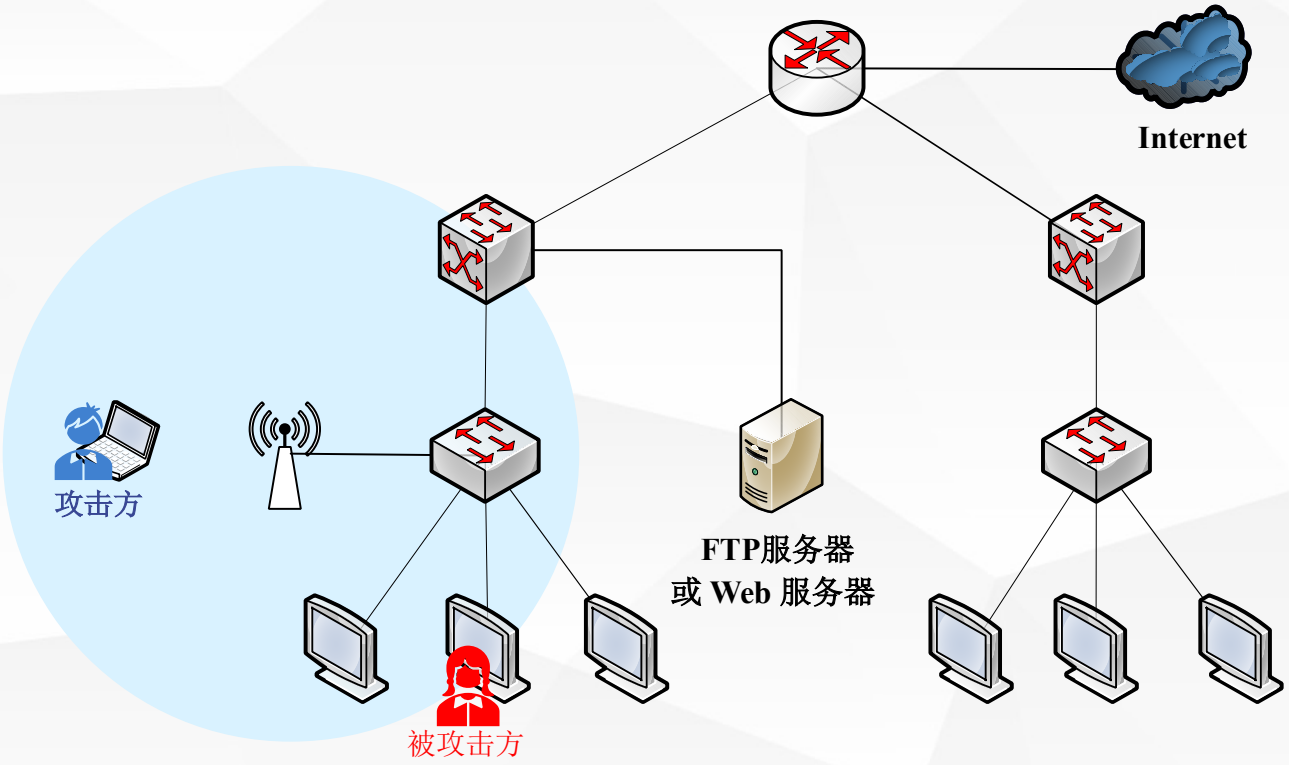
组员 3 任务

- 攻击方
  - 扫描局域网中的 MAC 地址
  - 选择服务器和客户端进行攻击
  - 查看截获的用户名和密码

提出并验证防御方案

03

案例回顾



04

思考启示

IPv6 中取代了 ARP 协议的 NDP 协议是否存在此安全风险？如果存在，应当如何防御？

05

作业

- 团队合作完成实验，记录实验过程数据（截图、命令、抓包等）；
- 组长提交实验报告，详细记录实验过程，提出解决方案并思考问题。
- 完成小组自评、组间互评和课后讨论。