

第五章 网络层

地址解析协议

ARP

ARP — Address Resolution Protocol

ARP is defined in
RFC 826

任务

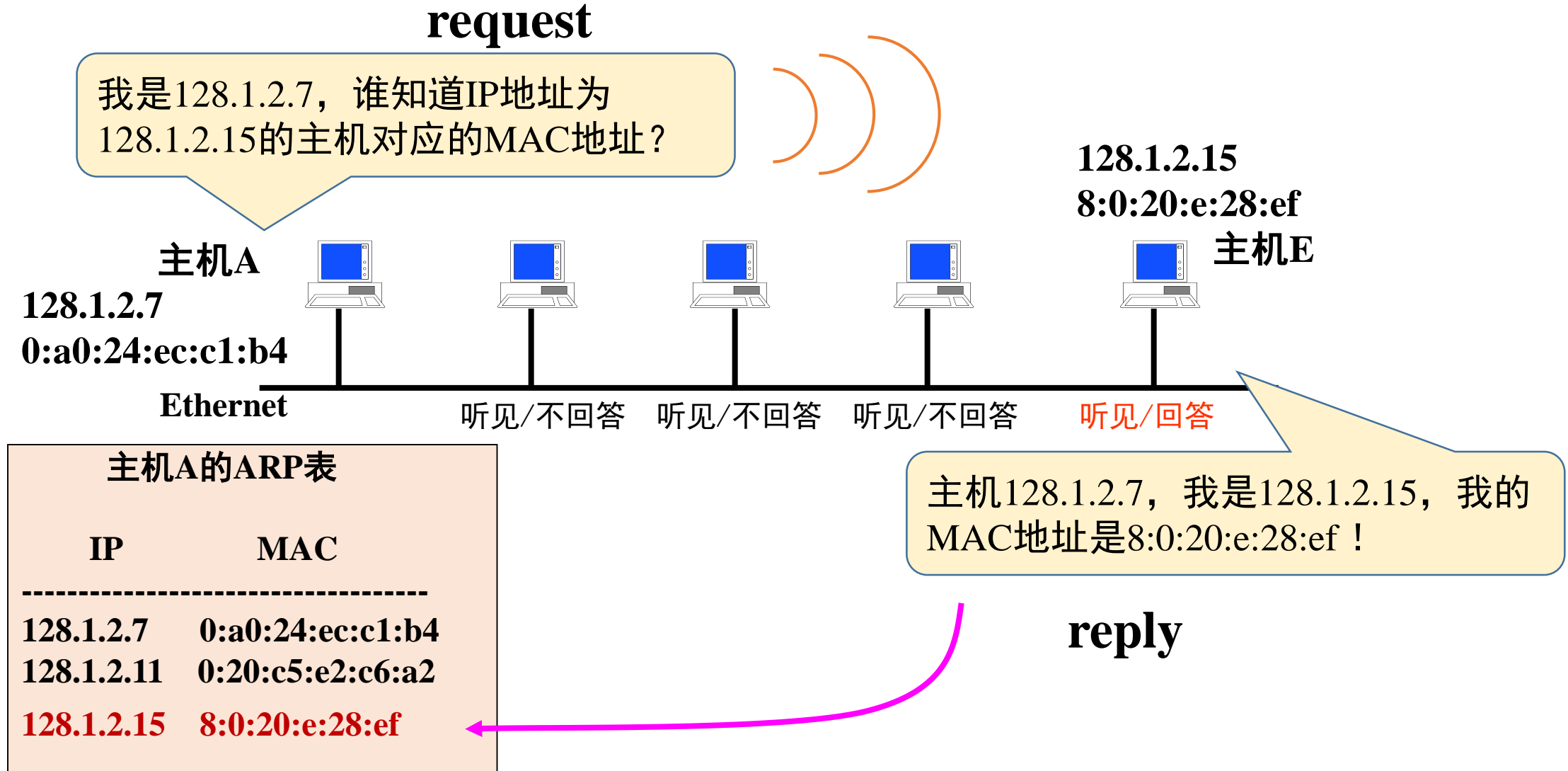
找到一个给定IP地址所对应的MAC地址



为什么需要地址解析



ARP的工作原理



ARP请求 (Request)

先导	11	目的地址	源地址	类型	数据	校验和
----	----	------	-----	----	----	-----

Packet 10 arrived at 8:23:43.75
Packet size=42 bytes
Destination=ff:ff:ff:ff:ff:ff
Source= 0:a0:24:ec:c1:b4
Ethertype=0806(ARP)

Hardware type=1
Protocol type=0800(IP)
Length of hardware address=6 bytes
Length of protocol address=4 bytes
Opcode 1 (ARP Request)
Sender's HD address= 0:a0:24:ec:c1:b4
Sender's IP address= 128.1.2.7
Target HD address= ?
Target IP address= 128.1.2.15

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help



Filter: arp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
100	14.031477	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.191? Tell 202.38.254.254
101	14.376052	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.243? Tell 202.38.254.254
102	14.434828	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.177? Tell 202.38.254.254
103	14.436926	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.206? Tell 202.38.254.254
104	14.531717	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.242? Tell 202.38.254.254
105	16.457350	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.197? Tell 202.38.254.254
109	16.884609	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.248? Tell 202.38.254.254

+ Frame 104: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

- Ethernet II, Src: Cisco_67:8c:00 (00:12:44:67:8c:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

+ Destination: Broadcast (ff:ff:ff:ff:ff:ff)

+ Source: Cisco_67:8c:00 (00:12:44:67:8c:00)

Type: ARP (0x0806)

Trailer: 00000000000000000000000000000000

- Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IP (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

[Is gratuitous: False]

Sender MAC address: Cisco_67:8c:00 (00:12:44:67:8c:00)

Sender IP address: 202.38.254.254 (202.38.254.254)

Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)

Target IP address: 202.38.254.242 (202.38.254.242)

```

0000  ff ff ff ff ff ff 00 12 44 67 8c 00 08 06 00 01  .... Dg.....
0010  08 00 06 04 00 01 00 12 44 67 8c 00 ca 26 fe fe  .... .. Dg...&..
0020  00 00 00 00 00 00 ca 26 fe f2 00 00 00 00 00 00  ....& .....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....

```

ARP回答 (Reply)

先导	11	目的地址	源地址	类型	数据	校验和
----	----	------	-----	----	----	-----

Packet 95 arrived at 8:44:21.15

Packet size=60 bytes

Destination= 0:a0:24:ec:c1:b4

Source= 8:0:20:e:28:ef

Ethertype=0806 (ARP)

Hardware type=1

Protocol type=0800(IP)

Length of hardware address=6 bytes

Length of protocol address=4 bytes

Opcode 2 (ARP Reply)

Sender's HD address= 8:0:20:e:28:ef

Sender's IP address= 128.1.2.15

Target HD address= 0:a0:24:ec:c1:b4

Target IP address= 128.1.2.7



Filter: arp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1888	26.303091	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.217? Tell 202.38.254.254
1893	26.544726	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.180? Tell 202.38.254.254
1900	27.663903	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.208? Tell 202.38.254.254
1901	28.269122	LgElectr_22:7e:d5	Broadcast	ARP	42	who has 202.38.254.254? Tell 202.38.254.155
1902	28.269723	Cisco_67:8c:00	LgElectr_22:7e:d5	ARP	60	202.38.254.254 is at 00:12:44:67:8c:00
1903	28.290843	LgElectr_22:7e:d5	Broadcast	ARP	42	who has 202.38.254.254? Tell 202.38.254.155
1904	28.291417	Cisco_67:8c:00	LgElectr_22:7e:d5	ARP	60	202.38.254.254 is at 00:12:44:67:8c:00
1905	28.331818	LgElectr_22:7e:d5	Broadcast	ARP	42	who has 202.38.254.254? Tell 202.38.254.155

+ Frame 1902: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

- Ethernet II, Src: Cisco_67:8c:00 (00:12:44:67:8c:00), Dst: LgElectr_22:7e:d5 (00:e0:91:22:7e:d5)

+ Destination: LgElectr_22:7e:d5 (00:e0:91:22:7e:d5)

+ Source: Cisco_67:8c:00 (00:12:44:67:8c:00)

Type: ARP (0x0806)

Trailer: 00000000000000000000000000000000

- Address Resolution Protocol (reply)

Hardware type: Ethernet (1)

Protocol type: IP (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2)

[Is gratuitous: False]

Sender MAC address: Cisco_67:8c:00 (00:12:44:67:8c:00)

Sender IP address: 202.38.254.254 (202.38.254.254)

Target MAC address: LgElectr_22:7e:d5 (00:e0:91:22:7e:d5)

Target IP address: 202.38.254.155 (202.38.254.155)

```

0000  00 e0 91 22 7e d5 00 12 44 67 8c 00 08 06 00 01  ...~... Dg.....
0010  08 00 06 04 00 02 00 12 44 67 8c 00 ca 26 fe fe  .... Dg...&..
0020  00 e0 91 22 7e d5 ca 26 fe 9b 00 00 00 00 00 00  ...~...& .....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....

```



怎样工作得更好？

- 为了让ARP的工作更加高效，下面是几种优化措施：
 - 缓存 ARP 结果
 - 在ARP请求中包括源机的 IP-to-MAC 地址的映射
 - 每台机器在启动的时候，广播它的IP-MAC地址对



免费ARP (Gratuitous ARP)

- 当一台主机启动时，发送要给一个免费ARP，（如果意外收到一个应答，即是IP地址发生了冲突）
- 当一个接口（interface）的配置发生了改变，会发送一个免费ARP

一台主机 (172.16.1.1, 0002 4A87 0D92) 发送的免费ARP

Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: FFFF.FFFF.FFFF		SRC MAC: 0002.4A87.0D92	
TYPE: 0x806	DATA (VARIABLE LENGTH)			FCS: 0x0	

ARP

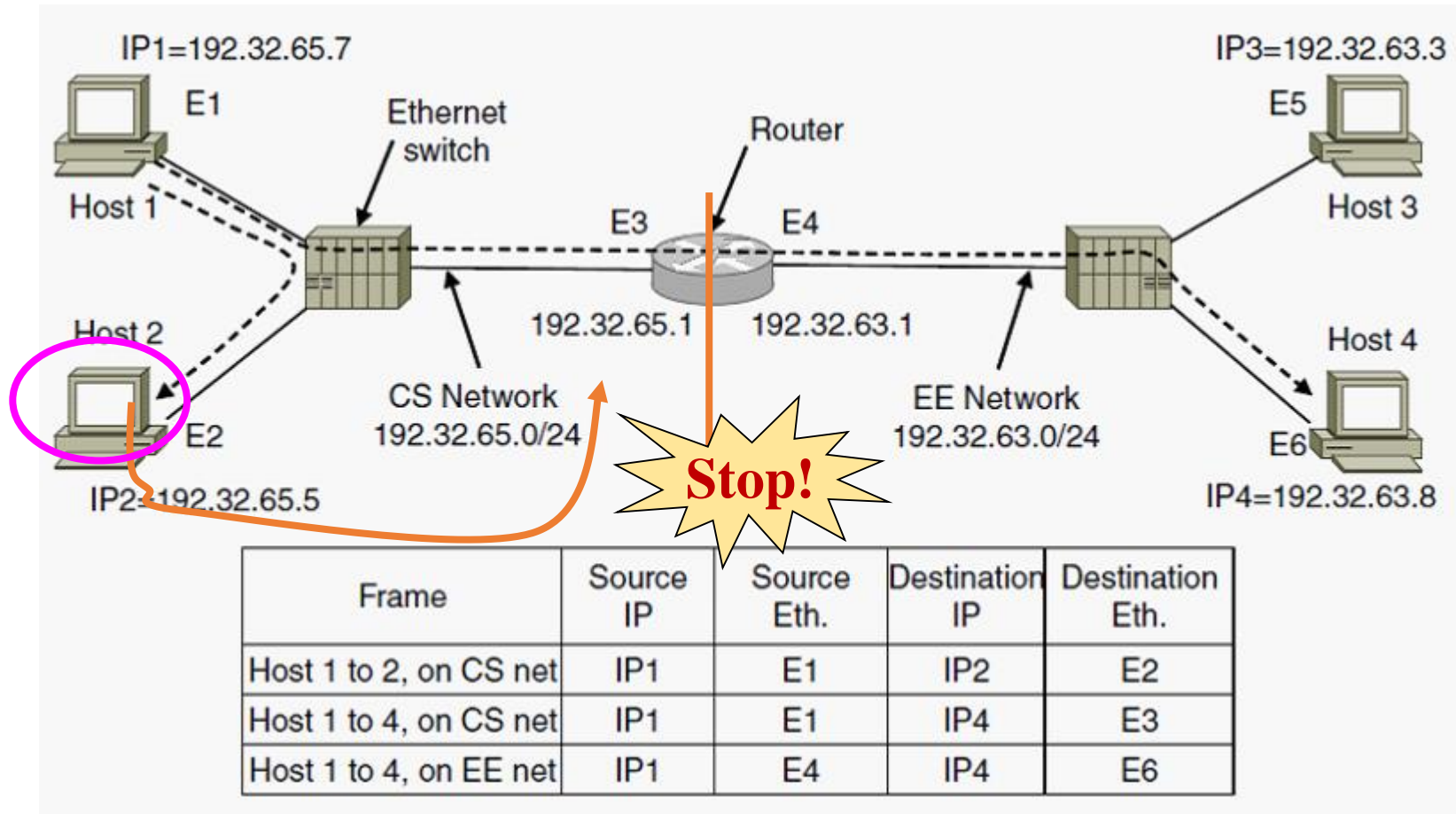
0	8	16	31 Bits
HARDWARE TYPE: 0x1		PROTOCOL TYPE:	
HLEN: 0x6	PLEN: 0x4	OPCODE: 0x1	
SOURCE MAC: 0002.4A87.0D92 (48 bits)		SOURCE IP (32 bits)	
172.16.1.1			
TARGET MAC: 0000.0000.0000 (48 bits)			
		TARGET IP: 172.16.1.1 (32 bits)	

Source IP
==
target IP



如果远程主机不在同子网呢？

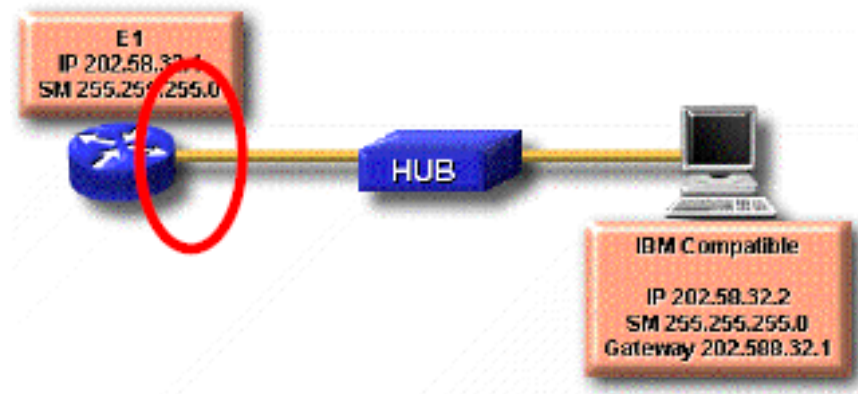
Host1 want to send packet to host4, but don't know its's MAC !





缺省网关（代理 ARP）

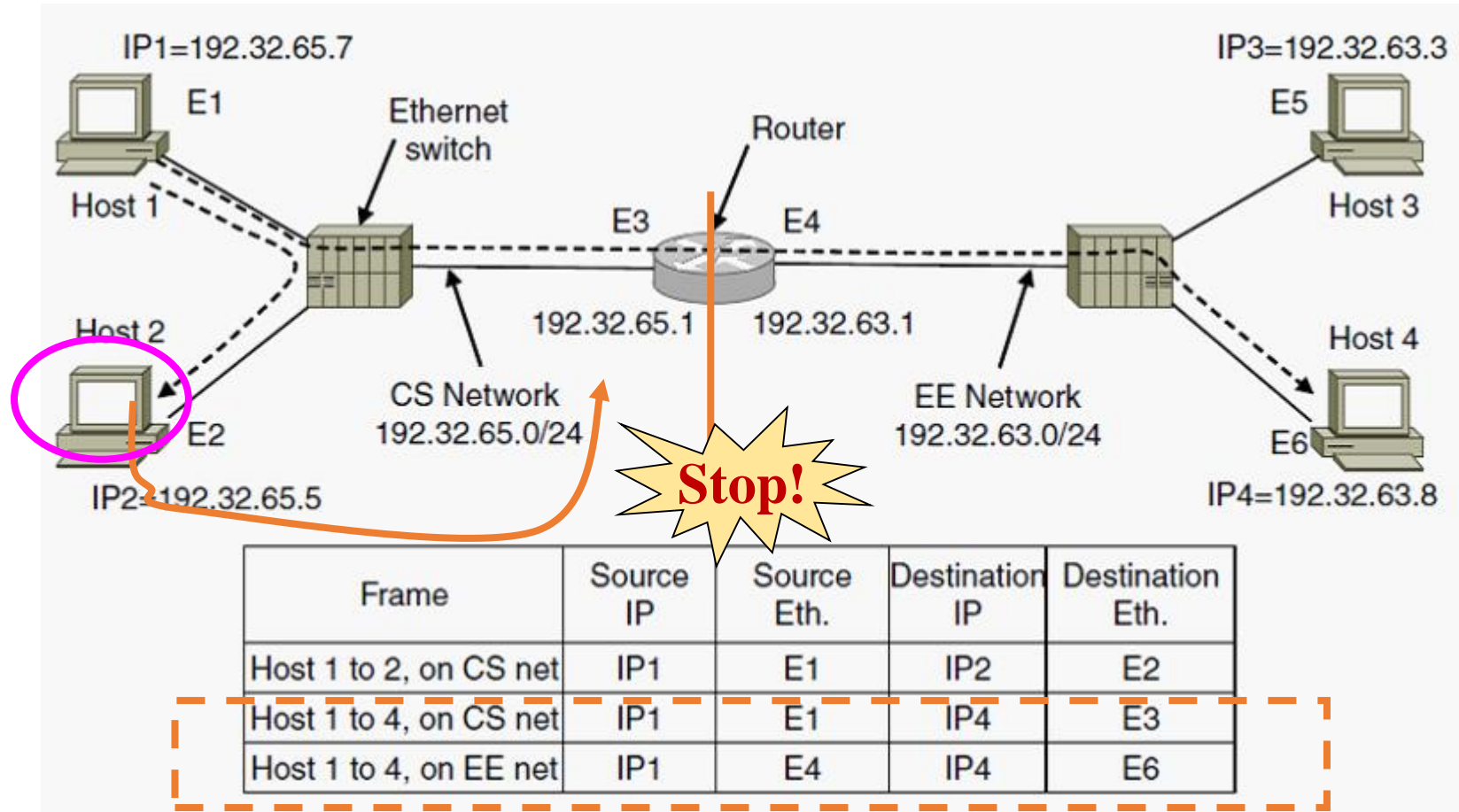
- 当源设备需要的目的地址与自己不在同一个网络时，如果源不知道目的MAC地址，它必须使用路由器的服务使它的数据达到目的，当路由器在这种方式下使用时，称为**缺省网关**。
- 缺省网关是与源设备所处的网段相连的路由器接口上的IP地址





如果远程主机不在同子网呢？

ARP Request: Target IP is 192.32.65.1(default gateway)





ARP table

- ❑ IP地址到MAC地址的映射表。
- ❑ 为了减少ARP请求的次数，每个设备拥有自己的ARP表，包括路由器。
- ❑ 储存在存储器（RAM）中，自动维护。（掉电消失）



自动维护ARP表

通过广播ARP请求中的源设备信息添加更新表

利用自己的ARP请求之应答信息来添加、更新表

删除超过一定时限的信息



ARP工具程序

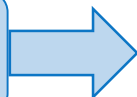


ARP.exe



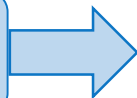
arpwatch

查看arp表内容



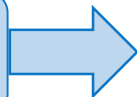
`arp -a`

删除arp表中指定的纪录



`Arp -d [IP 地址]`

添加记录

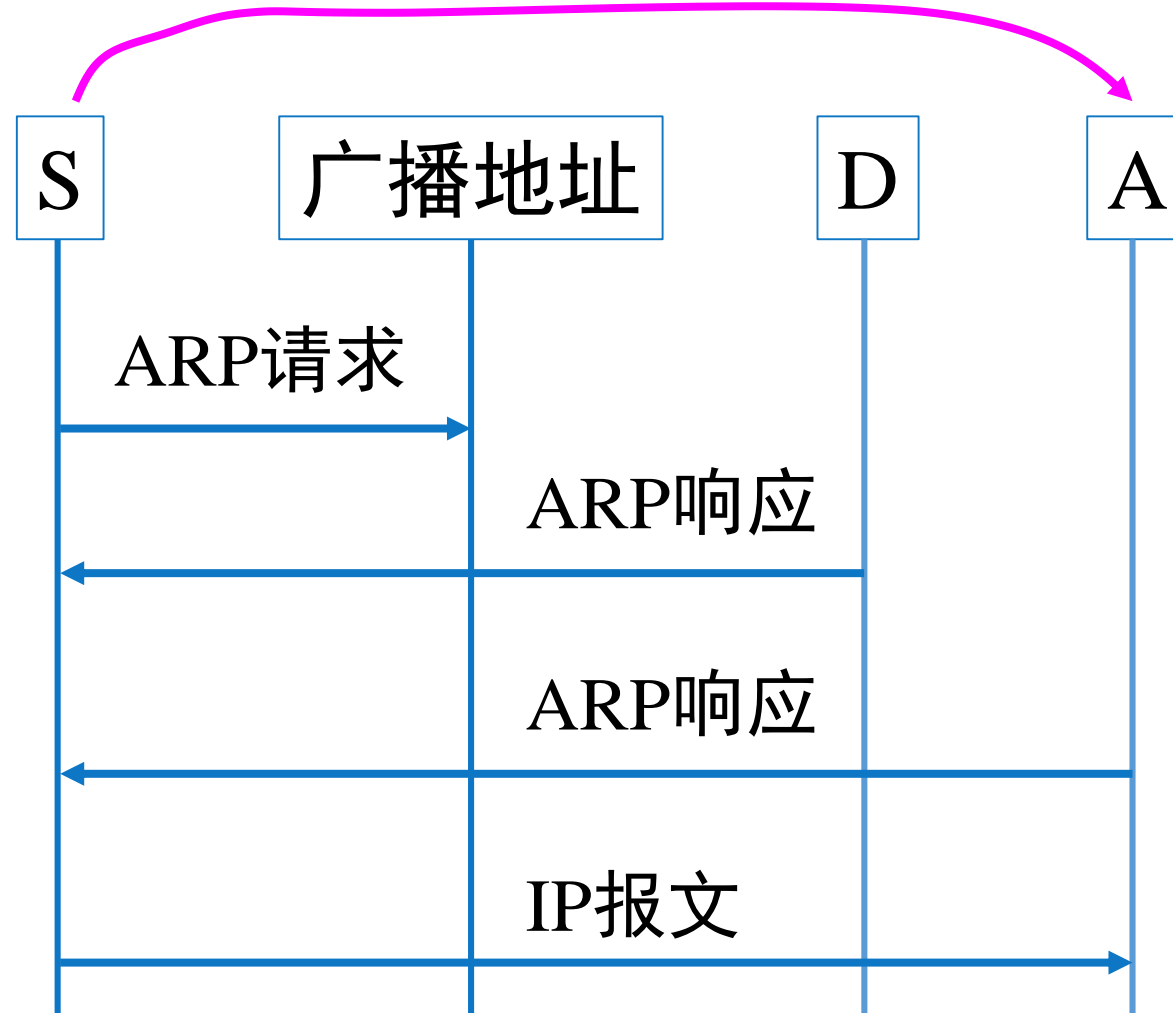


`Arp -s [IP地址] [MAC地址]`

什么是ARP 欺骗?

ARP spoofing /cheating

S want to communicate with D



怎样避免被ARP欺骗？

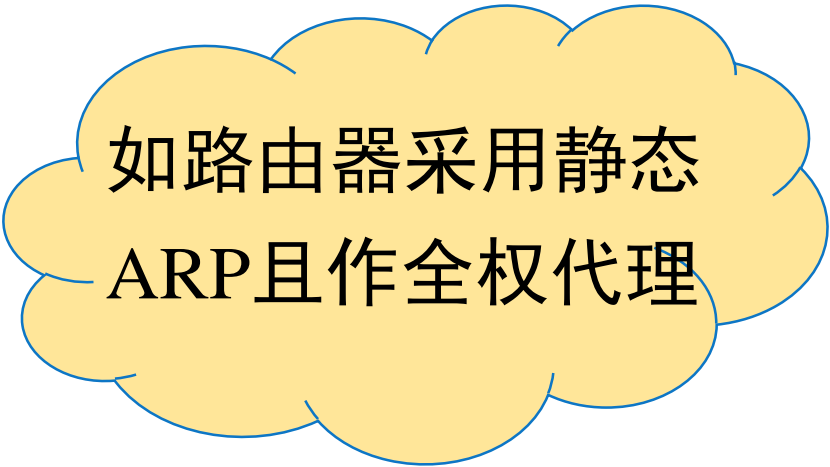
静态ARP

不马上写ARP缓存

设置ARP服务器

硬件屏蔽

⋮



如路由器采用静态
ARP且作全权代理



小结

- 当一台主机给对方发信息，只知道对方的IP地址，但却不知道对方的MAC地址，这时就要用到ARP
- 为了优化ARP工作，动态建立、更新和维护ARP表
 - 应答
 - ARP请求中的源IP/MAC地址信息
 - 免费ARP



小结

- 远程主机的MAC地址解析，需要用到默认网关
- ARP安全隐患

思考题

- ❑ ARP工作原理是怎样的？
- ❑ 远程主机的MAC地址如何解析？
- ❑ 如何维护ARP表？
- ❑ 什么是默认网关/缺省网关？
- ❑ ARP病毒是怎么产生的？

谢谢观看

致谢

本课程课件中的部分素材来自于：（1）清华大学出版社出版的翻译教材《计算机网络》（原著作者：Andrew S. Tanenbaum, David J. Wetherall）；（2）思科网络技术学院教程；（3）网络上搜到的其他资料。在此，对清华大学出版社、思科网络技术学院、人民邮电出版社、以及其它提供本课程引用资料的个人表示衷心的感谢！

对于本课程引用的素材，仅用于课程学习，如有任何问题，请与我们联系！