网络安全——

网络攻击—ARP攻击

北京邮电大学

郑康锋

zkfbupt@163.com

嗅探技术

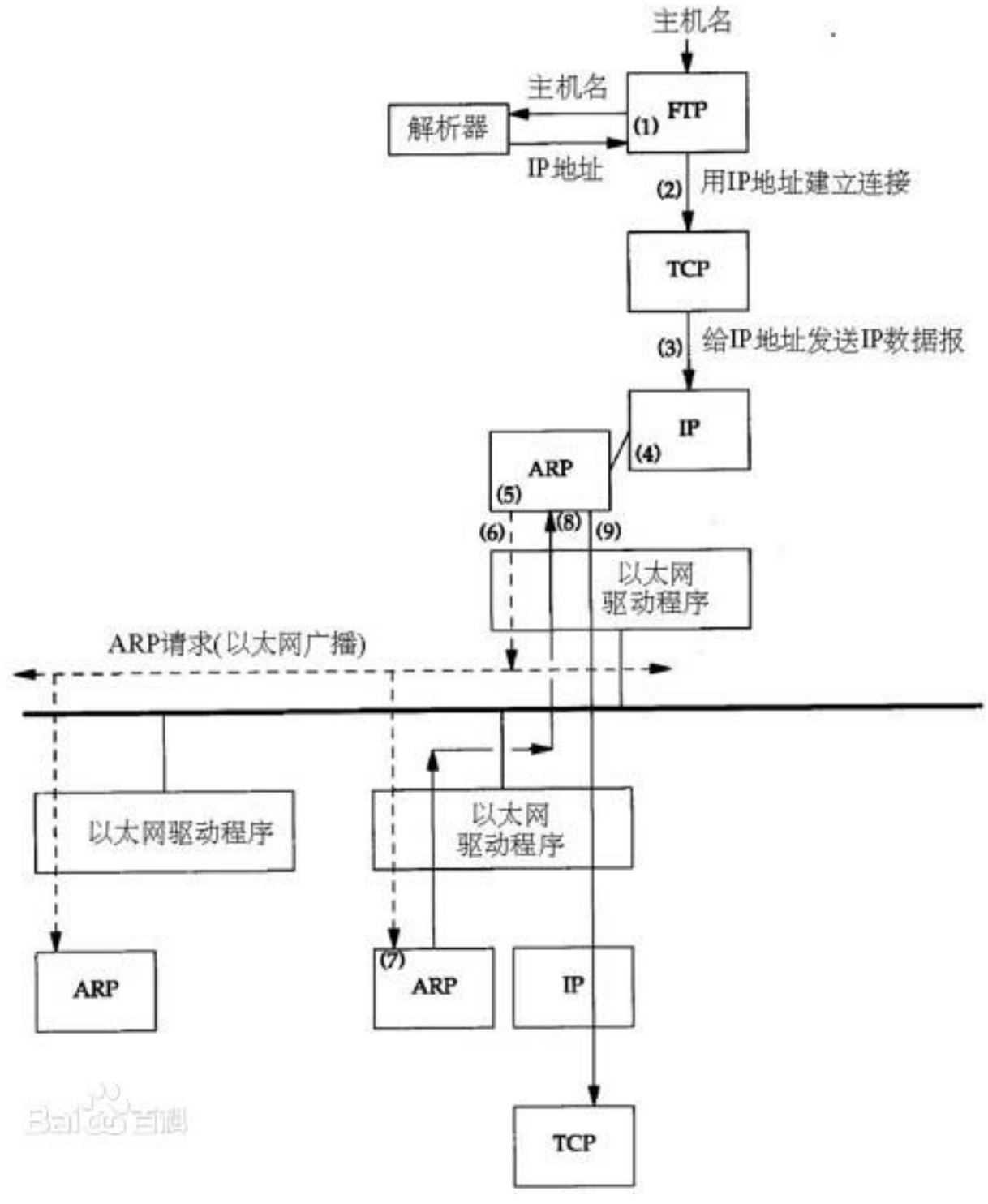
嗅探技术，是一种常用的收集有用数据信息的网络监听方法，是网络安全攻防技术中很重要的一种。

以太网嗅探。网卡一般具有四种接收工作模式：

- 广播（Broadcast）模式，可以接收局域网内目的地址为广播地址（全1地址）的所有数据报；
- 多播（Multicast）模式，可以接收目的地址为多播地址的所有数据报；
- 直接（Directory）模式，也就是单播（Unicast）模式，只接收目的地址为本机MAC地址的所有数据报；
- 混杂（Promiscuous）模式，能够接收通过网卡的所有数据报。

ARP协议

- 地址解析协议，即ARP（Address Resolution Protocol），是根据IP地址获取物理地址的一个TCP/IP协议。



注：资料及图片来自于百度百科。

ARP协议

ARP协议的几点解释：

- 网络通信一般以IP地址为源、目的地址，但工作在数据链路层的交换机、网卡等并不能识别IP地址,需要获取MAC地址才能通信。

- 主机设有一个ARP高速缓存，存放局域网中主机的IP地址和MAC地址对。当两台主机进行通信时，通过查询ARP缓存表来进行IP地址到MAC地址的转换。缓存表中不存在查找项时，运行ARP广播查找目标主机的MAC地址。

- ARP缓存表中的每一个映射地址项都有生存时间，进行定时更新。

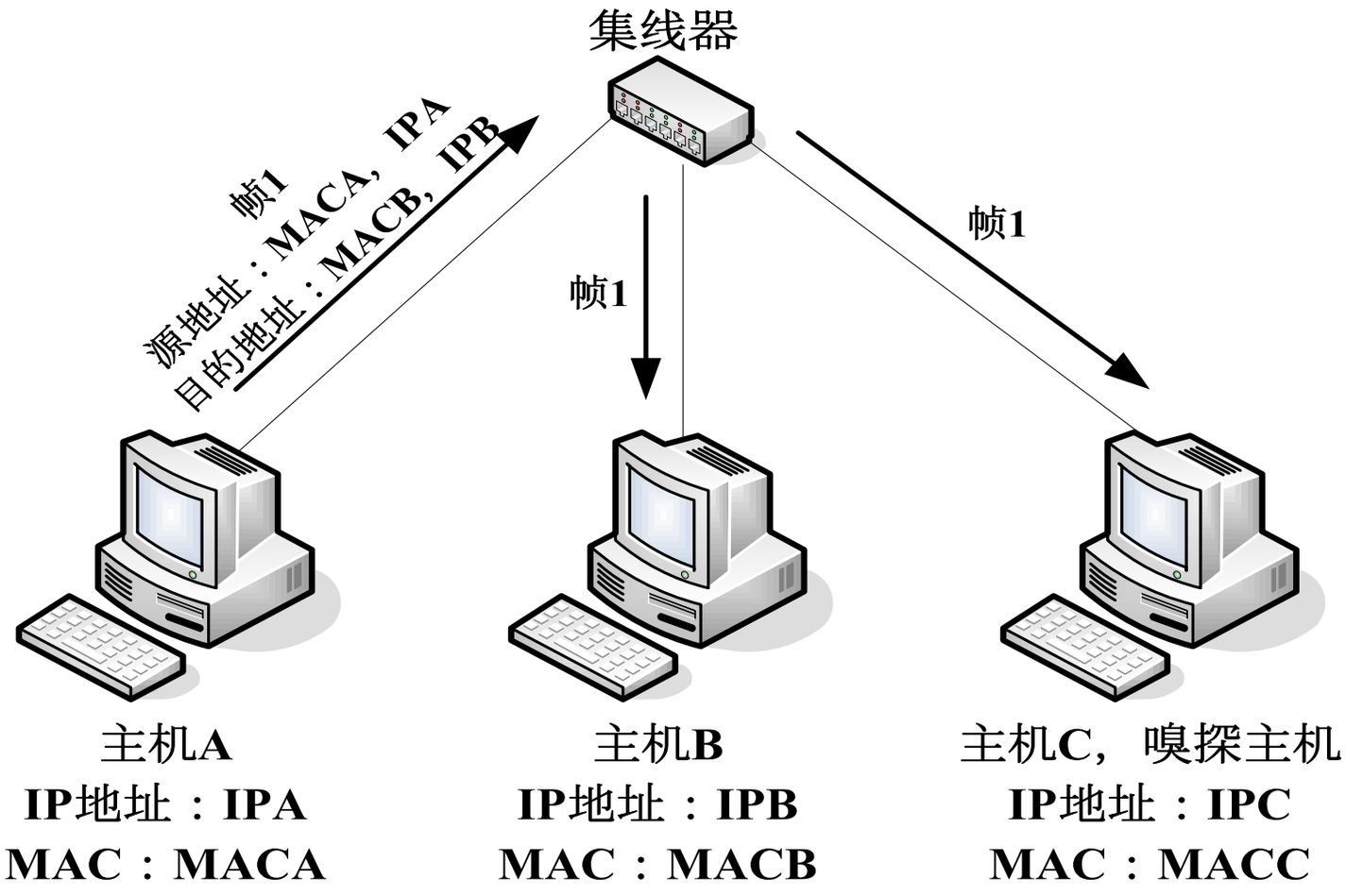
ARP协议

- HTYPE： the network protocol type. Example: Ethernet is 1.
- PTYPE：the internetwork protocol for which the ARP request is intended. For IPv4, this has the value 0x0800.
- OPER：the operation that the sender is performing: 1 for request, 2 for reply.
- SHA：MAC
- SPA：IP

Internet Protocol (IPv4) over Ethernet ARP packet		
octet offset	0	1
0	Hardware type (HTYPE)	
2	Protocol type (PTYPE)	
4	Hardware address length (HLEN)	Protocol address length (PLEN)
6	Operation (OPER)	
8	Sender hardware address (SHA) (first 2 bytes)	
10	(next 2 bytes)	
12	(last 2 bytes)	
14	Sender protocol address (SPA) (first 2 bytes)	
16	(last 2 bytes)	
18	Target hardware address (THA) (first 2 bytes)	
20	(next 2 bytes)	
22	(last 2 bytes)	
24	Target protocol address (TPA) (first 2 bytes)	
26	(last 2 bytes)	

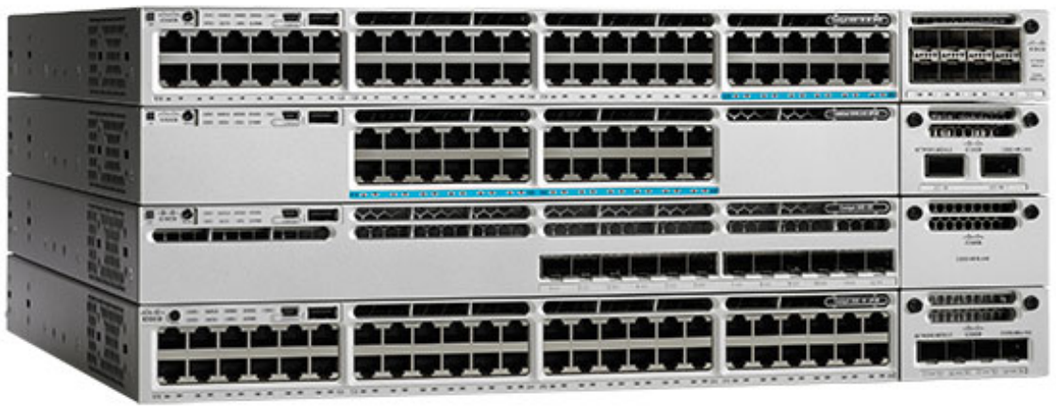
注：资料及图片来自于维基百科。

嗅探技术



- 网卡被设置成**混杂模式**时，无论监听到的数据帧目的地址如何，网卡能接收所有达到自身的数据。

交换机



交换机

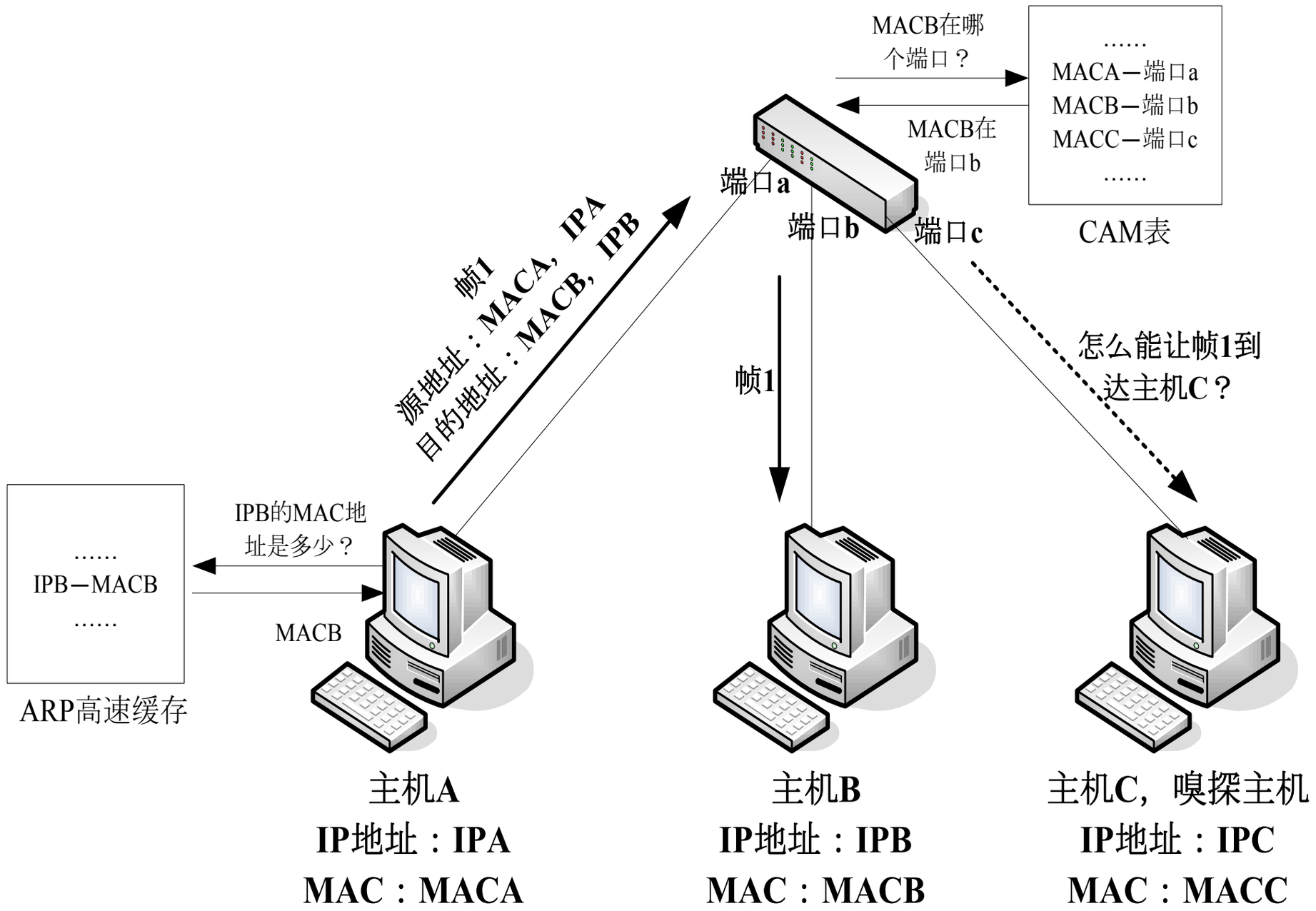
交换机（Switch）意为“开关”是一种用于电（光）信号转发的网络设备。它可以为接入交换机的任意两个网络节点提供独享的电信号通路。最常见的交换机是以太网交换机。

- 交换机工作于OSI参考模型的第二层，即数据链路层。交换机内部的CPU会在每个端口成功连接时，通过将MAC地址和端口对应，形成一张MAC表。

- 在通讯过程中，发往该MAC地址的数据包将仅送往其对应的端口，而不是所有的端口。

- 注：有二层交换机、三层交换机及四层交换机，本节只讨论二层交换机。三层交换机有MAC-IP映射。

ARP攻击技术


MACB在哪
个端口？
……
MACA—端口a
MACB—端口b
MACC—端口c
……
MACB在
端口b
CAM表
端口a
端口b
端口c
帧1
源地址：MACA，IPA
目的地址：MACB，IPB
帧1
怎么能让帧1到
达主机C？
IPB的MAC地
址是多少？
MACB
……
IPB—MACB
……
ARP高速缓存
主机A
IP地址：IPA
MAC：MACA
主机B
IP地址：IPB
MAC：MACB
主机C，嗅探主机
IP地址：IPC
MAC：MACC

ARP攻击技术

- **在交换式网络环境下，通信参与者有三个：**
  - 通信双方A和B
  - 交换机S
  - 攻击者C

- **要想达到嗅探的目的，可以有三个攻击点，（1）交换机S，（2）目标主机A和B，（3）自己C。**

ARP攻击技术

- **发送大量虚假MAC地址数据报**
  - 交换机虽然可以维护一张端口-MAC的地址映射表，但是由于交换机内存有限，地址映射表的大小也就有限。
  - 如果主机C发送大量虚假MAC地址的数据报，快速填满地址映射表。交换机在地址映射表被填满后，就会像HUB一样以广播方式处理数据报。
  - 这种方法不适合采用静态地址映射表的交换机，而且也不是所有交换机都采用这种转发处理方式。

ARP攻击技术

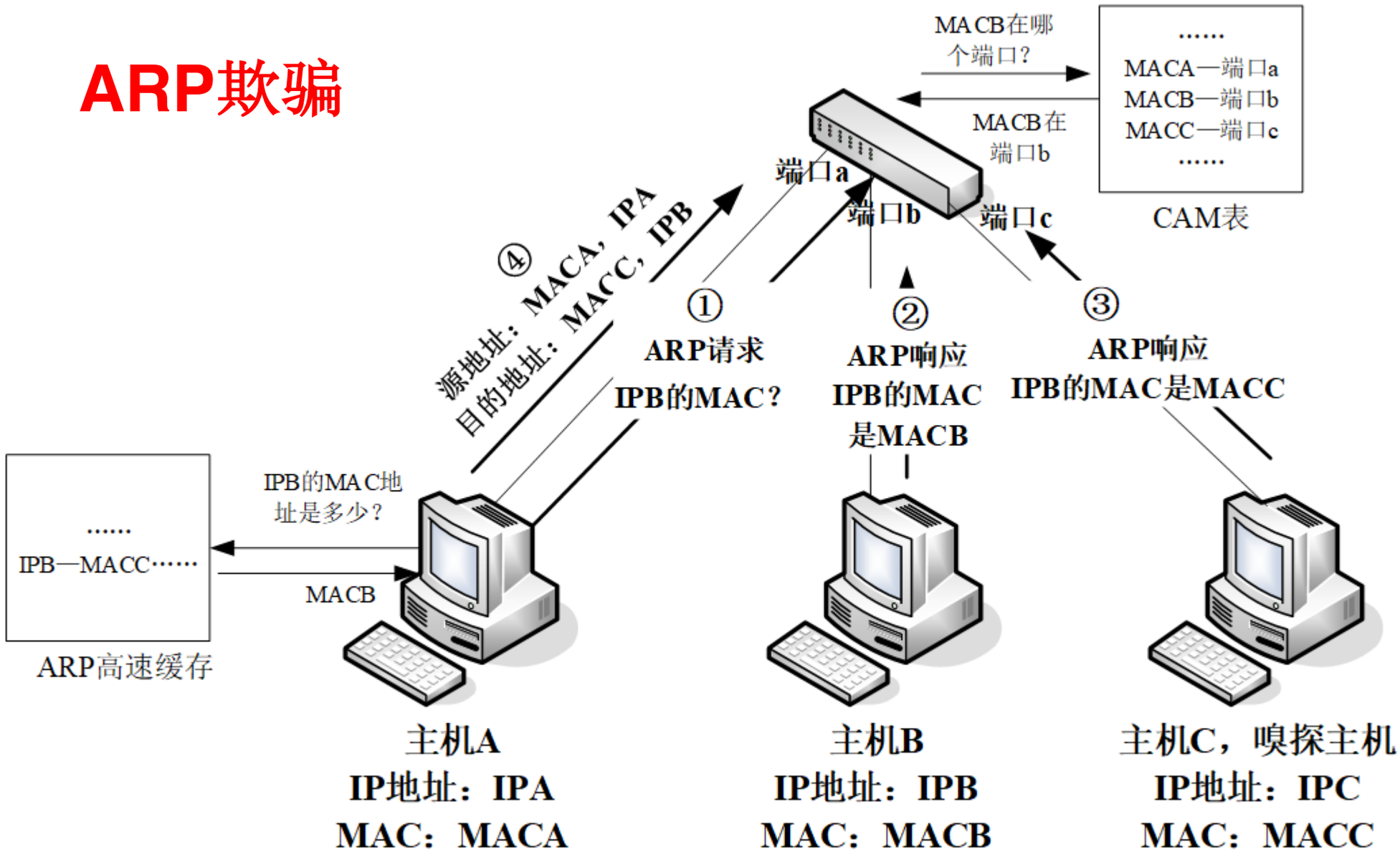
- **ARP欺骗**

  - ARP欺骗利用修改主机ARP缓存表的方法达到嗅探的目的，是一种中间人攻击。主机C为了达到嗅探的目的，会向主机A和主机B分别发送ARP应答包，告诉它们IP地址为IPB的主机MAC地址为MACC，IP地址为IPA的主机MAC地址为MACC。

  - 这样，主机A和主机B的ARP缓存中就会有IPB—MACC和IPA—MACC的记录。这样，主机A和主机B的通信数据都流向了主机C，主机C只要再发送到其真正的目的地就可以了。当然ARP缓存表项是动态更新的（一般为两分钟），如果没有更新信息，ARP映射项会自动删除。所以，主机C在监听过程中，还要不断地向主机A和主机B发送伪造的ARP应答包。

ARP攻击技术

- **ARP欺骗**



ARP攻击技术

- **修改本地MAC地址**

  - 也可以通过修改本地MAC地址为目标主机MAC地址来实现嗅探。把主机C的MAC地址修改为目标主机B的MAC地址，交换机会将MACB和端口c对应起来。

  - 在以后收到目的地址为MACB的数据报后，交换机会将包从端口c发送出去。这样就达到了监听的目的。

  - 但同样地，这种方法只适用于动态生成地址映射表的交换机，并且没有采用其它策略。

ARP攻击溯源

- **方法一：捕包分析**

  - 在网络内任意一台主机上运行抓包软件，捕获所有到达本机的数据包。如果发现有某个IP不断发送ARP　Request请求包，那么这台电脑一般就是病毒源。

  - 原理：无论何种ARP病毒变种，行为方式有两种，一是欺骗网关，二是欺骗网内的所有主机。最终的结果是，在网关的ARP缓存表中，网内所有活动主机的MAC地址均为中毒主机的MAC地 址；网内所有主机的ARP缓存表中，网关的MAC地址也成为中毒主机的MAC地址。前者保证了从网关到网内主机的数据包被发到中毒主机，后者相反，使得主机发往网关的数据包均发送到中毒主机。

ARP攻击溯源

- **方法二：**使用arp-a命令任意选两台不能上网的主机，在DOS命令窗口下运行arp-a命令。例如在结果中，两台电脑除了网关的IP，MAC地址对应 项，都包含了192.168.0.186的这个IP，则可以断定192.168.0.186这台主机就是病毒源。

- 原理：一般情况下，网内的主机只和网关通 信。正常情况下，一台主机的ARP缓存中应该只有网关的MAC地址。如果有其他主机的MAC地址，说明本地主机和这台主机最后有过数据通信发生。如果某台 主机（例如上面的192.168.0.186）既不是网关也不是服务器，但和网内的其他主机都有通信活动，且此时又是ARP病毒发作时期，那么，病毒源也 就是它了。

ARP攻击溯源

- 方法三：使用tracert命令在任意一台受影响的主机上，在DOS命令窗口下运行如下命令：tracert61.135.179.148。

- 假定设置的缺省网关为10.8.6.1，在跟踪一个外网地址时，第一跳却是10.8.6.186，那么，10.8.6.186就是病毒源。

- 原理：中毒主机在受影响主机 和网关之间，扮演了“中间人”的角色。所有本应该到达网关的数据包，由于错误的MAC地址，均被发到了中毒主机。此时，中毒主机越俎代庖，起了缺省网关的 作用。

ARP攻击防御方法

- 方法一：减少过期时间

#ndd –set /dev/arp arp_cleanup_interval 60000

#ndd -set /dev/ip ip_ire_flush_interval 60000

60000=60000毫秒 默认是300000

- 加快过期时间，并不能避免攻击，但是使得攻击更加困难，带来的影响是在网络中会大量的出现 ARP请求和回复，请不要在繁忙的网络上使用。

ARP攻击防御方法

- **方法二：建立静态ARP表**
- 这是一种很有效的方法，而且对系统影响不大。缺点是破坏了动态ARP协议。可以建立如下的文 件。

  test.nsfocus.com 08:00:20:ba:a1:f2

  user. nsfocus.com 08:00:20:ee:de:1f

- 使用arp –f filename加载进去，这样的ARP映射将不会过期和被新的ARP数据刷新，除非使用arp –d才能删除。但是一旦合法主机的网卡硬件地址改变，就必须手工刷新这个arp文件。这个方法，不适合于经常变动的网络环境。

ARP攻击防御方法

- **方法三：禁止ARP**

- 可以通过ipconfig interface –arp 完全禁止ARP，这样，网卡不会发送ARP和接受ARP包。但是使用前提是使用静态的ARP表，如果不在ARP表中的计算机，将不能通信。

- 这个方法不适用与大多数网络环境，因为这增加了网络管理的成本。但是对小规模的安全网络来说，还是有效可行的。

问题和讨论