局域网常见攻击

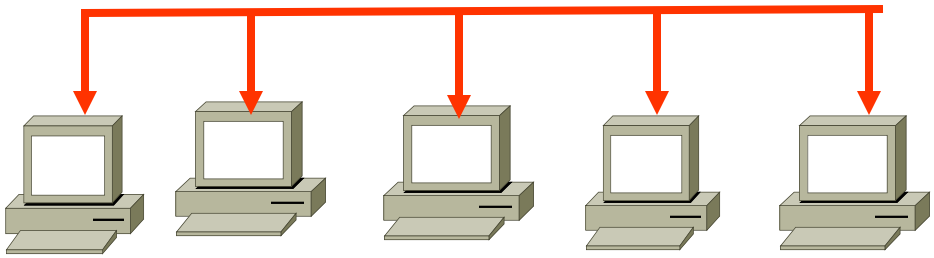
段海新
duanhx@tsinghua.edu.cn

Outline

1. 以太网工作原理
2. MAC Flood
3. MAC Spoofing
4. ARP Spoofing
5. DHCP attack

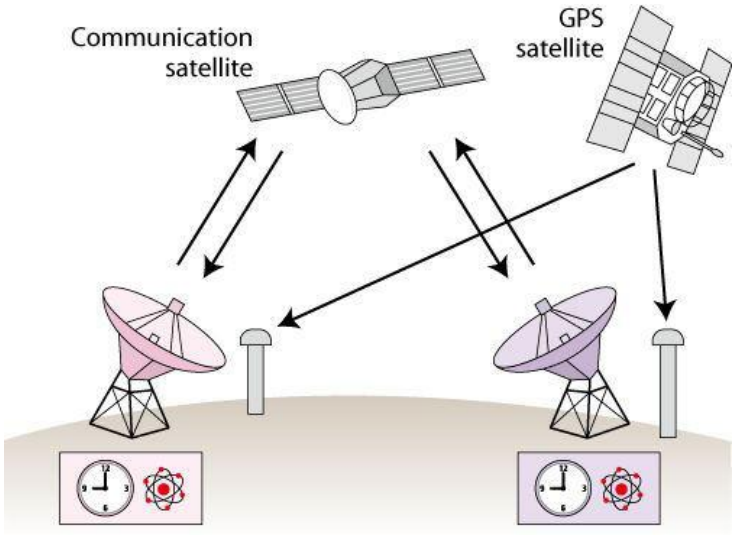
LAN with Broadcast Media

Cable



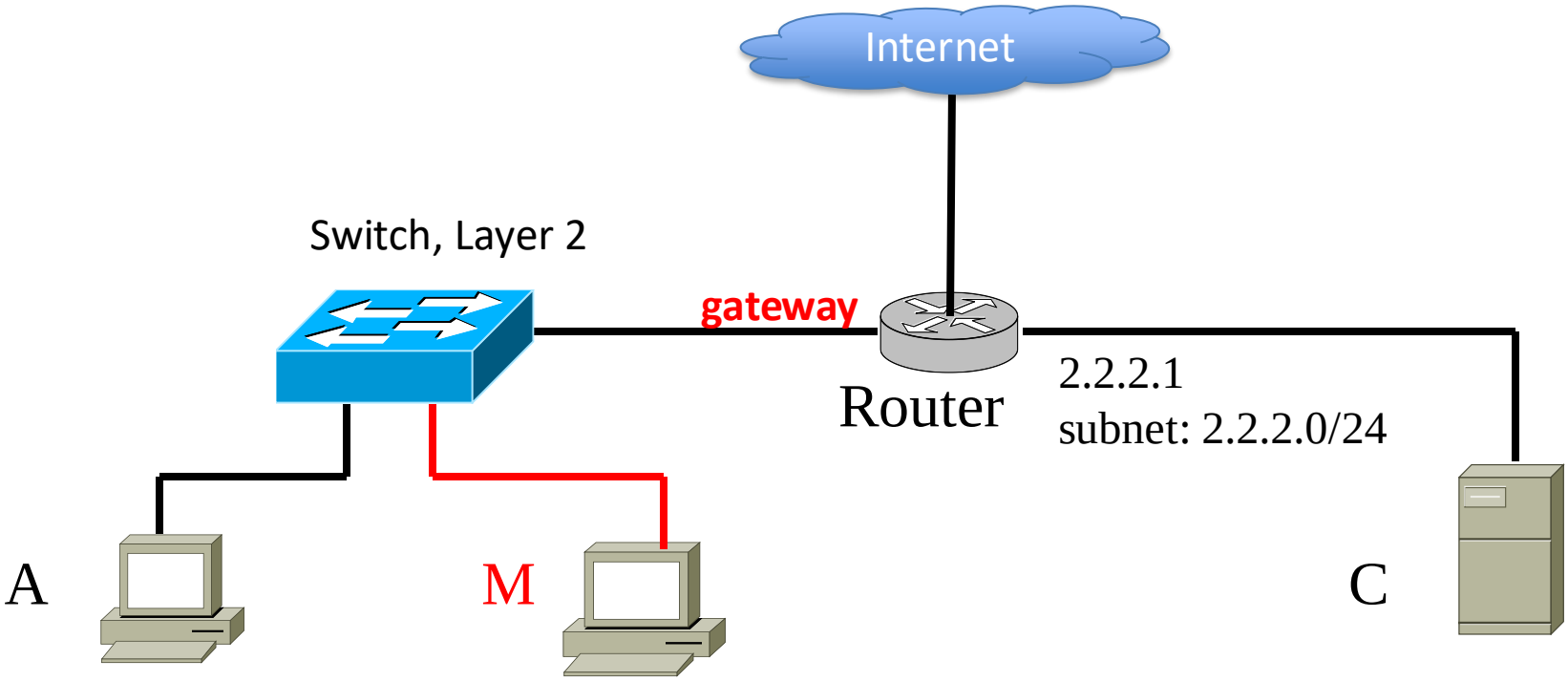
Wi-Fi, Mobile

Satellite



- Sniffer（监听）
- Spoof（假冒）
- Replay （重放）
- Injection（注入）

Local Area Network, EtherNet



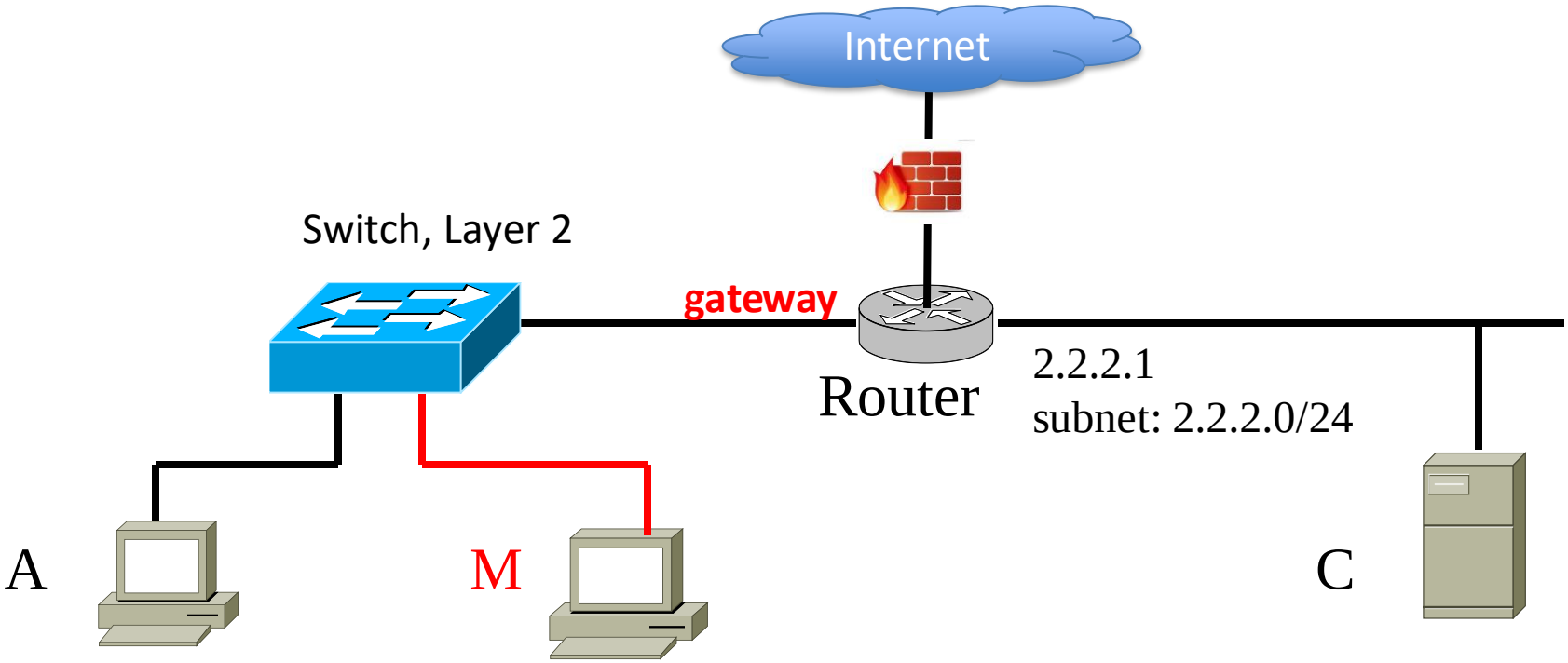
IP: 1.1.1.2
Subnet: 255.255.255.0
MAC: ABCDEF

IP: 1.1.1.3
Subnet: 255.255.255.0
MAC: ABCABC

IP: 2.2.2.20/24
MAC: ABCDDD

HostName: test.com

Local Area Network, EtherNet

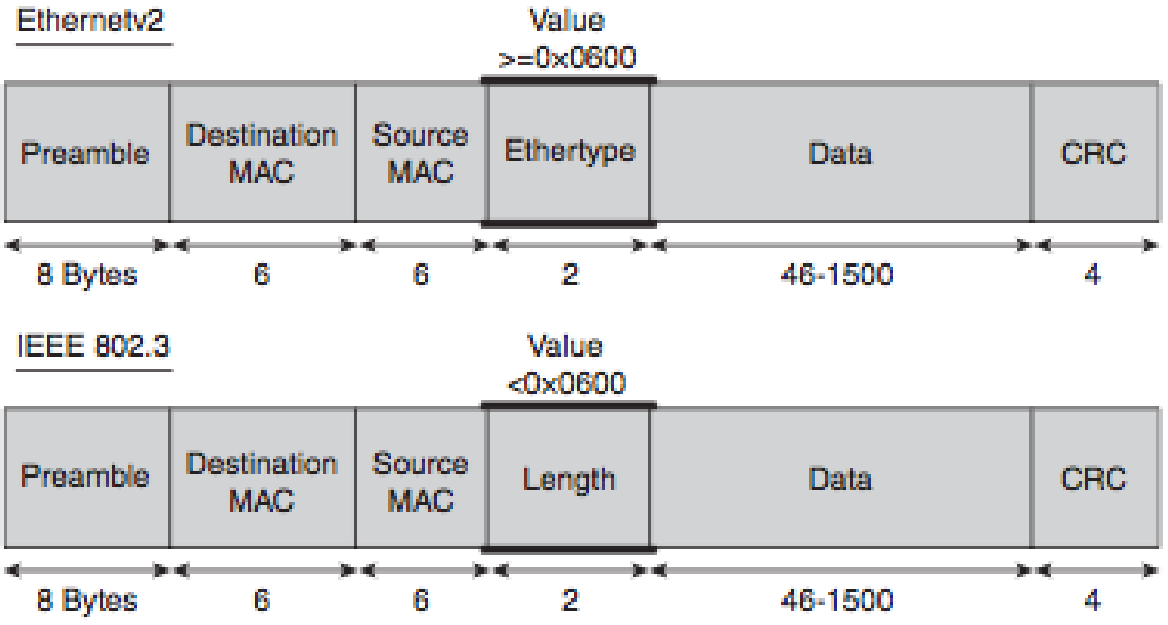


以太网帧结构

Ethernet Frame： 802.3 , Ethernet II, SNAP

http://standards.ieee.org/getieee802/802.3.html

Ethernet Frame Formats



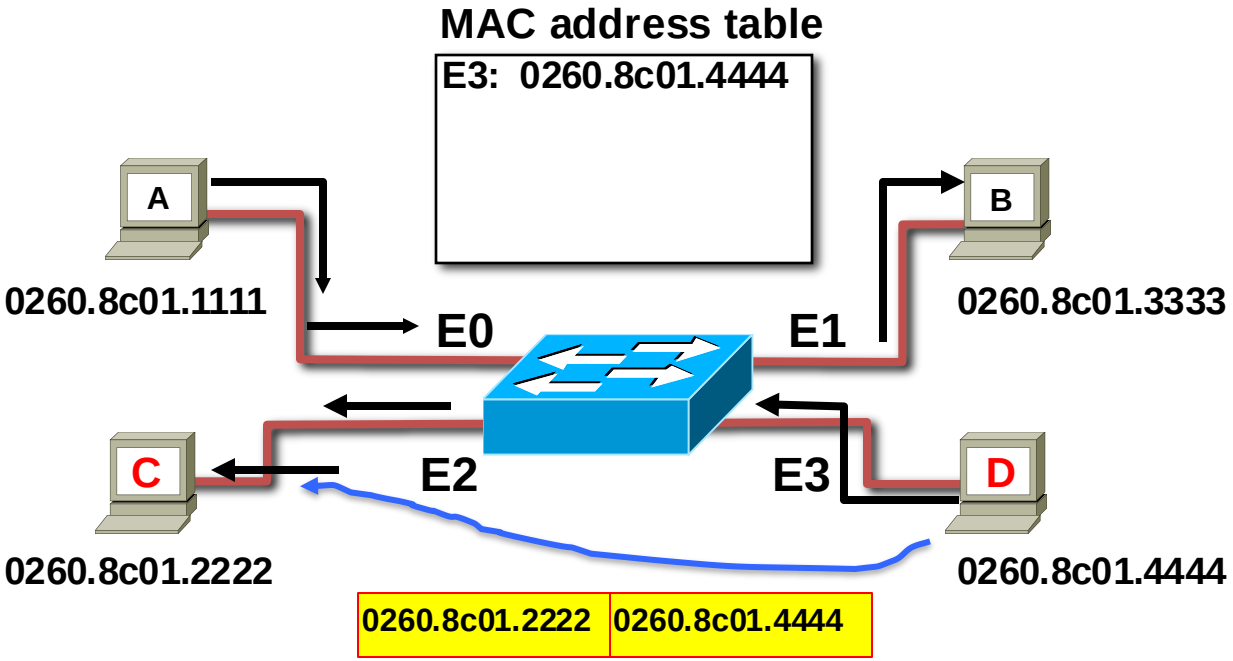
8c:2d:aa:4b:98:a7

Organizationally Unique Identifier (OUI) (the manufacturer)

Network Interface Controller-Specific (the serial number)

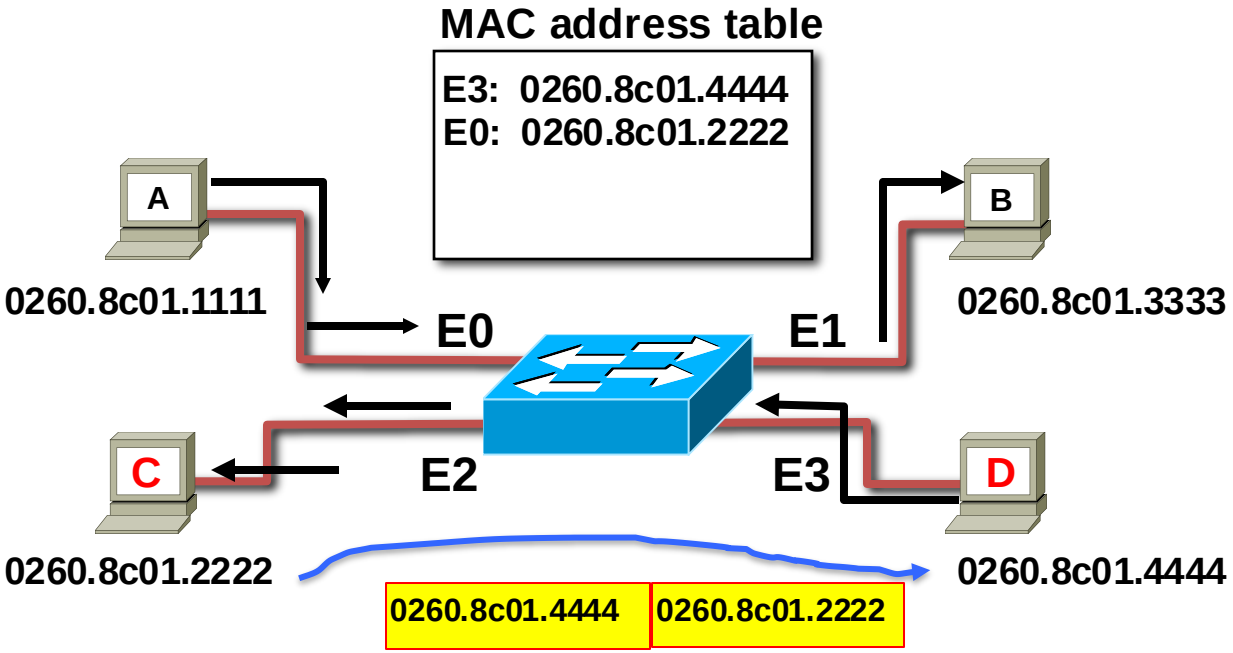
Broadcast： FF:FF:FF:FF:FF:FF

以太网交换机工作原理



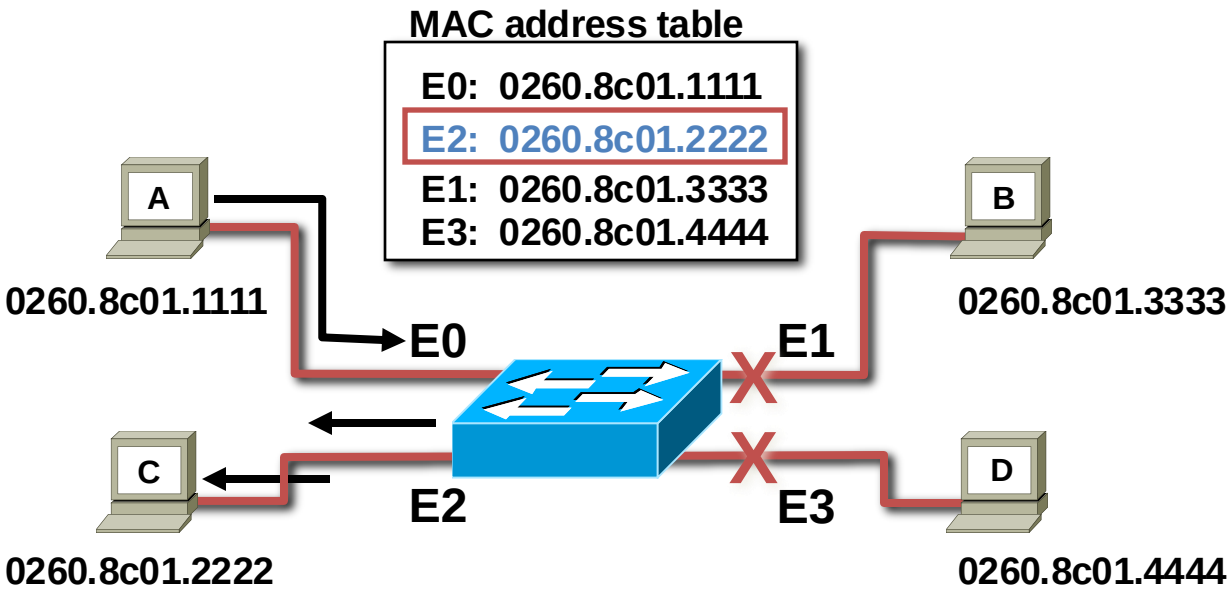
- D to C
- Switch caches station D MAC address to port E3 by learning the source Address of data frames
- The frame from station D to station C is flooded out to all ports except port E3 (unknown unicasts are flooded)
- (If a frame's destination MAC is FF-FF-FF-FF, it will be flooded)

以太网交换机工作原理



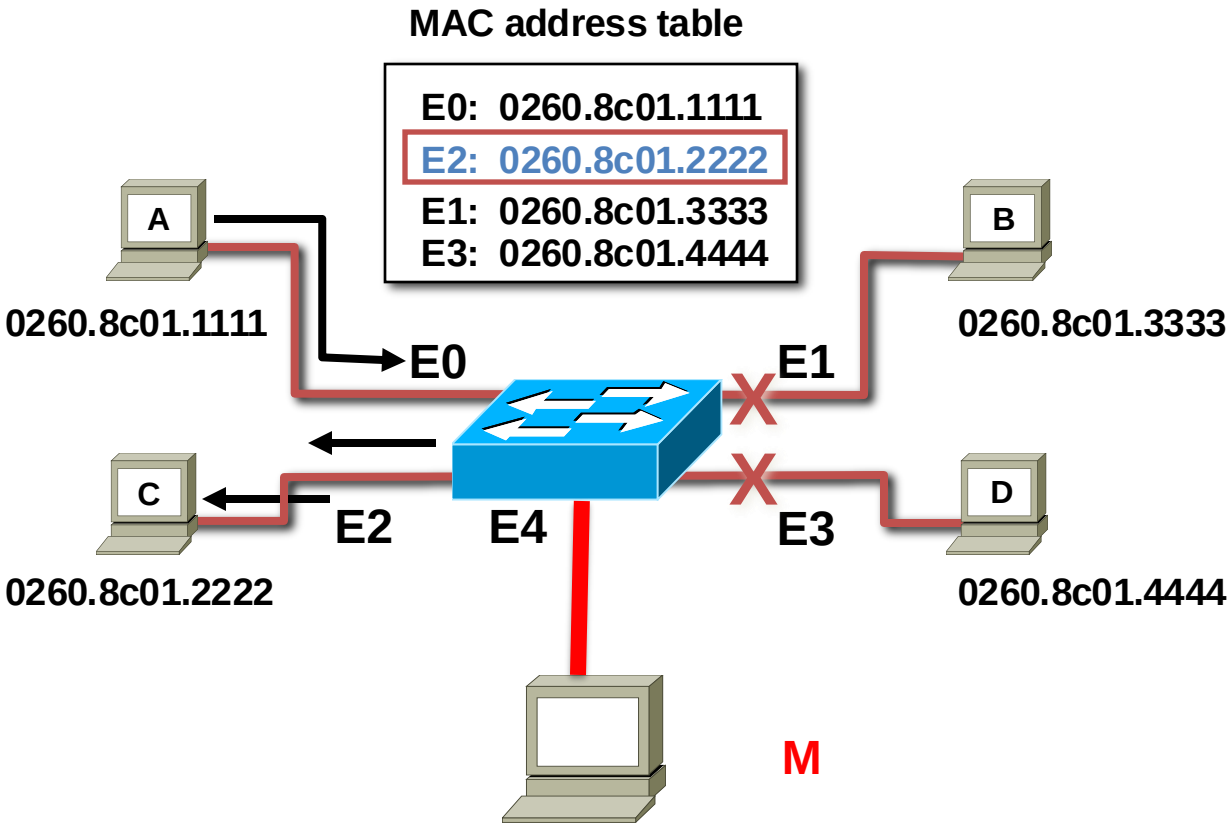
- D to C
- Switch caches station D MAC address to port E3 by learning the source Address of data frames
- The frame from station D to station C is flooded out to all ports except port E3 (unknown unicasts are flooded)
- (If a frame's destination MAC is FF-FF-FF-FF, it will be flooded)

How Switches Filter Frames



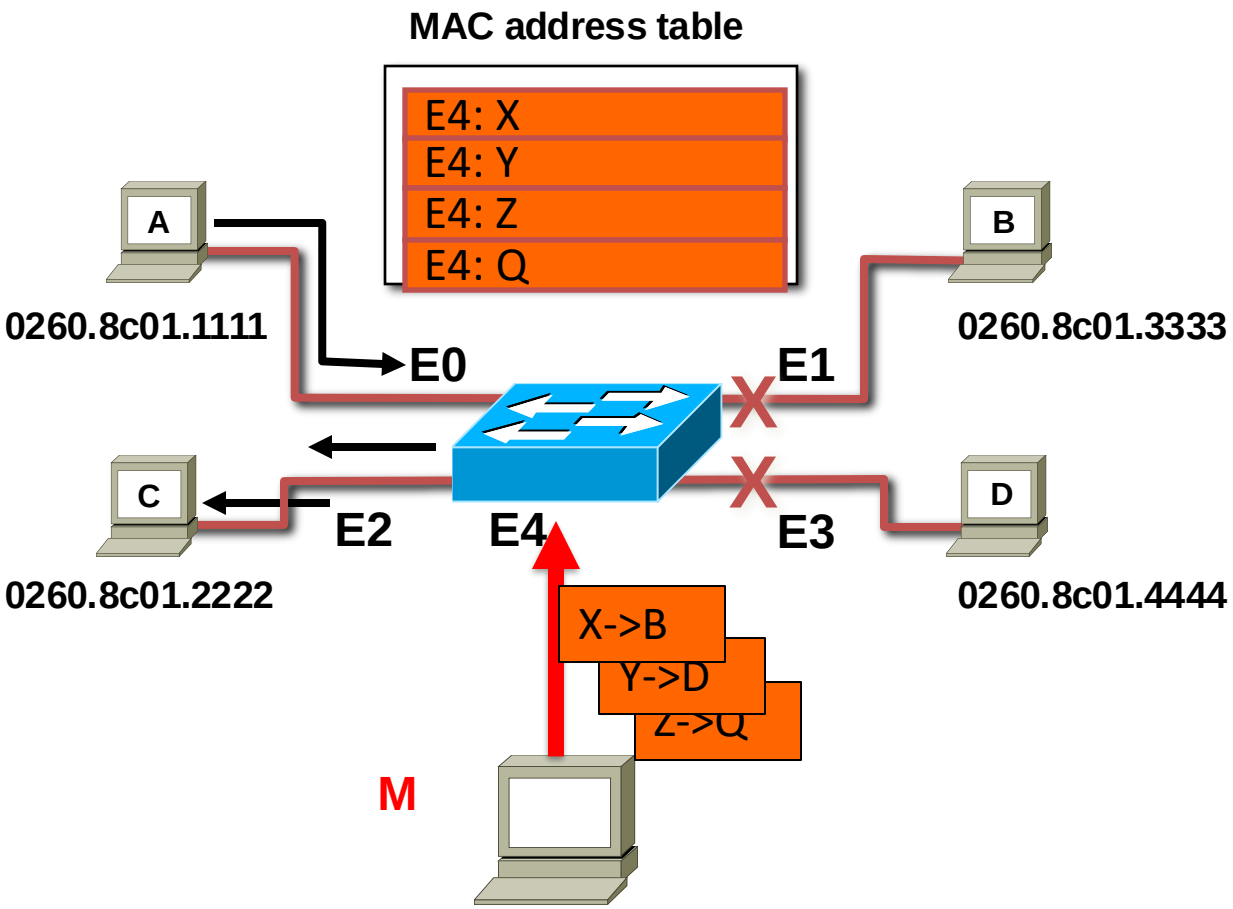
- Station A sends a frame to station C
- Destination is known, frame is not flooded

Sniffering in Switch(Layer 2) ?



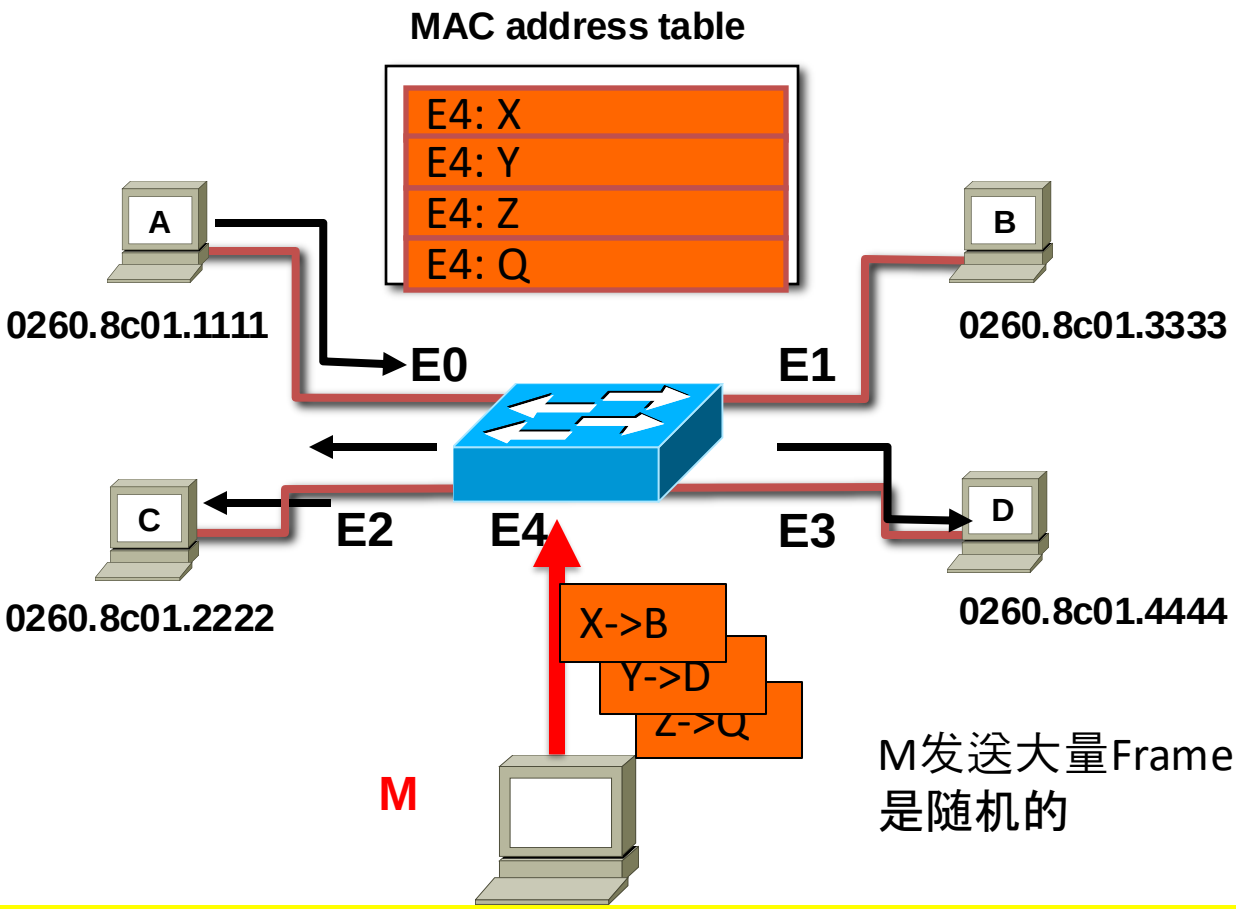
Can M sniffer traffic between A and C ?

MAC Flooding attack



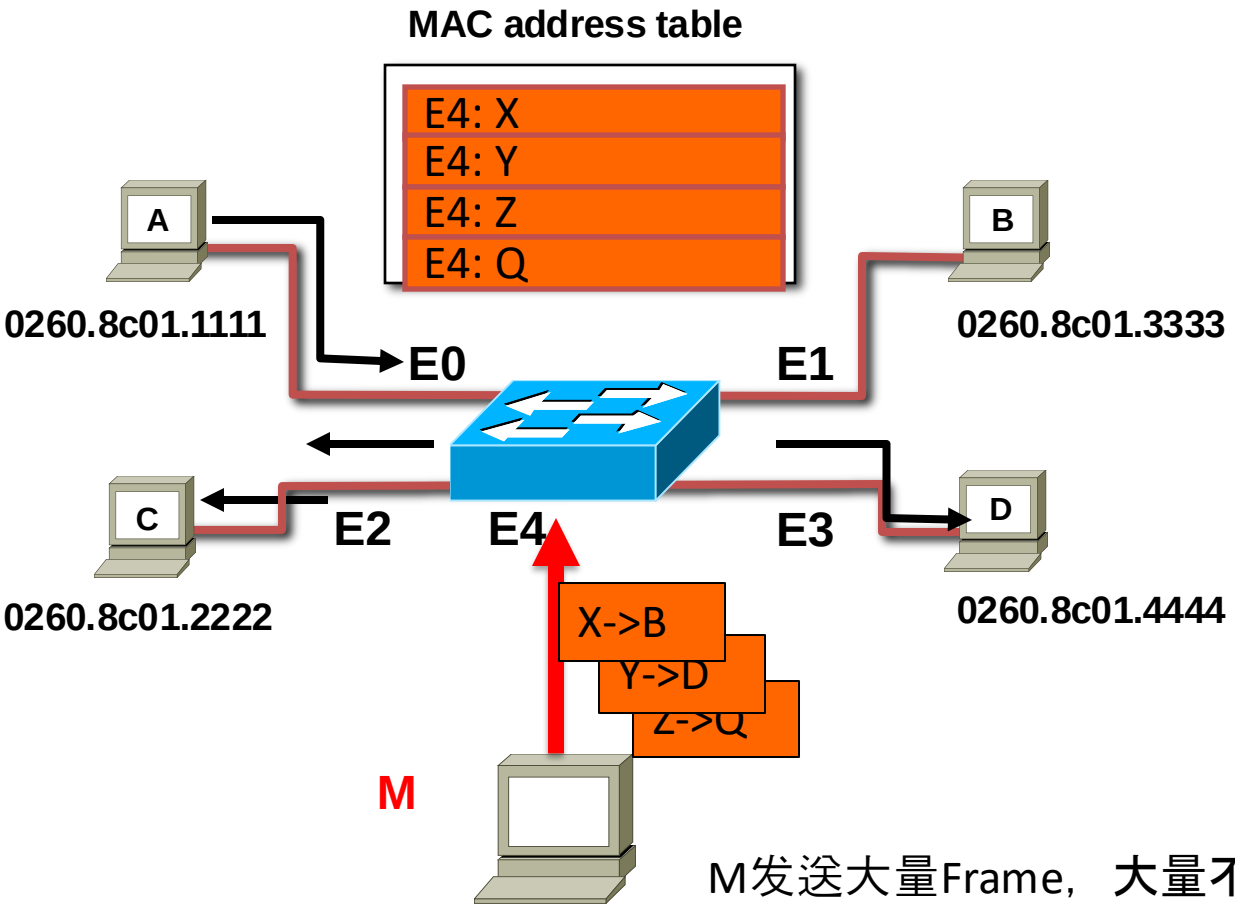
Tool: macof in http://www.monkey.org/~dugsong/dsniff/

MAC Flooding attack



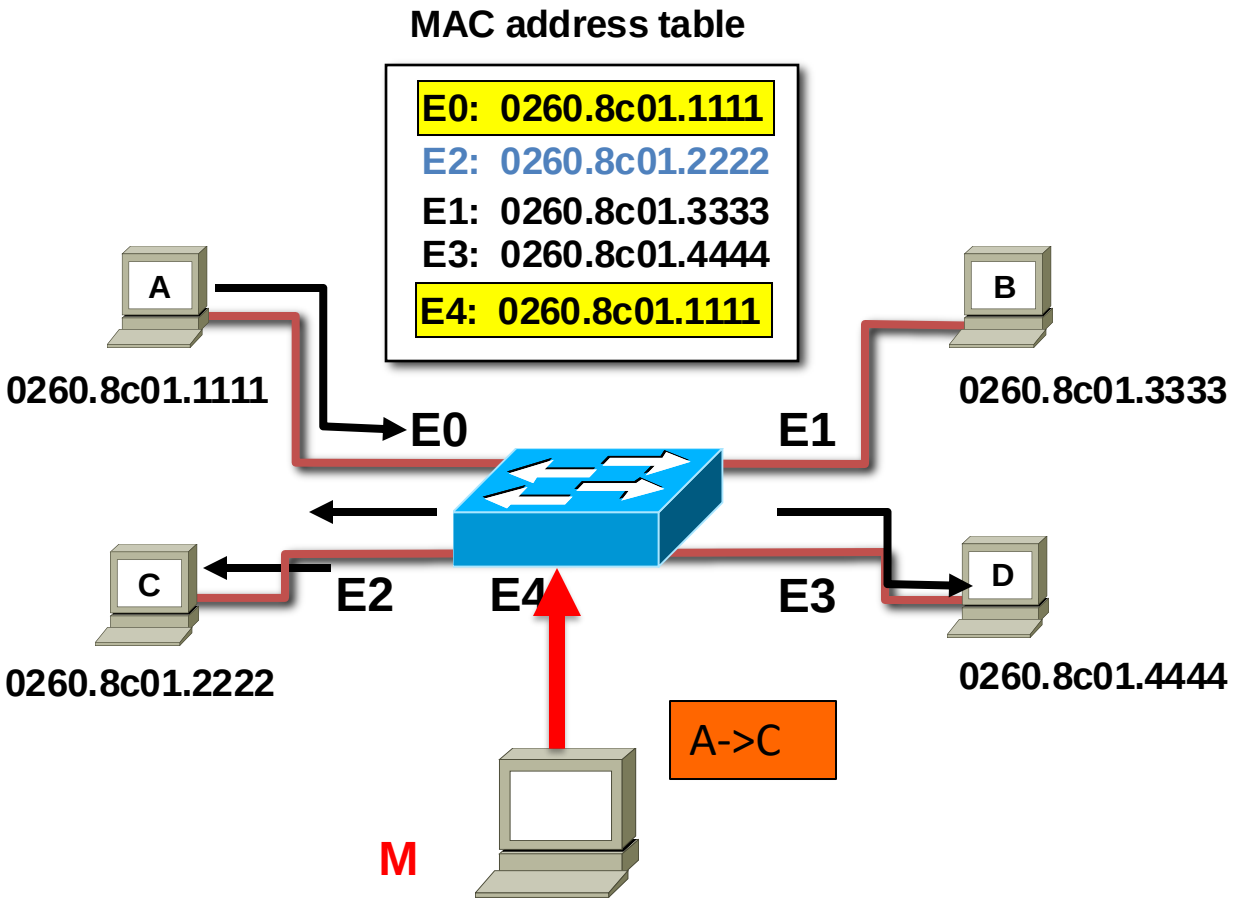
Can M sniffer traffic between A and C now ?

如何防范？



M发送大量Frame，大量不同的源MAC地址

MAC spoofing attack



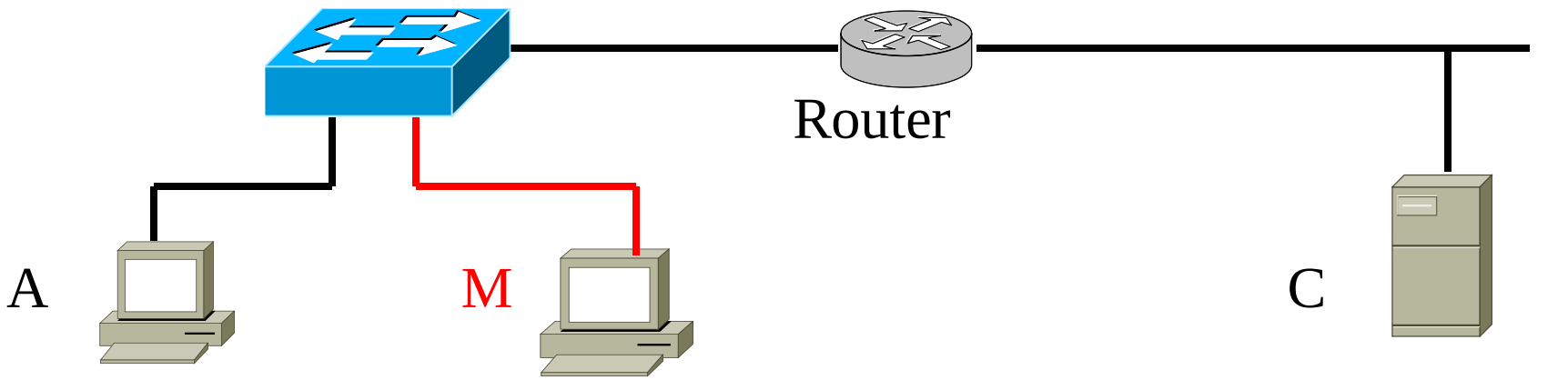
M发送Frame，假冒A的MAC地址（A-C）；
交换机把C回复给A的Frame转发给谁呢？

检测与缓解（Mitigation）

- 静态绑定终端的MAC地址到交换机的特定物理接口上
  - 缺点？
- 动态监听地址分配：DHCP Snooping
  - 交换机监听DHCP分配的 IP/MAC地址
- 监测到MAC地址端口移动时告警
- 限制每个端口上的MAC地址表数量

不同层次的地址标识

交换机：根据MAC地址转发或广播　　路由器：根据IP地址查找路由表，转发



不同层次的标识：

应用层：主机名字,如domain name，
电子邮件地址

网络层： IP Address

数据链路层： MAC address

- 你怎么得到对方的MAC地址、IP 地址
- 你怎么验证得到的信息真的？

标识之间的映射

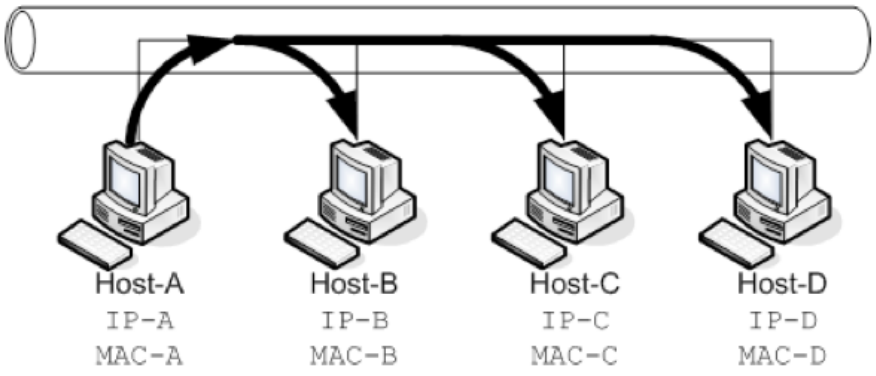
- Domain name ←→ IP : DNS
  - What is your DNS server?
  - Is the reply from your DNS server true?
- IP ←→ MAC
  - Address Resolution Protocol(ARP)
  - Reverse ARP→ BOOTP → DHCP
- DHCP
  - Not only： Gateway address, DNS, Proxy…

ARP / RARP

- RFC 826(1982), Informational, not standard
  - The method proposed here is presented for your consideration and comment. This is not the specification of a Internet Standard.
- RFC 5227(2008)
  - IPv4 address conflict detection
- RFC 5494(2009)
  - IANA Allocation Guidelines for the Address Resolution Protocol (ARP)

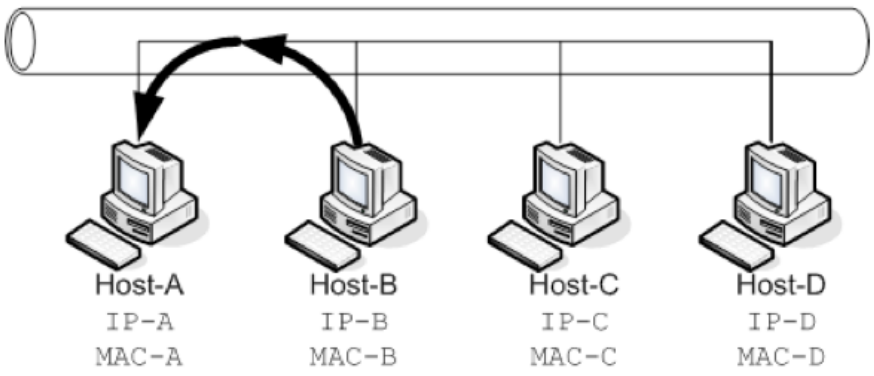
ARP Request and Reply

Ethernet	
Destination:	FF:FF:FF:FF:FF:FF
Source:	MAC-A
Type:	ARP
ARP	
Opcode	**Request**
Sender MAC	MAC-A
Sender IP	IP-A
Target MAC	0:0:0:0:0:0
Target IP	**IP-B**



A @All : 谁的IP地址是IP-B? 告诉我你的MAC地址

Ethernet	
Destination:	MAC-A
Source:	MAC-B
Type:	ARP
ARP	
Opcode	**Reply**
Sender MAC	**MAC-B**
Sender IP	**IP-B**
Target MAC	MAC-A
Target IP	IP-A

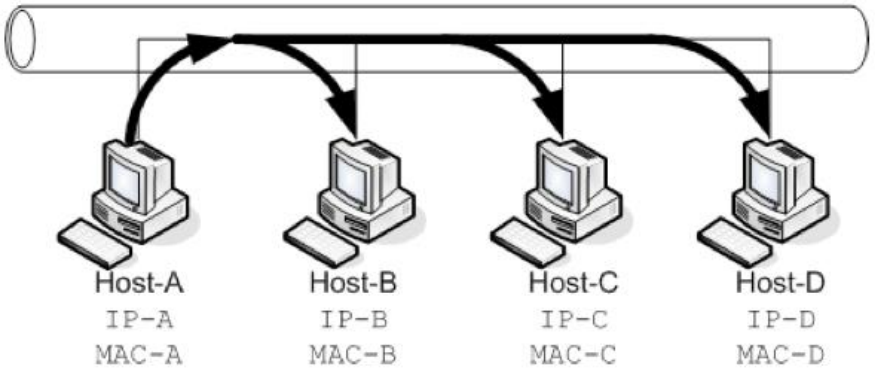


B →A :这是我的MAC地址 MAC-A

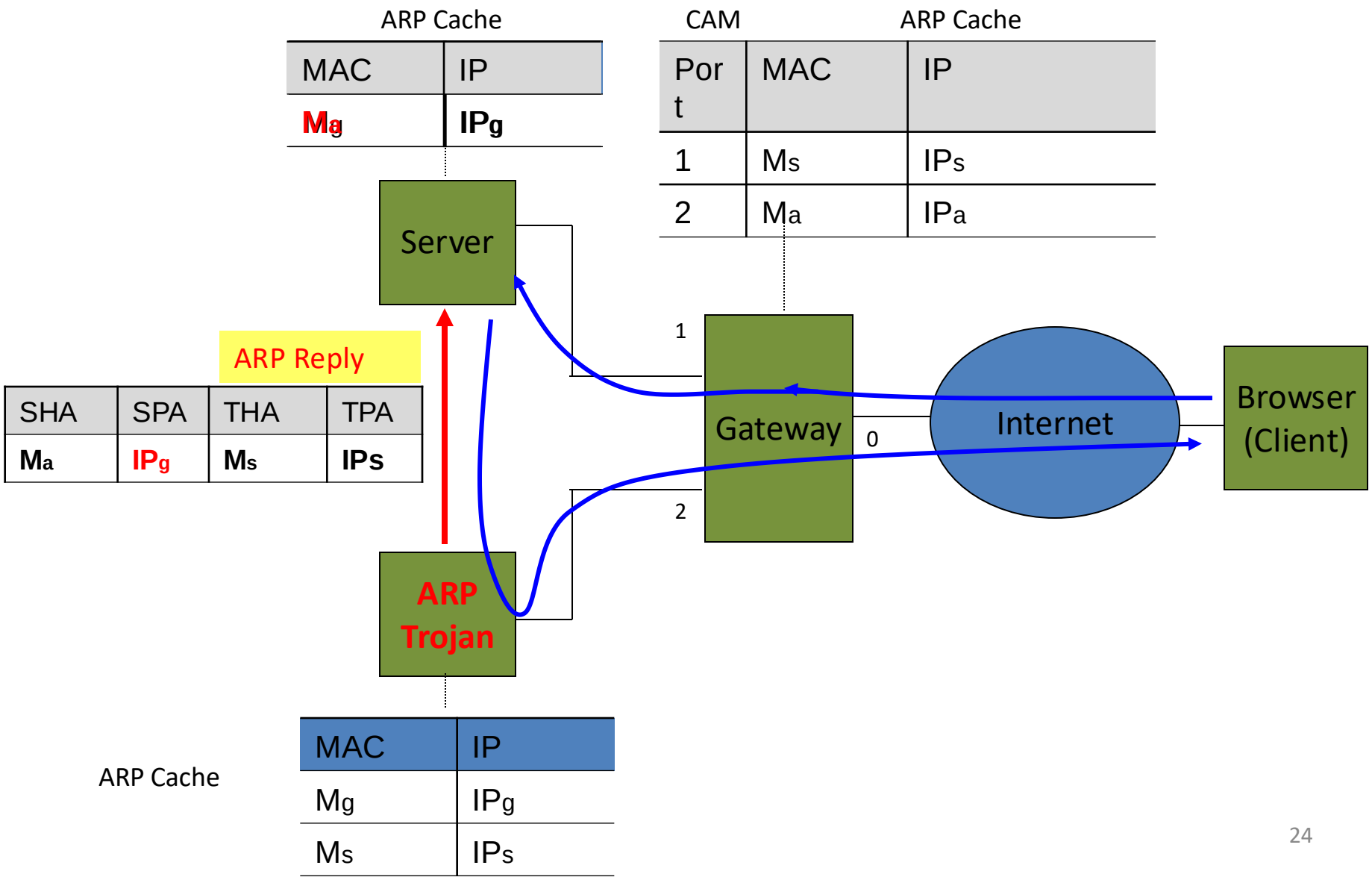
ARP Cache

- ARP请求是广播
- **ARP 缓存的维护**
  - **Static ：arp -s**
  - **Dynamic**
- **ARP reply unsolicited**
  - **Sent actively after booting, to refresh caches of neighbors**
  - **Unicast**

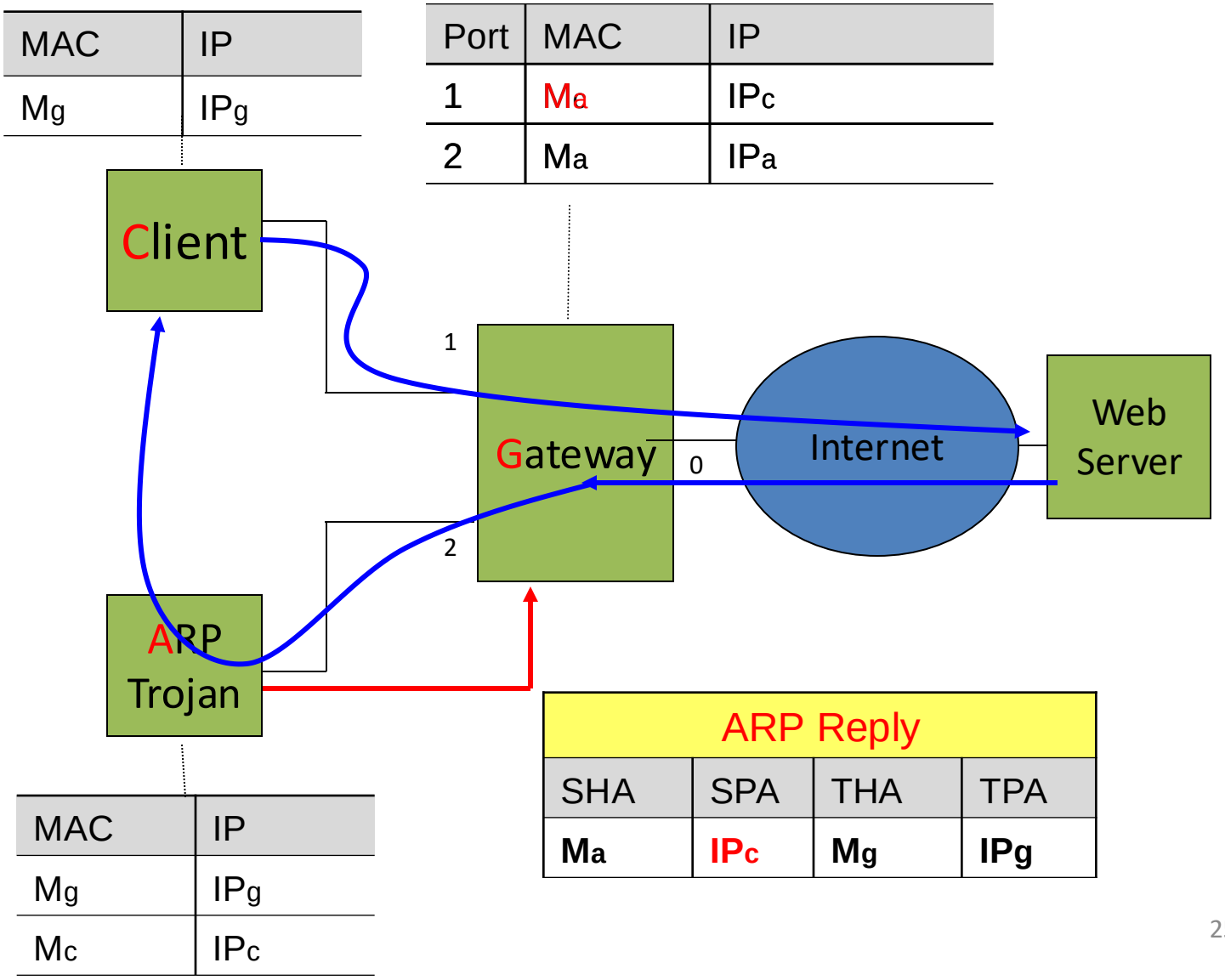
```
duanhx@duanhx-NUC11BTMi9:~$ arp -an
? (172.16.11.39) at <incomplete> on enp1s0f0
? (172.16.11.23) at <incomplete> on enp1s0f0
? (172.16.10.2) at e8:8d:28:56:6a:53 [ether] on enp1s0f1
? (172.16.11.17) at <incomplete> on enp1s0f0
? (172.16.11.16) at 00:e0:67:17:a9:70 [ether] on enp1s0f0
? (166.111.133.61) at f8:0d:ac:78:cc:ec [ether] on enp90s0
? (172.16.11.28) at <incomplete> on enp1s0f0
? (172.16.11.24) at 94:57:a5:10:c2:62 [ether] on enp1s0f0
? (166.111.133.33) at 98:0d:51:9f:6b:aa [ether] on enp90s0
? (172.16.11.2) at 24:4b:fe:f1:7f:b0 [ether] on enp1s0f0
? (166.111.133.44) at f8:a2:6d:df:b9:fb [ether] on enp90s0
? (172.16.11.13) at <incomplete> on enp1s0f0
? (172.16.11.12) at <incomplete> on enp1s0f0
? (172.16.11.14) at <incomplete> on enp1s0f0
? (166.111.133.40) at 00:1a:a9:4e:27:2c [ether] on enp90s0
? (172.16.11.11) at <incomplete> on enp1s0f0
? (172.16.11.10) at <incomplete> on enp1s0f0
? (166.111.133.1) at 54:2b:de:6d:11:87 [ether] on enp90s0
```



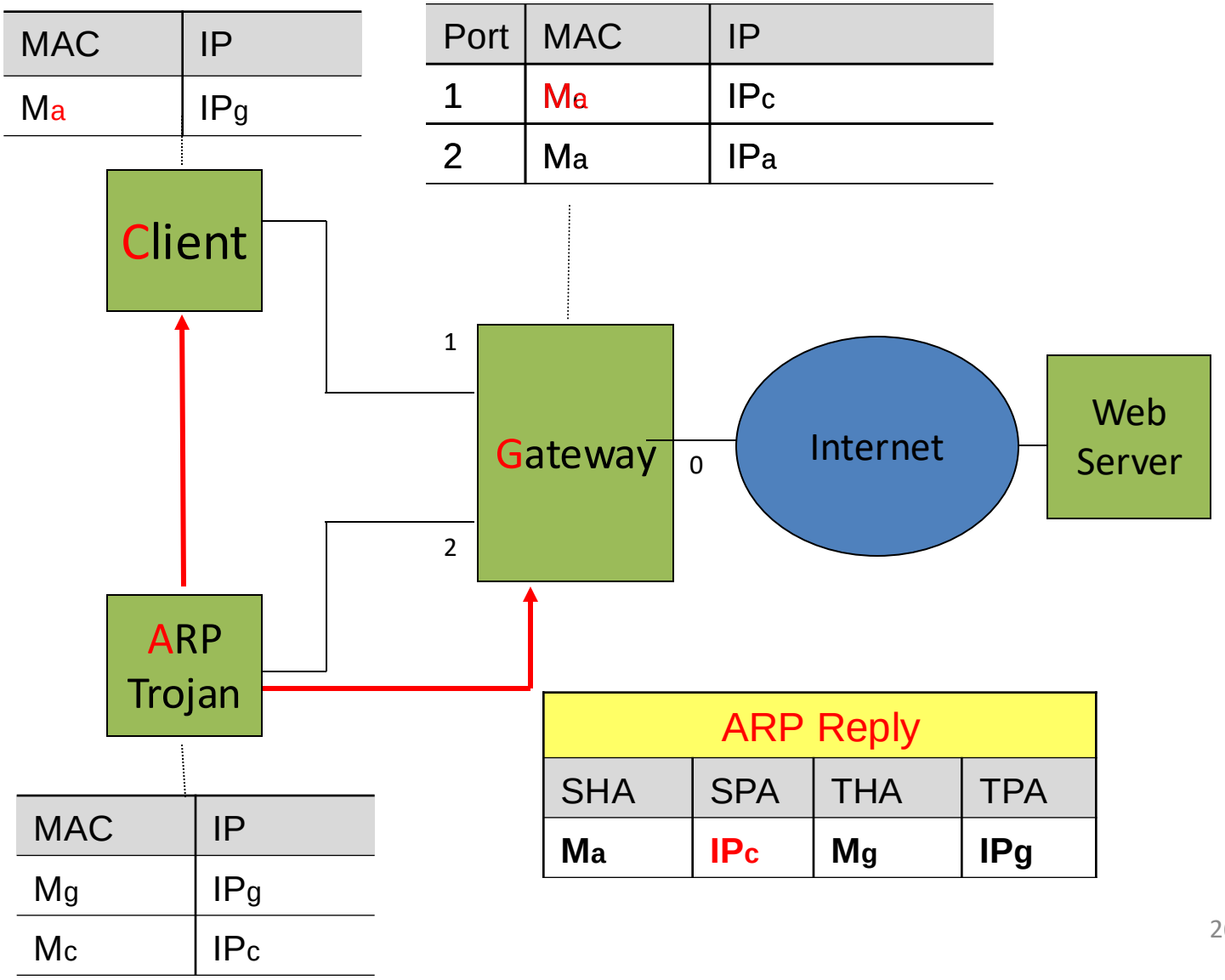
ARP Spoofing: spoofing gateway



ARP spoofing: spoofing neighbor, poisoning gateway

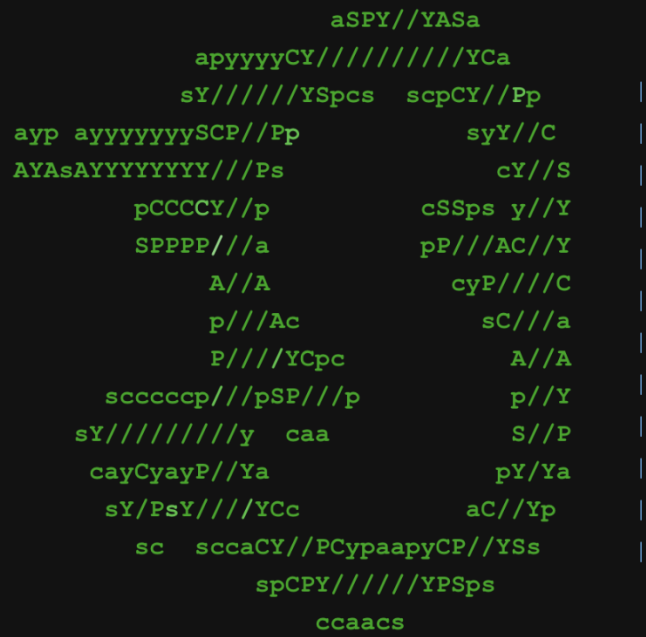


ARP spoofing: spoofing neighbor, poisoning gateway



Arp spoofing tools

- **arpoison https://github.com/Akagi201/arpoison/blob/master/arpoison.c**
- **Arpspoof https://github.com/smikims/arpspoof**
- **Netcommander: https://github.com/meh/NetCommander**
- **Aranea: https://github.com/ts-way/aranea**



What is Scapy?

Manipulate packets

Scapy is a powerful interactive packet manipulation library written in Python. Scapy is able to forge or decode packets of a wide number of protocols, send them on the wire, capture them, match requests and replies, and much more.

A REPL and a Library

Scapy can be used as a REPL or as a library. It provides all the tools and documentation to quickly add custom network layers.

Cross-platform

Scapy runs natively on Linux, macOS, most Unixes, and on Windows with Npcap. It is published under GPLv2. Starting from version 2.5.0+, it supports Python 3.7+ (and PyPy).

How to Build an ARP Spoofer in Python using Scapy

```
def get_mac(ip):
    """
    Returns MAC address of any device connected to the network
    If ip is down, returns None instead
    """
    ans, _ = srp(Ether(dst='ff:ff:ff:ff:ff:ff')/ARP(pdst=ip), timeout=3, verbose=0)
    if ans:
        return ans[0][1].src
```

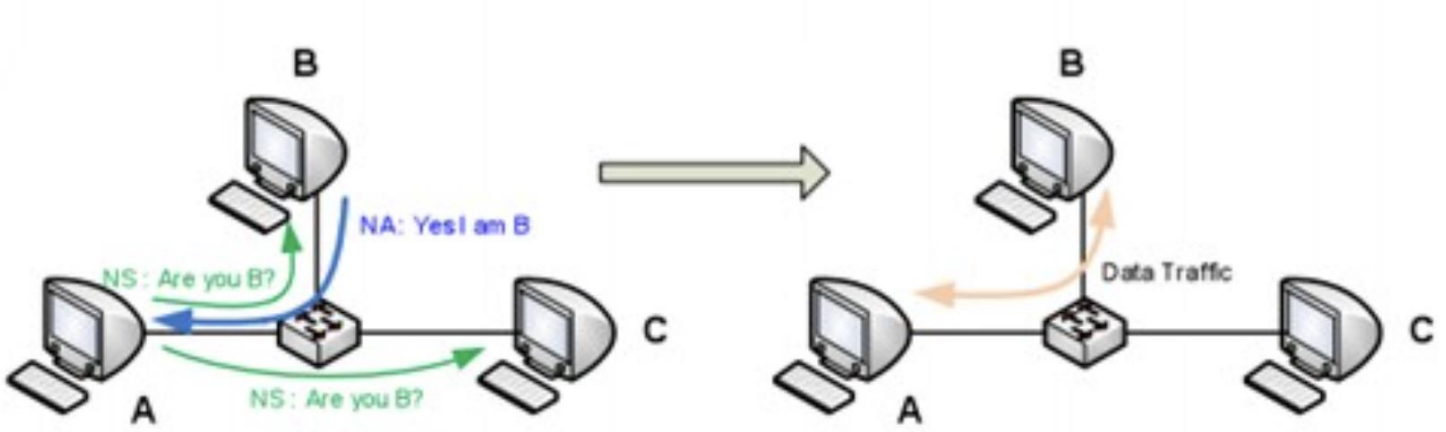
```
    # get the mac address of the target
    target_mac = get_mac(target_ip)
    # craft the arp 'is-at' operation packet, in other words; an ARP response
    # we don't specify 'hwsrc' (source MAC address)
    # because by default, 'hwsrc' is the real MAC address of the sender (ours)
    arp_response = ARP(pdst=target_ip, hwdst=target_mac, psrc=host_ip, op='is-at')
```

https://thepythoncode.com/article/building-arp-spoofer-using-scapy

Neighbor Discovery for IPv6

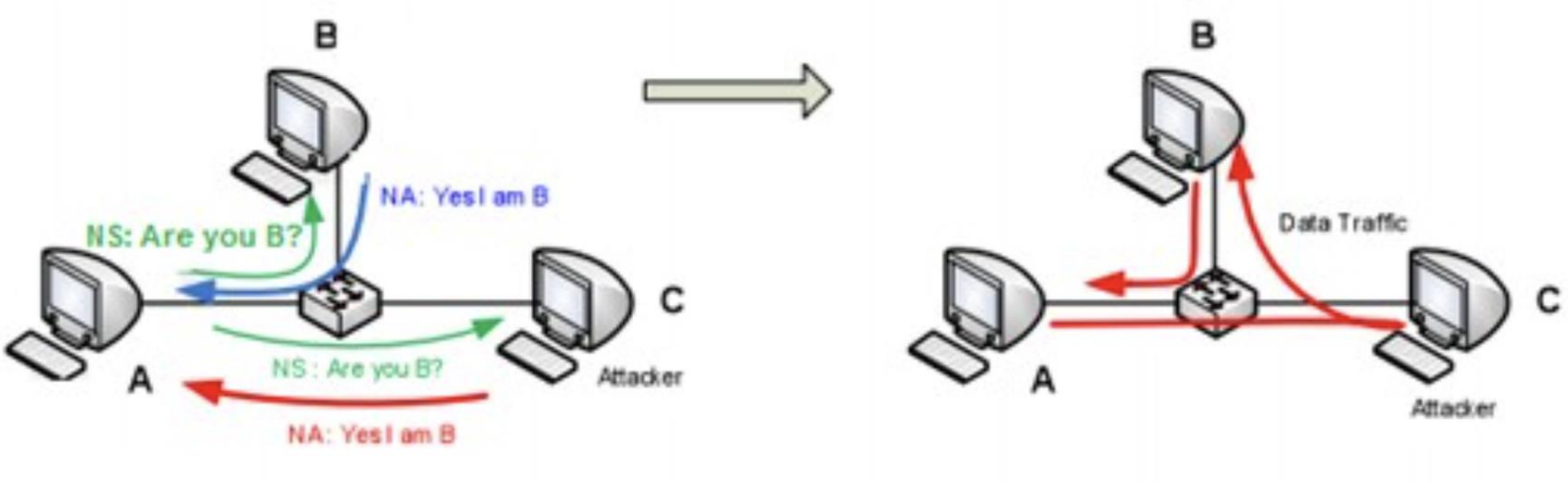
- Neighbor Discovery Protocol(ND), RFC 4861

* ICMPv6 neighbor discovery requires two types of ICMPv6.
  * They are ICMPv6 neighbor solicitation (ICMPv6 Type 135) and ICMPv6 neighbor advertisement (ICMPv6 type 136).



MITM attack with ND

* Attacker utilizes his computer with ***THC parasite6*** and allows IPv6 forwarding.
* Node A tries to find out the MAC address of Node B by sending ICMPv6 neighbor solicitation packet to multicast address forall nodes (FF02::1)

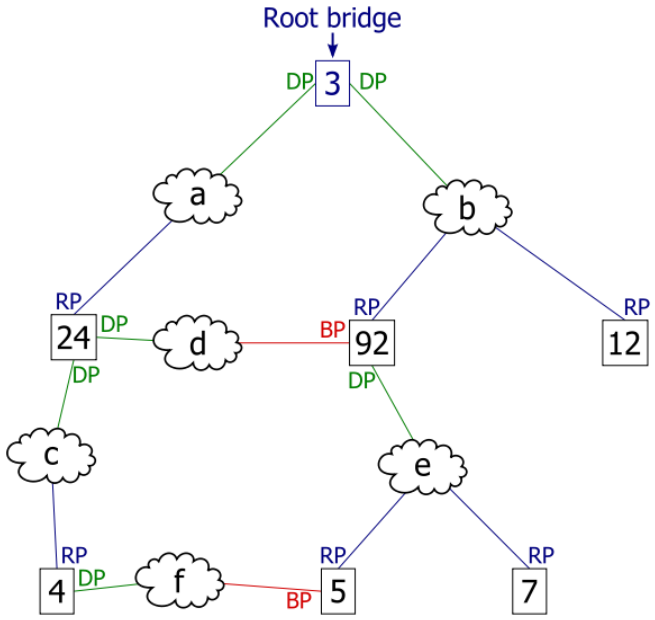


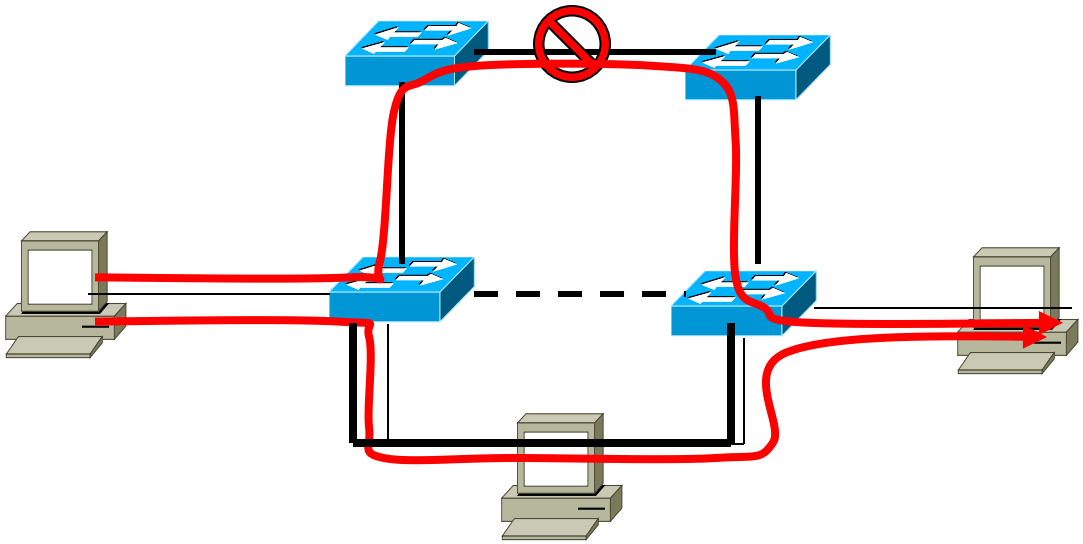
Prevention, Mitigation?

Discussion

局域网中的其他攻击

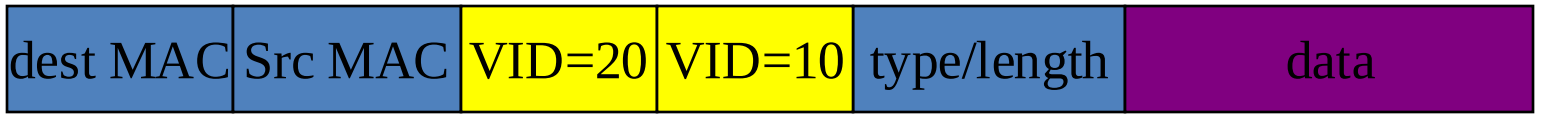
- **STP (Spanning Tree Protocol)攻击**
  - STP是交换机之间交换协议以避免环路的算法，但是一个连在两个交换机之间的主机可以伪装成交换机，让网络的流量流经自己，从而实现窃听或中间人攻击

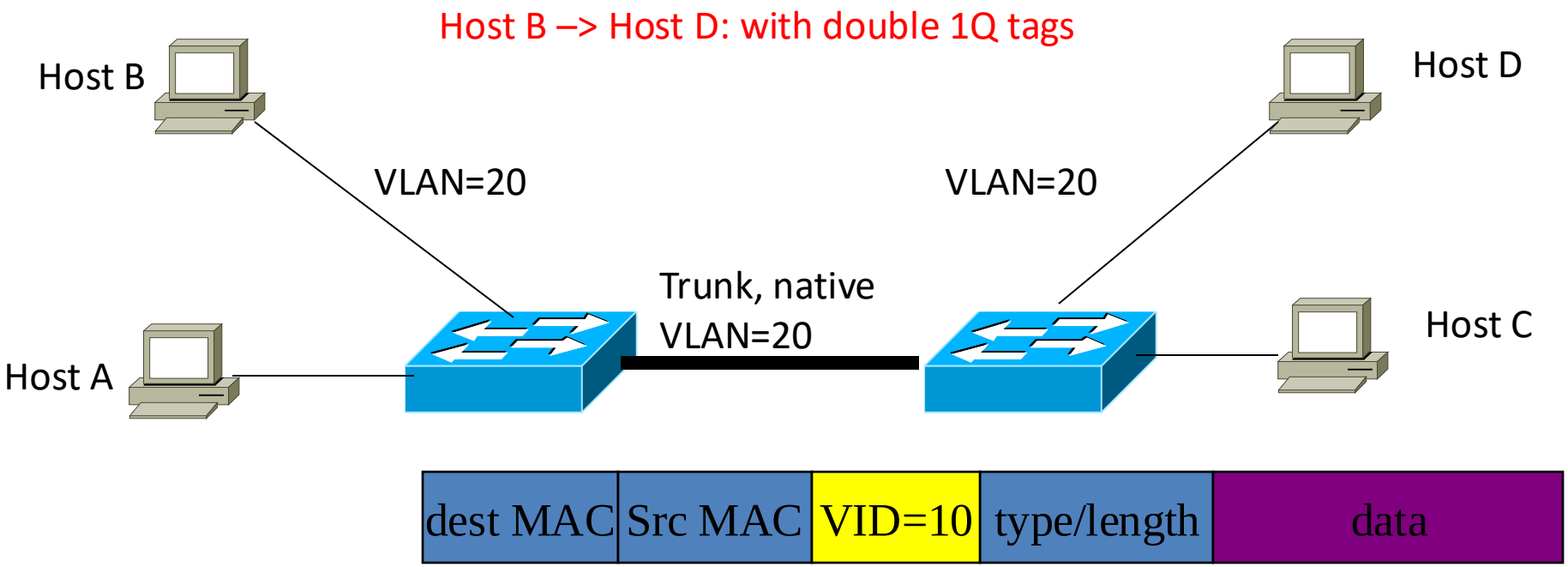




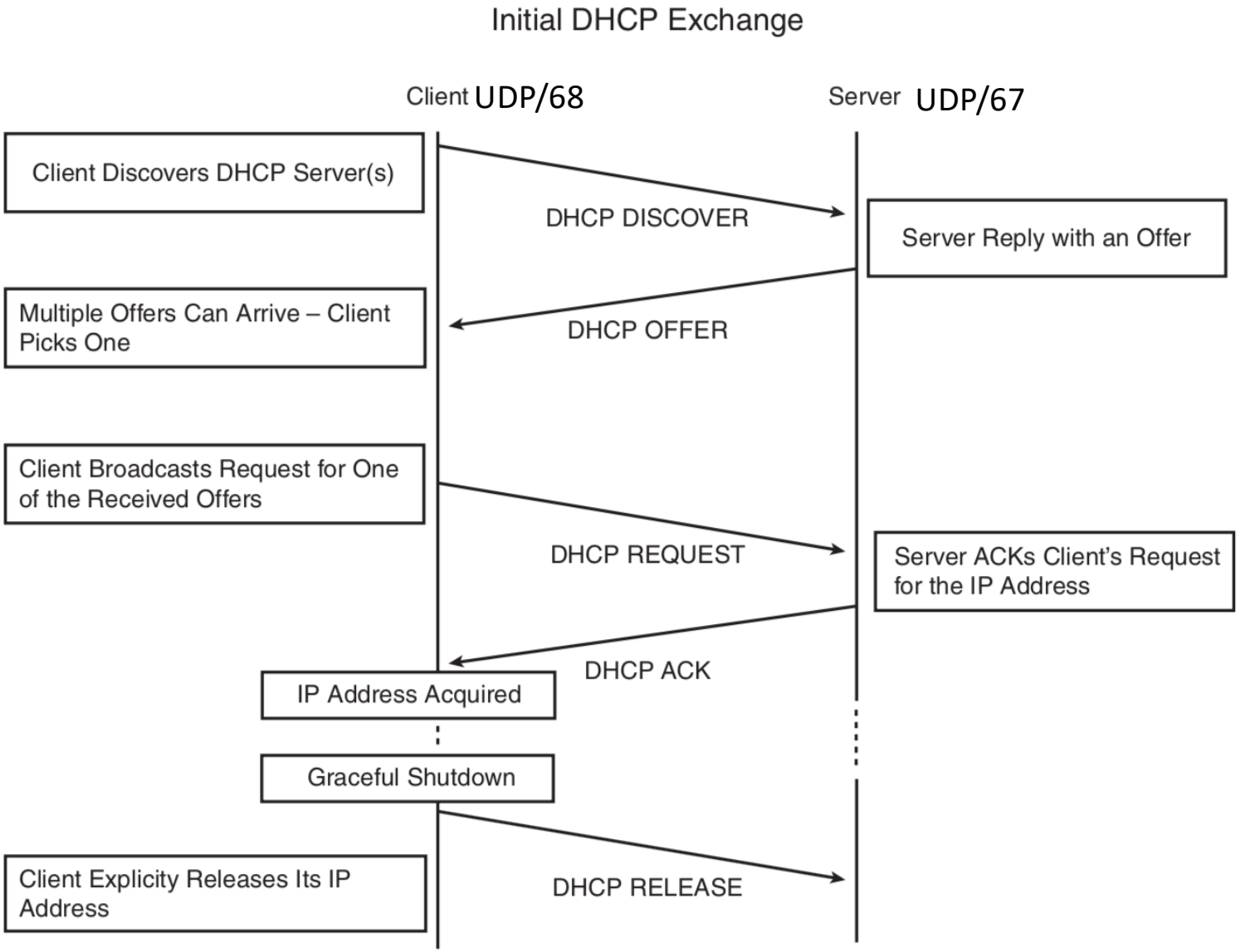
VLAN Hopping Attacks

- How can Host B send frame to Host C?
- Host B –> Host D: with double 1Q tags





Dynamic Host Configuration Protocol （DHCP）



Broadcast

Discover

Offer

Request

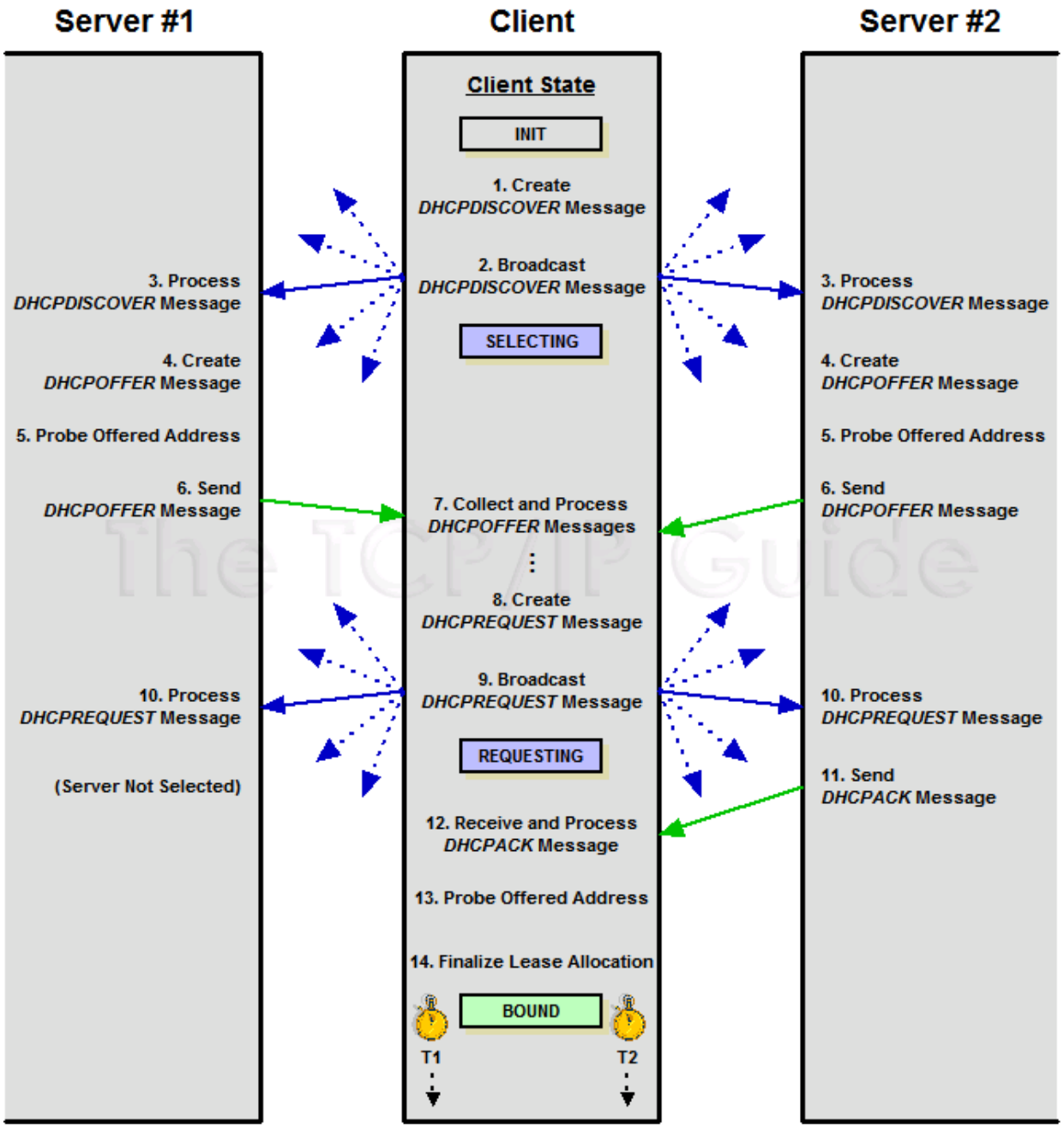
ACK

NAK

Release

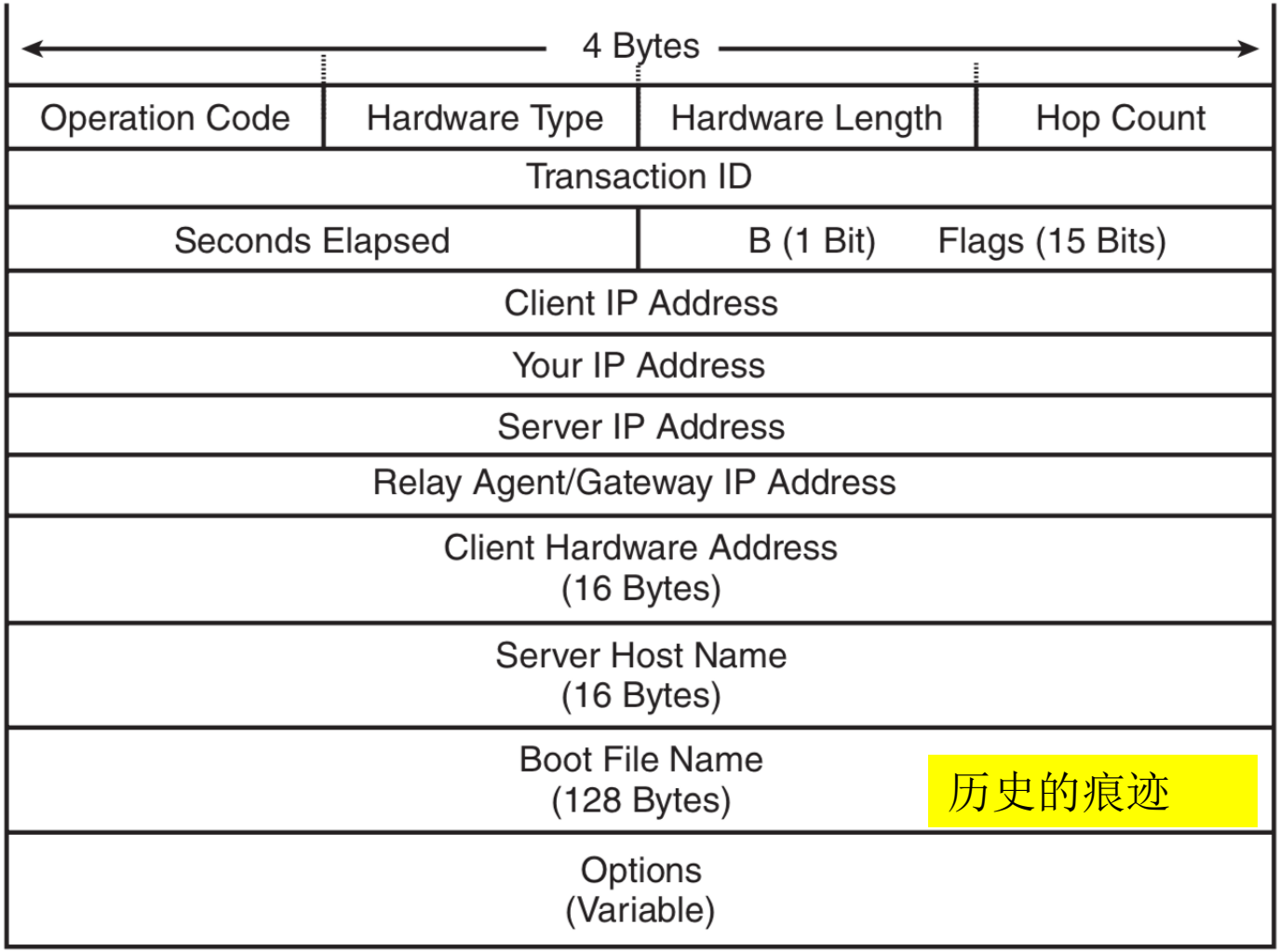
Inform

Decline



http://www.tcpipguide.com/free/t_DHCPLeaseAllocationProcess-2.htm

DHCP Packet Format



http://www.tcpipguide.com/free/t_DHCPMessageFormat.htm

DHCP Options

- IP, netmask
- Gateway/routers
- MTU
- Static route
- DNS server
- NTP server
- HTTP Proxies
- SMTP, POP3 server

Dynamic Host Configuration Protocol（DHCP）

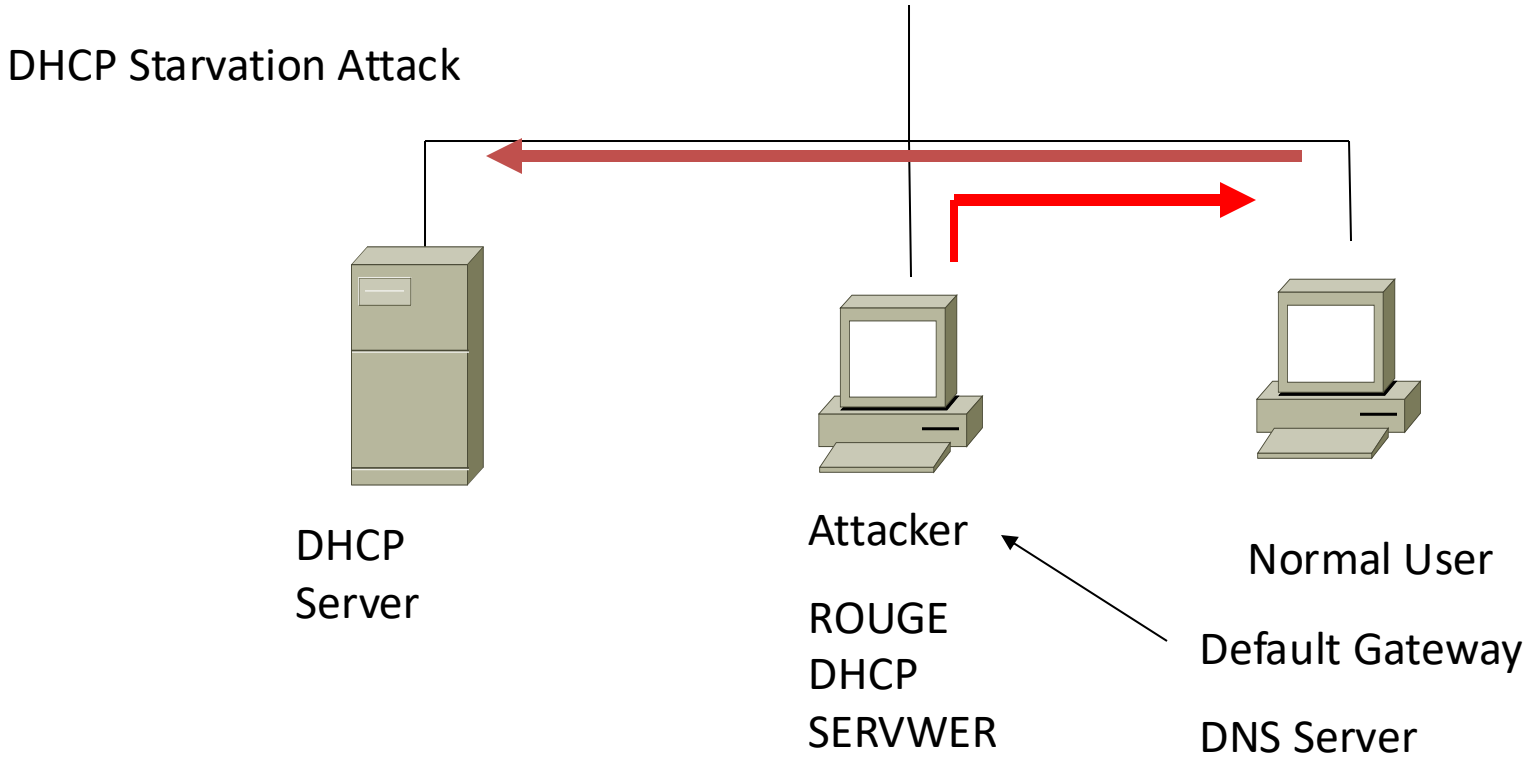
- RARP → BOOTP → DHCP
- DHCP RFC 2131， 1997
- Security Considerations in RFC2131

DHCP设计者自认为它是不安全的

  - DHCP is built directly on UDP and IP which are as yet inherently insecure. Furthermore, DHCP is generally intended to make maintenance of remote and/or diskless hosts easier. While perhaps not impossible, configuring such hosts with passwords or keys may be difficult and inconvenient. Therefore, **DHCP in its current form is quite insecure.**
  - Unauthorized DHCP servers may be easily set up. Such servers can then send false and potentially disruptive information to clients such as incorrect or duplicate IP addresses, incorrect routing information (including spoof routers, etc.), incorrect domain nameserver addresses (such as spoof nameservers), and so on. Clearly, once this seed information is in place, an attacker can further compromise affected systems.
  - Malicious DHCP clients could masquerade as legitimate clients and retrieve information intended for those legitimate clients. Where dynamic allocation of resources is used, a malicious client could claim all resources for itself, thereby denying resources to legitimate clients.

Security Issues of DHCP

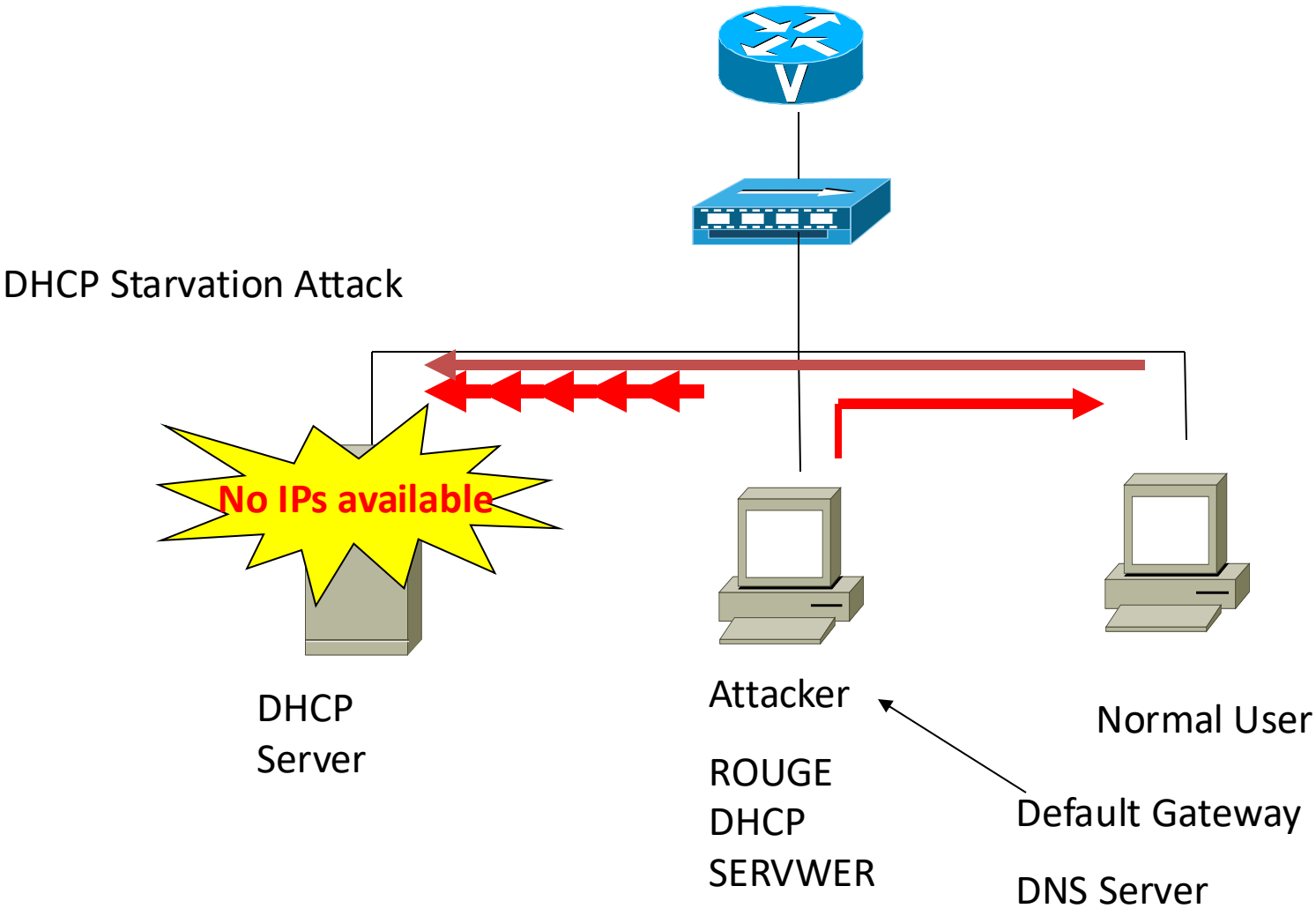
- **Unauthorized DHCP Servers**
  - Offering wrong Configuration information
    - OFFER
  - Redirect the client traffic to another router



Security Issues of DHCP

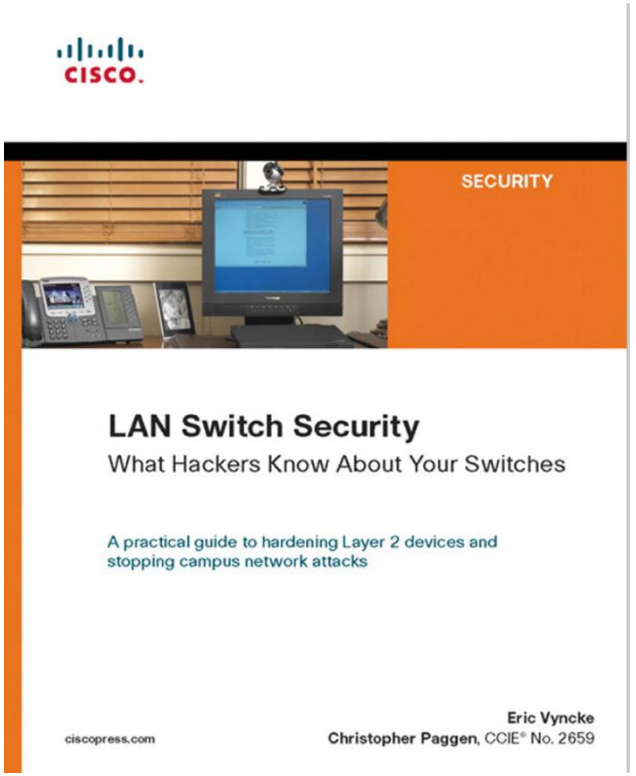
- **Unauthorized DHCP Servers**
  - Offering wrong Configuration information
    - OFFER
  - Redirect the client traffic to another router
- **Unauthorized DHCP Clients**
  - Masquerade as a legitimate DHCP client
  - Generate lots of bogus DHCP client requests to use up all the IP addresses in a DHCP server's pool.
    - DISCOVER：
    - RELEASE：

Combined DHCP attacks



References

E. Vyncke and C. Paggen, “Lan switch security: what hackers know about your switches,” pp. 1–361, Aug. 2007.



https://drive.google.com/file/d/1gzpS3lgsz2jd84ivcgb_4Y7Xv06xw7WN/view?usp=sharing

Threat special in Wireless LAN

- Requirement:
  - Confidentiality, Integrity, Availability
- New Challenges:
  - broadcast media,
  - mobile, portable devices
  - Limited resource
- ID and Authentication in WLAN are much difficult
  - Spoofing the SSID
  - Spoofing the client
- Sniffer, wiretapping
- Active attacks: replay, Man in the Middle
- Jamming

tsinghua-primo.hosted.exlibrisgroup.com.cn/primo-explore/search?query=any,contai...

水木搜索电子书导航

Kali Linux wireless

中文: 0-9 A B C D E F G H I J K L M N O P Q R S T

英文: 0-9 A B C D E F G H I J K L M N O P Q R S T

调整您的结果

排序 相关性

可获取性

在线全文 (32)

主题

作者

出版日期

从 到

2014 2022 确定

语种

出版机构

0个已选定 页数1 32个中的1-10个 个结果

1 图书

Kali Linux Wireless Penetration Testing Essentials

Alamanni, Marco.

: Packt Publishing ; 2015

在线访问

2 图书

Kali Linux Wireless Penetration Testing Beginner's Guide - Third Edition

Buchanan, Cameron, (author.) Ramachandran, Vivek, (author.)

Packt Publishing ; 2017

在线访问

3 图书

Mastering Kali Linux wireless pentesting : test your wireless network's security and master advanced wireless penetrati techniques using Kali Linux /

Sak, Brian, (author.) Ram, Jilumudi Raghu, (author.)

Birmingham : Packt Publishing ; 2016

在线访问

4 图书

Kali Linux wireless penetration testing beginner's guide : master wireless testing techniques to survey and attack wireless networks with Kali Linux /

Ramachandran, Vivek, (author.) Buchanan, Cameron, (author.)

Birmingham, England ; Mumbai, India : Packt Publishing ; 2015

在线访问

Kali Linux Wireless Penetration Testing Beginner's Guide Third Edition

Lab 2: ARP/DHCP 攻击

中间人攻击

- Scapy 编写ARP/DHCP欺骗工具

- MITM Proxy
- ip_forwarding
- iptables
- 目标：
  - Modify HTTP reply