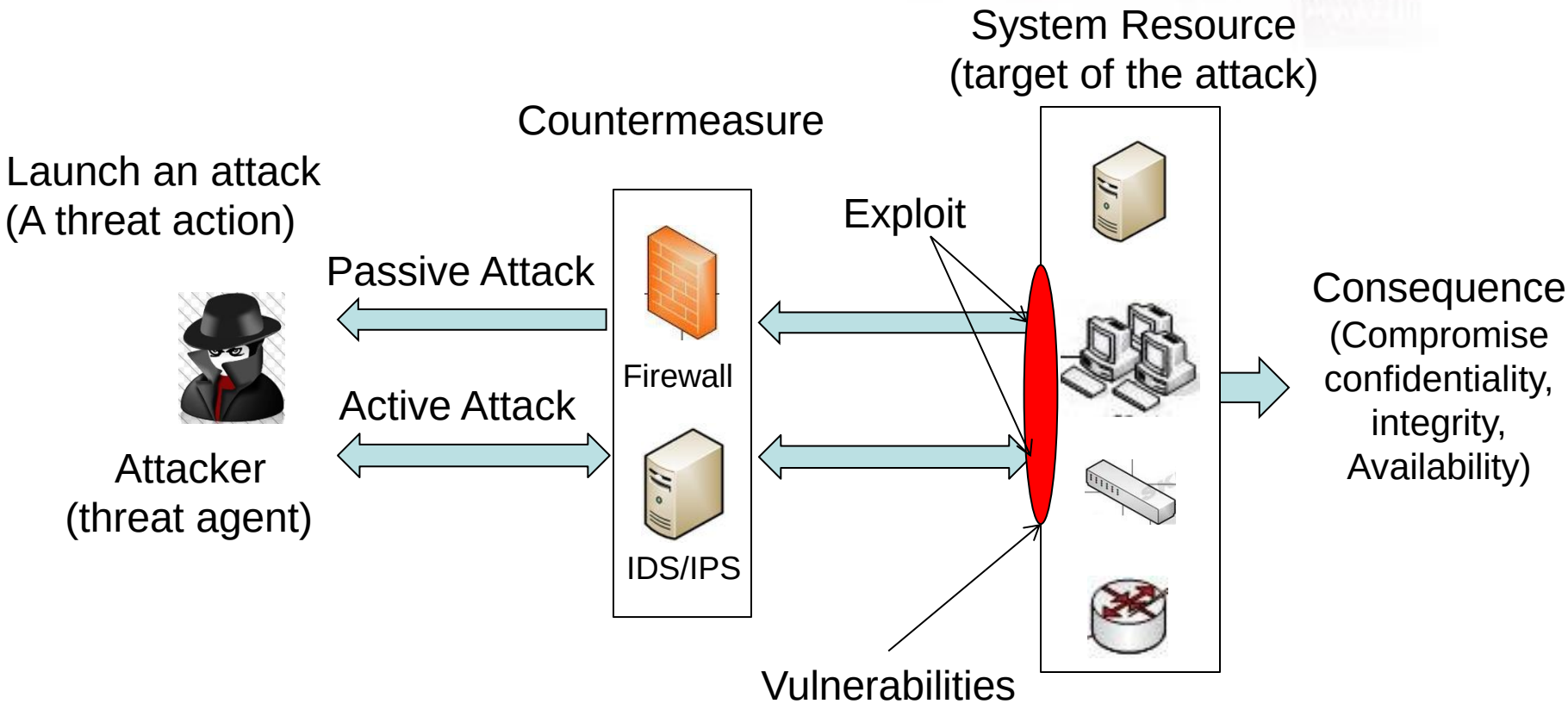
Network Attacks

(Layer 2 and Layer 3)

Chun-Jen (James) Chung

Arizona State University

Network Attack Scenarios



Network Attack

- *Network Attack*: An intrusion on the network infrastructure
  - analyze the target environment or collect information
  - exploit the existing open ports or vulnerabilities or perform the unauthorized access to resources
- *Passive vs. Active Attack*
  - Passive attack: attempts to learn or make use of information from the system but does not affect system resources
  - Active attack: attempts to alter system resources or affect their operation
- *Inside vs. Outside Attack*
  - Inside attack: initiated by insiders (who are authorized to access system resources but use them in a way not approved by the authority.
  - Outside attack: initiated from outside the security perimeter by an unauthorized or illegitimate user.

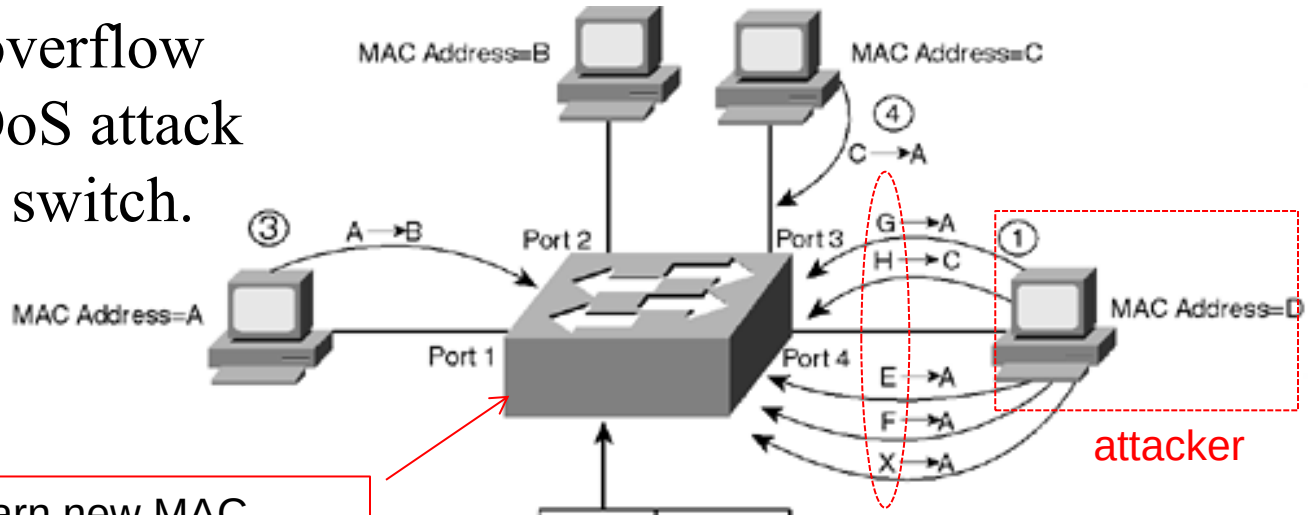
Layer 2 Attacks

Attacks in Layer 2

- The data link layer (L2) is a weak link in terms of security.
- Switches are key components at L2 communications and they are also used for L3 communications.
- They are susceptible to many of the same L3 attacks as routers, as well as many unique network attacks, which include
  - CAM table overflow
  - VLAN hopping
  - STP manipulation
  - ARP Spoofing (ARP Poisoning)
  - DHCP starvation

CAM Table Overflow

- Content addressable memory (CAM) table
  - a dynamic table in a network switch that maps MAC addresses to ports.
- CAN Table overflow is a type of DoS attack on a network switch.



Switch is unable to learn new MAC addresses and their associated ports, and turns into a hub so that all packets are treated as unknown destination MCA and flooded

② CAM Table

Port #	MAC Address
4	D
4	G
4	H
4	E
4	F
4	X

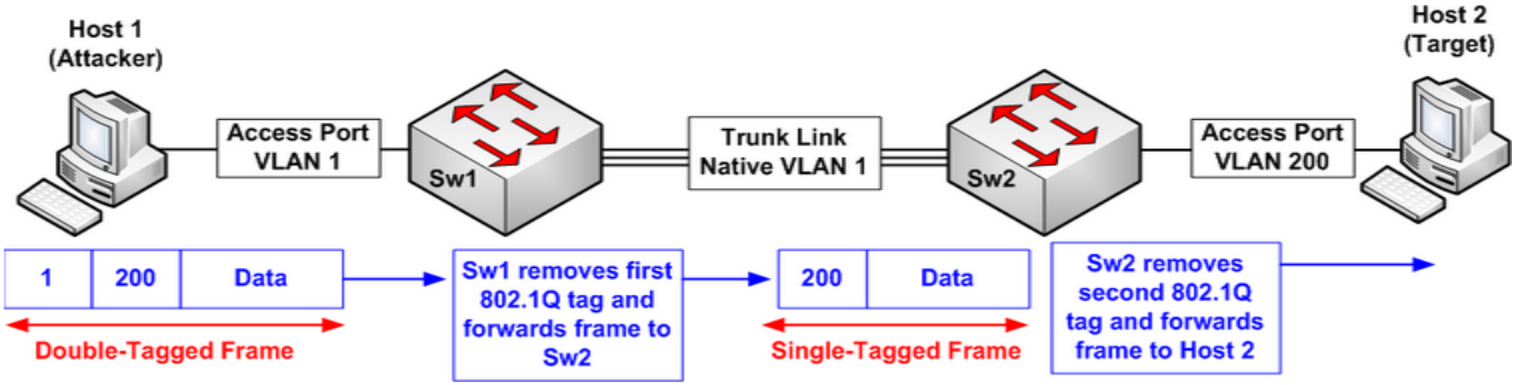
The MACs from port 4 Fill up CAM table

CAM Table Overflow attack & defense

- **macof** - MAC Flooding
  - **macof** is part of the **dsniff** (http://monkey.org/~dugsong/dsniff/) toolbox which is a collection of tools for network auditing and penetration testing.
  - In order to attack the CAM table and cause it to overflow, simply install dsniff, and type "macof" in a terminal window.
  - This immediately starts flooding the CAM table with *invalid MAC* addresses.
- Countermeasures – port security:
  - Hard-code MAC address to a corresponding port.
  - Limit the number of hosts to a port.

VLAN Hopping

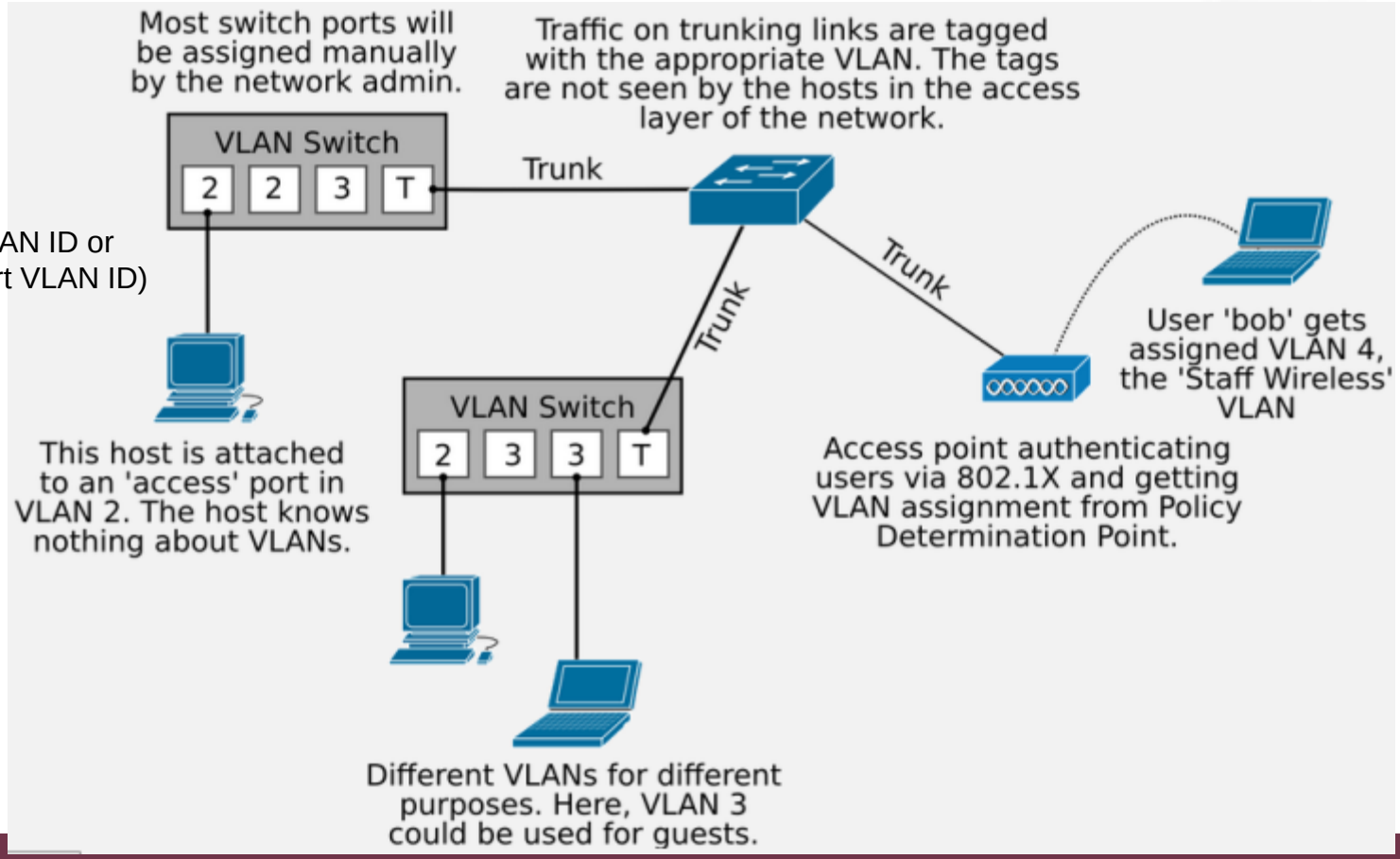
- Attacker send a double 802.1Q tags.
  - The first tag will get stripped off by the 1st switch, but a remaining tag contains a different VLAN to which the packet will be sent.



- Countermeasures
  - Use dedicated VLAN IDs for all trunk ports
  - Disable all unused switch ports and place them in an unused VLAN
  - Set all user ports to non-trunking mode

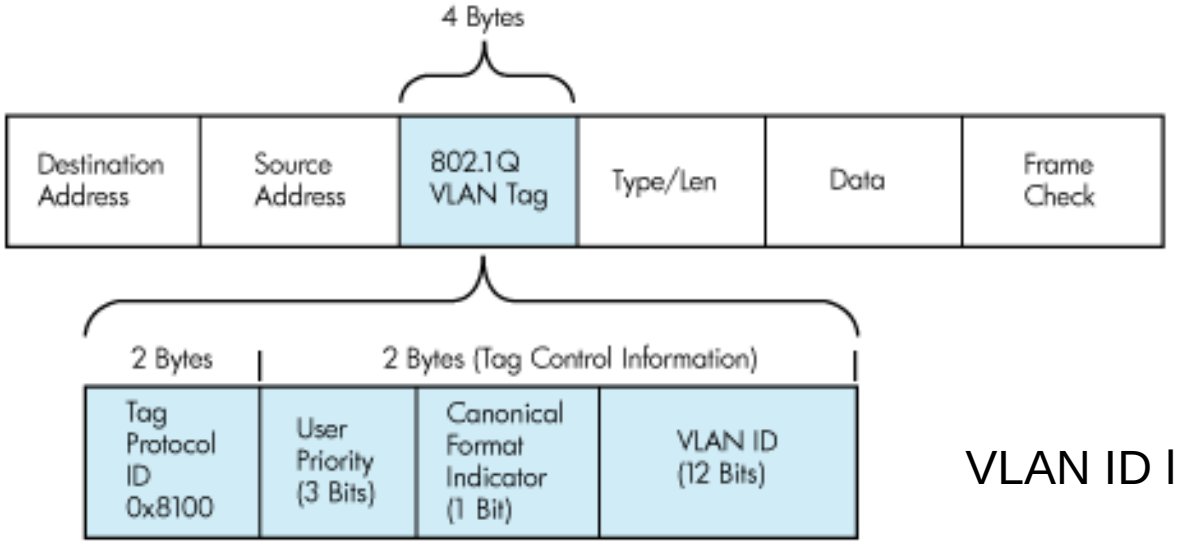
What is VLAN?

- A Virtual LAN (VLAN) is the ability to segregate a switch into separate broadcast-domains.



802.1Q

- VLAN tagging: networking standard that supports virtual LANs (VLANs) on an Ethernet network.
  - 4 bytes VLAN tag
  - 12 bit for VLAN ID



VLAN ID limitation?

STP Manipulation

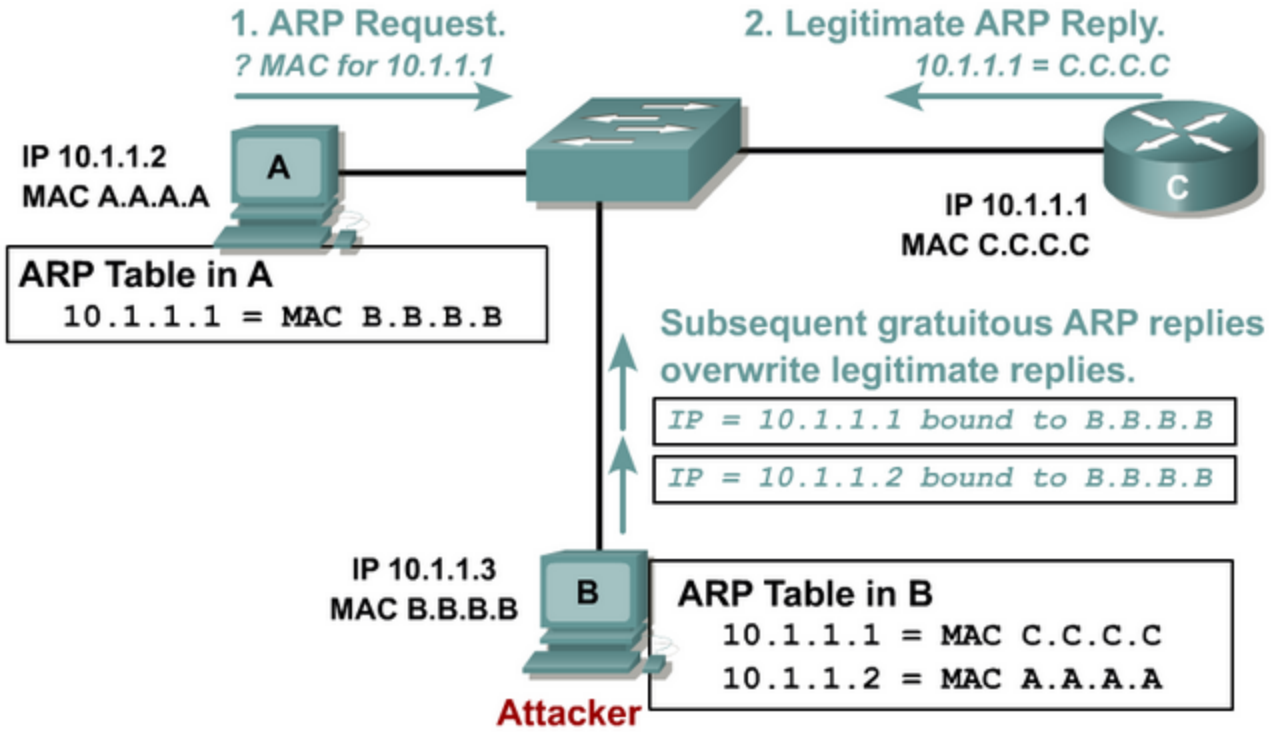
- Spanning-Tree Protocol is used in switched networks to prevent the creation of *bridging loops* in an Ethernet network topology.
- By attacking the STP, the network attacker hopes to spoof his/her system as the *root bridge* in the topology.
- Once attacker is able to impersonate the root bridge, he/she can redirect traffic and sniff it.
- Countermeasure
  - Enforces the placement of the root bridge
  - Disable the use of priority zero and hence becoming a root bridge

Spanning Tree Protocol

- Layer 2 LAN protocols, such as Ethernet, lack a mechanism to recognize and eliminate endlessly looping frames. Lacking such a mechanism, Layer 2 devices continue to retransmit looping traffic indefinitely.
- STP provides loop resolution by *managing the physical paths to given network segments*.
- STP allows physical path redundancy while preventing the undesirable effects of active loops in the network.
- STP is an IEEE committee standard defined as **802.1D**.

ARP Spoofing

- ARP spoofing attacks and ARP cache poisoning can occur because ARP allows a *gratuitous reply* from a host even if an ARP request was not received.

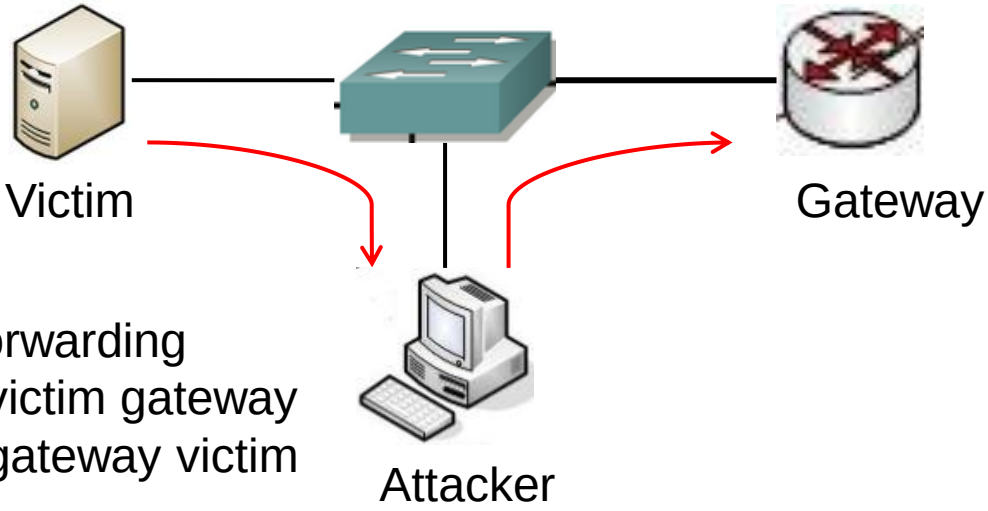


Gratuitous ARP

- Gratuitous in this case means a request/reply that is not normally needed according to the ARP specification
  - *GARP Request*: source and destination IP are both set to the IP of the machine issuing the packet, and the destination MAC is the broadcast address
  - *GARP Reply*: is a reply to which no request has been made
- Gratuitous ARPs are useful for four reasons:
  - help detect IP conflicts
  - assist in the updating of other machines' ARP tables
  - inform switches of the MAC address of the machine on a given switch port
  - Every time an IP interface or link goes up, the driver for that interface will typically send a gratuitous ARP to preload the ARP tables of all other local hosts

arpspoof

- ARP spoofing attack is considered as a man-in-the-middle attack.
- **arpspoof** and is distributed in the dsniff package



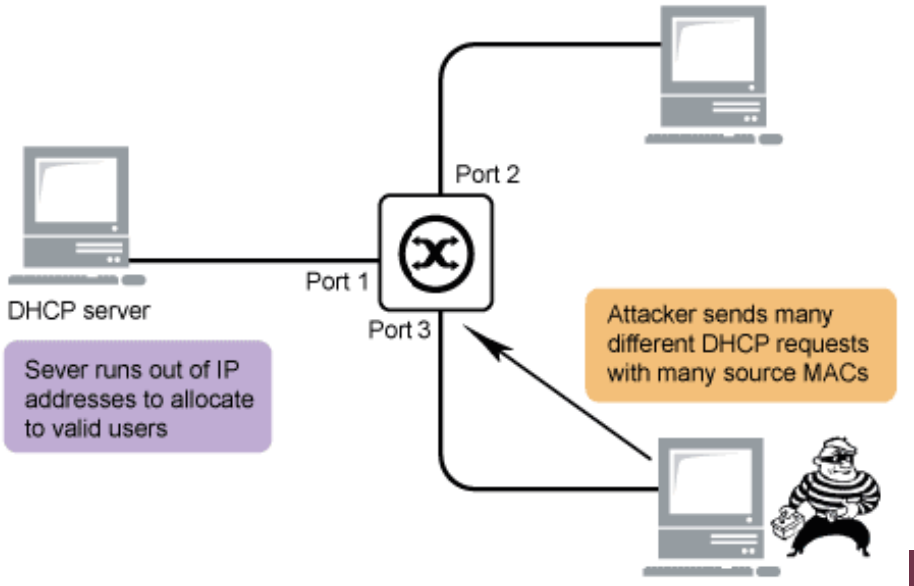

```
# enable ip forwarding
> arpsoof –t victim gateway
> arpsoof –t gateway victim
```

Protect ARP Cache

- Use intrusion detection tools:
  - Detect *fake ARP messages* and maintain *consistency* of the ARP table.
  - *arpwatch* (available on many UNIX platforms) maintains a database of Ethernet MAC addresses seen on the network, with their associated IP pairs.
  - Alerts the system administrator via e-mail if any change happens.
- Use *strong authentication* rather than source IP address
  - VPN protocols like SSH, SSL or IPSec can greatly improve security by achieving authentication, integrity and confidentiality.

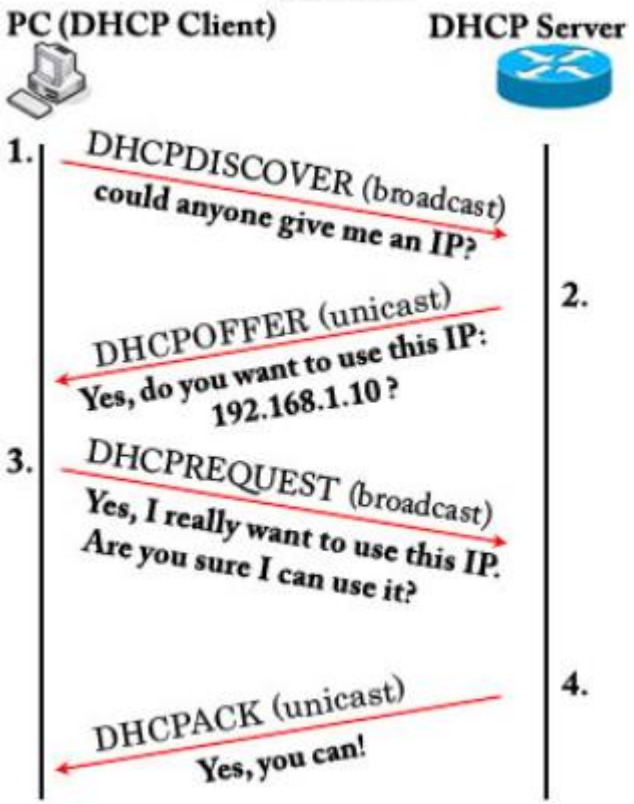
DHCP Starvation

- Attacker inundates DHCP server with countless DHCP requests from different source MAC addresses.
- DHCP server eventually runs out of IP addresses, and valid users are unable to obtain or renew an IP address.
- A type of DoS attack – consumes the resource (IP address)



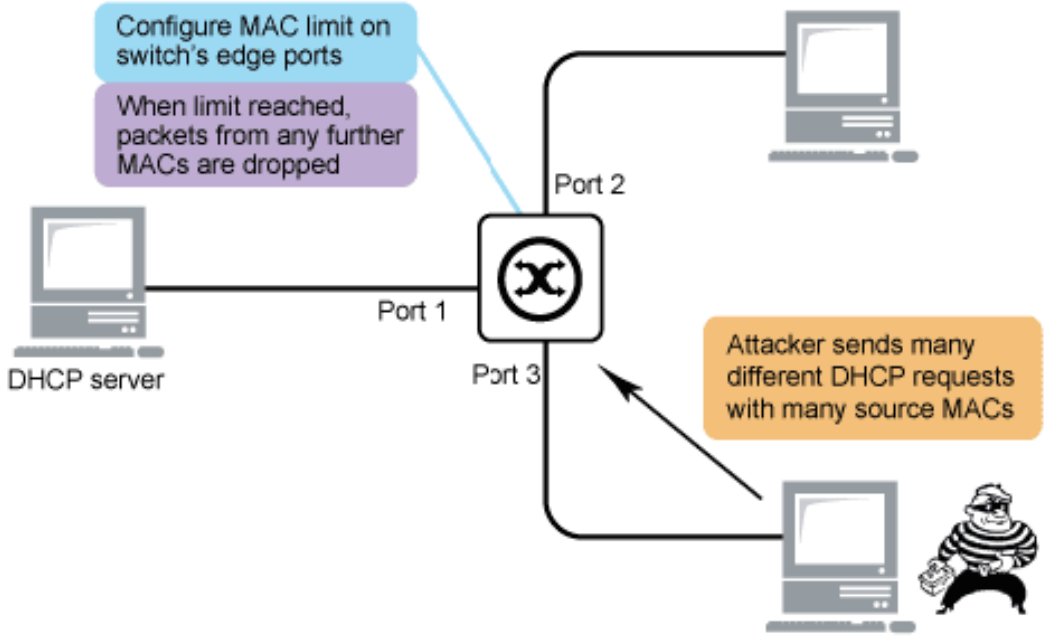
Dynamic Host Configuration Protocol

- DHCP is a protocol used on IP networks for dynamically distributing network configuration parameters
  - IP address, netmask, gateway, and DNS
- DHCP is a UDP protocol and uses different ports for client and server:
  - Port 67 is the destination port of a server
  - Port 68 is used by the client
- Use DHCP from client
  - "iface eth0 inet dhcp" in /etc/network/interfaces
  - "dhclient" to renew IP address



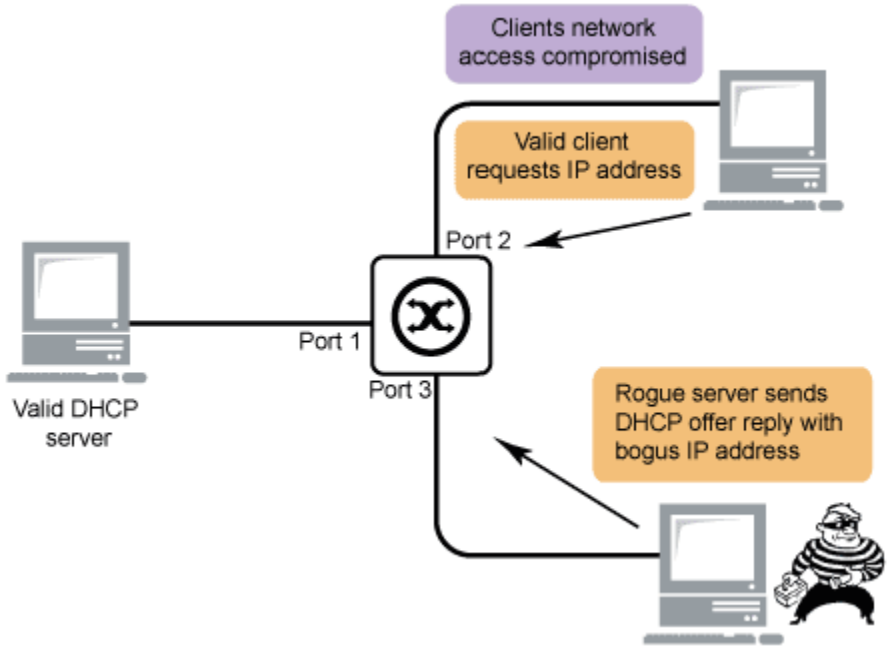
DHCP Starvation Defense

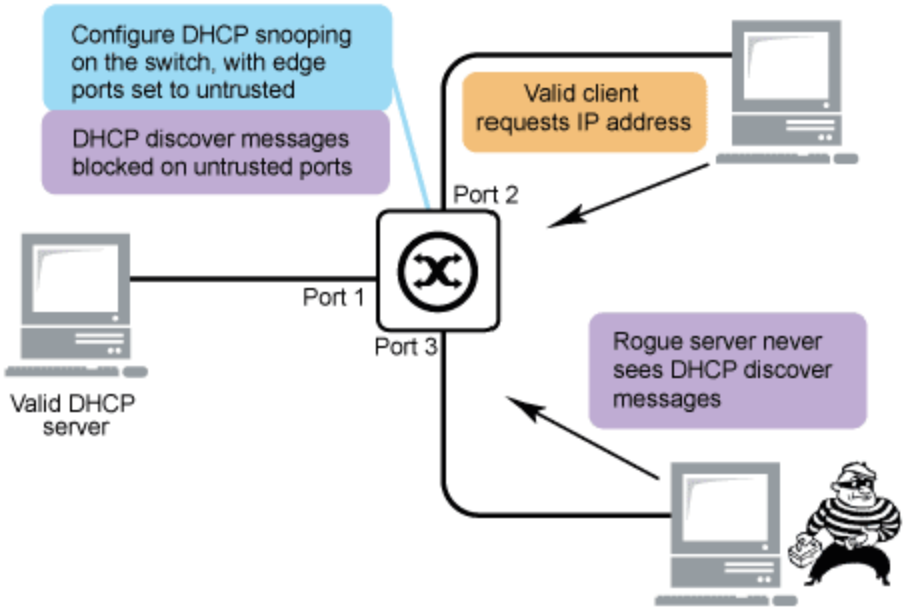
- Implement port security on switch
  - Configure the edge ports with a MAC learn limit



DHCP Rogue Server

- Attacker disguises itself as a DHCP server and response to DHCP requests with a bogus IP address.





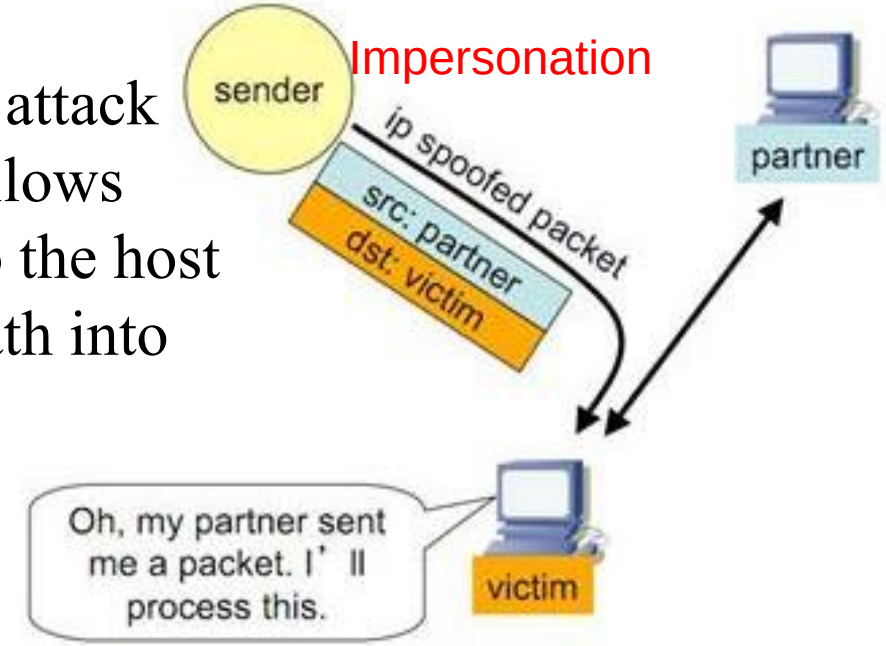
Layer 3 Attacks

Attacks in Layer 3

- The Network Layer (L3) is especially vulnerable to many DoS attacks and information privacy problems.
- The most popular protocol used in L3 is IP (Internet Protocol).
- The following are the key risks at L3 associated with the IP:
  - IP Spoofing
  - Teardrop attack
  - ICMP attacks
  - Ping Flood (ICMP Flood)
  - Ping to Death attack
  - Smurf attack

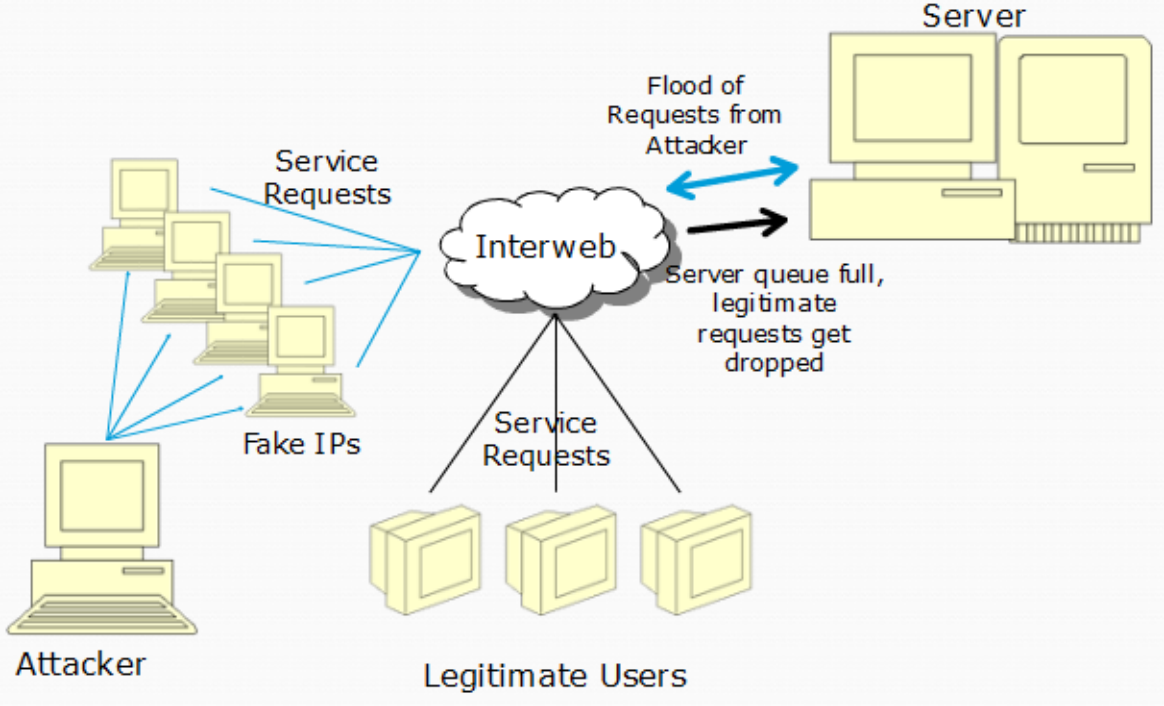
IP Spoofing Attack

- Attacker creates IP packets with a forged *source IP address* to conceal the identity of the sender or to impersonate another computing system.
- The prime goal of an IP spoofing attack is to establish a connection that allows the attacker to *gain root access* to the host and to *create a backdoor* entry path into the target system.
- Spoofing is also sometimes used to refer to ***header forgery*** because attacker forges the header of the packets with fake information.



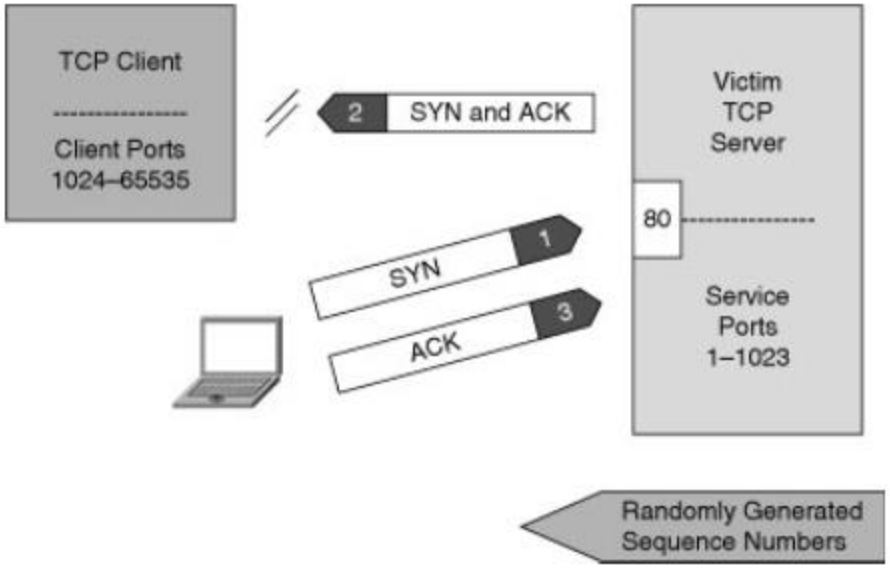
Flooding and DoS attack

- DoS attack with fake IPs
  - Attackers consume *bandwidth* and *resources* by flooding the target with as many packet as possible in a short amount of time.



IP Spoofing – Sequence Number Prediction

- The basis of IP spoofing lies in an inherent security weakness in TCP known as *sequence prediction*.
- Hackers can *guess or predict* the TCP sequence numbers that are used to construct a TCP packet without receiving any responses from the server.
- Their prediction allows them to spoof a trusted host on a local network.



IP spoofing-based attacks

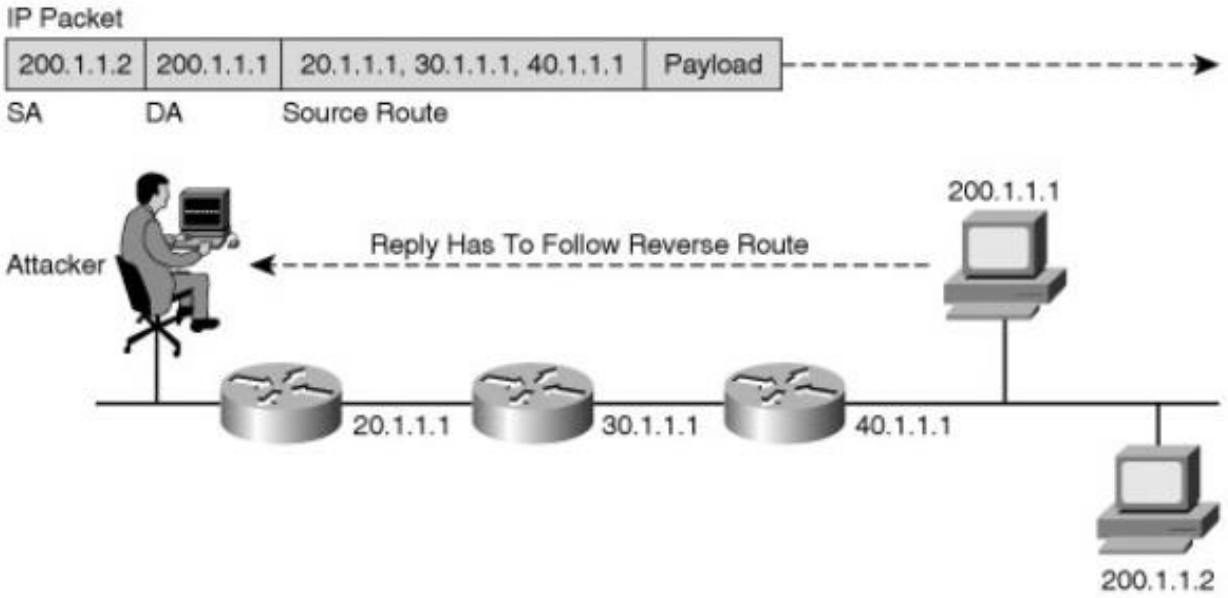
- Two threats in the transport layer rely on IP spoofing (see layer 4 attacks)
  - Session hijacking with non-blind spoofing
  - Blind Spoofing

IP Spoofing with Source Routing

- Strict source routing allows the source machine sending a packet to specify the path (entire route) it will take on the network.
- Loose source routing allows the attacker to specify just some of the hops that must be taken as the packet traverses the network.
- Attacker can locally create an interface with a bogus (spoofed) IP address, source connections from it using the source route options, and the target would return the packets along the reverse path to the spoofed address.
  - Create a type of MITM attack

Source Routing

- Source routing is the ability of the source to specify within the IP header *a full routing path* between endpoints.
- The destination must reply along a reverse path back to the source

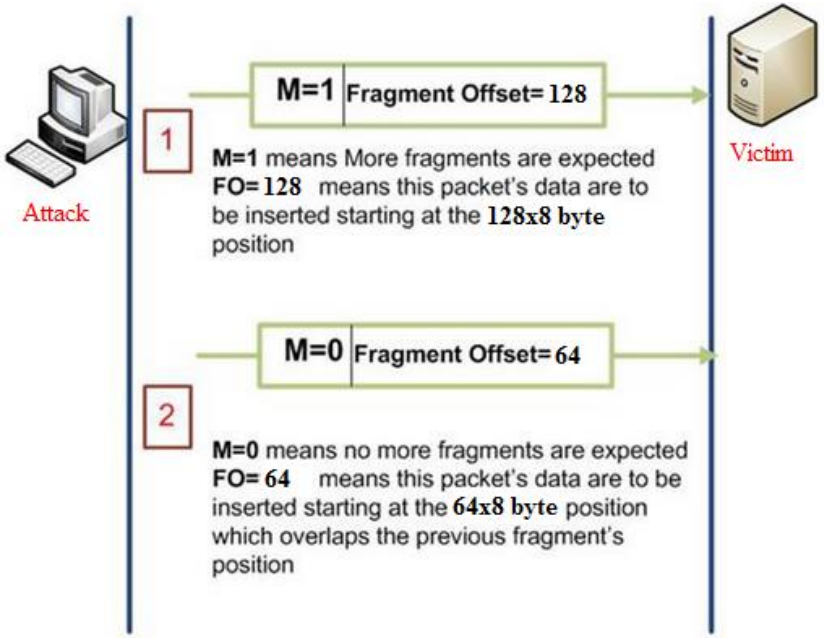


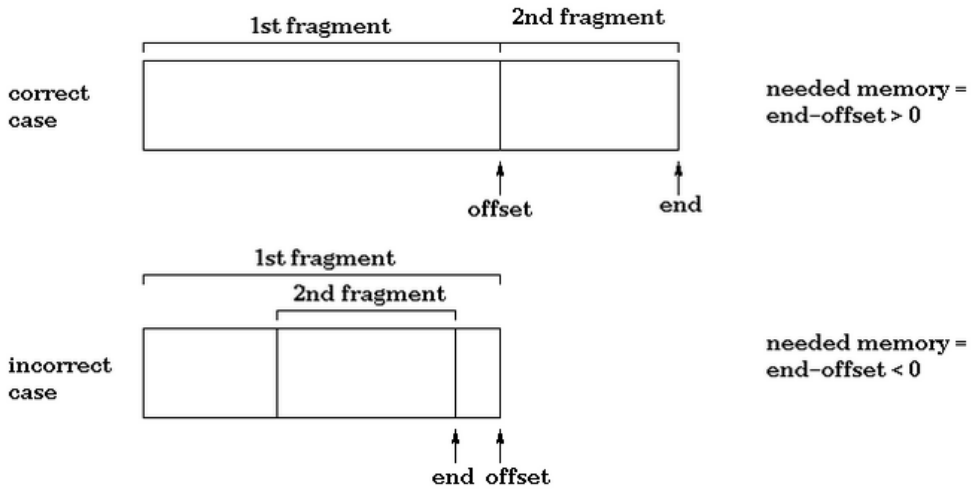
IP Spoofing Defenses

- Avoid applications that use IP addresses for authentication purposes
- Implement “anti-spoof” packet filters an your border routers and firewalls
- Disable source routing
- Avoid extending trust relations among different domains

Teardrop Attack

- Teardrop attack is a type of DoS attack to compromise the *availability* of the target system.
- It consists of an attacker sending a series of *fragmented IP* datagram pairs to the target system, and causes the system crash.





Teardrop Attack Remedy

- Many tools for teardrop attack are available such as
  - targa, SYNdrop, Boink, Nestea Bonk, TearDrop2 and NewTear
- Most modern releases of operating systems contain fixes for the Teardrop DoS attack and its variants.
- A simple reboot is the preferred remedy after this happen.

ICMP Attacks

- ICMP is used to *handle errors* and *exchange control messages*. It can be used to determine if a machine is responding.
- There is *no authentication* in ICMP, which leads to attacks using ICMP that can result in a DoS, or allowing the attacker to intercept packets.
- Forge ICMP messages also cause victim overwhelming.
- *ICMP Redirect message* is commonly used by gateways when a host has mistakenly assumed the destination is not on the local network.
  - If an attacker forges an ICMP "Redirect" message, it can cause another host to send packets for certain connections through the attacker's host.

Ping Flood (ICMP Flood)

- In legitimate situations the *ping* command is used by network administrators to test connectivity between two computers.
- In the *ping flood* attack, it is used to flood *large amounts of data* packets to the victim repeatedly in an attempt to overload it.

Normal Ping packets

```
ubuntu@VM-GW:~$ ping 172.24.55.6 -c 5
PING 172.24.55.6 (172.24.55.6) 56(84) bytes of data.
64 bytes from 172.24.55.6: icmp_req=1 ttl=64 time=0.991 ms
64 bytes from 172.24.55.6: icmp_req=2 ttl=64 time=1.16 ms
64 bytes from 172.24.55.6: icmp_req=3 ttl=64 time=1.03 ms
64 bytes from 172.24.55.6: icmp_req=4 ttl=64 time=0.926 ms
64 bytes from 172.24.55.6: icmp_req=5 ttl=64 time=1.05 ms

--- 172.24.55.6 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.926/1.032/1.163/0.088 ms
```

Large Size of Ping packets

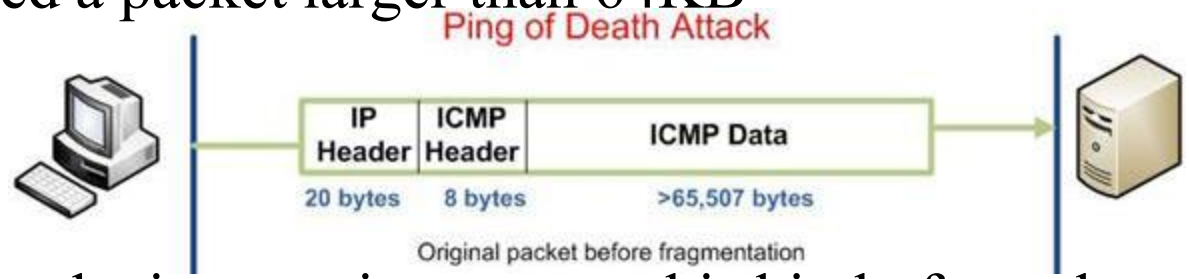
```
ubuntu@VM-GW:~$ ping 172.24.55.6 -c 5 -s 65500
PING 172.24.55.6 (172.24.55.6) 65500(65528) bytes of data.
65508 bytes from 172.24.55.6: icmp_req=1 ttl=64 time=14.5 ms
65508 bytes from 172.24.55.6: icmp_req=2 ttl=64 time=10.3 ms
65508 bytes from 172.24.55.6: icmp_req=3 ttl=64 time=10.0 ms
65508 bytes from 172.24.55.6: icmp_req=4 ttl=64 time=9.99 ms
65508 bytes from 172.24.55.6: icmp_req=5 ttl=64 time=10.2 ms

--- 172.24.55.6 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 9.994/11.025/14.528/1.756 ms
```

- This type of attack is generally useless on larger networks or websites, but it could be a threat if it becomes a *DDoS attack*.

Ping of Death

- *ICMP echo* with *fragmented packets*
- Maximum legal size of an ICMP echo packet:
  65535 - 20 - 8 = 65507
- *IP Fragmentation* allows bypassing the maximum size:
  (offset + size) > 65535 (64KB)
- OS cannot reassembled a packet larger than 64KB
  - It causes OS crash, reboot or hang

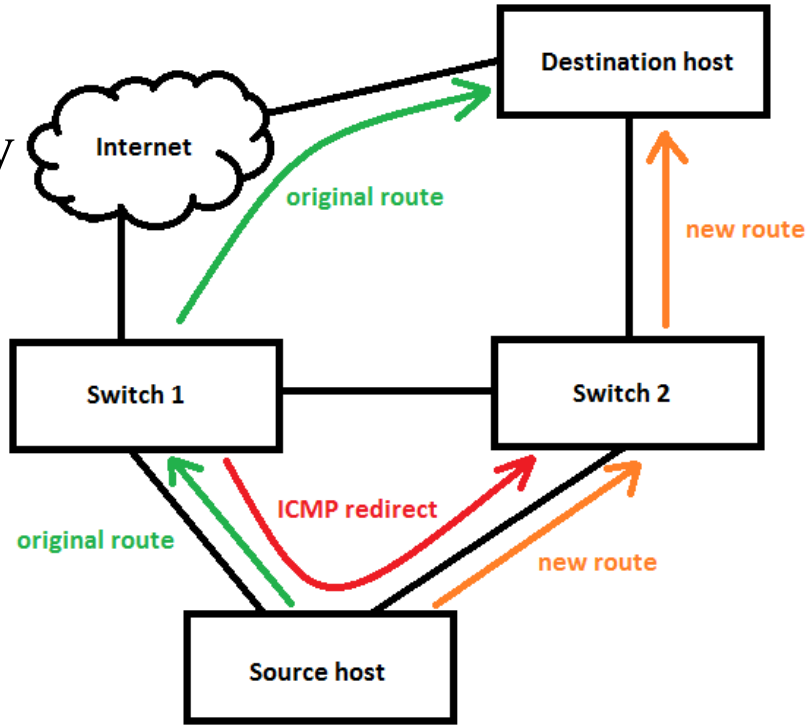


- Most of modern OS or devices are immune to this kind of attack.
- IDS signature: for any fragment offset + length > 64KB

alert icmp any any -> any any (**dsize:>65507**; msg:"Ping of Death Detected"; sid:7777);

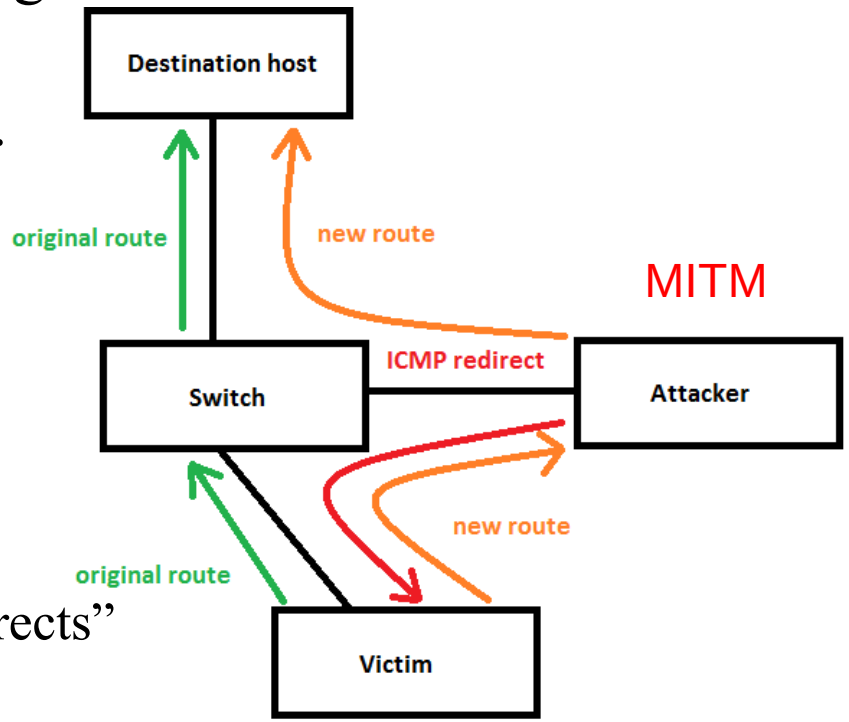
ICMP Redirect

- ICMP redirect is used to redirect source hosts to use a different gateway that is typically *closer* to the destination host.
- When the source host receives an ICMP redirect message it should *adapt its routing tables* accordingly and send the next packets through the new route.
  - This is often seen in combination with *source routing*.
- Usually, hosts should not send ICMP redirects and only gateways are allowed to do so.



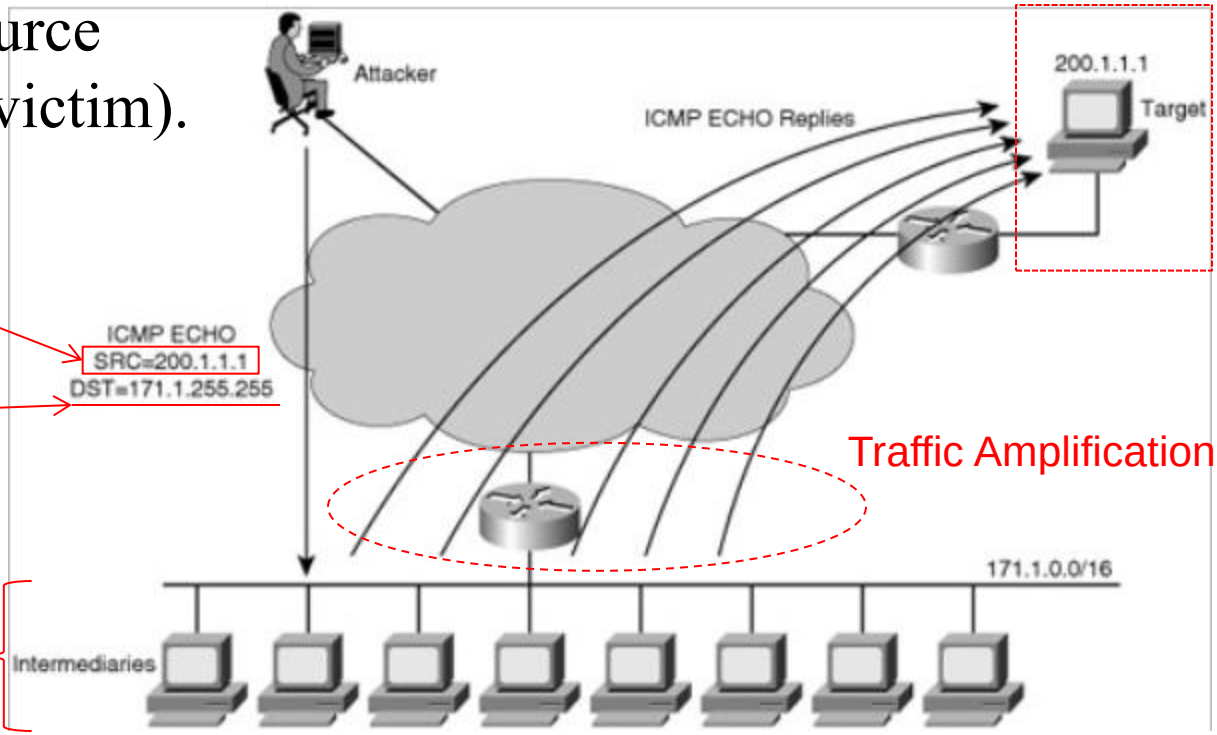
ICMP Redirect Attack

- The attacker simply sends ICMP redirect packets to the victim, to imitate a new optimal gateway.
- The victim re-route the traffic through the attacker and thus allowing the attacker to sniff its communication.
- The attacker can even spoof the source IP and MAC addresses to look as if it is coming from the real gateway.
- Countermeasure:
  - Disable "net.ipv4.conf.all.accept_redirects" in /etc/sysctl.conf.



Smurf Attack

- Smurf attack is a type of DoS attack where attacker spoofs *ICMP Echo Request* to a network *broadcast address*.
- All hosts that receive the Echo Requests will response to the spoofed source address (a victim).



severe network congestion

Forged IP

Broadcast IP

Traffic Amplification

If they do not filter ICMP traffic directed to IP broadcast address

Smurf Attack Defenses

- Put *filters* on routers and firewall to counteract *address spoofing*.
  - A *source IP address* should be assigned to the *same LAN segment*.
- Disable *directed IP broadcast packets* at firewall
  - Eliminate all ping request to a broadcast address
- IDS signature
  - Any node sending ping broadcast request more than some threshold within a time window

alert **icmp** any any -> any 172.24.55.**255** (msg:"stop smurfing me"; sid: 888)