Network Components and Network Based Attacks

November 2018

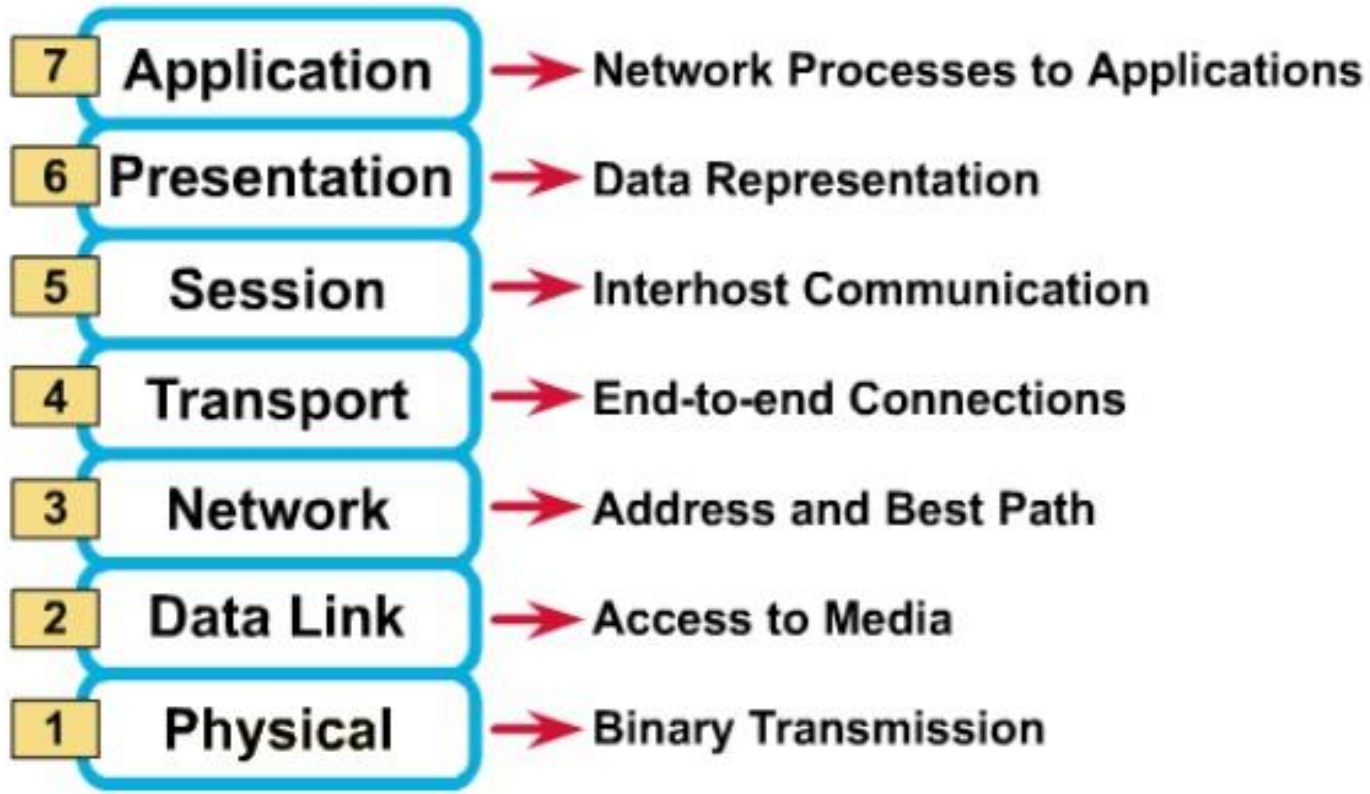
CS479 – Introduction to Cyber Security

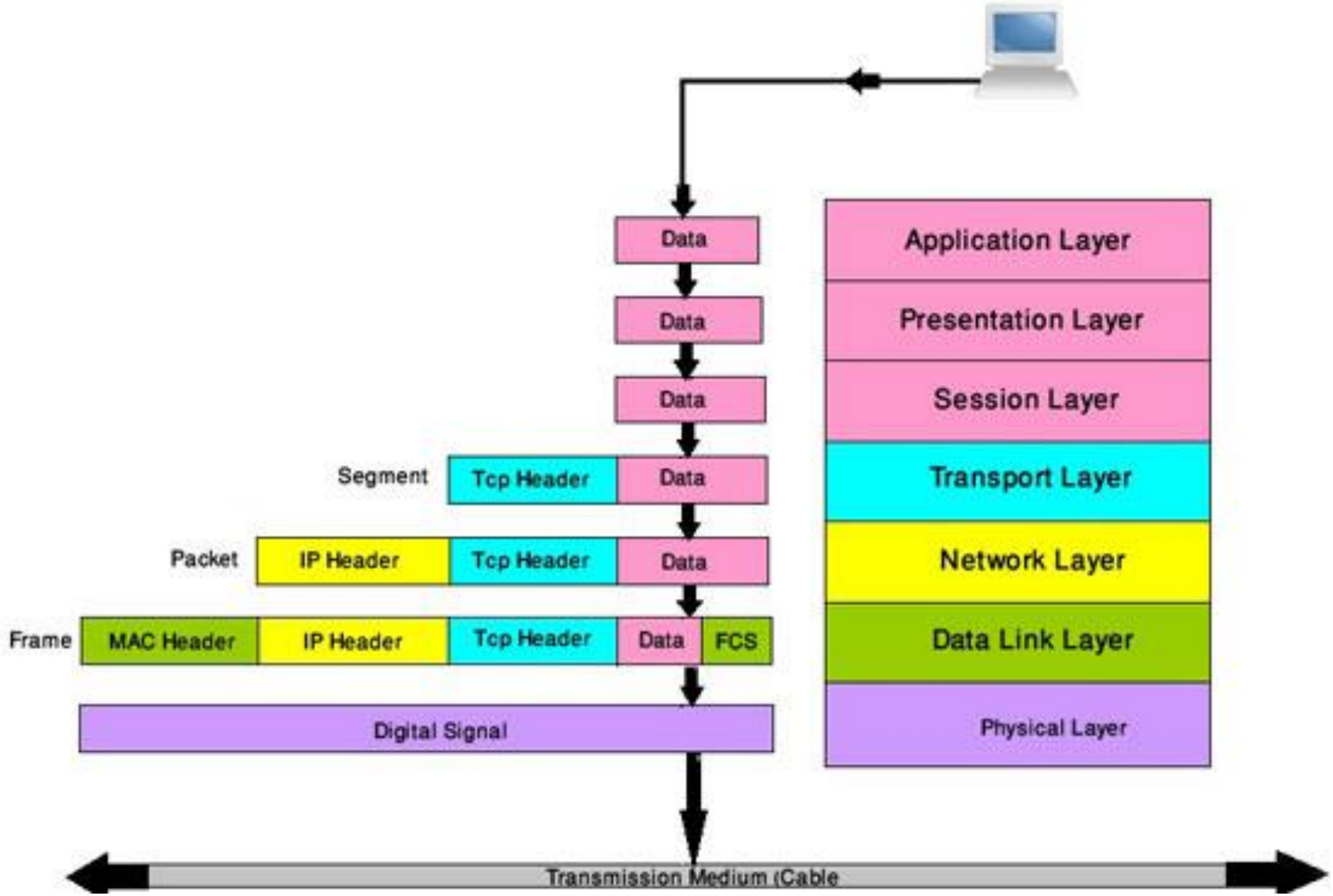
Bilkent University

Emre Yüce, Phd

Corporate Cyber Sec. Services Team Leader @HAVELSAN

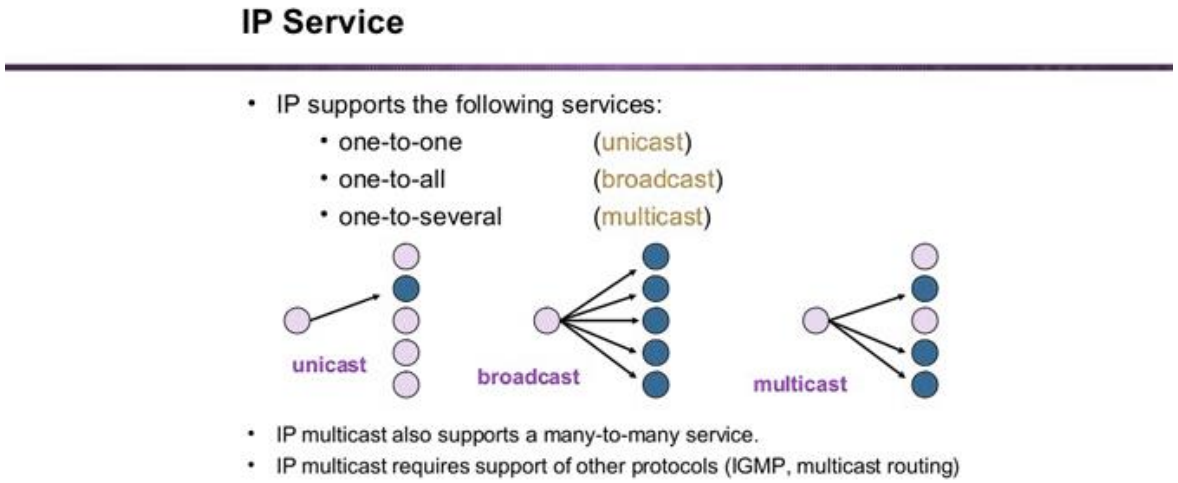
OSI Reference Model: 7 Layers




Data
Data
Data
Segment
Tcp Header
Data
Packet
IP Header
Tcp Header
Data
Frame
MAC Header
IP Header
Tcp Header
Data
FCS
Digital Signal
Transmission Medium (Cable
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Network Packet Types

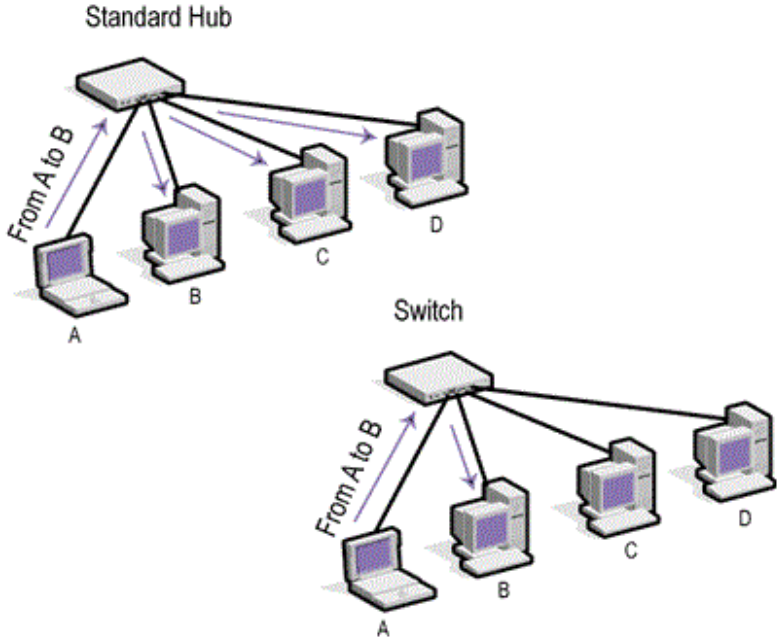
- Unicast: from one source to one destination i.e. One-to-One
- Broadcast: from one source to all possible destinations i.e. One-to-All
- Multicast: from one source to multiple destinations stating an interest in receiving the traffic i.e. One-to-Many



* https://www.esds.co.in/blog/difference-between-unicast-broadcast-and-multicast/#sthash.43xqyUom.dpbs

Switch vs Hub

- Switch learns MAC addresses at each port.
- Hub does not learn MAC addresses.
  - Each component can sniff network packets.



Network Addressing

- MAC address
  - 00:11:22:AA:BB:CC
- IPv4 addresses: 32 bit
  - Private IPv4 addresses

RFC1918 name	IP address range	number of addresses	largest CIDR block (subnet mask)	host id size	mask bits	*classful* description[Note 1]
24-bit block	10.0.0.0 – 10.255.255.255	16 777 216	10.0.0.0/8 (255.0.0.0)	24 bits	8 bits	single class A network
20-bit block	172.16.0.0 – 172.31.255.255	1 048 576	172.16.0.0/12 (255.240.0.0)	20 bits	12 bits	16 contiguous class B networks
16-bit block	192.168.0.0 – 192.168.255.255	65 536	192.168.0.0/16 (255.255.0.0)	16 bits	16 bits	256 contiguous class C networks

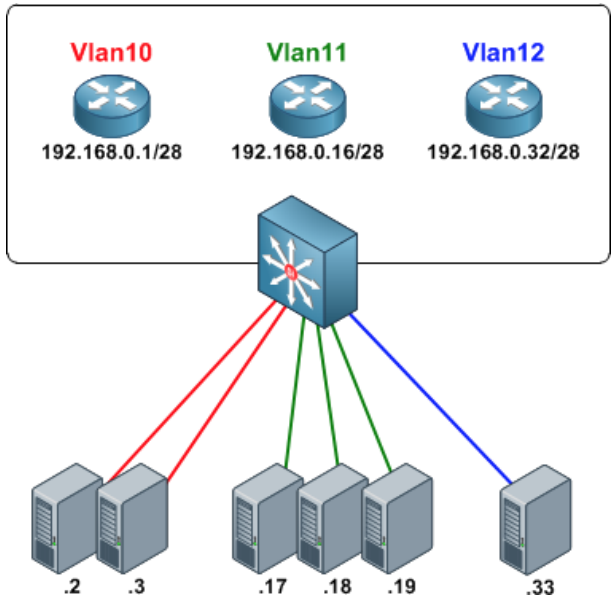
  - Public IPv4 addresses
- IPv6 addresses: 128 bit
- Subnet: CIDR notation!
- Default gateway

Classless Inter-Domain Routing (CIDR)

- 192.168.100.14/24 represents
  - the IPv4 address 192.168.100.14 and
  - its associated routing prefix 192.168.100.0,
  - or equivalently, its subnet mask 255.255.255.0,
  - which has 24 leading 1-bits.
- the IPv4 block 192.168.100.0/22 represents
  - the 1024 IPv4 addresses from 192.168.100.0 to 192.168.103.255.
- the IPv6 block 2001:db8::/48 represents
  - the block of IPv6 addresses from 2001:db8:0:0:0:0:0:0 to 2001:db8:0:ffff:ffff:ffff:ffff:ffff.
- ::1/128 represents the IPv6 loopback address. Its prefix length is 128 which is the number of bits in the address.

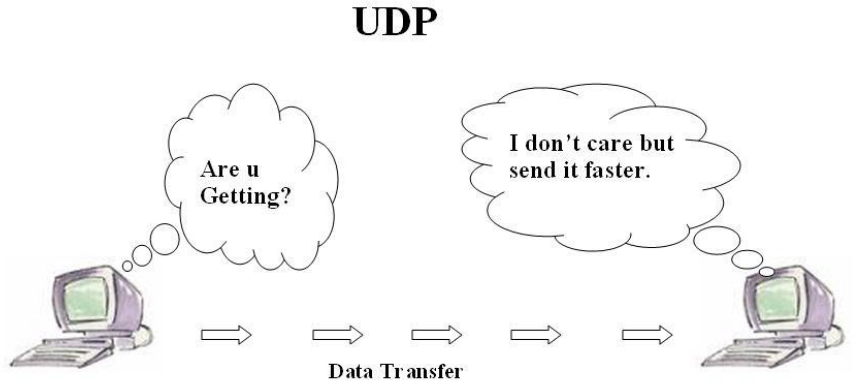
Virtual LAN (VLAN)

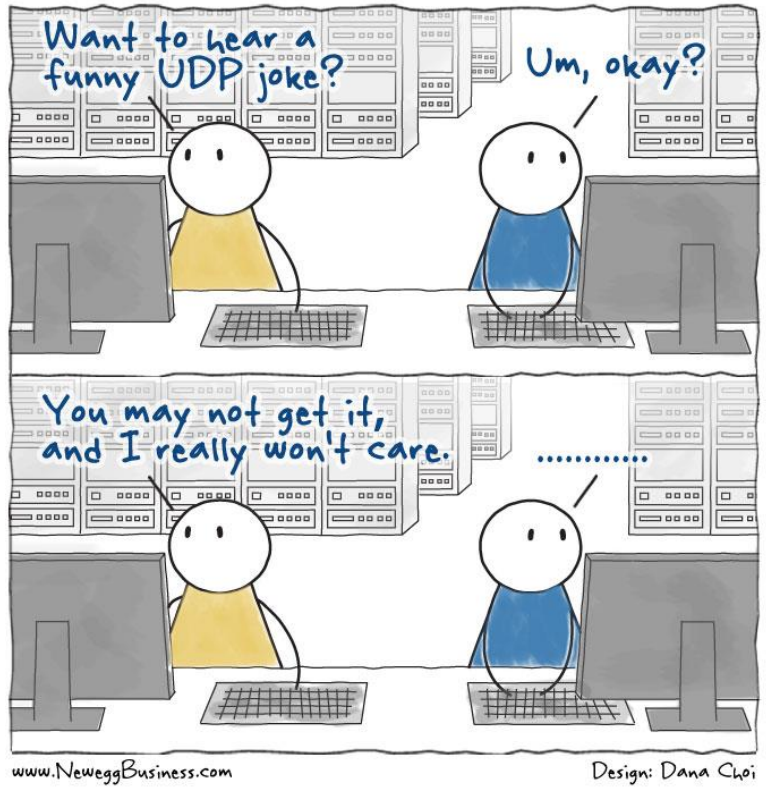
- Port definitions
  - access/untagged
  - trunk/tagged



User Datagram Protocol (UDP)

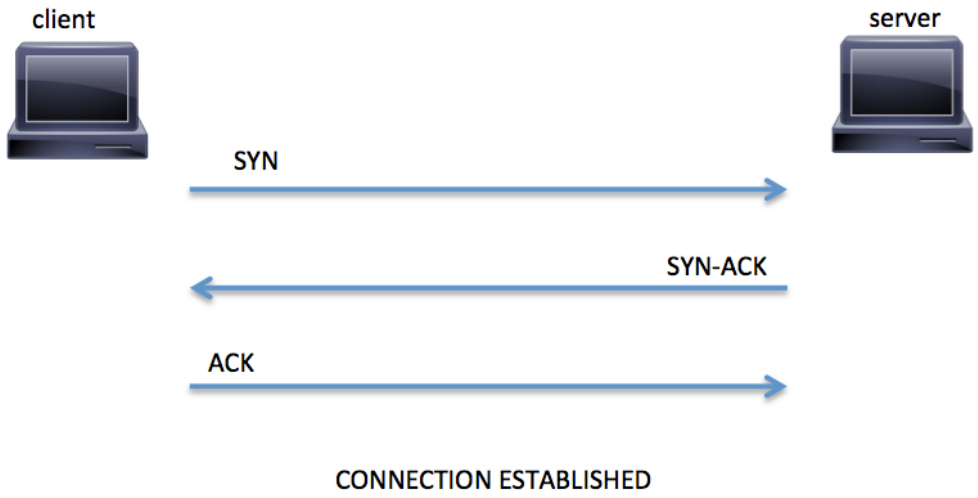
- Video, audio etc.
- Connectionless protocol
- Low-latency and loss-tolerating connections





Transmission Control Protocol (TCP)

- Connection-oriented protocol
- HTTP, FTP, SMTP etc.



Port Number	Protocol	Application
20	TCP	FTP data
21	TCP	FTP control
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP, TCP	DNS
67, 68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP (WWW)
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL

Internet Control Message Protocol (ICMP)

- Used by network devices, including routers, to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached.

Command Network Commands

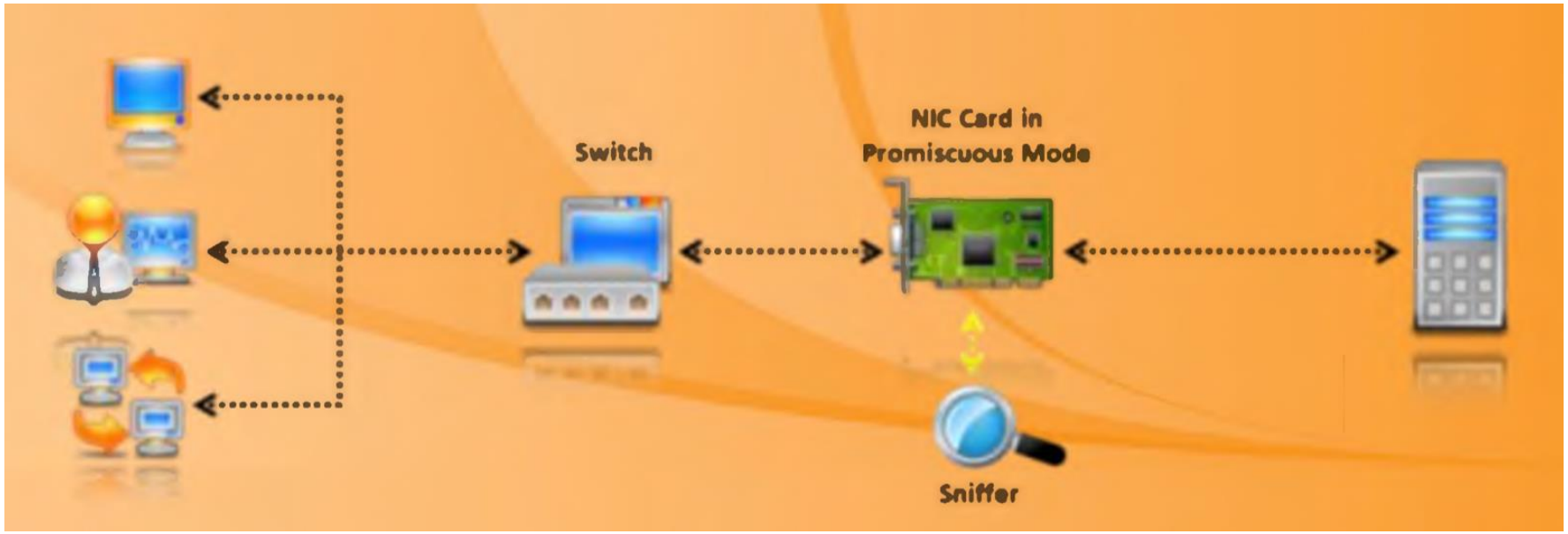
- Ping
- Netstat
- Telnet
- Traceroute/tracert
- Route
- ifconfig
- ipconfig
- Arp
- Nslookup
- Dig

Network Based Attacks

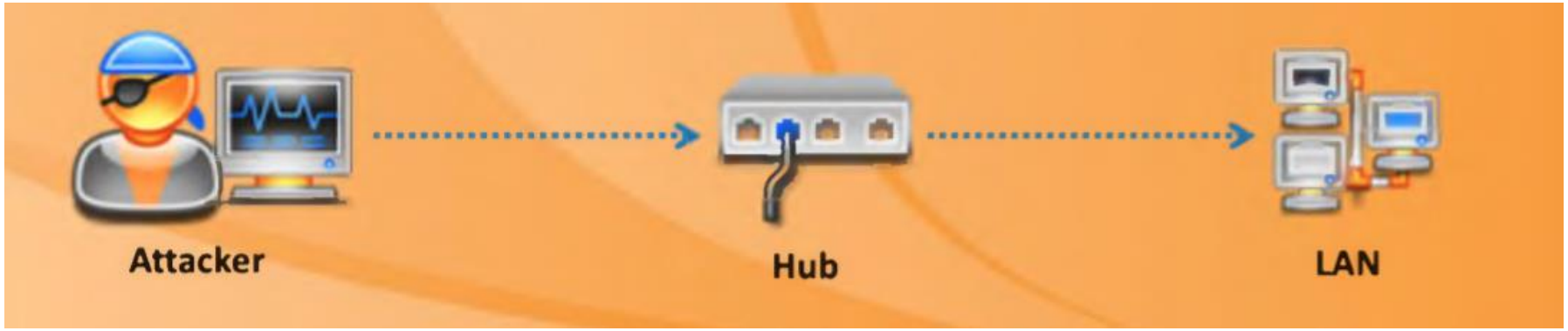
- Packet Sniffing
- Data Modification
- Spoofing
- Denial of Service
- Man-in-the-Middle

Packet Sniffing

- You can have
  - Email addresses and content
  - Username, passwords
  - Web traffic
  - DNS requests
  - Syslog



- Passive



- Active
  - Span/monitor port
  - Different attacks
    - Mac Flooding
    - ARP Poisoning
    - DHCP

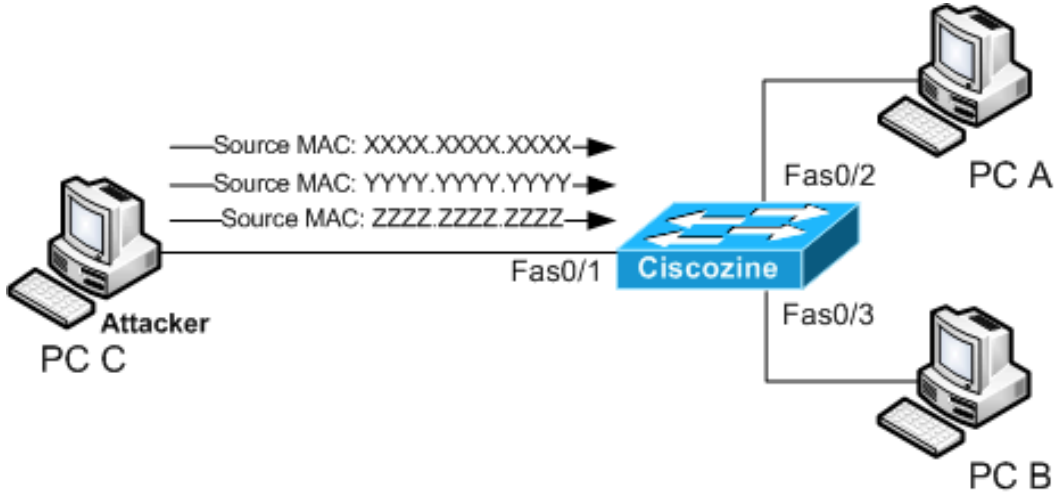
MAC Address Table

```
switch1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0011.5ccc.5c00    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    0009.5b44.9d2c    DYNAMIC     Fa0/1
   1    000f.66e3.352b    DYNAMIC     Fa0/1
   1    0012.8015.c940    DYNAMIC     Fa0/24
   1    0012.8015.c941    DYNAMIC     Fa0/24
   1    001a.adb3.bef7    DYNAMIC     Fa0/1
   1    0025.2266.d104    DYNAMIC     Fa0/1
   1    0026.b865.313e    DYNAMIC     Fa0/1
   1    64a7.6973.8e4d    DYNAMIC     Fa0/1
   1    6c71.d976.fce7    DYNAMIC     Fa0/1
   1    74f6.12d4.1e1c    DYNAMIC     Fa0/1
   1    a477.3344.98b6    DYNAMIC     Fa0/1
```

MAC Flooding Attack

- MAC table full
  - Traffic sent to all devices!



[redacted] - PuTTY

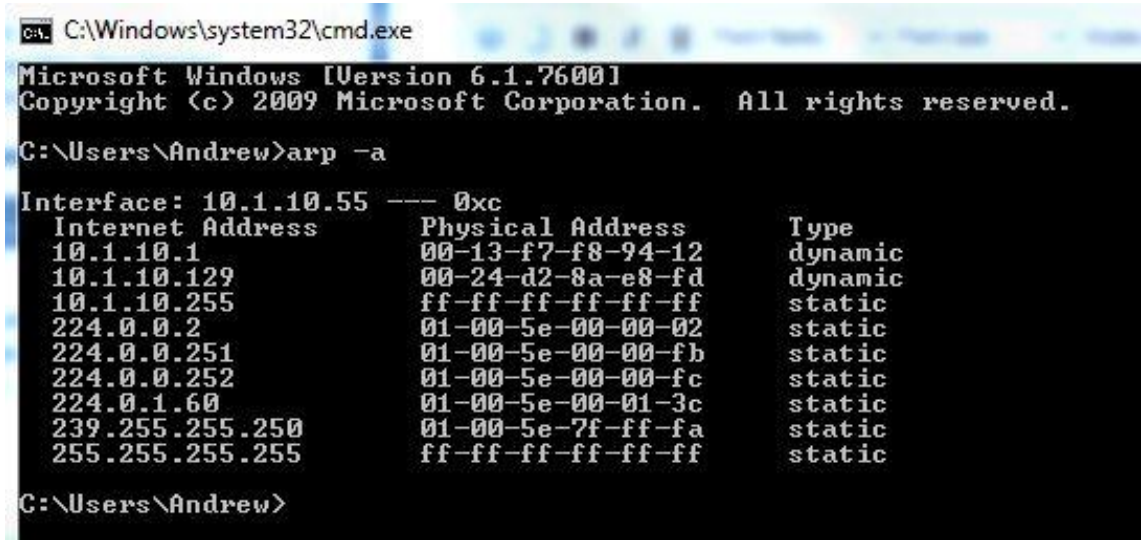
```
ciscoasa(config)#
ciscoasa(config)# show mac-address-table
interface                  mac  address          type       Age(min)
-------------------------------------------------------------------
outside                   f0de.f14e.01b2          dynamic     5
outside                   0010.4b33.4977          dynamic     4
outside                   0003.ba06.4b18          dynamic     5
inside                    0018.b924.4a83          dynamic     3
outside                   0003.ba06.5b60          dynamic     4
outside                   0016.cbac.c80a          dynamic     5
outside                   0024.7e13.e3be          dynamic     3
outside                   001a.3052.6c00          dynamic     5
outside                   0003.ba06.4ba8          dynamic     4
outside                   0012.7947.a2c0          dynamic     5
outside                   0014.38de.bb1e          dynamic     5
outside                   0017.088b.4cfe          dynamic     5
outside                   0014.38de.7cc0          dynamic     5
outside                   000f.4401.b7ae          dynamic     1
outside                   0003.ba0c.4039          dynamic     5
outside                   0014.5e88.22c6          dynamic     5
outside                   0003.ba06.4858          dynamic     4
outside                   0017.088b.6c7b          dynamic     5
outside                   0027.13b1.3cb6          dynamic     4
outside                   c42c.030a.abea          dynamic     5
```

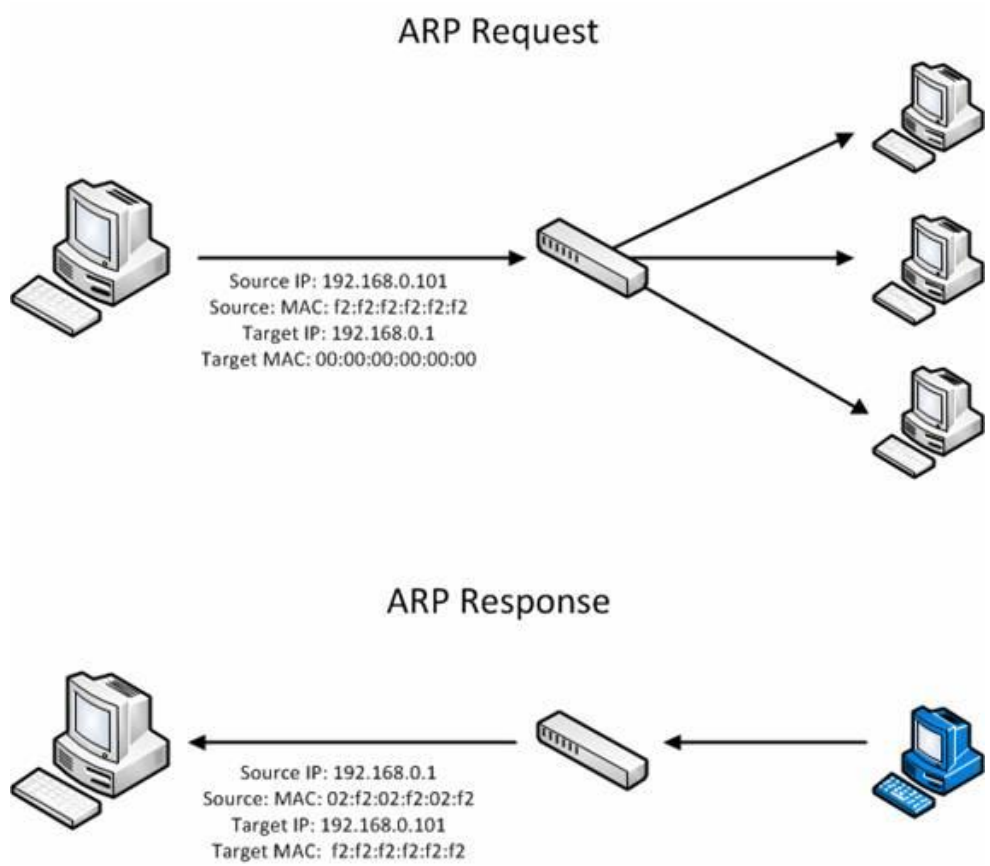
MAC Flooding Attack

- Tools
  - Macof
  - Yersinia
- Precautions
  - Port security:
    - Define MAC addresses static
    - Limit number of MAC addresses

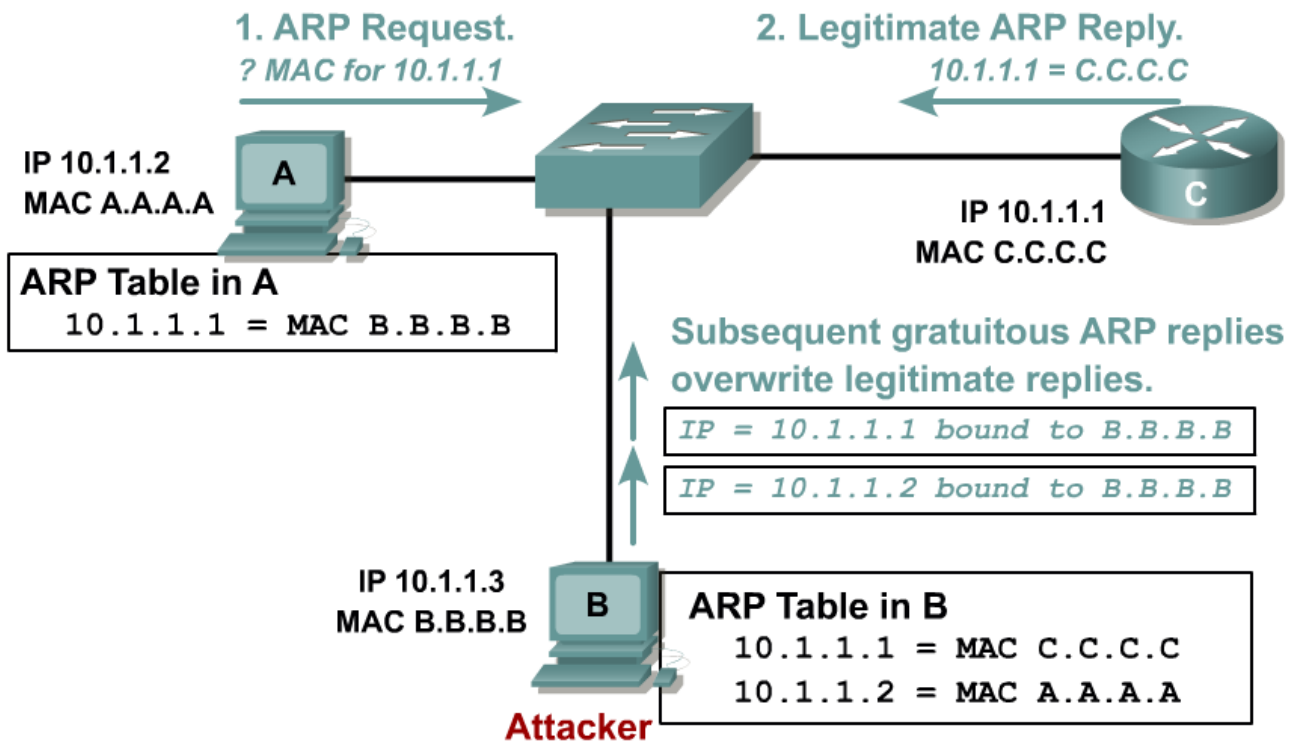
Address Resolution Protocol (ARP)

- IP-MAC relation
- Broadcast packets





ARP Poisoning Attack (MITM Attack)



ARP Poisoning Attack

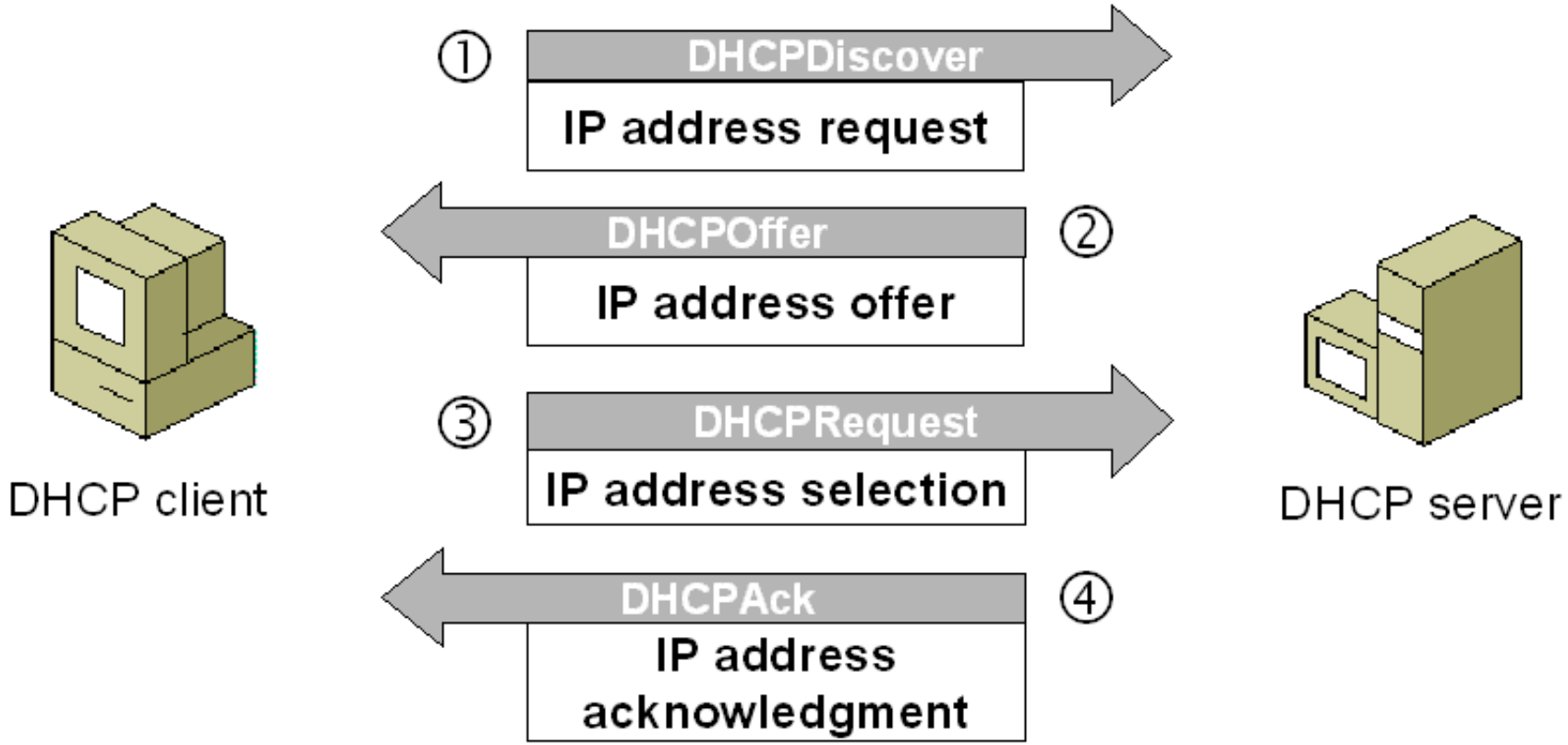
- Tools:
  - Arpspoof
  - Ettercap
  - Driftnet
  - NetworkMiner
  - Cain&Abel

ARP Poisoning Attack

- Precaution: Dynamic ARP inspection
  - On the switch
  - Using DHCP snooping database
  - Drops packet if IP-MAC is not valid.

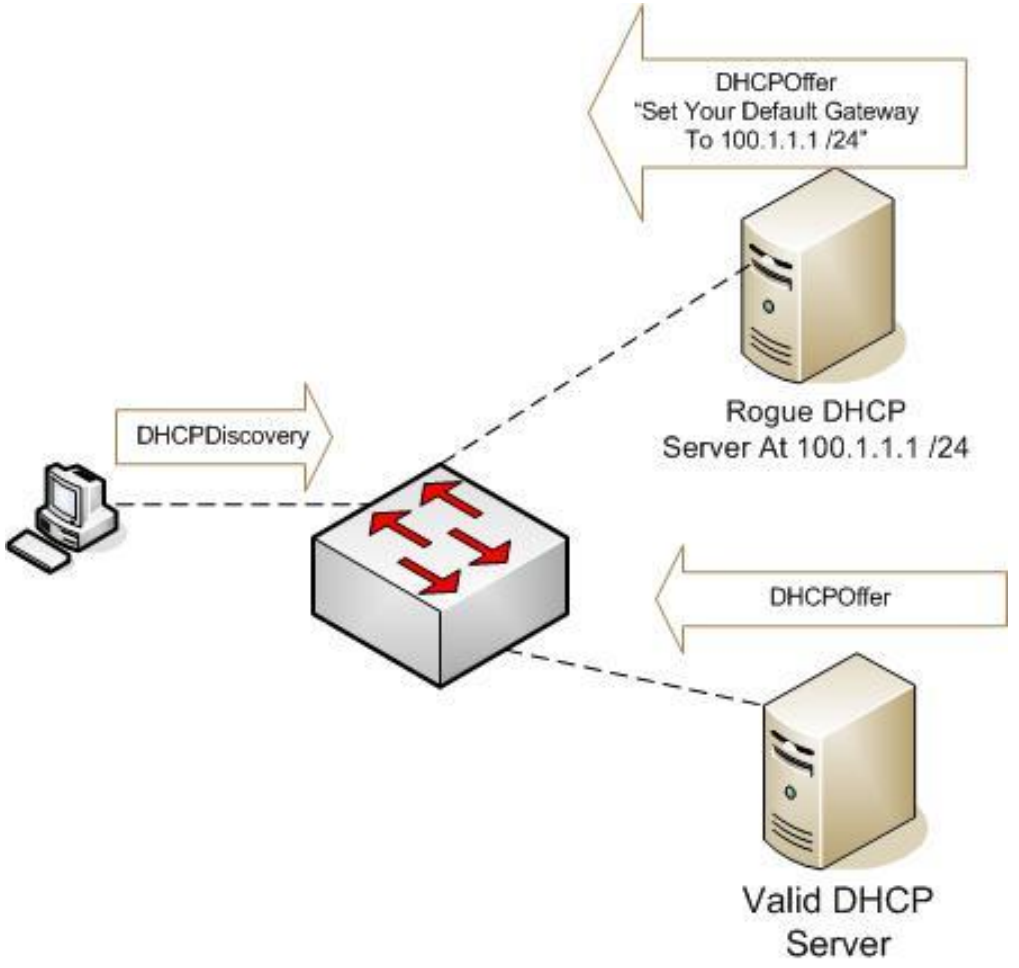
```
Switch#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:90:2B:5C:23:5A   192.168.1.10     86400       dhcp-snooping  1     FastEthernet0/2
00:01:97:99:01:4E   192.168.1.11     86400       dhcp-snooping  1     FastEthernet0/3
00:00:0C:5E:77:6D   192.168.1.12     86400       dhcp-snooping  1     FastEthernet0/2
00:90:2B:E6:02:63   192.168.1.13     86400       dhcp-snooping  1     FastEthernet0/2
00:02:17:D8:A2:56   192.168.1.14     86400       dhcp-snooping  1     FastEthernet0/2
00:50:0F:EA:87:05   192.168.1.15     86400       dhcp-snooping  1     FastEthernet0/2
00:30:A3:C8:95:47   192.168.1.16     86400       dhcp-snooping  1     FastEthernet0/2
00:60:70:01:D3:79   192.168.1.17     86400       dhcp-snooping  1     FastEthernet0/2
00:60:3E:33:A2:66   192.168.1.18     86400       dhcp-snooping  1     FastEthernet0/2
00:40:0B:A2:84:C6   192.168.1.19     86400       dhcp-snooping  1     FastEthernet0/2
00:09:7C:79:60:1E   192.168.1.20     86400       dhcp-snooping  1     FastEthernet0/2
00:E0:A3:87:85:D4   192.168.1.21     86400       dhcp-snooping  1     FastEthernet0/2
00:D0:BA:32:36:B0   192.168.1.22     86400       dhcp-snooping  1     FastEthernet0/2
00:30:F2:47:58:6E   192.168.1.24     86400       dhcp-snooping  1     FastEthernet0/2
Total number of bindings: 14
```

Dynamic Host Configuration Protocol (DHCP)



DHCP Rogue Server

- DHCP uses broadcast packets
  - Everyone can see!



DHCP Starvation

- DHCP IP pool is limited.
- What if you ran out of IP addresses?
  - New devices can not obtain IP address, yet can not join the network.
- A type of denial of service (DOS) attack.

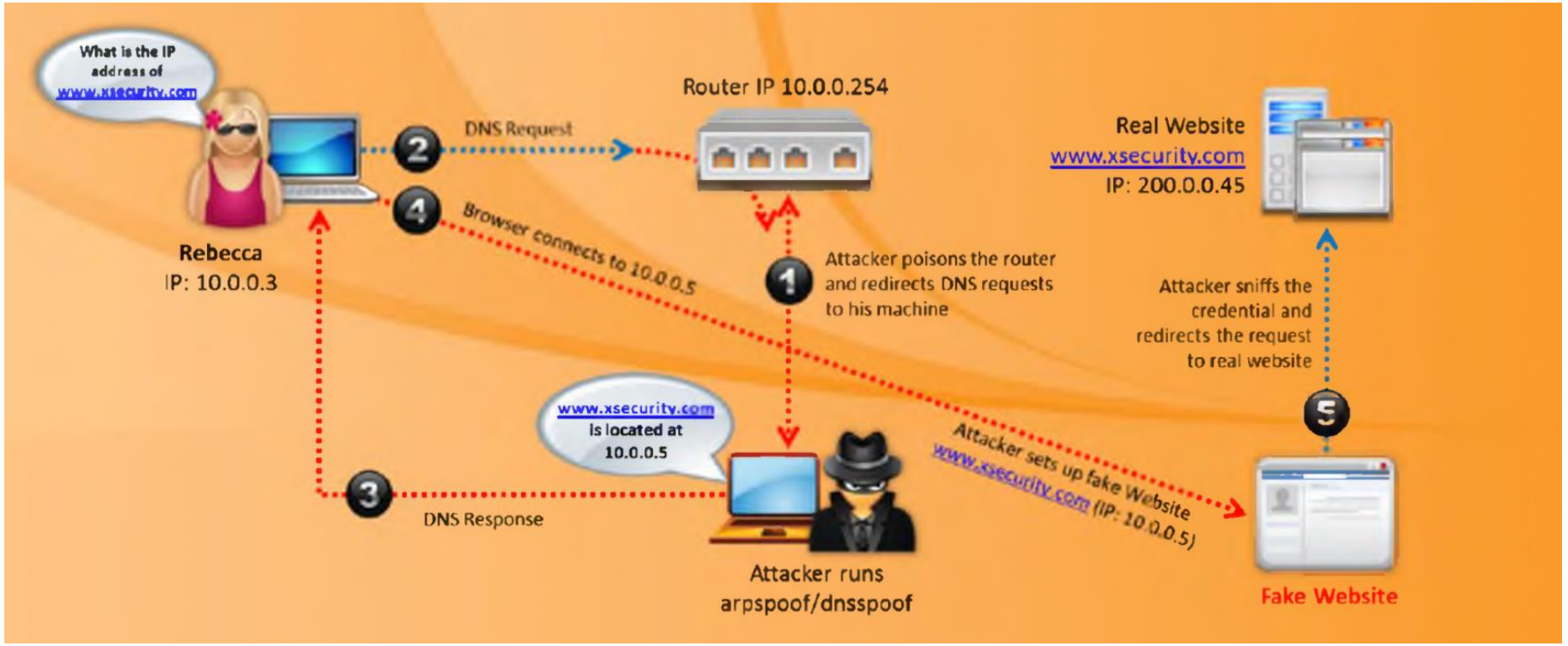
DHCP Attacks

- Precaution
- DHCP snooping
  - Block DHCP responses from user ports
  - Define authoritative DHCP server, drop packets from other DHCP servers.

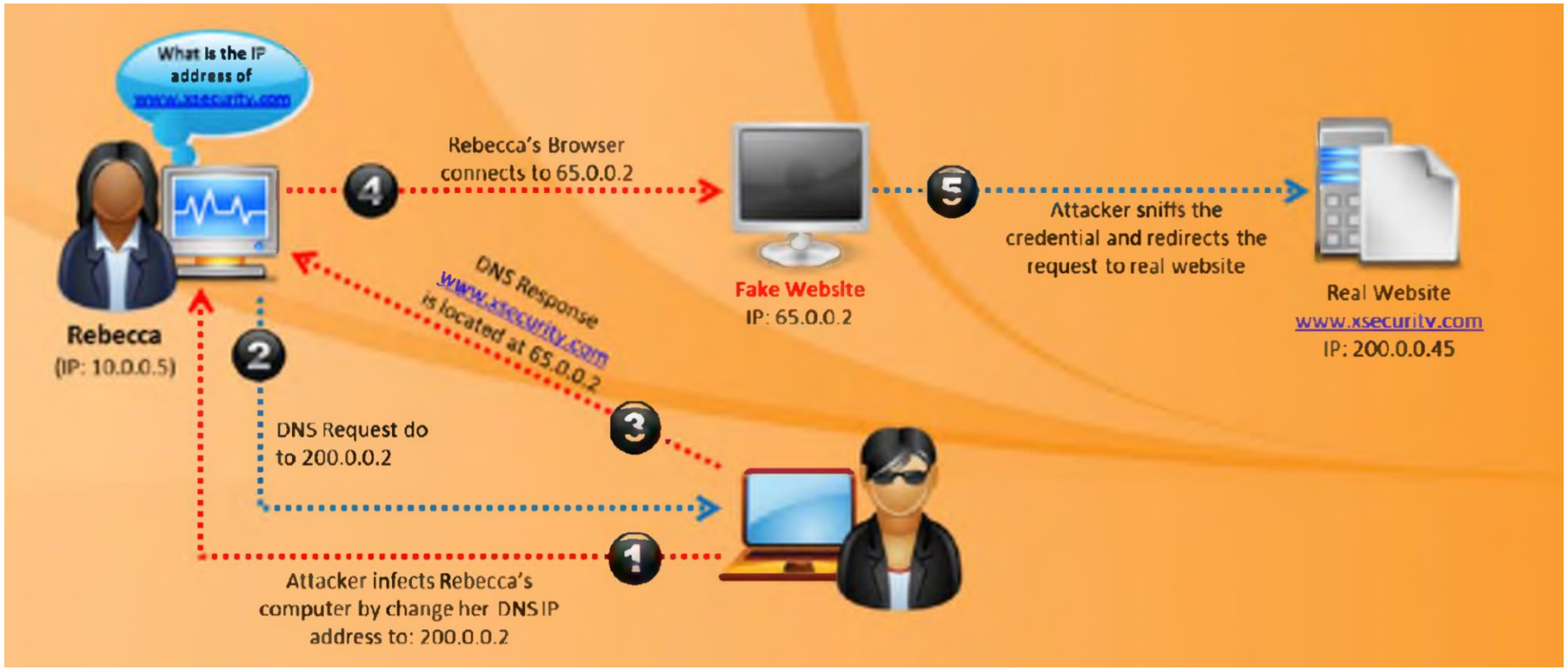
Domain Name System (DNS)

- Domain name – IP address relation
- Record types
  - A: IP address
  - CNAME: Alias
  - MX: Mail server
  - NS: DNS server
  - PTR: Reverse record
- nslookup -type=mx
- dig google.com A

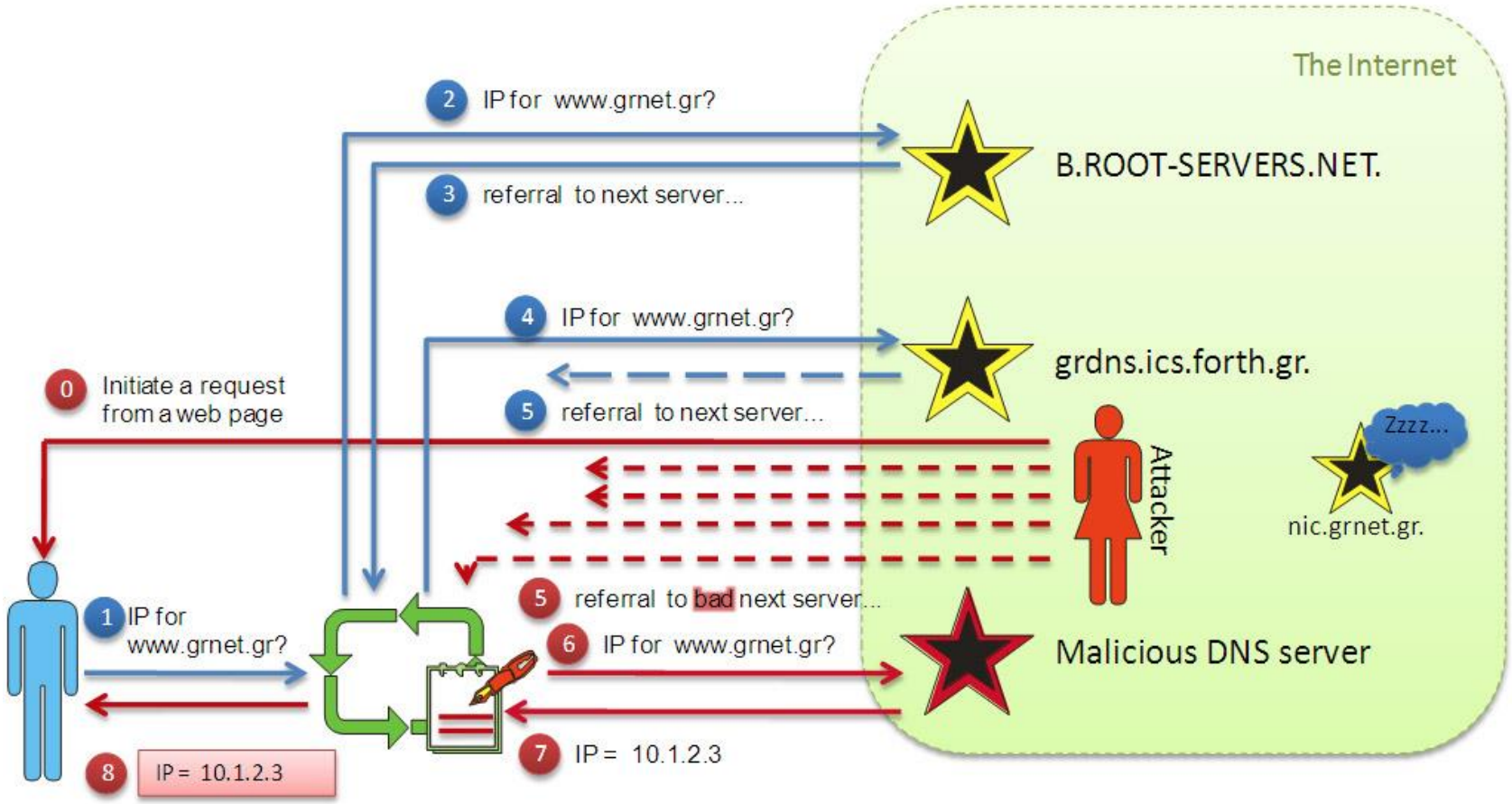
DNS Spoofing



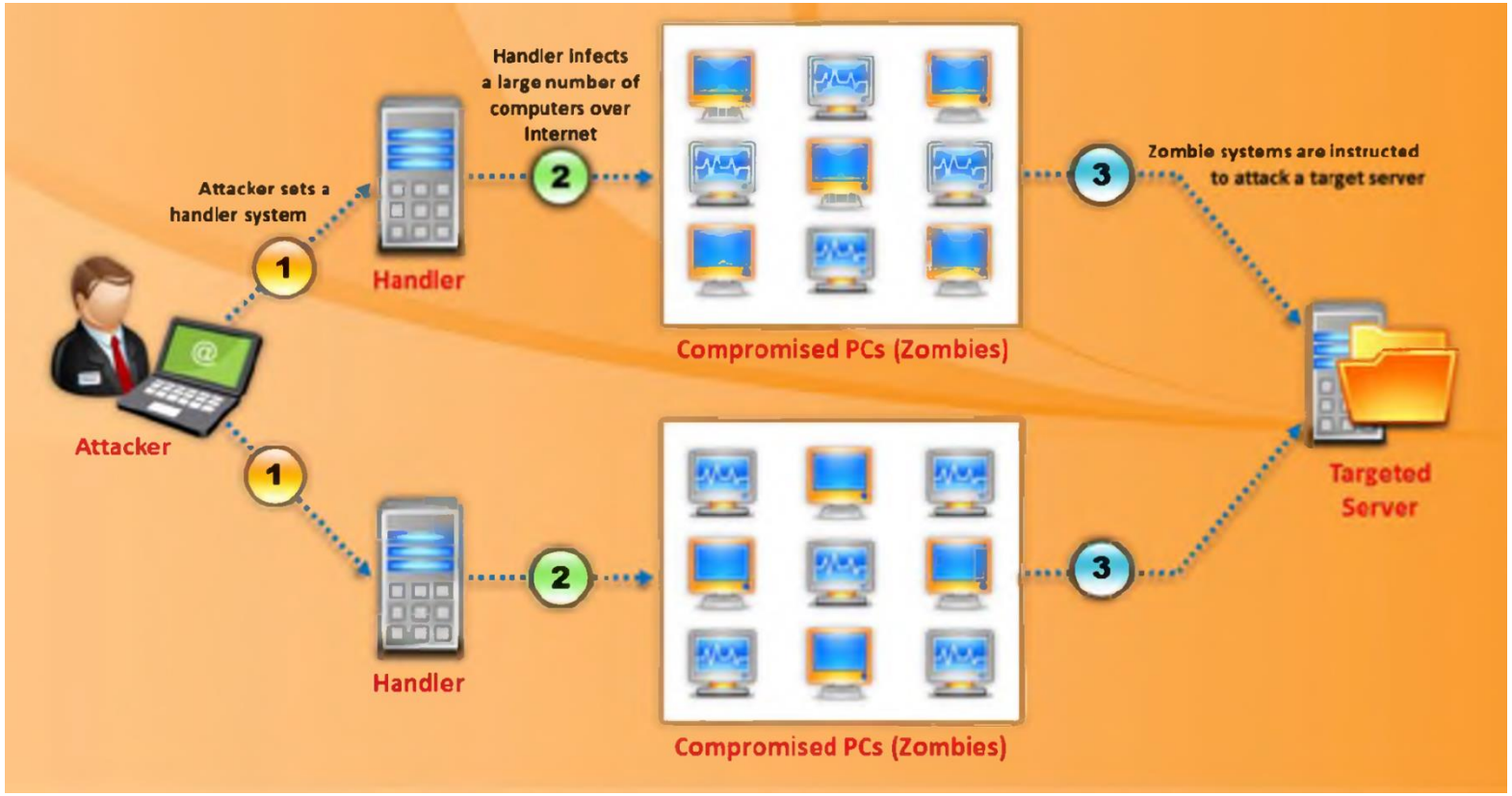
DNS Spoofing



DNS Cache Poisoning



DoS – DDoS Attacks



DoS – DDoS Attacks

- Bandwidth attacks
- Number of connections
- SYN/ACK/FIN Flood
- UDP Flood
- ICMP Flood
- Application layer attacks

DoS – DDoS Attacks

- Tools
  - Low Orbit Ion Cannon
  - High Orbit Ion Cannon
  - Hping
  - DoSHTTP
  - PHPDoS