

Attacks and Mitigation Techniques

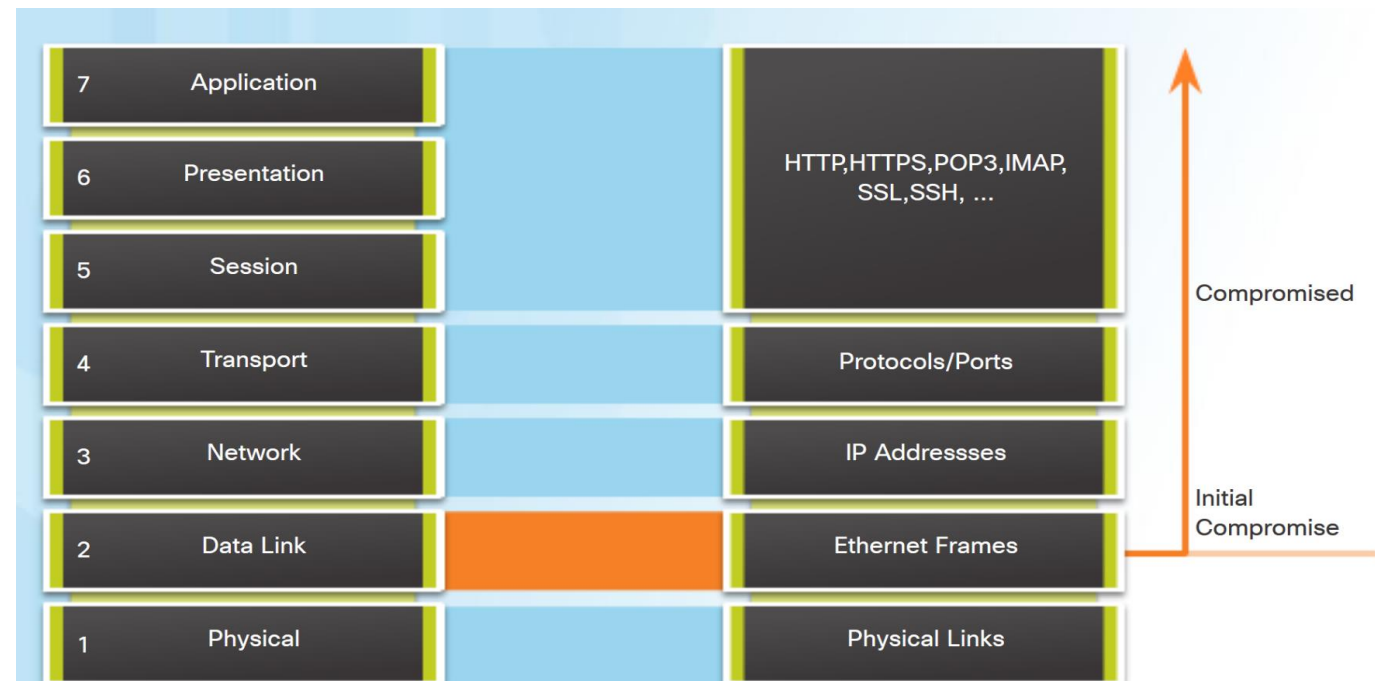
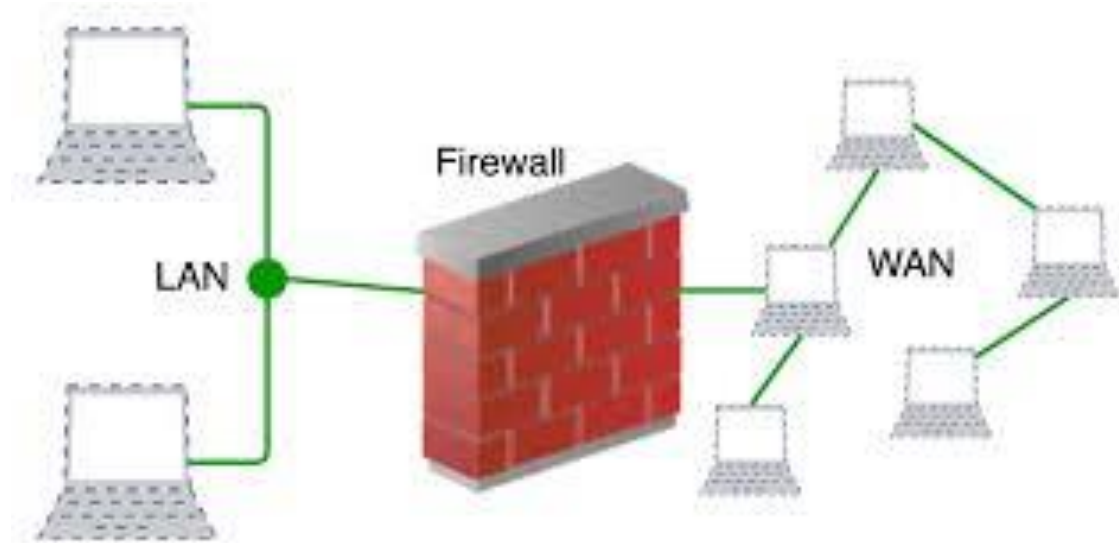
Common LAN Attacks

- Common security solutions using routers, Firewalls, Intrusion Prevention Systems (IPSs), and VPN devices protect Layer 3 up through Layer 7.
- Layer 2 must also be protected.
- **Common Layer 2 attacks include:**
 - MAC Address Table Flooding Attack
 - DHCP Attacks
 - CDP Reconnaissance Attack
 - Telnet Attacks
 - VLAN Attacks

Source :

http://vapenik.s.cnl.sk/pcsiete/CCNA4/05_Network_Security_and_Monitoring.pdf

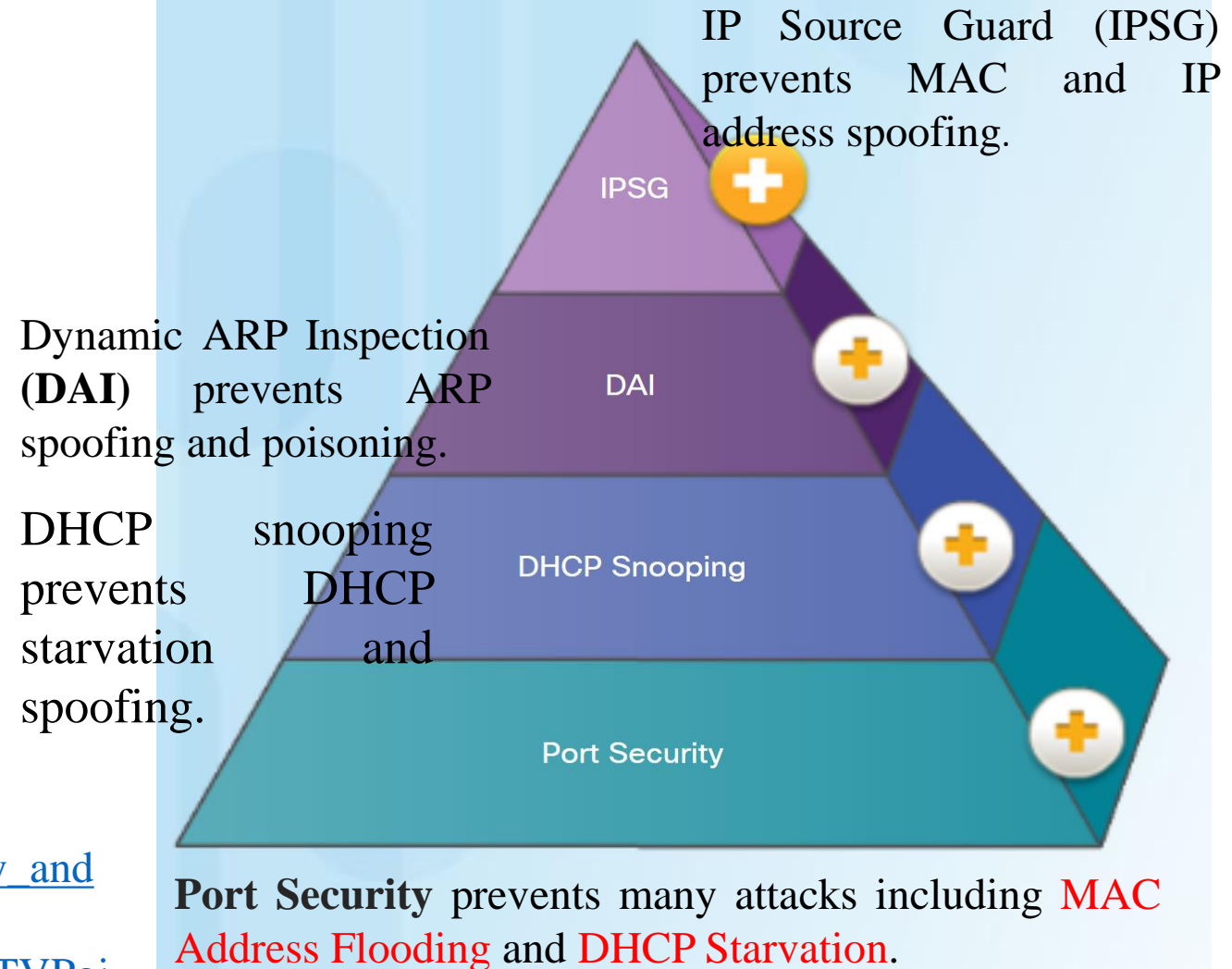
<https://drive.google.com/drive/folders/1aXNR1Zfr44dZcZOTVPoiVaWYOnlgqaZt>



Secure the LAN

Cisco Solutions to Mitigate Layer 2 Attacks

- Strategies to secure Layer 2 of a network:
 - Always use secure variants of protocols such as SSH, SCP, and SSL.
 - Use strong passwords and change often.
 - Enable CDP on select ports only.
 - Use a dedicated management VLAN.
 - Use ACLs to filter unwanted access.



Source :

http://vapenik.s.cnl.sk/pcsiete/CCNA4/05_Network_Security_and_Monitoring.pdf

<https://drive.google.com/drive/folders/1aXNR1Zfr44dZcZOTVPoiVaWYOnlgqaZt>

MAC Address Flooding Attack/ Content Addressable Memory (CAM) Table Flooding Attack

- It is a type of network attack where an attacker connected to a switch port floods the switch interface with very large number of Ethernet frames with different fake source MAC address.
- In a typical MAC flooding Attack, a switch is fed many Ethernet frames, each containing different source MAC addresses, by the attacker. The intention is to consume the limited memory set aside in the switch to store the MAC Address Table.
- After launching a successful MAC flooding attack, a malicious user can use a packet analyzer to capture sensitive data being transmitted between other computers, which would not be accessible were the switch operating normally.

MAC Address Review

48 Bit Hexadecimal (Base16) Unique Layer Two Address

1234.5678.9ABC

First 24 bits = Manufacture Code
Assigned by IEEE

0000.0cXX.XXXX

Second 24 bits = Specific Interface,
Assigned by Manufacture

XXXX.XX00.0001

All F's = Broadcast

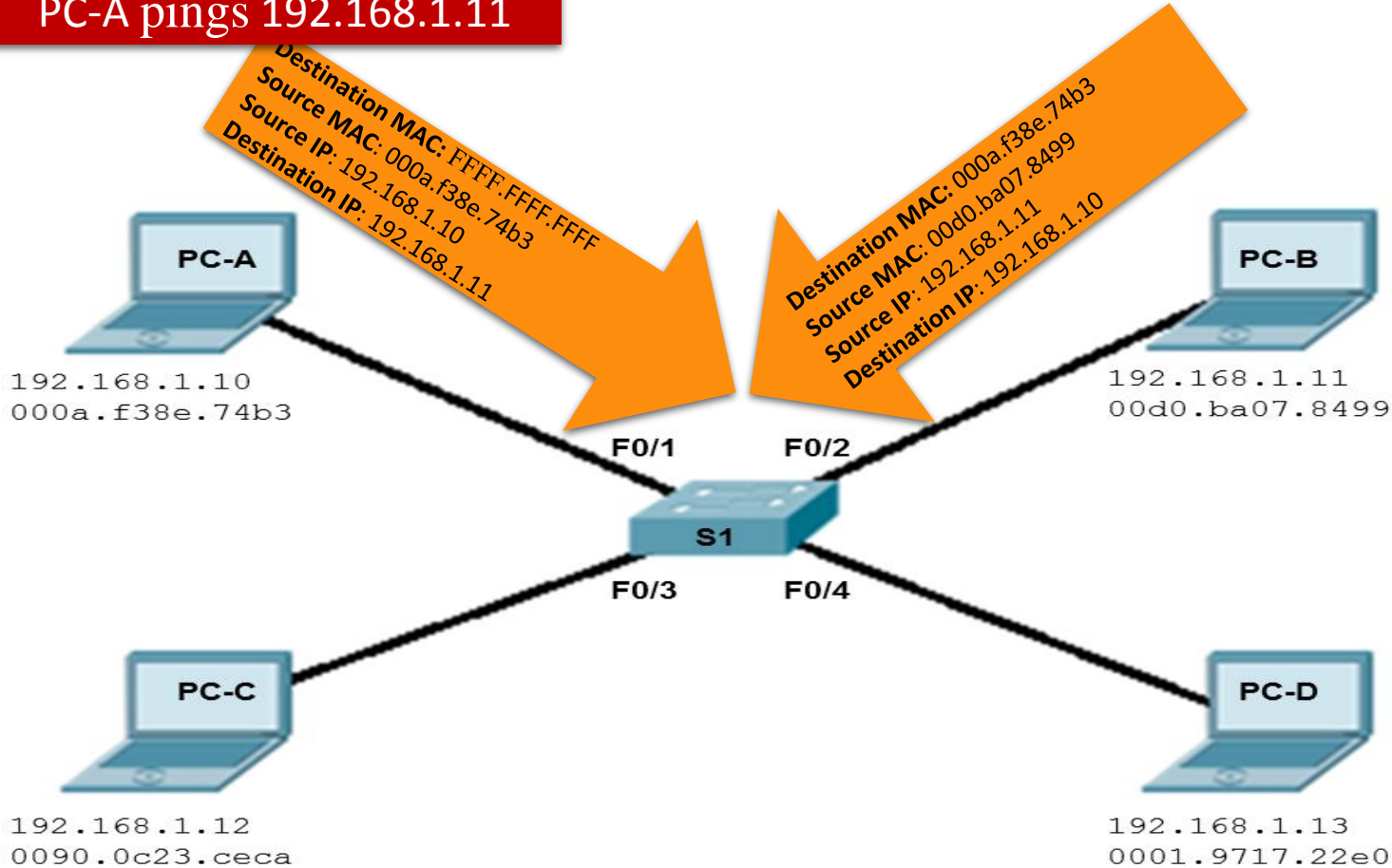
FFFF.FFFF.FFFF

Content Addressable Memory (CAM) Table Review

- The CAM Table stores information such as MAC addresses available on physical ports with their associated VLAN parameters.
- CAM Tables have a fixed size.

CAM Table Operation

PC-A pings 192.168.1.11



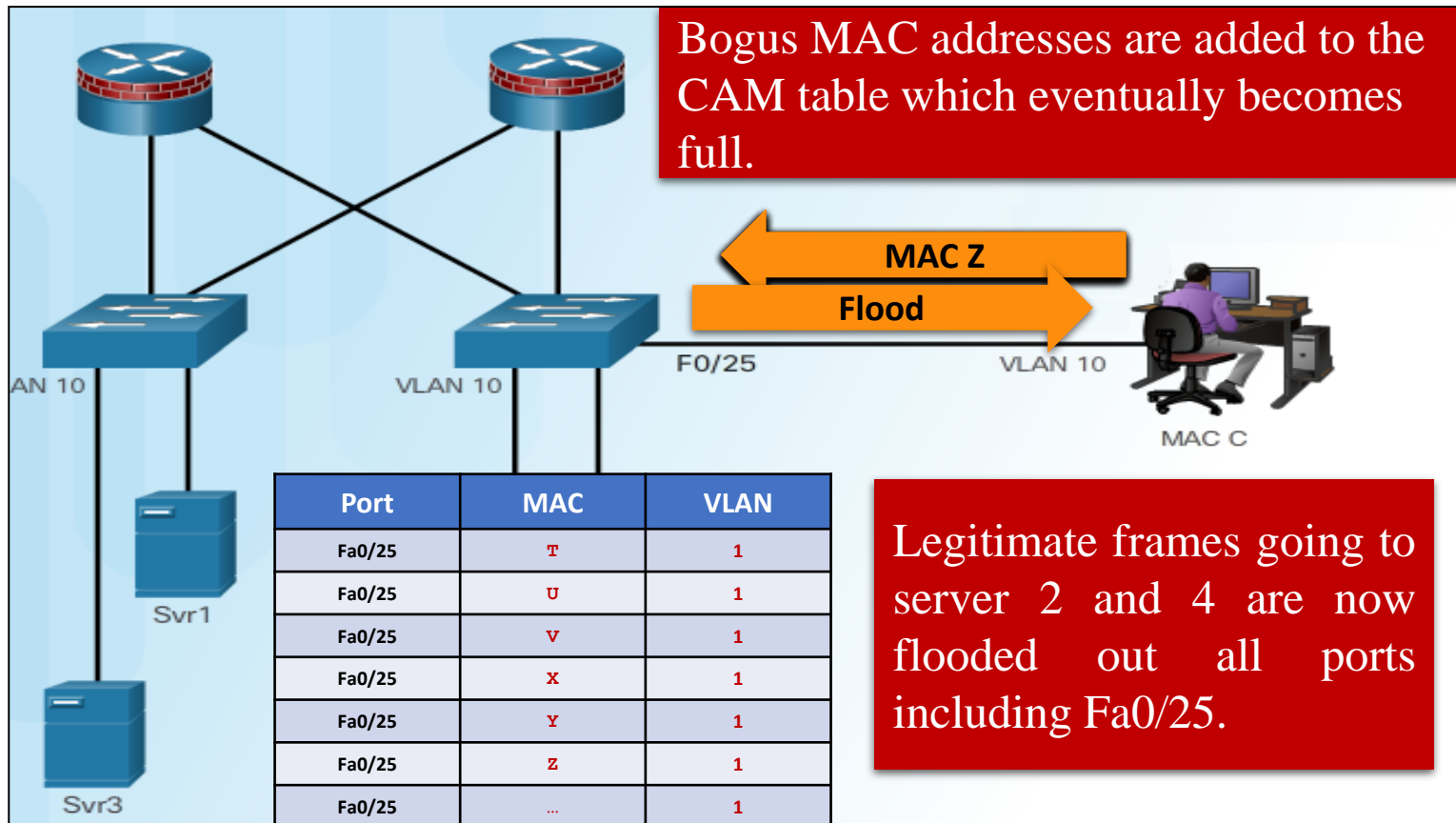
Eventually the CAM Table is complete

Port	MAC	VLAN
Fa0/1	000a.f38e.74b3	1
Fa0/2	00db.ba07.8499	1
Fa0/3	0090.0c23.ceca	1
Fa0/4	0001.9717.22e0	1

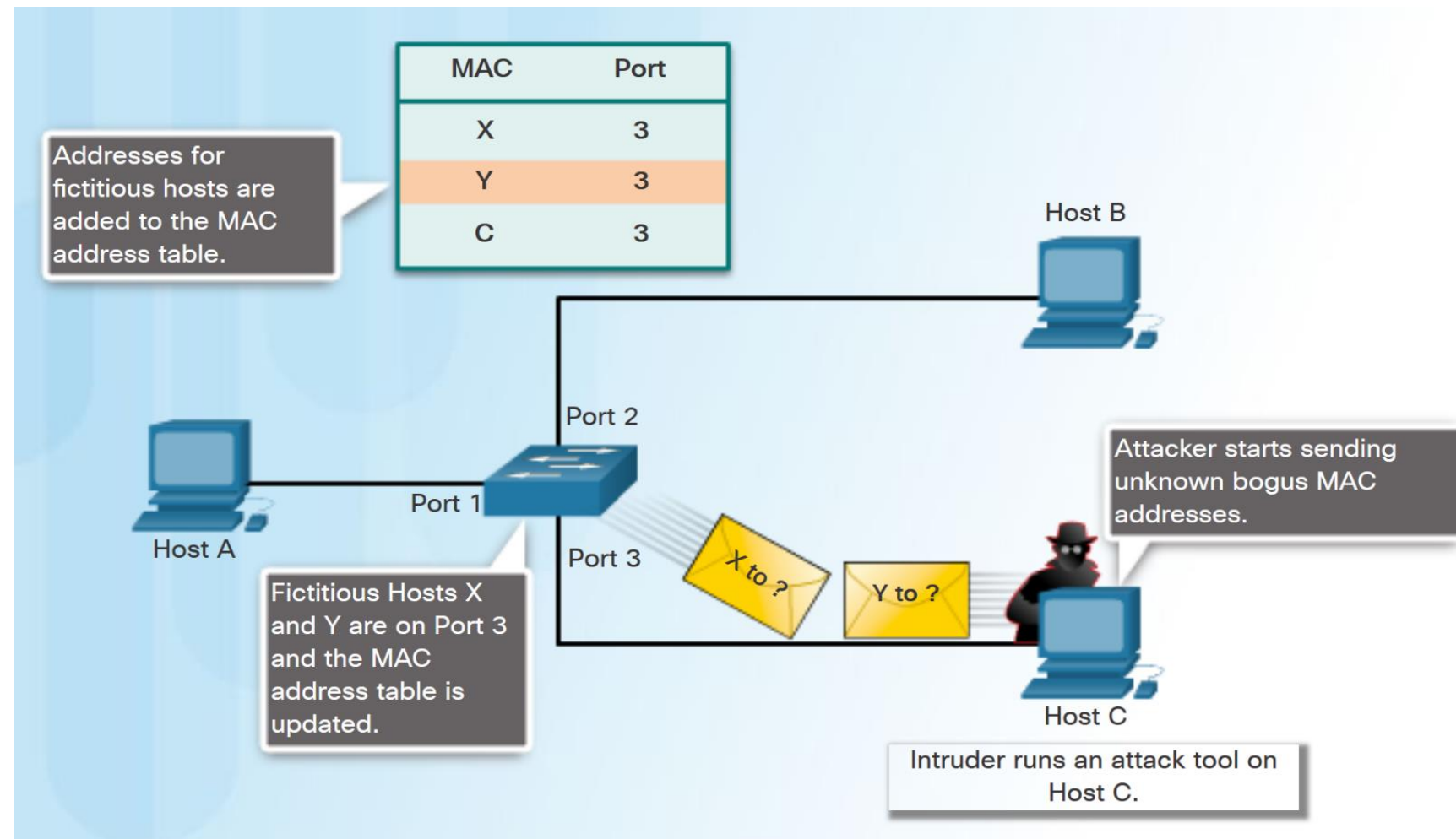
```
S1# show mac-address-table
      Mac Address Table
-----
Vlan  Mac Address      Type      Ports
----  -
1     0001.9717.22e0    DYNAMIC   Fa0/4
1     000a.f38e.74b3    DYNAMIC   Fa0/1
1     0090.0c23.ceca    DYNAMIC   Fa0/3
1     00d0.ba07.8499    DYNAMIC   Fa0/2
S1#
```

CAM Table Attack

Solution: Port Security



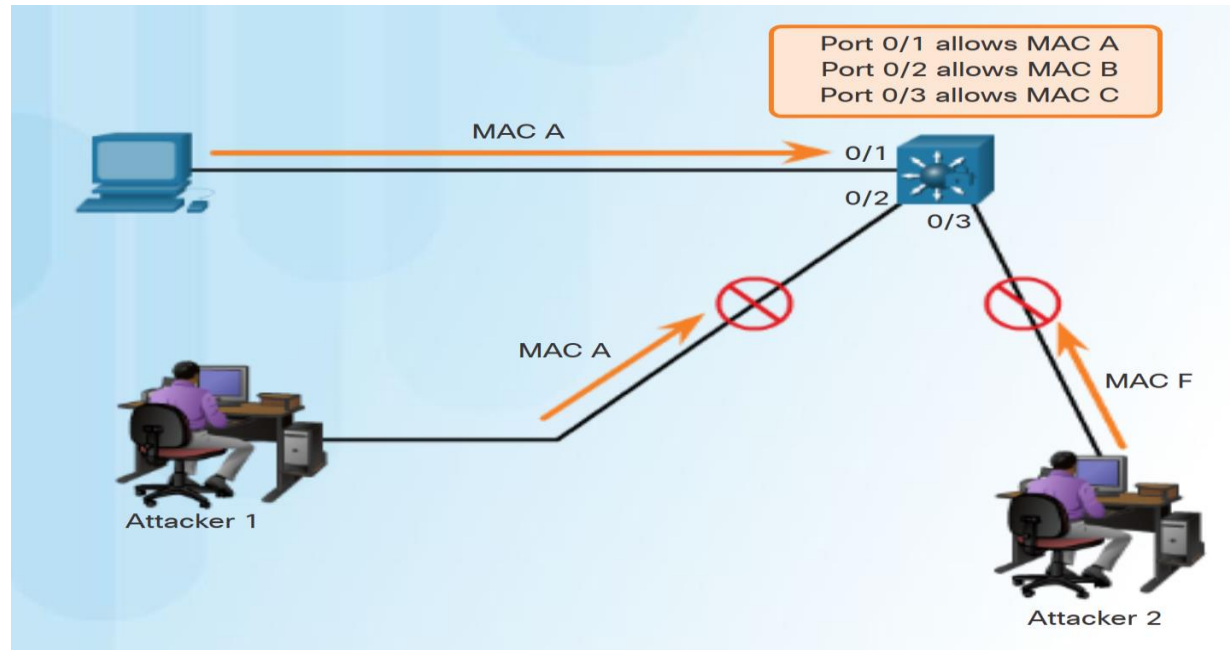
MAC Address Table Flooding Attack



- Common LAN switch attack is the MAC Address Table Flooding attack.
 - An attacker sends fake source MAC addresses until the switch MAC Address Table is full and the switch is overwhelmed.
 - Switch is then in **Fail-Open** mode and broadcasts all frames, allowing the attacker to capture those frames.
- Configure **Port Security** to mitigate these attacks.

Source : http://vapenik.s.cnl.sk/pcsiete/CCNA4/05_Network_Security_and_Monitoring.pdf

Mitigate MAC Address Flooding Table Attacks



- Enable port security to prevent MAC Address Flooding Attacks.
- Port security allows an administrator to do the following:
 - statically specify MAC addresses for a port.
 - permit the switch to dynamically learn a limited number of MAC addresses.
 - when the maximum number of MAC addresses is reached, any additional attempts to connect by unknown MAC addresses will generate a security violation.

Source : http://vapenik.s.cnl.sk/pcsiete/CCNA4/05_Network_Security_and_Monitoring.pdf

**How to launch MAC Address Flooding Attack/
Content Addressable Memory (CAM) Table Flooding Attack ?**

MAC Address Flooding Attack with **macof**

- **Macof sends random source MAC and IP addresses**
- **macof (part of dsniff) — <http://monkey.org/~dugsong/dsniff/>**
- **Syntax: macof [-i interface] [-s src] [-d dst] [-e tha] [-x sport] [-y dport] [-n times]**
 - i interface Specify the interface to send on.
 - s src Specify source IP address.
 - d dst Specify destination IP address.
 - e Specify target hardware address.
 - x sport Specify TCP source port.
 - y dport Specify TCP destination port.
 - n times Specify the number of packets to send.

Example-1 : macof -i eth0 -n 30

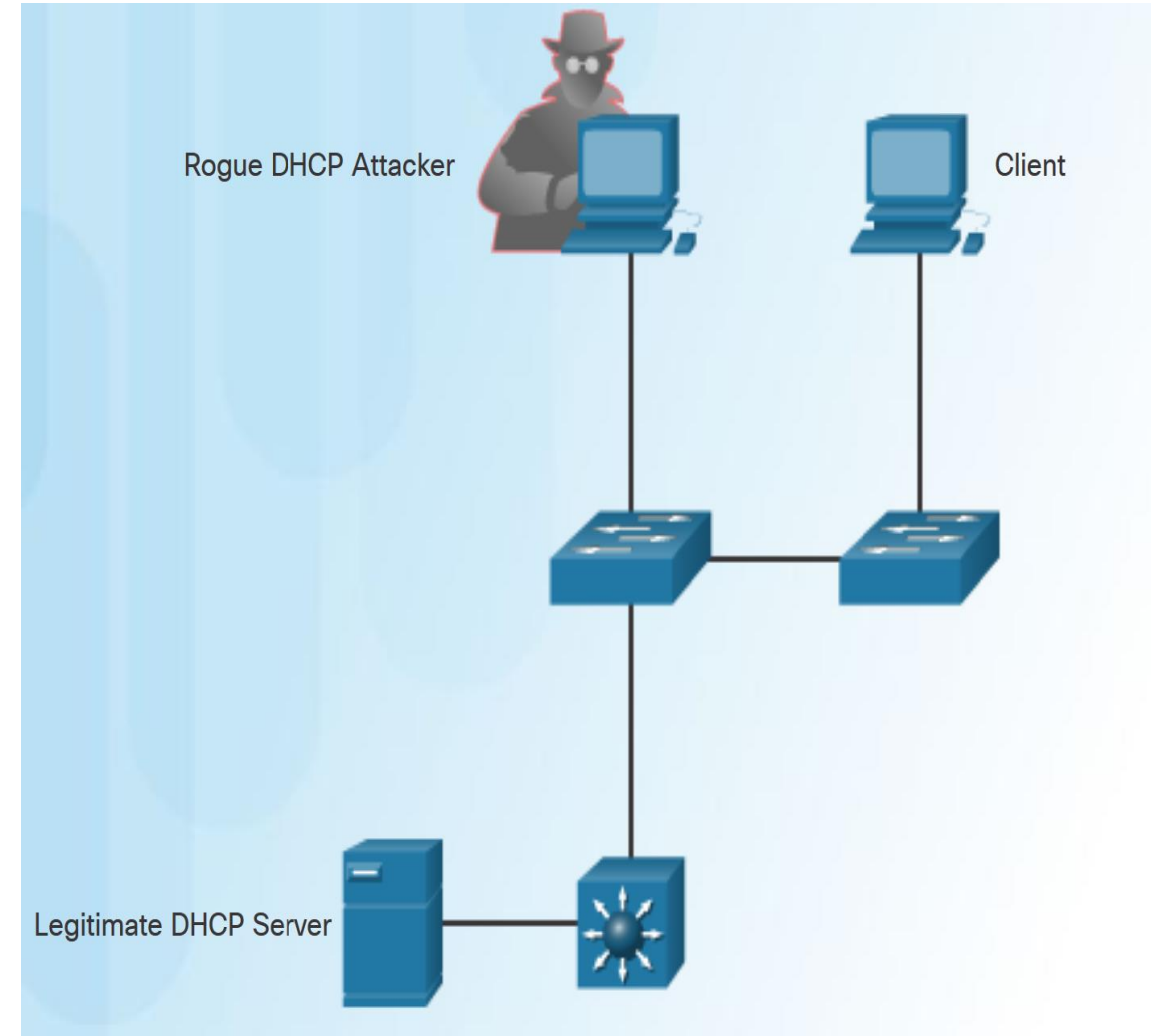
```
Applications ▾ Places ▾ Terminal ▾ Mon 18:18 1
root@kali-Linux-64bit: ~
File Edit View Search Terminal Help
root@kali-Linux-64bit:~# macof -i eth0 -n 30
9:88:18:2b:5a:6 a1:67:92:46:85:c0 0.0.0.0.59252 > 0.0.0.0.24482: S 26059836:26059836(0) win 512
95:48:0:2e:15:57 23:4f:84:1d:a9:e0 0.0.0.0.52316 > 0.0.0.0.48176: S 1173108290:1173108290(0) win 512
e0:aa:f6:16:87:10 8d:fd:dc:5f:7c:fc 0.0.0.0.34018 > 0.0.0.0.9825: S 1721555247:1721555247(0) win 512
53:a6:6d:6b:ed:72 f6:a3:1:5f:f5:3f 0.0.0.0.61953 > 0.0.0.0.6889: S 1020743140:1020743140(0) win 512
d2:6f:3f:58:51:1 1:6d:e0:1:b9:34 0.0.0.0.12133 > 0.0.0.0.11863: S 861410298:861410298(0) win 512
51:45:c9:b:2a:9 74:b9:a6:2:85:ae 0.0.0.0.59208 > 0.0.0.0.2697: S 1243805488:1243805488(0) win 512
5:5d:21:2a:14:d3 70:db:91:3e:1e:a 0.0.0.0.13624 > 0.0.0.0.1292: S 2048814656:2048814656(0) win 512
34:3:a4:19:70:30 ed:dd:57:63:b9:8b 0.0.0.0.38620 > 0.0.0.0.38029: S 1948802415:1948802415(0) win 512
0:34:21:c:b2:22 7b:f4:dc:72:3b:fc 0.0.0.0.5934 > 0.0.0.0.47231: S 1832454735:1832454735(0) win 512
e0:0:b4:5e:ae:7e 2c:62:69:49:96:f9 0.0.0.0.50956 > 0.0.0.0.48645: S 818778846:818778846(0) win 512
52:a9:a6:54:83:e0 8a:f4:51:6b:3d:bf 0.0.0.0.57981 > 0.0.0.0.33562: S 2057232116:2057232116(0) win 512
8e:5d:ba:3:b4:19 96:c6:30:10:a1:c8 0.0.0.0.46495 > 0.0.0.0.11550: S 765473502:765473502(0) win 512
89:92:16:73:13:40 db:15:fc:15:35:31 0.0.0.0.28629 > 0.0.0.0.183: S 312467466:312467466(0) win 512
bf:ce:63:61:a2:f0 4b:2b:b9:68:0:10 0.0.0.0.21765 > 0.0.0.0.4703: S 702241153:702241153(0) win 512
d9:fa:9a:4b:a5:e4 c5:46:88:1:3b:1d 0.0.0.0.50489 > 0.0.0.0.58086: S 1984828686:1984828686(0) win 512
d8:5b:37:34:fc:10 43:d4:88:11:e6:bb 0.0.0.0.61578 > 0.0.0.0.45573: S 59939994:59939994(0) win 512
e0:33:a6:31:50:d0 44:59:93:7a:8b:79 0.0.0.0.63949 > 0.0.0.0.46421: S 1429487843:1429487843(0) win 512
50:b7:9d:2c:8b:5c 51:a1:7f:40:3b:2c 0.0.0.0.35449 > 0.0.0.0.48896: S 440555452:440555452(0) win 512
55:b:64:59:e:2 e8:1:e9:24:85:4a 0.0.0.0.59898 > 0.0.0.0.11903: S 1579957468:1579957468(0) win 512
d:e5:a6:2c:8e:80 e0:cb:98:e:8c:65 0.0.0.0.59716 > 0.0.0.0.29672: S 1914338820:1914338820(0) win 512
e9:4a:2a:26:c:54 d2:24:16:37:e4:52 0.0.0.0.57851 > 0.0.0.0.35521: S 132156624:132156624(0) win 512
fe:d2:98:4d:69:f9 f6:a1:12:34:68:47 0.0.0.0.45161 > 0.0.0.0.44522: S 1712970851:1712970851(0) win 512
2f:9c:e3:1b:30:d4 b3:20:4e:2b:8b:92 0.0.0.0.52564 > 0.0.0.0.8963: S 1757434179:1757434179(0) win 512
b:91:54:11:16:ab ec:15:94:7b:47:fe 0.0.0.0.21496 > 0.0.0.0.24566: S 1518780931:1518780931(0) win 512
6d:d:84:26:20:bd d1:fc:40:65:fa:9 0.0.0.0.40438 > 0.0.0.0.13554: S 598978617:598978617(0) win 512
f8:8c:6c:73:ff:8b 74:14:31:20:65:cc 0.0.0.0.4737 > 0.0.0.0.27616: S 1429847083:1429847083(0) win 512
a3:f7:b0:31:c4:b3 b6:8b:e5:6b:d4:3a 0.0.0.0.52380 > 0.0.0.0.1541: S 577057576:577057576(0) win 512
9c:3f:11:2f:7e:89 e9:ad:5d:78:bf:50 0.0.0.0.63169 > 0.0.0.0.45423: S 1794110673:1794110673(0) win 512
9c:b9:46:58:25:e0 9e:ad:f:29:88:46 0.0.0.0.13547 > 0.0.0.0.16141: S 1744337186:1744337186(0) win 512
45:bd:4c:4e:6e:8a a9:eb:6b:e:2d:83 0.0.0.0.30916 > 0.0.0.0.4575: S 1752811949:1752811949(0) win 512
root@kali-Linux-64bit:~#
```


Example-2 : macof -i etho -n 30 -d 10.100.55.215

```
Applications ▾ Places ▾ Terminal ▾ Mon 18:26 1
root@kali-Linux-64bit: ~
File Edit View Search Terminal Help
root@kali-Linux-64bit:~# macof -i eth0 -n 30 -d 10.100.55.215
59:2d:35:7:f0:d6 51:f:e0:6c:a6:44 0.0.0.0.64221 > 10.100.55.215.49032: S 1206942238:1206942238(0) win 512
1:b2:e8:52:22:59 c7:2a:46:4:e8:20 0.0.0.0.61781 > 10.100.55.215.28628: S 1729584582:1729584582(0) win 512
3:38:23:65:46:13 9a:7f:4b:15:65:56 0.0.0.0.8447 > 10.100.55.215.5510: S 1451921892:1451921892(0) win 512
3e:4f:44:35:86:f1 71:f8:e9:38:76:9f 0.0.0.0.34891 > 10.100.55.215.7080: S 1367677239:1367677239(0) win 512
e0:88:a5:d:44:aa f5:a7:a9:32:b:96 0.0.0.0.13250 > 10.100.55.215.50456: S 1065881743:1065881743(0) win 512
9d:f5:d0:40:eb:bf df:6:50:7b:c4:bf 0.0.0.0.5493 > 10.100.55.215.21674: S 2023144160:2023144160(0) win 512
58:b6:50:3f:fc:c8 87:d5:10:2a:64:c6 0.0.0.0.61727 > 10.100.55.215.63423: S 319379949:319379949(0) win 512
ad:e7:5d:18:9e:8 ed:da:4:27:9c:18 0.0.0.0.44086 > 10.100.55.215.62266: S 1489296490:1489296490(0) win 512
b9:a6:43:0:47:7a c3:bb:ba:6f:4e:64 0.0.0.0.27497 > 10.100.55.215.26237: S 498651842:498651842(0) win 512
9b:38:58:43:25:45 db:73:17:8:1c:93 0.0.0.0.17648 > 10.100.55.215.37556: S 1852379850:1852379850(0) win 512
b7:6:1d:7d:f2:f8 22:fe:43:1:a:1b 0.0.0.0.2052 > 10.100.55.215.7420: S 81759418:81759418(0) win 512
6a:d:c9:3b:d5:84 2b:6a:2c:72:99:24 0.0.0.0.54942 > 10.100.55.215.53270: S 1331708097:1331708097(0) win 512
be:92:c2:28:9e:f6 43:e1:8c:16:fc:83 0.0.0.0.48373 > 10.100.55.215.65518: S 962808907:962808907(0) win 512
fd:a3:e1:20:64:18 af:5a:48:1e:4e:57 0.0.0.0.61929 > 10.100.55.215.22196: S 1242328374:1242328374(0) win 512
d5:47:e3:16:3e:54 27:ee:5a:e:e1:5 0.0.0.0.33111 > 10.100.55.215.25144: S 1802688152:1802688152(0) win 512
48:1:8f:37:21:92 b:6a:3f:53:2d:40 0.0.0.0.13290 > 10.100.55.215.14333: S 674179439:674179439(0) win 512
75:aa:7d:4a:8e:51 d7:1d:54:e:b7:6c 0.0.0.0.50318 > 10.100.55.215.26030: S 411555124:411555124(0) win 512
40:37:58:20:70:44 e6:cd:22:4a:80:c2 0.0.0.0.60487 > 10.100.55.215.48898: S 1880504564:1880504564(0) win 512
30:bf:29:1:42:8b 9:d3:ba:78:82:ed 0.0.0.0.24038 > 10.100.55.215.43726: S 2055178695:2055178695(0) win 512
4:54:b4:a:44:bc 28:25:ff:57:34:85 0.0.0.0.20149 > 10.100.55.215.45407: S 105519013:105519013(0) win 512
4e:ff:9f:76:9d:83 61:70:7c:62:b5:d6 0.0.0.0.38734 > 10.100.55.215.28350: S 1763390620:1763390620(0) win 512
5c:c:aa:4e:b9:dc 3c:28:46:3b:c0:64 0.0.0.0.61124 > 10.100.55.215.12420: S 662463258:662463258(0) win 512
d9:f9:90:14:65:35 b6:a4:6f:12:f3:39 0.0.0.0.29546 > 10.100.55.215.14106: S 1780363060:1780363060(0) win 512
e6:28:e9:5c:b1:ca 7a:5c:16:66:f0:ea 0.0.0.0.50734 > 10.100.55.215.15823: S 1164825064:1164825064(0) win 512
5f:c0:be:14:14:6 b4:91:68:2d:96:f 0.0.0.0.39894 > 10.100.55.215.62231: S 820188408:820188408(0) win 512
d4:78:8:69:5e:f6 de:2a:a2:18:ba:94 0.0.0.0.63717 > 10.100.55.215.19424: S 1585569851:1585569851(0) win 512
3:58:47:67:d7:75 57:19:fe:c:ec:e3 0.0.0.0.61703 > 10.100.55.215.9853: S 2124998638:2124998638(0) win 512
7c:ba:2f:32:66:24 c3:cf:3a:79:11:8e 0.0.0.0.20242 > 10.100.55.215.52525: S 2091945065:2091945065(0) win 512
6c:f6:97:72:31:7c b2:f0:55:5:ee:21 0.0.0.0.60519 > 10.100.55.215.25967: S 31879395:31879395(0) win 512
8e:c9:c6:14:a9:be 66:ac:88:3:57:eb 0.0.0.0.9670 > 10.100.55.215.4526: S 1135189560:1135189560(0) win 512
root@kali-Linux-64bit:~#
```


DHCP Attacks

- **DHCP Spoofing Attack** - An attacker configures a fake DHCP server on the network to issue IP addresses to clients.
- **DHCP Starvation Attack** - An attacker floods the DHCP server with bogus DHCP requests and leases all of the available IP addresses. This results in a Denial of Service (DoS) attack as new clients cannot obtain an IP address.
- Methods to mitigate DHCP attacks:
 - Configure DHCP snooping
 - Configure port security

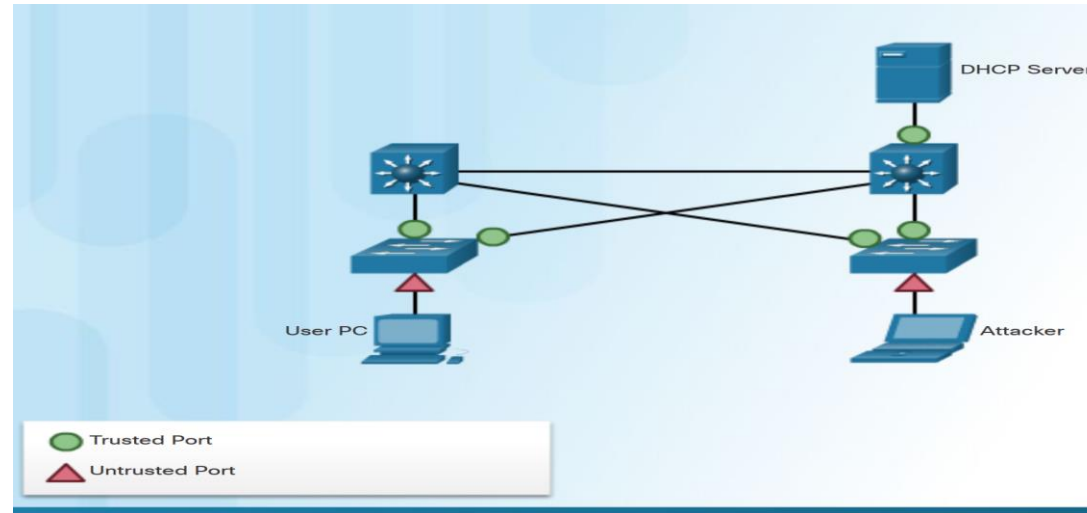


Source:

<https://drive.google.com/drive/folders/1aXNR1Zfr44dZcZOTVPoiVaWYOnlgqaZt>

http://vapenik.s.cnl.sk/pcsiete/CCNA4/05_Network_Security_and_Monitoring.pdf

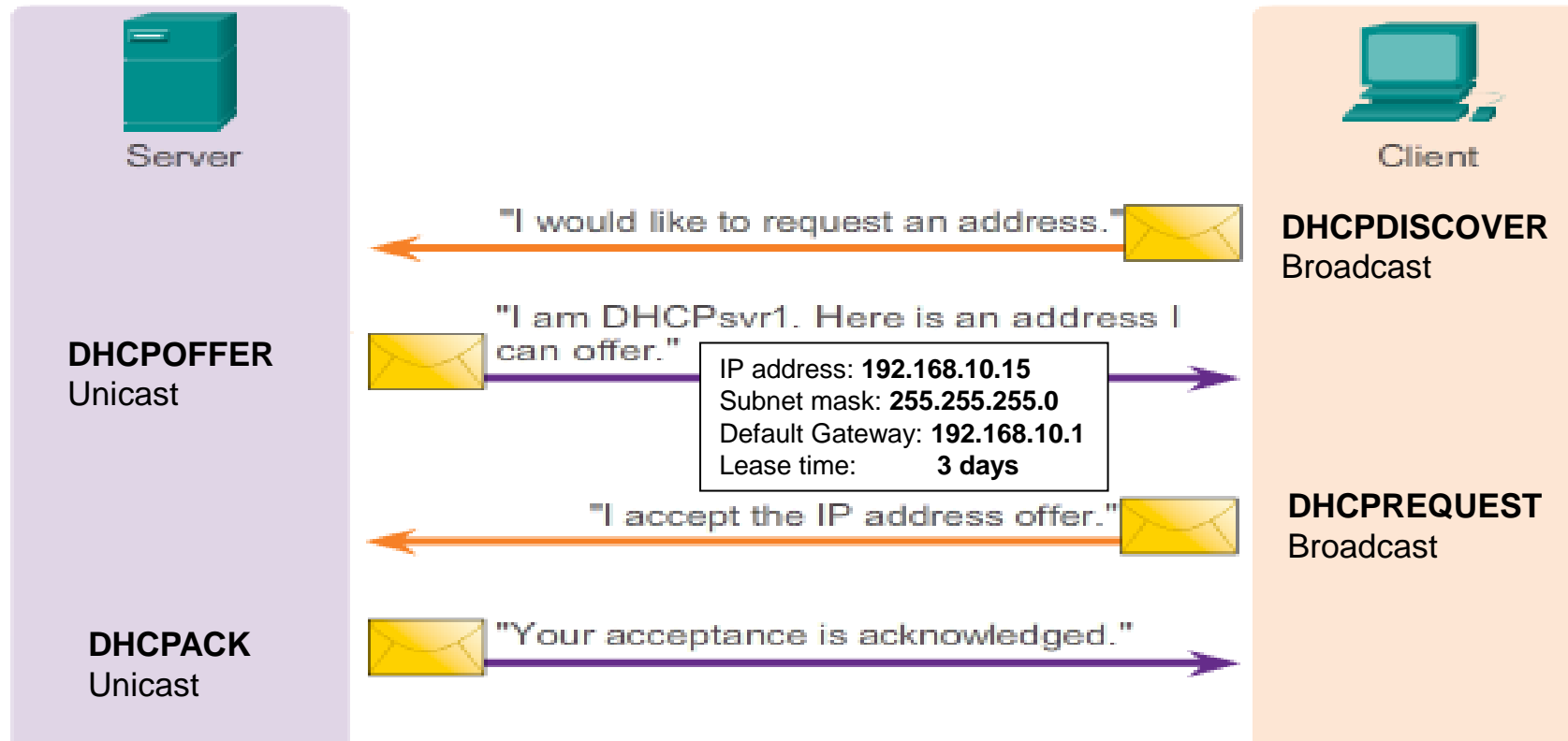
Mitigate DHCP Attacks



- To prevent DHCP attacks use DHCP snooping.
- With DHCP snooping enabled on an interface, the switch will deny packets containing:
 - Unauthorized DHCP server messages coming from an untrusted port.
 - Unauthorized DHCP client messages not adhering to the DHCP Snooping Binding Database or rate limits.
- DHCP snooping recognizes two types of ports:
 - **Trusted DHCP ports** - Only ports connecting to upstream DHCP servers should be trusted.
 - **Untrusted ports** - These ports connect to hosts that should not be providing DHCP server messages.

Source: http://vapenik.s.cnl.sk/pcsiete/CCNA4/05_Network_Security_and_Monitoring.pdf

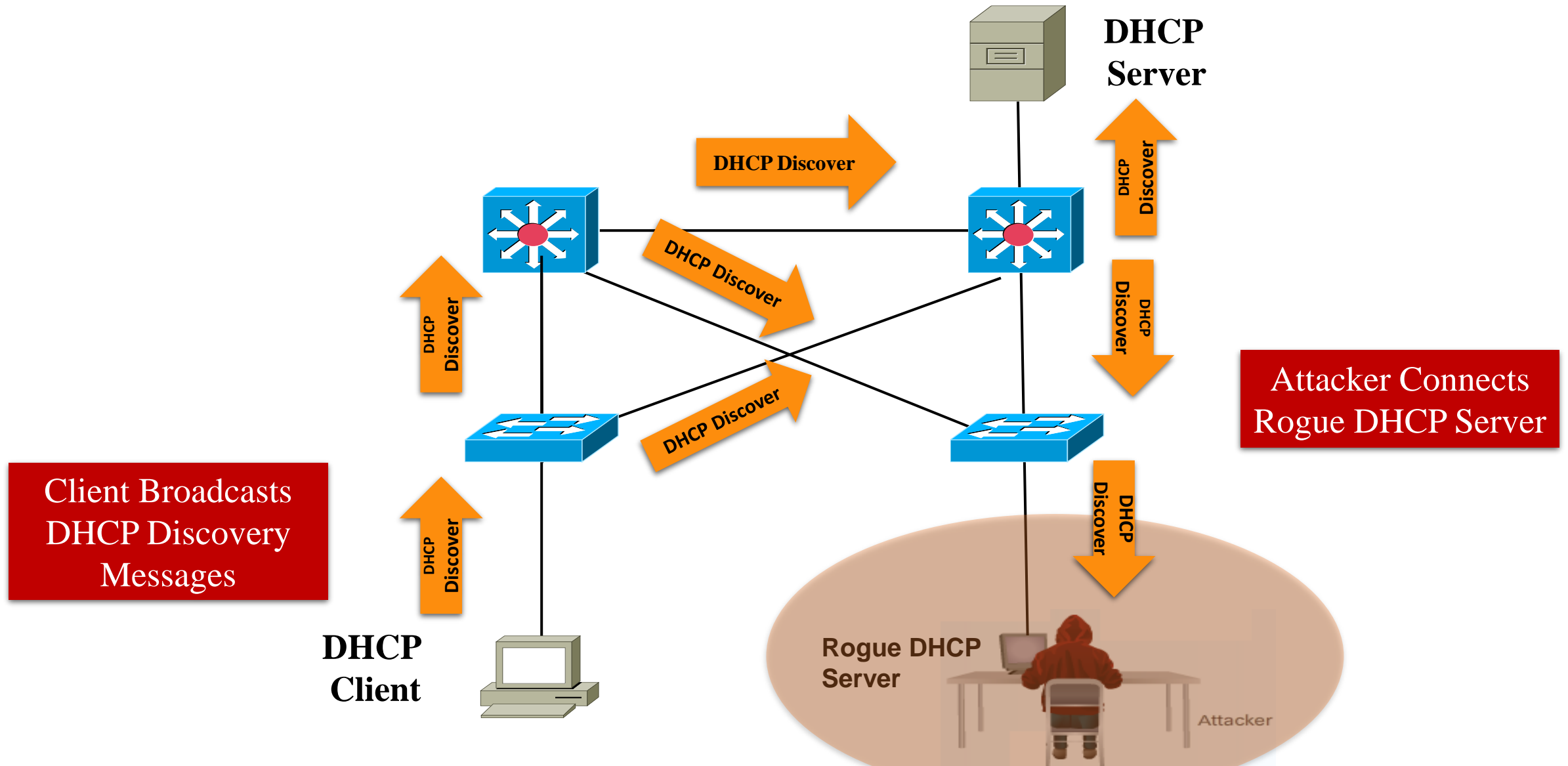
DHCP is a Network Protocol used to Automatically assign IP Information



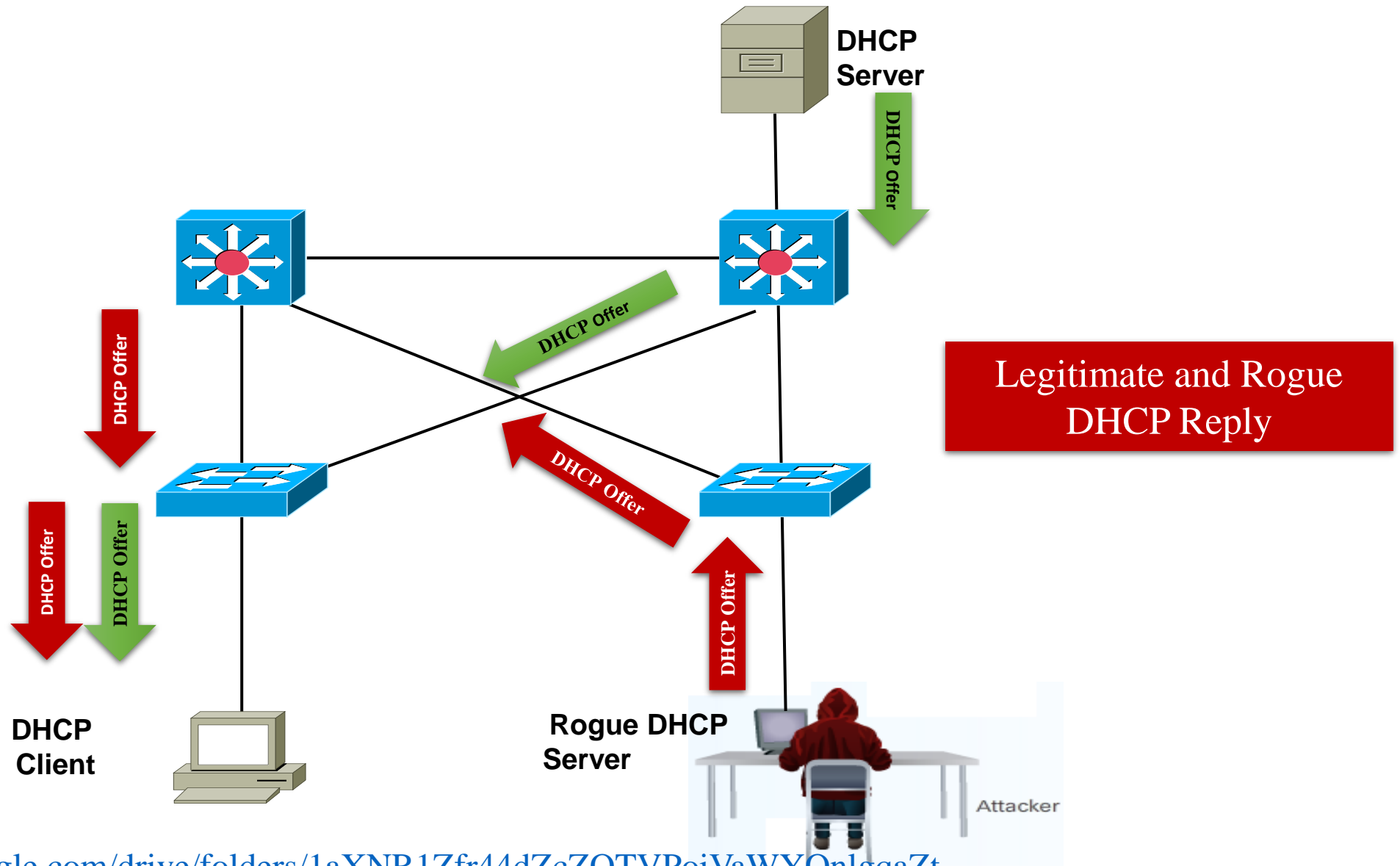
Two types of DHCP attacks are:

- **DHCP spoofing:** A fake DHCP server is placed in the network to issue DHCP addresses to clients.
- **DHCP starvation:** Attack denies service to the legitimate DHCP server.

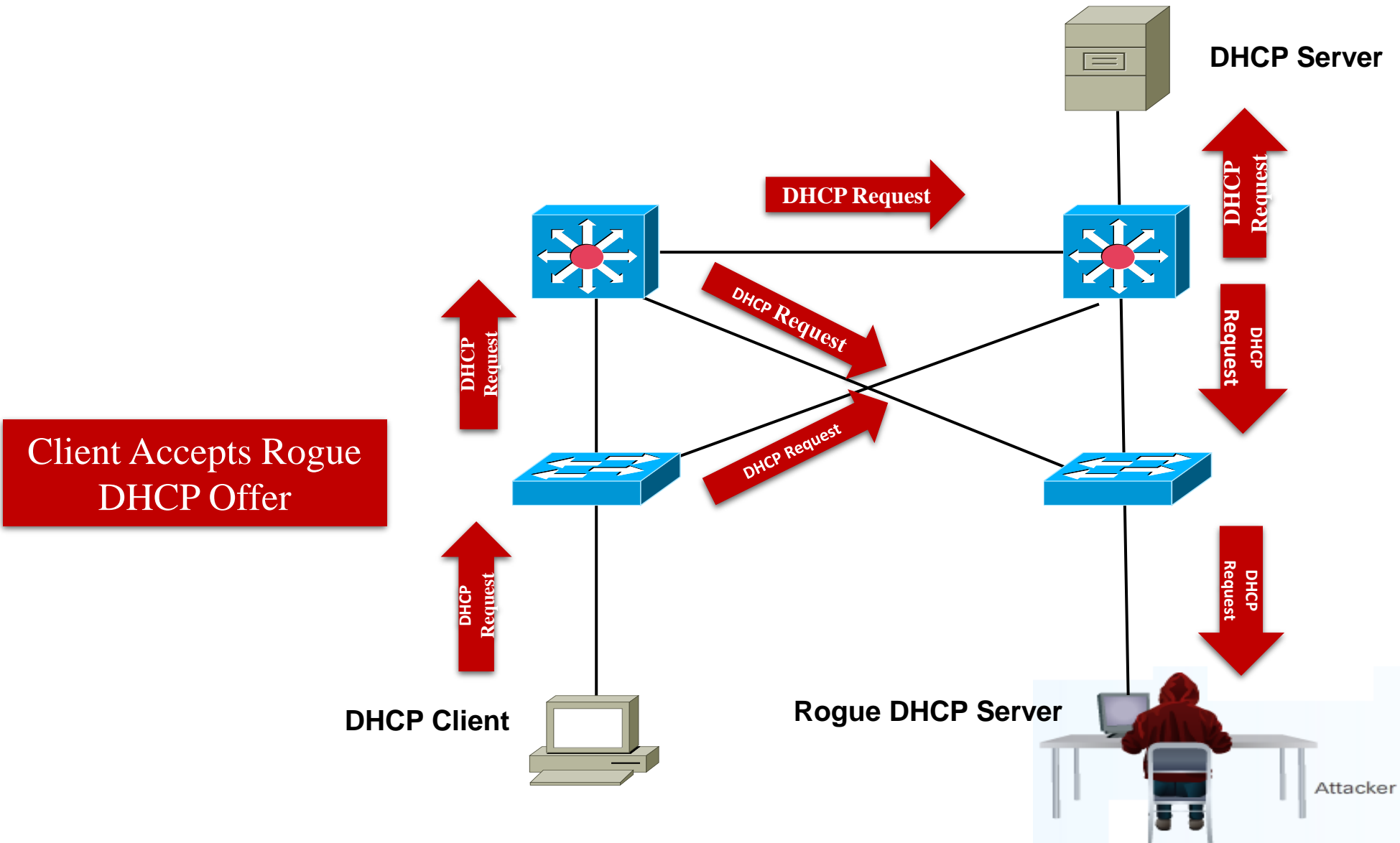
DHCP Spoofing Attack



DHCP Spoofing Attack Contd.

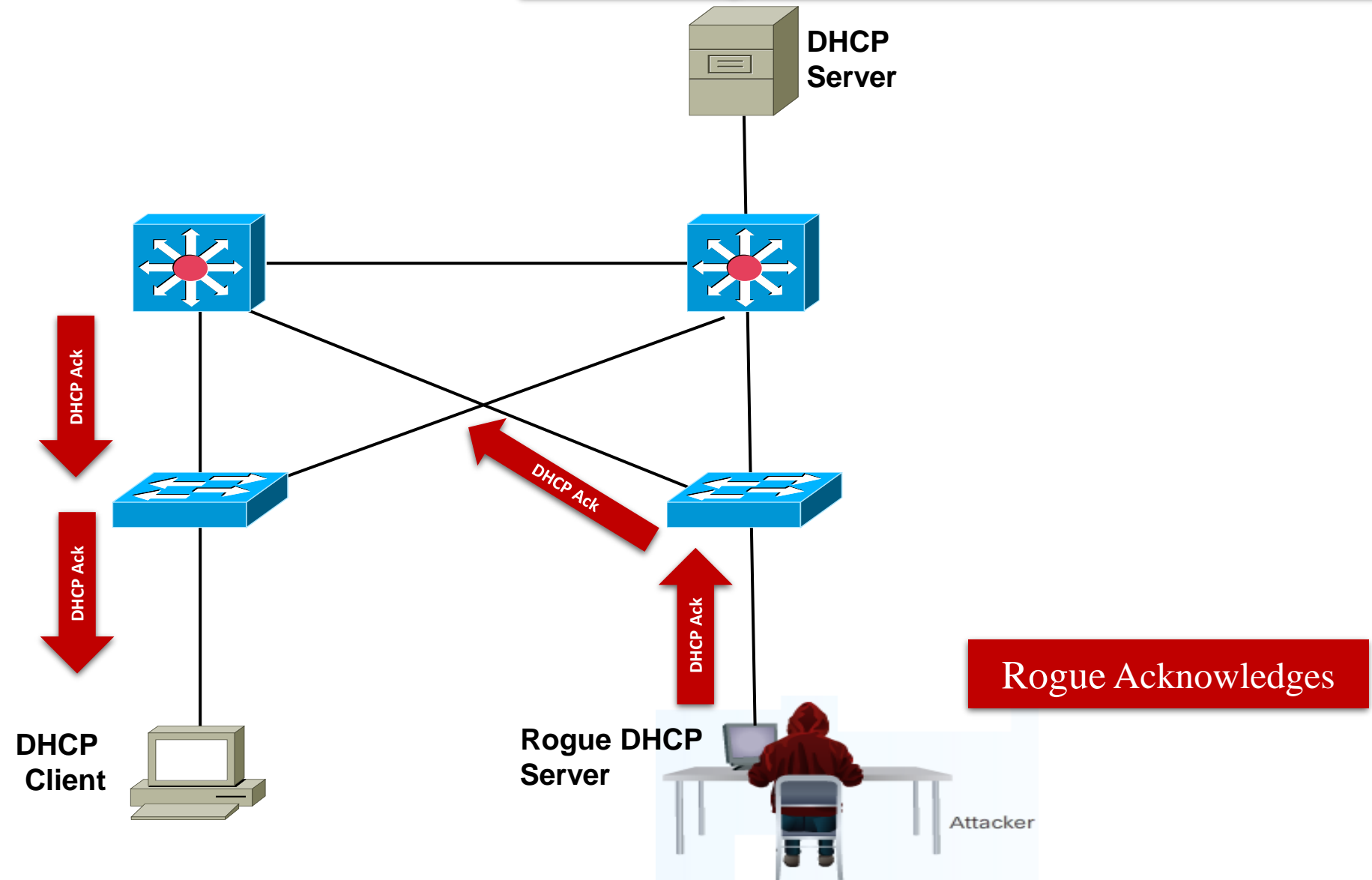


DHCP Spoofing Attack Contd.

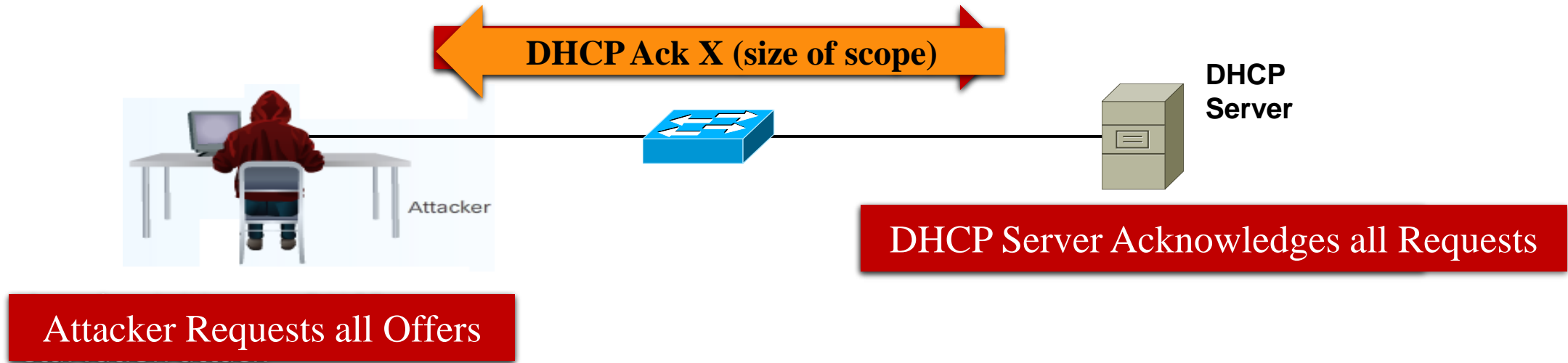


DHCP Spoofing Attack Contd.

• This creates a “man-in-the-middle” attack and can go entirely undetected as the intruder intercepts the data flow through the network.



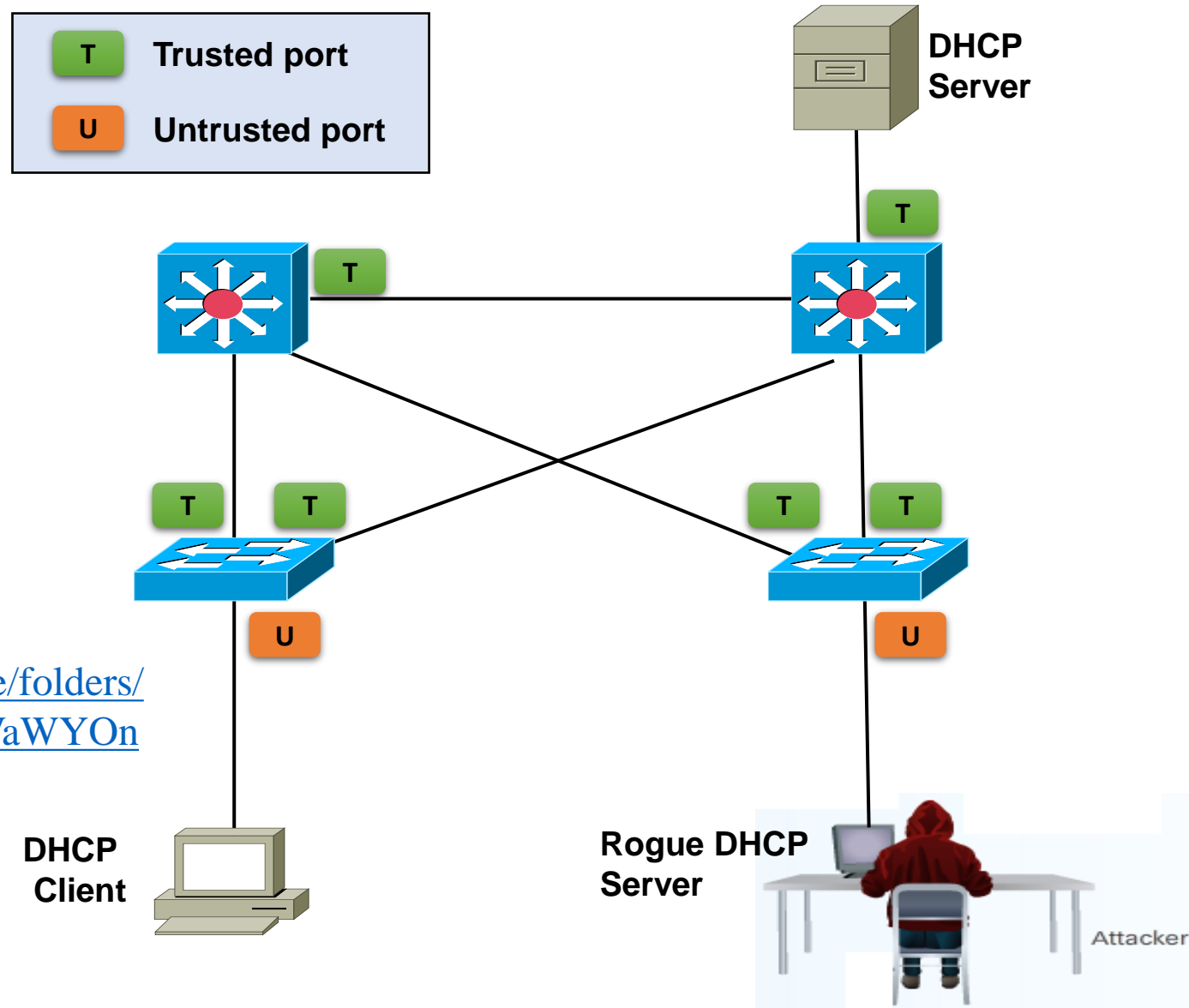
DHCP Starvation Attack



Solution: Configure DHCP Snooping

- DHCP snooping is a Cisco Catalyst feature that determines which switch ports can respond to DHCP requests.
- Ports are identified as:
 - **Trusted ports:** Host a DHCP server or can be an uplink toward the DHCP server and can source all DHCP messages, including DHCP offer and DHCP acknowledgement packets
 - **Untrusted ports:** Can source requests only.
- If a rogue device on an untrusted port attempts to send a DHCP offer packet into the network, the port is shut down.

Solution: Configure DHCP Snooping Contd.



Source:

<https://drive.google.com/drive/folders/1aXNR1Zfr44dZcZOTVPoiVaWYOnlgqaZt>

Switched Port Analyzer (SPAN and RSPAN)

- Network traffic passing through ports or VLANs can be analyzed by using **Switched Port Analyzer (SPAN)** or **Remote SPAN (RSPAN)**.
 - SPAN can send a copy of traffic from one port to another port on the same switch where a network analyzer or monitoring device is connected.
 - RSPAN can send a copy of traffic to a port on a different switch.
- SPAN is commonly deployed when an Intrusion Detection System(IDS)/Intrusion Prevention System (IPS)is added to a network.
 - IPS devices need to read all packets in one or more VLANs, and SPAN can be used to get the packets to the IPS devices.

SPAN Terminology

Source (SPAN) Port

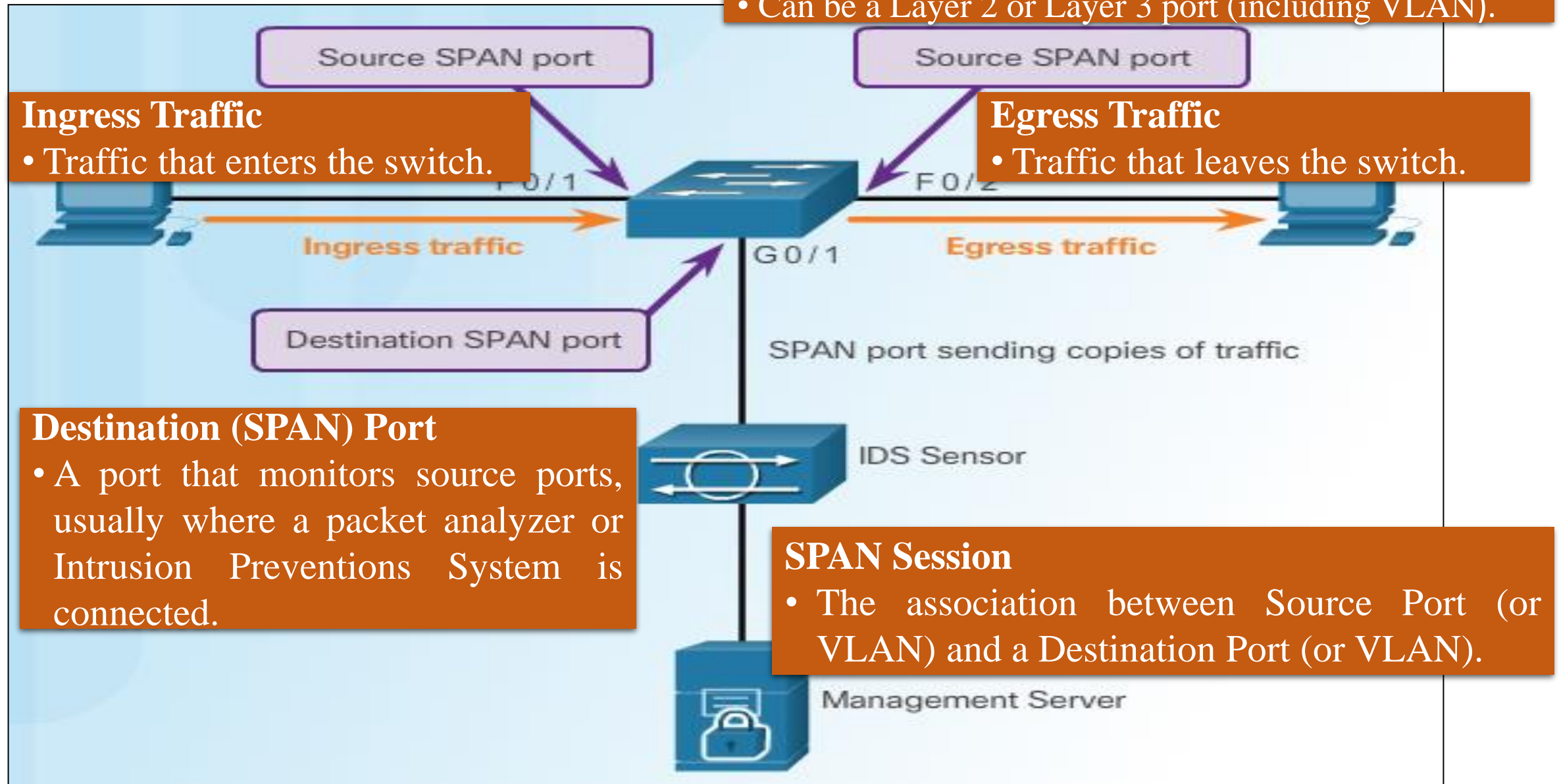
- A port that is monitored with use of the SPAN feature.
- Can be a Layer 2 or Layer 3 port (including VLAN).

Ingress Traffic

- Traffic that enters the switch.

Egress Traffic

- Traffic that leaves the switch.



Destination (SPAN) Port

- A port that monitors source ports, usually where a packet analyzer or Intrusion Prevention System is connected.

SPAN Session

- The association between Source Port (or VLAN) and a Destination Port (or VLAN).

Remote Switched Port Analyzer (RSPAN)

- RSPAN can copy traffic from ports or VLANs on one switch (i.e., source switch) to a port on a different switch (i.e., destination switch).
- A VLAN must be designated as the RSPAN VLAN and not be used for any other purposes.

Note:

- SPAN and RSPAN vary by switching platforms.

What is Scanning?

- Method to gather information regarding the devices running on the network
 - Typically to discover services or servers on a network
 - Which hosts are up?
 - Which services are offering?
- Do not confuse with “host vulnerability scanner” which further explore a computer by testing for common vulnerabilities (nessus, SAINT)

Why Scanning?

- Network Security assessment
- Evaluation and Auditing the security
 - Firewall Penetration Test (Policy Auditing)
 - Intrusion Detection System Proof/Evaluation
 - Identifying Unexpected New Servers
- Identifying open ports for proactively protect the network (Network and security admin)
- Identifying open ports for Attacking it (Hackers).

Nmap

- A well known and free security scanner written by Fyodor (<http://insecure.org/nmap/>)
 - First released Sept 1, 1997 in Phrack 51 “The Art of Port Scanning” (<http://www.phrack.org/issues.html?issue=51>)
 - Many updates since then:
 - **OS Detection** (<http://www.phrack.org/issues.html?issue=54&id=9#article>)
 - **Version scanning**
 - **ARP Scanning**
- **Usage** : nmap [scan types] [options] <host or net ...>

Why Nmap?

- An Excellent Tool
 - Long history of development and support
 - Continuous development and improvements
 - “Industry Standard” port scanner

Nmap Features

- **Host Discovery:** Which host is alive?
 - Identifying computers on a network, for example listing the computers which respond to pings (Ping Sweeps)
- **Port Scanning :** What services are available?
 - Enumerating the open ports on one or more target computers
- **Service and Version Detection :** Which version is running?
 - Determine the application name and version number
- **Operating System:** What platforms are served?
 - Remotely determining the OS and some hardware characteristics of network devices

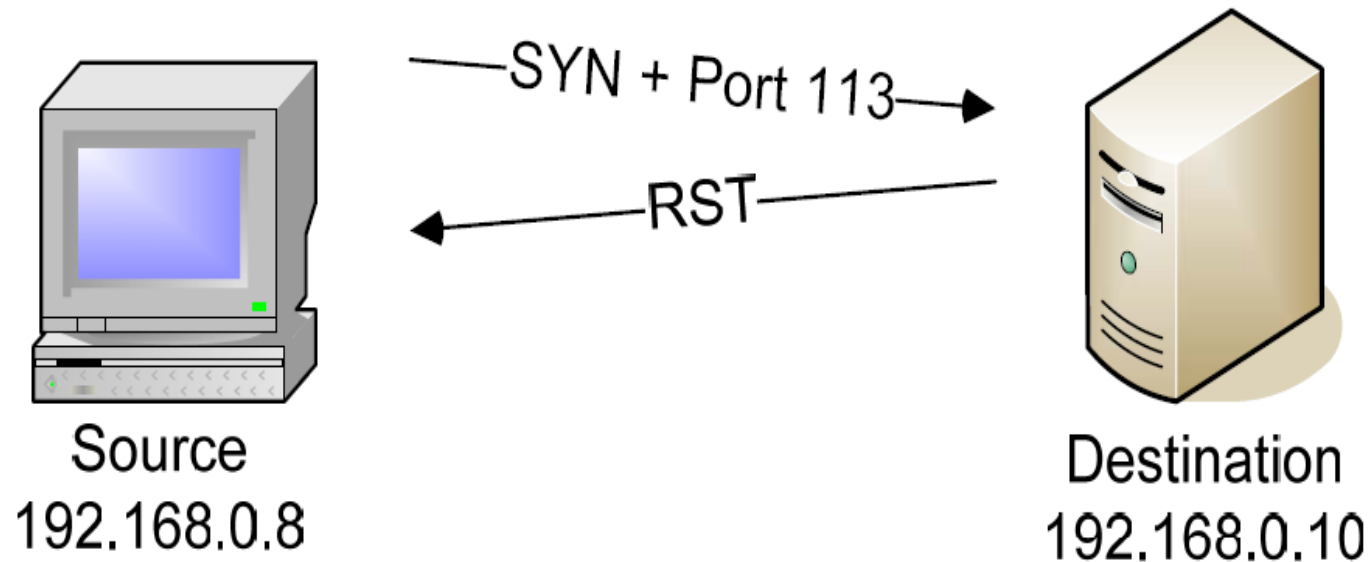
Nmap Scan Types

Nmap Scan	Command Syntax	Requires Privileged Access	Identifies TCP Ports	Identifies UDP Ports
TCP SYN Scan	-sS	YES	YES	NO
TCP connect() Scan	-sT	NO	YES	NO
FIN Scan	-sF	YES	YES	NO
Xmas Tree Scan	-sX	YES	YES	NO
Null Scan	-sN	YES	YES	NO
Ping Scan	-sP	NO	NO	NO
Version Detection	-sV	NO	NO	NO
UDP Scan	-sU	YES	NO	YES
IP Protocol Scan	-sO	YES	NO	NO
ACK Scan	-sA	YES	YES	NO
Window Scan	-sW	YES	YES	NO
RPC Scan	-sR	NO	NO	NO
List Scan	-sL	NO	NO	NO
Idlescan	-sI	YES	YES	NO
FTP Bounce Attack	-b	NO	YES	NO

Source : Secrets of Network Cartography: A Comprehensive Guide to nmap

TCP SYN Scan Operation

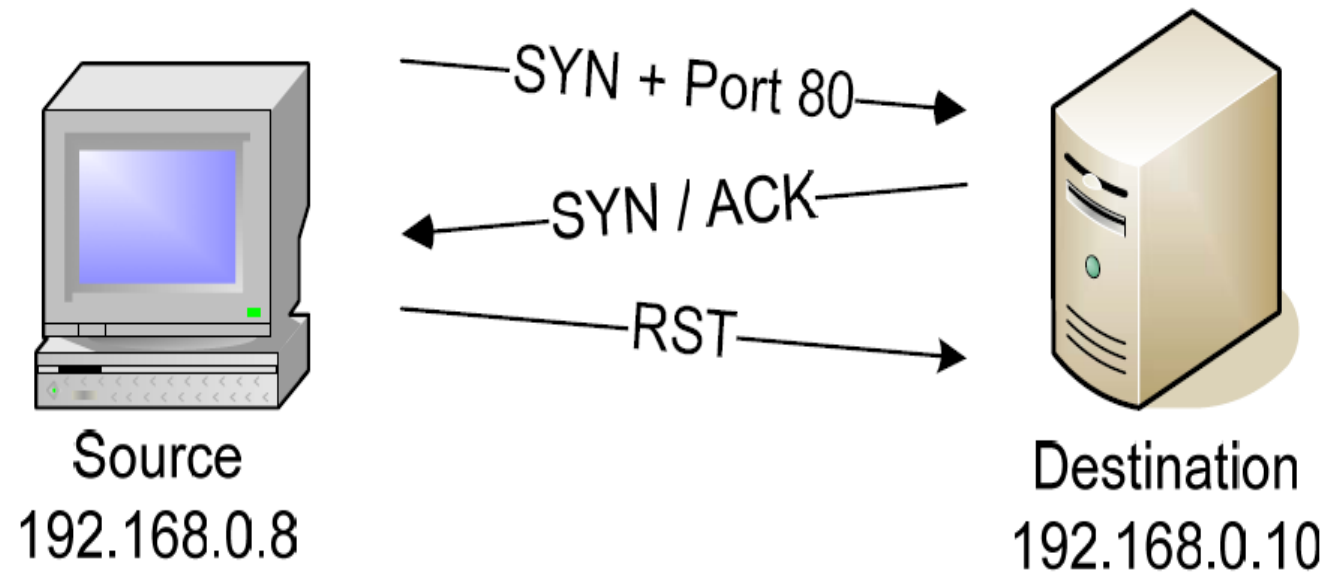
Most of the ports queried during the TCP SYN scan will probably be closed. These closed port responses to the TCP SYN frame will be met with a RST frame from the destination station.



Source	Destination	Summary
[192.168.0.8]	[192.168.0.10]	TCP: D=113 S=57283 SYN SEQ=2360927338 LEN=0 WIN=3072
[192.168.0.10]	[192.168.0.8]	TCP: D=57283 S=113 RST ACK=2360927339 WIN=0

Source : Secrets of Network Cartography: A Comprehensive Guide to nmap

If nmap receives an acknowledgment to a SYN request, then the port is open. Nmap then sends an RST to reset the session, and the handshake is never completed.

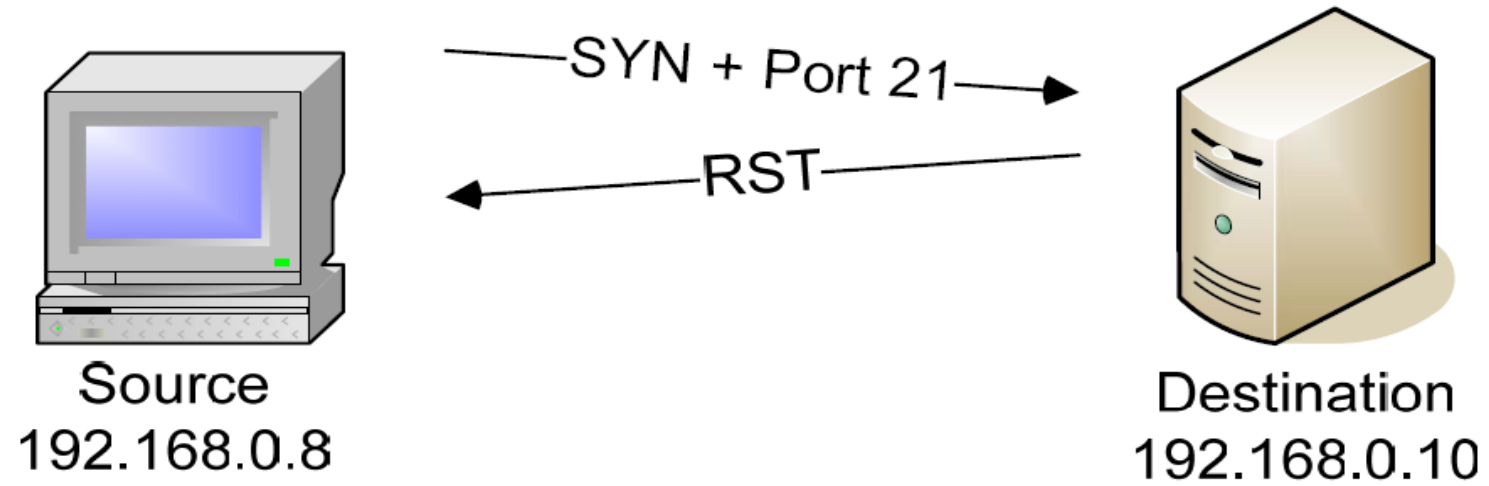


Source	Destination	Summary
[192.168.0.8]	[192.168.0.10]	TCP: D=80 S=57283 SYN SEQ=2360927338 LEN=0 WIN=3072
[192.168.0.10]	[192.168.0.8]	TCP: D=57283 S=80 SYN ACK =2360927339 SEQ=1622899389 LEN=0 WIN=65535
[192.168.0.8]	[192.168.0.10]	TCP: D=80 S=57283 RST WIN=0

Source : Secrets of Network Cartography: A Comprehensive Guide to nmap

TCP connect() Scan Operation

The TCP connect() scan to a closed port looks exactly like the TCP SYN scan:



Source	Destination	Summary
[192.168.0.8]	[192.168.0.10]	TCP: D=21 S=41441 SYN SEQ=3365539736 LEN=0 WIN=5840
[192.168.0.10]	[192.168.0.8]	TCP: D=41441 S=21 RST ACK=3365539737 WIN=0

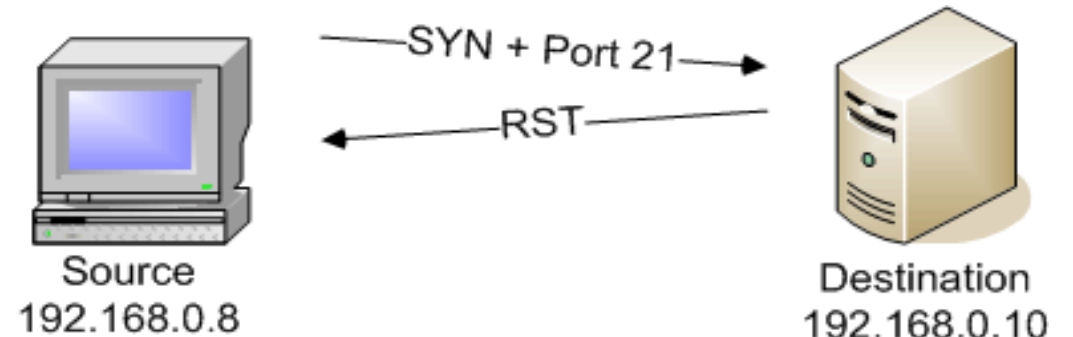
Source : Secrets of Network Cartography: A Comprehensive Guide to nmap

TCP connect() Scan

- With **connect()** call used by the operating system to **initiate a normal TCP connection to a remote device** (3-way handshake)
- No need of any special privileged access: Any user can use it.
- TCP connect scan is often logged by target host service.

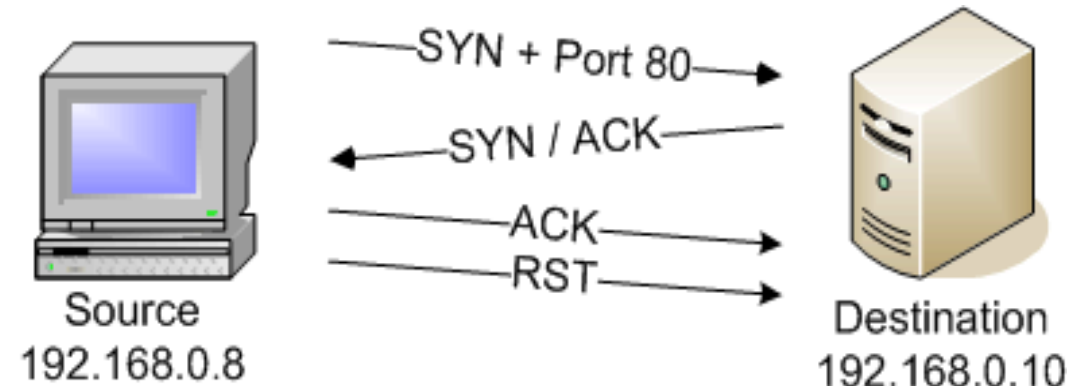
- Closed Port:

- Like the TCP SYN scan



- Open Port:

- completes the TCP 3W-Handshake (3WHS).
 - Then sends RST.



Denial of Service Attack

SECURITY

'Zombie' PCs caused Web outage, Akamai says

By Robert Lemos, and Jim Hu, CNET News.com

Published on ZDNet News: June 16, 2004, 1:37 PM PT

The attack that blacked out Google, Yahoo and other major Web sites earlier this week involved the use of a "bot net"-- a large network of zombified home PCs--Internet infrastructure provider Akamai Technologies said

- Too many requests for a particular web site "clog the pipe" so that no one else can access the site [S1].
- Also the using of land attack [S1].

- "Attack in which the primary goal is to deny the victim(s) access to a particular resource."
- A Denial of Service (DoS) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service.
- Denial of Service attacks are most frequently executed against network connectivity. The goal is to prevent hosts or networks from communicating on the network. An example of this type of attack is the "SYN flood" attack.

Categories of DoS attack

Bandwidth Attacks

- A bandwidth attack is the oldest and most common DoS attack.
- In this approach, the malicious hacker saturates a network with data traffic.
- A vulnerable system or network is unable to handle the amount of traffic sent to it and subsequently crashes or slows down, preventing legitimate access to users.

Protocol Exceptions

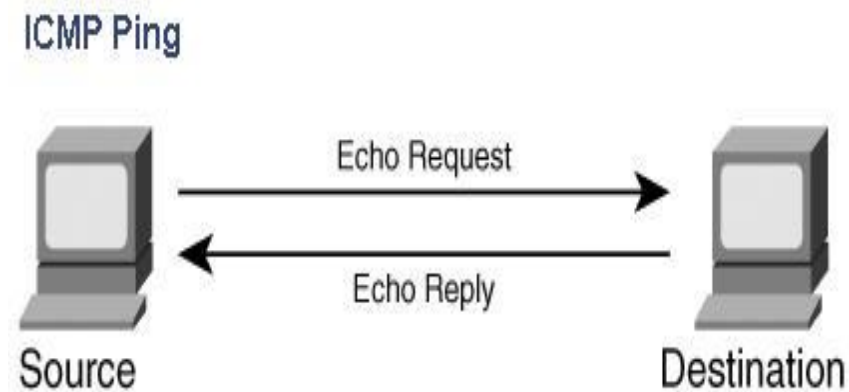
- A protocol attack is a trickier approach, but it is becoming quite popular. Here, the malicious attacker sends traffic in a way that the target system never expected, such as when an attacker sends a flood of SYN packets.

Logic Attacks

- The third type of attack is a logic attack. This is the most advanced type of attack because it involves a sophisticated understanding of networking. A classic example of a logic attack is a LAND attack, where an attacker sends a forged packet with the same source and destination IP address. Many systems are unable to handle this type of confused activity and subsequently crash

PING OF DEATH

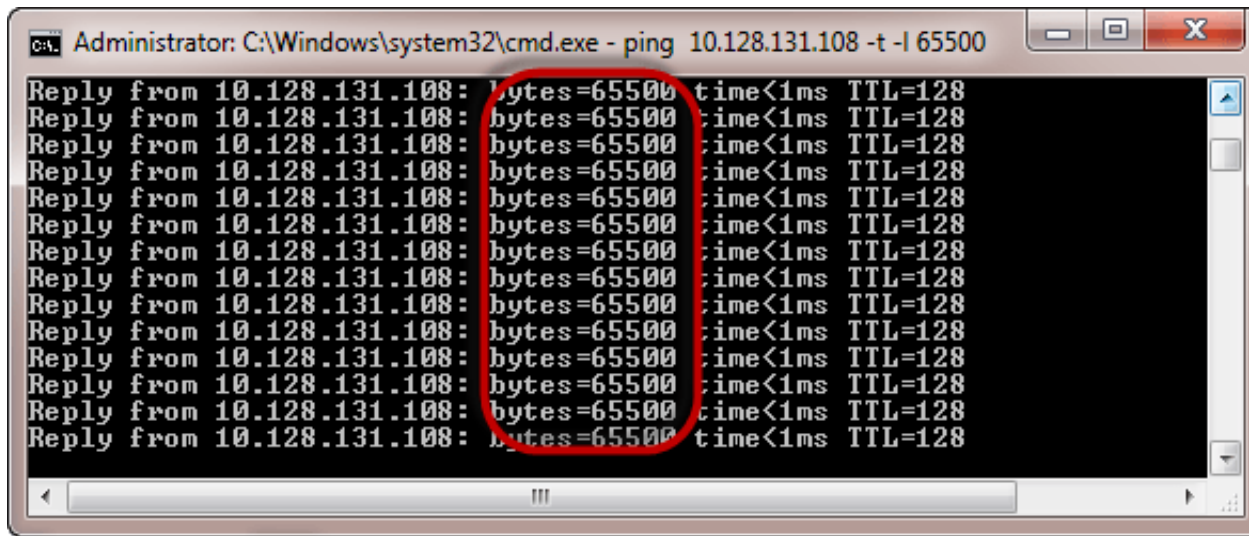
A Ping OF Death attack uses Internet Control Message Protocol (ICMP) ping messages. Ping is used to see if a host is active on a network. It also is a valuable tool for troubleshooting and diagnosing problems on a network. As the following picture, a normal ping has two messages:



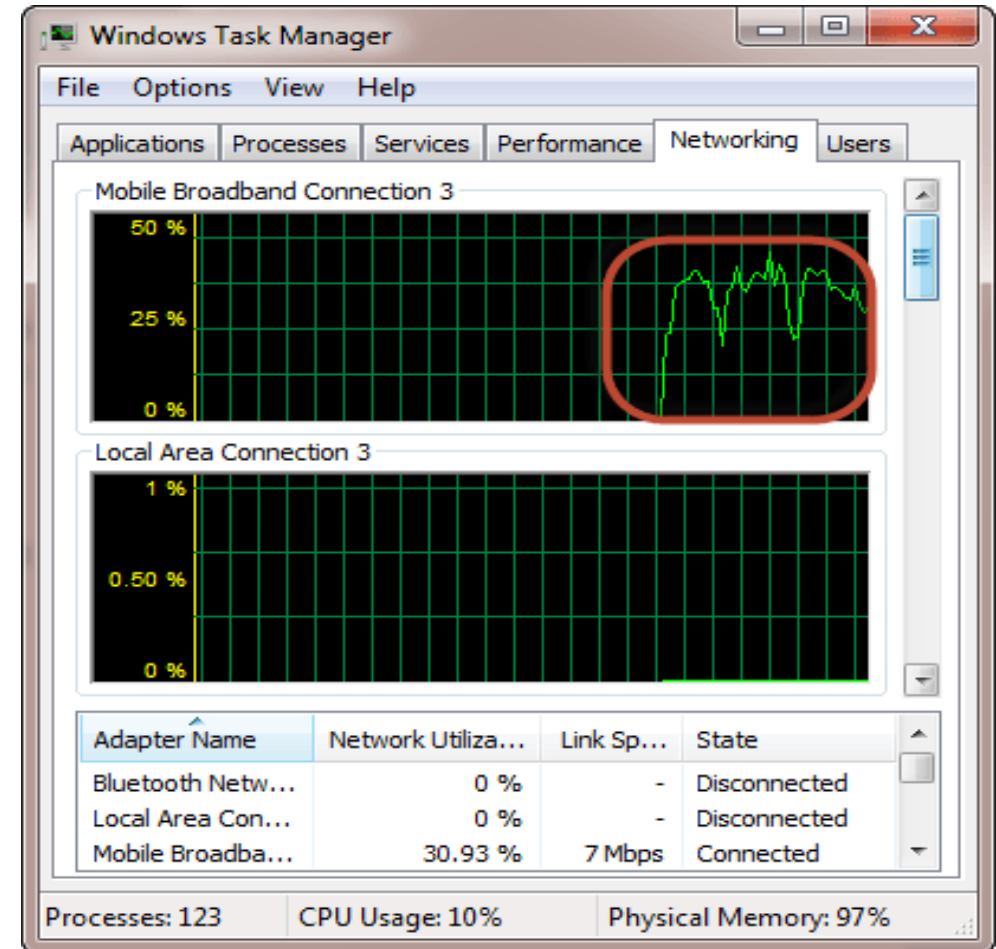
PING OF DEATH

- “ping” sends the data packets to the victim
 - “10.128.131.108” is the IP address of the victim
 - “-t” means the data packets should be sent until the program is stopped
 - “-l” specifies the data load to be sent to the victim
- You will get results similar to the ones shown below

```
ping 10.128.131.108 -t |65500
```



```
Administrator: C:\Windows\system32\cmd.exe - ping 10.128.131.108 -t -l 65500
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
```



If you want to see the effects of the attack on the target computer, you can open the task manager and view the network activities.

- Right click on the taskbar
- Select start task manager
- Click on the network tab
- You will get results similar to the following

Source: <https://www.guru99.com/ultimate-guide-to-dos-attacks.html>

Smurf Attack

- A Smurf attack is another DoS attack that uses ICMP. In this, a request is sent to a network broadcast address with the target as the spoofed source. When hosts receive the echo request, they send an echo reply back to the target. Sending multiple Smurf attacks directed at a single target in a distributed fashion might succeed in crashing it.
- A smurf attack is historically one of the oldest techniques to perform a Distributed Denial of Service (DDoS) amplification attack. This attack consists of sending a series of ICMP echo requests, with a spoofed source IP address to the network broadcast address. When this echo request is broadcast, all hosts on the LAN should simultaneously reply to the target for each spoofed request received. This technique is less effective against modern systems, as most will not reply to IP-directed broadcast traffic.

Smurf Attack Contd.

- In this attack, **Spoofed IP packets** containing ICMP Echo-Request with a source address equal to that of the attacked system and a broadcast destination address are sent to the intermediate network.
- Sending a ICMP Echo Request to a broadcast address triggers all hosts included in the network to respond with an ICMP response packet, thus creating a large mass of packets which are routed to the victim's spoofed address.

Hacking Activity: Launch a DoS attack

Nemesy is used to generate data packets and flood the target computer, router or server.

- Download Nemesy from <http://packetstormsecurity.com/files/25599/nemesy13.zip.html>
- Unzip it and run the program Nemesy.exe
- You will get the interface, Enter the target IP address, set **“0” as the infinite number of packets.** The **size field specifies the data bytes to be sent** and the **delay specifies the time interval in milliseconds.**

The following are some of the tools that can be used to perform DoS attacks.

- **Nemesy**– this tool can be used to generate random packets. It works on windows. This tool can be downloaded from <http://packetstormsecurity.com/files/25599/nemesy13.zip.html> . Due to the nature of the program, if you have an antivirus, it will most likely be detected as a virus.
- **Land and LaTierra**– This tool can be used for IP Spoofing and opening TCP connections.
- **Blast**–this tool can be downloaded from <http://www.opencomm.co.uk/products/blast/features.php>
- **Panther**- this tool can be used to flood a victim’s network with UDP packets.
- **Botnets**– these are multitudes of compromised computers on the Internet that can be used to perform a Distributed Denial of Service (DDoS) attack.

Source: <https://www.guru99.com/ultimate-guide-to-dos-attacks.html>

Low Orbit Ion Cannon (LOIC)

- The Low Orbit Ion Cannon (LOIC) is a tool commonly used to launch DoS and DDoS attacks. It was originally developed by Praetox Technology as a **network stress-testing application**, but it has since become open-source and is now mostly used with malicious intent [S2].
- It works by flooding a target server with TCP, UDP, or HTTP packets with the goal of disrupting service[S2].
- **UDP Attack:** To perform the UDP attack, select the method of attack as UDP. It has port 80 as the default option selected, but you can change this according to your need. Change the message string or leave it as the default.
- **TCP Attack:** This method is similar to UDP attack. Select the type of attack as TCP to use this.
- **HTTP Attack:** In this attack, the tool sends HTTP requests to the target server. A web application firewall can detect this type of attack easily.

Source[S2]: <https://www.cloudflare.com/learning/ddos/ddos-attack-tools/low-orbit-ion-cannon-loic/>

How to Launch DoS Attack by using LOIC

Follow these simple steps to enact a DOS attack against a website (but do so at your own risk).

Step 1: Run the tool.

Step 2: Enter the URL of the website in The URL field and click on Lock O. Then, select attack method (TCP, UDP or HTTP). These options are necessary to start the attack.

Step 3: Change other parameters per your choice or leave it to the default. Click on the Big Button. Attack is mounted on the target.

Firewalls

- What is a Firewall?
 - A hardware device, a software package, or a combination of both
 - A barrier between the Internet and an edge network (internal network)
 - A mechanism to filter Incoming (ingress) and outgoing (egress) packets.
 - May be hardware and/or software
 - Hardware is faster but can be difficult to update
 - Software is slower but easier to update

A Firewall is any device that prevents a specific types of information from moving between the outside world (untrusted network) and the inside world (trusted network).

The Firewall may be

- a separate computer system
- a service running on an existing router or server
- a separate network containing a number of supporting devices

Firewalls Categorized by Processing Modes

Firewall can be categorized by **processing mode, development era or structure.**

There are five major processing mode categories of firewall: **Packet Filtering Firewall, Application Gateways, Circuit Gateway, MAC layer Gateways** and **Hybrid Firewalls.**

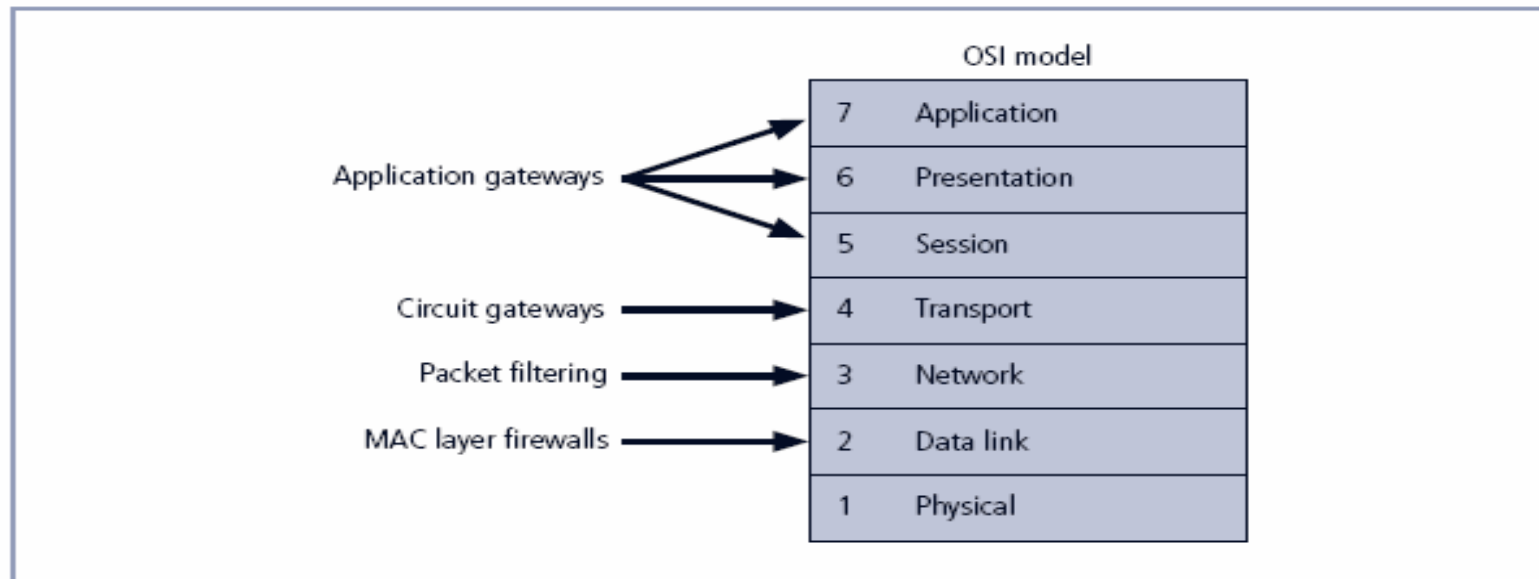


FIGURE 6-5 Firewall Types and the OSI Model

Packet Filtering Firewall Rule Conjuration

Firewall device is never accessible directly from the public network. If attacker can directly access the firewall, they may be able to modify or delete rules and allow unwanted traffic through.

Source Address	Port	Destination Address	Port	Action
Any	Any	10.10.10.1	Any	Deny
Any	Any	10.10.10.2	Any	Deny
10.10.10.1	Any	Any	Any	Deny
10.10.10.2	Any	Any	Any	Deny

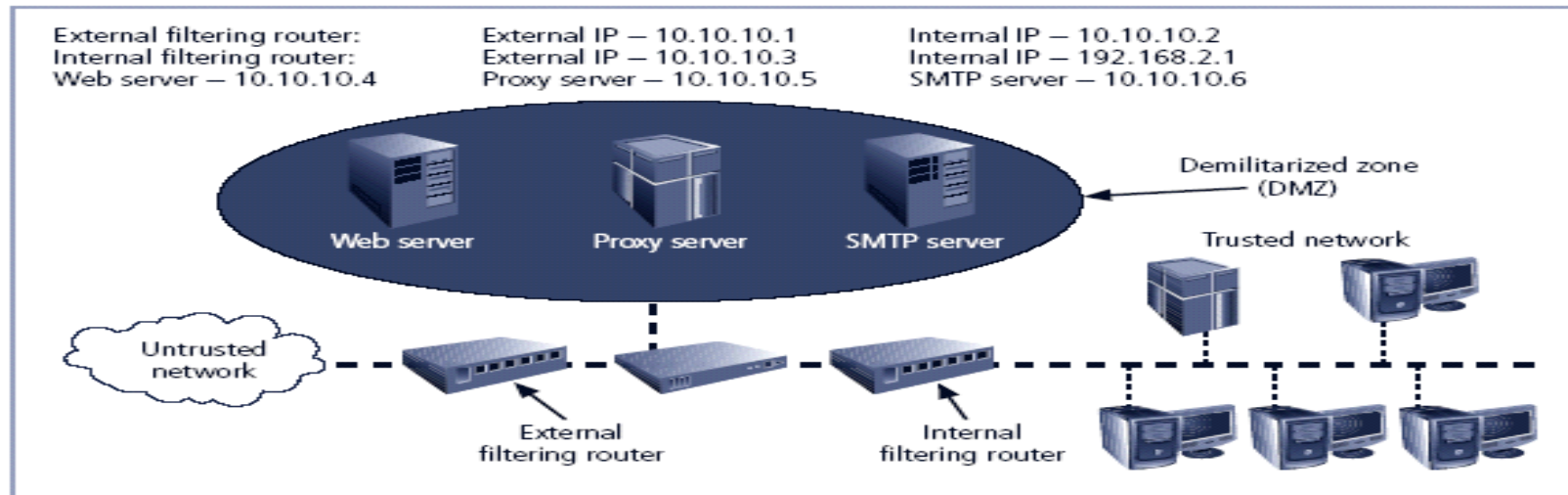


FIGURE 6-14 Example Network Configuration

Source: Principles and Practices of Information Security by Michael E. Whitman

Thanks