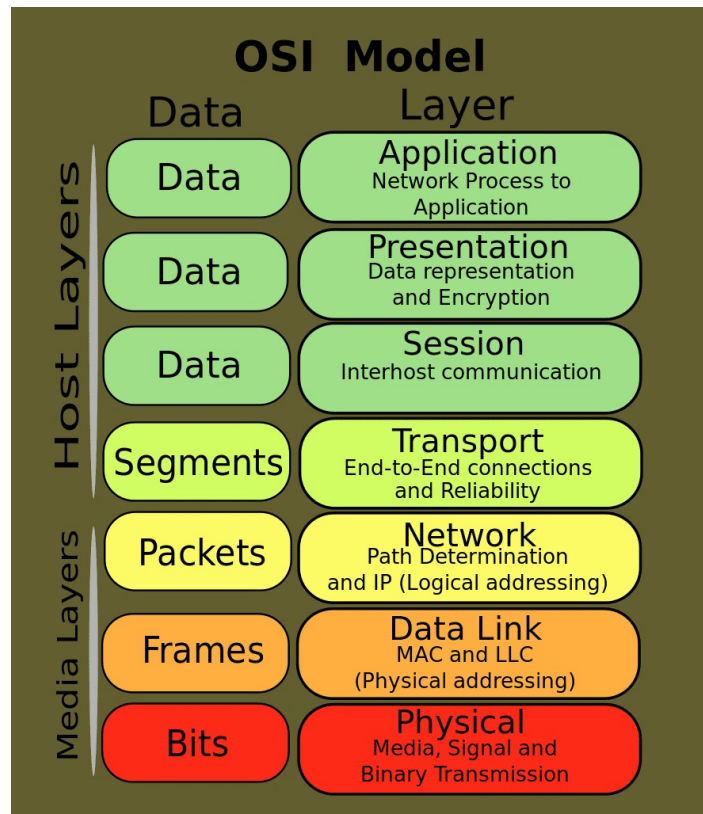


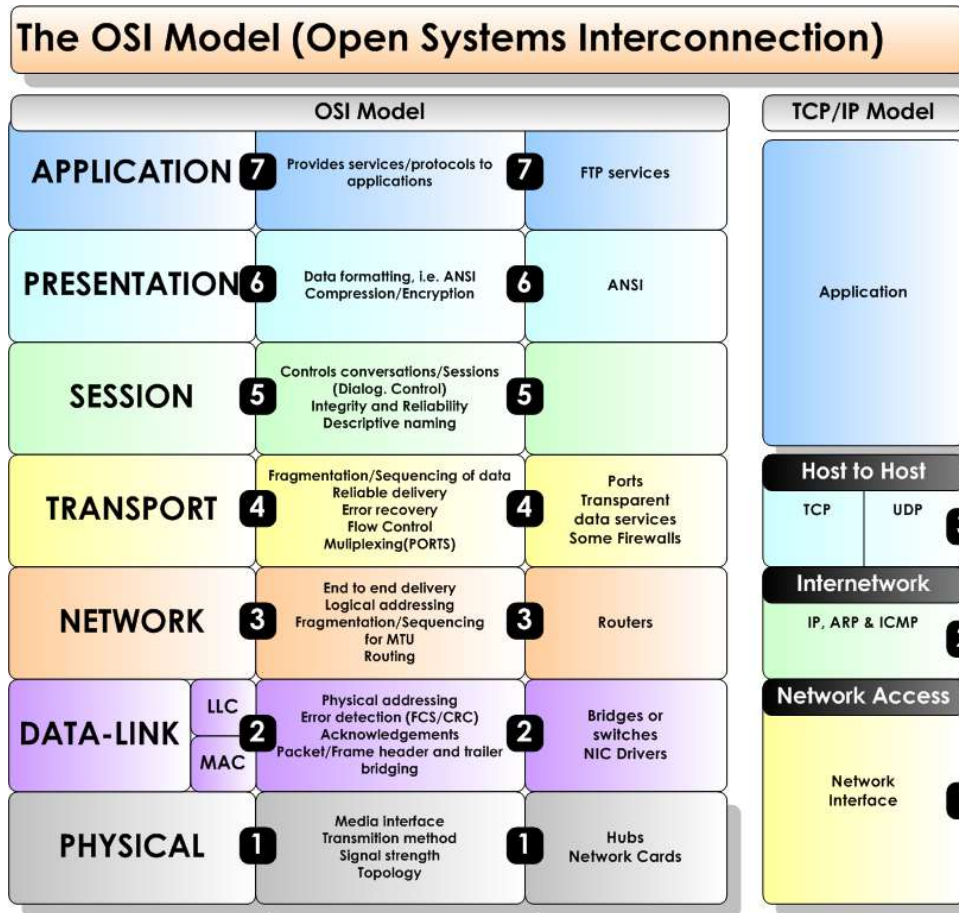
Securing Network in Cloud

Dr Mukti Padhya

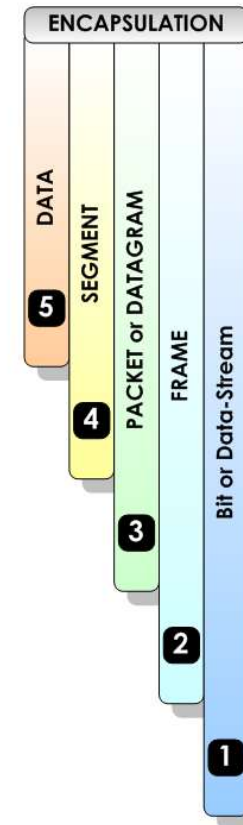
The Open Systems Interconnection model



The Open Systems Interconnection model



© Copyright 2008 Steven Iveson
www.networkstuff.eu



The Open Systems Interconnection model

1. Physical Layer

- It is the bottom-most or the first layer of the OSI Model
- It comprises the raw data which is further transmitted to the higher layers of the structure
- Preparing the physical devices in the network and accepting the received data for transmission
- The termination of connection between two nodes of a network also takes place at this stage
- This layer converts the digital bits into electrical, radio, or optical signals

2. Data Link Layer

- Access to get the data is achieved at this layer
- It breaks the input data into frames which makes analysing the data easier
- Ensures that the data received is free of any errors
- It controls the flow of data in the stipulated time duration and along with a set speed of transmission
- The data is sent to the next layer in the form of packets which are then reviewed for further processing

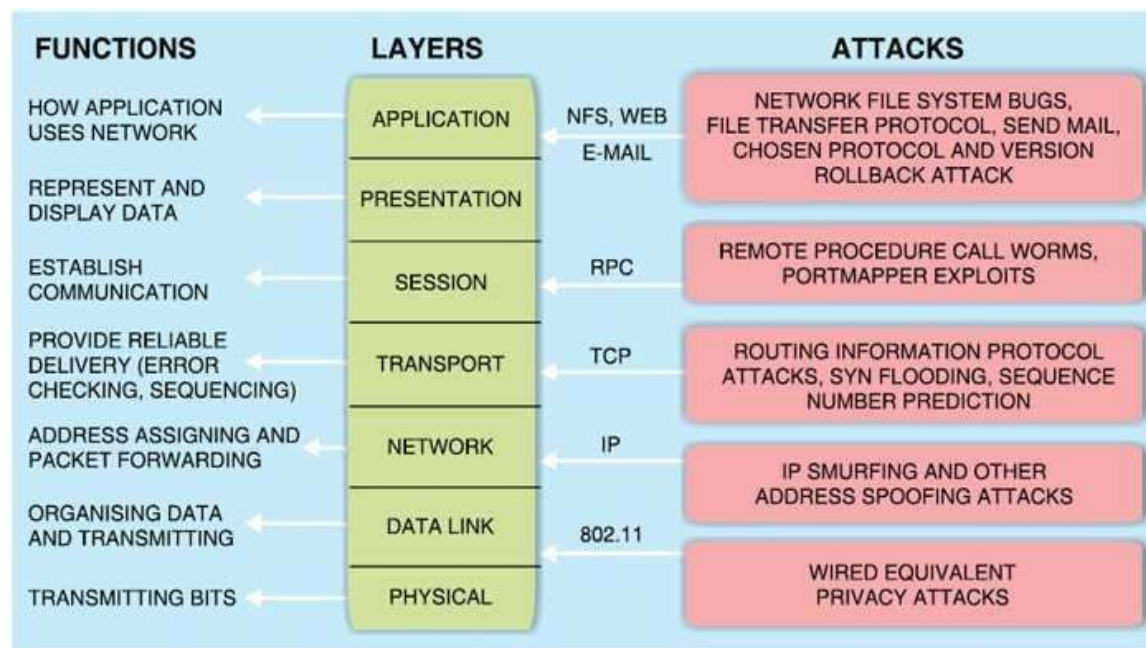
3. Network Layer

- It acts as a network controller
- Transferring of variable data from one node to another, connected in a network, takes place at this layer
- Each node has a specific address and the network layer ensures that the data is sent to its destination address
- The data is sent in the form of fragments which are then connected to each other once the processing is done

The Open Systems Interconnection model

- **4. Transport Layer**
 - The delivery of data packets is managed by the transport layer
 - It manages the flow of data, segmentation and desegmentation and error control
 - There are five classes of the transport protocol, starting from 0 and continuing till 4 (TP0 to TP4)
 - Fragmentation and reassembly of data packets occur at this stage
- **5. Session Layer**
 - The connection between the computers connected in a network is managed at this layer
 - Establishment, management and termination between the remote and local application takes place here
 - Authentication and authorisation happen at this layer
 - This layer can also terminate or end any session or transmission which is complete
- **6. Presentation Layer**
 - The data is converted into the syntax or semantics which an application understands
 - Before passing on the data any further, the data is formatted at this stage
 - Functions including compression, encryption, compatible character code set, etc. are also done at this layer of the model
 - It serves as a data translator for the network
- **7. Application Layer**
 - The interaction with the user or the user application takes place at this stage
 - When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit

Attacks on Different OSI Layers



Attack Possibilities by OSI Layer

OSI Layer	Protocol Data Unit (PDU)	Layer Description	Protocols	Examples of Denial of Service Techniques at Each Level	Potential Impact of DoS Attack	Mitigation Options for Attack Type
Application Layer (7)	Data	Message and packet creation begins. DB access is on this level. End-user protocols such as FTP, SMTP, Telnet, and RAS work at this layer	Uses the Protocols FTP, HTTP, POP3, & SMTP and its device is the Gateway	PDF GET requests, HTTP GET, HTTP POST, = website forms (login, uploading photo/video, submitting feedback)	Reach resource limits of services Resource starvation	Application monitoring is the practice of monitoring software applications using a dedicated set of algorithms, technologies, and approaches to detect zero day and application layer (Layer 7 attacks). Once identified these attacks can be stopped and traced back to a specific source more easily than other types of DDoS attacks
Presentation Layer (6)	Data	Translates the data format from sender to receiver	Uses the Protocols Compression & Encryption	Malformed SSL Requests -- Inspecting SSL encryption packets is resource intensive. Attackers use SSL to tunnel HTTP attacks to target the server	The affected systems could stop accepting SSL connections or automatically restart	To mitigate, consider options like offloading the SSL from the origin infrastructure and inspecting the application traffic for signs of attacks traffic or violations of policy at an applications delivery platform (ADP). A good ADP will also ensure that your traffic is then re-encrypted and forwarded back to the origin infrastructure with unencrypted content only ever residing in protected memory on a secure bastion host
Session (5)	Data	Governs establishment, termination, and sync of session within the OS over the network (ex: when you log off and on)	Uses the Protocol Logon/Logoff	Telnet DDoS-attacker exploits a flaw in a Telnet server software running on the switch, rendering Telnet services unavailable	Prevents administrator from performing switch management functions	Check with your hardware provider to determine if there's a version update or patch to mitigate the vulnerability
Transport (4)	Segment	Ensures error-free transmission between hosts: manages transmission of messages from layers 1 through 3	Uses the Protocols TCP & UDP	SYN Flood, Smurf Attack	Reach bandwidth or connection limits of hosts or networking equipment	DDoS attack blocking, commonly referred to as blackholing, is a method typically used by ISPs to stop a DDoS attack on one of its customers. This approach to block DDoS attacks makes the site in question completely inaccessible to all traffic, both malicious attack traffic and legitimate user traffic. Black holding is typically deployed by the ISP to protect other customers on its network from the adverse effects of DDoS attacks such as slow network performance and disrupted service
Network (3)	Packet	Dedicated to routing and switching information to different networks. LANs or internetworks	Uses the Protocols IP, ICMP, ARP, & RIP and uses Routers as its device	ICMP Flooding - A Layer 3 infrastructure DDoS attack method that uses ICMP messages to overload the targeted network's bandwidth	Can affect available network bandwidth and impose extra load on the firewall	Rate-limit ICMP traffic and prevent the attack from impacting bandwidth and firewall performance
Data Link (2)	Frame	Establishes, maintains, and decides how the transfer is accomplished over the physical layer	Uses the Protocols 802.3 & 802.5 and it's devices are NICs, switches bridges & WAPs	MAC flooding -- inundates the network switch with data packets	Disrupts the usual sender to recipient flow of data -- blasting across all ports	Many advances switches can be configured to limit the number of MAC addresses that can be learned on ports connected to end stations; allow discovered MAC addresses to be authenticated against an authentication, authorization and accounting (AAA) server and subsequently filtered
Physical (1)	Bits	Includes, but not limited to cables, pucks, and hubs	Uses the Protocols 100Base-T & 1000 Base-X and uses Hubs, patch panels, & RJ45 Jacks as devices	Physical destruction, obstruction, manipulation, or malfunction of physical assets	Physical assets will become unresponsive and may need to be repaired to increase availability	Practice defense in-depth tactics, use access controls, accountability, and auditing to track and control physical assets

Address Resolution Protocol (ARP) spoofing

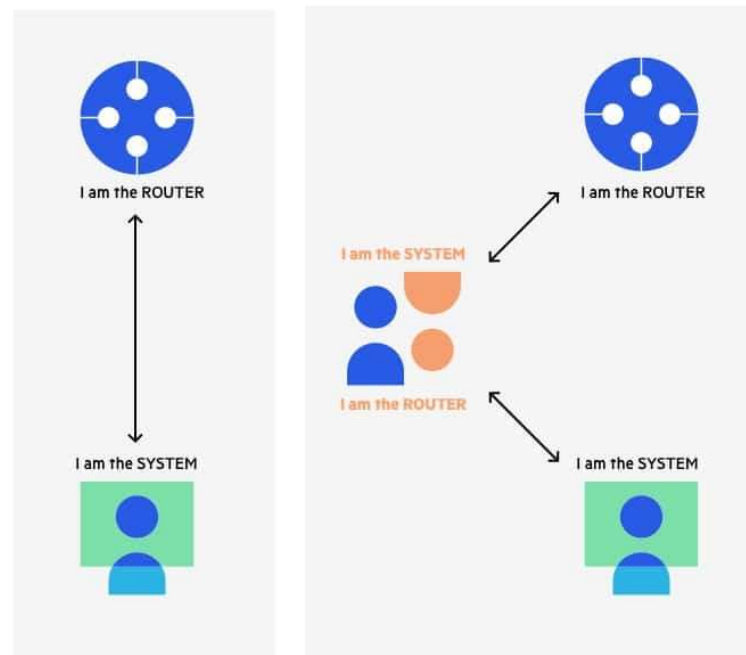
- Address Resolution Protocol (ARP) is a protocol that enables network communications to reach a specific device on the network. ARP translates Internet Protocol (IP) addresses to a Media Access Control (MAC) address, and vice versa. Most commonly, devices use ARP to contact the router or gateway that enables them to connect to the Internet.
- Hosts maintain an ARP cache, a mapping table between IP addresses and MAC addresses, and use it to connect to destinations on the network. If the host doesn't know the MAC address for a certain IP address, it sends out an ARP request packet, asking other machines on the network for the matching MAC address.
- The ARP protocol was not designed for security, so it does not verify that a response to an ARP request really comes from an authorized party. It also lets hosts accept ARP responses even if they never sent out a request. This is a weak point in the ARP protocol, which opens the door to ARP spoofing attacks.
- ARP only works with 32-bit IP addresses in the older IPv4 standard. The newer IPv6 protocol uses a different protocol, Neighbor Discovery Protocol (NDP), which is secure and uses cryptographic keys to verify host identities. However, since most of the Internet still uses the older IPv4 protocol, ARP remains in wide use.

What is ARP Spoofing (ARP Poisoning)

- An ARP spoofing, also known as ARP poisoning, is a Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices. The attack works as follows:
 1. The attacker must have access to the network. They scan the network to determine the IP addresses of at least two devices—let's say these are a workstation and a router.
 2. The attacker uses a spoofing tool, such as Arp spoof or Driftnet, to send out forged ARP responses.
 3. The forged responses advertise that the correct MAC address for both IP addresses, belonging to the router and workstation, is the attacker's MAC address. This fools both router and workstation to connect to the attacker's machine, instead of to each other.
 4. The two devices update their ARP cache entries and from that point onwards, communicate with the attacker instead of directly with each other.
 5. The attacker is now secretly in the middle of all communications.

Address Resolution Protocol (ARP) spoofing

The ARP spoofing attacker pretends to be both sides of a network communication channel



Address Resolution Protocol (ARP) spoofing

- Once the attacker succeeds in an ARP spoofing attack, they can:
- **Continue routing the communications as-is**—the attacker can sniff the packets and steal data, except if it is transferred over an encrypted channel like HTTPS.
- **Perform session hijacking**—if the attacker obtains a session ID, they can gain access to accounts the user is currently logged into.
- **Alter communication**—for example pushing a malicious file or website to the workstation.
- **Distributed Denial of Service (DDoS)**—the attackers can provide the MAC address of a server they wish to attack with DDoS, instead of their own machine.

How to Detect an ARP Cache Poisoning Attack

- Use the following command to display the ARP table, on both Windows and Linux:

`arp -a`

- The output will look something like this:

Internet Address	Physical Address
192.168.5.1	00-14-22-01-23-45
192.168.5.201	40-d4-48-cr-55-b8
192.168.5.202	00-14-22-01-23-45

How to Detect an ARP Cache Poisoning Attack

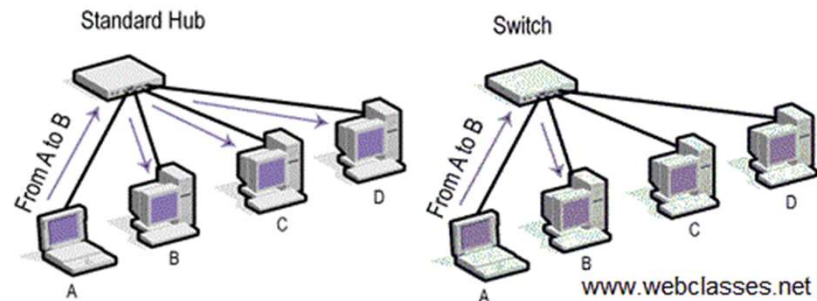
- If the table contains two different IP addresses that have the same MAC address, this indicates an ARP attack is taking place. Because the IP address 192.168.5.1 can be recognized as the router, the attacker's IP is probably 192.168.5.202.
- To discover ARP spoofing in a large network and get more information about the type of communication the attacker is carrying out, one can use the open source Wireshark protocol.

ARP Spoofing Prevention

- Here are a few best practices that can help you prevent ARP Spoofing on your network:
- **Use a Virtual Private Network (VPN)**—a VPN allows devices to connect to the Internet through an encrypted tunnel. This makes all communication encrypted, and worthless for an ARP spoofing attacker.
- **Use static ARP**—the ARP protocol lets you define a static ARP entry for an IP address, and prevent devices from listening on ARP responses for that address. For example, if a workstation always connects to the same router, you can define a static ARP entry for that router, preventing an attack.
- **Use packet filtering**—packet filtering solutions can identify poisoned ARP packets by seeing that they contain conflicting source information, and stop them before they reach devices on your network.
- **Run a spoofing attack**—check if your existing defenses are working by mounting a spoofing attack, in coordination with IT and security teams. If the attack succeeds, identify weak points in your defensive measures and remediate them.

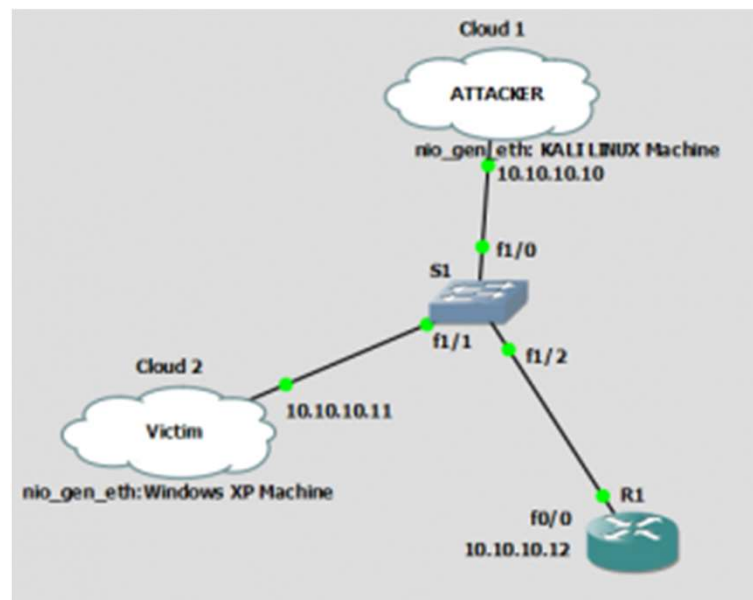
What is Content Addressable Memory table

- Hubs always perform frame flooding by sending a received packet from source (A) to all connected devices. Normally all devices will drop the received packet except the destination (B). Switches on the other hand have a table called **Content addressable memory (CAM)** which refers to a dynamic table that maps MAC addresses of the connected devices to the ports on the Switch. When the packet is sent from A to B the switch will search its CAM table for the port that corresponds to the MAC address of B and will only send the packet to B, which is more secure than the Hub flooding technique.
- BUT the question is what if this CAM table is full?



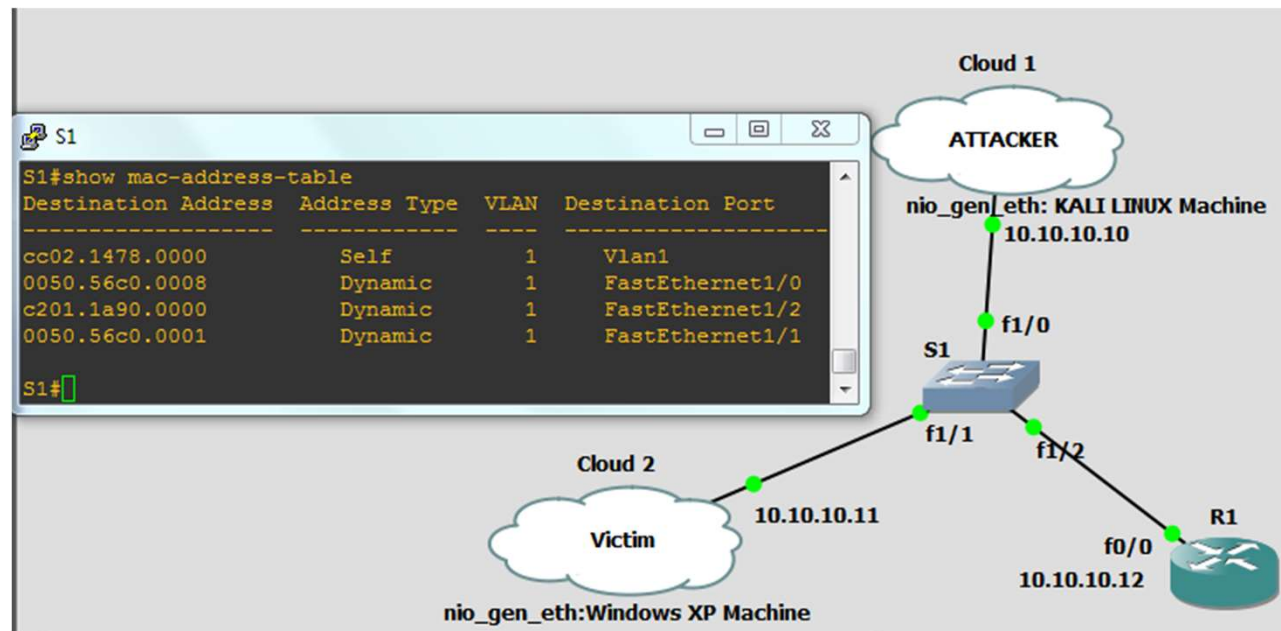
CAM Table Overflow Attack

- Assume virtual environment using GNS (virtualization of the Network), Virtual Box or a Virtual machine with two O/S's (Kali Linux and Window XP). here we have a network administrator running windows XP (victim) trying to manage its own router (R1) and a Kali Linux machine (Attacker) connected on the same switch (S1).



CAM Table Overflow Attack

- If we issue the command “**show mac-address-table**” on our switch we will see the CAM table of the Switch which shows the port and MAC addresses of the devices that are connected to it.



After pressing enter a huge number of fake random MAC addresses will be generated as seen below.

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
9594067(0) win 512
b8:98:eb:7c:bf:ee 42:83:e8:26:ff:13 0.0.0.0.55687 > 0.0.0.0.25808: S 761779879:7
61779879(0) win 512
c2:16:80:20:da:fb 74:8f:5c:4c:d9:8a 0.0.0.0.29810 > 0.0.0.0.30351: S 519706600:5
19706600(0) win 512
7a:f7:60:55:d3:28 94:11:54:76:15:80 0.0.0.0.42368 > 0.0.0.0.64499: S 946440424:9
46440424(0) win 512
37:23:d7:b:f5:56 43:5d:45:51:38:d9 0.0.0.0.50210 > 0.0.0.0.17533: S 826711423:82
6711423(0) win 512
f7:8b:34:5c:8:6 6c:22:a0:21:fc:43 0.0.0.0.38112 > 0.0.0.0.34131: S 981290977:981
```

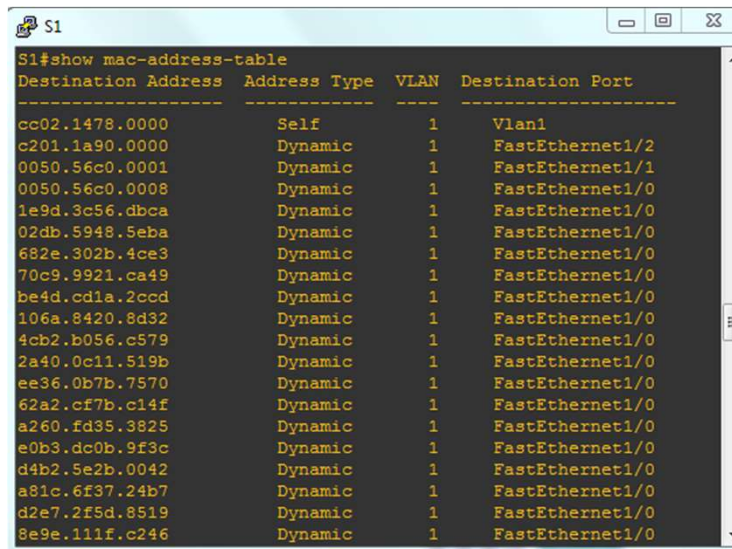
The switch will also dynamically store these MAC addresses in its CAM table. Now we will issue our first two commands on our switch again to see the changes made to the CAM table.

Here the number of the total MAC addresses stored is increasing each time we issue the same command because the Attacker's machine continues to generate a huge number of fake MAC addresses.

```
S1#show mac-address-table count
NM Slot: 1
-----
Dynamic Address Count:          6841
Secure Address (User-defined) Count: 0
Static Address (User-defined) Count: 0
System Self Address Count:      1
Total MAC addresses:             6842
Maximum MAC addresses:          8192

S1#show mac-address-table count
NM Slot: 1
-----
Dynamic Address Count:          7326
Secure Address (User-defined) Count: 0
Static Address (User-defined) Count: 0
System Self Address Count:      1
Total MAC addresses:             7327
Maximum MAC addresses:          8192
```

- The new CAM table entries will be as the following, notice the large number of MAC addresses assigned to the same port (interface FastEthernet 1/0)



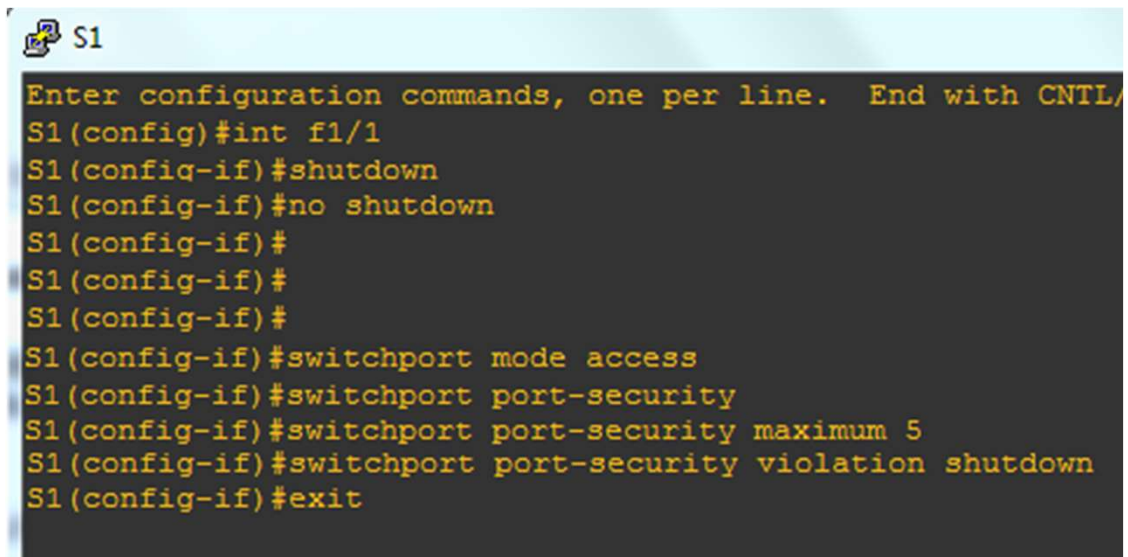
The screenshot shows a terminal window titled 'S1' with the command 'S1#show mac-address-table' executed. The output is a table with four columns: Destination Address, Address Type, VLAN, and Destination Port. The first entry is for the switch's own MAC address (cc02.1478.0000) on Vlan1. Subsequent entries show various dynamic MAC addresses assigned to FastEthernet1/2 and FastEthernet1/1, while a large number of other dynamic MAC addresses are assigned to FastEthernet1/0.

Destination Address	Address Type	VLAN	Destination Port
cc02.1478.0000	Self	1	Vlan1
c201.1a90.0000	Dynamic	1	FastEthernet1/2
0050.56c0.0001	Dynamic	1	FastEthernet1/1
0050.56c0.0008	Dynamic	1	FastEthernet1/0
1e9d.3c56.dbca	Dynamic	1	FastEthernet1/0
02db.5948.5eba	Dynamic	1	FastEthernet1/0
682e.302b.4ce3	Dynamic	1	FastEthernet1/0
70c9.9921.ca49	Dynamic	1	FastEthernet1/0
be4d.cd1a.2ccd	Dynamic	1	FastEthernet1/0
106a.8420.8d32	Dynamic	1	FastEthernet1/0
4cb2.b056.c579	Dynamic	1	FastEthernet1/0
2a40.0c11.519b	Dynamic	1	FastEthernet1/0
ee36.0b7b.7570	Dynamic	1	FastEthernet1/0
62a2.cf7b.c14f	Dynamic	1	FastEthernet1/0
a260.fd35.3825	Dynamic	1	FastEthernet1/0
e0b3.dc0b.9f3c	Dynamic	1	FastEthernet1/0
d4b2.5e2b.0042	Dynamic	1	FastEthernet1/0
a81c.6f37.24b7	Dynamic	1	FastEthernet1/0
d2e7.2f5d.8519	Dynamic	1	FastEthernet1/0
8e9e.111f.c246	Dynamic	1	FastEthernet1/0

- After a couple of minutes our humble switch is forwarding packets as a Hub !!
- Now the switch is flooding any received packet from any port to all other ports including the (Attacker), he will receive a copy of each packet sent from the administrator(Victim) or any other machine to the router (R1) or any other device connected to this switch.
- By using software like Ettercap the Attacker can change his NIC from the normal operation mode into promiscuous mode which causes the controller to pass all traffic it receives to the CPU rather than passing only the frames that the controller is intended to receive, this mode is normally used for packet sniffing and is also known as man in the middle attack.

CAM Table Overflow Attack : Recovery

To recover from this attack we first need to shutdown this port from the switch using the two commands **shutdown** & **no shutdown** on the attacked interface



```
S1
Enter configuration commands, one per line.  End with CNTL/Z
S1(config)#int f1/1
S1(config-if)#shutdown
S1(config-if)#no shutdown
S1(config-if)#
S1(config-if)#
S1(config-if)#
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 5
S1(config-if)#switchport port-security violation shutdown
S1(config-if)#exit
```

CAM Table Overflow Attack : Prevention

- To prevent this type of attack we will change the port to an access port by issuing **switchport mode access** and to apply port security on our port we type **switchport port-security**, after that we will assign the maximum number of MAC addresses to be stored in the CAM table for this interface using **switchport port-security maximum 5**.
- Finally we will choose our violation action that will be applied when the user (attacker) is trying to generate more than 5 MAC addresses associated to same port.
- We choose to shutdown this port **switchport port-security violation shutdown**. Now if the attacker attempts to perform this attack again on this switch his port will be automatically shutdown, also a log will be generated on the switch informing the administrator that the (attacker) MAC address on this port was trying to attack us and the port state is now down.

DHCP Starvation Attack

- What is DHCP?
- DHCP (Dynamic Host Configuration Protocol) is used to assign IP addresses to machines within any network automatically. It is also known as zeroconf protocol, as network administrators don't need to assign IP addresses to machines manually. To assign IP addresses, DHCP makes use of DORA packets which stands for Discover message, offer message, Request message, and acknowledgment message respectively.

DHCP Starvation Attack

- A DHCP Starvation attack can result in a Denial of Service (DoS) attack or a Man in the Middle (MITM) attack.
- To perform this attack, the attacker sends tons of bogus DHCP Discover messages with spoofed source MAC addresses. The DHCP server tries to respond to all these bogus messages, and as a result, the pool of IP addresses used by the DHCP server is depleted. Hence, a legitimate user won't be able to get an IP address via DHCP. This results in a DoS attack.
- Furthermore, the attacker can set up a rogue DHCP server to assign IP addresses to legitimate users. This rogue server can also provide the gateway router and DNS server to users. Now, all the network traffic can be routed via the attacker's machine, and this is nothing but the MITM attack.

DHCP Starvation Attack : Example

- The IP address of the DHCP server is 10.10.10.1/24 with a subnet mask of 255.255.255.0. So, the DHCP server can hand out 254 unique IP addresses. However, some IP addresses are reserved for static routing, so it could be less than 254. The attacker sends N DHCP Discover packets, where N is very large compared to 254. Hence, the DHCP server can no longer hand out IP addresses.
- DHCP Starvation attack can be prevented by implementing port security. Port security can be configured in a switch. With port security, you can limit the number of MAC addresses learned by the port. Hence, the switch would forward packets with known [MAC addresses](#), and discard others. This would prevent bogus packets from reaching the DHCP server.

CDP (Cisco Discovery Protocol) Attacks

- CDP is a Layer 2 protocol used by Cisco devices; it is used for discovering other directly connected Cisco devices in a network, This allows devices to auto-configure their connections hence it simplifies connectivity and configuration.
- Generally, CDP is enabled on most Cisco devices. As routers don't circulate it, the CDP data is transmitted through periodic broadcasts that are maintained locally in the cisco device CDP table.

CDP (Cisco Discovery Protocol)

- **Information in CDP message:**
 - It contains the version of IOS software.
 - It contains information about the IP addresses of the device.
 - The name of the devices.
 - The information about hardware platform.
 - It contains the hardware capabilities., and
 - The information about the interface that generated the CDP message.
- **Benefits of CDP:**
 - It allows the use of RTP (Real-Time Transport Protocol) and different network-layer protocols to locate devices and tells how they are configured.
 - It assists in troubleshooting TLV (Type Length Value) fields.
 - It can be used as a diagnostic tool to help in troubleshooting device and network-related issues.
 - It enables the detection of the IP address of a wrongly configured switch/router on the other side of a WAN-link.

CDP (Cisco Discovery Protocol)

```
Router2# show cdp neighbors
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge  
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,  
D - Remote, C - CVTA, M - Two-port Mac Relay
```

Device ID Port ID	Local Intrfce	Holdtme	Capability	Platform
Router 1 Ser0/0	Ser0/0	143	R S I	2500
Router 3 Fa1/0	Fa1/0	158	R S I	2500

```
Router3# show cdp neighbors
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge  
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,  
D - Remote, C - CVTA, M - Two-port Mac Relay
```

Device ID Port ID	Local Intrfce	Holdtme	Capability	Platform
Router 2 Fa1/0	Fa1/0	141	R S I	2500

CDP (Cisco Discovery Protocol) Attacks

- CDP database is comprised of a lot of data about the device such as capabilities, IP address, native [VLAN](#), software version, platform version, etc.
- And when all this information gets in the hand of a malicious user through a compromised system, they can use this information to find exploits for attacking the network.
- Generally carried out as a DoS attack.