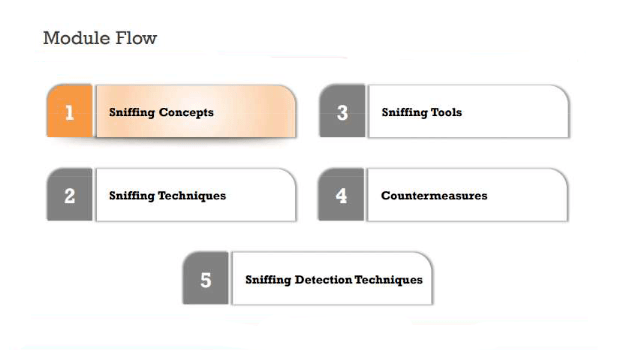
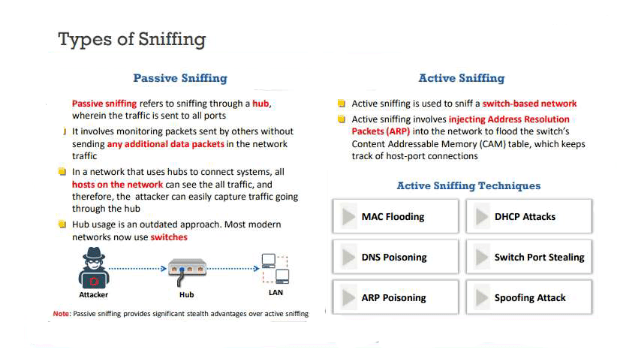
Module : Sniffing

Module flow



Sniffing Concepts

[Sniffing](https://www.greycampus.com/blog/information-security/what-is-a-sniffing-attack-and-how-can-you-defend-it) is a process of monitoring and capturing all data packets passing through given network. Sniffers are used by network/system administrator to monitor and troubleshoot network traffic. Attackers use sniffers to capture data packets containing sensitive information such as password, account information etc. Sniffers can be hardware or software installed in the system. By placing a packet sniffer on a network in promiscuous mode, a malicious intruder can capture and analyze all of the network traffic.



There are two types:

Active Sniffing:

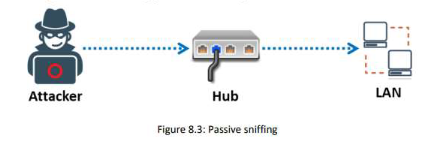
Sniffing in the switch is active sniffing. A switch is a point to point network device. The switch regulates the flow of data between its ports by actively monitoring the MAC address on each port, which helps it pass data only to its intended target. In order to capture the traffic between target sniffers has to actively inject traffic into the LAN to enable sniffing of the traffic. This can be done in various ways.

1 In this sniffing type, attacker directly interacts with target machine by sending packets and receiving responses.   
2 This sniffing is carried out through Switch. In this type, attacker tries to poison the switch by sending bogus MAC address.

3 Examples of active sniffing : ARP spoofing, MAC flooding, HTTPS and SSH spoofing, DNS spoofing etc.

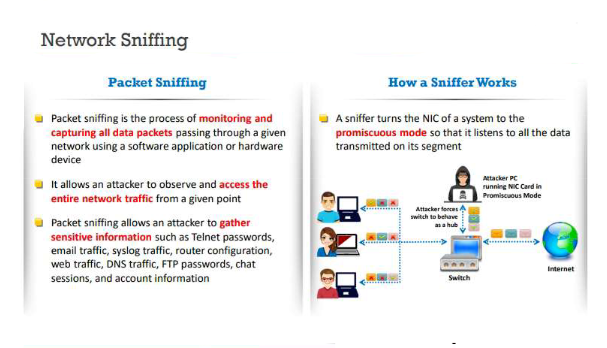
Passive Sniffing:

This is the process of sniffing through the hub. Any traffic that is passing through the non-switched or unbridged network segment can be seen by all machines on that segment. Sniffers operate at the data link layer of the network. Any data sent across the LAN is actually sent to each and every machine connected to the LAN. This is called passive since sniffers placed by the attackers passively wait for the data to be sent and capture them.



# Network Sniffing

Network sniffing is the practice of using a network interface on a computer system to monitor or capture information regardless of whether it is the specified destination for the information.

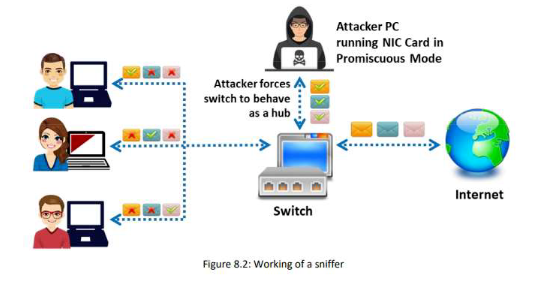


Working of Network Sniffing

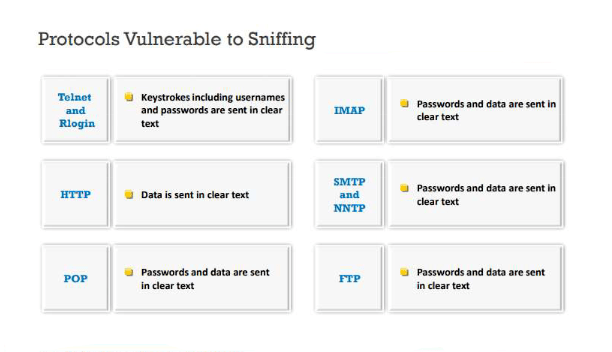
The Network sniffing tool intercept and log the network traffic with the software’s help for sniffing the data packets. This software helps in accessing the information of a complete network or a small part of the network. As we know, the networks used to send the packet for sending the data. The size of the data can be huge, and sending it in a single packet puts the load on the network that affects the data’s integrity. So whenever the data file has sent, it is mainly broken into small steps and then delivers to the destination. The data packet includes the destination of address, number of packets, reassembly order and source address. The data packet, once it reached the destination, then its footers and headers have been removed. The network has a filter that can discard the packet that is not addressed to the same network.

Once the network data has been received, the following action takes place:

* The data packets or content has been recorded.
* The software records the header section of the data packets to save space.
* The network data that has been captured is decoded and formatted so that the user can view the information.
* The packet sniffers analyze the error in network connection, communication, and other systems.
* The network sniffers sniff the sensitive data, like passwords, personal information and other card details.



Protocol Vulnerable to Sniffing



The following protocols are vulnerable to Sniffing

Telnet and Rlogin 🡺

HTTP 🡺

POP 🡺

IMAP 🡺

FTP 🡺

SMTP and NNTP 🡺

SNIFFING TECHNIQUES

## MAC ATTACKS

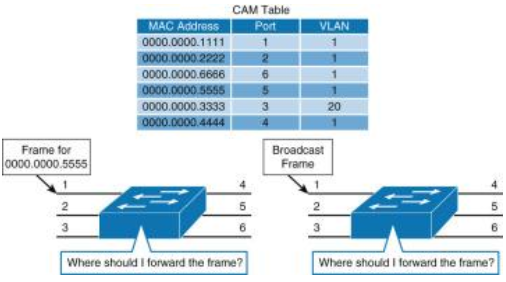
Before getting into Mac Attacks , we will learn about Mac Address

# What is MAC Address?

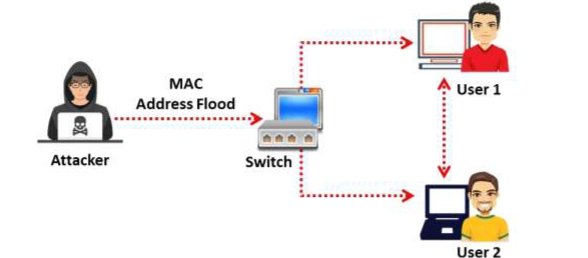
* MAC address is the physical address, which uniquely identifies each device on a given network. To make communication between two networked devices, we need two addresses: **IP address and MAC address.** It is assigned to the NIC (Network Interface card) of each device that can be connected to the internet.
* It stands for **Media Access Control**, and also known as **Physical address, hardware address, or BIA (Burned In Address).**
* It is globally unique; it means two devices cannot have the same MAC address. It is represented in a hexadecimal format on each device, such as **00:0a:95:9d:67:16.**
* It is 12-digit, and 48 bits long, out of which the first 24 bits are used for ***OUI***(Organization Unique Identifier), and 24 bits are for NIC/vendor-specific.
* It works on the data link layer of the OSI model.
* It is provided by the device's vendor at the time of manufacturing and embedded in its NIC, which is ideally cannot be changed.
* The **ARP protocol** is used to associate a logical address with a physical or MAC address.

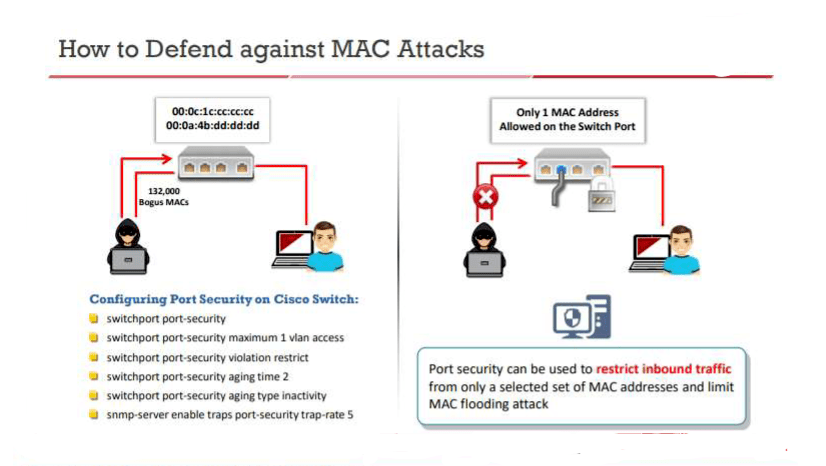
## CAM Table

Content Addressable Memory (CAM) table is a system memory construct used by Ethernet switch logic which stores information such as MAC addresses available on physical ports with their associated VLAN Parameters. The CAM table, or content addressable memory table, is present in all switches for layer 2 switching. This allows switches to facilitate communications between connected stations at high speed and in full-duplex regardless of how many devices are connected to the switch. Switches learn MAC addresses from the source address of Ethernet frames on the ports, such as Address Resolution Protocol (ARP) response packets.

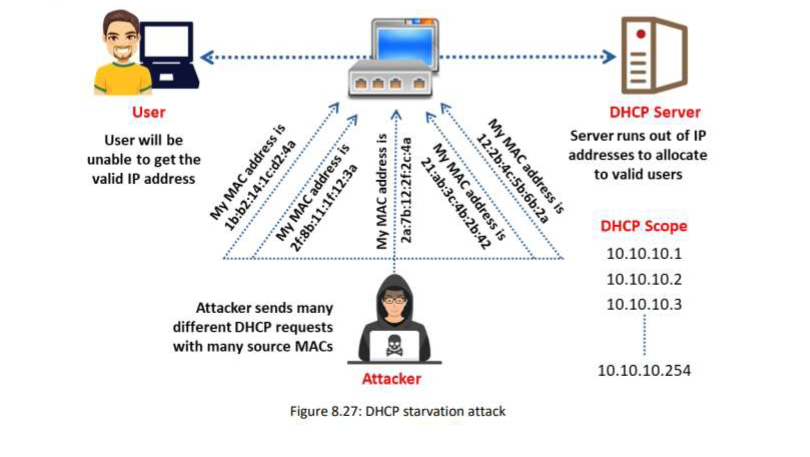


## MAC Flooding 🡺 MAC-flooding is an attack where the CAM table is flooded with fake MAC-IP pairs, so CAM table overflows causing traffic to flood all ports on switch (i.e) changing switch to behave like a hub.



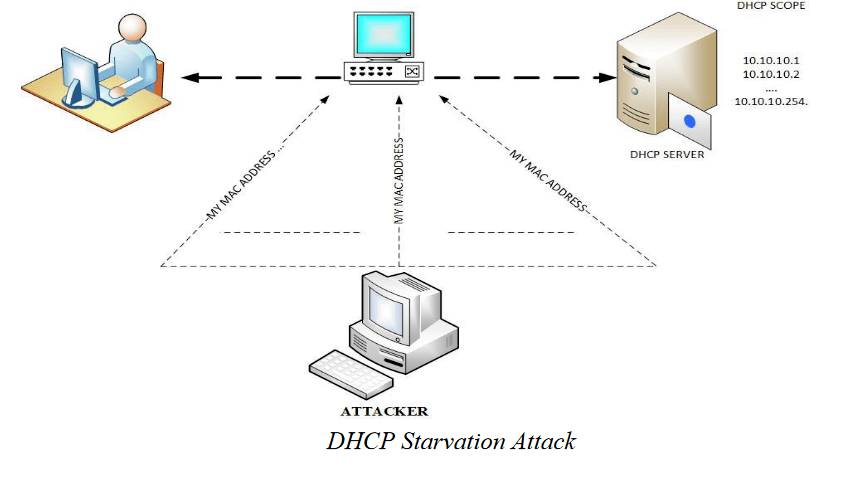


DHCP ATTACKS or Dynamic Host Configuration Protocol attacks



Dynamic Host Configuration Protocol (DHCP) is a client-server protocol that provides the IP address of a gas and provides configuration information (such as default gateway, subnet mask) A DHCP relay agent, which sends DHCP requests from one LAN over another LAN, so there doesn't have to be a DHCP server on each LAN, it involves the following steps:  
- DHCPDISCOVER request asking for DHCP configuration;  
- DHCP Relay agent unicast this message to DHCP server;  
- DHCP server unicasts DHCPOFFER;  
- Relay agent broadcast DHCPOFFER in the client’s network;  
- Client broadcast DHCPREQUEST asking for DHCP configuration;  
- Server unicasts DHCPPACK which contains configuration information  
As part of the DHCP STARVATION ATTACK attack, the hacker requests a large number of DHCPREQUEST and uses all available IP address, so the DHCP server can no longer issue an IP address and in turn leads to Denial of Service (DOS) attack. In the figure below, the attacker requests a large number of IP addresses for the DHCP server, which results in the denial of service to other users. Fig DHCP Starvation Attack

In the case of the ROGUE DHCP SERVER ATTACK attack, the attacker will introduce a rogue server. The DHCP server and the rogue server will respond to the client's DHCP request, the responding server will be picked up by the first one, so the rogue server will respond first. The client will send data to the dishonest server which in turn will send them to the real server. Therefore, the attacker monitors and captures all sensitive data, the client will not be aware of all these attacks. Port security will be able to limit the maximum number of MAC addresses in the switch port, thus avoiding DHCP attacks. The DHCP snooping feature is available on switches, and to protect you from  
rogue DHCP servers, DHCP snooping is configured on the port on which the valid DHCP server is connected. Therefore, the switch will not allow the other ports to respond to the DHCP request.



Some examples of DHCP starvation tools are listed below

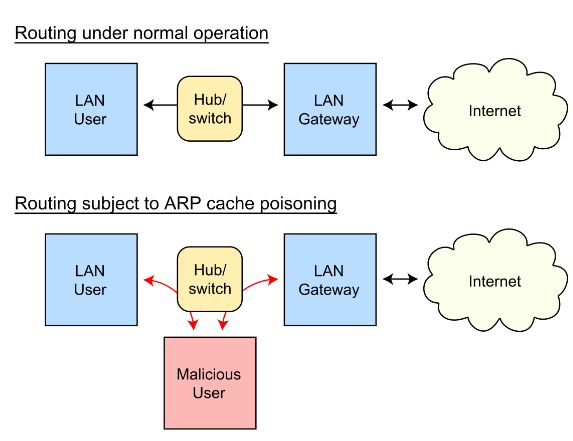
1 Hyenae

2 dhcpstarv

3 Gobbler

4 DHCPig

ARP Spoofing🡺 ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker’s MAC address with the IP address of a legitimate computer or server on the network. Once the attacker’s MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address. ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol. It is also known as ARP poisoning.



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](https://www.imperva.com/learn/application-security/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. If they do this for a large number of IPs, the target server will be bombarded with traffic.

## How to Detect an ARP Cache Poisoning Attack

Here is a simple way to detect that a specific device’s ARP [cache has been poisoned](https://www.imperva.com/learn/performance/browser-caching/), using the command line. Start an operating system shell as an administrator. 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

If the table contains two different IP addresses that have the same MAC address, this indicates an ARP [attack is taking place](https://www.imperva.com/learn/ddos/denial-of-service/). 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, you 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.

Tools for ARP Poisoning  
o Cain and Abel  
o WinArpAttacker  
o Ufasoft  
o dsniff

Spoofing Attacks

MAC Spoofing

DNS Spoofing

## 