

Chapter 8: Sniffing

Technology Brief

This chapter focuses on Sniffing concepts. By Sniffing, you can monitor all sorts of traffic either protected or unprotected. Using Sniffing attacker can gain such information which might be helpful for further attacks and can cause trouble for the victim. Furthermore, in this chapter, you will learn Media Access Control (MAC) Attacks, Dynamic Host Configuration Protocol (DHCP) Attacks, Address Resolution Protocol (ARP) Poisoning, MAC Spoofing Attack, DNS Poisoning. Once you have done with sniffing, you can proceed to launch attacks such as Session Hijacking, DoS Attacks, MITM attack, etc. Remember that Sniffers are not hacking tools, they are diagnostic tools typically used for observing network, troubleshooting issues.

Sniffing Concepts

Introduction to Sniffing

Sniffing is the process of scanning and monitoring of the captured data packets passing through a network using Sniffers. The process of sniffing is performed by using Promiscuous ports. By enabling promiscuous mode function on the connected network interface, allow capturing all traffic, even when traffic is not intended for them. Once the packet is captured, you can easily perform the inspection.

There are two types of Sniffing: -

1. Active Sniffing
2. passive Sniffing

Using Sniffing, the attacker can capture packet like Syslog traffic, DNS traffic, Web traffic, Email and other types of data traffic flowing across the network. By capturing these packets, an attacker can reveal information such as data, username, and passwords from protocols such as HTTP, POP, IMAP, SMTP, NMTP, FTP, Telnet, and Rlogin and other information. Anyone within same LAN, or connected to the target network can sniff the packets. Let focus how sniffers perform their action and what we get using sniffing.

Working of Sniffers

In the process of Sniffing, an attacker gets connected to the target network in order to sniff the packets. Using Sniffers, which turns Network Interface Card (NIC) of the attacker's system into promiscuous mode, attacker captures the packet. Promiscuous mode is a mode of the interface in which NIC respond for every packet it receives. As you can observe in the figure below, the attacker is connected in promiscuous mode, accepting each packet even those packet which is not intended for him.

Once the attacker captures the packets, it can decrypt these packets to extract information. The fundamental concept behind this technique is if you are connected to a target network with a switch as opposed to a hub, broadcast, and multicast traffic is transmitted on all ports. Switch forward the unicast packet to the specific port where the actual host is connected. Switch maintain its MAC table to validate who is connected to which port. In this case, attacker alters the switch configuration by using different techniques such as Port Mirroring or Switched Port Analyzer (SPAN). All packets passing through a certain port will be copied onto a certain port (the port on which attacker is connected with promiscuous mode). If you are connected to a hub, it will transmit all packet to all ports.

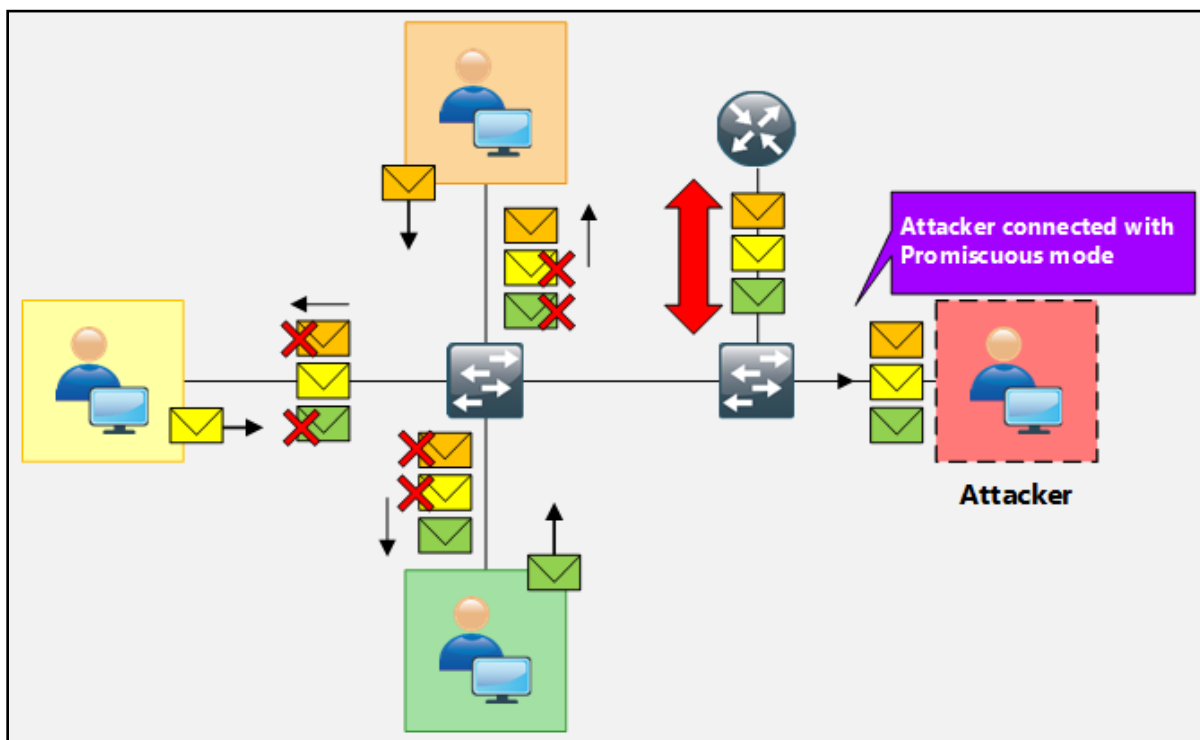


Figure 8-01 Packet Sniffing

Types of Sniffing

Passive Sniffing

Passive Sniffing is the sniffing type in which there is no need of sending additional packets or interfering the device such as Hub to receive packets. As we know, Hub broadcast every packet to its ports, which helps the attacker to monitor all traffic passing through hub without any effort.

Active Sniffing

Active Sniffing is the sniffing type in which attacker has to send additional packets to the connected device such as Switch to start receiving packets. As we know, a unicast packet from the switch is transmitted to a specific port only. The attacker uses certain

techniques such as MAC Flooding, DHCP Attacks, DNS poisoning, Switch Port Stealing, ARP Poisoning, and Spoofing to monitor traffic passing through the switch. These techniques are defined in detail later in this chapter.

Hardware Protocol Analyzer

Protocol Analyzers, either Hardware or Software analyzer are used to analyze the captured packets and signals over the transmission channel. Hardware Protocol Analyzers are the physical equipment which is used to capture without interfering the network traffic. A major advantage offered by these hardware protocol analyzers are mobility, flexibility, and throughput. Using these hardware analyzers, an attacker can: -

- Monitor Network Usage
- Identify Traffic from hacking software
- Decrypt the packets
- Extract the information
- Size of Packet

KEYSIGHT Technologies offers various products. To get updates and information, visit the website www.keysight.com. There is also another Hardware protocol analyzer products available in the market by different vendors like RADCOM and Fluke.

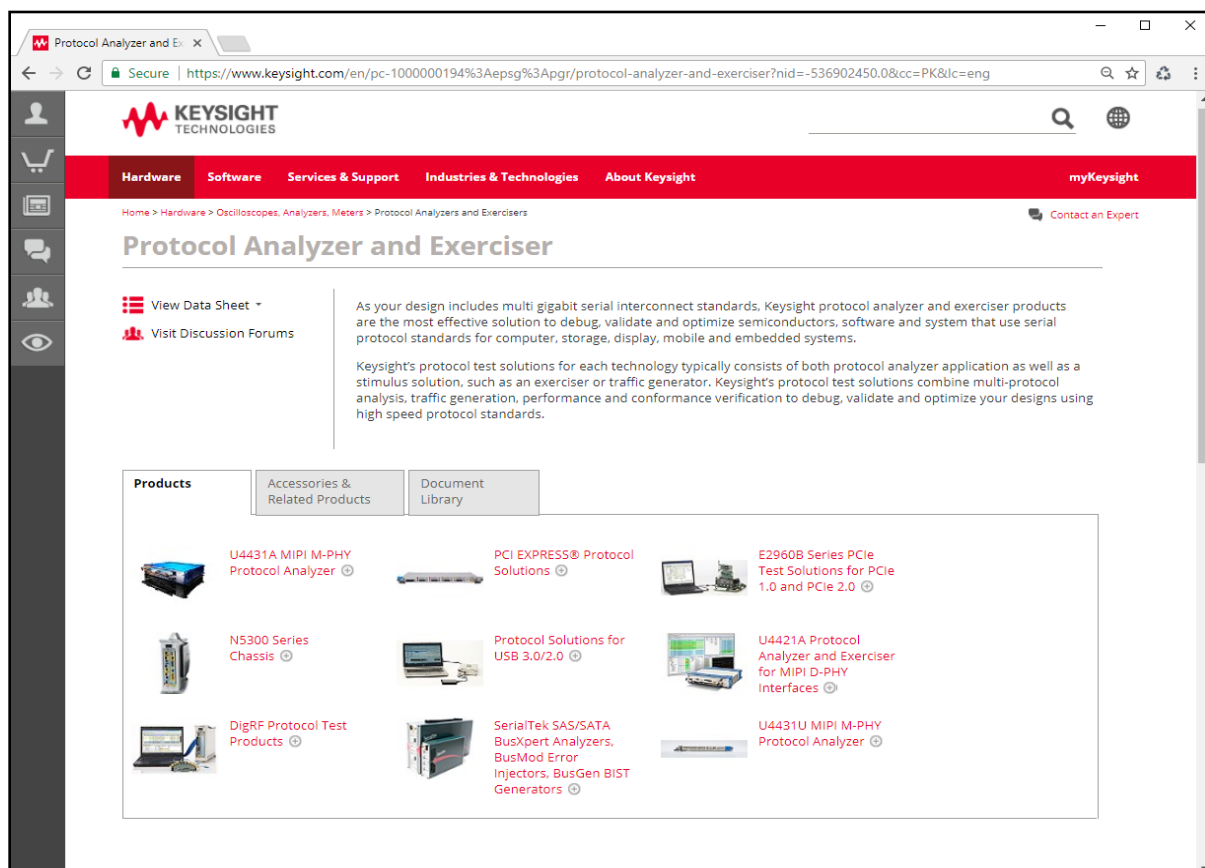


Figure 8-02 KEYSIGHT Technologies Hardware Protocol Analyser Products

SPAN Port

You have a user who has complained about network performance, no one else in the building is experiencing the same issues. You want to run a Network Analyser on the port like Wireshark to monitor ingress and egress traffic on the port. To do this, you can configure SPAN (Switch Port Analyser). SPAN allows you to capture traffic from one port on a switch to another port on the same switch.

SPAN makes a copy of all frames destined for a port and copies them to the SPAN destination port. Certain traffic types are not forwarded by SPAN like BDPUs, CDP, DTP, VTP, STP traffic. The number of SPAN sessions that can be configured on a switch is model dependent. For example, Cisco 3560 and 3750 switches only support up to 2 SPAN sessions at once, whereas Cisco 6500 series switches support up to 16.

SPAN can be configured to capture either inbound, outbound or both directions of traffic. You can configure a SPAN source as either a specific port, a single port in an Ether channel group, an Ether channel group, or a VLAN. SPAN cannot be configured with a source port of a MEC (Multi chassis Ether channel). You also cannot configure a source of a single port and a VLAN. When configuring multiple sources for a SPAN session, you simply specify multiple source interfaces.

One thing to keep in mind when configuring SPAN is if you are using a source port that has a higher bandwidth than the destination port, some of the traffic if the link is congested, traffic will be dropped.

Simple Local SPAN Configuration

Consider the following diagram in which a Router (R1) is connected to Switch through Switch's Fast Ethernet port 0/1, this port is configured as the Source SPAN port. Traffic copied from FE0/1 is to be mirrored out FE0/24 where our monitoring workstation is waiting to capture the traffic.

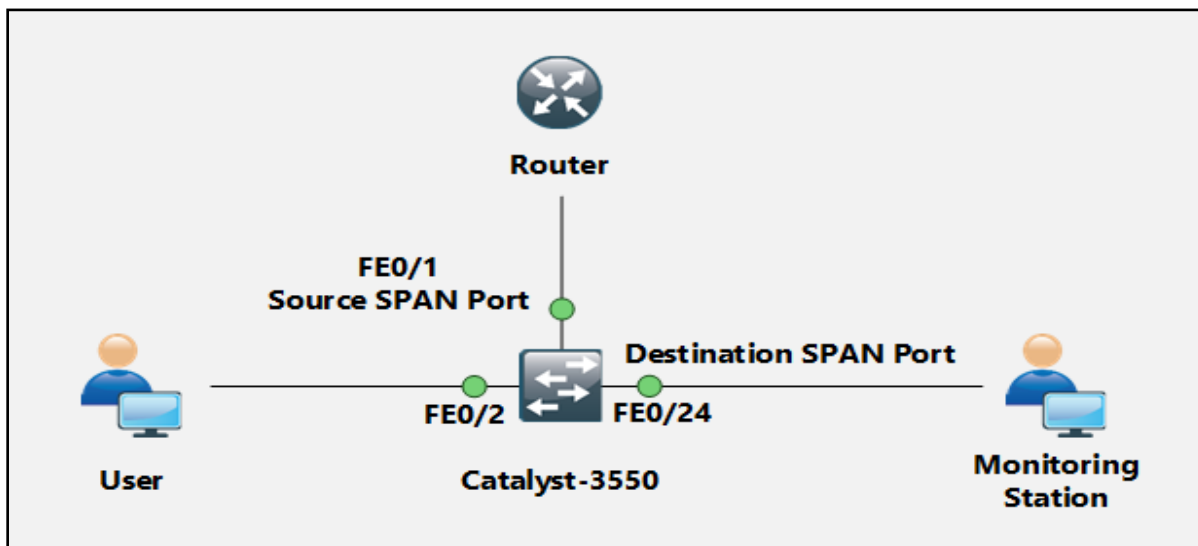


Figure 8-03 SPAN Port

Once we have our network analyzer is setup and running, the first step is to configure Fast Ethernet o/1 as a source SPAN port, configure Fast Ethernet o/24 as the destination SPAN port. After configuring both interfaces, destination's SPAN port LED (FEo/24) began flashing in synchronization with that of FEo/1's LED – an expected behavior considering all FEo/1 packets were being copied to FEo/24.

Wiretapping

Wiretapping is the process of gaining information by tapping the signal from wire such as telephone lines or the Internet. Mostly, wiretapping is performed by a third party to monitor the conversation. Wiretapping is basically electrical tap on the telephone line. Legal Wiretapping is called Legal Interception which is mostly performed by governmental or security agencies.

Wiretapping is classified into its two types: -

Active Wiretapping

Active Wiretapping is monitoring, recording of information by wiretapping, additionally active wiretapping includes alteration of the communication.

Passive Wiretapping

Monitoring and Recording the information by wiretapping without any alteration in communication.

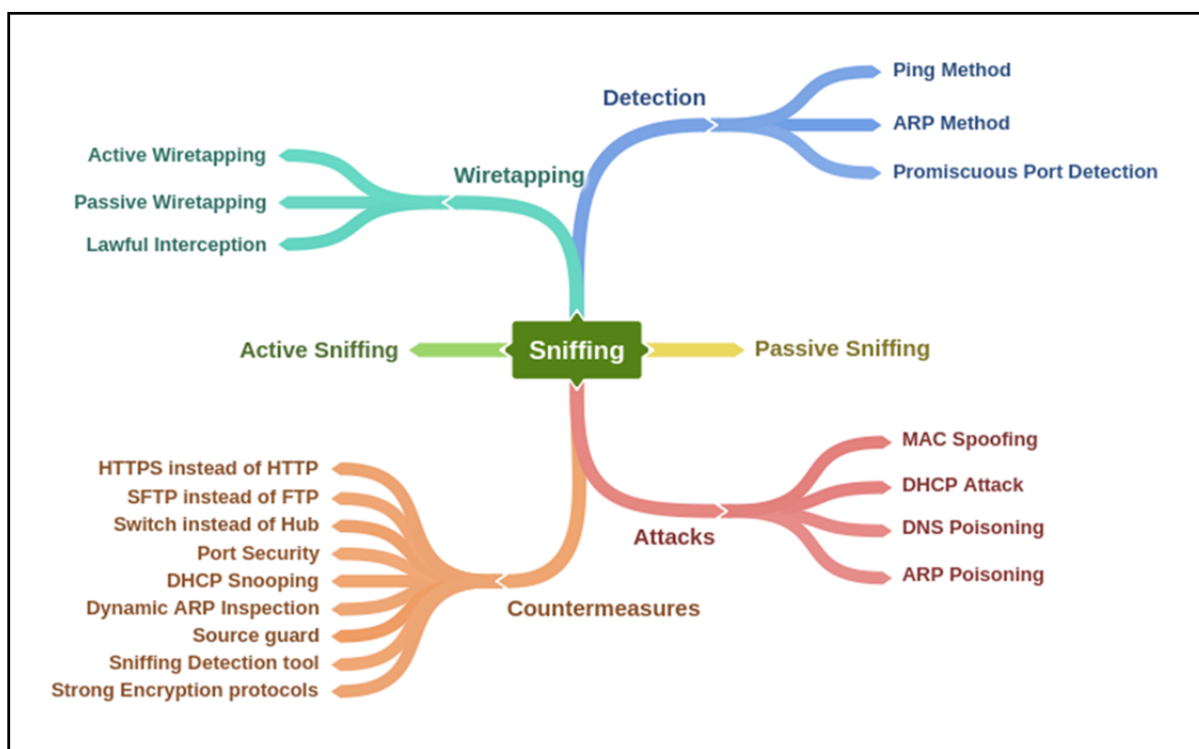
Lawful Interception

Lawful Interception (LI) is a process of wiretapping with legal authorization which allows law enforcement agencies to wiretap the communication of individual user selectively. Telecommunication standardization organization standardized the legal interception gateways for the interception of communication by agencies.

Planning Tool for Resource Integration (PRISM)

PRISM Planning Tool for Resource Integration stands for, Synchronization and Management. PRISM is a tool that is specially designed to collect information and process, passing through American servers. PRISM program is developed by Special Source Operation (SSO) division of National Security Agency (NSA). PRISM is intended for identification and monitoring of suspicious communication of target. Internet traffic routing through the US, or data stored on US servers are wiretap by NSA.

Mind Map



MAC Attacks

MAC Address Table / CAM Table

Media Access Control Address is in short known as MAC address or physical address of a device. MAC address is 48-bits unique identification number that is assigned to a network device for communication at data link layer. MAC address is comprised of Object Unique Identifier (QUI) 24-bits and 24-bits of Network Interface Controller (NIC). In case of multiple NIC, the device will have multiple unique MAC addresses.

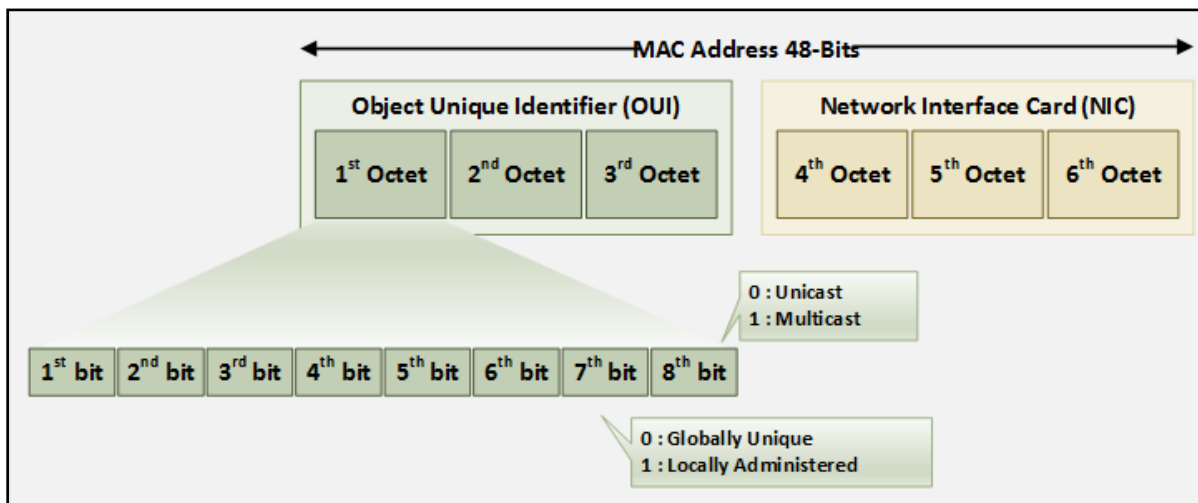


Figure 8-04 MAC-Address

MAC address table or Content-Addressable Memory (CAM) table is used in Ethernet switches to record MAC address, and its associated information which is used to forward packets. CAM table records a table in which each MAC address information such as associated VLAN information, learning type, and associated port parameters. These parameter helps at data-link layer to forward packets.

How Content Addressable Memory Works

To Learn the MAC address of devices is the fundamental responsibility of switches. The switch transparently observes incoming frames. It records the source MAC address of these frames in its MAC address table. It also records the specific port for the source MAC address. Based on this information, it can make intelligent frame forwarding (switching) decisions. Notice that a network machine could be turned off or moved at any point. As a result, the switch must also age MAC addresses and remove them from the table after they have not been seen for some duration.

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

Vlan	Mac Address	Type	Ports
1	e213.5864.ab8f	DYNAMIC	Gi0/0
1	fa16.3ee3.7d71	DYNAMIC	Gi1/0

Figure 8-05 MAC-Address Table

The switch supports multiple MAC addresses on all ports so we can connect individual workstation as well as multiple devices through switch or router as well. By the feature of

Dynamic Addressing, switch updates the source address received from the incoming packets and binds it to the interface from which it is received. As the devices are added or removed, they are updated dynamically. By default, aging time of MAC address is 300 seconds. The switch is configured to learn the MAC addresses dynamically by default.

MAC Flooding

MAC flooding is a technique in which attacker sends random mac addresses mapped with random IP to overflow the storage capacity of CAM table. As we know CAM table has its fixed length, switch then acts as a hub. It will now broadcast packet on all ports which help the attacker to sniff the packet with ease. For MAC Flooding, Unix / Linux utility “*macof*” offers MAC flooding. using *macof*, random source MAC and IP can be sent on an interface.

Switch Port Stealing

Switch port stealing is also a packet sniffing technique that uses MAC flooding to sniff the packets. In this technique, the attacker sends bogus ARP packet with the source MAC address of target and destination address of its own as the attacker is impersonating the target host let's say Host A. When this is forwarded to switch, the switch will update the CAM table. When Host A sends a packet, Switch will have to update it again. This will create the winning the race condition in which if the attacker sends ARP with Host A's MAC address, the switch will send packets to the attacker assuming Host A is connected to this port.

Defend against MAC Attacks

Port Security is used to bind the MAC address of known devices to the physical ports and violation action is also defined. So if an attacker tries to connect its PC or embedded device to the switch port, then it will shut down or restrict the attacker from even generating an attack. In dynamic port security, you configure the total number of allowed MAC addresses, and the switch will allow only that number simultaneously, without regard to what those MAC addresses are.

Configuring Port Security

Cisco Switch offers port security to prevent MAC attacks. You can configure the switch either for statically defined MAC Addresses only, or dynamic MAC learning up to the specified range, or you can configure port security with the combination of both as shown below. The following configuration on Cisco Switch will allow specific MAC address and 4 additional MAC addresses. If the switch has learned the static MAC address

Port Security Configuration

```
Switch(config)# interface ethernet o/o
```



```
Switch(config-if)#switchport mode access
Switch(config-if)# switchport port-security
//Enabling Port Security
Switch(config-if)# switchport port-security mac-address <mac-address>
//Adding static MAC address to be allowed on Ethernet 0/0
Switch(config-if)# switchport port-security maximum 4
//Configuring dynamic MAC addresses (maximum up to 4 MAC addresses) to be
allowed on Ethernet 0/0
Switch(config-if)# switchport port-security violation shutdown
//Configuring Violation action as shutdown
Switch(config-if)#exit
```

DHCP Attacks

Dynamic Host Configuration Protocol (DHCP) Operation

DHCP is the process of allocating the IP address dynamically so that these addresses are assigned automatically and also that they can be reused when hosts don't need them. Round Trip time is the measurement of time from discovery of DHCP server until obtaining the leased IP address. RTT can be used to determine the performance of DHCP. By using UDP broadcast, DHCP client sends an initial DHCP-Discover packet because it initially doesn't have network information to which they are connected. This DHCP-Discover packet is replied by DHCP server with DHCP-Offer Packet offering the configuration parameters. DHCP Client will send DHCP-Request packet destined for DHCP server for requesting for configuration parameters. Finally, DHCP Server will send the DHCP-Acknowledgement packet containing configuration parameters.

DHCPv4 uses two different ports:

- UDP port 67 for Server.
- UDP port 68 for Client.

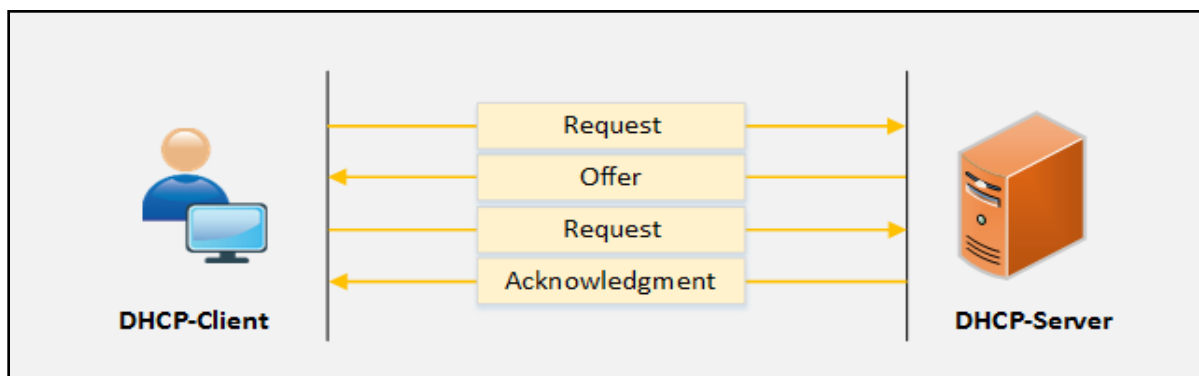
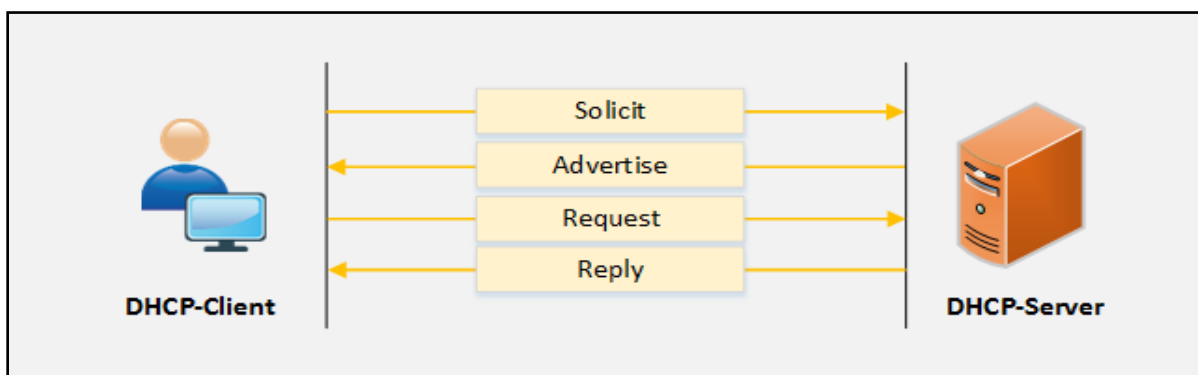


Figure 8-06 IPv4 DHCP process

DHCP Relay agent forwards the DHCP packets from server to client and Client to server. Relay agent helps the communication like forwarding request and replies between client and servers. Relay agent, when receiving a DHCP message, it generates a new DHCP request to send it out from another interface with including default gateway information as well as Relay-Agent information option (Option-82). When the Relay Agent gets the reply from the server, it removes the Option 82 and forwards it back to the client.

The working of Relay agent and DHCPv6 Server is same as the IPv4 Relay agent and DHCPv4 Server. DHCP server receives the request and assigns the IP address, DNS, Lease time and other necessary information to the client whereas relay server forwards the DHCP messages.

*Figure 8-07 IPv6 DHCP process*

DHCPv6 uses two different ports:

- UDP port 546 for clients.
- UDP port 547 for servers.

DHCP Starvation Attack

DHCP Starvation attack is a Denial-of-Service attack on DHCP server. In DHCP Starvation attack, Attacker sends bogus requests for broadcasting to DHCP server with spoofed MAC addresses to lease all IP addresses in DHCP address pool. Once, all IP addresses are allocated, upcoming users will be unable to obtain an IP address or renew the lease. DHCP Starvation attack can be performed by using tools such as “*Dhcpstarv*” or “*Yersinia*.”

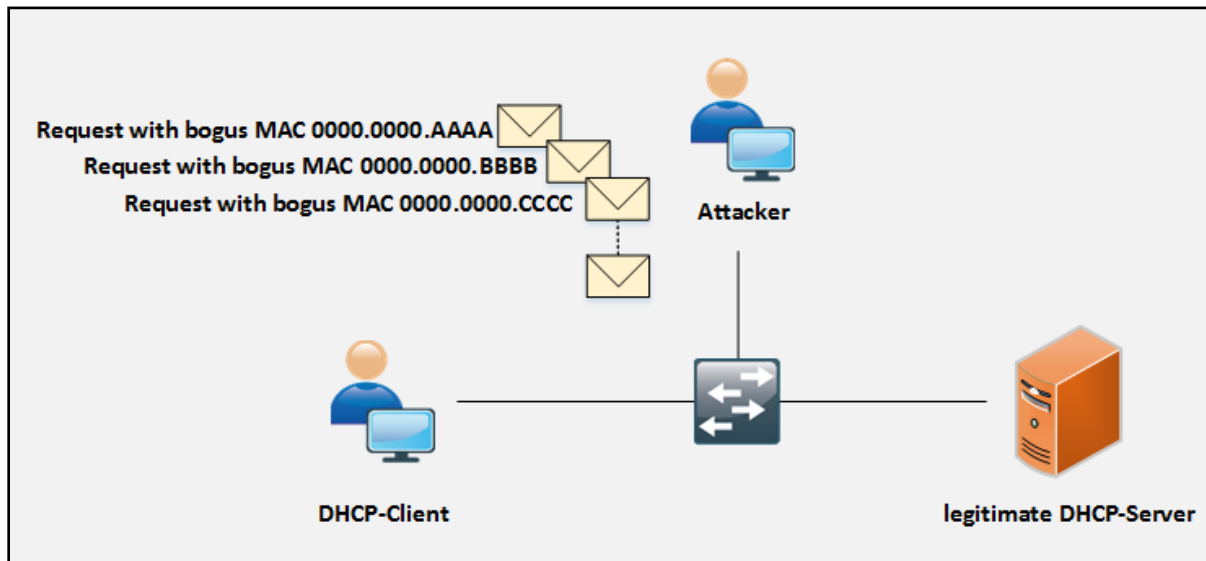


Figure 8-o8 DHCP Starvation Attack

Rogue DHCP Server Attack

Rogue DHCP Server attack is performed by deploying the rogue DHCP Server in the network along with the Starvation attack. When a legitimate DHCP server is in Denial-of-Service attacks, DHCP clients are unable to gain IP address from the legitimate DHCP server. Upcoming DHCP Discovery (IPv4) or Solicit (IPv6) packet are replied by bogus DHCP server with configuration parameter which directs the traffic towards it.

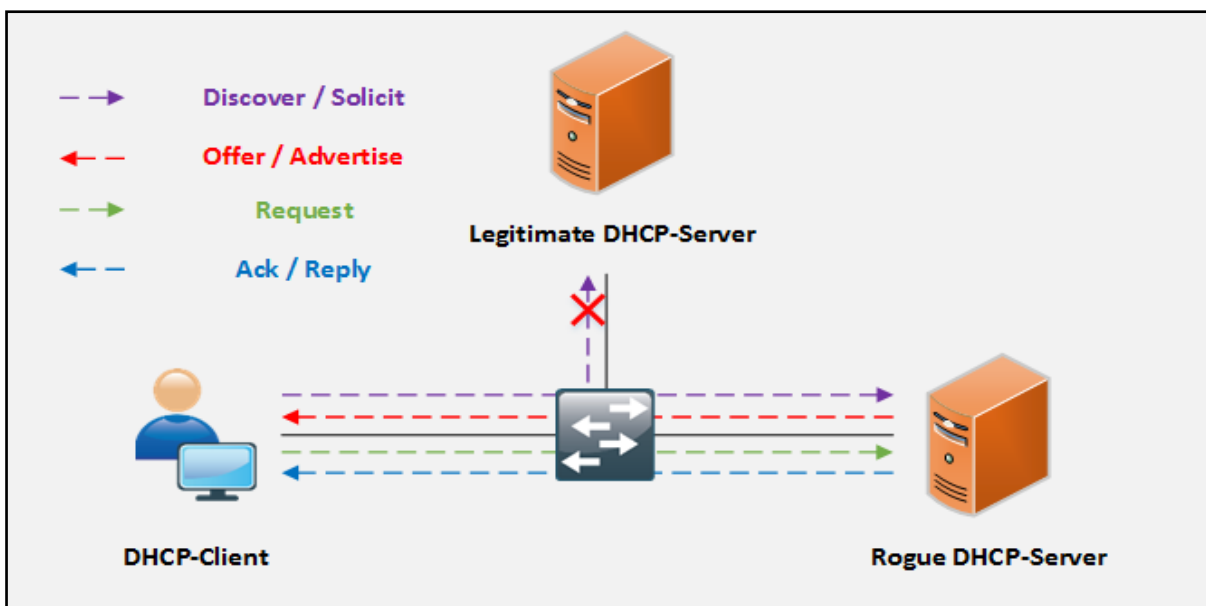


Figure 8-o9 Rogue DHCP Server Attack

Defending Against DHCP Starvation and Rogue Server Attack

DHCP Snooping

It is actually very easy for someone to accidentally or maliciously bring a DHCP server in a corporate environment. *DHCP snooping* is all about protecting against it. In order to mitigate such attacks, DHCP snooping feature is enabled on networking devices to identify the only trusted ports from DHCP traffic either in ingress or egress direction is considered legitimate. Any access port who tries to reply the DHCP requests will be ignored because the device will only allow DHCP process from the trusted port as defined by networking team. It is a security feature, which provides network security via filtering of untrusted DHCP messages and by building and maintaining a DHCP snooping binding database known as a DHCP snooping binding table. DHCP snooping differentiates between untrusted interfaces that are connected to the end user/host and trusted interfaces that are connected to the legitimate DHCP server or any trusted device.

Port Security

Enabling Port security will also mitigate these attack by limiting the learning of a maximum number of MAC addresses on a port, configuring violation action, aging time, etc.

ARP Poisoning

Address Resolution Protocol (ARP)

ARP is a stateless protocol that is used within a broadcast domain to ensure the communication by resolving the IP address to MAC address mapping. It is in charge of L3 to L2 address mappings. ARP protocol ensures the binding of IP addresses and MAC addresses. By broadcasting the ARP request with IP address, the switch can learn the associated MAC address information from the reply of the specific host. In the event that there is no map, or the map is unknown, the source will send a broadcast to all nodes. Just the node with a coordinating MAC address for that IP will answer to the demand with the packet that involves the MAC address mapping. The switch will learn the MAC address and its connected port information into its fixed length CAM table.

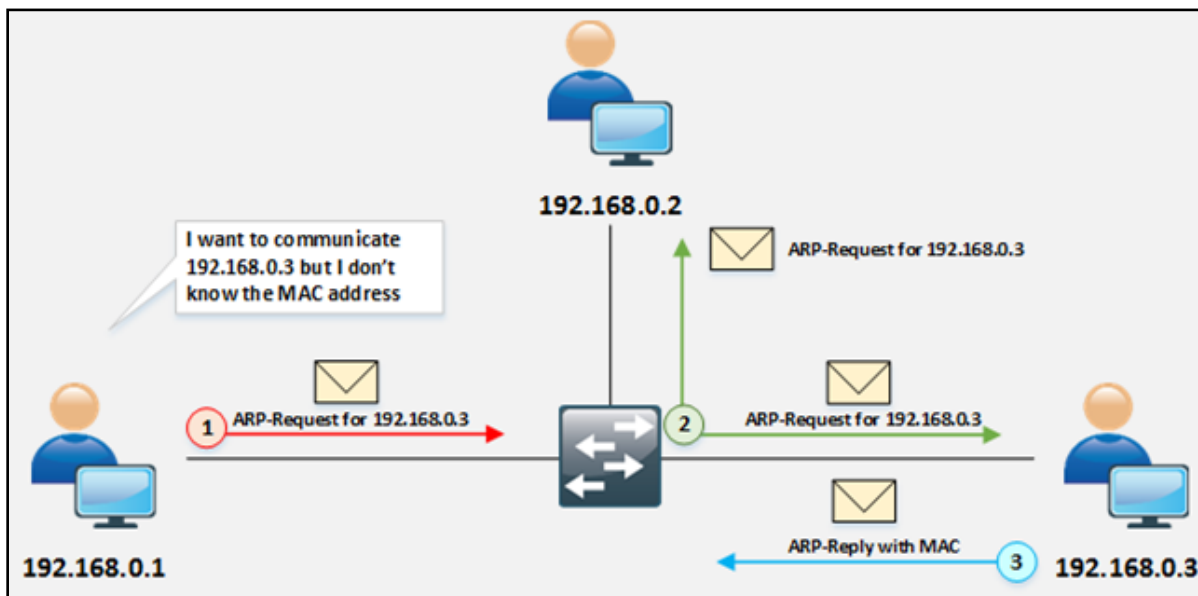


Figure 8-10 ARP Operation

As shown in the figure, the source generates the ARP query by broadcasting the ARP packet. A node having the MAC address, the query is destined for, will reply only to the packet. The frame is flooded out all ports (other than the port on which the frame was received) if CAM table entries are full. This also happens when the destination MAC address in the frame is the broadcast address. MAC flooding technique is used to turn a switch into a hub in which switch starts broadcasting each and every packet. In this scenario, each user can catch the packet even those packets which is not intended for.

ARP Spoofing Attack

In ARP spoofing, Attacker sends forged ARP packets over Local Area Network (LAN). In the case, Switch will update the attacker's MAC Address with the IP address of a legitimate user or server. Once attacker's MAC address is learned with the IP address of a legitimate user, the switch will start forwarding the packets to attacker intending that it is the MAC of the user. Using ARP Spoofing attack, an attacker can steal information by extracting from the packet received intended for a user over LAN. Apart from stealing information, ARP spoofing can be used for: -

- Session Hijacking
- Denial-of-Service Attack
- Man-in-the-Middle Attack
- Packet Sniffing
- Data Interception
- Connection Hijacking
- VoIP tapping
- Connection Resetting

- Stealing Password

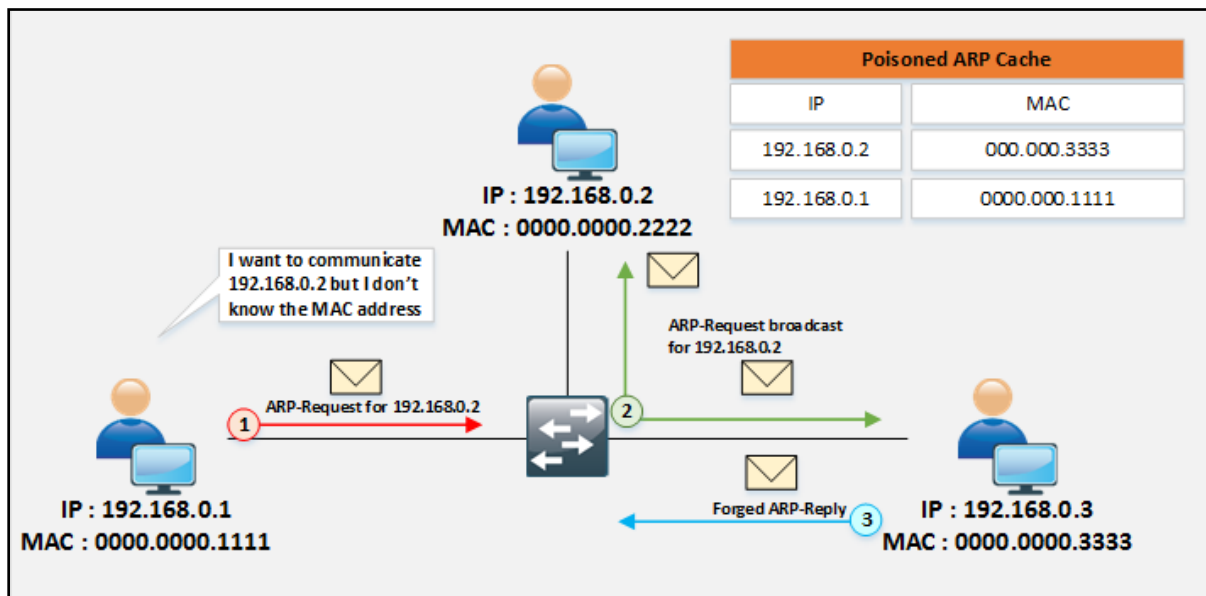


Figure 8-11 ARP Spoofing Attack

Defending ARP Poisoning

Dynamic ARP Inspection (DAI)

DAI is used with DHCP snooping, IP-to-MAC bindings can be a track from DHCP transactions to protect against ARP poisoning (which is an attacker trying to get your traffic instead of to your destination). DHCP snooping is required in order to build the MAC-to-IP bindings for DAI validation.

Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches

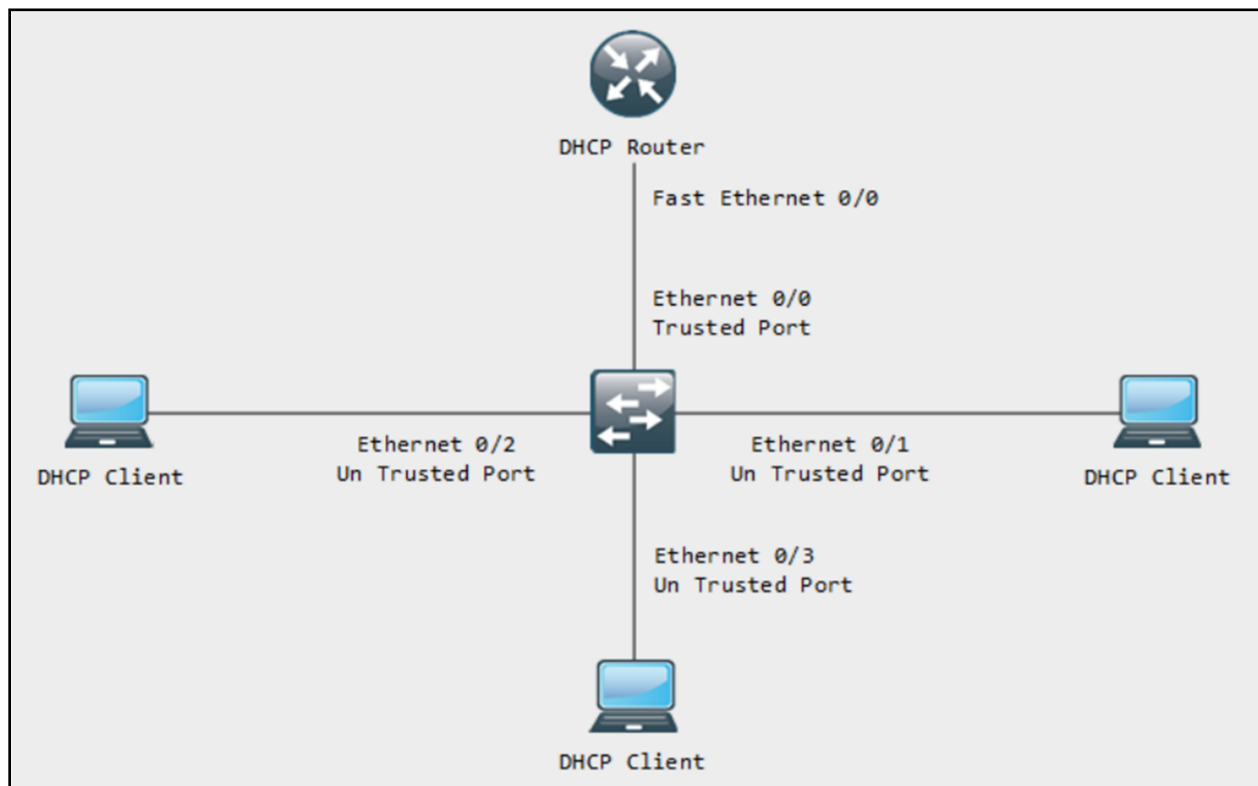


Figure 8-12 Configuring DHCP Snooping

Configuration:

```
Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1

Switch(config)#int eth 0/0
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#ex
Switch(config)#

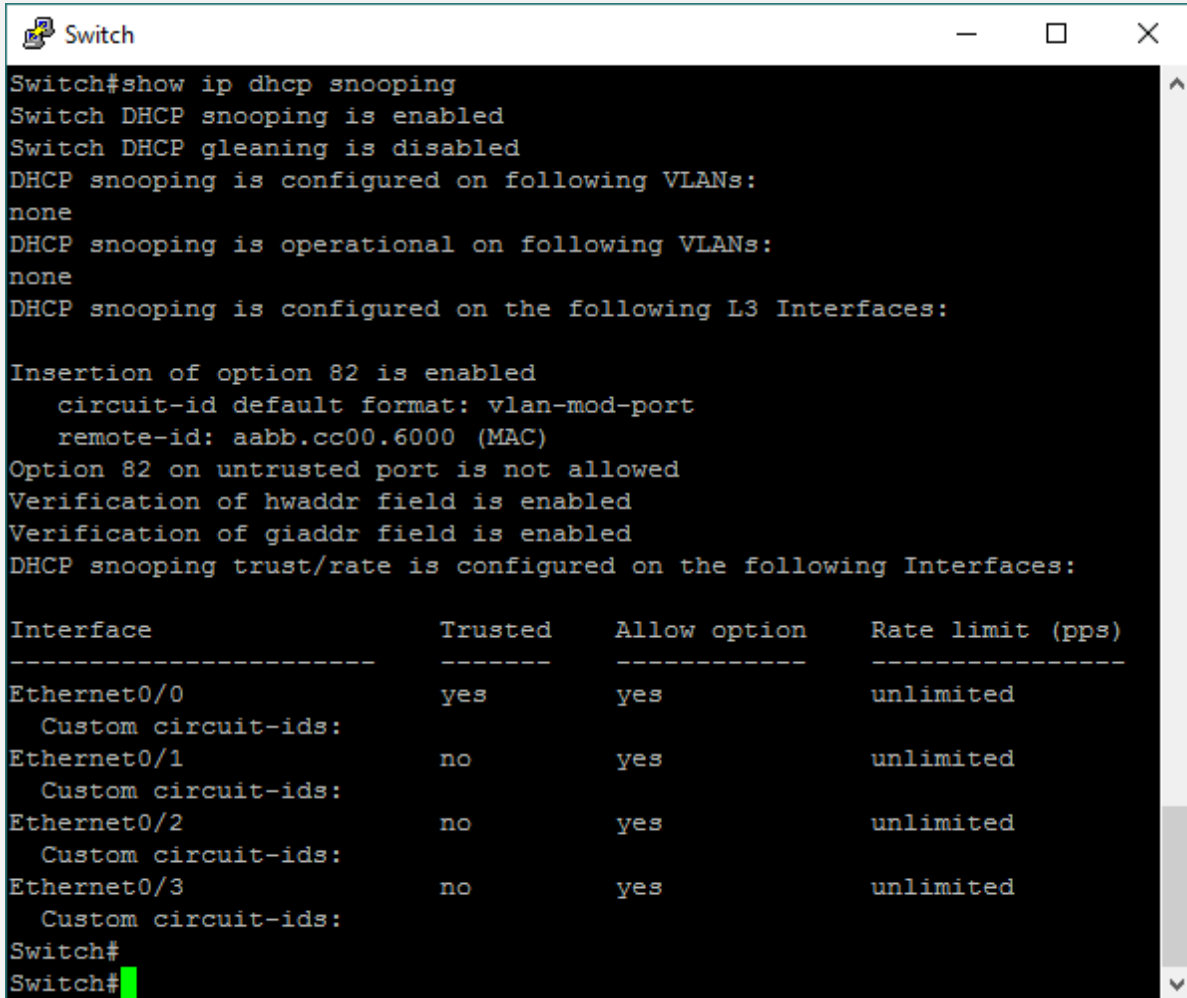
Switch(config)#int eth 0/1
Switch(config-if)#ip dhcp snooping information option allow-untrusted

Switch(config)#int eth 0/2
Switch(config-if)#ip dhcp snooping information option allow-untrusted
```

```
Switch(config)#int eth 0/3
Switch(config-if)#ip dhcp snooping information option allow-untrusted
```

Verification:

Switch# show ip dhcp snooping



```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
none
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: aabb.cc00.6000 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
```

Interface	Trusted	Allow option	Rate limit (pps)
Ethernet0/0	yes	yes	unlimited
Ethernet0/1	no	yes	unlimited
Ethernet0/2	no	yes	unlimited
Ethernet0/3	no	yes	unlimited

```
Switch#
Switch#
```

Figure 8-13 Verifying DHCP Snooping

Showing trusted and Untrusted Interfaces along with Allow Options.

Configuring Dynamic ARP Inspection

```
Switch(config)# ip arp inspection vlan <vlan number>
```

Verification Command: -

```
Switch(config)# do show ip arp inspection
```


Spoofing Attack

MAC Spoofing/Duplicating

MAC Spoofing is a technique of manipulating MAC address to impersonate the legitimate user or launch attack such as Denial-of-Service attack. As we know, MAC address is built-in on Network interface controller which cannot be changed, but some drivers allow to change the MAC address. This masking process of MAC address is known as MAC Spoofing. Attacker sniffs the MAC address of users which are active on switch ports and duplicate the MAC address. Duplicating the MAC can intercept the traffic and traffic destined to the legitimate user may direct to the attacker.

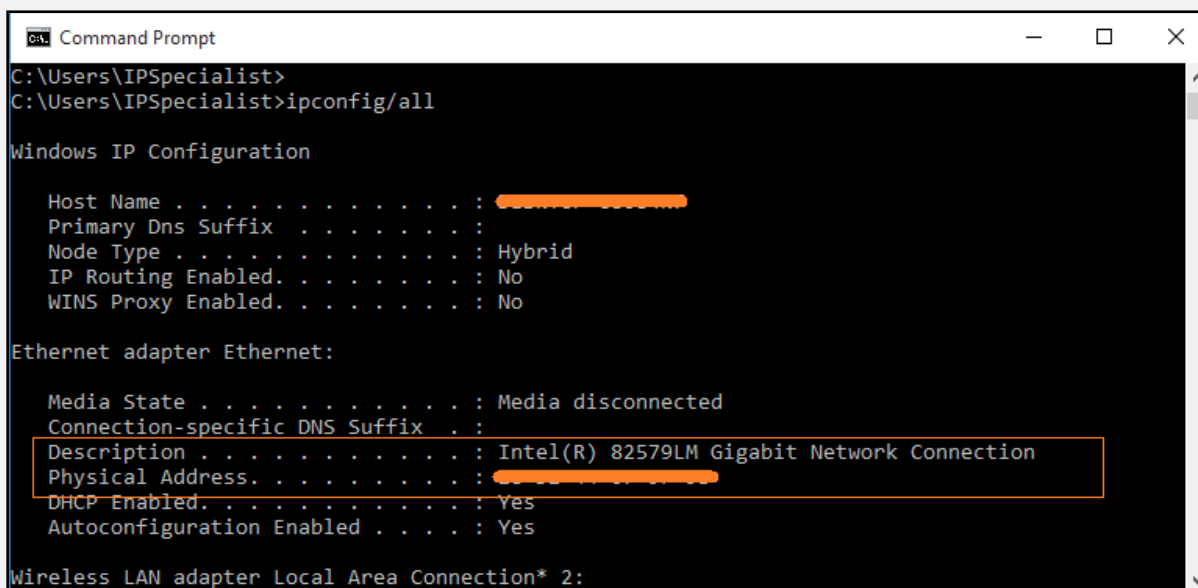
Lab 8-1: Configuring locally administered MAC address

Procedure:

1. Go to Command Prompt and type the command

C:\> ipconfig/all

Observe the MAC address currently used by the network adapter.



```
Command Prompt
C:\Users\IPSpecialist>
C:\Users\IPSpecialist>ipconfig/all

Windows IP Configuration

Host Name . . . . . : 
Primary Dns Suffix . . . . . : 
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) 82579LM Gigabit Network Connection
Physical Address. . . . . : 
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:
```

Figure 8-14 Finding MAC Address

2. Go to **Control Panel** and Click **Hardware and Sounds**

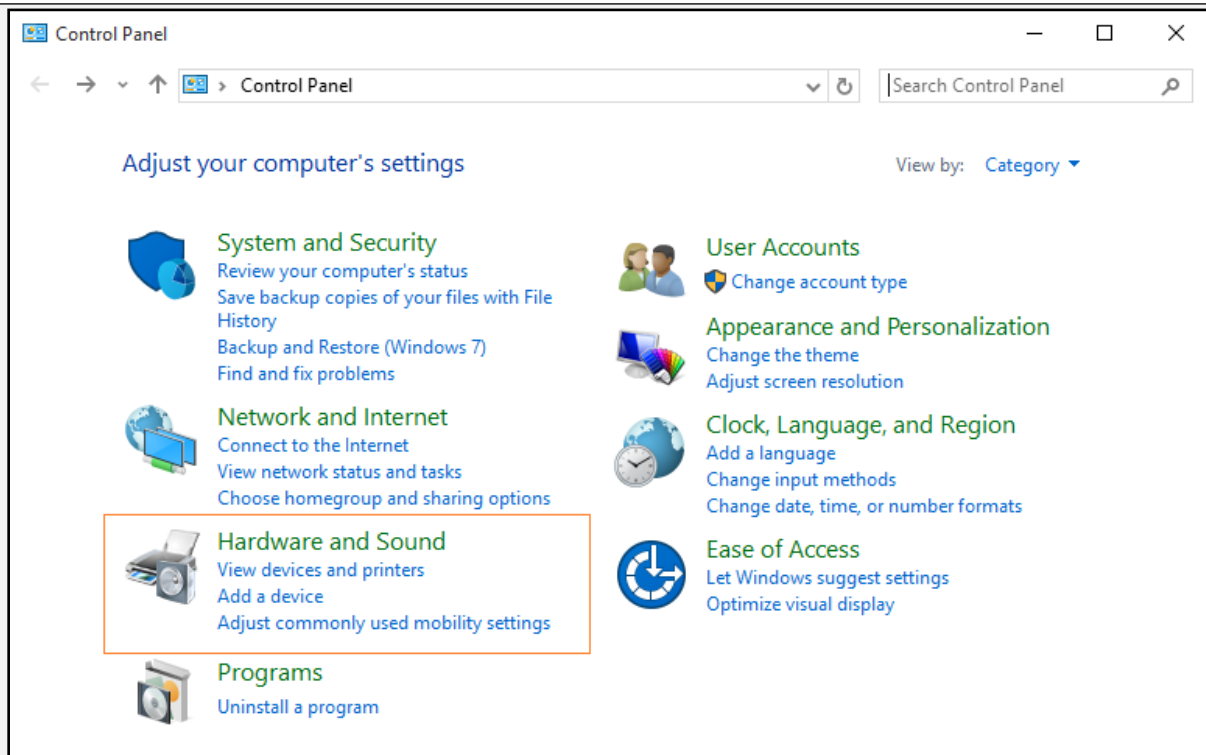


Figure 8-15 Control Panel

3. Click *Device Manager*

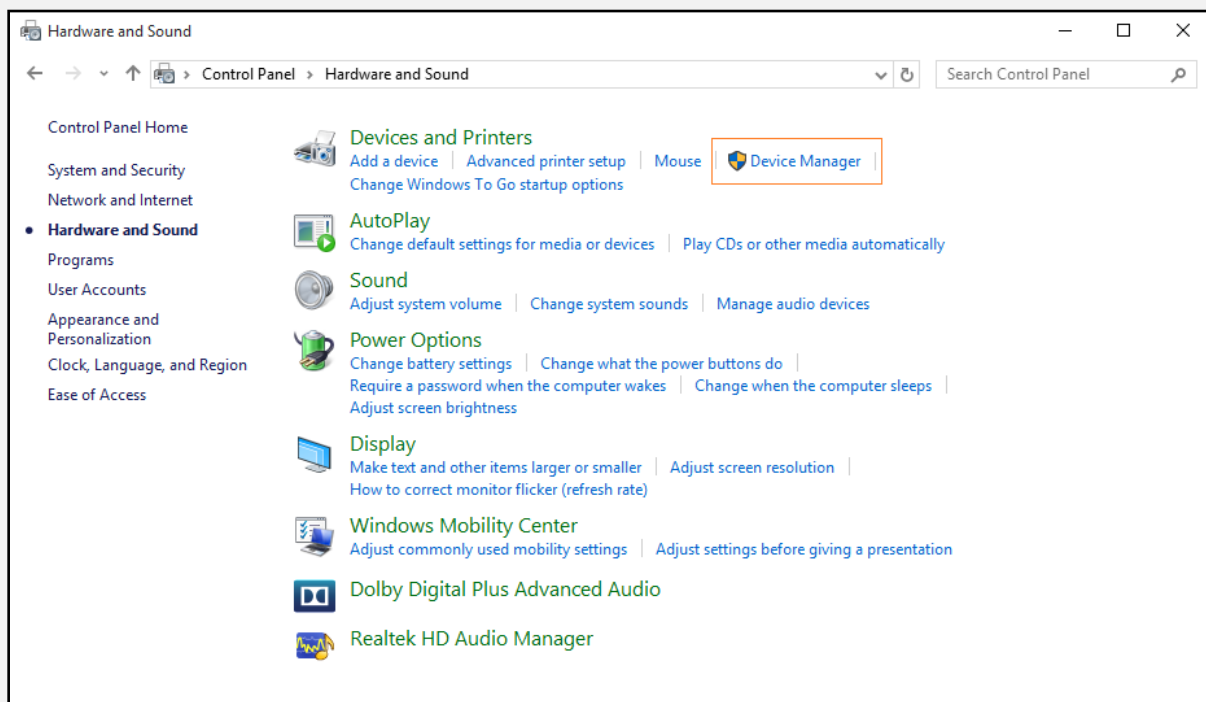


Figure 8-16 Hardware and Sounds

4. Select your Network Adapter

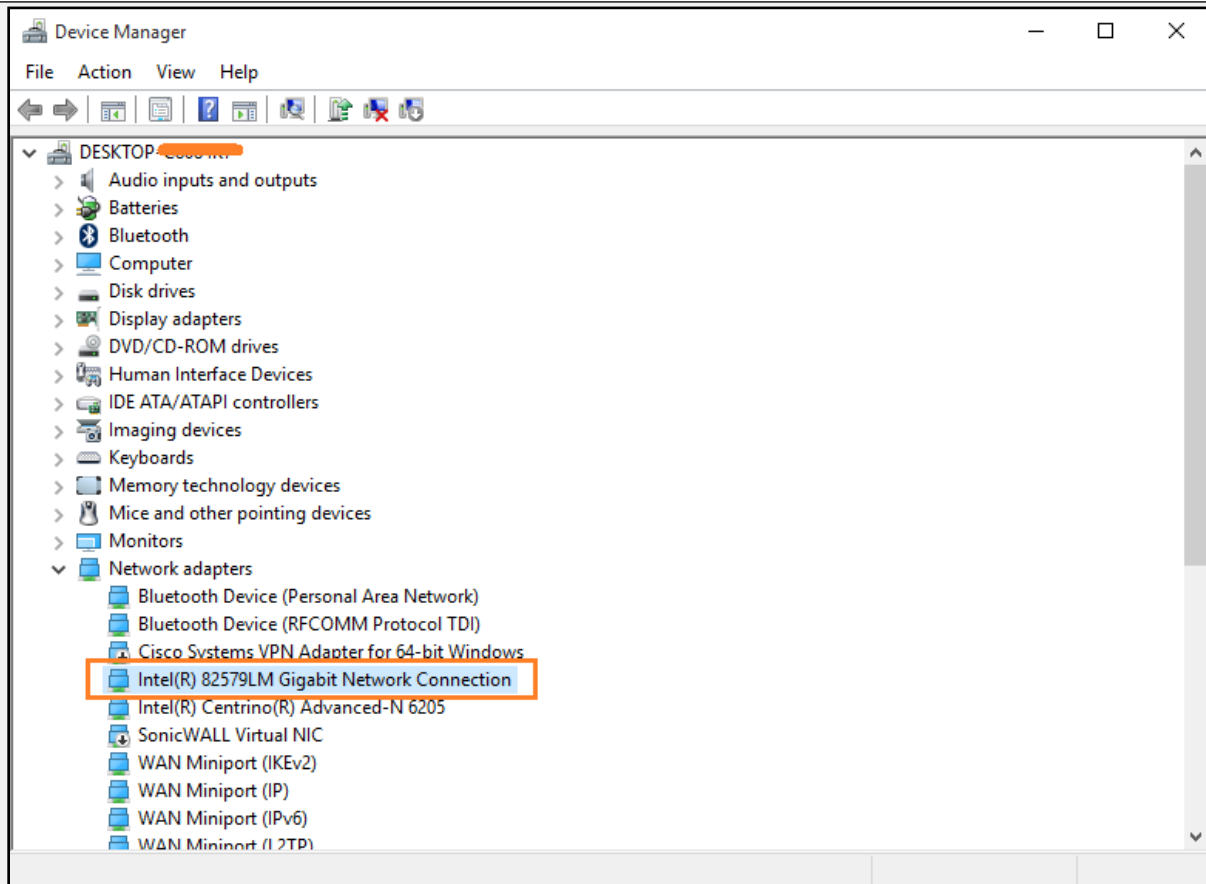


Figure 8-17 Device Manager

5. Right-Click on the desired Network Adapter and click **Properties**

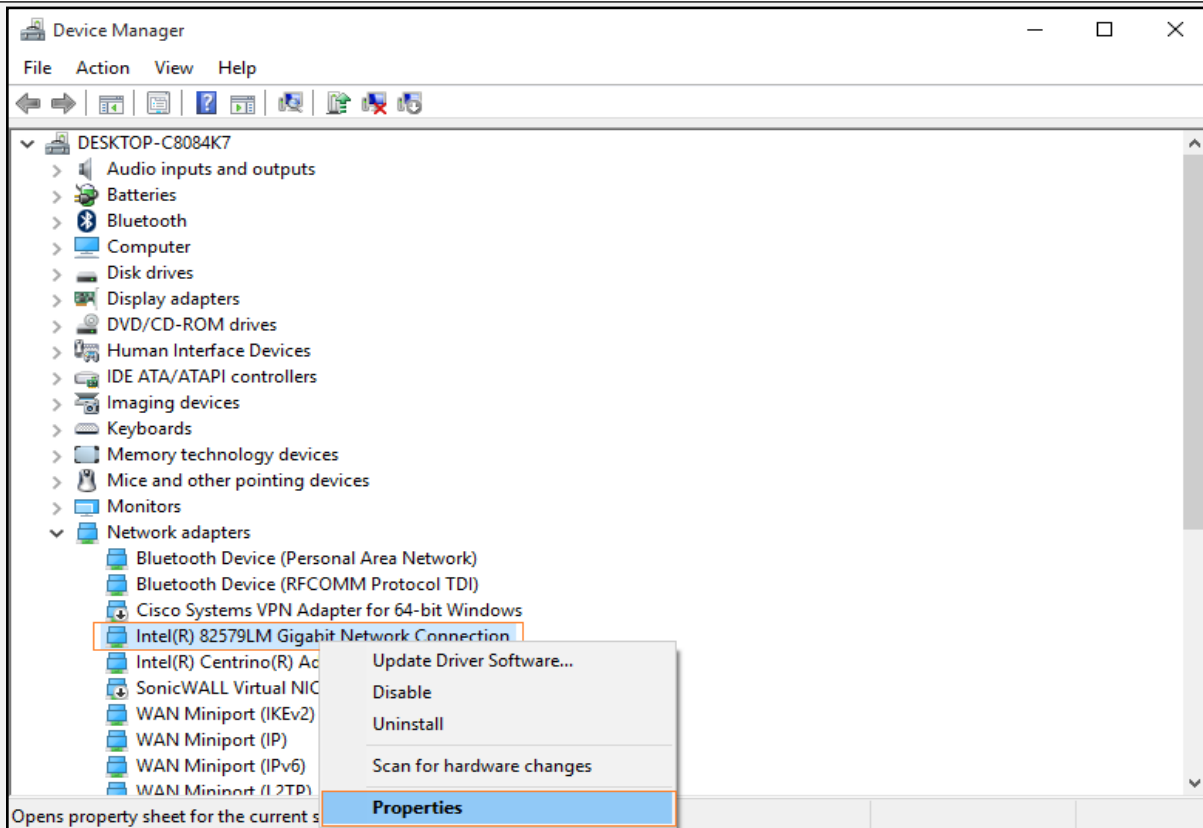


Figure 8-18 Network Adapters

6. Click **Advanced**
7. Select **Locally Administered Address**
8. Type a **MAC address**

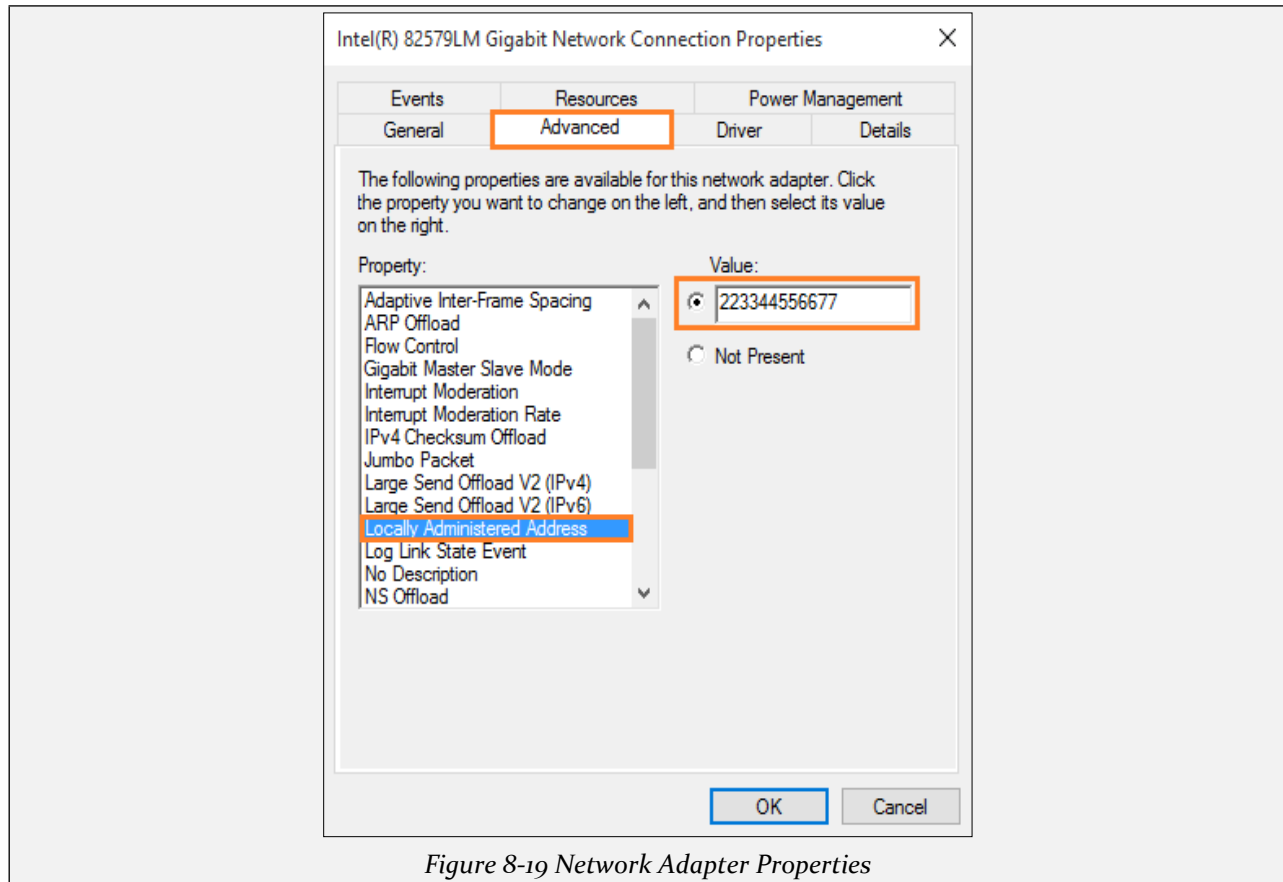


Figure 8-19 Network Adapter Properties

Verification

To verify, go to Command Prompt and type the following command

```
C:\> ipconfig/all
```

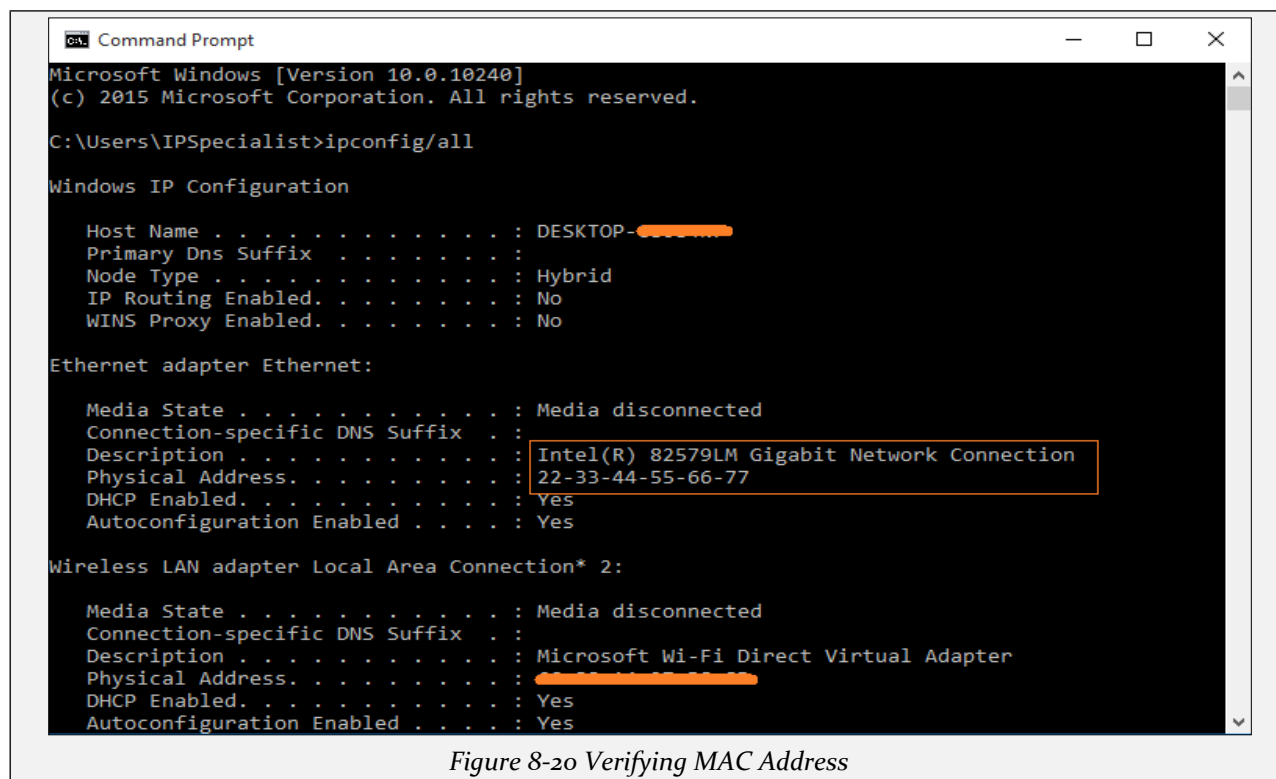


Figure 8-20 Verifying MAC Address

MAC Spoofing Tool

There several tools available which offer MAC spoofing with ease. Popular tools are: -

- Technitium MAC address Changer
- SMAC

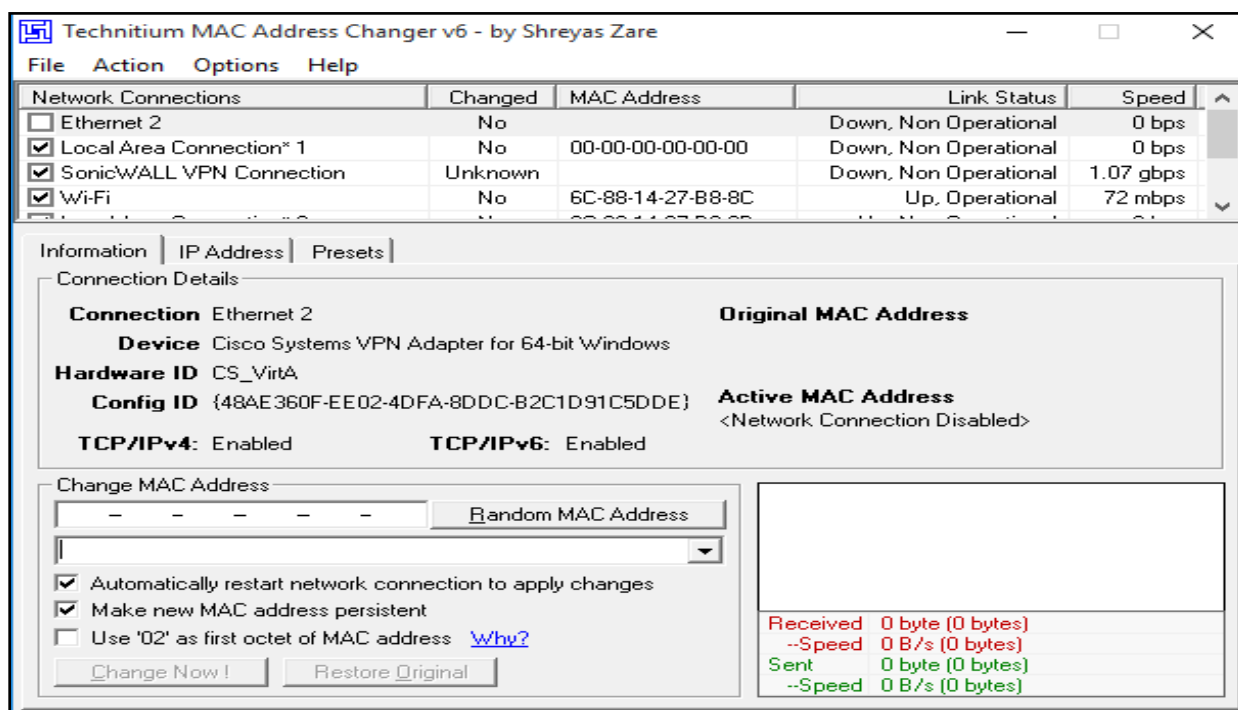


Figure 8-21 Technitium MAC Address Changer

How to Defend Against MAC Spoofing

In order to defend against MAC spoofing, DHCP Snooping, Dynamic ARP inspection are effective techniques to mitigate MAC spoofing attacks. Additionally, Source guard feature is configured on client facing Switch ports.

IP source guard is a port-based feature which provides Source IP address filtering at Layer 2. Source guard feature monitors and prevents the host from impersonating another host by assuming the legitimate host's IP address. In this way, the malicious host is restricted to use its assigned IP address. Source guard uses dynamic DHCP snooping or static IP source binding to match IP addresses to hosts on untrusted Layer 2 access ports.

Initially, all type of inbound IP traffic from the protected port is blocked except for DHCP packets. When a client receives an IP address from the DHCP server, or static IP source binding by the administrator, the traffic with an assigned source IP address is permitted from that port. All bogus packets will be denied. In this way, Source guard protects from the attack by claiming a neighbor host's IP address. Source guard creates an implicit port access control list (PACL).

DNS Poisoning

DNS Poisoning Techniques

Domain Name System (DNS) is used in networking to translate human-readable domain names into IP address. When a DNS server receives a request, it doesn't have the entry, it generates the query to another DNS server for the translation and so on. DNS server having the translation will reply to a request to the requesting DNS server, and then the client's query is resolved.

In case, when a DNS server receives a false entry, it updates its database. As we know, to increase performance, DNS servers maintain a cache in which this entry is updated to provide quick resolution of queries. This false entry causing poison in DNS translation continues until the cache expires. DNS poisoning is performed by attackers to direct the traffic toward the servers and computer owned or controlled by attackers.

Intranet DNS Spoofing

Intranet DNS Spoofing is normally performed over Local Area Network (LAN) with Switched Network. The attacker, with the help of ARP poisoning technique, performs Intranet DNS spoofing. Attacker sniff the packet, extract the ID of DNS requests and reply with the fake IP translation directing the traffic to the malicious site. The attacker must be quick enough to respond before the legitimate DNS server resolve the query.

Internet DNS Spoofing

Internet DNS Spoofing is performed by replacing the DNS configuration on the target machine. All DNS queries will be directed to a malicious DNS server controlled by the

attacker, directing the traffic to malicious sites. Usually, Internet DNS spoofing is performed by deploying a Trojan or infecting the target and altering the DNS configuration to direct the queries toward them.

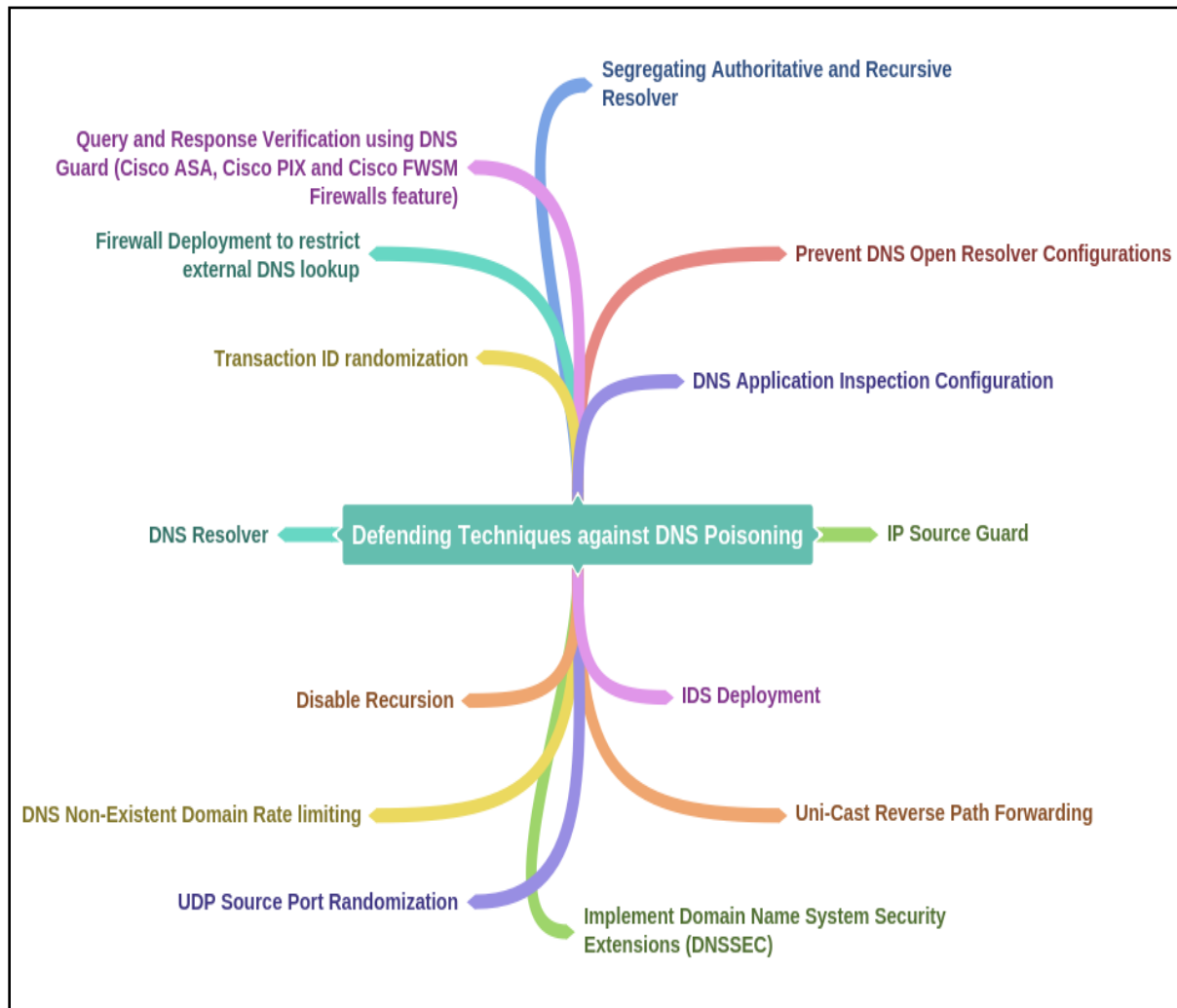
Proxy Server DNS Poisoning

Similar to Internet DNS Spoofing, Proxy Server DNS poisoning is performed by replacing the DNS configuration from the web browser of a target. All web queries will be directed to a malicious proxy server controlled by the attacker, redirecting the traffic to malicious sites.

DNS Cache Poisoning

As we know, Normally, Internet users are using DNS provided by the Internet Service Provider (ISP). In a corporate network, the organization uses their own DNS servers to improve performance by caching frequently or previously generated queries. DNS Cache poisoning is performed by exploiting flaws in DNS software. Attacker adds or alters the entries in DNS record cache which redirect the traffic to the malicious site. When an Internal DNS server is unable to validate the DNS response from authoritative DNS server, it updates the entry locally to entertain the user requests.

How to Defend Against DNS Spoofing



Sniffing Tools

Wireshark

Wireshark is the most popular, widely used Network Protocol Analyzer tool across commercial, governmental, non-profit and educational organizations. It is a free, open source tool available for Windows, Linux, MAC, BSD, Solaris and other platforms natively. Wireshark also offers a terminal version called “**TShark**.”

Lab 8-2: Introduction to Wireshark

Procedure:

Open Wireshark to capture the packets

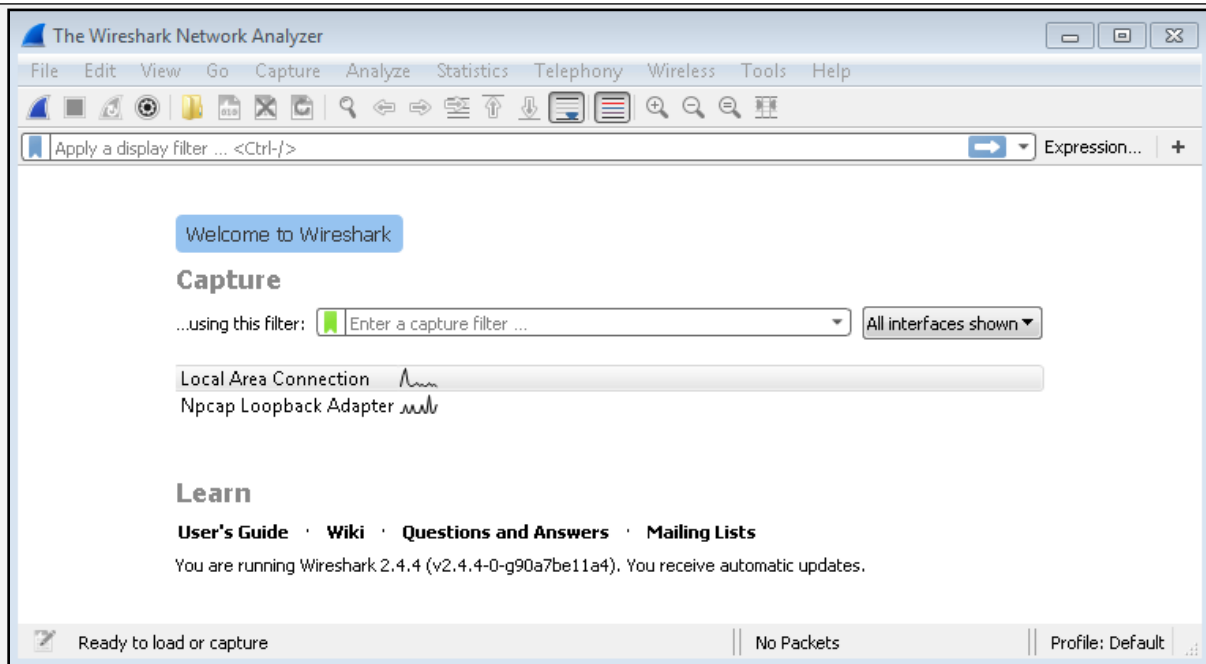


Figure 8-22 Wireshark Network Analyzer

Click **Capture > Options** to edit capture options.

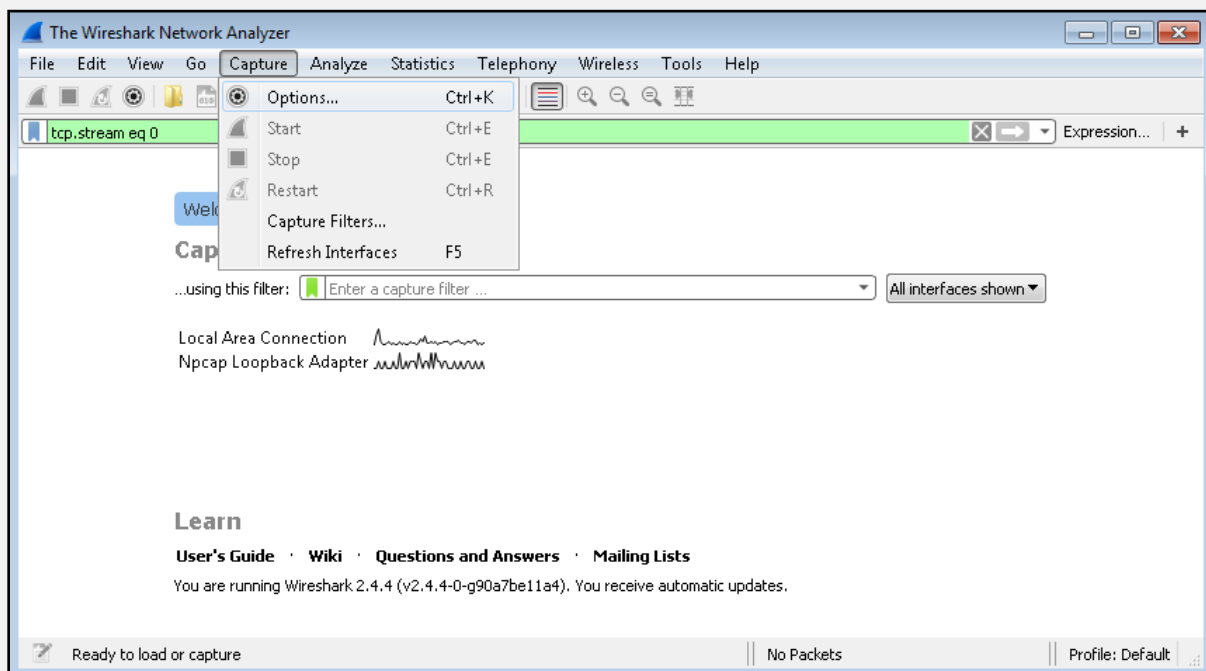


Figure 8-23 Wireshark Network Analyzer

Here, you can enable or disable promiscuous mode on an Interface. Configure the Capture Filter and Click **Start** button.

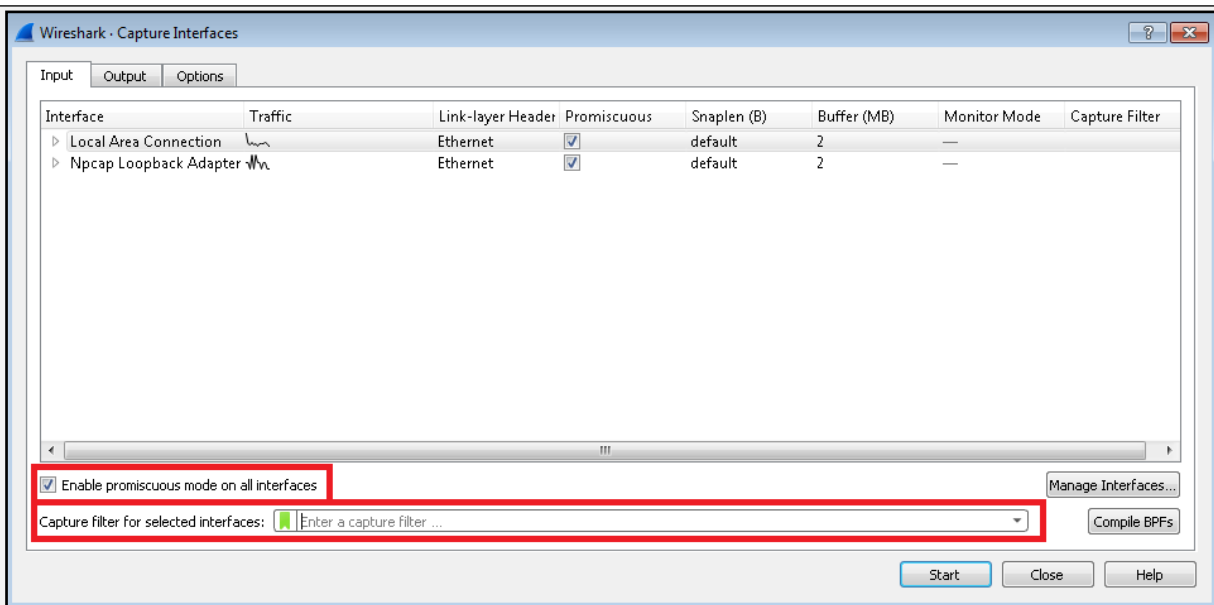


Figure 8-24 Wireshark Network Analyzer

Click **Capture > Capture Filter** to select Defined Filters. You can add the Filter by Clicking the Add/button below.

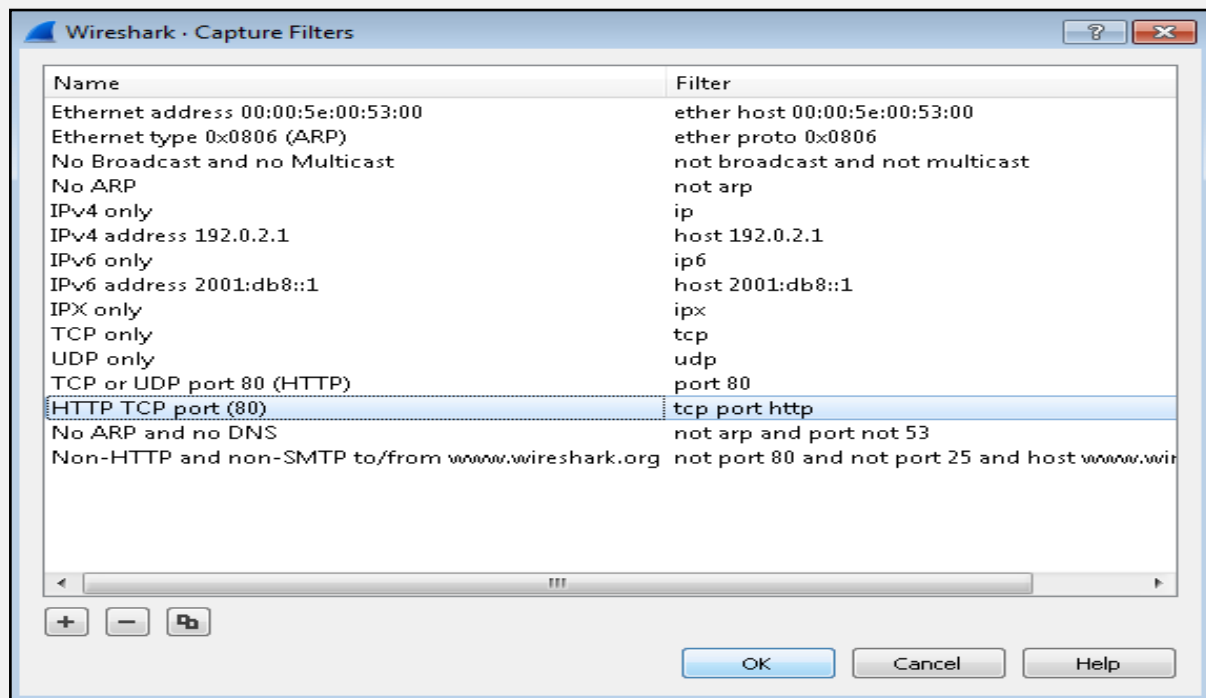


Figure 8-25 Wireshark Network Analyzer

Follow TCP Stream in Wireshark

Working on TCP based protocols can be very helpful by using Follow TCP stream feature. To examine the data from a TCP stream in the way that the application layer sees it. Perhaps you are looking for passwords in a Telnet stream.

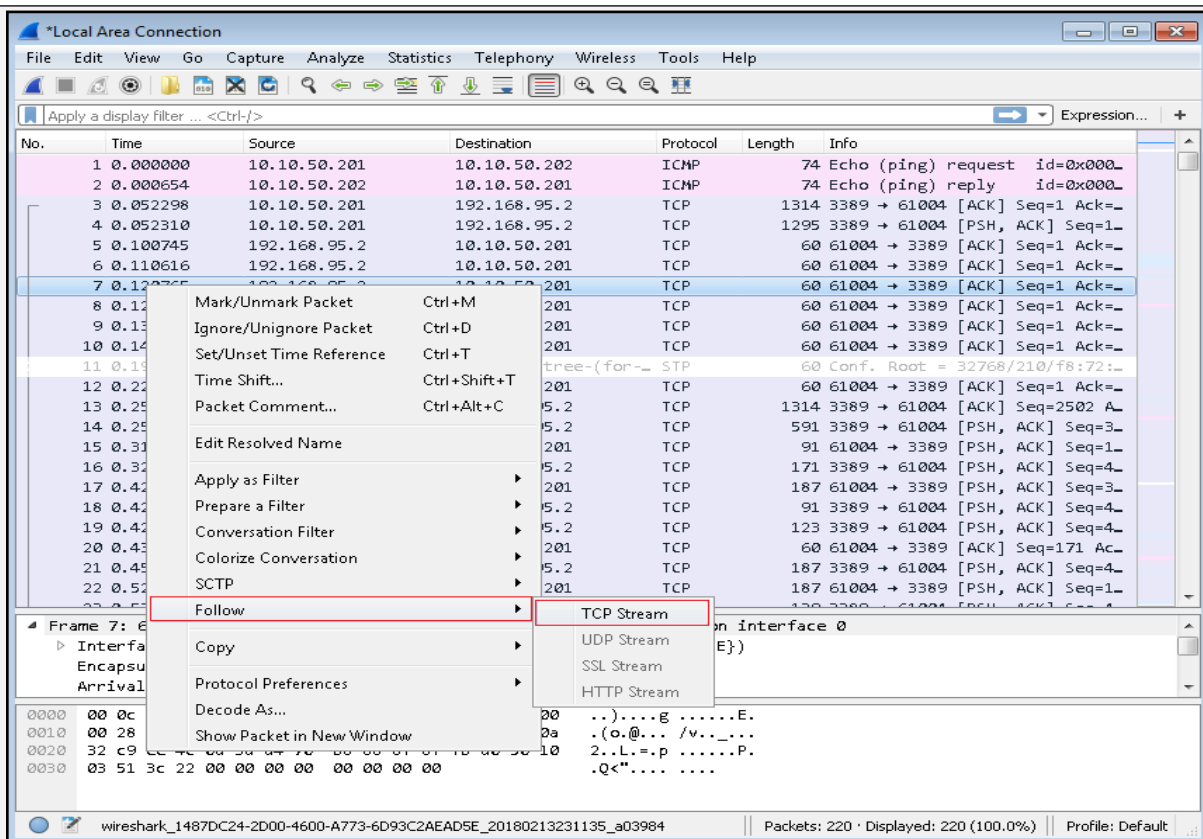


Figure 8-26 Wireshark Network Analyzer

Examine the data from the captured packet as shown below

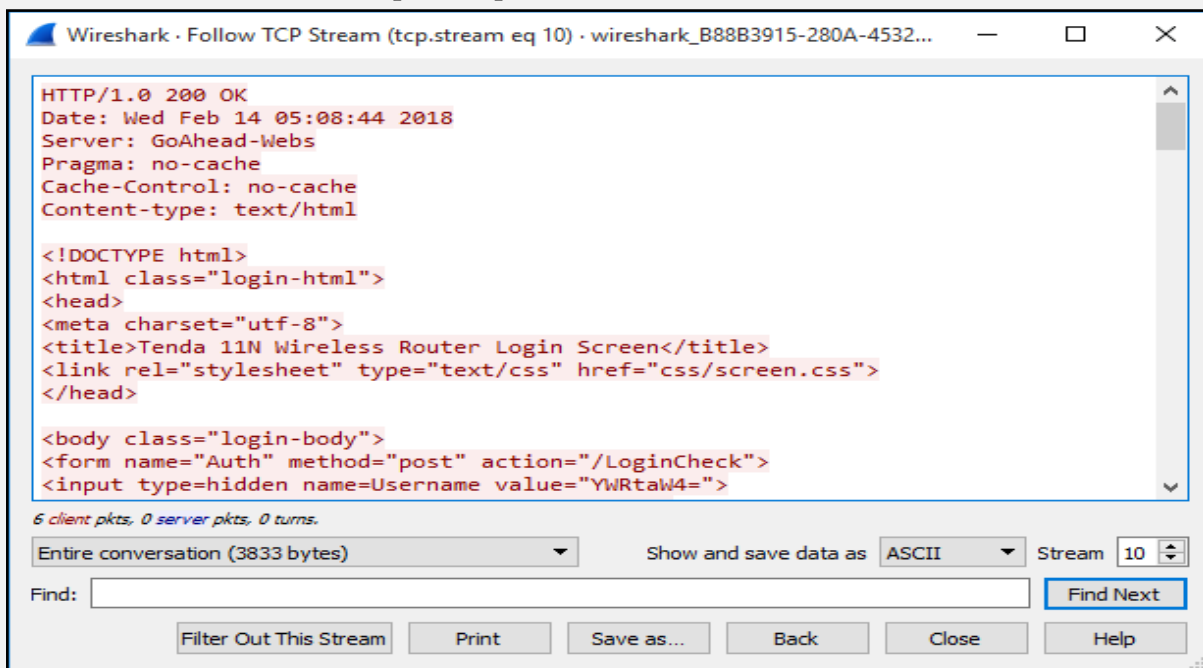


Figure 8-27 Wireshark Network Analyzer

Filters in Wireshark

The following are the filters of Wireshark to filter the output.

Operator	Function	Example
==	Equal	ip.addr == 192.168.1.1
eq	Equal	tcp.port eq 23
!=	Not equal	ip.addr != 192.168.1.1
ne	Not equal	ip.src ne 192.168.1.1
contains	Contains specified value	http contains "http://www.ipspecialist.net"

Table 8-01 Wireshark Filters

Countermeasures

Defending Against Sniffing

Best practice against Sniffing includes the following approaches to protect the network traffic.

- Using HTTPS instead of HTTP
- Using SFTP instead of FTP
- Use Switch instead of Hub
- Configure Port Security
- Configure DHCP Snooping
- Configure Dynamic ARP Inspection
- Configure Source guard
- Use Sniffing Detection tool to detect NIC functioning in a promiscuous mode
- Use Strong Encryption protocols

Sniffing Detection Techniques

Sniffer Detection Technique

Ping Method

Ping technique is used to detect sniffer. A ping request is sent to the suspect IP address with spoofed MAC address. If the NIC is not running in promiscuous mode, it will not respond to the packet. In case, if the suspect is running a sniffer, it responds the packet. This is an older technique and not reliable.

ARP Method

Using ARP, Sniffers can be detected with the help of ARP Cache. By sending a non-broadcast ARP packet to the suspect, MAC address will be cached if the NIC is running in promiscuous mode. Next step is to send a broadcast ping with spoofed MAC address. If the machine is running promiscuous mode, it will be able to reply the packet only as it has already learned the Actual MAC from the sniffed Non-broadcast ARP packet.

Promiscuous Detection Tool

Promiscuous Detection tools such as ***PromqryUI*** or ***Nmap*** can also be used for detection of Network Interface Card running in Promiscuous Mode. These tools are GUI based application software.