

7. _____ is used to bind malicious program while creating Trojan. A. Dropper

B. Wrapper

C. Crypter

D. Sniffer

8. _____ is used to drop malicious program at the target.

A. Dropper

B. Wrapper

C. Crypter

D. Sniffer

Chapter 8: Sniffing

Technology Brief

This chapter focuses on the concepts of Sniffing. By sniffing, you can monitor all sorts of traffic, either protected or unprotected. Using sniffing, an attacker can gain information that might be helpful for further attacks and can cause trouble for the victim. Furthermore, in this chapter, you will learn about Media Access Control (MAC) Attacks, Dynamic Host Configuration Protocol (DHCP) Attacks, Address Resolution Protocol (ARP) Poisoning, MAC Spoofing Attack, and DNS Poisoning. Once you are 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 networks and troubleshooting issues.

Sniffing Concepts

Introduction to Sniffing

Sniffing is the process of scanning and monitoring captured data packets passing through a network by using sniffers. The process of sniffing is carried out by using Promiscuous Ports. Enabling promiscuous mode function on the connected network interface allows capturing all traffic, even when the 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

Through sniffing, an attacker can capture packets like Syslog traffic, DNS traffic, Web traffic, email, and other types of data flowing across the network. By capturing these packets, an attacker can reveal information such as data, username, and passwords from protocols like HTTP, POP, IMAP, SMTP, NMTP, FTP, Telnet, and Rlogin, and other information. Anyone within the LAN or connected remotely can sniff the packets. Let's focus on how sniffers perform their actions and what can be achieved through sniffing.

The 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 turn the Network Interface Card (NIC) of the attacker's system into promiscuous mode, the attacker captures the packet. Promiscuous mode is a mode of the interface in which the NIC responds to every packet it receives. As you can observe in Figure 8-01, the attacker connected in promiscuous mode accepts each packet, even those packets that are not intended for him. Once the attacker captures the packets, he can decrypt these packets to extract information. The fundamental concept behind this technique is that if you are connected to a target network through a switch, broadcast and multicast traffic is forwarded on all ports. Switch forwards the unicast packet to the specific port where the actual host is connected. Switch maintains its MAC table to validate who is connected to which port. In this case, the attacker alters the switch's configuration by using different techniques such as Port Mirroring or Switched Port Analyzer (SPAN). All packets passing through a monitored port will be copied onto a mirror port (the port on which the attacker is connected with a promiscuous mode). If you are connected to a hub, it will transmit all packets to all ports.

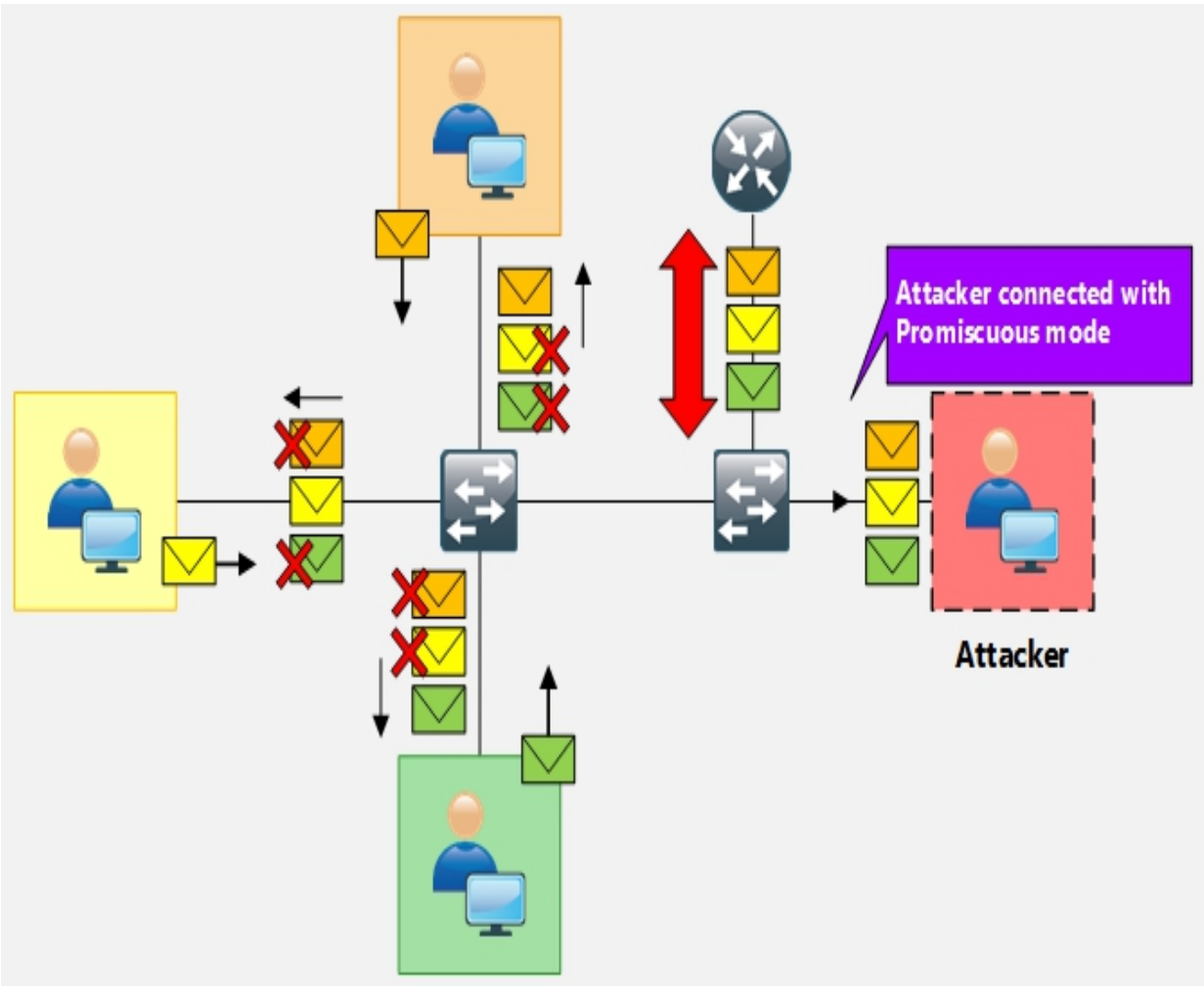


Figure 8-01: Packet Sniffing

Types of Sniffing

Passive Sniffing

Passive Sniffing is the type of sniffing in which there is no need to send additional packets or involve a device, such as a hub, to receive packets. As we know, hub broadcasts every packet to its port, which helps the attacker to monitor all traffic passing through a hub with no effort.

Active Sniffing

Active Sniffing is the type of sniffing in which an attacker has to send additional packets to the connected device, such as a 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, are used to analyze the captured packets and signals over the transmission channel. Hardware Protocol Analyzers are the physical equipment that captures the packets without interfering with network traffic. Major advantages 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
- Modify the size of packet

KEYSIGHT Technologies offers various products. To get updates and information, visit the website www.keysight.com. There are also other hardware protocol analyzer products available in the market from different vendors like RADCOM and Fluke.

The screenshot displays the Keysight Technologies website for Protocol Analyzer and Exerciser products. The browser window shows the URL: <https://www.keysight.com/en/pc-1000000194%3Aeps%3Aapgr/protocol-analyzer-and-exerciser?nid=-536902450.0&cc=PK&lc=eng>. The website features a red navigation bar with links to Hardware, Software, Services & Support, Industries & Technologies, and About Keysight. A sidebar on the left contains icons for user profile, shopping cart, document, chat, and eye. The main content area is titled "Protocol Analyzer and Exerciser" and includes a breadcrumb trail: Home > Hardware > Oscilloscopes, Analyzers, Meters > Protocol Analyzers and Exercisers. Below the title, there are links to "View Data Sheet" and "Visit Discussion Forums". A descriptive paragraph states: "As your design includes multi gigabit serial interconnect standards, Keysight protocol analyzer and exerciser products are the most effective solution to debug, validate and optimize semiconductors, software and system that use serial protocol standards for computer, storage, display, mobile and embedded systems." Another paragraph mentions: "Keysight's protocol test solutions for each technology typically consists of both protocol analyzer application as well as a stimulus solution, such as an exerciser or traffic generator. Keysight's protocol test solutions combine multi-protocol analysis, traffic generation, performance and conformance verification to debug, validate and optimize your designs using high speed protocol standards." Below this text is a "Products" section with three tabs: "Products", "Accessories & Related Products", and "Document Library". The "Products" tab is active, showing a grid of product images and descriptions:

- U4431A MIPI M-PHY Protocol Analyzer** (Image of a blue device)
- PCI EXPRESS® Protocol Solutions** (Image of a server rack)
- E2960B Series PCIe Test Solutions for PCIe 1.0 and PCIe 2.0** (Image of a laptop and a device)
- N5300 Series Chassis** (Image of a vertical chassis)
- Protocol Solutions for USB 3.0/2.0** (Image of a laptop and a device)
- U4421A Protocol Analyzer and Exerciser for MIPI D-PHY Interfaces** (Image of a laptop and a device)
- DigRF Protocol Test Products** (Image of a laptop and a device)
- SerialTek SAS/SATA BusXpert Analyzers, BusMod Error Injectors, BusGen BIST Generators** (Image of a server rack)
- U4431U MIPI M-PHY Protocol Analyzer** (Image of a device)

Figure 2-22: KEYSIGHT Technologies Hardware Protocol

Figure 8-02: KEYSIGHT Technologies Hardware Protocol Analyzer Products

SPAN Port

You have a user who has complained about network performance, while no one else in the building is experiencing the same issue. You want to run a Network Analyzer on the port, like Wireshark, to monitor ingress and egress traffic on the port. To do this, you can configure SPAN (Switch Port Analyzer). 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, for example 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 two 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 the 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 that if you are using a source port that has a higher bandwidth than the destination port, some of the traffic will be dropped when the link is congested.

Simple Local SPAN Configuration

Consider the following diagram in which a Router (R 1) 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 of FE0/24 where our monitoring workstation is waiting to capture the traffic.

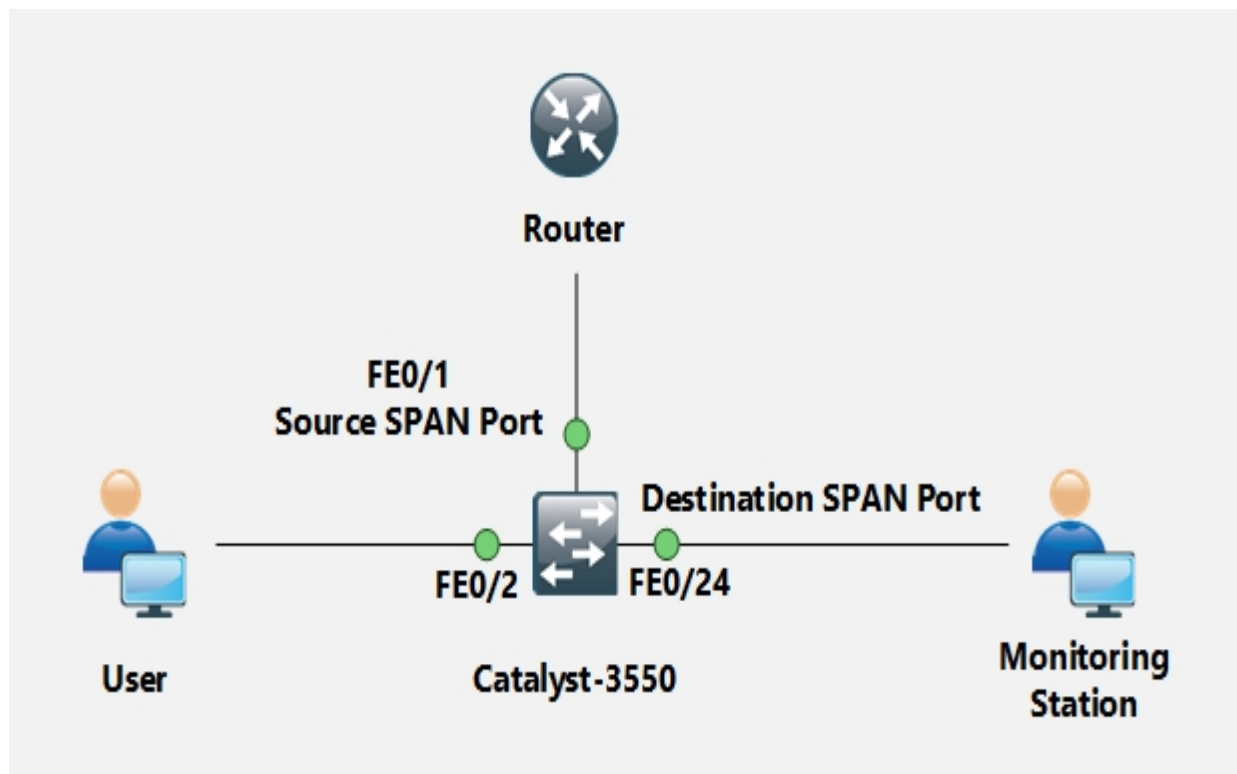


Figure 8-03: SPAN Port

Once we have our network analyzer setup and running, the first step is to configure Fast Ethernet 0/ 1 as a source SPAN port and configure Fast Ethernet 0/24 as the destination SPAN port. After configuring both interfaces, destination's SPAN port LED (FE0/24) will begin to flash in synchronization with that of FE0/ 1's LED – an expected behavior considering all FE0/ 1 packets are being copied to FE0/24.

Wiretapping

Wiretapping is the process of gaining information by tapping the signal from wires such as telephone lines or the internet. Usually, wiretapping is performed by a third party to monitor conversations. Wiretapping is basically an electrical tap on a telephone line. Legal Wiretapping is known as Legal Interception, which is mostly performed by governmental or security agencies.

Wiretapping is classified into two types:

Active Wiretapping

Active Wiretapping includes the monitoring and recording of information by wiretapping. It also includes alteration of communication.

Passive Wiretapping

In Passive Wiretapping, information is monitored and recorded by wiretapping without altering the communication.

Lawful Interception

Lawful Interception (LI) is a process of wiretapping with legal authorization that allows law enforcement agencies to selectively wiretap the communication of an individual user. The standard organization of the telecommunication sector standardized the legal interception gateways for agencies' interception of communication.

Planning Tool for Resource Integration (PRISM)

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

MAC Attacks

MAC Address Table/CAM Table

MAC is the abbreviation of Media Access Control. A MAC address is the physical address of a device. It is a 48-bit unique identification number that is assigned to a network device for communication at a data-link layer. A MAC address is comprised of a 24-bit Object Unique Identifier (OUI) and 24-bit Network Interface Controller (NIC). In cases of multiple NICs, the device will have multiple unique MAC addresses.

A 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 for forwarding packets. The CAM table records each MAC address—such as the associated VLAN information,

learning type, and associated port parameters. These parameters help at data-link layer to forward packets.

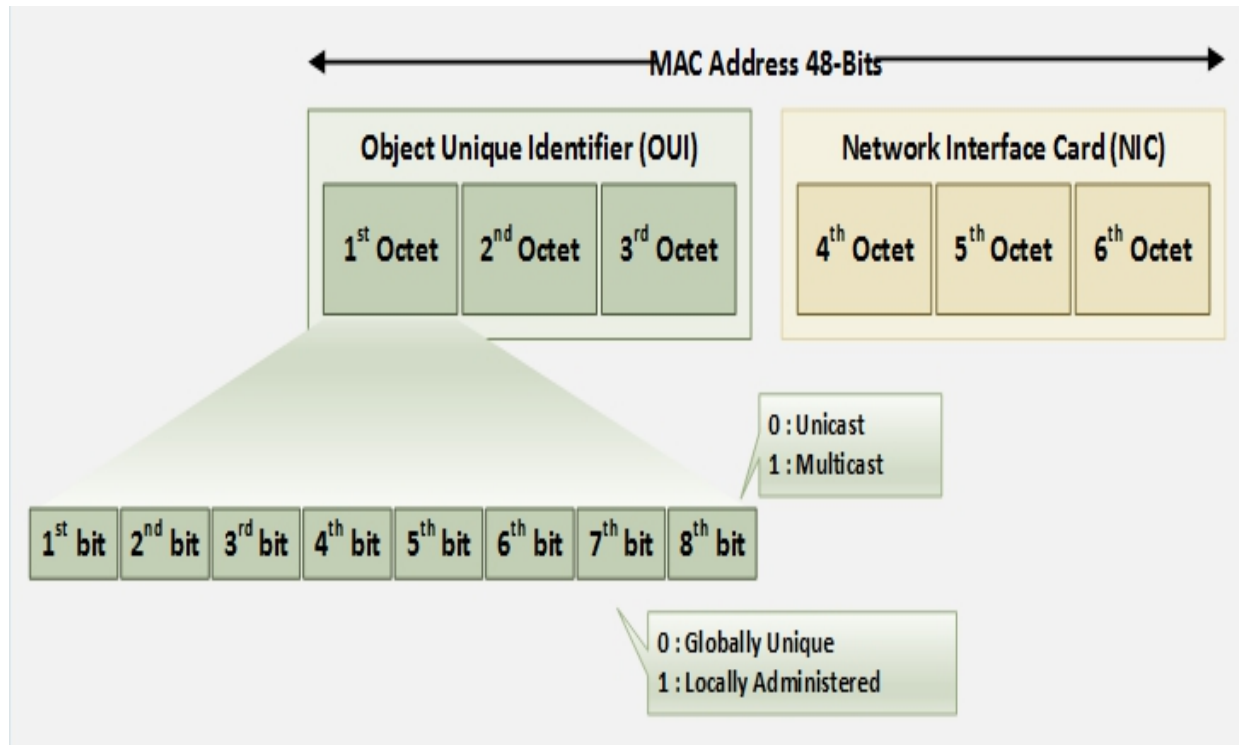


Figure 8-04: MAC Address
How Content Addressable Memory Works

Learning the MAC address of devices is the fundamental responsibility of switches. A 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. Remember 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 when they have not been seen for some time.

```
Switch
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

A switch supports multiple MAC addresses on all ports so we can connect individual workstations as well as multiple devices through a switch or router. Through the feature of Dynamic Addressing, a 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, the aging time of a 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 an attacker sends random MAC addresses mapped with random IP to overflow the storage capacity of a CAM table. A switch then acts as a hub because a CAM table has a fixed length. It will now broadcast the packet on all ports, which helps an attacker to sniff the packet with ease. A Unix/Linux utility, known as “macof”, offers MAC flooding. Using macof, a random source MAC and IP can be sent to 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 a false ARP packet with the source MAC address of the target and his

own destination address, as the attacker is impersonating the target host (let's say Host A). When this is forwarded to the switch, the switch will update the CAM table. When Host A sends a packet, switch will have to update it again. This will create a “winning the race” condition in which if the attacker sends the ARP with Host A's MAC address, the switch will send packets to the attacker assuming Host A is connected to this port.

Defending Against MAC Attacks

Port Security is used to secure the ports. You can either bind a known MAC address with a port (static) or specify the limit to learn the MAC on a port (dynamic). You can also enforce a violation action on a port. Hence, if an attacker tries to connect his PC or embedded device to the switch port, the port is configured to support a specific MAC address only. An attacker's attempt to connect on the port will violate the condition, and the port will shut down or restrict the traffic flow on that port. In dynamic port security, you must specify the 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

The 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 the Cisco Switch will allow a specific MAC address and four additional MAC addresses.

Port Security Configuration

```
Switch(config)# interface ethernet 0/0
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 can be reused when hosts do not need them. Round Trip time is the measurement of time from discovery of the DHCP server up to obtaining the leased IP address. RTT can be used to determine the performance of DHCP. By using UDP broadcast, a DHCP client sends an initial DHCP-Discover packet because it initially does not have information about the network to which they are connected. The DHCP server relies to the DHCP-Discover packet with a DHCP-Offer Packet offering the configuration parameters. The DHCP client will send a DHCP-Request packet destined for the DHCP server requesting configuration parameters. Finally, the 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

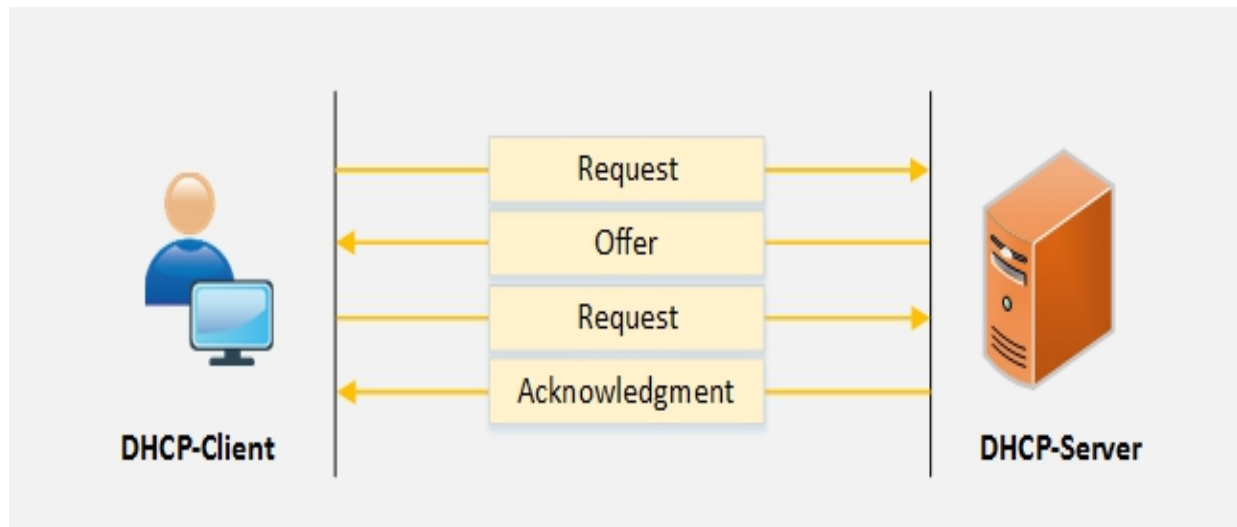


Figure 8-06: IPv4 DHCP Process

A DHCP Relay agent forwards the DHCP packets from server to client and client to server. The relay agent helps the communication by forwarding requests and replies between client and servers. The relay agent, when receiving a DHCP message, generates a new DHCP request including default gateway information as well as Relay-Agent information option (Option82) and sends it to remote DHCP server. 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 the relay agent and the DHCPv 6 server is same as the IPv4 relay agent and DHCPv4 server. The DHCP server receives the request and assigns the IP address, DNS, lease time, and other necessary information to the client, whereas the relay server forwards the DHCP messages.

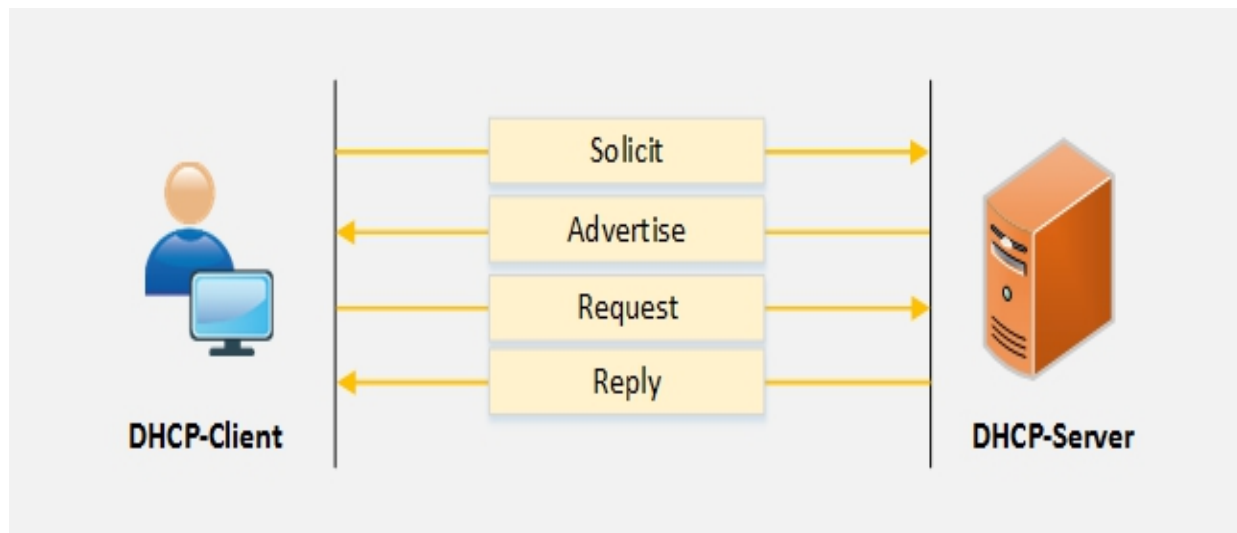


Figure 8-07: IPv6 DHCP Process

DHCPv6 uses two different ports:

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

DHCP Starvation Attack

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

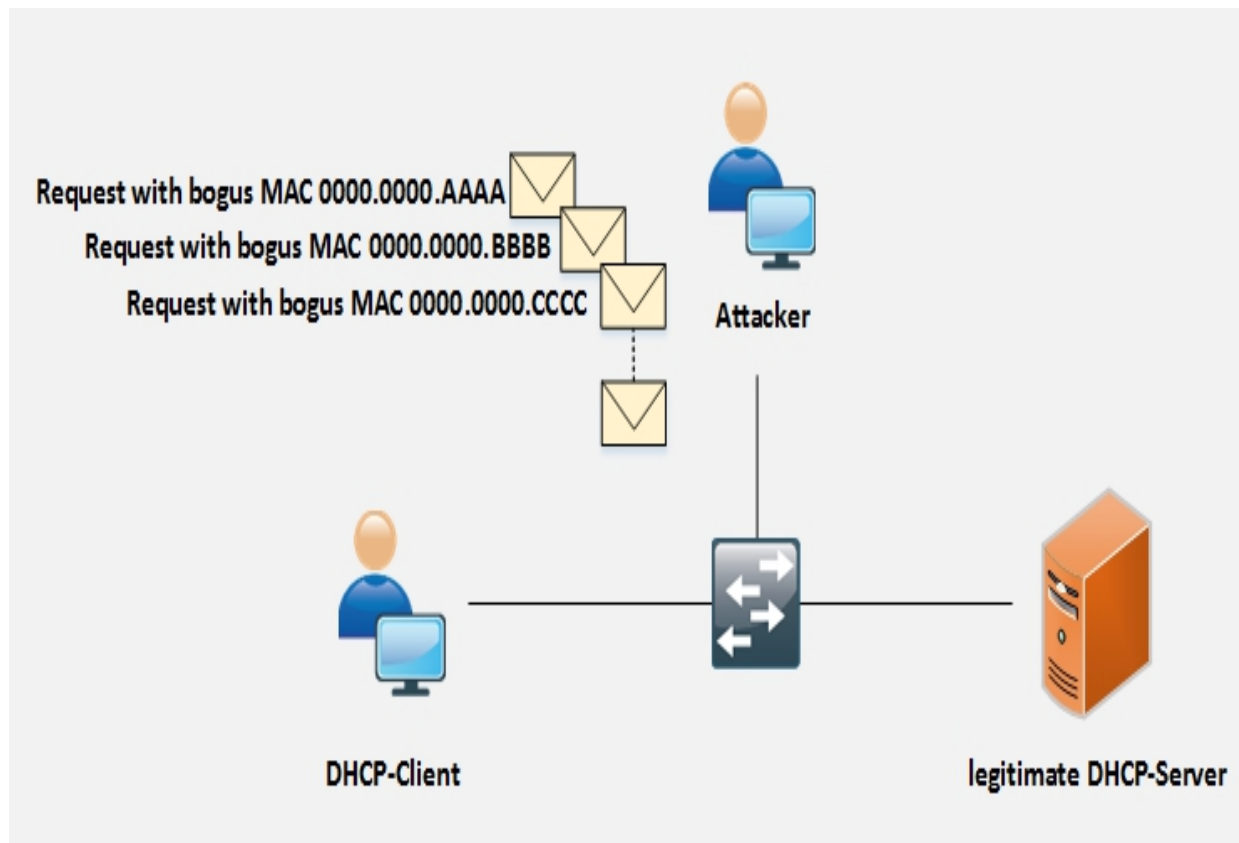


Figure 8-08: DHCP Starvation Attack
Rogue DHCP Server Attack

A 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 under denial-of-service attack, DHCP clients are unable to gain IP addresses from the legitimate DHCP server. Upcoming DHCP Discovery (IPv4) or Solicit (IPv6) packets are replied to by a fake DHCP server with a configuration parameter that directs traffic towards it.

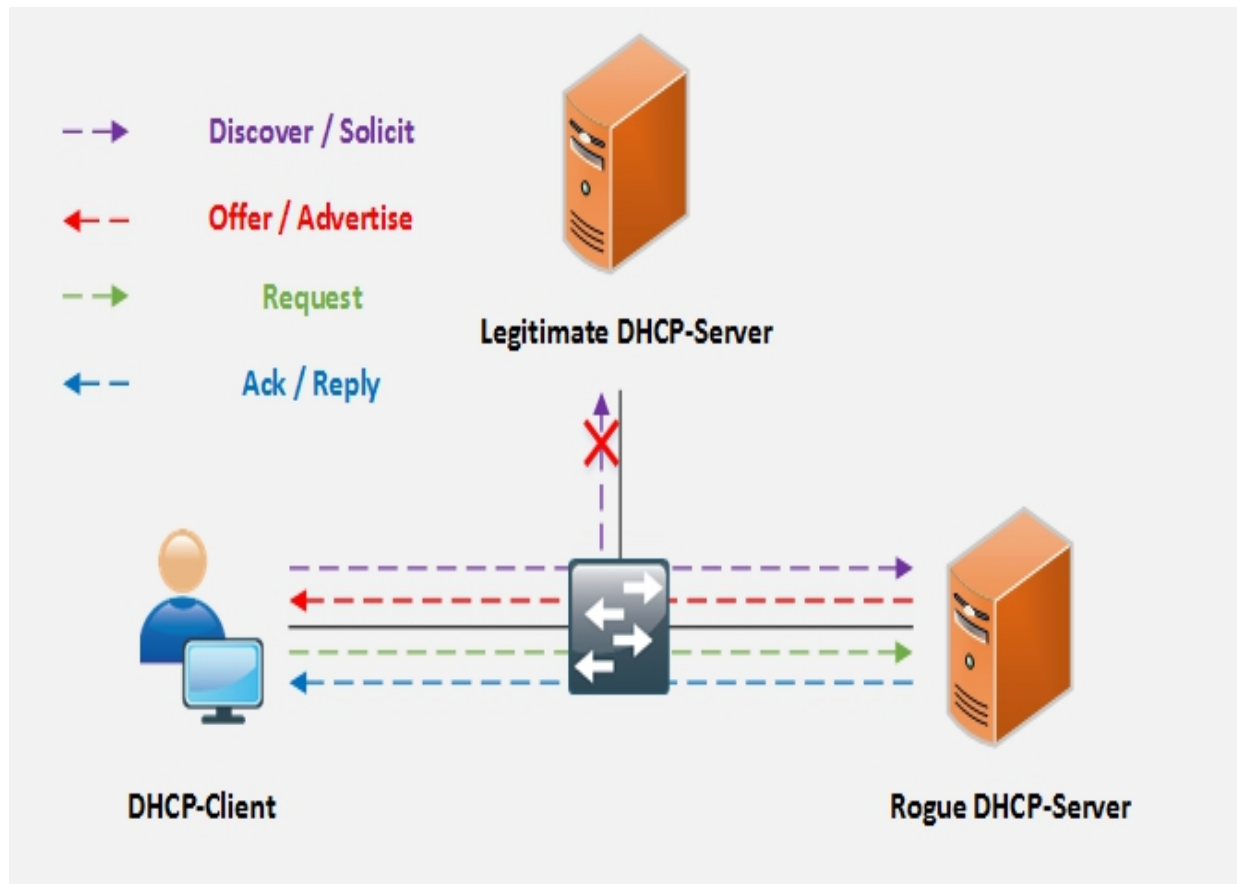


Figure 8-09: Rogue DHCP Server Attack

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 protection against such attacks. In order to mitigate against such attacks, the DHCP snooping feature is enabled on networking devices to identify from DHCP traffic only the trusted ports. It allows ingress and egress DHCP traffic. Any access port that tries to reply to the DHCP requests will be ignored because the device will only allow the DHCP process from a trusted port as defined by the networking team. It is a security feature that 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 against these attacks by limiting the port to learning a maximum number of MAC addresses, configuring violation actions, aging time, etc.

ARP Poisoning Address Resolution Protocol (ARP)

ARP is a stateless protocol that is 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 an 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. Only the node with a coordinating MAC address for that IP will answer the demand with the packet that involves the MAC address mapping. The switch will feed the MAC address and its connected port information into its fixed length CAM table.

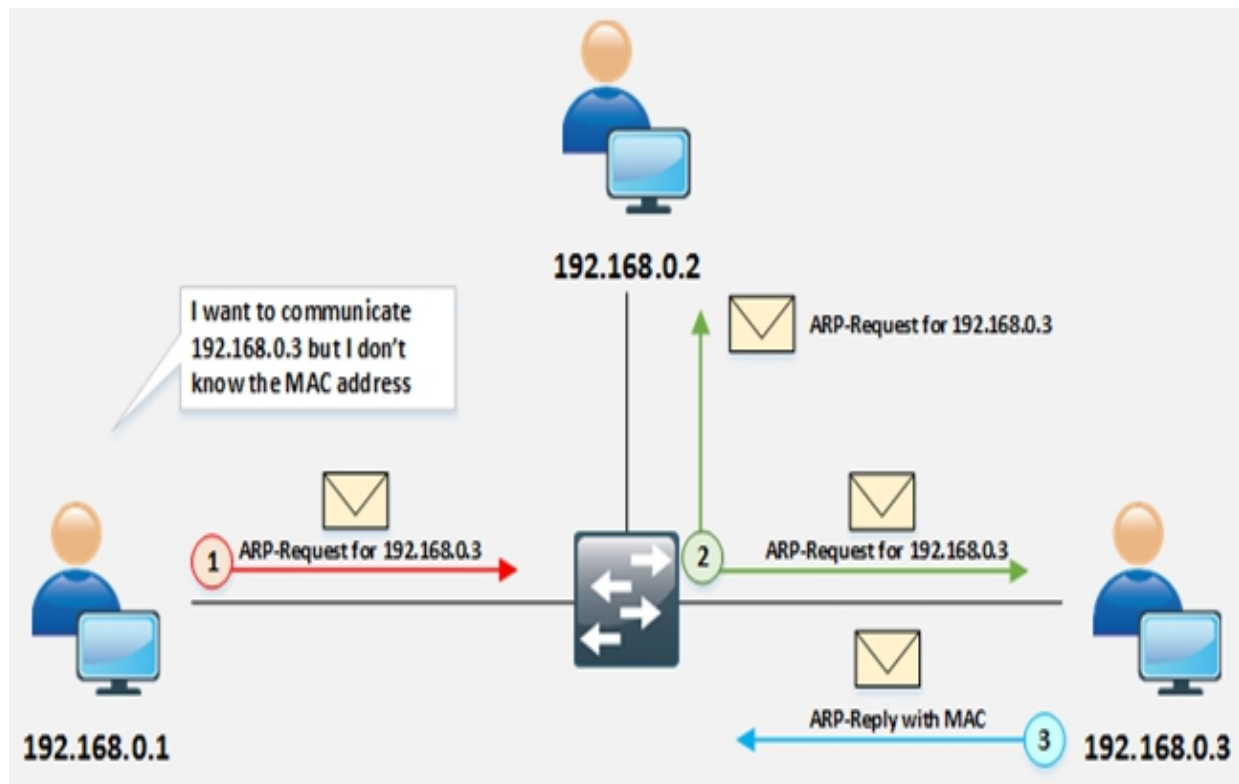


Figure 8–10: ARP Operation

As shown in Figure 8– 10, the source generates an ARP query by broadcasting the ARP packet. A node with the MAC address that the query is destined for will reply only to the packet. The frame is flooded out of 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. The MAC flooding technique is used to turn a switch into a hub, in which the switch starts broadcasting each and every packet. In this scenario, each user can catch the packets, even those that are not intended for them.

ARP Spoofing Attack

In ARP spoofing, an attacker sends forged ARP packets over a Local Area Network (LAN). In this case, the switch will update the attacker's MAC Address with the IP address of a legitimate user or server. Once an attacker's MAC address is learned, used within a broadcast domain to ensure together with the IP address of an authentic user, the switch will start forwarding the packets to the attacker, assuming that it is the MAC of the user. Using an ARP Spoofing attack, an attacker can steal

information by extracting it from the packet intended for a user over LAN that it received. 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 Passwords

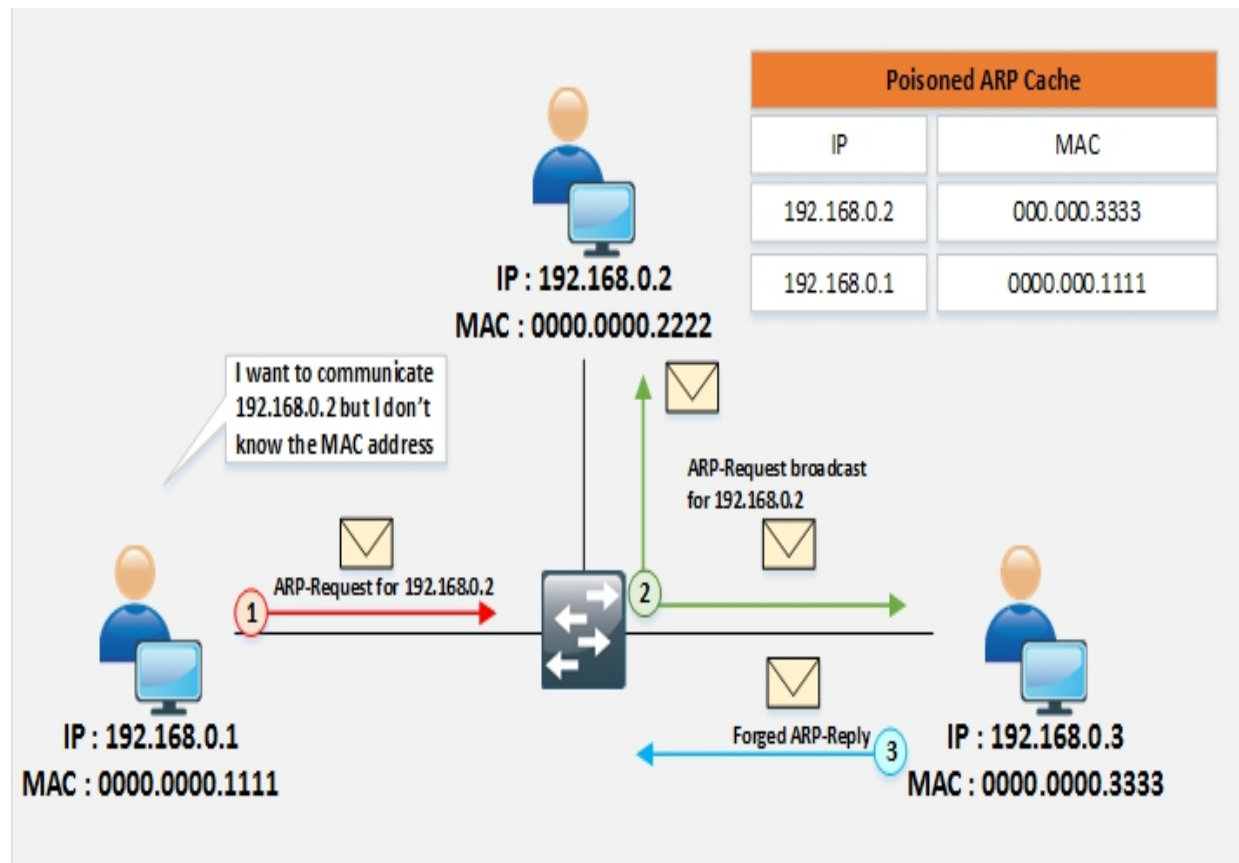


Figure 8-11: ARP Spoofing Attack

Defending ARP Poisoning
Dynamic ARP Inspection (DAI)

DAI is used with DHCP snooping. ARP is a layer 2 protocol that functions on IP-to-MAC bindings. Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets within a network. DAI investigates the ARP packets by intercepting, logging, and discarding the invalid IP-MAC address bindings. 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

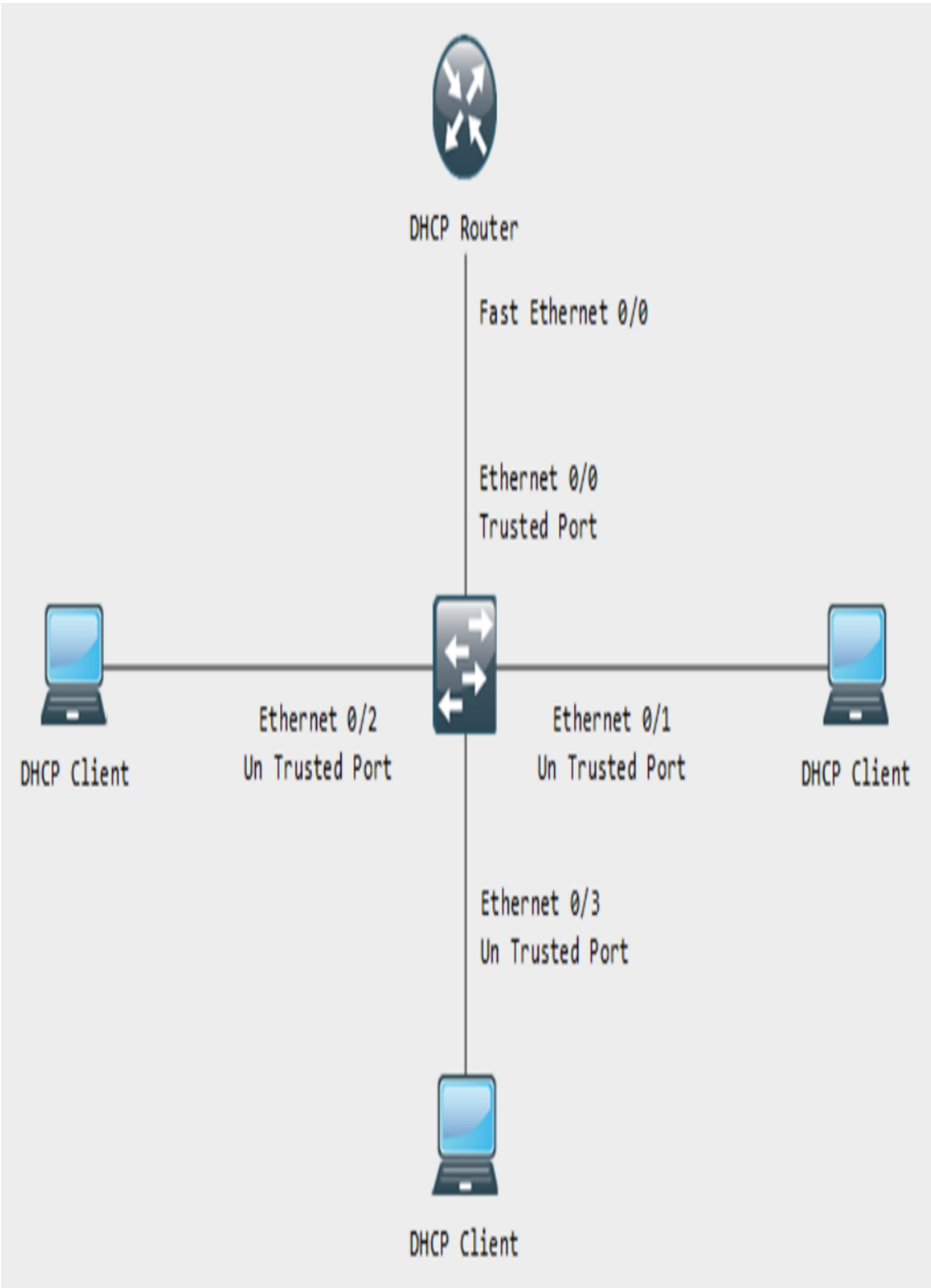


Figure 8–12: Configuring DHCP Snooping

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
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
  Custom circuit-ids:
Ethernet0/1              no        yes             unlimited
  Custom circuit-ids:
Ethernet0/2              no        yes             unlimited
  Custom circuit-ids:
Ethernet0/3              no        yes             unlimited
  Custom circuit-ids:
Switch#
Switch#
```

Figure 8-13: Verifying DHCP Snooping

The command output shown in the above figure displays 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

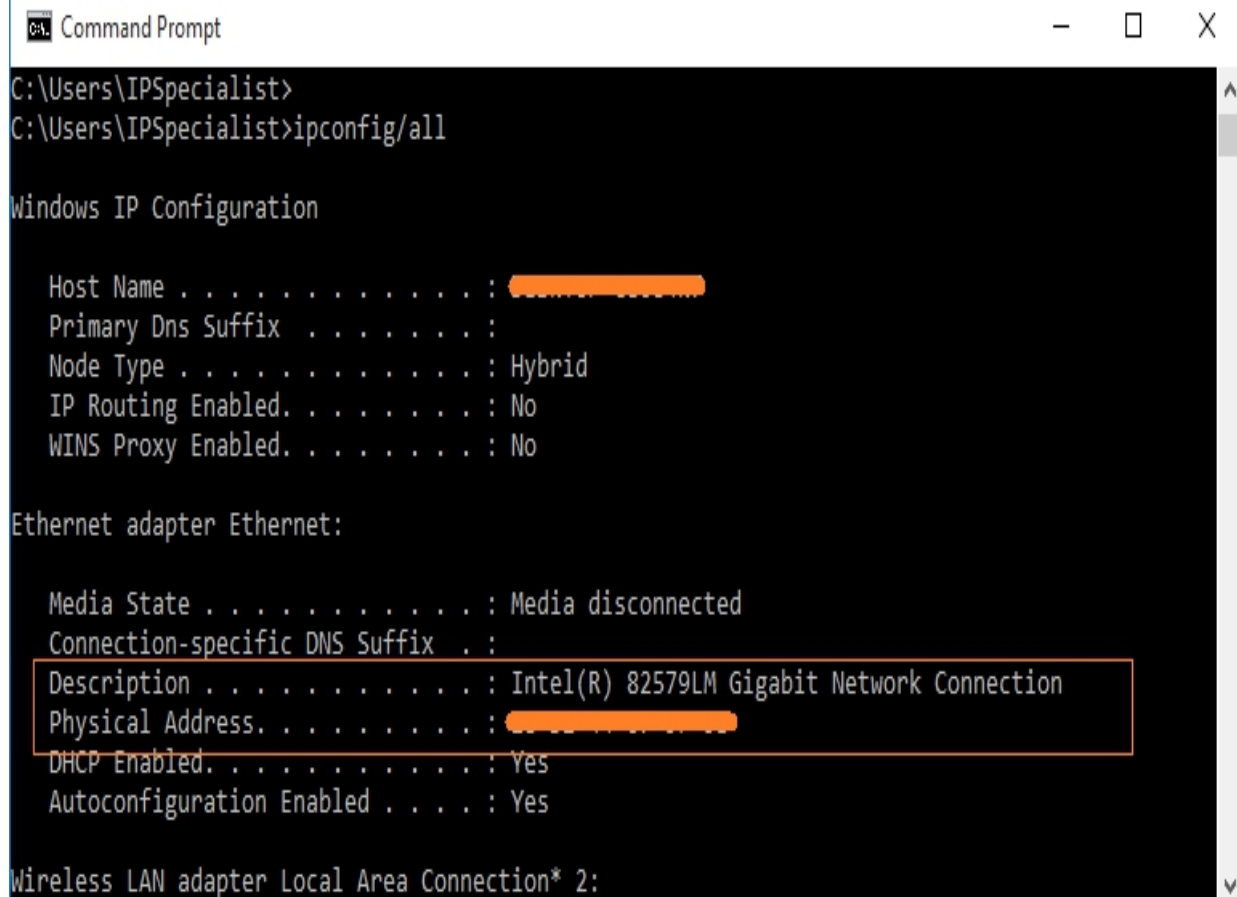
MAC Spoofing is the technique of manipulating a MAC address to impersonate the authentic user or launch attacks such as denial-of-service. A MAC address is built on a network interface controller that cannot be changed, but some drivers enable changing the MAC address. This masking process of MAC addresses is known as MAC Spoofing. An attacker sniffs users' MAC addresses that are active on switch ports and duplicates the MAC address. Duplicating the MAC can intercept the traffic and traffic destined to the legitimate user may be directed to the attacker.

Lab 8– 1: Configuring Locally Administered MAC Addresses Procedure:

1. Go to “Command Prompt” and type the command:

```
C:\W> 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 Addresses

2. Go to “Control Panel” and click “Hardware and Sounds”.

Figure 8–15: Control Panel

3. Click “Device Manager”.

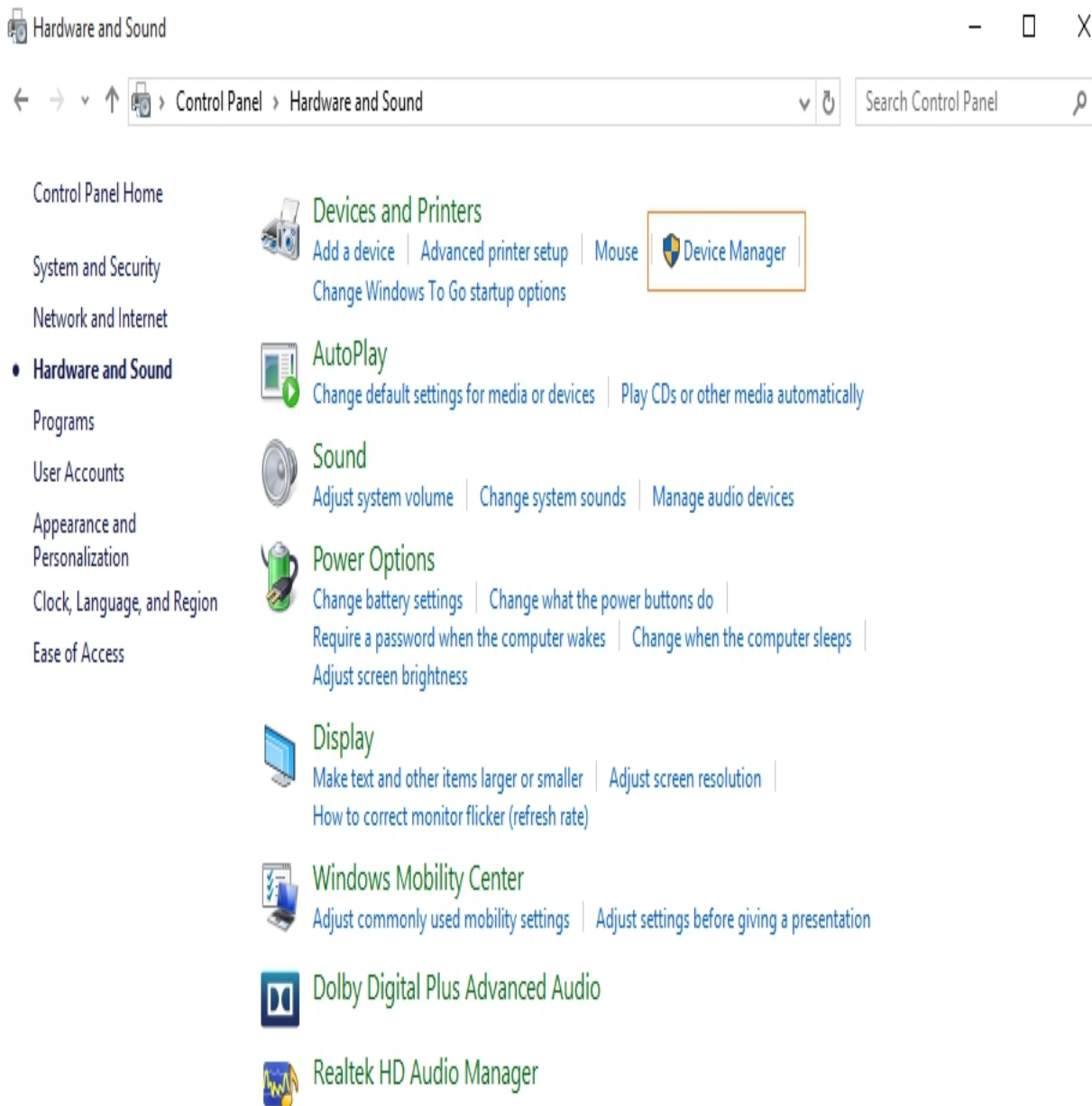


Figure 8–16: Hardware and Sounds

4. Select your Network Adapter.

Figure 8–17: Device Manager

5. Right click on the desired Network Adapter and click “Properties”.

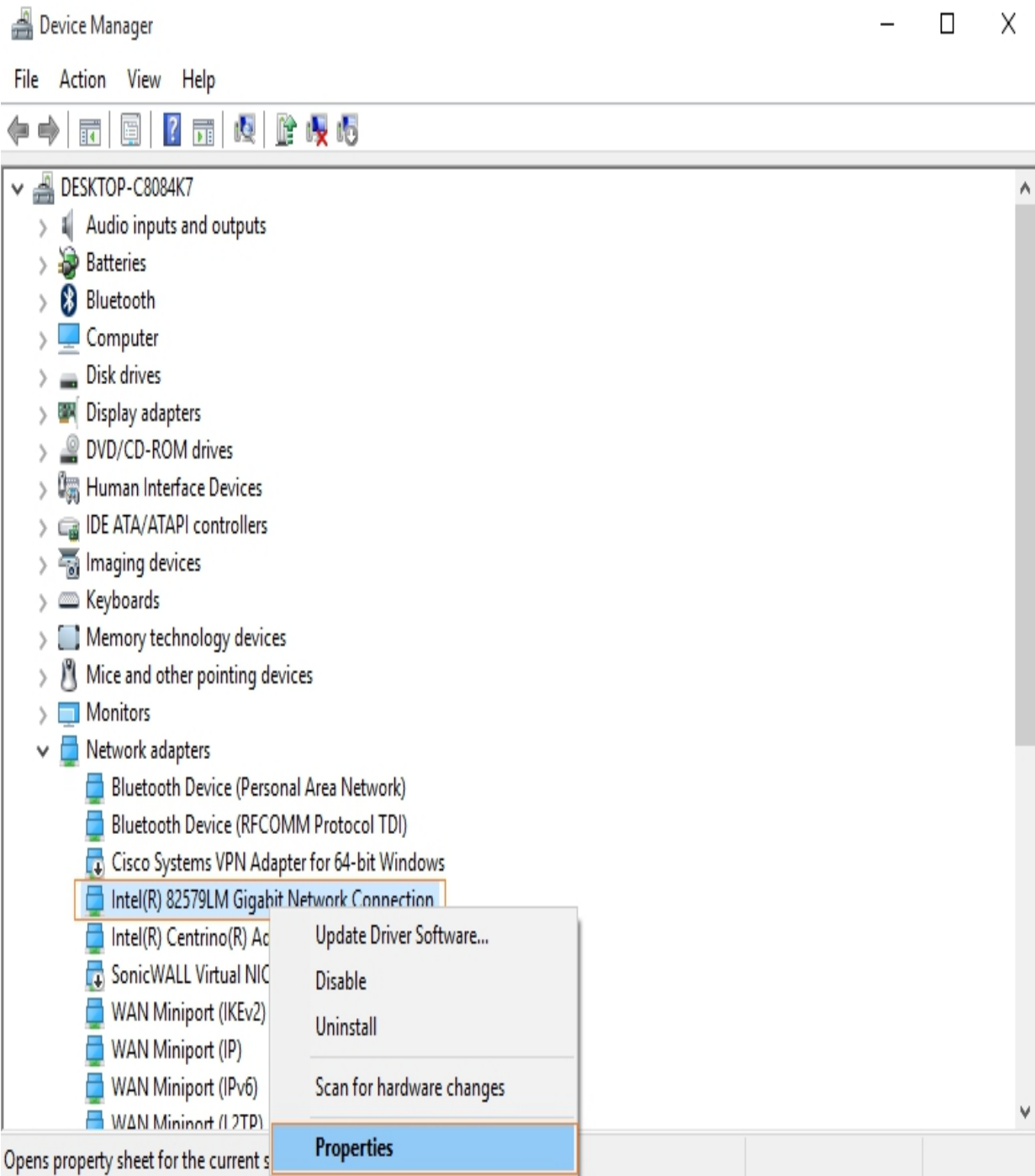


Figure 8–18 Network Adapters

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

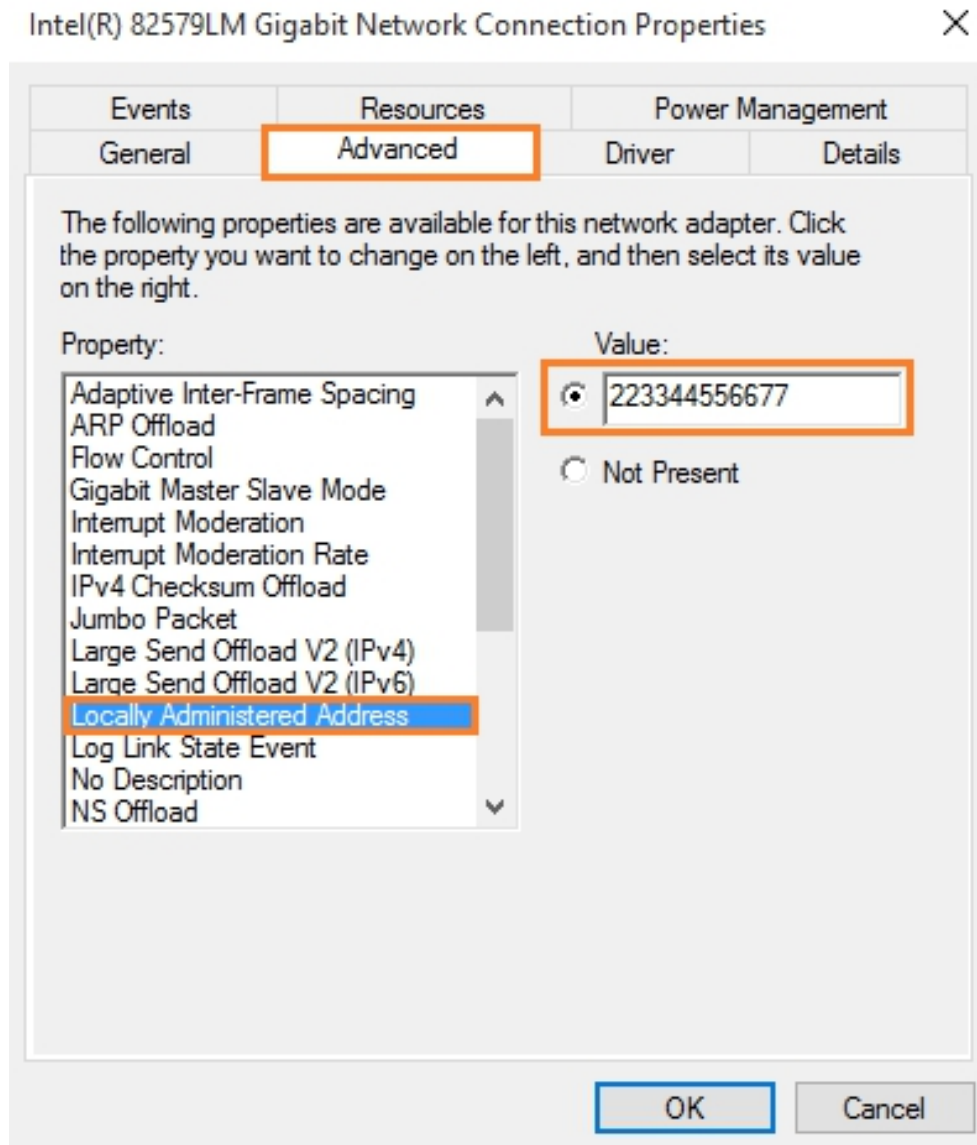


Figure 8–

19: Network Adapter Properties

Verification

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

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

```
Command Prompt
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\IPSpecialist>ipconfig/all

Windows IP Configuration

Host Name . . . . . : DESKTOP-
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. . . . . : 22-33-44-55-66-77
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . :
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

Figure 8–20: Verifying MAC Address

MAC Spoofing Tool

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

- Technitium MAC Address Changer

- SMAC

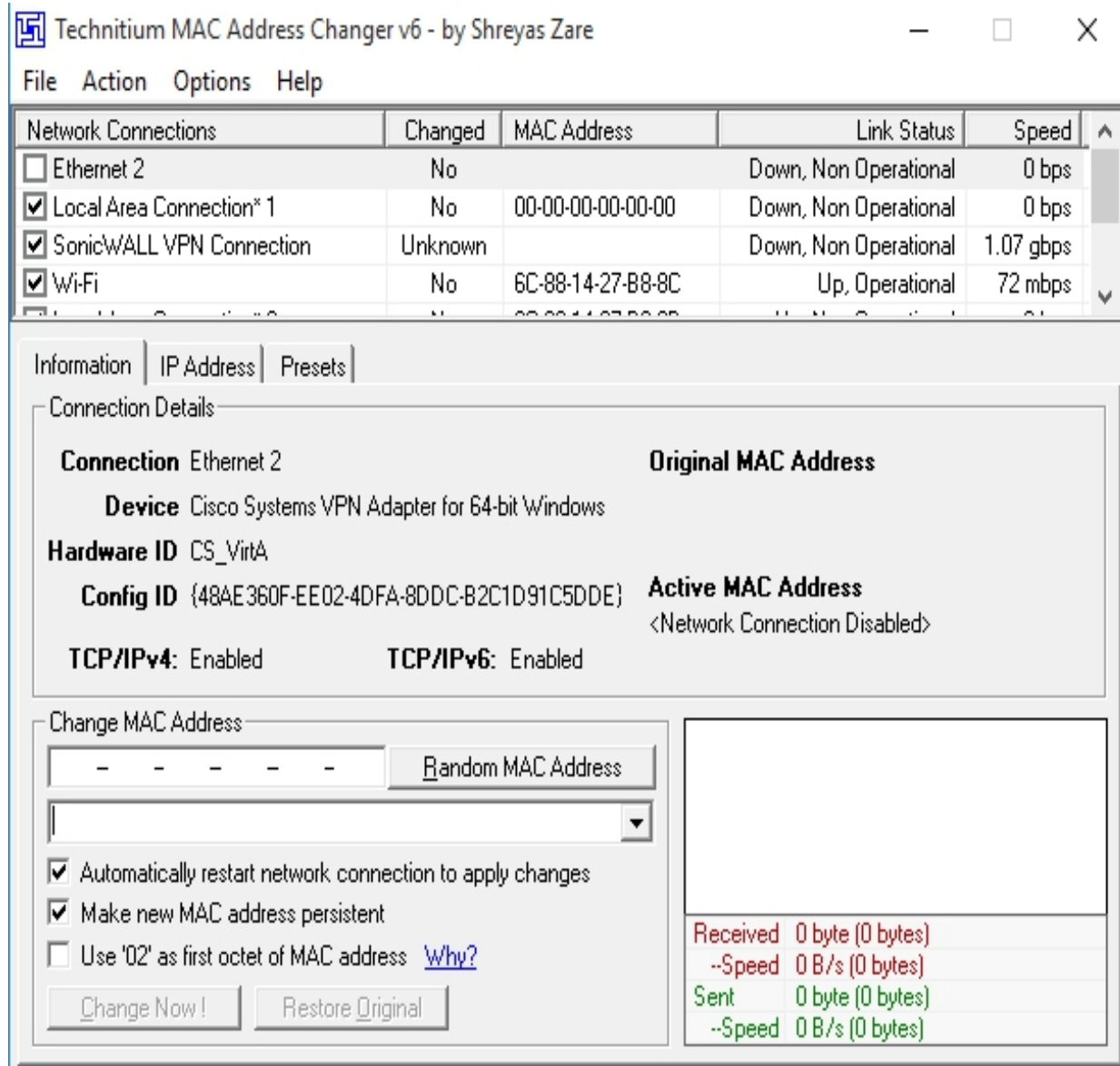


Figure 8-21: Technitium MAC Address Changer

How to Defend Against MAC Spoofing

In order to defend against MAC spoofing, DHCP Snooping and Dynamic ARP Inspection are effective techniques to use. Additionally, a source guard feature is configured on client facing switch ports.

An IP source guard is a port-based feature that provides a source IP address filtering at Layer 2. The source guard feature monitors and prevents the host from impersonating another host by assuming the

authentic host's IP address. In this way, the malicious host is restricted to using 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 types 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 against 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 an important protocol used in networking to maintain records and translate human-readable domain names into IP addresses. When a DNS server receives a request, it translates the human-readable domain name, such as "google.com", into its mapped IP address. When it does not find the mapping translation in its database, it generates the query to another DNS server for the translation and so on. The DNS server with the translation will reply to the requesting DNS server, and the client's query will be resolved.

In cases where 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 causes poison in DNS translation and continues to do so until the cache expires. DNS poisoning is performed by attackers to direct traffic toward the servers and computers owned or controlled by them.

Note: DNS cache poisoning, also known as DNS spoofing, is a type of attack that exploits vulnerabilities in DNS to divert internal network traffic away from legitimate servers toward fake ones.

A Start of Authority (SOA) record stores information about the Domain Name System (DNS) zone and other DNS records such as the email address of the administrator, when the domain was last updated, and how long the server should wait between refreshes.

Intranet DNS Spoofing

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

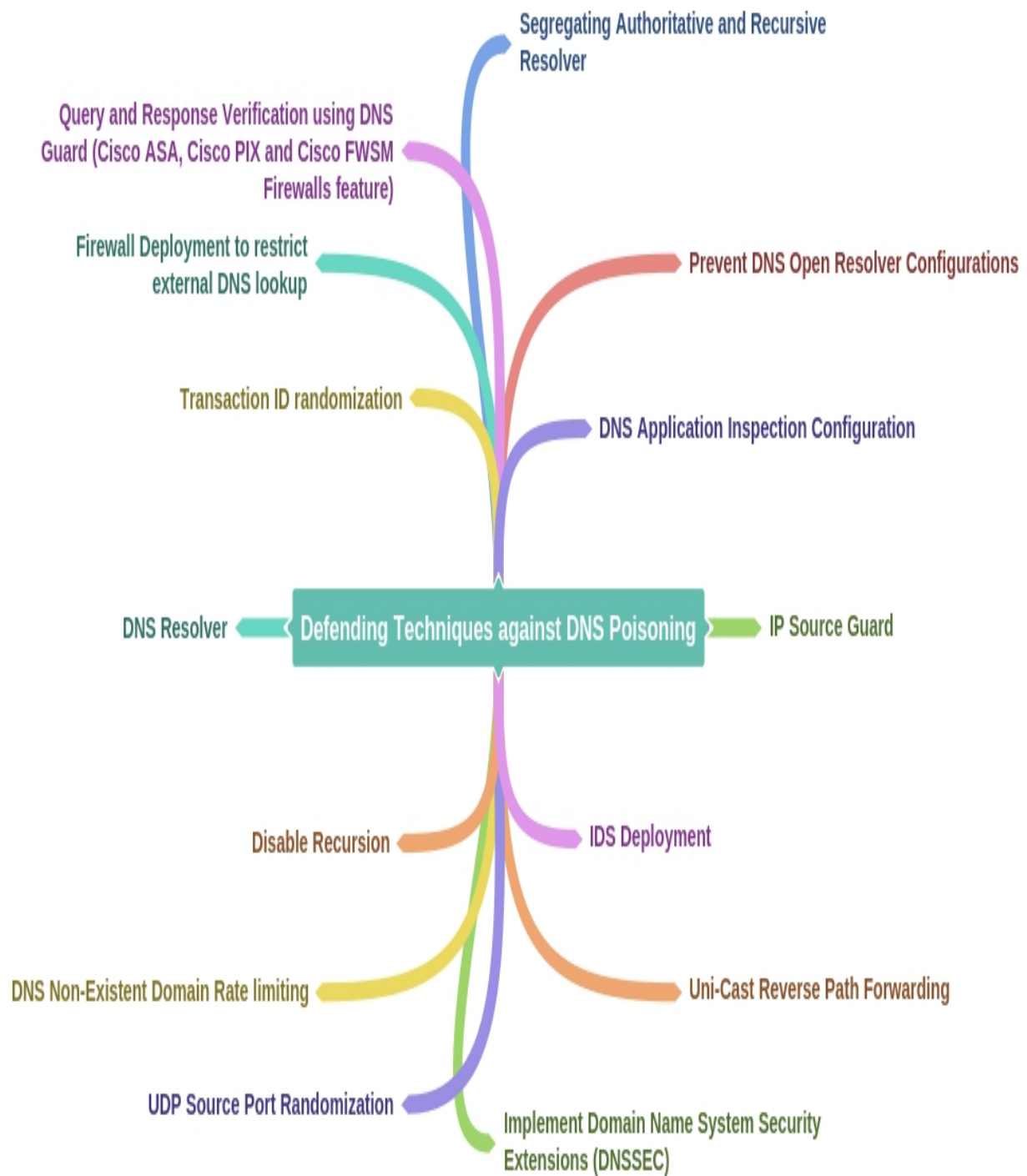
Similar to internet DNS Spoofing, Proxy Server DNS poisoning is performed by replacing the DNS configuration from the web browser of a target. All web queries are directed to a malicious proxy server controlled by the attacker, redirecting traffic to malicious sites.

DNS Cache Poisoning

Normally, internet users use DNS provided by the Internet Service Provider (ISP). In a corporate network, the organization uses their own DNS performance by caching frequently or previously generated servers to improve

queries. DNS Cache poisoning is performed by exploiting flaws in the DNS software. An attacker adds or alters the entries in the DNS record cache, which redirects traffic to the malicious site. When an internal DNS server is unable to validate the DNS response from the 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 and 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.

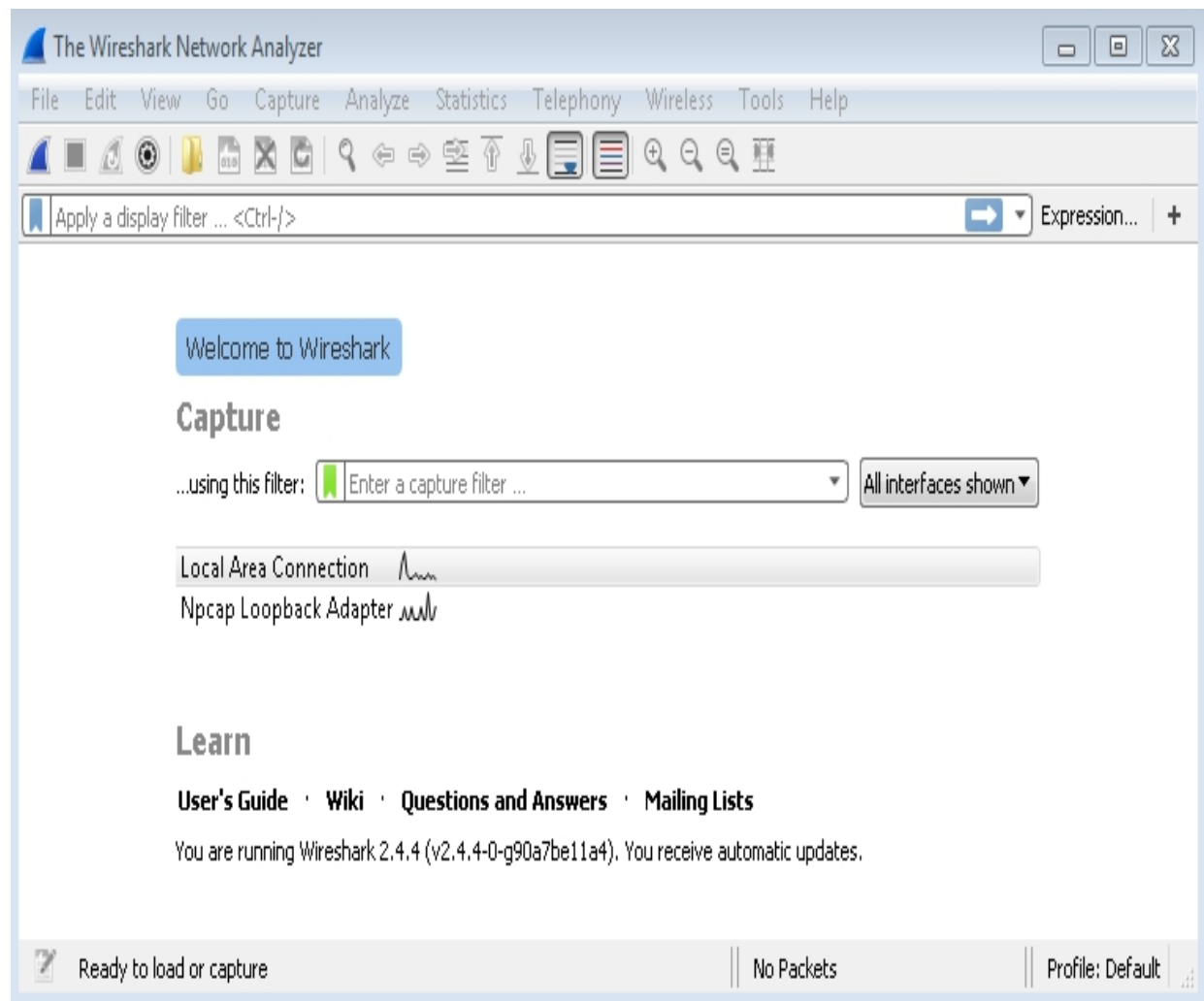


Figure 8–22: Wireshark Network Analyzer
Click “Capture” > “Options” to edit capture options.

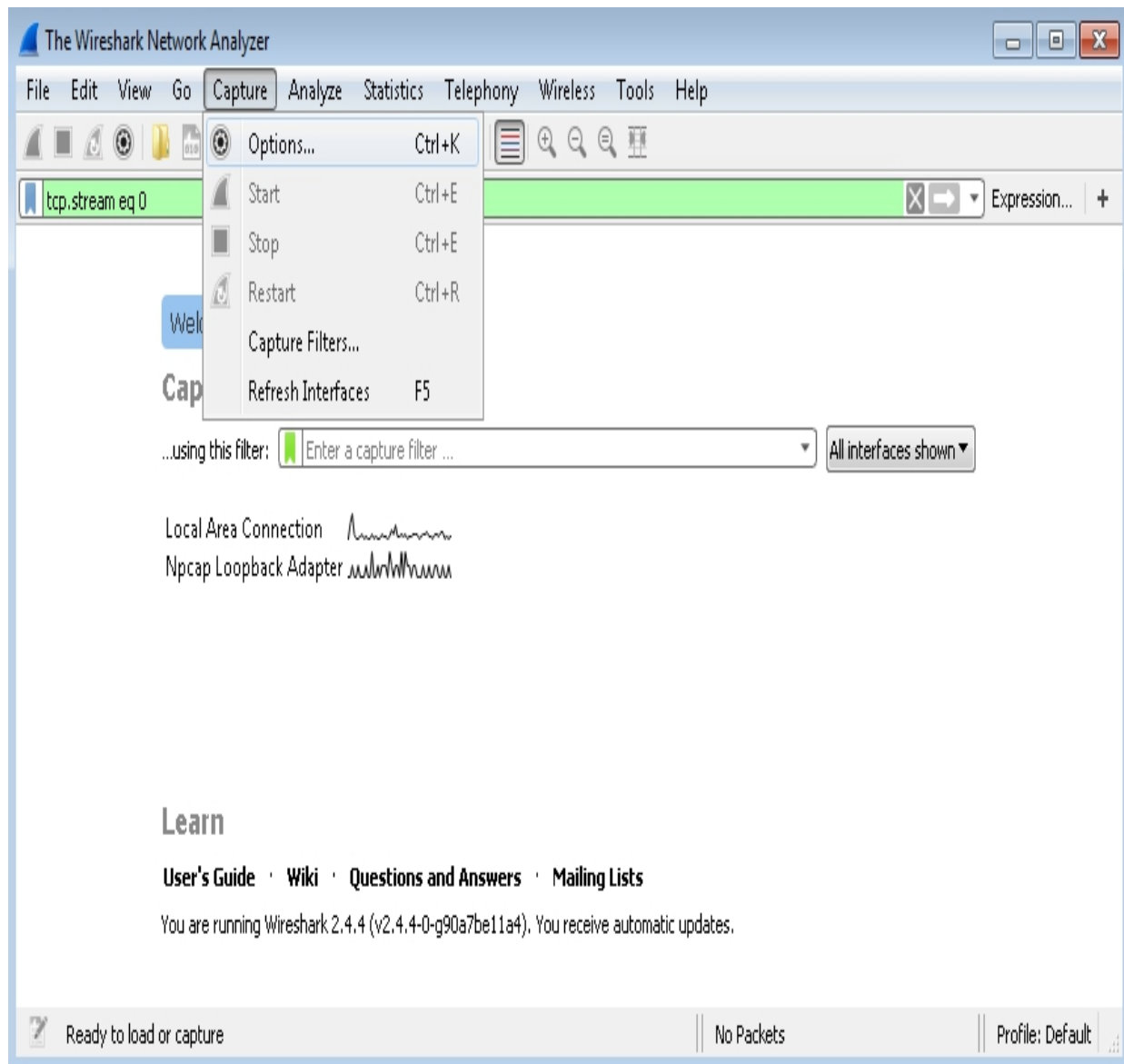


Figure 8–23: Wireshark Network Analyzer

Here, you can enable or disable a promiscuous mode on an interface. Configure the Capture Filter and click the “Start” button.

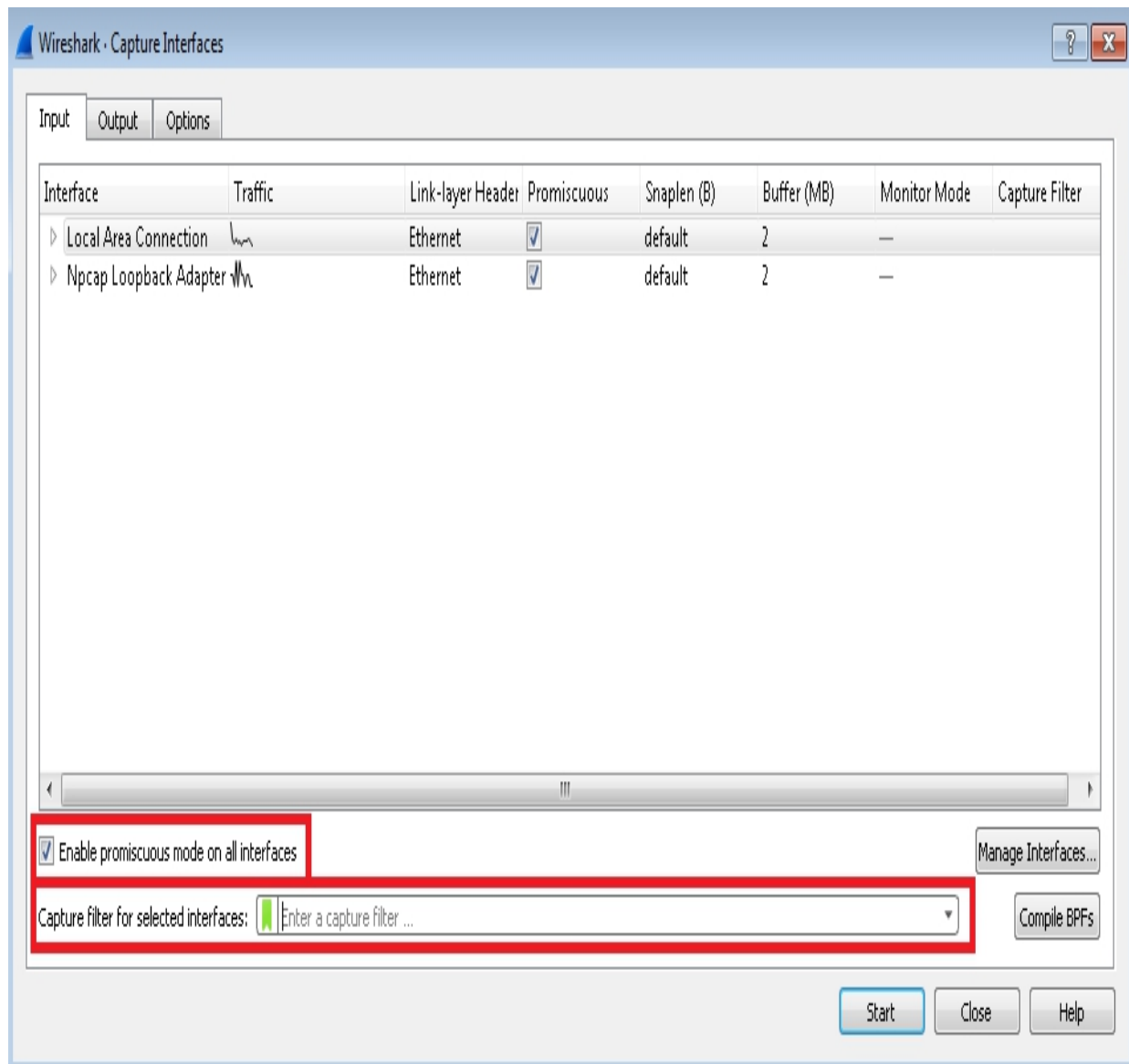


Figure 8–24: Wireshark Network Analyzer

Click “Capture” > “Capture Filter” to select Defined Filters. You can add the filter by clicking the “Add” button.

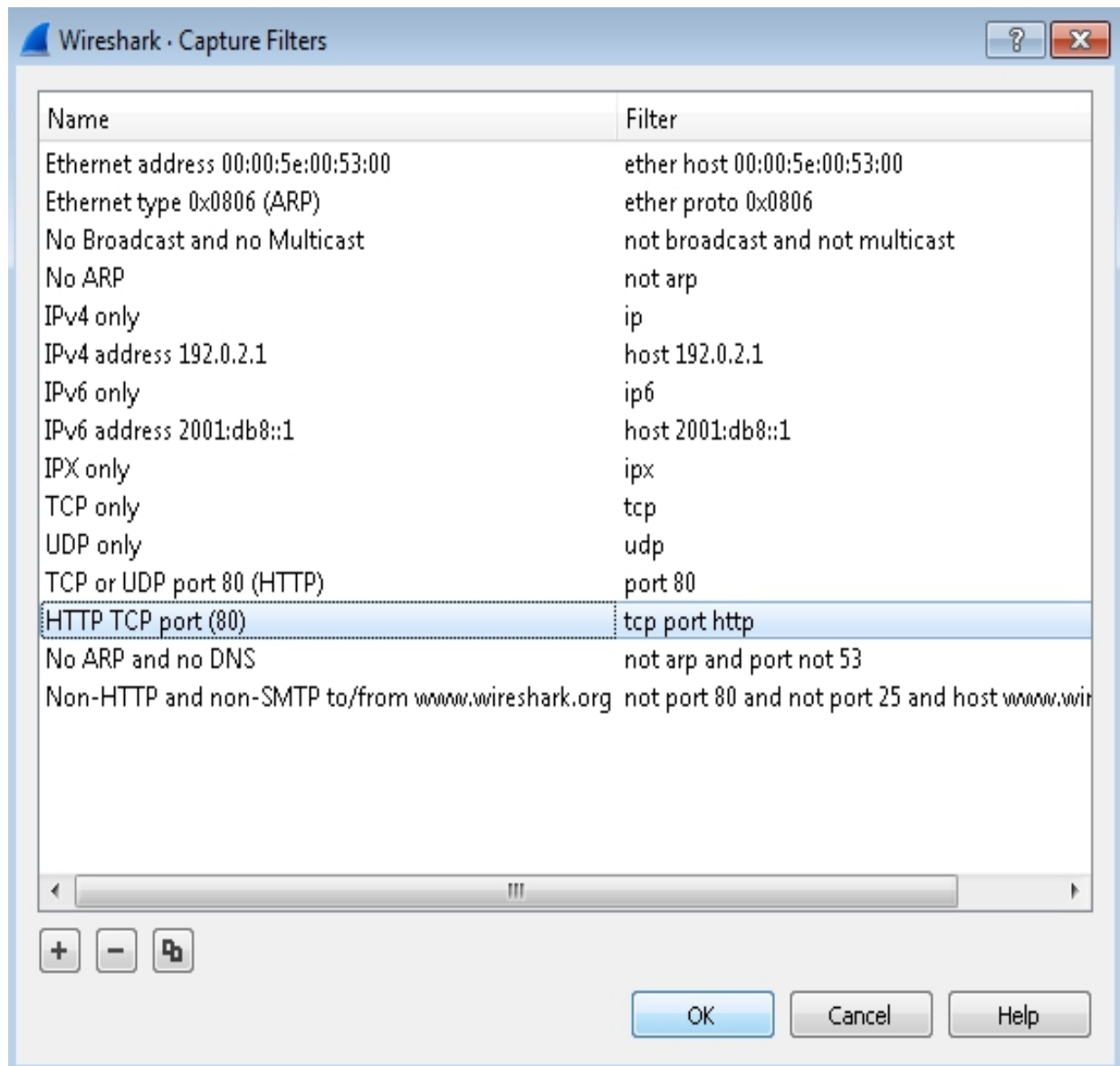


Figure 8-25: Wireshark Network Analyzer

Follow the TCP Stream in Wireshark

Working on TCP-based protocols can be very helpful by using the “Follow TCP Stream” feature.

This helps 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.

*Local Area Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.50.201	10.10.50.202	ICMP	74	Echo (ping) request id=0x000...
2	0.000654	10.10.50.202	10.10.50.201	ICMP	74	Echo (ping) reply id=0x000...
3	0.052298	10.10.50.201	192.168.95.2	TCP	1314	3389 → 61004 [ACK] Seq=1 Ack=...
4	0.052310	10.10.50.201	192.168.95.2	TCP	1295	3389 → 61004 [PSH, ACK] Seq=1...
5	0.100745	192.168.95.2	10.10.50.201	TCP	60	61004 → 3389 [ACK] Seq=1 Ack=...
6	0.110616	192.168.95.2	10.10.50.201	TCP	60	61004 → 3389 [ACK] Seq=1 Ack=...
7	0.120365	10.10.50.201	10.10.50.201	TCP	60	61004 → 3389 [ACK] Seq=1 Ack=...
8	0.120365	10.10.50.201	10.10.50.201	TCP	60	61004 → 3389 [ACK] Seq=1 Ack=...
9	0.130365	10.10.50.201	10.10.50.201	TCP	60	61004 → 3389 [ACK] Seq=1 Ack=...
10	0.140365	10.10.50.201	10.10.50.201	TCP	60	61004 → 3389 [ACK] Seq=1 Ack=...
11	0.190365	10.10.50.201	10.10.50.201	STP	60	Conf. Root = 32768/210/f8:72:...
12	0.220365	10.10.50.201	10.10.50.201	TCP	60	61004 → 3389 [ACK] Seq=1 Ack=...
13	0.250365	10.10.50.201	10.10.50.201	TCP	1314	3389 → 61004 [ACK] Seq=2502 A...
14	0.250365	10.10.50.201	10.10.50.201	TCP	591	3389 → 61004 [PSH, ACK] Seq=3...
15	0.310365	10.10.50.201	10.10.50.201	TCP	91	61004 → 3389 [PSH, ACK] Seq=1...
16	0.320365	10.10.50.201	10.10.50.201	TCP	171	3389 → 61004 [PSH, ACK] Seq=4...
17	0.420365	10.10.50.201	10.10.50.201	TCP	187	61004 → 3389 [PSH, ACK] Seq=3...
18	0.420365	10.10.50.201	10.10.50.201	TCP	91	3389 → 61004 [PSH, ACK] Seq=4...
19	0.420365	10.10.50.201	10.10.50.201	TCP	123	3389 → 61004 [PSH, ACK] Seq=4...
20	0.430365	10.10.50.201	10.10.50.201	TCP	60	61004 → 3389 [ACK] Seq=171 Ac...
21	0.450365	10.10.50.201	10.10.50.201	TCP	187	3389 → 61004 [PSH, ACK] Seq=4...
22	0.520365	10.10.50.201	10.10.50.201	TCP	187	61004 → 3389 [PSH, ACK] Seq=1...

Mark/Unmark Packet Ctrl+M

Ignore/Unignore Packet Ctrl+D

Set/Unset Time Reference Ctrl+T

Time Shift... Ctrl+Shift+T

Packet Comment... Ctrl+Alt+C

Edit Resolved Name

Apply as Filter

Prepare a Filter

Conversation Filter

Colorize Conversation

SCTP

Follow

TCP Stream

UDP Stream

SSL Stream

HTTP Stream

Copy

Protocol Preferences

Decode As...

Show Packet in New Window

Frame 7: 61004 → 3389 [ACK] Seq=1 Ack=...

Interface 0

Encapsulated

Arrival

0000 00 0c ..)....gE.

0010 00 28 .(o.@... /v..._...

0020 32 c9 2..L.=.pP.

0030 03 51 3c 22 00 00 00 00 00 00 00 00 .Q<"....

wireshark_1487DC24-2D00-4600-A773-6D93C2AEAD5E_20180213231135_a03984

Packets: 220 · Displayed: 220 (100.0%) Profile: Default

Figure 8–26: Wireshark Network Analyzer

Examine the data from the captured packet, as shown in Figure 8–27.

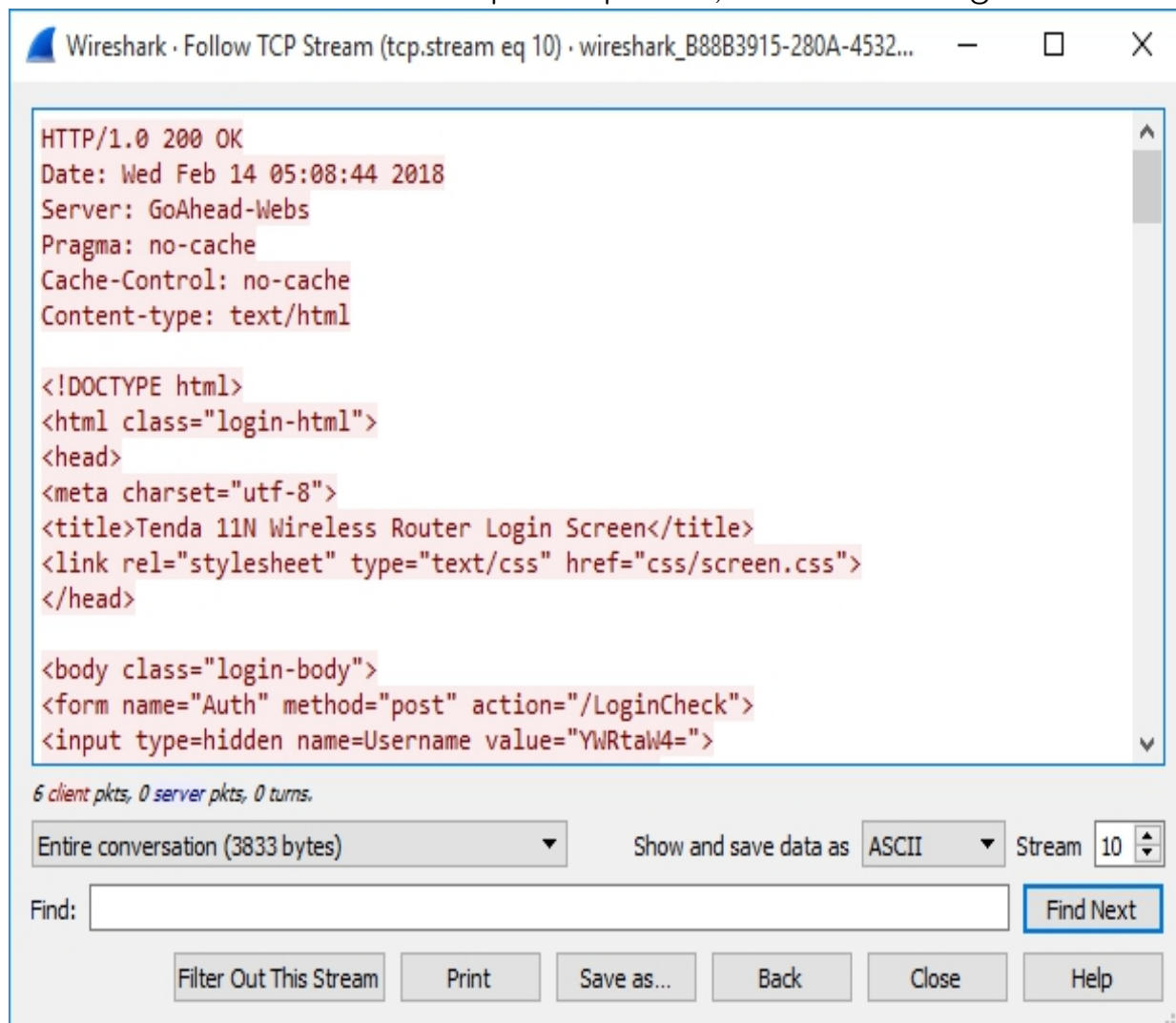


Figure 8–27: Wireshark Network Analyzer

Filters in Wireshark

Following are the Wireshark filters for filtering 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 practices against Sniffing include the following approaches to protecting 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

Ping Method

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

ARP Method

Using ARP, sniffers can be detected with the help of the ARP Cache. By sending a nonbroadcast ARP packet to the sniffer, the MAC address will be cached if the NIC is running in promiscuous mode. The next step is to send a broadcast ping with a spoofed MAC address. If the machine is running in promiscuous mode, it replies to the packets of the known MAC address from the sniffed non-broadcasted ARP packets.

Promiscuous Detection Tool

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

Mind Map

