Attacking the Foundation

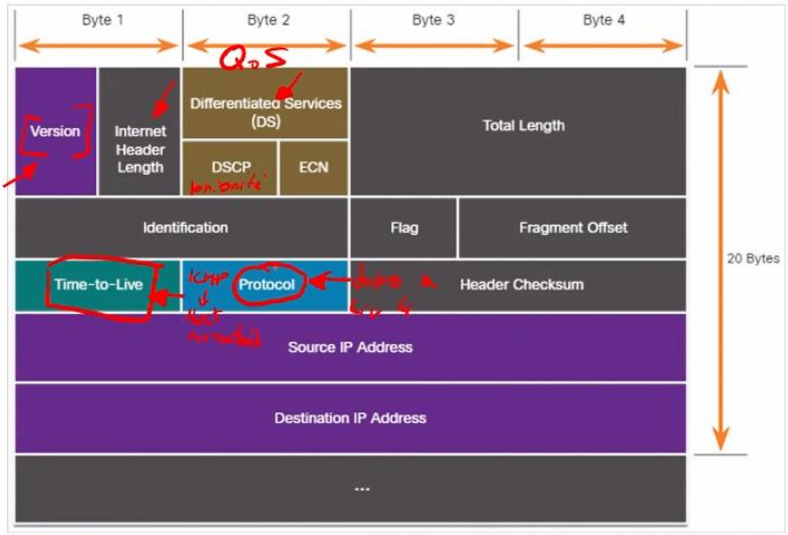
IPv4 and IPv6

- IP was designed as a Layer 3 connectionless protocol. It provides the necessary functions to deliver a packet from a source host to a destination host over an interconnected system of networks.
- IP makes no effort to validate whether the source IP address contained in a packet actually came from that source. For this reason, threat actors can send packets using a spoofed source IP address.
- Also, threat actors can tamper with the other fields in the IP header to carry out their attacks. So, it is important for security analysts to understand the different fields in both the IPv4 and IPv6 headers.

Attacking the Foundation

The IPv4 Packet Header

The fields in the IPv4 packet header are shown in the figure. There are 10 fields in the IPv4 packet header.



Attacking the Foundation

The IPv4 Packet Header (Contd.)

The following table describes the IPv4 header fields:

IPv4 Header Field	Description
Version	• Contains a 4-bit binary value set to 0100 that identifies this as an IPv4 packet.
Internet Header length	• A 4-bit field containing the length of the IP header. • The minimum length of an IP header is 20 bytes.
Differentiated Services or DiffServ (DS)	• Formerly called the Type of Service (ToS) field, the DS field is an 8-bit field used to determine the priority of each packet. • The six most significant bits of the DiffServ field are the Differentiated Services Code Point (DSCP). • The last two bits are the Explicit Congestion Notification (ECN) bits.
Total length	• Specifies the length of the IP packet including the IP header and the user data. • The total length field is 2 bytes, so the maximum size of an IP packet is 65,535 bytes.

Attacking the Foundation

The IPv4 Packet Header (Contd.)

IPv4 Header Field	Description
Identification, Flag, and Fragment offset	• As an IP packet moves, it might need to cross a route that cannot handle the size of the packet. The packet will be divided, or fragmented, into smaller packets and reassembled later. • These fields are used to fragment and reassemble packets.
Time-to-Live (TTL)	• Contains an 8-bit binary value that is used to limit the lifetime of a packet. • The packet sender sets the initial TTL value, and it is decreased by one each time the packet is processed by a router. • If the TTL field decrements to zero, the router discards the packet and sends an Internet Control Message Protocol (ICMP) Time Exceeded message to the source IP address.
Protocol	• Field is used to identify the next level protocol. • This 8-bit binary value indicates the data payload type that the packet is carrying, which enables the network layer to pass the data to the appropriate upper-layer protocol. • Common values include ICMP (1), TCP (6), and UDP (17).

Attacking the Foundation

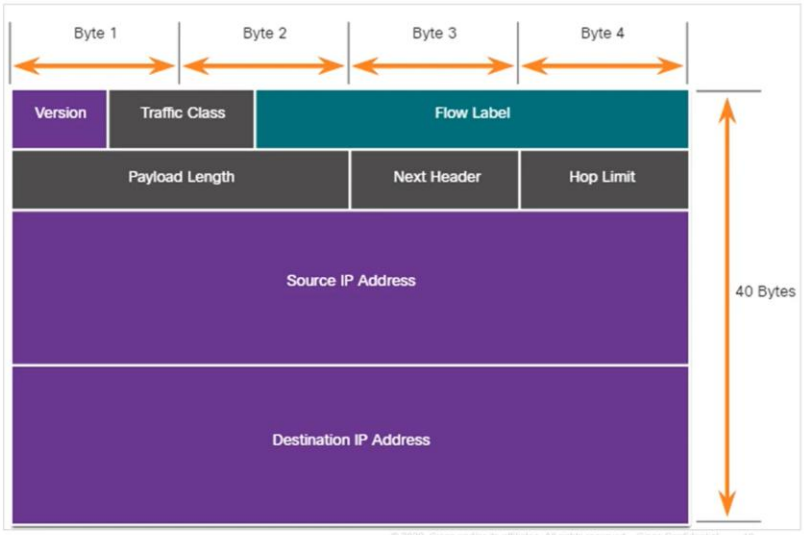
The IPv4 Packet Header (Contd.)

IPv4 Header Field	Description
Header checksum	• A value that is calculated based on the contents of the IP header. • Used to determine if any errors have been introduced during transmission.
Source IPv4 Address	• Contains a 32-bit binary value that represents the source IPv4 address of the packet. • The source IPv4 address is always a unicast address.
Destination IPv4 Address	• Contains a 32-bit binary value that represents the destination IPv4 address of the packet.
Options and Padding	• This is a field that varies in length from 0 to a multiple of 32 bits. • If the option values are not a multiple of 32 bits, 0s are added or padded to ensure that this field contains a multiple of 32 bits.

Attacking the Foundation

The IPv6 Packet Header

There are eight fields in the IPv6 packet header, as shown in the figure.



Attacking the Foundation

The IPv6 Packet Header (Contd.)

The following table describes the IPv6 header fields:

IPv6 Header Field	Description
Version	• This field contains a 4-bit binary value set to 0110 that identifies this as an IPv6 packet.
Traffic Class	• This 8-bit field is equivalent to the IPv4 Differentiated Services (DS) field.
Flow Label	• This 20-bit field suggests that all packets with the same flow label receive the same type of handling by routers.
Payload Length	• This 16-bit field indicates the length of the data portion or payload of the IPv6 packet.
Next Header	• This 8-bit field is equivalent to the IPv4 Protocol field. • It indicates the data payload type that the packet is carrying, enabling the network layer to pass the data to the appropriate upper-layer protocol.

Attacking the Foundation

The IPv6 Packet Header (Contd.)

IPv6 Header Field	Description
Hop Limit	• This 8-bit field replaces the IPv4 TTL field. • This value is decremented by a value of 1 by each router that forwards the packet. • When the counter reaches 0, the packet is discarded, and an ICMPv6 Time Exceeded message is forwarded to the sending host, indicating that the packet did not reach its destination because the hop limit was exceeded.
Source IPv6 Address	• This 128-bit field identifies the IPv6 address of the sending host.
Destination IPv6 Address	• This 128-bit field identifies the IPv6 address of the receiving host.

- An IPv6 packet also contain extension headers (EH) that provide optional network layer information.
- Extension headers are optional and are placed between the IPv6 header and the payload. EHs are used for fragmentation, security, to support mobility, and more.

16.2 IP Vulnerabilities

IP Vulnerabilities

IP Vulnerabilities

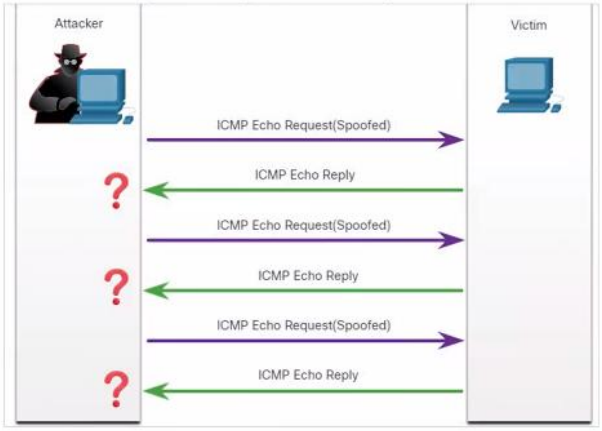
The following table lists some of the common IP-related attacks:

IP Attacks	Description
ICMP attacks	Threat actors use Internet Control Message Protocol (ICMP) echo packets (pings) to discover subnets and hosts on a protected network, to generate DoS flood attacks, and to alter host routing tables.
DoS attacks	Threat actors attempt to prevent legitimate users from accessing information or services.
DDoS attacks	Similar to a DoS attack, but features a simultaneous, coordinated attack from multiple source machines.
Address spoofing attacks	Threat actors spoof the source IP address in an attempt to perform blind spoofing or non-blind spoofing.
Man-in-the-middle attack (MiTM)	Threat actors position themselves between a source and destination to transparently monitor, capture, and control the communication. They could simply eavesdrop by inspecting captured packets or alter packets and forward them to their original destination.
Session hijacking	Threat actors gain access to the physical network, and then use an MiTM attack to hijack a session.

IP Vulnerabilities

ICMP Attacks

- ICMP was developed to carry diagnostic messages and to report error conditions when routes, hosts, and ports are unavailable. ICMP messages are generated by devices when a network error or outage occurs.
- The ping command is a user-generated ICMP message, called an echo request, that is used to verify connectivity to a destination.
- Threat actors use ICMP for reconnaissance and scanning attacks.
- Threat actors also use ICMP for DoS and DDoS attacks, as shown in the ICMP flood attack in the figure.



***Note**: ICMP for IPv4 (ICMPv4) and ICMP for IPv6 (ICMPv6) are susceptible to similar types of attacks.*

IP Vulnerabilities

ICMP Attacks (Contd.)

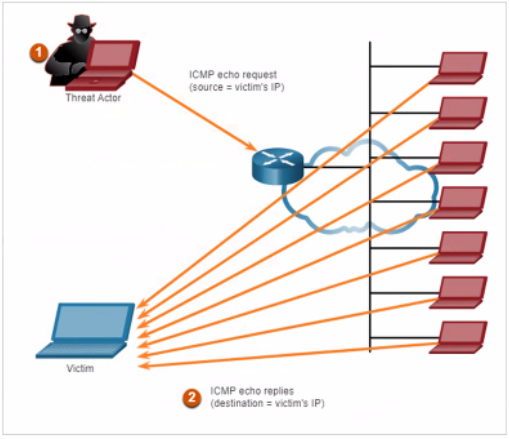
- Networks should have strict ICMP access control list (ACL) filtering on the network edge to avoid ICMP probing from the internet.
- The following table lists the common ICMP messages of interest to threat actors.

ICMP Message	Description
ICMP echo request and echo reply	This is used to perform host verification and DoS attacks.
ICMP unreachable	This is used to perform network reconnaissance and scanning attacks.
ICMP mask reply	This is used to map an internal IP network.
ICMP redirects	This is used to lure a target host into sending all traffic through a compromised device and create a MITM attack.
ICMP router discovery	This is used to inject bogus route entries into the routing table of a target host.

IP Vulnerabilities

Amplification and Reflection Attacks

- Threat actors often use amplification and reflection techniques to create DoS attacks.
- The figure shows how an amplification and reflection technique called a Smurf attack is used to overwhelm a target host.
  - **Amplification** - The threat actor forwards ICMP echo request messages to many hosts. These messages contain the source IP address of the victim.
  - **Reflection** - These hosts all reply to the spoofed IP address of the victim to overwhelm it.
- Threat actors also use resource exhaustion attacks.



***Note**: Newer forms of amplification and reflection attacks such as DNS-based reflection and amplification attacks and Network Time Protocol (NTP) amplification attacks are now being used.*

IP Vulnerabilities

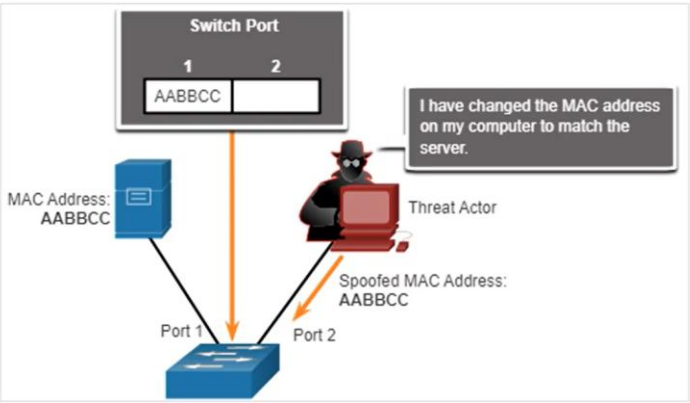
Address Spoofing Attacks

- IP address spoofing attacks occur when a threat actor creates packets with false source IP address information to either hide the identity of the sender, or to pose as another legitimate user.
- The threat actor can then gain access to otherwise inaccessible data or circumvent security configurations.
- Spoofing is usually incorporated into another attack such as a Smurf attack.
- Spoofing attacks can be non-blind or blind:
  - **Non-blind spoofing** - The threat actor can see the traffic that is being sent between the host and the target. The threat actor uses non-blind spoofing to inspect the reply packet from the target victim. Non-blind spoofing determines the state of a firewall and sequence-number prediction. It can also hijack an authorized session.
  - **Blind spoofing** - The threat actor cannot see the traffic that is being sent between the host and the target. Blind spoofing is used in DoS attacks.

IP Vulnerabilities

Address Spoofing Attacks (Contd.)

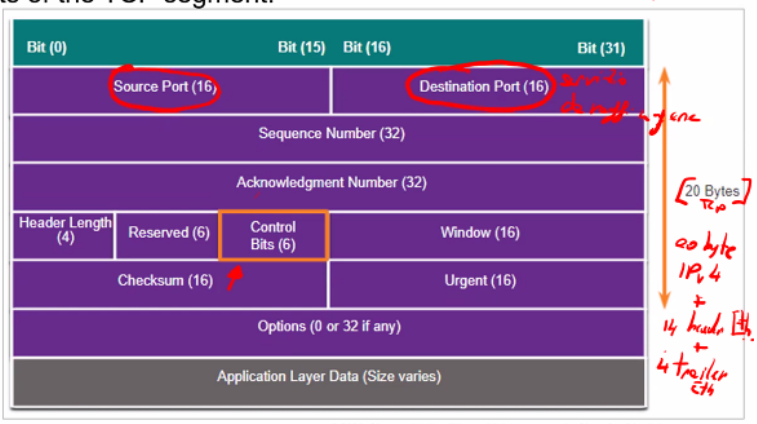
- MAC address spoofing attacks are used when threat actors have access to the internal network.
- Threat actors alter the MAC address of their host to match another known MAC address of a target host, as shown in the figure.
- The attacking host then sends a frame throughout the network with the newly-configured MAC address.
- When the switch receives the frame, it examines the source MAC address.



16.3 TCP and UDP Vulnerabilities

TCP Segment Header

- TCP segment information appears immediately after the IP header. The fields of the TCP segment and the flags for the Control Bits field are displayed in the figure.
- The following are the six control bits of the TCP segment:
  - **URG** - Urgent pointer field significant
  - **ACK** - Acknowledgment field significant
  - **PSH** - Push function
  - **RST** - Reset the connection
  - **SYN** - Synchronize sequence numbers
  - **FIN** - No more data from sender



TCP Services

TCP provides these services:

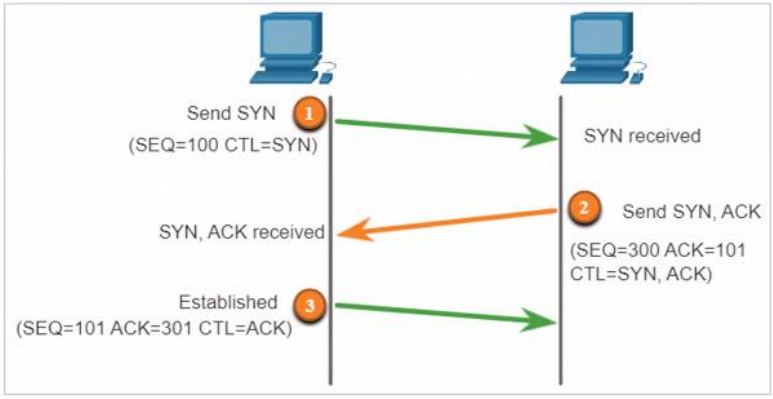
- **Reliable delivery** - TCP incorporates acknowledgments to guarantee delivery, instead of relying on upper-layer protocols to detect and resolve errors. If a timely acknowledgment is not received, the sender retransmits the data. Requiring acknowledgments of received data can cause substantial delays. Examples of application layer protocols that make use of TCP reliability include HTTP, SSL/TLS, FTP, DNS zone transfers, and others.
- **Flow control** - TCP implements flow control to address this issue. Rather than acknowledge one segment at a time, multiple segments can be acknowledged with a single acknowledgment segment.
- **Stateful communication** - TCP stateful communication between two parties occurs during the TCP three-way handshake. Before data can be transferred using TCP, a three-way handshake opens the TCP connection. If both sides agree to the TCP connection, data can be sent and received by both parties using TCP.

TCP Services (Contd.)

TCP Three-Way Handshake

A TCP connection is established in three steps:

- The initiating client requests a client-to-server communication session with the server.
- The server acknowledges the client-to-server communication session and requests a server-to-client communication session.
- The initiating client acknowledges the server-to-client communication session.

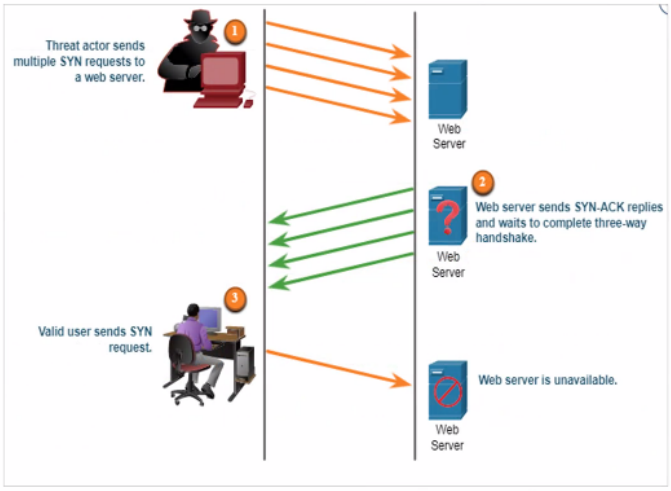


TCP Attacks

Network applications use TCP or UDP ports. Threat actors conduct port scans of target devices to discover which services they offer.

TCP SYN Flood Attack

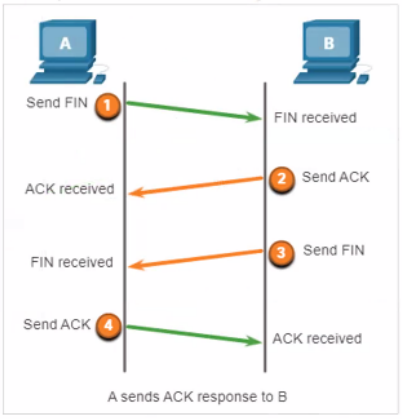
- The TCP SYN Flood attack exploits the TCP three-way handshake.
- The figure shows a threat actor continually sending TCP SYN session request packets with a randomly spoofed source IP address to a target.
- The target replies with a TCP SYN-ACK packet to the spoofed IP address and waits for a TCP ACK packet. Those responses never arrive.
- The target host has too many half-open TCP connections, and TCP services are denied to legitimate users.



TCP Attacks (Contd.)

TCP Reset Attack

- A TCP reset attack can be used to terminate TCP communications between two hosts.
- A threat actor could do a TCP reset attack and send a spoofed packet containing a TCP RST to one or both endpoints.
- Terminating a TCP session uses the following four-way exchange process:
- When the client has no more data to send in the stream, it sends a segment with the FIN flag set.
- The server sends an ACK to acknowledge the receipt of the FIN to terminate the session from client to server.
- The server sends a FIN to the client to terminate the server-to-client session.
- The client responds with an ACK to acknowledge the FIN from the server.



TCP Attacks (Contd.)

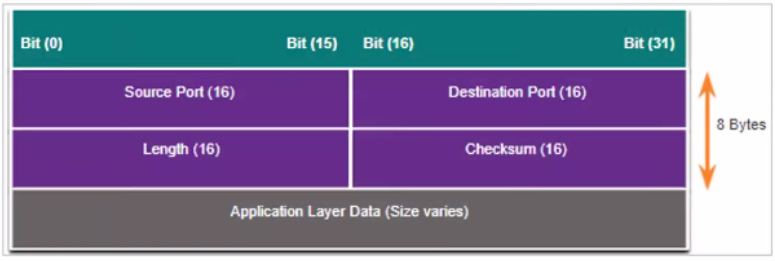
TCP Session Hijacking

- TCP session hijacking is another TCP vulnerability.
- A threat actor takes over an already-authenticated host as it communicates with the target.
- The threat actor must spoof the IP address of one host, predict the next sequence number, and send an ACK to the other host.
- If successful, the threat actor could send, but not receive, data from the target device.

TCP and UDP Vulnerabilities

UDP Segment Header and Operation

- UDP is commonly used by DNS, DHCP, TFTP, NFS, and SNMP.
- It is also used with real-time applications such as media streaming or VoIP. UDP is a connectionless transport layer protocol.
- The UDP segment structure, shown in the figure, is much smaller than TCP.
- Although UDP is normally called unreliable, this does not mean that applications that use UDP are always unreliable. It means that these functions are not provided by the transport layer protocol and must be implemented elsewhere if required.



- The low overhead of UDP makes it very desirable for protocols that make simple request and reply transactions.

TCP and UDP Vulnerabilities

UDP Attacks

- UDP is not protected by any encryption. Encryption can be added to UDP, but it is not available by default.
- The lack of encryption means that anyone can see the traffic, change it, and send it on to its destination.

UDP Flood Attacks

- In a UDP flood attack, all the resources on a network are consumed.
- The threat actor must use a tool like UDP Unicorn or Low Orbit Ion Cannon. These tools send a flood of UDP packets, often from a spoofed host, to a server on the subnet.
- The program will sweep through all the known ports trying to find closed ports. This will cause the server to reply with an ICMP port unreachable message.
- As there are many closed ports on the server, this creates a lot of traffic on the segment, which uses up most of the bandwidth. The result is very similar to a DoS attack.

16.4 Attacking the Foundation Summary

Attacking the Foundation Summary

What Did I Learn in this Module?

- IP was designed as a Layer 3 connectionless protocol.
- The IPv4 header consists of several fields while the IPv6 header contains fewer fields. It is important for security analysts to understand the different fields in both the IPv4 and IPv6 headers.
- There are different types of attacks that target IP. Common IP-related attacks include:
  - ICMP attacks
  - Denial-of-Service (DoS) attacks
  - Distributed Denial-of-Service (DoS) attacks
  - Address spoofing attacks
  - Man-in-the-middle attack (MiTM)
  - Session hijacking

Attacking the Foundation Summary

What Did I Learn in this Module? (Contd.)

- ICMP was developed to carry diagnostic messages and to report error conditions when routes, hosts, and ports are unavailable.
- TCP segment and UDP datagram information appear immediately after the IP header. It is important to understand Layer 4 headers and their functions in data communication.
- Threat actors can conduct a variety of TCP related attacks:
  - TCP port scans
  - TCP SYN Flood attack
  - TCP Reset Attack
  - TCP Session Hijacking attack
- The UDP segment (i.e., datagram) is much smaller than the TCP segment, which makes it very desirable for use by protocols that make simple request and reply transactions such as DNS, DHCP, SNMP, and others.

