Module 5:Network Protocols

Instructor Materials

CyberOps Associates v1.0

Module Objectives

Module Title: Network Protocols

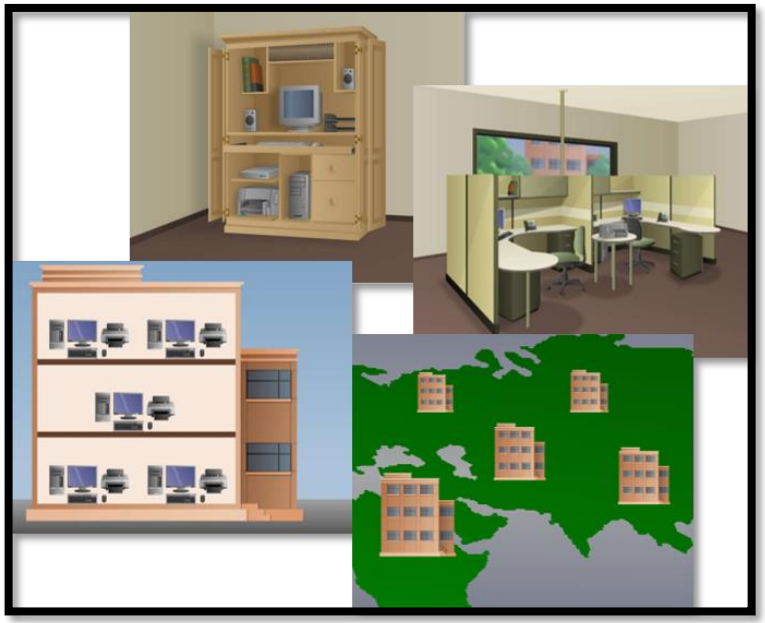
Module Objective: Explain how protocols enable network operations.

Topic Title	Topic Objective
Network Communications Process	Explain the basic operation of data networked communications.
Communications Protocols	Explain how protocols enable network operations.
Data Encapsulation	Explain how data encapsulation allows data to be transported across the network.

5.1 Network Communications Process

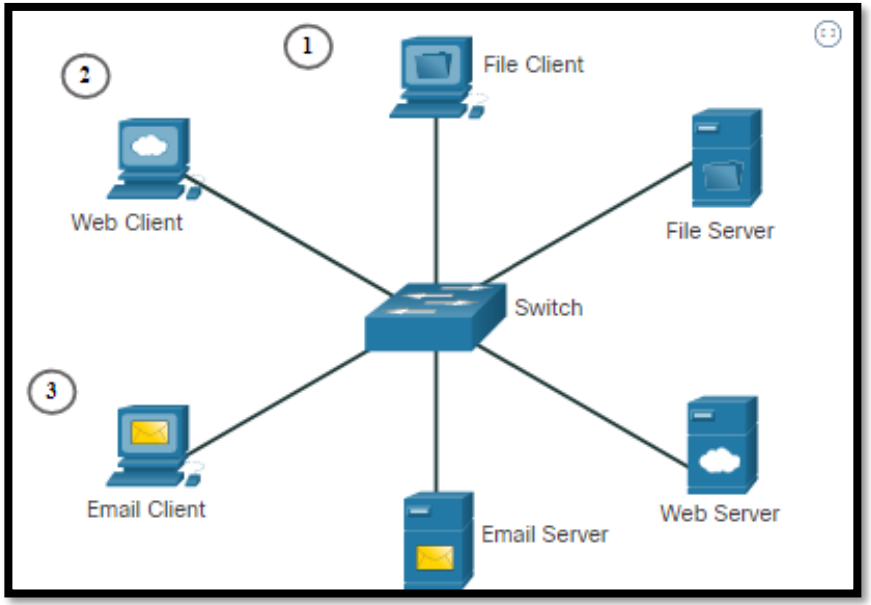
Networks of Many Sizes

- **Small Home networks:** Small home networks connect a few computers to each other and to the internet.
- **Small Office and Home Office (SOHO) networks:** The SOHO network allows a home office or a remote office to connect to a corporate network, or access centralized, shared resources.
- **Medium to Large networks**: These are used by corporations and schools and can have many locations with hundreds or thousands of interconnected hosts.
- **World Wide networks**: The internet is a network of networks that connects hundreds of millions of computers world-wide.



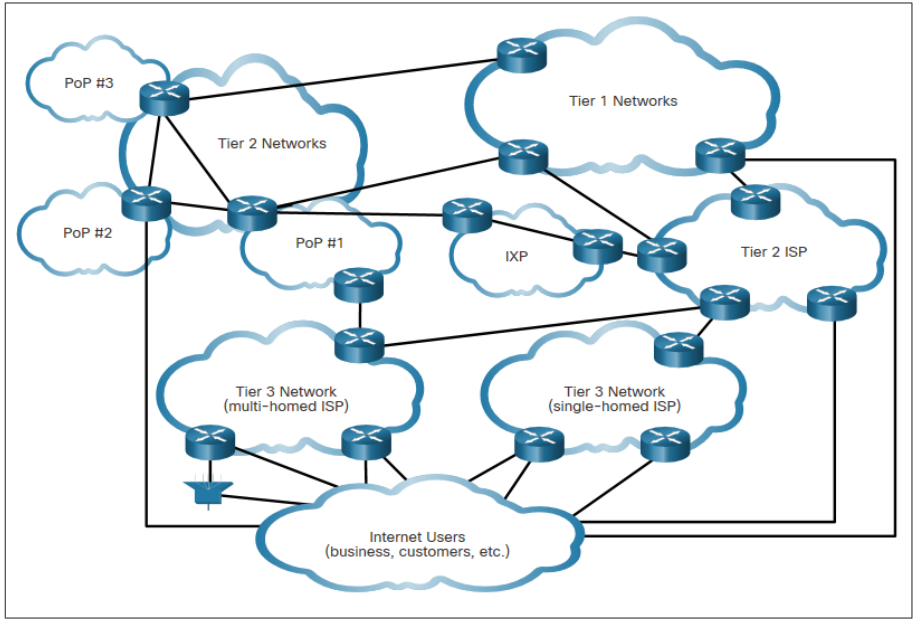
Client-Server Communications

- All computers that are connected to a network and that participate directly in network communication are classified as hosts. Hosts are also called end devices, endpoints, or nodes.
- Servers are simply computers with specialized software that enables servers to provide information to other end devices on the network.
- A server can be single-purpose, providing only one service, such as web pages or it can be multipurpose, providing a variety of services such as web pages, email, and file transfers.
- Client computers have software installed that enables them to request and display the information obtained from the server. A single computer can run multiple types of client software.



Tracing the Path (Contd.)

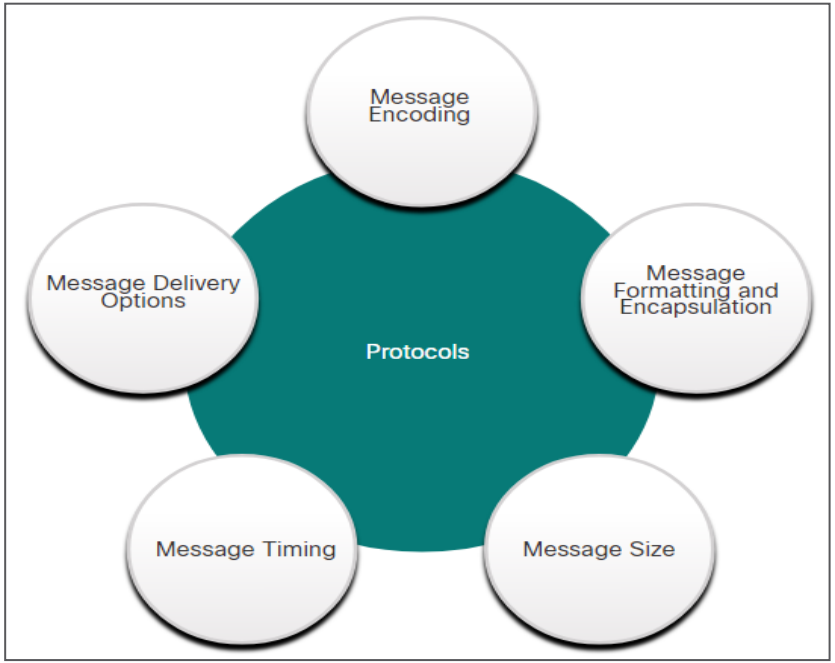
- A combination of copper and fiber-optic cables that go over land and under the ocean carry data traffic. These connections connect telecommunications facilities and ISPs distributed throughout the world.
- Global Tier 1 and Tier 2 ISPs connect portions of the internet together, usually through an Internet Exchange Point (IXP).
- Larger networks connect to Tier 2 networks through a Point of Presence (PoP), which is usually a location in the building where physical connections to the ISP are made. The Tier 3 ISPs connect homes and businesses to the internet.
- https://www.submarinecablemap.com/



5.2 Communications Protocols

What are Protocols?

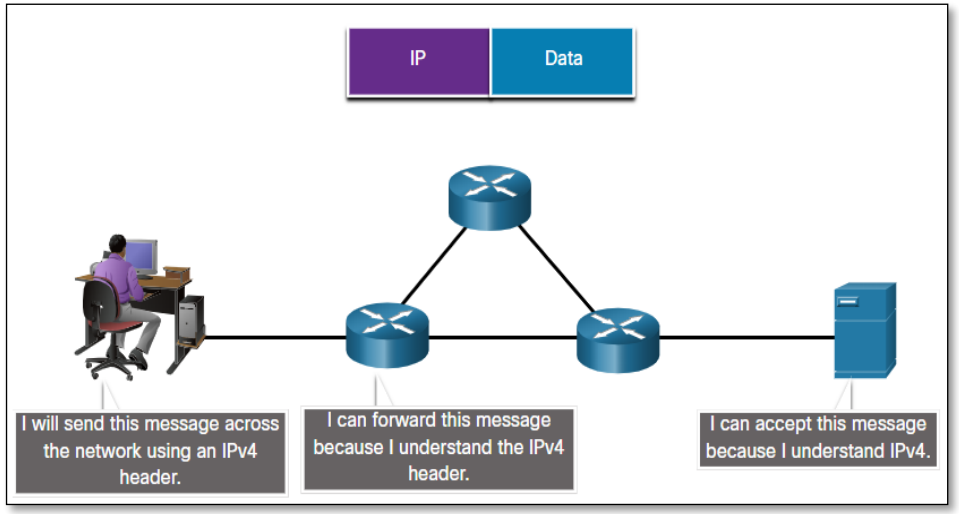
- Simply having a connection between end devices is not enough to enable communication. For communication to occur, devices must know “how” to communicate.
- Communication is governed by rules called protocols.
- These protocols are specific to the type of communication method occurring.
- Network protocols specify many features of network communication.
- Network protocols provide the means for computers to communicate on networks.
- Network protocols dictate the message encoding, formatting, encapsulation, size, timing, and delivery options.
- Networking protocols define a common format and set of rules for exchanging messages between devices.
- Some common networking protocols are Hypertext Transfer Protocol (HTTP), Transmission Control Protocol (TCP), and Internet Protocol (IP).

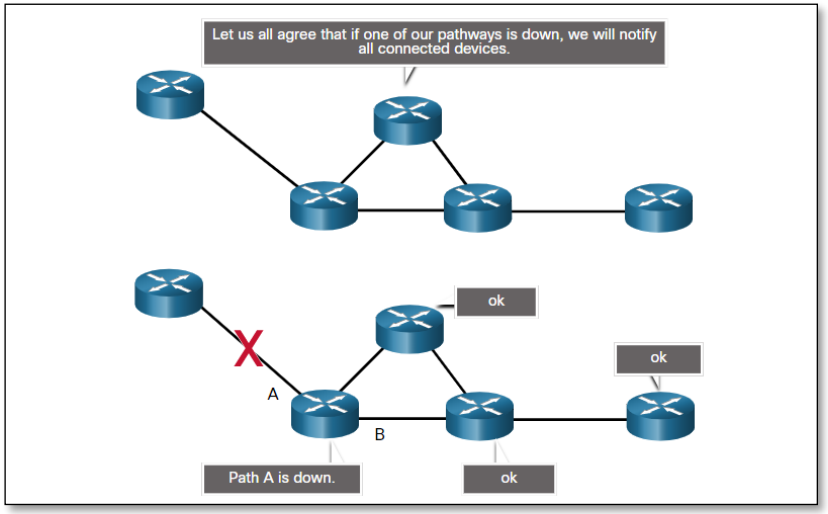


Network Protocols (Contd.)

Message Structure specifies how the message is formatted or structured.

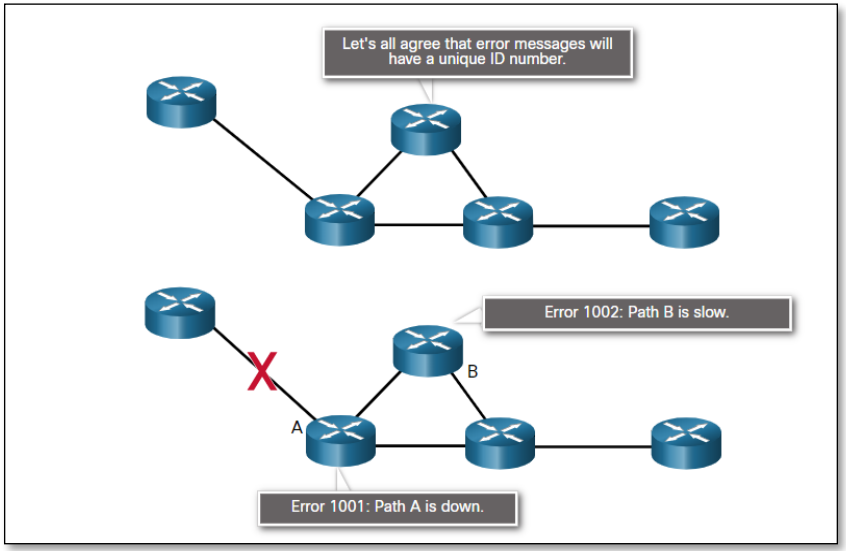
Path Sharing specifies the process by which networking devices share information about pathways with other networks.



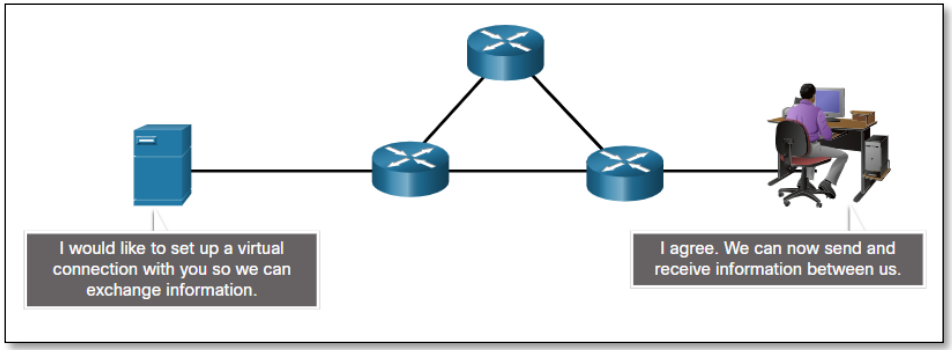


Network Protocols (Contd.)

Information Sharing specifies how and when error and system messages are passed between devices.

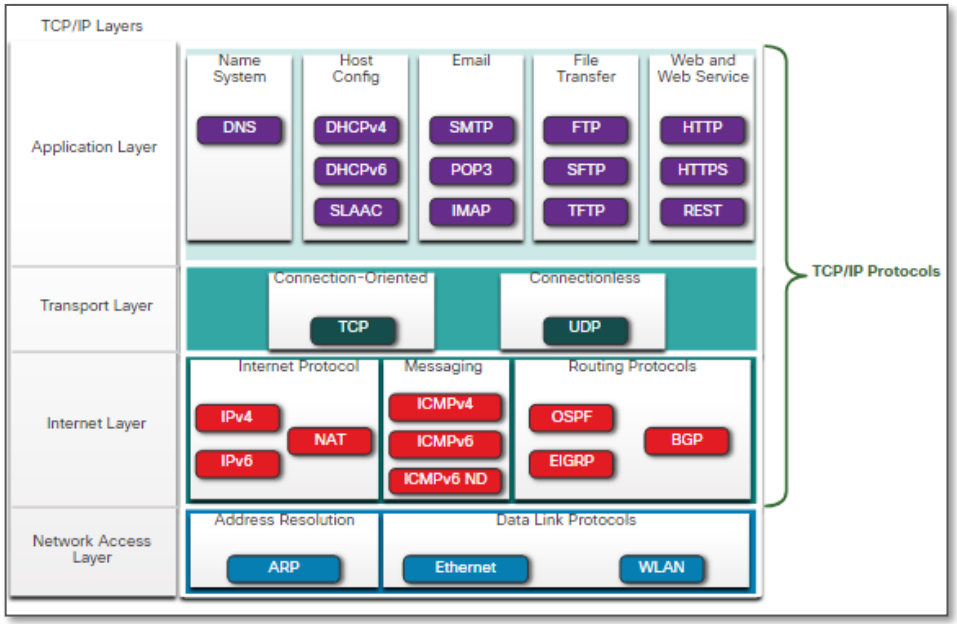


Session Management manages the setup and termination of data transfer sessions.



The TCP/IP Protocol Suite

- TCP/IP is the protocol suite used by the internet and the networks of today.
- TCP/IP has two important aspects for vendors and manufacturers:
  - Open standard protocol suite - This means it is freely available to the public and can be used by any vendor on their hardware or in their software.
  - Standards-based protocol suite - This means it has been endorsed by the networking industry and approved by a standards organization.



The TCP/IP Protocol Suite (Contd.)

Host Config

Protocol	Description
DHCPv4 (Dynamic Host Configuration Protocol for IPv4)	Dynamically assigns IPv4 addressing information to DHCPv4 clients at start-up and allows the addresses to be re-used when no longer needed.
DNS (Domain Name System)	Translates domain names into IP addresses.
DHCPv6 (Dynamic Host Configuration Protocol for IPv6)	It is similar to DHCPv4. Dynamically assigns IPv6 addressing information to DHCPv6 clients at start-up.
SLAAC (Stateless Address Autoconfiguration)	A method that allows a device to obtain its IPv6 addressing information without using a DHCPv6 server.

The TCP/IP Protocol Suite (Contd.)

Email

Protocol	Description
SMTP (Simple Mail Transfer Protocol)	Enables clients to send email to a mail server and enables servers to send email to other servers.
POP3 (Post Office Protocol version 3)	Enables clients to retrieve email from a mail server and download the email to the client's local mail application.
IMAP (Internet Message Access Protocol)	Enables clients to access email stored on a mail server as well as maintaining email on the server.

File Transfer

Protocol	Description
FTP (File Transfer Protocol)	Sets the rules that enable a user on one host to access and transfer files to and from another host over a network.
SFTP (SSH File Transfer Protocol)	Used to establish a secure file transfer session in which the file transfer is encrypted.
TFTP (Trivial File Transfer Protocol)	A simple and connectionless protocol with best-effort, unrecognized file delivery.

The TCP/IP Protocol Suite (Contd.)

Web and Web Service

Protocol	Description
HTTP (Hypertext Transfer Protocol)	A set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the World Wide Web.
HTTPS (HTTP Secure)	A secure form of HTTP that encrypts the data that is exchanged over the World Wide Web.
REST (Representational State Transfer)	A web service that uses application programming interfaces (APIs) and HTTP requests to create web applications

The TCP/IP Protocol Suite (Contd.)

- Transport Layer
  - **Connection-Oriented** - TCP (Transmission Control Protocol): Enables reliable communication between processes running on separate hosts and provides reliable transmissions that confirm successful delivery.
  - **Connectionless** - UDP (User Datagram Protocol): Enables a process running on one host to send packets to a process running on another host.

The TCP/IP Protocol Suite (Contd.)

Internet Layer

Internet Protocol

Protocol	Description
IPv4 (Internet Protocol version 4)	Receives message segments from the transport layer, packages messages into packets, and addresses packets for end-to-end delivery over a network. IPv4 uses a 32-bit address.
IPv6 (IP version 6)	Similar to IPv4 but uses a 128-bit address.
NAT (Network Address Translation)	Translates IPv4 addresses from a private network into globally unique public IPv4 addresses.

The TCP/IP Protocol Suite (Contd.)

Messaging

Protocol	Description
ICMPv4 (Internet Control Message Protocol for IPv4)	Provides feedback from a destination host to a source host about errors in packet delivery.
ICMPv6 (ICMP for IPv6)	Similar functionality to ICMPv4 but is used for IPv6 packets.
ICMPv6 ND (ICMPv6 Neighbor Discovery)	Includes four protocol messages that are used for address resolution and duplicate address detection.

Routing Protocols

Protocol	Description
OSPF (Open Shortest Path First)	Link-state routing protocol that uses a hierarchical design based on areas. OSPF is an open standard interior routing protocol.
EIGRP (Enhanced Interior Gateway Routing Protocol)	A Cisco proprietary routing protocol that uses a composite metric based on bandwidth, delay, load and reliability.
BGP (Border Gateway Protocol)	An open standard exterior gateway routing protocol used between Internet Service Providers (ISPs).

The TCP/IP Protocol Suite (Contd.)

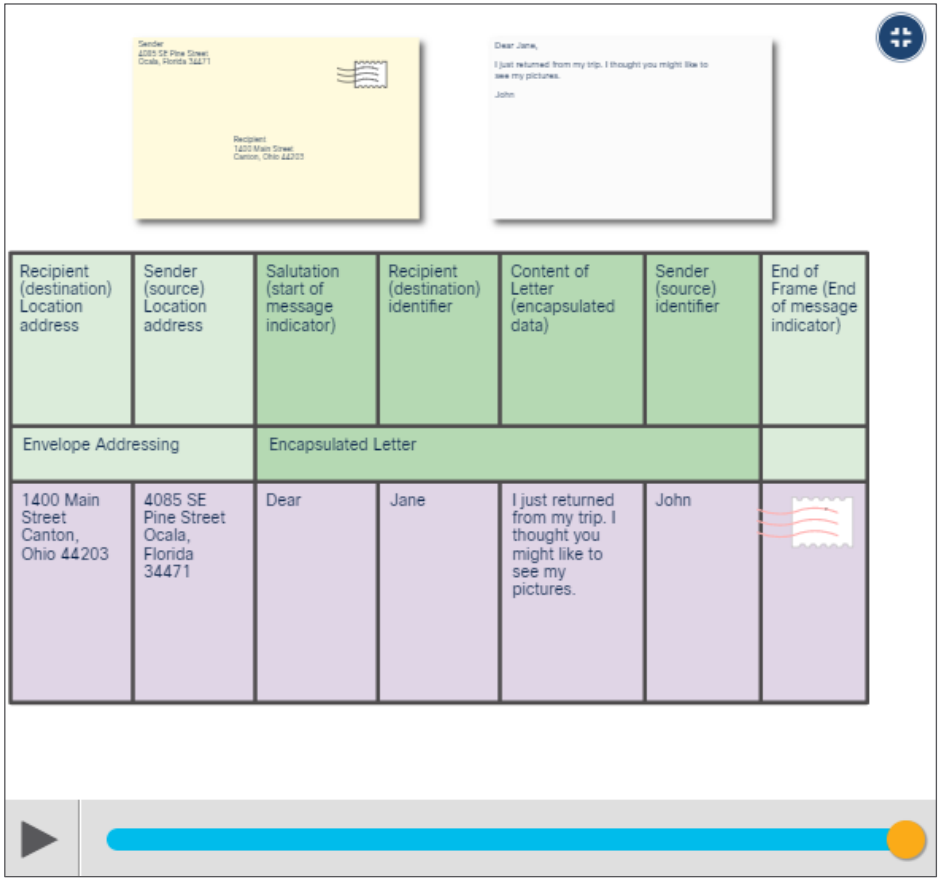
Network Access Layer

- **Address Resolution - ARP** (Address Resolution Protocol): Provides dynamic address mapping between an IPv4 address and a hardware address.
- **Data Link Protocols -**
  - **Ethernet**: Defines the rules for wiring and signaling standards of the network access layer.
  - **WLAN** (Wireless Local Area Network): Defines the rules for wireless signaling across the 2.4 GHz and 5 GHz radio frequencies.

Message Formatting and Encapsulation (Contd.)

Analogy:

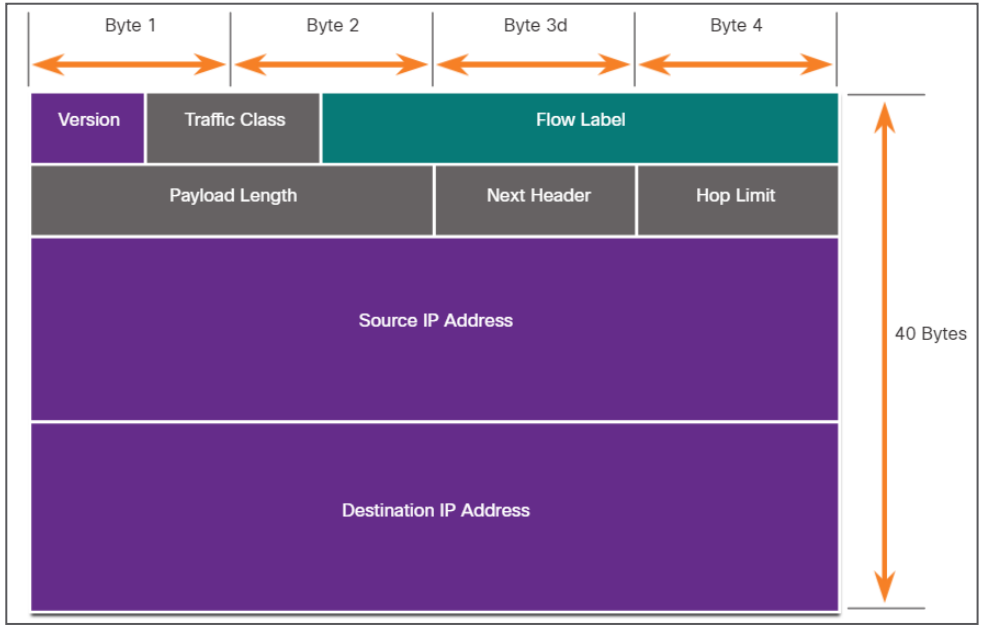
- When sending a letter, correct format is required. An envelope has the address of the sender and receiver, each located at the proper place on the envelope.
- The process of placing one message format (the letter) inside another message format (the envelope) is called encapsulation.
- De-encapsulation occurs when the process is reversed by the recipient and the letter is removed from the envelope.



Message Formatting and Encapsulation (Contd.)

Network:

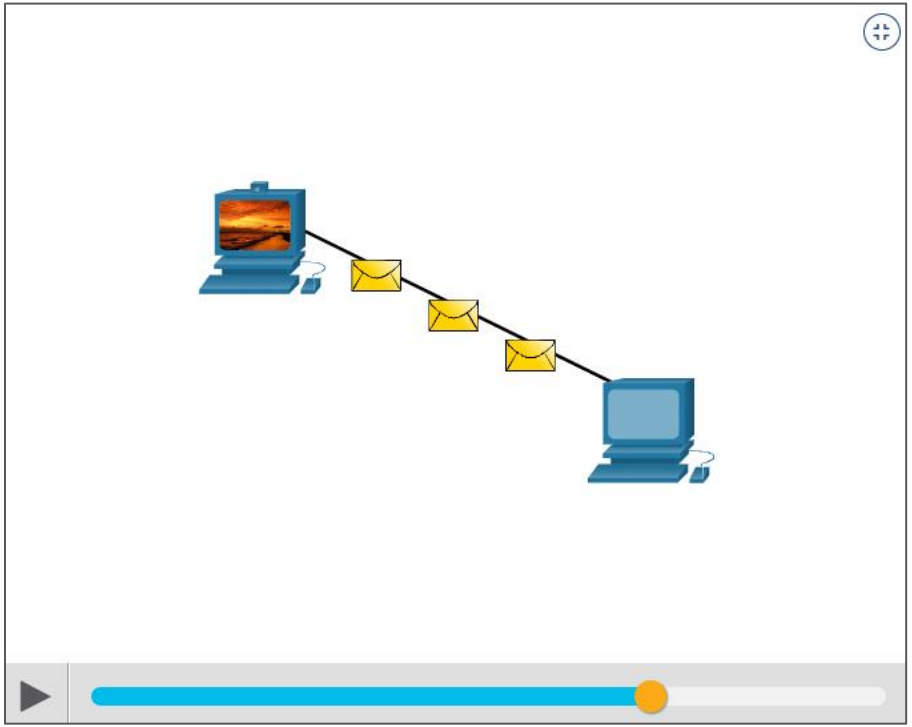
- Similar to sending a letter, a message that is sent over a computer network follows specific format rules for it to be delivered and processed.
- Internet Protocol (IP) is a protocol with a similar function to the envelope example.
- IP is responsible for sending a message from the message source to destination over one or more networks.



Message Size

Network:

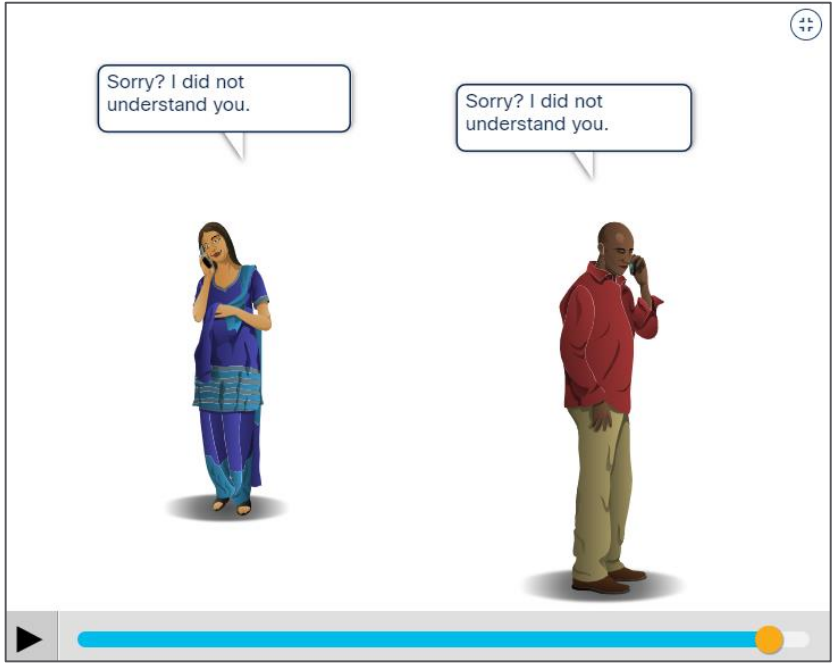
- Encoding between hosts must be in an appropriate format for the medium.
- Messages sent across the network are first converted into bits by the sending host
- Each bit is encoded into a pattern of sounds, light waves, or electrical impulses depending on the network media over which the bits are transmitted.
- The destination host receives and decodes the signals to interpret the message.



Message Timing

Message timing includes the following:

- **Flow Control -** Flow control defines how much information can be sent and the speed at which it can be delivered.
- **Response Timeout -** Hosts on the network use network protocols that specify how long to wait for responses and what action to take if a response timeout occurs.
- **Access method -** This determines when someone can send a message. When a device wants to transmit on a wireless LAN, it is necessary for the WLAN NIC to determine whether the wireless medium is available.



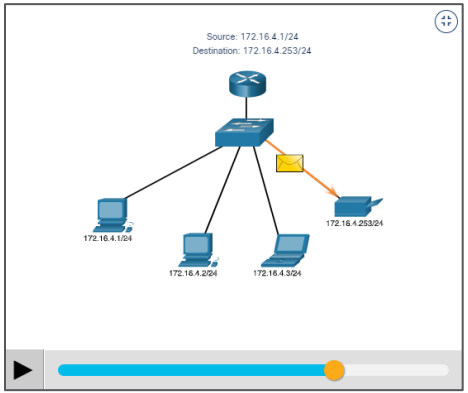
Unicast, Multicast, and Broadcast

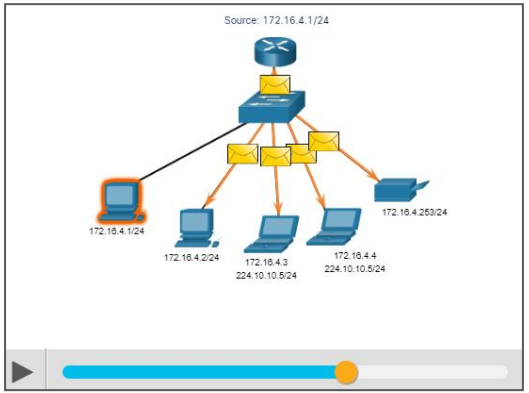
A message can be delivered in different ways. Hosts on a network various delivery options to communicate. The different methods of communication are called as unicast, multicast, and broadcast.

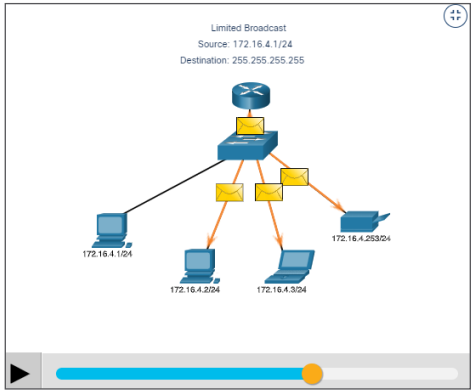
Unicast: A one-to-one delivery option means there is only a single destination for the message.

Multicast: When a host needs to send messages using a one-to many delivery option.

Broadcast: If all hosts on the network need to receive the message at the same time, a broadcast may be used. Broadcasting represents a one-to-all message delivery option.

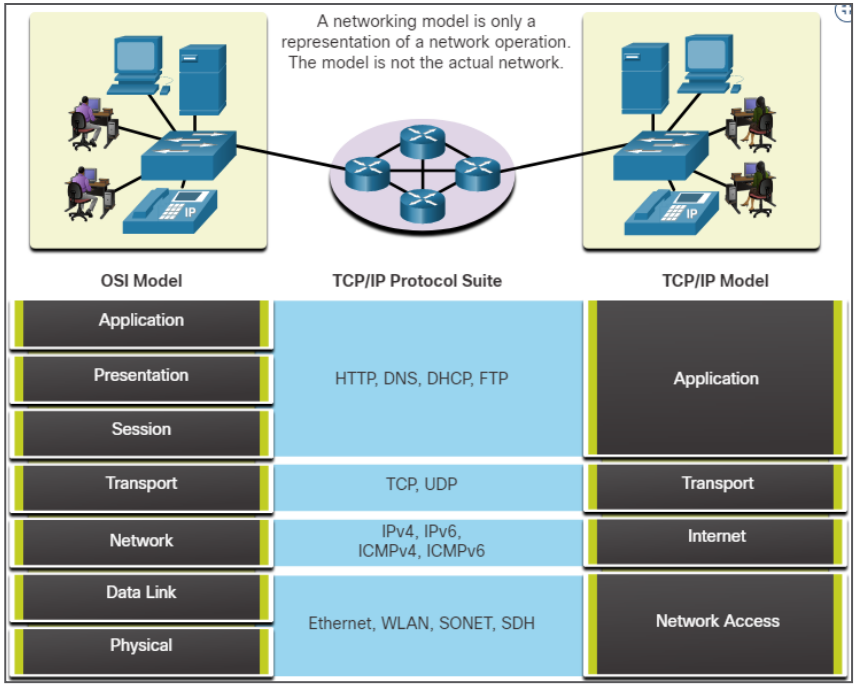






The Benefits of Using a Layered Model

- A layered model is used to modularize the operations of a network into manageable layers. These are the benefits of using a layered model:
- Assisting in protocol design
- Fostering competition
- Preventing technology or capability changes
- Providing a common language
- Two layered models that are used to describe network operations are:
  - Open System Interconnection (OSI) Reference Model
  - TCP/IP Reference Model



The OSI Reference Model (Contd.)

OSI Model Layer	Description
7 - Application	Contains protocols used for process-to-process communications
6 - Presentation	Provides representation of the data transferred between application layer services
5 - Session	Provides services to the presentation layer to organize its dialogue and to manage data exchange
4 - Transport	Defines services to segment, transfer, and reassemble the data for individual communications between the end devices
3 - Network	Provides services to exchange the individual pieces of data over the network
2 - Data Link	Describe methods for exchanging data frames between devices over a common media
1 - Physical	Describe the mechanical, electrical, functional, and procedural means to activate, maintain, and de-activate physical connections for a bit transmission between devices

The TCP/IP Protocol Model

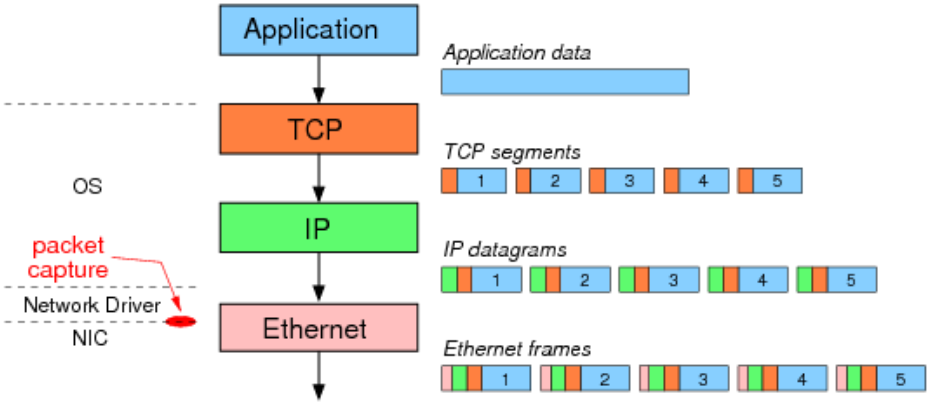
- The TCP/IP protocol model is also referred to as the internet model.
- It describes the functions that occur at each layer of protocols within the TCP/IP suite. TCP/IP is also used as a reference model.

TCP/IP Model Layer	Description
4 - Application	Represents data to the user, plus encoding and dialog control
3 - Transport	Supports communication between various devices across diverse networks
2 - Internet	Determines the best path through the network
1 - Network Access	Controls the hardware devices and media that make up the network

5.3 Data Encapsulation

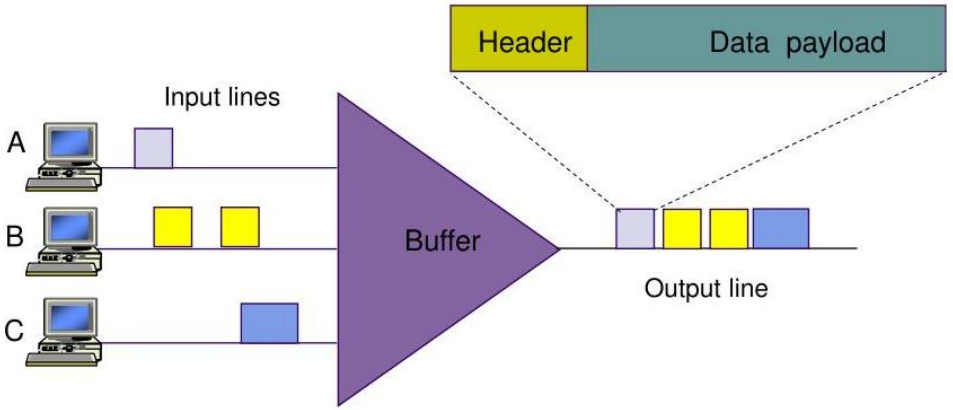
Segmenting Messages

- If large streams of data is sent across a network, it would result in delays. If any link in the interconnected network failed during the transmission, it will result in lost of complete message.
- Segmentation is the process of dividing a stream of data into smaller units for transmissions over the network.
- Segmentation is necessary as networks use the TCP/IP protocol to send data in individual IP packets. Each packet is sent separately and the packets containing segments for the same destination can be sent over different paths.



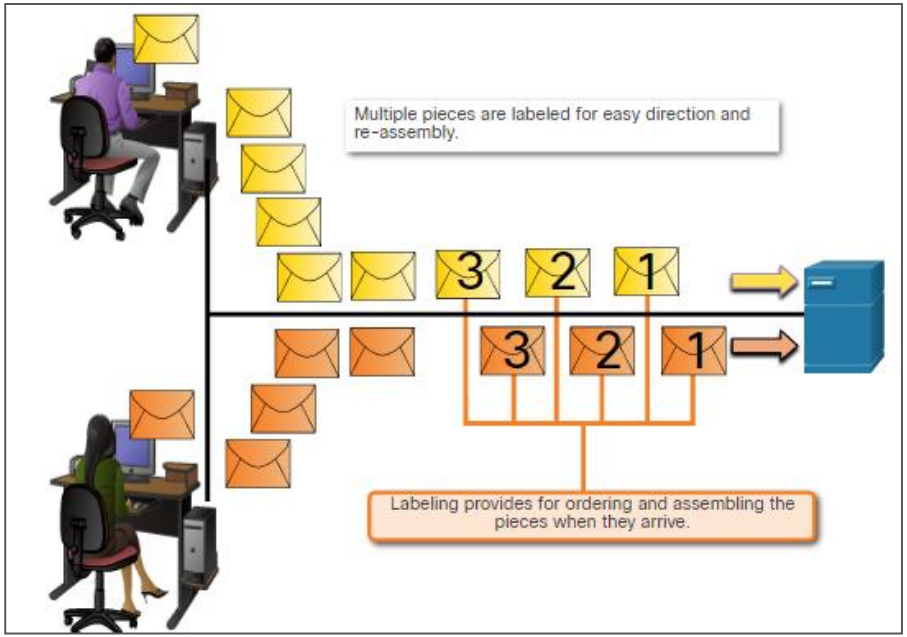
Multiplexing Messages (Contd.)

- **Increases speed -** As a large data stream is segmented into packets, more data can be sent over the network without tying up a communications link. This allows many different conversations to be interleaved on the network called multiplexing.
- **Increases efficiency -** If a single segment fails to reach its destination, only that segment needs to be retransmitted instead of resending the entire data stream.



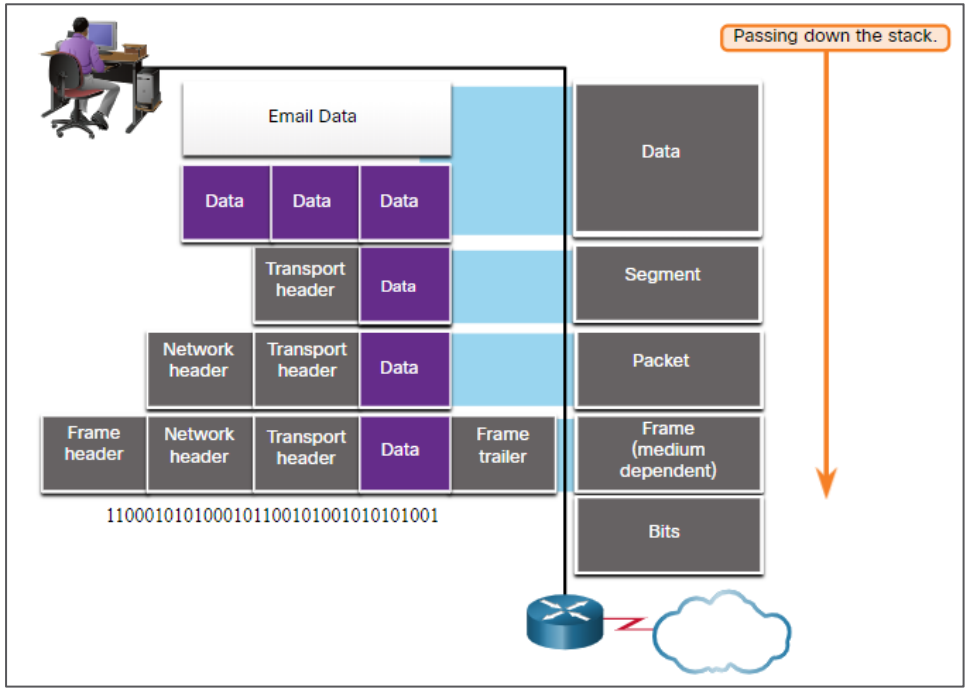
Sequencing

- While transmitting messages using segmentation and multiplexing, there is a possibility of data to reach the destination in a collapsed order.
- Each segment of the message must go through a sequencing process to ensure that it gets to the correct destination and can be reassembled similar to the content of the original message.
- TCP is responsible for sequencing the individual segments



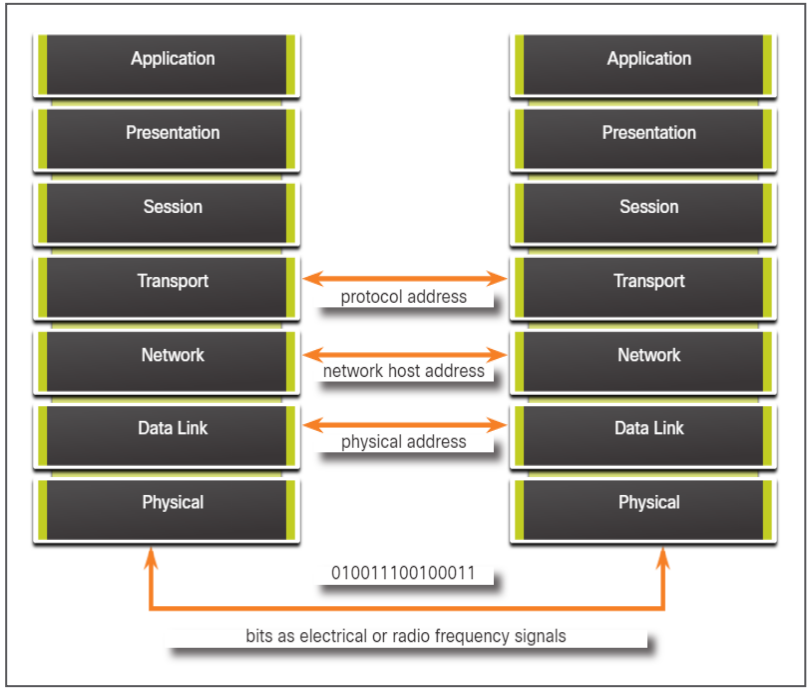
Protocol Data Units (Contd.)

- The form that a piece of data takes at any layer is called a **Protocol Data Unit (PDU)**.
- During encapsulation, each succeeding layer encapsulates the PDU that it receives from the layer above in accordance with the protocol being used.
- The PDUs for each form of data are:
  - **Data** - The general term for the PDU used at the application layer
  - **Segment** - Transport layer PDU
    - Note: If the Transport header is TCP, then it is a segment. If the Transport header is UDP then it is a datagram.
  - **Packet** - Network layer PDU
  - **Frame** - Data Link layer PDU
  - **Bits** - Physical layer PDU used when physically transmitting data over the medium



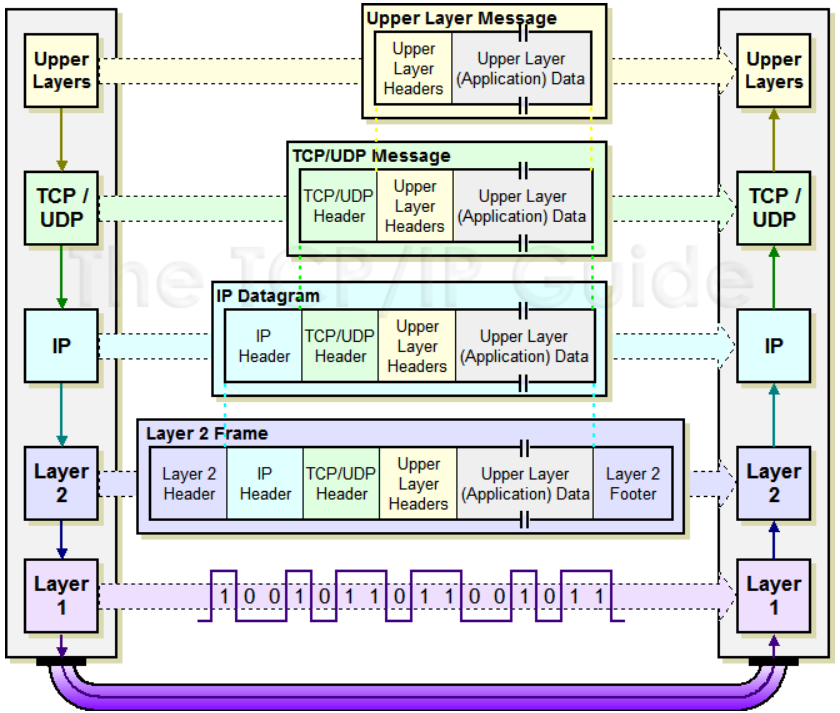
Three Addresses

- Network protocols require addresses to be used for network communication.
- The OSI transport, network, and data link layers use addressing in some form.
  - The transport layer uses protocol addresses in the form of port numbers to identify network applications.
  - The network layer specifies addresses that identify the networks that clients and servers are attached to.
  - Data link layer specifies the devices on the local LAN that should handle data frames.
- All three addresses are required for client-server communication.



Encapsulation Example

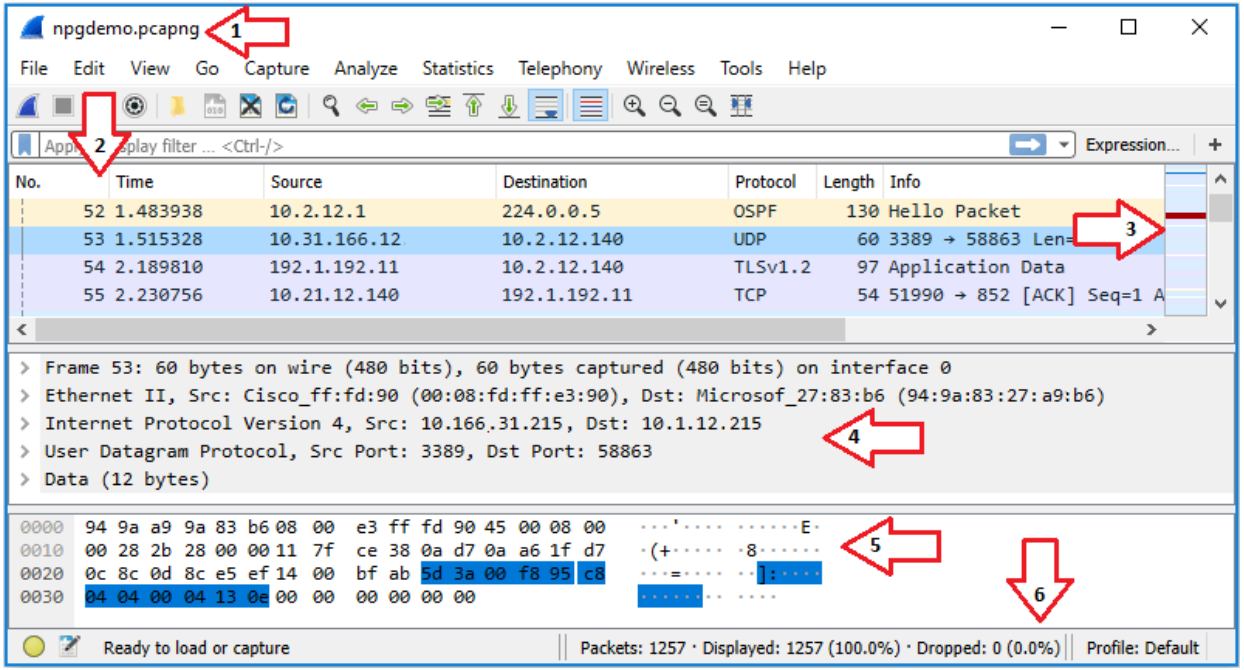
- When messages are being sent on a network, the **encapsulation** process works from top to bottom.
- At each layer, the upper layer information is considered data within the encapsulated protocol. For example, the TCP segment is considered data within the IP packet.
- This process is reversed at the receiving host and is known as **de-encapsulation**.
- De-encapsulation is the process used by a receiving device to remove one or more of the protocol headers.
- The data is de-encapsulated as it moves up the stack toward the end-user application.



Lab - Introduction to Wireshark

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education.

In this lab, you will use Wireshark to capture and analyze network traffic.



Thank you! Questions?

Vladimír Veselý

updated: 2024-02-16

https://www.fit.vutbr.cz/research/groups/nes@fit

Module 6: Ethernet and IP

Instructor Materials

CyberOps Associate v1.0

Module Objectives

Module Title: Ethernet and IP Protocol

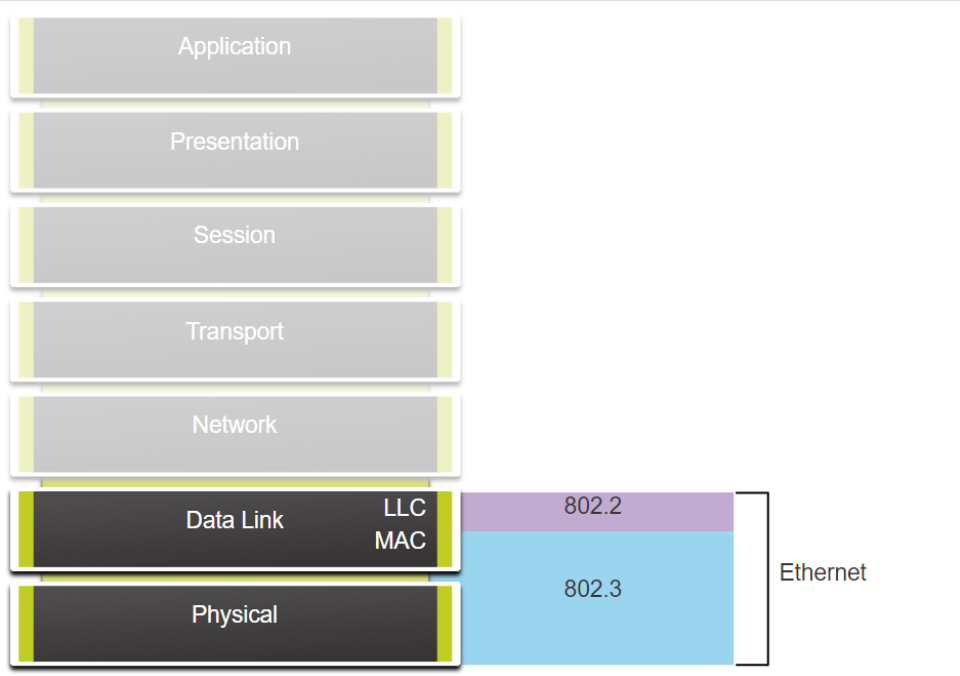
Module Objective: Explain how the Ethernet and IP protocols support network communication.

Topic Title	Topic Objective
Ethernet	Explain how Ethernet supports network communication.
IPv4	Explain how the IPv4 protocol supports network communications.
IP Addressing Basics	Explain how IP addresses enable network communication.
Types of IPv4 Addresses	Explain the types of IPv4 addresses that enable network communication.
The Default Gateway	Explain how the default gateway enables network communication.
IPv6	Explain how the IPv6 protocol supports network communications.

6.1 Ethernet

Ethernet Encapsulation

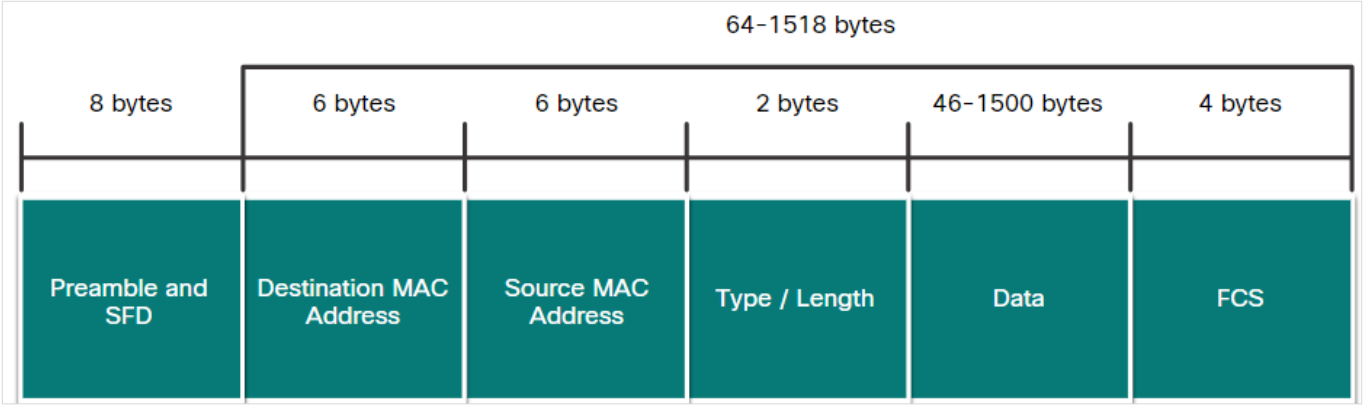
- Unlike wireless, Ethernet uses wired communications, including twisted pair, fiber-optic links, and coaxial cables.
- Ethernet operates in the data link layer and physical layer.
- It is a family of networking technologies defined in the IEEE 802.2 and 802.3 standards.
- Ethernet supports data bandwidths from 10 Mbps to 100,000 Mbps (100 Gbps)
- As seen in the figure, Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies.



Ethernet and the OSI Model

Ethernet Frame Fields

- The minimum Ethernet frame size is 64 bytes and the maximum is 1518 bytes. This includes all bytes from the destination MAC address field through the Frame Check Sequence (FCS) field.
- Any frame less than 64 bytes in length is considered a “collision fragment” or “runt frame” and is automatically discarded by receiving stations. Frames with more than 1500 bytes of data are considered “jumbo” or “baby giant frames”.



Ethernet Frame Fields

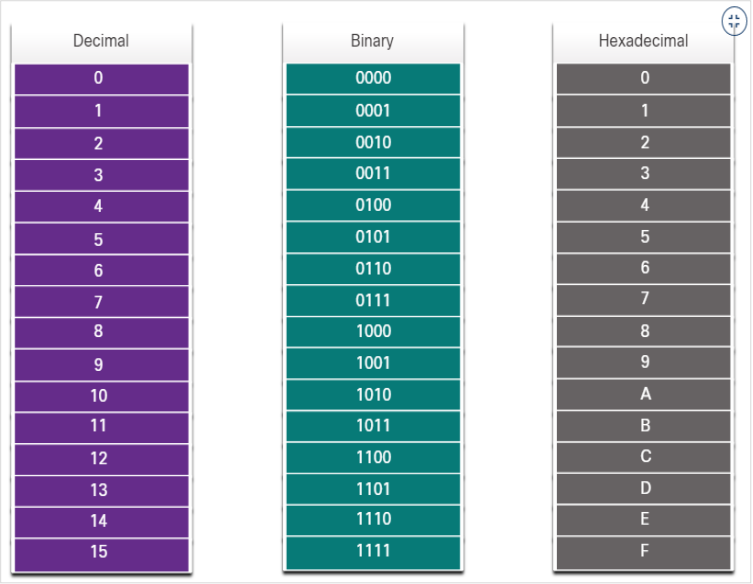
Ethernet Frame Fields

- The Ethernet fields and their description is as follows:

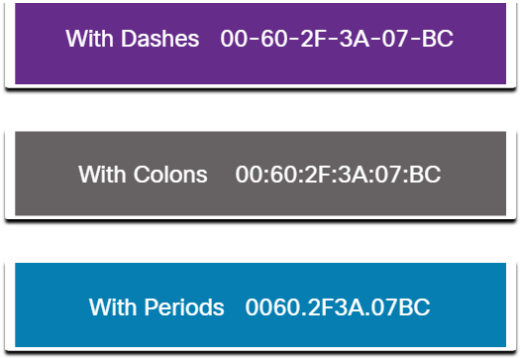
Field	Description
Preamble and Start Frame Delimiter	Used for synchronization between the sending and receiving devices.
Destination MAC Address	It is the identifier for the intended recipient. This address is used by Layer 2 to assist devices in determining if a frame is addressed to them. The address in the frame is compared to the MAC address in the device.
Source MAC Address	Identifies the originating NIC or interface of the frame.
Type / Length	Identifies the upper layer protocol encapsulated in the Ethernet frame.
Data Field	Contains the encapsulated data from a higher layer, an IPv4 packet.
Frame Check Sequence	Used to detect errors in a frame using Cyclic Redundancy Check (CRC).

MAC Address Format

- An Ethernet MAC address is a 48-bit binary value expressed as 12 hexadecimal digits.
- Hexadecimal digits uses numbers 0 to 9 and the letters A to F.
- Hexadecimal is commonly used to represent binary data.
- All data that travels on the network is encapsulated in Ethernet frames.



Decimal and Binary Equivalents of 0 to F Hexadecimal

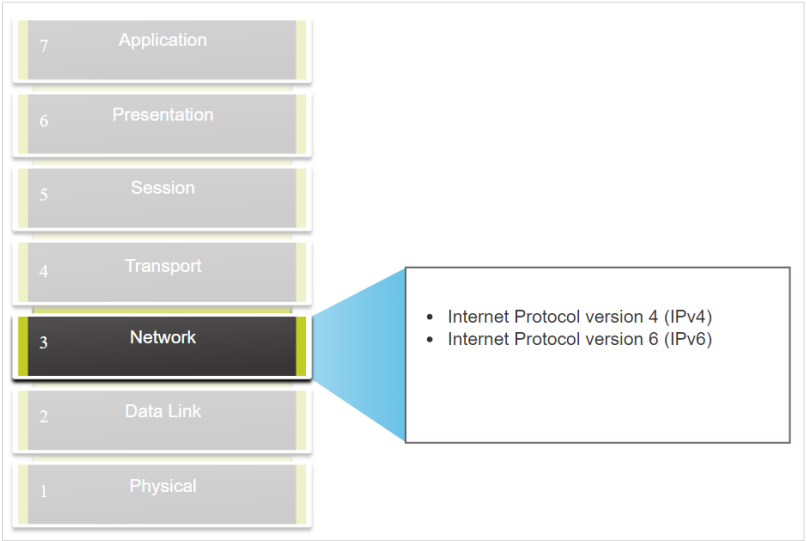


Different Representations of MAC Addresses

6.2 IPv4

The Network Layer

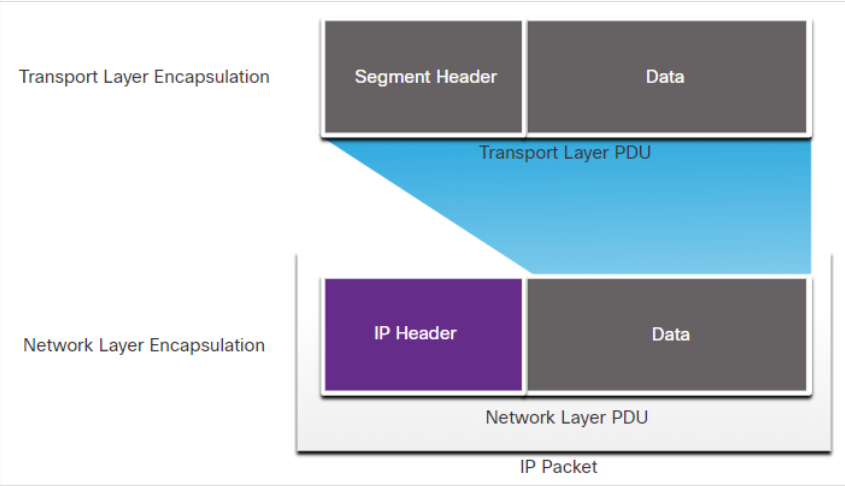
- The network layer provides services to allow end devices to exchange data across networks.
  - IPv4 and IPv6 are the principle network layer communication protocols.
  - Open Shortest Path First (OSPF) and Internet Control Message Protocol (ICMP) are other network layer protocols.
- Basic operations of network layer protocol:
  - **Addressing end devices** - Configured with a unique IP address for identification
  - Encapsulation - Encapsulates the Protocol Data Unit (PDU) from the transport layer into a packet.
  - **Routing** - Select the best path and direct packets towards destination host.
  - De-encapsulation – Performed by the destination host.



Network Layer Protocol

IP Encapsulation

- IP encapsulates the transport layer segment or other data by adding an IP header.
- IP Header is used to deliver the packet to the destination host. It is examined by Layer 3 devices.
- The process of encapsulating data layer by layer enables the services at the different layers to develop and scale without affecting the other layers.
- IP addressing information remains the same from the time the packet leaves the source host until it arrives at the destination host, except when translated by the device performing Network Address Translation (NAT) for IPv4.
- The encapsulated transport layer PDU or other data, remains unchanged during the network layer processes.



Characteristics of IP

- IP was designed as a protocol with low overhead.
- IP provides the functions that are necessary to deliver a packet from a source to a destination over an interconnected system of networks.
- The basic characteristics of IP are as follows:
  - **Connectionless** - There is no connection with the destination established before sending data packets.
  - **Best Effort** - IP is inherently unreliable because packet delivery is not guaranteed.
  - **Media Independent** - Operation is independent of the medium (for example, copper, fiber-optic, or wireless) carrying the data.

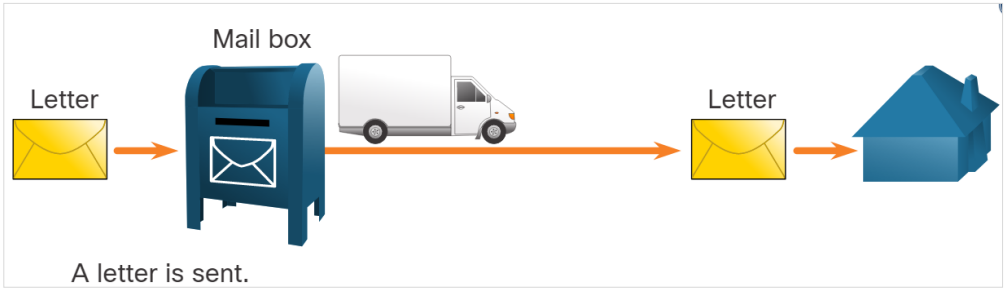
Connectionless

Connectionless - Analogy

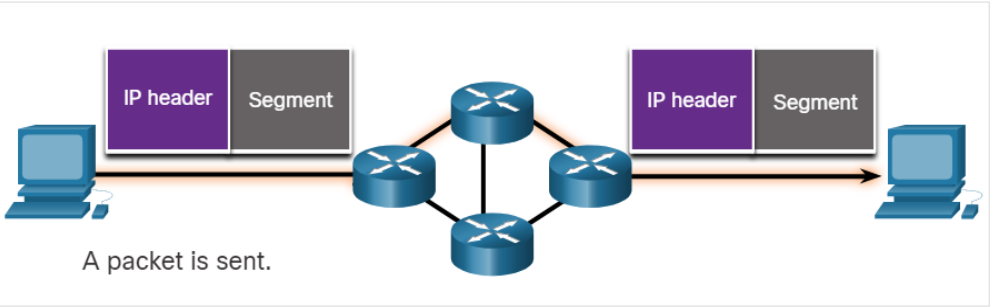
- There is no dedicated end-to-end connection created by IP before data is sent.
- Connectionless communication is conceptually similar to sending a letter to someone without notifying the recipient in advance.

Connectionless - Network

- IP requires no initial exchange of control information to establish an end-to-end connection before packets are forwarded.



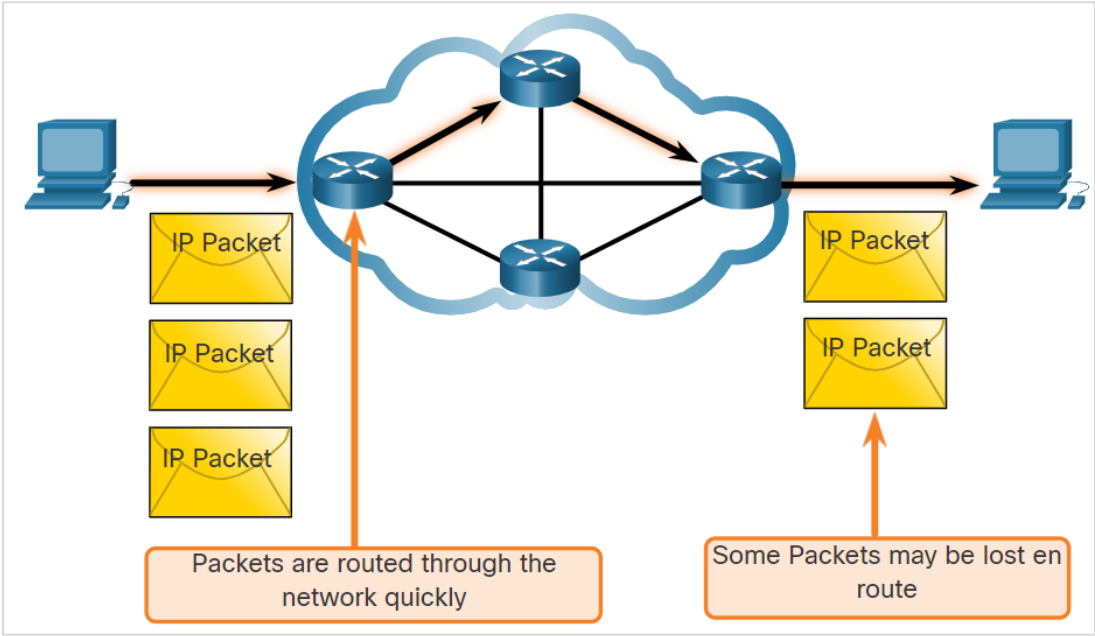
Connectionless - Analogy



Connectionless - Network

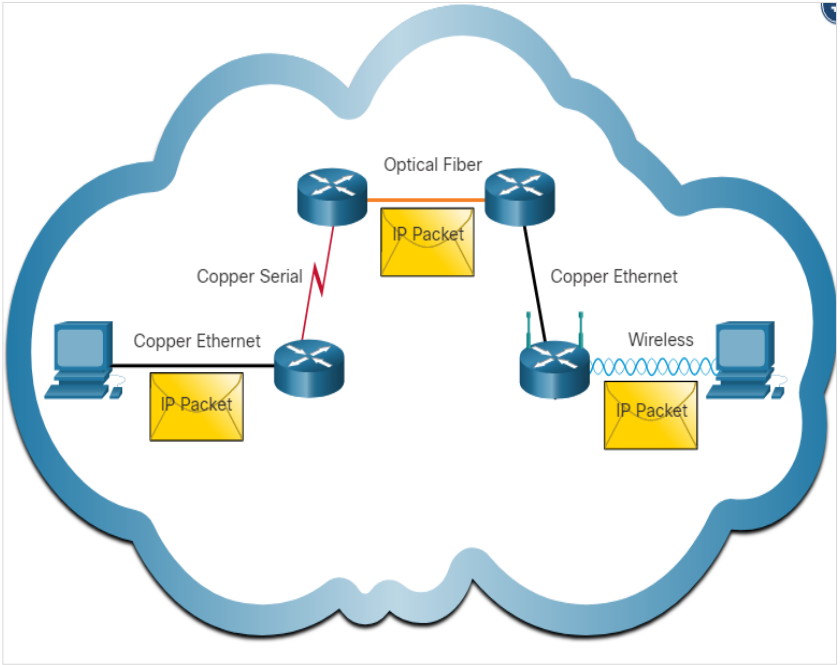
Best Effort

- As an unreliable network layer protocol, IP protocol does not guarantee that all the sent packets will be received.
- Other protocols manage the process of tracking packets and ensuring their delivery.
- The figure illustrates the unreliable or best-effort delivery characteristic of the IP protocol.



Media Independent

- IP operates independently of the media that carry the data at lower layers of the protocol stack.
- IP packets can be communicated as electronic signals over copper cable, as optical signals over fiber, or wirelessly as radio signals.
- The OSI data link layer is responsible for taking an IP packet and preparing it for transmission over the communications medium.
- The maximum size of the PDU that each medium can transport is referred to as the Maximum Transmission Unit (MTU).
- The data link layer passes the MTU value up to the network layer. Later, the network layer determines the size of the large packets.

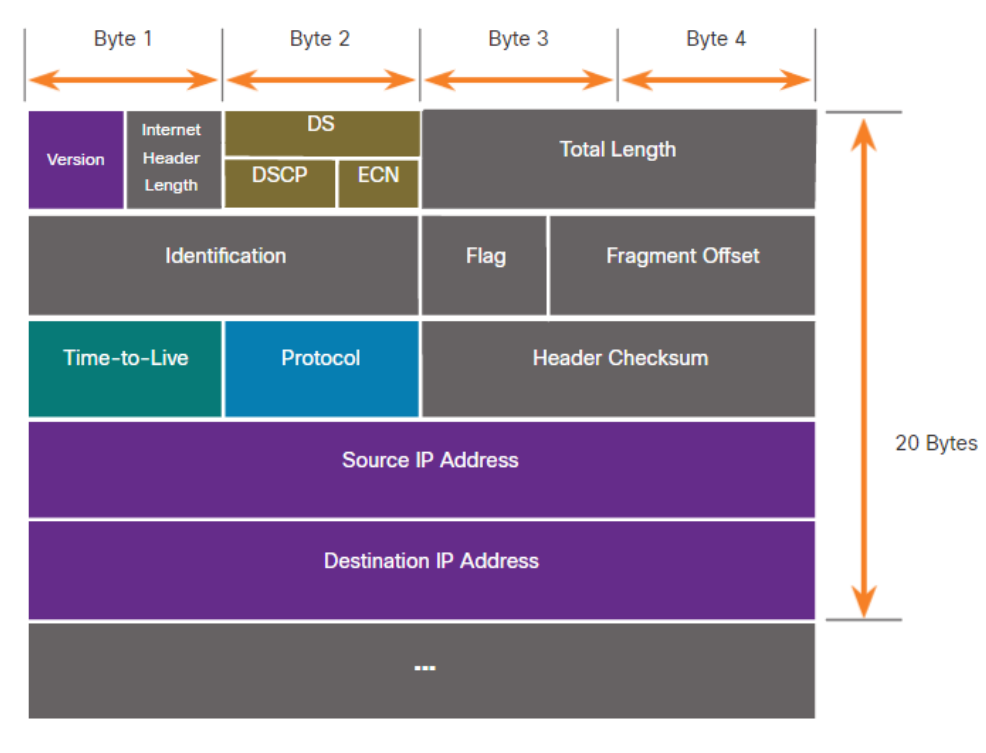


IPv4 Packet Header

- IPv4 is one of the primary network layer communication protocols.
- The IPv4 packet header is used to ensure that this packet is delivered to its next stop on the way to its destination end device.
- An IPv4 packet header consists of fields containing important information about the packet.
- These fields contain binary numbers which are examined by the Layer 3 process.

IPv4 Packet Header Fields

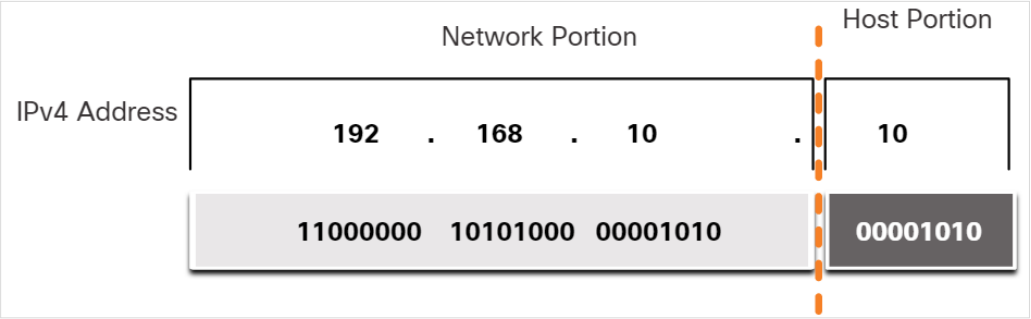
- The significant fields in the IPv4 header include the following:
  - Version
  - Differentiated Services or DiffServ (DS)
  - Header Checksum
  - Time to Live (TTL)
  - Protocol
  - Source IPv4 Address
  - Destination IPv4 Address



6.3 IP Addressing Basics

Network and Host Portions

- An IPv4 address is a 32-bit hierarchical address that is made up of a network portion and a host portion.
- The bits within the network portion of the address must be identical for all devices that are in the same network.
- The bits within the host portion of the address must be unique to identify a specific host within a network.
- If two hosts have the same bit-pattern in the specified network portion of the 32-bit stream, then those two hosts will reside in the same network.



The Subnet Mask

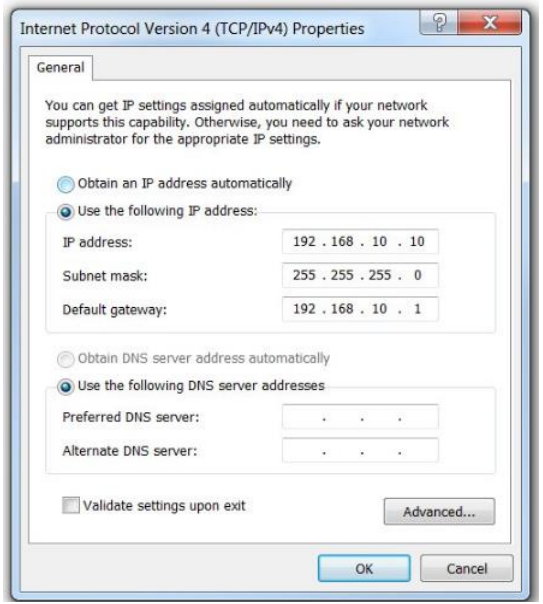
To assign IPv4 address to a host requires the following:

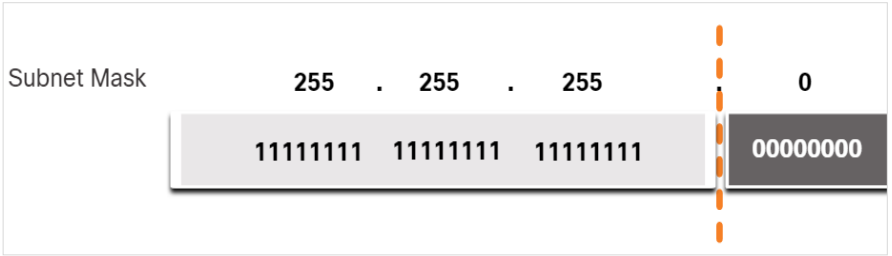
- **IPv4 address** - Unique IPv4 address of the host.
- **Subnet mask**- Used to identify the network/host portion.

Note: *A default gateway IPv4 address is required to reach remote networks and DNS server IPv4 addresses are required to translate domain names to IPv4 addresses.*

- **Subnet Mask**

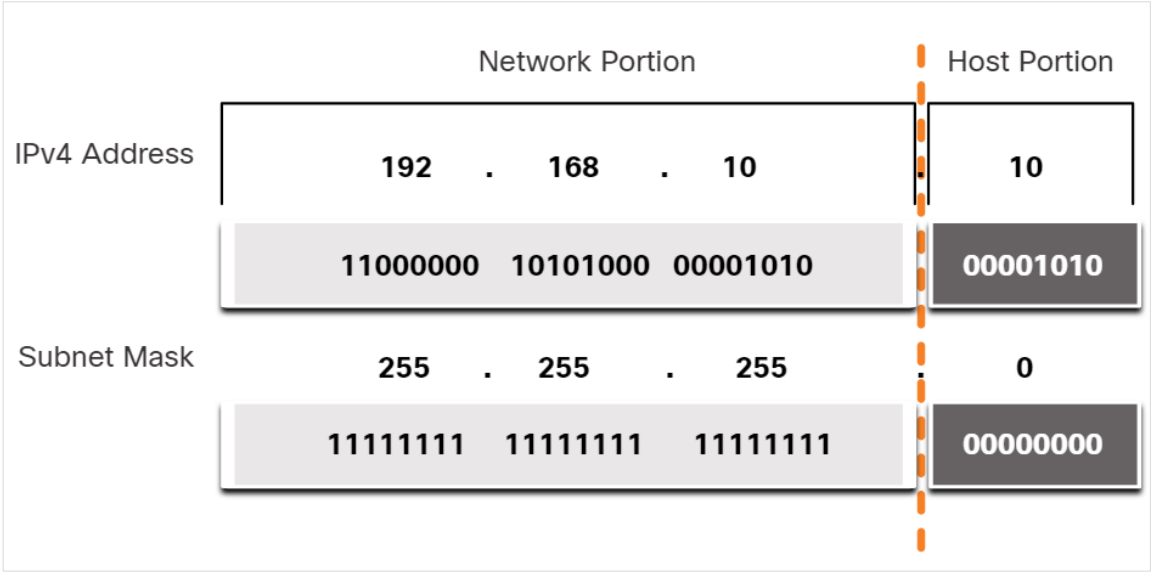
- When an IPv4 address is assigned to a device, the subnet mask is used to determine the network address of the device.
- Subnet mask is a consecutive sequence of 1 bits followed by a consecutive sequence of 0 bits.





The Subnet Mask (Contd.)

- To identify the network and host portions of an IPv4 address, the subnet mask is compared to the IPv4 address bit for bit, from left to right as shown in the figure.
- The subnet mask does not actually contain the network or host portion of an IPv4 address.
- The actual process used to identify the network portion and host portion is called ANDing.



Associating an IPv4 Address with its Subnet Mask

The Prefix Length

- The prefix length is the number of bits set to 1 in the subnet mask.
- It is written in “slash notation”, which is noted by a forward slash (/) followed by the number of bits set to 1.
- When representing an IPv4 address using a prefix length, the IPv4 address is written followed by the prefix length with no spaces.
- Note: A network address is also referred to as a prefix or network prefix. Therefore, the prefix length is the number of 1 bits in the subnet mask.
- When representing an IPv4 address using a prefix length, the IPv4 address is written followed by the prefix length with no spaces. For example, 192.168.10.10 255.255.255.0 would be written as 192.168.10.10/24.

The Prefix Length (Contd.)

The first column lists the subnet masks that can be used with a host address. The second column displays the converted 32-bit binary address. The last column displays the resulting prefix length.

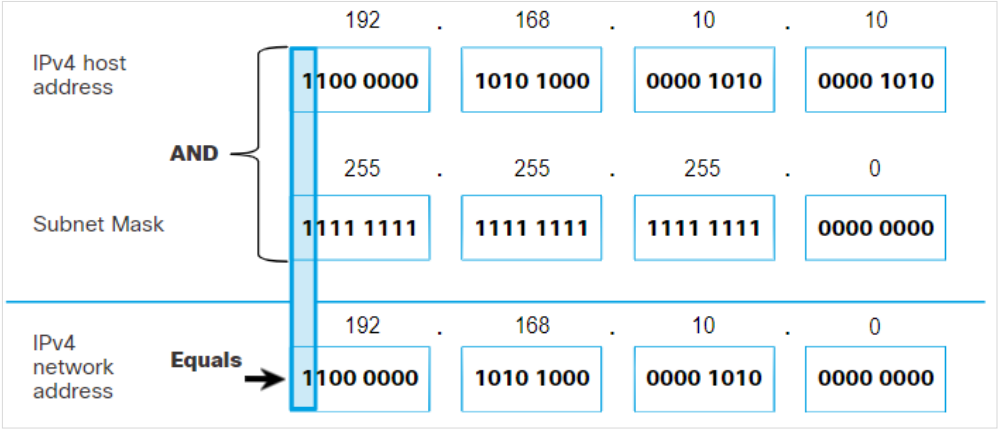
Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

Determining the Network: Logical AND

- A logical AND is one of three Boolean operations used in Boolean or digital logic.
- The AND operation is used in determining the network address.
- Logical AND is the comparison of two bits that produce the results as shown below
  - 1 AND 1 = 1
  - 0 AND 1 = 0
  - 1 AND 0 = 0
  - 0 AND 0 = 0
- To identify the network address of an IPv4 host, the IPv4 address is logically ANDed, bit by bit, with the subnet mask.
- Note: In digital logic, 1 represents True and 0 represents False. When using an AND operation, both input values must be True (1) for the result to be True (1).

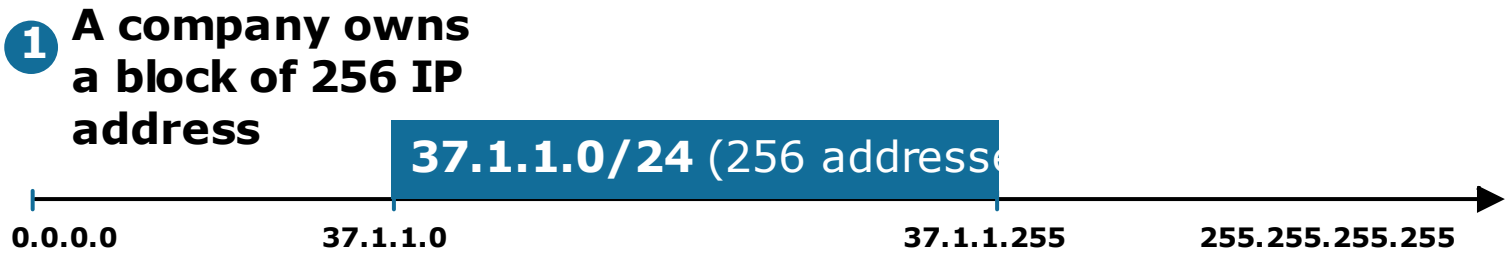
Determining the Network: Logical AND (Contd.)

- To illustrate how AND is used to discover a network address, consider a host with IPv4 address 192.168.10.10 and subnet mask of 255.255.255.0, as shown in the figure:
- **IPv4 host address (192.168.10.10)** - The IPv4 address of the host in dotted decimal and binary formats.
- **Subnet mask (255.255.255.0)** - The subnet mask of the host in dotted decimal and binary formats.
- **Network address (192.168.10.0)** - The logical AND operation between the IPv4 address and subnet mask results in an IPv4 network address shown in dotted decimal and binary formats.



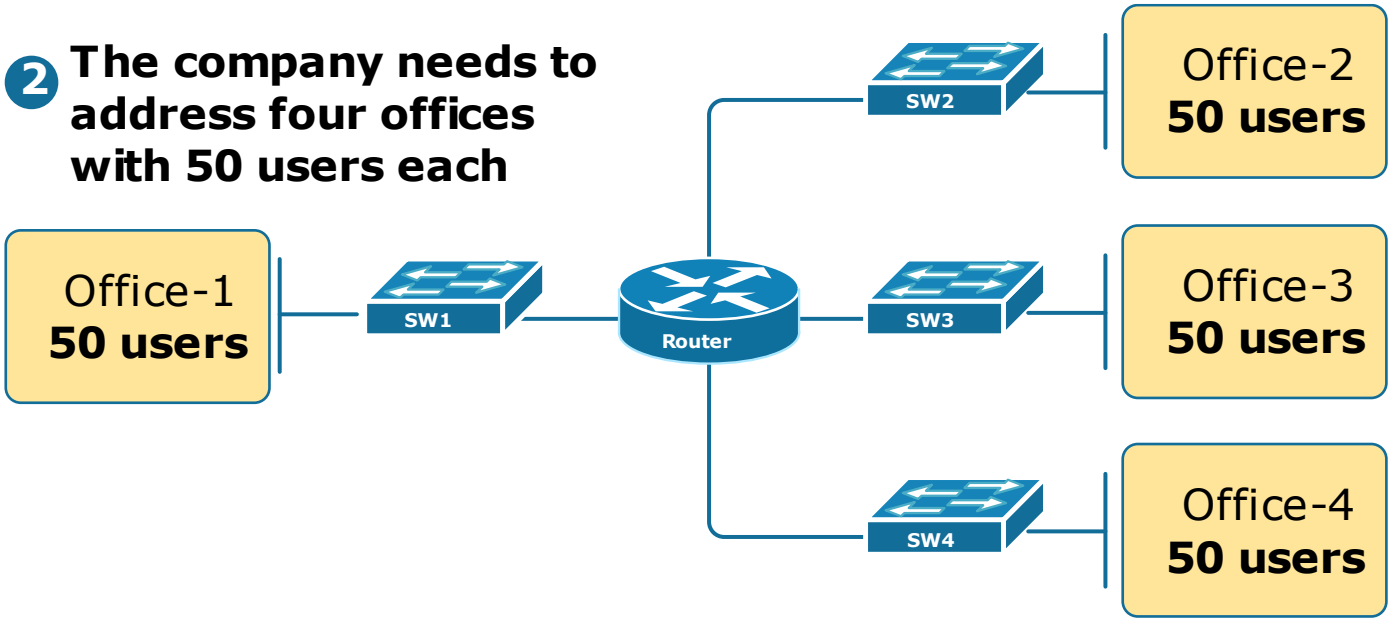
Subnetting: Example

- https://www.networkacademy.io/ccna/ip-subnetting/what-is-subnetting

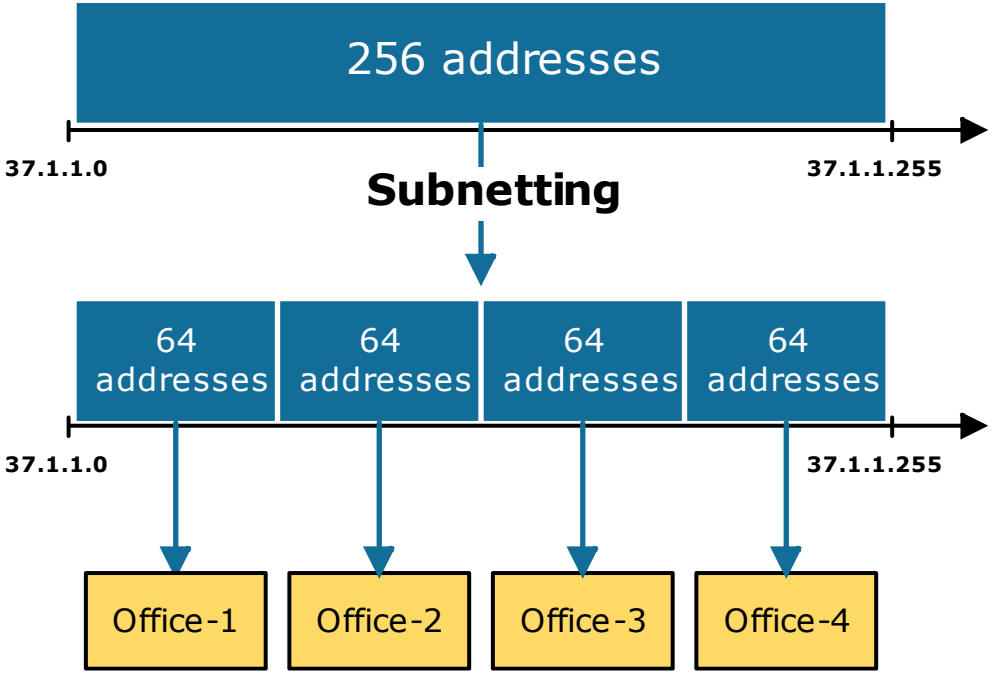


Subnetting: Example

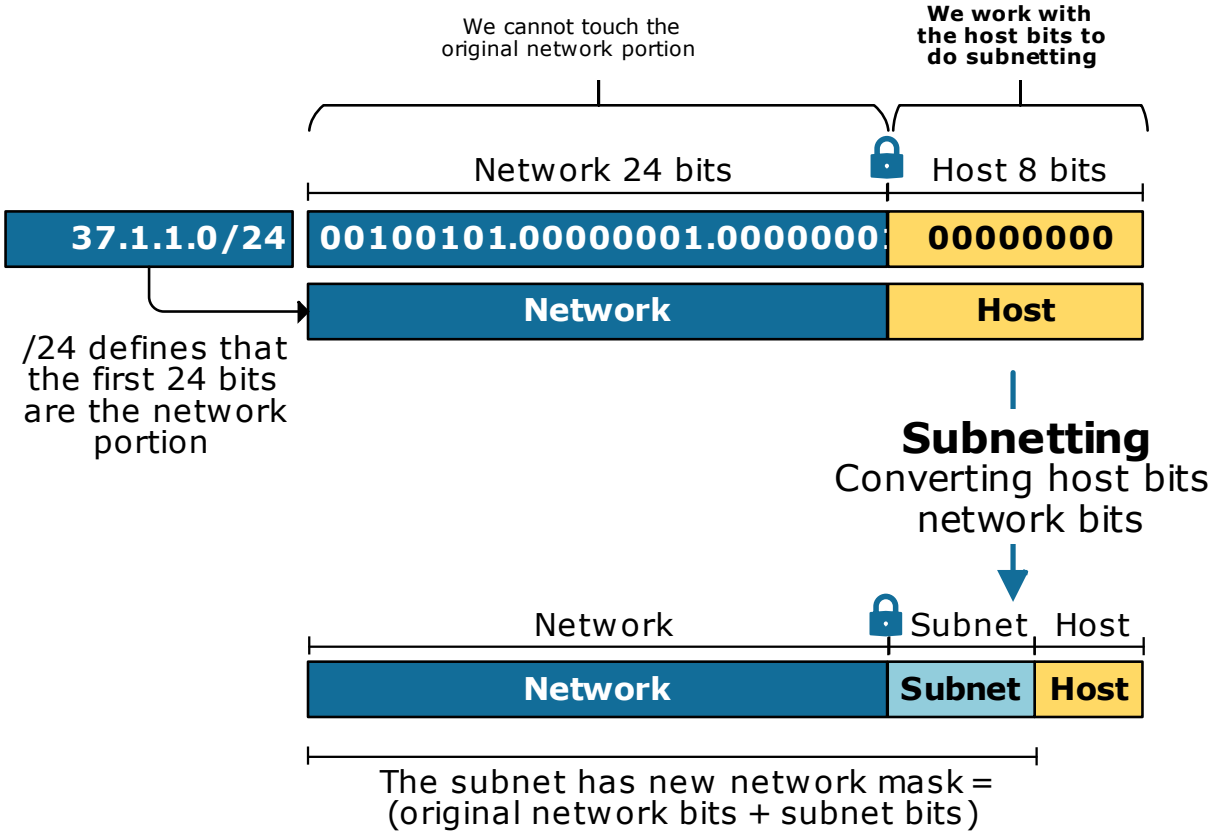
2 **The company needs to address four offices with 50 users each**



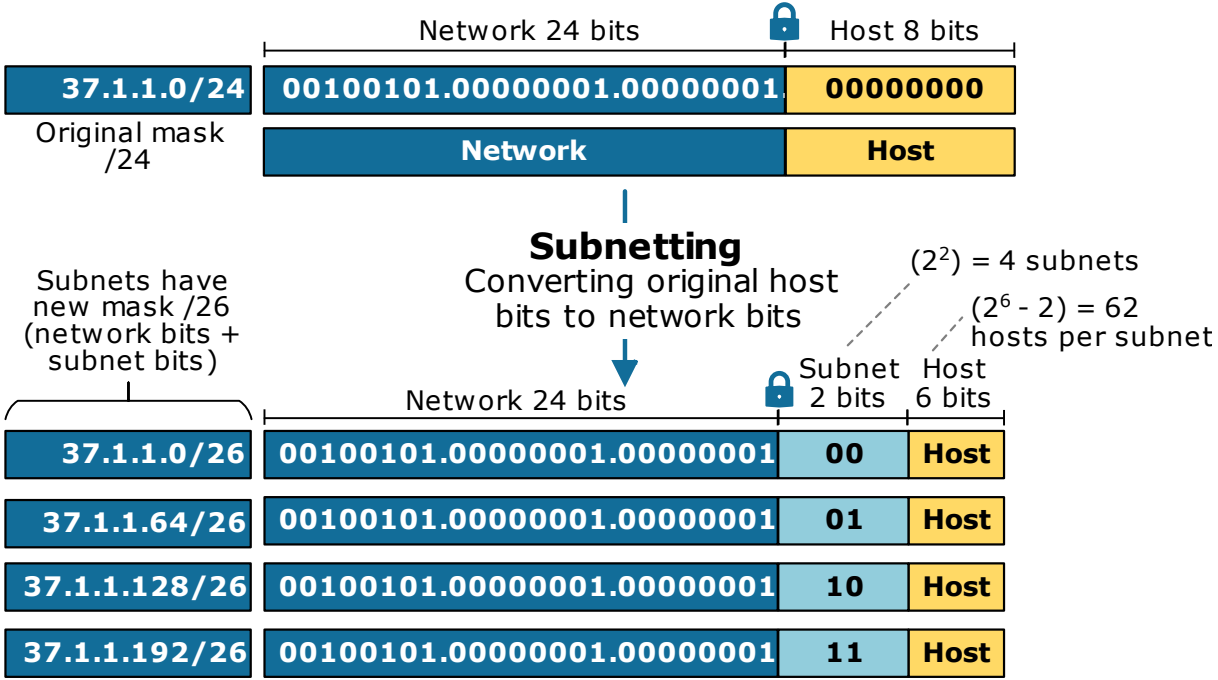
Subnetting: Example



Subnetting: Example

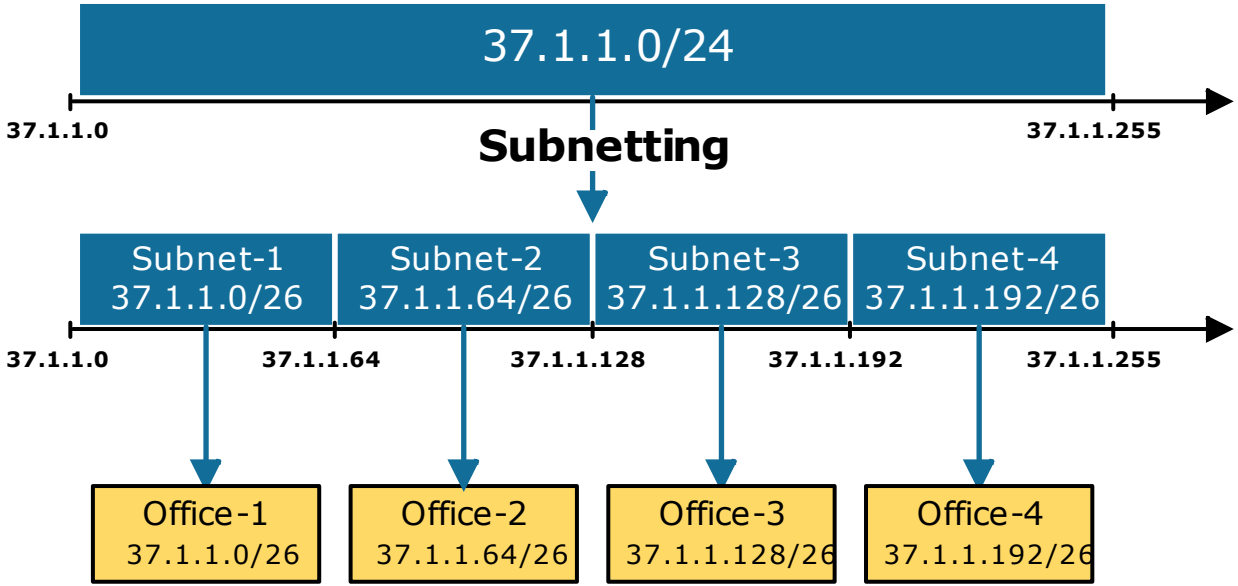


Subnetting: Example



2^subnet bits = number subnets created
2^host bits - 2 = number of hosts per subnet

Subnetting: Example



Subnetting: Execrcise

Find the subnet ID of
25.44.33.145
255.255.255.224

1. **Convert the address and mask to binary.**
   25.44.33.145 = 00011001.00101100.00100001.10010001
   255.255.255.224 = 11111111.11111111.11111111.111000(
2. **Determine the network and host portions** of the address using the mask - 1s define the network portion, 0s define the host portion.

	Network	Host
IP Address:	00011001.00101100.00100001.1	10001
Mask:	11111111.11111111.11111111.1	00000

Number of **network bits = 27** | Number of **host bits = 5**

3. **Determine the subnet ID** by converting all host bits to 0.

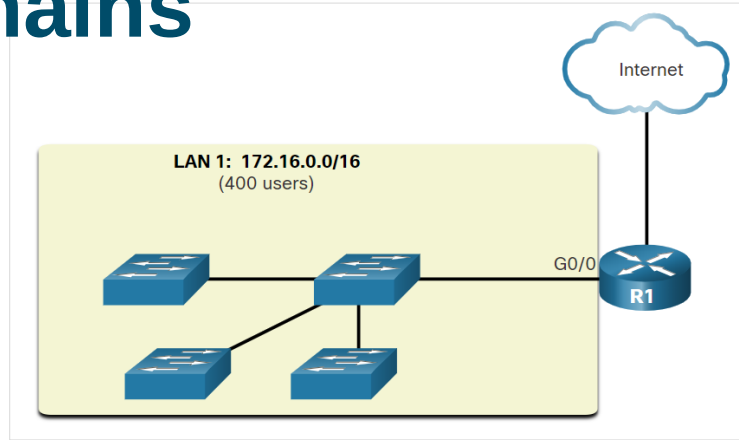
First address (all zeros) is the **Network Identifier**

	Network
IP Address:	00011001.00101100.00100001.1 00000

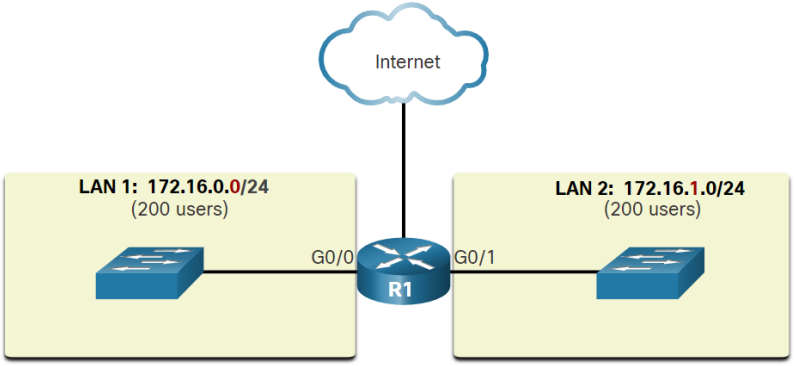
4. Convert the first address back to decimal:
   - the Network Identifier is **25.44.33.128/27**

Subnetting Broadcast Domains

- In the figure, LAN 1 connects 400 users that could each generate broadcast traffic, which can slow down network and device operations.
- The solution is to reduce the size of the network to create smaller broadcast domains in a process called subnetting. These smaller network spaces are called subnets.
- Subnetting reduces the overall network traffic and improves network performance.
- **Note**: *The terms subnet and network are often used interchangeably. Most networks are a subset of some larger address block.*



A Large Broadcast Domain

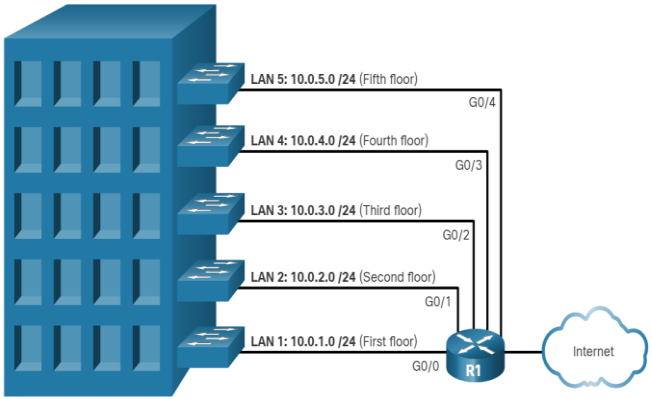


Communication between Networks

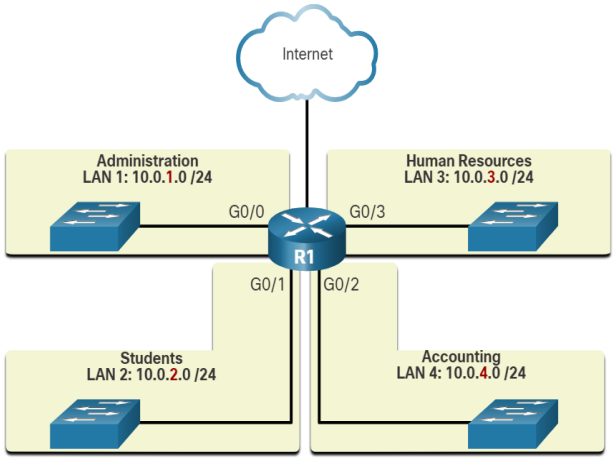
Subnetting Broadcast Domains (Contd.)

- Network administrators can group devices and services into subnets that may be determined by a variety of factors.

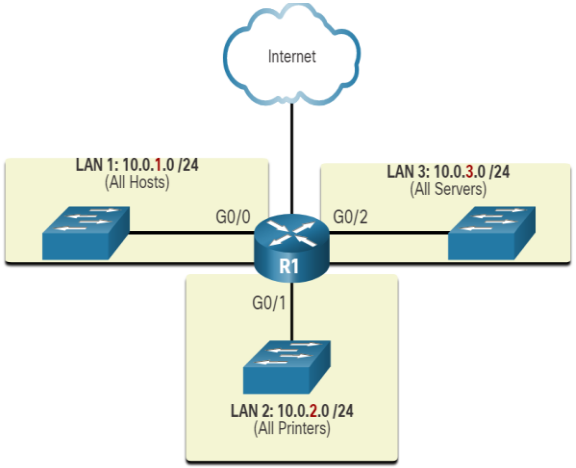
Location



By Department



Device Type



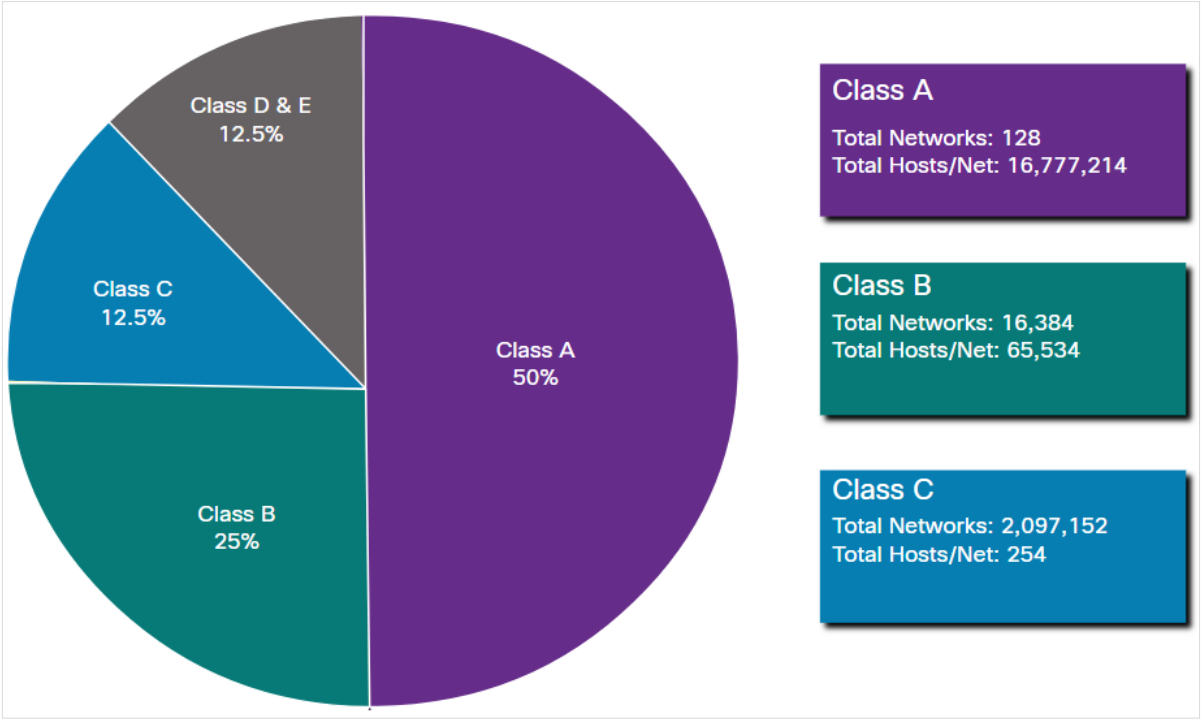
6.4 Types of IPv4 Addresses

IPv4 Address Classes and Default Subnet Masks

- The IPv4 addresses were based on the following classes:
  - Class A (0.0.0.0/8 to 127.0.0.0/8) – Designed to support extremely large networks with more than 16 million host addresses.
  - Class B (128.0.0.0 /16 – 191.255.0.0 /16) – Designed to support moderate to large size networks with up to approximately 65,000 host addresses.
  - Class C (192.0.0.0 /24 – 223.255.255.0 /24) – Designed to support small networks with a maximum of 254 hosts.
- Note: There is also a Class D multicast block consisting of 224.0.0.0 to 239.0.0.0 and a Class E experimental address block consisting of 240.0.0.0 – 255.0.0.0.

IPv4 Address Classes and Default Subnet Masks (Contd.)

- The classful system allocated :
- 50% of the available IPv4 addresses to 128 Class A networks
- 25% of the addresses to Class B
- Class C shared the remaining 25% with Class D and E.



Summary of Classful Addressing

Reserved Private Addresses

- There are blocks of addresses called private addresses that are used by most organizations to assign IPv4 addresses to internal hosts.
- Private IPv4 addresses are not unique and can be used by any internal network.
- Most common private address blocks:
  - 10.0.0.0 /8 or 10.0.0.0 to 10.255.255.255
  - 172.16.0.0 /12 or 172.16.0.0 to 172.31.255.255
  - 192.168.0.0 /16 or 192.168.0.0 to 192.168.255.255
  - The addresses within these address blocks are not allowed on the internet and must be filtered by internet routers.

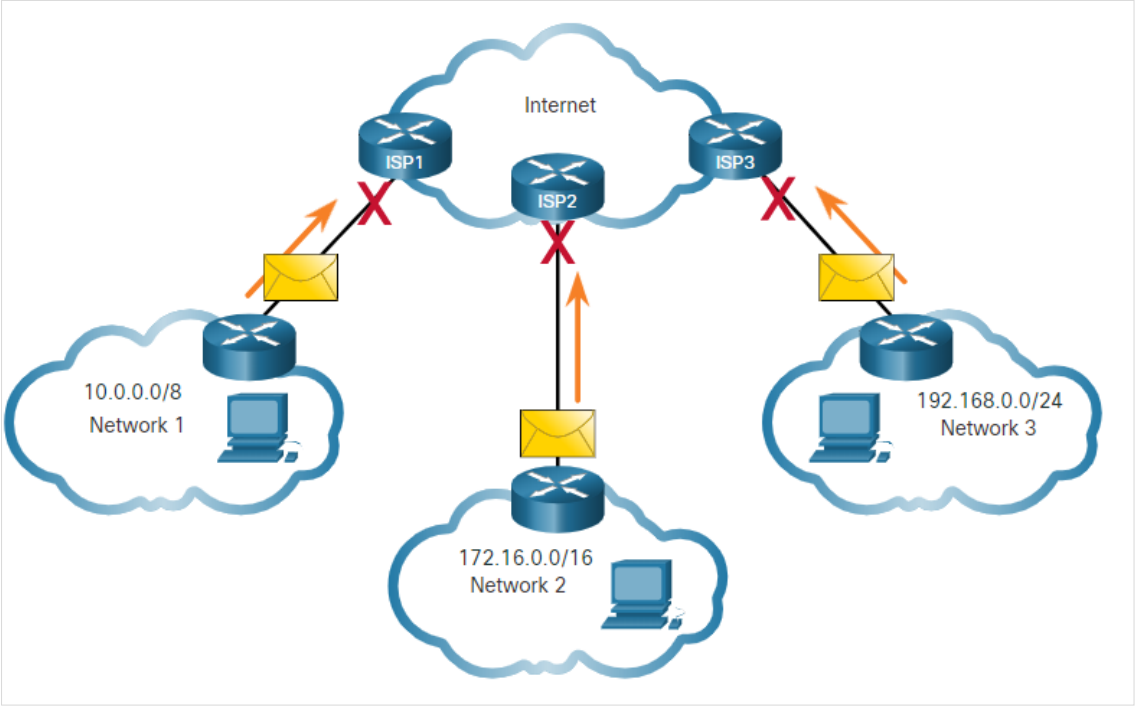
Reserved Private Addresses

Special address blocks

Address block	Address range	Number of addresses	Scope	Description
0.0.0.0/8	0.0.0.0–0.255.255.255	16 777 216	Software	Current (local, "this") network[1]
10.0.0.0/8	10.0.0.0–10.255.255.255	16 777 216	Private network	Used for local communications within a private network[3]
100.64.0.0/10	100.64.0.0–100.127.255.255	4 194 304	Private network	Shared address space[4] for communications between a service provider and its subscribers when using a carrier-grade NAT
127.0.0.0/8	127.0.0.0–127.255.255.255	16 777 216	Host	Used for loopback addresses to the local host[1]
169.254.0.0/16	169.254.0.0–169.254.255.255	65 536	Subnet	Used for link-local addresses[5] between two hosts on a single link when no IP address is otherwise specified, such as would have normally been retrieved from a DHCP server
172.16.0.0/12	172.16.0.0–172.31.255.255	1 048 576	Private network	Used for local communications within a private network[3]
192.0.0.0/24	192.0.0.0–192.0.0.255	256	Private network	IETF Protocol Assignments, DS-Lite (/29)[1]
192.0.2.0/24	192.0.2.0–192.0.2.255	256	Documentation	Assigned as TEST-NET-1, documentation and examples[6]
192.88.99.0/24	192.88.99.0–192.88.99.255	256	Internet	Reserved.[7] Formerly used for IPv6 to IPv4 relay[8] (included IPv6 address block 2002::/16).
192.168.0.0/16	192.168.0.0–192.168.255.255	65 536	Private network	Used for local communications within a private network[3]
198.18.0.0/15	198.18.0.0–198.19.255.255	131 072	Private network	Used for benchmark testing of inter-network communications between two separate subnets[9]
198.51.100.0/24	198.51.100.0–198.51.100.255	256	Documentation	Assigned as TEST-NET-2, documentation and examples[6]
203.0.113.0/24	203.0.113.0–203.0.113.255	256	Documentation	Assigned as TEST-NET-3, documentation and examples[6]
224.0.0.0/4	224.0.0.0–239.255.255.255	268 435 456	Internet	In use for multicast[10] (former Class D network)
233.252.0.0/24	233.252.0.0-233.252.0.255	256	Documentation	Assigned as MCAST-TEST-NET, documentation and examples (Note that this is part of the above multicast space.)[10][11]
240.0.0.0/4	240.0.0.0–255.255.255.254	268 435 455	Internet	Reserved for future use[12] (former Class E network)
255.255.255.255/32	255.255.255.255	1	Subnet	Reserved for the "limited broadcast" destination address[1]

Reserved Private Addresses (Contd.)

- In the figure, users in networks 1, 2, or 3 are sending packets to remote destinations. The ISP routers would see that the source IPv4 addresses in the packets are from private addresses and discard the packets.
- Most organizations use private IPv4 addresses for their internal hosts.
- Network Address Translation (NAT) is used to translate between private IPv4 and public IPv4 addresses.

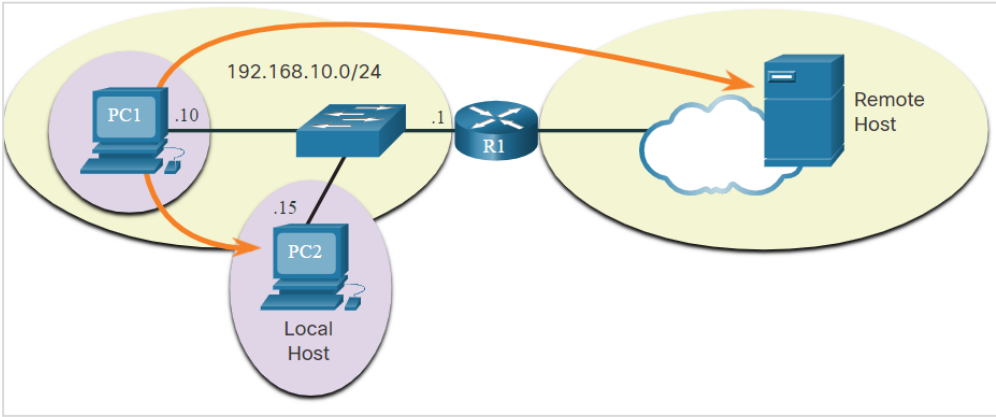


Private Addresses Cannot be Routed over the Internet

6.5 The Default Gateway

Host Forwarding Decision

- Another role of the network layer is to direct packets between hosts. A host can send a packet to: Itself, Local host, and Remote host.
- The figure illustrates PC1 connecting to a local host on the same network, and to a remote host located on another network.
- Whether a packet is destined for a local host or a remote host is determined by the source end device. The method of determination varies by IP version:
  - In IPv4 - The source device uses its own subnet mask along with its own IPv4 address and the destination IPv4 address to make this determination.
  - In IPv6 - The local router advertises the local network address to all devices on the network.

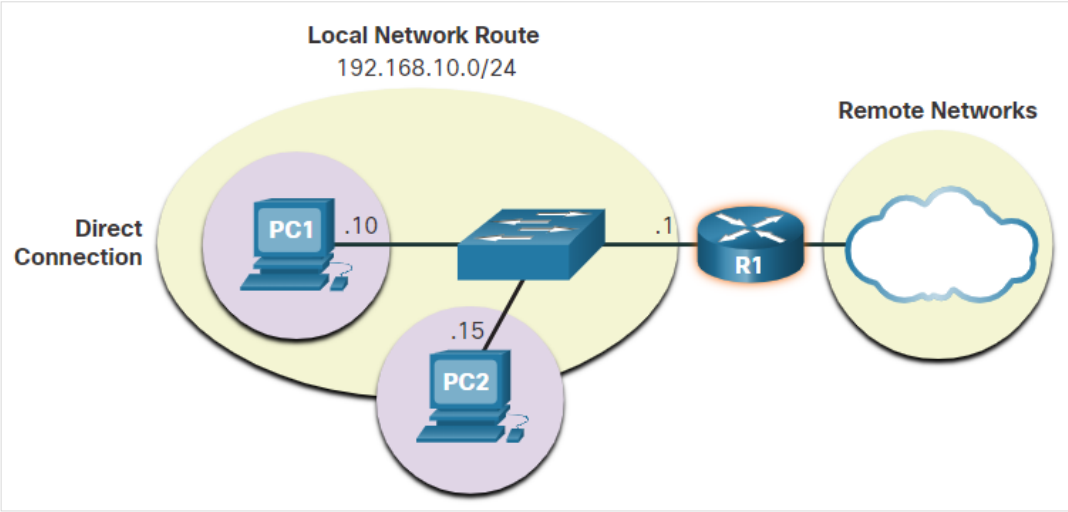


Default Gateway

- The default gateway is the network device that can route traffic to other networks.
- On a network, a default gateway is usually a router with these features:
  - It has a local IP address in the same address range as other hosts on the local network.
  - It can accept data into the local network and forward data out of the local network.
  - It routes traffic to other networks.
- A default gateway is required to send traffic outside the local network.
- Traffic cannot be forwarded outside the local network if there is no default gateway, or the default gateway address is not configured, or the default gateway is down.

A Host Routes to the Default Gateway

- In IPv4, the host receives the IPv4 address of the default gateway either dynamically from Dynamic Host Configuration Protocol (DHCP) or configured manually.
- In IPv6, the router advertises the default gateway address or the host can be configured manually.
- Having a default gateway configured creates a default route in the routing table of the PC.
- A default route is the route or pathway your computer will take when it tries to contact a remote network.



PC1 and PC2 are configured with the IPv4 address of 192.168.10.1 as the default gateway

Host Routing Tables

- On a Windows host, the route print or `netstat -r` command can be used to display the host routing table. Both commands generate the same output.
- The figure displays a sample topology and the output generated by the `netstat -r` command.

Host Routing Tables (Contd.)

- Entering the **netstat -r** command displays three sections related to the current TCP/IP network connections:
  - Interface List
  - IPv4 Route Table
  - IPv6 Route Table
- IPv4 Routing Table for PC1

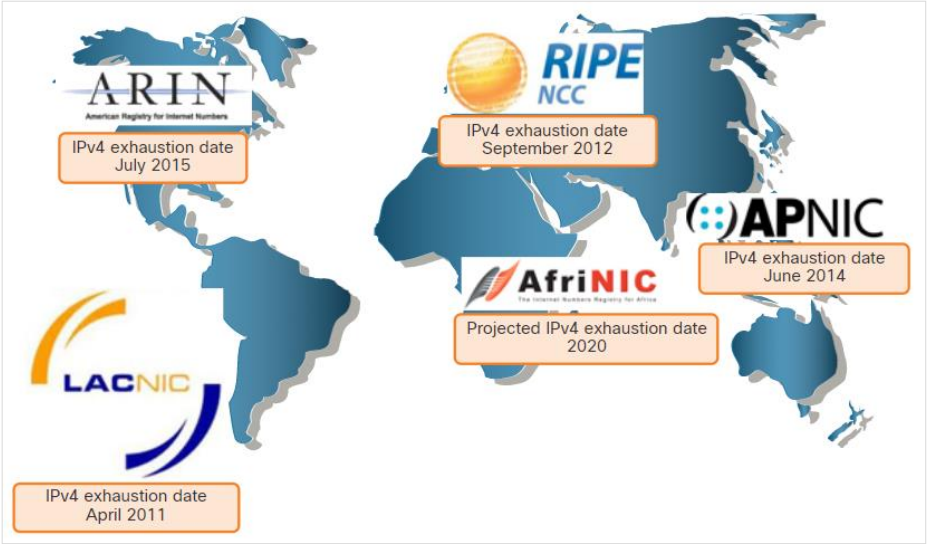
```
C:\Users\PC1> netstat -r

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.10.1    192.168.10.10      25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1     306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1     306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1     306
    192.168.10.0    255.255.255.0         On-link    192.168.10.10     281
   192.168.10.10  255.255.255.255         On-link    192.168.10.10     281
  192.168.10.255  255.255.255.255         On-link    192.168.10.10     281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1     306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10     281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1     306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10     281
```

6.6 IPv6

Need for IPv6

- IPv6 is designed to be the successor to IPv4.
- IPv6 has a larger 128-bit address space, providing 340 undecillion possible addresses.
- Mobile providers have been leading the way with the transition to IPv6.
- Most top ISPs and content providers such as YouTube, Facebook, and Netflix, have also made the transition.
- Many companies like Microsoft, Facebook, and LinkedIn are transitioning to IPv6-only internally.
- The depletion of IPv4 address space has been the motivating factor for moving to IPv6.



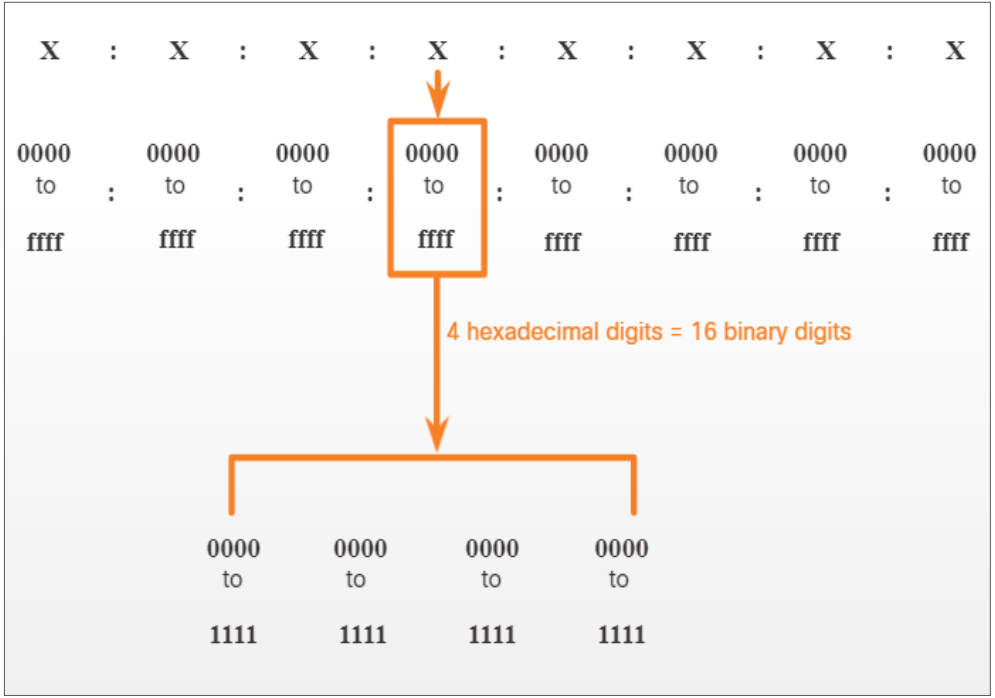
RIR IPv4 Exhaustion Dates

Need for IPv6 (Contd.)

- Internet of Things
  - The internet of today is more than email, web pages, and file transfers between computers.
  - The evolving internet is becoming an Internet of Things (IoT).
  - Computers, tablets, and smartphones will not be the only devices accessing the internet but there will also be sensor-equipped, internet-ready devices of tomorrow including everything from automobiles and biomedical devices, to household appliances and natural ecosystems.
  - With an increasing internet population, a limited IPv4 address space, issues with NAT and the IoT, the time has come to begin the transition to IPv6.

IPv6 Addressing Formats

- IPv6 addresses are 128 bits in length and written as a string of hexadecimal values.
- Every four bits is represented by a single hexadecimal digit for a total of 32 hexadecimal values.
- IPv6 addresses are not case-sensitive and can be written in either lowercase or uppercase.



16-bit Segments or Hextets

IPv6 Addressing Formats (Contd.)

- Preferred Format
  - The preferred format for writing an IPv6 address is x:x:x:x:x:x:x:x, with each “x” consisting of four hexadecimal values.
  - Each “x” is a single hextet which is 16 bits or four hexadecimal digits.
- Examples of IPv6 addresses in the preferred format

```
2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000: 0200
2001 : 0db8 : 0000 : 00a3 : abcd : 0000 : 0000: 1234
2001 : 0db8 : 000a : 0001 : c012 : 9aff : fe9a: 19ac
2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000: 0000
fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab: cdef
fe80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0001
fe80 : 0000 : 0000 : 0000 : c012 : 9aff : fe9a: 19ac
fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab: cdef
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0001
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0000
```

Rule 1 - Omit Leading Zeros

- Rule 1: Omit any leading 0s (zeros) in any hextet.
- The four examples of ways to omit leading zeros:
- 01ab can be represented as 1ab
  - 09f0 can be represented as 9f0
  - 0a00 can be represented as a00
  - 00ab can be represented as ab
  - This rule only applies to leading 0s, NOT to trailing 0s, otherwise the address would be ambiguous. 01ab. For example, refer to the below table.

Type	Format
Preferred	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
No leading 0s	2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200

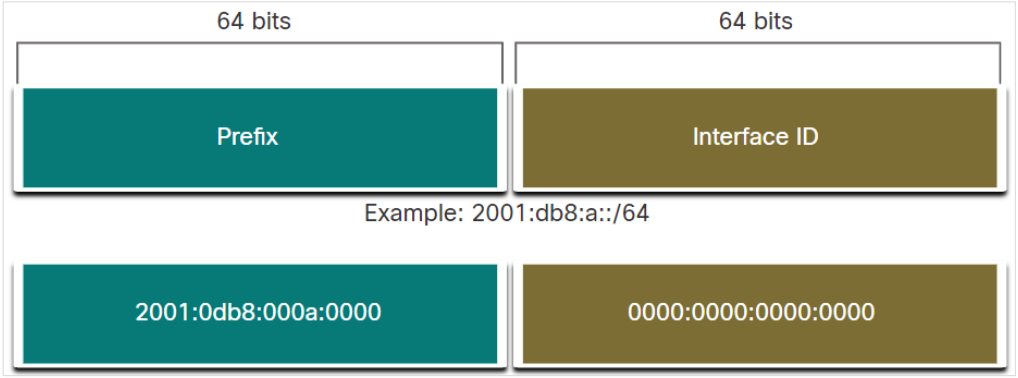
Rule 2 - Double Colon

- Rule 2: Double colon (::) can replace any single, contiguous string of one or more 16-bit hextets consisting of all zeros.
  - Example: 2001:db8:cafe:1:0:0:0:1 could be represented as 2001:db8:cafe:1::1.
  - The double colon (::) is used in place of the three all-0 hextets (0:0:0).
  - The double colon (::) can only be used once within an address.
  - When used with the omitting leading 0s technique, the notation of IPv6 address can often be greatly reduced. This is commonly known as the compressed format.
  - Example of incorrect use of the double colon: 2001:db8::abcd::1234.

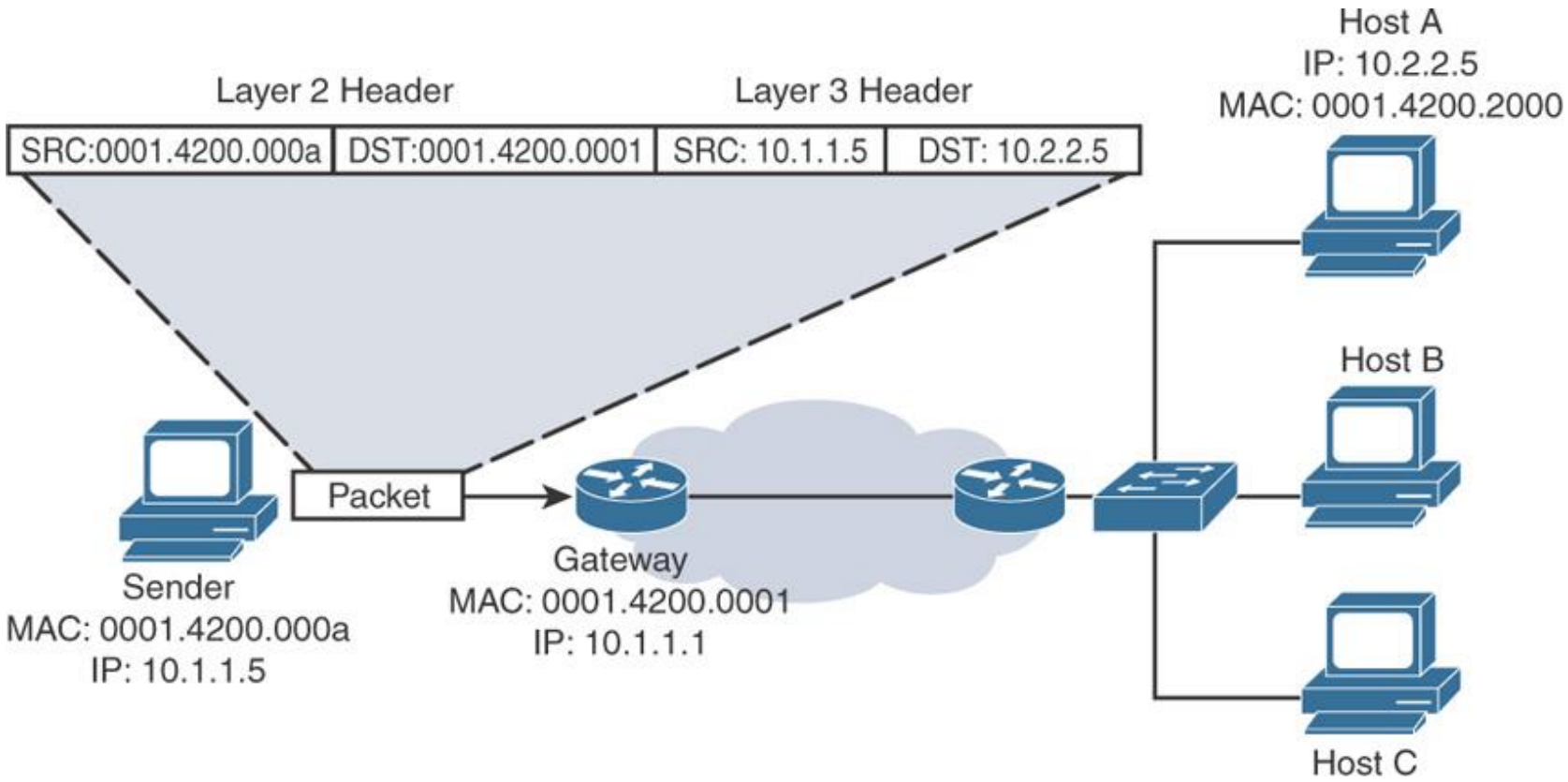
Type	Format
Preferred	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
Compressed/spaces	2001 : db8 : 0 : 1111 : : 200
Compressed	2001:db8:0:1111::200

IPv6 Prefix Length

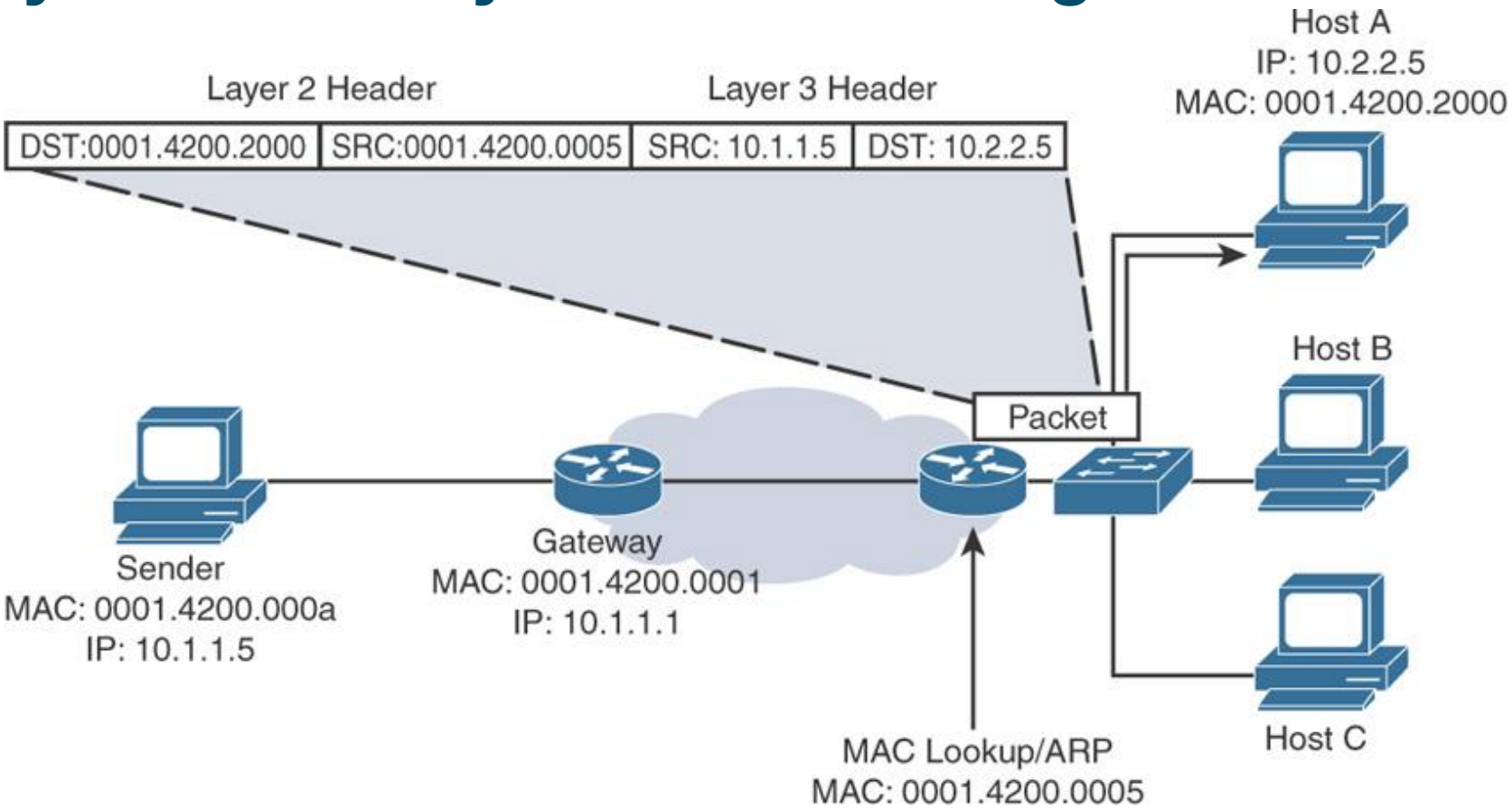
- The prefix can be identified by a dotted-decimal subnet mask or prefix length (slash notation).
- For example, an IPv4 address of 192.168.1.10 with dotted-decimal subnet mask 255.255.255.0 is equivalent to 192.168.1.10/24.
- In IPv4 the /24 is called the prefix, whereas in Pv6 it is called the prefix length.
- Similar to IPv4, the prefix length is represented in slash notation and is used to indicate the network portion of an IPv6 address. It can range from 0 to128.
- It is strongly recommended to use a 64-bit Interface ID for most networks.



Layer 2 and Layer 3 Addressing and Routing



Layer 2 and Layer 3 Addressing and Routing



Thank you! Questions?

Vladimír Veselý

updated: 2024-02-16

https://www.fit.vutbr.cz/research/groups/nes@fit

Module 7: Connectivity Verification

Instructor Materials

CyberOps Associate v1.0

Module 7: Connectivity Verification

CyberOps Associate v1.0

Module Objectives

Module Title: Connectivity Verification

Module Objective: Use ICMP connectivity verification tools

Topic Title	Topic Objective
ICMP	Explain how ICMP is used to test network connectivity.
Ping and Traceroute Utilities	Use Windows tools, ping, and traceroute to verify network connectivity.

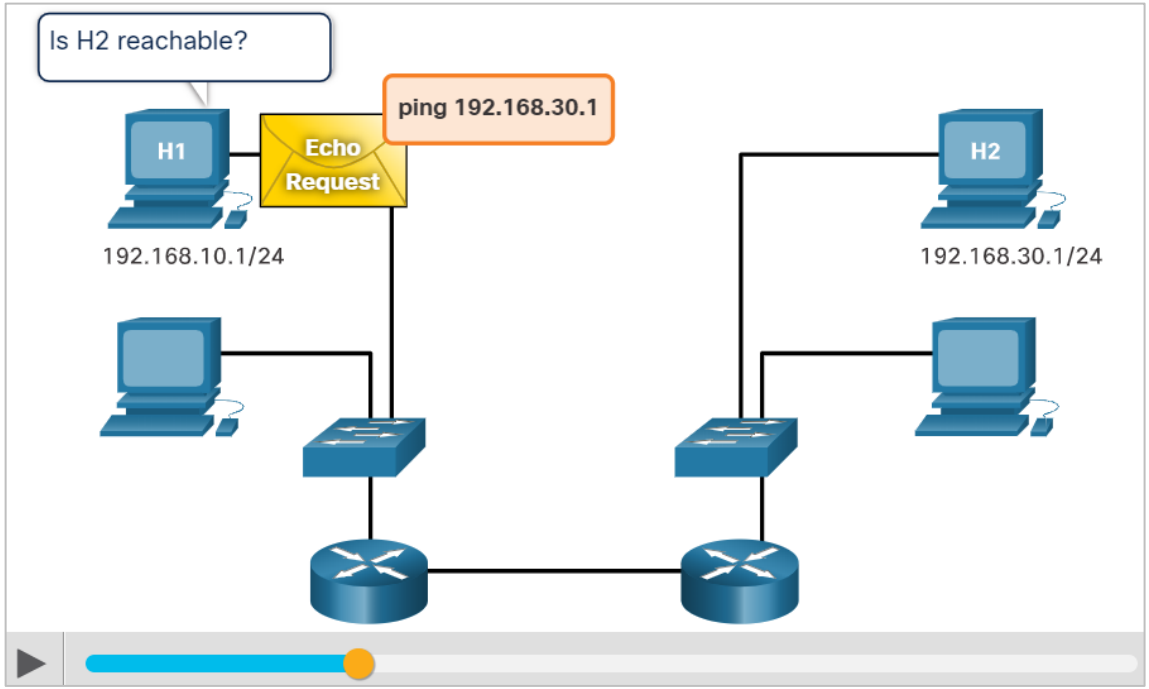
7.1 ICMP

ICMPv4 Messages

- The TCP/IP suite provide messages to be sent in the event of certain errors. These messages are sent using the services of ICMP.
- The purpose of these messages is to provide feedback about issues related to the processing of IP packets under certain conditions.
- ICMP messages are not required and are often not allowed within a network for security reasons.
- ICMP is available for both IPv4 and IPv6. ICMPv4 is the messaging protocol for IPv4. ICMPv6 provides the same services for IPv6 but includes additional functionality.
- ICMP messages common to both ICMPv4 and ICMPv6 include host confirmation, destination or service unreachable, time exceeded and route redirection.

ICMPv4: Host Confirmation

- An ICMP Echo Message can be used to determine if a host is operational.
- The local host sends an **ICMP Echo Request** to a host. If the host is available, the destination host responds with an **ICMP Echo Reply**.
- This use of the ICMP Echo messages is the basis of the ping utility.



ICMPv4: Destination or Service Unreachable

- When a host or gateway receives a packet that it cannot deliver, it can use an **ICMP Destination Unreachable** message to notify the source that the destination or service is unreachable.
- The message will include a code that indicates why the packet could not be delivered. The Destination Unreachable codes for ICMPv4 includes the following:
  - 0 - Net unreachable
  - 1 - Host unreachable
  - 2 - Protocol unreachable
  - 3 - Port unreachable
- ***Note:*** *ICMPv6 has slightly different codes for Destination Unreachable messages.*

ICMPv4: Time Exceeded

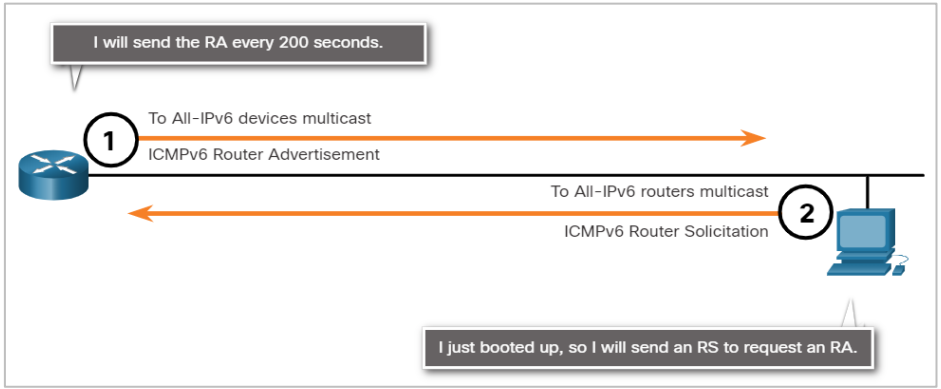
- An **ICMPv4 Time Exceeded** message is used by a router to indicate that a packet cannot be forwarded because the Time to Live (TTL) field of the packet was decremented to 0.
- If a router receives a packet and decrements the TTL field in the IPv4 packet to zero, it discards the packet and sends a Time Exceeded message to the source host.
- ICMPv6 also sends a Time Exceeded message if the router cannot forward an IPv6 packet because the packet has expired.
  - IPv6 does not have a TTL field. It uses the hop limit field to determine if the packet has expired.

ICMPv6 RS and RA Messages

- ICMPv6 has new features and improved functionality not found in ICMPv4. ICMPv6 messages are encapsulated in IPv6.
- It has four new protocols as part of the Neighbor Discovery Protocol (ND or NDP).
- Messaging between an IPv6 router and an IPv6 device:
  - **Router Solicitation (RS) message**
  - **Router Advertisement (RA) message**
  - **Messaging between IPv6 devices:**
  - **Neighbor Solicitation (NS) message**
  - **Neighbor Advertisement (NA) message**

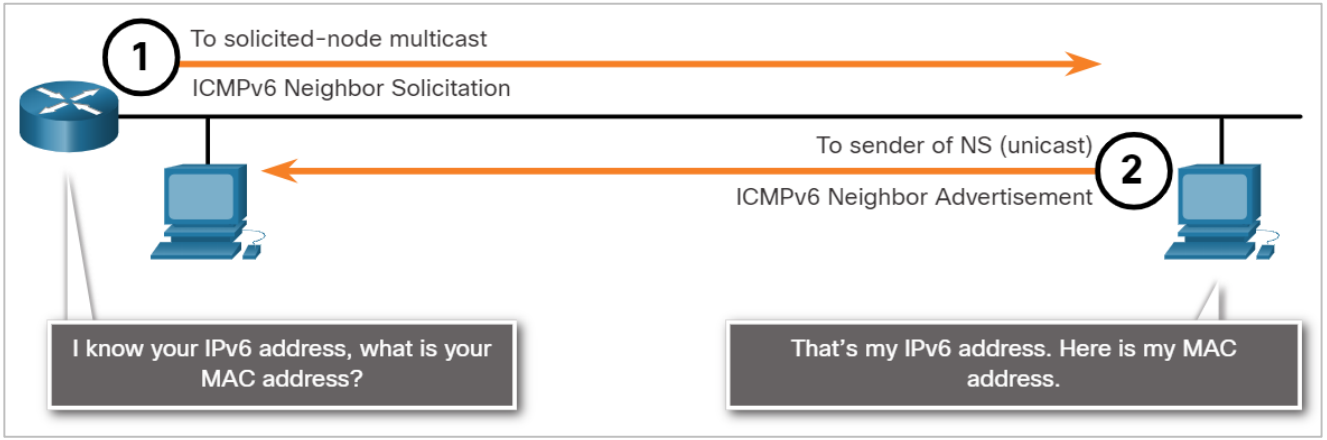
ICMPv6: Router Solicitation

- Between an IPv6 Router and an IPv6 Device
- RA messages are sent by routers to provide addressing information to hosts using Stateless Address Auto Configuration (SLAAC).
- A router will send an RA message periodically or in response to an RS message. A host using SLAAC will set its default gateway to the link-local address of the router that sent the RA.
- When a host is configured to obtain its addressing information automatically using SLAAC, the host will send an RS message to the router requesting an RA message.



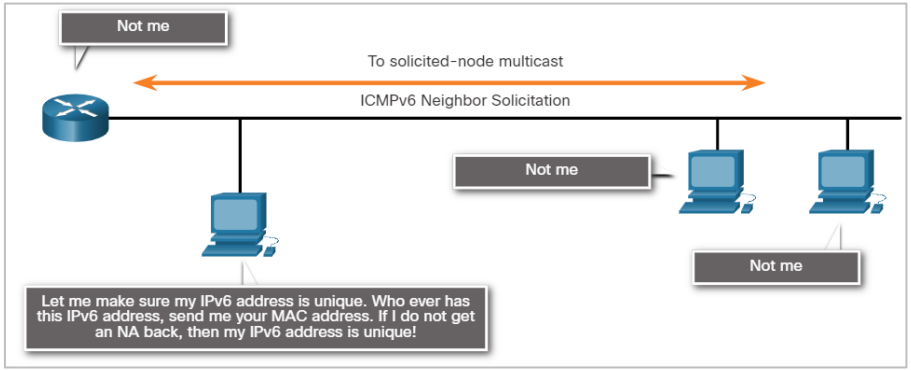
ICMPv6: Address Resolution

- Messaging Between IPv6 Devices
- NA messages are sent when a device knows the IPv6 address of a device but does not know its MAC address. This is equivalent to an ARP Request for IPv4.
- NA messages are sent in response to an NS message and match the target IPv6 address in the NS. The NA message includes the device's Ethernet MAC address. This is equivalent to an ARP Reply in IPv4.



ICMPv6: DAD

- Duplicate Address Detection (DAD)
- When a device is assigned a global unicast or link-local unicast address, the DAD is performed on the address to ensure that it is unique.
- To check the uniqueness of an address, the device will send an NS message with its own IPv6 address.
- If another device on the network has this address, it will respond with an NA message which will notify the sending device that the address is in use. If a corresponding NA message is not returned within a certain period of time, the unicast address is unique and acceptable for use.



7.2 Ping and Traceroute Utilities

Ping – Test Connectivity

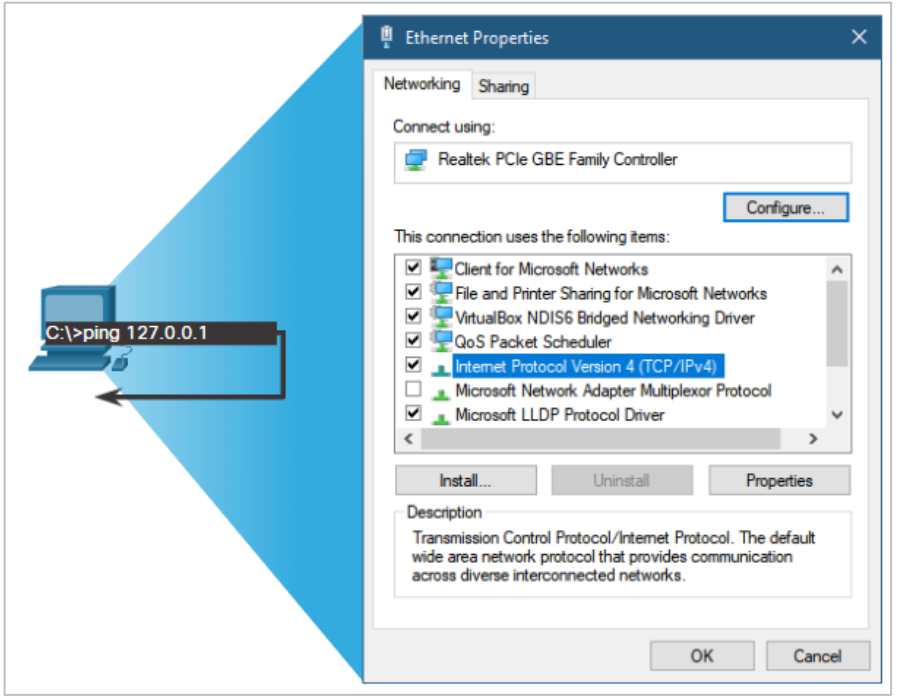
- Ping is an IPv4 and IPv6 testing utility that uses ICMP echo request and echo reply messages to test connectivity between hosts.
- To test connectivity to another host on a network, an echo request is sent to the host address using the **ping** command. If the host at the specified address receives the echo request, it responds with an echo reply.
- As each echo reply is received, **ping** provides feedback on the time between when the request was sent and when the reply was received. This can be a measure of network performance.
- Ping has a timeout value for the reply. If a reply is not received within the timeout, ping provides a message indicating that a response was not received.

Ping – Test Connectivity (Contd.)

- After all the requests are sent, the **ping** utility provides a summary that includes the success rate and average round-trip time to the destination.
- Type of connectivity tests performed with **ping** include the following:
  - Pinging the local loopback
  - Pinging the default gateway
  - Pinging the remote host

Ping the Loopback

- Ping can be used to test the internal configuration of IPv4 or IPv6 on the local host.
- To perform this test, **`ping`** the local loopback address of 127.0.0.1 for IPv4 (::1 for IPv6).
- A response from 127.0.0.1 for IPv4, or ::1 for IPv6, indicates that IP is properly installed on the host. This response comes from the network layer.
- This response tests IP down through the network layer of IP.
- An error message indicates that TCP/IP is not operational on the host.
- Pinging the local host confirms that TCP/IP is installed and working on the local host.
- Pinging 127.0.0.1 causes a device to ping itself.

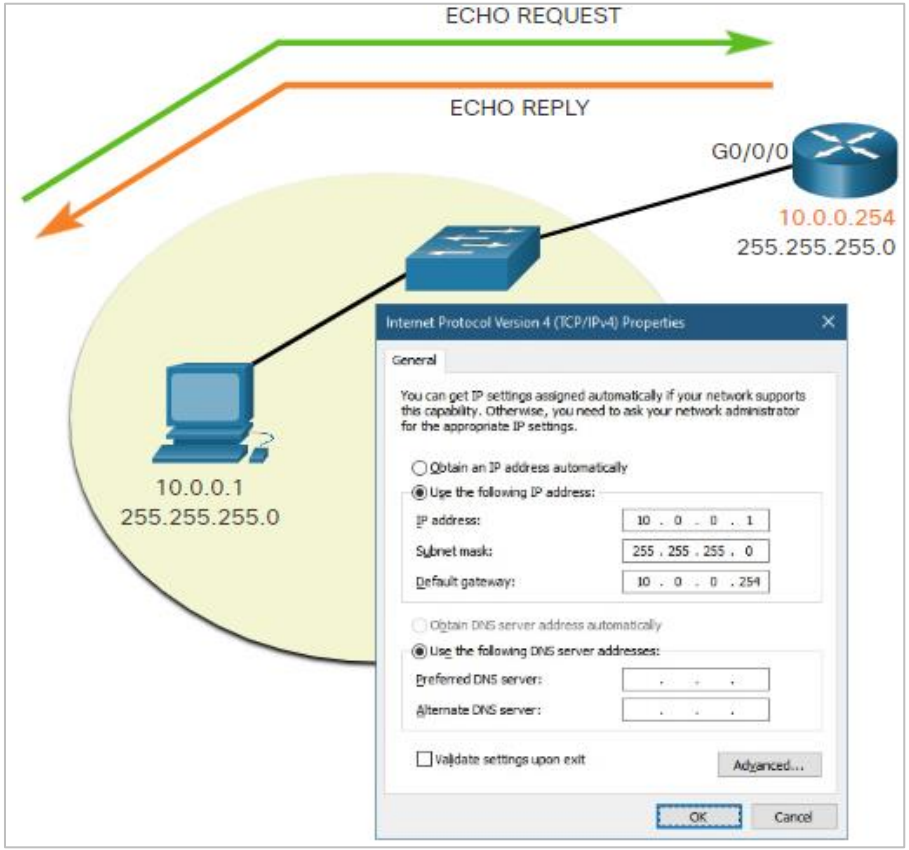


Ping the Default Gateway

- The **ping** can be used to test the ability of a host to communicate on the local network. This is done by pinging the IP address of the default gateway of the host.
- A successful **ping** to the default gateway indicates that the host and the router interface serving as the default gateway are both operational on the local network.
- For this test, the default gateway address is mostly used as the router is always operational. If the default gateway address does not respond, a **ping** can be sent to the IP address of another host on the local network that is operational.
- If either the default gateway or another host responds, then the local host can successfully communicate over the local network.
- If the default gateway does not respond but another host does, this could indicate a problem with the router interface serving as the default gateway.
- One possibility is that the wrong default gateway address been configured on the host or the router interface may be fully operational but have security applied to it.

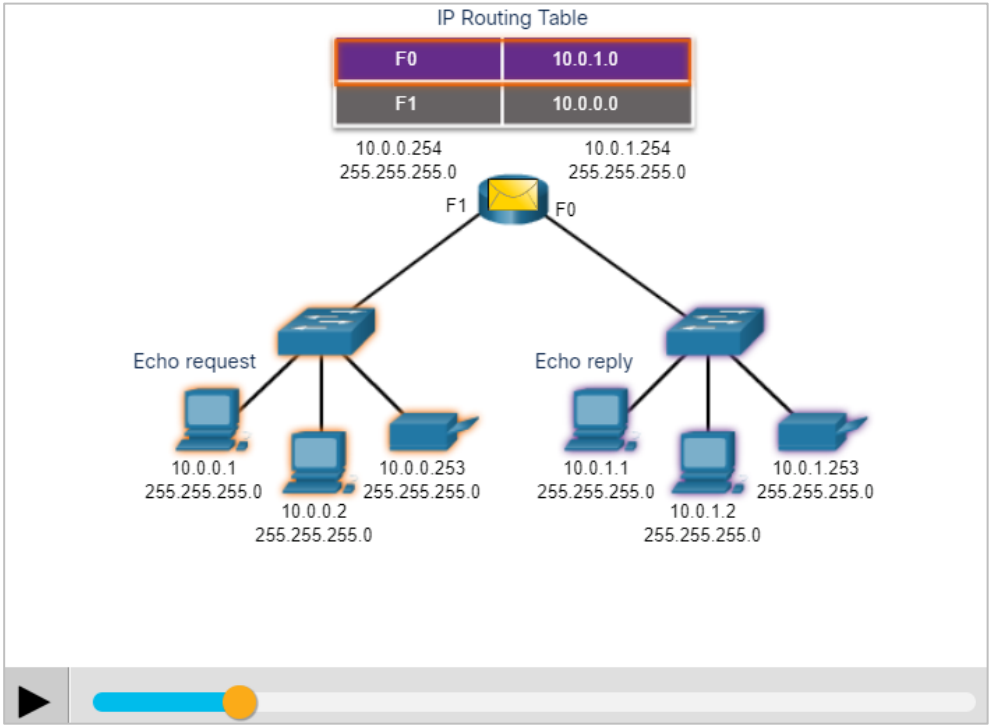
Ping the Default Gateway (Contd.)

- The host pings its default gateway, sending an ICMP echo request. The default gateway sends an echo reply confirming connectivity.



Ping a Remote Host

- Ping can also be used to test the ability of a local host to communicate across an internetwork. The local host can ping an operational IPv4 host of a remote network.
- The router uses its IP routing table to forward the packets.
- If this ping is successful, the operation of a large piece of the internetwork and the functionality of the remote host can be verified.
- A successful **`ping`** across the network confirms communication on the local network, the operation of the router as the default gateway, and the operation of all other routers in the path between the local network and the network of the remote host.



Traceroute - Test the Path

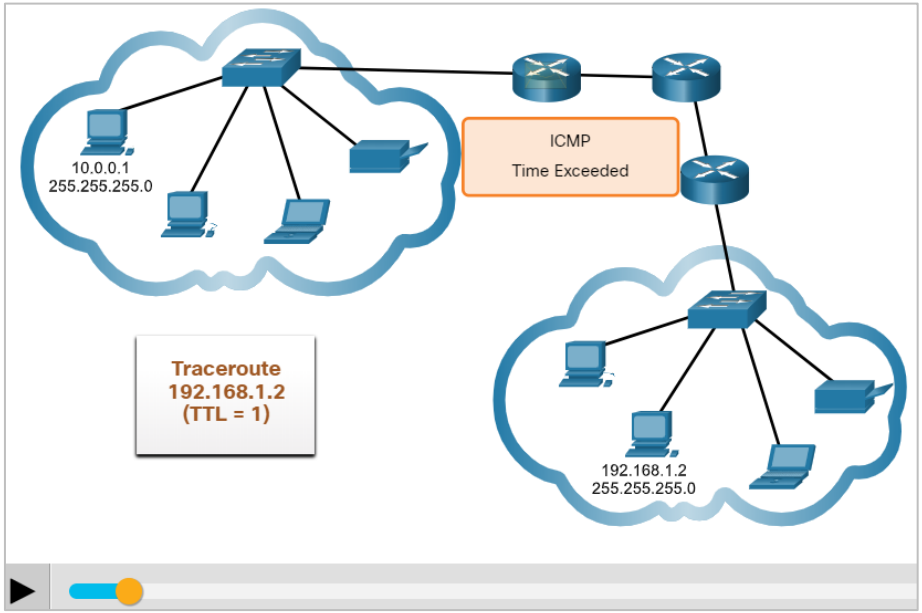
- Ping is used to test connectivity between two hosts but does not provide information about the details of devices between the hosts.
- Traceroute (**tracert**) is a utility that generates a list of hops that were successfully reached along the path. This list can provide important verification and troubleshooting information.
- If the data reaches the destination, then the trace lists the interface of every router in the path between the hosts.
- If the data fails at some hop along the way, the address of the last router that responded to the trace can provide an indication of where the problem or security restrictions are found.

Traceroute: Round Trip Time (RTT)

- The traceroute provides a round-trip time for each hop along the path and indicates if a hop fails to respond.
- The round-trip time is the time a packet takes to reach the remote host and for the response from the host to return.
- An asterisk (*) is used to indicate a lost or unreplied packet.
- This information can be used to locate a problematic router in the path or may indicate that the router is configured not to reply.
- If the display shows high response times or data losses from a particular hop, this is an indication that the resources of the router or its connections may be overused.

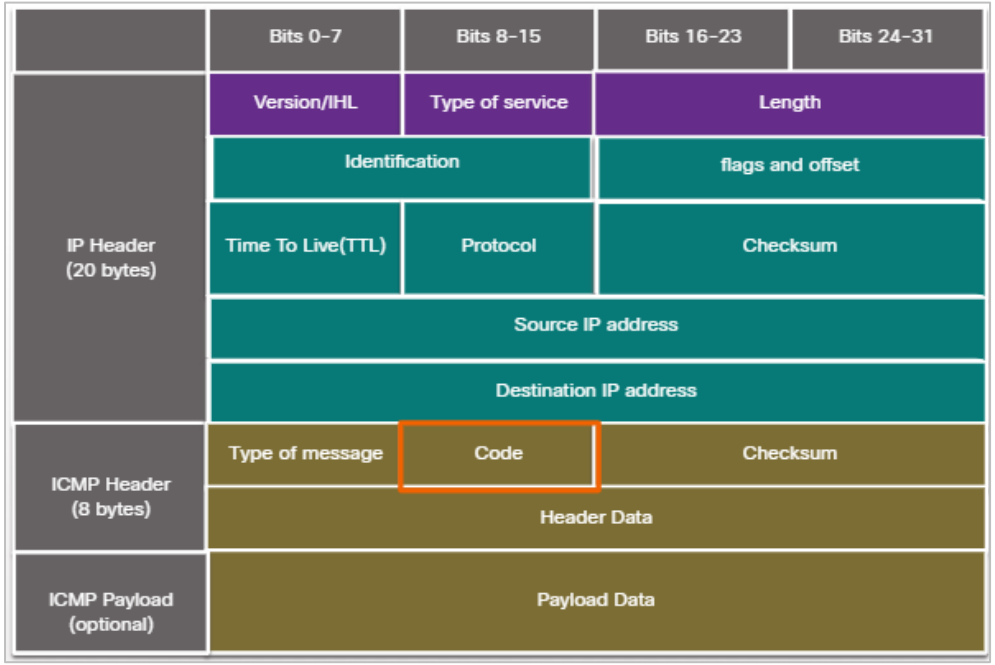
Traceroute - Test the Path (Contd.)

- IPv4 TTL and IPv6 Hop Limit: Traceroute uses the function of the TTL field in IPv4 and the Hop Limit field in IPv6 in the Layer 3 headers, along with the ICMP Time Exceeded message.
  - The first sequence of messages sent from traceroute have a TTL field value of 1 which causes the TTL to time out the IPv4 packet at the first router. This router then responds with an ICMPv4 Time Exceeded message. Traceroute now has the address of the first hop.
  - Traceroute then progressively increments the TTL field (2, 3, 4...) for each sequence of messages. This provides the trace with the address of each hop as the packets time out further down the path. The TTL field continues to be increased until the destination is reached.
  - After the final destination is reached, the host responds with either an ICMP Port Unreachable message or an ICMP Echo Reply message instead of the ICMP Time Exceeded message.



ICMP Packet Format

- ICMP is encapsulated directly into IP packets.
- ICMP acts as a data payload within the IP packet. It has a special header data field.
- It uses message codes to differentiate between different types of ICMP messages. These are some common message codes:
  - **0 –** Echo reply (response to a ping)
  - **3 –** Destination Unreachable
  - **5 –** Redirect (use another route to the destination)
  - **8 –** Echo request (for ping)
  - **11 –** Time Exceeded (TTL became 0)



Lab - Tracing a Route

In this lab, you will use two route tracing utilities to examine the internet pathway to destination networks. The objective will be to:

- Verify connectivity to a website
- Use the traceroute utility on the Linux command line
- Use a web-based traceroute tool

b. Open a terminal window in the VM to ping a remote server, such as www.cisco.com.

```
[analyst@secOps ~]$ ping -c 4 www.cisco.com
PING e2867.dsca.akamaiedge.net (184.24.123.103) 56(84) bytes of data.
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103):
icmp_seq=1 ttl=59 time=13.0 ms
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103):
icmp_seq=2 ttl=59 time=12.5 ms
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103):
icmp_seq=3 ttl=59 time=14.9 ms
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103):
icmp_seq=4 ttl=59 time=11.9 ms
```

Thank you! Questions?

Vladimír Veselý

updated: 2024-02-16

https://www.fit.vutbr.cz/research/groups/nes@fit

Module 8:
Address Resolution Protocol

Instructor Materials

CyberOps Associate v1.0

Module Objectives

- Module Title: Address Resolution Protocol
- Module Objective: Analyze address resolution protocol PDUs on a network.

Topic Title	Topic Objective
MAC and IP	Compare the roles of the MAC address and the IP address.
ARP	Analyze ARP by examining Ethernet frames.
ARP Issues	Explain how ARP requests impact network and host performance as well as potential security risks.

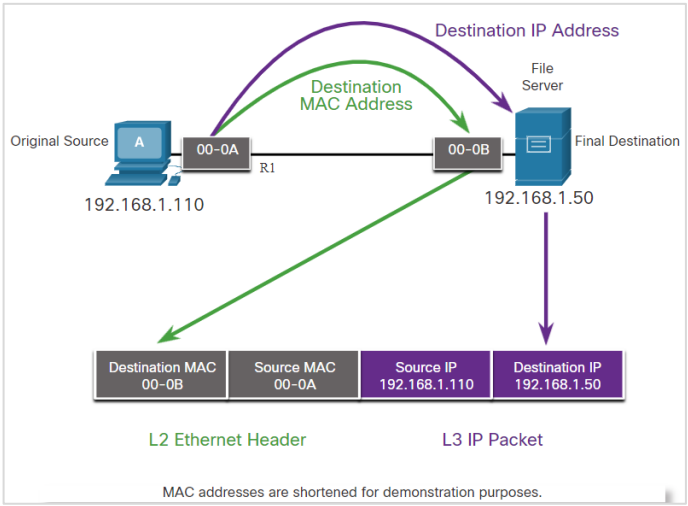
8.1 MAC and IP

Destination on Same Network

- The two primary addresses assigned to a device on an Ethernet LAN:

Primary Addresses on Ethernet LAN	Description
Physical Address (The Mac Address)	• Used for Ethernet NIC to Ethernet NIC communications on the same network. • If the destination IP address is on the same network, the destination MAC address will be that of the destination device.
Logical Address (The IP Address)	• Used to send the packet from the original source to the final destination. • The destination IP address may be on the same IP network as the source or may be on a remote network.

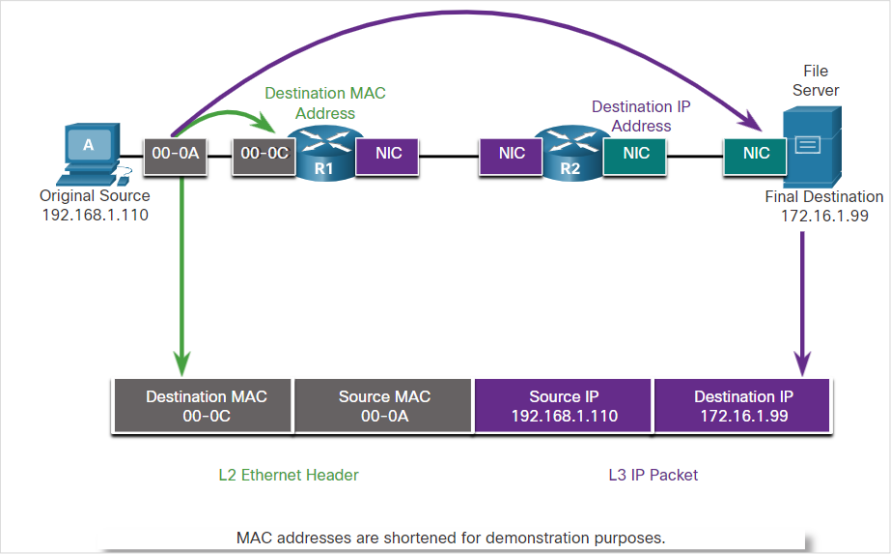
- ***Note**: Most applications use Domain Name System (DNS) to determine the IP address when given a domain name such as [www.cisco.com.](http://www.cisco.com)*



Communicating on a local network

Destination on Remote Network

- When the destination IP address is on a remote network, the destination MAC address will be the address of the host's default gateway. The process in the figure is as below:
  - Routers examine the destination IPv4 address.
  - When the router receives the Ethernet frame, it de-encapsulates the Layer 2 information.
  - Using the destination IP address, the router determines the next-hop device, and then encapsulates the IP packet in a new data link frame for the outgoing interface.
  - If the next-hop device is the final destination, the destination MAC address will be that of the device's Ethernet NIC.

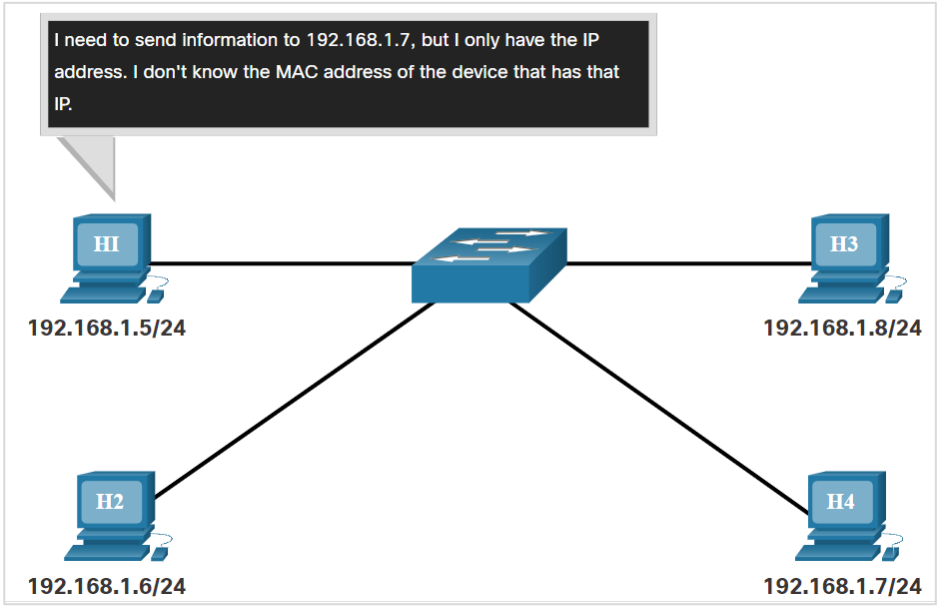


Communicating on a remote network

8.2 ARP

ARP Overview

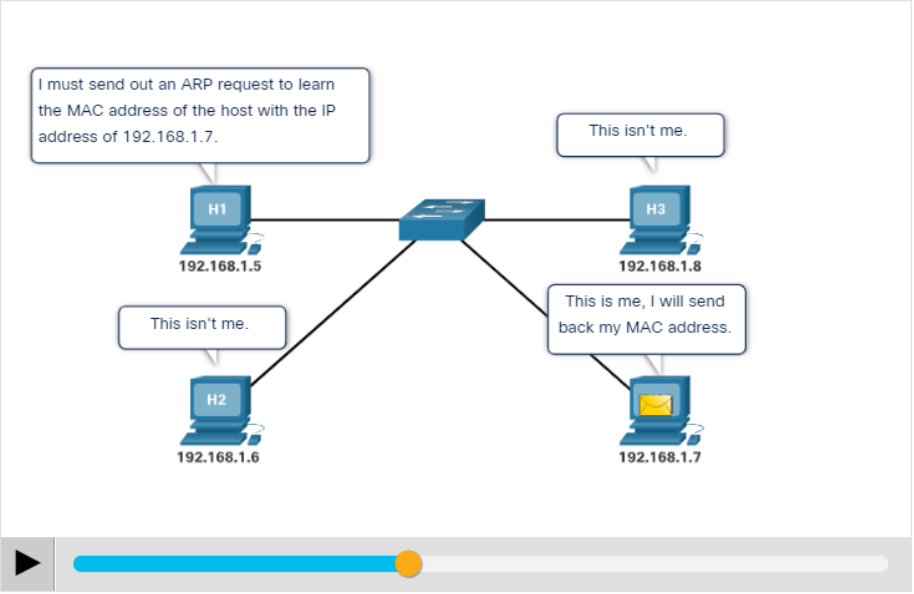
- The figure illustrates a problem while sending a packet to another host on the same local IPv4 network because the IP address is known but the MAC address of the device is unknown.
- A device uses Address Resolution Protocol (ARP) to determine the destination MAC address of a local device when it knows its IPv4 address.
- ARP provides two basic functions:
  - Resolving IPv4 addresses to MAC addresses
  - Maintaining a table of IPv4 to MAC address mappings



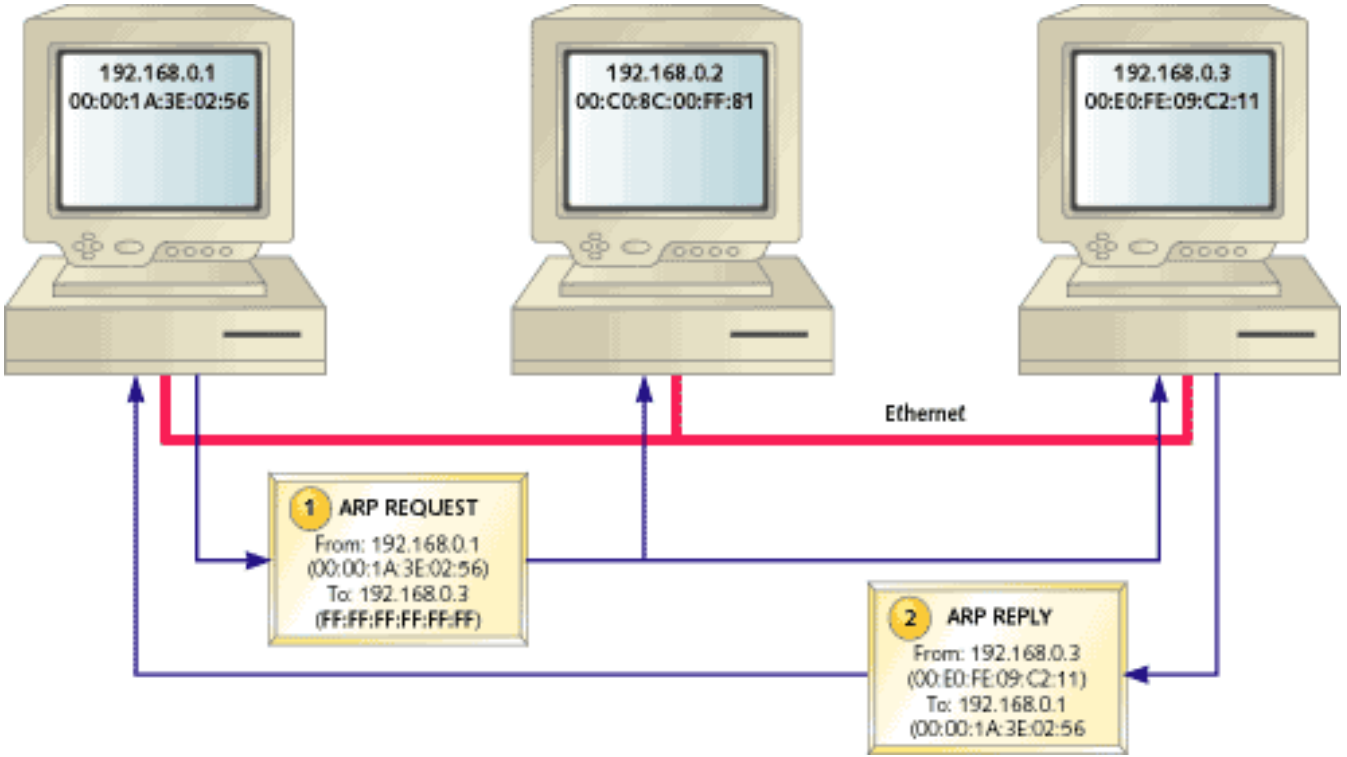
ARP Functions

- When a packet is sent to the data link layer to be encapsulated into an Ethernet frame, the device refers to a table called **ARP table** or ARP cache in its RAM memory to find the MAC address that is mapped to the IPv4 address.
- The sending device will search its ARP table for a destination IPv4 address and a corresponding MAC address, if the packet's destination IPv4 address is on the same network as the source IPv4 address.
- If the device locates the IPv4 address, its corresponding MAC address is used as the destination MAC address in the frame.

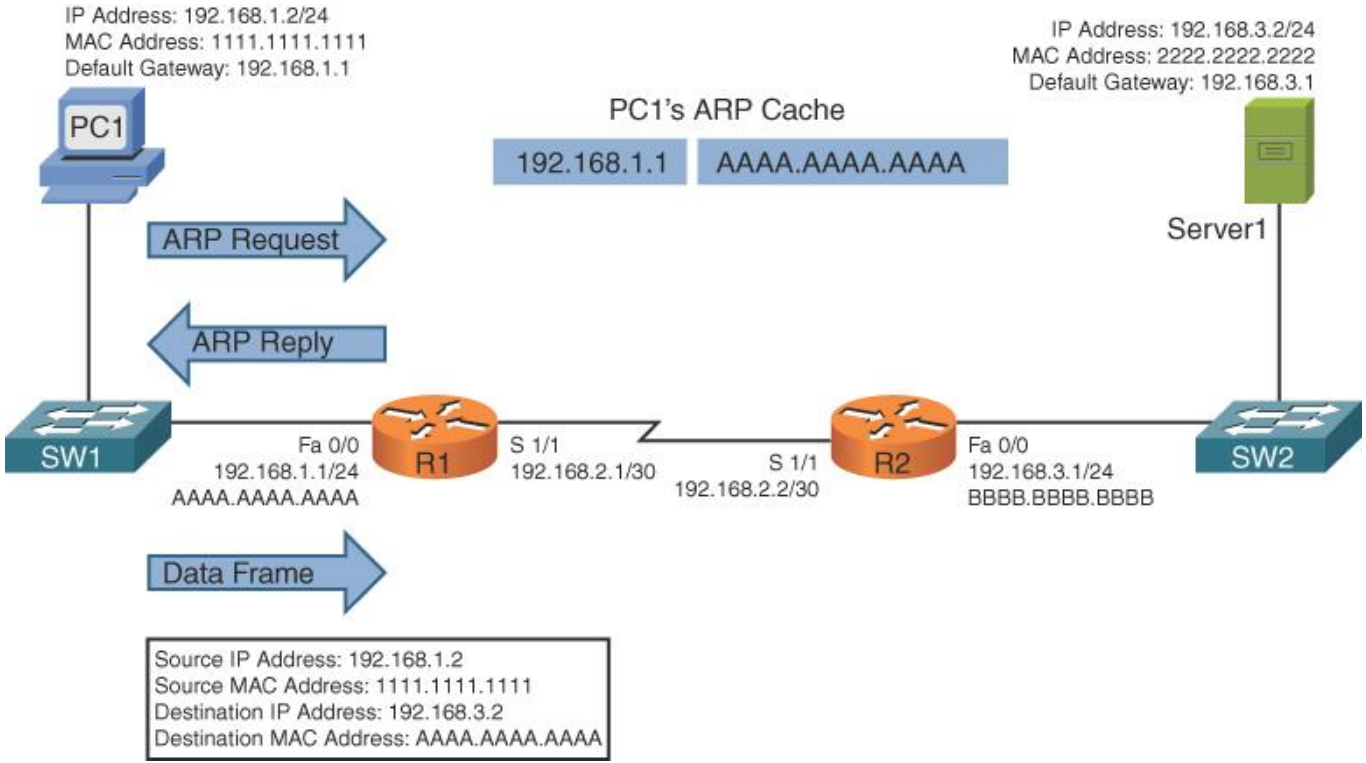
Click play in the figure to see an animation of the ARP function.



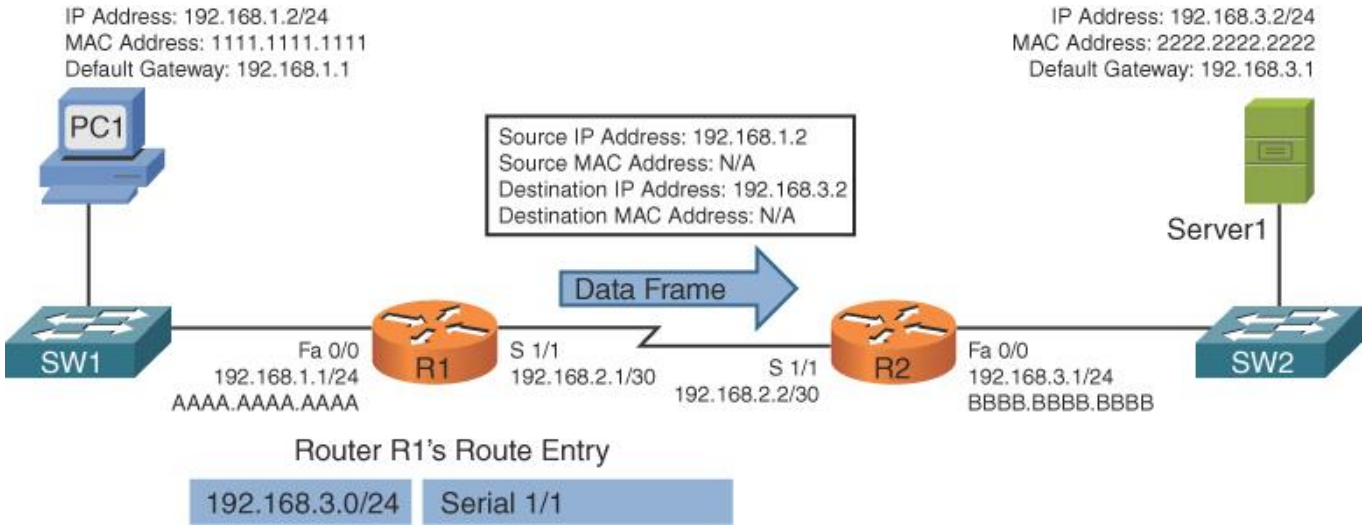
ARP Request and Response



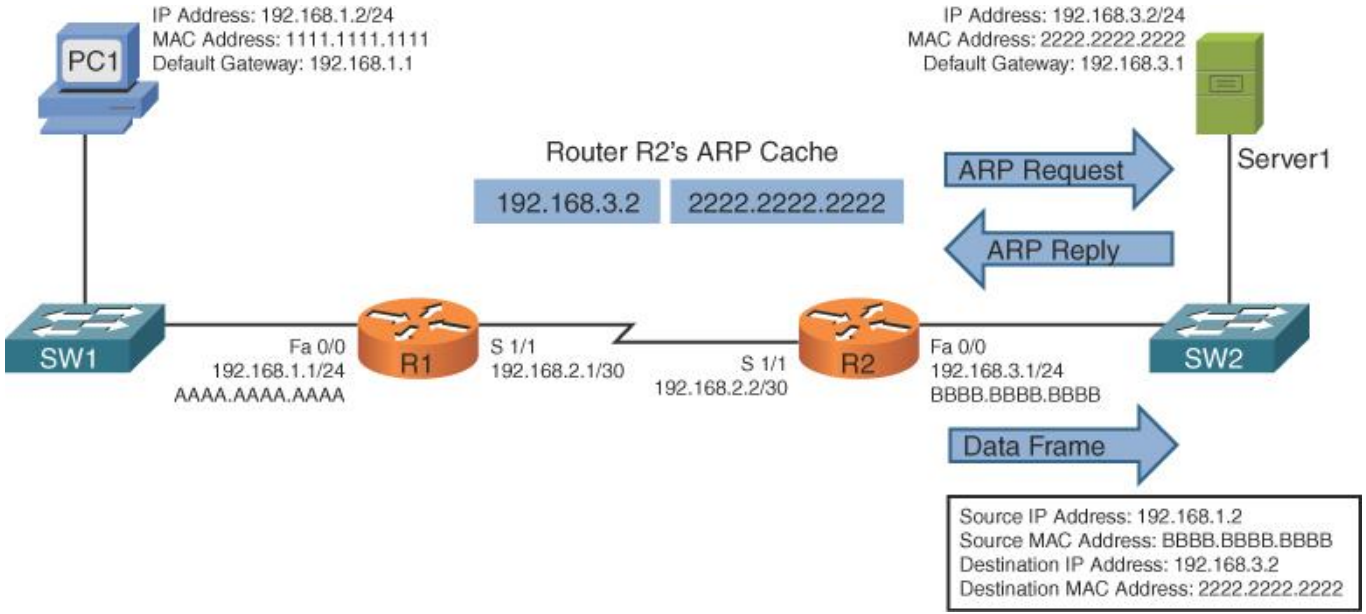
ARP Remote Connection



ARP Remote Connection

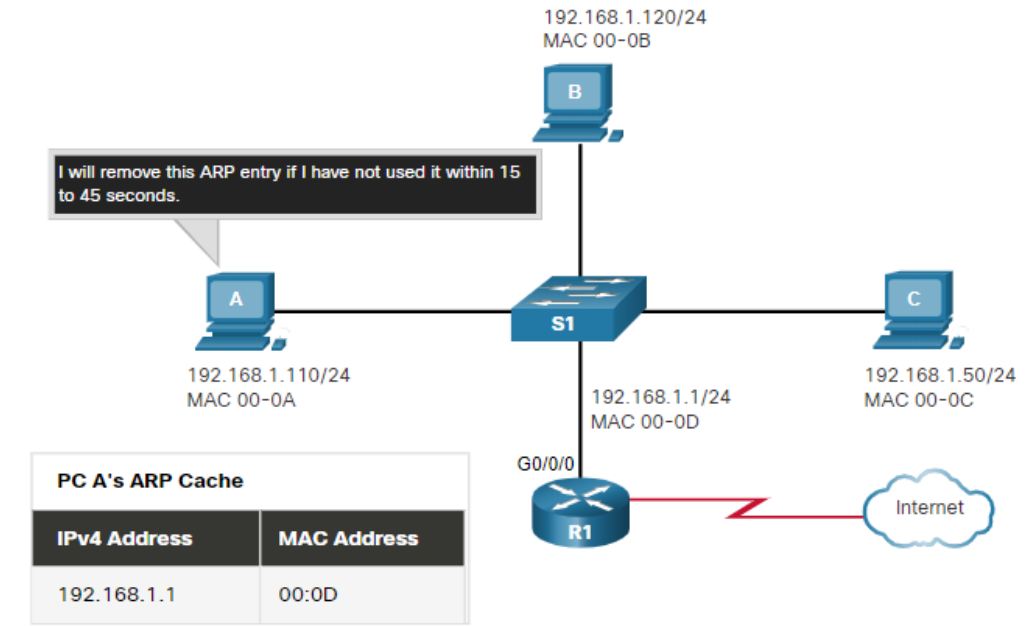


ARP Remote Connection



Removing Entries from an ARP Table

- For each device, an ARP cache timer removes the ARP entries that have not been used for a specified period of time.
- The times differ depending on the operating system of the device.
- Commands may also be used to manually remove some or all of the entries in the ARP table.
- After an entry has been removed, the process for sending an ARP request and receiving an ARP reply must occur again to enter the map in the ARP table.



ARP Tables on Networking Devices

On a Cisco router,
the **`show ip arp`** command is used to display the ARP table.

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1           -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
Internet  209.165.200.225         -   a0e0.af0d.e141  ARPA   GigabitEthernet0/0/1
Internet  209.165.200.226         1   a03d.6fe1.9d91  ARPA   GigabitEthernet0/0/1
R1#
```

On a Windows 10 PC,
the **`arp -a`** command is used to display the ARP table.

```
C:\Users\PC> arp -a
Interface: 192.168.1.124 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           c8-d7-19-cc-a0-86     dynamic
  192.168.1.101         08-3e-0c-f5-f7-77     dynamic
  192.168.1.110         08-3e-0c-f5-f7-56     dynamic
  192.168.1.112         ac-b3-13-4a-bd-d0     dynamic
  192.168.1.117         08-3e-0c-f5-f7-5c     dynamic
  192.168.1.126         24-77-03-45-5d-c4     dynamic
  192.168.1.146         94-57-a5-0c-5b-02     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
C:\Users\PC>
```

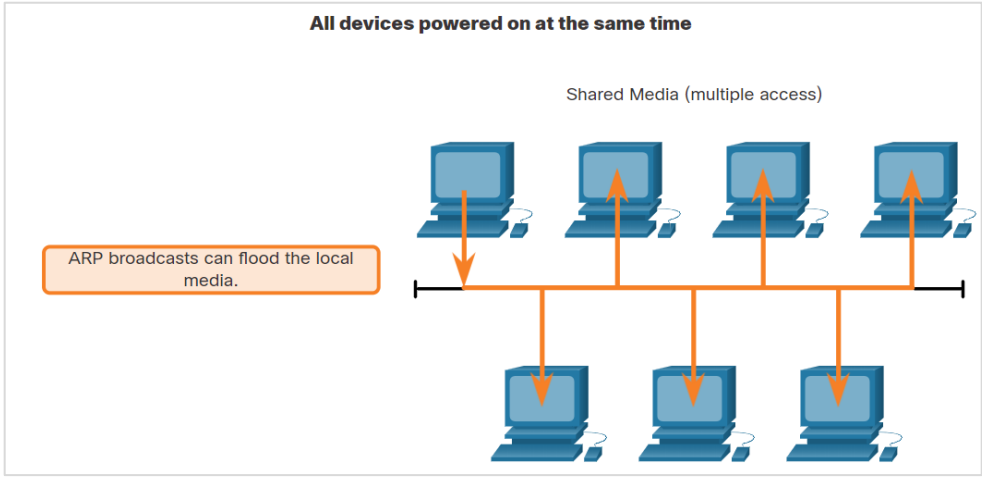
Lab - Wireshark to Examine Ethernet Frames

- In this lab, you will do the following:
- Use Wireshark to capture and view Ethernet Frames in order to investigate ARP and IP and MAC addressing.
- Capture and analyze ICMP frames.

8.3 ARP Issues

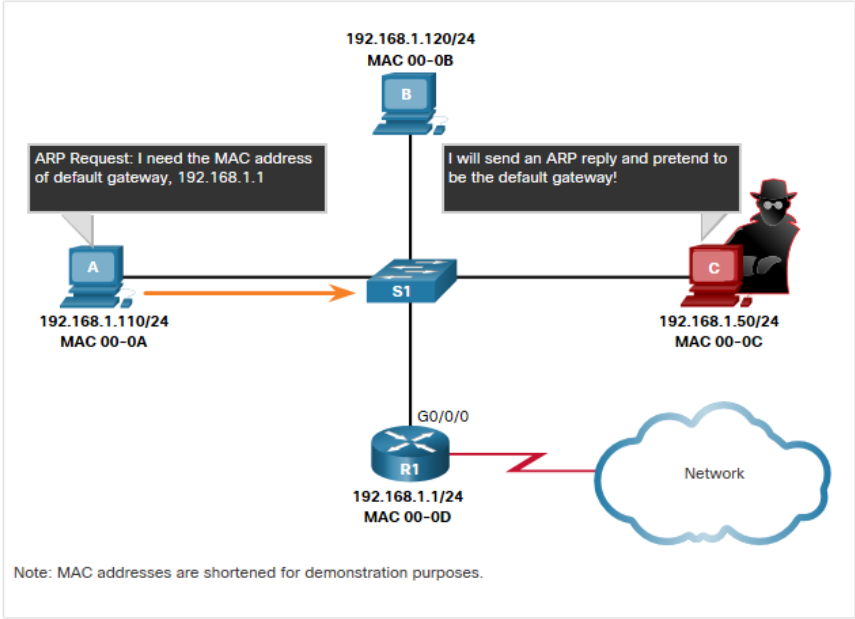
ARP Broadcasts

- As a broadcast frame, an ARP request is received and processed by every device on the local network.
- On a typical business network, these broadcasts would have minimal impact on network performance.
- If many devices start accessing network services at the same time, there can be reduction in performance for a short time.
- After the devices send out the initial ARP broadcasts and have learned the necessary MAC addresses, any impact on the network will be minimized.

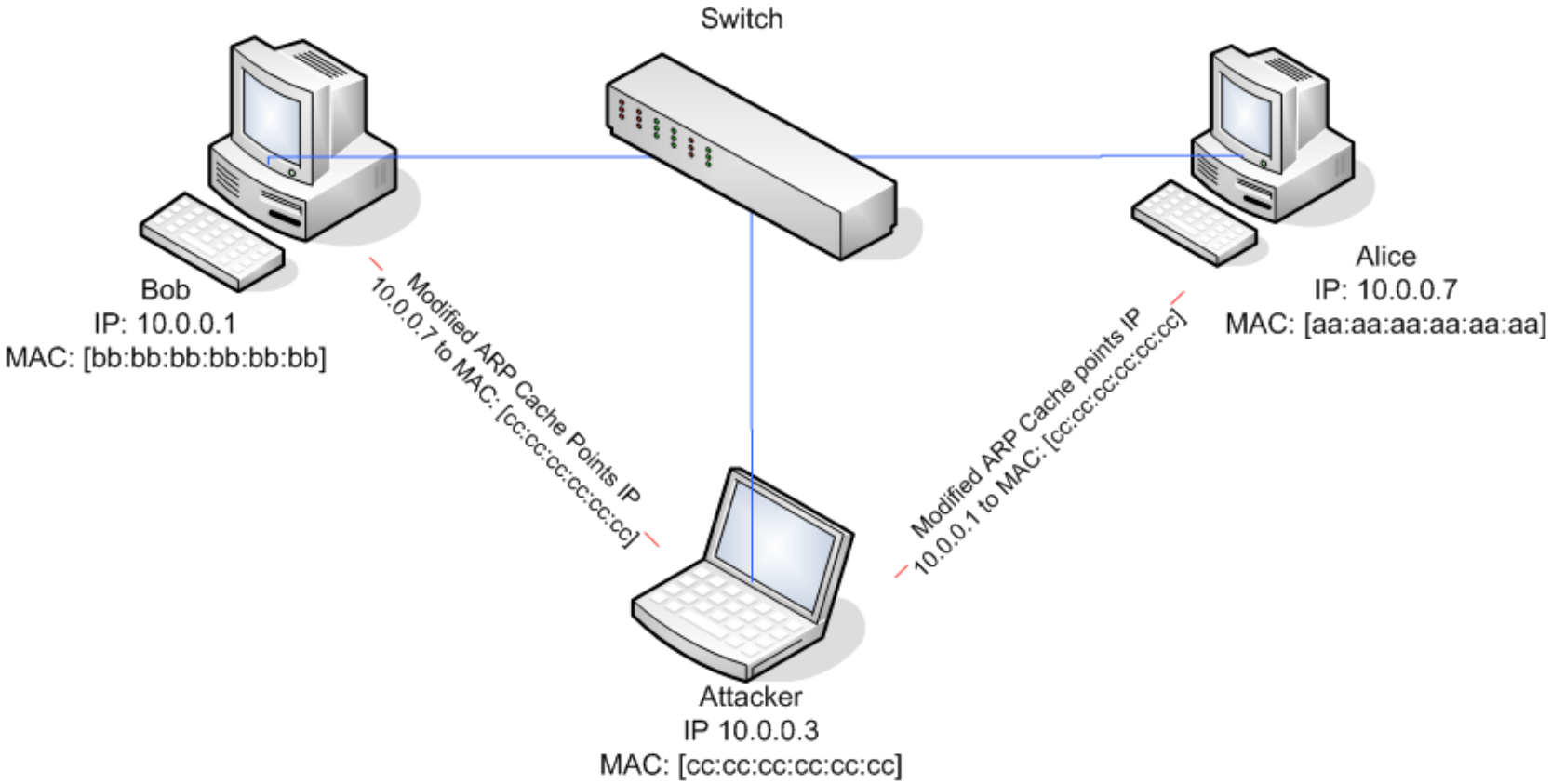


ARP Spoofing

- The use of ARP can lead to a potential security risk in some cases.
- A threat actor uses ARP spoofing to perform an ARP poisoning attack.
  - It is a technique used by a threat actor to reply to an ARP request for an IPv4 address belonging to another device, such as the default gateway.
  - The threat actor sends an ARP reply with its own MAC address.The receiver of the ARP reply will add the wrong MAC address to its ARP table and send these packets to the threat actor.



ARP Spoofing



Thank you! Questions?

Vladimír Veselý

updated: 2024-02-16

https://www.fit.vutbr.cz/research/groups/nes@fit