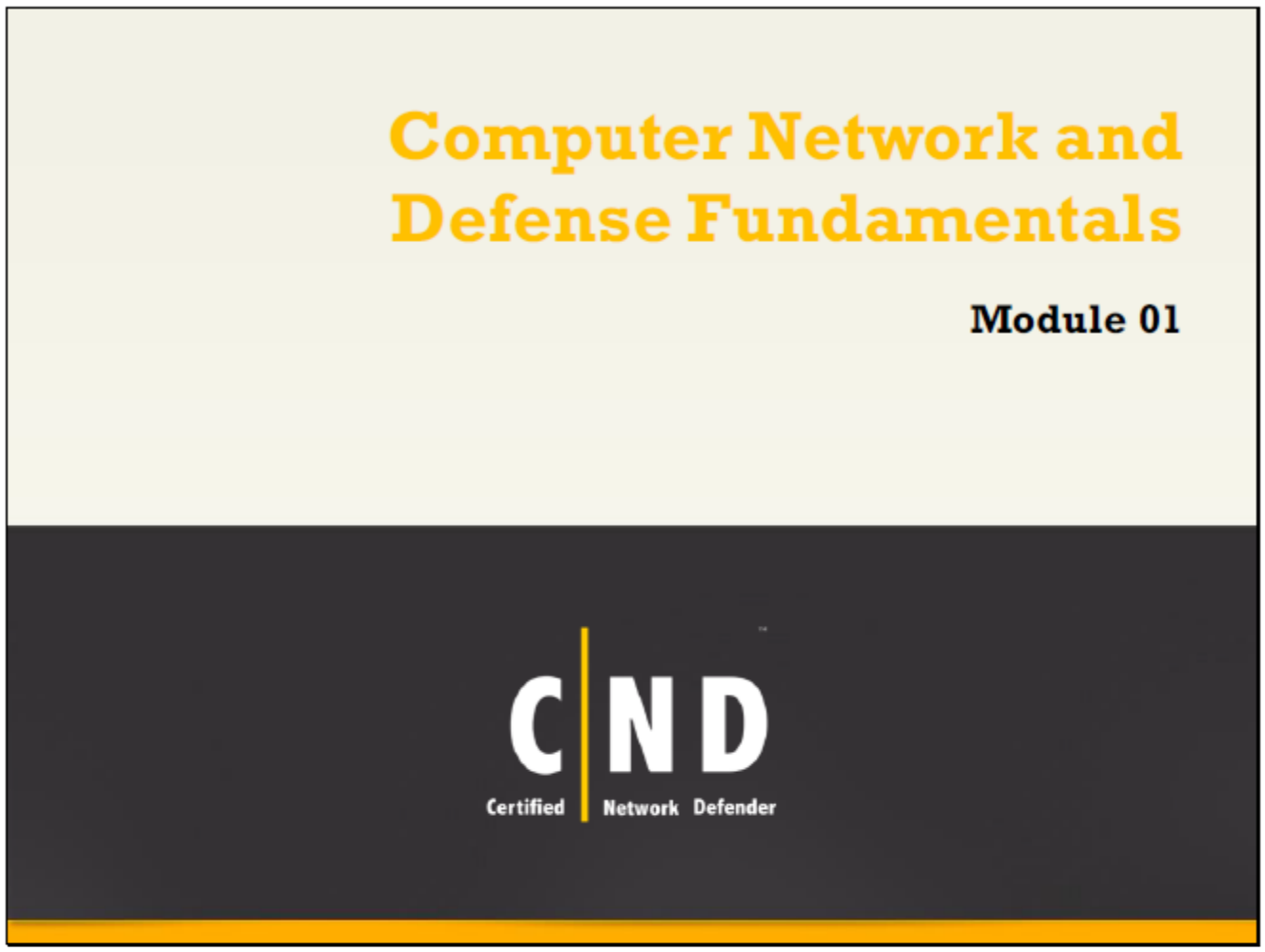
Computer Network and Defense Fundamentals

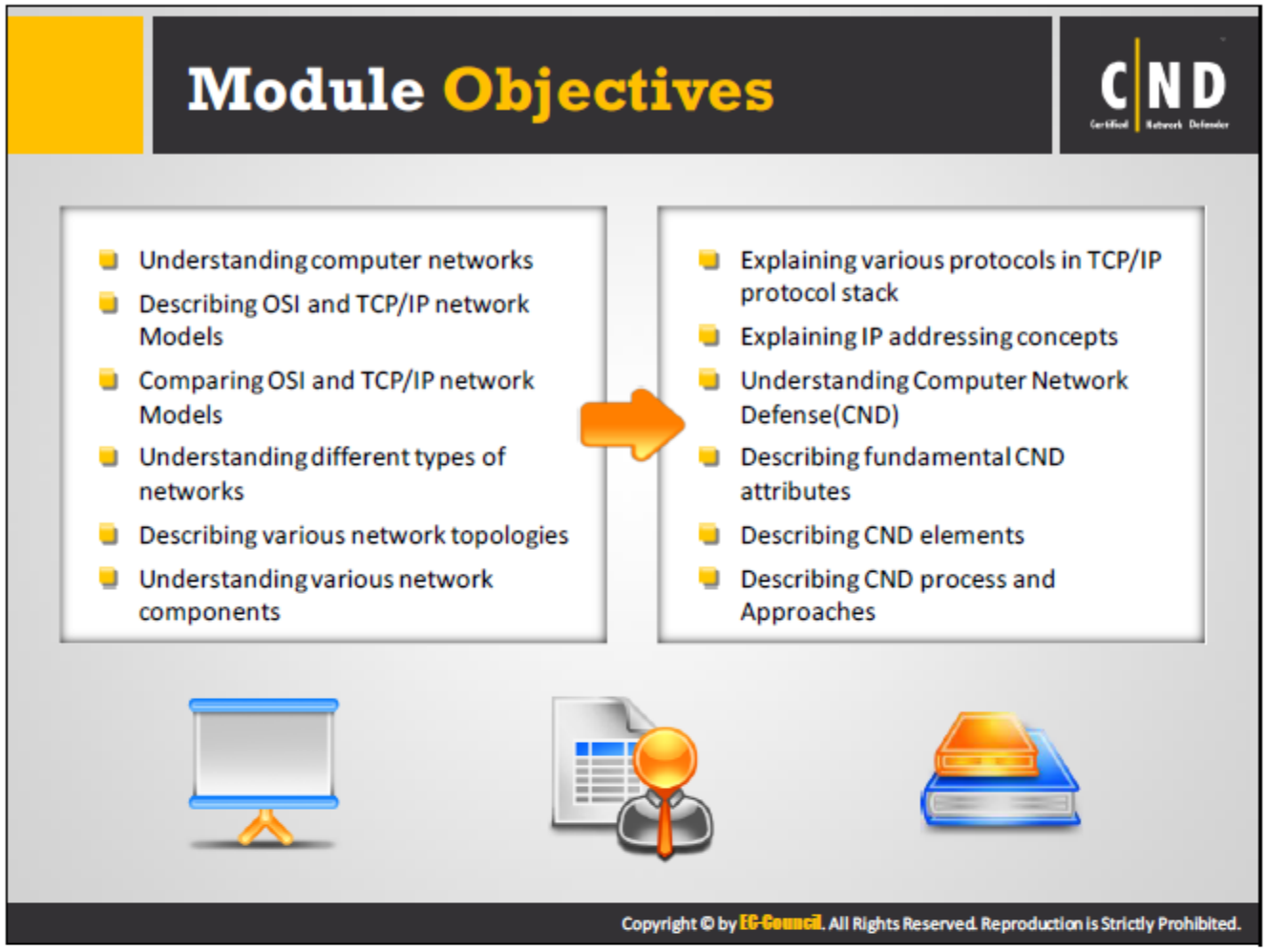
Module 01



Certified Network Defender

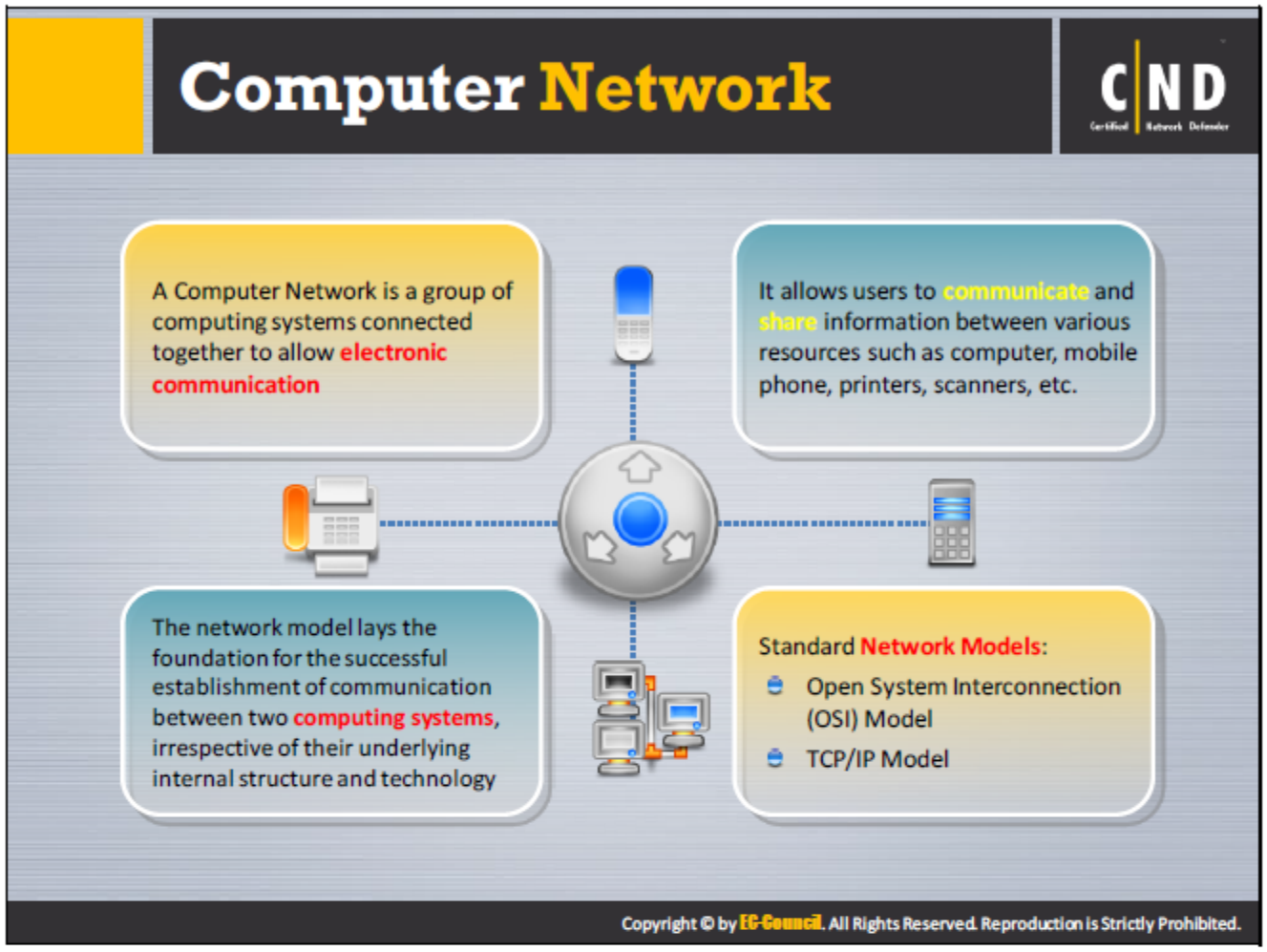
Module 01: Computer Network and Defense Fundamentals

Exam 312-38



The module briefs you on the basic concepts of computer network fundamentals, including types of networks, network topologies, network models, and various protocols used in computer networking.

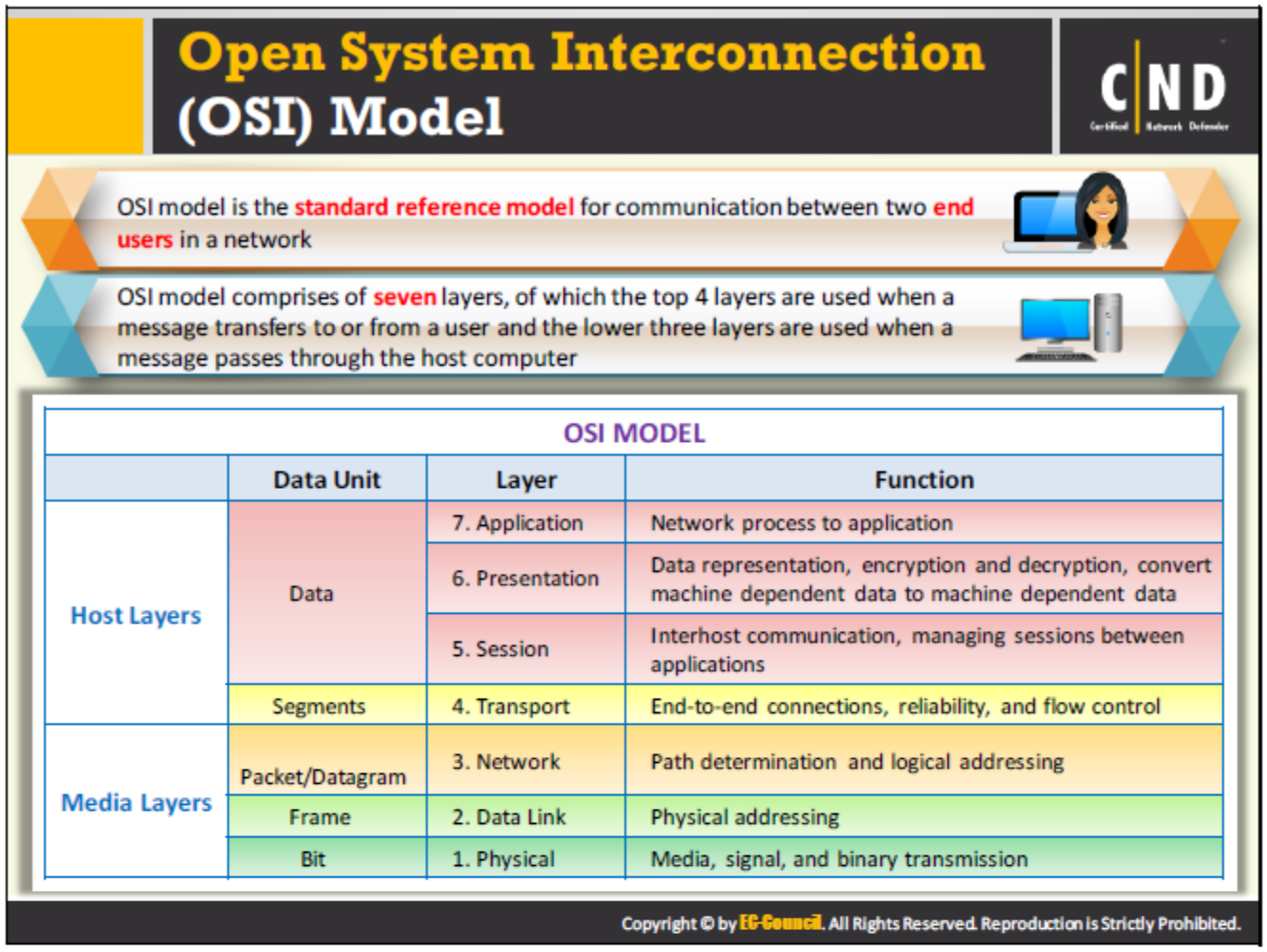
This module will also introduce you to the fundamental concepts on computer network defense. The module introduces you to different concepts about Computer Network Defense (CND) including CND attributes, different layers of CND, CND process, etc. The aim of this module is to provide students a brief overview of basic networking concepts and help you understand what CND comprises. These CND fundamentals are addressed and then elaborated on separately using subsequent modules to attain defense-in-depth (DID) network security.



A computer network is a group of computers connected to each other for easy sharing of information and resources. The computers share information using a data path. A commonly known computer network is the internet. Features of computer networks include:

- Allows sharing of resources from one computer to another.
- Allows storing files and other information in one computer and other computers accessing those files and information.
- Any device connected to a computer can access the files and information stored in another computer via the network.

In many fields such as electrical engineering, telecommunications, Computer science, Information technology make use of computer networking concepts. These allow for easy communication between the users by means of chat, email, instant messaging etc. The computer network allows sharing of data across the networks.



Open System Interconnection (OSI) is a reference model that defines the communication of data over the network. It is a framework that portrays the flow of data from one device to another over the network. The OSI model classifies the communication between two end-points into seven different groups of layers. The logic behind this division is that the communicating user provides functions of each of the seven layers. The communication between two users occurs as a downward flow of data through the layers of the source computer. Then, it traverses across the network and flows upwards through the layers of the destination computer.

Features of OSI model include:

- Provides a clear understanding regarding the communication over the network.
- Displays the working of software and hardware.
- Helps the users in understanding newer technologies.
- Easy comparison between the functional relationships between different networks.

The OSI model has a set of protocols that allows the object on one host to communicate with the corresponding object on another host.

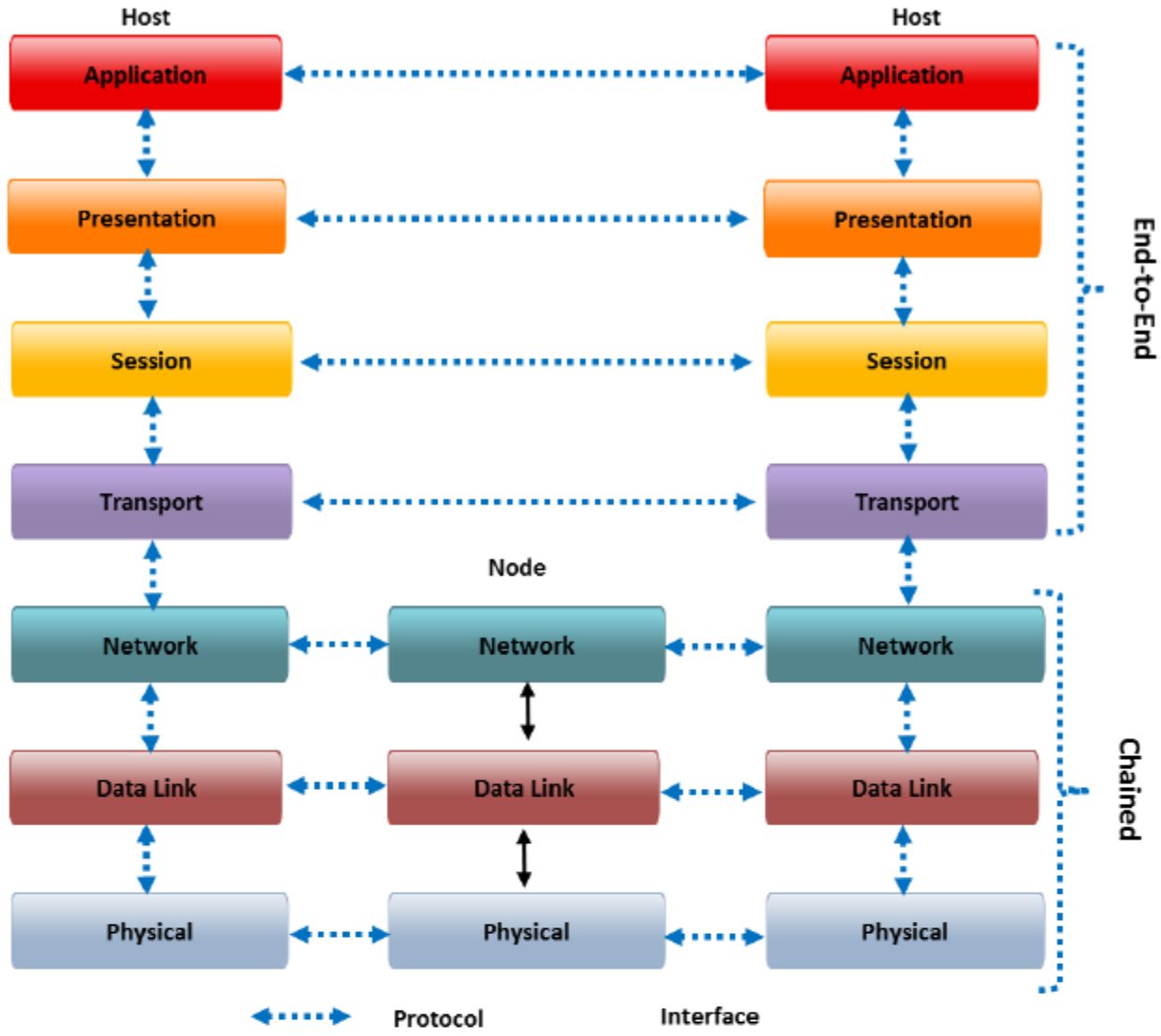
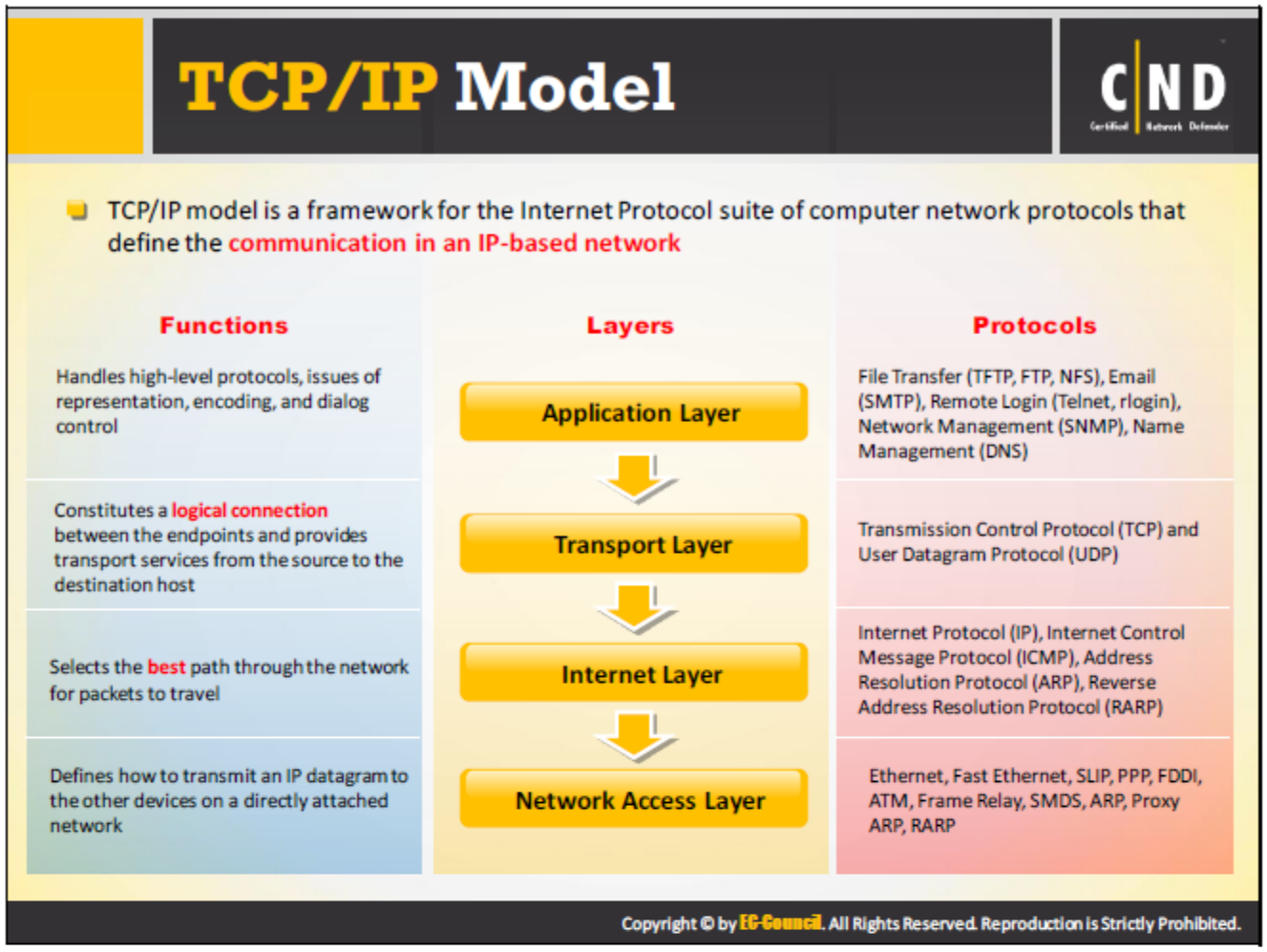


FIGURE 1.1: OSI Reference Model

Each layer in the OSI model has different levels of generalization and performs a distinct function. The principle involved in developing the seven layers of OSI model is as follows:

- Each layer needs to meet a different concept or overview. Thus creating each layer depends on the level of abstraction.
- Each layer needs to have a distinct functionality.
- The function performed by each layer needs to be in accordance with the standard protocols at each layer.
- All the functions should not be present in the same layer. Selection of layers depends on the number of functions performed.



The TCP/IP protocol is a four-layered protocol developed by the Department of Defense (DOD). Each layer in this model performs a different function and the flow of data occurs from layer 4 to 1 (from the sending machine) and from layer 1 to 4 (in the destination machine). The TCP/IP model describes the end-to-end communication between two machines and thereby determining the addressing, routing and transmission of the data. The four layers in the TCP/IP model include:

- Application layer (Layer 4): Provides data access to applications.
- Transport layer (Layer 3): Manages host-to-host interactions.
- Internet layer (Layer 2): Provides internetworking.
- Network Access layer (Layer 1): Provides communication of data present in the same network.

Network Access Layer – Layer 1

The Network Access layer is the lowest layer in the TCP/IP model. It handles the flow of data to the Internet layer between two hosts in the same network. The network-to-host layer adds a packet header to the data frame and sends it over a physical medium. The layer consists of functions such as modulation, bit and frame synchronization and error detection. The protocols used in this layer are: Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35.

Internet Layer – Layer 2

The Internet layer mainly deals with the communication of packets over the network.

It performs internetworking by sending data from the source network to the destination network. The functions performed by the Internet layer are as follows:

- Host addressing and identification
- Packet routing

The Internet layer is wholly responsible for managing the TCP/IP protocol framework. In this protocol, the sequence of the packets received at the destination network differs from the sequence of the packets sent from the source network. IP, ICMP, ARP, RARP are the protocols used in this layer.

Transport Layer – Layer 3

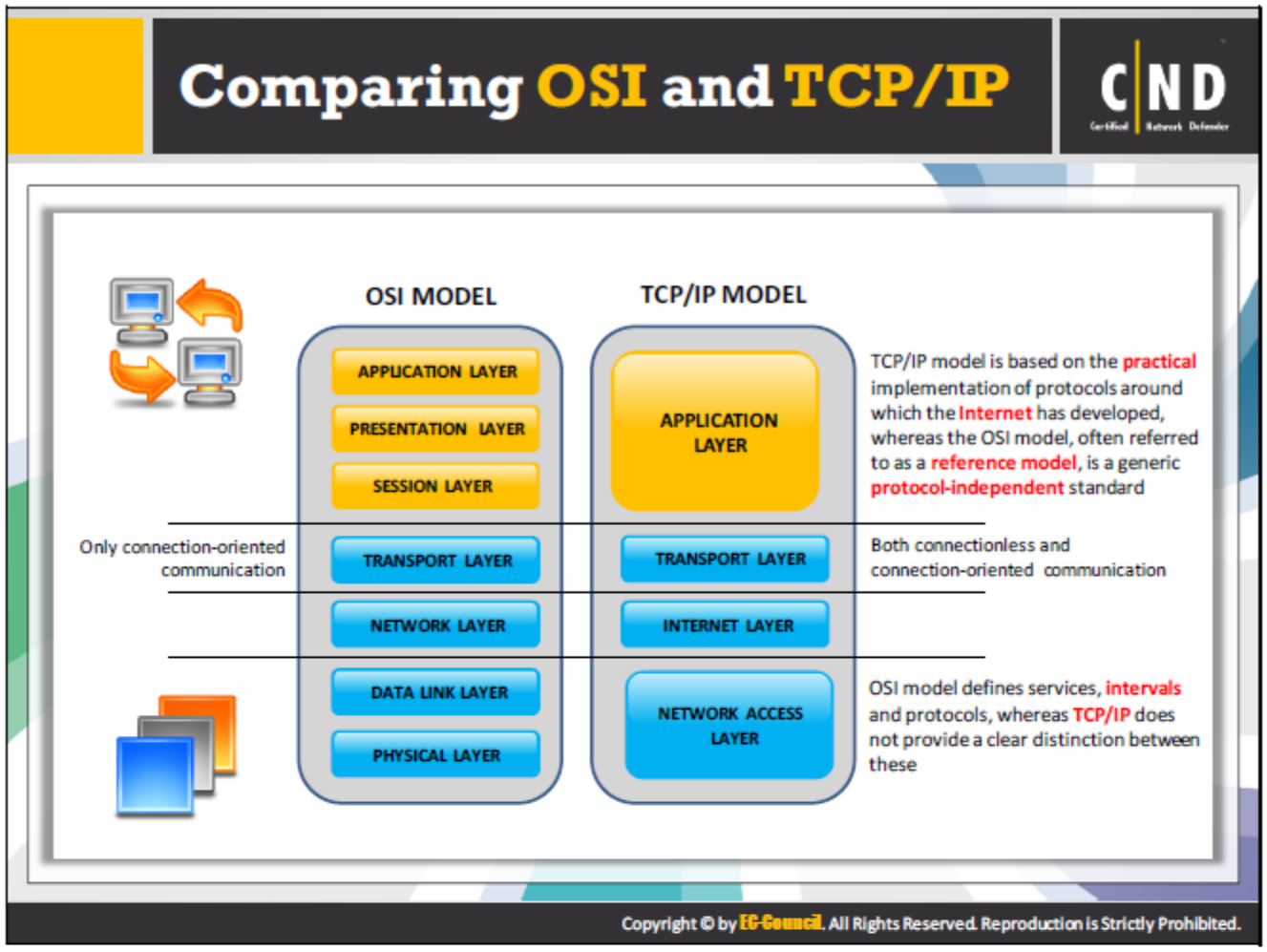
The Transport layer determines the status of the data communicating between the source and the destination. The functionalities of the Transport layer include end-to-end communication, error control, segmentation, flow control and application addressing. The end-to-end communication is of two types: connection oriented and connectionless oriented. TCP implements the connection oriented communication, whereas UDP initiates connectionless communication.

The TCP layer determines whether the data transmission occurs in a parallel path or in a single path. The layer enables the application to read and write to the transport layer by adding the header information to the data. The transport layer sends the data in small units in order for the network layer to handle the data more efficiently. TCP, UDP, RTP are the protocols used in the Transport layer.

Application Layer – Layer 4

The Application layer consists of the protocols used by the applications. These applications provide user services and data over the network connections recognized by the lower layer protocols. The application layer protocols deal with the client-server applications and other services which have well-known port numbers earmarked by the Internet Assigned Numbers Authority (IANA). HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows, and other application protocols are the protocols used in the application layer.

- **Advantages of TCP/IP model:**
  - It serves as a client-server architecture.
  - It functions independently.
  - It consists of many routing protocols.
  - Initiates a connection between two computers.
- **Disadvantages of TCP/IP model:**
  - Complex to setup.
  - No assurance of packet delivery in the transport layer.
  - Not an easy task to replace protocols.
  - No visible parting between the services, protocols and interfaces.

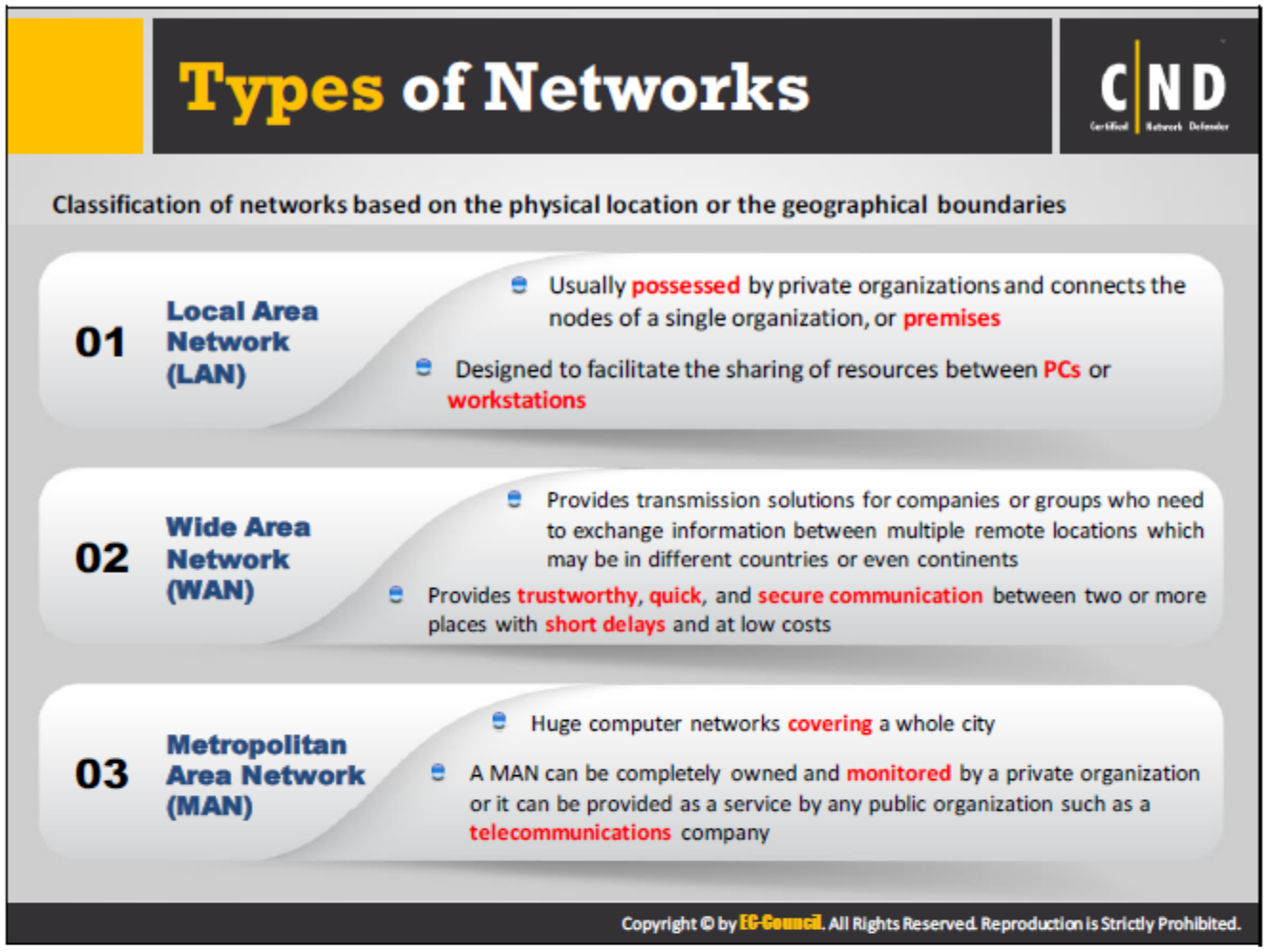


OSI Model

The main aim behind implementing the OSI model is to standardize and ease the communication between the communicating parties using certain standard protocols. It generalizes the communication between the computers in terms of layers. The OSI model has seven layers. In this model, a layer serves the layer above it that brings to a conclusion the working of each layer depends on the layers below it.

TCP/IP Model

TCP/IP remains as the basic protocol for communication. The TCP/IP protocol finds its application either in an intranet or in an extranet. TCP/IP consists of four layers, out of which the upper layers manage the assembling of the packets in the original message and the lower layers manage the address part of each packet and forwards it to the right destination.



These networks may differ in many ways. For example: by size, by functions, by the geographical distance. The services provided by the networks differ according to the layout of the networks.

The networks that differ by size depend on the area occupied by the network and the number of computers present in the network. The computers in a network can vary from one single computer to millions of computers. The different networks are based on the size of the area they cover:

- Local Area Network (LAN)
- Wide Area Network (WAN)
- Metropolitan Area Network (MAN)
- Personal Area Network (PAN)
- Campus Area Network (CAN)
- Global Area Network (GAN)

Local Area Network (LAN)

The LAN consists of computers and its related devices that share information over the same communication line. The LAN may extend only within an office building or home. The LAN can handle hundreds of users. The two commonly used LAN technologies are Ethernet and Wi-Fi. There are virtual LANs that enable the network administrators to provide a network connection to a group of nodes. LAN enables the use of many application programs and the users can

achieve those applications by simply downloading it from the LAN. Wireless LANs are becoming much more popular. This is due to more flexibility and a cost which is less when compared to wired-LANs.

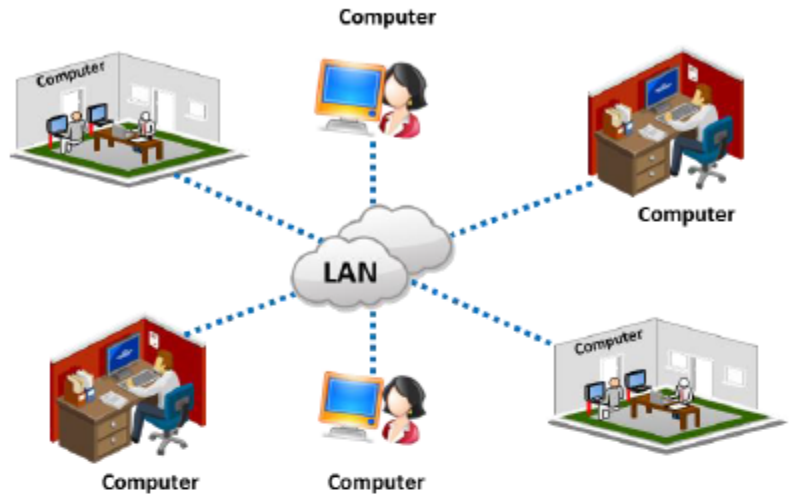


FIGURE 1.2: LAN (Local Area Network)

- **Advantages**:
  - Allows sharing of printers between the computers at home or office.
  - LAN provides the users the privilege to work from any system in the LAN.
  - Allows storage of files in a single folder and sharing it between the users on the network.
- **Disadvantages**:
  - As it provides file sharing facility, it requires separate security measures to restrict access to certain files and folders.
  - Any small issue in the file server can affect all the users on the server machine.

Wide Area Network (WAN)

The WAN is spread over a larger geographical area and is more far-reaching than a LAN. WANs usually connect the nodes in the network using leased telecommunication lines. These lines assist in carrying the information efficiently across the various computers in the network. WANs can connect different LANs in a network. Most often, public networks are connected to the wide-area network. The LANs connect to WANs for quick and secure transfer of data. However, WANs requires a group of authorities to manage.

- **Features of WAN:**
  - WAN networks generally provide larger and dedicated network services. It always tries to meet the services according to business requirements.
  - The WANs has a lower data transfer rate when compared to the transfer rate of LAN.

FIGURE 1.3: WAN (Wide Area Network)

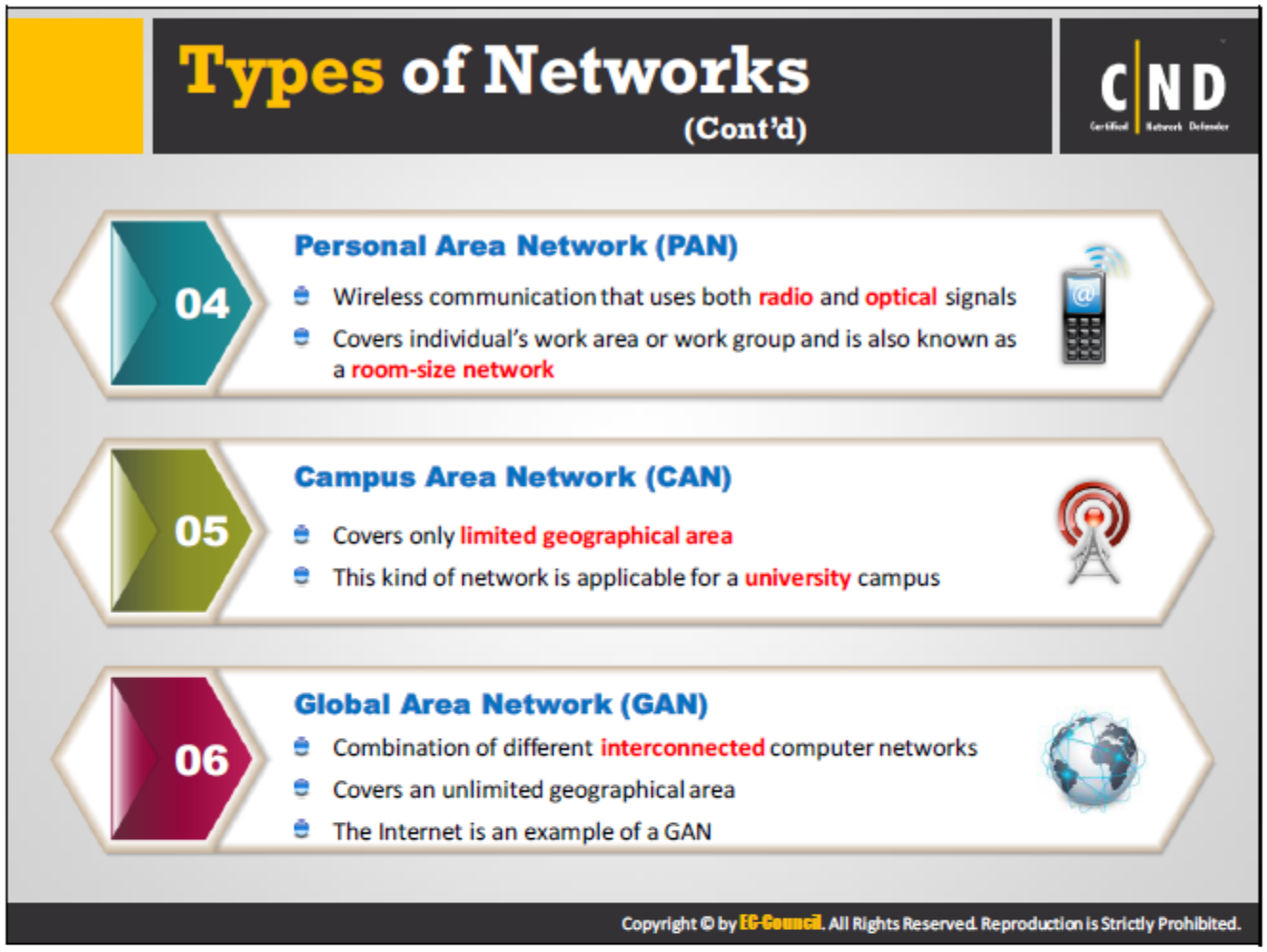
- **Advantages:**
  - A WAN connects places that are geographically apart from each other without a high cost and a difficulty in implementation.
- **Disadvantages:**
  - Very complex in structure.
  - Provides only lower bandwidth and has a higher risk of losing the connections.

Metropolitan Area Network (MAN)

A MAN stretches for an even larger geographical area than a LAN, but less than that of a WAN. It refers to the interconnection of networks spread across a city or town. Several LANs grouped together form MANs. MANs provide secure, efficient communication by making use of fiber optic cables. The MAN provides shared network connections to its users.

FIGURE 1.4: MAN (Metropolitan Area Network)

- **Advantages:**
  - The links connecting the computers in a MAN have a much higher bandwidth allowing for the easy sharing of data.
  - Allows multiple users to share the data at the same speed.
- **Disadvantages:**
  - Requires the need of installation before deploying it for the first time.
  - Costly when compared to LANs.



Personal Area Network (PAN)

A Personal Area Network refers to the interconnection of devices within a certain range of distance. For example, a person can connect a laptop, mobile, tablet etc. to the wireless network within a certain distance without having to physically plug in anything to the devices. This allows for file and information sharing within the devices connected to that network.

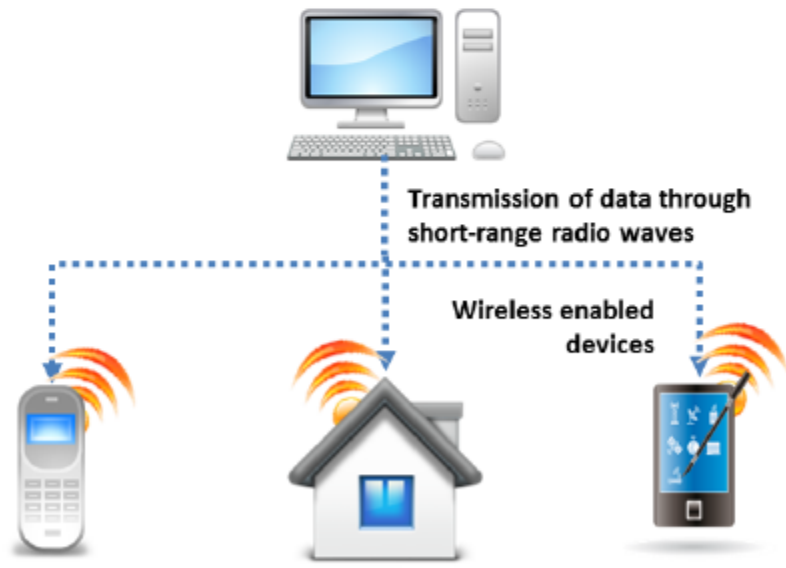


FIGURE 1.5: PAN (Personal Area Network)

Campus Area Network (CAN)

A campus area network consists of multiple connected local area networks within a certain geographical area. Most government organizations and universities make use of the campus area network. The size of the campus area network is much smaller than a MAN or a WAN. It uses optical fiber in order to connect the nodes in a campus network. For example, different buildings in a campus can use campus area network for interconnection and thereby allows the sharing of information within different departments. The implementation of a CAN requires less cost, is highly beneficial and economical due to high speed data transfer from any section of the network.

- **Features:**
  - Cost-effective.
  - Allows interconnection between various departments in a campus.
  - It provides a single shared data transfer rate.
  - Resistant to failure.
  - The campus area network is highly flexible to the changes of an evolving network.
  - CAN offers a highly secure network by implementing authentication of the users accessing the network.

Global Area Network (GAN)

The Global Area Network consists of different interconnected networks extending over an unlimited geographical area. The GAN covers a more geographical area than a LAN and a WAN.

A GAN enables transfer of data from one point to another even when they do not connect directly with each together. The points can connect using a central server or each point can pass the data from one point to another till it reaches the destined point.

The GAN supports mobile communication for a number of wireless LAN's. Broadband GAN is the most commonly used GAN. The BGAN uses portable terminals to connect the computers located at different locations to the internet.

- **Advantages of GAN:**
  - GAN allows the interconnection of multiple networks and it enables proper sharing of data without tampering with it.
  - Enables the storage of files in a central server, thereby allowing easy access of files across different networks.
  - GAN enforces security towards accessing of these files by imposing access restrictions.

Network Topologies

- Network topology is a specification that deals with a network's overall design and flow of data in it

Types of Topology

- **Physical Topology** – Physical layout of nodes, workstations and cables in the network
- **Logical Topology** – The way information flows between different components

Physical Network Topologies

Bus Topology
Network devices are connected to the central cable, called a bus, by the help of interface connectors

Star Topology
Network devices are connected to a central computer called hub which functions as a router to send messages

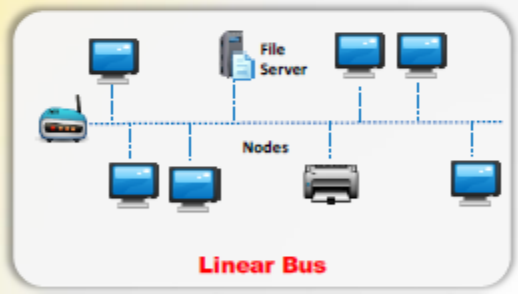
Ring Topology
Network devices are connected in a closed loop. Data travels from node to node, with each node along the way handling every packet

Mesh Topology
Network devices are connected in a way such that every device has a point-to-point link to every other device on the network

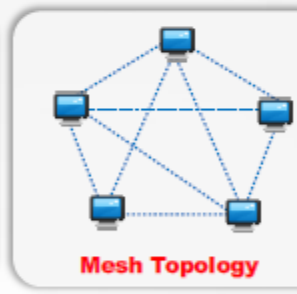
Tree Topology
It is a hybrid of bus and star topologies, in which groups of star-configured networks are connected to a linear bus backbone cable

Hybrid Topology
Combination of any two or more different topologies. Star-Bus or Star-Ring topologies are widely used

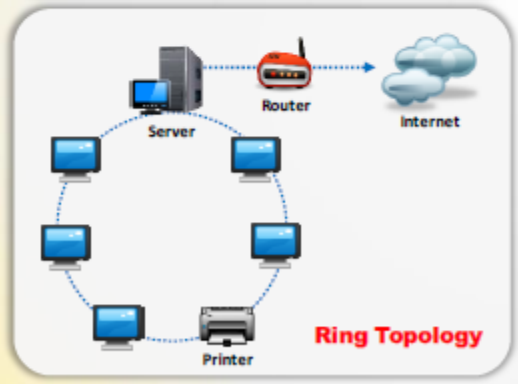
Network Topologies (Cont'd)



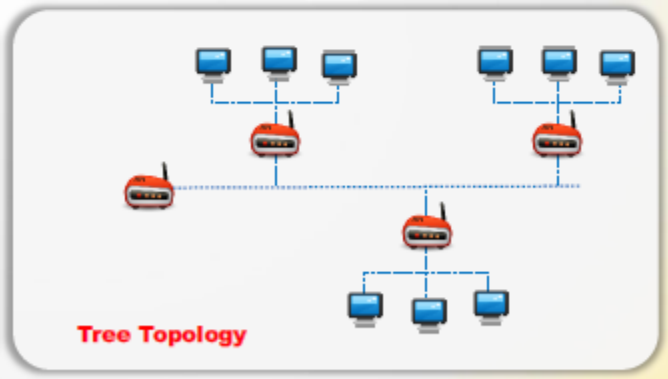
Linear Bus


Mesh Topology


Star Topology



Ring Topology


Tree Topology

The logic of connecting computers over the network is possible using topologies. The topology defines the structure of a network and determines the physical or logical layout of the network. The physical topology defines the structure of the components of the computer systems, whereas the logical topology defines the method of the flow of data in the network between the computers.

Various topologies available are:

Star Topology

Star topology consists of a central node (hub) connected to other computers in the network using a cable. Each node or computer in the network connects individually to the central node. Adding nodes to the star network is an easy task. Any damage to the connection between any node and the central node does not affect the working of the other nodes in the network. But, any damage to the hub can affect the star structure.

Here, the central node or hub acts as the server and the attached computers act as the clients. All data to the respective nodes passes through the central node or hub. The hub acts as the intersection for connecting all nodes present in the star network. The hub can connect to the hubs of other networks and act as a repeater or a signal booster. The computer nodes connect to the hub using unshielded twisted pair Ethernet cable. The following factors determine whether the hub is active or passive:

- The central node or hub performing processes like data amplification, regeneration, etc.
- The central node regulates the movement of the data.
- The network requiring electrical power resources.

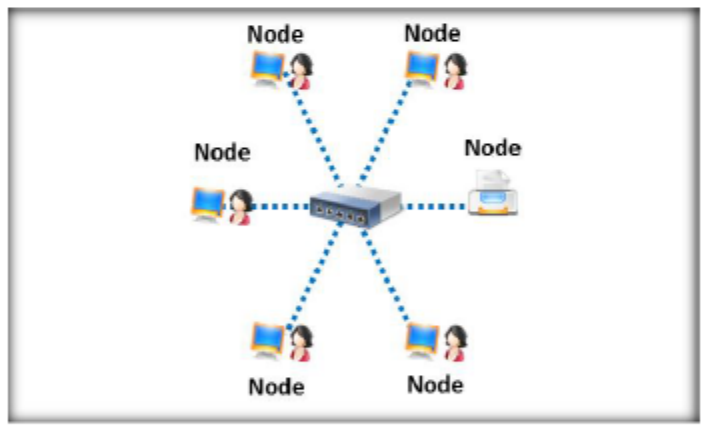


FIGURE 1.6: Star Topology

- **Advantages:**
  - Enables centralized management of the network through the central node or hub.
  - Enables easy addition and removal of other computer nodes to the star network.
  - Failure of one computer node does not make any impact on the rest of the nodes in the network.
  - Enable easy detection of failures and errors in the network. This allows for finding better methods to solve the issue.

- **Disadvantages:**
  - Any failure on the central node affects the whole network.
  - Using routers or switches as the central node increases the cost of implementing the network.
  - The addition of new nodes to the network depends on the capacity of the central node.

Bus Topology

Here, a single cable handles all the computers in the network. The single cable carries all the information intended for all nodes in the network. Any damage to the connection between any node and the main cable can affect the passage of data over the cable.

In the bus topology, the network broadcasts the signal sent by any node. The broadcasting of the signal allows the signal to reach all the nodes attached to the cable. The node having an IP and MAC address the same as given in the signal accepts those, while the other nodes reject those signals. Every cable in the bus network has a terminator attached to the both ends of the cable. The terminator helps in preventing the signals from bouncing. They capture the signals reaching the end of the cable. Signal bouncing can cause the signals to bounce back in the direction from where it came. If two signals bounce back at the same time from opposite directions, this can cause the collision of the signals.

There are two types of bus topologies: Linear and Distributed bus topology. In linear bus topology, there is only a single line attached to the two end points. In a distributed bus topology, it can have more than one linear pattern attached to the network.

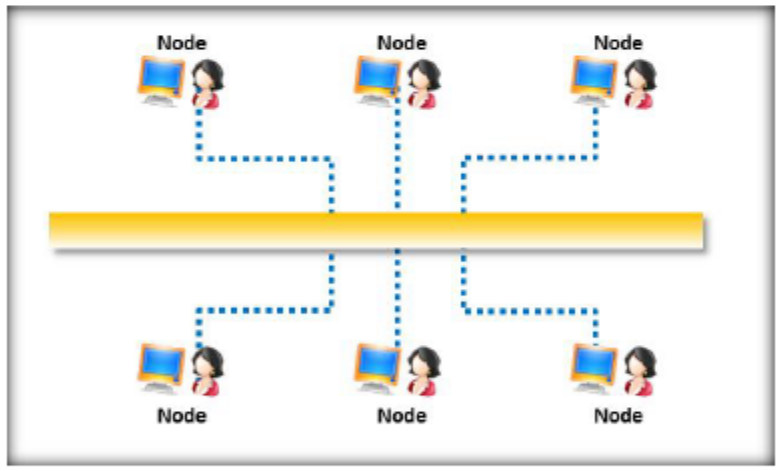


FIGURE 1.7: Bus Topology

- **Advantages:**
  - Easy to add new nodes to the bus network.
  - Low cost for implementation.
  - Works better in small networks.
  - Requires less cabling than a star network.

- **Disadvantages:**
  - Addition of computer nodes depend on the length of the cable.
  - Any issue in the main cable can affect the whole network.
  - Terminators at both ends of the cable is a must.
  - Very high maintenance cost.
  - Not suitable for networks with very high traffic.
  - As all nodes receive the signal sent from the source, it affects the security of the network.

Ring Topology

A Ring topology connects all nodes in the network. The data circulates in the network until the intended recipient accepts the data. Any damage to any of the nodes can affect the whole ring network. The data travels on the network in one direction. The sending and receiving of data takes place with the help of a TOKEN. In the concept of a TOKEN, the data are sent from the source and includes another piece of information and then passes the TOKEN to the next node. Each node checks if the signal is for itself. If yes, it receives the signal and passes the empty TOKEN to the network. Or else, the node passes the TOKEN to the next node. Only those nodes having the TOKEN can send data. Other nodes need to wait until they receive the empty TOKEN. Usually, schools, offices, small buildings make use of RING topology.

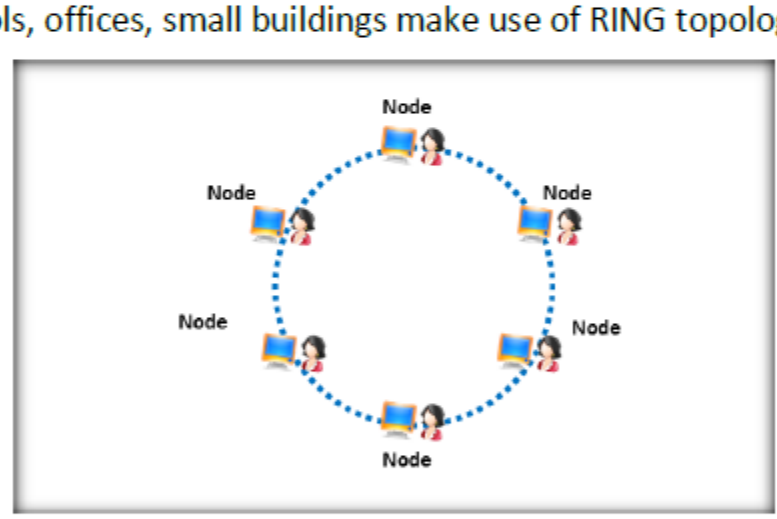


FIGURE 1.8: Ring Topology

- **Advantages:**
  - Unidirectional flow of traffic.
  - Every node can send data after receiving the empty token.
  - No need of any centralized network server in order to manage the computer nodes.
  - Better performance than Bus topology in scenarios where the traffic load increases.
  - Every computer node has the same level of access to the resources.
  - Adding new components to the system does not affect the performance of the whole network.

- **Disadvantages:**
  - Slow process as the signals need to pass through each node in the network.
  - Any issue in any one of the nodes can affect the entire network.
  - Needs a high amount of wired environment for connecting the network nodes, which increase the cost of implementation.
  - Sharing of bandwidth with all the nodes.

Mesh Topology

All the nodes or computers in the network connect with each other. The design confirms the passage of data between every computer even in the failure of any one computer. Each node in the network sends data to other nodes as well as passes the data from other nodes. However, the mesh topology does not find much use in organizations due to its huge cost for implementation and widely used in wireless networks.

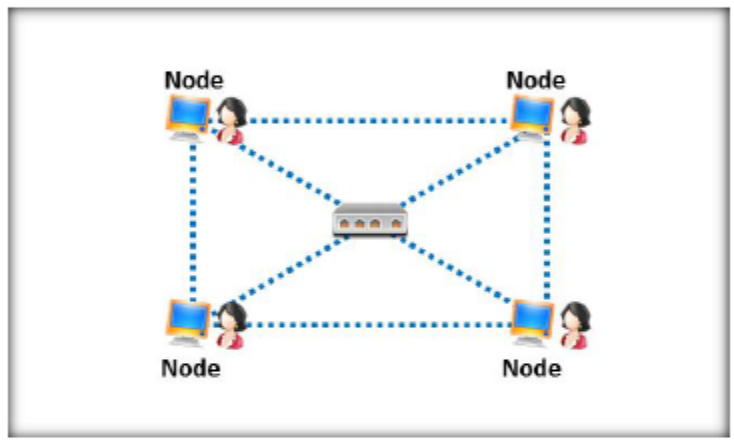


FIGURE 1.9: Mesh Topology

There are two types of Mesh topologies:

- Full Mesh Topology: All the nodes connect with each other in the network. If any node failure occurs, the full-mesh topology can redirect the traffic from that particular node to another node.
- Partial Mesh Topology: Here, only very few nodes connect to all nodes in the network, while other nodes connect only to one or two other nodes. Due to this fashion of connecting to very few nodes, the partial-mesh topology is far less costly and minimizes the redundancy of many connections.

Mesh topology uses either of the two technologies: Routing or flooding. In the routing process, the topology makes the message transmit through a path between the nodes. In order to ensure continuous transmission of data between the nodes, the topology needs to ensure that all connections between the nodes are proper and not broken.

- **Advantages:**
  - Allows continuous transmission of data.
  - Able to handle heavy load traffic.

- A node failure does not impact the whole network.
- Allows expansion and modification of networks without disturbing the network.

- **Disadvantages:**
  - High level of redundancy due to the presence of many connections.
  - Expensive compared to other network topologies.
  - Consumes more time for set-up and needs more administrative attention.

Tree Topology

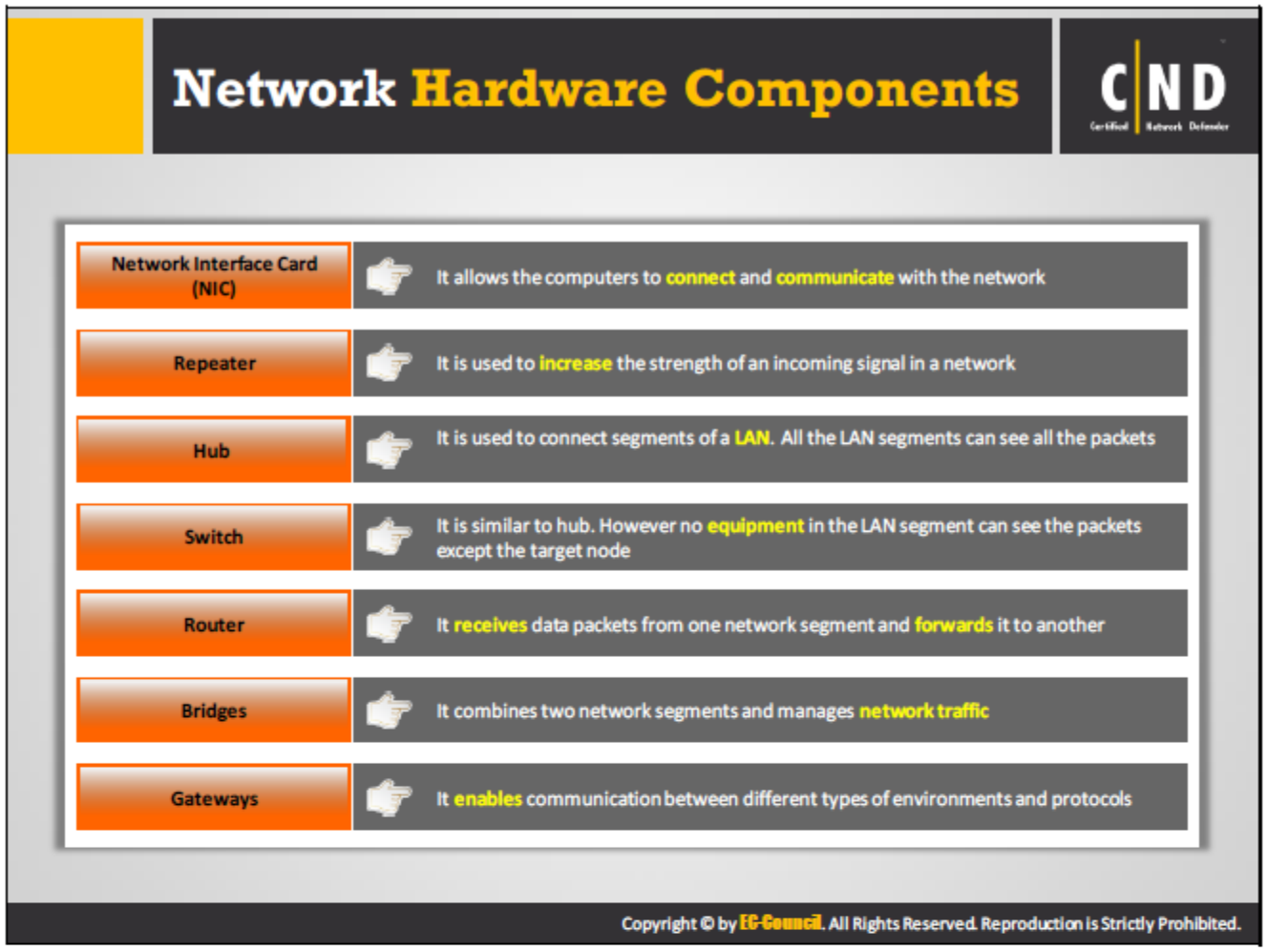
The tree topology consists of a combination of a bus topology and a star topology. Similarly, the tree topology consists of a main cable line attached to a star network. In the tree topology, many star topologies connect to the central transmission cable. Another name of the model is "extended star topology".

- **Advantages:**
  - Tree topology finds its usage in scenarios where it is difficult to implement the star and bus topology.
  - Allows easy expansion of the network.
  - Design of the star topology in the layout enables an easy management of the nodes.
  - Provides error detection and correction properties.
  - Each star network connects to the main cable through wiring.
  - Failure of one of the star networks does not affect the working of the other networks.
- **Disadvantages:**
  - Any damage to the main transmission cable can damage the whole topology or network.
  - Even though the tree topology enables easy expansion of the network, it becomes difficult for the network as a whole to manage the entire nodes and segments.
  - The rate of expansion depends solely on the type of main cable used.

Hybrid Topology

The hybrid topology combines the characteristics of two topologies together. These are mainly used in Wide area networks. The organization implements a hybrid topology according to the requirements of the organization. For example, if one section of an organization needs bus topology while another section needs ring topology, the organization can implement both these topologies using a hybrid topology. They combine multiple topologies into a single large topology.

- **Advantages:**
  - Provides error detection and correction without affecting the working of the other section of the network.
  - Allows easy addition of the nodes.
  - Allows the organization to design the network according to their needs.
  - Provides a combination of the features of multiple topologies.
- **Disadvantages:**
  - As it consists of multiple topologies, the organization needs to design it in an effective manner and needs to ensure that the designed architecture can provide the required throughput.
  - The implementation of a hybrid topology is a costly affair, as it includes more cabling and connections.



Network Interface Card (NIC)

Connecting to a network is an integral part of computing. The computers use a network interface card for connecting to the network. They connect to wired as well as wireless networks using certain electronic circuitry. Different names of NIC are Network interface controller, Network adapter, Local area network adapter, etc. They provide the computers with a dedicated full-time connection with the network. The computers on the LAN network contain a NIC that enables LAN transmission.

The role of a NIC in a wired connection is as follows:

- Transmission of data from one computer to another.
- Gathering the data to transmit through the network cable.
- Handle the data transmission from the computer through the data cable.
- Accept the data from the cable, convert it into bytes for processing by the CPU.

NICs are commonly used in Ethernet connections and the available configurations are: 10, 100, and 1000 Base-T. The recent computers are configured along with the Ethernet capabilities in the motherboard chipset. An Ethernet chip connected using a PCI or PCI express bus directly on the motherboard is another method for connecting. Thus, it minimizes the need of a separate NIC. In some situations, a NIC is integrated as components in a router, USB device, etc.

- **Advantages:**
  - A network interface card does not have to be fixed with a physical cable.
  - The NIC is used to send the data as well as receive the data.

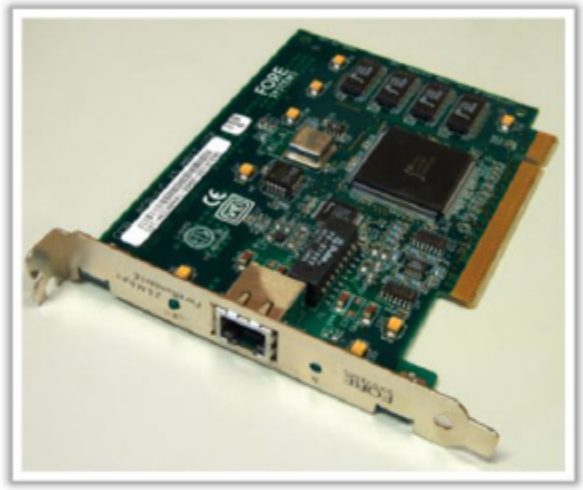


FIGURE 1.10: NIC card for wired network

FIGURE 1.11: Wireless PC Card Network Adapter

Repeater

Repeaters are network devices that are generally used for the restoration or the repetition of a signal. Repeaters can restore analog and digital signals misled due to transmission loss. Repeaters can only amplify the analog signals, whereas with a digital signal a repeater can restore the signal to its original quality. Repeaters can also pass the data between various subnetworks carrying different protocols.

There are different types of repeaters:

- **Telephone Repeater**: Help in increasing the telephone signal range in the telephone lines. The repeater locates its applications in the trunk lines carrying long distance calls. The telephone signal lines made of a pair of wires, consists of an amplifier circuit that use power from direct current (DC) to increase the power of the alternating current (AC) audio signal on the line.

- **Optical Communications Repeater**: These mainly increases the signal strength of the fiber optic cable. These cables carry digital information in the form of short pulses of light. The light is made up of particles called photons.
- **Radio Repeater**: Increase the signal strength of the radio signals. The radio repeater amplifies and retransmits the radio signals using the radio receiver connected to a radio transmitter.

A normal LAN implementation usually limits the physical size of the single cable segment according to the physical medium and the techniques used for transmission. The repeaters play an important role in constructing a network that exceeds the size of the single, physical, cable segment. The LAN implementation determines the number of repeaters that can be used. The repeaters used between two or more cables require the need of the same physical layer protocol in order to send the signals over all the cable segments.

- **Advantages of Repeaters:**
  - Very simple to use.
  - Less cost for implementation.
  - It strengthens the signals.
- **Disadvantages of Repeaters:**
  - Repeaters are the devices that augment the traffic on the network and sometimes transmit errors. There is a limit on the number of repeaters used across a network.
  - Users cannot monitor or inspect the repeaters through an inaccessible area and these devices do not have the facility to separate or filter the traffic.
  - The different segments of repeaters must be inspected thoroughly and periodically, if this is not done it can cause the repeaters operating on different segments and different media to become compromised.
  - Repeaters can augment the traffic on the network and have a restriction of the quantity deployed across a network.
  - Repeaters can transmit errors in the network.

Hub

A hub is a network device used to connect multiple network devices or segments of a LAN. The main activity of the hub is to forward the data arriving from one device to another device or port. The hub requires fiber optic Ethernet cables in order to connect various devices. Some hubs even work as a repeater that helps in amplifying the signals. The hub remains a common point of connection for many devices in the network. It can contain multiple numbers of ports. Upon the arrival of a packet at any port, other ports maintain a copy of the packet, thus enabling all LAN segments to view packets. A hub provides a sequence of ports to connect the network cables. The smallest hub can connect four computers to a network and with an extra

port to uplink to other hubs in the network. Hubs vary according to their size and have ports up to 12, 16, and 24 in number.

- **Types of hubs include:**
  - **Passive Hubs:** Passive hubs do not intensify the signal strength of the data prior to transferring the data packets, but act as a means to transfer data between the devices in the network.
  - **Active Hubs:** Active hubs strengthen the signal prior to transferring it to other devices in the network like the repeater. It has multiple ports and is called as multiport repeater.
  - **Intelligent Hubs:** Intelligent hubs are business critical hubs providing additional features. It behaves like a stack with units added to the top to minimize space.
  - **Switching Hubs:** Switching hubs view the destination address of every data packet before transferring them to the specified destination port.
  - **Repeater Hubs:** Repeater hubs relay the inbound traffic. However, active (or switching) hubs transmit the data that is addressed for that specific host, i.e. sniffer software is proved to be safe. Performance is also improved. Certain hubs offer security at the MAC level (such that it connects only the identified MAC addresses to specified ports). The present day hubs can also build VLANs (virtual LANs) that assemble specific ports into a virtual network, which is not transparent to other ports.
- **Advantages:**
  - It is a flexible, simple, and an economical device.
  - Expands the length between nodes.
  - Every port can make maximum use of the bandwidth without the use of CSMA/CD.
  - Adding hubs increases the number of ports.
  - Hubs organized by SNMP provide tools and statistics for better management.
  - Makes use of the available cables along with other network elements.
  - Hubs help to route the network traffic and prevent the crashing of networks. It can also combine the relatively slow Ethernet devices with those of higher speeds. This facilitates the addition of a variety of devices variant in speed.
- **Disadvantages:**
  - Hubs cannot help to control the traffic.
  - Data transfer rates decrease substantially with the increase in devices connected.
  - Attacker can compromise the unchecked hubs.
  - Computers connected to isolate hubs are isolated from the network.

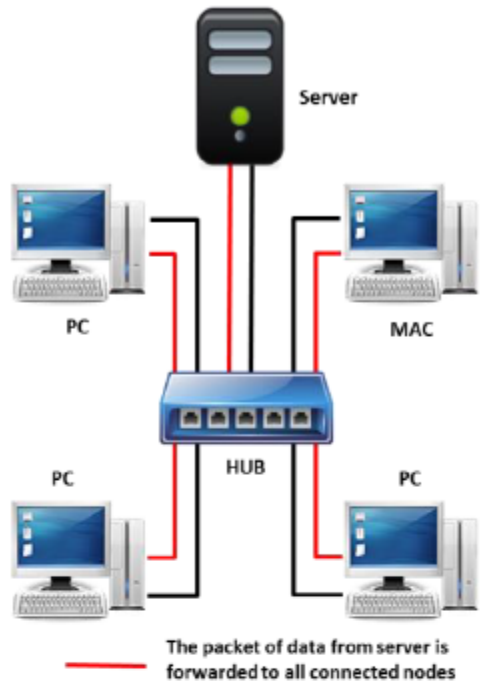


FIGURE 1.12: Hub

Switches

A networking switch is the fundamental device in a wired or wireless LAN. It receives signals from each terminal on the network through Ethernet cables in a wired network and through antenna emitting radio waves in a wireless LAN. In both the cases, the networking switch sends traffic across the LAN, permitting the computers to communicate with each other and share resources. All computers residing in the LAN should contain a NIC. This card allocates a distinctive MAC address to the machine in which it is setup. A wired NIC incorporates an Ethernet cable, which extends to a port on the back of the networking switch. If the NIC is wireless, the card will attribute a small antenna as a replacement for an Ethernet port. The antenna sends signals to the wireless networking switch, which also hosts an antenna rather than ports. Whether wireless or wired, the networking switch acts as a relay, analyzing traffic packets as they arrive from the various machines and sending the packets to the destination MAC address.

A transmission mode is the term used to define the direction of a signal or flow of information between two interconnected devices. Simplex mode, half-duplex mode and full-duplex mode are types of transmission modes. Information flows only in one direction in simplex mode, i.e., from sender to receiver. In half-duplex mode, data flow to and from but only in one direction at a time. Both stations can send and receive the data, but not at same time. The full-duplex mode transmits data in both directions at the same time.

- **Switch Functions:**

  A networking switch functioning in full-duplex mode implies a machine on the LAN that can receive and send data simultaneously. This is quicker than a networking hub, an alternating device that serves the same function as a switch, but functions in half-duplex mode, allowing each machine to send or receive at any given time. Another discrete difference between a networking switch and hub is that the switch sends traffic packets

only to destination addresses. On the other hand, a networking hub sends all traffic on the network to all nodes. The filters within each machine make the decision regarding rejection or acceptance of the packets. This practice makes the network vulnerable to eavesdropping. Network switches are low-priced devices, but price may vary based on a number of ports. For those who are using a cable modem or a DSL service, a broadband router with a switch inbuilt along with a firewall can replace the stand-alone networking switch.

- **Advantages:**
  - Networking switch has more advanced features than a networking hub.
  - Anti-sniffing software switches network to identify packet sniffers.
- **Disadvantages:**
  - Networking switch is not infallible, as an attacker can mislead it into employing packet sniffers.

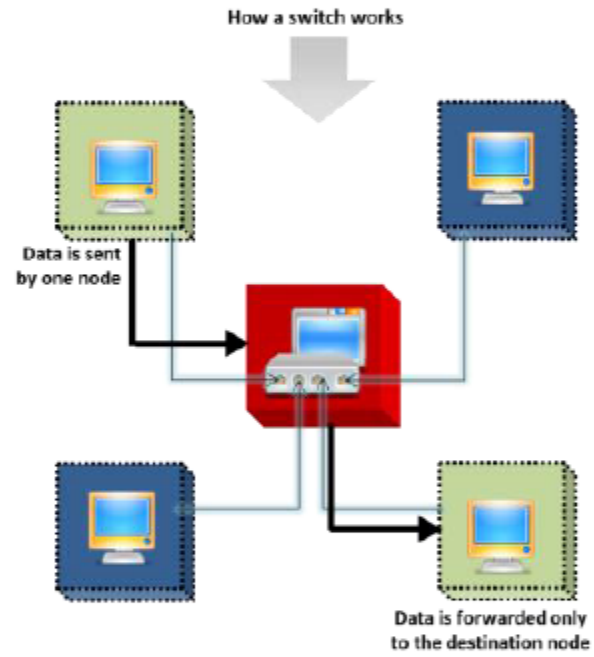


FIGURE 1.13: Working of switches

Routers

Routers are more complicated devices than the other devices like repeaters and bridges. Routers can access the addresses of the network layer and have embedded software that helps them in identifying the exact destination address. It looks from the multiple paths available between the addresses and checks the channel that is appropriate for the transmission of data.

- **Router Functions:**

  Router function in the physical, data link, and the network layers of the OSI model. Routers transmit packets among several interconnected networks. They send packets from a network to the other important destinations in a network. A packet sent from one destination to the other travels through the router initially and then moves to the other destination in a network. The destination router in turn transmits the packet until it

reaches the final destination. Routers behave as stations on the network, although irrespective of stations to which they belong, routers contain addresses and connect to more than two networks simultaneously.

When a router receives a packet in an interconnected network, it reads the address and sends the packet to the destination address. However, if it does not find the corresponding address in the network, it has the capability of forwarding the packet to the next connected network based on the best options available. After identifying the appropriate route for the packet to transmit, the router transmits the packet along the accurate network to other networks. If it finds as inappropriate, it sends the packets to the surrounding network or the adjacent router to select the next best path.

A router maintains a routing table to maintain the paths through which the routing occurs and also minimizes excess costs for routing across the network. Static routing is a type of routing where the network administrator monitors the entire routing processes. Routing includes many concepts such as least-cost routing, which shows the economic paths allotted for routing, i.e., selects the available shortest path. Shortest in terms of routing also implies a path that is secure and fast. Some routers also route packets across the network, which use more than one protocol.

Routers can associate with different networks such as LAN and WAN to broadcast the data. They are the devices that prevent the collisions of data during a broadcast. Sometimes, routers also act like other devices such as bridges, which can broadcast packets for a single protocol or a group of protocols. When a router receives packets from a multi-protocol router, it checks the packets (if packet matching with the protocols are configured) and then sends the packets depending on the addresses of the network layer. Routing includes concepts such as least-cost routing, which shows the paths allocated for routing and sends data in the shortest path available.

- **Advantages:**
  - Routers operate at the protocol level.
  - Remote management and design via SNMP.
  - Support intricate networks.
  - More filtering, lesser performance.
  - Provides security.
  - Cannot separate the broadcast collisions.
  - Regularly provide bridge functions.
  - Complicated routing protocols used such as RIP, IGRP, and OSPF.
- **Disadvantages:**
  - The security issues that routers face are that routers do not have security controls that are very efficient, which leads to compromising of the system.
  - Routers cause long delays in initializing the sessions for protocols such as FTP.

- **Check the following aspects before starting the transmission through routers:**
  - Mapping between the ports.
  - Internal addresses.
  - External addresses.
  - The port numbers of the internal and external addresses.
  - Routers are expensive compared to other devices.
  - Routers need only protocols designed for routing.
  - Routers are slower than other devices.
  - Routers lead to overhead, as they are not capable of separating the sent packets.

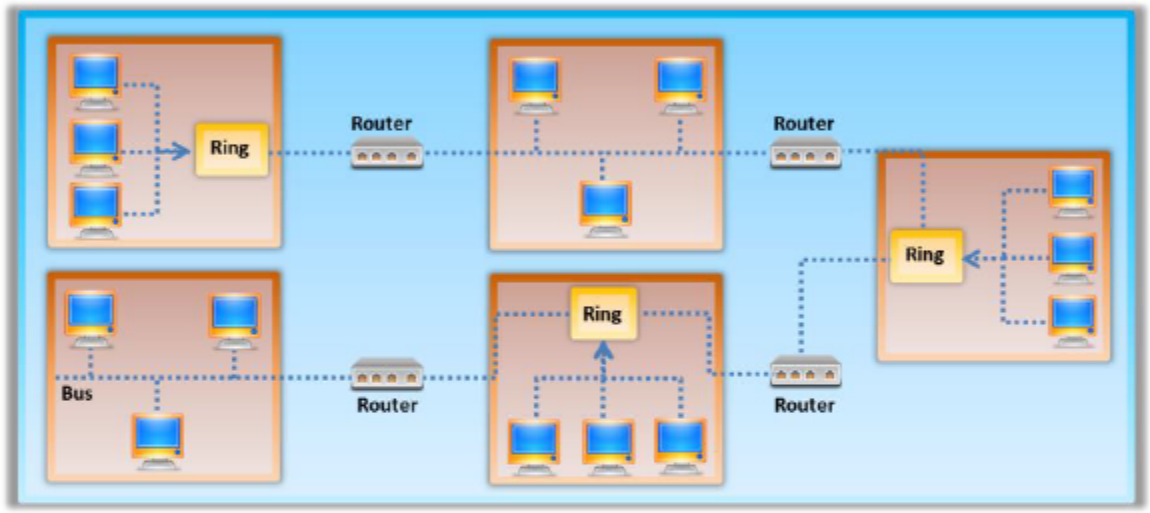


FIGURE 1.14: Working of routers

Bridges

A bridge filters the traffic at the network boundaries. Bridges read the MAC address of each frame (data packets) and forwards data to the addressed destination device. Bridges are logical devices that can maintain each segment's traffic separately. By segmenting the traffic, bridges prevent network congestion and segregation problems in the network traffic. Bridges operate in the data link layer of the OSI model. It maintains a database of MAC addresses located in a segment and permits only specific data frames addressed to that location while blocking unauthorized frames from entering a segment. When a data frame reaches a bridge for transmission, the bridge generates the signals and also finds the address of the destination, and then sends the duplicate to only the appropriate network segment.

Bridges contain a table called a 'look up' table that hosts various physical addresses of all the workstations linked to it. The table is an indicator as to which segments each workstation belongs. When a bridge comes across a packet of data, it checks the address and finds the matching corresponding addresses present in the table. After tallying, it traces out as to which network segment the packet belongs to and sends the packet to the appropriate segment. Bridges use the MAC address to make decisions on relaying network packets. They also act as filters determining if they have to relay the packets to a segment or not.

- **Transparent Bridging:**

  Bridges build a routing table to find whether a packet's destination address is matched with the routing table. If the address does not match, then the packet moves to all the devices in the network except the source to identify the correct destination for the packet. A system with a transparent bridge must satisfy three criteria:

  - Each station should forward the frame from one station to another.
  - Frames help the movements of the forwarding.
  - Avoid the loops.

- **Loop Problem:**

  Transparent bridges work efficiently if the redundant bridges do not exist in the network. If there are two LANs and are connected via two bridges, then a potential loop exists in the network.

- **Source Bridging:**

  The packets will have path information inserted into them in order to know the route.

  Like switches, bridges are also efficient in learning the MAC address of all the connected clients, peripherals, and the servers. Traditional bridges provide connectivity from a single workgroup to another workgroup. The multiport bridges connect two network segments with each other. Bridges inspect the information from the data link layer with a network signal. Bridges are fitted with network filters, which help them to read the source address, packet size, or type of protocol. These devices are simple to install on the network and are efficient to regulate the traffic.

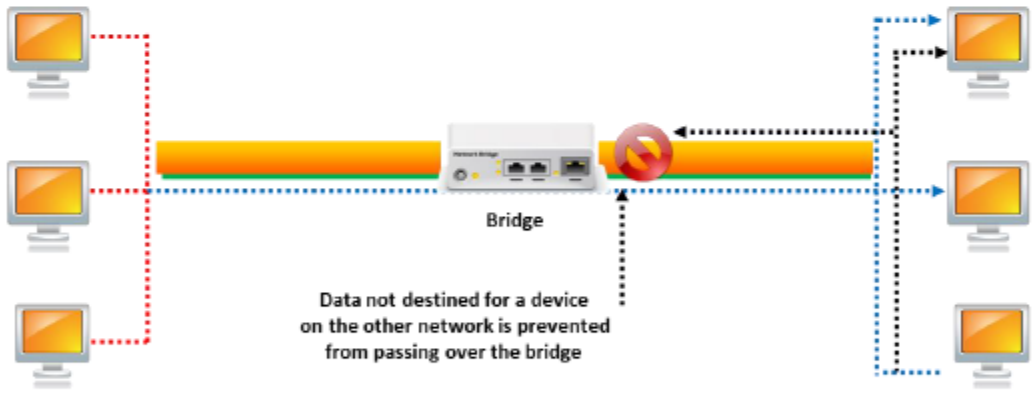


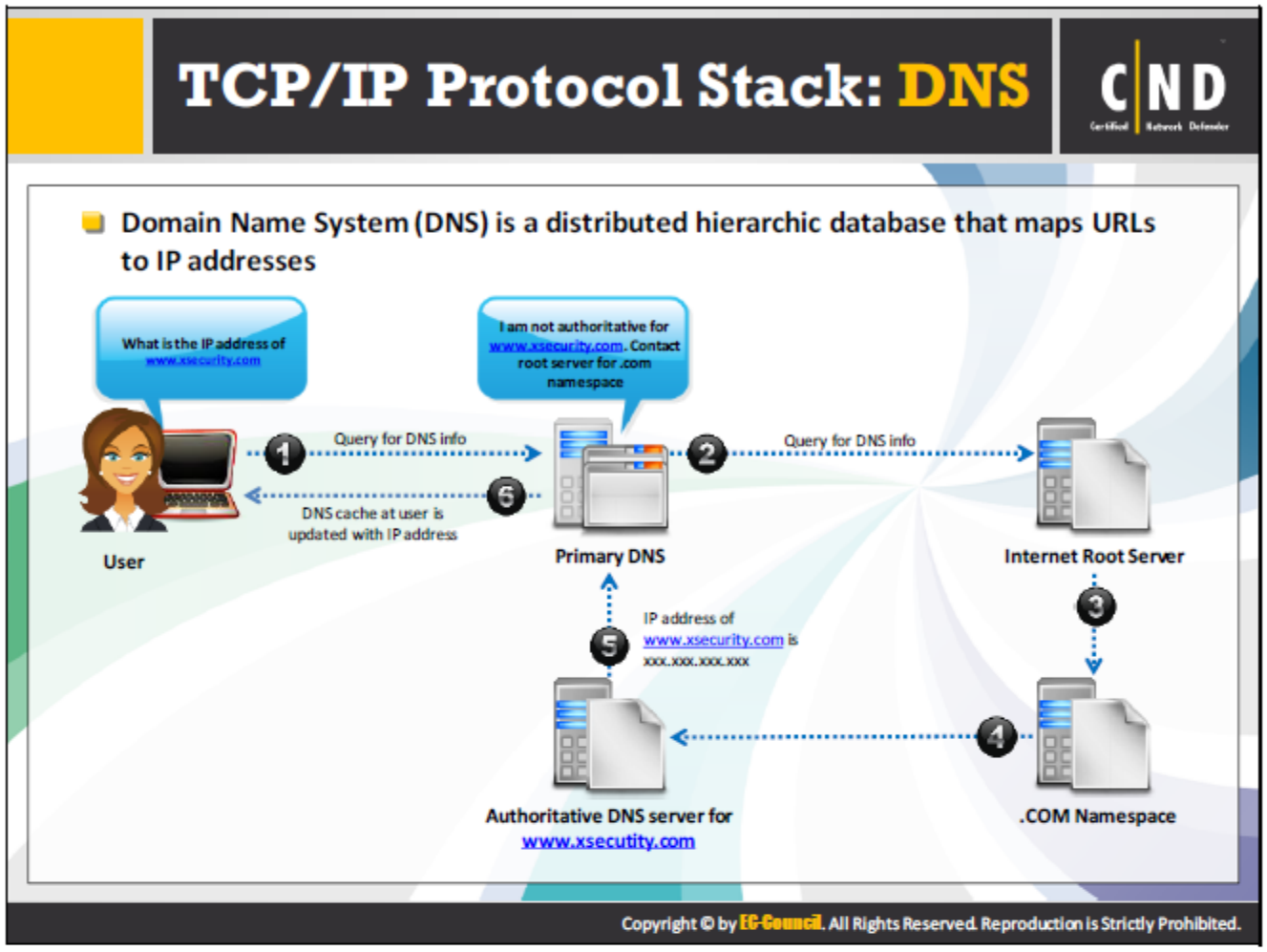
FIGURE 1.15: Bridges

Gateways

Gateways act as an entry point for other networks that try to connect to an internal network. In the same way, they act as an exit point for an internal network that tries to make a connection to external networks. A gateway can be a workstation or server that makes a two-way communication between networks and expands its area. Application and transport layers of the OSI model support gateways. They are capable of connecting devices that have different protocols and environments. They convert protocols that are different by assigning matching protocols to the packets and are called a protocol translator. If the gateways have to connect or

communicate between two different network architectures then they restructure and convert the data from one environment to the other environment. Gateways are task specific. They cannot filter data and sometimes they can transmit malicious packets without filtering. There are two types of gateways:

- **Transport Gateways:**
  - They are capable of connecting different devices with the connection oriented transport protocol.
  - They can transfer packets from one connection to the other by restructuring/reformatting.
- **Application Gateways:**
  - They are intelligent components that can understand the format/contents of the data and then permits transmission.
  - Email gateways translate messages and transfer them to mobile devices.
  - They act as a firewall or proxy server to restrict unauthorized traffic.



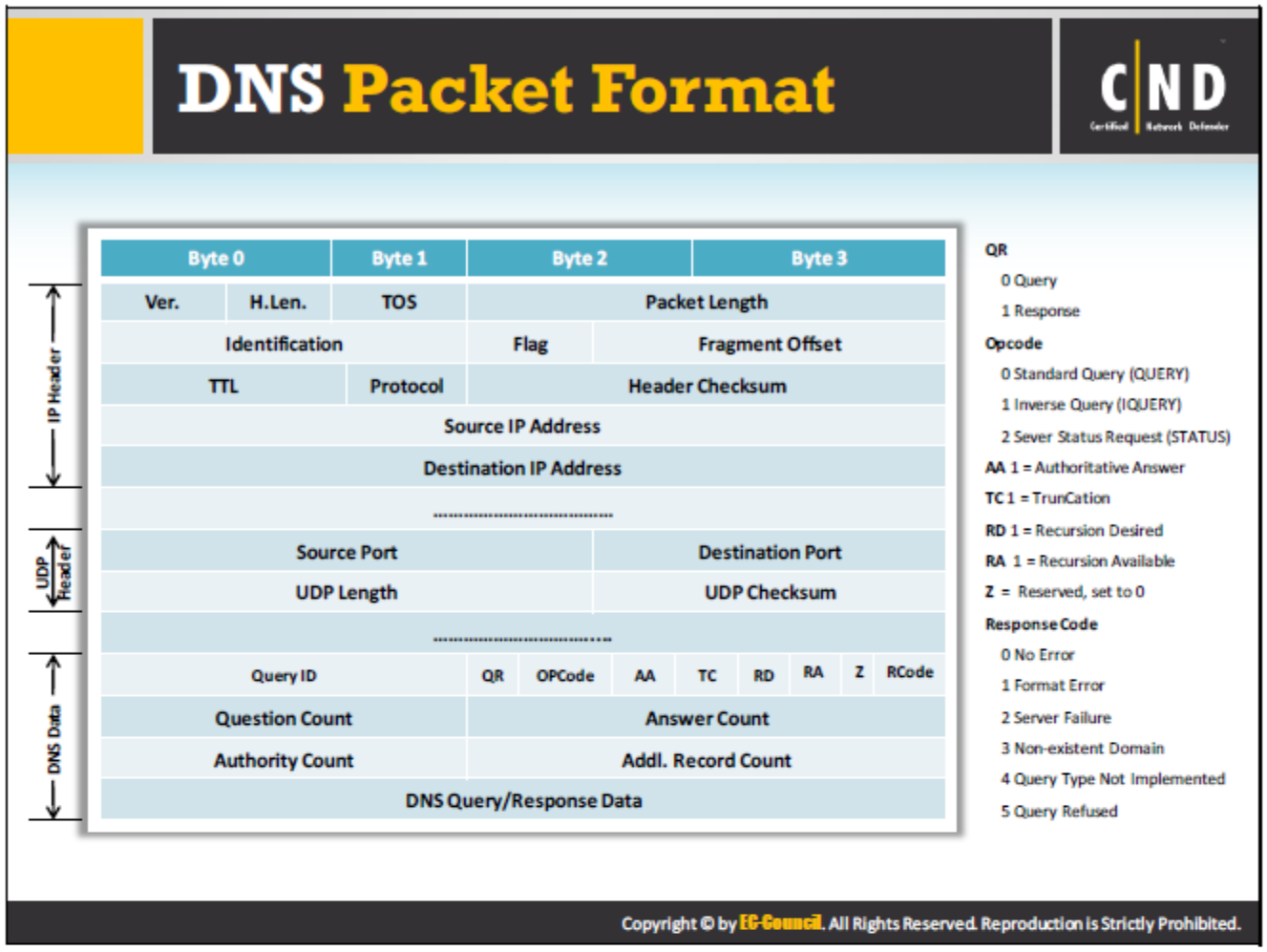
The domain name system (DNS) converts the host names and internet domains to IP addresses and vice-versa. The domain naming system finds its application in TCP/IP network. The DNS services convert the DNS name entered by the user to its corresponding IP addresses. For example, the DNS service converts the domain name ***www.Example.com*** to the IP address: 192.105.232.4

How DNS works:

The DNS works in a client-server model. The client accepts and receives responses from the DNS server. There are two types of requests:

- **Forward DNS lookup**: These are requests containing names and resulting in an IP address.
- **Reverse DNS lookup**: These are requests containing IP addresses and resulting in names.

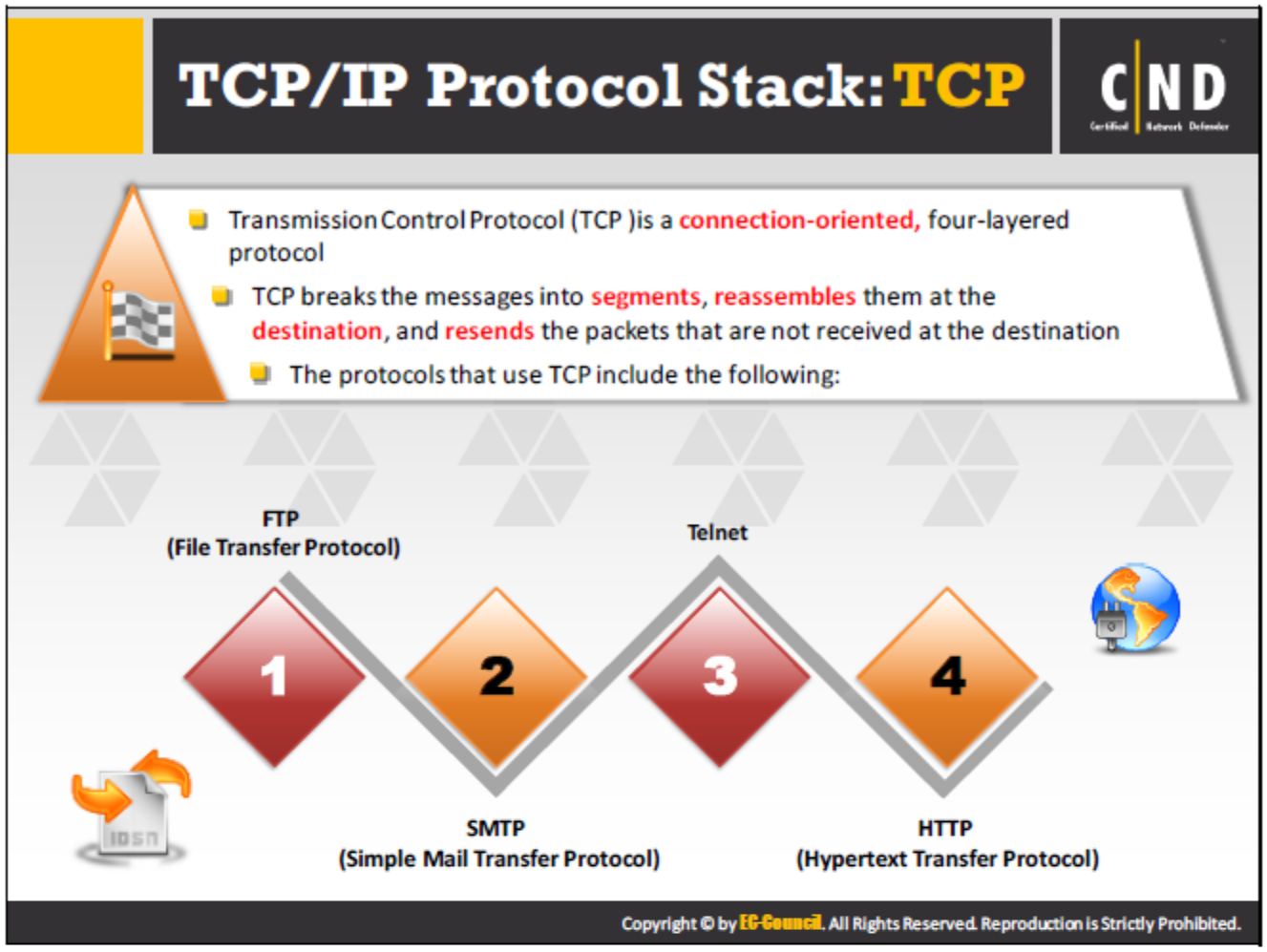
The DNS consists of a database present in various computers. The databases consist of names and IP addresses of the hosts and domains. The clients in these scenarios are web browsers. When the web browsers send in requests such as an internet host name, DNS resolver determines the servers IP address using the DNS server. The DNS resolver actually forwards the request to several other DNS servers if it does not achieve the desired mapping from the requested DNS server.



DNS packet header format consists of three sections namely IP header, UDP header and DNS data. Each section has different fields and different uses as described below:

- **IP Version (4 bits):** There are two types of IP packet and addressing IPv4 and IPv6. This bit specifies the current IP protocol version. Always set the value as 4.
- **Header Length (4 bits):** Length of the IP header where header represents 32-bit words along with IP options if any. The minimum value of the IP header is 5.
- **Type of Service (TOS) (8 bits):** Provides quality of service features. First three bits are for IP precedence, 4 bits for TOS and last one-bit left alone (not used).
- **Total Length (16 bits):** Specifies the length of the IP datagram in bytes. It includes the length of the header and the data.
- **Identification (16 bits):** Identifies the fragments of one datagram from those of another.
- **Fragment Offset (13 bits):** Used to reassemble the fragmented IP datagrams.
- **Time-To-Live (TTL):** It defines the lifetime of the IP datagram in the internet system. The TTL field is initially set to a number and decremented by every router. When the TTL reaches zero, it discards the datagram (Packet).
- **Protocol (8 bits):** Identifies the next encapsulated protocol that sits above the IP layer.
- **Header Checksum (16 bits):** Identifies the errors during IP datagram transmission and calculated based on the IP header.

- **Source / Destination IP address:** IP addresses of the sender and the receiver.
- **Source / Destination port numbers:** DNS servers listen on port 53. The first packet of any exchange always includes 53 as the UDP destination port. The source port is the random port that varies considerably.
- **Query ID:** Unique identifier also termed as transaction ID, created in the query packet that is left intact by the server sending the reply. It helps in matching the answers with the awaiting questions.
- **QR (Query / Response):** Set to "0" for a query by a client, "1" for a response from a server.
- **Opcode:** Set by client to "0" for a standard query.
- **AA (Authoritative Answer):** Set to "1" in a server response if this answer is Authoritative, if not "0".
- **TC (Truncated):** Set to "1" in a server response if the answer cannot fit in the 512-byte limit of a UDP packet response. Indicates the message was truncated.
- **RD (Recursion Desired):** Set in a query and indicates the query should be pursued recursively. This is set to 1 if it wishes the server to perform the entire lookup of the name recursively, or 0 if it just wants the best information the server has.
- **RA (Recursion Available):** A bit that is set (1) or cleared (0) in a response indicating that recursion is available.
- **Z (Reserved):** This is reserved and must be zero.
- **Rcode:** Response code from the server, indicates success or failure.
- **Question record count:** Indicates the number of DNS queries in the questions section.
- **Answer count:** Set by the server, these provide various kinds of answers to the query from the client.
- **Authority count:** Indicates the number of name server records in the authority record section.
- **Additional record count:** Indicates the number of resource records in the additional records section.
- **DNS Question/Answer data:** Holds the question/answer data referenced by the count fields above.



The transmission control protocol or TCP is a connection-oriented protocol that helps in configuring a network connection for various applications to carry data over the internet. The TCP enables a computer to send data to another computer present on the same network or in another network. The TCP ensures that the receiving devices receive all packets sent from the sender. If TCP finds that, the receiver has not received all the packets, then, it insists the sender resend the packets to the receiver. Two devices can disconnect the TCP connection between them after the receiver receives all the data sent from the sender. The TCP does not support the broadcasting of messages. It allows communication only between two devices. TCP and IP are two protocols that rule the internet overall. The TCP is also responsible for breaking the application data into packets and how these packets are accepted and sent through the network. The TCP is wholly responsible for managing the flow control of the data packets in the network. It maintains error-free data transmission and enables the retransmission of data during the instances of data loss. Applications like WWW, e-mail, remote administration and file transfer depend on transmission control protocol. For example, a web server uses the HTTP protocol to send an HTML file to a client. Here, it is the TCP that assists the HTTP to issue the connection and send the file. The TCP breaks the file or data into packets and numbers them. Then it sends them to the IP layer for delivery. The packets are sent through multiple routes and reach the destination IP address. The TCP at the client computer investigates for the arrival of all packets according to the sequence of the numbers represented in the packet. The TCP initiates a retransmission of the packets if any difference is found in the number of packets received.

Functions of TCP

- TCP acts as an interface between the application and the internet protocol.
- It provides a host-to-host connection to the transport layer in the internet model.
- TCP manages all handshaking and transmission details.
- TCP identifies the cases of packet loss and duplication due to network congestion, traffic load balancing and other irregular activities in the network.

TCP always uses an acknowledgement for every packet sent and received. In this technique, the receiver needs to respond using an acknowledgment to the data it receives. The sender maintains a record of the packets it sends and keeps a timer in order to manage the packet transmission. The timer helps in cases where the packets are lost. The acknowledgement technique actually confirms the arrival of each packet of data in the correct order.

TCP Services

TCP is a connection oriented protocol that enables flow control and consistent data delivery services. Consistent data delivery services are mandatory for applications such as file transfers, database services and other services. TCP depends on IP for consistent delivery of packets.

The application layer is responsible for handling the TCP connection between the two hosts over the network. TCP provides the following services to the application layer:

- **Full-Duplex transmission**: Full-duplex enables transmission of data in both directions over a signal carrier at the same time. For example, a telephone is full-duplex as it allows both parties involved in the call to talk at the same time. Most modems provide the users the option to choose between full-duplex and half-duplex. The selection of the option depends on the application the user is running.
- **Half-Duplex transmission**: Half-duplex transmission allows transmission of data transmission in both directions, but only in one direction at a time. For example, a walkie-talkie, wherein only one user can transmit data at a time.
- **Simplex transmission**: Only one user can transmit data at a time and only in one direction. Both parties involved in the transmission need to use the same frequency. For example, in TV and radio, the signals transmit only in one direction (from transmitter site to several receivers.)

Most of the TCP connections are duplex which means that it allows the data to flow in both directions. Simplex mode, full-duplex mode and half-duplex modes are different types of transmission modes that determine the flow of information between two communicating devices.

TCP Operation

The overall operation of the TCP describes the method of how the Transport Control Protocol manages the connections between two communicating parties. The TCP provides functions such as data handling, flow control and reliability in data transmission. These functions are

possible only in the presence of a proper and consistent connection. The criteria to identify the two communicating parties are as follows:

- Sender's IP address
- Sender's protocol port number
- Receiver's IP address
- Receiver's protocol port number

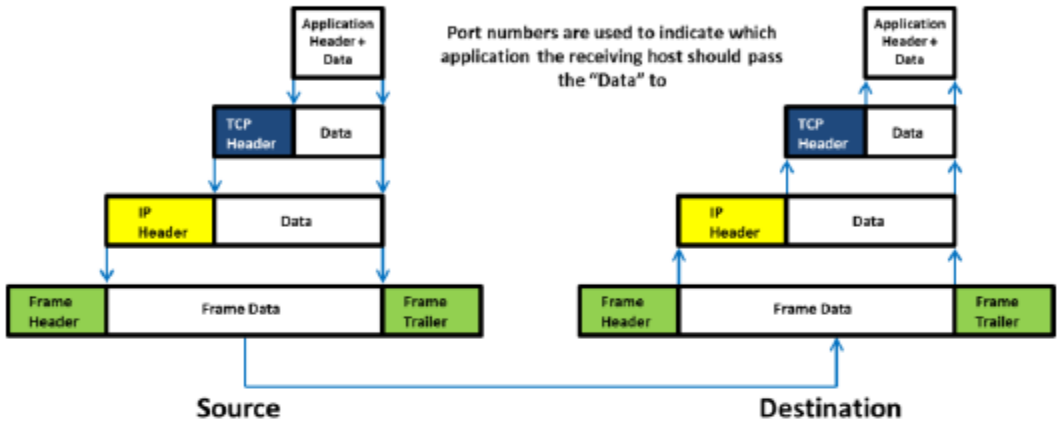


FIGURE 1.16: TCP Operation

A consistent TCP connection can be established using sliding window, sequencing numbers and acknowledgements and synchronization.

- **Sliding Window:** The TCP segment has a flag Window size that represents the size of the data that it can receive. Window size zero means that it cannot accept any data from the sender. The window size consisting of non-zero value means that it is ready to accept data from the sender. The sender needs to maintain a window size that represents the unacknowledged data and the size of the data it can send to the receiver.

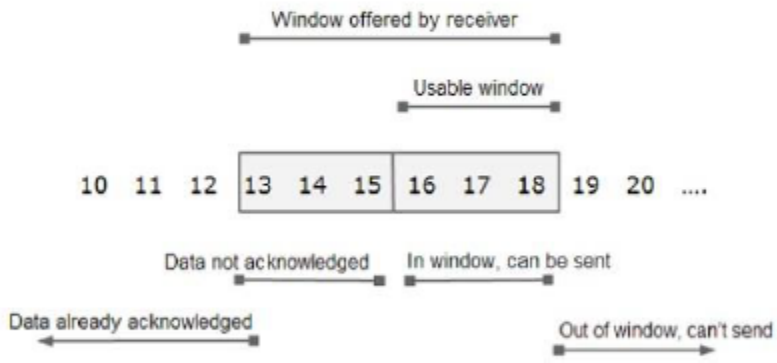


FIGURE 1.17: Sliding Window

In the above figure:

- The window size of the receiver is 6 which means the receiver can accept 6 bytes of data.
- The window size of the sender is 6, ranging from 13 to 18.
- Here, 13 to 15 bytes did not receive any acknowledgement from the receiver.

- Sender can send bytes ranging from 16 to 18.
- The left end of the window closes down as soon as the sender receives the acknowledgement for bytes 13 to 15.
- The window slides towards the right depending on the time taken by the receiver to send the acknowledgement to the sender.

- **Sequence and acknowledgement numbers:** The parties participating in the TCP session need to maintain a 32-bit sequence number in order to identify the amount of data sent. The sender sends a packet along with a sequence number and the receiver acknowledges it with an acknowledgement number in order to confirm the receipt of the data packets. The sender can provide any random sequence number as an initial sequence number. The sequence numbers can vary from 0 and 4,294,967,295.

Three-Way Handshake

A three-way handshake includes the communication between the client and the server in a TCP/IP network. The client and the server need to hand over packets with SYN and ACK flags in order to establish a consistent data communication. The other name for three-way handshake is TCP handshake. The client and the server agree upon an acknowledgement and a sequence number while launching the connection. The sender side determines the sequence number, whereas the receiver determines the acknowledgement number. The acknowledgement number represents the sequence number in addition to the number of bytes received. The three steps involved in the three-way handshake are as follows:

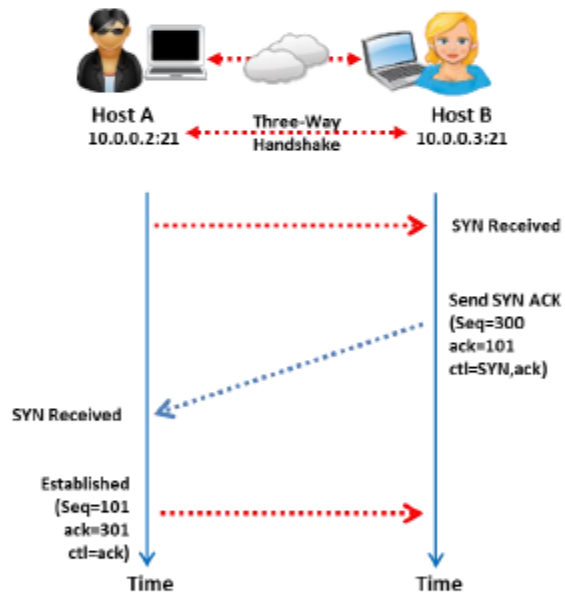
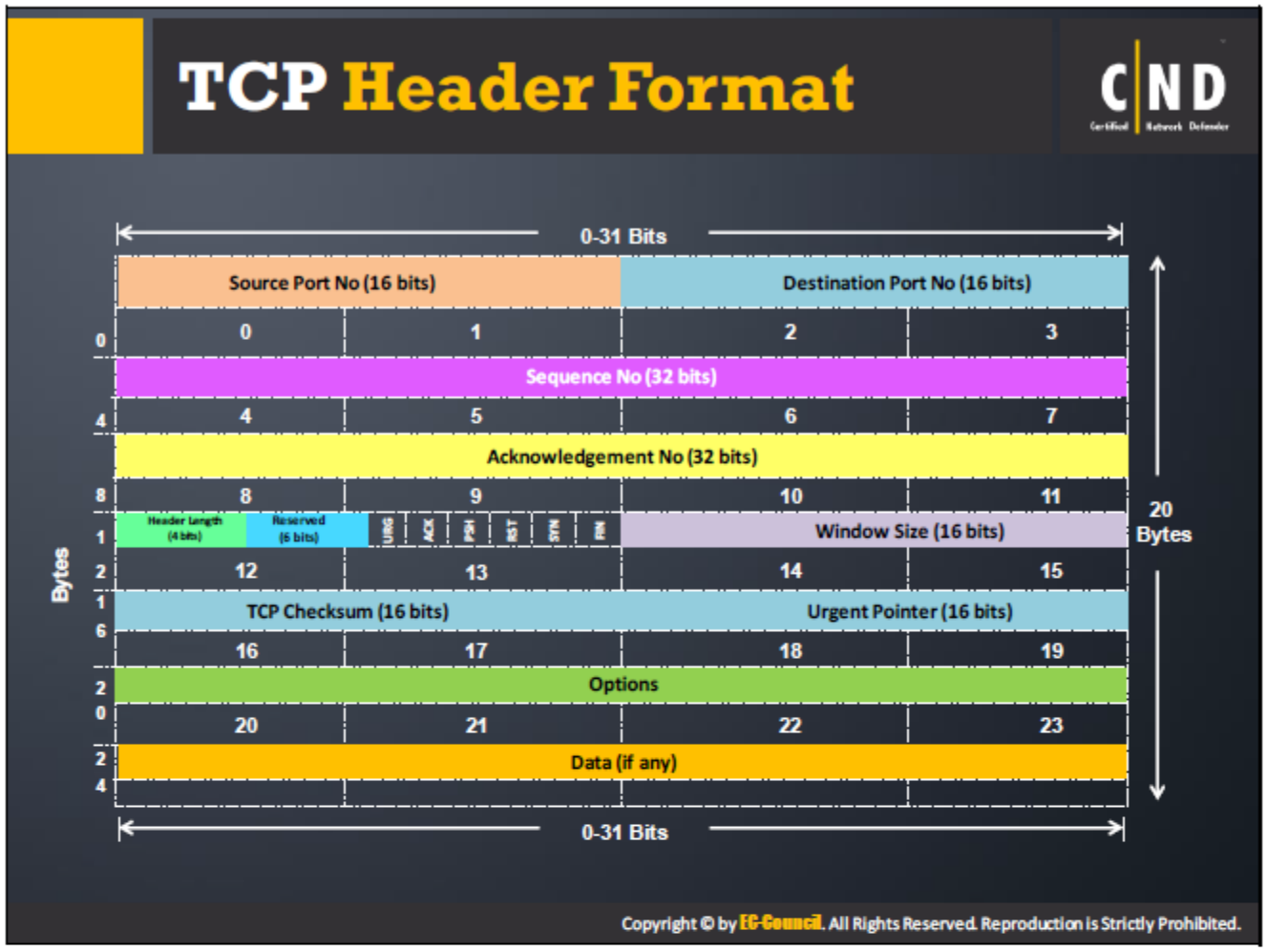


FIGURE 1.18: Three-Way Handshake

- Client sends a request to the server with an SYN flag set in order to establish a connection.
- Server accepts the request and sends an acknowledgement to the client along with the SYN flag.
- The client receives the SYN + ACK flag from the server and sends ACK to the sender.

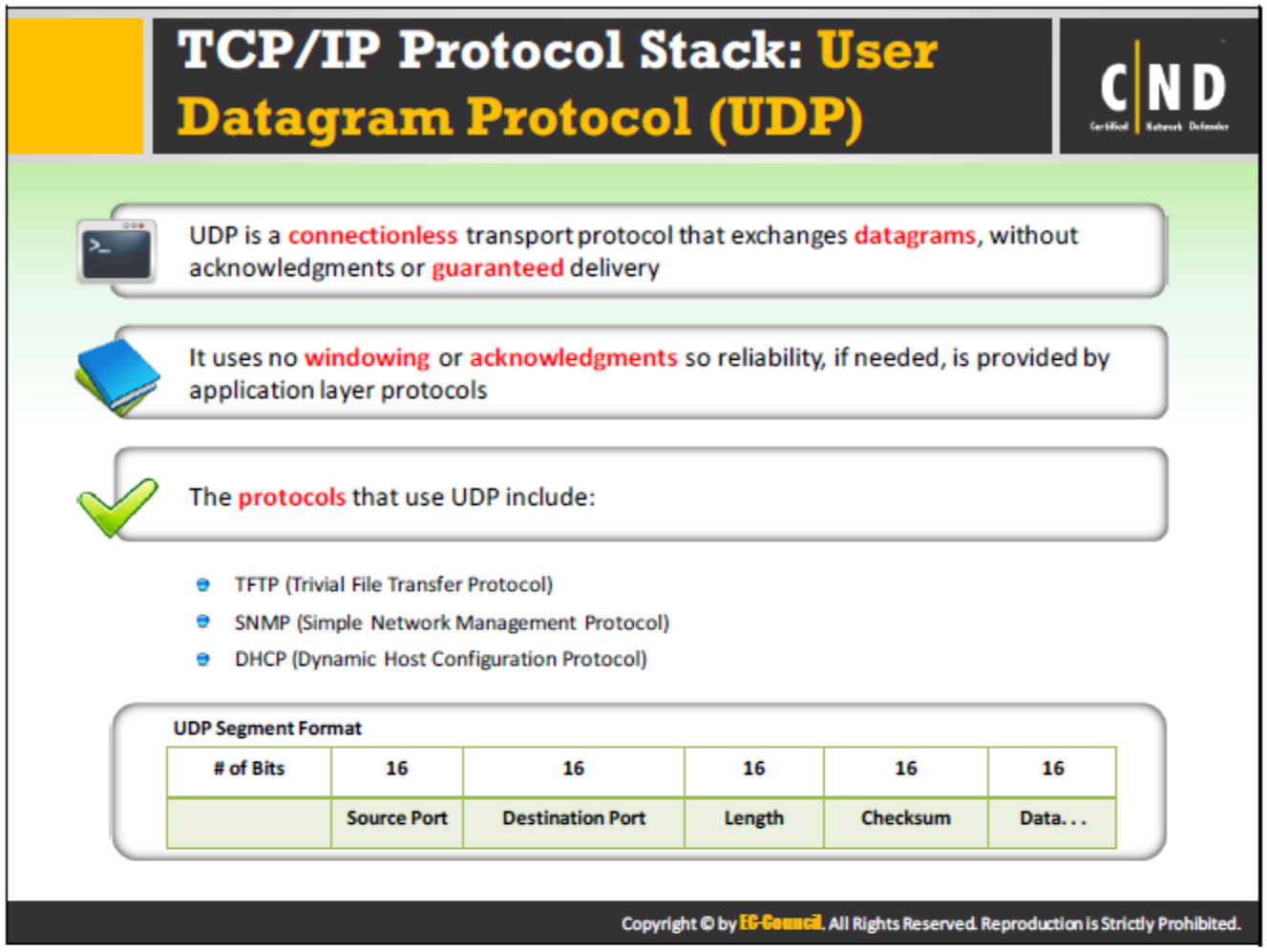
Thus, the above steps establish the connection between the client and the server. They can easily send data as they are aware of the sequence and acknowledgment numbers of each other.



The TCP breaks the data into packets and adds a header to every data packet creating a TCP segment. The TCP segment undergoes an encapsulation process into an IP datagram. The TCP segment consists of the TCP header and the data. The TCP header consists of ten mandatory fields and an optional extension field. The data section follows the TCP header. The data section consists of the data payload for the application. This header does not specify the length of the data section. Subtracting the combined length of the TCP header and the encapsulating header from the total IP datagram length, provides the length of the data section. Various fields present in the IP segment header section are as follows:

- **Source port (16 bits):** Numerical value that indicates the source port.
- **Destination port (16 bits):** Numerical value that indicates destination port.
- **Sequence number (32 bits):** It is the first data octet in the segment. The sequence number becomes ISN in the presence of SYN and the first data octet will be ISN+1.
- **Acknowledgment number (32 bits):** Once the ACK bit is set, this field constitutes of the next sequence number that the sender is actually expected from the receiver and sends these bits after establishing connection between two hosts.
- **Header length (4 bits):** It is the bit number that indicates the number of 32 bit words in the header. Another name for header length is Data Offset field.
- **Reserved (6 bits):** Used for future use. It should be initially set to zero.

- **Control bits (6 bits):** The control bits handle the connection establishment, data transmission and connection termination. The control bits in TCP header include:
  - **URG:** Urgent Pointer field significant.
  - **ACK:** Acknowledgment field significant.
  - **PSH:** Push Function. Whenever TCP receives a request to push data from the application, TCP need to just send the accumulated data without any intervention.
  - **RST:** Reset the connection. The Reset request forces the TCP to drop the connection instantly. The RST forces both the parties involved in the data transmission to break the connection that can lead to loss of data.
  - **SYN:** Synchronize sequence numbers.
  - **FIN:** Closing of connection. The FIN flag represents the closing of the TCP connection.
- **Window (16 bits):** You can set more than one control bit simultaneously. Number of octets the receiver wants to accept. This begins with the packet in the acknowledgement field.
- **Checksum (16 bits):** Header and the data are covered. Here the system calculates the checksum by attaching a pseudo header before or in front of a TCP segment.
- **Urgent (URG) pointer:** This field shows the data meant for quick transmission. Moreover, it points to the position where the urgent data actually ends.
- **Options:** Systems can deliver the options at the end of the header, but it should implement them completely and must have a length that is a multiple of 8-bits. The three different options include:
  - **End of option list:** This list gives the end of option list. Instead of using at the end of each option individually, it displays as the final option. This option comes into picture only when the end of the option does not coincide with the end of the TCP header.
  - **No operation:** This option clearly specifies the boundaries between multiple options and between other options. For instance, it aligns at the beginning of a subsequent option on a word boundary. There is no assurance that a sender will use this option. So, the receiver should be prepared to process the option even if it does not begin the subsequent option on a word boundary.
  - **Maximum segment size:** It is the maximum segment size that TCP can receive and the size is sent at the beginning of the connection establishment process.
  - **Padding:** Indicates that the TCP header ends and data begin at a 32-bit boundary. It consists of all zeros.
- **Data**: The bytes of data send in the segment.



UDP is a connection-less oriented protocol that provides low latency and less tolerating a connection between the applications on the Internet. Unlike TCP, UDP does not promise any consistent availability of data using acknowledgement and sequence numbers. The data passes over the network as datagrams. UDP offers two services, Port numbers in order to determine the different user requests and the checksum in order to confirm the receipt of the data. The broadcasting of messages requires the need of UDP.

Applications like gaming, video applications use UDP for a reliable data transmission. The data transmission using UDP may lead to packet loss, but does not affect the quality of the data transmitted over the network. Forward error correction is a technique that assists in improving the audio and video signals. UDP uses the lossless transmission mechanism for the transmission of large files. The lossless transmission mechanism helps in the retransmission of lost data packets, thereby increasing the data transfer rate. A UDP header format includes:

# of Bits	16	16	16	16	16
	Source Port	Destination Port	Length	Checksum	Data. . .

FIGURE 1.19: UDP header format

- **Source Port**: Refers to the port number of the port. This determines the location to send the reply packet. If the server host is the source host, then the port number can be a well-known port number, whereas, if the source port is the client, then the port number can be ephemeral port number.

- **Destination Port**: Refers to the packets from a client. Same as the destination port, if the destination port is a client, the port number can be an ephemeral port number, whereas if the destination port is a server, the port number can be any well-known port number.
- **Length**: The length field determines the length of the UDP header as well as the UDP data. The minimum specified length is 8 bytes.
- **Checksum**: The checksum performs the error-checking of the data and the header. It uses the standard internet checksum algorithm and verifies whether the correct destination receives the packet according to the IP address, port number and protocols specified in the header.

UDP Operation

The primary operation of UDP is to collect the data from the higher layer protocols and place it in UDP messages to forward the UDP datagrams to the internet protocol for transmission. UDP provides a checksum capability that helps in detecting the errors in the data transmission, ensures the proper transmission of the UDP message and detects whether the message reached the exact destination or not. The basic steps that are involved in the transmission of data using UDP are as follows:

- **Higher-Layer Data Transfer:** Application sends a message to the UDP software.
- **UDP Message Encapsulation:** Encapsulates the received message into the Data field of a UDP message. It occupies the headers of the UDP message, source port, the destination port and checksum value may be calculated.
- **Transfer Message to IP:** Pass UDP message to IP for transmission.

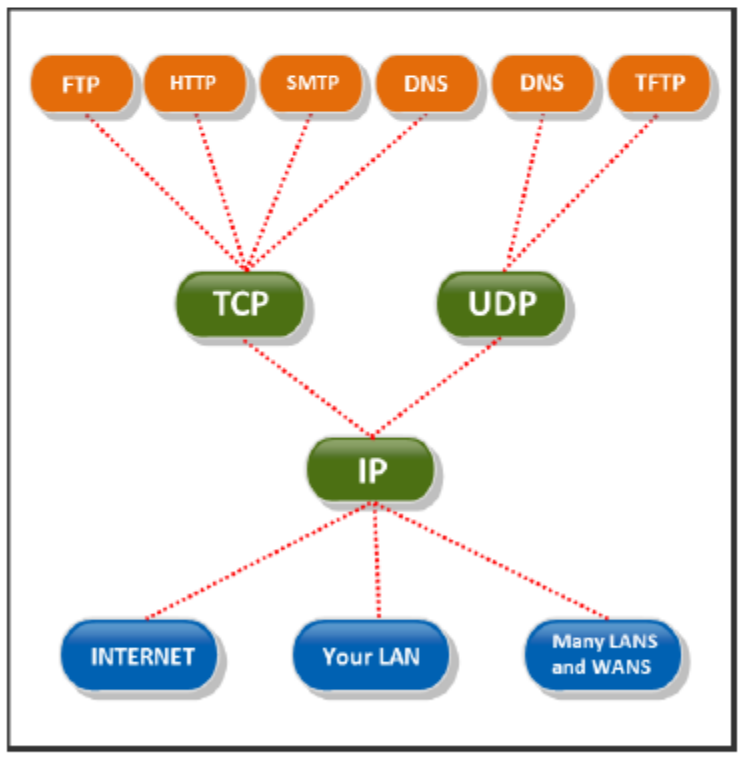
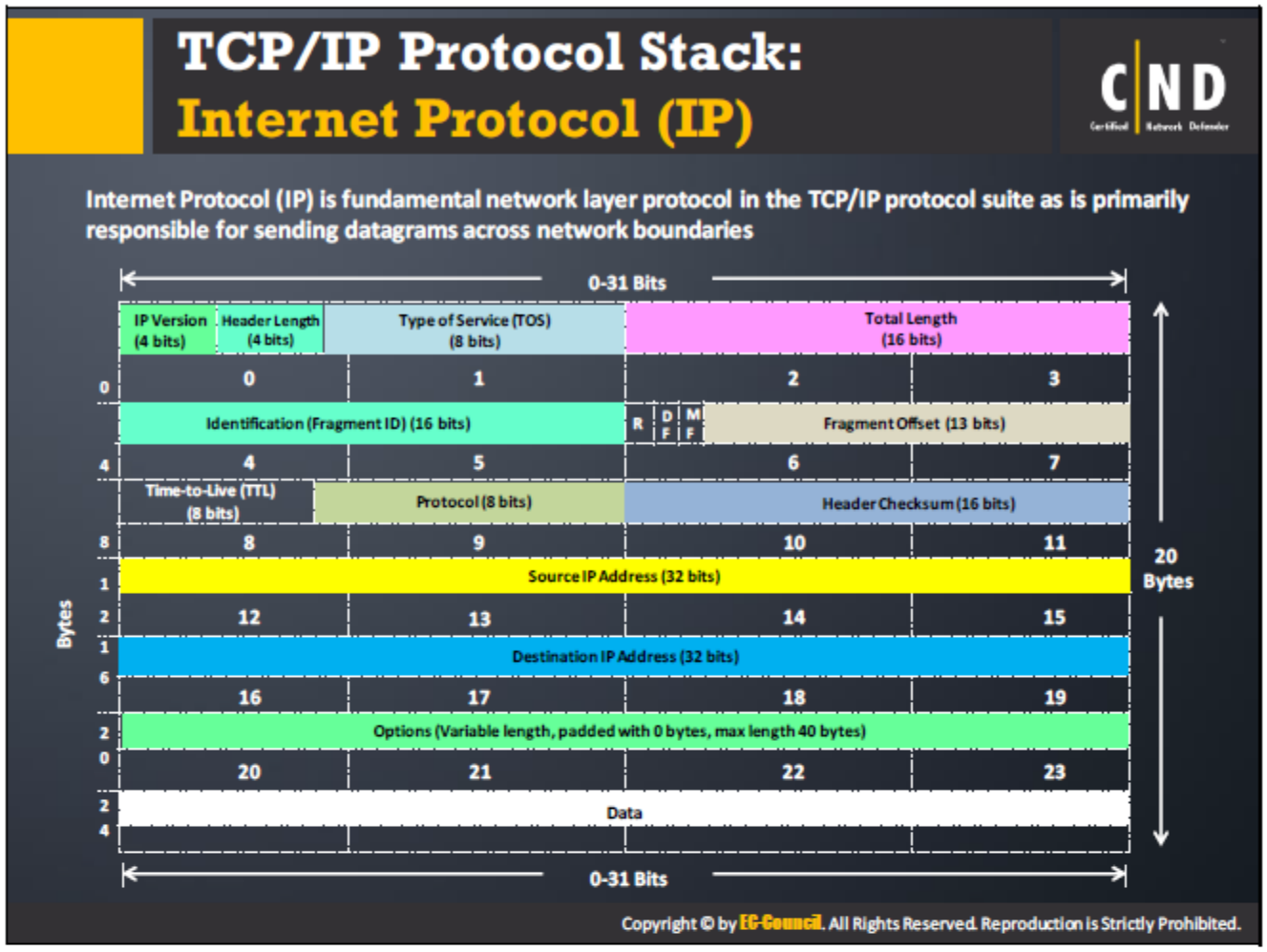


FIGURE 1.20: Passing messages to TCP and UDP

Comparison of UDP and TCP

- **TCP**:
  - Reliability: The TCP works well at the transport layer. It manages the message acknowledgement, retransmission and timeout. It confirms the arrival of all the packets at the receiver and attempts retransmission of lost packets again and again.
  - Ordered: It confirms that the messages arrive in an orderly manner or in sequence. It rearranges the data arriving in the wrong order.
  - Heavyweight: TCP manages reliability and congestion control.
  - Streaming: TCP manages data as a byte stream.
  - Connection-oriented: Creates a session between the hosts.
- **UDP**:
  - Unreliable: UDP does not confirm the arrival of packets at the destination. It does not attempt in retransmitting the lost packets or does not follow the concept of acknowledgement.
  - Not ordered: UDP does not confirm the sequence of the arrival of the packets at the destination.
  - Datagrams: UDP handles packets individually and deals with them only after its arrival at the destination.
  - Connection-less oriented: Does not create any session between the hosts.
  - Broadcasts: UDP can send packets or broadcast the packets to multiple devices.



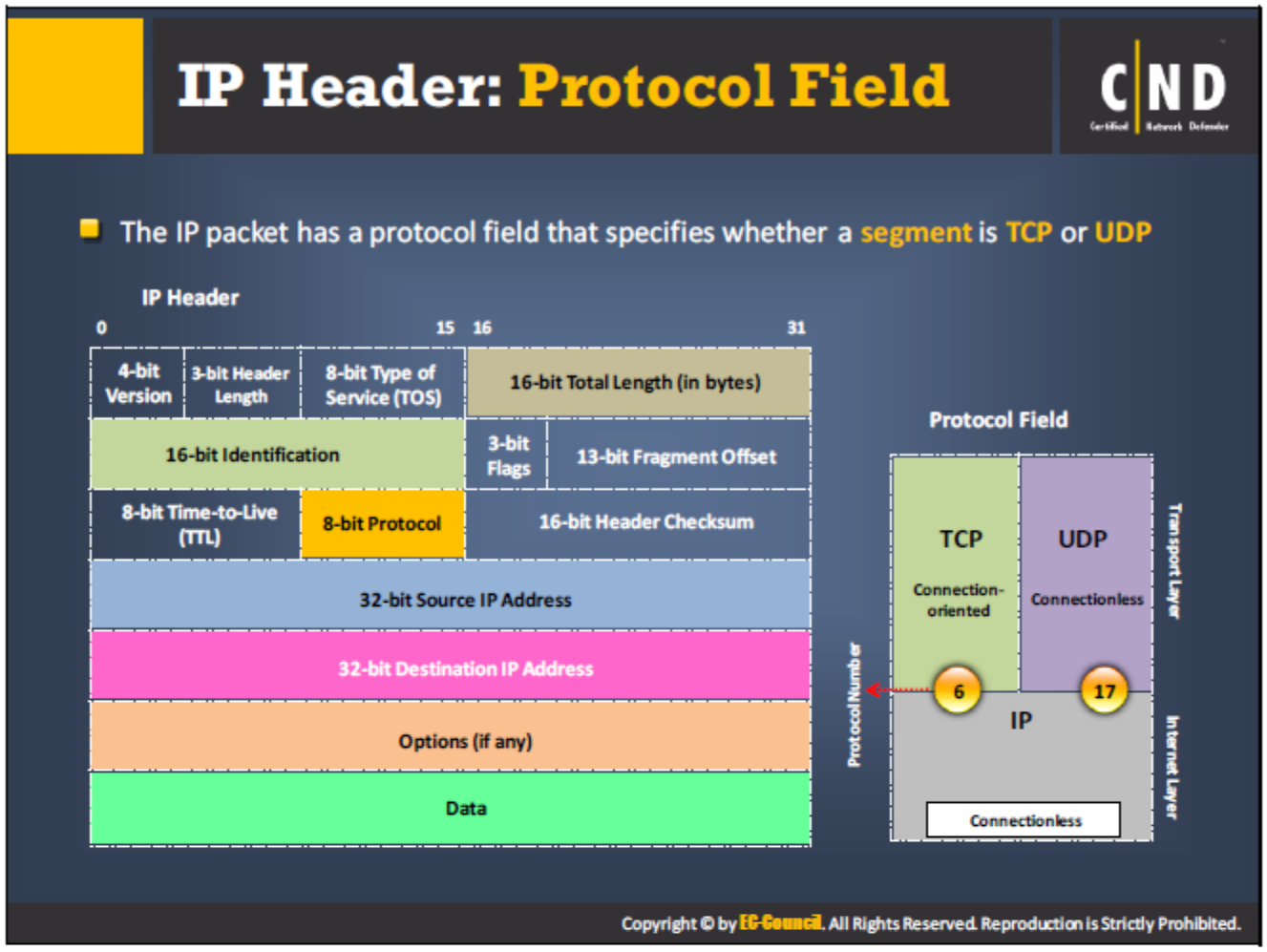
IP is a network layer protocol present in the TCP/IP communications protocol suite. The data is always sent as packets or data grams in networking. IP provides a unanimously defined address that eliminates the need to create a connection before sending data. IP also provides a datagram service that carries information or data to the destination without much guarantee regarding the confirmed arrival of these packets at the destination. The packets can be lost on the way to the destination or can arrive at the destination in a completely or partially damaged form.

There are two versions of IP available: Internet protocol version 4 (IPv4) and Internet protocol version 6 (IPv6). The commonly used version is IPv4 represented using a 32-bit address. The IPv6 is an improved version of IPv4 and represented using a 128-bit source and destination address. The IP header is an introduction to the IP packet that contains information like IP version, Source IP, destination IP, TTL, etc. The header normally is responsible for holding data required to traverse the data over the internet. The IP header has the same format as that of a data.

Various fields in the IP header are as follows:

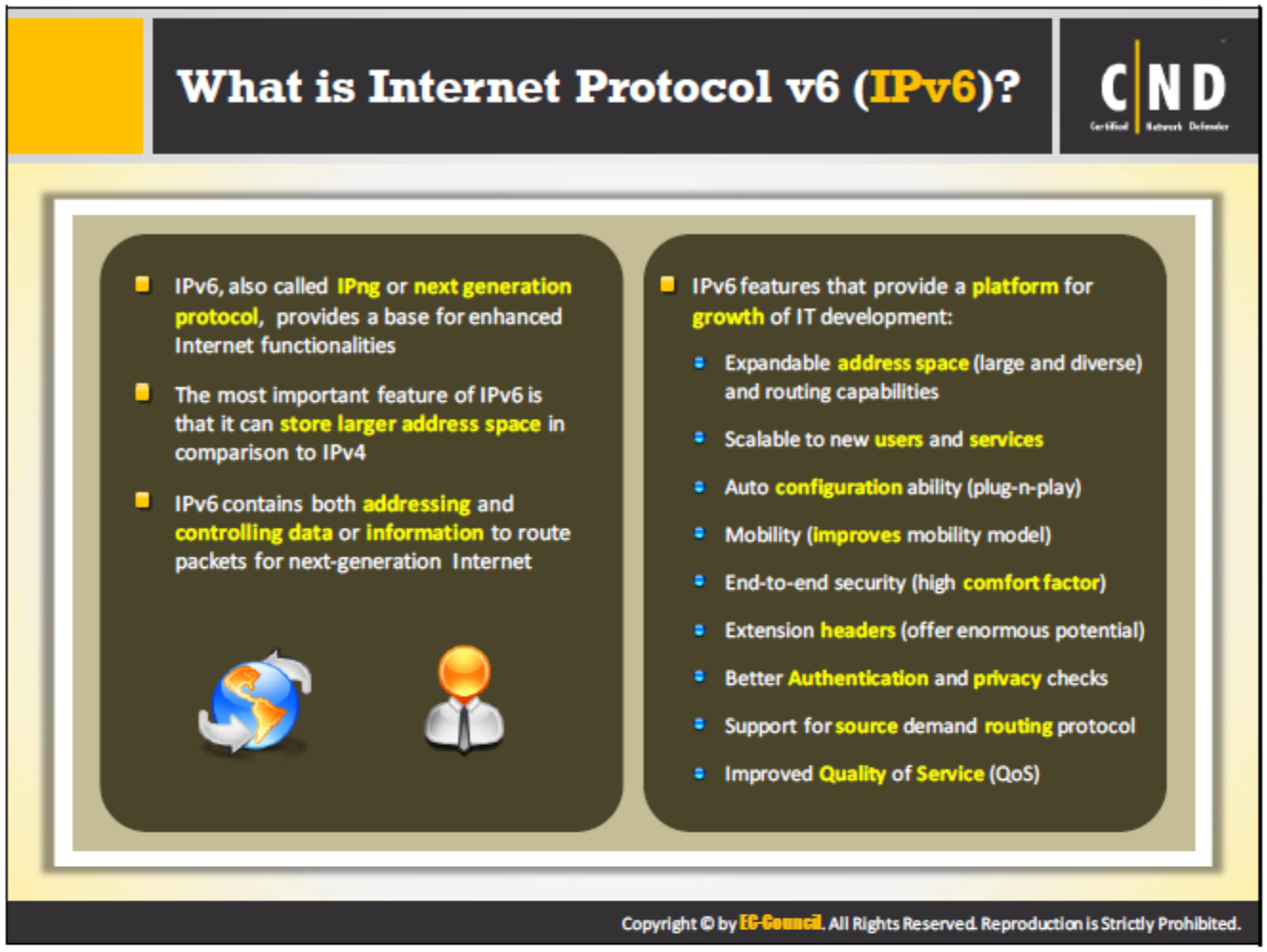
- **IP Version (4 bits):** There are two types of IP packet and addressing IPv4 and IPv6. This bit specifies the current IP protocol version. Always set the value as 4.
- **Header Length (4 bits):** Length of the IP header where header represents 32-bit words along with IP options if any. The minimum value of the IP header is 5.

- **Type of Service (TOS) (8 bits):** Provides quality of service features. First three bits are for IP precedence, 4 bits for TOS and last one-bit left alone (not used).
- **Total Length (16 bits):** Specifies the length of the IP datagram in bytes. It includes the length of the header and the data.
- **Identification (16 bits):** Identifies the fragments of one datagram from those of another.
- **Fragment Offset (13 bits):** Used to reassembly the fragmented IP datagrams.
- **Time-O-Live (TTL):** It defines the lifetime of the IP datagram in the internet system. The TTL field is initially set to a number and decremented by every router. When the TTL reaches zero, it discards the datagram (Packet).
- **Protocol (8 bits):** Identifies the next encapsulated protocol that sits above the IP layer.
- **Header Checksum (16 bits):** Identifies the errors during IP datagram transmission and calculated based on the IP header.
- **Source IP Address (32 bits):** This field represents the IP address of the sender.
- **Destination IP Address (32 bits):** This field represents the IP address of the receiver (destination).
- **Options (variable in length):** This is an optional field. List of options that are applicable for the active IP datagram.
- **Data (variable in length):** This field contains the data from the protocol layer that handed over the data to the IP layer.



The protocol field in the IP header determines the services available in the next higher levels in the protocol stack. The protocol field is eight bits in length and includes 256 protocols. Multiple higher layer protocols can use IP (multiplexing). "Assigned Numbers" specifies the values for various protocols. Protocol and some common values (1 octet) are as follows:

- 0 (0x00) IPv6 Hop-by-Hop Option
- 1 (0x01) ICMP protocol
- 2 (0x02) IGMP protocol
- 4 (0x04) IP over IP
- 6 (0x06) TCP protocol
- 17 (0x11) UDP protocol
- 41 (0x29) IPv6 protocol

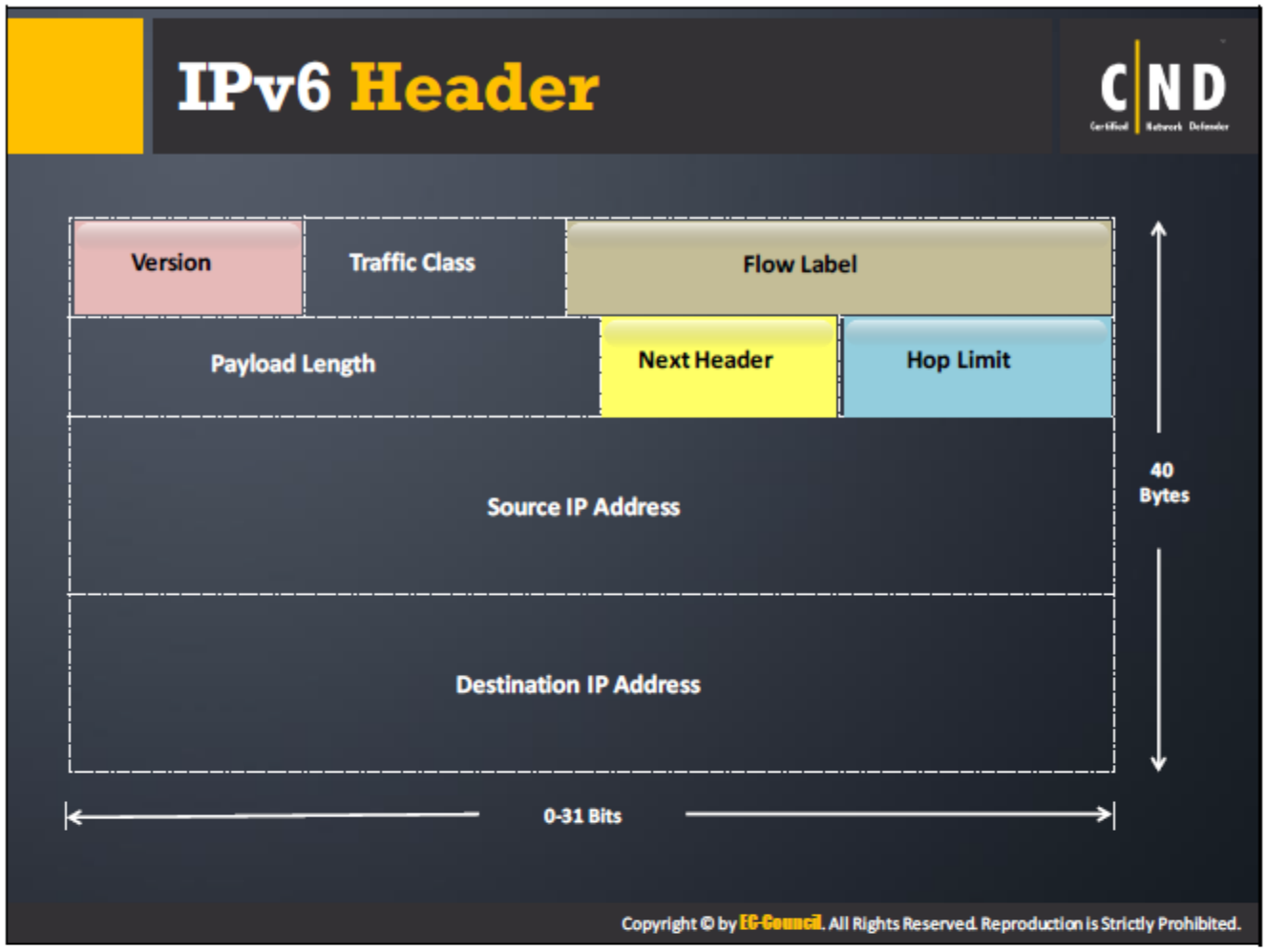


Internet protocol version 6 is the most recent version of the internet protocol. The internet protocol version 6 provides a mechanism for identifying the computers in the network and performs routing of the traffic across the internet. To meet the increasing requirements, Internet Engineering Task Force (IETF) started a working group called Internet Protocol next generation (IPng) to make research, experiments and recommendations for finding a new generation protocol for IP. It eventually found the specification for internet protocol, version 6 (IPv6) described in Internet standard document RFC 2460. Experts consider IPv6 as a replacement to IPv4. The IPv6 uses a source and destination address in order to carry data packets over the network, which is the same as in IPv4. IPv6 has a very large address space and consists of 128 bits as compared to 32 bits in IPv4.

The features of IPv6 include

- IPv6 internet layer protocol is for packet-switched internetworking, it provides end-to-end transmission of data across multiple IP networks.
- IPv6 is capable of providing large address space for increasing demands of internet users.
- It has a new format for packet header to minimize packet-processing problems with overhead routing entries. Routers can efficiently and easily process IPv6 headers.
- IPv6 have globally identified unique addresses with efficient, hierarchal and routing infrastructure that relies on prefix length rather than address classes. This allows the backbone routers to create small routing tables.

- IPv6 simplifies host configuration with stateless and stateful address configuration for network interfaces.
- In IPv6, hosts on a link are capable of automatically configuring themselves with a link called link-local addresses by responding to the prefixes mentioned by the local routers. When the host sends a link local address request to a local router for connecting to that network, it then responds to the request by sending its configuration parameters. This lets the host to configure automatically with the available router. IPv6 is even capable of configuring itself, even though there are no routers.
- IPv6 has an inbuilt security feature called integrated internet protocol security (IPsec). It is a set of internet standards based on cryptographic security services providing confidentiality, data integrity and authentication.
- IPv6 supports unicast and multicast communication along with a new communication type called anycast. In the anycast communication method, only the specific associated address in a network receives the messages.
- IPv6 provides better support for quality of service (QoS) with proper management of network traffic.



The IPv6 is four times larger than IPv4. However, the header of IPv6 is only two times larger than the IPv4. The IPv6 header consists of one fixed header and zero or more extension headers. The extension headers consist of information that assists the routers in determining the flow of a packet.

The IPv6 is 40 bits long and the fields in the fixed header consist of:

- **Version (4 bits):** Specifies the version of the internet protocol.
- **Traffic class (8 bits):** identifies the data packets that belong to the same traffic class and distinguishes the packets with different priorities.
- **Flow label (20 bits):** This field avoids reordering of data packets and maintains the sequential flow of data packets belonging to the communication.
- **Payload length (16 bits):** It informs the router about the length of the data which is present for a particular packet in its payload.
- **Next header (8 bits):** Identifies the type of header following the IPv6 header and located at the beginning of the data field (payload) of the IPv6 packet.
- **Hop limits (8 bits):** Replacement of time-to-live field in IPv4. Identifies and discards the packets that are stuck in an indefinite loop due to any routing information errors. When the counter reaches zero, it discards the packet.
- **Source IP address (128 bits):** IPv6 address of the sending host.
- **Destination IP address (128 bits):** IPv6 address of the receiving host (Destination).

Extension Header

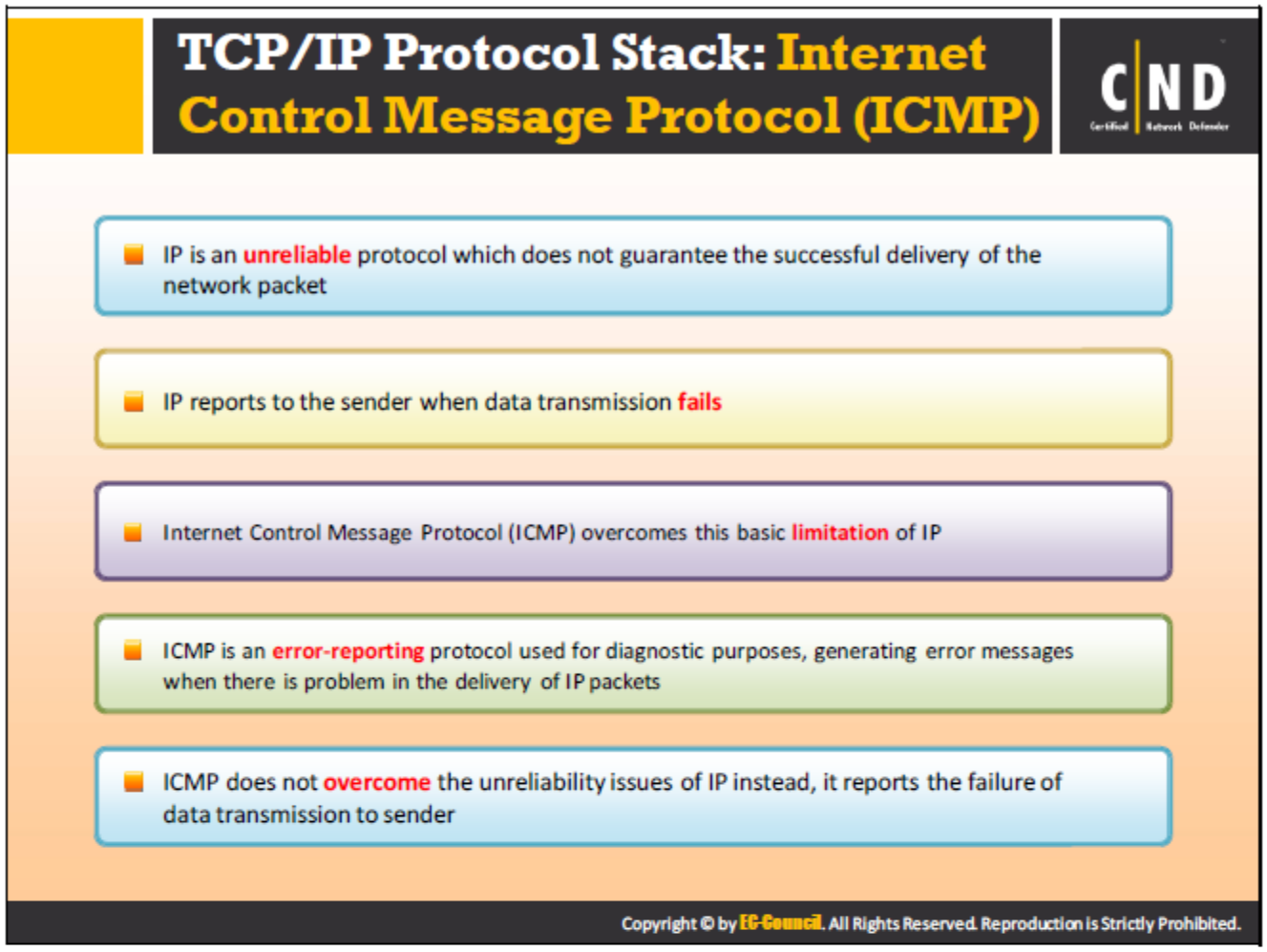
The fixed header consists of only required information. The information that is rarely used or is not required is always put between the fixed header and the upper layers of the extension header. Each extension header requires the need of a distinct value in order to identify the extension headers.

The IPv6 header points to the first extension header. Now, consider there are more than one extension header. Then, the extension header points to the next extension header. The last extension header points to the upper layer header. The sequence of the extension headers are as follows:

IPv6 header
Hop-by-Hop Options header
Destination Options header[1]
Routing header
Fragment header
Authentication header
Encapsulating Security Payload header
Destination Options header[2]
Upper-layer header

FIGURE 1.21: Sequence of IP header

The extension headers are arranged in a linked list manner represented using one header after the other.

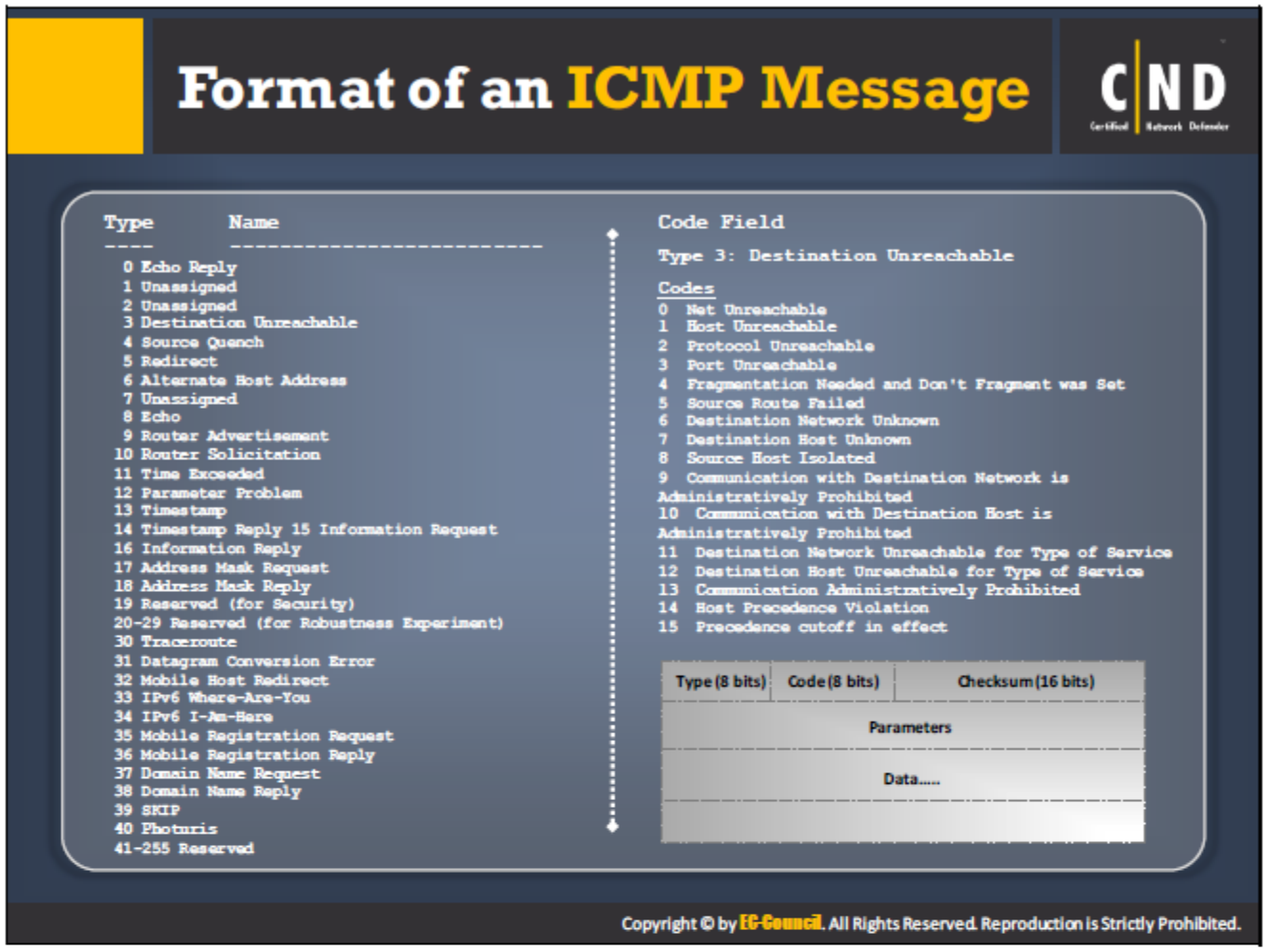


ICMP is an error reporting protocol used by networking devices like routers in order to send error messages. ICMP relays query messages by locating its application. ICMP is not a transport protocol that sends data between two communicating systems. Network administrators troubleshooting internet connections mainly use these. ICMP transmits messages as datagrams and consists of an IP header that encapsulates the ICMP data. The IP packets contain ICMP in the IP data field. The ICMP messages can also contain the IP header of the original message that assists the end system in understanding why and which packet failed. The IPv4 or IPv6 is followed by the ICMP header and identifies itself as protocol number 1.

The ICMP protocol consists of three fields:

- The major type identifies the ICMP message.
- The minor code that contains more information regarding the type field.
- The checksum that identifies the errors originated during transmission.

The ICMP data and the IP header follow the three fields in the ICMP protocol.



ICMP messages consist of an IP header that encapsulates the ICMP data. ICMP transmits the data as datagrams. ICMP packets are IP packets with ICMP in the IP data portion. ICMP messages also contain the entire IP header from the original message, so the end system knows which packet failed.

The structure of an ICMP message consists of three fields that have the same size and the same meaning in all ICMP messages. The values in the fields are not the same for each ICMP message type. The unique part contains fields that are specific to each type of message. The common message format is the same for ICMPv4 and ICMPv6.

- **Type:** This field identifies the ICMP message type. For ICMPv6, values from 0 to 127 are error messages and values 128 to 255 are informational messages. The length of this field is 1 byte. The types are defined as:

Type	Name
0	Echo Reply
1	Unassigned
2	Unassigned
3	Destination Unreachable
4	Source Quench
5	Redirect
6	Alternate Host Address
7	Unassigned
8	Echo
9	Router Advertisement
10	Router Solicitation
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
19	Reserved (for Security)
20-29	Reserved (for Robustness Experiment)
30	Traceroute
31	Datagram Conversion Error
32	Mobile Host Redirect
33	Pv6 Where-Are-You
34	IPv6 I-Am-Here
35	Mobile Registration Request
36	Mobile Registration Reply
37	Domain Name Request
38	Domain Name Reply
39	SKIP
40	Photuris
41	255 Reserved

TABLE 1.1: ICMP types

- **Code:** This field identifies the subtype of message within each ICMP message Type value. For each message, the field allows defining of up to 256 subtypes. The length of this field is 1 byte. The types are defined as:

Code	Name
0	Net Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragmentation Needed and Don't Fragment was Set
5	Source Route Failed
6	Destination Network Unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Communication with Destination Network is Administratively Prohibited
10	Communication with Destination Host is Administratively Prohibited
11	Destination Network Unreachable for Type of Service
12	Destination Host Unreachable for Type of Service
13	Communication Administratively Prohibited
14	Host Precedence Violation
15	Precedence cutoff in effect

TABLE 1.2: ICMP codes

- **Checksum:** The length of this field is 2 bytes. This 16-bit checksum field is calculated in a manner similar to the IP header checksum in IPv4. It provides error detection coverage for the entire ICMP message.
- **Data:** This field includes the specific fields used to implement each message type. The size of this field is variable.

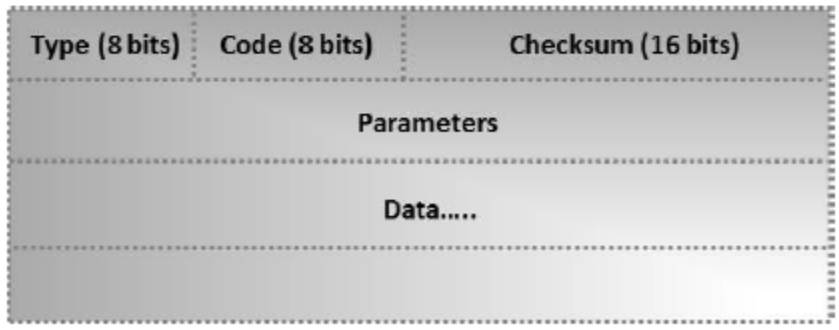
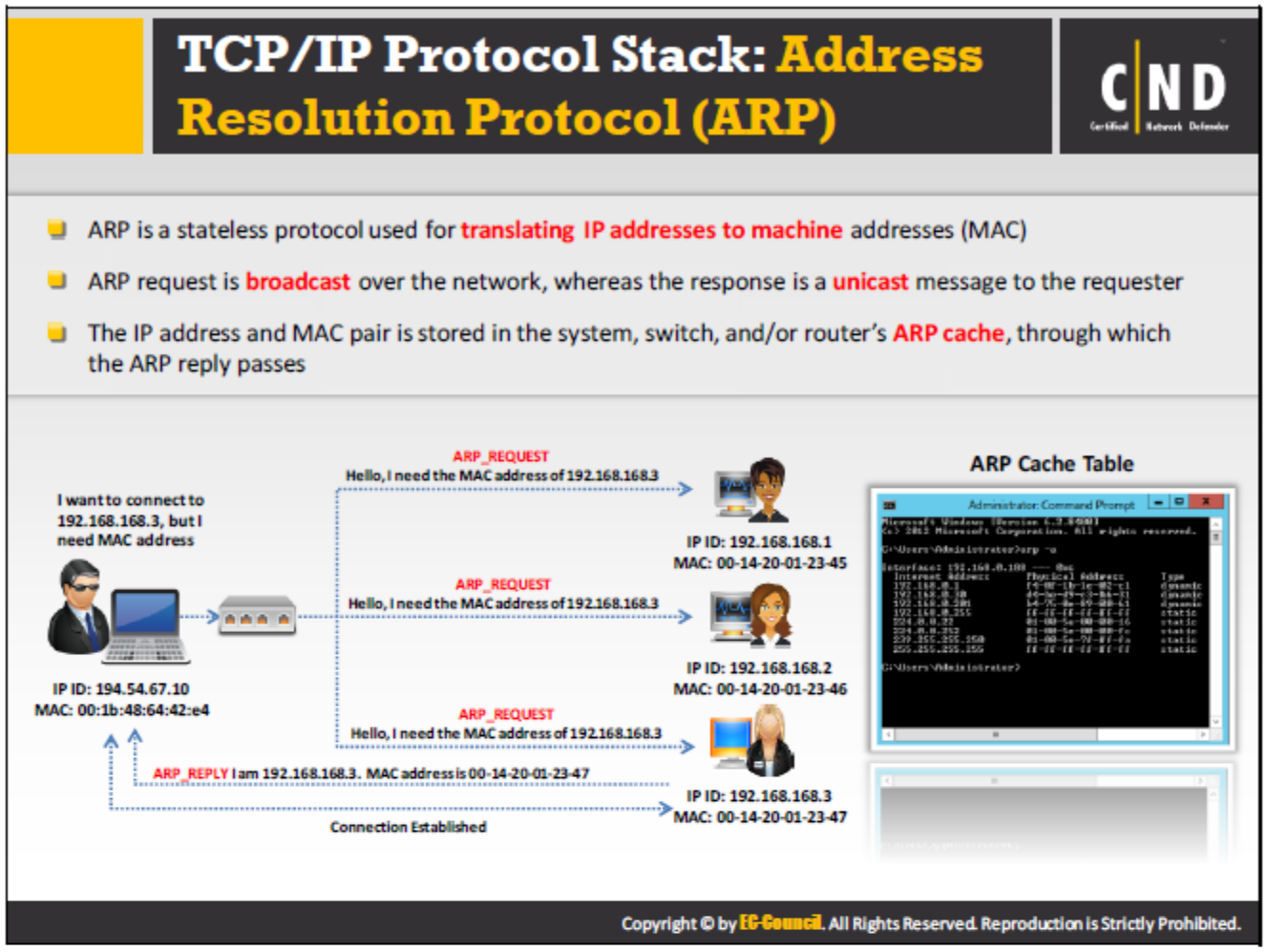


FIGURE 1.22: ICMP message format



The address resolution protocol deals with converting the IP address to a physical address (Mac address). The component address resolution refers to identifying the IP address of a computer in a network. ARP is RFC 826 and its Internet Standard is STD 37. The protocol operates below the network layer as a part of the interface between the OSI network and OSI link layer. IPv4 supports ARP when it is used over Ethernet.

The address resolution protocols are mainly a request and reply protocol and captured by the line protocol. The address resolution protocol links only within the limits of the boundaries and does not perform any communication across the internetwork nodes. The ARP maintains a table known as ARP cache that keeps track of the Mac addresses and its corresponding IP address. However, there are certain rules in maintaining the MAC addresses and IP addresses in the table that enables the conversion from one form to another.

Working of ARP

The term address resolution refers to the process of finding an address of a computer in a network. The process of ARP is as follows:

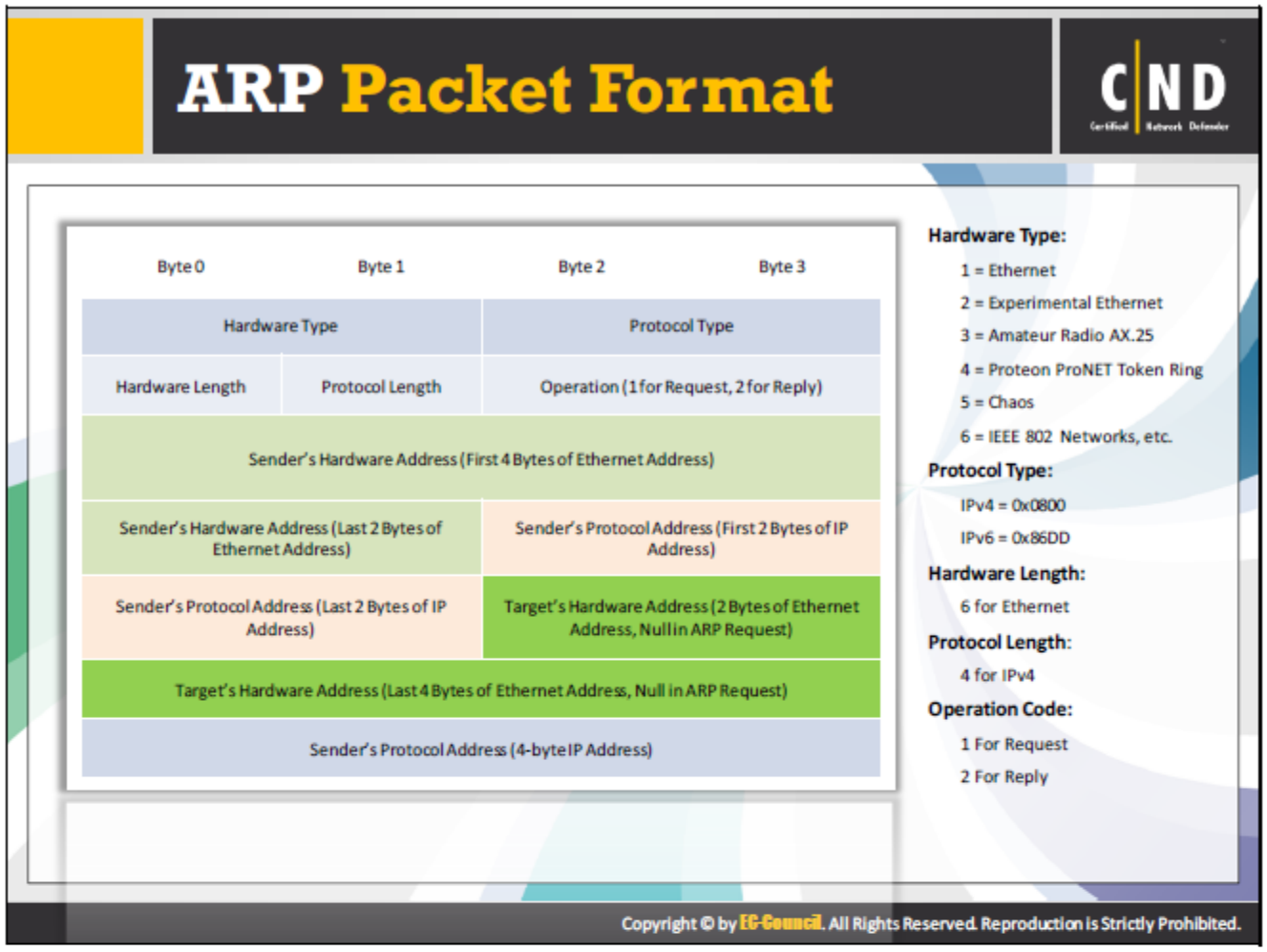
- A client process sends a request to the server process to find a physical host or MAC address that matches with the IP address.
- The server sends the message to all connected computers on the network to identify the network system for which the address was required.

- After finding the requested MAC address, the server sends a response to the client process with the requested MAC address.

ARP Cache Table

ARP cache table stores the matched sets of IP addresses and the corresponding MAC addresses of systems frequently communicating on the network. Each device on the network manages its own ARP cache table. There are two different ways to store cache entries into the ARP cache table:

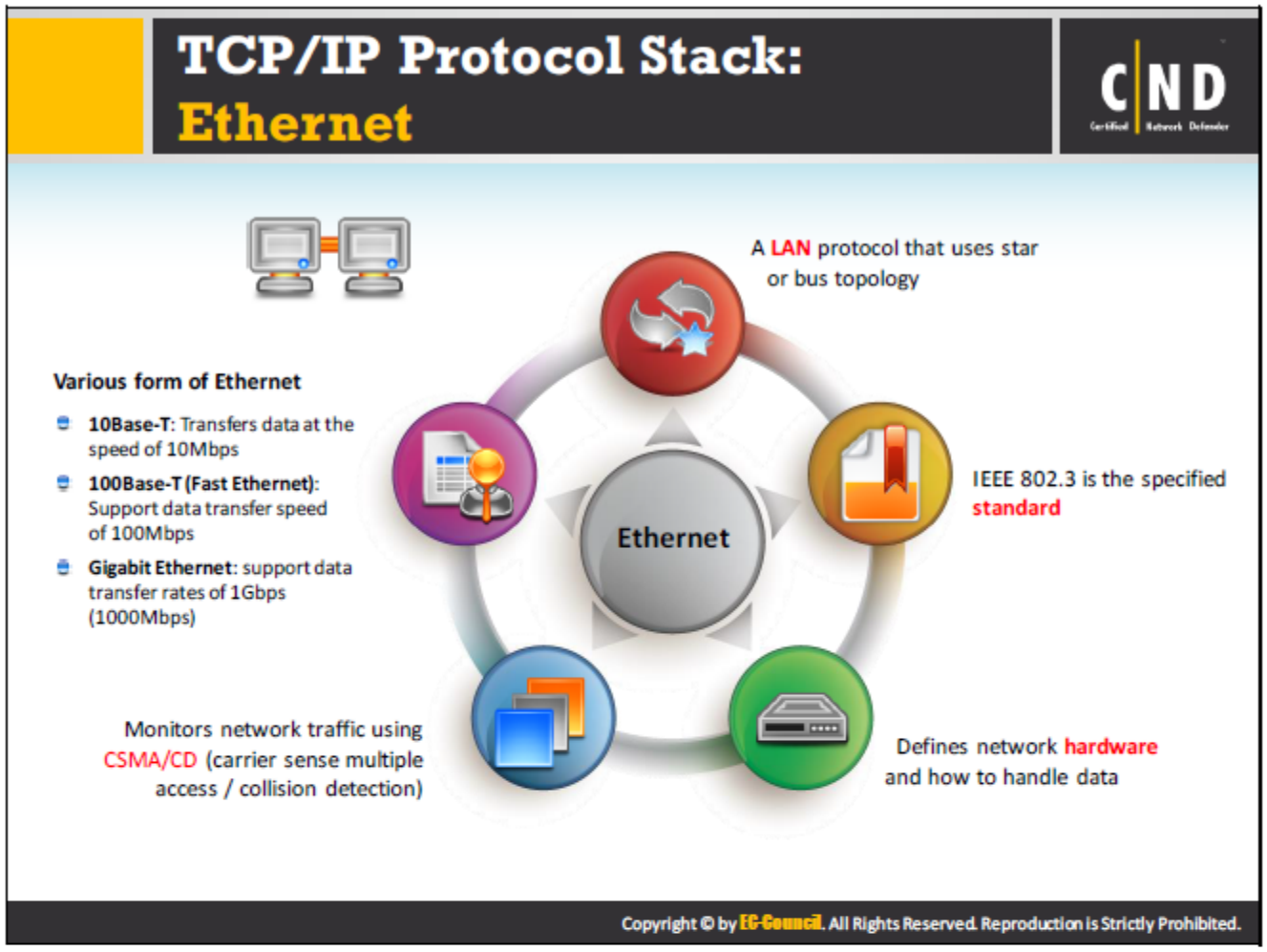
- **Static ARP Cache:** These address resolutions are manually added to the cache table for a device and they are kept in the cache on a permanent basis. To manage static entries, use tools such as the ARP software utility.
- **Dynamic ARP Cache:** These hardware/IP address pairs are added to the cache by the software itself because of successfully completed past ARP resolutions. They are kept in the cache only for a specific period and are then removed.



The standard ARP packet has the following fields:

- **Hardware Type:** This field identifies the type of hardware used for the local network transmitting the ARP message. The size of this field is 2 octets and the value of this field for Ethernet is 1.
- **Protocol Type:** This field specifies the network protocol for the intended ARP request. The value of the field for IPv4 is 0x0800 and IPv6 is 0x86DD. The permitted length of this field is 2 octets.
- **Hardware Length:** This field specifies the length (in octets) of a MAC address in fields 5 and 7 of the ARP packet. For Ethernet, the value of this field is 6.
- **Protocol Length:** This field specifies the length (in octets) of the protocol addresses in fields 6 and 8 of the ARP packet. The address length for IPv4 is 4.
- **Operation:** This field specifies the operation that the sender is performing. The value for ARP request is 1 and for ARP reply is 2.
- **Sender's Hardware Address:** This field contains the MAC address of the device sending the message such as the IP datagram source device on a request and the IP datagram destination on a reply.
- **Sender's Protocol Address:** This field contains the IP address of the device sending this message.

- **Target Hardware Address:** This field contains the MAC address of the intended receiver. In an ARP request, this field is ignored (zero). In an ARP reply, this field indicates the address of the host that originated the ARP request.
- **Target protocol address:** This field contains the IP address of the device of the intended destination.



Ethernet is the most commonly used LAN technology. It is a link layer protocol that determines the data transmission between the network devices present in the same network. It uses a bus or star topology and 10 BASE-T maintains a data transfer rate of 10 Mbps. Ethernet formed the basis for the IEEE 802.3 standard that determines the physical and lower software layers. The data transmission occurs in two units: packets and frames. The frame includes information like payload of the data and the physical or Mac address of the sender and the receiver. Every frame wraps itself in a packet that contains several bytes of information required for establishing the connection. It is preferred mostly since, it is easy to install, less expensive and allows high-speed data transfers. It monitors network traffic using CSMA/CD (carrier sense multiple access / collision detection). Ethernet most commonly uses 100 BASE-T that provides transmission speed up to 100 megabits per second. The Gigabit Ethernet provides a transmission speed of about 1000 Mbps and GigaBit Ethernet provides a transmission speed of about 1 Gbps. Other common LAN types include:

- Fast Ethernet
- Token Ring
- Fiber Distributed Data Interface (FDDI)
- Asynchronous Transfer Mode (ATM)
- LocalTalk

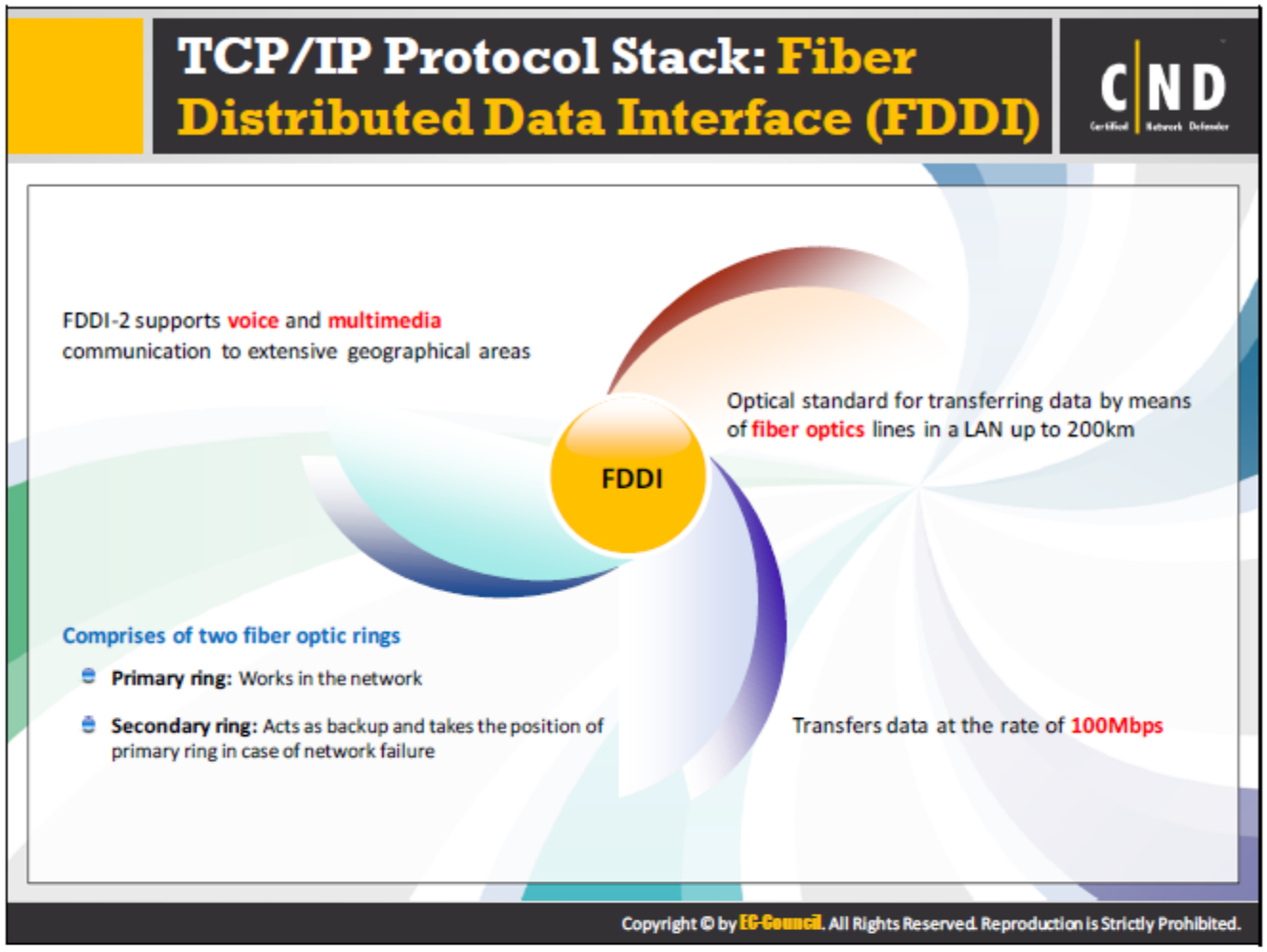
Features of LAN include:

- Enables easy handling, management and maintenance.
- Enables low-cost implementations.
- Allow a topological reliability for the network installation.

The Ethernet LANs consist of the following network nodes and connecting media. There are two types of classification of the network nodes:

- **Data terminal equipment (DTE):** The DTE represents the source or the destination of the data frames. The DTE's are devices like: workstations, file servers, print servers, etc.
- **Data communication equipment (DCE):** The network device that is responsible for receiving and passing the frames across the network. The DCE includes devices like repeaters, switches and routers.

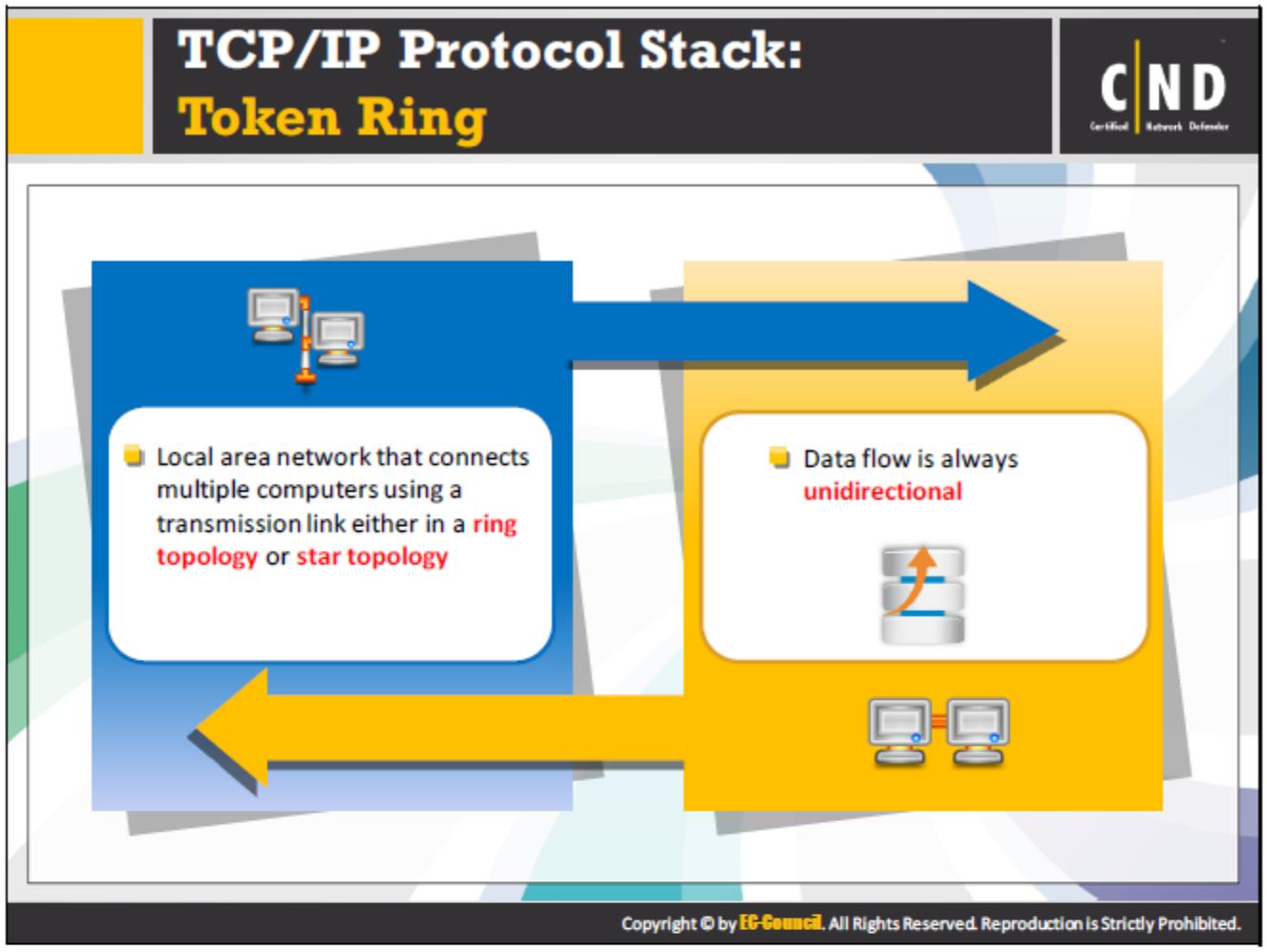
The Ethernet finds its main application in wired networking, although the wireless networking seems to take the place of the wired network. Experts say that the 802.11 ac provides more internet speed than 1Gb Ethernet. The important thing about wired networking is that it has less impact due to interference and is more secure than wireless networking.



FDDI is an optical standard used for transferring data by means of fiber optic lines in a LAN up to 200km. The data transmission occurs at the speed of 100Mbps through a fiber optic cable and uses a token ring to determine which workstation can transfer data at the specified time. FDDI uses a fiber optic cable wired in a ring topology. It uses a token passing access method (Please refer "token ring" topic) that provides equal responsibilities and privileges to all the computers connected to the network.

A normally operating FDDI ring passes the token to all the network devices, whereas an abnormal operating FDDI ring circulating the token to the devices connected to the ring becomes invisible abruptly after a certain period, indicating a network issue. Furthermore, you can set the priority levels using FDDI i.e., server is allowed to send a huge volume of data frequently compared to the client systems.

It consists of two rings, one is primary and the other is secondary. Primary ring carries data between the systems, whereas secondary ring acts as a backup to the primary ring. When this primary ring fails to operate in the network, the secondary ring comes into picture and performs all the operations usually carried out by the primary ring. This method transmits data at high speed, but with Fast Ethernet allows transfer of huge amounts of data at 100Mbps, all at a very low cost. However, organizations are now using Gigabit Ethernet, which transfers data at the rate of 1000Mbps. The latest version of FDDI is FDDI-2, which supports voice and multimedia communication to extensive geographical areas.



A local area network that consists of computers connected in a ring or bus topology and uses a token to manage the transmission of data between the two computers. The presence of a token can avoid the chances of a collision between the data transferred between the computers. The possession of the token will allow the network nodes the right to transmit the data, if any node receives the token, it captures the data and alters it with 1 bit of token, thus adding the data packets that it wants to transmit to the next node. Token ring allows the users to send the data only after arrival of token to their respective location, thus, preventing data collision between the workstations who want to send messages at the same time. The maximum size of token ring packet is 4500 bytes.

How a token ring functions:

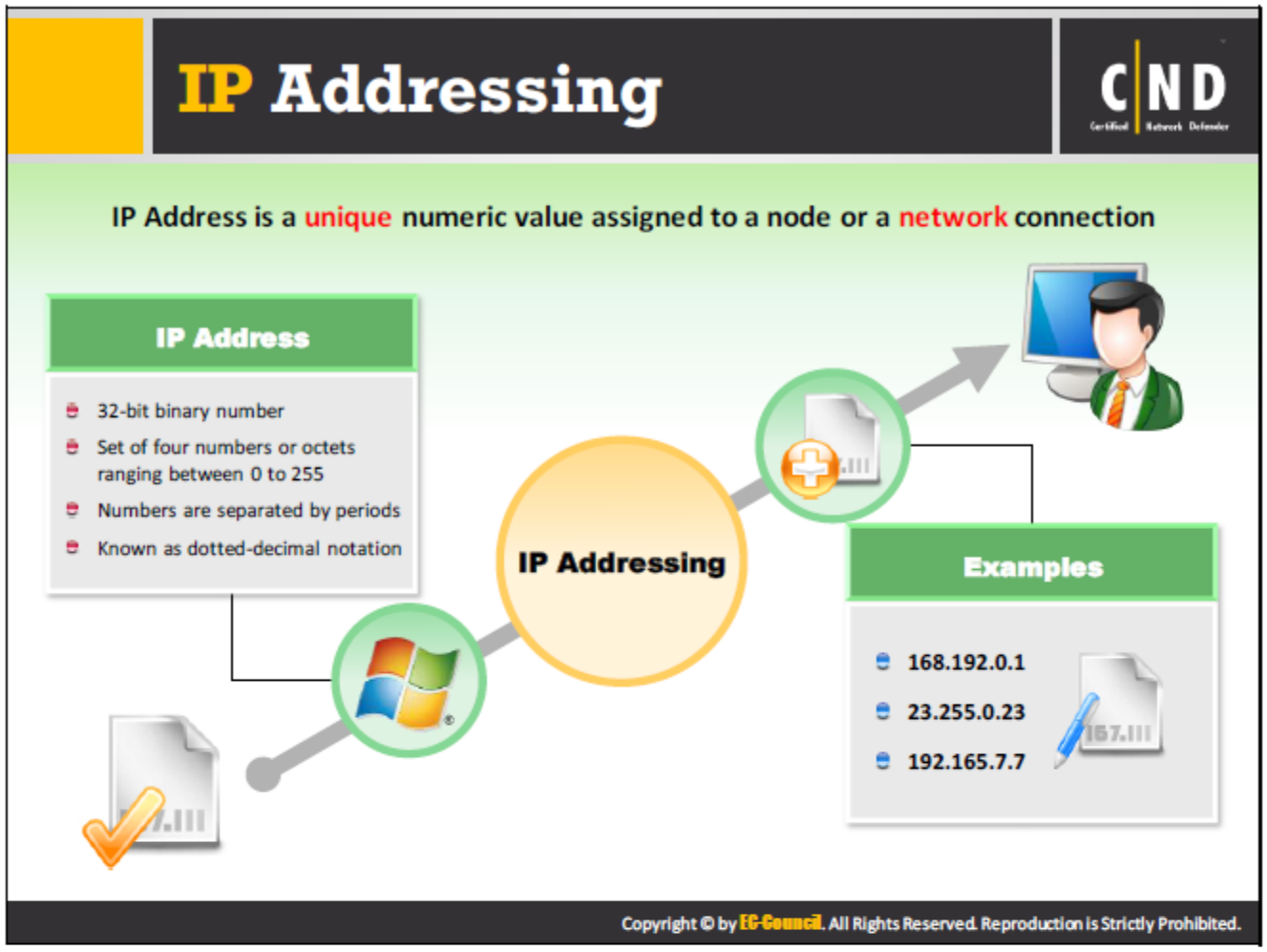
- Pass the empty frames across the network.
- The computers ready to send information to any other computer can insert a token into the frame including the data and the destination identifier.
- Inserting a token to a frame changes the token bit from 0 to 1 in the frame.
- Each computer checks with the frame and examines whether the destination address matches. If it does, then that computer simply copies the message and changes the token bit to 0.
- The frame deletes the information after computer with the destination address copies the information.

- The frame passes through the network as empty frame and is now ready to accept another data.

The components of a token ring frame are as follows:

Frame Field	Description
Start delimiter	Represents the start of the frame
Access control	Represents the priority of the frame and checks if it is a token or a data frame
Frame control	Includes Mac access control information for all the computers and end station information for only one computer
Destination address	Specifies the destination address
Source address	Specifies the address of the computer that sends the frame
Information or data	Contains the information to be sent
Frame check sequence	Includes the CRC error-checking
End delimiter	Specifies the end of the frame
Frame status	Includes the current status like if information copied etc.

TABLE 1.3: Components of token ring



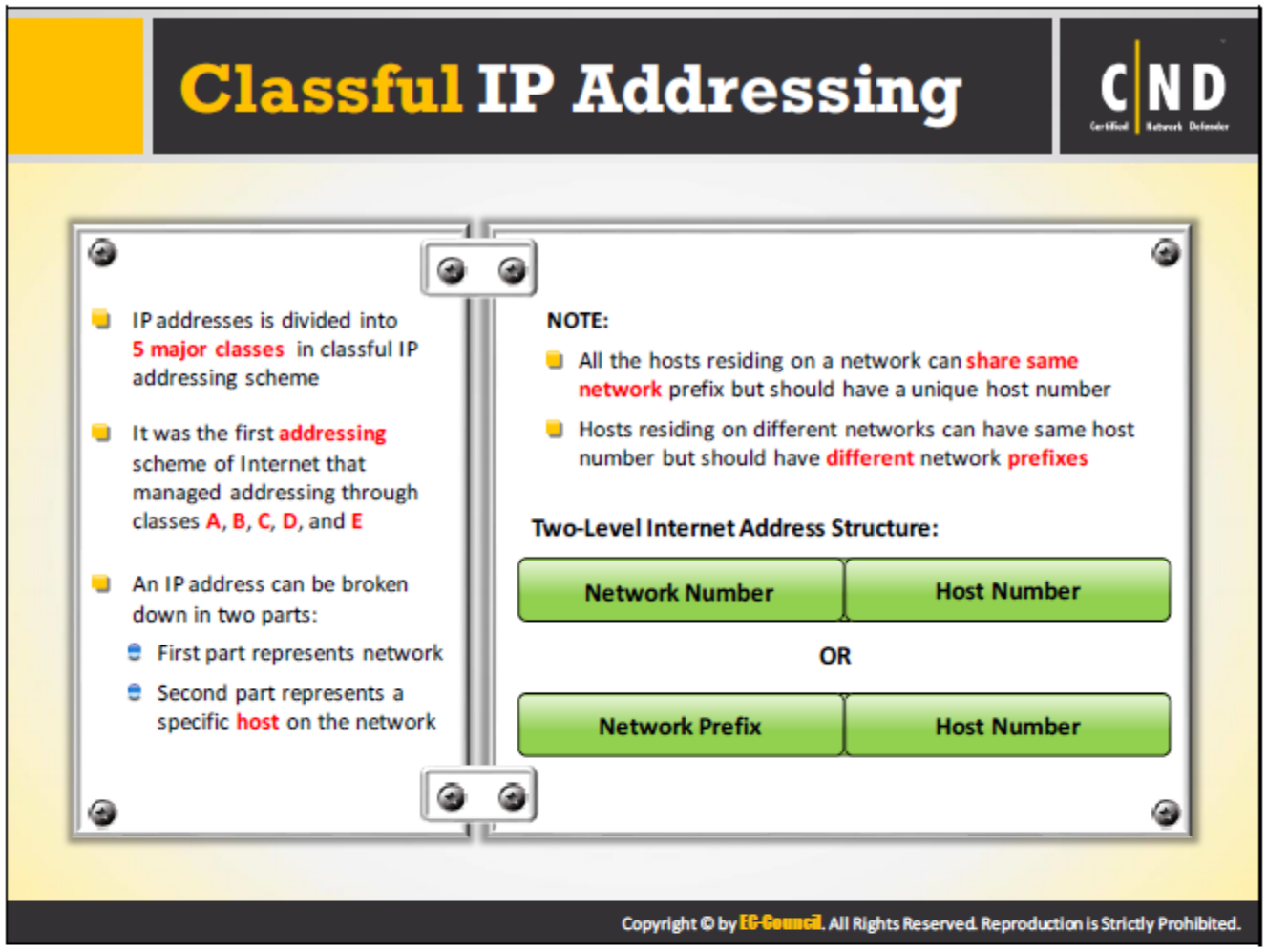
IP address refers to a number assigned to the computers transmitting data over the network and uses internet protocol for data transmission. The IP addresses consist of the following: host identification and location addressing. The assigned addresses make it easier to identify the computers in the network. The address normally consists of 32 binary bits divided into two parts: host part and the network part. The format of an IP address consists of the 32 bit numeric address written as four numbers separated by periods. Each number can range from 0 to 255. An example of an IP address is as follows: 1.160.10.240. The IP address can be either static or dynamic. The static IP address does not change and is permanent. The dynamic IP address changes every time a computer accesses the internet.

Important terms in IP addressing

- **Default Network:** In the default network, the default IP address is 0.0.0.0.
- **Loopback Address:** Loopback address is a unique IP address (127.0.0.1) designed for network testing where a network administrator sends packets to the device to identify problems during transmission.
- **Broadcast Address:** Broadcast address is a unique IP address (255.255.255.255) designed for sending messages to all the nodes in a network. A network administrator uses this address to send a common message to all the hosts residing in a network.
- **Internet Corporation for Assigned Names and Numbers (ICANN):** The Internet Corporation for Assigned Names and Numbers (ICANN) is the authority that manages the assignment of IP addresses, IP address spaces, and Protocol Identifier Assignments. The

aim of ICANN is to ensure that all the users have valid addresses. ICANN does not look after Internet content control, data protection, or unsolicited mail, but ICANN is responsible for the management of the new gTLDS (generic Top Level Domains).

- **Making the Address Space Friendly:** In order to make the address space friendly, it is necessary to make the address familiar and short. The information in the Internet includes of only two symbols: "1" and "0". These describe the two possible states: On/Off. The base10 number system is user-friendly. Imagine that a computer's address is 4,27,28,123,12. It is easier to remember the binary equivalent of that address in the Base2 system: 10010000, 11111010, 01010101, and 10111011.
- **Purpose of Dots:** It can be difficult to remember a particular decimal number address. To make it easier to remember, the decimal divides it into four parts. With the logical classification of the address, it is easier to identify a particular host on the network. The scheme depends on the decimal number and the address space used is binary. Certain schemes use the binary numbers, whereas others use the decimal numbers directly. Therefore, the 32-bit address space has four equal components of 8 bits each, such as 202.53.13.138.



Classful IP addressing is the Internet's first addressing scheme that managed addressing through classes, primarily A, B, and C. First standardized in September 1981, the Internet protocol (IP) specifies that each computer should have a unique, 32-bit address number to use the IP-based internet. Systems connected to more than one network interface would require a unique IP address for each network. Classful addressing divides the IP address into two parts. The first part identifies the network on which the host resides and the second part identifies the specific node or host on a network. Classes of an address determine parts belonging to the network address and parts belonging to the node address.

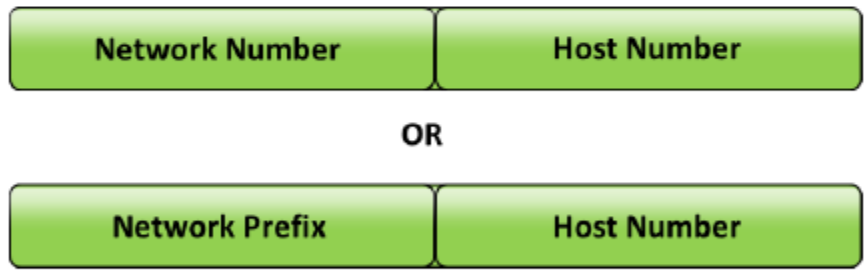


FIGURE 1.23: Two-Level Internet address structure

From the past few years, network number segment refers network prefix because the major part of each IP address determines the network number. All the hosts residing on a network can share the same network prefix, but should have a unique host number. Hosts residing on different networks can have a same host number, but should have different network prefixes.

Address Classes

Class A
- Has an **8-bit** network prefix
- Starts with binary **address 0**, decimal number can be anywhere between **1-126**
- First 8 bits (one octet) identify the network, remaining **24 bits** specify hosts residing in the network

Class B
- Has a **16-bit** network prefix
- Starts with binary **address 10**, decimal number can be anywhere between **128-191**
- First 16 bits (two octets) identify the network, remaining **16 bits** specify hosts residing in the network

Class C
- Has a **24-bit** network prefix
- Starts with binary **address 110**, decimal number can be anywhere between **192-223**
- First 24 bits (three octets) identify the network, remaining **8 bits** specify hosts residing in the network

Class D
- Starts with binary **address 1110**, decimal number can be anywhere between 224-239
- Supports multicasting

Class E
- Starts with binary **address 1111**, decimal number can be anywhere between 240-255
- Reserved for experimental use

Address Classes (Cont'd)

Table showing number of Networks and Hosts:

Class	Leading Bits	Size of Network Number Bit Field	Size of Host Number Bit Field	Number of Networks	Addresses Per Network
Class A	0	7	24	126	16,277,214
Class B	10	14	16	16,384	65,534
Class C	110	21	8	2,097,152	254
Class D (Multi cast)	1110	20	8	1,048,576	254
Class E (Reserved)	1111	20	8	1,048,576	254

IP Address Classes and class characteristics and uses

IP Address Class	Fraction of Total IP Address Space	Number of Network ID Bits	Number of Host ID Bits	Intended Use
Class A	1/2	8	24	Used for Unicast addressing for very large size organizations
Class B	1/4	16	16	Used for Unicast addressing for medium or large size organizations
Class C	1/8	24	8	Used for Unicast addressing for small size organizations
Class D	1/16	N/A	N/A	Used for IP multicasting
Class E	1/16	N/A	N/A	Reserved

Address classes play an important role in Internet routing. Internet designers have divided the IP address space into different address classes to provide support for network requirements and size such as class A, class B, class C, class D and class E.

Class A

IP address class defines IP address for large networks. The binary address starts with 0. The decimal number is in between 0-127 and mostly used by international companies. From the 32-bit address, the Class A address uses the leftmost 8-bits for identifying networks. The first 8 bits identify the network and the remaining 24 bits specify hosts residing in the network. In the recent years, class A networks are referred as "/8's" or "8's". Total of 126 (27-2)/8 networks can be defined in Class A network. Two classes are less because in the "class A" network as mentioned 0.0.0.0 is the default IP address and 127.0.0.0 is a loopback address. This network supports a maximum of 16,777,214 networks in a host and 231 (2,147,483,648) individual addresses. It contains 232 (4,294,967,296) addresses of IPv4 address space, which amounts to 50% of the total IPv4 unicast address space.

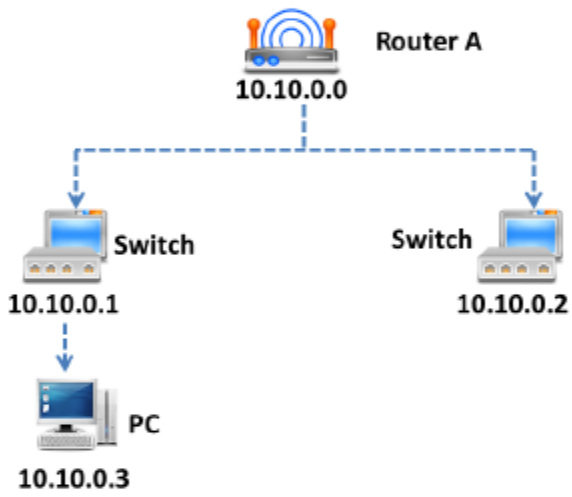


FIGURE 1.24: Class A network

Class B

Use class B addresses in medium-scale networks. It uses the leftmost 16-bits of this class and the binary address starts with 10. The decimal number is from 128 to 191. The first 16 bits (two octets) identify the network and the remaining 16 bits specify the hosts residing in the network.

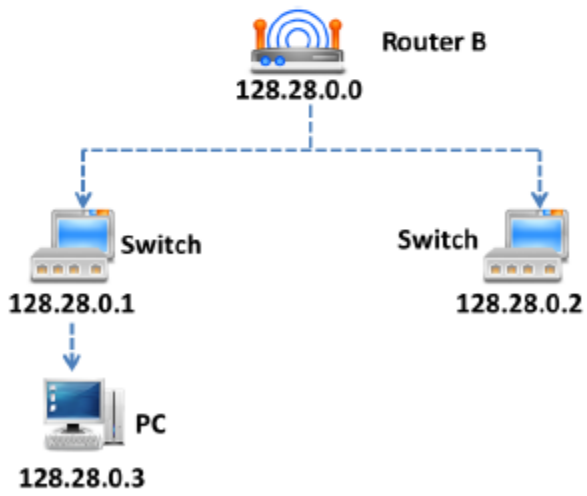


FIGURE 1.25: Class B network

In the recent years, class B networks are referred as "/16s" as they have 16 bits network prefix. About 16,384 (214) /16 networks can be defined in class B network where 65,534 (216-2) hosts are created per network and 230 (1,073,741,824) individual addresses. When calculated this amounts to 25% of the total IPv4 unicast address space.

Class C

Class C addresses have a 24-bit network prefix. The binary address of Class C starts from 110. The decimal number can be anywhere between 192 and 223. Class C addresses represent small businesses. It uses the first 24 bits (three octets) for identifying the network, while the rest of the 8 bits help in identification of the host on the network.

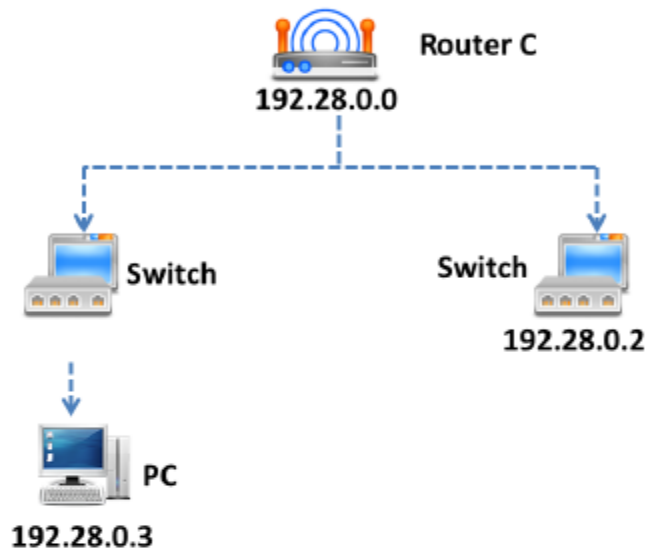
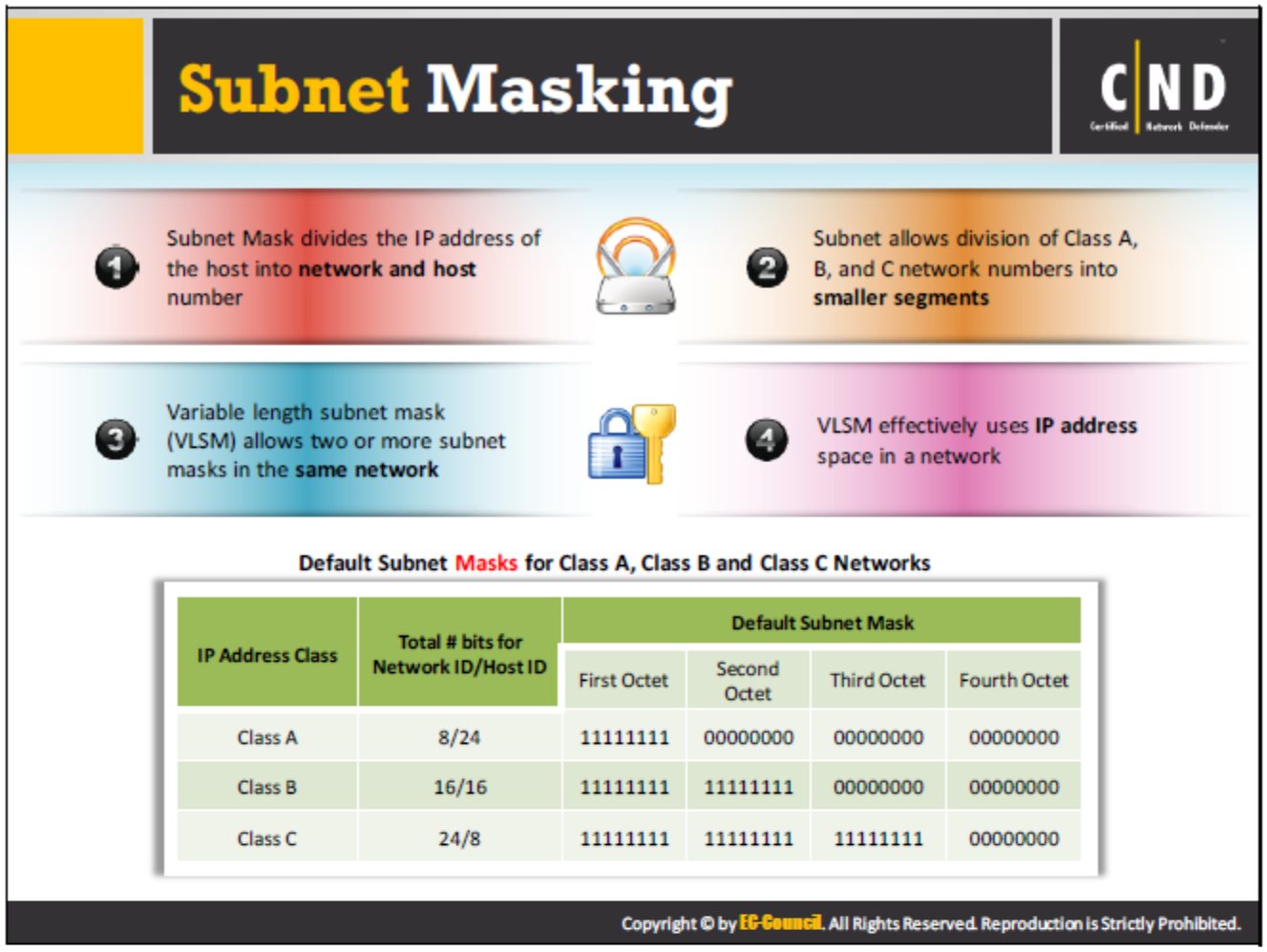


FIGURE 1.26: Class C network

Class D and Class E

In addition to the primary address classes, there are two other classes defined by the internet designers such as class D and class E. These are special classes designed for specific purposes where users do not even know they exist. Class D starts with binary address 1-1-1-0 and its decimal number can be anywhere from 224 to 239. Its main function is to support multicasting.

Class E starts with binary address 1-1-1-1, and its decimal number can be anywhere from 240 to 255. It serves experimental purposes.



Subnet mask provides information about the division of bits between subnet ID and host ID as well as the host ID containing the routing traffic. It is a 32-bit binary number. Subnet mask separates the IP address into two components, namely network address and host address. Use subnet calculator to retrieve the subnet mask information. The Subnet mask performs bitwise AND operation on the netmask to identify the network address of a particular IP address. Subnet mask bits was defined by setting network bits to all "1"s and setting host bits to all "0"s. Subnet masks are expressed using dot-decimal notation like an address.

Every host on the TCP/IP network requires a Subnet mask. Use a default subnet mask for the class based network ID's and use custom subnet masks when subnetting and supernetting is configured.

IP Address Class	Total # bits for Network ID/Host ID	Default Subnet Mask			
		First Octet	Second Octet	Third Octet	Fourth Octet
Class A	8/24	11111111	00000000	00000000	00000000
Class B	16/16	11111111	11111111	00000000	00000000
Class C	24/8	11111111	11111111	11111111	00000000

TABLE 1.4: Default subnet masks for Class A, Class B and Class C networks

Host IP address: 159.100.9.18

Binary format: 10011111.01100100.00001001.00010010

Class B network mask: 255.255.0.0

Binary format: 11111111.11111111.00000000.00000000

Class B address with 5 bits allocated to subnet ID and remaining 11 left for host ID

Subnet mask = /21

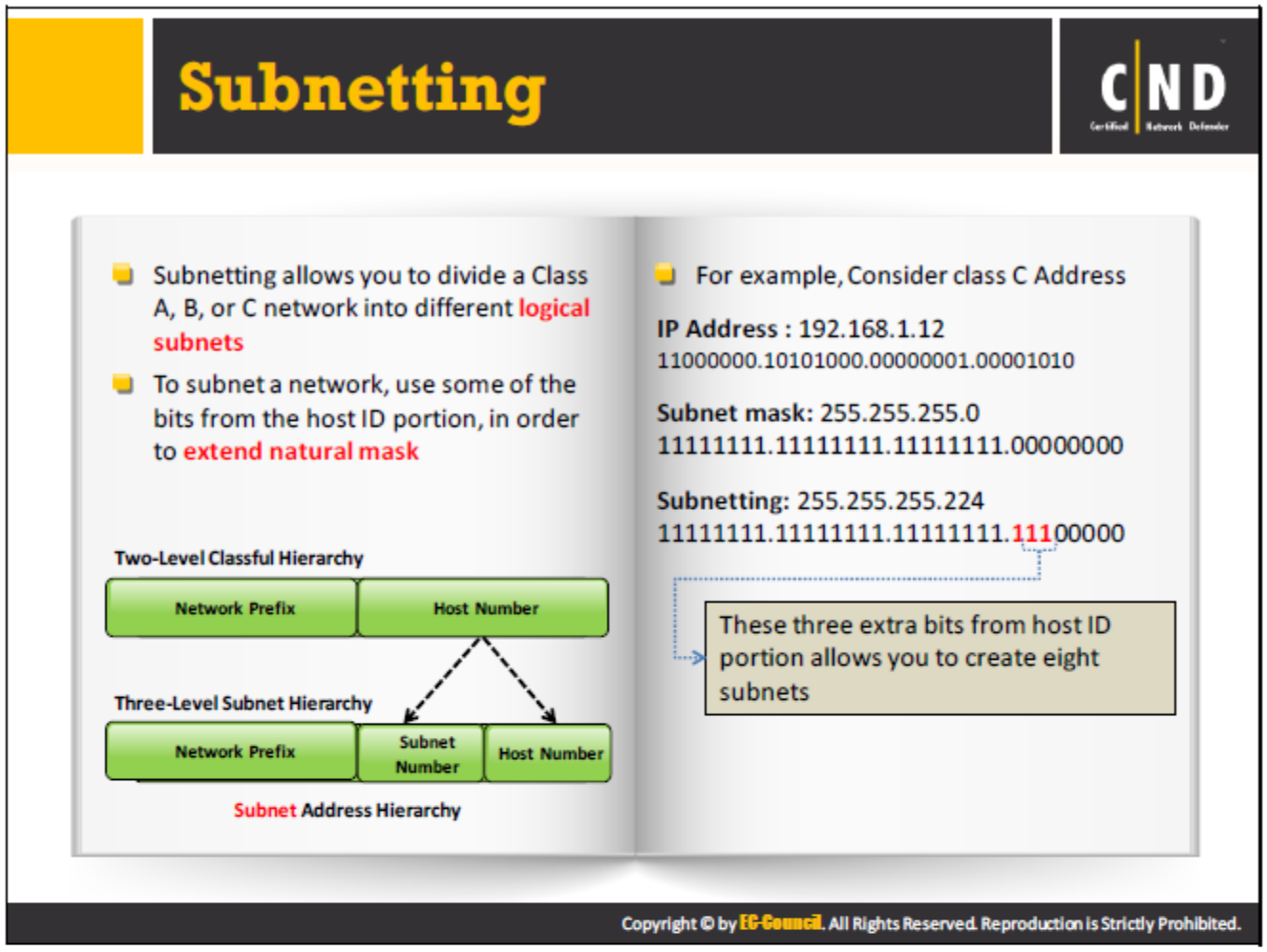
Prefix length notation: 11111111.11111111.11111000.00000000

Subnet mask in dot decimal notation: 255.255.248.0

Network ID = 159.100.0.0

Binary format: 10011111.01100100.00001000.00000000

Extended network address (net ID + subnet ID) = 159.100.8.0/21



The traditional internet designers have not foreseen the rapid growth of the internet and the change it has brought in as a communication system. Today, organizations are facing many problems with allocation of IP addresses, as the IP address space, especially IPv4 as it is in the depletion stage. This problem has occurred due to early decisions made by the internet designers in the formative stage. In the early evolution stage of internet, organizations were allocated address space based on their request rather than on their requirements. This has led to eventual depletion of IP address space. Many organizations that predicted the future of networking had invested in the internet, but organizations, which ignored the significance of the internet, later realized and obtained addresses but had to face problems with address shortage issues. Emerging organizations that are in the evolving stage have to face address storage problems due to premature depletion of IPv4 address space.

In order to overcome the problems of IP address space depletion, one can perform IP subnetting. Subnetting allows organization's network divided into two level structure, hosts and subnets. An organization's system administrator divides the host network, specifically the internal network, into two segments in order to make it unavailable to the external networks. The main advantage of subnetting to the organization is that they can divide the classful host number into a subnet id and host id based on their preferences and requirements.

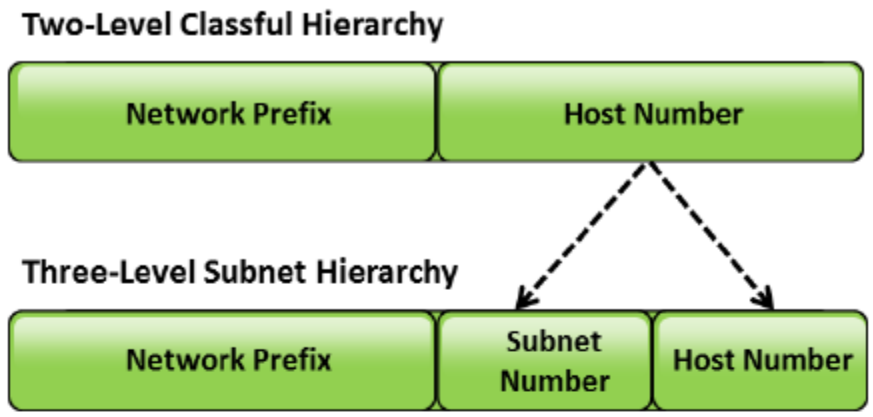


FIGURE 1.27: Subnet address hierarchy

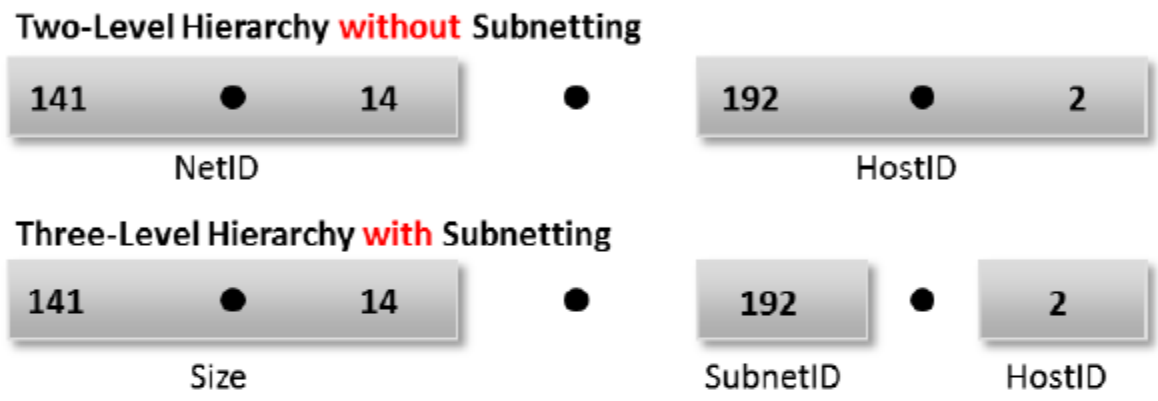


FIGURE 1.28: Two-level and Three-level subnetting

- Net address: 141.14.0.0
- Subnet address: 141.14.192.0
- Host address: 141.14.192.2

Routers use an extended network prefix to transmit the traffic between subnet devices. Extended network prefixes include the network prefix number and subnet ID.

In classful IP addressing, the router uses the first octet of an IP address to determine the address class, related network number and host number. In subnetting, as the division of address is arbitrary in nature, it becomes difficult for the router to determine the process of dividing it into subnet and host ID. Subnet mask provides information about the division of bits between subnet ID and host ID as well as the host ID containing the routing traffic. It is a 32-bit binary number.

Subnetting allows the division of Class A, B, and C network numbers into smaller segments. Variable length subnet mask (VLSM) allows two or more subnet masks in the same network. VLSM effectively uses IP address space in a network. VLSM provides flexibility to a network administrator to divide a network as per the requirement and preference of the organization and create subnets, sub-subnets and sub-sub-subnets.

FIGURE 1.29: Example of subnetting

Class B address = /16 network prefix

Network address = 131.175.0.0

Natural mask = 255.255.0.0

Subnetted with /24 network prefix

Subnet ID = third number in dotted notation

131.175.21.0

Supernetting

Class A and B addresses are in depletion stage

Supernetting combines various Class C addresses and creates a super network

Also known as Classless Inter-Domain Routing (CIDR), invented to keep IP addresses from exhaustion

Class C provides only 256 hosts in a network out of which 254 are available for use

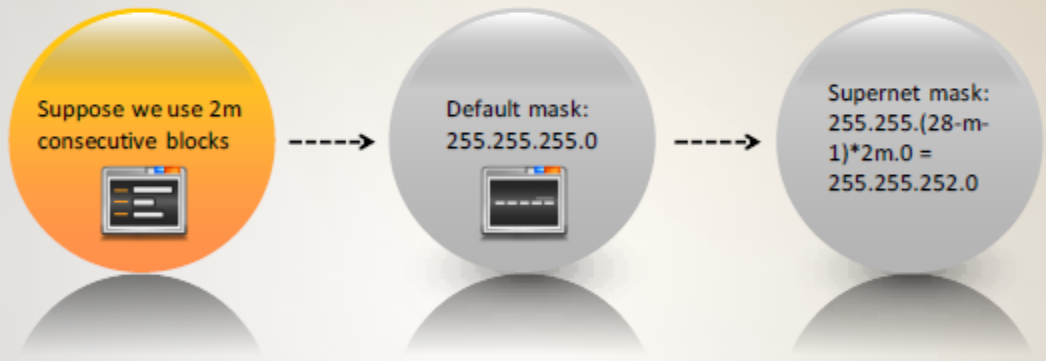
It applies to Class C addresses

Supernet mask is reverse of subnet mask

Subnet Mask	11111111 11111111 11111111 111 00000
Default Mask	11111111 11111111 11111111 000 00000
Supernet Mask	11111111 11111111 11111000 000 00000

Supernetting (Cont'd)

Supernetting Class C Example:



Class C address: ← Net ID →

With the growth of internet, classful addressing is a big problem for many organizations. Problems with classful addressing are a lack of flexibility in dividing addresses for an internal network, improper distribution of allocated address space that requires a router to create more and more routing table entries. Subnetting solves these problems to a certain extent, but IPv6 addressing brought 128-bit addressing system to eliminate addressing issues appropriately. This new system eliminates the need for address classes and creates a new addressing scheme to match the growing demand of internet users. This system advocates on creating a new classless addressing scheme known as Classless Inter-Domain Routing (CIDR). This system uses a concept of subnetting as a base and takes it a step further. Subnetting divides a single network into subnets whereas CIDR applies the subnetting principle to large networks. It aggregates networks into larger supernets with a concept known as supernetting.

- **Advantages of CIDR:**

  With CIDR, organizations can allocate address space efficiently as per their requirement and preference. In classful addressing, there are class A, B, and C networks. Class A network has around 16,277,214 addresses per network, class B network has 65,534 and class C has only 254 addresses. There is disproportion of address classes in this addressing system. CIDR eliminates the problem with class imbalances and routing entries by creating small entries for large networks.

  Network prefixes based on CIDR helps the router in determining the dividing point between net ID and host ID. Subnetting requires a subnet mask to determine the network ID and host ID. CIDR does not support a 32-bit binary subnet mask. Instead, CIDR uses "/" slash notation known as CIDR notation along with prefix length to show the network size.

Subnet Mask	11111111 11111111 11111111 **111** 00000
Default Mask	11111111 11111111 11111111 000 00000
Supernet Mask	11111111 11111111 11111**000** 000 00000

FIGURE 1.30: Supernetting

- **Supernetting Example:**

  Example showing a 4 Class C addresses in a network appear as a single network from outside

  4 address-contiguous networks:

  213.2.96.0: 11010101.00000010.01100000.00000000

  213.2.97.0: 11010101.00000010.01100001.00000000

  213.2.98.0: 11010101.00000010.01100010.00000000

  213.2.99.0: 11010101.00000010.01100011.00000000

Supernetmask: 255.255.252.0

Supernetaddress: 213.2.96.0/22

11010101.00000010.01100000.00000000

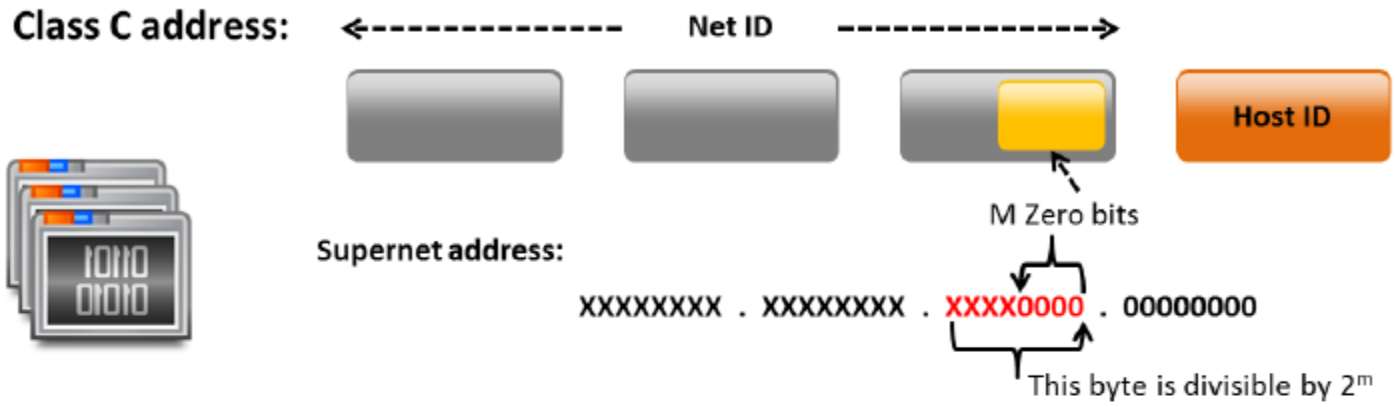
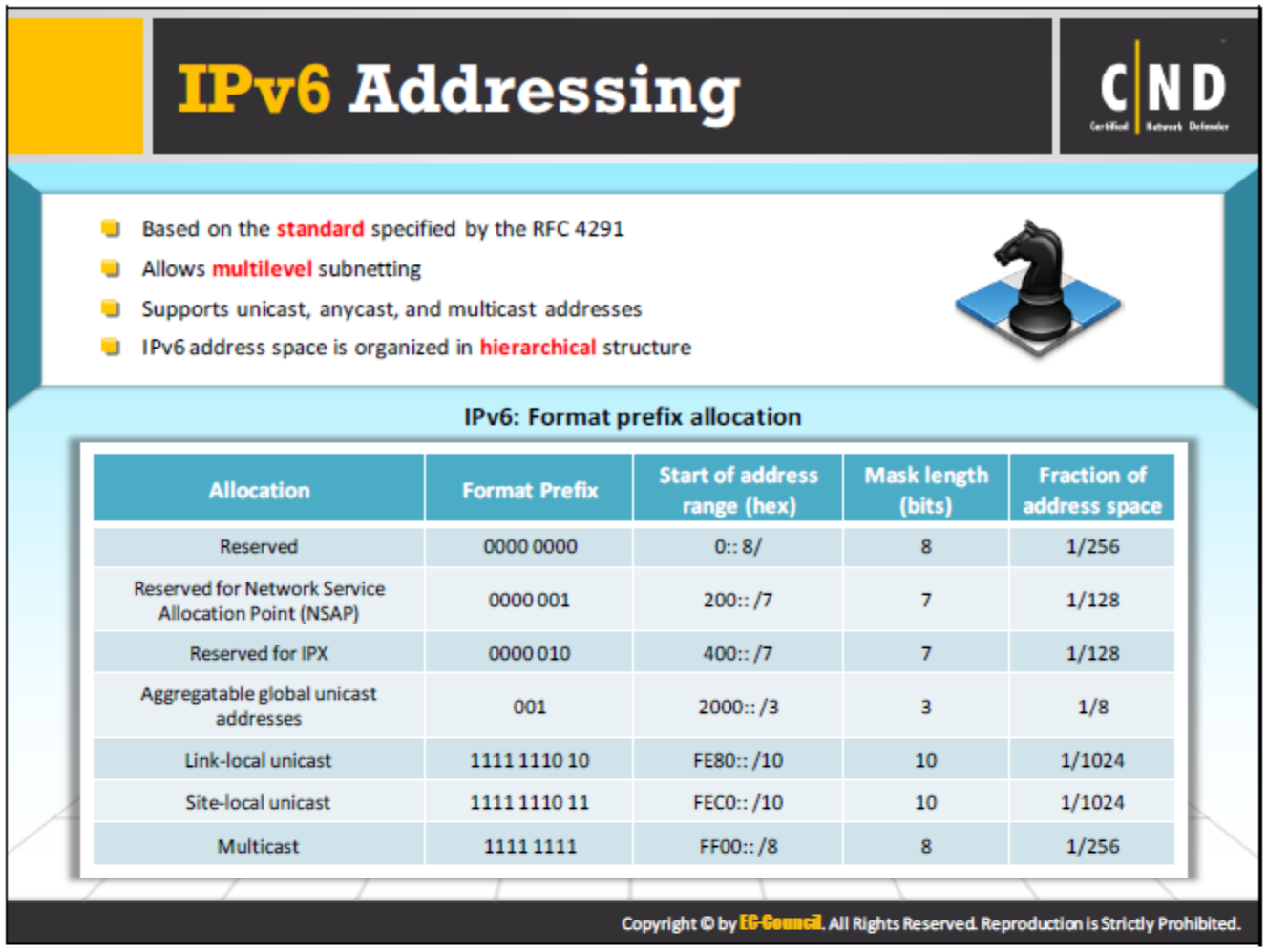


FIGURE 1.31: Supernetting with Class C address



IPv6 is capable of providing a large address space of 128 bits for increasing demands of internet users. It has a new format for packet header to minimize problems with overhead routing entries. IPv6 has globally identified unique addresses with efficient, hierarchal and routing infrastructure that relies on prefix length rather than address classes. This allows the backbone routers to create small routing tables. IPv6 simplifies host configuration with stateless and stateful address configuration for network interfaces. In IPv6, hosts on a link are capable of automatically configuring themselves with a link called link-local addresses by responding to the prefixes mentioned by the local routers. The host sends a link local address request to a local router for connecting to that network, which then responds to the request by sending its configuration parameters. This lets the host configure automatically with the available router. IPv6 is capable of configuring itself, even though there are no routers. IPv6 supports unicast and multicast communication along with a new communication type called anycast.

- **Unicast Address:** It is used to identify a single node in the network. The four different categories of Unicast address are:
  - **Global unicast addresses** is globally unique in the internet.
  - **Link-local addresses** not meant for routing, but confined to a single network segment.
  - **Unique local addresses**. These assist in private addressing and also avoids the chances of collision between two subnets.

- **Anycast Address:** In anycast communication method, only specific associated address in a network receives the messages. IPv6 provides better support for quality of service (QoS) with proper management of network traffic.
- **Multicast Address:** IPv6 packets sent to a multicast address identifies the group of interfaces, usually on different nodes. Only those hosts which are members of the multi-cast group can receive the multi-cast packets. The IPv6 multicast is a routable address and the routers forward these multicast packets to all the members of the multicast groups.

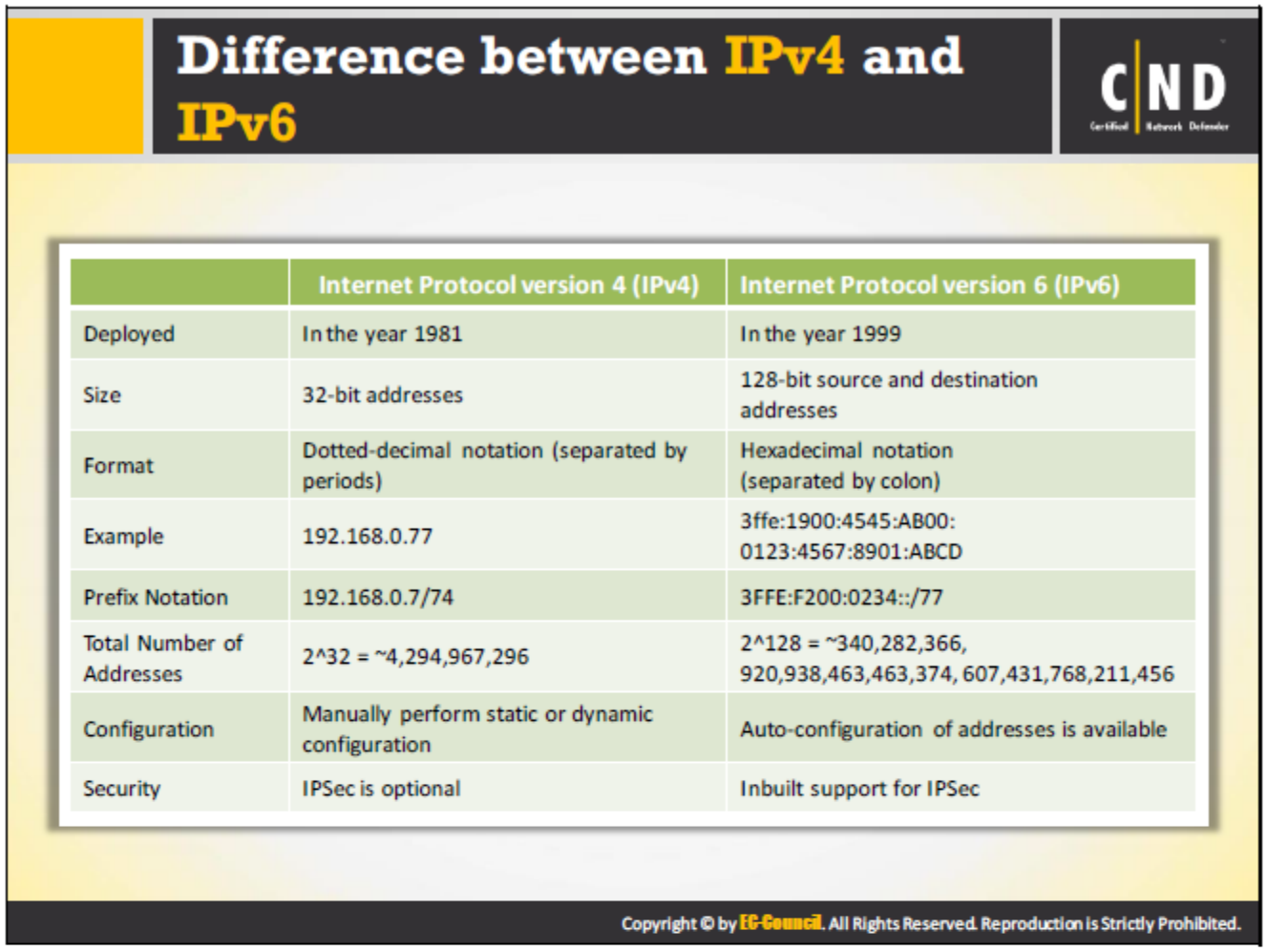
Allocation	Format Prefix	Start of address range (hex)	Mask length (bits)	Fraction of address space
Reserved	0000 0000	0:: 8/	8	1/256
Reserved for Network Service Allocation Point (NSAP)	0000 001	200:: /7	7	1/128
Reserved for IPX	0000 010	400:: /7	7	1/128
Aggregatable global unicast addresses	001	2000:: /3	3	1/8
Link-local unicast	1111 1110 10	FE80:: /10	10	1/1024
Site-local unicast	1111 1110 11	FEC0:: /10	10	1/1024
Multicast	1111 1111	FF00:: /8	8	1/256

TABLE 1.5: IPv6 format prefix allocation

The IPv6 notation includes eight groups of hexadecimal quartets separated by colons. An example for IPv6 is: 2001:cdba:0000:0000:0000:0000:3257:9652. The groups of zeroes in IPv6 address may be reduced to zero or removed. For example:

- 2001:cdba:0000:0000:0000:0000:3257:9652
- 2001:cdba:0:0:0:0:3257:9652
- 2001:cdba::3257:9652

The IPv6 addresses use Classless Inter Domain Routing (CIDR) notation. The subnet using the IPv6 protocol consists of a group of IPv6 addresses having the size value in the power of two. The initial bits in the IPv6 address forms the network prefix. The bits in the network prefix uses a forward slash ('/'). For example: 2001:cdba:9abc:5678::/64 represents the address 2001:cdba:9abc:5678.



Internet Protocol Version 4 (IPv4)

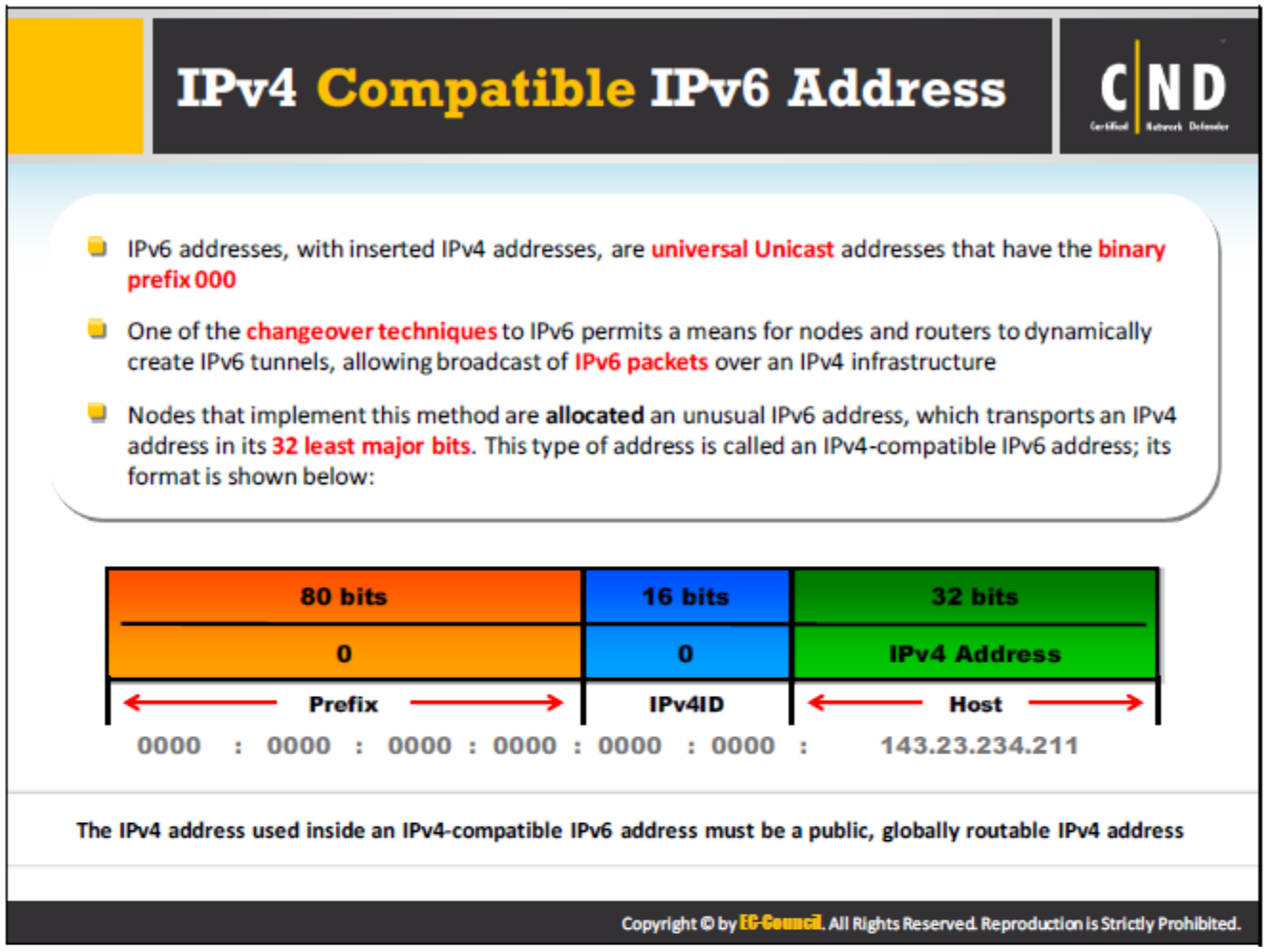
The fourth version of the internet protocol that identifies devices on a network through the technique of addressing. IPv4 mainly works in the packet-switched link layer networks. It uses a 32-bit address scheme, thereby permitting 2^32 addresses. The sender and the forwarding routers perform the fragmentation. There is no method to identify the method of packet flow. Checksum fields and option fields are available in IPv4. The IPv4 address uses IGMP to manage multicast. It is possible to broadcast messages. Configuration of IPv4 requires either manual configuration of IPv4 addresses or DHCP configuration.

Internet Protocol Version 6 (IPv6)

Also known as IPng (Internet Protocol Next Generation) is the advanced version of IPv4 and replaces IPv4. The IPv6 protocol allows better handling of hosts and data flowing on the internet. The main advantage of using IPv6 is that it reduces the exhaustion of IP addresses. The IPv6 addresses are 128-bit long and represented using hexadecimal. The sender performs the fragmentation part. The flow label field in the packet header of the IPv6 address format assists in identifying the flow of the packet. The Ipv6 address headers do not consist of any checksum or options field. The IPv6 consists of an auto-configuration mode that eliminates the need for manual configuration as in IPv4.

Advantages of IPv6 over IPv4:

- IPv6 provides a simplified method for the router task when compared with IPv4.
- IPv6 is more reliable to use than IPv4 and IPv6 can handle more payloads.
- IPv6 is more compatible for use in mobile networks than IPv4.



IPv4 compatible addresses obtained from IPv4 public addresses allow connecting IPv6 hosts over the IPv4 internet infrastructure. The IPv6 address encapsulates within the IPv4 header that eliminates the use or addition of IPv6 routers.

The IPv4 compatible IPv6 allows the IPv6 devices to insert IPv4 addresses in the IPv6 address through the IPv4 connected network. The IPv4 compatible IPv6 has a different address format with the first 96 bits set to all zeroes, followed by a dotted decimal IPv4 address.

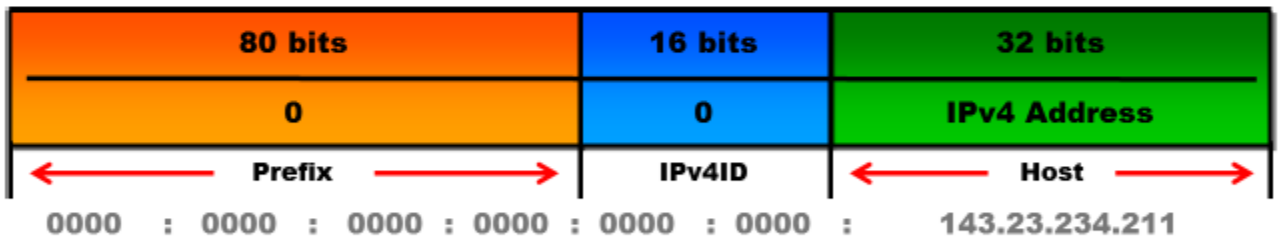
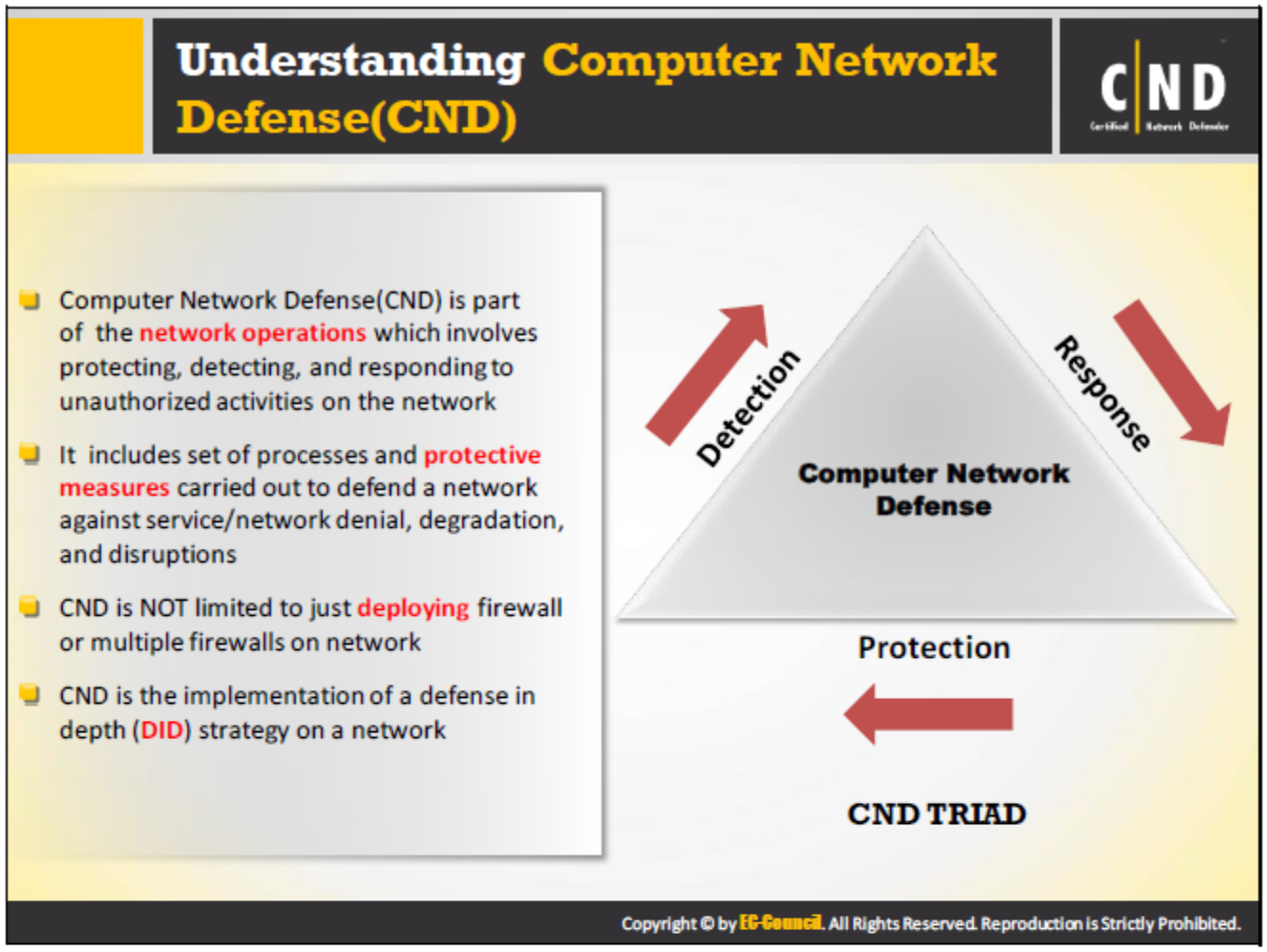


FIGURE 1.32: IPv4 address

They can be written as 0:0:0:0:0:0:A.B.C.D or ::A.B.C.D, where "A.B.C.D" represents the embedded IPv4 address.

The host or router at each end of an IPv4-compatible tunnel must support both the IPv4 and IPv6 protocol stacks. IPv4-compatible tunnels must configure between border-routers or between a border-router and a host. Using IPv4-compatible tunnels is an easy method to create tunnels for IPv6 over IPv4, but the technique does not scale for large networks.

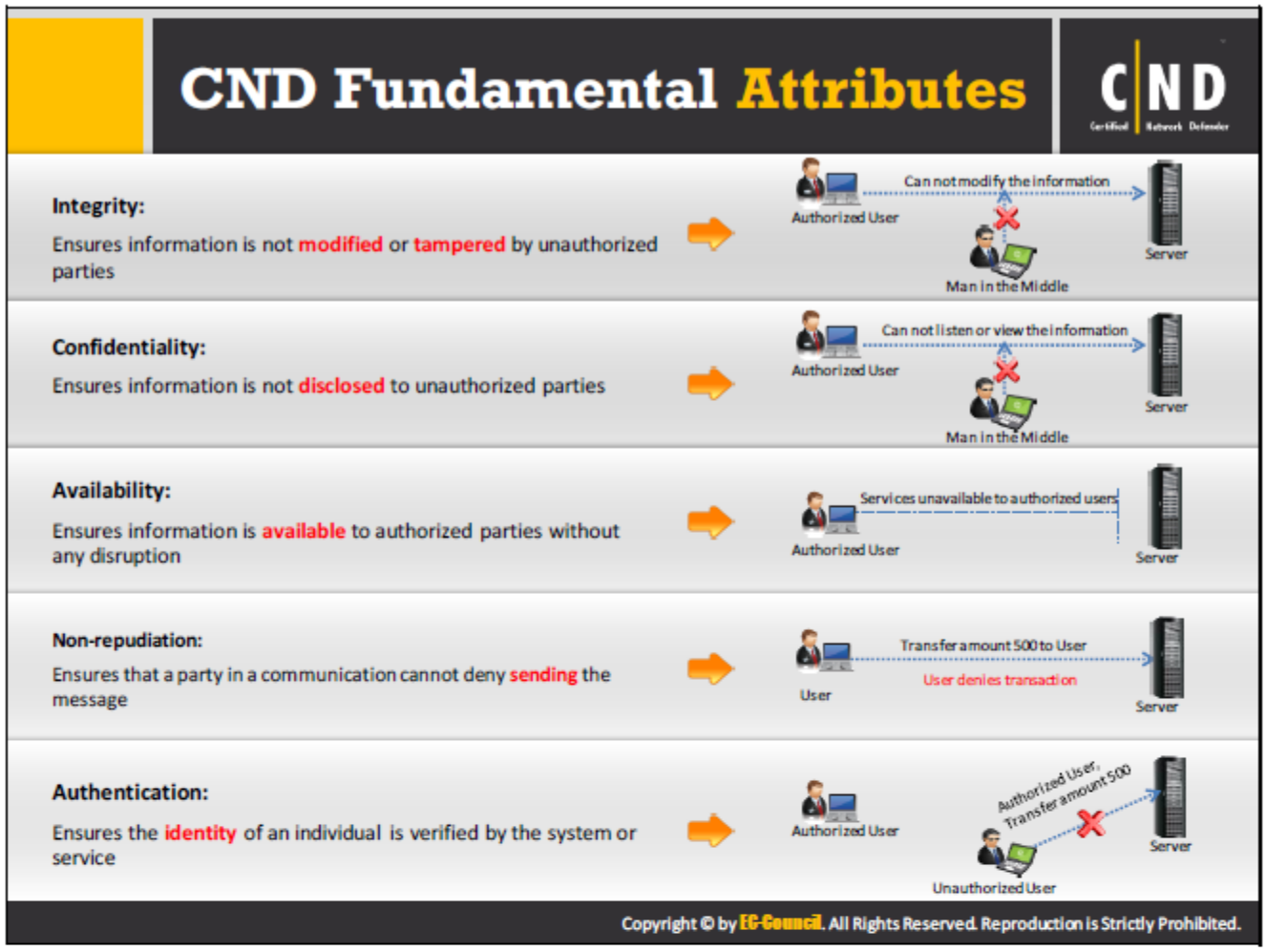


Computer network defense (CND) involves protecting, monitoring, analyzing, detecting and responding to unauthorized activities on the network and confirms the overall (Defense-in-depth) security of the network. Different types of unauthorized or illegal activities may include interrupting, damaging, exploiting or restricting access to networks or computing resources and stealing data and information from them.

Most of the organization considers network defense as involving the implementation of security measures which protect their network from attacks. Deploying a firewall or multiple firewalls on the network is enough to protect their infrastructure from a variety of threats. However, it alone does not ensure network defense. Even though firewalls are considered one of the security measures, it does not ensure defense in depth network security.

CND enables network administrators to defend and act against network attacks performed by malicious or adversarial computer systems or networks.

CND is part of Computer Network Operations (CNO) which deals with the overall network security achieved through detection, prevention, analysis, and response to various network attacks.

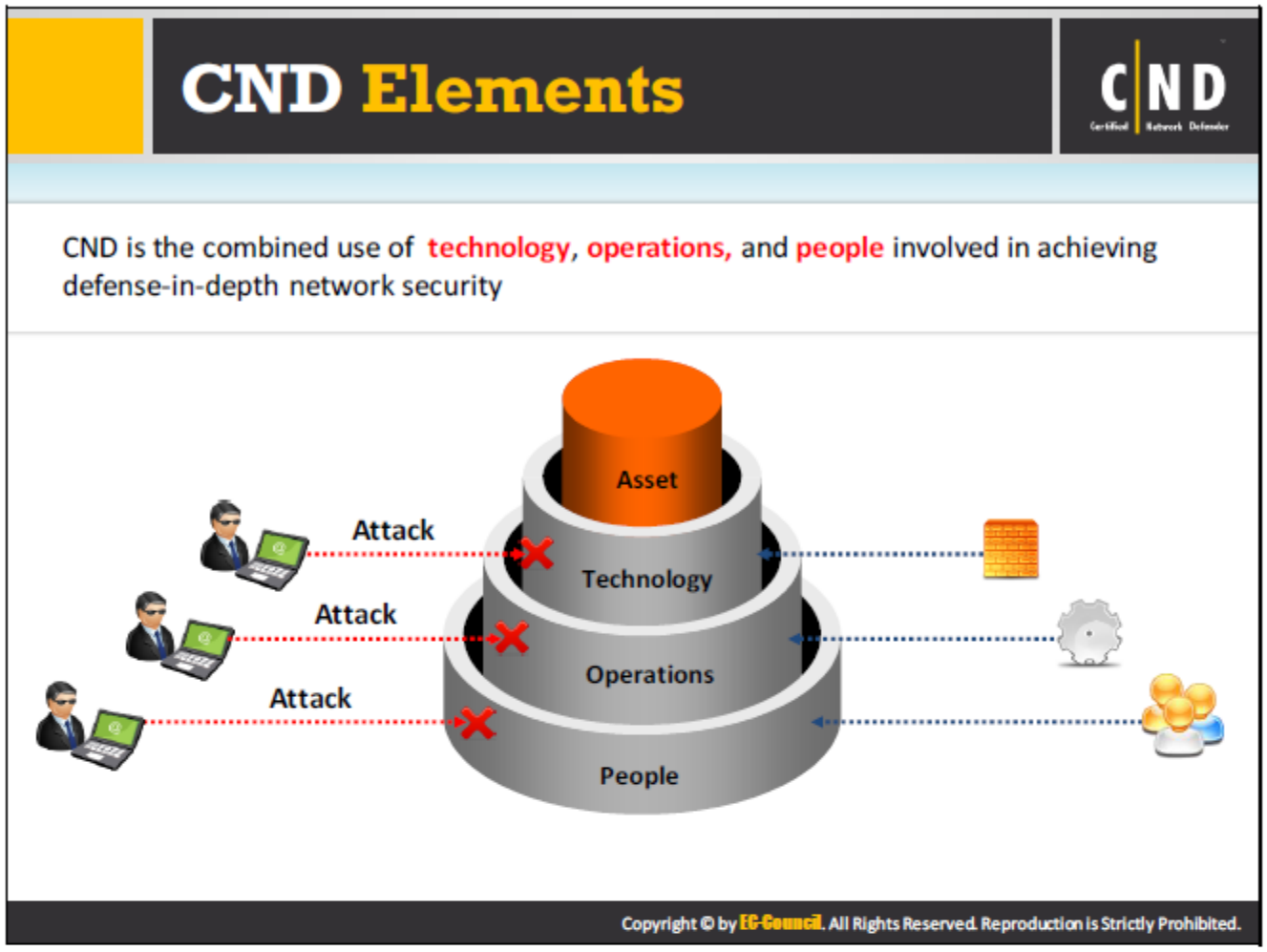


CND employs an Information Assurance (IA) principle which enforces taking appropriate countermeasures and response actions upon the threat alert or detection. Network operators should consider information assurance principles to evaluate if the data is sensitive or not, and to handle the situations when security implications occur on the network. This assists them in identifying network security vulnerabilities, monitoring the network of any intrusion attempts, or malicious activity, and defending the network by mitigating vulnerabilities.

CND should address the following Information Assurance (IA) principles to achieve a defense-in-depth network security

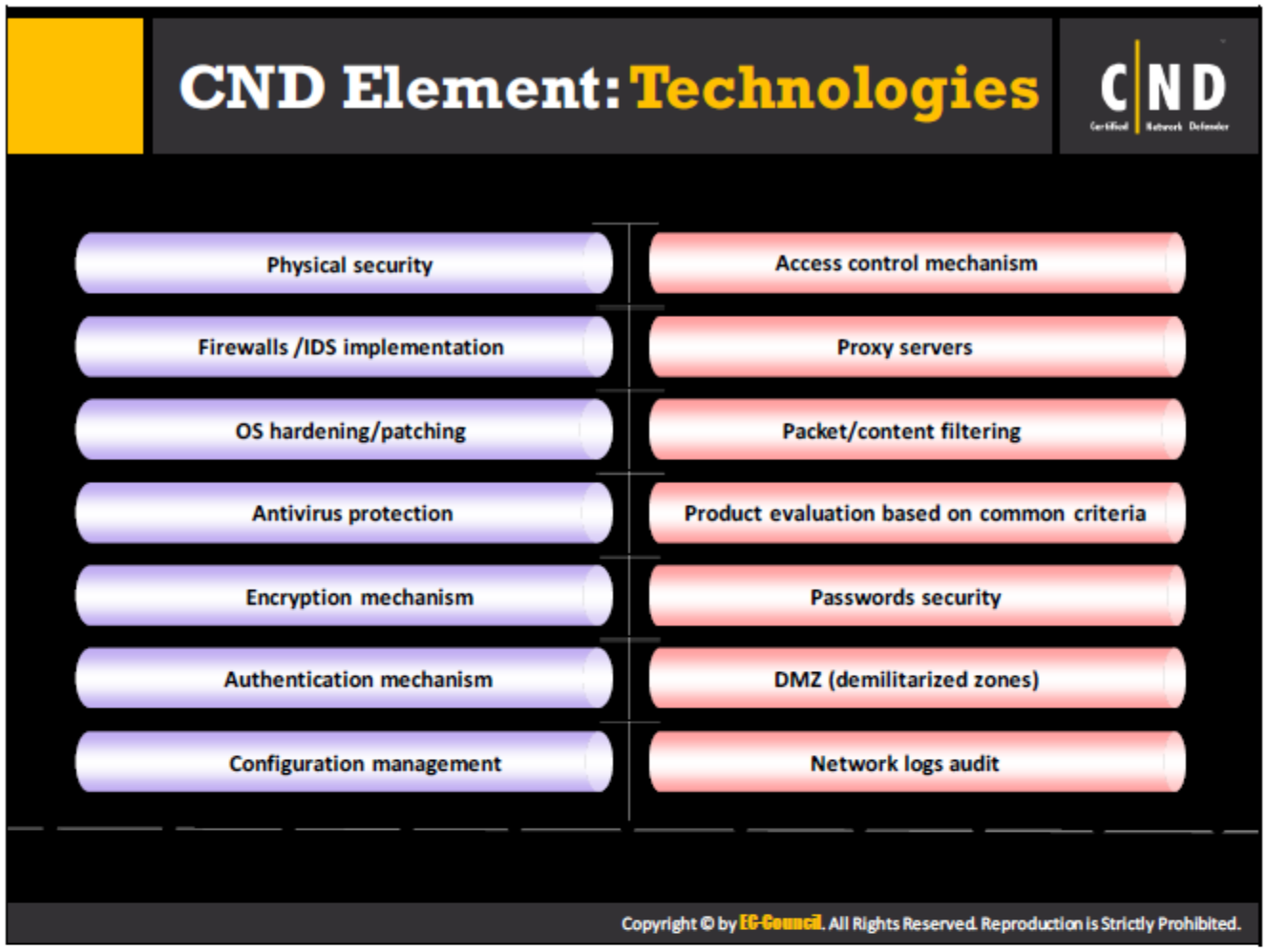
- **Availability:** Availability is the process of protecting the information systems or networks that hold the sensitive data to make them available for the end users whenever they request access.
- **Confidentiality:** Confidentiality allows only authorized users to access, use or copy information. Authentication works closely with confidentiality, if the user is not authenticated, they will not be granted access to confidential information. If a non-authorized user accesses the protected information, it implies that a breach of confidentiality has occurred.
- **Integrity:** Integrity protects the data and does not allow modification, deletion or corruption of data without proper authorization. This information assurance principle also works closely with Authentication to function properly.

- **Non-Repudiation:** Non-Repudiation is a service that validates the integrity of a digital signature's transmission: starting from where it originated to where it arrives. Non-repudiation grants access to the protected information by authorizing that the digital signature is from the intended party.
- **Authentication:** Authentication is a process of authorizing users with the credentials provided by comparing them to those in a database of authorized user's information on an authentication server to grant access to the network. It guarantees that the files or data passing through the network is safe.



The network defense is achieved with the appropriate implementation of technology, operations and people in the organization. These elements play an important role in attaining the proper defense in depth network security for the organization. Technology is not enough to protect the network from a variety of attacks. Certain operations are needed in order to configure these technologies and skilled individuals are required who can perform those operations.

The combined use of these elements contributes to achieving defense in depth network security.

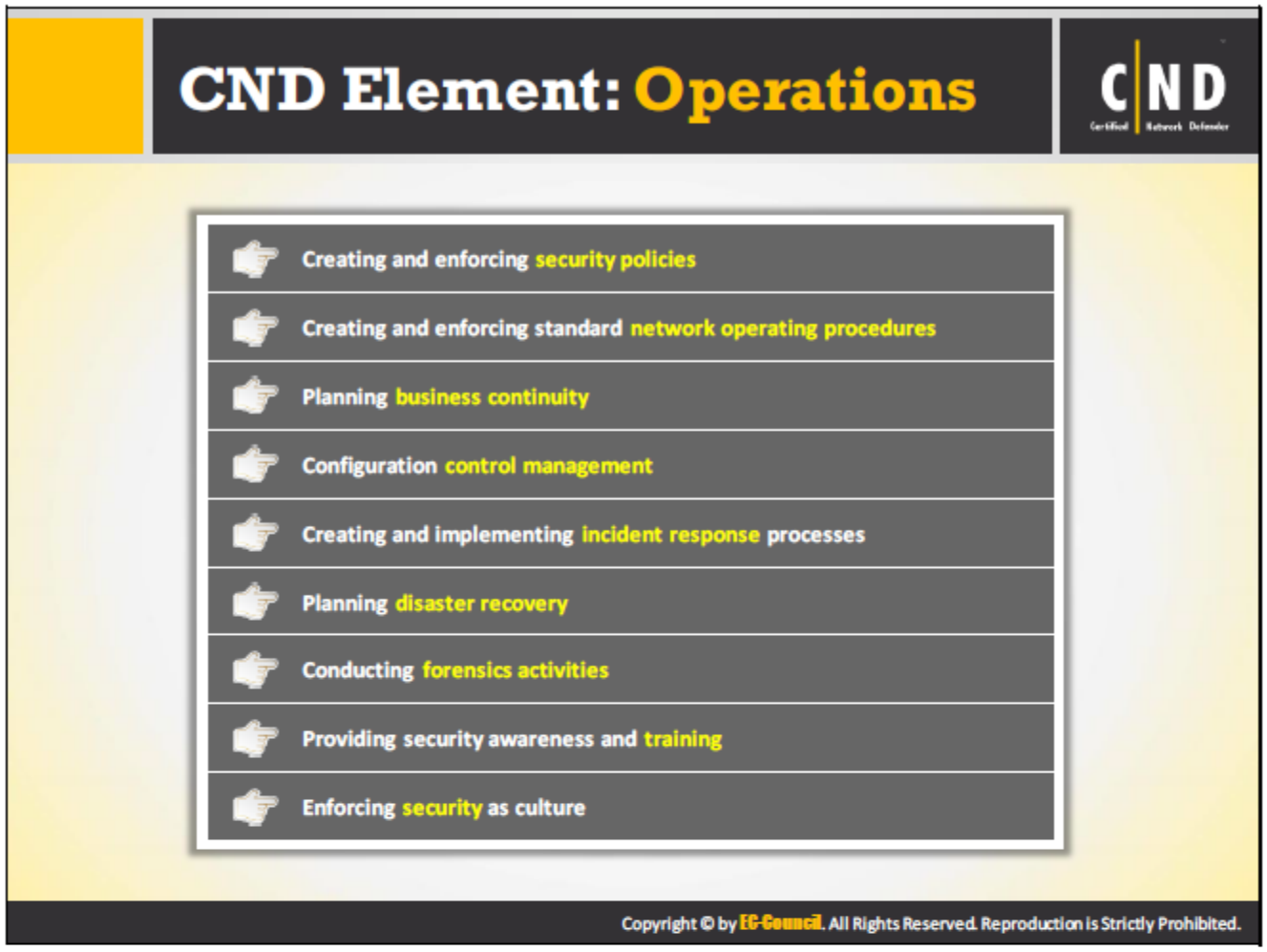


Implementations of the following technologies help an organization to protect their assets

- **Physical security:** The main aim in implementing the physical security is to secure the hardware, personnel, networks, data and information. Physical security can prevent all kinds of physical damage, theft or loss to an organization or an enterprise. It also provides protection from fire, vandalism and other natural disasters.
- **Access control mechanism:** The main aim in implementing the access control mechanism is to implement certain restrictions in users accessing the resources in the network. Controlling the access to devices and other resources can actually secure the network as well as to prevent the use of any rogue devices.
- **Firewalls/IDS implementation:** The main aim in implementing a firewall or IDS is to execute certain security policies for communication in the network. Firewalls can actually filter the trusted and untrusted network traffic and then allow the passage of traffic depending on those policies. The IDS system can identify and monitor any kind of illegal activities in the network level as well as in the host level.
- **Proxy servers:** The main aim in placing a proxy server in the network is to conceal the original IP address from the attackers and thereby increasing the level of security in the network. The proxy servers can also execute the user requests at a faster rate by the method of caching.

- **OS hardening/patching**: The main aim in performing the operating system hardening or patching is to prevent the level of any vulnerability in the network. The process of patching and hardening provides the latest security updates and issues at the application level, thereby enabling network administrators to solve the issue at a faster rate.
- **Packet/content filtering**: The main aim in implementing packet/content filtering is to prevent any kind of intrusion in the network. The content packet filtering method filters or searches for viruses, worms, intrusions or any other non-compliant protocols in the network. It blocks or prevents passage of packets based on the source and the destination addresses.
- **Antivirus protection:** The main aim in implementing anti-virus in the system is to secure the data and systems from viruses, botnets, Trojans, etc. These malware programs can actually gain the username and passwords of the user on the victim machine or compromise the data contained in a system. The anti-virus can alert the user regarding the presence of any malware program in the system.
- **Product evaluation based on common criteria:** The main aim in implementing the product evaluation is to ensure that the IT products meet the security standards required for deployment in the networks. The IT products need to meet the common criteria defined for each specific product. Meeting the common criteria ensures the security of the IT products deployed in the network.
- **Encryption mechanism:** The main aim in implementing the encryption mechanism is to provide the confidentiality and integrity of the information passed on the network. The encryption process confirms that the only sender and receiver of a message can actually read the message and prevents all kinds of unauthorized access. The mechanism also includes the use of an encryption key without which the sender and receiver cannot access the message.
- **Passwords security:** The main aim in implementing the password security is to ensure complete security of the passwords from all types of password attack. It protects the passwords from brute-force attack and eavesdropping mechanisms. The password security mechanism persuades the user to use long and complex passwords. It also brings in certain mandatory policies that each user needs to follow while creating passwords, thereby minimizing the chances of an attack on passwords.
- **Authentication mechanism:** The main aim in implementing authentication mechanism is to ensure the authenticity of the user requesting an access to a resource. The authentication mechanism checks the identity of the user against various methods like credentials, biometrics, etc. The method of authentication can restrict unauthorized access from the users.
- **DMZ (demilitarized zones):** The main aim in implementing the DMZ is to ensure the security of an organization's local area network from an untrusted network. The demilitarized zone can provide an extra layer of security to the network and prevent the attackers from accessing the internal servers and data through the internet.

- **Configuration management:** The main aim in implementing the configuration management is to provide the consistency in performance, functionalities and physical components of the resources in a network. It prevents the chances of any failure of equipment or any adverse changes in the system. The configuration management also provides an idea regarding the updates and upgrades required for a resource.
- **Network logs audit:** The main aim in implementing the network logs audit is to monitor the activities of a network. The review of network audits can actually increase the security of the network.

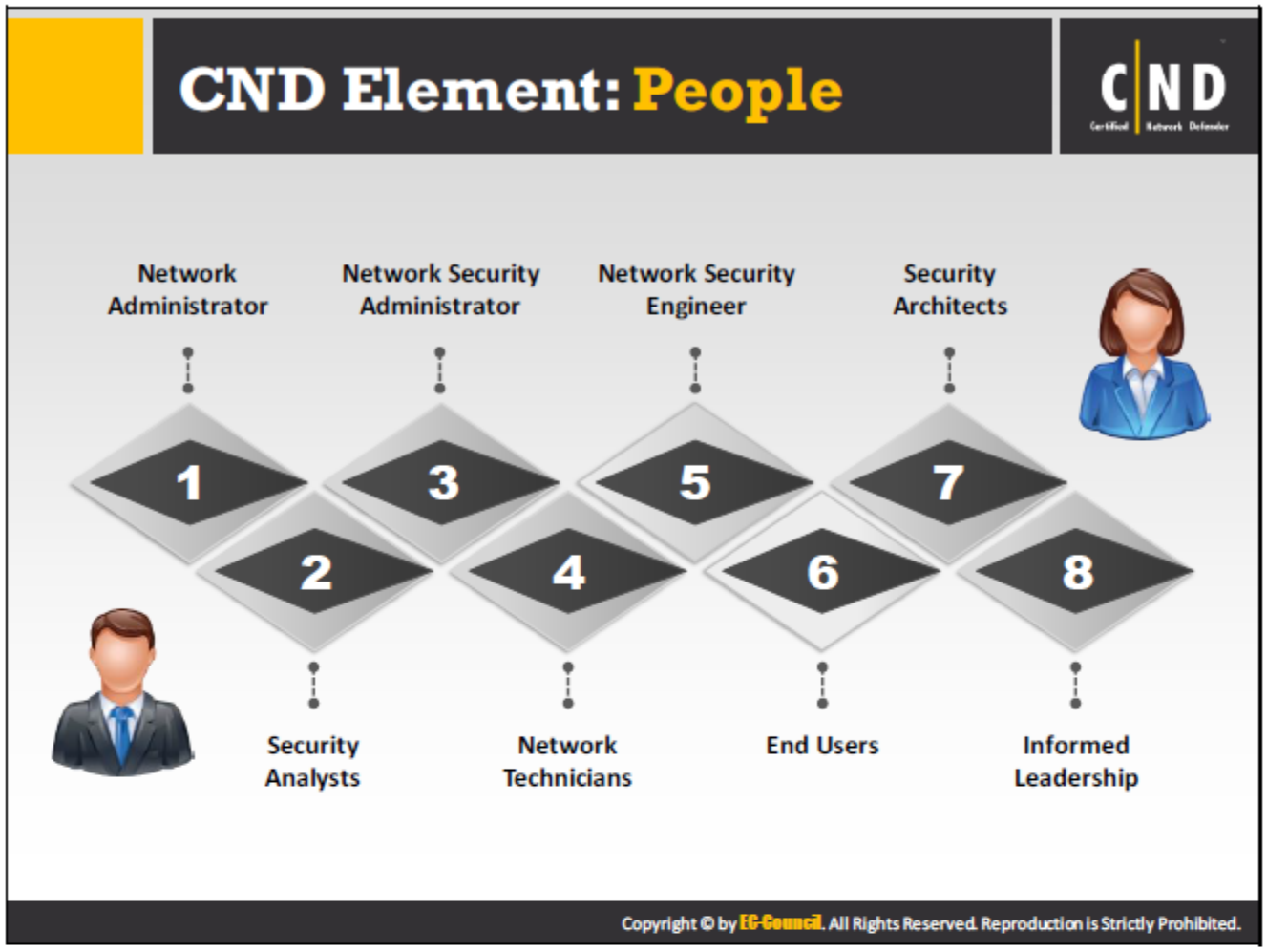


Performing following operations helps organizations to maintain the security of their assets

- **Creating and enforcing security policies:** Network operators need written security policies to monitor and manage a network efficiently. These policies set appropriate expectations regarding the use and administration of information assets on a network. Security policies describe what to secure on the network and the ways to secure them.
- **Creating and enforcing standard network operating procedures:** Standard network operating procedures are instructions intended to document the routine network activity. Network operators should rely on these procedures to ensure efficiency and security of the network. The main goal of network operating procedures is to carry out the network operations correctly and always in the same manner.
- **Planning business continuity and disaster recovery:** There are various threats and vulnerabilities to which business today is exposed, such as natural disasters, acts of terrorism, accidents or sabotage, outages due to an application error, hardware or network failures. Planning business continuity and disaster recovery is the act of proactively working out a way to prevent and manage the consequences of a disaster, limiting it to a minimum extent.
- **Configuration control management:** Network operators encounter many problems due to the lack of configuration management capabilities. Configuration control management involves initiating, preparing, analyzing, evaluating and authorizing proposals for change to a system.

- **Configuration control management includes:**
  - Device hardware and software inventory collection.
  - Device software management.
  - Device configuration collection, backup, viewing, archiving and comparison.
  - Detection of changes to configuration, hardware, or software.
  - Configuration change implementation to support change management.
- **Creating and implementing incident response processes:** Network operators create and implement an incident response process through planning, communication and preparation. Incident preparation readiness ensures quick and timely response to incidents. Network managers should determine whether to include law enforcement agencies during incident response or not as including; it can affect the organization positively or negatively.
- **Conducting forensics activities on incidents:** Computer Forensics Investigators examine the incident and conduct forensic analysis by using various methodologies and tools to ensure the computer network system is secure in an organization.

  While conducting forensics activities on incidents, people responsible for network management should:
  - Ensure that the professionals they hire are prepared to conduct forensic activities.
  - Ensure that their policies contain clear statements about forensic considerations.
  - Create and maintain procedures and guidelines for performing forensic activities.
  - Ensure that their security policies and procedures support the use of forensic tools.
- **Providing security awareness and training:** Some of the threats to network security come from within the organization. These inside attacks can be from uninformed users who can do harm to the network by visiting websites infected with malware, responding to phishing e-mails, storing their login information in an unsecured location, or even giving out sensitive information over the phone when exposed to social engineering. Network managers should make sure that the company's employees are not making costly errors that can affect network security. They should institute company-wide security-awareness training initiatives including training sessions, security awareness website(s), helpful hints via e-mail, or even posters. These methods can help ensure employees have a solid understanding of the company security policy, procedures and best practices.
- **Enforcing security as culture:** Network operators should enforce security as a culture in the organization. It helps knowing what behavior compromises security and how to educate employees to change their insecure behavior. The culture within an organization will have a significant influence on the likelihood of risks occurring, and the degree to which varying control approaches will be successful.

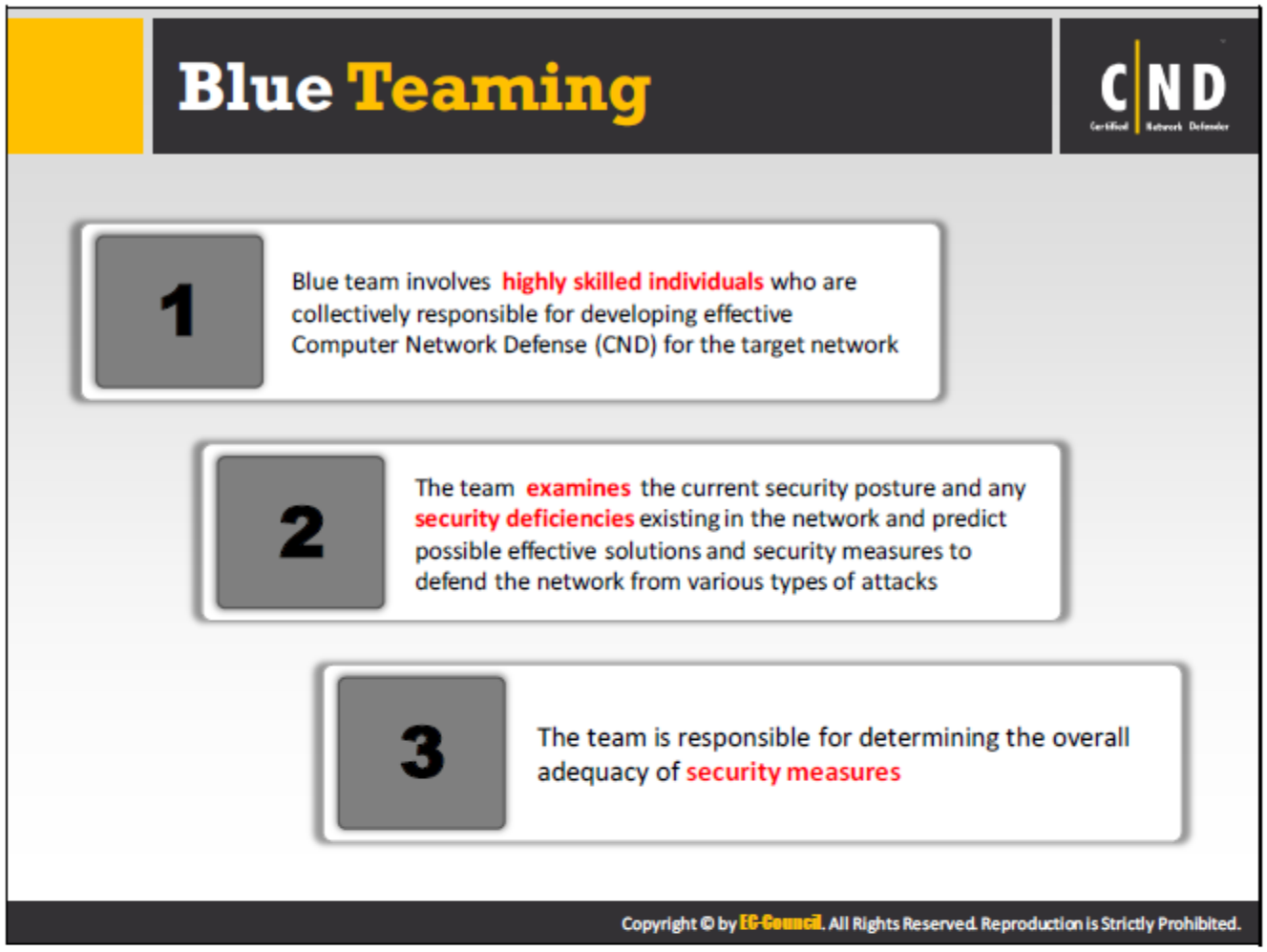


Network defense relies on the people involved in network operations. People are a crucial element of any organization's network security approach. The degree to which people embodies a culture of security will significantly influence that organization's ability to protect key assets. The people involved are responsible for maintaining, repairing and managing network and computer systems to improve their performance. They explore and solve network problems logically and consistently. They monitor the network for vulnerabilities before an outsider can exploit it. These people make use of CND technologies and operations to design and implement robust and secure the network.

People involved in computer network defense include:

- **Network Administrator:** The network administrator manages the whole network in an organization. They coordinate all systems, software, etc. and help in running the network of an organization smoothly.
- **Network Security Administrator:** The network security administrator is responsible for maintaining all the cyber security of an organization. They fix, control and monitor the security solutions of an organization.
- **Network Security Engineer:** The network security engineer mainly develops the countermeasures required for any cyber related issues in an organization. They monitor and manage the IT issues.

- **Security Architects:** The security architect supervises the implementation of the computer and network security in an organization. They need to find methods to implement the network and computer security in an efficient manner.
- **Security Analysts:** The security analyst maintains the privacy and integrity of the internal network in an organization. They need to evaluate the efficiency of the security measures implemented in an organization.
- **Network Technicians:** The network technician manages the hardware and software components of an organization. They fix and repair the issues related to these components.
- **End Users:** The end user refers to the people who use the end product deployed by an organization. The end user can access the developed products through Desktop, Laptop, iPads, Smart Phones, etc.
- **Informed Leadership:** The informed leadership can help an organization in taking exemplary decisions regarding the security of the network and systems in an organization. They need to be proactive enough to find the weaknesses and strengths in a network.

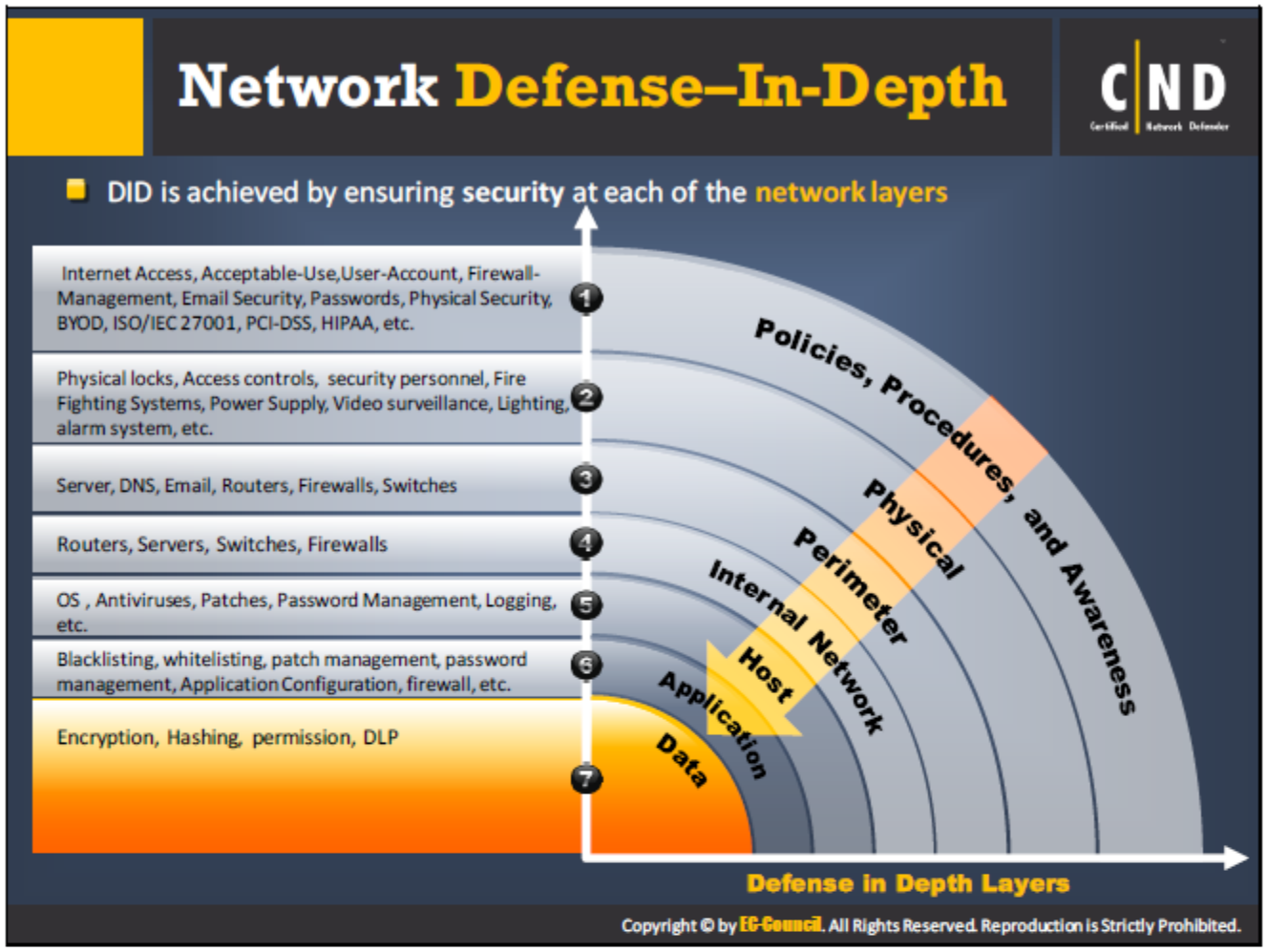


A Blue team is an internal security team who help in building a strong Computer Network defense (CND) for the Network. Blue team is a part of the Red/ Blue team exercise to defend the network. The Blue team defends the network from both real and red team attacks. Blue team security professionals have direct access to the network. The Blue Team is responsible for detecting the attacks and, in a limited form, for protecting the hosts. They identify known vulnerabilities on systems and do not address the requirements for an overarching security infrastructure. The goal of the Blue Team is to detect the attacks and execute some counter-measures to slow down or confuse the attackers.

- **Roles and Responsibilities:**
  - Blue team protects the network against the attacks by the red team.
  - Use tools to monitor and protect the network.
  - Implement preventive measures to minimize the attacks.
  - Create reports of the incidents to be sent to the management.
  - Blue team must gain knowledge of the threat actor's Tactics, Techniques and Procedures (TTPs) and prepare counter approaches to defend the network.
  - Understand advanced threat actor activities on the network using defensive techniques against these actors.
  - Understand the network using a realistic advanced attacker viewpoint.

- Find the operational readiness and incident response capabilities of the network using various tools and techniques.
- Assess the ability of internal network defenses in eliminating attacks from advanced threat actors.

- **Advantages of Blue Teaming:**
  - Enhance the security of the organization network.
  - Blue team members gain complete knowledge of the existing network defense.
  - Validate existing network defense, and help use them effectively.
  - Blue teams are more vigilant against attacks.
  - Forming Blue teams helps by improving the training for network defenders to protect the network.
  - Help structure a realistic security process for monitoring threats in advance.



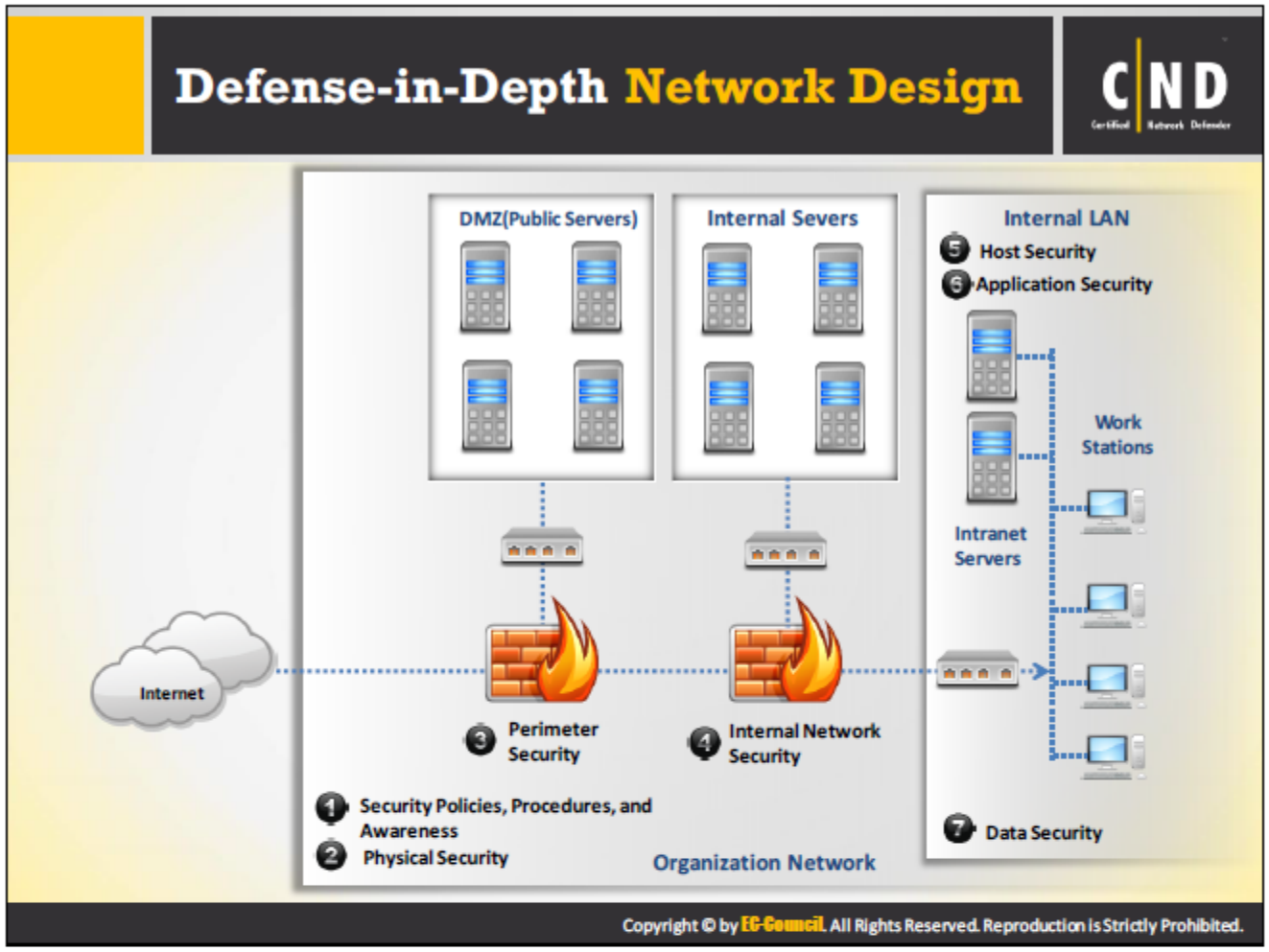
Defense in depth is a security strategy in which several protection layers are used throughout an information system. Defense-in-depth involves implementing security controls at different layers of network stack. It imposes a complex defense layered structure thereby making it difficult for the attackers to penetrate into the system and achieve their goal.

This strategy uses the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier. Defense in depth helps to prevent direct attacks against an information system and its data because a break in one layer leads the attacker only to the next layer. If a hacker gains access to a system, defense-in-depth minimizes any adverse impact and gives administrators and engineers time to deploy new or updated countermeasures to prevent a recurrence of intrusion or stop an intrusion from going any deeper.

Typical layers of Defense-in-depth approach include:

- **Policies, Procedures, and Awareness:** This is the first level of countermeasures that every organization must design and implement. It includes enforcing security policies to avoid misuse of resources or restrict unauthorized operations on the organization's resources.
- **Physical:** It involves ensuring security of organization assets from various physical threats.
- **Perimeter:** It involves the design and implementation of appropriate security measures at the perimeter level.

- **Internal Network:** It includes the design and implementation of security measures at an internal network.
- **Host:** It involves implementing security measures at each individual host level.
- **Application:** It involves implementing security measures at the application level.
- **Data:** It involves implementing security measures to data whether it is at rest or transit.



The first line of defense against attacks is the firewall, which can be configured to allow/deny traffic. Installing and configuring the Next-Generation firewalls with capabilities such as application control, identity awareness, IPS, web filtering, and advanced malware detection can increase complexity for the attacker to bypass them.

IDS/IPS is the second line of defense mechanism for a network even though it is included in the firewall as first line of defense. Having your IPS properly optimized and monitored is a good way to detect and block attackers that get past the first castle defense.

The network administrator should consider the following factors while developing and designing a secured network:

- The network topology and location of the hosts in a network.
- The right selection of hardware and software security technologies.
- Proper configuration of each component.

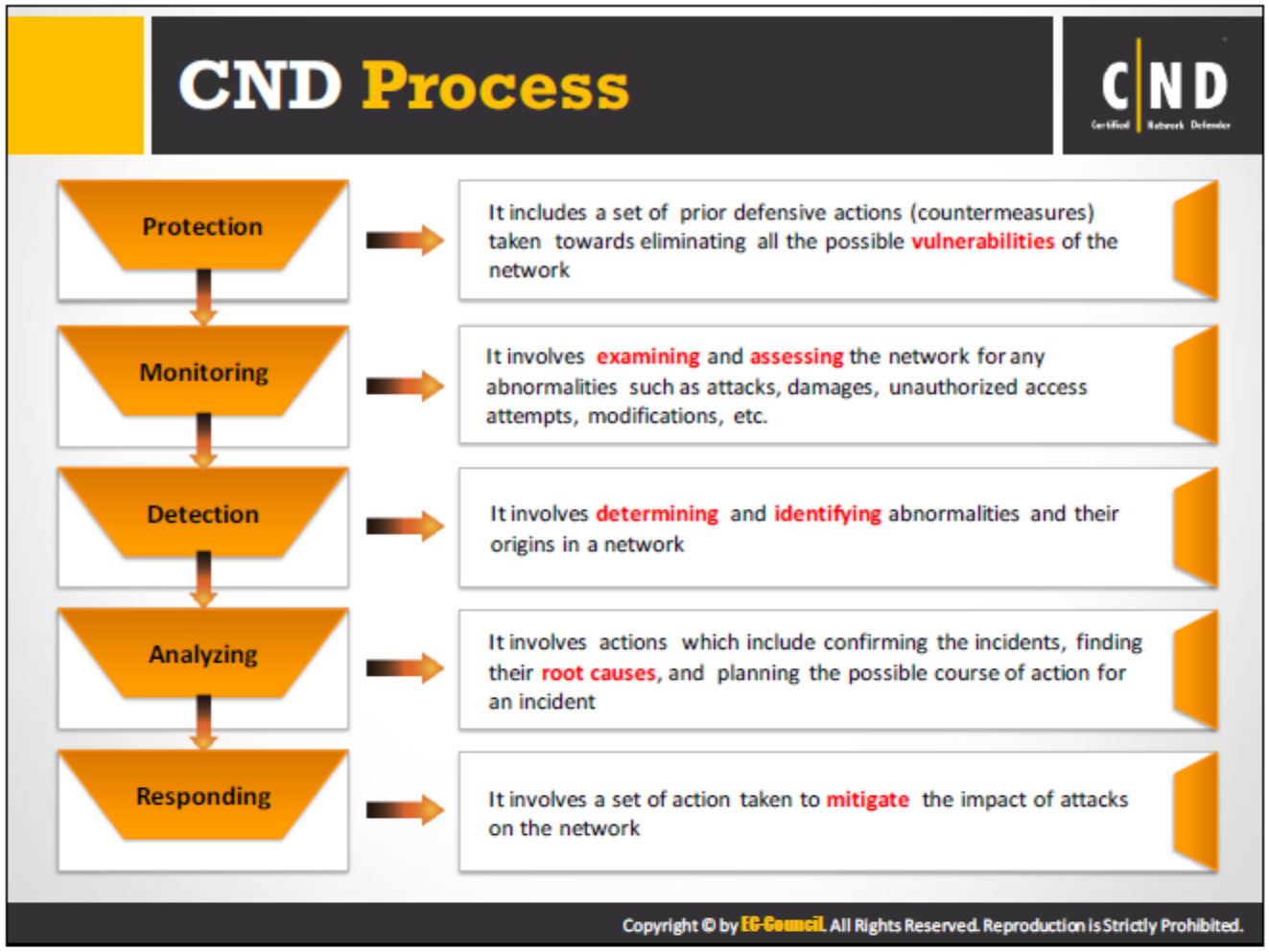
Network designers should always monitor and examine common security issues found in the network set up of a company to establish a secure network. They should also identify some best practices to secure the network.

The challenges encountered by the network designer are:

- Protecting the network from attacks that come from the internet.
- Protecting public servers such as web, e-mail and DNS servers.

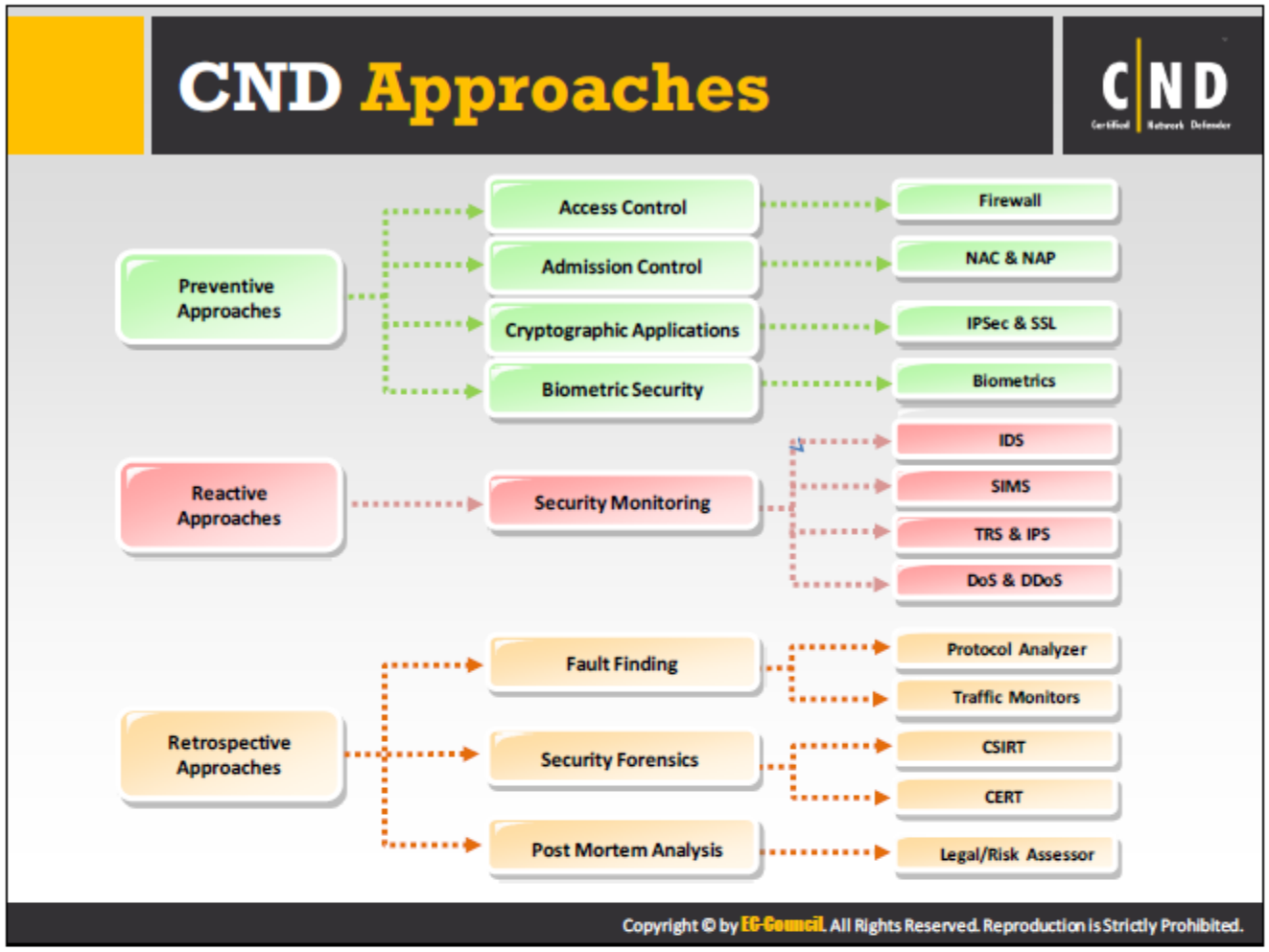
- Containing damage when a network or system is compromised.
- Preventing internal attacks against the network.
- Protecting highly important and sensitive information like customer databases, financial records and trade secrets.
- Developing guidelines for the administrators to handle the network in a secure manner.
- Enabling intrusion detection and logging capabilities.

Network designers need to take care of certain policies that help in the careful and efficient management of the organization. The policies created should follow the company standards and should include criteria like number of human resources needed, cost for securing the network etc. The network designer can proceed with the network design after the creation of these policies.



The CND process specifies the prevention, detection and response actions to security incidents in order to ensure complete computer network defense. It should be a continuous process. The following phases of the CND process assist network administrators in implementing network security effectively:

- **Protecting:** It includes a set of prior defensive actions (countermeasures) taken towards eliminating all the possible vulnerabilities on the network. It includes security measures such as Security Policies, Physical security, Host Security, Firewall, IDS, etc., used to offer network protection.
- **Monitoring:** It involves examining and assessing the network for any abnormalities such as attacks, damages, unauthorized access attempts, modifications, etc. It includes regular monitoring of network traffic using network monitoring and packet sniffing tools.
- **Detecting:** It involves determining and identifying any abnormalities and their location in the network. It includes identifying what is abnormal to the network.
- **Analyzing:** It involves actions, which includes confirming the incidents, finding their root causes, and planning a possible course of actions for an incident. It includes deciding whether the incident is actual security incidents or a false positive.
- **Responding:** It involves a set of actions taken to mitigate the impact of an attack on the network. It includes incident response, investigation, containment, and eradication steps for responding to the incidents.

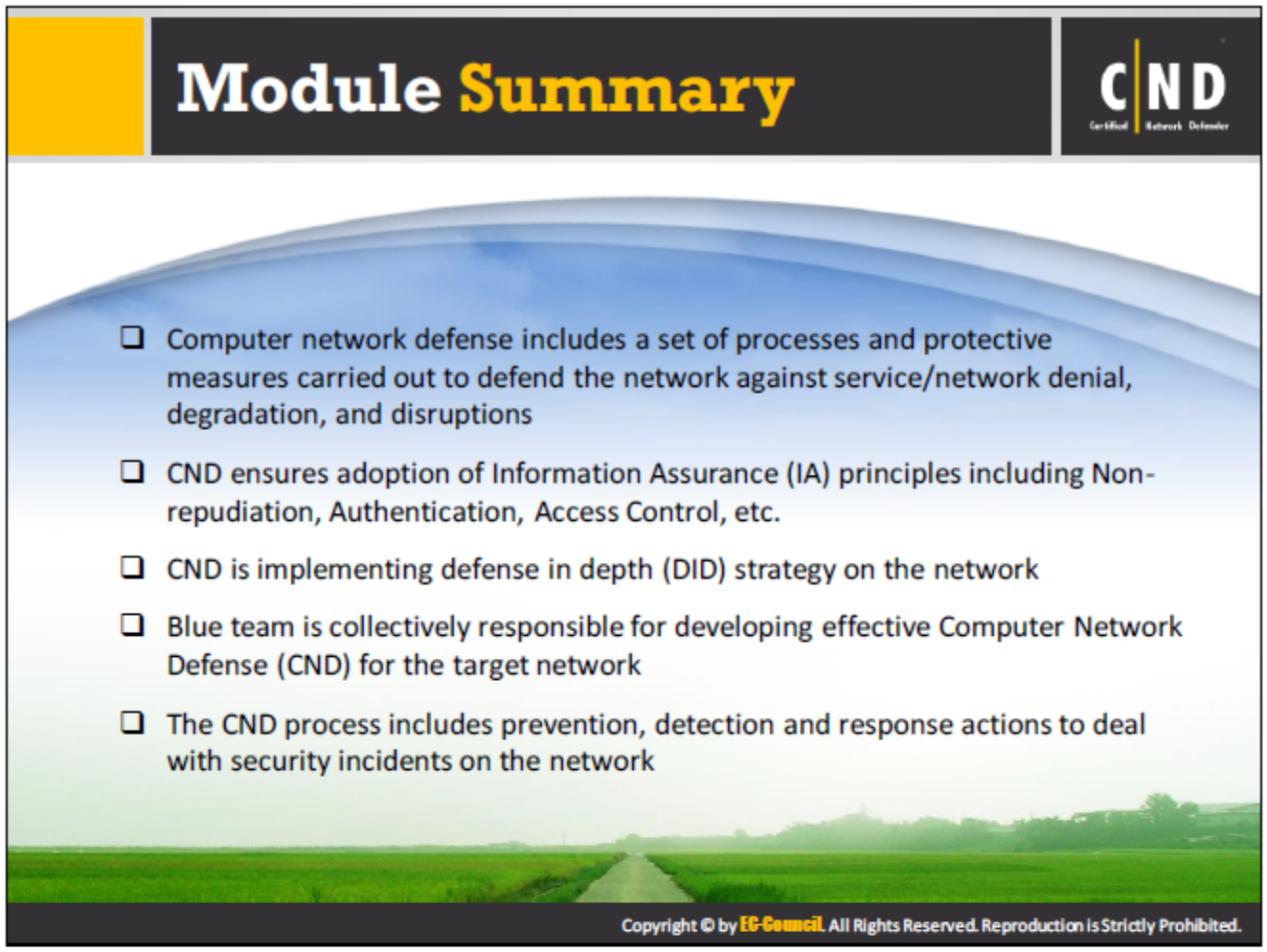


There are three main classifications of security defense techniques used for identification and prevention of threats and attacks in the target network.

- **Preventive Approach:** The preventive approach basically consists of methods or techniques that can easily avoid the presence of threats or attacks in the target network.

  The preventive approaches mainly used in the network are as follows:

  - Access control mechanisms such as a firewall.
  - Admission Control mechanisms such as NAC and NAP.
  - Cryptographic Applications such as IPSec and SSL.
  - Biometric techniques such as speech or facial recognition.
- **Reactive Approach:** The reactive approach is complementary to the preventive approach. The reactive approach prevents those attacks and threats which the preventative approach failed to. For example a DoS and DDoS attack. Implementing both preventive and reactive approaches will confirm the security of the network. The reactive approaches include security monitoring methods such as IDS, SIMS, TRS, IPS, etc.
- **Retrospective Approach:** The retrospective approach examines the reasons for attacks in the network. The approaches include:
  - Fault finding mechanisms which include a protocol analyzer and traffic monitors.
  - Security forensics techniques such as CSIRT and CERT.
  - Post-mortem analysis mechanism including legal/risk assessor.



This module provided you an overview on the fundamental concept of TCP/IP networking, including standard network models, types of network, topologies, TCP/IP protocol stack, IP addressing schemes.

The module also introduced you to Computer Network Defense (CND) and the different elements, which establish defense-in-depth network security. The module depicted the CND process and approaches which will be described in subsequent modules. With this module, you will understand the broad overview of computer network defense.