EC-Council

Building A Culture Of Security



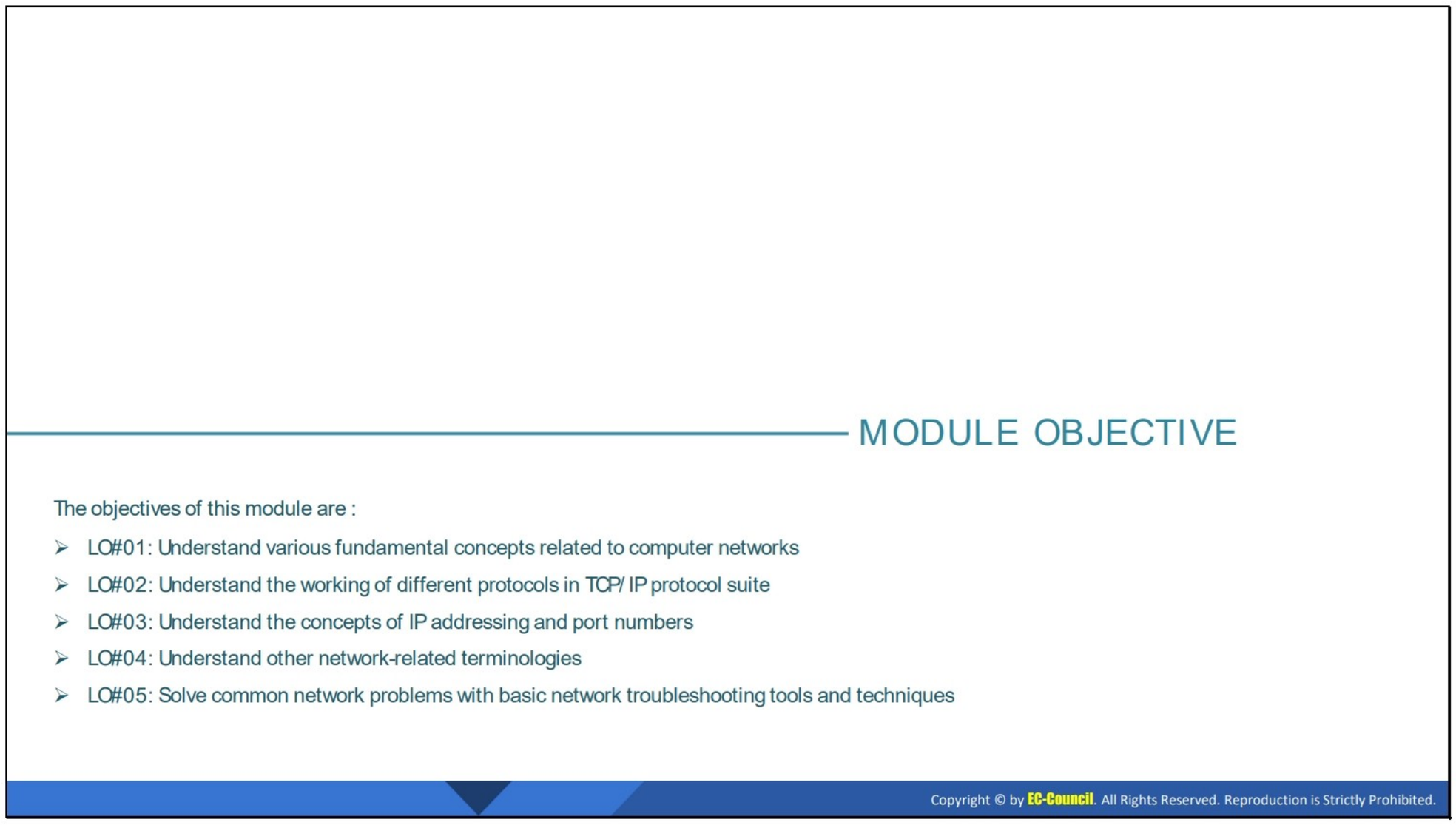
C|ND
Certified Network Defender

Certified Network Defender v3

APPENDIX A
COMPUTER NETWORK FUNDAMENTALS

EC-Council Official Curricula

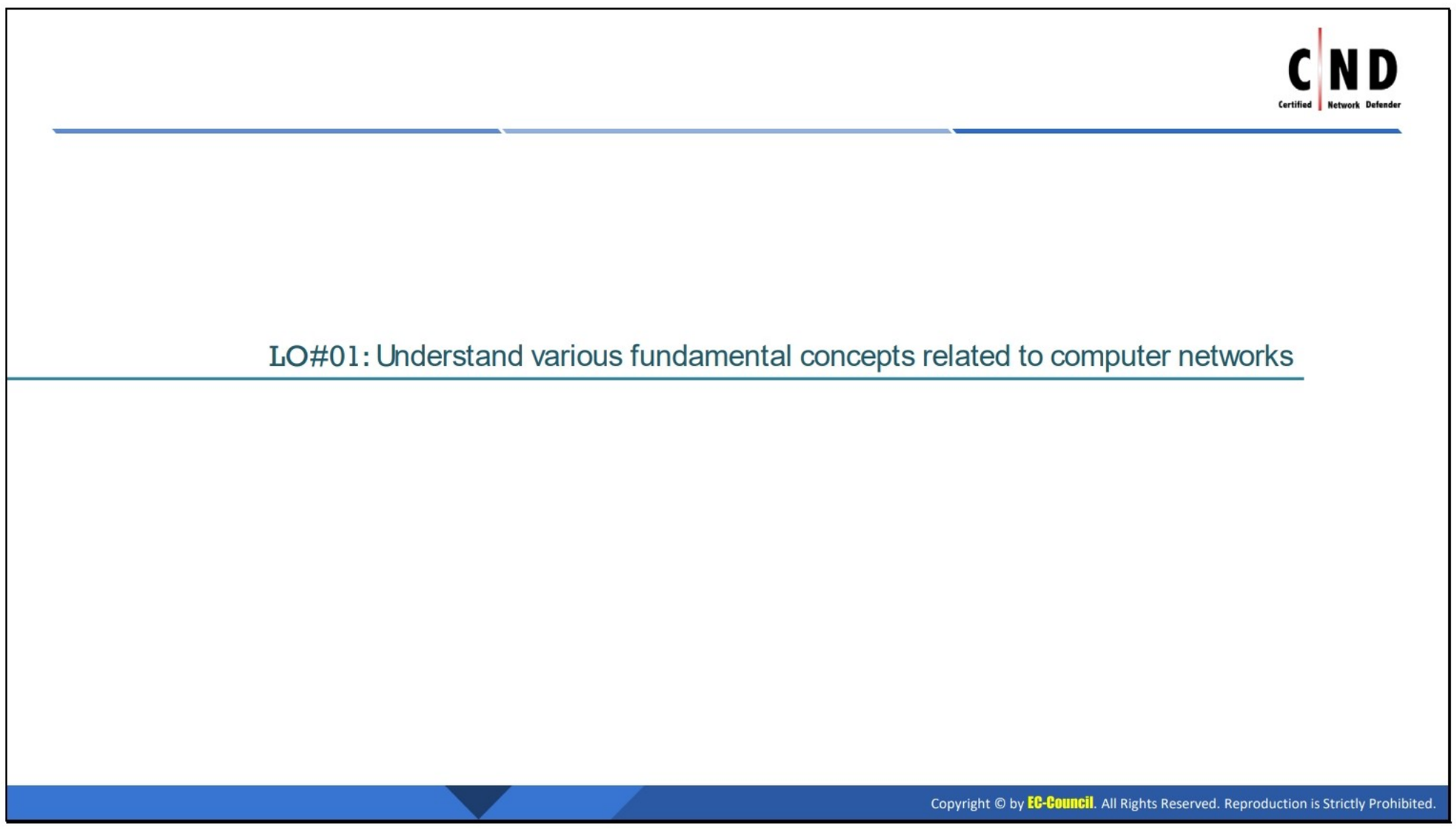
This page is intentionally left blank.



Module Objective

This module discusses the fundamentals of networking including Transmission Control Protocol (TCP)/Internet Protocol (IP) networking concepts and IP addressing concepts. The module also covers various tools and techniques used for troubleshooting network issues.

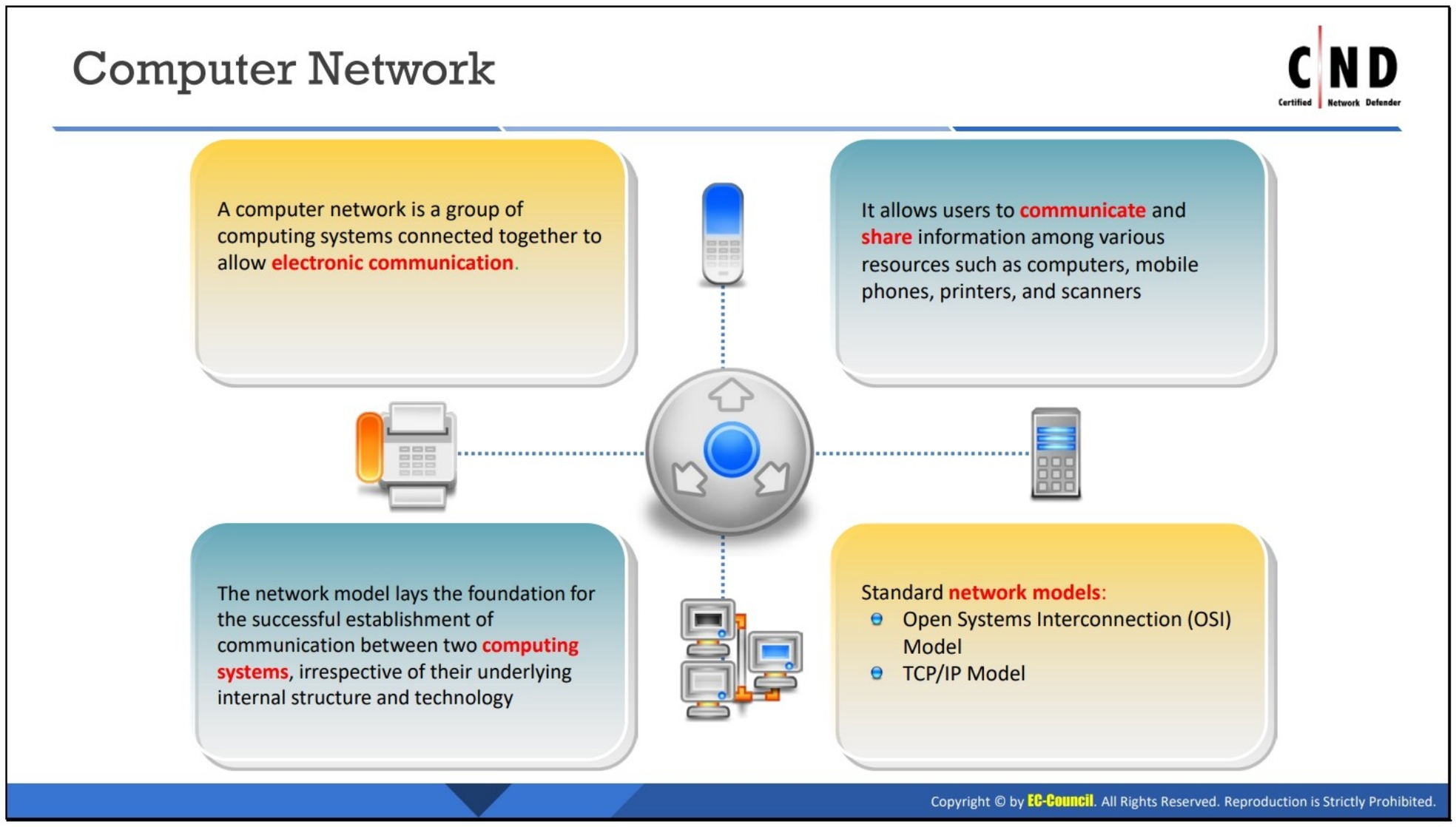
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#01: Fundamental Concepts Related To Computer Networks

This section discusses the basic concepts of computer network fundamentals, including types of networks, network topologies, network models, networking hardware, and various protocols used in computer networking.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Computer Network

A computer network is a connected group of computing systems that allows electronic communication and the easy sharing of information and resources. The computers share information using a data path.

The features of a computer network include the following:

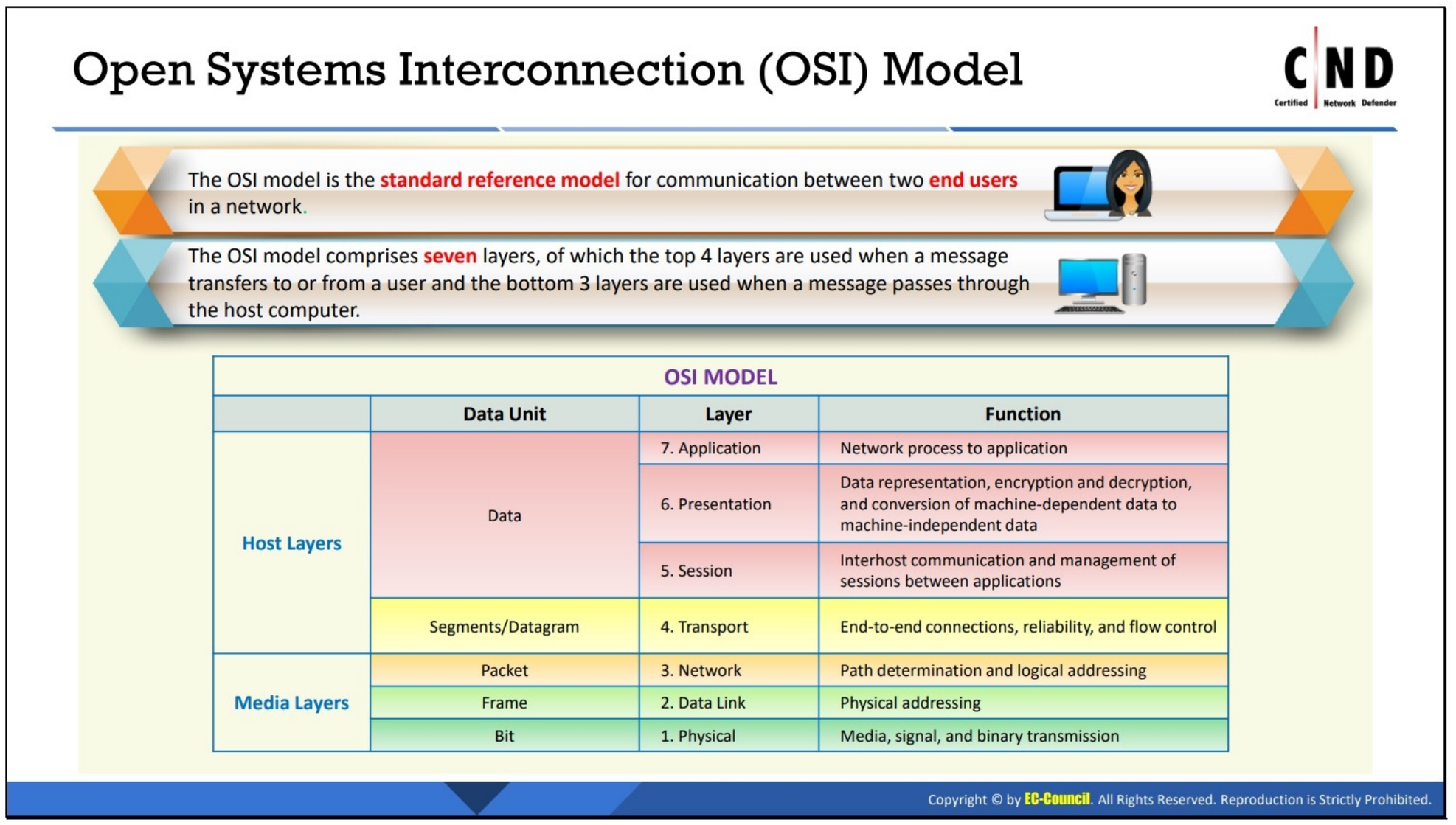
- It allows users to communicate and share information among various resources such as computers, mobile phones, printers, and scanners.
- The network model lays the foundation for the successful establishment of communication between two computing systems, irrespective of their underlying internal structure and technology.
- It allows the sharing of resources between two computers.
- It 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.

Many fields such as electrical engineering, telecommunications, computer science, and information technology make use of computer networking concepts. These allow for easy communication among users by means of chat, email, instant messaging, etc.

The following are the standard network models:

- Open Systems Interconnection (OSI) model
- TCP/IP model

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Open Systems Interconnection (OSI) Model

OSI is a reference model that defines the transmission of data over a network. It is a framework that characterizes the flow of data from one device to another over a 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 the 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. Subsequently, the flow traverses the network and propagates upwards through the layers of the destination computer.

The following are the features of the OSI model:

- Provides a clear understanding of the communication over a network
- Displays the working of software and hardware
- Helps users understand new technologies
- Easily compares the functional relationships between different networks

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

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

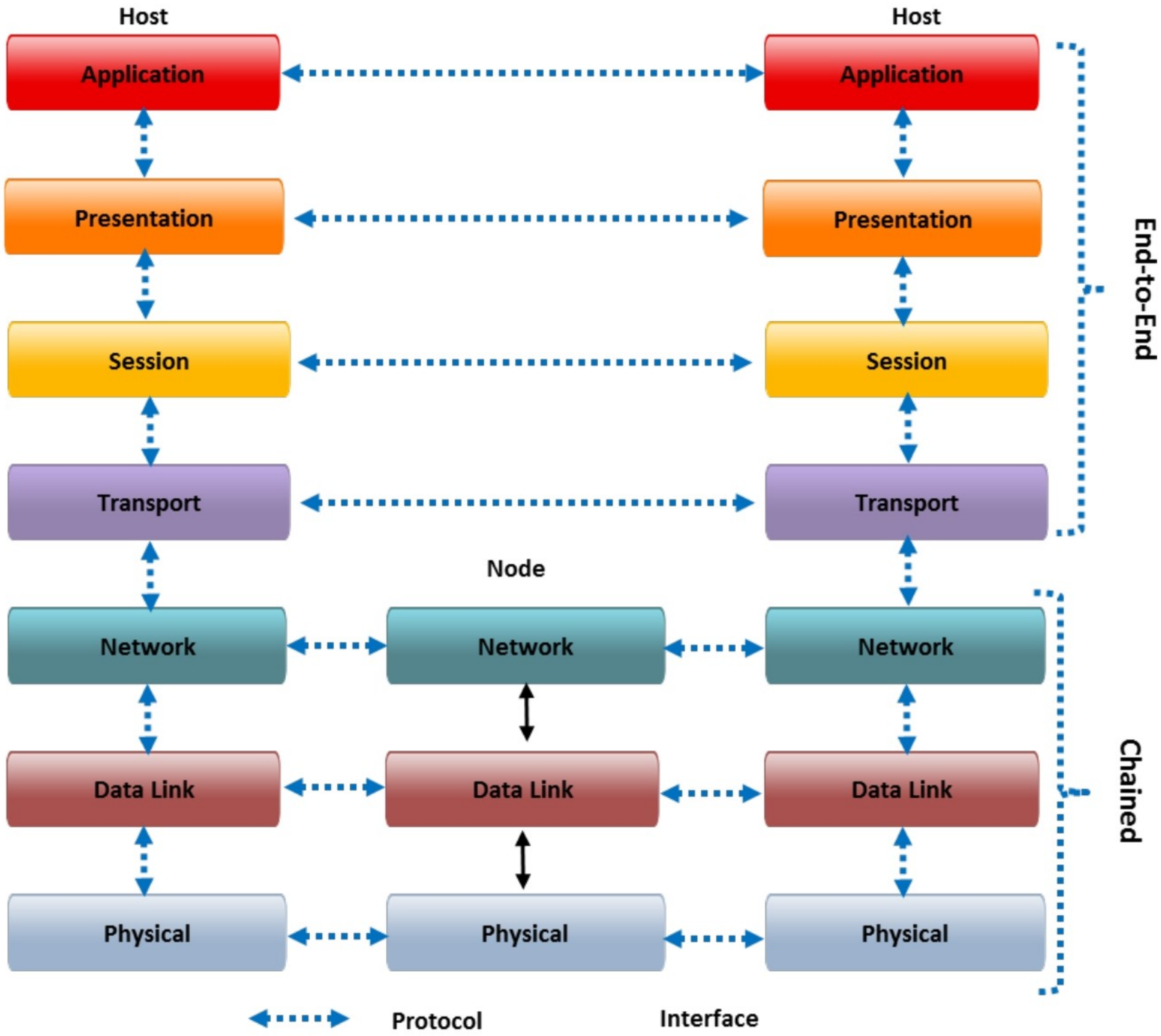
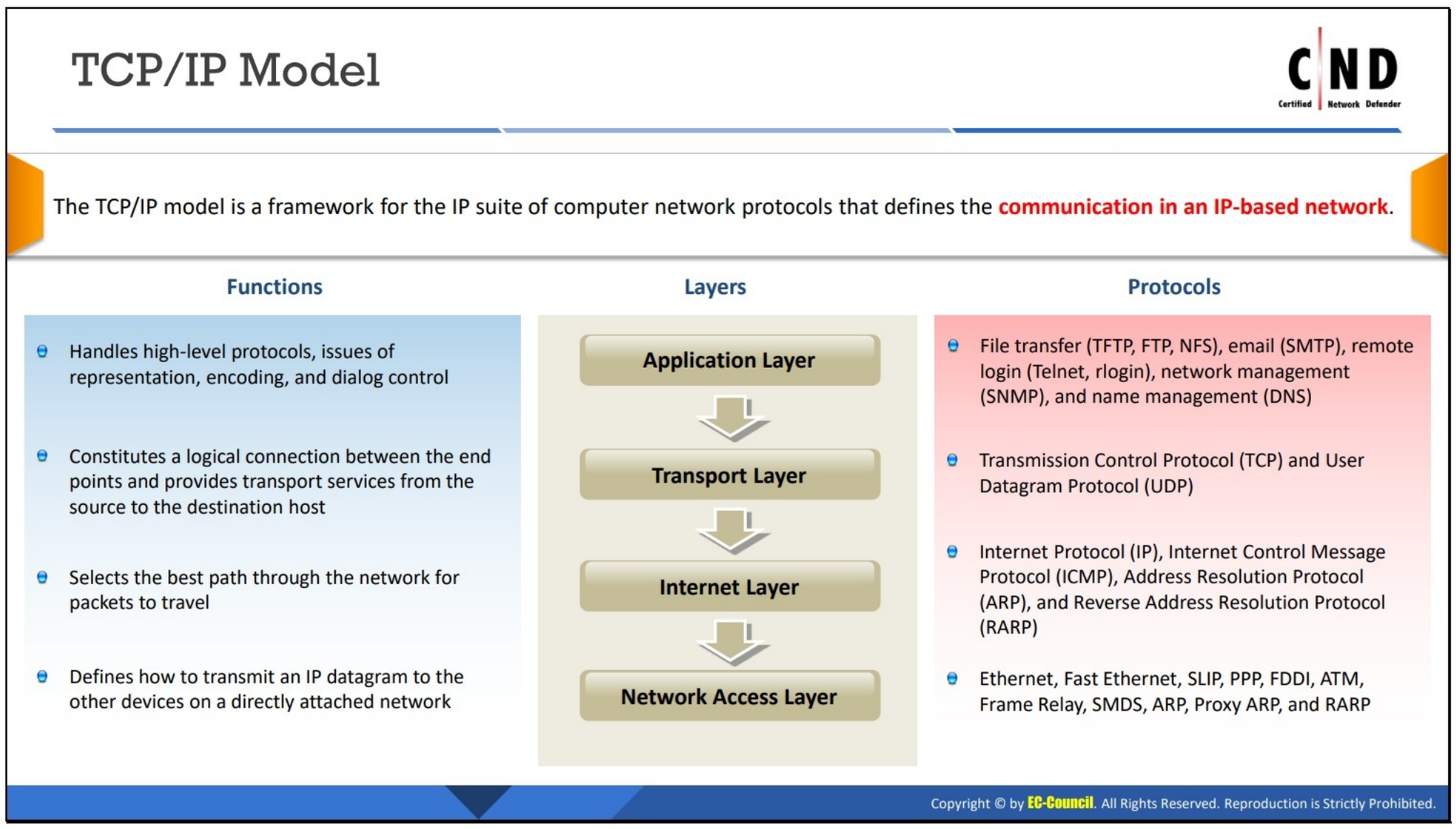


Figure A.1: OSI Reference Model

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

- Each layer needs to meet a different concept or overview. Thus, the creation of 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. The selection of layers depends on the number of functions performed.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



TCP/IP Model

The TCP/IP model is a framework for the IP suite of computer network protocols that defines the communication in an IP-based network. The TCP/IP model describes the end-to-end communication between two machines and thereby determines the addressing, routing, and transmission of data.

TCP/IP Layers

TCP/IP is a four-layered protocol developed by the Department of Defense (DOD). Each layer in this model performs a different function, and data flow occurs from layer 4 to 1 (from the sending machine) and from layer 1 to 4 (in the destination machine).

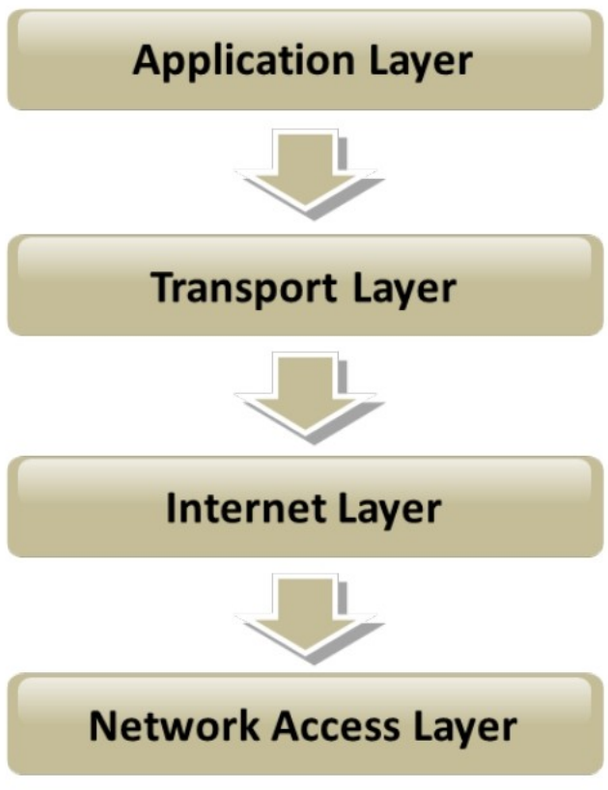


Figure A.2: TCP/IP Layers

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The four layers in the TCP/IP model are as follows:

- **Network access layer—layer 1**

  The network access layer is the lowest layer in the TCP/IP model and enables the communication of data present in the same network. It handles data flow 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, Fiber Distributed Data Interface (FDDI), X.25, Frame Relay, RS-232, and V.35.

- **Internet layer—layer 2**

  The Internet layer enables internetworking. It 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 framework. In this protocol, the sequence of the packets received at the destination network differs from that sent from the source network. The IP, Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), and Reverse Address Resolution Protocol (RARP) are the protocols used in this layer.

- **Transport layer—layer 3**

  The transport layer manages host-to-host interactions. It determines the status of data transmission between the source and destination. The functionalities of the transport layer include end-to-end communication, error control, segmentation, flow control, and application addressing. End-to-end communication is of two types: connection oriented and connectionless. TCP implements connection-oriented communication, whereas the User Datagram Protocol (UDP) initiates connectionless communication.

  The TCP layer determines whether 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 such that the network layer can handle the data efficiently. The TCP, UDP, and Real-time Transport Protocol (RTP) are the protocols used in the transport layer.

- **Application layer—layer 4**

  The application layer provides data access to applications. It 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 client–server applications and other services that have well-known port numbers earmarked by the Internet Assigned Numbers Authority (IANA). The application layer uses

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the Hypertext Transfer Protocol (HTTP), telecommunications network Telnet, File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Simple Network Management Protocol (SNMP), Domain Name System (DNS), Simple Mail Transfer Protocol (SMTP), X Window System Core Protocol, and other application protocols.

TCP/IP Functions

- Handles high-level protocols, issues of representation, encoding, and dialog control
- Constitutes a logical connection between the endpoints and provides transport services from the source to the destination host
- Selects the best path through the network for packets to travel
- Defines how to transmit an IP datagram to other devices on a directly attached network

TCP/IP Protocols

- File transfer (TFTP, FTP, and Network File System (NFS)), email (SMTP), remote login (Telnet and rlogin), network management (SNMP), and name management (DNS)
- TCP and UDP
- IP, ICMP, ARP, and RARP.
- Ethernet, Fast Ethernet, Serial Line Internet Protocol (SLIP), Point-to-Point Protocol (PPP), FDDI, Asynchronous Transfer Mode (ATM), Frame Relay, Switched Multimegabit Data Service (SMDS), ARP, Proxy ARP, and RARP.

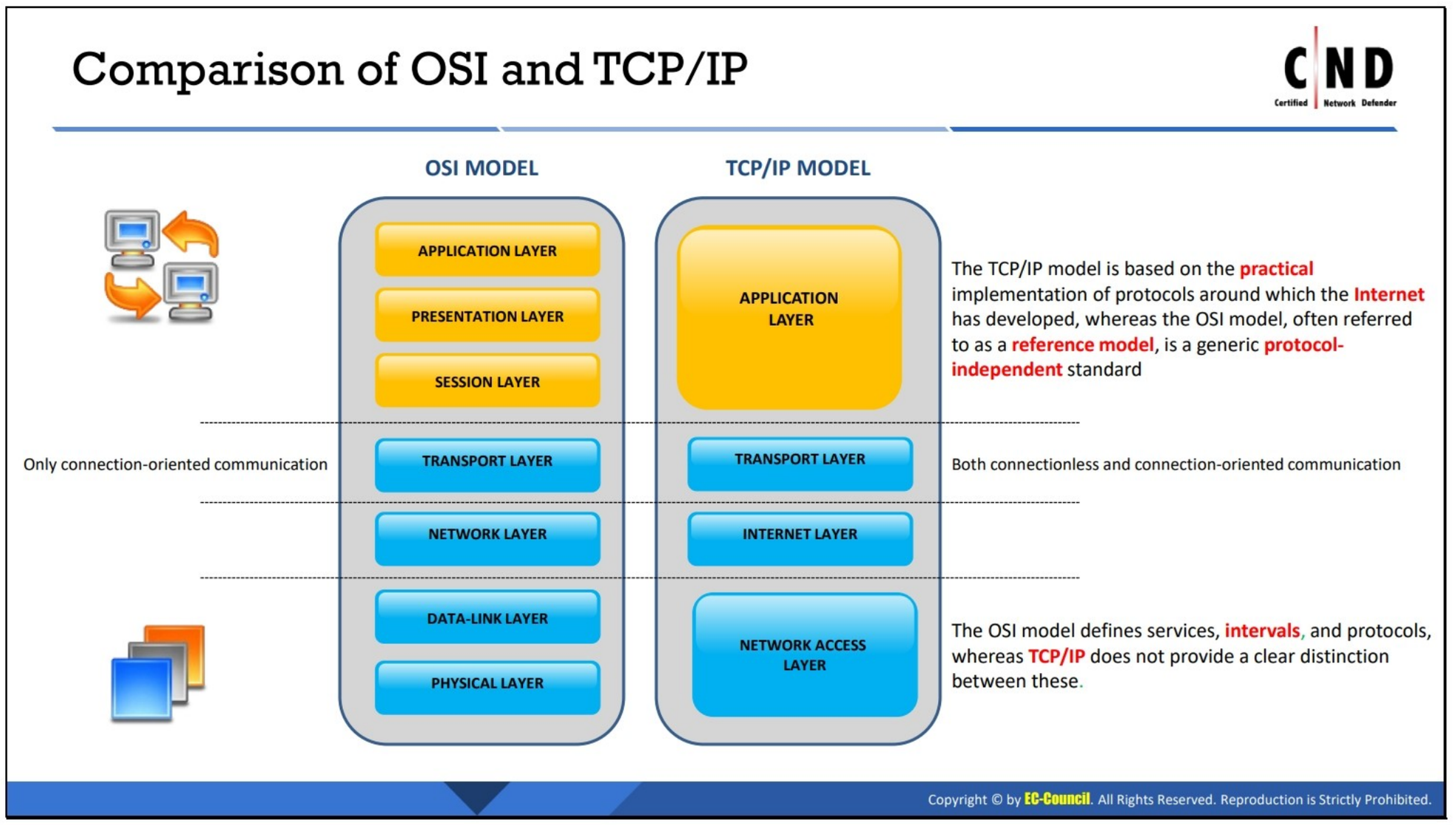
Advantages of the TCP/IP Model

- Serves as a client–server architecture
- Functions independently
- Consists of many routing protocols
- Initiates a connection between two computers

Disadvantages of the TCP/IP Model

- Complex to set up
- Difficult to replace protocols
- No visible partitioning between services, protocols, and interfaces

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Comparison of OSI and TCP/IP

OSI Model

The main aim of implementing the OSI model is to standardize and ease the communication between communicating parties by using certain standard protocols. It generalizes the communication between 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. It is only connection-oriented communication.

TCP/IP Model

TCP/IP remains the basic protocol for communication. TCP/IP is applied either in an intranet or 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 correct destination.

The TCP/IP model is based on the practical implementation of protocols around which the Internet has developed, whereas the OSI model, often referred to as a reference model, is a generic protocol-independent standard for both connectionless and connection-oriented communication. The OSI model defines services, intervals, and protocols, whereas TCP/IP does not provide a clear distinction between these.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Networks

- **Classification of networks based on the physical location or geographical boundaries.**

Local Area Network (LAN)

- Usually **possessed** by private organizations and connects the nodes of a single organization or **premises**
- Designed to facilitate the sharing of resources between **PCs** or **workstations**

Wide Area Network (WAN)

- Provides transmission solutions for companies or groups that need to exchange information between multiple remote locations, which may be in different countries or even continents
- Provides **trustworthy**, **quick**, and **secure communication** between two or more places with **short delays** and at low costs

Metropolitan Area Network (MAN)

- Huge computer networks **covering** a whole city
- Can be completely owned and **monitored** by a private organization or can be provided as a service by any public organization such as a **telecommunications** company

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Networks (Cont'd)

04 Personal Area Network (PAN)

- Wireless communication that uses both **radio** and **optical** signals
- Covers an individual's work area or work group and is also known as a **room-size network**



05 Campus Area Network (CAN)

- Covers a **limited geographical area**
- Applicable to a **university** campus



06 Wireless Networks (WLAN)

- Uses radio frequency (RF) signals to connect wireless-enabled devices in the network
- Uses IEEE standard 802.11



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Networks

These networks may differ in many aspects such as size, functions, and geographical distance. The services provided by the networks differ according to their layout. The networks that differ in size depend on the area occupied by the network and the number of computers present in the network. The number of computers in a network can vary from one to millions.

The following are different networks based on the size of the area they cover:

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Local area network (LAN)
- Wide area network (WAN)
- Metropolitan area network (MAN)
- Personal area network (PAN)
- Campus area network (CAN)

Local Area Network

A LAN consists of computers and related devices that share information over the same communication line. LANs are usually possessed by private organizations, and they connect the nodes of a single organization or premises. They are designed to facilitate the sharing of resources between PCs or workstations. A LAN may extend only within an office building or home. It can handle hundreds of users. Two commonly used LAN technologies are Ethernet and Wi-Fi. There are also virtual LANs that enable network defenders to provide a network connection to a group of nodes. A LAN enable the use of many application programs, and users can access those applications by simply downloading it from the LAN. Wireless LANs are becoming increasingly popular because they provide more flexibility at a lower cost than wired LANs.

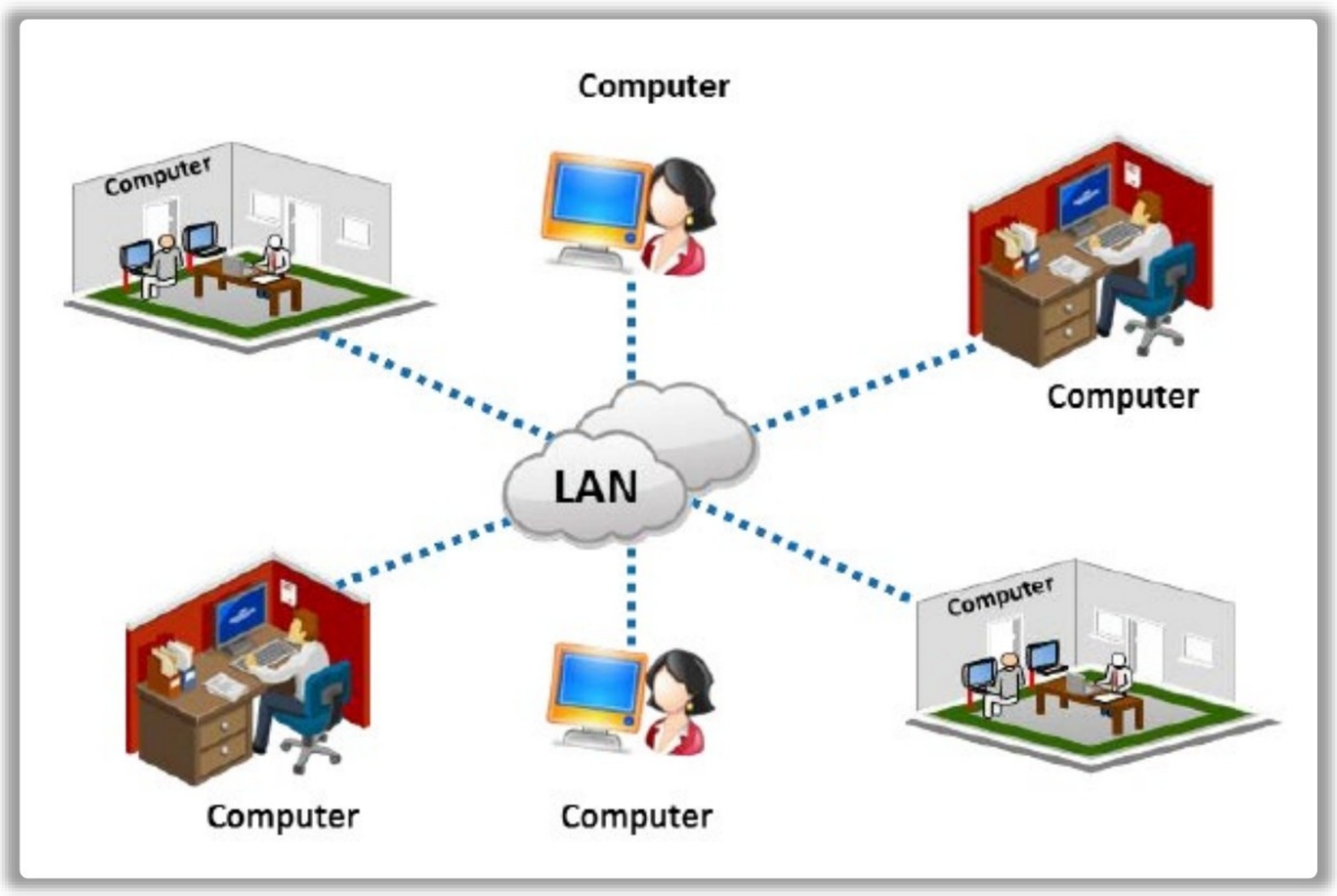


Figure A.3: LAN (Local Area Network)

- **Advantages:**
  - Allows the sharing of printers among computers at home or office
  - Provides users the privilege to work from any system in the LAN
  - Allows the storage of files in a single folder and sharing among users on the network

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Disadvantages:**
  - As it provides a 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

A WAN is spread over a larger geographical area and is more far-reaching than a LAN. WANs usually connect the nodes in their networks using leased telecommunication lines. These lines assist in carrying information efficiently across various computers in the network. WANs can connect different LANs in a network. Most often, public networks are connected to a WAN. LANs are connected to WANs for quick and secure data transfer. However, WANs require a group of authorities for management. WANs provide transmission solutions for companies or groups that need to exchange information among multiple remote locations, which may be in different countries or even continents. It provides trustworthy, quick, and secure communication between two or more places with short delays and at low costs.



Figure A.4: Wide Area Network

- **Features of WAN:**
  - WAN networks generally provide large and dedicated network services. They always attempt to provide the services according to business requirements.
  - WANs have lower data transfer rates than LANs.
- **Advantages:**

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- A WAN connects places that are geographically apart from each other without a high cost or difficulty in implementation.

- **Disadvantages:**
  - Very complex in structure
  - Provides a low bandwidth and has a relatively high risk of connection losses

Metropolitan Area Network

A MAN covers a geographical area that is larger than that covered by a LAN but smaller than that covered by a WAN. A MAN is an interconnection of networks spread across a city or town and consists of huge computer networks covering a whole city. It can be completely owned and monitored by a private organization or provided as a service by a public organization such as a telecommunications company. Several LANs grouped together form a MAN. MANs provide secure, efficient communication by utilizing fiber-optic cables. A MAN provides shared network connections to its users.

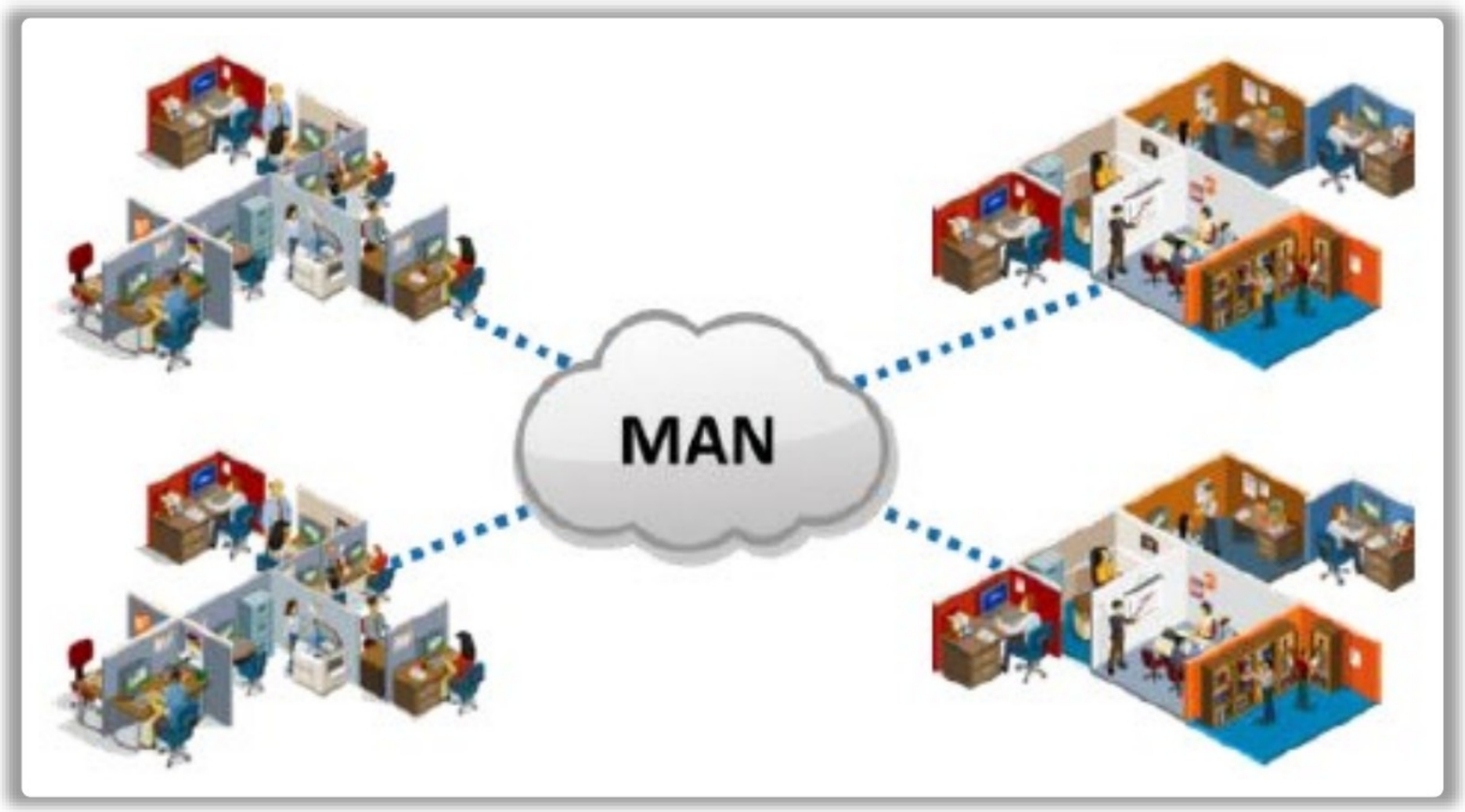


Figure A.5: Metropolitan Area Network

- **Advantages:**
  - The links connecting the computers in a MAN have a relatively high bandwidth, allowing for the easy sharing of data.
  - It allows multiple users to share data at the same speed.

- **Disadvantages:**
  - Requires installation before deployment
  - Costlier than LANs

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Personal Area Network

A PAN is the interconnection of devices within a certain distance. For example, a person can connect a laptop, smartphone, tablet etc. to a wireless network within a certain distance without having to physically plug in the devices. This allows for file and information sharing among the devices connected to that network. A PAN provides wireless communication through both radio and optical signals. It covers an individual's work area or work group and is also known as a room-size network.

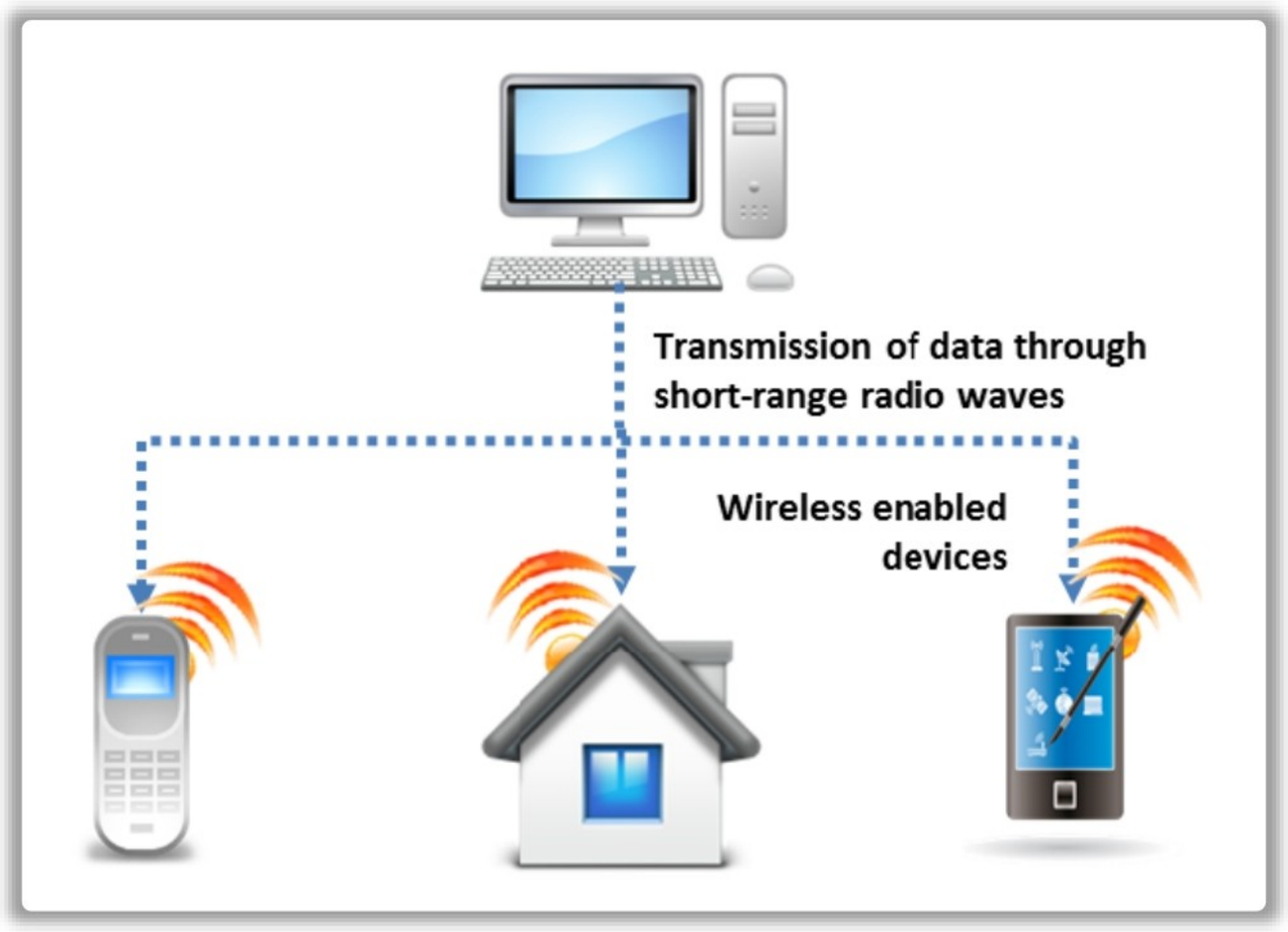


Figure A.6: Personal Area Network

Campus Area Network

A CAN consists of multiple LANs connected within a certain geographical area. Most government organizations and universities make use of CANs. A CAN covers a geographical area much smaller than those covered by a MAN or WAN. It uses optical fibers to connect the nodes in its network. For example, different buildings in a campus can use a CAN for interconnection, thereby allowing the sharing of information within different departments. The implementation of a CAN is relatively less expensive. It is highly beneficial and economical owing to its high data transfer speeds from any section of the network.

- **Features:**
  - Cost-effective
  - Allows interconnection between various departments in a campus
  - Provides a single shared data transfer rate
  - Resistant to failure
  - Highly flexible and accommodates the changes to an evolving network
  - Offers a highly secure network by implementing the authentication of the users accessing the network.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Networks

WLANs use radio frequency (RF) signals to connect wireless-enabled devices in the network. It uses IEEE standard 802.11 for communication.

- **Advantages**
  - Installation is easy and does not require wiring.
  - The network can be accessed from anywhere within the range of an access point.
  - Public places such as airports and schools can offer constant Internet connection using WLANs.
- **Limitations**
  - Wi-Fi security may not meet expectations.
  - The bandwidth available to a user decreases as the number of users on the network increases.
  - Wi-Fi standard changes may necessitate the replacement of wireless components.
  - Some electronic equipment can interfere with Wi-Fi networks.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Network Topologies

- Network topology is a specification that **deals with a network's overall design and the data flow** 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 a central cable, called a bus, with 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 travel from node to node, with each node along the way handling every packet

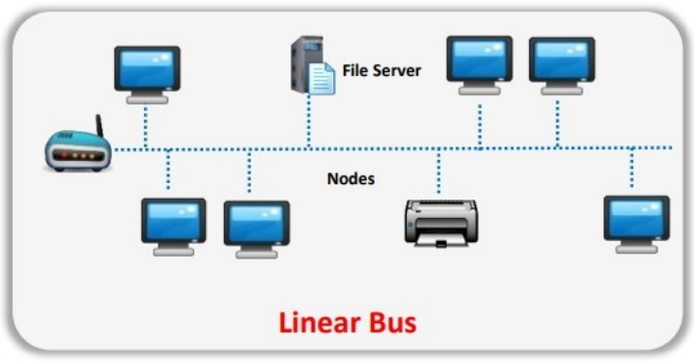
Mesh Topology
Network devices are connected in such a manner that every device has a point-to-point link to every other device on the network

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

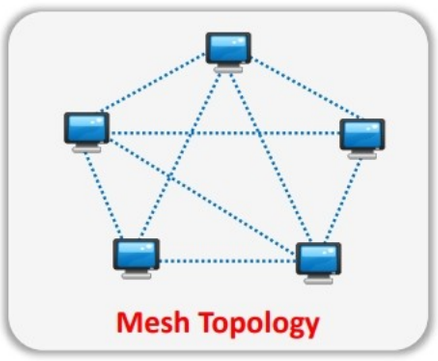
Hybrid Topology
It is a combination of two or more topologies. Star-bus or star-ring topologies are widely used

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

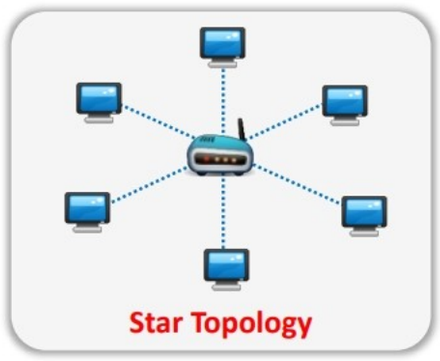
Network Topologies (Cont'd)



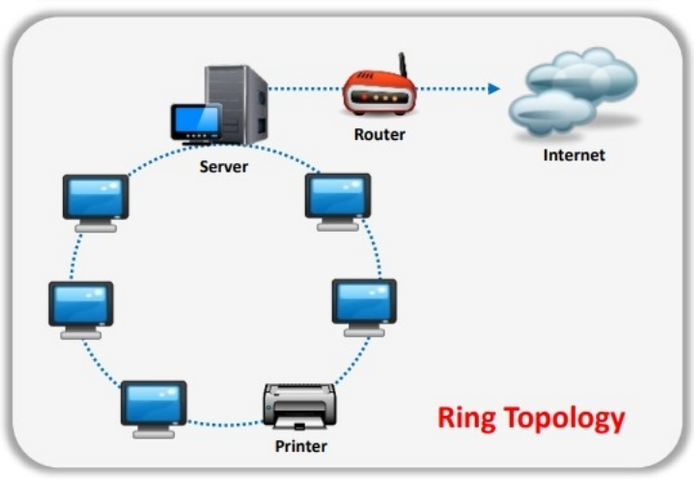
Linear Bus



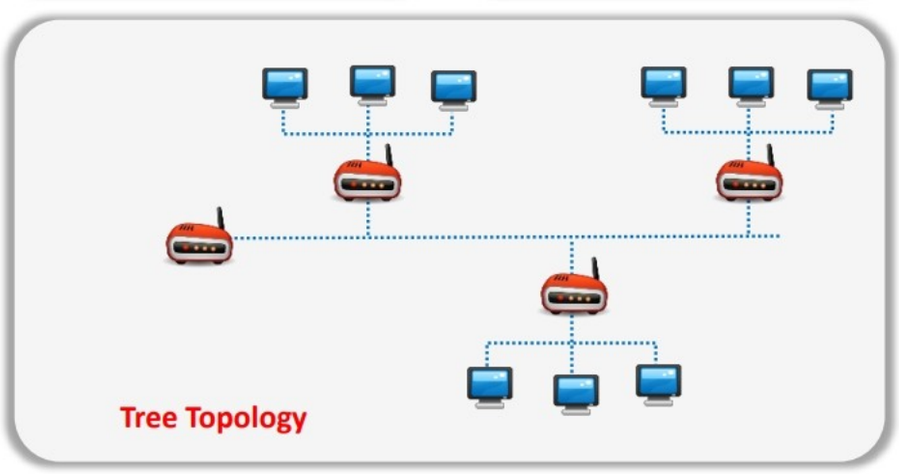
Mesh Topology



Star Topology



Ring Topology



Tree Topology

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Topologies

The network topology is a specification that deals with a network's overall design and the flow of data in it. The logic of connecting computers over a network is possible using topologies. A topology defines the structure of a network and determines its physical or logical layout.

Types of Topology

- **Physical topology**: Physical layout of nodes, workstations, and cables in the network

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Logical topology**: The way information flows between different components

The physical topology defines the structure of the components of the computer systems in the network, whereas the logical topology defines the method of data flow in the network between the computers.

The following are some physical network topologies.

- **Star topology**

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

  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. However, 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 pass 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 (UTP) Ethernet cables.

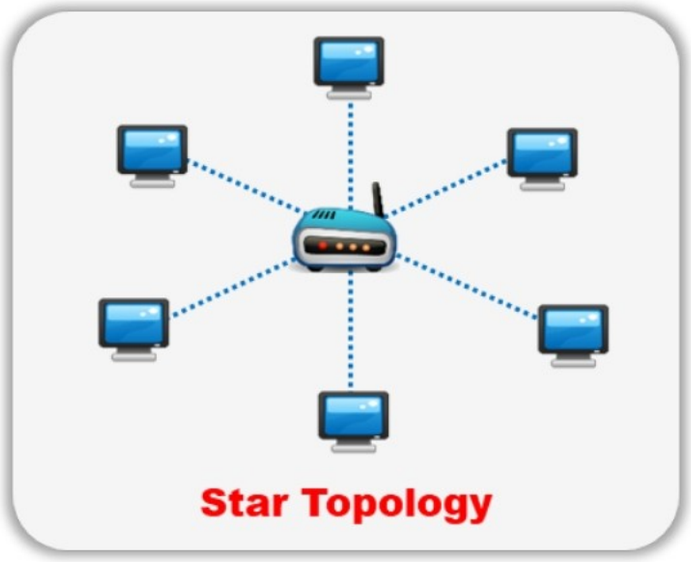


Figure A.7: Star topology

The following factors determine whether the hub is active:

- The central node or hub performs processes such as data amplification and regeneration.
- The central node regulates the movement of the data.
- The network requires electrical power resources.

Advantages:

- The star topology enables the centralized management of the network through the central node or hub.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- It enables easy addition and removal of other computer nodes to the star network.
- The failure of one computer node does not impact the rest of the nodes in the network.
- It enables the easy detection of failures and errors in the network, allowing 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**

  In this topology, network devices are connected to the central cable, called a bus, by the help of interface connectors. Here, a single cable handles all the computers in the network, i.e., it carries all the information intended for all the nodes in the network. Any damage to the connection between any node and the main cable can affect the transmission of data over the cable.

  In a 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 the IP and media access control (MAC) address given in the signal accepts it, while the other nodes reject the signal. Every cable in the bus network has a terminator attached to both ends. 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 simultaneously from opposite directions, the signals may collide. There are two types of bus topologies: linear and distributed bus topology. In a linear bus topology, only a single line is attached to the two end points. On the other hand, a distributed bus topology can have more than one linear pattern attached to the network.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

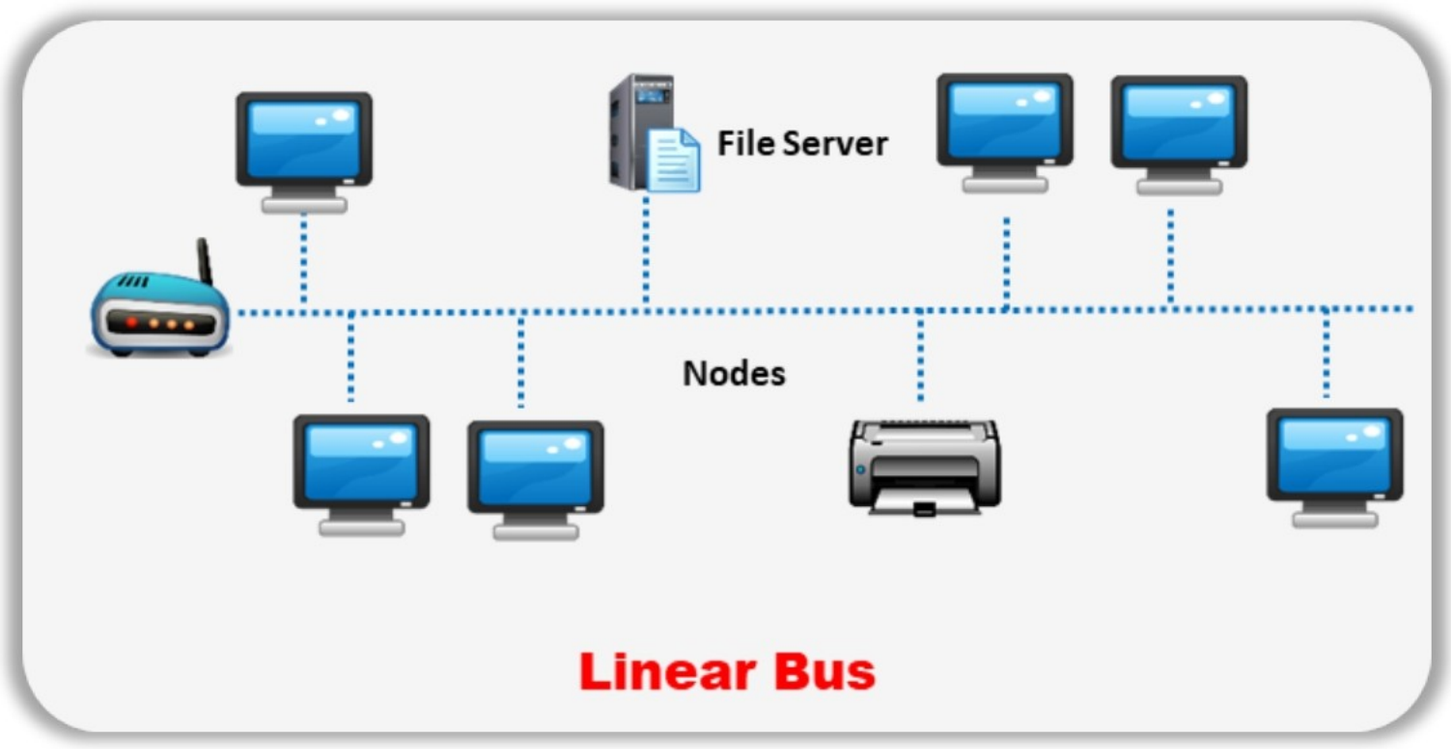


Figure A.8: Bus Topology

Advantages:

- Easy to add new nodes to the bus network
- Low implementation cost
- Works well in small networks
- Requires less cabling than a star network

Disadvantages:

- The addition of computer nodes depends on the cable length.
- Any issue in the main cable can affect the whole network.
- Terminators are mandatory at both ends of the cable.
- Maintenance is very expensive.
- It is not suitable for networks with exceedingly high traffic.
- As all nodes receive the signal sent from the source, the network security is poor.

- **Ring topology**

  In this topology, network devices are connected in a closed loop. Data travel from node to node, with each node along the way handling every packet. A ring topology connects all nodes in the network. The data circulate 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 travel on the network in one direction, and the sending and receiving of data occur with the help of a token. In the concept of a token, the data are sent from the source and include another piece of information called the token. The token is passed to the next node. Each node checks whether the signal is for itself. If yes, it receives the signal and passes the empty token to the network. 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

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

receive the empty token. Usually, schools, offices, and small buildings utilize ring topologies.

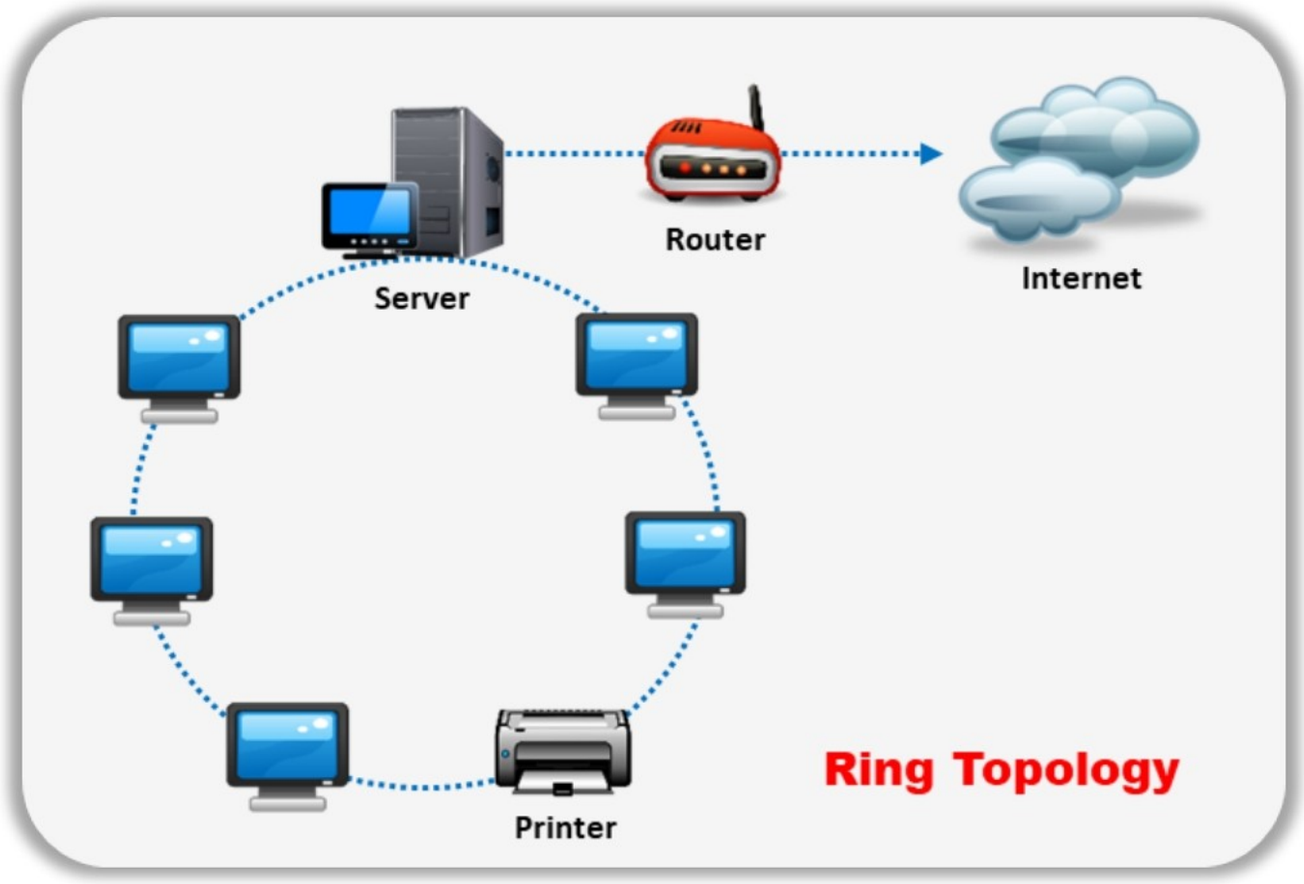


Figure A.9: Ring Topology

Advantages:

- The flow of traffic is unidirectional.
- Every node can send data after receiving the empty token.
- No centralized network server is needed to manage the computer nodes.
- It shows better performance than the bus topology in scenarios with a high traffic load.
- 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:

- The process is slow 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.
- It needs a large number of wires for connecting the network nodes, resulting in a high cost of implementation.
- The bandwidth is shared among all the nodes.

- **Mesh topology**

  In this topology, network devices are connected in such a manner that every device has a point-to-point link to every other device on the network. All the nodes or computers in the network are connected with each other. The design confirms the transmission of data

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

through every computer even in the case of failure of any one computer. Each node in the network sends data to other nodes and passes the data from other nodes. The mesh topology does not find much use in organizations owing to its huge implementation cost and is widely used in wireless networks.

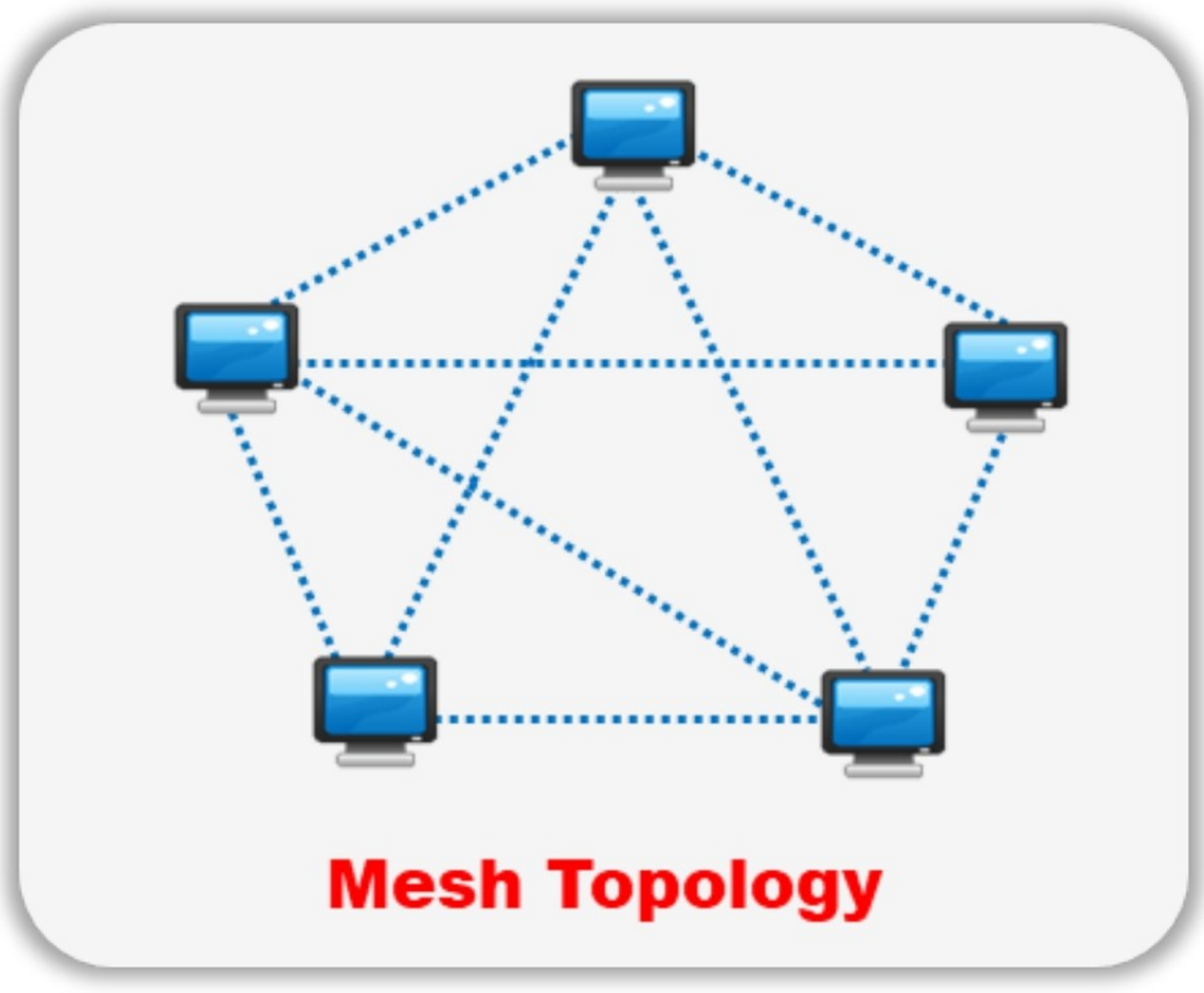


Figure A.10: Mesh Topology

There are two types of mesh topologies.

- **Full-mesh topology**: All the nodes are connected with each other in the network. If any node fails, the full-mesh topology can redirect the traffic from that node to another node.
- **Partial-mesh topology**: Very few nodes are connected to all nodes in the network, and other nodes are connected only to one or two other nodes. Consequently, the partial-mesh topology is far less costly and minimizes the redundancy of many connections.

Mesh topology uses either routing or flooding. In the routing process, the topology realizes data transmission through a path between nodes. In order to ensure continuous data transmission between the nodes, the topology needs to ensure that all connections between the nodes are working properly.

Advantages:

- It allows the continuous transmission of data.
- It can handle heavy traffic loads.
- A node failure does not impact the whole network.
- It allows the expansion and modification of networks without disturbing the network.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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 relatively more administrative attention

- **Tree topology**

The tree topology is a hybrid of bus and star topologies, in which groups of star-configured networks are connected to a linear bus backbone cable. It essentially consists of a main cable line attached to a star network. Many star topologies are connected to the central transmission cable. Another name for this model is "extended star topology."

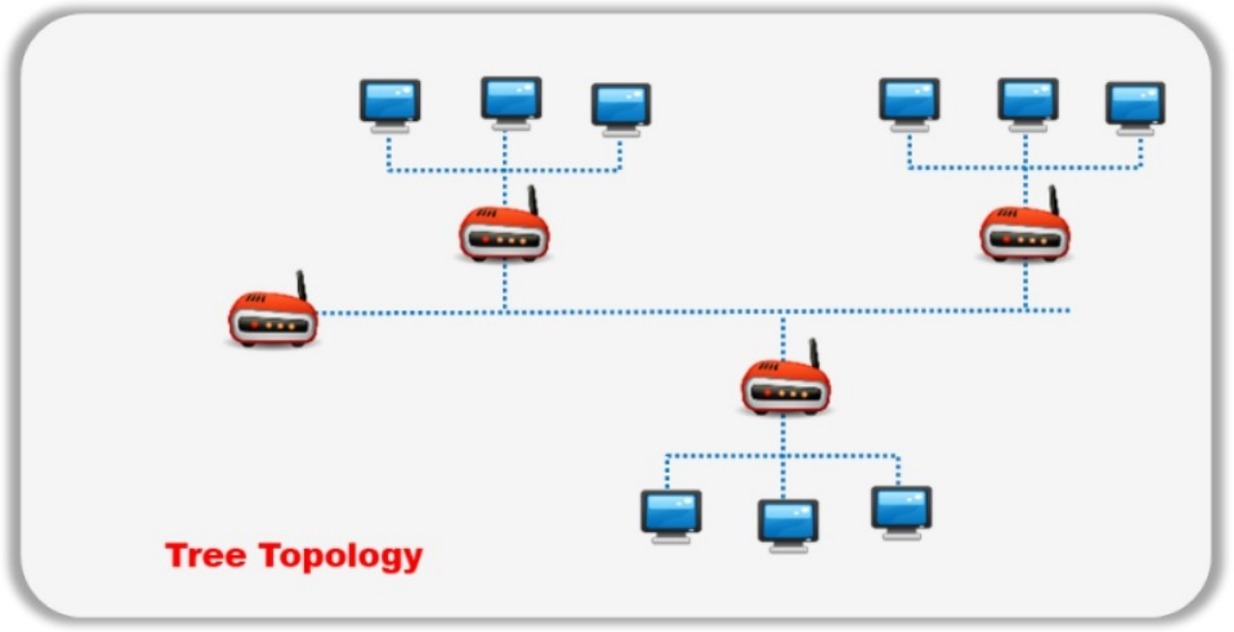


Figure A.11: Tree Topology

Advantages:

- Tree topology is useful in scenarios where it is difficult to implement star or bus topology.
- It allows easy expansion of the network.
- The star topology layout design enables the easy management of nodes.
- It provides error detection and correction properties.
- Each star network connects to the main cable through wiring.
- The 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 the easy expansion of the network, it is difficult for the network as a whole to manage entire nodes and segments.
- The rate of expansion depends solely on the type of main cable used.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Hybrid topology**

  A hybrid topology is a combination of any two or more different topologies. Star–bus or star–ring topologies are widely used. These are mainly used in WANs. Organizations implement hybrid topologies according to their requirements. For example, if one section of an organization needs a bus topology while another section needs a ring topology, the organization can implement both these topologies as a hybrid topology. Hybrid topologies combine multiple topologies into a single large topology.

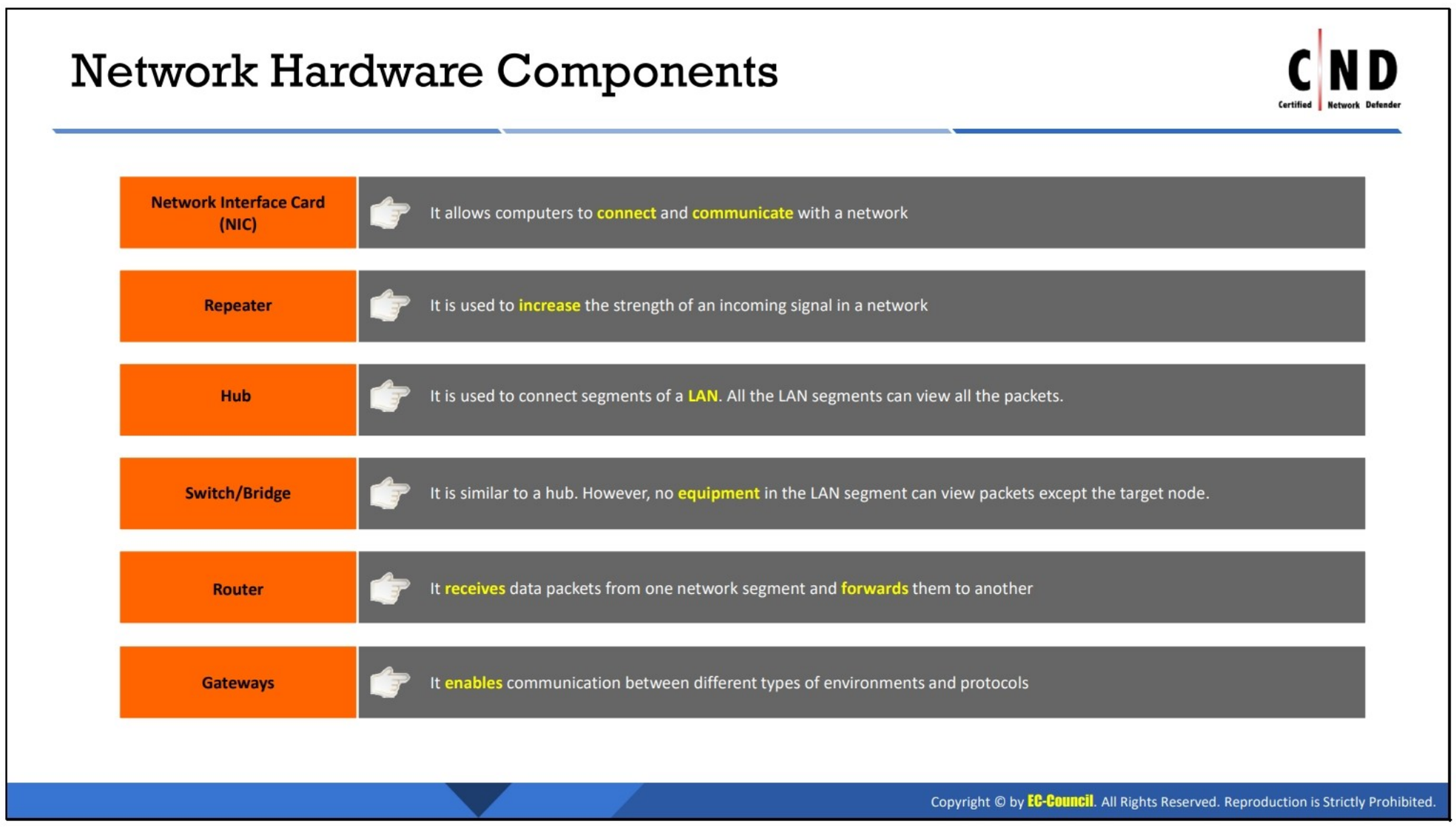
  Advantages:

  - Provides error detection and correction without affecting the working of other sections of the network
  - Allows the easy addition of nodes
  - Allows organizations 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 must ensure that the designed architecture can provide the required throughput.
  - The implementation of a hybrid topology is costly, as it includes relatively more cabling and connections.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Hardware Components

- **Network interface card (NIC)**

  Connecting to a network is an integral part of computing. Computers use an NIC for connecting and communicating with a network. They connect to wired as well as wireless networks using electronic circuitry. NICs are also known as network interface controllers, network adapters, LAN adapters, etc. They provide computers with a dedicated full-time connection to a network. The computers on a LAN contain an NIC that enables LAN transmission.

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

  - Transmission of data from one computer to another
  - Gathering of data to transmit through the network cable
  - Handling of the data transmission from the computer through the data cable
  - Reception of the data from the cable and conversion to bytes for processing by the CPU

  NICs are commonly used in Ethernet connections, and the available configurations are 10BASE-T, 100BASE-T, and 1000BASE-T. Recent computers are configured with Ethernet capabilities in the motherboard chipset. An Ethernet chip installed directly on the motherboard using a Peripheral Component Interconnect (PCI) or PCI Express (PCIe) bus is another method for connecting. This minimizes the need for a separate NIC. In some situations, an NIC is integrated as components in a router, USB device, etc.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

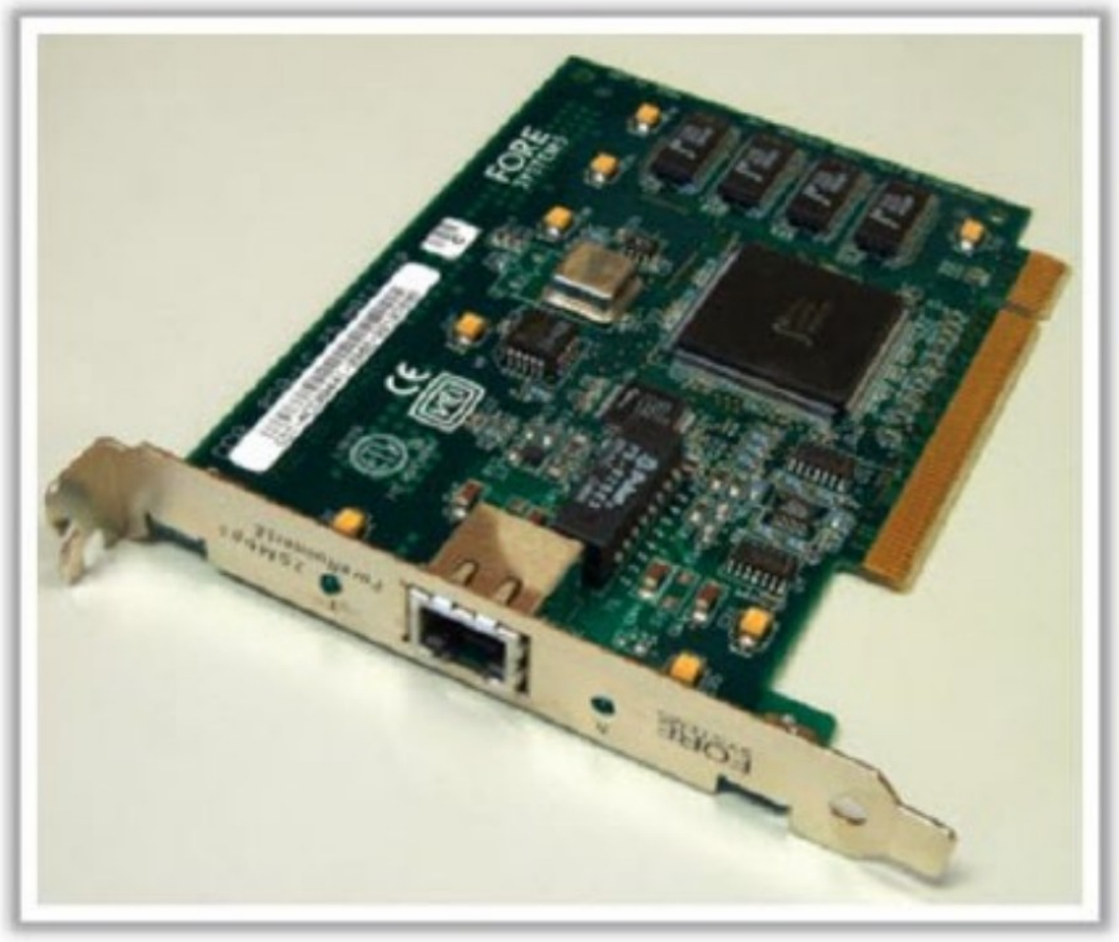


Figure A.12: NIC Card for Wired Networks



Figure A.13: Wireless PC Network Adapter

- **Repeater**

  A repeater is used to increase the strength of an incoming signal in a network. Repeaters are network devices that are generally used for the restoration or repetition of a signal. Repeaters can restore analog and digital signals affected by transmission loss. Repeaters

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

can only amplify analog signals, but they can restore digital signals to their original quality. Repeaters can also pass data between various subnetworks carrying different protocols.

The following are different types of repeaters.

- **Telephone repeater**:

  A telephone repeater helps in increasing the telephone signal range in telephone lines. The repeater is applied in trunk lines carrying long-distance signals. Telephone signal lines made of a pair of wires contain an amplifier circuit that uses direct current (DC) power to increase the power of the alternating current (AC) audio signal on the line.

- **Optical communications repeater:**

  Optical communications repeaters mainly increase the signal strength of fiber-optic cables. These cables carry digital information in the form of short light pulses. Light is made up of particles called photons.

- **Radio repeater:**

  Radio repeaters increase the signal strength of radio signals. A radio repeater amplifies and retransmits radio signals using a radio receiver connected to a radio transmitter.

A normal LAN implementation usually limits the physical size of a single cable segment according to the physical medium and the techniques used for transmission. 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 same physical layer protocol to send signals over all the cable segments.

Advantages of repeaters:

- Remarkably simple to use
- Inexpensive implementation
- Strengthens signals

Disadvantages of repeaters:

- Repeaters augment the traffic on the network and occasionally transmit errors.
- There is a limit on the number of repeaters that can be used across a network.
- Users cannot monitor or inspect repeaters through an inaccessible area, and repeaters do not have the ability to separate or filter the traffic.
- Different segments of repeaters must be inspected thoroughly and periodically. Otherwise, the repeaters operating on different segments and different media may become compromised.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Hub**

  A hub is a network device used to connect multiple network devices or segments of a LAN. It works in the half-duplex mode. All the LAN segments can access all the packets. The main activity of the hub is to forward the data arriving from one device to another device or port. Some hubs even work as a repeater that helps in amplifying signals. The hub is a common point of connection for many devices in the network. It can contain a sequence of ports to connect network cables. Upon the arrival of a packet at any port, the hub floods the packet out through all other ports so that all segments receive a copy. The smallest hub can connect four computers to a network and has an extra port for uplink to other hubs in the network. Hubs come in different sizes with up to 12, 16, or 24 ports.

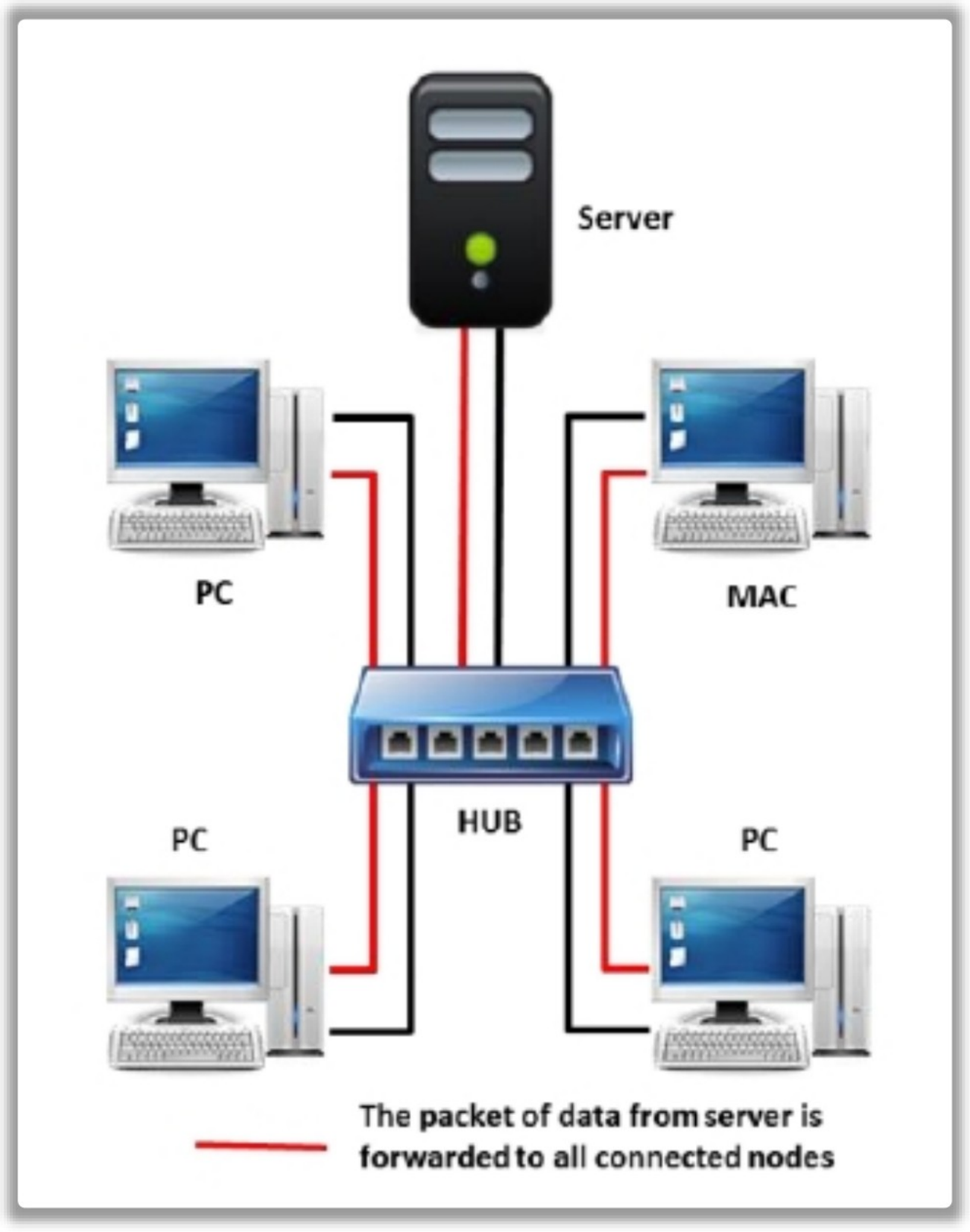


Figure A.14: Hub

The types of hubs include the following.

- **Passive hubs:**

  Passive hubs do not intensify the signal strength of the data prior to transferring data packets, but they act as a means to transfer data between the devices in the network.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Active hubs:**

  Active hubs strengthen the signal prior to transferring it to other devices in the network, similar to a repeater. Since it has multiple ports, it is also called a multiport repeater.

- **Intelligent hubs:**

  Intelligent hubs regenerate signals instead of amplifying them, removing restrictions on how many hubs a signal can cross before being nulled.

Advantages:

- It is a flexible, simple, and economical device.
- Active hubs can increase the length between nodes.
- Adding hubs increases the number of ports.

Disadvantages:

- Hubs cannot help control traffic.
- Data transfer rates decrease substantially with the increase in devices connected.

- **Switch/bridge**

  A switch or bridge is similar to a hub, but in a network using it, no equipment in the LAN segment other than the target node can view the packets. 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 an 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 networking switch functioning in the full-duplex mode is a machine on the LAN that can receive and send data simultaneously. The 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.

  A switch can break the collision domain to prevent network congestion. Each port of a switch is in a different collision domain, and the messages from different devices connected to different ports do not collide. However, a switch cannot break broadcast domains because the ports of a switch are in a single broadcast domain and the messages sent by a device connected to the switch might cause congestion.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

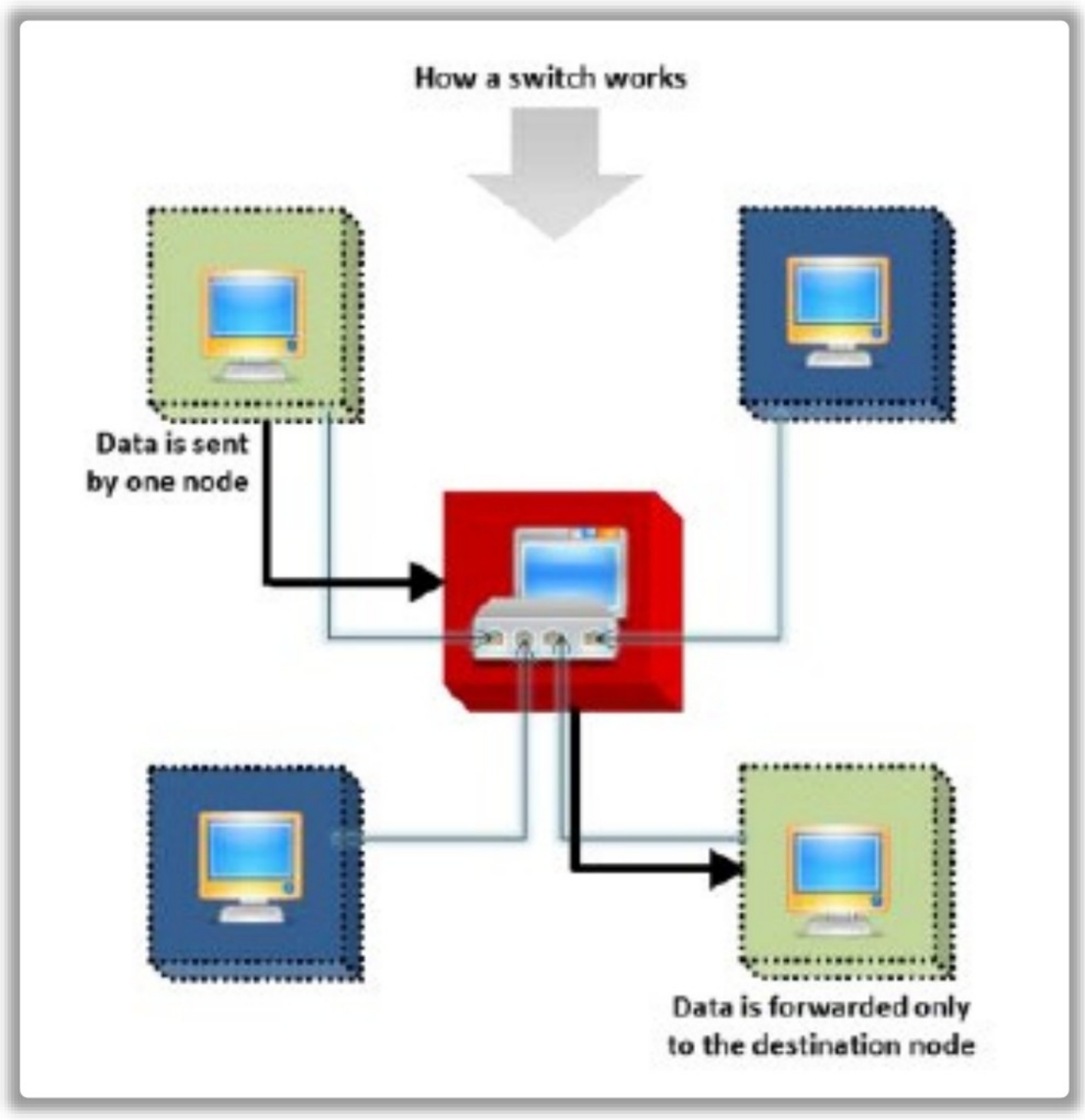


Figure A.15: Working of a Switch

Advantages:

- A networking switch has more advanced features than a networking hub.

Disadvantages:

- A networking switch is not infallible, as an attacker can mislead it by employing packet sniffers.

- **Router**

A router receives data packets from one network segment and forwards them to another. Routers are more complicated than other devices such as repeaters and bridges. It works in the full-duplex communication mode. Routers can access the addresses of the network layer and have embedded software that helps them identify the exact destination address. They examine the multiple paths available between the addresses and check the channel that is appropriate for the transmission of data.

Routers function at the network layer of the OSI model and transmit packets among several interconnected networks. They send packets from a network to other important destinations in a network. A packet sent from one destination to another travels through the router initially and then moves to the other destination in the network. The destination router, in turn, transmits the packet until it reaches the final destination. Routers behave as stations on the network, although they contain addresses and connect

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

to more than two networks simultaneously, irrespective of the stations to which they belong.

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 to transmit the packet, the router accurately transmits the packet along the network to other networks. If it finds the path as inappropriate, it sends the packets to a surrounding network or an adjacent router to select the next-best path.

A router keeps a routing table to maintain the paths through which the routing occurs and minimize excess costs for routing across a network. Static routing is a type of routing in which the network defender monitors entire routing processes. Routing includes many concepts such as least-cost routing, which allots economic paths for routing, i.e., selects the shortest available path. The shortest path in terms of routing should also be secure and fast. Some routers also route packets across networks that use more than one protocol.

Routers can be associated with different networks such as LANs and WANs to broadcast data. They prevent collisions of data packets during a broadcast. Occasionally, 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 is configured) and then sends them 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 available path.

The router can break both collision domains and broadcast domains to prevent network congestion since it can create a connection between two networks and a broadcast message sent from one network will be stopped from passing to another network.

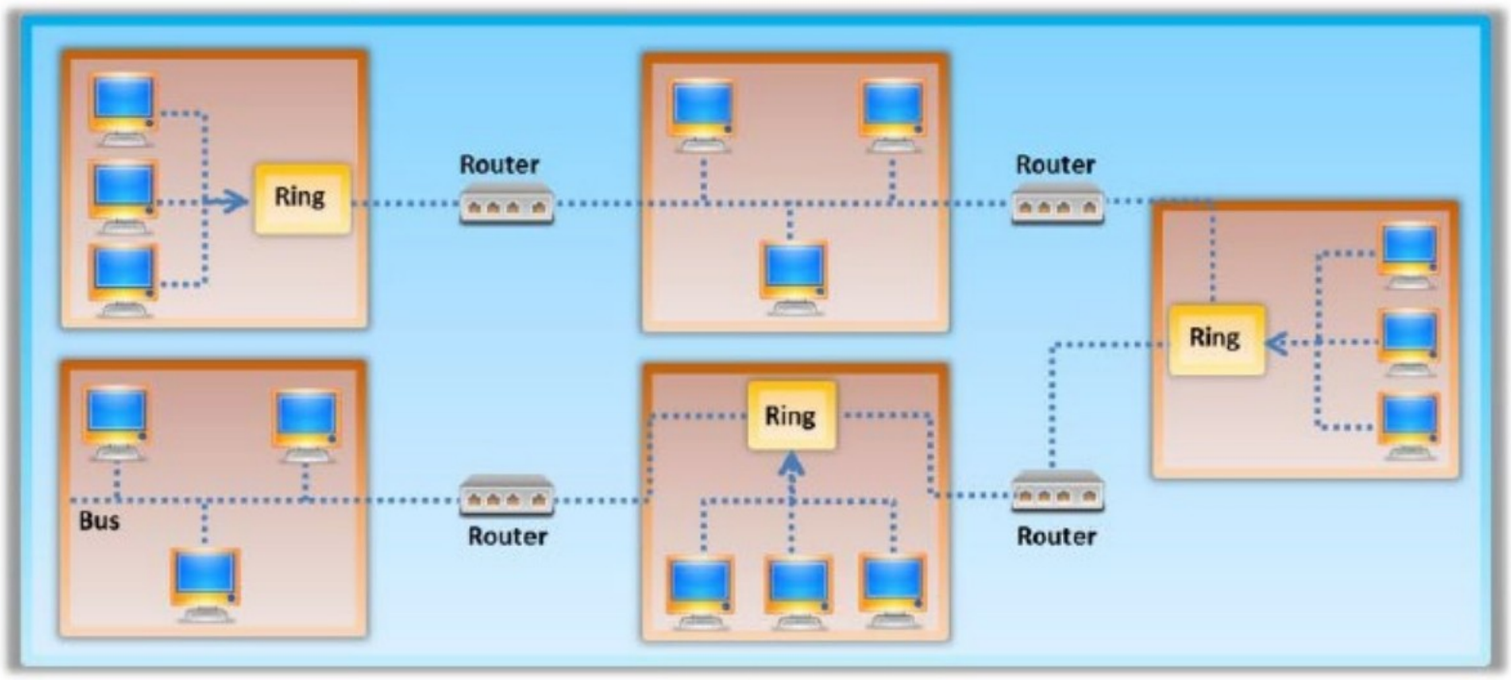


Figure A.16: Working of Routers

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Advantages:

- Operation at the protocol level
- Remote management and design via SNMP
- Support for intricate networks
- Greater filtering and lower performance
- Provides security
- Uses complicated routing protocols such as Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), and Open Shortest Path First (OSPF)

Disadvantages:

- Routers have security issues because they do not have very efficient security controls, which may cause the system to be compromised.
- Routers cause long delays in initializing the sessions for protocols such as FTP.

Check the following aspects before starting a transmission through routers:

- Mapping between ports
- Internal addresses
- External addresses
- Port numbers of the internal and external addresses
- Routers are more expensive than other devices.
- Routers need only protocols designed for routing.
- Routers are slower than other devices.
- Routers lead to overhead.

- **Gateways**

Gateways enable communication between different types of environments and protocols. They act as an entry point for other networks that attempt to connect to an internal network. In the same manner, gateways act as an exit point for an internal network that attempts to establish a connection to external networks. A gateway can be a workstation or server that performs two-way communication between networks and expands its area. The application and transport layers of the OSI model support gateways. They are capable of connecting devices that have different protocols and environments. They convert different protocols by assigning matching protocols to packets and are called protocol translators. If 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 they can occasionally transmit malicious packets without filtering. There are two types of gateways.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Transport gateways:

- They are capable of connecting different devices with a connection-oriented transport protocol.
- They can transfer packets from one connection to another by restructuring/reformatting.

Application gateways:

- They are intelligent components that can understand the format/contents of the data and then permit transmission.
- Email gateways translate messages and transfer them to mobile devices.
- They act as a firewall or proxy server to restrict unauthorized traffic.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of LAN Technology

Ethernet

- Ethernet is the **physical layer** of LAN technology. It maintains proper balance between the speed, cost, and ease of installation
- It describes the number of conductors required for establishing a connection, defines the required performance thresholds, and offers a framework for data transmission
- A standard Ethernet network can send data at a rate of up to 10 megabits per second (10 Mbps)
- The Ethernet standard, IEEE standard 802.3, specifies **configuration rules** for an Ethernet network and states the interaction of the elements in a network

Fast Ethernet

- The Fast Ethernet standard, IEEE 802.3u, is a new version of Ethernet that transmits data at a minimum rate of 100 Mbps
- Three types of Fast Ethernet are available in the market: 100BASE-TX for use with level-5 unshielded twisted pair (UTP) cables, 100BASE-FX for use with fiber-optic cables, and 100BASE-T4 that utilizes two extra wires with level-3 UTP cables

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of LAN Technology (Cont'd)

Gigabit Ethernet

- Gigabit Ethernet was defined by the IEEE 802.3-2008 standard and conveys Ethernet frames at a rate of 1 **Gbps**
- It is used on fast communication networks such as multimedia and Voice over IP (VoIP)
- It is also called "gigabit-Ethernet-over-copper" or 1000BASE-T, as its speed is 10 times more than that of 100BASE-T

10 Gigabit Ethernet

- 10 Gigabit Ethernet was first defined by the IEEE 802.3ae-2002 standard
- It conveys Ethernet frames at a rate of 10 Gbps. This makes it 10 times faster than Gigabit Ethernet
- In contrast to other Ethernet systems, 10 Gigabit Ethernet uses optical fiber connections

Asynchronous Transfer Mode (ATM)

- ATM is a **cell-based fast-packet communication** standard developed for transmitting information of different types such as voice, video, and data, in small, fixed-sized cells
- It operates on the data-link layer through fiber or twisted-pair cables
- It is mainly used on private long-distance networks, especially by Internet service providers (ISPs)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of LAN Technology (Cont'd)

- **Power over Ethernet (PoE)**
  - PoE is a networking feature defined by the IEEE 802.3af and 802.3at standards
  - It allows Ethernet cables to **supply power to network devices** over an existing data connection
  - PoE-capable devices can be power sourcing equipment (PSE), powered devices (PDs), or both. PSE is the device that transmits power, whereas PD is the device that is powered

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of LAN Technology (Cont'd)

- **Specifications of LAN Technology**

Name	IEEE Standard	Data Rate	Media Type	Maximum Distance
Ethernet	802.3	10 Mbps	10BASE-T	100 m
Fast Ethernet/ 100BASE-T	802.3u	100 Mbps	100BASE-TX 100BASE-FX	100 m 2000 m
Gigabit Ethernet/ GigE	802.3z	1000 Mbps	1000BASE-T 1000BASE-SX 1000BASE-LX	100 m 275/550 m 550/5000 m
10 Gigabit Ethernet	IEEE 802.3ae	10 Gbps	10GBASE-SR 10GBASE-LX4 10GBASE-LR/ER 10GBASE-SW/LW/EW	300 m 300 m MMF/ 10 km SMF 10 km/40 km 300 m/10 km/40 km

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of LAN Technology

- **Ethernet**
  - Ethernet is a physical-layer LAN technology that maintains proper balance between speed, cost, and ease of installation.
  - It describes the number of conductors required for making the connection and the required performance thresholds, and it offers a framework for data transmission.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- A standard Ethernet network can send data at a rate of up to 10 Mbps.
- The Ethernet standard, IEEE 802.3, specifies configuration rules for an Ethernet network and states the interaction of elements in a network.

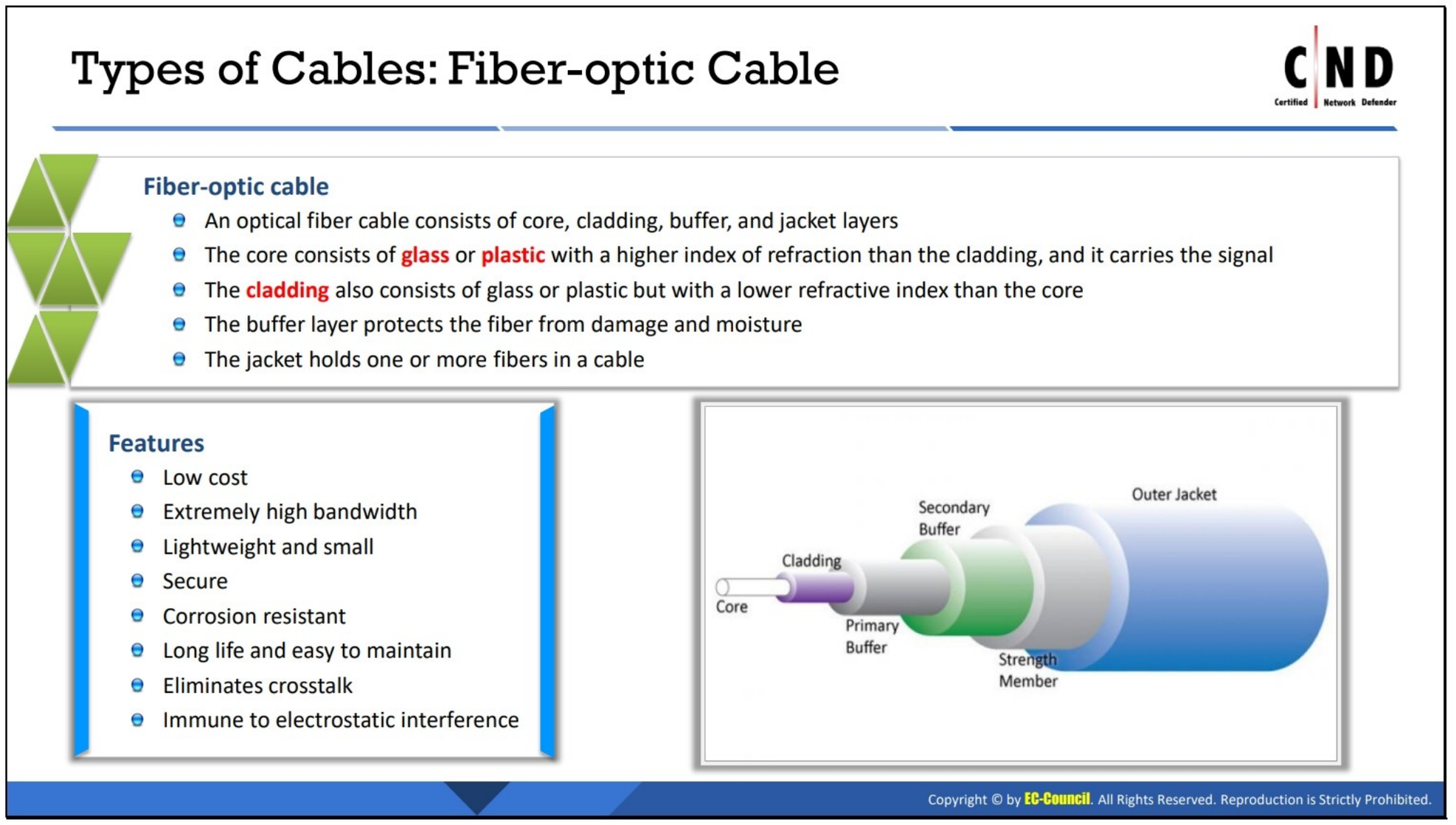
- **Fast Ethernet**
  - The Fast Ethernet standard, IEEE 802.3u, is a new version of Ethernet that transmits data at a minimum speed of 100 Mbps.
  - Three types of Fast Ethernet are available in the market: 100BASE-TX, for use with level-5 UTP cables; 100BASE-FX, for use with fiber-optic cables; and 100BASE-T4, for utilizing two extra wires with level-3 UTP cables.
- **Gigabit Ethernet**
  - Gigabit Ethernet was defined by the IEEE 802.3-2008 standard and conveys Ethernet frames at a speed of 1 Gbps.
  - It is used on fast communication networks such as multimedia and voice over IP (VoIP).
  - It is also called "Gigabit-Ethernet-over-copper" or 1000BASE-T, as its speed is 10 times that of 100BASE-T.
- **10 Gigabit Ethernet**
  - 10 Gigabit Ethernet was first defined by the IEEE 802.3ae-2002 standard.
  - It conveys Ethernet frames at a speed of 10 Gbps, making it 10 times faster than Gigabit Ethernet.
  - As compared to other Ethernet systems, 10 Gigabit Ethernet uses optical fiber connections.
- **Asynchronous Transfer Mode (ATM)**
  - The Asynchronous Transfer Mode (ATM) is a cell-based fast-packet communication standard developed for transmitting information of different types such as voice, video, and data, in small, fixed-sized cells.
  - It operates on the data-link layer through fiber or twisted-pair cables.
  - It is mainly used on private long-distance networks, especially by Internet service providers (ISPs).
- **Power over Ethernet (PoE)**
  - Power over Ethernet (PoE) is a networking feature defined by the IEEE 802.3af and 802.3at standards.
  - It allows Ethernet cables to supply power to network devices over an existing data connection.
  - PoE-capable devices can be power sourcing equipment (PSE), powered devices (PDs), or both. PSE is a device that transmits power, whereas PD is a device that is powered.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Name	IEEE Standard	Data Rate	Media Type	Maximum Distance
Ethernet	802.3	10 Mbps	10BASE-T	100 m
Fast Ethernet/ 100BASE-T	802.3u	100 Mbps	100BASE-TX; 100BASE-FX	100 m; 2000 m
Gigabit Ethernet/ GigE	802.3z	1000 Mbps	1000BASE-T; 1000BASE-SX; 1000BASE-LX	100 m; 275/550 m; 550/5000 m
10 Gigabit Ethernet	IEEE 802.3ae	10 Gbps	10GBASE-SR; 10GBASE-LX4; 10GBASE-LR/ER; 10GBASE-SW/LW/EW	300 m; 300 m multi-mode fiber (MMF)/10 km single-mode fiber (SMF); 10 km/40 km; 300 m/10 km/40 km

Table A.1: Specifications of LAN Technologies

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Cables: Fiber-optic Cable

Optical fiber cable consists of core, cladding, buffer and jacket layers. The core consists of glass or plastic with a higher index of refraction than the cladding, and it carries the signal. The cladding also consists of glass or plastic but with a lower refractive index than that of the core. The buffer protects the fiber from damage and moisture. The jacket holds one or more fibers in a cable.

Fiber-optic cables are made up of glass (or plastic) and are used for transmitting data (or signals) using light pulses. The IEEE 802.8 standard defines these cables. As they have high bandwidths, they are used for fast data communications. The outer layer of the cable contains a coating that protects it from catastrophic conditions due to heat, cold, and electromagnetic interferences. These cables are designed for achieving high performance during long-distance communications. To date, most long-distance wired networks such as the Internet and telephone networks use fiber-optic cables.

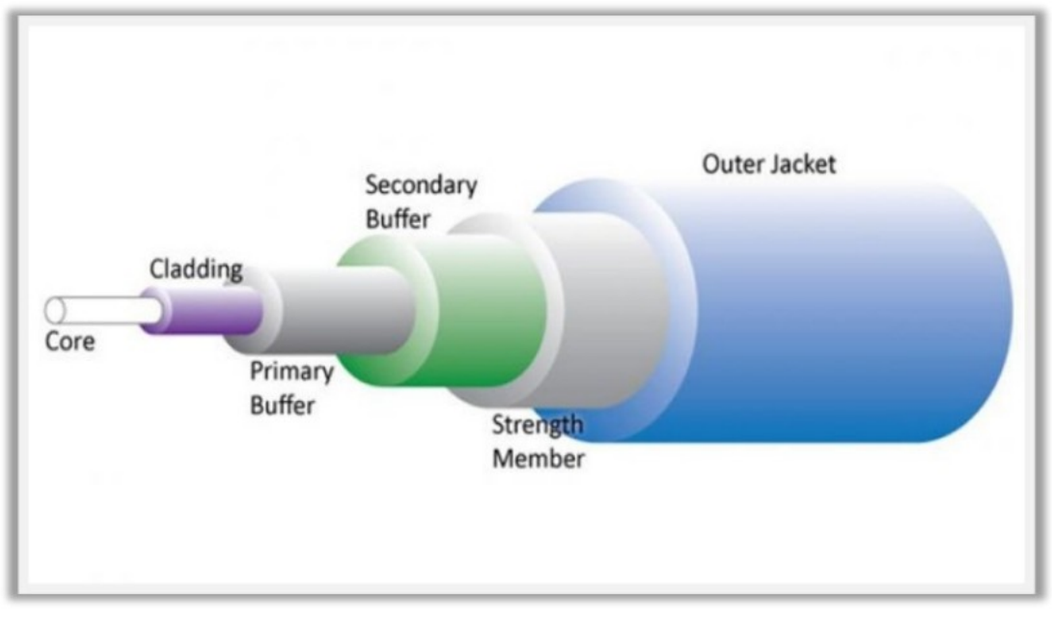


Figure A.17: Fiber-Optic Cable

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

A light-emitting diode (LED)/laser generates the light pulses used for the transmission of signals over fiber-optic cables. Glass strands as thick as human hair are used in this cable for the transmission of signals. Signal loss is avoided by the cladding outside the core. While the light propagates inside the core as a wave, the cladding reflects the waves that are directed outside and prevents signal loss.

Features

- Low cost
- Extremely high bandwidth
- Light weight and small size
- Secure
- Corrosion resistant
- Long life and easy to maintain
- Eliminates crosstalk
- Immune to electrostatic interference

Types of Fiber-optic Cables

There are two types of fiber-optic cables: single-mode fiber (SMF) and multi-mode fiber (MMF).

- **Single-mode fiber (SMF)**

  In this mode, the signal travels straight in a core with a diameter of 5–10 µm. While the signal travels in this mode, it does not bounce by colliding with the edges. Fiber-optic cables operating in this mode are generally used for television, telephone, and so on. Figure A.18 shows the transmission of light in an SMF.

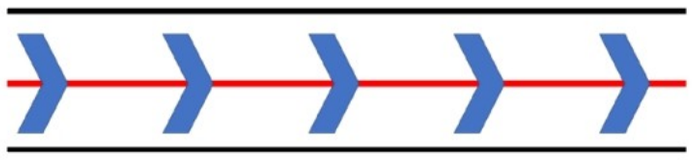


Figure A.18: Light Transmission in a Single-Mode Fiber

- **Multi-mode fiber (MMF)**

  In this mode, the light can take any path to travel inside the core as the diameter of the cable used for this mode is much higher than that used for the single mode. This mode is used for communication between devices separated by a short distance. Figure A.19 shows the transmission of light in an MMF:

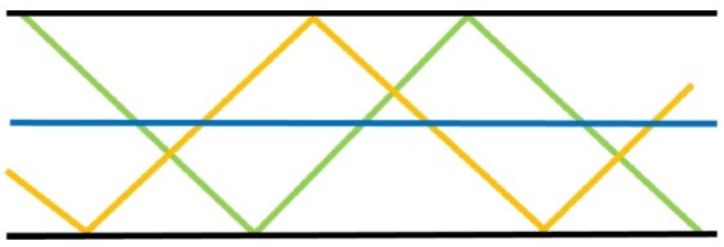
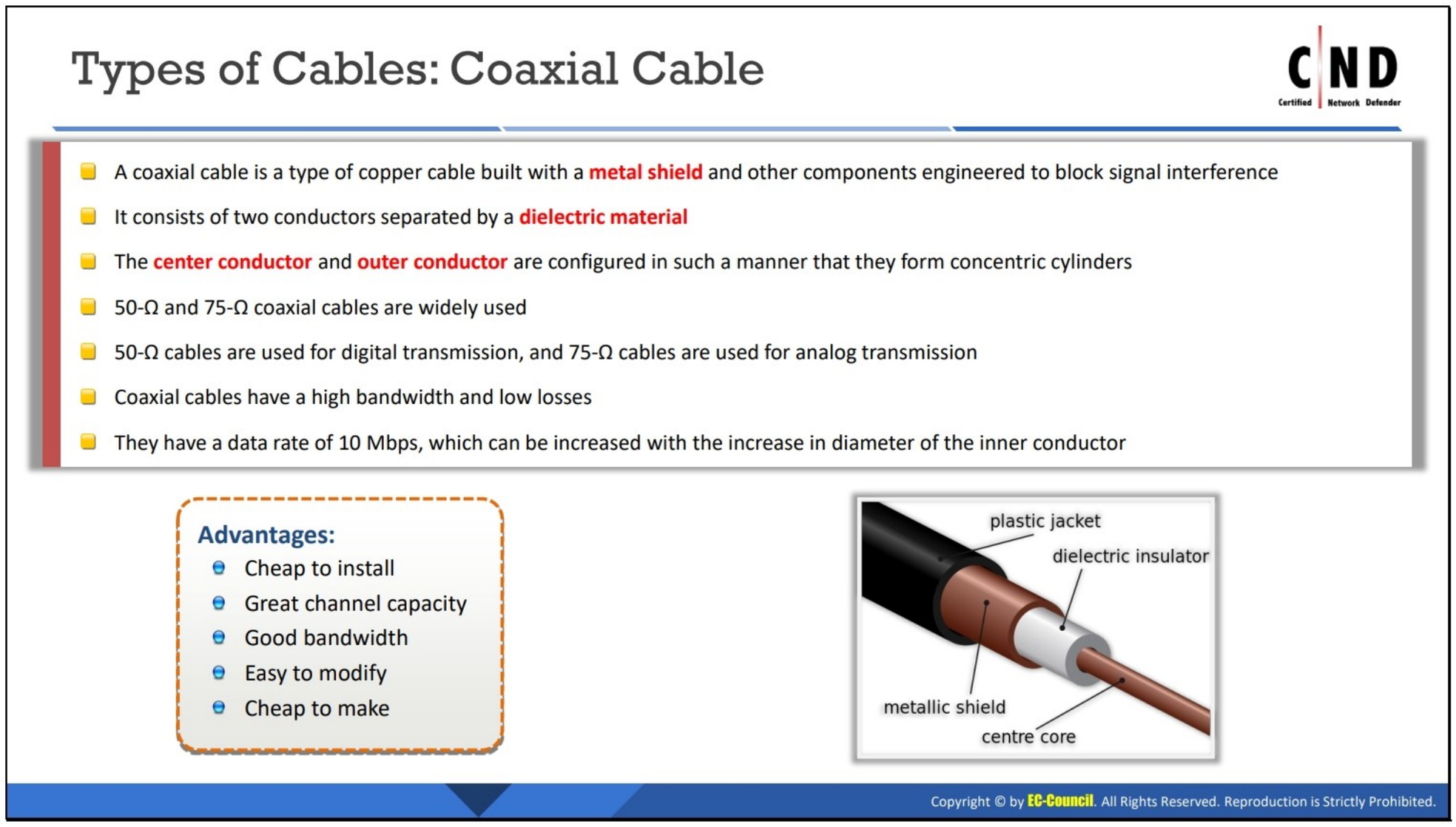


Figure A.19: Light Transmission in a Multi-Mode Fiber

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Cables: Coaxial Cable

Coaxial cables are the most commonly used cables for the transmission of signals for video, voice, and so on. These are named for their safe and reliable transmission of signals. These cables have high bandwidths and are capable of greater transmission.

A coaxial cable is a type of copper cable specially built with a metal shield and other components engineered to block signal interference. It consists of two conductors separated by a dielectric material. The center conductor and outer conductor are configured in such a way that they form concentric cylinders. Typically, coaxial cables are made of a thin copper wire covered by an insulating material. The insulation layer is covered with a copper mesh, and the mesh is further covered with an outer insulation layer. This design prevents electric noise to ensure that the signal remains undisturbed. Many applications use 50-Ω and 75-Ω coaxial cables: the 50-Ω cable is used for digital transmission, while the 75-Ω cable is used for analog transmission. These cables have low losses. It has a data rate of 10 Mbps, which can be increased with the increase in diameter of the inner conductor.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

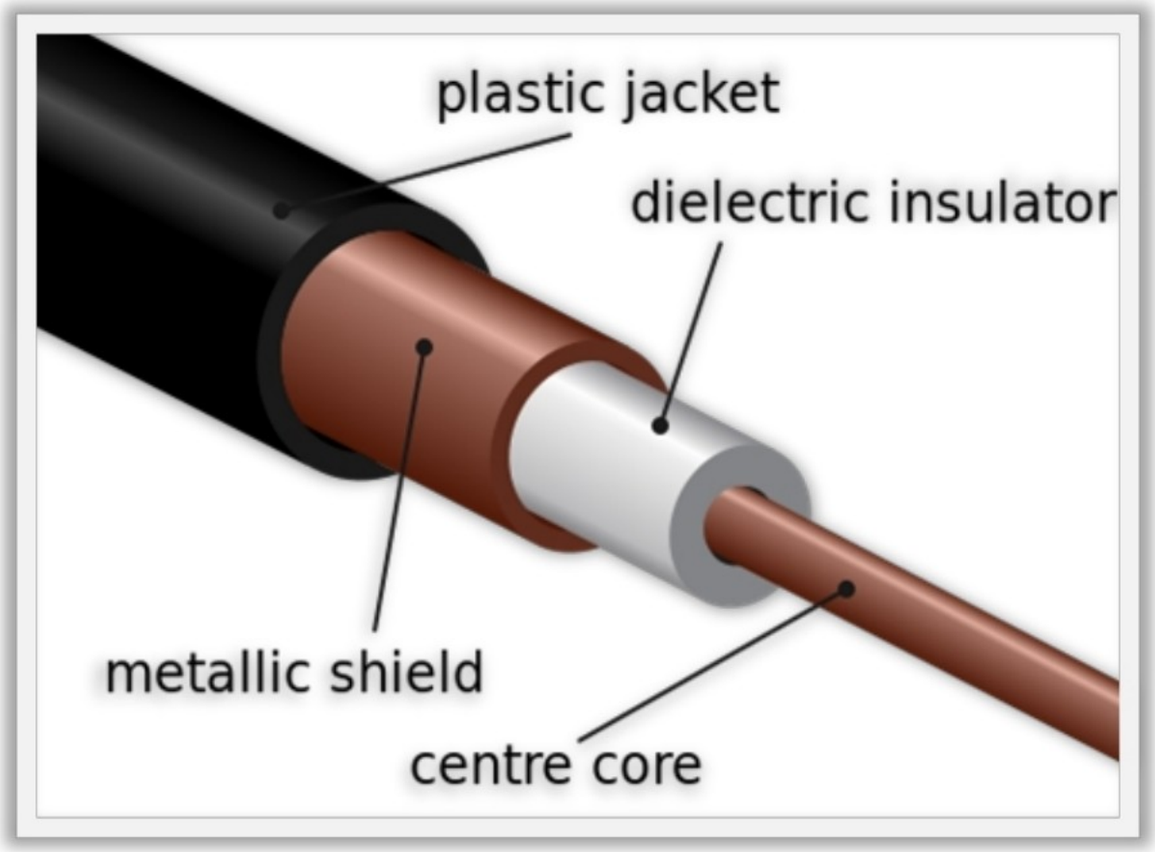


Figure A.20: Coaxial Cable

The following are some common types of coaxial cables.

- **Hardline**

  Hardline cables contain central conductors and shields above the insulating material that are made up of copper (aluminum or steel can also be used). They are used for transmitting high-strength military signals and broadcasting radio signals.



Figure A.21: Hardline Coaxial Cable

- **Twinaxial**

  Twinaxial cables are made up of two central conductors and are used for high-speed transmission in short-range communications.

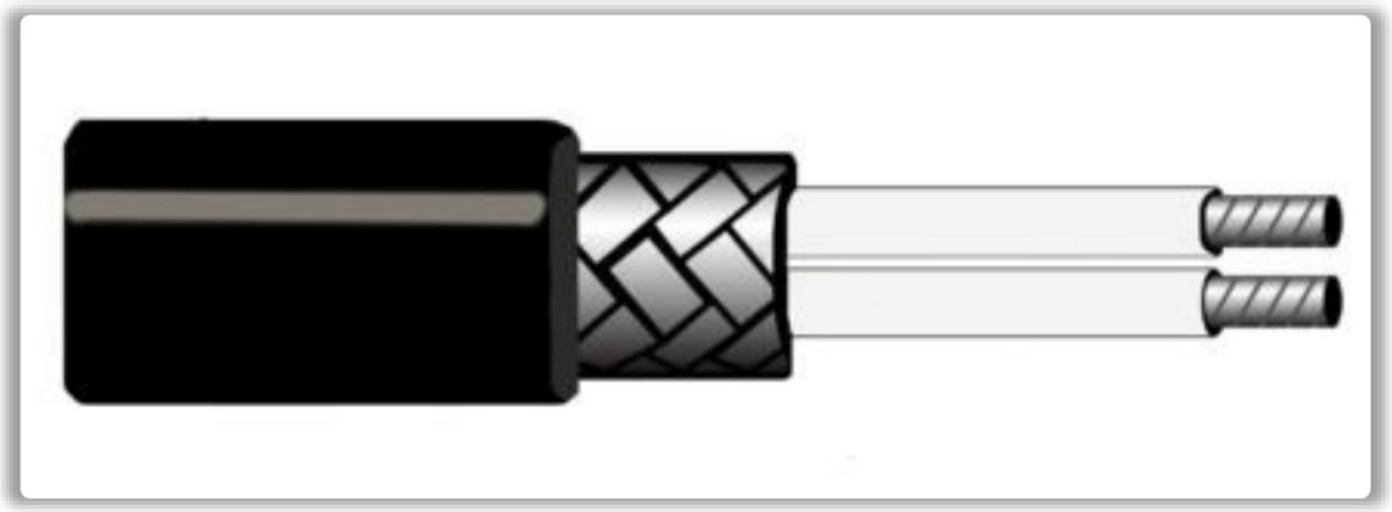


Figure A.22: Twinaxial Coaxial Cable

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Triaxial**

  Triaxial cables have an extra layer of insulating material and an extra copper shield compared to hardline cables. These cables have a high bandwidth and low noise interference.

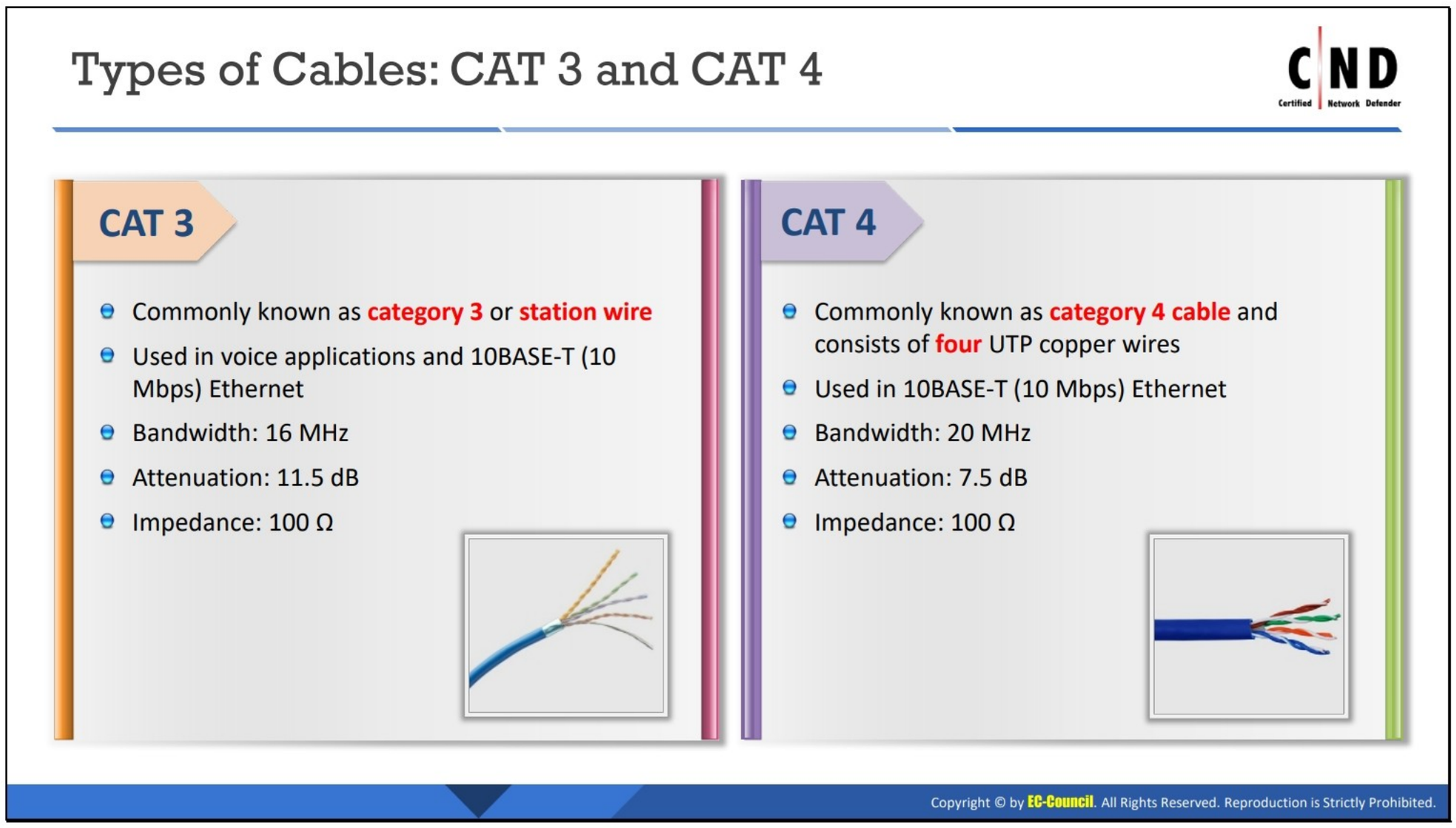


Figure A.23: Triaxial Coaxial Cable

Coaxial cables have the following advantages:

- Cheap to install
- Great channel capacity
- Good bandwidth
- Easy to modify
- Cheap to make

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Cables: CAT 3 and CAT 4

Some other types of cables include Category 3 (CAT 3), CAT 4, CAT 5, CAT 5e, CAT 6, and 10/100/1000BASE-T.

- **CAT 3**

  CAT 3 is one of the oldest wiring systems used for connecting two-line telephone configurations. These cables are used for communications that require a speed of up to 10 Mbps with a maximum frequency of 16 MHz.

  Features:

  - Commonly known as station wires
  - Used in voice applications and 10BASE-T (10 Mbps) Ethernet
  - Bandwidth : 16 MHz
  - Attenuation: 11.5 dB
  - Impedance: 100 Ω

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

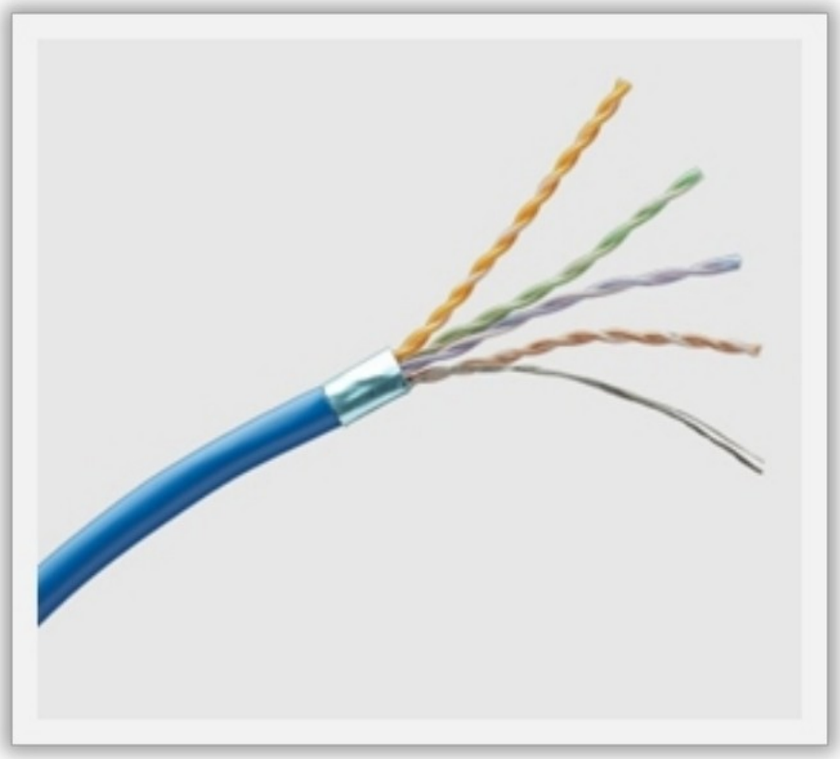


Figure A.24: CAT 3 Cable

- **CAT 4**

  The CAT 4 cable is made of four UTP copper wires that can transmit at a speed of 16 Mbps with a frequency of approximately 20 MHz. These are used for transmitting voice and data signals in telephone networks.

  Features:

  - Commonly known as category 4 cable and consists of four UTP copper wires
  - Used in 10BASE-T (10 Mbps) Ethernet
  - Bandwidth: 20 MHz
  - Attenuation: 7.5 dB
  - Impedance: 100 Ω

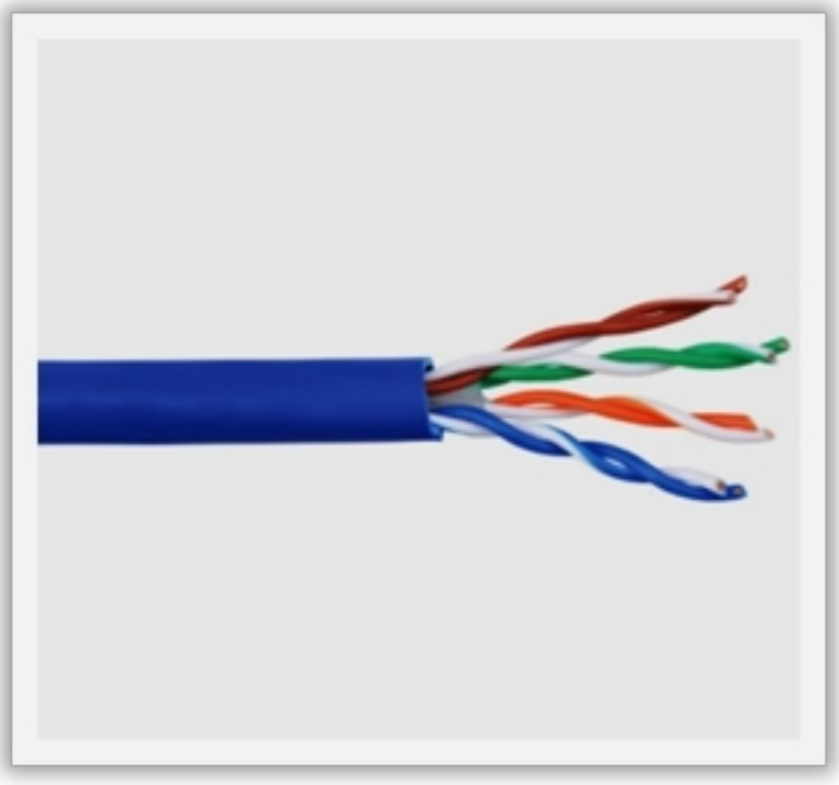
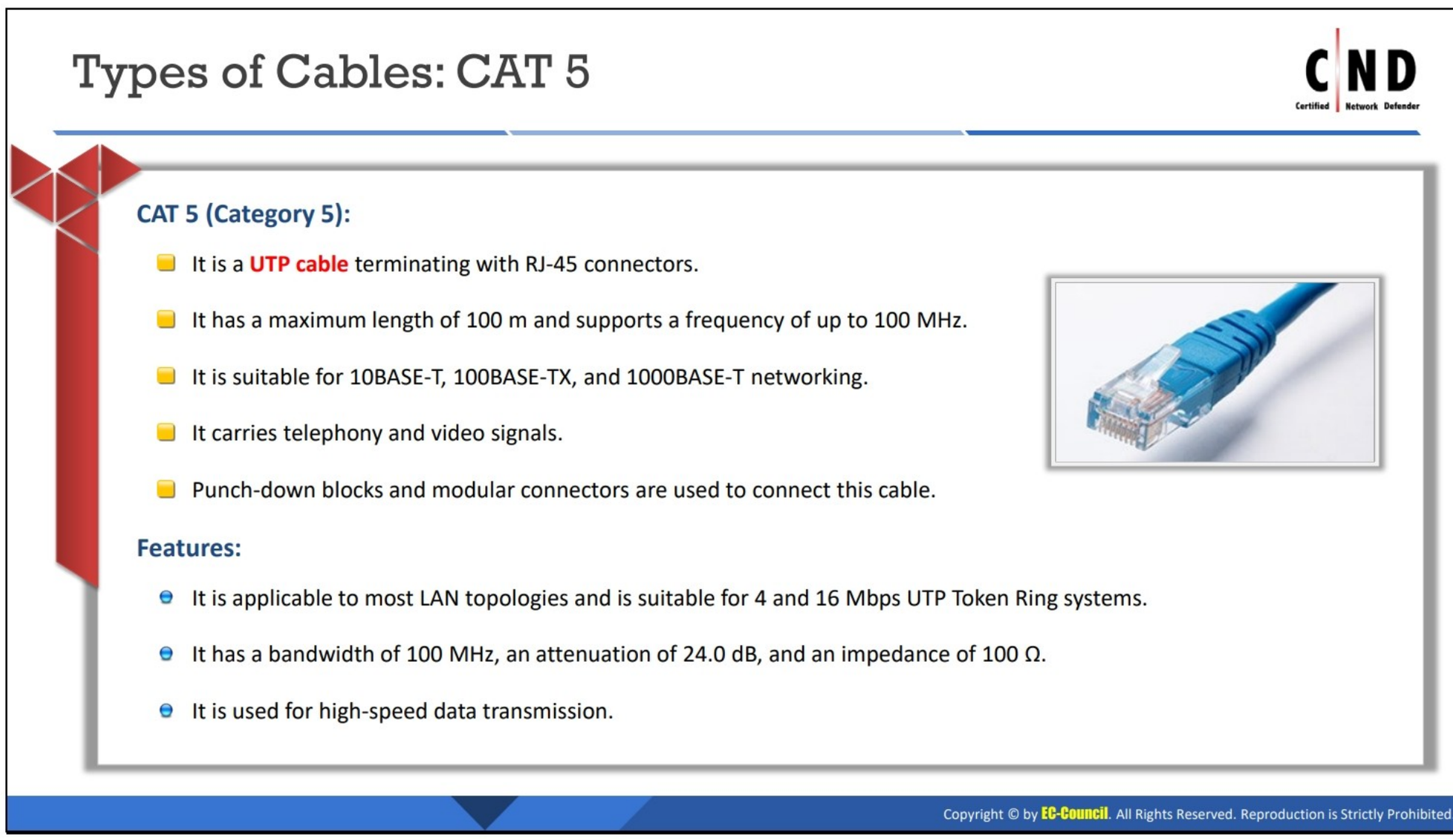


Figure A.25: CAT 4 Cable

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Cables: CAT 5

The CAT 5 cable used in computer networks has a maximum frequency of 100 MHz.

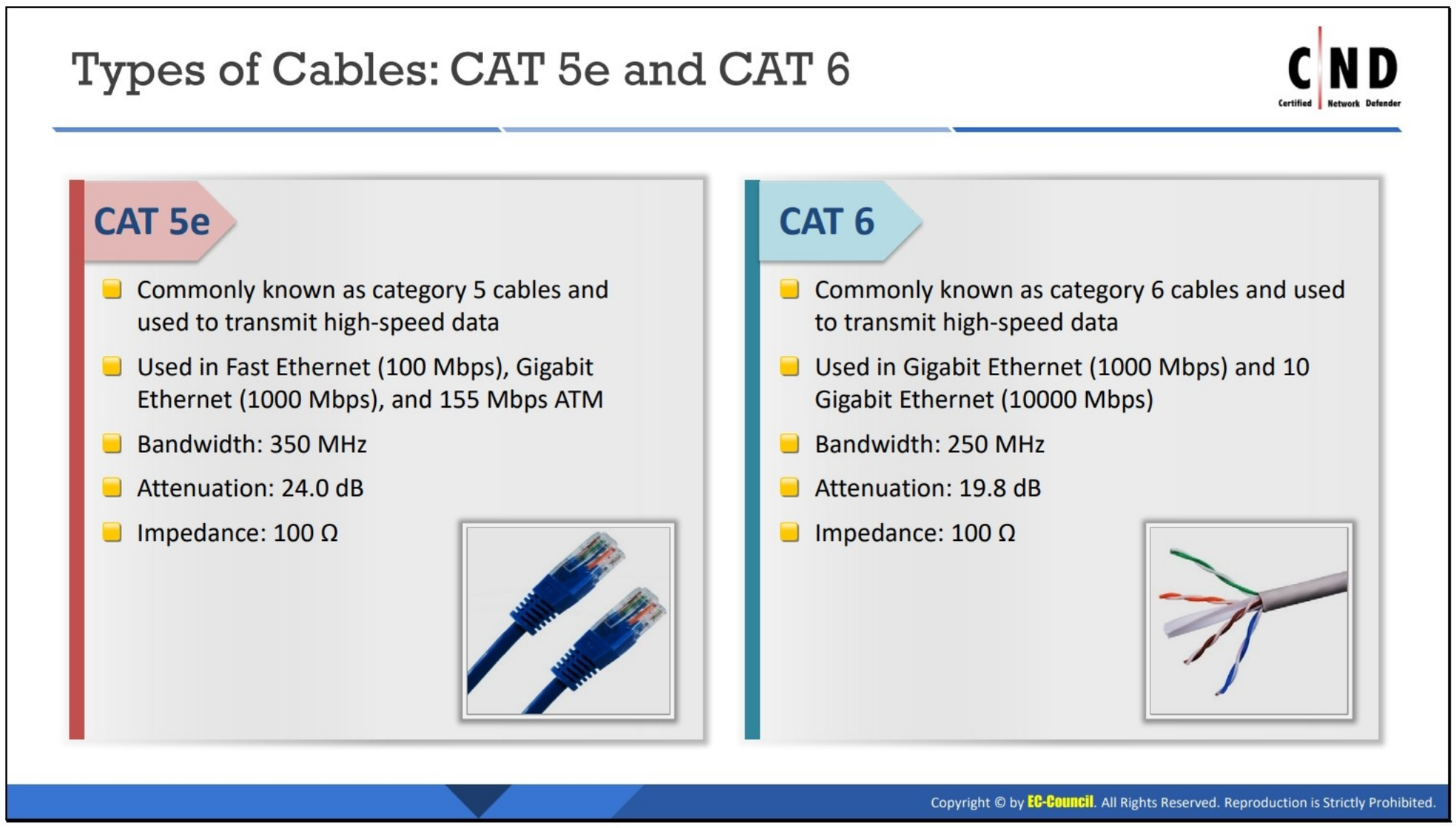
Features:

- It is a UTP cable terminating with RJ-45 connectors.
- It has a maximum length of 100 m and supports a frequency of up to 100 MHz.
- It is suitable for 10BASE-T, 100BASE-TX, and 1000BASE-T networking.
- It carries telephony and video signals.
- Punch-down blocks and modular connectors are used to connect this cable.
- It is applicable to most LAN topologies and is also suitable for 4- and 16-Mbps UTP Token Ring systems
- It has a bandwidth of 100 MHz, an attenuation of 24.0 dB, and an impedance of 100 Ω.
- It is used for high-speed data transmission.



Figure A.26: CAT 5 Cable

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Cables: CAT 5e and CAT 6

- **CAT 5e**

  The CAT 5e cable is an enhanced version of CAT 5 that is used for 1000BASE-T networks for transmitting data at a speed of 1 Gbps. These cables are twisted twice per centimeter. The CAT 5e cable uses four pairs of twisted wires for providing high-speed communications (Gigabit speed) at affordable cost.

  Features:

  - Used for high-speed data transmission
  - Used in Fast Ethernet (100 Mbps), Gigabit Ethernet (1000 Mbps), and 155 Mbps ATM
  - Bandwidth: 350 MHz
  - Attenuation: 24.0 dB
  - Impedance: 100 Ω



Figure A.27: CAT 5e Cable

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **CAT 6**

  CAT 6 cables are used for transmitting data at a speed of 10 Gbps with a frequency of 250 MHz. These cables are more tightly twisted with two or more twists per centimeter. They contain four pairs of copper wires for sending signals and achieve high performance.

  Features:

  - High-speed data transmission
  - Used in Gigabit Ethernet (1 Gbps) and 10 Gigabit Ethernet (10 Gbps)
  - Bandwidth: 250 MHz
  - Attenuation: 19.8 dB
  - Impedance: 100

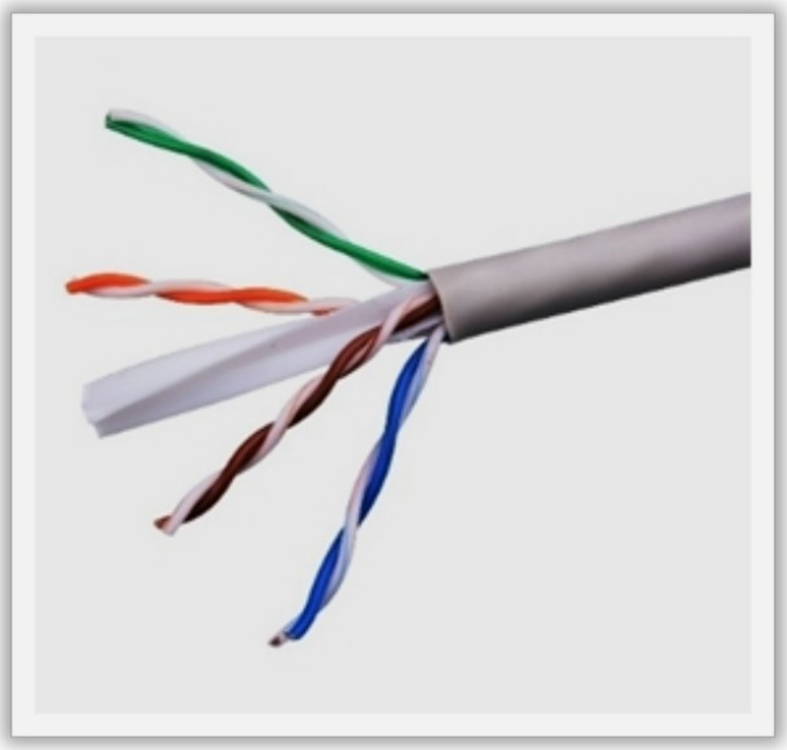
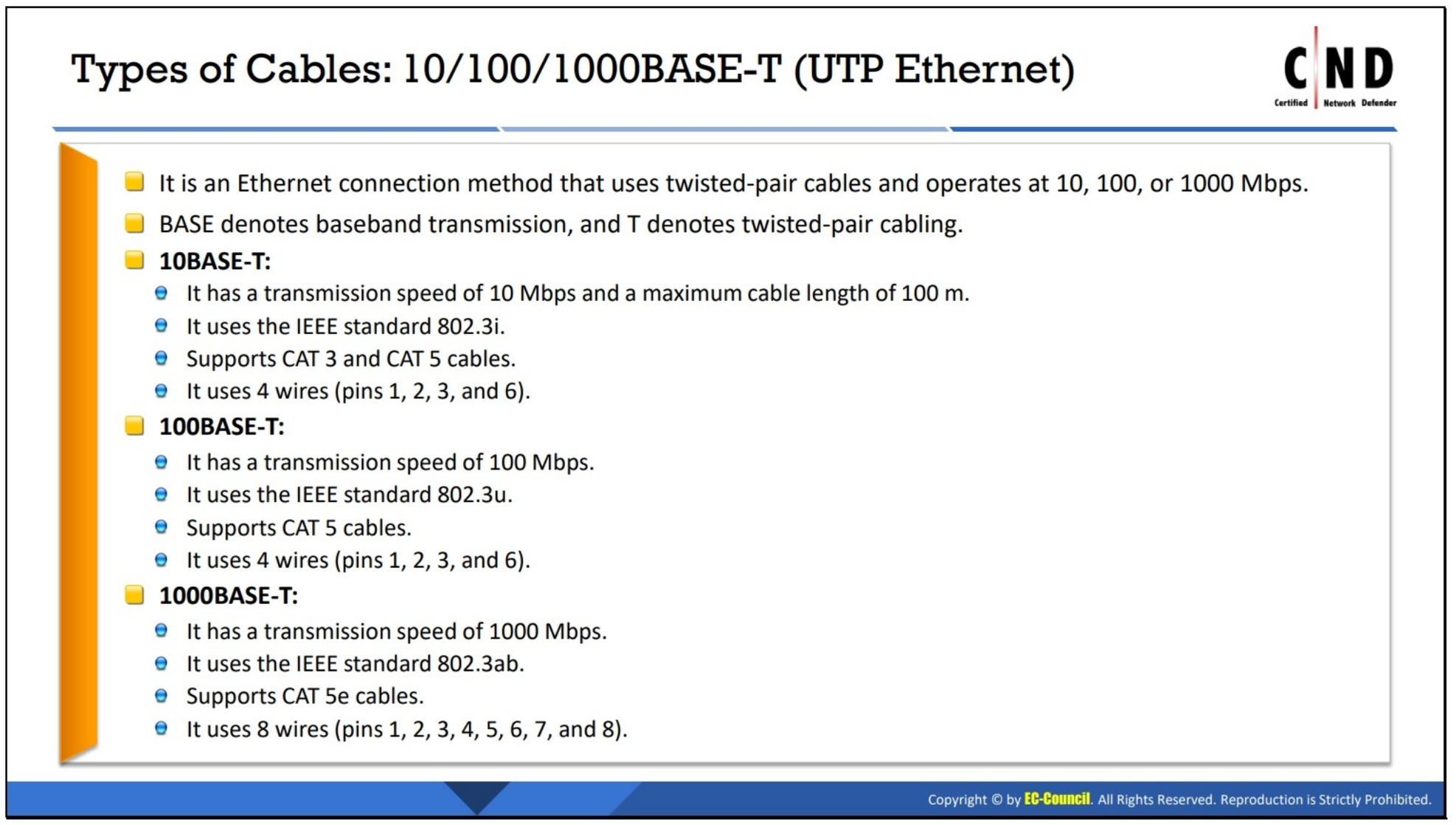


Figure A.28: CAT 6 Cable

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Cables: 10/100/1000BASE-T (UTP Ethernet)

The name 10BASE-T is from a twisted pair (T) that contains a baseband (BASE) for both sending and receiving Ethernet signals at a speed of 10 Mbps. The cable contains two insulated twisted pairs for transmitting data with one pair and receiving data with the other. The Ethernet connection method uses twisted-pair cables and operates at 10, 100, or 1000 Mbps.

- **10BASE-T**

  The Manchester encoding system is used for sending signals over 10BASE-T cables. The 10BASE-T pair is developed using an unshielded twisted pair (UTP) and an eight-position RJ-45 connector.

  Features:

  - Transmission speed of 10 Mbps and maximum cable length of 100 m
  - Uses the 802.3i IEEE standard
  - Supports CAT 3 and CAT 5 cables
  - Uses 4 wires (pins 1, 2, 3, and 6)

- **100BASE-T**

  100BASE-T cables are defined in the IEEE 802.3u standard and are used for transmitting data at a speed of 100 Mbps in shared media. These cables are divided into three distinct categories: 100BASE-T4, 100BASE-TX, and 100BASE-FX, which are referred to as the physical medium for carrying the signals.

  Features:

  - Transmission speed of 100 Mbps

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Uses the IEEE 802.3u standard
- Supports CAT 5 cables
- Uses 4 wires (pins 1, 2, 3, and 6)

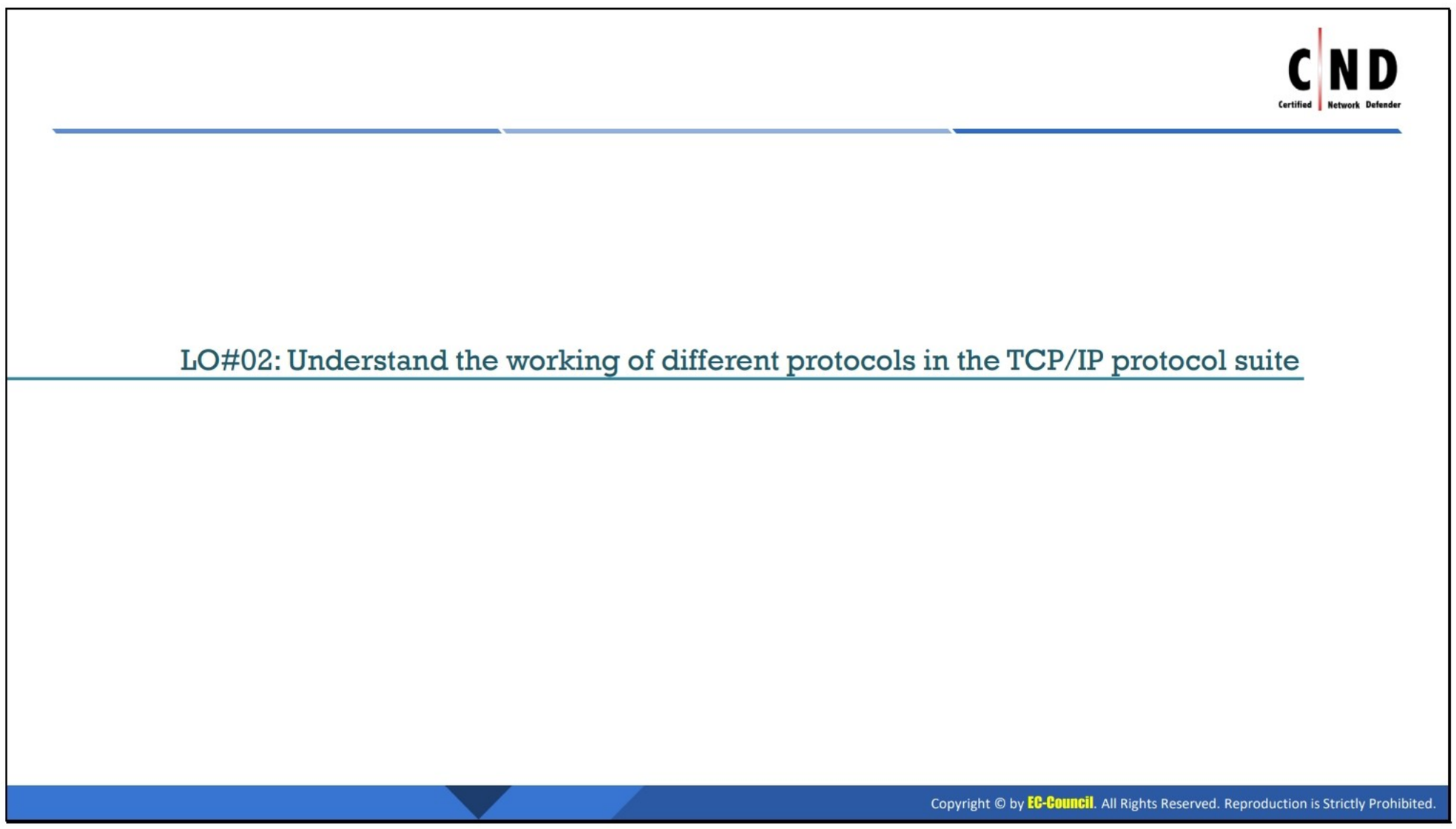
- **1000BASE-T**

  These cables are used for the high-speed transmission of signals at a speed of up to 1000 Mbps in shared media. The cable consists of four CAT 5 UTP wires for broadband connections. These cables are divided into types such as 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX, 1000BASE-CX, and 1000BASE-T

  Features:

  - Transmission speed of 1000 Mbps
  - Uses the 802.3ab IEEE standard
  - Supports CAT 5e cables
  - Uses 8 wires (pins 1, 2, 3, 4, 5, 6, 7, and 8)

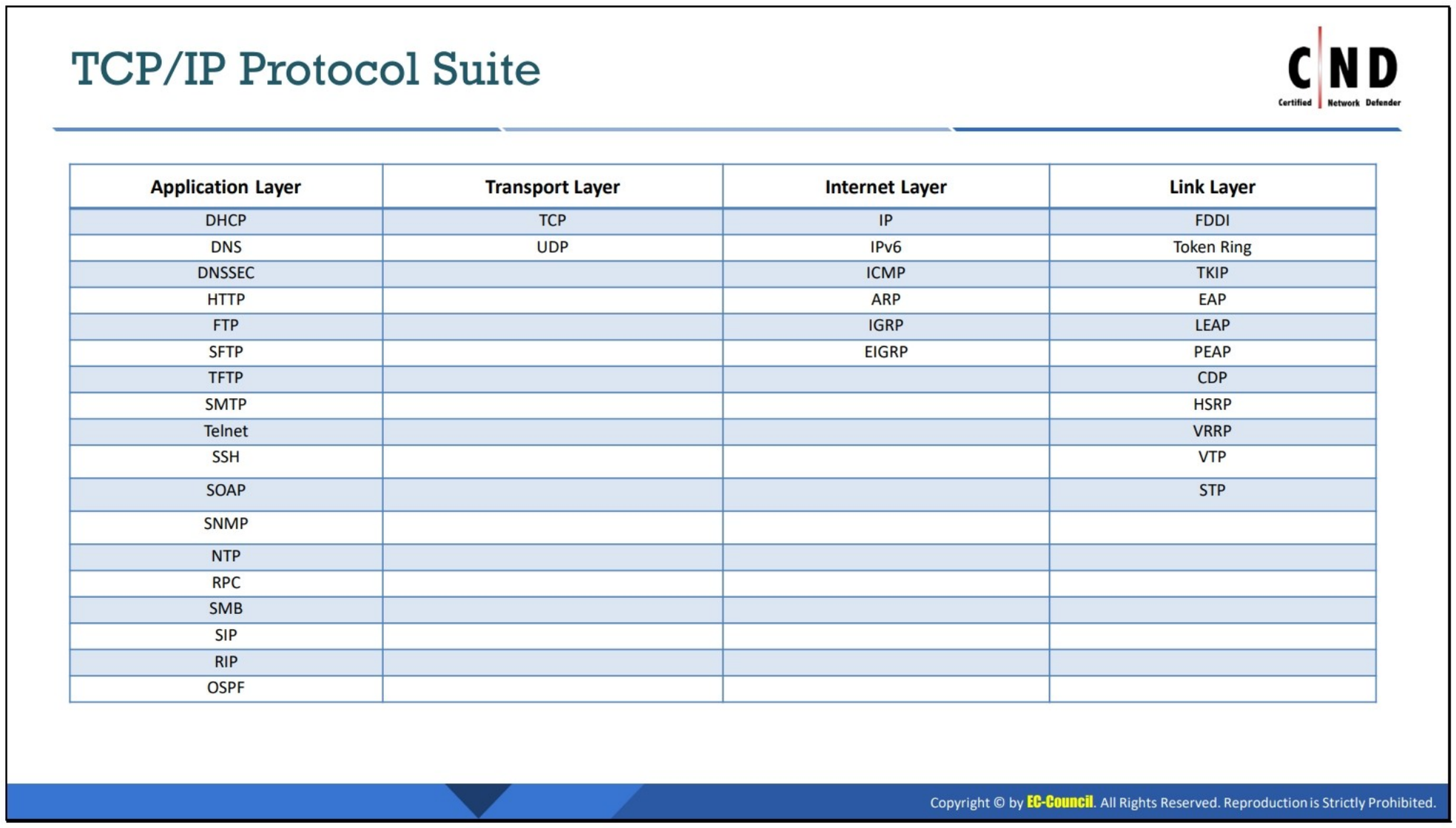
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#02: Working of Different Protocols in the TCP/IP Protocol Suite

This section discusses the TCP/IP model and related concepts. The packet format and the operation of protocols such as TCP, UDP, DNS, and Dynamic Host Configuration Protocol (DHCP) will be discussed in detail.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



TCP/IP Protocol Suite

Table A.2 lists the protocols in each TCP/IP layer.

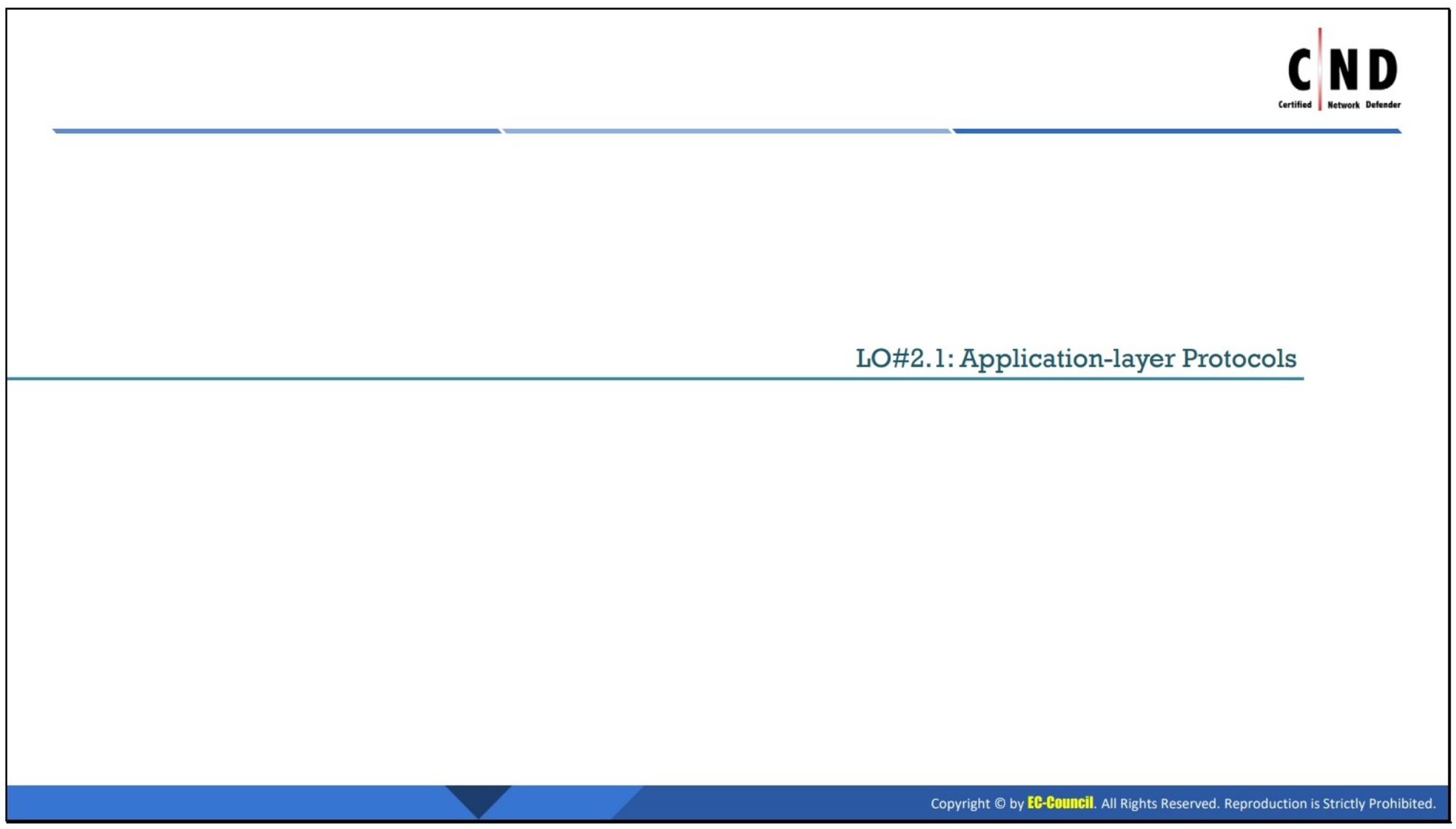
Application Layer	Transport Layer	Internet Layer	Link Layer
DHCP	TCP	IP	FDDI
DNS	UDP	IPv6	Token Ring
DNSSEC		ICMP	TKIP
HTTP		ARP	EAP
FTP		IGRP	LEAP
SFTP		EIGRP	PEAP
TFTP			CDP
SMTP			HSRP
Telnet			VRRP
SSH			VTP
SOAP			STP
SNMP			
NTP			

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

RPC			
SMB			
SIP			
RIP			
OSPF			

Table A.2: TCP/IP Protocol Suite

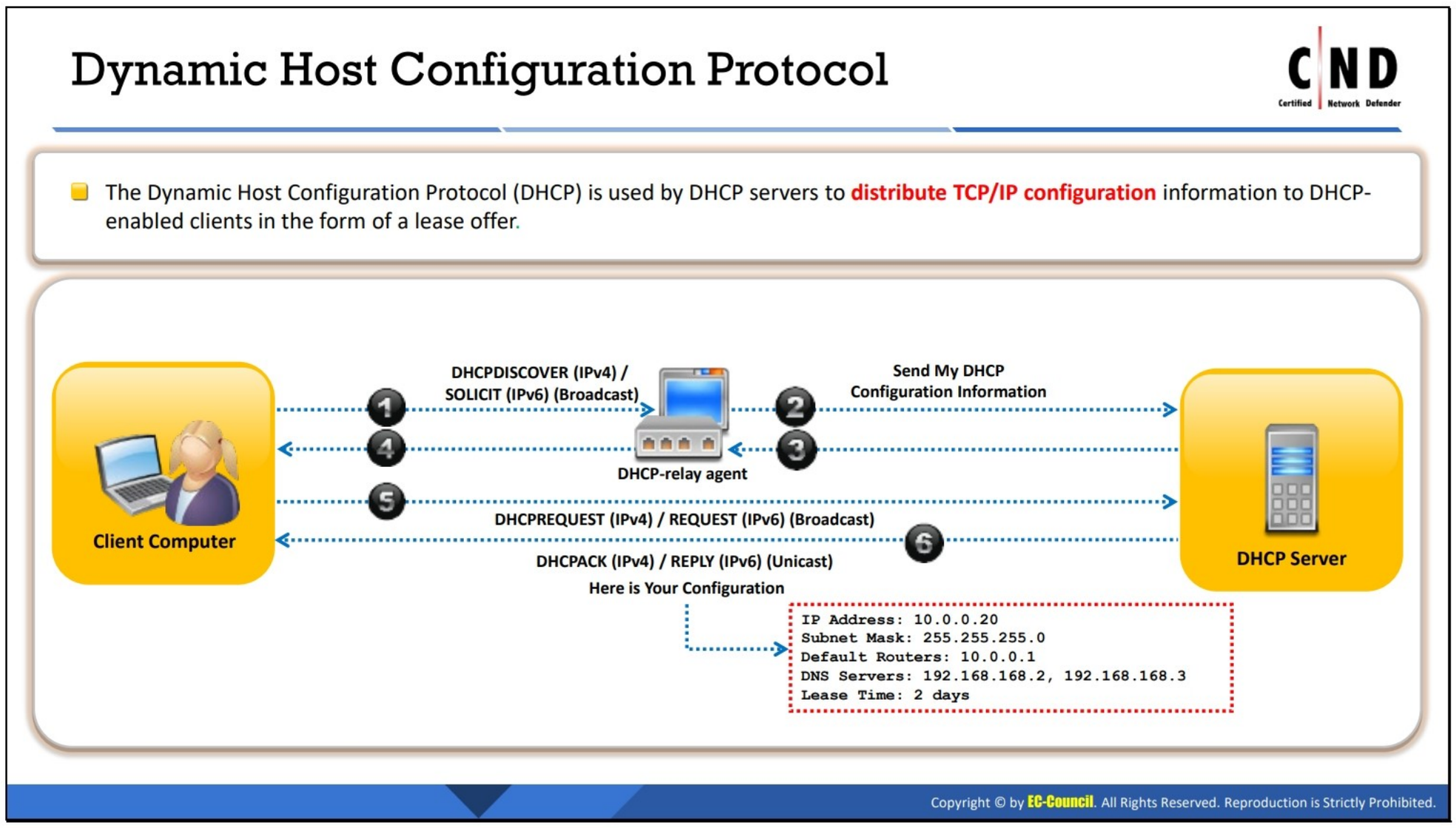
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#2.1: Application-Layer Protocols

This section discusses the fundamentals of application-layer protocols such as DHCP, DNS, Security Extensions (DNSSEC), HTTP, etc.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Dynamic Host Configuration Protocol

Every system should have an address to communicate with other devices in a network. Before the Bootstrap Protocol (BOOTP) and DHCP were created, IP address were manually assigned to systems. DHCP belongs to the application layer of the OSI model, and it assigns the IP address automatically. It allows both the dynamic and static mapping of the addresses to systems; in contrast, BOOTP allows only static mapping.

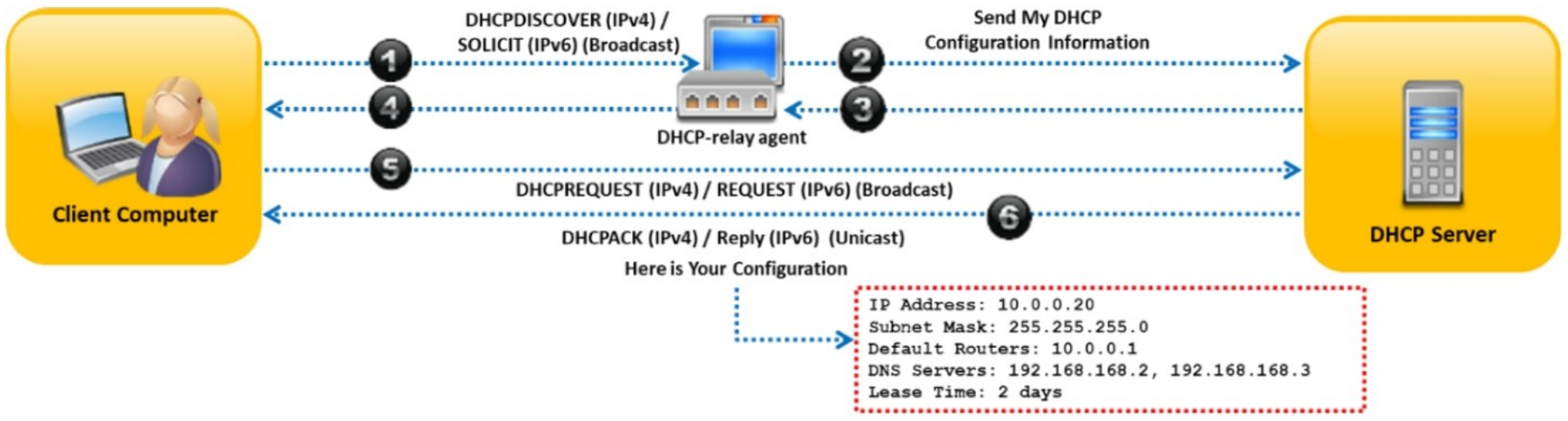


Figure A.29: Dynamic Host Configuration Protocol

DHCP performs many functions. The following are its two main functions:

- Assigns addresses to hosts or devices
- Defines a procedure that allows clients to communicate with servers for configuration

DHCP allocates addresses in three ways: manual, dynamic, and automatic.

Manual Allocation

- The manual method of address allocation is performed by the network administrator.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In manual allocation, an address in the table is mapped to a device the administrator assigned it to.
- DHCP maintains a centralized space (DHCP address database) for keeping track of information about devices and their assigned IP addresses.
- This reduces the burden on the network administrator by avoiding the need to check each device manually.

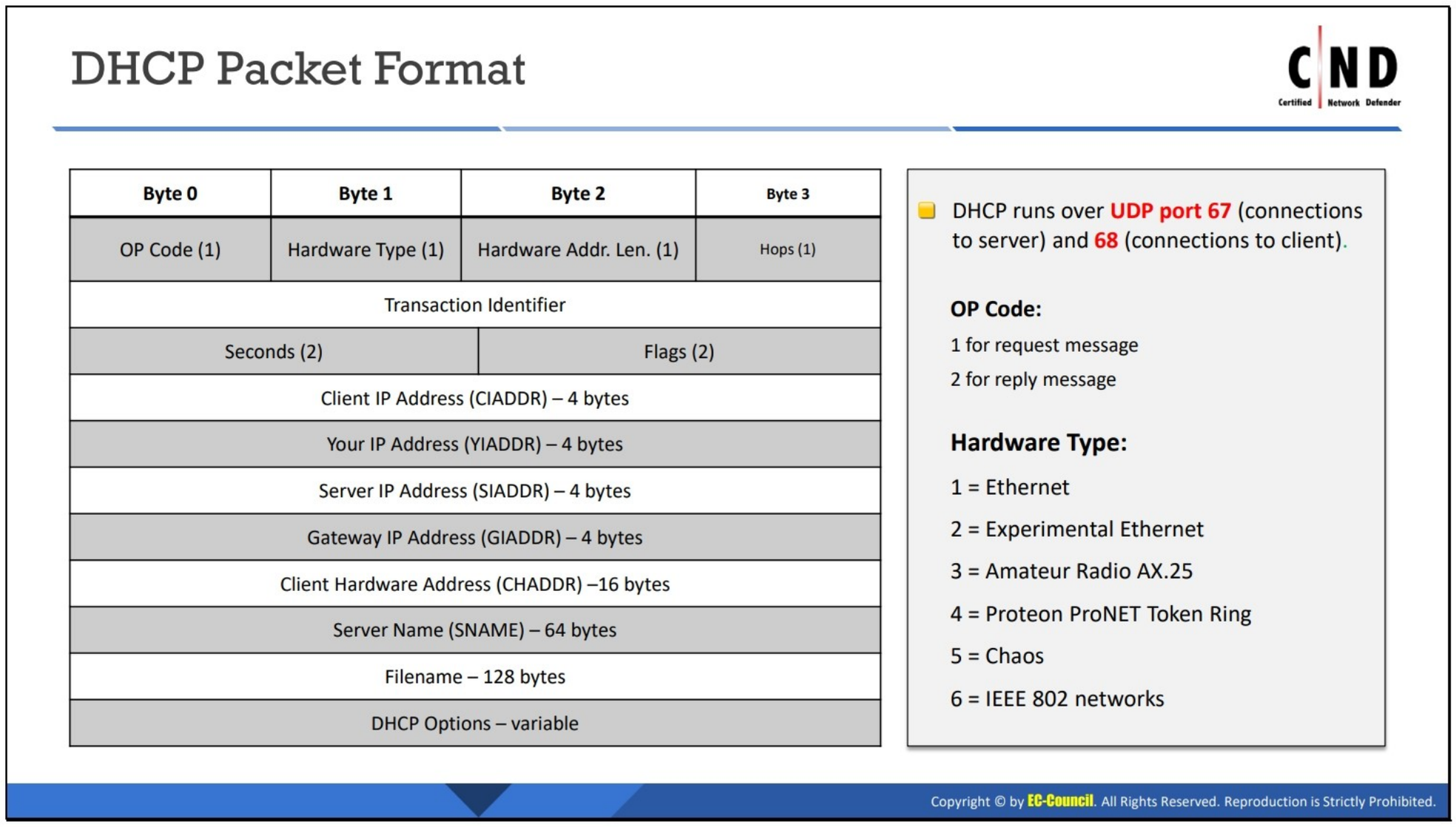
Dynamic Allocation

- DHCP dynamically assigns IP address to devices for a particular period of time.
- For this type of allocation, the network administrator creates a set of IP addresses, following which the DHCP server dynamically assigns those addresses to devices.
- A client can request the server for an IP address, which will make the DHCP server check for unallocated ones and assign one to that client.
- The advantages of using dynamic allocation are as follows:
  - Process automation
  - Control of the overall process through a centralized mechanism
  - Reuse of previously allocated addresses

Automatic Allocation

- IP addresses can be assigned permanently to devices through automatic allocation.
- This allocation is preferred by the DHCP server when the number of available IP addresses is greater than the number of devices.
- This is another kind of dynamic allocation in which devices can use the assigned IP address permanently.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DHCP Packet Format

DHCP runs over UDP ports 67 (connections to server) and 68 (connections to client). The DHCP packet carries a large amount of information. Many fields in the packet contain various details about the data inside it. The following are the fields in a DHCP packet.

- **Operation code**: This field informs whether the packet is a DHCP request or reply. The length of this field is 8 bits. In the operation code, also called OP Code, 1 is used for a request message, and 2 is used for a reply message.
- **Hardware type**: This field defines the type of hardware (the hardware can be anything such as an Ethernet or ATM device). Its length is 8 bits. The following are some of the digits used in the hardware type:
  - 1 = Ethernet
  - 2 = Experimental Ethernet
  - 3 = Amateur Radio AX.25
  - 4 = Proteon ProNET Token Ring
  - 5 = Chaos
  - 6 = IEEE 802 networks
- **Hardware length**: This field defines the length of the hardware; for example, the length is 6 for Ethernet. The length of this field is 8 bits
- **Hops**: This 8-bit field defines the number of hops to a DHCP server.
- **Transaction ID**: This 4-byte field contains a number used by both the client and server while communicating through requests and replies.

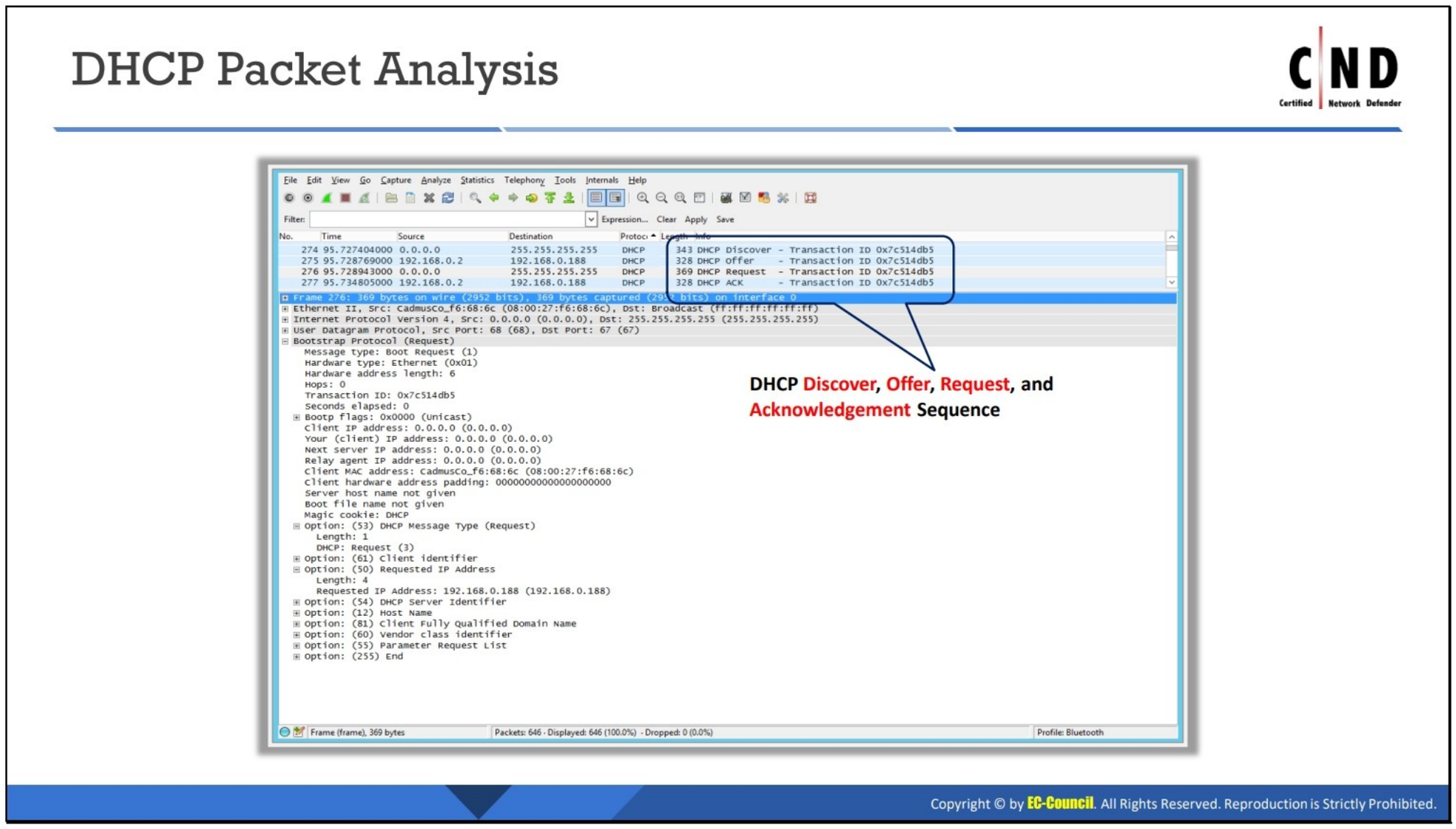
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Seconds elapsed**: This 16-bit field provides information about the number of seconds since the client sent its first request for an IP address.
- **Flags**: This 16-bit field defines the DHCP client's traffic (such as unicast and broadcast).
- **Client IP address**: This 4-byte field contains information about the client's IP address.
- **Your IP address**: This 4-byte field contains information about the client's IP address, which is set by the DHCP server in a reply to the client's request.
- **Server IP address**: This 4-byte field contains information about the server IP address, which is set by the DHCP server.
- **Gateway IP address**: This 4-byte field contains information about the gateway (router) IP address.
- **Client hardware address**: This field contains information about the MAC address of the client. Even if this field is not mentioned, the DHCP server can obtain the MAC address through the request frame from the client.
- **Server host name**: This 64-byte field defines the domain name (host name) of the DHCP server. This field is optional, and the server can fill it with its name; else, it is filled with zeros.
- **Boot file**: This 128-byte field contains information about the boot file for the client. This field is optional, and the server can fill it with its name; else it is filled with zeros.
- **Options**: This 64-byte field provides additional information for more features.

Byte 0	Byte 1	Byte 2	Byte 3
OP Code (1)	Hardware Type (1)	Hardware Addr. Len. (1)	Hops (1)
Transaction Identifier			
Seconds (2)		Flags (2)	
Client IP Address (CIADDR) – 4 bytes			
Your IP Address (YIADDR) – 4 bytes			
Server IP Address (SIADDR) – 4 bytes			
Gateway IP Address (GIADDR) – 4 bytes			
Client Hardware Address (CHADDR) –16 bytes			
Server Name (SNAME) – 64 bytes			
Filename – 128 bytes			
DHCP Options – variable			

Figure A.30: DHCP Packet Format

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DHCP Packet Analysis

The DHCP assigns new IP addresses or renews IP addresses by using four DHCP packets called Discover, Offer, Request, and Acknowledgement. This is also called the DORA process owing to the involvement of the four types of DHCP packets. Figure A.31 shows the DORA process.



Figure A.31: DHCP DORA Process

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

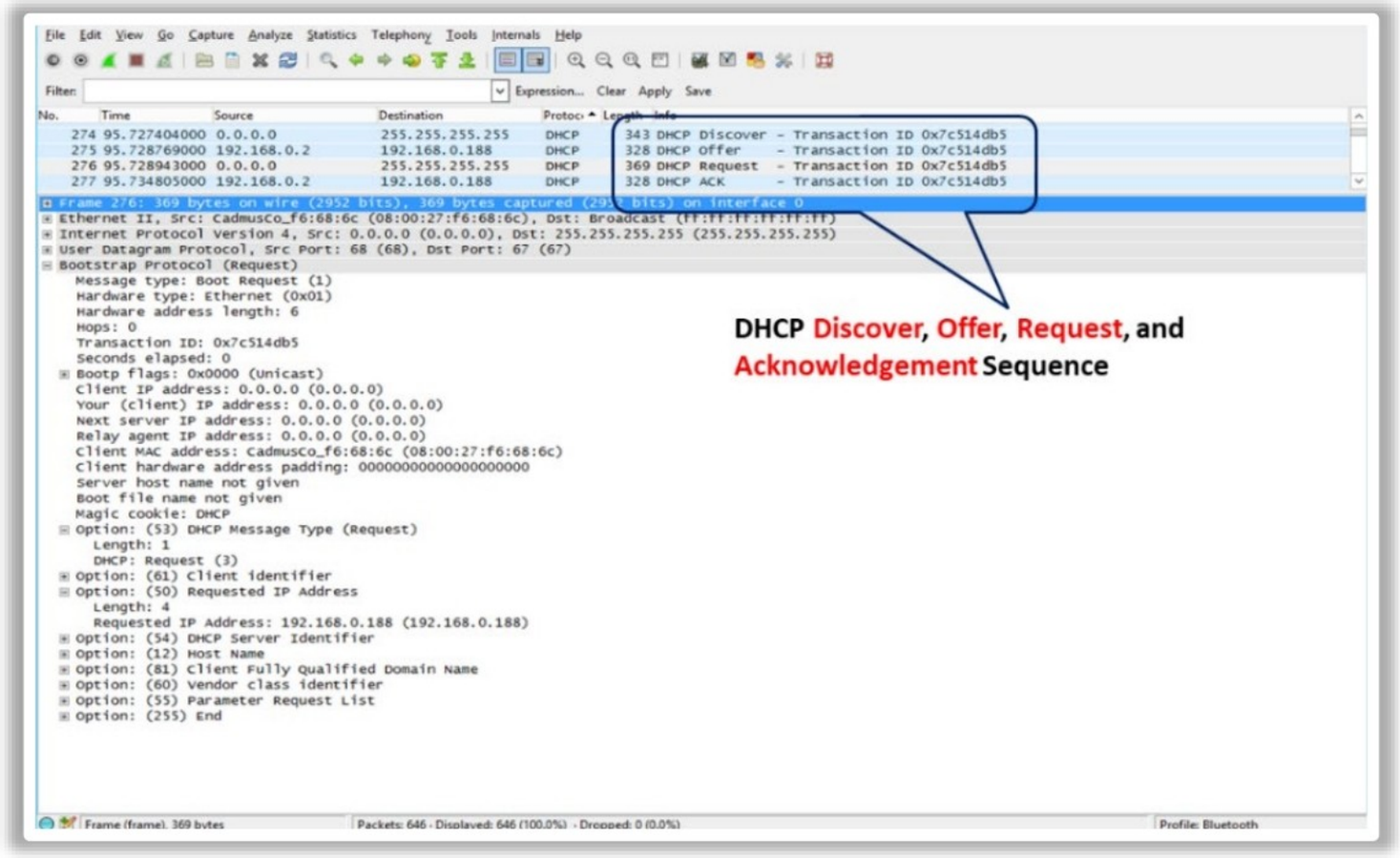


Figure A.32: DHCP DORA Process Captured using Wireshark

Discover packet: For requesting an IP address, the client has to send an initial request packet to identify the server in a network. As the client does not have any IP address at this point, it uses 0.0.0.0 as its initial address. It sends the discover packet to all the devices in a network (i.e., it sends the packet to 255.255.255.255) to discover the server.

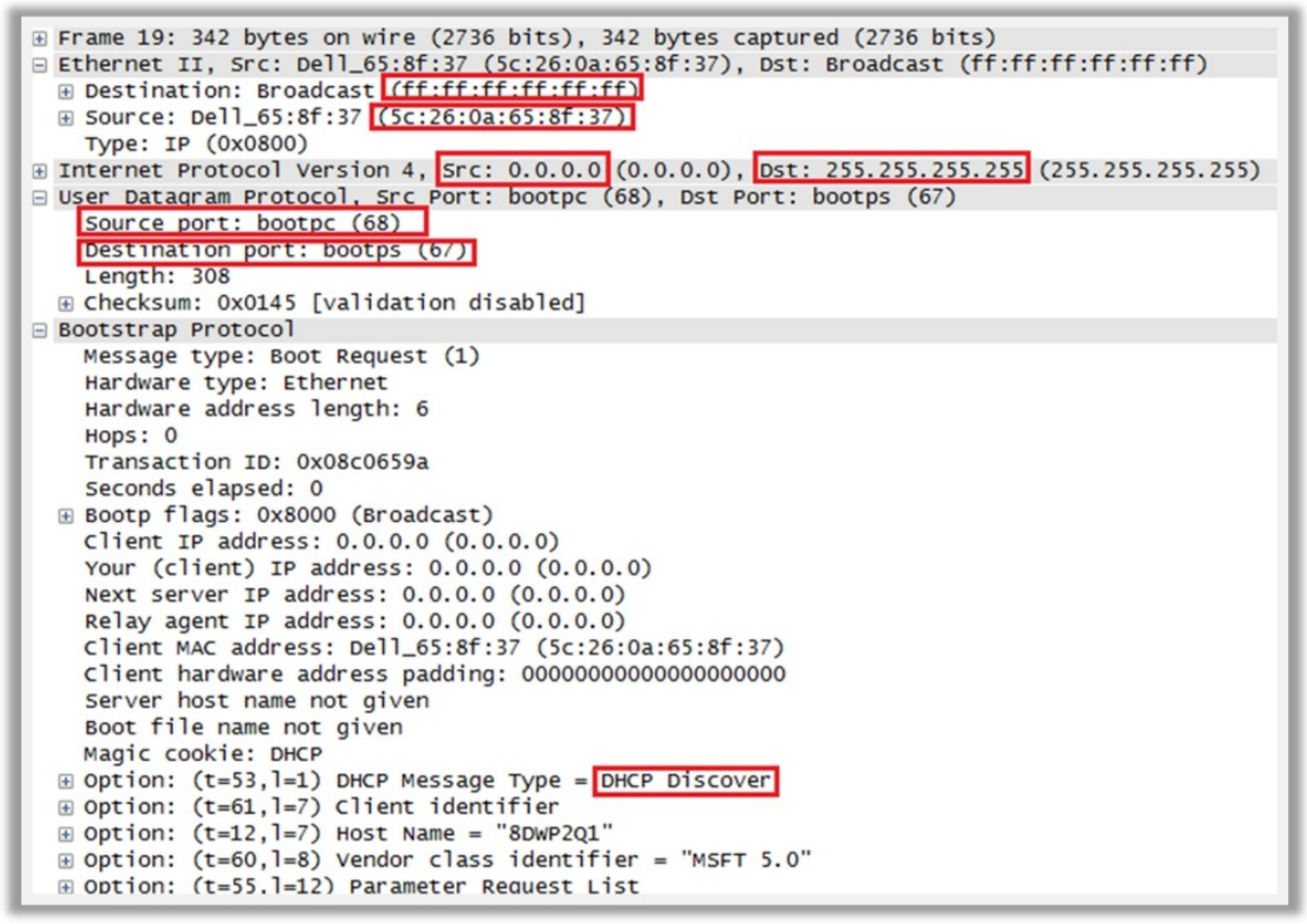


Figure A.33: DHCP Discover Packet

DHCP uses UDP as the transmission protocol for request packets sent by clients. The discovery packet contains the following four fields.

- **DHCP message type**: Defines the type of the packet

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Client identifier**: Defines information about the client
- **Requested IP address**: Defines the particular IP address requested by the client
- **Parameter request list**: Contains the list of configuration information the client is requesting for

Offer packet: The server communicates with the client through this packet for offering its services. For this communication, the server uses the client's hardware address obtained through ARP. In case of any communication failure, the offer packet is sent to the network through broadcasting. This packet carries the same transaction ID as that of the request packet, which is unique for this particular communication.

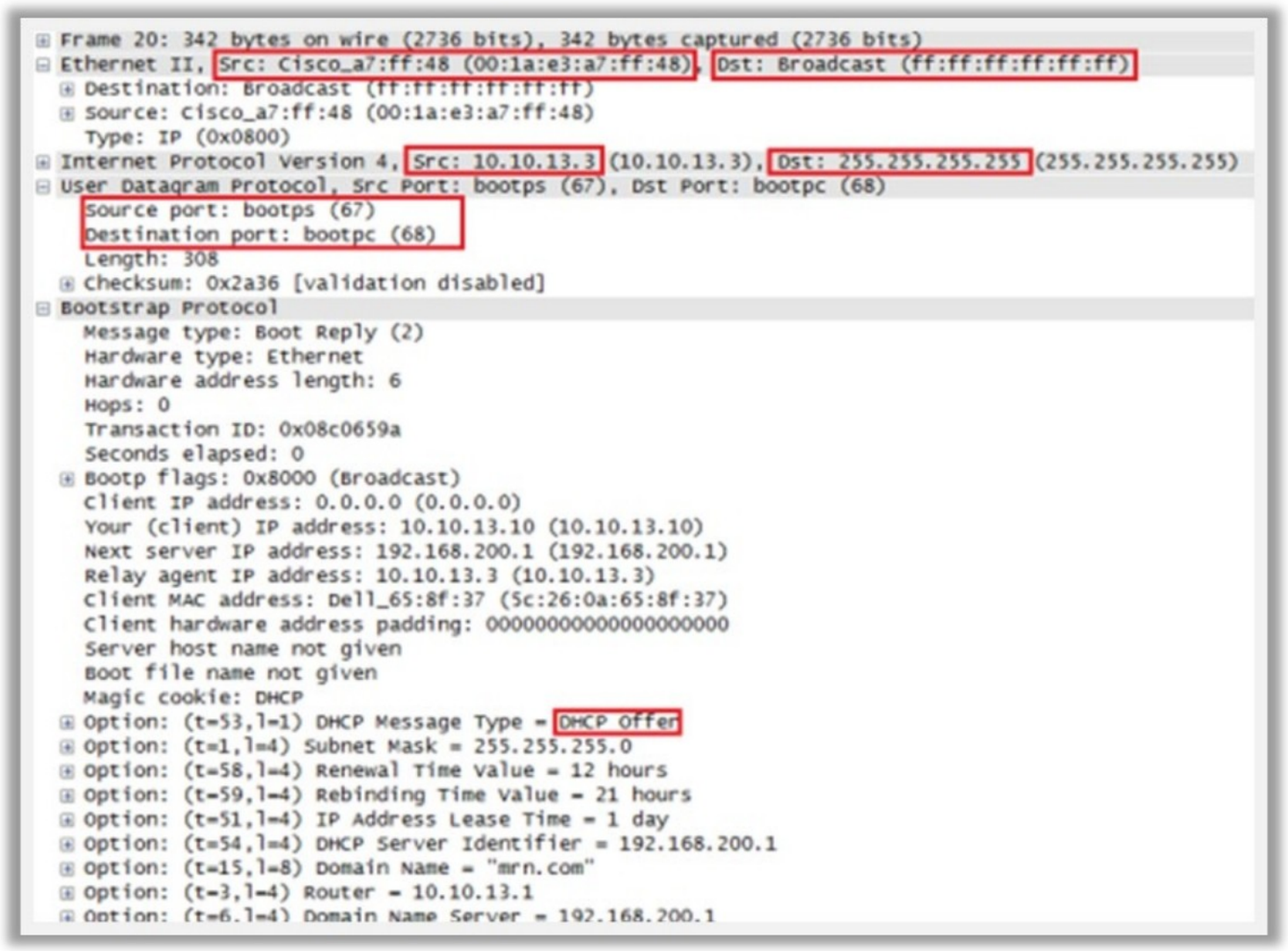


Figure A.34: DHCP Offer Packet

This packet provides information about the server and the IP address assigned to the client. The IP address assigned to the client can be viewed in the **Your (Client) IP address** field of the packet. This packet contains various options that provide additional details to the client.

Request packet: By sending this packet, the client informs the server that it is using the IP address provided by the server. As the process of assigning the IP address to the client is not completed, the client still uses the address 0.0.0.0 for its communication. This packet is another request to the server informing it that the client is using the address provided by it. Therefore, a new transaction ID will be generated for this packet.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
Frame 21: 363 bytes on wire (2904 bits), 363 bytes captured (2904 bits)
Ethernet II, Src: Dell_65:8f:37 (5c:26:0a:65:8f:37), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: Dell_65:8f:37 (5c:26:0a:65:8f:37)
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
  Source port: bootpc (68)
  Destination port: bootps (67)
  Length: 329
  Checksum: 0x015a [validation disabled]
Bootstrap Protocol
  Message type: Boot Request (1)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x08c0659a
  Seconds elapsed: 0
  Bootp flags: 0x8000 (Broadcast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 0.0.0.0 (0.0.0.0)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 0.0.0.0 (0.0.0.0)
  Client MAC address: Dell_65:8f:37 (5c:26:0a:65:8f:37)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (t=53,l=1) DHCP Message Type = DHCP Request
  Option: (t=61,l=7) Client identifier
  Option: (t=50,l=4) Requested IP Address = 10.10.13.10
  Option: (t=54,l=4) DHCP Server Identifier = 192.168.200.1
  Option: (t=12,l=7) Host Name = "8DwP2Q1"
  Option: (t=81,l=21) Client Fully Qualified Domain Name
  Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
  Option: (t=55,l=12) Parameter Request List
```

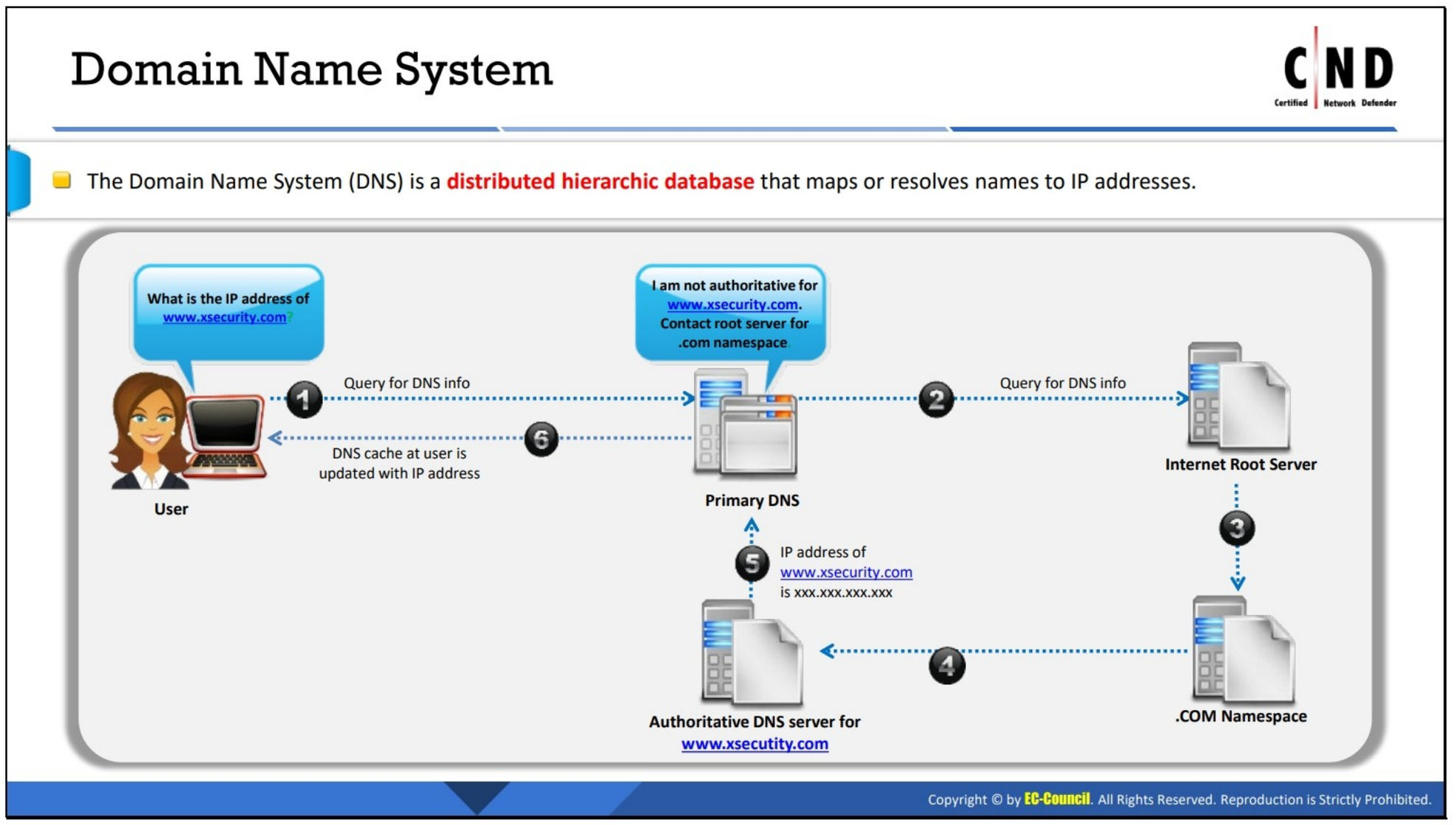
Figure A.35: DHCP Request Packet

Acknowledgement packet: Through this packet, the server accepts the client's request, assigns it the IP address, and records this information in its database table.

```
Frame 22: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: Cisco_a7:ff:48 (00:1a:e3:a7:ff:48), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: Cisco_a7:ff:48 (00:1a:e3:a7:ff:48)
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 10.10.13.3 (10.10.13.3), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
  Source port: bootps (67)
  Destination port: bootpc (68)
  Length: 308
  Checksum: 0xafe0 [validation disabled]
Bootstrap Protocol
  Message type: Boot Reply (2)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x08c0659a
  Seconds elapsed: 0
  Bootp flags: 0x8000 (Broadcast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 10.10.13.10 (10.10.13.10)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 10.10.13.3 (10.10.13.3)
  Client MAC address: Dell_65:8f:37 (5c:26:0a:65:8f:37)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (t=53,l=1) DHCP Message Type = DHCP ACK
  Option: (t=58,l=4) Renewal Time Value = 12 hours
  Option: (t=59,l=4) Rebinding Time Value = 21 hours
  Option: (t=51,l=4) IP Address Lease Time = 1 day
  Option: (t=54,l=4) DHCP Server Identifier = 192.168.200.1
  Option: (t=1,l=4) Subnet Mask = 255.255.255.0
  Option: (t=15,l=8) Domain Name = "mrn.com"
  Option: (t=3,l=4) Router = 10.10.13.1
  Option: (t=6,l=4) Domain Name Server = 192.168.200.1
```

Figure A.36: DHCP Acknowledgement Packet

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Domain Name System

The domain name system (DNS) converts host names and Internet domains to IP addresses and vice versa. It is applied in TCP/IP networks. DNS services convert the DNS name entered by the user to its corresponding IP address. DNS is a distributed hierarchic database that maps URLs to 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

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

- **Forward DNS lookup**: Requests containing names and resulting in an IP address
- **Reverse DNS lookup**: Requests containing IP addresses and resulting in names

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

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

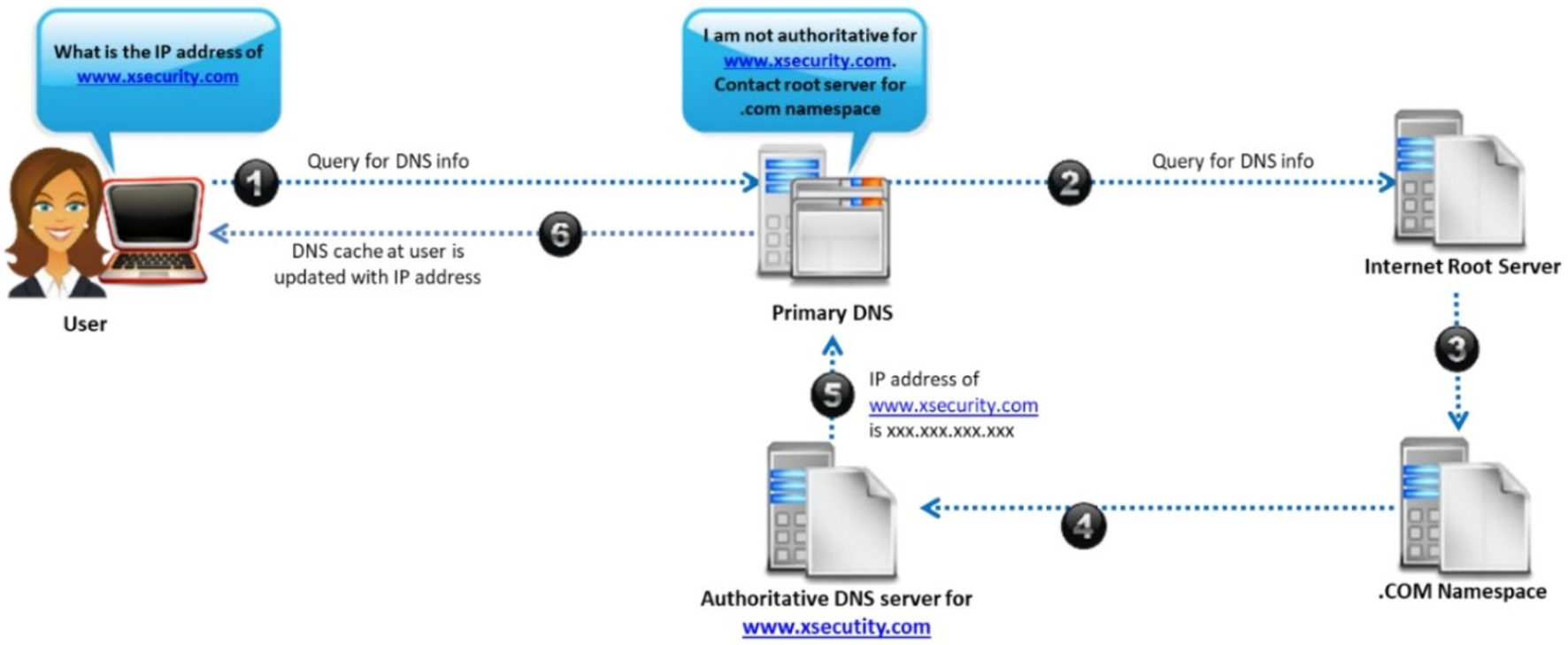
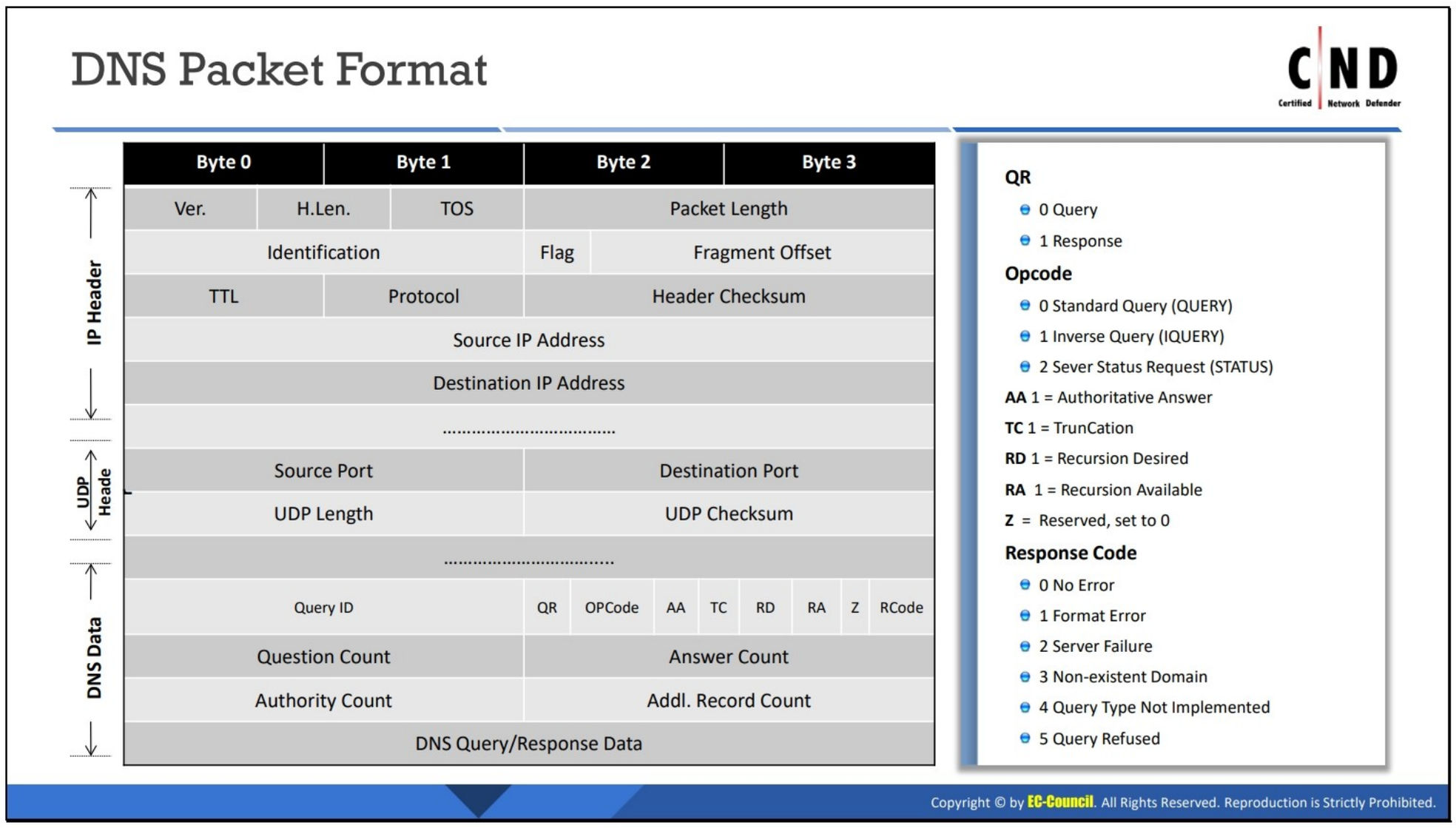


Figure A.37: Working of DNS

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DNS Packet Format

The DNS packet header consists of three sections: the 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 version. The value is always set as 4 for IPv4.
- **Header length (4 bits):** This field specifies the length of the IP header, which consists of 32-bit words along with IP options, if any. The minimum value of the IP header is 5.
- **Type of service (TOS) (8 bits):** This field provides quality of service features. The first three bits are for IP precedence, the next 4 bits are for TOS, and the last bit is left unused.
- **Total length (16 bits):** This field specifies the length of the IP datagram in bytes. It includes the length of the header and the data.
- **Identification (16 bits):** This field distinguishes the fragments of one datagram from those of another.
- **Fragment offset (13 bits):** This field is used to reassemble the fragmented IP datagrams.
- **Time to live (TTL):** This field 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):** This field identifies the next encapsulated protocol that sits above the IP layer.
- **Header checksum (16 bits):** This field identifies the errors during IP datagram transmission and is calculated based on the IP header.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Source/destination IP address:** This field specifies the IP addresses of the sender and 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 a random port that varies considerably.
- **Query ID:** This field is a unique identifier also termed as the transaction ID, and it is created in the query packet that is left intact by the server sending the reply. It helps in matching answers with awaiting questions.
- **Query/response (QR):** This field is set to "0" for a query by a client and "1" for a response from a server.
- **OP code:** This field is set by the client to "0" for a standard query, "1" for an inverse query (IQUERY), and "2" for sever status request (STATUS).
- **Authoritative answer (AA):** This field is set to "1" in a server response if this answer is authoritative; else, it is set to "0."
- **Truncated (TC):** This field is set to "1" in a server response if the answer cannot fit in the 512-byte limit of a UDP packet response. A value of "1" indicates that the message was truncated.
- **Recursion desired (RD):** This field is set in a query and indicates that the query should be pursued recursively. It is set to 1 if wishes the server to perform the entire lookup of the name recursively or 0 if the client simply wants the best information the server has.
- **Recursion available (RA):** A bit that is set (1) or cleared (0) in a response to indicate that recursion is available.
- **Reserved (Z):** This field is reserved and must be zero.
- **Response code:** This field contains the response code from the server and indicates success or failure.
  - 0—No error
  - 1—Format error
  - 2—Server failure
  - 3—Non-existent domain
  - 4—Query type not implemented
  - 5—Query refused
- **Question record count:** This field indicates the number of DNS queries in the questions section.
- **Answer count:** This field is set by the server and provides various kinds of answers to the query from the client.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Authority count:** This field indicates the number of name server records in the authority record section.
- **Additional record count:** This field indicates the number of resource records in the additional records section.
- **DNS question/answer data:** This field holds the question/answer data referenced by the count fields above.

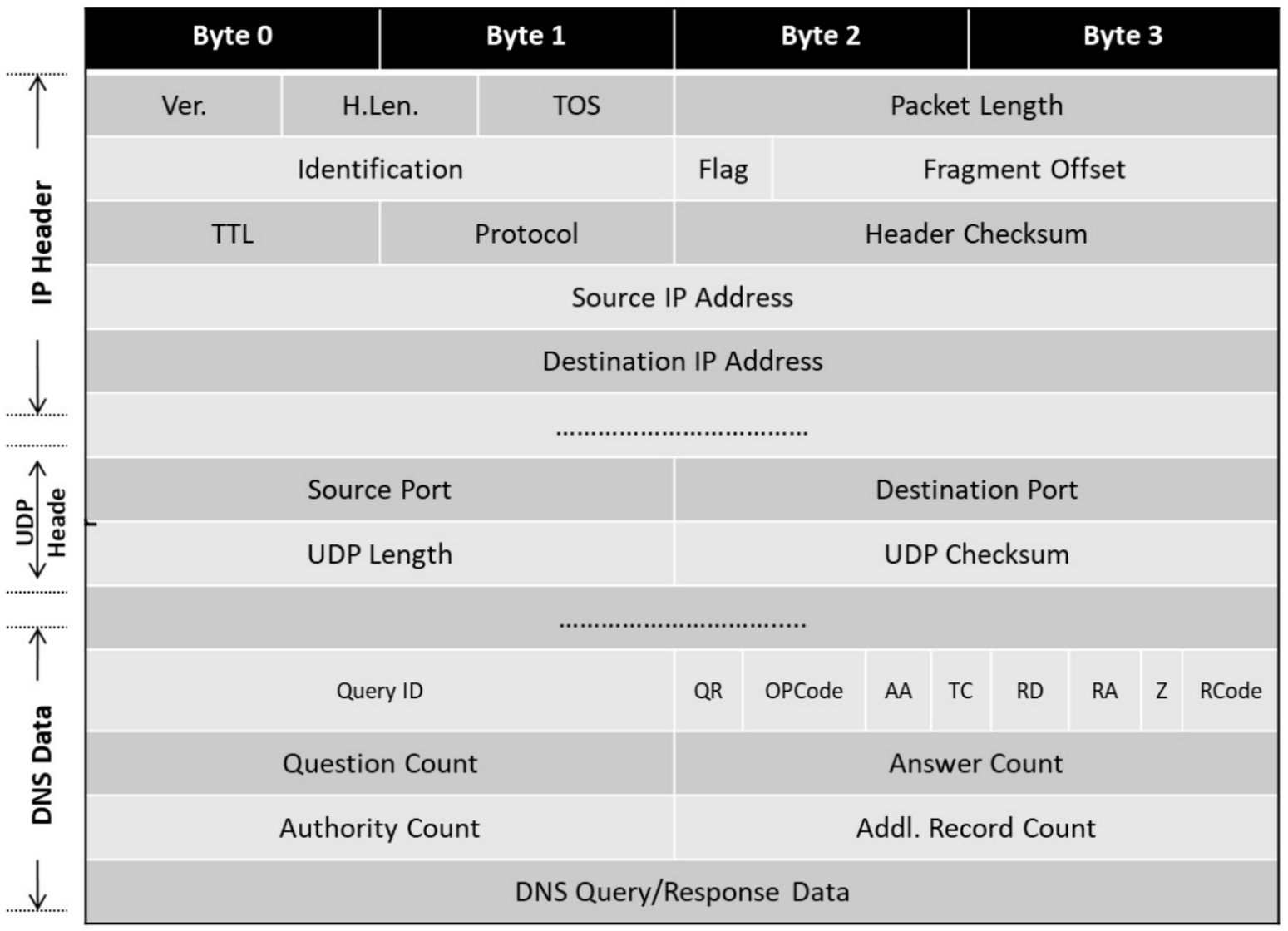
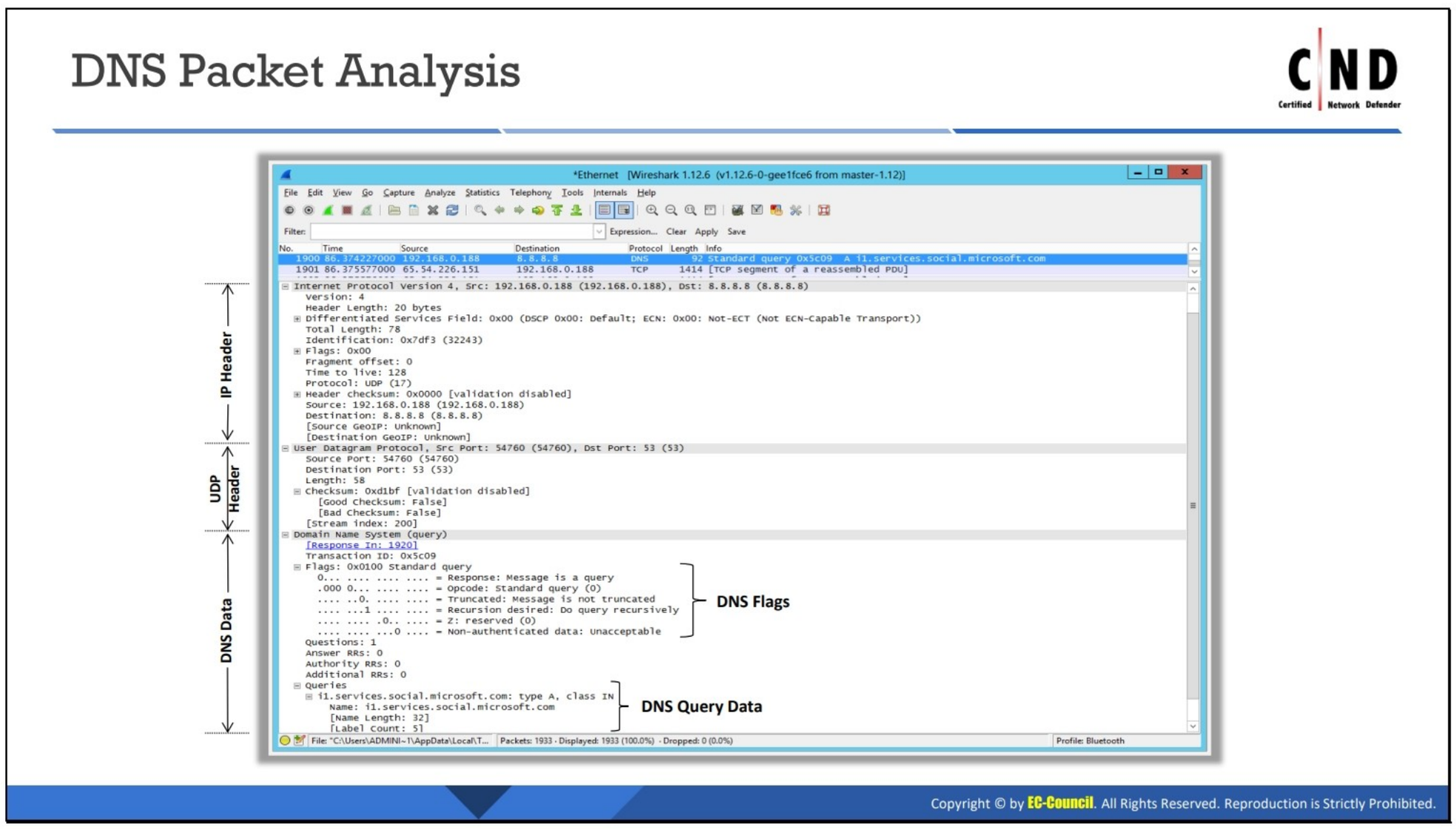


Figure A.38: DNS Packet Format

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DNS Packet Analysis

The DNS client/server communication involves two packets: one is the query packet, and the other is the response packet. If a client has an IP address and wants to know to whom the address belongs; it sends a query packet to the DNS server. The DNS server replies with a response packet that contains the information requested by the client. As in DHCP, DNS uses UDP as its transport protocol for communication.

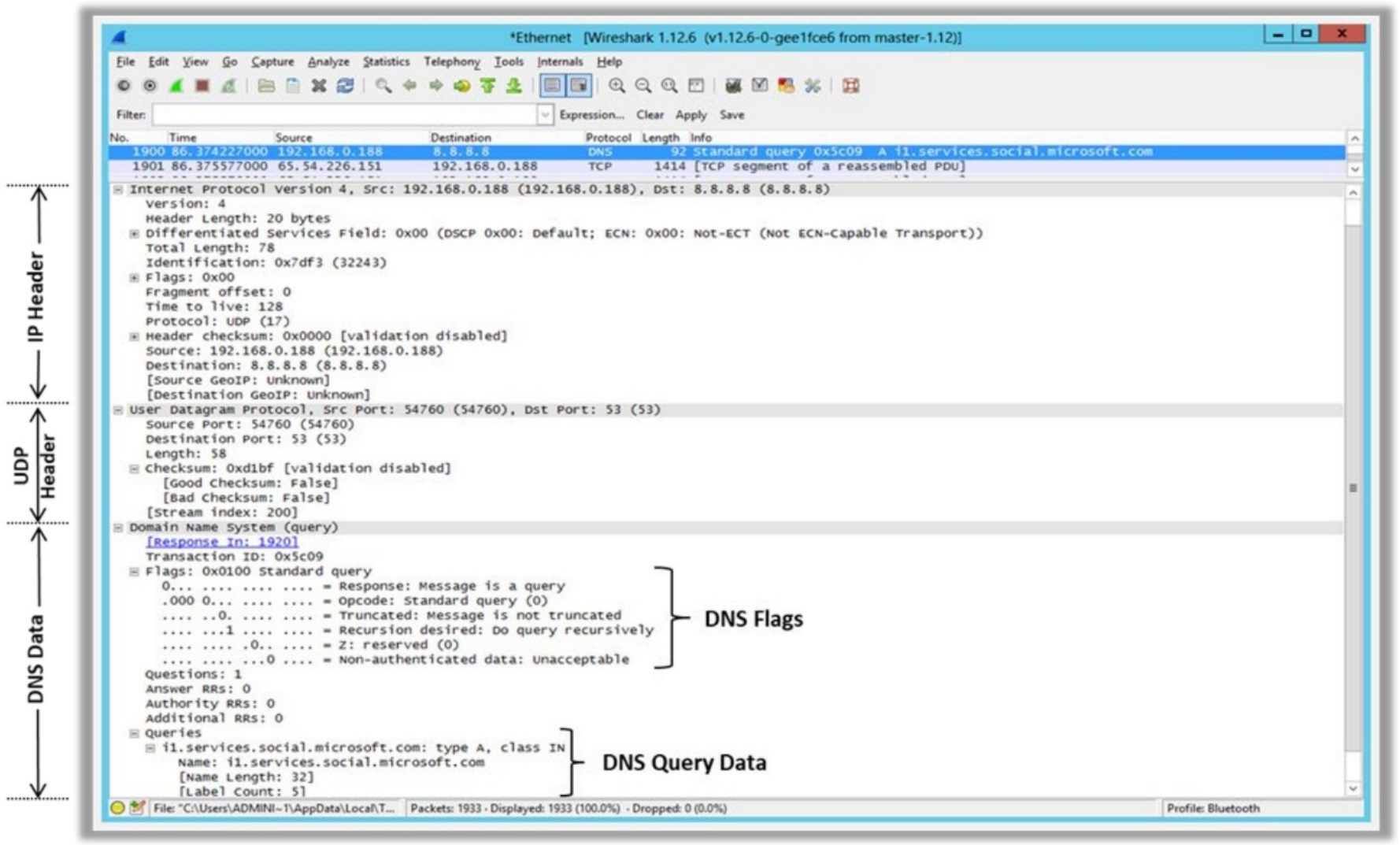


Figure A.39: Sample DNS Query Packet

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

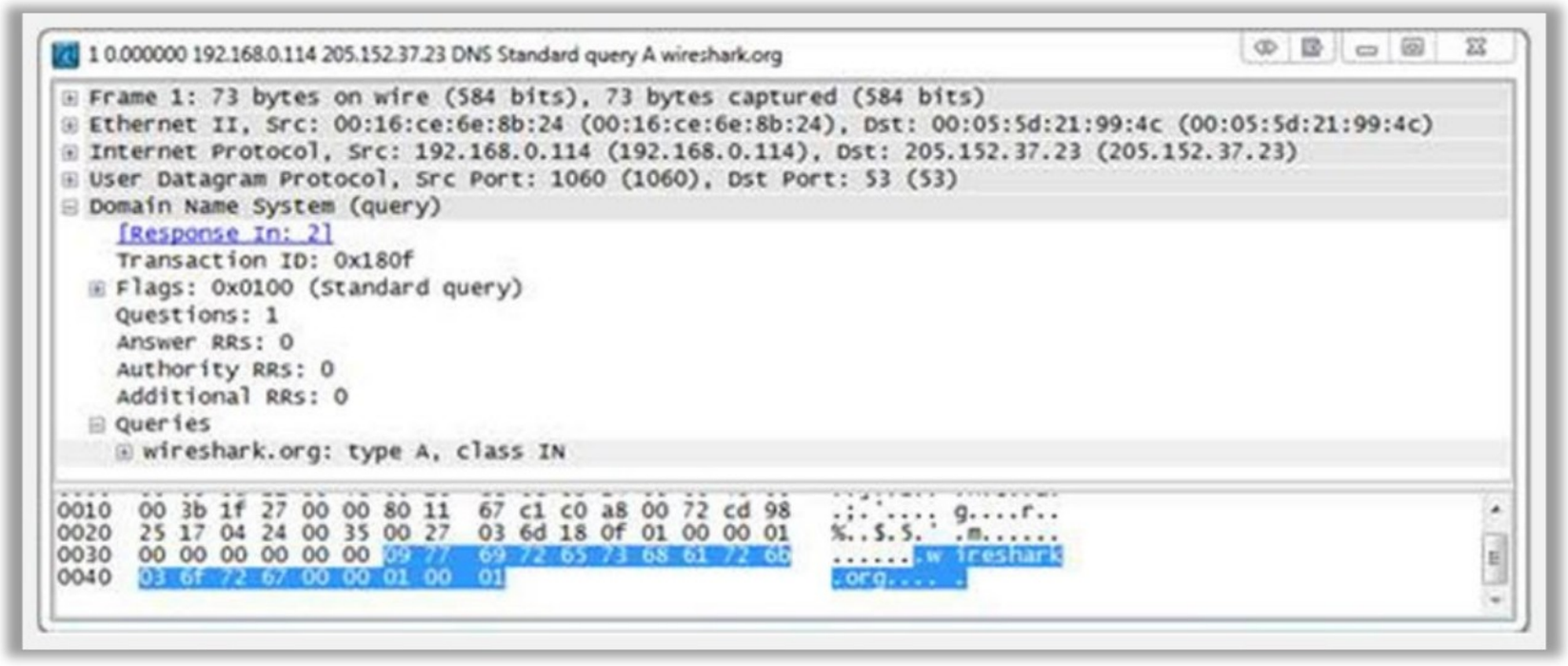


Figure A.40: DNS Query Packet

In the packet shown in Figure A.41, the client sends the query packet from port 1060 with IP address 192.168.0.114 to the DNS server port 53 (standard DNS port number) with IP address 205.152.37.23.

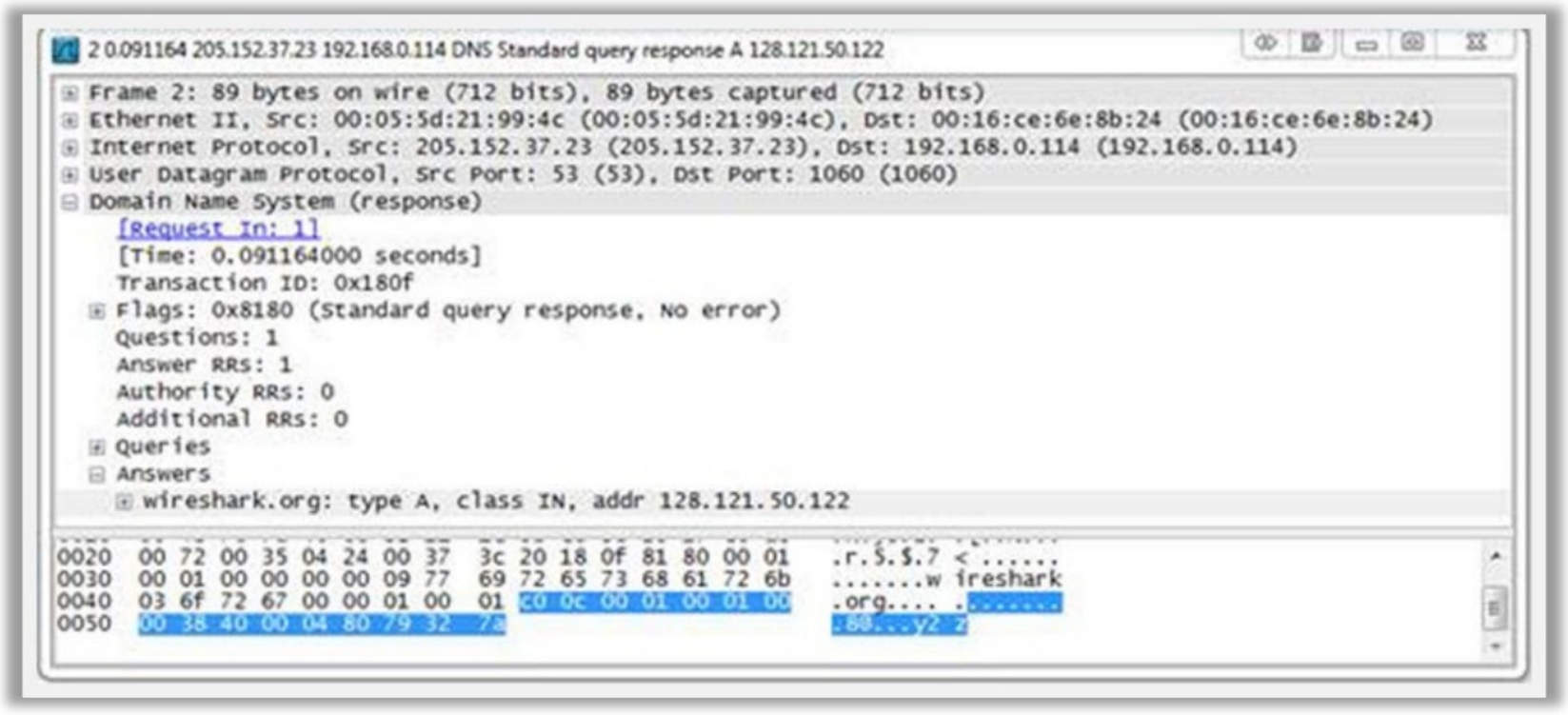
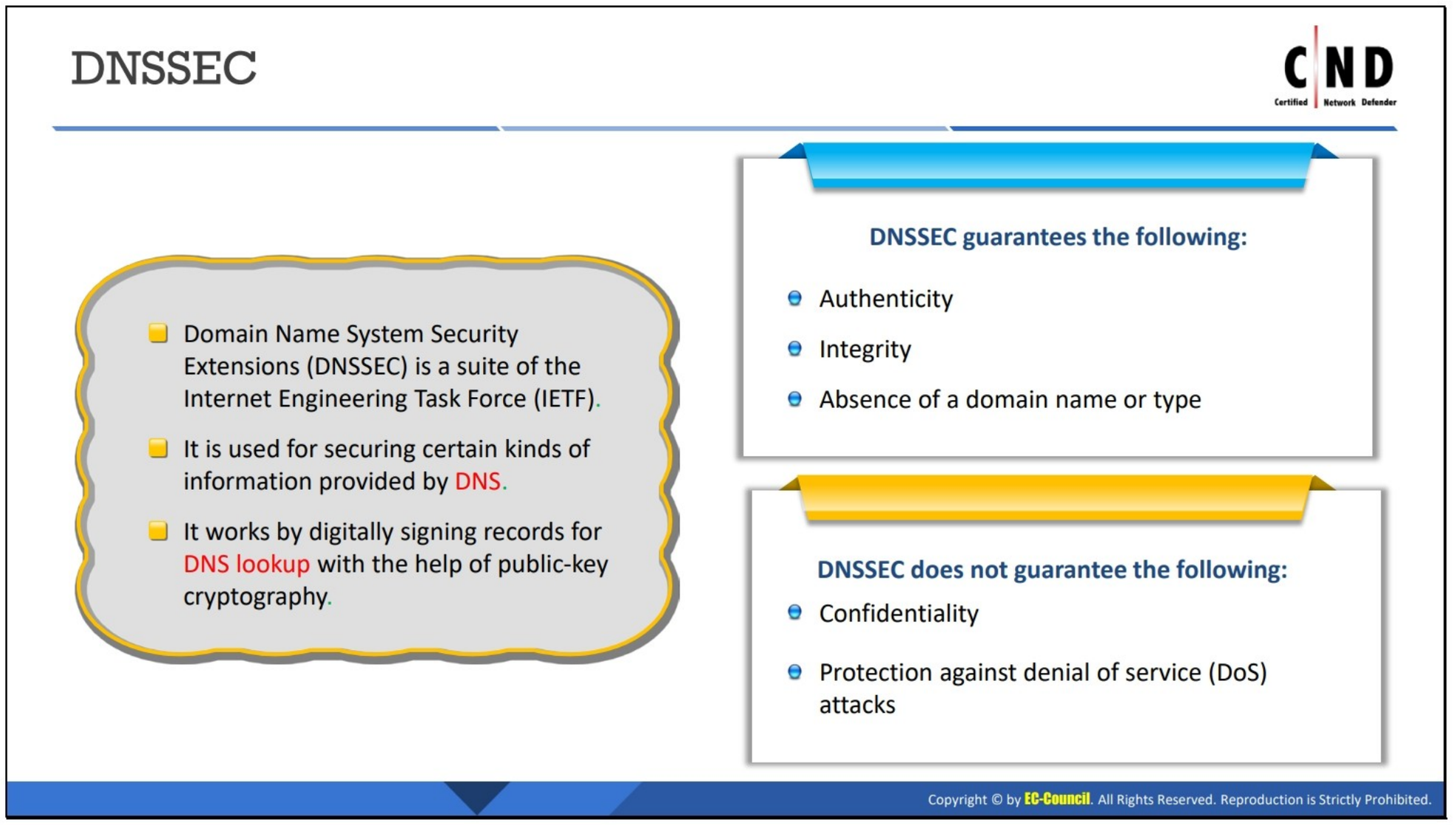


Figure A.41: DNS Response Packet

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DNSSEC

Domain Name System Security Extensions (DNSSEC) is a suite of specifications maintained by the Internet Engineering Task Force (IETF). It is used for securing certain kinds of information provided by DNS. It works by digitally signing records for DNS lookup with the help of public-key cryptography. DNSSEC provides security from attacks such as spoofing and poisoning, which aim to compromise DNS servers. DNSSEC secures DNS servers by validating DNS responses through authentication.

Figure A.42 shows the functioning of DNSSEC in validating responses and preventing attacks on the DNS server and client.

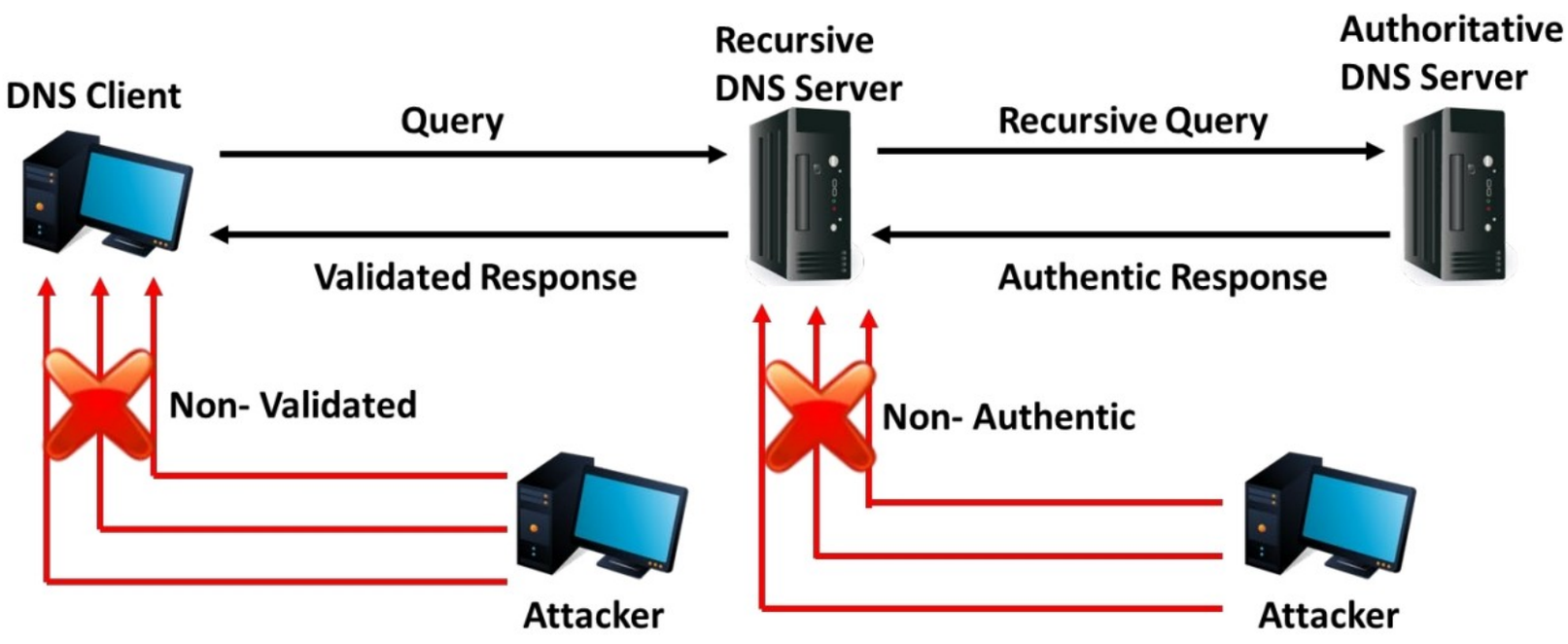


Figure A.42: DNSSEC Validation of Queries and Responses

For communication with DNSSEC, both parties should be configured with DNSSEC support. For security, DNSSEC requires four additional resources: resource record signatures (RRSIGs), DNS

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

public key (DNSKEY), next secure record (NSEC), and delegation signer (DS). With the combination of these four resources, DNSSEC provides the following functionalities:

- Maintains authentic responses to the desired requests only
- Maintains data integrity
- Monitors responses to requests made by clients

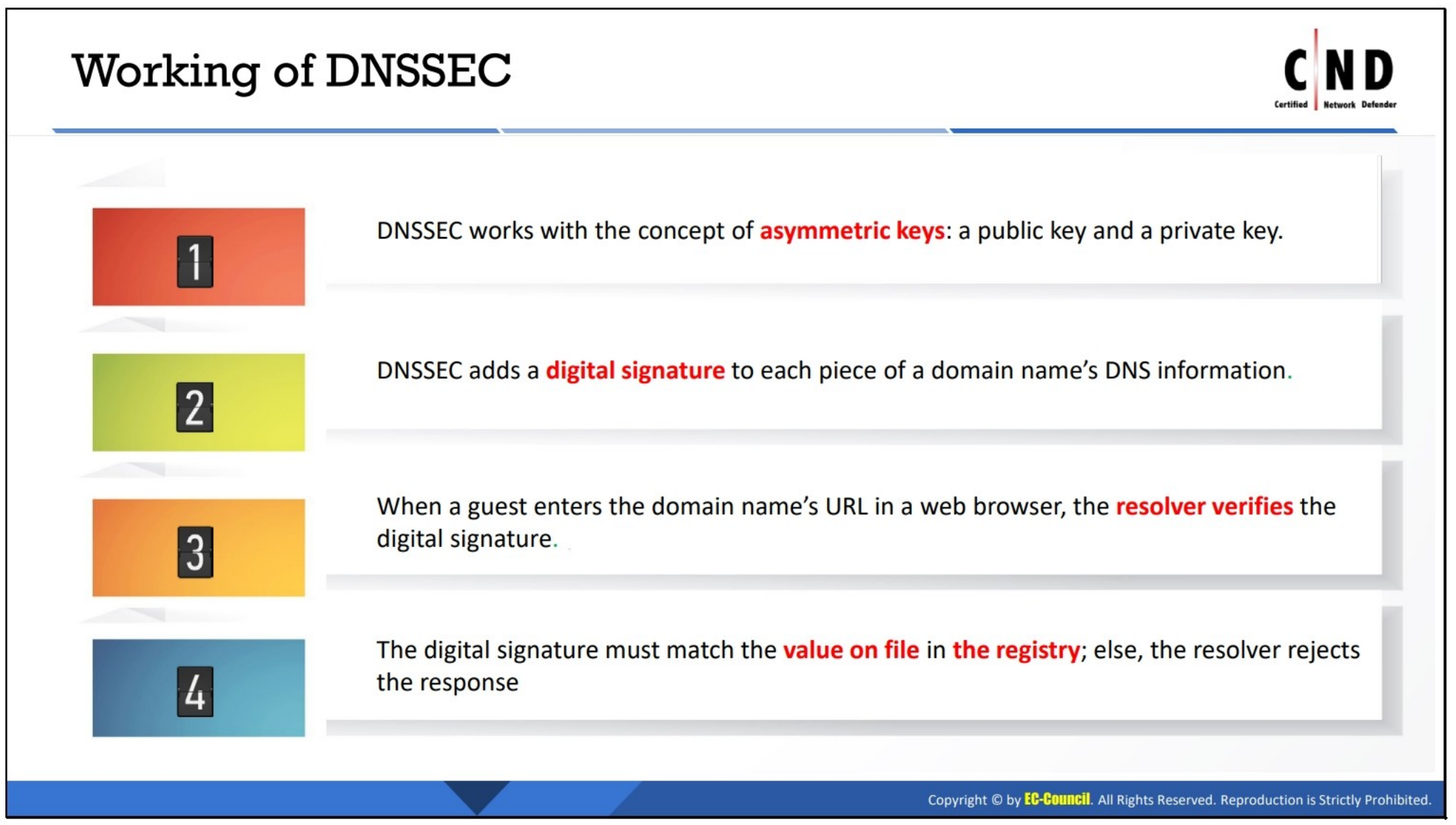
DNSSEC guarantees the following:

- Authenticity
- Integrity
- Absence of a domain name or type

DNSSEC does not guarantee the following:

- Confidentiality
- Protection against denial of service (DoS) attacks

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Working of DNSSEC

DNSSEC works with the concept of asymmetric keys: a public key and a private key. DNSSEC adds a digital signature to each piece of a domain name's DNS information. When a guest enters the domain name's URL in a web browser, the resolver verifies the digital signature. The digital signature must match the value on file in the registry; else, the resolver rejects the response.

Through the DNSSEC signing process, the DNS server zone is secured from attacks without any functional changes. By accepting DNSSEC signing, DNS responses are allowed for validation through digital signatures. These digital signatures are cryptographically encrypted. After completion of the signing process, the DNSSEC's resource records process the digital signatures and append them to DNS responses. Figure A.43 shows the signing of DNS resource records.

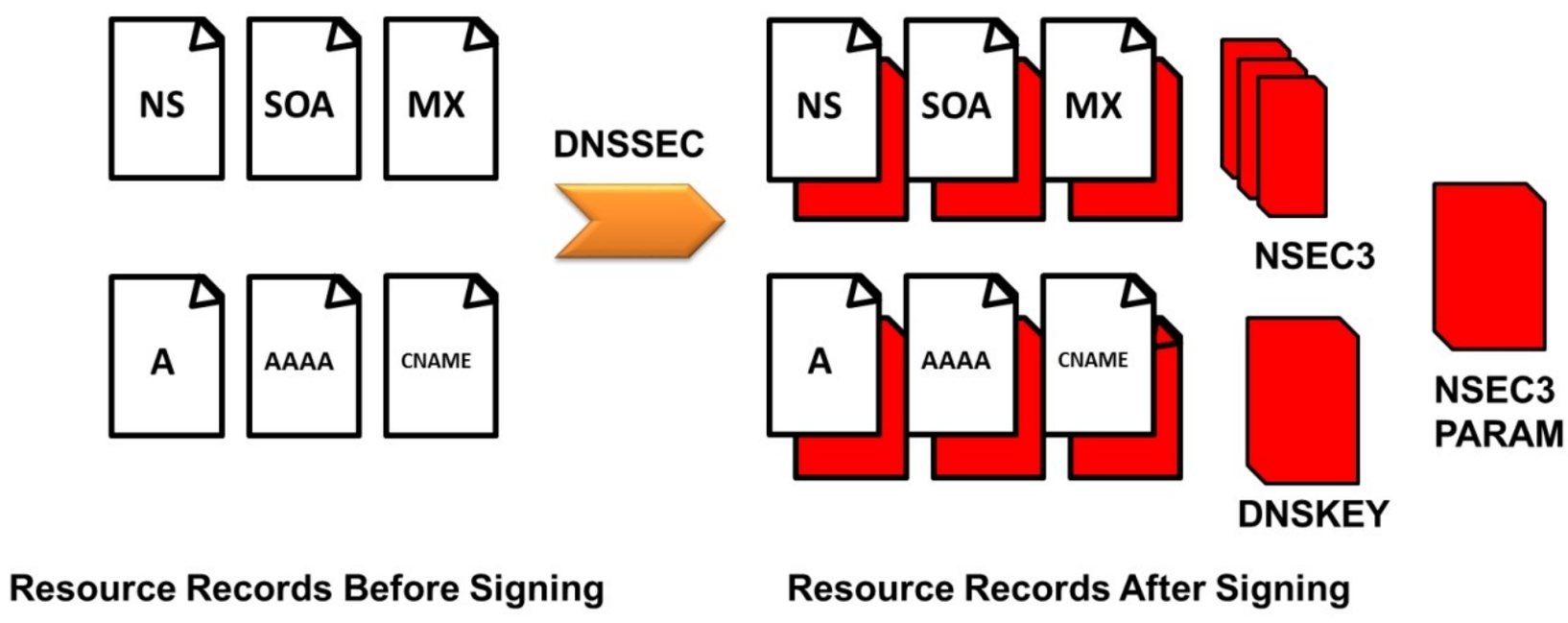


Figure A.43: Unsigned and Signed DNS Resource Records

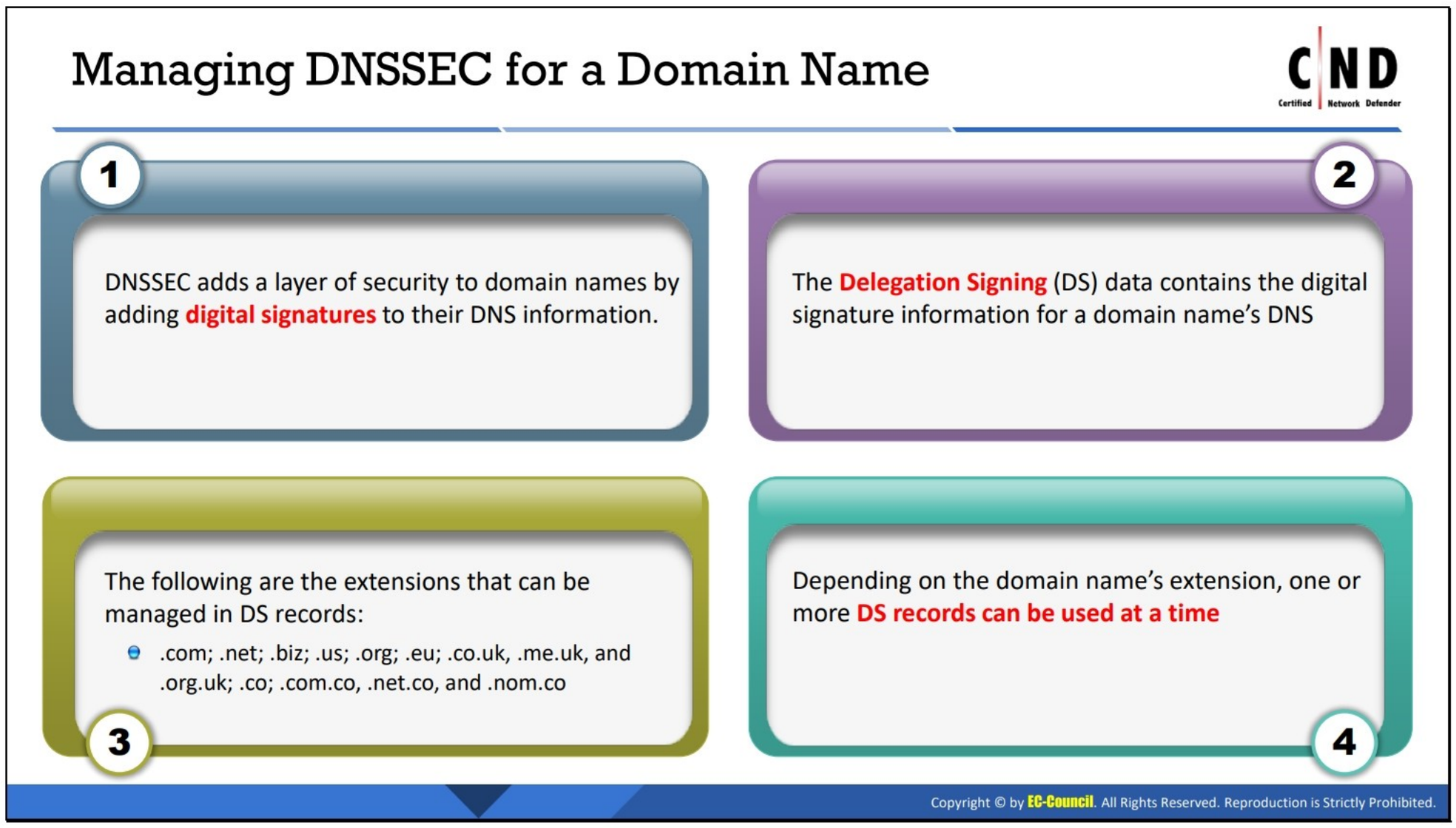
The red records are digitally signed records (RRSIGs) associated with each DNS record. These signatures ensure that the DNS responses are from a valid DNSSEC-signed DNS zone and not from

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

an attacker. The DNSKEY holds the public key of the encrypted records, whereas the hash of a DNSKEY record is stored in DS. NSE3 is used for the explicit denial of existence of a DNS record.

DNSSEC validation: DNS responses are validated through the decryption of their digital signatures; this decryption is performed with DNSKEY resource records. During this validation process, the hash values of the DNSSEC resource record are compared, and a response is sent accordingly. If the hash values are identical, then a DNS reply is sent to the DNS client; else, a SERVFAIL is sent.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



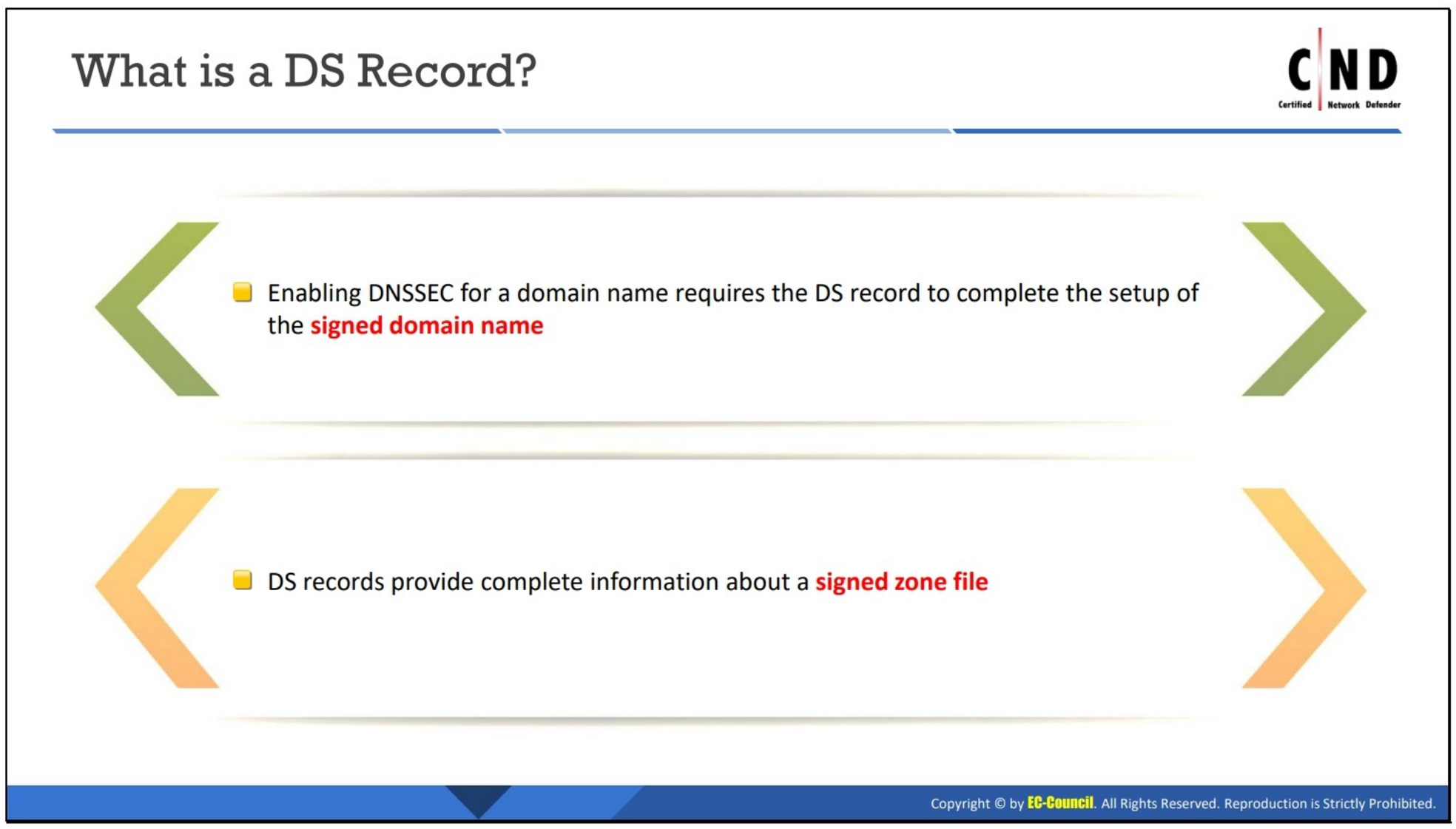
Managing DNSSEC for a Domain Name

DNSSEC adds a layer of security to domain names by adding digital signatures to their DNS information. The Delegation Signing (DS) data contains the digital signature information for the corresponding domain name's DNS. The signed zone file information can be obtained through the DS record. The DS records can be managed by adding new records or editing or deleting existing records. Depending on the domain name's extension, one or more DS records can be used at a time.

The following are some extensions that can be managed in DS records:

.com, .net, .biz, .us, .org, .eu, .co.uk, .me.uk, .org.uk, .co, .com.co, .net.co, and .nom.co

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is a DS Record?

DS records provide complete information about a signed zone file. The record is primarily used in the process of DNS and DNSKEY authentication. Enabling DNSSEC for a domain name requires this information to complete the setup of the signed domain name. The DS record is used for referencing the DNSKEY record through the following fields.

- **Key tag**: This is a numeric element that can be used for referencing the identified DNSKEY record. The key tags of the DS record and RRSIG record are identical.
- **Algorithm**: This field contains a number called the algorithm number of the DNSKEY record. This number is referred to by the DS record for the DNSKEY record. The DS record, RRSIG record, and DNSKEY record possess the same algorithm number.
- **Digest**: This the cryptographic hash value of the DNSKEY record.
- **Digest type**: The DS record uses the digest of the DNSKEY record to refer to it.

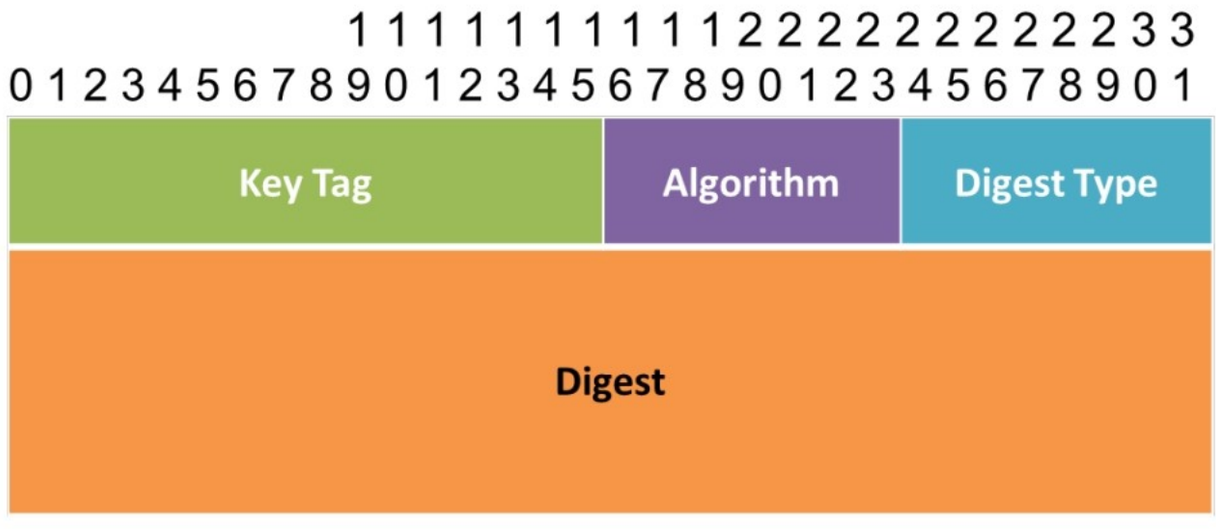
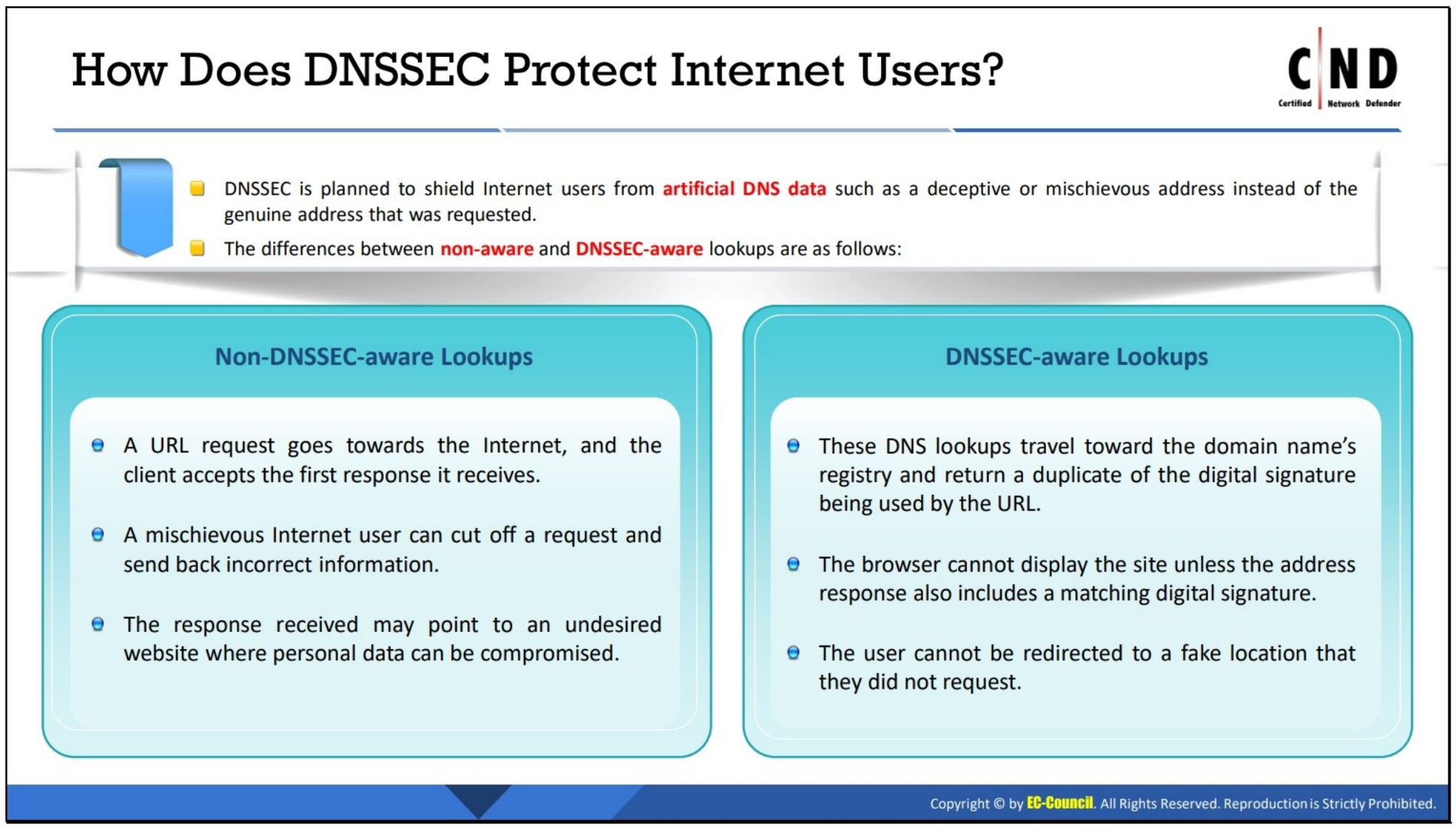


Figure A.44: DS Record Format

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How Does DNSSEC Protect Internet Users?

DNSSEC provides foolproof security services to Internet users. Users can freely browse the Internet as DNSSEC ensures that they always connect to genuine DNS servers instead of malicious ones.

DNSSEC is planned to shield Internet users from artificial DNS data such as a deceptive or mischievous address instead of the genuine address that was requested.

The differences between non-aware and DNSSEC-aware lookups are discussed below.

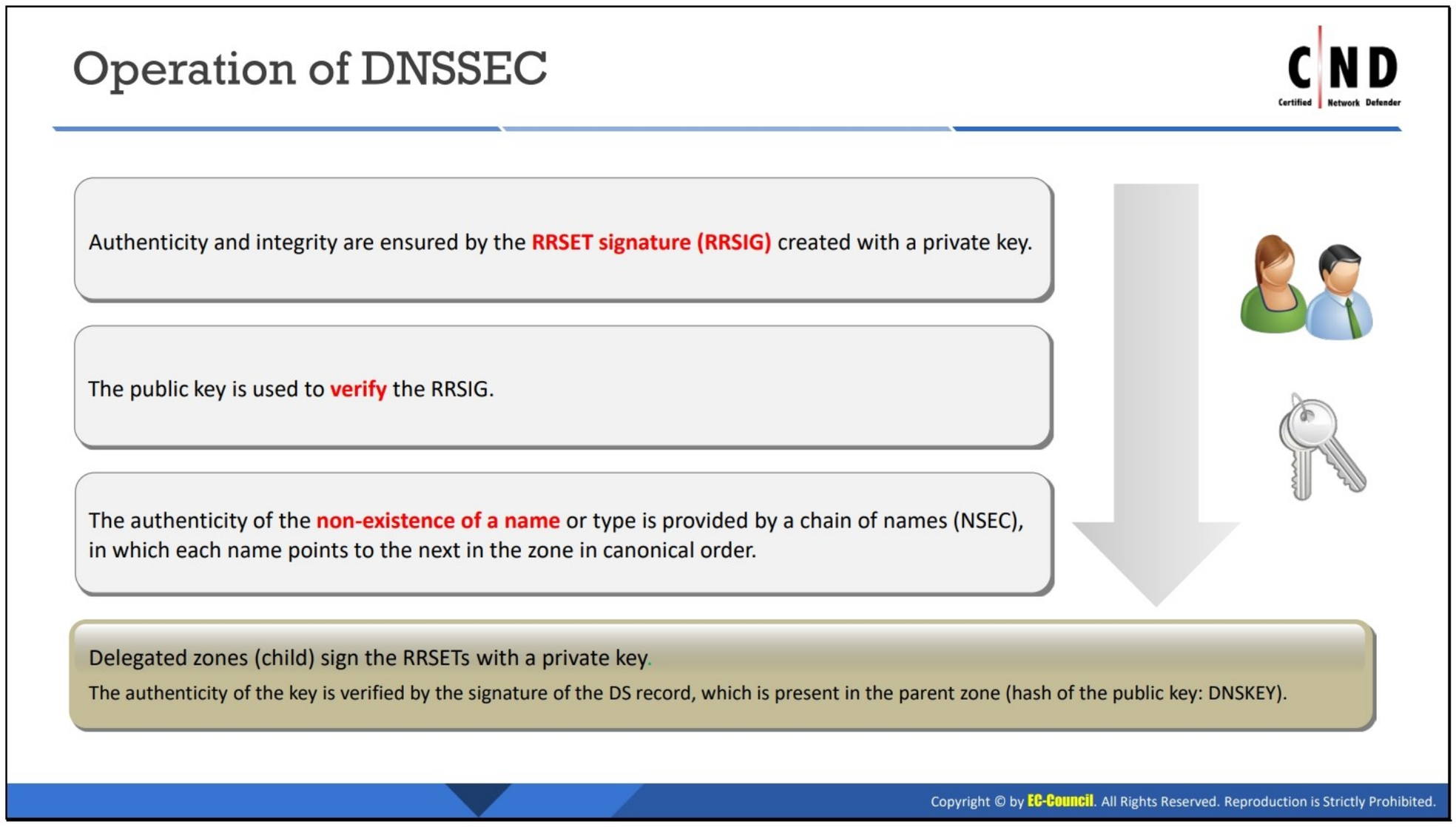
Non-DNSSEC-aware lookups:

- A URL request goes towards the Internet, and the client accepts the first response it receives.
- A mischievous Internet user can cut off a request and send back incorrect information.
- The response received may point to an undesired website where personal data can be compromised.

DNSSEC-aware lookups:

- These DNS lookups travel toward the domain name's registry and return a duplicate of the digital signature being used by the URL.
- The browser cannot display the site unless the address response also includes a matching digital signature.
- The user cannot be redirected to a fake location that they did not request.

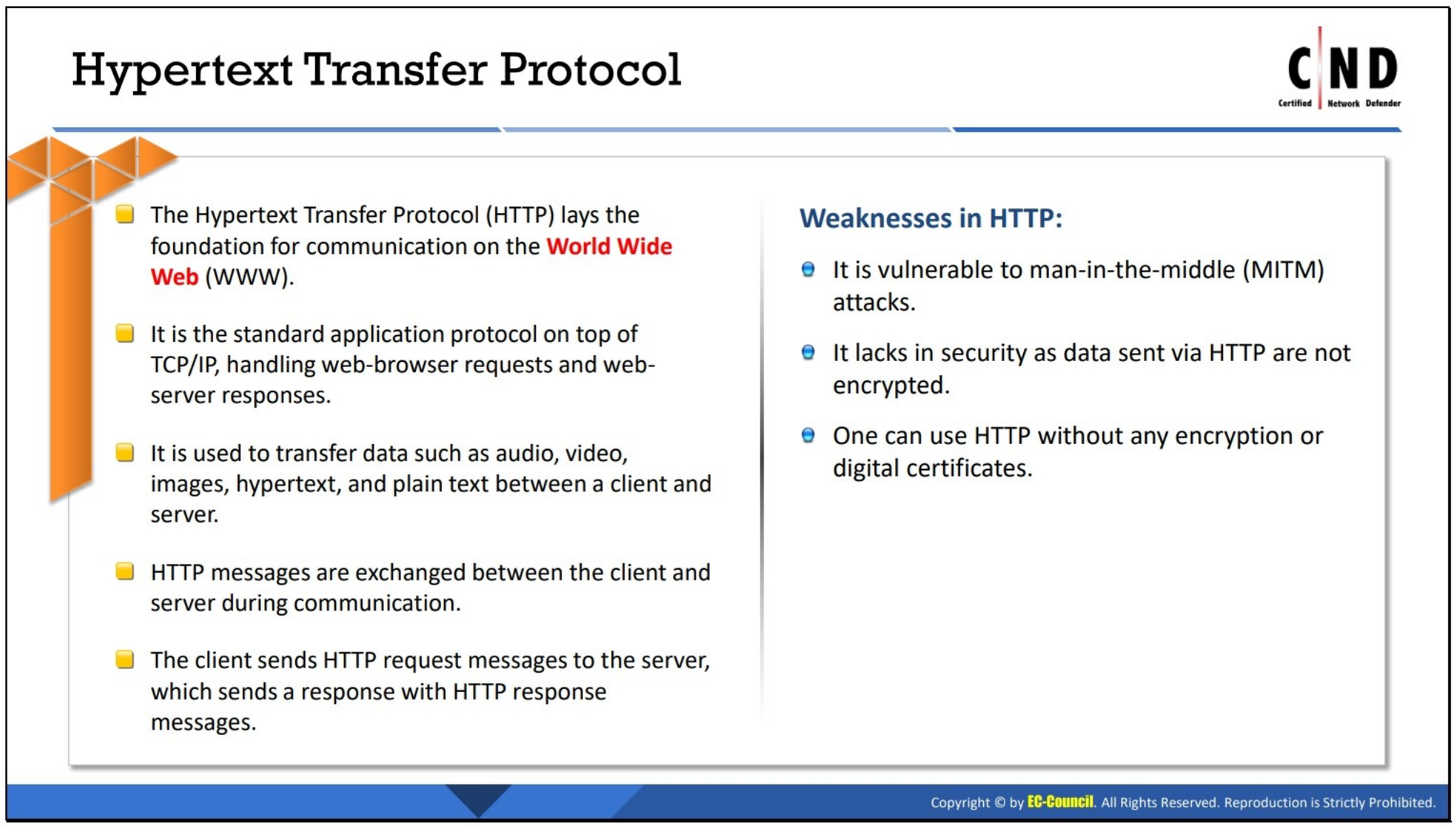
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Operation of DNSSEC

Authenticity and integrity are ensured by the RRSET signature (RRSIG) created with a private key. The public key is used to verify the RRSIG. The authenticity of the non-existence of a name or type is provided by a chain of names (NSEC), in which each name points to the next in the zone in canonical order. Delegated zones (child) sign RRSETs with a private key. The authenticity of the key is verified by the signature of the DS record, which is present in the parent zone (hash of the public key: DNSKEY).

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hypertext Transfer Protocol

HTTP lays the foundation for communication in the World Wide Web (WWW). It is the standard application protocol on top of TCP/IP, handling web-browser requests and web-server responses. It is used to transfer data such as audio, video, images, hypertext, and plain text between a client and server. HTTP messages are exchanged between the client and server during communication. The client sends HTTP request messages to the server, which sends a response with HTTP response messages.

HTTP is a major component for establishing communication between web browsers and web servers. Its provides users access to the web server's resources. There are numerous resources such as HTML pages, images, and text files available from web servers around the world; a user can access these resources from their house without much effort. When a user wishes to access a resource, they simply enter the URL of the resource in their browser, and an HTTP request message is sent to the server that contains the resource. If the resource is available and there is no issue with the request, then the server replies with an HTTP response message along with access to the request. To send a request to a web server, various request methods are available in HTTP for different types of user requests.

The following are some common HTTP requests.

- **GET**: This method is used to request and obtain a resource from the server.
- **PUT**: This method is used to send data to the server to store the data in its database.
- **DELETE**: This method is used for deleting a resource in the web server.
- **POST**: This method is used to send data to a server gateway application.
- **HEAD**: This method makes the same request as the GET method.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Apart from status codes, HTTP also contains a code called the HTTP status code, which is used by the server to intimate the result of the request made by the web browser. Based on these codes, the browser or user can know whether the request is successfully completed or any error occurred during the request.

The following are some common HTTP status codes and their meanings:

- **100**—Continue
- **200**—Ok
- **202**—Accept
- **204**—No content
- **400**—Bad request
- **404**—Not found
- **408**—Request timeout
- **500**—Internal server error
- **504**—Gateway timeout
- **505**—HTTP version not supported

HTTP request/response messages are quite easy for users to understand. Figures 0.45 and 0.46 show sample HTTP request and response messages, respectively.

```
GET /tutorials/other/top-20-mysql-best-practices/ HTTP/1.1
Host: net.tutsplus.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: PHPSESSID=r2t5uvjq435r4q7ib3vtdjq120
Pragma: no-cache
Cache-Control: no-cache
```

Figure A.45: HTTP Request

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
HTTP/1.x 200 OK
Transfer-Encoding: chunked
Date: Sat, 28 Nov 2009 04:36:25 GMT
Server: LiteSpeed
Connection: close
X-Powered-By: W3 Total Cache/0.8
Pragma: public
Expires: Sat, 28 Nov 2009 05:36:25 GMT
Etag: "pub1259380237;gz"
Cache-Control: max-age=3600, public
Content-Type: text/html; charset=UTF-8
Last-Modified: Sat, 28 Nov 2009 03:50:37 GMT
X-Pingback: http://net.tutsplus.com/xmlrpc.php
Content-Encoding: gzip
Vary: Accept-Encoding, Cookie, User-Agent

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-str
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Top 20+ MySQL Best Practices - Nettuts+</title>
<!-- ... rest of the html ... -->
```

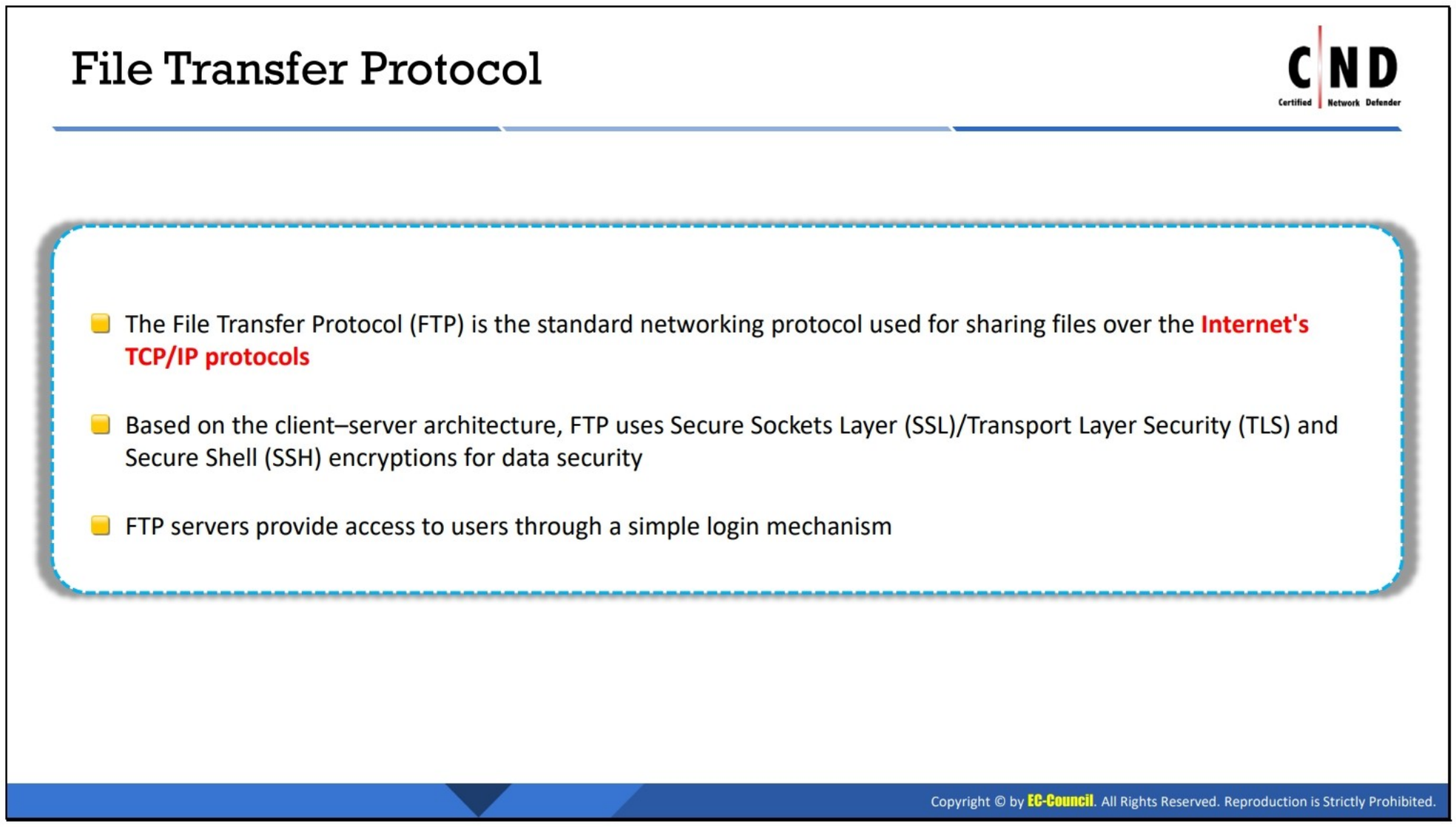
Figure A.46: HTTP Response

When a request is made, it must pass through many hurdles in the network(s) as well as many networking devices to reach its destination. Even the response message must face many issues to reach the client. To overcome these hurdles, HTTP relies on TCP/IP to send and receive the messages.

Weaknesses in HTTP:

- It is vulnerable to man-in-the-middle (MITM) attacks.
- It lacks in security as data sent via HTTP are not encrypted.
- One can use HTTP without any encryption or digital certificates.

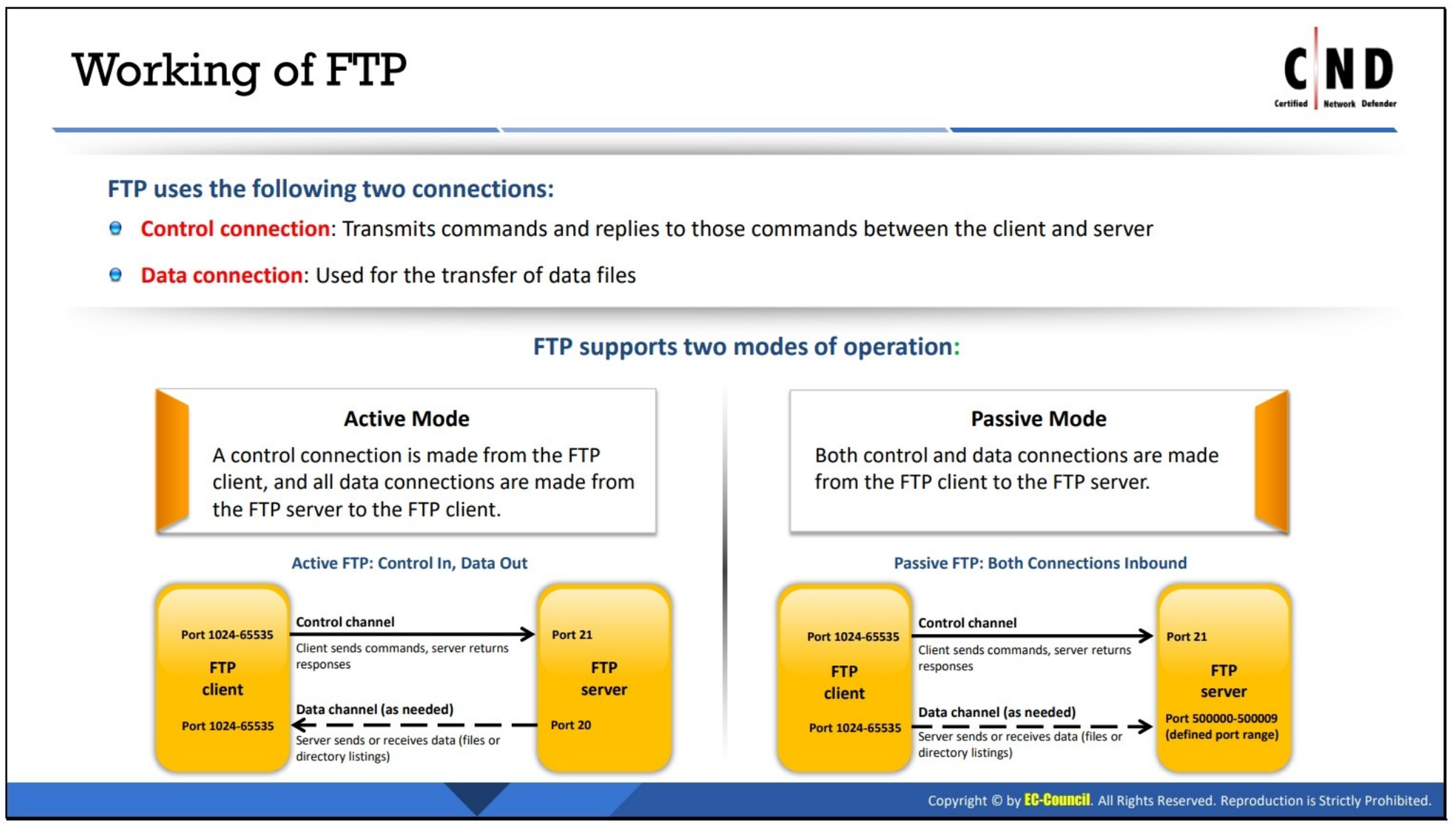
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



File Transfer Protocol

FTP is the standard networking protocol used for sharing files over the Internet's TCP/IP protocols. Based on the client–server architecture, FTP uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) and Secure Shell (SSH) encryptions for data security. FTP servers provide access to users through a simple login mechanism.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Working of FTP

FTP uses the following two connections.

- **Control connection**: Transmits commands and replies to those commands between the client and the server
- **Data connection**: Used for the transfer of data files

FTP supports two modes of operation: active and passive.

Active Mode

In the active mode, a control connection is made from the FTP client, and all data connections are made from the FTP server to FTP client.

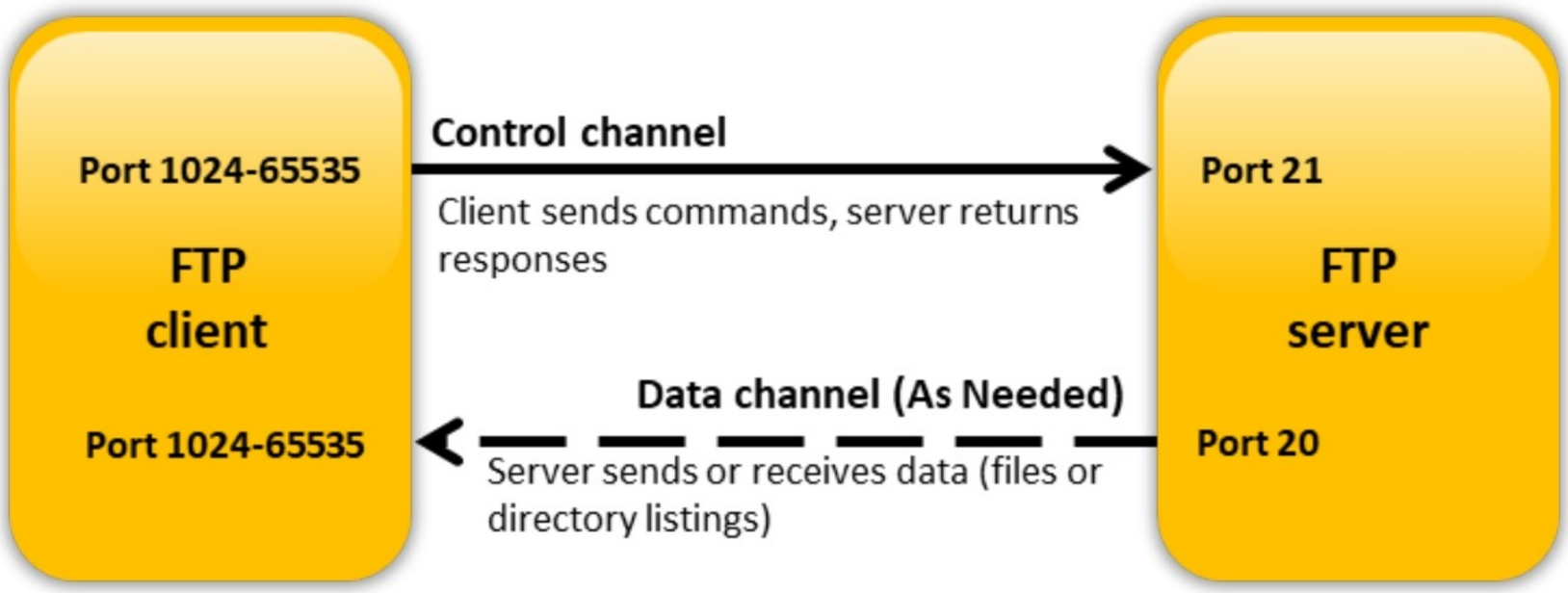


Figure A.47: Active FTP: Control In, Data Out

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Passive Mode

In the passive mode, both control and data connections are made from the FTP client to the FTP server.

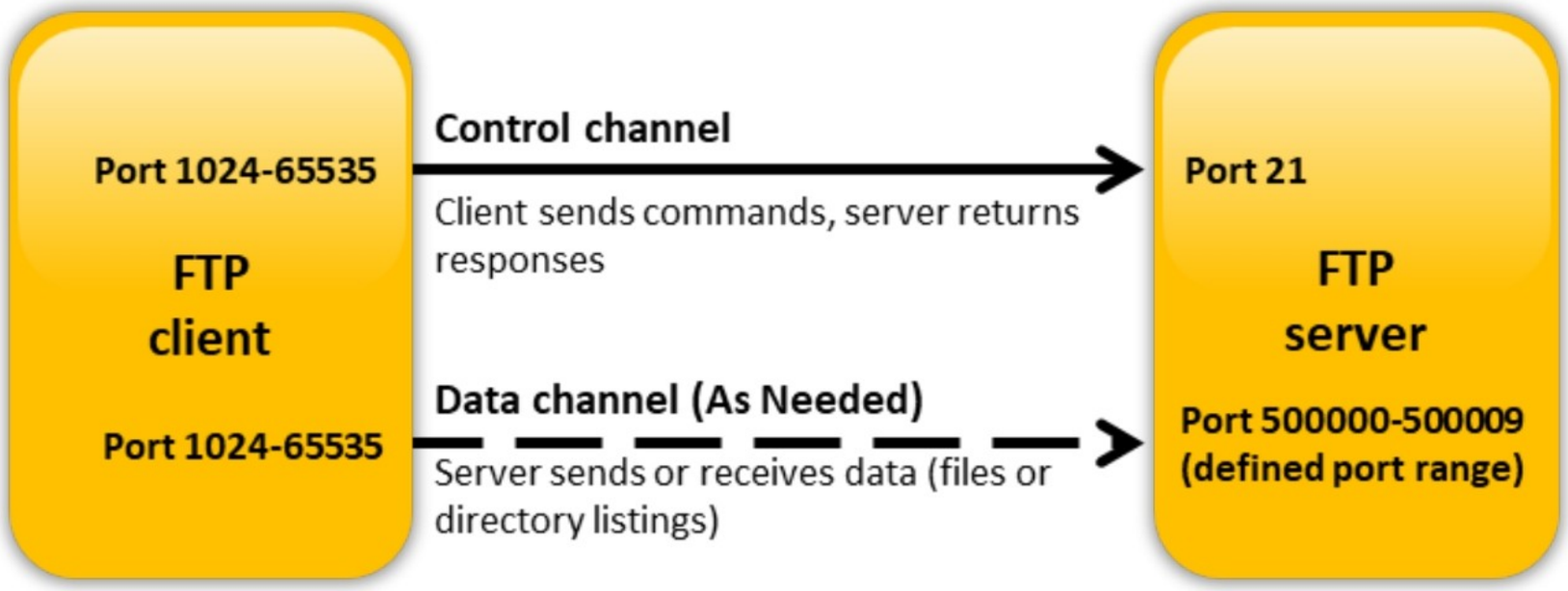
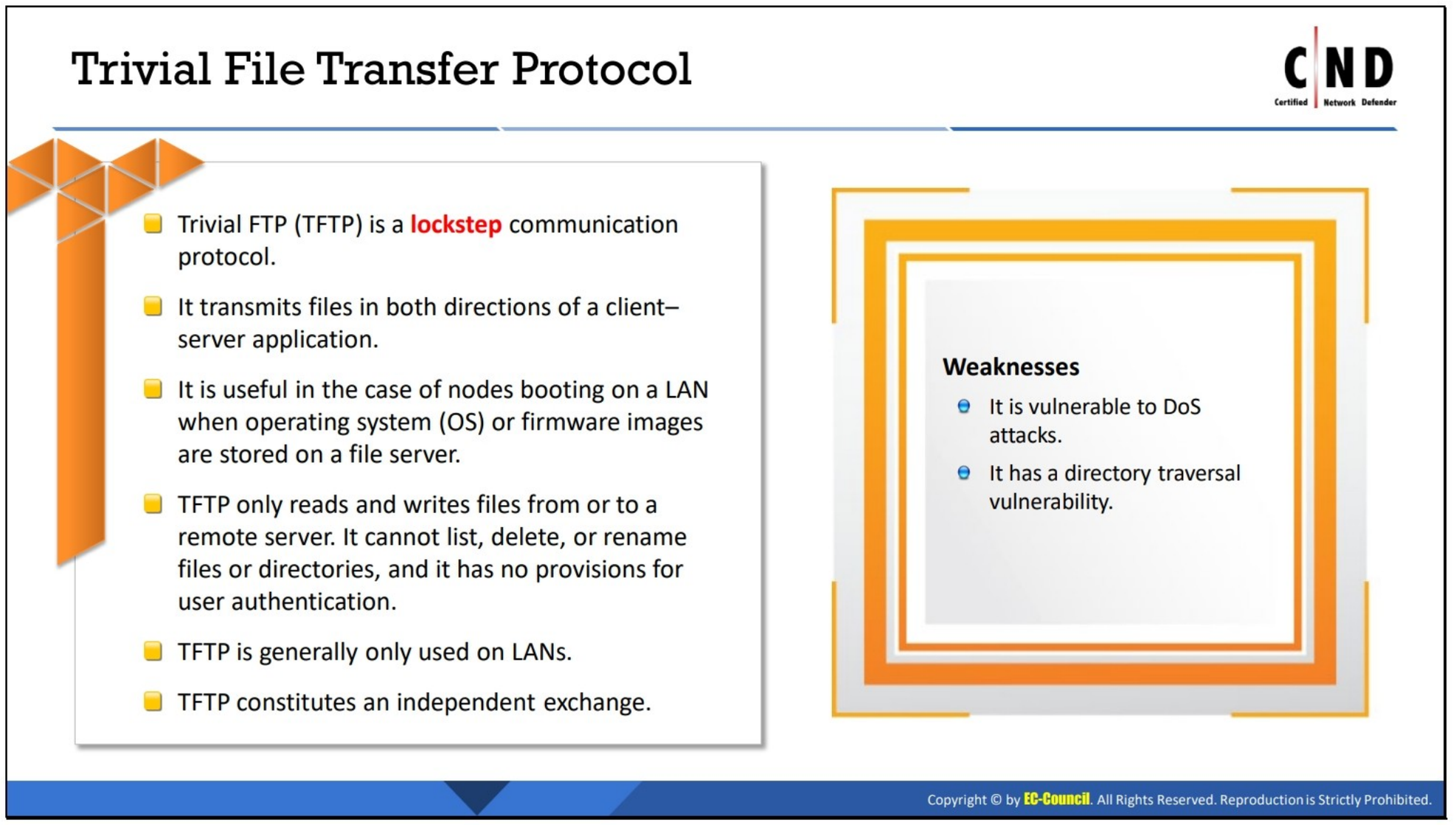


Figure A.48: Passive FTP: Both Connections are Inbound

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



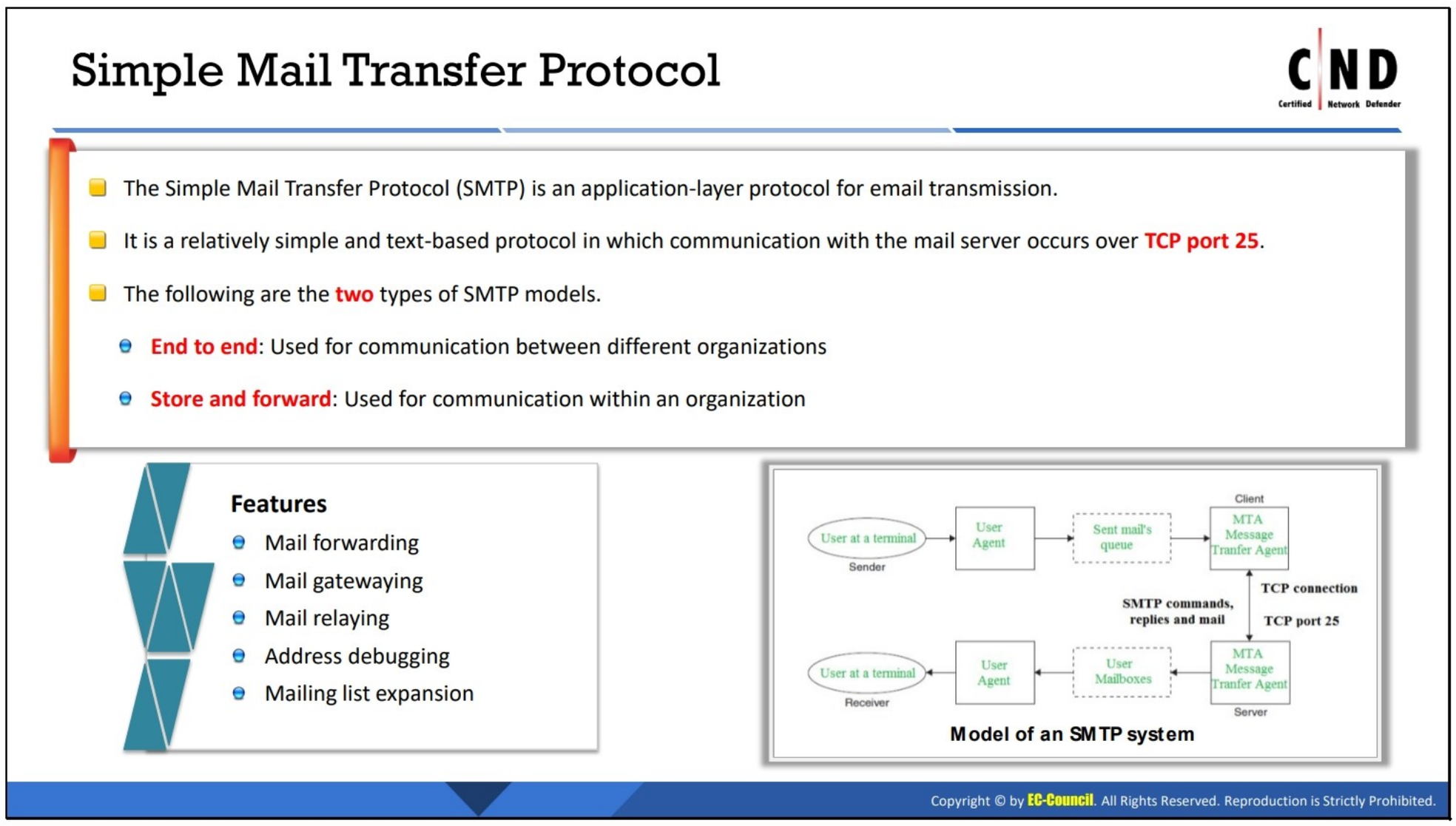
Trivial File Transfer Protocol

Trivial FTP (TFTP) is a lockstep communication protocol that transmits files in both directions of a client–server application. It is useful in the case of nodes booting on a LAN when operating system (OS) or firmware images are stored on a file server. TFTP only reads and writes files from or to a remote server. It cannot list, delete, or rename files or directories, and it has no provisions for user authentication. TFTP is generally only used on LANs. TFTP constitutes an independent exchange.

Weaknesses

- It is vulnerable to DoS attacks.
- It has a directory traversal vulnerability.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Simple Mail Transfer Protocol

SMTP is an application-layer protocol for email transmission. It is a relatively simple and text-based protocol in which communication with the mail server occurs over TCP port 25.

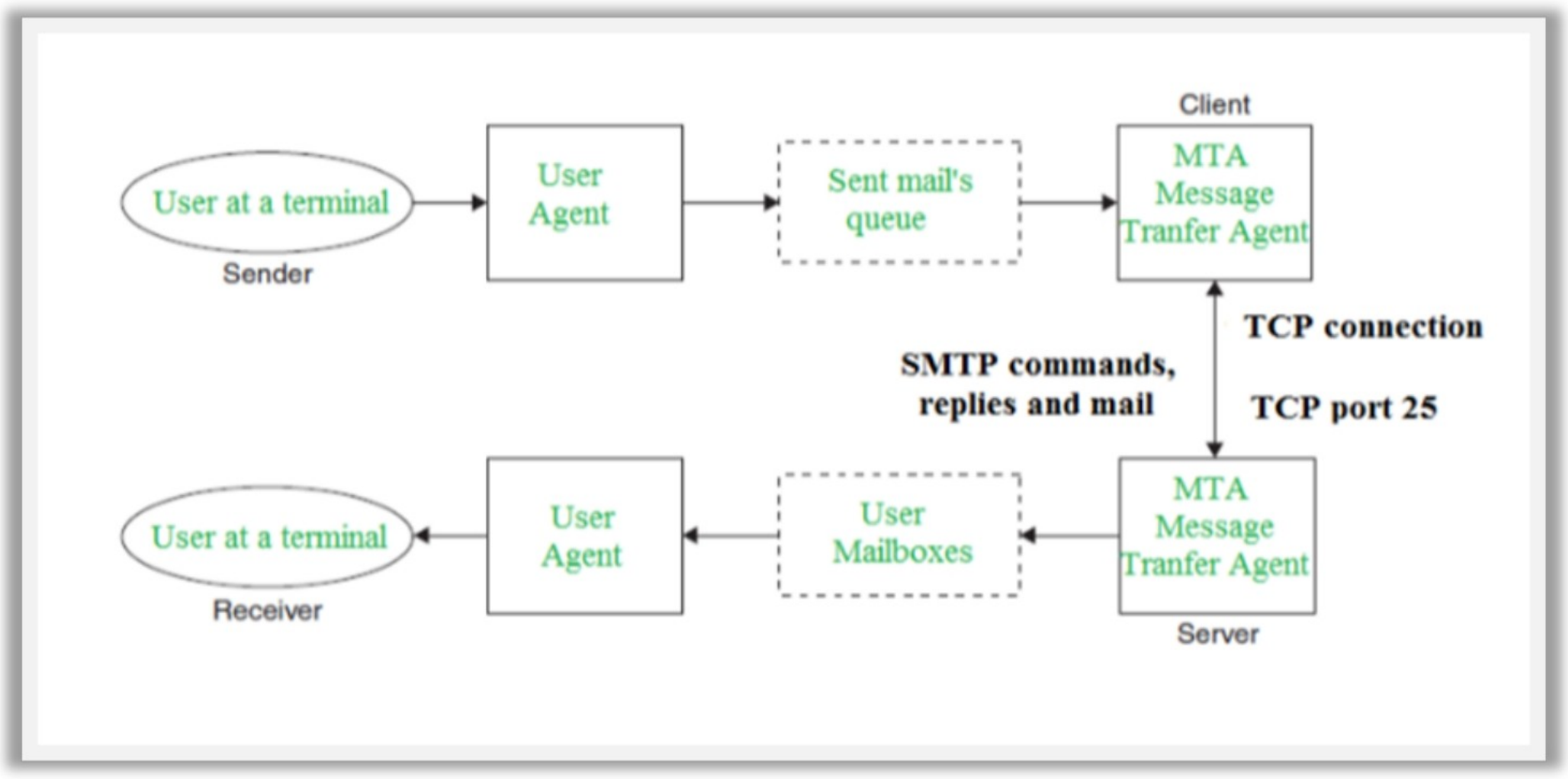


Figure A.49: Model of SMTP

The following are the two types of SMTP models.

- **End to end**: Used for communication between different organizations
- **Store and forward**: Used for communication within an organization

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Features of SMTP

- Mail forwarding
- Mail gatewaying
- Mail relaying
- Address debugging
- Mailing list expansion

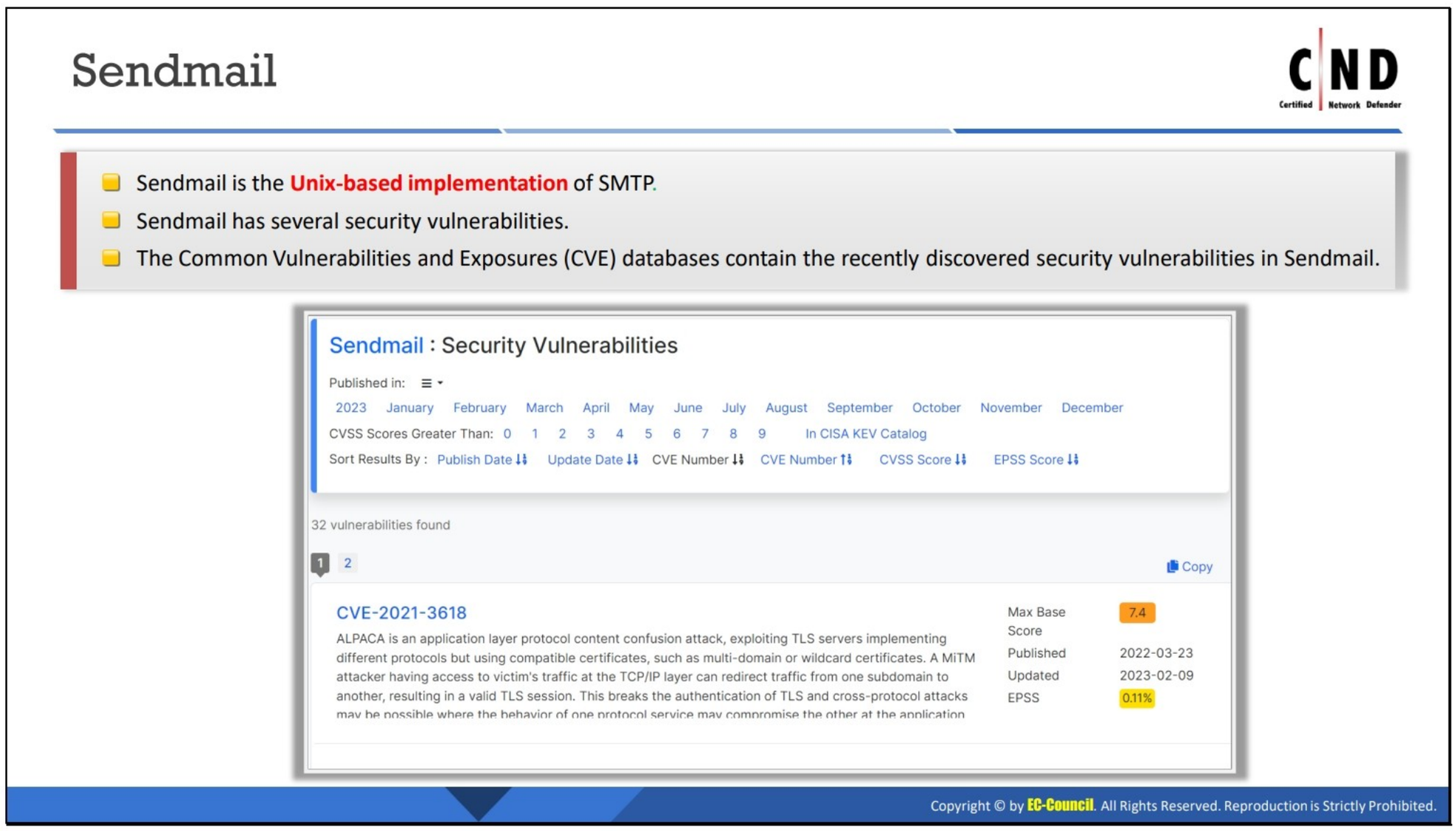
Advantages of SMTP

- SMTP provides the simplest form of communication through mail.
- It provides quick email delivery.
- It offers reliability in terms of outgoing email messages.
- It is easy to connect and can connect to any system having flexibility with existing applications.
- It is supported on many platforms.
- It has low implementation and administration costs.

Disadvantages of SMTP

- SMTP has poor security features.
- It is limited to 7-bit ASCII characters.
- It lacks the security features specified in X.400.
- Its simplicity limits its usefulness.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sendmail

Sendmail is a Unix-based implementation of SMTP. It is a general-purpose internetwork email routing facility that supports many kinds of mail transfer. Sendmail has several security vulnerabilities. The Common Vulnerabilities and Exposures (CVE) databases contain the recently discovered security vulnerabilities in Sendmail.

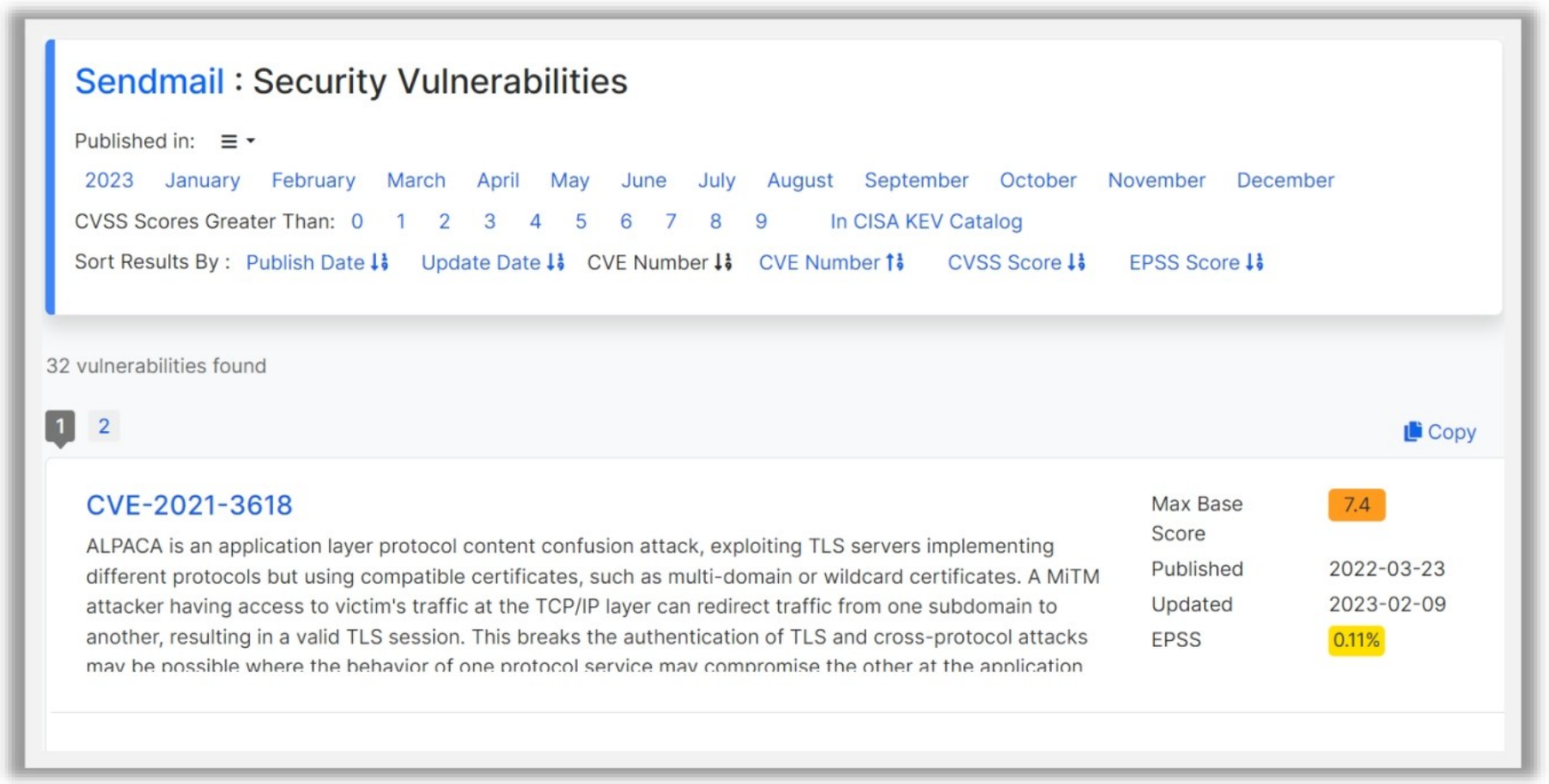
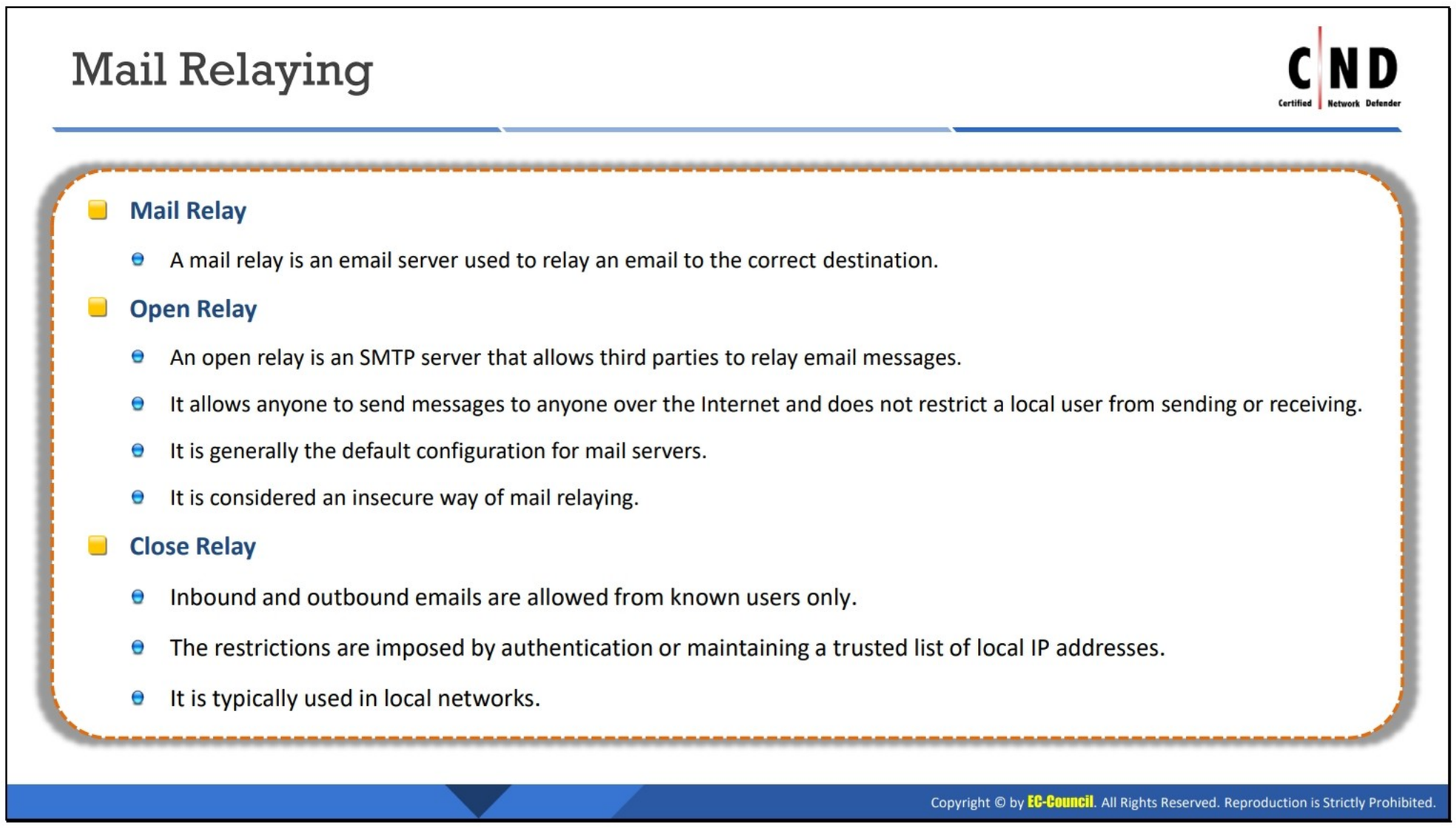


Figure A.50: Sendmail

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Mail Relaying

A mail relay is an email server used to relay an email to the correct destination. There are two types of mail relays: open relays and closed relays.

- **Open relay:**
  - An open relay is an SMTP server that allows third parties to relay emails.
  - It allows anyone to send messages to anyone over the Internet and does not restrict a local user from sending or receiving.
  - It is generally the default configuration for mail servers.
  - It is considered an insecure way of mail relaying.
- **Closed relay:**
  - Inbound and outbound emails are allowed from known users only.
  - The restrictions are imposed by authentication or maintaining a trusted list of local IP addresses.
  - It is typically used in local networks.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

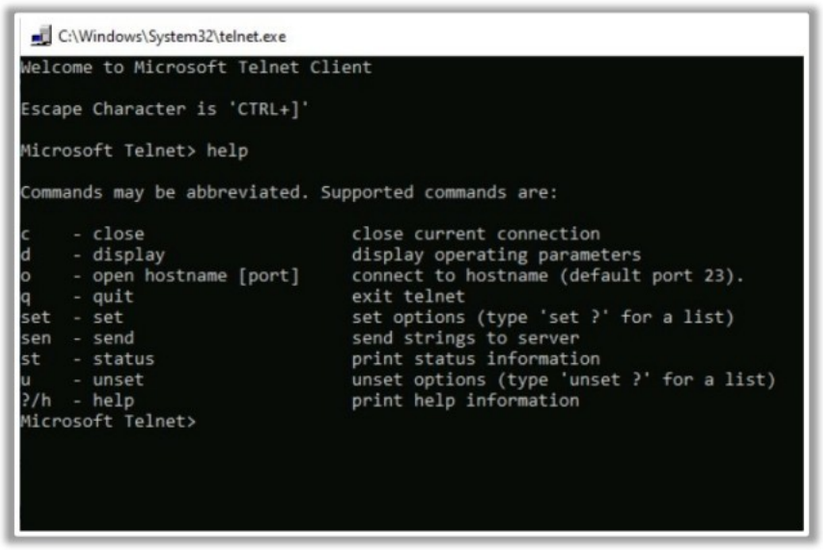
Telnet

- Telnet is a **TCP/IP protocol** used on LAN, which helps a user/administrator **access** computers remotely over a network.



Advantages

- Allows logging in to a remote computer and executing programs
- Allows remote control of web servers and enables communication with other servers on the network
- Fast and efficient even when the network and system loads are high



Weaknesses

- Vulnerable to DoS attacks
- Vulnerable to packet sniffing attacks
- Lacks security as it passes all data in cleartext
- Vulnerable to eavesdropping attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Telnet (Cont'd)

Cisco Reverse Telnet

- In reverse telnet, instead of providing a command shell to the host devices, the server side of the connection **reads** and **writes data** to a computer terminal line.
- Generally, it is implemented on embedded devices that have an Ethernet network interface and serial ports.
- The use of reverse telnet is not limited to modem connections or other asynchronous devices; reverse telnet can also be used for connecting to the console part of a router, switch, etc.
- To connect using reverse telnet, one should know the IP address of the terminal server hardware interfaces.

Weaknesses

- A remote attacker can send an extremely large number of packets to reverse telnet, causing a DoS attack.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Telnet

Telnet is a TCP/IP protocol used on LAN, which helps a user/administrator to access computers remotely over a network.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

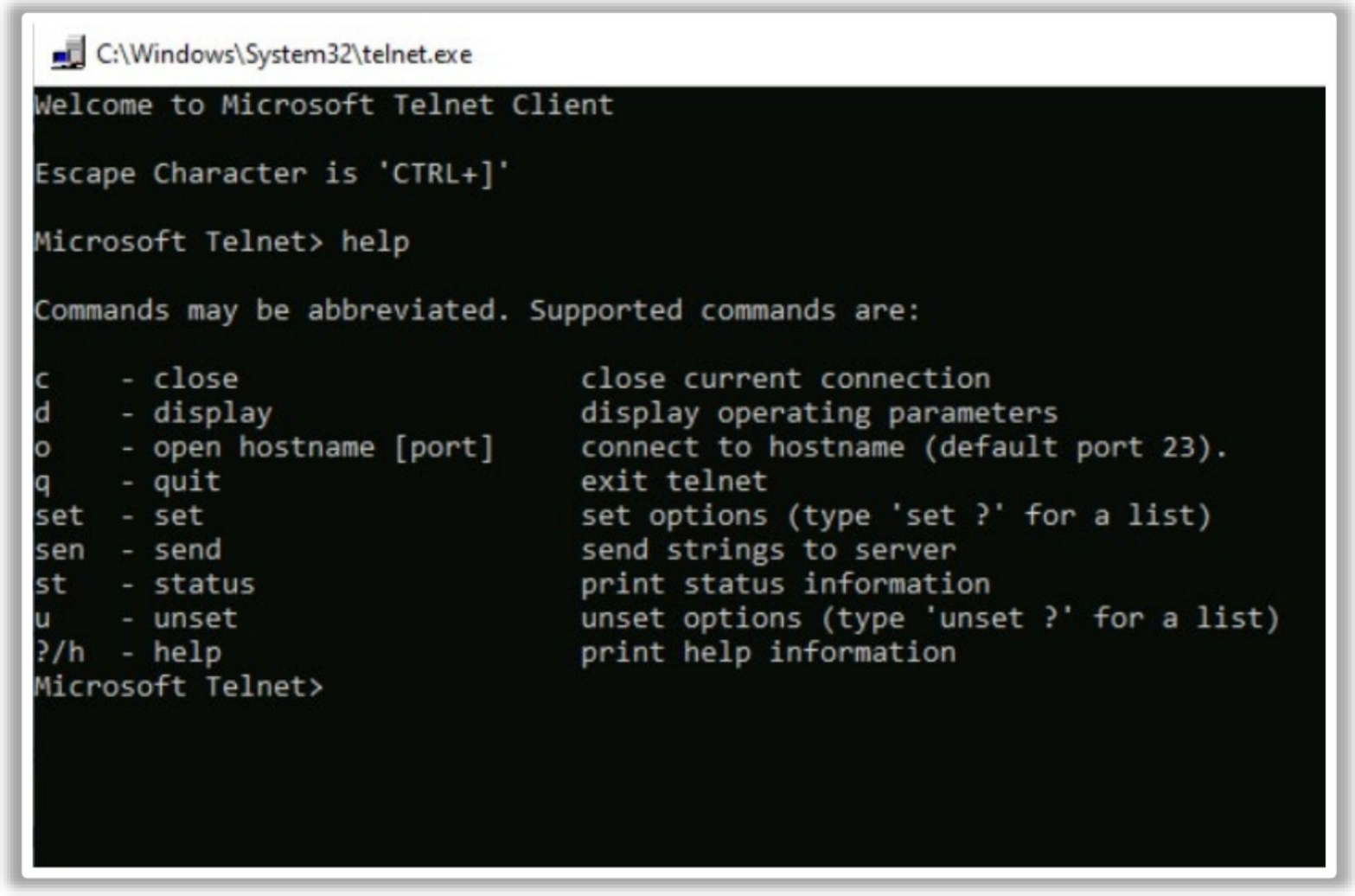


Figure A.51: Telnet

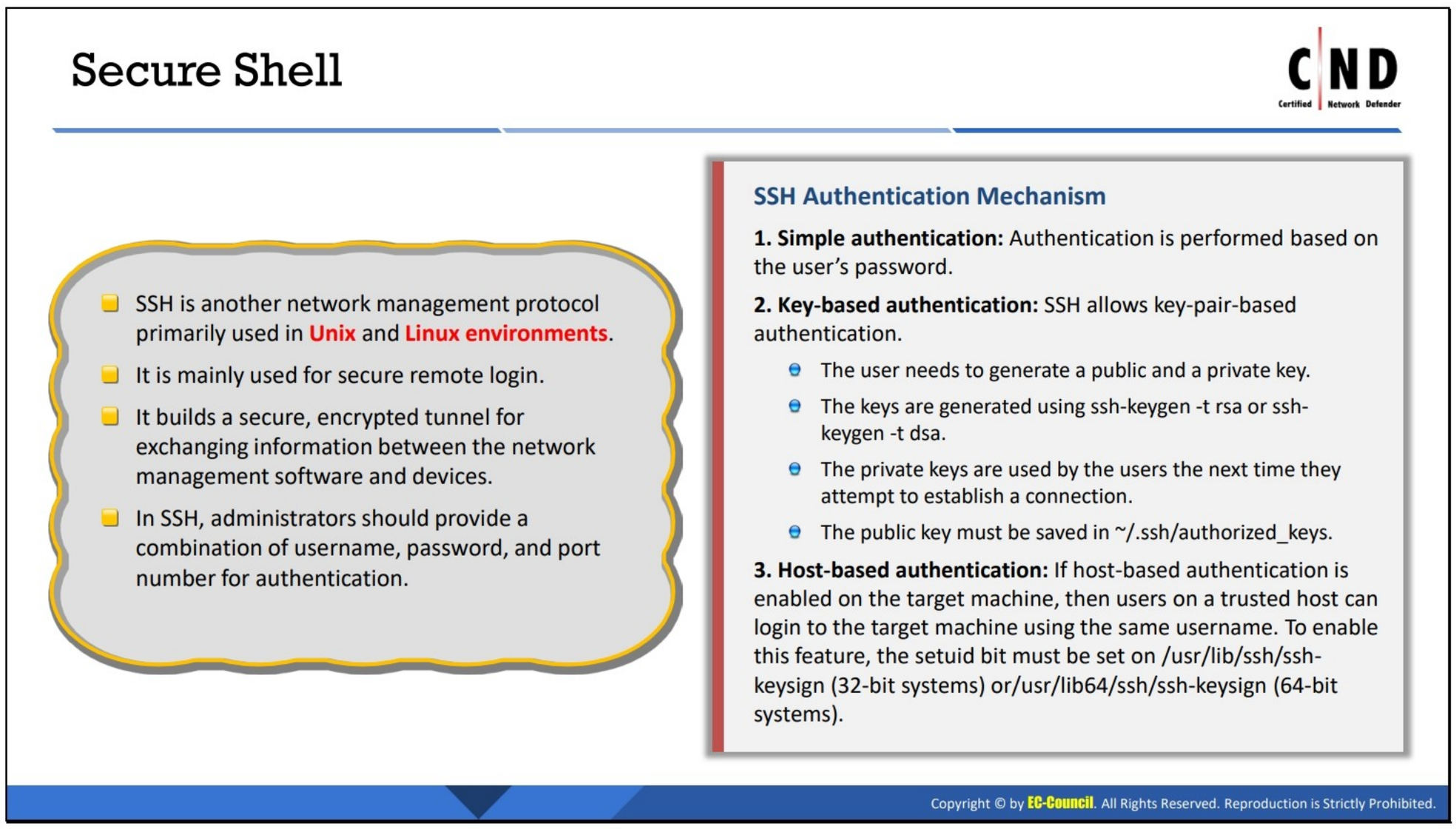
- **Advantages**
  - Allows logging in to a remote computer and executing programs.
  - Allows remote control of web servers and enables communication with other servers on the network
  - Fast and efficient even when the network and system loads are high
- **Weaknesses**
  - Vulnerable to DoS attacks
  - Vulnerable to packet sniffing attacks
  - Lacks security as it passes all data in cleartext
  - Vulnerable to eavesdropping attacks

Cisco Reverse Telnet

In reverse telnet, instead of providing a command shell to the host devices, the server side of the connection reads and writes data to a computer terminal line. Generally, it is implemented on embedded devices that have an Ethernet network interface and serial ports. The use of reverse telnet is not limited to modem connections or other asynchronous devices; reverse telnet can also be used for connecting to the console part of a router, switch, etc. To connect using reverse telnet, one should know the IP address of the terminal server hardware interfaces.

- **Weaknesses**
  - A remote attacker can send an extremely large number of packets to reverse telnet, causing a DoS attack.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Secure Shell

SSH is another network management protocol primarily used in Unix and Linux environments. It is mainly used for secure remote login. This protocol is equipped with strong authentication and encryption mechanisms to secure communications. This protocol was developed to overcome the insecure authentication (Telnet) and unencrypted transmission (FTP) of information. It builds a secure, encrypted tunnel for exchanging information between the network management software and devices. In SSH, administrators must provide a combination of username, password, and port number for authentication.

The following are some common features of SSH:

- Securely login to the remote host
- Securely send and receive files
- Execute commands on a remote host through a secure tunnel
- Key-based authentication
- Access control

SSH Functionality

The SSH protocol establishes a remote connection with a system by using a client–server connection model. In this model, the SSH client initially attempts to connect to the SSH server by identifying the server using its public key. When the connection is established between the SSH client and SSH server, the protocol implements a symmetric encryption and hashing algorithm for the communication to avoid unauthorized access and insecure connection. Figure A.52 illustrates this client–server communication.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

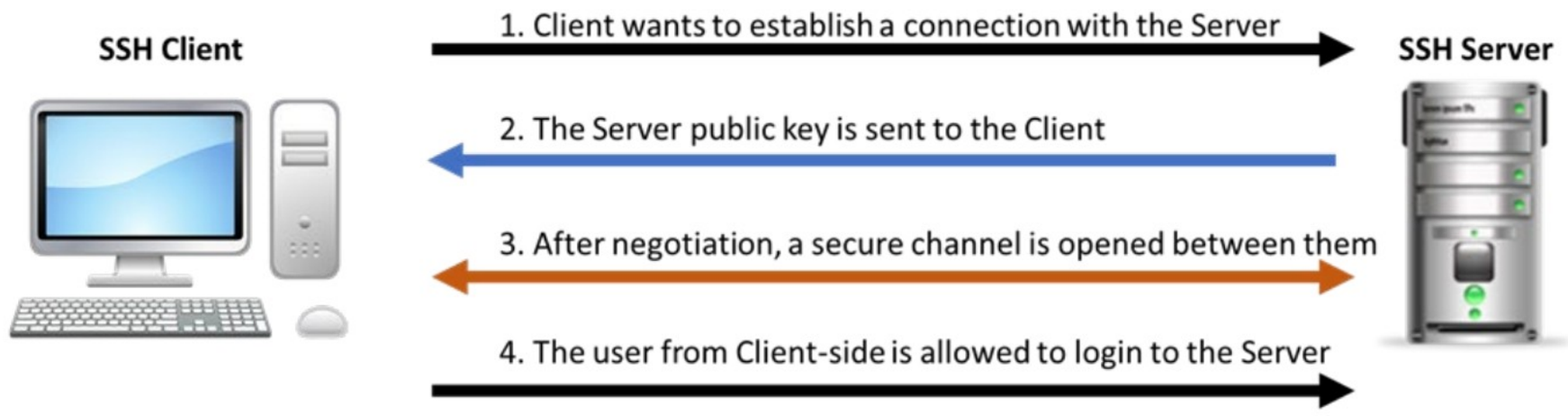


Figure A.52: SSH Functionality

SSH Authentication Mechanism

- **Simple authentication**: Authentication is performed based on the user's password.
- **Key-based authentication**: SSH allows key-pair-based authentication.
  - The user needs to generate a public and a private key.
  - The keys are generated using **`ssh-keygen -t rsa`** or **`ssh-keygen -t dsa`**.
  - The private keys are used by the users the next time they attempt to establish a connection.
  - The public key must be saved in **`~/.ssh/authorized_keys`**.
- **Host-based authentication**: If host-based authentication is enabled on the target machine, then users on a trusted host can login to the target machine using the same username. To enable this feature, the setuid bit must be set on **`/usr/lib/ssh/ssh-keysign`** (32-bit systems) or **`/usr/lib64/ssh/ssh-keysign`** (64-bit systems).

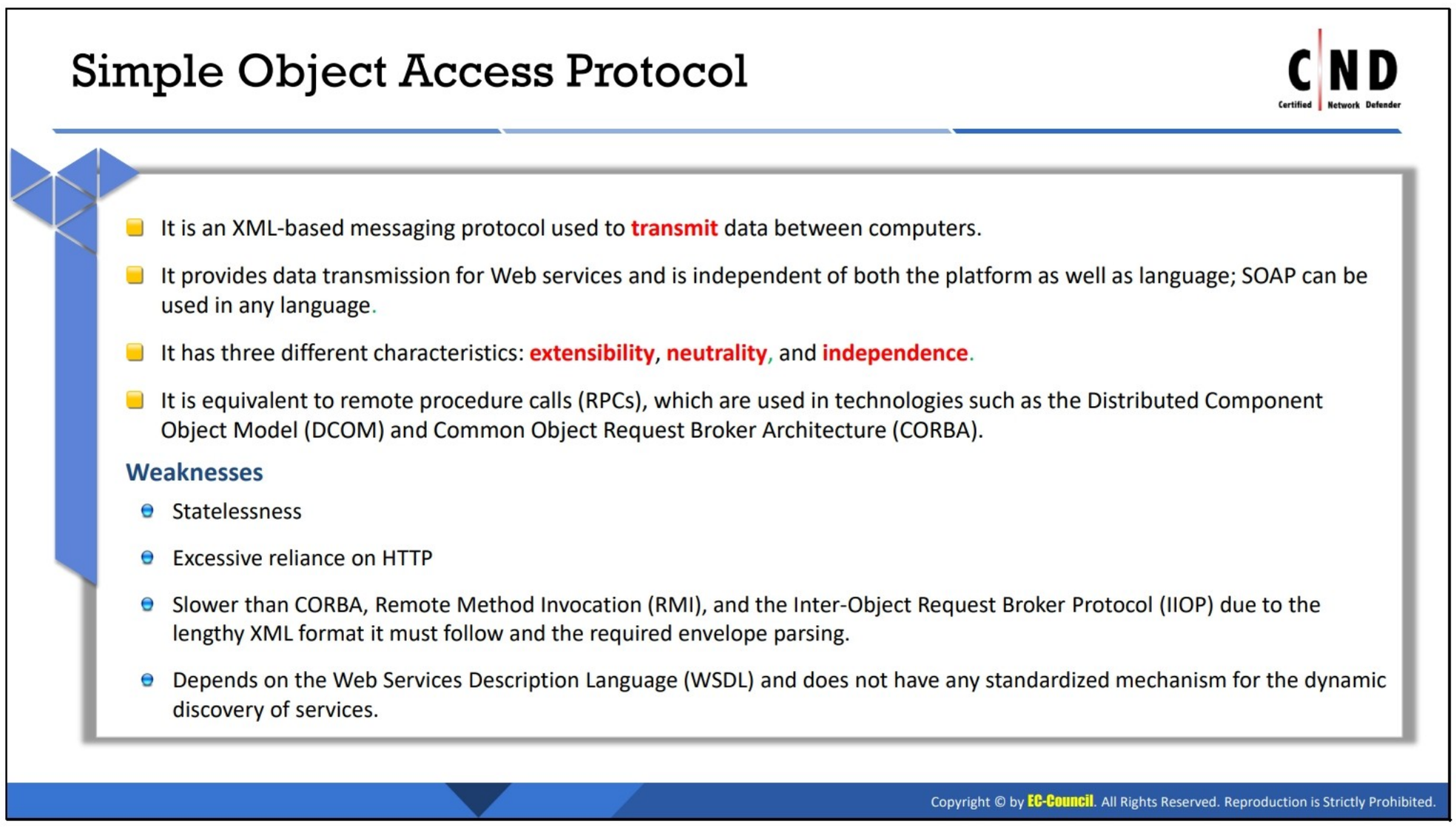
Weaknesses of SSH

- It is vulnerable to MITM attacks.
- It lacks confidentiality, integrity, and authenticity in access-control files.

Recommendation for Securing SSH

- A strong password and username should be used.
- Root logins need to be disabled.
- User logins should be limited.
- Protocol 1 should be disabled.
- Nonstandard ports should be used.
- Authentication must be performed using public or private keys.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Simple Object Access Protocol

Many OSes such as Windows, Linux, and Mac have their own functionalities, implementations, and user interfaces. Each OS runs different applications and is developed in a different environment. An application running on a Linux machine can communicate with another application in the same Linux machine or a different Linux machine. However, an application running on a Linux machine needs a medium to communicate with another application running in an OS other than Linux and its flavors. This medium is called the Simple Object Access Protocol (SOAP), which allows heterogeneous applications to communicate with each other using HTTP and the Extensible Markup Language (XML). This kind of communication between applications is necessary for certain tasks including online transactions such as bank payments.

Some applications might be developed using .NET, while others may be developed using Java. An application developed using .NET cannot communicate with one developed using Java. To overcome this hurdle, SOAP provides some specifications to be followed to enable an application in one machine to call an application in another machine by specifying encoding in HTTP headers and XML files.

As XML can be understood by most programming languages such as Java, .NET, and PHP, it is very useful in establishing co-ordination between applications. Although XML is used as a medium of communication between applications developed using various programming languages, XML is slightly tricky and requires some specifications such as the method of calling an application from another and of exchanging information between two applications, which are handled by SOAP.

SOAP is an XML-based messaging protocol used to transmit data between computers. It provides data transmission for web services and is independent of both the platform as well as language; SOAP can be used in any language. It has three different characteristics: extensibility, neutrality, and independence. It is equivalent to remote procedure calls (RPCs), which are used in

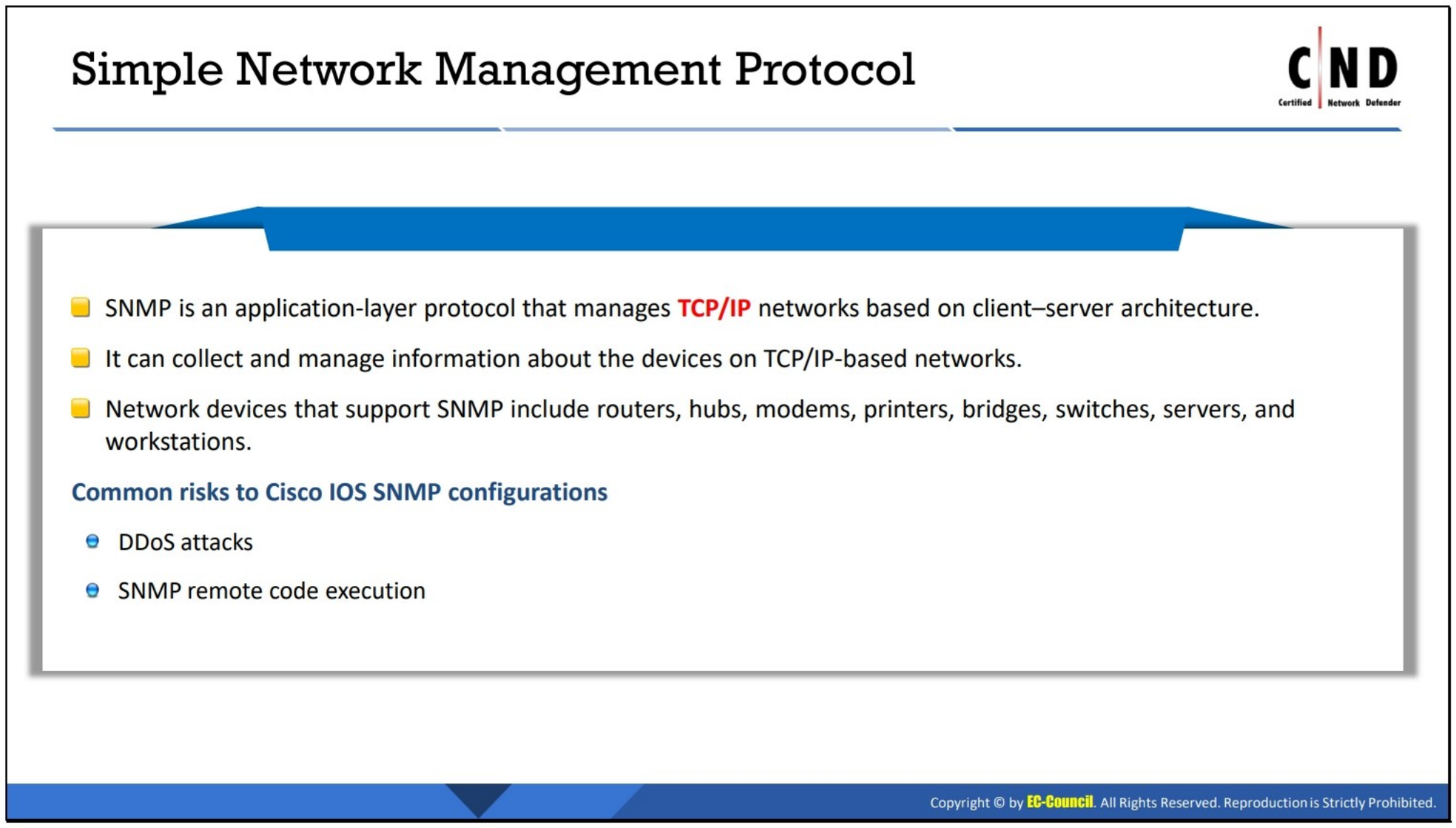
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

technologies such as the Distributed Component Object Model (DCOM) and Common Object Request Broker Architecture (CORBA).

Weaknesses

- Statelessness
- Excessive reliance on HTTP
- Slower than CORBA, Remote Method Invocation (RMI), and the Inter-Object Request Broker Protocol (IIOP) due to the lengthy XML format it must follow and the required envelope parsing
- Depends on the Web Services Description Language (WSDL) and does not have any standardized mechanism for the dynamic discovery of services

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Simple Network Management Protocol

As there may be many network devices that differ in properties in the same network, a common communication medium is required for exchanging information. To meet this requirement, the Simple Network Management Protocol (SNMP) was developed. SNMP is an application-layer protocol that manages TCP/IP networks based on the client–server architecture. It can collect and manage information about the devices in TCP/IP networks. SNMP supports all types of network devices such as routers, switches, printers, and Internet of things (IoT) devices. This protocol is particularly useful in managing and monitoring large networks that contain hundreds of nodes. By using this protocol, the management of nodes can be centralized to reduce the burden on network defenders.

Components of SNMP

SNMP has the following four components.

- **SNMP agent**: This component is used for gathering information about network devices and network errors and sending the information to the SNMP manager.
- **SNMP manager**: This component manages all the network devices by requesting information about the devices from the SNMP agents.
- **SNMP managed devices and resources**: The SNMP agents travel to these components and gather information.
- **Management information base (MIB)**: This component acts as a database that stores information in ".mib" format text files. It lists out all the objects of a network device by using an object identifier (OID).

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

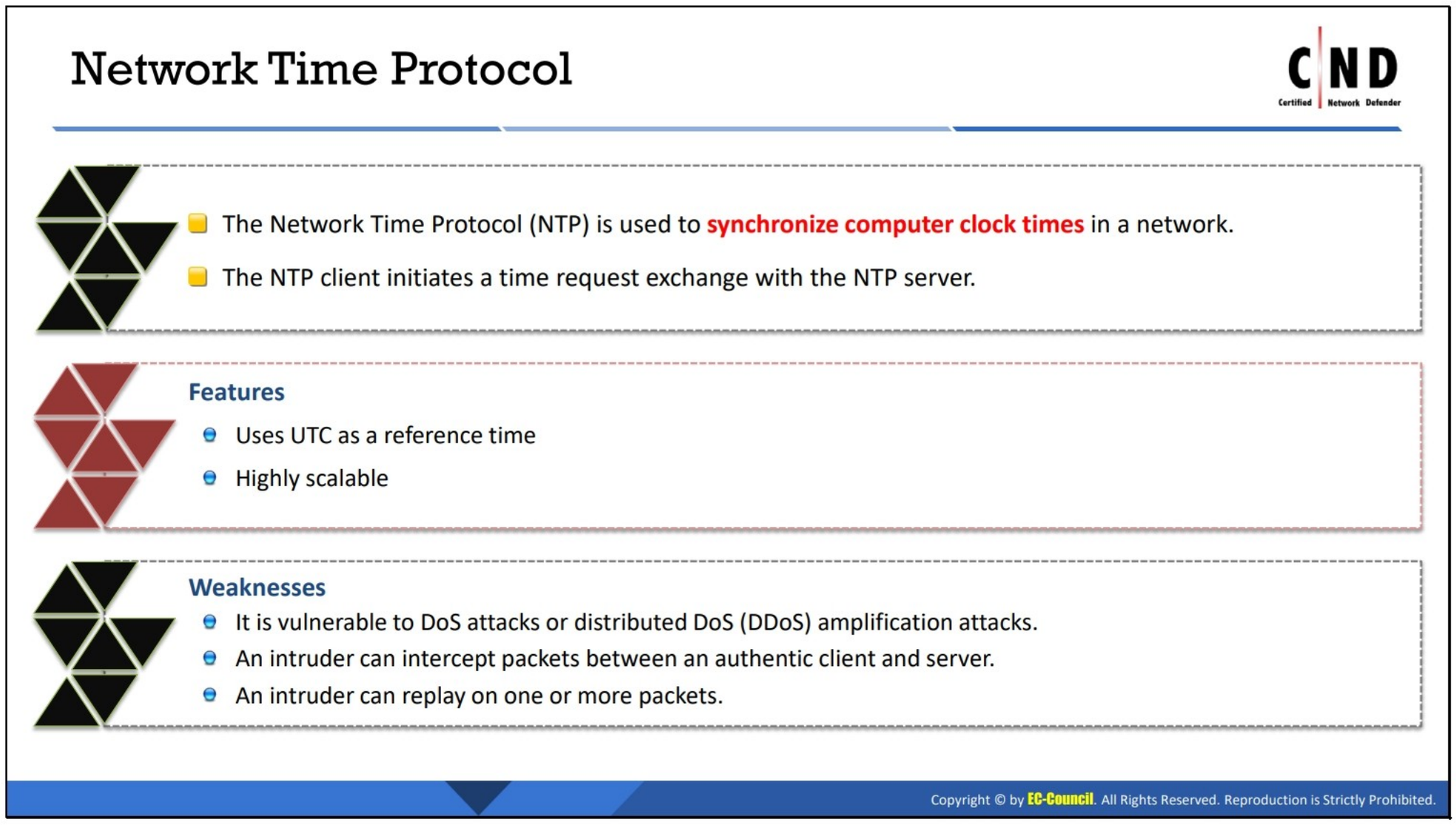
SNMP has the following threats and vulnerabilities:

- DoS attacks
- Masquerading
- Data manipulation
- Disclosure
- Traffic pattern analysis
- Network perimeter insecurity
- ICMP echo requests

The following are common risks to Cisco Internetwork Operating System (IOS) SNMP configurations:

- Distributed DoS (DDoS) attacks
- Remote code execution

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Time Protocol

The Network Time Protocol (NTP) is used to synchronize computer clock times in a network. The NTP client initiates a time request exchange with the NTP server. In a network, there might be many computers connected for exchanging data with other computers. In large networks, some computers might be miles away from others. For such networks, the time zone of a computer may be different from that of other network devices such as computers, servers, and routers. For better communication and for managing this large network in terms of security and maintenance, the device times should be synchronized. The clock time synchronization of network devices is handled using the specifications provided by NTP, which synchronizes the clocks of network devices by using the Coordinated Universal Time (UTC).

Working of NTP

If a computer wishes to access the resources of another computer that is physically far away from it, their clocks should be synchronized to avoid link delay. Therefore, the first computer (NTP client) sends a time-exchange request to the second computer (NTP server); based on the response from the server, the NTP client adjusts its clock to match that of the server. This clock adjustment cannot be performed with just a single request and response; in a period of five to ten minutes, there should be at least six time exchanges for adjustment. After the completion of the synchronization, the client must perform follow-up synchronizations every ten minutes with time-exchange requests.

NTP has the following features:

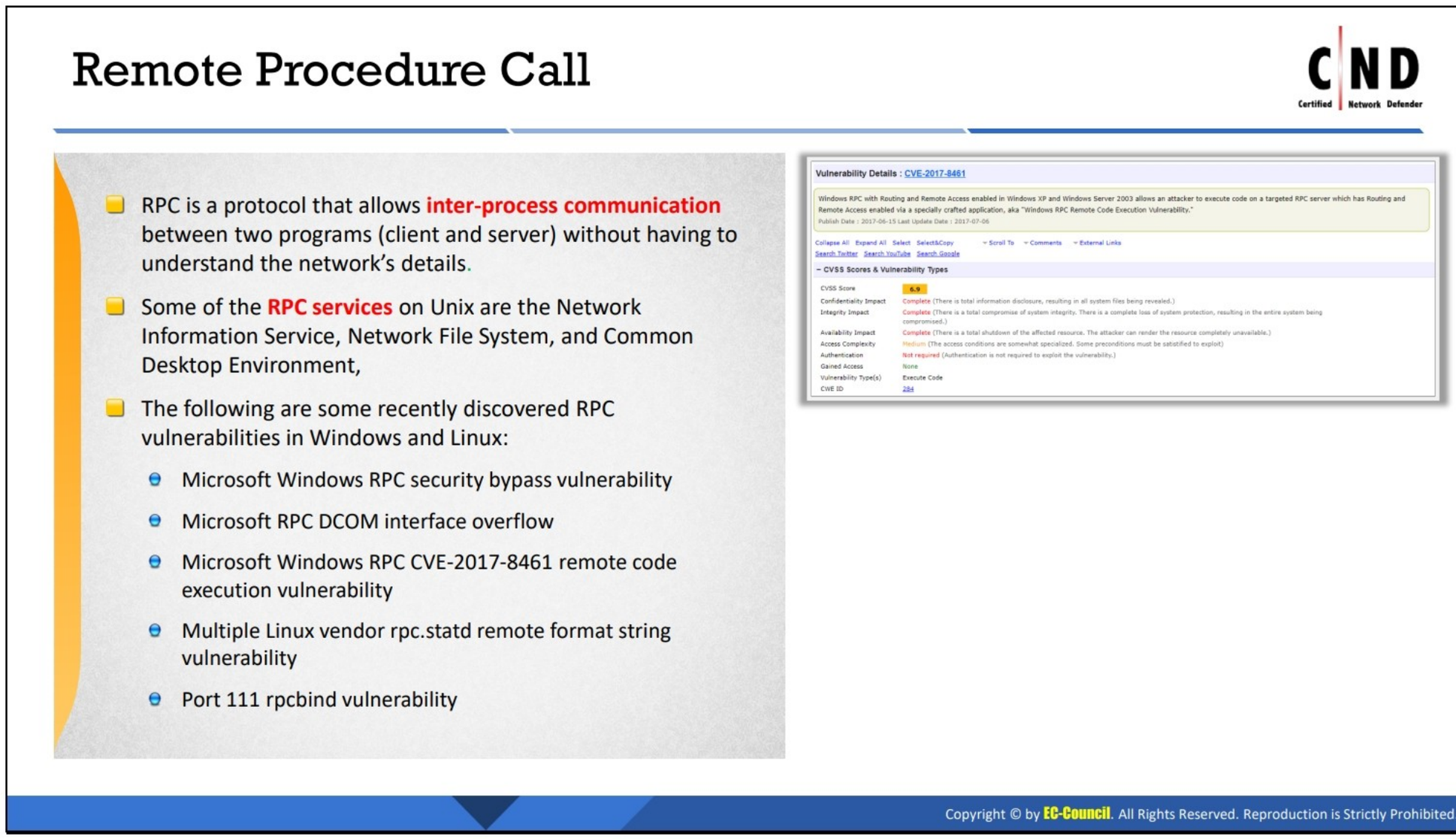
- Uses UTC as the reference time
- Highly scalable

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

NTP also has some weaknesses. In particular, it is vulnerable to many security attacks, some of which are listed below:

- It is vulnerable to DoS attacks or DDoS amplification attacks.
- An intruder can intercept packets between an authentic client and server.
- An intruder can replay one or more packets.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Remote Procedure Call

RPC is used for exchanging services between applications that reside in different computers. This works using the client–server model of communication, where the requesting computer is treated as a client and the responding computer is treated as a server.

After sending a request (call) to access the services, the client (calling program) is suspended for a while until the call reaches the destination program, the request is executed, and the result (response) is sent back to the client. Before proceeding with the communication, the client and server must authenticate themselves.

RPC is a protocol that allows inter-process communication between two programs (client and server) without having to understand the network's details. Some RPC services on Unix are the Network Information Service, Network File System, and Common Desktop Environment.

The following are some recently discovered RPC vulnerabilities in Windows and Linux:

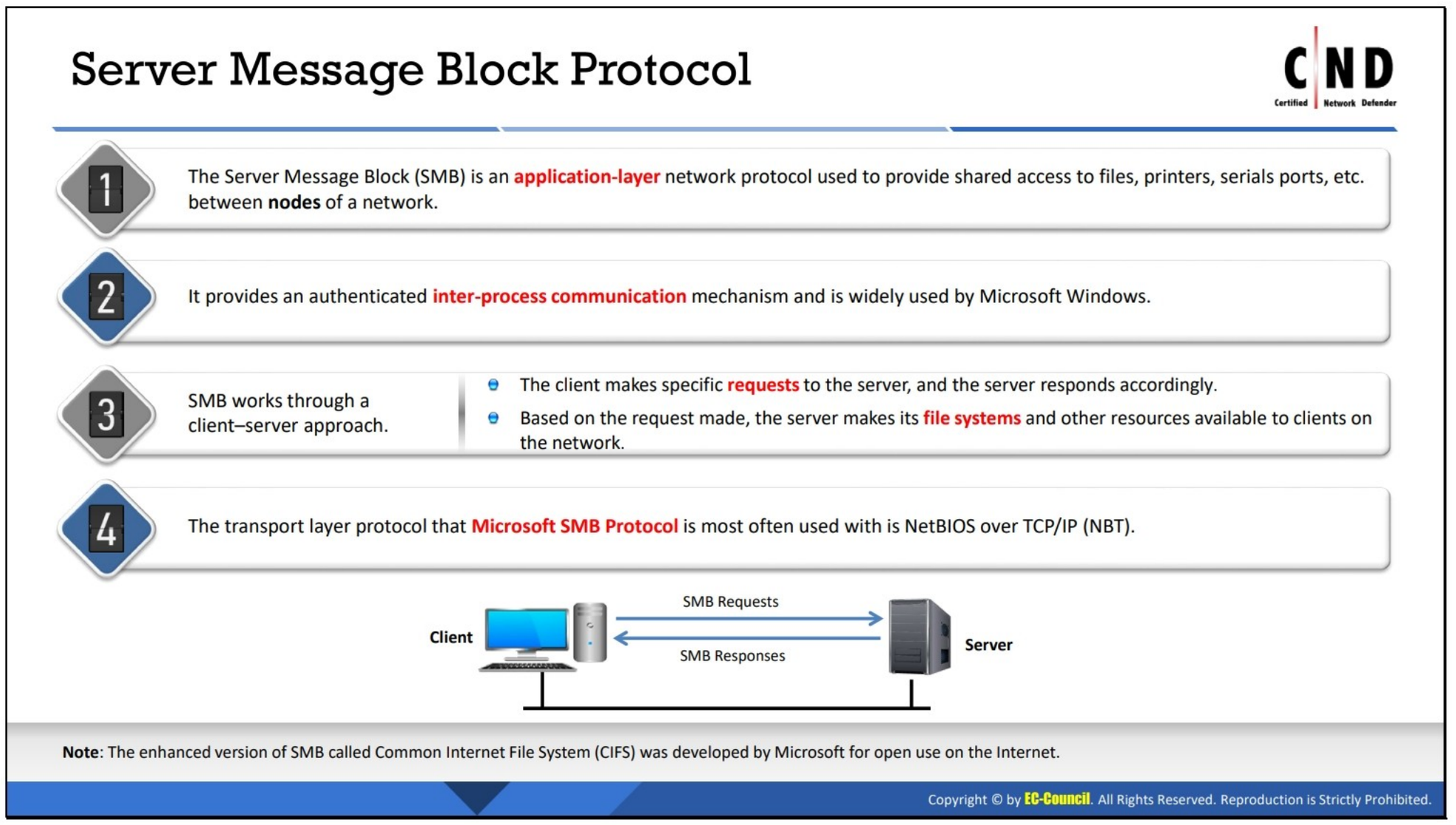
- Microsoft Windows RPC security bypass vulnerability
- Microsoft RPC DCOM interface overflow
- Microsoft Windows RPC CVE-2017-8461 remote code execution vulnerability
- Multiple Linux vendor **`rpc.statd`** remote format string vulnerability
- Port 111 **`rpcbind`** vulnerability

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure A.53: Details on a “Remote Procedure Call” Vulnerability

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Server Message Block Protocol

The Server Message Block (SMB) is an application-layer network protocol used to provide shared access to files, printers, serials ports, etc. between nodes of a network. It provides an authenticated inter-process communication mechanism and is widely used by Microsoft Windows. SMB works through a client–server approach. The client makes specific requests to the server, and the server responds accordingly. Based on the request made, server makes its file systems and other resources available to clients on the network. The transport layer protocol that Microsoft SMB Protocol is most often used with is NetBIOS over TCP/IP (NBT).

Note: The enhanced version of SMB called Common Internet File System (CIFS) was developed by Microsoft for open use on the Internet.

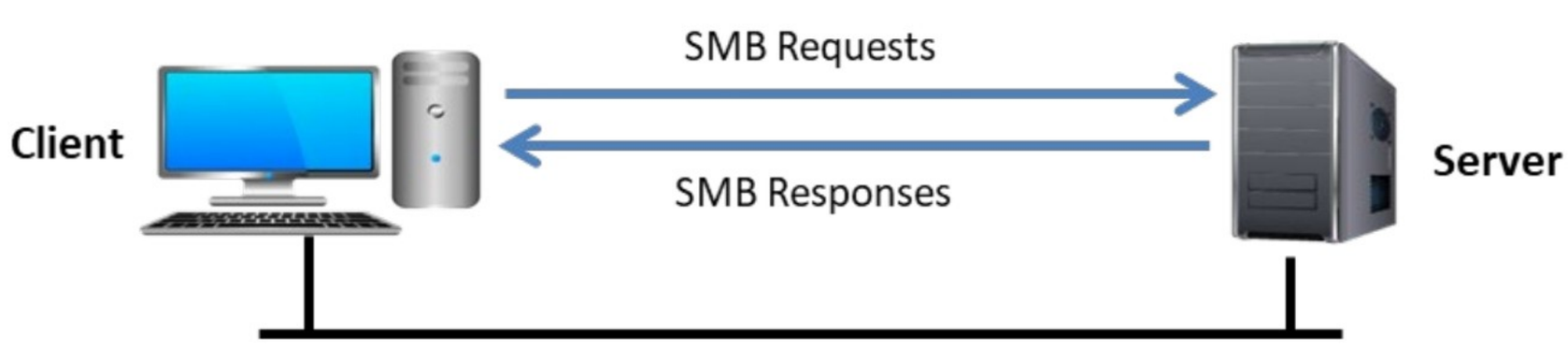
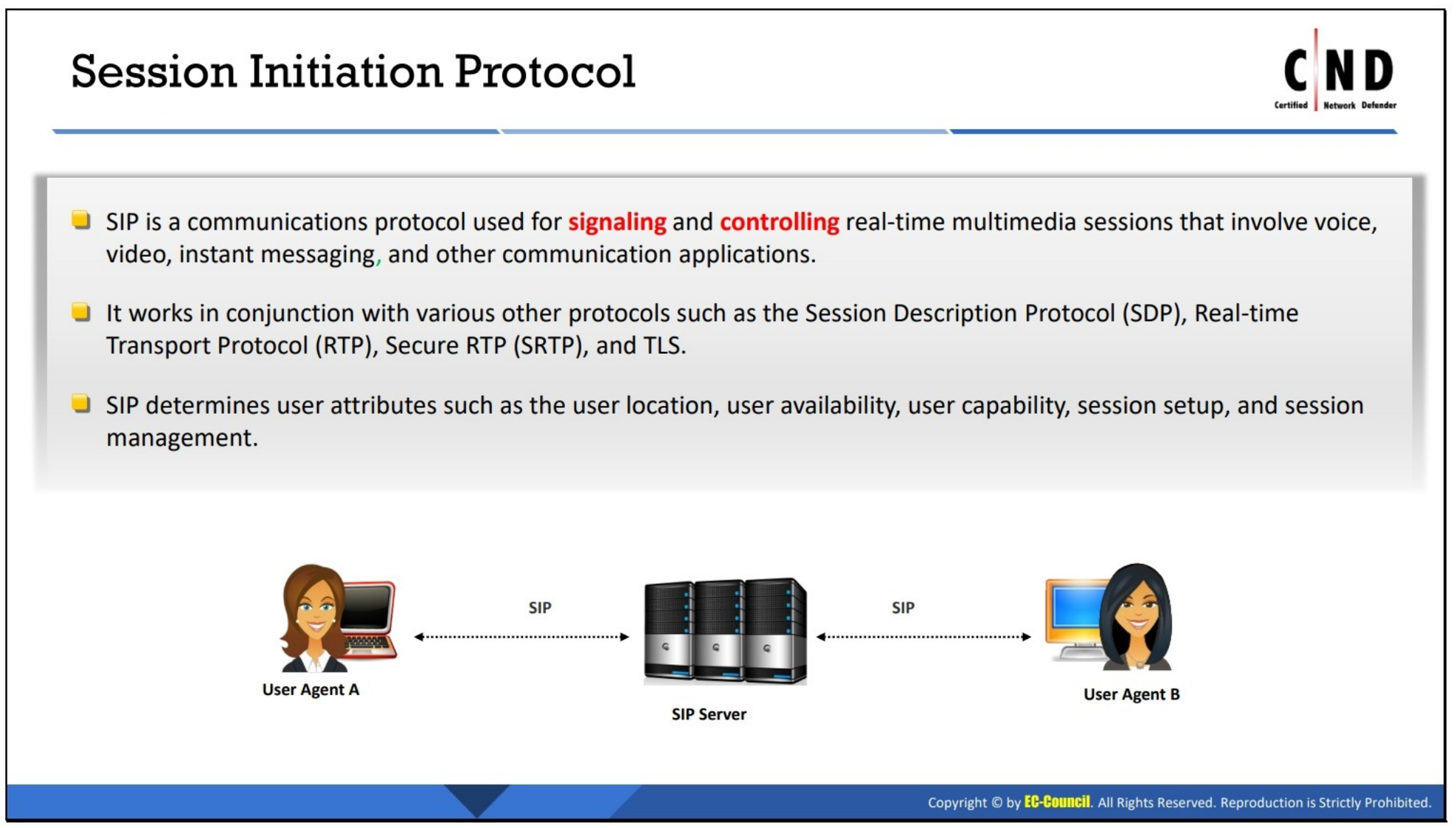


Figure A.54: "Server Message Block (SMB)" Requests and Responses

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



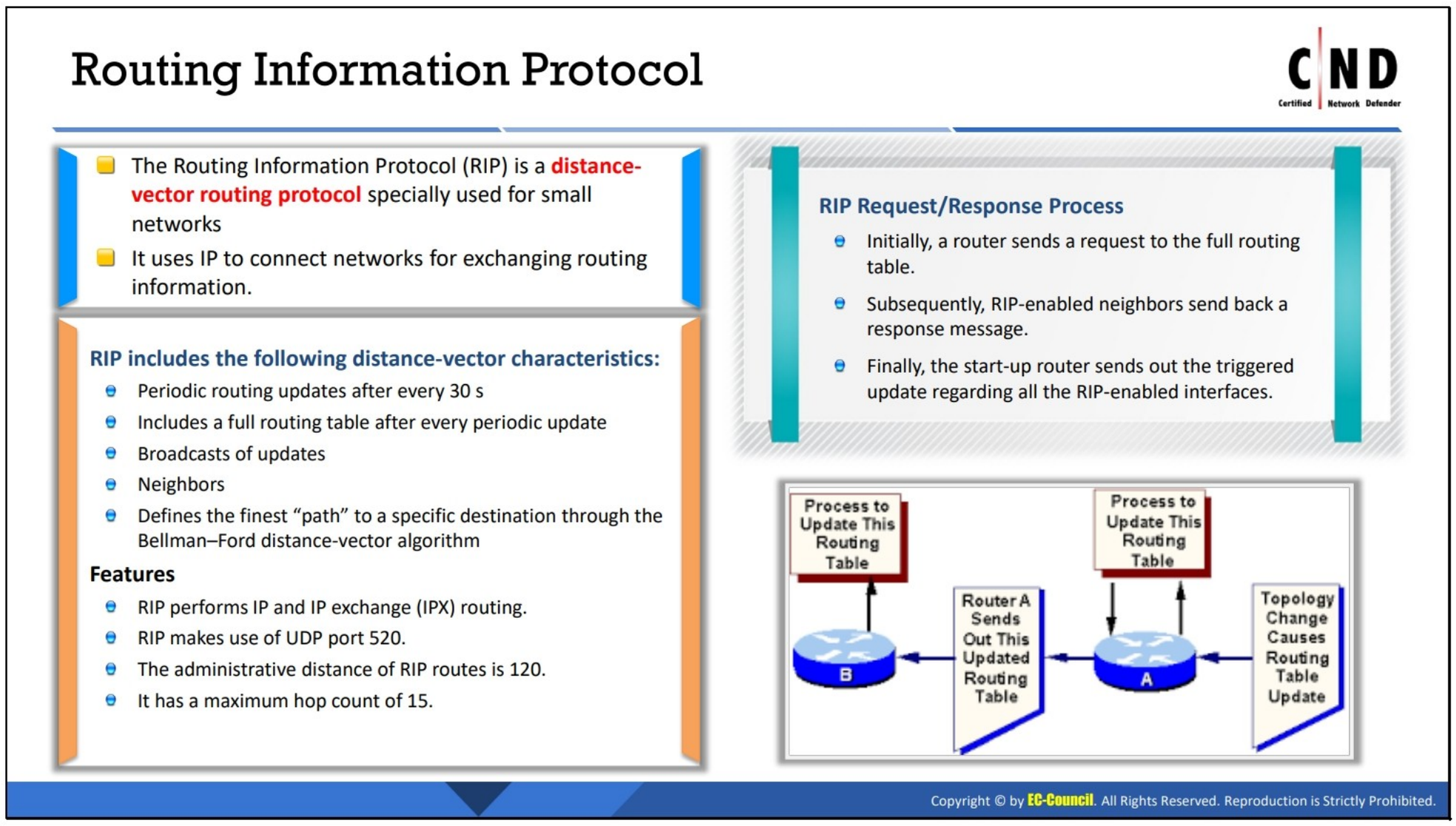
Session Initiation Protocol

The Session Initiation Protocol (SIP) is a communications protocol used for signaling and controlling real-time multimedia sessions that involve voice, video, instant messaging, and other communication applications. It works in conjunction with various other protocols such as the Session Description Protocol (SDP), RTP, Secure RTP (SRTP), and TLS. SIP determines user attributes such as the user location, user availability, user capability, session setup, and session management.



Figure A.55: Working of the Session Initiation Protocol

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Routing Information Protocol(RIP)

RIP is a distance-vector routing protocol specially used for small networks. It uses IP to connect networks for exchanging routing information.

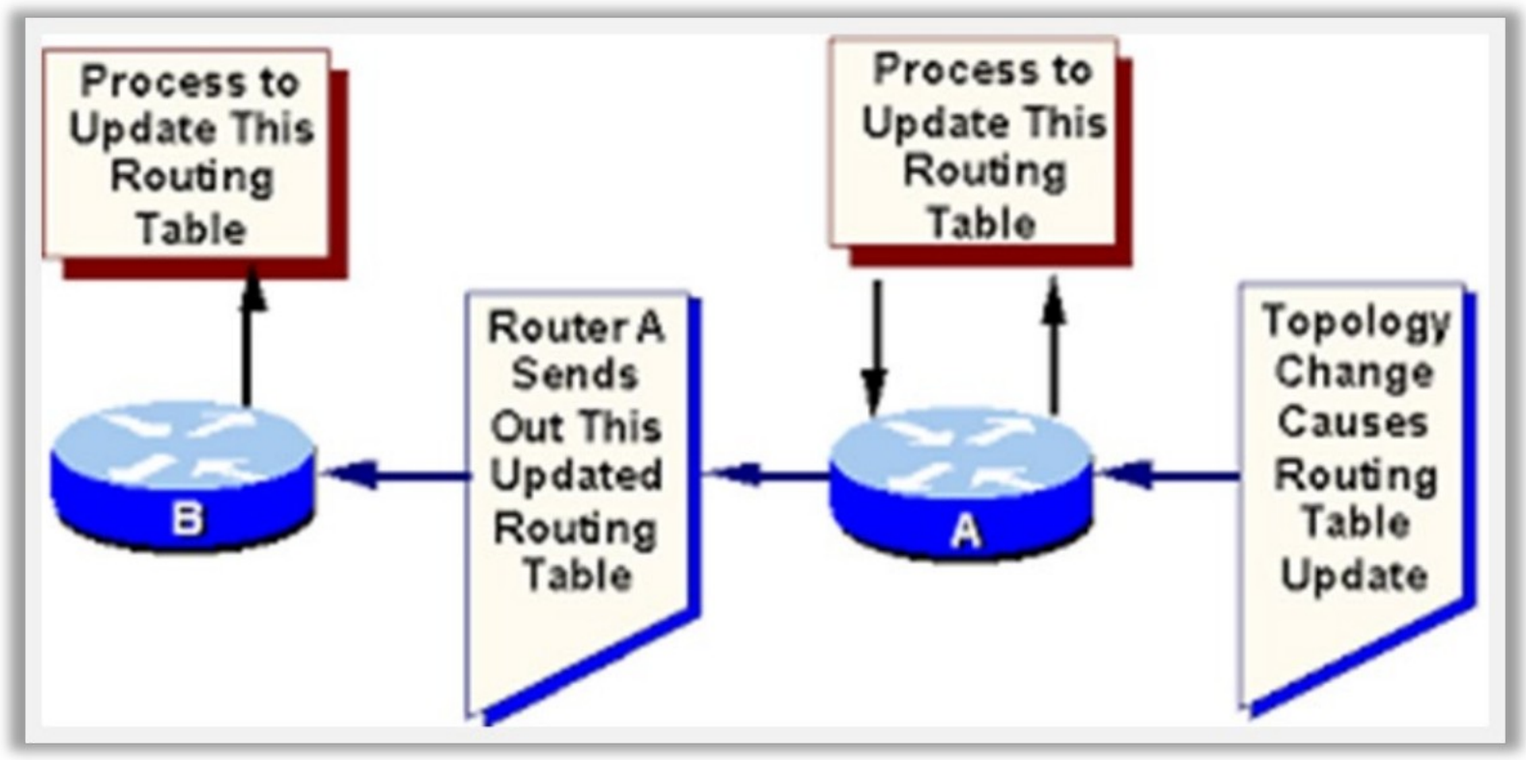


Figure A.56: Working of RIP

RIP includes the following distance-vector characteristics:

- Periodic routing updates after every 30 s
- Includes a full routing table after every periodic update
- Broadcasts of updates
- Neighbors

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Defines the finest "path" to a specific destination through the Bellman–Ford distance-vector algorithm

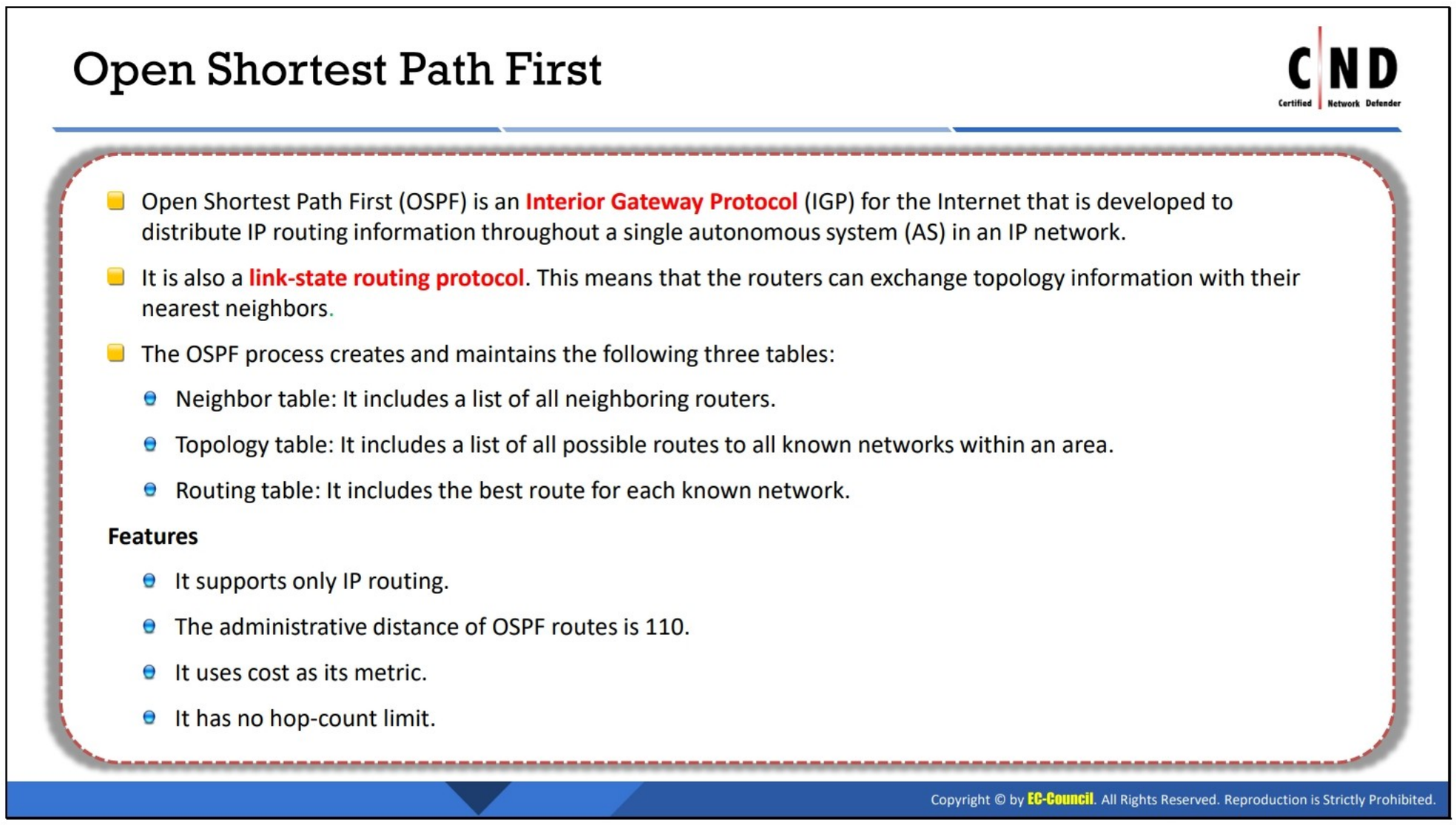
RIP Request/Response Process

- Initially, a router sends a request to the full routing table.
- Subsequently, RIP-enabled neighbors send back a response message.
- Finally, the start-up router sends out the triggered update regarding all the RIP-enabled interfaces.

Features

- RIP performs IP and IP exchange (IPX) routing.
- RIP makes use of UDP port 520.
- The administrative distance of RIP routes is 120.
- It has a maximum hop count of 15.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Open Shortest Path First

As discussed above, RIP is used for routing data packets in a network to send them to their destination system. It is used for routing packets irrespective of the distance to the destination. In contrast, the Open Shortest Path First (OSPF) protocol is used for finding the shortest path among all the available paths in a network. This protocol is a successor to RIP for packet routing. As in RIP, this protocol updates the routing table whenever a new shortest path is found and broadcasts the same to the other routers in the network that follow OSPF. However, only the updated part is sent in OSPF instead of the total routing information. The metrics used by the OSPF is the “cost” for calculating the shortest routing path.

OSPF is an Interior Gateway Protocol (IGP) for the Internet that is developed to distribute IP routing information throughout a single autonomous system (AS) in an IP network. It is also a link-state routing protocol. This means that the routers can exchange topology information with their nearest neighbors.

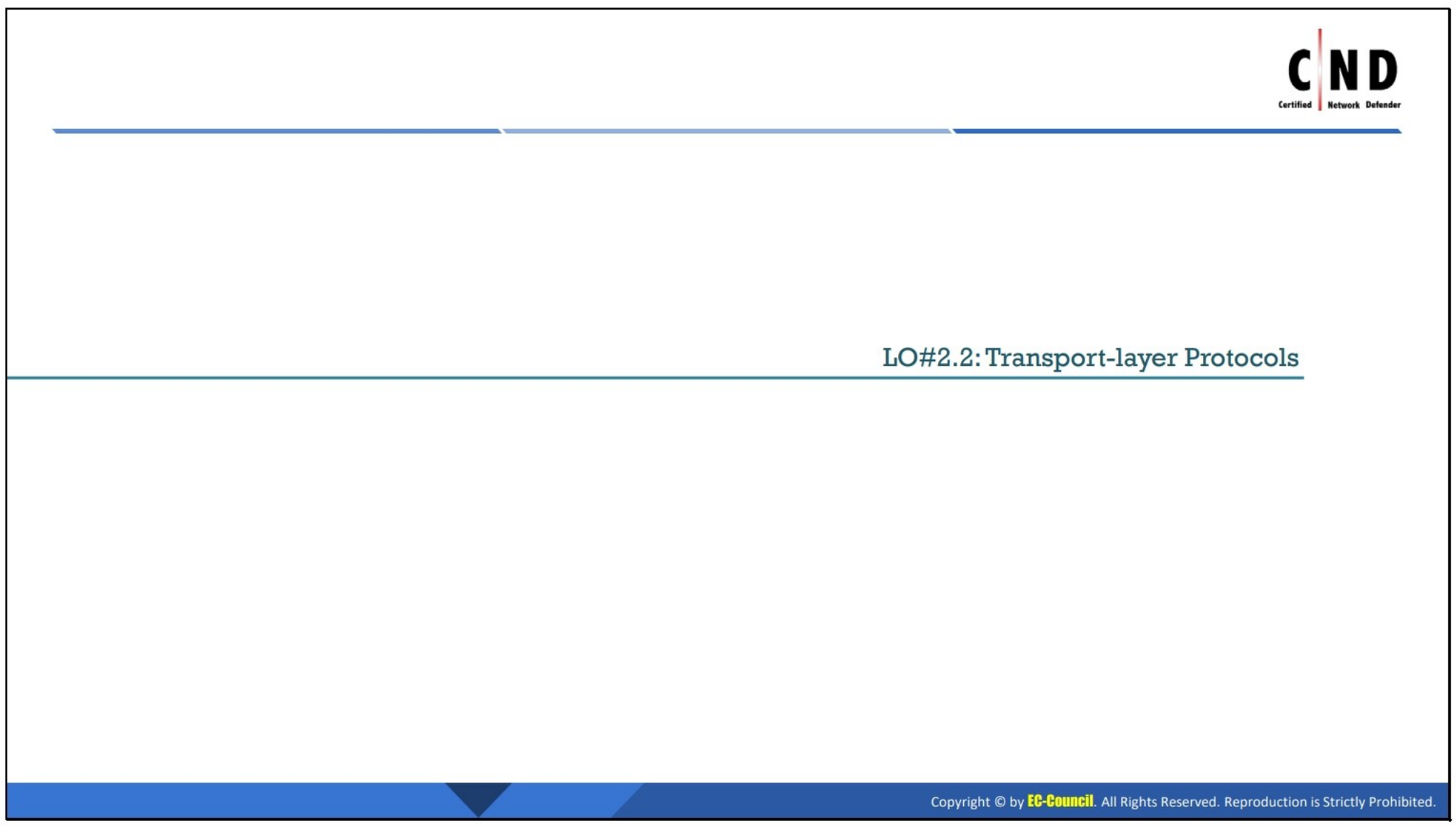
The OSPF process creates and maintains the following three tables.

- **Neighbor table**: It includes a list of all neighboring routers.
- **Topology table**: It includes a list of all possible routes to all known networks within an area.
- **Routing table**: It includes the best route for each known network.

Features

- It supports only IP routing.
- The administrative distance of OSPF routes is 110.
- It uses cost as its metric.
- It has no hop-count limit.

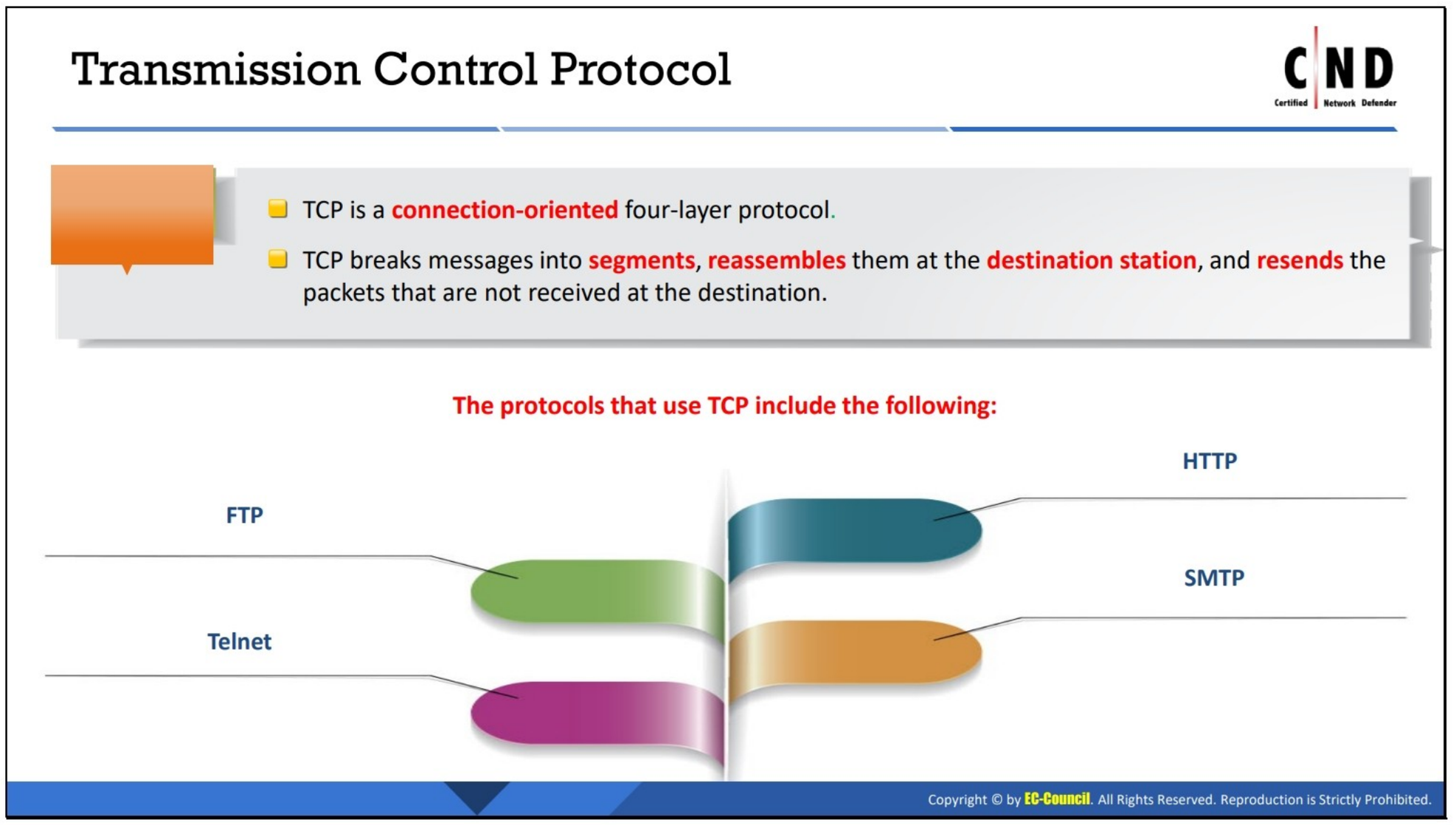
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#2.2: Transport-Layer Protocols

This section discusses the fundamentals of transport layer protocols such as TCP, UDP, SSL, and TLS.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Transmission Control Protocol (TCP)

TCP functions at layer 4 of the OSI model and assures reliable, error-free data transmission over networks. It is a connection-oriented protocol that provides full duplex simultaneous two-way transmission between devices. A checksum is provided to monitor the data transmission and request for lost or damaged data packets. The port numbers are very crucial in data transmission, and there are approximately 65535 TCP ports available.

TCP is a connection-oriented four-layer protocol. It breaks messages into segments, reassembles them at the destination station, and resends the packets that are not received at the destination.

The protocols that use TCP include the following:

- FTP
- Telnet
- HTTP
- SMTP

Three-way Handshake in TCP

The devices that wish to communicate through TCP follow a process called a three-way handshake, which signals that both the parties are ready for the communication.

The three stages are involved in the TCP handshake process are as follows.

- **Step 1**: The source device sends a TCP SYN packet to the destination host. It contains lower-layer protocol header information such as the initial sequence number and the maximum size; it does not contain any data.
- **Step 2**: The destination host responds with a TCP packet that contain SYN and ACK flags.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 3**: Finally, the source host again sends a TCP ACK to establish the TCP communication.

The TCP three-way handshake process is illustrated in Figure A.57.

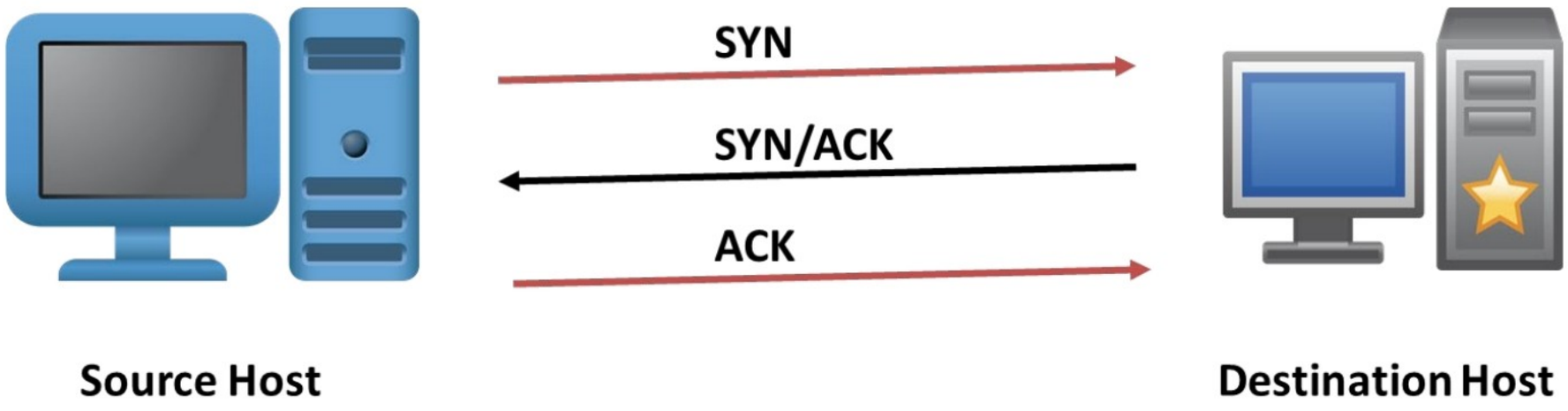


Figure A.57: TCP Three-Way Handshake

Characteristics of TCP

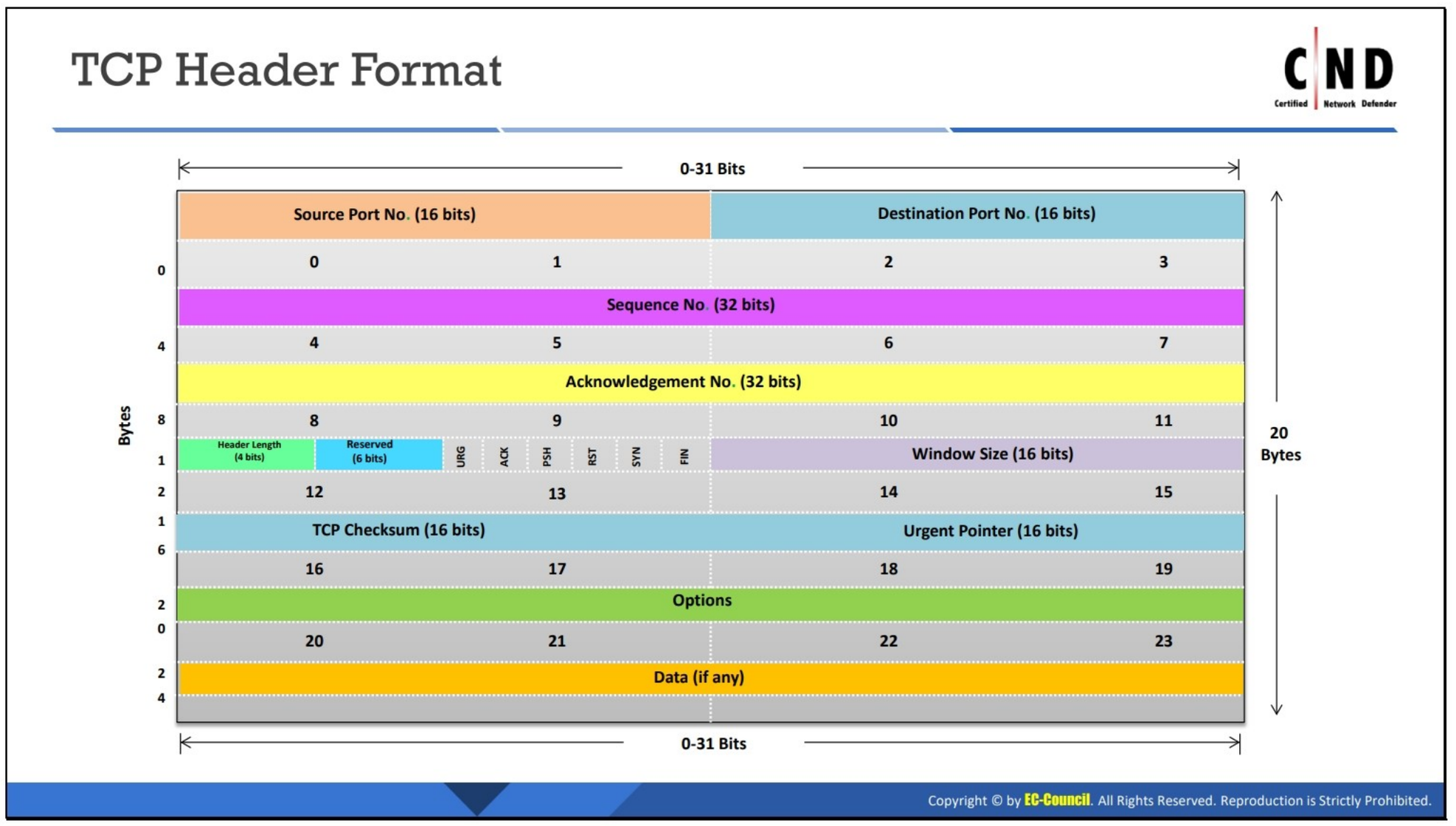
- Connection oriented
- Reliable data transmission
- Acknowledged
- Data management
- Bidirectional

Functionalities of TCP

TCP can perform the following functions.

- **Multiplexing**: Most applications prefer to transfer data using TCP, which ensures error-free and accurate data transfer. Therefore, various applications send various types of data to TCP, and these are multiplexed into a single data steam and sent to the destination.
- **Addressing**: TCP ports are used to identify the data that belong to a particular application.
- **Data flow and congestion management**: TCP controls the data flow between devices and ensures that the communication is congestion free.
- **Systematic connection procedure**: TCP defines a systematic method of connection establishment between two devices, connection management, and connection termination.
- **Data packaging and handling**: TCP collects all the data from applications and pack them into a message format and then sends the data to the destination. At the destination machine, TCP unpacks the messages and sends them to their respective destination applications.
- **Reliable and error free services**: TCP provides quality data transmission without any error or damage. However, the services are limited to technical errors and cannot address external errors created by attackers.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



TCP Header Format

Many functionalities that can be obtained through TCP. The TCP header fields are explained in detail below.

- **Source port**: The source device port that transmits the data
- **Destination port**: The destination device port that receives the data
- **Acknowledgement number**: A series of numbers assigned to the packets and are used to maintain the data sequence from devices
- **Flags**: Used to identify the type of the data; the six types of flags are URG, ACK, PSH, RST, SYN, and FIN
- **Window size**: The maximum size of the sequence that the destination can accept
- **Checksum**: Ensures that the data transmitted is error-free and there is no damage to the data
- **Urgent pointer**: Must be verified whenever an URG flag is set
- **Options**: Optional fields for additional information
- **Data**: Information about the data in the packet that are sent in the form of segments

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

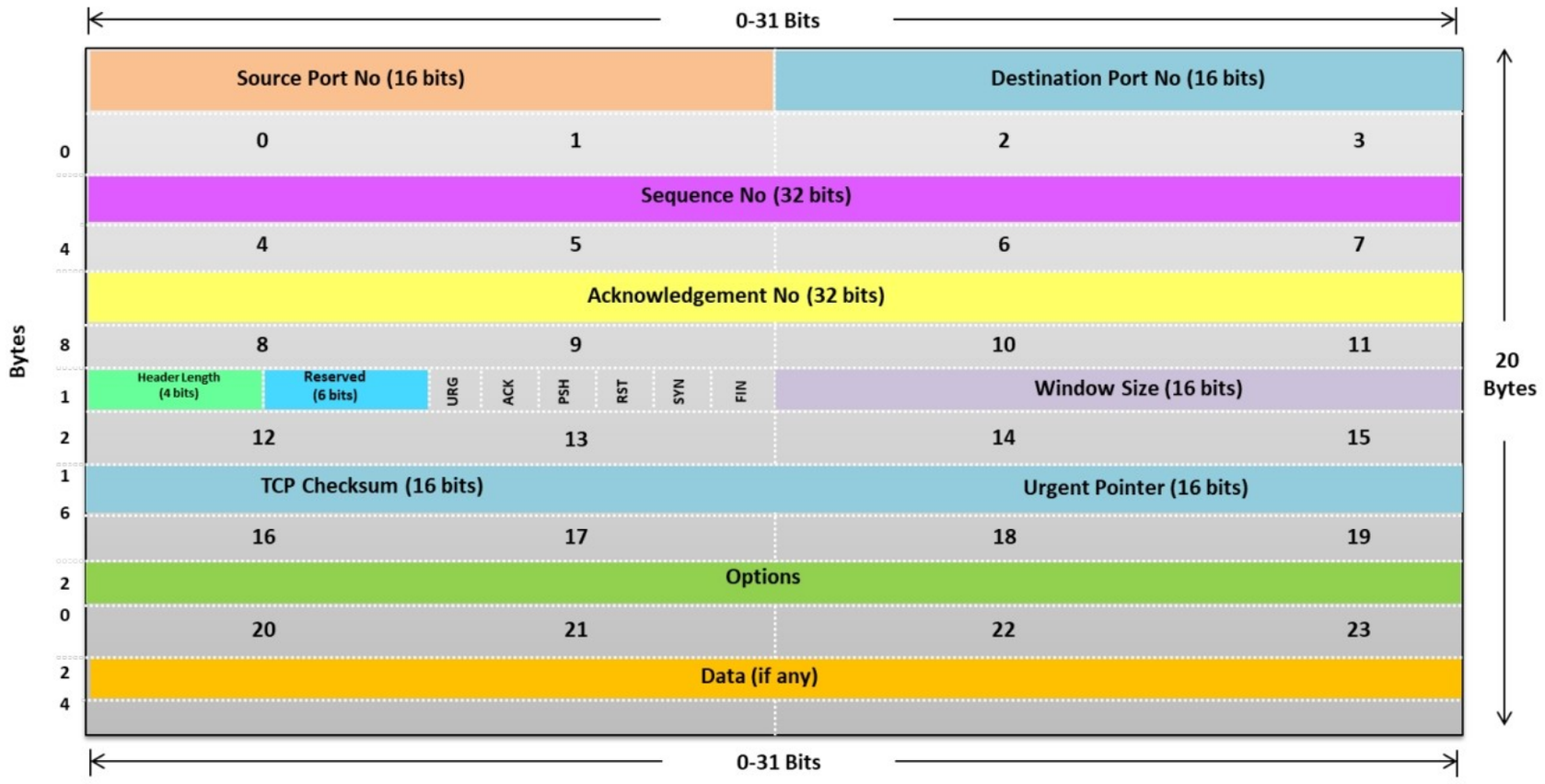
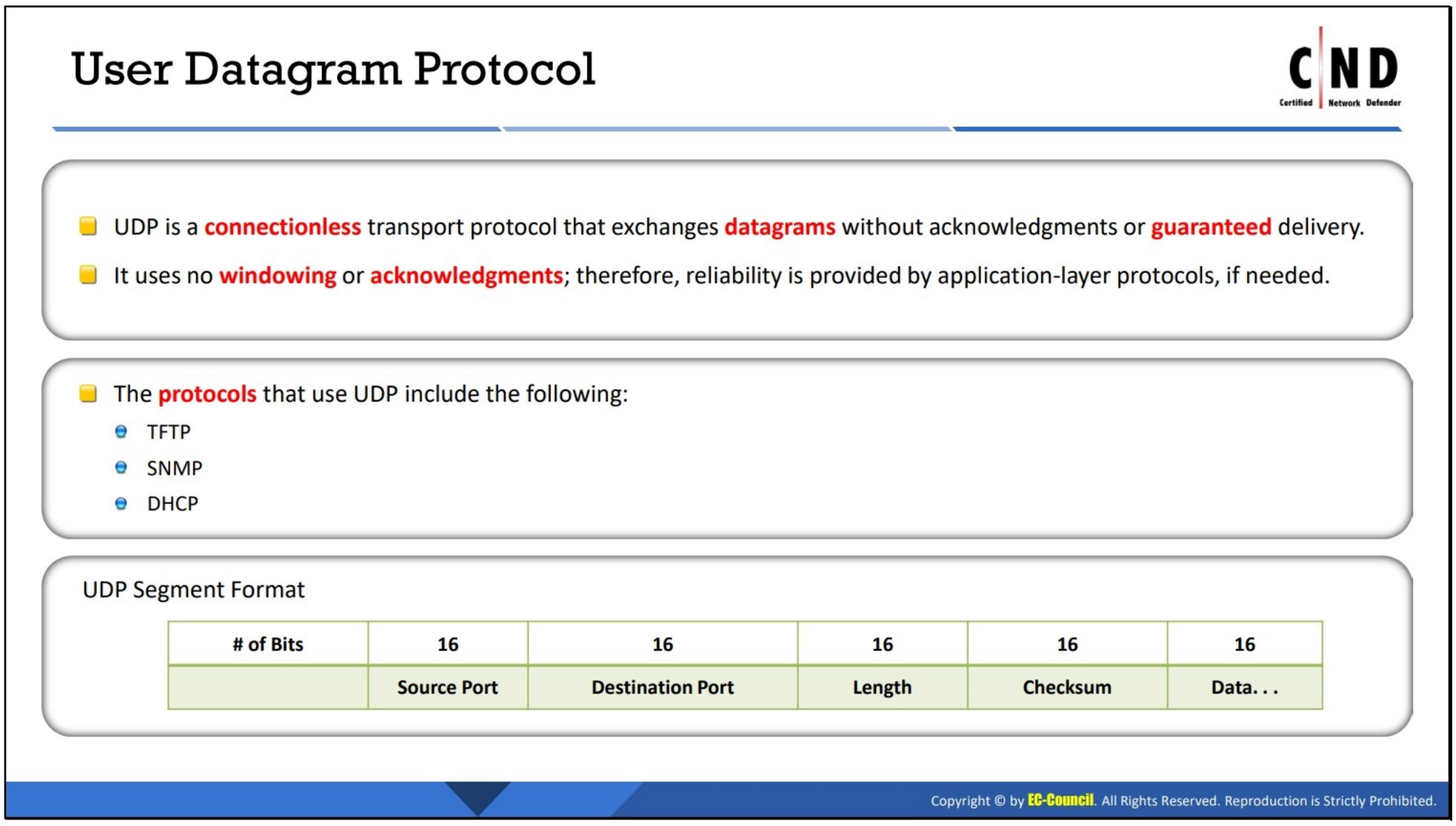


Figure A.58: TCP Header Format

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



User Datagram Protocol

UDP functions at layer 4 of the OSI model and provides faster data transmission than TCP. Unlike TCP, it does not require any connection (handshake process); therefore, it is called a connectionless protocol. Although UDP does not provide any transmission reliability, the protocols that depend on this feature for data transmission have their own error-handling mechanisms.

UDP is a connectionless transport protocol that exchanges datagrams without acknowledgments or guaranteed delivery. It uses no windowing or acknowledgments; therefore, reliability is provided by application layer protocols, if needed.

The protocols that use UDP include the following:

- TFTP
- SNMP
- DHCP

UDP Header

The UDP header contains less fields than the TCP header. The fields in the UDP header and their details are listed below.

- **Source port**: The port of the source host (UDP port)
- **Destination port**: The port of the receiving or destination host (UDP port)
- **Packet length**: The length of the header and data in bytes
- **Checksum**: Optional field that ensures the data transmitted is error-free and there is no damage to the data

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Data**: Information about the data in the packet that are sent in the form of segments

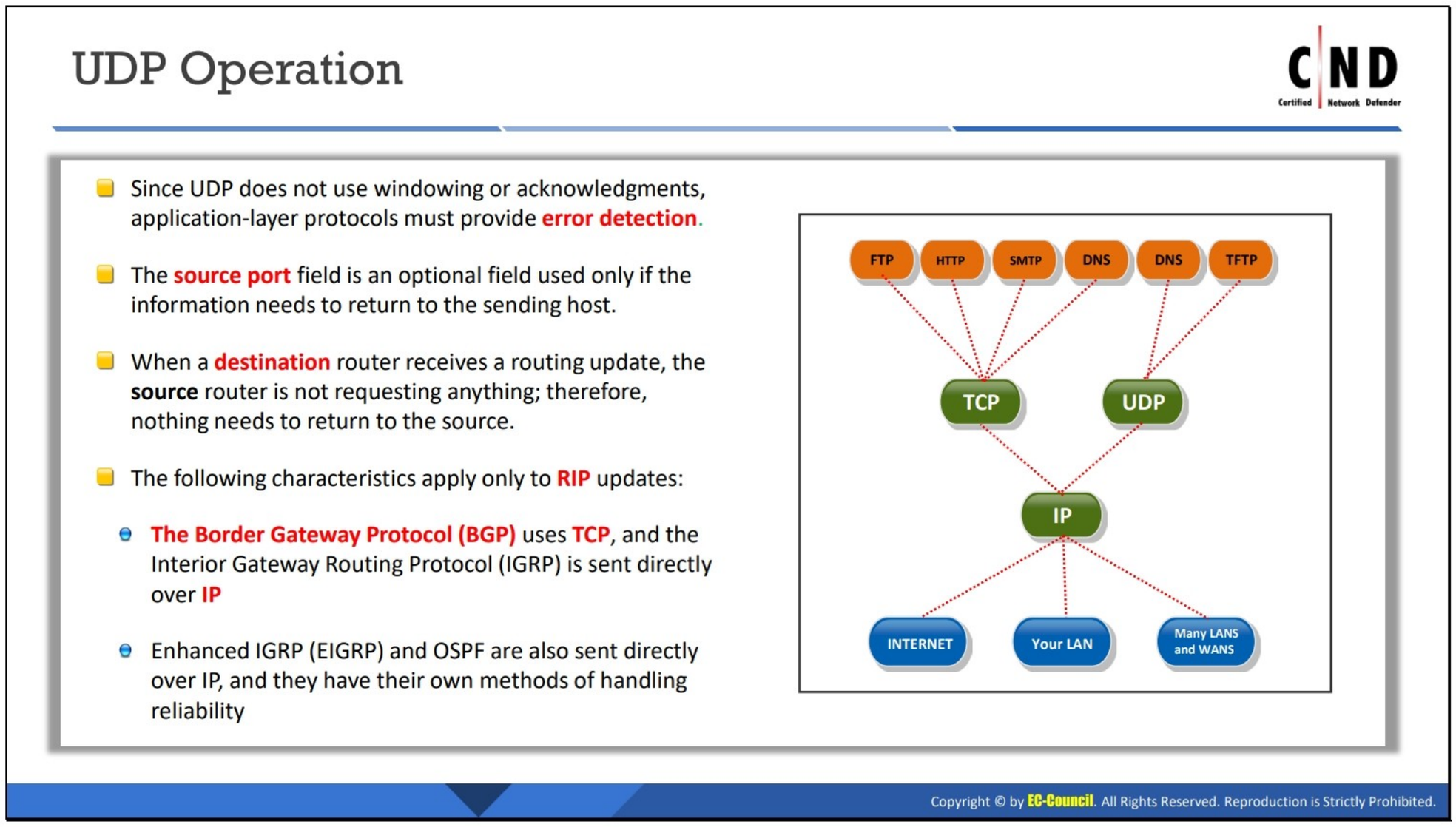
# of Bits	16	16	16	16	16
	Source Port	Destination Port	Length	Checksum	Data. . .

Figure A.59: UDP Segment Format

Characteristics of UDP

- The communication is between two processes.
- Owing to its connectionless nature, the packets in UPD do not have any relation and can choose their own paths.
- UDP does not provide any error-control or flow-control mechanisms.
- It does not control congestion when it occurs.
- It packs the data that it receives and sends the data across a network to the destination; at the destination, it unpacks the data.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



UDP Operation

The primary operation of UDP is to collect data from higher-layer protocols and place the data in UDP messages to forward the UDP datagrams to IP for transmission. UDP provides a checksum feature that helps in detecting errors in the data transmission, ensures the proper transmission of the UDP message, and detects whether the message reached the exact destination.

Since UDP does not use windowing or acknowledgments, application-layer protocols must provide error detection. The source port field is an optional field used only if the information needs to return to the sending host. When a destination router receives a routing update, the source router is not requesting anything; therefore, nothing needs to return to the source.

The following characteristics apply only to RIP updates:

- The Border Gateway Protocol (BGP) uses TCP, and IGRP is sent directly over IP.
- Enhanced IGRP (EIGRP) and OSPF are also sent directly over IP, and they have their own methods of handling reliability.

The basic steps involved in the transmission of data using UDP are as follows.

- **Higher-layer data transfer:** The application sends a message to the UDP software.
- **UDP message encapsulation:** The received message is encapsulated into the data field of a UDP message. It occupies the headers of the UDP message, and source port, destination port, and checksum value may be calculated.
- **Transfer message to IP:** The UDP message is passed to IP for transmission.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

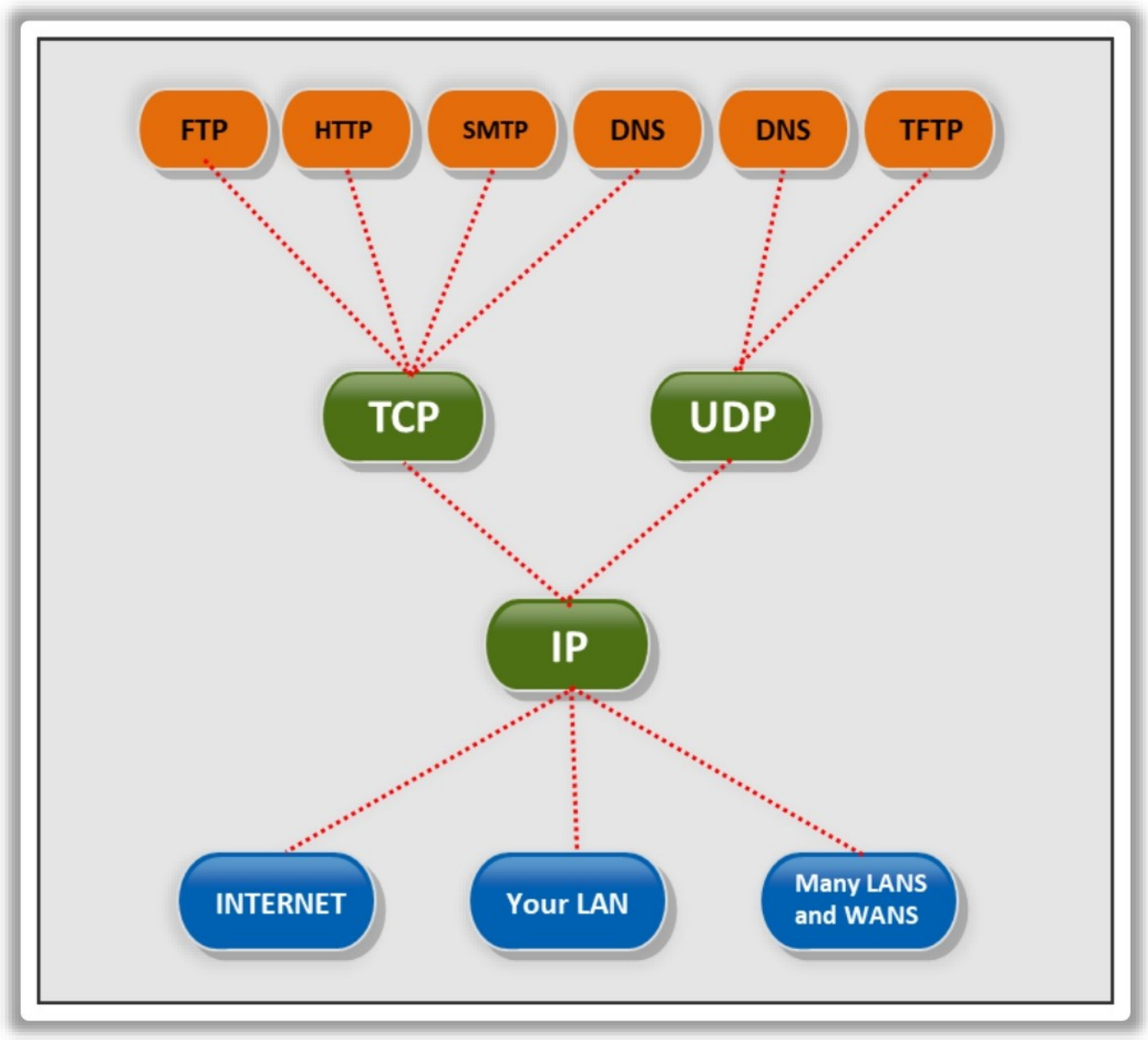


Figure A.60: Passing Messages to TCP and UDP

Comparison of UDP and TCP

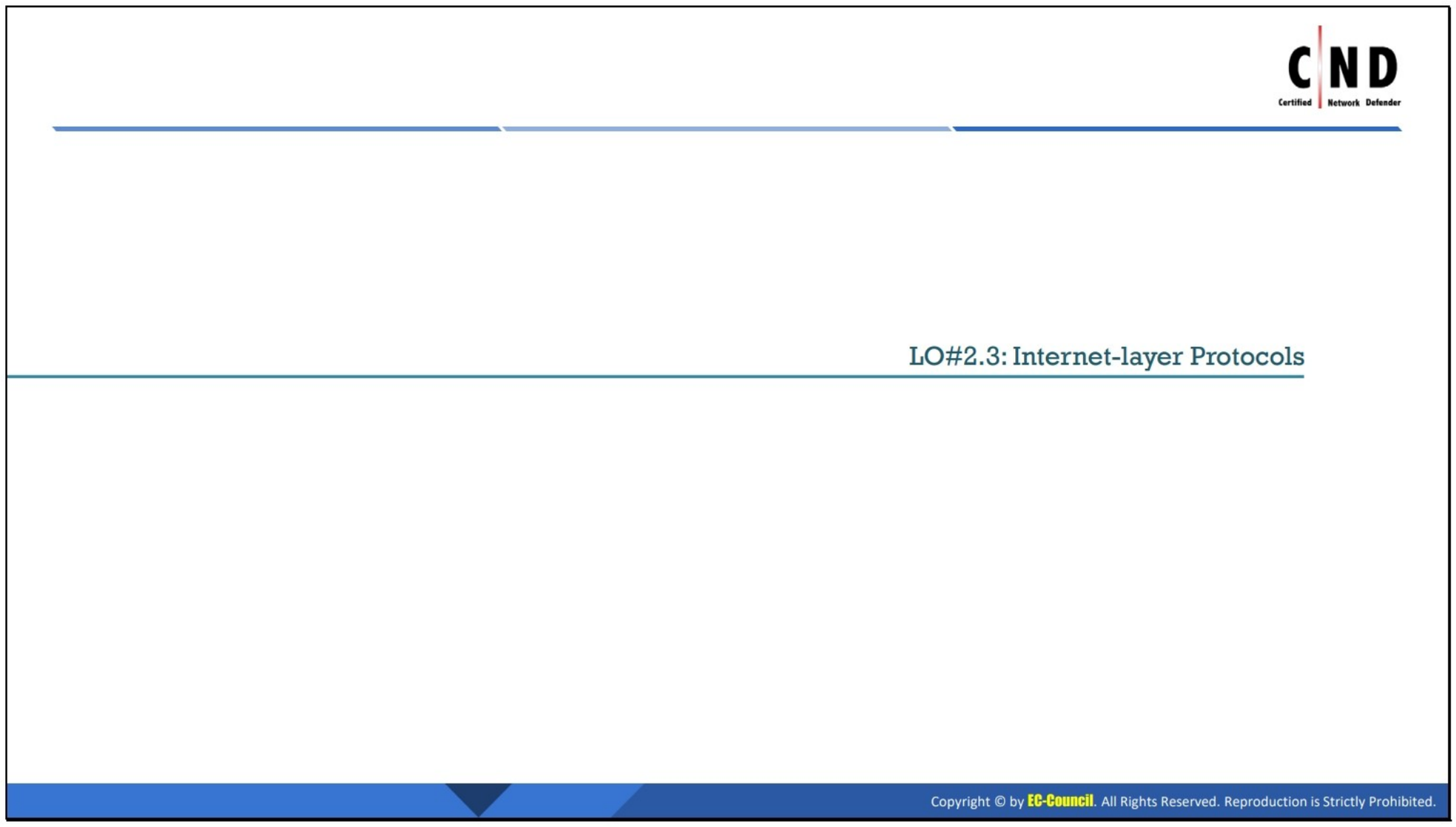
TCP has the following features.

- **Reliability**: TCP manages message acknowledgement, retransmission, and timeout. It confirms the arrival of all the packets at the receiver and attempts the 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 an incorrect order.
- **Heavyweight**: TCP manages reliability and congestion control.
- **Streaming**: TCP manages data as a byte stream.
- **Connection oriented**: TCP creates a session between the hosts.

UDP has the following features.

- **Unreliable**: UDP does not confirm the arrival of packets at the destination. It does not attempt to retransmit lost packets or follow the concept of acknowledgement.
- **Not ordered**: UDP does not confirm the sequence of arrival of the packets at the destination.
- **Datagrams**: UDP handles packets individually and deals with them only after their arrival at the destination.
- **Connectionless**: UDP does not create any session between the hosts.

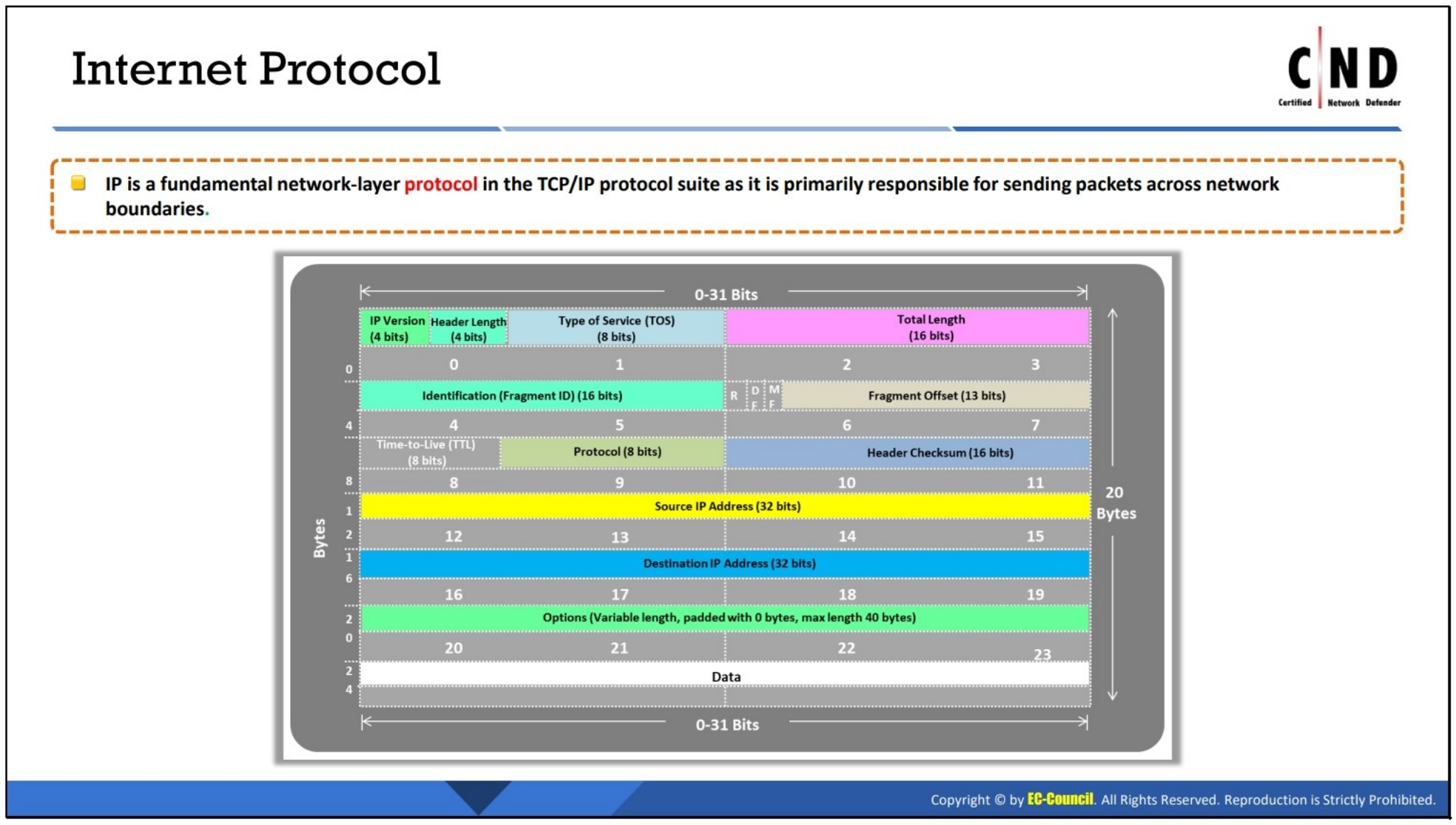
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#2.3: Internet-Layer Protocols

This section discusses the fundamentals and security aspects of Internet-layer protocols such as IPv4, IPv6, IP Security (IPsec), ICMP, ARP, IGRP, and EIGRP.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Internet Protocol (IP)

IP is a fundamental network-layer protocol in the TCP/IP protocol suite as it is primarily responsible for sending datagrams across network boundaries. It constitutes layer 3 of the OSI model protocol and is used for data communication between devices. This protocol accepts packets from TCP and UDP, and it sends them to their destination devices.

Characteristics of IP

- Based on the IP address of the device, this protocol sends data to the destination.
- Any network that implements the TCP/IP stack can allow IP data to travel through it.
- Like UDP, IP is also a connectionless protocol. It does not require any connection establishment for communication.
- This protocol does not guarantee that the data a is sent to the correct destination.
- The receiving host does not respond to the sender with an acknowledge message.

IP Header

The IP header provides a large amount of information. The following fields are a part of the IP header.

- **Version**: Defines the version of IP the packet belongs to
- **Header length**: Total length of the IP header
- **Type of service**: Defines the type of service that a router can be used for
- **Total length**: Defines the total length of the IP packet (header and data)
- **Identification**: A unique number used for the identification of the packet

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Flags**: Defines whether a packet is of the same sequence or a fragmented one
- **Fragment offset**: Provides a value used to line up a fragmented packet
- **Time to live**: Defines the total lifetime of the IP packet and can be calculated as number of hops per second
- **Protocol**: Defines the kind of packet that follows in the sequence
- **Header checksum**: Defines a mechanism that monitors the header information and informs about damaged or corrupted packets
- **Source IP address**: IP address of the sending host
- **Destination IP address**: IP address of the receiving host
- **Options**: Provides additional information about the IP such as routing and timestamps
- **Data**: Actual data of the IP

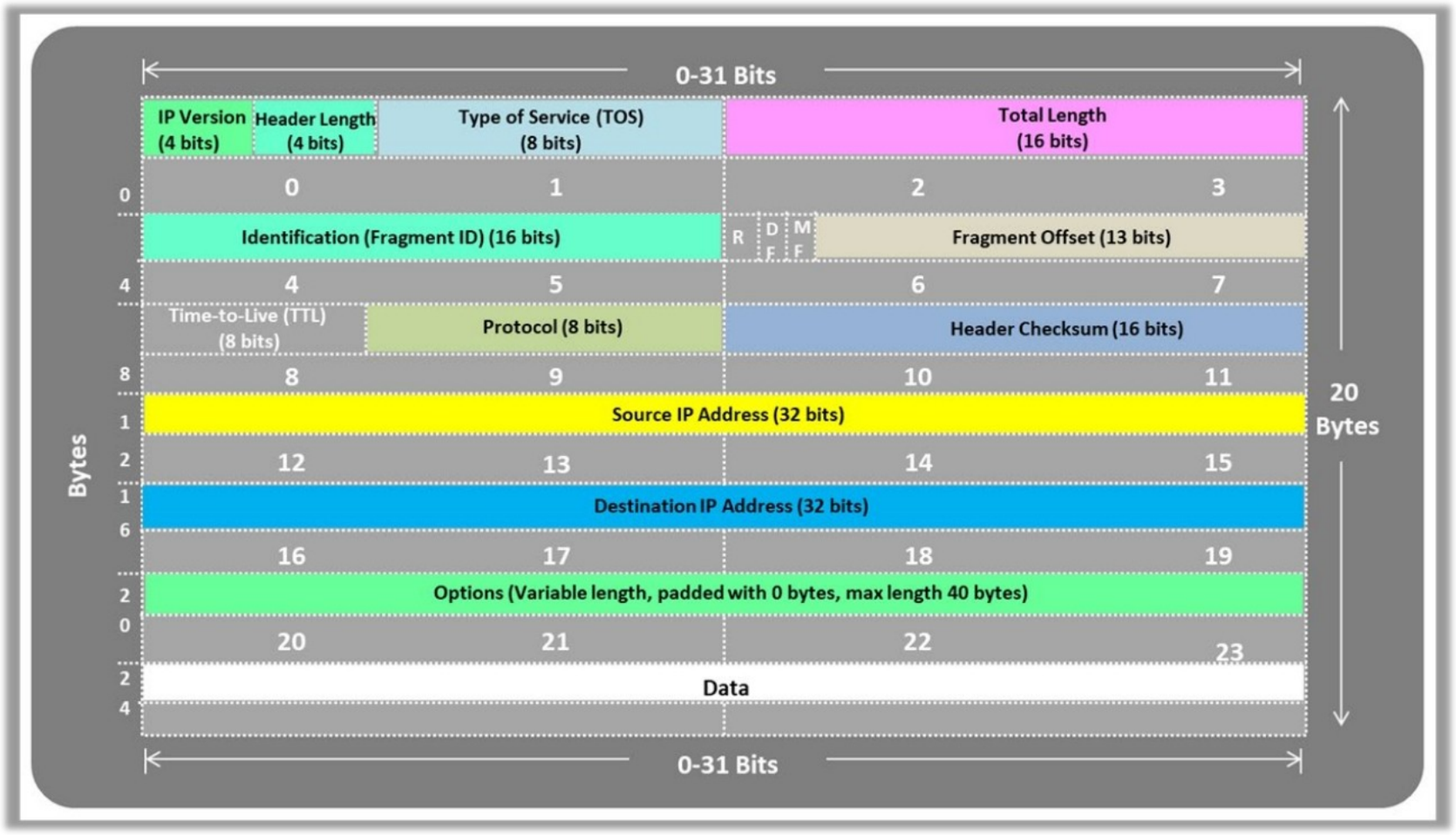
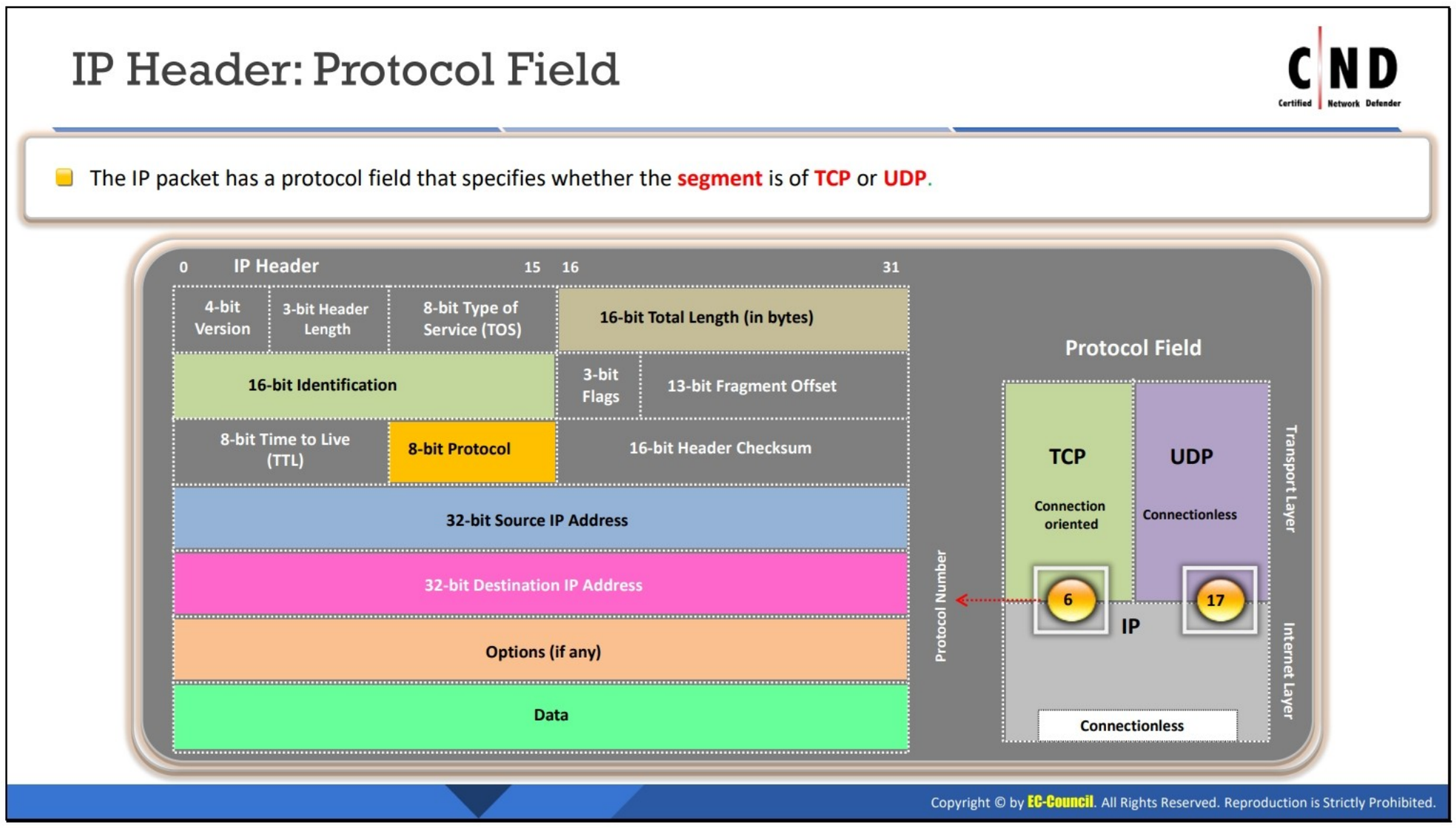


Figure A.61: IP Format

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IP Header: Protocol Field

The IP packet has a protocol field that specifies whether the segment is of TCP or UDP. The protocol field in the IP header is an 18-bit field that contains information about the protocol of the receiving host. IP is designed to carry all types of protocol information from the source to the destination. In this process, it assembles the data at the source and reassembles the data at the destination; these processes are called multiplexing and demultiplexing, respectively. By using the value in the protocol field, the IP demultiplexes the data at the destination host.

Table A.3 lists some commonly used IP protocol numbers.

Protocol	Number
Internet Control Message Protocol (ICMP)	1
Transmission Control Protocol (TCP)	6
Exterior Gateway Protocol (EGP)	8
User Datagram Protocol (UDP)	17
Host Monitoring Protocol (HMP)	20
Reliable Datagram Protocol (RDP)	27
General Routing Encapsulation (PPTP data over GRE)	47
Encapsulation Security Payload (ESP) IPsec	50
Internet Group Management Protocol (IGMP)	88
Open Shortest Path First (OSPF)	89

Table A.3: IP Protocol Numbers

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

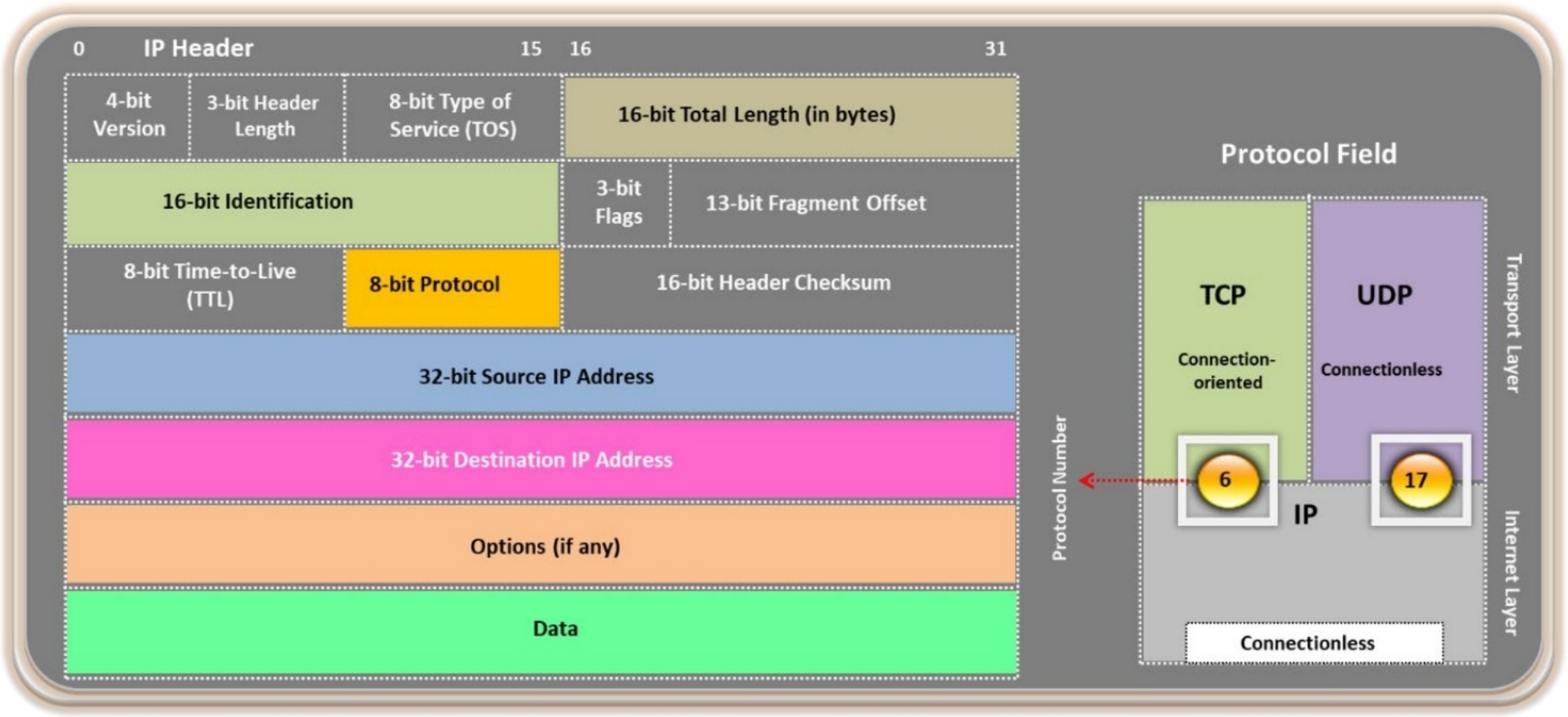
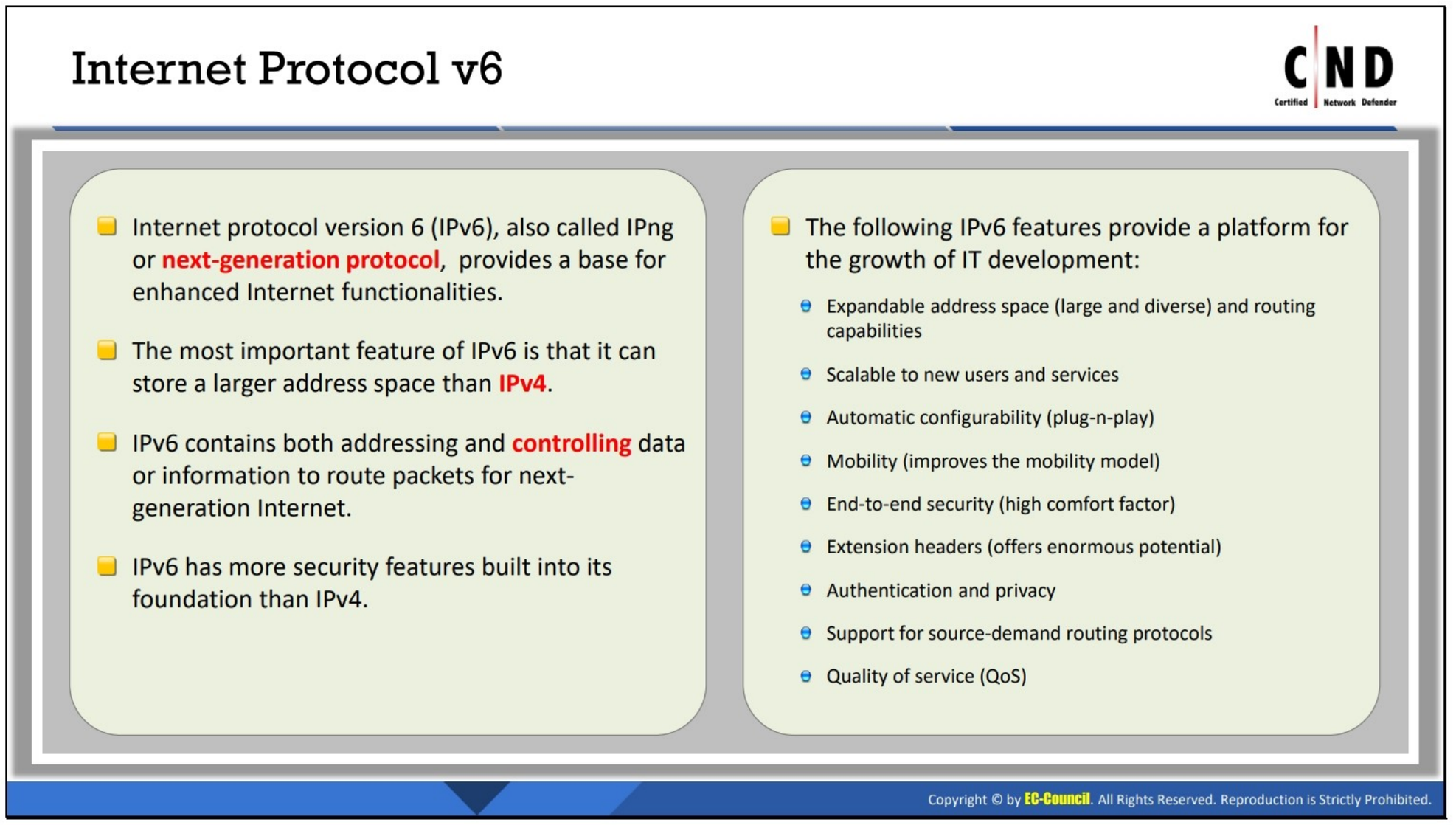


Figure A.62: IP Header Format

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Internet Protocol v6

Internet protocol version 6 (IPv6) is the most recent version of IP. It provides a mechanism for identifying computers in a network and routes traffic across the Internet. To meet the increasing requirements, the Internet Engineering Task Force (IETF) started a working group called the Internet Protocol next generation (IPng) to perform research and experiments as well as propose recommendations for developing a new-generation IP protocol. IPv6 provides a base for enhanced Internet functionalities. The working group eventually developed a specification for IPv6, as described in Internet standard document RFC 2460. Experts consider IPv6 as a replacement to IPv4. The most important feature of IPv6 is that it has a larger address space than IPv4. IPv6 uses a source and destination address to carry data packets over a network, as in IPv4. However, the address space of IPv6 is massive because it consists of 128 bits as compared to 32 bits in IPv4. IPv6 contains both addressing and controlling data or information to route packets for next-generation Internet. IPv6 has more security features built into its foundation than IPv4.

The features of IPv6 include the following:

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

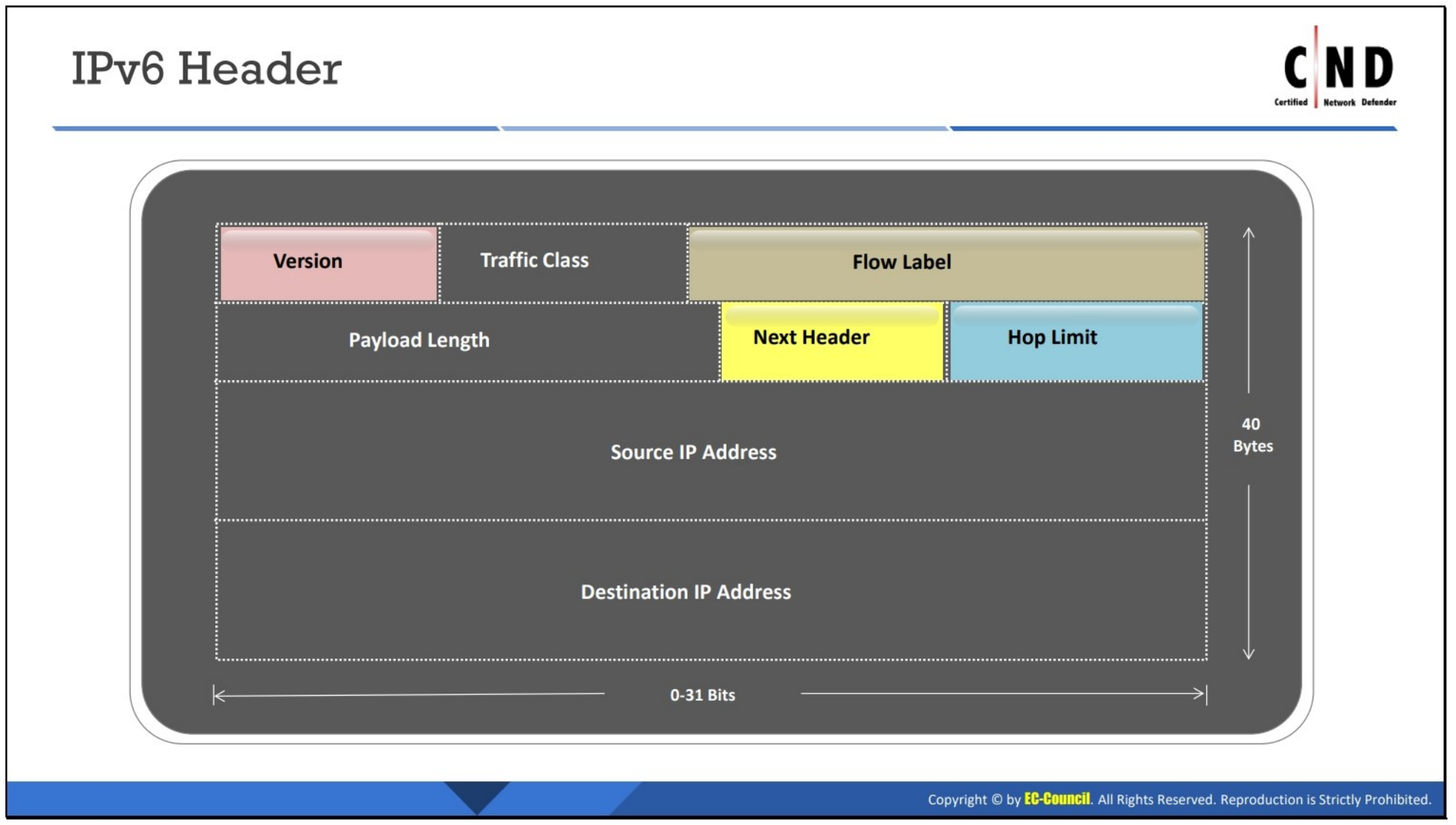
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- IPv6 simplifies the host configuration with stateless and stately address configuration for network interfaces.
- IPv6 has an inbuilt security feature called integrated IPsec. It is a set of Internet standards based on cryptographic security services providing confidentiality, data integrity, and authentication.
- IPv6 provides better support for quality of service (QoS) with the proper management of network traffic.

The following are some additional IPv6 features that provide a platform for the growth of IT development:

- Expandable address space (large and diverse) and routing capabilities
- Scalable to new users and services
- Automatic configurability (plug-n-play)
- Mobility (improves the mobility model)
- End-to-end security (high comfort factor)
- Extension headers (offers enormous potential)
- Authentication and privacy
- Support for on-demand routing protocols

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IPv6 Header

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

The fixed header of IPv6 is 40 bytes long and consists of the following fields:

- **Version (4 bits):** Specifies the IP version
- **Traffic class (8 bits):** Identifies the data packets that belong to the same traffic class and distinguishes packets with different priorities
- **Flow label (20 bits):** Avoids reordering of data packets and maintains the sequential flow of data packets belonging to the communication
- **Payload length (16 bits):** Informs the router about the length of the data 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 the time-to-live field in IPv4; identifies and discards packets that are stuck in an indefinite loop due to any routing information errors; discards the packet when the counter reaches zero
- **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**

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The fixed header consists of only the required information. The information that is rarely used or is not required is always placed between the fixed header and the upper layers of the extension header. Each extension header requires a distinct value to be identified.
- 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.
- Figure A.63 shows the sequence of the extension headers.

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 A.63: Sequence of IP Header

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

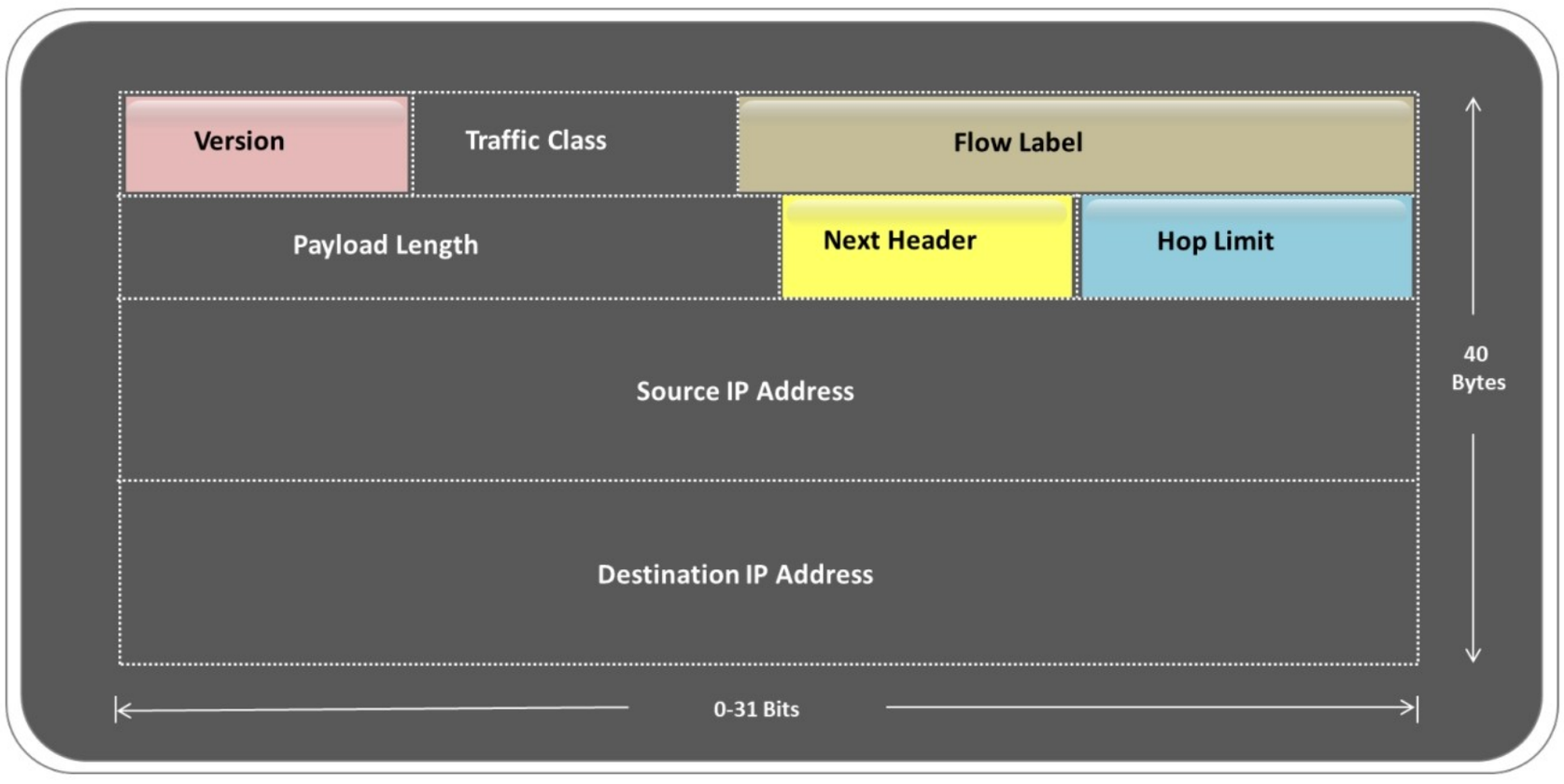
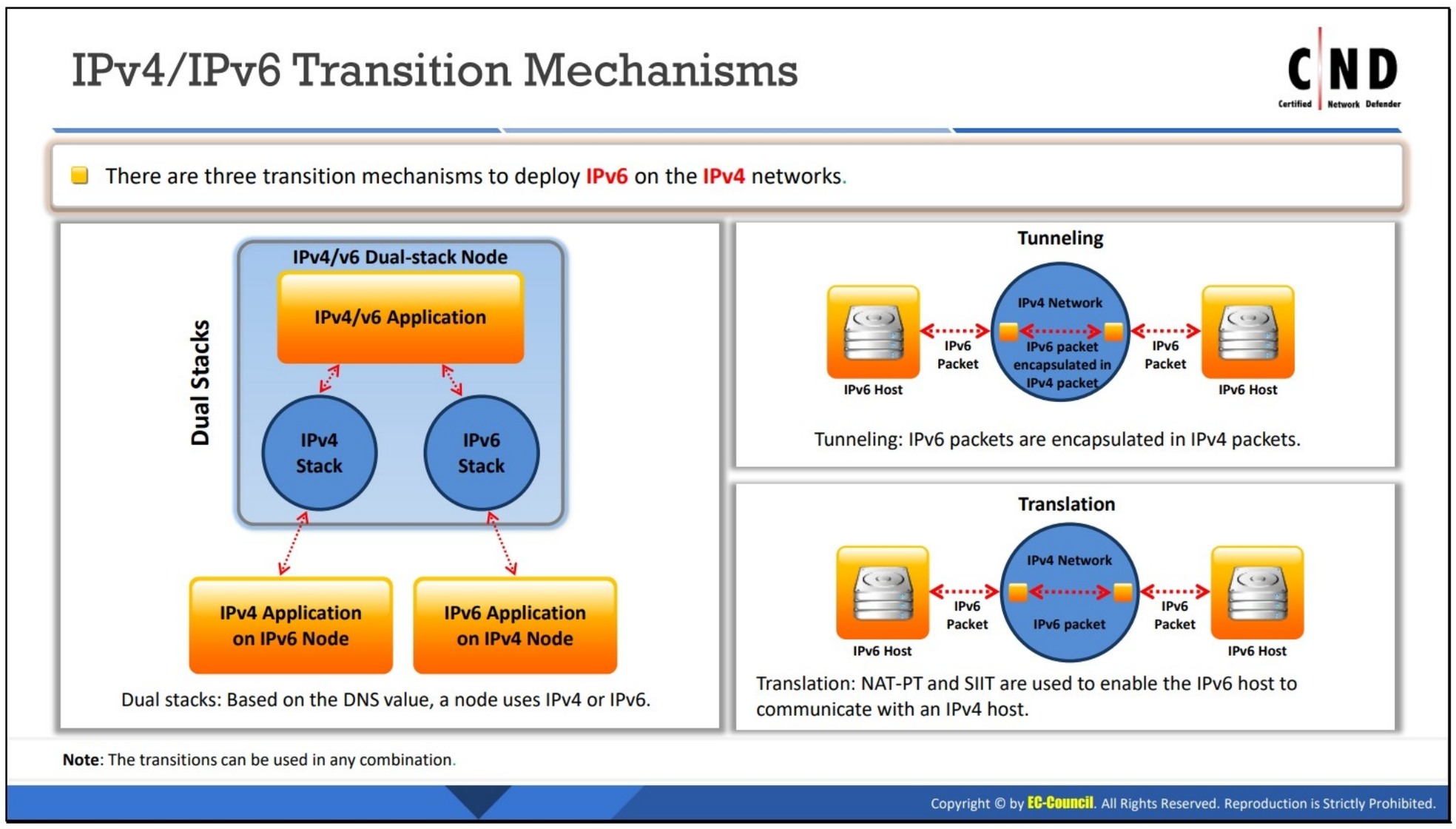


Figure A.64: IPv6 Header

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IPv4/IPv6 Transition Mechanisms

Owing to the yearly increase of Internet users worldwide, it has become difficult to manage with the IPv4 address space. To meet future requirements and demand for the address space, IPv6 was developed.

It has now become necessary to move networks to IPv6 addressing. However, moving towards IPv6 is a difficult task as it requires a good understanding of IPv6. Many models and tools have been developed for this purpose, which differ in their operation process. The IPv6 transition can be achieved through the compatibility maintenance of IPv6 with IPv4 while deploying.

There are three transition mechanisms to deploy IPv6 on IPv4 networks, as discussed below.

- **Dual stack**

  In this mechanism, the IPv4 implementation should be provided to IPv6 nodes to maintain compatibility with IPv4 nodes. After completion of this task, the nodes with both implementations are referred to as IPv4/IPv6 nodes. These nodes possess the mechanism of sending and receiving both types of information.

  There are three modes for operating IPv4/IPv6 nodes:

  - IPv4 stack enabled and IPv6 stack disabled (IPv4-only node)
  - IPv4 stack disabled and IPv6 stack enabled (IPv6-only node)
  - Both stacks enabled

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

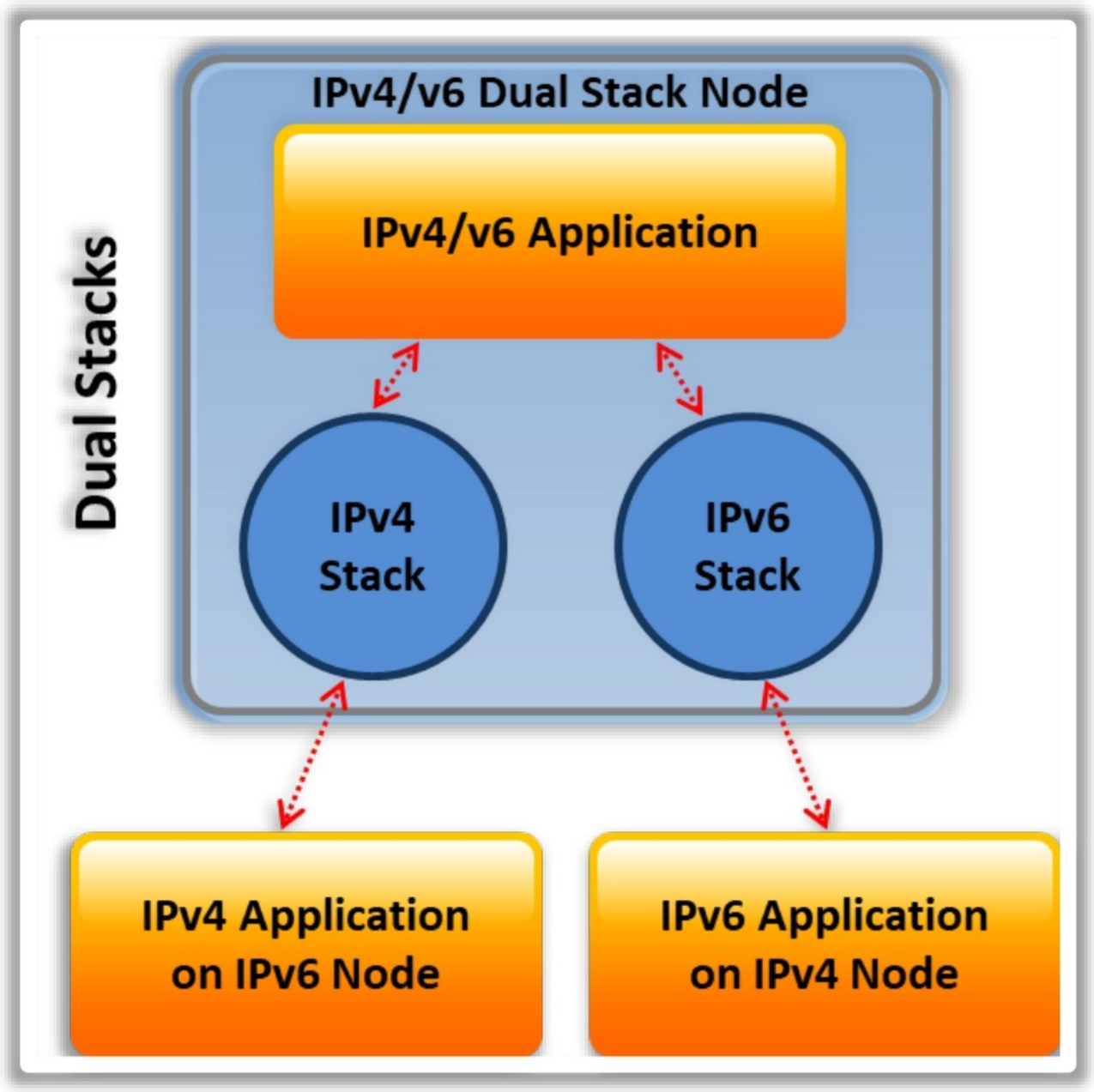


Figure A.65: Dual Stack

Advantages

- The dual-stack mechanism can be easily deployed on hosts and routers
- Irrespective of the dual-stack mechanism, the hosts can still identify the IPv4 address.
- It manages DNS address resolution issues.
- The deployment and management are flexible on most platforms.

Disadvantages

- It requires a relatively large memory space and high processing speed.
- The routing process is complex because of dual routing tables.

- **Tunneling**

  Through this mechanism, the existing IPv4 routing process allows IPv6 traffic to pass through. IPv6 information can be tunneled through the IPv4 routing path along with IPv4 information through the encapsulation of both types of packets.

  The tunneling can be performed in the following ways.

  - **Router-to-router**: The routers in a network that supports IPv4/IPv6 packets are connected through IPv4 routing infrastructure and allows IPv6 packets to travel through them.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Host-to-router**: The IPv4 routing path is used for transferring the IPv6 packet from IPv4/IPv6 hosts to IPv4/IPv6 routers in a network.
- **Host-to-host**: The IPv4/IPv6 hosts that are connected with each other through the IPv4 routing path can carry IPv6 information through them.
- **Router-to-host**: The IPv4/IPv6 routers choose an IPv4 routing path to send IPv6 packets to the IPv4/IPv6 hosts in a network.

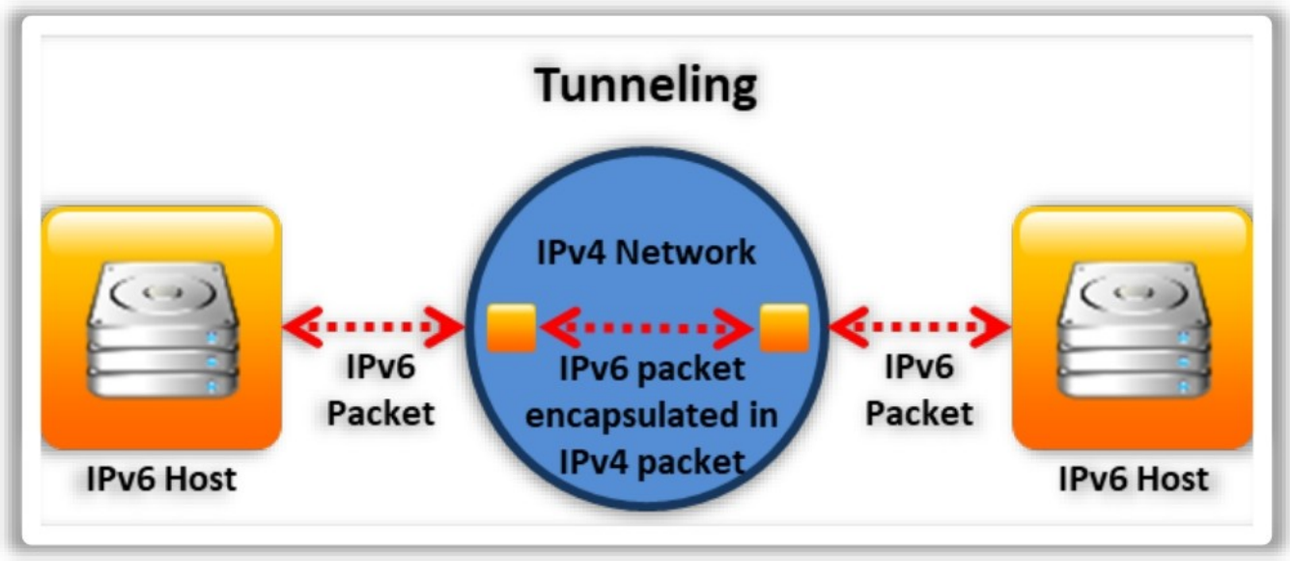


Figure A.66: Tunneling

The tunneling mechanism proceeds in the following manner:

- The source node encapsulates the IPv4 packets and IPv6 packets together into an IPv4 header and sends them to the other end.
- The destination node decapsulates the IPv4 header and separates the IPv4 and IPv6 packets for further processing.

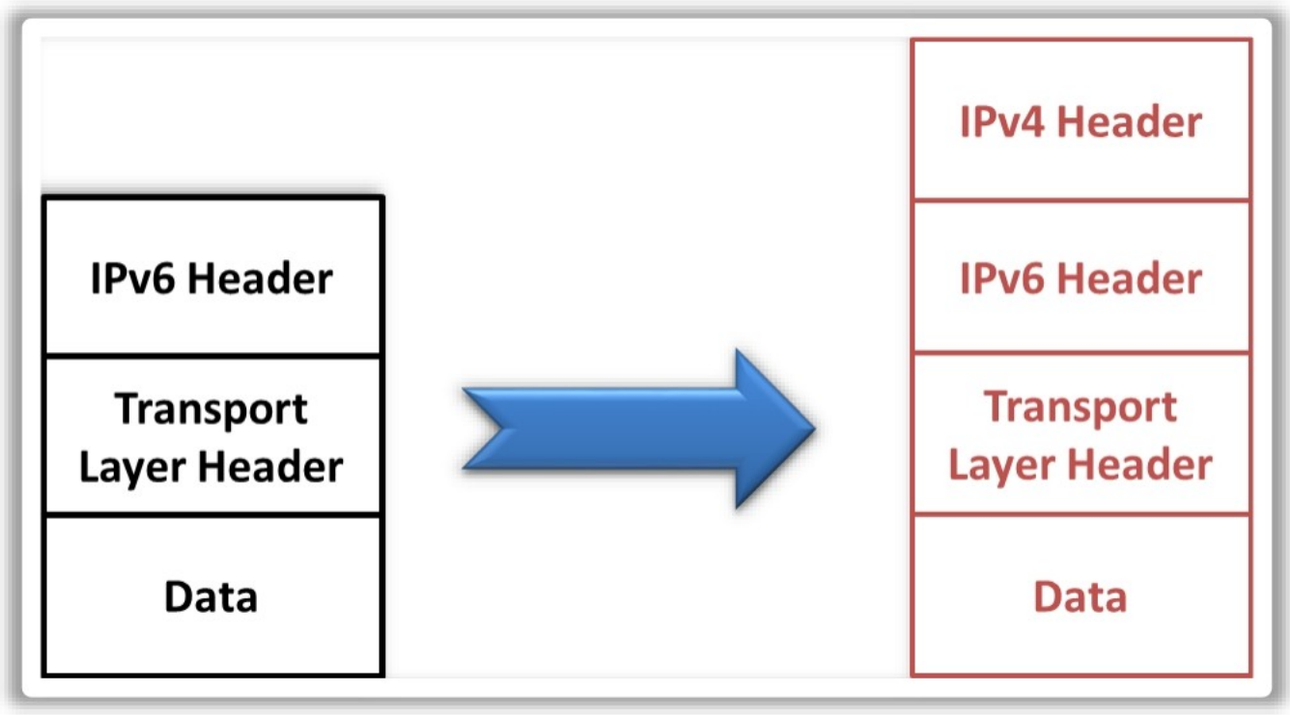


Figure A.67: Encapsulation of IPv6 into IPv4

Advantages

- IPv6 information is allowed to pass through an IPv4 network.
- It is flexible to deploy in many platforms.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Disadvantages

- Owing to the tunneling process, a packet delivery latency might occur.
- The encapsulation and decapsulation place a high load on processors.
- The configuration must be performed manually.

- **Translation**

  This mechanism utilizes a device in a network that functions as a translator from the IPv4 to IPv6 and vice versa. This translation process should be performed in to-and-fro directions for establishing the data transfer.

  The major difference between translation and tunneling is that, in translation, IPv4-only devices are used for transferring IPv6 data, while in tunneling, IPv4/IPv6 devices are used.

  Technically, it is not possible for IPv6 data to be transmitted in an IPv4 network. Therefore, a third-party technology called Network Address Translation–Protocol Translation (NAT–PT) is required to make this possible. NAT-PT uses the Application Layer Gateway (ALG) for translation of IPv4 to IPv6 and vice versa, as well as the translation of protocols such as DNS and ICMP.

  Owing to the issues with the functioning of ALG, NAT64 and DNS64 methods were developed, which separate the layer and address translation functionalities.

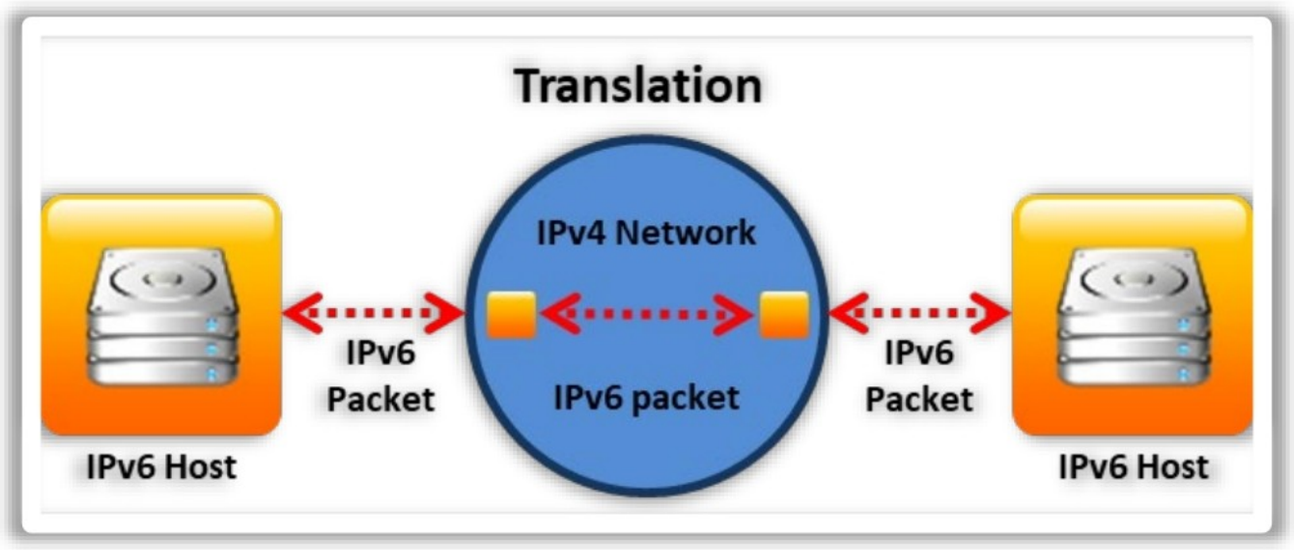
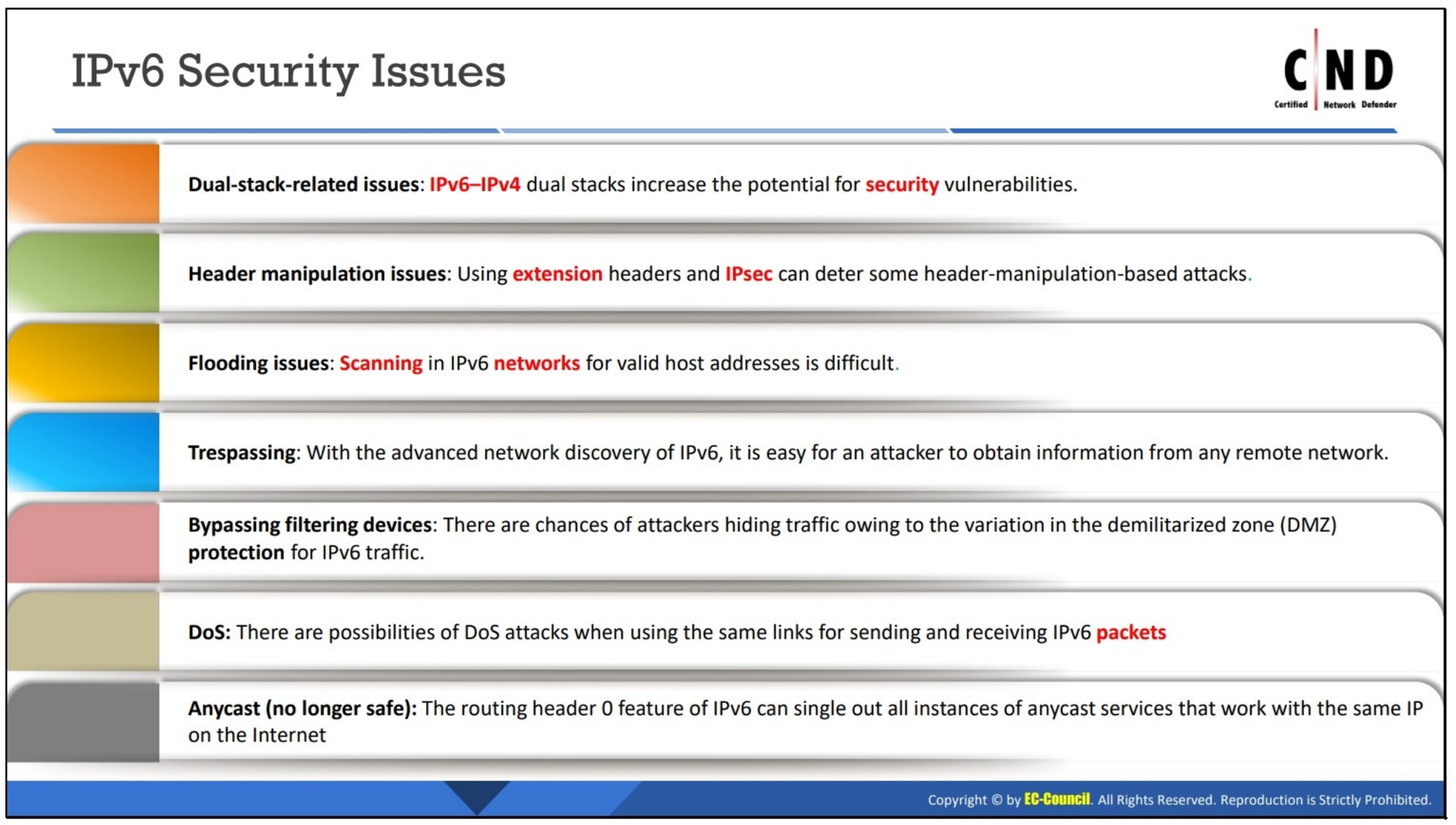


Figure A.68: Translation

Note: The transitions can be used in any combination.

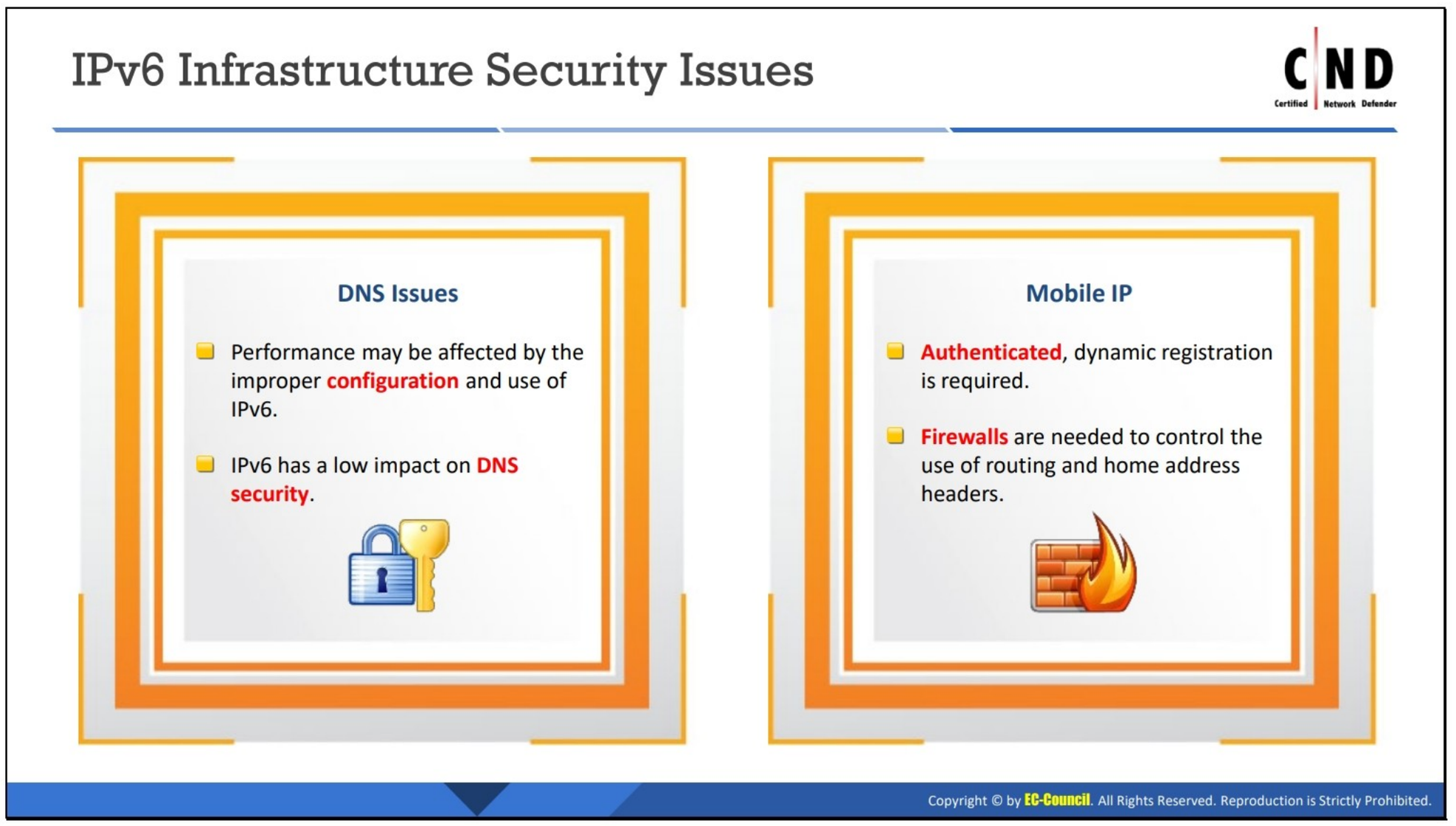
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IPv6 Security Issues

- **Dual-stack-related issues**: IPv6–IPv4 dual stacks increase the potential for security vulnerabilities.
- **Header manipulation issues**: Using extension headers and IPsec can deter some header-manipulation-based attacks.
- **Flooding issues**: Scanning in IPv6 networks for valid host addresses is difficult.
- **Trespassing**: With the advanced network discovery of IPv6, it is easy for an attacker to obtain information from any remote network.
- **Bypassing filtering devices**: There are chances of attackers hiding traffic owing to the variation in the demilitarized zone (DMZ) protection for IPv6 traffic.
- **DoS**: There are possibilities of DoS attacks when using the same links for sending and receiving IPv6 packets.
- **Anycast (no longer safe)**: The routing header 0 feature of IPv6 can single out all instances of anycast services that work with the same IP on the Internet.

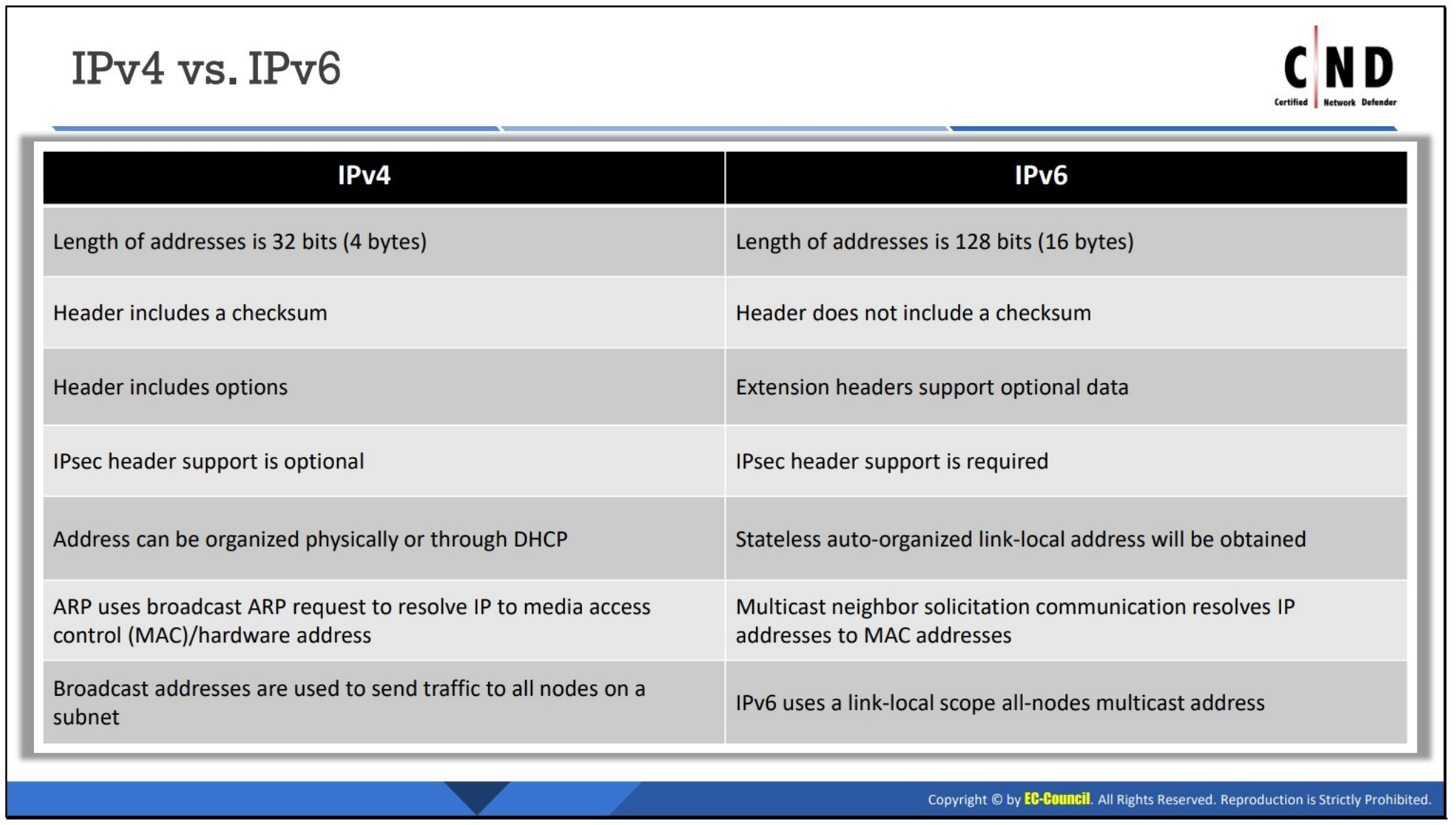
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IPv6 Infrastructure Security Issues

- **DNS Issues:**
  - Performance may be affected by the improper configuration and use of IPv6.
  - IPv6 has a low impact on DNS security.
  - The process of data exchange between DNS servers and resolvers is changed by the increased address length and other IPv6 enhancements.
  - Domain naming is a problem with some similar-looking domain names (for example, telcal.com and telpa1.com).
  - Security models related to source-address validation are weak.
  - The authorization mechanism must be manually set between the DNS server and a node, which consumes time.
- **Mobile IP:**
  - Authenticated, dynamic registration is required.
  - Firewalls are needed to control the use of routing and home address headers.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IPv4 vs. IPv6

IPv4

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

IPv6

Also known as IPng, IPv6 is an advanced version of IPv4 and will replace IPv4. IPv6 allows better handling of hosts and the data flowing on the Internet. The main advantage of using IPv6 is that it reduces the exhaustion of IP addresses. IPv6 addresses are 128 bits long and represented using hexadecimal digits. The sender performs fragmentation. 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 contain any checksum or options field. IPv6 has an auto-configuration mode that eliminates the need for manual configuration as in IPv4.

Advantages of IPv6 over IPv4

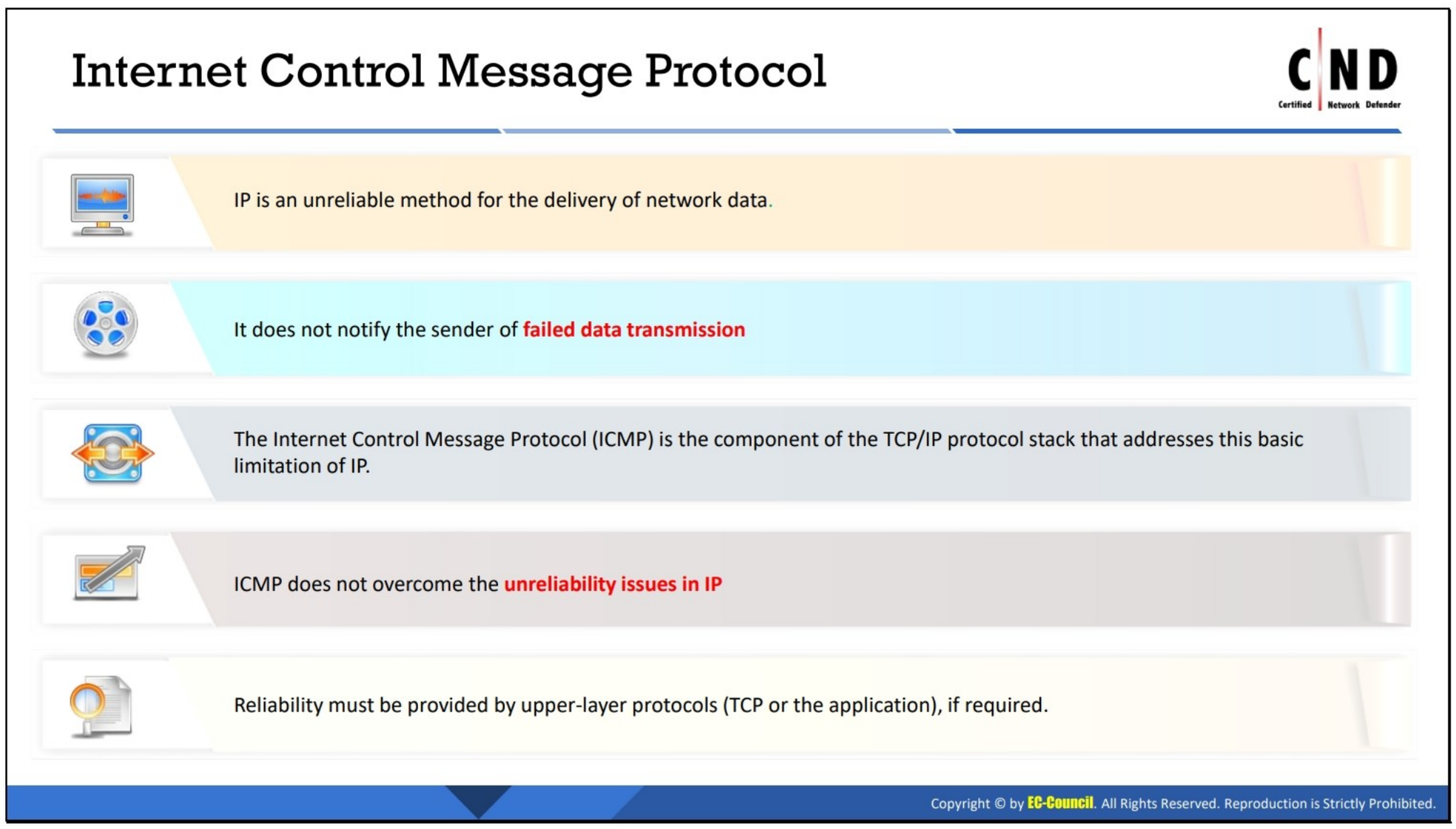
- IPv6 provides a simplified method for router tasks when compared with IPv4.
- IPv6 is more reliable than IPv4 and can handle more payloads.
- IPv6 is more compatible for use in mobile networks than IPv4.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	Internet Protocol version 4 (IPv4)	**Internet Protocol version 6 (IPv6)**
Year Deployed	1981	1999
Size	32-bit addresses	128-bit source and destination addresses
Format	Dotted-decimal notation (separated by periods)	Hexadecimal notation (separated by colons)
Example	192.168.0.77	3ffe:1900:4545:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.168.0.7/74	3FFE:F200:0234::/77
Total Number of Addresses	2^{32} = 4,294,967,296	2^{128} = 340,282,366, 920,938,463,463,374, 607,431,768,211,456
Configuration	Manual static or dynamic configuration	Auto-configuration of addresses is available
Security	IPsec is optional	Inbuilt support for IPsec

Table A.4: Comparison between IPv4 and IPv6

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Internet Control Message Protocol (ICMP)

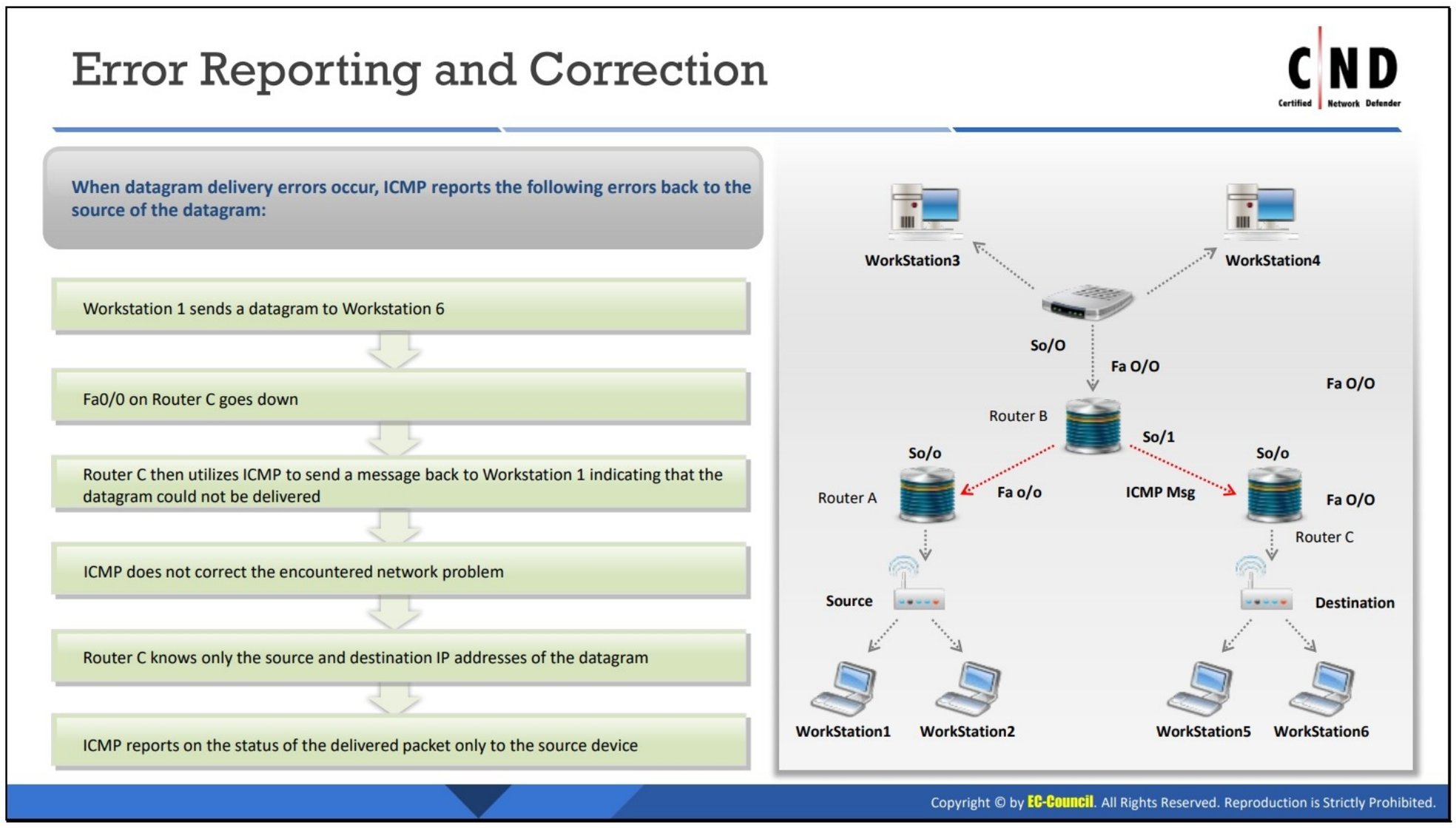
IP is an unreliable method for the delivery of network data. It does not notify the sender of failed data transmission. The Internet Control Message Protocol (ICMP) is the component of the TCP/IP protocol stack that addresses this basic limitation of IP. ICMP does not overcome the unreliability issues in IP. Rather, reliability must be provided by upper-layer protocols (TCP or the application), if required.

ICMP is an error reporting protocol used by networking devices such as routers 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. It is mainly used by network administrators troubleshooting Internet connections. ICMP transmits messages as datagrams and consists of an IP header that encapsulates 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. IPv4 or IPv6 is followed by the ICMP header, which identifies itself as protocol number 1.

ICMP consists of three fields:

- Major type that identifies the ICMP message
- Minor code that contains more information regarding the type field
- Checksum that identifies the errors during transmission

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Error Reporting and Correction

Error reporting and correction are two of the main functionalities of ICMP. Whenever an error occurs during transmission, ICMP sends an error report to the source machine that sent the data. The responsibility of ICMP is error reporting, while error correction is performed by higher-level protocols such as TCP and UDP. ICMP reports to the source machine regarding an issue based on the source IP information available in the IP header.

ICMP is capable of handling various types of errors such as the following.

- **Destination unreachable**: If the router or host is unable to trace the destination of a packet, it reverts with this message to the source machine.
- **Source quench**: Whenever flow-control or congestion-control mechanisms are deployed during IP packet transmission, ICMP notifies the source.
- **Time exceeded**: Every datagram packet contains a routing time. An error in the routing table may cause a packet to route around the network from one router to another. The routing time decreases by 1 for each router the packet visits. Finally, a "time exceeded" message is sent to the source when the routing time reaches zero.

  In case of a fragmented packet, all the packets should reach the destination machine within the time set by the destination machine. The "time exceeded" message is sent to the source when the time set by destination is over.
- **Parameter problems**: This message is sent to the source when there is a missing field in the header part of the packet.
- **Redirection**: In general, all the routers in a network follow a mechanism that allows them to update the routing table. This update is performed dynamically to inform the routers

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

to verify the next available router that receives the IP packet. However, the hosts cannot update their routing table dynamically; instead, it must be performed statically.

When the host wants to send a packet to the wrong router instead of the original source, the wrong router that received this packet traces the original router and sends the packet to it along with a redirection message to the host.

The ICMP error reporting mechanism has the following characteristics:

- An ICMP cannot report another ICMP's errors.
- It cannot handle the errors of a fragmented packet.
- It cannot handle the error of a packet that contains multiple destinations.

This error message contains information such as the IP header and 8 bytes of data (port and sequence numbers) about the packet on which the error occurred.

For example, when a datagram delivery error occurs, ICMP reports the following errors back to the source of the datagram:

- Workstation 1 sends a datagram to Workstation 6.
- Fa0/0 on Router C goes down.
- Router C then utilizes ICMP to send a message back to Workstation 1 indicating that the datagram could not be delivered.
- ICMP does not correct the encountered network problem.
- Router C knows only the source and destination IP addresses of the datagram.
- ICMP reports on the status of the delivered packet only to the source device.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

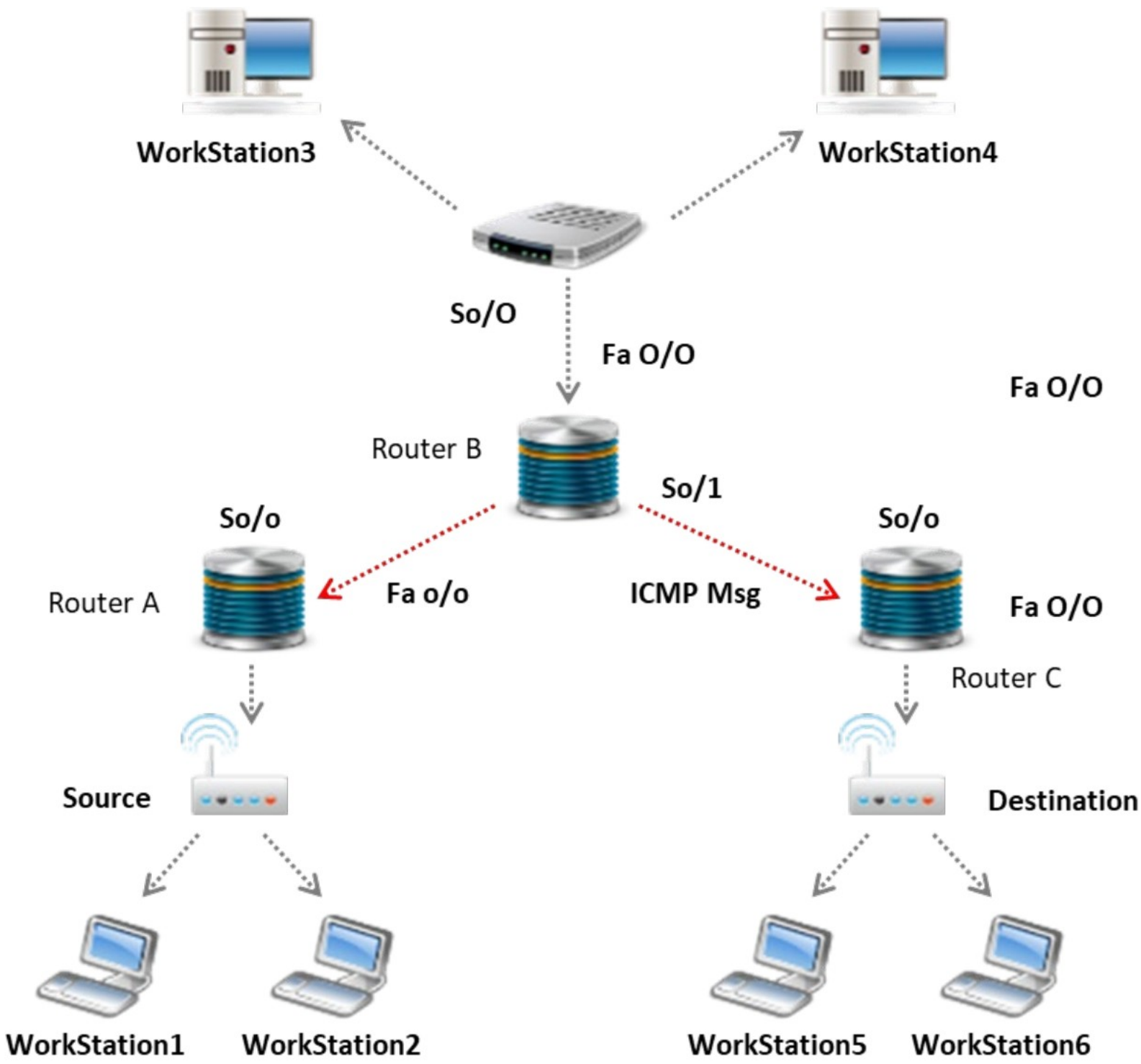
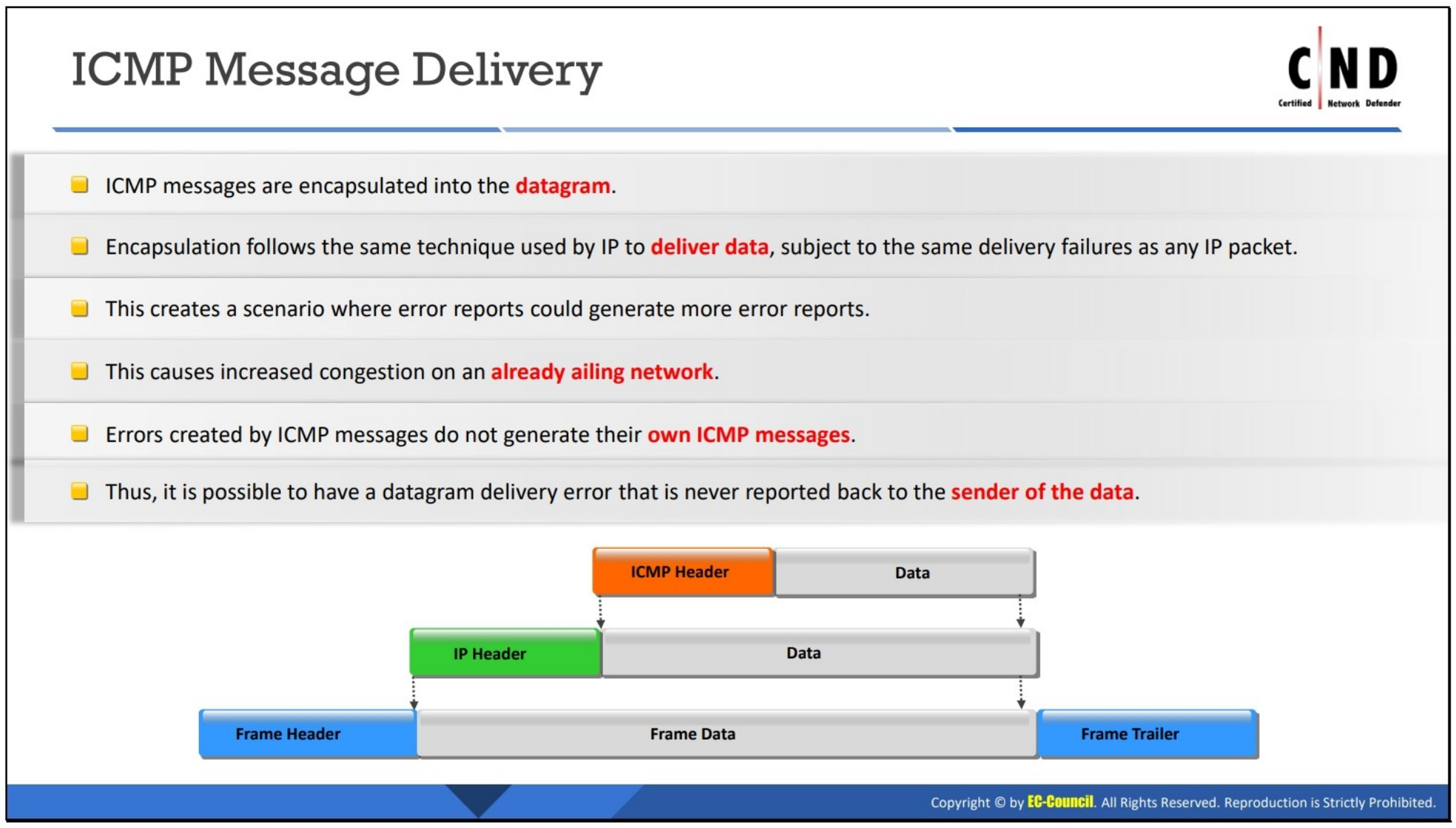


Figure A.69: Working of ICMP for Error Reporting

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ICMP Message Delivery

ICMP messages are encapsulated into the datagram. Encapsulation follows the same technique used by IP to deliver data and is subject to the same delivery failures as any IP packet. This creates a scenario where error reports could generate more error reports. This causes increased congestion on an already ailing network. Errors created by ICMP messages do not generate their own ICMP messages. Thus, it is possible to have a datagram delivery error that is never reported back to the sender of the data.

There are two types of messages that ICMP can carry: error reporting and (informative) query messages. Error reports, as discussed above, are used to inform the source machine that an error occurred during the IP packet transmission. The query messages are used to pass information among hosts in a network.

Message	Type	Details
Error reporting	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query (Informative)	8 or 0	Echo request/Echo reply
	13 or 14	Timestamp request/ Timestamp reply

Table A.5: ICMP Messages

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The message type field is 8 bits long and allows defining 256 types of message values. In ICMPv4, the message type values are assigned based on their arrival sequentially. Therefore, it is difficult hard to predict the type of message based on its type value. However, from ICMPv6 onwards, these types are segregated as 0 to 127 for error messages and 128 to 255 for query messages.

In case of the error message types, if the type values are unknown, then they should be sent to the higher-layer protocols.

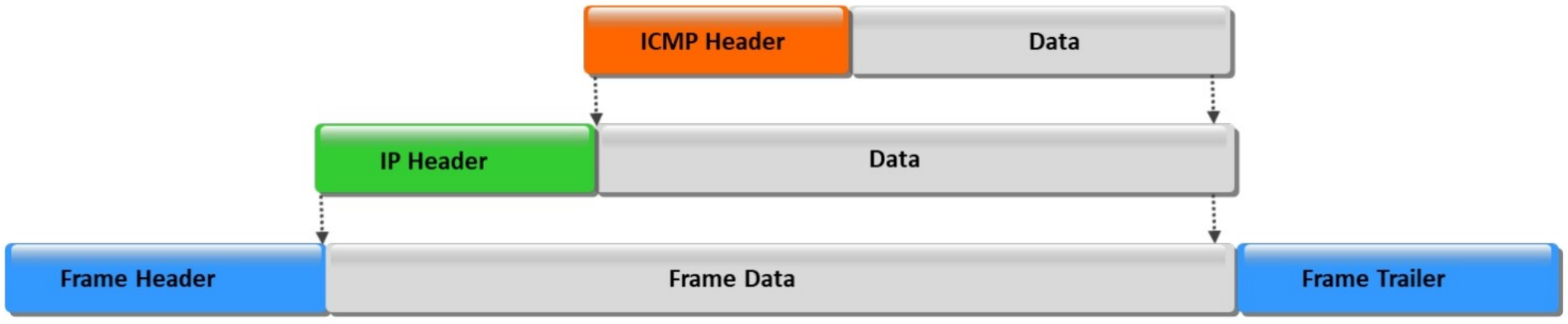
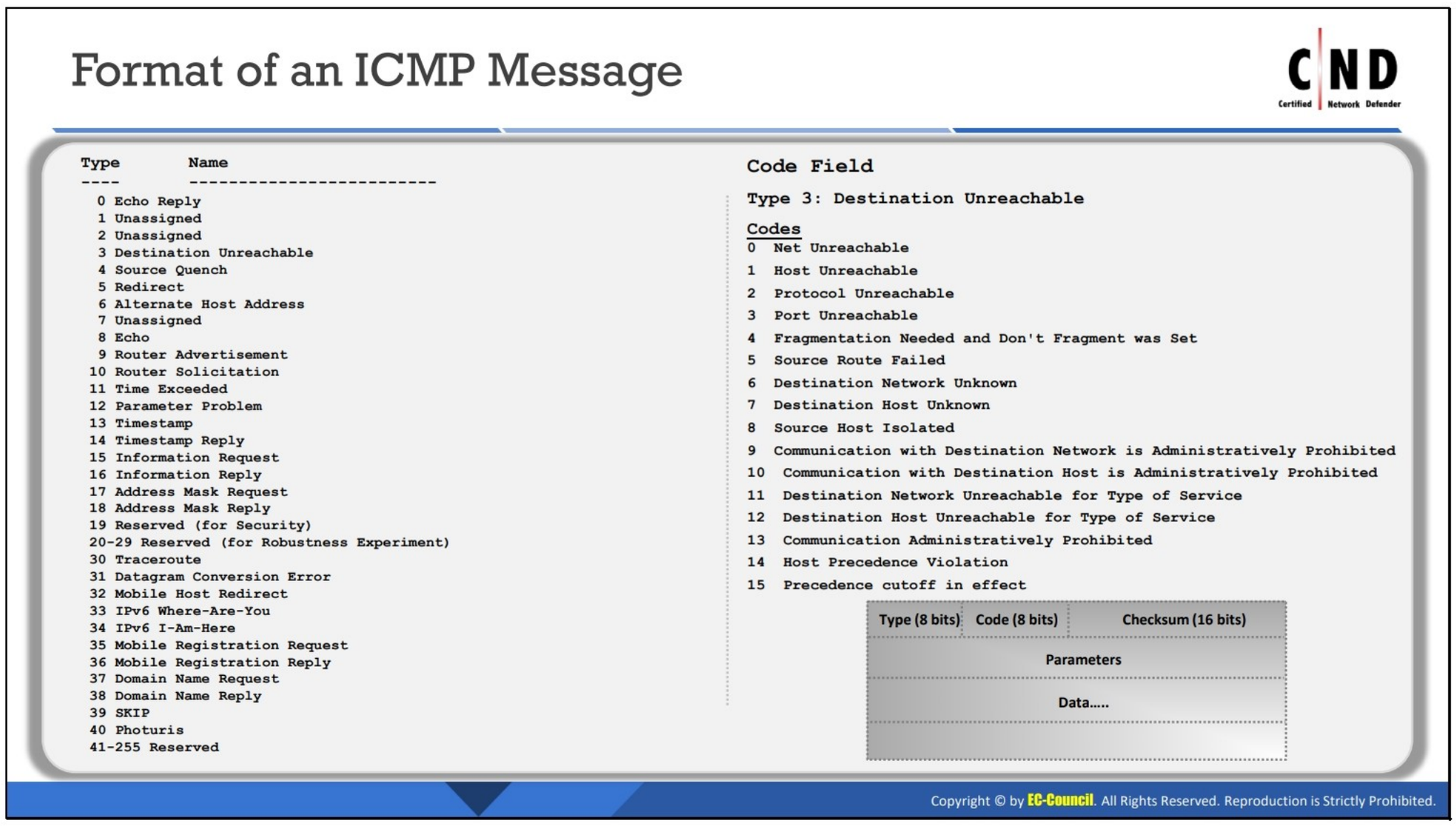


Figure A.70: ICMP Message Frame

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Format of an ICMP Message

The ICMP data and IP header follow the three fields in ICMP. 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 that the end system can identify which packet failed.

An ICMP message consists of three fields that have the same size and meaning across all ICMP messages. The values in these fields differ among various ICMP message types. A unique part contains fields that are specific to each message type. 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 from 128 to 255 are informational messages. The length of this field is 1 byte. The types are defined as listed in Table A.6.

Type	Name
0	Echo Reply
1	Unassigned
2	Unassigned
3	Destination Unreachable
4	Source Quench
5	Redirect
6	Alternate Host Address

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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	IPv6 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 A.6: ICMP Types

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Code:** This field identifies the message subtype within each ICMP message type value. For each message, the field allows defining up to 256 subtypes. The length of this field is 1 byte. The types are defined as listed in Table A.7.

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 A.7: 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.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

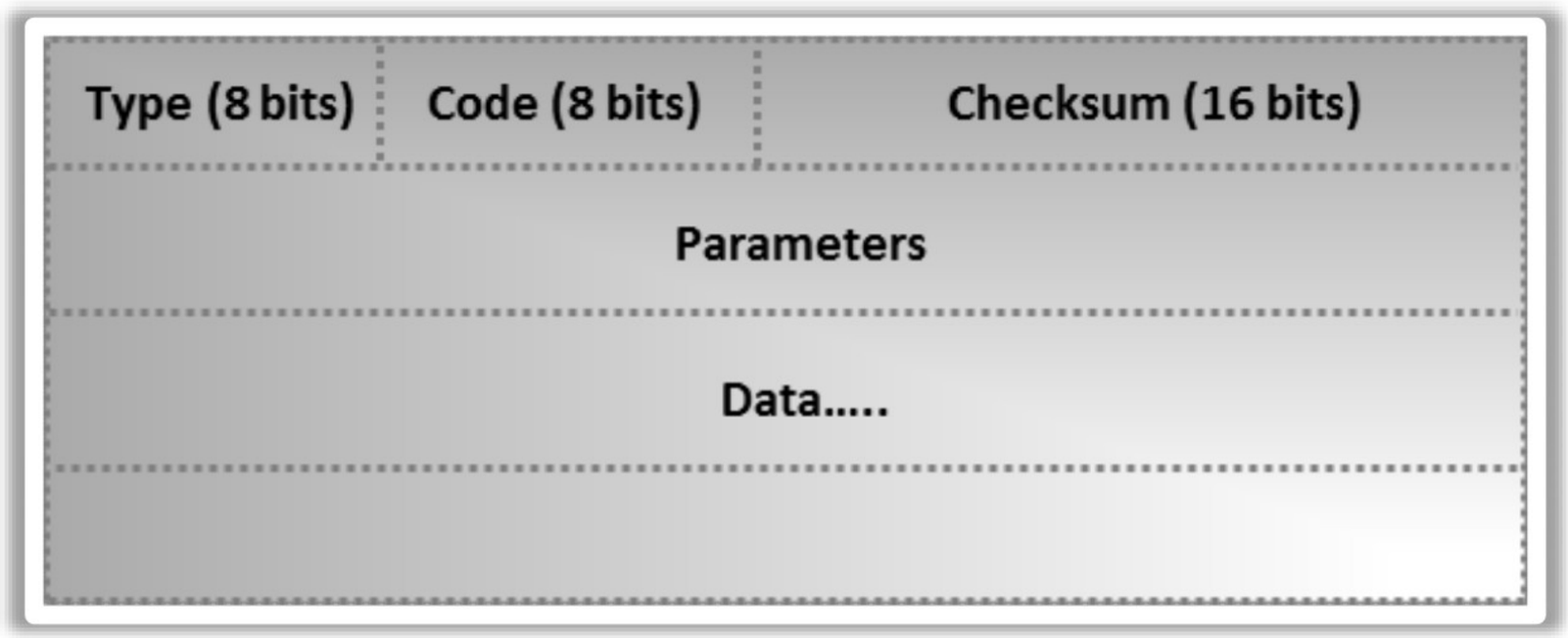
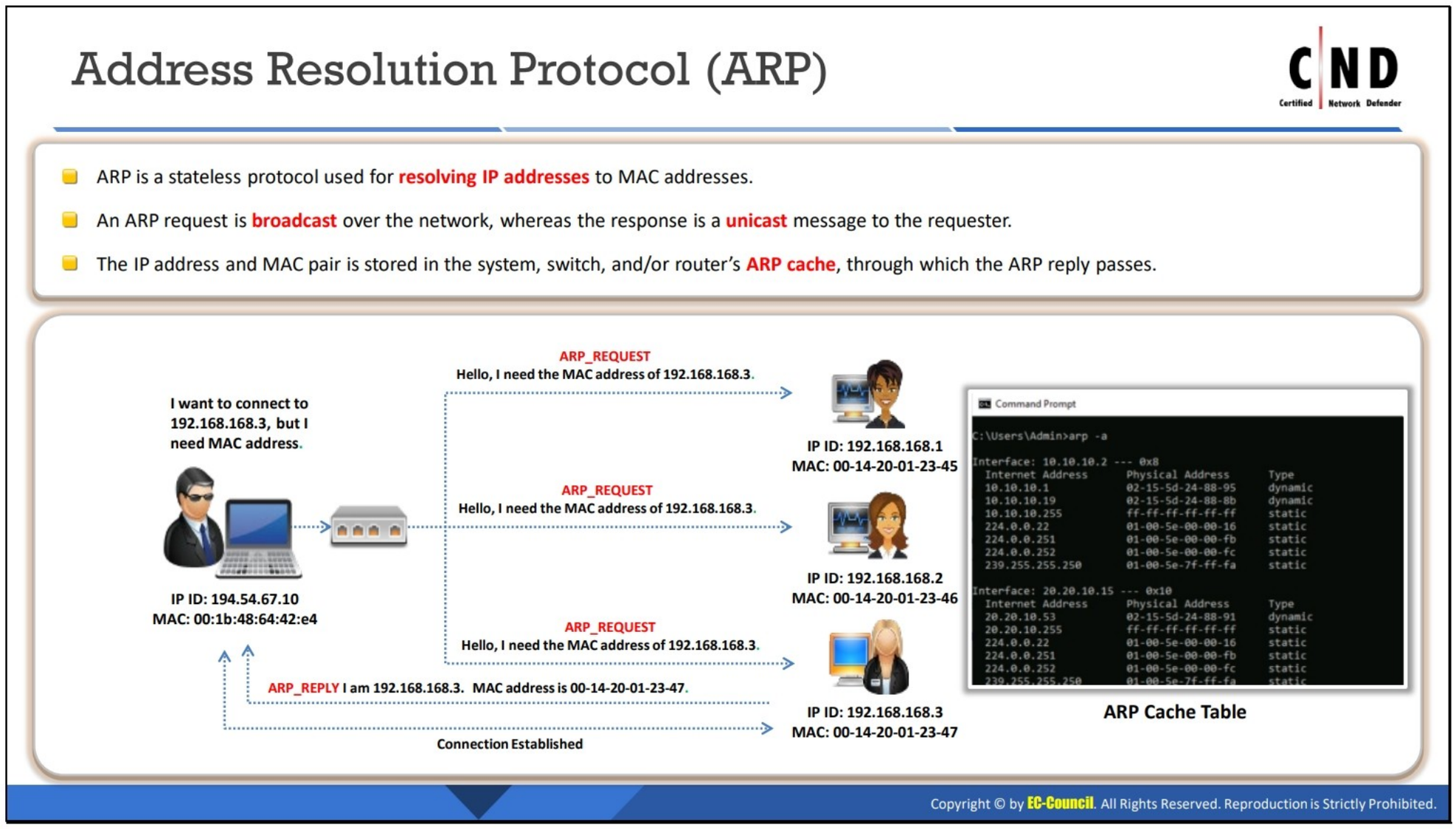


Figure A.71: ICMP Message Format

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Address Resolution Protocol (ARP)

ARP is a stateless protocol used for resolving IP addresses to MAC addresses. The ARP request is broadcast over the network, whereas the response is a unicast message to the requester. The IP and MAC address pair is stored in the system, switch, and/or router's ARP cache, through which the ARP reply passes.

ARP converts the IP address to a physical address (MAC address). The component address resolution refers to the identification of 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.

ARPs are mainly request and reply protocols and are captured by the line protocol. ARP links only within the limits of the boundaries and does not perform any communication across internetwork nodes. ARP maintains a table known as ARP cache that keeps track of MAC addresses and its corresponding IP addresses. However, there are certain rules in maintaining the MAC 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 the physical 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 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 requested.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

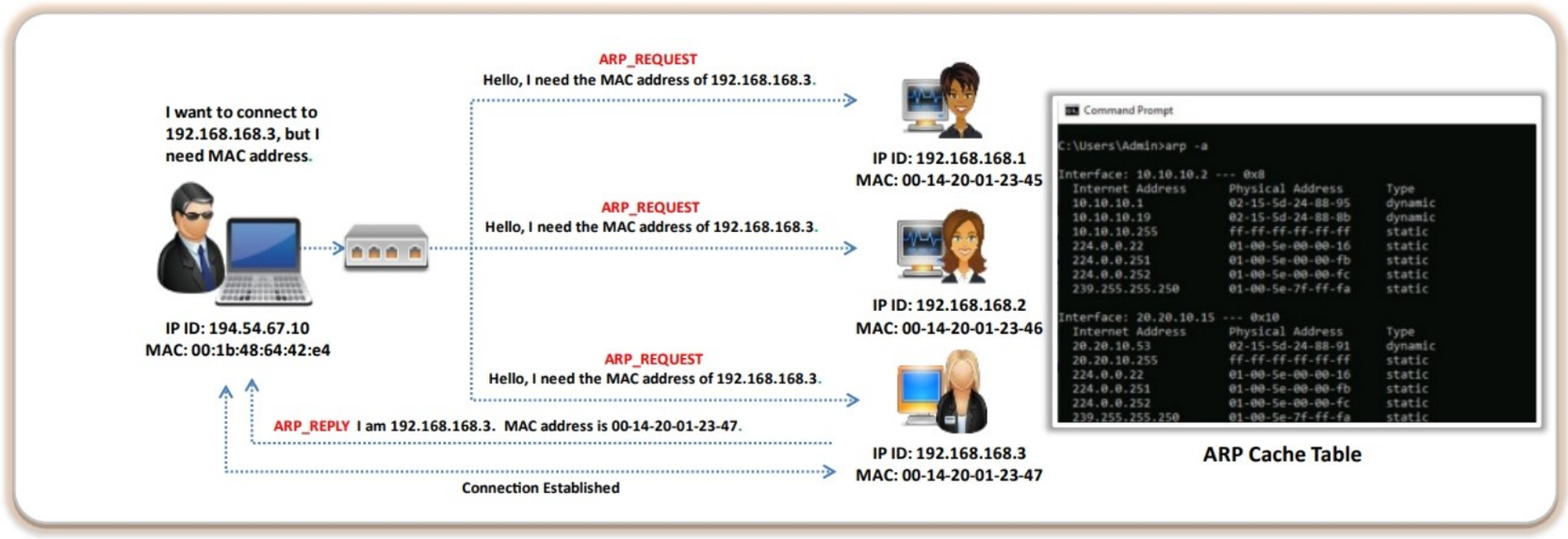


Figure A.72: Working of ARP

ARP Cache Table

The ARP cache table stores matched sets of IP and MAC addresses of systems frequently communicating on the network. Each device on the network manages its own ARP cache table. The following are the two 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 are kept in the cache on a permanent basis. To manage static entries, tools such as the ARP software utility are used.
- **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.

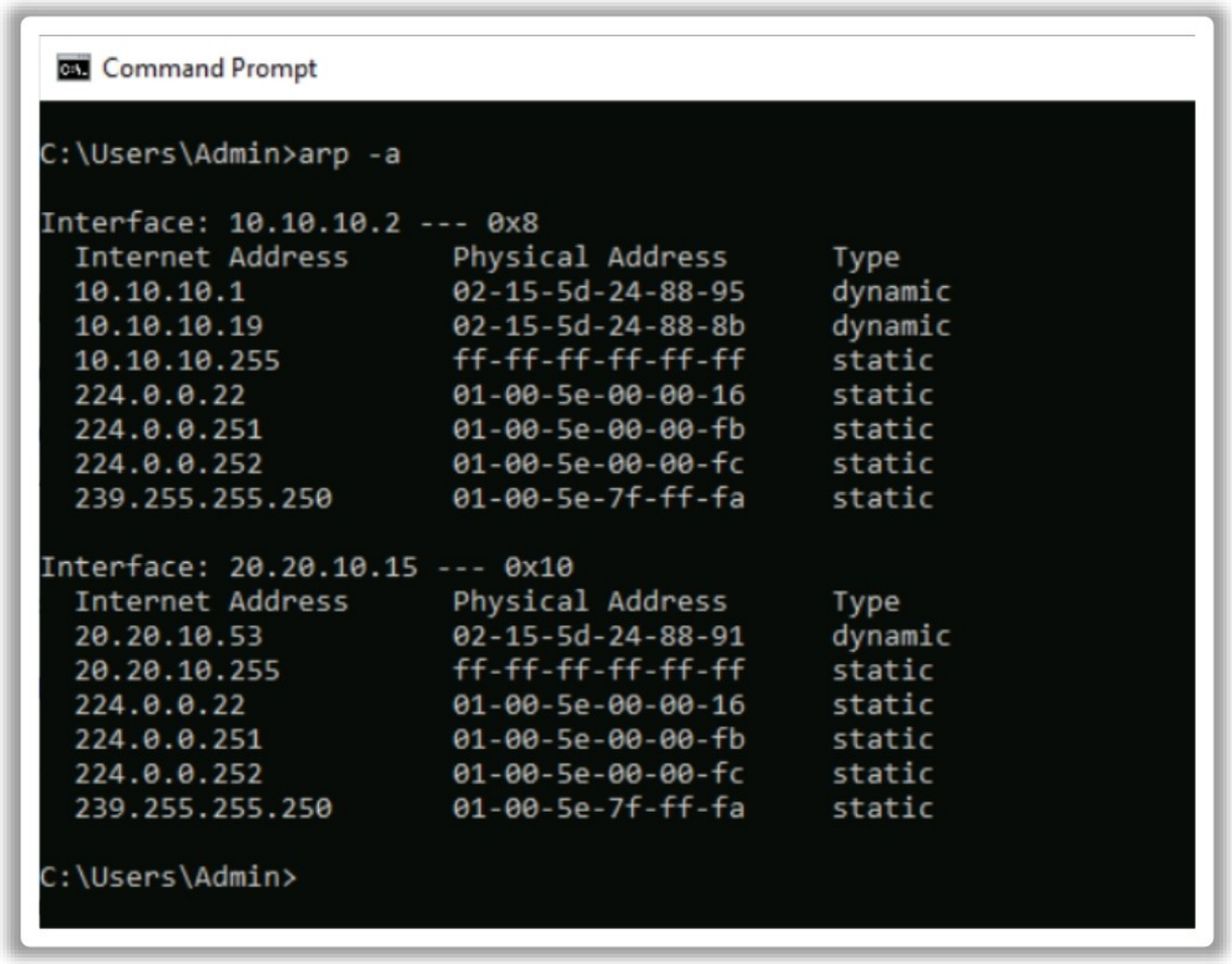
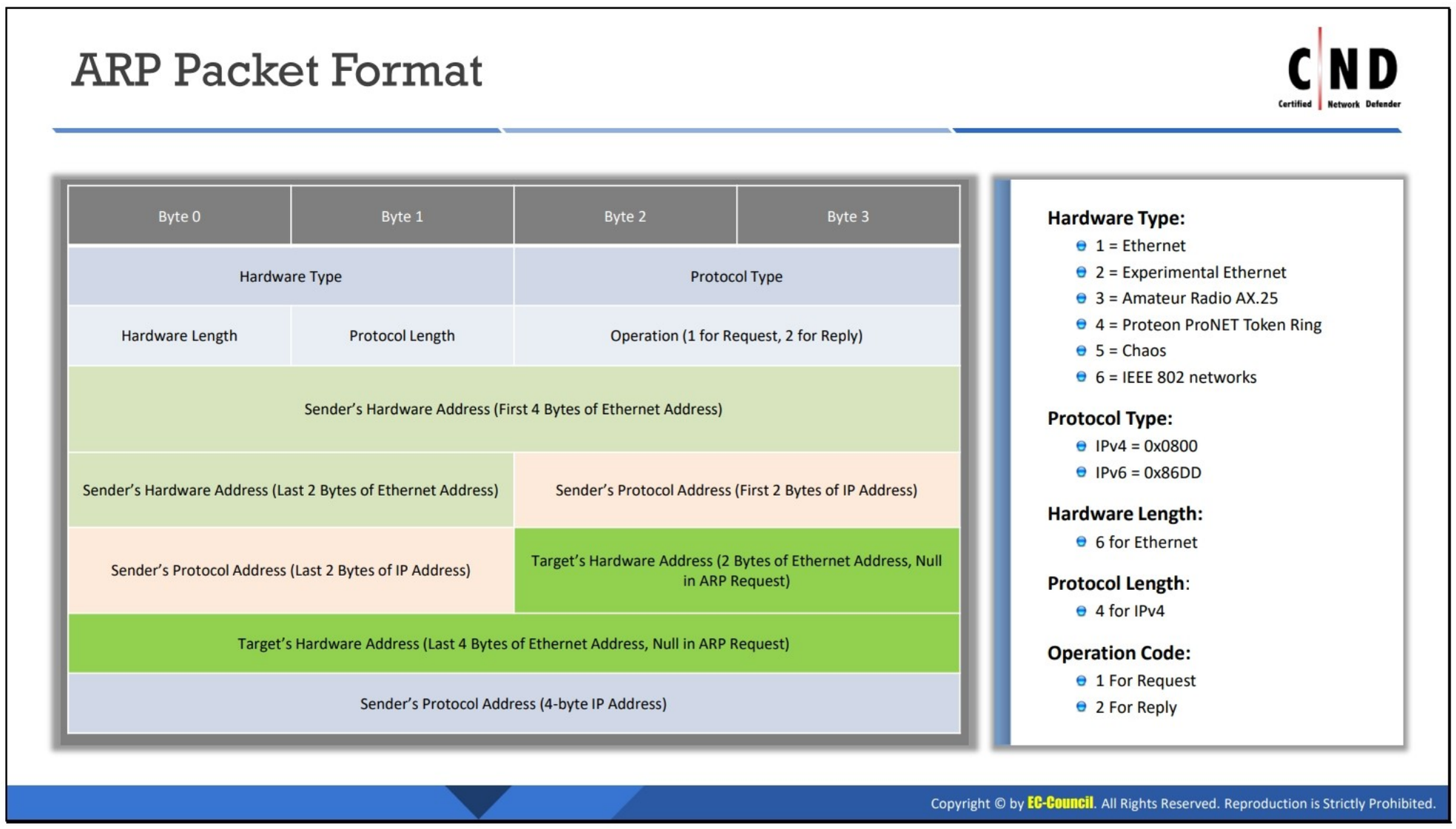


Figure A.73: ARP Table

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ARP Packet Format

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.

  The following are some hardware type values:

  - 1 = Ethernet
  - 2 = Experimental Ethernet
  - 3 = Amateur Radio AX.25
  - 4 = Proteon ProNET Token Ring
  - 5 = Chaos
  - 6 = IEEE 802 networks

- **Protocol type:** This field specifies the network protocol for the intended ARP request. The value of the field for IPv4 is 0x0800 and that for 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.

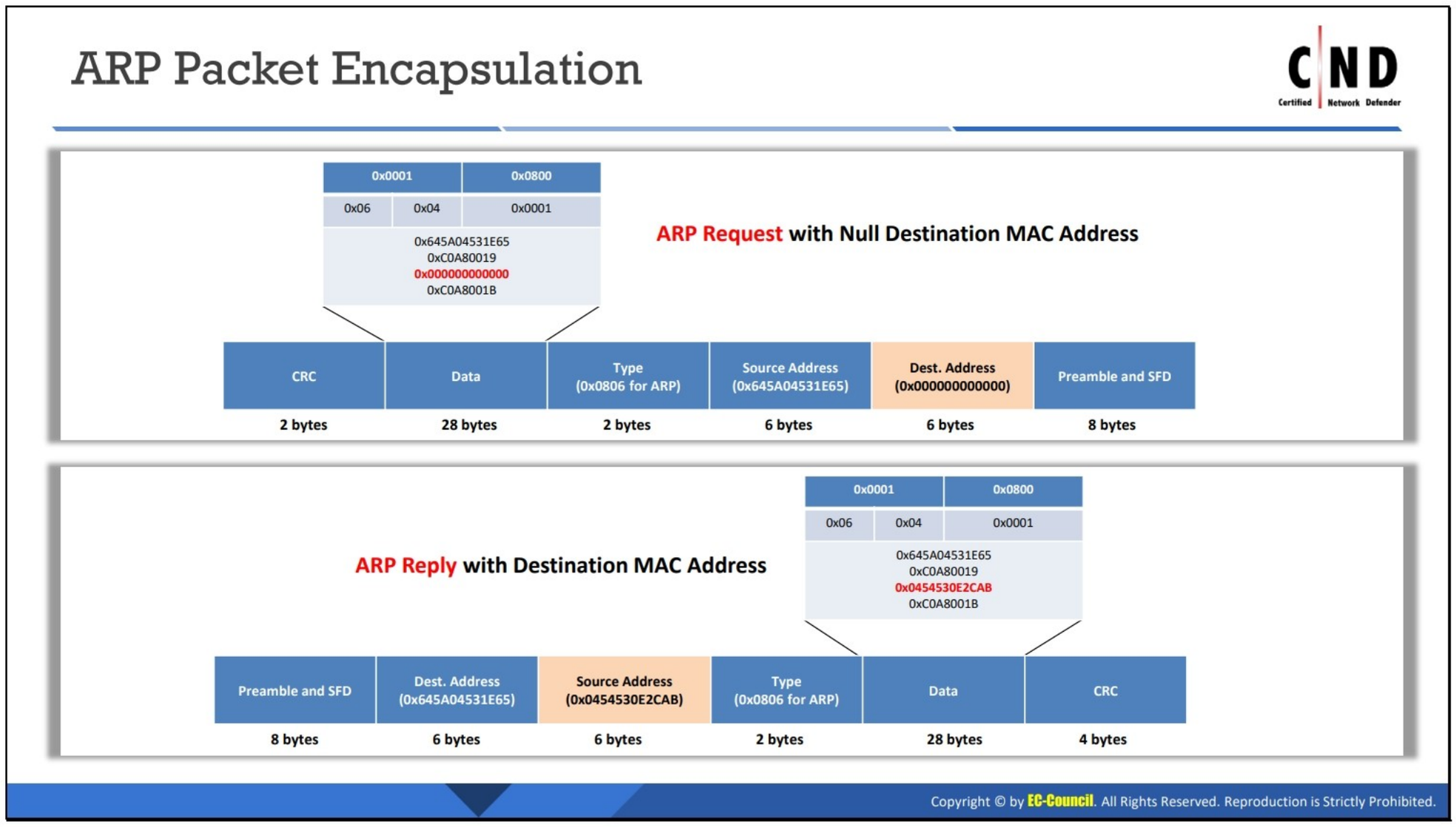
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Operation:** This field specifies the operation that the sender is performing. The value for an ARP request is 1 and that for an 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 the 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 from which the ARP request originated.
- **Target protocol address:** This field contains the IP address of the device of the intended destination.

<table>
<tr><th>Byte 0</th><th>Byte 1</th><th>Byte 2</th><th>Byte 3</th></tr>
<tr><td colspan="2">Hardware Type</td><td colspan="2">Protocol Type</td></tr>
<tr><td>Hardware Length</td><td>Protocol Length</td><td colspan="2">Operation (1 for Request, 2 for Reply)</td></tr>
<tr><td colspan="4">Sender's Hardware Address (First 4 Bytes of Ethernet Address)</td></tr>
<tr><td colspan="2">Sender's Hardware Address (Last 2 Bytes of Ethernet Address)</td><td colspan="2">Sender's Protocol Address (First 2 Bytes of IP Address)</td></tr>
<tr><td colspan="2">Sender's Protocol Address (Last 2 Bytes of IP Address)</td><td colspan="2">Target's Hardware Address (2 Bytes of Ethernet Address, Null in ARP Request)</td></tr>
<tr><td colspan="4">Target's Hardware Address (Last 4 Bytes of Ethernet Address, Null in ARP Request)</td></tr>
<tr><td colspan="4">Sender's Protocol Address (4-byte IP Address)</td></tr>
</table>

Figure A.74: ARP Packet Format

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ARP Packet Encapsulation

An ARP request message is created for multicasting to a network for obtaining the target machines' physical address. Therefore, all the fields of the request message are filled except for the target physical address, and the message is sent to all the devices in the network. At the data-link layer, the message is encapsulated into the Ethernet frame that contains the source and destination addresses (physical address of the source and physical broadcast address). The Ethernet frame with the destination IP address reaches all the routers and hosts in a network. Based on the target IP address, one machine would respond out of all the devices. Then, the target device sends a unicast ARP reply to the source machine with the target physical address. Now, the sender sends the information to the target device.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

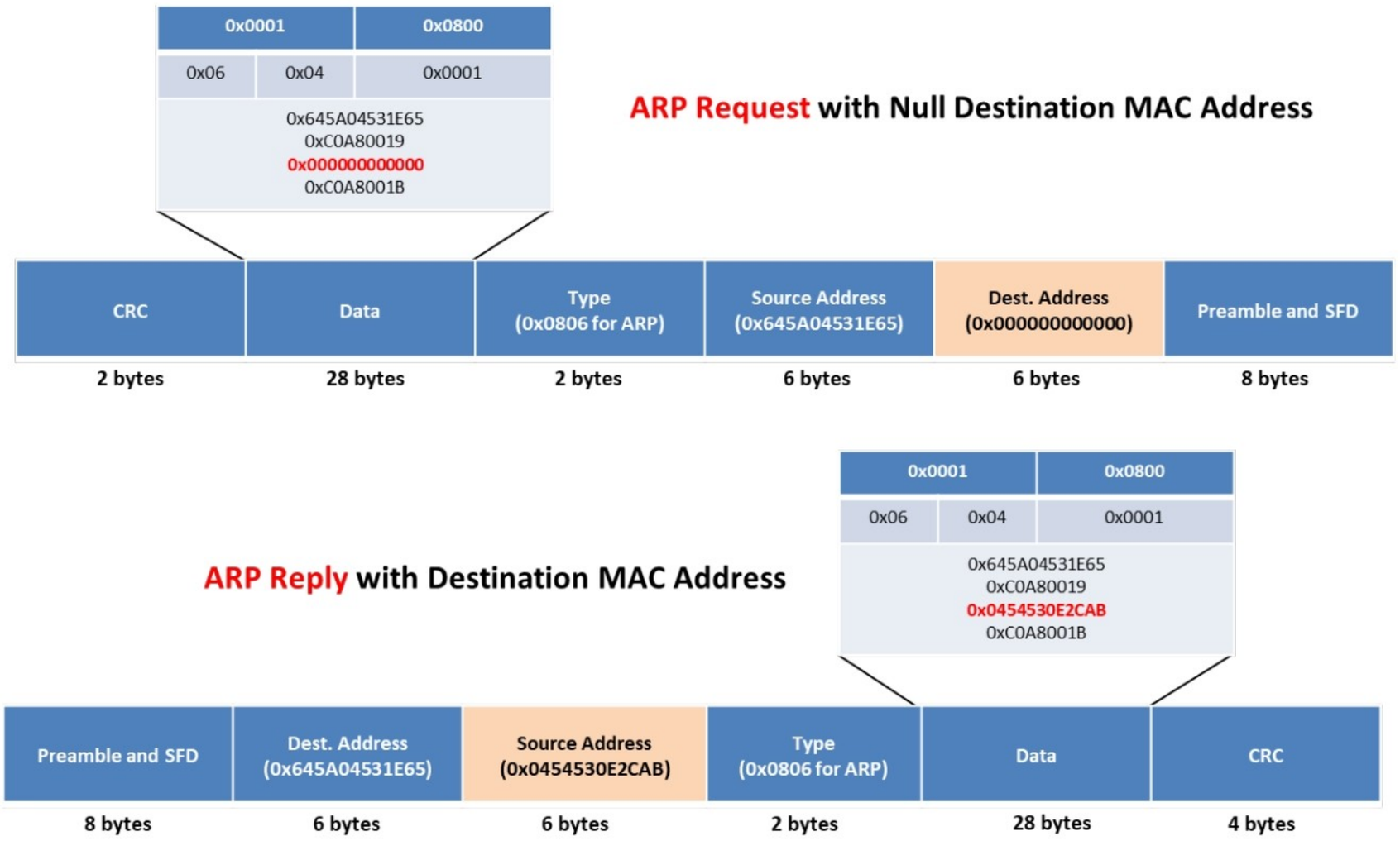
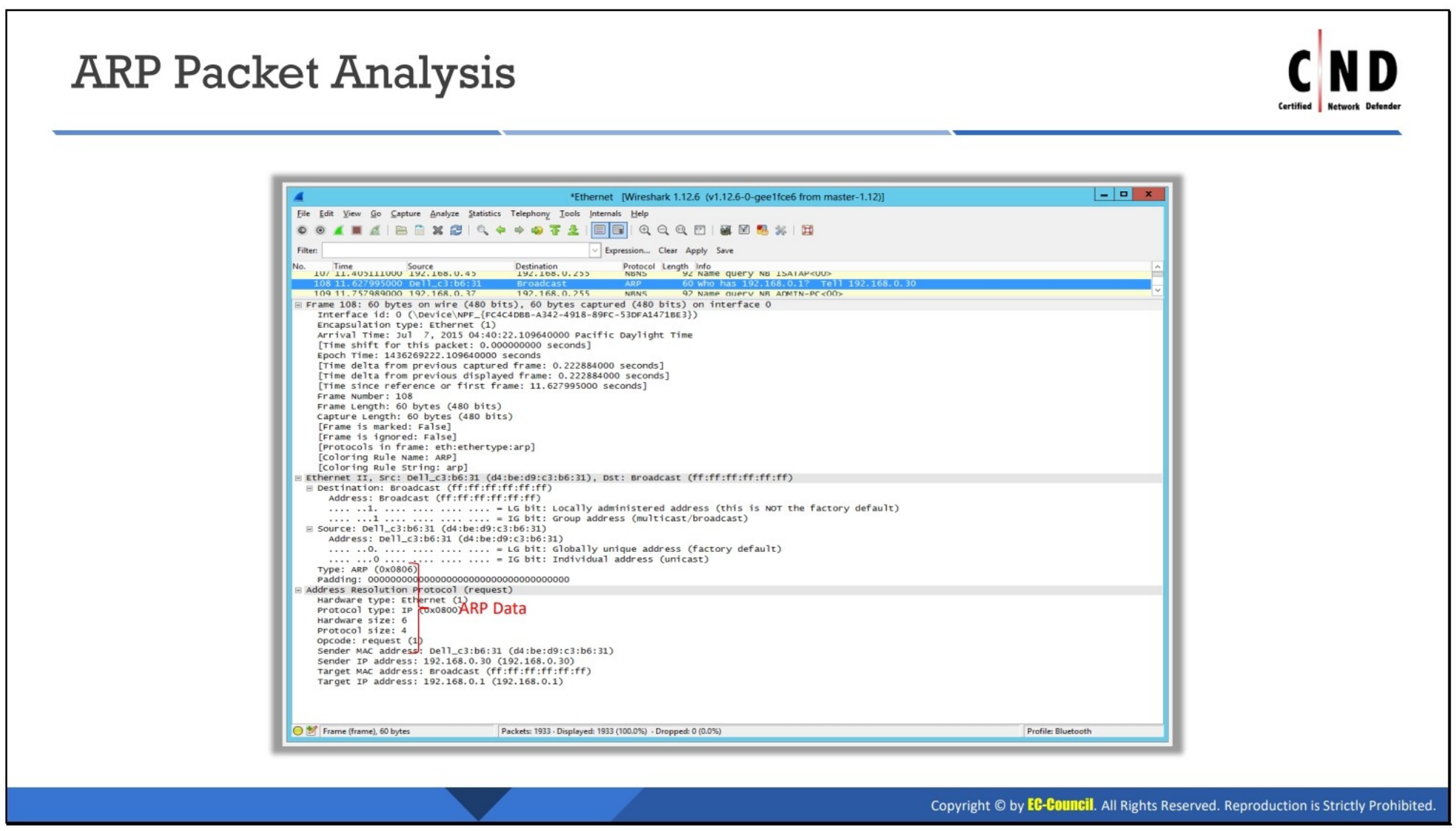


Figure A.75: ARP Packet Encapsulation

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ARP Packet Analysis

The ARP contains an opcode field for determining the information and the type of information addresses at layers 2 and 3. The protocol type is included for supporting all kinds of address lengths. Various types of address combinations such as the sender hardware address, sender protocol address, target hardware address, and target protocol address are included as fields in this packet format.

Figure A.76 shows the ARP packet format.

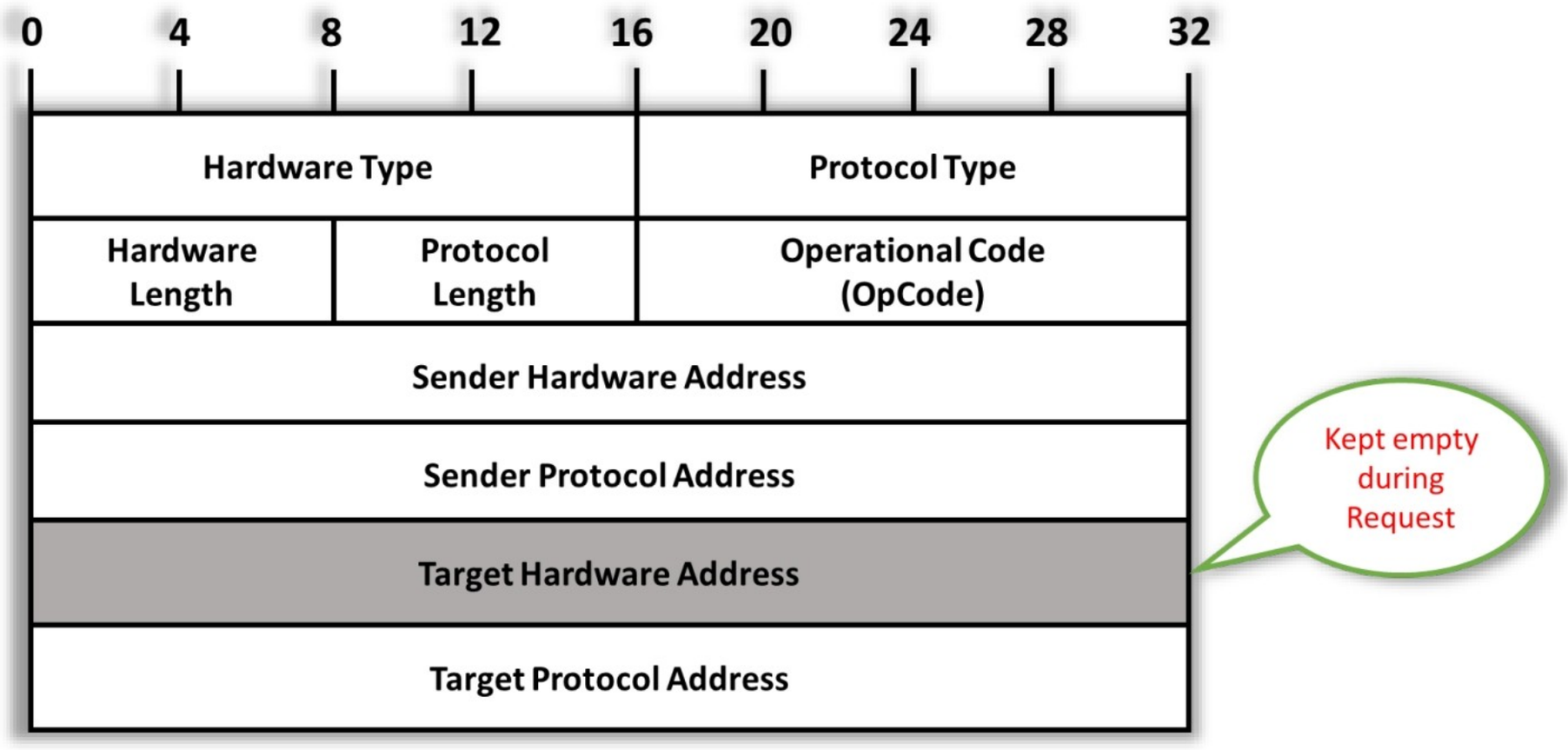


Figure A.76: ARP Packet Format

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are the fields of an ARP packet.

- **Hardware type (2 bytes)**: This field defines the type of hardware network such as Ethernet, on which ARP is running.
- **Protocol type (2 bytes)**: This field defines the type of protocol; for example, the protocol type of IPv4 is 0800_{16}.
- **Hardware length (1 byte)**: This field defines the length of the hardware address (physical address).
- **Protocol length (1 byte)**: This field defines the length of the protocol address (logical address).
- **OP code (2 bytes)**: This field defines the type of packet such as ARP request and ARP reply, for which the value is 1 and 2, respectively.
- **Sender hardware address**: This field defines the hardware address (physical) of the sender, and its length varies.
- **Sender protocol address**: This field defines the protocol address (logical) of the sender, and its length varies.
- **Target hardware address**: This field defines the hardware address (physical) of the target, and its length varies.
- **Target protocol address**: This field defines the protocol address (logical) of the target, and its length varies.

Tables 0.10 and 0.11 list some hardware types and OP codes.

Hardware Type	Value
Reserved	0
Ethernet	1
IEEE 802 Networks	6
ARCneT	7
SMDS	14
HDLC	17
Fiber Channel	18
Asynchronous Transfer Mode	19
Serial Line	20

Table A.8: Values of the Hardware Type field in ARP Packets

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ARP Message Type	Opcode
ARP Request	1
ARP Reply	2
RARP Request	3
RARP Reply	4
DRARP Request	5
DRARP Reply	6
DRARP Error	7
InARP Request	8
InARP Reply	9

Table A.9: Values of the "Opcode" Field in ARP packets

Figure A.77 shows ARP data captured in Wireshark.

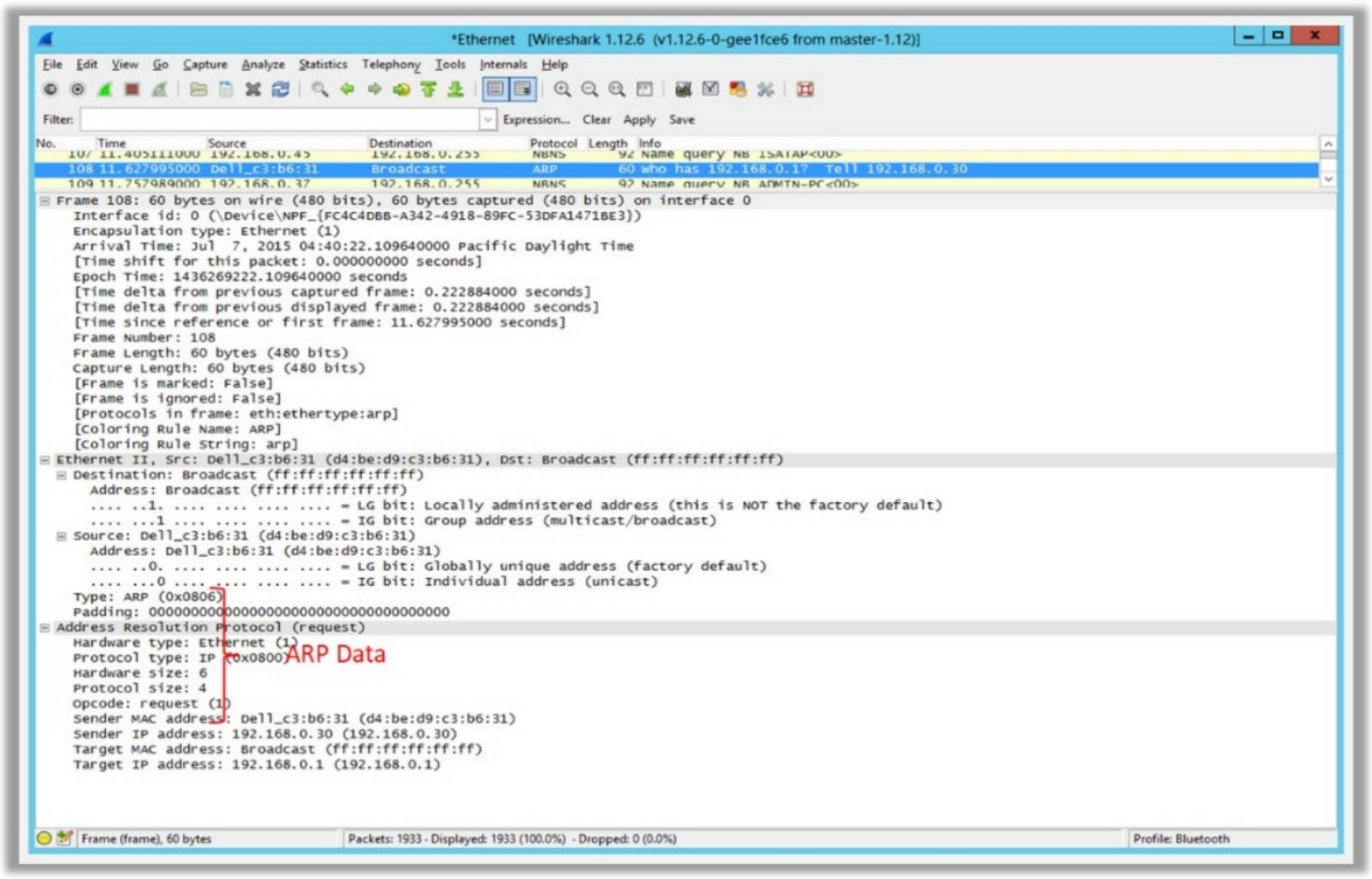
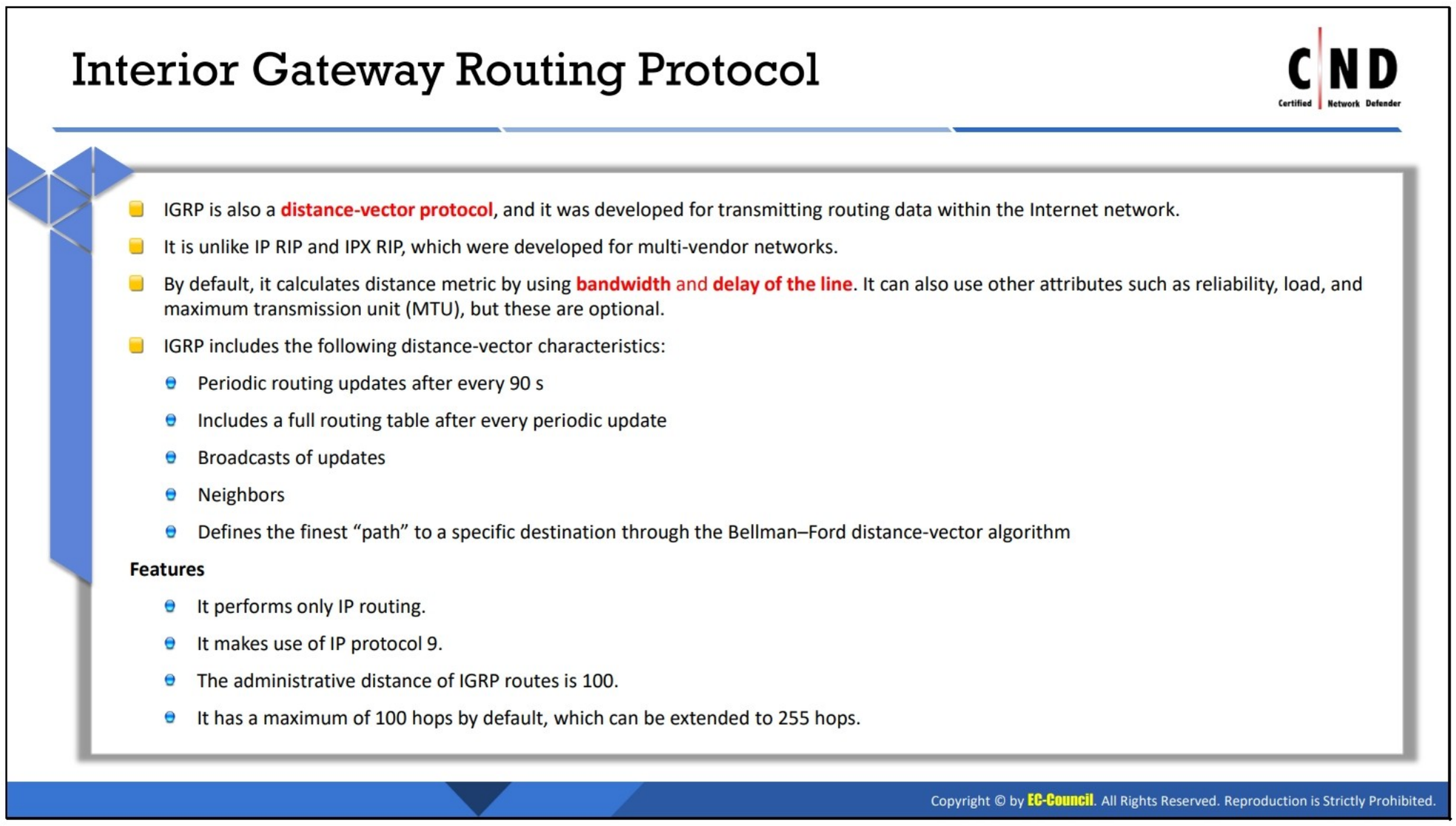


Figure A.77: ARP Data Captured in Wireshark

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Interior Gateway Routing Protocol

IGRP is also a distance-vector protocol, and it was developed for transmitting routing data within the Internet network. It is unlike IP RIP and IPX RIP, which were developed for multi-vendor networks. By default, it calculates the distance metric by using the bandwidth and delay of the line. It can also use other attributes such as reliability, load, and maximum transmission unit (MTU), but these are optional.

IGRP includes the following distance-vector characteristics:

- Periodic routing updates after every 90 s
- Includes a full routing table after every periodic update
- Broadcasts of updates
- Neighbors
- Defines the finest "path" to a specific destination through the Bellman–Ford distance-vector algorithm

Features

- IGRP performs only IP routing.
- It makes use of IP protocol 9.
- The administrative distance of IGRP routes is 100.
- It has a maximum of 100 hops by default, which can be extended to 255 hops.

This protocol contains specifications that define how gateways must coordinate while routing packets. It was developed to maintain packet routing consistently without any issues irrespective

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

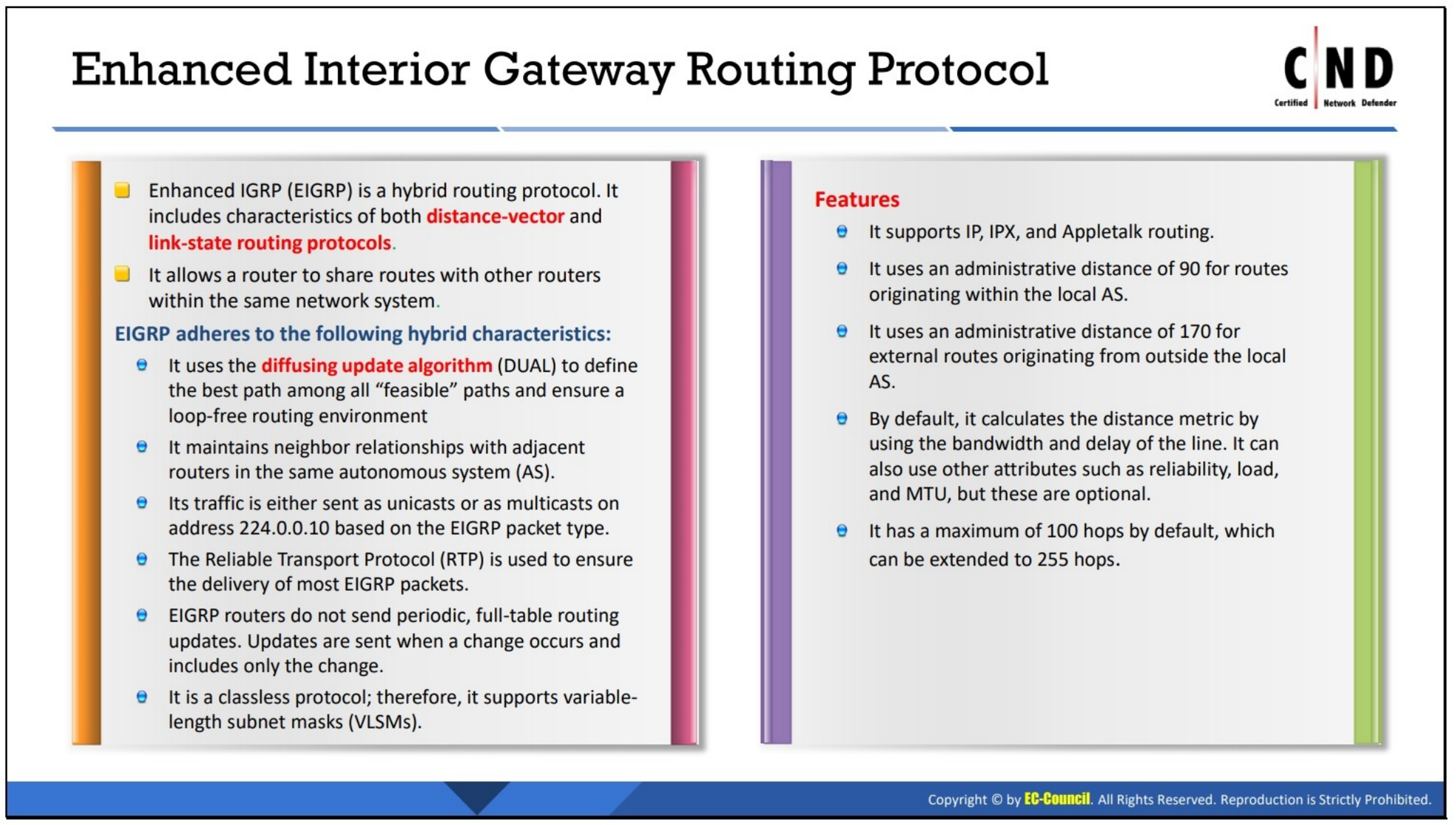
of the network size. Though RIP performs the same task, it is limited to small networks. Whenever networks change their infrastructure, IGRP responds quickly and routes packets accordingly with low bandwidth.

This protocol uses bandwidth and delay as its metrics to measure the routing path of a destination as shown below:

Metric = [K1 * Bandwidth + (K2 * Bandwidth)/(256 - Load) + K3 * Delay] * [K5/(Reliability + K4)].

For the above formula, K1 = K3 = 1, and K2 = K4 = K5 = 0.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enhanced Interior Gateway Routing Protocol (EIGRP)

Enhanced IGRP (EIGRP) is a hybrid routing protocol. It includes characteristics of both distance-vector and link-state routing protocols and allows a router to share routes with other routers within the same network system. EIGRP is an enhanced version of IGRP that allows routers to exchange information in a more advanced way compared to the other routing protocols. Both IGRP and EIGRP are inter-related in such a manner that all the routers that run under these protocols can exchange information with each other. If a router in a network functions using EIGRP and if it has no information on a packet's destination in its routing table, it requests another router to find the path; if the other router couldn't find the path, it asks some other neighbors. This process continues until a path for the destination system is found in the network. The routers exchange the latest changes made to their routing tables to other routers, and they update their tables. All the routers in a network should be active and periodically exchange their information with other routers. To be active and to know the status of the network, the routers exchange "Hello" messages with their neighbors. If any router is found to be inactive or not sending "Hello" messages, then the other routers treat the router as either down or dead.

EIGRP adheres to the following hybrid characteristics:

- It uses the diffusing update algorithm (DUAL) to define the best path among all "feasible" paths and ensure a loop-free routing environment.
- It maintains neighbor relationships with adjacent routers in the same autonomous system (AS).
- Its traffic is either sent as unicasts or as multicasts on address 224.0.0.10 based on the EIGRP packet type.

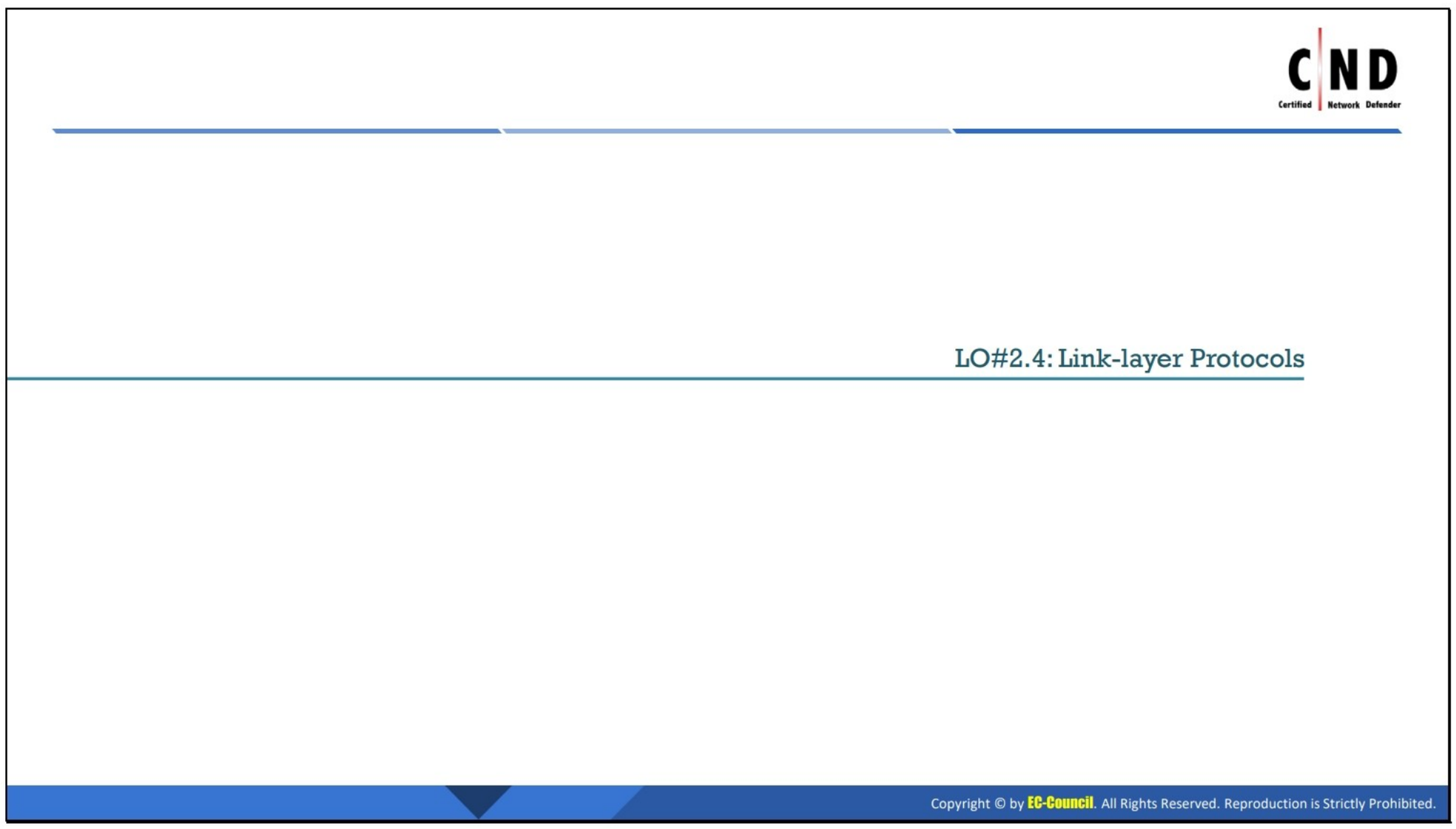
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The Reliable Transport Protocol (RTP) is used to ensure the delivery of most EIGRP packets.
- EIGRP routers do not send periodic, full-table routing updates. Updates are sent when a change occurs and includes only the change.
- It is a classless protocol; therefore, it supports variable-length subnet masks (VLSMs).

Features

- It supports IP, IPX, and Appletalk routing.
- It uses an administrative distance of 90 for routes originating within the local AS.
- It uses an administrative distance of 170 for external routes originating from outside the local AS.
- By default, it calculates the distance metric by using the bandwidth and delay of the line. It can also use other attributes such as reliability, load, and MTU, but these are optional.
- It has a maximum of 100 hops by default, which can be extended to 255 hops.

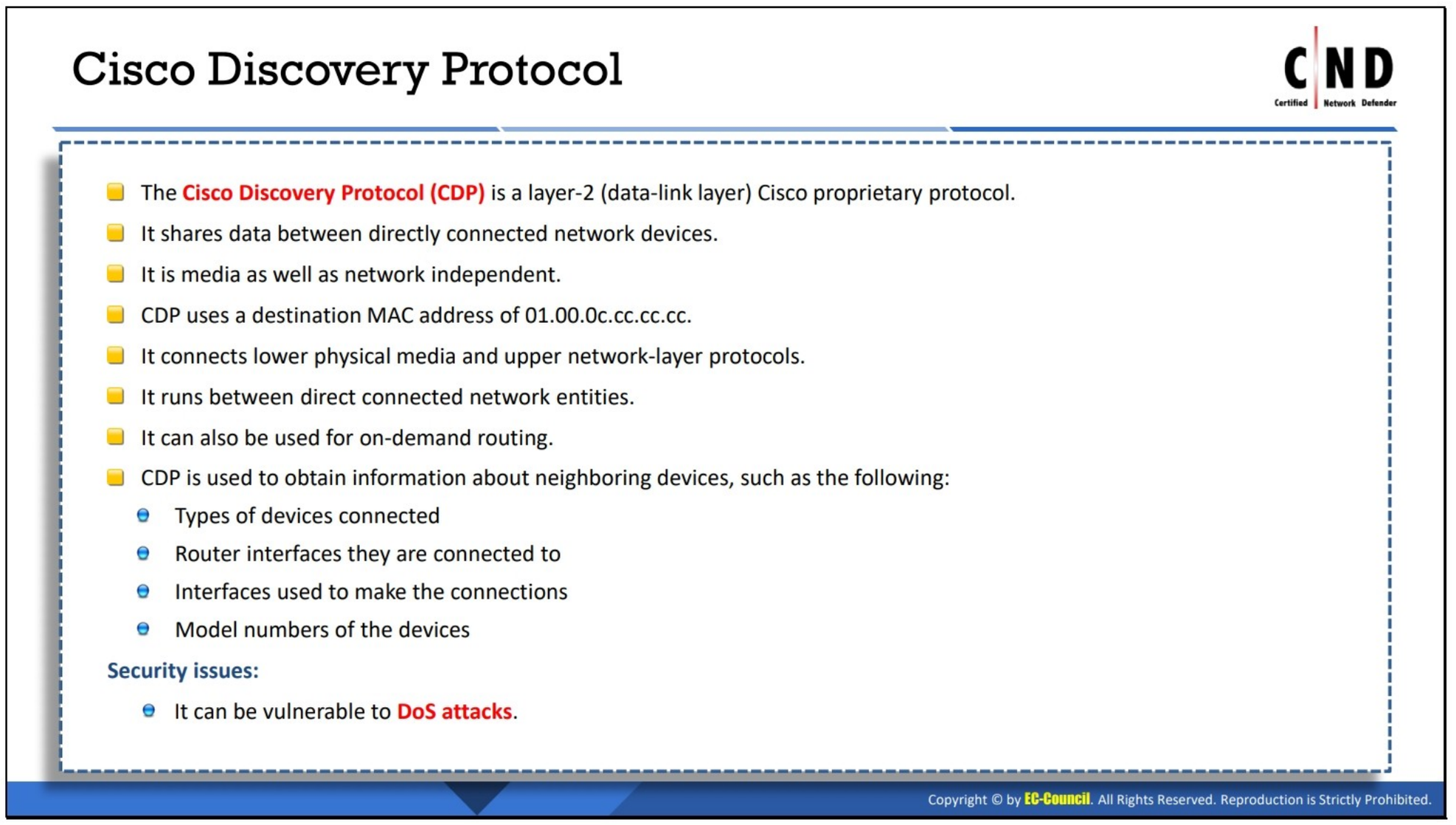
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#2.4: Link-Layer Protocols

This section discusses the link-layer protocols such as FDDI, Temporal Key Integrity Protocol (TKIP), Extensible Authentication Protocol (EAP), Cisco Discovery Protocol (CDP), Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), Virtual LAN (VLAN) Trunking Protocol (VTP), and Spanning Tree Protocol (STP).

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cisco Discovery Protocol

CDP is a layer-2 (data-link layer) Cisco proprietary protocol that shares data between directly connected network devices. This protocol is used for network monitoring and troubleshooting by obtaining information about devices (Cisco devices) such as their status and configuration details, enabling the management of these devices. Cisco devices in a network can send messages to other directly connected devices in the network; these messages are called CDP advertisements. In brief, all Cisco-based networks use CDP as their medium for communication.

CDP is used to obtain information about neighboring devices, such as the following:

- Types of devices connected
- Router interfaces they are connected to
- Interfaces used to make the connections
- Model numbers of the devices

CDP Functioning

As a data-link layer in the OSI model, CDP allows Cisco networking devices to be aware of each other and communicate by exchanging hardware and software information. It is media as well as network independent. CDP uses a destination MAC address of 01.00.0c.cc.cc.cc. Cisco devices multicast their identity by sending CDP messages using 01.00.0c.cc.cc.cc on each network interface. It connects lower physical media and upper network layer protocols. Further, it runs between directly connected network entities. It can also be used for on-demand routing.

Devices that do not support CDP reject CDP messages, and only those that can understand CDP messages (Cisco devices) respond to multicast CDP messages. A table called the CDP table contains information about all the Cisco devices in the network, and every device must update

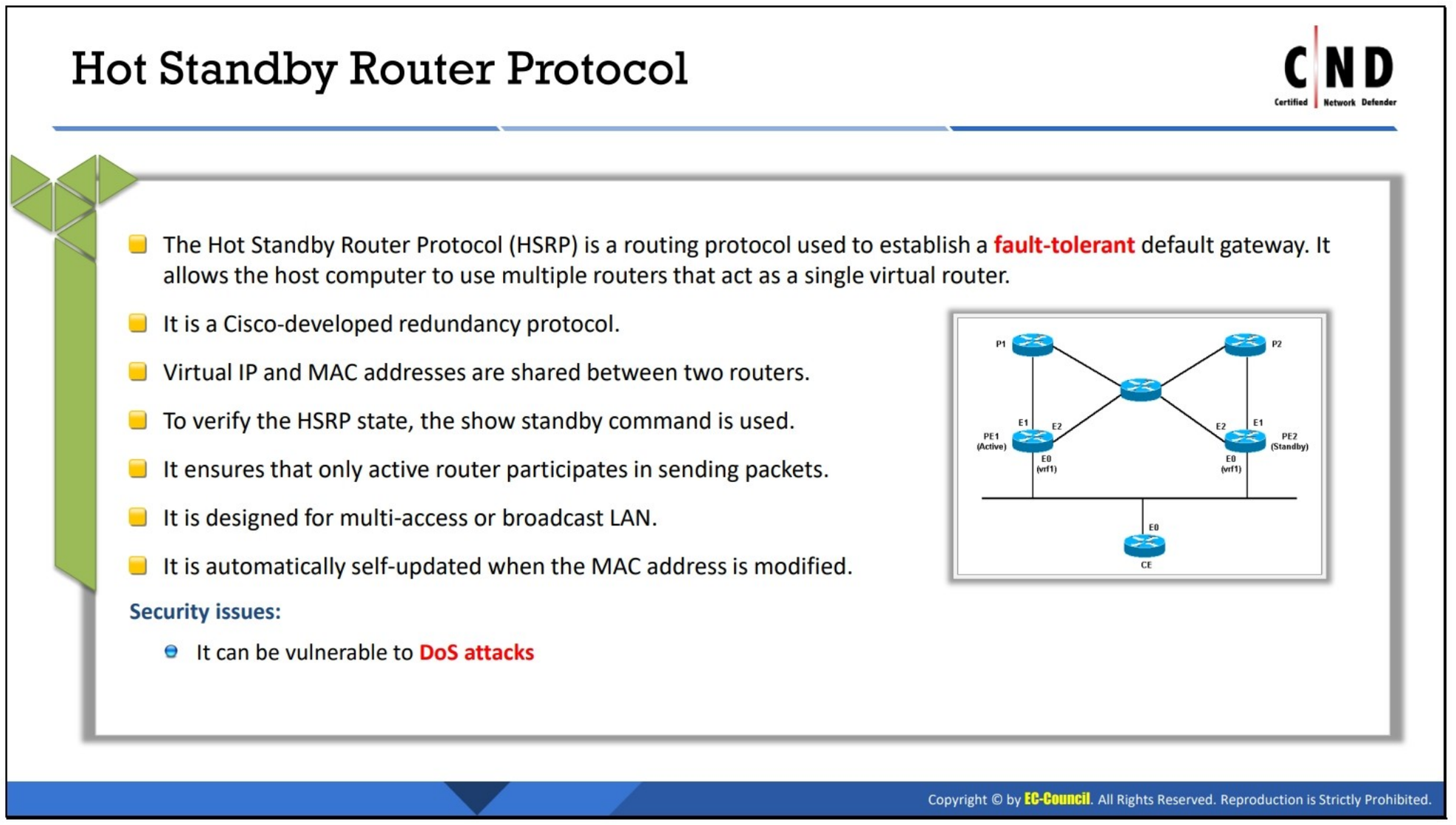
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

their information by sending a CDP message every 180 s. After receiving this message, the CDP table is updated. If no update is received from any device, the information in the table on that device is discarded.

CDP Security Issues

As CDP contains information about devices, there is a possibility for a security attack to obtain this information. The attacker can use this information and attempt to exploit the network using a DoS attack. The attacker can utilize the accessibility of Cisco devices that are connected directly and send fake CDP messages to those devices. Consequently, the attacker could obtain information about those devices and use this information to perform further attacks.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hot Standby Router Protocol

HSRP is a routing protocol used to establish a fault-tolerant default gateway. It allows the host computer to use multiple routers that act as a single virtual router. It is a Cisco-developed redundancy protocol in which virtual IP and MAC address are shared between two routers. The show standby command is used to verify the HSRP state. It ensures that only the active router participates in packet transmission. It is designed for multi-access or broadcast LAN. Further, it is automatically self-updated when the MAC address is modified.

Organizations such as e-commerce sites need their host to function continuously to provide services to customers. The host that maintains the e-commerce domain must be available for the users all the time without delay; otherwise, the organization's customer satisfaction will be negatively impacted. To overcome this issue and to keep the host running all the time, HSRP was developed. The protocol defines specifications for maintaining a set of routers as a single virtual router for a host to run without any delay if one router is down. Although, the virtual router is designed with many routers, only one router can forward and receive data packets from and to the host. Based on the IP addresses of the routers, one router is chosen as the active one, and all the others become inactive. Whenever an active router fails or shuts down, then the router with next-highest priority becomes active. The major security issue with HSRP is that it can be vulnerable to DoS attacks.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

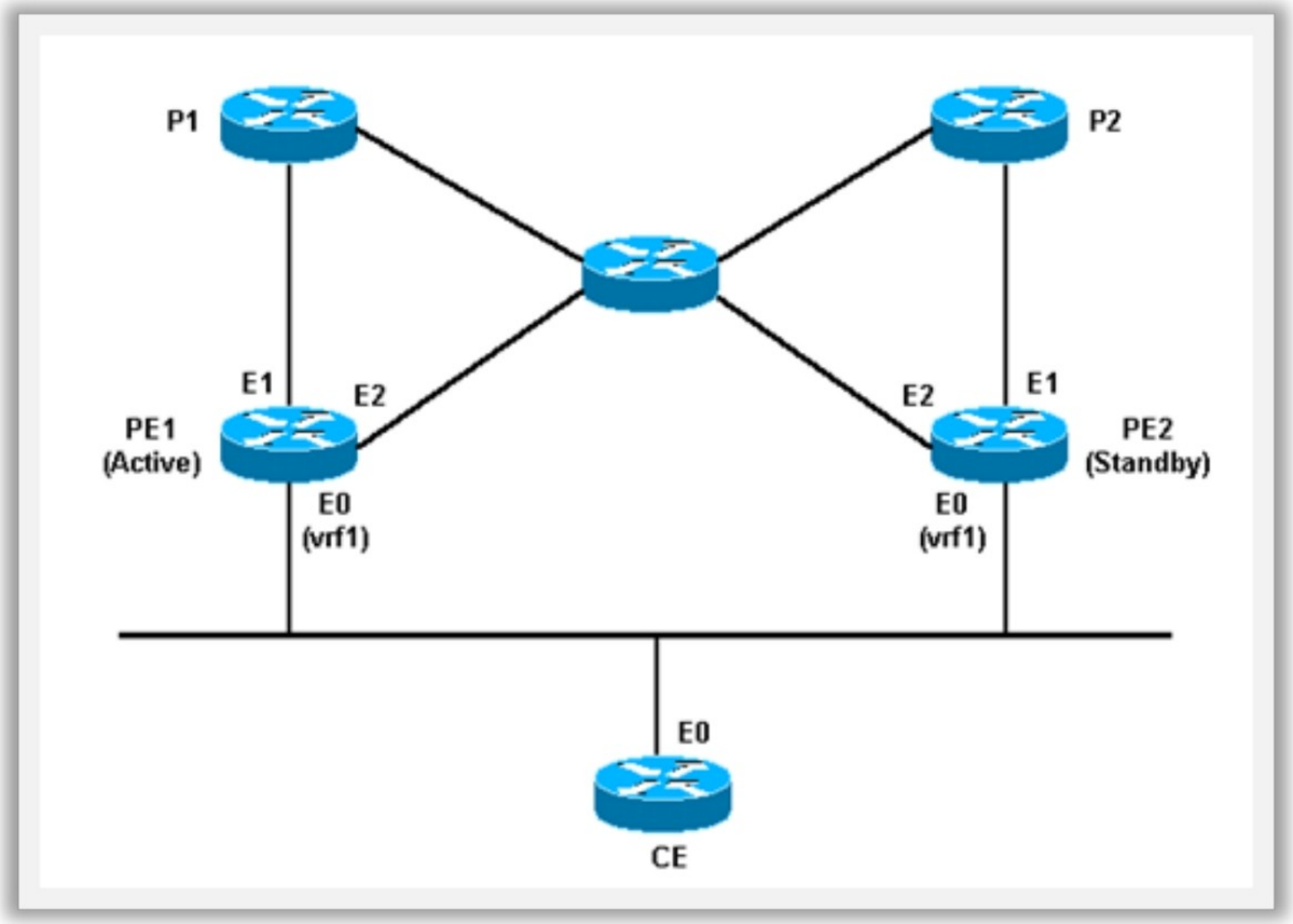
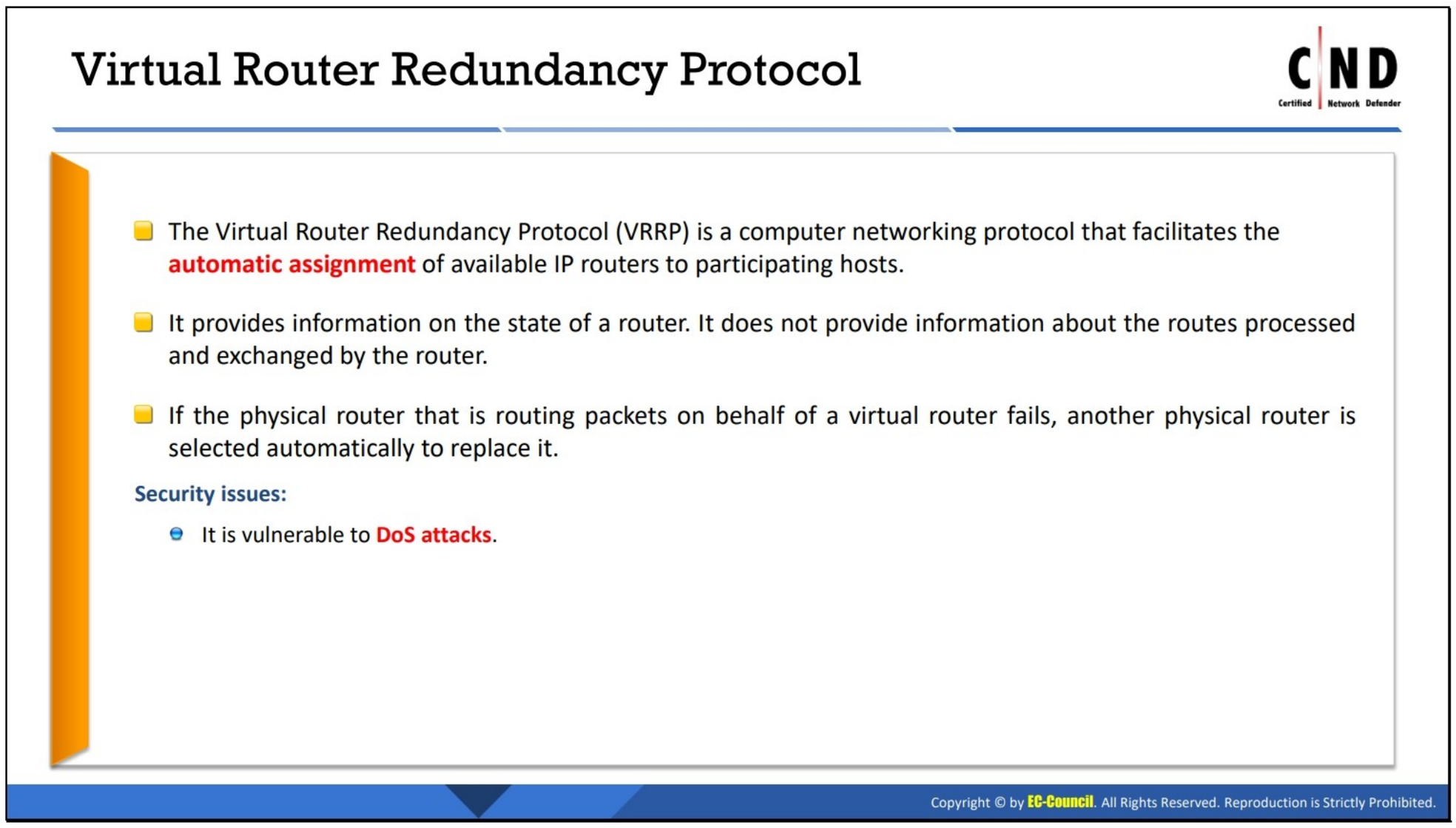


Figure A.78: Working of the Hot Standby Router Protocol

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Virtual Router Redundancy Protocol

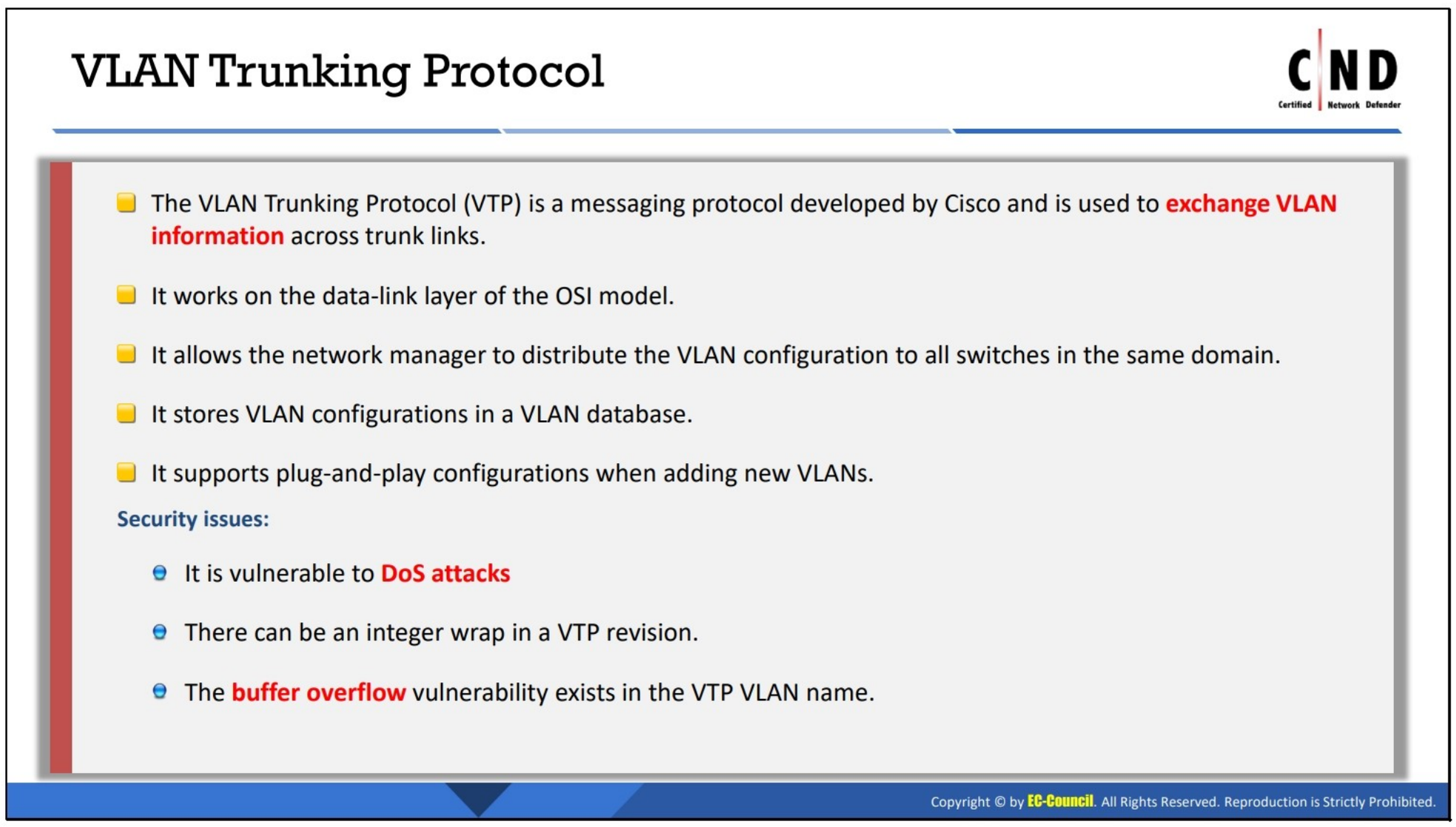
VRRP is a computer networking protocol that facilitates the automatic assignment of the available IP routers to participating hosts. It provides information on the state of a router. However, it does not provide information about routes processed and exchanged by the router. If the physical router that is routing packets on behalf of a virtual router fails, this protocol automatically selects another physical router to replace it.

This protocol provides the means for a backup routing mechanism in which a backup router is provided to a LAN when the main router has not been functioning for a while. For this purpose, all routers are provided with an IP address called a virtual IP address, and one of the routers is treated as the master and is used for forwarding packets; the remaining routers are treated as backup routers.

Routers are selected and then assigned priorities; the router with the highest priority is selected as the master, and the router with the next-highest priority will be the master in case the current master router fails. To maintain co-ordination among all the routers, the master router takes the initiative and sends messages called advertisements to all the backup routers to intimate the present condition every second. If the backup routers fail to receive the advertisement from the master, then the router with the second-highest priority would start acting as the master.

To avoid security attacks on VRRP infrastructure, the protocol contains authentication mechanisms such as plaintext authentication and MD5 authentication. However, it is vulnerable to DoS attacks.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



VLAN Trunking Protocol

VTP allows all the VLANs in a network to share their configuration details with other VLANS in the network. To share this information among the VLANs in a network, trunks are used between VLANs, switches, and routers for connections with each other. The complexities of configuring all the VLANs and VLAN trunking increase with the increase of the network size. Therefore, maintaining all of this connectivity and ensuring smooth operation are difficult for network administrators. To avoid such complexity, Cisco developed VTP. By using this protocol, all the operations on VLANs can be performed at one place, and this facility makes the administrators' work much easier.

VTP Operation

When a new VLAN is installed in a network that contains other VLANs and switches, VTP advertises about this new VLAN to all the switches in the network and allows them to update their configurations.

VTP Modes

There are three modes in VTP:

- Server mode
- Client mode
- Transparent mode

Security Issues with VTP

There are many security issues related to VTP, and the following are some of them:

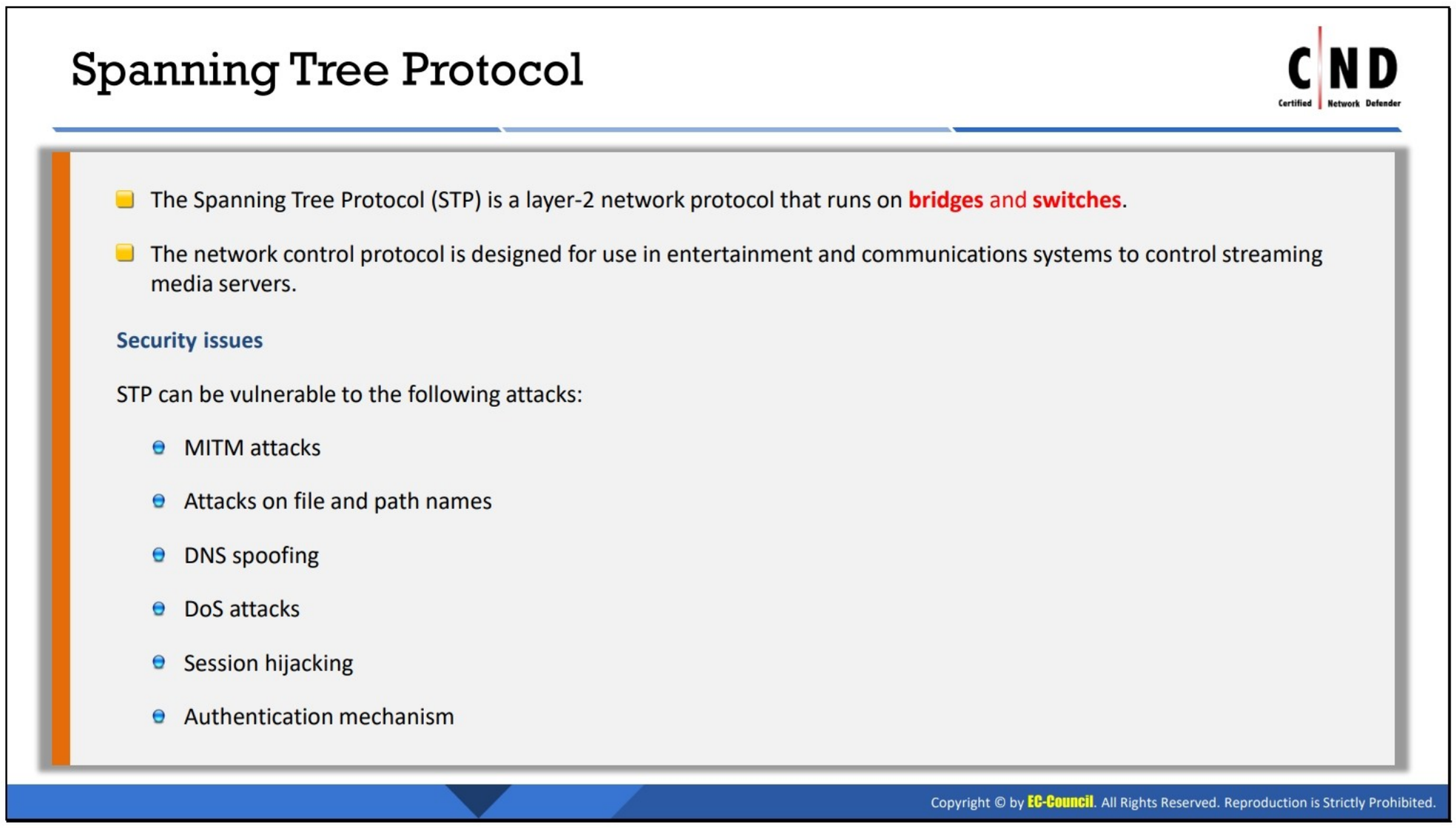
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

MAC attacks: The Content Addressable Memory (CAM) table is a repository for storing information about MAC addresses and their respective VLAN details. Attackers attempt to compromise the CAM table by performing a buffer overflow attack. As the CAM table contains limited entries, it becomes overloaded, allowing no further MAC address to be stored.

VLAN hopping attacks: In this attack, the attacker attempts to introduce themselves as a router that wishes to connect to the trunk. If any of the routers in the network believes the attacker router and grants access, then the attacker gains access to all the VLAN traffic.

Apart from these attacks, there a few more attacks that could compromise VTP such as ARP attacks, double-encapsulation VLAN hopping attacks, VLAN query protocol attacks, and CDP attacks.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Spanning Tree Protocol

STP is a layer-2 network protocol that runs on bridges and switches. The network control protocol is designed for use in entertainment and communications systems to control streaming media servers. The protocol defines specifications that help avoid looping between endpoints when the network is interconnected with switches or bridges. For example, if a network is formed with two or more computers and two switches connected between them, then the messages that are forwarded between the computers are handled by both the switches, causing loops through which messages travel in that network. To avoid this drawback, STP allows only one switch to function.

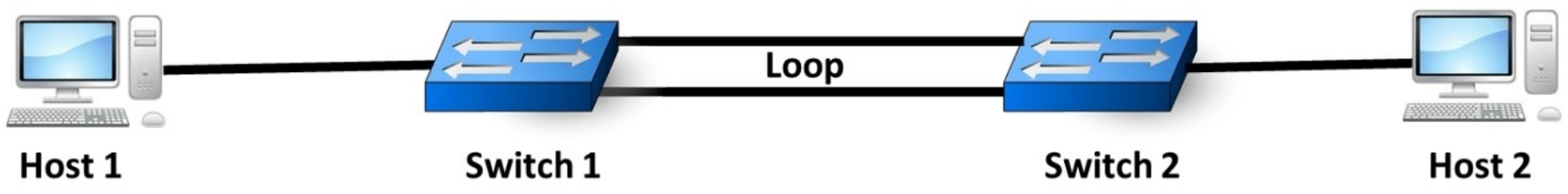


Figure A.79: Network without STP

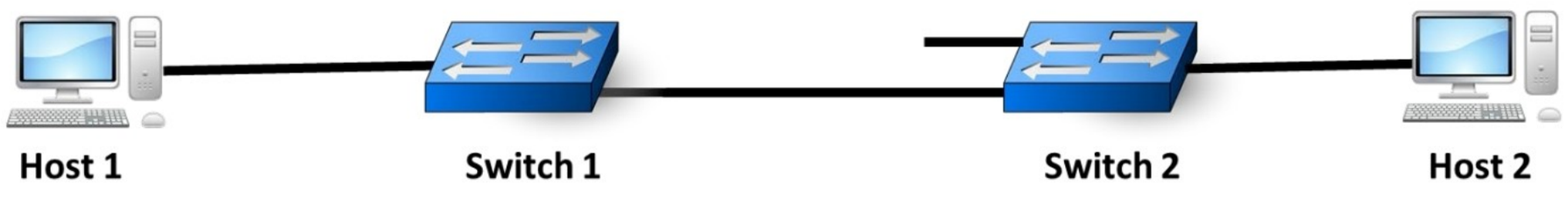


Figure A.80: Network with STP

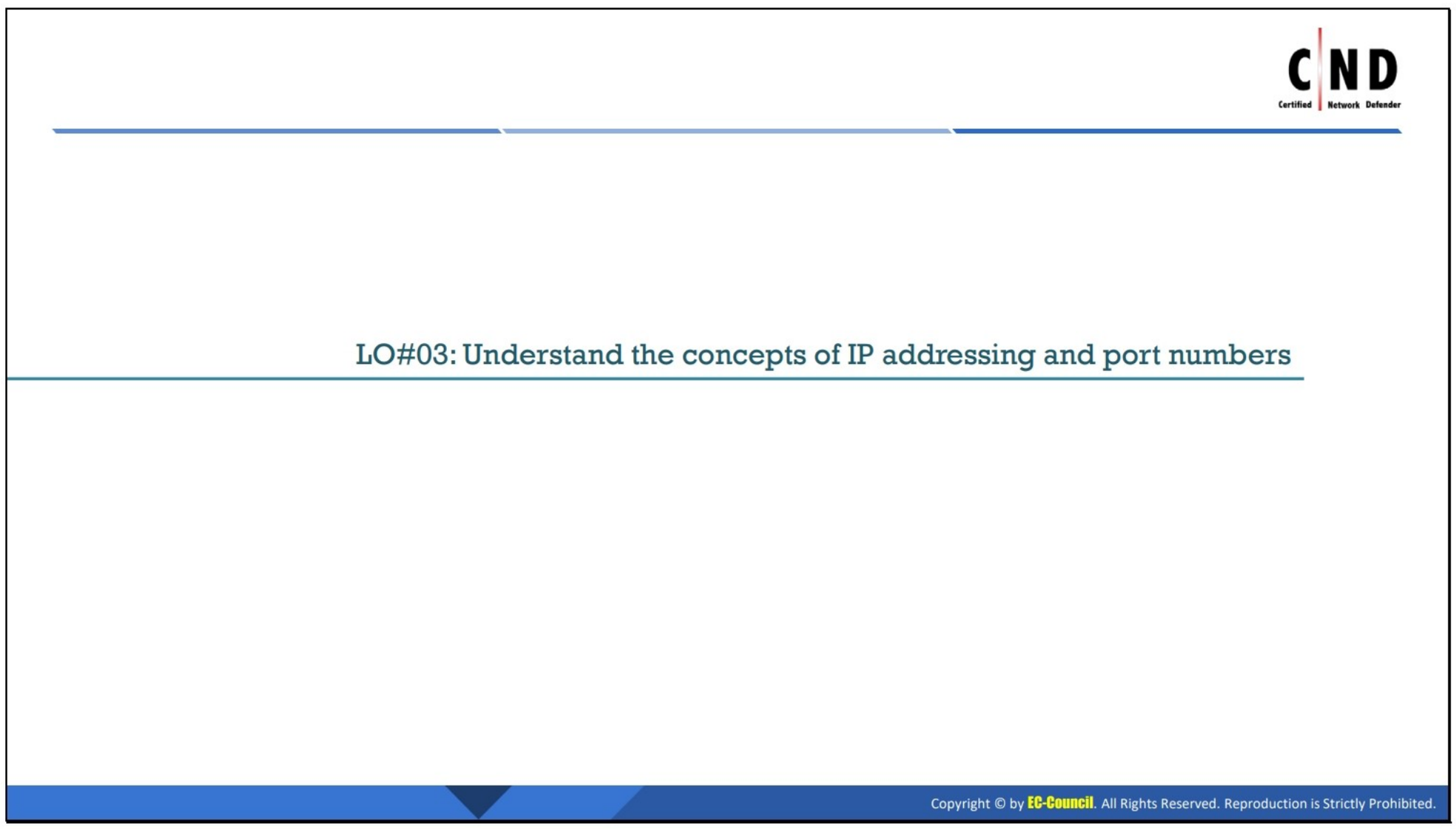
STP uses the bridge IDs of the switches, which are a combination of the bridge priority and MAC address. If the priority of the switches is the default (32,768), then the switch with the lowest MAC address is used for forwarding packets.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

STP can be vulnerable to the following attacks:

- MITM attacks
- Attacks on file and path names
- DNS spoofing
- DoS attacks
- Session hijacking
- Authentication mechanism attacks

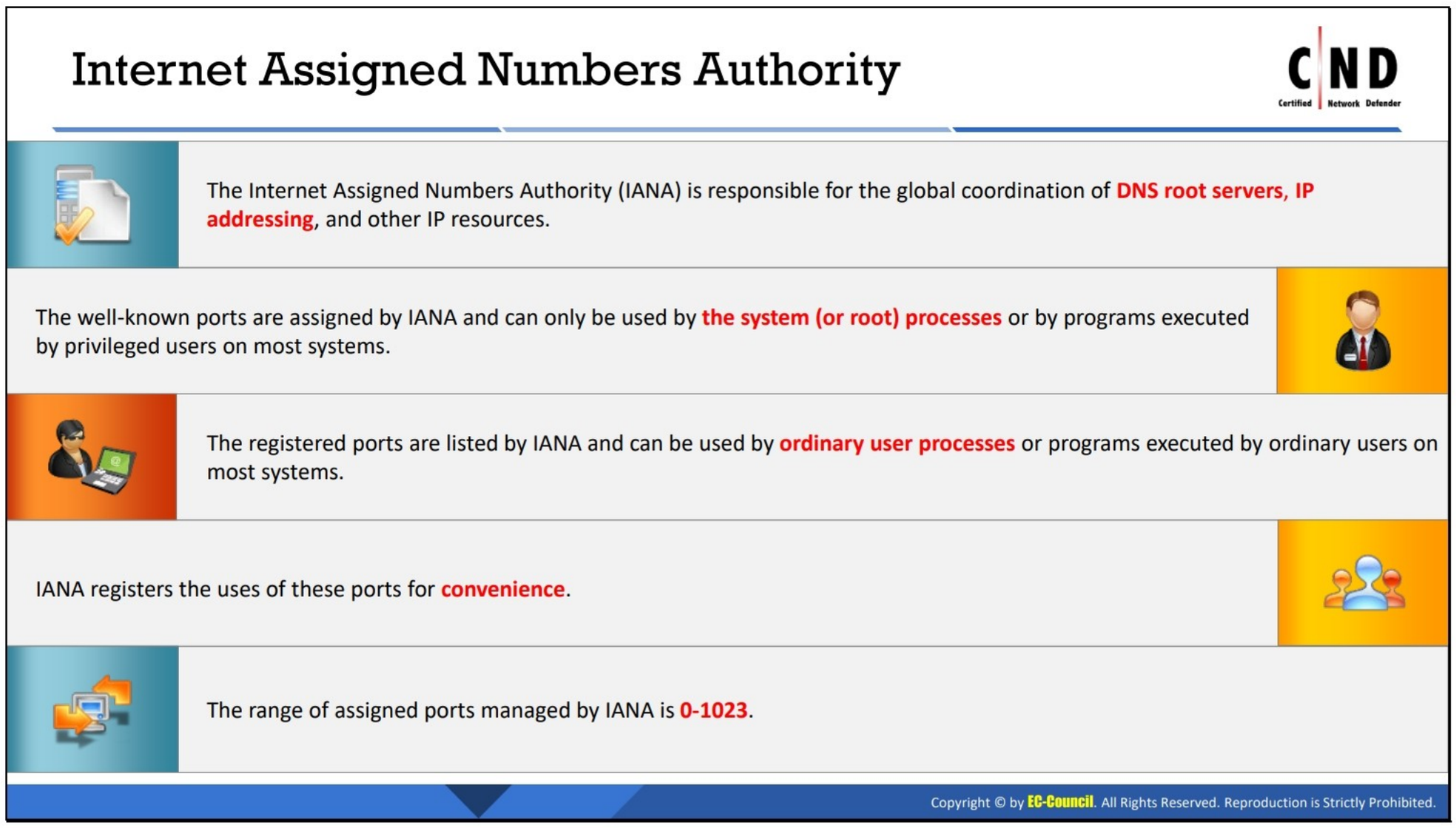
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#03: Concepts of IP Addressing and Port Numbers

This section discusses the fundamentals of basic networking concepts such as IP addressing and port numbers.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Internet Assigned Numbers Authority

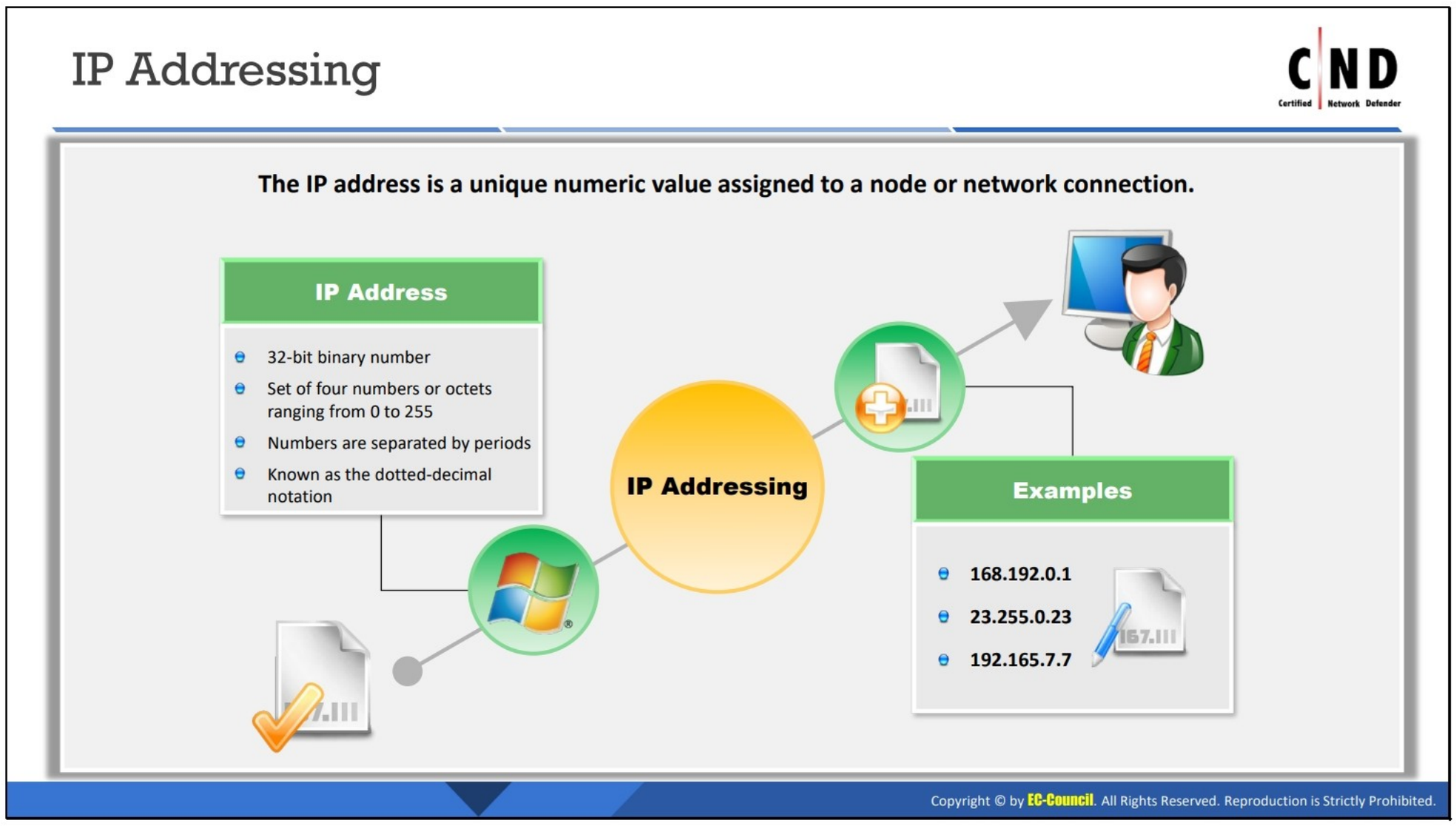
IANA monitors and manages key elements of the Internet globally. It is responsible for the global coordination of DNS root servers, IP addressing, autonomous system number allocation, and other Internet resources. The well-known ports are assigned by IANA and can only be used by the system (or root) processes or by programs executed by privileged users on most systems. The registered ports are listed by IANA and can be used by ordinary user processes or programs executed by ordinary users on most systems. IANA registers the uses of these ports for convenience. The range of assigned ports managed by the IANA is 0–1023.

Developed protocols are published as Requests for Comment (RFCs) by IANA. RFC documents are used to understand and analyze the Internet and its related terminologies. IANA performs these tasks in collaboration with the Internet Engineering Task Force (IETF).

The activities of IANA are broadly described into three categories:

- DNS management
- Internet addresses management
- Management of the IP numbering system

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IP Addressing

The IP address is a number assigned to computers transmitting data over a network by using IP. An IP address consists of the following: host identification and location addressing. The assigned addresses make it easy to identify the computers in a network. The address normally consists of 32 binary bits divided into two parts: a host part and network part. It is written as four numbers separated by periods. Each number can range from 0 to 255. The following are some sample IP addresses: 168.192.0.1, 23.255.0.23, and 192.165.7.7. The IP address can be either static or dynamic. Static IP addresses do not change and are permanent. Dynamic IP addresses change every time a computer accesses the Internet.

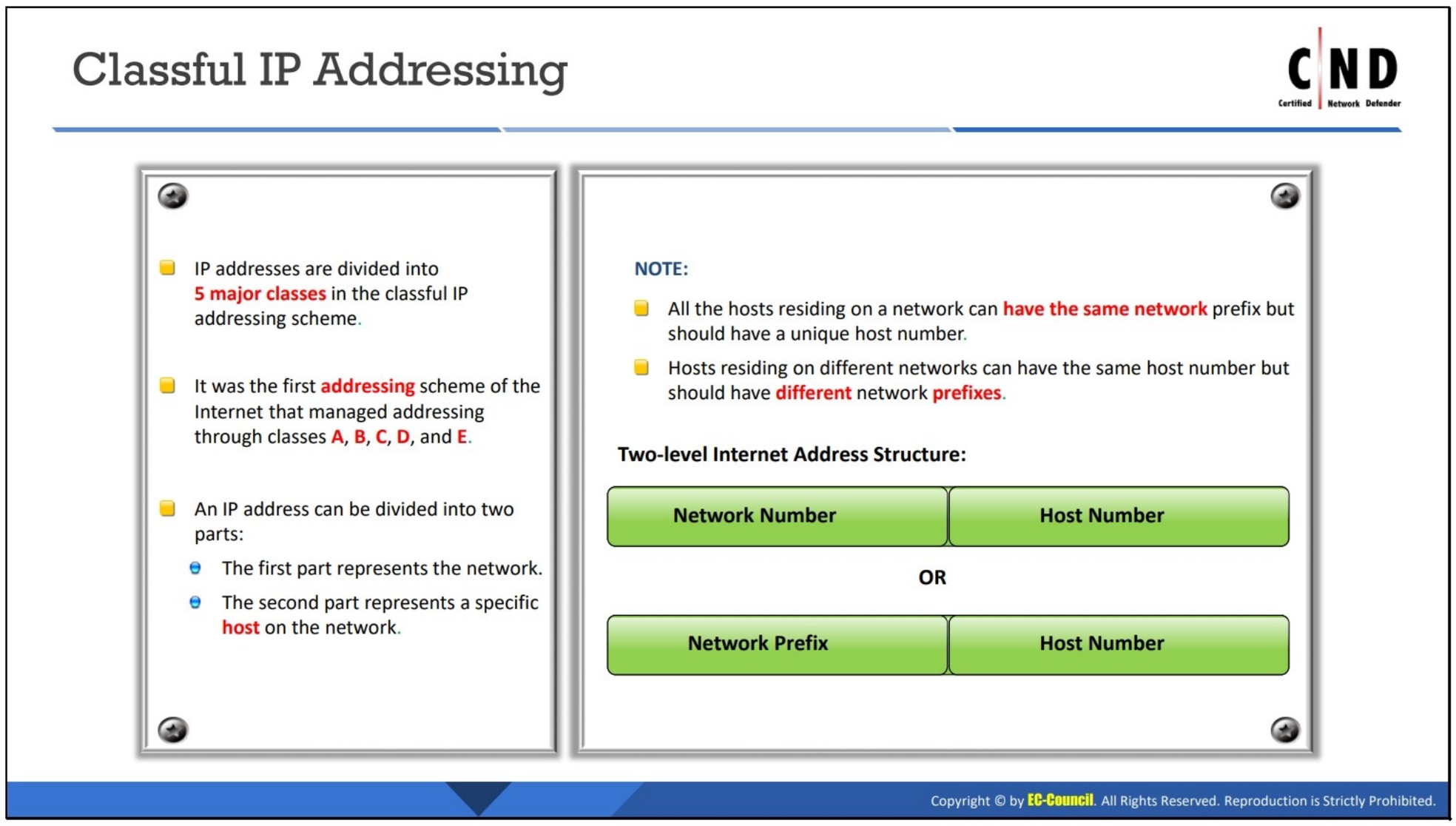
Important Terms in IP Addressing

- **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 identifiers. The aim of ICANN is to ensure that all users have valid addresses. ICANN does not supervise Internet content control, data protection, or unsolicited mail, but ICANN is responsible for the management of new generic top-level domains (gTLDS).

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Making the address space friendly**: To make an address space friendly, it should be familiar and short. All the information on the Internet is the binary format, but the base-10 number system is much more user-friendly. Imagine that a computer's address is 4,27,28,123,12. This number is easier to remember than its equivalent in the base-2 system: 10010000, 11111010, 01010101, and 10111011.
- **Purpose of dots**: It can be difficult to remember a decimal number address. To make it easier to remember, it is divided into four parts. With the logical classification of addresses, it is easy to identify a particular host on a network. The scheme depends on the decimal numbers, and the address space used is binary. Certain schemes use 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.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Classful IP Addressing

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, IP specifies that each computer should have a unique, 32-bit address 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 the parts belonging to the network address and the parts belonging to the node address.

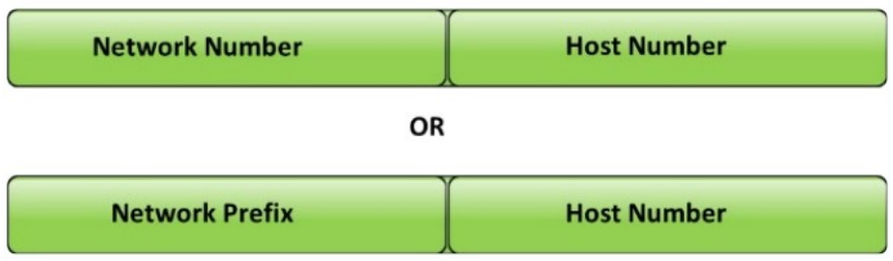


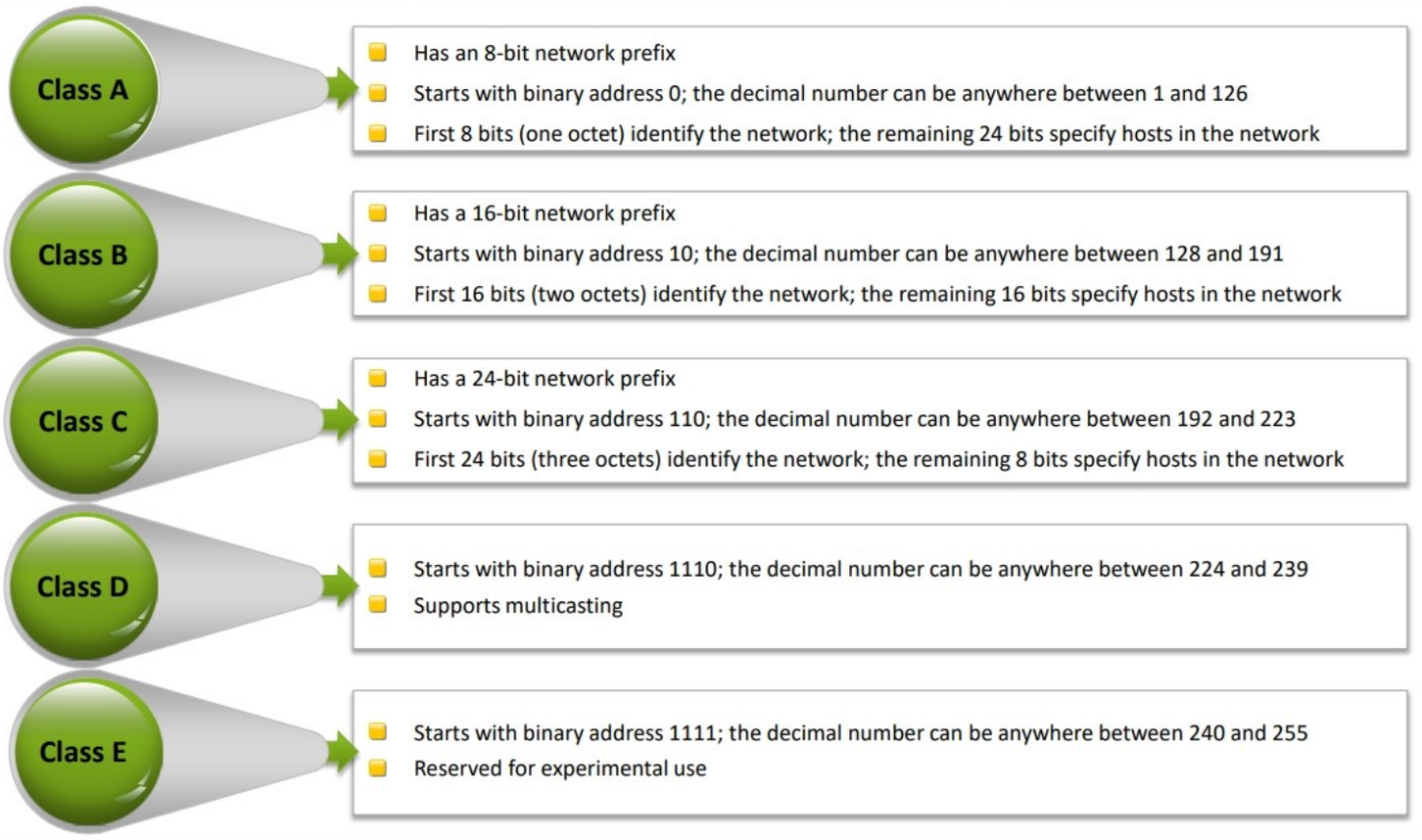
Figure A.81: Two-Level Internet Address Structure

From the past few years, the network number segment refers the network prefix because the major part of each IP address determines the network number. All the hosts residing on a network can have the same network prefix but should have a unique host number. Hosts residing on different networks can have the same host number but should have different network prefixes. IP addresses are divided into 5 major classes in the classful IP addressing scheme. It was the first Internet addressing scheme that managed addressing through classes A, B, C, D, and E. An IP address can be divided into two parts:

- The first part represents the network.
- The second part represents a specific host on the network.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Address Classes



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Address Classes (Cont'd)

Numbers 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 (Multicast)	1110	20	8	1,048,576	254
Class E (Reserved)	1111	20	8	1,048,576	254

Characteristics and Uses of IP Address Classes

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 in very large organizations
Class B	1/4	16	16	Used for unicast addressing in medium or large organizations
Class C	1/8	24	8	Used for unicast addressing in small organizations
Class D	1/16	N/A	N/A	Used for IP multicasting
Class E	1/16	N/A	N/A	Reserved

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Address Classes

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

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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 (Multicast)	1110	20	8	1,048,576	254
Class E (Reserved)	1111	20	8	1,048,576	254

Table A.10: Numbers of Networks and Hosts for Five IP Address Classes

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 in very large organizations
Class B	1/4	16	16	Used for unicast addressing in medium or large organizations
Class C	1/8	24	8	Used for unicast addressing in small organizations
Class D	1/16	N/A	N/A	Used for IP multicasting
Class E	1/16	N/A	N/A	Reserved

Table A.11: Characteristics and Uses of IP Address Classes

Class A

The IP address class defines IP addresses for large networks. The binary address starts with 0. The decimal number is in the range of 0–127 and mostly used by international companies. In the 32 bits of an address, a 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 recent years, class-A networks are referred to as “/8” or “8” networks. A total of 126 (27-2) /8 addresses can be defined in a class-A network. The number of addresses is less by 2 because in a class-A network, 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 addresses in a host and 231 (2,147,483,648) individual addresses. It contains 232 (4,294,967,296) addresses of the IPv4 address space, which amounts to 50% of the total IPv4 unicast address space.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

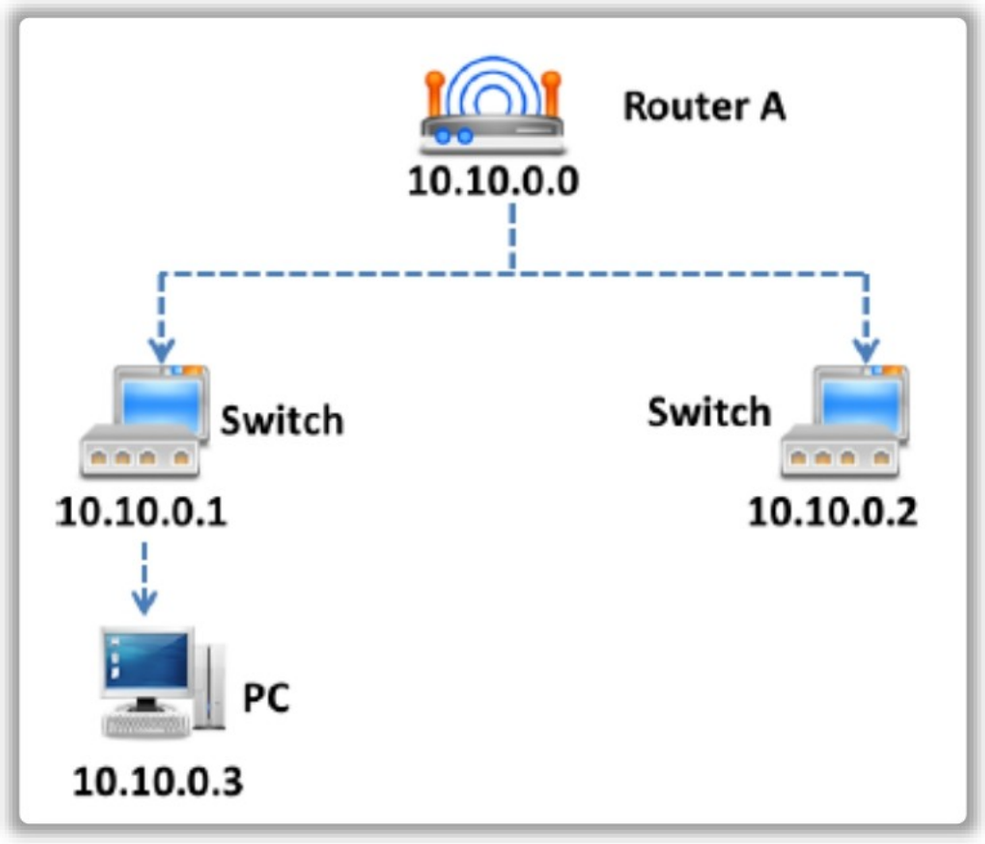


Figure A.82: Class-A Network

Class B

Class-B addresses are used in medium-scale networks. The leftmost 16 bits of class-B addresses form the network prefix, and the binary address starts with 10. The decimal number ranges 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. In recent years, class-B networks have been referred to as "/16" networks as they have a 16-bit network prefix. A total of 16,384 (214) /16 addresses can be defined in a class-B network, where 65,534 (216-2) hosts are created per network and 230 (1,073,741,824) individual addresses. This amounts to 25% of the total IPv4 unicast address space.

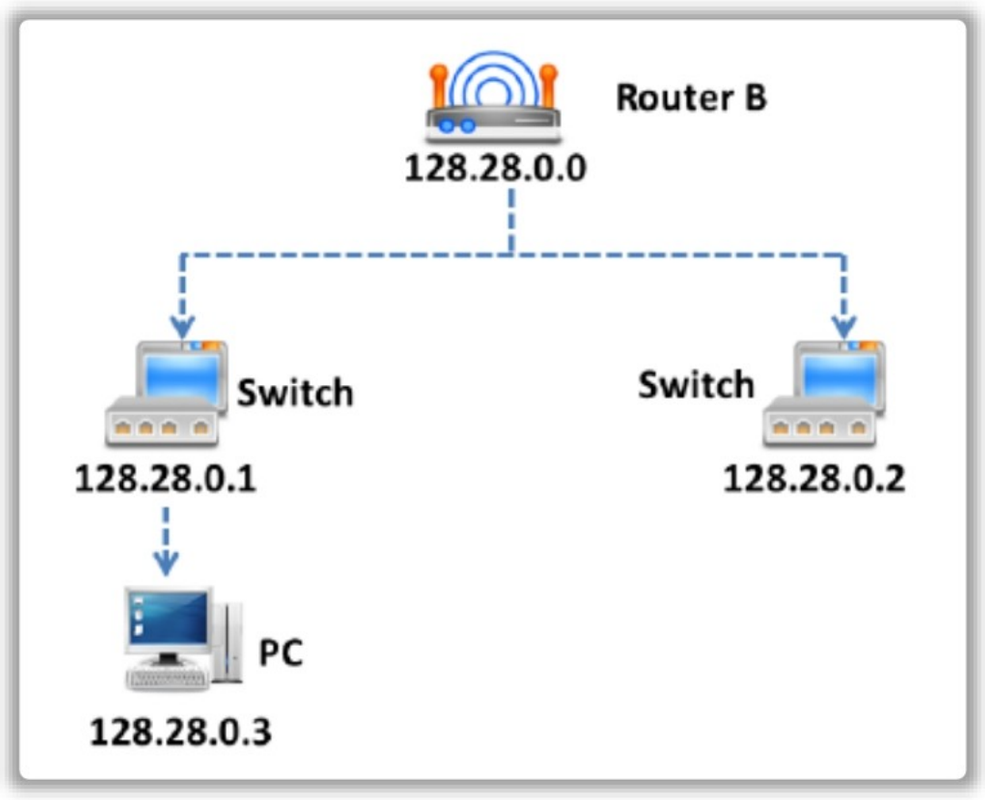


Figure A.83: Class-B Network

Class C

Class-C addresses have a 24-bit network prefix. The binary address of Class C starts from 110. The decimal number ranges from 192 to 223. Class-C addresses are used by small businesses. The

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

first 24 bits (three octets) are used for identifying the network, while the remaining 8 bits help in the identification of the host on the network.

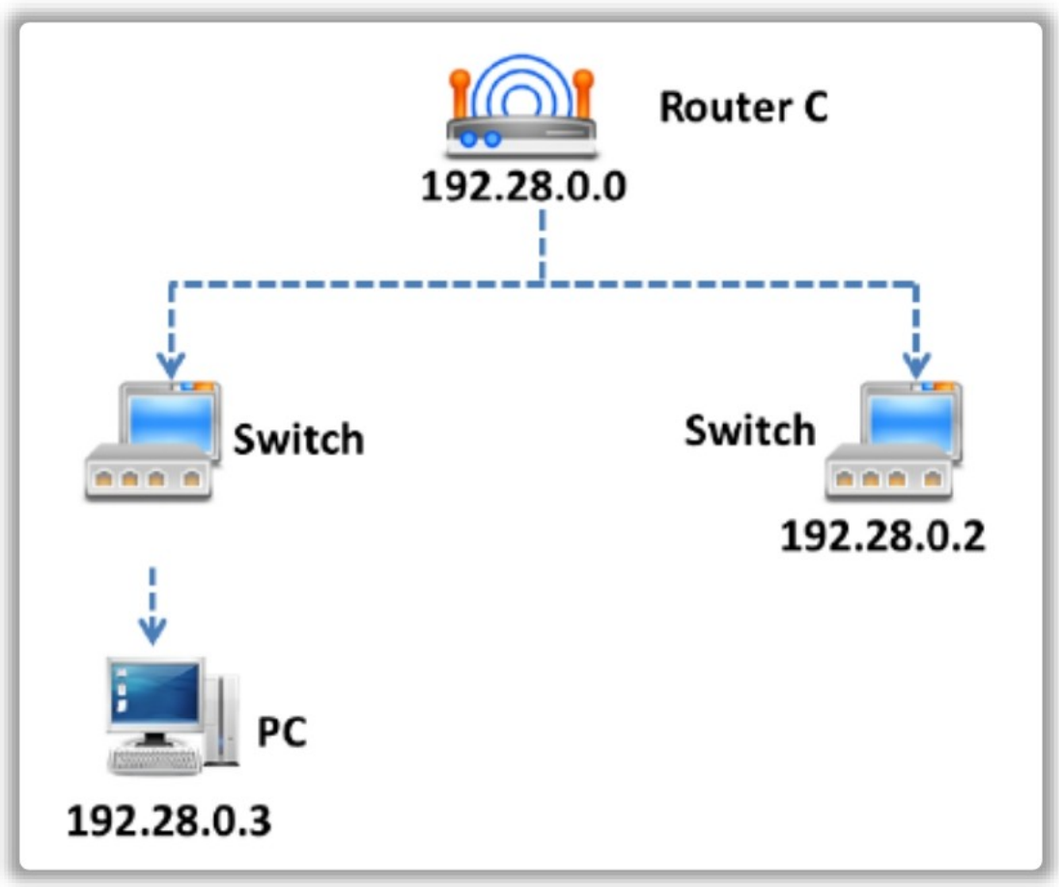


Figure A.84: Class-C Network

Class D and Class E

In addition to the primary address classes, two classes are defined by the Internet designers: class D and class E. These are special classes designed for specific purposes, and users do not even know they exist. Class D starts with the binary address 1-1-1-0, and its decimal number ranges from 224 to 239. Its main function is to support multicasting. Class E starts with the binary address 1-1-1-1, and its decimal number ranges from 240 to 255. It serves experimental purposes.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Subnet Masking

C|ND Certified Network Defender

1. A subnet mask divides the IP address of the host into **network and host** numbers.
2. A subnet allows the division of class A, B, and C network numbers into **smaller segments**.
3. A variable-length subnet mask (VLSM) allows two or more subnet masks in the **same network**.
4. VLSM effectively uses the **IP address** space in a network.

Default Subnet Masks for Class A, Class B, and Class C Networks

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Subnet Masking

A subnet mask provides information about the division of bits between the subnet ID and host ID as well as the host ID containing the routing traffic. It is a 32-bit binary number. The subnet mask separates the IP address into two components, namely the network address and host address. The subnet calculator is used to retrieve the subnet mask information. The subnet mask performs the bitwise AND operation on the netmask to identify the network address of a particular IP address. Subnet mask bits are defined by setting all network bits to "1" and setting all host bits to "0." Subnet masks are expressed using the dot-decimal notation of an address. Every host on the TCP/IP network requires a subnet mask. A default subnet mask is used for class-based network IDs, and custom subnet masks are used when subnetting and supernetting are configured. Subnet masks have the following features:

- A subnet mask divides the IP address of the host into network and host numbers.
- A subnet allows the division of network numbers of class A, B, and C into smaller segments.
- A variable-length subnet mask (VLSM) allows two or more subnet masks in the same network.
- VLSM effectively uses the IP address space in a network.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

IP Address Class	Total Number of Bits for Network ID/Host IP	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 A.12: Default Subnet Masks for Class-A, Class-B, and Class-C Networks

A sample case is presented below:

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

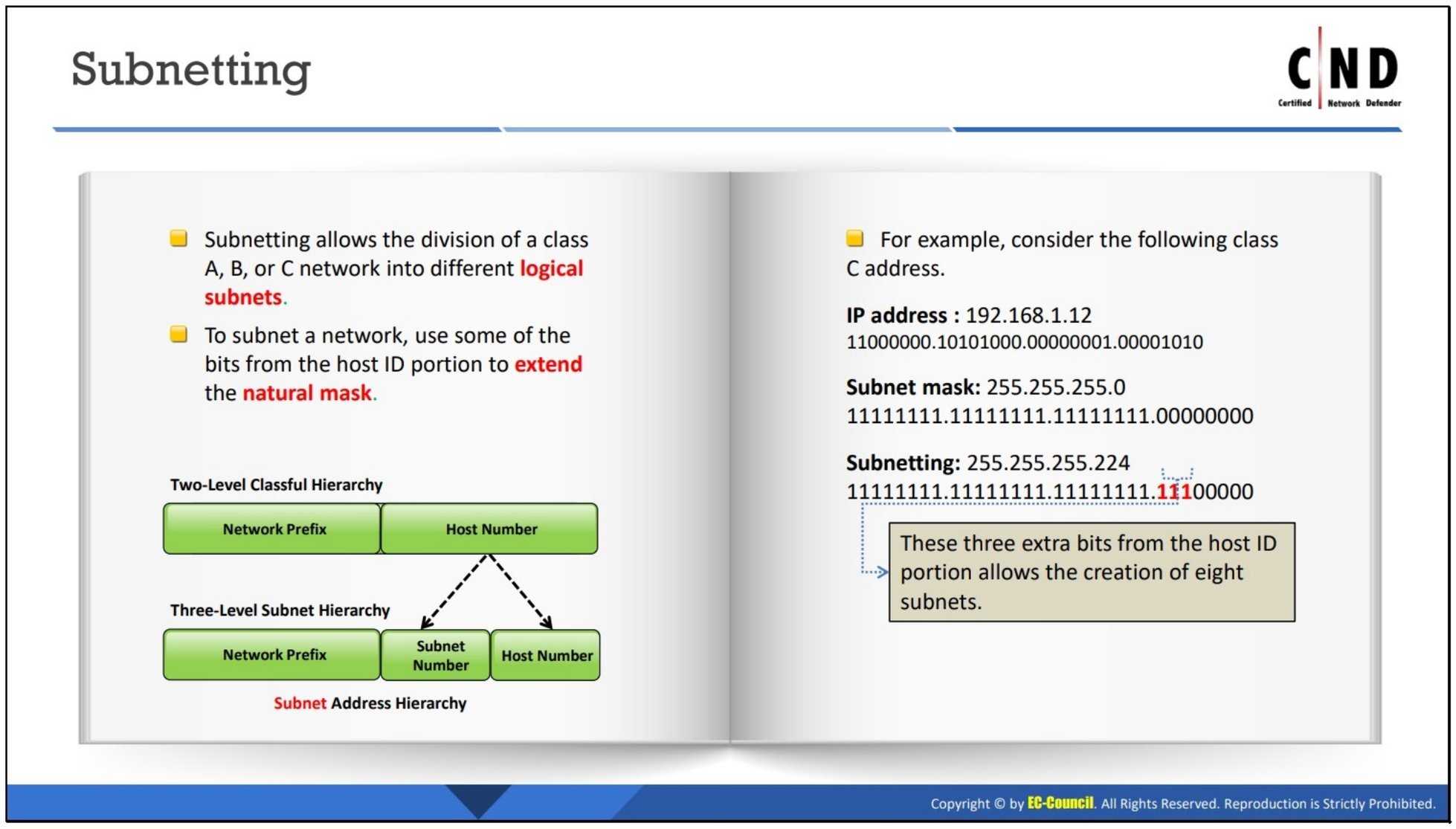
Subnet mask in dot decimal notation: 255.255.248.0

Network ID = 159.100.0.0

Binary format: 10011111.01100100.00001000.00000000

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

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Subnetting

The initial designers of the Internet did not foresee its rapid growth and the change it has brought in as a communication system. Today, organizations are facing many problems with the allocation of IP addresses, as the IP address space, especially IPv4, is in the depletion stage. This problem has occurred because of early decisions made by the Internet designers in the formative stage. In the early evolution stage of the Internet, organizations were allocated address spaces based on their request, rather than their requirements. This has led to the eventual depletion of the IP address space. Many organizations that predicted the future of networking had invested in the Internet, but organizations that ignored the significance of the Internet later realized that they had to obtain addresses and faced address shortage issues. Emerging organizations also face address storage issues due to the premature depletion of the IPv4 address space. In order to overcome the problems of IP address space depletion, one can perform IP subnetting. Subnetting allows an organization's network to be divided into a two-level structure consisting of hosts and subnets. An organization's system administrator divides the host network, specifically the internal network, into two segments to make it unavailable to external networks. The main advantage of subnetting is that the organization can divide the classful host number into a subnet ID and host ID based on its preferences and requirements.

Subnetting allows an organization to divide a network of class A, B, or C into different logical subnets. To subnet a network, some of the bits from the host ID portion are used to extend the natural mask.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

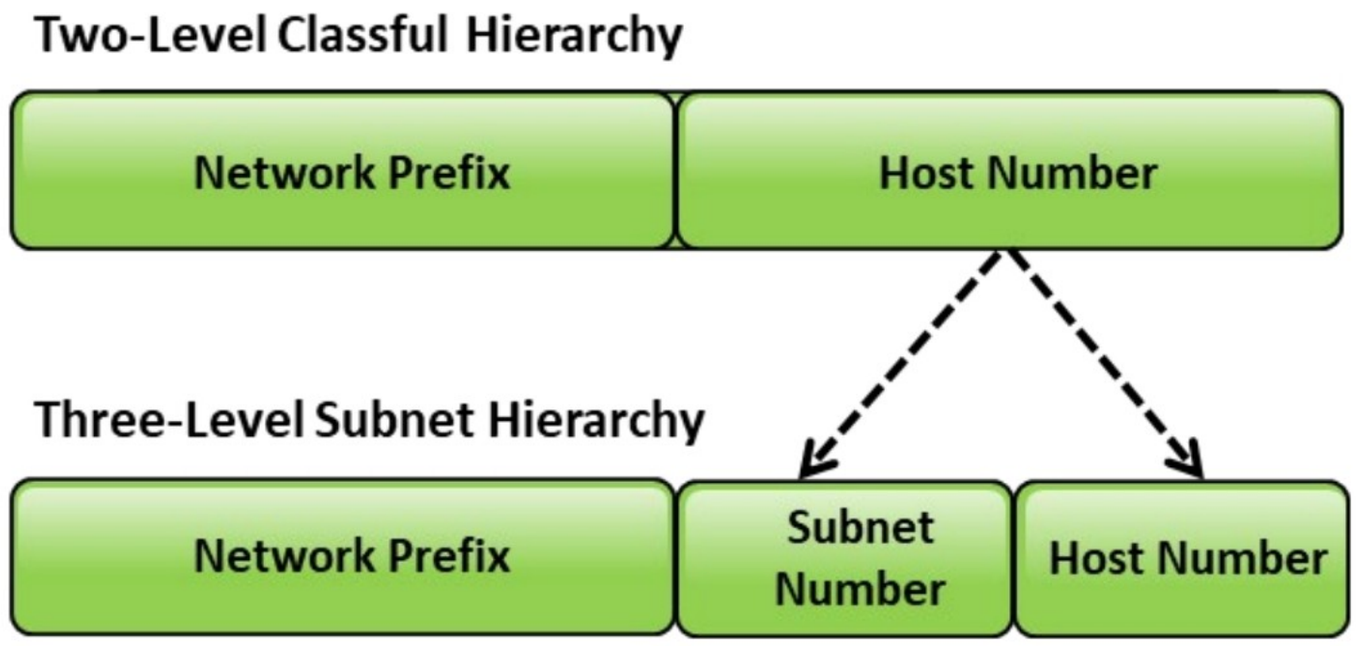


Figure A.85: Subnet address Hierarchy

For example, consider the following class-C address:

IP Address: 192.168.1.12 11000000.10101000.00000001.00001010

Subnet mask: 255.255.255.0 11111111.11111111.11111111.00000000

Subnetting: 255.255.255.224 11111111.11111111.11111111.11100000

In the above address, three extra bits from the host ID portion allow the creation of eight subnets.

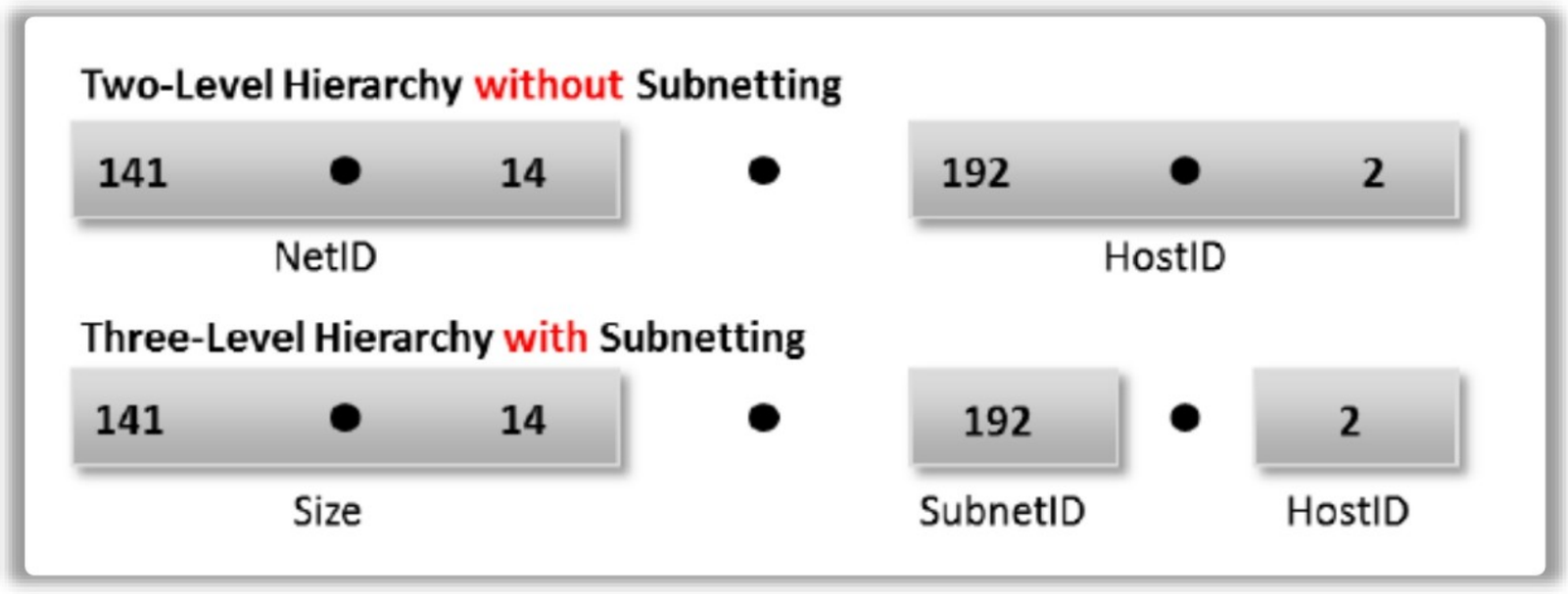


Figure A.86: Two-Level and Three-Level Subnetting

- **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 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 address division is arbitrary in nature, it is difficult for the router to determine the process of dividing an address into subnet and host IDs. A subnet mask provides information about the division of bits between the 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 network numbers of class A, B, and C into smaller segments. VLSM allows two or more

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

subnet masks in the same network. VLSM effectively uses the IP address space in a network. VLSM provides flexibility to a network administrator to divide a network as per the requirements and preferences of the organization and to create subnets, sub-subnets, and sub-sub-subnets.

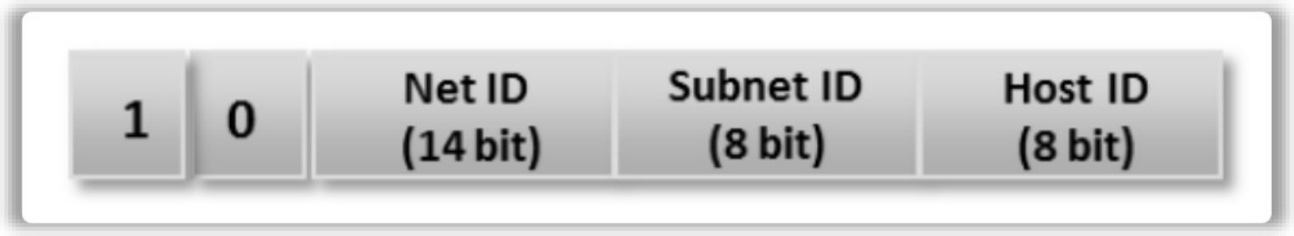
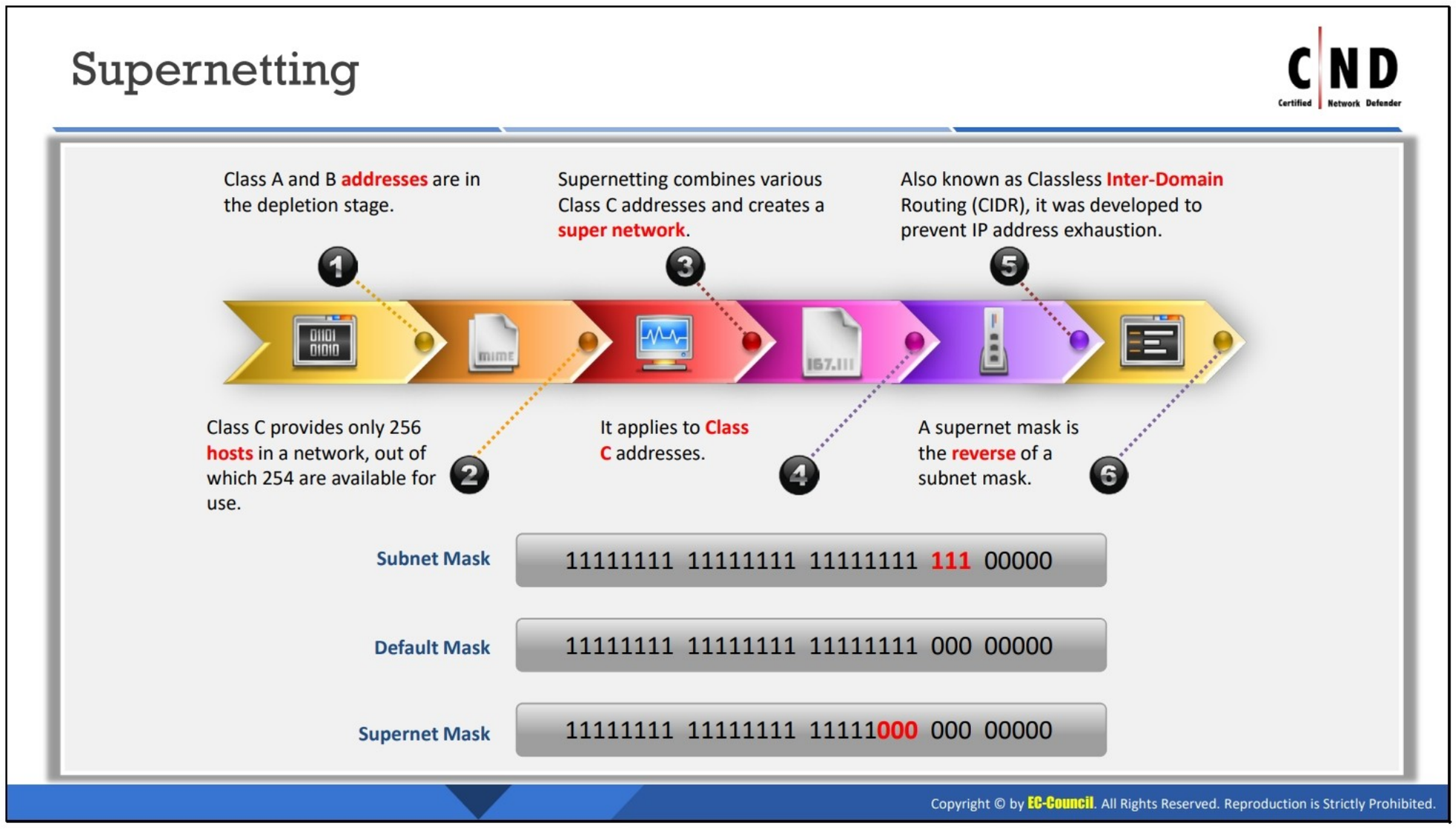


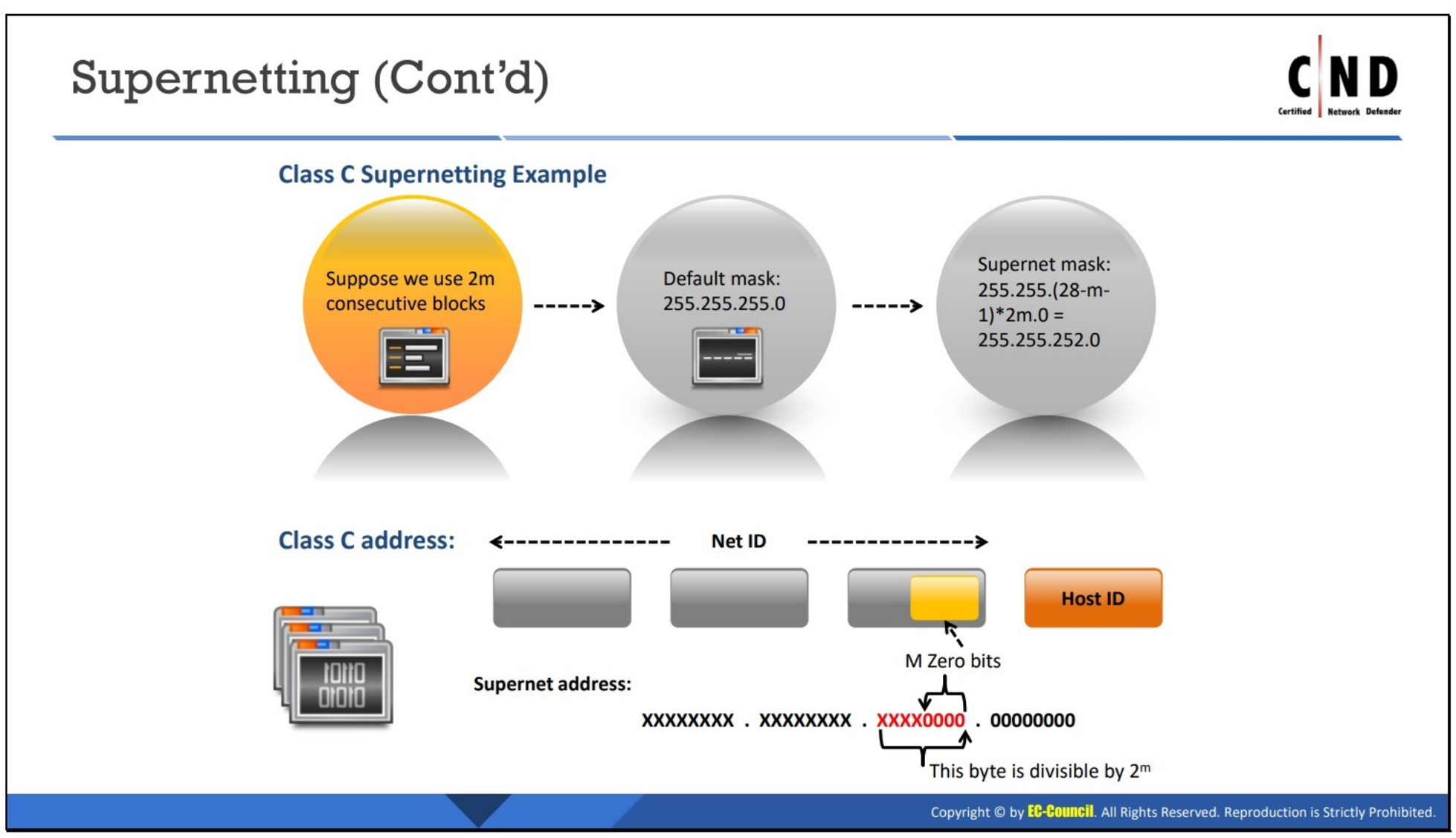
Figure A.87: Example of Subnetting

The following is an example of subnetting for a class-B address:

```
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
```


Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Supernetting

With the growth of the Internet, classful addressing has become a significant problem for many organizations. The problems with classful addressing are a lack of flexibility in dividing addresses for an internal network; an improper distribution of the allocated address space would require a router to create an increasing number of routing table entries. Subnetting solves these problems to a certain extent, but IPv6 addressing has a 128-bit addressing system to eliminate addressing issues appropriately. This new system eliminates the need for address classes and creates a new

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

addressing scheme to match the growing demand of Internet users. This system advocates the creation of a new classless addressing scheme known as Classless Inter-Domain Routing (CIDR). This system uses the 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 spaces efficiently as per their requirements and preferences. In classful addressing, there are networks of class A, B, and C. Class-A networks have approximately 16,277,214 addresses per network, class-B networks have 65,534 addresses, and class-C networks have only 254 addresses. Therefore, addresses are classified disproportionately in this addressing system. CIDR eliminates this 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 division point between the 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, it uses the slash ("/") notation known as CIDR notation along with the prefix length to show the network size.

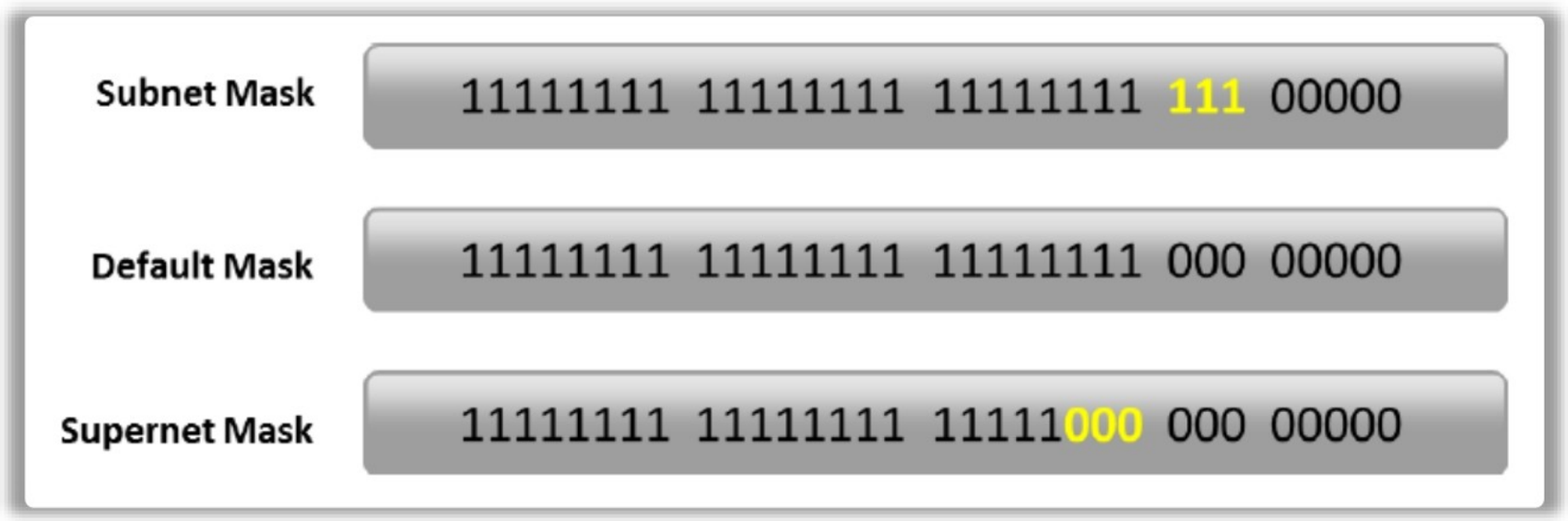


Figure A.88: Example of Supernetting

Example of Supernetting

Addresses of class A and B are in the depletion stage. Class C allows only 256 hosts in a network, out of which 254 are available for use. Supernetting combines various Class-C addresses and creates a supernet. It applies to Class-C addresses. CIDR was developed to keep IP addresses from exhaustion. The supernet mask is the reverse of the subnet mask.

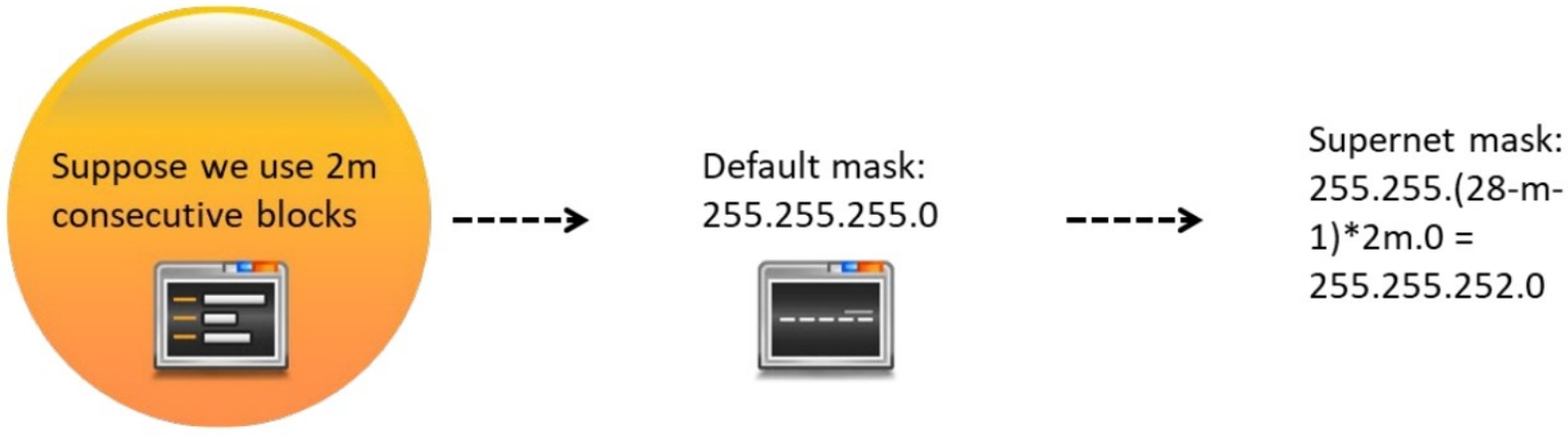


Figure A.89: Example of Supernetting

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following is an example showing 4 class-C addresses in a network appearing as a single network from outside:

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

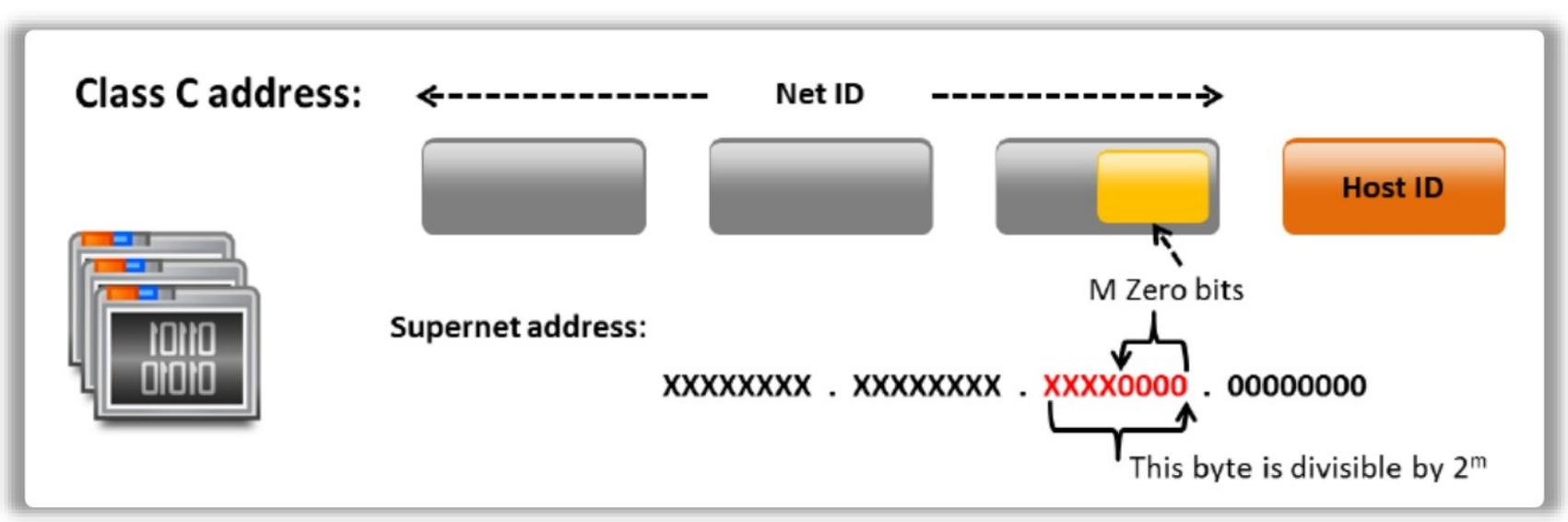
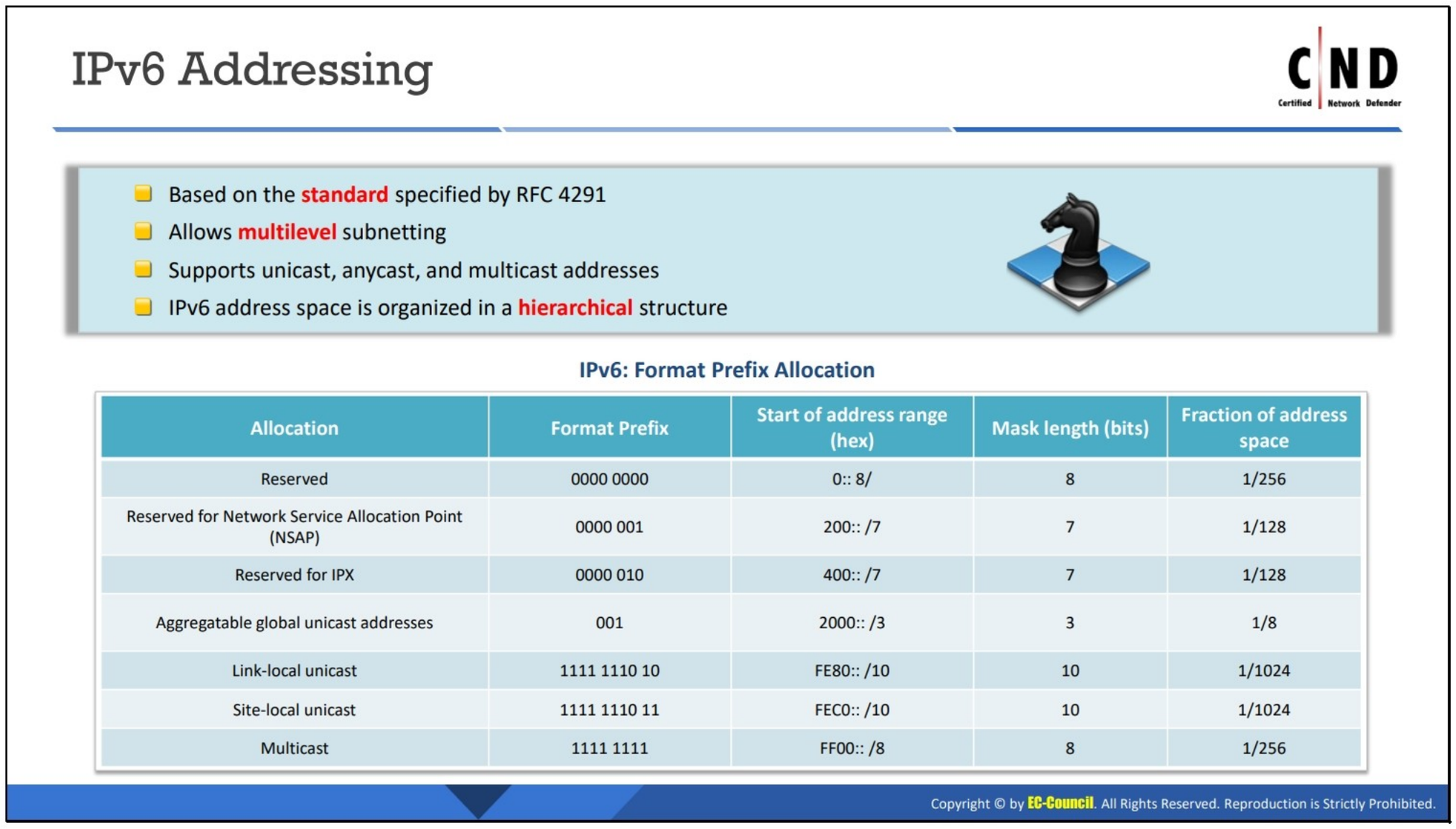


Figure A.90: Supernetting with a “Class-C” Address

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IPv6 Addressing

Based on the standard specified by RFC 4291, IPv6 allows multilevel subnetting. It supports unicast, anycast, and multicast addresses. The IPv6 address space is organized in a hierarchical structure.

IPv6 provides a large address space of 128 bits for meeting the increasing demands of Internet users. It has a new format for the packet header to minimize problems with overhead routing entries. IPv6 has globally identified unique addresses with efficient, hierarchal routing infrastructure that relies on the prefix length rather than address classes. This allows backbone routers to create small routing tables. Furthermore, IPv6 simplifies host configuration with stateless and stateful address configurations for network interfaces. It 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 addresses are as follows:

- Global unicast addresses are globally unique on the Internet.
- Link-local addresses are not meant for routing but confined to a single network segment.
- Local addresses are unique. These assist in private addressing and avoids chances of collision between two subnets.

Anycast address: In the anycast communication method, only specific associated address in a network receives messages. IPv6 provides better support for QoS with the 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 that are members of the multicast group can receive

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the multicast packets. The IPv6 multicast is a routable address, and routers forward these multicast packets to all the members of the multicast group.

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 A.13: IPv6 Format Prefix Allocation

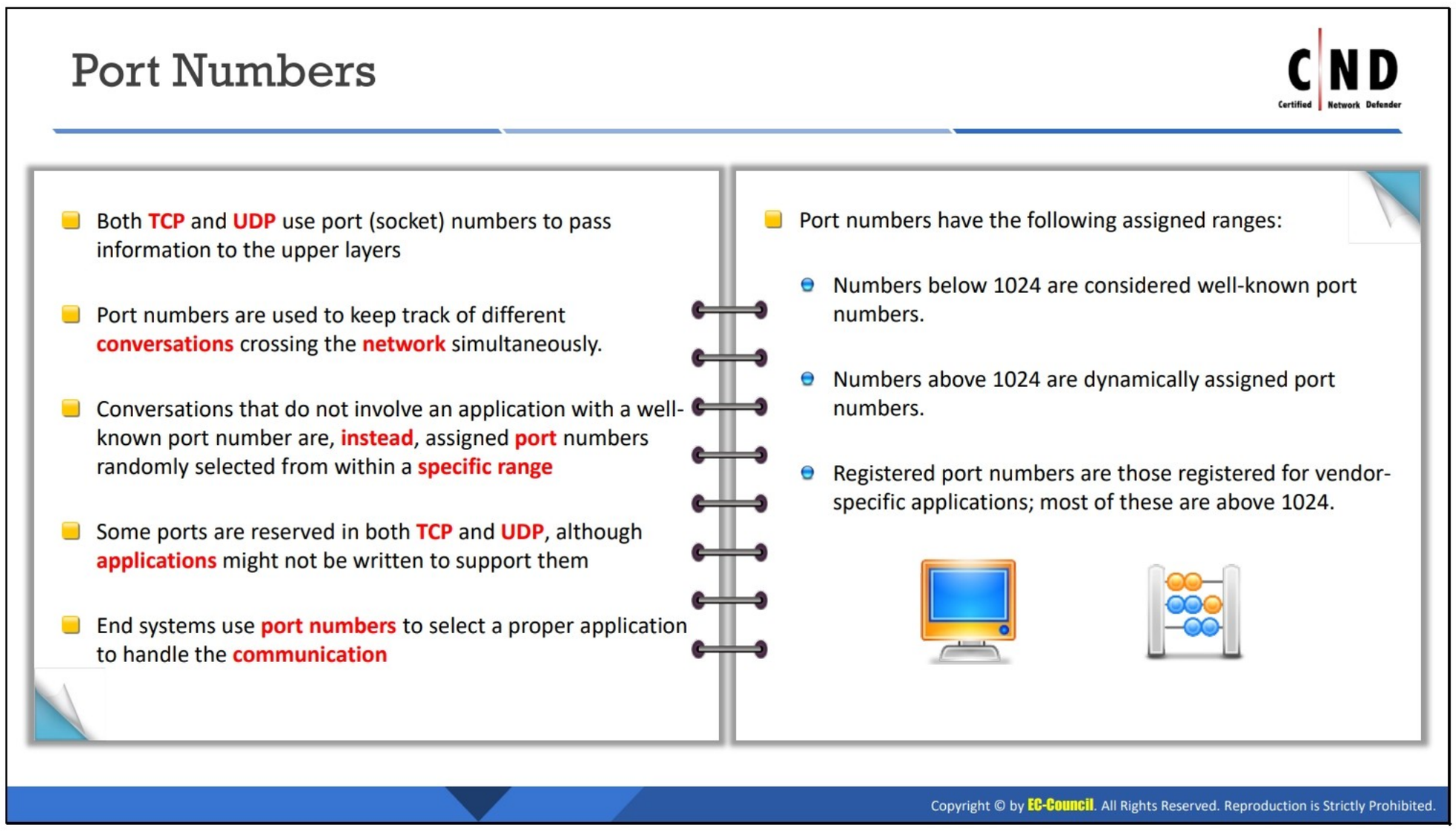
The IPv6 notation includes eight groups of hexadecimal quartets separated by colons. An example for IPv6 is **2001:cdba:0000:0000:0000:0000:3257:9652**. The groups of zeroes in an IPv6 address may be reduced to zero or removed, as in the following examples:

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

IPv6 addresses use the CIDR notation. The subnet using the IPv6 protocol consists of a group of IPv6 addresses having a size value in powers of two. The initial bits in the IPv6 address form the network prefix. The bits in the network prefix use a forward slash (“/”).

For example, **2001:cdba:9abc:5678::/64** represents the address **2001:cdba:9abc:5678**.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



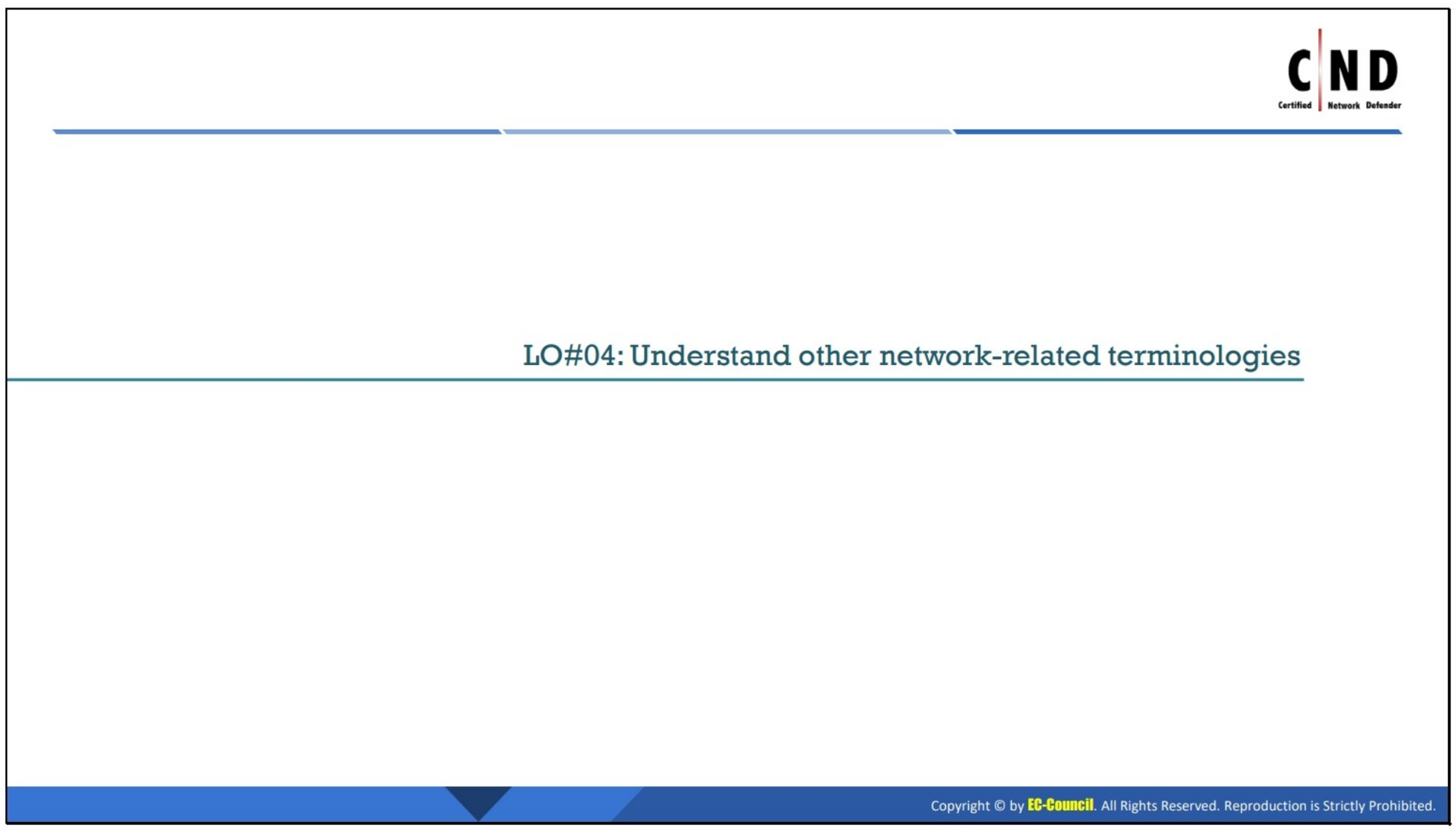
Port Numbers

Both TCP and UDP use port (socket) numbers to pass information to the upper layers. Port numbers are used to keep track of different messages crossing the network simultaneously. Conversations that do not involve an application with a well-known port number are, instead, assigned port numbers randomly selected from within a specific range. Some ports are reserved in both TCP and UDP, although applications might not be written to support them. End systems use port numbers to select a proper application to handle communication.

Port numbers have the following assigned ranges:

- Numbers below 1024 are considered well-known port numbers.
- Numbers above 1024 are dynamically assigned port numbers.
- Registered port numbers are those registered for vendor-specific applications; most of these are above 1024.

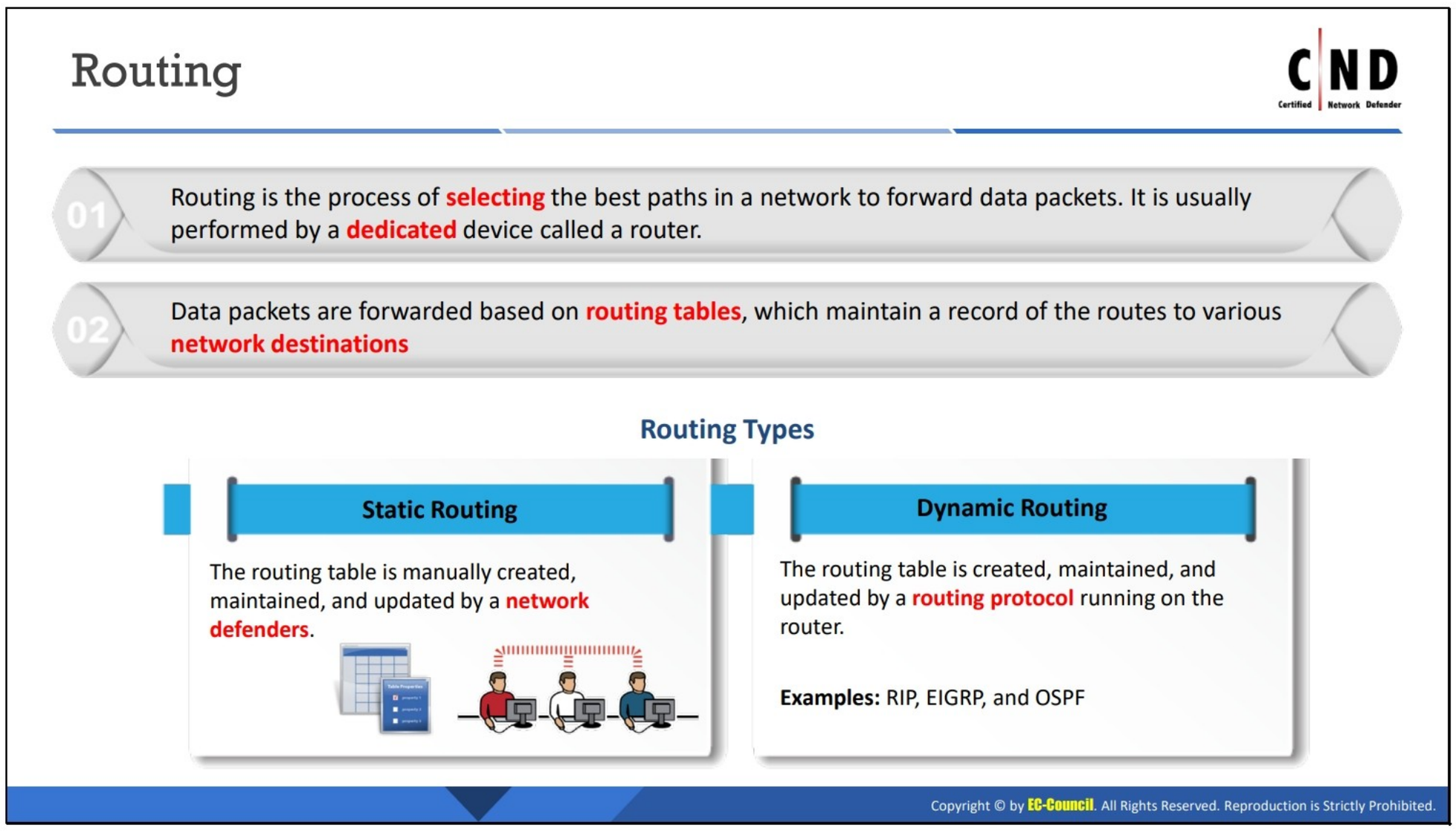
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#04: Other Network-Related Terminologies

To understand networks, it is essential to understand the terminology related to networking. This section describes network terminologies such as routing, Network Address Translation (NAT), Port Address Translation (PAT), and VLAN.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Routing

Routing is the process of selecting the best paths in a network to forward data packets. It is usually performed by a dedicated device called a router. It is an important feature of the Internet as it transmits data packets from one node to another. Intermediate nodes are basically network hardware devices such as routers, bridges, gateways, firewalls, and switches. Data packets are forwarded based on routing tables, which maintain a record of routes to various network destinations.

Routing functions somewhat similarly to bridging, but they are not the same. The main difference is that routing is performed at layer 3, i.e., the network layer, of the OSI reference model, whereas bridging is performed at layer 2, i.e., the data-link layer. As routing occurs at layer 3 of the OSI reference model, deep analysis must be performed to determine the best path for data packets.

Routing Types

- **Static routing**

  In this type of routing, the routing table is created, maintained, and updated by a network administrator manually.

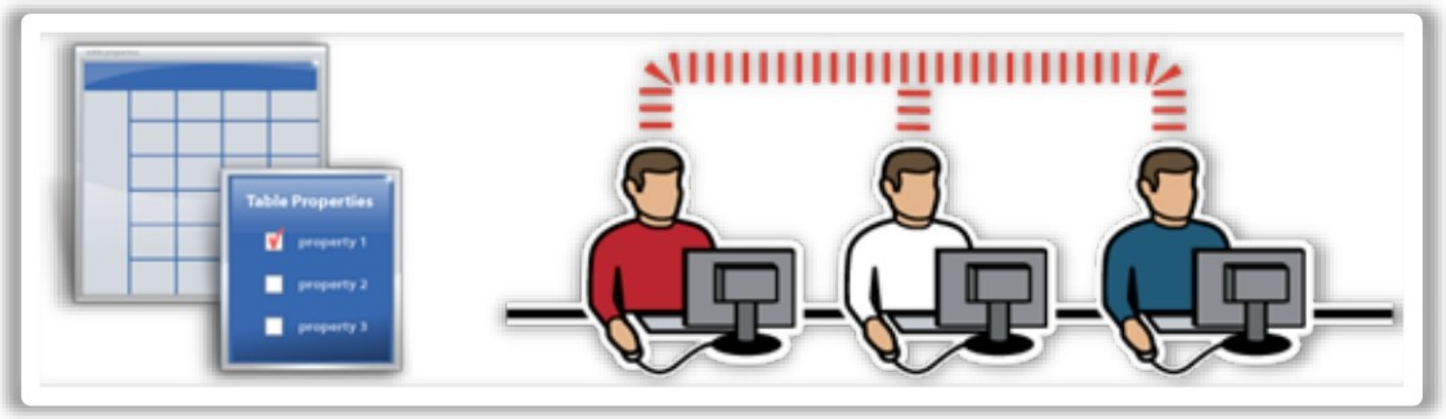


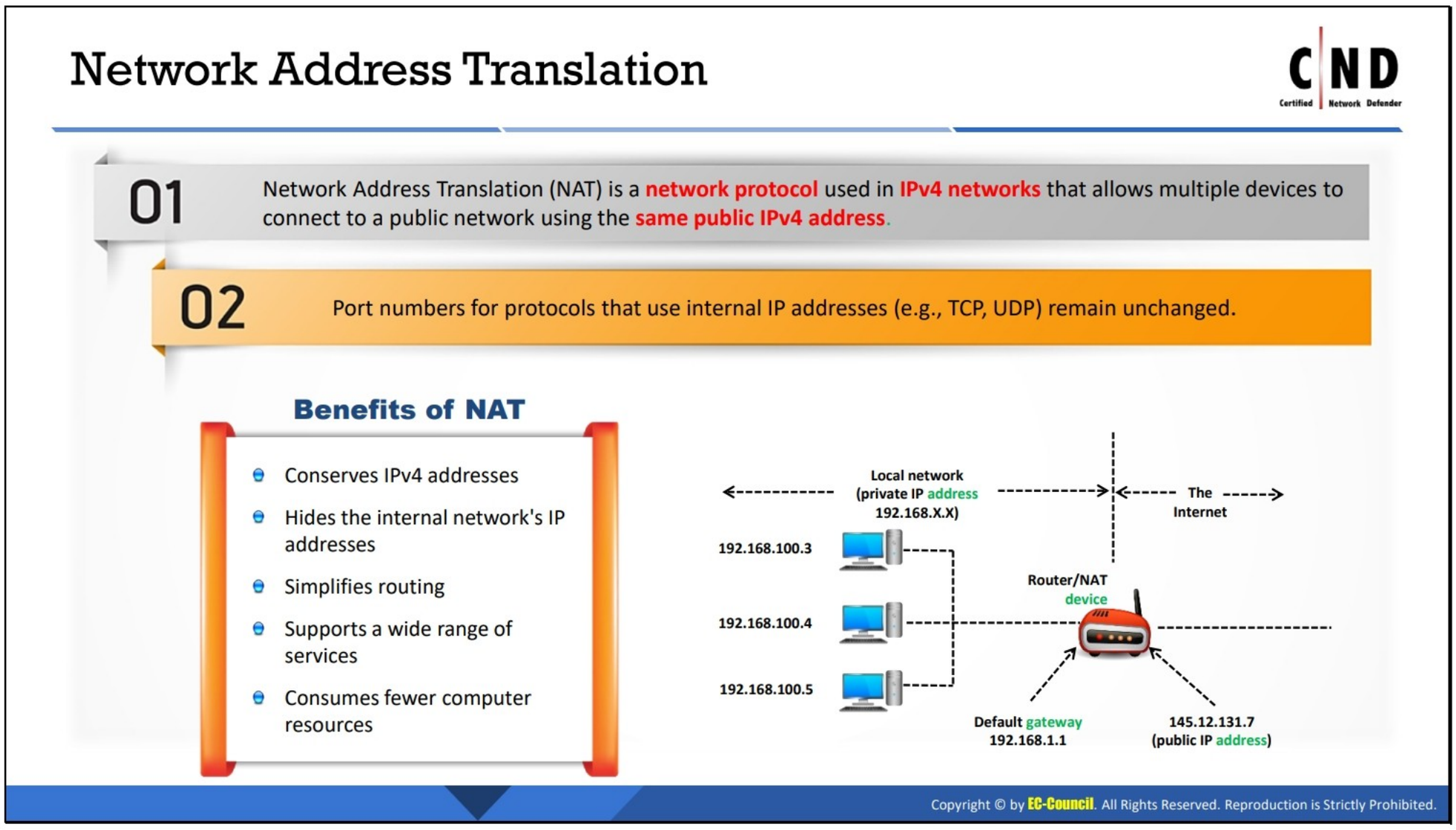
Figure A.91: Static Routing

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Dynamic routing**

  In this type of routing, the routing table is created, maintained, and updated by a routing protocol running on the router. Examples include RIP, EIGRP, and OSPF.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Address Translation

Network Address Translation (NAT) is a network protocol used in IPv4 networks that allows multiple devices to connect to a public network using the same public IPv4 address. It helps hide an internal network layout and forces connections to go through a choke point. NAT works with the help of a router, thereby helping in sending and modifying packets.

When an internal machine sends a packet to an outside machine, NAT modifies the source address of the packet to make it appear as if it originated from a valid address. When the outside machine sends the packet to the internal machine, NAT modifies the destination address to turn the visible address into the correct internal address. NAT can also modify the source and destination port numbers. Port numbers for protocols that use internal IP addresses (e.g., TCP and UDP) remain unchanged.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

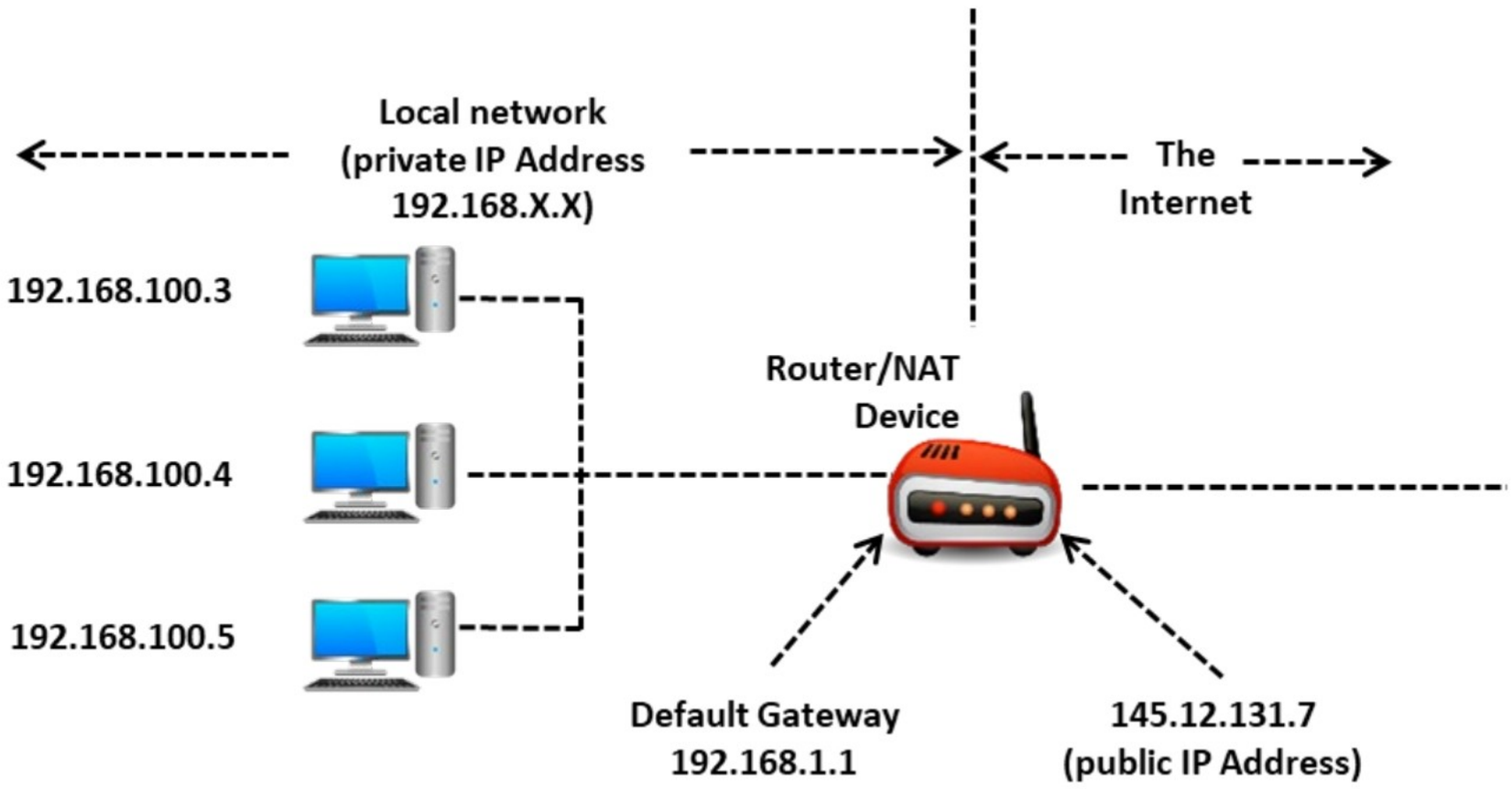


Figure A.92: Network Address Translation

NAT systems use the following schemes for translating between internal and external addresses:

- NAT can assign one external host address for each internal address and always apply the same translation. This slows down connections and does not provide any savings in the address space.
- NAT can dynamically allocate an external host address without modifying the port numbers when the internal host initiates a connection. This restricts the number of internal hosts that can simultaneously access the Internet to the number of available external addresses.
- NAT can create a fixed mapping from internal addresses to externally visible addresses but use port mapping so that multiple internal machines use the same external addresses.
- NAT can dynamically allocate a pair of external host address and port each time an internal host initiates a connection. This is the most efficient use of external host addresses.

Benefits of NAT

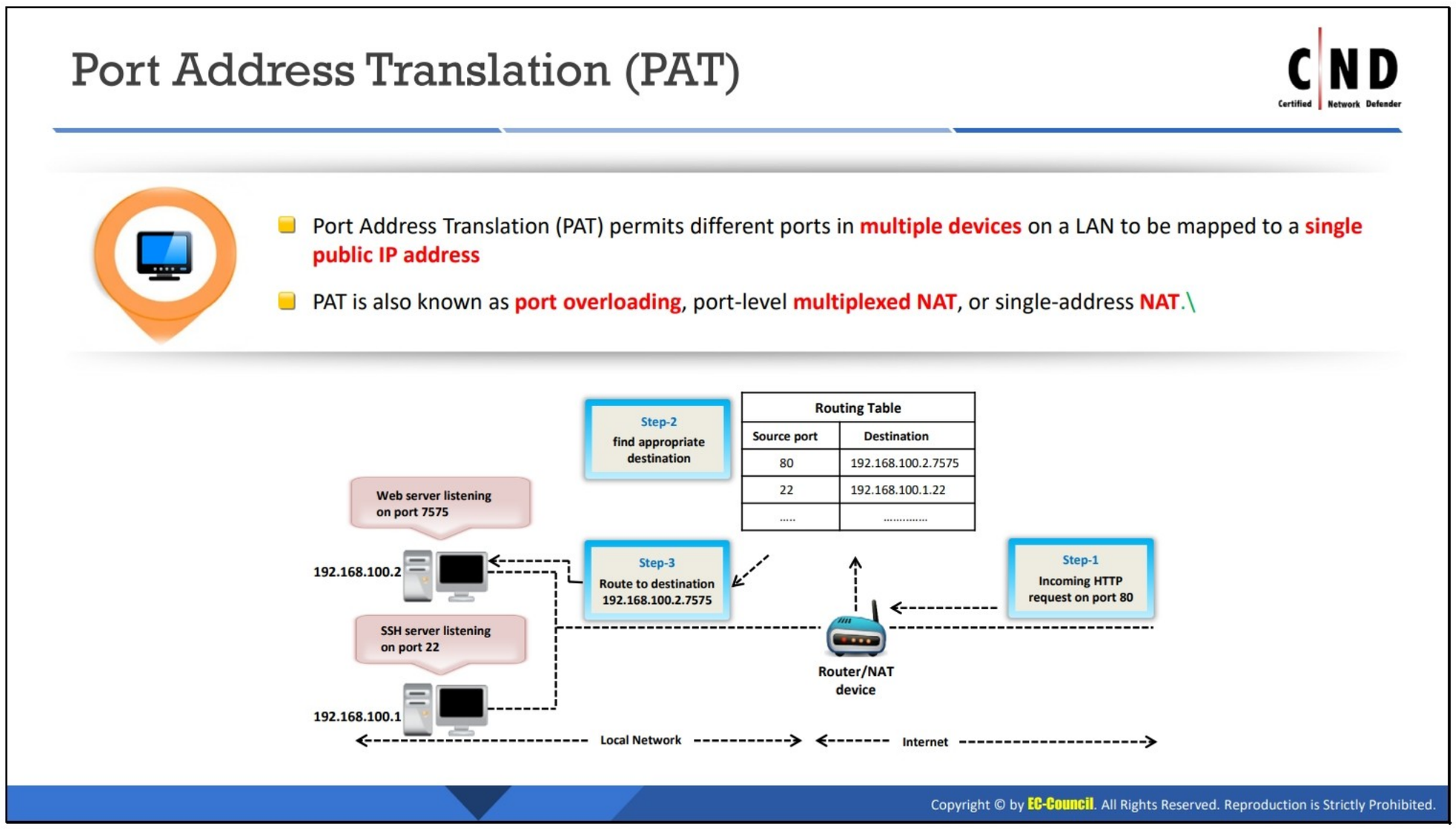
- NAT helps enforce a firewall's control over outbound connections.
- It restricts incoming traffic and allows only packets that are part of a current interaction initiated from the inside.
- It helps hide an internal network's IP addresses, thereby reducing the success of attacks on the network or system.
- NAT conserves IPv4 addresses.
- It simplifies routing.
- It supports a wide range of services.
- It consumes fewer computer resources.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Drawbacks of NAT

- The NAT system must guess how long it should keep a particular translation, which is impossible to guess correctly every time.
- NAT interferes with encryption and authentication systems to ensure the security of data.
- The dynamic allocation of ports may interfere with packet filtering.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Address Translation (PAT)

Port Address Translation (PAT) is an extended form of NAT. It is also known as port overloading, port-level multiplexed NAT, or single-address NAT. It translates the communications occurring between hosts on a private network as well as on a public network.

PAT permits different ports in multiple devices on a LAN to be mapped to a single public IP address. To map different ports in multiple devices to a single public IP address, each private address is tracked by a port number.

A PAT device is located between an external network and an internal network, i.e., at the network perimeter. Its operation is visible to both the external and internal hosts.

Working Principle of PAT

- When a network host located in a private network sends its first data packet to a host in an external network, its source IP address is translated by PAT with a single public IP.
- Subsequently, the PAT device sets a port number to this connection, inserts it in the TCP/UDP header source port, and locates the IP data packet on the external network.
- Next, the PAT device enters information about the internal IP address, TCP or UDP, internal source port, and assigned external port to its translation table.
- Successive data packets from the same TCP connection are always translated by the same external port number.
- The receiver of the data packets located in the external network will change the source IP address and source port with the corresponding destination fields, if it sends a response.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

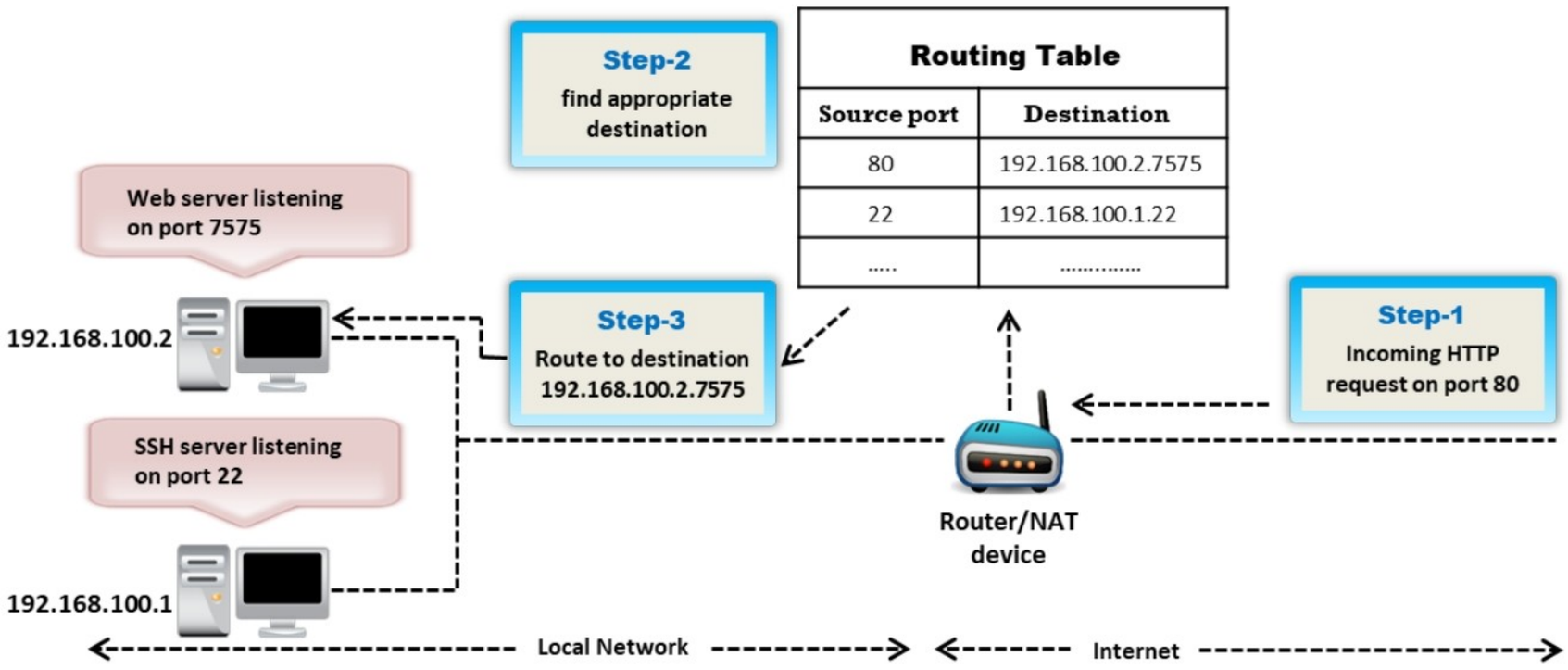


Figure A.93: Port Address Translation

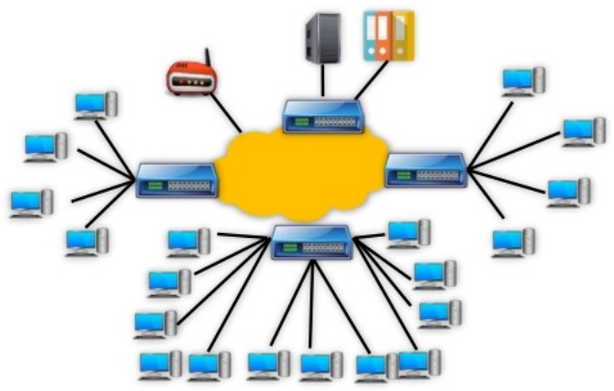
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

VLAN

A virtual LAN (LAN) is a group of networks that are **logically** connected to the same wire and communicate with each other despite being in different **geographical** locations.

These networks are configured through **software** rather than **hardware**

Configuring VLANs is cheaper than creating a **routed network** as routers are costlier than switches



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

VLAN (Cont'd)

Advantages

- VLANs reduce the number of devices for a specific network topology.
- They make the management of physical devices less complex.
- They increase security options by separation and specific frame delivery.
- They contribute to increasing performance and security.
- They facilitate the formation of virtual workgroups.
- They feature simplified administration.
- They reduce cost.

Disadvantages

- VLANs rely on switches to perform well.
- Packet leaks occur from one VLAN to the next.
- Packets can be injected into a VLAN for launching an attack.
- Solved by IPsec.

Security Implications of VLANs

- Keeps hosts separated by VLANS and limits what devices can talk to those hosts
- Increases security options by separation and specific frame delivery
- Controls inter-VLAN routing through the use of IP access lists
- Deploys VTP domain, VTP pruning, and password protections
- Ensures physical security

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Virtual Local Area Network

A virtual LAN (VLAN) is a group of networks that are logically connected to the same wire and communicate with each other despite being in different geographical locations. These networks are configured through software rather than hardware. Configuring VLANs is cheaper than creating a routed network as routers are costlier than switches.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

A VLAN behaves as a physical LAN, but it can group different hosts together, even if they are not directly linked to the same network. Moreover, it also partitions the network into different broadcast domains according to the functional and security requirements of the network system.

VLAN uses the VLAN tagging technique, in which a VLAN ID is inserted into a packet header to determine the VLAN to which the packet belongs.

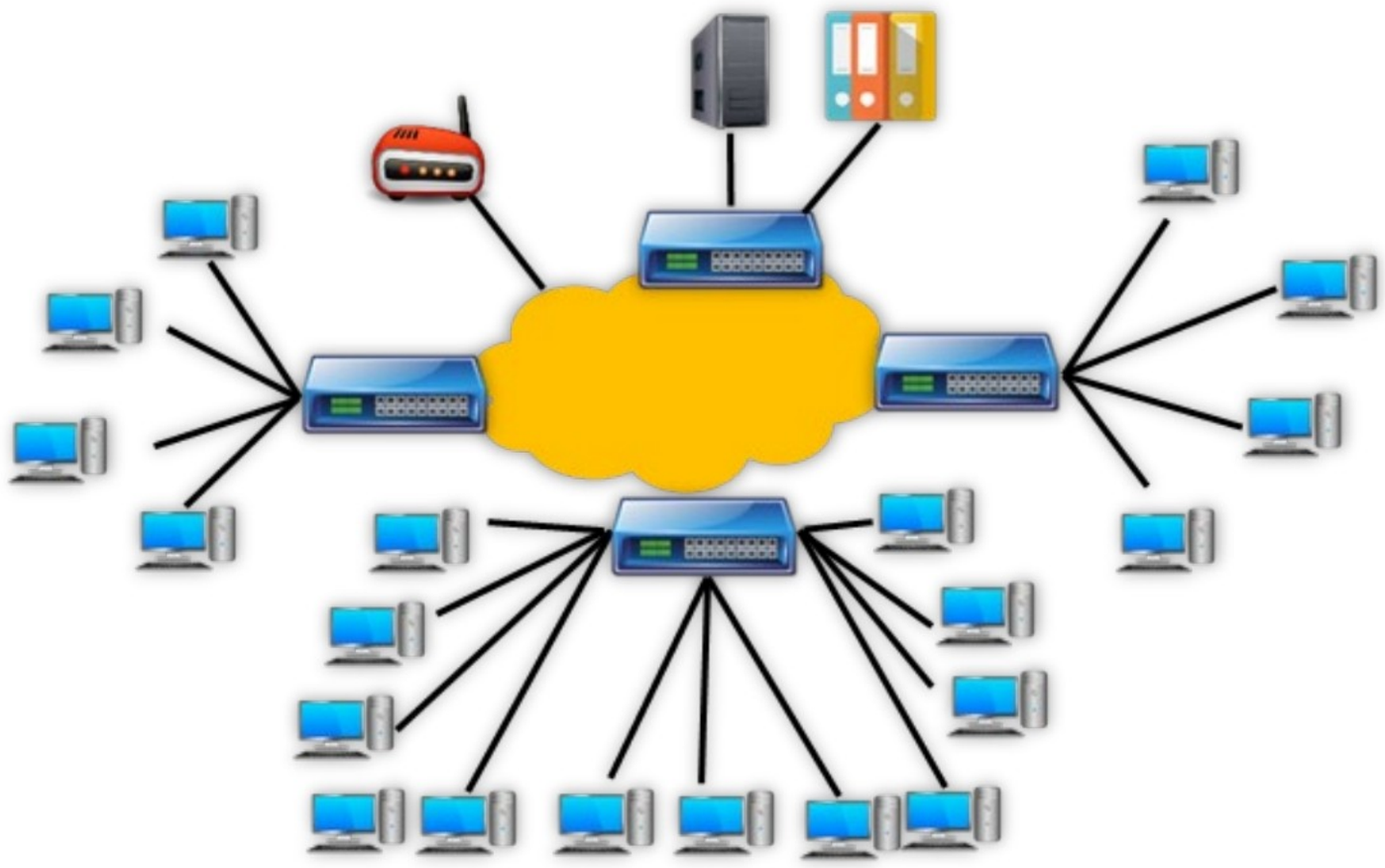


Figure A.94: Virtual Local Area Network

Advantages

- VLANs reduce the number of devices for a specific network topology.
- They make the management of physical devices less complex.
- They increase security options by separation and specific frame delivery.
- They contribute to increasing performance and security.
- They facilitate the formation of virtual workgroups.
- They feature simplified administration.
- They reduce cost.

Disadvantages

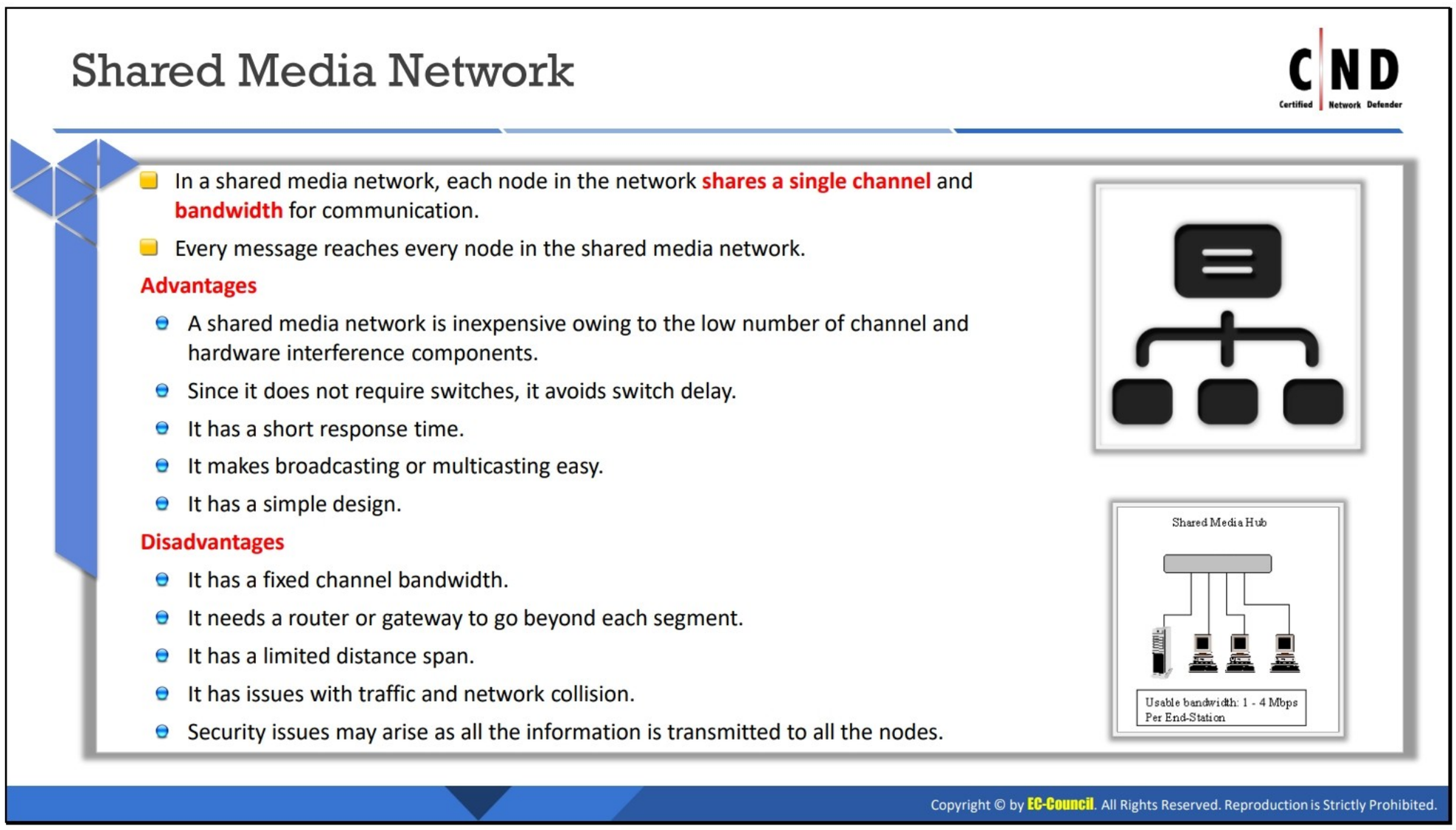
- VLANs rely on switches to perform well.
- Packet leaks occur from one VLAN to the next.
- Packets can be injected into a VLAN for launching an attack.
- Solved by IPsec

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Security Implications of VLANs

- Hosts can be kept separated by VLANs to limit which devices can talk to those hosts.
- Security options can be increased by separation and specific frame delivery.
- Inter-VLAN routing can be controlled using IP access lists.
- VTP domain, VTP pruning, and password protections can be deployed.
- VLANs ensure physical security.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Shared Media Network

In a shared media network, each node in the network shares a single channel and bandwidth for communication. Every message reaches every node in the shared media network, in the form of data packets. A data packet contains an address field that specifies the intended recipient. When a node receives a packet, it checks the address field. If a packet belongs to that node, it processes the packet; otherwise, it ignores that packet.

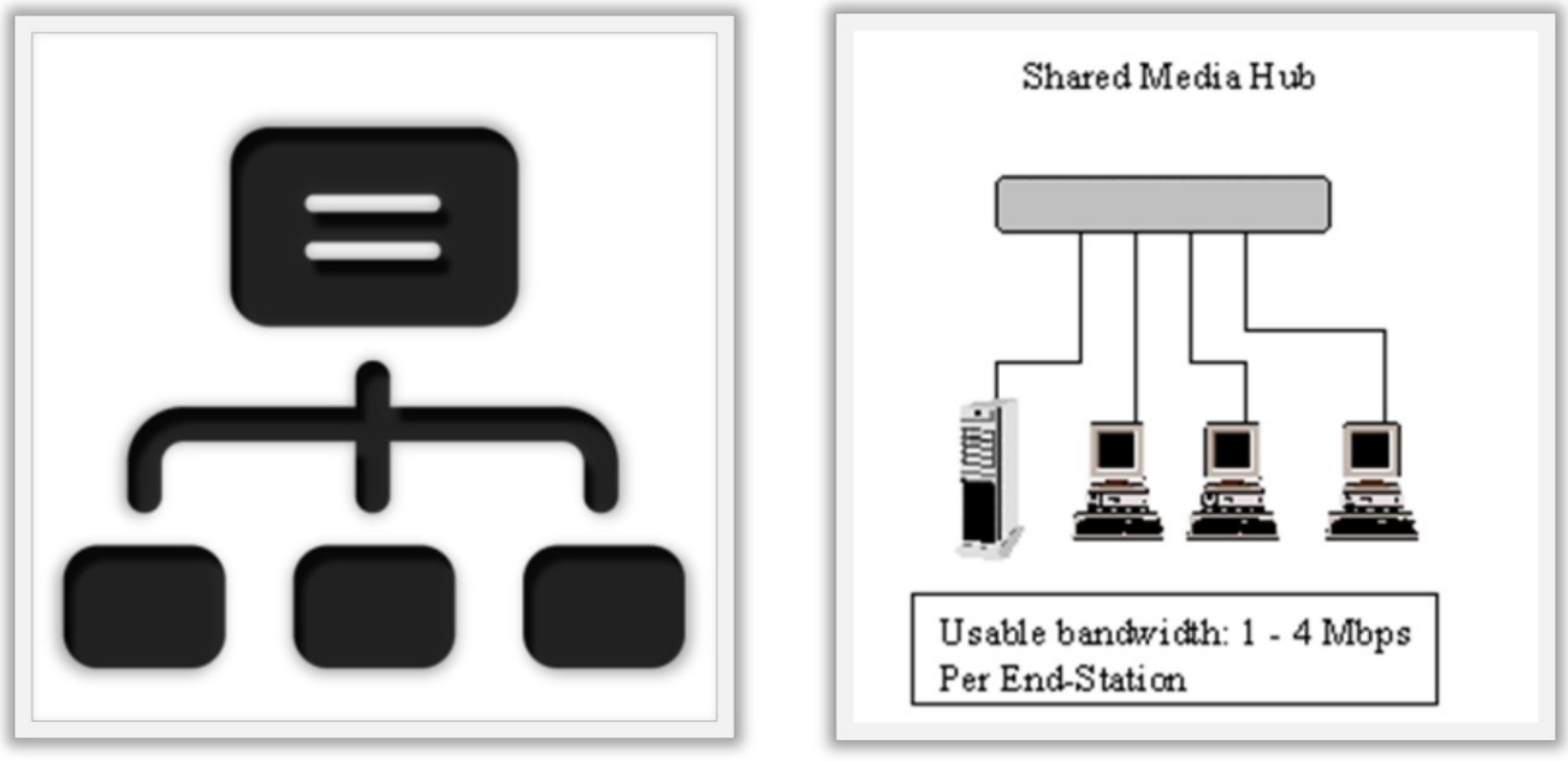


Figure A.95: Shared Media Networks

Some shared media networks such as Ethernet support broadcasting and multicasting mechanisms, where data are transmitted to multiple nodes simultaneously.

Advantages

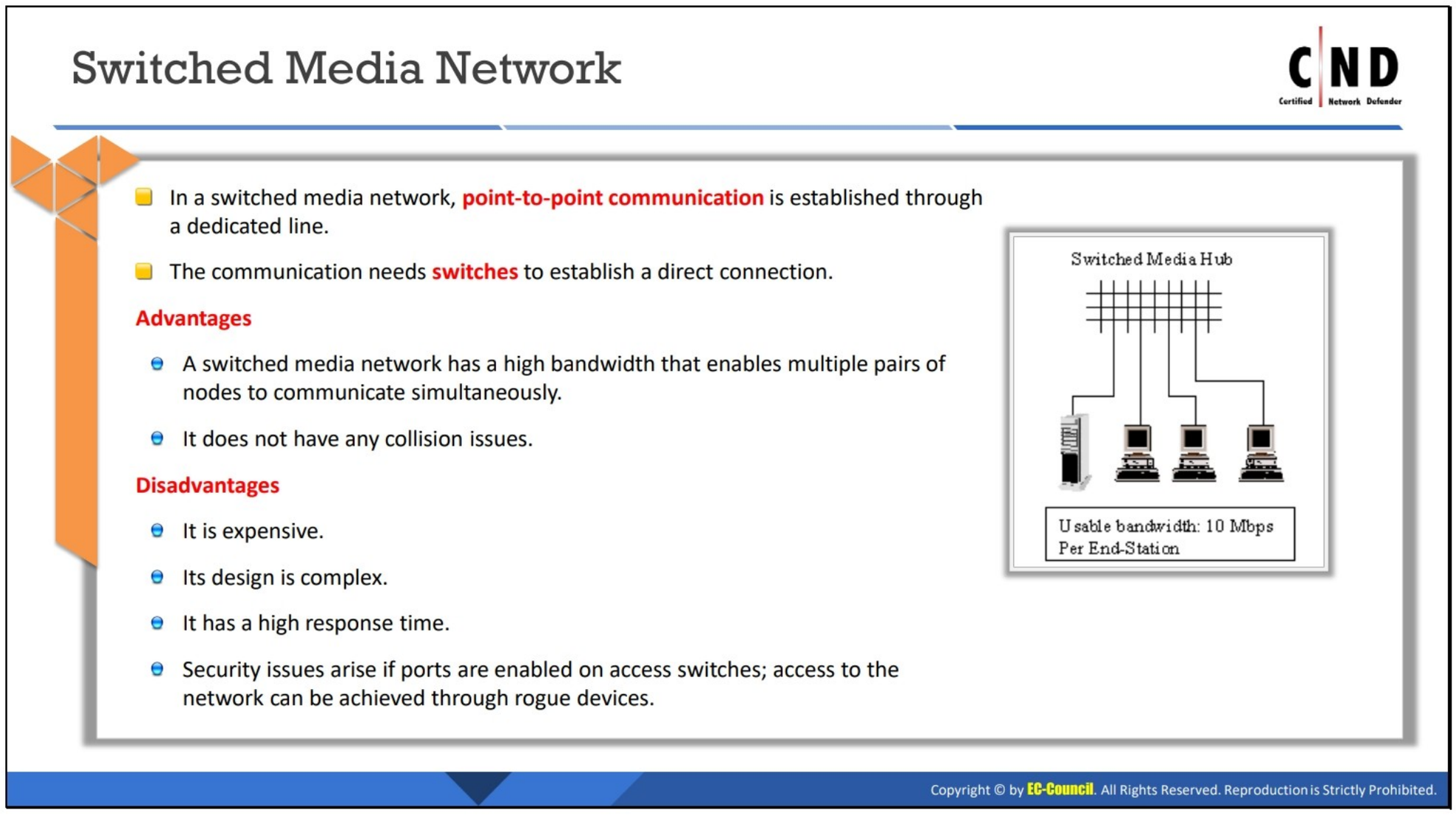
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- A shared media network is inexpensive owing to the low number of channel and hardware interference components.
- Since it does not require switches, it avoids switch delay.
- It has a short response time.
- It makes broadcasting or multicasting easy.
- It has a simple design.

Disadvantages

- A shared media network has a fixed channel bandwidth.
- It needs a router or gateway to go beyond each segment.
- It has a limited distance span.
- It has issues with traffic and network collision.
- Security issues may arise as all the information is transmitted to all the nodes.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Switched Media Network

In a switched media network, point-to-point communication is established through a dedicated line. The communication needs a switch to establish a direct connection.

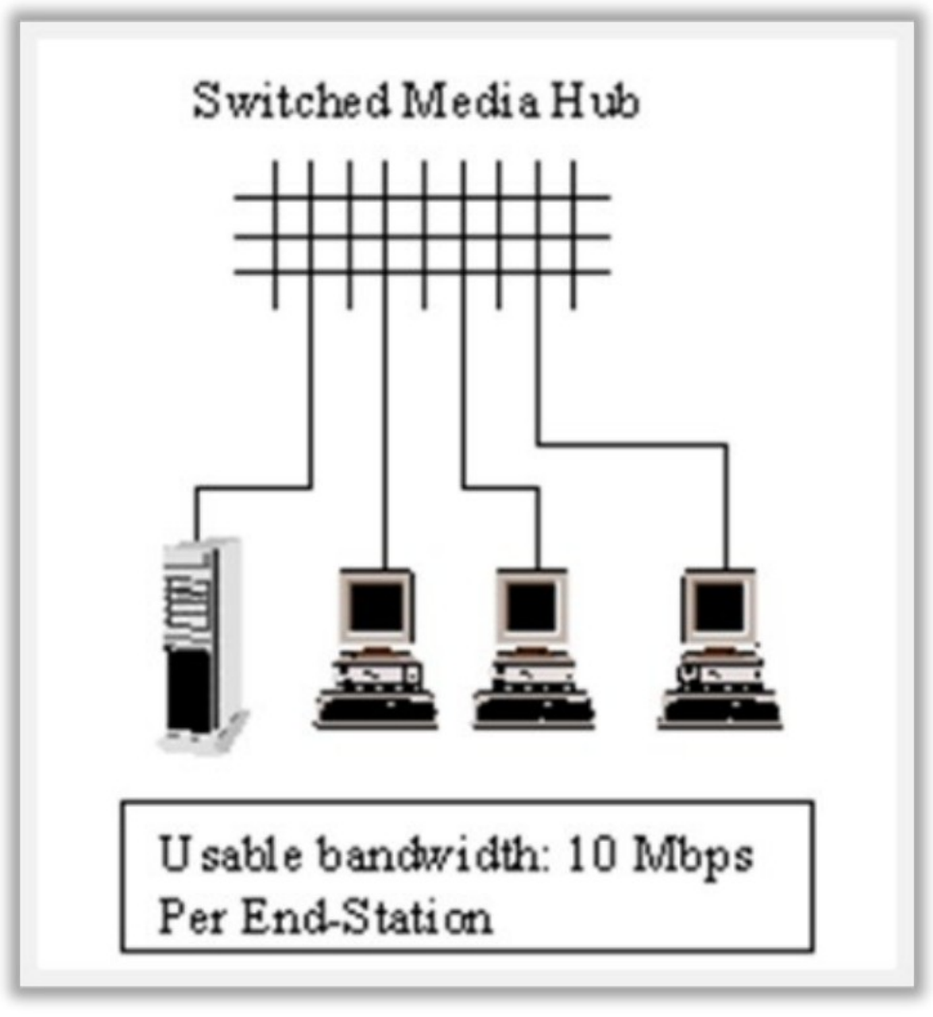


Figure A.96: Switched Media Network

Switched media network is divided into three types: circuit switched network, message switched network, and packet switched network.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Circuit switched network**: A circuit switched network establishes a dedicated communication channel ("circuit") between the sender and the receiver throughout the connection. In this type of network, routing decisions are made at the time of circuit establishment.
- **Message switched network**: Unlike a circuit switched network, a message switched network does not establish a dedicated communication channel between the sender and receiver. In this type of network, a node sends a message by appending the destination address in it. Here, messages are transmitted from node to node throughout the network. When a node receives a message, it stores the message on its disk until the next device is ready to receive it and forwards the message to the next node. Therefore, this network is also known as store-and-forward switching.
- **Packet switched network**: A packet switched network breaks a message into small parts known as data packets. Each packet contains a header with a source, a destination, and intermediate node addresses. Moreover, each packet takes different routes to reach the respective destination.

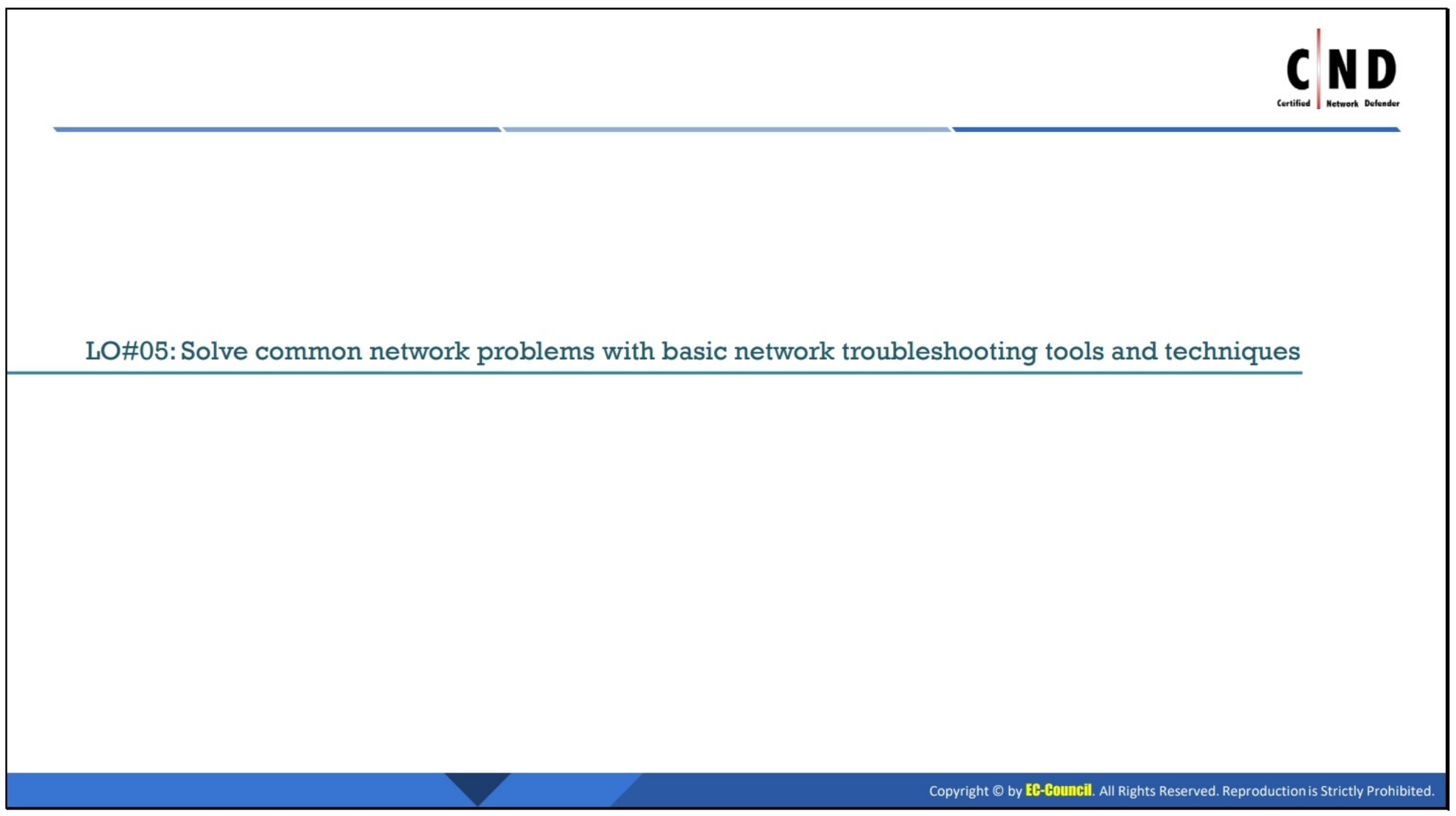
Advantages

- A switched media network has a high bandwidth that enables multiple pairs of nodes to communicate simultaneously.
- It does not have any collision issues.

Disadvantages

- Switched media networks are expensive.
- Their design is complex.
- They have a high response time.
- Security issues arise if ports are enabled on access switches; access to the network can be achieved through rogue devices.

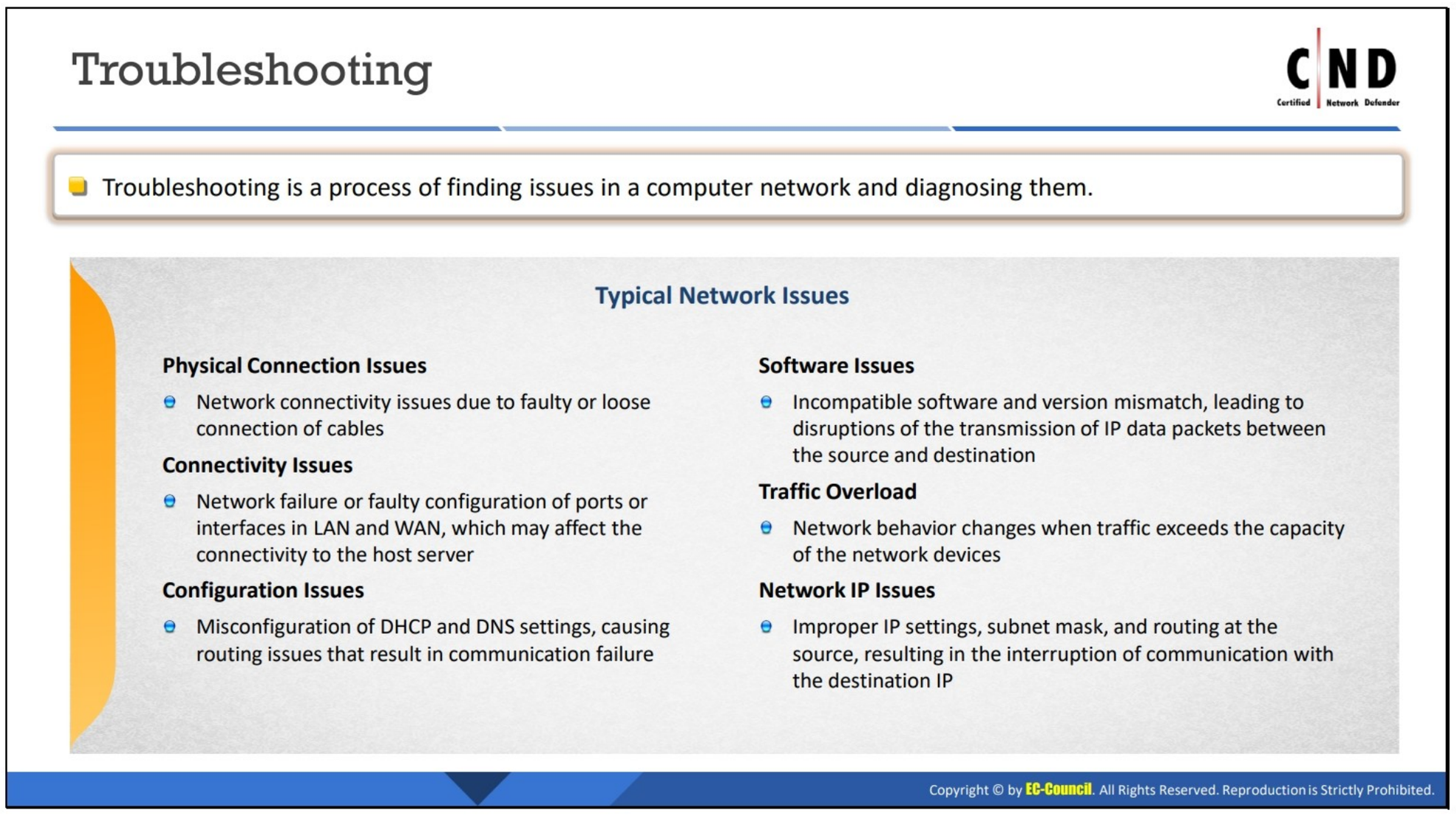
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#05: Solve Common Network Problems with Basic Network Troubleshooting Tools and Techniques

This section discusses common network issues and various troubleshooting techniques to resolve them. It introduces some troubleshooting utilities such as ping, traceroute/tracert, ipconfig/ifconfig, nslookup, netstat, and PuTTY/Tera Term.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Troubleshooting

Troubleshooting is a process executed by network engineers/administrators to find issues in a computer network and diagnose them to enhance the network performance. It comprises systematic measures and processes to identify, diagnose, and resolve network issues to recover normal network operations on end nodes. Troubleshooting is primarily performed by network engineers/administrators. The process of troubleshooting can be performed manually or by using automated tools (network diagnostic software).

Some of the processes involved in network troubleshooting are as follows:

- Finding and resolving the faulty network connection of a system
- Configuring network devices (routers, switches, etc.)
- Installing physical equipment (cables, Wi-Fi devices, etc.)
- Updating firmware devices
- Removing viruses using antivirus software
- Adding, configuring, and reinstalling devices

Typical Network Issues

The issues that generally occur in a network are as follows:

- **Physical connection issues:** These issues occur due to faulty, shortened, or damaged cables in a network. For example, cut cables, incorrect cable connections, and connector problems may result in poor network connectivity.
- **Connectivity issues:** These issues are caused by faulty/physical shutting down of the port or interface on which devices are connected in a LAN or WAN. For example, the

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

malfunction of a hub, router, or switch may affect the network connectivity with the host server.

- **Configuration issues:** These issues occur due to the faulty configuration of DHCP and DNS settings, routing issues, IP looping, etc. and may result in communication failure.
- **Software issues:** These issues are caused by software compatibility issues and mismatched software versions. These may result in the interruption of the transmission of IP data packets between the source and destination.
- **Traffic overload issues:** These issues occur due to traffic that exceeds the normal capacity of a network device. For example, transfers of an excessive amount of information due to a poor network setup may result in abnormal network behavior or slow connectivity.
- **Network IP issues:** These issues are caused by the faulty configuration of IP addresses, subnet masks, and routing at the source and may result in interruption in reaching the destination IP through the network.

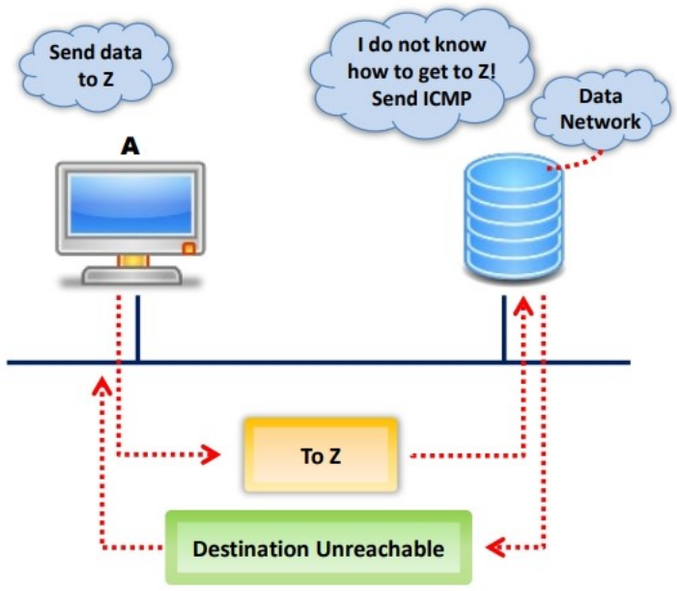
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Example of Issues: Unreachable Networks

- **Network communication** depends on certain basic conditions being met.
  - Sending and receiving devices must have the TCP/IP protocol stack properly configured:
    - The IP address and subnet mask must be properly configured.
    - A default gateway must also be configured if datagrams are to travel outside of the local network
  - A router must also have the TCP/IP protocol stack properly configured on its interfaces, and it must use an appropriate routing protocol
  - If these conditions are not met, then network communication cannot occur.

Examples of Problems

- The sending device may address the datagram to a non-existent IP address.
- The destination device is not connected to its network.
- The router's connecting interface is down.
- The router does not have the information necessary to find the destination network.

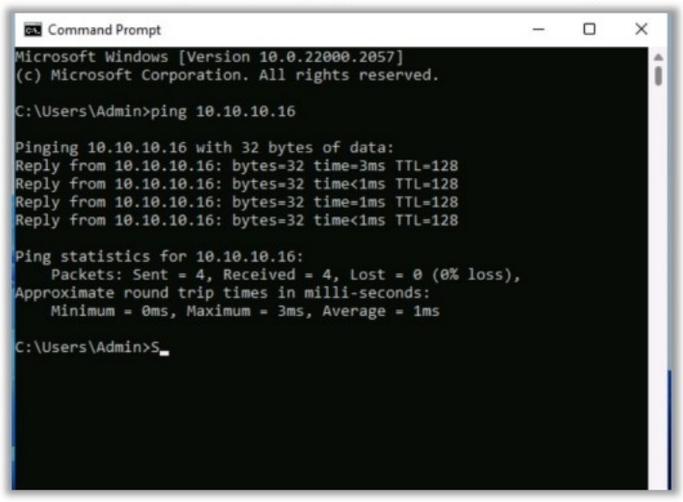


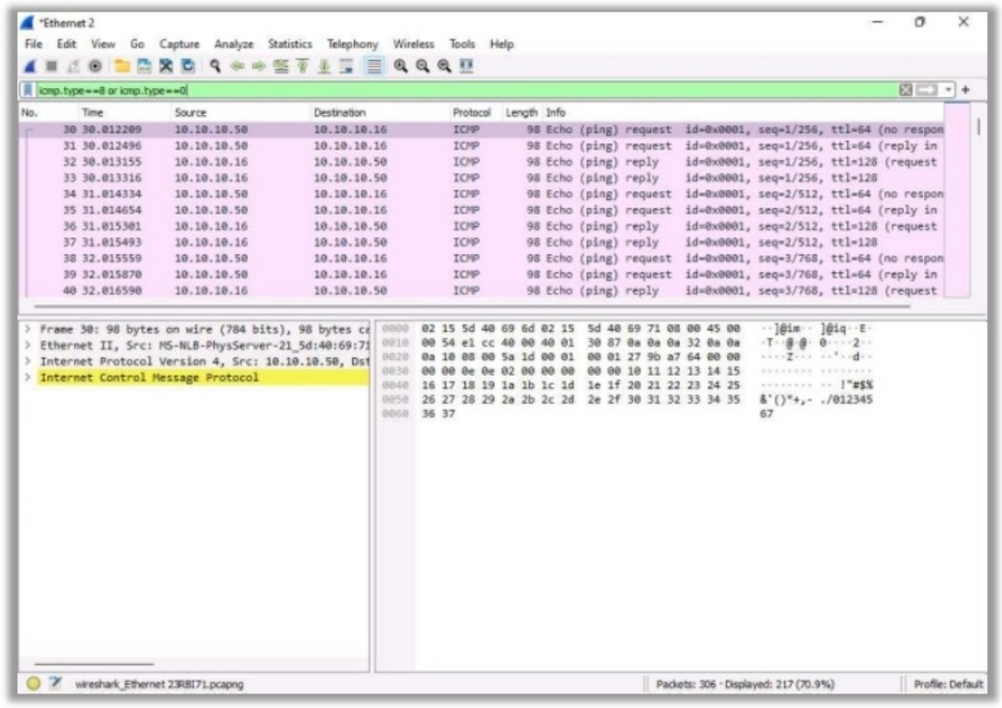
- An ICMP destination **unreachable message** is sent in the case of the following:
  - The host or port is unreachable.
  - The network is unreachable.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Example of Issues: Unreachable Networks (Cont'd)

Echo Request/Reply When host is up



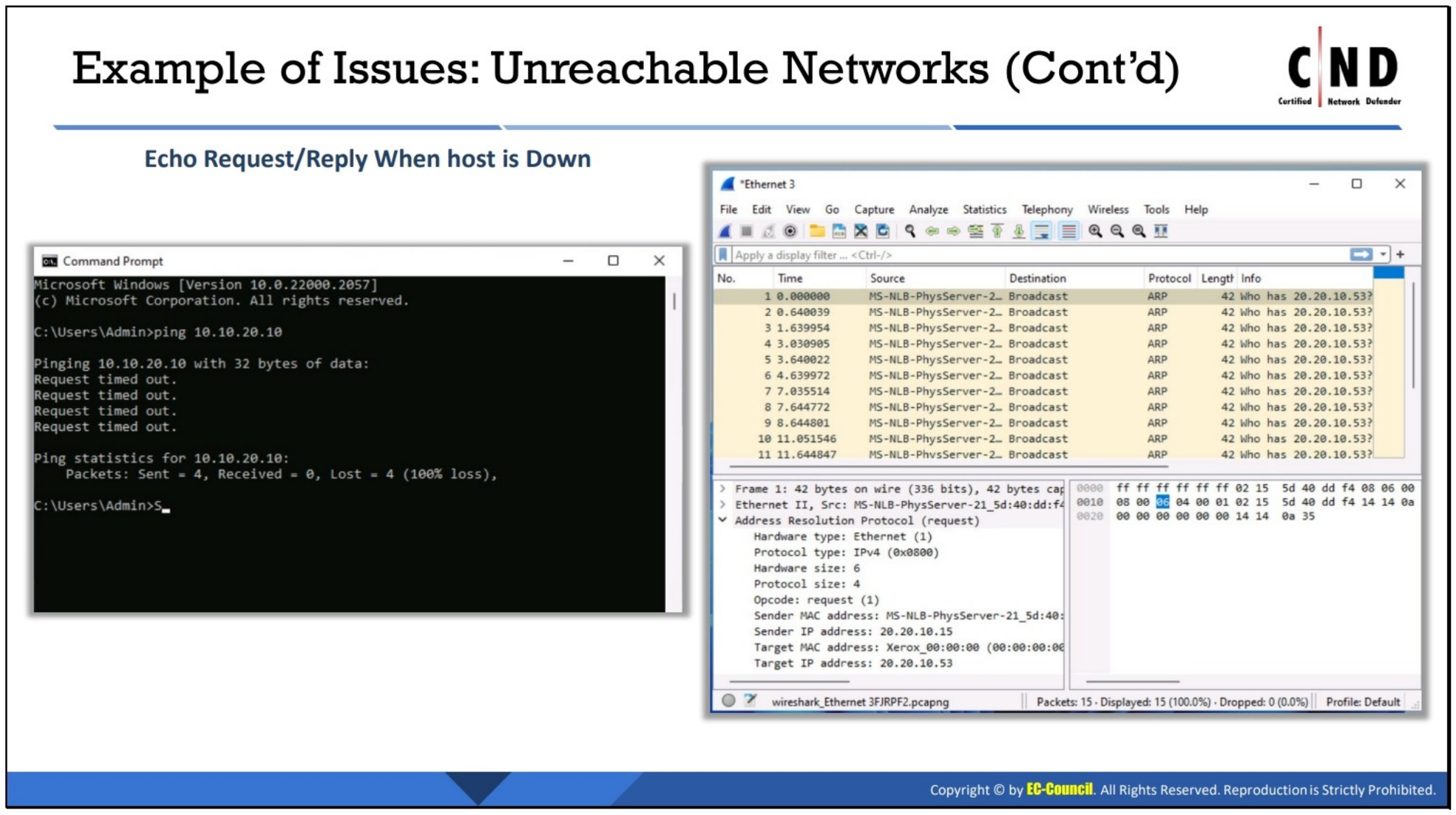


Type (8 bits)	Code (8 bits)	Checksum (16 bits)
Parameters		
Data……		

Echo = Type 8; Echo Reply = Type 0

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Example of Issues: Unreachable Networks

Network communication depends on certain basic conditions being met.

- Sending and receiving devices must have the TCP/IP protocol stack properly configured:
  - The IP address and subnet mask must be properly configured.
  - A default gateway must also be configured if datagrams are to travel outside of the local network.
- A router must also have the TCP/IP protocol stack properly configured on its interfaces, and it must use an appropriate routing protocol.
- If these conditions are not met, then network communication cannot occur.
- The following are examples of problems:
  - The sending device may address the datagram to a non-existent IP address.
  - The destination device is not connected to its network.
  - The router's connecting interface is down.
  - The router does not have the information necessary to find the destination network.
- An ICMP destination unreachable message is sent in the case of the following issues:
  - Host or port unreachable
  - Network unreachable

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

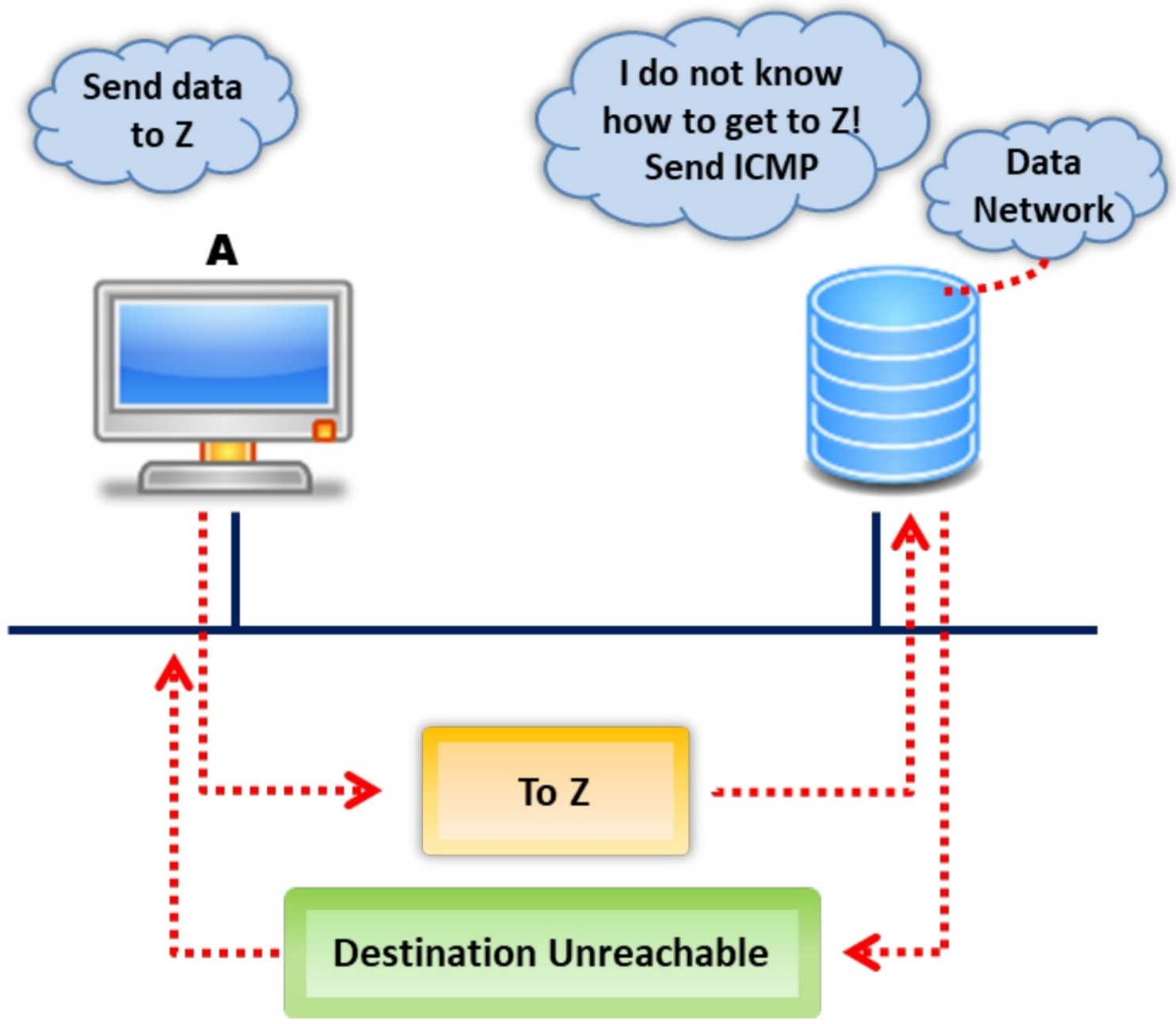


Figure A.97: Unreachable Destination

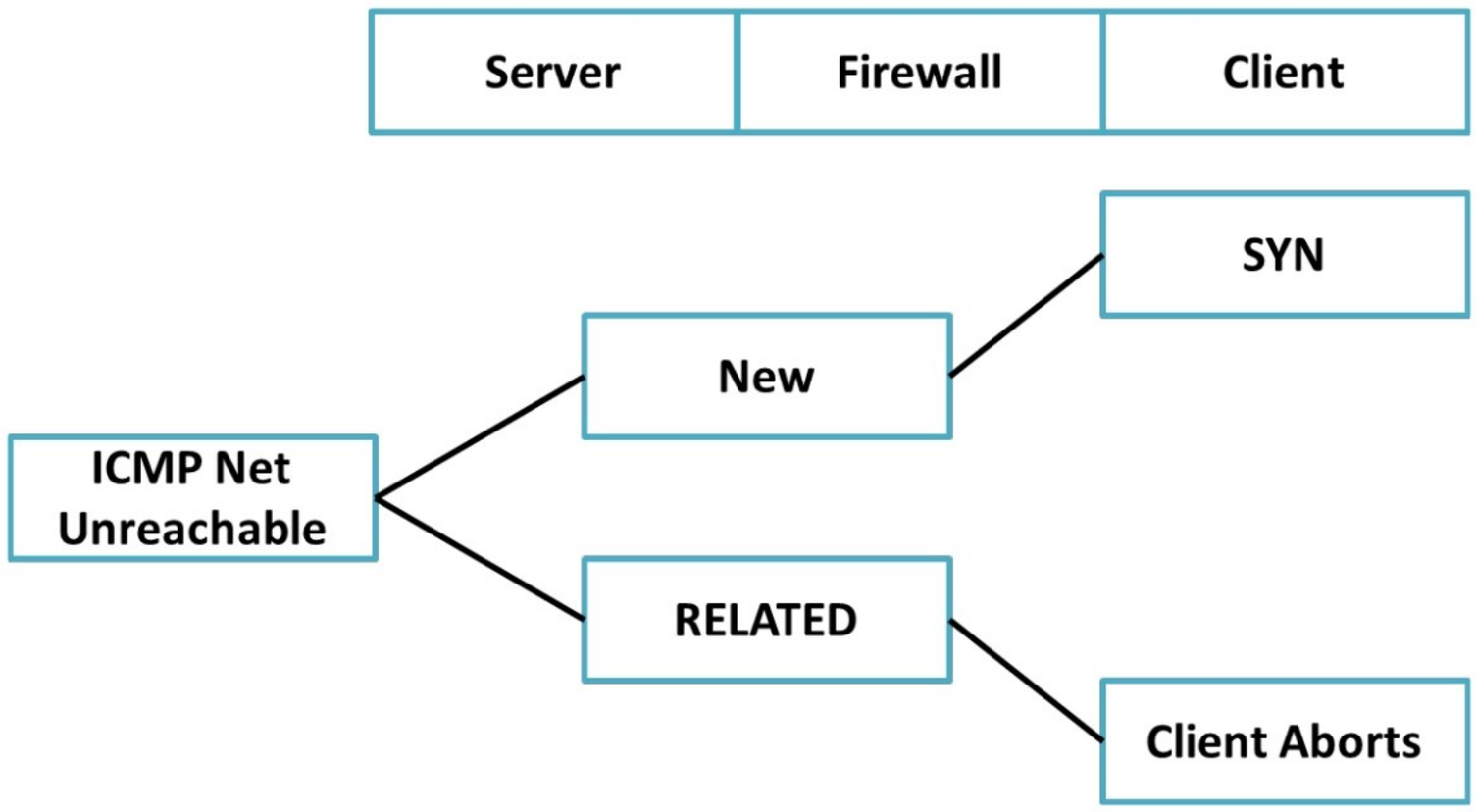


Figure A.98: Unreachable-Destination Problems arising when Specific Conditions are not Met

ICMP Echo (Request) and Echo Reply

An ICMP echo request is a query-based ICMP message that helps in diagnosing a network. By using this message, a system in the network can be tested to verify whether it is ready for data transmission. To do so, the first system that wishes to communicate with another system sends

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

an ICMP echo request message. If the second system is ready for the communication, it responds with an ICMP echo reply message.

Format of ICMP Echo Requests and Replies

Figure A.99 shows the fields in an ICMP echo request/reply.

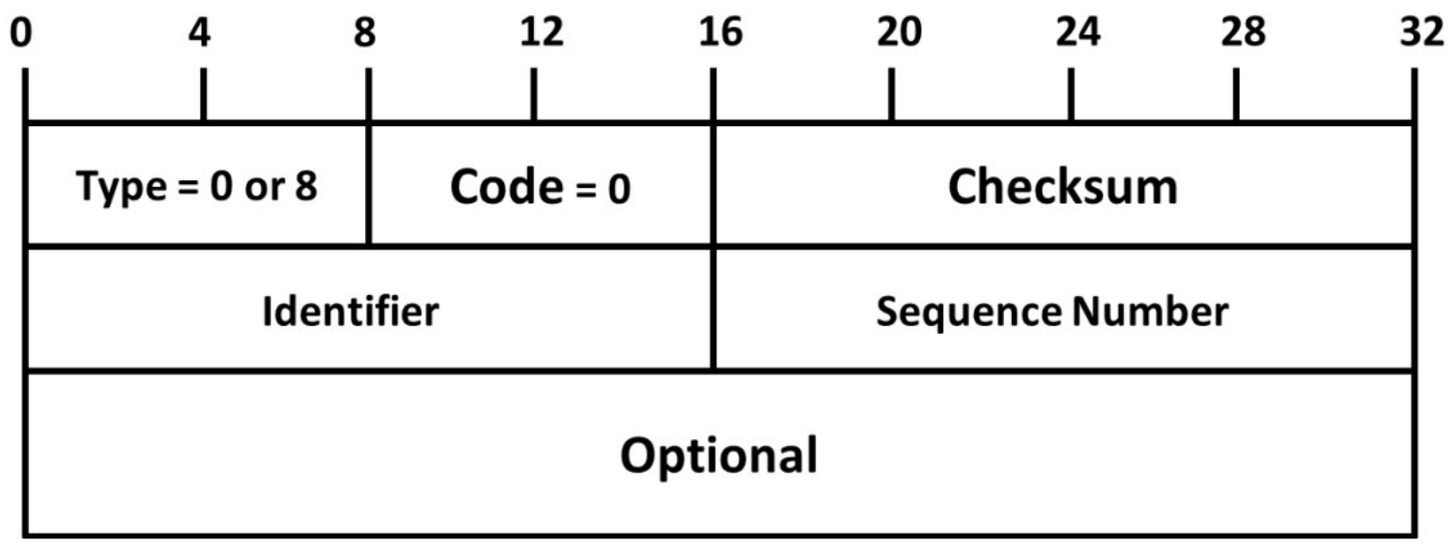


Figure A.99: Format of an ICMP Echo Request/Reply

Each field in the ICMP echo request/reply format is described below.

- **Type (1 byte)**: This field defines the type of the ICMP message. For an ICMP echo request, its value is 8, and for an ICMP echo reply, its value is 0.
- **Code (1 byte)**: This field does not define anything for these message types; therefore, it is set to 0.
- **Checksum (2 bytes)**: This field defines a checksum for the ICMP header.
- **Identifier (2 bytes)**: This field is used to compare echo request and echo reply messages.
- **Sequence number (2 bytes)**: This field contains a number for comparing echo request and echo reply messages.
- **Optional (variable)**: This is an optional field that contains information about the message.

ICMP echo requests and replies can be sent through the ping command. This command provides important information such as how many echo request messages were pinged, the message size, and how many responses were received.

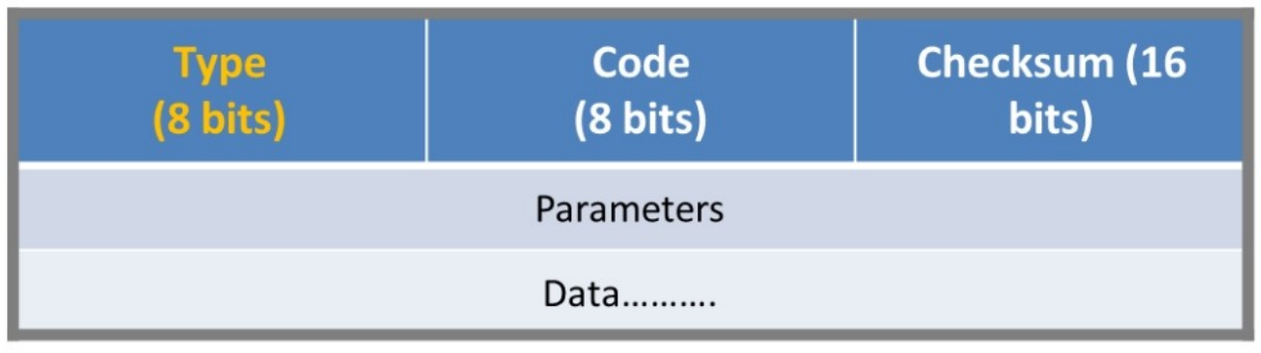


Figure A.100: ICMP Echo and Response

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

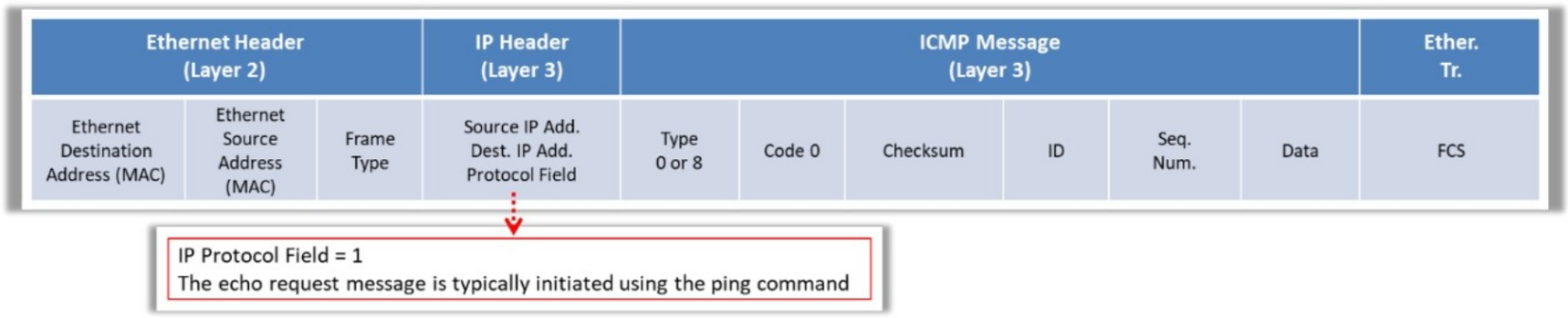
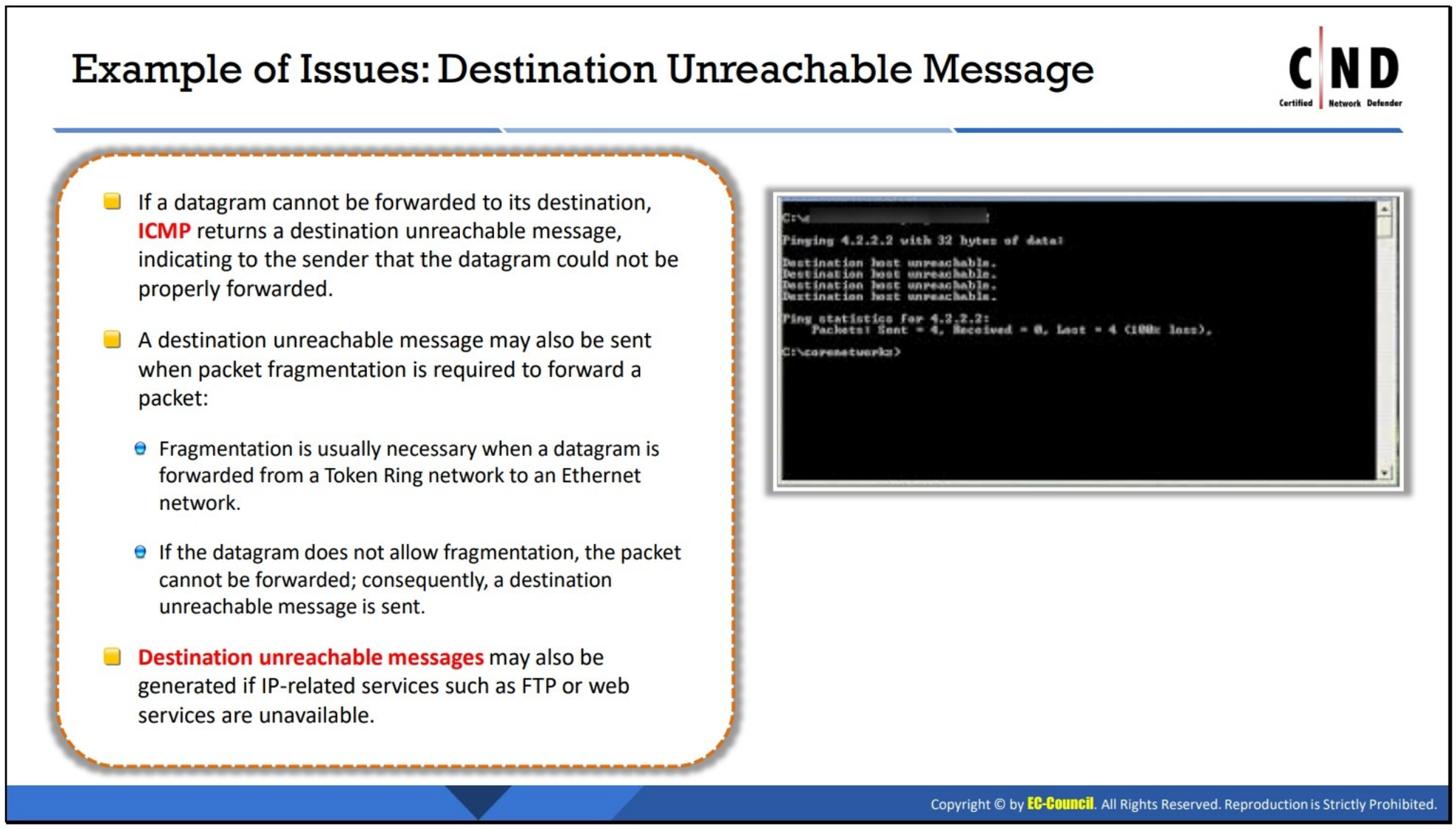


Figure A.101: ICMP Frame

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Example of Issues: Destination Unreachable Message

We have already discussed the concept of unreachable networks in previous sections. As we know, IP is a connectionless protocol that does not consider the information being sent. If a host that IP attempts to send information to is unavailable, this has to be notified to IP. This notification can be accomplished using ICMP destination unreachable message.

If a datagram cannot be forwarded to its destination, ICMP returns a destination unreachable message indicating to the sender that the datagram could not be properly forwarded.

A destination unreachable message may also be sent when packet fragmentation is required to forward a packet:

- Fragmentation is usually necessary when a datagram is forwarded from a Token Ring network to an Ethernet network.
- If the datagram does not allow fragmentation, the packet cannot be forwarded; consequently, a destination unreachable message is sent.

Destination unreachable messages may also be generated if IP-related services such as FTP or web services are unavailable.

Figure A.102 shows the fields in an ICMP destination unreachable message.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

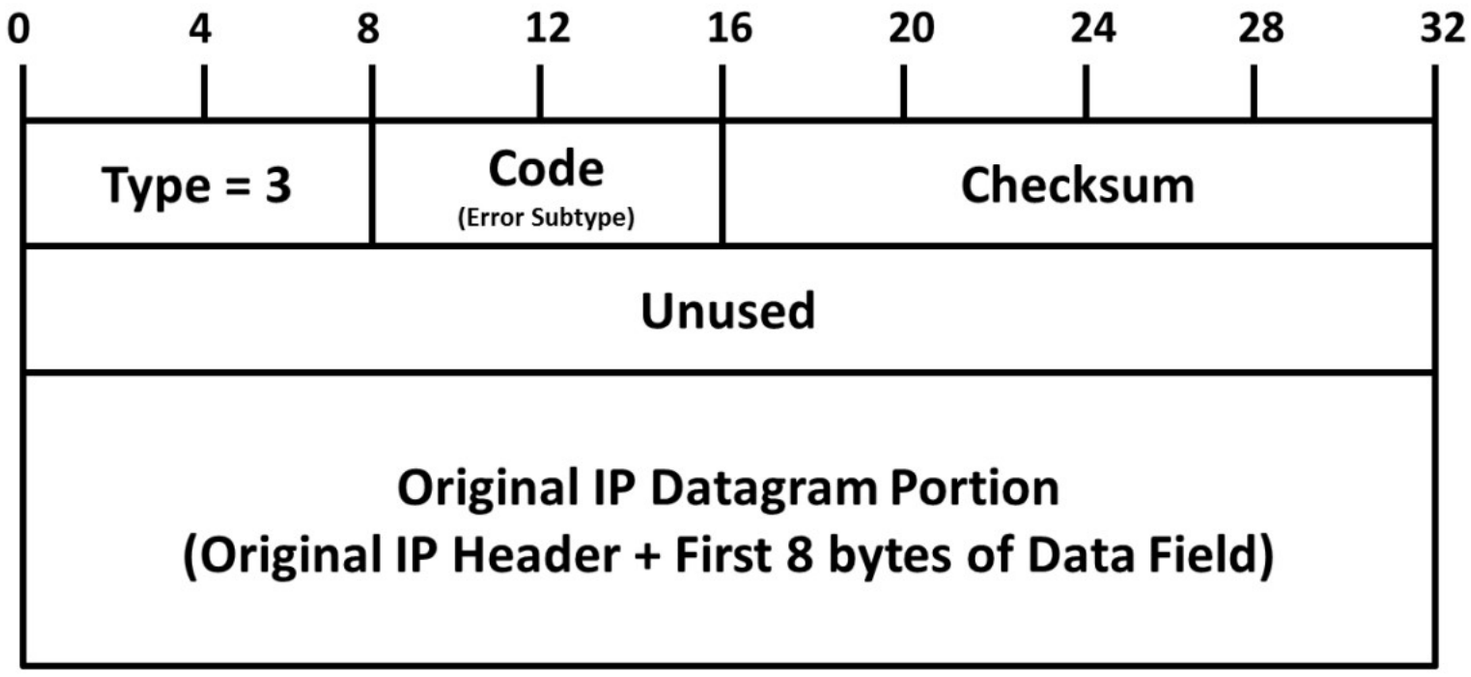
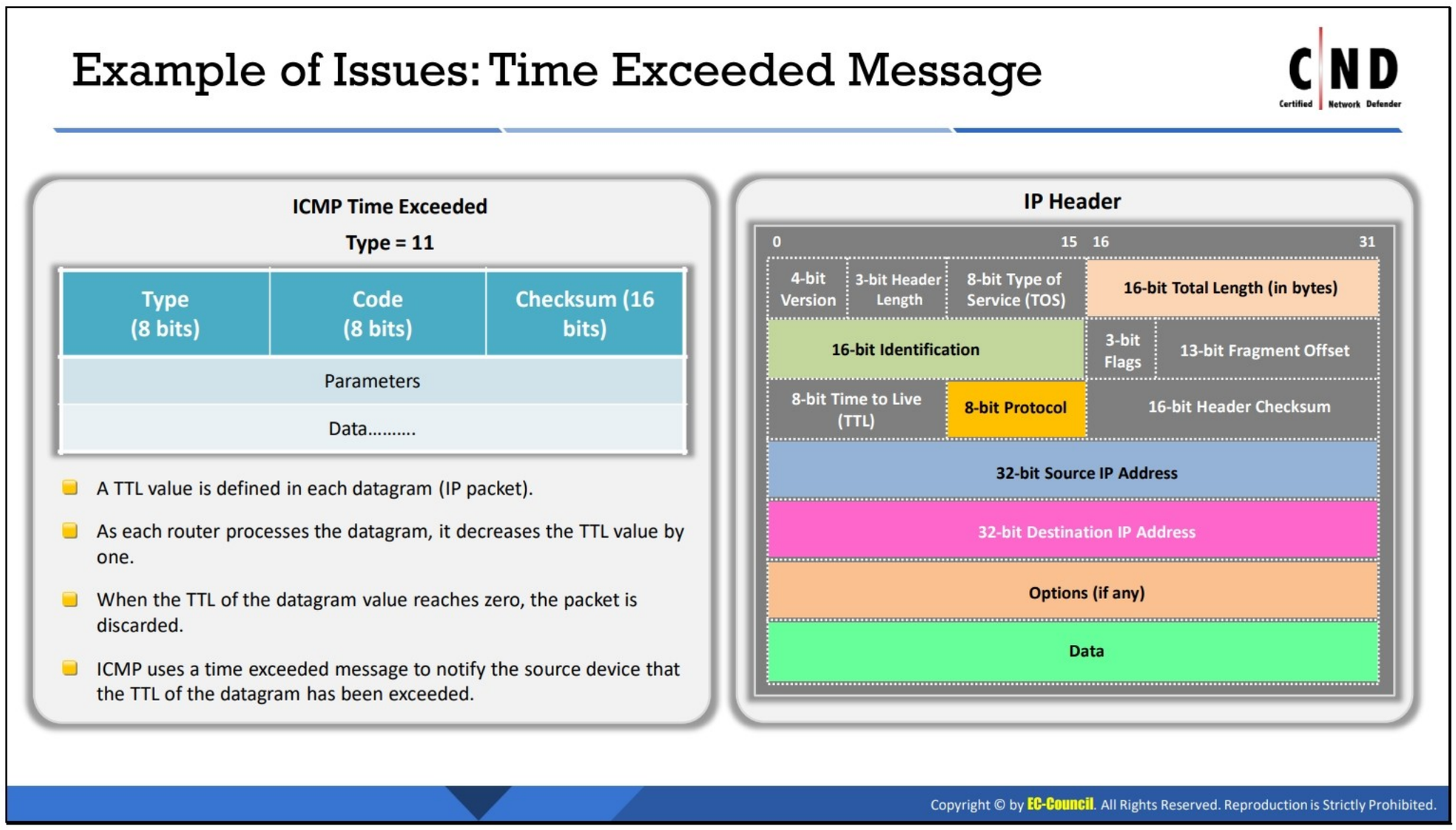


Figure A.102: Format of an ICMP Destination Unreachable Message

Each field in the ICMP destination unreachable message is described below.

- **Type (1 byte)**: This field defines the type of the ICMP message; for a destination unreachable message, its value is 3.
- **Code (1 byte)**: This field defines the reason behind the error, and a series of numbers represent various types of errors; for example, code 0 represents a network unreachable error, and code 1 represents a host unreachable error.
- **Checksum (2 bytes)**: This field defines a checksum for the ICMP header.
- **Unused (4 bytes)**: This field is left blank.
- **Original datagram portion (variable)**: This field defines the IP header of the datagram and the first 8 bytes of the datagram that prompted this error message to be sent.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Example of Issues: Time Exceeded Message

In huge networks with hundreds of interconnected devices, the packet delay is a common problem. This delay might be caused by too many routers to choose the shortest path, router issues, router loop, etc.

The router loop problem arises in the following kind of scenario:

- Let there be two networks exchanging information.
- The first network sends a packet to router R1, and R1 must choose the shortest path to reach the second network.
- R1 chooses router R2 as the shortest path and sends the packet to it.
- R2 chooses router R3 as the shortest path and sends the packet to it.
- R3 chooses router R1 as the shortest path and sends the packet to it.
- Likewise, the packet loops around these routers indefinitely, causing the router loop problem.

A router loop is a serious problem that causes packets to loop around a network continuously. To avoid this kind of overhead, the IP header of a packet contains a time to live (TTL) field that sets the number of hops the packet can travel. Each time the packet reaches a router, its TTL value reduces by 1, and the process continuous until TTL = 0. At this moment, the packet loses its lifetime and expires. The device at which the packet expired, sends an ICMP time exceeded message to the source machine that sent the packet.

Figure A.103 shows the TTL expiry scenario.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

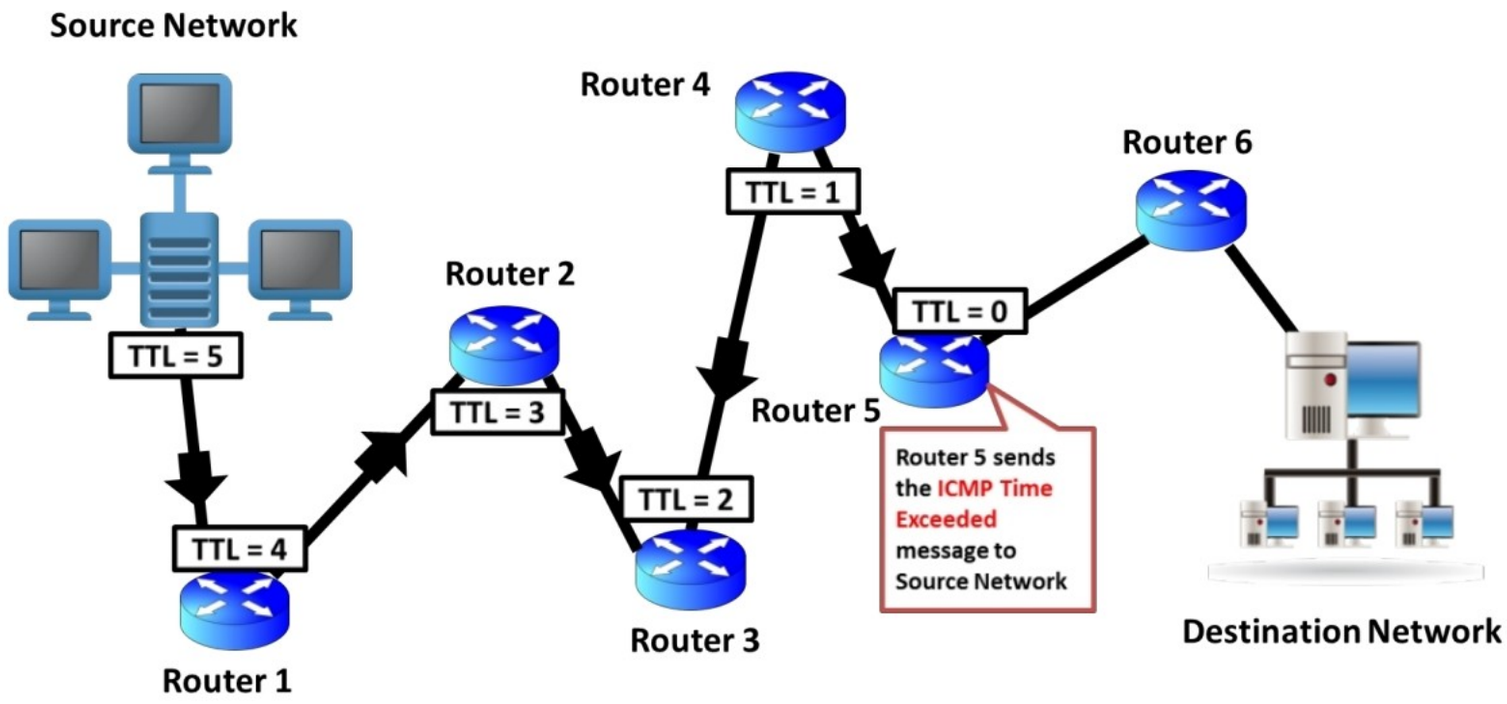


Figure A.103: TTL Expiry Scenario

There is another scenario that leads to packet expiry and creates an error message. In certain situations, the IP packet is fragmented into small parts; these fragments choose different routing paths to reach the destination. It is the duty of the destination machine to join all these fragments into a full packet after the arrival of all the packets. If a fragment took the shortest path and reached the destination while the others are yet to reach, the destination host must wait till it gathers all the fragments. This may cause the destination host to wait for a long or even indefinite amount of time if any fragments was lost. To avoid such a scenario, the destination host sets a timer when it collects the first fragment and waits for the others. If this timer expires, the destination host discards the fragments that it received and sends an ICMP time exceeded message to the source host.

The ICMP time exceeded message contains the following fields.

- **Type (1 byte)**: This field defines the type of ICMP message; for a time exceeded message, it is set to 11.
- **Code (1 byte)**: This field defines the reason behind the error, and a series of numbers represent various types of errors; for example, code 0 represents the expiration of TTL, and code 1 represents fragment reassembly timeout.
- **Checksum (2 bytes)**: This field defines a checksum for the ICMP header.
- **Unused (4 bytes)**: This field is not used and left blank.
- **Original datagram portion**: This field contains the IP header and first 8 bits of the IP packet that was discarded because of the time exceeded error.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ICMP Time Exceeded

Type = 11

Type (8 bits)	Code (8 bits)	Checksum (16 bits)
Parameters		
Data.....		

Figure A.104: ICMP Time Exceeded Frame

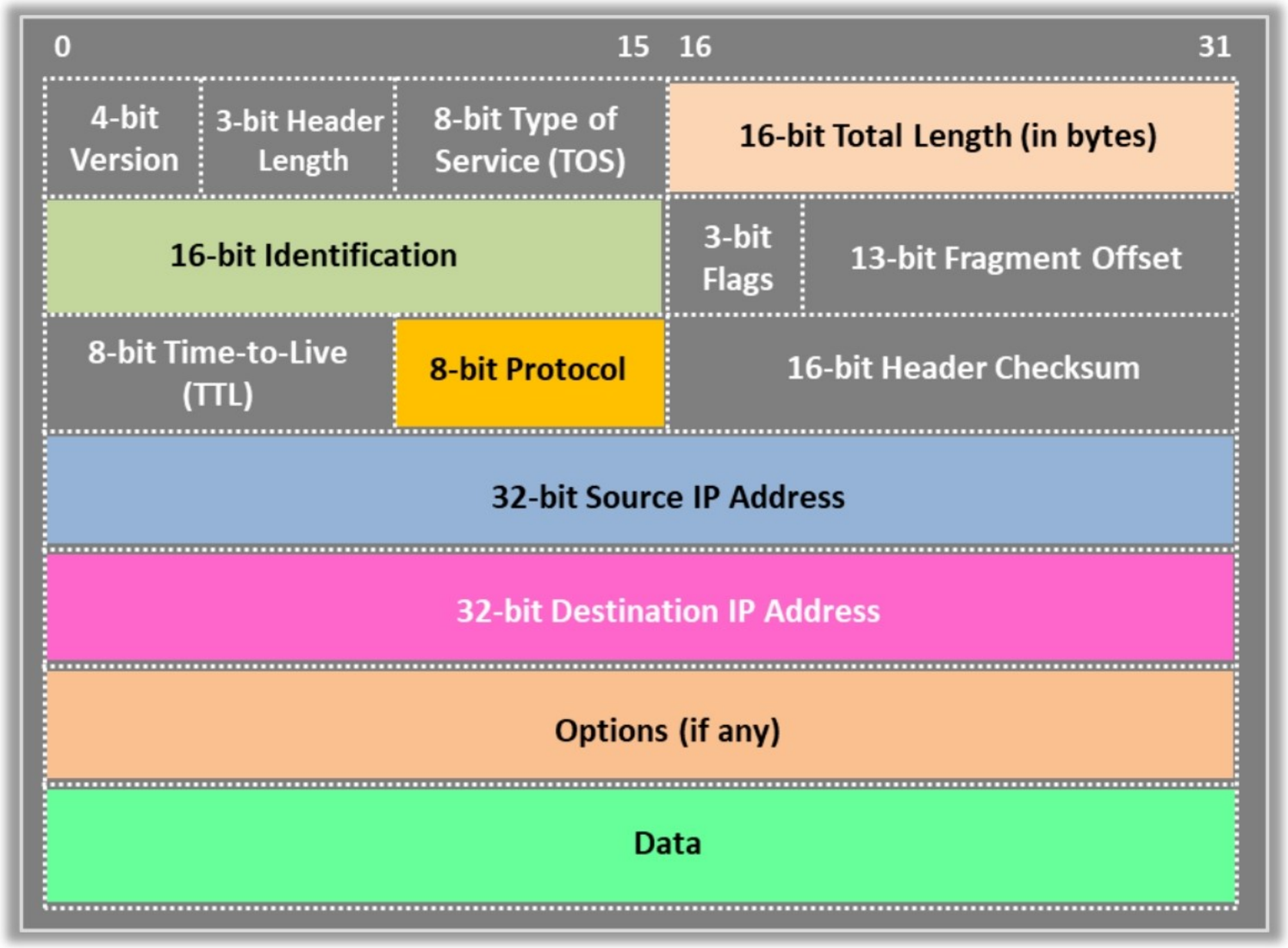
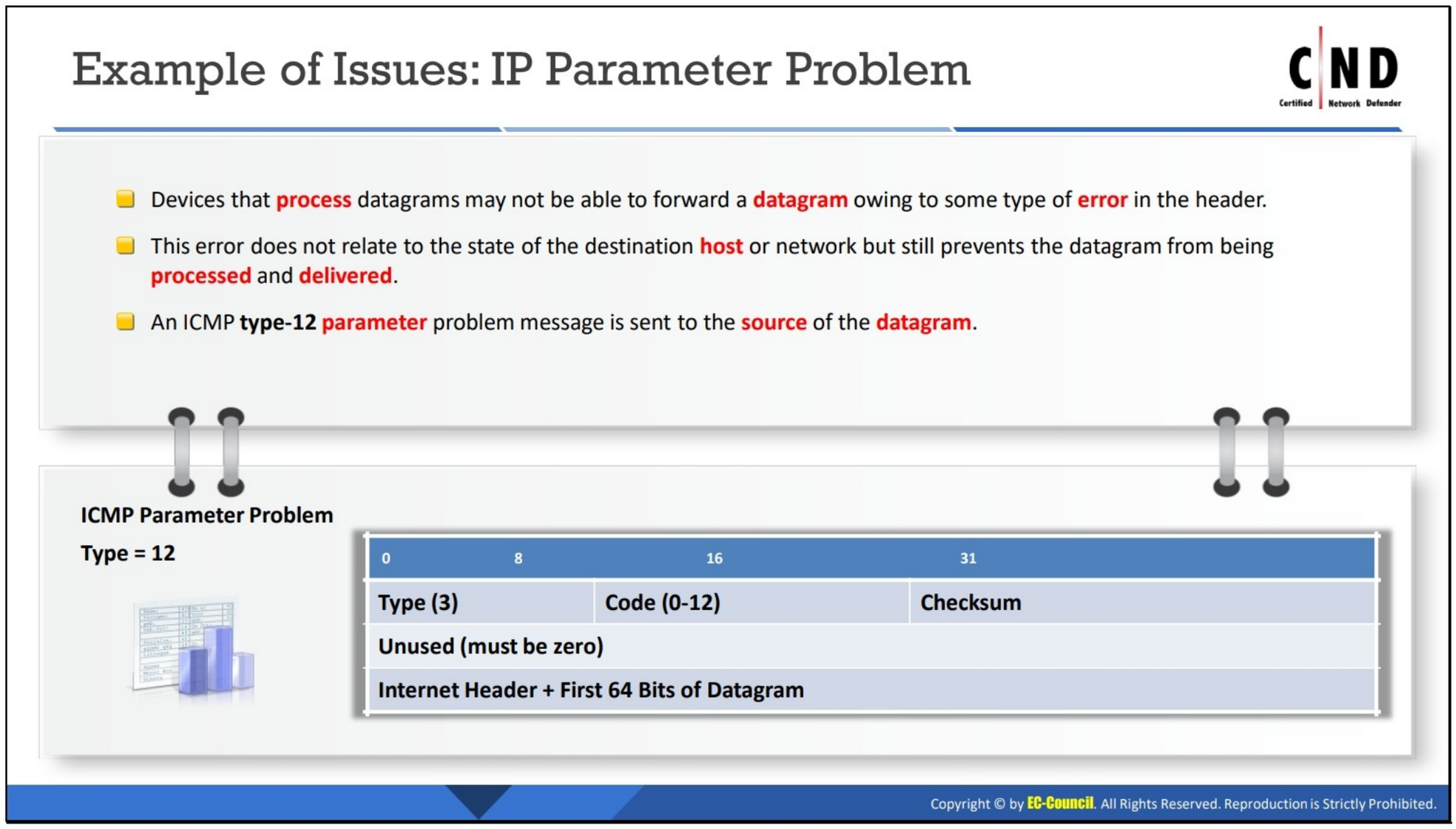


Figure A.105: IP Header

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Example of Issues: IP Parameter Problem

Devices that process datagrams may not be able to forward a datagram owing to some type of error in the header. This error does not relate to the state of the destination host or network but still prevents the datagram from being processed and delivered. An ICMP type-12 parameter problem message is sent to the source of the datagram.

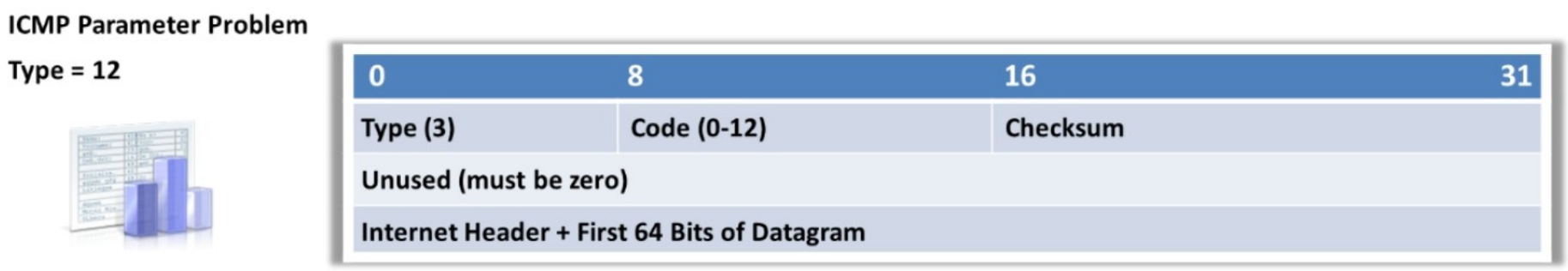


Figure A.106: IP Parameter Problem

The parameter problem occurs when invalid data exist in the fields of an IP header. In this case, the device that traced this invalid information from the IP header sends an ICMP parameter problem message to the source machine that sent the packet. This message contains a pointer that points to the field that caused the error, instead of error codes.

Figure A.107 shows the format of the ICMP parameter problem message.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

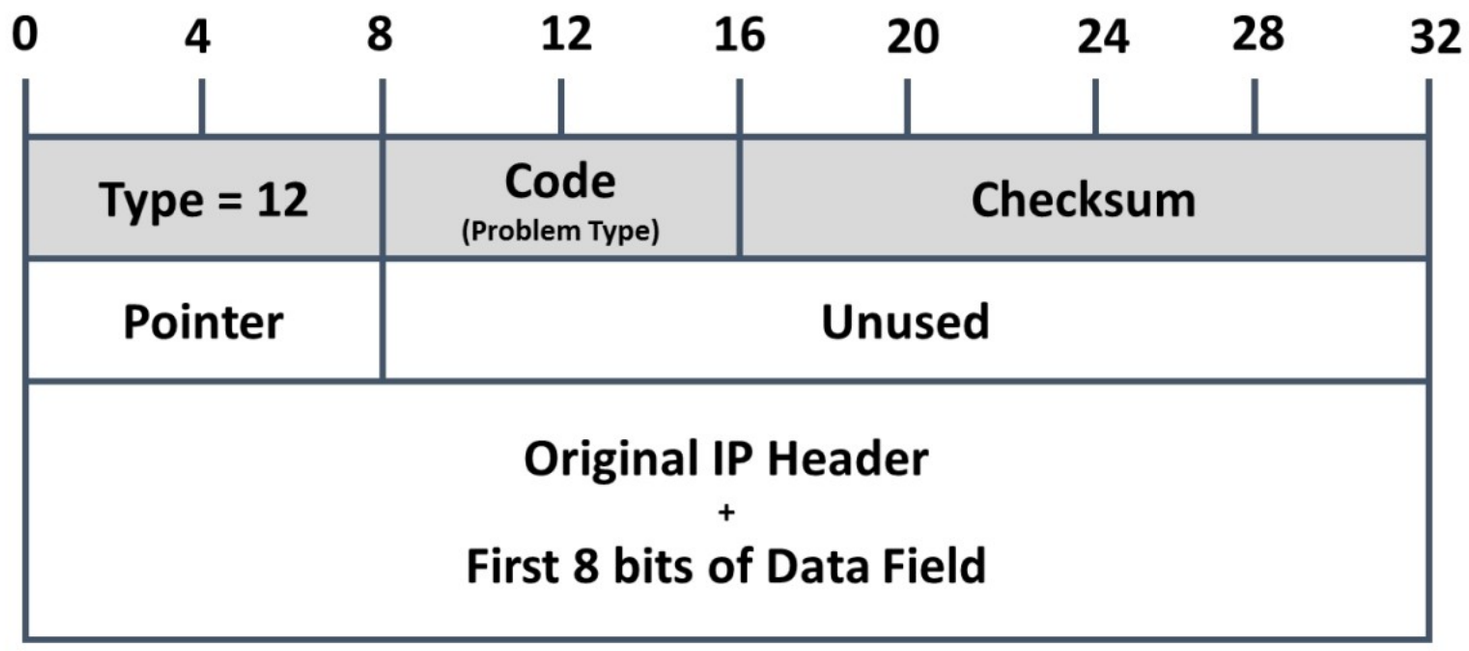


Figure A.107: Format of an ICMP Parameter Problem Message

Each field of an ICMP parameter problem message is discussed below.

- **Type (1 byte)**: This field defines the type of the ICMP message; for parameter problem messages, it is set to 12.
- **Code (1 byte)**: This field defines the reason behind the error.
- **Checksum (2 bytes)**: This field defines a checksum for the ICMP header.
- **Pointer (1 byte)**: This field defines the cause of this message by pointing to the field that is responsible.
- **Unused (3 bytes)**: This field is not used and left blank.
- **Original datagram portion**: This field contains the IP header and first 8 bits of the IP packet that was discarded because of the parameter problem.

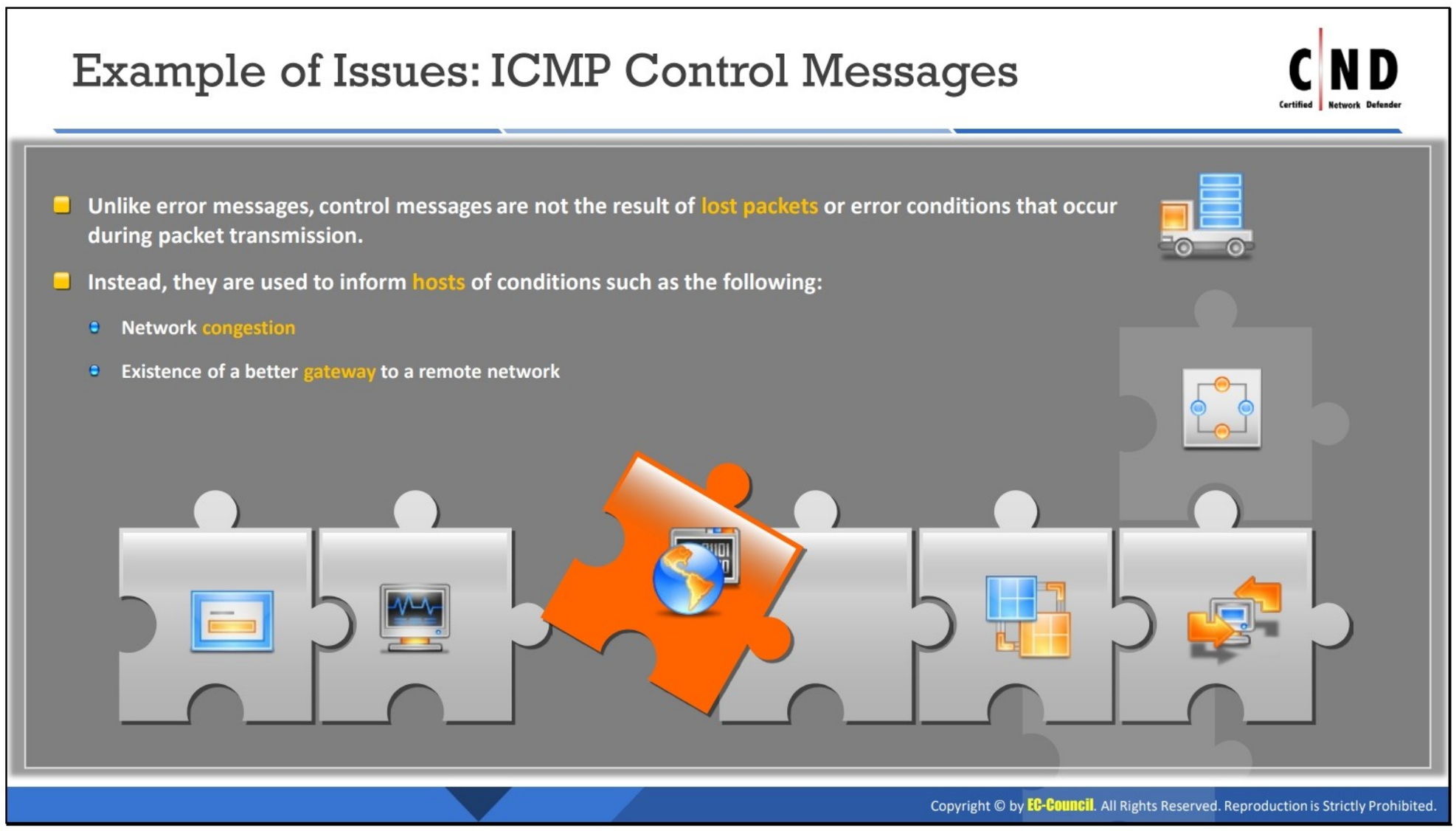
Code and Pointer fields of the ICMP Parameter Problem Message

We have already discussed that the pointer field is used to point out the field that caused the parameter problem. Generally, the pointer to the field that caused this error message contains the code value 0. However, to provide a meaningful reason for the generation of the parameter problem message, two more code values are introduced, as described in Table A.15.

Code	Message	Details
0	Pointer for the field	It is a common way of showing the error field through the pointer.
1	Missing mandatory field	When a required field is missed, this code is indicated. The pointer cannot point an empty filed.
2	Bad length	Invalid size of the datagram packet indicates that the error is in whole packet but not with a particular field. Here there is nothing to do with a pointer to a field.

Table A.14: Pointer and Code Fields in an ICMP Parameter Problem Message

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



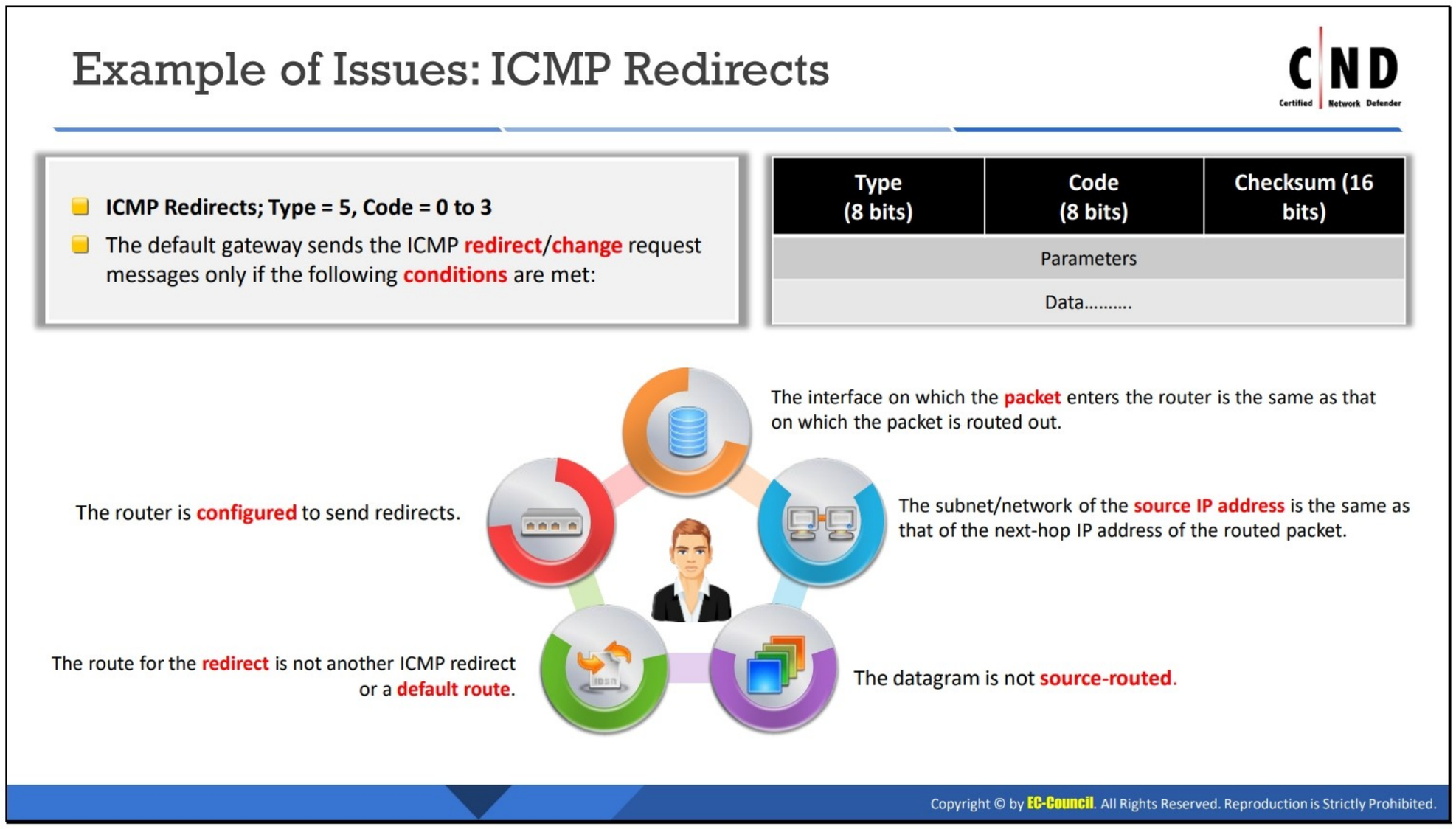
Example of Issues: ICMP Control Messages

Unlike error messages, control messages are not the result of lost packets or error conditions that occur during packet transmission.

Instead, they are used to indicate conditions such as the following:

- Network congestion
- Existence of a better gateway to a remote network

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Example of Issues: ICMP Redirects

Routers are used for transmitting IP packets from one network to the other; they contain a routing table that provides the route to a network. Therefore, whenever an IP packet reaches a host that it does not belong to, the host sends the packet to a router near it. The router takes the responsibility of sending the packet to the correct host (destination).

ICMP redirect messages are used by routers to inform the host that another router is available in the same network that can deal with the packet more easily. Let us consider an example to understand this message more clearly.

Consider three hosts in a network A, B, and C and three local routers X, Y, and Z. If host A wishes to send an IP packet to host C, it sends the packet to X. Based on the routing table information, X comes to know that Z is the nearest router to host C and an easy way to route. X informs host A about this to avoid further communication through this route to host C and sends an ICMP redirect message to host A. Along with this message, X sends the IP packet to Z so that the packet is forwarded to its destination.

Figure A.108 illustrates the functionality of the ICMP redirect message.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

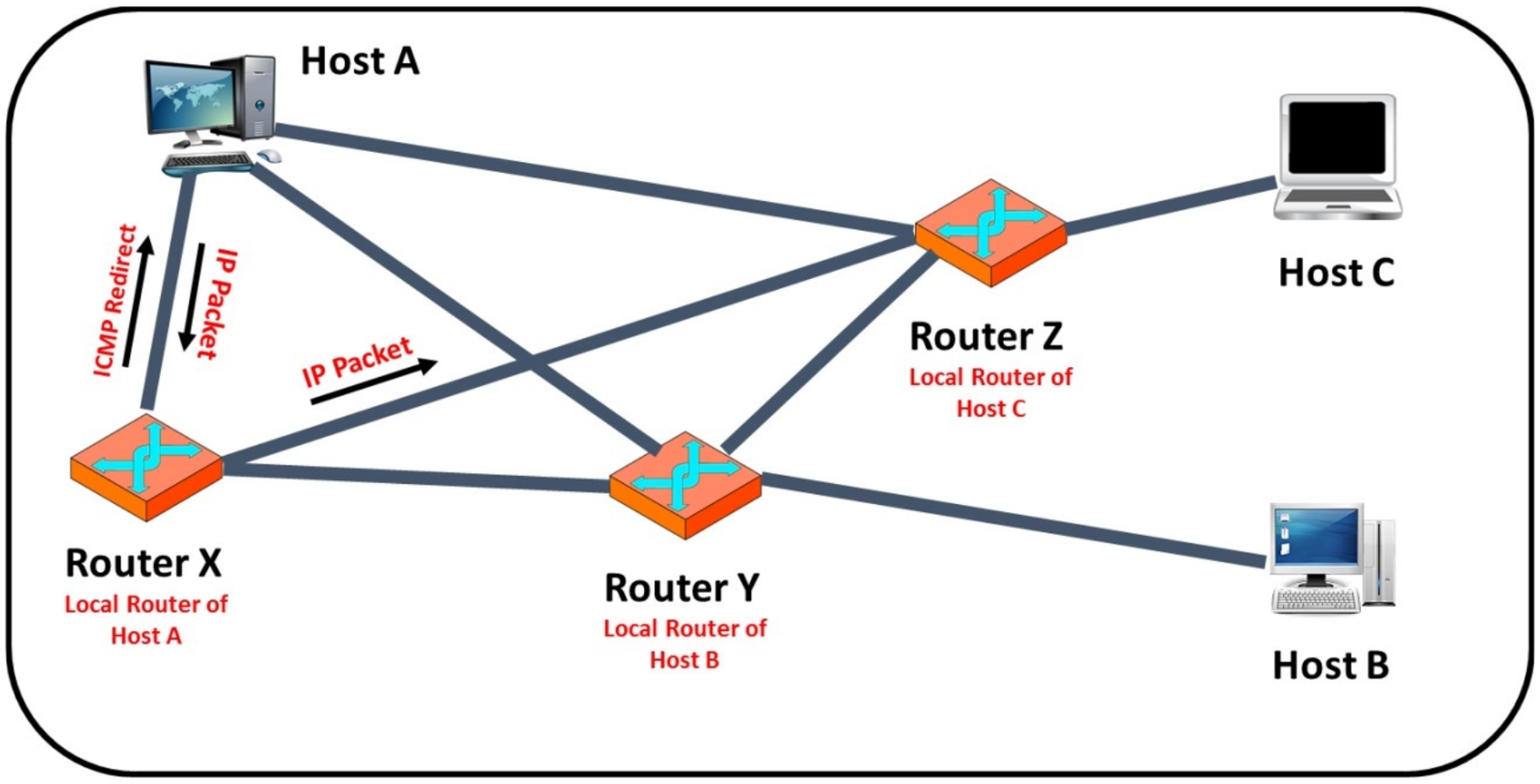


Figure A.108: Schematic of an ICMP Redirect Message

ICMP Redirect Message Format

The following are the fields in an ICMP redirect message:

- **Type (1 Byte)**: This field defines the ICMP message type; for ICMP redirect messages, it is set to 5.
- **Code (1 byte)**: This field defines the reason behind this message.
- **Checksum (2 bytes)**: This field defines a checksum for the ICMP header.
- **Internet address (4 bytes)**: This field defines the address of the router that is local to the destination for further communication.
- **Original datagram portion (variable)**: This field contains the IP header and first 8 bits of the IP packet that reached the wrong router.

Type (8 bits)	Code (8 bits)	Checksum (16 bits)
Parameters		
Data…….		

Figure A.109: Format of an ICMP Redirect Message

ICMP Redirects of Type 5 and Code 0–3

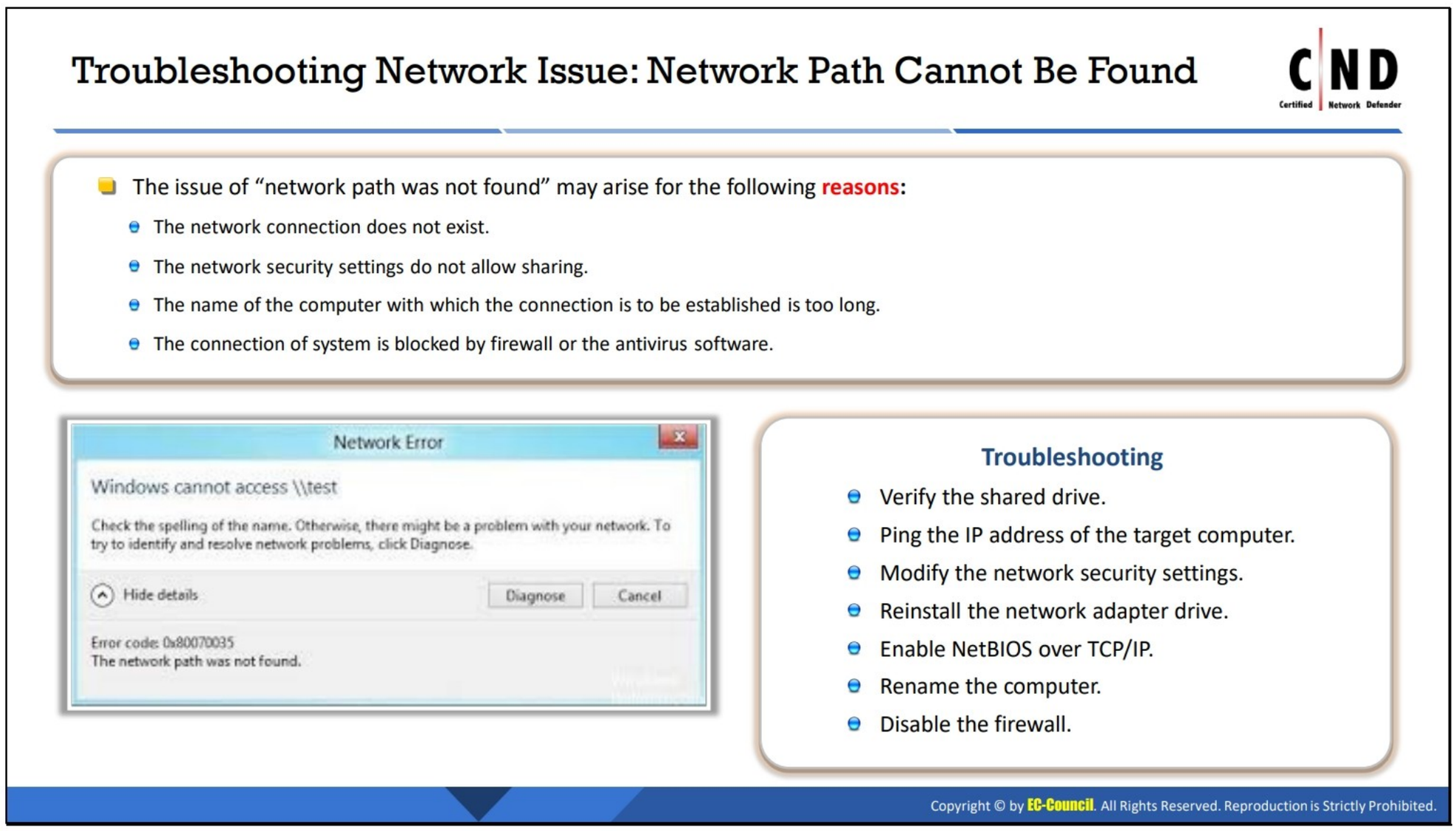
The default gateway sends ICMP redirect/change request messages only if the following conditions are met:

- The router is configured to send redirects.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The route for the redirect is not another ICMP redirect or a default route.
- The interface on which the packet enters the router is the same as that on which the packet is routed out.
- The subnet/network of the source IP address is the same as that of the next-hop IP address of the routed packet.
- The datagram is not source-routed.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Troubleshooting Network Issue: Network Path Cannot Be Found

Error code: 0x80070035, "The network path was not found," appears when hosting a system on a network to access files from another system without Ethernet.

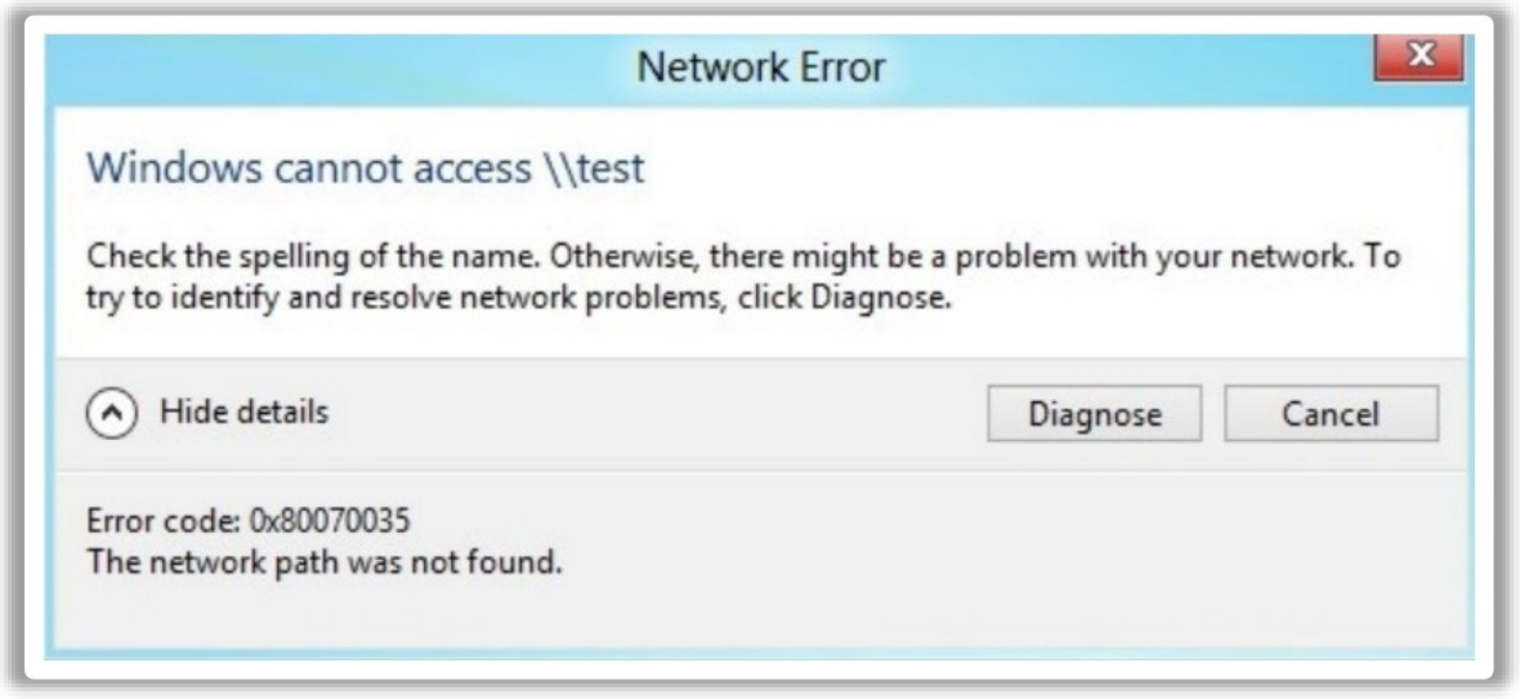


Figure A.110: Network Error

A few different and unrelated technical problems generate this error. This issue often occurs for the following reasons:

- The network connection does not exist.
- Network security settings do not allow sharing.
- The name of the computer with which the connection is to be established is too long.
- The connection or system is blocked by firewall or antivirus software.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Methods to Troubleshoot "The Network Path Cannot Be Found" Error

- **Verify the shared drive:**
  - Right-click the drive that is to be shared and select **Properties**.

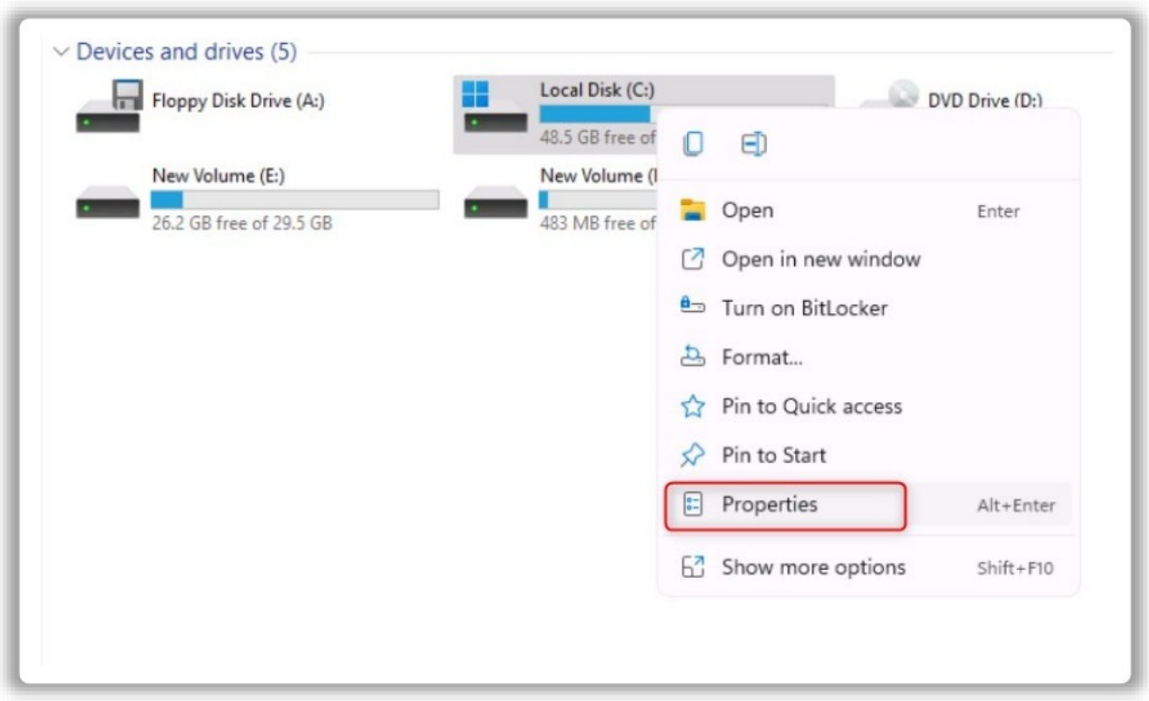


Figure A.111: Select the Drive to be Shared

  - Navigate to the **Sharing** tab. Click **Advanced Sharing…** if it says **Network Path: Not Shared** under the section **Network File and Folder Sharing**.

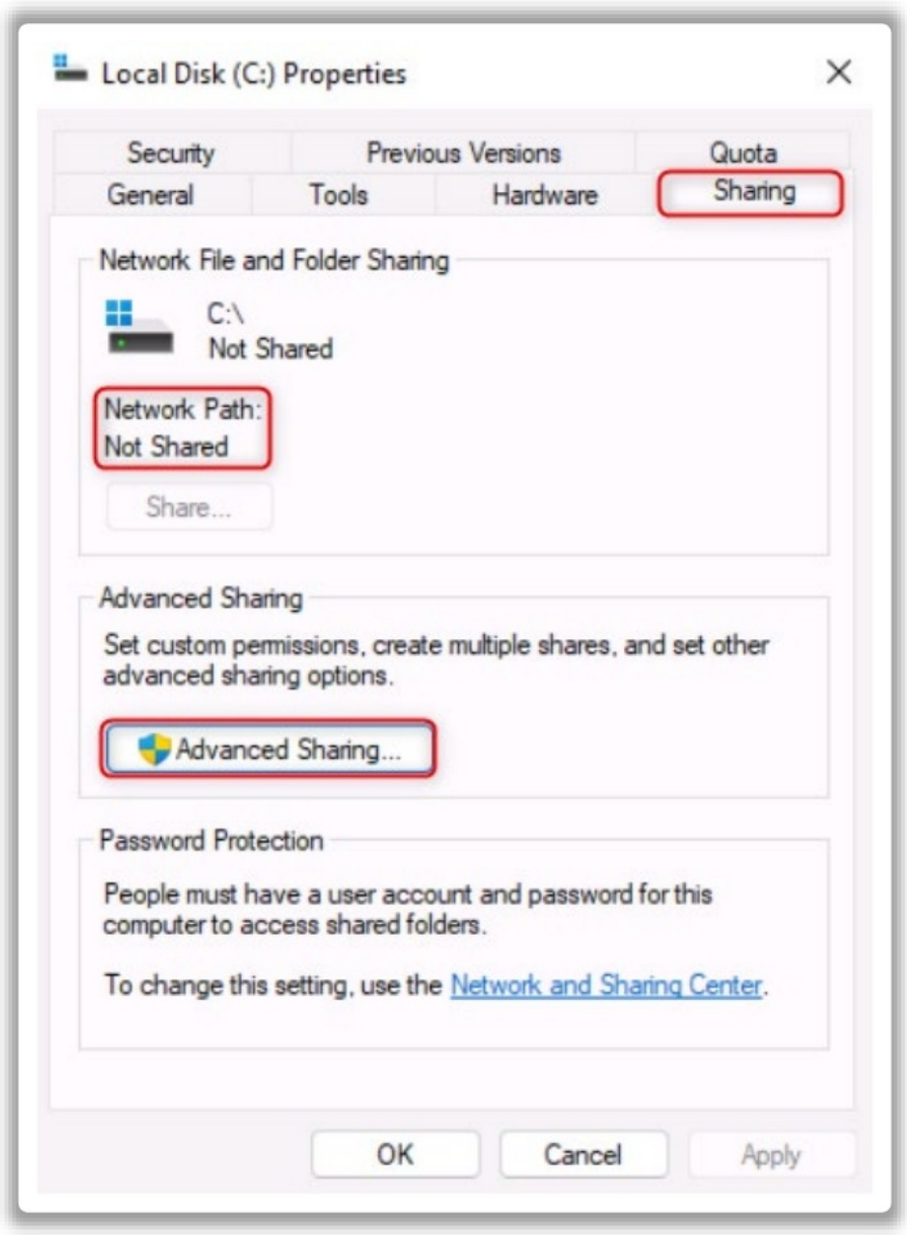


Figure A.112: Share the Selected Drive

  - Tick the box for **Share this folder,** ensure the **Share name** is correct, and click **Apply** and **OK**.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- To ensure the drive is shared, open the **Run** window in the system that needs to access the drive, type the name of the drive, and click **OK**.

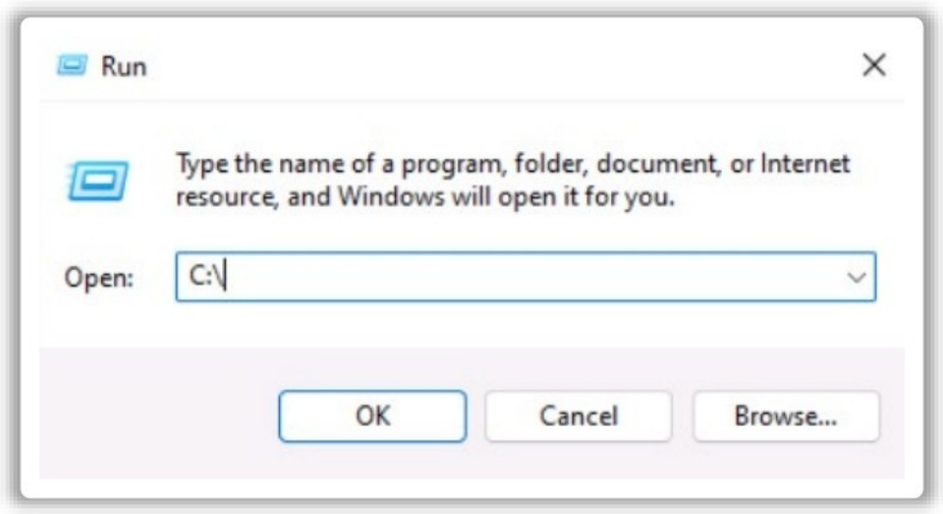


Figure A.113: Ensure the Drive is Shared

- **Ping the IP address of the target system:**
  - On the target system, type in the following command in the command prompt.

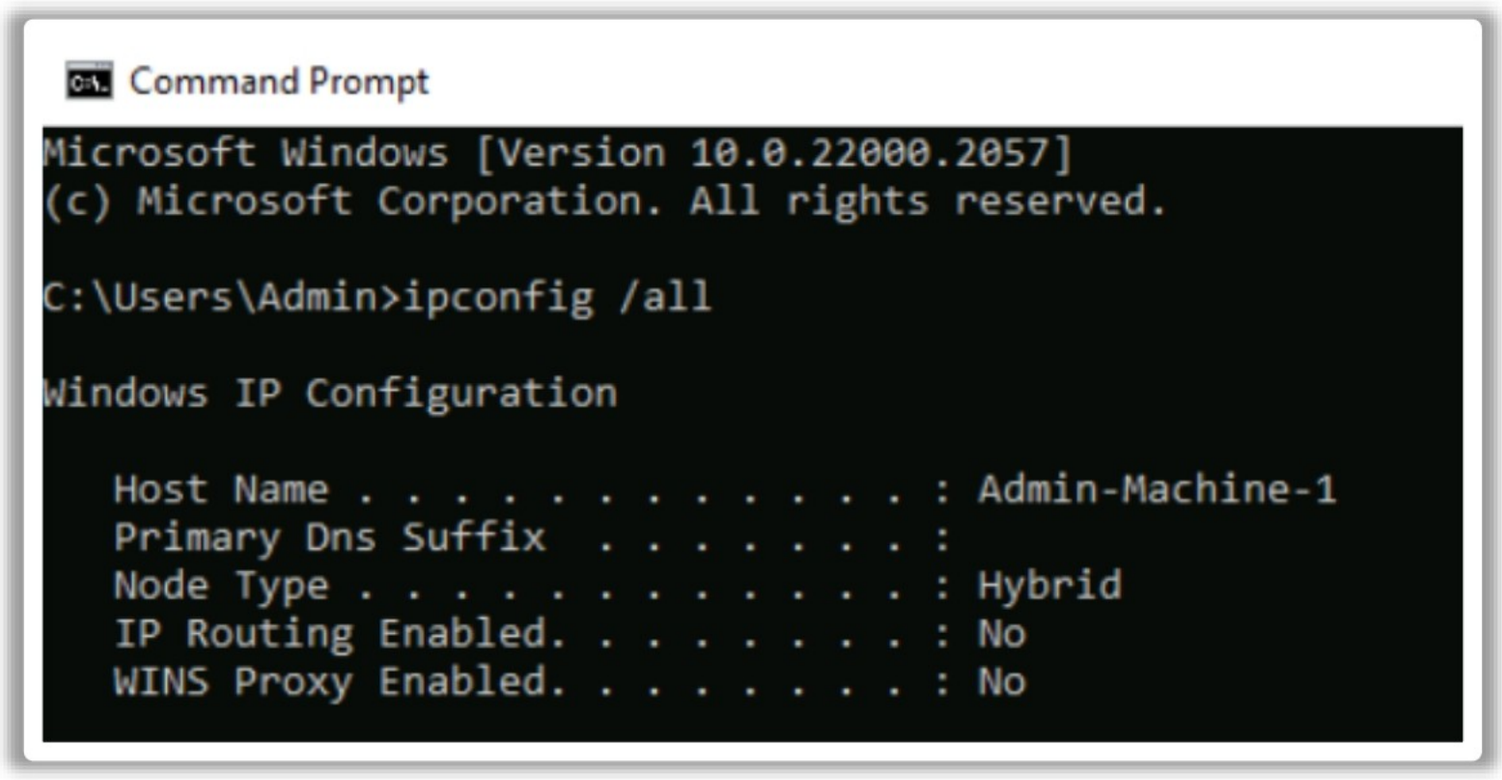


Figure A.114: Execute “ipconfig” Command

  - Locate the category **IPv4 Address** and note down the address (192.168.43.157) here.

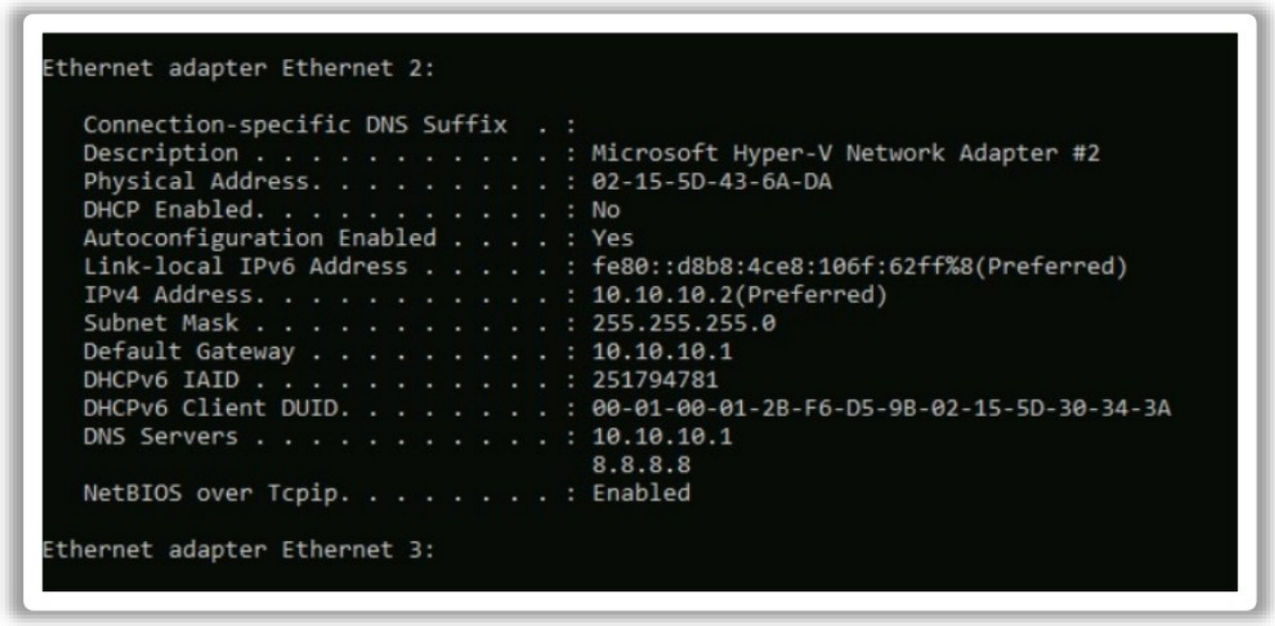


Figure A.115: Locate IPv4

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Again, type in the **Run** window **\\IPv4 Address\(the drive that is to be accessed)**.

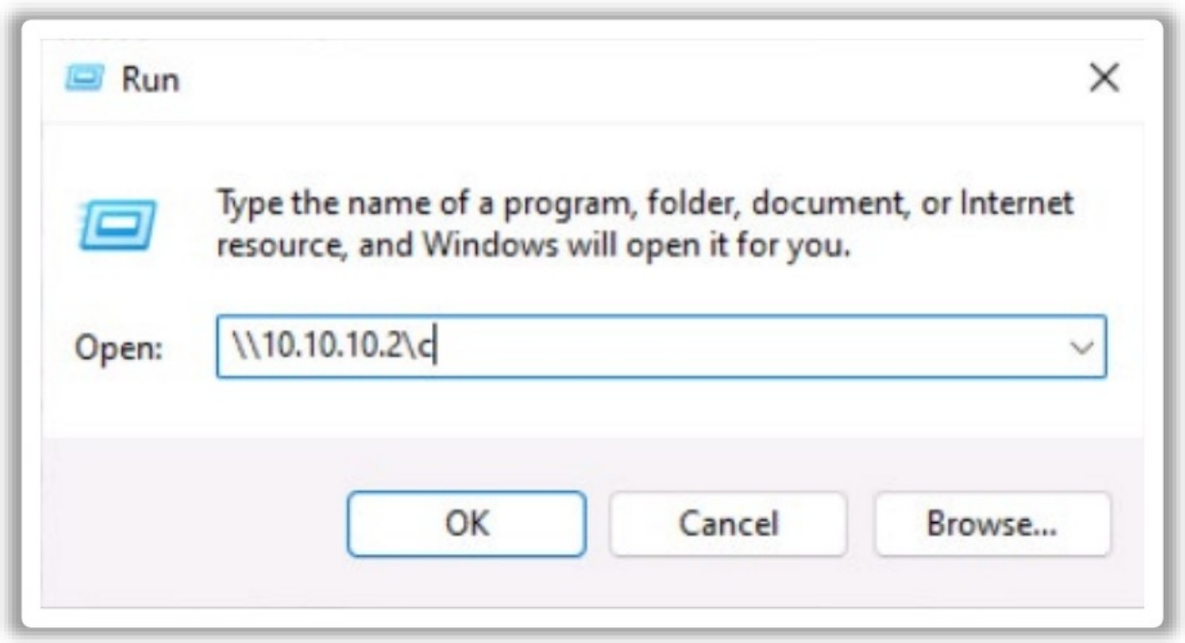


Figure A.116: Ensure the Drive to be Accessed

- Ensure that the specified drive is the one that is shared (the C drive in this case).

- **Modify the network security settings:**

  In case the above two methods did not work, check whether the problem is with the network connection.

  - Double-click **Local Policies/Security Options/Network security: LAN Manager authentication level**.
  - From the drop-down menu, select **Send LM & NTLM-use NTLMv2 session security if negotiated** and click **Apply** and **OK**.
  - Try accessing the shared drive now.

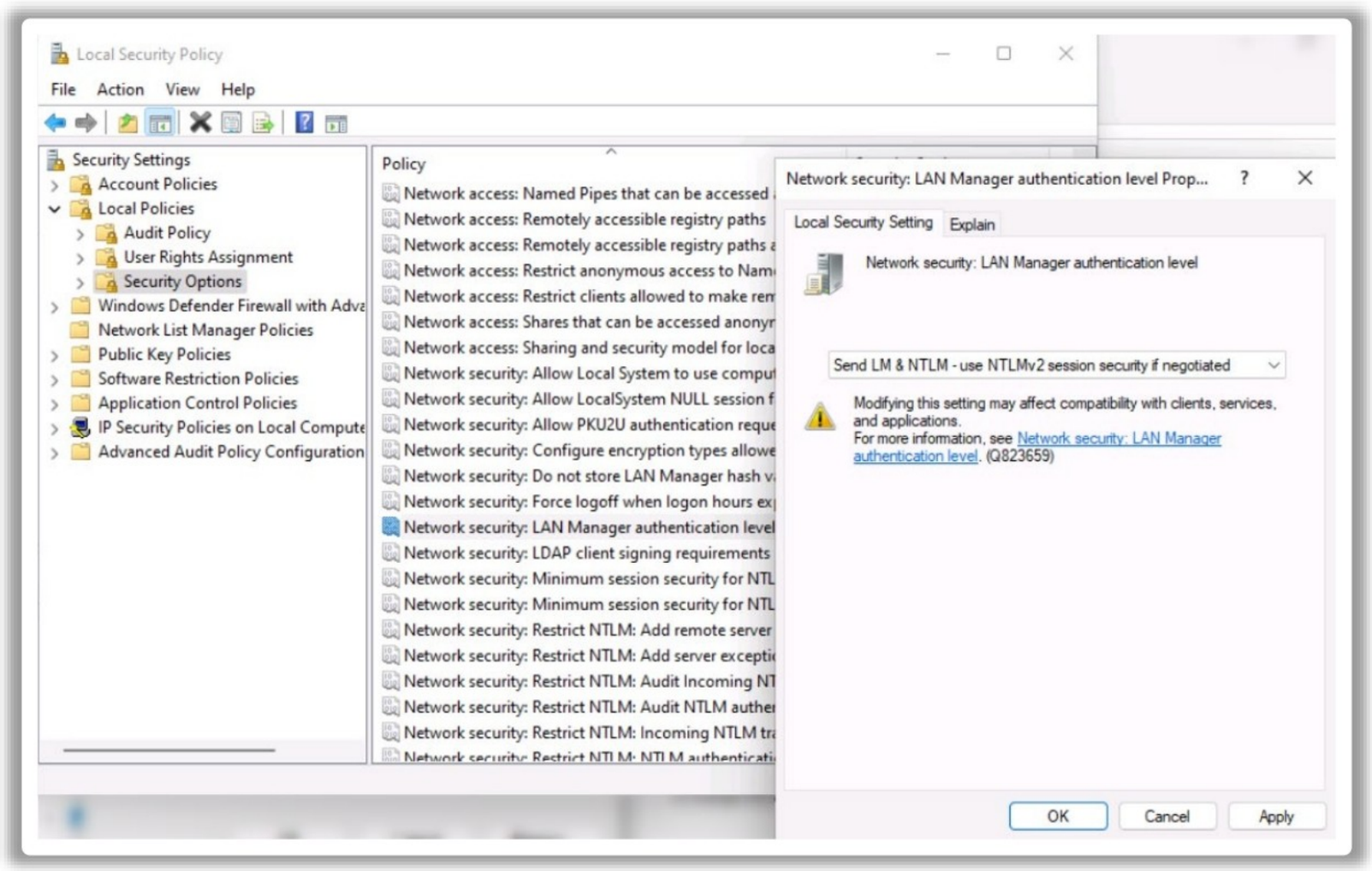


Figure A.117: Modify Network Security Settings

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Reinstall network adapters**
  - Connect the computer to the Internet with a physical wire and run the command **devmgmt.msc**.
  - Click the **View** tab in the **Device Manager** window and check **Show hidden devices**.

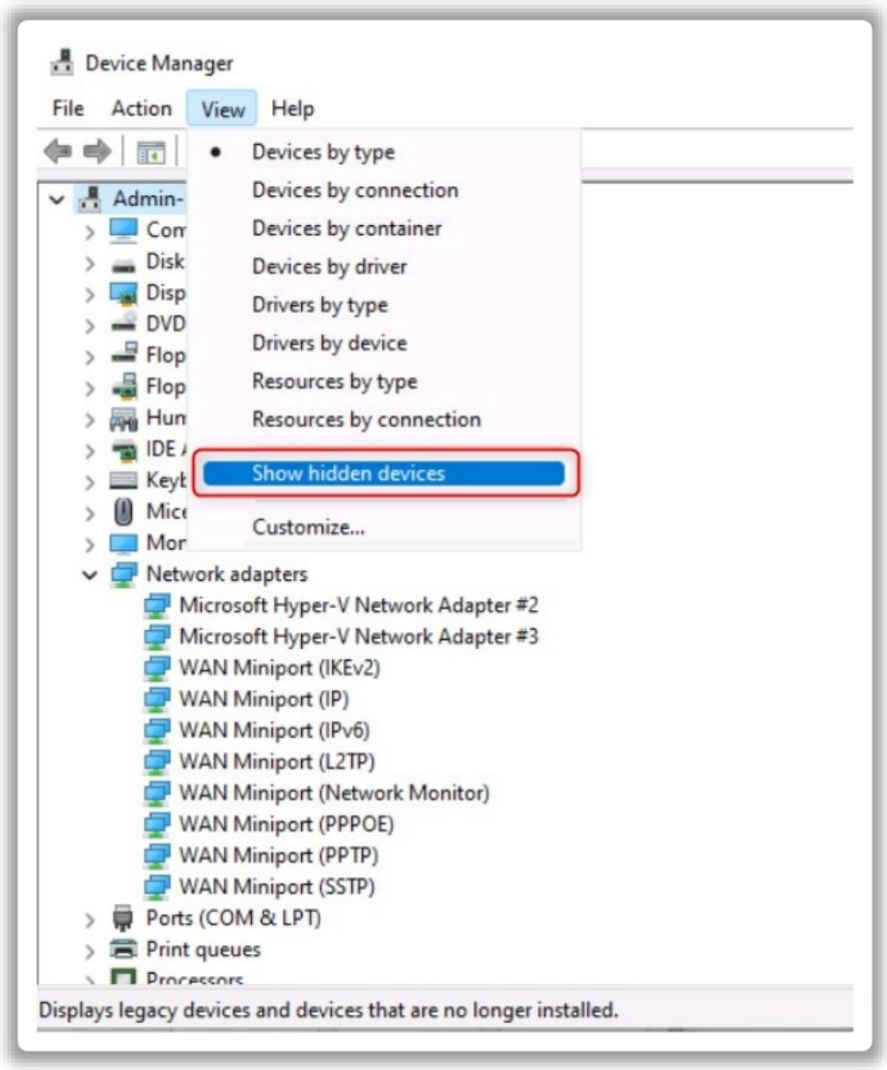


Figure A.118: Check "Show hidden devices"

The hidden adapters are shown with light-colored translucent icons when the list of network adapters is expanded.

- Right-click all the drivers and uninstall them by selecting **Uninstall device**.

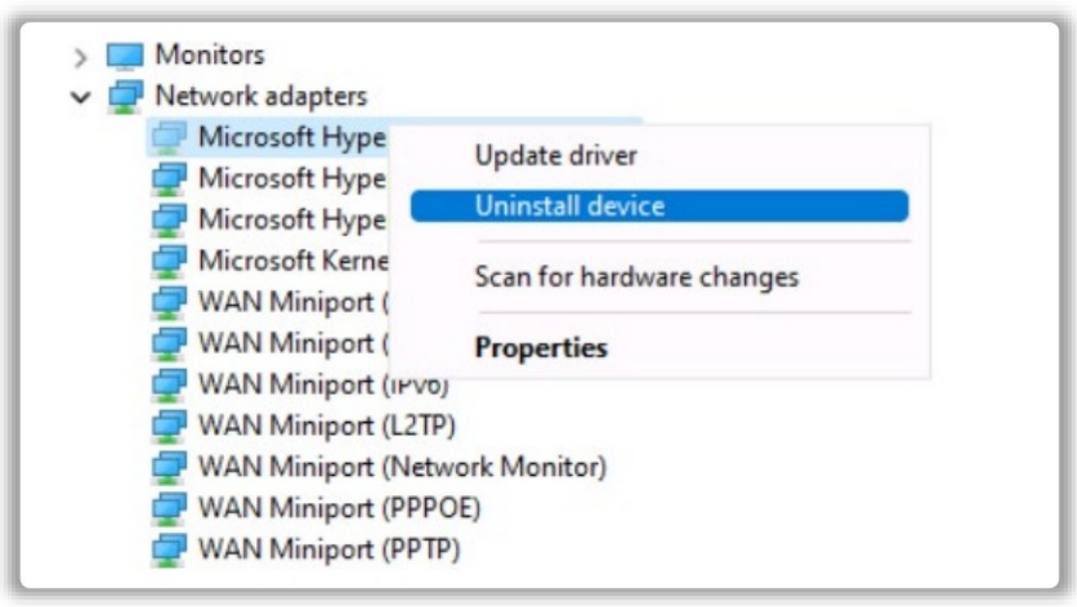


Figure A.119: Uninstall Network Adapter

- Reboot the system and check if the issue is resolved.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Enable NetBIOS over TCP/IP**
  - Run the command **ncpa.cpl**.

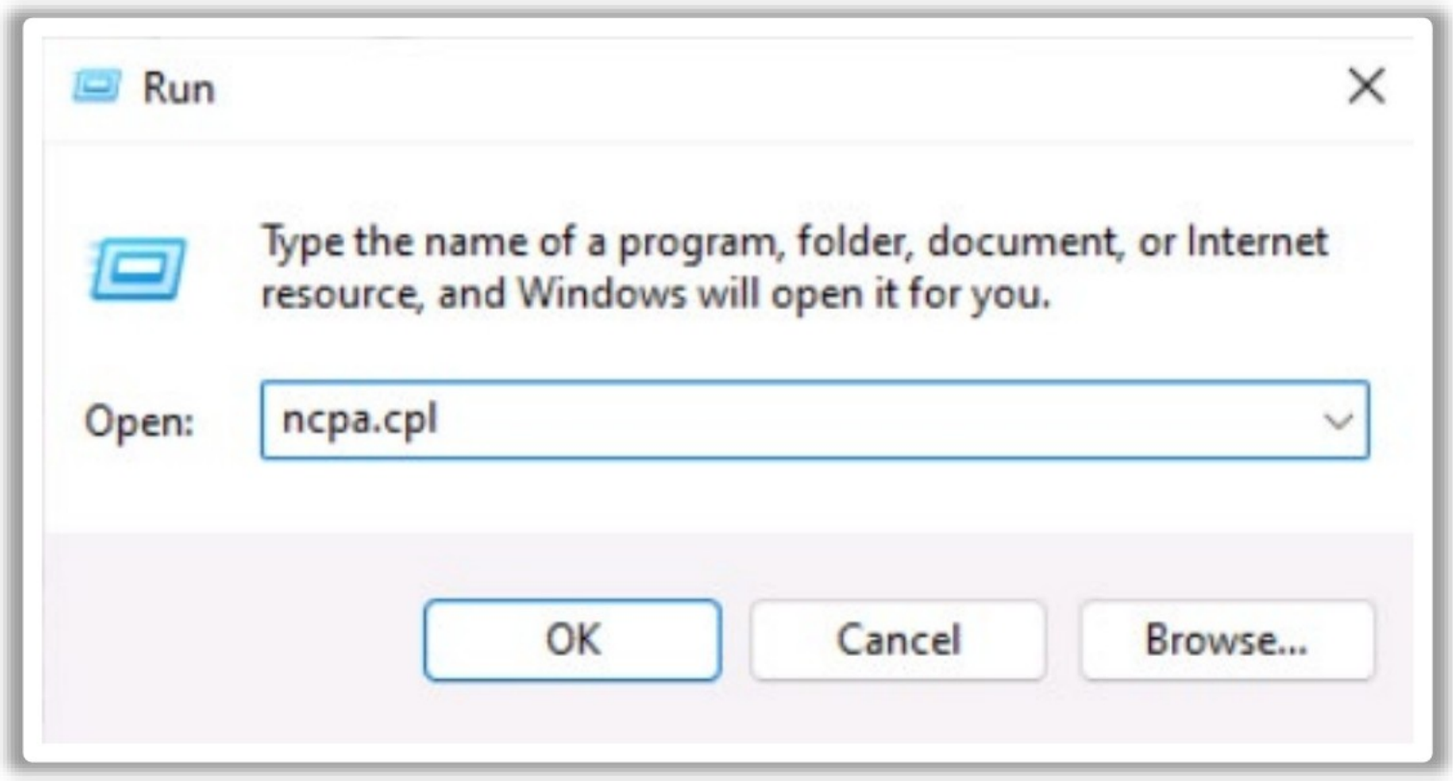


Figure A.120: Run "ncpa.cpl"

  - Right-click the active Wi-Fi or Ethernet connection and select **Properties**.
  - Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

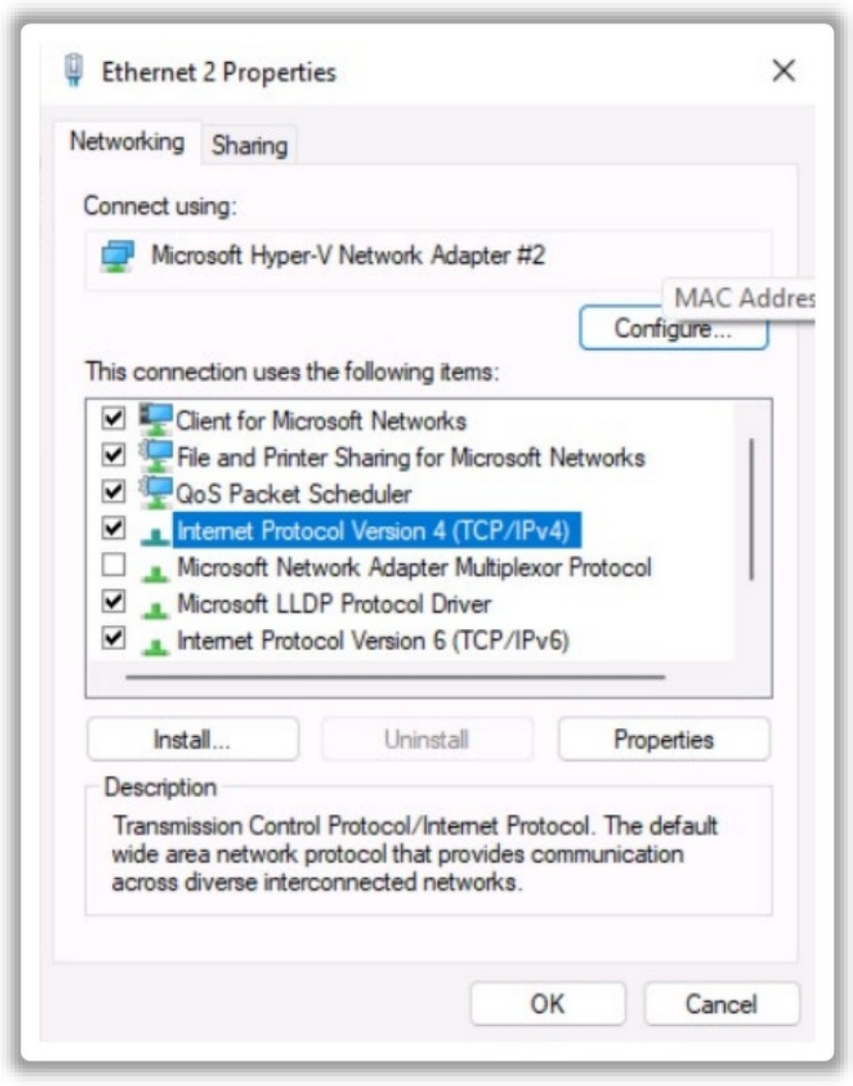


Figure A.121: Select Properties of TCP/IPv4

  - Click **Advanced** in the next window and switch to the **WINS** tab under **Advanced TCP/IP Settings**.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Under **NetBIOS setting**, check **Enable NetBIOS over TCP/IP** and click **OK**.

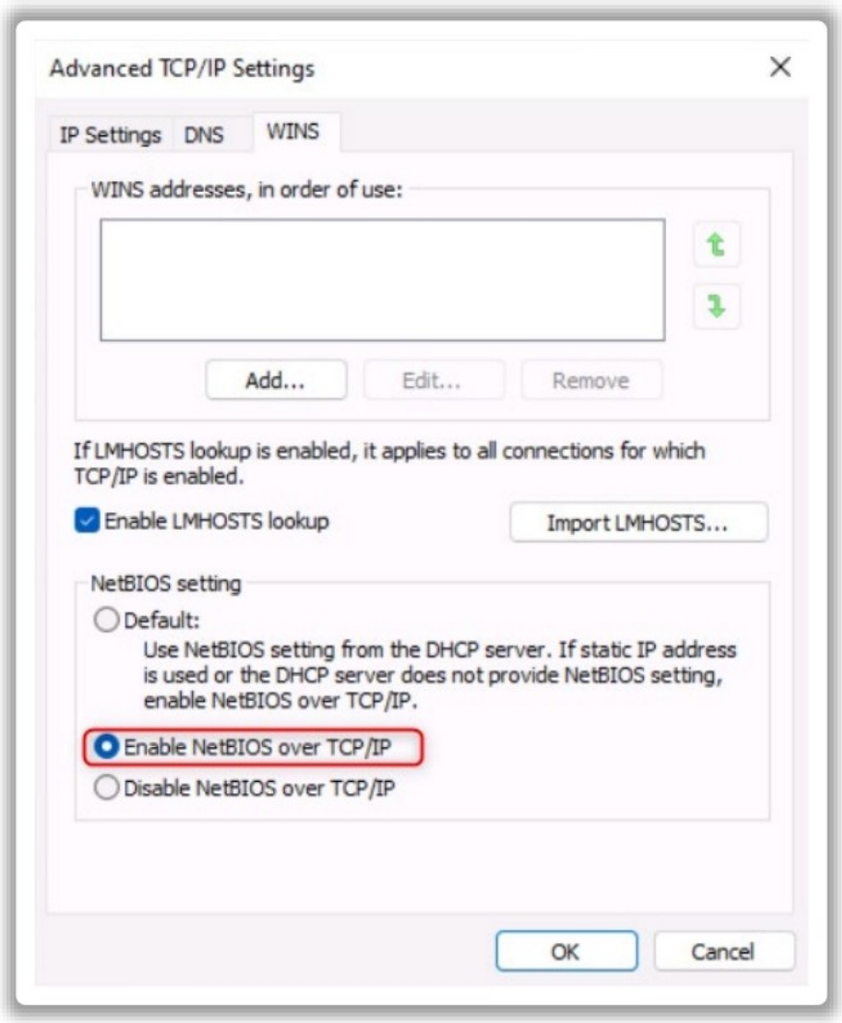


Figure A.122: Enable NetBIOS over TCP/IP

- Reboot the PC to save the changes.

- **Rename the computer**
  - Go to **Control Panel/Credential Manager**.
  - Select **Windows Credentials** and click **Add a Windows credential**.

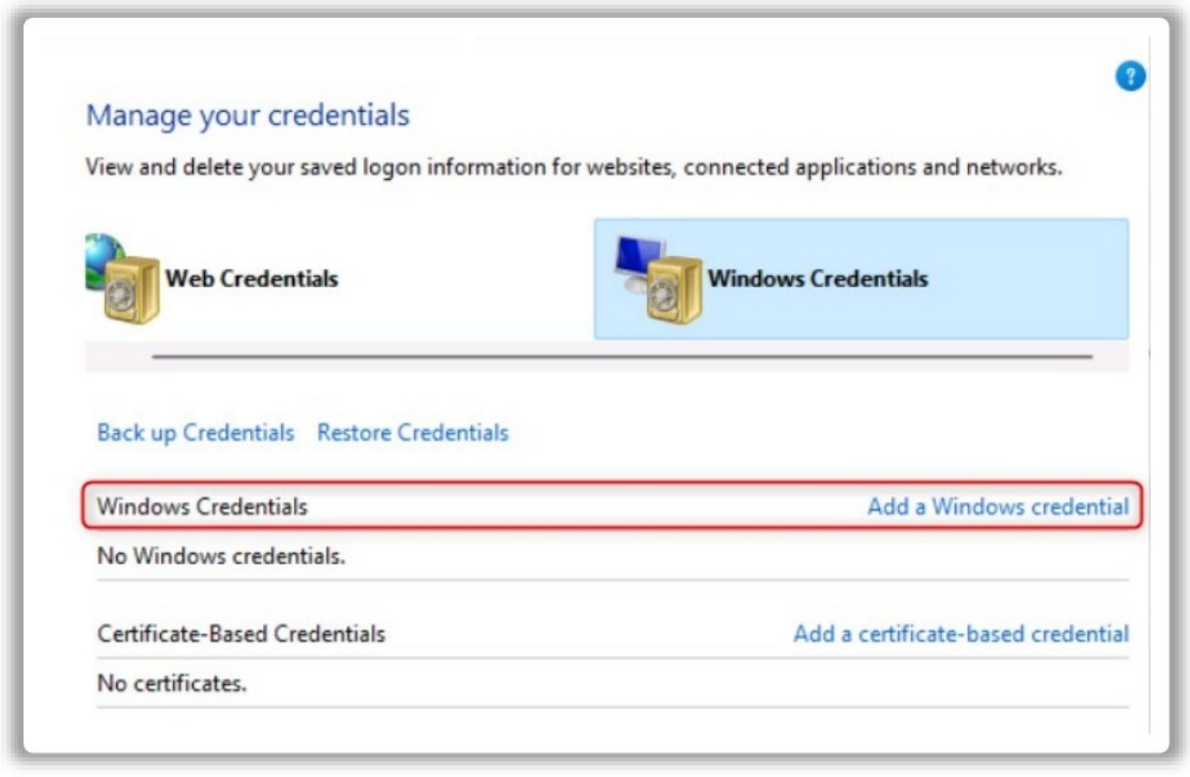


Figure A.123: Add a Windows Credential

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Sequentially enter the username and password of each machine connected to the network.

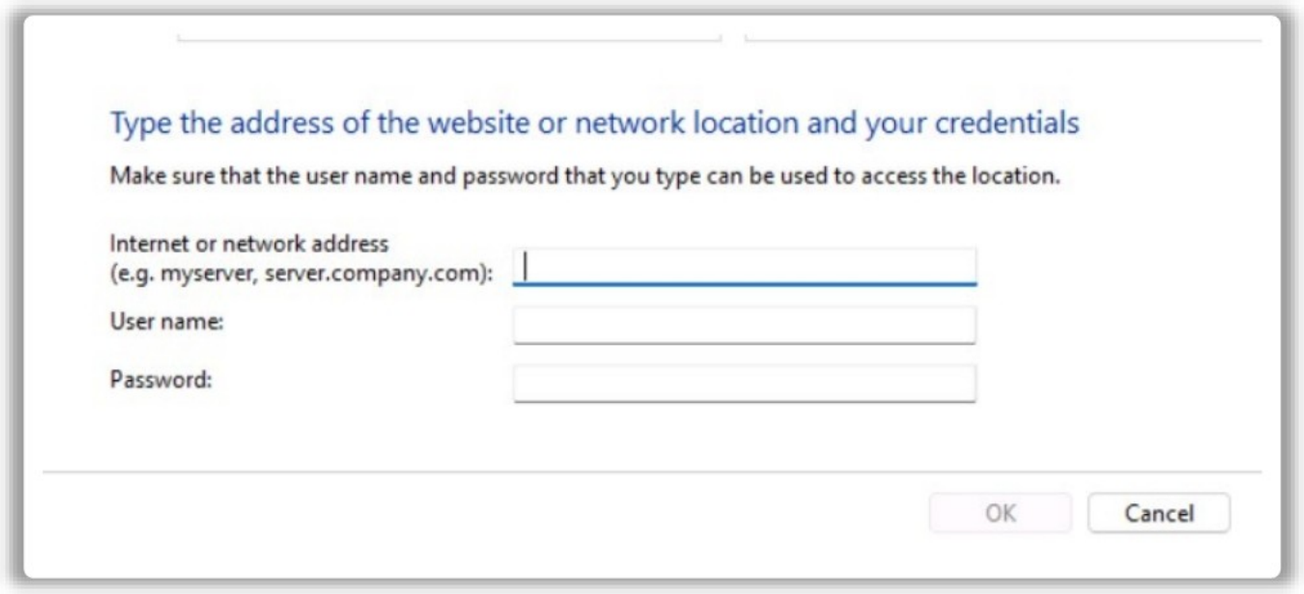


Figure A.124: Enter Credentials for Machine

- Follow the above procedure for the connected PCs.

- **Disable antivirus and firewall**
  - Right-click the antivirus program icon from the system tray and select **Disable**.

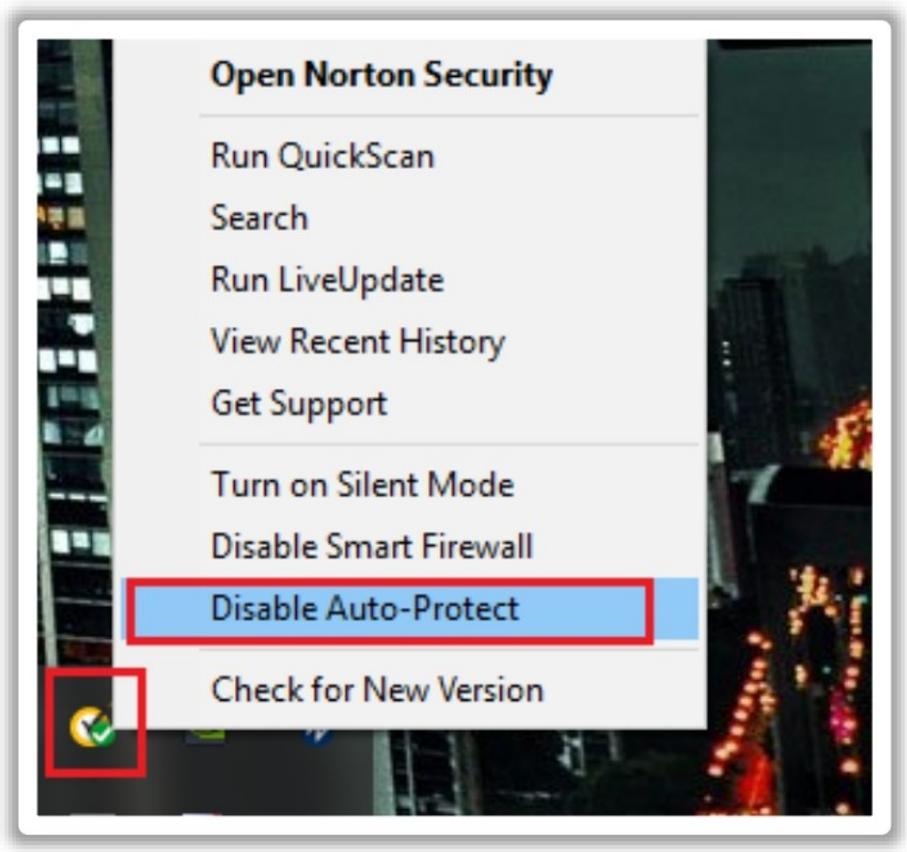


Figure A.125: Disable Anti-virus

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select the time frame for which the antivirus program will remain disabled.

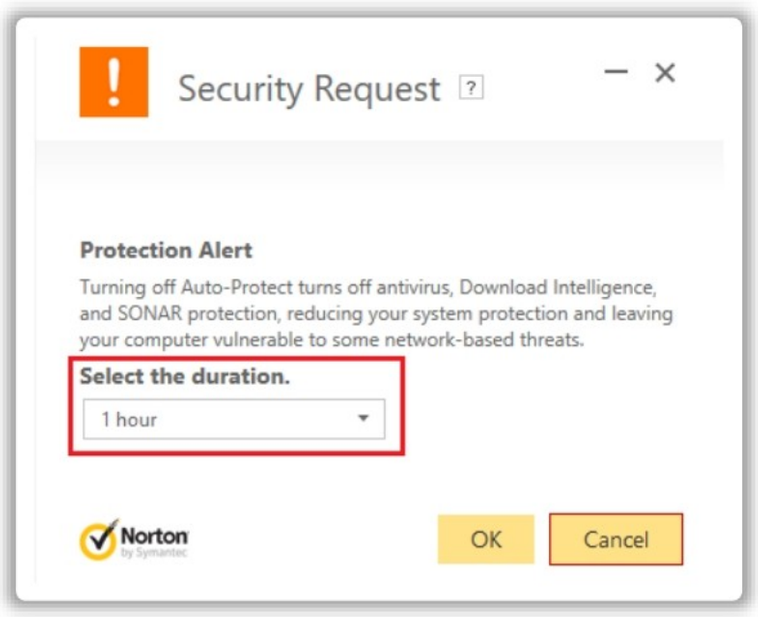


Figure A.126: Duration Selection

- Once done, check whether the error is resolved.
- Go to **Control Panel/System and Security**.
- Click **Windows Firewall**.

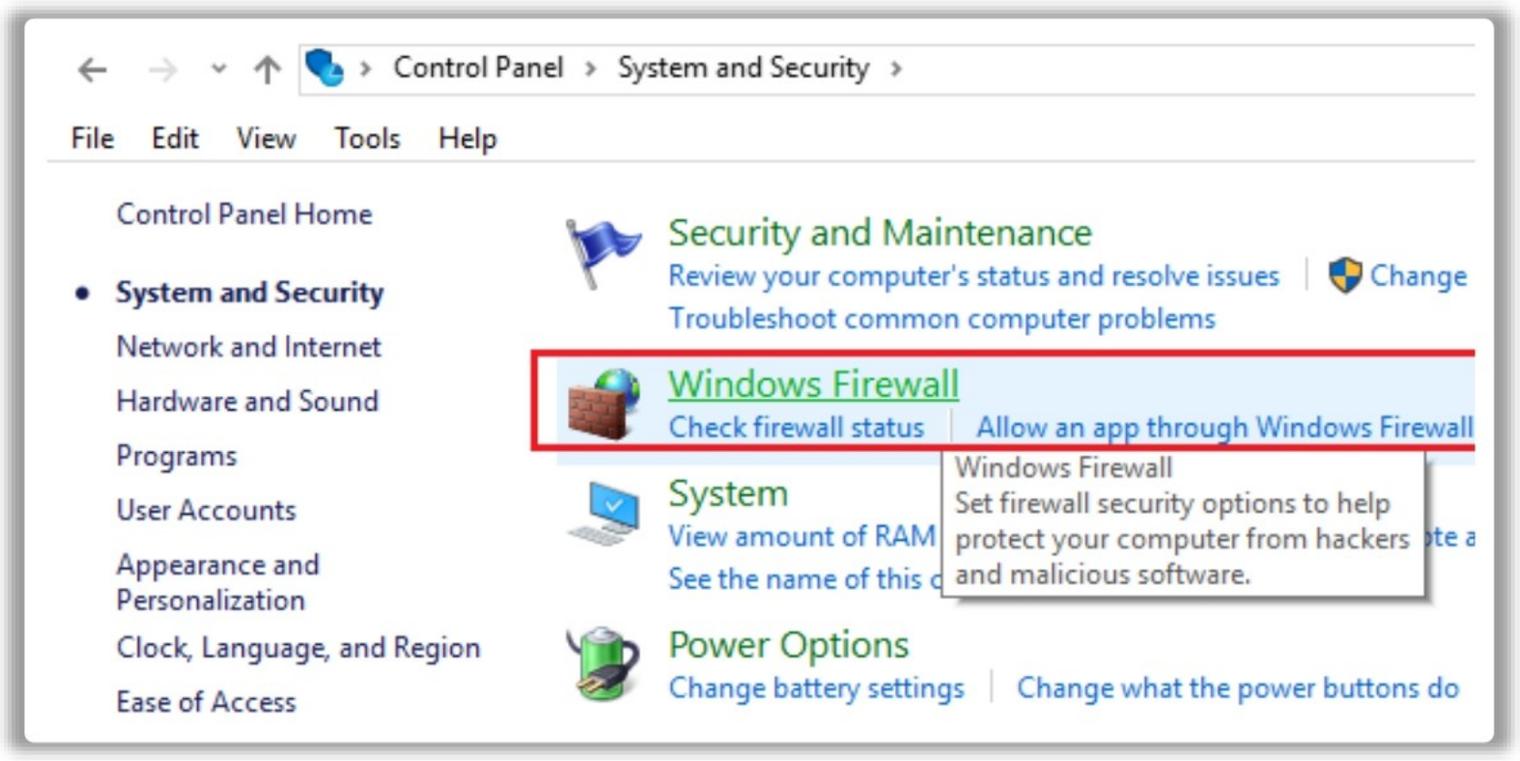


Figure A.127: Click “Windows Firewall”

- Click **Turn Windows Firewall on or off** from the left pane.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

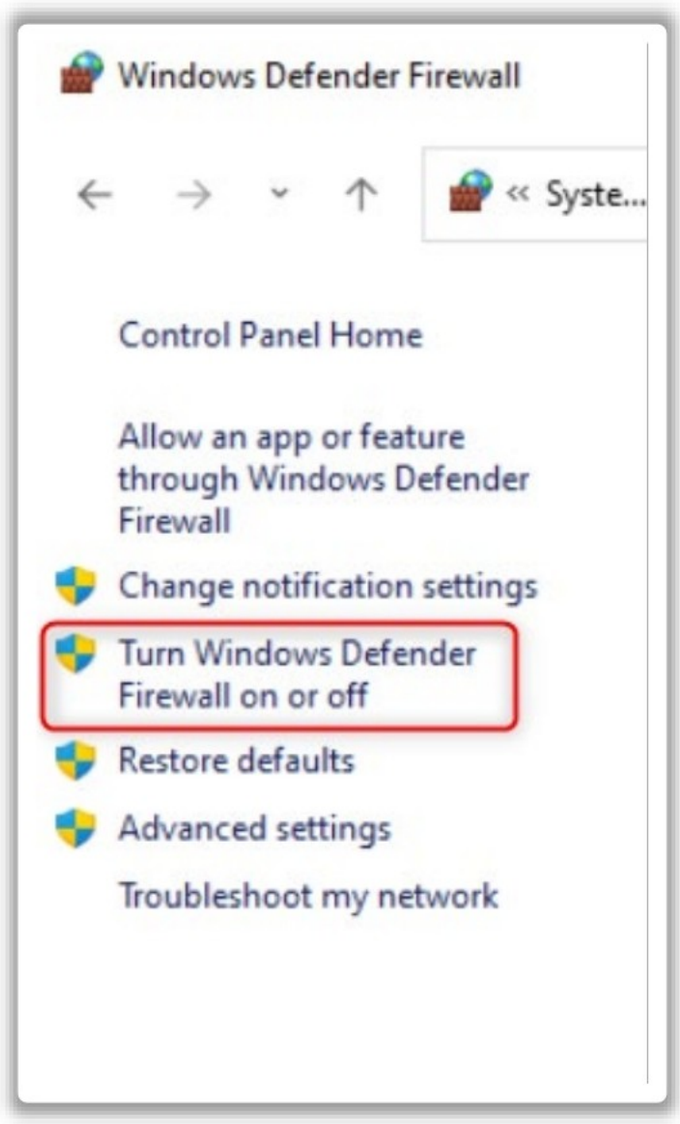
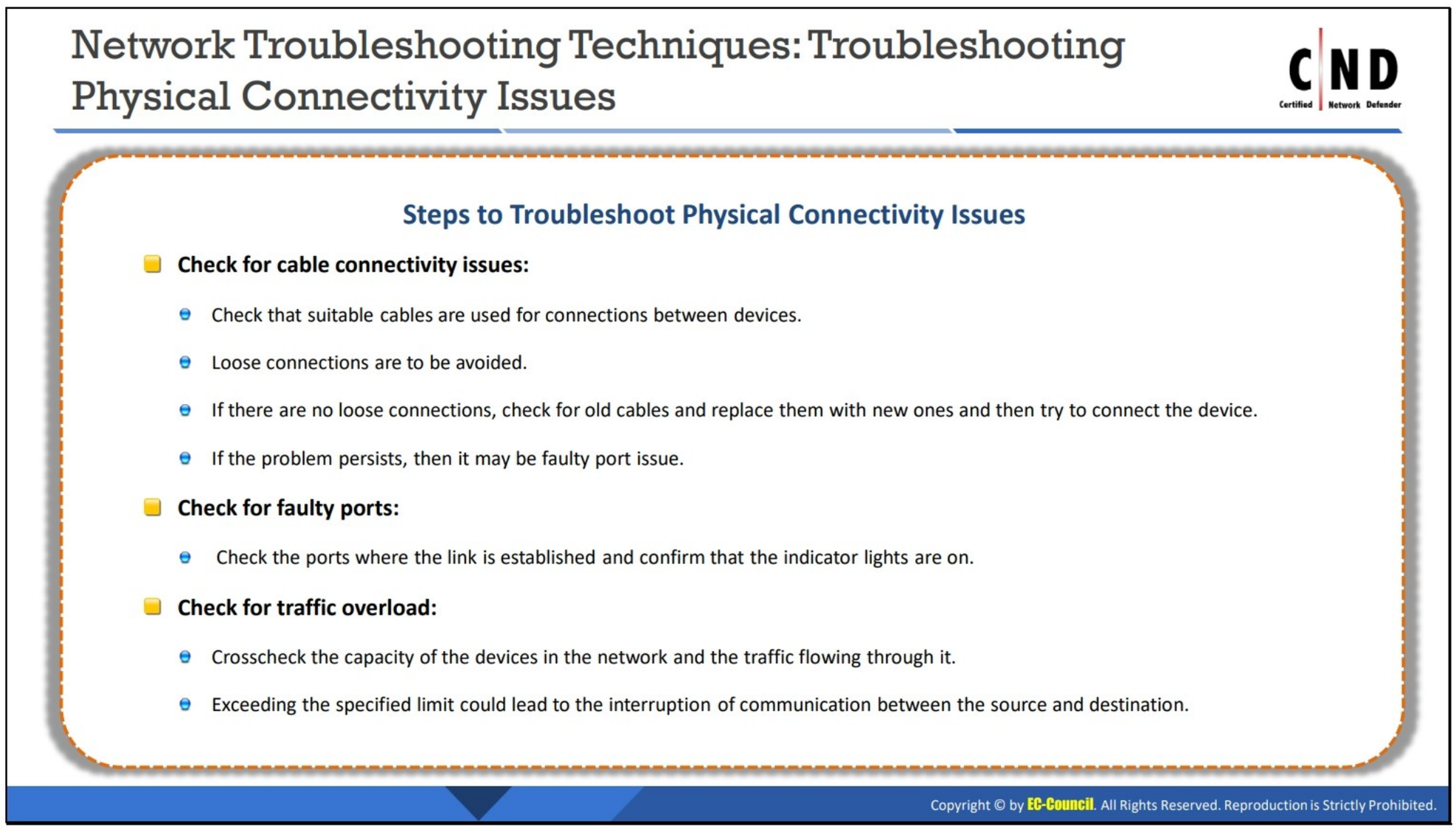


Figure A.128: Select "Turn Windows Firewall on or off" Option

- Select **Turn off Windows Firewall** and restart the PC.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Troubleshooting Techniques: Troubleshooting Physical Connectivity Issues

Steps to Troubleshoot Physical Connectivity Issues

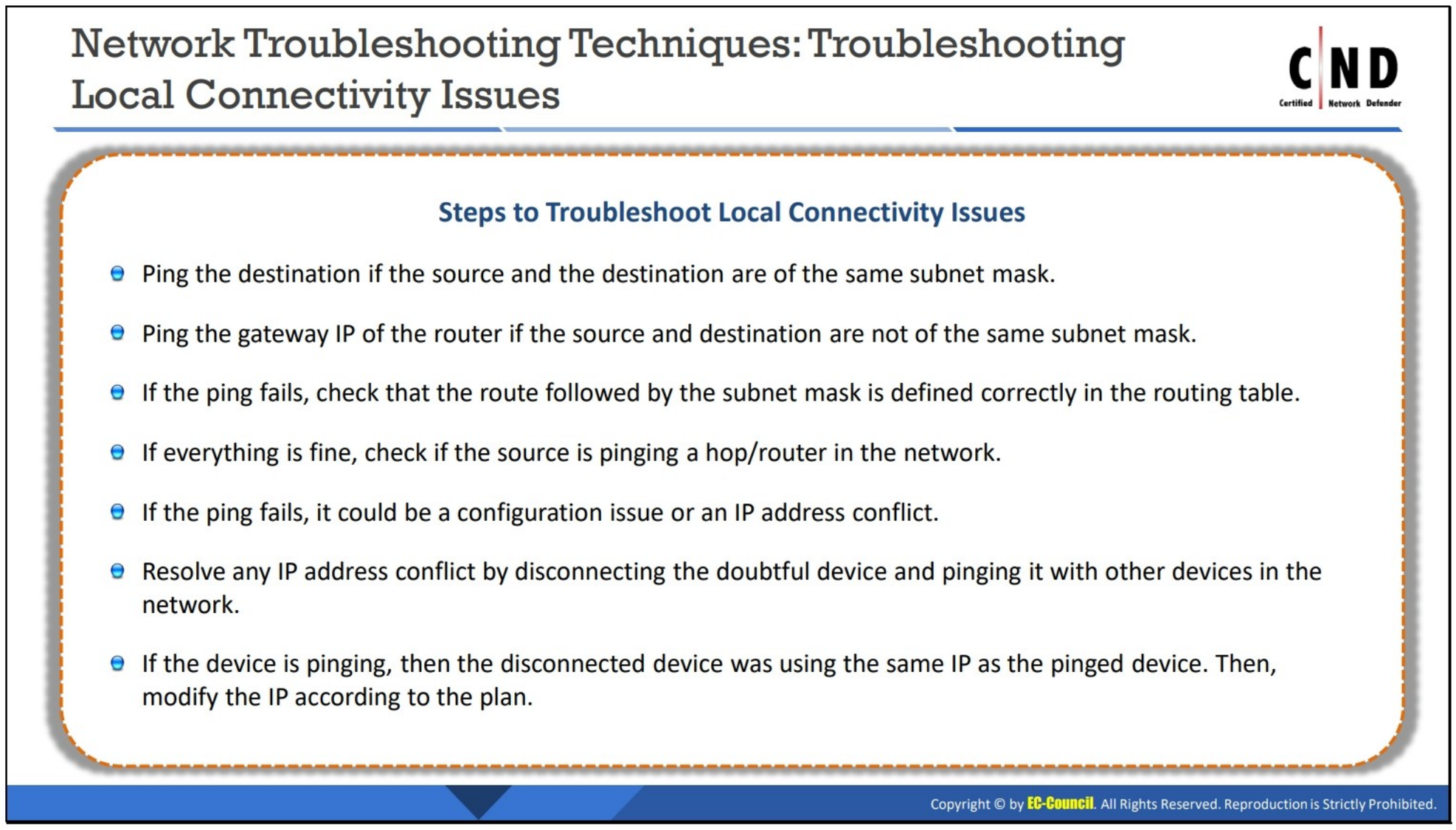
Check for cable connectivity issues: The user should primarily check that the network cable is plugged in. If the cable is not plugged in, then plug it into the network card of the computer. If the cable is securely plugged in, then reboot the system and check for cable connectivity issues.

The cable used to connect computers may be physically damaged, shorted, or faulty. Check that suggested and suitable cables are used for connections between devices. For example, check that the connectivity between a router and computer is established using a crossover pair of cables. Loose connections are to be avoided. If there are no loose connections, check for old cables and replace them with new ones and attempt to connect the device. If the problem persists, then it can be a faulty port issue.

Check for faulty ports: Check the ports where the link is established and confirm that the indicator lights are on. The user should verify the duplex mode and speed. If the port is working properly but the connectivity issue persists, then check the indicator lights on each device to determine the working status of the port. Check whether the port is physically radiating or the indicator lights are off. From the light status, the user can determine whether the port is physically malfunctioning. In this scenario, the user should configure the link on some other free port/interface.

Check for traffic overload: Crosscheck the capacity of the devices in the network and the traffic flowing through it. Exceeding the specified limit could lead to the interruption of communication between the source and destination. If traffic overload occurs at the link or interface, then it would function abnormally at some point; therefore, the user should verify these criteria to avoid any connectivity issues.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



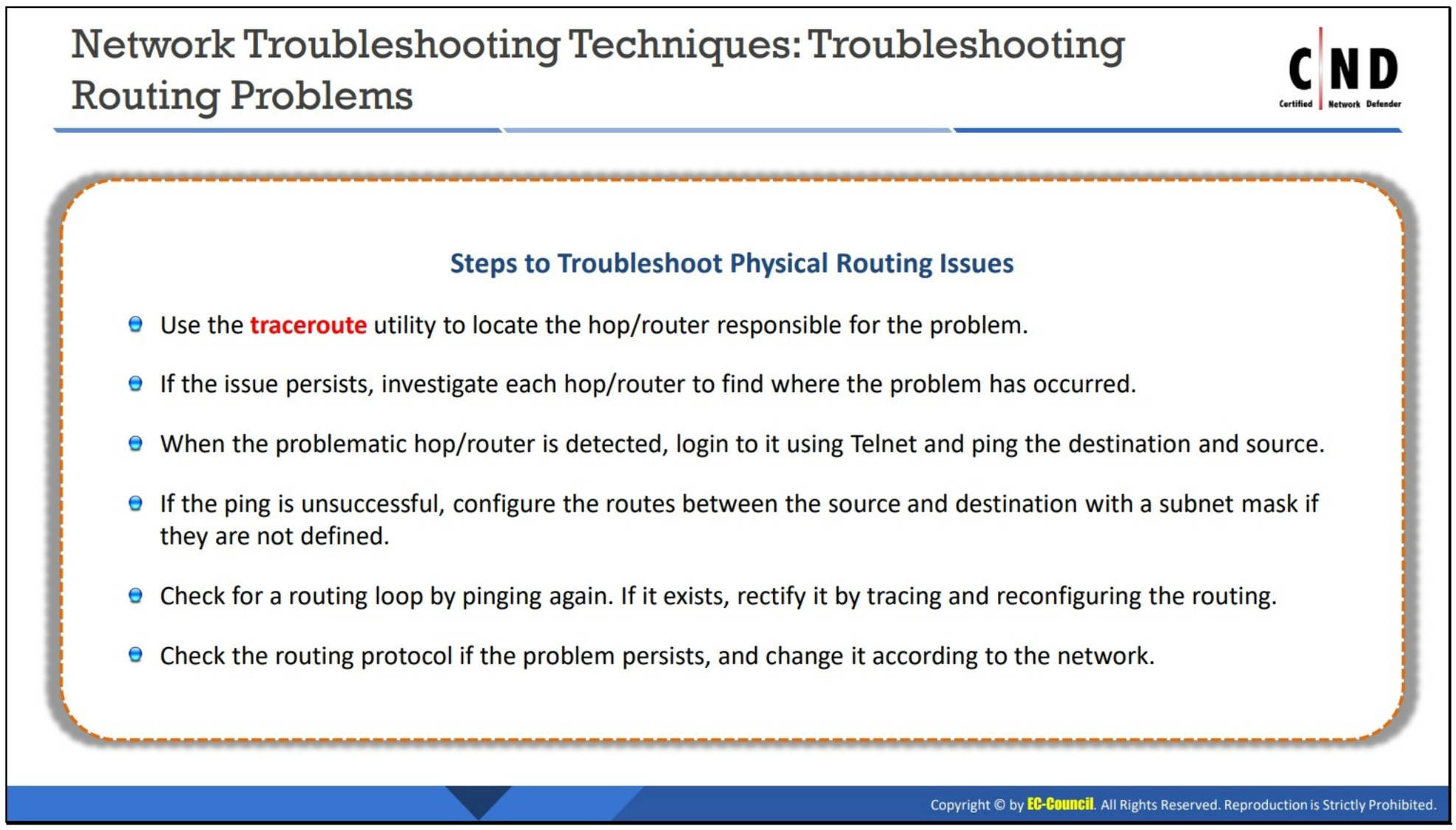
Network Troubleshooting Techniques: Troubleshooting Local Connectivity Issues

If the user encounters LAN connectivity issues, then to identify the root cause and resolve the issue, it is recommended to follow the steps below.

Steps to Troubleshoot Local Connectivity Issues

- The user should ping the destination IP if the source and destination are of the same subnet mask.
- The user should ping the gateway IP of the router if the source and destination are not of the same subnet mask.
- In case both pings fail, then the user must check whether the configuration settings of the subnet mask and the route to the destination are defined properly in the routing table.
- If the configuration settings are fine, then the user should check whether the source host can ping a different hop in the LAN network other than the destination host.
- If the user is unable to ping another device, then there might be various issues such as IP address conflict, configuration issues, and physical connectivity issues.
- To rectify any IP address conflict, the user should disconnect all doubtful devices from the LAN. At this point, the user needs to ping the device from some other device on the same subnet/LAN. A successful ping signifies that the disconnected device is using the same IP as the pinged device; then, modify the IP according to the plan. If the local connectivity issue persists, then there might be a problem with the physical connectivity or configuration.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Troubleshooting Techniques: Troubleshooting Routing Problems

When data packets are routed across a network, there are chances of fault occurrence. Based on the type of fault, the user should make a plan to resolve the fault. The type of faults that are observed between source and destination hosts when data packets are routed across a network are as follows:

- Failure to define the route in a router between the source and destination
- Usage of an incorrect routing protocol to find the route to the next hop/destination
- Fault in the router's software
- Firewall or filter hindering the movement of data packets to the destination node
- Configuration faults at the source router end

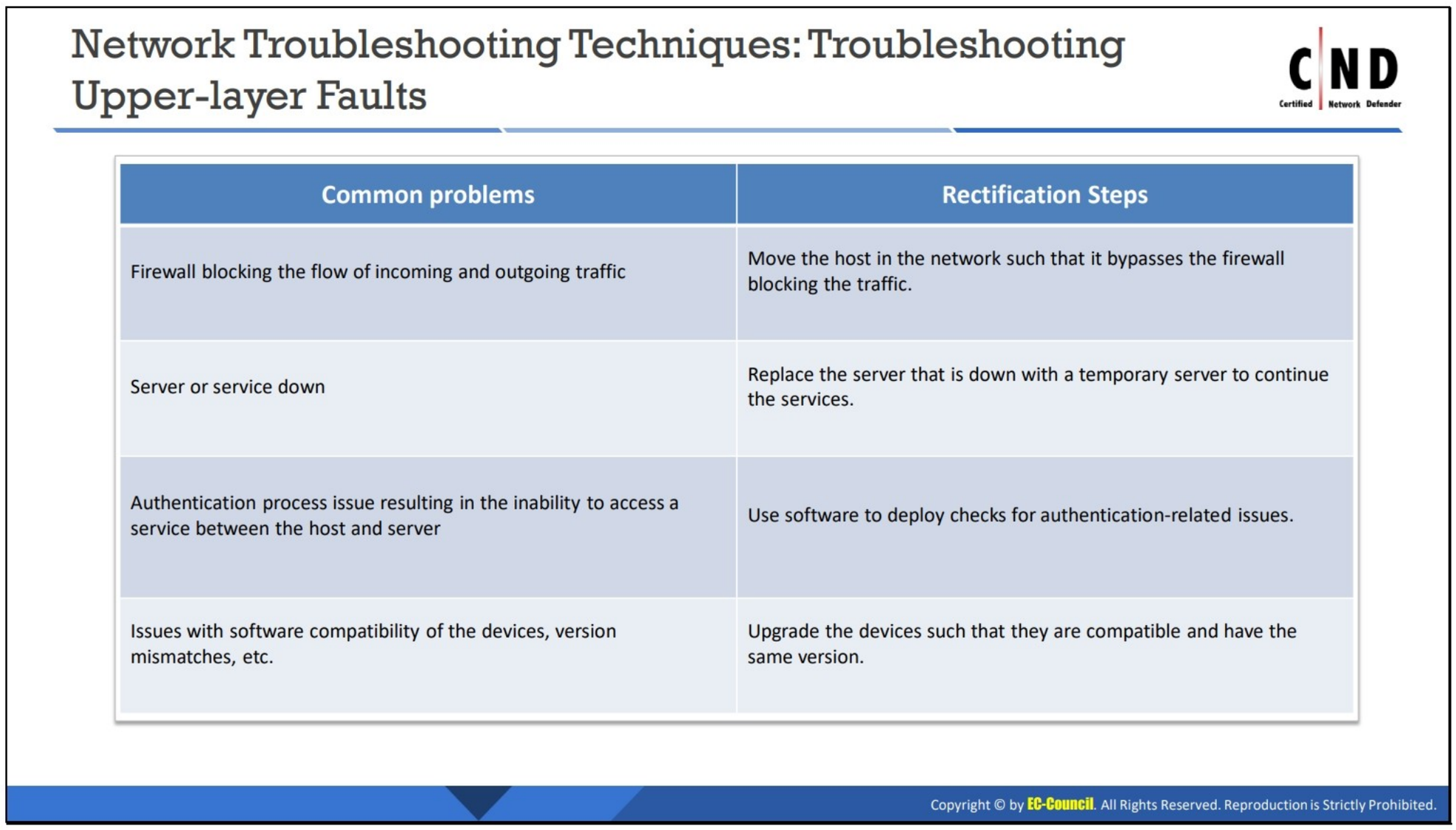
Steps to Troubleshoot Routing Issues

- The first step to troubleshoot routing issues is to locate the hop between the source and destination where the problem occurred.
- From the source to the destination, verify the IP connectivity and routing protocols at each hop.
- Use the traceroute utility to locate the hop/router responsible for the problem.
- After identifying the hop where the problem occurred, login to the router through Telnet and ping the source and destination hosts.
- If the ping is unsuccessful, then the routing table should be verified for the route between the source and destination.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- If there is a small percentage of successful ping responses, then there might be multiple defined paths to reach the destination, among which one results in failure owing to the occurrence of a routing loop in the path. To resolve this issue, the looping hop should be traced, and the configuration should be rectified.
- After rectification, if the problem persists, then check the used routing protocol and change it according to the network.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Troubleshooting Techniques: Troubleshooting Upper-layer Faults

If the user has already checked the physical connectivity, local connectivity, IP connectivity, and routing issues but was unable to find a fault, then there is a chance that the fault has occurred in the transport- and application-layer protocols.

The following are potential reasons for the occurrence of faults:

- The data connection is not working.
- The firewall/packet filter prevents the incoming and outgoing traffic.
- A specific service on the server is not working.
- There are authentication and access concerns between the client and server host.
- There are issues related to the incompatibility of software or mismatch of its version between the source and destination host.

The following table outlines rectification steps based on the category of the fault.

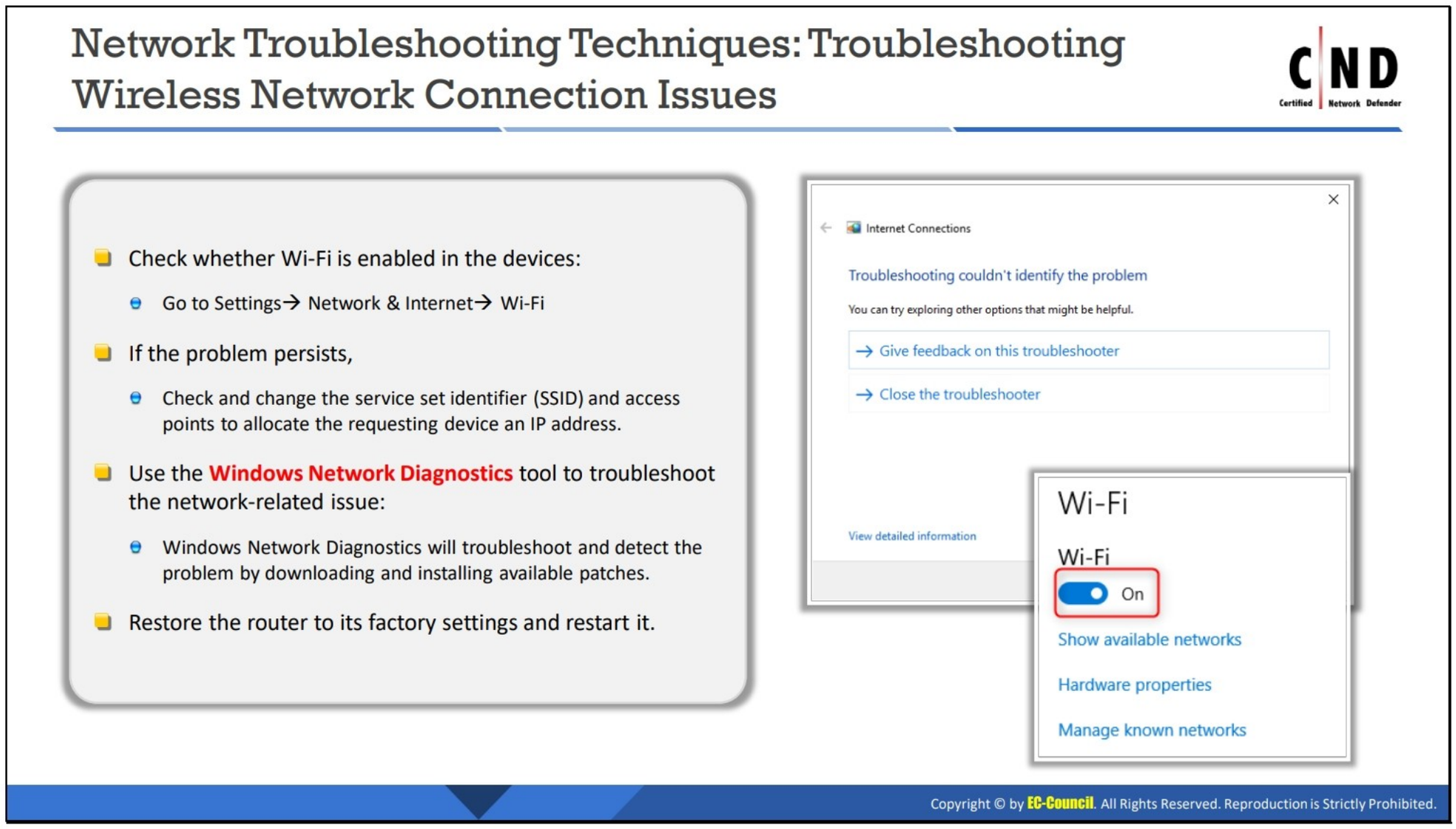
Common Problems	Rectification Steps
Firewall blocking the flow of incoming and outgoing traffic	Move the host in the network such that it bypasses the firewall blocking the traffic.
Service/server down	Replace the server that is down with a temporary server to continue services.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Authentication process issue resulting in the inability to access services between the host and server	Use software to deploy checks for authentication-related issues.
Issues with the software compatibility of devices, version mismatches, etc.	Upgrade the devices such that they are compatible and have the same software version.

Table A.15: Rectification Steps Based on the Category of the Fault

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Troubleshooting Techniques: Troubleshooting Wireless Network Connection Issues

To troubleshoot a wireless network connection issue, the user primarily needs to check whether Wi-Fi is enabled on the devices by performing the following steps:

- Click on the **Start Menu** button and go to **Settings**. Next, click on **Network & Internet**.
- Enable **Wi-Fi**.

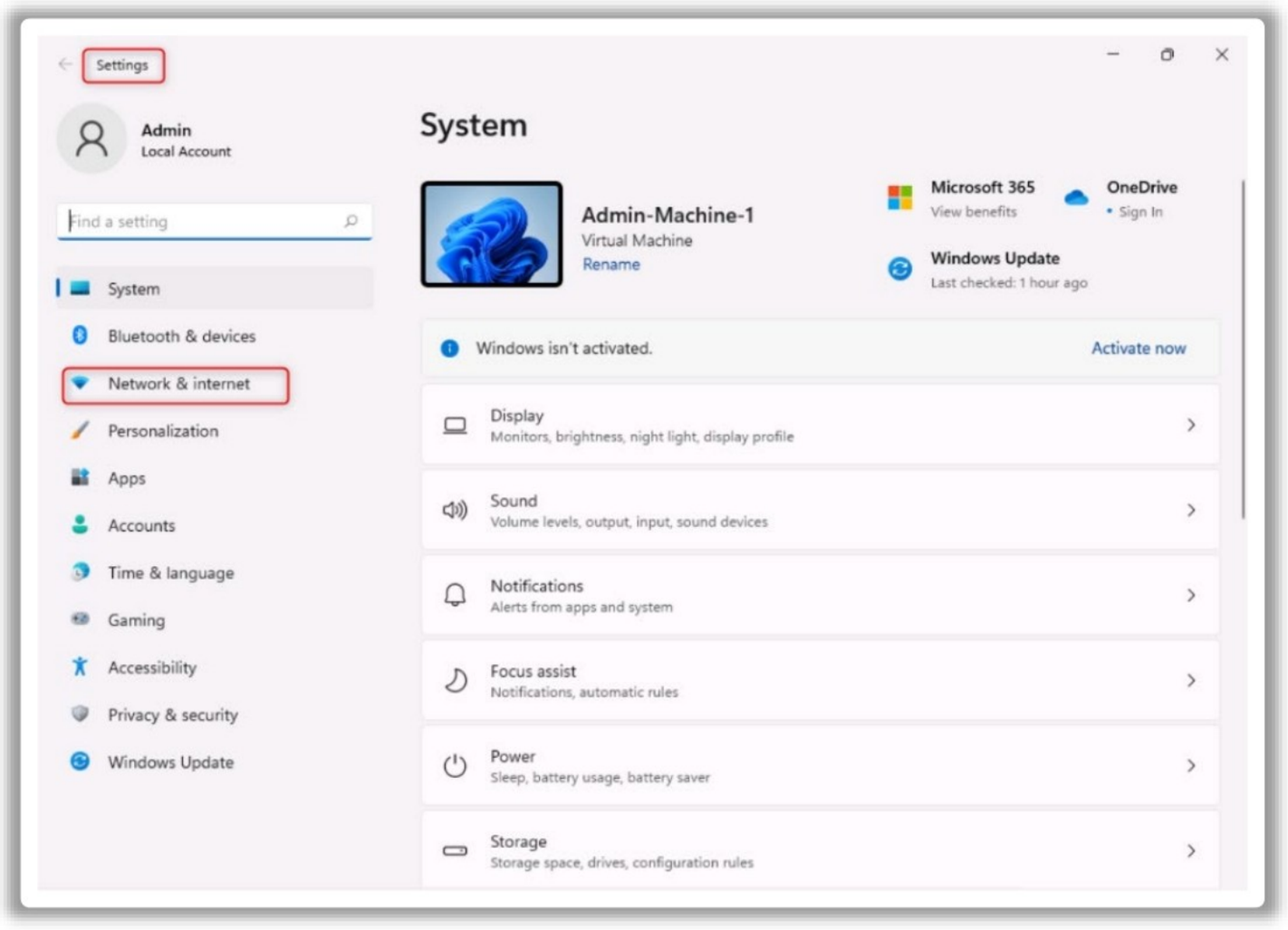


Figure A.129: Go To "Network & Internet" Setting

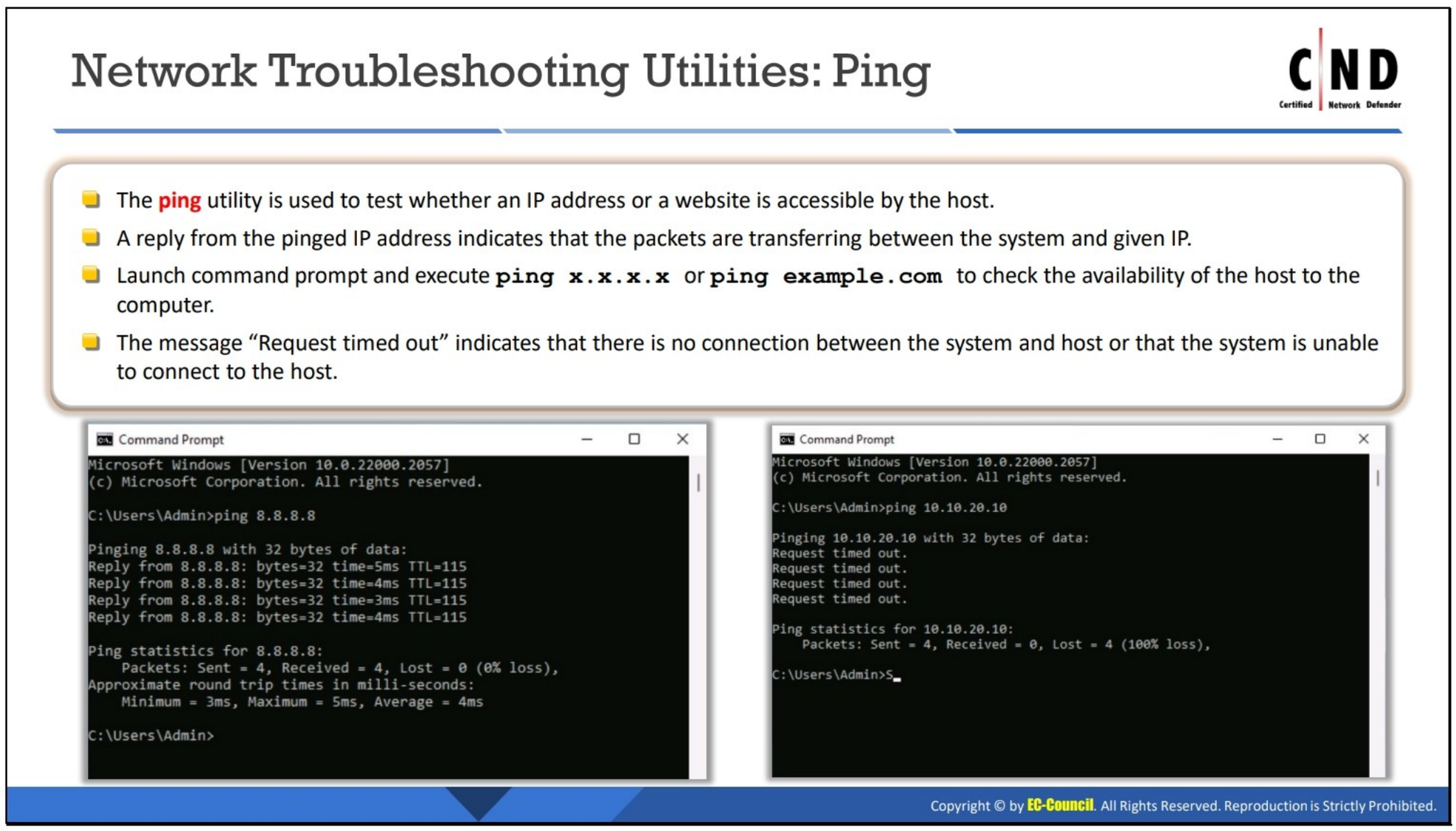
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

If Wi-Fi is not listed in **Network & Internet**, then the user would not be able to connect to the wireless network. If there is no Wi-Fi on the computer, then the Internet access icon will also be missing from the taskbar.

Steps to Troubleshoot Wireless Network Connection Issues

- If the user is unable to connect the device using Wi-Fi, then the user must first check the LAN and WAN cable connections. Ensure that the Ethernet cable connection is tight, and check the status of indicator lights. If the light is not green, then there might be a problem with the cable or port. Then, the user must change the faulty port or cable connection.
- If the problem persists, then the user should check the Wi-Fi network adaptor settings and enable network adaptor settings. The user should ensure that the airplane mode on the device is disabled. If the airplane mode is enabled, then the device would not allow wireless network connectivity.
- If the problem persists, check and change the service set identifier (SSID) and access points to allocate the requesting device an IP address.
- Use the Windows Network Diagnostics tool to troubleshoot network-related issues. Windows Network Diagnostics will troubleshoot the defect/problem by downloading and installing available patches.
- Restore the router to its factory settings and restart it.
- After performing all the steps, if the user is unable to resolve the wireless network connectivity issue, then there might be other reasons such as a firewall or packet filter preventing the user from connecting to the network or an issue with the authentication protocol. Hence, the user should reconfigure all the network settings and verify the IP routing by using ping.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Troubleshooting Utilities: Ping

The ping utility is used to test whether an IP address or a website is accessible by a host. Ping works by sending ICMP echo requests to the targeted host and waiting for ICMP echo replies. It measures the Internet speed and reports errors and losses of data packets. A reply from the pinged IP address indicates that the packets are transferring between the system and given IP. Launch the command prompt and execute **`ping x.x.x.x`** or **`ping example.com`** to check the availability of the host to the computer.

Network Troubleshooting Using Ping

The primary step is to ping the remote host. If the user has trouble connecting to a website, then the user must ping the URL. If the ping is returned, then the network is working properly, and the issues lie somewhere else.

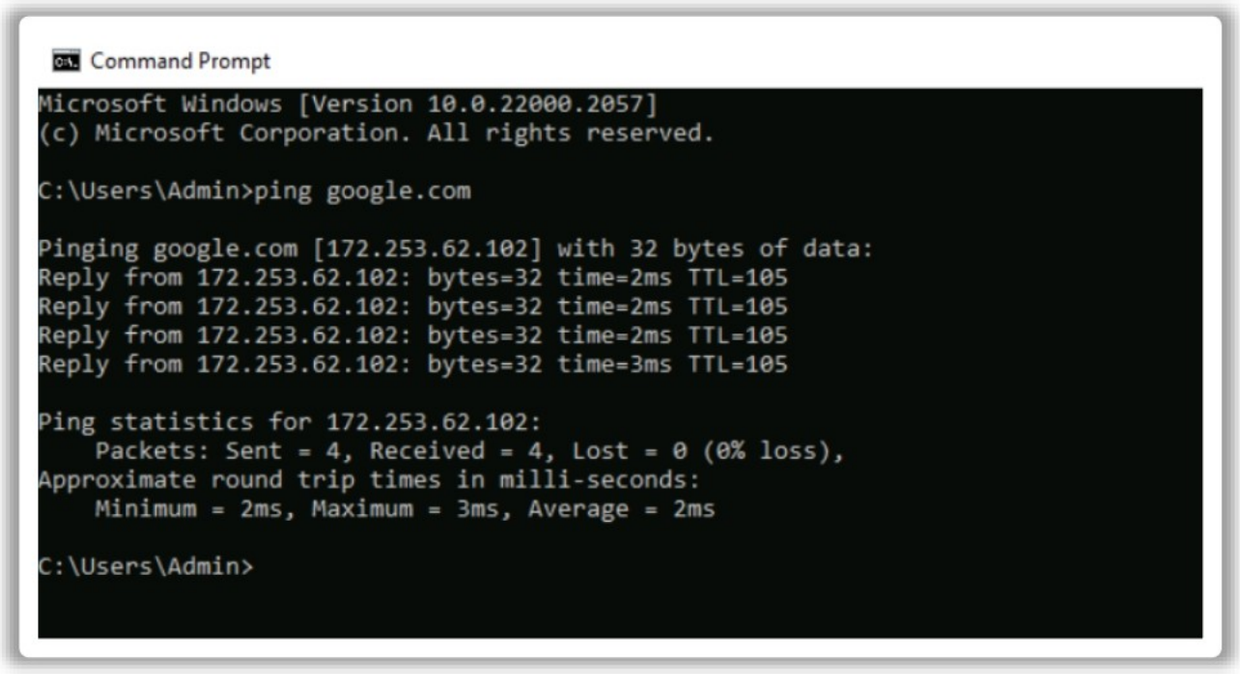


Figure A.130: Ping a Website

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The four replies in the screenshot above indicate that the network connection is good and the server is reachable. In this scenario, the fault could lie with the web-server configuration. If the ping is missed, then there might be a problem with the network. If the replies have a wide variation in the maximum and minimum time of the ping, then there could be connection issues such as network congestion.

To test connectivity, some administrators ping Google's primary DNS server (**`ping 8.8.8.8`**) because it is easy to remember and is continuously running.

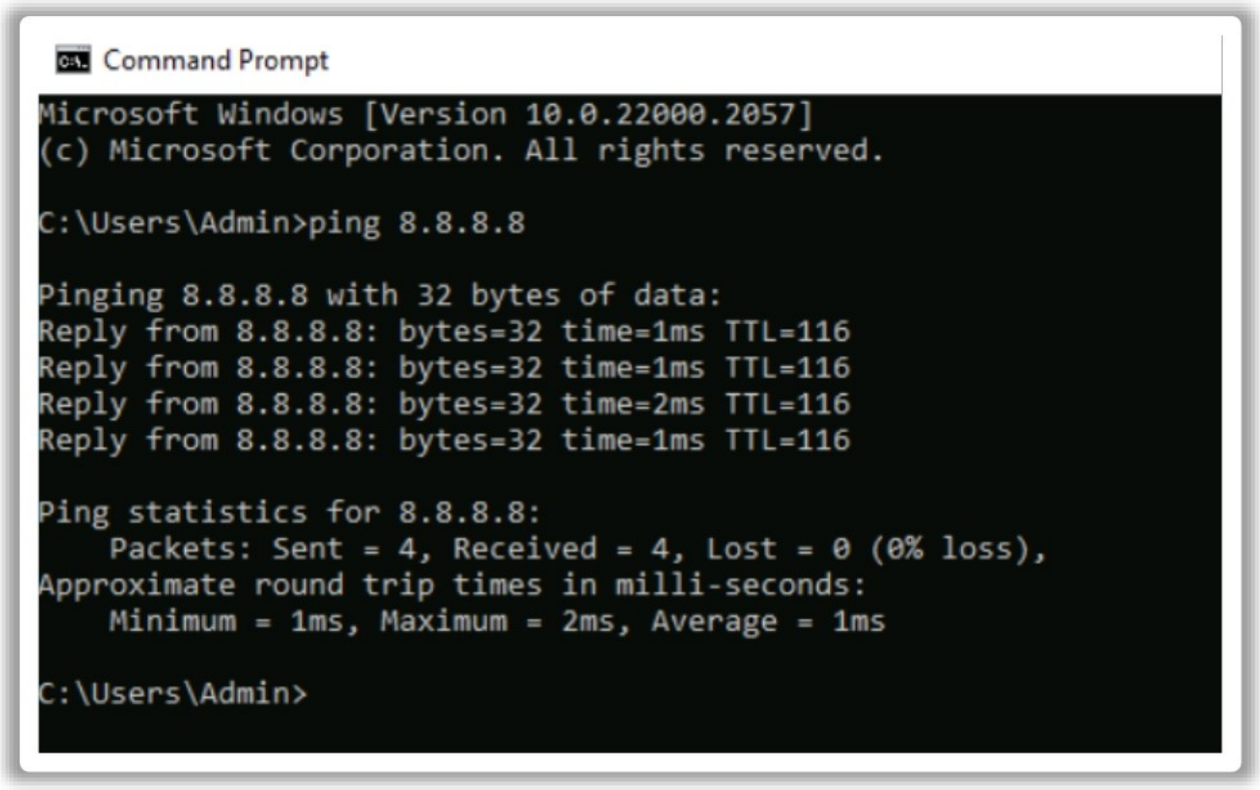


Figure A.131: Ping Google's Primary DNS Server

The message "Request timed out" in the screenshot above shows that there is no connection between the system and host, or the system is unable to connect to the host. It also indicates that the host might be down or unreachable, the host might be behind a firewall, or the user does not have network connectivity.

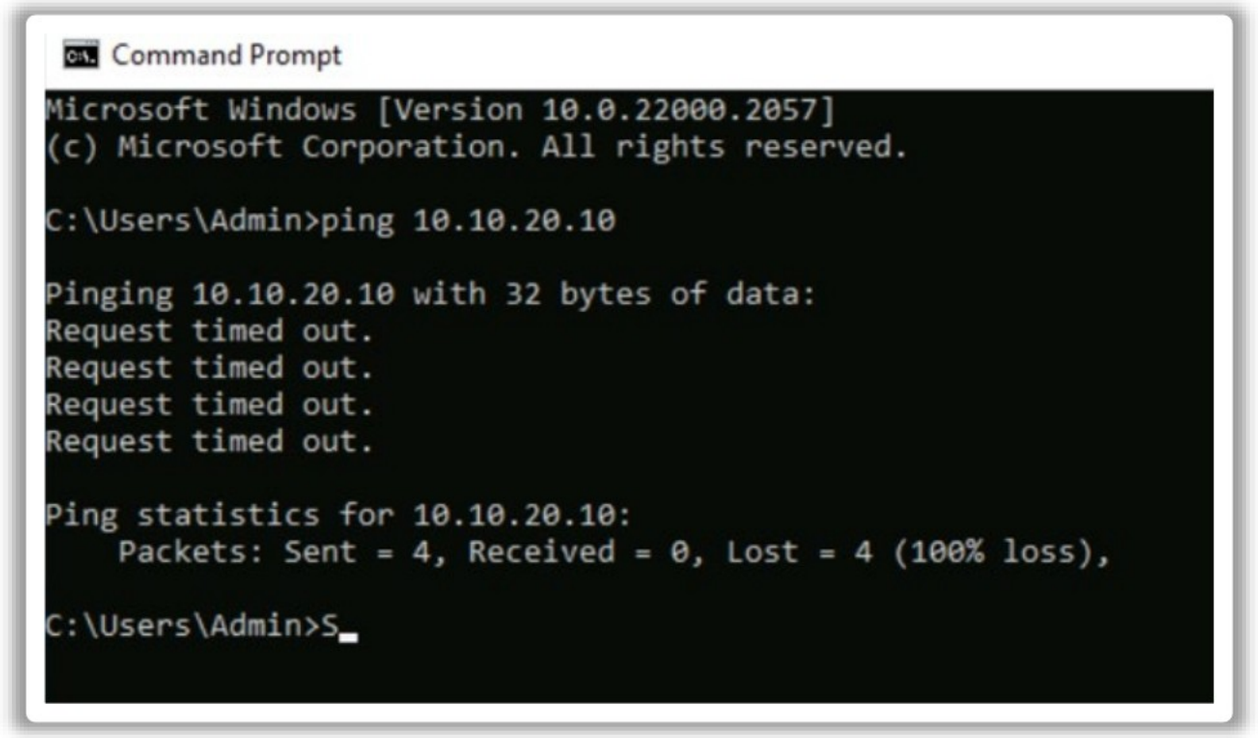
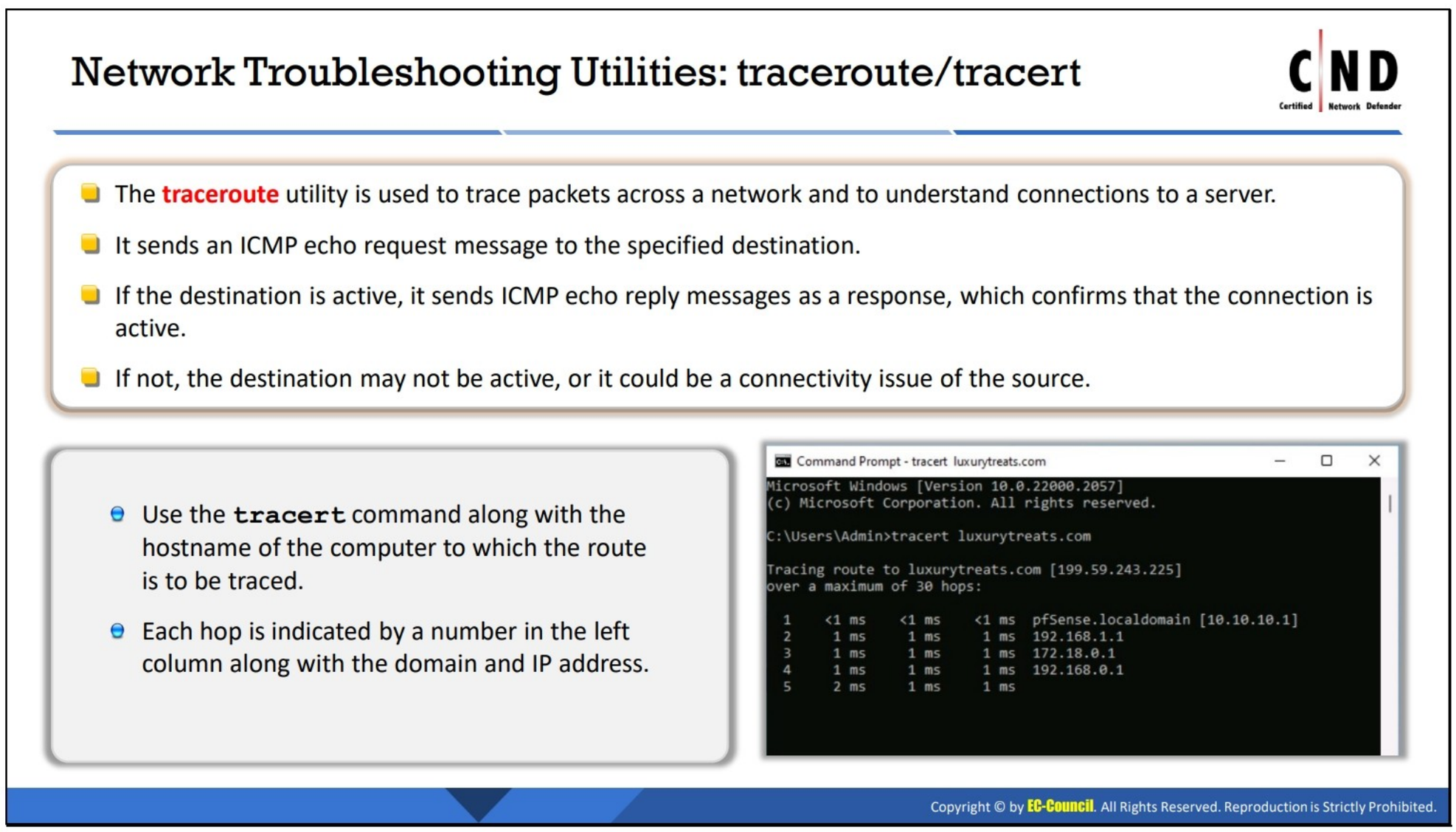


Figure A.132: No Connection between a System and a Host

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Troubleshooting Utilities: traceroute/tracert

The multi-OS-compatible command-line tool trace route (tracert)/traceroute is used to trace packets across a network and to understand connections to a server. It allows the user to understand Internet connection problems, including packet loss and high latency.

tracert (for Windows) uses ICMP. It sends ICMP echo request messages to the specified destination. If the destination is active, it sends ICMP echo reply messages as a response, confirming that the connection is active. Otherwise, the destination may not be active, or it could be a connectivity issue of the source.

Steps to Use tracert (for Windows)

- Run the traceroute command with example.com (any website):

```
tracert example.com
```

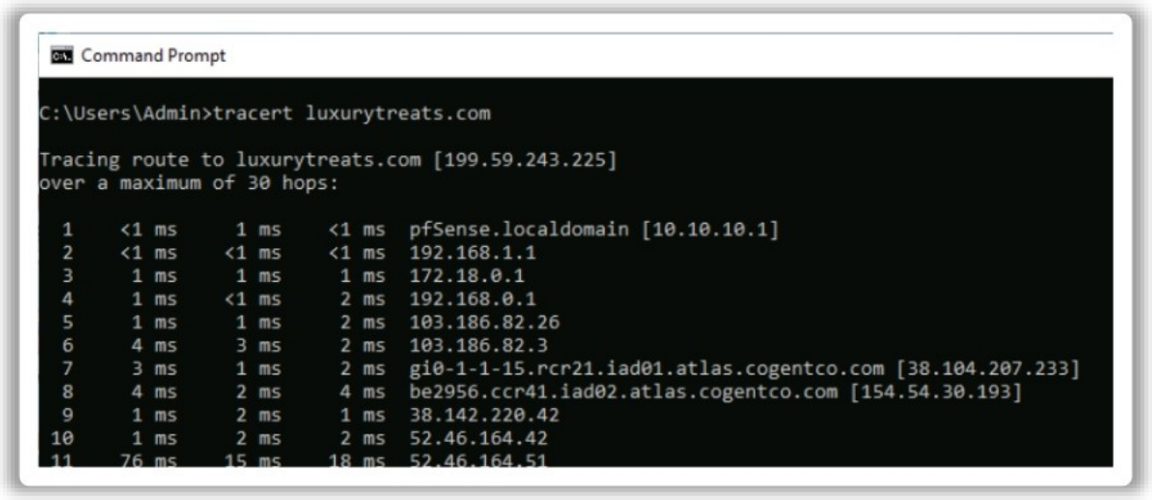


Figure A.133: Run the Command “tracert”

Observe the route take form as the system receives responses from the routers along the way.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Run the tracert command for another website hosted in different regions of the world. Observe how the paths differ.

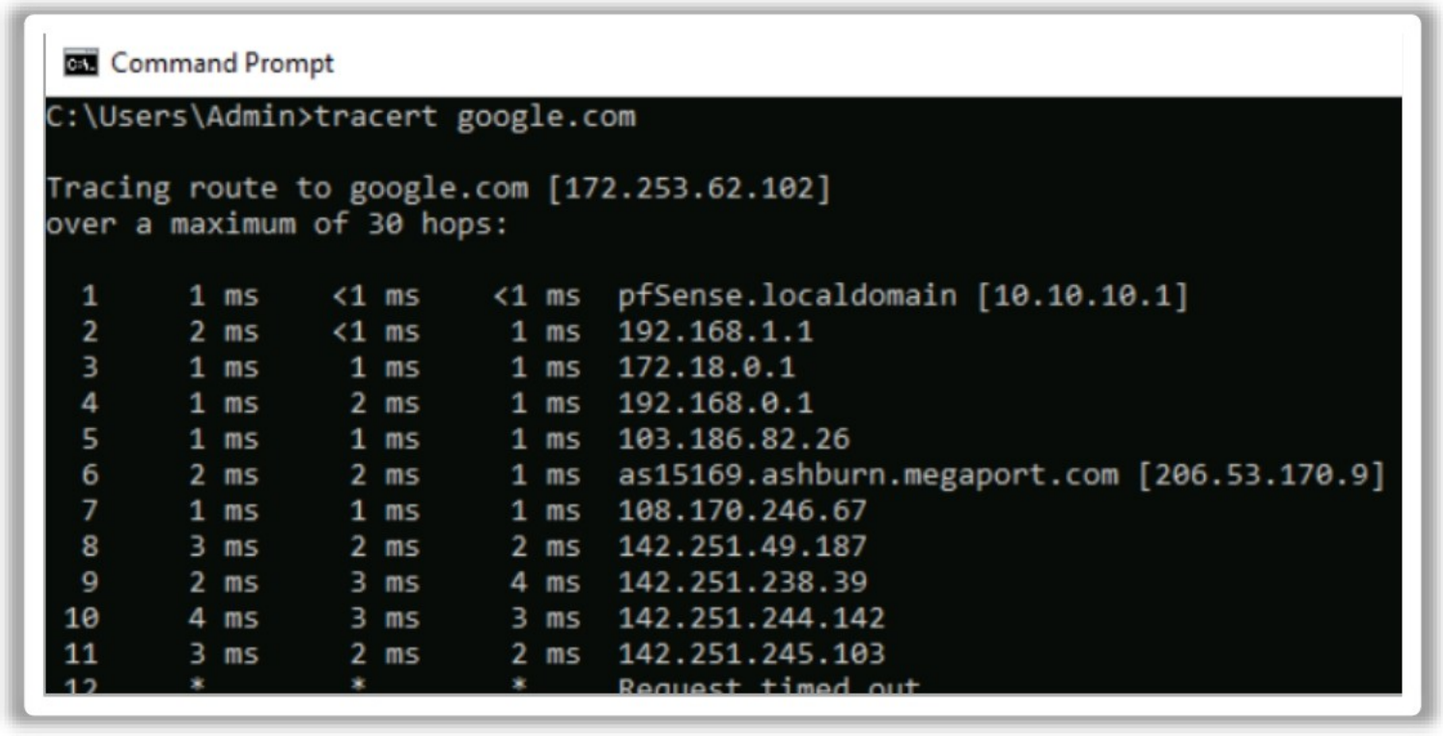


Figure A.134: Run the Command "tracert"

In the above screenshot, the first line represents the home router, assuming the user is behind a router. The remaining lines represent the ISP. The format of each line is as follows:

`Hop RTT1 RTT2 RTT3 Domain Name [IP Address]`

Hop: When a packet passes by a router, it is said to have performed a "hop."

RTT1, RTT2, or RTT3: Also referred to as "latency," it is the round-trip time that a packet takes to perform a hop and return to the system (in milliseconds).

*: This output is produced when no response is received, indicating packet loss.

Domain name (IP address): The domain name allows the user to determine the location of a router. If it is not available, only the IP address of the router is displayed.

traceroute (for *nix Systems)

Traceroute uses UDP on typical *nix systems and sends traffic to port 33434 by default:

`traceroute example.com`

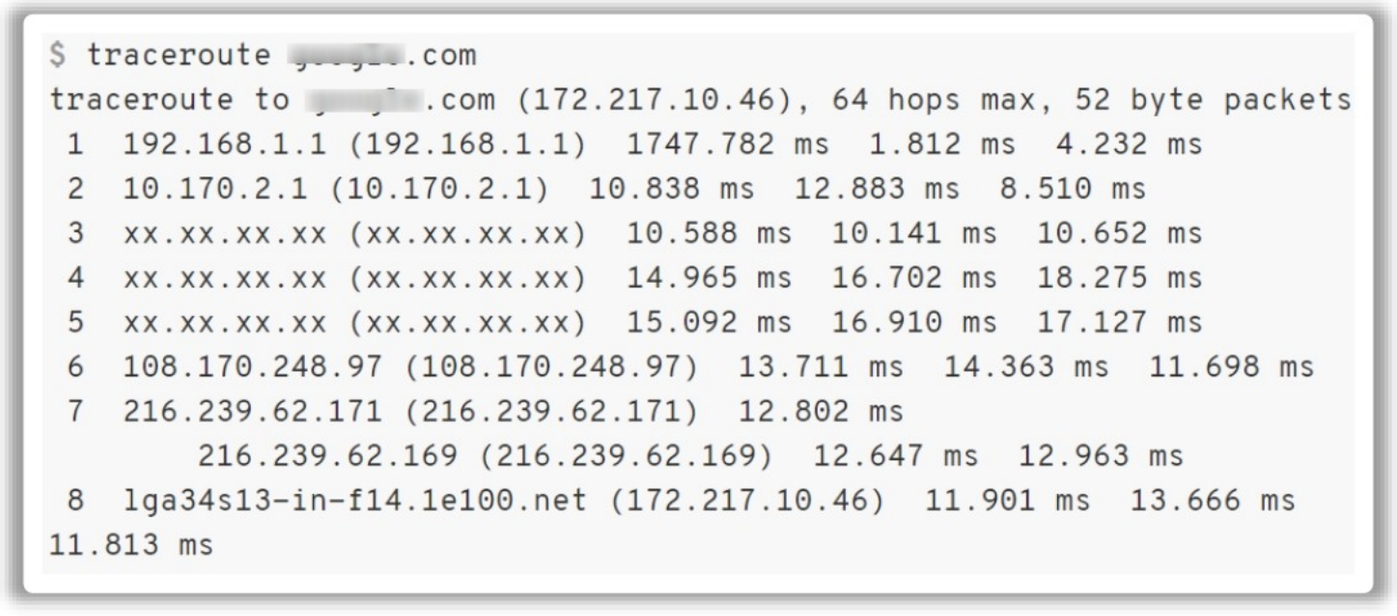
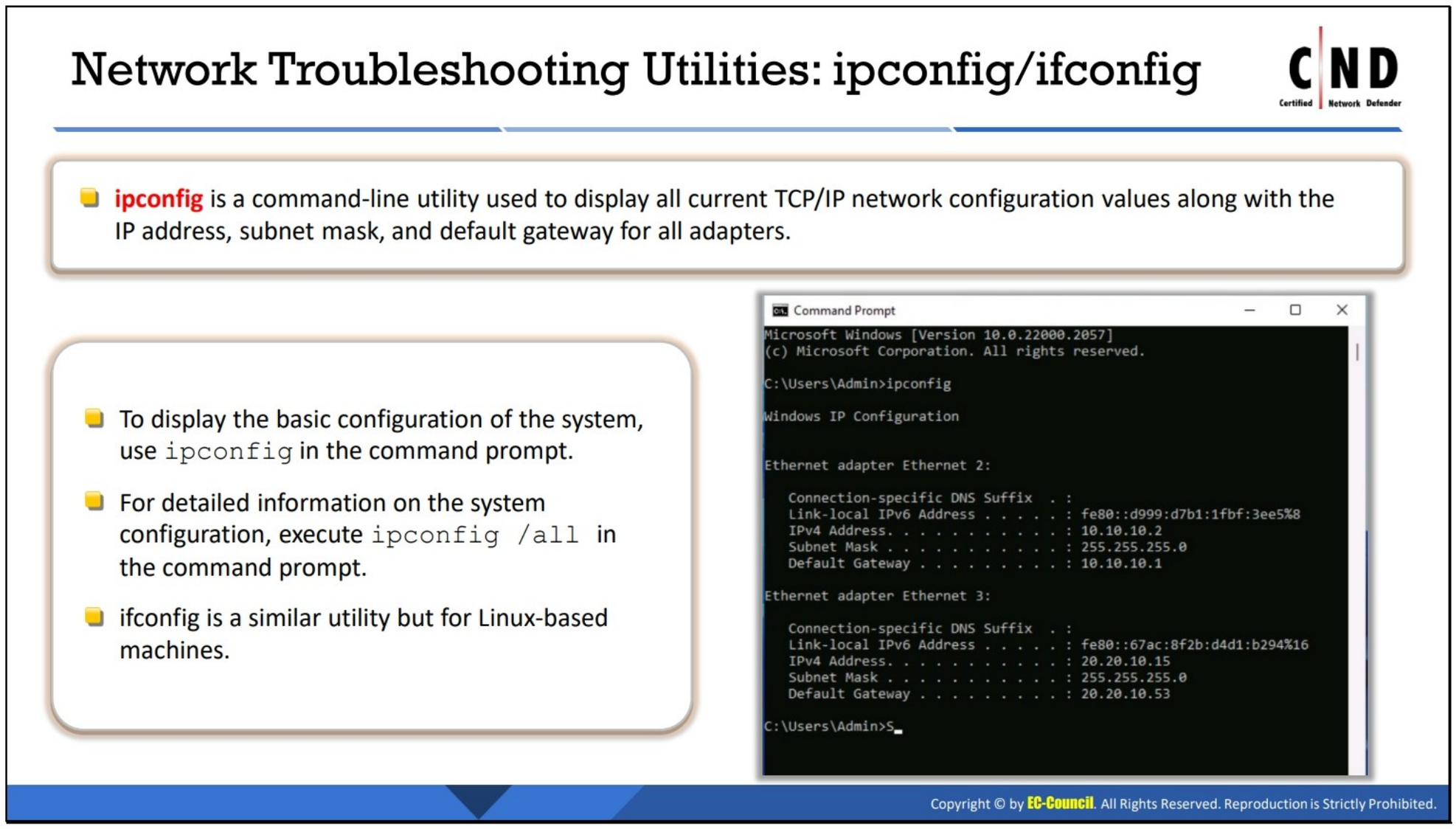


Figure A.135: Use "traceroute" for *nix Systems

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Troubleshooting Utilities: ipconfig/ifconfig

ifconfig: When troubleshooting a networking issue, the Linux- or Unix-based OS utility interface configuration (ifconfig) helps display the specific IP address of the affected hosts, netmask of a network interface, and maximum transmission unit (MTU). This utility provides commands to configure and enable/disable a network interface.

Steps to Use ifconfig

- To display the network settings of all the active network interfaces on the system, use ifconfig without any options.

```
# ifconfig

eth0      Link encap:Ethernet  HWaddr 00:0C:29:28:FD:4C
          inet addr:192.168.50.2  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe28:fd4c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6093 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4824 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6125302 (5.8 MiB)  TX bytes:536966 (524.3 KiB)
          Interrupt:18 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:480 (480.0 b)  TX bytes:480 (480.0 b)
```

Figure A.136: Display Network Settings of a Network Interface

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- To display the details of all network interfaces, use the command as shown in the screenshot below.

```
# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0c:29:9b:49:bc
          inet addr:192.168.134.128  Bcast:192.168.134.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe9b:49bc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11545 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6177 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:923360 (923.3 KB)  TX bytes:1712607 (1.7 MB)

eth1      Link encap:Ethernet  HWaddr 00:0c:29:8b:89:bc
          inet addr:  Bcast:  Mask:
          inet6 addr: fe80::20c:29ff:fe9b:49bc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11545 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6177 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:923360 (923.3 KB)  TX bytes:1712607 (1.7 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

virbr0    Link encap:Ethernet  HWaddr 3a:bf:4c:fb:90:b6
          inet addr:192.168.122.1  Bcast:192.168.122.255  Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
```

Figure A.137: Display a Network Interface Details

- Use the interface (eth0) command to display only specific interface details such as the IP address and MAC address.

```
# ifconfig eth0

eth0      Link encap:Ethernet  HWaddr 00:0C:29:28:FD:4C
          inet addr:192.168.50.2  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe28:fd4c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6119 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4841 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6127464 (5.8 MiB)  TX bytes:539648 (527.0 KiB)
          Interrupt:18 Base address:0x2000
```

Figure A.138: Display any Specific Interface Details

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- To assign an IP address and gateway to interface on the fly, use the following command:

```
# ifconfig eth0 192.168.50.5 netmask 255.255.255.0
```

  The setting will be removed if system reboots.

- To enable a specific interface, use the following command:

```
# ifup eth0
```

- To disable a specific Interface, use the following command:

```
ifdown eth0
```

- To set the required MTU, use the following command, where XXXX represents the size:

```
# ifconfig eth0 mtu XXXX
```

- To set the interface in the promiscuous mode to capture all the packets and to analyze them later, use the following command:

```
# ifconfig eth0 – promisc
```

- To configure an IP address, specify the interface to be configured, IP address, and subnet address.

```
[redacted]:~ # ifconfig eth0 5.5.5.5 netmask 255.255.255.0
[redacted]:~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:17:1B:27
          inet addr:5.5.5.5  Bcast:5.5.5.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe17:1b27/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:201 errors:0 dropped:0 overruns:0 frame:0
          TX packets:196 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:22370 (21.8 Kb)  TX bytes:17563 (17.1 Kb)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1060 (1.0 Kb)  TX bytes:1060 (1.0 Kb)
```

Figure A.139: Display an Interface, IP, and Subnet Address

- To enable/disable an interface, perform the following:
  - Use the “up” or “ifup” flag with the interface name (for example, eth0) that will activate a network interface.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use the “down” or “ifdown” flag with the interface name that will deactivate the specified network interface.

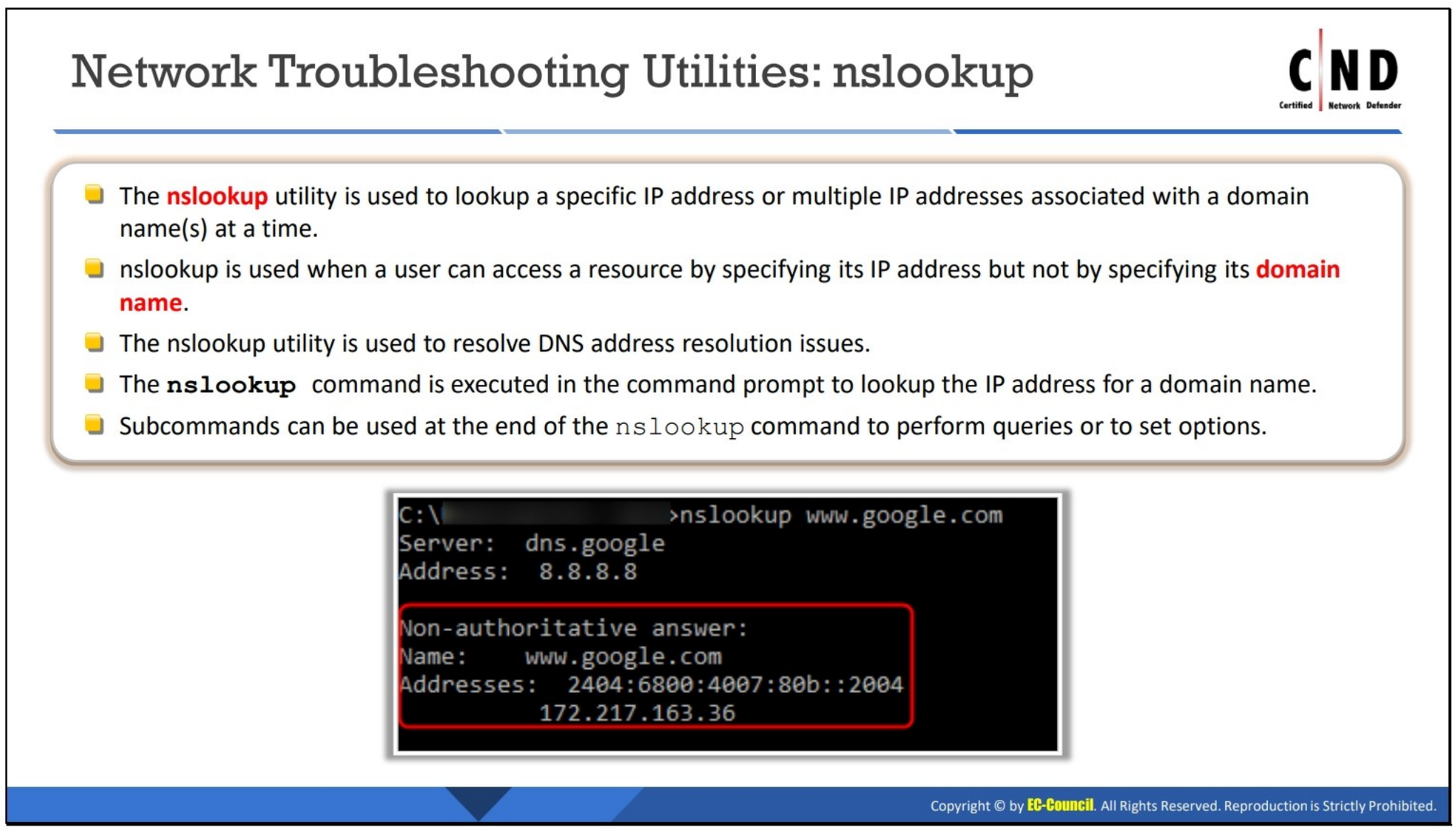
```
[redacted]:~ # ifconfig eth0 down
[redacted]:~ # ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1060 (1.0 Kb)  TX bytes:1060 (1.0 Kb)

[redacted]:~ # ifconfig eth0 up
[redacted]:~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:17:1B:27
          inet addr:192.168.208.133  Bcast:192.168.208.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe17:1b27/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:201 errors:0 dropped:0 overruns:0 frame:0
          TX packets:199 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:22370 (21.8 Kb)  TX bytes:17841 (17.4 Kb)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

Figure A.140: Enable/Disable an Interface

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Troubleshooting Utilities: nslookup

nslookup is a program that allows the administrator or system user to enter a host name and retrieve the corresponding IP address or DNS record. It is also used for reverse DNS lookup to find the host name for a given IP address. The nslookup utility is used to look up a specific IP address or multiple IP addresses associated with a domain name(s) at a time. nslookup is used when a user can access a resource by specifying its IP address but not by specifying its domain name. nslookup safeguards against phishing attacks and prevents cache poisoning.

The nslookup utility is used to resolve DNS address resolution issues. The nslookup command is executed in the command prompt to look up the IP address for a domain name. Subcommands can be used at the end of the nslookup command to perform queries or to set options. The optimal mail servers SMTP, Post Office Protocol (POP), and Internet Message Access Protocol (IMAP) for the desired domain can also be searched using nslookup.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Searching for the Domain Name Using nslookup

The user should enter the domain name into the command line to find the IP address or vice versa. nslookup gives the results shown in the screenshot below for google.com.

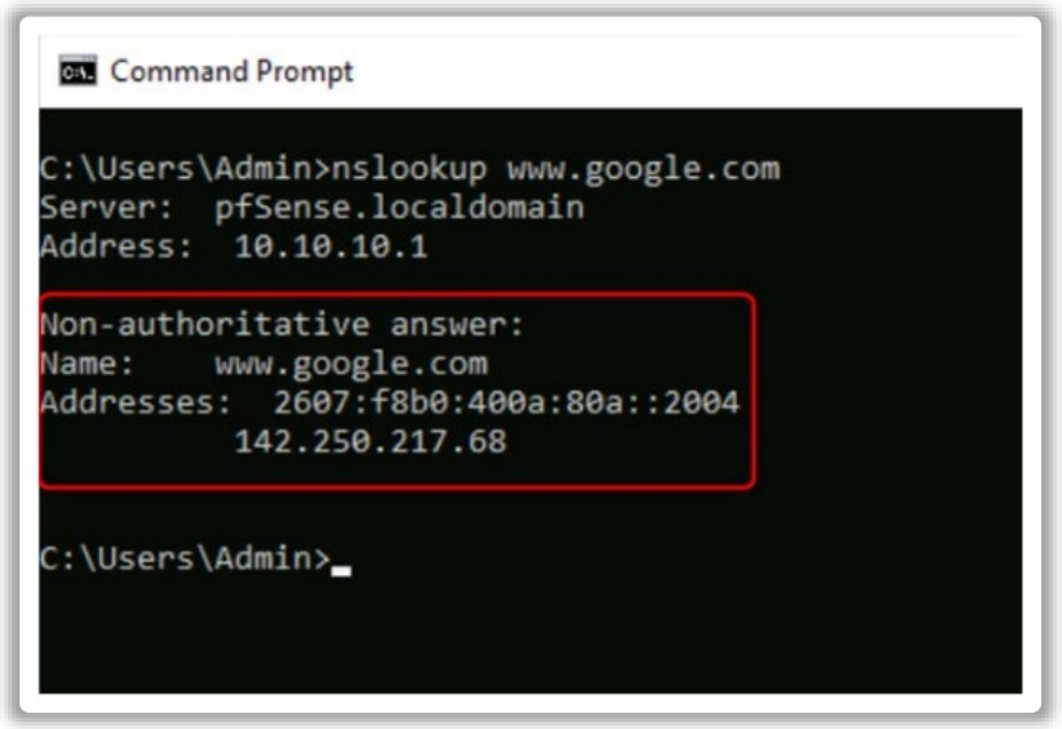
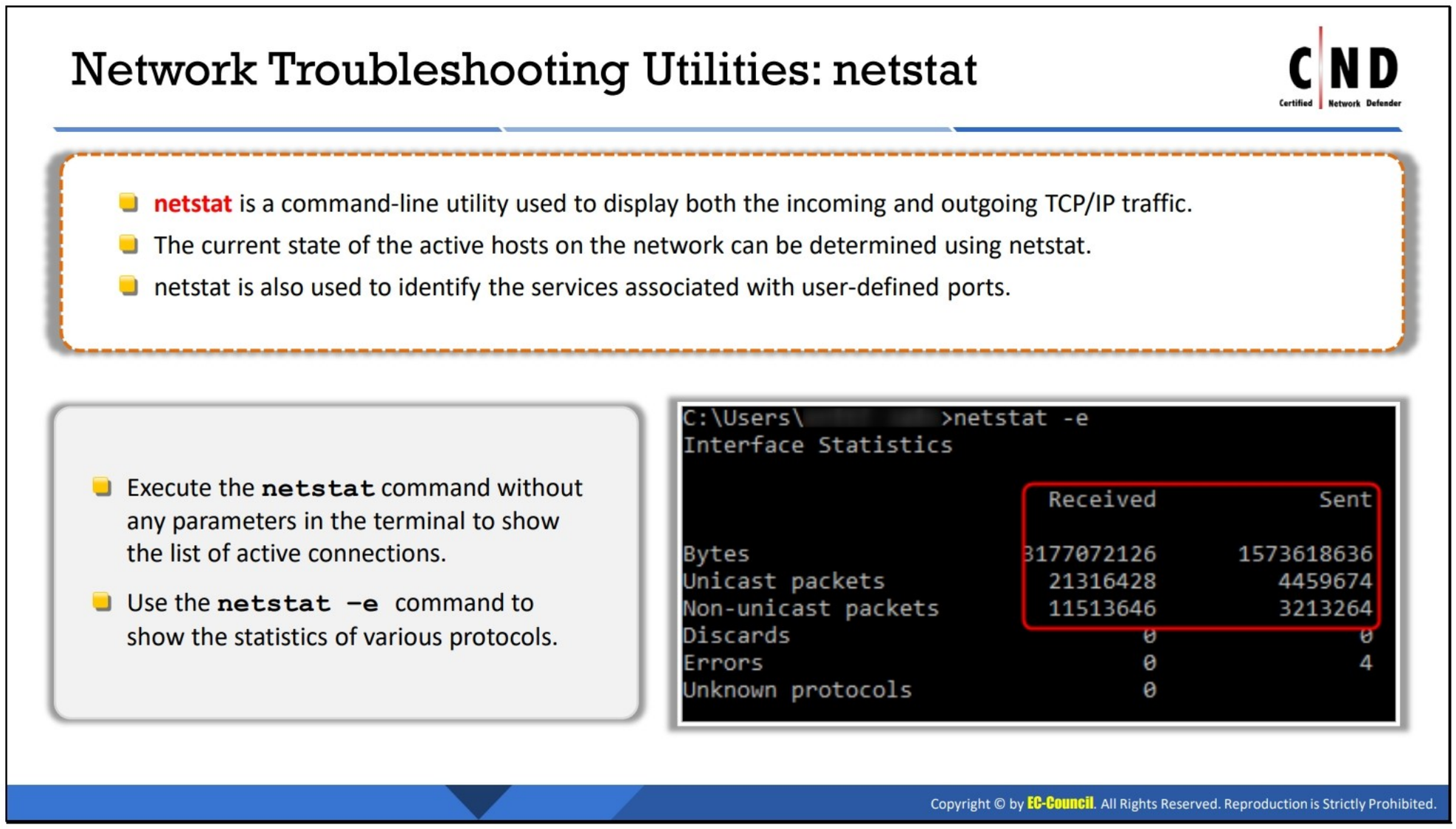


Figure A.141: Search Domain Name using “nslookup” Command

The notification **Non-authoritative answer** indicates that the local DNS server failed to provide an answer to the query itself and contacted other name servers. The results of nslookup consist of IPv4 (four-figure) and IPv6 addresses (long and dived with colons) of the google domain.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Troubleshooting Utilities: netstat

The Linux utility network statistics (netstat) displays network connections (incoming and outgoing), network statistics, protocol statistics, and routing tables. It also displays the connections that are not established properly and the connections that are being torn down, and it helps solve slowdowns, bottlenecks, or outage problems in networks.

Steps to Use netstat

- Perform the following to list various listening ports:
  - The command shown below lists all the listening ports of TCP and UDP connections.

```
# netstat -a | more

Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:sunrpc                    *:*                         LISTEN
tcp        0     52 192.168.0.2:ssh             192.168.0.1:egs             ESTABLISHED
tcp        1      0 192.168.0.2:59292           www.gov.com:http            CLOSE_WAIT
tcp        0      0 localhost:smtp              *:*                         LISTEN
tcp        0      0 *:59482                     *:*                         LISTEN
udp        0      0 *:35036                     *:*
udp        0      0 *:npmp-local                *:*

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     16972  /tmp/orbit-root/linc-76b-0-6fa08790553d6
unix  2      [ ACC ]     STREAM     LISTENING     17149  /tmp/orbit-root/linc-794-0-7058d584166d2
unix  2      [ ACC ]     STREAM     LISTENING     17161  /tmp/orbit-root/linc-792-0-546fe905321cc
unix  2      [ ACC ]     STREAM     LISTENING     15938  /tmp/orbit-root/linc-74b-0-415135cb6aeab
```

Figure A.142: List the Ports of TCP and UDP Connections

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The command shown below lists TCP port connections.

```
# netstat -at

Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 localhost:ipp               *:*                         LISTEN
tcp        0      0 localhost:smtp              *:*                         LISTEN
tcp        0     52 192.168.0.2:ssh             192.168.0.1:egs             ESTABLISHED
tcp        1      0 192.168.0.2:59292           www.gov.com:http            CLOSE_WAIT
```

Figure A.143: List TCP Port Connections

- The command shown below lists UDP port connections.

```
# netstat -au

Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
udp        0      0 *:35036                     *:*
udp        0      0 *:npmp-local                *:*
udp        0      0 *:mdns                      *:*
```

Figure A.144: List UPD Port Connections

- Perform the following to list various listening connections:
  - The command shown below lists all listening connections.

```
# netstat -l

Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:sunrpc                    *:*                         LISTEN
tcp        0      0 *:58642                     *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
udp        0      0 *:35036                     *:*
udp        0      0 *:npmp-local                *:*

Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     16972  /tmp/orbit-root/linc-76b-0-6fa08790553d6
unix  2      [ ACC ]     STREAM     LISTENING     17149  /tmp/orbit-root/linc-794-0-7058d584166d2
unix  2      [ ACC ]     STREAM     LISTENING     17161  /tmp/orbit-root/linc-792-0-546fe905321cc
unix  2      [ ACC ]     STREAM     LISTENING     15938  /tmp/orbit-root/linc-74b-0-415135cb6aeab
```

Figure A.145: List All Listening Connections

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The command shown below lists all TCP listening ports.

```
# netstat -lt

Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:dctp                      *:*                         LISTEN
tcp        0      0 *:mysql                     *:*                         LISTEN
tcp        0      0 *:sunrpc                    *:*                         LISTEN
tcp        0      0 *:munin                     *:*                         LISTEN
tcp        0      0 *:ftp                       *:*                         LISTEN
tcp        0      0 localhost.localdomain:ipp   *:*                         LISTEN
tcp        0      0 localhost.localdomain:smtp  *:*                         LISTEN
tcp        0      0 *:http                      *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 *:https                     *:*                         LISTEN
```

Figure A.146: List TCP Listening Ports

- The command shown below lists all UDP listening ports.

```
# netstat -lu

Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
udp        0      0 *:39578                     *:*
udp        0      0 *:meregister                *:*
udp        0      0 *:vpps-qua                  *:*
udp        0      0 *:openvpn                   *:*
udp        0      0 *:mdns                      *:*
udp        0      0 *:sunrpc                    *:*
udp        0      0 *:ipp                       *:*
udp        0      0 *:60222                     *:*
udp        0      0 *:mdns                      *:*
```

Figure A.147: List UDP Listening Ports

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Perform the following to list statistics for different protocols.
  - The command shown below lists the statistics for all protocols.

```
# netstat -s

Ip:
    2461 total packets received
    0 forwarded
    0 incoming packets discarded
    2431 incoming packets delivered
    2049 requests sent out
Icmp:
    0 ICMP messages received
    0 input ICMP message failed.
    ICMP input histogram:
    1 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 1
Tcp:
    159 active connections openings
    1 passive connection openings
    4 failed connection attempts
    0 connection resets received
    1 connections established
    2191 segments received
    1745 segments send out
    24 segments retransmited
    0 bad segments received.
    4 resets sent
Udp:
    243 packets received
    1 packets to unknown port received.
    0 packet receive errors
    281 packets sent
```

Figure A.148: List Statistics for All Protocols

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The command shown below lists statistics for TCP.

```
# netstat -st

Tcp:
    2805201 active connections openings
    1597466 passive connection openings
    1522484 failed connection attempts
    37806 connection resets received
    1 connections established
    57718706 segments received
    64280042 segments send out
    3135688 segments retransmited
    74 bad segments received.
    17580 resets sent
```

Figure A.149: List Statistics for TCP

- The command shown below lists statistics for UDP.

```
# netstat -su

Udp:
    1774823 packets received
    901848 packets to unknown port received.
    0 packet receive errors
    2968722 packets sent
```

Figure A.150: List Statistics for UDP

- The command shown below displays the service name with PID.

```
# netstat -tp

Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 192.168.0.2:ssh            192.168.0.1:egs             ESTABLISHED 2179/sshd
tcp        1      0 192.168.0.2:59292          www.gov.com:http            CLOSE_WAIT  1939/clock-applet
```

Figure A.151: List the Service Names with PID

- The command shown below displays the kernel IP routing table.

```
# netstat -r

Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.0.0     *               255.255.255.0   U         0 0          0 eth0
link-local      *               255.255.0.0     U         0 0          0 eth0
default         192.168.0.1     0.0.0.0         UG        0 0          0 eth0
```

Figure A.152: List the Kernel IP Routing Table

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The command shown below displays network interface packet transactions.

```
# netstat -i

Kernel Interface table
Iface       MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0       1500   0     4459      0      0      0     4057      0      0      0 BMRU
lo        16436   0        8      0      0      0        8      0      0      0 LRU
```

Figure A.153: Display Network Interface Packet Transactions

- The command shown below displays the kernel interface table.

```
# netstat -ie

Kernel Interface table
eth0      Link encap:Ethernet  HWaddr 00:0C:29:B4:DA:21
          inet addr:192.168.0.2  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feb4:da21/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4486 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4077 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2720253 (2.5 MiB)  TX bytes:1161745 (1.1 MiB)
          Interrupt:18 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:480 (480.0 b)  TX bytes:480 (480.0 b)
```

Figure A.154: Display Kernel Interface Table

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The command shown below prints netstat information continuously.

```
# netstat -c

Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 tecmint.com:http   sg2nlhg007.shr.prod.s:36944 TIME_WAIT
tcp        0      0 tecmint.com:http   sg2nlhg010.shr.prod.s:42110 TIME_WAIT
tcp        0    132 tecmint.com:ssh    115.113.134.3.static-:64662 ESTABLISHED
tcp        0      0 tecmint.com:http   crawl-66-249-71-240.g:41166 TIME_WAIT
tcp        0      0 localhost.localdomain:54823 localhost.localdomain:smtp  TIME_WAIT
tcp        0      0 localhost.localdomain:54822 localhost.localdomain:smtp  TIME_WAIT
tcp        0      0 tecmint.com:http   sg2nlhg010.shr.prod.s:42091 TIME_WAIT
tcp        0      0 tecmint.com:http   sg2nlhg007.shr.prod.s:36998 TIME_WAIT
```

Figure A.155: Output of “netstat” Command

- The command shown below lists listening programs.

```
# netstat -ap | grep http

tcp        0      0 *:http                  *:*                     LISTEN      9056/httpd
tcp        0      0 *:https                 *:*                     LISTEN      9056/httpd
tcp        0      0 tecmint.com:http   sg2nlhg008.shr.prod.s:35248 TIME_WAIT   -
tcp        0      0 tecmint.com:http   sg2nlhg007.shr.prod.s:57783 TIME_WAIT   -
tcp        0      0 tecmint.com:http   sg2nlhg007.shr.prod.s:57769 TIME_WAIT   -
tcp        0      0 tecmint.com:http   sg2nlhg008.shr.prod.s:35270 TIME_WAIT   -
tcp        0      0 tecmint.com:http   sg2nlhg009.shr.prod.s:41637 TIME_WAIT   -
tcp        0      0 tecmint.com:http   sg2nlhg009.shr.prod.s:41614 TIME_WAIT   -
unix  2      [ ]         STREAM     CONNECTED     88586726 10394/httpd
```

Figure A.156: List Listening Programs

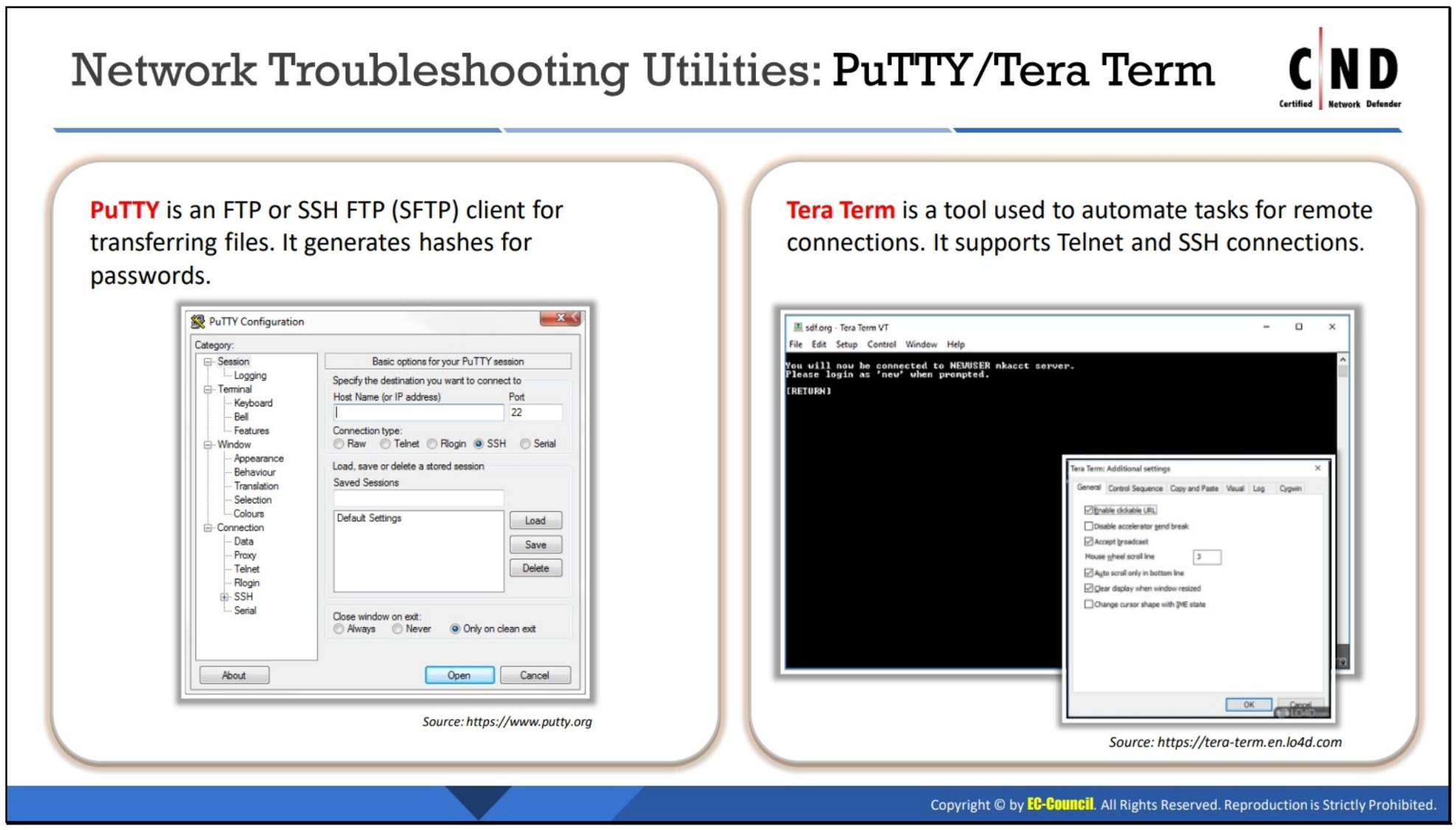
- The command shown below displays raw network statistics.

```
# netstat --statistics --raw

Ip:
    62175683 total packets received
    52970 with invalid addresses
    0 forwarded
Icmp:
    875519 ICMP messages received
        destination unreachable: 901671
        echo request: 8
        echo replies: 16253
IcmpMsg:
        InType0: 83
IpExt:
    InMcastPkts: 117
```

Figure A.157: List Raw Network Statistics

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Troubleshooting Utilities: PuTTY/Tera Term

The open-source graphical user interface (GUI) client PuTTY is a terminal emulator application that supports protocols such as SSH, Telnet, Rlogin, and serial for Windows and Unix-like OSes. It helps access and manage remote Linux servers.

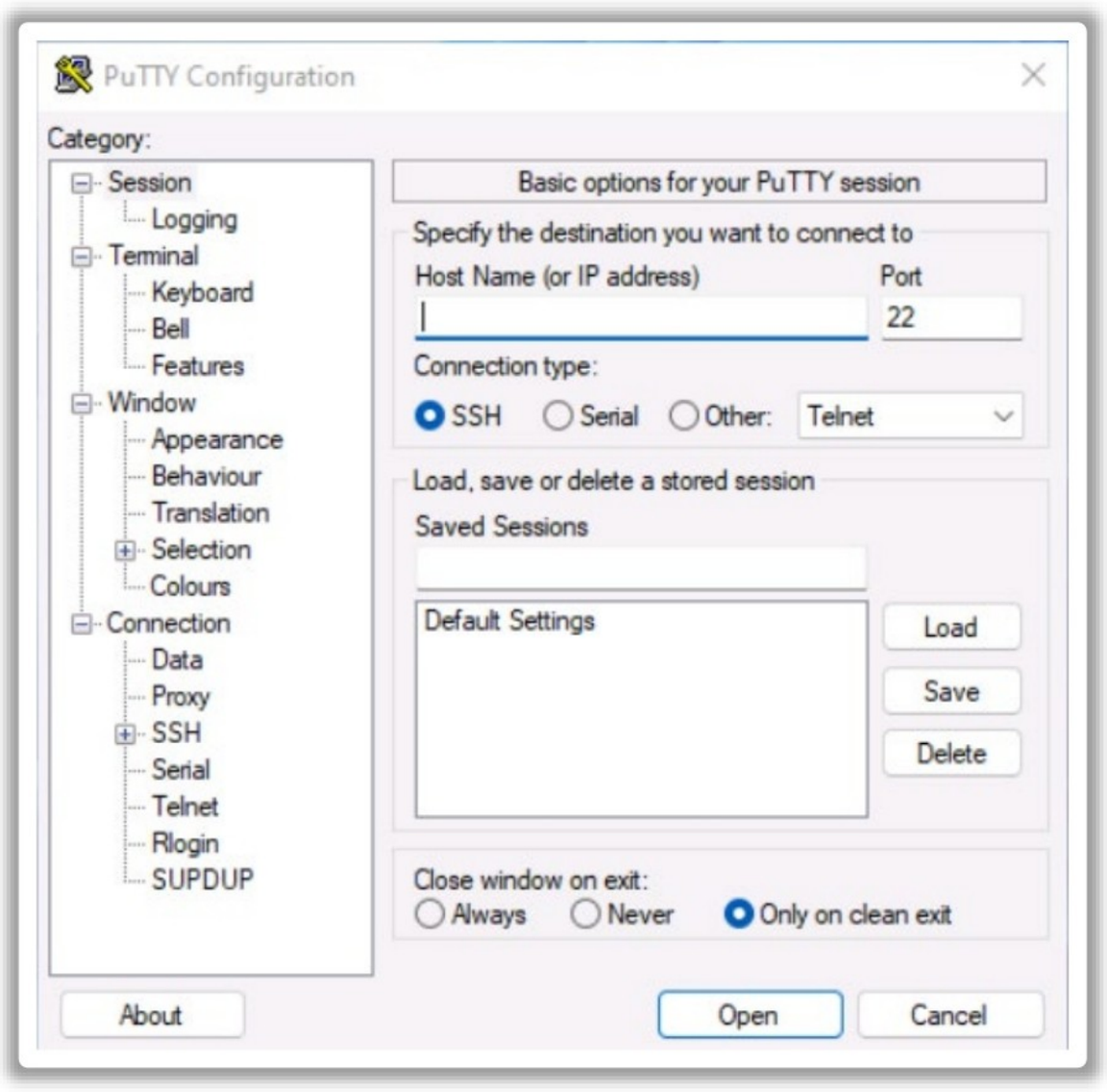


Figure A.158: Putty Configuration

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Features of PuTTY

- Control over the SSH encryption key and protocol version
- Command-line Secure Copy Protocol (SCP) and SSH File Transfer Protocol (SFTP) clients called “pscp” and “psftp,” respectively
- Control over port forwarding with SSH (local, remote, or dynamic port forwarding), including built-in handling of X11 forwarding
- Emulates most xterm, VT102 control sequences, as well as much of ECMA-48 terminal emulation
- IPv6 support
- Supports the Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES), Arcfour, Blowfish, and DES
- Public-key authentication support
- Support for local serial port connections

Steps to Use PuTTY to Access Remote Linux Servers

- Launch PuTTY and select the **Session** tab from the left pane.
- Enter the **Host Name (or IP address)** of the remote system to be connected and select **Connection type.** The selected connection type fills the default **Port** number automatically. Here, selecting **SSH** fills **Port** number 22. Click **Open**.

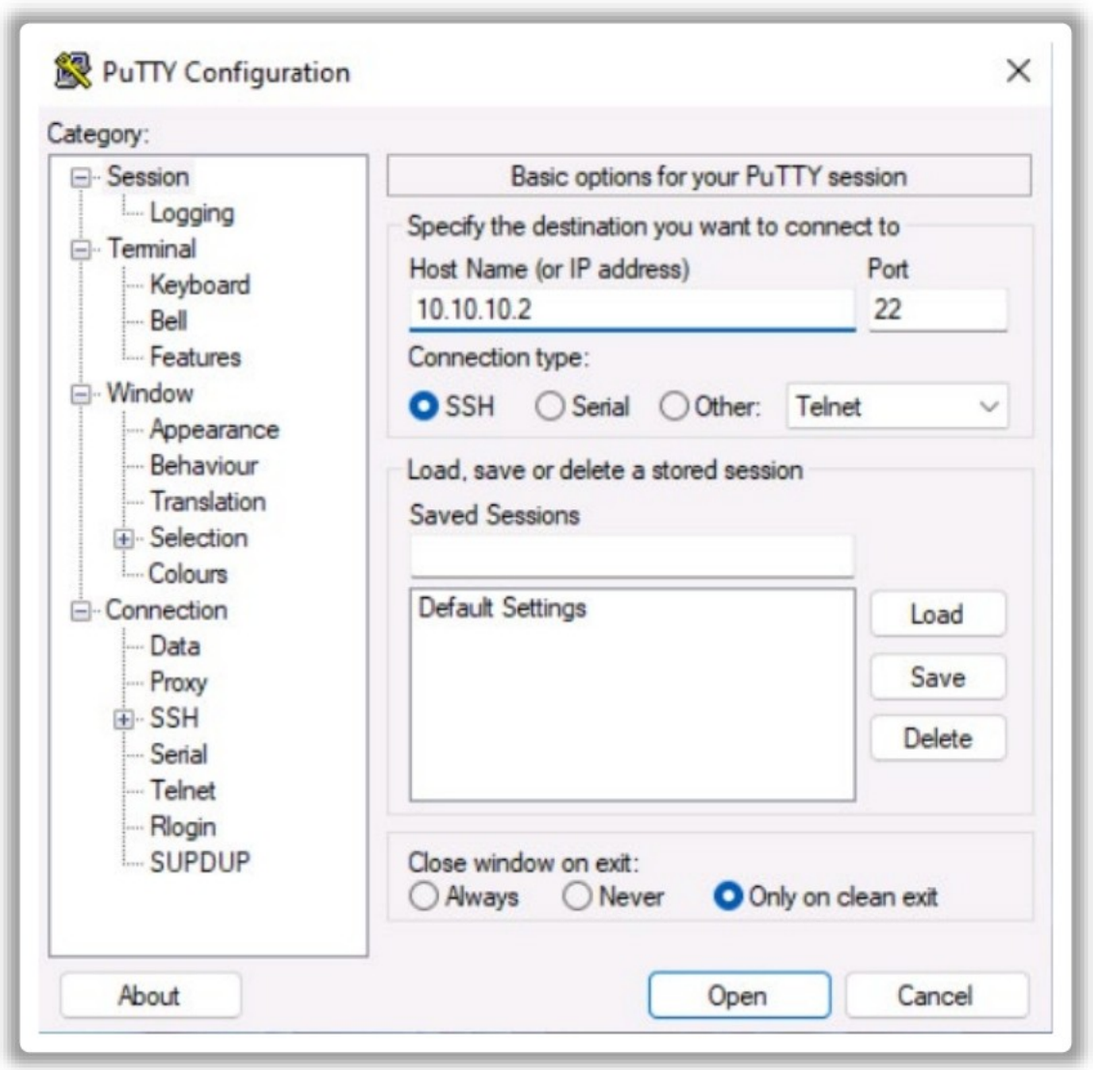


Figure A.159: Use Putty to Access Remote Linux Servers

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- If this is the first time the user is connecting to this remote system, PuTTY will display a security alert dialog box. Click **Accept** to add the remote system's host key to PuTTY's cache.

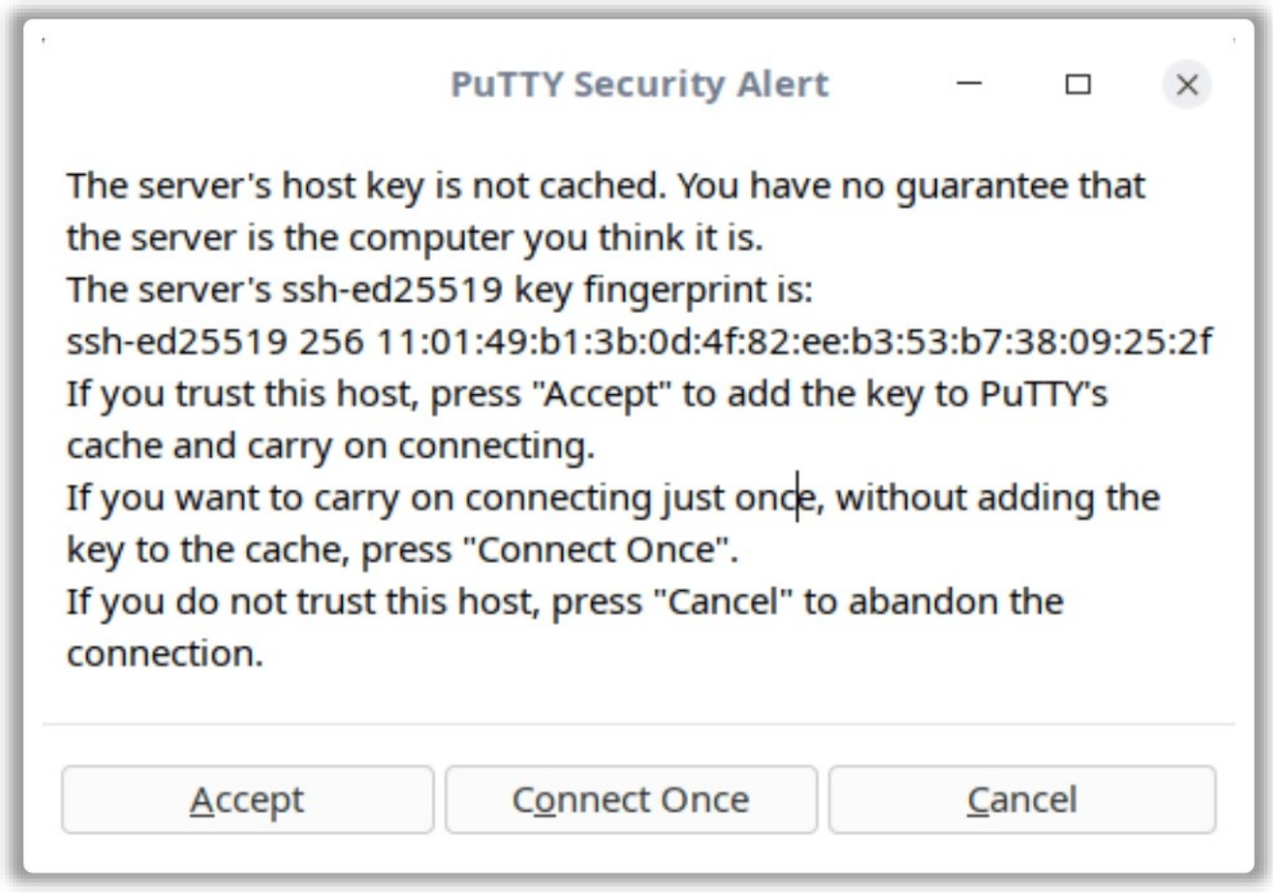


Figure A.160: Putty Security Alert

- Enter the remote system's username and password. A connection is established to the remote system via SSH using PuTTY.

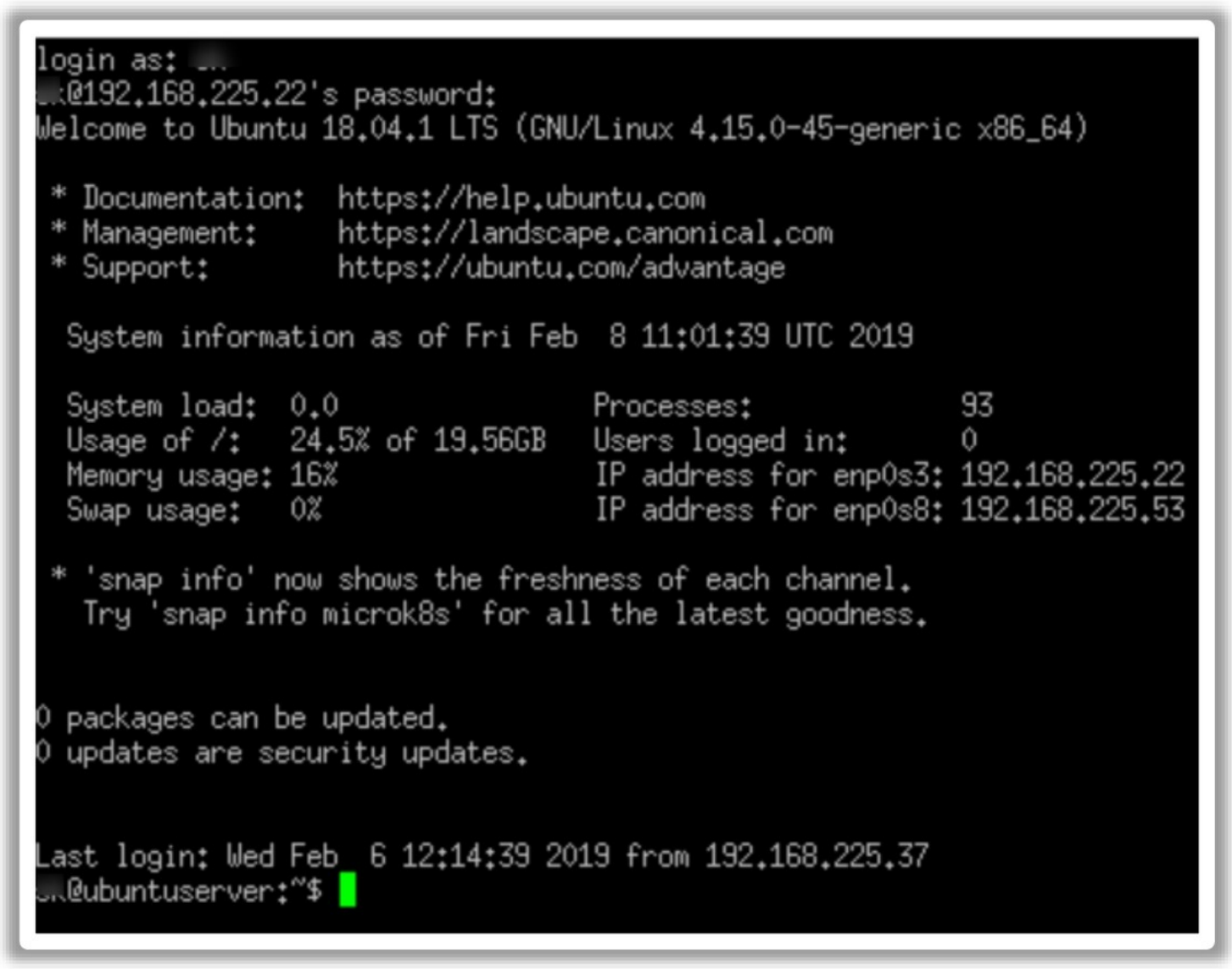


Figure A.161: Establish Remote System Connection

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Steps to Access Remote Systems Configured with Key-based Authentication

- Enter **Host Name** (**or IP address)** in the **Session** section.
- In the **Category** pane, expand **Connection**, expand **SSH**, expand **Auth**, and then choose **Credentials to authenticate with**.
- Browse the location of the **.ppk** key file and click **Open**.

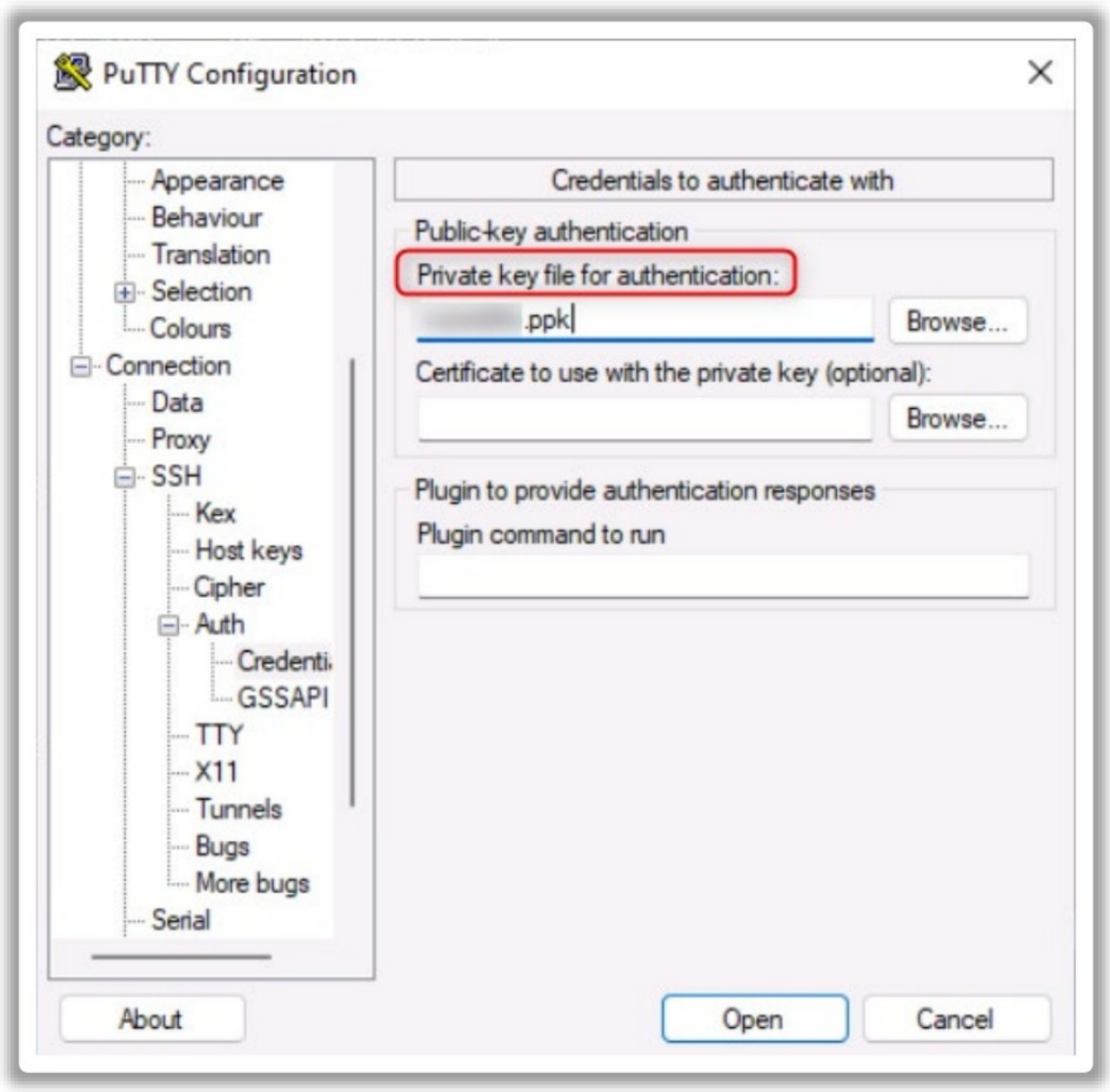
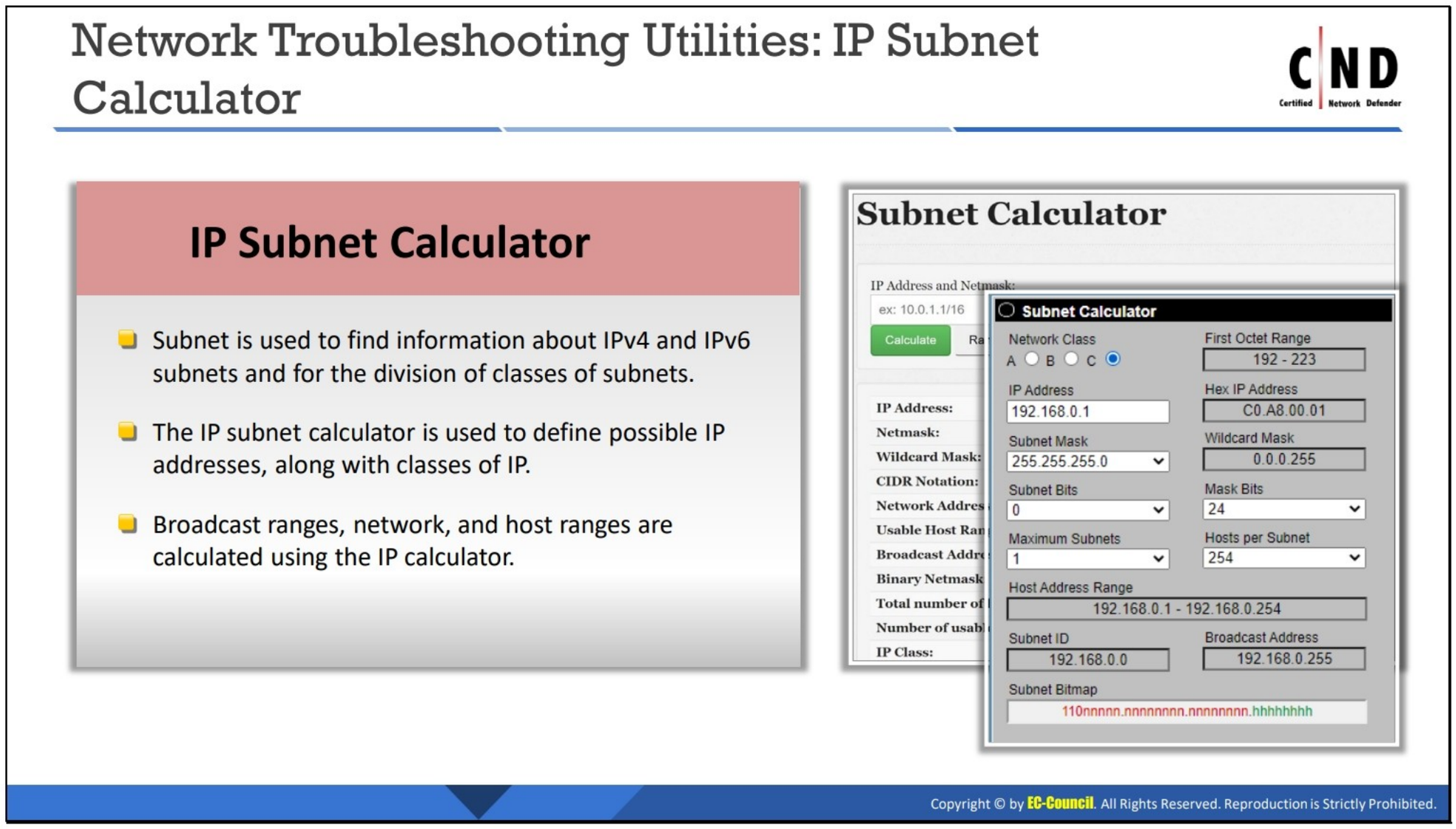


Figure A.162: Browse for the Key File

- Click **Accept** to add the host key if it is the first time the user is connecting to the remote system. Enter the remote system's passphrase to connect.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Troubleshooting Utilities: IP Subnet Calculator

A subnet is used to find information about IPv4 and IPv6 subnets as well as for the division of classes of subnets. For example, the SolarWinds Advanced Subnet Calculator helps ensure that IP addresses are not in conflict with one another and saves time in managing DHCP, DNS, and IP addresses. It allows the calculation of subnet masks and IP address management with the following:

- Breaking down the IP address
- Performing forward and reverse DNS resolution
- Offering classful subnet calculations and CIDR subnet calculations
- Providing a complete report of subnet addresses based on calculations

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

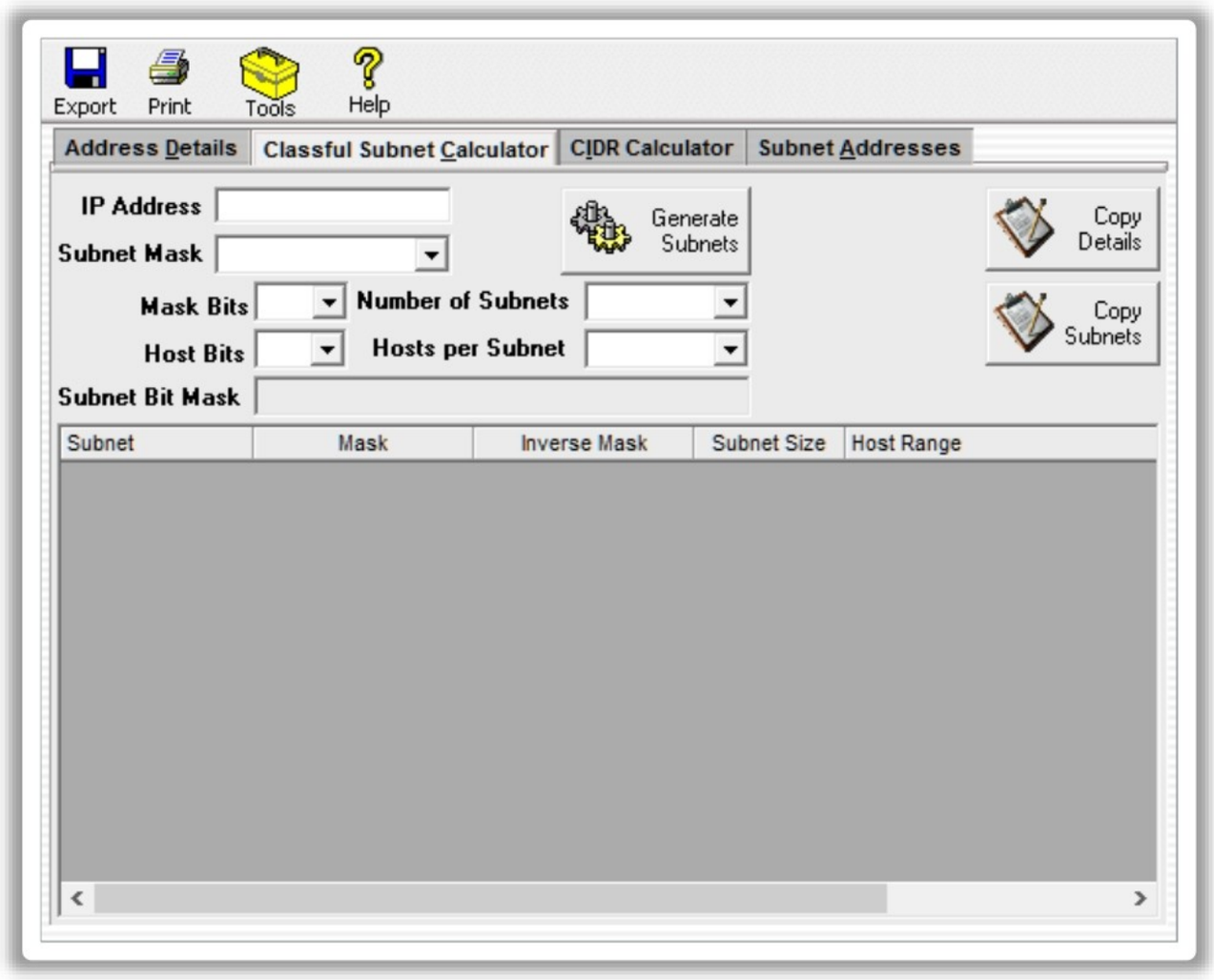


Figure A.163: Solarwind's Advanced Subnet Calculator

Tunnels Up Subnet Calculator

The web-based Tunnels Up Subnet Calculator is an IPv4 and IPv6 calculator that allows for the input of a netmask, a Cisco wildcard mask/CIDR notation. It allows performing reverse subnetting if the number of hosts is known and the netmask is unknown.

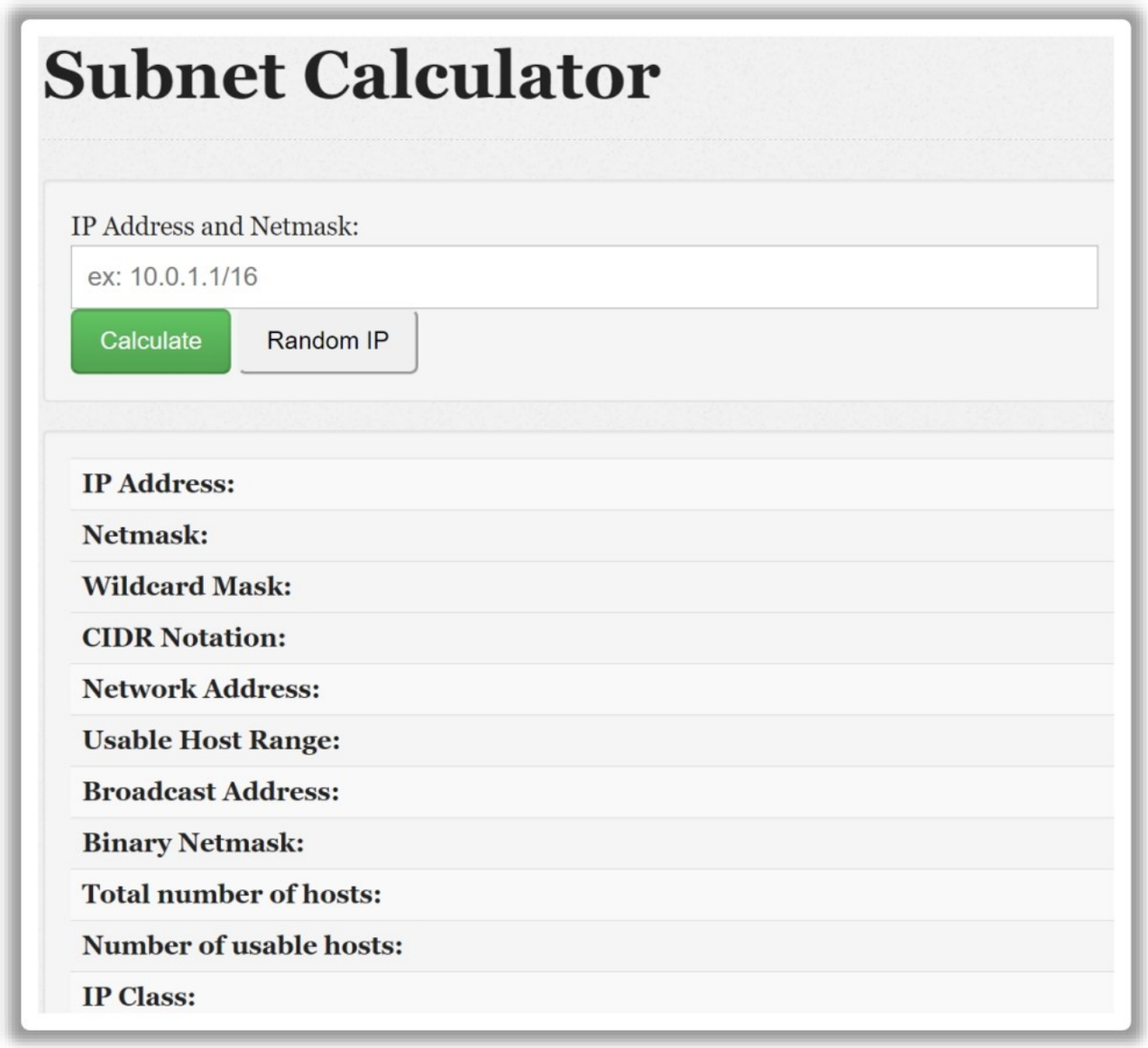
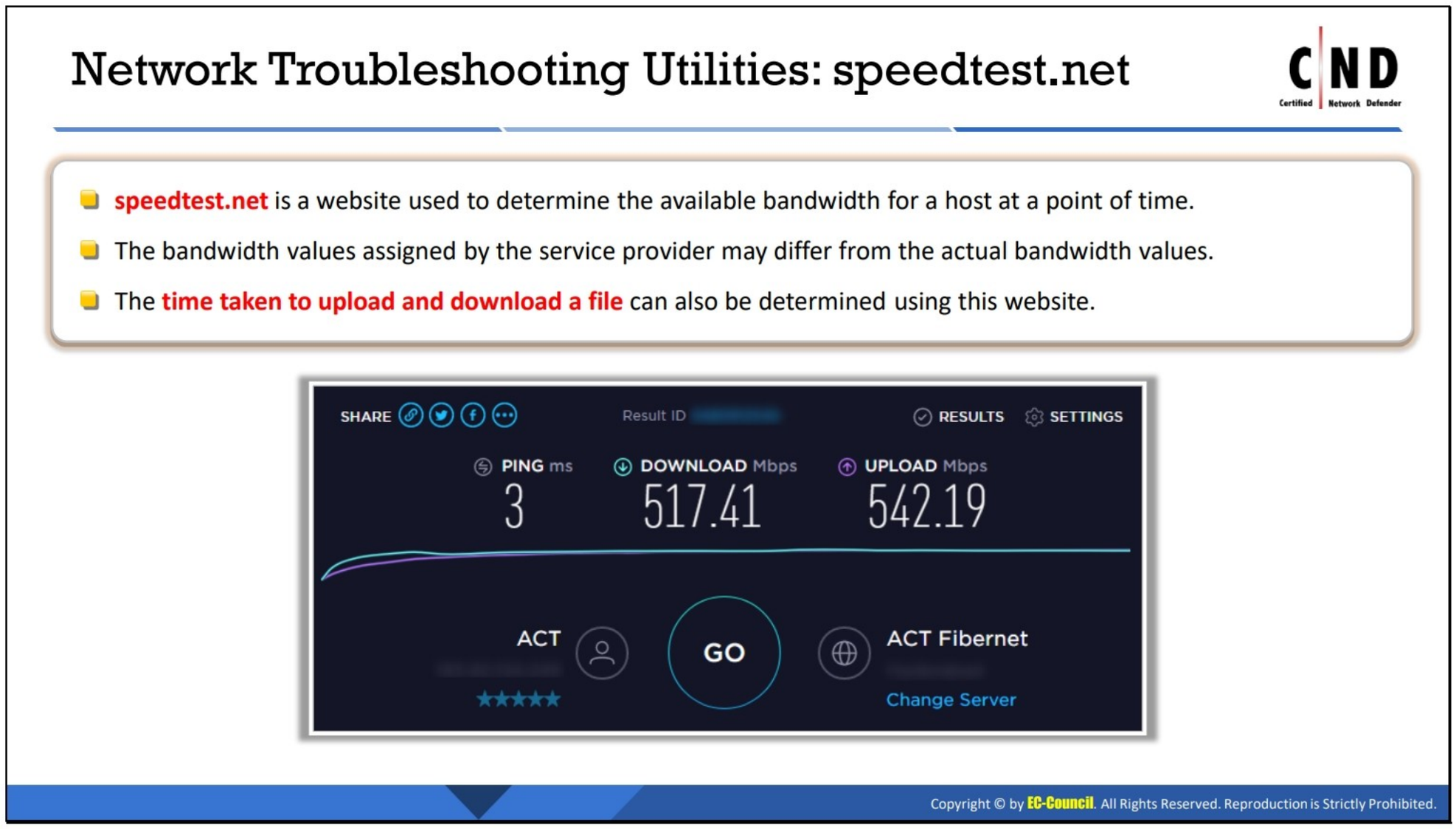


Figure A.164: Subnet Calculator

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Troubleshooting Utilities: speedtest.net

The website speedtest.net is used to determine the available bandwidth for a host at a point of time. It provides free analysis of Internet access performance metrics. For example, it provides metrics such as the connection data rate (speed) and latency (connection delay). For enhanced test accuracy, it uses TCP sockets and a custom protocol for communication between servers and users.

The time taken to upload and download a file can also be determined using this website. All the tests performed by speedtest.net measure the data rate in the download direction (from the server to the user) and that in the upload direction (the user to the server).

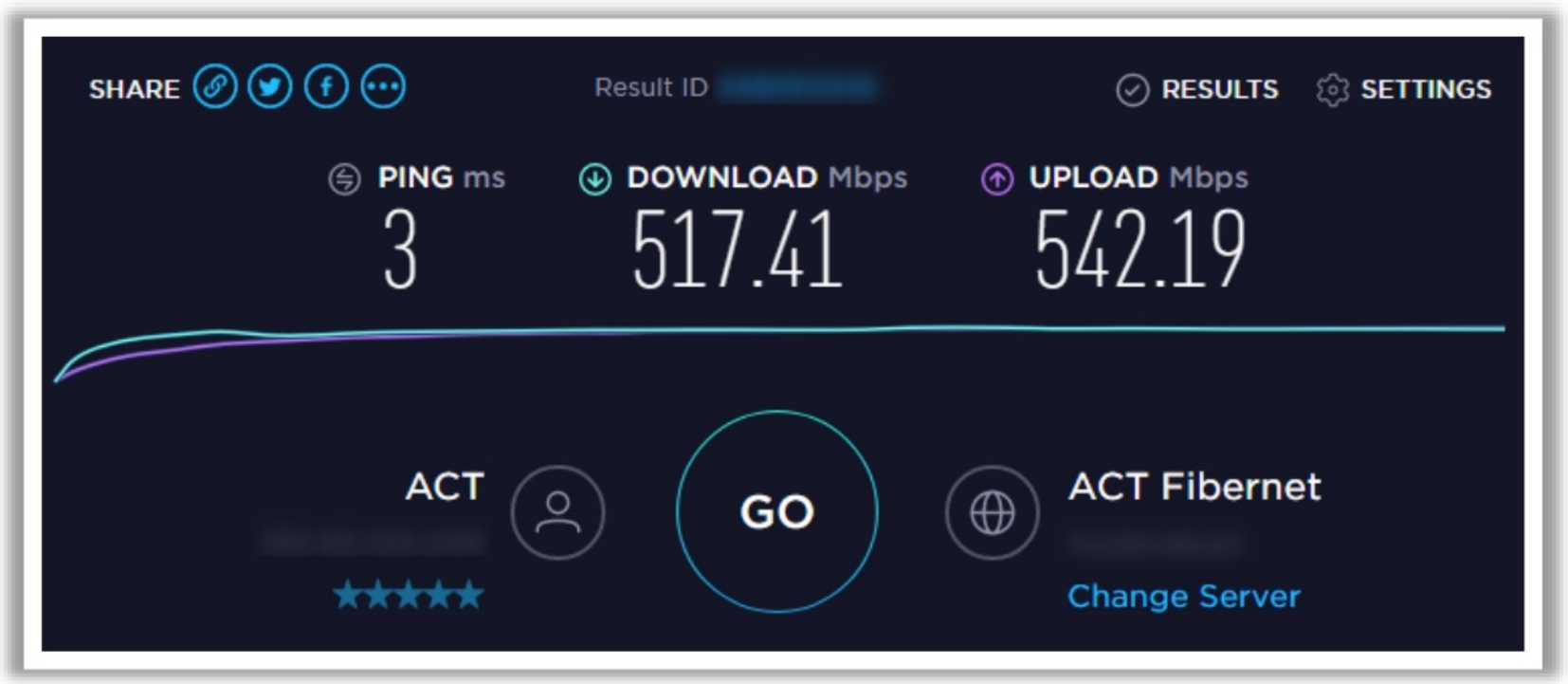
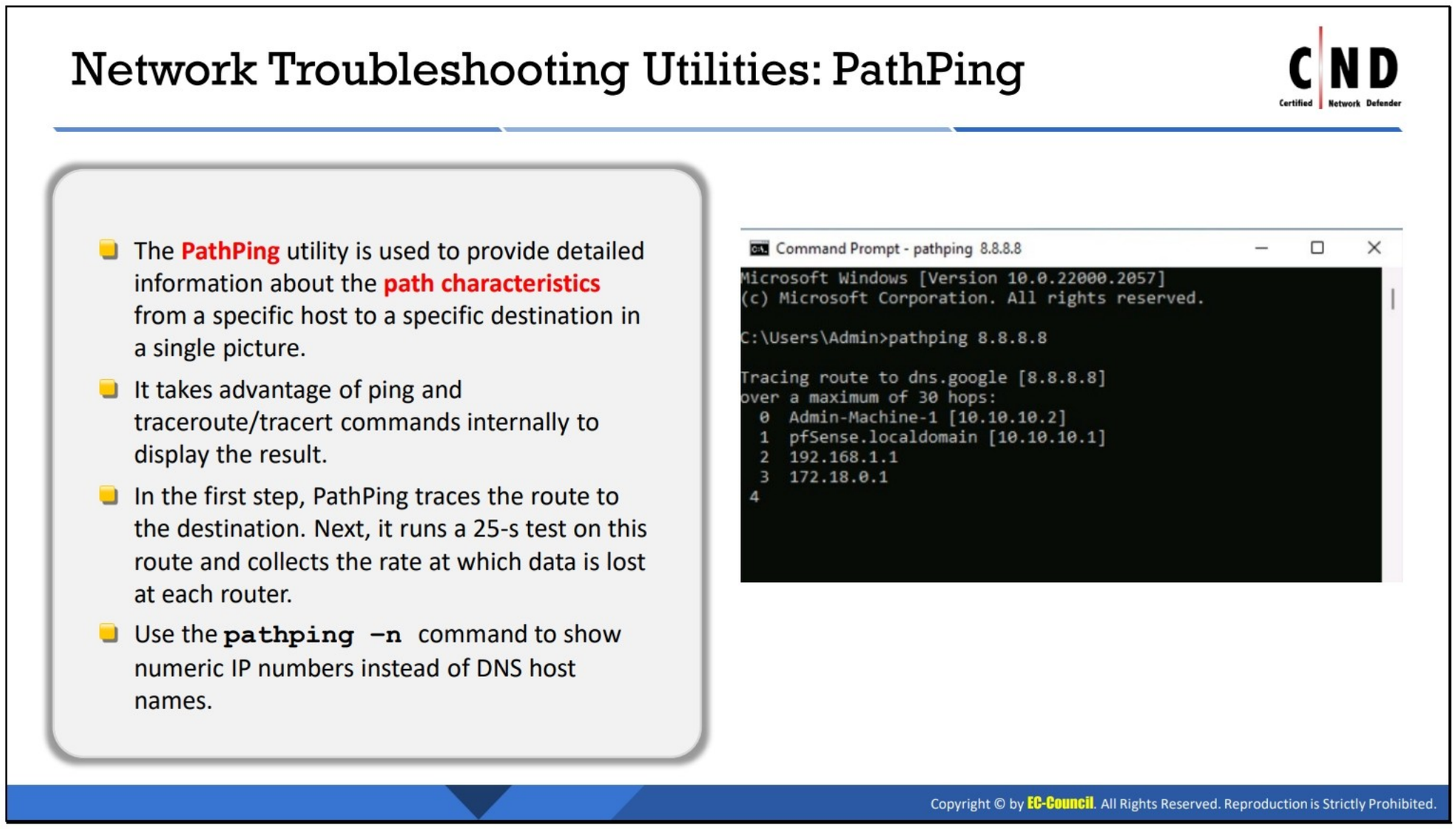


Figure A.165: Working of “Speedtest.net”

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Networking Troubleshooting Utilities: PathPing

The PathPing utility provides detailed information about the path characteristics from a specific host to a specific destination in a single picture by taking advantage of the ping and tracert/traceroute commands. It helps diagnose packet loss and slow speed faults. Initially, running PathPing traces the route to a destination address and launches a 25-s test for each hop to show the PathPing statistics on the data loss to each hop.

Steps to Use PathPing for Networking Troubleshooting

- Run the command **`pathping <IP address>`** in command prompt. Interrupt PathPing at any time by holding down the ctrl + C.

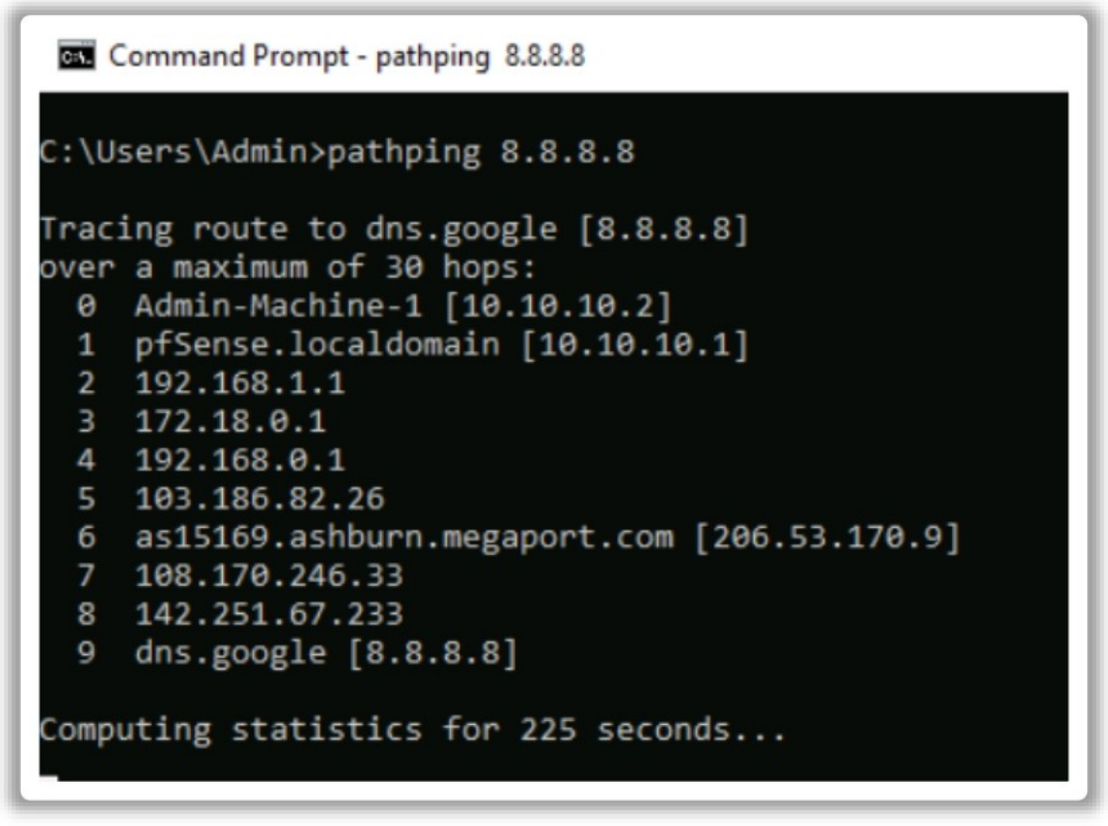


Figure A.166: Run the Command “pathping”

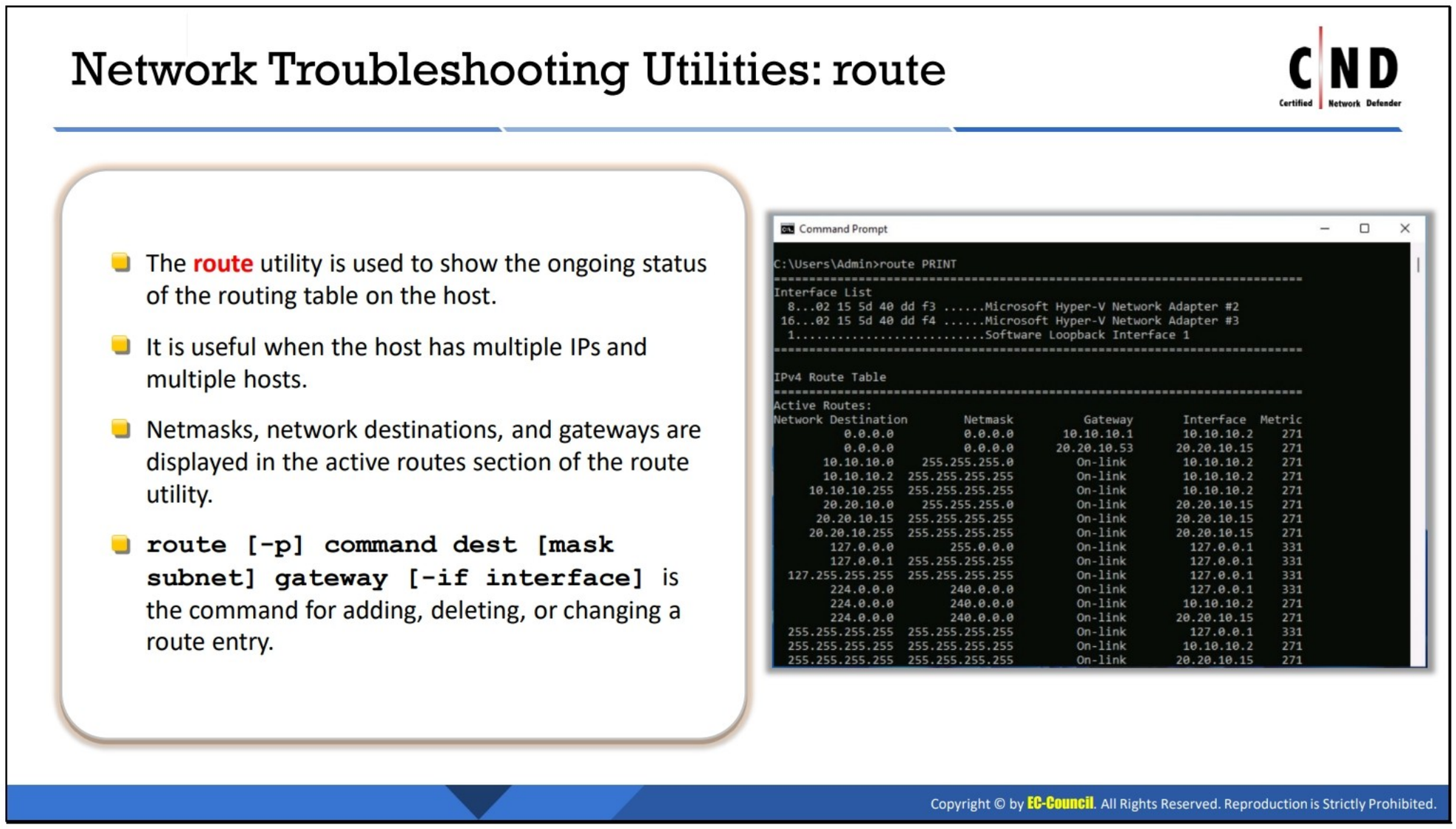
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use the command **`pathping -n`** to show numeric IP numbers instead of DNS host names.

```
C:>pathping -n www.[redacted].com
Tracing route to [redacted].com [209.68.34.15]
over a maximum of 30 hops:
  0  192.168.168.21
  1  66.193.195.81
  2  66.193.200.5
  3  168.215.55.173
  4  168.215.55.101
  5  168.215.55.77
  6  66.192.250.38
  7  66.192.252.22
  8  208.51.224.141
  9  206.132.111.118
 10  206.132.111.162
 11  64.214.174.178
 12  192.168.1.191
 13  209.68.34.15
Computing statistics for 325 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           192.168.168.21
                                 0/ 100 =  0%   |
  1   1ms    0/ 100 =  0%     0/ 100 =  0%  66.193.195.81]
                                 0/ 100 =  0%   |
  2   14ms   0/ 100 =  0%     0/ 100 =  0%  66.193.200.5
                                 0/ 100 =  0%   |
  3   10ms   0/ 100 =  0%     0/ 100 =  0%  168.215.55.173
                                 0/ 100 =  0%   |
  4   10ms   0/ 100 =  0%     0/ 100 =  0%  168.215.55.101
                                 0/ 100 =  0%   |
  5   12ms   0/ 100 =  0%     0/ 100 =  0%  168.215.55.77
                                 0/ 100 =  0%   |
  6   14ms   0/ 100 =  0%     0/ 100 =  0%  66.192.250.38
                                 0/ 100 =  0%   |
  7   14ms   0/ 100 =  0%     0/ 100 =  0%  66.192.252.22
                                 0/ 100 =  0%   |
  8   14ms   0/ 100 =  0%     0/ 100 =  0%  208.51.224.141
                                 0/ 100 =  0%   |
  9   81ms   0/ 100 =  0%     0/ 100 =  0%  206.132.111.118
                                 0/ 100 =  0%   |
 10   81ms   0/ 100 =  0%     0/ 100 =  0%  206.132.111.162]
                                 0/ 100 =  0%   |
 11   84ms   0/ 100 =  0%     0/ 100 =  0%  64.214.174.178]
                                 0/ 100 =  0%   |
 12   --- 100/ 100 =100%   100/ 100 =100%  192.168.1.191
                                 0/ 100 =  0%   |
 13   85ms   0/ 100 =  0%     0/ 100 =  0%  209.68.34.15
Trace complete.
```

Figure A.167: Display IP Numbers instead of Domain Names

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Networking Troubleshooting Utilities: route

The route utility is used to show the ongoing status of and modifications to the routing table on the Windows host. It is useful when the host has multiple IPs and multiple hosts. Netmasks, network destinations, and gateways are displayed in the active routes section of the route utility. In Unix/Linux, the route command can be used without any command-line switches. The command shows similar outputs for both Windows and Unix/Linux.

Steps to Use the Print Command for Network Troubleshooting

- In Windows, use the command **print** to view the routing table (IPv4 and IPv6).

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
C:\>route print
===========================================================================
Interface List
 8 ...00 12 3f a7 17 ba ......  Intel(R) PRO/100 VE Network Connect
 1 ...........................  Software Loopback Interface 1
 9 ...02 00 54 55 4e 01 ......  Teredo Tunneling Pseudo-Interface
10 ...00 00 00 00 00 00 00 e0  isatap.{D0F85930-01E2-402F-B0FC-
31DFF887F06F}
===========================================================================
IPv4 Route Table
===========================================================================
Active Routes:
Network          Netmask        Gateway       Interface     Metric
Destination
0.0.0.0          0.0.0.0         192.168.1.1  192.168.1.110   276
127.0.0.0        255.0.0.0       On-link      127.0.0.1       306
127.0.0.1        255.255.255.255 On-link      127.0.0.1       306
127.255.255.255  255.255.255.255 On-link      127.0.0.1       306
192.168.1.0      255.255.255.0   On-link      192.168.1.110   276
192.168.1.110    255.255.255.255 On-link      192.168.1.110   276
192.168.1.255    255.255.255.255 On-link      192.168.1.110   276
224.0.0.0        240.0.0.0       On-link      127.0.0.1       306
224.0.0.0        240.0.0.0       On-link      192.168.1.110   276
255.255.255.255  255.255.255.255 On-link      127.0.0.1 306
255.255.255.255  255.255.255.255 On-link      192.168.1.110   276
===========================================================================
Persistent Routes:
Network Address     Netmask     Gateway Address   Metric
        0.0.0.0     0.0.0.0     192.168.1.1       Default
===========================================================================
IPv6 Route Table
===========================================================================
Active Routes:
If Metric Network Destination   Gateway
9       18 ::/0                 On-link
1       306 ::1/128             On-link
9       18 2001::/32            On-link
9       266 2001:0:4136:e38c:2c6c:670:3f57:fe91/128
                                On-link
8       276 fe80::/64           On-link
9       266 fe80::/64           On-link
10      281 fe80::5efe:192.168.1.110/128
                                On-link
8       276 fe80::cca:9067:9427:a911/128
                                On-link
9       266 fe80::2c6c:670:3f57:fe91/128
                                On-link
1       306 ff00::/8            On-link
9       266 ff00::/8            On-link
8       276 ff00::/8            On-link
===========================================================================
Persistent Routes:
  None
C:\>
```

Figure A.168: View Routing Table

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

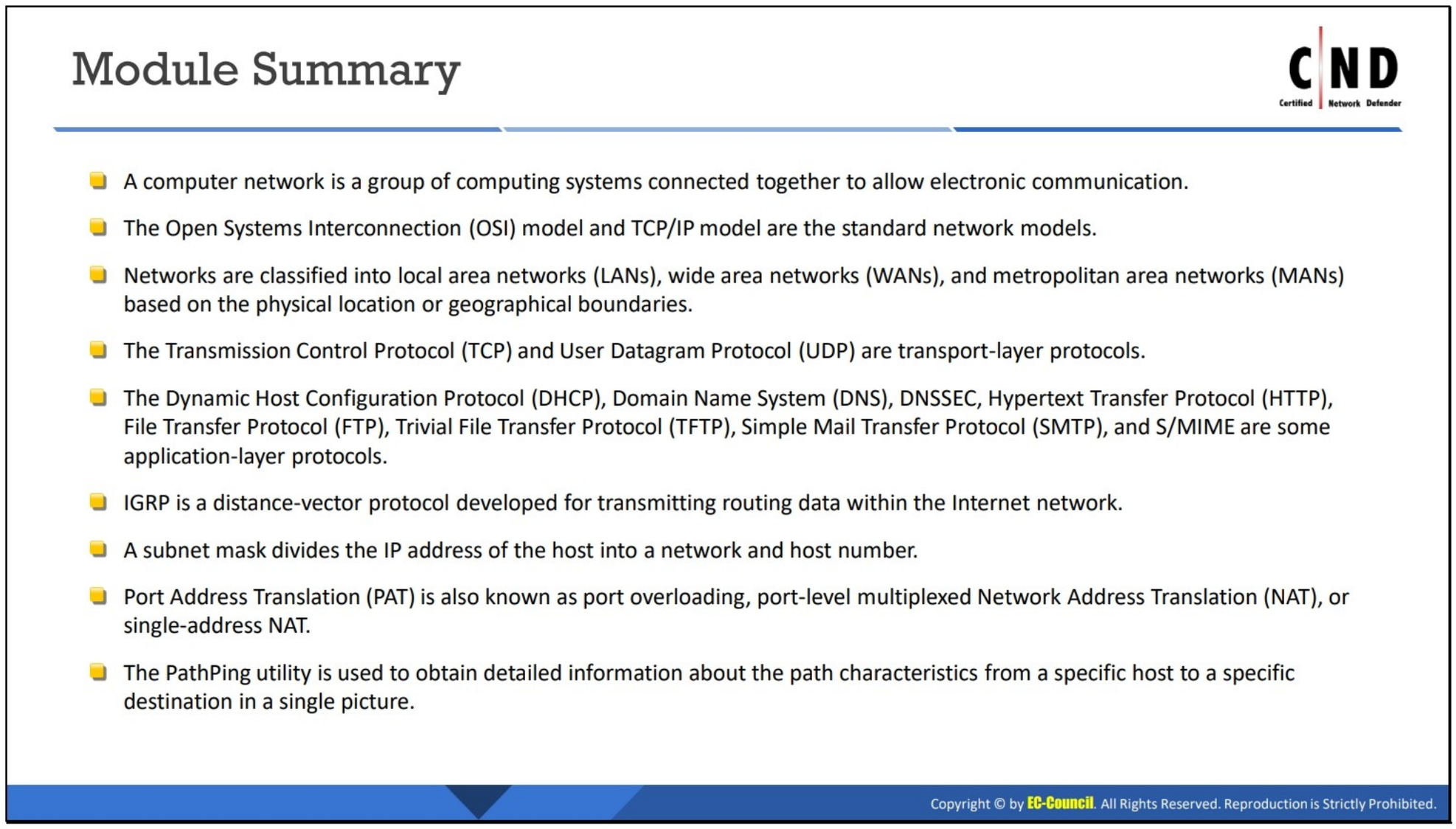
- To add, delete, or change a route entry, use the following command:

```
route [-p] command dest [mask subnet] gateway [-if interface]
```

Example:

```
C:\>route -p add 192.168.5.0 mask 255.255.255.0 192.168.1.500
C:\>route change 192.168.5.0 mask 255.255.255.0 192.168.1.542
                    C:\>route delete 192.168.5.0
```


Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

The following are the key points discussed in this module:

- A computer network is a group of computing systems connected together to allow electronic communication.
- The Open Systems Interconnection (OSI) model and TCP/IP model are the standard network models.
- Networks are classified into local area networks (LANs), wide area networks (WANs), and metropolitan area networks (MANs) based on the physical location or geographical boundaries.
- The Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are transport-layer protocols.
- The Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), DNSSEC, Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Simple Mail Transfer Protocol (SMTP), and S/MIME are some application-layer protocols.
- A subnet mask divides the IP address of the host into a network and host number.
- Port Address Translation (PAT) is also known as port overloading, port-level multiplexed Network Address Translation (NAT), or single-address NAT.
- The PathPing utility is used to obtain detailed information about the path characteristics from a specific host to a specific destination in a single picture.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council

Building A Culture Of Security



C|ND

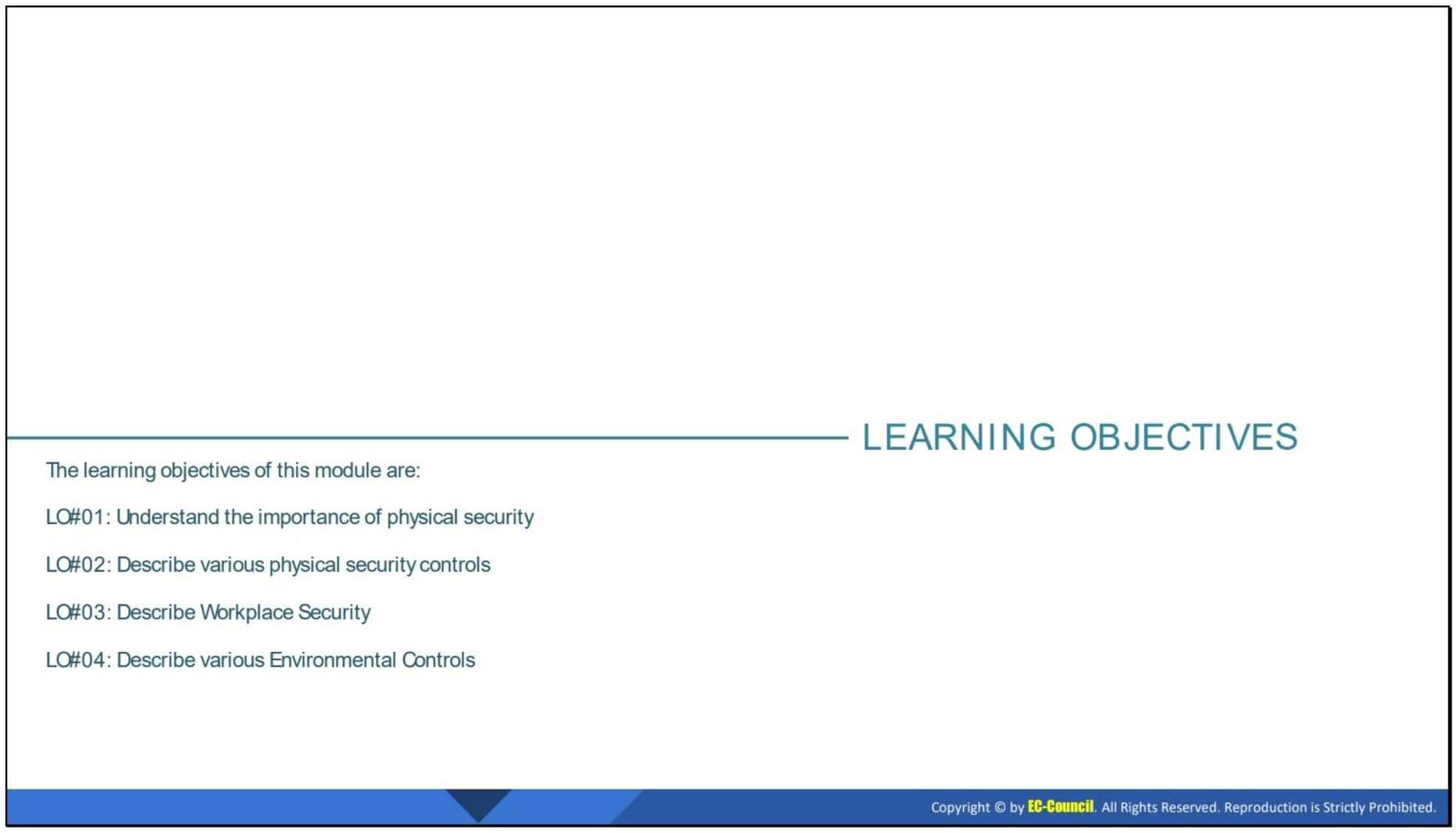
Certified Network Defender

Certified Network Defender v3

APPENDIX B
PHYSICAL NETWORK SECURITY

EC-Council Official Curricula

This page is intentionally left blank.

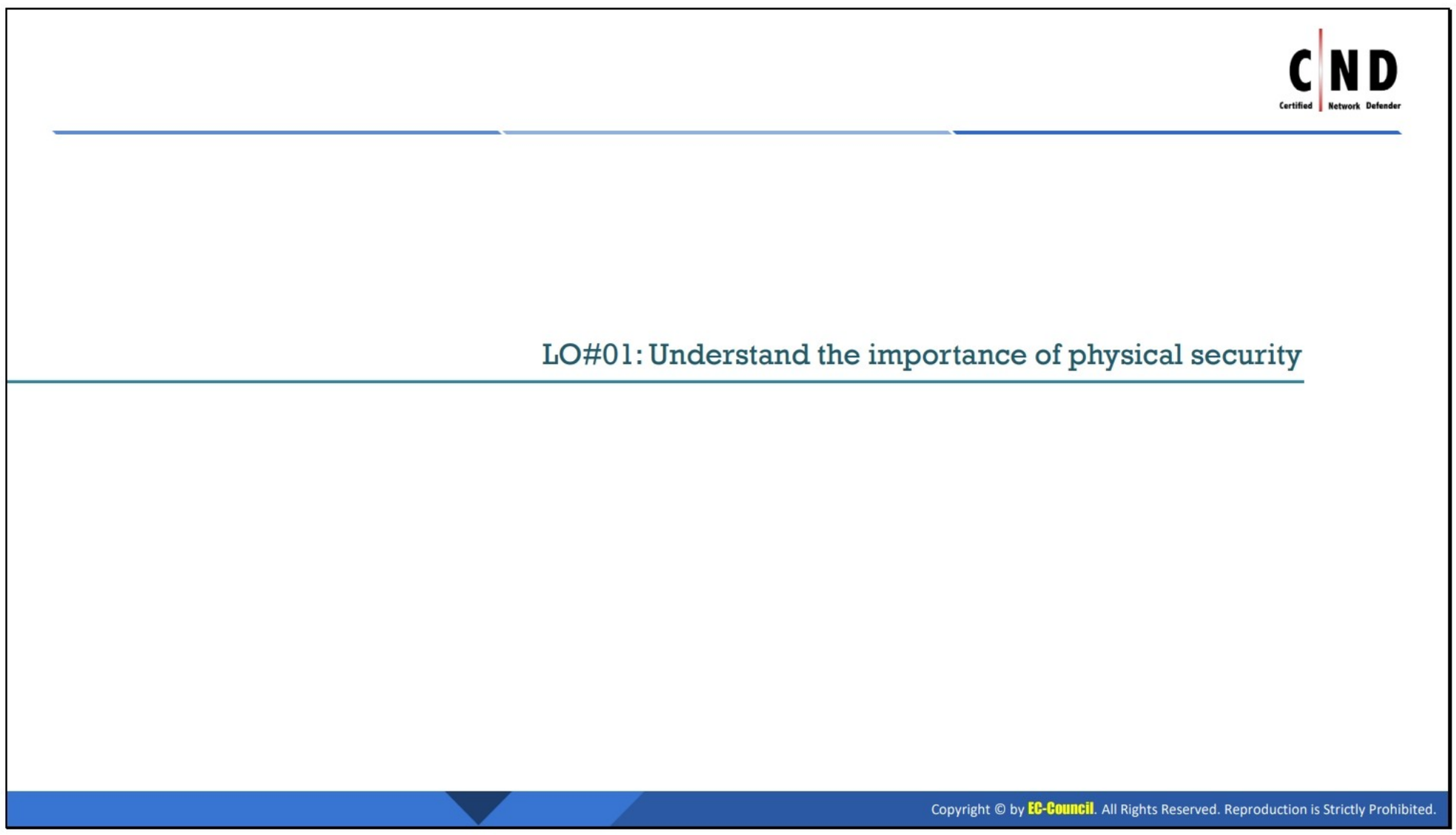


Learning Objectives

The learning objectives of this module are:

- Understand the Importance of Physical Security
- Describe Various Physical Security Controls
- Describe Workplace Security
- Describe Various Environmental Controls

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#01: Importance of Physical Security

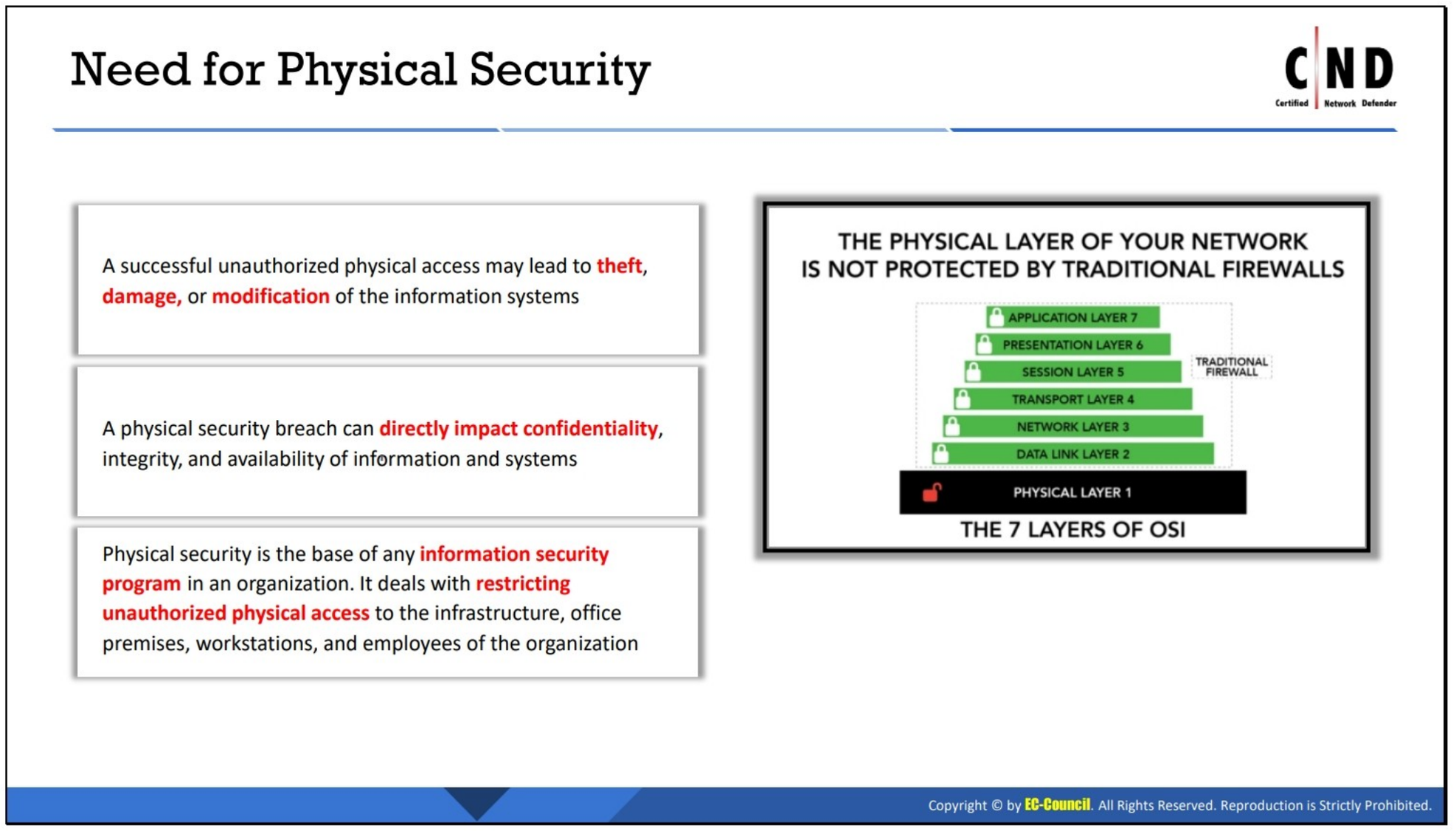
This section explains the importance of physical security in organizations.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

First Rule of Network Security: Physically Safeguard your Systems and Networks.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Need for Physical Security

Although cyber-attacks are becoming more complex, attackers are continuing to use various techniques to compromise the physical security of an organization. Organizations are focusing more on strengthening their IT security which overshadows the importance of physical security. Physical security is the most-overlooked aspect of security and it has been brought to the forefront of many organizations over the last five years. Knowing this fact, attackers are taking advantage of loopholes to compromise the physical security of the organization. According to data collected by the US Dept. of Health and Human Services Breach Portal, it has been found that physical security breaches are among the most occurring security incidents in organizations.

According to the findings of the fifth annual Horizon Business Continuity Institute (BCI) Scan Report, physical security is now perceived as a growing concern for business continuity professionals. According to this report, a degree of concern has been expressed concerning the possibility of both an act of terrorism and a security incident such as vandalism, theft or fraud disrupting their organization at some point.

Physical security breaches are totally different than other security breaches. They can be carried out with little to no technical knowledge. The real physical security concerns arise when traditional security measures such as a firewall, IDS, etc., does not ensure physical security. Deploying a firewall at various levels ensures security from different types of attacks but it does not hold true with the physical security of the organization. The firewall has nothing to do with physical security as traditional firewalls work above the physical layer of the OSI model.

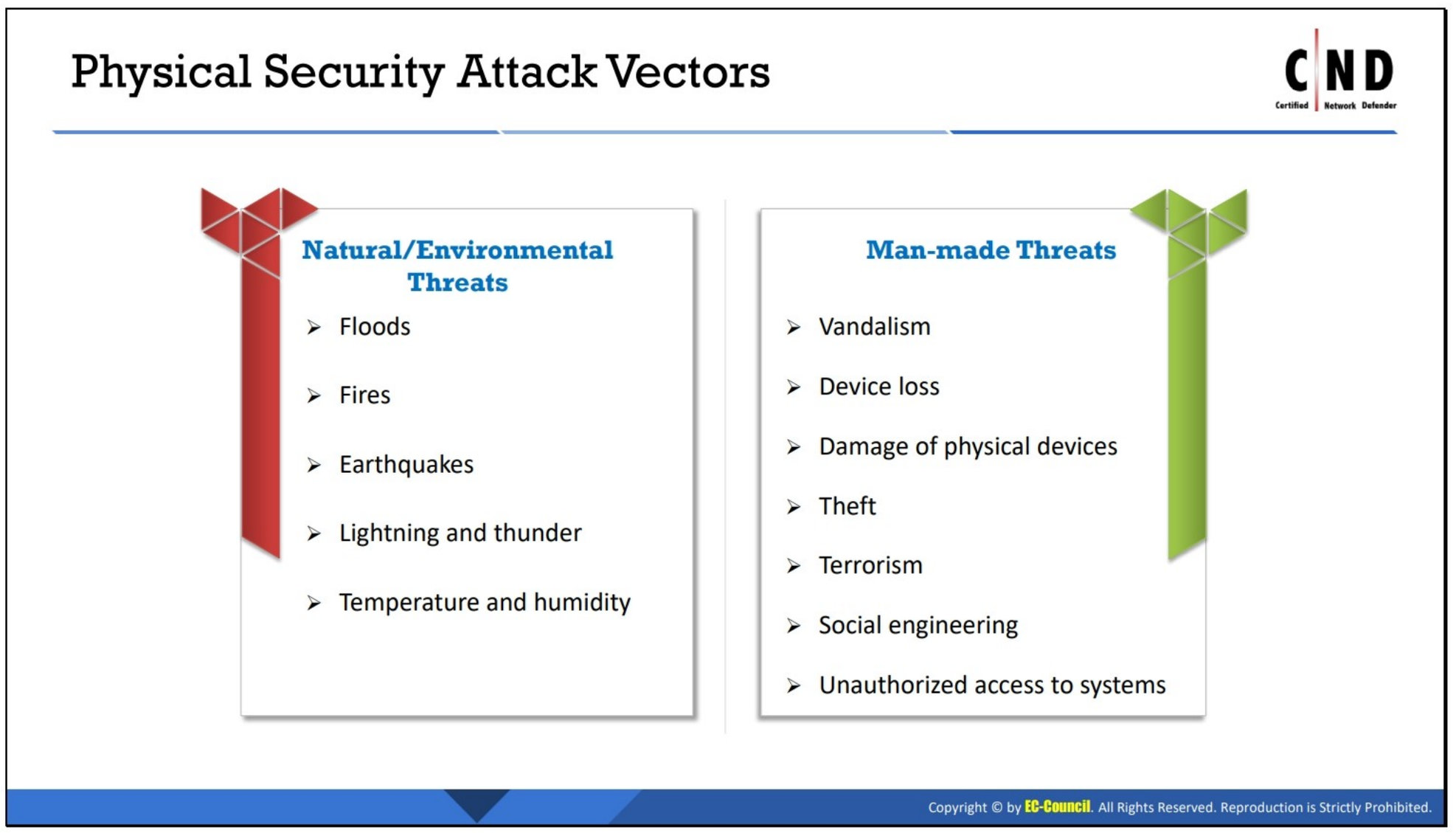
Physical security cannot be dealt with in the same way as network, application, or database security. Separate security measures are required to ensure physical security. Physical security should be dealt with at the physical layer of the OSI model.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

A physical layer includes

- All cabling and network systems.
- Physical access to cables and systems.
- Power support for cables and systems.
- Environment supporting the systems.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Physical Security Attack Vectors

Organizations are at risk with the following types of physical security threats:

Natural/Environmental Threats

- **Floods:** Floods commonly occur due to heavy rains or the melting of ice. Heavy rains increase the level of water beyond the carrying capacity of a river and this results in a flood. Floods may affect electrical systems and server rooms in an organization. Server rooms located in the basement have a greater chance of getting affected by floods.
- **Fires:** Fires mainly occur due to short circuits or poor building materials. These may affect the operational facility and computer rooms in an organization. Fires can completely damage the hardware, cabling system, and other important components.
- **Earthquakes:** An earthquake is the sudden release of stored energy in the Earth's crust that creates seismic waves. It disrupts the physical infrastructure in an organization. It damages computers and other hardware devices and documents in the sensitive areas inside an organization. It can affect the safety or security of the organization. Earthquakes mainly affect the cabling, the wiring system and the physical building itself. Any damage in the cabling system affects the working of the computer systems.
- **Lightning and Thunder**: Lighting and thunder occur due to environmental changes. It necessitates the shutdown of all outdoor activities. Lightning and thunder lead to power and voltage fluctuations that in turn affect the working of the system. It may affect memory chips and other hardware components of the system. It may lead to a short circuit in the cabling and other wiring systems, if they are not covered properly. The information system may stop working with one strike. Lightning may damage all electrical and electronic appliances and lead to the loss of all sensitive information.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

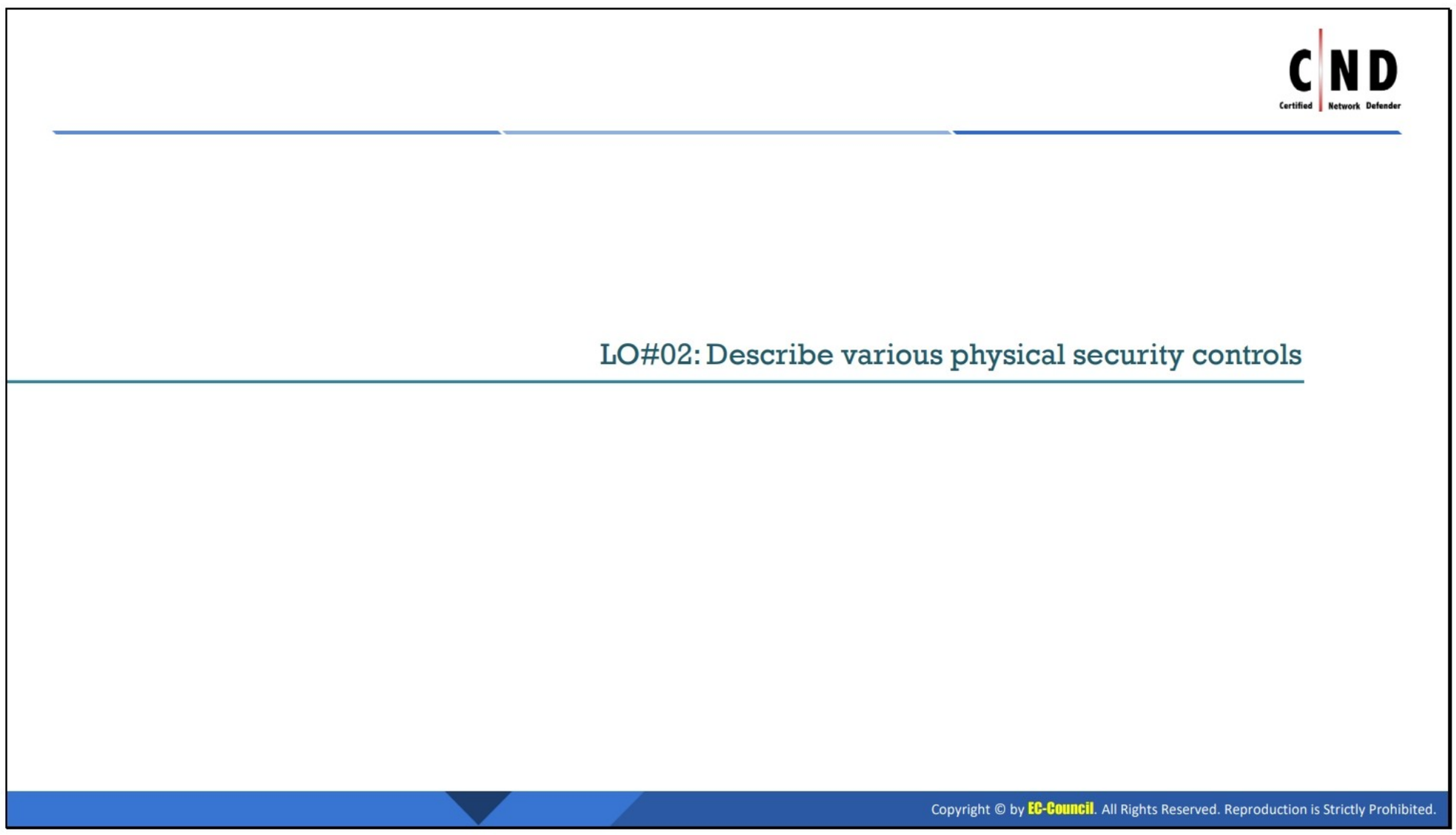
- **Temperature and Humidity**: Computer systems operate between a range of temperatures, otherwise they will function in an inappropriate manner. Computer systems do not like hot areas. Computer systems may get damaged if the temperature rises or lowers by extreme amounts. Even though every computer system has cooling systems, performance of a computer still depends on the exterior temperature conditions. Electrical and electronic appliances in an organization may be affected by the change in the humidity. High humidity leads to issues like Corrosion, short-circuits and damages the magnetic tapes, optical storage media. Low humidity affects the electronic devices mainly due to electric discharge.

Man-made Threats

The biggest threat to physical components and the network is from man-made errors, both intentional or unintentional errors. A wide range of possibilities include hackers/crackers, theft, fire, and human error. Some of the examples of human error that may lead to man-made threats are the unintentional pressing of a wrong button, unplugging the wrong device, etc. Typical man-made threats include mechanical, electrical disturbance, pollution, radio frequency interference, explosion, etc.

- **Vandalism**: Disgruntled employees or former employees may try to compromise the system by willingly breaking or harming the system components. During civil unrest or a disaster, there is a chance of the systems being mishandled.
- **Device Loss**: Unauthorized access may give way to the loss of important information and devices. Device theft is a concern if not properly secured.
- **Damage of Physical Devices:** Improper device maintenance activities such as how the device is handled or the information, not replacing damaged devices, poor cabling can damage the physical devices to great extent.
- **Theft:** Lack of proper security and locks may result in equipment theft.
- **Terrorism:** Terrorism activities such as planting a vehicle bomb, human bomb, postal bomb in and around the organization's premises, will impact physical security in many ways.
- **Social Engineering:** Social engineering is defined as an illegal act of getting personal information from other people. The attacker gains unauthorized physical access by performing social engineering on an organization's employees.
- **Unauthorized access to systems**: Both internal users and external users can try to gain unauthorized access to a system or information about the organization.

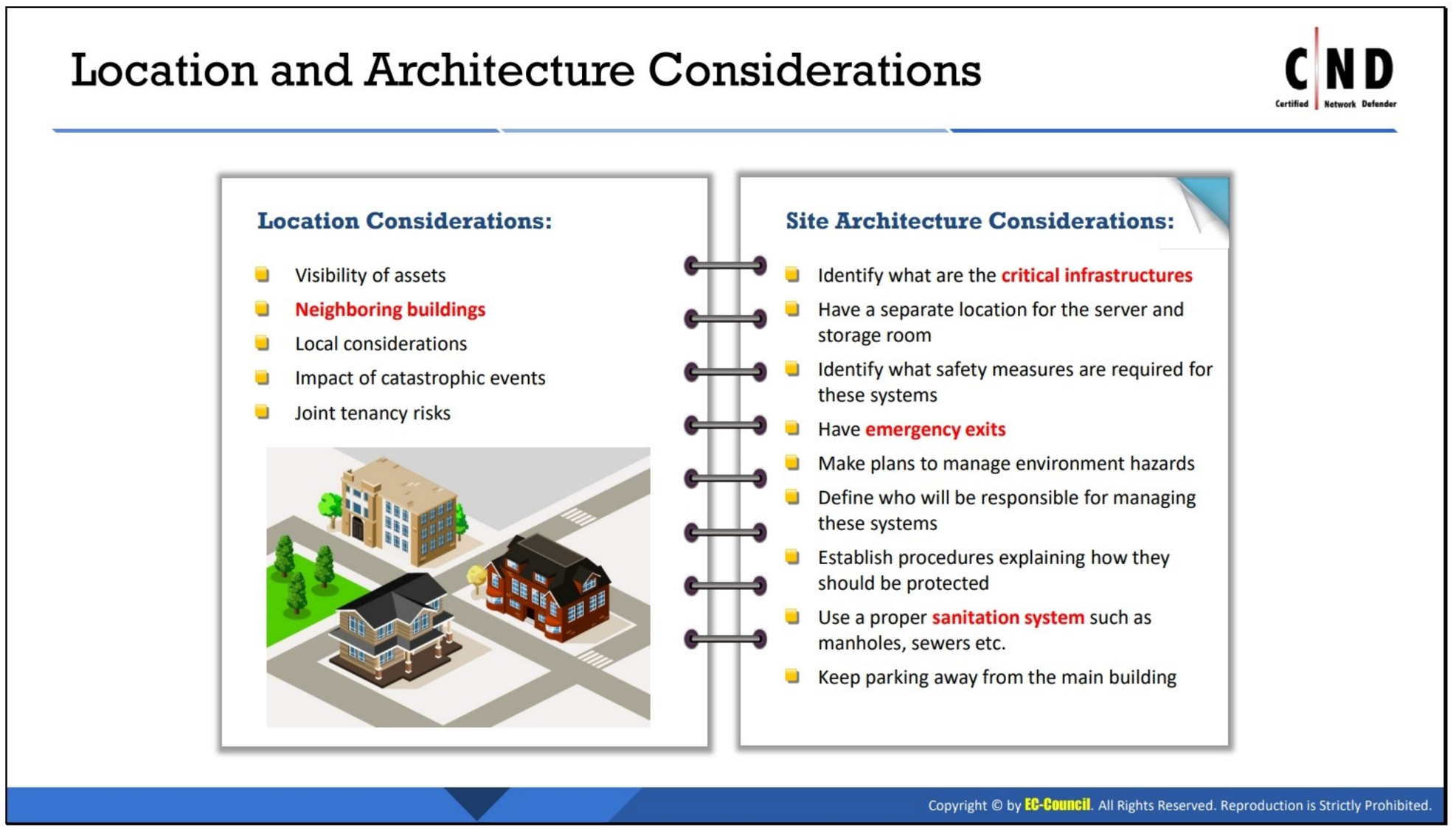
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#02: Physical Security Controls

This section explains various physical security controls that can be used in organizations.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Location and Architecture Considerations

Organizations should consider various factors that may affect physical security before planning to buy or lease a building for an organization. It may include the facility location, neighboring buildings, power and water supply, sewage systems, proximity to public and private roads, transportation, emergency support, fire station, hospital, airport, local crime or rate of riots and prior security incidents that happened in the surrounding area. The location should not be prone to natural disasters such as floods, tornadoes, earthquakes, hurricanes, excessive snow or rainfall, mudslides, fires etc.

Site Architecture Considerations

After gaining adequate information about the facility location details, planning and designing of the internal infrastructure and architecture should be done. While planning and designing the site architecture, an organization should prepare a list of all of its assets in the facility.

The organization should consider the following points while designing the infrastructure and architecture:

- Decide the number of entrances required for the building, including the main entrance, staircase, parking, lift, hallway, and reception area.
- Find the neighboring facilities around your site location and check the internal and external architecture for them. Talk to the supervisors or owners of the buildings to gain additional insights about the surroundings.
- Analyze the assets that can be impacted by catastrophic failures and visibility of assets from outsiders

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Think about the joint tenancy factor, if the facility is shared with other companies and their impact on your sensitive information and critical assets
- Identify the necessary critical infrastructure that is required for managing the physical security, storing sensitive data and running business operations effectively.

These critical infrastructure systems may not use standard information technology [IT]) for safety, performance, and reliability but they are critical to business operations. An improper or faulty implementation of certain physical measures such as electricity, backup, storage facilities, lighting, wiring and cooling systems can be critical to the business operations of the organization.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Fire Fighting Systems

Types of Fire Fighting Systems	
Active fire protection (manual or automatic)	**Passive fire protection (structural consideration)**
Fire detection Smoke, flame and heat detectors Fire suppression Fire extinguisher Standpipe system Sprinkler systems	Use of fire-resistant construction materials Compartmentalization of the overall building Emergency exits Minimizing inflammable sources Maintenance of fire fighting systems Emergency procedures Educating the occupants

Fire Class	Fire Source	Suppressant					
		Water	Foam	Dry Chemical	Wet Chemical	Clean Agents and CO_2	Special Chemicals
A	Ordinary solid combustibles	Y	Y	Y	Y		
B	Flammable liquids & gases		Y	Y		Y	
C	Electrical equipment			Y		Y	
D	Combustible metals		Y				Y
K	Oils and fats		Y		Y		

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Fire Fighting Systems

Fire is a risk that can occur with or without any warnings usually from man-made errors, short circuits, defective and faulty equipment. Fire protection is an important aspect of physical security. Firefighting systems mainly deal with detecting and alerting the occupants to the fire incidents. Fire incidents may be identified either manually or automatically.

Different types of firefighting systems include:

Active Fire Protection

Active fire protection provides an alert to the occupants of an organization regarding a fire incident. This type of fire protection system is generally used in commercial places, process industries and warehouses in order to protect the storage vessels, processing plant, etc. The main aim of implementing an active fire protection system includes controlling the spread of fire and extinguishing it as soon as possible, thereby facilitating the clearance of occupants in an organization. The system requires a certain amount of actions to handle the fire incidents. These actions may be performed either manually or automatically.

Certain active fire systems include water sprinklers, fire/smoke alarm systems, spray systems and fire extinguishers. Fire/Smoke alarms indicate the presence of any fire or smoke in the building. Water sprinklers reduce the spread of the fire and fire extinguishers help put the fire out. Water sprinklers fall under the category of automatic fire protection systems, whereas fire extinguishers and stand pipes fall under the category of manual fire protection systems.

Active fire protection systems include:

- **Fire Detection System:** Fire detection system helps detect a fire incident before letting the fire spread.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Automatic fire detection systems include:

- **Smoke Detectors:** Smoke detectors generally detect the presence of smoke and send an alert about the suspected fire incident in an organization. Upon detection of smoke, detectors send out an alarm to the fire alarm control panel or generate an audio/visual alarm.
- **Flame Detectors:** Flame detectors mainly deal with the detection of flames in a fire incident. Flame detectors normally include sensors which detect the existence of flames. The working of a flame detector includes:
  - Generate an alarm on fire flame detection.
  - Cutting the supply of gas through the fuel line.
  - Activate the fire suppression system.

  Flame detectors work more efficiently and faster than a smoke detector and a heat detector.
- **Heat Detectors:** Heat detectors are used to detect and respond to thermal energy generated due to fire incidents. Heat detectors are further classified into: fixed temperature heat detectors and rate-of-rise heat detectors.

- **Fire Suppression:** A fire suppression system is used to quench the fire without much human interaction. Fire suppression systems regulate the destruction and device loss. A fire suppression system can be classified as: manual and automatic. Commonly used fire suppression systems include:
  - **Fire Extinguisher:** Fire extinguishers deal with extinguishing fires at the initial stage. These may not be used in case of a fire covering a large area. A fire extinguisher normally consists of an agent that is discharged, inside a cylindrical vessel. Fire extinguisher systems need to be checked often in order to ensure they are working properly in case of fire. Fire extinguishers are usually inspected yearly or bi-yearly by a trained professional. They can also be recharged.

    Dry chemicals, water, wet chemical, water additives, clean agents and carbon-dioxide are used as agents in fire extinguisher systems. The following table provides details about selecting the proper extinguisher based on various types of fire sources:

Fire Class	Fire Source	Suppressant					
		Water	Foam	Dry Chemical	Wet Chemical	Clean Agents and CO_2	Special Chemicals
A	Ordinary solid combustibles	Y	Y	Y	Y		
B	Flammable liquids & gases		Y	Y		Y	
C	Electrical equipment			Y		Y	
D	Combustible metals		Y				Y
K	Oils and fats		Y		Y		

Figure B.1: Classification for Fire Extinguishers

- **Standpipe System:** Standpipe systems deal with the connection of hose lines to the water supply. This provides a pre-piped water system for organizations and provides

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

water supply to hose lines in certain locations. Three types of standpipe systems include: Class I – A, Class II – A, Class III – A. These types differ in accordance with the thickness of the hose lines used and the volume of water that is used for fire suppression.

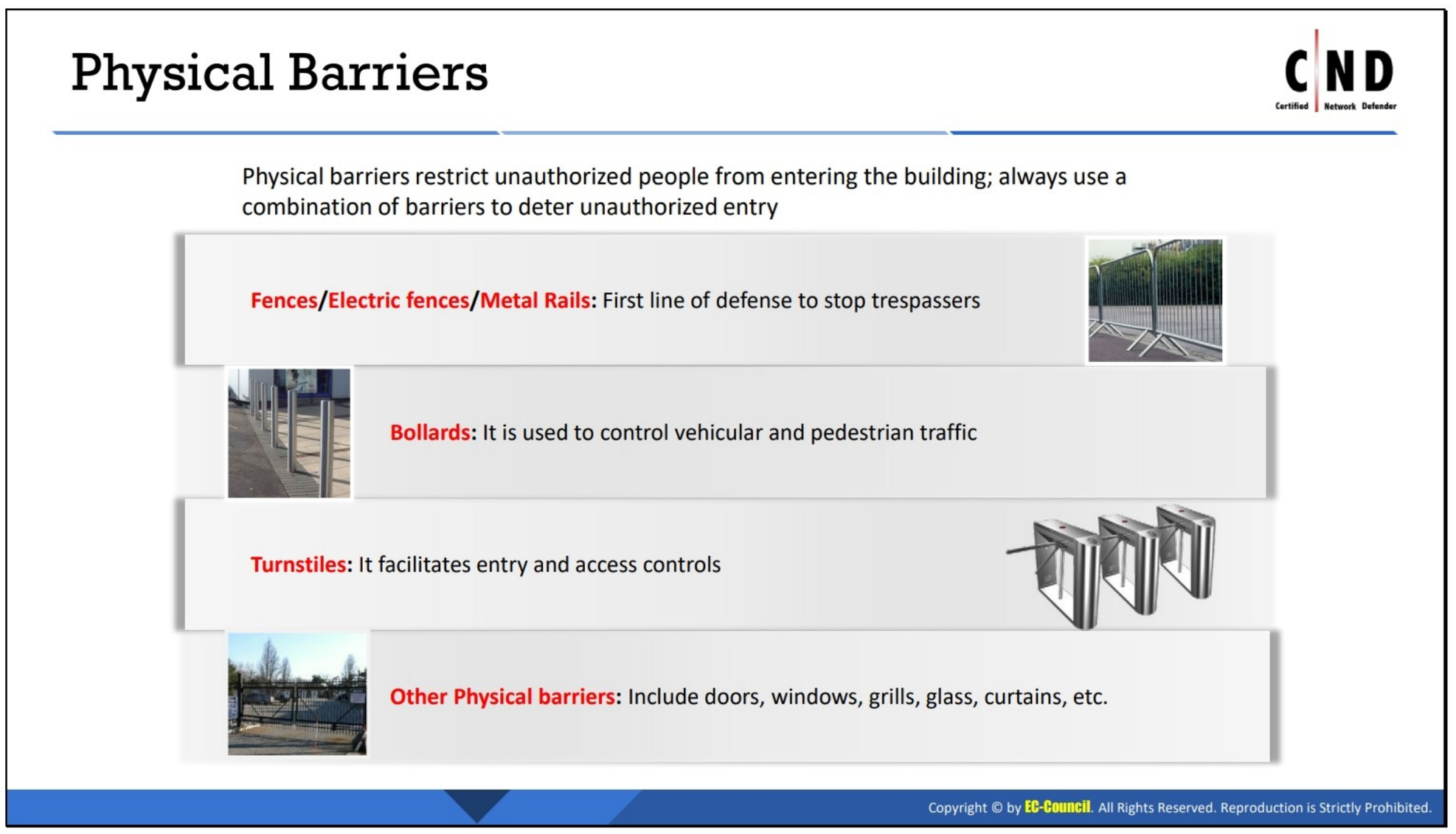
- **Sprinkler System:** Fire sprinkler system maintains a water supply system in order to supply water to a water distribution piping system that controls the sprinklers. Sprinklers are used in order to avoid human and asset loss. These are mainly used in areas where fire fighters are not able to reach with their hose lines.

Passive Fire Protection

Passive fire protection systems are used to prevent the fire from spreading further across the organization. Fire-resistant doors, windows and walls may be used for passive fire protection. This facilitates protecting occupants inside the organization and reduces the rate of damage due to the fire. Passive fire protection systems do not need to be activated by the other systems and no operational assistance is required in implementing passive fire protection systems.

- Passive fire protection is put into practice in the following ways:
  - Minimal use of flammable materials.
  - Building additional floors and rooms in a building slowing down the spread of the fire.
  - Providing adequate training to the occupants regarding the procedures to follow when a fire occurs.
  - Proper maintenance of fire related systems.
  - Adequate amount of emergency exits.
- Steps to deal with fire incidents:
  - Detect fire.
  - Evacuate occupants in the building to another safe location.
  - Notify the fire department and safety department regarding the fire.
  - Close down all electrical and electronic systems in order to avoid the fire spreading.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Physical Barriers

Many factors determine the physical security of an organization. All these factors are essential and contribute to the successful operation of physical security in an organization. The main goal of physical security relates to the control and prevention of unauthorized access, while physical barriers restrict unauthorized people from entering the building. Physical barriers define the physical boundary of your area and also divides vehicle traffic from pedestrians. Use of a physical barrier deters and delays an outsider from entering the premises. An intruder or outsider can compromise a barrier by spending time, money, planning and contemplating on the site architecture. In order to discourage these intruders, it is a good policy to use a multilayer approach such as external barriers, middle barriers and internal barriers. External barriers are fences, walls, etc.; although they are built to form a structure, they inadvertently act as an obstruction. Middle barriers are equipment used to obstruct the traffic and people. Internal barriers are doors, windows, grills, glass, curtains, etc.

Types of Physical Barriers used in a building are:

- **Fences/ Electric Fences/ Metal Rails:** It's a first line of defense that stops a trespasser and most commonly used across the globe. Fences/metal rails/electric fences generally mark the restricted areas, controlled areas and prevents unauthorized access.

  The aim of deploying physical barriers is:

  - Blocks and deters attackers.
  - Marks the boundary of the organization.
  - Protects the security guards from external attacks.
  - Prevents the entry of vehicles.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Protection against explosive attacks.



Figure B.2: Metal Rails

- **Bollards:** A bollard may be defined as a short vertical post which controls and restricts motor vehicles to the parking areas, offices etc. This facilitates the easy movement of people. Bollards are mainly used in building entrances, pedestrian areas and areas that require safety and security. It is effective in controlling pedestrian and vehicle traffic in sensitive areas.



Figure B.3: Bollards

- **Turnstiles:** This type of physical barrier allows entry to only one person at a time. Entry may be achieved only by the insertion of a coin, ticket or a pass. It allows the security personnel to closely watch the people entering the organization and stop any suspicious persons at the gate. However, the use of a turnstile can affect the fast evacuation of the occupants in case of a fire emergency.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure B.4: Turnstiles

- **Other Barriers:** It includes installing doors, windows, grills, glass, curtains to limit the access to certain area.
  - **Doors:** It can be used as a good source in controlling the access of users in a restricted area. Door security may be increased with the installation of CCTV cameras, proper lighting systems, locking technology, etc.
  - **Windows**: An intruder can use windows to gain unauthorized access to restricted areas. Proper security measures should be considered while installing windows. Some of these considerations include:
    - Method of opening the window.
    - Assembling and construction of window.
    - Technique used in locking the window.
    - Hinges used for the window.
  - **Grills:** Grills should be used with doors and windows for better security. Grills may be used for internal as well as external security.
  - **Glass:** Sliding glass doors, sliding glass windows provide a better level of physical security.



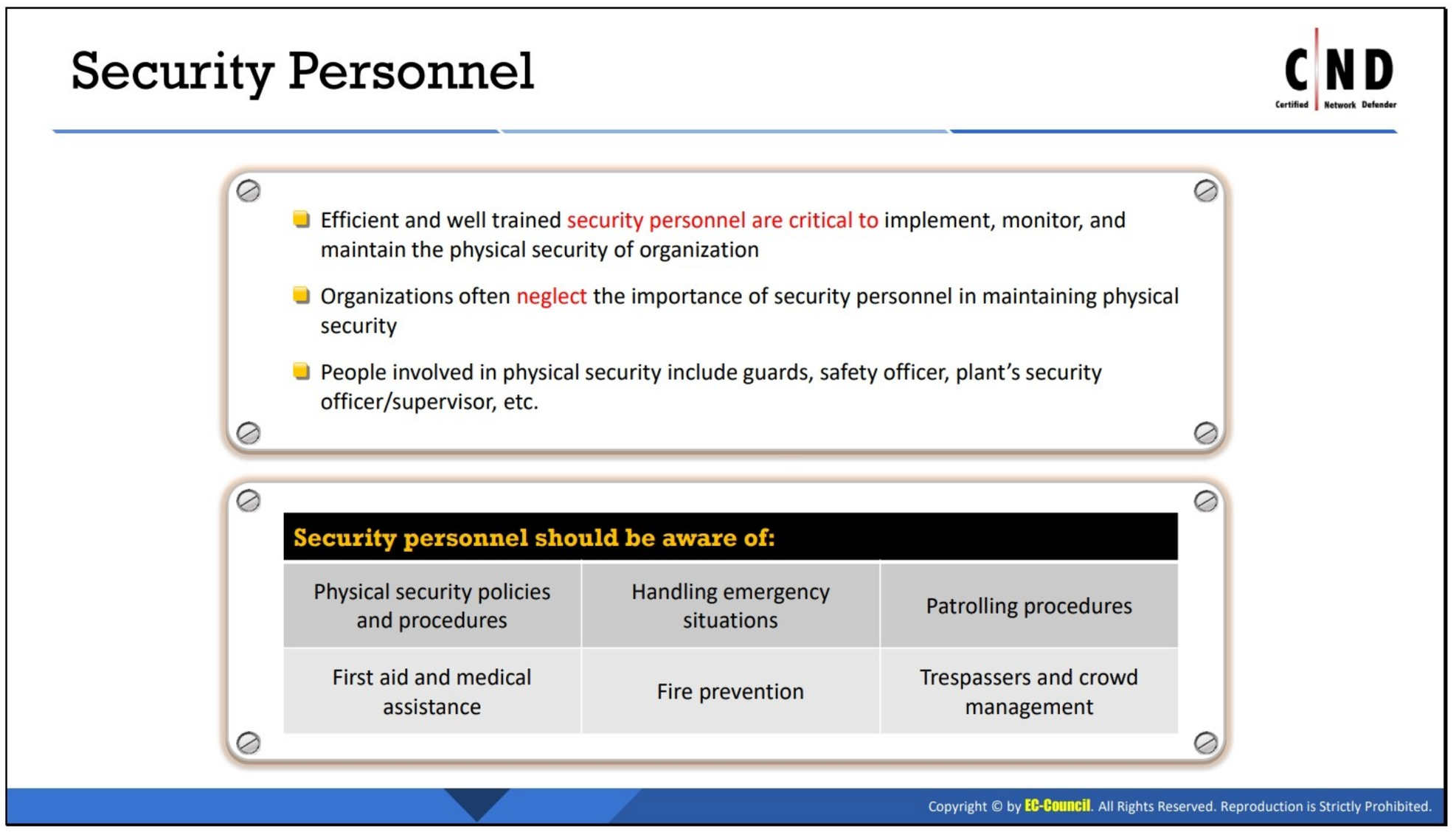
Figure B.5: Other Barriers

- The following are security considerations for physical barriers:
  - Use a combination of barriers to deter unauthorized entry.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use bullet resistant windows and glass.
- Install doors both at the main entrance and inner building.
- Lock doors and windows.
- Use electric security fences to detect climbing and cutting of wires.
- Use alarms to alert any intrusions from the fences.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Security Personnel

Security personnel/guards are hired to implement, monitor and maintain the physical security of an organization. They are individuals who are responsible for developing, evaluating, and implementing security functions such as installing security systems to protect sensitive information from loss, theft, sabotage, misuse, and compromise. Hiring skilled and trained security personnel can be an effective security measure for any organization. They play a crucial role in physical security. Organizations are not considering them as a core competency that they want to invest in as part of their strategic plan.

Organizations should hire security personnel by themselves and provide adequate training on physical security or they can contact dedicated physical security service firms who handle physical security for them. There are organizations that are dedicated to training security officers, provide standardized procedures, and manage the security on a 24x7x365 schedule, by sharing guards across different organizations.

People involved in Physical Security are:

- **Guards**: Their responsibilities include screening visitors and employees at the main gates or entrance, documenting names and other details about the visitor, conducting regular patrols in the premises, inspecting packages, luggage, and vehicles, managing vehicle traffic, guiding visitors to the reception area after noting their details, etc. Guards should maintain visitor logs and record entry and exit information. (CCTV) to act as a deterrent as well as provide a mechanism to detect and possibly prevent an intrusion is normally handled by guards.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

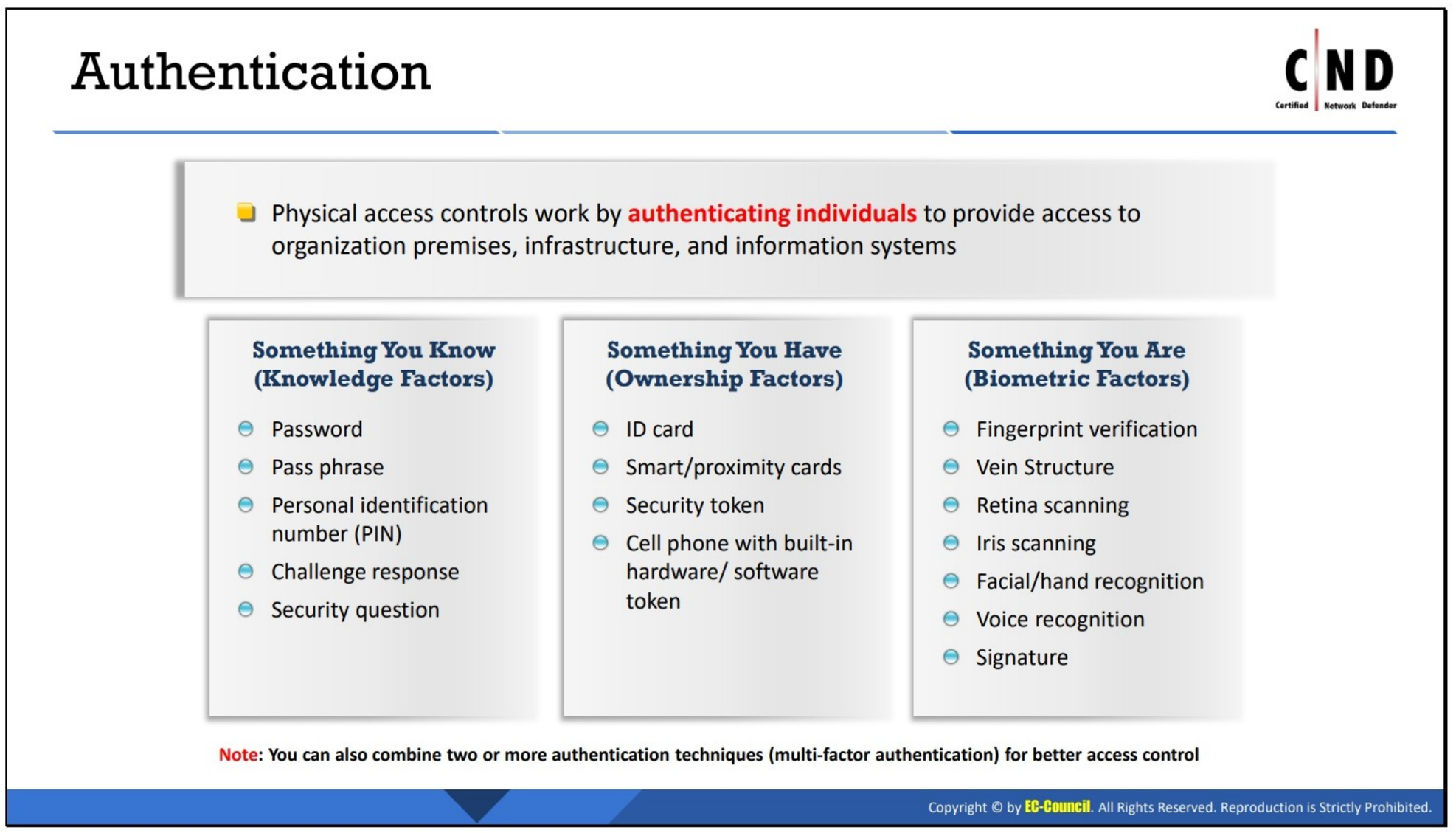
- **The plant's security officers/supervisors**: Their responsibilities include training and monitoring activities of the guards, assisting guards during crisis situations, handling crowds, and maintaining keys, locks, lights, greenery, etc. of the facility.
- **Safety officers**: Their responsibilities include implementing and managing safety-related equipment installed around the facility and ensuring proper functioning of this equipment.
- **Chief Information Security Officer (CISO)**: In the past, it was common place for the CISO of an organization to be an extremely technically competent individual who has held various positions within an enterprise security function or may even have come from a networking or systems background. Today, a CISO is required to be much more than technically competent. The modern CISO must have a diversified set of skills in order to successfully dispatch their duties and establish the appropriate level of security and security investment for their organization.

Continuous training for your security personnel will provide maximum benefits and an effective team for your organization. Regardless of the position, security-related personnel should be selected based upon experience and qualification required for the job. Executives should thoroughly evaluate the personnel's past experiences and based upon this information provide adequate training to fill the gap between ability and skills necessary for the job.

An organization should train newly hired security personnel on following areas:

- Organizational culture, ethics and professionalism.
- Security policies and procedures.
- Policy enforcement.
- Trespassers and crowd management.
- Handling emergency situations.
- Human and public relations.
- Patrolling procedures.
- Managing workplace violence.
- First aid and medical assistance.
- Fire prevention.
- Vehicle traffic management.
- Handling foreign guests, invitees, etc.
- Report writing.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Authentication

Physical access controls work by authenticating individuals to provide access to organization premises, infrastructure, and information systems

Something You Know (Knowledge Factors)

Passwords, passphrases or PIN based authentication offers an easy way of authenticating users. Users have to supply their unique password, passphrase or PIN to authenticate with the system.

- **Passwords**: Passwords generally contain a combination of letters and numbers. Users created their password at the time of their first login with the system. Organizations should enforce a strong password creation policy.
- **Passphrase:** Passphrase is similar to a password, but is generally longer for added security. It is generally used with cryptographic programs and systems. The user supplies a passphrase as an encryption key to these cryptographic programs and systems.
- **Personal Identification Number (PIN)**: A numerical password provided in order to authenticate a user with system. The PIN is generally used for authentication while using an ATM card. PIN lengths can be a maximum of 12 characters long.
- **Challenge Response**: A question and answer type authentication where the system throws a challenge to users and users have to provide a valid response in order to confirm their identity. One of the examples of the challenge response system is CAPTCHA. CAPTCHAs are distorted images with hidden letters. The user needs to retrieve the hidden letters and respond to it to confirm their identity. This kind of authentication system is used to ensure the input is human generated not computer generated.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Security Questions**: Security questions are used as an extra step for authentication. These are generally used by banks and wireless providers to reconfirm the identity of the user. Security questions are generally implemented with "forgot password" features which reconfirms or proves your identity.

Something You Have (Ownership Factors)

- **ID Card:** Identity document (ID card) can be used to authenticate users with the system. It includes ID cards such as a driver's license, photo ID card, passport, etc. Generally, an ID card is the same size as a credit card.
- **Smart Card:** A smart card is a credit card-sized plastic device that contains a silicon computer chip and memory. It can store, process, and output data in a secure manner. It commonly stores cryptographic keys, digital certificates, identification credentials, and other information. It provides strong two-factor authentication using a PIN number. The International Organization for Standardizations (ISO) uses the term Integrated Circuit Card (ICC) instead of smart cards. The smart card has the dimension of 85.6 mm x 53.98 mm x 0.76 mm which is similar to ATM cards and credit cards. Smart cards can provide additional functionality such as credential storage.
  - **Benefits of Smart Cards**: There are many benefits of smart cards such as:
    - **Lower Administrative Costs**: As there are fewer passwords in the network, the cost to support and manage the system decreases.
    - **Reduce Losses and Liabilities**: Security is increased as encryption and a strong two-factor authentication protects the data.
    - **Increased Convenience**: Smart cards are portable and simple to use. The convenient factor for this system of authentication is high.
  - **Smart Card Uses**: One of the important factors behind smart card use is the fact that multiple applications are involved. A smart card provides portable secure storage for the digital certificates. The smart card can also be used for many applications, such as:
    - Logon/logoff authentication of an operating system.
    - Authentication to website.
    - Sending/receiving of source email.
    - Encryption of data files.
- **Proximity Cards**: A proximity card is also similar to a credit card. Several companies use proximity cards to control physical access. When using this card, the employee holds their card within a few inches from the reader. The card reader receives a unique ID from the card and transmits it to the central computer that tells the receiver whether or not to open the door.

  Proximity cards are harder to duplicate and have more control when turning off access. Some systems combine the logical and physical access on the same card. Different

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

techniques are used for card sensing like an integrated circuit which is embedded in the card to generate a code magnetically or electrostatically and circuits are embedded with the code that is tuned to varying resonant frequencies. It is a best practice to place the company's logo and address on the keycard so if it is lost or stolen, it can be returned.

- **Security Token:** Security tokens are generally used for verifying the identity of a user by means of electronic devices. Users may store cryptographic keys like digital signatures, biometric data etc. as a security token. Tokens consist of secret information that verifies the identity of the user. The information may be stored using the following tokens:
  - **Static Password Token**: Contains hidden information that is available during each authentication step
  - **Synchronous Dynamic Password Token**: Uses a cryptographic algorithm that uses a synchronized clock between the token and the authentication server
  - **Asynchronous Token**: Generates a one-time password using a cryptographic algorithm
  - **Challenge Response Token**: Uses public key cryptography
- **Mobile phone with a built-in Hardware/Software Token:** Mobile phone with built-in hardware/software tokens is a two-factor authentication security device that authenticates the services running on a computer device. Software tokens are placed on the devices and are easy to replicate. Hardware tokens are stored as credentials inside the hardware device and are unable to be replicated.

Something You Are (Biometric Factors)

- **Fingerprinting:** Fingerprint verification or scanning is a popular biometric authentication technology used for authenticating individuals. In the fingerprint verification, the entire fingerprint image of an individual is obtained and stored in a database. The identity of the user is confirmed by comparing the fingerprint with the stored image. If it matches, authentication becomes successful. Biometric fingerprint scanning systems do not store a full image of the fingerprint in a database. A small template created from the fingerprint is stored.

  Fingerprint scanning devices come in different packages. For example: a stand-alone device for the desktop PC, to small portable devices for laptop computers, built-in keyboards and built-in mice.
- **Retinal Scanning:** It is another method of biometric authentication where authentication is made based on a retinal scan of the individual. The retina is a part of the human eye and holds different characteristics for each person. Even identical twins have a different retinal pattern. The retina is a thin layer of nerves (about 1/50thof an inch, or a 0.5 mm thick) found on the back of the eye. As a part of the eye, the retina transmits impulses through the optic nerves to the brain. Retina scanning is difficult compared to other scans in biometric technology. To present the raw biometric data, users must move their head into position with their eye very close (less than an inch) to the scanner for it to read the

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

retina through the pupil. During the scan process, the user will focus on a green light in the scanner. After generating the template, it provides an excellent matching.

- **Iris Scanning:** Each individual holds a unique iris pattern same as the retina. It can be different in structure such as ligaments, furrows, striation, ridges, and zigzags. Iridian technology measures 247 independent variables in an iris.

  Iris scanning is a process of taking images of an iris and creating biometric templates used in matching functions. Similar to fingerprints, it also requires a device to capture the image and software to process the image. The iris scanning device uses a camera, which can be either a still or a video camera to capture the iris information. The camera captures a high-resolution image of the iris and then the device will locate the border between the pupil and the iris. The device will then convert the data to a grayscale image. This gray scale image identifies the unique feature of the iris.

- **Vein Structure Scanning:** Vein structure scanning is also known as vascular biometrics and mainly depends on the patterns in a user's vein. The vein scanning technique focuses on authenticating a person's identity by checking the patterns of the vein structure. Veins are normally found under the skin and scanning requires the flow of blood in the veins.

  Users need to place the palm, the back of the hand or the wrist on the scanner. The scanner takes a picture of the part placed on the scanner using infrared light. Hemoglobin absorbs infrared light and it highlights the veins in the picture. A reference template is created according to the shape and location of the vein structure.

- **Face or Hand Recognition**

  - **Facial Recognition**: Facial scanning or facial recognition is famous due to large-scale implementations that have taken place for surveillance purposes. It works by picking out the unique characteristics of a human face and matching these against facial images in a database. These are the facial characteristics that a face scanning system looks for:

    - Size of eyes
    - Distance between the eyes
    - Depth of the eye sockets
    - Location of the nose
    - Size of the nose
    - Location of the chin
    - Size of the chin
    - Jaw line
    - Size, position, and shape of the cheekbone

    The facial scanning process starts with the acquisition of an image of a human face. This image can be acquired by using any imaging source, static cameras or video

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

cameras, both analog and digital. After capturing the isolated facial image, the system will create a face print of that image. The face print is the template for the system. This is the process of translating the facial image into unique code or a data set that can represent the facial image.

- **Hand Recognition:** Hand Recognition is a biometric technique used to identify a user by the shape of their hand. It is a simple and accurate procedure. The use of this technique requires special hardware and can integrate into any system or device. It uses finger width/height, thickness and shape for identification purposes. The user places the hand on a metal surface, which has a guidance page on it. The pages align the hand in a proper position so the device can read the hand attributes. The device then verifies the user details in its database.

- **Voice Recognition:** Human voice scanning and recognition is another method of biometric authentication where a user's voice is recorded using voice recognition software and it performs a matching function to identify the individual. It is based on identifying a unique characteristic of the human voice. This system uses voice recognition software to allow users to interact with the computer by issuing commands verbally instead of using an input device, such as a mouse. Any microphone, landline telephone, cellular telephone, or any other device is used to capture the human voice.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Physical Locks

Various types of locking systems are available to improve the restriction of unauthorized physical access. The organization should select an appropriate locking system according to their security requirements.

Different types of locks are:

- **Mechanical Locks**: Provide an easy method to restrict unauthorized access in an organization. Mechanical locks come with or without keys. There are two types of mechanical locks.
  - **Warded Lock**: Contains a spring loaded bolt attached to a notch. A key inserted into the notch moves the bolt backward and forward. Only the correct keys can be inserted into the notch and it blocks the wrong key.
  - **Tumbler Lock**: Consists of pieces of metal inside a slot in the bolt. This prevents the bolt from movement. A correct key contains grooves that allow the bolt to move by raising the metal pieces above the bolt. It is further classified into Pin Tumbler, Disk Tumbler and Lever Tumbler locks.
- **Digital Locks:** Digital locks use fingerprint, smart card or a PIN on the keypad to unlock. It is easy to handle and does not require keys, so there is no chance of forgetting or losing the keys. It provides automatic locking for doors. The user only has to use their fingerprint impression, swipe the smart card or enter the PIN to unlock it.
- **Electric/Electromagnetic Locks**: Electric locks or an electronic locking system operates on an electric current. Locking and unlocking is achieved by supplying and eliminating power.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

It mainly uses magnets or motors to activate or deactivate the locks. It does not require keys to be maintained for the locking system.

An electromagnetic lock or magnetic lock consists mainly of an electromagnet and an armature plate. The locking device consists of two types of status “Fail Safe” or “Fail Secure”. Fail secure locks remain locked even during power loss, whereas Fail safe remains inactive when de-energized. The electromagnetic part may be placed on the door frame and the armature plate may be placed on the door. The magnetic flux created by the electromagnet gets attracted towards the armature plate and this initiates the door closing process.

- **Combination Locks:** It has a combination of numbers and letters. The user needs to provide the combination to open the lock. Users may enter the combination sequence either through a keypad or by using a rotating dial that intermingles with several other rotating discs. Combination locks do not use keys for functioning.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Concealed Weapon/Contraband Detection Devices

Contraband Detection Devices act as an important physical security control as it restricts activities and/or a person carrying contraband substances from entering the premises. Contraband substances are illegal materials such as explosives, bombs, weapons, etc., which should be banned from the premises. The person trying to enter into the office with contraband substances can be considered an act of terrorism. Contraband Detection Devices are able to detect substances, even though it is covered with other objects.

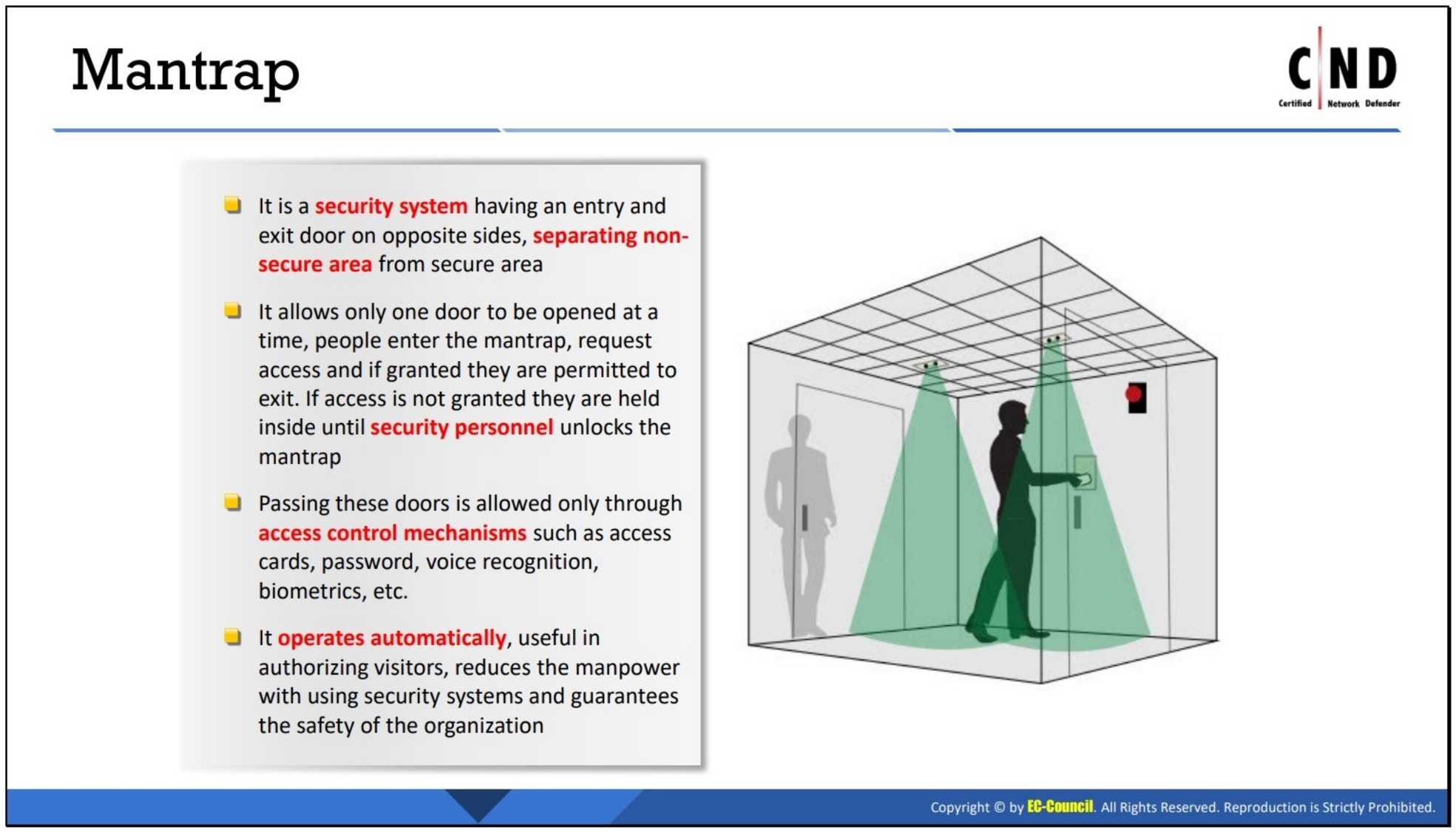
Different types of devices are used to detect contraband materials such as a handheld metal detector, walkthrough metal detector, X-ray inspection system, etc.

Walkthrough metal detectors are mainly used in airport terminals, schools, sports stadiums etc. These help check people who have admission to certain areas. The walk through detectors should be maintained and properly monitored. It should be deployed at each entry point of the organization.

Handheld metal detectors allow people to be screened more closely and to detect any suspected elements. Handheld detectors are used in all places where the walk through detectors are used.

X-ray inspection systems are easy to handle and use. They use X-rays instead of visible light to screen the objects.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Mantrap

Mantrap is another type of physical access security control which is used for catching trespassers. It is most widely used to separate non-secure areas from secure areas and prevents unauthorized access. It is a mechanical locking mechanism comprised of a small space with two sets of interlocking doors. The first set of doors must close before the second set opens. User authentication at mantrap doors is performed using smart cards, keypad/PIN or biometric verification. The closing and opening of doors is handled automatically or through security guards.

How Do Mantraps work?

- **Step 1:** Authenticates the person trying to access
- **Step 2:** The first door opens after authentication. The person walks in.
- **Step 3:** First door closes soon after the person enters the room. Now the person gets locked inside the room. This signals the second door to get unlocked.
- **Step 4:** The second door opens with the person walking out of the room. The first door gets automatically locked soon after the second door opens.
- **Step 5:** The second door gets into locked state soon after the person walks out the second door.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Warning Signs

- Warning signs are use to ensure someone does not inadvertently intrude in any **restricted areas**
- Appropriate warning signs should be placed at each access control point

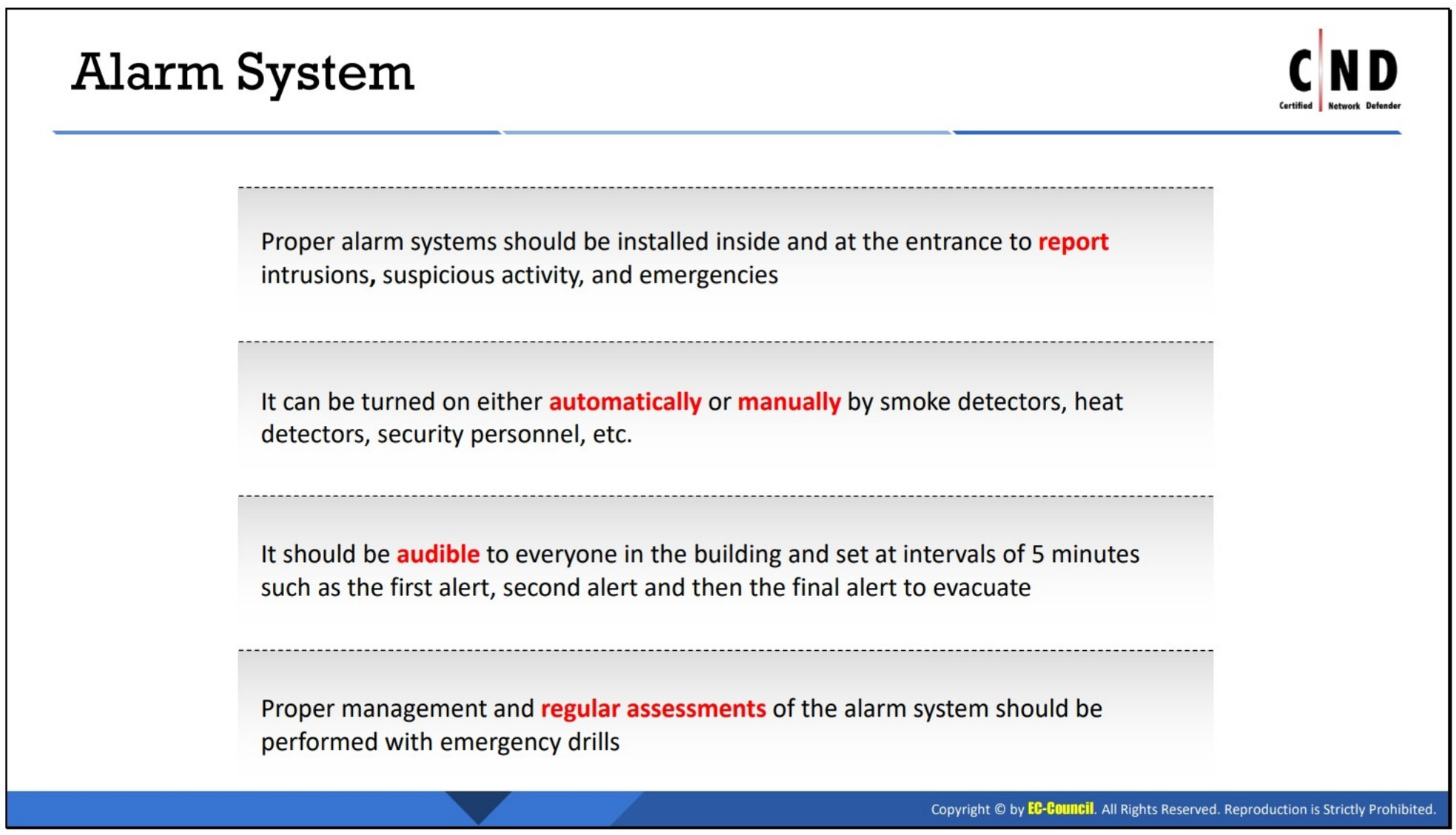


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Warning Signs

Warning signs are generally used in order to restrict any unauthorized access in an organization. Warning signs are kept at entrance points, boundaries of the locality and sensitive areas. Warning signs should be visible to users such that people will understand the prohibited areas where they should not enter. Warning signs also help organizations to clear a large amounts of people from entering into sensitive areas. Warning Signs are generally kept at all sensitive areas where there could be a threat of damaging and distrusting of information, assets, or life. For example, a typical use of warning is kept on an Electrical fence. It may pose a threat to life, when someone touches an electric fence unknowingly. Typical warning signs are RESTRICTED AREA, WARNING, CAUTION, DANGER, BEWARE, etc.

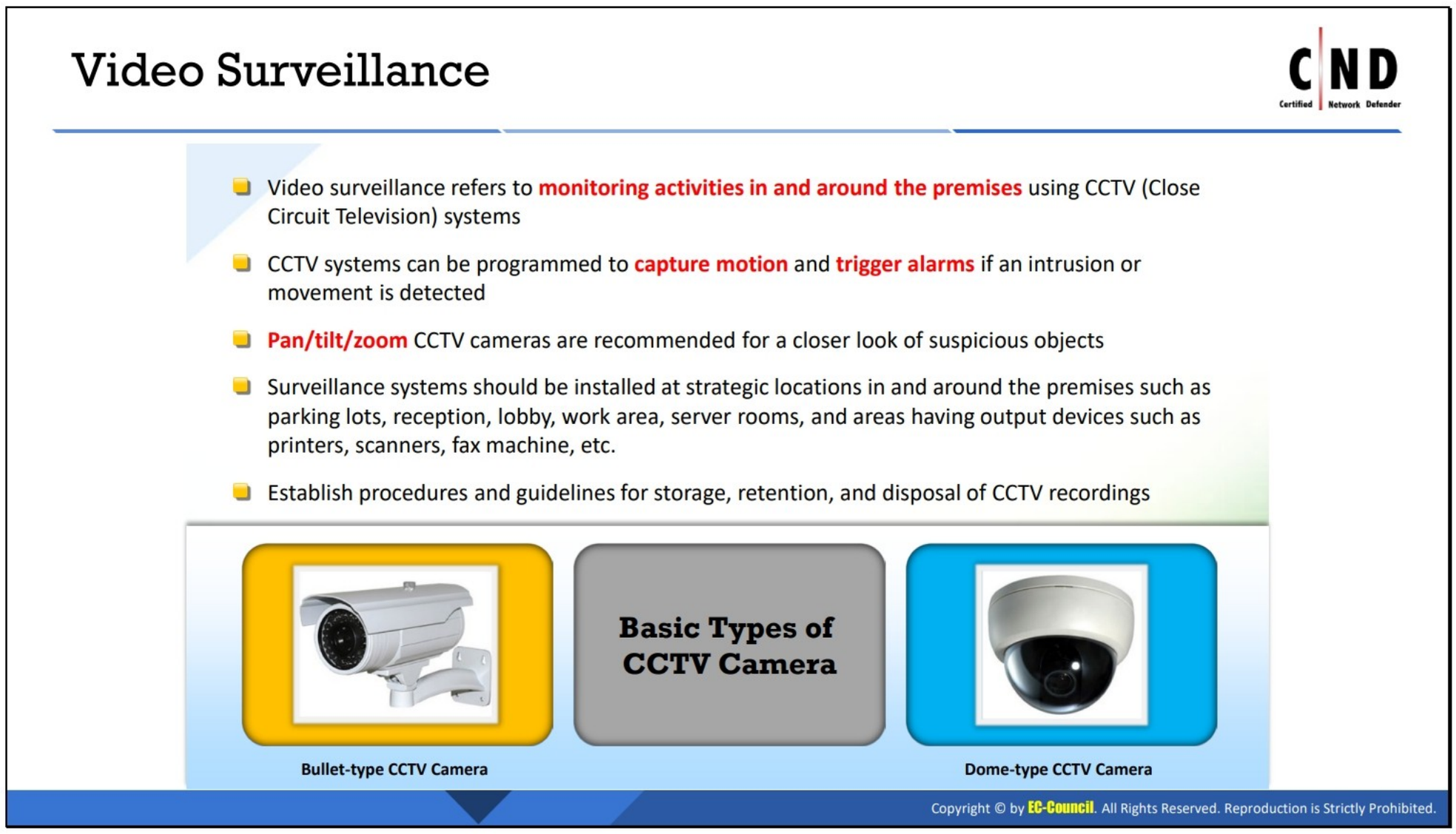
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Alarm System

Alarms are used to draw attention when there is a breach or during an attempt of breach. Alarm sounds can be different types based on a facility such as sirens, flash lighting with a sound, email, and/or voice alerts. The organization should divide their large facilities such as buildings, floors, sections, and offices into small security zones and depending upon their significance, the appropriate alarm system should be placed. Security zones that store high priority data are given multilevel security, such as restricting access with access control devices, biometrics, surveillance, locks and alarms to draw attention in any event of intrusion. Organizations should have a proper power backup to alarm systems so that it will work in emergencies and also during a power shutdown. All wiring and components of an alarm should be protected from tampering and even conceal the alarm box with proper locks and limited access.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Video Surveillance

Video surveillance is considered as an important component of physical security. These systems protect an organization's assets and building from intruders, theft, etc. CCTV is used as part of the organization's security system. CCTV covers a large area and is often placed near gates, reception, hallways, and at the workplace. It captures illicit activities inside the premises and also helps monitor activities inside, outside and at the entrance. They are even programmed to capture motion and initiate an alarm whenever it detects a motion or an object. They help identify activities that need attention, collect images as evidence and aid in an alarm system. The devices used for video surveillance should be automatic, powerful, and capable of pan/tilt/zoom to capture the action and store them for later review.

There are many things that need to be considered for installation, management and maintenance of a video surveillance system in an organization such as the camera, lens, resolution, recording time, recording equipment, cabling, monitoring system, storage devices and centralized control system/equipment. Recording activities through CCTV and storing this footage for reference can also help facilities provide evidence in a court of law. It is also important to decide what type of lens, resolution, and coverage area your camera should cover, along with recording the time and date of the video. Another important aspect is storing video recordings and for how long they will be stored. What will happen with the old video recordings and how will they be disposed?

The following are a few considerations for video surveillance systems:

- Install surveillance systems at the parking lot, reception, lobby, and workstation.
- Place output devices such as printers, scanners, fax machine, etc., in public view under surveillance.
- Integrate surveillance with an alarm system.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Establish a procedure for the amount of time the recorded video should be kept and then later disposed.
- Store all devices in a secure location with limited access.
- Use proper disposal systems such as deleting contents, overwriting, and physical destruction.

Different types of CCTV cameras available are:

- **Dome CCTV:** Mainly used in indoor security and surveillance purposes. Dome CCTV are built as a dome shaped model to prevent the cameras from any sort of damage or destruction. It is impossible to locate the direction at which the cameras are moving and thus allows for observing areas at a wide angle and cover larger areas. Speed Dome CCTV camera units provide the facility with pan/tilt/zoom and spin features, allowing the operator to move the camera according to their need.



Figure B.6: Dome CCTV

- **Bullet CCTV:** It is used for indoor and outdoor surveillance. These are generally placed in protective covers that prevent it from dust, rain or any other disturbances. Bullet CCTV is normally a long, cylindrical and tapered shape that facilitates for long distance surveillance.



Figure B.7: Bullet CCTV

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **C-Mount CCTV Camera:** It consists of detachable lenses, which provide surveillance for more than 40.ft. Other CCTV camera lenses provide only 35 – 40 ft. coverage. C-Mount allows different lenses to be used according to the distance to be covered.



Figure B.8: C-Mount CCTV Camera

- **Day/Night CCTV Camera:** It is commonly used for outdoor surveillance. It can capture images even during low light and darkness conditions. These types of camera do not require infrared illuminators in order to capture images. These can capture clear images during glare, direct sunlight, reflections etc.



Figure B.9: Day/Night CCTV Camera

- **Infrared Night Vision CCTV Camera:** It is commonly used for outdoor surveillance and can capture images in complete darkness. You can use an infrared LED's for areas having poor lighting.



Figure B.10: Infrared Night Vision CCTV Camera

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Network/IP CCTV Camera:** It consists of wired and wireless models. It allows sending images over the internet. It is easier to install a wireless IP camera than a wired camera as they do not require any cabling.



Figure B.11: Network/IP CCTV Camera

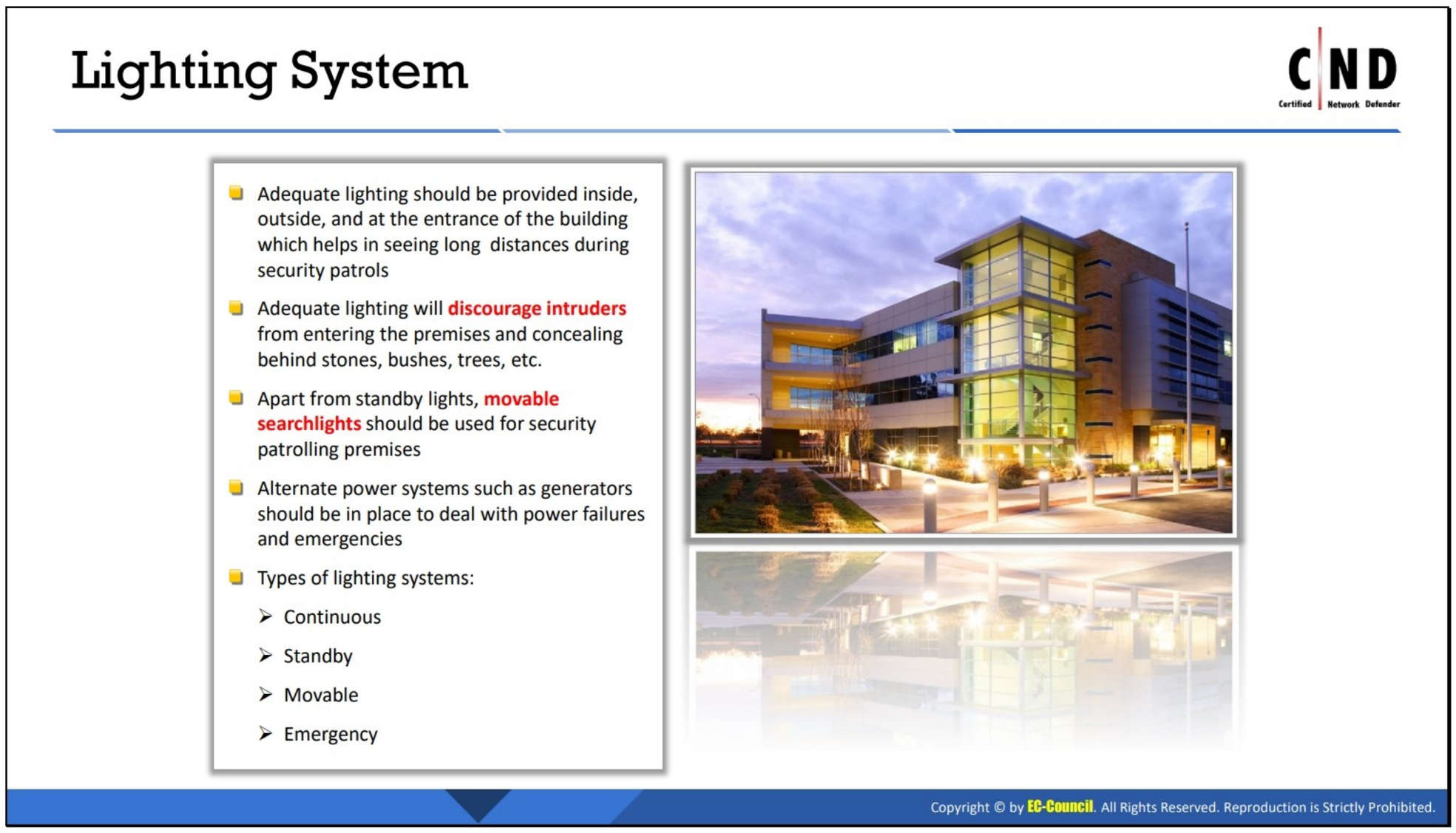
- **Wireless CCTV Camera:** Wireless CCTV cameras are easier to install and use different modes for wireless transmission.



Figure B.12: Wireless CCTV Camera

- **High-Definition HD CCTV Camera**: It is mainly used in sensitive locations that require more attention. It allows operators to zoom into a particular area.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

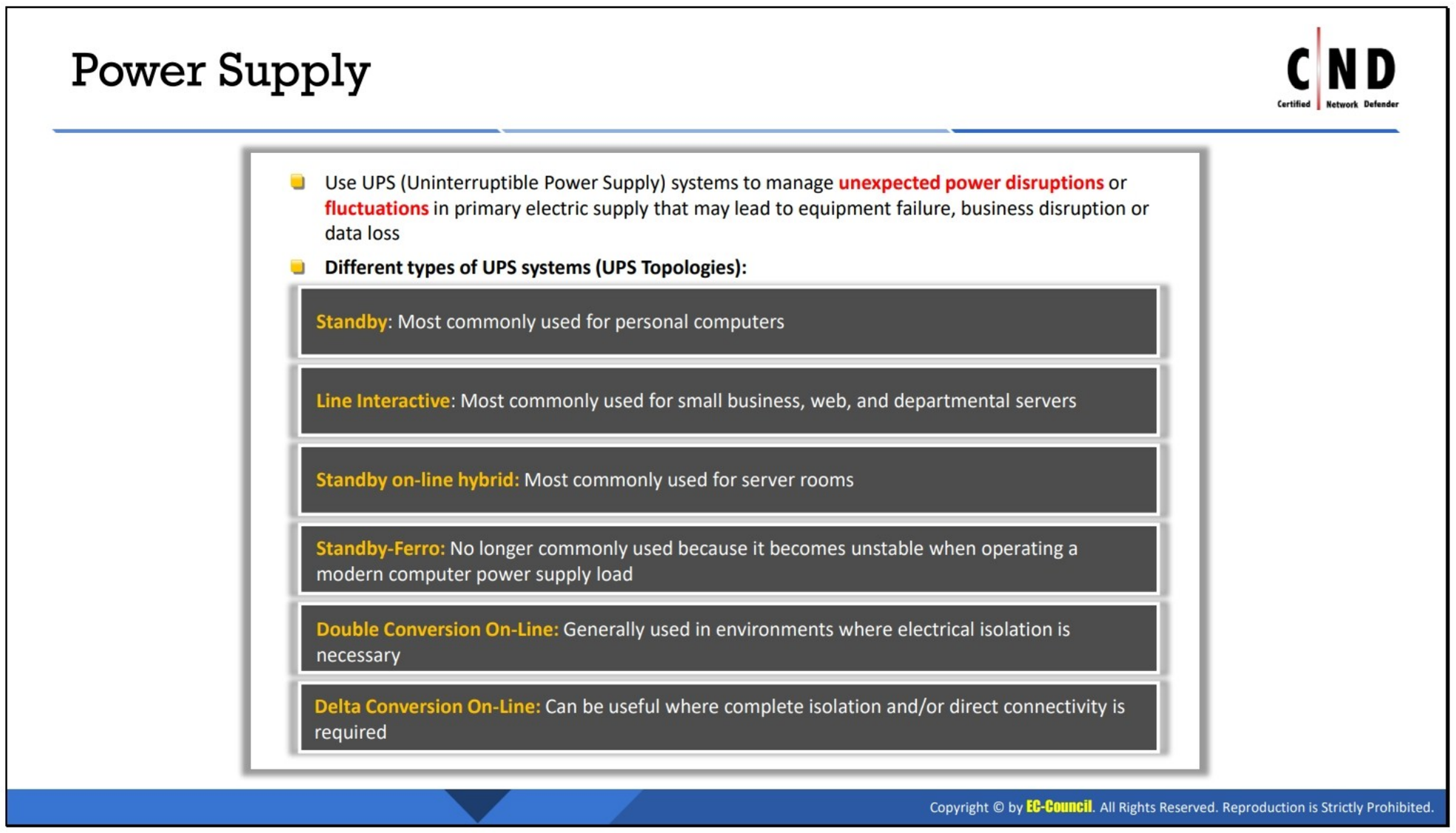


Lighting System

Security lighting is an important aspect of physical security of a facility. If the organization has not implemented an adequate lighting system in and around the organization, it can drastically degrade the function or performance of all other security measures. For example, if the organization does not have lighting at rear corners, near bushes, plants, parking, and near surveillance cameras, then it is difficult to find people or objects hidden in these locations. With poor lighting, it will be difficult to identify people entering the premises, as an intruder may act as an employee or use tricks to circumvent the security. Lighting systems in a location depend on its layout and sensitivity.

- **Continuous Lighting**: Fixed sets of lights arranged so they provide continuous lighting to a large area throughout the night.
- **Standby Lighting**: Used whenever any suspicious activity is detected by security personnel or by an alarm system. These operate either manually or automatically.
- **Movable Lighting**: Manually controlled lighting system that provides a lighting system at night or only when needed. Normally used as an extension of a continuous or standby lighting system.
- **Emergency Lighting**: Used mainly during power failures or if other normal lighting systems do not operate properly.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Power Supply

Facilities may suffer blackouts or power outages that could make the systems inoperable unless appropriate alternative power management capabilities are kept in place. Power outages could impact the ability to provide information technology as expected and also in maintaining physical security. Power spikes, surges, or blackouts could result in too much or not enough power and could damage equipment.

Consider the following security measures to deal with blackouts or power outages:

- Be prepared for power fluctuations.
- Use Uninterruptible power supply (UPS) to manage power outages.
- Safeguard systems from environmental threats.
- Protect systems from adverse effects of static electricity at a workplace.
- Use plugging equipment properly.

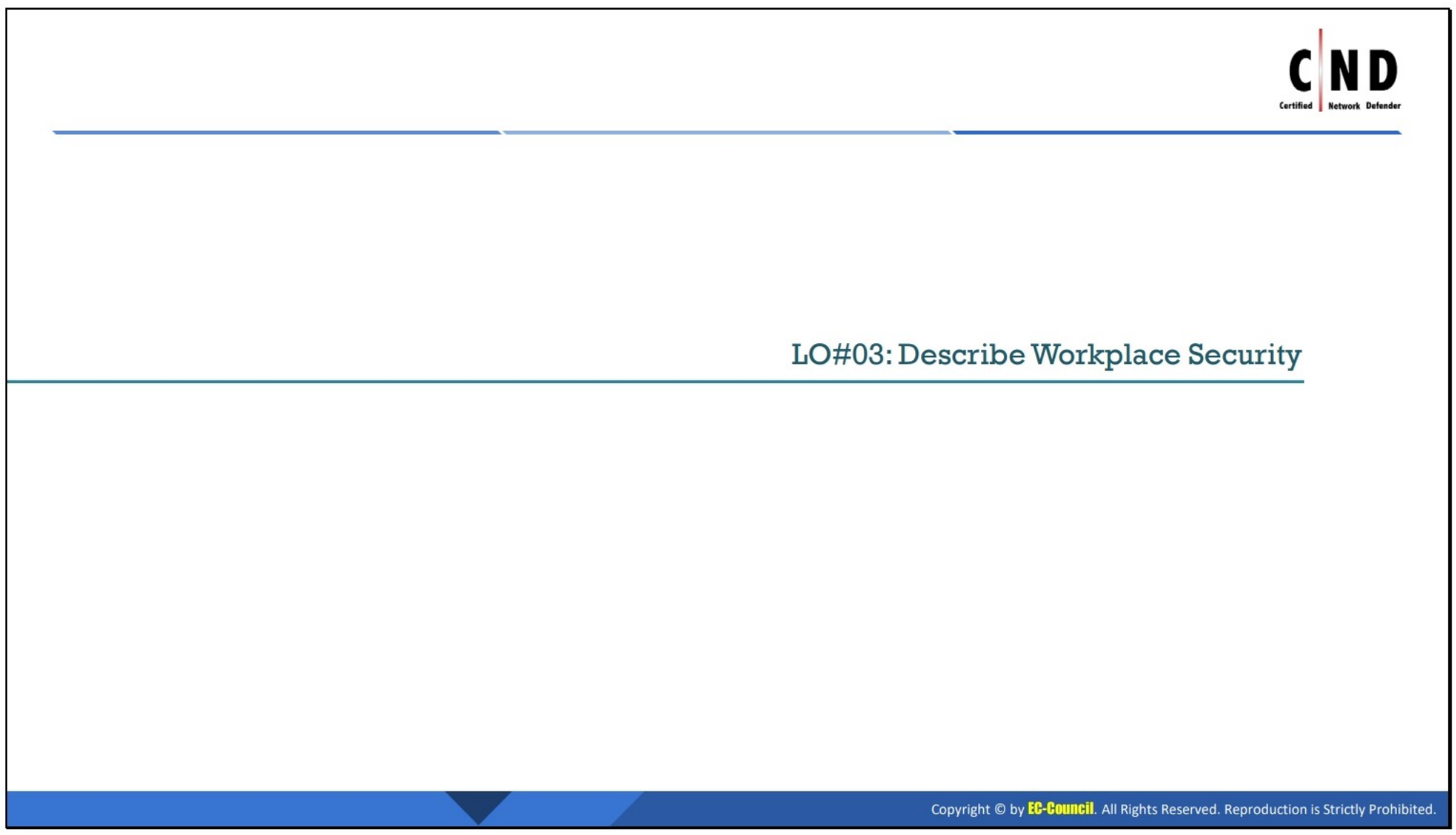
An Uninterruptible Power Supply (UPS) allows computers to function properly during a power failure. It protects the computers during fluctuations in the power supply as well. An UPS contains a battery that senses power fluctuations in the primary device. Users need to save all the data when the UPS senses the power fluctuation. The operator needs to provide measures which must be followed at the time of power loss. An UPS is commonly used to protect computers, data centers, telecommunication equipment etc.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Different types of UPS include:

- **Standby:** An offline battery backup facilitating the maintenance of the primary device from a power fluctuation. A standby power supply contains AC-DC circuitry that connects to the UPS during a power fluctuation.
- **Line Interactive:** Line interactive mainly deals with maintaining continuous power fluctuations. This method of a power supply needs very little battery usage.
- **Stand by On-line hybrid:** These are mainly used to supply power below 10k VA. It is connected to the battery during a power failure.
- **Stand by Ferro:** A Ferro resonant transformer is used for filtering the output. Stand by Ferro provides ample time for switching from main power to battery power.
- **Double conversion on-line:** It is used to supply power above 10k VA. It provides an ideal electric output presentation, and its constant wear on the power components reduces the dependability. It exhibits a transfer time only during a large load of current.
- **Delta conversion on-line:** It contains an inverter that supplies the load voltage. It is available in a range between 5k VA to 1 MW. It controls the power input performance and charging the UPS battery.

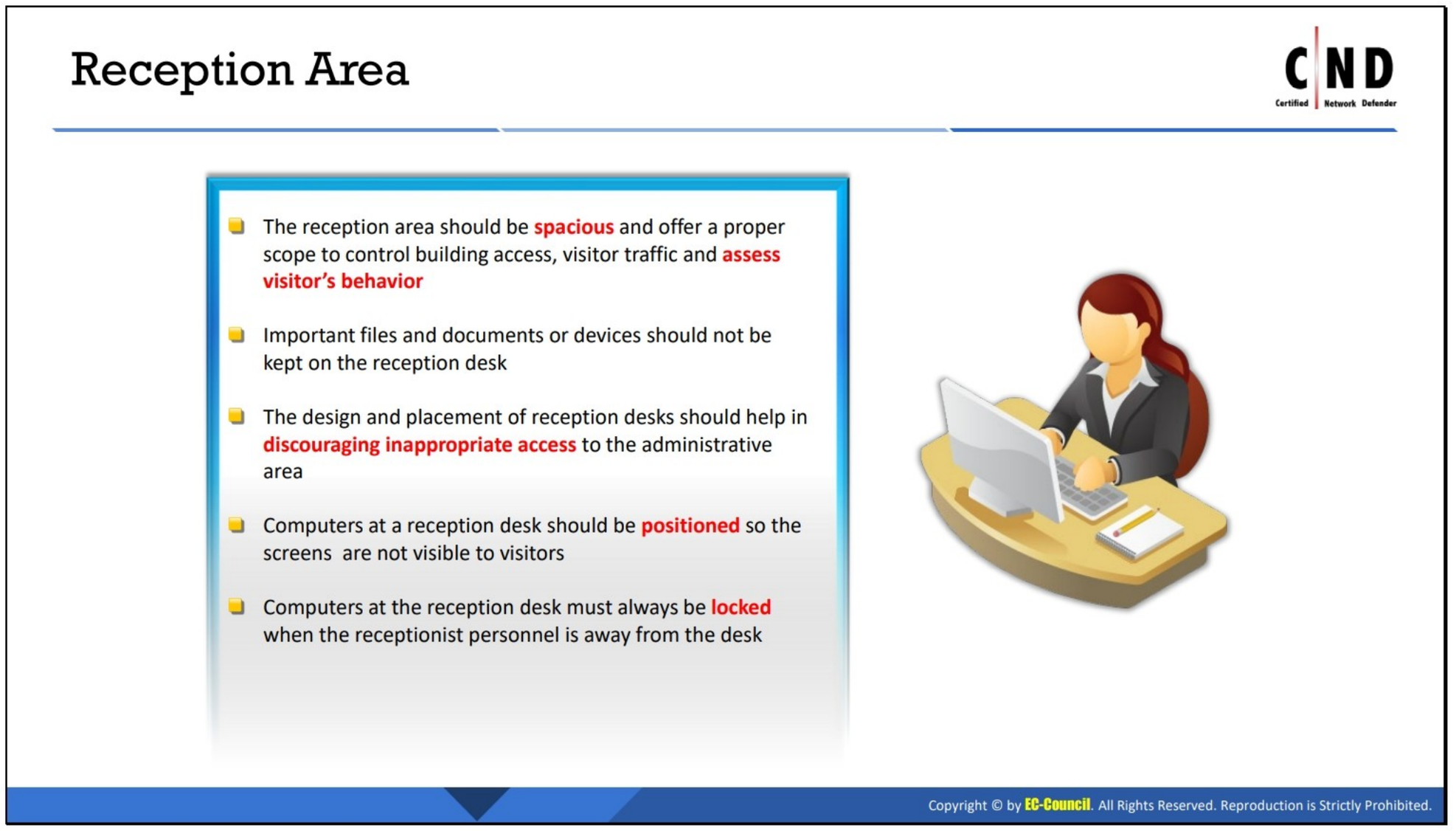
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#03: Workplace Security

This section explains workplace security in the office environment.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

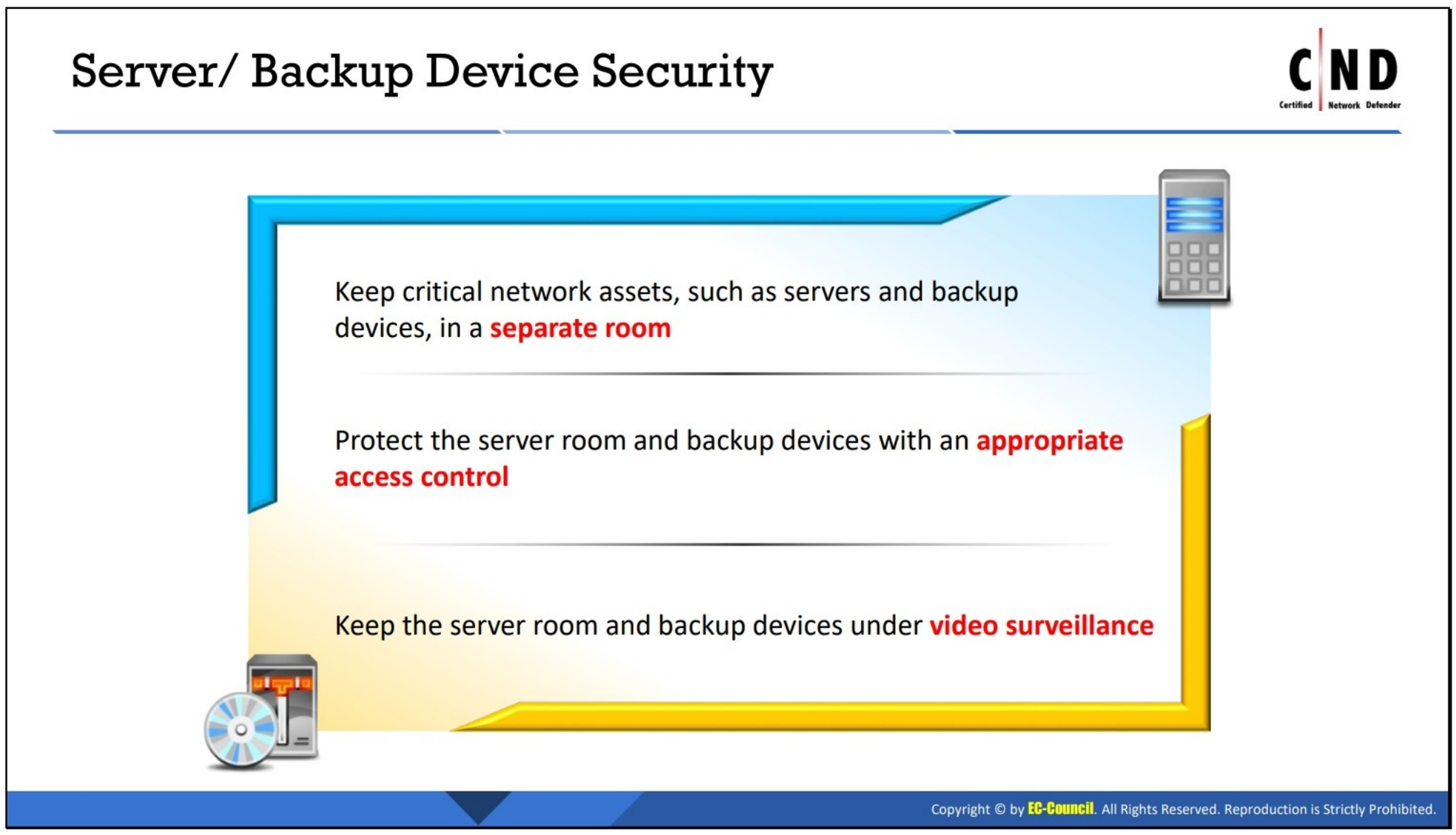


Reception Area

The reception area is always the initial contact for an unknown between them and the organization. The reception area can be vulnerable to physical security breaches as it provides easy access to strangers. Organizations often have regular visits from clients, the general public, invitees, etc., and require staff to greet, assist and direct them. Receptionists should be able to recognize or identify any unusual behavior, including solicitors and peddlers, charity organizations, ex-employees, etc. The reception personnel should maintain eye contact, non-confrontational facial expressions or posture while meeting people. They should be proficient enough to handle emergency situations and follow procedures to call immediate attention, alarm, radio, first aid, etc.

The reception area should be small in size. This provides a better area to closely monitor visitors and the reception area. Reception personnel should observe people entering the company. They should notice and record odd behavior for any strangers. There should be certain benchmarks to judge people arriving to the organization. Their intentions have to be noted, whether a person is searching for someone or for something.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



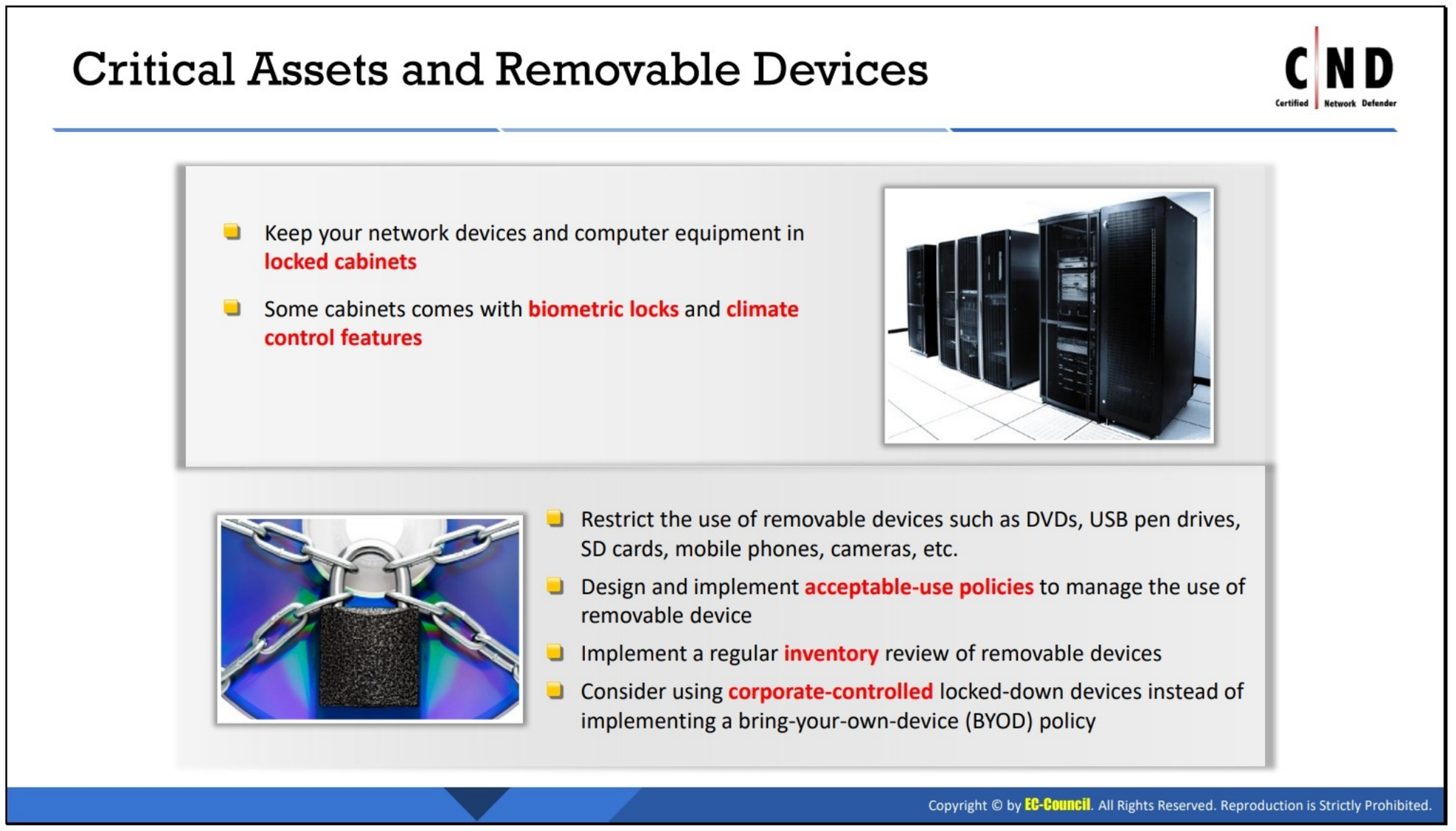
Server/ Backup Device Security

The organization should consider the physical security of their critical servers and backup devices. Physical access to these devices should be restricted. Only approved personnel should have access to these devices.

Typical physical security measures for server and backup devices are:

- Keep the server and backup devices in a separate room. This reduces the accessibility of these devices from the public and unknown people.
- Mount the CCTV, smart card, biometric authentication to track and monitor unauthorized physical access to the server and backup devices.
- Use rack mount servers. This restricts attackers from stealing or damaging the servers.
- The server should be attached to an UPS so that it protects the server from file damage or corruption due to temporary power loss.
- Keep the devices in locked drawers, cabinets or rooms.
- Backup devices should be stored at off-site locations and ensure that they are secured.
- Do not encourage employees to take backup on CD, DVD, USB, or external hard disks. Ensure the backups are locked up at all times in a drawer, safe or separate room.
- Do not allow employees to leave an area carrying a backup device with them. Use motion sensing alarms to detect movement of any backup device.
- Implement full disk encryption on backup devices.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

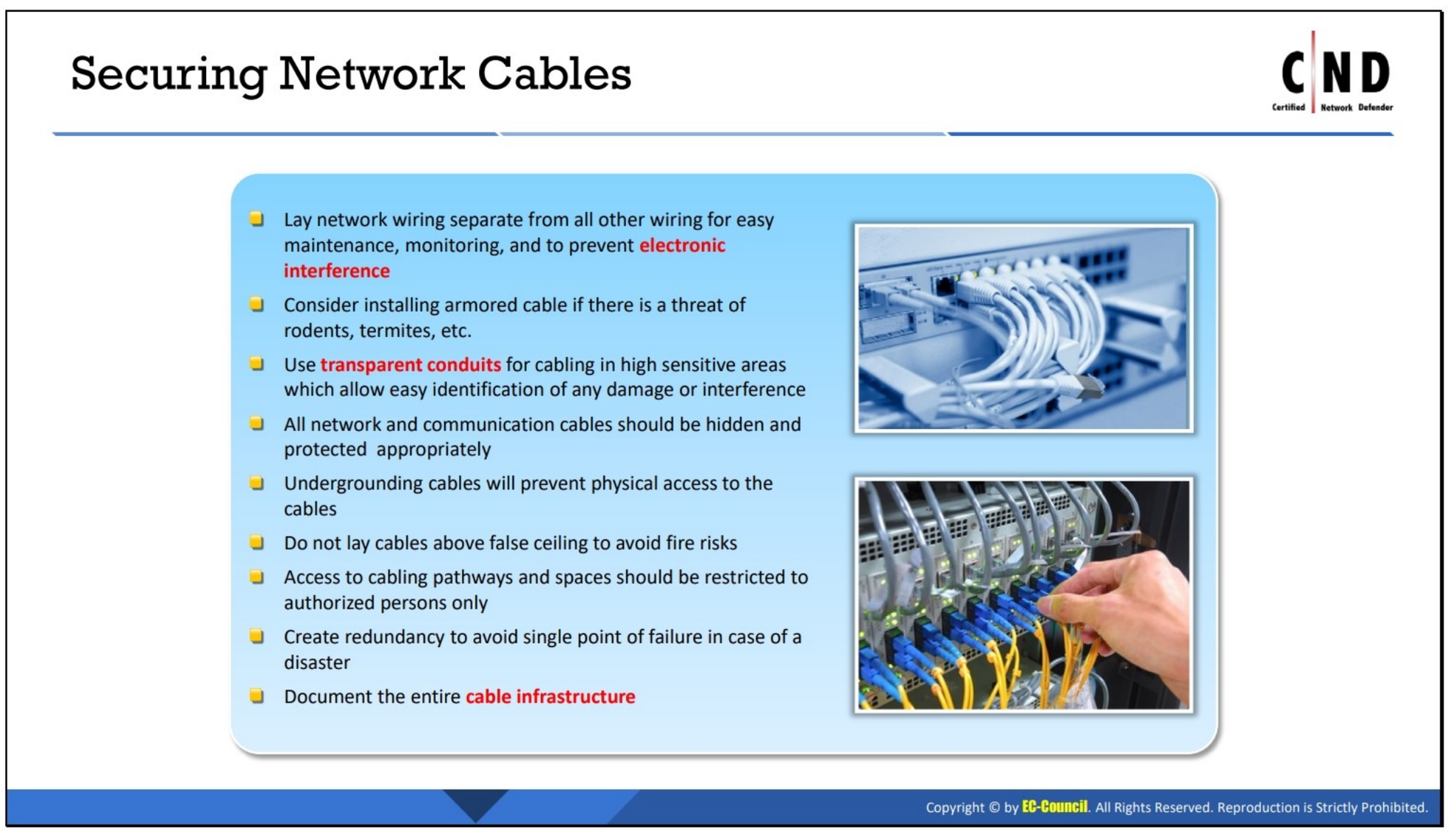


Critical Assets and Removable Devices

The organization should always pay attention to their server and backup storage device security. At the same time, they should not ignore the security of their other critical assets such as workstations, routers and switches, printers, other network equipment, removable devices, etc. The organization should employ all the physical security measures of server/backup devices to critical assets and removable devices.

- **Workstations**: Workstations at unoccupied desks, empty offices, receptionist's desk, etc. are more vulnerable to physical security breaches. Disconnect or remove such unoccupied workstations or otherwise lock the doors to the room where the workstation is located.
- **Routers and Switches**: Keep these critical network devices in a locked room.
- **Printers**: Like servers and workstations, printers can store important information, should be bolted down, and located in separate places.
- **Removable Devices**: Portable removable devices such as laptops, handheld computers, mobile devices, SD cards, USB, Bluetooth etc. can pose physical security risks. Keep these devices in a drawer, a safe or permanently attach a cable lock.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Securing Network Cables

Network cable security is often overlooked as an aspect of physical security. The organization should consider the importance of cable security before planning and installing any cabling. Network cabling should be nice and neat, if it is not an organization can suffer from unplanned downtime. With flawed or insecure network cabling, an attacker can easily access sensitive information by passing other security controls. Wiretapping, physical damage or thefts are the risks associated with network cabling.

Types of Cable used in Network Cabling

- **Unshielded Twisted Pair (UTP) Cable**:

  It reduces the crosstalk and interference between pairs of wires. UTP cable is prone to wiretapping. An attacker can easily tap the information flowing through network cables.

  - **Advantages**
    - Easy to install.
    - Suitable for domestic and office Ethernet connections.
  - **Disadvantages**
    - Easily susceptible to electromagnetic and radio frequency interference.
    - Less commonly used for long distance networking.

- **Shielded Twisted Pair (STP) Cable:**

  In STP cable, each pair of wires is individually shielded with foil. It is less susceptible to external interference as the shielding absorbs all the EMI and RFI signals.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Advantages**
  - Immune to crosstalk and interference.
  - Ensures secured data transmission.
- **Disadvantages**
  - More expensive than UTP.
  - More difficult to install than UTP.

- **Fiber Optic**:

  It is made up of made of glass or plastic. Fiber optic cabling is least susceptible to wiretapping threats.

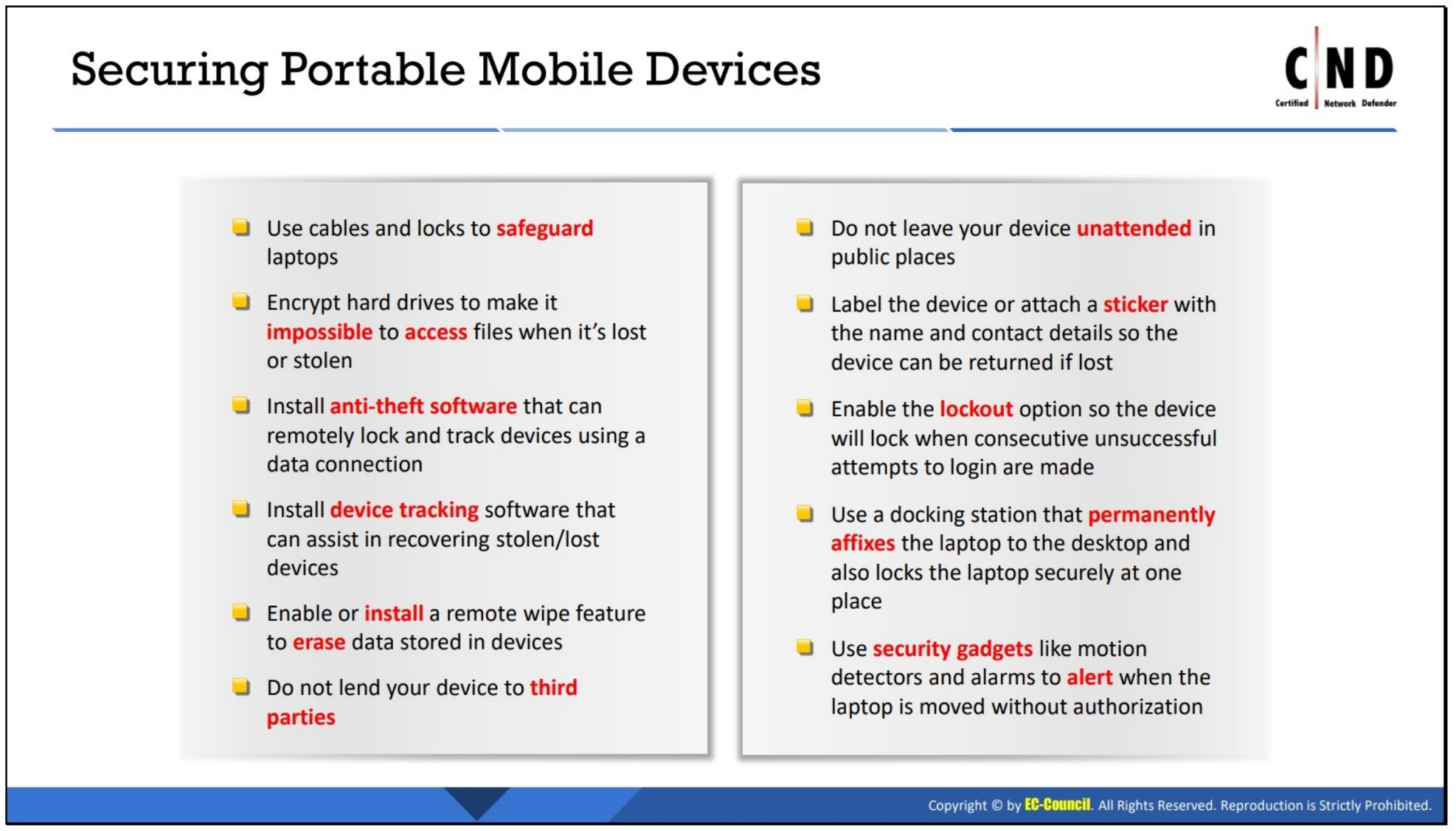
  - **Advantages**
    - Can carry information over greater distances.
    - Immunity to electromagnetic interference.
    - No crosstalk.
  - **Disadvantages**
    - Limited physical arc of cable.
    - Highly expensive.
    - Need optical transmitters and receivers.

- **Coaxial Cable:**

  Coaxial cable is made up of a single copper conductor at its center. A plastic layer provides an insulated center conductor and a braided metal shield. The metal shield prevents interference from fluorescent lights, motors, etc.

  - **Advantages**
    - Can carry information over greater distances.
    - Moisture resistant.
  - **Disadvantages**
    - It does not bend easily and is difficult to install.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

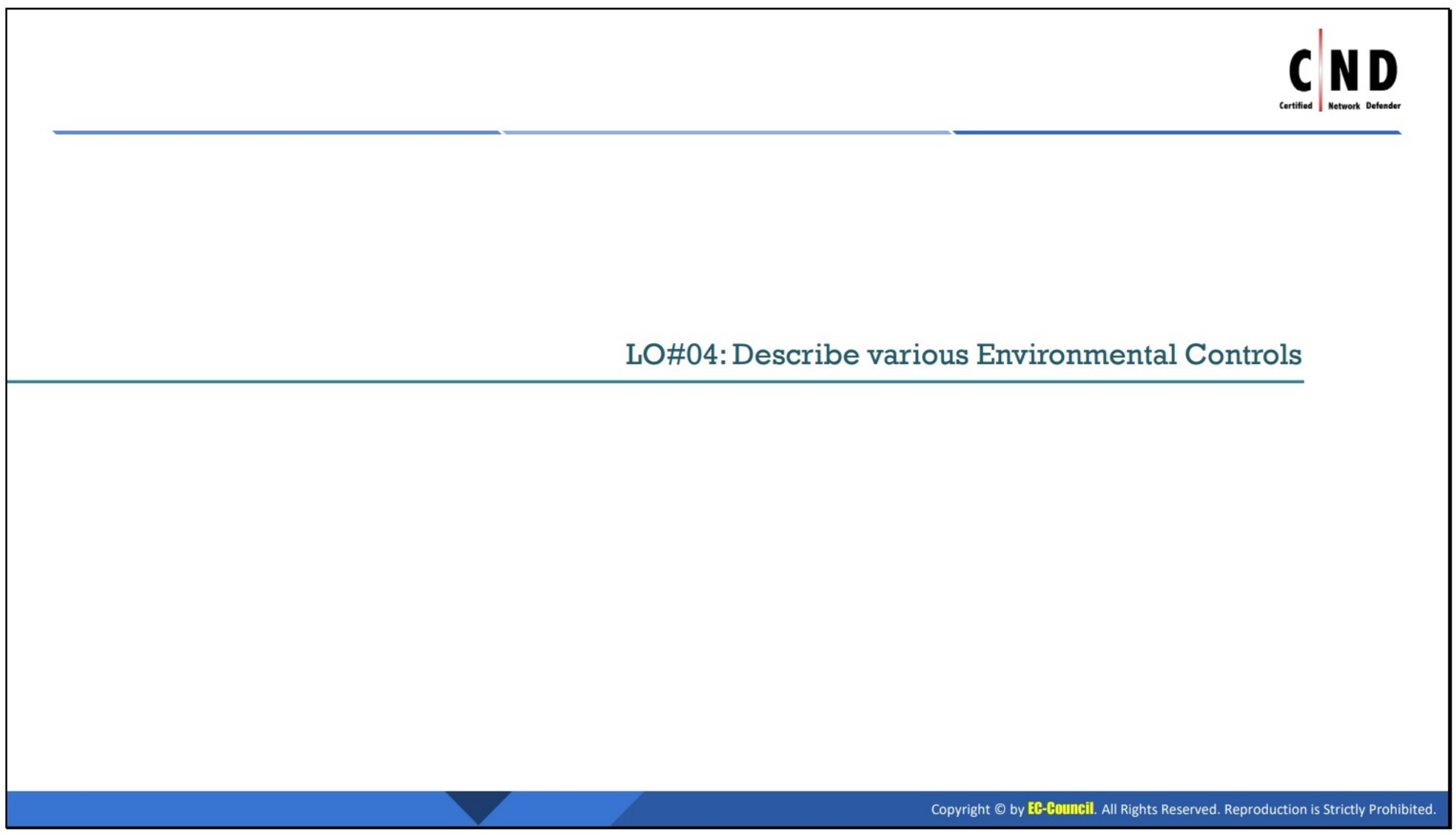


Securing Portable Mobile Devices

The use of portable mobile devices in an organization has risen over the past few years. The risk of physical security threats to these devices also has increased. These devices often are vulnerable to physical threats such as theft, loss, damage, resale, etc. The organization should take proper care to deal with any security incidents related to these devices.

- Apply all security measures common for these network devices such as servers, backup devices, portable devices, etc.
- Physically secure the mobile device location.
- Apply proper access control procedures for these devices.

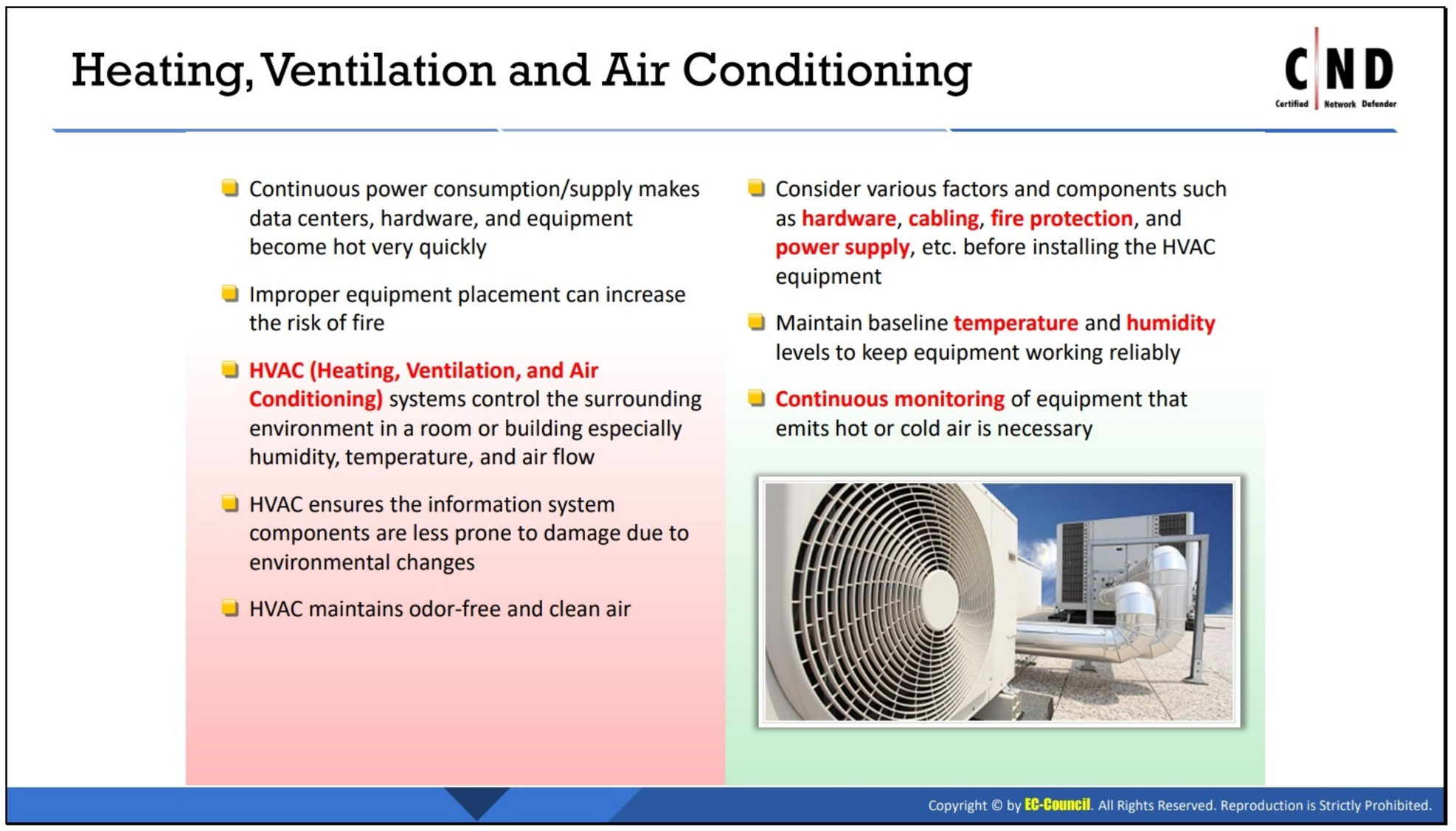
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#04: Environmental Controls

This section explains various environmental controls.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Heating, Ventilation and Air Conditioning

It is a special system that controls the surrounding environment in a room or building, especially the humidity conditions in the air and ventilation. It is deployed to maintain comfortable temperatures in a room so the hardware is not affected by the moisture and changes in the air. In these controlled conditions, the hardware and the components are also safer and less prone to damage from environmental factors. The HVAC also purifies the air in the room from smoke, odor, heat and dust particles. Having an environment where the air is odor free, clean and the humidity is under control provides a good atmosphere for the people working with that organization. These ventilation systems are desired mostly in medium to large scale organizations involving heavy equipment and a larger amount of staff. A pre-programmed sensing device is used to check for changes in the temperature and it acts accordingly. Manual controlling the HVAC also can be done.

A refrigeration component is added to a HVAC system, also known as HVAC&R or HVACR (heating, ventilating and air-conditioning & Refrigeration) system

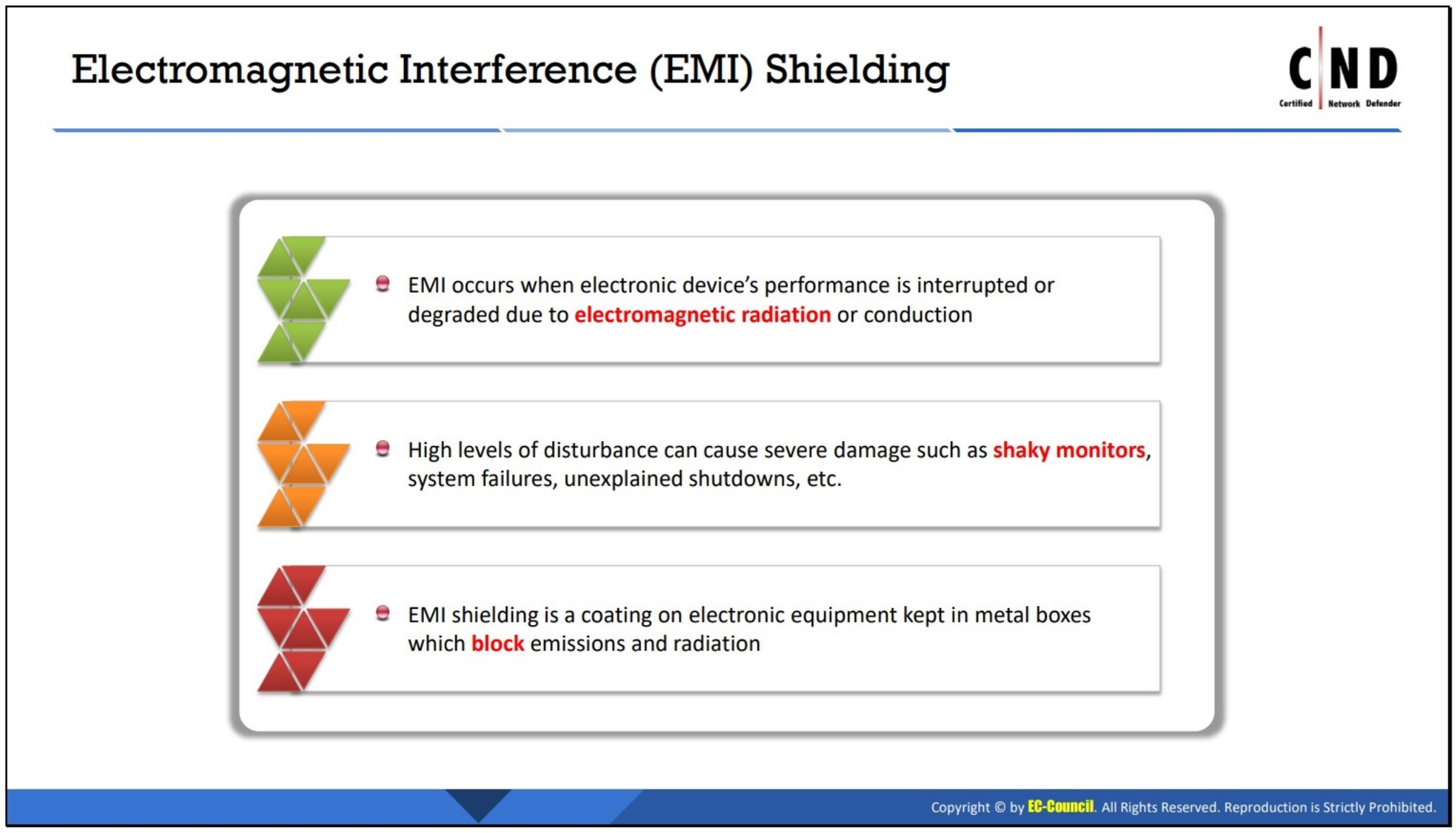
Types of HVAC Systems

- **Heating and Air-Conditioning Split System:** The most traditional and commonly used HVAC system. You may find the components of the system both inside and outside the building. HVAC split systems have:
  - An air conditioner in order to cool the refrigerant.
  - Furnaces, a fan or evaporator coil: Converting the refrigerant and circulates the air.
  - Duct: Allow air flow throughout the building.
  - Air quality fittings like air cleaners, air purifiers etc.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Hybrid Heat Split System:** This is an advanced version of a split system having better energy effectiveness. Here, the heat pump provides an electrically fueled HVAC instead of gas furnace heat. A typical hybrid heat split system includes:
  - Heat Pump: Cool/heat the refrigerant.
  - Furnaces/Evaporator Coil: Converts refrigerant and circulates the air.
  - Duct: Allow air flow throughout the building.
  - Control or Thermostat: An interface to control the system.
  - Air quality fittings like air cleaners, air purifiers etc.
- **Duct – Free Split Heating and Air Conditioning System:** Most commonly used in locations where the traditional split systems cannot be used. A typical duct-free split system includes:
  - An air conditioner in order to cool the refrigerant.
  - Fan Coil: Converts the refrigerant and circulates the air.
  - Refrigerant tubing and wires: Connects outdoor unit to the fan coil.
  - Control or Thermostat: An interface to control the system.
  - Air quality fittings like air cleaners, air purifiers etc.
- **Packaged Heating and Air-Conditioning System:** Most appropriate air conditioning system used mainly in locations where the space required for fixing all the components of a split system is available. Packaged units can be used in spaces that range from an entire building to one room units. Packaged heating and air-conditioning system includes:
  - Packaged Products: A heat pump or an air conditioner combined with a fan coil or an evaporator coil in a single unit.
  - Control or Thermostat: An interface to control the system.
  - Air quality fittings like air cleaners, air purifiers etc.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



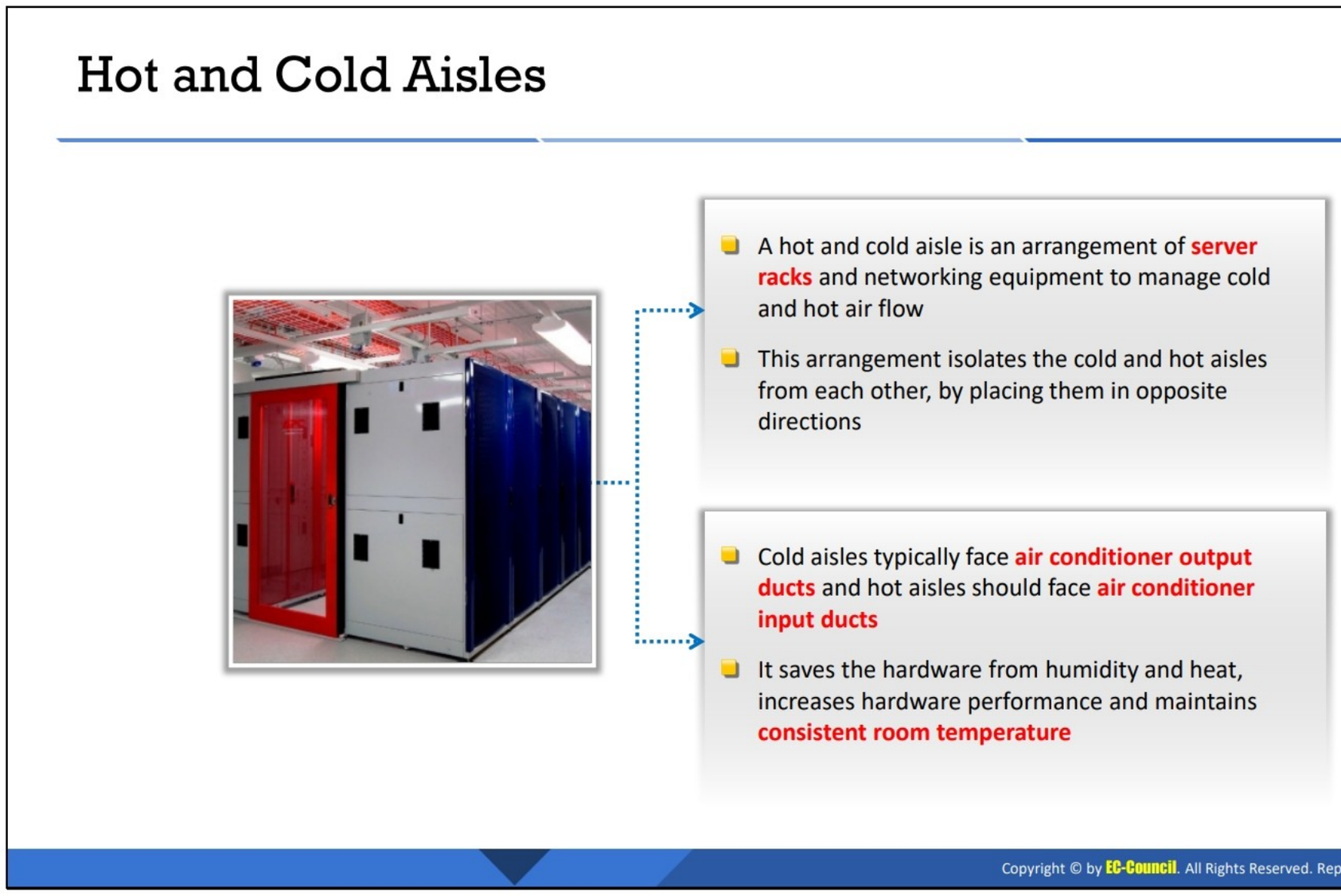
Electromagnetic Interference (EMI) Shielding

Electromagnetic radiation emitted from different electronic devices interferes with surrounding devices and causes a problem with their functions. EMI shielding is the practice of coating the electronic equipment with metals so the electromagnetic waves do not interfere with other devices or block the field with certain materials. EMI shields separate one part of the equipment from another.

Shielding uses materials such as metals or metal foams. An electric field produces a charge on the conducting material applying an electromagnetic field on a conductor. The conductor produces another charge which cancels the effect of the externally applied electric charge on it. This causes no change in the conducting material. When the electric field is applied to the material, it produces eddy currents (currents that flow within a material in closed loops). These currents cancel the effect of the magnetic field. In this way the shielded material has no outside effects or disturbances on it.

As organizations use heavy equipment, electronic hardware interference will become a problem and EMI shielding will be needed for all devices in these types of environments. Many industries, such as telecommunication, hospitals, etc. prefers to use EMI shielding.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hot and Cold Aisles

It is a systematic arrangement of equipment to maintain air flow and to save energy. Many organizations follow hot and cold aisle alignment, mostly used in server rooms, data centers, etc. where heavy electronic equipment comes into use.

In the rack of heavy equipment or servers they are arranged so the front of them faces the cold air coming from the air conditioners. The backs of the equipment face the back of the next rack of equipment. This goes on for all the equipment in the room. This arrangement pushes the hot air coming from the back of the equipment to one end of the room. The cooling conditions are kept so that the hot air coming out of the equipment is sucked out and does not mix with the cool air inside the room. Place the cooling system below the room or above the room depending on the convenience.

Cold Aisle: Advantages and Disadvantages

- **Advantages:**
  - Easy to implement as it does not require any supplementary architecture to give out air.
  - Requires doors only at the end.
  - Less expensive.
  - Can easily fit into an existing data center with issues like power, network distribution etc.
  - Can be used with a raised floor supply space.
  - Controls the air supply to match with the severe airflow.
- **Disadvantages:**

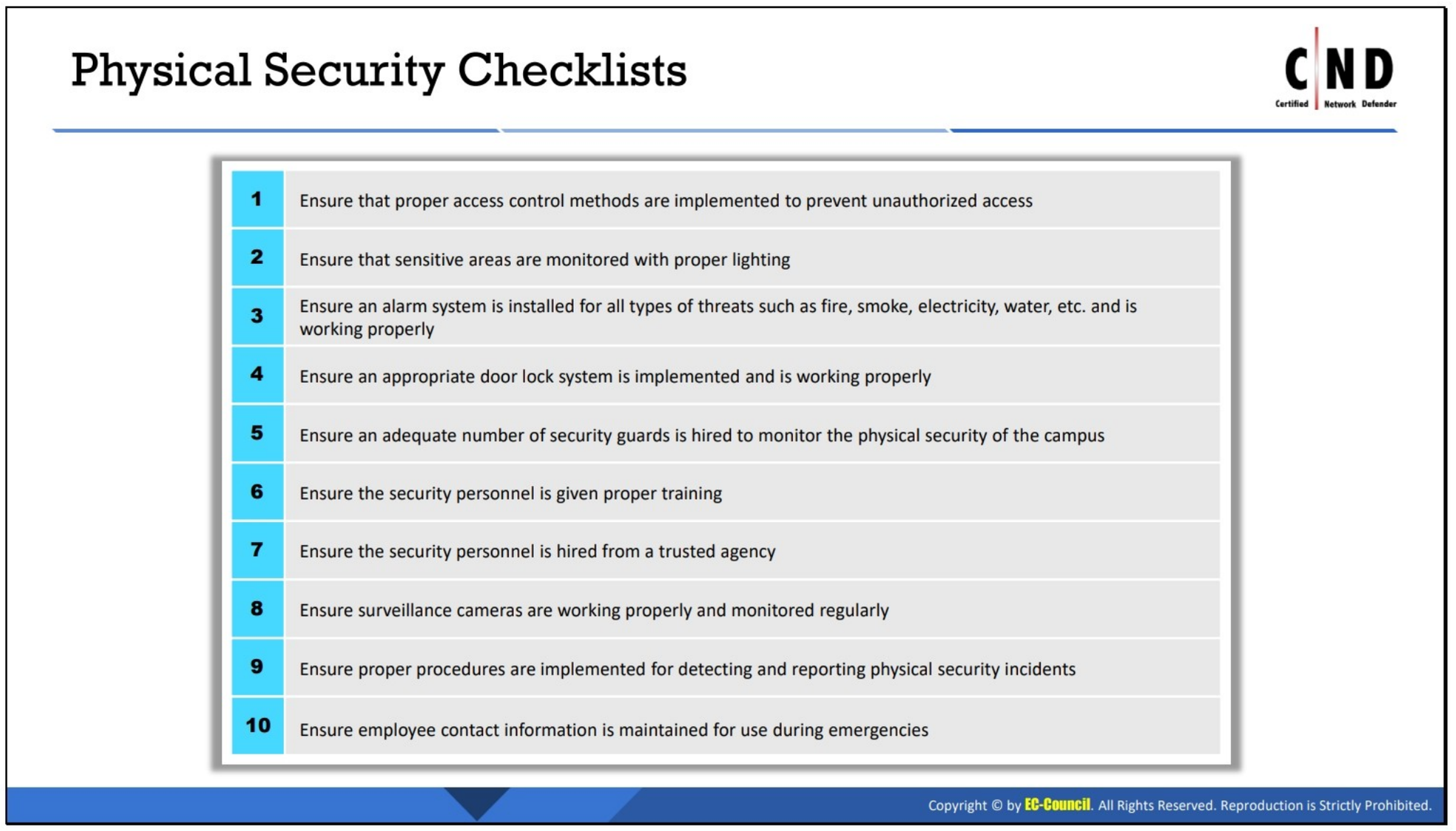
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Creates operational issues, if low-density storage or communication racks are installed in the data center space.
- Most of the cold aisles have ceilings immediately above the aisle affecting fire and lighting design.
- Air leaked from the raised floors and openings under the equipment enters the air paths to the cooling units. This affects the efficiency of the system.

Hot Aisle: Advantages and Disadvantages

- **Advantages:**
  - Leakage from the raised floor openings are passed over to the cold space.
  - More effective.
  - Works well in a slab environment by supplying an adequate volume of air and covering the exhaust air.
  - Provides cooling to general data center space.
  - Perfect distribution of air throughout the space.
- **Disadvantages:**
  - Always requires an additional space for the flow of air from the hot aisle to the cooling unit.
  - Very expensive.
  - Hot aisles it uncomfortable for technicians during maintenance work.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Physical Security Checklists

Physical security can be built in layers, or follow a Defense-in-Depth strategy to implement physical security for the organization. The organization should consider implementing all the physical security controls and measures to ensure a Defense-in-Depth physical security for their organization.

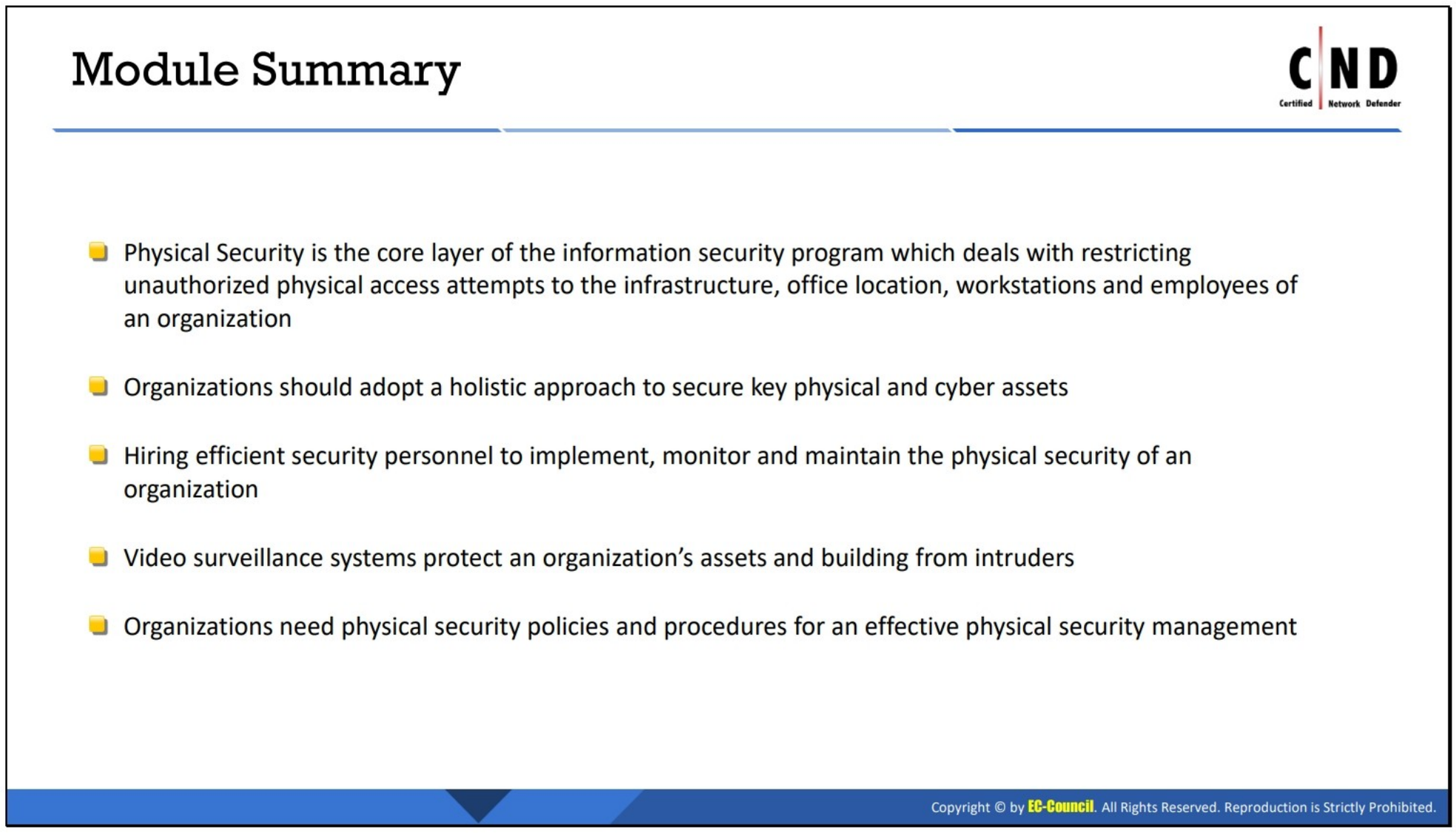
The following checklist will help an organization ensure they are implementing proper security controls and measures:

- **Follow copyright rules and licensing restrictions:** The organization should enforce copyright rules and licensing restrictions in order to prevent outsiders or insiders from creating illegal copyrighted copies of the software.
- **Store all removable and important items in the locker when not in use:** Employees should ensure to lock all sensitive information and important devices in a locker. Do not leave any important information unattended as it may catch the eye of an attacker.
- **Keep the sensitive areas under surveillance:** The organization should ensure security for sensitive areas like server rooms, etc. CCTV surveillance and guards may be enforced in order to maintain security in the sensitive areas. The organization should enforce 24x7 surveillance for the sensitive areas.
- **Always advise employees to swipe the card at the entrance:** Swiping ID cards at the entrance helps the organization to audit the login details of the employees in case of an incident.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Do not keep any combustible material in the workplace area:** Always keep any sort of combustible materials away from the workplace area. This ensures the safety of the employees, the information stored and the devices stored inside the workplace area.
- **Always ensure company satisfaction:** Employ security measures that guarantee satisfaction of the employees. The policies and procedures imposed by the organization should ensure compatibility with the company infrastructure. Physical security measures imposed should detect, report, correct and prevent attacks.
- **Evaluate the physical security of the location:** Proper security ensures the security of the employees and the information in the organization. Preventing attackers from entering the workstations and server rooms, authenticating each person using ID cards or biometric ensures better security of the location. Other security measures include ensuring locking cabinets, doors and windows, proper surveillance using CCTV, proper lighting etc.
- **Do not disconnect consoles from ports:** Disconnecting cables or consoles from ports will lead to a disconnection for the user. You should make sure the cables are all connected to the ports and are working properly.
- **Use of alarms and sensors during fire, smoke etc.:** The organization should ensure proper use of sensors and alarms in order to detect fire or smoke on the premises. An organization may include sensors for devices in order to detect if anyone tries to take those devices out of the organization.
- **Prevent damage to hardware and software:** Any damage to the hardware or software results in damage of the information systems in the organization. Damage to the hardware will lead to the damage of the electronic and mechanical systems used in data processing. Damage to software leads to the damage in the programs and instructions used for data development.
- **Do not leave any devices or important data in the parking areas or cars:** Any unattended devices or data may attract attackers and may lead to the loss of these valuable items or information. The organization should employ an adequate number of security guards to monitor all parked cars. Proper lighting must be installed to watch these areas clearly. Employ security cameras in sensitive areas and log the who is accessing those areas.
- **Avoid storing confidential information on mobile devices:** Storing sensitive information in a mobile device is not recommended as it is easy to manipulate the data stored in a mobile phone. Attackers may gain access to your mobile devices and then acquire all of its sensitive information.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

In this module, we have discussed the importance of physical security, and its role in the organization's information security program. This module introduced you to the various physical security controls and security measures that organizations should consider while implementing physical security. It will help the organization implement their Defense-in-Depth strategy for physical security.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.

EC-Council

Building A Culture Of Security

C|ND

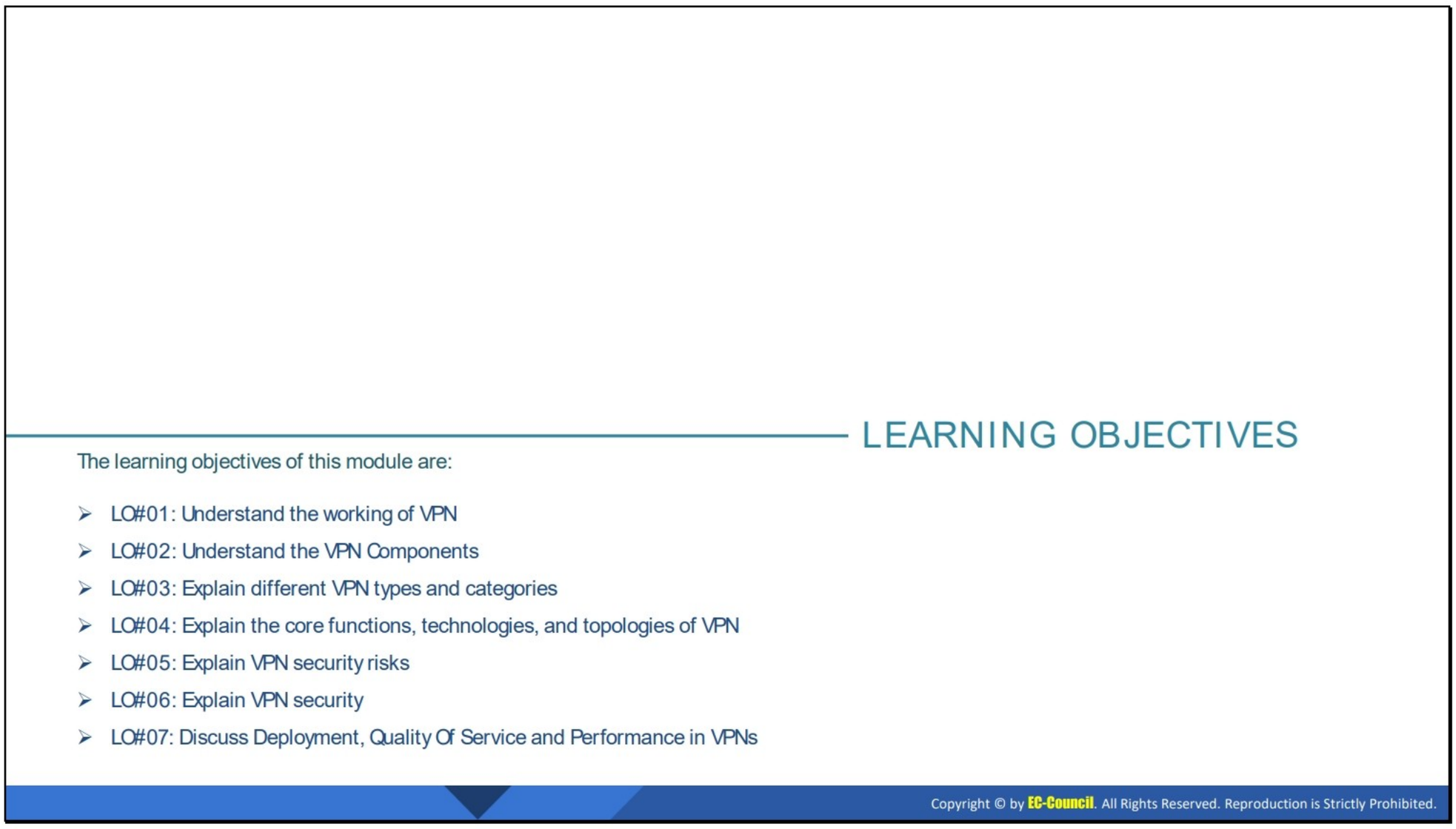
Certified Network Defender

Certified Network Defender v3

APPENDIX C
VIRTUAL PRIVATE NETWORK (VPN) SECURITY

EC-Council Official Curricula

This page is intentionally left blank.

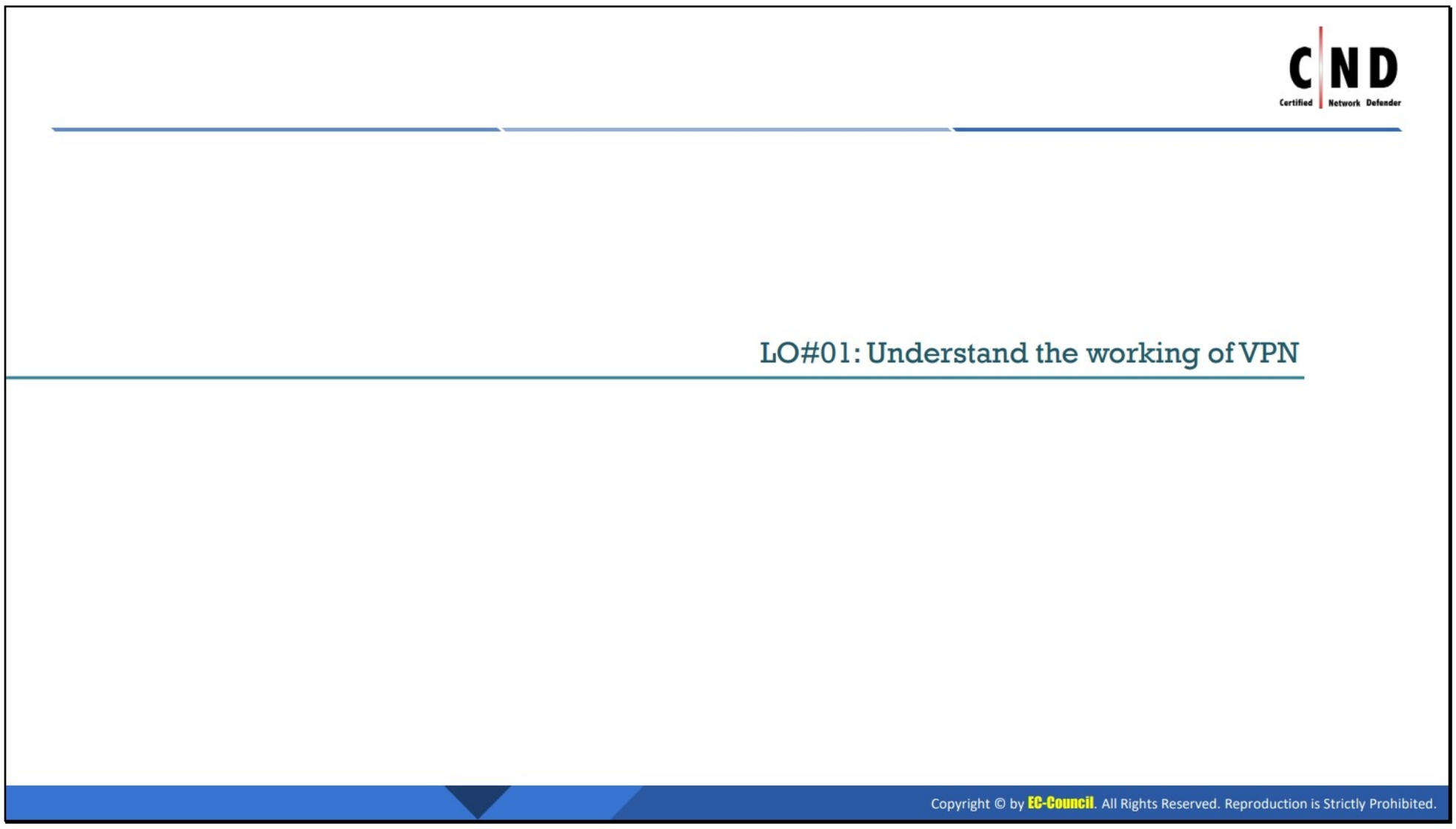


Learning Objectives

The learning objectives of this module are:

- Understand the working of VPN
- Understand the VPN Components
- Explain different VPN types and categories
- Explain the core functions, technologies, and topologies of VPN
- Explain VPN security risks
- Explain VPN security
- Discuss Deployment, Quality Of Service and Performance in VPNs

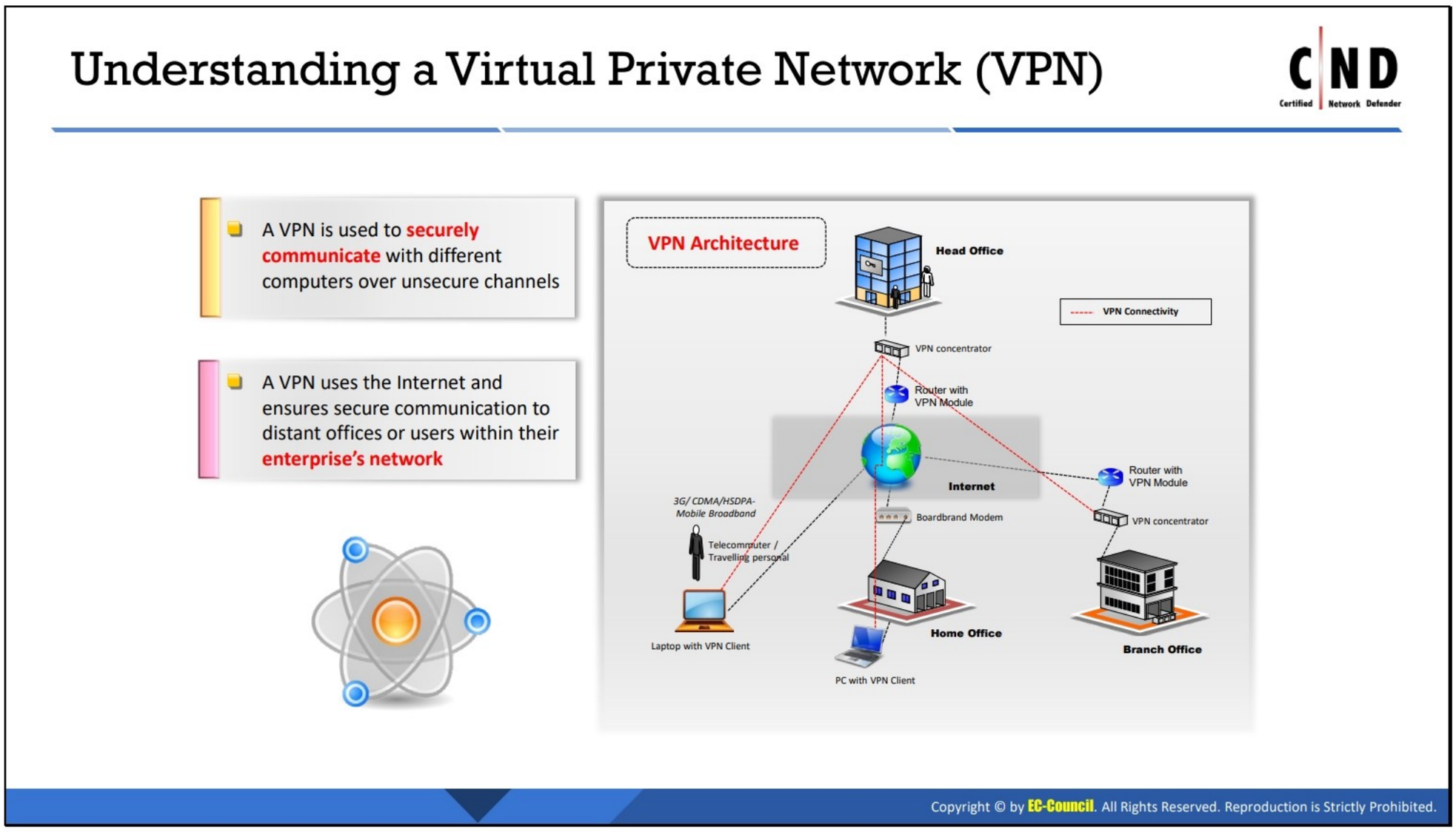
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#01: Working of VPN

This section explains fundamental concepts about VPN.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understanding a Virtual Private Network (VPN)

Most of the organization has its offices located at different locations around the world. There is a need for establishing a remote connection between these offices as a result. Previously, remote access was established through leased lines with the help of dial-up telephone links such as ISDN, DSL, cable modem, satellite, and mobile broadband. However, establishing remote connections with these leased lines is quite expensive and the costs rise when the distance between the offices increases.

To overcome the drawback of traditional remote access technologies, organizations are adopting Virtual Private Networks (VPNs) to provide remote access to their employees and distant offices.

A virtual private network (VPN) offers an attractive solution for network defenders to connect their organization's network securely over the Internet. VPN is used to connect distant offices or individual users to their organization's network over a secure channel.

VPN uses a tunneling process to transport encrypted data over the internet. IPSec is the common protocol used in VPN at the IP level. VPN ensures the data integrity check by using a message digest and ensures data transmission is not tampered with. VPN guarantees the quality of service (QoS) through service level agreements (SLA's) with the service provider.

- **Typical features of VPN**:
  - Establishes a connection between the remote system and a LAN across an intermediary network such as the Internet.
  - VPNs allow cheap long-distance connections over the Internet since both endpoints require a local Internet link which serves as a free long-distance carrier.
  - VPN uses tunneling or encapsulation protocols.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- VPNs use encryption to provide a secure connection to a remote network over the Internet and protect your communication.
- They provide virtual access to the physical network as if you are physically located in the office.

- **Advantages of VPNs:**
  - VPNs are inexpensive.
  - They provide a framework for corporate intranets and extranets.
  - Ensures secured transfer of data.
  - VPN allows you to access both web applications and websites in complete anonymity.
- **Disadvantages of VPNs:**
  - Designing and implementing the VPN is a complex issue, it requires experts for configuring.
  - Reliability depends on the service provider that you choose.
- **VPN Architecture:**

  A certain set of protocols and standards need to be followed while establishing a VPN architecture. Network defenders should decide the scope, implementation, and deployment of the VPN along with continuous network monitoring in order to ensure the security of a VPN. They should be continuously aware of the overall architecture and scope of the VPN.
- **Protocols used in deploying a VPN:**

  For deploying virtual private networks, there are two primary options IPsec and SSL. Each protocol has its own unique advantages and utilized depending on the requirement of the user or the organization's IT processes.
- **IPsec VPN:**

  IPsec-based VPN is the most commonly used deployment solution by most of the organizations. It is a set of protocols and standards developed by the internet engineering task force (IETF) for secure communication on the IP layer. It ensures the security of each packet in communication by encrypting and authenticating them. IPsec connections are established using VPN client software which is pre-installed and it mainly focuses on the company managed desktops.
  - **Advantages:**
    - IPsec VPNs can support all IP-based applications to an IPsec VPN product.
    - It offers tremendous versatility and customizability through the modification of the VPN client software.
    - Organizations can control the VPN client functions by using the APIs in IPsec client software.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Ensures secure exchange of IP packets between remote networks or hosts and an IPsec gateway located at the edge of your private network.

The three basic applications when using IPsec VPN's (associated with business requirements) are:

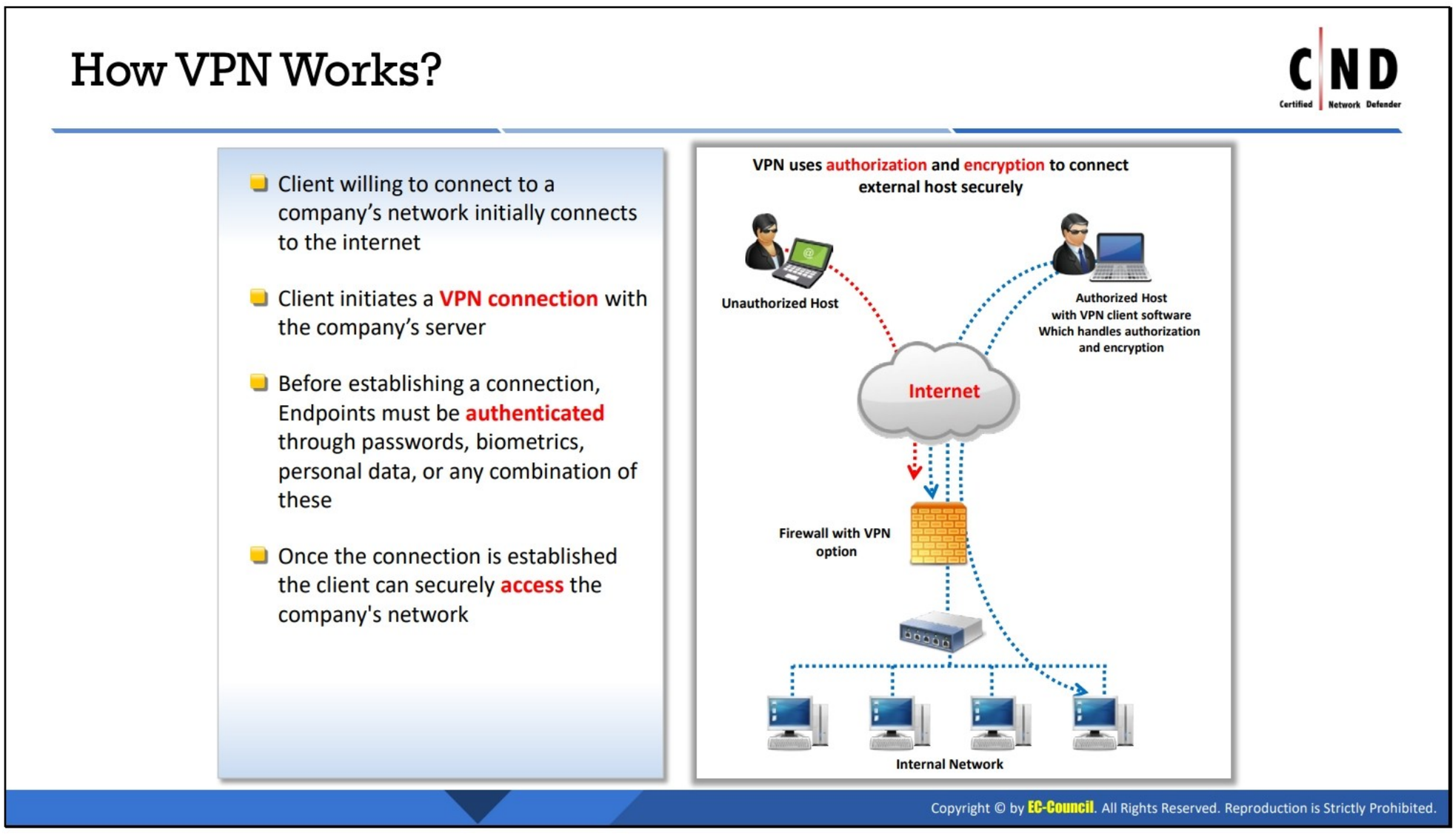
- **Remote-Access VPNs:** These allow individual users, such as telecommuters, to connect to a corporate network. This application creates an L2TP/PPTP session. IPSec encryption protects this L2TP/PPTP session.
- **Intranet VPNs:** This helps connect branch offices to the corporate headquarters, creating a transparent Intranet.
- **Extranet VPNs:** This allows companies to connect with their business partners (for example, suppliers, customers, and joint ventures).

- **SSL VPN (web-based):**

SSL-based VPNs provide remote-access connectivity using a Web browser and its native SSL encryption irrespective of the location. SSL doesn't require any special client software to be pre-installed and is capable of any type of connectivity. The connectivity ranges from company-managed desktops and non-company-managed desktops, such as employee-owned PCs, contractors or business partner desktops. It helps in reducing desktop software maintenance as it downloads the software dynamically whenever there is a need.

- **Advantages:**
  - It offers additional features like easy connectivity from non-company-managed desktops, little or no desktop software maintenance.
  - It provides accessibility to the SSL library and access to port 443 TCP.
  - It will work wherever someone can gain access to HTTPS websites such as Internet Banking, Secure Webmail, or Intranet sites.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



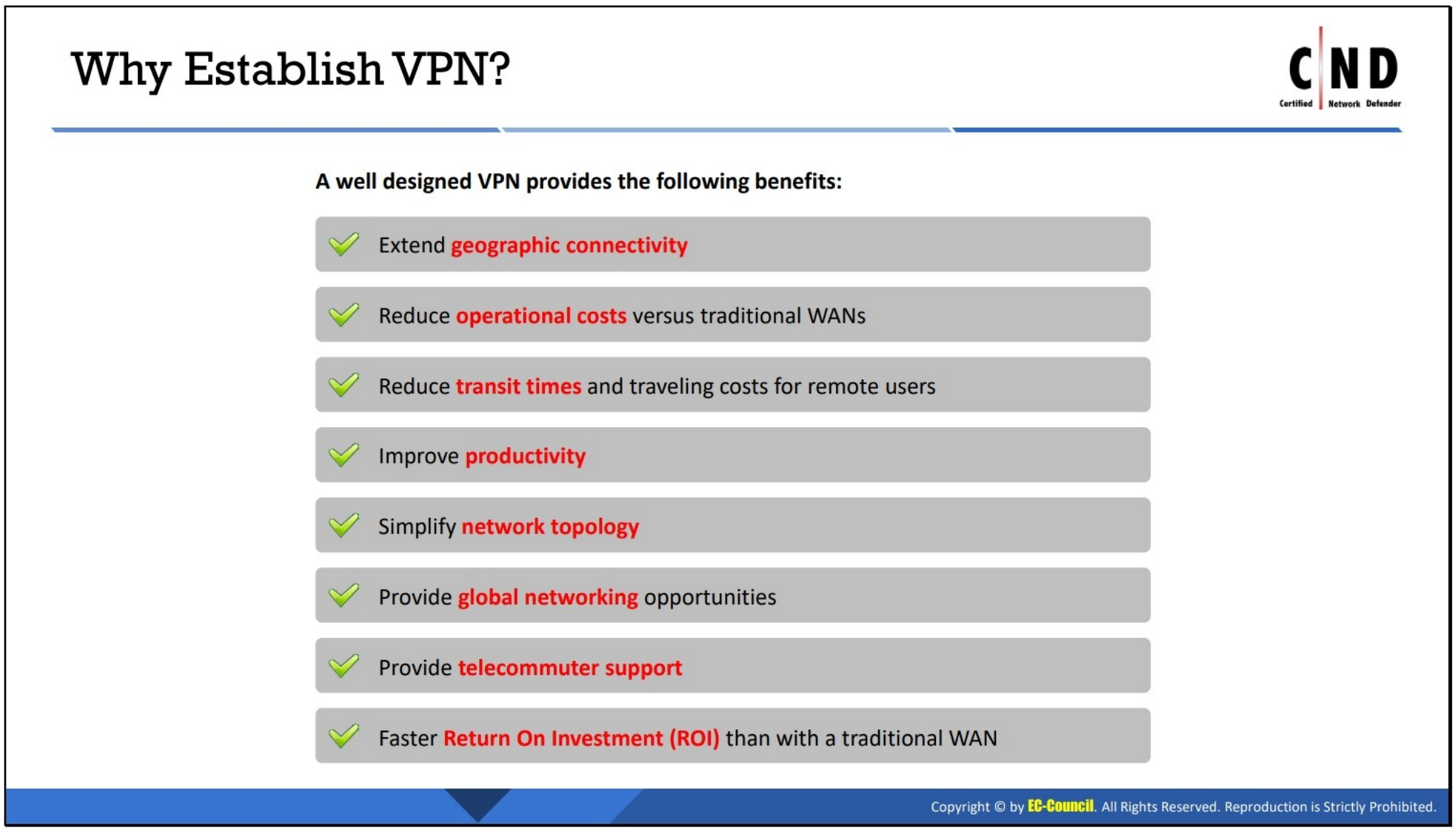
How VPN Works?

A VPN enables a secured connection over the Internet from a public network to a private network placed at a far-off site. All the network traffic in a VPN is encrypted and passes through a virtual secure tunnel, placed between the client and the VPN server.

All the packets passing through a VPN is encrypted or decrypted with respect to inbound or outbound traffic. The packets are encrypted at the client-side and the packets are decrypted at the VPN server. For example, when a client with a VPN connection enabled, browses Youtube.com. This outbound traffic is encrypted at the client-side. The encrypted data is then sent to the nearest VPN server and passes it to the gateway server. Here, the data is decrypted and sent to the server hosting Youtube.com. When Youtube.com sends a reply request, the VPN server performs the reverse process on the outbound traffic.

A VPN keeps a close look on any insecure networks. It creates a new IP address for the encrypted packet concealing the real IP address which disables attackers from finding the real IP address of the packets sent.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Why Establish VPN?

The easy accessibility of sensitive data over the Internet poses a serious security threat to organizations. Attackers easily exploit and gain access to sensitive information if it traverses on an unsecured public network such as the Internet. A VPN ensures reliable communication through an encrypted tunnel, preventing attackers from gaining access to organization information. A well designed and implemented VPN can provide the following benefits:

- Enables a secured connection across multiple geographical locations.
- It saves time and expenditure for employees as it allows the sharing of information between a corporate office and its regional office.
- Enhances the level of output for remote users.
- Improves the security of data by concealing the IP address from attackers.
- Handles multiple connections simultaneously and provides the same quality of service for each connection.
- Ability to provide a secure connection to larger enterprises.
- Implementation of a VPN increases the bandwidth and efficiency of the network.
- Less maintenance cost.

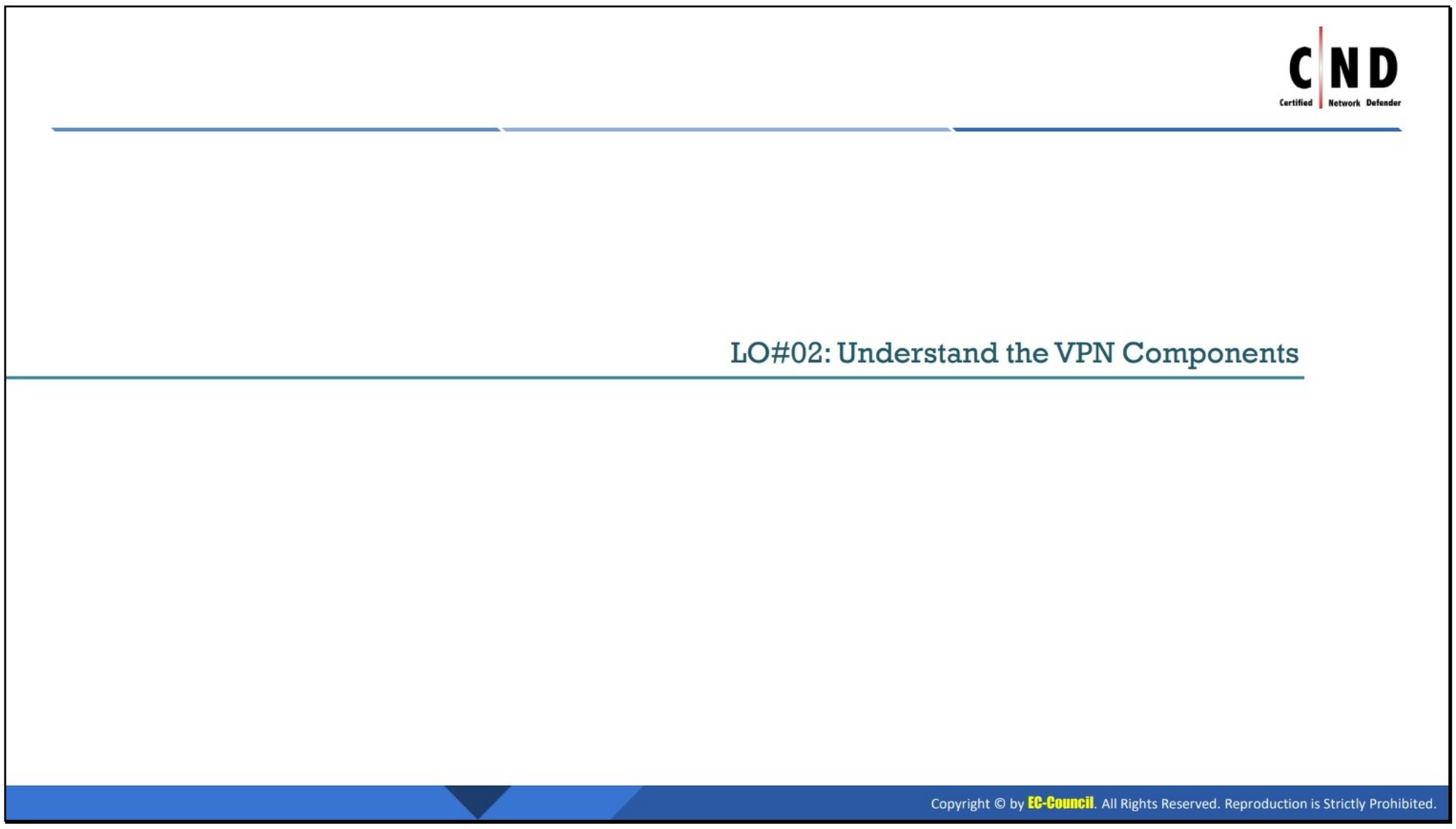
This encrypted traffic proves beneficial when the user connects its system to Wi-Fi hotspots in public places. The encryption makes it difficult for eavesdroppers in the network to identify the encrypted data.

A VPN allows users to access the servers across the world making it easy for them to access all types of content. Users do not have to face restrictions like geo-blocking while browsing. A VPN

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

allows the user to stay anonymous without sharing their device information in the network. By hiding this data, a VPN restricts websites from spying or monitoring the user. To avoid excessive monitoring from third party websites or attackers, users should install a VPN for safe browsing.

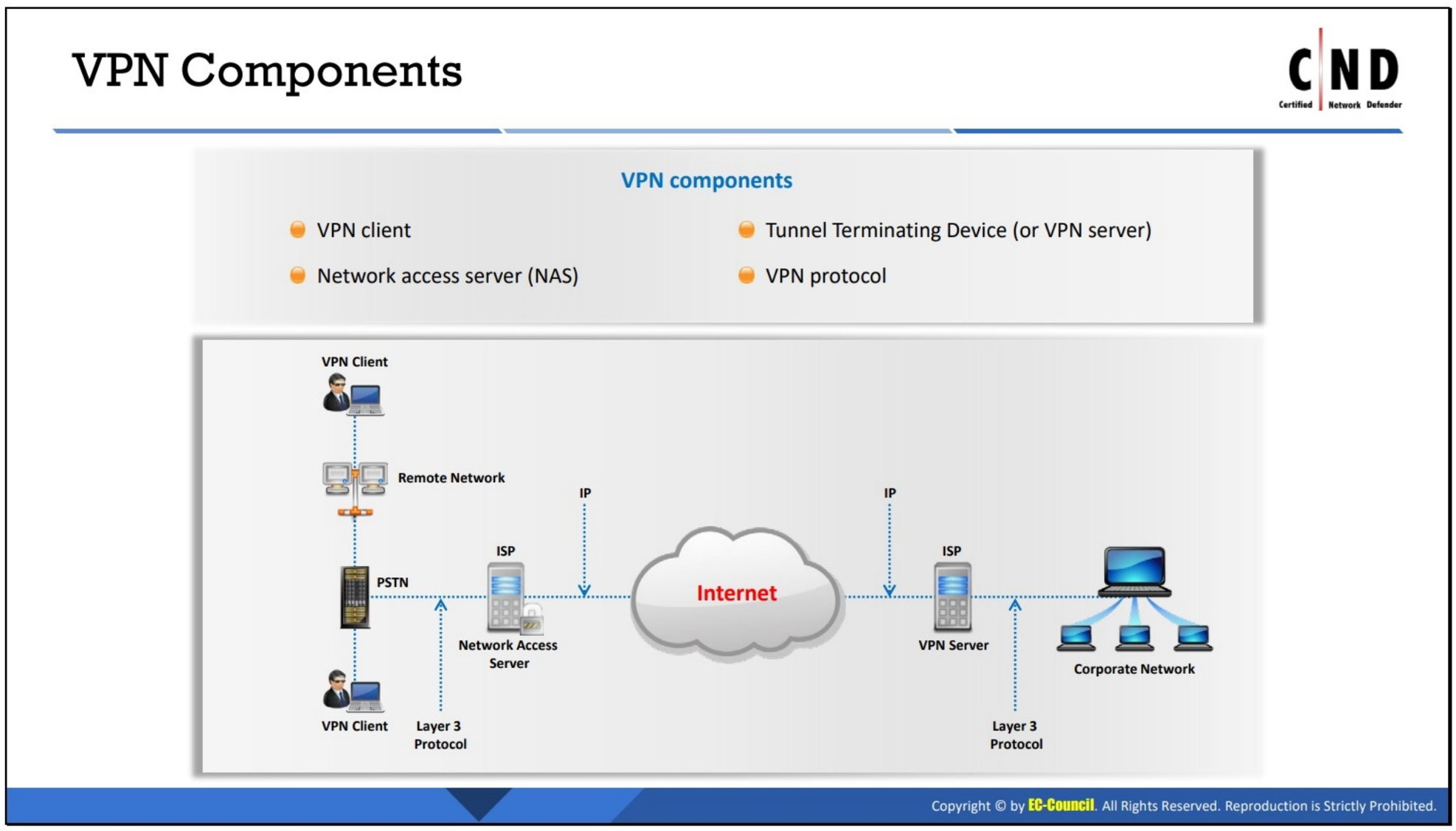
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#02: VPN Components

This section explains various components of a VPN.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



VPN Components

The VPN architecture consists of four main components:

- VPN client: A computer that initiates a secure remote connection to a VPN server.
- Network access server (NAS): It is also called a media gateway or a remote-access server (RAS). It is responsible for setting up and maintaining each tunnel in a remote-access VPN. Users need to connect to the NAS to use a VPN.
- Tunnel terminating device (or VPN server): A computer that accepts VPN connections from VPN clients.
- VPN protocol: It includes VPN specific protocols used to manage tunnels and encapsulate private data. It includes the use of PPTP and L2TP protocols along with IPsec.

The following diagram shows the use of various VPN components in a remote access VPN:

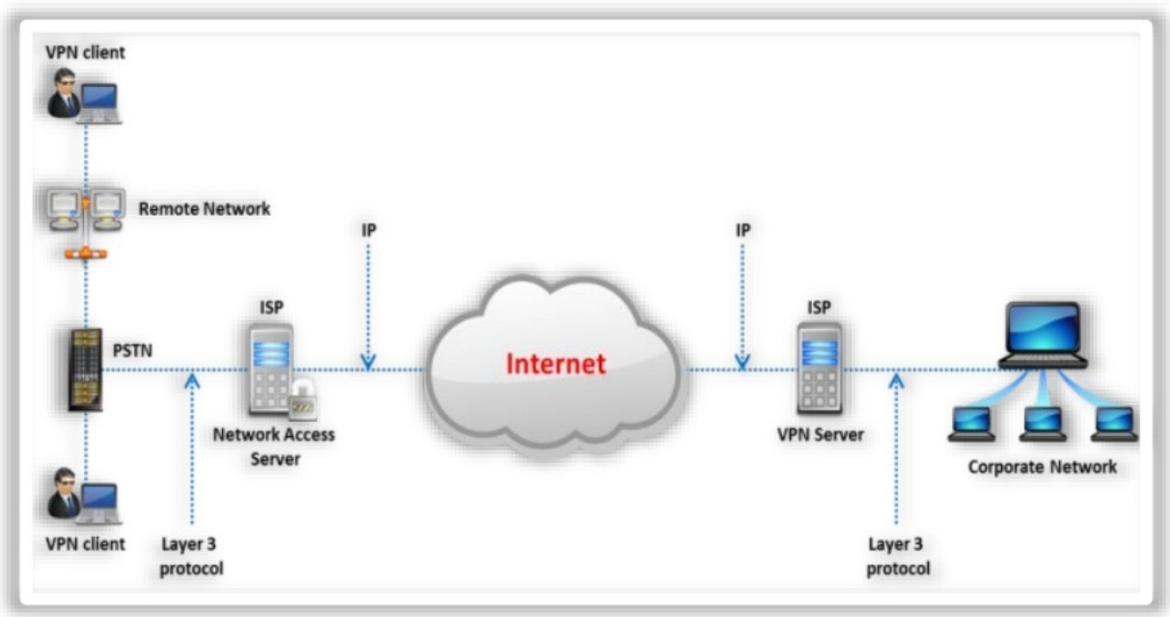


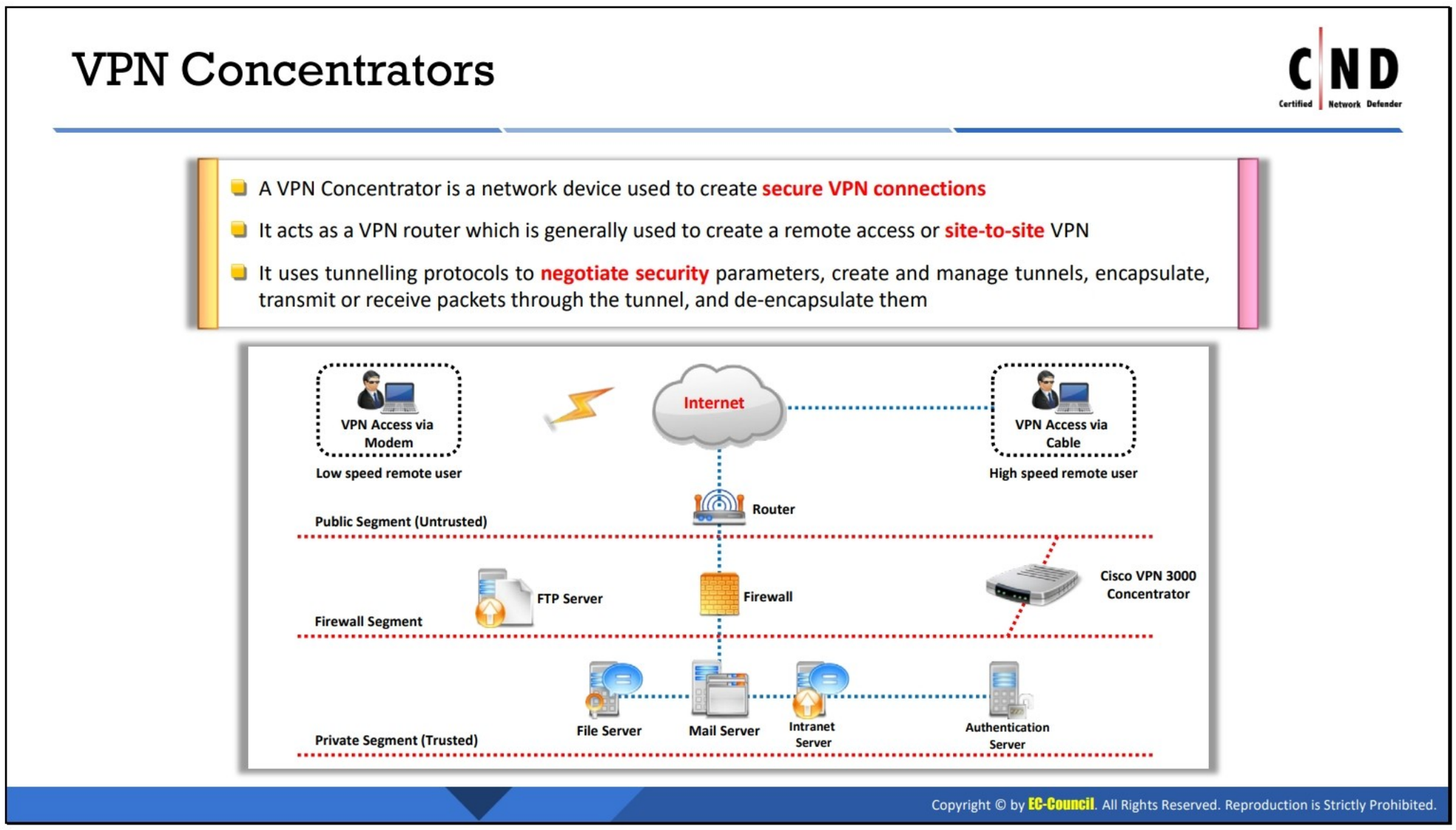
Figure C.1: VPN components in a remote access VPN

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

A typical remote access VPN connection is established as follows:

- The remote user propagates a PPP connection with an ISP's NAS through a PSTN.
- The packets sent by the user are sent to the tunnel connecting NAS and VPN server after authenticating the user.
- The packet is encrypted before placing it in the tunnel.
- The location of the VPN server depends on the model used for the VPN implementation.
- The VPN server accepts the packet from the tunnel, decrypt, and sends it to the final destination.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



VPN Concentrators

VPN concentrators normally enhance the security of the connections made through a VPN. These are generally used when a single device needs to handle a large number of VPN tunnels. They are best used for developing a remote-access VPN and site-to-site VPN.

VPN concentrators implement the security of the tunnels using tunneling protocols. These protocols manage the following:

- Manage the flow of packets through the tunnel.
- Encryption and decryption of packets.
- Manage the creation of tunnels.

A VPN concentrator works in two ways:

- Receives plain packets at one end, encrypts at the other end, and forwards the packet to the final destination.
- Receives encrypted packets at one end, decrypts at the other end, and forwards the packet to the final destination.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

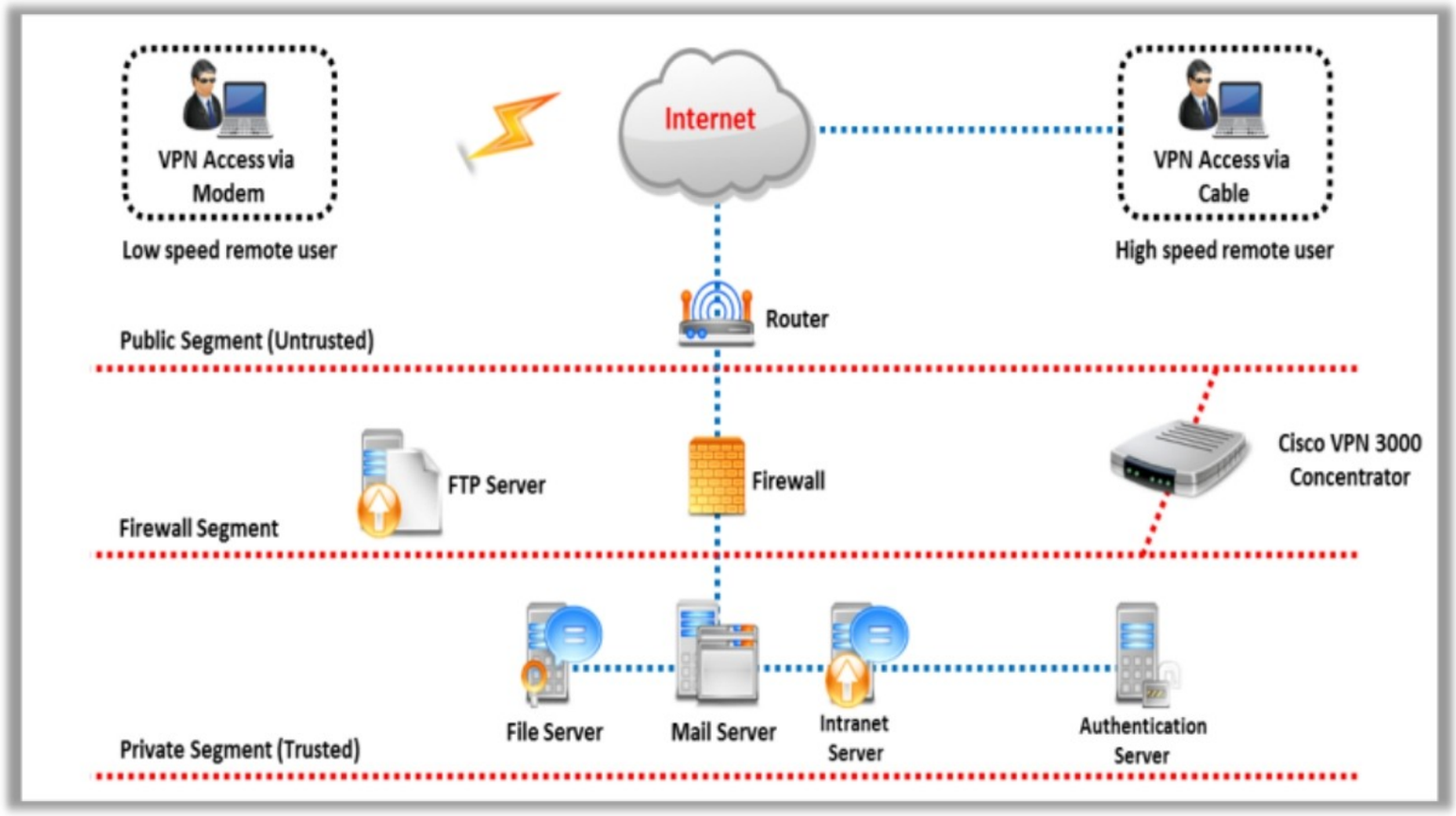
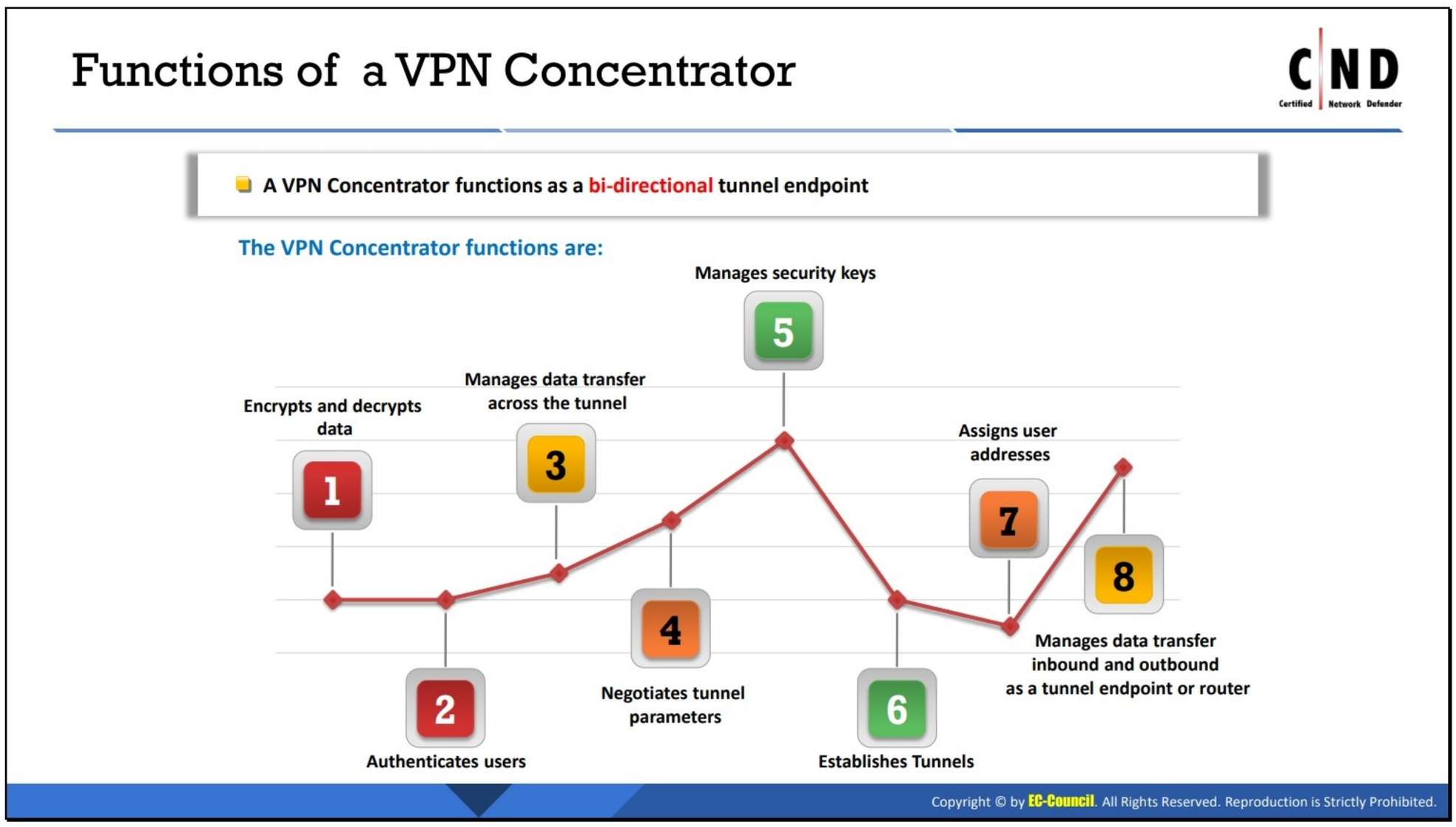


Figure C.2: VPN concentrator

In the figure, the VPN concentrator is placed in parallel with the firewall supporting remote users who have both a slow and fast Internet speed. If the VPN is placed behind the firewall, the implementation requires additional configuration changes and is vendor dependent.

VPN concentrators provide a high level of security for SSL and IPsec VPN architecture. A normal VPN tunnel requires IPsec to be implemented on the network layer of the OSI model. A major benefit of using a VPN concentrator is that the client is considered to be present outside the network and can access the network as if it is connected.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

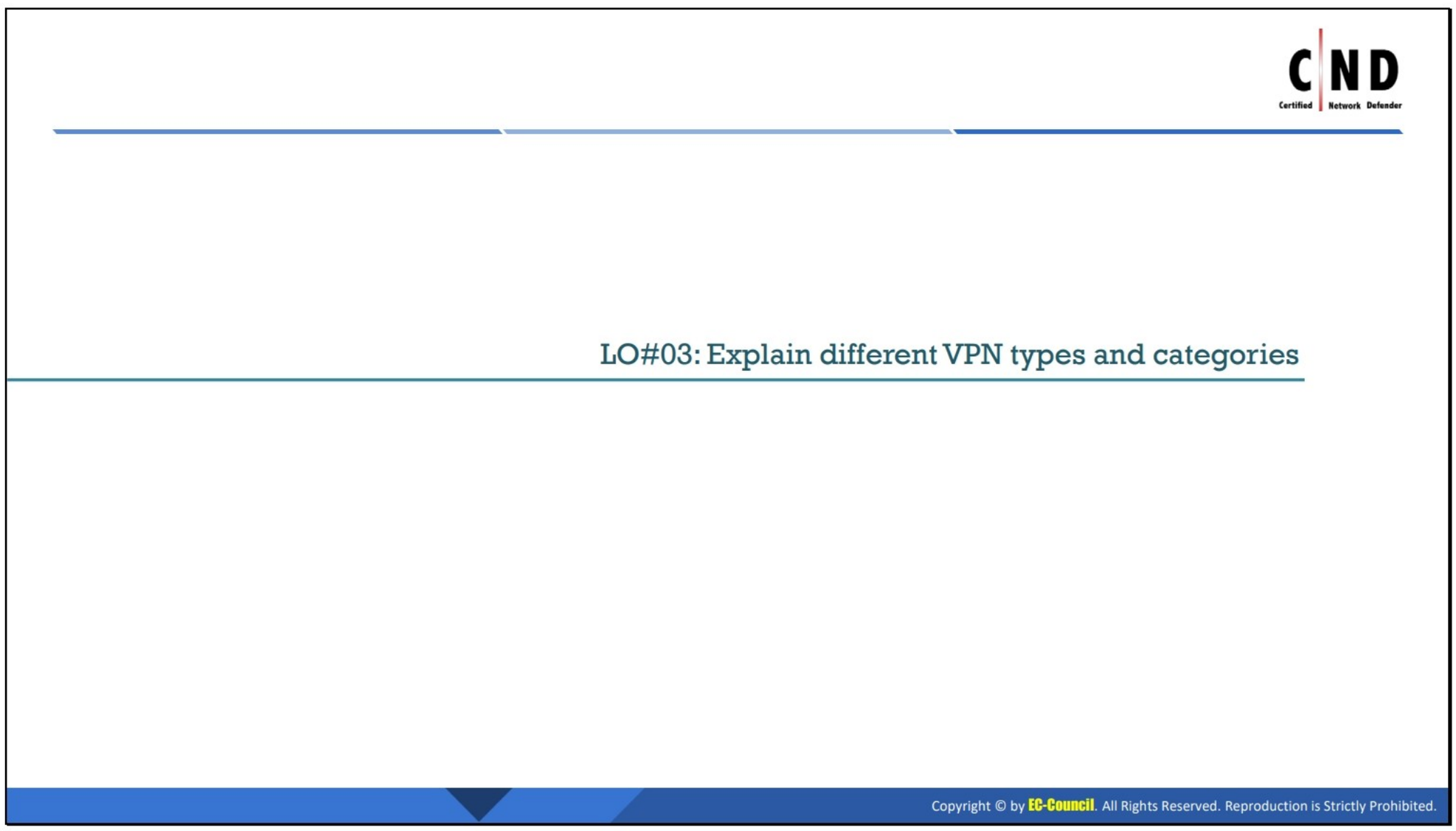


Functions of a VPN Concentrator

A VPN concentrator adds more security controls to the router, improving the security of the communication. The functions of a VPN concentrator are as follows:

- **Data encryption:** The VPN concentrator encrypts the data. Being bi-directional, it initially encrypts the plain packets it receives and later decrypts them at the end of the tunnel before sending them to the destination.
- **Managing tunnels:** By adding the features of advanced data and network security, a VPN concentrator has the ability to create and manage large VPN tunnels. These tunnels ensure data integrity among the systems.
- **User Authentication:** A VPN concentrator authenticates users at either the computer level or at the user level. Authentication at the computer level takes place using the Layer Two Tunneling Protocol (L2TP) protocol whereas authentication at the user level takes place using the Point-to-Point Tunneling Protocol (PPTP).
- **Traffic handler:** A VPN concentrator routes the tunneled and non-tunneled traffic depending on the server configuration. It simultaneously handles traffic of a corporate network as well as Internet resources.

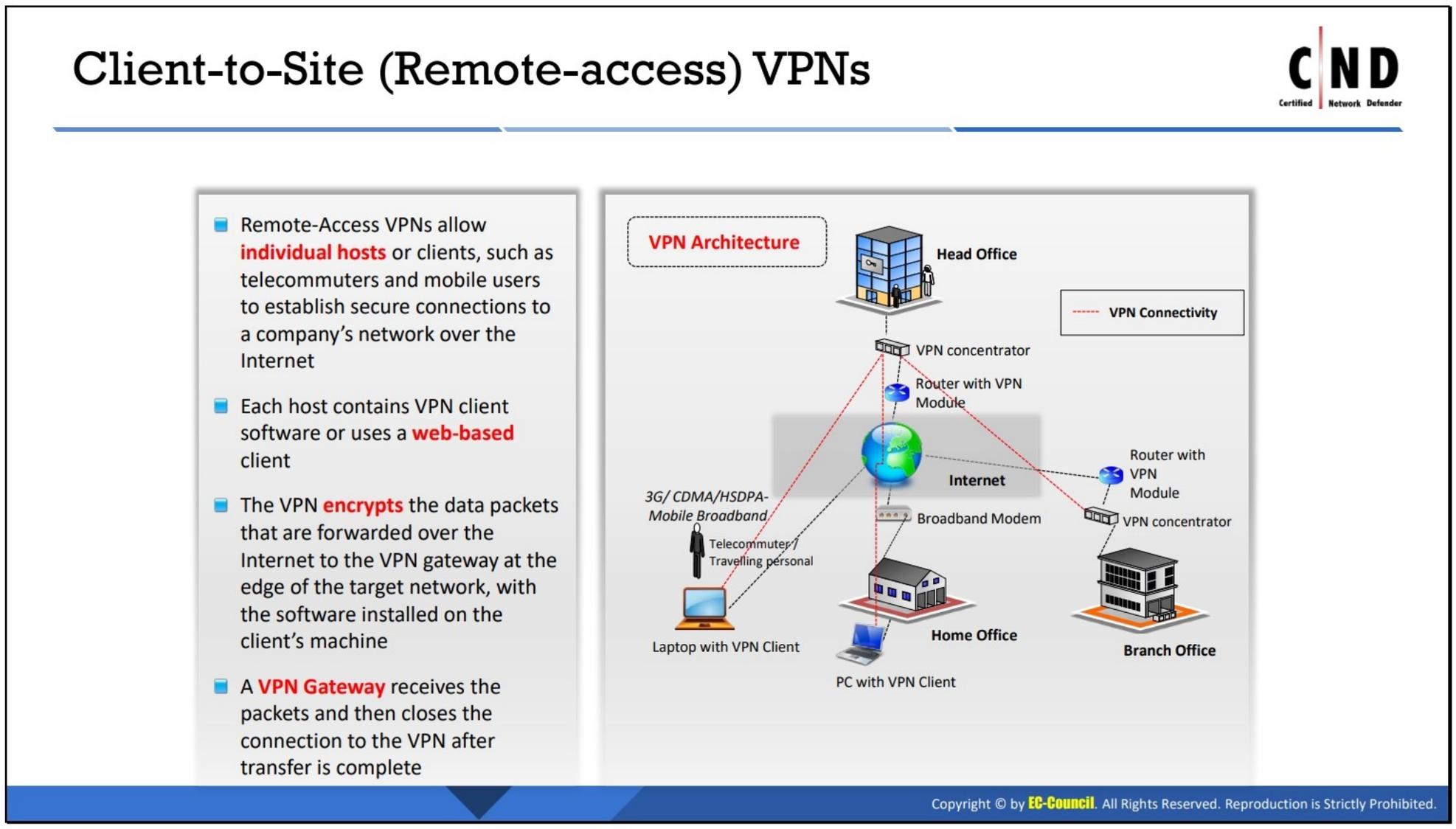
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#03: Different VPN Types and Categories

This section explains different types of VPN and their categories.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Client-to-Site (Remote-access) VPNs

Remote-access VPNs are used mainly to connect individual hosts to a private network. This allows the users to access the information provided in the private network. An older name for a remote-access VPN is a virtual private dial-network (VPDN) in which a dial-up configuration is required for the connection to a server.

Every host using remote-access needs to have the VPN client software installed, that wraps and encrypts the data before the host sends any traffic over the Internet to a VPN gateway. After reaching the gateway, the data is unwrapped, decrypted, and passed over to the final destination in a private network. The gateway performs the reverse process in order to send the data packets back to the user. The remote-access VPN consists of two types of components:

- **Network access server (NAS) or remote-access server (RAS)**: NAS is required while users are accessing a VPN. A separate authentication process is involved while authenticating users accessing a VPN
- **Client software**: Users accessing a VPN from their own network need to install software that helps create and manage the VPN connection

VPN client software and a VPN gateway are required for the hosts supporting a remote-access VPN. Most of the VPN gateways support only IPSec while maintaining VPN services.

Advantages

- Minimizes the connection cost for the users.
- Encryption of data packets provides an added security layer. This hides the IP address of the packets and prevents the attackers from accessing the packets.

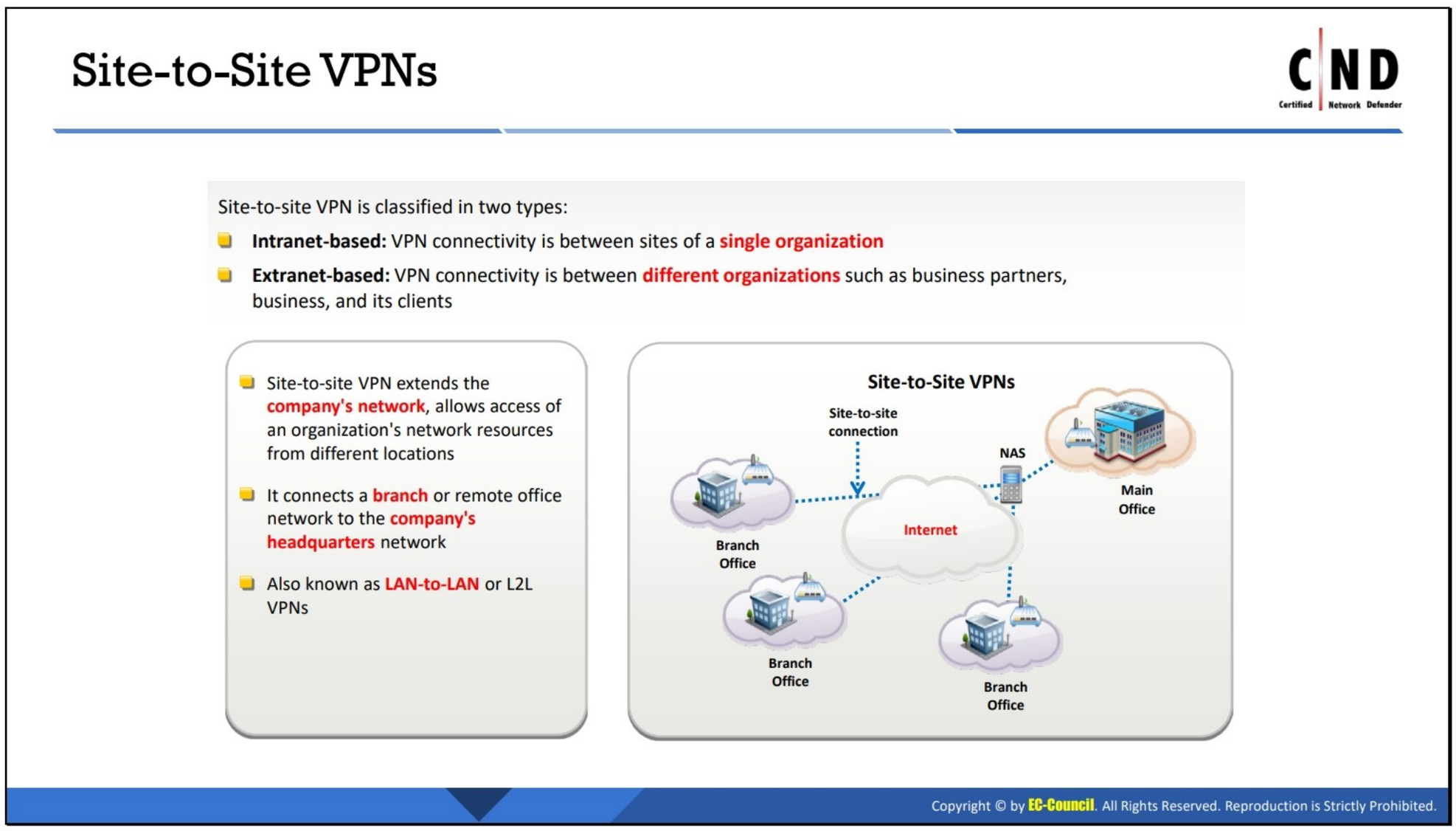
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Handle the large number of users. The VPN provides the same service even if more users are added to the VPN network.
- Sharing of files from a remote location.

Disadvantages

- Computers without any anti-virus installed pose a threat to the VPN connection.
- Implementing many VPN connections simultaneously may affect the bandwidth of the network.
- Time-consuming accessing files, applications over the Internet.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Site-to-Site VPNs

The site-to-site VPN helps connects all the networks together. For example, the branch offices of an organization can be connected to the main campus through a site-to-site VPN. The main differentiation between a remote and a site-to-site VPN is that site-to-site VPNs do not require the need for any client software. The entire traffic is sent through a VPN gateway that encrypts the data packets passing through it.

In a site-to-site VPN, the outbound traffic is passed through a tunnel to the VPN gateway. The data packets in the outbound traffic are encrypted at the gateway and are passed to the tunnel over the Internet. The traffic is sent to the nearest gateway to the target location. The nearest gateway decrypts the data packets and they are then forwarded to the final destination.

A site-to-site VPN consists of two types:

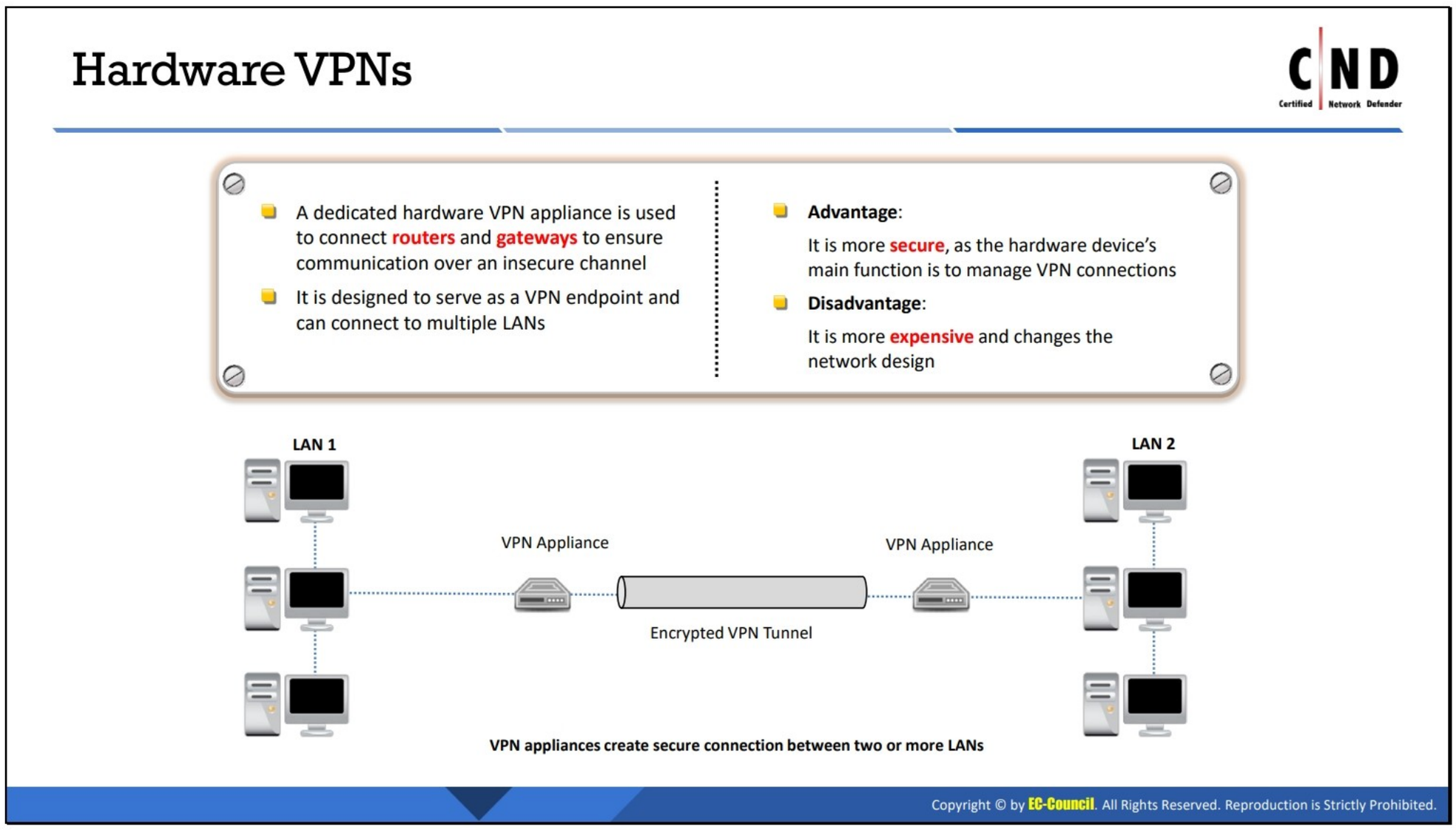
Intranet-based

Creates an intranet VPN in order to connect each individual LAN to a single WAN.

Extranet-based

Extranet VPN connects every single LAN of an organization. The extranet VPN configuration prevents any access to an intranet VPN.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hardware VPNs

Hardware-based VPNs are separate devices that consist of individual processors and hardware firewalls. They easily manage authentication and encryption of the data packets. The main advantage of using a hardware-based VPN is that they provide more protection than the software variant.

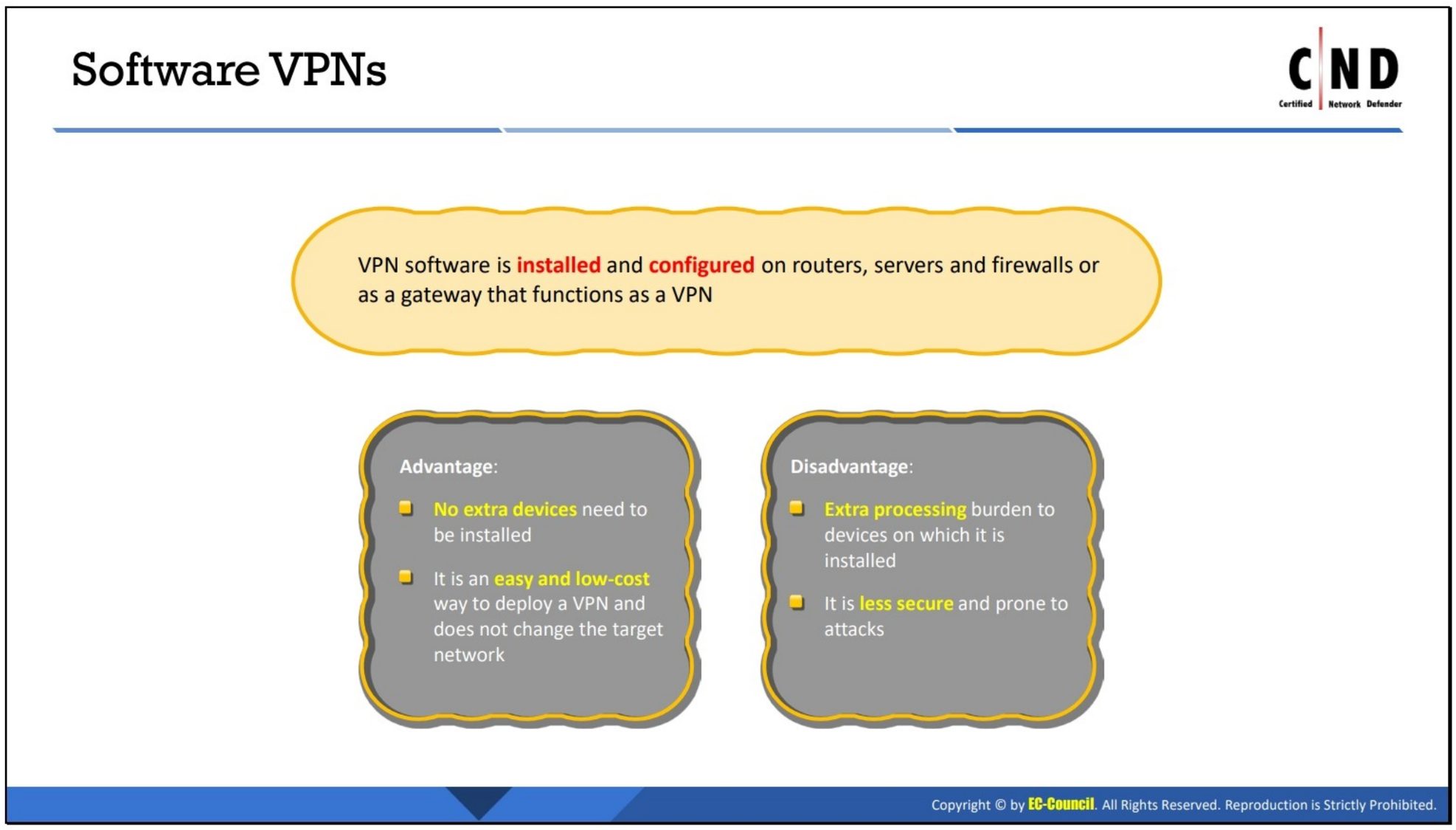
Advantage

- Provides load balancing especially for large client loads.

Disadvantage

- It is more expensive than a software VPN.
- More useful for large business organizations than for smaller ones.
- Less scalability.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Software VPNs

Software-based VPNs are best suited for network traffic management and when the same party does not manage the VPN endpoints. Traffic management is performed using a tunneling process depending on the protocol and address of the traffic. Hardware encryption accelerators are used in order to improve the performance of the network.

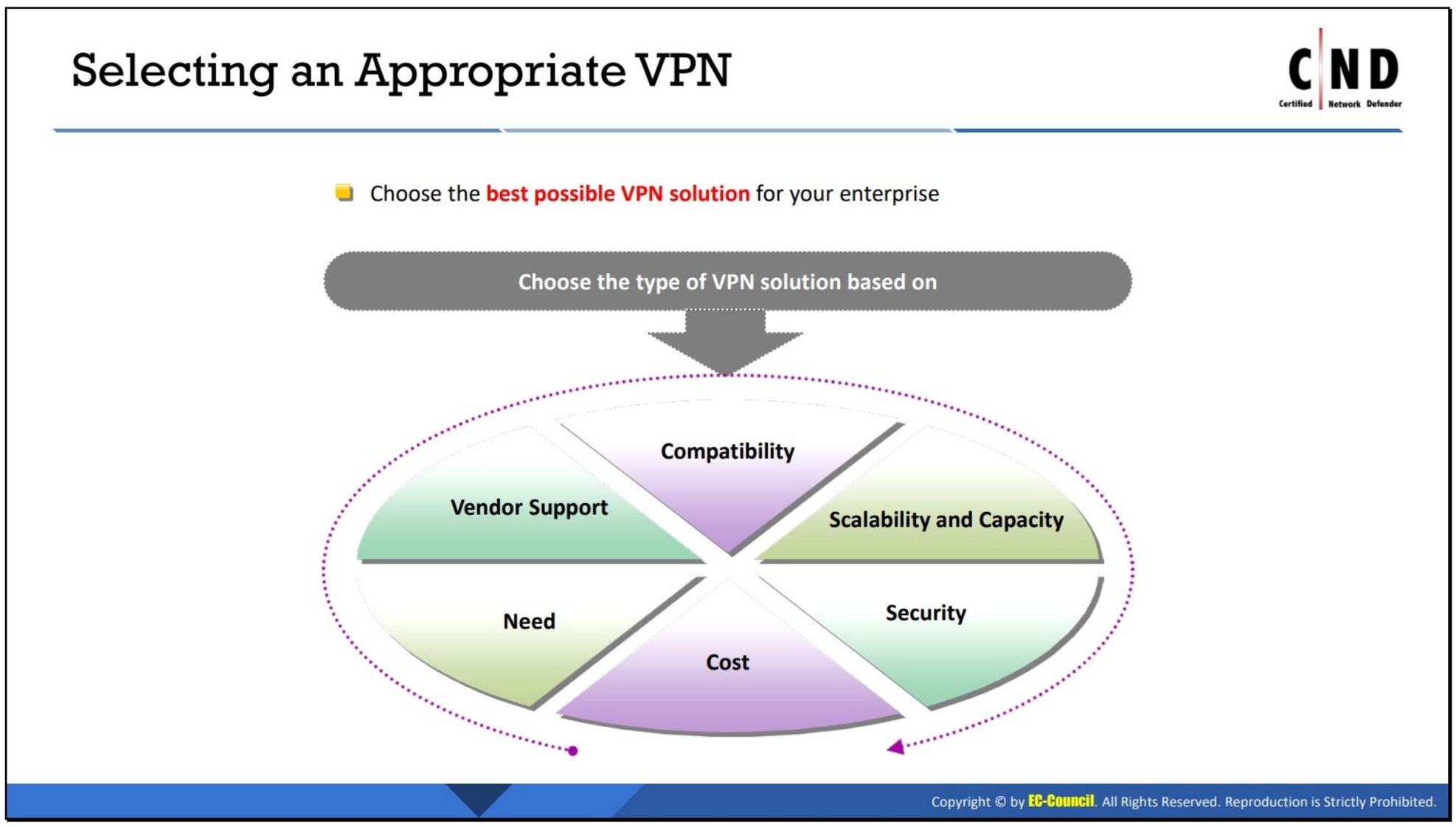
Advantages

- Minimizes the cost of additional hardware purchases.
- It is easy to deploy and does not change the target network.
- More scalability.

Disadvantage

- Increased processing tasks for devices implementing the VPN.
- Security is an issue and is prone to more attacks as they need to share the server with other servers and operating systems.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Selecting an Appropriate VPN

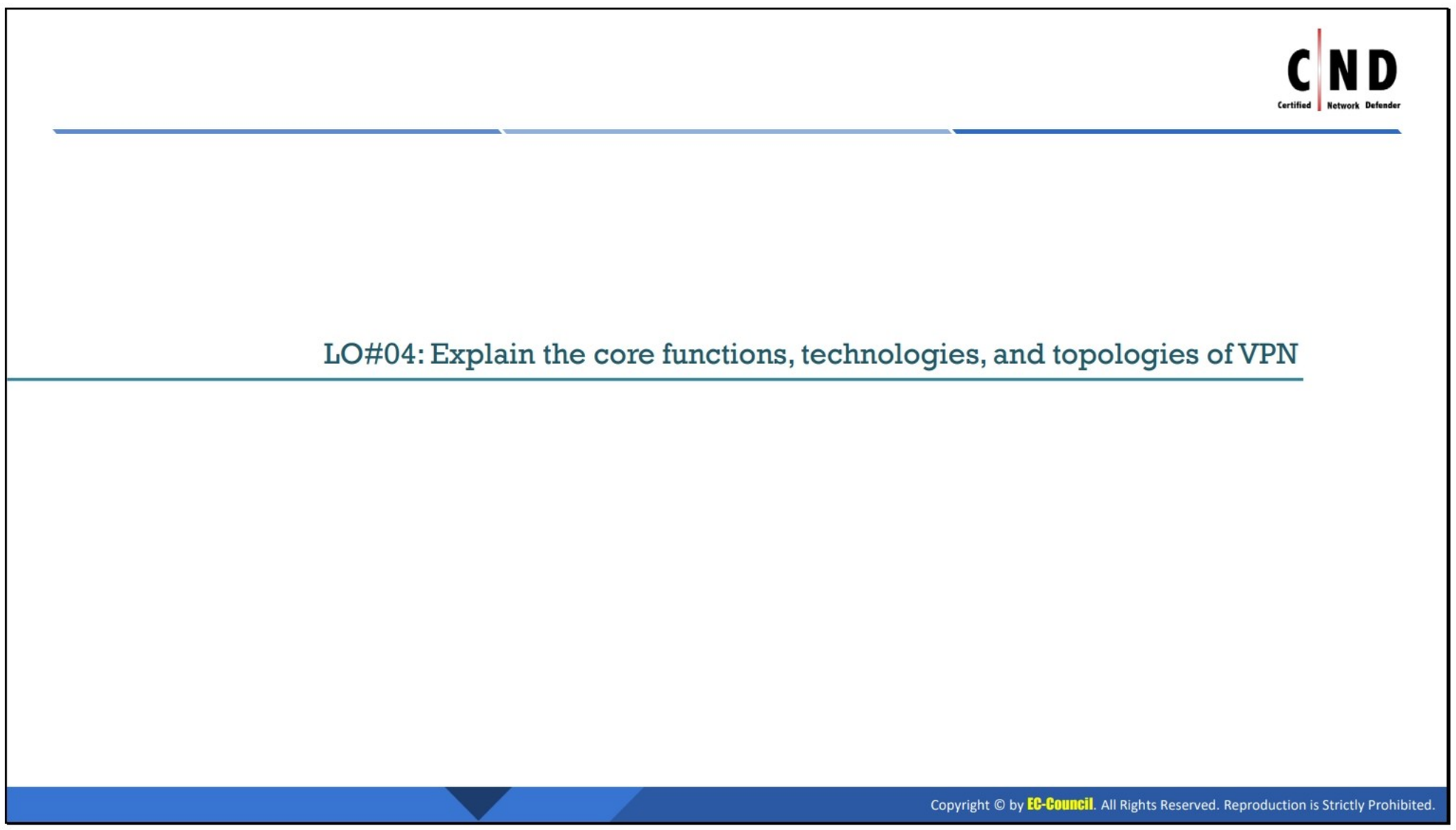
The selection of an appropriate VPN depends on many factors such as cost, protocols, technical issues, etc. The following are a few factors to consider while selecting a VPN:

- **Compatibility**: The organization should consider the compatibility of the selected VPN within the organization's network and determine whether it is possible to adopt the selected VPN. Selecting and implementing a VPN which is not compatible, will add an extra expense on the company's expenditure and cause security issues.
- **Scalability**: Increasing the number of employees working for an organization is a common trend. As the number of employees increases, the configured VPN also needs to accommodate the extra number of employees at the same time. The inability to handle the increasing number of users adversely affects the performance of the network. The organization must select a VPN that can handle any number of users at any time without affecting the performance of the network.
- **Security**: Security is an important factor while selecting a VPN. Two major criteria in selecting a VPN are:
  - **Authentication**: Organizations need to select an appropriate authentication method depending on the type of network on which the VPN is implemented.
  - **Encryption**: Organizations should be highly alert regarding the encryption process for the selected VPN. Some VPNs do not provide direct encryption, allowing attackers to get information from the network.
- **Capacity**: Organizations need to foresee the number of users joining the organization in the future and then select the VPN accordingly.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Cost**: An organization should consider cost as a factor while selecting VPNs.
- **Need**: The need for a VPN depends on the requirements of an organization. Whether remote employees need access to the network or there are encrypted traffic rules. Each organization is different and these differences will decide the appropriate VPN choice.
- **Vendor Support**: Two different factors in vendor support are as follows:
  - The number of servers present and their location: The VPN is selected according to the location of the vendor server and the activities performed.
  - Does the vendor limit connections, use bandwidth throttling or restrict service? VPNs that control bandwidth, reduce Internet speeds, or limits them in any way are not used in an organization. Also, care should be taken while dealing with the protocols and services running in the network. The organization needs to decide on whether the existing services and protocols running are actually needed by the organization or not.

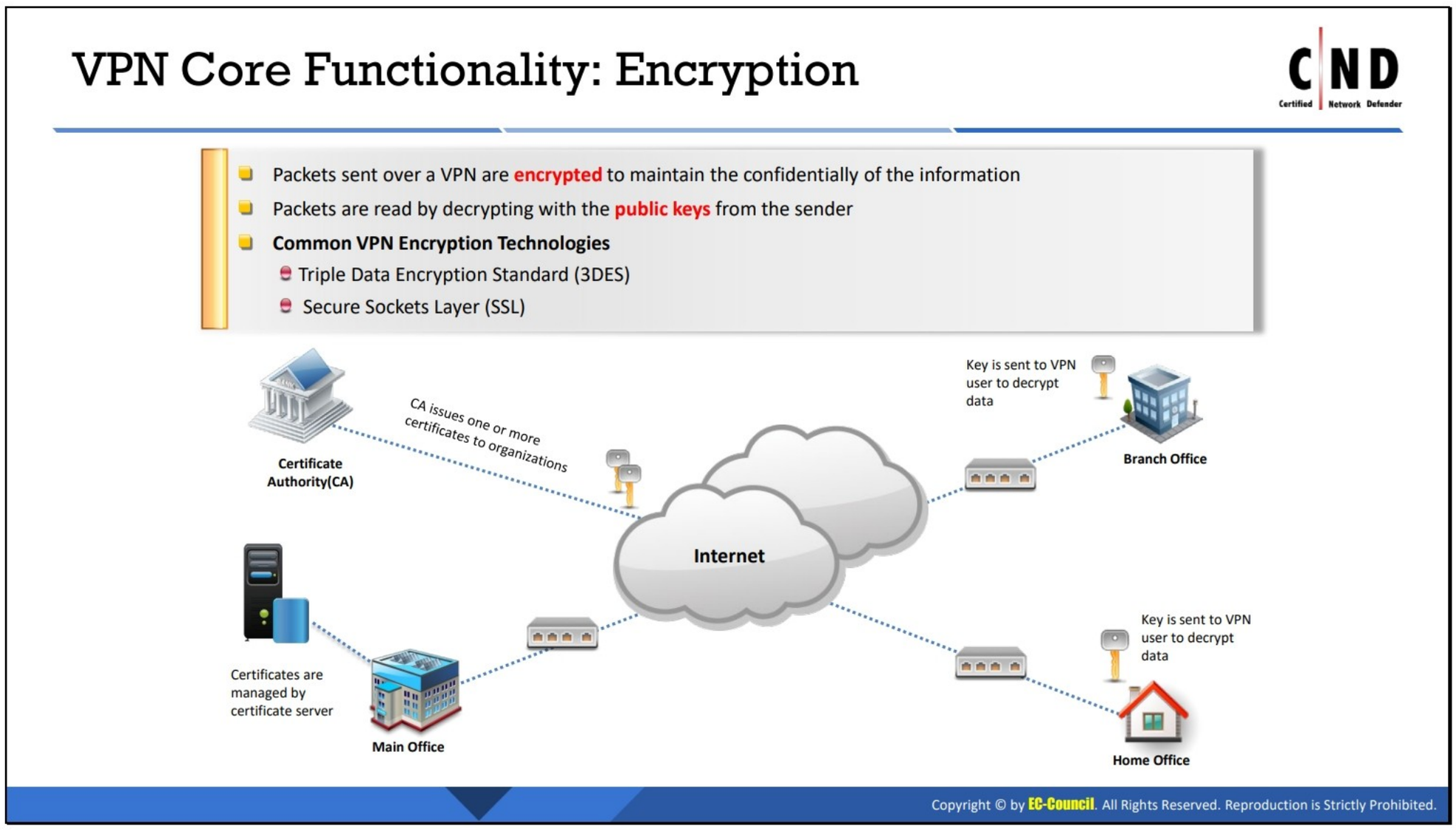
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#04: Core Functions, Technologies, and Topologies of VPN

This section discusses the core functions, technologies, and topologies of a VPN.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



VPN Core Functionality: Encryption

A VPN uses encryption to provide an additional layer of security to data transmitted over the VPN. Encryption plays an important role when sensitive data is carried over the Internet in an organization. All data that enters the VPN tunnel is encrypted and decrypts as soon as it reaches the end of the tunnel. An encryption key is used in the process of encryption and decryption. Encryption disables monitoring, logging, or tampering of the data in an organization.

Encryption helps secure the data passing through the network. The sender encrypts the data passing through the network and the receiver decrypts the data. It requires no encryption on the communication link between a dial-up client and the internal service provider, as the process of encryption takes place between the VPN client and the VPN server.

In VPN encryption, both the sender and the receiver need to have a common encryption key that is sent along with the data. If a packet traveling through the VPN connection does not have the keys associated with it, then it is of no use to the computer. There are many mechanisms to determine the length of the encryption key. The encryption of messages using the same key enables easy interpretation of the encrypted data. The administrator can always select the encryption keys used for a connection.

In end-to-end encryption, the encryption occurs between the client application and the server. IPsec is used with an end-to-end connection, once a remote access connection is made. IPsec works as follows:

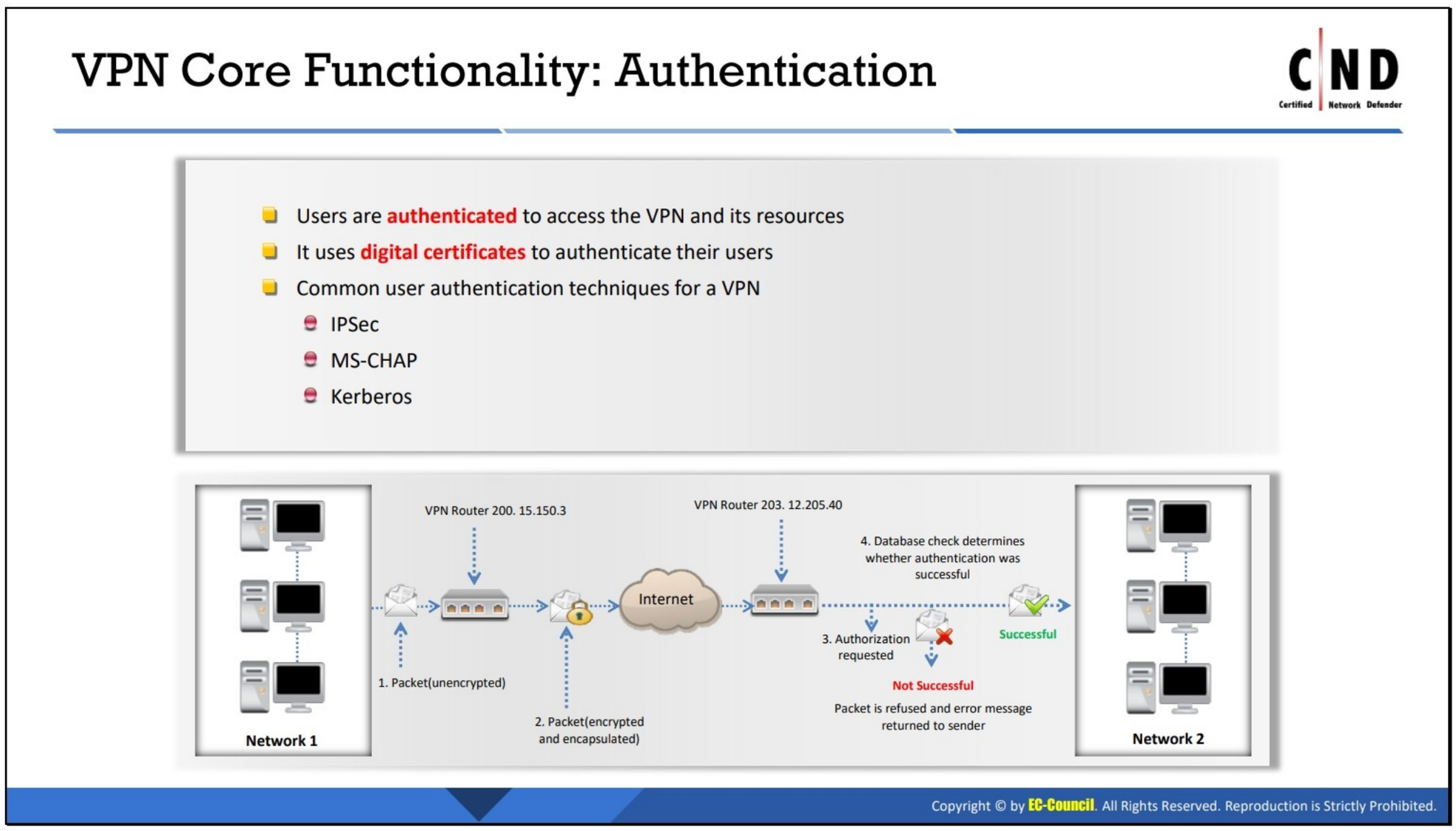
- Encryption of a packet using an encryption key. The key is known only to the sender and the receiver.
- An encapsulation header, a sub-protocol, conceals the sensitive information of the packets including sender identity.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

VPN encryption technologies

- Triple DES algorithm: A 64-bit block of data that processes each block three times with a 56-bit key. 3DES prevents the chances of breaking the encryption key.
- Secure Socket Layer (SSL): A secure technology that enables the communication between the server and the client. SSL technology enables the secure transaction of credit card numbers, login credentials etc. over the internet.
- Open VPN: It is an open-source VPN and works with the SSL protocol.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



VPN Core Functionality: Authentication

Authentication is an integral part of VPN technology, as the hosts receiving a VPN communication need to ensure the authenticity of the hosts initiating and sending the VPN connections. A VPN employs three kinds of authentication:

- **User authentication:** The VPN deploys the mutual authentication concept. The VPN server authenticates the VPN client to check whether the client has the permission to connect. Also, the VPN client can authenticate a VPN server for proper permissions.
- **Computer authentication with L2TP/IPSec:** Remote-access computers are authenticated for proper permissions using IPsec and L2TP/IPsec.
- **Data authentication and Integrity:** All L2TP/IPsec packets sent are included with a cryptographic checksum based on the encryption key. Only the sender and the receiver know this checksum. This is to ensure the data sent is not manipulated during transit.

Authentication techniques used in VPN

- **IPsec Family**
  - **Internet Protocol Security (IPsec):** All application traffic is secured using the IP network. IPsec conducts session authentication and data packet authentication for any two securely connected entities. IPsec ensures a secure connection between two networks or remote networks to the main network.
  - **Layer2 Tunneling Protocol (L2TP):** This protocol initiates a connection between two L2TP connections. L2TP is always combined with the IPsec protocol in order to confirm security.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Kerberos**

  Kerberos consists of a record of clients and their private keys. Only the client and Kerberos know the details of the private key. Kerberos generates session keys that encrypt messages between two clients.

- **PAP**

  Password Authentication Protocol uses a clear-text authentication mechanism for authenticating users. The PAP sends a username and password as per the NAS request. The NAS receives the username and password in clear text form, which means the NAS receives the details in an unencrypted form. This makes it easy for attackers to establish a connection with the NAS to acquire all the information.

- **SPAP (Shiva Password Authentication Protocol)**

  A reversible encryption mechanism that is more secure than PAP. SPAP plays its role when a Shiva client is attempting to access a server. However, this authentication mechanism is less secure than CHAP or MS-CHAP.

- **CHAP (Challenge Handshake Authentication Protocol)**

  The CHAP protocol is more secure than PAP. It uses an encryption authentication technique which transmits a password representation instead of an actual password during the authentication process. The server sends a challenge message to the client to authenticate users. Users respond with a hash value created using a hash algorithm. The server then compares this hash value with its own calculation of the hash. If it matches, then authentication is acknowledged. The remote client creates a hash of the session ID, challenge and password. It uses the MD-5 one-way hashing algorithm.

- **MS-CHAP**

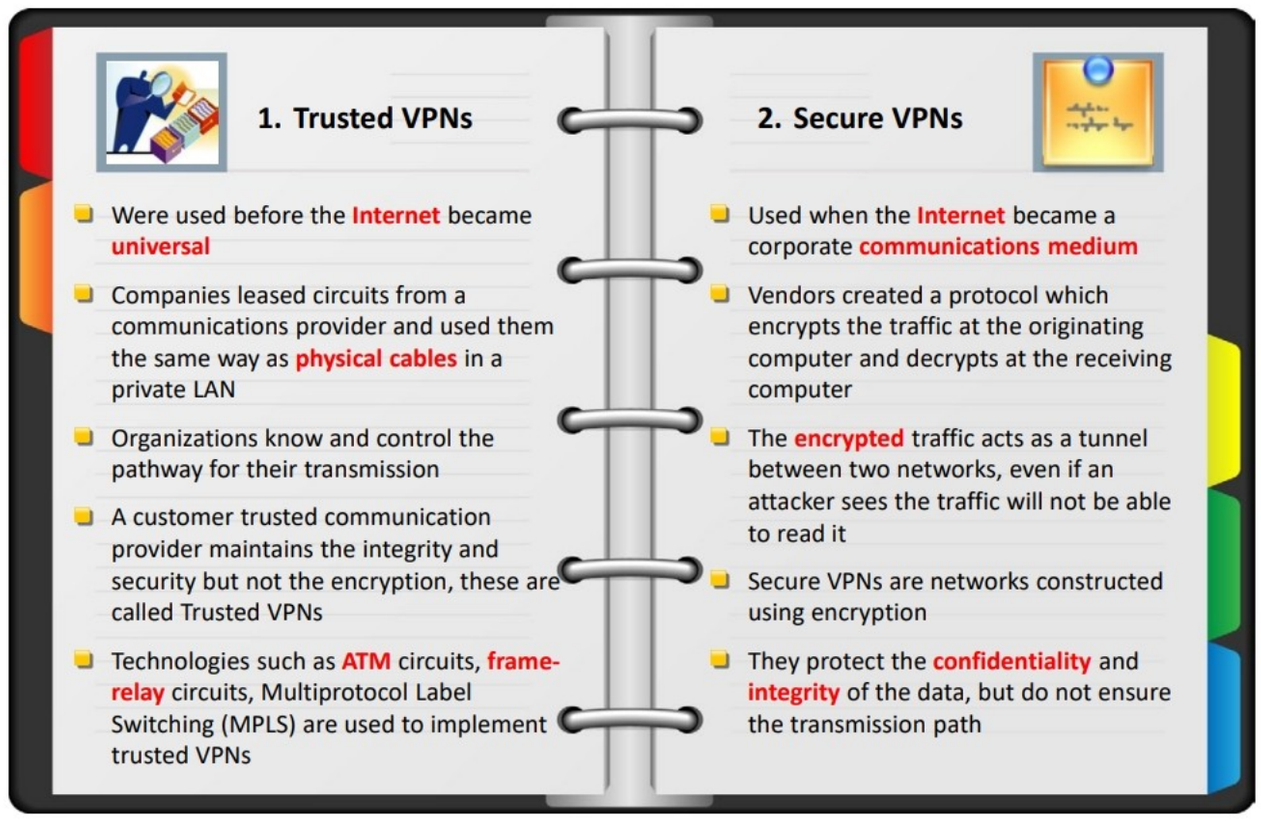
  The Microsoft Challenge Handshake Authentication Protocol uses a remote access server to send a session identifier and a challenge string to the remote access client. The client, in turn, sends an encrypted form of the identifier and challenge string to the server. This encrypted form is irreversible.

- **EAP (Extensible Authentication Protocol)**

  With EAP, the data for authentication is compared against an authentication database server. The EAP authentication protocol allows new plug-ins to be added at the client and server.

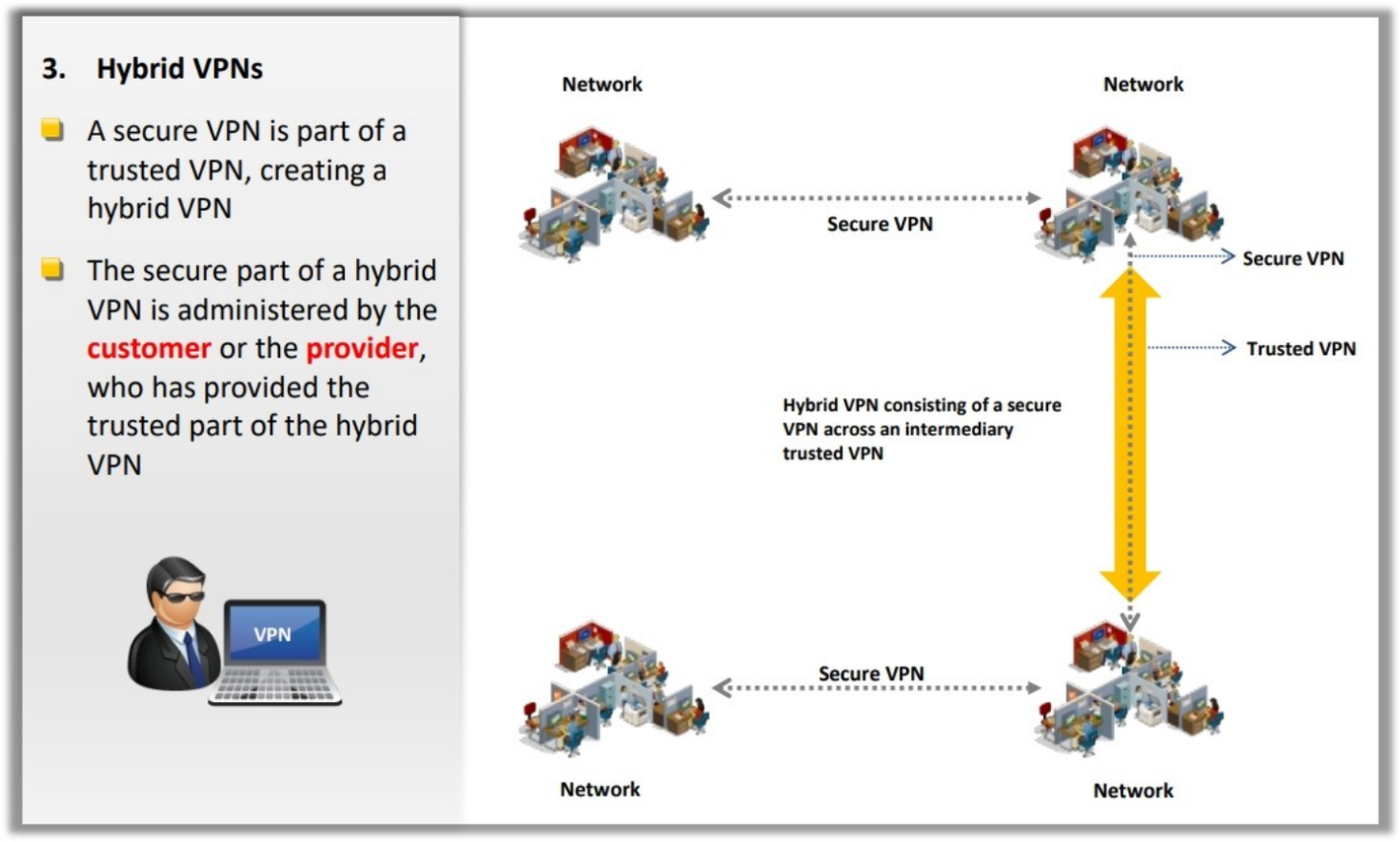
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

VPN Technologies



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

VPN Technologies (Cont'd)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

VPN Technologies

VPN technology enables organizations to connect mobile and remote users with network access and also to connect separate branches of the same organization to a single network.

Common technologies used to deploy VPNs for secure data transmission are:

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Trusted VPN

Even before the popularity of the Internet, service providers provided customers with specific circuits that could not be used by anyone else. This gave customers privacy and the ability to have their own IP addresses and policies. In order to provide security measures and avoid sniffing of the data, VPN providers are entrusted to maintain circuit integrity. This type of VPN is called a trusted VPN. The technologies used for implementing trusted VPNs over an Internet Protocol network are Asynchronous Transfer Mode (ATM) circuits, frame relay circuits, and MLPS.

ATM and frame relay operates at layer 2 of the OSI model and MLPS operates in between the data link layer and network layer. The requirements for a trusted VPN are:

- Any changes in the path of a VPN can be made only by a trusted VPN.
- All routing and addressing methods need to be described before creating a trusted VPN.
- Only a VPN provider can inject, change, or delete the data in the path of a VPN.

Secure VPN

The main goal behind implementing a secure VPN is to ensure complete security of the data in transit. In a secure VPN, all the data packets sent through the tunnel undergoes an encryption process at one end of the tunnel and decryption process at the other end of the tunnel. This prevents any attempt from the attacker to achieve data in transit. The main requirements for secure VPNs are:

- All the data packets in the traffic are encrypted and authenticated prior to sending it to the client.
- The client and server need to be in a mutual understanding before initiating the connection between each other.
- Confirm the security of the connection from unauthorized users.

Hybrid VPN

Hybrid VPNs are those with trusted VPNs as part of the secure VPNs. They implement different network components of an organization at the same time in order to confirm security at very low costs. A network defenders takes extra time in differentiating between the data transfer among the secured VPNs that are part of the trusted VPNs. The main requirements for hybrid VPNs are:

- There should be a clear differentiation between the trusted VPN and the secure VPN.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

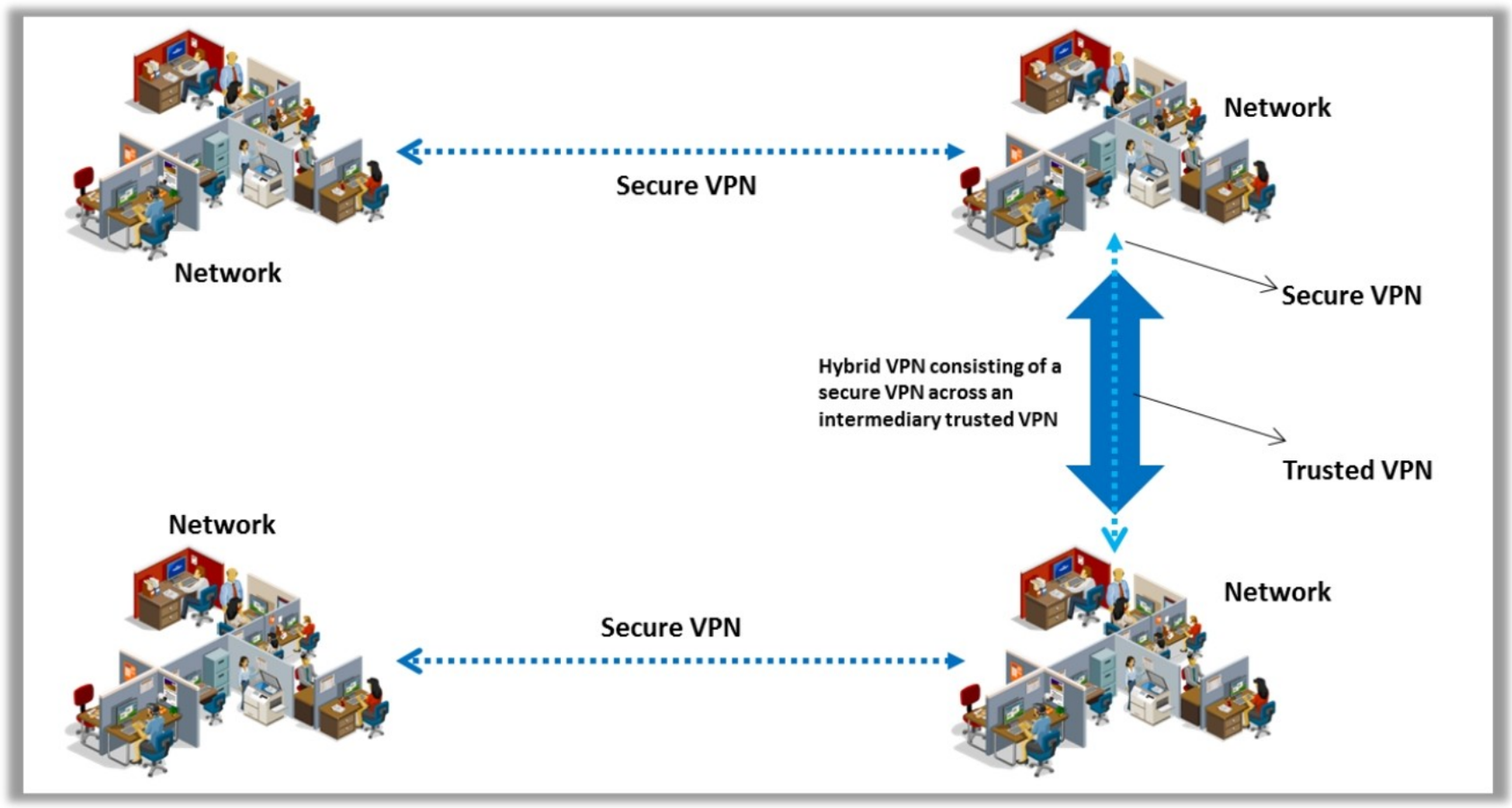
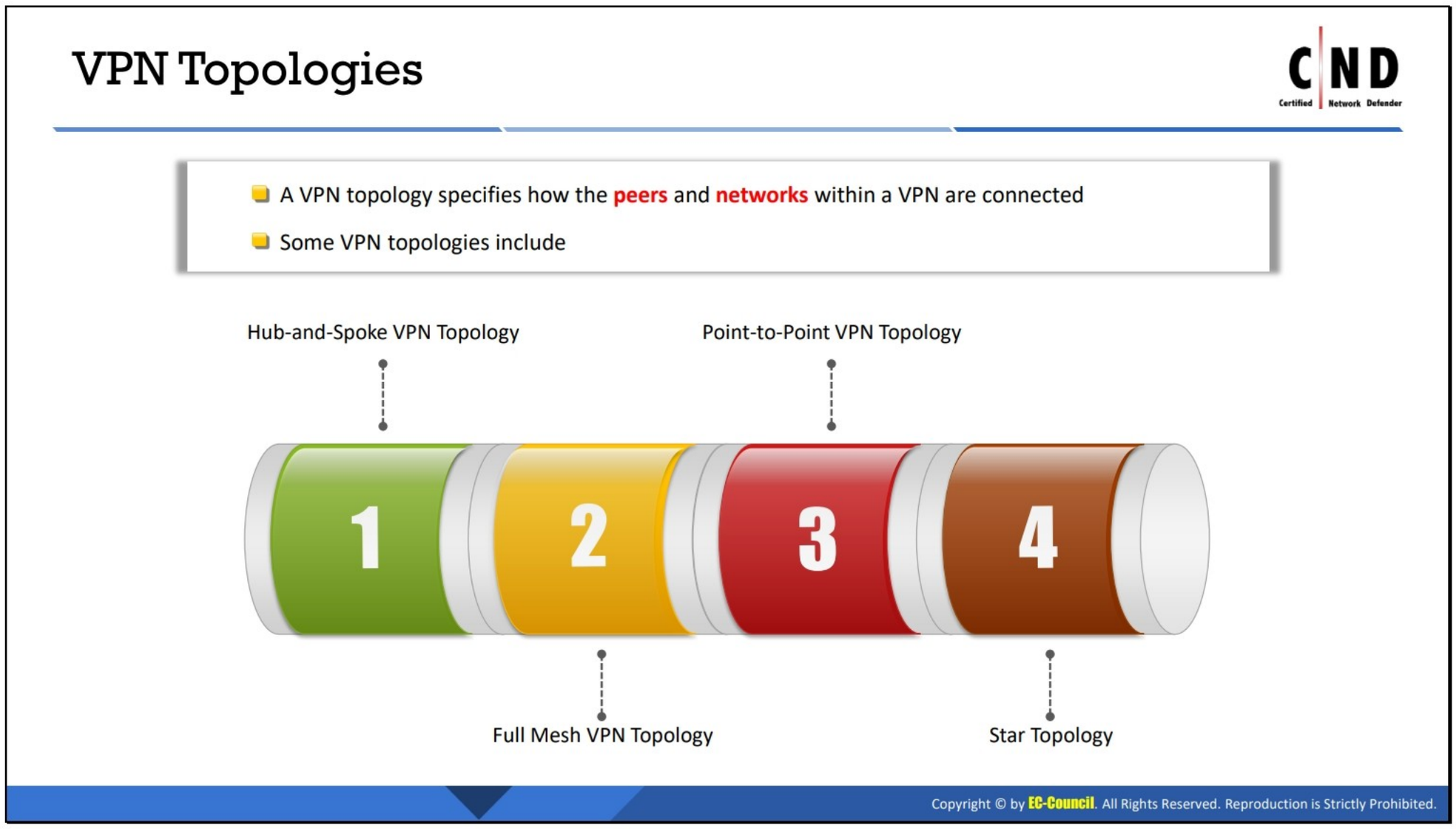


Figure C.3: Hybrid VPN

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



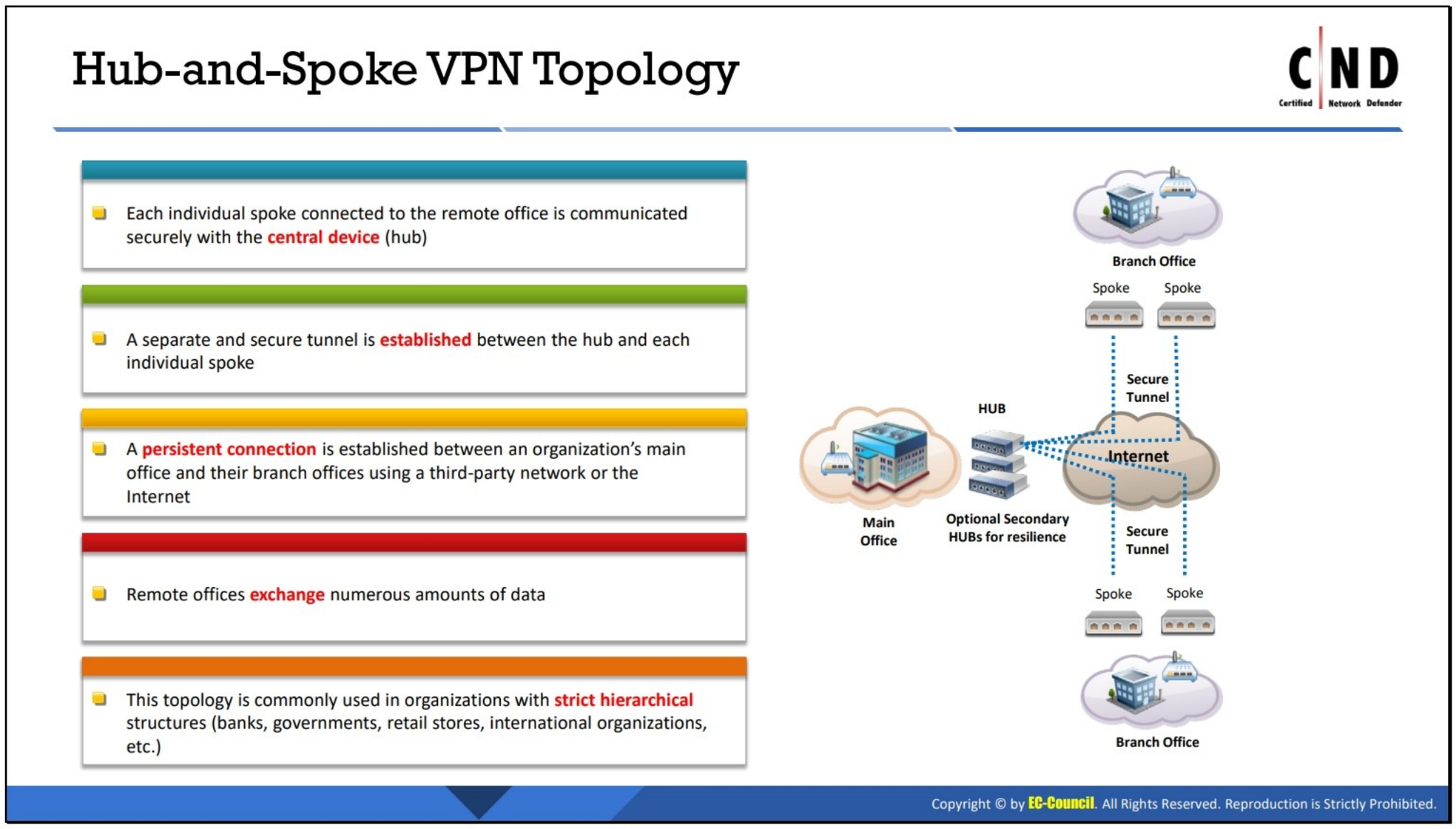
VPN Topologies

A VPN topology mainly deals with the specifications of how nodes in a network are connected and how they communicate with the other nodes. A VPN enables companies in a different network to communicate with each other and allows data sharing. VPN topologies enable the organization to design the way they can communicate with other networks. The different VPN topologies are:

- Hub-and-Spoke
- Point-to-Point
- Full Mesh
- Star

It is important to note that the selection of topologies depends on the requirements of the organization. For example, a Star topology is best suited in environments where the company needs to share information with another company located in a different network. A Mesh topology is best suited for an intranet.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hub-and-Spoke VPN Topology

In hub-and-spoke technology, the main organization is considered the hub, and its remote offices are considered the spokes. The spokes access the VPN through the hub. This topology is mainly used in banking and international organizations. The hub controls two types of communication:

- Communication between a spoke and a hub
- Communication between the spokes

This topology is used to represent an intranet VPN connecting an organization's main office to its regional offices. The hubs facilitate the sharing of numerous amounts of data. There are separate tunnels for data transfer between the hub and the spoke. All the data transfers happen through the hub. The hub-and–spoke topology can become a multilevel topology depending on the growth of the network.

In a multi-site network, the central hub controls the data transfer or is considered as the gateway for the remote sites to communicate with each other. For example, a cell phone tower in an area is the hub and all the mobile devices in and around the cell phone tower are the spokes. The network defender need to always maintain a thorough study of the hub-and-spoke technology in their network.

Advantages

- Less expensive and easy to repair when one of the spokes doesn't work.
- Bonded circuits in between the hub and the spoke increase the flexibility of the network.
- Offers better security as each device in the network is separated from the other through one single connection to the hub.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- These provide high performance, centralization, and simplicity.

Disadvantages

- Any issue in the hub can affect the connection between the hub and spoke and the connection between the different spokes.

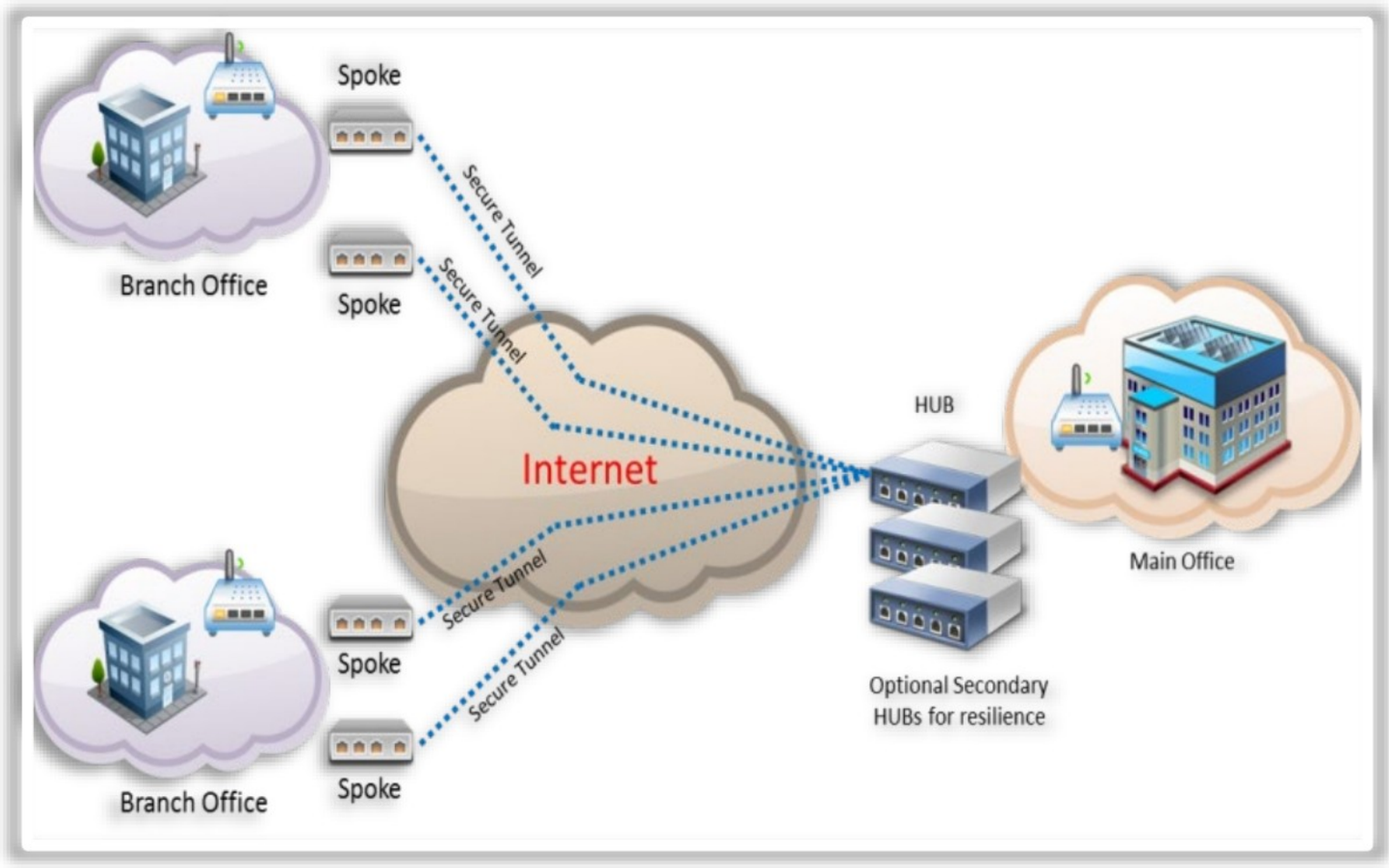


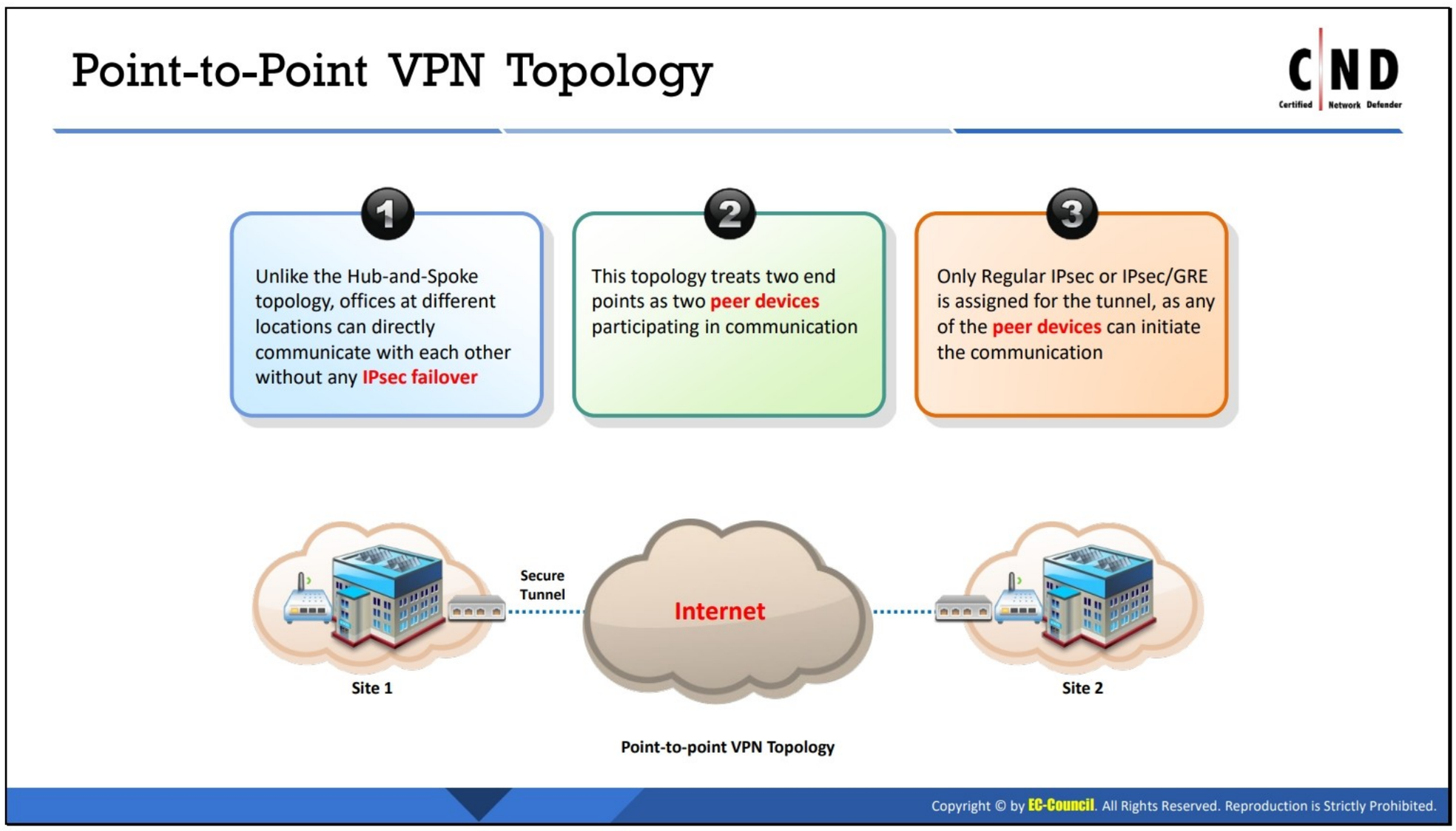
Figure C.4: Hub and Spoke VPN topology

The figure clearly explains the process of hub-and-spoke topology. In the figure, each spoke at the branch offices makes a secured connection with the hub at the main office. These secured connections are made across the Internet. The main office can have more than one hub at a time, only one hub is used to connect to each spoke. The other hubs are kept as backup hubs for flexibility.

This topology works well if the traffic is between the hub and spoke rather than between the spokes or the remote sites. This is because traffic between two spokes needs to go through the hub first and then forwarded to the respective spoke. This increases the chance of a bottleneck at the hub due to more spoke-to-spoke connections. All IPsec technologies can be used in this topology.

If the hub faces any issue in the connection, IPsec failover transfers the connection to a backup hub, used by all spokes. It is possible to configure multiple hubs as the main hub.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Point-to-Point VPN Topology

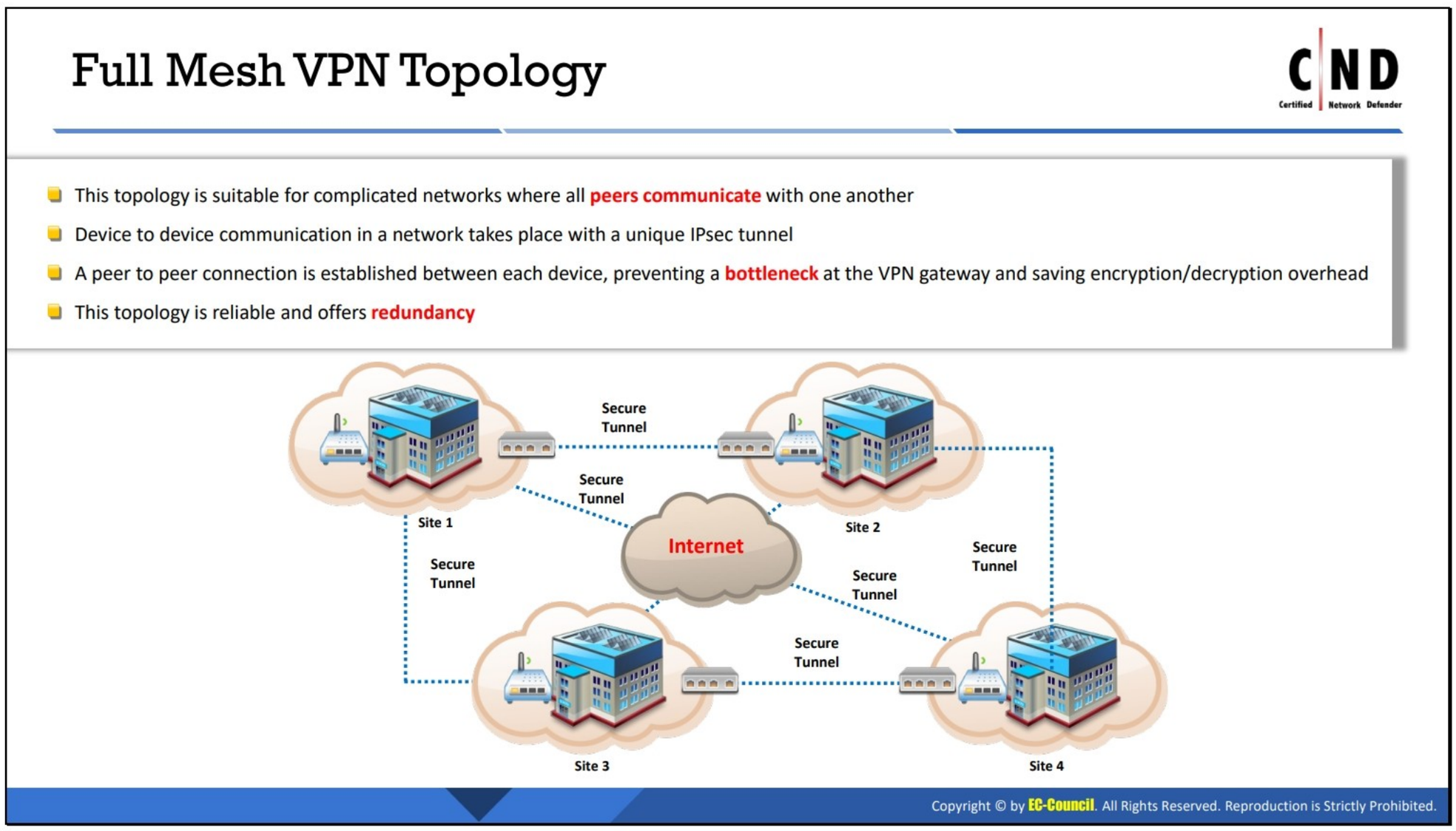
In a point-to-point topology, any two endpoints are considered as peer devices which can communicate with each other. Any of the devices can be used to initiate the connection. The IPsec technology assigned can be either IPsec or IPsec/GRE.

Commonly configured as a regular IPsec point-to-point VPN also known as an extranet. This is where a connection is established between a device in a regularly managed network and an unmanaged device in the service provider's network.

The major features of point-to-point topology are as follows:

- Easy routing of data as it needs to pass through only one router.
- Optimal routing between customer sites.
- Introduces encryption and authentication to confirm the integrity of packets in transit.
- Uses a tunneling process in order to capture data packets with normal IP packets for forwarding over IP-based networks.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Full Mesh VPN Topology

In a fully meshed VPN network, all peers can communicate with each other, making it a complex network. This topology allows all the devices in a network to communicate directly with each other through an IPsec channel. This reduces the chance of any holdup at the gateway and reduces the overhead of encryption and decryption of the device. A fully meshed VPN can implement normal IPsec, IPsec/GRE, and GET VPN technologies.

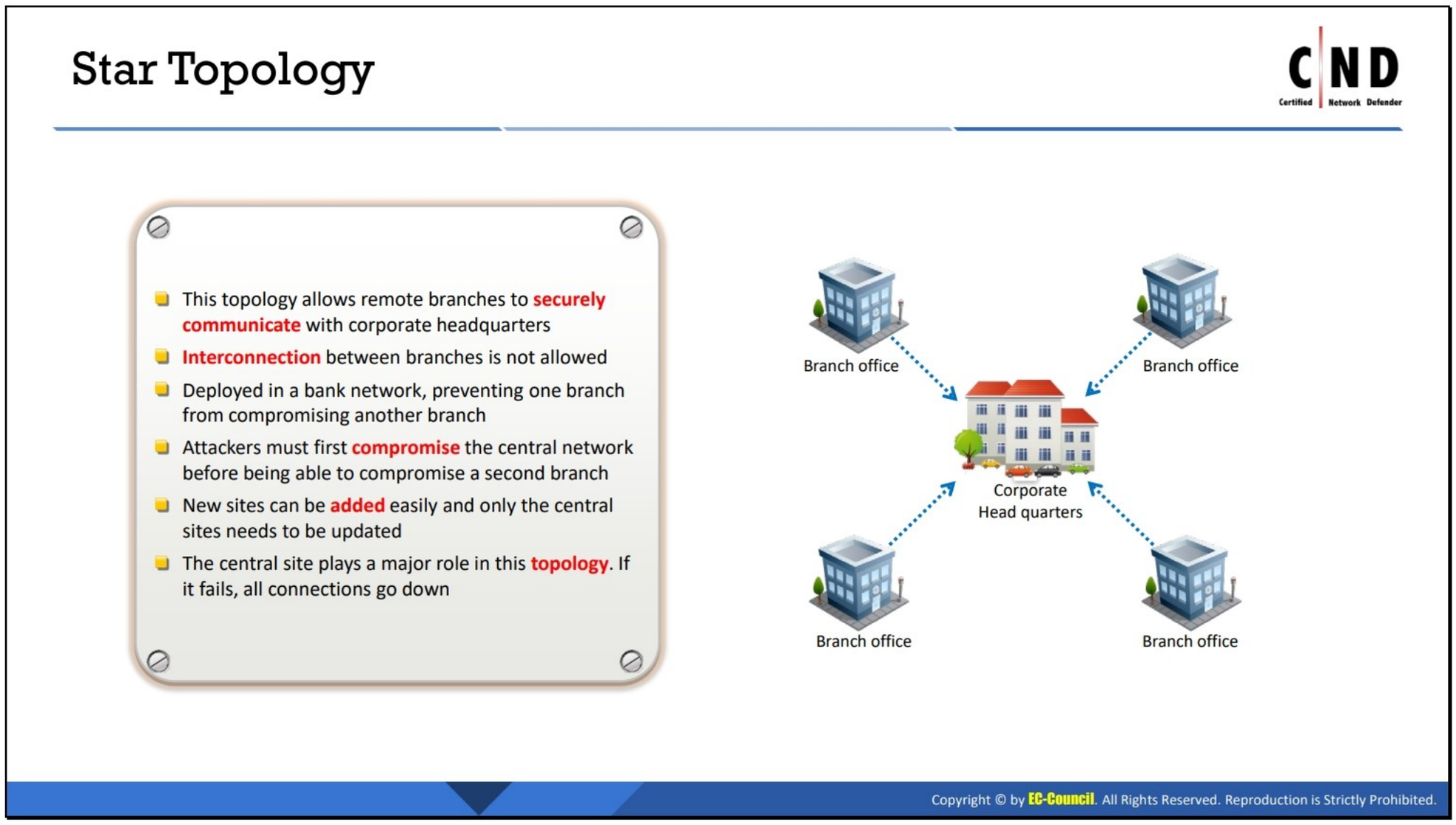
Advantages

- Any failure on one of the devices does not affect the entire network.
- Very reliable.
- Prevents any sort of block at the gateway.

Disadvantages

- Increases the number of devices connected to the network making it difficult to manage.
- Possible chances of redundancy in network connections.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Star Topology

This is the most commonly used topology in almost all organizations. Here, all the remote offices communicate with the corporate office but at the same time deny communication between the remote offices. Each device on the network is connected to a central hub that manages the traffic through the network.

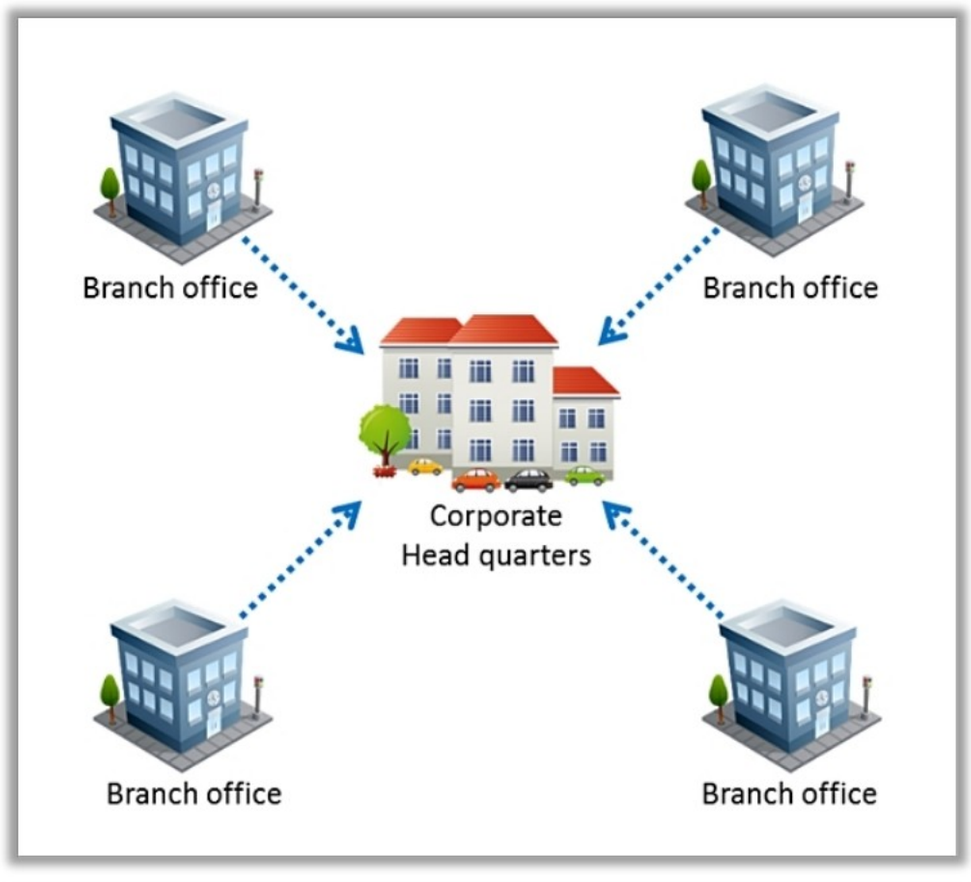


Figure C.5: Star topology

In the figure, all the branch offices can communicate with each other through the corporate headquarters. But in this topology, no two branch offices can initiate a separate communication as these are allowed only through the corporate network.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

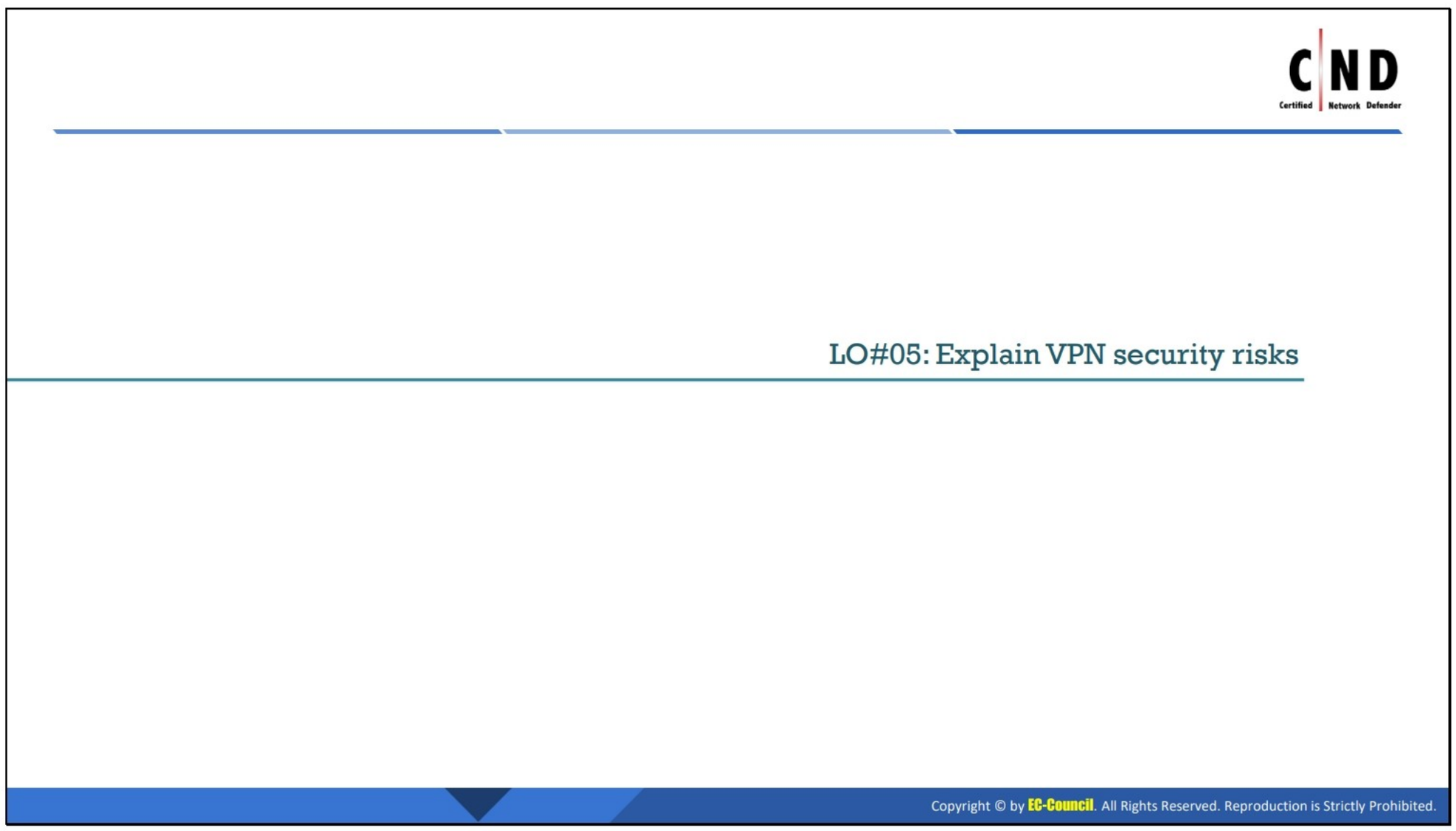
Advantages

- Most suitable for a financial infrastructure as the compromise on one system does not compromise another branch without detection.
- Any attack on the branch offices can be performed through the main branch. Any manipulation in the network can be easily detected by the network defender.
- Easy to add and remove new branch offices to the main office without affecting the neighboring sites. But, it is mandatory to update the main site regarding the new addition or removal of the sites.

Disadvantages

- Any failure in the central site affects the communication of all other sites.
- No two sites can communicate with each other directly.
- Adding more sites to the network can actually affect the capacity of the main site.

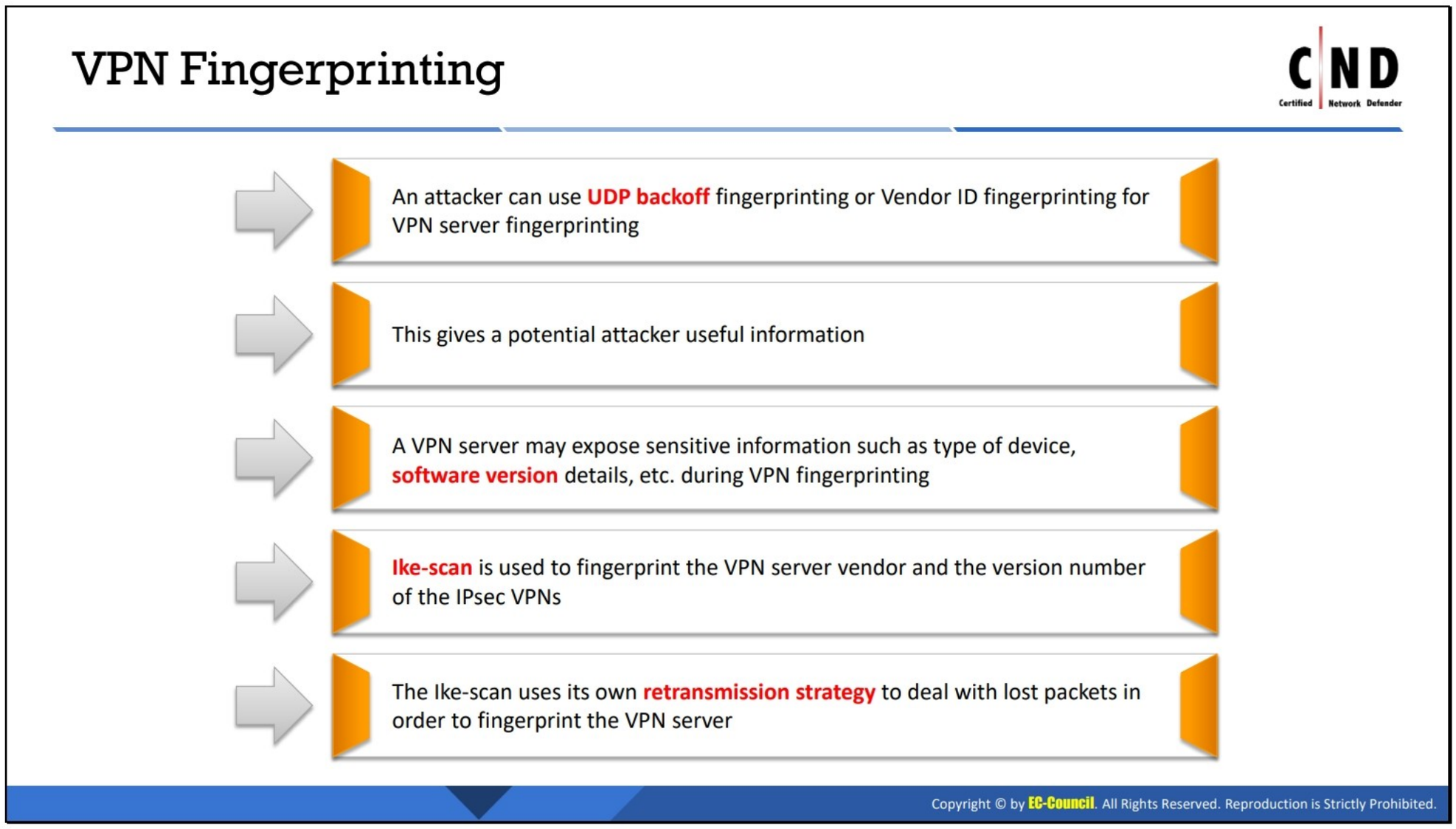
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#05: VPN Security Risks

This section discusses various VPN related security risks.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



VPN Fingerprinting

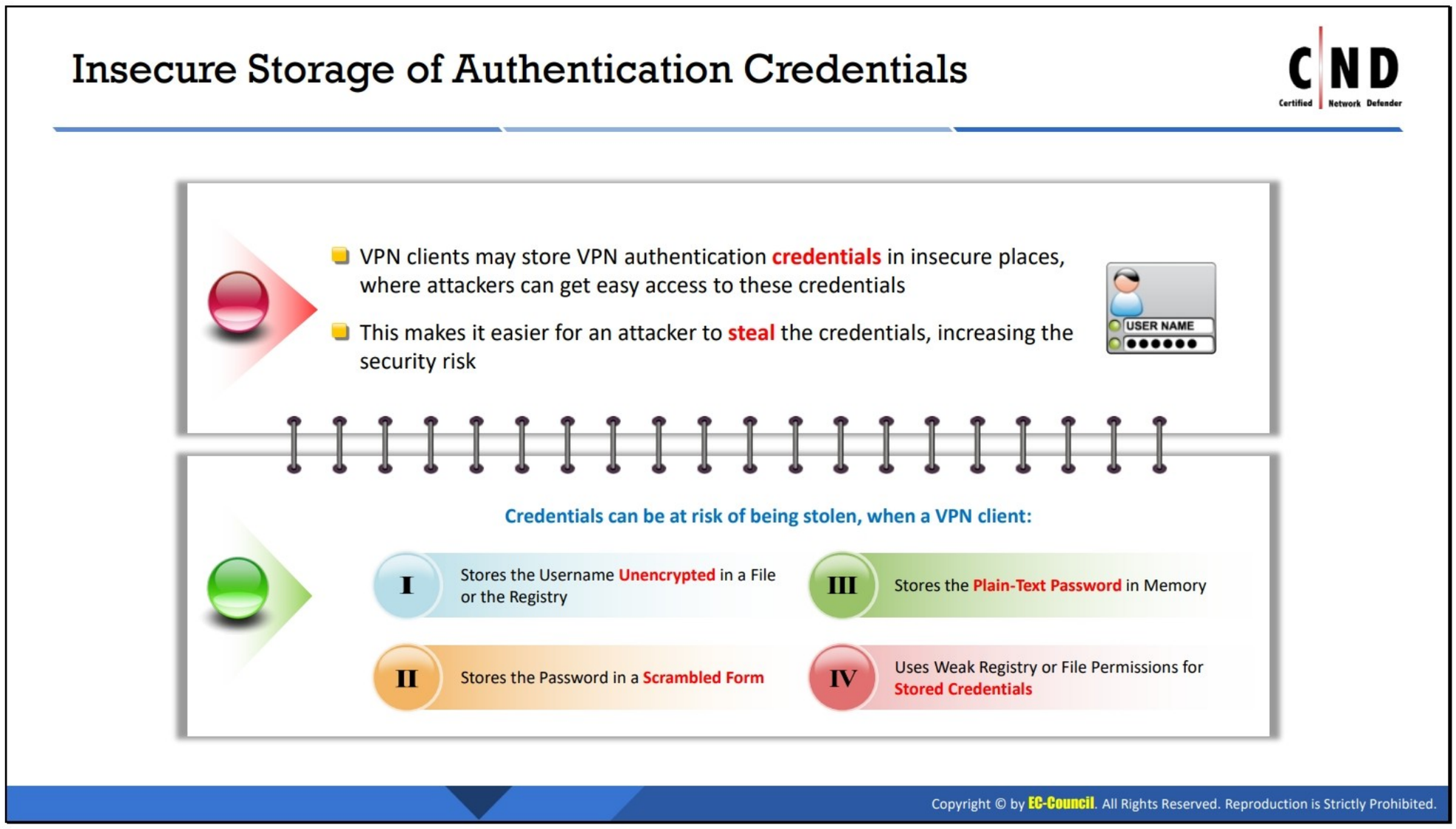
A VPN transmits data using various protocols such as TCP, IP, UDPC, IPsec, etc. Among these UDP is not a reliable transport layer protocol and completely depends on the application to provide reliability. The main technique UDP uses for reliability is retransmission with backoff which allows the application to replace any lost packets.

Because of certain vulnerabilities in transmission protocols, several VPN servers are prone to fingerprinting. For example, UDP needs backoff and with this, the attacker could fingerprint the VPN or Vendor ID.

The VPN fingerprinting technique allows the attacker to access useful information such as the type of connections implemented, devices used, and operating systems deployed. Some systems, such as Cisco PIX or Nortel Contivity, potentially reveal crucial data like the general type of devices deployed for building the network, while other systems display the software version details.

Attackers also trace out the IKE (Internet Key Exchange) scan to fingerprint the VPN server vendor and the version number of IPsec VPNs. The IKE-scan uses its own retransmission strategy to deal with lost packets and this helps attackers to fingerprint the VPN server. The IKE-scan log can find similar patterns to determine which IKE implementation a specific host has deployed.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

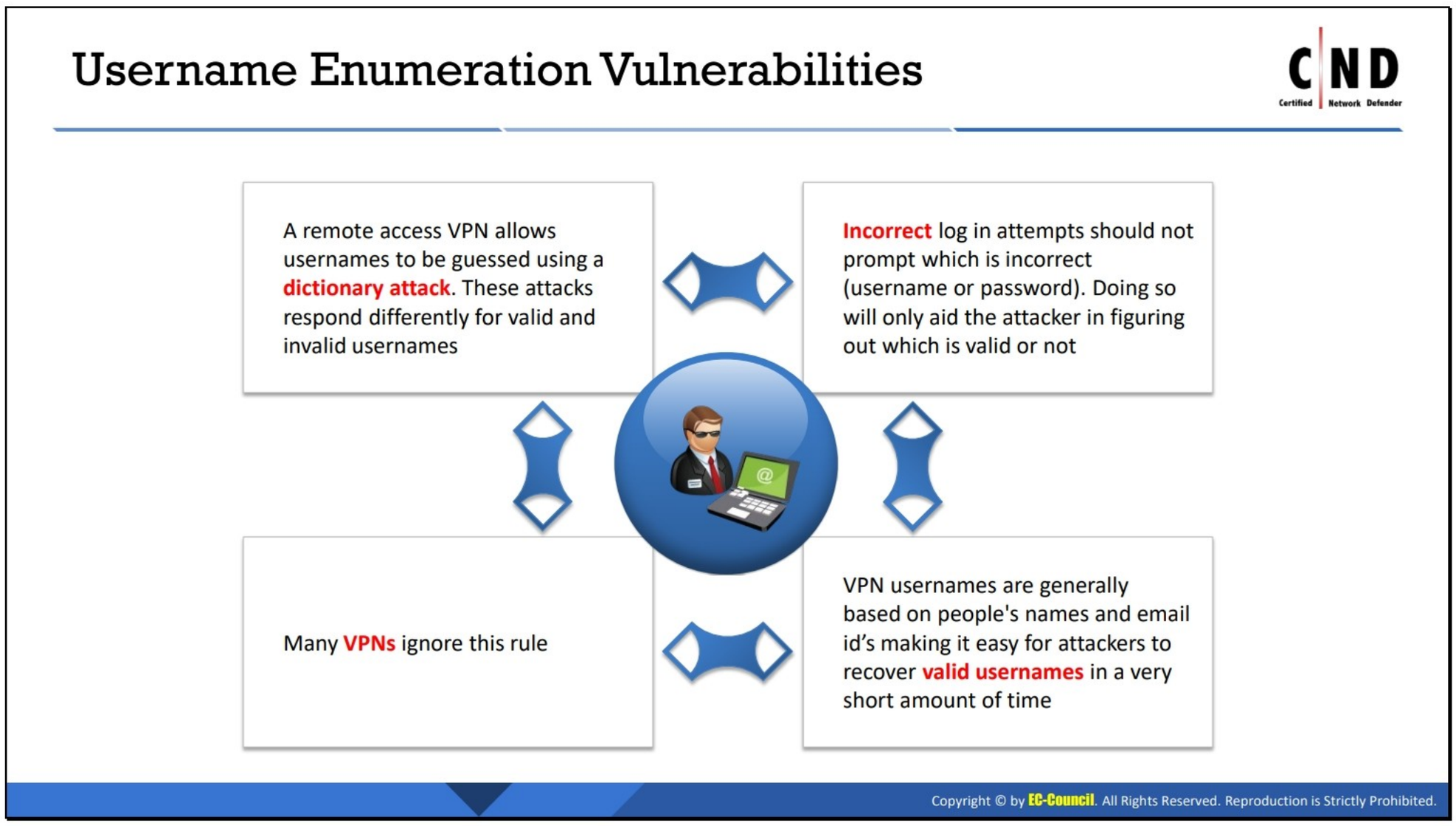


Insecure Storage of Authentication Credentials

There are certain security issues if the credentials are not stored and protected appropriately. These security issues are due to an insecure method of storing authentication credentials by VPN clients. Common VPN issues with authentication and credentials:

- **Storing the username unencrypted in a file or a registry:** Attackers can easily perform an offline attack on the authentication process if the credentials are stored in an encrypted format. This is possible if and only if the VPN is using the IKE aggressive mode.
- **Storing the password in a scrambled form**: If an attacker succeeds in gaining access to the client computer, they can easily gain the password. Even though the password is in a scrambled form, there is no key required to decrypt it. This provides for the attacker to implement a decryption algorithm to crack the VPN encryption.
- **Storing the plain-text in memory**: Passwords stored in plain-text are always susceptible to attack. Any user with access to the client machine can initiate the VPN client to dump the process memory using a tool known as pmdump. This tool will get access to the credentials.
- **Weak registry or file permissions for stored credentials**: Passwords are easy to get if they are not stored in a secure location and assigned with strict permissions.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Username Enumeration Vulnerabilities

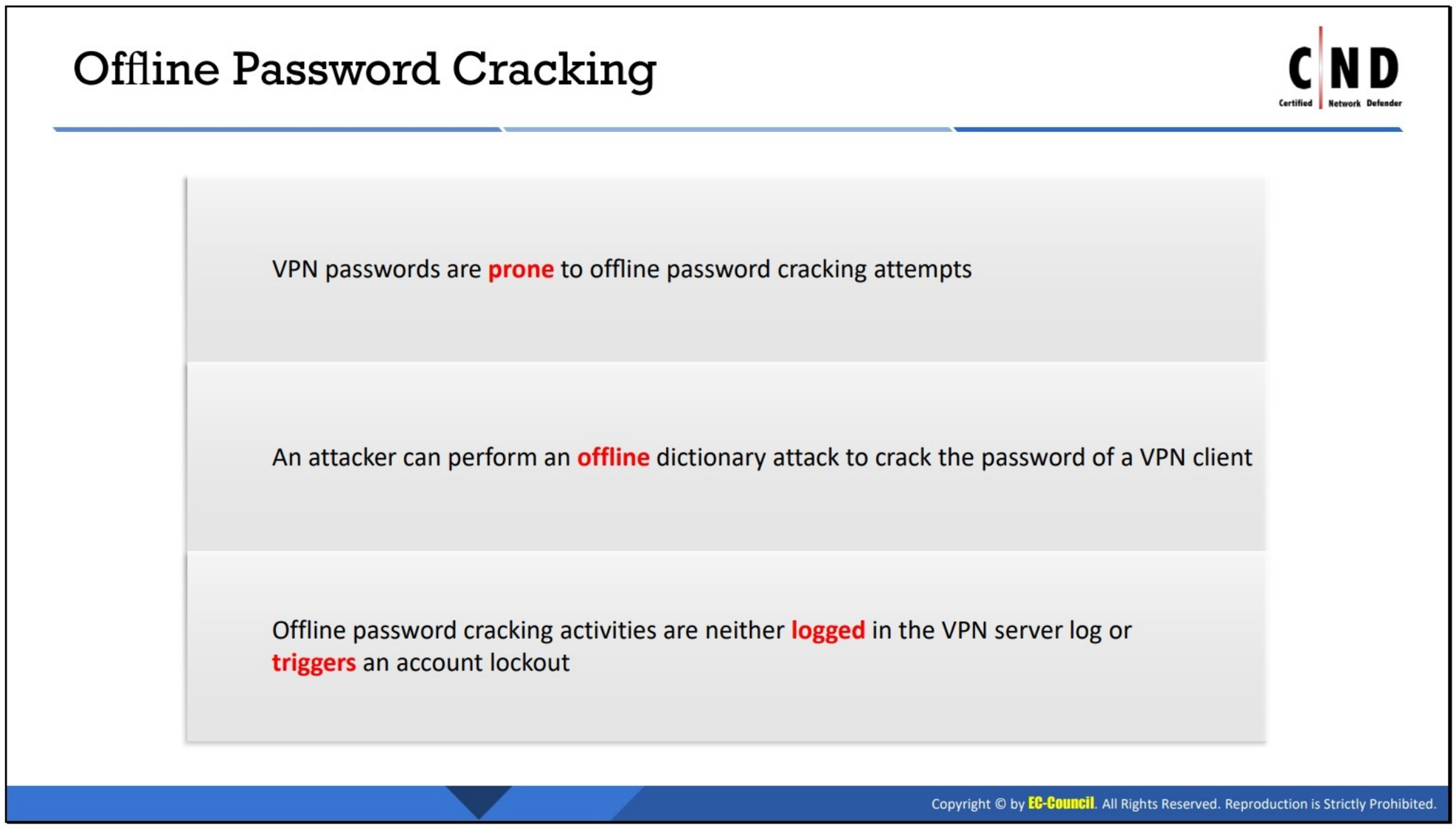
Many remote-access VPN uses the IKE aggressive mode with a pre-shared key authentication method. The client sends an IKE packet to the VPN server which responds using another IKE packet. These packets contain several payloads, including the identity payload sent by the client and hash payload sent by the server. The identity payload contains the username and the hash payload contains the password. Certain flaws identified in the flow of packets are as follows:

- Few VPN servers only respond to valid usernames.
- Few VPN servers respond with an error to incorrect usernames.
- Few VPN servers respond to valid and invalid usernames. The hash payload process uses invalid usernames with null passwords.

In all the above instances, the attacker confirms the difference between the valid and invalid usernames from their computational differences. An attacker guesses the correct password using the IKE aggressive mode can easily uncover the hash from the VPN server. This hash can be used with a brute-force-attack in order to gain the password.

Identifying all the possible types of attacks which can occur on the login page, account registration and password changes will help prevent username enumeration vulnerabilities.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



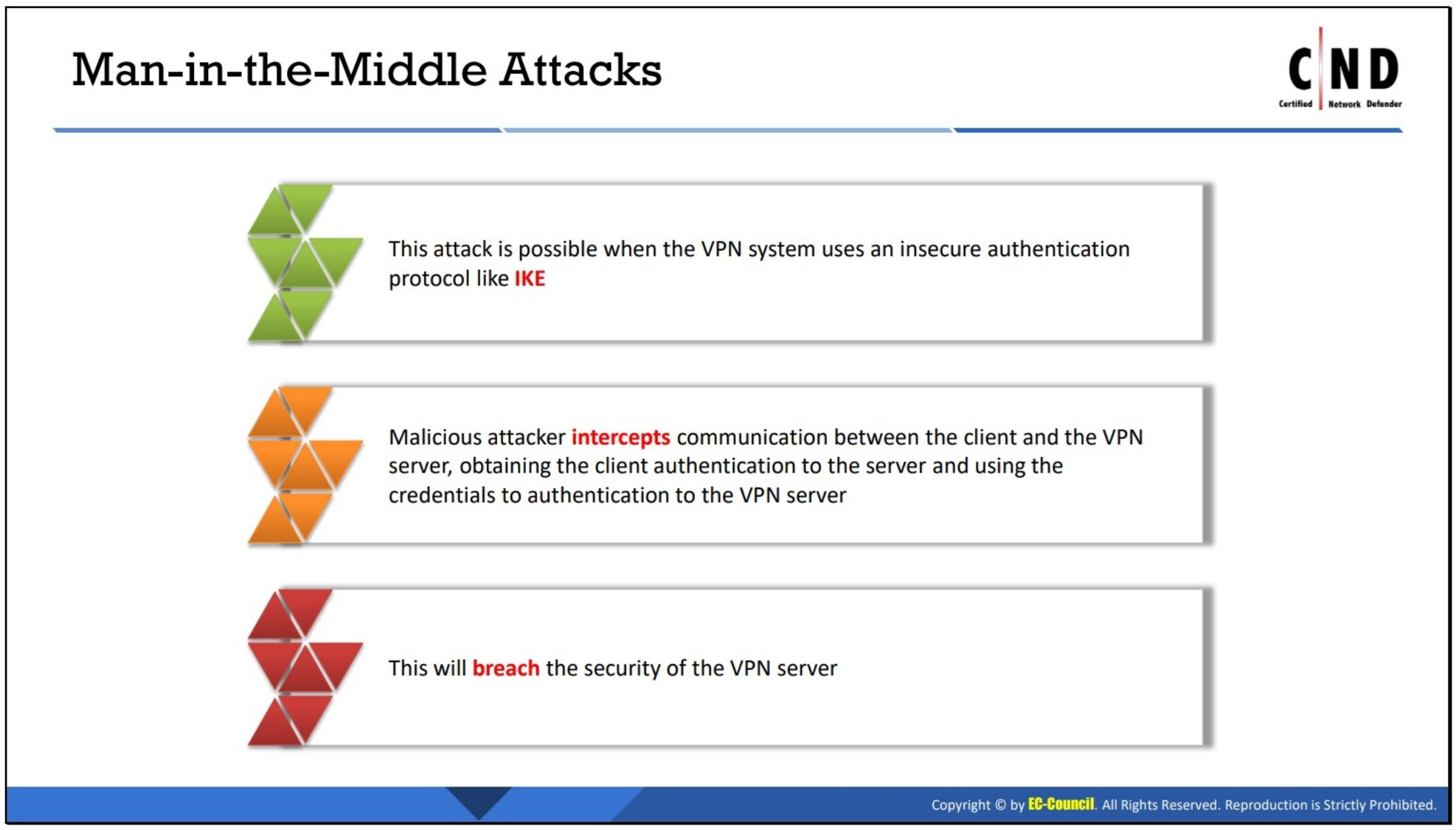
Offline Password Cracking

Offline password cracking is one of the most common flaws of a VPN. An attacker can perform an offline password crack by gaining access to the password hashes. Once the attacker gets the user credentials, they can easily gain the hash access from the VPN server.

When the VPN server gives a response to the client, it consists of the contents like a key exchange, identity, header, and hash. The server responding with the hash query from the client is called a hash responder. Since the responses are not in an encrypted form, an attacker gets access to the hash responder and uses a pre-shared key to perform the attack. The attack is offline and as a result, the VPN log server does not create any log entry. The attack goes unnoticed by the network defender.

Simple passwords and using simple words have increased the frequency of passwords being cracked. To prevent password cracking in the network, implement hash functions like MD5 and SHA.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

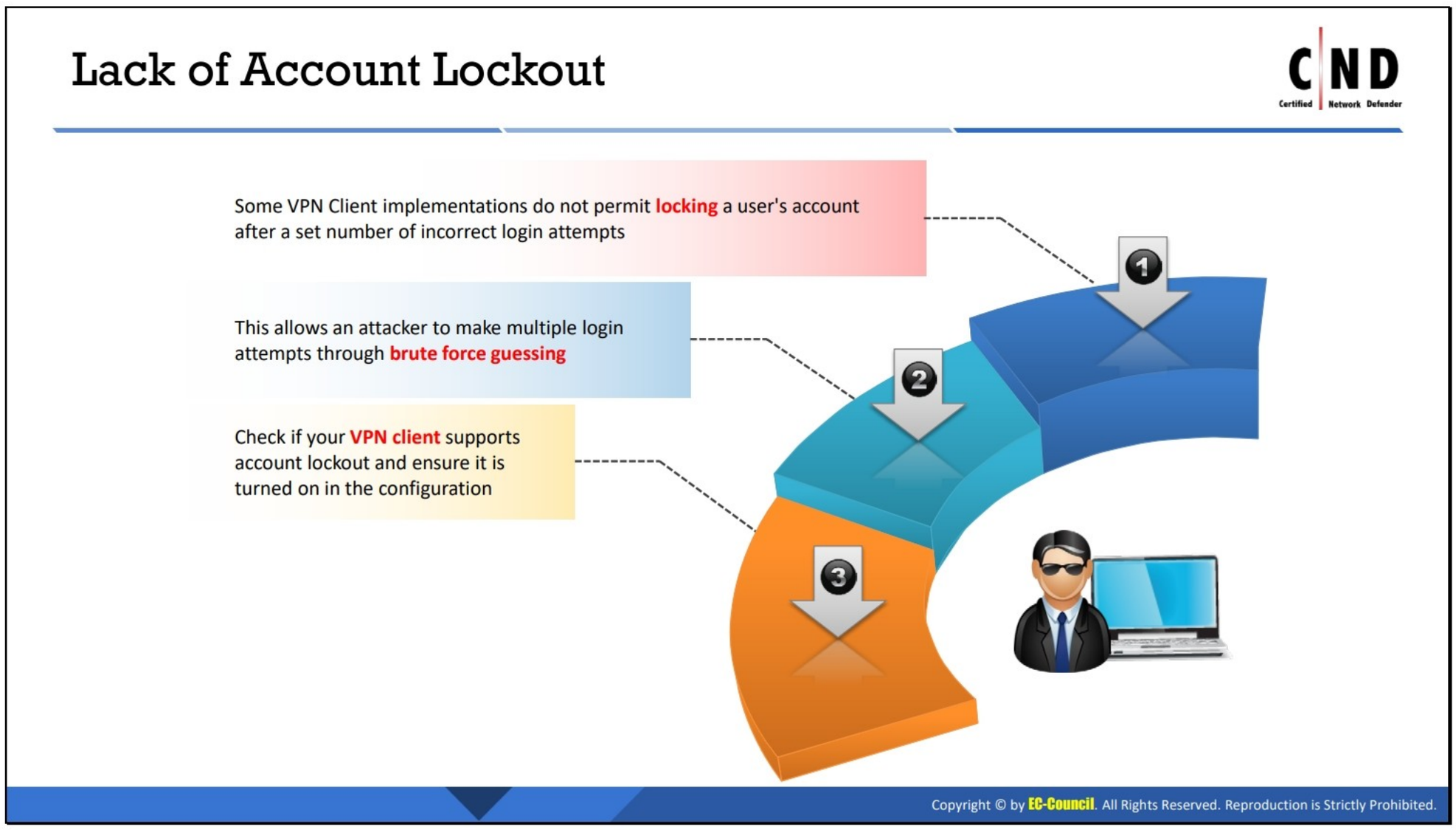


Man-in-the-Middle Attacks

Attackers may use insecure authentication protocols such as IKE to perform Man-in-the–Middle attacks on a VPN. An attacker intercepts the communication between the client and the server and obtains the client authentication to the server. The attacker then utilizes these authentication credentials to login and access the VPN server, allowing for complete control over the VPN Server.

Man-in-the-Middle attacks occur during data transfer through the VPN and allow an attacker to intercept, insert, delete, and modify messages, reflect messages back to the sender, replay old messages, and redirect messages.

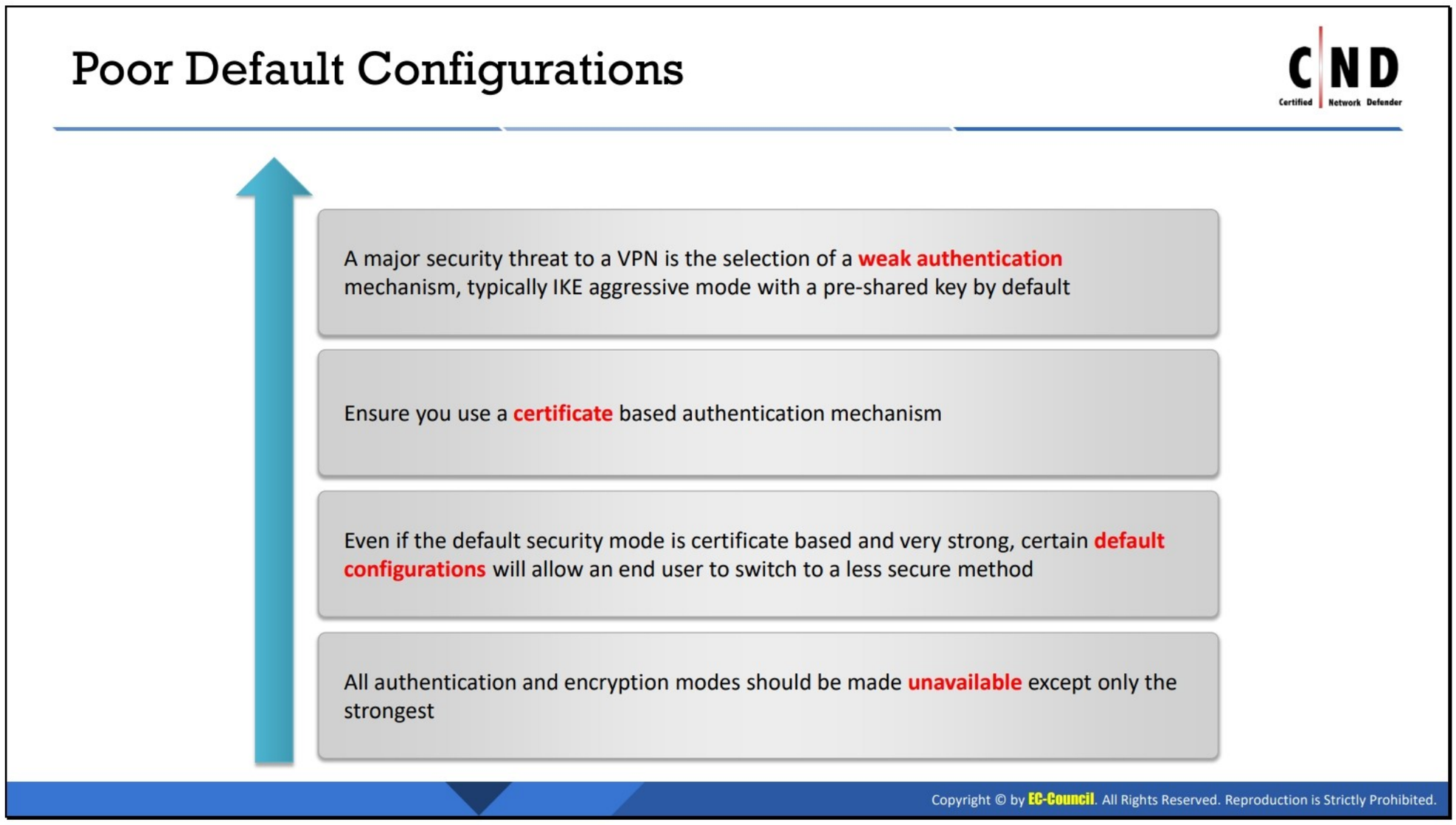
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Lack of Account Lockout

The main aim of using the account lockout feature is to restrict the number of login attempts to a certain limit and if anyone goes on trying login beyond the limit, the account will automatically get locked out. This feature prevents you from password cracking attacks such as brute force, dictionary attacks, etc. However, there are a few VPNs that do not provide an account lockout feature and this enables users to perform login attempts repeatedly. Attackers can take advantage of the lack of an account lockout feature to gain account credentials and it reduces the security of the account details.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Poor Default Configurations

Almost all organizations have an automated configuration set-up. However, if the organization remains with the default configuration for the VPN, attackers may exploit these default configurations to compromise the security of the VPN. The organization can go for a better and secure configuration management solution.

There are certain default configurations that allow an end user to switch to a less secure method like IKE, even in the presence of stronger certificates. It is mandatory to restrict all weak authentication and encryption modes. Normally, the end user does not attempt to change the default configurations of the system thinking the vendors provided the correct and secure configuration for the system. The default configurations support many ciphers and modes, ESP and AH. These may include both strong and weak ciphers. An attacker with access to the client machine can prompt the end user to use the weaker cipher which will make things easier for them. The end user may not notice the cipher and configuration was changed because the VPN still functions normally.

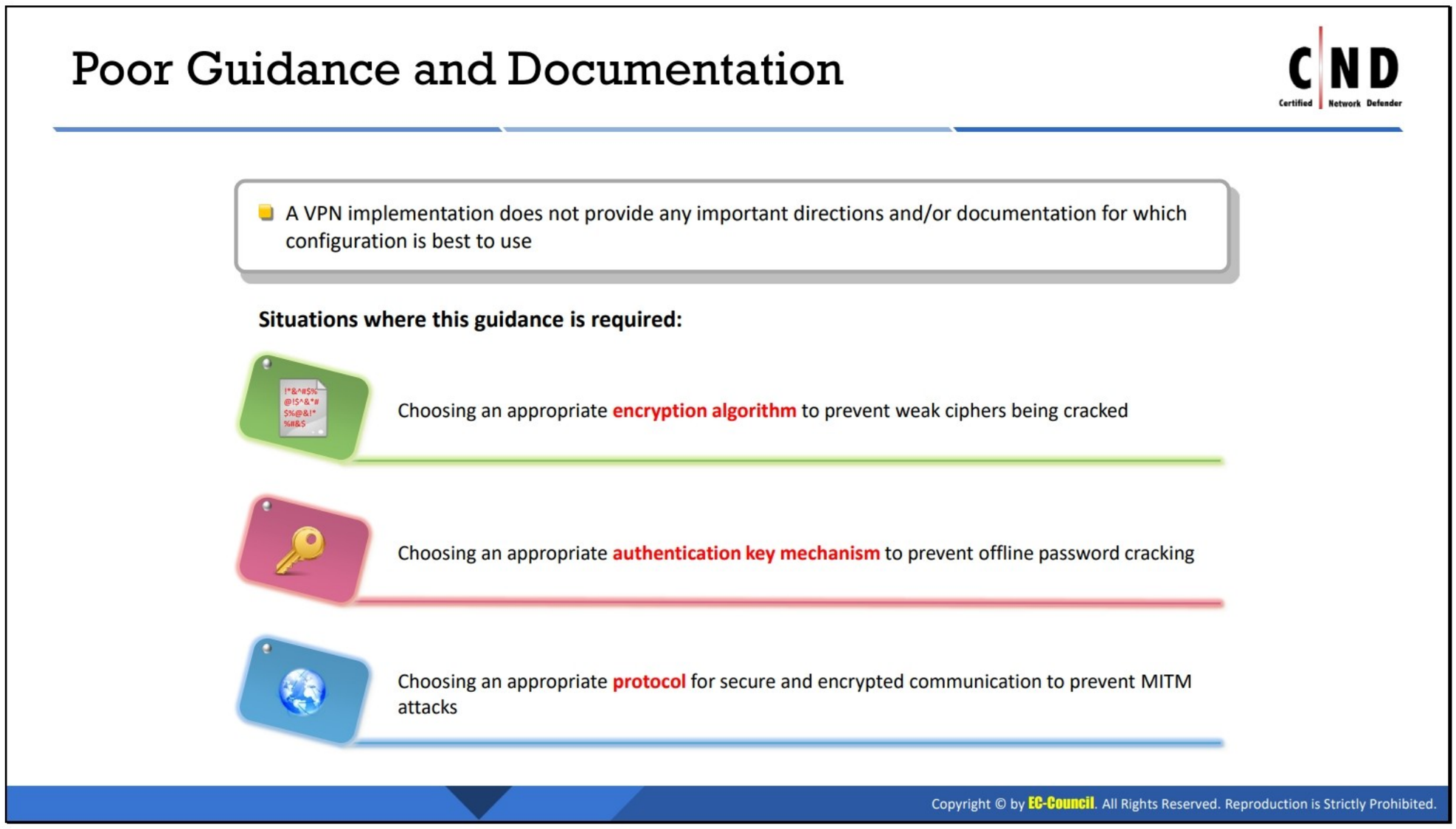
The selection of weak authentication mechanisms such as IKE aggressive mode with a pre-shred key allows attackers to gain authentication credentials. It must be ensured that mechanisms selected for protecting VPNs have a certificate-based authentication mechanism enabled.

Common Default Configuration Flaws

VPN vendors usually provide a default password, which users fail to change. The default passwords are known and it makes it easy for attackers to enter the network and get access to the systems.

- Users may change the configuration setting of the VPN without prior knowledge of the setting.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



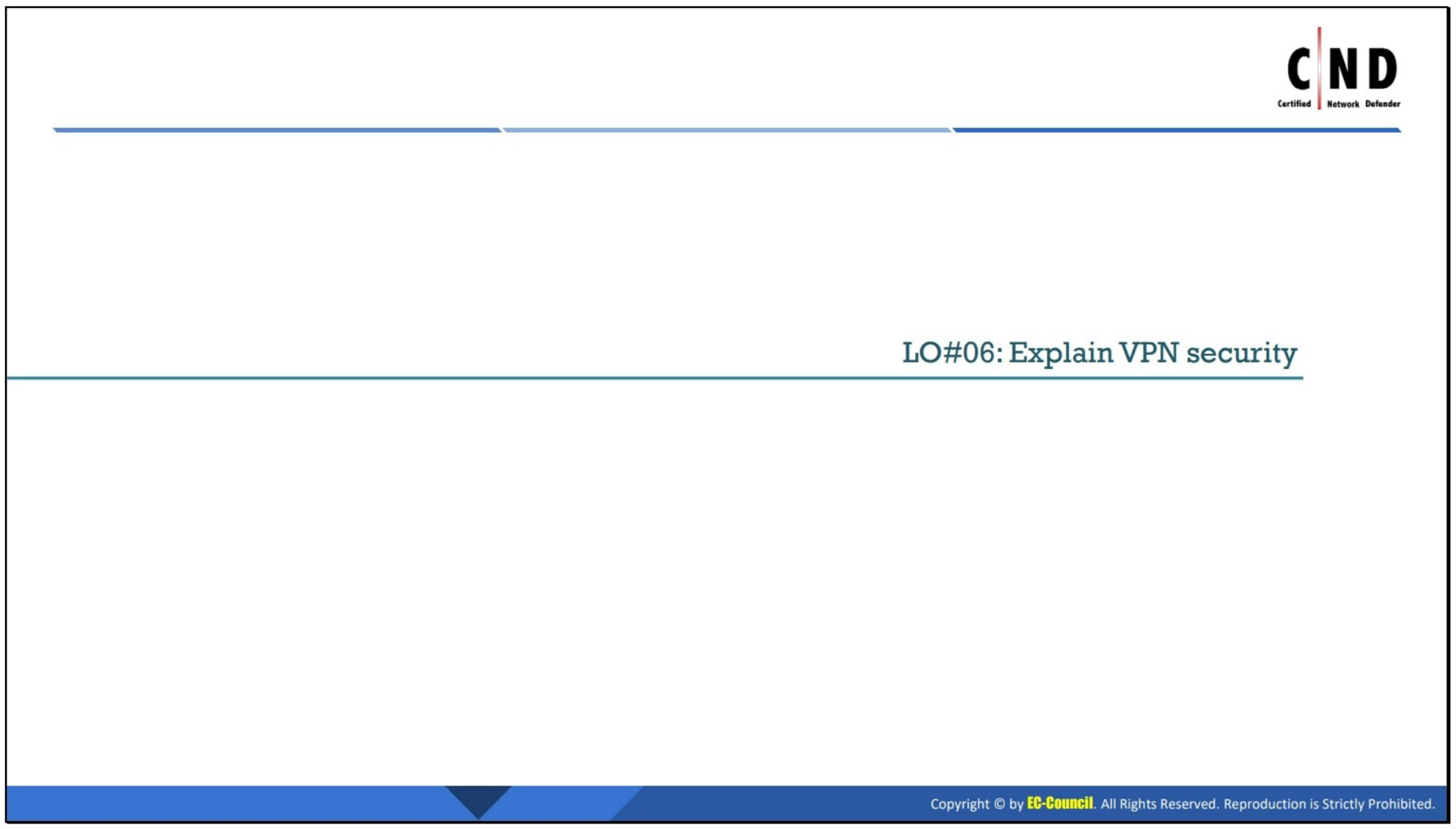
Poor Guidance and Documentation

There are instances where the end user is not aware of the correct configuration for the VPN. Improper guidance and documentation regarding the VPN implementation can lead the customers to make mistakes while using a VPN. Poor guidance can lead to security vulnerabilities in the configuration and implementation of a VPN. An incorrect implementation provides a way for attackers to gain access to the VPN. The following are situations where this guidance is required:

- Using weak ciphers like export-grade or single DES which can be cracked easily.
- While using the weak key authentication such as pre-shared key with IKE aggressive mode, which sends the username and vulnerable offline password to crack if a valid username is identified.
- Choosing the AH protocol which does not encrypt VPN traffic.

Users are not provided any warning message when the implementation is incorrect. Making it very difficult for the user to know the risks and dangers associated with the improper configuration.

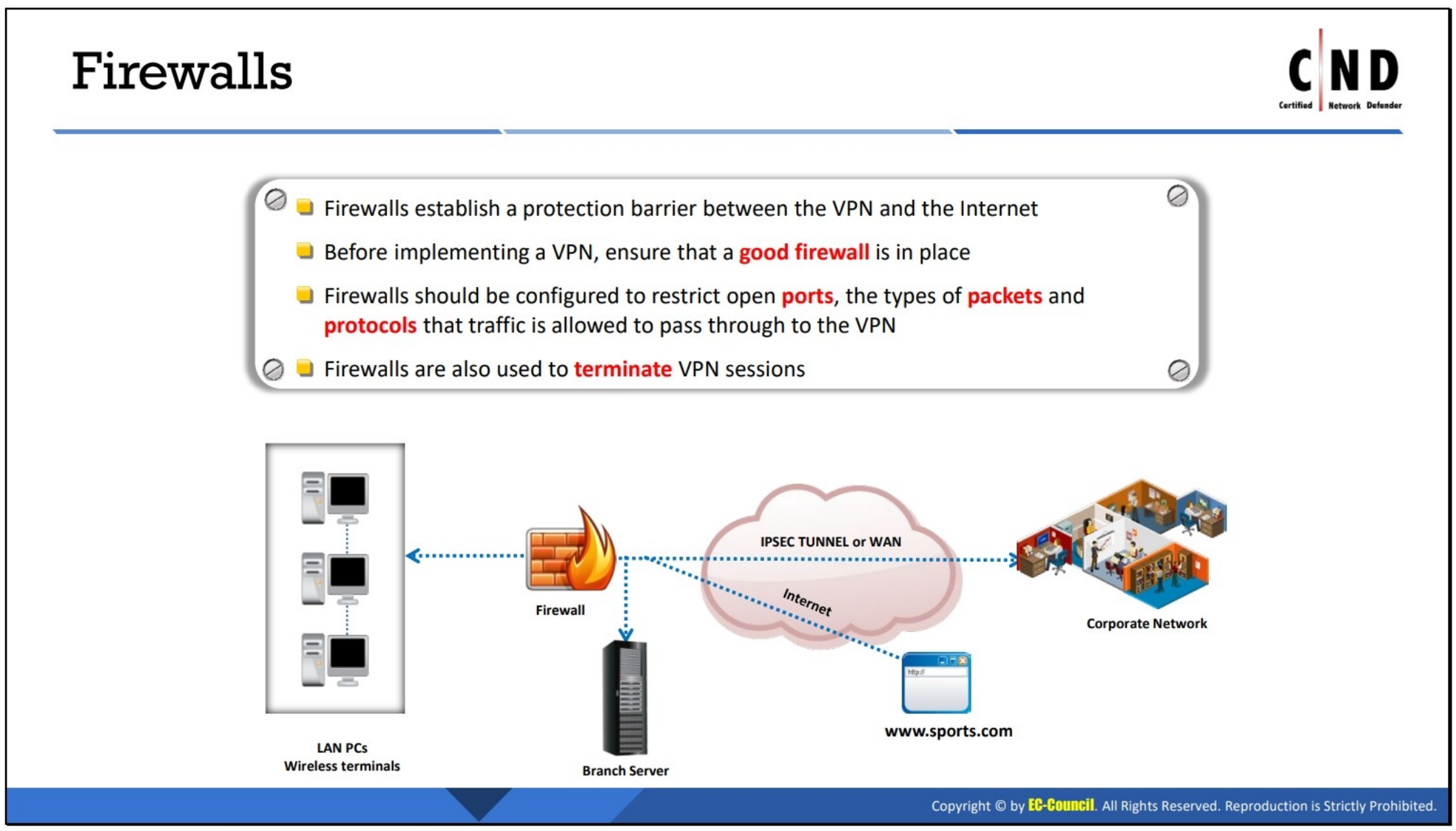
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#06: VPN Security

This section discusses various VPN security measures.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

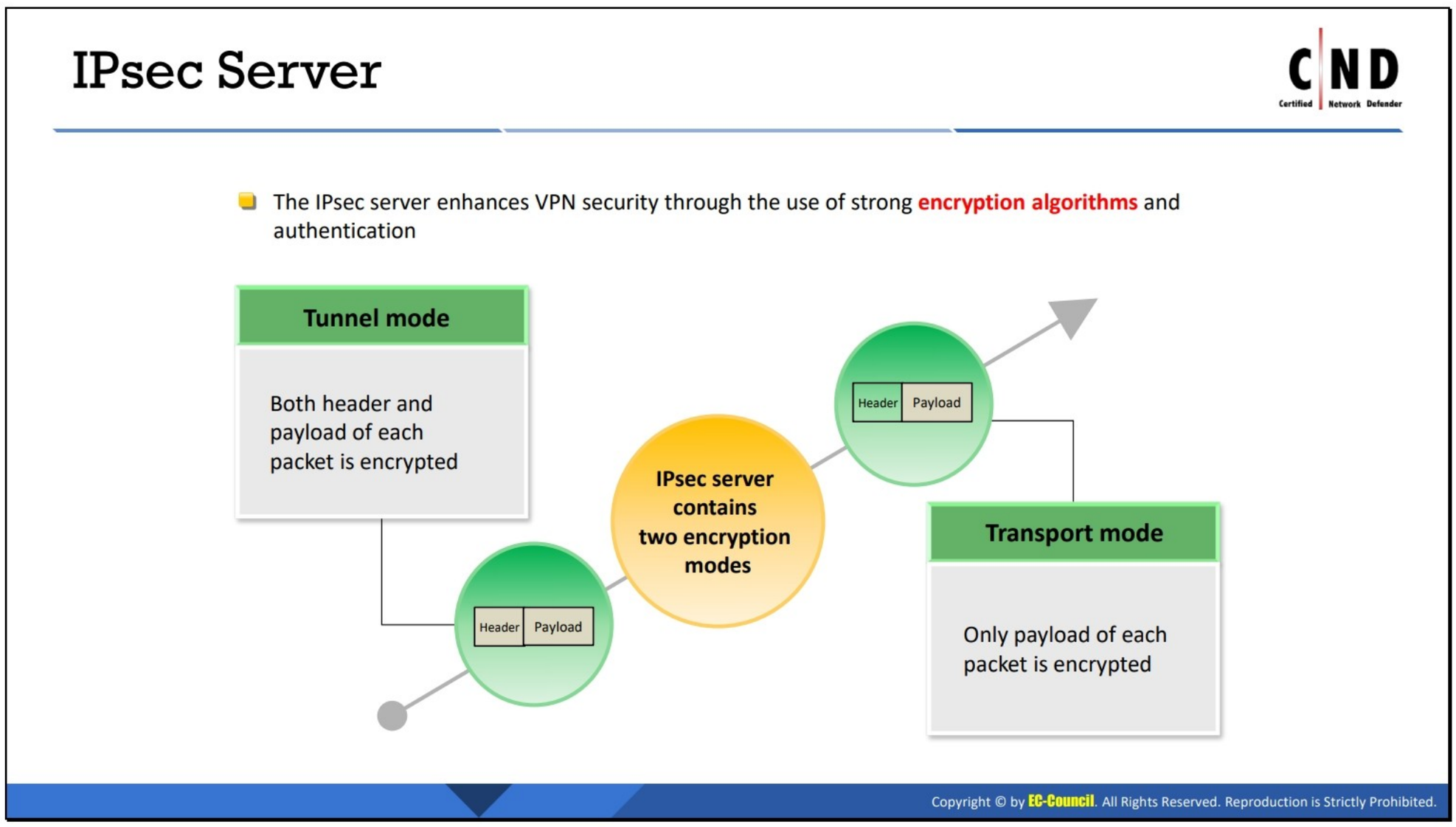


Firewalls

A firewall can allow or deny the flow of data through the network. These generally help in protecting the network from attackers. Firewalls can be used in two ways with a VPN:

- The VPN server is attached to the Internet and the firewall is located between the VPN server and intranet.
  - Here, packet filters are added in order to allow only VPN traffic to and from the IP address of the VPN server.
- A firewall is attached to the Internet and the VPN server is located between the firewall and intranet.
  - Here, the firewall has input and output filters on the Internet interface in order to maintain traffic and passage of traffic to the VPN server.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IPsec Server

The IPsec server consists of two types of encryption modes:

Transport Mode

This is the default mode for an IPsec server. These are generally used for end-to-end communication between a server and a client. In transport mode, IPsec encrypts the IP payload through an Authentication header (AH) or Encapsulating Security Payload (ESP) header. The IP payloads can be TCP segments (containing TCP header and TCP segment data), UDP message (containing a UDP header and a message data), and ICMP messages (containing ICMP header and ICMP message data).

AH does not generally encrypt the data and only provides authentication, integrity, and anti-replay protection. In an AH, it is possible to read the data but it denies any kind of change to the data. AH assess Integrity Check Value (ICV) over the source and destination address; therefore, it cannot be utilized to traverse NATs. ESP traverses NATs as it does not utilize the outermost address value for ICV calculation. When AH and ESP are used together, then ESP will be applied first, followed by AH that authenticates the entire new packet

- **AH in Transport Mode:** The AH can be used individually or along with ESP. The AH header will protect the entire packet. In transport mode, a new IP header is not created before the data packet, but a copy of the original IP header is placed with minor changes in the protocol ID. Hence, it failed to provide complete protection to all the fields in the IP header. AH is recognized in the New IP header with an IP protocol ID of 51.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

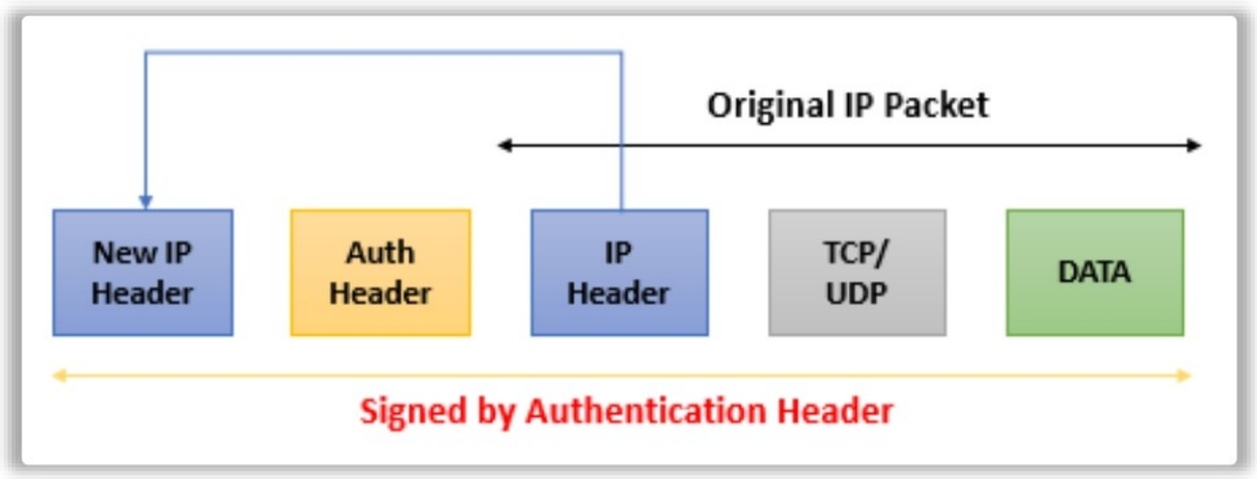


Figure C.6: AH in Transport Mode

- **ESP in Transport Mode:** The original IP header moved to the front position. If the sender's IP header will be placed in the front position by making minor changes to the protocol ID, it will prove that the transport mode will not protect or encrypt the original IP header and the ESP will be recognized in the New IP header with an IP protocol ID of 50.

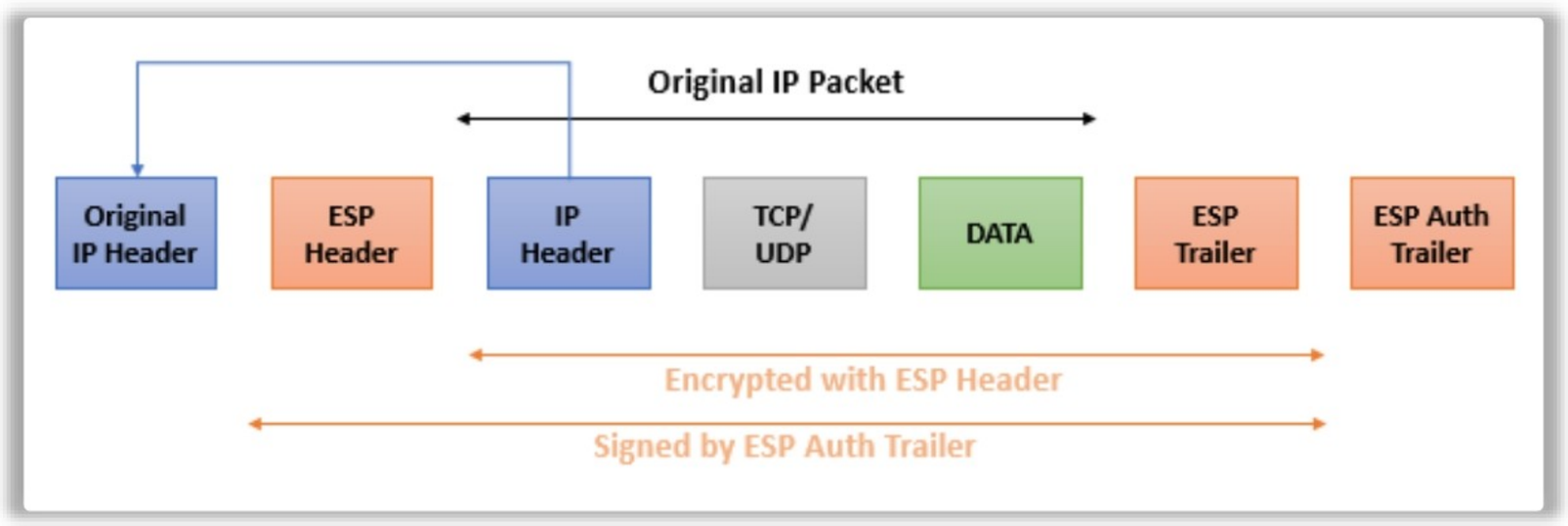


Figure C.7: ESP in Transport Mode

Tunnel Mode

In tunnel mode, IPsec encrypts both the IP payload and the header to protect an entire IP packet by encapsulating it with an AH or ESP header and an additional IP header. This mode is useful for protecting traffic between different networks and is primarily used for interoperability with gateways.

The tunnel mode of IPsec is generally implemented in configurations such as gateway-to-gateway, server-to-gateway and server-to-server. The IPsec tunnel mode is useful in protecting traffic while it is passing through untrusted networks.

- **AH in Tunnel Mode**: The AH header will be used individually or along with ESP. It will defend the entire packet. However, AH does not safeguard all the fields of the New IP Header due to some change in transit. It will safeguard everything that does not change in transit. AH is recognized in the New IP Header with an IP protocol ID of 51.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

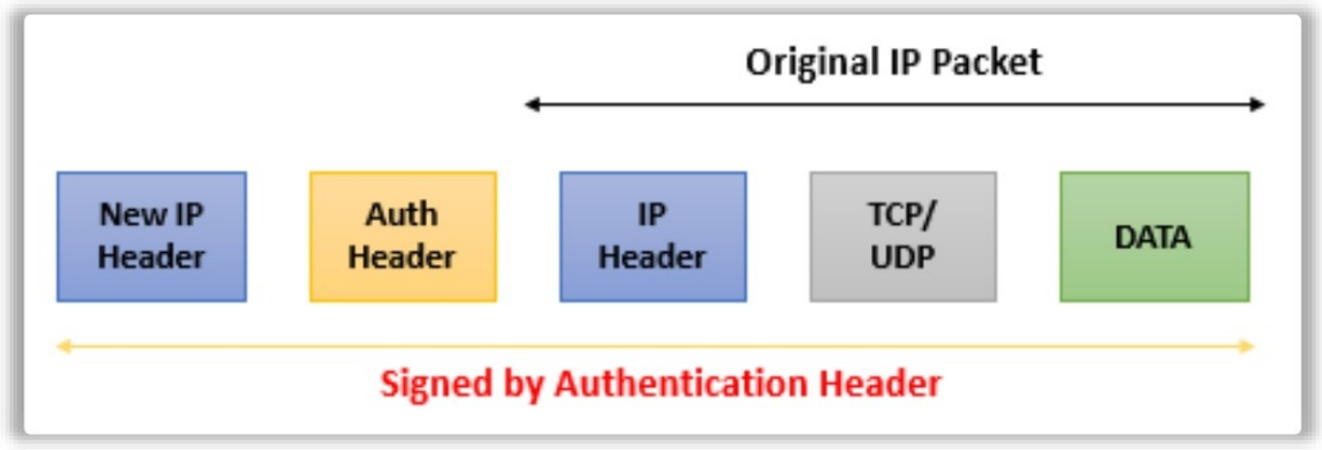


Figure C.8: AH in Tunnel Mode

- **ESP in Tunnel Mode**: ESP is recognized in the New IP header with an IP protocol ID of 50.

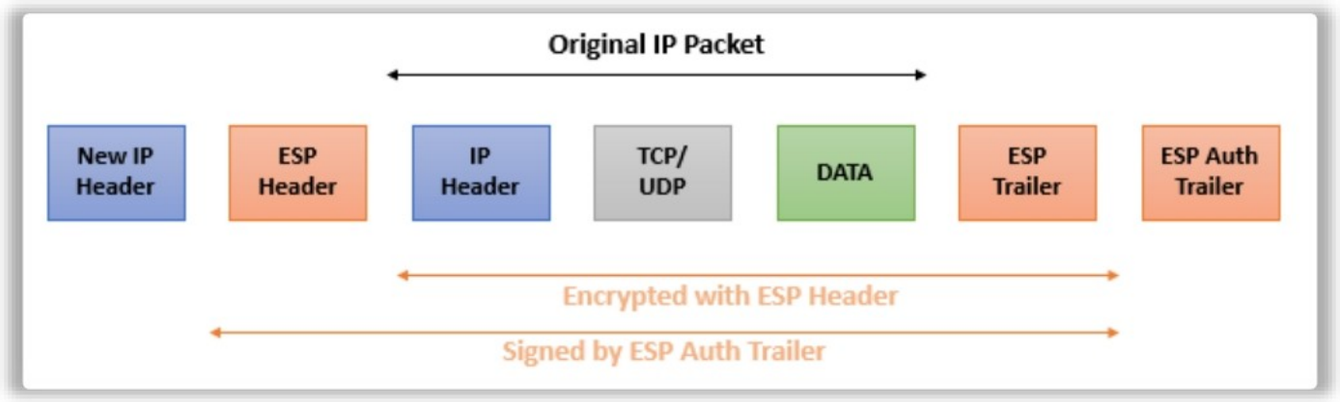


Figure C.9: ESP in Tunnel Mode

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AAA Server

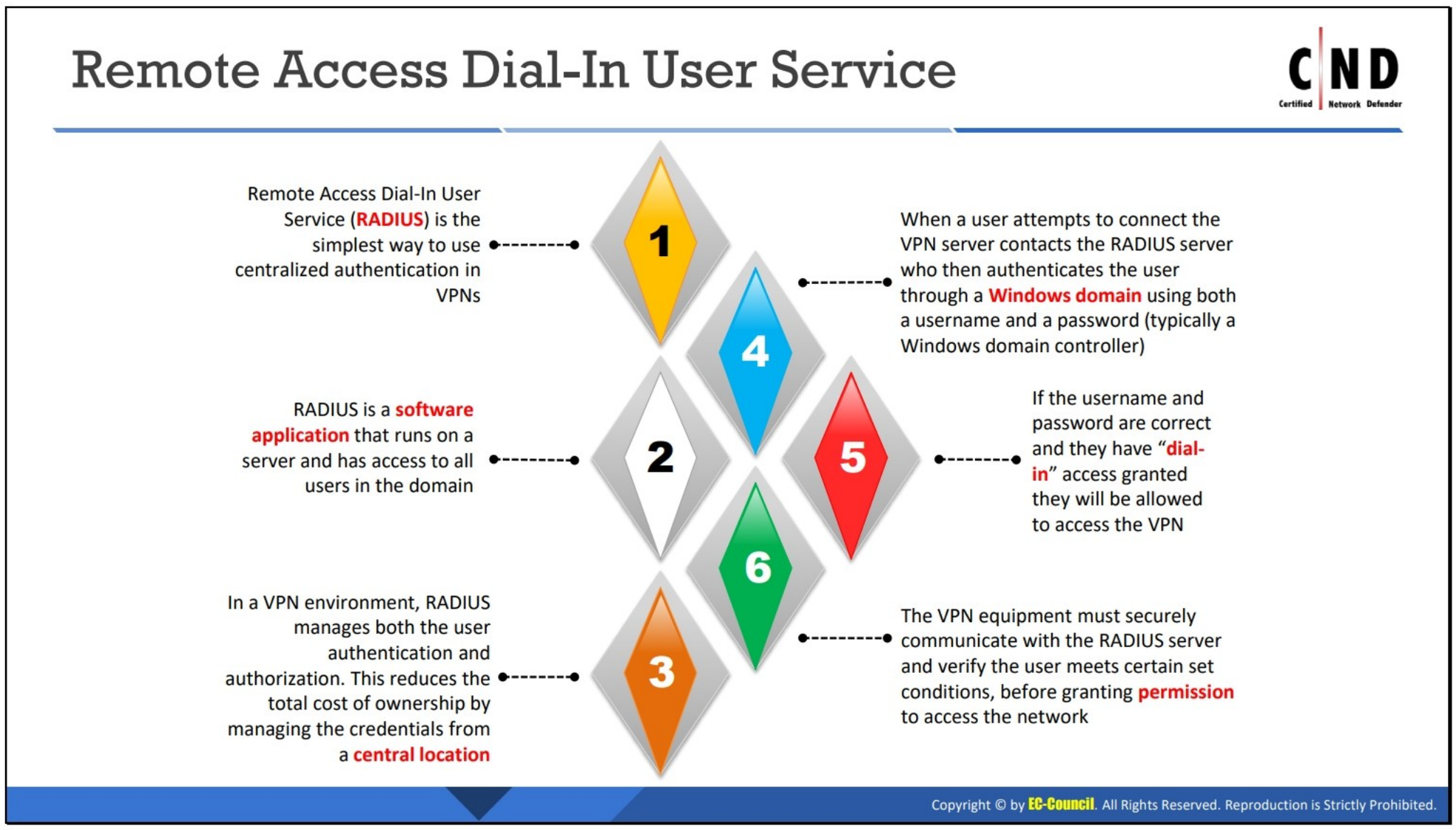
Authentication, Authorization, and Accounting (AAA) provides additional secure access in a remote-access environment. An AAA server provides users an extra layer of protection and control when compared to an ACL alone. The access control list (ACL) enables outside users to access TELNET present in the DMZ network. AAA gives permits to only a few users for accessing the application after proper authorization and authentication have occurred. This can be implemented using:

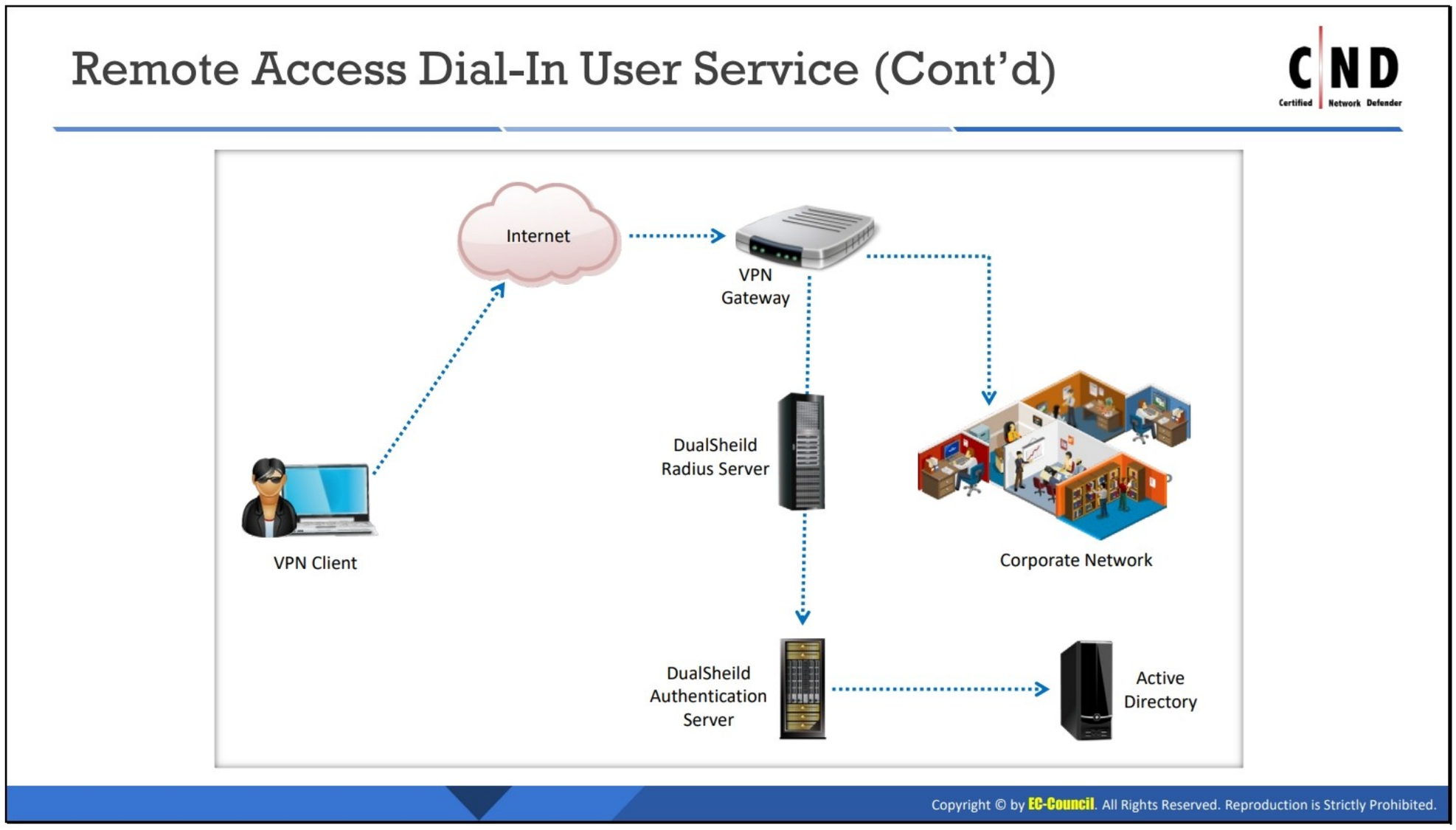
- Who you are (authentication) by verifying the user credentials such as username and password
- What you are allowed to do (authorization) is verified in order to offer access controls such as management commands, network access, and VPN access
- What do you actually do (accounting), refers to what type of traffic the users access through the VPN. This option tracks traffic that passes through the VPN and records all user activity

The authentication protocols used for an AAA server are:

- RADIUS
- TACACS+
- RSA SecurID
- Windows NT
- Kerberos
- LDAP

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Remote Access Dial-In User Service

RADIUS is a client/server protocol which authenticates and authorizes dial-in-users to access the system or device. RADIUS maintains profiles in their databases enabling the remote servers to share the data enabling a centralized administration of data. Companies using a VPN network implements RADIUS for data authentication.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In RADIUS, the VPN server interacts with the RADIUS server once the user attempts a connection. The RADIUS server authenticates the user using their credentials. The user is granted access if and only if the user provides the correct credentials and has dial-in access. The RADIUS server sends a RADIUS message to the RADIUS client in response to the request for authentication.

The RADIUS messages are sent as user datagram protocol (UDP) messages and the UDP payload of a RADIUS packet can include only one RADIUS message.

Various RADIUS message types are:

- Access-request: Sent by the RADIUS client to request authentication.
- Access-accept: Sent by the RADIUS server in response to the access-request message.
- Access-reject: Sent by access-server to the RADIUS client informing them the connection request is rejected.
- Access-challenge: Sent by the RADIUS server to the RADIUS client in response to the access-request from the client.
- Accounting–request: Sent by the RADIUS client to request the information for a permitted connection.
- Accounting–response: Sent by the RADIUS server in response to the accounting-request message from the RADIUS client.

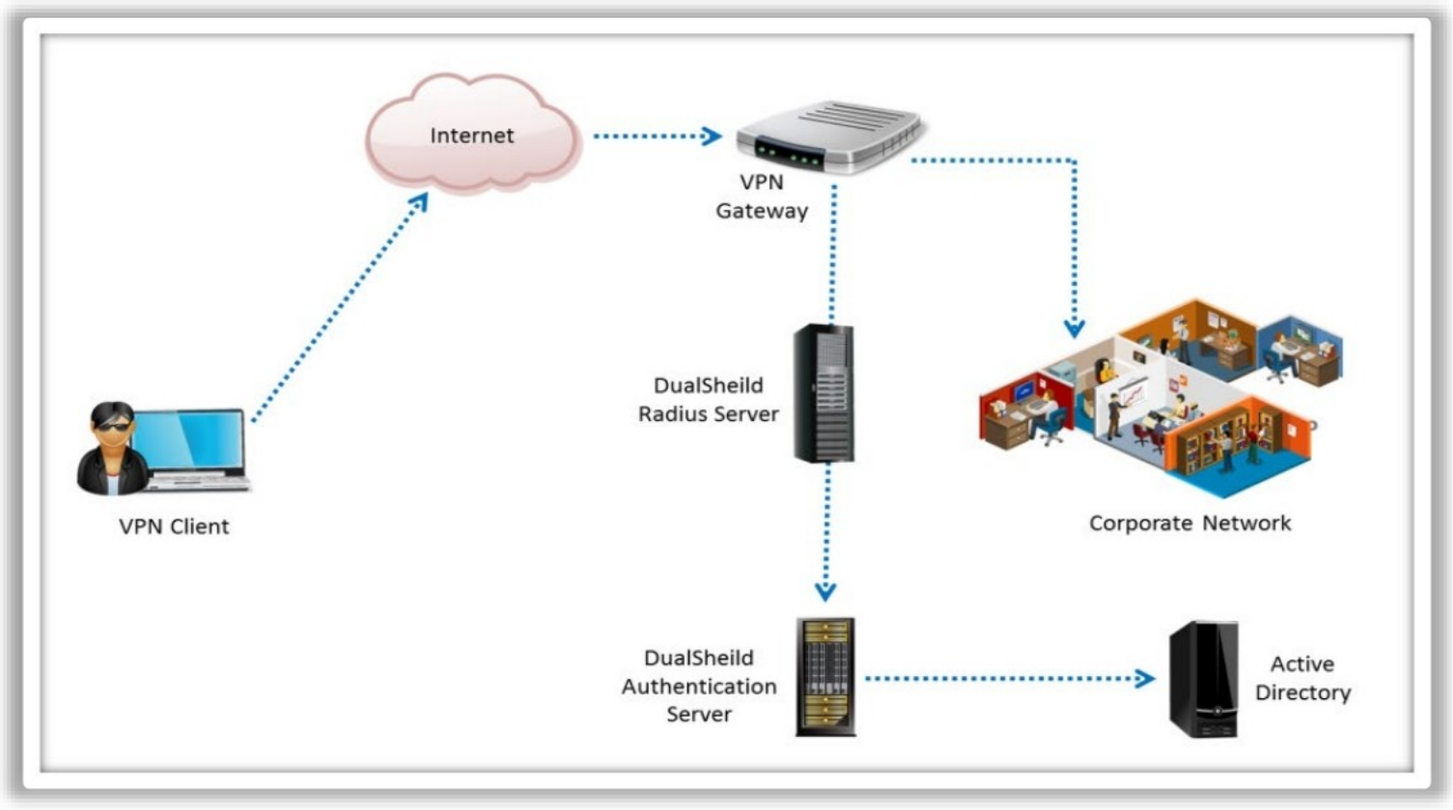


Figure C.10: RADIUS

A RADIUS message consists of a RADIUS header and RADIUS attributes. The RADIUS attributes provide information regarding the number of connection attempts, username, password, service requested by the user, etc. Each has a separate RADIUS attribute and they share information between RADIUS servers, RADIUS clients, and RADIUS proxies.

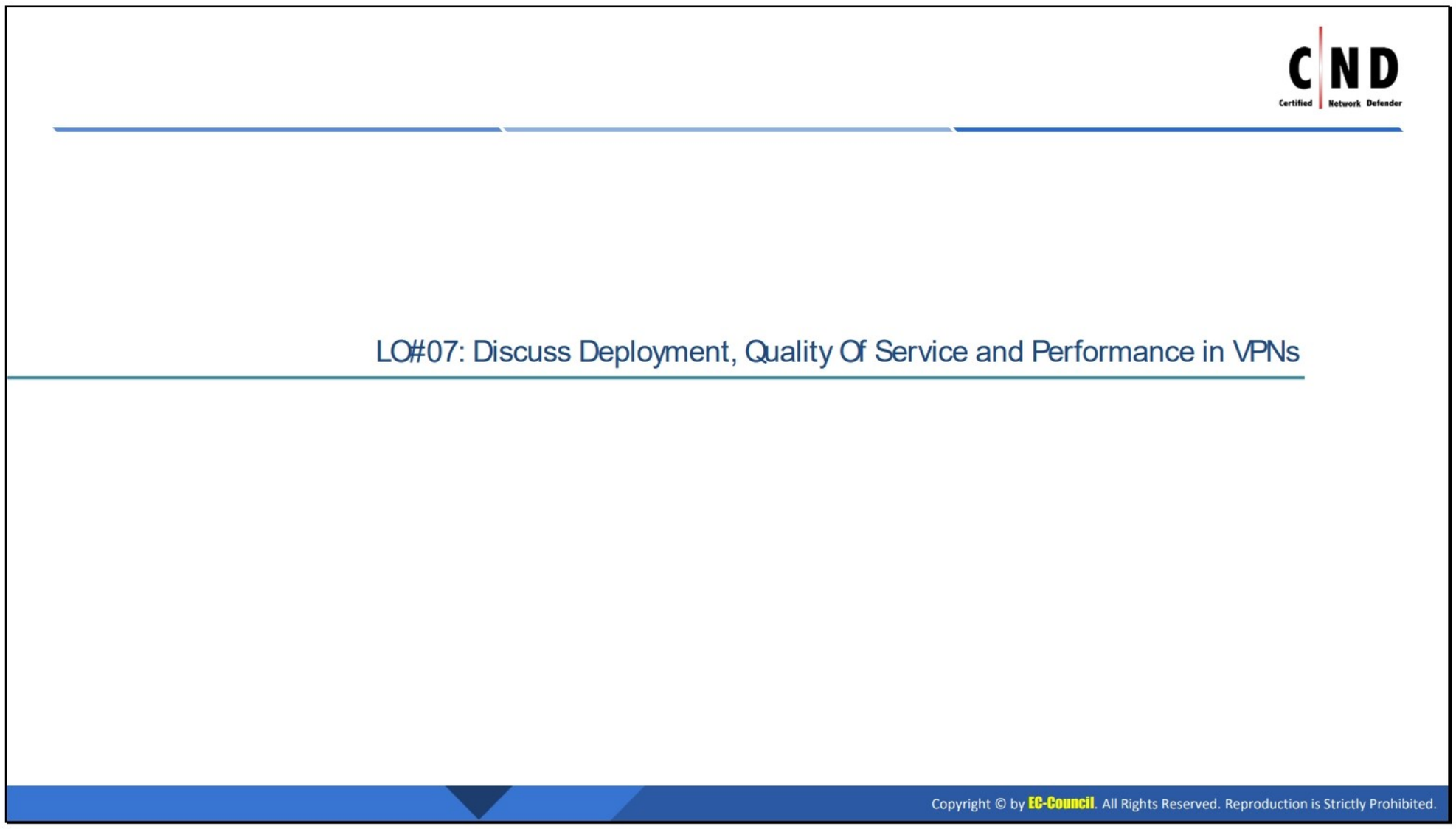
The RADIUS components are:

- Access clients
- Access servers

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- RADIUS proxies
- RADIUS servers
- User account databases

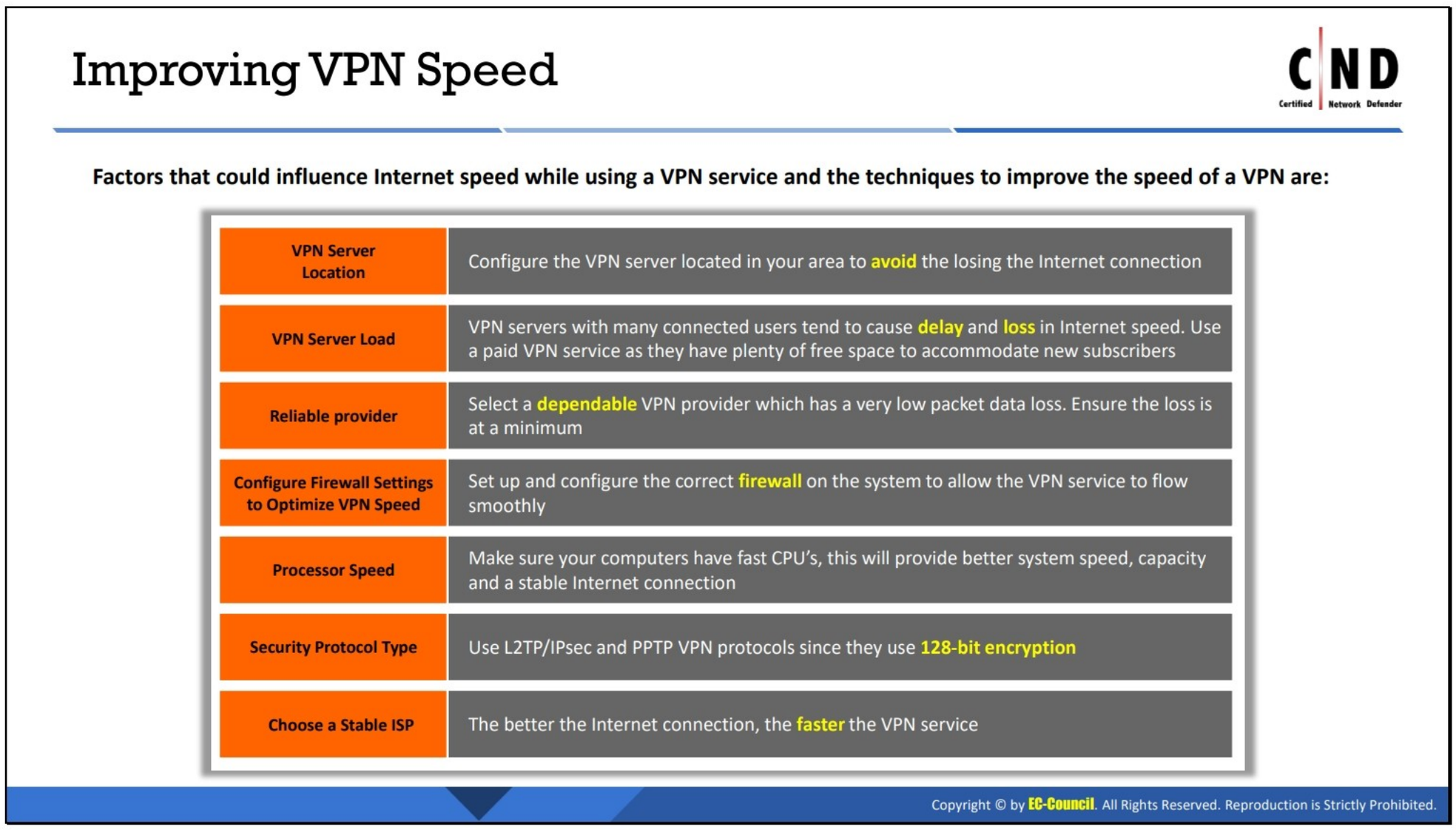
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#07: Deployment, Quality of Service and Performance in VPNs

This section discusses the concepts of VPN deployment and best practices for improving quality of service, and performance in VPNs.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Improving VPN Speed

Many people using a VPN connection are concerned about the speed of the VPN affecting their internet connection. Factors influencing VPN speeds are:

VPN Server Location

A VPN server at distance would take lots of time for the data packet to move back and forth through, use a VPN Server located near your area to avoid any loss of Internet bandwidth. This will help in improving the VPN speed.

VPN Server Load

A VPN server with many connections causes a delay and loss. To avoid this, use a paid VPN service since they have plenty of free space to accommodate new subscribers.

Reliable Provider

A good and reliable VPN provider offers a zero percent data packet loss for their VPN services. For better performance select a dependable virtual private network provider which has a minimum amount of packet data loss.

Configure Firewall Settings to Optimize VPN Speed

Generally, system firewall settings affect the CPU speed and that affects the VPN and Internet speed. To increase the VPN speed, set up the correct firewall on the system to allow the VPN service to flow smoothly.

Processor Speed

In order to avoid losses in bandwidth and connection, furnish your computer with a faster and better CPU or processor to have better system speed, capacity, and a stable internet connection.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Security Protocol Type

The VPN speed depends upon the level of security encryption. A VPN solution provider offers basic VPN security protocols like OpenVPN, SSTP, L2TP/IPsec, and PPTP. To get a good and stable Internet connection, opt for L2TP/IPsec and PPTP VPN protocols as they use 128-bit encryption.

Choose a Stable ISP

The speed of an Internet connection depends on the ISP limitation, which in turn influences the speed of the connection for the VPN subscription. The higher the Internet connection limit, the faster is VPN service.

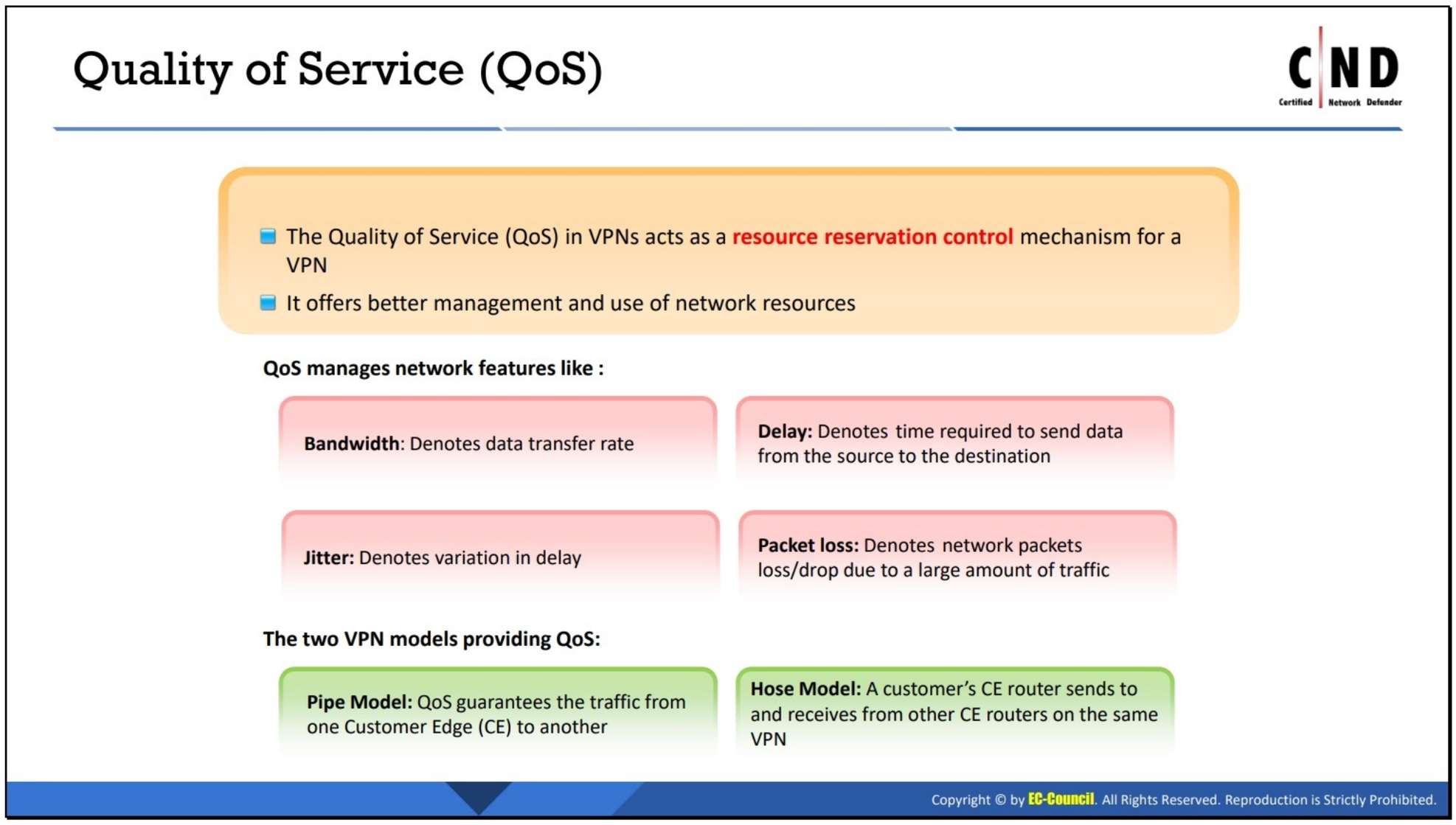
Choose a Wired Connection

Wired connections increase the speed and minimize the latency. Wireless connections use a shared connection between the devices affecting the speed of the VPN.

Choose a Proper Device

Certain devices are incapable of handling overhead due to the encryption of a VPN tunnel. These devices are best used with a better processor.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Quality of Service (QoS)

Quality of Service in VPNs is an end-to-end mechanism that provides different services to different applications, users, or data flows according to business requirements. Service providers provide a quality service by defining the service level agreement (SLA) which further describes the QoS factors. QoS is required in a VPN as different applications have different requirements and it is mandatory to provide all required services so the VPN functions properly. Factors that affect the QoS:

- **Bandwidth**: Determines the data limit applicable during a data transmission
- **Delay**: Total time required to transmit data from the source location to the destination
- **Jitter**: Variation in latencies for packets in a given data stream
- **Packet loss**: Loss or ID ordering of data packets in a stream
- **Throughput:** Number of bytes received per second at the destination
- **Network Address Translation (NAT)**: The presence of Network Address Translation (NAT) or proxy devices between the client and the gateway can affect the connectivity in an undesirable manner. The connectivity always needs a client configuration prior to the implementation of the tunnel.
- **Goodput (Packets)**: The ratio on the number of data packets sent versus the total number of packets transmitted in the network.
- **Goodput (Bytes)**: The ratio of bytes of data sent versus the total number of bytes transmitted in the network.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

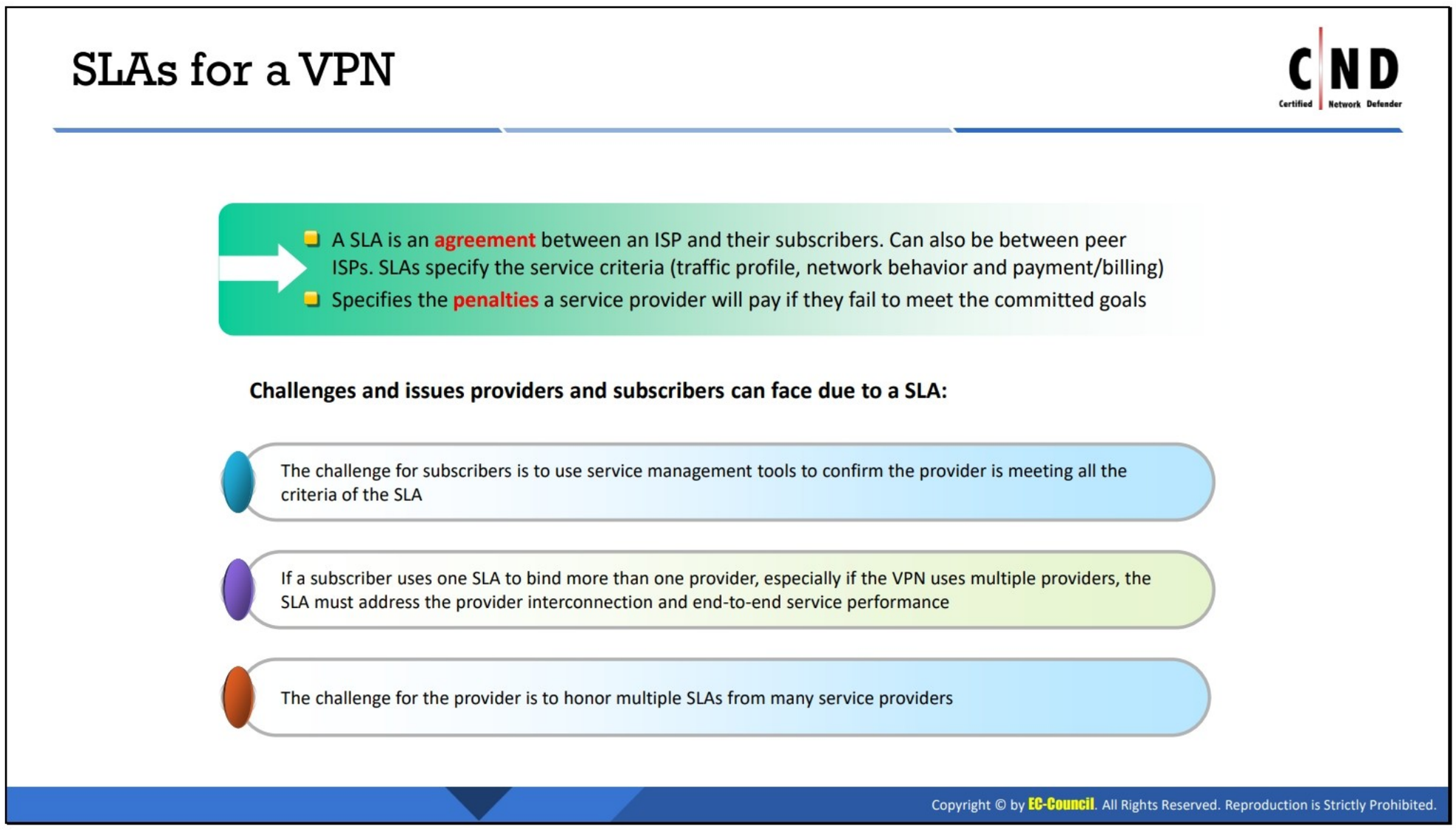
- **Data Dropped**: Data lost or dropped at the destination may be due to improper access to the medium.

An SSL (Secure Socket Layer) VPN is used to provide the remote user with access to web applications, client/server applications, and internal network connections. It provides a secure way for mobile users to access network resources. Deployment considerations of SSL VPNs include:

SSL VPN is categorized into:

- **SSL portal VPN**: Allows secure access of network devices by enabling a single SSL connection to a web site. Portal refers to the website that permits the user to access other services.
- **SSL tunnel VPN**: Enables web browsers to access multiple network services, applications, and protocols. This is facilitated by a tunnel under the SSL. The SSL tunnel allows a web browser to access services that cannot be accessed by SSL portals.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



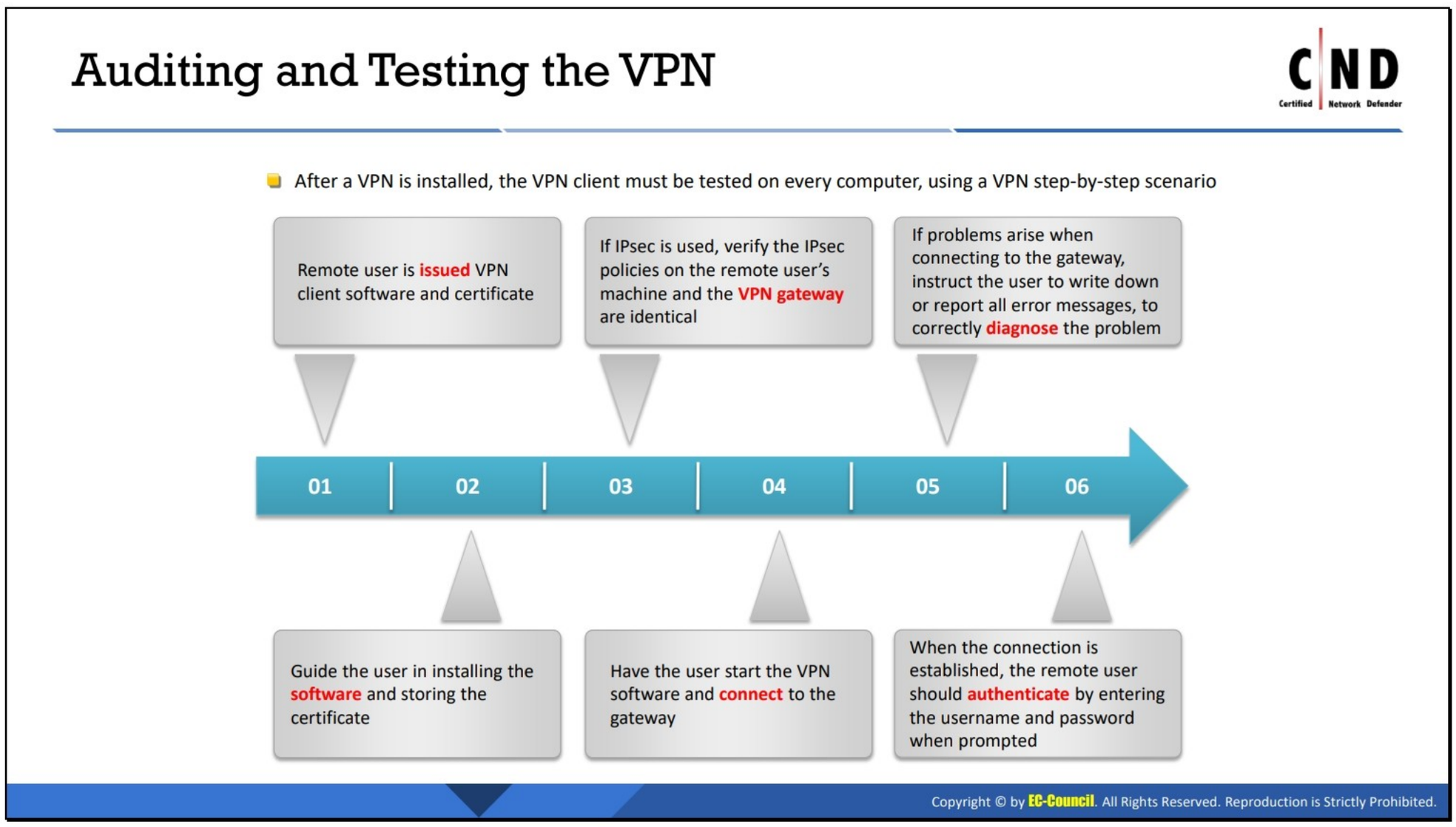
SLAs for a VPN

A service level agreement (SLA) is a contract between the ISP, its subscribers, and between any peer ISP's. The SLA specifies traffic profile, network behavior, payment/billing etc., and the penalties are given for not following or meeting the prescribed criteria. The SLA can be fixed through a phone call, fax or using bandwidth brokers (BBs). Bandwidth brokers are agents allocating resources and controlling the traffic of the administrative domain. These brokers keep a mutual agreement between each of the neighboring domains. The SLA can be either static or dynamic. Static agreements are defined with the initialization of the service and changes frequently. These agreements are negotiated by human interaction whereas negotiating dynamic agreements require an automated protocol between the BBs.

Providers and subscribers face certain challenges and technical issues using SLAs:

- The challenge for subscribers is to devise and operate service measurement tools showing an indication of what extent the SLA is honored by the provider.
- When subscribers use an SLA to bind more than one provider, when the subscriber's VPN spans multiple provider domains, the SLA must also encompass provider interconnection and the end-to-end service performance.
- The challenge for the provider is to honor multiple SLAs from many service providers.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



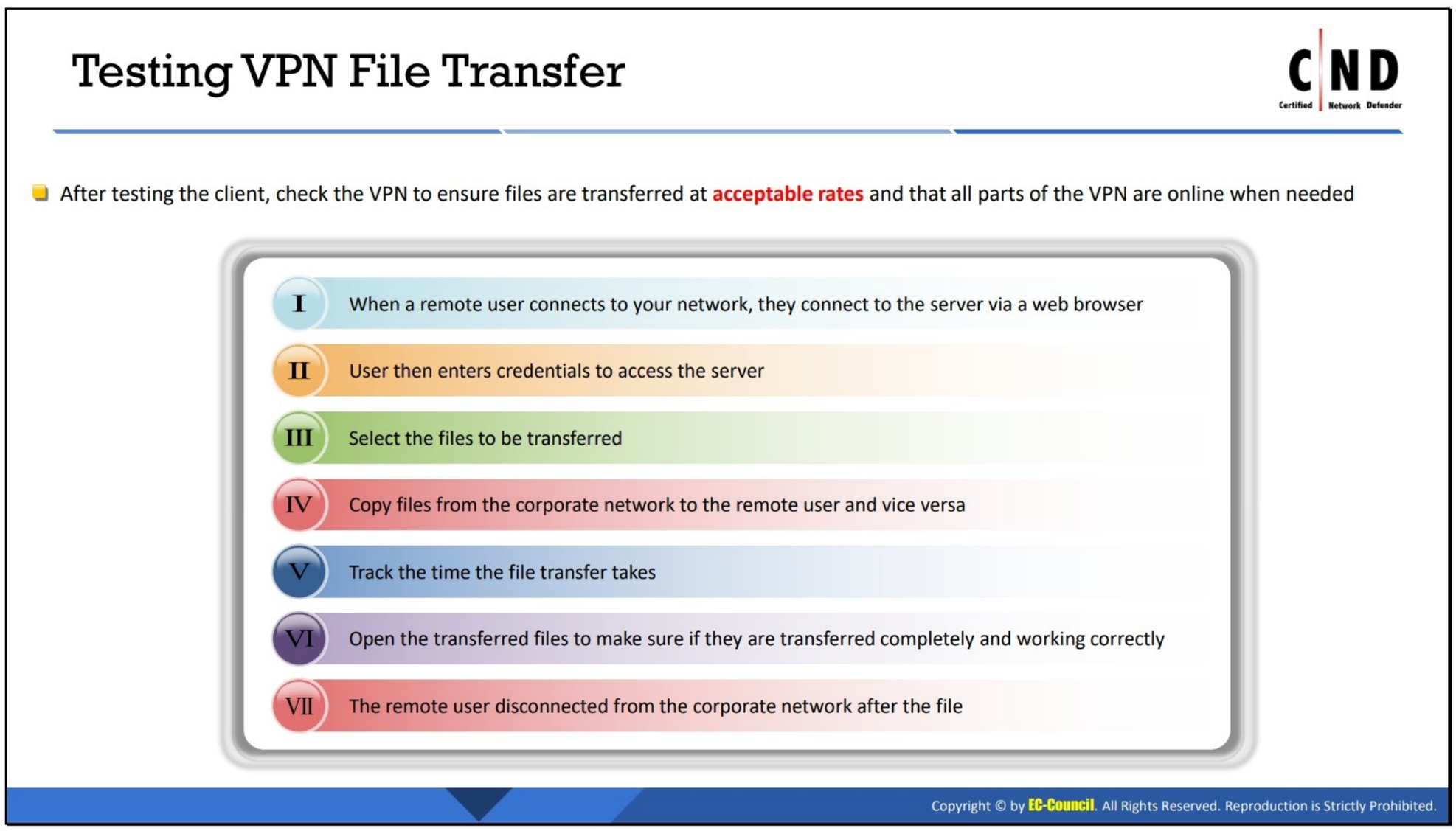
Auditing and Testing the VPN

VPN testing can provide the network defender with an idea of the weaknesses in the implementation. The auditing of a VPN mainly concentrates on the standards, guidelines and procedures. VPN audits depend on other types of security audits such as a configuration audit, network security audit, server security audit etc.

After a VPN is installed, the VPN client must be tested on each computer using a VPN step-by-step scenario:

- The remote user is issued the VPN client software and certificate.
- Guide the user to install the software and store the certificate successfully.
- If IPsec is being used, verify the IPsec policies on the remote user's machine and the VPN gateway are identical.
- Have the user start the VPN software and connect to the gateway.
- If problems arise while connecting to the gateway, ask the user to write down or report all error messages to correctly diagnose the problem.
- Once the connection is established, the remote user should authenticate entering their username and password when prompted.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



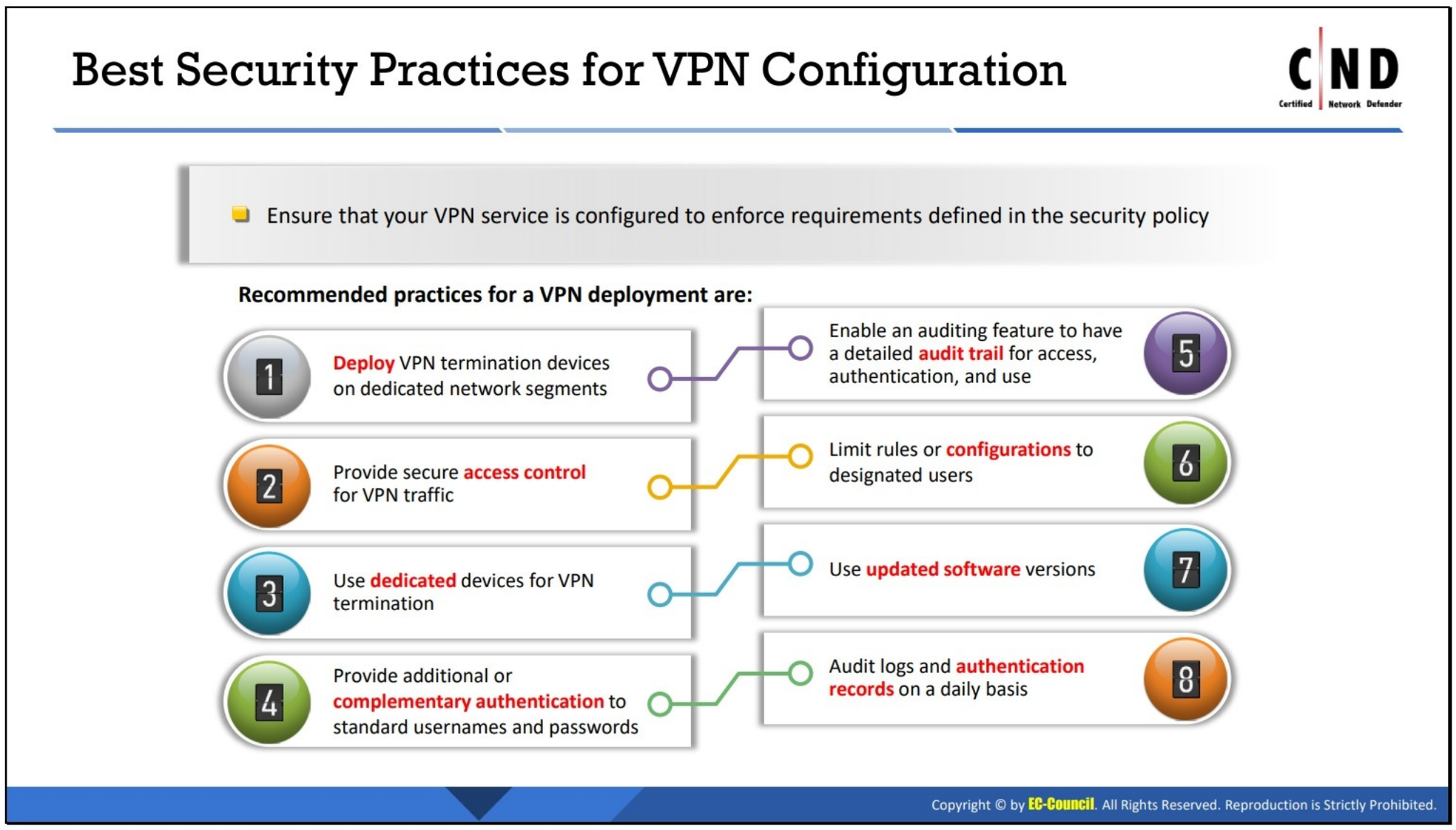
Testing VPN File Transfer

To ensure a successful file transfer between the VPN host and the client are at an acceptable rate, all the VPN ports and other VPN components are to be checked for their online availability such as VPN gateway, Tunnel, etc.

Steps involved in checking the VPN file transfer between the host and the client are:

- The remote user should need a web browser to connect to the network.
- Users should enter credentials to access the server. Then the user is to be authenticated and given access to the server contents if found genuine.
- The user has to select the required files from a list of folders that are to be transferred to his system.
- Copy the files from the corporate network to the client system in the specified user location or directory and vice versa.
- Track the file transfer time either download or uploading of the file.
- Open the transferred files in the client system to ensure they are transferred successfully and in a working state.
- The remote user should be disconnected when the file transfer is complete.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Best Security Practices for VPN Configuration

Ensure that your VPN service is configured to enforce requirements defined in the security policy

Recommended practices for a VPN deployment are:

- Deploy VPN termination devices on dedicated network segments
- Provide secure access control for VPN traffic
- Use dedicated devices for VPN termination
- Provide additional or complementary authentication to standard usernames and passwords
- Enable an auditing feature to have a detailed audit trail for access, authentication, and use
- Limit rules or configurations to designated users
- Use updated software versions
- Audit logs and authentication records daily

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Recommendations for VPN Connections

- Provide a **dedicated firewall** for every VPN connection/server
- The VPN should follow **federal information processing standards** (FIPS), approved encryption and integrity protection algorithms
- VPN traffic should be **filtered** and inspected by internal firewalls
- VPN should provide **flexible and secure** communication between the remote connections and the organization's server
- Use **digital certifications** and device authentication methods for VPN connections
- Use symmetric and asymmetric forms of **cryptography** in the VPN
- Implement **strong application** level security on each application level
- Provide secure **data transmission** and information transfer between the networks

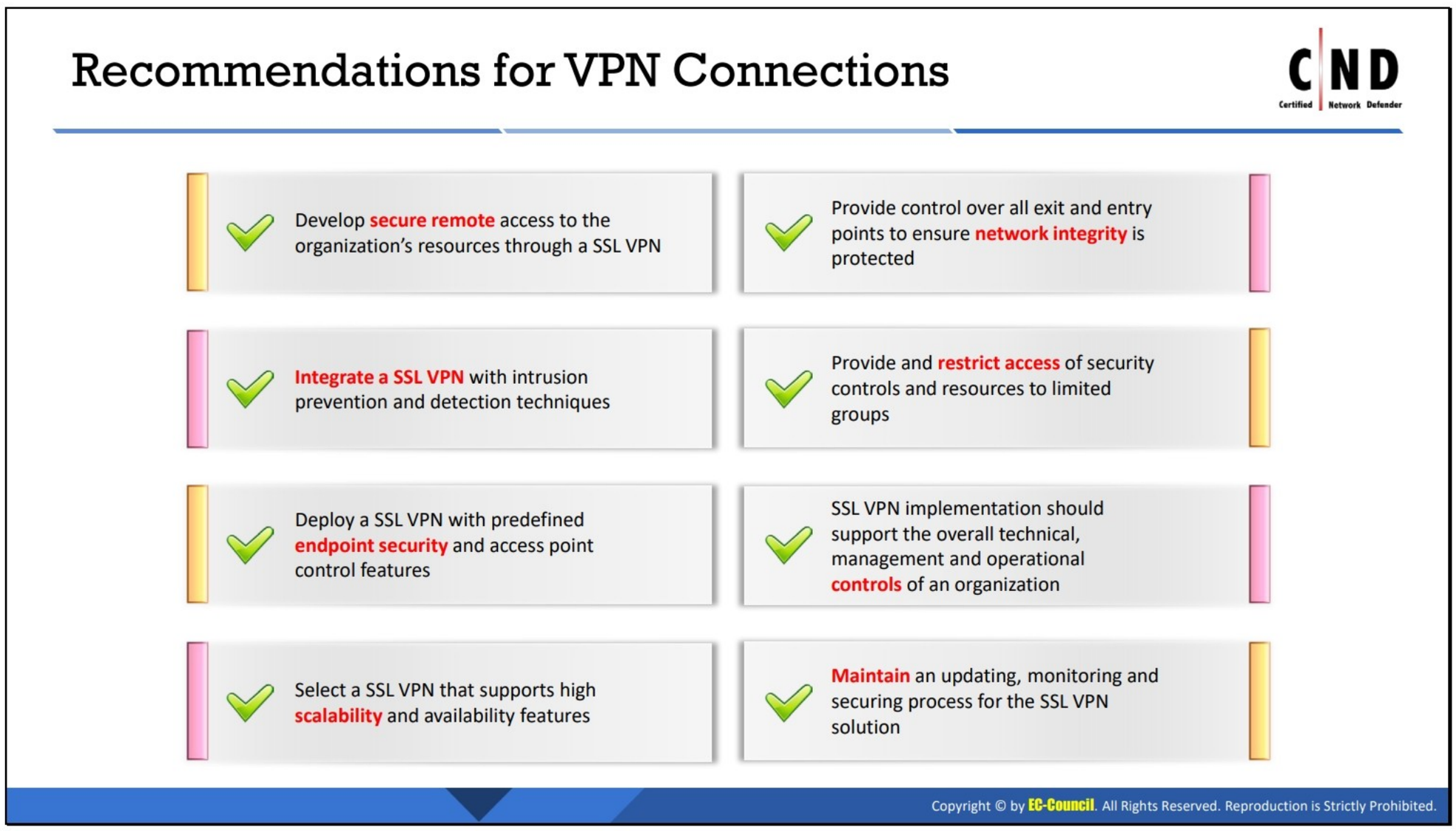
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recommendations for VPN Connections

- **Configure** user authentication, access and restriction to the VPN network
- Manage and configure **IPsec gateways** to protect communication between networks
- Design **packet filters** with restrictions on limiting network traffic for additional protection
- Set rules and **time limits** for termination and disconnection of idle connections
- Define the **communication** channel for packet filters between the remote and main office
- Maintain a list of **authorized users** and regularly check for unauthorized access points
- Strictly **restrict and specify** the type of communication permitted between packet filters
- Deploy and plan **SSL VPN** connections according to the requirements of the organization

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



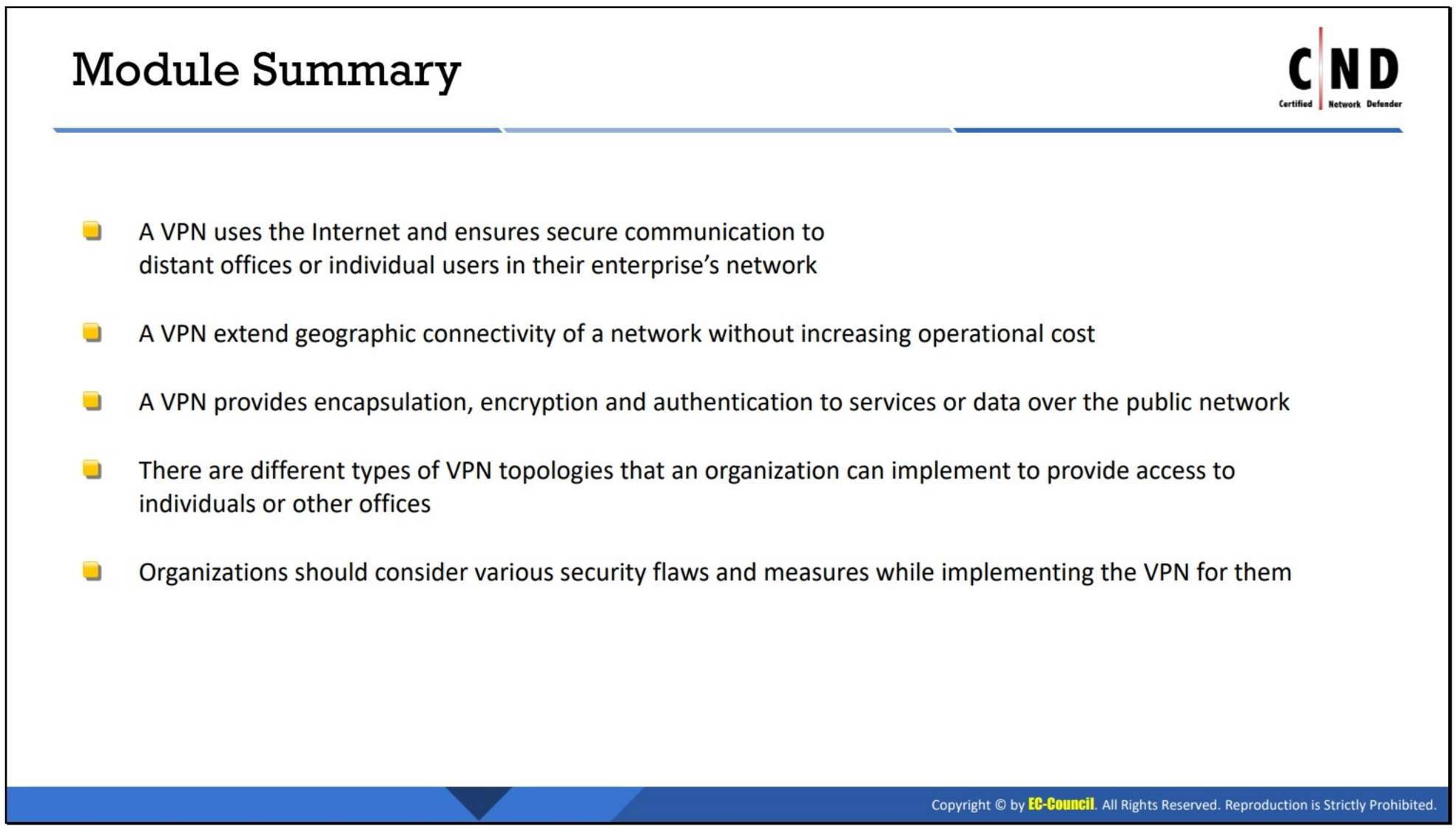
Recommendations for VPN Connections

- Provide a dedicated firewall for every VPN connection/server
- VPN traffic should be filtered and inspected by internal firewalls
- Use digital certifications and device authentication methods for VPN connections
- Implement strong application level security on each application level
- The VPN should follow federal information processing standards (FIPS), approved encryption and integrity protection algorithms
- VPN should provide flexible and secure communication between the remote connections and the organization's server
- Use symmetric and asymmetric forms of cryptography in the VPN
- Provide secure data transmission and information transfer between the networks
- Configure user authentication, access and restriction to the VPN network
- Design packet filters with restrictions on limiting network traffic for additional protection
- Define the communication channel for packet filters between the remote and main office
- Strictly restrict and specify the type of communication permitted between packet filters
- Manage and configure IPsec gateways to protect communication between networks
- Set rules and time limits for termination and disconnection of idle connections
- Maintain a list of authorized users and regularly check for unauthorized access points
- Deploy and plan SSL VPN connections according to the requirements of the organization

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Develop secure remote access to the organization's resources through a SSL VPN
- Integrate a SSL VPN with intrusion prevention and detection techniques
- Deploy a SSL VPN with predefined endpoint security and access point control features
- Select a SSL VPN that supports high scalability and availability features
- Provide control over all exit and entry points to ensure network integrity is protected
- Provide and restrict access of security controls and resources to limited groups
- SSL VPN implementation should support the overall technical, management and operational controls of an organization
- Maintain an updating, monitoring and securing process for the SSL VPN solution

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

In this module, you have learned the need for establishing a VPN, different VPN components, VPN topologies and technologies. You have also learned the various security flaws that exist due to improper/insecure configuration and implementation of a VPN. The module guides you on configuring and implementing VPN security through various security techniques, best practices and recommendations. With this module, you will able to select the appropriate VPN topology and technology based on your organization's needs and will able to configure it securely.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council

Building A Culture Of Security



C|ND

Certified Network Defender

Certified Network Defender v3

APPENDIX D

ENDPOINT SECURITY – MAC SYSTEMS

EC-Council Official Curricula

This page is intentionally left blank.

MODULE OBJECTIVE

The objectives of this module are :

- LO#01: Understanding macOS and security concerns
- LO#02: Discussing macOS user access and password management
- LO#03: Discussing various macOS security features
- LO#04: Discussing macOS user access and password management
- LO#05: Implementing macOS hardening techniques
- LO#06: Discussing macOS network security and remote security
- LO#07: macOS patch management

C|ND Certified Network Defender

LO#01: Understanding macOS and security concerns

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Mac Operating System (macOS)

- The primary operating system for Apple's Mac computers, macOS, is developed and marketed by Apple Inc. since 2001

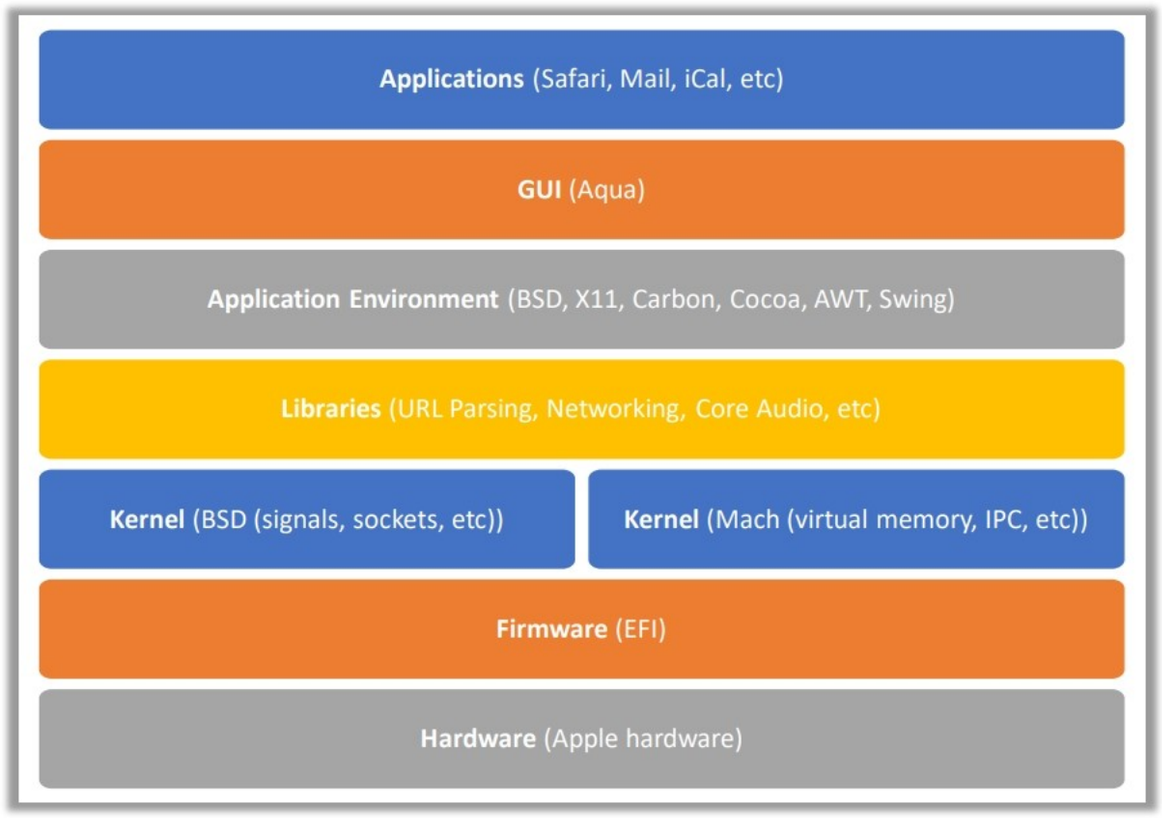
Operating system	Version
macOS Sonoma	14.1
macOS Ventura	13.6.1
macOS Monterey	12.7.1
macOS Big sur	11.7.10
macOS Catalina	10.15.7
macOS Mojave	10.14.6
macOS High Sierra	10.13.6
macOS Sierra	10.12.6
OS X El Capitan	10.11.6
OS X Yosemite	10.10. 5

Operating system	Version
OS X Mavericks	10.9.5
OS X Mountain Lion	10.8.5
OS X Lion	10.7.5
Mac OS X Snow Leopard	10.6.8
Mac OS X Leopard	10.5.8
Mac OS X Tiger	10.4.11
Mac OS X Panther	10.3.9
Mac OS X Jaguar	10.2.8
Mac OS X Puma	10.1.5
Mac OS X Cheetah	10.0.4

Versions of macOS OS

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

macOS Architecture



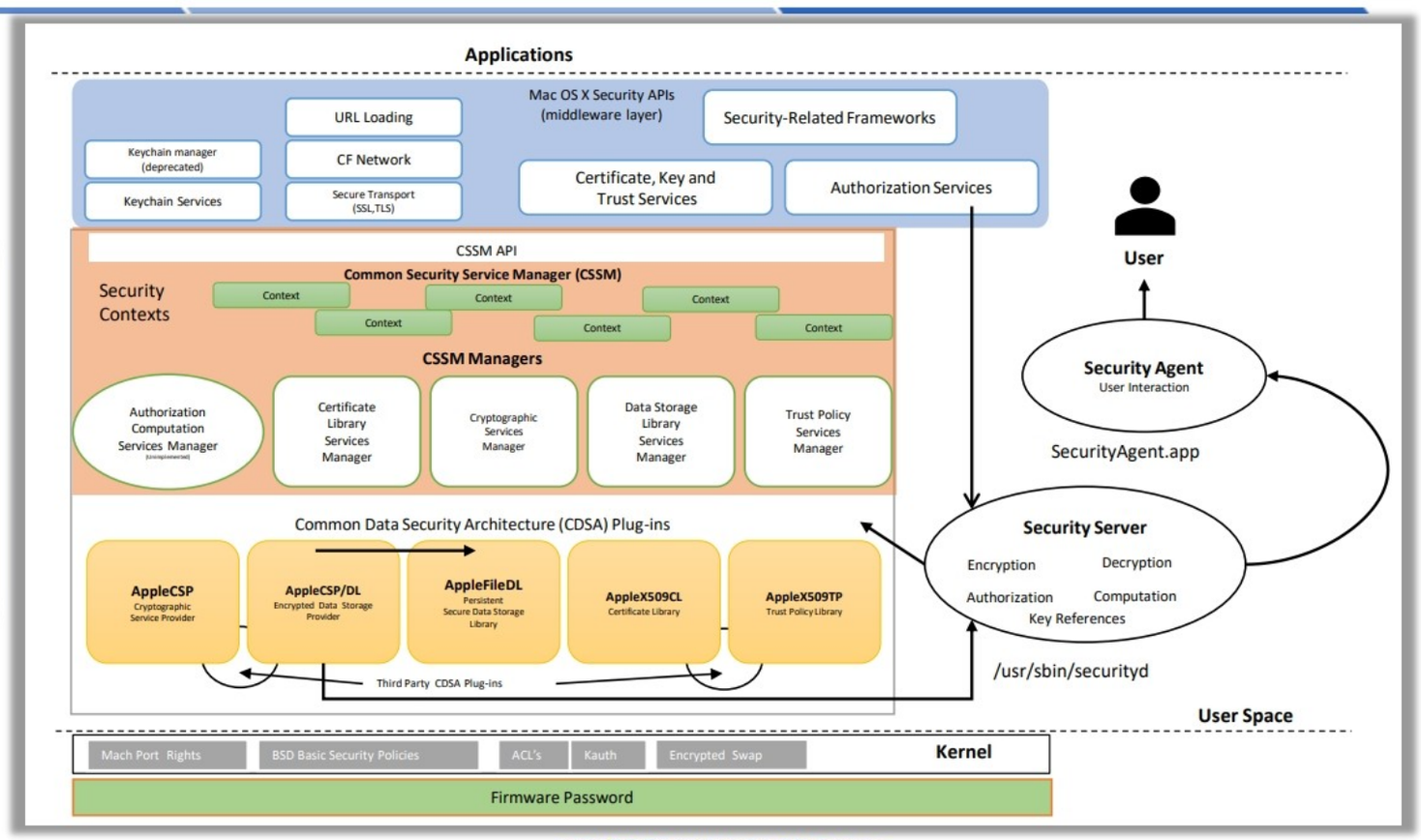
Basic Architecture of macOS Structure

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

macOS Security Architecture

- macOS incorporates a robust security architecture designed to **protect user data,** prevent **unauthorized access**, and ensure the integrity of the system

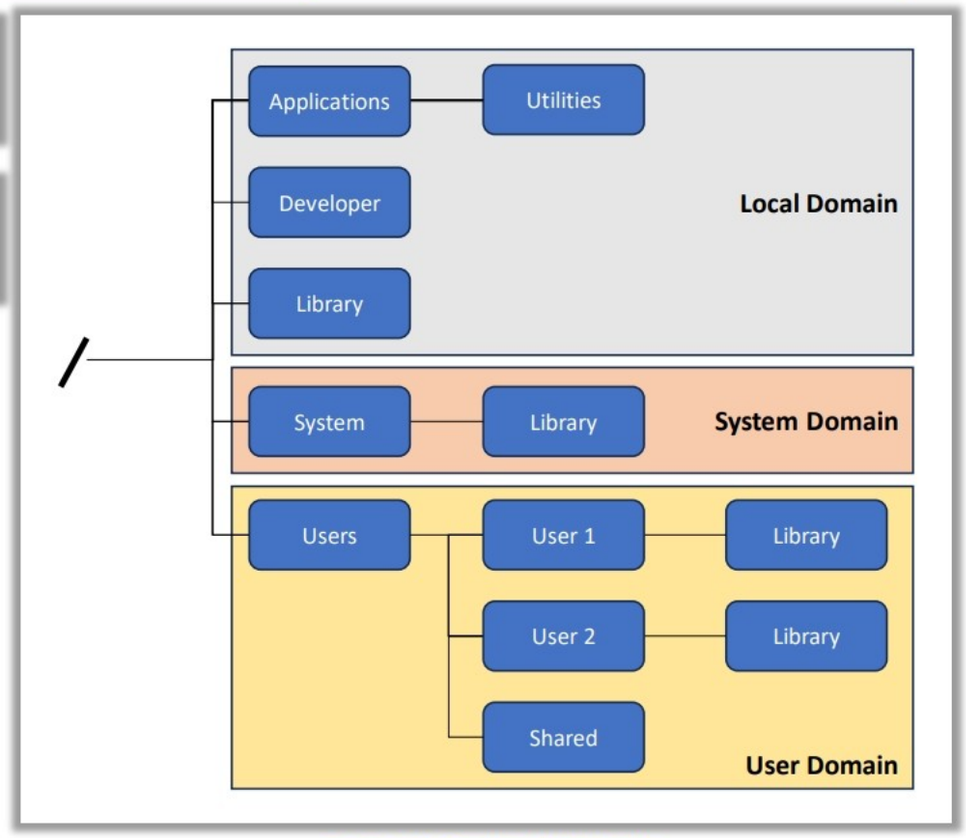


macOS Security Architecture

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

macOS File System

- Apple File System (APFS) is the default file system in macOS
- In macOS, the file system is divided into three domains, which separate files and resources based on their intended usage:
  - The ***user domain*** consists of resources about the user logs into the system
  - The ***system domain*** consists of vital resources such as operating systems, user groups, and topologies of arrangement of files
  - The ***local domain*** not just consists of a single file but holds several directories in the root volume. By default, this domain is managed by the system but users with admin privileges can edit and modify items in it



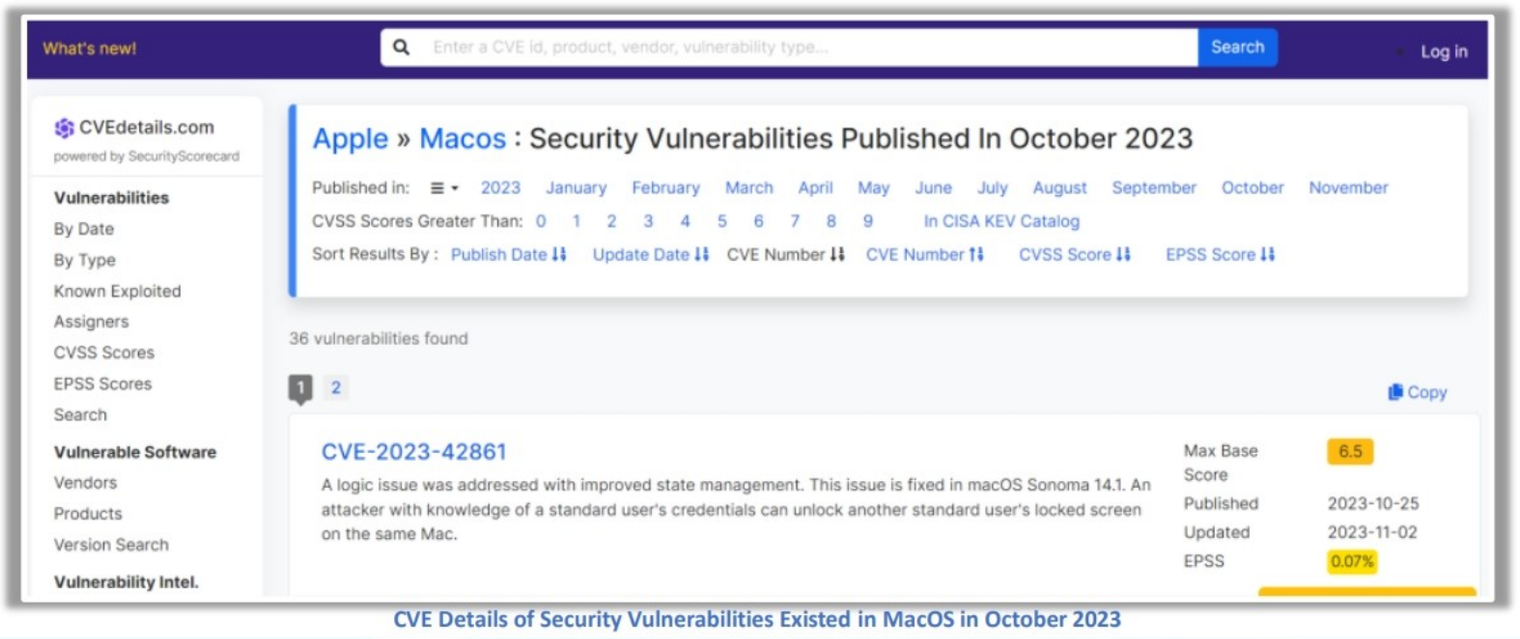
macos File System Hierarchy

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

macOS Security Concerns

- macOS is generally considered to be a secure platform but has its own set of security considerations and concerns
- Unpatched OS, **improper configurations**, weak passwords, lack of anti-malware software, leaving unnecessary services and processes enabled, etc. can provide a path to attackers to compromise macOS system security



CVE Details of Security Vulnerabilities Existed in MacOS in October 2023

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#02: Discussing macOS security components

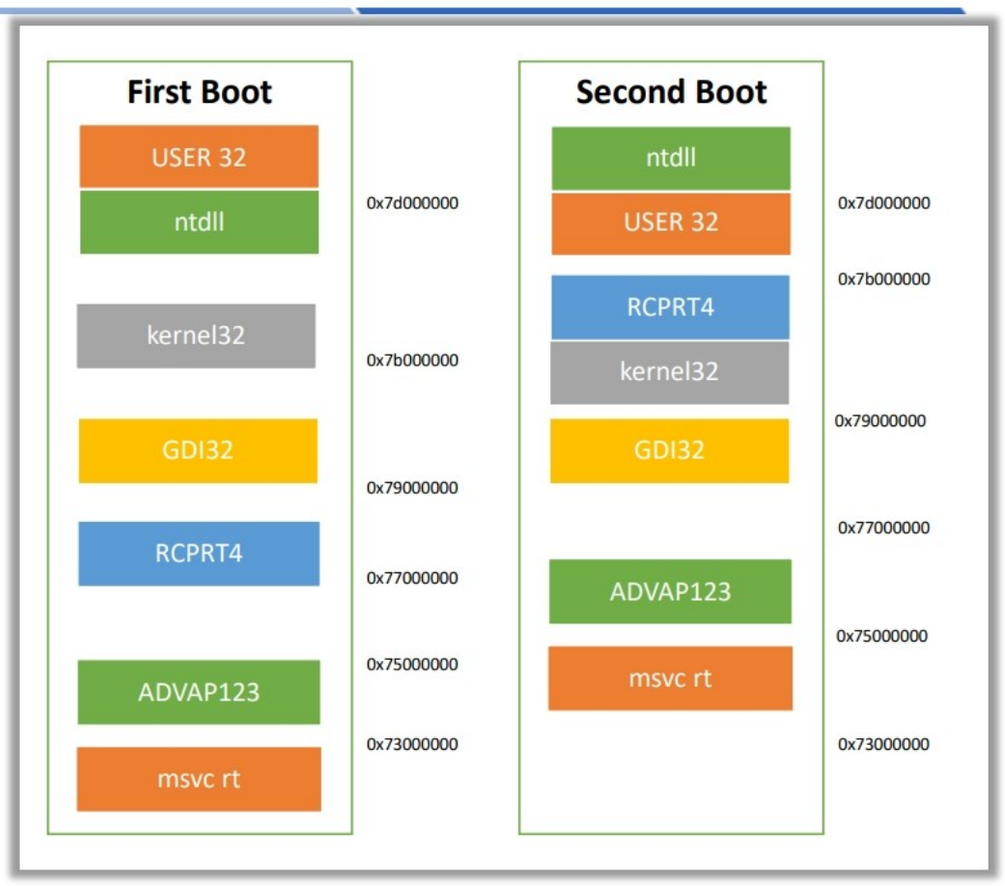
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Address Space Layout Randomization (ASLR)

- Address space layout randomization (ASLR) randomizes the memory addresses used by system and application components during the system's boot process, making it difficult for attackers to predict the location of specific code or data

- macOS implements different levels of **randomization** to **enhance security**. The degree of randomization depends on system architecture and configuration



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

XNU Kernel

macOS is built on the XNU (X is Not Unix) kernel, which is a hybrid kernel combining elements of the **Mach microkernel** and components from FreeBSD

Kernel-level Security Features to Protect OS and Data

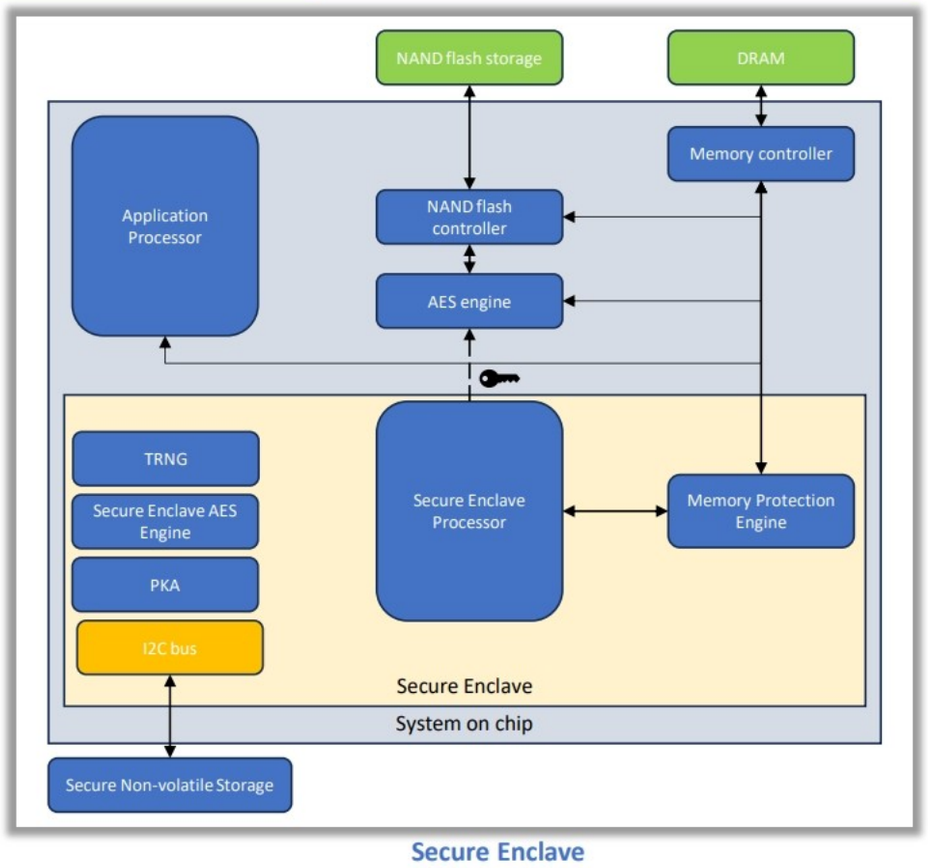
- **System integrity protection (SIP):** SIP (rootless) security feature restricts the root user and certain processes from modifying critical system files and directories. This helps prevent unauthorized modifications that could compromise system integrity
- **Code signing:** macOS enforces code signing for kernel extensions (kexts) and certain system components to ensure that the code being loaded into the kernel is from a trusted source and has not been tampered with
- **Kernel extension (Kext) loading:** The loading of kernel extensions requires explicit user approval and prevents unauthorized or malicious kernel extensions from loading without user consent
- **Kernel address space layout randomization (KASLR):** KASLR is a security technique that randomizes the memory addresses used by the kernel during system boot
- **Stack smashing protection:** macOS incorporates stack canaries and other techniques to protect against stack buffer overflow attacks
- **Virtual memory protection:** macOS uses virtual memory protection mechanisms to isolate the memory space of different processes and the kernel to prevent unauthorized access to or modification of memory that belongs to the kernel
- **XPC services:** Cross process communication services are used to facilitate communication between processes while maintaining a level of isolation and prevent unauthorized access to sensitive resources

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Secure Enclave

- The Secure Enclave, available in Macs with the T2 chip, is designed to provide a secure and isolated environment for handling **sensitive operations** related to security, encryption, and biometric data
- It is a dedicated co-processor that operates independently of the main processor (CPU) and has its **own secure boot process**
- It is designed to be **resistant to physical tampering**. It is difficult to extract sensitive information or compromise its **security mechanisms**, even if an attacker has physical access to the device

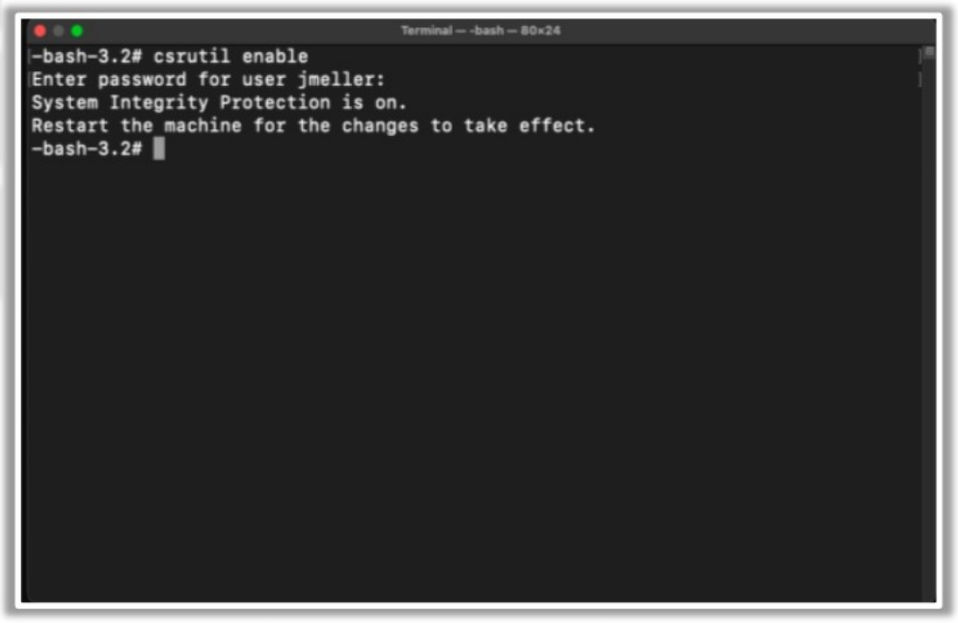


Secure Enclave

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

System Integrity Protection (SIP)

- System integrity protection (SIP) protects a Mac system by preventing the **execution** of malicious code
- This feature enables automatic authorization of applications that a user downloads
- **Benefits of this SIP are as follows:**
  - **Protect system file** from malicious software
  - **Prevents root-level access** by restricting the users' actions
  - **Enhances kernel security** by ensuring that only valid kernel extensions can be loaded into the kernel



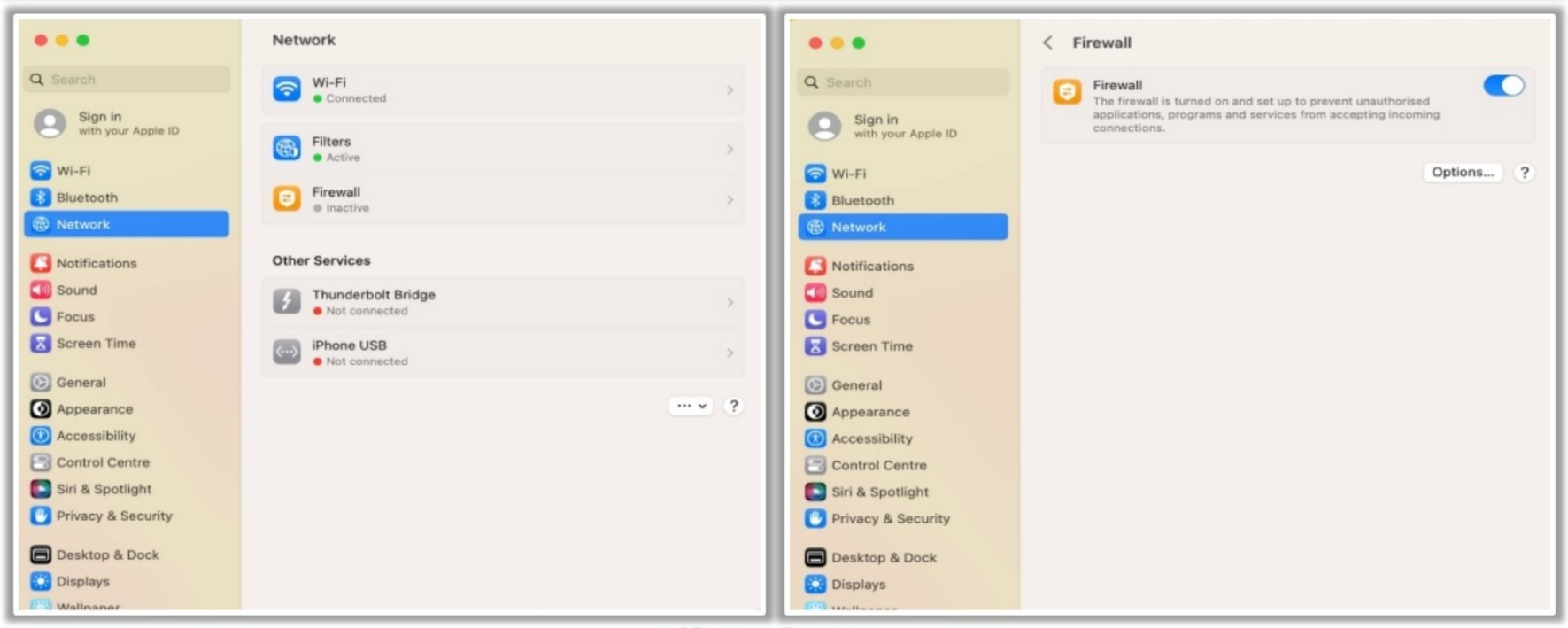
Enabling System Integrity Protection from Terminal

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Firewall

- macOS built-in firewall provides a layer of security by **controlling incoming and outgoing network traffic** and protects it from potentially harmful connections
- The firewall settings can be configured through the Security & Privacy preferences on Mac System



Enabling Firewall in a Mac

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

XProtect

- XProtect is a built-in anti-virus in macOS designed to provide basic protection against certain types of malware to safeguard users from malicious software and potential security threats
- It uses YARA signatures (a tool to conduct signature-based detection of malware) and removes malware
- **XProtect checks for known malicious content whenever:**
  - An app is first launched
  - An app has been changed (in the file system)
  - XProtect signatures are updated

- **To access XProtect on Mac:**
  - Go to **Macintosh HD/Library/Apple/System/Library/CoreServices/XProtect.bundle**
  - Control-click on **XProtect.bundle** and then choose **Show Package Contents**
  - Click **Contents/Resources**; press the space bar to open the **XProtect.plist** file



Example Working of XProtect

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

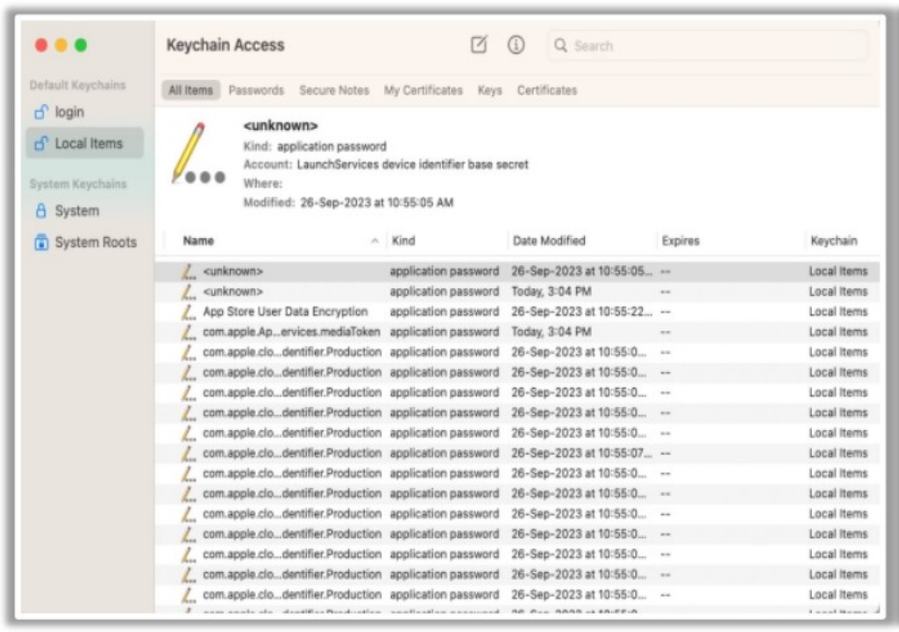
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

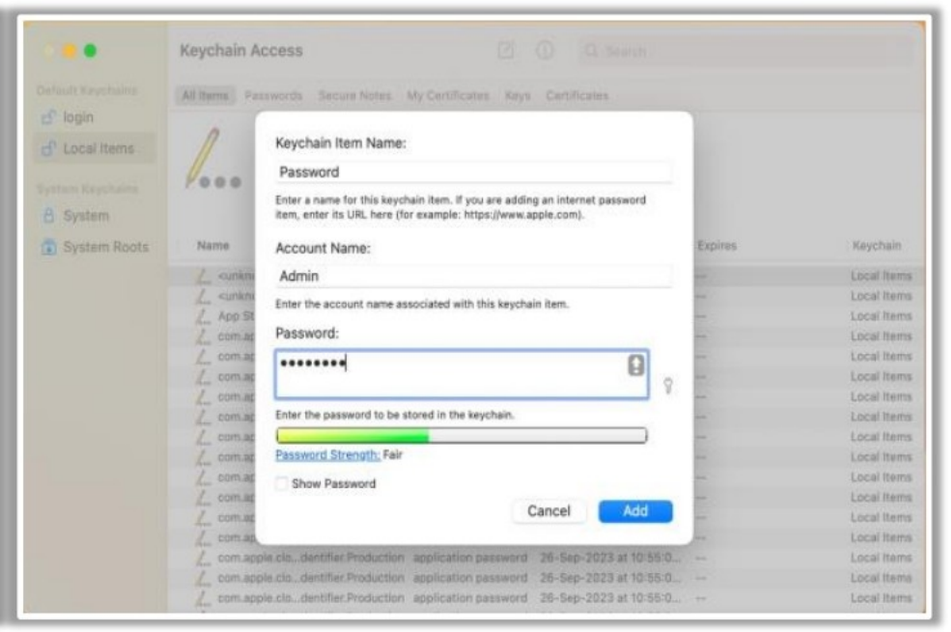
LO#03: Discussing various macOS security features

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Keychain Access

- Keychain Access is a macOS application that serves as a **password management system**, allowing users to store and manage various types of sensitive information, including passwords, encryption keys, certificates, and secure notes



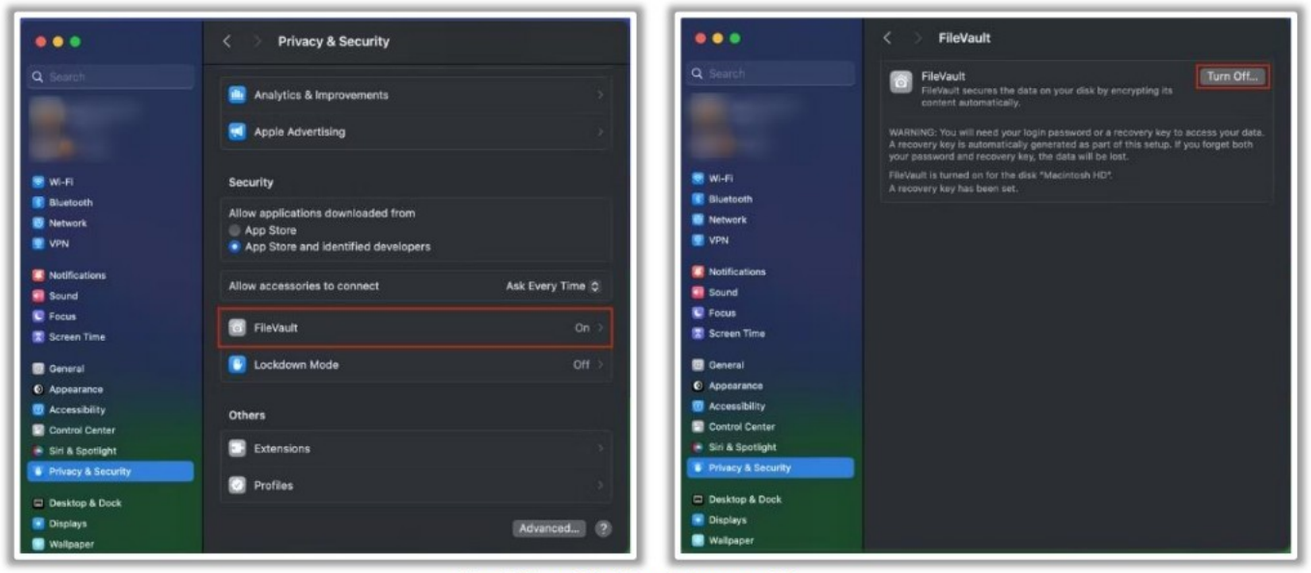


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FileVault

- FileVault is a disk encryption program available in macOS designed to **provide robust data protection** by encrypting the entire contents of a startup disk
- This feature enhances the **security of user data**, ensuring that unauthorized access to information on a Mac's startup disk is prevented. It uses full-disk XTS-AES-128 encryption with a 256-bit key



Enabling File Vault in macOS

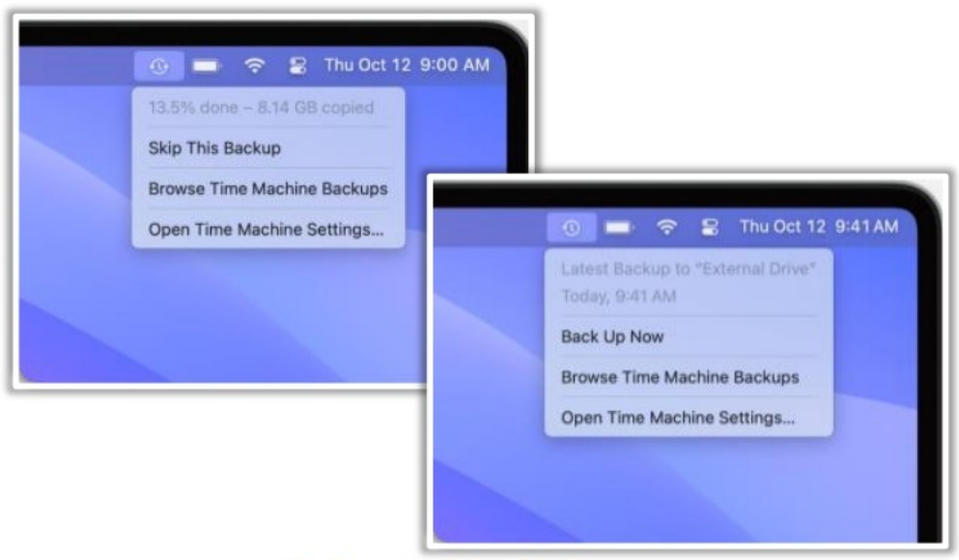
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Time Machine

- Time Machine is a backup solution **integrated** into macOS that provides **automatic, incremental backups** of your entire system
- It allows you to easily restore files, applications, or even your entire system to a previous state



Backup a Disk using Time Machine



Backup using Time Machine

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Secure Boot

- Secure Boot ensures that the operating system is loaded from the legitimate disk and protects the OS from boot kits
- This feature enables the user to set up a firmware password thereby **preventing unauthorized users** from loading the OS from the unallocated disk
- There are three levels of security in this Secure Boot:
  - **Full Security** offers the highest level of security
  - **Medium Security** enforces only a limited level of security requirements
  - **No Security** does not enforce any security requirements

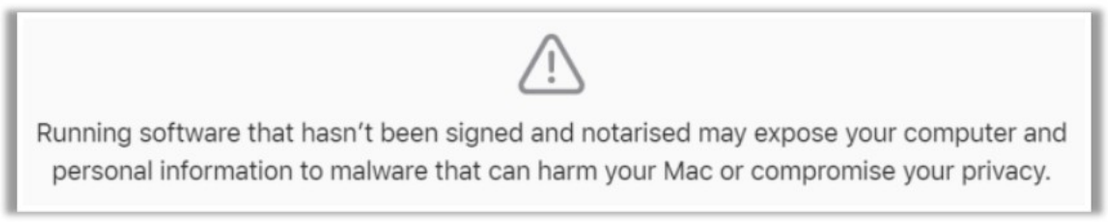


Secure Boot Feature of macOS

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Gatekeeper

- Gatekeeper is designed to **protect users** from installing malicious or unauthorized software
- It ensure that only **trusted** and **verified applications** are allowed to run on a Mac
- Gatekeeper works by checking the **digital signatures of applications** to verify their origin and whether they have been tampered



macOS Requests Approval to Ensure that you are not Misled into Running Software



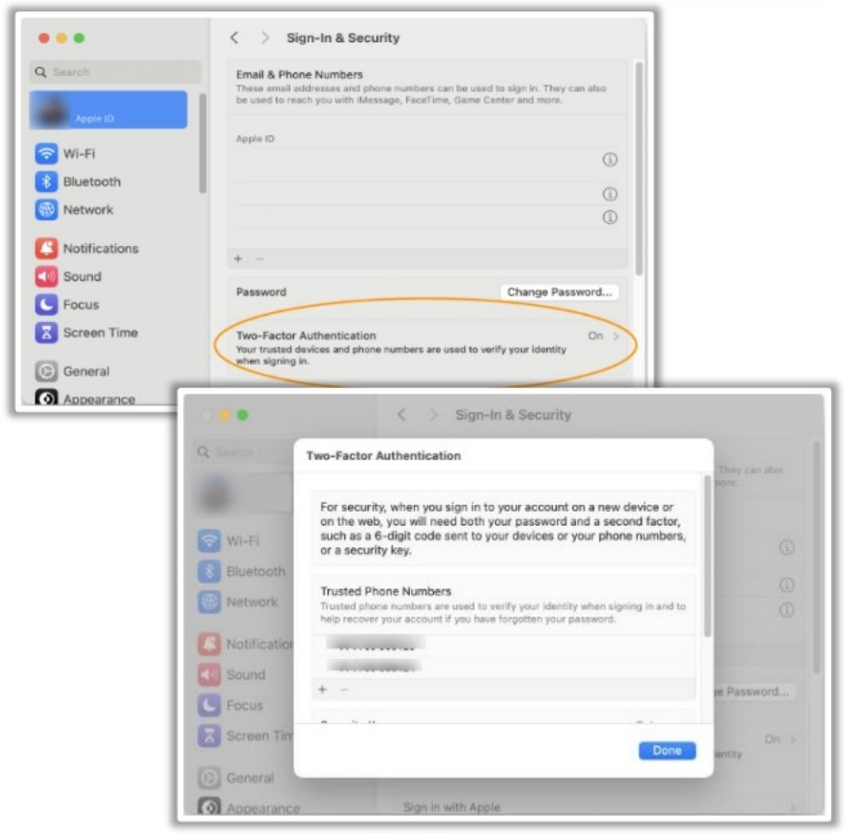
Alert that an Application will Damage Mac/the App is Damaged

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

macOS Secure Authentication

- Two-factor authentication in macOS is an additional security feature that ensures only authorized user can access the account
- This feature **requires two verification steps** to identify the user
- This feature enables the user to use either a six-digit **verification code** or a **physical security key**
- To set up 2FA, enable 2FA authentication initially, create a recovery key, and setup trusted devices
- In supported Mac models, Touch ID and Face ID provide biometric authentication, adding an **extra layer of security** for unlocking the device and authorizing certain actions



Using 2FA

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Security Features

- NIST RMF is a **structured and continuous process** that integrates information security and risk management activities into the system development life cycle

An Apple Device with macOS Network Security Support Includes:

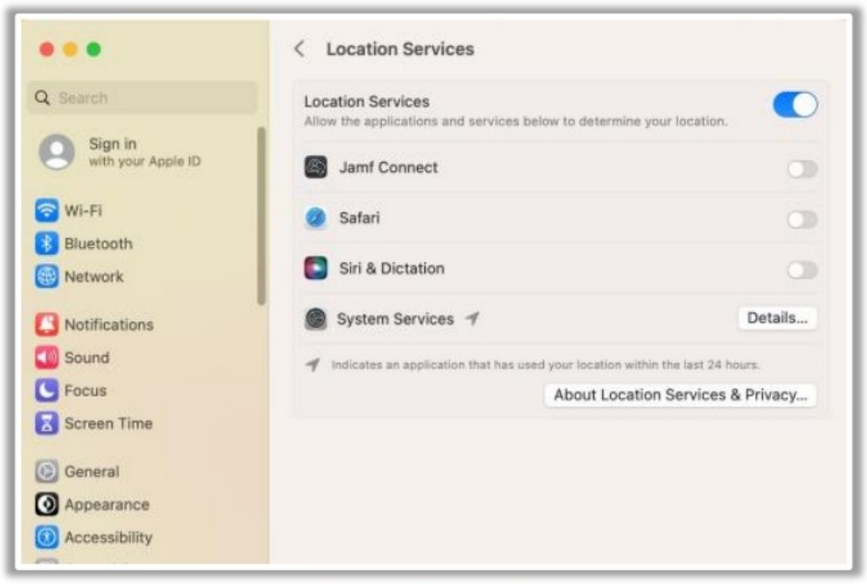
Categorize	Select	Implement	Assess	Authorize	Monitor
Define criticality/sensitivity of information system according to potential worst-case and adverse impact to mission/business	Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment	Implement security controls within enterprise architecture using sound system engineering practices; apply security configuration changes	Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, and meeting security requirements for information system)	Determine risk to organizational operations and assets, individuals, other organizations, and the nation; if acceptable, authorize operation	Continuously track changes to the information system that may affect security controls and reassess control effectiveness

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Privacy Controls

- MacOS includes privacy controls that prompt users for permission before allowing apps to **access sensitive data** or perform certain actions, such as accessing the camera, microphone, or location services
- **Location-based permissions:** macOS allows users to control which apps have access to their location information. This can be managed in the "Security & Privacy" preferences under the "Privacy" tab



Location-based Permissions

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Safari Privacy Settings

- **Intelligent tracking prevention:** Safari includes features such as **intelligent tracking prevention (ITP)** to limit cross-site tracking by advertisers
- **Privacy report:** Safari provides a privacy report that shows the number of trackers prevented from profiling users



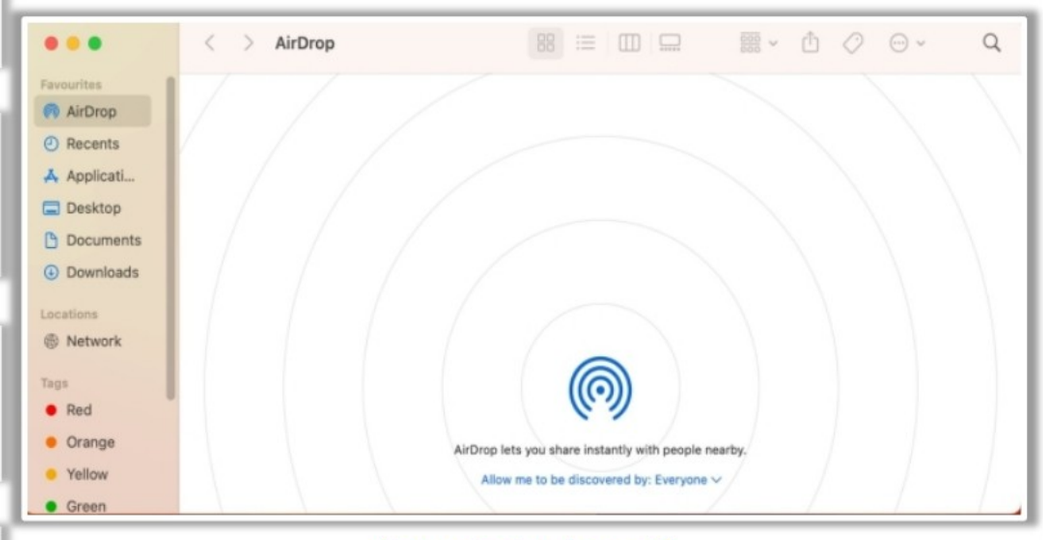
Safari Anti-tracking Feature

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Airdrop Security

- AirDrop is a feature on macOS that **allows users to wirelessly share files** between Macs and other Apple devices like iPhones, iPads, and iPod touches
- AirDrop uses a combination of **Bluetooth and Wi-Fi technology** for file transfer. The data sent via AirDrop is encrypted during transit
- To use AirDrop, both Wi-Fi and Bluetooth must be enabled on the devices involved in the transfer. It is important to ensure that these connections are secure
- Users can configure the visibility settings for AirDrop in the Control Center on iOS devices and Finder on Macs



Airdrop Feature in macOS

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#04: Discussing macOS user access and password management

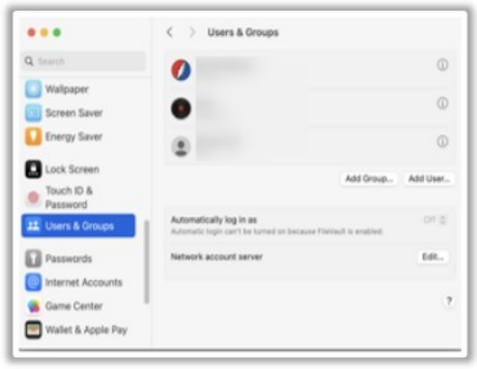
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Use Separate User Log-ins

- Using separate user log-ins on macOS enhances **privacy, access control**, and overall system security
- Each user account on macOS has its own set of files, preferences, and access rights, providing a level of isolation between users
- Setup different user accounts based on the need and restrict them from making system-wide changes

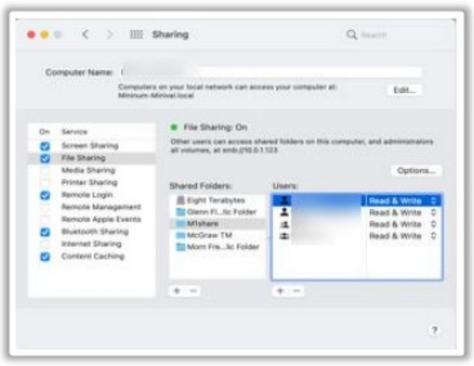
Different Types of Accounts



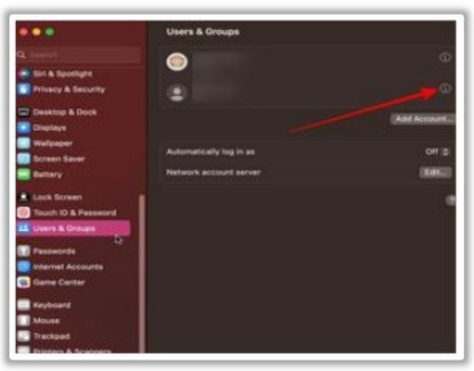
Account Type: Administrator can manage other users, install apps, and can also change settings



Account Type: Standard user can change their own settings but cannot manage other users



Account Type: Shared-only users are restricted access to specific volumes and permissions



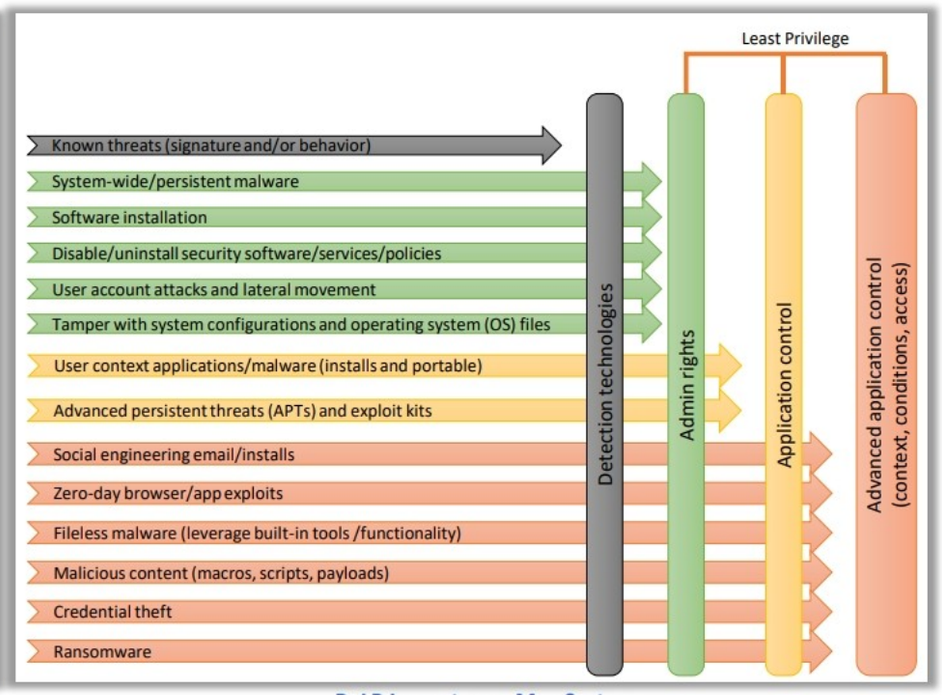
Account Type: Guest users are restricted to grant temporary or short-term access to system

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Implement Principle of Least Privilege (PoLP)

- Implement Principle of Least Privilege (POLP) to **restrict access rights for users** and applications to only those who are authorized

- **Steps to implement least privilege:**
  - **Identify user roles and responsibilities:** Identify user roles and assign minimal permissions to the Mac user based on the job role
  - **Eliminate local admin rights:** Remove local admin rights and provide on-demand elevated privileges for the Mac users based on the need
  - **Create user groups:** Create common groups with users having similar job functions; assign privileges and permissions to files and resources based on groups
  - **Limit network and application access:** Limit access to network resources that is necessary for user job role



PoLP Impact on a Mac System

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

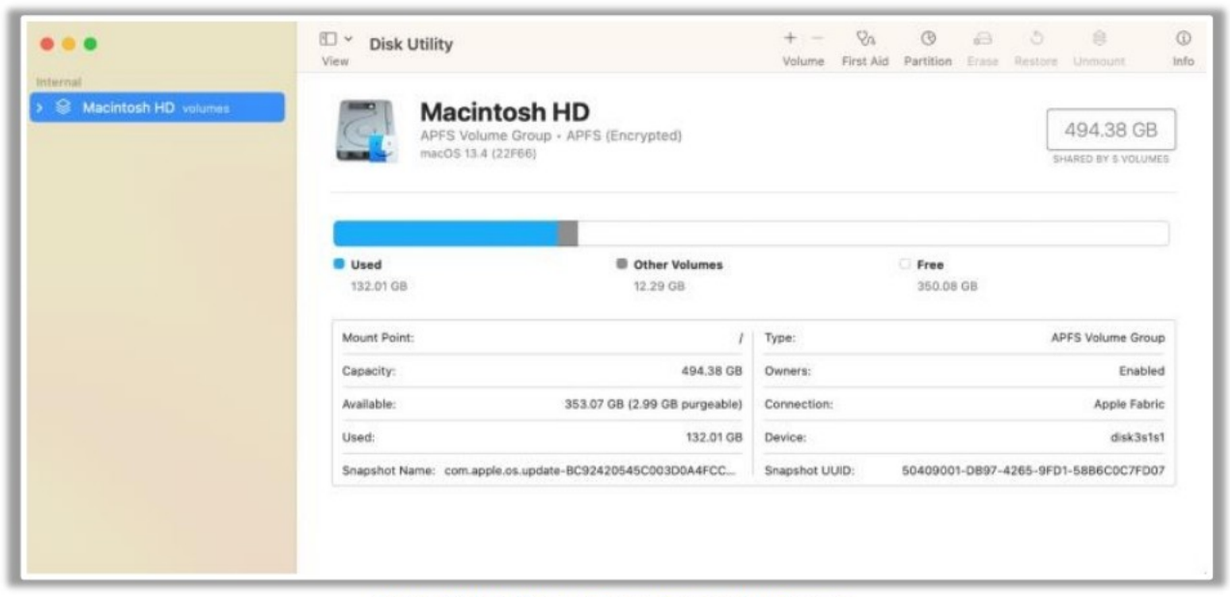
User Account - Password Best Practices

- Request the Mac user to use at least **two special characters**
- Restrict **reusing** the same or similar passwords used in the past
- Ensure that the user account is locked after **10 failed login attempts**
- Ensure that the password has a **minimum 8 characters** to a maximum of 16 characters
- Ensure that the password has **at least one letter and one number**
- Ensure that the password **does not allow simple or default passwords**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Implement Encryption for Removeable Storage

- Encrypt and protect removable storage device with a password in **Disk Utility** on macOS when formatting internal/external storage device
- Initially, erase the device to encrypt and **protect the device** with a password using Disk Utility



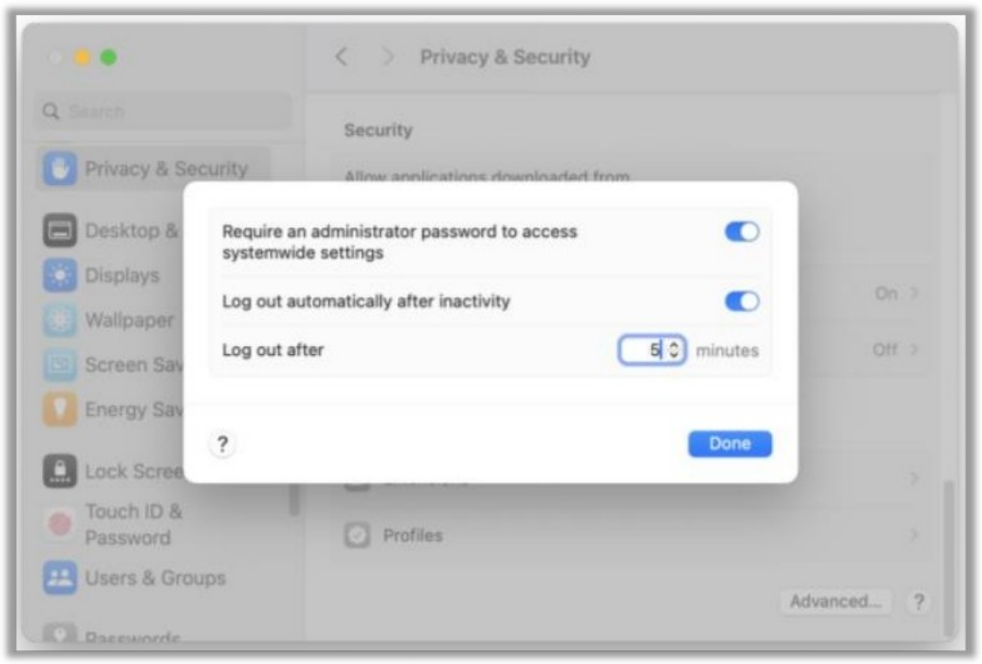
Using Disk Utility to Secure Removable Storage

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Enable Automatic Logout

- User can enable automatic logout from the user account and define a **period of inactivity**
- This feature secures information on the Mac when the system is left unattended for a longer period

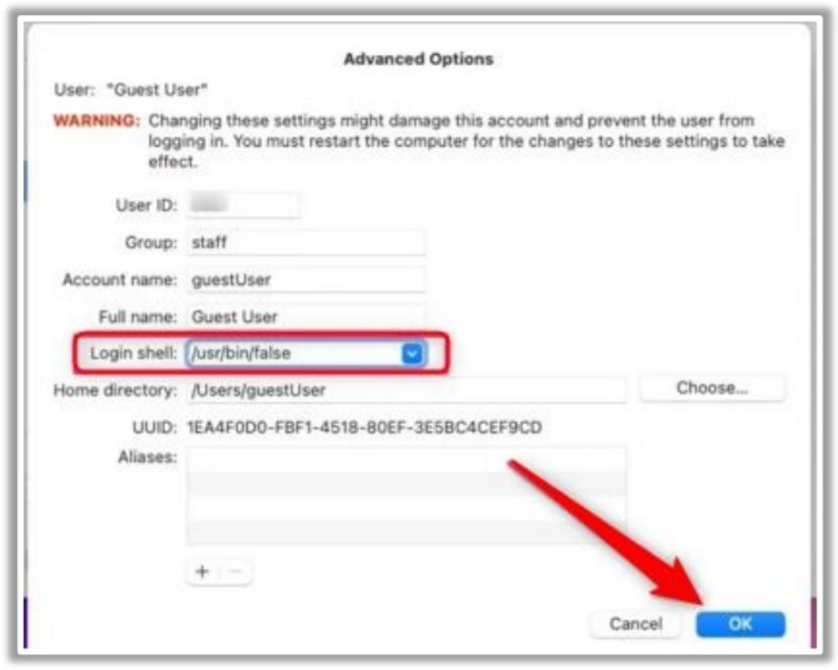


Enabling and Setting Automatic Logout

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Disable Unnecessary Accounts

- Disabling an account prevents **the user from logging in** and accessing the system
- Disable inactive user accounts that have been not used for long
- Do remember to **disable user account of employees** who have resigned from the organization
- An attacker can gain access to the system through compromised **unused**/**inactive user accounts**



Disabling User Account

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Review User Permissions

- Regularly review and **audit user permissions** to ensure that they align with security policies and requirements
  - Review Account Information
  - Check Group Memberships
  - Verify Admin Privileges
  - Verify Automatic Login
  - Review FileVault Status
  - Check Folder and File Permissions
  - Advanced Permissions

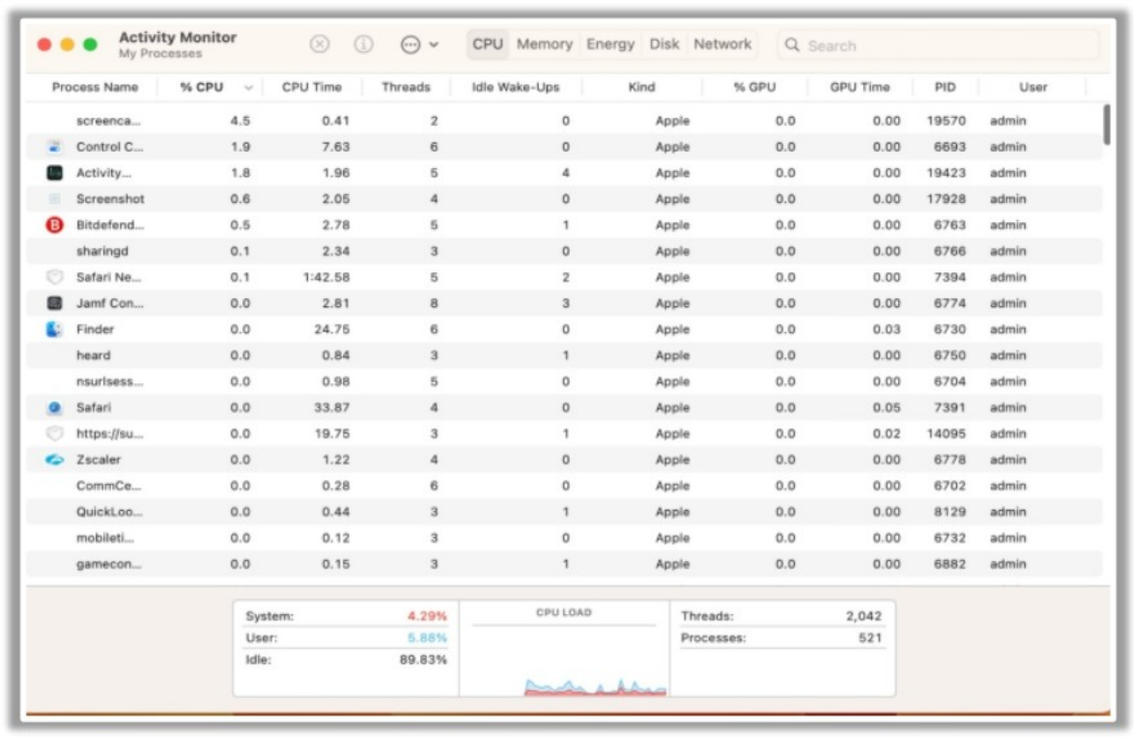


Review User Permissions

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Disable Unnecessary Protocols and Services

- Use **Activity Monitor** to obtain information about the running processes and disable the unnecessary protocols and services that are running in background



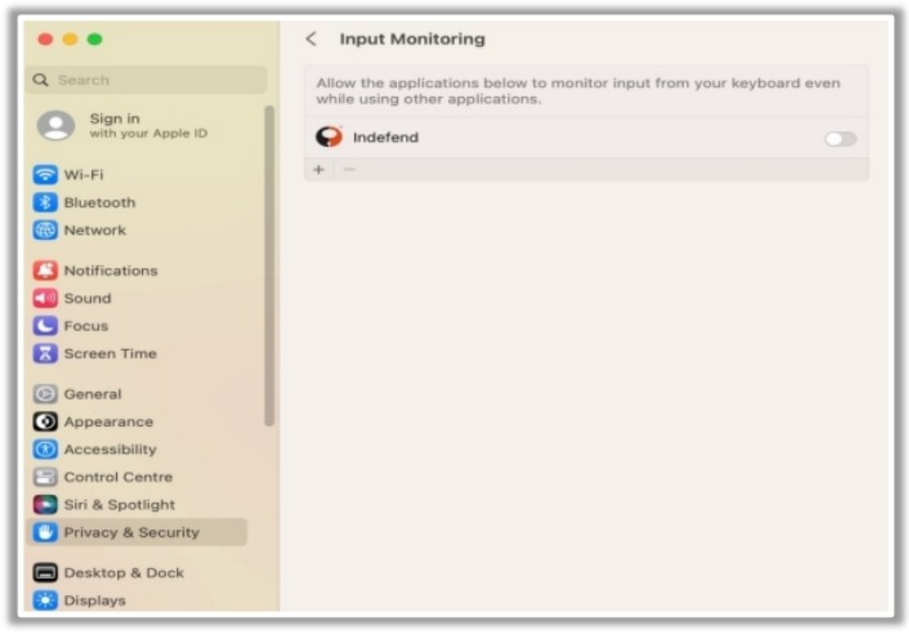
Disabling Unnecessary Services using Activity Monitor

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Monitor Security & Privacy Settings

- Use **Security & Privacy** settings to manage the information Mac makes available to others and secure encrypted data
- To change these settings, Go to **Apple** menu -> **System Settings** -> click **Security & Privacy** in the sidebar. Toggle between **Allow** and **Don't Allow** in the privacy settings



Monitor Security & Privacy Settings

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

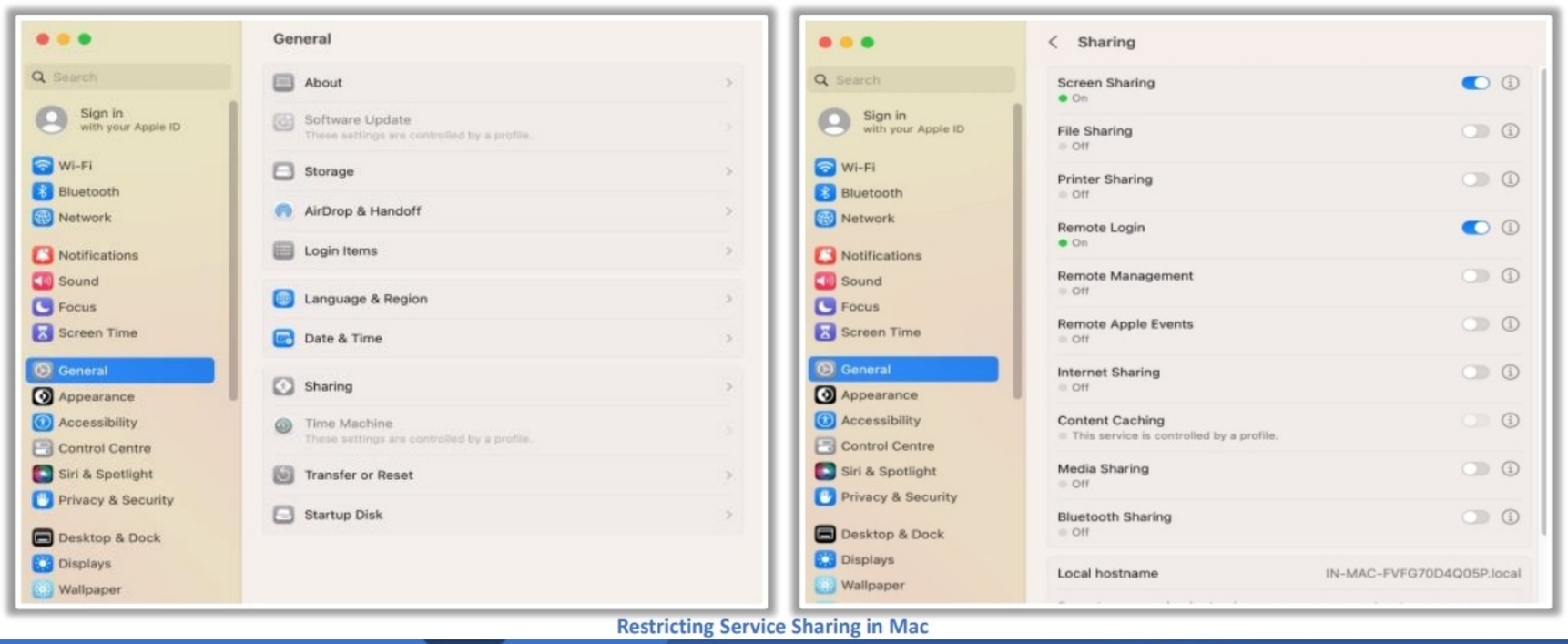
LO#05: Implementing macOS hardening techniques

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Restrict Service Sharing

- Manage and restrict service sharing by configuring specific settings related to file sharing, screen sharing, and other services
- Restricting service sharing **enables control access** to your Mac and enhances overall security

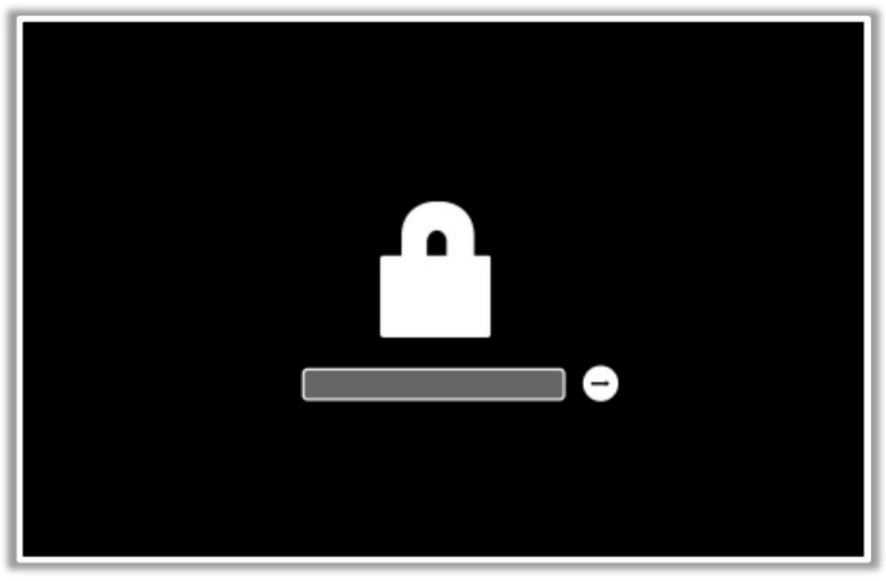


Restricting Service Sharing in Mac

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Set a Firmware Password

- Setting a firmware password on a Mac adds an **additional layer of security** by requiring the password to be entered before anyone can access certain functions, such as starting up from a different disk or entering the macOS Recovery environment



Result of Setting Firmware Password

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Disable Remote Management

- Remote Management allows you to **control your Mac** remotely
- Keep the remote management feature turned off unless it is actively used since users who have access to remote management can view screen, install any software, etc

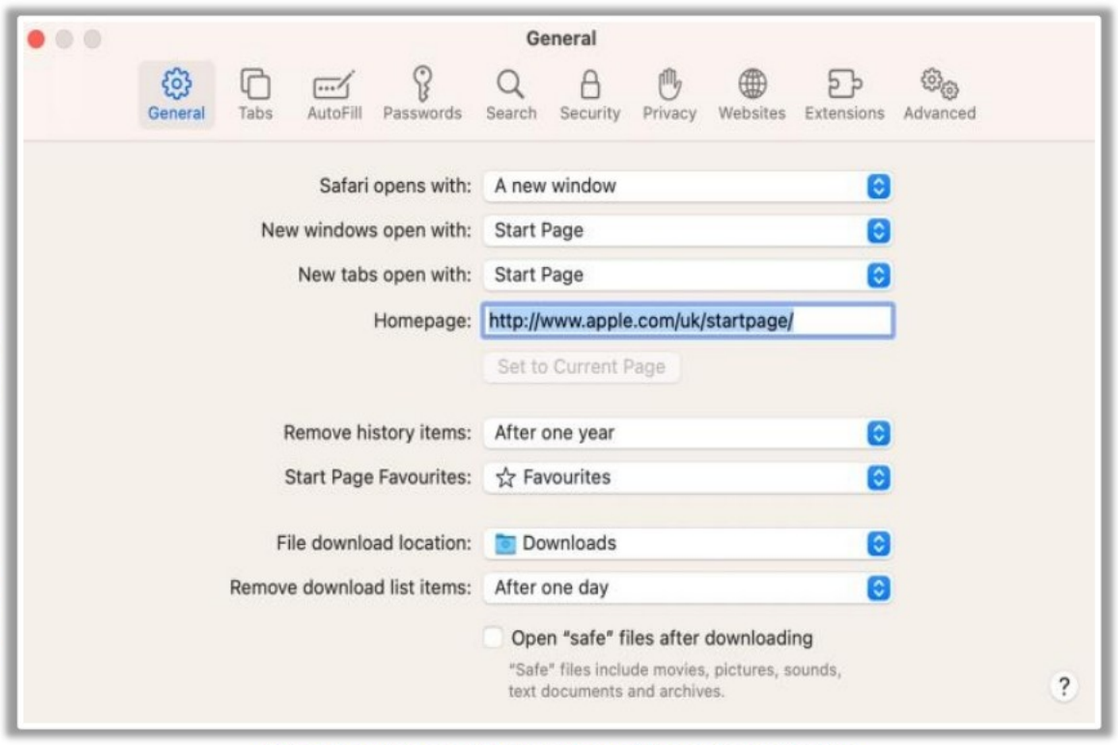


Disabling Remote Management

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Disable Automatic Opening of Downloaded Files

- When certain files are downloaded in Safari, they get executed by default without any user actions
- Although this behavior enables quick access, it **can impose security risks** as well
- To fix this, disable automatic opening of downloaded files



Disabling Automatic Opening of Downloaded Files

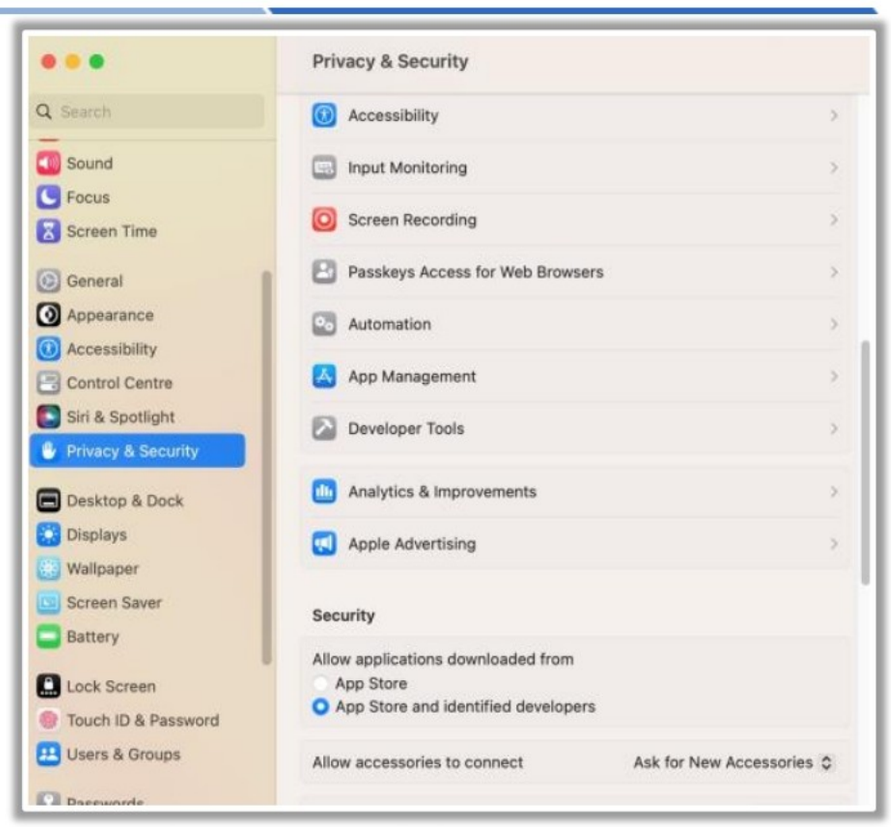
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Use Anti-malware Software

- Protect a Mac system from malware by using software only from reliable sources
- Apple uses the following process to quickly identify and block malware
  - **Preventing the execution of malware**: This is done by **Appstore**, or **Gatekeeper** combined with **Notarization**
  - **Block malware from running on client systems**: This is done by **Gatekeeper** and **XProtect**
  - **Mitigating the malware**: This is done **by XProtect**

- **Steps to specify the sources of software to be installed on Mac**
  - Go to **Apple** menu -> **System Settings**, -> click **Privacy & Security**
  - Go to **Security** and select the sources from which software is to be installed:
    - **App Store** allows apps only from the Mac App Store
    - **App Store and identified developers** allows apps from the Mac App Store and apps from identified developers

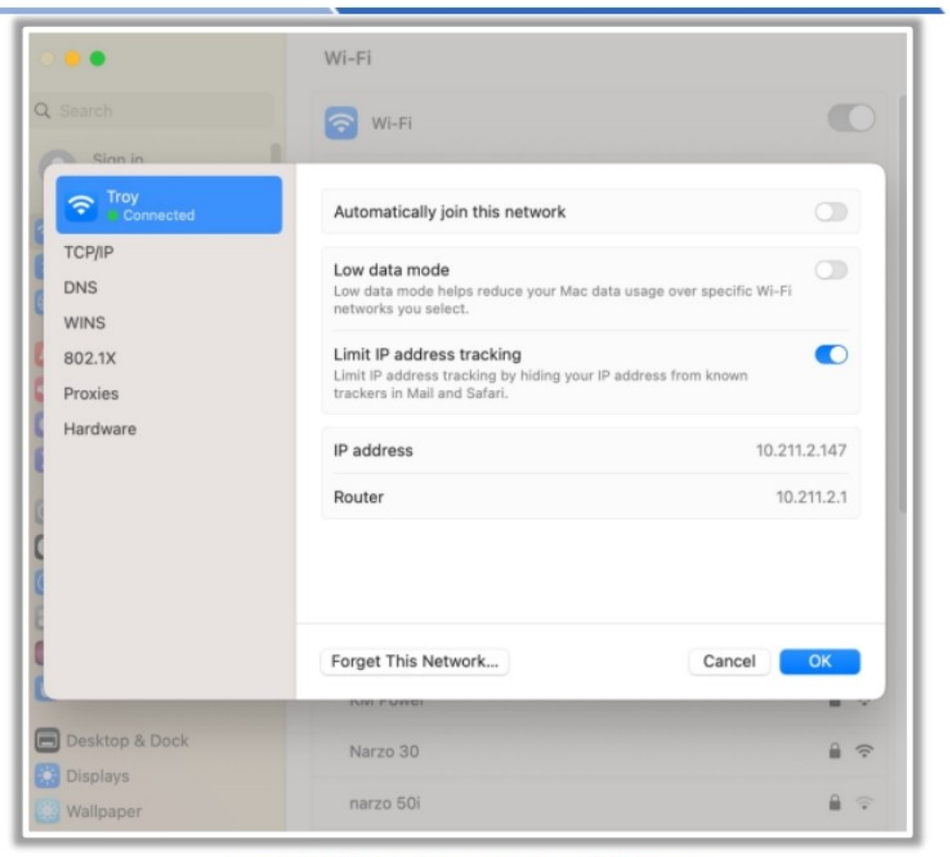


Specifying the Sources of Software to be Installed on Mac

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Turn off Wi-Fi Automatic Join Feature

- The Wi-Fi Automatic Join feature enables a device to automatically connect to known or trusted Wi-Fi networks without any credentials to be entered each time
- Turning off this feature enhances the user's control over the device and improves its privacy and security



Turning off Wi-Fi Automatic Join Feature

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Remove or Uninstall Unnecessary Software/Packages

- Regularly review all the installed software and packages, and clean up those that are no longer in use to run the OS securely and freely

Steps for uninstalling unnecessary software/packages are as follows:

- Open **Launchpad** -> find the **application to be uninstalled** -> click and hold the app icon until it starts to jiggle -> click on the **"X"** symbol appearing on the app's icon to uninstall it



Uninstalling Unnecessary Software/Package

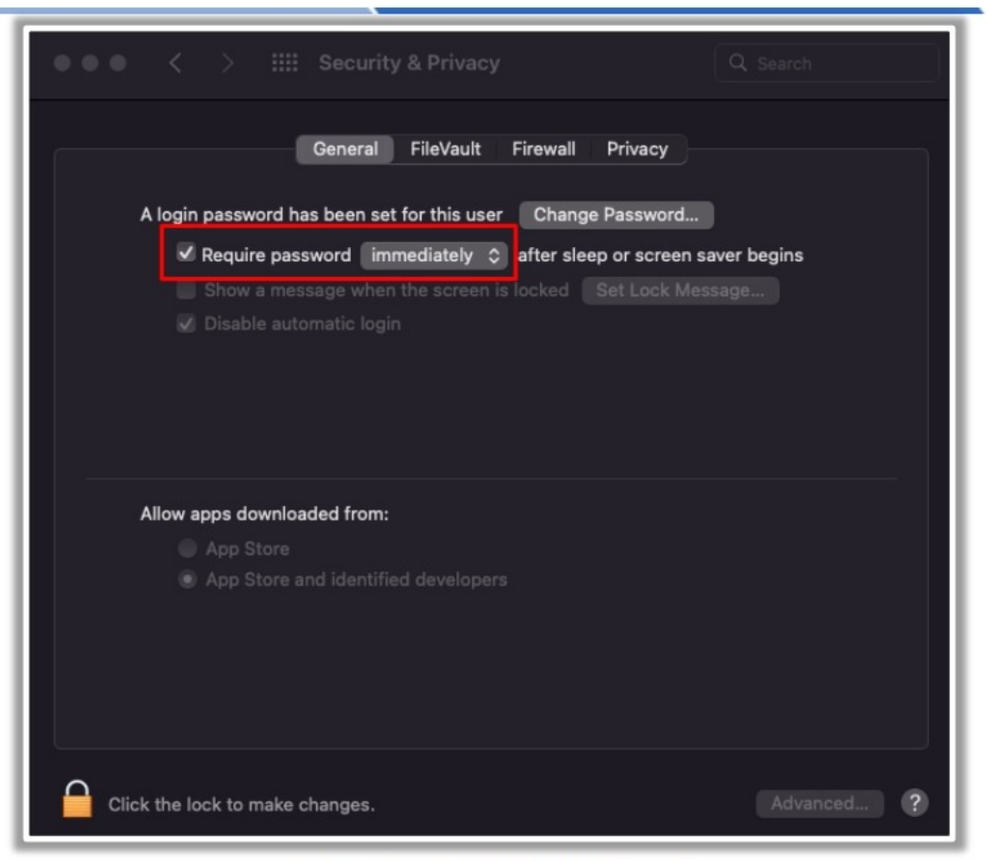
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enable Password Protected Screen Saver

- Enabling a password protected screen saver ensures that only authorized user can access the machine

Steps for enabling a password protected screen saver are as follows:

- Go to Apple menu -> **System settings** -> click **Lock screen** -> click the **pop-menu** next to "**Require password after screen saver begins or display is turned off**"



Enabling Password Protected Screen Saver

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Disable Spotlight Suggestions

- Spotlight suggestions in macOS helps the user quickly find applications, documents, emails, and so on
- Disable Spotlight suggestions by turning off Siri suggestions to let Spotlight search only the content of your Mac and not the web

Steps for disabling Spotlight suggestions are as follows:

- Go to **Apple menu** -> **System settings** -> click **Siri and suggestions** -> **Scroll down** -> **Search results** -> Deselect the **Siri suggestions** tick box

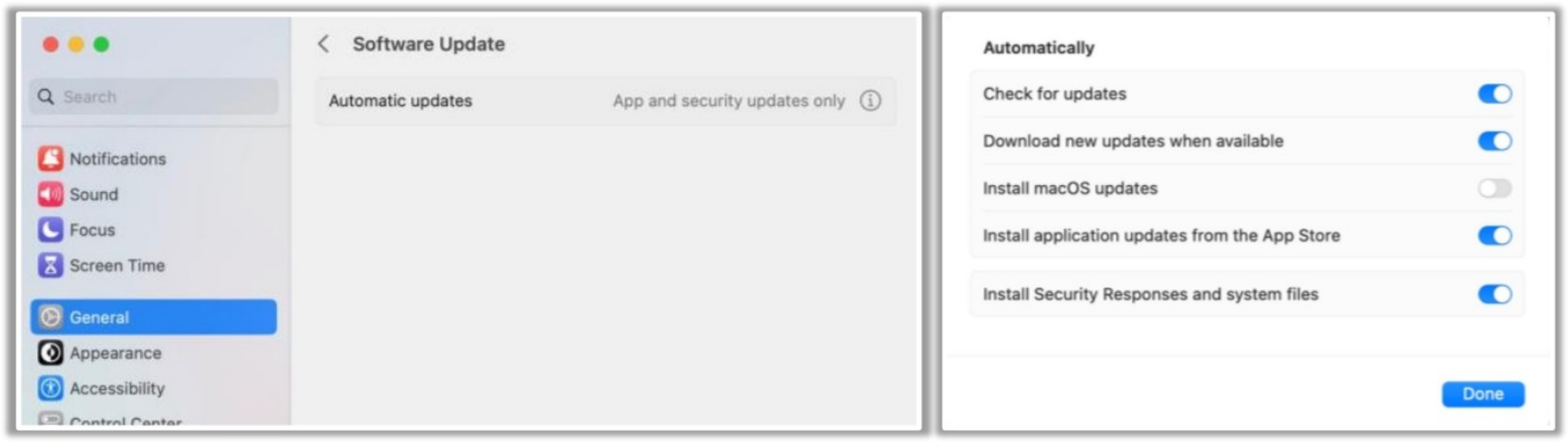


Disabling Spotlight Suggestions

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enable Auto Updates

- Enable auto-update to keep the **system updated** with latest security measures



Enabling Automatic Updates

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

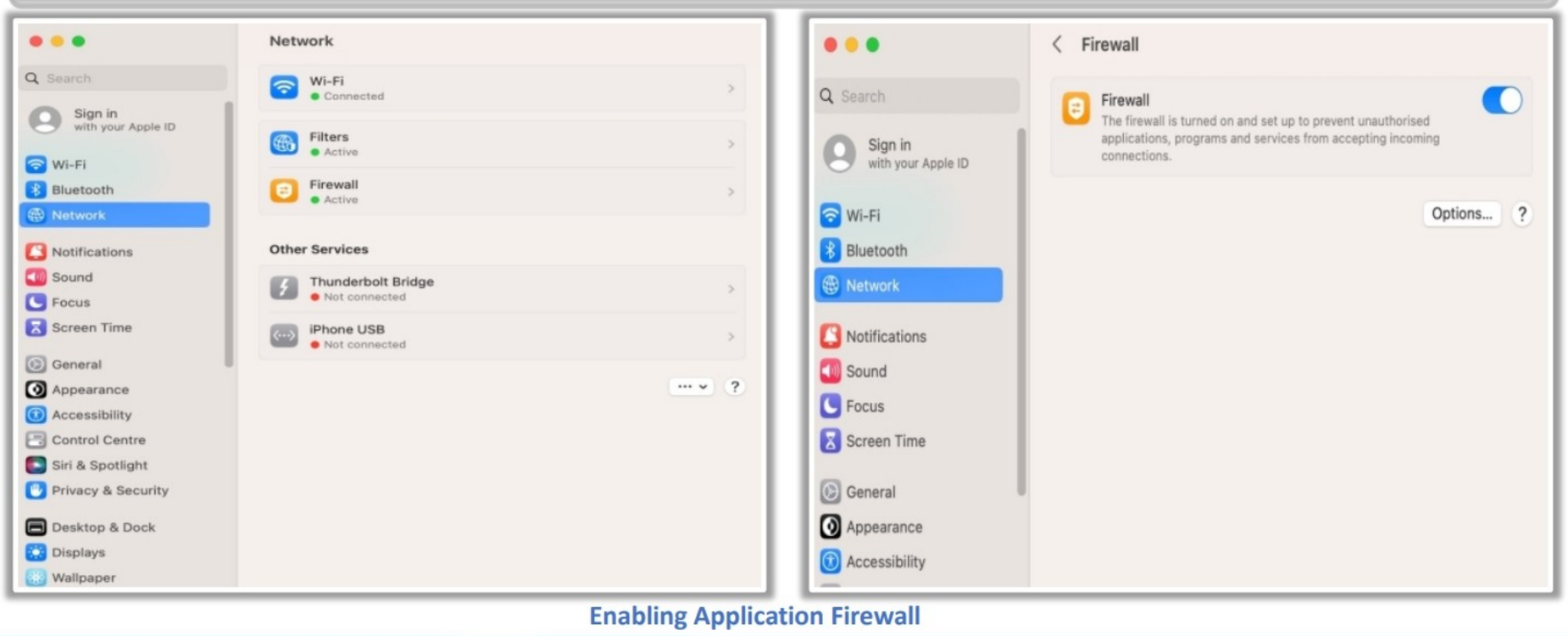
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

LO#06: Discussing macOS network security and remote security

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Security: Turn on Application Firewall

- Turn on Application Firewall to protect Mac from **unauthorized connections** initiated by other computers when connected



Enabling Application Firewall

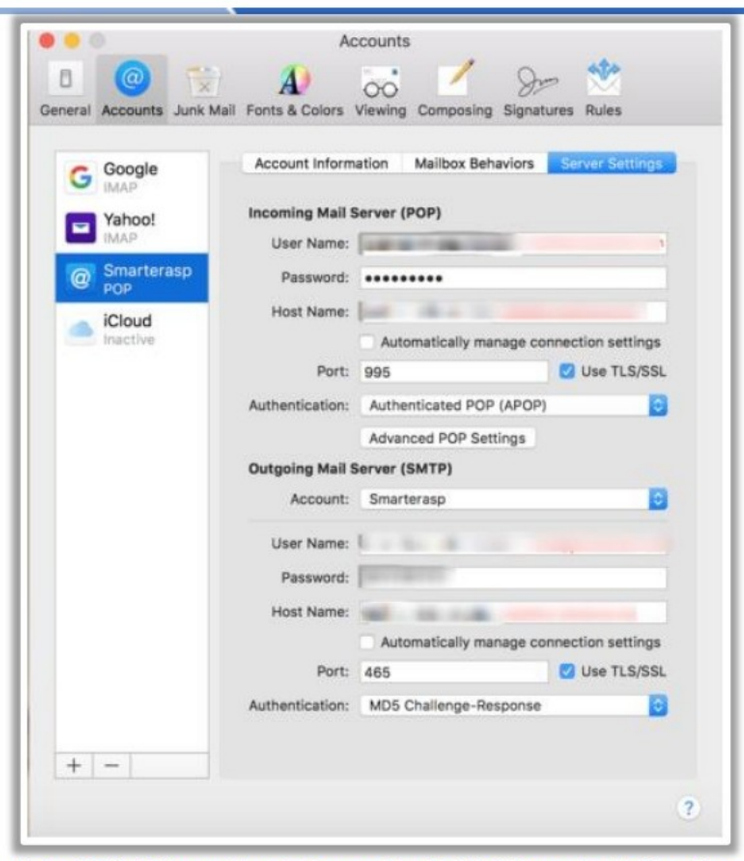
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Network Security: Use SSL/TLS Encryption

Use SSL/TLS encryption while connecting to the outgoing mail server on Mac

Ask the email provider to share information to connect to the **outgoing mail server using SSL** for the outgoing mail server (SMTP)



Using SSL/TLS Encryption to Connect to the Mail Server in Mail on Mac

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Security: Enable Network Segmentation

Set up virtual local area network (VLAN) on Mac to create independent virtual networks within a local area network (LAN), which allows the physical network to be segmented and thus secures network administration



Creating a VLAN

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

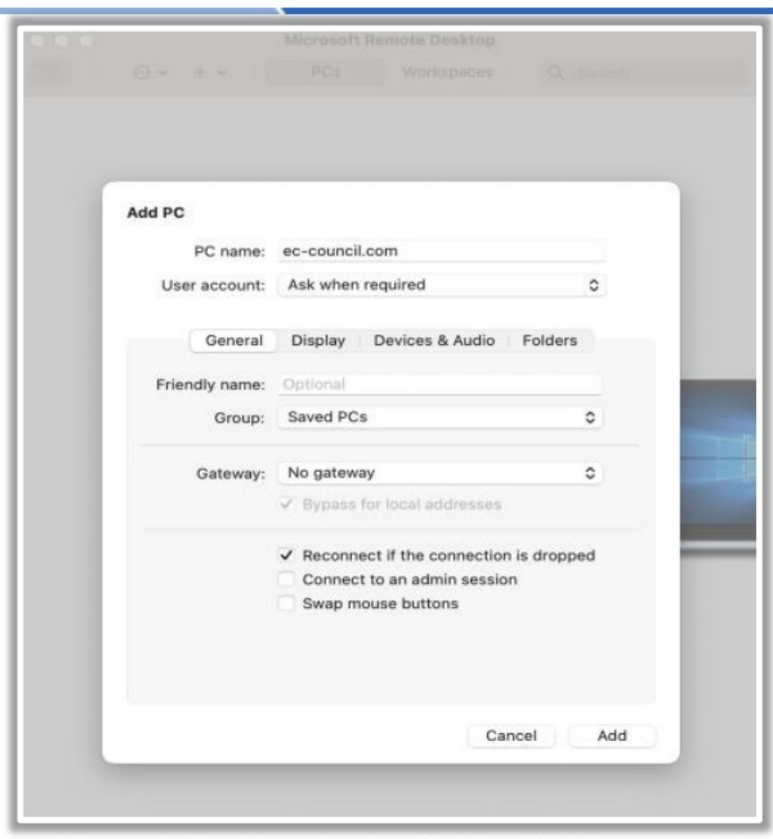
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Remote Security: Setup Remote Desktop

- Set up Apple Remote Desktop to **control the screen and user communication**, manage a list of systems, and so on

Requirements to Setup Remote Desktop

- Ensure Mac system is running OS X 10.10.5 or later
- Ensure Mac client system has version 3.6 or later of the Remote Desktop client software for full control
- Ensure the non-Mac client system has virtual network computing (VNC)–compatible software



Setting up RDP to Connect to a Non-Mac Client (Windows computer) from MacOS

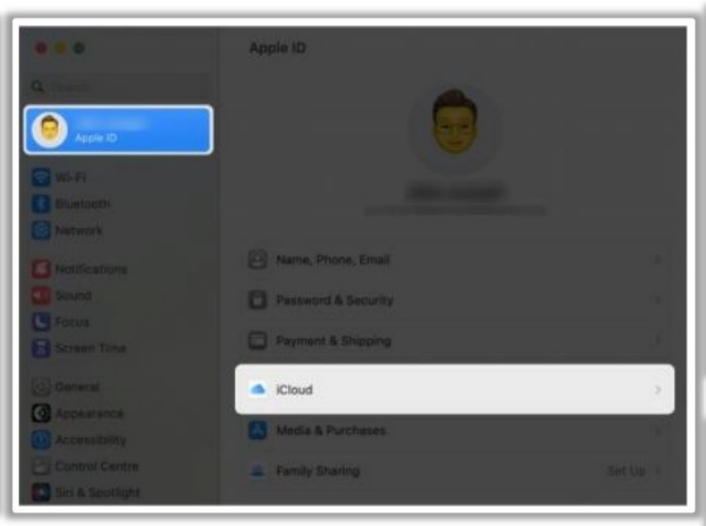
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Remote Security: Use IP Filtering

Turn off iCloud Private Relay temporarily for a website that requires your IP address to be visible and relies on IP filtering, monitoring, or rate-limiting



Step 1: System Settings



Step 2: Select iCloud



Step 3: Select Private Relay



Step 4: Turn Off Relay

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

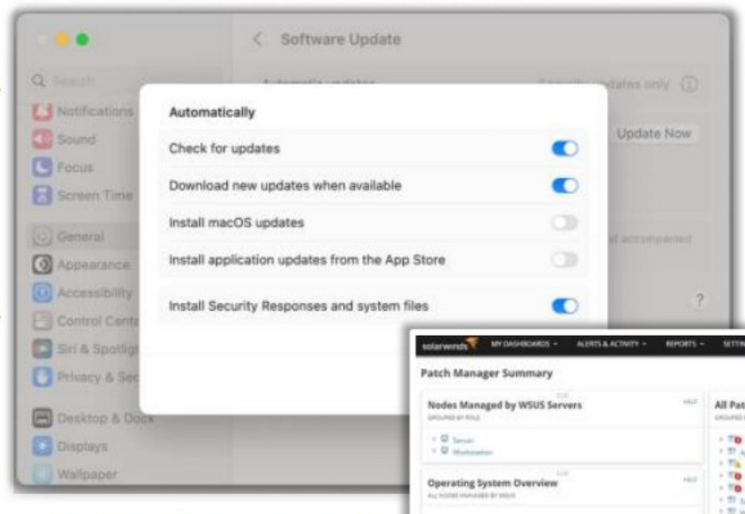
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

LO#07: macOS patch management

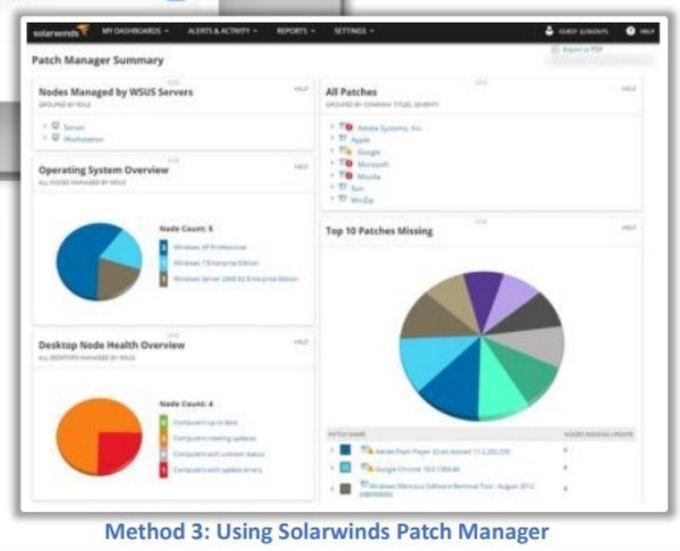
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

macOS Patch Management

- macOS patch management refers to the process of **updating the macOS** and all the Mac applications regularly
- This process also involves gathering all information about **missing patches** from the end point and installing them to enhance the security of the operating system
- Apple does not have standardized patching schedule for MacOS security. Thus, MacOS system admins should consistently check devices for **patch availability**
- **Method 1:** Type **`sudo softwareupdate -i update_pkg_name`** to install new updates on macOS



Method 2: Using Configuration Profile



Method 3: Using Solarwinds Patch Manager

Source: *www.solarwinds.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Challenges in macOS Patch Management

C|ND Certified Network Defender

Challenges in macOS Patch Management

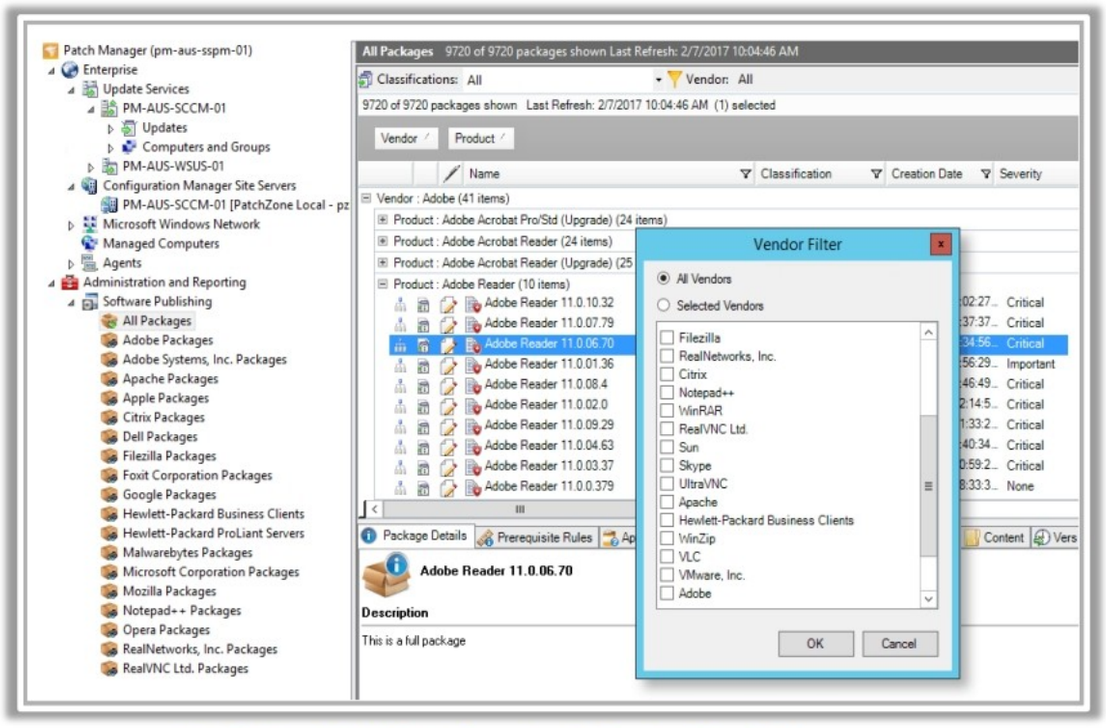
- Time-consuming patching process
- Lack of endpoint visibility
- Scheduling installation at the right time
- Prioritizing patches for deployment
- Managing multiple systems

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Prioritize Critical Patches

C|ND Certified Network Defender

- Prioritizing critical patches is a crucial step in the patch management process as this steps help **identify and mitigate** the highest risks first
- Organizations can delay larger patches such as operating system updates if there are no **critical vulnerabilities** to be patched
- Higher the number of various versions of MacOS used across the organization, higher is the **level of risk** that needs to be managed by the system admins. Thus, it is a best practice to **use a single updated version** of MacOS across all systems



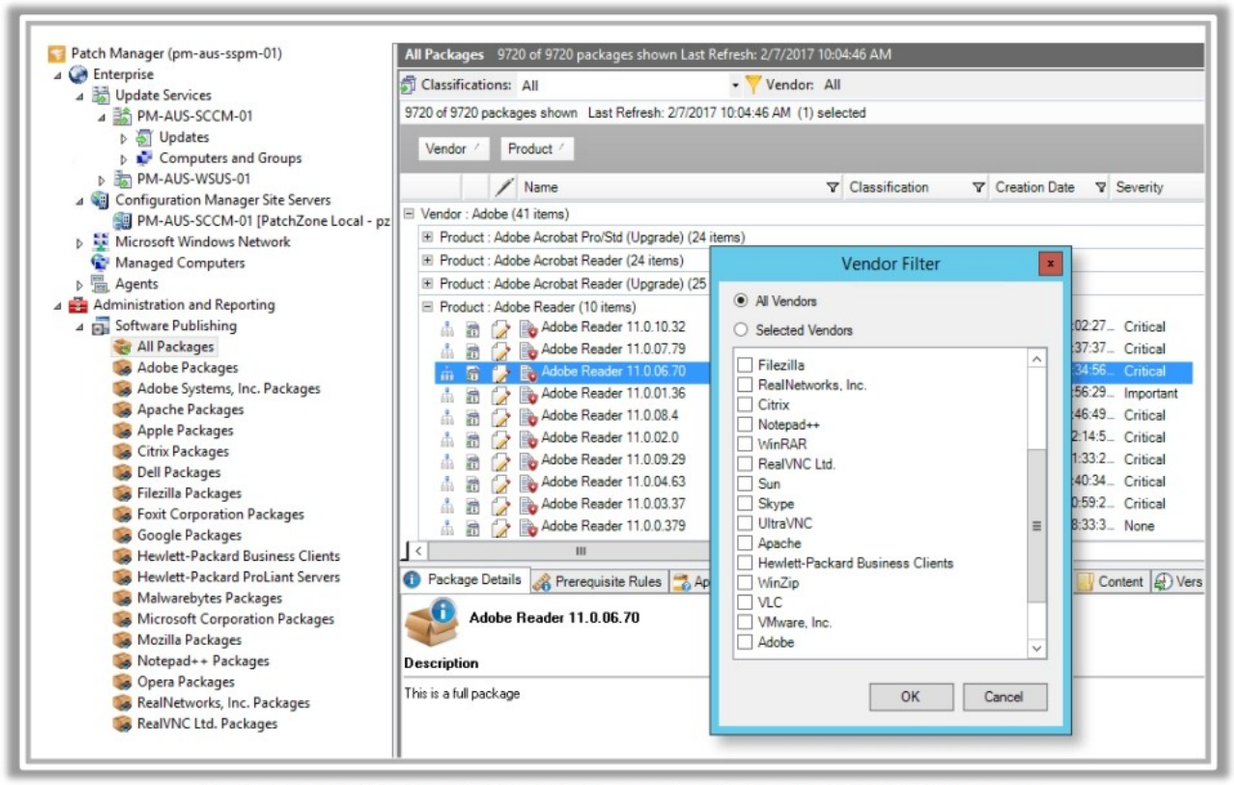
Prioritizing Critical Patches using Solarwinds Patch Manager

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Test Patches Before Deploying

- Sometimes, a patch can cause **compatibility issues**. Thus, it is a best practice to test the patch across a small group of systems to avoid compatibility issues
- As the organization gets enough time to test the patches in simulated environment, they should **ensure to buffer the users** from any surprises

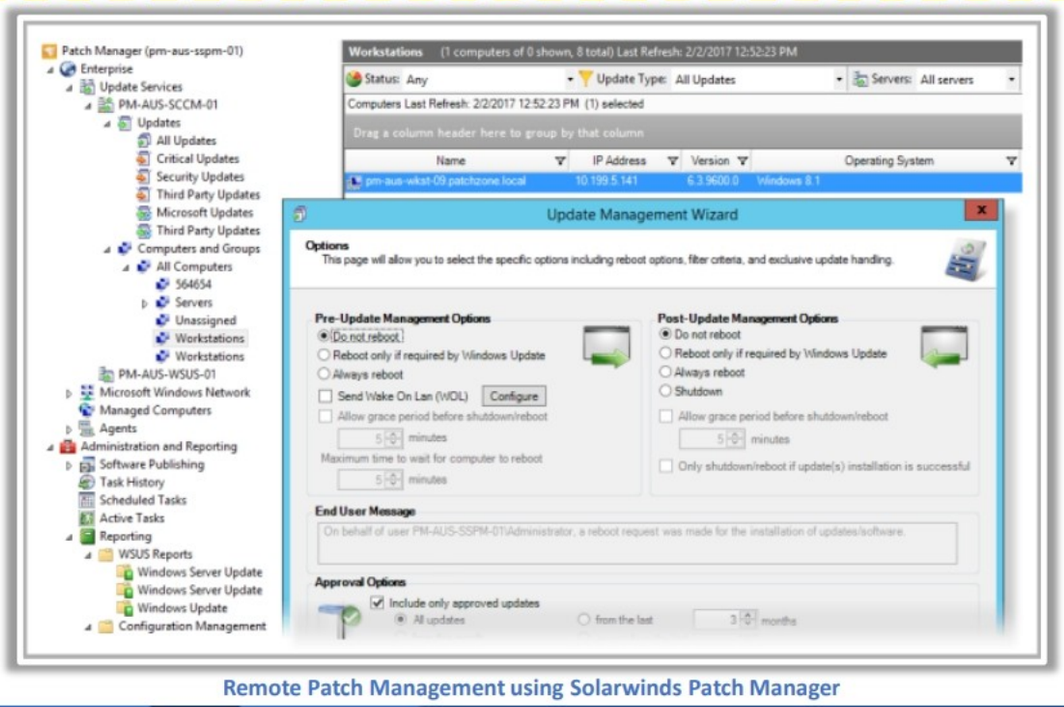


Analyzing and Testing Critical Patches using Solarwinds Patch Manager

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Remote Patch Management

- Use the remote patch management software that enables organizations to check for the latest updates and the status of their deployment



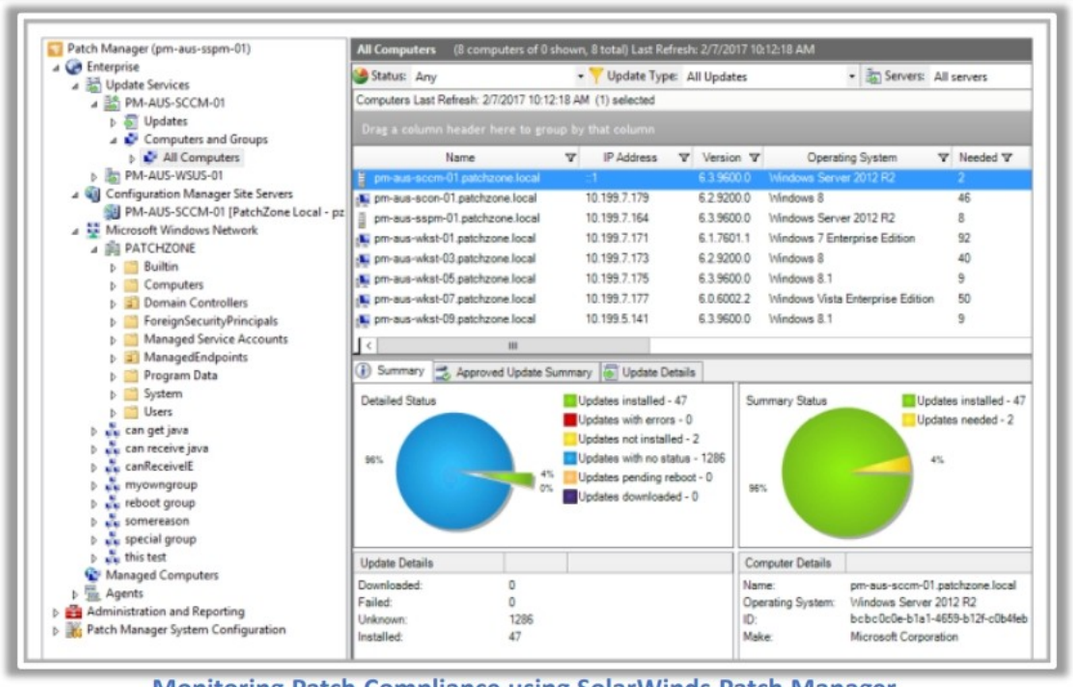
Remote Patch Management using Solarwinds Patch Manager

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Monitor Patch Compliance

- Monitor patch compliance to check whether all **the patches are compliant**, i.e., the **patches are updated** to meet organizational security standards

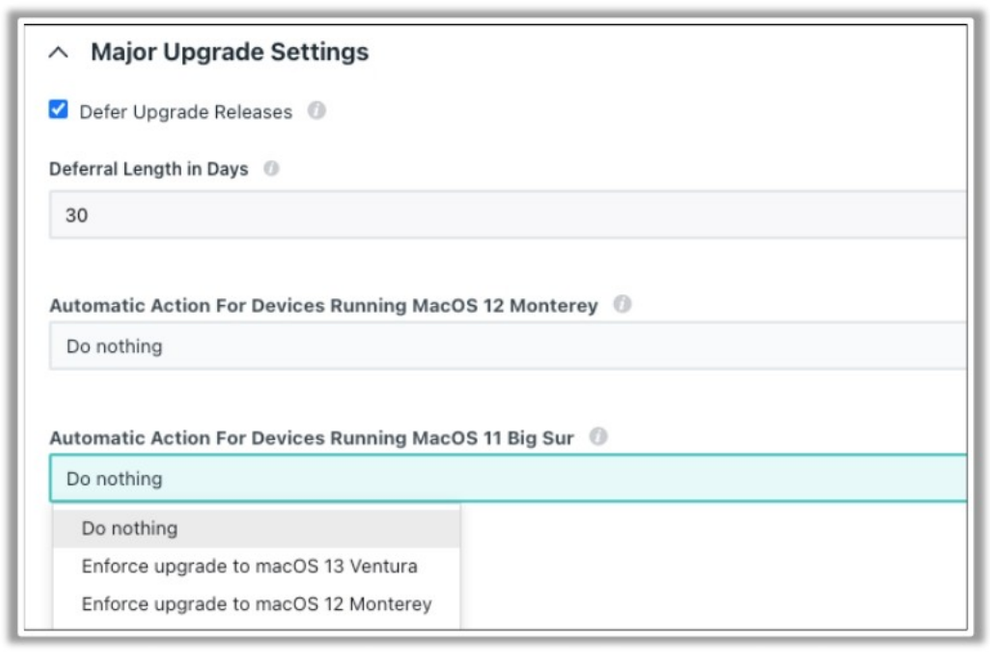


Monitoring Patch Compliance using SolarWinds Patch Manager

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Create Patch Management Policy

- Create a patch management policy that is comprised of **steps and procedures to manage and mitigate** vulnerabilities in an organization through a regular and well-documented process



Creating Patch Management Policy using JumpCloud's Automated Patch Management

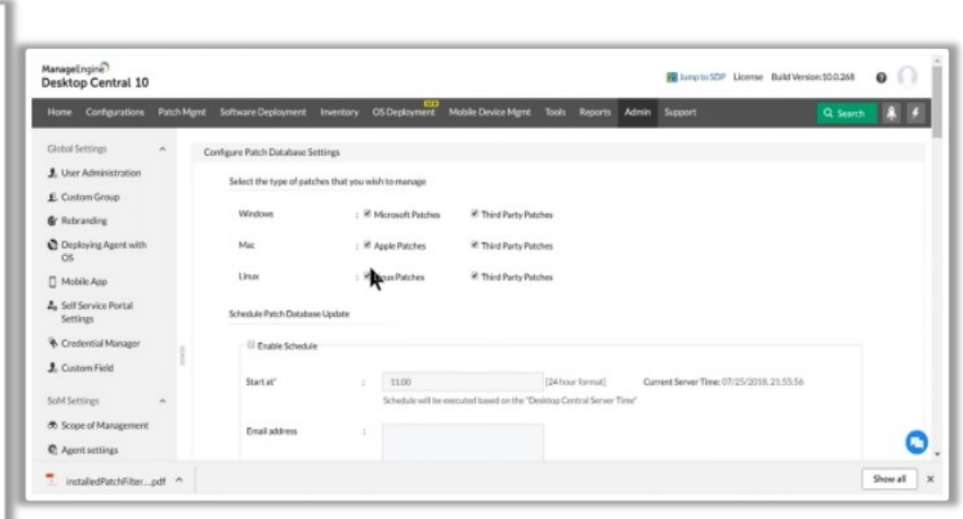
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Patch Management Tool: ManageEngine Patch Manager Plus

- Patch Manager Plus, a MacOS patch management tool, involves managing MacOS endpoints by gathering a complete list of all the **missing patches through a scan**, testing the missing patches in non-production machines checking for compatibility issues, and then **rolling out into production environment** for deployment

- **Key features:**
  - Automated patch management
  - Cross-platform and heterogeneous end support
  - Flexible deployment policies
  - Test and approve patches before bulk deployment
  - Decline patches based on IT needs
  - Reports and compliance audits



Patch Manager Plus Deployment in MacOS

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

macOS Patch Management Solutions

ManageEngine Endpoint Central
https://www.manageengine.com

ManageEngine Patch Manager Plus
https://www.manageengine.com

Heimdal Patch & Asset management
https://heimdalsecurity.com

ninjaOne Patch management
ninjaOne Patch management
https://www.ninjaone.com

Atera Patch management
https://lp.atera.com

jumpcloud Patch management
https://jumpcloud.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- The primary operating system for Apple's Mac computers, macOS, is developed and marketed by Apple Inc. since 2001
- Apple File System (APFS) is the default file system in macOS
- The macOS security features included are Keychain Access, FileVault, Time Machine, Secure Boot, Gatekeeper, etc
- The macOS user access and password management can be done using separate user log-ins, implementing Principle of Least Privilege (PoLP), implementing encryption for removeable storage, enabling automatic logout, etc
- The macOS hardening techniques included are setting a firmware password, disabling remote management, disabling automatic opening of downloaded files, uninstalling unnecessary software, etc
- The macOS network security and remote security involves turning on application firewall, using SSL/TLS encryption, enabling network segmentation, setting up remote desktop, and using IP filtering
- The challenges involved in macOS patch management and various patch management tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.