



CompTIA Network+ N10-009 Course Notes



**Technical  
Institute of America**

**Network+ N10-009**

**Course Notes**

Andrew Ramdayal



## CompTIA Network+ N10-009 Course Notes

# CompTIA Network+ N10-009

- **90-minute time limit**
- **Maximum of 90 Questions**
  - Multiple choice
    - Pick one or many answers.
  - **Performance-based (Simulators)**
    - These are hands-on troubleshooting scenarios where you'll have to perform a series of steps/commands
    - Match objects to a diagram.
- **720 (80%) out of a scale of 100-900**

[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)



CompTIA Network+ N10-009 Course Notes

# CompTIA Network+

## N10-009

Domain	% of Exam
<b>1. Network Concepts</b>	23%
<b>2. Network Implementation</b>	20%
<b>3. Network Operations</b>	19%
<b>4. Network Security</b>	14%
<b>5. Network Troubleshooting</b>	24%
<b>Total</b>	100%



## CompTIA Network+ N10-009 Course Notes

# Introduction to networking

No objectives

With the help of network you can access the data of one computer from other computer, it may be videos, images, files or web servers, etc.

## What is a network

A computer network is a system of interconnected computers and other devices that communicate and share resources and information.

Networks can be categorized by their size and structure.

The main purpose of all networks is to share resources (data, devices, applications, etc.)



## CompTIA Network+ N10-009 Course Notes

# What is on a network

**Hosts** are devices or systems on a network that use, provide, or share resources and services, such as computers, servers, and network-enabled devices. Generally any device with an IP address



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)



## CompTIA Network+ N10-009 Course Notes

# What is on a network

**Server** is a computer or system that provides resources, data, services, or programs to other computers, known as clients, over a network.





## CompTIA Network+ N10-009 Course Notes

# What is on a network

**Workstation** is a high-performance computer designed for technical or scientific applications, often used by one person at a time.





## CompTIA Network+ N10-009 Course Notes

# What is on a network

**Client machine** is a computer or device that accesses services, applications, or resources provided by a server over a network.





## CompTIA Network+ N10-009 Course Notes

# What is on a network

**Network Devices** allows servers, workstations, and client computers to connect and share resources. Such routers, switches, AP, and firewalls.





## CompTIA Network+ N10-009 Course Notes

# Types of network

## **Local Area Network (LAN):**

Covers a small geographic area like a home, office, or building. Typically used for sharing resources such as files and printers.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)



## CompTIA Network+ N10-009 Course Notes

# Types of network

**Wide Area Network (WAN):**  
Spans a large geographic area,  
often a country or continent.  
The internet is the largest  
example of a WAN.





## CompTIA Network+ N10-009 Course Notes

# Types of network

**Metropolitan Area Network (MAN):** Covers a larger area than a LAN but smaller than a WAN, such as a city.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

13



## CompTIA Network+ N10-009 Course Notes

# Types of network

**Campus Area Network (CAN)** is a type of network that interconnects multiple local area networks (LANs) within a limited geographical area, such as a university campus, corporate campus, or a large industrial complex.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)



## CompTIA Network+ N10-009 Course Notes

# Types of network

**Storage Area Network (SAN)** is a high-speed network that provides access to consolidated data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, so that they appear to servers as locally attached devices.



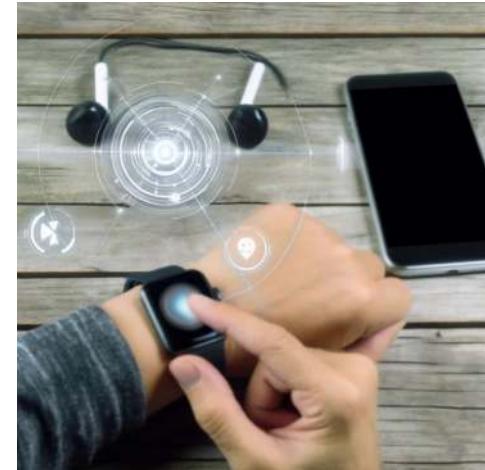


## CompTIA Network+ N10-009 Course Notes

# Types of network

## **Personal Area Network (PAN):**

Covers a very small area, usually within a single room. Examples include Bluetooth connections between a phone and a headset.

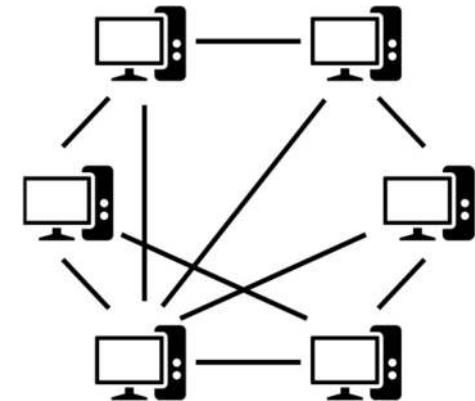


[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)



# Network Architecture

**Peer-to-peer network:** decentralized network architecture where each device (peer) in the network can act both as a client and a server, allowing direct sharing of resources, data, and services among all connected devices without the need for a central server.



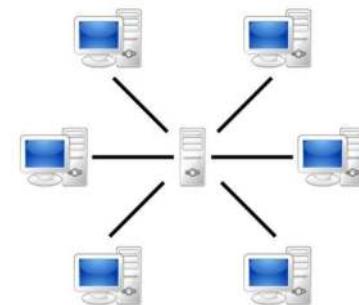
<https://en.wikipedia.org/wiki/Peer-to-peer>



# Network Architecture

**Client-server network:** a network architecture where multiple client devices (computers, smartphones, etc.) connect to a central server to access shared resources, services, and applications.

The server manages and provides the requested services while the clients initiate requests and utilize the services provided by the server.



<https://en.wikipedia.org/wiki/Peer-to-peer>

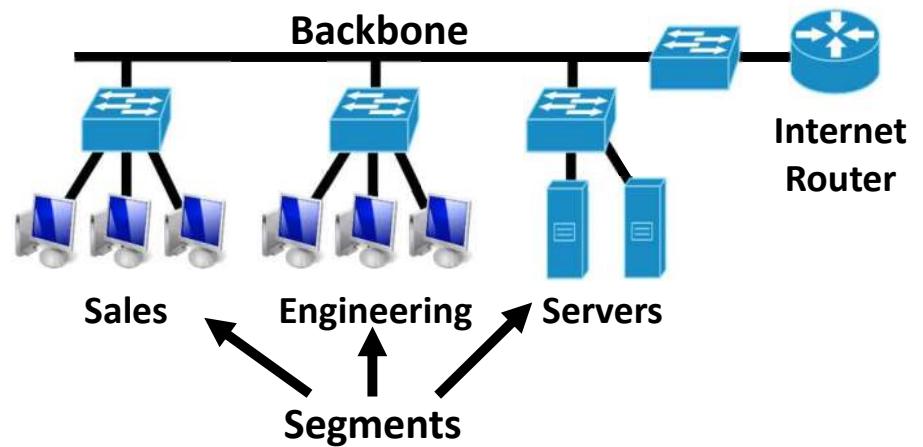
[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)



## Backbone and Segments

A **network backbone** is the main infrastructure that interconnects various segments of a computer network, providing a central pathway for data exchange.

It is typically composed of high-speed, high-capacity links and core routers or switches, which handle the bulk of network traffic and ensure efficient data transmission across the network.





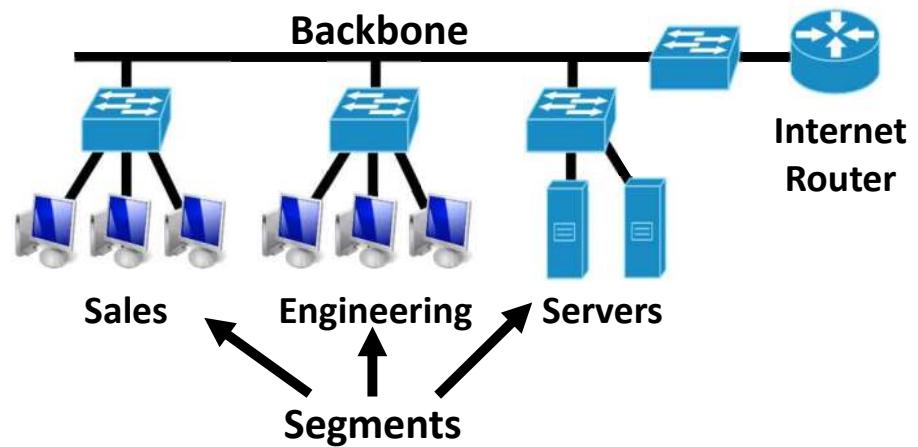
## CompTIA Network+ N10-009 Course Notes

# Backbone and Segments

**Network segments**, on the other hand, are smaller subnetworks or clusters of devices that connect to the backbone.

Each segment can include a variety of networked devices such as computers, servers, switches, and other hardware.

Segments often represent different departments or areas within an organization, and they rely on the backbone to communicate with other segments and access shared resources and services.





## Network Topologies

Network topologies describe the **layout or arrangement of elements** (links, nodes, etc.) of a computer network.

There are several types, each with **unique configurations and characteristics**, influencing the network's performance, reliability, and scalability.



## Point-to-Point

This topology involves a **direct connection** between two networking devices, typically using a single cable or wireless link.

It is mainly used for **dedicated connections**, such as those between a main office and a branch office, or between two pieces of network equipment.



Site-to-Site WAN link



Host-to-Host PAN link



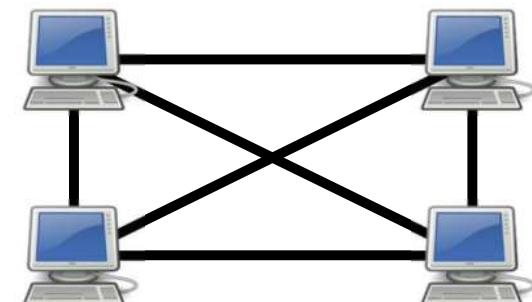
## CompTIA Network+ N10-009 Course Notes

# Mesh

Mesh topology is a network setup where each host is connect to every other host, creating a network with **no central connecting point**.

This topology ensures **high availability and redundancy** because if any one link fails, data can be rerouted through multiple alternative paths.

- Advantages
  - Most fault-tolerant
- Disadvantages
  - Most expensive
  - Most complex
  - Most difficult to expand

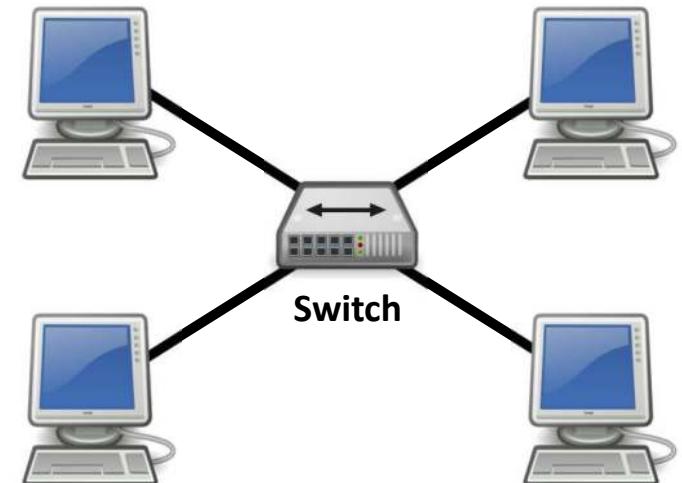




## Star/Hub-and-Spoke

In a star or hub-and-spoke topology, **all nodes are connected to a central node such as hubs/switches/Wireless access points.**

This setup simplifies network management and troubleshooting but **creates a single point of failure**, as the failure of the central hub can bring down the entire network.





## CompTIA Network+ N10-009 Course Notes

# Hybrid

**Hybrid topology **combines two or more different topologies** to form a resultant topology that leverages the advantages and mitigates the disadvantages of the constituent topologies.**

It offers **flexibility** in network design and can be tailored to meet specific needs or constraints of an organization.

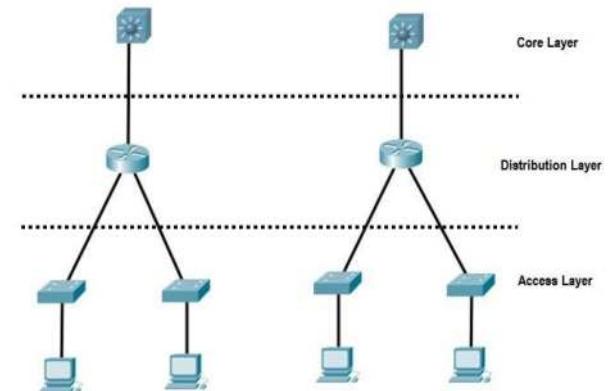


## CompTIA Network+ N10-009 Course Notes

# Three-tier Hierarchical Model

The three-tier hierarchical network model is a structured approach to network design that breaks the network into three distinct layers.

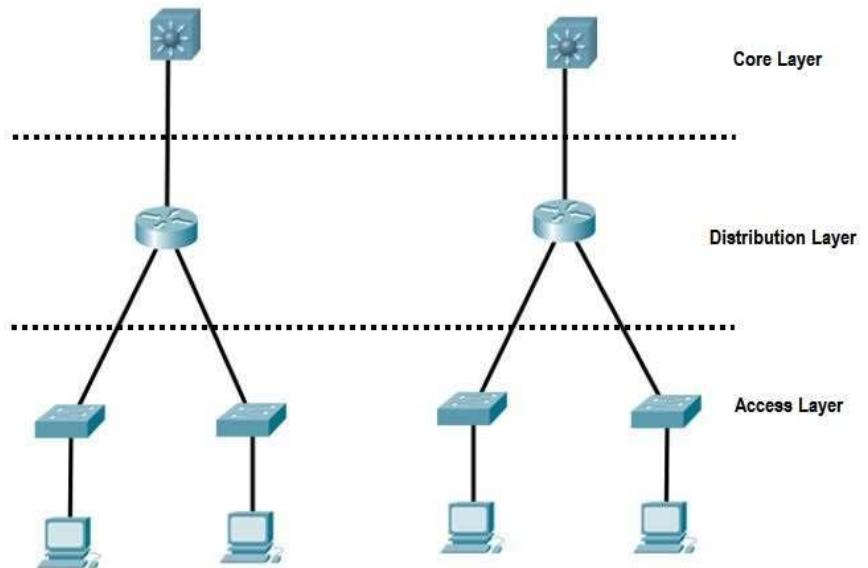
**Each layer is designed to serve a specific purpose**, optimizing scalability, performance, and maintainability.





CompTIA Network+ N10-009 Course Notes

# Three-tier Hierarchical Model



<https://www.techtutsonline.com/cisco-three-layer-hierarchical-model/>  
[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com) 27



## Core Layer

The core layer is the backbone of the network, handling high-speed packet switching across the entire network.

It is **responsible for fast and reliable routing** of data and should have high redundancy and fault tolerance to prevent downtime.



## CompTIA Network+ N10-009 Course Notes

# Distribution Layer

The distribution layer acts as the intermediary between the core and access layers, managing routing, filtering, and WAN access.

It **aggregates the data** received from the access layer switches before it is transmitted to the core layer for routing to the final destination.



## Access Layer

The access layer is the network's point of entry for devices and end users, connecting them to the network.

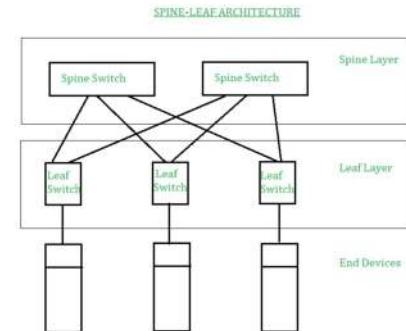
This layer includes switches and access points that **provide connectivity** to desktop PCs, laptops, and other network devices.



## Spine and Leaf

Spine and leaf architecture is a **two-layer** network topology that is highly scalable and **minimizes latency** by ensuring that every leaf switch (access layer) is separated by no more than two switches from any other leaf switch.

In this topology, leaf switches form the access layer where devices are connected, while spine switches serve as the backbone for data transport, connecting all leaf switches without interconnecting with each other.

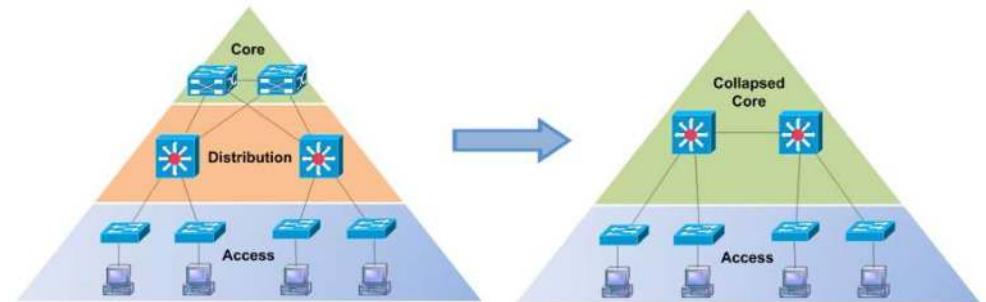


<https://www.geeksforgeeks.org/spine-leaf-architecture/>



CompTIA Network+ N10-009 Course Notes

## Collapsed Core Architecture





## Collapsed Core Architecture

**Collapsed core architecture** merges the core and distribution layers into a single layer, simplifying the network design and reducing hardware costs.

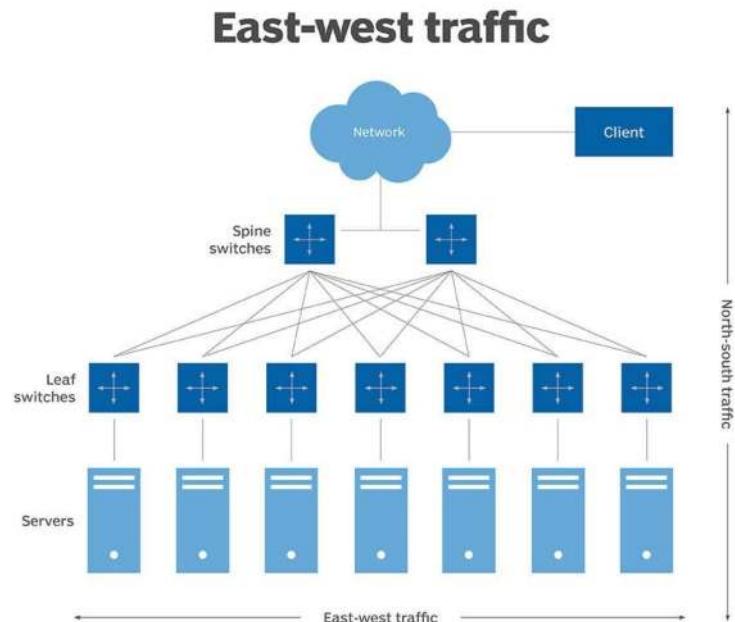
This approach is ideal for **small to medium-sized networks** where managing separate layers is unnecessary.

The architecture facilitates easier management and maintenance, while enhancing performance by reducing latency between the network's core and distribution functions.



## CompTIA Network+ N10-009 Course Notes

# North-South Traffic



© 2017 TechTarget. All rights reserved. TechTarget

<https://www.techtarget.com/searchnetworking/definition/east-west-traffic>



## CompTIA Network+ N10-009 Course Notes

# North-South Traffic

This describes the flow of network traffic between the **data center** and the **outside world** (e.g., the internet or other data centers), focusing on inbound and outbound traffic patterns.

It typically involves client-to-server communication, where clients access services **hosted in the data center**.



## CompTIA Network+ N10-009 Course Notes

# East-West Traffic

Refers to the traffic flow **within the data center**, especially in modern data centers.

This includes server-to-server, server-to-storage, and VM-to-VM traffic, highlighting the importance of efficient **internal networking** to support high volumes of internal data exchange.

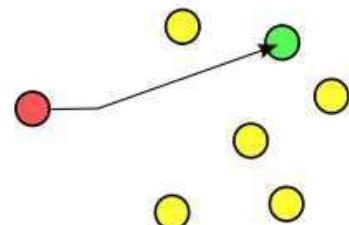


## Unicast

Unicast is a one-to-one form of communication where data is **sent from one source to one specific destination** identified by a unique IP address.

It is the **most common form of IP communication**, used for most internet traffic, including web browsing, email, and file transfers.

Unicast communication ensures that data packets are **delivered to a single, specific recipient** over a network.



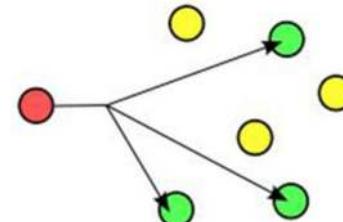


## Multicast

Multicast is a method of communication where data is sent **from one or more sources to multiple destinations simultaneously** over a network, using a specific multicast group address.

Multicast is efficient for applications like streaming video or audio, **where the same data needs to be delivered to multiple recipients**, reducing the bandwidth consumption compared to sending separate copies of the data to each recipient.

This approach is used in both IPv4 and IPv6 networks to **optimize the delivery of packets to multiple destinations**.





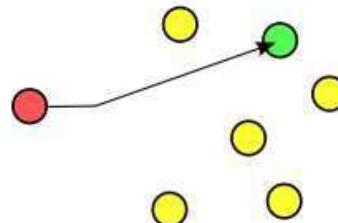
## CompTIA Network+ N10-009 Course Notes

# Anycast

Anycast is a network addressing and routing method where data is sent to the **nearest or best destination as determined by routing protocols**, from among multiple potential destinations sharing the same address.

It is used in IPv6 (and to a lesser extent in IPv4) to provide fast and efficient delivery of services by directing users to the closest server, **commonly used in DNS and CDN (Content Delivery Network) services.**

Anycast can improve network performance and availability by **automatically routing requests to the nearest data center.**



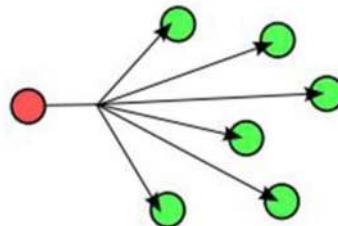


## Broadcast

Broadcast is a communication method where a message is sent from **one sender to all potential receivers** within a network segment.

In IPv4, the broadcast address is used to **send data to all devices on a LAN** simultaneously, such as when a device requests an IP address via DHCP.

Broadcast is not supported in IPv6; instead, multicast addresses are used for similar purposes.





## CompTIA Network+ N10-009 Course Notes

# OSI Model

1.1



CompTIA Network+ N10-009 Course Notes

# (OSI) Reference Model Concepts



## CompTIA Network+ N10-009 Course Notes

# What is a Protocol

*"In networking, a protocol is a set of rules for formatting and processing data. Network protocols are like a common language for computers. The computers within a network may use vastly different software and hardware; however, the use of protocols enables them to communicate with each other regardless."*

<https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/>

### Common Protocols:

- HTTP
- HTTPS
- SMTP
- FTP
- TCP
- UDP



CompTIA Network+ N10-009 Course Notes

## What is a Protocol





## CompTIA Network+ N10-009 Course Notes

# (OSI) Model

<b>Layer 7</b>	<b>Application</b>
<b>Layer 6</b>	<b>Presentation</b>
<b>Layer 5</b>	<b>Session</b>
<b>Layer 4</b>	<b>Transport</b>
<b>Layer 3</b>	<b>Network</b>
<b>Layer 2</b>	<b>Data Link</b>
<b>Layer 1</b>	<b>Physical</b>



Open Systems Interconnection



## (OSI) Model Layers

- **Internetworking models** are used to organize and describe network functions. Each layer describes a different set of unique functions.
- The **Open System Interconnection (OSI) Model** is made up of **seven layers** containing various types of hardware and software.
  - Created to achieve **interoperability** of diverse vendor devices
  - Partitions communication systems into abstraction layers
  - **Protocols** are the standard terms that computers use to understand each other



# (OSI) Model Layers

- **Mnemonics**

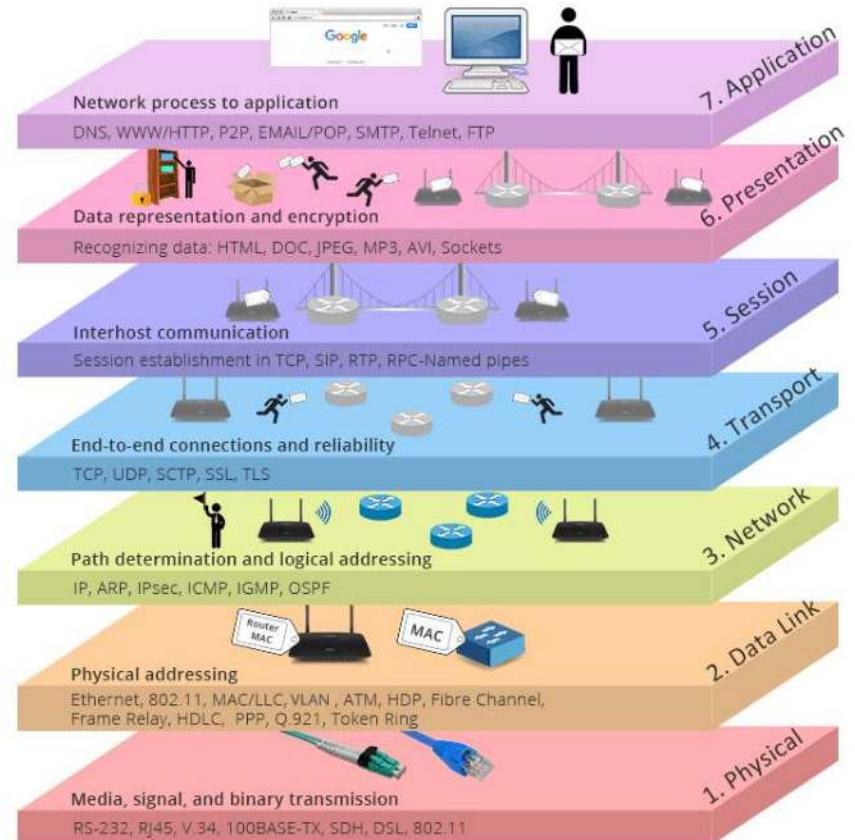
- All People Seem To Need Data Processing
- Please Do Not Throw Sausage Pizza Away

Layer 7	Application
Layer 6	Presentation
Layer 5	Session
Layer 4	Transport
Layer 3	Network
Layer 2	Data Link
Layer 1	Physical



## CompTIA Network+ N10-009 Course Notes

# (OSI) Model Layers



<https://community.fs.com/article/tcpip-vs-osi-whats-the-difference-between-the-two-models.html>

[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)



## CompTIA Network+ N10-009 Course Notes

# (OSI) Model Layers

<b>Layer 7</b>	<b>Application</b>	Generates data to be transmitted, processes data that is received
<b>Layer 6</b>	<b>Presentation</b>	Gets the data ready for the application layer by converting, translating, encoding, compressing, and encrypting data.
<b>Layer 5</b>	<b>Session</b>	Provides dialog control by allowing multiple persistent connections from different sources to be properly combined or synchronized.
<b>Layer 4</b>	<b>Transport</b>	Handles the End-to-End communication either via TCP for connection-oriented communication or UDP for connectionless communication.
<b>Layer 3</b>	<b>Network</b>	Provides communication between different networks via IP addresses
<b>Layer 2</b>	<b>Data Link</b>	Provides communication within the same network via MAC addresses
<b>Layer 1</b>	<b>Physical</b>	Converts bits into electrical signal over copper cables, or pulses of light for fiber optic cables, or radiofrequency for wireless communications



# Encapsulation / De-encapsulation

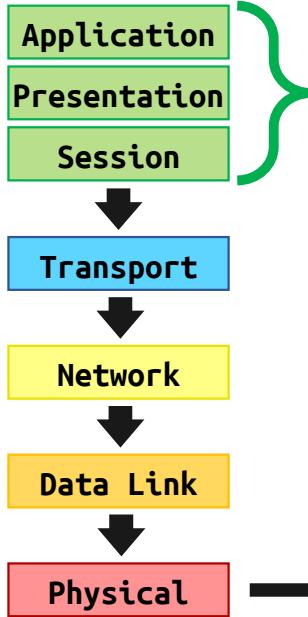
Computer 1

Computer 2

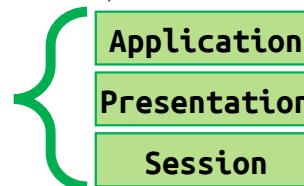


Data Transfer

Encapsulation



Bits



Mnemonic

Don't

Stop

Pouring

Free

Beer



## CompTIA Network+ N10-009 Course Notes

# Layer 7 – Application

This is the entry door to network services at a lower level

Apps uses this layer to get services when they TX or RX data over a network

Applications sit on top of this layer

Responsible for interfacing user applications, network mgmt. services, remote access etc.

The playground of hackers today



## CompTIA Network+ N10-009 Course Notes

# Layer 7 – Application

- Simple Mail Transfer Protocol (SMTP) – 25
- Simple Network Management Protocol (SNMP) - 161
- Hypertext Transfer Protocol (HTTP) – 80
- Line Printer Daemon (LPD)
- File Transfer Protocol (FTP) – 21
- Telnet – 23
- Trivial File Transfer Protocol (TFTP) – 69
- Electronic Data Interchange (EDI)
- Post Office Protocol version 3 (POP3) – 110
- Internet Message Access Protocol (IMAP) – 143
- Network News Transport Protocol (NNTP)
- Secure Remote Procedure Call (S-RPC) RPC - Session
- Secure Electronic Transaction (SET)



## CompTIA Network+ N10-009 Course Notes

### Layer 6 – Presentation Layer

Concerned about the format

Apps must use a common format

The main services are:

- Data Conversion
- Character Code Translation
- Compression
- Encryption & Decryption



## CompTIA Network+ N10-009 Course Notes

### Layer 6 – Presentation Layer

- American Standard Code For Information Interchange (ASCII)
- Extended Binary-Coded Decimal Interchange Mode (EBCDIC)
- Tagged Image file Format (TIFF)
- Joint Photographic Experts Group (JPEG)
- Motion Picture Experts Group (MPEG)
- Musical Instrument Digital Interface (MIDI)



## CompTIA Network+ N10-009 Course Notes

# Layer 5 – Session

Provides Logical persistent connection between peer hosts

Conversation between applications exchanging information

Creates, monitors, tears down sessions

Full Duplex, Half Duplex, Simplex



## CompTIA Network+ N10-009 Course Notes

### Layer 5 – Session

- Network File System (NFS)
- Structured Query Language (SQL)
- NetBIOS
- Remote Procedure Call (RPC)



## CompTIA Network+ N10-009 Course Notes

# Layer 4 – Transport

One of the busiest layers

Creates an End-to-End  
transport between peer hosts

UDP and TCP are at this layer

UDP is connectionless, best  
effort

TCP is connection oriented &  
reliable

TCP uses Flags



## CompTIA Network+ N10-009 Course Notes

# Layer 4 – Transport

- Transmission Control Protocol (TCP)
  - full-duplex connection-oriented
- User Datagram Protocol (UDP)
  - simplex connectionless
- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)
- Sequenced Packet Exchange (SPX)
- TCP and UDP Ports
- Well-Known Ports: Ports 0 - 1023
- Registered Ports: Ports 1024 - 49151
- Dynamic or Private Ports: Ports 49152 – 65535



## CompTIA Network+ N10-009 Course Notes

# Layer 3 – Network

Move data between two hosts  
not physically connected

Use logical addresses (IP)

IP is at this layer

Addressing (uses IP addresses)

IP does not guarantee delivery

It only finds the best delivery  
route

Uses routing tables to deliver  
the info

Devices: Routers



## CompTIA Network+ N10-009 Course Notes

# Layer 3 – Network

- Internet Protocol (IP)
- connectionless
- Internet Control Message Protocol (ICMP)
- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGP)
- Internet Group Management Protocol (IGMP)
- Supports multicasting
- Internetwork Packet Exchange (IPX)
- Internet Protocol Security (IPSec)
- Network Address Translation (NAT)
- Simple Key Management for Internet Protocols (SKIP)



## CompTIA Network+ N10-009 Course Notes

# Layer 2 – Data Link Layer

Get packets from the Network Layer

Transmit frames

Detects errors within frames

Converts information into bits

Use MAC/Hardware addresses to communicate

Move data to the next physically connected device

Two Sub Layers

- Logical Link Layer (LLC)
- Media Access Control (MAC)

Devices: Switches and bridges



## Media Access Control layer

The Media Access Control (MAC) layer is a sublayer of the OSI model's Data Link Layer that **manages protocol access** to the physical network medium.

**It is responsible for the addressing and channel access control mechanisms** that enable several nodes to communicate within a network, typically using MAC addresses.



## Logical Link Control layer

The Logical Link Control (LLC) layer is the upper sublayer of the OSI model's Data Link Layer that provides **flow control and error control**.



## CompTIA Network+ N10-009 Course Notes

# Layer 2 – Data Link Layer

- Address Resolution Protocol (ARP)
  - Resolves IP into MAC
- Reverse Address Resolution Protocol (RARP)
  - Resolves MAC into IP addresses
- Point-to-Point Protocol (PPP)
- Serial Line Internet Protocol (SLIP)
- Layer 2 Forwarding (L2F)
- Layer 2 Tunneling Protocol (L2TP) ↗
- Point to Point Tunneling Protocol (PPTP)
- Ethernet (IEEE 802.3) – only remaining
- Token Ring (IEEE 802.5)
- Fiber Distributed Data Interface (FDDI)
- Asynchronous Transfer Mode (ATM)
- Copper DDI (CDDI)



## Layer 1 – Physical

Receive bits from the Data Link Layer

Bits converted into electrical signals

Photons or beam of light if on Fiber

Physical Topologies

Devices: Cables, Connectors, wireless access point, hub, modems etc...



## CompTIA Network+ N10-009 Course Notes

# Layer 1 – Physical

- EIA/TIA-232 and EIA/TIA-449
- X.21
- High-Speed Serial Interface (HSSI)
- Synchronous Optical Networking (SONET)
- V.24 and V.35
- Integrated Services Digital Network (ISDN)
- Digital Subscriber Line (DSL)
- 10BASE-T, 10BASE2, 10BASE5, 100BASE-TX, 100BASE-FX, 100BASE-T, 1000BASE-T, 1000BASE-SX



## CompTIA Network+ N10-009 Course Notes

# Lesson 3: Network device

1.2



CompTIA Network+ N10-009 Course Notes

# Networking Appliances, Applications, and Functions



## CompTIA Network+ N10-009 Course Notes

# Physical and virtual appliances

Physical appliances are **dedicated hardware devices** focused on specific network functions, offering high performance and reliability but at a higher cost and with space requirements.

Virtual appliances, on the other hand, are **software-based solutions** that run on virtual machines, providing similar functionalities with greater flexibility, scalability, and cost efficiency, but potentially at the expense of raw performance.



## CompTIA Network+ N10-009 Course Notes

# Router

A router operates at the **network layer** of the OSI model, directing data packets between different networks based on IP addresses.

Routers use **routing tables** to determine the best path for forwarding packets to their destination, connecting **multiple networks** together, such as a local network to the Internet.

Routers also provide network **security** features like firewalls and VPN support.





## CompTIA Network+ N10-009 Course Notes

# Switch

A switch operates at the **data link** layer of the OSI model, forwarding data based on MAC addresses.

It creates **separate collision domains** for each port, improving network efficiency by reducing collisions.

Layer 2 switches are used to connect devices **within the same network or VLAN**.





## CompTIA Network+ N10-009 Course Notes

# Firewall

A **firewall** is a network security device that **monitors** incoming and outgoing network traffic and decides whether to **allow** or **block** specific traffic based on a defined set of **security rules**.

**Firewalls** are crucial for establishing a **barrier** between secure **internal** networks and **untrusted** external networks, such as the internet, and can be hardware-based, software-based, or a combination of both.





## CompTIA Network+ N10-009 Course Notes

# IDS/IPS Device

**Intrusion Detection Systems (IDS)** can detect malicious network activity

- Uses signature identification techniques like antimalware
- Additionally, can detect malicious activity based on anomalous behavior

An **Intrusion-prevention system (IPS)** is used to actively drop packets or connections that are identified as malicious.

- Rules must be configured on an IPS for it to be able to identify traffic as malicious
- These devices can operate at multiple layers





## CompTIA Network+ N10-009 Course Notes

# Load Balancer

A **load balancer** **distributes** incoming network traffic across **multiple servers** to ensure no single server becomes overwhelmed, improving the reliability and availability of applications.

It operates at **various layers** of the OSI model, making decisions based on IP addresses, TCP/UDP ports, or application-level content to optimize resource use, maximize throughput, minimize response time, and avoid overload of any single resource.





## CompTIA Network+ N10-009 Course Notes

# Proxy Server

A proxy server acts as an **intermediary** between a user's device and the internet, receiving requests from clients, **forwarding** them to the relevant server, and returning the server's response to the client.

It can provide **additional functionality** such as content caching, access control, and filtering, enhancing security and performance.





## CompTIA Network+ N10-009 Course Notes

# Network-Attached Storage

NAS is a **dedicated file storage device** connected to a network, allowing multiple users and client devices to retrieve and store data from a centralized location.

NAS systems are designed for **easy file sharing, data backups, and centralized data management**, supporting a variety of file-based protocols such as NFS, SMB/CIFS, and AFP.

They offer a **scalable and cost-effective** solution for businesses and home users needing to share files across different platforms and devices.





## CompTIA Network+ N10-009 Course Notes

# Storage Area Network (SAN)

A Storage Area Network (SAN) is a dedicated, high-speed network that **provides access to consolidated, block-level data storage**.

SANs are designed to **handle large volumes of data transfers**, improving the availability and performance of applications by offloading storage functions and direct access to multiple storage devices.

They are commonly used in enterprise environments to enhance storage solutions and data management.





## CompTIA Network+ N10-009 Course Notes

# Access Point

An access point (AP) is a networking device that allows **wireless devices** to connect to a wired network using Wi-Fi or related standards.

**APs operate at the data link layer**, bridging the wireless and wired segments of a network.

They **extend the wireless coverage** of a network and can manage multiple connections simultaneously, providing **network access to wireless devices** within their range.





## CompTIA Network+ N10-009 Course Notes

# Wireless LAN Controller (WLC)

A Wireless LAN Controller manages **wireless access points** in a network, centralizing control of the wireless LAN (WLAN).

WLCs simplify the **deployment** and **management** of wireless networks, including configuration, security policies, and managing guest access, enhancing the efficiency and security of wireless networks.



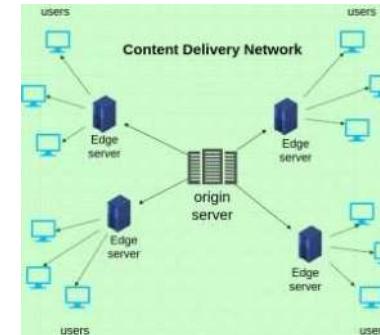


## CompTIA Network+ N10-009 Course Notes

# Content Delivery Network (CDN)

A **globally distributed network of proxy servers** and data centers designed to deliver internet content rapidly to users.

**CDNs cache content** like web pages, videos, and images in multiple locations around the world to reduce latency and improve access speed for users regardless of their location.



<https://cloudkul.com/blog/what-is-content-delivery-network/>

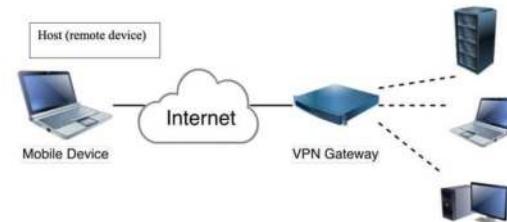


## CompTIA Network+ N10-009 Course Notes

# Virtual Private Network (VPN)

A Virtual Private Network (**VPN**) is a technology that creates a **safe and encrypted** connection over a less secure network, such as the internet.

**VPNs** are used to establish **secure connections** between remote users or remote sites and an organization's private network, allowing for secure data transmission across public networks as if the devices were **directly connected** to the private network.



<https://www.sdxcentral.com/security/definitions/what-is-encryption-definition/what-is-virtual-private-network-vpn/what-are-vpn-best-practices/>



## CompTIA Network+ N10-009 Course Notes

# Quality of Service (QoS)

Quality of Service (QoS) refers to the **set of technologies and policies** used to manage and prioritize network traffic to ensure the performance of critical applications and services.

QoS assigns **different priorities** to different types of traffic, ensuring that essential services like voice and video communications are given higher priority over less critical data.

This helps in reducing latency, jitter, and packet loss, enhancing the overall user experience in networks with **limited bandwidth**.



## CompTIA Network+ N10-009 Course Notes

# Time to Live (TTL)

Time to Live (TTL) is a field in the header of IP packets that specifies the **maximum** time or number of hops a packet is allowed to traverse before being **discarded** by a router.

TTL helps prevent packets from **looping indefinitely** in the network, with each router decrementing the TTL value by one until it reaches zero, at which point the packet is **dropped**.



## CompTIA Network+ N10-009 Course Notes

# IP Addressing

1.7



# Subnet Configuration and IP Addressing



## CompTIA Network+ N10-009 Course Notes

# IPv4

IPv4 is the fourth version of the Internet Protocol, using a 32-bit address scheme to provide approximately 4.3 billion unique addresses, but it has **largely exhausted its address space due** to the exponential growth of the internet.



## CompTIA Network+ N10-009 Course Notes

# IP Addresses V4

Unicast Type	Address Range	Description
Public IP Address	<b>Class A:</b> 1.0.0.0 – 126.255.255.255 <b>Class B:</b> 128.0.0.0 – 191.255.255.255 <b>Class C:</b> 192.0.0.0 – 223.255.255.255	<ul style="list-style-type: none"><li>• Public addresses are designated to be used on the Internet</li></ul>
Private IP Address	<b>Class A:</b> 10.0.0.0 – 10.255.255.255 <b>Class B:</b> 172.16.0.0 – 172.31.255.255 <b>Class C:</b> 192.168.0.0 – 192.168.255.255	<ul style="list-style-type: none"><li>• Private addresses are designated to be used in LAN</li></ul>
Automatic Private IP Address (APIPA)	169.254.0.0 – 169.254.255.255	<ul style="list-style-type: none"><li>• APIPA addresses are self assigned by a host when a DHCP request fails</li></ul>



# Other IP Addresses V4

Address Type	Address Range	Description
Multicast Address	224.0.0.0 – 224.255.255.255	<ul style="list-style-type: none"><li>Provides service-based group messaging</li><li><b>One-to-many</b> communications</li></ul>
Broadcast Address Layer 3	255.255.255.255	<ul style="list-style-type: none"><li>Provides communications to <b>all host</b> at the <b>network layer</b></li></ul>
Broadcast Address Layer 2	FF:FF:FF:FF:FF:FF	<ul style="list-style-type: none"><li>Provides communications to <b>all host</b> at the <b>datalink layer</b></li></ul>
Loopback Address	127.0.0.0 – 127.255.255.255	<ul style="list-style-type: none"><li>Loopback addresses allows a host to communicate to itself</li><li>Used for <b>testing</b> a network interface</li></ul>



## Public IP

**Public IP addresses are globally unique addresses assigned to devices connected to the internet, ensuring each device can be uniquely identified and communicated with from any other device globally.**



## CompTIA Network+ N10-009 Course Notes

# Private IP

Private IP addresses are used within private networks and are **not routable on the internet**; they are used to allow multiple devices within a network to communicate with each other and with the internet (through a translating device) without using a unique public IP address for each device. The ranges are:

- **10.0.0.0 to 10.255.255.255**,
- **172.16.0.0 to 172.31.255.255**
- **192.168.0.0 to 192.168.255.255**



## CompTIA Network+ N10-009 Course Notes

# Automatic Private IP Addressing (APIPA)

Automatic Private IP Addressing (APIPA) is a feature of Windows operating systems that **automatically assigns a unique IP address** from the range:

**169.254.0.1 to 169.254.255.254**

to a computer **when it fails to obtain an IP address from a DHCP server**.

APIPA allows for **automatic, ad hoc network communication within a single subnet** when a DHCP server is not available, but it does not provide internet access.

This mechanism ensures that devices can **still communicate locally** even in the absence of manual or DHCP-based IP configuration.



## CompTIA Network+ N10-009 Course Notes

# IPv4 vs. IPv6

IPv4 and IPv6 are two versions of the Internet Protocol, each with its own system for addressing devices on a network. IPv4, established in the early 1980s, uses 32-bit addresses, resulting in about 4.3 billion unique addresses.

IPv6, introduced to tackle IPv4's limitations, employs 128-bit addresses, vastly expanding the address space.



## IPv4 Subnetting

**IPv4 subnetting** is the practice of **dividing a network into two or more smaller network segments**, or **subnets**, to improve efficiency, security, and management of **IP address allocations**.

It involves **segmenting** a larger network based on the requirement for a different number of **hosts** or to **isolate** network traffic, which can **enhance performance and security**.

**Subnetting** allows for **more efficient use of an organization's allocated IP address space** by enabling the creation of **logically segmented** networks within the same physical network infrastructure.



# Classless (Variable-Length Subnet Mask) VLSM

Classless Inter-Domain Routing (CIDR), involving Variable-Length Subnet Mask (VLSM), is a method for allocating IP addresses and routing that allows for flexible subnetting **beyond the traditional class-based IP addressing**.

With VLSM, **subnets can have different sizes**, allowing for efficient allocation of IP addresses according to the specific needs of each subnet, **reducing the waste of IP addresses**.

This approach **supports more efficient use of IP address space**, accommodating a wide range of subnet sizes within the same network by allowing each subnet to use a mask length that is appropriate for its size and requirements.



## Classful

Classful networking is an early method for the allocation of IP addresses, which **divides the address space into fixed length groups known as classes**.

This method, which predates Classless Inter-Domain Routing (CIDR), **categorizes IP addresses into Classes A, B, C, D, and E**, each with a default subnet mask and a predefined number of networks and hosts per network.

Classful addressing was used to **simplify routing but was inefficient due to its rigid structure**, leading to the eventual development and adoption of CIDR to better utilize IP address space.



# Classless Inter-Domain Routing (CIDR) Notation

**CIDR notation is a method for specifying IP addresses and their associated routing prefix that allows for variable-length subnet masking (VLSM), effectively replacing the classful network design.**

CIDR notation uses a slash ("/") followed by a number to specify the length of the prefix or subnet mask (e.g., 192.168.1.0/24), which indicates that the first 24 bits of the IP address are the network portion.

This method significantly increases the efficiency of IP address allocation, **allowing for more flexible and efficient use of IP address space across the internet.**



## CompTIA Network+ N10-009 Course Notes

# IPv6

**IPv6 is the most recent version of the Internet Protocol designed to replace IPv4, offering a vastly expanded address space, improved security features, and enhanced functionality.**

**It addresses the limitations of IPv4, including the exhaustion of available addresses, by using 128-bit addresses to support a virtually unlimited number of devices on the internet.**

**IPv6 introduces several new concepts and functionalities to improve routing efficiency, simplify network configuration, and enhance security.**



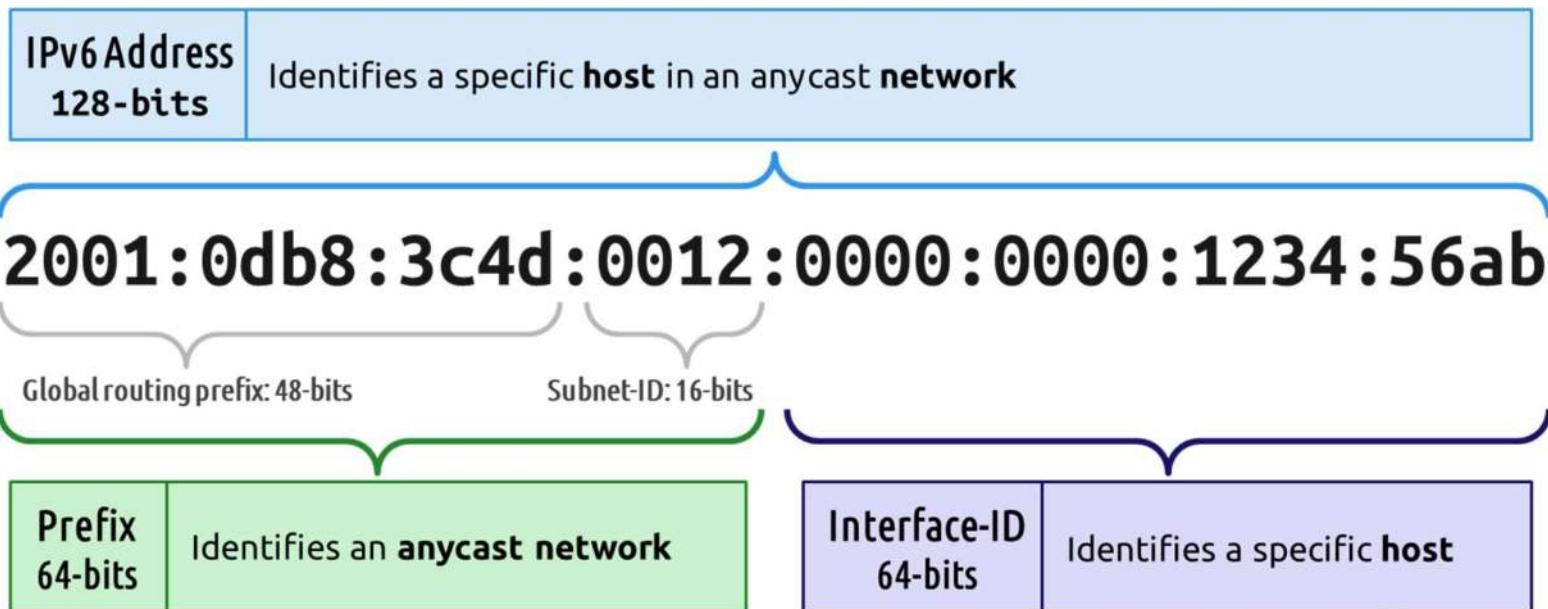
## CompTIA Network+ N10-009 Course Notes

# IPv6

- **IPv6 (Internet Protocol version 6)** is the standard designated to replace IPv4
- **IPv6 Benefits**
  - **More addresses**
    - An IPv6 address is **128 bits** long which leads to us having  $3.4 \times 10^{38}$  number of addresses.
  - **Easier to secure**
    - **IPSec** is built-in as a standard which should lead to better security practices.
  - **Better performance**
    - IPv6 eliminates **broadcast** and replaces it with "**Anycast**".
  - **More efficient communications**
    - Being **multicast-based** means IPv6 will be less wasteful when communicating to many
  - **Easier to configure and manage networks**
    - IPv6 is designed to be **plug and play** for local communications via **Link-Local** addresses
    - IPv6 supports **autoconfiguration** where a host can use its **MAC address** as part of their IPv6 address



## IPv6





## IPv6 Shortened Expression

- Original

2001:0db8:3c4d:0012:0000:0000:1234:56ab

- Drop leading zeros

- Can be applied to any number of fields

2001:**db8**:3c4d:**12**:0000:0000:1234:56ab

- Note four zeros with a single zero

- Can be applied to any number of fields

2001:db8:3c4d:12:**0:0**:1234:56ab

- Note fields of all zeros as a double colon "::"

- Can be applied to any number of fields

- Can only appear once in an address

2001:db8:3c4d:12::1234:56ab



# Other IPv6 Addresses Types

Address Type	Address Range	Description
Multicast Address	FF00/8	<ul style="list-style-type: none"><li>Provides service-based group messaging</li><li><b>One-to-many</b> communications</li></ul>
Loopback Address	::1	<ul style="list-style-type: none"><li>Loopback addresses allows a host to communicate to itself</li><li>Used for testing a network interface</li></ul>
Anycast Address	N/A	<ul style="list-style-type: none"><li>Identifies an anycast network</li><li><b>One-to-nearest</b> communications</li><li>Replaces broadcast from IPv6</li></ul>
Unspecified	::	<ul style="list-style-type: none"><li>Identified as <b>default route</b> in a routing table</li><li>Identified as “<b>any</b>” IP address in a filter list</li></ul>



## CompTIA Network+ N10-009 Course Notes

# Lesson 5 Networking Protocols

1.4



## CompTIA Network+ N10-009 Course Notes

# File Transfer Protocol (FTP) 20/21

File Transfer Protocol (FTP) is a standard network protocol used for the **transfer of computer files between a client and server** on a computer network.

FTP uses two ports: 20 for data transfer and **21 for control (commands and responses)**.

It allows users to upload, download, delete, and manage files on a remote server but **does not encrypt its traffic**, including credentials.



## CompTIA Network+ N10-009 Course Notes

# Secure File Transfer Protocol (SFTP) 22

Secure File Transfer Protocol (SFTP) is an extension of SSH to provide a secure method for transferring files.

It utilizes SSH's port 22 to ensure all data and commands are encrypted and secure, providing a more secure alternative to traditional FTP.

SFTP offers advanced features like file access, file transfer, and file management functionalities over any reliable data stream.

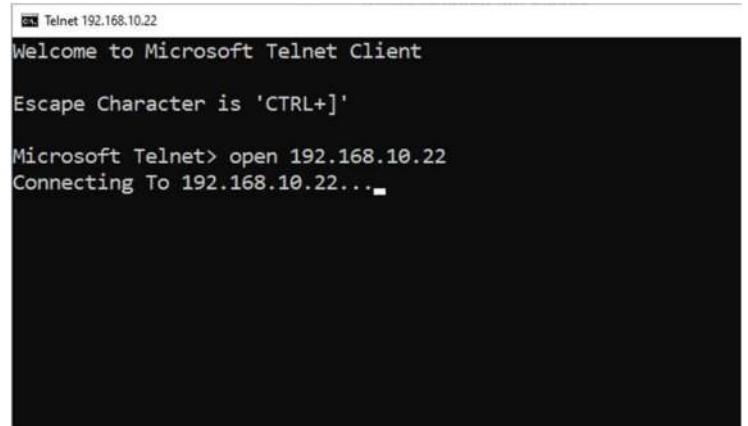


## CompTIA Network+ N10-009 Course Notes

# Telnet 23

Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a **virtual terminal connection**.

It operates on port 23 and is **known for being insecure** since it transmits data, including login credentials, in plaintext, making it susceptible to interception and eavesdropping.



A screenshot of a Microsoft Telnet Client window. The title bar says "Telnet 192.168.10.22". The main text area shows the following output:

```
Microsoft Telnet Client
Welcome to Microsoft Telnet Client
Escape Character is 'CTRL+]'

Microsoft Telnet> open 192.168.10.22
Connecting To 192.168.10.22...
```



## CompTIA Network+ N10-009 Course Notes

# Secure Shell (SSH) 22

Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network.

Port 22 is used by SSH for **providing a secure channel over an unsecured network** in client-server architecture, supporting secure logging in, file transfers (via SCP and SFTP), and port forwarding.

**SSH encrypts all traffic** (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.



## CompTIA Network+ N10-009 Course Notes

# Domain Name System (DNS) 53

Domain Name System (DNS) is a **hierarchical and decentralized naming system** for computers, services, or other resources connected to the Internet or a private network.

It associates various information with domain names assigned to each of the participating entities and uses **port 53 for queries**, which can be sent via TCP or UDP.

DNS translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols.



## CompTIA Network+ N10-009 Course Notes

# Dynamic Host Configuration Protocol (DHCP) 67/68

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on IP networks whereby a DHCP server **dynamically assigns an IP address** and other network configuration parameters to each device on a network.

DHCP operates on UDP ports 67 (server) and 68 (client), facilitating **automatic and centralized management of IP addressing**.

It allows devices to join a network and obtain valid IP addresses, subnet masks, gateways, and DNS server information **without manual configuration**.



## CompTIA Network+ N10-009 Course Notes

# Trivial File Transfer Protocol (TFTP) 69

Trivial File Transfer Protocol (TFTP) is a simple, lock-step, file transfer protocol with **no authentication**, used for transferring files smaller in size.

It uses UDP port 69 and is typically used for **transferring boot files or configurations** to devices in a local network, such as routers and switches.

Due to its simplicity and lack of security features, **TFTP is generally used in controlled environments.**



## CompTIA Network+ N10-009 Course Notes

# Hypertext Transfer Protocol (HTTP) 80

Hypertext Transfer Protocol (HTTP) is the foundation of data communication for the World Wide Web, where it provides a **standard for web browsers and servers to communicate**.

HTTP operates on TCP port 80 and is used to **transfer hypermedia documents**, such as HTML.

It is a stateless protocol, meaning each command is executed independently, **without any knowledge of the commands that came before it**.



## CompTIA Network+ N10-009 Course Notes

# HTTPS/TLS 443

HTTPS, when using Transport Layer Security (TLS), **enhances security further compared to SSL**, which it aims to replace.

It operates on the same port (443) and **provides secure web browsing** by encrypting the data and ensuring the integrity and security of the data transmitted between browsers and websites.

**TLS is the standard security technology for establishing an encrypted link between web servers and browsers.**



## CompTIA Network+ N10-009 Course Notes

# Simple Mail Transfer Protocol (SMTP) 25

Simple Mail Transfer Protocol (SMTP) is the standard protocol for email transmission across the Internet.

SMTP uses port 25 for sending messages from an email client to an email server or between servers.

It is used primarily for sending emails, whereas email retrieval is typically handled by protocols such as POP3 or IMAP.



## CompTIA Network+ N10-009 Course Notes

# SMTP TLS 587 (SMTPS)

SMTP TLS (Simple Mail Transfer Protocol over Transport Layer Security) uses TCP port 587 for **secure email transmission** between email clients and servers.

This protocol enhances the security of SMTP by **encrypting the data** to protect against eavesdropping attacks.

Port 587 is preferred for submitting email to be relayed by a server, making it a standard for secure client-to-server communication in **email applications**.



## CompTIA Network+ N10-009 Course Notes

# Post Office Protocol v3 (POP3) 110

Post Office Protocol version 3 (POP3) is a standard mail protocol used to **retrieve emails from a remote server** to a local client over a TCP/IP connection.

POP3 operates on port 110 and allows emails to be downloaded to the client's machine and, optionally, deleted from the server.

It is designed for situations where the email **client accesses the mail server infrequently** or needs to operate offline.



## CompTIA Network+ N10-009 Course Notes

# POP3 over SSL 995

POP3 over SSL (Post Office Protocol version 3 over Secure Sockets Layer) operates on TCP port 995 and is used for **securely retrieving email from a remote server** to a local client over an SSL-encrypted connection.

This protocol ensures that email messages and authentication details are **securely transmitted**, protecting them from eavesdropping.

Port 995 is designated for secure email retrieval, providing an **encrypted alternative** to the standard POP3 connection.



## CompTIA Network+ N10-009 Course Notes

# Internet Message Access Protocol (IMAP) 143

Internet Message Access Protocol (IMAP) is a protocol for email retrieval and storage.

Unlike POP3, IMAP allows for the manipulation of mailbox messages by **multiple clients**, as messages are kept on the server and can be marked for deletion, flagged, or moved between folders.

IMAP is particularly useful for users who access their email **from multiple devices**, as it provides a way to sync mail across all devices.



## CompTIA Network+ N10-009 Course Notes

# IMAP over SSL 993

IMAP over SSL (Internet Message Access Protocol over Secure Sockets Layer) uses TCP port 993 to **securely access email messages** on a mail server, allowing users to retrieve and manage their email with encryption.

This secure version of **IMAP protects the transmission of email data** and credentials against interception.

Port 993 is the **standard for encrypted communication with IMAP** email servers, ensuring that all data passed between the email client and server is secure.



## CompTIA Network+ N10-009 Course Notes

# Network Time Protocol (NTP) 123

Network Time Protocol (NTP) is used to **synchronize the clocks** of computers over a network.

NTP operates on UDP port 123 and is designed to **mitigate the effects of variable latency** over packet-switched, variable-latency data networks.

It provides **high precision time correction** to networked devices, ensuring that the system time across all devices in the network is closely synchronized.



## CompTIA Network+ N10-009 Course Notes

# Simple Network Management Protocol (SNMP) 161/162

Simple Network Management Protocol (SNMP) is used for **managing devices on IP networks**.

SNMP operates on UDP port 161 for sending commands from a **management station to the network devices**, and devices report back using UDP port 162.

It enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

Only use V3 as it is secure and encrypted. V1 and V2 are not encrypted and sends all data as cleartext.



## CompTIA Network+ N10-009 Course Notes

# Lightweight Directory Access Protocol (LDAP)

## 389

Lightweight Directory Access Protocol (LDAP) is a protocol for accessing and maintaining **distributed directory information services** over an IP network.

LDAP operates on TCP/UDP port 389 and is used for **querying and modifying items** in directory service databases like Microsoft Active Directory, OpenLDAP, and other directory services that follow the X.500 standard.

It provides a mechanism for connecting to, searching, and modifying **internet directories**.



## CompTIA Network+ N10-009 Course Notes

# Lightweight Directory Access Protocol (over SSL) (LDAPS) 636

LDAPS (Lightweight Directory Access Protocol over SSL) operates on TCP port 636, providing a secure method of accessing and maintaining **distributed directory information services** over an IP network.

This protocol **encrypts LDAP traffic using SSL** to prevent unauthorized access to sensitive information in the directory.

LDAPS is used for **secure directory services queries and modifications**, ensuring confidentiality and integrity.



## CompTIA Network+ N10-009 Course Notes

# Server Message Block (SMB) 445

Server Message Block (SMB) protocol is used for **network file sharing**, allowing computers to read and write files and request services from server programs in a computer network.

SMB operates on TCP port 445 and is used primarily by **Windows systems** for file sharing, network browsing, printing services, and inter-process communication.

The use of port 445 helps in direct IP-based communication **without the need for NetBIOS over TCP/IP**.



## CompTIA Network+ N10-009 Course Notes

# Syslog 514

Syslog is a standard for **message logging**, allowing devices and servers to send event notification messages across IP networks to event message collectors, also known as Syslog servers.

It provides a way to **track and record system messages** and is crucial for network and system monitoring, troubleshooting, and security auditing.

Syslog can use various transport protocols, including UDP (typically on port 514), TCP, and SSL/TLS for secure transmission of log messages.



## CompTIA Network+ N10-009 Course Notes

# Structured Query Language (SQL) Server 1433

SQL Server, a **relational database management system (RDBMS)** developed by Microsoft, uses TCP port 1433 for client connections.

This port is used for standard **communication to and from SQL Servers**, handling queries, transactions, and database operations.

Port 1433 is essential for applications and services that need to access the database stored on the SQL Server.



# Remote Desktop Protocol (RDP) 3389

Remote Desktop Protocol (RDP) is a Microsoft protocol that enables **remote connections** to other computers, primarily running **Windows operating systems**.

It uses TCP port 3389 to provide a user with a **graphical interface to another computer** over a network connection.

RDP is widely used for remote administration, remote work, and IT support, offering encrypted and secure access to remote desktops and applications.



## CompTIA Network+ N10-009 Course Notes

# Session Initiation Protocol (SIP)

**Session Initiation Protocol (SIP)** is a **signaling protocol** used for initiating, maintaining, modifying, and terminating real-time sessions that involve video, voice, messaging, and other communications applications and services.

SIP is fundamental to the operation of **VoIP** (Voice over Internet Protocol) systems, enabling the **establishment of call sessions and multimedia distribution**.

It operates at the **application layer** and can use various transport protocols, including TCP and UDP, typically using port 5060 for unsecured communications and port 5061 for secured communications (using TLS).



## CompTIA Network+ N10-009 Course Notes

# Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP) is used for sending diagnostic or control messages between network devices, helping **manage and troubleshoot network issues**.

ICMP is utilized for **error reporting**, such as unreachable hosts or network segments, and for **operational queries** like echo requests and replies (used by tools like ping).

It operates directly on top of IP, providing **feedback** about issues in the communication environment **without carrying application data**.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.4598]
(c) Microsoft Corporation. All rights reserved.

C:\Users\andy>ping google.com

Pinging google.com [142.250.80.46] with 32 bytes of data:
Reply from 142.250.80.46: bytes=32 time=5ms TTL=60
Reply from 142.250.80.46: bytes=32 time=7ms TTL=60
Reply from 142.250.80.46: bytes=32 time=3ms TTL=60
Reply from 142.250.80.46: bytes=32 time=3ms TTL=60

Ping statistics for 142.250.80.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 7ms, Average = 4ms

C:\Users\andy>
```

[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

127



# TCP (Transmission Control Protocol )

Transmission Control Protocol (TCP) is a connection-oriented protocol that provides **reliable, ordered, and error-checked delivery** of a stream of bytes between applications running on hosts communicating via an IP network.

TCP ensures that data packets are transmitted in sequence and without errors, **using acknowledgments, retransmissions, and flow control mechanisms.**

This protocol is used for applications where **data integrity and delivery assurance** are crucial, such as web browsing, email, and file transfers.



## CompTIA Network+ N10-009 Course Notes

### TCP

- **Acknowledgments** are exchanged by senders and receivers to verify and recover data transmissions.
- **Flow control** prevents one host from overflowing the buffers of the other.
- **Windowing** defines the amount of data the receiver will wait to receive before it sends an ACK.
- **Sequence numbers** are used in segments to verify their order and to help recover if there's data loss.



## CompTIA Network+ N10-009 Course Notes

# Connectionless vs. Connection-Oriented

Connection-oriented communication, such as that used by TCP (Transmission Control Protocol), requires a connection to be established between devices before data is exchanged, ensuring data is delivered in the correct order and retransmitted if lost, providing a **reliable communication channel**.

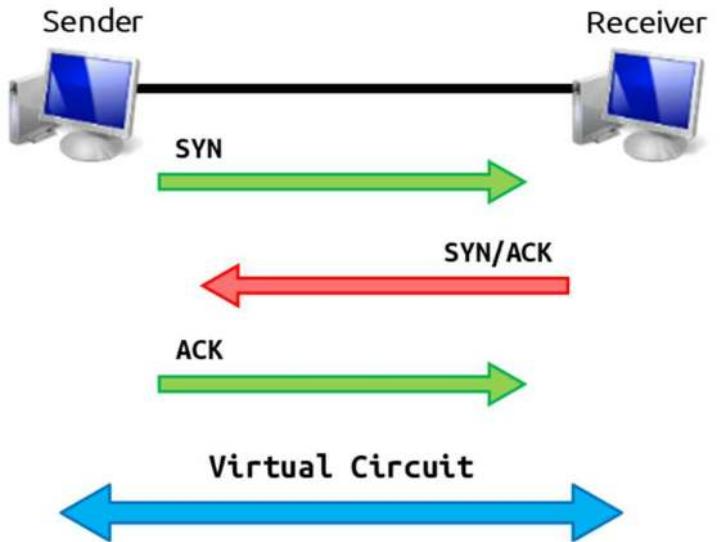
Connectionless communication, such as that used by the UDP (User Datagram Protocol), involves **sending data between devices without establishing a dedicated connection**, making it fast but less reliable, as delivery is not guaranteed, and data may arrive out of order.

The choice between connectionless and connection-oriented protocols **depends on the application's requirements** for speed, reliability, and order of data delivery.



## CompTIA Network+ N10-009 Course Notes

# TCP 3-Way Handshake

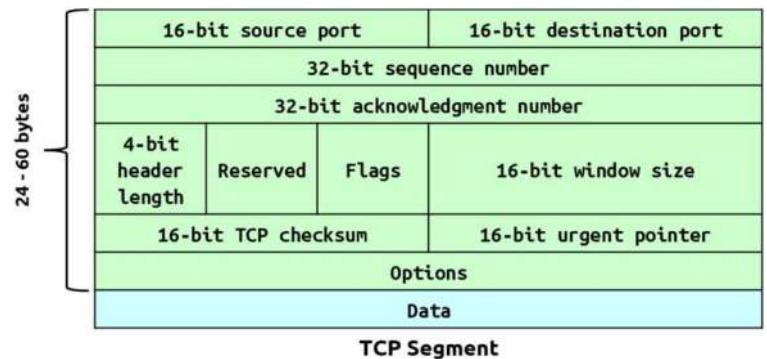




## CompTIA Network+ N10-009 Course Notes

# TCP

- Reliable
- Connection-oriented
- Sequenced
- Acknowledgements
- Windowing flow control
- 24 - 60 bytes (high overhead)





## CompTIA Network+ N10-009 Course Notes

# UDP

User Datagram Protocol (UDP) is a connectionless protocol that allows the transmission of data **without establishing a prior connection** between the sending and receiving hosts.

UDP provides a **fast but less reliable** method of communication, as it does not guarantee packet delivery, order, or error checking.

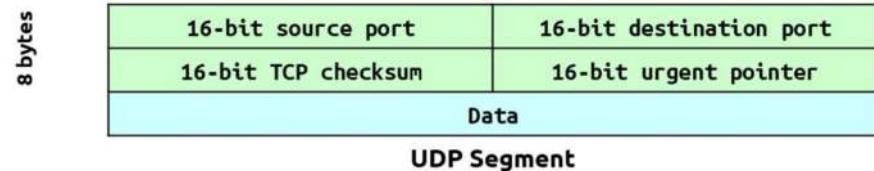
It is suitable for applications that require **speed and efficiency over reliability**, such as streaming audio and video or gaming.



## CompTIA Network+ N10-009 Course Notes

# UDP

- Unreliable
- Connectionless
- No virtual circuit
- Un-sequenced
- No acknowledgments
- No windowing or flow control
- 8 bytes (lightweight)





## CompTIA Network+ N10-009 Course Notes

# Generic Routing Encapsulation (GRE)

Generic Routing Encapsulation (GRE) is a **tunneling protocol** developed by Cisco that can encapsulate a wide variety of network layer protocol packet types inside IP tunnels.

GRE creates a virtual point-to-point link to various brands of routers at remote points over an IP internetwork, enabling the encapsulation of packets from **different protocols**, making it versatile for various networking purposes.

It is commonly used for VPNs and carrying network protocols across networks that do not **natively support** them.



## CompTIA Network+ N10-009 Course Notes

# Internet Protocol Security (IPSec)

Internet Protocol Security (IPSec) is a suite of protocols designed to secure IP communications by authenticating and encrypting each IP packet in a data stream.

IPSec operates in two modes: **Transport mode**, which encrypts the payload of each packet but leaves the header untouched, and **Tunnel mode**, which encrypts both the header and payload and is used for VPN connections.

It is widely used for **securing internet communications** and establishing VPNs.



## CompTIA Network+ N10-009 Course Notes

# Authentication Header (AH)/Encapsulating Security Payload (ESP)

Authentication Header (AH) is a component of IPSec used for providing **authentication, integrity, and nonrepudiation through digital signatures**

Encapsulating Security Payload (ESP) provides:

- Confidentiality
- Encryption

While AH provides **authentication and integrity**, ESP adds **encryption** to ensure confidentiality of the data being transmitted.



## CompTIA Network+ N10-009 Course Notes

# Lesson 6: Network Cabling

1.5



## CompTIA Network+ N10-009 Course Notes

# 802.3 Standards

This set of standards, also known as Ethernet, defines the protocols for wired LAN (Local Area Network) technology, covering aspects like frame formats and physical layer specifications.



## CompTIA Network+ N10-009 Course Notes

# Network Cable Properties

- **Transmission Speeds**
  - Copper cables achieve speeds of up to 40 Gigabits
  - Fiber cables achieve speeds above 100 Gigabits
- **Distance**
  - Copper cables can reach distances of 1,100 meters (3,609 feet)
  - Fiber cables can reach distances of 40 kilometers+ (25 miles)
- **Duplex**
  - Half duplex: One-way communication
  - Full duplex: Two-way communications



## CompTIA Network+ N10-009 Course Notes

# Cable Speeds

Cable speeds vary by type, impacting network performance; Ethernet cables like Cat 5, 5e, 6, and 6a support speeds from 100 Mbps to 10 Gbps over varying distances.

Coaxial cables are used for broadband internet, supporting **high-speed** data transmission, while fiber optic cables (single-mode and multimode) offer the highest speeds, up to 100 Gbps, over long distances.

Key factors affecting cable speed include cable quality, installation, and environmental interference.



## CompTIA Network+ N10-009 Course Notes

# Network Cable Properties

- **Noise Immunity**
  - EMI(Electro-Magnetic Interference) is a condition when signals from a device or cable leak out and disrupt signals of another device or cable
  - Copper cables are highly susceptible to interference
    - Use shielded cables to protect against EMI
  - Fiber cables are NOT susceptible to EMI
- **Frequency**
  - Higher frequency = Faster transmission speeds
- **Attenuation**
  - Longer the cable the weaker the signal.



## CompTIA Network+ N10-009 Course Notes

# Coaxial

Coaxial cable, is a type of electrical cable consisting of a central conductor, insulating layer, metallic shield, and plastic jacket, **used for transmitting television, satellite, and broadband internet signals**.

RG-6 is the most common type. Coax is **thicker and has better shielding** compared to twisted pair, making it **less susceptible to interference and attenuation**, ideal for high-frequency applications like cable TV and internet services.

It is **commonly used in residential and commercial installations** for its durability and high-quality signal transmission.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

143



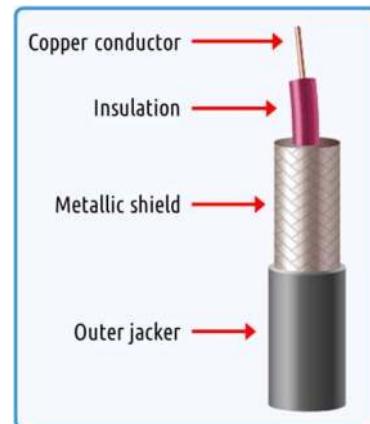
## Coaxial/RG-6

### ■ Advantage

- Shielding protects against EMI
- Long transmission distance (1100 meters)
- More affordable than fiber optic cables

### ■ Disadvantage

- More expensive than twisted pair cable
- Copper core can snap if mishandled





## Coaxial/RG-6

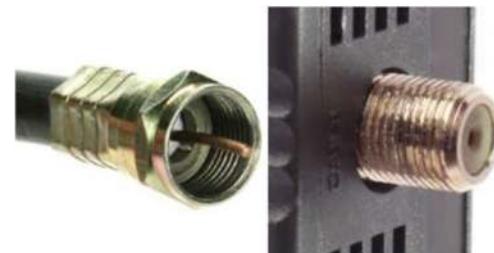
### ■ BNC Connector

- Secure locking connector
- Commonly used in the old bus and ring networks.



### ■ F Connector

- Twisting hand screw commonly found on cable modems.





## Fiber-Optic

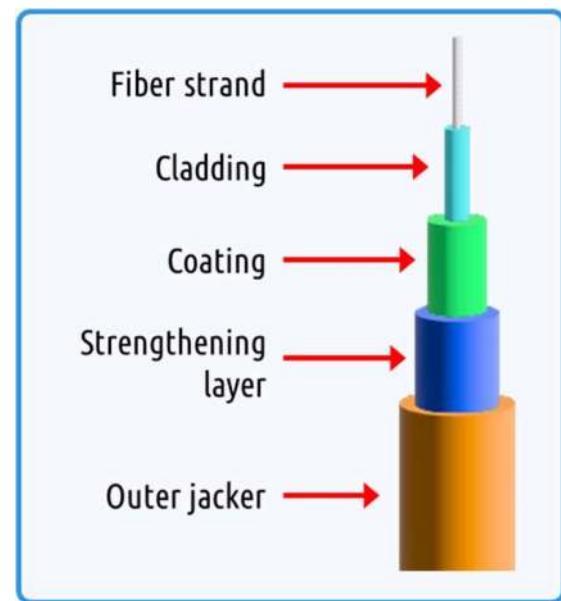
Fiber-optic cabling uses **light** to transmit data, offering significantly **higher speeds** and **greater bandwidth** than traditional copper cables.

It consists of glass or plastic fibers that carry light signals over long distances with minimal loss, making it ideal for **high-speed data** transmission in telecommunications and **internet backbone** infrastructures.





# Fiber-Optic



**Fiber Optic Cable**



## CompTIA Network+ N10-009 Course Notes

# Single-Mode

Single-mode fiber optic cable is designed for **long-distance communication**, using a single strand of glass fiber with a small diameter that allows only one mode of light to propagate.

This design **minimizes attenuation and dispersion over distances**, making it suitable for high-speed, high-bandwidth transmissions over lengths of up to several kilometers without the need for signal repeaters.

Single-mode fiber is **commonly used in telecommunications and cable TV networks**.



## CompTIA Network+ N10-009 Course Notes

# Multimode

**Multimode** fiber optic cable uses **larger diameter fibers that allow multiple modes of light to propagate simultaneously**, making it suitable for short-distance transmission of data.

This type of fiber is typically used **within buildings or in campus networks**, supporting data rates at shorter distances, usually up to 500 meters for **data applications** and up to 2 kilometers for **telecom applications**.

**Multimode** fibers are more affordable and easier to work with compared to single-mode fibers, making them a **popular choice for local-area networks (LANs) and other short-range applications**.



## CompTIA Network+ N10-009 Course Notes

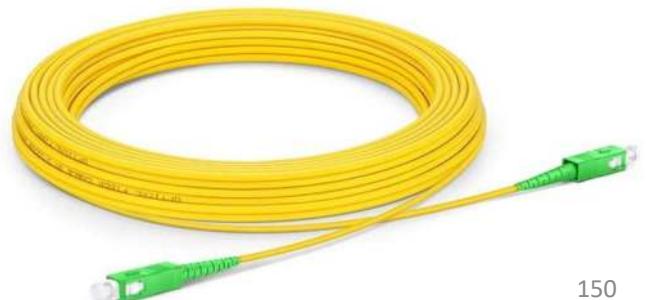
# Fiber-Optic

### ■ Advantage

- NOT susceptible to EMI
- Longest transmission distance
- Fastest speeds into the Tbps

### ■ Disadvantage

- Most expensive cable
- Most difficult to install
- Difficult to troubleshoot issues
- Expensive tools needed for installation and troubleshooting
- Can't easily repair cables in the field



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.co](http://www.tiaexams.co)

150



## CompTIA Network+ N10-009 Course Notes

# Fiber-Optic

- ST Connector
  - ST (straight tip)
  - Used in SMF installations



- SC Connector
  - SC (standard connector / subscriber connector / square connector)
  - Snaps-in style connector
  - Used in SMF and MMF installations



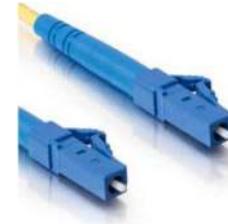


## CompTIA Network+ N10-009 Course Notes

# Fiber-Optic

- LC Connector

- LC (Lucent connection / local connection / little connector)
- Snaps-in style connector
- Small form-factor connector
- Used in SMF and MMF installations



- Dual LC Connector

- SC (standard connector / subscriber connector / square connector)
- Snaps-in style connector
- Used in SMF and MMF installations



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

152



## CompTIA Network+ N10-009 Course Notes

# Fiber-Optic

- Multi-fiber push on (MPO)
  - Snaps-in style connector
  - Small form-factor connector
  - Used in SMF and MMF installations, more commonly used in MMF.





## Direct Attach Copper

DAC cables are used for short-range connections between networking equipment.

They offer a **cost-effective, low-power** alternative for close-range connectivity.





## CompTIA Network+ N10-009 Course Notes

# Twinaxial

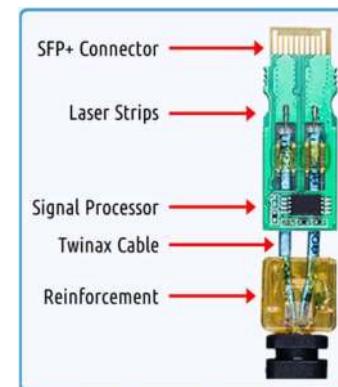
Twinaxial Cables are used in data centers for high-speed short-distance copper 10 Gigabit or 40 Gigabit Ethernet connections.

### Advantage

- Shielding protects against EMI
- More affordable than fiber optic cables

### Disadvantage

- More expensive than coax and twisted pair cables
- Very short-distance connections (0.5 – 7 meters)



10G SFP+ Direct Attach Cable

[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)



## CompTIA Network+ N10-009 Course Notes

# Twisted Pair

Twisted Pair cables consist of eight wires that are twisted into four pairs.

This is the most used networking cable in homes and offices.

### Advantage

- Easier to install and manage than coax or fiber optic cables
- STP has protection against EMI
- Least expensive cable

### Disadvantage

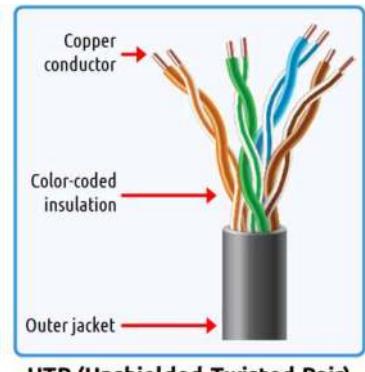
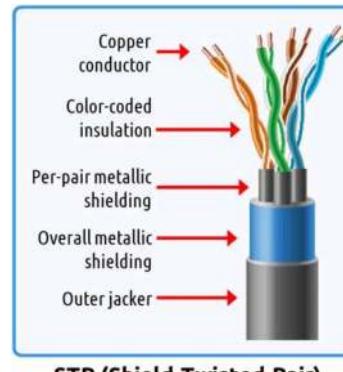
- Transmission distance is limited to 100 meters (328 feet)
- UTP has no protection against EMI



# Twisted Pair

## Twisted Pair Types

- STP (Shield Twisted Pair): Has shielding to protect against EMI
- UTP (Unshielded Twisted Pair): Does NOT have shielding to protect against EMI





## CompTIA Network+ N10-009 Course Notes

# Twisted Pair

- RJ11 Connector
  - 4 pin connector
  - Found on dial-up modems and analog telephones



- RJ45 Connector
  - 8 pin connector
  - Found on desktops, laptops, servers, etc..





## CompTIA Network+ N10-009 Course Notes

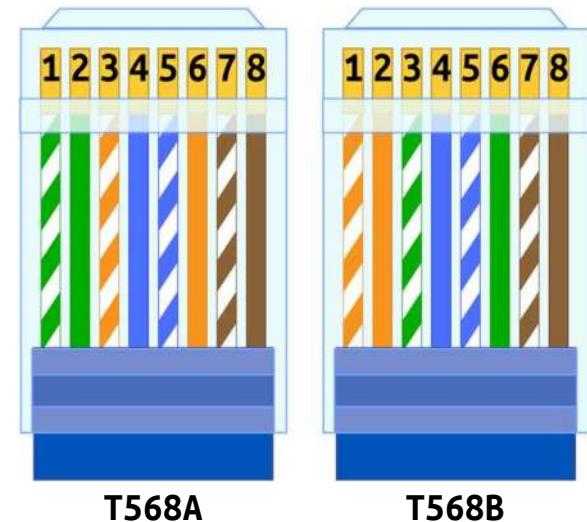
# Twisted Pair Categories

Category	Speed	Distance	Note
Cat 5	100 Mbps	100 meters	<ul style="list-style-type: none"><li>Used in older networks</li></ul>
Cat 5e	1,000 Mbps / 1 Gbps	100 meters	<ul style="list-style-type: none"><li>More twist per foot allows it to handle disturbances to achieve faster speeds</li></ul>
Cat 6	10,000 Mbps / 10 Gbps 1,000 Mbps / 1 Gbps	55 meters 100 meters	<ul style="list-style-type: none"><li>Includes a piece of plastic to separate the 4 wire pairs which minimizes crosstalk</li></ul>
Cat 6a	10,000 Mbps / 10Gbps	100 meters	<ul style="list-style-type: none"><li>Thicker wires to carry a more powerful signal for longer distance</li></ul>
Cat 7	10,000 Mbps / 10Gbps	100 meters	<ul style="list-style-type: none"><li>Strict manufacturing guidelines and per-pair shielding optimizes this cable for longer runs</li></ul>
Cat 8	25Gbps – 40Gbps	30 meters	<ul style="list-style-type: none"><li>Designed for very high frequencies to operate at very high speeds</li><li>Intended for data center usage for short-range connections</li></ul>



# Wiring Standards

There are two standard RJ45 pinouts for the individual arrangement of the wire connections to the RJ45 connectors within an Ethernet cable: the T568A and T568B standards. T568B is the more commonly used.





CompTIA Network+ N10-009 Course Notes

## Wiring Standards



Straight-through cables are created by terminating by both ends of a cable using T568A.



Straight-through cables are created by terminating by both ends of a cable using T568B.

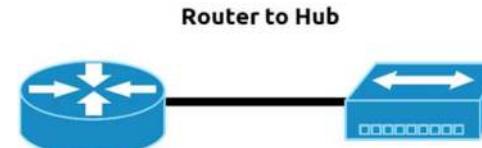
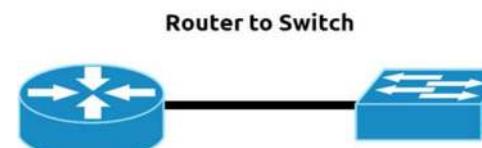
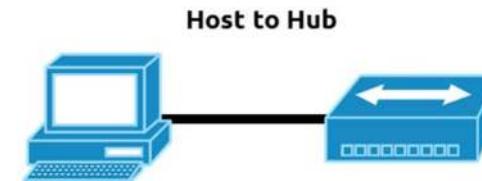
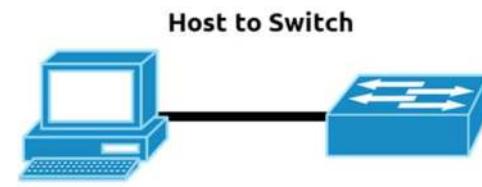


Crossover cables are created by terminating one of a cable with T568A and the other with T568B



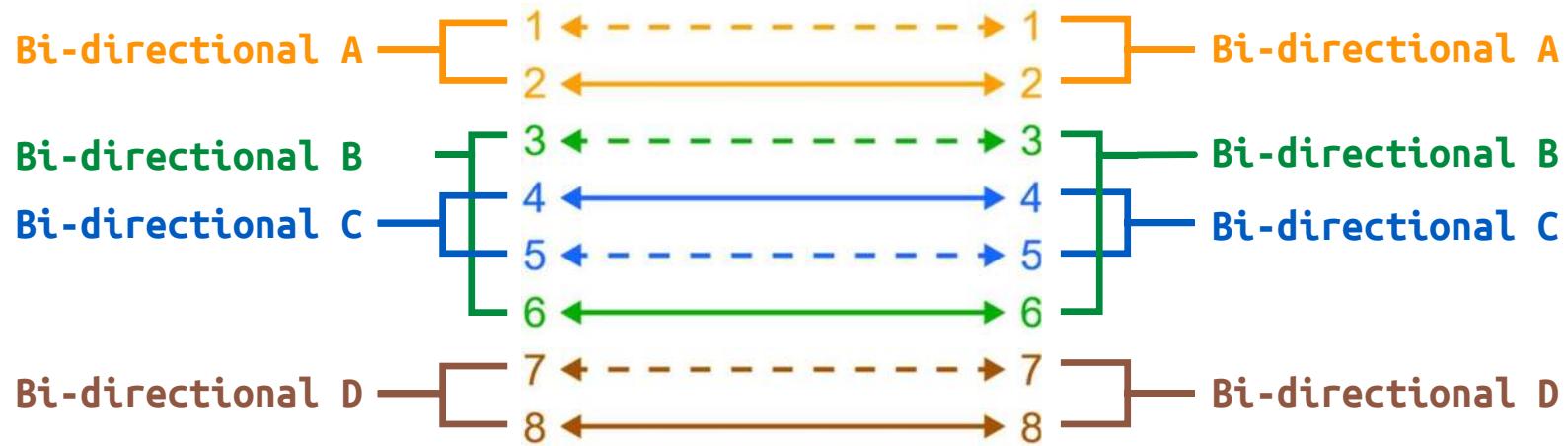
# Straight-through Cable Wiring

Straight-through cables are used to connect, unlike devices





CompTIA Network+ N10-009 Course Notes  
**Straight-through Cable Wiring**





# Crossover Cable Wiring

Crossover cables are used to connect like devices

**Switch to Switch**



**Hub to Hub**

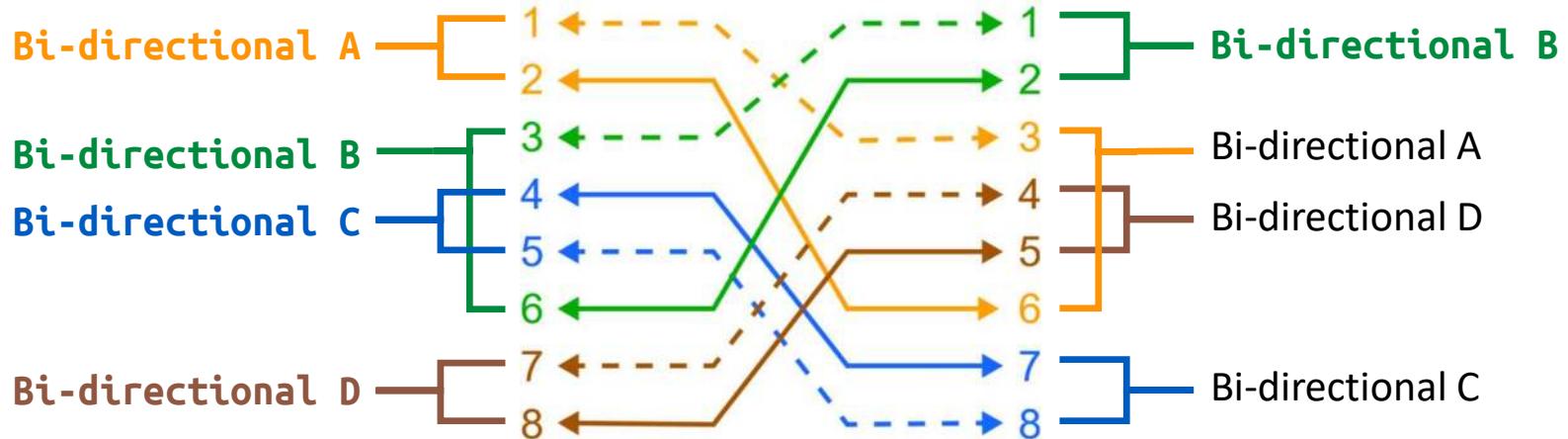


**Host to Host**





CompTIA Network+ N10-009 Course Notes  
**Crossover Cable Wiring**

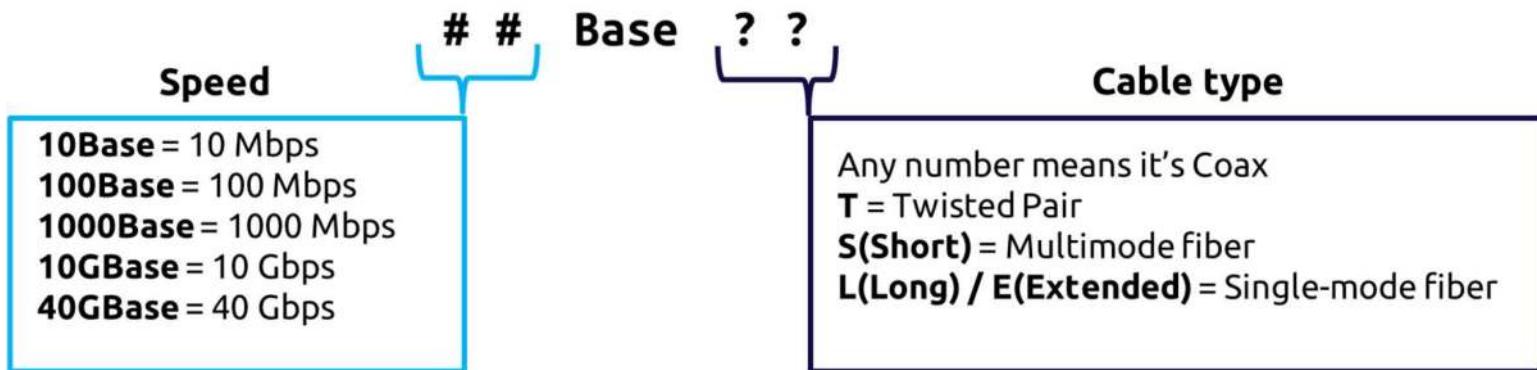




CompTIA Network+ N10-009 Course Notes

# Ethernet at the Physical Layer

- 10Base2
- 10Base5
- 10BaseT
- 100BaseTX
- 100BaseFX
- 1000BaseCX
- 1000BaseT
- 1000BaseSX
- 1000BaseLX
- 10GBaseT
- 10GBaseSR
- 10GBaseLR
- 10GBaseER
- 10GBaseSW
- 10GBaseLW
- 10GBaseEW
- 40GBaseT





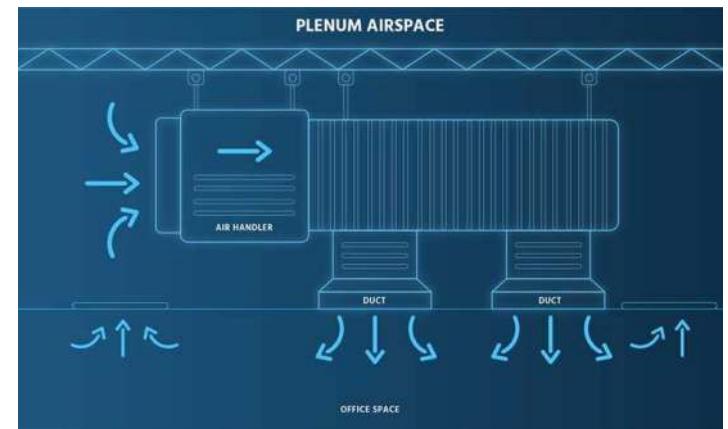
## CompTIA Network+ N10-009 Course Notes

# Plenum Rating

These terms describe the **fire resistance** of cables.

Plenum-rated cables are designed to resist fire and emit low smoke when exposed to flame, making them safe for use in the **air spaces of buildings**.

Non-plenum cables are less expensive but **produce more toxic fumes when burned** and are typically used where they are not exposed to circulating air ducts.





# Transceivers

Transceivers are devices that can **both transmit and receive data**, often used in networking to interface with cables of different types, such as converting electrical signals to optical signals for fiber optic cables.

**SFP (Small Form-factor Pluggable)** is an optical module transceiver used for data and telecommunications.

Supports speeds of up to 4.25gbps

SFP+ is an enhanced version that supports data rates up to 10gbps

**QSFP (Quad Small Form-factor Pluggable)** is a connector that is used for fiber optic or electrical copper connections.

Supports speeds of up to 28gbps

QSFP+ is an enhanced version that supports data rates up to 40gbps



10GB SFP+



40GB QSFP+



## CompTIA Network+ N10-009 Course Notes

# Media Converters

Media converters are a type of transceiver that **convert data signals from one media type to another** (e.g., copper cable to fiber optic cable), enabling the integration of different network technologies.

- Single-Mode Fiber to Ethernet
- Multimode Fiber to Ethernet
- Fiber to Coaxial
- Single-Mode to Multimode Fiber



Single-mode Fiber, SC to  
Ethernet, RJ45



Multimode Fiber, LC to  
Ethernet, RJ45



Fiber, SFP to Coax, BNC



# Lesson 7: Modern Network Environments

Objectives 1.8



## CompTIA Network+ N10-009 Course Notes

# Software-defined networking

Software-defined networking (SDN) is an innovative networking paradigm that **decouples** the network control and forwarding functions, enabling network management through software applications.



## CompTIA Network+ N10-009 Course Notes

### SD-WAN

SD-WAN is a specific application of software-defined networking (SDN) technology applied to WAN connections, which are used to **connect enterprise networks**—including branch offices and data centers—over large geographic distances.

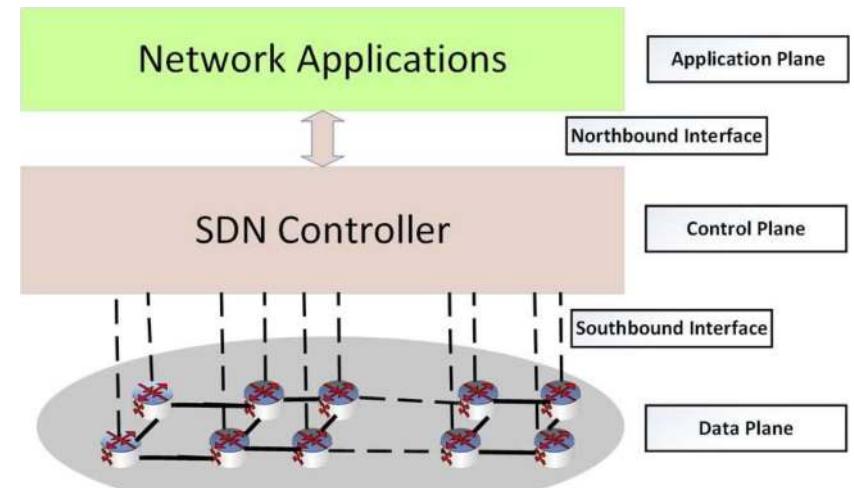
This technology enhances business efficiency by **dynamically routing traffic** across the optimal path using a centralized control function, ensuring high performance and reliability for critical applications.



## SDN Function

SDNs (Software-Defined Networks) separate the network architecture into three distinct planes: the

- **Data plane:** responsible for packet forwarding
- **Control plane:** which manages network traffic and policies
- **Application plane:** which hosts network applications and services, leveraging the control plane to execute high-level tasks.





## Application Aware

**SD-WAN** technology intelligently identifies applications and can prioritize traffic based on business requirements, ensuring critical applications have the bandwidth and path reliability they need.



## CompTIA Network+ N10-009 Course Notes

# Zero-Touch Provisioning

This feature allows for the **remote deployment of network devices** with minimal manual intervention.

Network devices can **automatically download configuration settings** from a central location, simplifying branch deployments.



## Transport Agnostic

SDN is **flexible** with the type of connectivity it uses, whether it's MPLS, broadband, LTE, or a combination, allowing for cost-effective and reliable internet access from different service providers.



## Central Policy Management

Centralized management enables network administrators to set policies that manage and **configure all SDN devices** across the network from a single interface, enhancing security and efficiency.



## VXLAN

**VXLAN** (Virtual Extensible Local Area Network) is a **network virtualization technology** that enhances the scalability of large-scale cloud computing environments.

It **extends Layer 2 segments** over an underlying Layer 3 network, enabling the creation of a large number of virtualized LANs.



## CompTIA Network+ N10-009 Course Notes

### DCI

VXLAN is particularly effective for Data Center Interconnect (DCI) by enabling the stretching of Layer 2 networks across geographically dispersed data centers.

This capability allows for **seamless mobility of virtual machines** between data centers without changing underlying network configurations.



## CompTIA Network+ N10-009 Course Notes

# Layer 2 Encapsulation

VXLAN uses Layer 2 encapsulation to encapsulate Ethernet frames within UDP packets.

This encapsulation allows VXLAN to create a logical network for VMs across different physical networks, providing scalability **beyond the traditional 4096 (12 bits) VLANs limit to 16.78 million (24 bits) VLANs.**



## CompTIA Network+ N10-009 Course Notes

# Zero Trust

Zero Trust is a security model based on the principle of "**never trust, always verify.**"

It requires **strict identity verification** for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.

Zero Trust minimizes potential attack vectors by **treating all users as potential threats** and enforcing strict access controls and not assuming trust based on network location.



## CompTIA Network+ N10-009 Course Notes

# Policy-Based Authentication

In a Zero Trust framework, policy-based authentication requires all users, both internal and external, to be **authenticated and continuously validated** for security configuration and posture before being granted access to data and applications.

Authentication policies can include multifactor authentication (MFA), biometrics, and behavioral analytics to ensure that only legitimate users gain access.



## CompTIA Network+ N10-009 Course Notes

# Authorization in Zero Trust Architecture

Authorization in ZTA is **dynamic** and **strictly enforced** before access to resources is allowed.

This process is **context-aware**, taking into account the user's identity, location, device health, service or workload, data classification, and anomalies.

Access to resources is granted on a **per-session basis**, ensuring that the access rights of users are constantly evaluated and adjusted based on the latest security intelligence and context.



## CompTIA Network+ N10-009 Course Notes

# Least Privilege

The principle of least privilege requires that users, systems, and programs are granted only the **minimum levels of access** — or permissions — needed to perform necessary tasks.

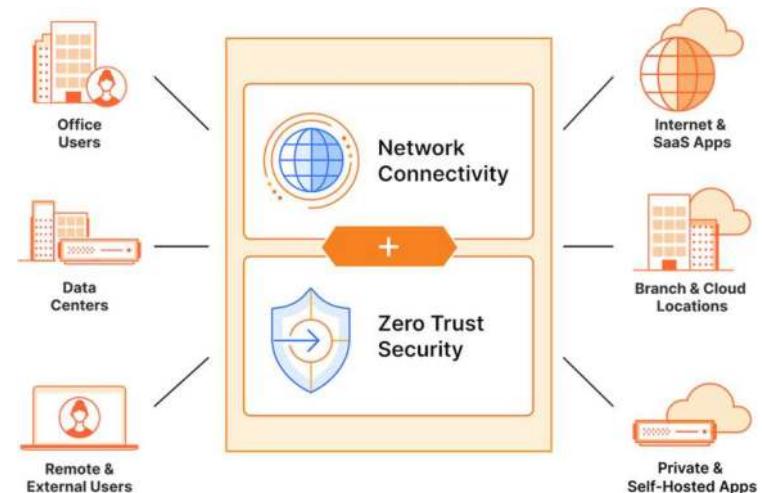
Implementing least privilege **minimizes the potential damage** from accidental or malicious actions by **limiting access rights** for users to the bare minimum necessary to perform their work.



## CompTIA Network+ N10-009 Course Notes

# SASE/SSE

SASE (Secure Access Service Edge) and SSE (Security Service Edge) are emerging frameworks that **combine network security functions with WAN capabilities** to support the dynamic secure access needs of organizations' distributed workforces and cloud-first strategies.



<https://www.cloudflare.com/learning/access-management/what-is-sase/>



## CompTIA Network+ N10-009 Course Notes

# Secure Access Service Edge (SASE)

**SASE integrates comprehensive WAN services and security functions directly into the network fabric.**

This provides secure network connectivity and access to resources regardless of location.



## CompTIA Network+ N10-009 Course Notes

# Security Service Edge (SSE)

SSE focuses more on the security aspects, **centralizing various security services** like secure web gateways, cloud access security brokers (CASB), and zero trust network access (ZTNA).

These services are provided **in the cloud** to ensure secure access and data protection across all environments.

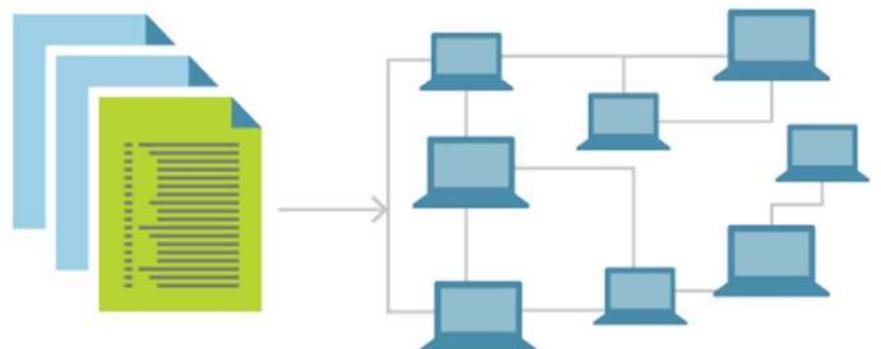


## CompTIA Network+ N10-009 Course Notes

# Infrastructure as Code

Infrastructure as Code (IaC) is a key practice in cloud computing and DevOps that involves **managing** and **provisioning** computing infrastructure through machine-readable **definition files**, rather than physical hardware configuration or interactive configuration tools.

It enables IT infrastructure to be **automatically** managed, monitored, and provisioned through code, improving consistency, efficiency, and reducing manual errors.



<https://learn.microsoft.com/en-us/devops/deliver/what-is-infrastructure-as-code>



## CompTIA Network+ N10-009 Course Notes

# Automation in IaC

Automation is at the core of IaC, enabling rapid and consistent environment setups

This approach reduces human errors and increases efficiency in deploying infrastructure.



## CompTIA Network+ N10-009 Course Notes

# Playbooks, Templates, and Reusable Tasks

IaC utilizes playbooks, templates, and reusable tasks to **define and orchestrate the steps needed** for infrastructure setup, modification, and management.

These elements are critical for ensuring that infrastructure deployment is repeatable and scalable.



## CompTIA Network+ N10-009 Course Notes

# Configuration Drift and Compliance

IaC helps **prevent configuration drift**, which occurs when the environment's current state deviates from its intended state due to manual changes or updates.

IaC also aids in **maintaining compliance** with defined standards and policies by automating configurations and deployments.



## CompTIA Network+ N10-009 Course Notes

# Upgrades

With IaC, upgrades to infrastructure can be **managed systematically through code revisions**.

This method ensures that upgrades are less disruptive and that all changes are version controlled and reversible.



## CompTIA Network+ N10-009 Course Notes

# Dynamic Inventories

IaC supports the use of dynamic inventories, where infrastructure resources are **automatically discovered and managed** based on real-time data.

This flexibility is essential for managing environments that need to adjust quickly to changing demands or configurations.



## Source Control in IaC

**Source control** is integral to the Infrastructure as Code paradigm, **providing a system for tracking changes**, collaborating, and maintaining the integrity of code that defines infrastructure.



## Version Control

Version control systems **keep track of every modification to the code** in a special kind of database.

If a mistake is made, developers can **turn back the clock** and compare earlier versions of the code to help fix the mistake while minimizing disruption to all team members.



## CompTIA Network+ N10-009 Course Notes

# Central Repository

A central repository in source control systems acts as the **single source of truth** for all code changes, allowing team members to collaborate effectively, accessing and updating code securely and efficiently.



## CompTIA Network+ N10-009 Course Notes

# Conflict Identification

Source control systems automatically detect conflicts when **multiple team members make changes to the same part of the code.**

This feature is crucial for preventing overwrites and ensuring that all changes are reconciled before code is merged.



## Branching

Branching is a feature of source control that allows developers to **diverge from the main line of development** and continue to work independently without affecting others' work.

This is particularly useful for developing new features, fixing bugs, or experimenting in a controlled environment.



## CompTIA Network+ N10-009 Course Notes

# IPv6 Addressing

IPv6 is the **most recent version** of the Internet Protocol designed to replace IPv4, offering a **vastly expanded address space**, improved security features, and enhanced functionality.

It addresses the limitations of IPv4, including the exhaustion of available addresses, by using 128-bit addresses to support a **virtually unlimited number of devices** on the internet.

IPv6 introduces several new concepts and functionalities to **improve routing efficiency, simplify network configuration, and enhance security**.



## CompTIA Network+ N10-009 Course Notes

# Mitigating Address Exhaustion

IPv6 addresses the limitations of IPv4, including address exhaustion, by providing an **almost limitless** pool of IP addresses.

This ensures the scalable growth of the internet, accommodating an increasing number of devices and users globally.



## CompTIA Network+ N10-009 Course Notes

# Compatibility Requirements

Transitioning to IPv6 involves compatibility strategies to ensure that IPv6 and IPv4 systems can **operate concurrently**.

This is necessary because the internet will operate in a **mixed IPv4 and IPv6 environment for many years**.



## Tunneling

Tunneling in IPv6 is a method used to transmit IPv6 packets over an existing IPv4 network infrastructure.

This allows for the coexistence of both protocols during the transition period from IPv4 to IPv6.

Tunneling works by encapsulating IPv6 packets within IPv4 packets, enabling them to be transported across IPv4 networks as if they were IPv4 packets.



## CompTIA Network+ N10-009 Course Notes

# Dual Stack

**Dual stack** refers to a network configuration where **devices run both IPv4 and IPv6 protocols simultaneously**.

This allows the devices to **communicate over both types of networks**, facilitating a gradual transition from IPv4 to IPv6.

In a **dual stack** environment, network services and applications can operate over IPv4 or IPv6, **depending on the destination address availability and network conditions**.



## CompTIA Network+ N10-009 Course Notes

### NAT64

**NAT64** is a network address translation technology that **facilitates communication** between IPv6 and IPv4 devices.

It translates IPv6 addresses into IPv4 addresses and vice versa, enabling interoperability in environments not yet fully IPv6-capable.



## CompTIA Network+ N10-009 Course Notes

# Lesson 8

## IP Routing



## Routing

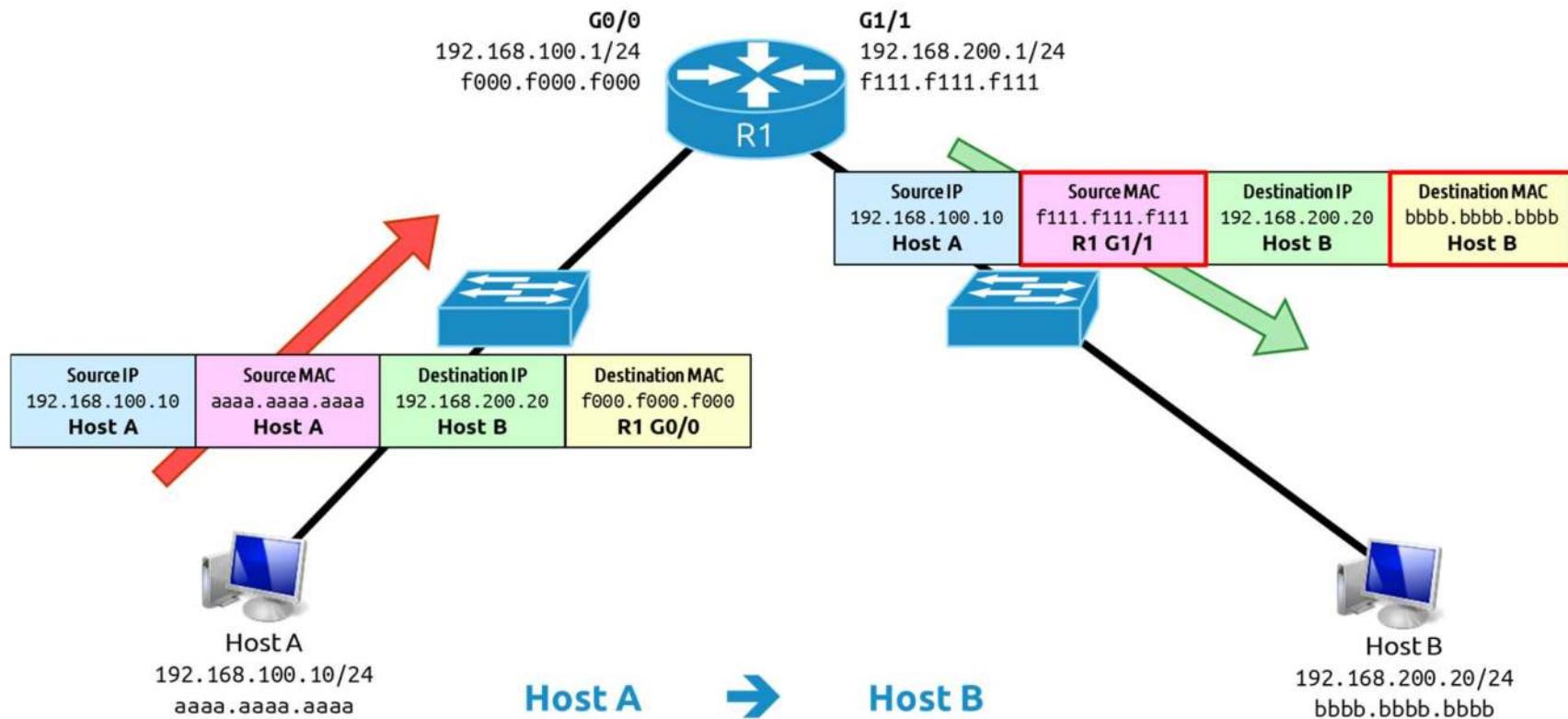
Routing is the process of **selecting paths** in a network along which to send network traffic.

Routing is performed by devices known as routers, which use routing tables and algorithms to determine the most **efficient path** for data packets to travel from their source to their destination.



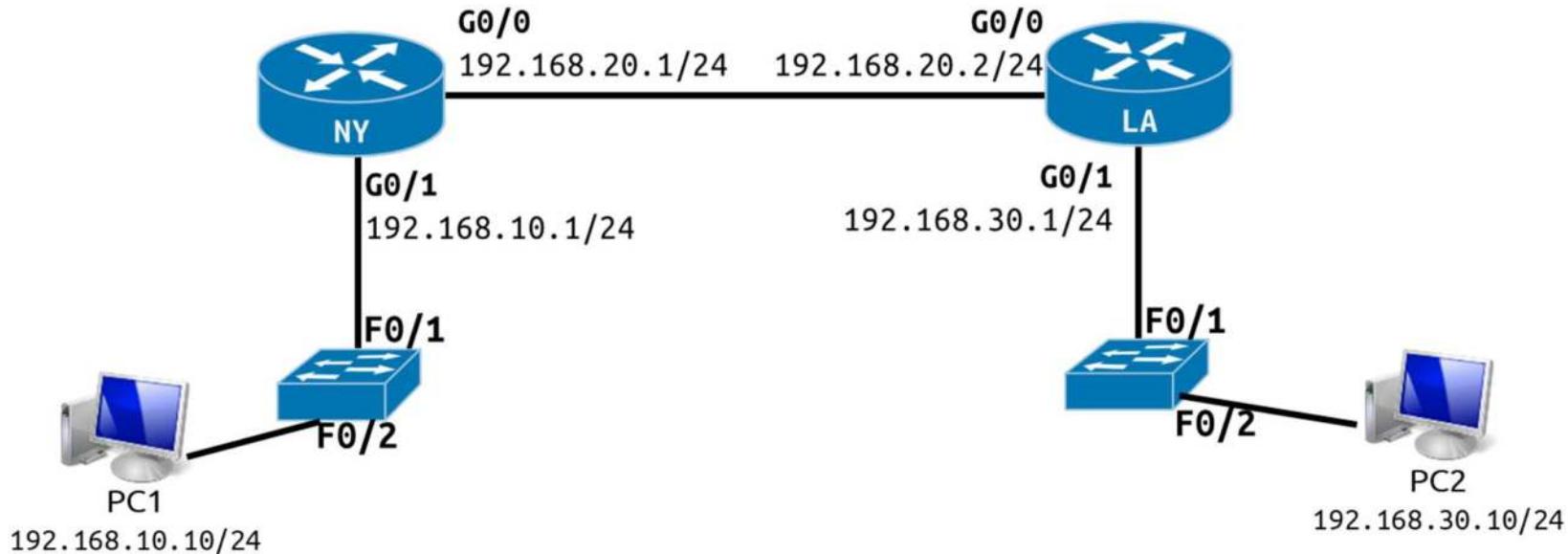
## CompTIA Network+ N10-009 Course Notes

# Routing Process





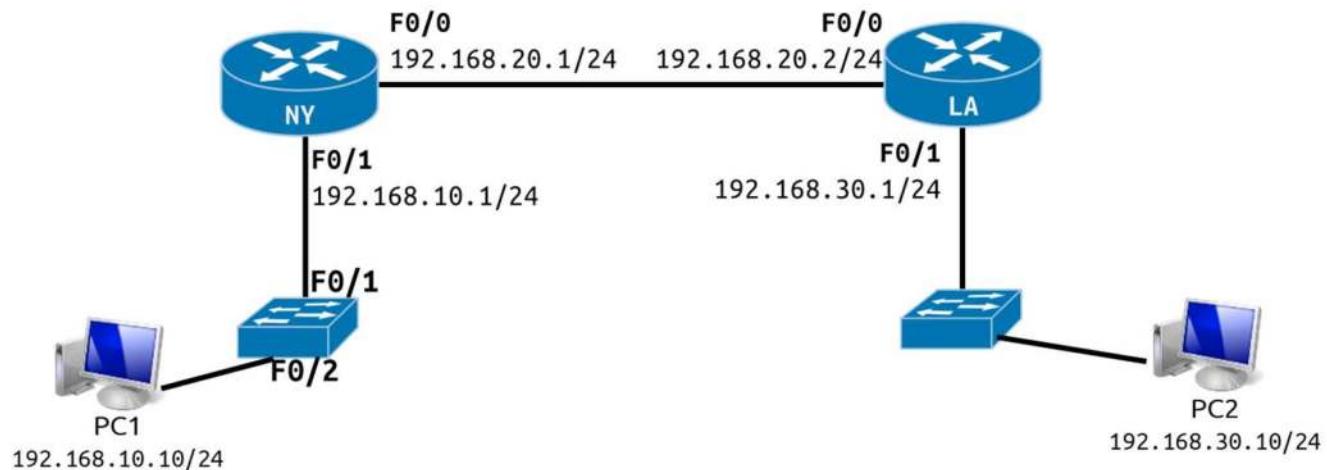
# Routing Diagram Setup





## CompTIA Network+ N10-009 Course Notes

# Routing



**NY Routing Table**

	Destination	Mask	Exit Interface
1	192.168.10.0/24	255.255.255.0	F0/1
2	192.168.20.0/24	255.255.255.0	F0/0
3	192.168.30.0/24	255.255.255.0	F0/0

**LA Routing Table**

	Destination	Mask	Exit Interface
1	192.168.10.0/24	255.255.255.0	F0/0
2	192.168.20.0/24	255.255.255.0	F0/0
3	192.168.30.0/24	255.255.255.0	F0/1



## Static Routing

Static routing involves **manually** configuring routers with specific paths to reach network destinations.

It is **simple** to implement in small networks but **lacks the flexibility and scalability** of dynamic routing, as it does not automatically adjust to network changes.



## Dynamic Routing

**Dynamic routing** automatically adjusts the paths used to send data through the network.

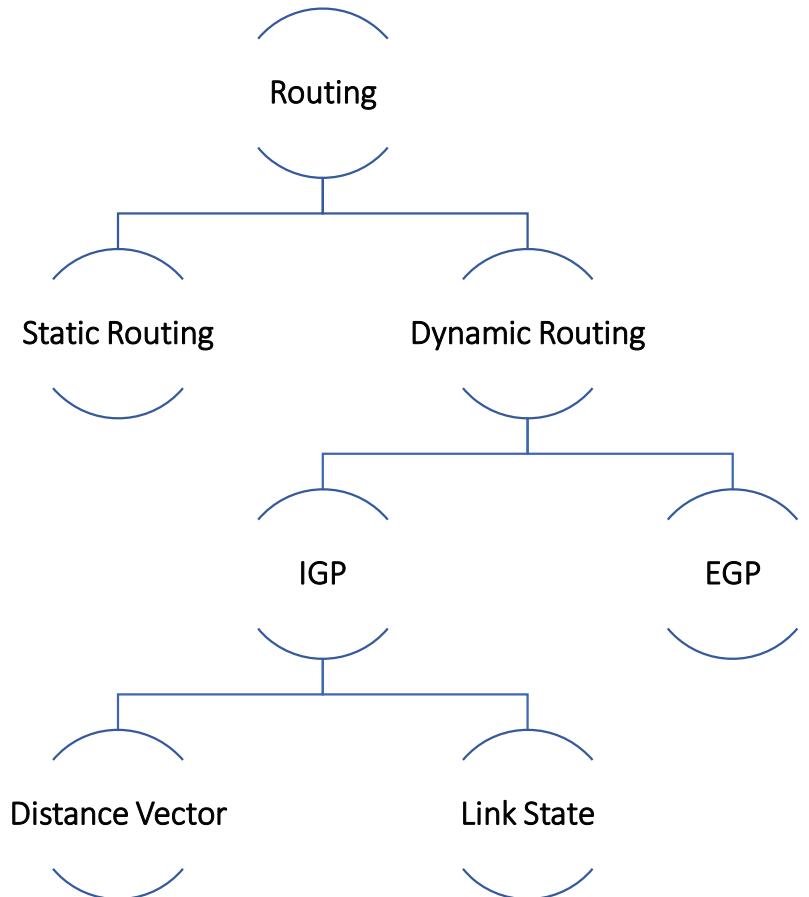
**Routers** communicate with each other using **dynamic routing protocols**, sharing information about network topology and traffic conditions.

This allows the network to **adapt to changes**, such as link failures or congestion, ensuring data takes the most efficient route.



## CompTIA Network+ N10-009 Course Notes

# Routing





# Routing Protocol Categories

**Interior Gateway protocols (IGP)** are used by organizations to route their LAN in one location to their LAN in another.

Example: NY branch router to LA branch router of the same organization

**Exterior Gateway protocols (EGP)** are used by organizations to route one customer's WAN link to another customer's WAN link.

Example: The Internet, every organization has a connection to many other organizations.

BGP (Border Gateway Protocol) is the only EGP protocol, and it is used to route the Internet

Every organization has its own Autonomous System (AS) which is comprised of all their network locations interconnected.



# Interior Gateway Protocol

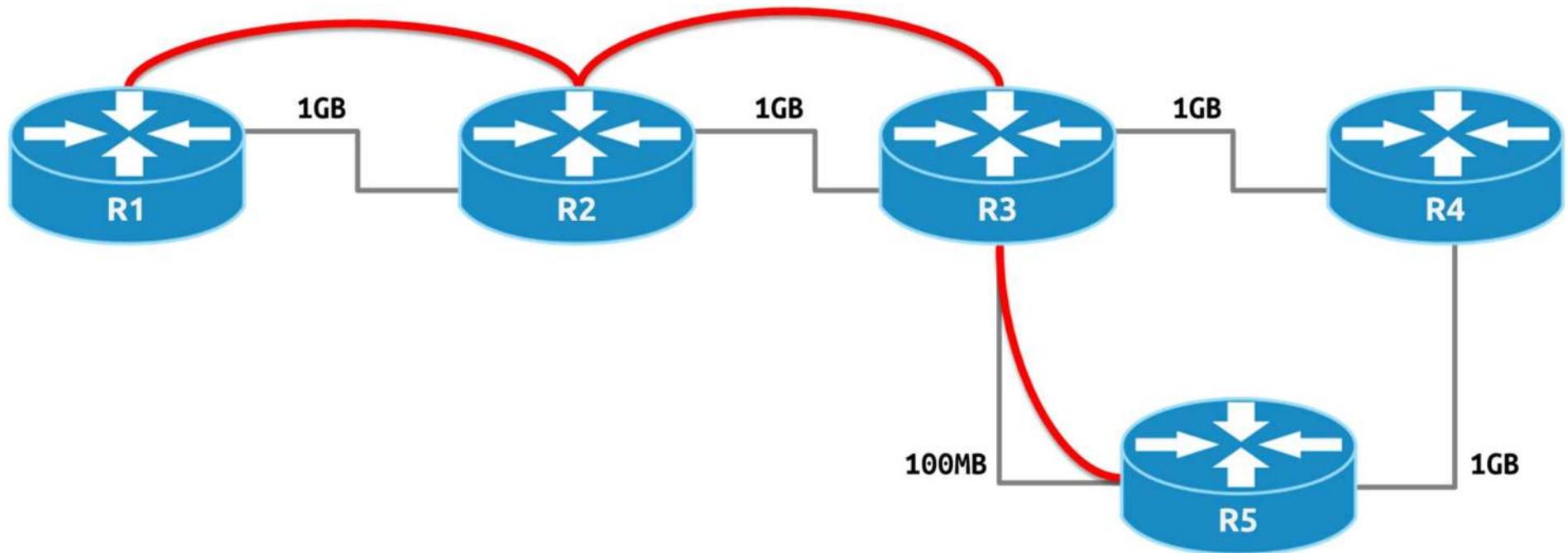
**Distance-vector** is a **hops-based routing protocol**, it'll forward packets using the path with the fewest number of hops.

**Link-state** is a **bandwidth-based routing protocol**, it'll forward packets using the path with the highest bandwidth.

Protocol Type	Metric	Max Hops	Routing Protocols
Distance-vector	Fewest Hops	15 hops	RIPv1, RIPv2, and IGRP
Link-state	Highest Bandwidth	Unlimited	IS-IS and OSPF



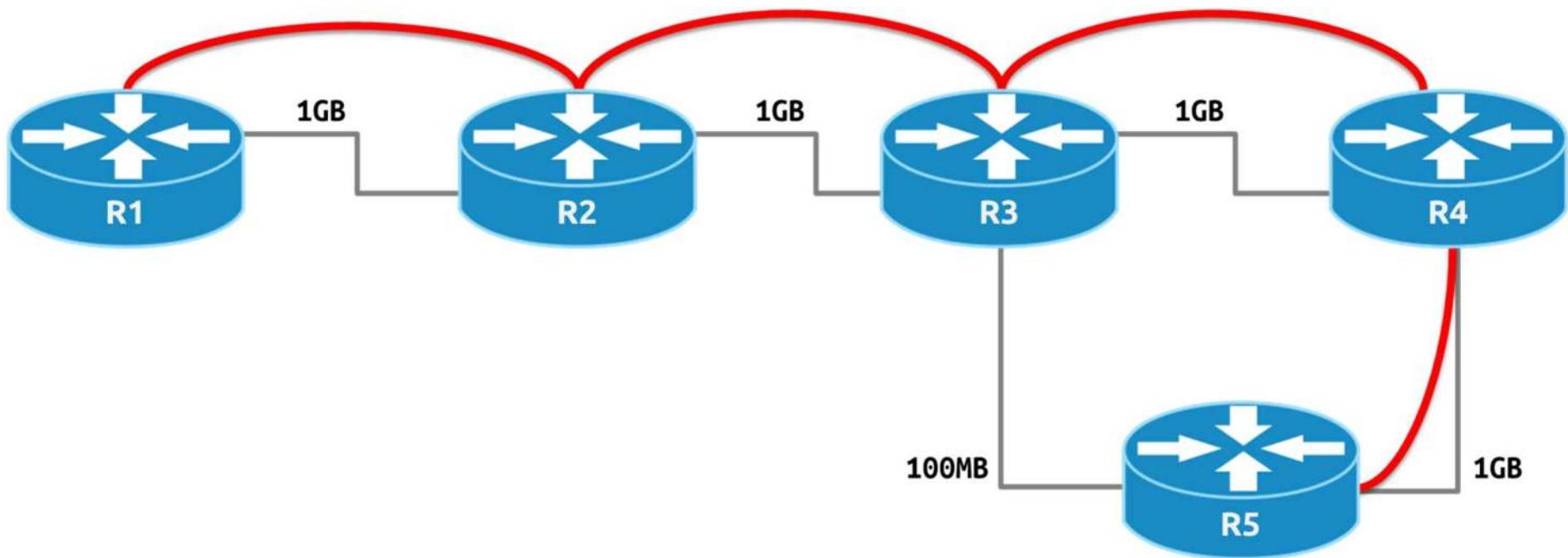
CompTIA Network+ N10-009 Course Notes  
**Distance-vector - Hops**





CompTIA Network+ N10-009 Course Notes

## Link-state - Bandwidth





# Routing Information Protocol (RIP)

One of the oldest distance-vector routing protocols. Uses hop count as a metric, with a maximum of 15 hops.

## Versions:

- **RIPv1:** Classful protocol, no subnet information.
- **RIPv2:** Classless, supports subnetting, includes subnet mask info. Multicast updates and simple authentication.

## • Use Cases:

- Suitable for small to medium-sized networks.
- Limited scalability, slower convergence compared to modern protocols like OSPF and EIGRP.



# Open Shortest Path First

**Link-state routing protocol.** Fast convergence and supports large networks.

## Key Features:

- Hierarchical design with areas to optimize traffic.
- Updates sent only when topology changes, reducing overhead.
- Supports VLSM (Variable Length Subnet Masking) and CIDR (Classless Inter-Domain Routing).

## Advantages:

- Efficient, scalable, and flexible.
- Provides load balancing and fault tolerance.
- Suitable for large, complex networks.



## CompTIA Network+ N10-009 Course Notes

# Enhanced Interior Gateway Routing Protocol

Enhanced distance-vector protocol.  
Combines features of distance-vector and link-state protocols.

### Key Features:

- Supports VLSM and CIDR.
- Sends partial updates only when changes occur.
- Uses metrics like bandwidth, delay, load, and reliability.

### Advantages:

- Highly efficient, scalable, and quick convergence.
- Provides loop-free paths and load balancing.
- Suitable for medium to large networks, especially those with Cisco devices.



## Metric

The metric is a value associated with routes, used by routing protocols to evaluate the cost of path traversal.

**Lower metric values typically indicate more desirable routes.**

Different routing protocols may use various factors, such as bandwidth, delay, hop count, or even custom values, to calculate this metric.



## CompTIA Network+ N10-009 Course Notes

# Border Gateway Protocol

Essential for inter-domain routing on the internet. Uses path attributes to select the best route.

### Key Features:

- Supports CIDR for efficient IP address allocation.
- Employs policies for route selection and advertisement.
- Uses TCP for reliable communication between BGP peers.

### Advantages:

- Highly scalable and flexible.
- Manages large routing tables and complex policies.
- Crucial for ISPs and large enterprises with multiple connections to the internet.



## CompTIA Network+ N10-009 Course Notes

# Route Selection

Route selection is a critical process in network routing that **determines the best path** for data to travel from source to destination.

It uses specific criteria such as administrative distance, prefix length, and metric to choose the most efficient route.



## CompTIA Network+ N10-009 Course Notes

# Administrative Distance

Administrative distance is a metric used by routers to rank the trustworthiness of routes received from different routing protocols.

**Lower values indicate more preferred routes**, helping routers decide which routes to use when multiple paths to the same destination exist from different sources.

Route Source	Default Distance Values
Connected interface	0
Static route	1
External Border Gateway Protocol (BGP)	20
Enhanced Interior Gateway Routing Protocol (EIGRP)	90
OSPF	110
Routing Information Protocol (RIP)	120
Unknown*	255 223

[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)



## CompTIA Network+ N10-009 Course Notes

# Prefix Length

The prefix length in networking specifies the **number of contiguous bits** of the network mask that are set to 1.

This notation is an **integral part of CIDR** and helps in defining network boundaries and available hosts within those networks, enhancing both routing efficiency and address allocation.

**192.168.20.0/26**



## VRRP/FHRP

### First-Hop Redundancy

Protocols (FHRPs) are used to achieve high availability with multiple physical redundant routers.

- **HSRP (Hot Standby Router Protocol)**
  - Cisco proprietary redundancy protocol
- **VRRP (Virtual Router Redundancy Protocol)**
  - Open standard redundancy



## CompTIA Network+ N10-009 Course Notes

# Virtual IP (VIP)

A Virtual IP (VIP) address is an IP address that is **not tied to a specific physical network interface** on a device.

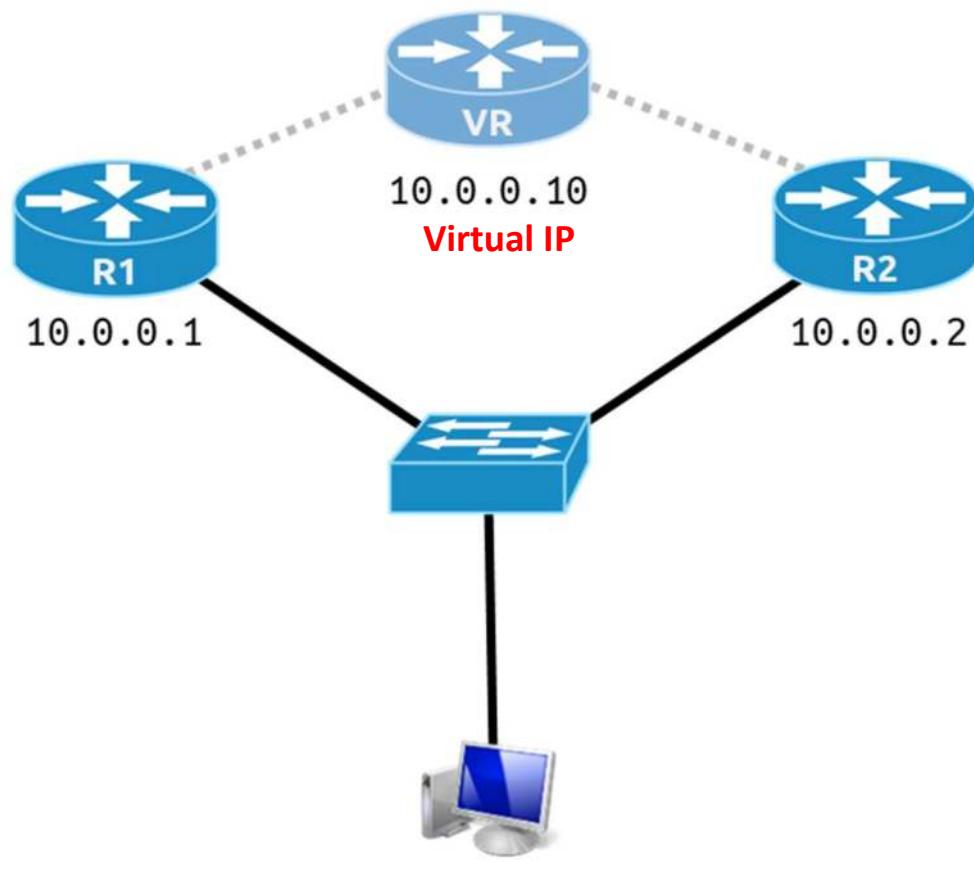
It is used to **provide redundancy and load balancing for services hosted on multiple servers**, allowing several servers to share the same IP address.

VIPs are **commonly used in network load balancers and failover configurations** to ensure continuous availability and scalability of critical applications and services.



## CompTIA Network+ N10-009 Course Notes

# VRRP/FHRP



10.100.100.100

Gateway: **10.0.0.10**

[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)



## Subinterface

A subinterface in networking is a virtual interface created by **dividing** a single physical interface into multiple logical interfaces.

This is commonly used in scenarios where multiple VLANs (Virtual Local Area Networks) exist on a **single router or switch** interface to manage traffic segregation and support various services or protocols over a single physical link.



## CompTIA Network+ N10-009 Course Notes

# Network Address Translation (NAT)

Network Address Translation (NAT) translates one IP address to another IP address

NAT can be provided by a Router or Firewall.

### Advantages

- Conserve public IP addresses
- Eliminates address overlap events with other LANs
- Makes it easier to connect to the internet
- Eliminates address renumbering if your network changes

### Disadvantages

- Translation delays the forwarding of packets
- Cause loss of end-to-end IP traceability
- Certain applications will not function with NAT enabled



## CompTIA Network+ N10-009 Course Notes

# Network Address Translation (NAT)

Network Address Translation (NAT) translates one IP address to another IP address

NAT can be provided by a Router or Firewall.

### Advantages

- Conserve public IP addresses
- Eliminates address overlap events with other LANs
- Makes it easier to connect to the internet
- Eliminates address renumbering if your network changes

### Disadvantages

- Translation delays the forwarding of packets
- Cause loss of end-to-end IP traceability
- Certain applications will not function with NAT enabled



## CompTIA Network+ N10-009 Course Notes

# Network Address Translation (NAT)

- **Static NAT (One-to-One)**
  - Translate one internal address to one external address
  - ONLY required if an internal host needs to be accessible from the Internet
- **Dynamic NAT (Many-to-Many)**
  - Translate many different internal addresses to many different external addresses
  - NOT commonly used since it can limit internet access
- **Port Address Translation (Many-to-One)**
  - Translates many different internal addresses to one external address
  - MOST commonly used to access the Internet
  - Also known as overloading NAT or PNAT



## CompTIA Network+ N10-009 Course Notes

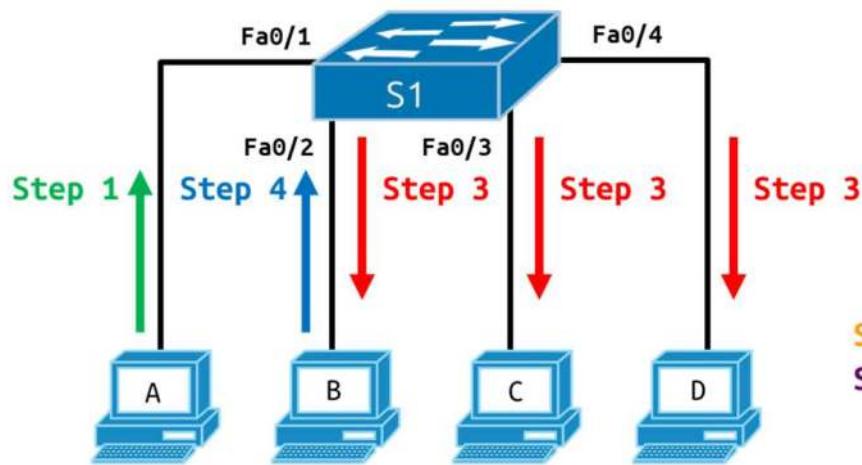
# Lesson 9

### Managing switches



## MAC Address Learning

**Address learning:** switches learn the source MAC addresses of a frame and store it in a Content Addressable Memory (CAM) filter table also referred to as a MAC address table.



CAM/MAC forward/filter				
S1# show mac-address-table				
Mac Address Table				
Vlan	Mac Address	Type	Ports	
Step 2	1	0000.0000.aaaa	DYNAMIC	Fa0/1
Step 5	1	0000.0000.bbbb	DYNAMIC	Fa0/2



## CompTIA Network+ N10-009 Course Notes

# VLAN

**VLANs(Virtual LANs)** are used to logically segment a switch into multiple broadcast domains

- **VLAN Benefits**

- **Broadcast Control**

- Each VLAN is a broadcast domain
    - Broadcast is contained within the VLAN

- **Improves Security**

- Host can only communicate within their VLAN
    - Inter-VLAN communication requires the use of a router or a layer 3 switch

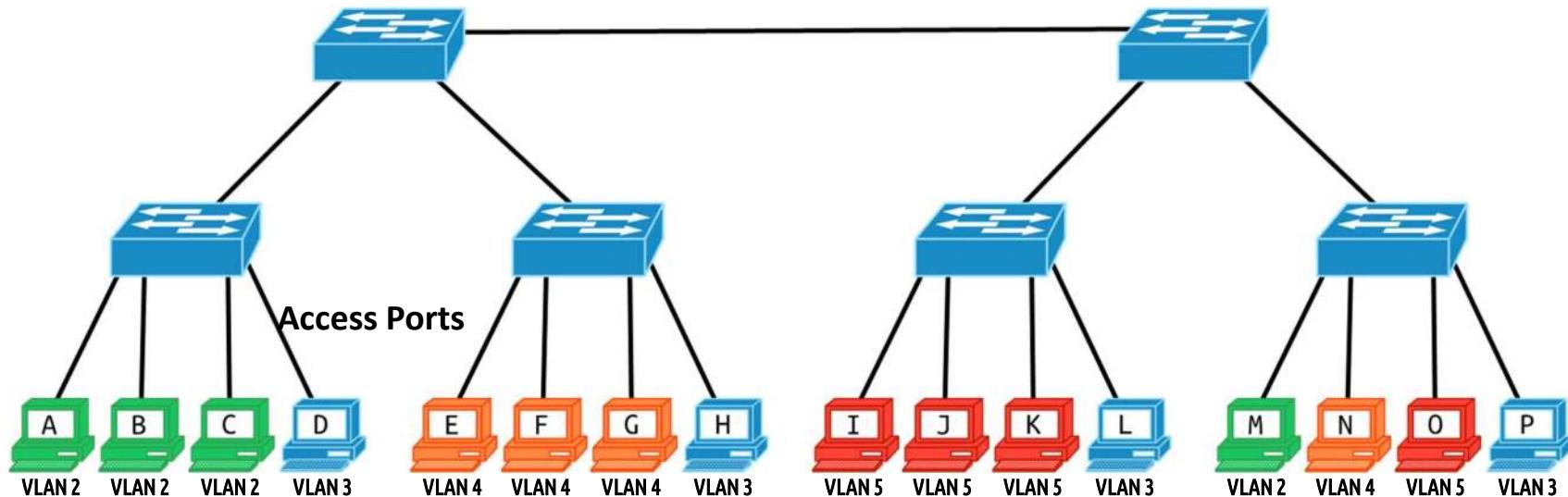
- **Flexibility and Scalability**

- Host in the same VLAN can always communicate with each other, even if they are connected on different switches in the same network



## CompTIA Network+ N10-009 Course Notes

# VLAN



Sales	VLAN 2	172.20.102.0/24
Shipping	VLAN 3	172.20.103.0/24
Engineering	VLAN 4	172.20.104.0/24
Finance	VLAN 5	172.20.105.0/24



## CompTIA Network+ N10-009 Course Notes

# VLAN Database

The VLAN database is where VLAN configurations are stored on a network device, such as a switch.

This database includes information like VLAN IDs and associated properties, enabling the switch to organize and manage network traffic accordingly.

```
S1#show vlan
VLAN Name          Status    Ports
---- -----
1     default       active   Fa0/3, Fa0/4, Fa0/5, Fa0/6
                           Fa0/7, Fa0/8, Fa0/9, Fa0/10
                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                           Fa0/23, Fa0/24, Gig0/1, Gig0/2
2     sales          active   Fa0/1
3     finance         active   Fa0/2
1002  fddi-default   active
1003  token-ring-default   active
1004  fddinet-default   active
1005  trnet-default    active
```



## CompTIA Network+ N10-009 Course Notes

# Port Tagging/802.1Q

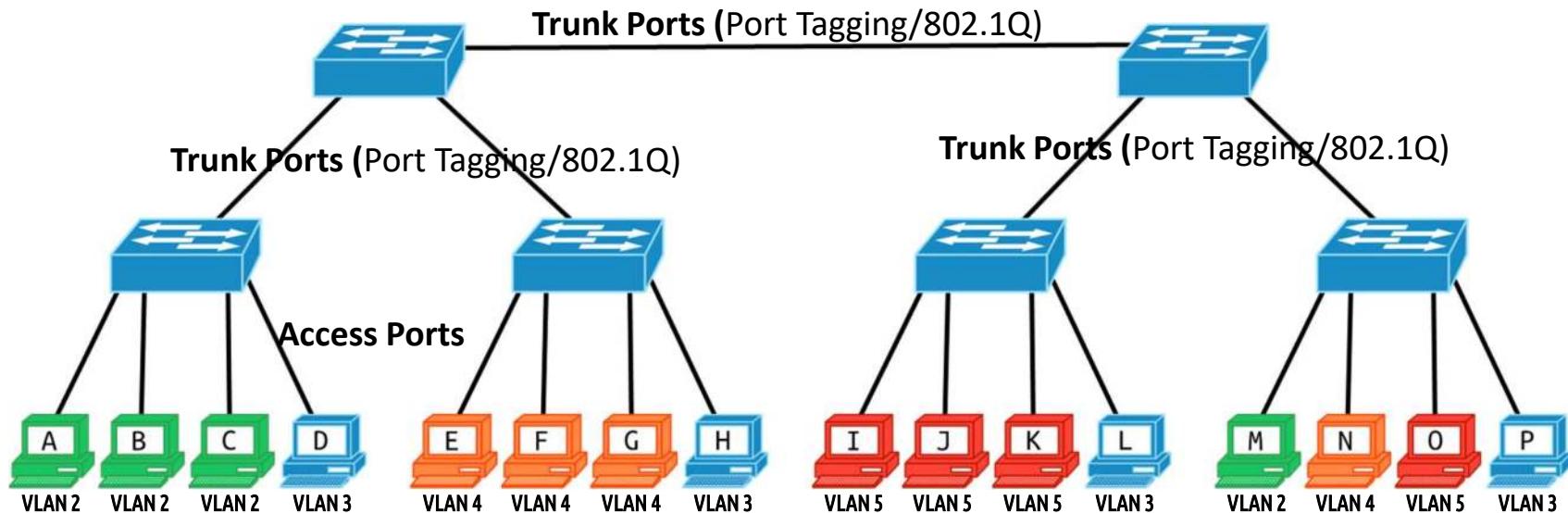
Port tagging, based on the IEEE 802.1Q standard, is a method of **inserting** a VLAN identifier into Ethernet frames to distinguish between different VLANs on a trunk link.

This allows multiple VLANs to **share** a single physical connection, enabling efficient use of network resources and traffic segregation.



## CompTIA Network+ N10-009 Course Notes

# VLAN



Sales	VLAN 2	172.20.102.0/24
Shipping	VLAN 3	172.20.103.0/24
Engineering	VLAN 4	172.20.104.0/24
Finance	VLAN 5	172.20.105.0/24



## Switch Virtual Interface

An SVI is a **virtual interface** on a switch that provides Layer 3 processing for VLANs.

It allows the switch to route traffic between VLANs by assigning IP addresses to VLAN interfaces, essentially **enabling inter-VLAN routing on layer 2 switches**.





## CompTIA Network+ N10-009 Course Notes

# Interface Configuration

Interface configuration involves **setting various parameters on network device interfaces** to optimize performance and functionality.

These settings can include VLAN assignments, link aggregation, and physical properties like speed and duplex mode.

```
31(config)#inter
31(config)#interface f0/1
31(config-if)#swit
31(config-if)#switchport mod
31(config-if)#switchport mode acc
31(config-if)#switchport mode access
31(config-if)#sw
31(config-if)#switchport acc
31(config-if)#switchport access vlan 2
31(config-if)#exit
31(config)#inter
31(config)#interface f0/2
31(config-if)#swit
31(config-if)#switchport mod
31(config-if)#switchport mode acc
31(config-if)#switchport mode access
31(config-if)#swit
31(config-if)#switchport acc
31(config-if)#switchport access vlan 3
```



## Native VLAN

The Native VLAN is the default VLAN on a trunk port that **carries untagged traffic**.

It is essential for ensuring that untagged traffic from older devices that don't support VLAN tagging is still routed correctly.



## CompTIA Network+ N10-009 Course Notes

# Voice VLAN

A **Voice VLAN** is designed to prioritize and **separate voice traffic** from other types of data traffic on the network.

This specialization ensures **quality of service (QoS)** for voice over IP (**VoIP**) communications, reducing latency, jitter, and packet loss for critical voice communications.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

242



## CompTIA Network+ N10-009 Course Notes

# Speed

Speed denotes the **data transfer rate** of a network connection, typically measured in megabits per second (Mbps) or gigabits per second (Gbps).

Configuring port speed ensures compatibility with connected devices and optimizes network performance.



## CompTIA Network+ N10-009 Course Notes

# Duplex

Duplex refers to the communication mode of a network connection.

Full duplex allows **simultaneous** two-way communication, while **half duplex** permits data transmission in **one direction at a time**.

Full duplex increases network efficiency, especially in high-traffic environments.



## CompTIA Network+ N10-009 Course Notes

# Spanning Tree Protocol

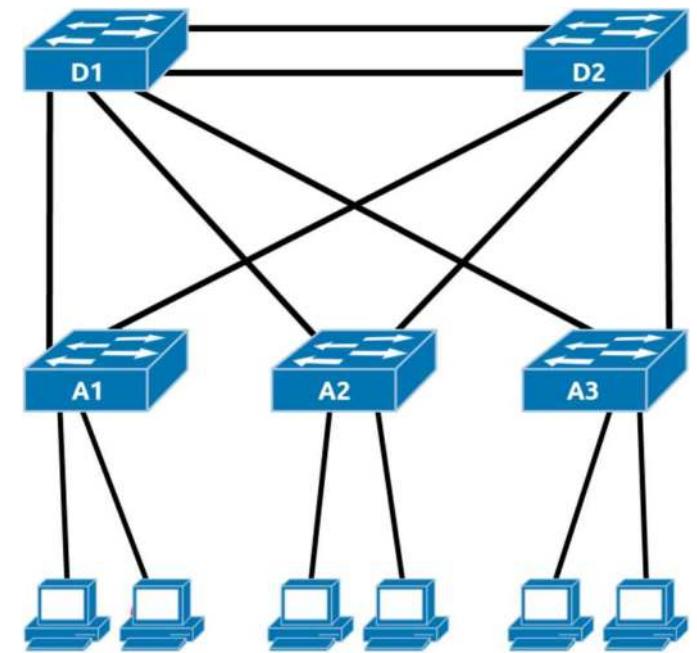
The Spanning Tree Protocol (STP) helps **prevent network loops** in a network's Ethernet topology by creating a spanning tree that logically blocks redundant paths.

If a network link fails, STP recalculates the paths and **unblocks** necessary links to ensure network traffic can still be **routed effectively**, maintaining network reliability and performance.



CompTIA Network+ N10-009 Course Notes

## Spanning Tree Protocol





## CompTIA Network+ N10-009 Course Notes

# Link Aggregation

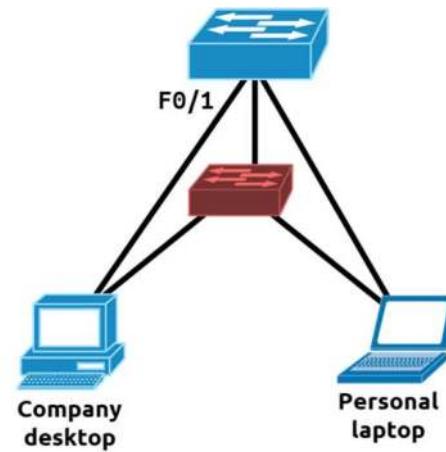
Port aggregation involves **combining** multiple network ports into a single group, increasing the bandwidth and providing **redundancy** for higher data throughput and reliability.

It allows for the **consolidation** of multiple links between switches or between switches and servers, enhancing the overall network capacity and fault tolerance.



## Port Security

Port Security allows us to control which devices and how many devices can be connected to a switch port based on the MAC address of the connected host.



```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport port-security maximum 1
Switch(config-if)# switchport port-security violation shutdown
Switch(config-if)# switchport port-security mac-address sticky
```



## CompTIA Network+ N10-009 Course Notes

# Port Mirroring/Spanning

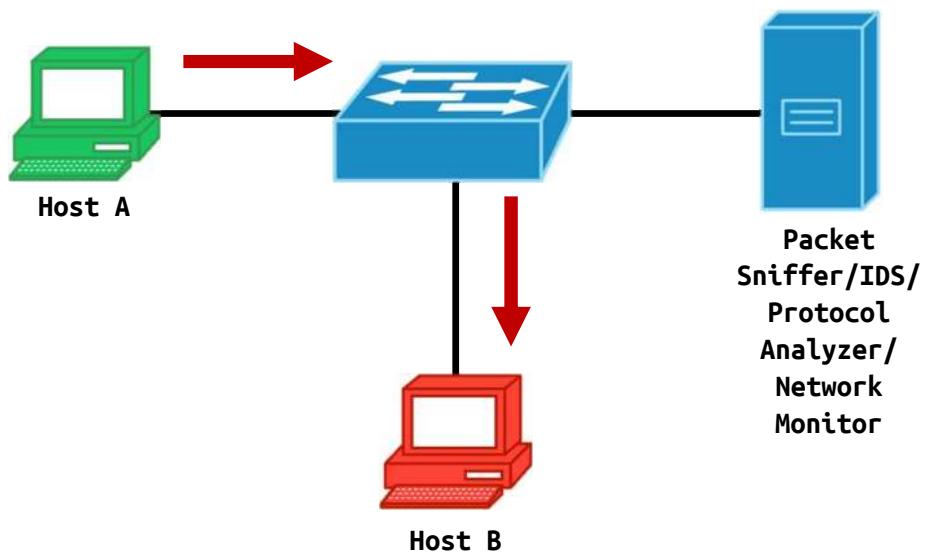
Allows you to redistribute traffic from one port to another

- SPAN (Switch Port Analyzer) / RSPAN (Remote SPAN)
- This is used to monitor traffic for troubleshooting
- Commonly used to monitor traffic with a packet sniffer or an IDS (Intrusion Detection System)

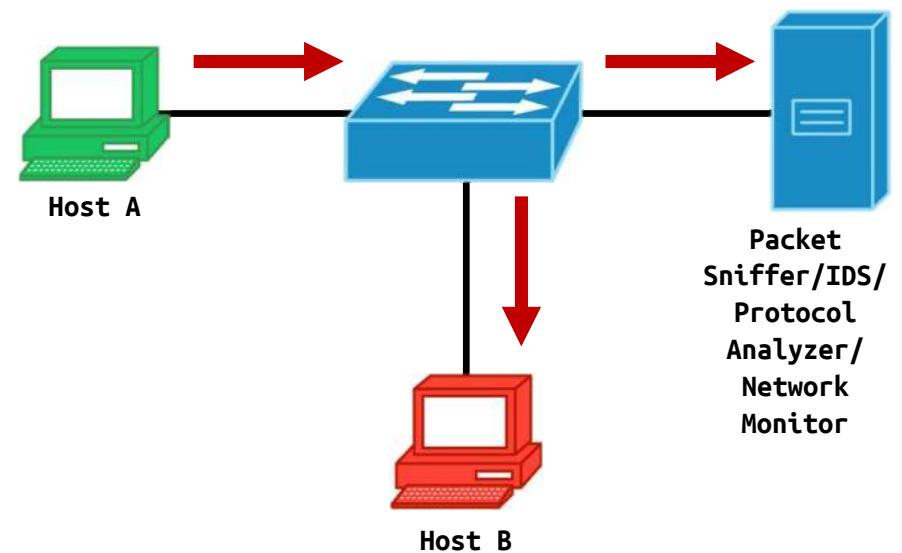


## Port Mirroring/Spanning

Standard switch operation



Port mirroring in effect





## CompTIA Network+ N10-009 Course Notes

# Maximum Transmission Unit (MTU)

The Maximum Transmission Unit (MTU) is the largest size of a packet or frame that can be sent in a packet- or frame-based network such as the Internet.

MTU sizes are variable, dependent on the physical medium and network protocol, with a common MTU for Ethernet being 1500 bytes.

Exceeding the MTU can result in the fragmentation of packets, which can decrease network efficiency and increase latency.



## CompTIA Network+ N10-009 Course Notes

# Jumbo Frames

Jumbo frames refer to Ethernet frames larger than the standard maximum of 1500 bytes, typically up to 9000 bytes.

Using jumbo frames can reduce overhead and improve performance in high-throughput networks, but **all network devices must support this feature** to avoid fragmentation.



## CompTIA Network+ N10-009 Course Notes

# Lesson 10

## Wireless Networking



## Channels

**WiFi channels** are **subdivisions** of the frequency bands used for wireless communication, allowing multiple networks to operate simultaneously without **interference**.

The availability and allowed **channels** can vary by country, subject to **regulatory** impacts that dictate the specific channels and power levels that can be used.



## Regulatory Impacts

Regulatory impacts refer to the rules and regulations set by **governmental or international** bodies that govern the use of wireless frequencies and channels to prevent interference between different communication systems.

These regulations affect the **availability** of certain frequencies and channels in different regions, impacting the design and deployment of wireless networks.



## CompTIA Network+ N10-009 Course Notes

# Channel Width

**WiFi Channels:** Subdivisions of a frequency band used for organizing and managing wireless communication.

- The availability and allowed channels can vary by country, subject to **regulatory** impacts that dictate the specific channels and power levels that can be used.

**Frequency:** The specific part of the electromagnetic spectrum used for WiFi, typically 2.4 GHz and 5 GHz bands.

**Relation:** Channels are specific ranges within a frequency band, each with a designated center frequency and bandwidth.



## Channel Width

Channel width refers to the frequency span of a wireless channel.

**Wider channels (e.g., 40 MHz, 80 MHz) offer more bandwidth**, which can increase data transmission speeds but may also increase the likelihood of interference in congested areas.



## CompTIA Network+ N10-009 Course Notes

# Frequency Options in Wireless Networking

Wireless networks operate across multiple frequency bands: 2.4 GHz for broad coverage and device compatibility, 5 GHz for higher data speeds and reduced congestion, and the newly introduced 6 GHz for even greater capacity and speed in dense environments.



## Non-Overlapping Channels

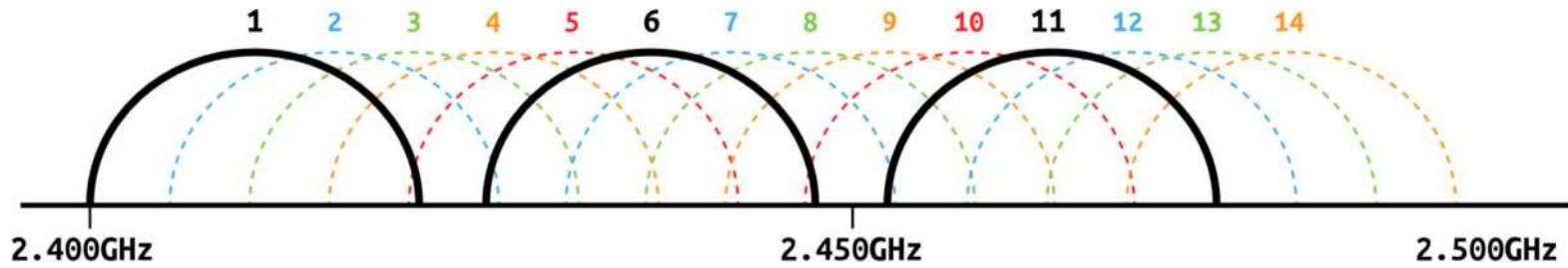
Non-overlapping channels are channels that **do not interfere with each other** and are crucial in environments with multiple wireless access points.

For instance, in 2.4 GHz Wi-Fi, channels 1, 6, and 11 are commonly used in the US because they do not overlap.



## CompTIA Network+ N10-009 Course Notes

# 2.4GHz





## 2.4GHz

The 2.4GHz band is widely used for wireless networking, offering a good **balance** between range and bandwidth.

- **Long range** communications because it has better penetration through barriers
- **Slower** data rates compared to 5GHz
- Higher rate of **interference** because of its longer range. E.g. microwave ovens.
- **Non-overlapping** channels **1, 6, and 11** offer the best chance of minimizing interference



## CompTIA Network+ N10-009 Course Notes

### 5GHz

The 5GHz band provides **faster data rates** at shorter distances compared to 2.4GHz and is **less likely to experience interference** from other household devices.

- Short range communication because of poor penetration through barriers
- Faster data rates than 2.4GHz
- Low chance of interference because of its shorter range





## CompTIA Network+ N10-009 Course Notes

# 6GHz

The introduction of the 6GHz band expands the **bandwidth** for wireless networks, doubling the spectrum available compared to the 5GHz band.

This increase supports higher data rates, lower latency, and more simultaneous connections, making it ideal for high-demand applications and environments.

The 6GHz band is particularly beneficial for **next-generation Wi-Fi technologies** like Wi-Fi 6E, which are designed to take full advantage of this increased capacity and performance.





## CompTIA Network+ N10-009 Course Notes

# Band Steering

**Band steering** is a network management technology that **automatically detects wireless devices capable of dual-band operations** and steers them to the less congested 5 GHz or 6 GHz band.

This process helps to balance the network load, maximize throughput, and improve overall wireless performance by minimizing interference found more commonly in the 2.4 GHz band.

By **optimizing the distribution** of devices across available bands, band steering enhances the efficiency and reliability of wireless networks, especially in areas with high network density.





## CompTIA Network+ N10-009 Course Notes

# 802.11h

802.11h is a standard that **enhances** 802.11 by adding support for dynamic frequency selection (DFS) and transmit power control (TPC) to comply with European regulations for 5 GHz WLANs.

**DFS** helps in avoiding interference with radar systems and other devices operating in the 5 GHz band.

**TPC** manages the power output of devices to reduce interference and ensure efficient use of the frequency spectrum.

- It adjusts the transmission power of the device based on the distance between devices and other network conditions, which helps in minimizing interference and conserving energy.



# Wireless Standards

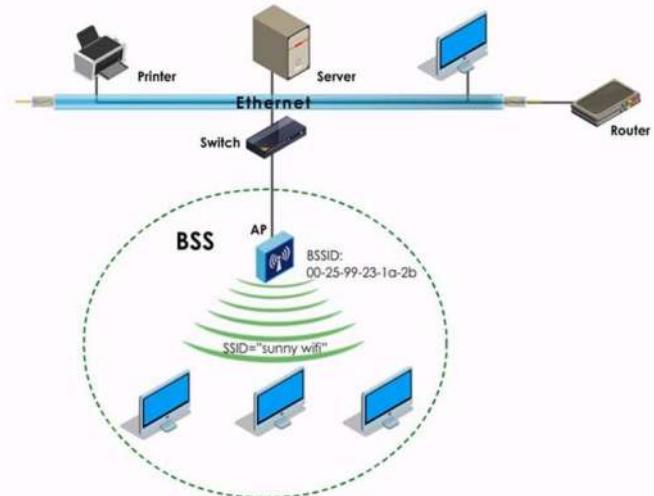
Standard	Frequency	Max Data Rate	Compatibility	Year
802.11a Wi-Fi 1	5 GHz	54 Mbps	802.11n/ac/ax	1999
802.11b Wi-Fi 2	2.4 GHz	11 Mbps	802.11g/n/ac/ax	1999
802.11g Wi-Fi 3	2.4 GHz	54 Mbps	802.11b/n/ac/ax	2003
802.11n Wi-Fi 4	2.4 GHz, 5 GHz	600 Mbps	802.11a/b/g/ac/ax	2009
802.11ac Wi-Fi 5	2.4 GHz, 5 GHz	3.5 Gbps	802.11a/b/g/n/ax	2012
802.11ax Wi-Fi 6	2.4 GHz, 5 GHz	9.6 Gbps	802.11a/b/g/n/ac	2019



## BSS vs. SSID vs. BSSID vs. ESS vs. ESSID

- **BSS**

- **Basic Service Set (BSS)** refers to a group of wireless devices operating with the same Access Point (AP). The **BSSID** is the physical MAC address of the AP and is included in the packets.



<https://medium.com/networks-security/wireless-lan-wap-bss-bssid-ssid-ess-ssid-5de3a81957f0>

[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

267



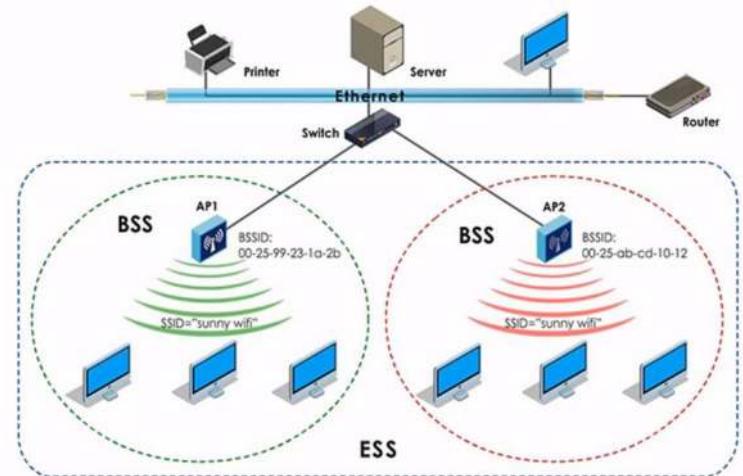
# BSS vs. SSID vs. BSSID vs. ESS vs. ESSID

- **SSID**

- **Service Set Identifier (SSID)**, also known as the network name, is a unique character string used to identify an AP.

- **ESS & ESSID**

- An **Extended Service Set (ESS)** is created by adding more APs to one Service Set. The network name for this extended set is called the **Extended Service Set Identifier (ESSID)**. All APs in an ESS broadcast the same SSID to users.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

<https://medium.com/networks-security/wireless-lan-wap-bss-bssid-ssid-ess-ssid-5de3a81957f0>



## CompTIA Network+ N10-009 Course Notes

# BSSID

The BSSID is a unique identifier that serves as the MAC address for a wireless access point (AP) and is used to differentiate one AP within a larger network or between multiple networks.

It is essential in environments where **multiple access points are deployed**, as it helps client devices identify and connect to the specific physical device providing the network service.

Since BSSIDs operate at the MAC address level, **they are crucial for low-level network functions** such as association and authentication processes within a WiFi network.





## CompTIA Network+ N10-009 Course Notes

### ESSID

An ESSID, also known as a Network Name, is used to identify a set of interconnected access points as a single network in larger WiFi deployments.

Unlike the BSSID, which identifies individual access points, the ESSID is shared among all APs in an Extended Service Set (ESS) to allow seamless connectivity for client devices as they move between APs.

The use of ESSID facilitates the creation of large, scalable wireless networks, providing **continuous connectivity** across different physical locations within the covered area, enhancing user mobility and network efficiency.





## Wireless Network Interface Card

- Required to connect to a wireless network or host
  - Defines support for the 802.11a/b/g/n/ac/ax/axe standards
  - Defines support for wireless encryption standards
  - Most devices have integrated wireless NICs, but not all





## Wireless Access Point

- Wireless Access Point (WAP/AP)
  - Use RF(Radio Frequency) to provide connections for wireless hosts
  - Creates a wireless star topology
  - Uses CSMA/CA to manage collisions
  - Layer 2 device
  - Creates a single collision domain and a single broadcast domain
  - Requires an IP Address (virtual IP address) for configuration and administration



Aruba 630 Wi-Fi 6E AP



Linksys 54g AP



# Autonomous Access Points

Autonomous Access Points **operate independently**, managing all aspects of networking—from security to data routing—on their own.

- Ideal for straightforward, smaller network environments where individual management of each AP is feasible.





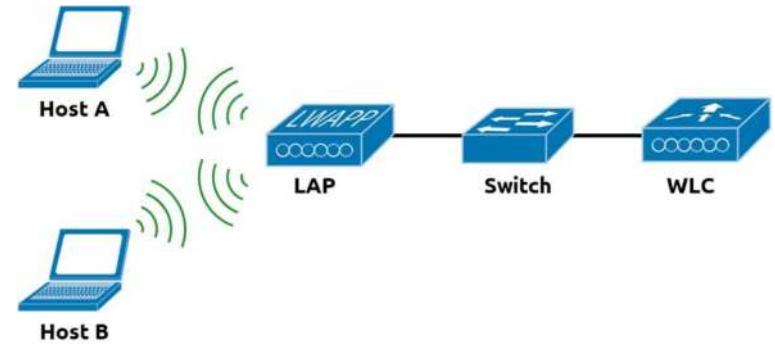
# Lightweight Access Point

Lightweight Access Point (LAP) is managed via a wireless LAN controller (WLC)

- Use to increase coverage, availability, and performance
- Can NOT be managed directly



Ubiquiti Unifi AX Pro





## CompTIA Network+ N10-009 Course Notes

# Wireless Antennas

- **Omni-directional Antennas** transmit a signal in all directions
  - **Most common** antenna type included in consumer and business wireless devices
  - **Shorter range** compared to a directional antenna



Dome Omni-directional Antenna



## Wireless Antennas

- **Directional Antennas** transmit a signal in one direction
  - Longer range compared to an Omni-directional antenna
  - **Yagi-Uda** antennas focus a wireless signal for up to a mile
  - **Parabolic antennas** focus a wireless signal for up to 8 miles



Yagi Directional Antenna



Parabolic Directional Antenna



## Wireless Network Types

Wireless network types vary based on configuration, usage, and structure.

Understanding these differences is crucial for deploying effective wireless solutions tailored to specific needs and environments.

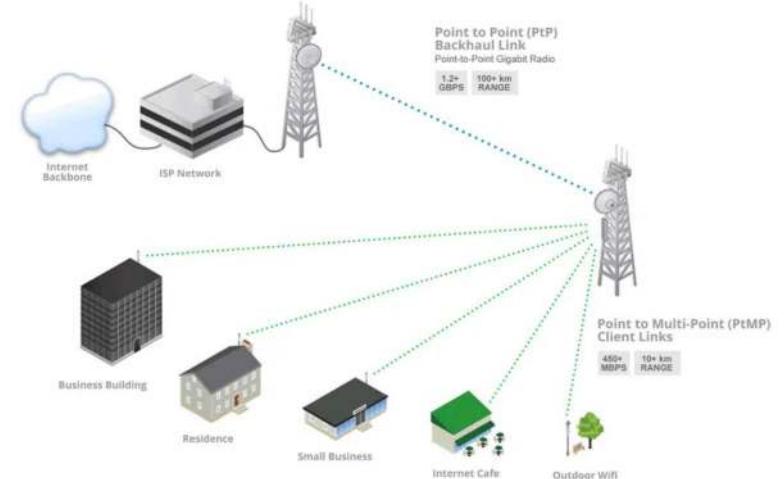


## CompTIA Network+ N10-009 Course Notes

# Point-to-Point Networks

Point-to-point networks establish a **direct connection** between two wireless devices.

This type of network is commonly used for **linking two locations** in a WAN or providing a dedicated pathway for data transmission, ensuring consistent and reliable connectivity.





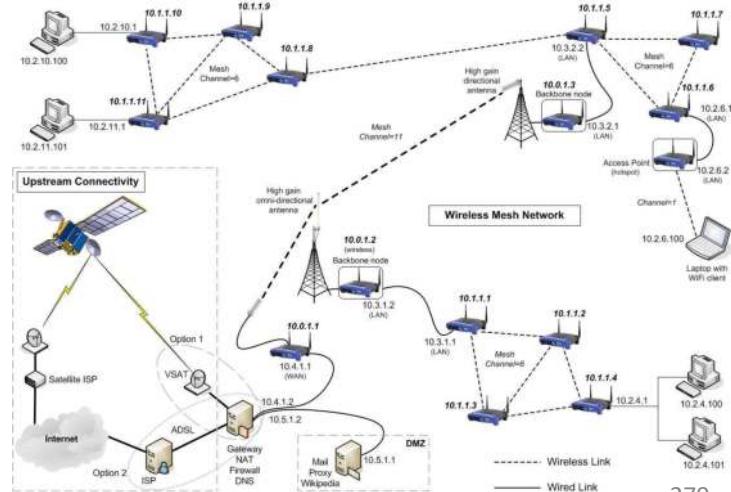
## CompTIA Network+ N10-009 Course Notes

# Mesh Networks

Mesh networks consist of **nodes** that connect directly and dynamically to as many other nodes as possible.

This configuration creates **multiple pathways** for data to travel between points, enhancing reliability and redundancy.

Mesh networks are **self-healing and scalable**, making them ideal for large areas like smart cities and IoT applications.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

279



## CompTIA Network+ N10-009 Course Notes

# Ad Hoc Networks

Ad hoc networks are **decentralized** and do not rely on a pre-existing infrastructure.

Nodes within an ad hoc network communicate directly without the use of a router or a network server, making them **suitable for temporary setups** in situations where quick deployment is necessary, such as emergency response or military operations.



Ad Hoc Mode

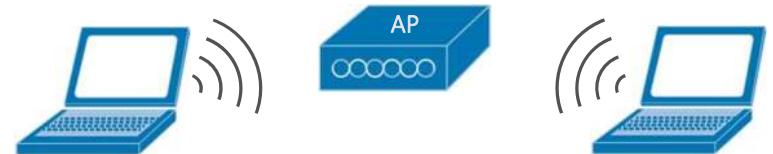


## CompTIA Network+ N10-009 Course Notes

# Infrastructure Networks

Infrastructure networks **rely on fixed routers** or access points that manage traffic to and from wireless devices.

This is the **most common type of network** setup for residential and commercial internet connections, providing stable and controlled connectivity, with the access points serving as the hub for all wireless communication in the network.



Infrastructure Mode



## CompTIA Network+ N10-009 Course Notes

# Encryption

Encryption is crucial in wireless networking to secure data transmissions against unauthorized access and interception.

It involves **converting data into a coded format** that can only be accessed and read by devices with the correct decryption key.



## WPA2

WPA2 is a **security protocol** developed to secure wireless computer networks.

- Users authenticate using an **alpha numeric passphrase (PSK)** via **CCMP(Counter mode Cypher block chaining Message authentication code Protocol)**
- Encrypts with **AES (Advance Encryption Standard)**
- Vulnerable to the KRACK attack



## WPA3

**WPA3 is the latest security protocol** for wireless networks, introduced to address vulnerabilities found in WPA2 and provide enhanced security measures.

- Users authenticate using Simultaneous Authentication of Equals(SAE) via GCMP(Galois/Counter Mode Protocol)
- Encrypts with AES (Advance Encryption Standard)
- Vulnerable to the Dragonblood attack



## Guest Networks

**Guest networks** are **separate access networks** provided by businesses or institutions to allow visitors limited internet access without exposing the main network.

They help maintain network security by **isolating guest user traffic** from critical internal resources.

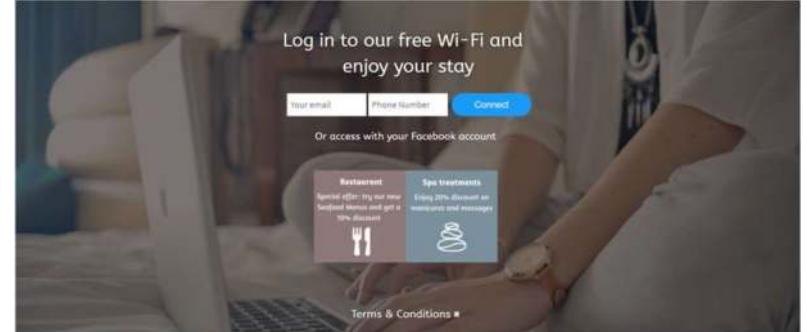


## CompTIA Network+ N10-009 Course Notes

# Captive Portals

Captive portals are **web pages** that appear **automatically** when a user connects to a public or semi-public Wi-Fi network, requiring interaction before network access is granted.

They are **commonly used in guest networks** to manage access through authentication, terms of service agreements, or payment information.





## Authentication in Wireless Networks

**Authentication** is a **critical security process** in wireless networks, ensuring that only authorized devices can connect.

It verifies the identities of devices attempting to connect, using various methods to prevent unauthorized access.



## CompTIA Network+ N10-009 Course Notes

# Pre-shared Key vs. Enterprise Authentication

**Pre-shared Key (PSK)**: This method involves a **simple, shared key known to all users** of the network, commonly used in home and small office environments.

It offers **ease of setup** but **lower security** as the key is shared among users.

**Enterprise Authentication**: Uses a more secure approach by **employing a RADIUS server** to manage each user's authentication individually.

This method is suited for larger organizations, providing **stronger security** through individual credentials and enhanced control over network access.



## CompTIA Network+ N10-009 Course Notes

# Lesson 11

## Installing a Network



## CompTIA Network+ N10-009 Course Notes

# Important Installation Implications

Proper planning of physical installations is crucial for network performance and scalability.

The selection of locations for network components like IDFs and MDFs affects accessibility, maintenance, and future expansion capabilities.



## CompTIA Network+ N10-009 Course Notes

# Selecting Locations for Network Installations

The choice of location for network installations impacts signal quality, network speed, and system reliability.

Considerations include environmental factors, distance to users, and compliance with safety regulations to ensure optimal network function and longevity.



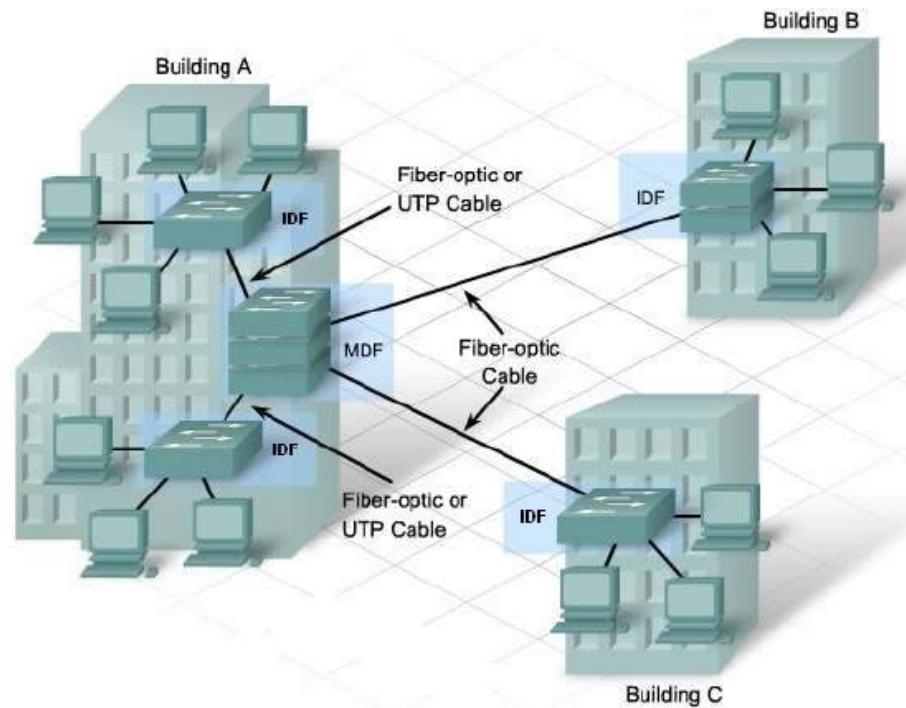
## Main Distribution Frame (MDF)

The MDF is the **primary hub** of a network's cabling system, where incoming service providers' lines meet the internal network.

It should be **centrally located** to minimize cable lengths and facilitate easy access for configuration and troubleshooting, ensuring robust network management and scalability.



# Main Distribution Frame (MDF)





## CompTIA Network+ N10-009 Course Notes

# Intermediate Distribution Frame (IDF)

An **IDF** serves as a secondary hub in network infrastructure, positioned to reduce the distance data must travel between the **MDF** and end users.

It is typically located on each floor or section of a building to handle local network traffic, enhancing performance and reducing latency.



## Rack Size

Selecting the appropriate rack size is crucial for accommodating networking equipment and **ensuring efficient use of space.**

Factors to consider include the number of devices, future expansion needs, and available physical space in the installation area.

4-Post 42U  
Server Rack  
Cabinet



1U Server



2U Server



## Port-side Exhaust/Intake

Proper ventilation is essential to prevent **overheating** and maintain **optimal performance** of networking equipment.

Positioning devices to ensure adequate airflow and considering port-side exhaust/intake configurations can help dissipate heat effectively and prolong equipment lifespan.



## CompTIA Network+ N10-009 Course Notes

# Cabling

Cabling plays a critical role in network connectivity, carrying data between devices and infrastructure components.

Proper cable management, including the use of patch panels and fiber distribution panels, ensures organization, accessibility, and ease of maintenance.





## Patch Panels

Patch panels serve as **centralized points for connecting and managing network cables**, facilitating easy troubleshooting and reconfiguration.

They help streamline cable management, reduce clutter, and provide a structured approach to cable organization within the rack.



Front of patch panel RJ45 jacks



Rear of patch panel 110 block



## CompTIA Network+ N10-009 Course Notes

# Fiber Distribution Panels

**Fiber distribution panels** are used to **terminate and distribute** fiber optic cables within the network infrastructure.

They ensure **efficient routing** of fiber connections, minimize signal loss, and provide a centralized location for managing fiber connect'





## CompTIA Network+ N10-009 Course Notes

# Lockable Cabinets

Lockable cabinets offer enhanced security by **restricting physical access** to networking equipment and sensitive data.

They help **prevent unauthorized tampering** or theft, safeguarding the integrity and confidentiality of the network infrastructure.





## CompTIA Network+ N10-009 Course Notes

# Power Management in Network Installations

**Effective power management** is crucial for maintaining **network reliability** and **operational efficiency**.

Proper planning ensures that all network components receive **stable and sufficient power**, preventing downtime and equipment damage.



# Uninterruptible Power Supply (UPS)

An UPS **provides emergency power** to a load when the input power source or mains power fails.

A battery backup that will keep your critical equipment powered even when there is a disruption in service

- Runtime vs Capacity
- Runtime informs on how long connected devices can be powered for
- Capacity is how much power a battery can store
- Higher capacity should equal a longer run time





# Power Distribution Units (PDUs)

Power Distribution Units (PDUs) are devices designed to **distribute electric power** to various components within a network or data center.

PDUs can range from simple power strips to complex units providing **remote monitoring** and control over multiple power outlets.





## CompTIA Network+ N10-009 Course Notes

# Managing Power Load

Calculating the power load is essential to determine the **total power requirements** of all network equipment in the installation.

Adequate power provisioning helps in balancing loads, optimizing power usage, and planning for future capacity needs without overloading circuits.



## CompTIA Network+ N10-009 Course Notes

# Voltage Considerations

Different network devices may require different voltage levels; thus, understanding voltage requirements is vital for compatibility and safety.

Ensure that power supplies and backup systems are correctly configured to handle the **specific voltage needs of the equipment**, minimizing the risk of electrical issues and maximizing performance.





## CompTIA Network+ N10-009 Course Notes

# Environmental Factors in Network Installations

**Environmental conditions** significantly impact the **longevity** and **efficiency** of network equipment.

Managing factors such as humidity, temperature, and fire suppression is crucial to ensure stable and reliable network operation.



## Humidity Control

Proper humidity levels are essential to **prevent corrosion and static electricity buildup**, which can damage network components.

Maintaining relative humidity within a specified range (typically 45-55%) helps protect sensitive electronic equipment and ensures optimal performance.





## CompTIA Network+ N10-009 Course Notes

# Fire Suppression Systems

Integrating efficient fire suppression systems within network environments is vital for **protecting hardware against fire damage**.

These systems should be designed to be **non-damaging to electronic equipment**, often using gas or clean agent extinguishers rather than water-based solutions.





## Fire Suppression Systems

- **Wet pipe:** water is contained in the pipes for fast response
- **Dry pipe:** no water in pipes, it must be released from a holding tank
- **Preaction:** like dry pipe except it requires a thermal-fusible link to melt before the water is released
- **Deluge:** releases a large about of water in a room to extinguish the fire
- **Clean Agents:** non-conductive, gaseous fire extinguisher that leaves no residue behind.





# Temperature Management

Consistent temperature control is critical to avoid **overheating** or cold-related malfunctions in network equipment.

The recommended temperature for most networking environments is kept cooled, with **active cooling solutions** to maintain this range.





## CompTIA Network+ N10-009 Course Notes

# Lesson 12

## Cloud Concepts and Connectivity Options



## CompTIA Network+ N10-009 Course Notes

# Network Functions Virtualization (NFV)

NFV involves the **decoupling of network functions from hardware devices** and running them as software instances on virtual machines or containers.

In cloud computing, NFV allows for **flexible deployment and management** of networking services like firewalls, load balancers, and intrusion detection systems.

It **reduces the need for dedicated hardware** and enables dynamic scaling and management, which enhances resource utilization and reduces costs.





## CompTIA Network+ N10-009 Course Notes

# Virtual Private Cloud (VPC)

A VPC is an **isolated network space within a public cloud** designed to provide a similar level of segmentation, control, and security as a private data center.

Users can define their own IP address range, configure subnets, route tables, and network gateways.

This allows enterprises to **run their cloud resources in a virtual network** that they can control, similar to how they would manage a network in their own data center.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

313



## CompTIA Network+ N10-009 Course Notes

### Network Security Groups and List

Network security groups are used to **control inbound and outbound traffic** to cloud resources within a VPC.

Similar to network security groups, network security lists are also used for **managing and securing network traffic** in a cloud environment.

They generally provide **stateful or stateless traffic filtering on a subnet level**, enabling more **granular control** over traffic between subnets within the same VPC or across different VPCs.

These act as a **virtual firewall** for associated instances to control traffic based on rules that specify allowed or denied ports, protocols, and source/destination IP addresses.

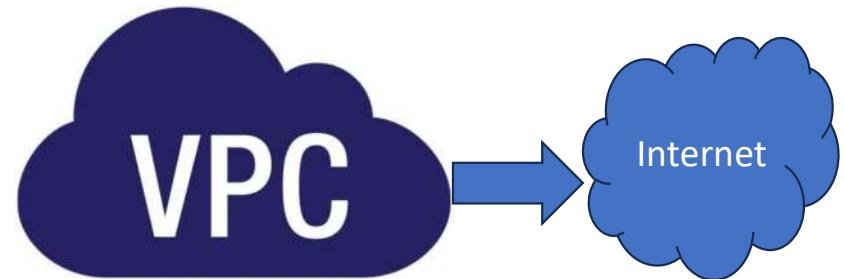


## Internet Gateway

An internet gateway serves as a bridge between a company's VPC and the internet.

**It enables internet access for the resources within the VPC.**

This gateway facilitates communications between instances in the cloud and external networks.





## CompTIA Network+ N10-009 Course Notes

# NAT Gateway

A NAT gateway allows instances in a private subnet to connect to the internet or other external services while preventing the internet from initiating a connection with those instances or seeing their private IP addresses.

This is crucial for instances that require outbound internet access (for updates, for example) but do not need inbound internet connections.

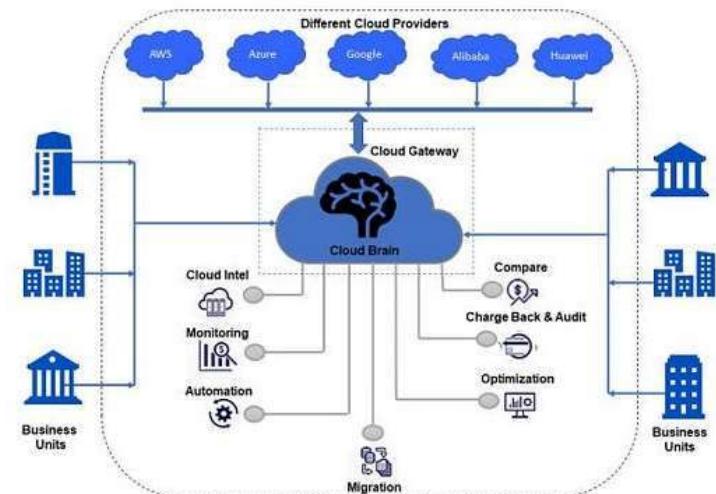


## CompTIA Network+ N10-009 Course Notes

# Cloud Gateways

Cloud gateways serve as intermediary devices or services that **connect cloud environments with different networks**, including private data centers or other cloud services.

They facilitate communication, data transfer, and management between these dissimilar environments, ensuring that users and applications can securely and efficiently access cloud resources.





## Cloud Connectivity Options

Cloud connectivity options refer to the various **methods through which data and applications can connect to and interact with cloud environments.**

These options are crucial for ensuring efficient, secure, and reliable access to cloud resources from different locations.

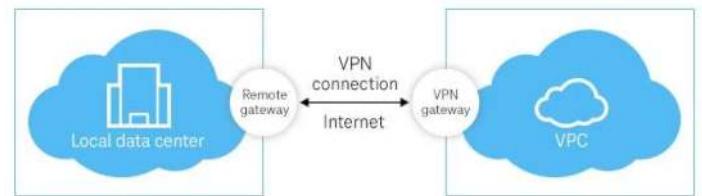


## CompTIA Network+ N10-009 Course Notes

# Virtual Private Network (VPN)

A Virtual Private Network (VPN) is a technology that creates a **safe and encrypted** connection over a less secure network, such as the internet.

VPNs are used to establish **secure connections** between remote users or remote sites and an organization's private network, allowing for secure data transmission across public networks as if the devices were **directly connected** to the private network.



<https://www.open-telekom-cloud.com/en/products-services/core-services/virtual-private-network>



# Private-Direct Connection to Cloud Provider

A **private-direct** connection refers to a **dedicated network link** between an organization's on-premises infrastructure and a cloud service provider's data center.

This direct connection **bypasses the public internet**, offering more reliable, secure, and faster connectivity for accessing cloud services.

It is ideal for businesses with stringent **performance** and **security** requirements for their **cloud-based** applications and data.



## Deployment Models

Deployment models in networking and cloud computing refer to the specific **configurations** and **environments** in which technology services and infrastructure are implemented.



## CompTIA Network+ N10-009 Course Notes

# Public

- **Public Cloud**

- Multitenant third-party service
- Hardware resources are shared with other disparate organizations
- Most affordable and least secure





## CompTIA Network+ N10-009 Course Notes

# Private

- **Private Cloud**

- Single tenant service
- No hardware resources are shared with other organizations
- First-party or third-party service
- Most secure and most expensive
- Can be hosted by the company or cloud provider





# Community Cloud

- **Community Cloud**
  - Multitenant shared service
  - Organizations with a shared interest manage the service
    - Mission, Security, Policy, and Compliance considerations
  - Managed by the organization or a third party
  - Can be on-premise or off-premise





## CompTIA Network+ N10-009 Course Notes

# Hybrid

- **Hybrid Cloud**

- Combination of any cloud with services also being hosted on-premise
- Are bounded together using standardized or proprietary technologies
- Enables data and application portability
  - i.e Load balancing between clouds





## Service Models

Service models in cloud computing describe the **various types of services** offered over the internet, enabling businesses and users to access computing resources and applications without the need to invest in **physical infrastructure**.



## CompTIA Network+ N10-009 Course Notes

# Software as a Service (SaaS)

SaaS delivers **applications** over the internet, accessible through a web browser, eliminating the need for installations and maintenance on individual devices.

It allows users to access software applications on a **subscription** basis, providing convenience and cost savings on software **licensing** and **infrastructure**.



<https://citrusbug.com/blog/saas-application-example> 327

[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)



# Infrastructure as a Service (IaaS)

IaaS provides virtualized computing resources over the internet, offering a fully **outsourced** service for computing infrastructure.

Users can **rent** servers, storage space, and networking capabilities, scaling resources up or down based on demand, which is ideal for businesses looking for **flexibility** and **scalability** without the capital expenditure of physical hardware.



<https://www.filecloud.com/blog/2020/03/what-is-iaas-infrastructure/>

[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

328

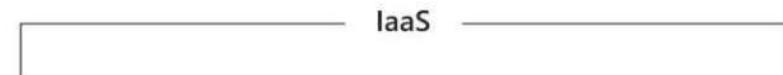


## CompTIA Network+ N10-009 Course Notes

# Platform as a Service (PaaS)

PaaS offers a **cloud platform** and tools to allow developers to build, test, deploy, and manage applications without worrying about the underlying infrastructure.

This model provides a development environment, application hosting, and a deployment platform, **streamlining** the development process and reducing the **complexity** of managing hardware and software layers.



Servers and storage



Networking firewalls / security



Data center physical plant / building

<https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-iaas>

[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

329



## CompTIA Network+ N10-009 Course Notes

# Service Models

	SaaS	PaaS	IaaS
User	Customer	Customer	Customer
Application	Provider	Customer	Customer
Operating System	Provider	Provider	Customer
Hardware	Provider	Provider	Provider
Network	Provider	Provider	Provider
Facility	Provider	Provider	Provider
Regulatory Compliance	Customer	Customer	Customer



## Cloud Traits

- **Multitenancy**

- Public and community clouds operate on shared resources

- **Elasticity**

- Resources can be allocated and reallocated to support service availability and performance
- Can be done automatically

- **Scalability**

- Services can scale up as needed
- CPU cores, RAM, storage, and bandwidth can be increased when needed
- More servers can also be added if needed



## CompTIA Network+ N10-009 Course Notes

# Lesson 13

## IP Services



## CompTIA Network+ N10-009 Course Notes

# Dynamic Addressing

**Dynamic addressing automates the assignment of IP addresses** to devices on a network using DHCP (Dynamic Host Configuration Protocol).

This method ensures **efficient management** of IP addresses, reducing configuration errors and administrative overhead by automatically providing devices with IP addresses, subnet masks, gateway information, and DNS settings.

It is particularly useful in environments with **frequently changing network devices**, such as wireless networks and temporary connections, simplifying network management and connectivity for users.

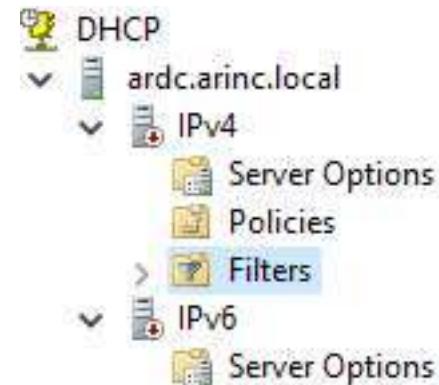


# DHCP (Dynamic Host Configuration Protocol)

DHCP is a network management protocol used on IP networks whereby a DHCP server **dynamically assigns** **an IP address** and other network configuration parameters to each device on the network, allowing them to communicate on an IP network.

It **automates** the process of configuring devices on IP networks, making it easy to manage network settings centrally.

DHCP enables devices to join an IP network **without requiring manual configuration** of IP settings, improving the efficiency of network management.



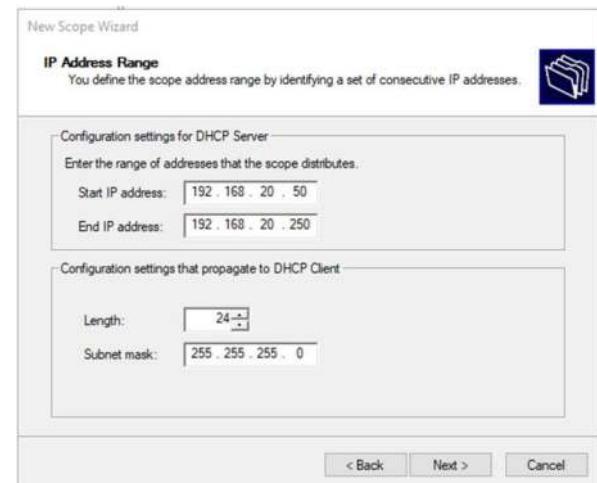


## CompTIA Network+ N10-009 Course Notes

# Scope

A DHCP scope is a **defined range of IP addresses** that a DHCP server can use to assign to clients.

Each scope is configured with a range of IP addresses and other network settings, such as subnet mask, default gateway, DNS servers, and lease duration. Scopes are essential for **organizing and managing IP address distribution** in different segments of a network.





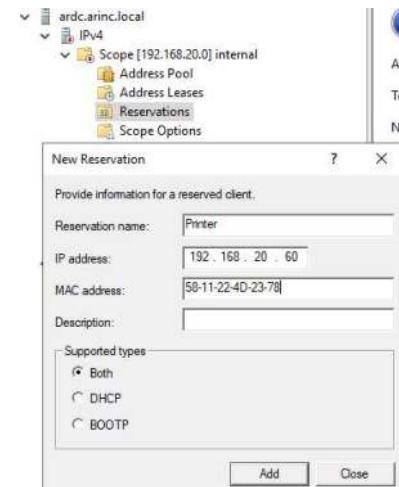
## CompTIA Network+ N10-009 Course Notes

# Reservation

A DHCP reservation is a specific IP address within a DHCP scope that is **reserved for use by a specific device**, identified by its MAC address.

When the device requests an IP address, the DHCP server assigns it the reserved IP address, ensuring the device receives the **same IP address** every time.

Reservations are used for devices that need a **consistent IP address** but still benefit from DHCP's centralized management.





## CompTIA Network+ N10-009 Course Notes

# Lease Time

Lease time refers to the **duration** for which a DHCP server grants a device the right to use a specific IP address.

Once the lease time **expires**, the device must either **renew** its current IP address lease with the DHCP server or **obtain a new one**.

Lease time settings can help manage the **availability** of IP addresses in a network, especially in environments with frequent **device changes**.

New Scope Wizard

**Lease Duration**  
The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

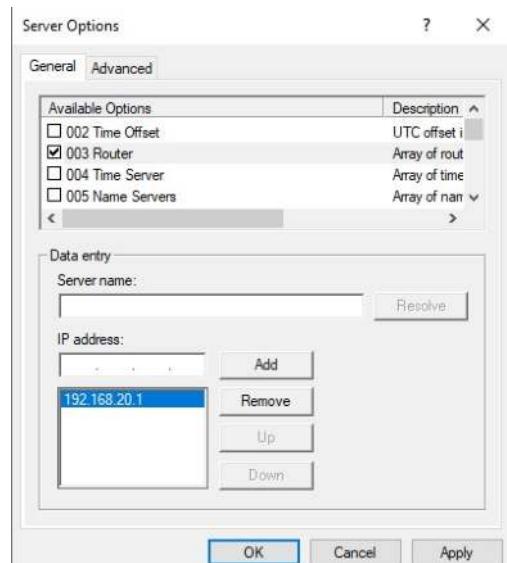
Days:  Hours:  Minutes:

< Back Next > Cancel



# DHCP Options and Functionality

DHCP Options extend the capabilities of the DHCP server, allowing it to pass configuration parameters like Domain Name System (DNS) servers, Network Time Protocol (NTP) servers, and Windows Internet Name Service (WINS) servers to DHCP clients.



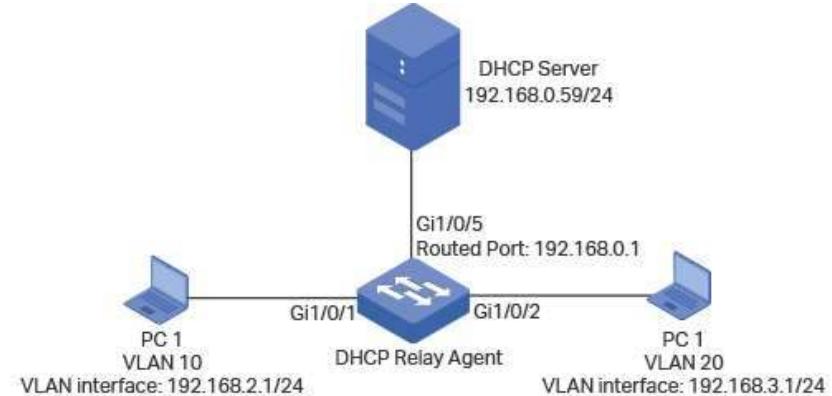


## DHCP Relay

A DHCP relay is a network function that **forwards DHCP requests** from clients on one network to a DHCP server on another network.

This allows devices on subnets **without a direct DHCP server** to obtain IP addresses and other network configuration details.

DHCP relay agents are used to extend the reach of DHCP servers **across multiple subnets**, making network management more efficient.





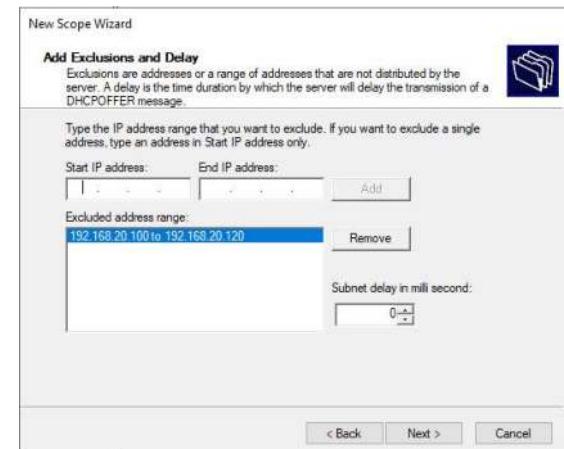
## CompTIA Network+ N10-009 Course Notes

# Exclusion Ranges

Exclusion ranges are subsets of a DHCP scope that are **not used for dynamic assignment**.

These IP addresses are reserved for **manual assignment** or for devices that require a fixed IP address, such as printers, servers, or routers.

Setting up exclusion ranges ensures that there are no IP address conflicts between dynamically assigned addresses and those assigned statically.





## CompTIA Network+ N10-009 Course Notes

# Stateless Address Autoconfiguration (SLAAC)

Stateless Address Autoconfiguration (SLAAC) is a feature in IPv6 that allows a device to **automatically configure its own IP address** without the need for manual configuration or DHCP.

Using SLAAC, a device can generate its own IPv6 address **based on the router advertisement it receives** and its own hardware (MAC) address.

This capability **provides plug-and-play connectivity for IPv6 devices**, reducing the need for additional configuration and easing the deployment of IPv6 networks.

FE80::7207:12FF:FE34:5678



## CompTIA Network+ N10-009 Course Notes

# Name Resolution

Name resolution is the process of **converting human-readable domain names into IP addresses** that networking equipment can understand and use to route data.

It is facilitated by DNS (Domain Name System), which acts like a phone book for the internet, allowing users to access websites using **domain names** rather than complex numerical IP addresses.



## Domain Name System

**DNS** is a **naming system** for computers, services, or other resources connected to the Internet or a private network.

It translates more readily memorized **domain names** to the numerical **IP addresses** needed for locating and identifying computer services and devices with the underlying **network protocols**.

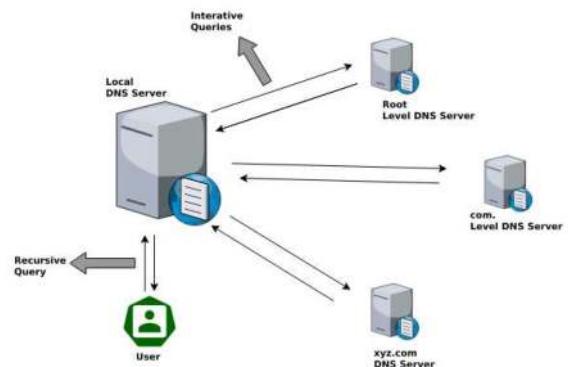
**DNS** is **essential for the functionality of the internet**, making it possible to use easy-to-remember domain names instead of **IP addresses**.



## Recursive DNS Queries

Recursive DNS queries involve a DNS server taking on the responsibility of retrieving data from other DNS servers on behalf of the client, providing a complete answer.

This process is essential when the local DNS server does not immediately have the answer, requiring it to perform multiple queries across the DNS infrastructure to resolve the name fully.





## DNS Zone Types

DNS zones are **portions** of the domain name space in the Domain Name System (DNS), which are managed by a specific entity or administrator.

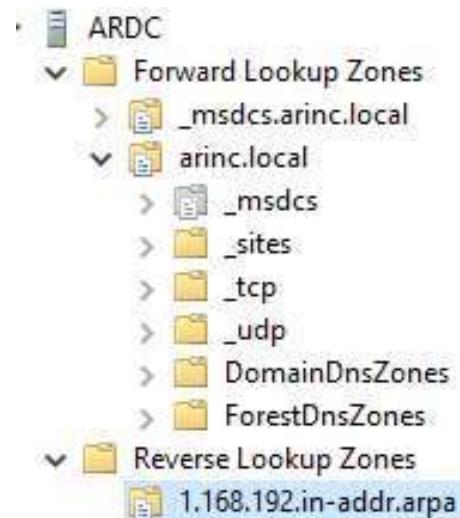
Understanding different zone types is crucial for effective DNS management and ensuring proper domain resolution.



## Forward Zone

A forward zone in DNS is used to **resolve domain names to IP addresses**.

It contains records like A, AAAA, and MX, facilitating the **translation** of human-readable domain names into machine-readable IP addresses.

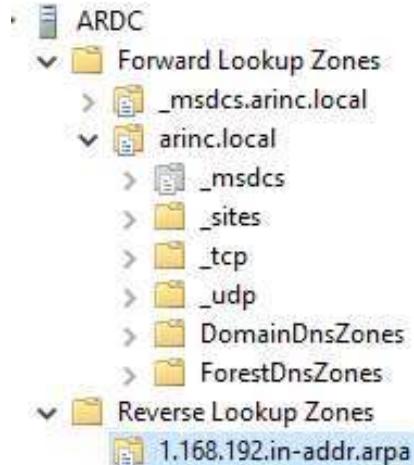




## Reverse Zone

Reverse zones handle the mapping of IP addresses **back to domain names**, essentially the opposite of forward zones.

This zone type is used in **reverse DNS lookups**, where the IP address is known and the associated hostname is needed, often for network troubleshooting and security verification.





## Authoritative vs. Non-Authoritative

**Authoritative DNS Zone:** This zone has the **final authority** over its own records, providing definitive answers to queries about domain names within its zone without needing to query other sources.

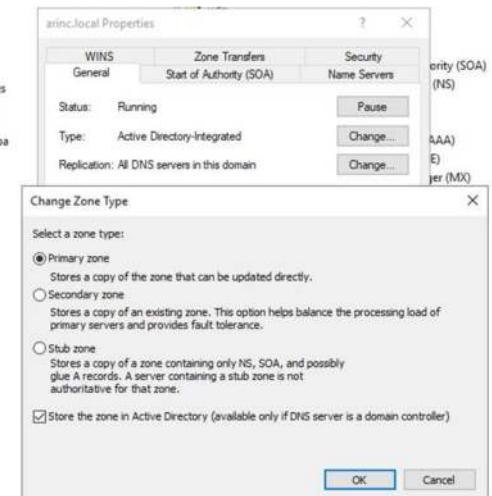
**Non-Authoritative DNS Zone:** A non-authoritative zone provides information that has been **obtained from another server**, not from the original source, usually cached data from previous queries.



## CompTIA Network+ N10-009 Course Notes

# Primary vs. Secondary Zones

**Primary DNS Zone:** The primary zone is the main zone file **where DNS records are stored** and managed. It allows changes to **DNS records directly**.

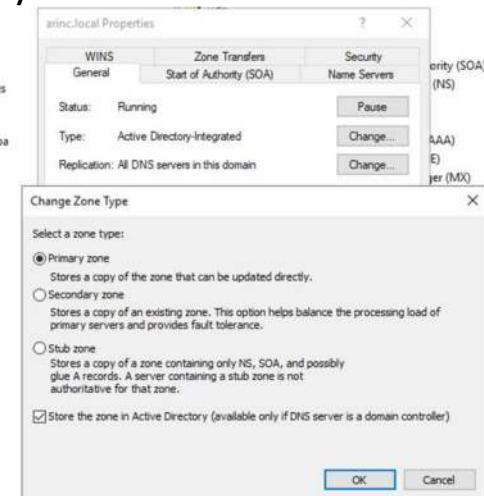




## CompTIA Network+ N10-009 Course Notes

# Primary vs. Secondary Zones

**Secondary DNS Zone:** A secondary zone is a **read-only copy of the primary zone** that serves as a backup, reducing the load on the primary server and increasing redundancy for fault tolerance.





## CompTIA Network+ N10-009 Course Notes

# DNS Security Extensions (DNSSEC)

DNSSEC enhances DNS security by providing **authentication** of DNS data, verifying its integrity and ensuring it has not been tampered with during internet navigation.

It uses **digital signatures** to validate that the DNS responses come from the authentic source, significantly reducing the risk of cache poisoning and other DNS-based attacks.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)



## CompTIA Network+ N10-009 Course Notes

# DNS over HTTPS (DoH) and DNS over TLS (DoT)

DNS over HTTPS (DoH) and DNS over TLS (DoT) are protocols designed to **encrypt DNS queries**, ensuring that DNS requests and responses are secure from eavesdropping and man-in-the-middle attacks.

DoH routes DNS queries through the HTTPS protocol, while DoT uses the TLS protocol, both enhancing privacy and security by preventing unauthorized interception of DNS data.

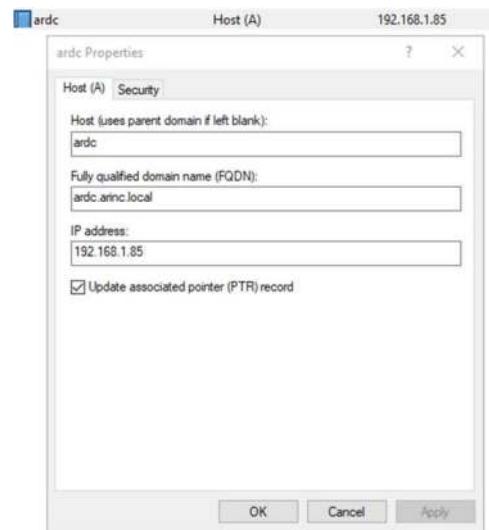


## CompTIA Network+ N10-009 Course Notes

# Address (A) Record

The Address (A) Record maps a domain name to its **corresponding IPv4 address**, allowing users to **access websites using human-readable domain names** instead of numerical IP addresses.

It is one of the **most commonly used** record types in DNS settings.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

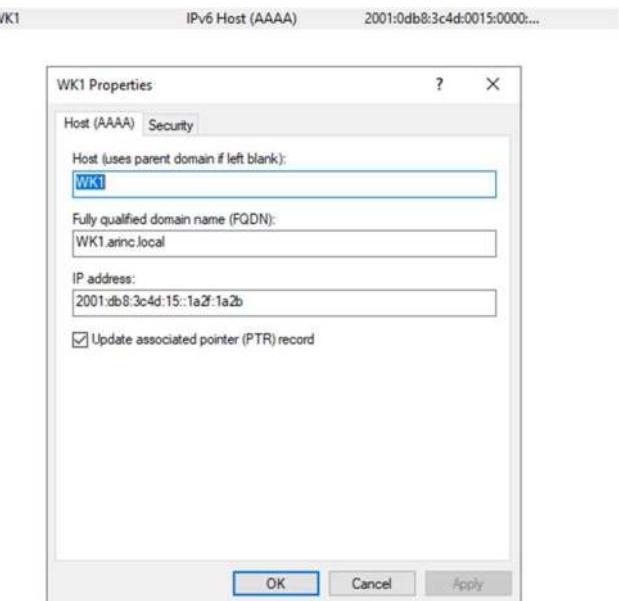
353



## CompTIA Network+ N10-009 Course Notes

# AAAA Record

The AAAA Record functions similarly to the A record but **maps a domain name to an IPv6 address**, which accommodates the longer numeric addresses used by the newer IPv6 protocol.

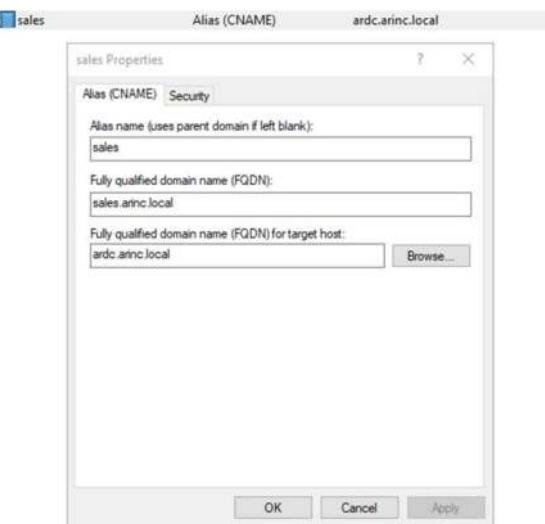




# Canonical Name (CNAME) Record

A CNAME Record maps an **alias name** to a true or canonical domain name.

This is used when multiple domain names **resolve to the same IP address**, allowing for easier management and changes in the network.

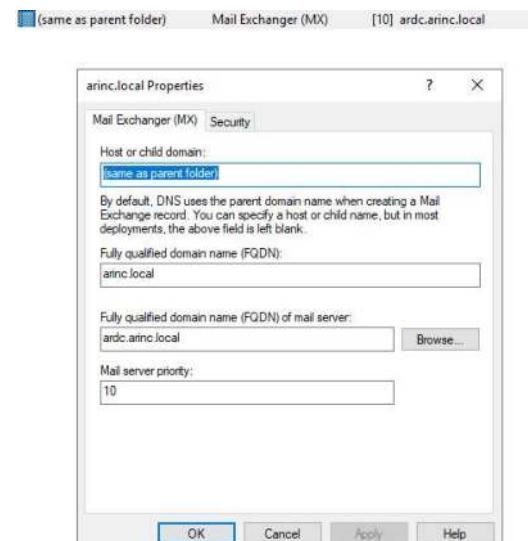




# Mail Exchange (MX) Record

MX Records are used to **specify the mail servers** responsible for receiving email messages on behalf of a domain.

This record points to the domain's email server(s) and prioritizes mail delivery if multiple servers are listed.



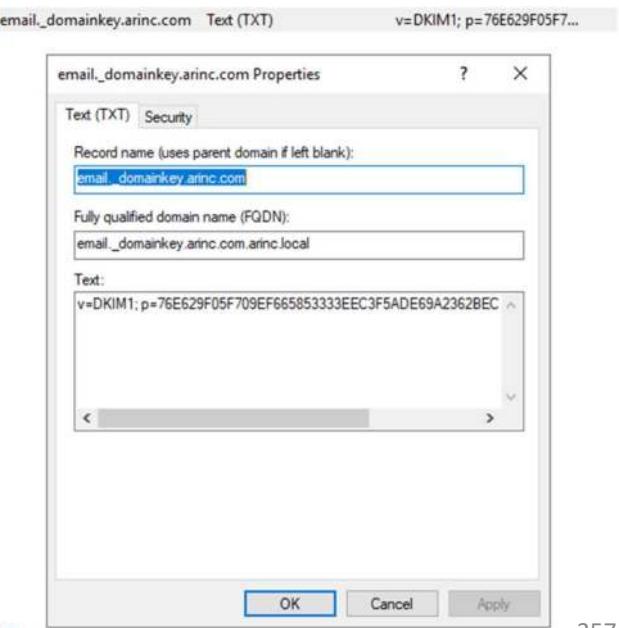


## CompTIA Network+ N10-009 Course Notes

# Text (TXT) Record

**TXT** Records hold **text information** for sources outside of the domain.

This information can be used for a variety of purposes, such as **verifying domain ownership** and **implementing email security measures like SPF and DKIM**.



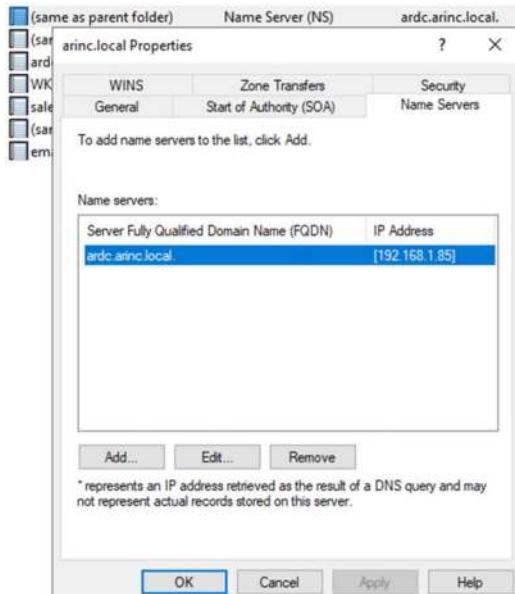


## CompTIA Network+ N10-009 Course Notes

# Nameserver (NS) Record

NS Records identify the DNS servers responsible for a **specific domain**, indicating authoritative servers that can answer queries for the domain.

These records help in **delegating subdomains** and managing multiple DNS servers.



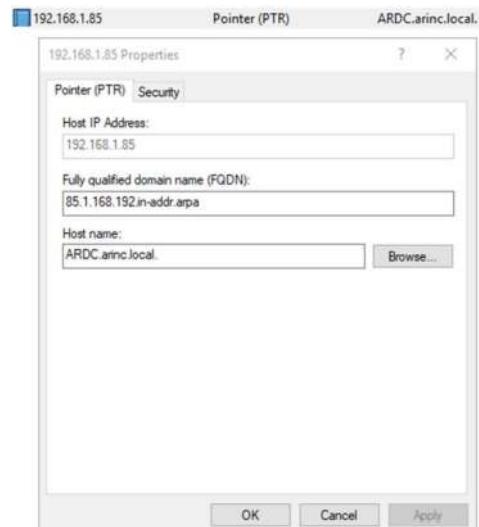


## CompTIA Network+ N10-009 Course Notes

# Pointer (PTR) Record

PTR Records map an IP address to a domain name, essentially the opposite of A or AAAA records.

They are primarily used for **reverse DNS lookups**, where the IP address is known, but the hostname is needed. This record type is particularly useful for **network troubleshooting** and security checks.





## CompTIA Network+ N10-009 Course Notes

# Hosts File

The hosts file is a computer file used by an operating system to **map hostnames to IP addresses**.

It serves as a **simple form of local DNS** resolution, which the system checks before querying external DNS servers, allowing for manual override of DNS lookup.

This file is **commonly used for testing website deployments** and blocking access to unwanted sites by redirecting domain names to incorrect or loopback IP addresses.

```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97    rhino.acme.com        # source server
#      38.25.63.10    x.acme.com            # x client host
#
# localhost name resolution is handled within DNS itself.
#      127.0.0.1    localhost
#      ::1          localhost
#
142.250.80.78    google.com
142.250.80.78    www.google.com|
```

[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

360



## Time Protocols

Time synchronization protocols are essential for ensuring **consistent and accurate** time across all devices within a network.

They play a critical role in network operations, logging, security, and ensuring the proper sequence of events in distributed systems.



## CompTIA Network+ N10-009 Course Notes

# Network Time Protocol (NTP)

NTP is one of the **oldest and most commonly used protocols** to synchronize the clocks of computers over a network.

It uses a **hierarchical system** of time sources to minimize the impact of variable network latency and can adjust clocks to within milliseconds of Coordinated Universal Time (UTC).

```
Console> (enable) set ntp server 172.20.52.65
NTP server 172.20.52.65 added.
Console> (enable) set ntp client enable
NTP Client mode enabled
Console> (enable) show ntp
```

```
Current time: Tue Jun 23 1998, 20:29:25
Timezone: '', offset from UTC is 0 hours
Summertime: '', disabled
Last NTP update: Tue Jun 23 1998, 20:29:07
Broadcast client mode: disabled
Broadcast delay: 3000 microseconds
Client mode: enabled
```

```
NTP-Server
-----
172.16.52.65
Console> (enable)
```



## Network Time Security (NTS)

NTS is an extension of NTP, designed to provide **security improvements** over the original protocol.

It adds **encryption and authentication** to NTP, ensuring that the time data exchanged between clients and servers is both secure and reliable, protecting against various types of tampering and attacks.



## Precision Time Protocol (PTP)

PTP, defined in IEEE 1588, is used for **very precise time synchronization**, typically in measurement and control systems where high precision is required.

Unlike NTP, which can achieve millisecond-level accuracy, PTP can synchronize clocks to within **nanoseconds** across a local area network (LAN).



## CompTIA Network+ N10-009 Course Notes

# Lesson 14

## Network Documentation



# Common Documentation

Common documentation in networking provides **visual and textual records** essential for the design, management, and troubleshooting of network infrastructures.

These documents are crucial for ensuring **clarity** and **consistency** across IT and network teams.

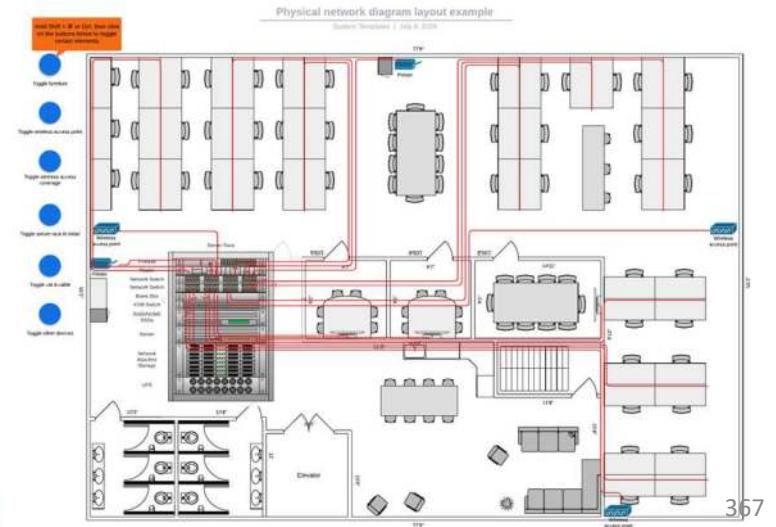


CompTIA Network+ N10-009 Course Notes

# Physical Network Diagram

A physical network diagram illustrates the **physical connections between network devices** such as routers, switches, and firewalls, as well as their **physical locations**.

This diagram helps in understanding the **layout** of the network hardware and facilitates **troubleshooting** and network **maintenance**.

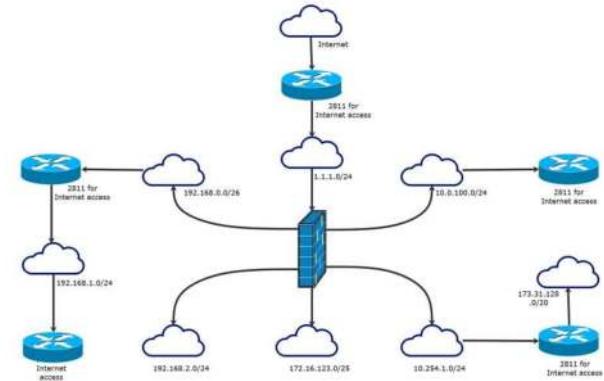




# Logical Network Diagram

A logical network diagram illustrates how **data flows within a network**, showing the **interconnections** between devices, subnets, and other network components without detailing the physical connections.

It focuses on illustrating the architecture and protocols operating within the network, helping in understanding routing, IP addressing, and network segmentation.

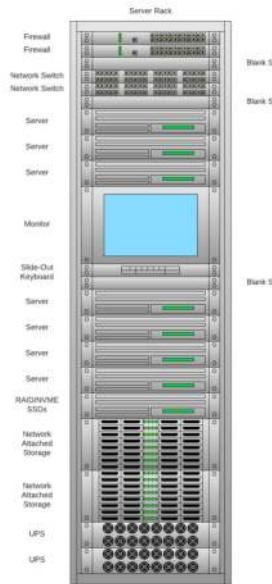




# Rack Diagram

A rack diagram provides a detailed view of the **equipment mounted in server racks**, including servers, switches, routers, and other networking devices.

This visualization aids in space management, airflow planning, and the organization of physical assets **within data centers or server rooms**.





## CompTIA Network+ N10-009 Course Notes

# Cable Maps/Diagrams

**Cable maps and diagrams** are essential tools for **documenting the physical and logical layout** of network cables and equipment.

They provide a **clear visual representation** that aids in installation, troubleshooting, and future upgrades by detailing connections, pathways, and network topology.

Maintaining **accurate and up-to-date** diagrams ensures efficient network management and quick resolution of issues.



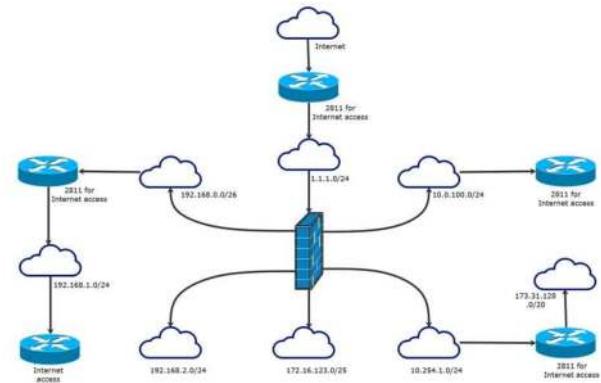


## CompTIA Network+ N10-009 Course Notes

# Network Diagrams

Network diagrams are crucial for **visualizing the structure and components of a network**, facilitating understanding, management, and troubleshooting.

They can represent physical connections (Layer 1), data link configurations (Layer 2), and logical pathways (Layer 3).





## Layer 1,2,3 Diagrams

- Layer 1 diagrams focus on the **physical components** of the network, such as cabling, devices, and geographic locations.
  - They are essential for planning physical network deployments and for managing the physical connections between network devices.
- Layer 2 diagrams detail how switches, bridges, and other **data link layer devices** interact and the paths that Ethernet frames travel within the network.
  - VLAN information, and other **data link level details are typically illustrated** to provide insights into the configuration of network segments.
- Layer 3 diagrams provide a **high-level view** of network topology and routing, including how different network segments and devices **route traffic**.
  - They often include information such as IP addresses, subnets, and routing protocols, which are crucial for understanding and managing the logical routing of data.



## CompTIA Network+ N10-009 Course Notes

# Asset Inventory in Network Management

Asset inventory is critical for managing the hardware, software, and licensing of network resources effectively.

Keeping an **updated inventory** helps in strategic planning, compliance, and budgeting for upgrades and maintenance.



## CompTIA Network+ N10-009 Course Notes

# Hardware Inventory

A detailed hardware inventory includes all **physical devices** such as routers, switches, servers, and other networking equipment.

It tracks specifications, locations, and the condition of each asset, assisting in lifecycle management and replacement scheduling.





## CompTIA Network+ N10-009 Course Notes

# Software Inventory

Software inventory encompasses all **system and application software** running within the network, documenting versions, installations, and configurations.

This information is vital for ensuring compatibility, planning upgrades, and managing security patches.

Software Name	Version	Manufacturer	License Type	Category	Network Installed	Action	Managed Installed	Self
Dell Deliverv Ser...	2.0.753.0	Dell Inc.	Unidentified	Not Assigned	1		1	
Intel(R) Connect L...	8.7.30402.191461	Intel Corporation	Unidentified	Not Assigned	1		1	
Dell SupportAssist	5.5.5.16206	Dell Inc.	Unidentified	Not Assigned	1		1	
ManageEngine DCM...	11.2.2001.1W	Zoho Corp	Unidentified	Not Assigned	1		1	
Microsoft .NET Run...	5.0.17.31213	Microsoft Corp.	Unidentified	Not Assigned	1		1	
ManageEngine D...	10.0.0.0	Zoho Corp	Unidentified	Not Assigned	1		1	
Microsoft Visual C...	14.27.295120	Microsoft Corp.	Unidentified	Not Assigned	1		1	
Realtek Audio Driver	6.0.7561.1	Realtek Semicon.	Unidentified	Not Assigned	1		1	
7-Zip 22.01 (beta)	22.01	Apir Plane	Unidentified	Not Assigned	1		1	
Update for Windows	4.91.0.0	Microsoft Corp.	Unidentified	Not Assigned	1		1	
Mozilla Firefox	98.0.2	Mozilla	Unidentified	Not Assigned	1		1	
Dell Power Manager	3.11.0	Dell Inc.	Unidentified	Not Assigned	1		1	

<https://www.manageengine.com/products/desktop-central/software-inventory.html>



## CompTIA Network+ N10-009 Course Notes

# Licensing Management

Effective licensing management ensures **compliance** with software use rights and avoids legal and financial penalties.

It involves tracking the number of licenses, usage rights, expiration dates, and renewals for all software products.





## CompTIA Network+ N10-009 Course Notes

# Warranty Support Management

Keeping detailed records of warranty and support agreements for network assets helps **manage service claims** and technical support efficiently.

This inventory ensures **timely access to vendor support** and prevents disruptions due to hardware or software failures.





# IP Address Management (IPAM)

IP Address Management (IPAM) is a crucial tool for **organizing, tracking, and managing** the IP address space within a network.

It helps **prevent IP conflicts** by providing a clear inventory of allocated and available IP addresses, supports the integration and management of DHCP and DNS services, and enhances network reliability and security through meticulous tracking of IP address assignments.

Effective IPAM also aids in **compliance** and **strategic network planning** by ensuring efficient use of IP resources.

The screenshot displays the IP Address Manager interface with three main sections:

- Top 10 DHCP Scopes by Utilization:** A table showing the utilization of DHCP scopes. The columns are Scope Name, % IP Space Used, IPs Available, and IPs Used. The data includes:

Scope Name	% IP Space Used	IPs Available	IPs Used
Top_WiFi_Austri2	28.38%	104	150
Top_WiFi_Austri1	33.20%	56	108
Top_WiFi_Austri1	33.20%	181	182
WiFi_Bridge	50.00%	25	25
WiFi_Core	49.02%	26	25
WiFi_Austri2	49.02%	26	25
Curitiba-Dell	48.44%	132	122
WiFi_Austri1	45.80%	71	60
WiFi_Austri2	44.78%	74	60
WiFi_Austri2	41.67%	79	58

- IP Address Conflicts:** A table showing IP address conflicts. The columns are IP ADDRESS, TIME, SUBNET, TIME OF CONFLICT, ASSOCIATED MAC, and CONFLICTING MAC. The data includes:

IP ADDRESS	TIME	SUBNET	TIME OF CONFLICT	ASSOCIATED MAC	CONFLICTING MAC
10.199.22.0	29 Jan 2017 7:38:08PM	10.199.22.0/24	29 Jan 2017 7:38:08PM	00:47:95:29:DF:7E	00:89:CB:32:21:11
10.1.1.10	29 Jan 2017 7:32:18PM	10.1.1.0/24	29 Jan 2017 7:32:18PM	00:12:9B:85:04:E5	00:08:56:85:04:E4

- Last 25 IPAM Events:** A table showing the last 25 IPAM events. The columns are TIME, SYSTEM, and MESSAGE. The data includes:

TIME	SYSTEM	MESSAGE
12/29/2017 1:28 AM	SYSTEM	The IP address 10.199.22.2 is in conflict. The following devices were detected on network with same IP address: Other Leases MAC: 00:47:95:29:DF:7E, MAC: 00:89:CB:32:21:11
12/29/2017 1:28 AM	SYSTEM	The conflict for IP Address 10.199.22.2 is resolved with MACs: 00:47:95:29:DF:7E, 00:89:CB:32:21:11
12/29/2017 1:32 AM	SYSTEM	The conflict for IP Address 10.1.1.10 is resolved with MACs: 00:12:9B:85:04:E5, 04:0B:58:50:EA:64
12/29/2017 1:32 AM	SYSTEM	The IP address 10.1.1.10 is in conflict. The following devices were detected on network with same IP address: Other Leases MAC: 00:12:9B:85:04:E5, MAC: 04:0B:58:50:EA:64
12/29/2017 1:27 AM	SYSTEM	The conflict for IP Address 10.199.22.3 is resolved with MACs: 00:10:18:AC:71:22, 76:95
12/29/2017 1:27 AM	SYSTEM	The IP address 10.199.22.3 is in conflict. The following devices were detected on network with same IP address: Other Leases MAC: 00:10:18:AC:71:22, 76:95



## CompTIA Network+ N10-009 Course Notes

# Service-level Agreement

A Service-level Agreement (SLA) is a formal document that **outlines the expected service standards a provider must meet**, as agreed upon with a client.

It **details the specifics of services**, including responsibilities, performance metrics, and remedies or penalties for breaches, ensuring **clear expectations** for service quality and availability.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

379



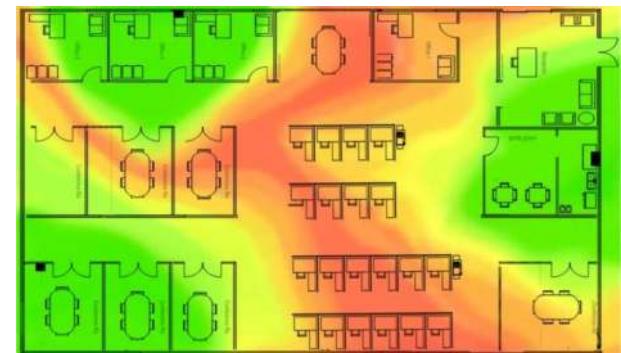
## Wireless Survey and Heat Map

**Purpose of Wireless Survey:** A wireless survey **assesses the coverage and performance** of a wireless network within a specified area.

It identifies the **optimal placement** for access points and detects areas of signal weakness or interference.

Heat maps visually represent the **wireless signal strength** and coverage across different areas of a location.

They are **generated from data collected during the wireless survey**, providing a color-coded map that illustrates signal intensity and helps in planning network improvements for consistent and efficient wireless coverage.



<https://www.i-techs.com/wireless-network-site-survey-heat-mapping/>

[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

380



## Life-Cycle Management in Networking

Life-cycle management involves overseeing the **entire lifespan** of network equipment from acquisition to disposal.

This process ensures that networking infrastructure remains efficient, up-to-date, and secure throughout its operational life.

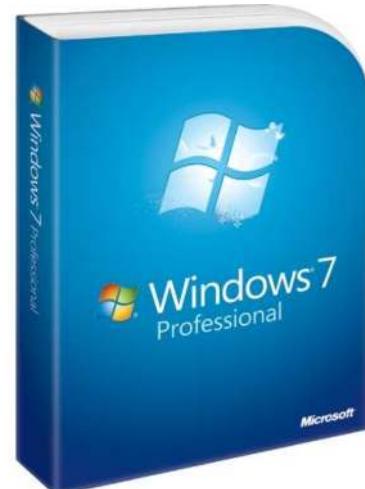


## CompTIA Network+ N10-009 Course Notes

# End-of-Life (EOL)

End-of-Life (EOL) refers to the point when a product is **no longer produced**, or sold, by the manufacturer.

Understanding and planning for EOL is critical to **avoid operational risks** and ensure that replacement strategies are in place before support and updates are unavailable.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

382



## CompTIA Network+ N10-009 Course Notes

# End-of-Support (EOS)

End-of-Support (EOS) marks the date when a manufacturer stops providing technical support and software updates for a product.

Planning for EOS is essential to maintain network security and functionality, as lack of updates can expose the network to vulnerabilities and compatibility issues.





## CompTIA Network+ N10-009 Course Notes

# Software Management in Network Lifecycle

Software management is a critical aspect of lifecycle management, focusing on maintaining, updating, and optimizing software across network devices.

**Effective software management** ensures that systems remain secure, functional, and in compliance with industry standards.



## CompTIA Network+ N10-009 Course Notes

# Patches and Bug Fixes

Regular application of patches and bug fixes is essential to address vulnerabilities, improve functionality, and prevent potential security breaches.

A **structured patch management strategy** helps in timely deployment across the network, minimizing disruption and protecting against emerging threats.



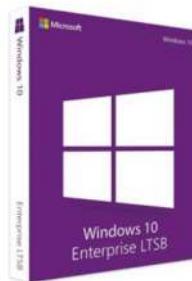


## CompTIA Network+ N10-009 Course Notes

# Operating System (OS) Management

Operating system management involves **regular updates and maintenance** to ensure network devices operate efficiently and securely.

OS updates can include security enhancements, new features, and performance improvements, which are vital for the stability and security of the network.





## CompTIA Network+ N10-009 Course Notes

# Firmware Updates

Firmware within network devices controls basic hardware functions and requires updates to fix bugs, close security vulnerabilities, and sometimes enhance device capabilities.

Managing firmware updates is crucial for the hardware's reliability and performance, **requiring careful scheduling** to avoid operational interruptions.





# Decommissioning of Network Assets

Decommissioning involves the **safe removal and disposal** of outdated or unnecessary network equipment.

This process should ensure data is **securely erased** and hardware is disposed of in an environmentally friendly manner, following **legal and regulatory guidelines** to mitigate risks associated with data breaches and environmental impact.





# Change Management in Networking

**Change management** is a **systematic approach** to handling all changes made to a network's configuration and its environment, ensuring that **standardized methods** and procedures are used for efficient and prompt handling of all changes.

It minimizes the impact of change-related incidents upon service quality, and consequently **improves the day-to-day operations of the organization**.



# Request Process Tracking/Service Request

The request process tracking, or service request management, is a key component of change management that involves logging, progressing, and analyzing change requests to ensure they are carried out **effectively and efficiently**.

This system helps in **maintaining control and documentation** throughout the lifecycle of a change, from initiation and approval to implementation and review, **ensuring that all changes meet the specified requirements** and are aligned with business objectives.



## CompTIA Network+ N10-009 Course Notes

# Configuration Management

Configuration management in networking involves the **maintenance and control** of all hardware and software configurations within an IT infrastructure.

It ensures that the system **operates as intended** by maintaining consistency of performance and security settings across all network devices.





## Production Configuration

Production configuration refers to the settings and setups that are **actively used** in the operational environment of the network.

It is critical to **regularly monitor and manage** these configurations to ensure optimal network performance and to quickly address any deviations or issues that arise.



## CompTIA Network+ N10-009 Course Notes

# Backup Configuration

Backup configuration involves **storing a copy** of the device configurations to **prevent data loss** in case of hardware failure, software issues, or other disruptions.

**Regular updates and testing** of backup configurations are essential to ensure they can be effectively restored when needed, providing continuity and reducing downtime.





## CompTIA Network+ N10-009 Course Notes

# Baseline/Golden Configuration

A baseline or golden configuration is a **template of approved settings** and configurations that serves as a standard for deploying new devices or restoring existing ones.

This **standardized approach** helps in maintaining consistency, security, and manageability across the network, simplifying troubleshooting and expansions.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

394



## CompTIA Network+ N10-009 Course Notes

# Lesson 15

## Network Monitoring Technologies



## CompTIA Network+ N10-009 Course Notes

# Simple Network Management Protocol

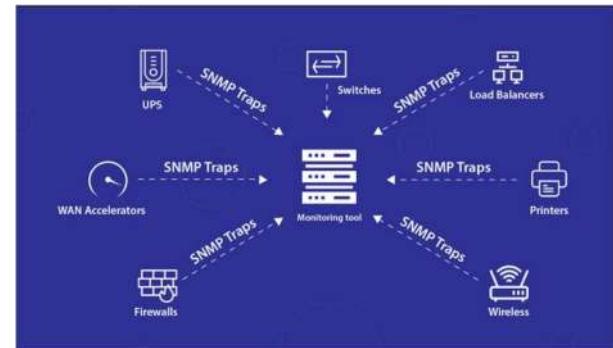
SNMP is a widely used protocol for **network management**, allowing administrators to monitor, configure, and control network devices.

It operates at the application layer of the OSI model, providing a **standardized framework** for managing devices in a network.



## SNMP Traps

SNMP traps are unsolicited messages sent from an SNMP-enabled device to a management station, **notifying** it of significant events or conditions.

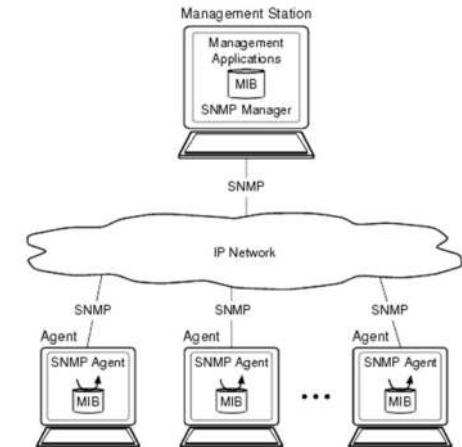


<https://www.site24x7.com/blog/complement-your-network-monitoring-with-snmp-traps>



## Management Information Bases (MIBs)

MIBs contain information about network devices, such as their status, capacity, and performance, in the form of data objects.





## CompTIA Network+ N10-009 Course Notes

# SNMP v2c and V3

- **SNMP v2c** (Simple Network Management Protocol version 2 community-based) is an **extension of the original** SNMP protocol, offering enhancements like bulk retrieval capabilities.
  - It lacks robust security features, relying on plain text community strings for authentication.
- **SNMP v3** is the **most secure version** of the Simple Network Management Protocol, providing important security enhancements over its predecessors.
  - It supports strong authentication and encryption, significantly improving the security of network management operations.



## CompTIA Network+ N10-009 Course Notes

# Community Strings in SNMP

Community strings grants access to device's information. There are two common community strings that are used

- Public: which mainly provides read-only access and
- Private: which generally provides read-write access.

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#

Router(config)#snmp-server community public RO

Router(config)#snmp-server community private RW



# Authentication in SNMP v3

**SNMP v3 enhances security** through robust authentication mechanisms that verify the identity of the source and destination before allowing access to network data.



## CompTIA Network+ N10-009 Course Notes

# Flow Data

Flow data involves **capturing and analyzing** metadata about network traffic, such as source and destination IP addresses, port numbers, and protocol types.

It is essential for understanding traffic patterns, bandwidth usage, and for identifying potential security threats or bottlenecks within the network.

The screenshot shows a Wireshark interface with several network frames listed. Frame 343 is selected, showing details like Source (172.17.0.1), Destination (172.17.249.22), Protocol (TCP), Length (40), and Info (HTTP ACK). The packet bytes are shown in hex and ASCII. Below the frame details, there is a summary of the flow, including Source (172.17.0.1), Destination (172.17.249.22), Protocol (HTTP), and various statistics like bytes transferred (40B), round trip time (RTT) (0.000ms), and jitter (0.000ms). A detailed description of the flow is provided, mentioning a POST request to /index.php?route=product/product&product\_id=100&category\_id=100&language\_id=1 and a response with status code 200 OK.

[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

402

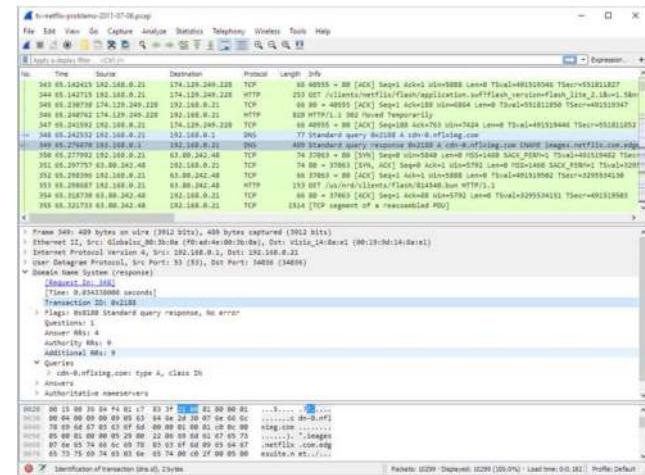


## CompTIA Network+ N10-009 Course Notes

# Packet Capture

Packet capture (pcap) is the process of **intercepting and logging** traffic that passes over a digital network.

As a diagnostic tool, packet capture helps network administrators to thoroughly **examine network traffic** to diagnose performance issues and detect malicious activities.





## Baseline Metrics

**Baseline metrics** establish a **standard level of normal network performance**, including typical traffic volume, performance speeds, and error rates.

Establishing these metrics is crucial for effective network management as it aids in the **early detection of issues** and ensures network performance remains within expected parameters.



## Anomaly Alerting/Notification

Anomaly alerting and notification systems are designed to **automatically detect and report deviations** from baseline metrics, signaling potential performance or security issues.

These systems help ensure **rapid response** to unusual activity, maintaining network integrity and performance by prompting timely intervention.



## CompTIA Network+ N10-009 Course Notes

# Log Aggregation

**Log aggregation** is the process of **collecting, consolidating, and analyzing** computer-generated log messages from various sources across the network.

This **centralized approach** helps in monitoring, diagnosing, and managing data to ensure efficient network operations and security compliance.

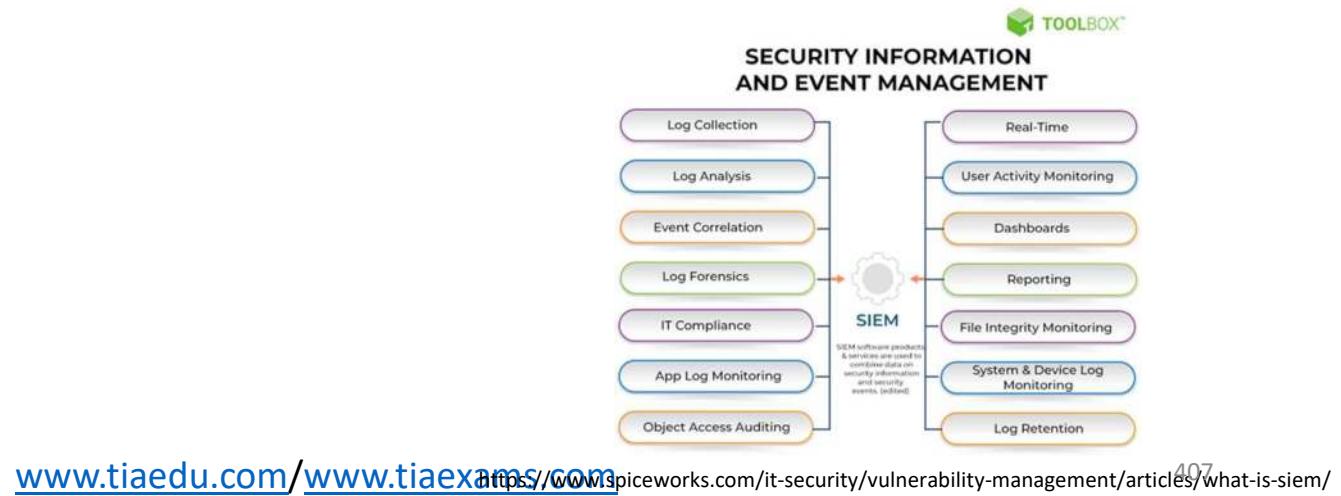
**splunk>**<sup>®</sup>



# Security Information and Event Management

SIEM technology provides **real-time analysis** of security alerts generated by network hardware and applications.

It **aggregates and correlates** log data, enabling automated alerting and reporting, and supports proactive security measures by identifying potential threats based on unusual activity patterns.





## Syslog Collector

A syslog collector is a dedicated tool used for **gathering log data** generated by devices within a network.

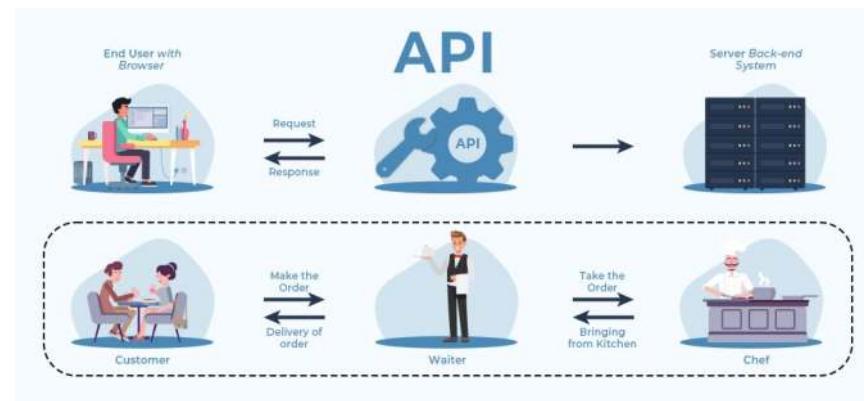
It plays a critical role in log aggregation by **centralizing syslog messages** from multiple sources, which simplifies management, enhances security monitoring, and aids in troubleshooting.



## API Integration

Application Programming Interfaces (APIs) are used in network management to allow **seamless integration** between different software systems.

APIs facilitate automated network configurations, data extraction, and the synchronization of network management tools, enhancing efficiency and scalability.



<https://www.geeksforgeeks.org/what-is-an-api/>



## CompTIA Network+ N10-009 Course Notes

# Network Solutions

Network solutions encompass various tools and techniques used to manage, monitor, and secure the network infrastructure.

They **ensure optimal network performance**, security, and reliability through continuous oversight and proactive management.



## Network Discovery

Network discovery involves **identifying** devices, servers, and other hardware components connected to a network.

Ad hoc network discovery is performed **manually on an as-needed basis**, providing immediate visibility into the network when specific issues or updates arise.

Scheduled network discovery is automated and **occurs at regular intervals**, ensuring consistent and up-to-date network mapping.

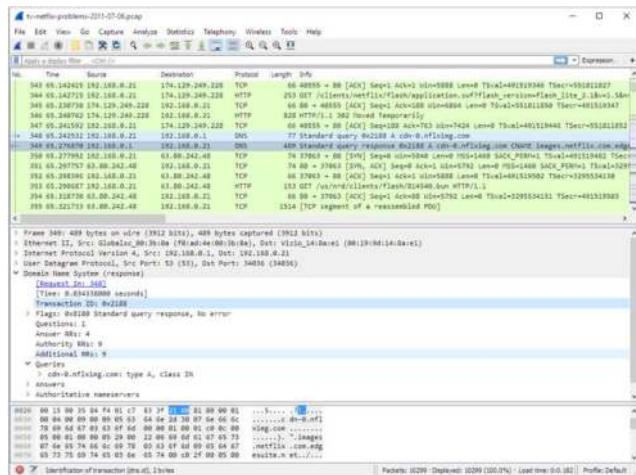


## CompTIA Network+ N10-009 Course Notes

# Traffic Analysis

Traffic analysis involves examining the data packets flowing through the network to identify usage patterns, bandwidth consumption, and potential bottlenecks.

It provides insights that help optimize network performance and ensure adequate bandwidth distribution.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

412



# Monitoring

Performance monitoring tracks various metrics such as response times, throughput rates, and error rates to **evaluate the health and efficiency of the network**.

Availability monitoring ensures that all critical network components are **operational** and **accessible** to users.

- It detects **downtime and failures**, helping network teams to quickly address issues and minimize service disruptions.

Configuration monitoring involves **tracking changes** to network device configurations to prevent unauthorized modifications and ensure compliance with security policies.



## CompTIA Network+ N10-009 Course Notes

# Lesson 16

## Disaster Recovery (DR) Concepts



## Recovery Point Objective

RPO is the maximum acceptable amount of data loss **measured in time** before a disaster occurs.

It determines the **maximum age of files** that must be recovered from backup storage for normal operations to resume without **significant losses**.

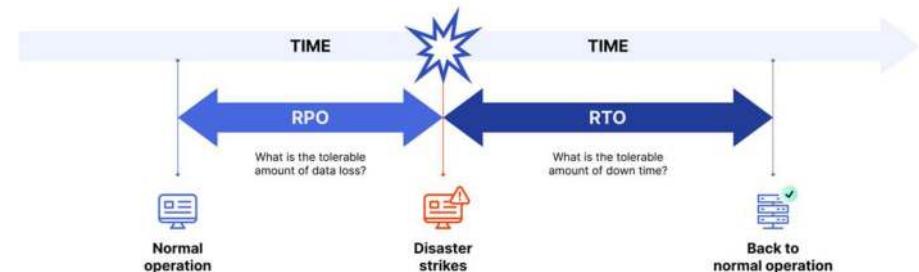


## CompTIA Network+ N10-009 Course Notes

# Recovery Time Objective

RTO is the targeted **duration of time** and a service level within which a **business process must be restored** after a disaster or disruption to **avoid unacceptable consequences** associated with a break in business continuity.

RTO is the time that you set to recover the lost data.



<https://www.altis-dxp.com/rpo-vs-rto-understanding-disaster-recovery/>



## Mean Time Between Failure (MTBF)

**MTBF** is the **calculated average time between failures of a system** or component during its operational lifespan.

A higher **MTBF** suggests greater **reliability** and **stability** of the network component or system.



## CompTIA Network+ N10-009 Course Notes

# Mean Time to Repair

**MTTR** is the **average time required to repair a failed component** or device and return it to normal operations.

It measures the **efficiency** of the repair process, with a lower **MTTR** indicating more efficient fault recovery.



## Recovery Sites

- **Cold Sites** are the most affordable but take the most time to recover
  - Contains no equipment, connections, or data
  - Days to weeks to recover
- **Warm Sites** are more expensive than cold sites but offer faster recovery
  - Contains some equipment, and connections, but out of date configurations and data sets
  - Hours to days to recover
- **Hot Sites** are the most expensive but offer the fastest recovery time
  - Contacts all equipment, connections, and recent configurations and data sets
  - Minutes to hours to recover





## Active-Active vs. Active-Passive

In an active-active configuration, **both systems run simultaneously**, distributing the load to maximize performance and availability.

In an active-passive setup, **one system is operational while the other stands by**, ready to take over in case the primary system fails, ensuring continuity but with potential downtime during the switchover.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

420



## Disaster Recovery Testing

**Testing** is a critical component of disaster recovery planning, ensuring that recovery procedures are **effective and up-to-date**.

Regular **testing** helps organizations **prepare for and manage** potential disruptions, minimizing downtime and data loss during actual disaster scenarios.



## CompTIA Network+ N10-009 Course Notes

# Tabletop Exercises

Tabletop exercises are discussion-based sessions where team members walk through various disaster scenarios to **evaluate the effectiveness of the disaster recovery plan**.

These exercises help **identify gaps** in the recovery plan and enhance the preparedness of the team by simulating decision-making processes **without activating actual resources**.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

422



## Validation Tests

Validation tests involve the **actual execution of the disaster recovery processes** to verify that systems and data can be restored in accordance with the recovery objectives.

These tests are crucial for confirming the practical applicability of the disaster recovery plan and for training staff on their roles during recovery operations.





## CompTIA Network+ N10-009 Course Notes

# Lesson 17

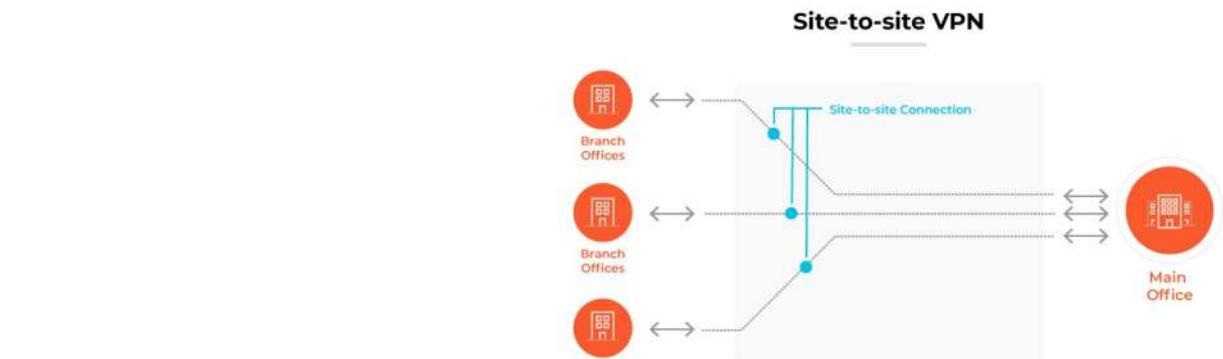
## Network Access



## Site-to-Site VPN

A Site-to-Site VPN connects entire networks to each other, allowing branches or remote offices to communicate securely over the internet as if they were within the same local network.

This type of VPN is commonly used to connect **geographically dispersed** offices of an organization, enabling secure and private communications using encrypted tunnels over public networks.

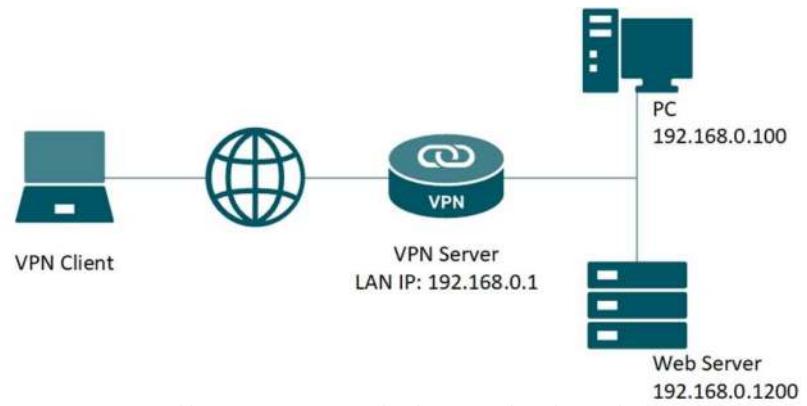




## Client-to-Site VPN

Client-to-Site VPN, also known as Remote Access VPN, allows individual clients (such as employees working remotely) to **connect to the corporate network securely over the internet**.

It provides users with **secure access** to network resources and applications as if they were physically on the network, typically using VPN client software.



<https://www.tp-link.com/us/support/faq/3044/>



## CompTIA Network+ N10-009 Course Notes

# Clientless VPN

A Clientless VPN allows users to securely access network resources **through a web browser** without the need for installing dedicated VPN client software.

This type of VPN is useful for providing access to specific applications or services and is often utilized for secure, remote access to web applications and internal networks.



<https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/913943/ssl-vpn-custom-landing-page>



## CompTIA Network+ N10-009 Course Notes

# Split Tunnel vs. Full Tunnel VPN

**Split Tunnel VPN:** In a split tunnel configuration, **only network traffic for the corporate site** passes through the VPN tunnel, while other traffic accesses the internet directly.

This can reduce the load on the VPN gateway but may expose the traffic to security risks.

**Full Tunnel VPN:** With a full tunnel configuration, **all of the client's internet traffic** is routed through the VPN to the corporate network.

This **increases security** as all traffic is encrypted but can lead to **higher bandwidth usage and slower performance**.



## CompTIA Network+ N10-009 Course Notes

# Connection Methods

Various connection methods are utilized to interact with network devices and systems, each serving **specific purposes** from configuration and management to troubleshooting.



# Graphical User Interface (GUI)

A GUI provides a **visual interface** to interact with a computer or network device, making it accessible for users who prefer point-and-click interactions over command-line interfaces.

GUIs are commonly used in network management software, providing dashboards, configuration menus, and monitoring tools that simplify complex processes.



## CompTIA Network+ N10-009 Course Notes

# Console Connection

Console connections provide direct, physical access to network devices through a **console port**, typically using a **cable and a terminal emulator**.

This method is essential for initial device setup, recovery, and troubleshooting when **remote access is not possible** or the device is not yet configured for network connectivity.

```
Router# show version
Cisco Internetwork Operating System Software
IOS # 4500 Software (C4500-J-M), [Version 11.2(13)], RELEASE SOFTWARE (fc1)
Copyright © 1986-1998 by cisco Systems, Inc.
Compiled Tue 31-Mar-98 13:18 by tlane
System image version
Image text-base: 0x600088A0, data-base: 0x607BC000
ROM version
ROM: System Bootstrap, [Version 5.1(1)] daveu 1], RELEASE SOFTWARE (fc1)
Router uptime is 1 hour, 37 minutes
System restarted by power-on
Elapsed time since
last restart, and
cause of that restart
System image file is "flash:c4500img", booted via flash
Running default software
Shared memory
cisco 4500 (R4K) processor (revision 0x00) with 32768K/4096K bytes of memory.
Processor board ID 02152924
R4600 processor, Implementation 32, Revision 2.0
G.703/E1 software, Version 1.0.
Bridging software.
Main memory
SuperLAT software copyright 1990 by Meridian Technology Corp.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
TM3270 Emulation software.
Interface hardware
2 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface[2]
recognized by software
128K bytes of non-volatile configuration memory.
4096K bytes of processor board System flash (Read/Write)
4096K bytes of processor board Boot flash (Read/Write)
Configuration register is 0x2102
```



## CompTIA Network+ N10-009 Course Notes

# SSH (Secure Shell)

SSH is a **cryptographic network protocol** for secure remote login and other secure network services over an unsecured network.

It provides a **secure channel** over an **insecure network**, replacing older protocols like Telnet that do not encrypt communications, and is widely used for managing servers and network devices remotely.

The screenshot shows a PuTTY terminal window titled "192.168.1.1 - PuTTY". The command "root@192.168.1.1's password:" is displayed, followed by the busybox prompt: "busybox v1.4.2 (2007-08-27 09:18:59 CDT) built-in shell (ash)". Below this, the help command "Enter 'help' for a list of built-in commands." is shown. A decorative ASCII art menu follows, featuring a grid of squares and the text "W I R E L E S S F R E E D O M". At the bottom, a cocktail recipe for a "WHITE RUSSIAN" is listed: "Mix the Vodka and kahlua together", "1 oz Vodka", "1/2 oz Kahlua", "over ice", "then Float the cream on top", and "1/2oz cream". The root prompt "root@00c1260b04c0:~\$" is at the bottom right.

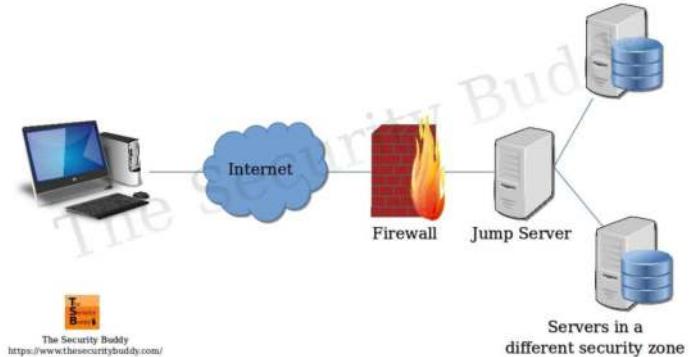


## CompTIA Network+ N10-009 Course Notes

# Jump Box/Host

A jump box, also known as a jump host, is a **secure computer** that all administrators first connect to before launching any administrative task or accessing more sensitive parts of the network.

It acts as a **stepping stone** from one security zone to another, providing a **controlled means of access** between different trust levels within or across network environments, often used to manage devices within a demilitarized zone (DMZ).



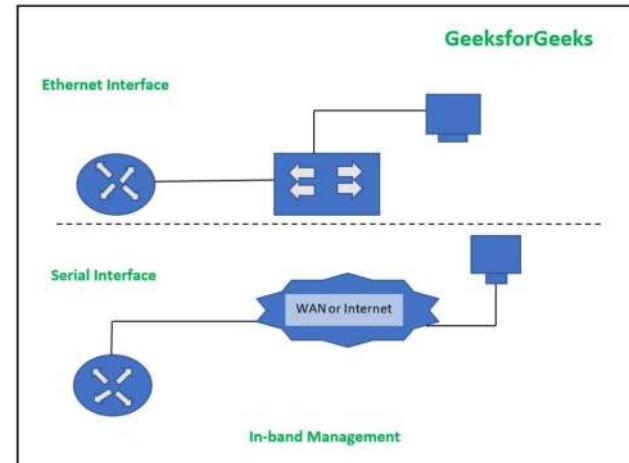


## CompTIA Network+ N10-009 Course Notes

# In-Band Management

In-band management involves administering network devices through the **same network connections and paths** used for normal data traffic.

This method allows network administrators to remotely manage devices using standard network tools and protocols, such as SSH.



<https://www.geeksforgeeks.org/compare-in-band-and-out-of-band-management-access/>

[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

434

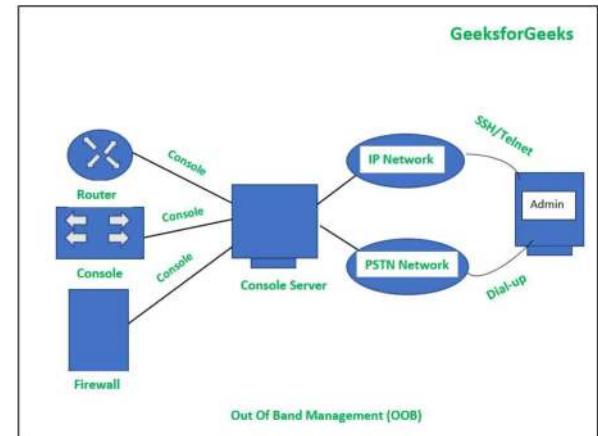


## CompTIA Network+ N10-009 Course Notes

# Out-of-Band Management

Out-of-Band management uses a **separate, dedicated channel** for device administration, independent of the primary network infrastructure.

This approach ensures access to network devices for monitoring, maintenance, and recovery **even when the main network is down**, providing a reliable alternative for critical management tasks that enhances security and uptime.



<https://www.geeksforgeeks.org/compare-in-band-and-out-of-band-management-access/>



## CompTIA Network+ N10-009 Course Notes

# Lesson 18

## Logical Security



## Logical Security

Logical security encompasses measures and protocols implemented in software to protect data, network resources, and systems from **unauthorized access and attacks**.



CompTIA Network+ N10-009 Course Notes

# CIA Triad





# CIA Triad

- Confidentiality: Ensuring that sensitive information is accessed only by an authorized person and kept away from those not authorized to possess it.
- Integrity: Assuring the accuracy and reliability of information and systems. Checks if data or systems has been altered
- Availability: Ensuring that data and resources are available to authorized users when needed.



## CompTIA Network+ N10-009 Course Notes

# Confidentiality

- Confidentiality refers to the measures taken to ensure that sensitive information is not disclosed to unauthorized individuals, entities, or processes.
- Involves preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Here's a breakdown of what this entails:
  - **Access Controls:** Mechanisms such as passwords, biometric verification, or access cards that limit resource access to authorized personnel to prevent unauthorized access to information.
  - **Encryption:** The process of encoding information in such a way that only authorized parties can read it. If an unauthorized party intercepts the encrypted data, they will not be able to interpret it without the encryption key.



## CompTIA Network+ N10-009 Course Notes

# Confidentiality

- **Secure Communication:** Using secure protocols like SSL/TLS for transmitting data to prevent interception by unauthorized entities.
- **Policies and Procedures:** Establishing guidelines for who has access to information and under what conditions, and what the protocols are for handling and sharing that information.
- **Training and Awareness:** Educating employees and users about the importance of confidentiality and how to ensure it is maintained.
- **Data Classification:** Categorizing data based on its level of sensitivity and the impact to the organization if it is disclosed or improperly accessed.



# Integrity

- Integrity refers to the trustworthiness and veracity of data or resources.
- It is about protecting data from unauthorized changes to ensure that it is reliable and correct.
- Here are key aspects of integrity within IT security:
  - Data Accuracy
  - Data Consistency
  - Data Trustworthiness



# Integrity

- Various methods and mechanisms are used, such as:
- Checksums and Cryptographic Hash Functions: These are algorithms that produce a short, fixed-size bit string from arbitrary-length strings of data. If the data changes, so will the hash value, which can be used to detect changes or corruption.
- Digital Signatures: Provide a means to verify that a message, document, or other data file comes from a specific entity and has not been altered.
- Access Controls: Limit data access to authorized users to prevent unauthorized modifications.



# Availability

- Availability refers to ensuring that data, systems, and services are accessible to authorized users when needed,
- Here's how availability is maintained in IT:
  - Redundancy: Creating multiple copies of data or system components that can take over in case of a failure.
  - Fault Tolerance: Building systems that can continue operating properly even if some of their components fail.
  - Backup Systems: Regularly backing up data and systems to enable recovery in case of data loss or corruption.



# Availability

- Disaster Recovery Plans: Having a plan in place to recover from significant adverse events, such as natural disasters, power outages, or cyberattacks.
- The goal of ensuring availability is to prevent service disruptions due to system failures, infrastructure problems, or malicious attacks like Distributed Denial of Service (DDoS).



## CompTIA Network+ N10-009 Course Notes

### Risk

The probability of a threat  
exploiting a vulnerability

$$\text{Risk} = \text{Threat} * \text{Vulnerability}$$



## CompTIA Network+ N10-009 Course Notes

# Risk

- **Asset**
  - Anything within an environment that should be protected.
- **Asset Valuation**
  - A dollar value assigned to an asset based on actual cost and nonmonetary expenses.
- **Threats**
  - Any potential occurrence that may harm the asset.
- **Threat Agent / Actors**
  - People, programs, hardware, or systems that use threats to cause harm
- **Threat Events**
  - Threat events are occurrences that lead to the exploitations of vulnerabilities.
- **Threat Vector**
  - A threat vector or attack vector is the path or means by which an attack or attacker can gain access to a target in order to cause harm



## CompTIA Network+ N10-009 Course Notes

# Risk

- **Vulnerabilities**
  - The weakness in an asset or the absence or the weakness of a safeguard or countermeasure that could be exploited.
- **Exposure**
  - Actual or anticipated damage from a threat.
- **Safeguards**
  - Anything that removes or reduces a risk
- **Attack**
  - The threat exploiting the vulnerability
- **Breach**
  - The occurrence of a security mechanism being bypassed or thwarted by a threat agent.



- **Authentication:** This is the process of verifying the identity of a user, device, or other entity in a computer system, typically as a prerequisite to granting access to resources in a system.
- **Authorization:** Once a user is authenticated, the authorization process determines what that user is permitted to do by matching user or system credentials against an access control list.
- **Accounting (sometimes referred to as Auditing):** Accounting is ensured by keeping a track of activities. It involves the logging and monitoring of user actions



# Authentication

- Verifying the identity of a user, device, or other entity in a system, usually as a prerequisite for accessing resources in that system.
  - Comes after identification



## CompTIA Network+ N10-009 Course Notes

# Multifactor Authentication

MFA is a security system that requires **more than one method of authentication** from independent categories of credentials to verify the user's identity for a login or other transaction.

This approach combines **two or more distinct authentication factors**, significantly increasing security.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

451



## CompTIA Network+ N10-009 Course Notes

# MFA (Authentication Factors)

Something You Know: Commonly used but **vulnerable to theft or guessing or brute force.**

Examples: Passwords, PINs, answers to security questions.

Something You Have: Adds a layer of security by **requiring a physical device** in possession of the user.

Examples: Mobile devices with authentication apps, smart cards, security tokens.

Something You Are: **Highly secure**, but implementation can be **complex and costly**.

Examples: Biometric verification methods.

Somewhere You Are (Location-Based Authentication): Adds **contextual security** by restricting access to specific locations.

Examples: Authentication based on the user's geographic location, using GPS or network-based methods.



## CompTIA Network+ N10-009 Course Notes

# Authentication

- **Factors of Authentication:**
  - **Something you know:** This involves verifying identity based on knowledge of something confidential, such as a password, PIN, or answers to secret questions.
  - **Something you have:** This involves items in your possession that can be used to verify your identity, such as security tokens, smart cards, or a mobile phone (used for receiving OTPs or push notifications).
  - **Something you are:** This refers to biometrics - unique physical characteristics such as fingerprints, facial recognition, iris scans, or voice patterns.
  - **Somewhere you are:** Authentication can also be based on the user's location, which can be determined through IP addresses, GPS, or other geolocation methods.
  - **Something you do:** Behavioral biometrics such as keystroke dynamics or mouse use patterns can also be used to authenticate a user.



# Authentication

- **Multiple Factor Authentication (MFA):**
  - Is a security process that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.
  - MFA combines two or more independent credentials: what the user knows (password), what the user has (security token), and what the user is (biometric verification).



## CompTIA Network+ N10-009 Course Notes

# Authentication

- Authenticating People can be done using:
  - **Biometrics:** Utilizing physical characteristics (e.g., fingerprints, facial recognition, retina scans) unique to an individual.
  - **Knowledge-Based Authentication:** Requiring information only the user should know (e.g., passwords, PINs, security questions).
  - **Multiple Factor Authentication (MFA):** Combining something the user knows (password) with something they have (a phone or token) or are (biometric verification).
- Authenticating Systems can be done using:
  - **Certificates and Keys:** Using digital certificates and cryptographic keys to establish trust between machines.
  - **IP Allow list:** Allowing only systems with certain IP addresses to access a service or network.
  - **MAC Address Filtering:** Restricting access to a network to devices with specific MAC addresses.



# Authorization

- **Authorization determines what that user is allowed to do by establishing their rights and privileges.**
- **Can be done using:**
  - Permissions and Privileges: It involves granting permissions to access specific resources or data. Permissions define the actions permitted, such as read, write, execute, delete, or modify.
  - Access Control: Authorization is enforced through access control mechanisms such as an Access control lists (ACLs).
  - Authorization Models such as Mandatory Access Control (MAC) or Discretionary Access Control (DAC).



## CompTIA Network+ N10-009 Course Notes

# Identity and Access Management (IAM)

**Identity and Access Management (IAM)** is a **framework of business processes**, policies, and technologies that facilitates the management of electronic or digital identities.

By **controlling user access** to critical information within an organization, **IAM** systems ensure that the right people access the right resources at the right times for the right reasons.

This system is crucial for security and regulatory **compliance**, offering tools for automating user provisioning, managing privileges, enforcing security policies, and auditing user activities across the network.



## CompTIA Network+ N10-009 Course Notes

# Access Controls

Access controls are mechanisms and policies used to **manage and restrict access to resources in an information system**.

Various types of access controls include DAC, MAC, RBAC, and ABAC, each with its specific **use cases and implications** for security and compliance.

The effective implementation of access controls requires **balancing security, complexity, and usability**, and is a vital part of any comprehensive cybersecurity strategy.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

458



## CompTIA Network+ N10-009 Course Notes

# Access Controls (DAC and MAC)

### Mandatory Access Control (MAC):

MAC is a security model in which access rights are regulated by a **central authority** based on different levels of security clearance.

Use Case: Common in **government and military** systems where classified information is involved.

Key Aspect: Users cannot change access permissions; they are set and enforced by a system **administrator**.

### Discretionary Access Control (DAC):

In DAC, the **resource owner** decides on access levels. It is the most flexible access control model.

Use Case: Used in environments where **users** need control over the resources they own, like setting file permissions in an operating system.

Key Aspect: Risk of **users granting excessive access**, potentially leading to security breaches.



## CompTIA Network+ N10-009 Course Notes

# Access Controls (RBAC)

**RBAC (Role-Based Access Control):**  
assigns permissions based on a user's **role** within an organization.

Use Case: **Common in corporate environments** where roles define job functions and access needs.

Key Aspect: **Streamlines access management**, especially in organizations with many users and roles.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

460



# Access Controls

## Rule-Based Access Control:

Access decisions are **based on a set of rules defined by the system administrator**.

Use Case: Useful in environments requiring **stringent access control**, like securing network resources.

Key Aspect: Rules can be based on various criteria, such as source/destination IP addresses in firewalls.

## ABAC (Attribute-Based Access Control):

uses policies that **evaluate attributes** (or characteristics) of users, the environment, and resources.

Use Case: Effective in **complex environments** with diverse and dynamic user attributes.

Key Aspect: Provides **fine-grained control**, allowing for more nuanced access decisions based on multiple factors.



## CompTIA Network+ N10-009 Course Notes

# Principle of Least Privilege

Refers to the practice of limiting access rights for users, accounts, and computing processes to only those resources absolutely required to perform their functions or tasks.

Dictates that individuals or systems should be granted the minimum levels of access – or permissions – necessary to perform their duties.

- Applications:
  - **User Access Control:** For employees, access to systems and data is restricted based on their job requirements. For example, a marketing employee may not need access to financial systems.
  - **Administrative Accounts:** System administrators may have accounts with extensive privileges for their job, but they should use accounts with standard privileges for routine, non-administrative tasks.
  - **Software and Processes:** Applications and services should also operate with the least privilege. They should have only the permissions necessary to function correctly, limiting their ability to access or modify system resources and data.



## Single Sign-On

**Single Sign-On** is a common feature where users **log in once** and gain **access to multiple systems** without the need to re-authenticate. This enhances user experience and productivity.





## SSO (Importance)

Reduced Password Fatigue: SSO reduces the number of passwords users must manage, **decreasing the likelihood of weak password practices**.

Centralized Authentication Control: Provides centralized control over user access to multiple systems, making it **easier to enforce security policies**.

Reduced IT Workload: **Simplifies the management of user accounts** and credentials, reducing the workload on IT departments.



## CompTIA Network+ N10-009 Course Notes

# LDAP

**LDAP** (Lightweight Directory Access Protocol) is a protocol for accessing and maintaining **distributed directory information services**, like user and group details, over an IP network.

Usage: Primarily used for directory services and information lookup. Commonly utilized for **storing user credentials and groups** in an enterprise environment.

The foundation for Microsoft Active Directory and used as Linux Open LDAP.



## Federation

Federation in cybersecurity is the process of **linking and managing identities** across different systems and organizational boundaries.

It enables users to use the same identity or set of credentials to **access multiple applications or services**.

It allows for single sign-on and **streamlined access management**, enhancing user experience and operational efficiency.

Federation involves identity providers, service providers, and specific protocols, and is crucial for **centralized authentication** and compliance.



## SAML

SAML (Security Assertion Markup Language) is an open standard for exchanging authentication and authorization data between parties, specifically **between an identity provider and a service provider**.

Usage: Widely used for SSO to allow users to log in to multiple applications with one set of credentials.

Characteristics: SAML uses XML for data exchange and is focused on both authentication and authorization. It's **particularly useful in enterprise-level SSO**.



# SAML (Key Components)

**Identity Providers (IdPs):** Services that **authenticate users** and provide identity information to service providers. Examples include Okta, Microsoft Azure AD, and Google Identity.

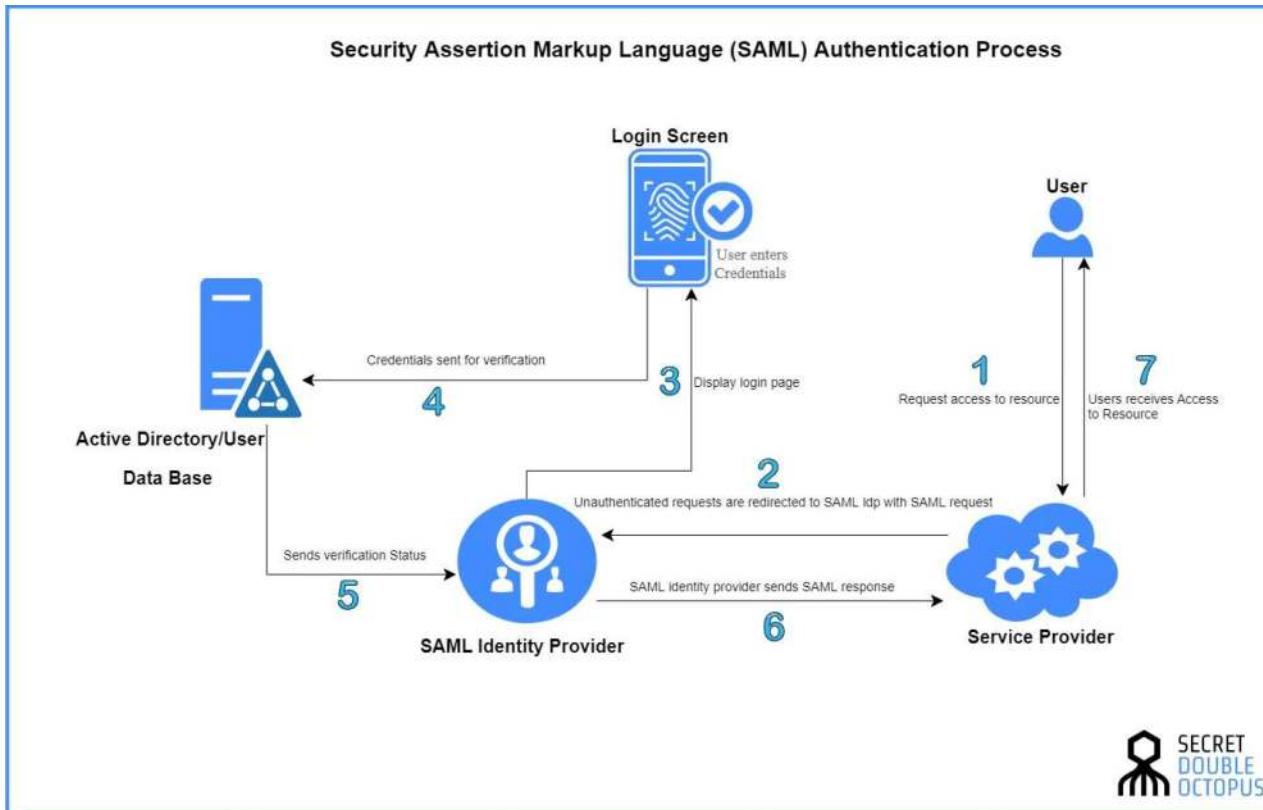
- Attestation (formal verification that something is true), is done by the IdPs. They attest that user is who they claim to be.

**Service Providers (SPs):** The applications or services that rely on information from the IdP to **provide access** to the user.



## CompTIA Network+ N10-009 Course Notes

# SAML



<https://frontegg.com/blog/implementing-saml-authentication-in-enterprise-saas-applications>



## OAuth

OAuth is an open standard for access delegation.

It is used to grant websites or applications access to their information on other websites but without giving them the passwords.

Usage: Commonly used for authorizing third-party applications to **access a user's data without exposing user credentials**.

Characteristics: OAuth is about **authorization** (not authentication) and is used to grant **limited access to an application** on behalf of the user.



## OpenID Connect

OpenID Connect is an identity layer on top of OAuth 2.0. It allows clients to verify the identity of the end-user based on the authentication performed by an **authorization server**.

Usage: Primarily used for authentication in **modern web applications** and **mobile applications**.

Characteristics: OpenID Connect extends OAuth 2.0 for use cases involving identity assertion.

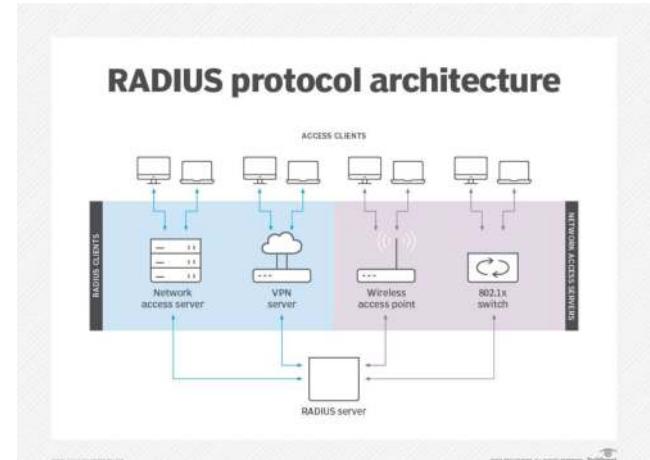


## CompTIA Network+ N10-009 Course Notes

### Remote Authentication Dial-In User Service/Terminal Access Controller Access-Control System Plus (TACACS+)

RADIUS or TACACS+ is a **networking protocol** that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service.

It is widely used by ISPs and enterprises to manage access to the network, keeping track of logging by users and ensuring their **credentials** are correct.





## CompTIA Network+ N10-009 Course Notes

# Time-based Authentication

Time-based Authentication involves the use of a **time-limited code** or token as part of the authentication process.

Typically used **in conjunction with a mobile app or token device**, this method generates a code that expires after a short duration and is required for successful authentication, **enhancing security by adding a temporal element** that reduces the window for unauthorized access.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

473



## Geofencing

Geofencing is a location-based service in which a software program uses GPS, RFID, Wi-Fi, or cellular data to **trigger a pre-programmed action** when a mobile device or RFID tag enters or exits a virtual boundary set up around a geographical location, known as a geofence.

Allows businesses to restrict access to secure areas, or monitor asset movement **within specified geographic zones**.



<https://www.areusdev.com/what-is-geo-fencing-and-why-so-many-companies-are-starting-to-use-its-advantages/>

474



## Physical Security

Physical security is crucial for protecting assets, personnel, and data from physical actions and events that could cause serious loss or damage.

This includes a variety of measures such as surveillance cameras, locking mechanisms, and access control systems to prevent unauthorized access and maintain safety.



## CompTIA Network+ N10-009 Course Notes

# Security Cameras

Security cameras play a vital role in physical security by providing real-time monitoring and recording of activities within and around facilities.

They **act as a deterrent** to unauthorized actions and can **provide crucial evidence** in the event of security breaches or incidents.





## CompTIA Network+ N10-009 Course Notes

# Locks

Locks are fundamental to securing entrances and sensitive areas within a facility, controlling who can enter specific spaces.

Modern security systems **integrate electronic locks with access control systems**, allowing for sophisticated management of entry permissions and tracking access history.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)



## Deception and Disruption Technology

Deception and Disruption Technology refers to a set of cybersecurity strategies and tools designed to **mislead, confuse, or disrupt the actions of malicious actors.**

These technologies are used to **create traps or illusions** that protect real network assets by diverting attackers to **decoy systems or files.**



## Honeypot

A honeypot is a security mechanism set up to **detect, deflect, or study hacking attempts.**

It acts as a decoy, imitating a real computer system, network, or information system, but is **isolated and monitored**.

Attackers engaging with a honeypot **provide valuable information** about their techniques and intentions without endangering the actual network.





## Honeynet

A honeynet is essentially a network of honeypots.

It simulates a network environment to attract attackers.

This setup is **more complex** and can provide **deeper insights** into how attackers interact with networks, what strategies they use, and how they move laterally within a network.



## Honeyfile

These are **decoy files** placed within a network's file system.

Honeyfiles are designed to **appear legitimate and contain attractive data**, but they are monitored for access.

Unauthorized access to a honeyfile can **alert security personnel** to a potential breach or insider threat.



## Honeytoken

Similar to a honeyfile, a honeytoken is a broader term that refers to **any decoy data or token inserted into a system**.

This could be a fake user account, database record, or any other type of digital bait that, if interacted with, indicates a compromise or unauthorized access.



## Audits and Regulatory Compliance

Audits and regulatory compliance are critical for ensuring that organizations adhere to **legal and industry standards** for data protection and security.

**Regular audits** help verify compliance, identify weaknesses, and implement improvements to safeguard sensitive information.



## CompTIA Network+ N10-009 Course Notes

# Data Locality

Data locality refers to the **geographical location** where data is stored, processed, and managed.

Compliance with **data locality regulations** ensures that data handling practices meet regional legal requirements,



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

484



## CompTIA Network+ N10-009 Course Notes

# Payment Card Industry Data Security Standards

PCI DSS is a set of security standards designed to ensure that all companies that accept, process, store, or transmit **credit card information** maintain a secure environment.

**Compliance** with PCI DSS involves implementing measures such as encryption, access controls, and regular monitoring to protect cardholder data from breaches and fraud.



## CompTIA Network+ N10-009 Course Notes

# General Data Protection Regulation (GDPR)

**GDPR** is a comprehensive data protection regulation that governs the processing and movement of personal data within the **European Union (EU)** and beyond.

It imposes **strict requirements** on organizations, including obtaining consent for data collection, ensuring data accuracy, implementing security measures, and providing individuals with rights over their data, such as access, correction, and deletion.



## Network Segmentation Enforcement

**Network segmentation enforcement** involves dividing a network into smaller segments or subnets to **improve security and performance**.

This strategy helps limit access to sensitive data, reduce the attack surface, and contain potential breaches within a segment.



## CompTIA Network+ N10-009 Course Notes

# Guest Network

Guest networks provide internet access to visitors **without exposing the main network** and its sensitive resources.

Implementing segmentation for guest networks helps maintain security and privacy by ensuring **guests cannot access internal systems and data**.





## BYOD Segmentation

Bring Your Own Device (BYOD) policies allow employees to use personal devices for work purposes, which can introduce **security risks**.

Segmentation of BYOD devices ensures they operate on a separate network segment, **limiting their access** to sensitive data and systems while providing necessary **connectivity for productivity**.





## CompTIA Network+ N10-009 Course Notes

# Industrial Control Systems

- **Industrial Control System (ICS)** is a general term that encompasses several types of systems used in industrial production
  - **Supervisory control and data acquisition (SCADA)** systems, distributed control systems (DCS), and other smaller control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures
  - ICSs are typically used in industries such as electrical, water, oil, gas, and data
  - Field devices control local operations such as
    - Opening and closing valves and breakers
    - Collecting data from sensor systems
    - Monitoring the local environment for alarm conditions



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

490



## CompTIA Network+ N10-009 Course Notes

# Internet of Things

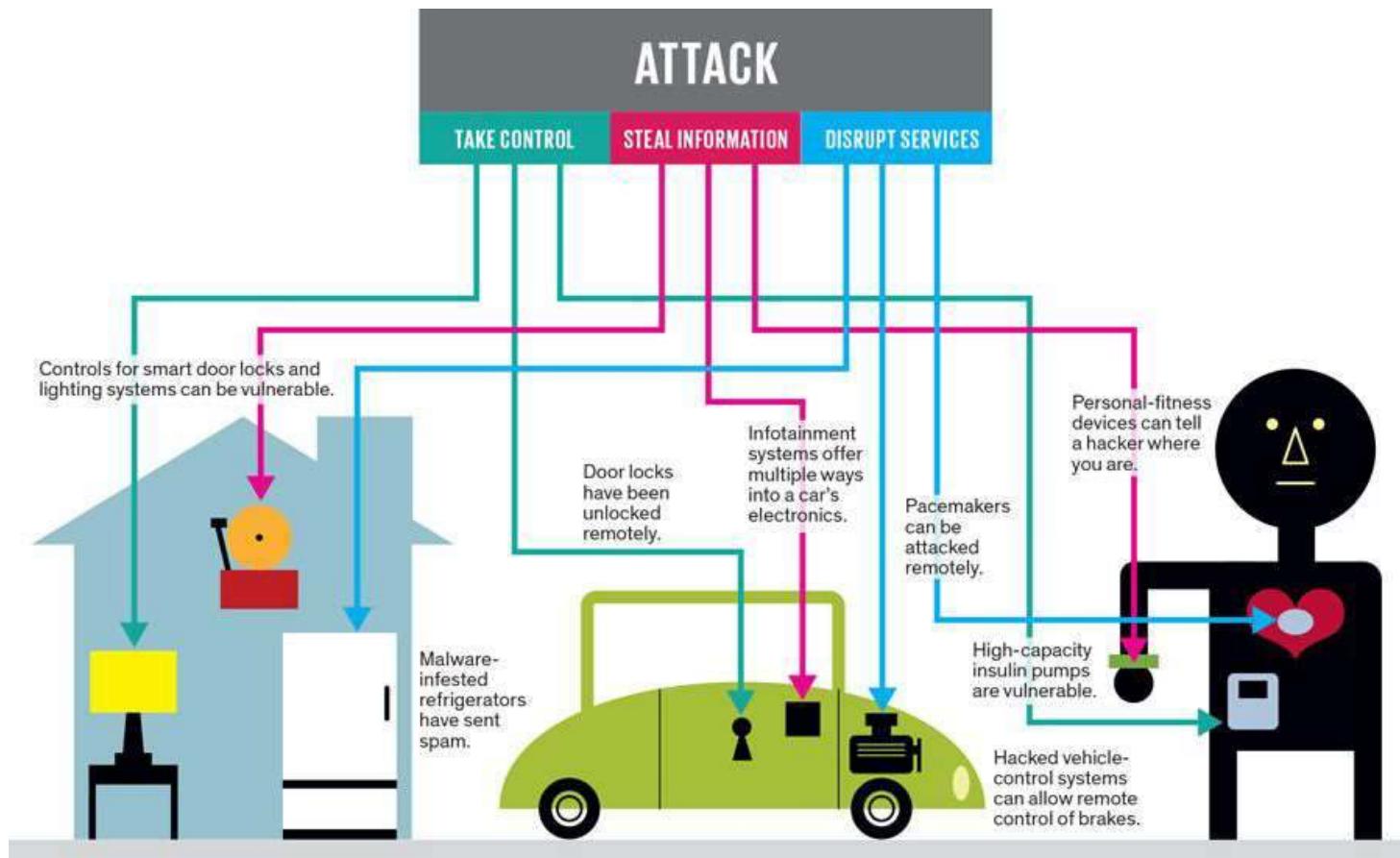
The Internet of Things (IoT) is the network of physical objects that traditionally do NOT require access to the internet. They provide home and office automation, remote control, monitoring, and other conveniences.

Embedded systems with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data

Includes house appliances, HVAC systems, A/V systems, cars, and can include almost any other device that requires electrical power.



# Internet of Things



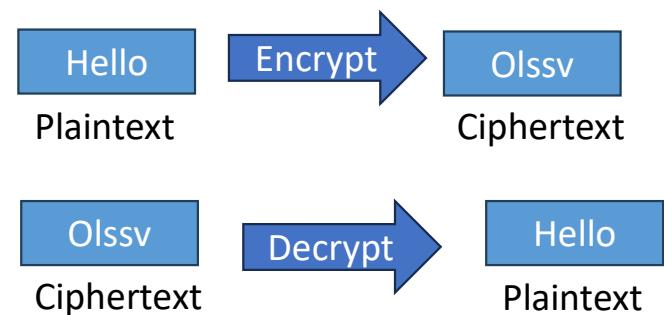


# Encryption in Logical Security

Encryption is a **fundamental component** of logical security, used to **convert readable data into a secure format** that can only be read or processed after it is decrypted.

This process is vital for protecting sensitive information from being accessed or understood by **unauthorized parties**.

Encryption requires the use of a **cryptographic key**: a set of mathematical values that both the sender and the recipient of an encrypted message agree on.





## CompTIA Network+ N10-009 Course Notes

# Encryption of Data in Transit

Data in transit refers to information that is being transferred over a network, from one device to another or across the internet.

Encrypting data in transit ensures that it remains secure and private while it moves between endpoints, protecting it from interception and tampering by malicious actors.

Common protocols include HTTPS, SSL/TLS, and VPN.



# Encryption of Data at Rest

Data at rest includes any data **stored on physical media**, from hard drives to USB drives, awaiting use or retrieval.

Encrypting data at rest prevents unauthorized access by ensuring that data is **only accessible via proper cryptographic keys**, safeguarding it against theft, loss, or unauthorized viewing.

Techniques include full disk encryption (FDE) and encrypted file systems.



## Goals of Cryptography

- **Confidentiality:** Ensuring that information is accessible only to those authorized to have access. Encryption plays a crucial role in maintaining confidentiality by converting readable data (plaintext) into a scrambled, unreadable format (ciphertext) that can only be converted back to its original form with the correct decryption key.
- **Integrity:** Guaranteeing that information is protected from unauthorized or accidental changes. Cryptographic hash functions, for example, are used to produce a unique hash value for data, which can be used later to verify that the data has not been altered.



## Goals of Cryptography

- **Authentication:** Verifying the identity of a user, device, or entity in a communication process. For example digital certificates are cryptographic techniques that can confirm the identity of the parties involved in a communication.
- **Non-repudiation:** Preventing an entity from denying their involvement in a transaction or activity. Digital signatures ensure that once a party signs a document or a message, they cannot later deny having signed it.



## Symmetric Encryption

- Symmetric Key Algorithms are a type of cryptographic algorithm that use the same key for both encryption and decryption.
- This shared key is used to convert plaintext (readable data) into ciphertext (encoded data) and vice versa.



## Symmetric Encryption

- **Key Sharing:** Since the same key is used for both encrypting and decrypting data, it must be shared and kept secret between the communicating parties. Securely distributing and managing this key is a crucial aspect of using symmetric cryptography.
- **Speed and Efficiency:** Symmetric key algorithms are generally faster and more efficient than asymmetric key algorithms, making them suitable for encrypting large amounts of data. This efficiency is due to simpler mathematical operations compared to asymmetric cryptography.



## CompTIA Network+ N10-009 Course Notes

# Symmetric Encryption

- **Applications:** Symmetric key algorithms are used in various applications like encrypting data for secure storage, securing data in transit (e.g., in VPNs or wireless networks), and for encrypting files and databases.
- **Key Management Challenges:** The major challenge with symmetric key cryptography is key management. Since the same key is used for encryption and decryption, it must be securely shared and stored, which can be challenging, especially in large networks or systems.
- **Security:** The strength of a symmetric cipher typically depends on the key length (longer keys are harder to crack due to increased possible combinations) and the security of the algorithm itself.



## CompTIA Network+ N10-009 Course Notes

# Symmetric Encryption

- **Symmetric key problems:**
- **Key Distribution and Management:** The biggest challenge with symmetric key cryptography is the secure distribution and management of the keys. Since the same key is used for both encryption and decryption, it must be shared among the communicating parties in a secure manner. If a key is intercepted or leaked during distribution, the security of the encrypted data is compromised.
- **Scalability Issues:** In a large network, the number of required keys can grow rapidly. For  $N$  users to communicate securely with each other,  $N(N-1)/2$  unique key pairs are needed. This exponential growth makes key management impractical in large systems or networks.



## Symmetric Encryption

- **Symmetric key problems:**
- **Key Storage and Protection:** Keys must be securely stored to prevent unauthorized access. If a key is stolen or exposed, an attacker can decrypt any data encrypted with that key. Secure key storage becomes more complex as the number of users in a system increases.
- **Lack of Non-repudiation:** Symmetric key cryptography does not provide non-repudiation since the same key is used by all parties. This means that it cannot be determined which specific user performed an encryption or decryption operation, which is a drawback in scenarios where proof of authorship is important.



## Asymmetric Encryption

- Asymmetric encryption, also known as public-key cryptography, is a cryptographic system that **uses pairs of keys**: a public key, which may be disseminated widely, and a private key, which is known only to the owner.
- Overview of asymmetric encryption:
  - Key Pairs:
    - Public Key: Can be used to encrypt and decrypt. Is **shared with anyone**.
    - Private Key: Can be used to encrypt and decrypt. Is **kept with the owner**.
  - Encryption and Decryption Process Example:
    - Encryption: A sender encrypts the data using the recipient's public key. Once encrypted, the data can only be decrypted by the corresponding private key.
    - Decryption: The recipient uses their private key to decrypt the data. Since only the recipient possesses the private key, the data remains secure.



## CompTIA Network+ N10-009 Course Notes

# Asymmetric Encryption

- Advantages:
  - Solves the **key distribution problem** of symmetric encryption, as public keys can be shared openly.
  - Provides a **method for digital signatures**, which is important for authentication and non-repudiation.
- Disadvantages:
  - More **computationally intensive** than symmetric encryption, making it slower for large amounts of data.
  - Requires **careful management of the private key**; if the private key is compromised, the security of the system is compromised.
- Asymmetric encryption is a cornerstone of modern internet security, providing a means to securely encrypt data and verify identities in a world where trusting communication channels is not always possible.



## CompTIA Network+ N10-009 Course Notes

# Public Key Infrastructure (PKI)

- A framework used to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
- The purpose of PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking, and confidential email.
- Functioning of PKI:
  - Encryption and Decryption: PKI allows users to encrypt and decrypt data using public and private keys.
  - Digital Signatures: PKI provides for the creation and verification of digital signatures, ensuring the authenticity and integrity of data.
  - Certificate Management: The CA issues and revokes certificates as needed. Certificates have a defined lifecycle and must be managed accordingly.



## CompTIA Network+ N10-009 Course Notes

# Public Key Infrastructure (PKI)

- X.509 Digital Certificates
  - X.509 Digital Certificates Attributes
    - Version number
    - Subject name
      - Common name
      - Distinguished name
    - Subject public key
    - Issuer name
    - Validity period
    - Signature algorithm ID
    - Serial number
  - Certificate Types
  - CA Certificate
    - Grants an organization the ability to be a certificate authority.
  - End Entity Certificates
    - Domain Validation (DV) certificate is issued if control of a domain is proven.
    - Extended Validation (EV) certificate is a higher level of assurance if the CA can verify that the applicant is a legitimate business.
  - Wildcard Certificates:
    - a wildcard certificate is a type of digital certificate used in SSL/TLS encryption, typically for securing websites.
    - It is a versatile SSL certificate that allows multiple subdomains of a single domain to be secured with a single certificate.
    - \*.tiaedu.com, \*.Microsoft.com



## CompTIA Network+ N10-009 Course Notes

# Public Key Infrastructure (PKI)

- Self Signed Vs. Third-party
  - Digital certificates can be either self-signed or issued by a third-party Certificate Authority (CA).
  - Self-Signed Certificates:
    - Creation: A self-signed certificate is created and signed by the entity it represents, rather than by a trusted third-party CA. Essentially, the creator vouches for itself.
    - Trust Level: These certificates are not inherently trusted by others, as there's no independent verification of the identity of the entity. Trust must be established out-of-band, meaning users must have a separate, secure way to verify the certificate's authenticity.
    - Use Cases: Often used in test environments, internal networks, or applications where the users can reliably verify the certificate's authenticity without needing an external CA. They are also common in situations where the overhead of obtaining a CA-signed certificate is not justified.
    - Cost: There's no cost associated with creating a self-signed certificate.



## CompTIA Network+ N10-009 Course Notes

# Public Key Infrastructure (PKI)

- Self Signed Vs. Third-party
  - Third-Party Certificates (CA-Signed Certificates):
    - Creation: A third-party certificate is issued and signed by a trusted CA. The CA verifies the identity of the entity requesting the certificate, ensuring that the entity is who it claims to be.
    - Trust Level: High. Because a trusted CA verifies the identity of the certificate holder, these certificates are inherently trusted by users and systems that trust the CA. This trust is central to most secure internet communications, like HTTPS.
    - Use Cases: Widely used on the public internet for websites, email servers, and other public-facing services where establishing trust with end-users is essential. CA-signed certificates are a cornerstone of secure online transactions and communications.
    - Cost: Obtaining a certificate from a CA typically involves a cost, which varies depending on the type of certificate and the level of validation provided by the CA.



## CompTIA Network+ N10-009 Course Notes

# Lesson 19

## Network Attacks



## CompTIA Network+ N10-009 Course Notes

# Malware

- Malware, short for malicious software, is any software intentionally designed to cause damage to a computer, server, client, or computer network.
- Malware is a critical threat that encompasses a range of harmful or intrusive software, including:
  - Viruses
  - Worms
  - trojan horses
  - Ransomware
  - Spyware
  - Keyloggers
  - Logic bomb
  - Rootkit



## Viruses

- A virus is a type of malicious software (malware) designed to spread to other computers.
- It typically attaches itself to legitimate software and executes its code when the host software runs
- **Propagation:** Unlike worms, which can spread across networks on their own, viruses usually require some form of user action to replicate, such as opening a file or running a program.



# Viruses

- **Infection Mechanisms:**
  - **File Infector Viruses:** These attach themselves to executable files and spread to other executables when the program is run.
  - **Macro Viruses:** These are written in the macro language of applications (like Microsoft Word) and are spread through documents.
  - **Boot Sector Viruses:** They infect the master boot record of a hard drive, ensuring they are executed when the computer boots up.
- **Detection and Removal:**
  - **Antivirus Software:** Uses signatures to detect known viruses and heuristics to detect new, unknown viruses.
  - **Regular Updates:** Keeping antivirus software updated with the latest virus definitions is crucial for protection.
  - **System Scans:** Regular scanning for viruses to detect and remove them from the system.



## Worm

- A worm is a type of malware that **replicates itself** in order to spread to other computers.
- Unlike a virus, it does not need to attach itself to an existing program or require user intervention to spread.
- Worms typically exploit vulnerabilities in network services to propagate across networks.





# Worm

- Here are several steps and measures that are typically taken:
  - Patch Management
  - Antivirus and Antimalware Solutions
  - Network Segmentation and Access Controls
  - Firewalls
  - Traffic Filtering
  - Disable Unnecessary Services
  - User Training and Awareness



## CompTIA Network+ N10-009 Course Notes

# Trojan

- Short for "Trojan horse," is a type of malware that disguises itself as legitimate software or is hidden within legitimate software.
- Named after the ancient Greek story of the deceptive wooden horse that led to the fall of the city of Troy.
- Trojan often tricks users into loading and executing it on their systems.





## CompTIA Network+ N10-009 Course Notes

# Trojan

- Here are several steps and measures that are typically taken:
  - Patch Management
  - Antivirus and Antimalware Solutions
  - Network Segmentation and Access Controls
  - Firewalls
  - Traffic Filtering
  - User Training and Awareness



## CompTIA Network+ N10-009 Course Notes

# Ransomware

- A type of malicious software designed to block access to a computer system or encrypt files until a sum of money is paid, typically in the form of cryptocurrency.
- It's a direct threat to the availability of data and the normal operation of businesses and personal computing use.
- **Ransomware Characteristics:**
  - Encryption
  - Payment Demand
- **Distribution Methods:**
  - Ransomware can spread through phishing emails, malicious web advertisements, and vulnerabilities in software and networks.



## CompTIA Network+ N10-009 Course Notes

# Ransomware





## CompTIA Network+ N10-009 Course Notes

# Ransomware

- Here are several steps and measures that are typically taken:
  - Patch Management
  - Antivirus and Antimalware Solutions
  - Network Segmentation and Access Controls
  - Firewalls
  - Traffic Filtering
  - User Training and Awareness
  - Data Backups



## CompTIA Network+ N10-009 Course Notes

# Ransomware

- A type of malicious software designed to block access to a computer system or encrypt files until a sum of money is paid, typically in the form of cryptocurrency.
- It's a direct threat to the availability of data and the normal operation of businesses and personal computing use.
- **Ransomware Characteristics:**
  - Encryption
  - Payment Demand
- **Distribution Methods:**
  - Ransomware can spread through phishing emails, malicious web advertisements, and vulnerabilities in software and networks.



## CompTIA Network+ N10-009 Course Notes

# Spyware

- A type of malware that is designed to gather data from a user or organization without their knowledge or consent.
- It can monitor and collect various types of personal and sensitive information, such as internet usage data, login credentials, and confidential information.
- Characteristics of Spyware:
  - Data Collection: It can log keystrokes, capture screen images, record browsing history, and access files.
  - Surveillance: Some spyware can activate cameras and microphones to surveil the physical environment.
  - Stealth: Spyware typically runs hidden in the background and may be disguised as legitimate software.
  - Communication: Collected data is usually transmitted to a third party, often a cybercriminal.



## CompTIA Network+ N10-009 Course Notes

# Spyware

- Here are several steps and measures that are typically taken:
  - Patch Management
  - Antivirus and Anti-Spyware Software
  - Secure Browsing Habits
  - Firewalls
  - Traffic Filtering
  - User Training and Awareness



## CompTIA Network+ N10-009 Course Notes

# Rootkit

- A rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence from administrators and other system users.
- Rootkits can be installed by a malicious intruder after gaining access to a system or can piggyback on other software installations.



## CompTIA Network+ N10-009 Course Notes

# Rootkit

- Here are several steps and measures that are typically taken:
  - Secure System Access
  - Antivirus and Anti-Rootkit Tools
  - System Hardening
  - Patch Management
  - Secure Boot:
    - Use hardware and software that supports secure boot processes to prevent unauthorized code from running during system startup.



## CompTIA Network+ N10-009 Course Notes

# Logic bomb

- A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.
- Unlike viruses, logic bombs do not replicate themselves.
- They are dormant until triggered by a specific event, such as a date/time, the launch of a program, the deletion of a user account, or a certain command.
- Characteristics of Logic Bombs:
  - Condition-based Trigger: They are activated by conditions written into the code.
  - Malicious Intent: Once activated, they perform destructive activities, such as deleting files or corrupting data.
  - Stealth: Logic bombs can be hard to detect as they lie dormant until triggered.
  - Insider Threat: Often, logic bombs are deployed by disgruntled employees with legitimate access to the system.



## CompTIA Network+ N10-009 Course Notes

### Logic bomb

- Here are several steps and measures that are typically taken:
  - Code Reviews and Auditing
  - Access Controls
  - Change Management
  - Regular Backups
  - Security Awareness Training
  - Antivirus and Antimalware Software



## CompTIA Network+ N10-009 Course Notes

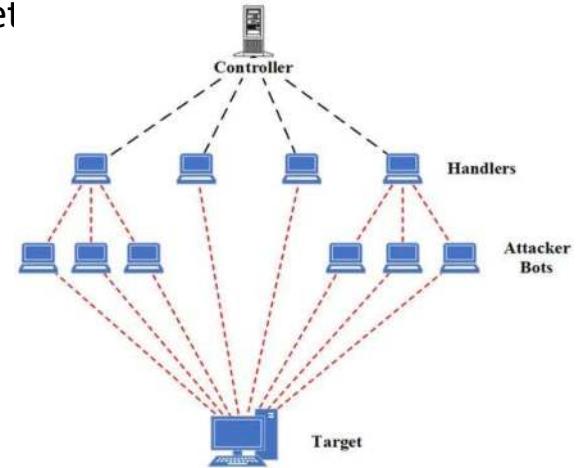
# Distributed denial-of-service

- A malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.
- They utilize multiple compromised computer systems as sources of attack traffic.
- These systems can include computers and other networked resources such as IoT devices.
- **Live DDOS Map**  
<https://www.netscout.com/ddos-attack-map>



## Distributed denial-of-service

- Network Based DDOS
  - A perpetrator uses multiple compromised systems, often infected with a Trojan, to launch a single massive attack. These systems form a net



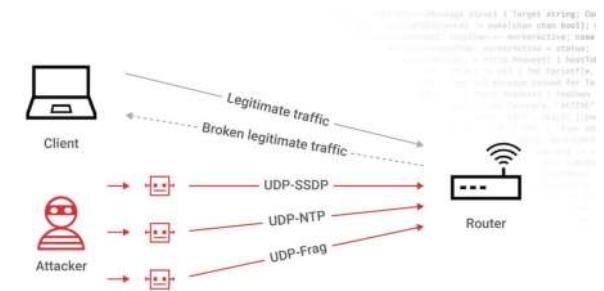
<https://www.mdpi.com/1999-5903/15/2/76>



## CompTIA Network+ N10-009 Course Notes

# Distributed denial-of-service

- UDP Floods
  - the attacker overwhelms random ports on the targeted host with IP packets containing UDP datagrams. The aim is to flood the network with enough UDP packets to slow down or crash the targeted system



What is a UDP flood attack?

<https://www.akamai.com/glossary/what-is-udp-flood-ddos-attack>

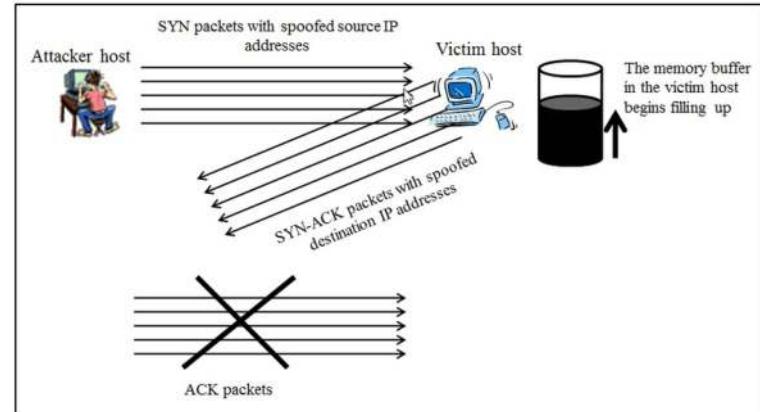




## CompTIA Network+ N10-009 Course Notes

# Distributed denial-of-service

- SYN Floods
  - A SYN Flood is a type of Denial-of-Service (DoS) attack that targets the TCP (Transmission Control Protocol) connection sequence, known as the TCP three-way handshake.
  - This attack exploits the way TCP connections are established and can overwhelm a system, rendering it unable to respond to legitimate



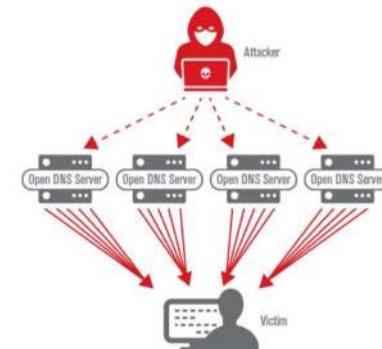
[https://www.researchgate.net/figure/The-TCP-SYN-flood-attack-Hands-on-lab-exercise-on-TCP-SYN-flood-attack\\_fig3\\_320654932](https://www.researchgate.net/figure/The-TCP-SYN-flood-attack-Hands-on-lab-exercise-on-TCP-SYN-flood-attack_fig3_320654932)



## CompTIA Network+ N10-009 Course Notes

# Distributed denial-of-service

- Amplification Attacks
  - These attacks exploit the characteristics of certain protocols to magnify the amount of traffic that is sent to a target, causing a denial of service.
  - Uses protocols such as DNS or IP Addressing
- Reflected DDOS
  - Characterized by its use of reflection, meaning the attacker forces third-party servers to direct traffic to the victim, often without the third party's knowledge.
  - IP Spoofing is one way of doing this.



<https://blog.verisign.com/security/dns-based-threats-dns-reflection-amplification-attacks/>



## CompTIA Network+ N10-009 Course Notes

# Distributed denial-of-service

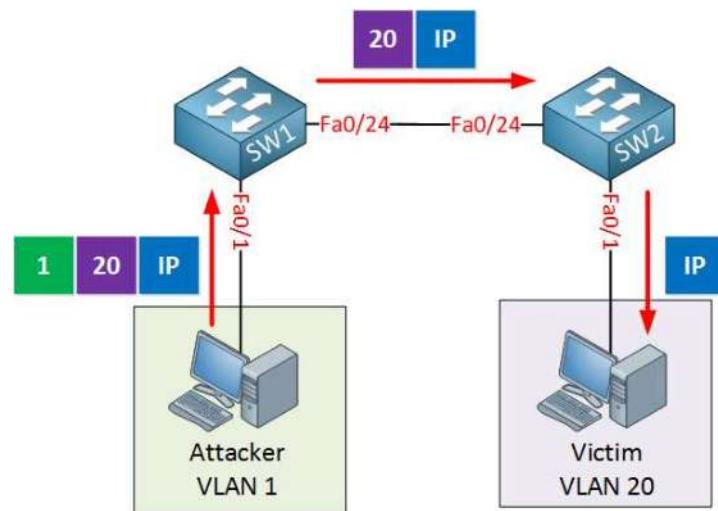
- Denial-of-service (DDoS) attacks can be mitigated by:
  - Increase Bandwidth
  - DDoS Protection Services (Cloudflare)
    - <https://www.cloudflare.com/ddos/>
  - Network Hardware with DDoS Protection
    - Some network hardware, like routers and firewalls, come with built-in DDoS protection features.



## VLAN Hopping

VLAN hopping is a network attack technique that exploits vulnerabilities to **send packets from one VLAN to another**, bypassing Layer 2 security measures.

Attackers can potentially access sensitive information or systems on a network segmented for security.



<https://networklessons.com/cisco/ccnp-switch/vlan-hopping>

[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

533



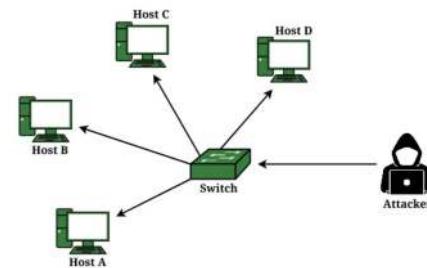
## CompTIA Network+ N10-009 Course Notes

# MAC Flooding

MAC flooding is an attack technique where an attacker **overwhelms a network switch** with fake MAC addresses, causing the switch to enter a fail-open mode.

This leads to the switch acting like a hub, **broadcasting all incoming traffic** to all ports, which can be exploited to intercept sensitive data or cause network disruption.

MAC Flooding and Spoofing



<https://www.geeksforgeeks.org/how-to-prevent-mac-flooding/>

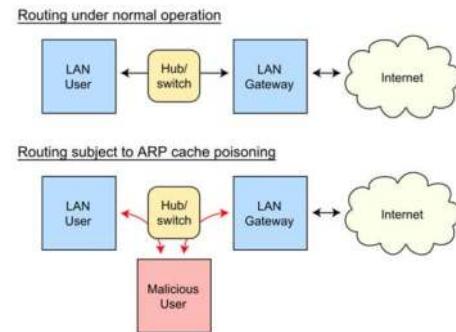


## CompTIA Network+ N10-009 Course Notes

# ARP Spoofing

ARP spoofing is a technique where an attacker **sends falsified ARP** (Address Resolution Protocol) messages over a local area network.

This results in the **linking of an attacker's MAC address with the IP address of a legitimate computer or server** on the network, allowing the attacker to intercept, modify, or stop data meant for the legitimate host.



[https://en.wikipedia.org/wiki/ARP\\_spoofing](https://en.wikipedia.org/wiki/ARP_spoofing)

[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

535



## CompTIA Network+ N10-009 Course Notes

# Address Resolution Protocol (ARP) Poisoning

ARP poisoning involves sending **malicious ARP messages to a local network**, associating the attacker's MAC address with the IP address of a legitimate device.

This allows the attacker to **intercept, modify, or block data** intended for the legitimate IP address, leading to potential data breaches or on-path attacks.



## CompTIA Network+ N10-009 Course Notes

# Domain Name System (DNS)

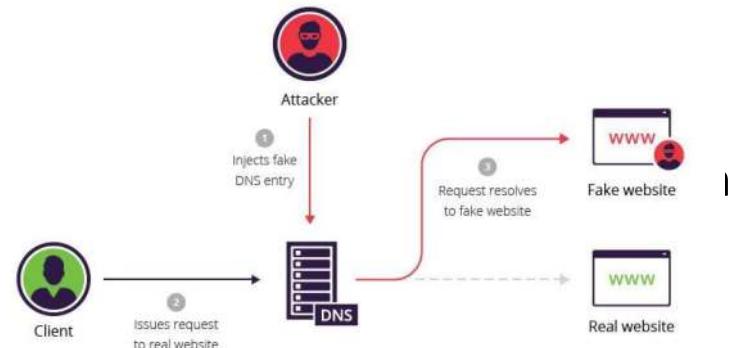
- DNS is essentially the internet's phone book; it translates human-readable domain names (like [www.example.com](http://www.example.com)) into numerical IP addresses that computers use to connect to each other.





# Domain Name System (DNS)

- Various security concerns and attack vectors:
  - DNS Spoofing (or Cache Poisoning): This attack involves corrupting the DNS cache with false information.



<https://www.imperva.com/learn/application-security/dns-spoofing/>



# Domain Name System (DNS)

- DNS Amplification Attacks: These are a type of DDoS attack where the attacker exploits publicly-accessible DNS servers to flood a target with DNS response traffic. It's an amplification attack because a small query generates a much larger response in terms of traffic load.



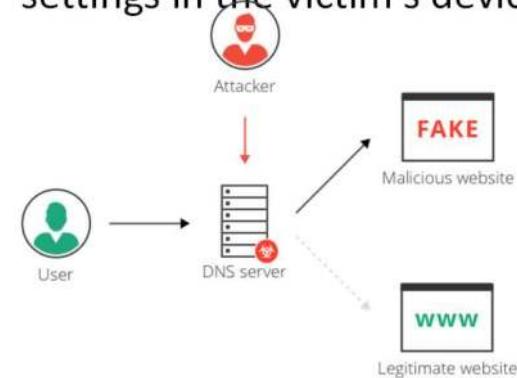
# Domain Name System (DNS)

- DNS Tunneling: DNS tunneling involves encoding the data of other programs or protocols in DNS queries and responses. It can be used for legitimate purposes (like bypassing network security controls) but is often used maliciously to exfiltrate data from a compromised system.



# Domain Name System (DNS)

- DNS Hijacking: In this attack, the attacker diverts queries to a malicious DNS server, leading users to fraudulent websites or intercepting internet traffic. This can be done by compromising the DNS server itself or by modifying the DNS settings in the victim's device.



<https://www.imperva.com/learn/application-security/dns-hijacking-redirection/>



## CompTIA Network+ N10-009 Course Notes

# Domain Name System (DNS)

- Mitigation Strategies:
  - DNSSEC (DNS Security Extensions): This adds security provisions to the DNS, ensuring that the DNS responses come from the correct source and haven't been tampered with.
  - Securing DNS Servers: Regularly updating and patching DNS servers to protect against vulnerabilities.
  - Monitoring and Analysis: Keeping an eye on DNS traffic for unusual patterns that might indicate an attack.



## Rogue Devices and Services

**Rogue Devices: Unauthorized devices** that are connected to a network without permission.

These can include rogue access points, computers, or other hardware that can be used to intercept or manipulate network traffic, leading to potential security breaches.

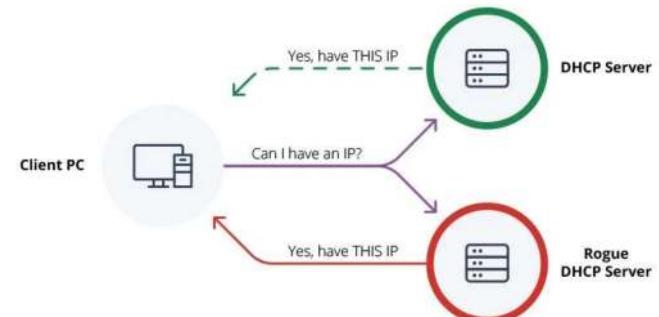
Prominent examples include rogue DHCP servers and Access Points.



## Rogue DHCP

A rogue DHCP server is an **unauthorized DHCP server** on a network that provides **incorrect IP addresses** to clients.

This can lead to network disruption, on-path attacks, or other security breaches as clients might receive configuration settings that **route their traffic through the attacker's machine**.



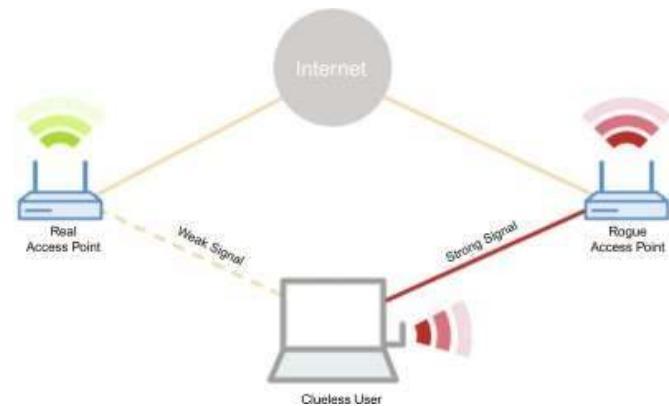
<https://www.auvik.com/franklyit/blog/rogue-dhcp-server/>



## Rogue Access Point

A rogue AP is an **unauthorized Wi-Fi access point** installed on a network without the network administrator's consent.

It poses a security risk by potentially allowing unauthorized access to network resources and data.



<https://www.sciencedirect.com/topics/computer-science/rogue-access-point>

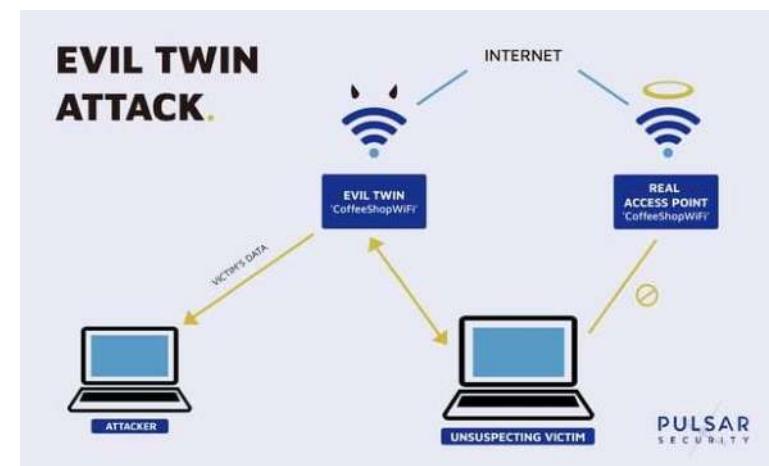


## CompTIA Network+ N10-009 Course Notes

# Evil Twin

An evil twin is a malicious Wi-Fi access point that **masquerades** as a legitimate one by **using the same SSID**.

Attackers use it to deceive users into connecting, enabling the attacker to **intercept** sensitive information transmitted over the network.



<https://blog.pulsarsecurity.com/what-is-an-evil-twin-and-how-do-you-spot-one>



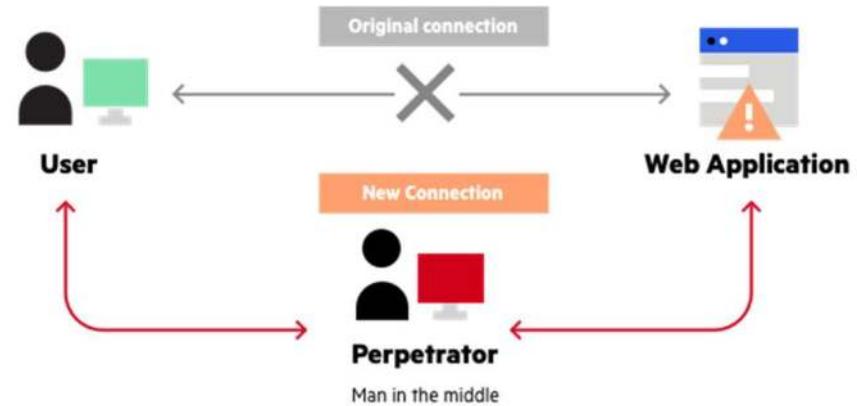
## On-path Attack

- In IT security, the term "On-path" refers to a type of attack where the attacker positions themselves in the communication path between two parties.
- This type of attack was previously known as a "Man-in-the-Middle" (MitM) attack.



## CompTIA Network+ N10-009 Course Notes

# On-path Attack





## On-path Attack

- Here's how an on-path attack works:
  - **Intercepting Communication:** The attacker intercepts the data traffic flowing between two parties (such as a user and a website). This can be achieved through various means like compromising network equipment, exploiting unsecured Wi-Fi networks, or using ARP spoofing in a local network.
  - **Eavesdropping:** In its simplest form, an on-path attack allows the attacker to passively listen to the communication, gaining access to any transmitted information, such as login credentials, personal information, or corporate data.



## CompTIA Network+ N10-009 Course Notes

# On-path Attack

- Here's how an on-path attack works:
  - **Session Hijacking:** The attacker can hijack sessions, such as web sessions, by stealing session tokens, allowing them to impersonate the victim and gain unauthorized access to systems or information.
  - **Data Manipulation:** More sophisticated on-path attackers can alter the communication. They can modify the data being sent between the parties, inject malicious content, or redirect users to fraudulent sites.



## CompTIA Network+ N10-009 Course Notes

# On-path Attack

- Here's how an on-path attack works:
  - **SSL Stripping:** In this form of on-path attack, the attacker downgrades a secure HTTPS connection to an unencrypted HTTP connection, enabling them to view and modify the data exchanged.



## CompTIA Network+ N10-009 Course Notes

# Social Engineering

- Refers to a range of malicious activities accomplished through human interactions.
- It involves tricking people into breaking normal security procedures and best practices to gain unauthorized access to systems, networks, or physical locations, or for financial gain.





## CompTIA Network+ N10-009 Course Notes

# Phishing

Phishing attacks typically have one or more of the following objectives:

- Credential Theft
- Financial Fraud
- Malware Distribution
- Identity Theft

Here are several steps and measures that are typically taken:

- User Education
- Email Filtering
- Two-Factor Authentication (2FA)
- Incident Response



# Dumpster Diving

Dumpster Diving is a technique used by attackers to retrieve sensitive information from **discarded materials**, such as documents, hardware, and other items thrown away by an organization.

This practice can **uncover valuable information** like passwords, personal identification details, financial records, or proprietary data that can be used to facilitate further attacks or identity theft.

To mitigate this risk, organizations should implement **secure disposal practices**, such as shredding documents, securely wiping data from electronic devices, and using locked disposal bins for sensitive materials.





## CompTIA Network+ N10-009 Course Notes

# Shoulder Surfing

Shoulder surfing involves directly observing or using technology to watch **over someone's shoulder** as they enter sensitive information, such as PINs at ATMs, passwords on laptops, or security codes on mobile phones.

It's a **straightforward but effective** way to gain unauthorized access to personal or confidential information.





## CompTIA Network+ N10-009 Course Notes

# Tailgating

Tailgating occurs when an unauthorized person follows an authorized individual into a restricted area without the latter's knowledge or consent.

It's a **physical security breach** that can lead to unauthorized access to secure locations.



<https://trustair.com/art-hacking-humans-social-engineering/>



## CompTIA Network+ N10-009 Course Notes

# Lesson 20

## Network Security Defense



## Hardening Techniques

Measures and practices taken to **reinforce the security** of a system or network.

The goal is to **reduce vulnerabilities** and **minimize the attack surface** to protect against threats such as unauthorized access, attacks, or data breaches.

These techniques often involve **configuring system and network settings** in a way that **maximizes security**.



## CompTIA Network+ N10-009 Course Notes

# Hardening Techniques

Encryption involves **converting data into a coded format** that can't be easily understood by unauthorized users. It's used to protect data both at rest (like on hard drives) and in transit (like over the internet).

Disabling Ports/Protocols unsurprisingly, involves **disabling unused or unnecessary network ports** and communication protocols on a device to minimize vulnerabilities and reduce the attack surface.

Endpoint protection involves **installing security software on individual devices** (endpoints) like computers and smartphones. This software typically includes antivirus, anti-malware, and sometimes additional features like firewalls and intrusion detection systems.



## CompTIA Network+ N10-009 Course Notes

# Hardening Techniques

- A host-based firewall is a software application that controls network traffic to and from a **single host** (like a computer or server), managing what traffic is allowed based on **predefined security rules**.
  - Unlike network firewalls that protect a network's perimeter, host-based firewalls provide **granular control over individual device traffic**.
- HIPS (Host Intrusion Prevention System) is a **comprehensive security solution** installed on individual hosts. It **monitors and analyzes** system behavior and configurations to prevent unauthorized access and other anomalous activities.



## CompTIA Network+ N10-009 Course Notes

# Hardening Techniques

- Default Password Changes
  - This is the practice of **altering the pre-set (default) passwords** that come with hardware and software products.
  - Manufacturers often set these default passwords to be the **same for all similar units** for ease of initial setup, but they are usually **well-known** and can be **easily exploited** by attackers.



<https://www.coretech.us/blog/is-your-phone-saying-you-have-weak-security-heres-what-it-means>



## CompTIA Network+ N10-009 Course Notes

# Hardening Techniques

- Removal of Unnecessary Software
  - Involves identifying and uninstalling software applications that are no longer needed or pose security risks
  - Removing such software can enhance security by reducing the potential attack surface and improve system performance by freeing up resources.
  - Reduced Attack Surface: Unnecessary or outdated software can contain vulnerabilities that are exploited by cyber attackers. Removing these applications lessens the number of potential security weaknesses.
  - Prevention of Data Breaches: Software that is not regularly updated or is no longer supported can be an easy target for breaches, leading to data theft or loss.



## CompTIA Network+ N10-009 Course Notes

# Network Access Control

The primary goal of **NAC** is to **prevent unauthorized access** to network resources and to ensure that all devices and users on the network **comply** with the established security policy.

This helps in **mitigating risks** posed by non-compliant or infected devices.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

563



## CompTIA Network+ N10-009 Course Notes

# Network Access Control

**Health Checks:** Assessing the **security status** of devices, including the presence of antivirus software, system updates, and security patches.

**Compliance with Regulations:** Helping organizations comply with security **regulations** by ensuring only compliant devices can access sensitive data.



## CompTIA Network+ N10-009 Course Notes

# Network Access Control

**Pre-Admission Control:** Includes device **authentication** and policy **enforcement** before allowing access to the network.

**Post-Admission Control:** Involves continuous **monitoring** of devices to ensure they remain **compliant** with security policies after gaining network access.





## CompTIA Network+ N10-009 Course Notes

# 802.1X

This is an **IEEE standard** for port-based Network Access Control (PNAC).

It is used to **authenticate devices** that are attempting to connect to a LAN or WLAN.

How it Works:

When a **device attempts to connect** to a network with 802.1X enabled, the **authenticator blocks all traffic** (except 802.1X traffic) until the client is authenticated.

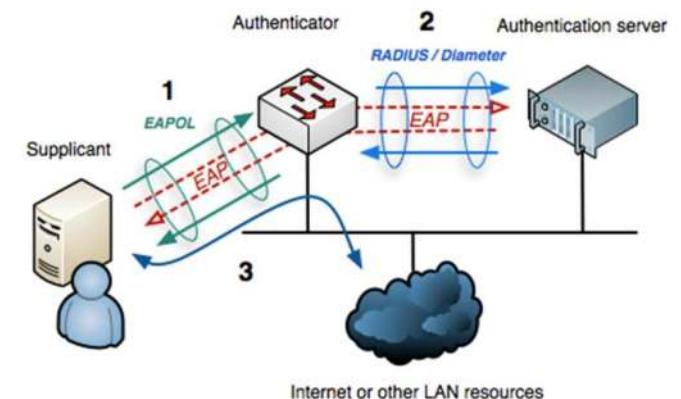
The **supplicant** (client device) **sends credentials** to the authenticator, which forwards them to the **authentication server**.

If the server **approves the credentials**, it instructs the authenticator to **allow access** to the supplicant.



## CompTIA Network+ N10-009 Course Notes

# 802.1X



[https://en.wikipedia.org/wiki/IEEE\\_802.1X#/media/File:802.1X\\_wired\\_protocols.png](https://en.wikipedia.org/wiki/IEEE_802.1X#/media/File:802.1X_wired_protocols.png)



## CompTIA Network+ N10-009 Course Notes

# EAP

EAP (Extensible Authentication Protocol) is a **framework** frequently used in network access control for various **authentication** methods.

EAP is designed to support **multiple authentication mechanisms**, including passwords, tokens, certificates, and public key encryption.

**Widely used in protocols** like PPP (Point-to-Point Protocol) and as a part of IEEE 802.1X standard for network access control.

Often used in conjunction with Remote Authentication Dial-In User Service (RADIUS) servers for **centralized authentication** in larger networks.



## CompTIA Network+ N10-009 Course Notes

# MAC Filtering

**MAC filtering** is a security measure that **allows network access only to devices with specific MAC addresses** listed in the access control list.

This can help prevent unauthorized devices from connecting to the wireless network, though it is **not foolproof due to the potential for MAC address spoofing**.



## CompTIA Network+ N10-009 Course Notes

# Key Management

**Key Management** involves the creation, distribution, storage, and maintenance of **cryptographic keys** used for securing data.

Effective key management ensures that keys are **generated securely**, stored safely, and accessible only to authorized entities.

It includes practices such as key rotation, revocation, and backup to prevent unauthorized access and to maintain the **integrity and confidentiality** of sensitive information.





## CompTIA Network+ N10-009 Course Notes

# Firewalls

- A network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules
- Typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted
- Implemented in Software or HW (appliances)
- Enforces security policies on traffic
- Controls the flow of traffic
- Does not differentiate data versus commands
- Controls flow of traffic between networks or hosts





## CompTIA Network+ N10-009 Course Notes

# Firewall Types

### Packet Filtering Firewalls:

- The most basic type, which inspects packets and permits or denies them based on source and destination IP addresses, ports, and protocols.

### Stateful Inspection Firewalls:

- More advanced than packet filtering, these firewalls track the state of active connections and make decisions based on the context of the traffic.

### Web Application Firewall (WAF):

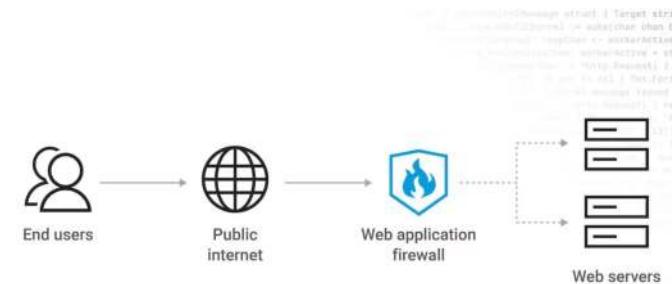
- WAFs are specifically designed to protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet.
- They are particularly effective in preventing web application attacks such as cross-site scripting (XSS), SQL injection, and session hijacking.
- WAFs operate at the application layer and apply a set of rules to an HTTP conversation. These rules are generally customized to the application, so they can be more effective in preventing threats specific to the application.
- WAFs can be deployed as hardware, software, or as part of a cloud service.



CompTIA Network+ N10-009 Course Notes

# Firewall Types

## Web Application Firewall (WAF):



What is a WAF?





## CompTIA Network+ N10-009 Course Notes

# Firewall Types

### Unified Threat Management (UTM):

- UTMs provide a comprehensive solution that combines multiple security features and services in a single device.
- These features typically include anti-virus, anti-spyware, firewall, intrusion detection and prevention, and content filtering.
- The main advantage of UTM is its simplicity and ease of management, as it consolidates various security functions into one device, making it ideal for small to medium-sized businesses.

### Next-Generation Firewalls (NGFW):

- NGFWs are a more advanced form of the traditional firewall, integrating additional functionalities such as deep packet inspection, intrusion prevention systems, and application awareness.
- **Deep Packet Inspection:** Unlike traditional firewalls, NGFWs go beyond port/protocol inspection and blocking, to inspect the data within the packets themselves, thereby providing more robust security.
- **Threat Intelligence Integration:** Many NGFWs integrate with threat intelligence services to provide up-to-date information about emerging threats.



## CompTIA Network+ N10-009 Course Notes

# Firewall

A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.

At its most basic, a firewall is a barrier between a private internal network and the public Internet.

We will be covering:

- Rules
- Access lists
- Ports/protocols
- Screened subnets



# Firewall

## Rules:

- Function: Firewall rules are **specific configurations** that control how the firewall operates. These rules determine which traffic should be **allowed** or **blocked**.
- Example: A rule might specify that **all inbound traffic** on port 80 (HTTP) is allowed, while **all inbound traffic** on port 23 (Telnet) is blocked.

## Access Lists

- Function: Access lists are a **series of commands** applied to a firewall, which selectively **filter traffic** based on the source and destination addresses, protocols, and ports.

## Ports/Protocols

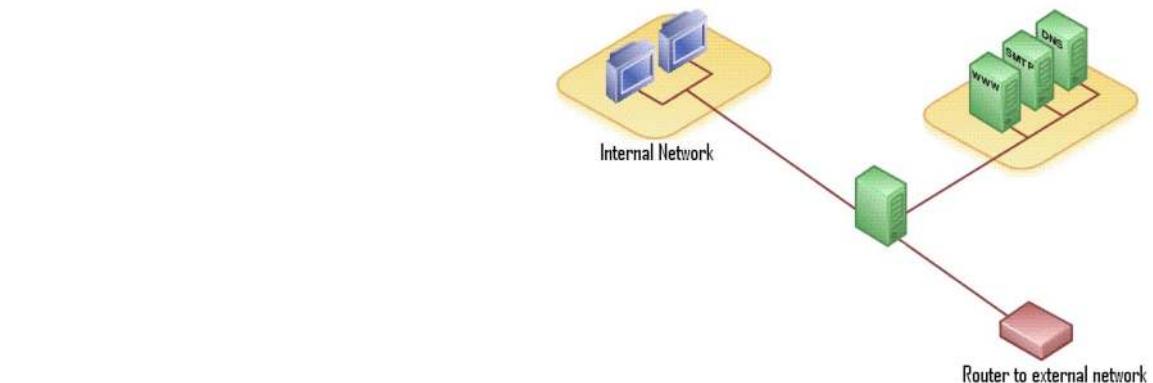
- Ports and protocols are essential components in network communications that must be secured by firewalls.



## Screened Subnets

Concept: A screened subnet or DMZ is a physical or logical **subnetwork** that contains and exposes an organization's external-facing services to an untrusted network, usually the Internet.

Implementation: Firewalls are configured to allow limited traffic from the DMZ to the internal network, with **strict rules** to control what types of interactions are allowed.



[https://en.wikipedia.org/wiki/Screened\\_subnet](https://en.wikipedia.org/wiki/Screened_subnet)

[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

577



## CompTIA Network+ N10-009 Course Notes

# Access Control List

**Access Control List (ACL):** This is a list used by routers and other network devices to authorize or deny traffic to or from **particular IP addresses, based on a set of rules.**

The screenshot shows the SONICWALL Network Security Appliance interface. The left sidebar menu includes: Dashboard, System, Network (selected), Interfaces, PortShield Groups, Failover & LB, Zones, DNS, Address Objects (selected), Services, Routing, NAT Policies, ARP, and Neighbor Discovery. The main pane displays a list of address objects:

Object ID	Object Name	Type	Details	Action Buttons
9	WLAN Interface IP	Group		
10	All WAN IP	Group		
11	All Interface IP	Group		
12	All X0 Management IP	Group		
13	All SonicPoints	Group		
14	All Authorized Access Points	Group		
15	All Rogue Access Points	Group		
16	Default ACL Allow Group	Group	Wireless Client 10 00:11:22:33:44:55 MAC Address: WLAN	
17	Default ACL Deny Group	Group	No Entries	
18	Node License Exclusion List	Group		

<https://www.sonicwall.com/pt-br/support/knowledge-base/configuring-acls-mac-filter-list-for-individual-virtual-access-point/170503259376841/>



## Web Filter

Implementing a web filter is essential for **controlling** the websites and content that users can access, thus mitigating the risk of exposure to malicious content.





## CompTIA Network+ N10-009 Course Notes

# Agent-Based

Agent-based web filtering involves installing software agents on **individual user devices**.

These agents enforce web access policies set by the organization, regardless of the network the device is connected to.

Use Case: This approach is particularly useful for managing the web access of **remote or mobile employees** who might not always be connected to the corporate network.





## Centralized Proxy

A centralized proxy, often part of a larger network security appliance, acts as an **intermediary** between users and the internet.

All web traffic passes through this proxy, which enforces web filtering policies.

Advantages: This method offers **centralized** management and control, making it easier to enforce **consistent** web access policies across the entire organization.





## Universal Resource Locator Scanning

Function: URL scanning involves examining the URLs requested by users to determine if they should be allowed or blocked.

This can be based on a **database** of categorized URLs.

Application: URL scanning is effective in preventing access to **known** malicious or inappropriate websites.

It's a fundamental component of most web filtering solutions.



## CompTIA Network+ N10-009 Course Notes

# Content Categorization

Content categorization **classifies** web pages into different categories (like social media, adult content, gaming, etc.) based on their content.

Purpose: This allows organizations to block or allow **entire categories** of websites, making policy enforcement more **streamlined** and **consistent**.





## CompTIA Network+ N10-009 Course Notes

# Block Rules

Block rules in web filtering are **specific criteria** set to block access to certain websites or content.

These rules can be based on URLs, keywords, categories, or other identifiable aspects of web content.

Customization: Organizations can customize block rules to align with their security **policies**, regulatory **compliance** needs, and organizational **culture**.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

584



## Reputation

Reputation-based filtering uses the **reputation score** of websites to determine whether they should be allowed or blocked.

Mechanism: Reputation scores are usually derived from various factors like the **website's history**, the **presence of malware**, and **user feedback**.

Effectiveness: This method is particularly effective in protecting against **newly created** malicious sites that may not yet be categorized or have a known URL pattern.





## CompTIA Network+ N10-009 Course Notes

# Lesson 21

## Troubleshooting Methodology



## 7 Steps Identify The Problem

1. Identify the problem
2. Establish a theory of probable cause
3. Test the theory to determine the cause
4. Establish a plan of action to resolve the problem and identify potential effects
5. Implement the solution or escalate as necessary
6. Verify full system functionality and implement preventive measures if applicable
7. Document findings, actions, outcomes, and lessons learned throughout the process



## Step 1: Identify The Problem

Identifying the problem is the **crucial first step** in the troubleshooting methodology.

It involves **understanding the symptoms, gathering detailed information, and engaging with affected users** to accurately define the issue.





## CompTIA Network+ N10-009 Course Notes

# Gather Information

This involves **collecting all relevant details** about the issue from various sources such as system logs, user reports, and network performance data.

This initial step is critical for understanding the scope and impact of the problem.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexam.com](http://www.tiaexam.com)



## CompTIA Network+ N10-009 Course Notes

### Question Users

**Direct interaction** with users who have encountered the problem to get firsthand descriptions of what they experienced.

This can **provide clues** that are not evident in system logs or performance metrics.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

590



## CompTIA Network+ N10-009 Course Notes

# Identify Symptoms

Carefully note down the **specific symptoms** and signs of the problem as reported by users and observed in the system.

This helps in **diagnosing the issue** more accurately.



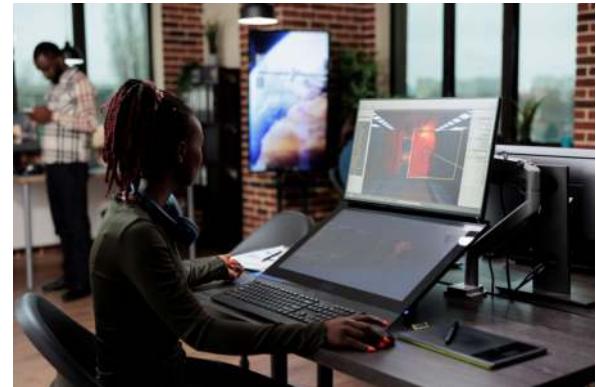


## CompTIA Network+ N10-009 Course Notes

# Determine if Anything has Changed

**Investigate** whether there have been any recent changes to the system or network environment that could have triggered the problem.

Changes can include software updates, hardware modifications, or alterations in configuration settings.





## CompTIA Network+ N10-009 Course Notes

# Duplicate the Problem, if Possible

Attempt to recreate the issue under controlled conditions to better understand its causes and identify potential solutions.

Replicating the problem can also help in verifying that the issue has been resolved once changes are made.





## CompTIA Network+ N10-009 Course Notes

# Approach Multiple Problems Individually

If there are several issues at hand,  
**tackle them one at a time.**

This **methodical** approach prevents confusion and ensures that each problem is **thoroughly resolved** before moving on to the next.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

594



## Step 2: Establish a Theory of Probable Cause

Establishing a theory of probable cause involves **formulating potential reasons** for the identified problem based on collected information and observations.

This step leverages technical knowledge, experience, and logical reasoning to **narrow down the possible causes**, providing a focused direction for troubleshooting efforts.

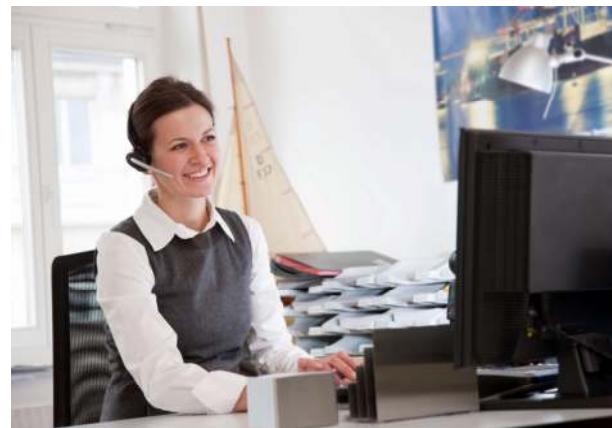


## CompTIA Network+ N10-009 Course Notes

# Question the Obvious

Begin by examining the **most straightforward and common** causes of the problem.

This step often involves **checking for simple issues** that are frequently overlooked, such as disconnected cables, incorrect settings, or power outages.





## CompTIA Network+ N10-009 Course Notes

# Consider Multiple Approaches

**Keep an open mind** to various potential causes and solutions.

By considering different possibilities, you can more accurately pinpoint the root cause of an issue.





## CompTIA Network+ N10-009 Course Notes

# Top-to-bottom/bottom-to-top OSI model

Use the OSI model as a framework to systematically troubleshoot network issues.

You can start troubleshooting from either the top (application layer) and work your way down to the physical layer, or vice versa, **depending on the symptoms** and the nature of the problem.

This structured approach ensures that no layer is overlooked.





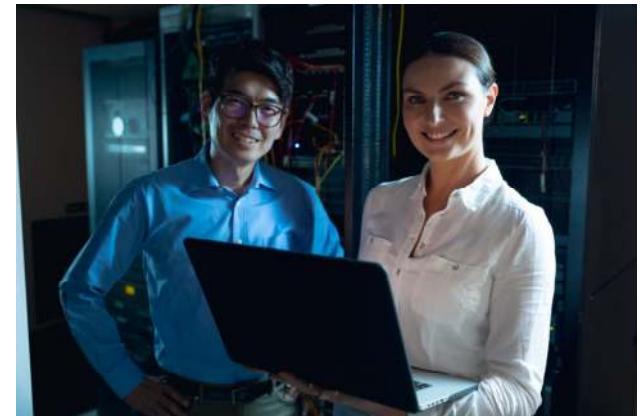
## CompTIA Network+ N10-009 Course Notes

# Divide and Conquer

**Break down the problem** into smaller, more manageable parts.

By **isolating sections** of the network or system, you can more easily identify where the issue is occurring.

This technique helps in efficiently pinpointing the source of a problem.





## CompTIA Network+ N10-009 Course Notes

# Step 3: Test the Theory to Determine the Cause

Testing the theory involves applying practical methods to **verify** whether the hypothesized cause of the problem is accurate.

This step is critical for **confirming the root cause**, allowing for targeted troubleshooting and ensuring that subsequent solutions address the actual issue.



## CompTIA Network+ N10-009 Course Notes

If the theory is confirmed,  
determine the next steps to  
resolve the problem

When testing confirms your theory, you  
then plan and **implement a solution** to fix  
the issue.

This step might include repairing or  
replacing hardware, updating software, or  
changing configurations.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

601

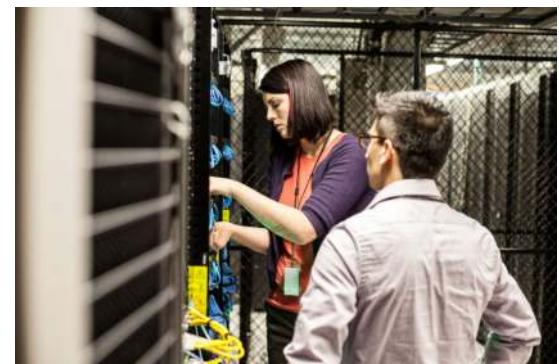


## CompTIA Network+ N10-009 Course Notes

If the theory is not confirmed, establish a new theory or escalate

If the initial theory does not hold up under testing, it's time to **develop a new theory** based on the information gathered.

If unable to identify the cause after multiple attempts, the issue should be escalated to a **higher-level support** or specialist with more expertise in the area of concern.





## CompTIA Network+ N10-009 Course Notes

### Step 4: Establish a plan of action to resolve the problem and identify potential effects

Once the cause of the problem is determined, **develop a detailed plan** to fix it, considering how the proposed actions might impact the system or network operations.





## Step 5: Implement the solution or escalate as necessary

**Execute the plan** to resolve the issue.

If the problem is beyond your capability or resources, escalate it to a higher level of expertise.



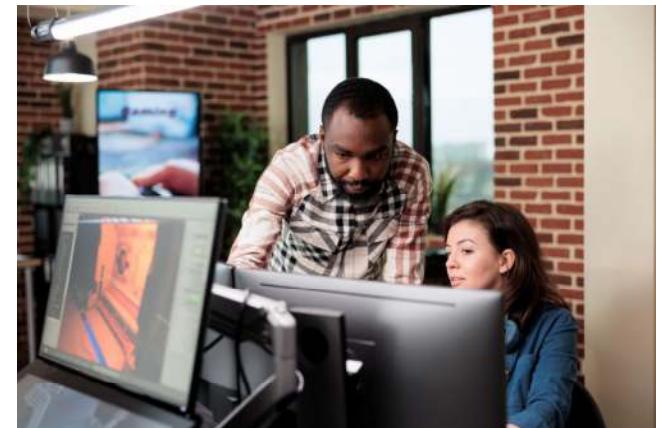


## CompTIA Network+ N10-009 Course Notes

**Step 6: Verify full system functionality and, if applicable, implement preventive measures**

After the solution is implemented, **test the system to ensure that it is fully operational** and the original problem has been resolved.

Also, put in place any measures that could prevent the issue from recurring.





## Step 7: Document findings, actions, outcomes, and lessons learned

**Record** the problem, how it was diagnosed, the solution implemented, and the outcome of those actions.

This documentation can be invaluable for addressing similar issues in the future and for improving the overall IT support process.





## CompTIA Network+ N10-009 Course Notes

# Lesson 22

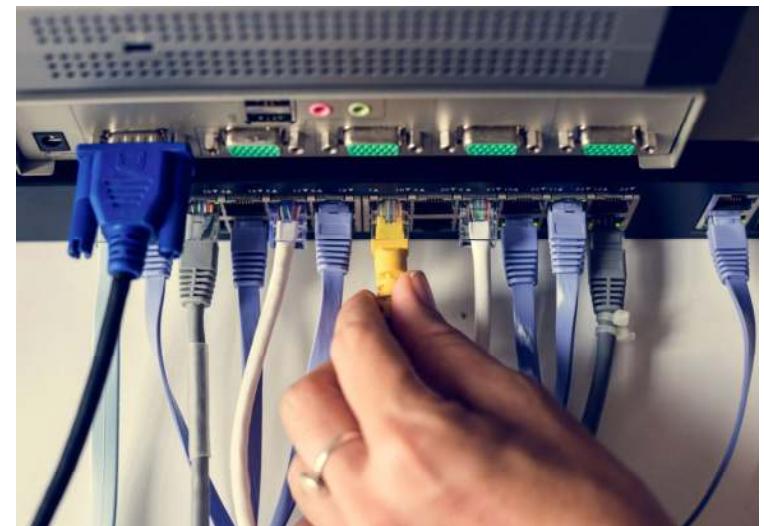
Troubleshoot Common Cabling and Physical



## Cable Issues

Cable issues can significantly impact network **performance** and **reliability**.

Understanding different types of cables and their appropriate use is crucial for ensuring optimal network functionality.





## CompTIA Network+ N10-009 Course Notes

# Incorrect Cable Issues

Using incorrect cables can lead to network failures, reduced performance, and connectivity problems.

Ensuring the **correct cable** type for specific applications and environments is essential for maintaining network integrity.



## CompTIA Network+ N10-009 Course Notes

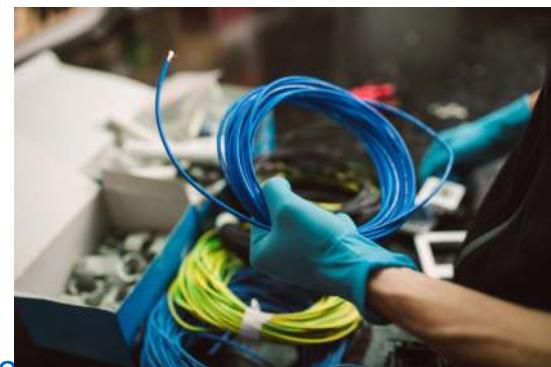
# Single Mode vs. Multimode

Single Mode: Used for **long-distance** transmissions, single mode fibers have a **smaller core** and support **higher bandwidth** with less signal attenuation.

Multimode: Suitable for **shorter distances**, multimode fibers have a **larger core**, which allows **multiple light modes** but can cause **more signal dispersion** and attenuation over longer distances.

Incorrect Use: Using single mode fiber where multimode is required, or vice versa, can cause **signal loss** and **inefficient** data transmission.

Impact: This mismatch can result in increased **attenuation**, **poor signal quality**, and **reduced bandwidth**, affecting overall network performance.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

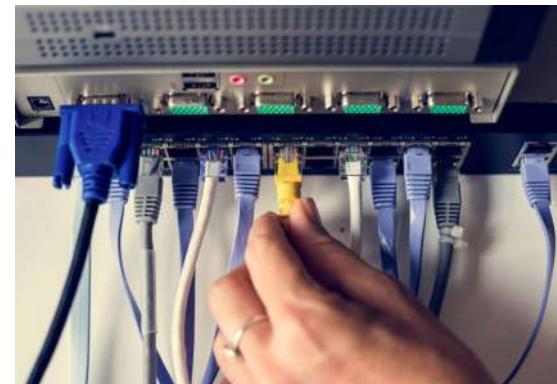
610



## Category 5/6/7/8 Cable Issues

Incorrect Category: Using a lower category cable (e.g., Cat5) instead of a higher category (e.g., Cat6, Cat7, or Cat8) can **limit data transfer speeds** and lead to **increased errors**.

Impact: This can cause **network slowdowns**, increased latency, and an inability to support high-speed applications or data-intensive operations.





## CompTIA Network+ N10-009 Course Notes

# Shielded Twisted Pair (STP) vs. Unshielded Twisted Pair (UTP) Cable Issues

**Incorrect Shielding:** Using UTP cables in environments with high electromagnetic interference (EMI) instead of STP can result in **signal degradation and data corruption.**

**Impact:** This can lead to frequent data retransmissions, increased error rates, and reduced network reliability and performance.



## Signal Degradation

Signal degradation occurs when the quality of the signal **diminishes over distance** or due to interference, leading to poor network performance.

Common causes include using incorrect cable types, physical damage, and environmental factors such as **electromagnetic interference (EMI)** or **radio frequency interference (RFI)**.



## CompTIA Network+ N10-009 Course Notes

# Crosstalk

**Crosstalk** is a specific type of signal degradation where a signal transmitted on **one cable or channel interferes with a signal on another cable or channel**.

Types of Crosstalk:

- Near-End Crosstalk (NEXT): Interference measured at the transmitting end.
- Far-End Crosstalk (FEXT): Interference measured at the receiving end.

Using **incorrect or low-quality cables**, such as those with insufficient shielding or untwisted pairs, can increase the risk of crosstalk.

Effects include corrupted data, reduced data transmission speeds, and an overall decrease in network reliability and performance.



## CompTIA Network+ N10-009 Course Notes

# Interference

The **disruption of signal transmission** caused by electromagnetic signals from other electronic devices or cables.

Interference can lead to data corruption and loss of connectivity, affecting network performance.





## CompTIA Network+ N10-009 Course Notes

# Attenuation

The **gradual loss of signal strength** as it travels through a cable or medium.

Attenuation increases with distance and can affect the quality of the communication, requiring the use of repeaters or amplifiers to maintain signal integrity.





## CompTIA Network+ N10-009 Course Notes

# Improper Termination

Improper termination occurs when network cables are **not correctly terminated** with the appropriate connectors or techniques.

### Issues:

- Signal loss and reflection, leading to data transmission errors and reduced network performance.
- Increased electromagnetic interference (EMI), causing further degradation of signal quality.

Proper termination is essential to ensure reliable connectivity and optimal performance in network installations.





# Transmitter (TX)/Receiver (RX) Transposed

**TX/RX transposition** happens when the **transmitter and receiver wires are incorrectly connected**, causing communication failures.

## Issues:

- Devices cannot establish a proper link, leading to a **complete loss of communication** between networked devices.
- Troubleshooting becomes more complex and time-consuming, as the issue is often not immediately obvious.

Ensuring correct **TX/RX** alignment during installation is crucial for maintaining proper network functionality and communication.



## Interface Issues

Interface issues can significantly impact network performance, leading to reduced efficiency and increased troubleshooting efforts.

Monitoring interface counters helps identify and diagnose these problems early, ensuring network reliability and stability.



## Increasing Interface Counters

Interface counters **track various metrics** related to network traffic and errors.

**Increasing counters indicate potential issues** that need to be addressed to maintain optimal network performance.





## Cyclic Redundancy Check (CRC) Errors

CRC errors occur when there is a mismatch in the **data checksum**, indicating data corruption during transmission.

### Issues:

- Caused by faulty cables, electromagnetic interference (EMI), or hardware failures.
- Result in data retransmission, increased latency, and reduced network throughput.



## Runts, Giants, Drops

Runts are packets that are **smaller than the minimum allowed size** (usually less than 64 bytes).

Giants are packets that **exceed the maximum allowed size** (usually greater than 1518 bytes for Ethernet frames).

Drops occur when **packets are discarded** due to congestion, buffer overflow, or configuration issues.



## CompTIA Network+ N10-009 Course Notes

# Port Status Issues

Port status issues can affect network connectivity and performance, requiring attention to maintain proper network operation.

Understanding different port statuses helps in diagnosing and resolving network problems effectively.





## Error Disabled

A port in error disabled status has been **automatically shut down** by the network device due to a detected issue.

### Causes:

- Security violations, such as port security breaches.
- Network problems, such as excessive errors or link flaps.

### Resolution:

- Identify and resolve the underlying issue before re-enabling the port to prevent recurrence.



## Administratively Down

A port marked as **administratively down** has been **manually disabled** by a network administrator.

### Causes:

- Intentional shutdown for maintenance, configuration changes, or security reasons.

### Resolution:

- The port can be re-enabled through administrative action once the necessary changes or maintenance are completed.



# Suspended

A port in suspended status is **temporarily disabled**, usually due to network policies or dynamic configurations.

## Causes:

- Policy enforcement, such as violation of network access controls or dynamic adjustments by protocols like LACP.

## Resolution:

- Address the policy or configuration that caused the suspension, and the port may automatically re-enable or require manual intervention.



## CompTIA Network+ N10-009 Course Notes

# Hardware Issues

Hardware issues can significantly impact network performance and reliability, necessitating timely identification and resolution.

Common hardware issues include problems with Power over Ethernet (PoE) and transceivers, which are critical for maintaining network functionality.



## CompTIA Network+ N10-009 Course Notes

# Power over Ethernet (PoE) Issues

**PoE allows network cables to carry electrical power, simplifying the installation of networked devices like IP cameras and wireless access points.**



## CompTIA Network+ N10-009 Course Notes

# Power Budget Exceeded

When the total power consumption of connected PoE devices exceeds the available power budget of the switch, **some devices may not receive sufficient power.**

### Symptoms:

- Devices failing to power on or operating intermittently.

### Resolution:

- Review and manage the power requirements of all connected devices, and upgrade the PoE switch if necessary to support higher power demands.



629



## Incorrect Standard

Using devices and switches that adhere to **different PoE standards** (e.g., IEEE 802.3af, 802.3at, 802.3bt) can result in compatibility issues.

### Symptoms:

- Devices not receiving power or insufficient power.

### Resolution:

- Ensure all devices and switches comply with the **same PoE standard** and upgrade equipment if necessary for compatibility.



## Transceiver Issues

Transceivers are modules used to connect network devices via fiber optic or copper cables, and issues with them can affect data transmission.

Common Issues: Mismatched transceivers and signal strength problems.





## Mismatched Transceivers

Using **incompatible transceivers** can lead to connectivity and performance issues.

### Symptoms:

- No link light, data errors, or intermittent connections.

### Resolution:

- Verify that transceivers are compatible with each other and the devices they are connected to, ensuring they are from the **same vendor or meet the same standards**.



## Signal Strength

Poor signal strength in transceivers can result in data transmission errors and reduced network performance.

### Symptoms:

- High error rates, dropped packets, or no connectivity.

### Resolution:

- Check and clean fiber connectors, ensure proper cable length and quality, and verify transceiver specifications to maintain adequate signal strength.



## CompTIA Network+ N10-009 Course Notes

# Lesson 23

## Troubleshoot Network Services



## Switching Issues

Switching issues can **disrupt network connectivity and performance**, leading to significant operational challenges.

Common switching issues include problems with the Spanning Tree Protocol (STP), which is critical for preventing network loops and ensuring efficient data flow.





## CompTIA Network+ N10-009 Course Notes

# STP in Switching Issues

Proper implementation and management of STP are crucial for **preventing network loops** and maintaining efficient data flow.

Addressing issues with root bridge selection, port roles, and port states ensures a stable and reliable network environment.



## STP and Network Loops

The Spanning Tree Protocol (STP) prevents network loops by creating a loop-free logical topology.

### Network Loops:

- Occur when multiple active paths exist between network switches, causing broadcast storms and network congestion.
- Resolution: STP automatically blocks redundant paths to prevent loops, ensuring a stable network.



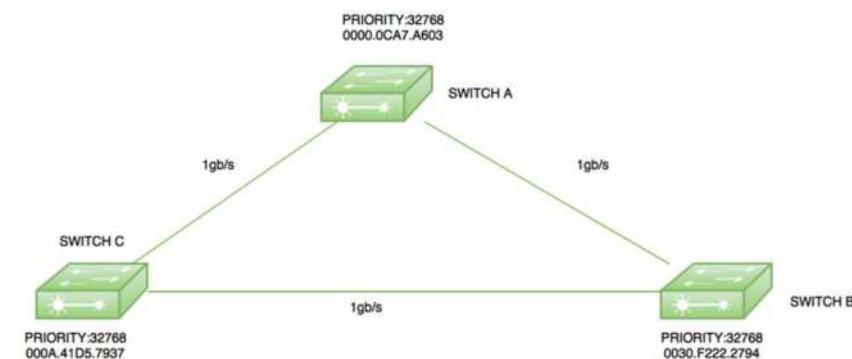
## CompTIA Network+ N10-009 Course Notes

# Root Bridge Selection

The root bridge is the **central reference point** in an STP-enabled network.

### Root Bridge Selection:

- Determined by the **lowest bridge ID**, which consists of a priority value and the MAC address.
- Issues: Incorrect root bridge selection can lead to suboptimal network performance.
- Resolution: Adjust bridge **priorities** to ensure the most appropriate switch becomes the root bridge.





## STP Port Roles

**STP assigns specific roles to switch ports to maintain a loop-free network.**

### Port Roles:

- Root Port: The best path to the root bridge.
- Designated Port: The best path to a specific network segment.
- Blocked Port: Prevents loops by not forwarding traffic.



## CompTIA Network+ N10-009 Course Notes

# STP Port States

**STP ports transition through several states** to ensure network stability.

### Port States:

- Blocking: Prevents traffic to avoid loops.
- Listening: Prepares to forward traffic without adding to the MAC table.
- Learning: Adds MAC addresses to the table without forwarding.
- Forwarding: Actively forwards traffic.

**Issues:** Incorrect port states can cause connectivity problems.

**Resolution:** Verify and configure port states appropriately to ensure smooth network operation.



## CompTIA Network+ N10-009 Course Notes

# Incorrect VLAN Assignment

Incorrect VLAN assignment can lead to **network segmentation issues**, where devices are unable to communicate with each other or unauthorized devices gain access to restricted segments.

### Issues:

- Devices on different VLANs unable to communicate as intended.
- Security vulnerabilities if sensitive data is accessible from unauthorized VLANs.

### Resolution:

- Verify and correct VLAN assignments on switches and routers to ensure devices are on the intended network segments.
- **Regularly audit VLAN** configurations to maintain proper segmentation and security.



## CompTIA Network+ N10-009 Course Notes

# Access Control Lists (ACLs)

ACLs are used to **control network traffic** by specifying which users or systems can access network resources and under what conditions.

### Issues:

- Misconfigured ACLs can **block legitimate traffic** or allow unauthorized access, leading to security breaches and connectivity problems.

### Resolution:

- Carefully review and update ACLs to ensure they are **correctly configured** to permit or deny traffic based on the network's security policies.
- Implement **regular audits** and testing of ACLs to ensure they function as intended and do not inadvertently disrupt network operations.



## CompTIA Network+ N10-009 Course Notes

# Route Selection Issues

Effective route selection is critical for network performance and reliability.

Common issues can lead to suboptimal routing, increased latency, and network failures.

Identifying and resolving these issues ensures efficient and accurate data transmission across the network.





## Routing Table Issues

**Stale Routes:** Routes that are **no longer valid** but remain in the routing table can cause misrouting of packets.

- **Resolution:** Regularly update and clean routing tables to remove outdated routes.

**Misconfigured Static Routes:** Incorrect static route entries can lead to **packet loss and routing loops**.

- **Resolution:** Verify static route configurations and ensure they align with network topology.

**Dynamic Routing Protocol Conflicts:** Inconsistent routing information due to **misconfigured or conflicting routing protocols**.

- **Resolution:** Ensure proper configuration and compatibility of dynamic routing protocols like OSPF, EIGRP, and BGP.



## CompTIA Network+ N10-009 Course Notes

# Default Route Issues

**Missing Default Route:** Absence of a default route can cause packets destined for unknown networks to be dropped.

- Resolution: **Configure a default route** to handle traffic for unspecified destinations.

**Incorrect Default Route:** Misconfigured default routes can direct traffic to the wrong gateway, causing connectivity issues.

- Resolution: **Verify and correct the default route configuration** to ensure accurate routing.



## CompTIA Network+ N10-009 Course Notes

# Address Pool Exhaustion

Address pool exhaustion occurs when the available IP addresses in a network's DHCP scope or subnet are **depleted**.

### Common Issues:

- Over-subscription: **Too many devices** attempting to obtain IP addresses from a limited pool.
- Improper Scope Configuration: DHCP scopes not configured to meet network demands, leading to **insufficient IP allocation**.
- Leased IPs Not Released: Devices **not releasing IP addresses properly**, causing addresses to be marked as in-use unnecessarily.

### Resolutions:

- Expand the DHCP scope or subnet to include more IP addresses.
- Implement IP address management (IPAM) to monitor and optimize IP address allocation.
- Ensure proper lease times and release mechanisms are configured.



# Incorrect Default Gateway

An incorrect default gateway configuration can **prevent devices from communicating** with other networks, including the internet.

## Common Issues:

- Misconfigured Gateway Address: Devices pointing to a non-existent or incorrect gateway IP.
- Gateway IP Outside Subnet: Default gateway IP **not within the same subnet** as the device, causing routing failures.
- Multiple Gateways: Conflicting default gateway settings leading to inconsistent routing behavior.

## Resolutions:

- Verify and correct the default gateway IP address on affected devices.
- Ensure the default gateway is within the correct subnet range.
- **Standardize default gateway configurations** across the network to avoid conflicts.



## CompTIA Network+ N10-009 Course Notes

# Incorrect IP Address

Incorrect IP address configuration can cause devices to fail in communicating with the network, leading to connectivity issues.

### Common Issues:

- Manual Configuration Errors: **Typographical errors or incorrect entries** when assigning IP addresses manually.
- Static vs. DHCP Conflicts: Manually assigned static IP addresses **conflicting with dynamically assigned DHCP addresses.**

### Resolutions:

- Double-check and verify IP address configurations for accuracy.
- **Use DHCP reservations** for devices that require a static IP address to avoid conflicts.



## CompTIA Network+ N10-009 Course Notes

# Duplicate IP Address

Duplicate IP addresses occur when two devices on the same network are assigned **the same IP address**, causing network conflicts.

### Common Issues:

- Manual Configuration: Same IP address assigned manually to multiple devices.
- DHCP Lease Issues: DHCP server assigning an IP address that is already in use.

### Resolutions:

- Use IP address management tools to detect and resolve IP conflicts.
- Ensure that DHCP scopes are properly configured to avoid overlaps with static IP ranges.
- Regularly monitor the network for IP conflicts and resolve them promptly.



## CompTIA Network+ N10-009 Course Notes

# Incorrect Subnet Mask

An incorrect subnet mask can lead to **improper network segmentation**, causing devices to fail in communicating with each other.

### Common Issues:

- Configuration Errors: Subnet masks entered incorrectly during network setup.
- Incompatible Subnets: Devices configured with subnet masks that don't match the network's addressing scheme.

### Resolutions:

- **Verify subnet mask configurations** to ensure they match the network design.
- **Educate network administrators** on proper subnetting techniques and the importance of accurate subnet mask configuration.
- **Use network planning tools** to design and implement correct subnetting schemes.



## CompTIA Network+ N10-009 Course Notes

# Lesson 24

## Troubleshoot Performance Issues



## CompTIA Network+ N10-009 Course Notes

# Congestion/Contention

Congestion occurs when network demand exceeds capacity, leading to slowdowns and delays.

### Common Causes:

- Excessive simultaneous data transfers.
- Network security issues, such as malware

### Resolutions:

- **Upgrade network infrastructure** to handle higher traffic volumes.
- Scan network for malware. Implement IDS/IPS





## CompTIA Network+ N10-009 Course Notes

# Bottlenecking

Bottlenecking happens when a particular part of the network limits overall performance, creating a point of congestion.

### Common Causes:

- Insufficient bandwidth on a network link.
- Overloaded network devices (e.g., routers, switches).

### Resolutions:

- **Identify and upgrade the bottleneck** component to increase capacity.
- **Distribute traffic load** more evenly across the network.





# Bandwidth

**Bandwidth** refers to the maximum data transfer rate of a network connection.

## Issues:

- Limited bandwidth can lead to slow network performance.
- Bandwidth-hungry applications can monopolize available resources.

## Resolutions:

- **Monitor bandwidth usage** and optimize allocation.
- **Implement traffic shaping** and prioritization policies.



## CompTIA Network+ N10-009 Course Notes

# Throughput Capacity

Throughput capacity is the actual rate at which data is successfully transmitted through the network.

## Issues:

- Network inefficiencies and congestion can reduce throughput.
- Discrepancies between theoretical bandwidth and actual throughput.

## Resolutions:

- **Optimize network configurations** and reduce interference.
- Ensure hardware and software are capable of supporting desired throughput levels.



## CompTIA Network+ N10-009 Course Notes

# Latency

Latency is the time it takes for data to travel from the source to the destination.

### Issues:

- High latency can lead to delays in data transmission, affecting real-time applications.
- Causes include long transmission distances and network congestion.

### Resolutions:

- **Use high-speed connections** and reduce the number of hops.
- **Optimize routing paths** and use content delivery networks (CDNs).



## Packet Loss

Packet loss occurs when data packets fail to reach their destination, leading to incomplete data transmission.

### Issues:

- Causes include network congestion, faulty hardware, and interference.
- Leads to retransmissions, reduced throughput, and degraded application performance.

### Resolutions:

- **Improve network infrastructure** and hardware reliability.
- **Use error detection** and correction mechanisms.



# Jitter

Jitter refers to the variability in packet arrival times, affecting the quality of real-time communications.

## Issues:

- High jitter can lead to choppy audio and video in VoIP and video conferencing.
- Causes include network congestion and route changes.

## Resolutions:

- **Implement QoS** to prioritize real-time traffic.
- **Use jitter buffers** to smooth out packet arrival times.



## CompTIA Network+ N10-009 Course Notes

# Wireless Issues

Wireless networks often encounter **performance challenges** that can disrupt connectivity and data flow.

These issues may arise from interference, channel overlap, signal degradation, insufficient coverage, client disassociation, and roaming misconfiguration.

Such problems can lead to slower data rates, connection drops, and inconsistent network performance.





## CompTIA Network+ N10-009 Course Notes

# Wireless Interference

### Issues:

- **Interference** from other electronic devices and physical obstructions can cause reduced network performance.
- Symptoms include slow data rates, high latency, and frequent connection drops.

### Resolutions:

- **Identify and reduce interference** sources, and use wireless channels with minimal interference.



# Channel Overlap

## Issues:

- **Overlapping channels** result in increased interference and reduced throughput.
- Symptoms include degraded signal quality and slower network speeds.

## Resolutions:

- **Configure access points** to use non-overlapping channels, such as 1, 6, and 11 in the 2.4 GHz band.
- **Implement automatic channel selection** to avoid overlap.



## Signal Degradation or Loss

Weak signal strength and high error rates due to distance or physical obstructions.

### Issues:

- **Signal degradation** leads to weaker signal strength and increased error rates.
- Symptoms include intermittent connectivity, slower data transfer rates, and higher packet loss.

### Resolutions:

- **Optimize access point placement** and use signal boosters or repeaters to extend coverage.



# Insufficient Wireless Coverage

Wireless connectivity is poor or nonexistent and can prevent users from accessing the network reliably.

## Issues:

- **Insufficient coverage** results in dead zones with poor or no connectivity.
- Symptoms include difficulty connecting to the network and unreliable connectivity in certain areas.

## Resolutions:

- **Conduct a wireless site survey** to identify coverage gaps and deploy additional access points as needed.



# Client Disassociation Issues

## Issues:

- **Frequent disassociation** causes unstable connections and constant reconnecting.
- Symptoms include interrupted network access and inconsistent performance.

## Resolutions:

- Ensure **strong and stable signal strength** and address potential sources of interference.



# Roaming Misconfiguration

## Issues:

- **Poorly configured roaming** can lead to slow handoffs between access points, causing temporary disconnections.
- Symptoms include lag during movement within the network and dropped connections.

## Resolutions:

- **Optimize roaming settings** on access points to facilitate smooth transitions between them.



## CompTIA Network+ N10-009 Course Notes

# Lesson 25

## Using Network Tools



## CompTIA Network+ N10-009 Course Notes

# Software Tools

Software tools are essential for managing, analyzing, and securing networks.

They range from **diagnostic utilities** that help in identifying and resolving network issues to **monitoring tools** that track the performance and security of the network infrastructure.

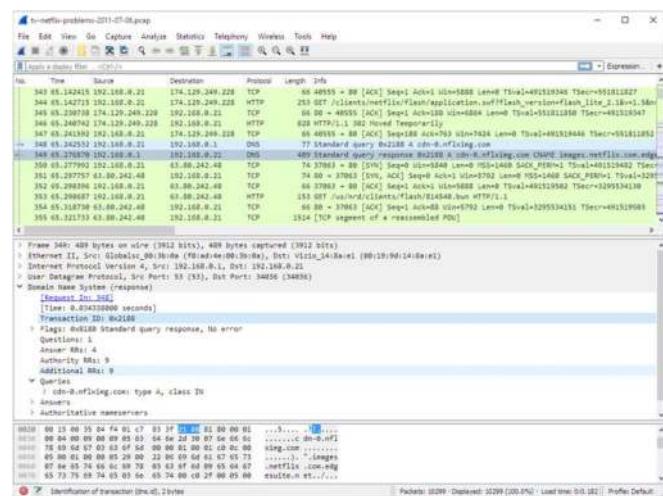


## CompTIA Network+ N10-009 Course Notes

# Protocol Analyzer/Packet Capture

Software that **captures** data packets traveling over a network.

It allows for **detailed analysis** of network traffic to identify issues, monitor performance, and ensure secure data transmission.



A screenshot of the Wireshark network traffic analyzer. The interface shows a list of captured frames, each with detailed information including source and destination IP addresses, port numbers, and protocol type. The list includes various protocols such as DNS, HTTP, and TCP. Below the list, there is a hex dump and ASCII representation of selected bytes, along with a timeline showing the sequence of events. The status bar at the bottom indicates the total number of packets (10299), displayed packets (10299), and load time (0.001).





## CompTIA Network+ N10-009 Course Notes

# Command Line Tools

Command line tools are foundational for network administration and troubleshooting.

These text-based interfaces offer **precise control over network devices**, such as routers, switches, and servers, allowing for detailed management and diagnostics.



## CompTIA Network+ N10-009 Course Notes

# Ping (Windows/Linux)

**Sends ICMP echo requests to a target host to test connectivity and measure round-trip time for messages sent to the target device.**

```
C:\Users\andy>ping google.com

Pinging google.com [142.251.35.174] with 32 bytes of data:
Reply from 142.251.35.174: bytes=32 time=4ms TTL=119
Reply from 142.251.35.174: bytes=32 time=4ms TTL=119
Reply from 142.251.35.174: bytes=32 time=6ms TTL=119
Reply from 142.251.35.174: bytes=32 time=6ms TTL=119

Ping statistics for 142.251.35.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 6ms, Average = 5ms
```



## Traceroute/tracert (Windows)

**Traces the path packets take from the source to the destination, showing each hop along the route.**

traceroute is used on Unix/Linux, and tracert on Windows.

```
C:\Users\andy>tracert google.com
Tracing route to google.com [142.250.65.206]
over a maximum of 30 hops:
1 <1 ms <1 ms <1 ms Fios_Quantum_Gateway.fios-router.home [192.168.1.1]
2 2 ms 1 ms 1 ms lo0-100.NYCMNY-VFTTP-341.verizon-gni.net
3 4 ms 4 ms 6 ms 100.41.32.0
4 * * * Request timed out.
5 7 ms 4 ms 6 ms customer.alter.net [63.125.121.2]
6 7 ms 4 ms 5 ms 142.251.247.113
7 6 ms 3 ms 4 ms 142.251.60.239
8 6 ms 4 ms 5 ms lga25s72-in-f14.le100.net [142.250.65.206]

Trace complete.
```



## CompTIA Network+ N10-009 Course Notes

# Nslookup(Windows)

**Queries DNS servers to find the IP address associated with a hostname (nslookup) or to get DNS information about a domain (dig).**

```
C:\Users\andy>nslookup
Default Server: Fios_Quantum_Gateway.fios-router.home
Address: 192.168.1.1

> google.com
Server: Fios_Quantum_Gateway.fios-router.home
Address: 192.168.1.1

Non-authoritative answer:
Name: google.com
Addresses: 2607:f8b0:4006:820::200e
           142.250.65.206
```



# CompTIA Network+ N10-009 Course Notes

# Tcpdump (Linux)

A powerful command-line packet analyzer; **it captures or filters TCP/IP packets** that are received or transmitted over a network.



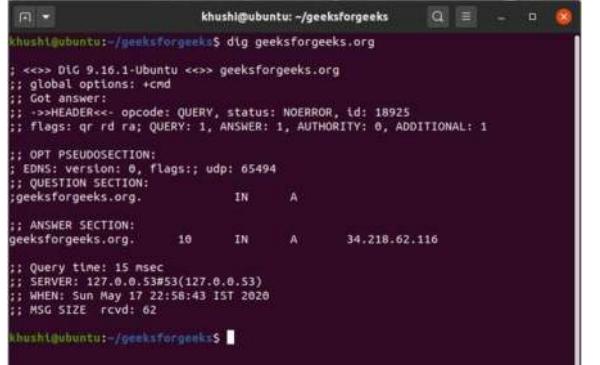
## CompTIA Network+ N10-009 Course Notes

# Dig (Linux)

**Dig** (Domain Information Groper) is a powerful command-line tool used for **querying DNS (Domain Name System) servers**.

**Retrieves detailed information** about DNS records, such as A, AAAA, CNAME, MX, and NS records.

**Diagnoses DNS issues** by providing insights into domain name resolution and server responses.



```
khushi@ubuntu:~/geeksforgeeks$ dig geeksforgeeks.org
; <>> DIG 9.16.1-Ubuntu <><> geeksforgeeks.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18925
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
geeksforgeeks.org.           IN      A
;; ANSWER SECTION:
geeksforgeeks.org.           10     IN      A      34.218.62.116
;; Query time: 15 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun May 17 22:58:43 IST 2020
;; MSG SIZE rcvd: 62
khushi@ubuntu:~/geeksforgeeks$
```

[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)

674



## CompTIA Network+ N10-009 Course Notes

### netstat

**Displays network connections** (both incoming and outgoing), routing tables, and a number of network interface statistics.

```
C:\Users\andy>netstat -a

Active Connections

Proto  Local Address          Foreign Address        State
TCP    0.0.0.0:135           DESKTOP-ATMVBQA:0   LISTENING
TCP    0.0.0.0:445           DESKTOP-ATMVBQA:0   LISTENING
TCP    0.0.0.0:3389          DESKTOP-ATMVBQA:0   LISTENING
TCP    0.0.0.0:5040          DESKTOP-ATMVBQA:0   LISTENING
TCP    0.0.0.0:5357          DESKTOP-ATMVBQA:0   LISTENING
TCP    0.0.0.0:7680          DESKTOP-ATMVBQA:0   LISTENING
TCP    0.0.0.0:8019          DESKTOP-ATMVBQA:0   LISTENING
```



## CompTIA Network+ N10-009 Course Notes

# ipconfig/ifconfig/ip

**Displays or configures the network configuration of a device.**

ipconfig is used on Windows,  
ifconfig on older Unix/Linux systems, and ip on modern Linux systems.

```
C:\Users\andy>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::4cb0:2e50:101d:a55e%15
  IPv4 Address. . . . . : 192.168.20.35
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . : fios-router.home
  Link-local IPv6 Address . . . . . : fe80::33a6:2de1:13fe:e1a3%12
  IPv4 Address. . . . . : 192.168.1.171
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1
```



## CompTIA Network+ N10-009 Course Notes

arp

Displays or modifies the IP-to-MAC address **translation tables** used by the Address Resolution Protocol (ARP).

```
C:\Users\andy>arp -a

Interface: 192.168.1.171 --- 0xc
  Internet Address      Physical Address      Type
  192.168.1.1           20-c0-47-38-c2-ec  dynamic
  192.168.1.80          a8-a1-59-29-11-1c  dynamic
  192.168.1.95          00-11-32-b5-1f-a8  dynamic
  192.168.1.129         cc-75-e2-3b-7a-0a  dynamic
  192.168.1.130         cc-75-e2-99-4e-c3  dynamic
  192.168.1.156         20-50-e7-97-b7-b2  dynamic
  192.168.1.165         ac-3a-7a-db-60-8d  dynamic
  192.168.1.177         f8-04-2e-e0-52-ec  dynamic
  192.168.1.178         dc-54-d7-13-b6-12  dynamic
  192.168.1.194         00-40-7f-b4-b6-b8  dynamic
  192.168.1.196         cc-9e-a2-2d-d5-c4  dynamic
```



## CompTIA Network+ N10-009 Course Notes

# nmap

A network scanning tool that **discovers devices and services on a network** by sending packets and analyzing the responses.

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-29 18:12 CDT
Nmap scan report for 10.0.0.1
Host is up (0.015s latency).
Nmap scan report for 10.0.0.23
Host is up (0.00081s latency).
Nmap scan report for 10.0.0.89
Host is up (0.0075s latency).
Nmap scan report for 10.0.0.138
Host is up (0.057s latency).
Nmap scan report for 10.0.0.164
Host is up (0.012s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 28.34 seconds
```



## CompTIA Network+ N10-009 Course Notes

# Link Layer Discovery Protocol (LLDP) / Cisco Discovery Protocol (CDP)

LLDP and CDP are **network discovery protocols** used to exchange information about devices on the same network.

LLDP: A **vendor-neutral protocol** used to discover and share information between network devices, such as identity, capabilities, and neighbors.

- Usage: Helps in identifying network topology, troubleshooting connectivity issues, and ensuring proper network configuration.

CDP: A **Cisco-proprietary protocol** similar to LLDP, specifically used in Cisco networks to share information about directly connected Cisco devices.

- Usage: Facilitates network management and troubleshooting by providing detailed information about neighboring Cisco devices.



## CompTIA Network+ N10-009 Course Notes

# Speed Tester

A **speed tester** is a tool used to **measure the performance** of a network connection by testing the upload and download speeds.

### Functions:

- **Evaluates the bandwidth capacity** and performance of a network connection.
- **Identifies potential issues** such as bandwidth bottlenecks, latency, and jitter.

### Usage:

- Commonly used to verify internet speed and ensure service level agreements (SLAs) are met.
- **Helps in troubleshooting performance** issues by pinpointing slow network segments.



## CompTIA Network+ N10-009 Course Notes

# Hardware Tools

Hardware tools are essential in diagnosing, troubleshooting, and maintaining network infrastructure.

These tools provide network administrators with the ability to **identify and resolve physical layer problems**, ensuring optimal network performance and reliability.



## CompTIA Network+ N10-009 Course Notes

# Toner

A toner is a tool used to trace and identify individual wires or cables within a bundle.

### Functions:

- Consists of a **tone generator and a probe**; the generator sends a signal through the cable, which the probe detects.
- Helps in identifying and locating cables in complex wiring systems.

### Usage:

- Commonly **used in cable installations and maintenance** to ensure correct wiring and organization





## Cable Tester

A cable tester is used to **verify the integrity and performance of network cables.**

### Functions:

- **Tests for continuity**, signal strength, and wiring faults such as shorts, opens, and cross connections.

### Usage:

- Essential for **validating new cable installations** and diagnosing existing cable issues.





## CompTIA Network+ N10-009 Course Notes

# Taps

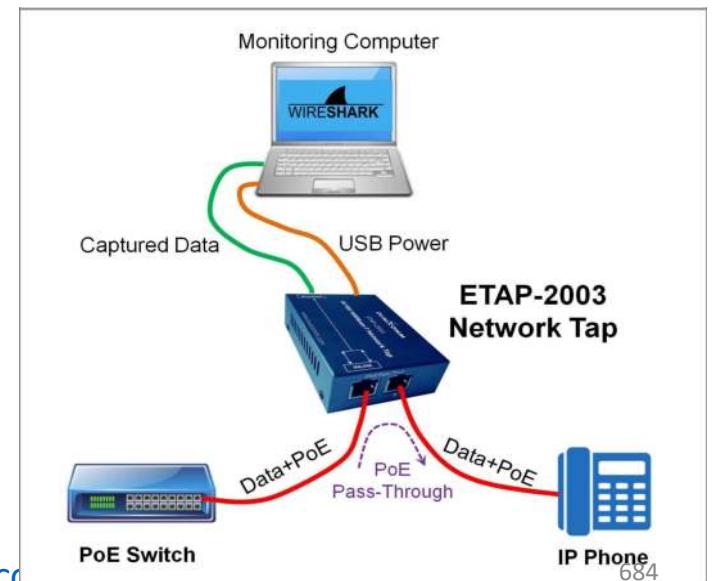
A network tap is a hardware device that provides a way to **access the data flowing across a network cable**.

### Functions:

- **Creates a copy of the data packets** for monitoring and analysis without interrupting the network flow.

### Usage:

- Used in **network monitoring and security** applications to analyze traffic for troubleshooting, performance monitoring, and intrusion detection.



[www.tiaedu.com](http://www.tiaedu.com)/[www.tiaexams.com](http://www.tiaexams.com)...



## CompTIA Network+ N10-009 Course Notes

# Wi-Fi Analyzer

A Wi-Fi analyzer is a tool used to **scan and analyze wireless network signals**.

### Functions:

- **Detects Wi-Fi networks**, measures signal strength, identifies channel usage, and detects interference sources.

### Usage:

- **Helps in optimizing Wi-Fi network performance** by identifying the best channels and detecting issues such as interference and weak signals.





## Visual Fault Locator

A visual fault locator is a tool used to **identify faults in fiber optic cables**.

### Functions:

- Emits a **visible red laser light** that travels through the fiber, revealing breaks, bends, or faulty connectors.

### Usage:

- **Used in fiber optic cable installation** and maintenance to quickly locate and diagnose issues.





## CompTIA Network+ N10-009 Course Notes

# Basic Networking Device Commands

Basic networking device commands are fundamental tools for network administrators in diagnosing and resolving network issues.

These commands allow for **quick assessment and troubleshooting** of network devices, such as routers, switches, and servers.

By using commands to display configuration settings, check connectivity, monitor performance, and view logs, administrators can **identify and address problems efficiently**.





## show mac-address-table

The show mac-address-table command displays the MAC address table of a network switch.

### Usage:

- Helps in identifying which MAC addresses are associated with which ports.
- Useful for **troubleshooting connectivity issues** and ensuring proper network segmentation.

### Benefits:

- **Provides visibility into network device connections**, aiding in detecting unauthorized devices and optimizing port usage.



## show route

The show route command displays the routing table of a router or **Layer 3 switch**.

### Usage:

- Shows active routes, route sources, and next-hop addresses.
- Essential for verifying correct routing and diagnosing routing issues.

### Benefits:

- Helps ensure that data packets are taking the optimal path through the network, improving performance and reliability.



## show interface

The **show interface** command provides detailed information about the **status and configuration of network interfaces**.

### Usage:

- **Displays interface status**, traffic statistics, and error counts.
- Useful for diagnosing issues such as link failures, duplex mismatches, and interface errors.

### Benefits:

- **Enables monitoring of interface health and performance**, facilitating prompt resolution of physical layer problems.



## show config

The show config command displays the current configuration of the network device.

### Usage:

- Shows all configured settings, including IP addresses, routing protocols, and security settings.
- Useful for verifying configuration consistency and identifying misconfigurations.

### Benefits:

- Assists in maintaining and auditing network device configurations, ensuring alignment with network policies and standards.



## show arp

The show arp command displays the **ARP table**.

### Usage:

- Maps IP addresses to MAC addresses.
- Useful for troubleshooting IP-to-MAC address resolution issues.

### Benefits:

- Helps in **identifying and resolving connectivity issues** related to ARP, ensuring reliable IP communication.



## show vlan

The show vlan command displays information about **VLAN** configurations on a switch.

### Usage:

- Shows VLAN IDs, names, and associated ports.
- Useful for verifying VLAN setup and troubleshooting VLAN-related issues.

### Benefits:

- Ensures proper network segmentation and enhances security by managing VLAN configurations effectively.



## show power

The show power command provides information about the **power status and consumption of PoE devices**.

### Usage:

- Displays power allocation, usage, and available power.
- Useful for managing PoE budgets and diagnosing power-related issues.

### Benefits:

- Helps ensure that PoE devices receive adequate power, maintaining network reliability and performance.