CompTIA Network+ N10-009

Full Learning Guide

Welcome to your complete Network+ N10-009 learning guide.
*This manual is designed to **teach you every domain deeply**, not just summarize.*

Learning Objectives and Expectations

You'll master:

- Every critical networking concept you must know
- How protocols, devices, and designs fit together
- How to think like a networking professional, not just memorize

Each domain guide includes:

- Full concept breakdowns and real-world implementation examples
- Common troubleshooting and configuration scenarios
- Exam tips and memory tricks

Network+ N10-009 Domains

Each domain is weighted differently, with Network Troubleshooting being the largest:

- **Domain 1:** Networking Concepts (23%)
- **Domain 2:** Network Implementation (20%)
- **Domain 3:** Network Operations (19%)
- **Domain 4:** Network Security (14%)
- **Domain 5:** Network Troubleshooting (24%)

Quick Reminder: How the Exam Works

- **Number of Questions:** Up to 90
- **Format:** Multiple choice + Performance-Based Questions (PBQs)
- **Time Limit:** 90 minutes
- **Passing Score:** 720/900 (about 80%)
- **Test Provider:** Pearson VUE (in person or online)

Top 10 Network+ Exam Tips

1. **Review Core Topics Lightly Before the Exam**: ports, protocols, OSI/TCP-IP models, VLANs, routing protocols, and subnetting.
2. **Get Good Sleep the Night Before:** A clear mind is your best tool for scenario-based and troubleshooting questions.
3. **Arrive Early and Be Prepared**: Bring valid IDs, prepare your workspace if testing remotely, and avoid last-minute tech issues.
4. **Stay Calm and Confident**: Deep breaths help regulate focus and memory recall. You've prepared for this.
5. **Skip PBQs if Needed — Come Back Later**: Don't let a simulation eat 10 minutes. Flag and return after finishing multiple-choice.
6. **Manage Your Time Strategically**: Average ~1 minute per question. Mark and return if stuck — don't waste 5 minutes on one item.
7. **Read Questions Very Carefully**: Look for qualifiers like **NOT**, **BEST**, or **FIRST**. They change the whole question.
8. **Use Elimination First**: Cross out the clearly wrong answers to improve your odds when guessing.
9. **Never Leave a Question Unanswered**: There's no penalty for guessing. If time is running out, mark anything — you might get it right.
10. **Use Extra Time Wisely to Review Flags**: If you're unsure and marked it, revisit if time permits — but only change your answer if you're certain.

Remember — you don't need to be perfect to pass!

The Network+ **passing score is about 80%**. That means you can miss up to 15–18 questions and still succeed.

Don't panic if you don't know one or two topics. Stay calm, keep working through the test, and **trust your preparation**.

Domain 1: Networking Concepts (23%)

Goal of Domain 1:

This domain provides the foundational concepts for understanding how networks operate, including models, protocols, topologies, services, and traffic types. Mastery of this domain is essential for the rest of the exam.

1.1 (OSI) model layers and encapsulation concepts

Key Concepts to Learn:

- OSI Model – 7 Layers
- Encapsulation and decapsulation
- Protocol data units (PDUs)
- Layer-specific functions and examples

OSI Model Overview

The **OSI (Open Systems Interconnection)** model is a conceptual framework used to understand and describe how data flows across networks. It is composed of **7 layers**, from physical transmission of data to end-user application access.

Layer 7 – Application

- Interfaces directly with end-user applications.
- Responsible for network services like file transfers, email, and DNS.
- Protocols: HTTP, FTP, SMTP, DNS, SNMP

Layer 6 – Presentation

- Formats and translates data between the application and network.
- Handles encryption, compression, and character encoding.
- Example functions: JPEG conversion, ASCII translation, TLS encryption

Layer 5 – Session

- Manages sessions between applications.
- Responsible for connection setup, maintenance, and termination.
- Examples: NetBIOS, RPC

Layer 4 – Transport

- Provides end-to-end communication services for applications.
- Handles segmentation, error control, and flow control.
- Protocols: TCP (reliable), UDP (unreliable)
- PDU: Segment

Layer 3 – Network

- Handles logical addressing and routing.
- Determines best path to the destination using routing protocols.
- Protocols: IP, ICMP, IGMP, OSPF, BGP
- Devices: Routers
- PDU: Packet

Layer 2 – Data Link

- Provides node-to-node communication and error detection.
- Uses MAC addresses for identification.
- Protocols: Ethernet, PPP, HDLC, Frame Relay
- Devices: Switches, bridges
- PDU: Frame

Layer 1 – Physical

- Transmits raw bits over a physical medium.
- Includes electrical signals, light pulses, cables, connectors.
- Devices: Hubs, repeaters, network cables
- PDU: Bits

Memory Aid:

- Bottom-Up: Please Do Not Throw Sausage Pizza Away
- Top-Down: All People Seem To Need Data Processing

Encapsulation and Decapsulation

Encapsulation is the process of wrapping data with protocol-specific headers as it moves **down** the OSI layers before transmission.

Decapsulation is the reverse process occurring at the receiving device as data moves **up** the OSI layers.

Example: Sending an email

- Application Layer (SMTP adds header)
- Transport Layer (TCP adds port info)
- Network Layer (IP adds source/destination IP)
- Data Link Layer (MAC address info)
- Physical Layer (transmits as bits)

1.2 Compare and contrast the use of networking hardware

Key Concepts to Learn:

- Roles and layers of devices: routers, switches, firewalls, access points
- Physical vs. virtual appliances
- Control and data planes

Network Devices

Router

- Operates at Layer 3
- Directs packets between different networks
- Uses IP addresses to determine routing paths
- Can perform NAT, DHCP, ACL filtering

Switch

- Operates at Layer 2 (Layer 3 switches add routing)
- Forwards traffic based on MAC addresses
- Creates separate collision domains
- Can support VLANs and PoE

Firewall

- Operates across Layers 3–7
- Filters traffic based on rules
- Next-gen firewalls can inspect application-layer data

Wireless Access Point (AP)

- Operates at Layer 2
- Provides 802.11 wireless connectivity to clients
- May be autonomous or controller-based

Modem

- Modulates/demodulates analog signals for digital communication
- Connects to ISP via DSL, cable, or fiber

Hub

- Operates at Layer 1
- Repeats incoming signal to all ports
- Creates a single collision domain

Bridge

- Connects two LAN segments
- Learns MAC addresses and filters traffic accordingly

Load Balancer

- Distributes traffic among multiple servers
- Can operate at Layer 4 or Layer 7
- Improves performance and redundancy

IDS/IPS

- IDS (Intrusion Detection System): Monitors and alerts
- IPS (Intrusion Prevention System): Actively blocks malicious traffic

Proxy Server

- Intermediary between client and destination
- Can cache content and filter traffic

VPN Concentrator

- Manages multiple VPN connections
- Terminates VPN tunnels and performs encryption/decryption

Physical vs Virtual Appliances

Physical Appliances

- Hardware-based devices
- Dedicated function (e.g., Cisco ASA firewall)

Virtual Appliances

- Software-based, runs on hypervisors or cloud platforms
- Common in SDN and virtualized environments

1.3 Summarize cloud concepts and connectivity options

Key Concepts to Learn:

- Cloud models (IaaS, PaaS, SaaS)
- Deployment models (Public, Private, Hybrid)
- Cloud connectivity methods
- NFV, VPC, Direct Connect

Cloud Service Models

IaaS (Infrastructure as a Service)

- Provides virtualized hardware resources
- You manage OS, apps, and data
- Examples: AWS EC2, Azure VMs

PaaS (Platform as a Service)

- Provider manages OS and infrastructure
- You manage applications and data
- Examples: Google App Engine, Heroku

SaaS (Software as a Service)

- Provider manages everything
- You use the software through browser/app
- Examples: Gmail, Office 365, Salesforce

Cloud Deployment Models

Public Cloud

- Services offered over the internet to multiple customers
- Shared infrastructure

Private Cloud

- Infrastructure dedicated to a single organization
- May be on-premises or hosted

Hybrid Cloud

- Combines public and private
- Allows data and applications to move between environments

Connectivity Options

VPN

- Site-to-site or remote access
- Encrypted tunnel over the public internet

Direct Connect / ExpressRoute

- Private dedicated connection to cloud provider
- More secure and consistent performance

VPC (Virtual Private Cloud)

- Isolated virtual network within a cloud provider
- Define subnets, route tables, gateways

NFV (Network Function Virtualization)

- Replaces traditional hardware with virtual appliances
- Example: virtual firewalls, routers

1.4 Explain common networking protocols and their use cases

Key Concepts to Learn:

- Common protocol ports and purposes
- TCP vs UDP
- Application layer protocols

TCP vs UDP

TCP (Transmission Control Protocol)

- Connection-oriented
- Reliable (ACKs, retransmissions)
- Slower but accurate

UDP (User Datagram Protocol)

- Connectionless
- Unreliable but faster
- Used in VoIP, video, DNS

Important Protocols

Protocol	Port	Transport	Function
HTTP	80	TCP	Web browsing
HTTPS	443	TCP	Secure web
FTP	20/21	TCP	File transfer
SFTP	22	TCP	Secure FTP
SSH	22	TCP	Secure remote login
Telnet	23	TCP	Unsecure remote login
SMTP	25	TCP	Send email
IMAP	143	TCP	Retrieve email
POP3	110	TCP	Retrieve email
DNS	53	UDP/TCP	Name resolution
DHCP	67/68	UDP	Dynamic IP assignment
SNMP	161/162	UDP	Network monitoring
RDP	3389	TCP	Remote desktop
SMB	445	TCP	File/print sharing
LDAP	389	TCP	Directory services
SIP	5060/5061	UDP	VoIP signaling

1.5 Explain common networking services

Key Concepts to Learn:

- DHCP and DNS
- NAT and PAT
- VPN and tunneling
- NTP, IPAM

DHCP (Dynamic Host Configuration Protocol)

- Assigns IP address, subnet mask, gateway, DNS
- Process: DORA (Discover, Offer, Request, Acknowledge)

DNS (Domain Name System)

- Resolves domain names to IP addresses
- Record types: A (IPv4), AAAA (IPv6), MX (mail), CNAME (alias), PTR (reverse)

NAT (Network Address Translation)

- Translates private to public IPs
- Allows multiple devices to share one IP

PAT (Port Address Translation)

- Uses different port numbers to distinguish internal clients

VPN

- Secure tunnel over untrusted network
- Types: Site-to-site, Remote access
- Protocols: IPsec, SSL/TLS

NTP (Network Time Protocol)

- Synchronizes time across devices
- Uses hierarchical strata of servers

IPAM (IP Address Management)

- Tracks IP allocations and subnet usage

1.6 Compare and contrast various types of network traffic

Key Concepts to Learn:

- Traffic types: Unicast, Broadcast, Multicast, Anycast
- IPv4 and IPv6 traffic
- Control vs. data plane

Unicast

- One-to-one communication

Broadcast

- One-to-all (IPv4 only)
- Used for ARP, DHCP Discover

Multicast

- One-to-many (specific group)
- Uses 224.0.0.0/4 IPv4 range

Anycast

- One-to-nearest (used in IPv6 and DNS)

1.7 Compare and contrast the characteristics of network topologies, types, and technologies

Key Concepts to Learn:

- Physical vs logical topologies
- Network types: LAN, WAN, MAN, CAN, PAN
- WAN types: MPLS, Metro-E, Leased Line, DSL

Topologies

- **Star:** All nodes connect to a central switch
- **Bus:** All nodes on one backbone
- **Ring:** Nodes in a circular path
- **Mesh:** Every node connects to every other node
- **Hybrid:** Combination of topologies

Network Types

- **LAN:** Local Area Network
- **WAN:** Wide Area Network
- **MAN:** Metropolitan Area Network
- **CAN:** Campus Area Network
- **PAN:** Personal Area Network

WAN Technologies

- **MPLS:** Private circuit, labeled switching
- **Metro-E:** Ethernet across city area
- **Leased Line (T1/E1):** Dedicated bandwidth
- **DSL/Cable:** Broadband over existing lines

1.8 Summarize emerging networking technologies

Key Concepts to Learn:

- SDN, SD-WAN
- Zero Trust
- Infrastructure as Code (IaC)
- VXLAN, SASE, SSE
- IPv6 transition mechanisms

SDN (Software Defined Networking)

- Centralized control plane
- Uses API and controllers (OpenFlow)

SD-WAN

- Software-driven WAN routing
- Enables policy-based traffic routing over multiple link types

Zero Trust

- "Never trust, always verify"
- Every device/user must authenticate regardless of location

Infrastructure as Code

- Networks and infrastructure defined in version-controlled code
- Tools: Terraform, Ansible

VXLAN (Virtual Extensible LAN)

- Extends VLANs across Layer 3 networks
- Supports large-scale segmentation

SASE (Secure Access Service Edge)

- Combines SD-WAN + cloud security
- Enforces policies at edge, closer to users

SSE (Security Service Edge)

- Security side of SASE
- Includes CASB, SWG, ZTNA

IPv6 Transition

- Dual Stack: Runs IPv4 and IPv6 simultaneously
- Tunneling: Encapsulate IPv6 inside IPv4 (6to4, Teredo)
- NAT64/DNS64: Allows IPv6 clients to communicate with IPv4-only servers

Domain 1 Summary

Things You Must Memorize:

- OSI layers, functions, and examples
- Port numbers and protocols
- Cloud models and deployment types
- Differences between SDN, SD-WAN, SASE
- Traffic types: unicast, broadcast, multicast, anycast
- Common services: DHCP, DNS, NAT, NTP

Domain 2: Network Implementation (20%)

Goal of Domain 2:

This domain covers the actual deployment and configuration of networking devices and technologies including routing, switching, wireless, and physical installations. It emphasizes practical implementation skills and is foundational for most real-world IT tasks.

2.1 Compare and contrast routing technologies and bandwidth management concepts

Key Concepts to Learn:

- Static vs Dynamic routing
- Routing protocols: RIP, OSPF, EIGRP, BGP
- Administrative Distance
- Metric, convergence, and failover
- Route summarization and longest prefix match
- QoS and traffic shaping
- NAT/PAT
- First Hop Redundancy Protocols (FHRP)

Static Routing

- **Manually configured routes**
- Use cases: Small networks, stub networks
- Benefits: Simplicity, low overhead, security
- Drawbacks: No auto-failover, no scalability

Dynamic Routing

- **Uses routing protocols to automatically exchange routes**
- Benefits: Scales well, adapts to network changes
- Drawbacks: Higher CPU and bandwidth usage

Routing Protocol Types

Distance-Vector

- Shares entire routing table
- Slow convergence
- Example: **RIP**
  - Max 15 hops
  - Metric: hop count
  - Not suitable for large networks

Link-State

- Builds complete topology map
- Fast convergence
- Example: **OSPF**
  - Metric: Cost (based on bandwidth)
  - Supports VLSM and CIDR
  - Hierarchical design with Areas

Hybrid (Advanced Distance-Vector)

- Combines best of both types
- Example: **EIGRP** (Cisco proprietary)

Path-Vector

- Maintains path info
- Example: **BGP**
  - Used for internet routing
  - Uses AS numbers and attributes
  - Slow convergence, policy-based

Administrative Distance (AD)

- Determines trustworthiness of routing source
- Lower value = more preferred
- Examples:
  - Connected: 0
  - Static: 1
  - EIGRP: 90
  - OSPF: 110
  - RIP: 120
  - External BGP: 20

Metric and Longest Prefix Match

- **Metric** determines best path within a protocol
  - RIP: Hop count
  - OSPF: Cost
  - EIGRP: Bandwidth + delay
- **Longest prefix match** overrides AD
  - 192.168.1.0/24 preferred over 192.168.0.0/16

Route Summarization

- Combines multiple routes into one
- Reduces routing table size
- Requires contiguous networks
- E.g., 192.168.0.0/24 + 192.168.1.0/24 = 192.168.0.0/23

Convergence

- Time taken for routers to agree on topology changes
- Fast convergence = more stable network
- Link-state converges faster than distance-vector

First Hop Redundancy Protocols (FHRP)

- Provide virtual gateway IP
- Allow transparent failover
- Types:
  - **HSRP** (Cisco): active/standby
  - **VRRP** (Open): master/backup
  - **GLBP** (Cisco): load balancing among gateways

NAT and PAT

- **NAT**: Translates private to public IP
- **PAT**: Many-to-one translation using port numbers
- Benefits: conserves IPv4 addresses, adds security

Bandwidth Management and QoS

Traffic Shaping

- Delays packets to conform to bandwidth policy
- Smooths bursty traffic

Policing

- Drops or marks traffic that exceeds limit
- Used by ISPs for rate enforcement

Quality of Service (QoS)

- Ensures performance for critical applications
- Prioritization based on:
  - Application (VoIP, video)
  - User
  - Protocol (UDP/TCP)
- Techniques:
  - Queuing (FIFO, priority, weighted fair)
  - Marking (DSCP, CoS)
  - Classification (by IP, port, etc.)

2.2 Given a scenario, configure and verify switching technologies

Key Concepts to Learn:

- VLANs, Trunking (802.1Q)
- Native VLAN
- Inter-VLAN routing
- Port types: access, trunk
- STP (Spanning Tree Protocol)
- Link aggregation (LACP/EtherChannel)
- Port security
- PoE/PoE+ standards
- Switch stacking

VLANs (Virtual LANs)

- Logically segment network at Layer 2
- Each VLAN = separate broadcast domain
- Assign ports to VLANs
- VLAN IDs: 1–4094 (1 = default)

Access Port

- Carries traffic for one VLAN
- Connects to end device

Trunk Port

- Carries multiple VLANs
- Tags frames with VLAN ID using 802.1Q

Native VLAN

- VLAN that is untagged on a trunk
- Must match on both ends

Inter-VLAN Routing

- VLANs can't communicate without Layer 3 device
- Methods:
  - **Router-on-a-stick** (subinterfaces)
  - **Multilayer switch (SVI)**

STP (Spanning Tree Protocol)

- Prevents loops in Layer 2 networks
- Blocks redundant links
- Root bridge election (lowest bridge ID)
- Port roles:
  - Root Port, Designated Port, Blocking
- Versions:
  - 802.1D (original), 802.1w (Rapid STP), 802.1s (MSTP)
- Enhancements:
  - **PortFast** (for access ports)
  - **BPDU Guard** (shuts down on unexpected BPDU)

Link Aggregation

- Combine multiple links into one logical link
- Increases bandwidth and redundancy
- Protocols:
  - **LACP (IEEE 802.3ad)**
  - **PAgP** (Cisco proprietary)

Port Security

- Limits MAC addresses on a port
- Actions on violation: shutdown, restrict, protect
- Enhances access control

Power over Ethernet (PoE)

- Provides power and data over Ethernet
- Standards:
  - 802.3af (PoE): 15.4W
  - 802.3at (PoE+): 25.5W
  - 802.3bt (PoE++): up to 90W

Switch Stacking

- Multiple switches act as one
- Single management point
- Used for scalability and redundancy

2.3 Given a scenario, configure and verify wireless technologies

Key Concepts to Learn:

- Wireless standards: 802.11a/b/g/n/ac/ax
- Frequencies and channels
- Antenna types
- Wireless security: WPA2/WPA3
- Authentication: PSK, 802.1X
- SSID, BSSID, ESSID
- Wireless controllers

Wireless Standards

Standard	Band	Max Speed	Notes
802.11a	5 GHz	54 Mbps	Legacy
802.11b	2.4 GHz	11 Mbps	Legacy
802.11g	2.4 GHz	54 Mbps	Legacy
802.11n	2.4/5 GHz	600 Mbps	Introduced MIMO
802.11ac	5 GHz	>1 Gbps	Uses MU-MIMO, wider channels
802.11ax	2.4/5/6 GHz	>10 Gbps	Wi-Fi 6, OFDMA

Channels and Interference

2.4 GHz

- Channels: 1–11 (US)
- Non-overlapping: 1, 6, 11

5 GHz

- More channels
- Less interference
- Subject to DFS

6 GHz

- Wi-Fi 6E
- Clean spectrum

Antenna Types

- **Omni-directional:** 360° coverage
- **Directional:** Focused coverage (Yagi, parabolic)
- Use cases:
  - Indoor coverage = omni
  - Long-distance bridge = directional

Wireless Security

WEP

- Deprecated, weak security

WPA

- TKIP encryption, no longer recommended

WPA2

- AES encryption, secure
- Modes:
  - Personal (PSK)
  - Enterprise (802.1X + RADIUS)

WPA3

- Replaces PSK with SAE
- Stronger encryption

Authentication Types

PSK (Pre-Shared Key)

- Single passphrase
- Easy to deploy, poor scalability

802.1X

- Uses RADIUS server
- Per-user authentication
- Supports certificates or credentials

Wireless Architecture

SSID

- Network name broadcasted by AP

BSSID

- MAC address of the AP radio

ESSID

- Same SSID across multiple APs for roaming

Wireless Controller

- Manages multiple APs
- Centralizes configuration and updates

CAPWAP/LWAPP

- Protocols between AP and controller

2.4 Explain the purposes of various network services

Key Concepts to Learn:

- DHCP and relay
- DNS resolution
- NTP, IPAM
- IP addressing schemes (public/private, APIPA)

DHCP (Dynamic Host Configuration Protocol)

Functions:

- Assign IP, subnet mask, gateway, DNS

Process:

- Discover → Offer → Request → Acknowledge (DORA)

DHCP Options:

- Option 3 = Gateway
- Option 6 = DNS
- Option 15 = Domain Name

Relay Agent:

- Forwards DHCP packets between subnets
- Configured with ip helper-address

DNS (Domain Name System)

Function:

- Resolves FQDNs to IP addresses

Record Types:

- A = IPv4
- AAAA = IPv6
- MX = Mail server
- CNAME = Alias
- PTR = Reverse DNS

Forward vs Reverse Lookup:

- Forward = name to IP
- Reverse = IP to name

IPAM (IP Address Management)

Tracks:

- IP allocations
- Subnet usage
- DHCP pools

Benefits:

- Prevents conflicts
- Supports audits
- Integrates with DNS and DHCP

NTP (Network Time Protocol)

Synchronizes clocks

- Critical for logs, security, Kerberos

Stratum levels:

- Stratum 0: atomic clock
- Stratum 1: connected to 0

- Stratum 2+: syncs from above

APIPA (Automatic Private IP Addressing)

Range:

- 169.254.0.0/16

Used when:

- DHCP server not reachable

Only allows:

- Local subnet communication

2.5 Explain common physical and logical network topologies

Key Concepts to Learn:

- Physical vs logical topology
- Common topologies: Star, Mesh, Ring, Bus
- Network types: LAN, WAN, MAN, CAN, PAN
- Point-to-point and multipoint

Topologies

Star

- All nodes connect to central switch
- Most common modern topology

Bus

- All nodes share single backbone
- Legacy, vulnerable to single point failure

Ring

- Nodes connected in a loop
- Data passes through each node

Mesh

- Every node connects to every other
- Provides high redundancy
- Full or partial mesh

Hybrid

- Mix of two or more topologies

Logical vs Physical

- **Physical:** Real layout of cables/devices
- **Logical:** How traffic flows

Network Types

LAN (Local Area Network)

- Small geographic area
- High-speed Ethernet/Wi-Fi

WAN (Wide Area Network)

- Large area: cities, countries
- Uses leased lines, MPLS

MAN (Metropolitan Area Network)

- Spans a city

CAN (Campus Area Network)

- Multiple buildings in one org

PAN (Personal Area Network)

- Close-range devices (Bluetooth)

Point-to-Point

- Direct link between two endpoints
- Common in WAN links

Point-to-Multipoint

- One central node connects to multiple endpoints
- Common in wireless or satellite links

Domain 2 Summary

Things You Must Memorize:

- Differences between RIP, OSPF, BGP, EIGRP
- VLAN and trunk configurations
- 802.11 standards and wireless security types
- DHCP relay and DNS record types
- Topology definitions and diagrams

Domain 3: Network Operations (19%)

Goal of Domain 3:

This domain covers the management, documentation, monitoring, and resilience of networks. It focuses on the daily processes that keep the network functional, secure, and recoverable.

3.1 Explain the purpose of organizational processes and policies

Key Concepts to Learn:

- Types of documentation (diagrams, inventories)
- Change and configuration management
- Asset and IP address management
- Life cycle and support processes
- SLAs and baselines

Documentation Types

Physical Network Diagram

- Maps the layout of cables, devices, and ports
- Helps with troubleshooting and planning

Logical Network Diagram

- Shows IP subnets, routing relationships, VLANs
- Useful for understanding data flows

Rack Diagram

- Visual layout of devices in racks (by rack units/U)
- Assists with installation and power planning

Cable Map

- Tracks where cables start and terminate (patch panels to jacks)
- Avoids confusion during moves or troubleshooting

Layer-Specific Diagrams

- Layer 1: Cables, interfaces
- Layer 2: VLANs, switches
- Layer 3: IP addresses, routers

Inventory and Asset Management

Asset Management

- Keeps track of all hardware and software
- Includes: Model, serial number, warranty status, location, assigned user

Licensing

- Records of software keys and usage rights
- Essential for compliance audits

Warranty and Support Contracts

- Document when warranties expire
- Schedule proactive replacements

IP Address Management (IPAM)

Tracks:

- IP assignments (static and DHCP)
- Subnet allocations
- Usage stats

Prevents:

- Conflicts, misuse, and overuse
- Enables planning for future growth

Change Management

Purpose:

- Ensure changes are planned, tested, and approved

Steps:

1. Request (proposal)
2. Review/approval
3. Implementation plan
4. Communication
5. Testing and rollback
6. Documentation

Benefits:

- Minimizes disruptions
- Tracks who changed what and when

Configuration Management

Baseline Configuration

- Standard settings for new devices
- Used for comparison and auditing

Version Control

- Track configuration changes over time
- Enables rollbacks if needed

Configuration Backups

- Regular automated exports of switch/router/firewall configs

---

Life Cycle Management

Stages:

1. Procurement
2. Deployment
3. Maintenance
4. EOL (End-of-Life)
5. Decommissioning

Include:

- Update schedules
- Patch tracking
- Secure disposal policies

Service Level Agreements (SLAs)

Defines:

- Uptime (e.g., 99.9%)
- Latency
- Response times
- Support levels

Used for:

- Contracts with ISPs, cloud vendors
- Internal IT guarantees

Baseline Documentation

Captures:

- Normal performance stats (CPU, bandwidth, error rate)
- Used to detect anomalies

Includes:

- Network maps
- System logs
- Historical performance trends

3.2 Given a scenario, use appropriate statistics and sensors to ensure network availability

Key Concepts to Learn:

- Network monitoring protocols (SNMP, NetFlow, Syslog)
- Tools (NMS, SIEM, packet analyzers)

- Performance metrics
- Scheduled vs ad hoc monitoring
- Port mirroring, baselining

SNMP (Simple Network Management Protocol)

Versions:

- v1/v2c: Community strings (insecure)
- v3: Encrypted and authenticated

Port: 161 (queries), 162 (traps)

Use:

- Collect data like bandwidth, uptime, CPU
- Receive trap alerts on events

Components:

- Agent (on device)
- NMS (management station)
- MIB (Management Information Base)

NetFlow/sFlow/IPFIX

Use:

- Collect flow statistics (who talks to whom, how much)

Used for:

- Bandwidth analysis
- Application usage monitoring
- Security alerts (DDoS, scanning)

Syslog

Port: 514 (UDP)

Centralized log collection

- Routers, switches, servers send logs to a central server
- Useful for audit trails and security

Performance Metrics

Availability: Uptime percentage
Latency: Time for packet to travel
Jitter: Variation in latency
Error rate: CRC errors, packet drops
Throughput: Actual data rate
Utilization: Percentage of capacity used

Baselining

Establish "normal" performance

- Helps identify unusual behavior (spikes, slowdowns)

Used for:

- Capacity planning
- Security alerting (deviation from baseline)

Scheduled vs Ad Hoc Monitoring

Scheduled:

- Ongoing checks (SNMP polling, ping tests)
- Alerts if thresholds exceeded

Ad Hoc:

- Manual checks during troubleshooting

Packet Capture

Tools: Wireshark, tcpdump
Used for:

- Deep analysis of network issues
- Checking for retransmissions, malformed packets
- Inspecting protocol behavior

Port Mirroring (SPAN)

Switch copies traffic from one port to another

- Connect to analyzer or IDS/IPS
- Passive monitoring without disrupting traffic

SIEM (Security Information and Event Management)

Collects logs from many sources

- Correlates events
- Sends alerts on unusual activity
- Helps with compliance (PCI, HIPAA)

3.3 Explain disaster recovery and high availability concepts

Key Concepts to Learn:

- RPO and RTO
- Backup types and testing
- Redundancy models
- Disaster recovery sites
- High availability setups

Key Metrics

RPO (Recovery Point Objective)

- Maximum acceptable data loss
- Affects backup frequency

RTO (Recovery Time Objective)

- Time to restore service
- Affects disaster planning

MTTR (Mean Time to Repair)

- Average fix time after failure

MTBF (Mean Time Between Failures)

- Average time between hardware failures

Backup Types

Full

- Entire data set
- Longest to run, fastest to restore

Incremental

- Changes since last backup
- Fast backup, slow restore

Differential

- Changes since last full backup
- Middle ground for time

Offsite Backup

- Cloud or physical external location
- Protects against site-wide failure

Backup Testing

Restoration Tests

- Verify you can restore successfully

Scheduling

- Regular intervals to validate backup integrity

Redundancy and High Availability

Hardware Redundancy

- Dual NICs, dual power supplies
- RAID for storage

Link Redundancy

- Dual WAN or switch uplinks
- Use STP, LACP, VRRP/HSRP for failover

Server Clustering

- Multiple nodes act as one
- Failover automatic if one fails

Disaster Recovery Sites

Cold Site

- Empty facility
- Longest RTO

Warm Site

- Some hardware, needs data/config restore

Hot Site

- Fully equipped and up-to-date
- Fastest recovery, most expensive

Active-Active vs Active-Passive

Active-Active

- Load balanced
- Both systems serve traffic

Active-Passive

- One system on standby
- Failover only if active fails

3.4 Explain common remote access and site-to-site methods

Key Concepts to Learn:

- VPN types and protocols
- Tunneling
- RADIUS vs TACACS+
- Remote access tools

VPN (Virtual Private Network)

Site-to-Site

- Connects two LANs over the internet

Remote Access

- Allows individual users to connect to company network

Protocols:

- **IPsec:** Layer 3, site-to-site or remote
- **SSL/TLS:** Browser-based, remote access
- **L2TP/IPsec:** Layer 2 tunneling
- **GRE:** Tunnels non-IP traffic, not secure by itself

Tunneling Concepts

Encapsulation

- Wrap original packet in another protocol

Encryption

- Secure tunnel over untrusted network

Split Tunneling

- Route only company traffic through VPN
- All other traffic goes directly to internet

Authentication Servers

RADIUS

- UDP-based (port 1812)
- Centralized authentication
- Used for network access (VPN, 802.1X)

TACACS+

- TCP-based (port 49)
- Cisco proprietary
- More granular control (authentication, authorization, accounting)

Remote Management Tools

SSH

- Encrypted remote CLI access

Telnet

- Unencrypted; avoid using

RDP

- GUI-based remote control (Windows)

VNC

- Cross-platform remote desktop tool

Out-of-band Management

- KVM over IP, console servers
- Used when device/network is unreachable normally

Domain 3 Summary

Things You Must Memorize:

- SNMP vs Syslog vs NetFlow vs SIEM
- RPO vs RTO vs MTTR
- VPN protocols and remote access tools
- Change management and configuration baselines
- Disaster recovery site types

Domain 4: Network Security (14%)

Goal of Domain 4:

This domain focuses on identifying, preventing, and responding to security threats across networks. It covers foundational concepts, real-world threats, and best practices to harden devices and control access.

4.1 Explain common security concepts

Key Concepts to Learn:

- CIA Triad
- Authentication, Authorization, Accounting (AAA)
- Security zones and segmentation
- Defense in depth
- Zero Trust
- Risk, threat, vulnerability, exploit

CIA Triad

Confidentiality

- Prevent unauthorized access to data
- Tools: encryption, access control

Integrity

- Ensure data is not altered without detection
- Tools: hashing (SHA-256), digital signatures

Availability

- Ensure systems are up and accessible when needed
- Tools: redundancy, failover, DDoS protection

AAA – Authentication, Authorization, Accounting

Authentication

- Verify identity (password, MFA, certificate)

Authorization

- Grant access rights based on role

Accounting

- Log and audit actions (who did what, when)

Defense in Depth

Layered security approach

- Physical security → Firewall → IDS/IPS → Encryption → Endpoint protection

Example layers:

- Door locks
- Network segmentation
- Firewalls
- Patch management
- Access controls

Zero Trust Model

"Never trust, always verify"

- Every user/device is treated as potentially compromised
- Enforced via continuous authentication, access limits, micro-segmentation

---

Risk Terminology

Risk

- Potential for damage from a threat exploiting a vulnerability

Threat

- Actor or action that can cause harm (e.g., hacker, malware)

Vulnerability

- Weakness that can be exploited (e.g., open port, unpatched software)

Exploit

- Actual method or code used to breach a system

Mitigation

- Steps taken to reduce risk

4.2 Compare and contrast common types of attacks

Key Concepts to Learn:

- Social engineering attacks
- DoS/DDoS
- MITM (Man-in-the-Middle)
- Malware types
- Network-layer attacks (MAC flooding, ARP spoofing)
- Wireless attacks

Social Engineering

Phishing – Email scams
Spear phishing – Targeted phishing
Whaling – Targeted at executives
Vishing – Voice phishing
Smishing – SMS phishing
Pretexting – Lying to gain trust
Tailgating – Following someone into secure area
Dumpster Diving – Searching trash for info

Defense:

- User education
- Spam filters
- MFA

Malware

Virus – Needs host file to spread
Worm – Self-replicates, spreads across networks
Trojan – Masquerades as a legitimate app
Ransomware – Encrypts files, demands payment
Spyware – Collects info
Adware – Displays ads
Keylogger – Records keystrokes
Rootkit – Hides malicious presence

Denial of Service (DoS) / Distributed DoS (DDoS)

Goal: Overwhelm a system or service

DoS: One attacker
DDoS: Multiple sources (botnet)

Types:

- ICMP flood
- SYN flood
- Application layer attacks

Defense: Firewalls, load balancing, anti-DDoS services

Man-in-the-Middle (MitM)

Intercepts communication between two parties

Methods:

- ARP poisoning
- DNS spoofing
- Fake SSL certificates

Defense:

- Encryption (TLS, IPsec)
- Strong ARP inspection
- Certificate pinning

ARP Spoofing / Poisoning

Attacker tricks devices into associating wrong MAC address with an IP

- Enables MITM attacks on LAN

Defense:

- Dynamic ARP Inspection
- Use static ARP where possible

MAC Flooding

Overloads switch MAC table, forces flooding of frames

- Attacker can sniff unicast traffic

Defense:

- Port security (limit MACs per port)

VLAN Hopping

Attacker gains access to traffic in other VLANs

Methods:

- Switch spoofing (trick switch into forming trunk)
- Double tagging (nested VLAN tags)

Defense:

- Disable DTP (use static trunks)
- Tag native VLANs explicitly
- Avoid VLAN 1 as native

DNS Poisoning

Inserts false DNS entries

- Redirect users to malicious sites

Defense:

- DNSSEC
- Secure recursive resolvers

Rogue Access Point

Unauthorized AP connected to the network

- Bypasses wired controls

Evil Twin: Fake AP imitating real one

Defense:

- Wireless IDS/IPS
- 802.1X authentication
- AP management

4.3 Explain network hardening techniques

Key Concepts to Learn:

- Device hardening (patches, passwords, services)
- Secure protocols (SSH, HTTPS)
- Physical security
- Honeypots and deception
- Firewall types
- ACLs and rules
- VLAN segmentation
- NAC (802.1X, port security)

Device Hardening

Disable unused ports and services
Change default credentials
Update firmware and OS
Limit access methods (SSH > Telnet)
Use secure management (HTTPS, SNMPv3)
Implement logging and backups

Secure Network Protocols

- **SSH** over Telnet
- **HTTPS** over HTTP
- **SFTP** over FTP
- **SNMPv3** over v1/v2c
- **TLS** over SSL

Avoid using cleartext protocols

Physical Security

- Locked doors, cages
- Cable locks, rack security
- Surveillance cameras
- Badge/keycard access
- Biometric authentication

ACLs (Access Control Lists)

- Filter traffic on routers, firewalls, switches
- Match by source/destination IP, protocol, port
- First-match rule set
- Implicit deny at the end

VLAN Segmentation

- Isolate traffic for departments/devices
- Prevent broadcast storms
- Apply ACLs to control inter-VLAN communication

Example:

- VLAN 10 – Admins
- VLAN 20 – Sales
- VLAN 30 – Guests (internet-only)

Port Security

- Restrict MAC addresses per switch port
- Violation actions: Shutdown, restrict, protect
- Prevents rogue device attachment

Network Access Control (NAC)

- Validates device before granting access
- Uses **802.1X** with RADIUS server
- Can quarantine non-compliant devices
- Can assign VLAN dynamically based on user/device role

Honeypots and Honeynets

Honeypot: Decoy system to attract attackers
Honeynet: Network of honeypots

Used for:

- Detection
- Research
- Delaying attackers

Firewall Types

- **Packet Filter (stateless):** Filters based on header info only
- **Stateful:** Tracks active connections
- **Next-Gen Firewall:** Deep packet inspection, application-layer awareness
- **Host-based firewall:** Local OS firewall
- **Cloud firewall (FWaaS):** Off-premise filtering

4.4 Explain authentication and access controls

Key Concepts to Learn:

- Authentication methods (passwords, MFA)
- Directory services (LDAP, AD)
- Authentication servers (RADIUS, TACACS+)

- Access control models (RBAC, least privilege)
- Certificate-based authentication
- MFA and biometric access

Authentication Methods

- **Username/password**
- **PIN**
- **Biometrics** (fingerprint, retina)
- **Certificates** (X.509)
- **Tokens** (TOTP apps)
- **Smartcards**
- **SSO** (Single Sign-On)

Access Control Models

Least Privilege – Users get only necessary access
Role-Based Access Control (RBAC) – Access based on job roles
Attribute-Based Access Control (ABAC) – Based on user, resource, and environment attributes

Directory Services

LDAP (389) / LDAPS (636)

- Used to query and update directory entries (Active Directory, OpenLDAP)

Active Directory

- Microsoft's directory service
- Supports authentication, authorization, policy enforcement

Authentication Servers

RADIUS

- UDP port 1812
- Centralized authentication for network access
- Combines auth + accounting

- Used with 802.1X, VPNs

TACACS+

- TCP port 49
- Cisco proprietary
- Separate auth, author, accounting
- Preferred for device management

MFA (Multi-Factor Authentication)

Factors:

- Something you know (password)
- Something you have (token, smartcard)
- Something you are (biometric)

MFA > 2FA

- MFA requires 2+ categories
- 2FA is a subset of MFA

Certificate-Based Authentication

- Uses X.509 digital certificates
- Often used with:
  - VPNs
  - 802.1X
  - S/MIME for email
- Requires PKI (Public Key Infrastructure)

Domain 4 Summary

Things You Must Memorize:

- Definitions of CIA, AAA, and Zero Trust
- Malware and attack types (phishing, DoS, ARP spoofing)
- NAC technologies (802.1X, port security)
- Secure network protocols and their ports
- Authentication servers: RADIUS vs TACACS+

Domain 5: Network Troubleshooting (24%)

Goal of Domain 5:

This domain covers how to approach, diagnose, and resolve a wide variety of network issues using structured methodologies and tools. It represents the largest percentage of the exam and is vital for real-world technical troubleshooting.

5.1 Apply network troubleshooting methodologies

Key Concepts to Learn:

- Structured troubleshooting steps
- Common diagnostics process
- Root cause analysis
- Escalation and documentation

Troubleshooting Steps

1. **Identify the problem**
   - Gather information from users, logs, alerts
   - Ask: What changed? When did it start?
   - Define scope: one user, a department, entire network?
2. **Establish a theory of probable cause**
   - Consider simple causes first
   - Use OSI model as a guide (physical → application)
3. **Test the theory to determine cause**
   - Swap cables, ping endpoints, isolate variables
   - If theory is wrong, go back to step 2
4. **Establish a plan of action**
   - Implement fix with minimal disruption
   - Schedule downtime if needed
5. **Verify full system functionality**
   - Test full services and related systems
   - Confirm with user
6. **Document findings and actions**
   - Record the problem, resolution, and timeline
   - Useful for audits, training, and trend tracking

Best Practices:

- Follow change control if required
- Use rollback plan in case the fix fails
- Maintain communication with stakeholders

5.2 Troubleshoot common cable and physical interface issues

Key Concepts to Learn:

- Cable testing and replacement
- Signal loss and attenuation
- Speed/duplex mismatches
- Interface errors and counters
- Transceiver problems

Cable Issues

Open/short circuits

- Wire not properly terminated or broken

Incorrect pinout

- T568A vs T568B standards mismatch

Bad crimp

- Cable connector not properly attached

Exceeding max distance

- Cat5e/6 = 100m max (328 ft)

Wrong cable type

- Crossover vs straight-through
- Fiber multimode vs single mode

EMI interference

- Caused by fluorescent lights, motors, etc.

Tools to use:

- Cable tester
- Time Domain Reflectometer (TDR)
- Optical Time Domain Reflectometer (OTDR for fiber)
- Tone generator and probe

Interface Errors and Indicators

CRC Errors

- Frame checksum errors
- Often due to interference or faulty cables

Late collisions

- Caused by duplex mismatches

Runts/Giants

- Packets too small or too large

Interface flapping

- Link goes up/down repeatedly (bad cable, port, or SFP)

Solution:

- Check logs, replace transceivers or cables, reconfigure settings

---

Speed and Duplex Mismatches

- Occur when one device is set to auto, the other is hard-coded
- Causes slow speeds, collisions, or no connectivity

Fix:

- Set both sides to auto or explicitly match both speed/duplex

Fiber-Specific Issues

- Dirty connectors: use fiber cleaner
- Wrong type (multimode vs single-mode)
- Damaged fiber: inspect with light source or OTDR
- Bend radius exceeded: reduces signal quality

5.3 Troubleshoot common network service issues

Key Concepts to Learn:

- DHCP, DNS, and IP addressing issues
- VLAN misconfigurations
- Routing and gateway problems
- NAT/firewall-related failures

DHCP Issues

Symptoms:

- APIPA address (169.254.x.x)
- No internet or local connectivity

Possible Causes:

- DHCP scope exhausted
- DHCP server unreachable
- Relay agent misconfigured

Fixes:

- Renew lease
- Check server status
- Ensure IP helper address is correct on router

DNS Issues

Symptoms:

- Can ping IP but not hostname
- Website loads via IP, not via domain name

Fixes:

- Verify DNS settings in client config
- Use nslookup or dig to test queries
- Flush DNS cache (ipconfig /flushdns)

Gateway and Routing Problems

Symptoms:

- Local network access works, internet doesn't
- No response beyond first hop in traceroute

Possible Causes:

- Wrong default gateway
- Missing or incorrect static route
- Dynamic routing failure (OSPF, RIP down)

Tools:

- tracert, ping, route print, show ip route

NAT and Firewall Issues

Symptoms:

- Internal users can't reach internet
- Port forwarding not working

Fixes:

- Check NAT tables on edge router
- Verify ACLs and firewall rules
- Ensure translations are applied properly

VLAN and Trunk Problems

Symptoms:

- Hosts on same subnet/VLAN can't communicate
- Switch shows VLAN up but no traffic passes

Causes:

- Wrong port assignment
- Trunk misconfiguration (missing allowed VLAN)
- Native VLAN mismatch

Commands:

- show vlan brief
- show interface trunk

MTU Problems

Symptoms:

- Web pages partially load, large pings fail
- VPN clients can't access all resources

Fix:

- Adjust MTU size on endpoints or routers
- Use ping -f -l to test maximum MTU without fragmentation

5.4 Troubleshoot common network performance issues

Key Concepts to Learn:

- High latency and jitter
- Packet loss and bandwidth saturation
- Wireless congestion and roaming problems
- QoS misconfiguration

High Latency

Symptoms:

- Slow response time
- Long ping/traceroute delays

Causes:

- WAN congestion
- Overloaded router/firewall
- ISP issues

Fixes:

- Upgrade bandwidth
- Implement QoS
- Load balancing or rerouting

Packet Loss

Symptoms:

- VoIP call drops
- Video/audio glitches

Causes:

- Faulty cable or port
- Congestion
- Wireless interference

Fixes:

- Replace cables
- Check error counters
- Increase buffer size or bandwidth

Bandwidth Saturation

Symptoms:

- Slow internet
- High latency during peak hours

Causes:

- Streaming, large downloads
- Backup jobs

Fixes:

- Identify top talkers (NetFlow, SNMP)
- Apply rate limiting or QoS
- Schedule heavy jobs off-hours

Wireless-Specific Performance Issues

Poor signal

- Move APs or clients
- Install additional APs

Co-channel interference

- Change channels (especially in 2.4 GHz)

AP overload

- Too many users on one AP
- Use band steering or load balancing

Roaming issues

- Enable 802.11k/r/v
- Tune signal strength and overlap

5.5 Use the appropriate network software tools and commands

Key Concepts to Learn:

- Tools: ping, tracert, ipconfig, nslookup, netstat
- SNMP and syslog tools
- Traffic analyzers (Wireshark)
- Cable testers, tone generator, TDR

Command-Line Tools

ping

- Test connectivity
- Packet loss and latency info

tracert/traceroute

- Trace path to destination
- Identify delays or dropped routes

ipconfig (Windows) / ifconfig or ip (Linux)

- View IP configuration
- Renew DHCP: ipconfig /release, ipconfig /renew

nslookup / dig

- Query DNS servers
- Find A, MX, CNAME, PTR records

netstat

- Show open connections and listening ports
- Useful for identifying malware or app issues

arp

- View ARP table
- Detect MAC/IP mismatches

Monitoring Tools

Wireshark

- Packet capture and protocol analysis
- Deep inspection of traffic

tcpdump

- Command-line packet capture

SNMP Tools

- Poll routers/switches for performance data
- Set traps for alerts

Syslog Collectors

- Centralize device logs
- Filter and analyze for events

SIEM Tools

- Correlate logs for security monitoring
- Example: Splunk, AlienVault, QRadar

Hardware Tools

Cable Tester

- Check wiring continuity and pinout

TDR / OTDR

- Locate cable breaks or impedance faults

Tone Generator and Probe

- Trace cable path through patch panels

Multimeter

- Check electrical signals and resistance

Loopback Plug

- Test NICs and router interfaces

Domain 5 Summary

Things You Must Memorize:

- The 6-step troubleshooting process
- Common errors: CRC, collisions, flapping, duplex mismatch
- DHCP/DNS/NAT failure symptoms and fixes
- Wireless performance problems (interference, signal loss)
- CLI tools and when to use them: ping, tracert, ipconfig, netstat, nslookup

Terms and Definitions

A

ACL (Access Control List)
A set of rules on a device that controls which traffic is allowed or denied based on IP address, protocol, or port.

Active Directory
Microsoft's centralized directory service used for authentication and resource management.

Active-Passive
A high availability configuration where only one system is active at a time, and the other takes over if it fails.

Active-Active
A setup where multiple systems share the load simultaneously and provide redundancy.

Ad hoc
A wireless connection mode where devices communicate directly without an access point.

Anycast
A network addressing and routing scheme where data is routed to the nearest instance of a service.

AP (Access Point)
A wireless device that allows Wi-Fi clients to connect to a wired network.

APIPA (Automatic Private IP Addressing)
169.254.x.x IP assigned when DHCP fails; allows local-only connectivity.

ARP (Address Resolution Protocol)
Used to resolve an IP address to a MAC address on a local network.

B

Backbone
The main infrastructure or high-speed line that connects various segments of a network.

Bandwidth
The maximum data transfer rate of a connection, usually measured in Mbps or Gbps.

Baseline
A record of normal operating performance used for comparison during troubleshooting.

BGP (Border Gateway Protocol)
A routing protocol used to exchange routing information between autonomous systems on the internet.

Broadcast
Traffic sent from one device to all devices on the local network.

Bridge
A Layer 2 device that connects and filters traffic between two network segments.

BPDU (Bridge Protocol Data Unit)
Messages exchanged by switches for Spanning Tree Protocol.

C

Caching
Storing data locally to reduce retrieval time or bandwidth usage.

CAM Table (Content Addressable Memory)
A table in a switch that maps MAC addresses to ports.

CIDR (Classless Inter-Domain Routing)
IP addressing scheme that allows subnetting using variable-length subnet masks.

CNAME (Canonical Name)
A DNS record that creates an alias for another domain.

Core Switch
A switch at the center of a network that connects distribution or access layer switches.

CRC (Cyclic Redundancy Check)
An error-detection mechanism used to validate data integrity in frames.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
A protocol for detecting and managing collisions in Ethernet networks.

D

Data Link Layer
OSI Layer 2; responsible for framing, MAC addressing, and error detection.

DHCP (Dynamic Host Configuration Protocol)
Protocol that automatically assigns IP addresses and other settings to clients.

DNS (Domain Name System)
Translates domain names to IP addresses.

DoS (Denial of Service)
Attack that floods a system to make it unavailable to users.

DDoS (Distributed Denial of Service)
A DoS attack from multiple sources.

Default Gateway
The router IP address used to access other networks.

DMZ (Demilitarized Zone)
A semi-trusted network segment used to host public-facing servers.

E

Egress
Outbound traffic leaving a network.

EIGRP (Enhanced Interior Gateway Routing Protocol)
A Cisco proprietary advanced distance-vector routing protocol.

Encapsulation
The process of adding headers to data as it moves down the OSI layers.

ESSID (Extended Service Set Identifier)
A single SSID used across multiple wireless access points to support roaming.

F

FHRP (First Hop Redundancy Protocol)
A group of protocols (e.g., HSRP, VRRP) that provide a virtual IP for gateway redundancy.

Firewall
A device or software that filters traffic based on security rules.

Full-Duplex
Communication mode allowing simultaneous transmission and reception.

G

Gateway
A device that routes traffic between different networks.

GRE (Generic Routing Encapsulation)
A tunneling protocol that encapsulates packets for transport across IP networks.

GUI (Graphical User Interface)
A visual interface for managing devices or software.

H

Hashing
A process that transforms data into a fixed-size value to verify integrity.

Hop
A point a packet passes through from source to destination.

Host
A device on a network that has an IP address.

HSRP (Hot Standby Router Protocol)
Cisco protocol that allows multiple routers to share a virtual IP address for redundancy.

I

ICMP (Internet Control Message Protocol)
Used for diagnostics like ping and traceroute.

IDS (Intrusion Detection System)
Monitors traffic and alerts on suspicious activity.

IPS (Intrusion Prevention System)
Monitors and actively blocks malicious traffic.

IMAP (Internet Message Access Protocol)
Used by email clients to retrieve messages from a server.

Ingress
Inbound traffic entering a network.

IP (Internet Protocol)
Provides addressing and routing for packets across networks.

IPAM (IP Address Management)
Tools or processes used to manage IP address space and allocations.

J

Jitter
Variation in packet arrival times, affecting real-time traffic like VoIP.

K

Key Management
Processes used to generate, distribute, store, rotate, and revoke encryption keys.

L

LACP (Link Aggregation Control Protocol)
Combines multiple physical links into one logical link for bandwidth and redundancy.

LAN (Local Area Network)
A network that spans a small geographic area, such as a single office.

Latency
The time it takes for a packet to travel from source to destination.

Load Balancer
Distributes incoming traffic across multiple servers.

Loopback Address
127.0.0.1; used to test the local TCP/IP stack.

M

MAC Address
A unique hardware address assigned to a network interface card (NIC).

MAC Filtering
A security feature that allows only listed MAC addresses to connect.

Mesh Topology
A network layout where each node connects directly to every other node.

MIB (Management Information Base)
A database used by SNMP to manage devices.

N

NAT (Network Address Translation)
Translates private IP addresses to public ones.

NetBIOS
An older protocol used for name resolution and file sharing on Windows networks.

NetFlow
A network monitoring protocol used to capture traffic flow statistics.

Network Layer
OSI Layer 3; handles routing and IP addressing.

NTP (Network Time Protocol)
Synchronizes time across devices.

O

OSI Model

A conceptual model with 7 layers used to describe network communication.

OSPF (Open Shortest Path First)

A link-state routing protocol used within large enterprise networks.

P

Packet

A formatted unit of data at the Network Layer (Layer 3).

PAT (Port Address Translation)

A type of NAT where multiple devices share a single IP by using different port numbers.

Phishing

A form of social engineering used to trick users into revealing sensitive information.

PoE (Power over Ethernet)

Delivers electrical power and data over the same Ethernet cable.

Port

A number that identifies a specific process or service on a host (e.g., HTTP = port 80).

Protocol

A set of rules for communication between devices.

Q

QoS (Quality of Service)

Mechanism that prioritizes traffic to ensure performance for critical applications.

R

RADIUS (Remote Authentication Dial-In User Service)

Protocol used for centralized authentication of remote users and devices.

RJ45
Standard connector used for Ethernet cabling.

RIP (Routing Information Protocol)
A distance-vector routing protocol using hop count as metric.

Root Bridge
The central switch in a spanning tree topology.

Routing Table
List of routes that a router uses to determine where to forward packets.

S

SaaS (Software as a Service)
A cloud model where software is accessed online without local installation.

Scope (DHCP)
Range of IP addresses assigned by DHCP server.

Segment
A portion of a network, often referring to a broadcast or collision domain.

Session Layer
OSI Layer 5; responsible for maintaining connections.

SFP (Small Form-Factor Pluggable)
A compact transceiver used in networking hardware for fiber/copper interfaces.

SIEM (Security Information and Event Management)
Centralized platform for collecting, analyzing, and reporting security data.

SLA (Service Level Agreement)
A contract that defines expected service performance.

SNMP (Simple Network Management Protocol)
Used to monitor and manage network devices.

SSH (Secure Shell)
Encrypted protocol for secure remote command-line access.

SSID (Service Set Identifier)
Name of a wireless network.

STP (Spanning Tree Protocol)
Prevents loops in Layer 2 networks.

T

TCP (Transmission Control Protocol)
Reliable, connection-oriented transport protocol.

Telnet
Unsecured protocol used for remote CLI access (replaced by SSH).

Throughput
Amount of data successfully transmitted in a given time.

Traceroute
Tool used to trace the path packets take to a destination.

U

UDP (User Datagram Protocol)
Connectionless, fast protocol without guarantees.

Unicast
One-to-one communication.

UPS (Uninterruptible Power Supply)
Backup power system to maintain device operation during outages.

V

VLAN (Virtual LAN)
Logical segmentation of a network at Layer 2.

VLSM (Variable Length Subnet Mask)
Allows subnets of different sizes.

VPN (Virtual Private Network)
Encrypted tunnel between remote sites or users and the corporate network.

VRRP (Virtual Router Redundancy Protocol)
Allows multiple routers to share a virtual IP for redundancy.

W

WAN (Wide Area Network)
A network that spans a large geographic area.

WEP (Wired Equivalent Privacy)
Deprecated wireless security protocol.

WPA2/WPA3
Modern wireless security protocols using AES encryption.

Wireshark
A packet analyzer tool used for traffic inspection.

X

XML (Extensible Markup Language)
A structured data format used in some protocols like SAML for authentication.

Z

Zero Trust
Security model where nothing is trusted by default, even inside the network.