

CompTIA N+ (N10-009) Day 2

Chapter 3: Internet, Transport, and Application Layer Protocols

TCP/IP Protocols Overview

The TCP/IP suite includes protocols at multiple layers that handle communication, addressing, and data transfer.

TCP vs UDP (Transport Layer)

Feature	TCP	UDP
Reliability	Reliable – ensures delivery through acknowledgments and retransmissions	Best-effort – no guarantee of delivery
Connection Type	Connection-oriented – requires a handshake before data transfer	Connectionless – sends data without prior setup
Sequencing	Yes – maintains order of segments	No – packets may arrive out of order
PDU Name	Segment	Datagram
Common Uses	File transfer (FTP), secure communication (HTTPS, SSH), email (SMTP)	VoIP, video streaming, DNS queries, DHCP, TFTP, NTP

Tip: Be able to match services to the correct protocol on the exam.

TCP 3-Way Handshake & Termination (Flags)

- **SYN** – Initiates a connection request.
 - **SYN/ACK** – Acknowledges the request and sends its own request to connect.
 - **ACK** – Final acknowledgment; connection established.
 - **FIN/ACK** – Graceful connection termination.
 - **RST** – Immediately resets a connection without completing termination.
-

UDP

- No handshake; sends data immediately.
 - Faster but less reliable.
 - No sequencing or retransmission.
 - Common in time-sensitive applications.
-

Internet Control Message Protocol (ICMP)

Used for network messaging, error reporting, and diagnostics. It is connectionless.

Network Messaging:

- **Destination Unreachable** – The packet could not be delivered. Causes include:
 - No route to host/network
 - Host or network is down
 - Firewall blocking traffic
 - Protocol or port unreachable
- **Redirect** – Informs a host of a more efficient route.
- **Time Exceeded** – Packet's TTL expired before reaching destination.

Network Diagnostics:

- **Ping** – Sends Echo Request and waits for Echo Reply to test reachability.
 - **Traceroute** – Maps the path packets take to a destination, identifying each hop.
-

Common Protocols			
Protocol	Name	Port(s)	Function / Description
FTP	File Transfer Protocol	TCP 20 (data), 21 (control)	Transfers files between client and server.
SSH	Secure Shell	TCP 22	Secure remote login and command execution.
SFTP	SSH File Transfer Protocol	TCP 22	Secure file transfer over SSH.
Telnet	Telnet	TCP 23	Unencrypted remote terminal access.
SMTP	Simple Mail Transfer Protocol	TCP 25	Sending email.
DNS	Domain Name System	UDP/TCP 53	Resolves domain names to IP addresses.
DHCP	Dynamic Host Configuration Protocol	UDP 67 (server), 68 (client)	Assigns IP addresses dynamically.
TFTP	Trivial File Transfer Protocol	UDP 69	Simple, unsecured file transfer.
HTTP	HyperText Transfer Protocol	TCP 80	Web page transfer protocol.
POP3	Post Office Protocol v3	TCP 110	Retrieves email from server.
NTP	Network Time Protocol	UDP 123	Synchronizes clocks across devices.
IMAP	Internet Message Access Protocol	↓ CP 143	Retrieves and manages email on a server.

SNMP	Simple Network Management Protocol	UDP 161/162	Network device monitoring and management; also sets TRAPs.
LDAP	Lightweight Directory Access Protocol	TCP 389	Directory services protocol.
SMTPS	SMTP Secure (SMTP over SSL/TLS)	TCP 465 or 587	Secure sending of email.
LDAPS	LDAP over SSL/TLS	TCP 636	Secure directory access.
FTPS	FTP Secure (FTP over SSL/TLS)	TCP 989, 990	Secure file transfer using SSL/TLS.
Secure IMAP	IMAP over SSL/TLS	TCP 993	Secure email retrieval.
Secure POP3	POP3 over SSL/TLS	TCP 995	Secure email retrieval.
SIP	Session Initiation Protocol	UDP/TCP 5060, 5061	Initiates, maintains, and terminates real-time sessions (VoIP, video calls).
SQL	Structured Query Language	TCP 1433	Database query language with default SQL Server port.
SQLnet	Oracle SQL*Net	TCP 1521	Oracle database connection protocol.
RTMP	Real-Time Messaging Protocol	TCP 1935	Streaming audio, video, and data over the internet.
MySQL	MySQL Database	TCP 3306	MySQL database server port.
RDP	Remote Desktop Protocol	TCP 3389	Remote desktop access.
HTTPS	HyperText Transfer Protocol Secure	TCP 443 ↓	Secure web traffic (HTTP over TLS/SSL).
Syslog	System Logging Protocol	UDP 514	Transmits event messages for system logging.
TLS and SSL	Transport Layer Security / Secure Sockets Layer	Varies	Protocols for encrypting communications.

Chapter 4: Ethernet Communication Fundamentals

UTP (Unshielded Twisted Pair) Cable Types and Ethernet Standards

UTP Type	Ethernet Standard	Cable Rating	Max Speed	Max Distance	Connector	🔗
Cat 3	10BASE-T	Cat 3	10 Mbps	100 meters	RJ-45	
Cat 5	100BASE-TX	Cat 5	100 Mbps	100 meters	RJ-45	
Cat 5e	1000BASE-T	Cat 5e	1 Gbps	100 meters	RJ-45	
Cat 6	1000BASE-T / 10GBASE-T	Cat 6	1 Gbps / 10 Gbps	100 meters for 1 Gbps; ~55 meters for 10 Gbps	RJ-45	
Cat 6a	10GBASE-T	Cat 6a	10 Gbps	100 meters	RJ-45	
Cat 8	25GBASE-T / 40GBASE-T	Cat 8	25 Gbps / 40 Gbps	30 meters	RJ-45	

Note: Cat 8 cables are wrapped with copper tape shielding to reduce electromagnetic interference and crosstalk, improving signal quality at high speeds.

Copper Media - Twisted-Pair Cable

- **STP (Shielded Twisted Pair)** – Adds shielding to reduce the impact of noise (EMI) and also includes grounding.
- **Plenum** – Plenum-rated cable is designed for use in air ducts and “plenum” spaces. It reduces the toxicity of smoke and fumes released by the cable during a fire.

Fiber Standards

Ethernet Standard	Minimum Cable Type	Max Speed	Max Distance	Connector Type
100BASE-SX	MMF (Multi-Mode Fiber)	100 Mbps	Up to 550 meters	LC
1000BASE-SX	MMF	1 Gbps	Up to 550 meters	LC
1000BASE-LX	SMF (Single-Mode Fiber)	1 Gbps	Up to 10 km	LC or SC
10GBASE-SR	MMF	10 Gbps	Up to 400 meters	LC
10GBASE-LR	SMF	10 Gbps	Up to 10 km	LC
100GBASE-SR4	MMF	100 Gbps	Up to 100-150 m	MPO/MTP

Fiber Optic Cable Types

- **MMF (Multi-Mode Fiber):**
 - Larger core diameter (typically 50 or 62.5 microns).
 - Supports multiple light modes, suitable for shorter distances.
 - Used in buildings or data centers.
- **SMF (Single-Mode Fiber):**
 - Smaller core diameter (~9 microns).
 - Supports single light mode, suitable for longer distances.
 - Used in WANs, long-distance telecommunication.

Common Fiber Connector Types

- **LC (Lucent Connector):**
 - Small form factor, commonly used for both MMF and SMF.
 - Popular in data centers due to compact size.
- **SC (Subscriber Connector or Standard Connector):**
 - Larger connector, often used with SMF.
 - Easy to plug/unplug.
- **MPO/MTP (Multi-Fiber Push On/Pull Off):**
 - High-density connector supporting multiple fibers (12, 24, or more).
 - Commonly used for 40G and 100G fiber links.

Fiber Optic Polarity

css Copy Edit

```
RX A <- B / A <- B / A <- B TX  
TX B -> A / B -> A / B -> A RX
```

If the polarity is incorrect, the cable will not establish a connection.

Small Form Factor Pluggables (SFP)

Module	Ethernet Standard	Speed
SFP	1000BASE-SX/LX	1 Gbps
SFP+	10GBASE-SR/LR	10 Gbps
QSFP	40GBASE-SR4/LR4	40 Gbps
QSFP+	40GBASE-SR4/LR4	40 Gbps
QSFP28	100GBASE-SR4/LR4	100 Gbps

Definitions

- **Hot Swappable:** The ability to insert or remove a device (or module) without shutting down or powering off the system.
- **Small Form Factor Pluggables (SFPs) are hot swappable modules,** meaning you can replace or upgrade them while the host device remains powered on and operational.

What Causes No Link?

- Assume bad or improper wiring.
 - TX/RX (Transmit/Receive) wires reversed.
 - Incorrect SFP module installed.
 - Wrong SFP module type used.
-

Fiber Color Coding

- **SMF (Single-Mode Fiber)** = Blue
 - **MMF (Multi-Mode Fiber)** = Black
-

Direct Attach Copper (DAC)

Definition:

DAC cables, also called Twinax cables, are copper cables with transceivers permanently attached at each end. They are used for short-distance, high-speed connections (usually within racks or between adjacent racks) and offer lower latency and cost compared to optical modules.

Ethernet Duplex

Half Duplex Operation

- Forced when connected to hubs or repeaters.
- Devices can **send or receive** but **not both simultaneously**.
- Uses **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection) to handle collisions:
 - Only one sender can transmit at a time in a collision domain.
 - If two devices transmit simultaneously, a collision occurs, triggering a backoff algorithm.

Full Duplex Operation

- Forced when connected to switches.
- Devices can **send and receive simultaneously**.
- Collisions **do not occur** in full duplex mode.
- **CSMA/CD is disabled** in this mode.

Auto-Negotiate Duplex

- Modern devices generally use auto-negotiation for duplex settings.
- If negotiation fails, devices often default to **half duplex**, which can cause issues.
- Manually configuring duplex disables auto-negotiation, so both ends of the link must be configured to match.

Duplex Mismatch

- Happens when one side is set to full duplex and the other to half duplex (usually due to manual settings or auto-negotiation failure).
 - The full duplex side sends continuously without collision checks.
 - The half duplex side listens for collisions and backs off repeatedly.
 - This mismatch severely degrades network performance and can cause intermittent connectivity.
-

Speed Configuration Settings

- **Auto:** Negotiates speed automatically (10/100/1000/10000 Mbps etc.).
 - Manual speed setting disables auto-negotiation.
 - **Speed Mismatch** results in the port going offline or no link.
-

Ethernet Frame Structure

Ethernet Frame Structure		
Field	Size	Description
Preamble	8 bytes	Synchronization bits to signal start of frame
Destination MAC Address	6 bytes (48 bits)	Address of receiving device
Source MAC Address	6 bytes (48 bits)	Address of sending device
EtherType	2 bytes	Identifies protocol of payload (e.g., IPv4)
Data	46-1500 bytes	Payload including headers
CRC	4 bytes	Error checking

- **MTU (Maximum Transmission Unit):** Maximum payload size per frame (default is 1500 bytes).
- Data payload includes:
 - IP Header (20 bytes)
 - TCP Header (20 bytes)
 - TCP Payload (typically 1460 bytes)
- Minimum data size is 46 bytes.
- **Jumbo Frames:** Can be up to 9000 bytes, recommended for:
 - HDMI over IP
 - SAN traffic over Ethernet
 - iSCSI
 - FCoIP
 - Replication/backup traffic

Note: Jumbo Frames must be supported and enabled on every device and switch interface along the path or else default MTU (1500 bytes) is used.

Common Ethernet Frame Errors

- **Runts:** Frames smaller than 64 bytes; often caused by faulty NICs or collisions.
- **Giants:** Frames larger than allowed MTU; often caused by MTU mismatches.

Ethernet at Layer 1 (Physical Layer)

Wiring - Cubicle to Patch

- Refers to the physical cabling from the user's cubicle or workstation patch panel to the network patch panel or switch.

Patch Panel

Definition:

A patch panel is a hardware unit with multiple ports that organizes and connects incoming and outgoing cables. It allows flexible management and easy rerouting of network connections by patch cords.

Crosstalk

- **Definition:** Unwanted electromagnetic interference from adjacent wires or cables that causes signal degradation.
 - Twisting wire pairs at different rates reduces crosstalk and EMI (electromagnetic interference).
-

Near-End Crosstalk (NEXT)

- Interference measured at the **same end** of the cable where the signal is transmitted.
 - Caused by signal coupling between adjacent wire pairs at the transmitter side.
-

Far-End Crosstalk (FEXT)

- Interference measured at the **opposite end** of the cable from the transmitter.
 - Caused by signals leaking into other pairs and detected at the receiver side.
-

Interference

Definition:

Interference is unwanted electrical or electromagnetic energy that disrupts or degrades the normal operation of a signal on a network cable. It can come from external sources (like motors, fluorescent lights, or radios) or from other cables (crosstalk).

Attenuation

Definition:

Attenuation is the gradual loss of signal strength as it travels over a cable. The longer the cable or the lower the quality, the more the signal weakens, which can cause errors or loss of connectivity.

Ethernet CRC (Cyclic Redundancy Check)

- **Definition:** A mathematical algorithm used to detect errors in Ethernet frames.
- The **FCS (Frame Check Sequence)** field at the end of the frame carries the CRC value for verification.
- Frames fail the CRC check if the data is corrupted during transmission.

CRC Errors Occur Due To:

- Noise or interference
- Collisions (only in half duplex mode)
- Bad or damaged wiring
- General cabling issues
- Late collisions

Note: CRC errors cause frames to be discarded, leading to retransmissions and reduced network performance.

Cable Wiring Standards: T568A and T568B

- **T568A Wiring Standard:**

Pinout colors:

1. Green/White
2. Green
3. Orange/White
4. Blue
5. Blue/White
6. Orange
7. Brown/White
8. Brown

- **T568B Wiring Standard:**

Same cable pairs as T568A but different pin order:

1. Orange/White
2. Orange
3. Green/White
4. Blue
5. Blue/White
6. Green
7. Brown/White
8. Brown

Cable Types: Crossover vs Straight-through vs Rollover

- **Straight-through Cable:**

Both ends use the same wiring standard (T568A to T568A or T568B to T568B).

Used for: Connecting different device types, e.g., PC to switch (MDI to MDI-X).

- **Crossover Cable:**

One end wired as T568A and the other as T568B.

Used for: Connecting similar devices directly, e.g., PC to PC (MDI to MDI) or switch to switch (MDI-X to MDI-X).

- **Rollover Cable:**

The wiring order is reversed pin-to-pin (pin 1 to pin 8, pin 2 to pin 7, etc.).

Used for: Connecting a PC terminal to a router's console port (console cable).

MDI and MDI-X

- **MDI (Medium Dependent Interface):** Standard Ethernet port (typically on PCs, servers, routers).
- **MDI-X:** Ethernet port with transmit and receive pairs swapped (typically on switches).

Auto MDI/MDI-X:

Devices with this feature can automatically detect and correct cable type issues by swapping transmit and receive pairs internally.

Important:

- Works only when speed and duplex are set to auto.
 - Manually setting speed or duplex disables Auto MDI/MDI-X and may cause connection problems.
-

Ethernet Tools and Diagnostics

- **Tone Generator (Tone/Probe):**
Device that sends a tone down a cable so you can trace it with a probe, useful for identifying cable runs or locating breaks.
- **Cable Tester:**
Tests continuity, wiring correctness, and faults in cables. Possible results include:
 - **Reversed:** Pairs wired backwards (Tx and Rx swapped).
 - **Split:** Wires from different pairs are mixed incorrectly.
 - **Open:** Broken wire with no continuity.
 - **Short:** Two or more wires touching causing a short circuit.
- **Visual Fault Locator:**
A laser device used with fiber optic cables to detect breaks or bends by visibly shining light through the fiber.
- **Cable Cutter:**
Tool to cut cables cleanly.
- **Cable Stripper:**
Tool to remove insulation without damaging wires.
- **Cable Crimper:**
Tool to attach connectors (e.g., RJ-45) to cables.

Corrected PoE Standard Chart with Estimated Power Delivered			
Standard	Max Power Supplied by Switch (Watts)	Approximate Power Delivered to Device (Watts)	Description
802.3af (PoE)	15.4 W	~12.95 W	Original PoE standard, suitable for IP phones, simple cameras.
802.3at (PoE+)	30 W	~25.5 W	Enhanced PoE for higher-power devices like PTZ cameras, access points.
802.3bt Type 3	60 W	~51 W	Also called PoE++, supports more power-hungry devices like video phones, advanced wireless APs.
802.3bt Type 4	100 W	~71-90 W	Highest power PoE for devices like pan-tilt-zoom cameras, laptops, thin clients.

PoE Power Budget

- Use command: `show power inline` (or `sh power inline`) on supported switches to display current PoE usage and budget.
- **Note:** If a device requires more PoE power than available, it may pass POST (Power-On Self Test) but will reboot repeatedly after booting the OS due to insufficient power.