Day 30: TCP and UDP

CCNA 200-301 Study Guide: Transport Layer (Layer 4)

1.0 The Role of the Transport Layer (Layer 4)

The Transport Layer serves as the bridge between application-level protocols and the network-level protocols responsible for routing. It manages the end-to-end conversation between applications on different hosts.

1.1 Core Functions

- Session Multiplexing: Allows a host to handle multiple simultaneous sessions (e.g., multiple browser tabs) by assigning unique source port numbers to each session.
- Application Identification: Uses destination port numbers to direct incoming data to the correct service (e.g., Port 80 for HTTP).
- Segmentation: Breaks large data streams into smaller "segments" that fit within the network's Maximum Transmission Unit (MTU).

2.0 Deep Dive: TCP (Transmission Control Protocol)

TCP is connection-oriented and designed for applications that require absolute data integrity. It has a 20-byte header.

2.1 Key Characteristics

- Reliable: Uses acknowledgments (ACKs) and retransmissions for lost data.
- Ordered: Uses Sequence Numbers to ensure data is reassembled in the correct order.
- Flow Control: Uses Windowing to prevent a sender from overwhelming a receiver.

2.2 Connection Management

- The Three-Way Handshake (Establishment):
  1. SYN: Client sends a request to synchronize.
  2. SYN-ACK: Server acknowledges and requests a return connection.
  3. ACK: Client acknowledges the server.
- The Four-Way Handshake (Termination): Uses FIN and ACK flags to gracefully close both sides of the virtual circuit.

2.3 Reliability Mechanisms

- Forward Acknowledgment: The ACK number indicates the next byte expected (e.g., if you receive byte 1000, you send ACK 1001).
- Sliding Window: A dynamic flow control mechanism that adjusts how much data can be sent before an ACK is required based on network conditions.

3.0 Deep Dive: UDP (User Datagram Protocol)

UDP is connectionless and prioritizes speed over reliability. It has a lightweight 8-byte header.

3.1 Key Characteristics

- Best-Effort Delivery: No acknowledgments, no retransmissions, and no sequencing.
- Low Overhead: No connection setup delay (no handshake).
- No Flow Control: Sends data as fast as the application allows.

3.2 Strategic Use Cases

Ideal for real-time traffic like VoIP and Video Streaming, where a dropped packet is better than a delayed/retransmitted one that causes jitter.

4.0 Head-to-Head Comparison: TCP vs. UDP

Feature	TCP	UDP
Type	Connection-Oriented	Connectionless
Handshake	Yes (3-Way)	No
Reliability	Reliable (ACKs/Retransmits)	Unreliable (Best-effort)
Sequencing	Yes	No
Flow Control	Yes (Sliding Window)	No
Header Size	20 Bytes	8 Bytes
Common Uses	HTTP, FTP, SMTP, SSH	VoIP, DNS, DHCP, SNMP

5.0 Layer 4 Addressing: Port Numbers

Ports are 16-bit addresses (0 – 65,535) used to identify specific application processes.

5.1 Port Number Ranges

- Well-Known Ports (0 – 1,023): Common services (HTTP, SSH, etc.).
- Registered Ports (1,024 – 49,151): Assigned for specific vendor applications.
- Ephemeral Ports (49,152 – 65,535): Temporary source ports used by clients.

5.2 Essential Well-Known Ports for the CCNA

Protocol	Port(s)	Transport	Description
FTP	20, 21	TCP	File Transfer (21-Control, 20-Data)
SSH	22	TCP	Secure Remote Access
Telnet	23	TCP	Unencrypted Remote Access
SMTP	25	TCP	Sending Email
DNS	53	UDP/TCP	Name Resolution
DHCP	67, 68	UDP	Dynamic IP Assignment
TFTP	69	UDP	Trivial FTP
HTTP	80	TCP	Web Browsing (Cleartext)
POP3	110	TCP	Retrieving Email
SNMP	161, 162	UDP	Network Management
HTTPS	443	TCP	Secure Web Browsing
Syslog	514	UDP	System Logging

6.0 Practical Context & Key Exam Takeaways

6.1 Session Tracking

- Request: Source Port: 51234 (Ephemeral) $\rightarrow$ Destination Port: 80 (Well-Known).
- Reply: Source Port: 80 $\rightarrow$ Destination Port: 51234.
- The reversal of port numbers is how a host keeps track of distinct conversations.

6.2 The DNS Exception

DNS primarily uses UDP 53 for speed. However, it switches to TCP 53 if the response exceeds 512 bytes or during Zone Transfers between servers.

6.3 Core Analogy

- TCP is a Certified Letter: Requires a signature, has tracking, and pages are numbered.
- UDP is a Postcard: Fast and cheap; you drop it in the mail and hope it arrives.

Revision #1
Created 2026-03-14 19:32:12 UTC by Tony Utter
Updated 2026-03-14 19:32:30 UTC by Tony Utter