Network Protocols and Port Numbers - Complete Study Notes

Introduction

This study guide covers the most important network protocols, their corresponding port numbers, and the transport protocols they use. These protocols are frequently asked in competitive exams like NET, GATE, KVS, and other computer science examinations.

Key Components Covered:

1. Protocol Names (Application Layer protocols)
2. Port Numbers (16-bit numbers in Transport Layer)
3. Transport Protocols (TCP or UDP)

Transport Layer Fundamentals

Port Number System

- **Total Port Numbers:** 2^16 = 65,536 (16-bit system)
- **Well-defined Port Numbers:** 0-1023 (used for standard applications)
- **Purpose:** Used by transport layer for process identification

Transport Protocols

1. **TCP (Transmission Control Protocol)**
   - Connection-oriented
   - Reliable data transfer
   - Used where reliability is required
2. **UDP (User Datagram Protocol)**
   - Connectionless
   - Fast data transfer
   - Used where speed is prioritized over reliability

Detailed Protocol Analysis

1. ECHO Protocol

Port Number: 7
Transport Protocol: TCP/UDP (both supported)

Purpose:

- Measures Round Trip Time (RTT)
- Tests connectivity between client and server
- Used by administrators to check server connectivity

How it works:

- Client sends request to server
- Server responds back
- Total time = Round Trip Time

Similar Technology:

- **PING:** Uses ICMP protocol but serves similar purpose
- Both help determine if connection is established
- If response comes = connected to server
- No response = connection not established

---

2. FTP (File Transfer Protocol)

Port Numbers: 20 (data), 21 (commands)
Transport Protocol: TCP

Why Two Port Numbers:

- FTP is an "out-of-line" protocol
- **Port 20:** Used for actual data transfer
- **Port 21:** Used for control commands

Common FTP Commands:

- start
- quit
- stat
- help

Why TCP:

- Reliability is essential
- Complete file must be transferred
- Partial file transfer is unacceptable

- File won't open if incomplete

---

3. SSH (Secure Shell)

Port Number: 22
Transport Protocol: TCP

Purpose:

- Provides security through cryptographic functions
- Creates secure connections between client and server
- Uses key exchange mechanism

How it works:

- Client and server connect through secured keys
- Creates a tunnel for secure communication
- Enables private connection over unsecured/public networks (like internet)
- Uses tunneling technology

Use Case:

- Secure communication over unsecured internet
- Remote secure access

---

4. TELNET

Port Number: 23
Transport Protocol: TCP

Purpose:

- Remote login capability
- Frequently asked in competitive exams
- Connection-oriented protocol

---

5. SMTP (Simple Mail Transfer Protocol)

Port Number: 25
Transport Protocol: TCP

Purpose:

- Used for sending emails (mail transfer)
- Push mails to server
- Requires reliable, connection-oriented transfer

Frequently Asked:

- Common exam question about port number

---

6. DNS (Domain Name System)

Port Number: 53
Transport Protocol: UDP (primarily)

Purpose:

- Converts domain names to IP addresses
- Fast resolution required

Why UDP:

- Speed is prioritized
- No connection establishment needed
- Quick request-response cycle
- Consistent speed requirement

Process:

- Send domain name → Get IP address
- Fast result expected

Note: Can also use TCP, but UDP is default for speed

---

7. DHCP (Dynamic Host Configuration Protocol)

Port Numbers: 67, 68
Transport Protocol: UDP

Purpose:

- Assigns dynamic IP addresses
- Alternative to static IP assignment

Static vs Dynamic IP:

- **Static IP:** Pre-assigned (used in computer labs, colleges, universities)
- **Dynamic IP:** Assigned on-demand by DHCP

How DHCP Works:

1. Client sends MAC address
2. Requests IP address from DHCP server
3. DHCP dynamically assigns IP from available pool
4. No DHCP needed for static IP environments

Why Two Port Numbers (Out-of-line protocol):

- Different ports for data transfer and control statements
- Similar to FTP structure

Why UDP:

- No connection establishment needed
- Speed is priority
- No time wastage required
- Reliability not critical for IP assignment

---

8. TFTP (Trivial File Transfer Protocol)

Port Number: 69
Transport Protocol: UDP

Purpose:

- File transfer without connection establishment
- Faster alternative to FTP

Key Differences from FTP:

- **FTP:** Establishes connection → 3-way handshake → transfers data → more time
- **TFTP:** Direct file transfer → no connection → faster → risk of data loss

When to Use TFTP:

- When speed is more important than reliability
- Application can tolerate potential data loss
- No connection overhead acceptable

Trade-offs:

- **Advantage:** Fast transfer
- **Disadvantage:** Possible packet loss, no retransmission

---

9. HTTP (Hypertext Transfer Protocol)

Port Number: 80
Transport Protocol: TCP

Importance:

- Extremely important protocol
- Used by all web browsers
- All web page transfers use HTTP

Usage:

- Every web request goes through HTTP
- All browser-to-server communication
- Foundation of World Wide Web

Connection Type:

- Connection-oriented (TCP-based)
- Reliable transfer required for web content

---

10. POP (Post Office Protocol)

Port Numbers:

- Version 2: 109
- Version 3: 110 (latest) **Transport Protocol:** TCP

Purpose:

- Retrieves/downloads emails from server
- "Pops" mails from server to local system

SMTP vs POP Relationship:

- **SMTP (Port 25):** Sends/pushes mails to server
- **POP (Port 110):** Retrieves/pulls mails from server

- Work in parallel - one for sending, one for receiving

Why TCP:

- Both SMTP and POP use TCP
- Reliable email transfer required
- Work as complementary protocols

---

11. NTP (Network Time Protocol)

Port Number: 123
Transport Protocol: UDP

Purpose:

- Synchronizes clocks between clients and server
- Network time synchronization

Scenario:

- Multiple clients connected to server
- All need synchronized time
- Server and client machine times must match

Why UDP:

- Simple time query
- No connection needed
- Just finding current time
- Speed preferred over reliability

---

12. HTTPS (HTTP Secure)

Port Number: 443
Transport Protocol: TCP

Importance:

- Secured version of HTTP
- Most modern applications use HTTPS
- Default for major websites

Examples of HTTPS Usage:

- Banking: SBI, PNB
- E-commerce: Amazon, Flipkart
- Search: Google
- All payment portals

Security Features:

- Uses SSL (Secure Socket Layer)
- Similar to SSH functionality
- Cryptographic functions
- Cipher text conversion
- Authentication required
- Username/password verification
- Session-based access

How HTTPS Works:

1. Request converted to cipher text
2. Username/password authenticated
3. Session established
4. Secure communication within session
5. All data encrypted during transfer

User Experience:

- Users don't need to type HTTP/HTTPS
- Simply type domain name (google.com, amazon.com)
- Browser automatically uses HTTPS

---

13. RIP (Routing Information Protocol)

Port Number: 520
Transport Protocol: UDP

Purpose:

- Implements distance vector routing
- Used in network layer (IP layer)
- Routing protocol for network topology

Routing Concepts:

- **Distance Vector Routing:** Concept implemented by RIP
- **Link State Routing:** Concept implemented by OSPF

How RIP Works:

- Sends routing information to neighbor nodes
- Broadcasts distance matrix to neighbors
- No connection formation needed
- Simple broadcast mechanism
- Shares connectivity distance information

Why UDP:

- No connection establishment for broadcasting
- Simple matrix sharing with neighbors
- Broadcast-based communication

Important Notes and Tips

Protocol Categories by Transport Type

TCP Protocols (Reliability Required):

- FTP (20, 21) - File transfer needs complete data
- SSH (22) - Security requires reliable connection
- TELNET (23) - Remote login needs stability
- SMTP (25) - Email delivery must be reliable
- HTTP (80) - Web pages need complete transfer
- POP (110) - Email retrieval must be complete
- HTTPS (443) - Secure web transfer

UDP Protocols (Speed Required):

- DNS (53) - Fast domain resolution
- DHCP (67, 68) - Quick IP assignment
- TFTP (69) - Fast file transfer
- NTP (123) - Quick time synchronization
- RIP (520) - Fast routing updates

Flexible Protocols (Can use both):

- ECHO (7) - Can use TCP or UDP based on need
- DNS (53) - Primarily UDP, but can use TCP

Exam Strategy

Most Important Protocols (Frequently Asked):

- FTP (20, 21)
- SSH (22)
- TELNET (23)
- SMTP (25)
- DNS (53)
- HTTP (80)
- HTTPS (443)

Key Points to Remember:

- Port numbers are fixed assignments
- Transport protocol choice depends on application needs
- Out-of-line protocols use multiple ports
- Security protocols typically use TCP
- Speed-critical protocols typically use UDP

Memory Tips

Common Port Numbers:

- 7: ECHO
- 20/21: FTP
- 22: SSH
- 23: TELNET
- 25: SMTP
- 53: DNS
- 67/68: DHCP
- 69: TFTP
- 80: HTTP
- 110: POP3
- 123: NTP

- 443: HTTPS
- 520: RIP

Protocol Relationships:

- SMTP + POP = Complete email system
- HTTP + HTTPS = Web protocols (secure/unsecure)
- FTP + TFTP = File transfer (reliable/fast)
- TCP = Reliability, UDP = Speed

Conclusion

Understanding these protocols, their port numbers, and transport mechanisms is crucial for:

- Competitive examinations
- Network administration
- System design
- Troubleshooting network issues

Remember: Where UDP is used, TCP can also be used (with added reliability), but where TCP is used, UDP may not always be suitable due to reliability requirements.

Study Tip: Focus on the reasoning behind protocol choices - why certain applications need TCP vs UDP, and why specific port numbers are assigned to specific services.