Network Basics - Comprehensive Exam Notes

1. Introduction to Network Protocols

What is a Network Protocol?

- **Definition**: A set of rules used for communication between entities in different systems
- **Purpose**: Enables two entities to communicate successfully by "speaking the same language"
- **Key Elements**:
  - **What** is communicated
  - **How** it is communicated
  - **When** it is communicated

Layered Communication

- **Concept**: Complex communication tasks are divided into multiple layers
- **Benefit**: Each layer can have its own protocol, simplifying the overall system
- **Example**: Maria (Spanish) and Ann (English) using sign language as a common protocol

Real-World Analogy

- **Face-to-face communication**: Single layer (sign language)
- **Remote communication**: Multiple layers (encoding machines creating secret codes)
- This demonstrates how physical separation requires additional protocol layers

---

2. OSI Model (Open Systems Interconnection)

Background

- **Created**: 1983 by ISO (International Organization for Standardization)
- **Purpose**: Standardize network communication protocols
- **Structure**: 7 layers organized into upper and lower layers

Layer Classification

- **Upper Layers (Layers 5-7)**: Local and end-user focused
- **Lower Layers (Layers 1-4)**: Network and communication services focused

The 7 OSI Layers (Top to Bottom)

1. **Application Layer (Layer 7)**
   - User interface and application services
   - Examples: HTTP, FTP, SMTP
2. **Presentation Layer (Layer 6)**
   - Data formatting, encryption, compression
   - Character encoding, data translation
3. **Session Layer (Layer 5)**
   - Session management and control
   - Establishes, maintains, terminates connections
4. **Transport Layer (Layer 4)**
   - End-to-end data delivery
   - Error correction, flow control
   - Examples: TCP, UDP
5. **Network Layer (Layer 3)**
   - Routing and logical addressing
   - Path determination across networks
   - Example: IP
6. **Data Link Layer (Layer 2)**
   - Node-to-node delivery
   - Error detection and correction
   - Examples: Ethernet, Wi-Fi
7. **Physical Layer (Layer 1)**
   - Physical transmission of raw bits
   - Hardware specifications
   - Examples: cables, radio frequencies

---

3. TCP/IP Protocol Suite

Background

- **Development**: Created before the OSI model
- **Evolution**: Originally 4 layers, now commonly described as 5 layers
- **Practical Usage**: More widely implemented than pure OSI

TCP/IP vs OSI Model Comparison

OSI Layer	TCP/IP Layer	Function
Application, Presentation, Session	Application	User applications and services
Transport	Transport	End-to-end communication
Network	Internet	Routing and logical addressing
Data Link	Data Link	Frame transmission
Physical	Physical	Physical transmission

Key Differences

- **OSI**: 7 layers, theoretical framework
- **TCP/IP**: 5 layers (originally 4), practical implementation
- **Layer Mapping**: OSI's top 3 layers combine into TCP/IP's Application layer

---

4. Communication Process Across Layers

Physical Layer Communication

- **Data Type**: Raw bits (011...101)
- **Scope**: Direct electrical/optical signals
- **Path**: Travels through each physical link in the network

Data Link Layer Communication

- **Data Unit**: Frames
- **Components**: Header (H2) + Data (D2)
- **Function**: Node-to-node delivery with error detection
- **Address Changes**: Physical addresses change at each hop

Network Layer Communication

- **Data Unit**: Datagrams/Packets
- **Components**: Header (H3) + Data (D3)
- **Function**: End-to-end routing
- **Address Consistency**: Logical addresses remain constant

Transport Layer Communication

- **Data Unit**: Segments
- **Components**: Header (H4) + Data (D4)
- **Function**: Process-to-process delivery
- **Reliability**: Ensures complete data transmission

Application Layer Communication

- **Data Unit**: Messages
- **Components**: Data (D5)
- **Function**: User application communication
- **Simplicity**: Pure data exchange between applications

---

5. Addressing in TCP/IP

Four Levels of Addresses

1. Physical Address (Layer 2)

- **Format**: MAC address (e.g., 07:01:02:01:2C:4B)
- **Length**: 48 bits (6 bytes)
- **Scope**: Local network segment
- **Characteristic**: Changes at each network hop

2. Logical/IP Address (Layer 3)

- **IPv4 Format**: Dotted decimal (e.g., 130.130.215.2)
- **IPv6 Format**: Hexadecimal with colons
- **Scope**: Global internet
- **Characteristic**: Remains constant end-to-end

3. Port Address (Layer 4)

- **Format**: 16-bit number (e.g., 80)
- **Range**: 0-65535
- **Function**: Identifies specific application/service
- **Well-known Ports**:
  - FTP: 20 (data), 21 (control)
  - SSH: 22

  - TELNET: 23
  - SMTP: 25
  - HTTP: 80

4. Application-Specific Address (Layer 7)

- **Format**: Domain names (e.g., www.uow.edu.au)
- **Function**: Human-readable identifiers
- **Resolution**: Converted to IP addresses via DNS

Address Resolution Process

1. **Application**: Uses domain name
2. **DNS**: Resolves to IP address
3. **IP**: Routes to correct network
4. **ARP**: Resolves IP to MAC address
5. **Physical**: Transmits to specific hardware

---

6. Internet Security Threats

1. Packet Sniffing

- **Definition**: Unauthorized interception of network packets
- **Method**: Attacker reads all packets passing through network
- **Risk**: Can capture unencrypted data (passwords, personal information)
- **Prevention**:
  - Use encryption (HTTPS, VPN)
  - Implement network segmentation
  - Use switched networks instead of hubs

2. IP Spoofing

- **Definition**: Forging source IP address in packets
- **Method**: Attacker generates raw IP packets with false source addresses
- **Risk**: Receiver cannot verify actual packet source
- **Impact**: Can bypass IP-based security measures
- **Prevention**:

    - Implement ingress filtering
    - Use authentication mechanisms
    - Deploy intrusion detection systems

3. Denial of Service (DoS)

- **Definition**: Overwhelming target with malicious traffic
- **Method**: Flood of packets "swamps" receiver's capacity
- **Variants**:
    - **DoS**: Single source attack
    - **DDoS**: Multiple coordinated sources
- **Common Attacks**:
    - SYN flood attacks
    - UDP floods
    - Ping of death
- **Prevention**:
    - Rate limiting
    - Traffic filtering
    - Load balancing
    - DDoS protection services

---

7. Key Concepts for Exam Success

Essential Definitions

- **Protocol**: Set of communication rules
- **Encapsulation**: Adding headers at each layer
- **Routing**: Path selection for data transmission
- **Addressing**: Identifying network entities at different layers

Layer Functions Memory Aid

- **Physical**: "Please" - Physical transmission
- **Data Link**: "Do" - Direct node-to-node delivery
- **Network**: "Not" - Network routing
- **Transport**: "Throw" - Transport reliability

- **Session**: "Sausage" - Session management
- **Presentation**: "Pizza" - Presentation formatting
- **Application**: "Away" - Application services

Common Exam Questions

1. **Layer identification**: Match protocols to OSI layers
2. **Address types**: Identify address formats and purposes
3. **Communication flow**: Trace data through network layers
4. **Security threats**: Explain attack methods and countermeasures
5. **Protocol comparison**: OSI vs TCP/IP differences

Study Tips

- **Understand, don't memorize**: Focus on concepts and relationships
- **Practice scenarios**: Work through communication examples
- **Know the numbers**: Memorize well-known port numbers
- **Security awareness**: Understand threat mechanisms and defenses
- **Real-world application**: Connect concepts to actual network technologies

---

8. Additional Resources

Recommended Video

- **Warriors of the Net**: Animated introduction to TCP/IP networking
- **URL**: http://www.youtube.com/watch?v=TBxZgOGjyZc
- **Value**: Visual representation of packet journey through network layers

Further Reading

- Behrouz A. Forouzan, "TCP/IP Protocol Suite"
- OSI Model detailed specifications
- Current network security best practices