Networking

Protocols & Ports

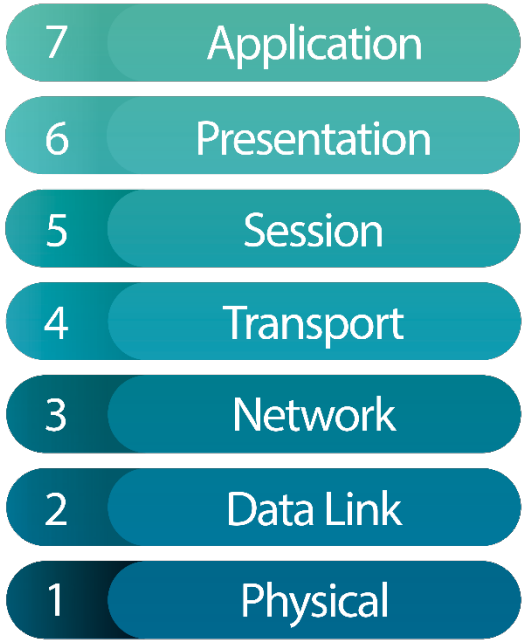
Protocols & Ports

- Guiding Question: How do protocols at the upper layers of the OSI model facilitate secure and efficient communication across networks?

- Students will:
  - Explain the roles of the Session, Presentation, and Application layers in network communication.
  - Identify and describe common Application Layer protocols and their functions.
  - Match key protocols to their corresponding port numbers and understand their importance.

Layers 5 -7

- Layers 5-7 of the OSI Model work together to help applications communicate across networks.
- They establish connections, format data, and provide services to users.
- **Application Layer**
  - User interfaces and network services.
- **Presentation Layer**
  - Data formatting and encryption.
- **Session Layer**
  - Connection management.



Protocols & Ports

- Most protocols are associated with a specific port number.
- The port number indicates to the computer which application should handle the incoming data.
- Ports are like doors – they are openings to handle a specific type of packet.
- **Example:** A web browser uses the HTTP protocol which usually uses Port 80.
  - This port is not mandatory, but a website that is NOT listening on Port 80 will have to let each user know the custom port that is being used.

Why Ports Matter

- **Traffic Direction**
  - Ports guide data to the right application.
- **Standardization**
  - Common ports work across all networks.
- **Security Control**
  - Firewalls can block specific ports.
- **Multiple Services**
  - Different ports allow simultaneous connections.

Remote Access Protocols

- **Telnet – Port 23**
  - Allows remote access but sends data in plain text.
  - Terminal commands only.
  - Not secure for sensitive information.
- **SSH – Port 22**
  - Secure Shell provides encrypted command-line access to remote devices.
  - Used by administrators to securely manage servers.
  - Terminal commands only.
- **RDP – Port 3389**
  - Remote Desktop Protocol gives graphical interface access to Windows computers.

File Transfer Protocols

- **FTP – Ports 20/21**
  - File Transfer Protocol transfers files between computers.
  - Not secure.
- **SFTP – Port 22**
  - Secure FTP uses SSH to secure file transfers with encryption.
- **TFTP – Port 69**
  - Trivial FTP is transported by UDP to provide fast file transfers for network devices.

Web Browsing Protocols

- **HTTP – Port 80**
  - Hypertext Transfer Protocol transfers web pages and content. Not encrypted.
  - Used for basic browsing.
- **HTTPS – Port 443**
  - HTTP Secure encrypts data between browser and server.
  - Used for secure transactions.
  - Each browser has a symbol in the address bar, usually a padlock, to let you know you are browsing securely using HTTPS.

Email Protocols

- **SMTP - Port 25**
  - Simple Mail Transport Protocol is used to deliver email to a server.
- **SMTPS – Port 587**
  - SMTP Secure delivers email using encryption for security.
- **POP3 - Port 110**
  - Post Office Protocol v3 is used to receive and store email until the user connects to the server and collects the email.
  - Some servers use IMAP, an older mailbox protocol.

Database Communication

Databases store and organize information. SQL Server uses port 1433 to communicate with client applications that need to access data.

- **SQL – Port 1433**
  - Structured Query Language is used for database management.
  - There are many versions of SQL used by specific types of databases like Microsoft, Oracle, MongoDB, SQLLite, etc. These may use a port other than 1433.