Session 7 – Chapter 11 (pg. 491-580)

2025 CISSP Mentor Program

CHAPTER 11

Evan Francen

FRSecure

2025 CISSP MENTOR PROGRAM

AGENDA – SESSION 7

Chapter 11 (from the book)

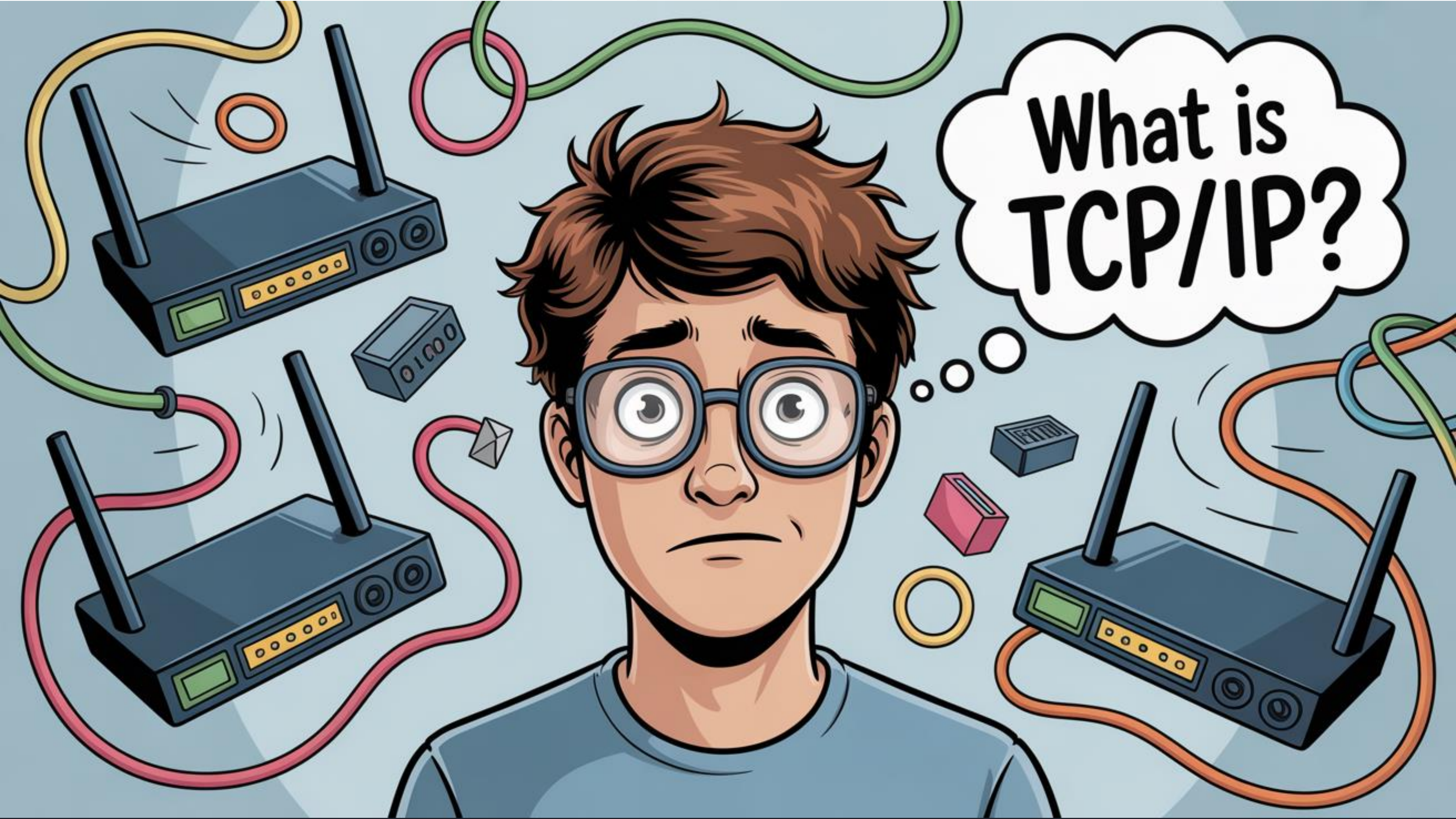
Chapter 11 - Secure Network Architecture and Components

- OSI Model
- TCP/IP Model
- Analyzing Network Traffic
- Common Application Layer Protocols
- Transport Layer Protocols
- Domain Name System
- Internet Protocol (IP) Networking
- ARP Concerns
- Secure Communications Protocols
- Implications of Multilayer Protocols
- Segmentation
- Edge Networks
- Wireless Networks
- Satellite Communications
- Cellular Networks
- Content Distribution Networks (CDNs)
- Secure Network Components

No worries.

Only 266 slides in this lesson.

(P.S. For anyone who cares, I never want to see a PowerPoint slide deck ever again)


What is TCP/IP?

Because he was outstanding in his field.

2025 CISSP MENTOR PROGRAM

CHAPTER 11

OSI Model

CHAPTER 11

OSI Model

The **OSI (Open Systems Interconnection) Model** is a conceptual framework used to understand how different networking protocols interact in a layered architecture. It breaks down the complex process of data communication into 7 distinct layers, each with a specific role.

- Developed in the late 1970s/early 1980s by the International Organization for Standardization (ISO)
- Officially published in 1984.
- Prior to OSI, proprietary networking systems from IBM, DEC, Xerox, etc. could not talk with each other.
- A universal framework that has **stood the test of time**.

CHAPTER 11

OSI Model

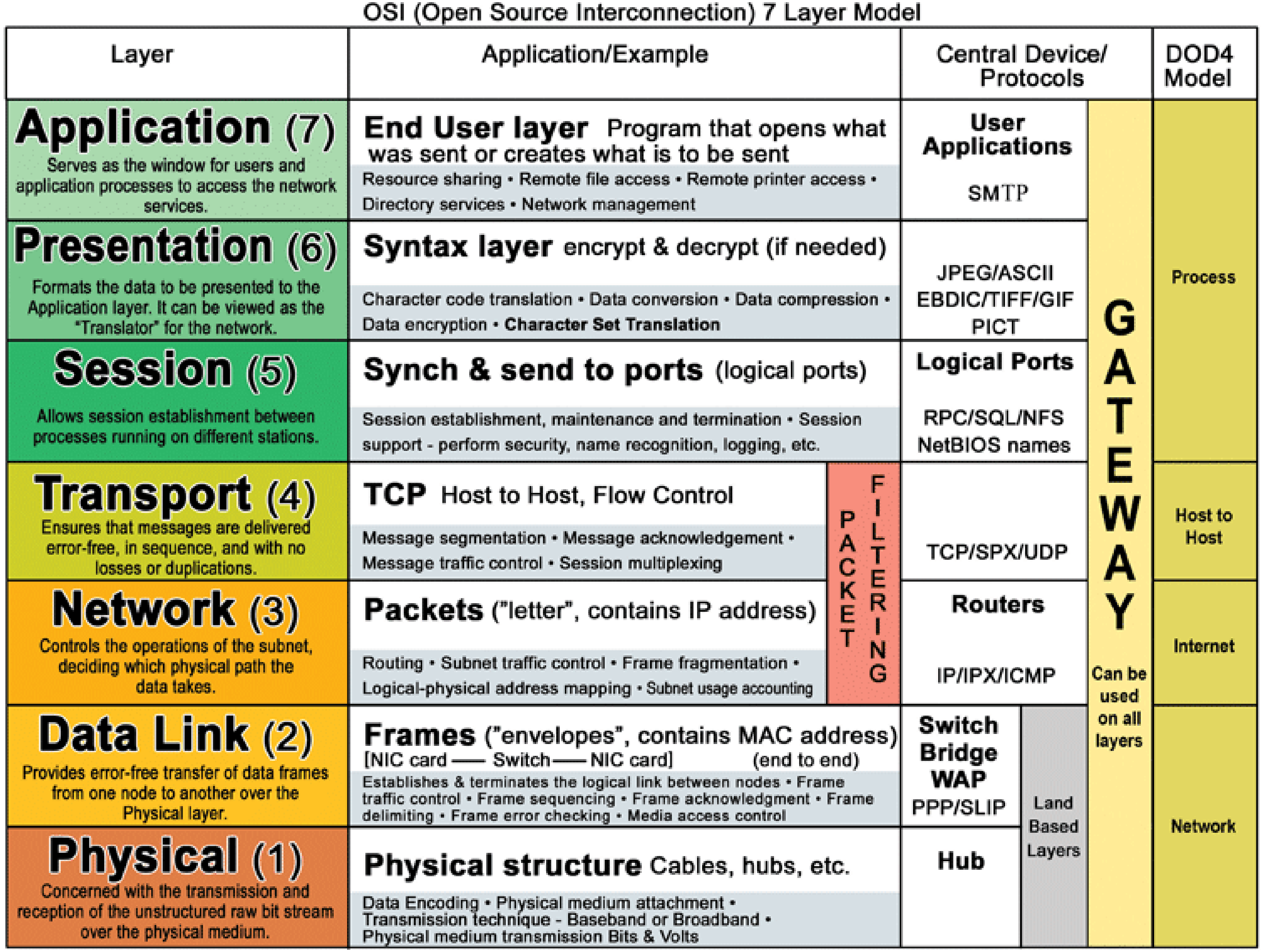
The **OSI (Open Systems Interconnection) Model** is a conceptual framework used to understand how different networking protocols interact in a layered architecture. It breaks down the complex process of data communication into 7 distinct layers, each with a specific role.

- Developed in the late 1970s/early 1980s by the International Organization for Standardization (ISO)
- Officially
- Prior to O each othe
- A univers

Protocols = Rules

Purpose of the OSI Model

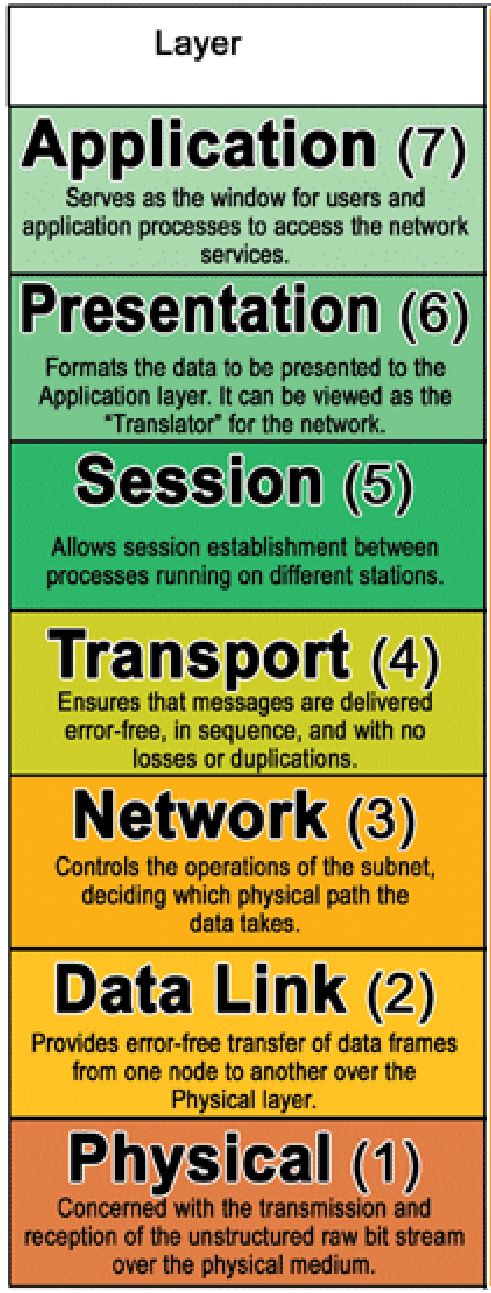
- **Standardization** - Enables interoperability between different hardware and software systems by defining standard functions at each layer.
- **Modularity** - Breaks networking into 7 logical layers, making it easier to understand, develop, troubleshoot, and secure.
- **Vendor-Neutral Reference** - Provides a conceptual model that can be applied across different platforms and technologies.
- **Troubleshooting Aid** - Helps security professionals and network engineers isolate issues by analyzing layer-by-layer.



OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP		**GATEWAY** Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP			Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card —— Switch —— NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch** **Bridge** **WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

OSI (Open Source Interconnection) 7 Layer Model



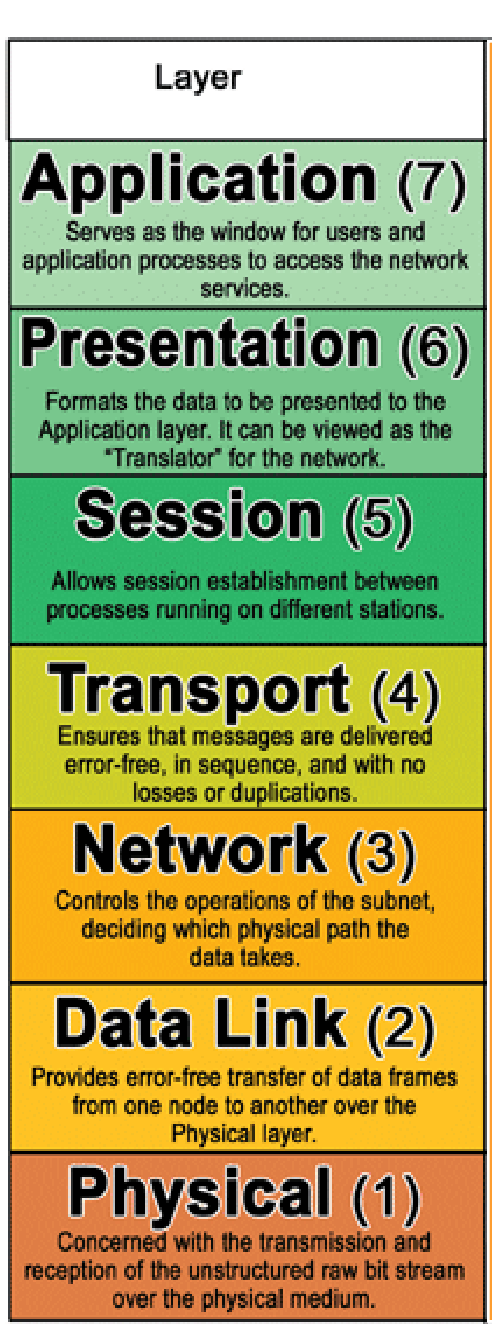
Layer
Application (7) Serves as the window for users and application processes to access the network services.
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.
Session (5) Allows session establishment between processes running on different stations.
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.

Mnemonic #1

"Please Do Not Throw Sausage Pizza Away"

- Physical
- Data Link
- Network
- Transport
- Session
- Presentation
- Application

Bottom up…



OSI (Open Source Interconnection) 7 Layer Model

Layer
Application (7) Serves as the window for users and application processes to access the network services.
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.
Session (5) Allows session establishment between processes running on different stations.
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.

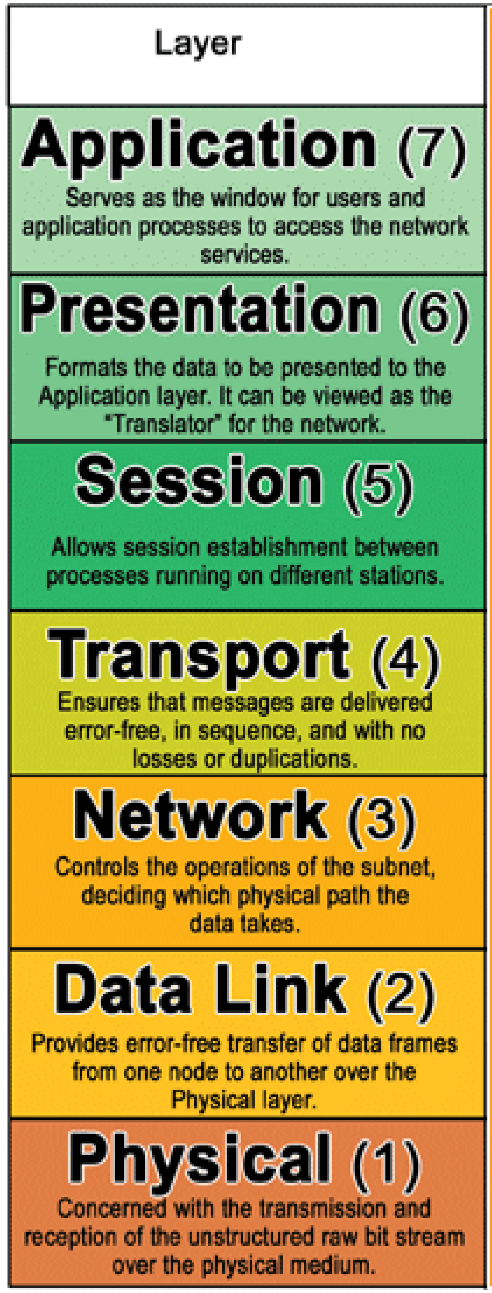
Mnemonic #2

"All People Seem To Need Data Processing"

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

Top down…

OSI (Open Source Interconnection) 7 Layer Model



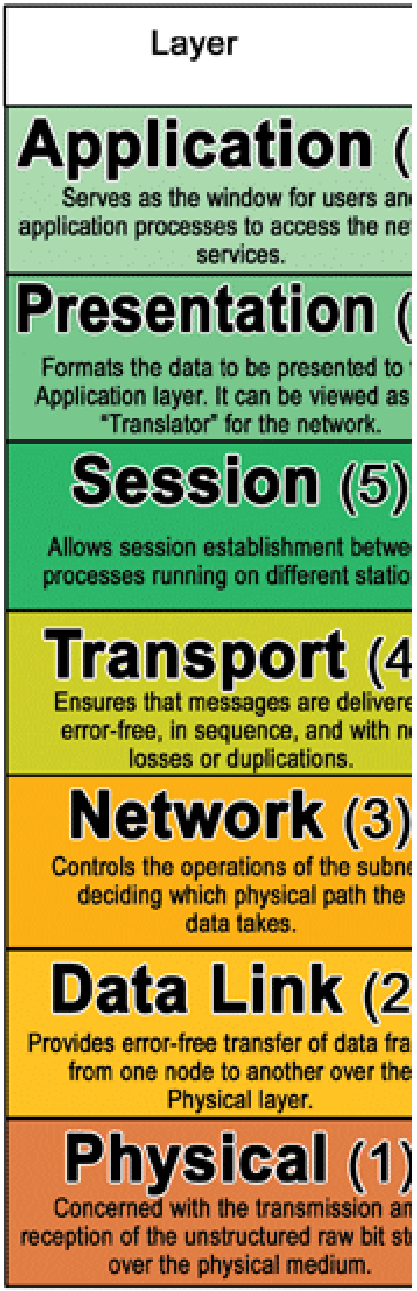
Layer
Application (7) Serves as the window for users and application processes to access the network services.
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.
Session (5) Allows session establishment between processes running on different stations.
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.

Mnemonic #3

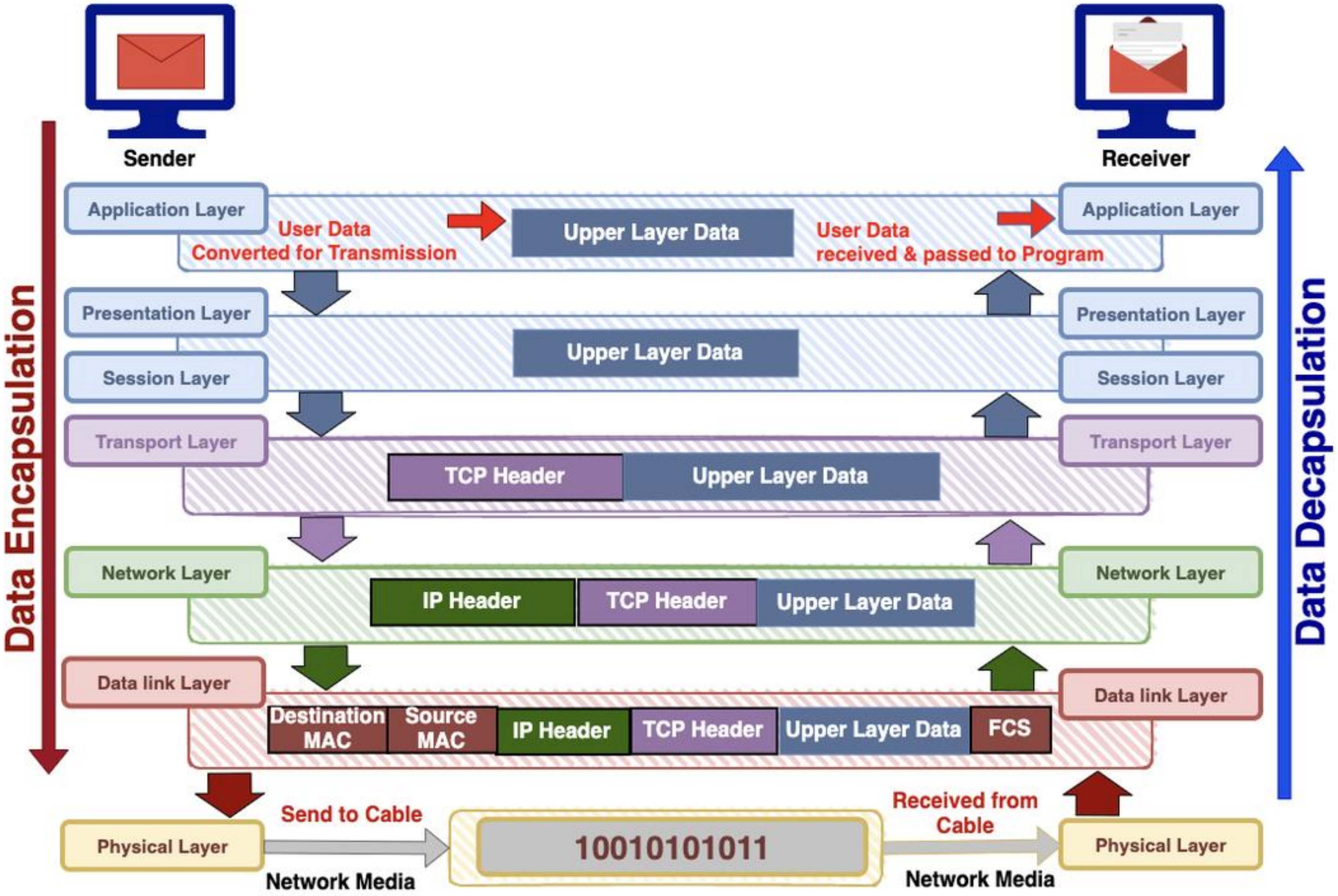
"People Don't Need To See Paula Abdul"

- Physical
- Data Link
- Network
- Transport
- Session
- Presentation
- Application

Bottom up…



Layer
Application (Serves as the window for users an application processes to access the ne services.
Presentation (Formats the data to be presented to Application layer. It can be viewed as "Translator" for the network.
Session (5) Allows session establishment betwe processes running on different statio
Transport (4 Ensures that messages are delivere error-free, in sequence, and with n losses or duplications.
Network (3) Controls the operations of the subn deciding which physical path the data takes.
Data Link (2 Provides error-free transfer of data fra from one node to another over the Physical layer.
Physical (1) Concerned with the transmission an reception of the unstructured raw bit st over the physical medium.



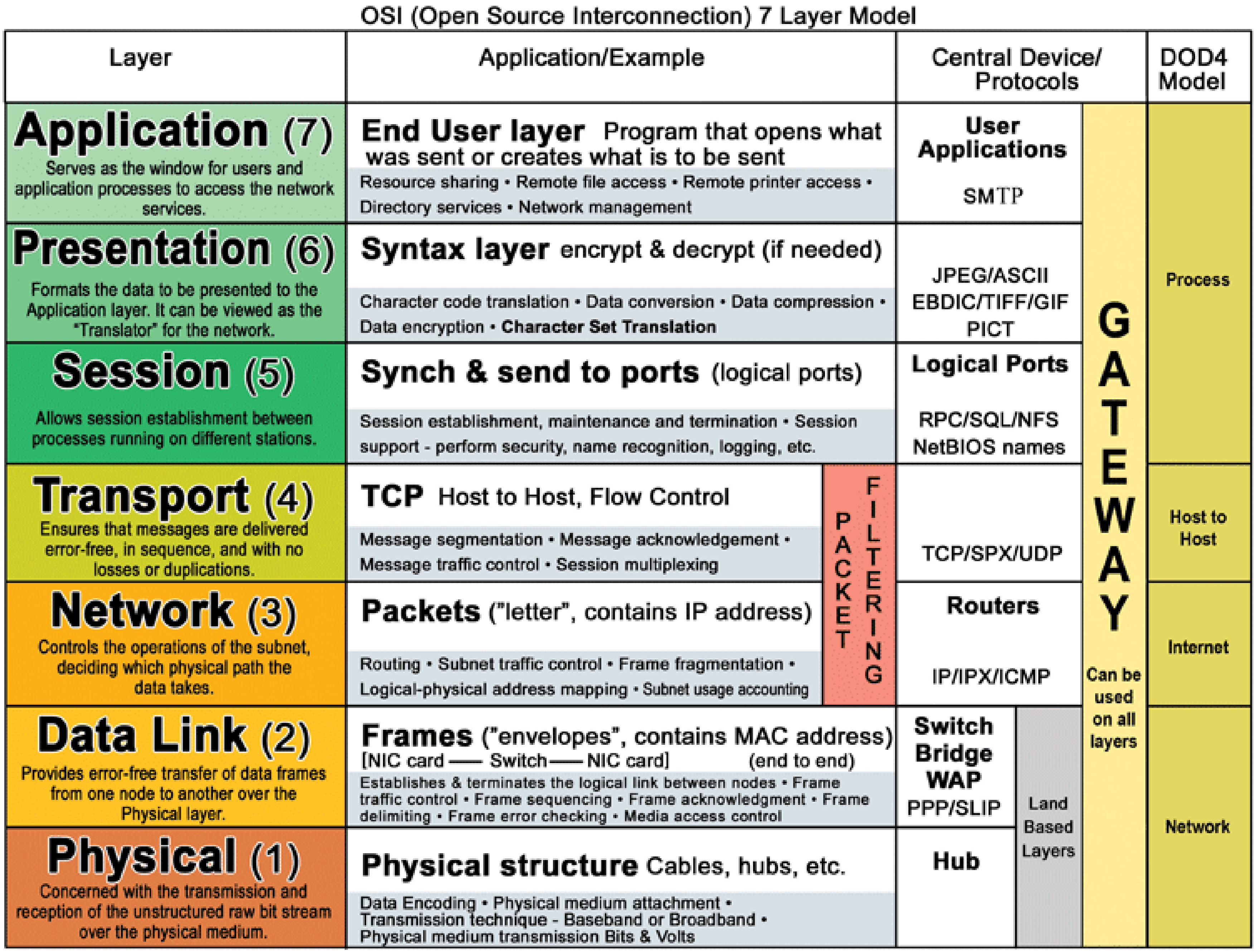
Protocol Data Units (PDUs)

Segments (TCP)
Datagrams (UDP)

Packets

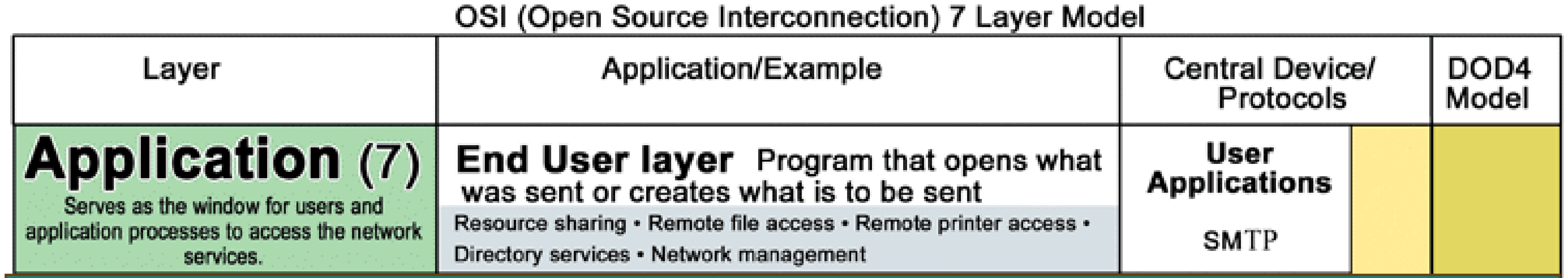
Frames

Bits



OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP		**GATEWAY** Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP			Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card —— Switch —— NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			



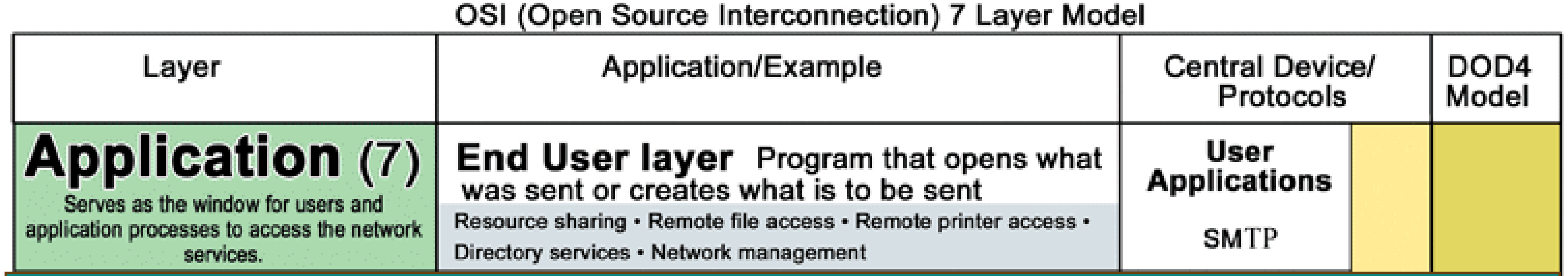
OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	**User Applications** SMTP		

Application Layer

- The top layer (Layer 7) of the OSI Model.
- The layer closest to the end user.
- Responsible for interfacing directly with software applications that use the network.
- Does NOT provide the applications themselves, but provides services applications use
- Enables functions like:
  - Email (SMTP)
  - Web browsing (HTTP/HTTPS)
  - File transfers (FTP)
  - DNS lookups

If the user sees it or interacts with it, it’s probably at the Application Layer.



OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols	DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	**User Applications** SMTP	

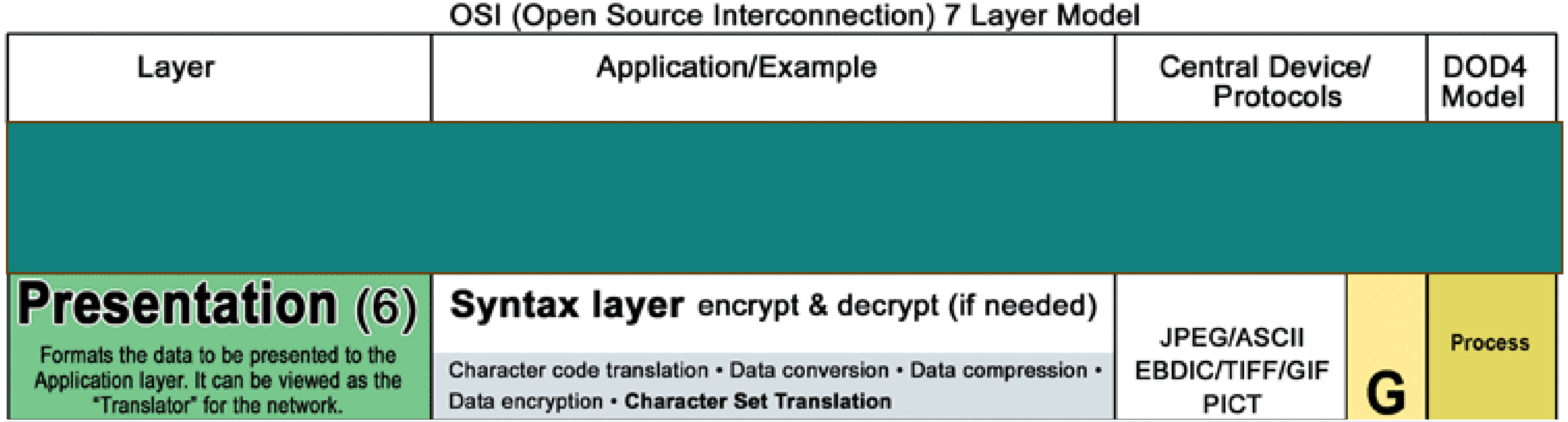
Application Layer

- The top layer (Layer 7) of the OSI Model.
- The layer closest to the end user.
- Responsible for interfacing directly with software applications that use the network.
- Does NOT provide the applications themselves, but provides services applications use
- Enables
  - Ema
  - We
  - File
  - DN

Security Relevance:

- Many attacks target this layer (e.g., SQL injection, cross-site scripting, buffer overflows).
- Security controls at this layer include:
  - Input validation
  - Secure coding practices
  - Application firewalls (WAFs)

If the user sees it or interacts with it, it's probably at the Application Layer.



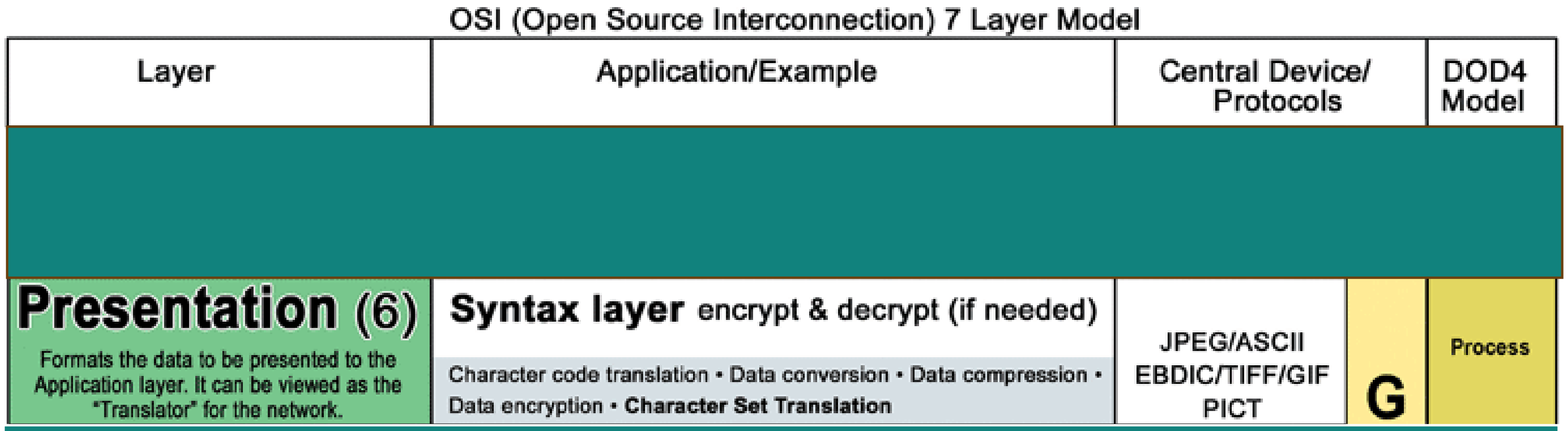
OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols		DOD4 Model
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**	JPEG/ASCII EBDIC/TIFF/GIF PICT	G	Process

Presentation Layer

- Layer 6 of the OSI Model.
- Prepare data for the Application Layer.
- **Data translation**: Converts data between different formats (e.g., EBCDIC to ASCII).
- **Encryption/decryption**: Applies security functions like SSL/TLS (often debated as Layer 6 or 7).
- **Compression**: Reduces file sizes for efficient transmission (e.g., JPEG, MPEG, ZIP)

It's like the translator and security guard between the network and the app.



OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols		DOD4 Model
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**	JPEG/ASCII EBDIC/TIFF/GIF PICT	G	Process

Presentation Layer

- Layer 6 of the OSI Model.
- Prepare data for the Application Layer.
- **Data translation**: Converts data between different formats (e.g., EBCDIC to ASCII).
- **Encryption/decryption**: Applies security functions like SSL/TLS (often debated as L
- **Compressior**
  MPEG, ZIP)

Security Relevance:

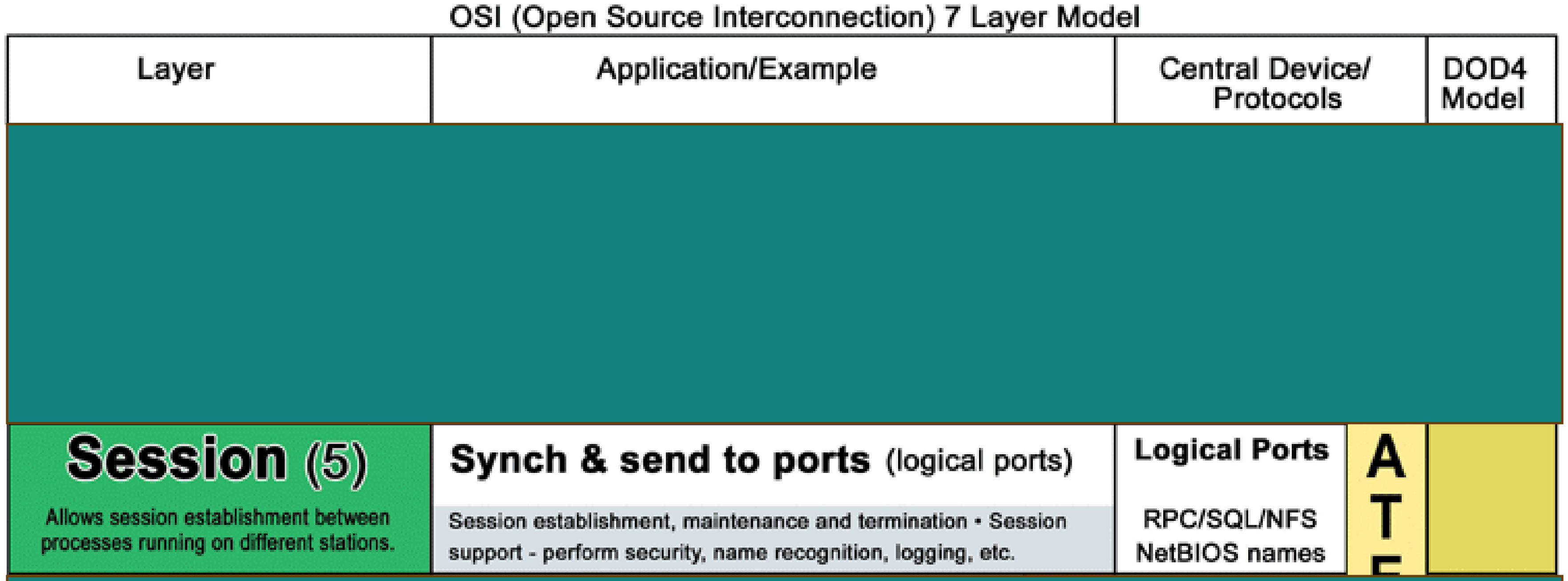
- This is where TLS/SSL encryption happens in many models.
- Poor handling here can lead to data leakage or cipher downgrade attacks.

It's like the translator and security guard between the network and the app.

20

C

O



OSI (Open Source Interconnection) 7 Layer Model

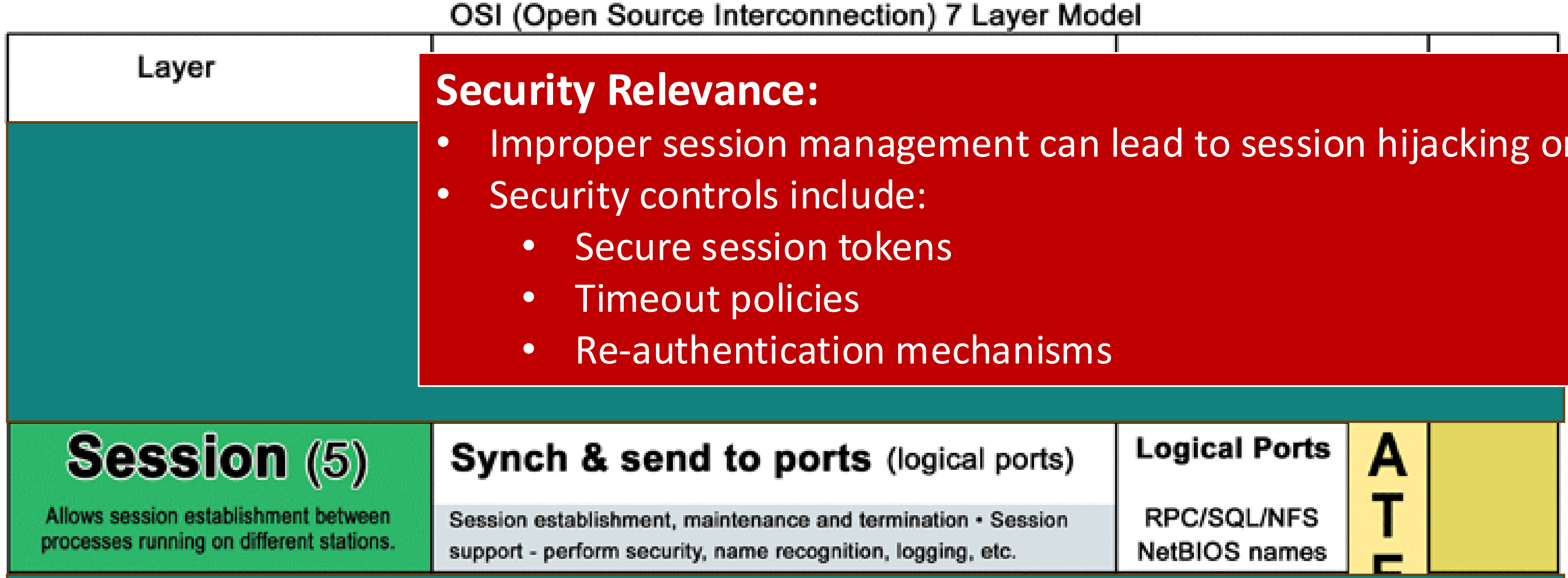
Layer	Application/Example	Central Device/ Protocols		DOD4 Model
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	**Logical Ports** RPC/SQL/NFS NetBIOS names	**A T**	

Session Layer

- Layer 5 of the OSI Model.
- **Session establishment, maintenance, and teardown** - Coordinates conversations between systems (like setting up a Zoom call, maintaining it, then hanging up).
- **Synchronization** - Manages checkpoints and recovery (e.g., in long data transfers).
- **Dialog control** - Determines who can send data, and when (full-duplex, half-duplex).

Like a call center operator—it sets up the call, keeps it going, and ends it cleanly.

OSI (Open Source Interconnection) 7 Layer Model



Layer				
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	**Logical Ports** RPC/SQL/NFS NetBIOS names	A T E	

Security Relevance:

- Improper session management can lead to session hijacking or replay attacks.
- Security controls include:
  - Secure session tokens
  - Timeout policies
  - Re-authentication mechanisms

Session Layer

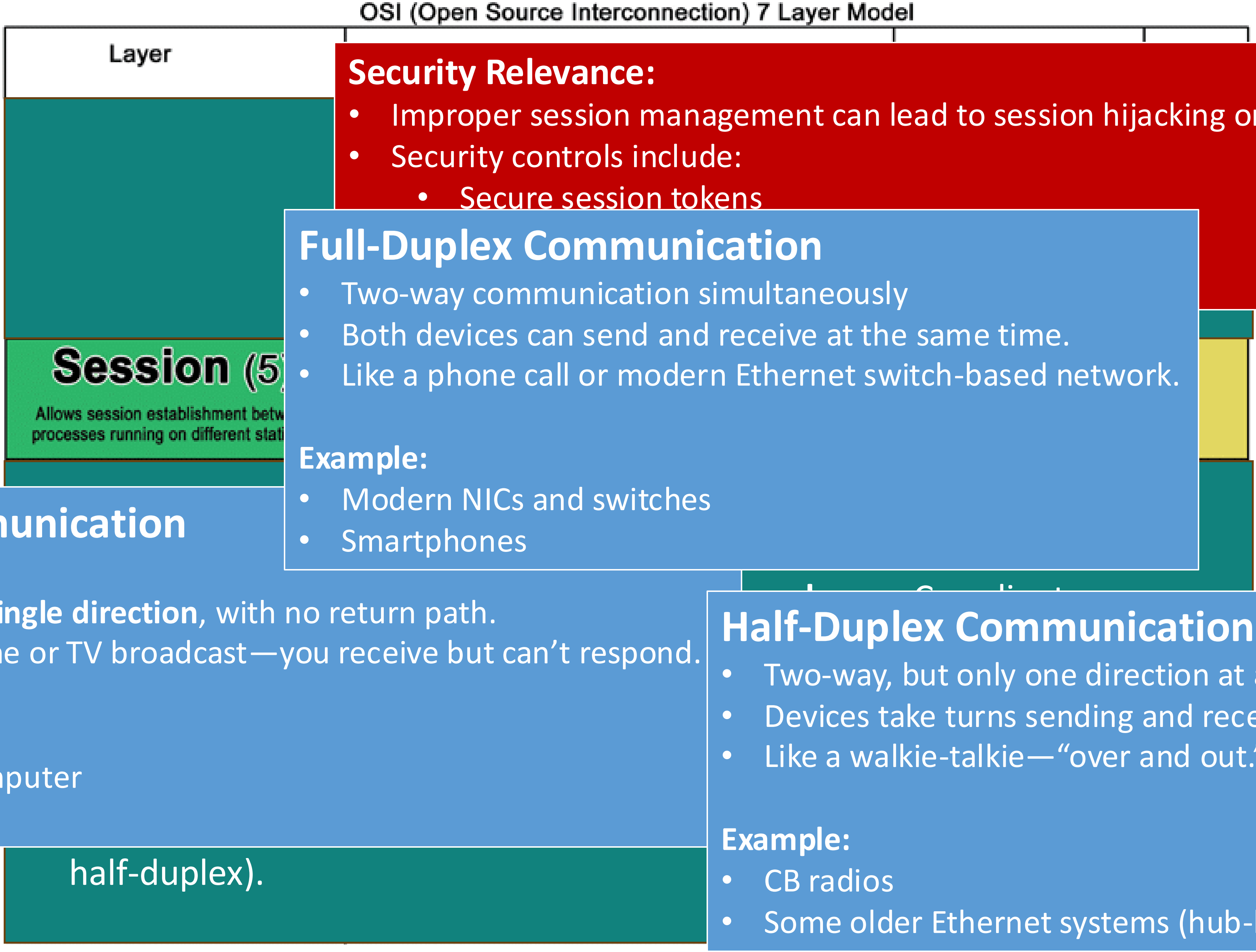
- Layer 5 of the OSI Model.
- **Session establishment, maintenance, and teardown** - Coordinates conversations between systems (like setting up a Zoom call, maintaining it, then hanging up).
- **Synchronization** - Manages checkpoints and recovery (e.g., in long data transfers).
- **Dialog control** - Determines who can send data, and when (full-duplex, half-duplex).

Like a call center operator—it sets up the call, keeps it going, and ends it cleanly.

20

C

O



OSI (Open Source Interconnection) 7 Layer Model

Layer

Session (5)

Allows session establishment betw

processes running on different stati

half-duplex).

Security Relevance:

- Improper session management can lead to session hijacking or replay attacks.
- Security controls include:
  - Secure session tokens

Full-Duplex Communication

- Two-way communication simultaneously
- Both devices can send and receive at the same time.
- Like a phone call or modern Ethernet switch-based network.

Example:

- Modern NICs and switches
- Smartphones

Simplex Communication

- One-way only
- Data flows in a **single direction**, with no return path.
- Like a megaphone or TV broadcast—you receive but can't respond.

Example:

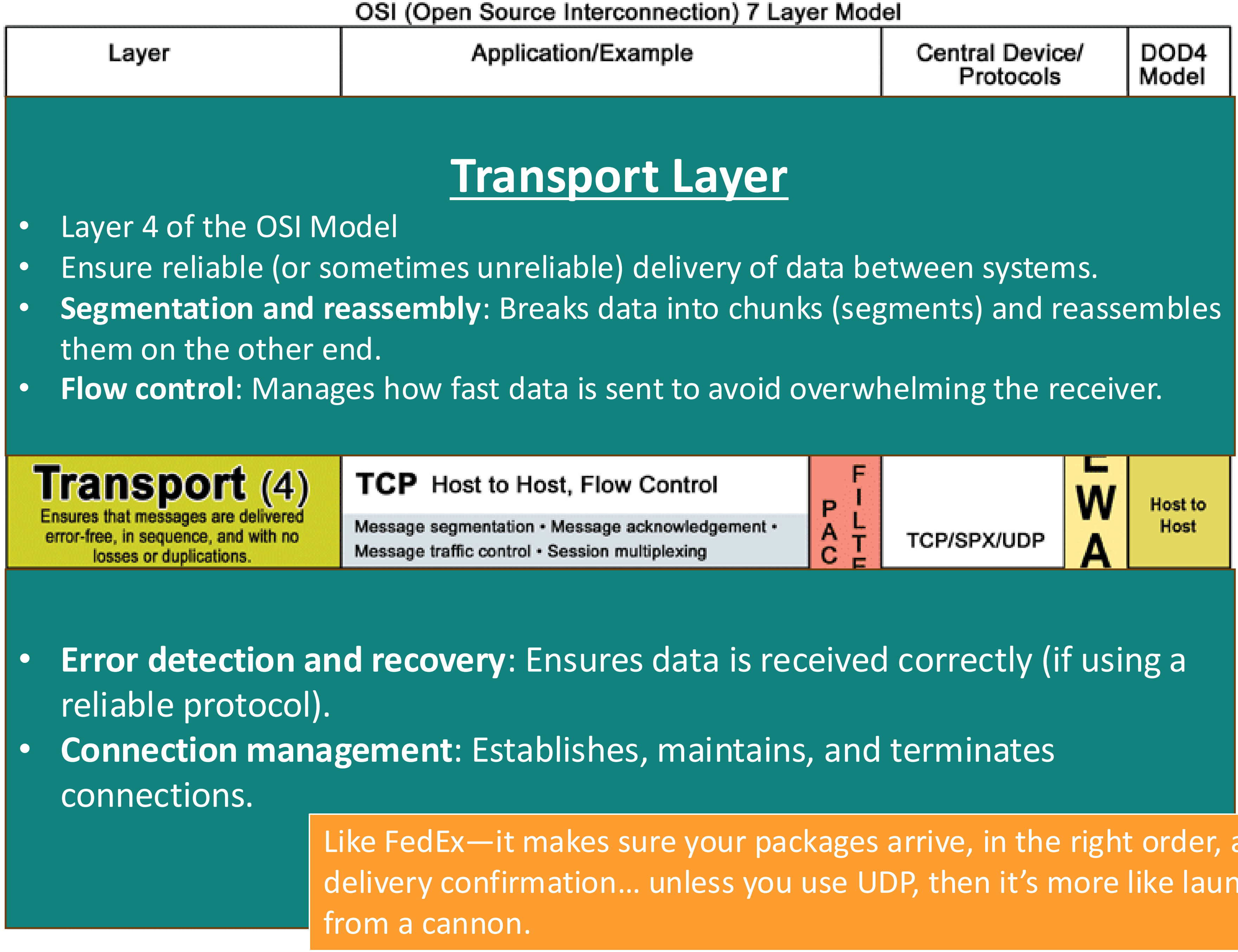
- Keyboard to computer
- FM radio

Half-Duplex Communication

- Two-way, but only one direction at a time
- Devices take turns sending and receiving.
- Like a walkie-talkie—"over and out."

Example:

- CB radios
- Some older Ethernet systems (hub-based)



OSI (Open Source Interconnection) 7 Layer Model

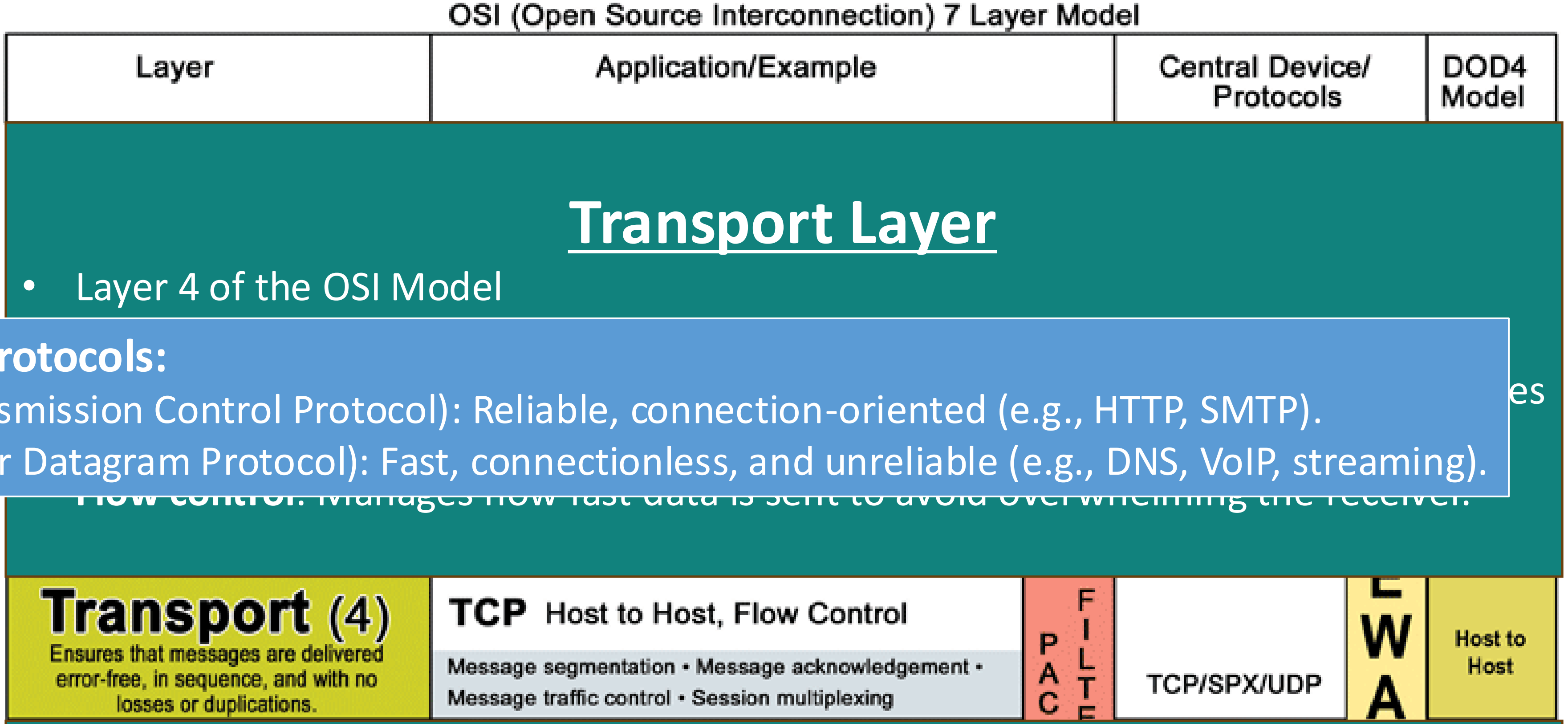
Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PAC FILTE	TCP/SPX/UDP	W A	Host to Host

Transport Layer

- Layer 4 of the OSI Model
- Ensure reliable (or sometimes unreliable) delivery of data between systems.
- **Segmentation and reassembly**: Breaks data into chunks (segments) and reassembles them on the other end.
- **Flow control**: Manages how fast data is sent to avoid overwhelming the receiver.

- **Error detection and recovery**: Ensures data is received correctly (if using a reliable protocol).
- **Connection management**: Establishes, maintains, and terminates connections.

Like FedEx—it makes sure your packages arrive, in the right order, and with delivery confirmation… unless you use UDP, then it's more like launching T-shirts from a cannon.



OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PAC FILTE	TCP/SPX/UDP	L W A	Host to Host

Transport Layer

- Layer 4 of the OSI Model

es

Common Protocols:

- TCP (Transmission Control Protocol): Reliable, connection-oriented (e.g., HTTP, SMTP).
- UDP (User Datagram Protocol): Fast, connectionless, and unreliable (e.g., DNS, VoIP, streaming).

Flow control: Manages how fast data is sent to avoid overwhelming the receiver.

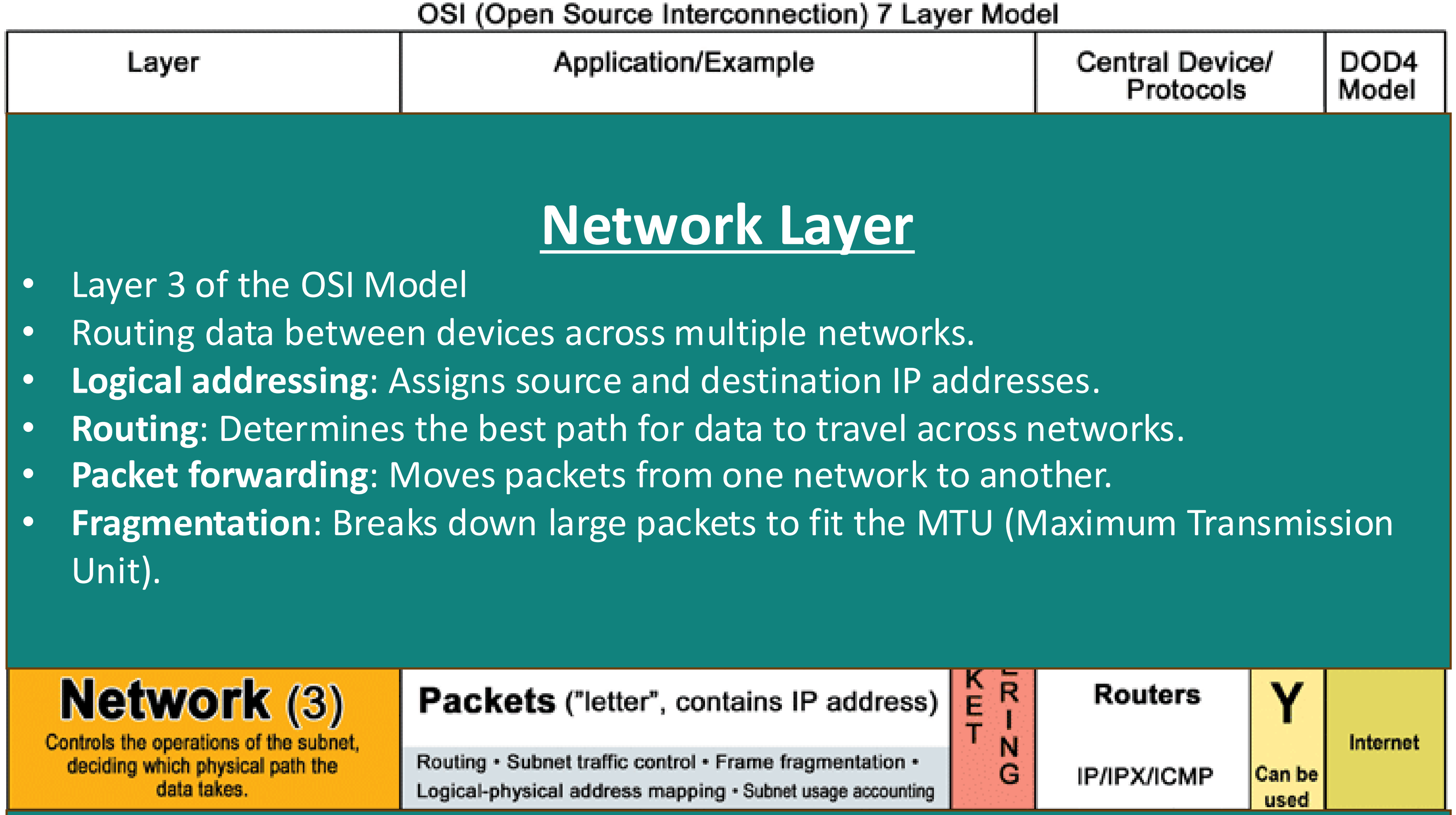
f using a

Security Relevance:

- Attacks like port scanning, SYN floods, and session hijacking happen at this layer.
- Controls include firewalls, IDS/IPS, and stateful inspection.

connections.

Like FedEx—it makes sure your packages arrive, in the right order, and with delivery confirmation… unless you use UDP, then it's more like launching T-shirts from a cannon.



OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	KET RING	**Routers** IP/IPX/ICMP	**Y** Can be used	Internet

Network Layer

- Layer 3 of the OSI Model
- Routing data between devices across multiple networks.
- **Logical addressing**: Assigns source and destination IP addresses.
- **Routing**: Determines the best path for data to travel across networks.
- **Packet forwarding**: Moves packets from one network to another.
- **Fragmentation**: Breaks down large packets to fit the MTU (Maximum Transmission Unit).

Like using a GPS—deciding where your data goes and how it gets there.

Network Layer

- Layer 3 of the OSI Model

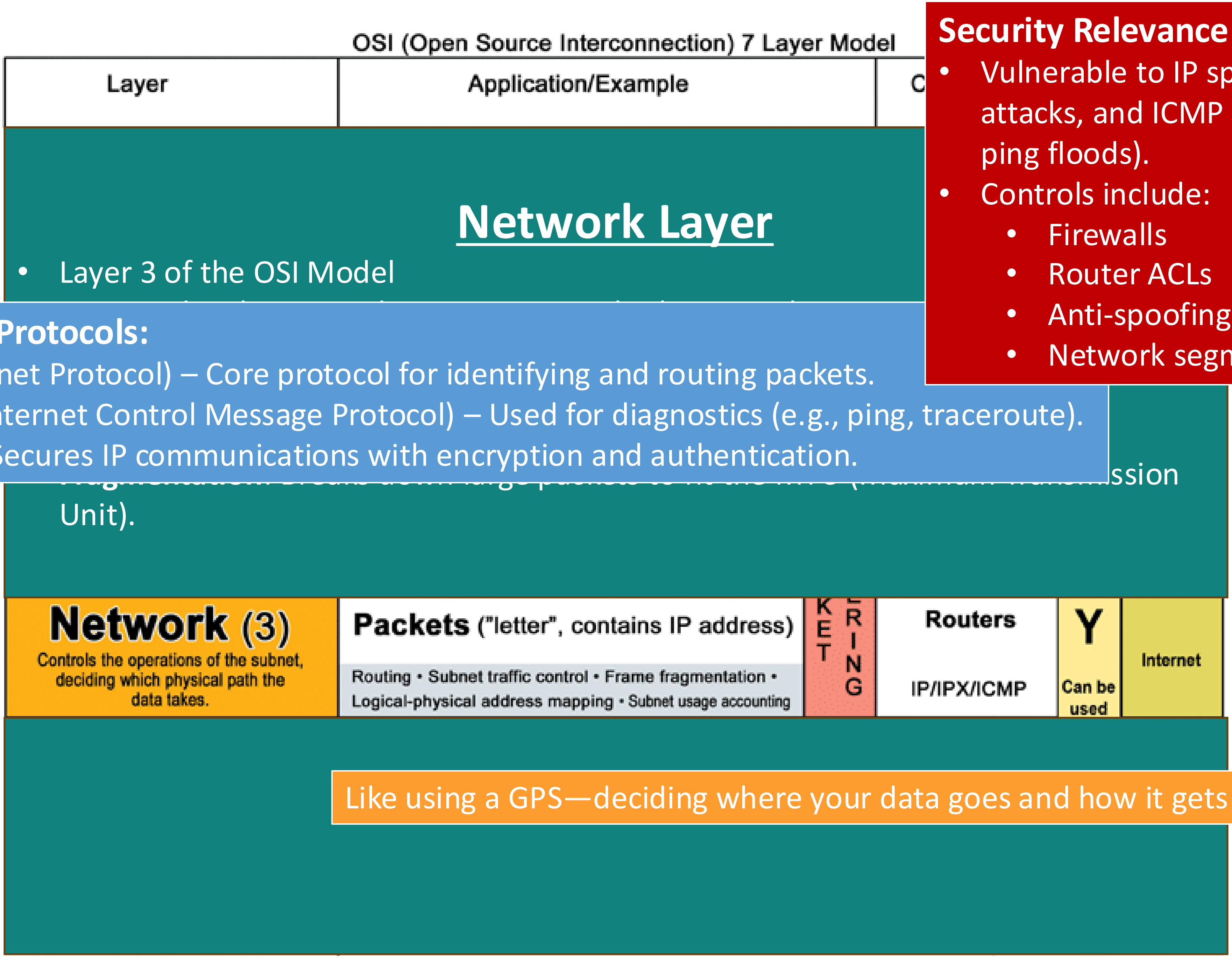
ssion Unit).

Common Protocols:

- IP (Internet Protocol) – Core protocol for identifying and routing packets.
- ICMP (Internet Control Message Protocol) – Used for diagnostics (e.g., ping, traceroute).
- IPsec – Secures IP communications with encryption and authentication.

Security Relevance:

- Vulnerable to IP spoofing, routing attacks, and ICMP misuse (e.g., ping floods).
- Controls include:
  - Firewalls
  - Router ACLs
  - Anti-spoofing filters
  - Network segmentation



OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	C				
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	KET	RING	Routers IP/IPX/ICMP	Y Can be used	Internet

Like using a GPS—deciding where your data goes and how it gets there.

Routing protocols determine how routers communicate with each other to find the best path for forwarding packets across a network.

They fall into two main categories:

1. **Interior Routing Protocols (IGPs)**
2. **Exterior Routing Protocols (EGPs)**

- IP (Internet Protocol) – Core protoc
- ICMP (Internet Control Message Pr
- IPsec – Secures IP communications

Unit).

Interior Gateway Protocols (IGPs)

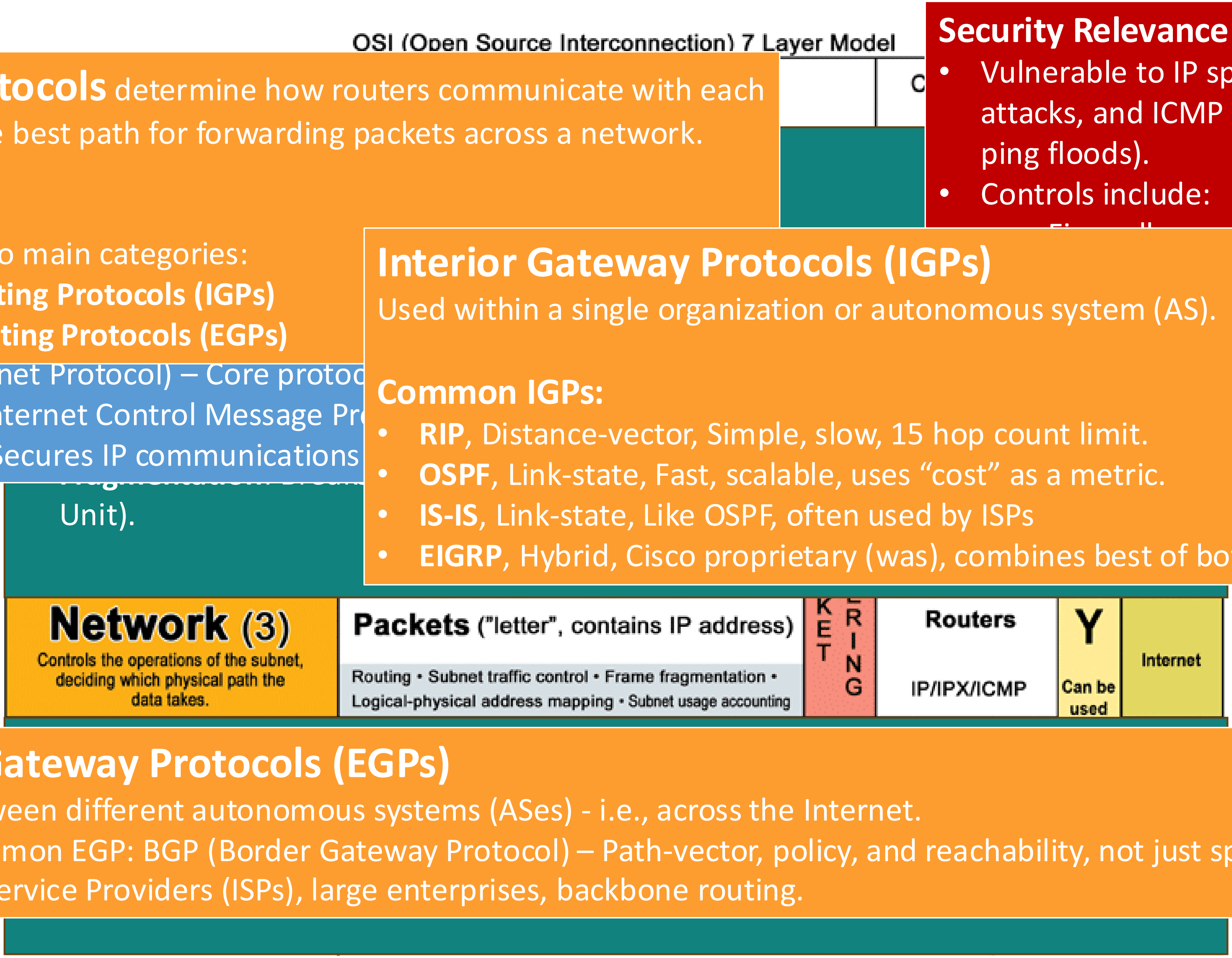
Used within a single organization or autonomous system (AS).

Common IGPs:

- **RIP**, Distance-vector, Simple, slow, 15 hop count limit.
- **OSPF**, Link-state, Fast, scalable, uses "cost" as a metric.
- **IS-IS**, Link-state, Like OSPF, often used by ISPs
- **EIGRP**, Hybrid, Cisco proprietary (was), combines best of both types.

Security Relevance:

- Vulnerable to IP spoofing, routing attacks, and ICMP misuse (e.g., ping floods).
- Controls include:



OSI (Open Source Interconnection) 7 Layer Model

Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	KET RING	**Routers** IP/IPX/ICMP	**Y** Can be used	Internet

Exterior Gateway Protocols (EGPs)

- Used between different autonomous systems (ASes) - i.e., across the Internet.
- Most Common EGP: BGP (Border Gateway Protocol) – Path-vector, policy, and reachability, not just speed and cost.
- Internet Service Providers (ISPs), large enterprises, backbone routing.

FRSECURE

Security Relevance:

- Vulnerable to IP spoofing, routing attacks, and ICMP misuse (e.g.,

Routing protocols determine how routers communicate with each other to find

They fall into

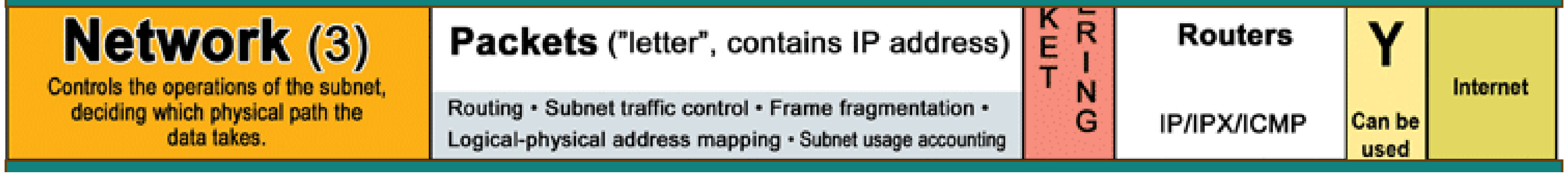
1. **Interior**
2. **Exterior**

- IP (I
- ICM
- IPse

Feature	IGP (Interior)	EGP (Exterior)
Scope	Within an AS	Between ASes
Common Protocols	RIP, OSPF, EIGRP, IS-IS	BGP
Trust Model	Assumes trust	Assumes untrusted neighbors
Convergence Speed	Fast (esp. OSPF)	Slower (but stable)
Complexity	Lower	Higher (policy-driven, scalable)
Control	More centralized	Distributed, policy-based

- **EIGRP**, Hybrid, Cisco proprietary (was), combines best of both types.

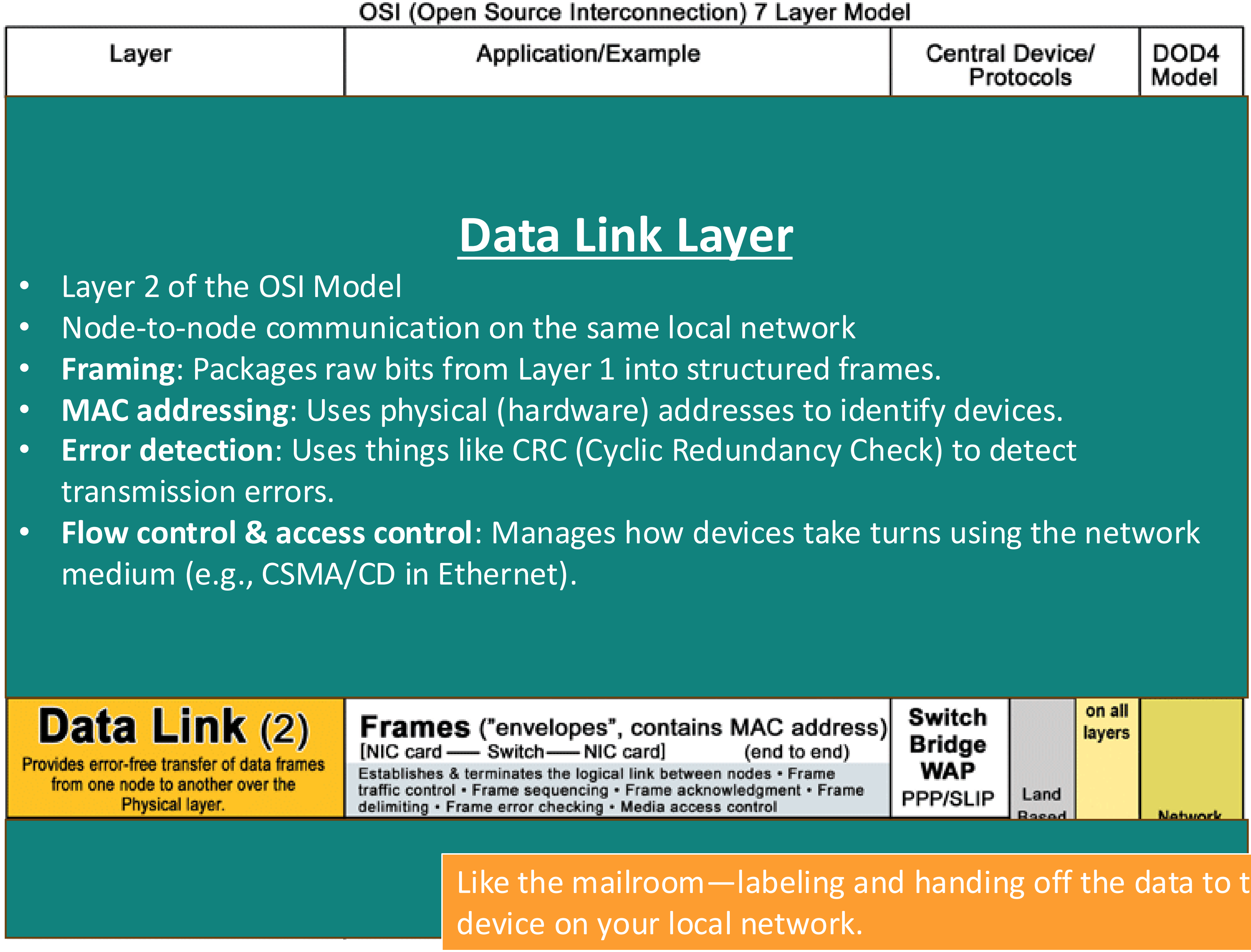
OSI (Open Source Interconnection) 7 Layer Model



Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	KET	RING	**Routers** IP/IPX/ICMP	**Y** Can be used	Internet

Exterior Gateway Protocols (EGPs)

- Used between different autonomous systems (ASes) - i.e., across the Internet.
- Most Common EGP: BGP (Border Gateway Protocol) – Path-vector, policy, and reachability, not just speed and cost.
- Internet Service Providers (ISPs), large enterprises, backbone routing.



OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols			DOD4 Model
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card —— Switch —— NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	**Switch** **Bridge** **WAP** PPP/SLIP	Land Based	on all layers	Network

Data Link Layer

- Layer 2 of the OSI Model
- Node-to-node communication on the same local network
- **Framing**: Packages raw bits from Layer 1 into structured frames.
- **MAC addressing**: Uses physical (hardware) addresses to identify devices.
- **Error detection**: Uses things like CRC (Cyclic Redundancy Check) to detect transmission errors.
- **Flow control & access control**: Manages how devices take turns using the network medium (e.g., CSMA/CD in Ethernet).

Like the mailroom—labeling and handing off the data to the right device on your local network.

OSI (Open Source Interconnection) 7 Lay

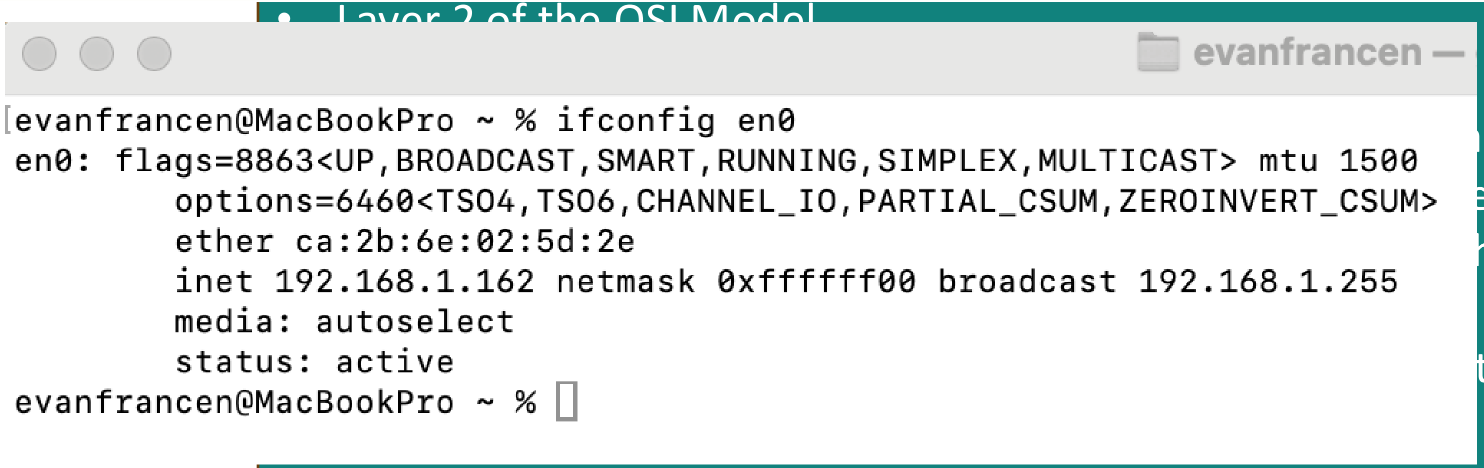
Common Protocols & Technologies:

ayer.

MAC Address

- Unique hardware identifier assigned to a network interface card (NIC)
- 48-bit address, usually displayed in hexadecimal, like 00:1A:2B:3C:4D:5E
- Built into the NIC by the manufacturer (burned-in address), but can sometimes be spoofed
- **Globally unique**: The first 24 bits identify the manufacturer (OUI), the last 24 bits are specific to the device

- Layer 2 of the OSI Model



```
[evanfrancen@MacBookPro ~ % ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6460<TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether ca:2b:6e:02:5d:2e
        inet 192.168.1.162 netmask 0xffffff00 broadcast 192.168.1.255
        media: autoselect
        status: active
evanfrancen@MacBookPro ~ %
```

mes.

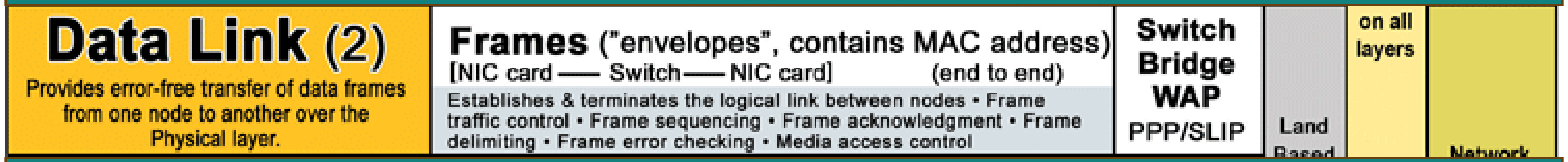
entify c

heck) t

turns u

Security Relevance:

- Vulnerable to:
  - MAC spoofing
  - ARP poisoning
  - Switch port attacks
- Controls include:
  - Port security on switches
  - Dynamic ARP inspection
  - VLAN segmentation



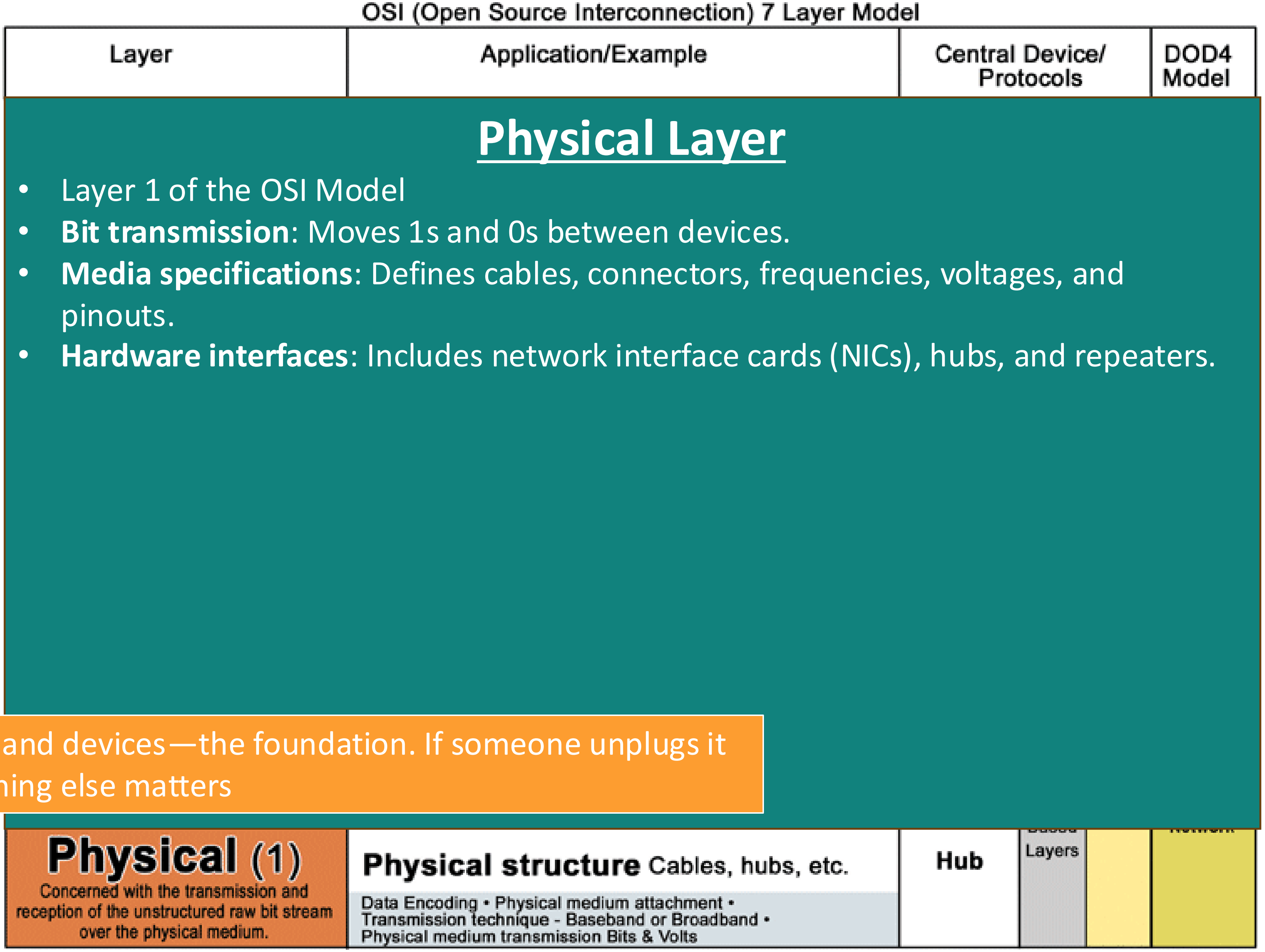
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	Switch Bridge WAP PPP/SLIP	Land Based	on all layers	Network

Like the mailroom—labeling and handing off the data to the right device on your local network.

20

C

O



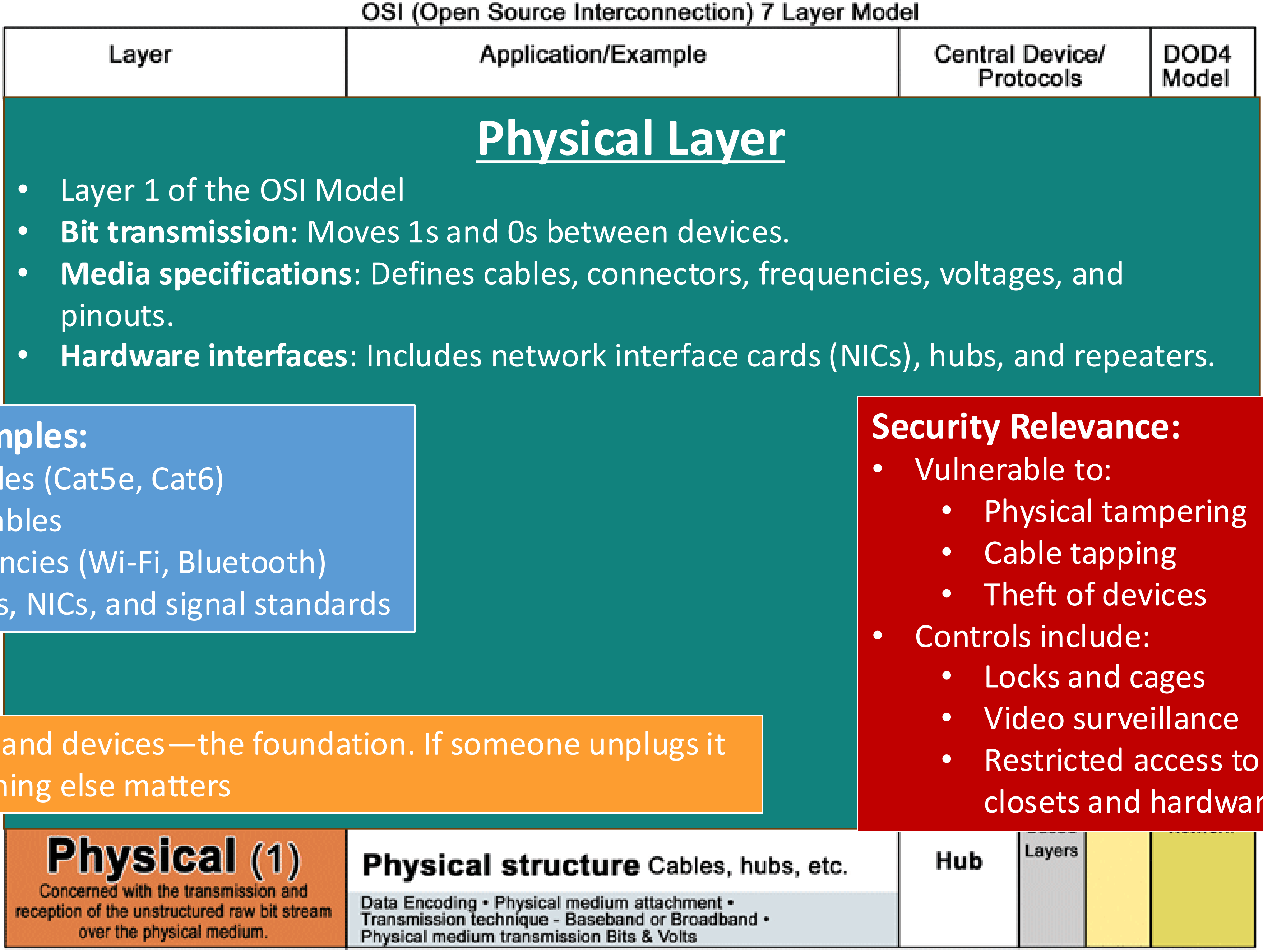
OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols	DOD4 Model
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	**Hub** Layers	

Physical Layer

- Layer 1 of the OSI Model
- **Bit transmission**: Moves 1s and 0s between devices.
- **Media specifications**: Defines cables, connectors, frequencies, voltages, and pinouts.
- **Hardware interfaces**: Includes network interface cards (NICs), hubs, and repeaters.

The wires, signals, and devices—the foundation. If someone unplugs it or taps into it, nothing else matters



OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols	DOD4 Model
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	Hub Layers	

Physical Layer

- Layer 1 of the OSI Model
- **Bit transmission**: Moves 1s and 0s between devices.
- **Media specifications**: Defines cables, connectors, frequencies, voltages, and pinouts.
- **Hardware interfaces**: Includes network interface cards (NICs), hubs, and repeaters.

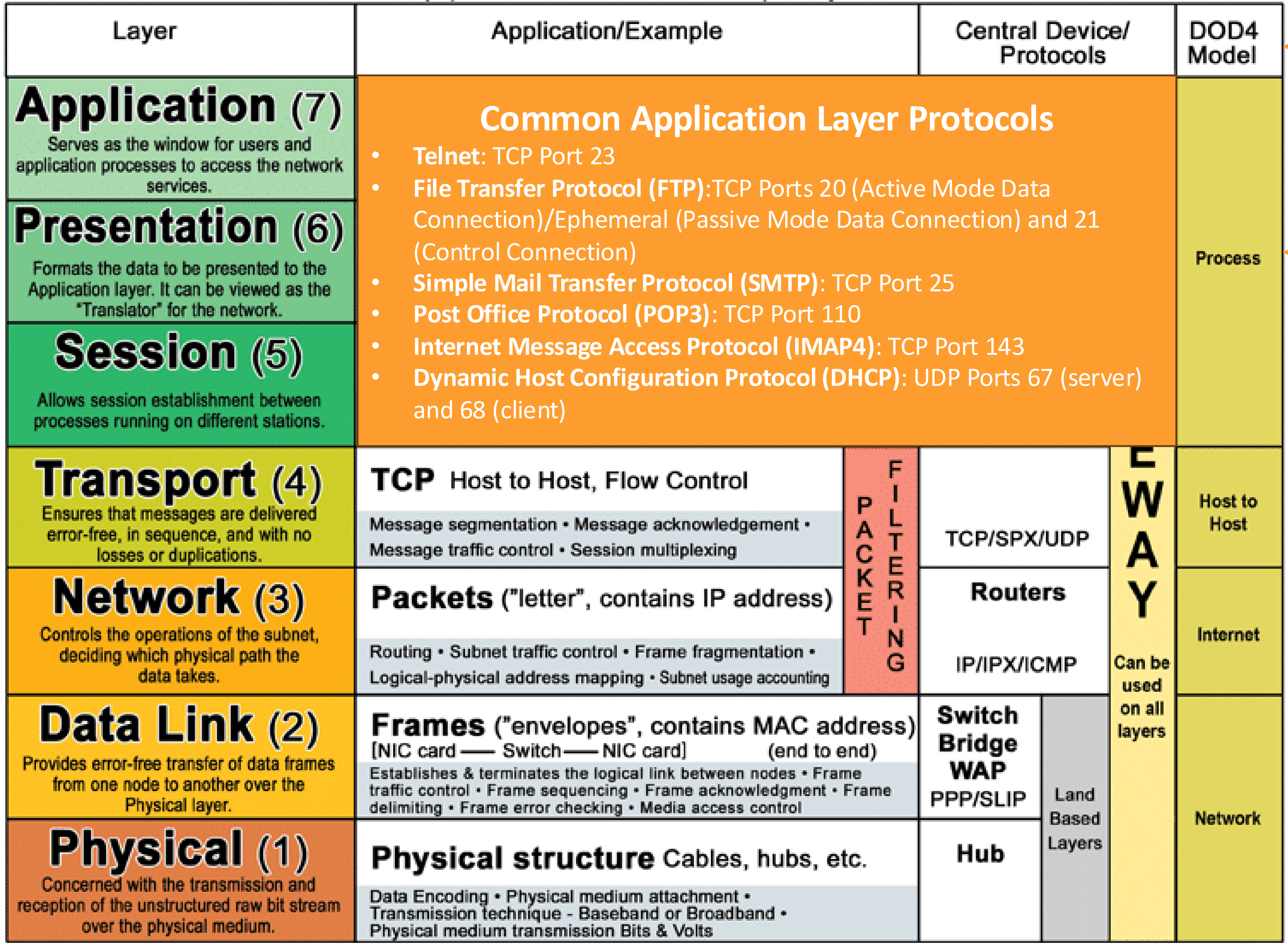
Common Examples:

- Ethernet cables (Cat5e, Cat6)
- Fiber optic cables
- Radio frequencies (Wi-Fi, Bluetooth)
- Physical ports, NICs, and signal standards

Security Relevance:

- Vulnerable to:
  - Physical tampering
  - Cable tapping
  - Theft of devices
- Controls include:
  - Locks and cages
  - Video surveillance
  - Restricted access to wiring closets and hardware

The wires, signals, and devices—the foundation. If someone unplugs it or taps into it, nothing else matters



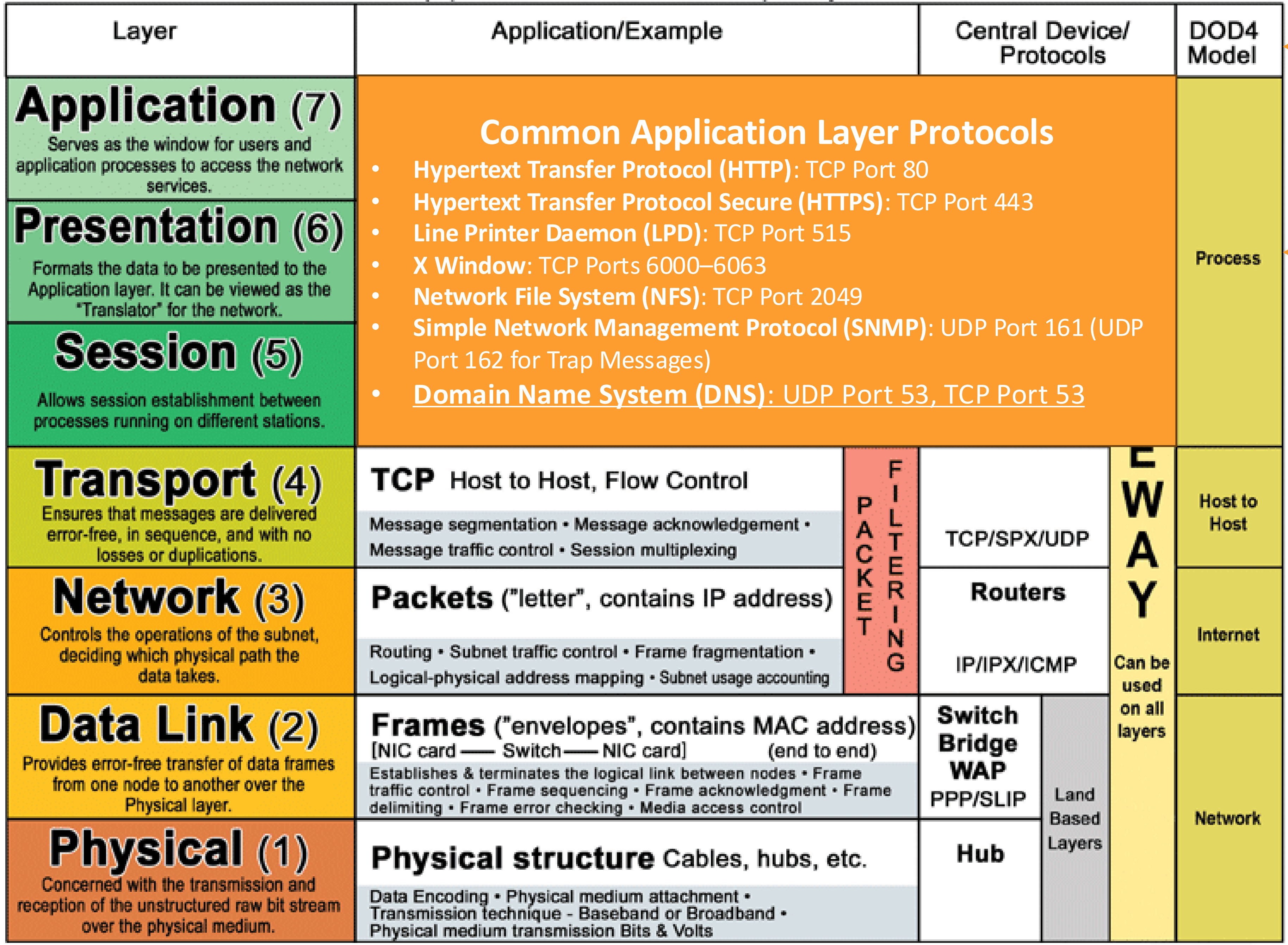
Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.						Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.						
Session (5) Allows session establishment between processes running on different stations.						
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		E W A Y Can be used on all layers	Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP			Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

Common Application Layer Protocols

- **Telnet**: TCP Port 23
- **File Transfer Protocol (FTP)**:TCP Ports 20 (Active Mode Data Connection)/Ephemeral (Passive Mode Data Connection) and 21 (Control Connection)
- **Simple Mail Transfer Protocol (SMTP)**: TCP Port 25
- **Post Office Protocol (POP3)**: TCP Port 110
- **Internet Message Access Protocol (IMAP4)**: TCP Port 143
- **Dynamic Host Configuration Protocol (DHCP)**: UDP Ports 67 (server) and 68 (client)

AKA "TCP/IP Model"

AKA "Application"



Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.						Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.						
Session (5) Allows session establishment between processes running on different stations.						
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		EWAY Can be used on all layers	Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP			Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card —— Switch —— NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

Common Application Layer Protocols

- **Hypertext Transfer Protocol (HTTP)**: TCP Port 80
- **Hypertext Transfer Protocol Secure (HTTPS)**: TCP Port 443
- **Line Printer Daemon (LPD)**: TCP Port 515
- **X Window**: TCP Ports 6000–6063
- **Network File System (NFS)**: TCP Port 2049
- **Simple Network Management Protocol (SNMP)**: UDP Port 161 (UDP Port 162 for Trap Messages)
- **Domain Name System (DNS)**: UDP Port 53, TCP Port 53

AKA "TCP/IP Model"

AKA "Application"

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Domain Name System (DNS)

Computers don’t speak human, they speak binary.

DNS is like the phonebook of the Internet. It translates human-readable domain names (like example.com) into IP addresses (like 93.184.216.34) so computers can locate and communicate with each other.

Purpose of DNS:

- Makes the Internet usable for humans.
- Allows us to type easy-to-remember names instead of numeric IP addresses.
- Supports scalability and flexibility of web services.

How DNS Works (Simplified Flow):

1. User types a domain (e.g., www.example.com) in a browser.
2. The system checks local DNS cache for the IP.
3. If not found, it queries a recursive resolver (usually your ISP or a public DNS like Google).
4. The resolver queries a root name server (.) → directs to a TLD server (.com) → then to the authoritative name server for example.com.
5. The authoritative server returns the IP address.
6. The resolver caches it and sends it back to your device.
7. Your device connects to the web server via its IP.

CHAPTER 11

Domain Name System (DNS)

Computers don’t speak human, they speak binary.

uman-readable domain names (like
omputers can locate and communicate with each

TLD (Top-Level Domain)

- This is the last part of a domain name—the “root-level” category.
- It tells you the domain’s type or origin.

Examples:

- .com (commercial)
- .org (organization)
- .gov (U.S. government)
- .edu (education)
- .us, .mx, .uk (country-code TLDs)

In www.example.com, the .com is the TLD.

Registered Domain Name (a.k.a. Second-Level Domain)

- This is the name you purchase and register under a TLD.
- It’s what you actually own (as long as you keep paying for it).
- Combined with the TLD, it becomes your primary domain.

Example:

In example.com, the registered domain is example.com.
You register this name with a domain registrar like GoDaddy, Namecheap, etc.

4. The resolver queries a roo
   authoritative name server
5. The authoritative server returns the IP address.
6. The resolver caches it and sends it back to your device.
7. Your device connects to the web server via its IP.

CHAPTER 11

Domain Name System

TLD (Top-Level Domain)

- This is the last part of a domain name—the “ro
- It tells you the domain’s type or origin.

Examples:

- .com (commercial)
- .org (organization)
- .gov (U.S. government)
- .edu (education)
- .us, .mx, .uk (country-code TLDs)

In www.example.com, the .com is the TLD.

Regi

Doma

- Thi
- It’s
- Co

Example:

In example.com, the registered domain is example.com.
You register this name with a domain registrar like GoDaddy, Namecheap, etc.

Subdomain (or Hostname)

- A subdomain is a prefix added to your registered domain to represent specific services, systems, or sites under the same domain.
- The hostname refers to a specific device or service under a domain (can be the same as a subdomain).

Examples:

- www.example.com – www is a subdomain (commonly used for web)
- mail.example.com – used for mail servers
- app1.internal.example.com – a deeper subdomain

You can create as many subdomains as you want, without extra cost—once you own the domain.

4. The resolver queries a roo
   authoritative name server
5. The authoritative server returns the IP address.
6. The resolver caches it and sends it back to your device.
7. Your device connects to the web server via its IP.

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Domain Name System

TLD (Top-Level Domain)

- This is the last part of a domain name—the “ro
- It tells you the domain’s type or origin.

Examples:

- .com (commercial)
- .org (organization)
- .gov
- .edu
- .us, .

In www

Regi

Doma

- Thi

Subdomain (or Hostname)

- A subdomain is a prefix added to your registered domain to represent specific services, systems, or sites under the same domain.
- r a domain (can

Ex

- sed for web)
-
- xtra cost—once

Security Relevance:

- DNS is critical infrastructure and a target for attacks:
  - DNS spoofing
  - Cache poisoning
  - DNS tunneling (data exfiltration)
  - DDoS via open resolvers
- **Protections include:**
  - DNSSEC (DNS Security Extensions)
  - Internal DNS filtering
  - Monitoring and logging queries

Key DNS Record Types:

- A – Maps domain to IPv4 address
- AAAA – Maps domain to IPv6 address
- CNAME – Alias for another domain
- MX – Mail exchange (email servers)
- NS – Nameserver for the domain
- TXT – Misc data (e.g., SPF, DKIM for email security)

registered domain is example.com.

e with a domain registrar like GoDaddy,

6. The resolver caches it and sends it back to your device.
7. Your device connects to the web server via its IP.

CHAPTER 11

Domain Name System (DNS)

Computers don’t speak human, they speak binary.

DNS Poisoning (a.k.a DNS Cache Poisoning)

How It Works:

1. **User requests a legitimate domain** (e.g., bank.com).
2. The local **DNS resolver** doesn’t have it cached, so it queries upstream servers.
3. Meanwhile, an attacker **spoofs a fake DNS response**, tricking the resolver into accepting it.
4. The resolver **caches the false IP address** (e.g., for bank.com → 6.6.6.6).
5. All users relying on that resolver now get **redirected to the attacker’s site**, which may look identical to the real one (phishing, malware, etc.).

Attack Goals:

- Phishing: Steal usernames/passwords.
- Malware: Trick users into downloading infected files.
- Man-in-the-Middle: Intercept or manipulate traffic.

How to Defend Against It:

- DNSSEC (DNS Security Extensions): Authenticates DNS responses with digital signatures.
- Use trusted DNS resolvers (like Google DNS or Cloudflare).
- Keep DNS servers patched to prevent known exploits.
- Short TTLs (time-to-live) for DNS cache to limit exposure.

CHAPTER 11

Domain Name System (DNS)

Computers don’t speak human, they speak binary.

Rogue DNS Server

How It Works:

1. The attacker sets up a fake DNS server that returns spoofed IP addresses for legitimate domains.
2. They trick users or systems into using this rogue server by:
   - Altering DHCP settings on a network
   - Infecting the victim’s device with malware
   - Man-in-the-middle attacks (e.g., on public Wi-Fi)
3. When the victim tries to visit a site like example.com, the rogue DNS server returns the attacker’s IP,

Attack Goals:

- Phishing: Redirect victims to fake login pages.
- Malware delivery: Serve drive-by downloads.
- Surveillance: Monitor or log DNS queries and behavior.

How to Defend Against It:

- Use trusted, static DNS settings (e.g., 1.1.1.1 or 8.8.8.8).
- Monitor for suspicious DNS traffic or unexpected DNS servers.
- Use DNSSEC and endpoint protection.
- Disable unauthorized DHCP servers on the network.

CHAPTER 11

Domain Name System (DNS)

Computers don't speak human, they speak binary.

DNS Pharming

Attack Goals:

- Steal credentials (phishing)
- Install malware
- Spy on traffic

How It Works:

There are two main types of DNS pharming:

1. **Local Pharming:**
   - The attacker infects the victim's computer or router and alters the hosts file or DNS settings.
   - When the user types bank.com, the device resolves it to a malicious IP address, even though the URL looks normal.
2. **Remote (Server-Level) Pharming**:
   - The attacker poisons a legitimate DNS server or sets up a rogue DNS server.
   - All users relying on that DNS server are silently redirected to malicious lookalike websites.

How to Defend Against It:

- Use DNSSEC to verify authenticity of DNS responses.
- Keep antivirus and firmware up to date, especially for routers.
- Use secure DNS resolvers (like Cloudflare or Google).
- Monitor and audit DNS traffic.

CHAPTER 11

Domain Name System (DNS)

Computers don’t speak human, they speak binary.

DNS Query Spoofing

How It Works:

1. A DNS resolver sends a query for a domain (e.g., example.com).
2. The attacker intercepts or guesses the request.
3. They quickly send a fake DNS response with a spoofed IP address, pretending to be the legitimate authoritative DNS server.
4. If the forged response arrives before the real one, the resolver accepts it and caches the malicious IP.

Result:

Users are silently redirected to:

- Phishing sites
- Malware-infected servers
- Attacker-controlled systems

How to Defend Against It:

- Use DNSSEC to validate DNS responses with digital signatures.
- Apply source port randomization to make spoofing harder.
- Use trusted recursive DNS resolvers.
- Monitor for anomalous DNS traffic.

CHAPTER 11

Domain Name System (DNS)

DNS Hijacking

eak human, they speak binary.

Goals:

- Phishing
- Credential theft
- Traffic manipulation
- Ad fraud
- Surveillance

How It Works:

DNS hijacking can occur in several ways:

1. **Router Hijacking** - The attacker gains access to a user’s router and changes its DNS settings to point to a malicious DNS server.
2. **Client-Level Hijacking** - Malware on the user’s device modifies DNS settings or the hosts file, altering where domain names resolve.
3. **ISP or Third-Party Hijacking** - Some ISPs or rogue DNS providers intercept mistyped domains and redirect users to ads or tracking pages.
4. **Domain Registrar Hijacking** - The attacker compromises a domain registrar account and redirects legitimate domains to malicious servers.

How to Defend Against It:

- Use secure DNS resolvers (e.g., 1.1.1.1, 8.8.8.8).
- Lock DNS and domain registrar accounts with MFA.
- Secure routers and endpoint devices.
- Use DNSSEC to verify DNS data integrity.

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Domain Name System (DNS)

DNS Homograph Attack

Why it's dangerous:

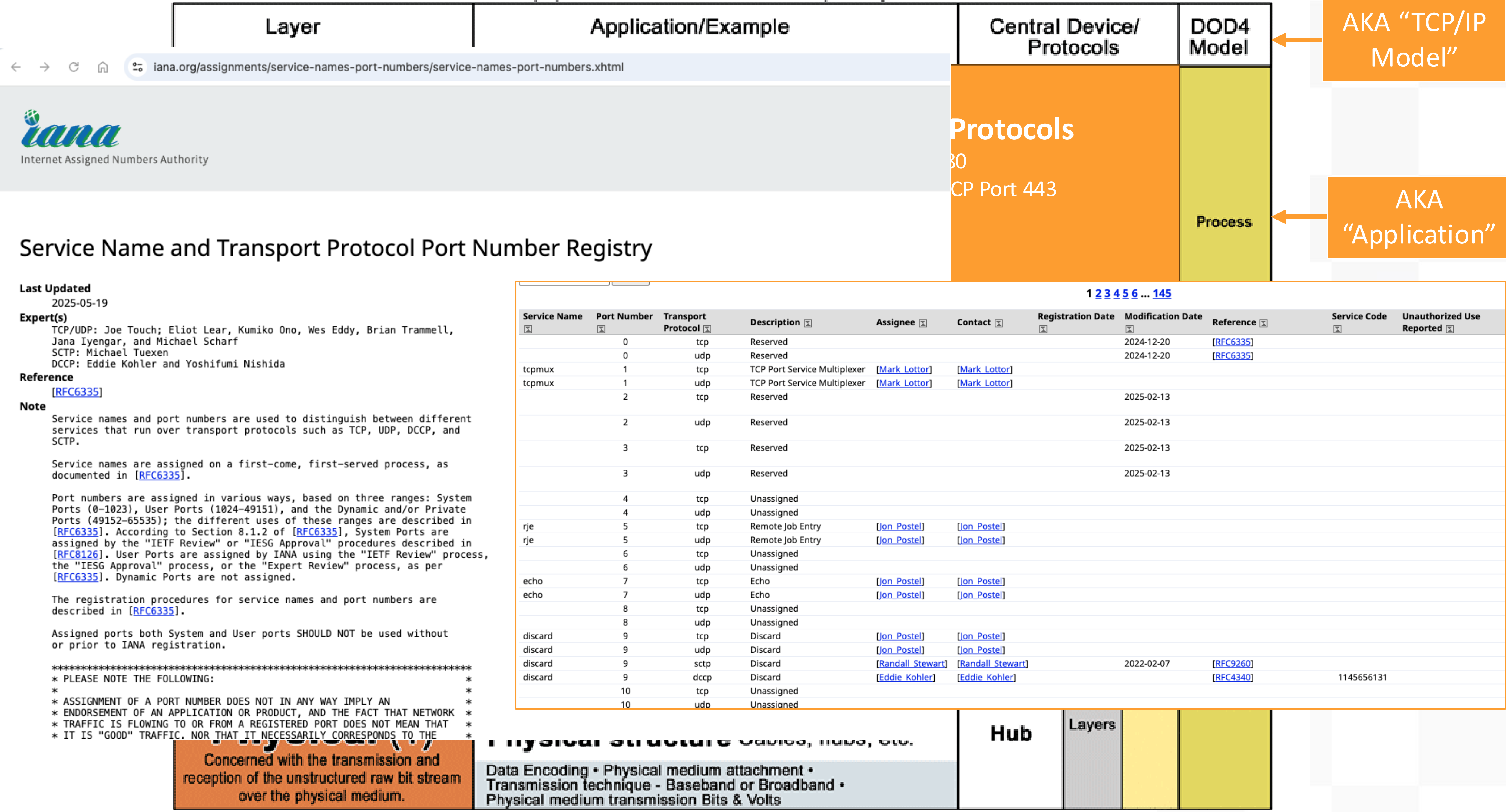
- Hard to detect without inspecting the underlying character encoding (Punycode).
- Even trained users may not notice the visual deception.
- Works well in URLs sent by email, SMS, or even in ads.

How It Works:

1. The attacker uses non-English characters (e.g., Cyrillic a, which looks like Latin a) to create a fake domain that visually mimics a real one.
2. The domain name looks legitimate to the naked eye—like www.apple.com vs www.apple.com (notice the Cyrillic "a").
3. Victims click the fake link and are redirected to a malicious site for:
   - Credential theft (phishing)
   - Malware delivery
   - Identity fraud

How to Defend Against It:

- Use modern browsers that warn about suspicious Unicode domains.
- Employ email security filters that check for homograph attacks.
- Train users to hover over links and check actual URLs.
- Enable anti-phishing and DNS filtering tools.


Layer
Application/Example
Central Device/ Protocols
DOD4 Model
AKA "TCP/IP Model"
Protocols
30
CP Port 443
Process
AKA "Application"
Hub
Layers
Physical Structure Cables, hubs, etc.
Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.
Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts

iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Internet Assigned Numbers Authority

Service Name and Transport Protocol Port Number Registry

Last Updated
2025-05-19

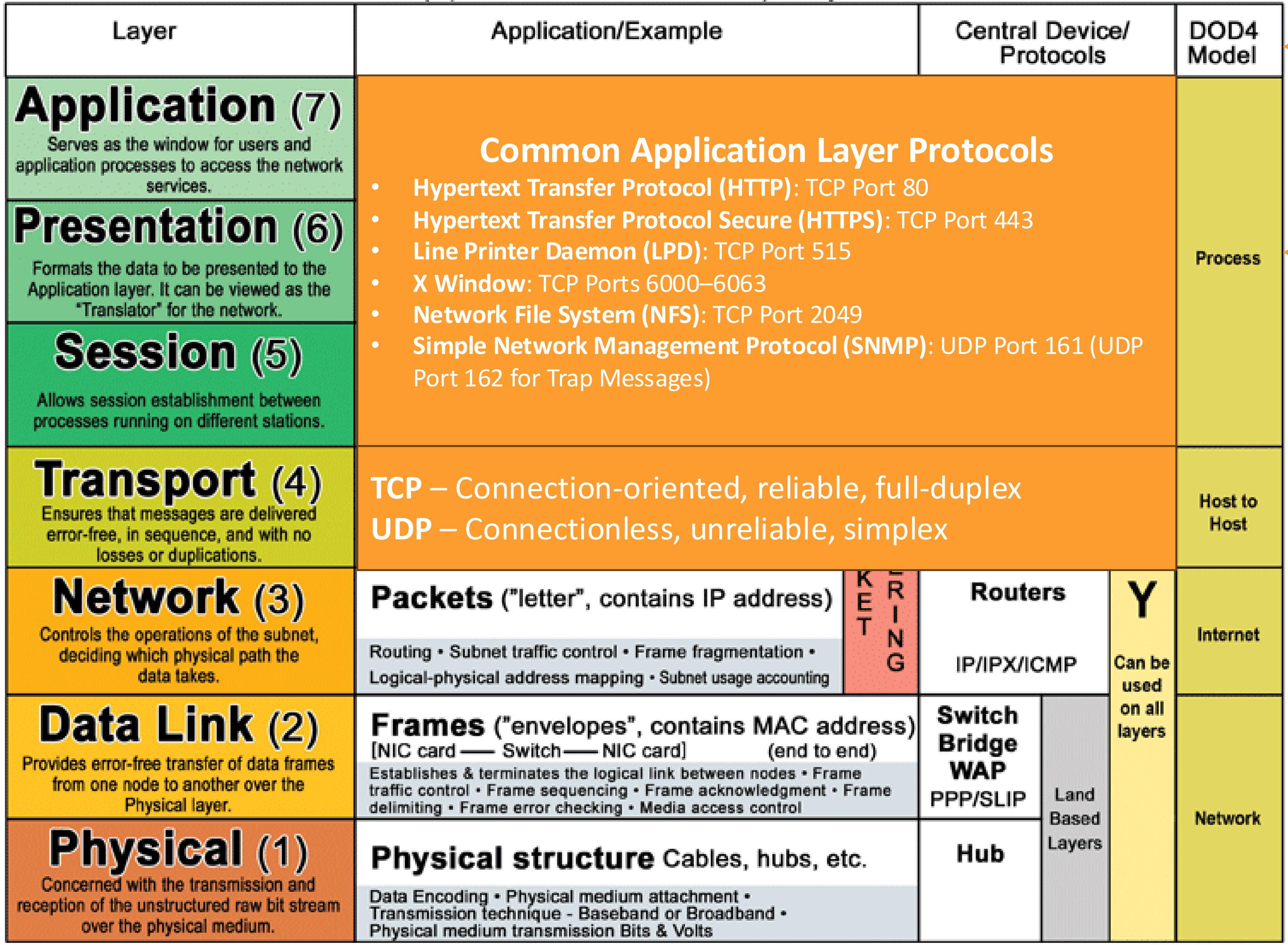
Expert(s)
```
TCP/UDP: Joe Touch; Eliot Lear, Kumiko Ono, Wes Eddy, Brian Trammell,
Jana Iyengar, and Michael Scharf
SCTP: Michael Tuexen
DCCP: Eddie Kohler and Yoshifumi Nishida
```

Reference
[RFC6335]

Note
```
Service names and port numbers are used to distinguish between different
services that run over transport protocols such as TCP, UDP, DCCP, and
SCTP.

Service names are assigned on a first-come, first-served process, as
documented in [RFC6335].

Port numbers are assigned in various ways, based on three ranges: System
Ports (0-1023), User Ports (1024-49151), and the Dynamic and/or Private
Ports (49152-65535); the different uses of these ranges are described in
[RFC6335]. According to Section 8.1.2 of [RFC6335], System Ports are
assigned by the "IETF Review" or "IESG Approval" procedures described in
[RFC8126]. User Ports are assigned by IANA using the "IETF Review" process,
the "IESG Approval" process, or the "Expert Review" process, as per
[RFC6335]. Dynamic Ports are not assigned.

The registration procedures for service names and port numbers are
described in [RFC6335].

Assigned ports both System and User ports SHOULD NOT be used without
or prior to IANA registration.

************************************************************************
* PLEASE NOTE THE FOLLOWING:                                           *
*                                                                      *
* ASSIGNMENT OF A PORT NUMBER DOES NOT IN ANY WAY IMPLY AN             *
* ENDORSEMENT OF AN APPLICATION OR PRODUCT, AND THE FACT THAT NETWORK  *
* TRAFFIC IS FLOWING TO OR FROM A REGISTERED PORT DOES NOT MEAN THAT   *
* IT IS "GOOD" TRAFFIC, NOR THAT IT NECESSARILY CORRESPONDS TO THE     *
```

1 2 3 4 5 6 ... 145

Service Name	Port Number	Transport Protocol	Description	Assignee	Contact	Registration Date	Modification Date	Reference	Service Code	Unauthorized Use Reported
	0	tcp	Reserved				2024-12-20	[RFC6335]		
	0	udp	Reserved				2024-12-20	[RFC6335]		
tcpmux	1	tcp	TCP Port Service Multiplexer	[Mark_Lottor]	[Mark_Lottor]					
tcpmux	1	udp	TCP Port Service Multiplexer	[Mark_Lottor]	[Mark_Lottor]					
	2	tcp	Reserved				2025-02-13			
	2	udp	Reserved				2025-02-13			
	3	tcp	Reserved				2025-02-13			
	3	udp	Reserved				2025-02-13			
	4	tcp	Unassigned							
	4	udp	Unassigned							
rje	5	tcp	Remote Job Entry	[Jon_Postel]	[Jon_Postel]					
rje	5	udp	Remote Job Entry	[Jon_Postel]	[Jon_Postel]					
	6	tcp	Unassigned							
	6	udp	Unassigned							
echo	7	tcp	Echo	[Jon_Postel]	[Jon_Postel]					
echo	7	udp	Echo	[Jon_Postel]	[Jon_Postel]					
	8	tcp	Unassigned							
	8	udp	Unassigned							
discard	9	tcp	Discard	[Jon_Postel]	[Jon_Postel]					
discard	9	udp	Discard	[Jon_Postel]	[Jon_Postel]					
discard	9	sctp	Discard	[Randall_Stewart]	[Randall_Stewart]		2022-02-07	[RFC9260]		
discard	9	dccp	Discard	[Eddie_Kohler]	[Eddie_Kohler]			[RFC4340]	1145656131	
	10	tcp	Unassigned							
	10	udp	Unassigned							

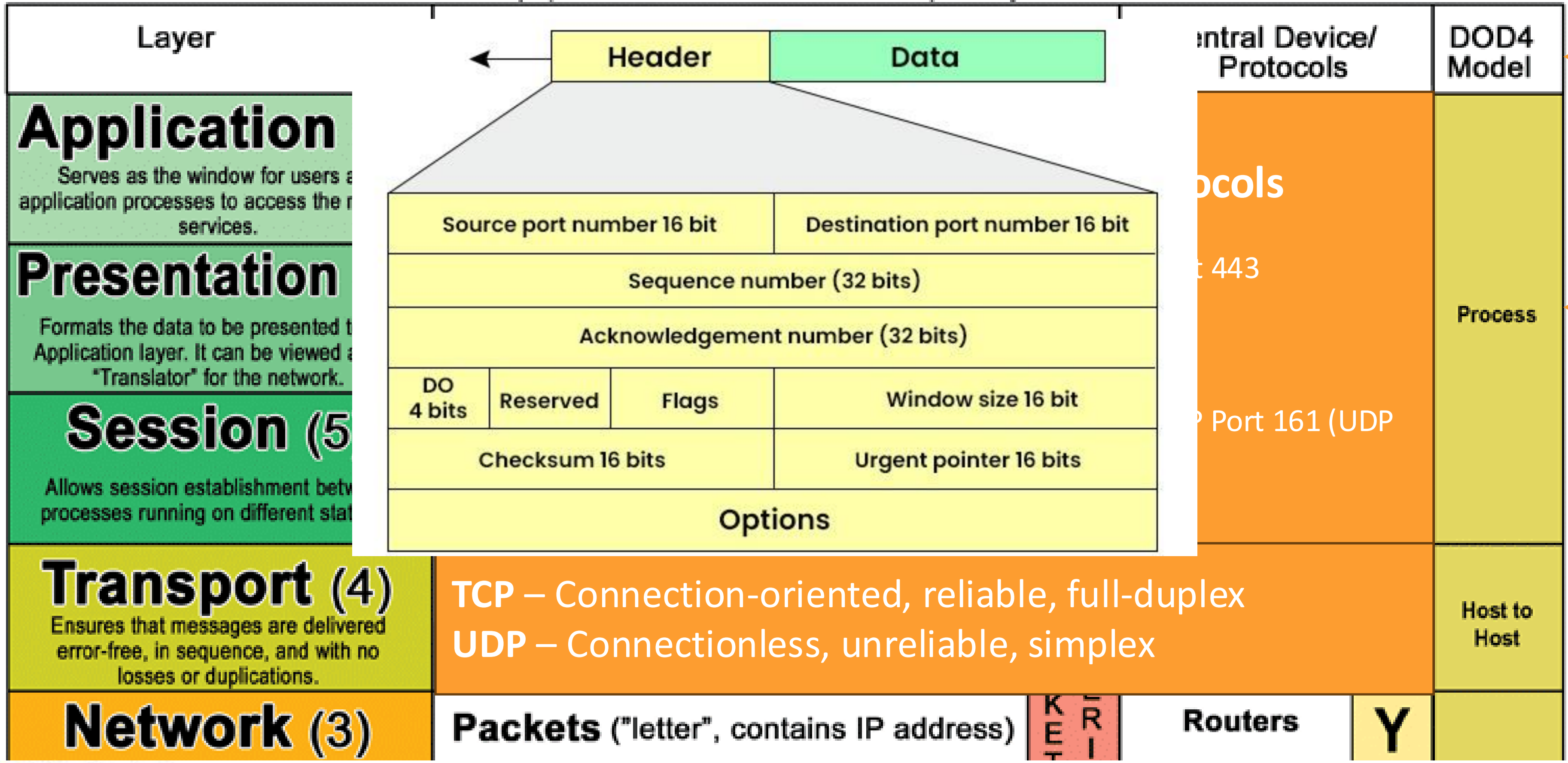


Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**Common Application Layer Protocols** • **Hypertext Transfer Protocol (HTTP)**: TCP Port 80 • **Hypertext Transfer Protocol Secure (HTTPS)**: TCP Port 443 • **Line Printer Daemon (LPD)**: TCP Port 515 • **X Window**: TCP Ports 6000–6063 • **Network File System (NFS)**: TCP Port 2049 • **Simple Network Management Protocol (SNMP)**: UDP Port 161 (UDP Port 162 for Trap Messages)					Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.						
Session (5) Allows session establishment between processes running on different stations.						
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** – Connection-oriented, reliable, full-duplex **UDP** – Connectionless, unreliable, simplex					Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	KET RING	**Routers** IP/IPX/ICMP		**Y** Can be used on all layers	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card —— Switch —— NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch** **Bridge** **WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

AKA "TCP/IP Model"

AKA "Application"

The "port" identifies the application


Layer
Header
Data
ntral Device/
Protocols
DOD4
Model
Application
Serves as the window for users a
application processes to access the n
services.
Presentation
Formats the data to be presented t
Application layer. It can be viewed a
"Translator" for the network.
Session (5
Allows session establishment betw
processes running on different stat
Transport (4)
Ensures that messages are delivered
error-free, in sequence, and with no
losses or duplications.
Network (3)
ocols
t 443
P Port 161 (UDP
Process
Host to
Host
Packets ("letter", contains IP address)
K
E
T
R
I
Routers
Y

Source port number 16 bit			Destination port number 16 bit
Sequence number (32 bits)			
Acknowledgement number (32 bits)			
DO 4 bits	Reserved	Flags	Window size 16 bit
Checksum 16 bits			Urgent pointer 16 bits
Options			

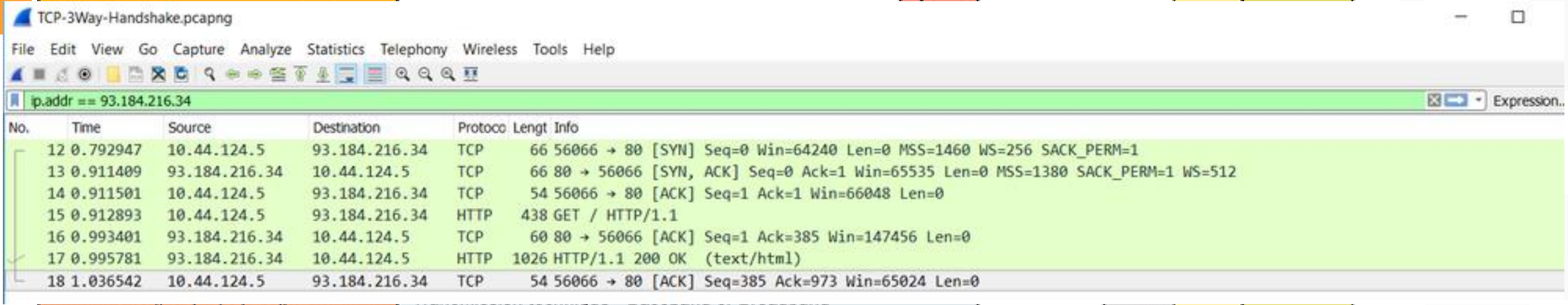
TCP – Connection-oriented, reliable, full-duplex

UDP – Connectionless, unreliable, simplex

AKA "TCP/IP Model"

AKA "Application"

The "port" identifies the application


TCP-3Way-Handshake.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

```
ip.addr == 93.184.216.34

No.  Time      Source         Destination    Protoco Lengt Info
  12 0.792947  10.44.124.5    93.184.216.34  TCP      66 56066 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  13 0.911409  93.184.216.34  10.44.124.5    TCP      66 80 → 56066 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM=1 WS=512
  14 0.911501  10.44.124.5    93.184.216.34  TCP      54 56066 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
  15 0.912893  10.44.124.5    93.184.216.34  HTTP    438 GET / HTTP/1.1
  16 0.993401  93.184.216.34  10.44.124.5    TCP      60 80 → 56066 [ACK] Seq=1 Ack=385 Win=147456 Len=0
  17 0.995781  93.184.216.34  10.44.124.5    HTTP   1026 HTTP/1.1 200 OK  (text/html)
  18 1.036542  10.44.124.5    93.184.216.34  TCP      54 56066 → 80 [ACK] Seq=385 Ack=973 Win=65024 Len=0
```

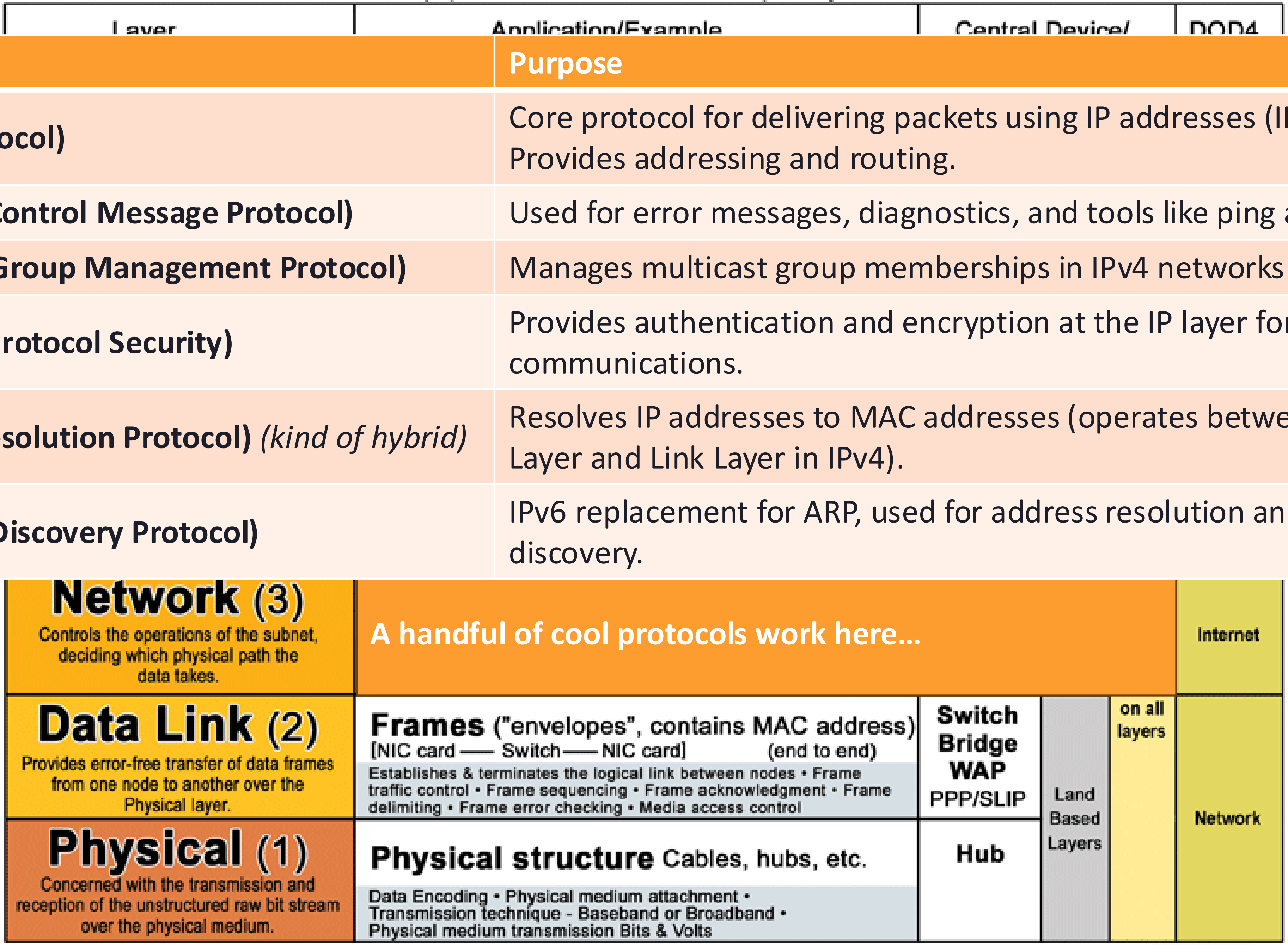
over the physical medium.

Physical medium transmission Bits & Volts

AKA "TCP/IP

Protocol	Purpose
IP (Internet Protocol)	Core protocol for delivering packets using IP addresses (IPv4 and IPv6). Provides addressing and routing.
ICMP (Internet Control Message Protocol)	Used for error messages, diagnostics, and tools like ping and traceroute.
IGMP (Internet Group Management Protocol)	Manages multicast group memberships in IPv4 networks.
IPSec (Internet Protocol Security)	Provides authentication and encryption at the IP layer for secure network communications.
ARP (Address Resolution Protocol) *(kind of hybrid)*	Resolves IP addresses to MAC addresses (operates between Internet Layer and Link Layer in IPv4).
NDP (Neighbor Discovery Protocol)	IPv6 replacement for ARP, used for address resolution and router discovery.

identifies the application



Layer	Application/Example	Central Device/			DOD4
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**A handful of cool protocols work here…**				Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	**Switch** **Bridge** **WAP** PPP/SLIP	Land Based Layers	on all layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	**Hub**			

CHAPTER 11

IP Addresses (v4)

- A 32-bit numeric identifier assigned to devices on a network, allowing them to communicate with each other using the Internet Protocol (IP).
- Used at the Internet Layer (Layer 3) of the OSI model.

CHAPTER 11

IP Addresses (v4)

- A 32-bit numeric identifier assigned to devices on a network, allowing them to communicate with each other using the Internet Protocol (IP).
- Used at the Internet Layer (Layer 3) of the OSI model.
- **Format**:
  - Written as four decimal numbers (called octets) separated by dots
  - Each number ranges from 0 to 255
  - **Example**: 192.168.1.1

Each octet is 8 bits

0 = 00000000, 255 = 11111111

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

11000000 10101000 00000001 00000001

11111111 11111111 11111111 00000000 = 255.255.255.0

192.168.1.0 is the network, 1 is the host

There are two parts to an IP address, the network address and the host address, enter “Subnet Mask”.

CHAPTER 11

IP Addresses (v4)

Classes

- There's "classful" and "classless". Let's start with classful:

Class	First Binary Digits	Decimal Range (1st Octet)	# of Networks	# of Hosts
A	0	1 – 126	126	16,777,214
B	10	128 – 191	16,384	16,384
C	110	192 – 223	2,097,152	254
D	1110	224 – 239	Reserved for multicasting	
E	1111	240 - 255	Experimental/future use	

CHAPTER 11

IP Addresses (v4)

Classes

- There’s “classful” and “classless”. Let’s start with classful:

CIDR (Classless Inter-Domain Routing) was introduced in 1993 by the Internet Engineering Task Force (IETF) as a solution to two growing problems with the early Internet:

of Hosts
16,777,214

1. Class-Based IP Addressing Was Wasteful

- The old system divided IPs into rigid “classes” (A, B, C), with fixed subnet sizes:
  - Class A = ~16 million hosts
  - Class B = ~65,000 hosts
  - Class C = 254 hosts
- Organizations had to choose a class—even if they didn’t need all the IPs—leading to massive address space waste.

2. Routing Table Bloat

- The number of entries in global routing tables exploded because each classful network needed a separate route.
- Routers and ISPs were struggling to keep up.

CHAPTER 11

IP Addresses (v4)

Classes

- There's "classful" and "classless". Let's start with classful:

CIDR (Classless Inter-Domain Routing) was introduced in 1993 by the Internet Engineering Task Force (IETF) as a solution to two growing problems with the early Internet:

of Hosts
16,777,214

1. **Class-Based IP Addressing Was Wasteful**

The Solution: CIDR (RFC 1518 & 1519)

- CIDR replaced class-based addressing with prefix-based (bitwise) routing.
- Allowed IP blocks to be allocated in variable sizes (e.g., /20, /28, etc.).
- Introduced route aggregation (a.k.a. supernetting) to reduce the size of routing tables.

Example: Multiple /24 routes could be summarized as a single /20.

assive address space waste.

2. **Routing Table Blo**
   - The number of entri … separate route.
   - Routers and ISPs we

Why CIDR Was a Game Changer:

- Slowed down IPv4 exhaustion.
- Improved routing efficiency.
- Made the system more scalable and flexible for ISPs and enterprises.

2025 CISSP MENTOR PROGRAM

CHAPTER 11

IP Addresses (v4)

Classes

- There's "classful" and "classless". Let's start with classful:

Class	First Binary Digits	Decimal Range (1st Octet)	# of Networks	# of Hosts	CIDR Notation
A	0	1 – 126	126	16,777,214	/8
B	10	128 – 191	16,384	16,384	/16
C	110	192 – 223	2,097,152	254	/24
D	1110	224 – 239	Reserved for multicasting		
E	1111	240 - 255	Experimental/future use		

Hypothetical

- Our enterprise network has decided to use a 172.16.0.0 network internally.
- In our network design, one network segment will require no more than 500 hosts on it.
- How should we subnet the network to enable this with the least amount of waste and most amount of control?

I'll answer this during the live session.

2025 CISSP MENTOR PROGRAM

CHAPTER 11

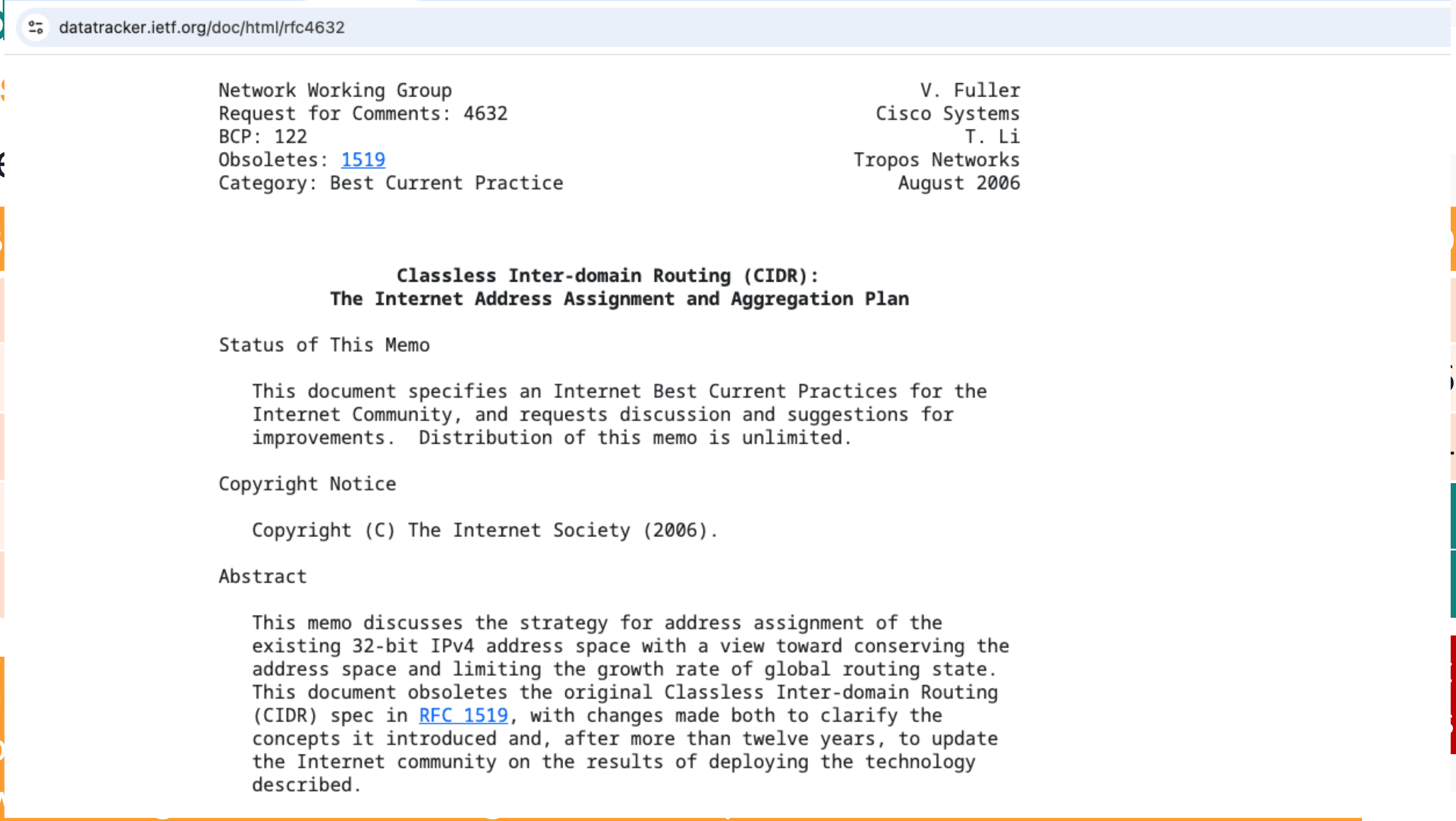
IP Ad

Classe

- There

Class	First B	R Notation
A	0	
B	10	
C	110	
D	1110	
E	1111	

his during
ession.



```
Network Working Group                                          V. Fuller
Request for Comments: 4632                                 Cisco Systems
BCP: 122                                                           T. Li
Obsoletes: 1519                                          Tropos Networks
Category: Best Current Practice                              August 2006


            Classless Inter-domain Routing (CIDR):
      The Internet Address Assignment and Aggregation Plan

Status of This Memo

   This document specifies an Internet Best Current Practices for the
   Internet Community, and requests discussion and suggestions for
   improvements.  Distribution of this memo is unlimited.

Copyright Notice

   Copyright (C) The Internet Society (2006).

Abstract

   This memo discusses the strategy for address assignment of the
   existing 32-bit IPv4 address space with a view toward conserving the
   address space and limiting the growth rate of global routing state.
   This document obsoletes the original Classless Inter-domain Routing
   (CIDR) spec in RFC 1519, with changes made both to clarify the
   concepts it introduced and, after more than twelve years, to update
   the Internet community on the results of deploying the technology
   described.
```

Hypothetica

- Our enterp
- In our netw
- How should we subnet the network to enable this with the least amount of waste and most amount of control?

CHAPTER 11

IP Addresses (v4)

Private IP Addressing & NAT

- **RFC 1918**, titled "*Address Allocation for Private Internets*", was published in 1996 by the IETF to address the growing **shortage of IPv4 addresses** and to support internal (private) network growth.
- Reserve specific IP address ranges for use only within private networks, and to exclude them from global (public) routing on the Internet.

CHAPTER 11

IP Addresses (v4)

Private IP Addressing & NAT

- **RFC 1918,** titled “Address Allocation for Private Internets” was published in 1996 by the IETF internal (p
- Reserve sp exclude th

What It Did:

1. **Defined Three Private IP Ranges:**

Class	Address Range	CIDR
A	10.0.0.0 – 10.255.255.255	10.0.0.0/8
B	172.16.0.0 – 172.31.255.255	172.16.0.0/12
C	192.168.0.0 – 192.168.255.255	192.168.0.0/16

2. **Restricted Their Use to Private Networks:**
   - These IPs cannot be routed on the public Internet.
   - Routers on the Internet should drop any traffic from these ranges.
3. **Enabled NAT (Network Address Translation):**
   - Devices in private networks can share a single public IP to access the Internet.
   - NAT became a key strategy for delaying IPv4 exhaustion.

CHAPTER 11

IP Addresses (v4)

Private IP Addressing & NAT

Network Address Translation (NAT)

NAT allows devices with private IP addresses to communicate with public networks (like the Internet) by translating private IPs into a public IP (and vice versa).

Types of NAT:

1. **Static NAT**
   - One-to-one mapping of private IP to public IP.
   - Useful when hosting services internally (e.g., web servers).
2. **Dynamic NAT**
   - Maps private IPs to a pool of public IPs.
   - Allocation is temporary and not guaranteed.
3. **PAT (Port Address Translation)**
   - Also called NAT overload.
   - Many private IPs share a single public IP, differentiated by port numbers.
   - Most common form of NAT used in homes and small businesses.

3
0/12
.0/16

n these ranges.

ic IP to access the Internet.

stion.

2025 CISSP MENTOR PROGRAM

CHAPTER 11

IP Version 6

Why IPv6 Was Created:

- To provide vastly more address space
- To simplify routing and network configuration
- To eliminate the need for NAT
- To improve efficiency and security

- IPv6 (Internet Protocol version 6) is the next-generation IP protocol developed to replace IPv4, addressing its limitations—most notably the exhaustion of available IPv4 addresses.

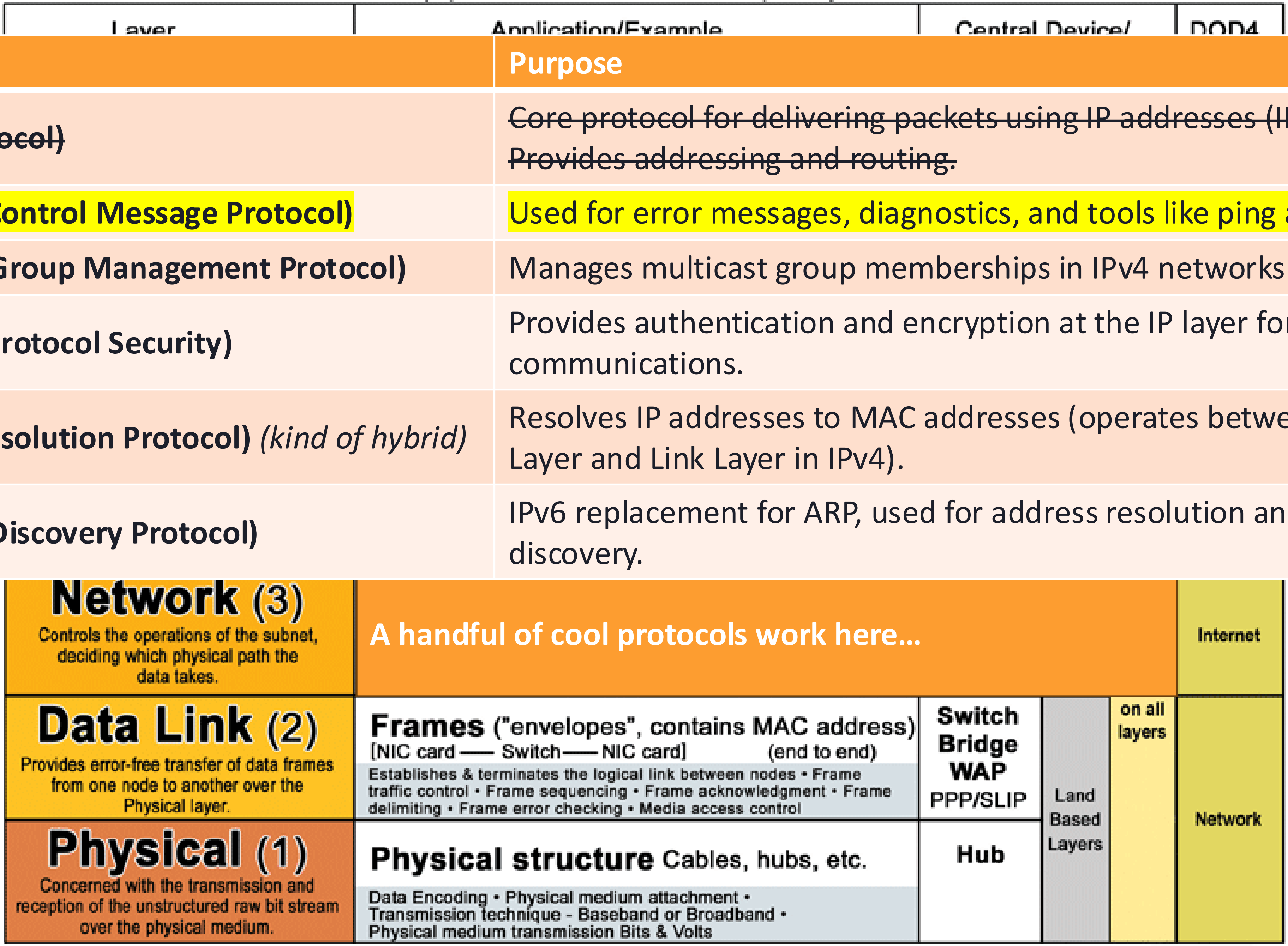
Key Differences: IPv4 vs. IPv6

Feature	IPv4	IPv6
Address Size	32-bit	128-bit
Address Format	Decimal (e.g., 192.168.1.1)	Hexadecimal (e.g., 2001:0db8::1)
Total Addresses	~4.3 billion	~340 undecillion (3.4×10^{38})
Header Simplicity	Complex, includes checksum	Simplified header, more efficient routing
Security	Optional (IPsec not built-in)	IPsec support is **mandatory**
Configuration	Manual or DHCP	Supports **stateless auto-configuration**
Broadcasting	Supported	**No broadcasting** (uses multicast instead)
NAT	Common and required	**Not needed** (every device gets a unique IP)

AKA “TCP/IP
”

Protocol	Purpose
~~IP (Internet Protocol)~~	~~Core protocol for delivering packets using IP addresses (IPv4 and IPv6). Provides addressing and routing.~~
ICMP (Internet Control Message Protocol)	Used for error messages, diagnostics, and tools like ping and traceroute.
IGMP (Internet Group Management Protocol)	Manages multicast group memberships in IPv4 networks.
IPSec (Internet Protocol Security)	Provides authentication and encryption at the IP layer for secure network communications.
ARP (Address Resolution Protocol) *(kind of hybrid)*	Resolves IP addresses to MAC addresses (operates between Internet Layer and Link Layer in IPv4).
NDP (Neighbor Discovery Protocol)	IPv6 replacement for ARP, used for address resolution and router discovery.

identifies the application



Layer	Application/Example	Central Device/			DOD4
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**A handful of cool protocols work here…**				Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	**Switch** **Bridge** **WAP** PPP/SLIP	Land Based Layers	on all layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	**Hub**			

CHAPTER 11

ICMP is the Internet's messenger—it doesn't move data; it tells you why your data didn't move.

ICMP (Internet Control Message Protocol)

A supporting protocol used by network devices to send error messages and operational information—it works at the Internet Layer (Layer 3) of the OSI model, alongside IP.

What ICMP Does:

- Reports errors (e.g., "host unreachable," "TTL expired")
- Used for diagnostic tools like:
  - *ping* – tests if a host is reachable
  - *traceroute* – maps the path packets take through the network
- Communicates network status between devices

ICMP Is Not Used to Exchange Data, but it can be abused:

- ICMP Flood (DoS)
- Ping of Death
- ICMP tunneling (data exfiltration)

Security Considerations:

- Often rate-limited or filtered at firewalls
- Can be disabled entirely on sensitive hosts to reduce attack surface

CHAPTER 11

IGMP is how your devices raise their hand and say, ‘I want in on that multicast stream.

IGMP (Internet Group Management Protocol)

A Layer 3 (Internet Layer) protocol used in IPv4 networks to manage multicast group memberships. It allows devices (hosts and routers) to join or leave multicast groups, which are used for one-to-many communication (like streaming video or live events).

What IGMP Does:

- Allows a host to **signal interest** in receiving multicast traffic (e.g., for a specific video stream).
- Informs local routers which devices want to receive traffic for a given **multicast IP address**.
- Helps optimize network traffic by only sending multicast data to networks where **interested hosts** exist.

Common IGMP Versions:

- IGMPv1 – Basic join capability
- IGMPv2 – Adds leave functionality and faster response
- IGMPv3 – Supports source-specific multicast (receive only from certain senders)

Security Considerations:

- Multicast flooding if IGMP is not properly filtered
- Should be restricted with Layer 2 controls like IGMP snooping on switches

Protocol	Purpose
~~IP (Internet Protocol)~~	~~Core protocol for delivering packets using IP addresses (IPv4 and IPv6). Provides addressing and routing.~~
~~ICMP (Internet Control Message Protocol)~~	~~Used for error messages, diagnostics, and tools like ping and traceroute.~~
IGMP (Internet Group Management Protocol)	Manages multicast group memberships in IPv4 networks.
IPSec (Internet Protocol Security)	Provides authentication and encryption at the IP layer for secure network communications.
ARP (Address Resolution Protocol) *(kind of hybrid)*	Resolves IP addresses to MAC addresses (operates between Internet Layer and Link Layer in IPv4).
NDP (Neighbor Discovery Protocol)	IPv6 replacement for ARP, used for address resolution and router discovery.

AKA "TCP/IP

”

identifies the application

Layer	Application/Example	Central Device/			DOD4
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**A handful of cool protocols work here…**				Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	**Switch** **Bridge** **WAP** PPP/SLIP	Land Based Layers	on all layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	**Hub**			

CHAPTER 11

IGMP is how your devices raise their hand and say, ‘I want in on that multicast stream.

IGMP (Internet Group Management Protocol)

A Layer 3 (Internet Layer) protocol used in IPv4 networks to manage multicast group memberships. It allows devices (hosts and routers) to join or leave multicast groups, which are used for one-to-many communication (like streaming video or live events).

What IGMP Does:

- Allows a host to **signal interest** in receiving multicast traffic (e.g., for a specific video stream).
- Informs local routers which devices want to receive traffic for a given **multicast IP address**.
- Helps optimize network traffic by only sending multicast data to networks where **interested hosts** exist.

Common IGMP Versions:

- IGMPv1 – Basic join capability
- IGMPv2 – Adds leave functionality and faster response
- IGMPv3 – Supports source-specific multicast (receive only from certain senders)

Security Considerations:

- Multicast flooding if IGMP is not properly filtered
- Should be restricted with Layer 2 controls like IGMP snooping on switches

IGMP is how your devices raise their hand and say, 'I want in on

Unicast vs. Multicast vs. Broadcast

Unicast

- One-to-one communication
- Data is sent from one source to one specific destination
- Most common type of network traffic (e.g., web browsing, file transfers)

Example:
A user visiting example.com → the

ast

What IGMP Does:

- Allows a host to **signa**
- Informs local routers
- Helps optimize netwo **hosts** exist.

Comm

Multicast

- One-to-many (selective) communication
- Data is sent to multiple recipients, but only to those who explicitly joined the group
- Efficient for things like video streaming, online games, or financial feeds

Example:
A live sports stream sent to all subscribed users using a multicast group

om certain senders)

Broadcast

- One-to-all communication on a local network
- Data is sent to every device on the broadcast domain (e.g., all devices on a subnet)
- Can cause network noise and is generally avoided in larger networks

Example:
ARP requests (e.g., "Who has IP 192.168.1.1? Tell me!")

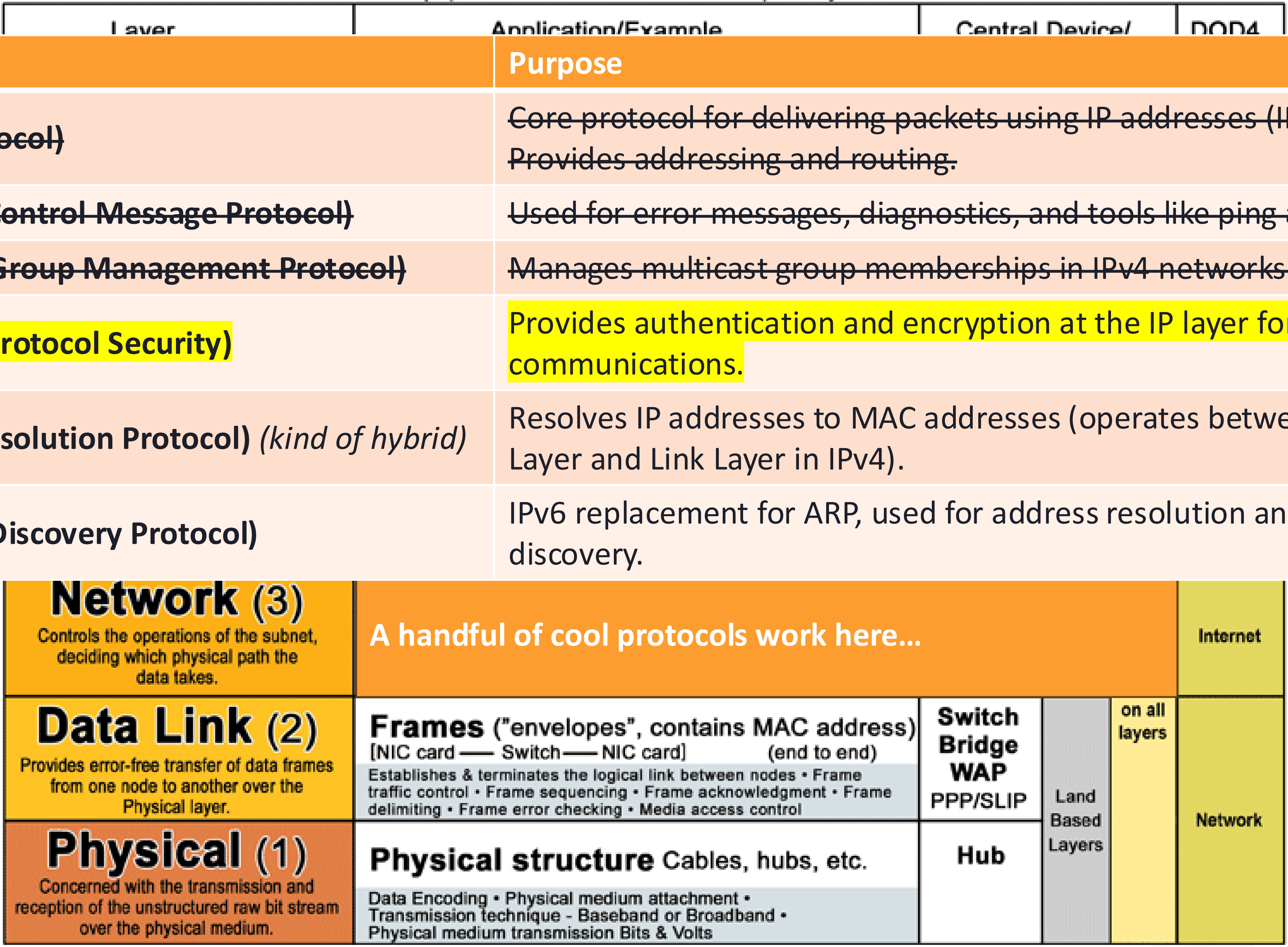
ns:
GMP is not properly filtered
with Layer 2 controls like
itches

AKA “TCP/IP

Protocol	Purpose
~~IP (Internet Protocol)~~	~~Core protocol for delivering packets using IP addresses (IPv4 and IPv6). Provides addressing and routing.~~
~~ICMP (Internet Control Message Protocol)~~	~~Used for error messages, diagnostics, and tools like ping and traceroute.~~
~~IGMP (Internet Group Management Protocol)~~	~~Manages multicast group memberships in IPv4 networks.~~
IPSec (Internet Protocol Security)	Provides authentication and encryption at the IP layer for secure network communications.
ARP (Address Resolution Protocol) *(kind of hybrid)*	Resolves IP addresses to MAC addresses (operates between Internet Layer and Link Layer in IPv4).
NDP (Neighbor Discovery Protocol)	IPv6 replacement for ARP, used for address resolution and router discovery.

”

identifies the application



Layer | Application/Example | Central Device/ | DOD4

Network (3)
Controls the operations of the subnet, deciding which physical path the data takes.

A handful of cool protocols work here…

Internet

Data Link (2)
Provides error-free transfer of data frames from one node to another over the Physical layer.

Frames ("envelopes", contains MAC address)
[NIC card — Switch — NIC card] (end to end)
Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control

Switch
Bridge
WAP
PPP/SLIP

Land Based Layers

on all layers

Network

Physical (1)
Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.

Physical structure Cables, hubs, etc.
Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts

Hub

CHAPTER 11

IPSec works under the hood—encrypting and authenticating IP packets before they ever reach the app. It's like armor at Layer 3.

IPSec (Internet Protocol Security)

A suite of protocols used to secure IP traffic by providing confidentiality, integrity, and authentication at the Network Layer (Layer 3) of the OSI model.

CHAPTER 11

IPSec works under the hood—encrypting and authenticating IP packets before they ever reach the app. It's like armor at Layer 3.

IPSec (Internet Protocol Security)

A suite of protocols used to secure IP traffic by providing confidentiality, integrity, and authentication at the Network Layer (Layer 3) of the OSI model.

- It's commonly used for VPNs, site-to-site encryption, and secure tunneling across untrusted networks like the Internet.

CHAPTER 11

IPSec works under the hood—encrypting and authenticating IP packets before they ever reach the app. It's like armor at Layer 3.

IPSec (Internet Protocol Security)

A suite of protocols used to secure IP traffic by providing confidentiality, integrity, and authentication at the Network Layer (Layer 3) of the OSI model.

- It's commonly used for VPNs, site-to-site encryption, and secure tunneling across untrusted networks like the Internet.

How IPSec Works (Simplified):

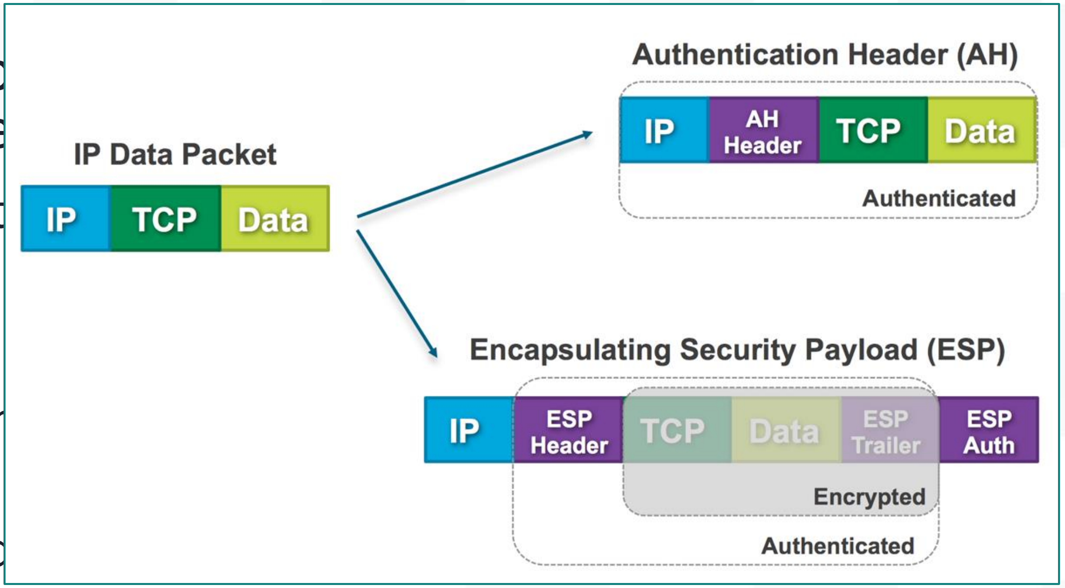
1. Two devices negotiate a secure connection using a protocol called **IKE (Internet Key Exchange)**.
2. They establish **Security Associations (SAs)** to define how the traffic will be protected (algorithms, keys, lifetimes).
3. Traffic is protected using one or both of these modes:
   - **Authentication Header (AH)**: Provides integrity and authentication (but no encryption).
   - **Encapsulating Security Payload (ESP)**: Provides encryption, integrity, and authentication.

IPSec works under the hood—encrypting and authenticating IP packets before they ever reach the app. It’s like armor at Layer 3.

IPSec (Internet Protocol Security)

A suite of protocols used to secure IP traffic b and authentication at the Network Layer (Laye

- It’s commonly used for VPNs, site-to-site encrypt untrusted networks like the Internet.



How IPSec Works (Simplified):

1. Two devices negotiate a secure connection usi **Exchange)**.
2. They establish **Security Associations (SAs)** to c (algorithms, keys, lifetimes).
3. Traffic is protected using one or both of these modes:

y and authentication (but no

Two Modes of Operation

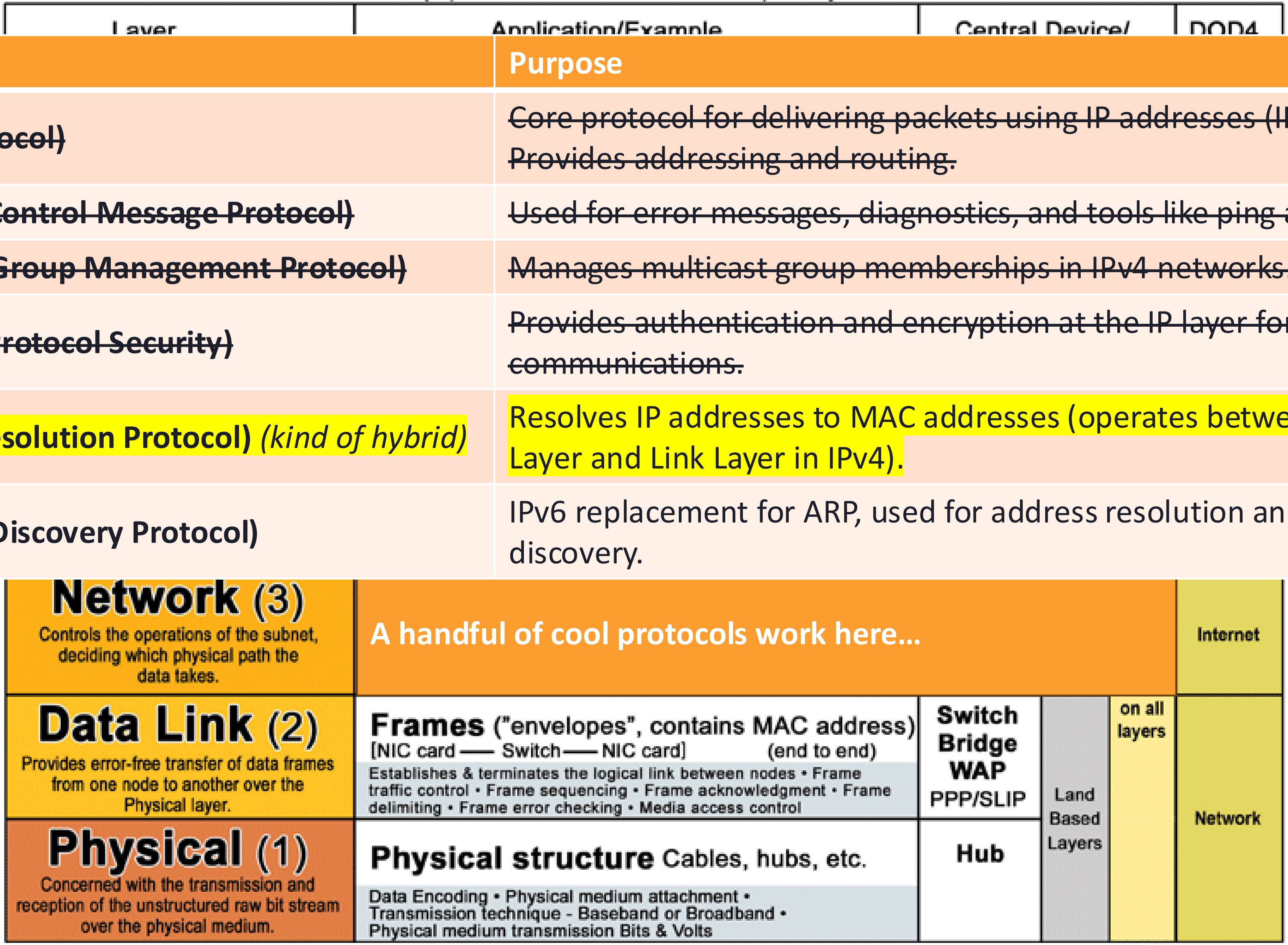
Mode	Use Case	Description
Transport	Host-to-host (e.g., internal systems)	Encrypts only the **payload** of the IP packet
Tunnel	Network-to-network (e.g., VPNs)	Encrypts the **entire IP packet** and wraps it in a new one

AKA “TCP/IP

Protocol	Purpose
~~IP (Internet Protocol)~~	~~Core protocol for delivering packets using IP addresses (IPv4 and IPv6). Provides addressing and routing.~~
~~ICMP (Internet Control Message Protocol)~~	~~Used for error messages, diagnostics, and tools like ping and traceroute.~~
~~IGMP (Internet Group Management Protocol)~~	~~Manages multicast group memberships in IPv4 networks.~~
~~IPSec (Internet Protocol Security)~~	~~Provides authentication and encryption at the IP layer for secure network communications.~~
ARP (Address Resolution Protocol) *(kind of hybrid)*	Resolves IP addresses to MAC addresses (operates between Internet Layer and Link Layer in IPv4).
NDP (Neighbor Discovery Protocol)	IPv6 replacement for ARP, used for address resolution and router discovery.

”

identifies the application



Layer	Application/Example	Central Device/			DOD4
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**A handful of cool protocols work here…**				Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	**Switch** **Bridge** **WAP** PPP/SLIP	Land Based Layers	on all layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	**Hub**			

CHAPTER 11

ARP is the protocol that says, ‘I know where you live (IP), but what’s your phone number (MAC)?’

ARP (Address Resolution Protocol)

A protocol used to map an IP address (Layer 3) to a MAC address (Layer 2) so that devices can communicate on a local network (LAN).

CHAPTER 11

ARP is the protocol that says, ‘I know where you live (IP), but what’s your phone number (MAC)?’

ARP (Address Resolution Protocol)

A protocol used to map an IP address (Layer 3) to a MAC address (Layer 2) so that devices can communicate on a local network (LAN).

- Operates only in IPv4 networks and is essential for packet delivery at the Data Link layer

CHAPTER 11

ARP is the protocol that says, 'I know where you live (IP), but what's your phone number (MAC)?'

ARP (Address Resolution Protocol)

A protocol used to map an IP address (Layer 3) to a MAC address (Layer 2) so that devices can communicate on a local network (LAN).

- Operates only in IPv4 networks and is essential for packet delivery at the Data Link layer

How ARP Works:

1. A device wants to send data to a known IP address (e.g., 192.168.1.5) **but doesn't know the MAC address**.
2. It sends an **ARP Request** (a broadcast):

   "Who has IP 192.168.1.5? Tell me."
3. The device with that IP responds with an **ARP Reply** (unicast):

   "192.168.1.5 is at MAC AA:BB:CC:DD:EE:FF."
4. The sender **caches** the response in its **ARP table** for future use.

2025 CISSP MENTOR PROGRAM

CHAPTER 11

ARP is the protocol that says, ‘I know where you live (IP), but what’s your phone number (MAC)?’

ARP (Address Resolution Protocol)

A protocol used to map an IP address (Layer 3) to a MAC address (Layer 2) so that devices can communicate on a local network (LAN).

- Operates only in IPv4 networks and is essential for packet delivery at the Data Link layer

How ARP Works:

now

Security Concerns:

- Vulnerable to ARP spoofing/poisoning, where an attacker sends fake ARP replies to redirect traffic
- Defenses include:
  - Static ARP entries
  - Dynamic ARP Inspection (DAI) on switches

“192.168.1.5 is at MAC AA:BB:CC:DD:EE:FF.”

4. The sender **caches** the resp

Key Characteristics:

- Works only within the local subnet (not across routers)
- Cached entries have a time-to-live (TTL)
- Transparent to the user—handled automatically by the OS

CHAPTER 11

ARP is the protocol that says, ‘I know where you live (IP), but what’s your phone number (MAC)?’

ARP (Address Resolution Protocol) Poisoning

A man-in-the-middle (MITM) attack where a malicious actor sends false ARP messages on a local network to trick devices into associating the attacker’s MAC address with a legitimate IP address.

ARP is the protocol that says, ‘I know where you live (IP), but what’s your phone number (MAC)?’

ARP (Address Resolution Protocol) Poisoning

A man-in-the-middle (MITM) attack where a malicious actor sends false ARP messages on a local network to trick devices into associating the attacker’s MAC address with a legitimate IP address.

How ARP Poisoning Works:

1. The attacker sends fake ARP replies to one or more devices on the LAN.
2. The victim(s) update their ARP tables, believing the attacker’s MAC belongs to a legitimate IP (e.g., the gateway).
3. All traffic intended for that IP (like the gateway) is sent to the attacker instead.
4. The attacker can:
   - Intercept the traffic (MITM)
   - Modify or drop packets
   - Relay it to the real destina

Defenses Against ARP Poisoning:

- Static ARP entries for critical devices
- Dynamic ARP Inspection (DAI) on managed switches
- Use encrypted protocols (HTTPS, SSH) to mitigate sniffing impact
- Monitor ARP tables for suspicious changes

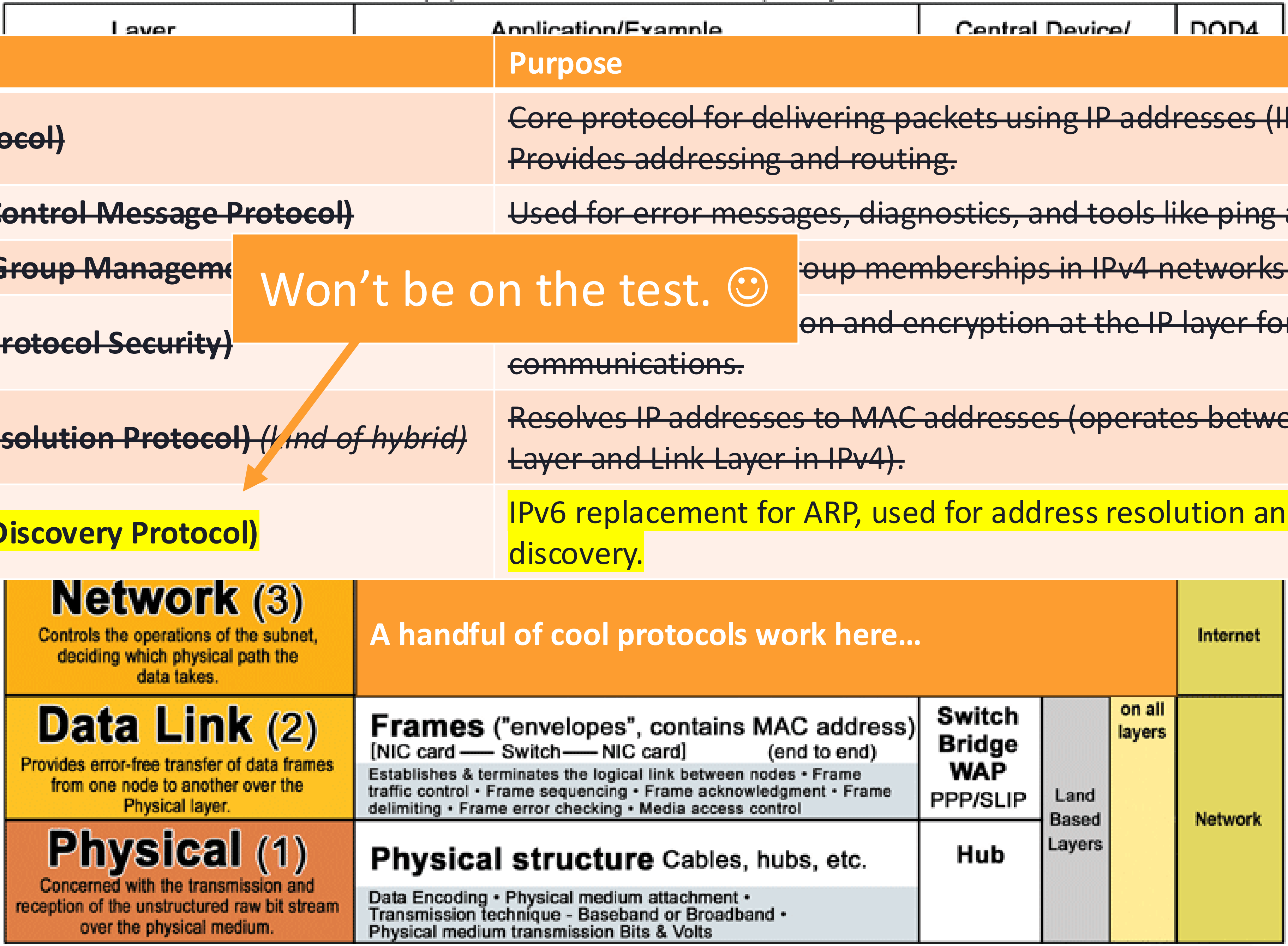
AKA “TCP/IP

Protocol	Purpose
~~IP (Internet Protocol)~~	~~Core protocol for delivering packets using IP addresses (IPv4 and IPv6). Provides addressing and routing.~~
~~ICMP (Internet Control Message Protocol)~~	~~Used for error messages, diagnostics, and tools like ping and traceroute.~~
~~IGMP (Internet Group Manageme~~	~~oup memberships in IPv4 networks.~~
~~IPSec (Internet Protocol Security)~~	~~on and encryption at the IP layer for secure network communications.~~
~~ARP (Address Resolution Protocol)~~ ~~*(kind of hybrid)*~~	~~Resolves IP addresses to MAC addresses (operates between Internet Layer and Link Layer in IPv4).~~
NDP (Neighbor Discovery Protocol)	IPv6 replacement for ARP, used for address resolution and router discovery.

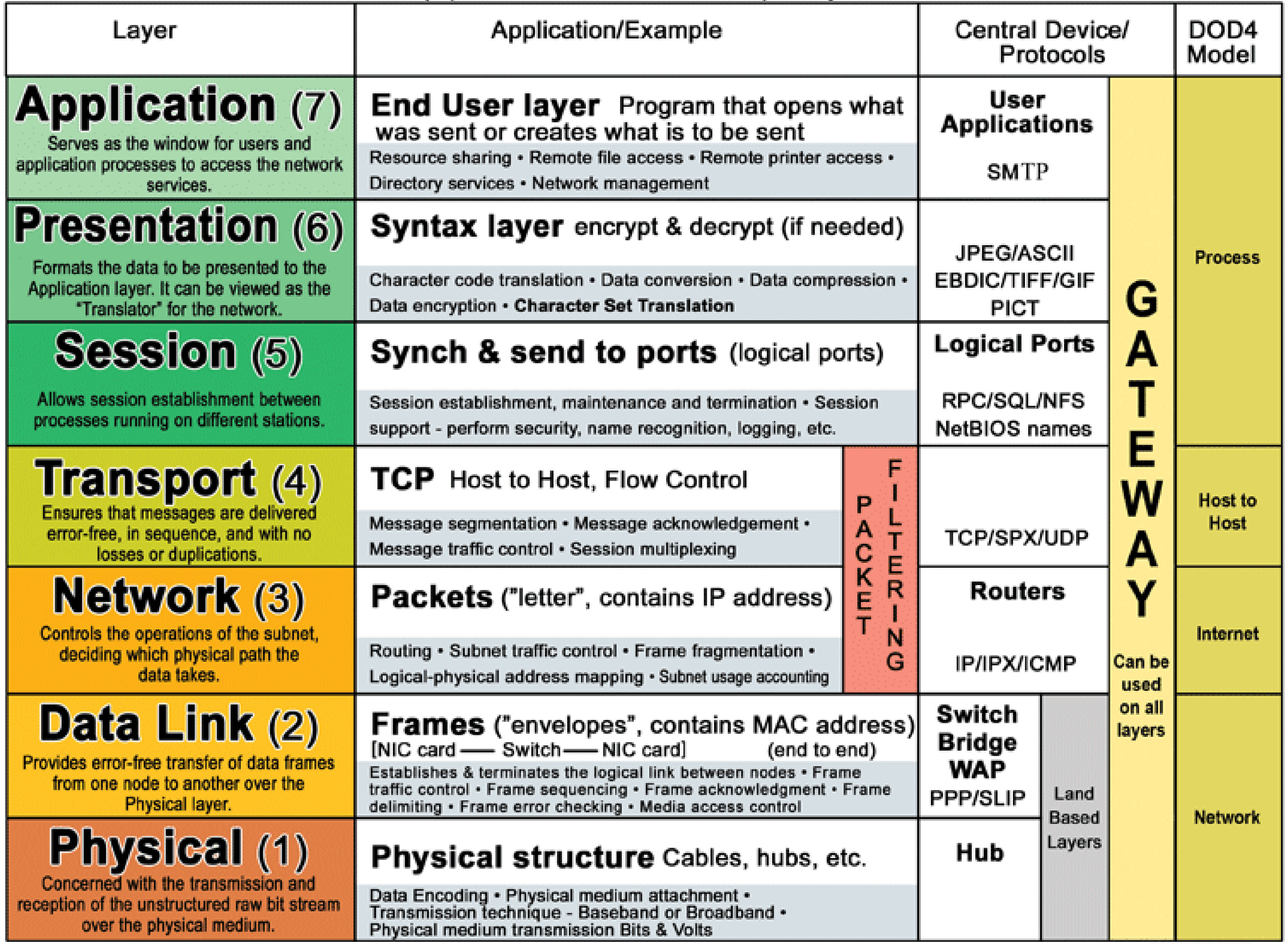
Won’t be on the test. ☺

”

identifies the application



Layer	Application/Example	Central Device/			DOD4
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	A handful of cool protocols work here…				Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	**Switch** **Bridge** **WAP** PPP/SLIP	Land Based Layers	on all layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	**Hub**			



Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP		**GATEWAY** Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP			Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch** **Bridge** **WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Secure Communication Protocols (other than IPSec)

Kerberos is like a passport system for your network—you get a ticket from the authority and show it to services as proof of identity, all without flashing your password every time.

CHAPTER 11

Secure Communication Protocols (other than IPSec)

Kerberos – Brief Explanation (in Networking Context)

A network authentication protocol that uses tickets and symmetric key cryptography to allow secure, mutual authentication between users and services over untrusted networks—without sending passwords.

CHAPTER 11

Secure Communication Protocols (other than IPSec)

Kerberos is like a passport system for your network—you get a ticket from the authority and show it to services as proof of identity, all without flashing your password every time.

Kerberos – Brief Explanation (in Networking Context)

A network authentication protocol that uses tickets and symmetric key cryptography to allow secure, mutual authentication between users and services over untrusted networks—without sending passwords.

- Originally developed at MIT and is widely used in Windows Active Directory environments.

How Kerberos Works (Simplified):

1. **Authentication** – A user logs in and requests access from the **Key Distribution Center (KDC)**.
2. The KDC responds with a **Ticket Granting Ticket (TGT)** encrypted with the user's secret key.
3. The user presents the TGT to the **Ticket Granting Service (TGS)** to request access to a specific service.
4. The TGS returns a **Service Ticket**, which the user presents to the service (e.g., a file server).
5. The service accepts the ticket and grants access—both sides trust the KDC.

CHAPTER 11

Kerberos is like a passport system for your network—you get a ticket from the authority and show it to services as proof of identity, all without flashing your password every time.

Secure Communication Protocols (other than IPSec)

Kerberos – Brief Explanation (in Networking Context)

A network authentication protocol that uses tickets and symmetric key cryptography to allow secure, mutual authentication between users and services over untrusted networks—without sending passwords.

Key Components:

- KDC (Key Distribution Center) – Trusted third party that issues tickets.
- TGT (Ticket Granting Ticket) – Proves identity to the TGS.
- TGS (Ticket Granting Service) – Issues service-specific tickets.
- Tickets – Time-limited tokens used instead of passwords.

tive Directory environments.

e **Key Distribution Center (KDC)**.

ypted with the user's secret key.

3. The user presents the … a specific service.

Benefits:

- No plaintext passwords on the wire
- Mutual authentication (both user and service verify each other)
- Single Sign-On (SSO) capability

4. The TGS returns a **Se**… rver).

nts access—both sides trust the KDC.

Which layer of the OSI Model do you think Kerberos operates (primarily)?

SSH is like a secure tunnel for admins—it encrypts everything and gives you full remote control without exposing your credentials.

CHAPTER 11

Secure Communication Protocols (other than IPSec)

SSH (Secure Shell)

A cryptographic network protocol used to securely access and manage remote systems over an untrusted network.

CHAPTER 11

SSH is like a secure tunnel for admins—it encrypts everything and gives you full remote control without exposing your credentials.

Secure Communication Protocols (other than IPSec)

SSH (Secure Shell)

A cryptographic network protocol used to securely access and manage remote systems over an untrusted network.

- Replaces older, insecure protocols like Telnet and rlogin.

What SSH Does:

- Provides confidentiality and integrity through encryption
- Supports remote command-line access, file transfers, and tunneling
- Commonly used by system administrators and network engineers

Key Features:

- Encrypted communication (protects against eavesdropping)
- Mutual authentication using passwords, public keys, or certificates
- Port forwarding/tunneling capabilities
- Supports SCP and SFTP for secure file transfers

CHAPTER 11

Secure Communication Protocols (other than IPSec)

The Signal Protocol is the gold standard for private messaging—every message is encrypted with a different key, so even if one gets cracked, the rest stay safe.

Signal Protocol

A modern cryptographic protocol designed to provide end-to-end encryption for private messaging and calls.

CHAPTER 11

Secure Communication Protocols (other than IPSec)

The Signal Protocol is the gold standard for private messaging—every message is encrypted with a different key, so even if one gets cracked, the rest stay safe.

Signal Protocol

A modern cryptographic protocol designed to provide end-to-end encryption for private messaging and calls.

- Replaces older, insecure protocols like Telnet and rlogin.

CHAPTER 11

The Signal Protocol is the gold standard for private messaging—every message is encrypted with a different key, so even if one gets cracked, the rest stay safe.

Secure Communication Protocols (other than IPSec)

Signal Protocol

A modern cryptographic protocol designed to provide end-to-end encryption for private messaging and calls.

- Replaces older, insecure protocols like Telnet and rlogin.

How It Works (Simplified):

- Uses a combination of:
  - Double Ratchet algorithm – for constantly changing encryption keys per message
  - X3DH (Extended Triple Diffie-Hellman) – for initial key agreement
  - Prekeys – for asynchronous communication (even if the recipient is offline)
- Every message is encrypted with a unique session key, providing forward secrecy.
- Post-compromise security: If a device is compromised, past messages remain secure.

Purpose:

- To ensure confidentiality, integrity, forward secrecy, and deniability in real-time communications.
- Even the service provider cannot read the messages.

CHAPTER 11

Secure Communication Protocols (other than IPSec)

Secure Remote Procedure Call (Secure RPC)

Secure RPC lets remote systems talk to each other like they're local—but it wraps those conversations in authentication and encryption.

A network communication protocol that enables a program on one computer to securely execute code or access services on another computer—as if it were local—while ensuring authentication, integrity, and confidentiality.

Purpose:

- To enable trusted communication between distributed systems or services, especially in client-server architectures.
- Used heavily in enterprise environments for secure service calls, authentication, and directory services.

How It Provides Security:

- Adds security features on top of standard RPC:
- Authentication of users/services (often with Kerberos)
- Encryption of data in transit
- Integrity checking to ensure messages aren't tampered with

Common Use Cases:

- NFS (Network File System) with Kerberos
- Active Directory and Windows Domain Services
- Enterprise systems requiring secure inter-process communication

CHAPTER 11

Converged Protocols

Converged protocols bring everything onto one wire—great for efficiency, but if you don't secure that wire, everything is at risk.

Refer to network protocols that combine multiple types of traffic—data, voice, and video—onto a single network infrastructure, typically over IP-based networks.

Purpose:

- To simplify infrastructure by eliminating the need for separate networks (e.g., one for phones, one for computers).
- To improve efficiency, cost-effectiveness, and scalability.

Examples of Converged Protocols:

- VoIP (Voice over IP): Transmits voice calls over IP networks.
- SIP (Session Initiation Protocol): Sets up and manages multimedia communication sessions.
- MPLS (Multiprotocol Label Switching): Supports multiple types of traffic (e.g., data, voice, video) over a single WAN.
- FCoE (Fibre Channel over Ethernet): Transports storage traffic over Ethernet networks.

Benefits:

- Reduces hardware and cabling costs
- Streamlines management and maintenance
- Supports unified communications (UC)

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Converged Protocols

Converged protocols bring everything onto one wire—great for efficiency, but if you don't secure that wire, everything is at risk.

Refer to network protocols that combine multiple types of traffic—data, voice, and

ased networks.

Security Considerations:

- Converging protocols increases complexity and risk:
  - QoS (Quality of Service) must be enforced for voice/video
  - Requires strong segmentation, encryption, and traffic prioritization
  - Compromises in one system (e.g., VoIP) can impact the entire network

the need for

s, one for

computers).

- To improve efficiency, cost-effectiveness, and scalability.

Examples of Converged Protocols:

- VoIP (Voice over IP): Transmits voice calls over IP networks.
- SIP (Session Initiation Protocol): Sets up and manages multimedia communication sessions.
- MPLS (Multiprotocol Label Switching): Supports multiple types of traffic (e.g., data, voice, video) over a single WAN.
- FCoE (Fibre Channel over Ethernet): Transports storage traffic over Ethernet networks.

Benefits:

- Reduces hardware and cabling costs
- Streamlines management and maintenance
- Supports unified communications (UC)

CHAPTER 11

Converged Protocols

Voice over Internet Protocol (VoIP)

VoIP turns your voice into packets. Great for cost and flexibility—but if you don't secure the stream, your conversation's fair game.

A technology that allows you to make voice calls over IP networks, including the Internet, instead of traditional telephone lines (PSTN).

CHAPTER 11

Converged Protocols

Voice over Internet Protocol (VoIP)

VoIP turns your voice into packets. Great for cost and flexibility—but if you don't secure the stream, your conversation's fair game.

A technology that allows you to make voice calls over IP networks, including the Internet, instead of traditional telephone lines (PSTN).

How VoIP Works (Simplified):

1. Voice is captured by a microphone and converted into digital data.
2. That data is compressed and packetized using codecs (like G.711 or G.729).
3. Packets are sent over an IP network (e.g., your LAN, WAN, or the Internet).
4. At the destination, packets are reassembled and converted back into audio.

Core VoIP Components:

- IP Phones / Softphones: Devices that send and receive VoIP calls.
- VoIP Gateway: Bridges VoIP calls to traditional phone networks (PSTN).
- SIP (Session Initiation Protocol): Manages call setup, teardown, and control.
- RTP (Real-time Transport Protocol): Delivers the actual voice data.

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Converged Protocols

Voice over Internet Protocol (VoIP)

VoIP turns your voice into packets. Great for cost and flexibility—but if you don't secure the stream, your conversation's fair game.

A technology that allows you to mak
of traditional telephone lines (PSTN)

Benefits:

- Lower cost (especially for long-distance calls)
- Flexibility (can call from anywhere with Internet)
- Supports voice, video, and messaging over the same network

How VoIP Works (Simplified):

1. Voice is captured by a micropho
2. That data is compressed and packetized using codecs
3. Packets are sent over an IP network (e.g., your LAN, W
4. At the destination, packets are reassembled and conv

Security Concerns:

- Eavesdropping (use encryption: SRTP, TLS)
- DoS attacks on VoIP services
- Caller ID spoofing and toll fraud
- Must implement QoS (Quality of Service) to ensure call clarity

Core VoIP Components:

- IP Phones / Softphones: Devices that send and receive VoIP calls.
- VoIP Gateway: Bridges VoIP calls to traditional phone networks (PSTN).
- SIP (Session Initiation Protocol): Manages call setup, teardown, and control.
- RTP (Real-time Transport Protocol): Delivers the actual voice data.

CHAPTER 11

SDN turns your network from hardware-bound to software-driven—making it smarter, faster, and way easier to control… but only if you lock down that controller.

Software-Defined Networking (SDN)

A modern network architecture that separates the control plane from the data plane, allowing centralized, programmable control of the network.

CHAPTER 11

SDN turns your network from hardware-bound to software-driven—making it smarter, faster, and way easier to control… but only if you lock down that controller.

Software-Defined Networking (SDN)

A modern network architecture that separates the control plane from the data plane, allowing centralized, programmable control of the network.

How SDN Works (Simplified):

1. **Control Plane**:
   - Makes decisions about where traffic should go
   - Centralized in an SDN controller
2. **Data Plane** (Forwarding Plane):
   - Moves packets based on rules from the controller
   - Resides in switches/routers
3. **Applications**: Use APIs to talk to the controller and define behavior (e.g., traffic shaping, security policies)

CHAPTER 11

SDN turns your network from hardware-bound to software-driven—making it smarter, faster, and way easier to control… but only if you lock down that controller.

Software-Defined Networking (SDN)

A modern network architecture that separates the control plane from the data plane, allowing centralized, programmable control of the network.

How SDN Works (Simplified):

1. **Control Plane**:
   - Makes decisions about where traffic should go
   - Centralized in an SDN controller
2. **Data Plane** (Forwarding Plane):
   - Moves packets based on rules from the controller
   - Resides in switches/routers
3. **Applications**: Use APIs to talk to the controller and define behavior (e.g., traffic shaping, security policies)

Purpose:

- To make networks more agile, flexible, and easier to manage
- To enable automation, dynamic configuration, and centralized oversight

Core Protocol: OpenFlow is a common protocol used to communicate between the SDN controller and network devices.

CHAPTER 11

SDN turns your network from hardware-bound to software-driven—making it smarter, faster, and way easier to control… but only if you lock down that controller.

Software-Defined Networking (SDN)

A modern network architecture that separates the control plane from the data plane, allowing centralized, programmable control of the network.

How SDN Works (Simplified):

1. **Control Plane**:

ere traffic should go

roller

):

ules from the controller

s

3. **Applications**: Use APIs to talk to th ffic shaping, security policies)

Benefits:

- Centralized management
- Improved network visibility
- Rapid deployment of services and policies
- Automation and orchestration

Purpose:

- To make networks more agile, flexible, and easier to manage
- To enable automation, dynamic configuration, and centralized oversight

Security Considerations:

- SDN introduces a central point of failure (the controller)
- Requires strong access controls, encryption, and monitoring
- Enables dynamic security controls (e.g., automatic isolation of infected hosts)

Core Protocol: OpenFlow is a common protocol u between the SDN controller and network devices

CHAPTER 11

Network segmentation is like watertight doors on a ship—one compartment floods, the whole thing doesn't sink.

Segmentation

The practice of dividing a network into smaller, isolated segments or subnetworks, each with its own access controls and security boundaries.

- Limits how far traffic—and threats—can move within a network.

CHAPTER 11

Segmentation

Network segmentation is like watertight doors on a ship—one compartment floods, the whole thing doesn't sink.

The practice of dividing a network into smaller, isolated segments or subnetworks, each with its own access controls and security boundaries.

- Limits how far traffic—and threats—can move within a network.

Purpose:

- Improve security by containing breaches or malware
- Reduce lateral movement of attackers inside the network
- Improve performance and traffic management
- Enforce least privilege by controlling access between segments

Security Use Cases:

- Separating user devices from critical systems
- Isolating IoT devices or guest Wi-Fi
- Containing compromised machines in breach scenarios
- Enforcing Zero Trust principles

How It's Done:

- VLANs (Virtual LANs) – Logically separate traffic within switches
- Subnetting – Divides IP address space into isolated segments
- Firewalls & ACLs – Control traffic between segments
- Physical segmentation – Using separate hardware (less common now)

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Segmentation

Network segmentation is like watertight doors on a ship—one compartment floods, the whole thing doesn't sink.

The practice of dividing a network into smaller, isolated segments or subnetworks, each with its

k.

Micro-segmentation is an advanced form of network segmentation that isolates workloads or applications down to the individual device or process level, not just by subnet or VLAN. It's a key strategy in Zero Trust architecture.

Purpose:

- Provide granular, fine-tuned control over east-west traffic (traffic inside the data center or cloud)
- Prevent lateral movement of threats—even between workloads on the same subnet
- Enforce least privilege access between apps, services, and users

How It Works:

- Uses software-defined controls (like host-based firewalls or hypervisor policies)
- Enforced via:
  - Firewall rules
  - Security groups
  - Agents on endpoints
  - SDN or virtualization platforms (e.g., VMware NSX, AWS Security Groups)

rity Use Cases:

parating user devices from
tical systems
olating IoT devices or guest Wi-Fi
ntaining compromised
achines in breach scenarios
forcing Zero Trust principles

CHAPTER 11

Edge Networks

Edge networks push intelligence closer to the action—so decisions happen faster, but security must keep up at every edge point.

Refers to a distributed computing architecture where processing, storage, and services occur closer to the data source or end user, rather than relying solely on centralized data centers or cloud infrastructure.

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Edge Networks

Edge networks push intelligence closer to the action—so decisions happen faster, but security must keep up at every edge point.

Refers to a distributed computing architecture where processing, storage, and services occur closer to the data source or end user, rather than relying solely on centralized data centers or cloud infrastructure.

Purpose:

- Reduce latency (faster response times)
- Minimize bandwidth usage by processing data locally
- Improve performance, reliability, and resilience for real-time applications

How It Works:

- Data is processed at or near the “edge” of the network—such as on IoT devices, local servers, or edge routers.
- Only essential data is sent back to the cloud or data center.
- Common in IoT, autonomous vehicles, industrial control systems, and smart cities.

CHAPTER 11

Edge Networks

Edge networks push intelligence closer to the action—so decisions happen faster, but security must keep up at every edge point.

Refers to a distributed computing architecture where processing, storage, and services occur closer to the data source or end user, rather than relying solely on centralized data centers or cloud infrastructure.

Purpose:

- Reduce latency (faster response times)
- ally
- real-time applications
- Data is processed a
  or edge routers.
- Only essential data i
- Common in IoT, autonomous vehicles, industrial control systems, and smart cities.

Examples of Edge Network Components:

- Smart sensors in factories
- Content Delivery Network (CDN) edge servers
- Mobile base stations
- Local edge gateways

Security Considerations:

- Broader attack surface due to many distributed endpoints
- Requires endpoint security, network segmentation, and strong authentication
- Must ensure secure data transmission and local device hardening

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Wireless Networks

Wired networks are locked doors. Wireless networks are open windows—great for access, but easy to exploit if you don't secure them properly.

Use radio frequency (RF) signals instead of cables to transmit data between devices.

CHAPTER 11

Wireless Networks

Wired networks are locked doors. Wireless networks are open windows—great for access, but easy to exploit if you don't secure them properly.

Use radio frequency (RF) signals instead of cables to transmit data between devices.

Types of Wireless Networks:

1. WLAN (Wireless Local Area Network)

- Most common type—used in homes, offices, schools
- Based on **IEEE 802.11** standards (Wi-Fi)
- Connects devices like laptops, phones, and printers to a local network

Pros: High-speed, widely supported

Cons: Limited range (~100-300 feet), interference, security risks if unsecured

CHAPTER 11

Wireless Networks

Wired networks are locked doors. Wireless networks are open windows—great for access, but easy to exploit if you don't secure them properly.

Use radio frequency (RF) signals instead of cables to transmit data between devices.

Types of Wireless Networks:

2. **WPAN (Wireless Personal Area Network)**

- Short-range communication (a few meters)
- Based on Bluetooth, Zigbee, or Infrared
- Used for connecting personal devices (e.g., headphones, wearables, keyboards)

Pros: Low power, good for IoT and peripherals

Cons: Limited range and data rates, easier to jam or interfere

CHAPTER 11

Wireless Networks

Wired networks are locked doors. Wireless networks are open windows—great for access, but easy to exploit if you don't secure them properly.

Use radio frequency (RF) signals instead of cables to transmit data between devices.

Types of Wireless Networks:

3. **WMAN (Wireless Metropolitan Area Network)**

- Covers a city-sized area
- Based on WiMAX (IEEE 802.16) or 4G/5G infrastructure
- Used for broadband Internet access in urban areas

Pros: Covers wide areas, supports mobile users

Cons: Expensive infrastructure, regulatory complexity

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Wireless Networks

Wired networks are locked doors. Wireless networks are open windows—great for access, but easy to exploit if you don't secure them properly.

Use radio frequency (RF) signals instead of cables to transmit data between devices.

Types of Wireless Networks:

4. **WWAN (Wireless Wide Area Network)**

- Covers large geographic areas (nationwide or global)
- Based on cellular networks (3G, 4G, 5G)
- Used for mobile data (e.g., LTE, 5G on smartphones)

Pros: Long-range, global access

Cons: Dependent on carrier, can be slower and costlier than wired networks

Security Considerations for All Wireless Networks:

- Must use encryption (e.g., WPA3 for Wi-Fi)
- MAC filtering and network segmentation improve control
- Wireless is inherently more exposed—anyone in range can attempt to connect or intercept

Other Wireless Technologies:

- Satellite networks – for rural or hard-to-reach areas
- Mesh networks – decentralized networks where each node forwards traffic (great for resilient coverage)

Standard	Common Name	Max Theoretical Data Rate	Frequency Band	Channel Width	Access Method
802.11	Legacy Wi-Fi	2 Mbps	2.4 GHz	20 MHz	CSMA/CA
802.11a	Wi-Fi 1	54 Mbps	5 GHz	20 MHz	CSMA/CA
802.11b	Wi-Fi 2	11 Mbps	2.4 GHz	20 MHz	CSMA/CA
802.11g	Wi-Fi 3	54 Mbps	2.4 GHz	20 MHz	CSMA/CA
802.11n	Wi-Fi 4	600 Mbps (with 4x4 MIMO)	2.4 & 5 GHz	20/40 MHz	CSMA/CA, MIMO
802.11ac	Wi-Fi 5	~6.9 Gbps (with 8x8 MIMO)	5 GHz	20/40/80/160 MHz	CSMA/CA, MU-MIMO (downlink)
802.11ax	Wi-Fi 6 / 6E	~9.6 Gbps	2.4, 5, & 6 GHz	20–160 MHz	OFDMA, MU-MIMO (bi-dir)
802.11be	Wi-Fi 7 (future)	Up to ~46 Gbps (projected)	2.4, 5, & 6 GHz	Up to 320 MHz	OFDMA, MU-MIMO, Multi-link

Quick Definitions:

- CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance (standard Wi-Fi method)
- MIMO: Multiple Input, Multiple Output (uses multiple antennas)
- MU-MIMO: Multi-User MIMO (serves multiple clients at once)
- OFDMA: Orthogonal Frequency Division Multiple Access (splits channels into sub-channels for efficiency)

Standard	Common Name	Max Theoretical Data Rate	Frequency Band	Channel Width	Access Method
802.1				MHz	CSMA/CA
802.1				MHz	CSMA/CA
802.1				MHz	CSMA/CA
802.1				MHz	CSMA/CA
802.1				40 MHz	CSMA/CA, MIMO
802.1				40/80/160 MHz	CSMA/CA, MU-MIMO (downlink)
802.1				160 MHz	OFDMA, MU-MIMO (bi-dir)
802.11be	Wi-Fi 7 (future)	Up to ~46 Gbps (projected)	2.4, 5, & 6 GHz	Up to 320 MHz	OFDMA, MU-MIMO, Multi-link

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

- Used in Wi-Fi networks (802.11)
- Devices listen before they talk to avoid collisions.
- If the medium is clear, the device sends data; if busy, it waits or uses a random backoff timer.
- Unlike Ethernet's CSMA/CD (collision detection), Wi-Fi can't detect collisions—so it tries to avoid them.

✅ Good for: Shared wireless environments

❌ Limitation: Can lead to performance drops with many users

Quick Definitions:

- CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance (standard Wi-Fi method)
- MIMO: Multiple Input, Multiple Output (uses multiple antennas)
- MU-MIMO: Multi-User MIMO (serves multiple clients at once)
- OFDMA: Orthogonal Frequency Division Multiple Access (splits channels into sub-channels for efficiency)

Standard	Common Name	Max Theoretical Data Rate	Frequency Band	Channel Width	Access Method
802.1				MHz	CSMA/CA
802.1				MHz	CSMA/CA
802.1				MHz	CSMA/CA
802.1				MHz	CSMA/CA
802.1				40 MHz	CSMA/CA, MIMO
802.1				40/80/160 MHz	CSMA/CA, MU-MIMO (downlink)
802.11ax	Wi-Fi 6 / 6E	~9.6 Gbps	2.4, 5, & 6 GHz	20–160 MHz	OFDMA, MU-MIMO (bi-dir)
802.11be	Wi-Fi 7 (future)	Up to ~46 Gbps (projected)	2.4, 5, & 6 GHz	Up to 320 MHz	OFDMA, MU-MIMO, Multi-link

MIMO (Multiple Input, Multiple Output)

- Uses **multiple antennas** at both transmitter and receiver ends.
- Allows multiple data streams to be sent **simultaneously** over the same frequency.
- Boosts **throughput**, **range**, and **reliability** in Wi-Fi (starting with 802.11n and beyond).

✅ Good for: High-performance wireless networks (Wi-Fi 4, 5, 6)
❌ Limitation: Needs hardware support and line-of-sight benefits

Quick Definitions:

- CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance (standard Wi-Fi method)
- MIMO: Multiple Input, Multiple Output (uses multiple antennas)
- MU-MIMO: Multi-User MIMO (serves multiple clients at once)
- OFDMA: Orthogonal Frequency Division Multiple Access (splits channels into sub-channels for efficiency)

Standard	Common Name	Max Theoretical Data Rate	Frequency Band	Channel Width	Access Method
802.1				MHz	CSMA/CA
802.1				MHz	CSMA/CA
802.1				MHz	CSMA/CA
802.1				MHz	CSMA/CA
802.1				40 MHz	CSMA/CA, MIMO
802.11ac	Wi-Fi 5	~6.9 Gbps (with 8x8 MIMO)	5 GHz	20/40/80/160 MHz	CSMA/CA, MU-MIMO (downlink)
802.11ax	Wi-Fi 6 / 6E	~9.6 Gbps	2.4, 5, & 6 GHz	20–160 MHz	OFDMA, MU-MIMO (bi-dir)
802.11be	Wi-Fi 7 (future)	Up to ~46 Gbps (projected)	2.4, 5, & 6 GHz	Up to 320 MHz	OFDMA, MU-MIMO, Multi-link

TDMA (Time Division Multiple Access)

- Divides time into **slots and** assigns each user/device a **specific time slot** to transmit.
- Devices **take turns** using the same frequency.

✓ Good for: Organized and predictable communication

✗ Limitation: Idle slots if users have no data to send

Quick Definitions:

- CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance (standard Wi-Fi method)
- MIMO: Multiple Input, Multiple Output (uses multiple antennas)
- MU-MIMO: Multi-User MIMO (serves multiple clients at once)
- OFDMA: Orthogonal Frequency Division Multiple Access (splits channels into sub-channels for efficiency)

CDMA (Code Division Multiple Access)

- Allows multiple devices to transmit simultaneously over the same frequency using unique codes.
- Each receiver filters out signals using its own unique code.

✓ Good for: Mobile phone networks (used in 3G)
✗ Limitation: More complex to implement and manage

Standard	Common Name	Max Theoretical Data Rate	Frequency Band	Channel Width	Access Method
802.1				MHz	CSMA/CA
802.1				MHz	CSMA/CA
802.1				MHz	CSMA/CA
802.1				MHz	CSMA/CA
802.1				40 MHz	CSMA/CA, MIMO
802.11ac	Wi-Fi 5	~6.9 Gbps (with 8x8 MIMO)	5 GHz	20/40/80/160 MHz	CSMA/CA, MU-MIMO (downlink)
802.11ax	Wi-Fi 6 / 6E	~9.6 Gbps	2.4, 5, & 6 GHz	20–160 MHz	OFDMA, MU-MIMO (bi-dir)
802.11be	Wi-Fi 7 (future)	Up to ~46 Gbps (projected)	2.4, 5, & 6 GHz	Up to 320 MHz	OFDMA, MU-MIMO, Multi-link

Quick Definitions:

- CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance (standard Wi-Fi method)
- MIMO: Multiple Input, Multiple Output (uses multiple antennas)
- MU-MIMO: Multi-User MIMO (serves multiple clients at once)
- OFDMA: Orthogonal Frequency Division Multiple Access (splits channels into sub-channels for efficiency)

Standard	Common Name	Max Theoretical Data Rate	Frequency Band	Channel Width	Access Method
802.1				MHz	CSMA/CA
802.1				MHz	CSMA/CA
802.1				MHz	CSMA/CA
802.1				MHz	CSMA/CA
802.1				40 MHz	CSMA/CA, MIMO
802.1					)
802.11ax	Wi-Fi 6 / 6E	~9.6 Gbps	2.4, 5, & 6		bi-dir)
802.11be	Wi-Fi 7 (future)	Up to ~46 Gbps (projected)	2.4, 5, & 6 GHz	Up to 320 MHz	OFDMA, MU-MIMO, Multi-link

OFDMA (Orthogonal Frequency Division Multiple Access)

- Splits a wide channel into smaller subcarriers and assigns these to different users.
- Used in Wi-Fi 6 (802.11ax) and 4G/5G.
- Allows simultaneous transmission by multiple users, increasing efficiency and reducing latency.

✅ Good for: Dense environments (stadiums, offices)

❌ Limitation: Requires compatible hardware and firmware

Think of CSMA/CA as polite conversation, TDMA as scheduled speeches, CDMA as everyone talking in their own language, and OFDMA as splitting a big stage into mini-stages.

Quick Definitions:

- CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance (standard Wi-Fi method)
- MIMO: Multiple Input, Multiple Output (uses multiple antennas)
- MU-MIMO: Multi-User MIMO (serves multiple clients at once)
- OFDMA: Orthogonal Frequency Division Multiple Access (splits channels into sub-channels for efficiency)

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Wireless Networks

SSID, ESSID

Wired networks are locked doors. Wireless networks are open windows—great for access, but easy to exploit if you don’t secure them properly.

CHAPTER 11

Wireless Networks

SSID, ESSID

Wired networks are locked doors. Wireless networks are open windows—great for access, but easy to exploit if you don't secure them properly.

SSID stands for **Service Set Identifier**. It's the **name of a wireless network** that a device sees when scanning for Wi-Fi (e.g., Starbucks_WiFi, HomeNetwork123).

- It identifies a **single access point or network segment**.
- Broadcasted by access points to help devices find and connect to them.
- Can be **up to 32 characters** in length.

ESSID stands for **Extended Service Set Identifier**.

- It refers to a **network with multiple access points** (APs) sharing the **same SSID** and connected to the **same wired backbone**.
- Used in **enterprise** or large environments to enable **seamless roaming** (e.g., in schools, hospitals, or corporate offices).

Think of:

- SSID = One access point's network name
- ESSID = A unified name shared across multiple access points in a single logical network

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Wireless Networks

Security Best Practices for SSID/ESSID

Your SSID is your network's name tag—make it smart, not sensitive. Security comes from encryption and isolation, not from hiding the name.

CHAPTER 11

Wireless Networks

Your SSID is your network’s name tag—make it smart, not sensitive. Security comes from encryption and isolation, not from hiding the name.

Security Best Practices for SSID/ESSID

1. **Use a Unique, Non-Revealing SSID**
   - Avoid default names like Linksys, NETGEAR, or CorpWiFi (easier to target).
   - Don’t include sensitive info (company name, floor number, etc.).

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Wireless Networks

Your SSID is your network's name tag—make it smart, not sensitive. Security comes from encryption and isolation, not from hiding the name.

Security Best Practices for SSID/ESSID

1. **Use a Unique, Non-Revealing SSID**
   - Avoid default names like Linksys, NETGEAR, or CorpWiFi (easier to target).
   - Don't include sensitive info (company name, floor number, etc.).
2. **Disable SSID Broadcast Only with Caution**
   - Hiding the SSID doesn't truly secure it—tools like Wireshark can still detect it.
   - Hidden SSIDs can cause devices to probe constantly, which can expose the SSID and increase attack surface.

Your SSID is your network's name tag—make it smart, not sensitive. Security comes from encryption and isolation, not from hiding the name.

Security Best Practices for SSID/ESSID

1. **Use a Unique, Non-Revealing SSID**
   - Avoid default names like Linksys, NETGEAR, or CorpWiFi (easier to target).
   - Don't include sensitive info (company name, floor number, etc.).
2. **Disable SSID Broadcast Only with Caution**
   - Hiding the SSID doesn't truly secure it—tools like Wireshark can still detect it.
   - Hidden SSIDs can cause devices to probe constantly, which can expose the SSID and increase attack surface.
3. **Use Strong Encryption**
   - Always use WPA2 or WPA3 with a strong passphrase.
   - Avoid WEP and open networks unless absolutely necessary.

CHAPTER 11

Wireless Networks

Your SSID is your network's name tag—make it smart, not sensitive. Security comes from encryption and isolation, not from hiding the name.

Security Best Practices for SSID/ESSID

1. **Use a Unique, Non-Revealing SSID**
   - Avoid default names like Linksys, NETGEAR, or CorpWiFi (easier to target).
   - Don't include sensitive info (company name, floor number, etc.).
2. **Disable SSID Broadcast Only with Caution**
   - Hiding the SSID doesn't truly secure it—tools like Wireshark can still detect it.
   - Hidden SSIDs can cause devices to probe constantly, which can expose the SSID and increase attack surface.
3. **Use Strong Encryption**
   - Always use WPA2 or WPA3 with a strong passphrase.
   - Avoid WEP and open networks unless absolutely necessary.
4. **Segment with Multiple SSIDs When Appropriate**
   - Use separate SSIDs for guests, IoT devices, or BYOD.
   - Apply VLANs and firewall rules between SSIDs.
5. **Monitor for Rogue SSIDs**
   - Attackers can create Evil Twin networks using similar SSIDs to trick users.
   - Use wireless intrusion detection/prevention systems (WIDS/WIPS) to catch this.

CHAPTER 11

Wireless Networks

Wired Equivalent Privacy (WEP)

WEP was a good idea at the time, but a disaster in practice. If you see it in the wild today, it's a red flag.

A **legacy** security protocol for wireless networks, introduced as part of the original IEEE 802.11 standard in 1997.

CHAPTER 11

Wireless Networks

Wired Equivalent Privacy (WEP)

WEP was a good idea at the time, but a disaster in practice. If you see it in the wild today, it's a red flag.

A **legacy** security protocol for wireless networks, introduced as part of the original IEEE 802.11 standard in 1997.

How WEP Works:

- Uses RC4 stream cipher for encryption.
- Employs a shared static key (usually 40 or 104 bits) plus a 24-bit initialization vector (IV).
- Encrypts data frames between wireless clients and access points.

CHAPTER 11

Wireless Networks

Wired Equivalent Privacy (WEP)

WEP was a good idea at the time, but a disaster in practice. If you see it in the wild today, it's a red flag.

A **legacy** security protocol for wireless networks, introduced as part of the original IEEE 802.11 standard in 1997.

Security Status:

- WEP is considered broken and insecure.
- Replaced by WPA and later WPA2/WPA3.

How WEP Works:

- Uses RC4 stream cipher for encryption.
- Employs a shared static key (usually 40 or 104 bits) plus a 24-bit initialization vector (IV).
- Encrypts data frames between wireless clients and access points.

Why WEP Is Weak and Deprecated:

- IV is too short and often reused, making it vulnerable to key recovery attacks.
- RC4 implementation flaws allow attackers to crack WEP keys in minutes using tools like Aircrack-ng.
- Lacks strong integrity checking, making it susceptible to packet injection and replay attacks.

CHAPTER 11

Wireless Networks

Wi-Fi Protected Access (WPA)

WPA patched the holes in WEP, but it wasn’t built to last. It’s better than WEP—but not by today’s standards.

- A wireless security protocol developed as an interim fix for WEP’s flaws.
- It was introduced by the Wi-Fi Alliance in 2003 and is based on the IEEE 802.11i draft standard.

WPA patched the holes in WEP, but it wasn't built to last. It's better than WEP—but not by today's standards.

Wi-Fi Protected Access (WPA)

- A wireless security protocol developed as an interim fix for WEP's flaws.
- It was introduced by the Wi-Fi Alliance in 2003 and is based on the IEEE 802.11i draft standard.

How WPA Works:

- Uses **TKIP (Temporal Key Integrity Protocol)**:
    - Dynamically generates a new encryption key for every packet
    - Still based on RC4, but much more secure than WEP
- Includes Message Integrity Check (MIC) to prevent packet tampering
- Supports 802.1X authentication for enterprise environments (WPA-Enterprise) or pre-shared key (PSK) for home use (WPA-Personal)

Limitations:

- TKIP was an improvement over WEP but still relies on outdated encryption (RC4)
- Vulnerable to certain attacks (e.g., Beck–Tews attack)
- Was eventually replaced by WPA2, which introduced AES encryption

CHAPTER 11

Wireless Networks

Wi-Fi Protected Access 2 (WPA2)

WPA2 is what WPA should've been—strong encryption, wide support, and still common today. Just don't use it with a weak password.

- The second-generation wireless security protocol developed by the Wi-Fi Alliance, introduced in 2004.
- Replaced WPA and became the mandatory security standard for all certified Wi-Fi devices starting in 2006.

CHAPTER 11

Wireless Networks

WPA2 is what WPA should've been—strong encryption, wide support, and still common today. Just don't use it with a weak password.

Wi-Fi Protected Access 2 (WPA2)

- The second-generation wireless security protocol developed by the Wi-Fi Alliance, introduced in 2004.
- Replaced WPA and became the mandatory security standard for all certified Wi-Fi devices starting in 2006.

How WPA2 Works:

- Uses AES (Advanced Encryption Standard) with CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for:
  - Confidentiality (encryption)
  - Integrity (data authenticity)
- Supports:
  - WPA2-Personal (with a pre-shared key or PSK)
  - WPA2-Enterprise (uses 802.1X with RADIUS authentication for large networks)

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Wireless Networks

Wi-Fi Protected Access 2 (WPA2)

WPA2 is what WPA should've been—strong encryption, wide support, and still common today. Just don't use it with a weak password.

- The second-generation wireless security protocol developed by the Wi-Fi Alliance, introduced in 2004

Strengths:

- Much stronger encryption than WPA's RC4/TKIP
- Widely supported and trusted for over a decade
- Enables robust enterprise authentication via certificate-based systems

for all certified Wi-Fi devices

- Uses AES (A
  Chaining Me
  - Confide
  - Integrity

Limitations:

- Vulnerable to brute-force attacks if the pre-shared key is weak
- Susceptible to KRACK (Key Reinstallation Attack) if patches aren't applied
- Doesn't include modern features like individualized encryption per user/device

- Supports:
  - WPA2-Personal (with a pre-shared key or PSK)
  - WPA2-Enterprise (uses 802.1X with RADIUS authentication for large networks)

CHAPTER 11

Wireless Networks

WPA3 fixes the biggest holes in WPA2. It's like locking the doors, windows, and throwing away the default keys—finally bringing Wi-Fi security into the modern era.

Wi-Fi Protected Access 3 (WPA3)

- The latest Wi-Fi security standard, introduced in 2018 by the Wi-Fi Alliance.
- Addresses known weaknesses in WPA2, in both personal and enterprise environments.

CHAPTER 11

Wireless Networks

Wi-Fi Protected Access 3 (WPA3)

WPA3 fixes the biggest holes in WPA2. It's like locking the doors, windows, and throwing away the default keys—finally bringing Wi-Fi security into the modern era.

- The latest Wi-Fi security standard, introduced in 2018 by the Wi-Fi Alliance.
- Addresses known weaknesses in WPA2, in both personal and enterprise environments.

Key Features of WPA3:

1. **SAE (Simultaneous Authentication of Equals)**:
   - Replaces the WPA2 pre-shared key (PSK) handshake
   - Provides resistance to offline dictionary attacks
   - Offers forward secrecy (compromising one session doesn't reveal past sessions)
2. **Stronger Encryption**:
   - Minimum of 128-bit encryption for personal use
   - 192-bit encryption required for WPA3-Enterprise (high-security environments)
3. **Individualized Data Encryption**: In open networks (like coffee shops), WPA3 uses Opportunistic Wireless Encryption (OWE) to encrypt each user's traffic—even without a password
4. **Enhanced Protection for IoT Devices**: Easy Connect (DPP) makes it easier and more secure to onboard devices without screens (e.g., printers, smart bulbs)

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Wireless Networks

802.1X, EAP, LEAP, and PEAP

802.1X is the bouncer, EAP is the protocol passport, and PEAP makes sure your credentials aren't shouted across the street. Just don't invite LEAP—it's old, weak, and unreliable.

CHAPTER 11

Wireless Networks

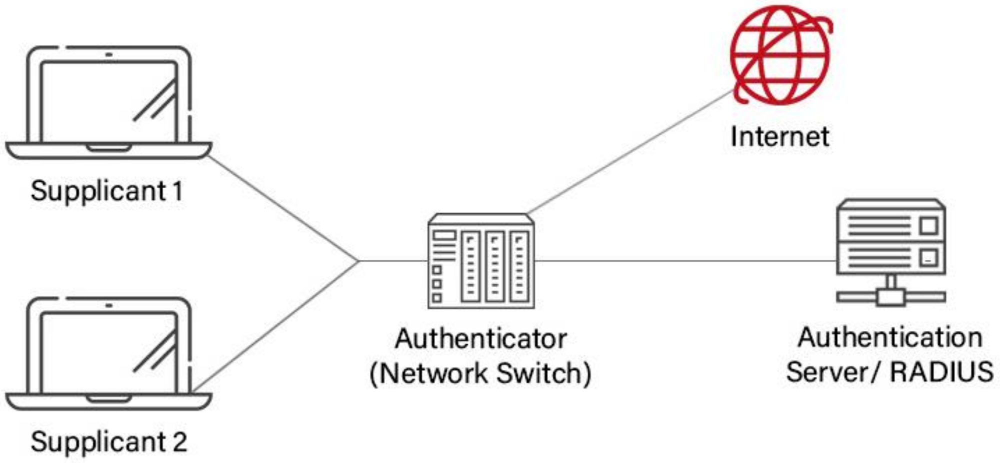
802.1X, EAP, LEAP, and PEAP

802.1X is the bouncer, EAP is the protocol passport, and PEAP makes sure your credentials aren’t shouted across the street. Just don’t invite LEAP—it’s old, weak, and unreliable.

802.1X – Port-Based Network Access Control

- Framework for authenticating devices on wired or w
- Defines how access is granted before full network
- Commonly used in enterprise Wi-Fi and VPNs.

The components of 802.1X



Key Roles:

- Supplicant – The device/user trying to connect
- Authenticator – The network device (e.g., switch or AP) enforcing access control
- Authentication Server – Usually a RADIUS server that validates credentials

2025 CISSP MENTOR PROGRAM

CHAPTER 11

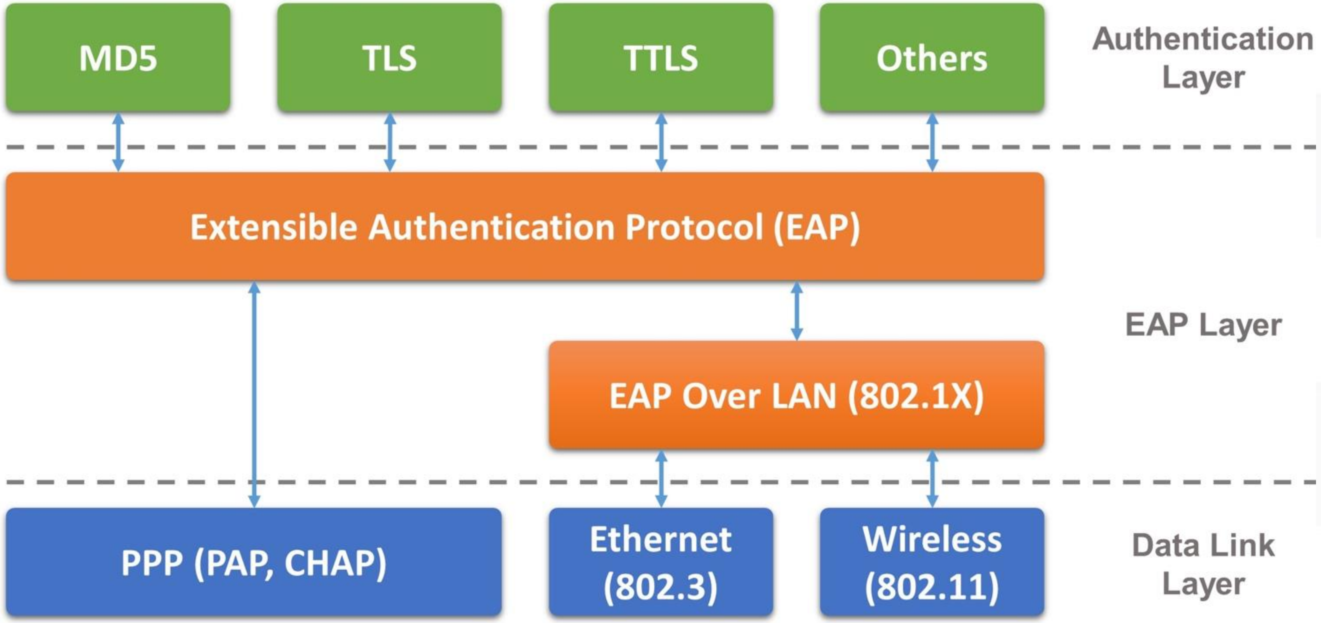
Wireless Networks

802.1X is the bouncer, EAP is the protocol passport, and PEAP makes sure your credentials aren't shouted across the street. Just don't invite LEAP—it's old, weak, and unreliable.

802.1X, EAP, LEAP, and PEAP

EAP (Extensible Authentication Protocol)

- A framework (not a protocol itself) used within 802.1X to support various authentication methods.
- Supports things like:
  - Passwords
  - Certificates
  - Tokens
  - Biometrics



CHAPTER 11

Wireless Networks

Wi-Fi Protected Setup (WPS)

WPS was built for convenience, not security. If your router has it on—and you don't need it—**turn it off**.

A network security standard introduced in 2007 to make it easier for users to connect devices to a secure wireless network without manually entering a password.

CHAPTER 11

Wireless Networks

Wi-Fi Protected Setup (WPS)

WPS was built for convenience, not security. If your router has it on—and you don't need it—**turn it off**.

A network security standard introduced in 2007 to make it easier for users to connect devices to a secure wireless network without manually entering a password.

How WPS Works:

There are several WPS connection methods:

1. **Push Button (PBC):** Press a button on the router and then on the device within 2 minutes to connect.
2. **PIN Entry**: Enter an 8-digit PIN (usually printed on the router) into the device or vice versa.
3. **NFC or USB** (rare): Use NFC tap or USB transfer to configure wireless settings.

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Wireless Networks

Wi-Fi Protected Setup (WPS)

WPS was built for convenience, not security. If your router has it on—and you don't need it—**turn it off**.

A network security standard introduced in 2007 to make it easier for users to connect devices to a secure wireless network without manually entering a password.

How WPS Works:

There are several WPS connectio

1. **Push Button (PBC):** Press a b connect.
2. **PIN Entry**: Enter an 8-digit PIN (usually printed on the router) into the device or vice versa.

Security Recommendations:

- Disable WPS in your router's settings if not needed.
- Use strong WPA2/WPA3 passwords instead.
- If WPS must be used, prefer the Push Button method, not the PIN.

Security Weaknesses:

- WPS PIN method is vulnerable to brute-force attacks, as the 8-digit PIN can be guessed in a few hours.
- Attack tools like Reaver and PixieWPS can exploit this flaw.
- WPS doesn't work with enterprise-grade WPA2-Enterprise authentication.

CHAPTER 11

Wireless Networks

Captive Portals

Captive portals aren’t real security—they’re gatekeepers for access control. Great for guest management, but not a substitute for encryption or endpoint protection.

A web page that is automatically displayed to users when they first connect to a public or semi-public Wi-Fi network, requiring them to take some action before gaining full network access.

CHAPTER 11

Wireless Networks

Captive portals aren’t real security—they’re gatekeepers for access control. Great for guest management, but not a substitute for encryption or endpoint protection.

Captive Portals

A web page that is automatically displayed to users when they first connect to a public or semi-public Wi-Fi network, requiring them to take some action before gaining full network access.

Purpose:

- Enforce user authentication or terms of service acceptance
- Collect user data or payment (e.g., in hotels, airports, cafés)
- Limit access to unauthorized users

CHAPTER 11

Wireless Networks

Captive Portals

Captive portals aren't real security—they're gatekeepers for access control. Great for guest management, but not a substitute for encryption or endpoint protection.

A web page that is automatically displayed to users when they first connect to a public or semi-public Wi-Fi network, requiring them to take some action before gaining full network access.

Purpose:

- Enforce user authentication or terms of service acceptance
- Collect user data or payment (e.g., in hotels, airports, cafés)
- Limit access to unauthorized users

How It Works:

1. User connects to an open or secured Wi-Fi network.
2. Any attempt to access a website redirects the user to the captive portal page.
3. The portal may require: Login credentials (username/password)/Email or phone verification/ /Payment/Agreement of terms of use.
4. After successful interaction, network access is granted (often via MAC or IP whitelisting)

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Wireless Networks

Captive Portals

Captive portals aren’t real security—they’re gatekeepers for access control. Great for guest management, but not a substitute for encryption or endpoint protection.

A web page that is automatically ı public or semi-
public Wi-Fi network, requiring the vork access.

Security Considerations:

- Not encrypted by default—use HTTPS-based portals or secure tunneled connections (e.g., VPN) afterward
- Susceptible to phishing if not implemented properly (attackers can spoof captive portals)
- Often used with RADIUS or backend authentication systems

Purpose:

- Enforce user authenticatio
- Collect user data or payme
- Limit access to unauthoriz

How It Works:

1. User connects to an open or secured Wi-Fi network.
2. Any attempt to access a website redirects the user to the captive portal page.
3. The portal may require: Login credentials (username/password)/Email or phone verification/ /Payment/Agreement of terms of use.
4. After successful interaction, network access is granted (often via MAC or IP whitelisting)

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Wireless Networks

General Wi-Fi Security Procedure

From the book...

CHAPTER 11

Wireless Networks

General Wi-Fi Security Procedure

From the book…

1. Update firmware.
2. Change the default administrator password to something unique and complex.
3. Enable WPA2 or WPA3 encryption.
4. Enable ENT authentication or PSK/SAE with long, complex passwords.
5. Change the SSID (the default is often the vendor name).
6. Change the wireless MAC address (to hide OUI and device make/model that may be encoded into the default MAC address).
7. Decide whether to disable the SSID broadcast based on your deployment requirements (even though this doesn't increase security).
8. Enable MAC filtering if the pool of wireless clients is relatively small (usually less than 20) and static.
9. Consider using static IP addresses or configure DHCP with reservations (applicable only for small deployments).

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Wireless Networks

General Wi-Fi Security Procedure

From the book...

10. Treat wireless as external or remote access and separate the WAP from the wired network using a firewall.
11. Treat wireless as an entry point for attackers and monitor all WAP-to-wired-network wired-network communications with a NIDS.
12. Deploy a wireless intrusion detection system (WIDS) and a wireless intrusion prevention system (WIPS).
13. Consider requiring the use of a VPN across a Wi-Fi link.
14. Implement a captive portal.
15. Track/log all wireless activities and events.

STOP

CHAPTER 11

Wireless Networks

DHCP is like handing out room keys at a hotel—fast and automatic, but if a fake concierge shows up, guests get misdirected.

DHCP (Dynamic Host Configuration Protocol)

A network management protocol used to automatically assign IP addresses and other network configuration settings (like subnet mask, default gateway, and DNS servers) to devices on a network.

CHAPTER 11

Wireless Networks

DHCP is like handing out room keys at a hotel—fast and automatic, but if a fake concierge shows up, guests get misdirected.

DHCP (Dynamic Host Configuration Protocol)

A network management protocol used to automatically assign IP addresses and other network configuration settings (like subnet mask, default gateway, and DNS servers) to devices on a network.

Purpose: To eliminate the need for manual IP configuration, simplify network administration, and reduce configuration errors.

How DHCP Works (4-Step Process – DORA):

1. **Discover** – Client sends a broadcast to find a DHCP server
2. **Offer** – Server responds with an available IP and configuration info
3. **Request** – Client requests to use the offered IP address
4. **Acknowledgment** (ACK) – Server confirms and leases the IP address

CHAPTER 11

Wireless Networks

DHCP is like handing out room keys at a hotel—fast and automatic, but if a fake concierge shows up, guests get misdirected.

DHCP (Dynamic Host Configuration Protocol)

A network management protocol used to automatically assign IP addresses and other network configuration settings (like subnet mask, default gateway, and DNS servers) to devices on a network.

Purpose: To e
reduce config

Security Considerations:

- No authentication by default—vulnerable to rogue DHCP servers and DHCP spoofing
- Should be paired with features like DHCP snooping, port security, and network segmentation to prevent abuse

How DHCP W

DHCP Details:

- Operates at: Application Layer (OSI Layer 7), uses UDP ports 67 (server) and 68 (client)
- Leases IPs for a limited time, after which renewal or reallocation is required
- Supports static reservations and IP exclusions

4. **Acknowledgment** (ACK) – Server confirms and leases the IP address

CHAPTER 11

Wireless Networks

HIDS, HIPS, NIDS, and NIPS

HIDS (Host-Based Intrusion Detection System)

- Monitors activity on a single host (e.g., server, workstation).
- Detects suspicious behavior like file integrity changes, log tampering, or unauthorized access.
- Works after the fact (detects intrusions but doesn't block them).

Good for: Monitoring critical servers, detecting malware, insider threats.

HIPS (Host-Based Intrusion Prevention System)

- Like HIDS, but with the added ability to block or prevent malicious actions.
- Can stop known attacks, terminate processes, or quarantine files.
- Often includes behavior-based and signature-based detection.

Good for: Protecting endpoints in real time, stopping ransomware or exploits.

CHAPTER 11

Wireless Networks

HIDS, HIPS, NIDS, and NIPS

HIDS/HIPS protect the house. NIDS/NIPS guard the street. Use both for layered defense.

NIDS (Network-Based Intrusion Detection System)

- Monitors network traffic in real time to detect anomalies or known attack signatures.
- Passive—alerts only, does not block traffic.
- Often deployed at network chokepoints (e.g., between DMZ and internal network).

Good for: Detecting port scans, unusual protocols, data exfiltration attempts.

NIPS (Network-Based Intrusion Prevention System)

- Like NIDS but actively blocks or drops malicious traffic.
- Can reset connections, block IPs, or apply rate-limiting.
- Positioned inline (i.e., traffic passes through it).

Good for: Stopping DoS attacks, worms, and known exploits before they hit hosts.

CHAPTER 11

Wireless Networks

Bluetooth

Bluetooth is great for convenience, but convenience is the enemy of security. Disable it when you don't need it.

- A short-range wireless communication technology designed for connecting devices over short distances without cables.
- Operates in the 2.4 GHz ISM band and is widely used for personal area networks (PANs).

CHAPTER 11

Wireless Networks

Bluetooth

Bluetooth is great for convenience, but convenience is the enemy of security. Disable it when you don't need it.

- A short-range wireless communication technology designed for connecting devices over short distances without cables.
- Operates in the 2.4 GHz ISM band and is widely used for personal area networks (PANs).

Purpose: To enable **low-power, low-bandwidth** wireless communication between devices like:

- Headphones
- Keyboards & mice
- Smartphones
- Smartwatches
- IoT devices

How It Works:

- Devices form a piconet: one master and up to seven slaves.
- Communication is based on frequency hopping spread spectrum (FHSS) to reduce interference.
- Range typically:
  - ~10 meters for standard devices (Class 2)
  - Up to 100 meters for high-power devices (Class 1)

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Wireless Networks

Bluetooth

Bluetooth is great for convenience, but convenience is the enemy of security. Disable it when you don’t need it.

Security Features:

- Pairing with PINs or passkeys
- Supports encryption, authentication, and frequency hopping
- Vulnerable to attacks like Bluejacking, Bluesnarfing, and Bluetooth spoofing if not properly secured

signed for connecting devices over short

Bluetooth Versions:

- Bluetooth Classic – higher throughput, used for audio and data
- Bluetooth Low Energy (BLE) – lower power, used in fitness trackers, sensors, etc.

- Headphones
- Keyboards & mice
- Smartphones
- Smartwatches
- IoT devices

How It Works:

- Devices form a piconet: one master and up to seven slaves.
- Communication is based on frequency hopping spread spectrum (FHSS) to reduce interference.
- Range typically:
  - ~10 meters for standard devices (Class 2)
  - Up to 100 meters for high-power devices (Class 1)

CHAPTER 11

Wireless Networks

Bluetooth Attacks

Bluetooth is like your front porch—great when you invite people, but dangerous if you leave the door unlocked. Disable discoverability and keep firmware updated.

CHAPTER 11

Wireless Networks

Bluetooth is like your front porch—great when you invite people, but dangerous if you leave the door unlocked. Disable discoverability and keep firmware updated.

Bluetooth Attacks

Bluesniffing

- A passive attack that involves scanning for discoverable Bluetooth devices.
- Similar to “war driving” but for Bluetooth.
- Often used as reconnaissance to find targets for other attacks.
- **Risk Level**: Low by itself, but sets the stage for more serious exploits.

CHAPTER 11

Wireless Networks

Bluetooth Attacks

Bluetooth is like your front porch—great when you invite people, but dangerous if you leave the door unlocked. Disable discoverability and keep firmware updated.

Bluesniffing

- A passive attack that involves scanning for discoverable Bluetooth devices.
- Similar to “war driving” but for Bluetooth.
- Often used as reconnaissance to find targets for other attacks.
- **Risk Level**: Low by itself, but sets the stage for more serious exploits.

Bluesmacking

- A denial-of-service (DoS) attack using oversized or malformed L2CAP (Logical Link Control and Adaptation Protocol) packets.
- Can crash or freeze the target device by overwhelming it.
- **Risk Level**: Medium, more disruptive than dangerous.

CHAPTER 11

Wireless Networks

Bluetooth Attacks

Bluetooth is like your front porch—great when you invite people, but dangerous if you leave the door unlocked. Disable discoverability and keep firmware updated.

Bluejacking

- The act of sending unsolicited messages or contacts to nearby Bluetooth devices.
- Exploits the Bluetooth object exchange (OBEX) protocol.
- Typically harmless, more of a prank or annoyance.
- **Risk Level**: Low but could be used for social engineering.

CHAPTER 11

Wireless Networks

Bluetooth is like your front porch—great when you invite people, but dangerous if you leave the door unlocked. Disable discoverability and keep firmware updated.

Bluetooth Attacks

Bluejacking

- The act of sending unsolicited messages or contacts to nearby Bluetooth devices.
- Exploits the Bluetooth object exchange (OBEX) protocol.
- Typically harmless, more of a prank or annoyance.
- **Risk Level**: Low but could be used for social engineering.

BLUFFS (Bluetooth Forward and Future Secrecy)

- Modern cryptographic attack (2022) that targets Bluetooth Secure Connections pairing mode.
- Exploits flaws in session key derivation to interfere with future sessions, decrypt data, and hijack connections
- Affects Bluetooth 4.2 and later, including BLE.
- **Risk Level**: **High** — real-world implications if not patched.

CHAPTER 11

Wireless Networks

Bluetooth Attacks

Bluetooth is like your front porch—great when you invite people, but dangerous if you leave the door unlocked. Disable discoverability and keep firmware updated.

Bluesnarfing

- An attack that allows an attacker to steal data (contacts, emails, files) from a vulnerable device via Bluetooth.
- Exploits flaws in older OBEX implementations.
- Works on discoverable and misconfigured devices.
- **Risk Level**: **High** — can compromise personal or corporate data.

CHAPTER 11

Wireless Networks

Bluetooth Attacks

Bluetooth is like your front porch—great when you invite people, but dangerous if you leave the door unlocked. Disable discoverability and keep firmware updated.

Bluesnarfing

- An attack that allows an attacker to steal data (contacts, emails, files) from a vulnerable device via Bluetooth.
- Exploits flaws in older OBEX implementations.
- Works on discoverable and misconfigured devices.
- **Risk Level**: **High** — can compromise personal or corporate data.

Bluebugging

- A powerful attack where the attacker gains control over the victim's device using Bluetooth.
- Can make/receive calls, send/receive texts, access contacts and call logs, and perform other unauthorized actions
- Exploits legacy pairing vulnerabilities.
- **Risk Level**: **Very High** — essentially a remote device takeover.

CHAPTER 11

Wireless Networks

RFID

RFID adds convenience but can quietly leak identity or location data. Always evaluate the balance between usability and privacy.

- Wireless technology used for identifying and tracking objects or people using radio waves.
- Allows data to be transmitted from a small tag to a reader without physical contact.

CHAPTER 11

Wireless Networks

RFID adds convenience but can quietly leak identity or location data. Always evaluate the balance between usability and privacy.

RFID

- Wireless technology used for identifying and tracking objects or people using radio waves.
- Allows data to be transmitted from a small tag to a reader without physical contact.

How It Works:

- An RFID tag contains a microchip and an antenna.
- A nearby RFID reader emits radio waves to power the tag (if passive) and read or write data.
- Data is sent back from the tag to the reader and processed by a connected system.

Identification
Access Control
Tracking
Anti-counterfeiting
Management
Counting
MILK

CHAPTER 11

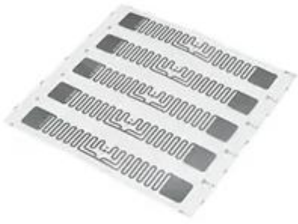
Wireless Networks

RFID Types

RFID adds convenience but can quietly leak identity or location data. Always evaluate the balance between usability and privacy.

1. **Passive RFID**
    - No internal power source
    - Activated by the reader's signal
    - Short range (up to a few meters)
2. **Active RFID**
    - Has a battery
    - Longer range (tens to hundreds of meters)
    - Used in real-time tracking systems
3. **Semi-passive** (or semi-active):Battery-powered but only transmits when activated by a reader

Active RFID



Passive RFID

BAP RFID

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Wireless Networks

RFID Types

RFID adds convenience but can quietly leak identity or location data. Always evaluate the balance between usability and privacy.

1. **Passive RFID**
   - No internal power source
   - Activated by the reader's signal

2

   - Used in real-time tracking systems

3. **Semi-passive** (or semi-active):Battery-powered but only

Security Concerns:

- Eavesdropping on tag-reader communication
- Cloning or spoofing RFID tags
- Unauthorized tracking or surveillance
- Weak or no encryption on many consumer RFID systems

Passive RFID

BAP RFID

Common Uses:

- Inventory and asset tracking
- Access control (e.g., employee badges)
- Toll collection (e.g., EZ Pass)
- Contactless payment systems
- Animal microchips

CHAPTER 11

Wireless Networks

NFC (Near Field Communication)

NFC is like a digital handshake—quick, close, and (usually) safe—but always watch who you're shaking hands with.

A short-range wireless communication technology that allows devices to exchange data when they are within a few centimeters of each other—typically 4 cm or less.

CHAPTER 11

Wireless Networks

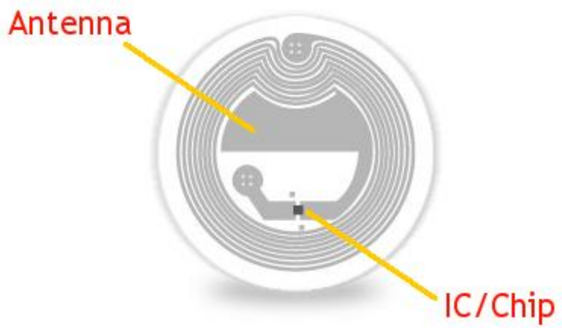
NFC is like a digital handshake—quick, close, and (usually) safe—but always watch who you're shaking hands with.

NFC (Near Field Communication)

A short-range wireless communication technology that allows devices to exchange data when they are within a few centimeters of each other—typically 4 cm or less.

How NFC Works:

- Operates at 13.56 MHz (HF band) and is based on RFID technology.
- Communication can be:
  - **One-way** (reader → tag)
  - **Two-way** (peer-to-peer)
- Initiates data exchange when devices tap or come very close together.



CHAPTER 11

Wireless Networks

NFC (Near Field Communication)

NFC is like a digital handshake—quick, close, and (usually) safe—but always watch who you're shaking hands with.

NFC Modes:

- Reader/Writer Mode – Reads data from passive tags (e.g., posters, smart cards)
- Peer-to-Peer Mode – Devices exchange data (e.g., contact info, files)
- Card Emulation Mode – Device acts like a smart card (e.g., contactless payments via Google Pay or Apple Pay)

exchange data when

- Communication can be:
  - **One-way** (reader → tag)

very close tog

Security Features:

- Short range limits attack surface
- Supports encryption and secure elements (e.g., in phones for payment credentials)
- Still vulnerable to:
  - Eavesdropping
  - Relay attacks
  - Data modification or interception

Common Uses:

- Mobile payments (tap-to-pay)
- Access control (key cards, badges)
- Transit systems
- Smart posters or tags
- Device pairing (Bluetooth or Wi-Fi)

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Wireless Networks

Common Wireless Attacks - Explained

Wireless isn't the weak point—bad configuration and lazy security are. You can't stop attackers from scanning, but you can stop giving them open doors.

CHAPTER 11

Wireless Networks

Wireless isn’t the weak point—bad configuration and lazy security are. You can’t stop attackers from scanning, but you can stop giving them open doors.

Common Wireless Attacks - Explained

1. **Evil Twin Attack**

   Think of it as a wireless phishing trap.

   - Attacker sets up a fake access point that mimics a legitimate one (same SSID).
   - Victims connect to the rogue AP, unknowingly giving up credentials or allowing man-in-the-middle (MITM) monitoring.

CHAPTER 11

Wireless Networks

Wireless isn’t the weak point—bad configuration and lazy security are. You can’t stop attackers from scanning, but you can stop giving them open doors.

Common Wireless Attacks - Explained

1. **Evil Twin Attack**

   Think of it as a wireless phishing trap.

   - Attacker sets up a fake access point that mimics a legitimate one (same SSID).
   - Victims connect to the rogue AP, unknowingly giving up credentials or allowing man-in-the-middle (MITM) monitoring.

2. **Rogue Access Point (Rogue AP)**

   Like a secret tunnel under your firewall.

   - A non-authorized AP plugged into a corporate network, often by a careless or malicious insider.
   - Can bypass perimeter security and open a backdoor into internal resources.

CHAPTER 11

Wireless Networks

Wireless isn't the weak point—bad configuration and lazy security are. You can't stop attackers from scanning, but you can stop giving them open doors.

Common Wireless Attacks - Explained

1. **Evil Twin Attack**

   Think of it as a wireless phishing trap.

   - Attacker sets up a fake access point that mimics a legitimate one (same SSID).
   - Victims connect to the rogue AP, unknowingly giving up credentials or allowing man-in-the-middle (MITM) monitoring.

2. **Rogue Access Point (Rogue AP)**

   Like a secret tunnel under your firewall.

   - A non-authorized AP plugged into a corporate network, often by a careless or malicious insider.
   - Can bypass perimeter security and open a backdoor into internal resources.

3. **Deauthentication Attack**

   - Attacker sends spoofed deauth frames to disconnect users from a wireless AP.
   - Often used as a prelude to Evil Twin or credential capture attacks (e.g., with tools like Aircrack-ng or WiFi Pumpkin).

   A shove to knock you off your Wi-Fi so you reconnect to something evil.

CHAPTER 11

Wireless Networks

Wireless isn't the weak point—bad configuration and lazy security are. You can't stop attackers from scanning, but you can stop giving them open doors.

Common Wireless Attacks - Explained

Like wiretapping a phone call, but for data.

4. Packet Sniffing (Eavesdropping)
    - Capturing unencrypted wireless traffic using tools like Wireshark or Kismet.
    - Exposes sensitive data if encryption is weak (e.g., WEP) or if open networks are used.

CHAPTER 11

Wireless Networks

Wireless isn't the weak point—bad configuration and lazy security are. You can't stop attackers from scanning, but you can stop giving them open doors.

Common Wireless Attacks - Explained

4. **Packet Sniffing (Eavesdropping)**
   - Capturing unencrypted wireless traffic using tools like Wireshark or Kismet.
   - Exposes sensitive data if encryption is weak (e.g., WEP) or if open networks are used.

Like wiretapping a phone call, but for data.

5. **Wi-Fi Phishing (Captive Portal Hijacking)**
   - Attacker redirects users to a fake login portal to harvest credentials.
   - Often combined with Evil Twin attacks.

You connect at Starbucks, but the portal's a trap.

CHAPTER 11
Wireless Networks

Wireless isn't the weak point—bad configuration and lazy security are. You can't stop attackers from scanning, but you can stop giving them open doors.

Common Wireless Attacks - Explained

4. **Packet Sniffing (Eavesdropping)**
   - Capturing unencrypted wireless traffic using tools like Wireshark or Kismet.
   - Exposes sensitive data if encryption is weak (e.g., WEP) or if open networks are used.

Like wiretapping a phone call, but for data.

5. **Wi-Fi Phishing (Captive Portal Hijacking)**
   - Attacker redirects users to a fake login portal to harvest credentials.
   - Often combined with Evil Twin attacks.

You connect at Starbucks, but the portal's a trap.

6. **WEP Cracking**
   - Exploits vulnerabilities in the Wired Equivalent Privacy (WEP) protocol to recover the encryption key.
   - Outdated and trivially broken today—should never be used.

Like locking your door with a zip tie.

CHAPTER 11

Wireless Networks

Wireless isn't the weak point—bad configuration and lazy security are. You can't stop attackers from scanning, but you can stop giving them open doors.

Common Wireless Attacks - Explained

Just because it's "WPA2" doesn't mean it's unbreakable—password strength matters.

7. **WPA/WPA2 Pre-Shared Key Cracking**
   - Capturing the 4-way handshake and running a dictionary or brute-force attack to guess the password.
   - Especially effective if the passphrase is weak.

CHAPTER 11

Wireless Networks

Wireless isn't the weak point—bad configuration and lazy security are. You can't stop attackers from scanning, but you can stop giving them open doors.

Common Wireless Attacks - Explained

Just because it's "WPA2" doesn't mean it's unbreakable—password strength matters.

7. **WPA/WPA2 Pre-Shared Key Cracking**
   - Capturing the 4-way handshake and running a dictionary or brute-force attack to guess the password.
   - Especially effective if the passphrase is weak.
8. **Bluetooth Attacks**
   - Bluesnarfing (stealing data),
   - Bluejacking (sending messages),
   - Bluebugging (controlling devices),
   - BLUFFS (modern crypto attack),
   - Bluesmacking (DoS).

Small range ≠ small risk

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Wireless Networks

Wireless isn't the weak point—bad configuration and lazy security are. You can't stop attackers from scanning, but you can stop giving them open doors.

Common Wireless Attacks - Explained

It's like blasting static to drown out a conversation.

9. **RF Jamming (Wireless DoS)**
   - Floods the wireless spectrum with noise, disrupting legitimate communication.
   - Often illegal and hard to defend against.

CHAPTER 11

Wireless Networks

Wireless isn't the weak point—bad configuration and lazy security are. You can't stop attackers from scanning, but you can stop giving them open doors.

Common Wireless Attacks - Explained

It's like blasting static to drown out a conversation.

9. **RF Jamming (Wireless DoS)**
   - Floods the wireless spectrum with noise, disrupting legitimate communication.
   - Often illegal and hard to defend against.
10. **Near Field Exploits (NFC/RFID Attacks)**
    - Skimming, replay attacks, or eavesdropping on contactless payments or access cards.
    - Especially dangerous in crowded places (airports, subways, conferences).

That "tap and go" badge might just give you away.

Best Defenses:

- Use WPA3 or WPA2-Enterprise
- Enforce strong passwords
- Disable WPS
- Monitor for rogue devices
- Train users on safe Wi-Fi practices
- Implement network segmentation and intrusion detection

CHAPTER 11

Wireless Networks

Satellite Communications

Satellite links can reach anywhere, but that reach goes both ways—remote access requires robust encryption and authentication.

Satellite communications (SatCom) use artificial satellites in Earth's orbit to relay radio signals between ground stations or mobile terminals over long distances—even to remote or oceanic regions where traditional infrastructure is unavailable.

CHAPTER 11

Wireless Networks

Satellite links can reach anywhere, but that reach goes both ways—remote access requires robust encryption and authentication.

Satellite Communications

Satellite communications (SatCom) use artificial satellites in Earth's orbit to relay radio signals between ground stations or mobile terminals over long distances—even to remote or oceanic regions where traditional infrastructure is unavailable.

How It Works:

1. A ground station (uplink) sends a signal to a satellite.
2. The satellite receives, amplifies, and retransmits the signal back to Earth (downlink) to a receiver.
3. This can support two-way communication, broadcasting, or data relays.

CHAPTER 11

Wireless Networks

Satellite links can reach anywhere, but that reach goes both ways—remote access requires robust encryption and authentication.

Satellite Communications

Satellite communications (SatCom) use artificial satellites in Earth's orbit to relay radio signals between ground stations or mobile terminals over long distances—even to remote or oceanic regions where traditional infrastructure is unavailable.

How It Works:

1. A ground station (uplink) sends a signal to a satellite.
2. The satellite receives, amplifies, and retransmits the signal back to Earth (downlink) to a receiver.
3. This can support two-way communication, broadcasting, or data relays.

Types of Satellites:

- GEO (Geostationary Earth Orbit) – ~35,786 km; appears fixed above one point. Good for TV, weather.
- LEO (Low Earth Orbit) – ~500–2,000 km; fast, low-latency, used in satellite internet (e.g., Starlink).
- MEO (Medium Earth Orbit) – ~2,000–20,000 km; used in GPS and some comms.

CHAPTER 11

Wireless Networks

Satellite Communications

Satellite links can reach anywhere, but that reach goes both ways—remote access requires robust encryption and authentication.

Satellite communications (SatCom) use artificial satellites in Earth's orbit to relay radio signals between ground stations or mobile terminals over long distances—even to remote or oceanic regions where traditional infrastructure is unavailable.

Common Uses:

- Global internet coverage (e.g., Starlink, OneWeb)
- Military and intelligence communications
- GPS and navigation systems
- Maritime and aviation comms
- Broadcasting (TV, radio)

l to a satellite.

transmits the signal back to Earth (downlink) to a

Security Considerations:

- Susceptible to eavesdropping, signal jamming, and spoofing
- Encryption is essential
- Satellite links can introduce latency, weather-related degradation, and line-of-sight limitations

Types of Satellites:

- GEO (Geostationary Ea d for TV, weather.
- LEO (Low Earth Orbit) – ~500–2,000 km; fast, low-latency, used in satellite internet (e.g., Starlink).
- MEO (Medium Earth Orbit) – ~2,000–20,000 km; used in GPS and some comms.

CHAPTER 11

Wireless Networks

Cellular networks aren’t just phones anymore—they’re the backbone of modern connectivity. But mobility demands security at every handoff.

Cellular Networks

A type of wireless communication system that divide geographic areas into “cells”, each served by a cell tower (base station). They enable mobile devices to communicate with each other and the broader telephone and internet networks using radio waves.

CHAPTER 11
Wireless Networks

Cellular networks aren't just phones anymore—they're the backbone of modern connectivity. But mobility demands security at every handoff.

Cellular Networks

A type of wireless communication system that divide geographic areas into "cells", each served by a cell tower (base station). They enable mobile devices to communicate with each other and the broader telephone and internet networks using radio waves.

How It Works:

1. A mobile device connects to the nearest cell tower.
2. Voice and data are transmitted via radio frequency (RF) to the tower.
3. The tower connects to the core network, which routes traffic to other towers, the internet, or the telephone network.

As users move, their connection is handed off to nearby cells to maintain service.

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Wireless Networks

Cellular networks aren’t just phones anymore—they’re the backbone of modern connectivity. But mobility demands security at every handoff.

Cellular Networks

A type of wireless communication system that divi n served by a cell tower (base station). They enable mobile c ther and

(RF) to the tower.

es traffic to other towers, the internet, or

Generations of Cellular Networks

Generation	Key Features
1G	Analog voice only
2G	Digital voice, basic SMS
3G	Mobile internet, video calls
4G (LTE)	High-speed internet, HD streaming
5G	Ultra-fast, low latency, IoT support

Key Technologies:

- FDMA, TDMA, CDMA, OFDMA – techniques for sharing spectrum
- SIM cards – store subscriber info for network access
- Roaming – allows access across regions or carriers

Security Considerations:

- Encrypted communication (varies by generation)
- SIM-based authentication (e.g., IMSI, Ki)
- Vulnerable to:
  - IMSI catchers (stingrays)
  - SS7 protocol exploits
  - Jamming and spoofing attacks

CHAPTER 11

Content Distribution Networks (CDNs)

A globally distributed system of servers and data centers designed to deliver web content, applications, and media to users more quickly, reliably, and securely.

CDNs improve speed, reliability, and security—but caching sensitive data improperly can lead to serious information leaks.

CHAPTER 11

CDNs improve speed, reliability, and security—but caching sensitive data improperly can lead to serious information leaks.

Content Distribution Networks (CDNs)

A globally distributed system of servers and data centers designed to deliver web content, applications, and media to users more quickly, reliably, and securely.

How CDNs Work:

1. When a user requests content (like a video, image, or webpage), the CDN routes the request to the closest edge server geographically.
2. The edge server delivers cached content or fetches it from the origin server if needed.
3. This minimizes latency, reduces bandwidth costs, and improves load times.

What CDNs Deliver:

- Static files (images, CSS, JS)
- Dynamic content (with caching strategies)
- Software updates
- Video streaming
- API acceleration

Benefits of CDNs:

- Faster performance for users worldwide
- DDoS mitigation and improved security (WAF, bot filtering)
- Reduced origin server load
- Global scalability and availability

Security Features:

- TLS/SSL encryption
- Web Application Firewalls (WAF)
- Rate limiting and bot mitigation
- Protection against DNS amplification and layer 7 DDoS attacks

CHAPTER 11

Intranet vs. Extranet

The difference isn't the tech—it's the trust boundary. An intranet is inside the castle walls; an extranet invites guests through the gate—with guards watching.

CHAPTER 11

Intranet vs. Extranet

The difference isn't the tech—it's the trust boundary. An intranet is inside the castle walls; an extranet invites guests through the gate—with guards watching.

Intranet

A private, internal network used within an organization to share information, tools, applications, and resources among employees.

- **Access**: Restricted to authorized users within the organization
- **Purpose**: Improves collaboration, communication, and workflow efficiency
- **Examples**: Internal websites, HR portals, document repositories, internal chat systems

CHAPTER 11

Intranet vs. Extranet

The difference isn't the tech—it's the trust boundary. An intranet is inside the castle walls; an extranet invites guests through the gate—with guards watching.

Intranet

A private, internal network used within an organization to share information, tools, applications, and resources among employees.

- **Access**: Restricted to authorized users within the organization
- **Purpose**: Improves collaboration, communication, and workflow efficiency
- **Examples**: Internal websites, HR portals, document repositories, internal chat systems

Extranet

An extension of an intranet that provides limited access to external parties, such as partners, vendors, or customers.

- **Access**: Controlled access for authorized outsiders
- **Purpose**: Enables secure collaboration with third parties
- **Examples**: Supplier portals, client dashboards, B2B extranets

Security Considerations:

- Intranet: Internal access controls, segmentation, endpoint protection
- Extranet: VPNs, firewalls, multi-factor authentication, and strict access policies

CHAPTER 11

Screened Subnet (DMZ) vs. Screened Host

Use a screened subnet when you care about layered defense. Use a screened host when you're on a budget—but harden the hell out of it.

CHAPTER 11

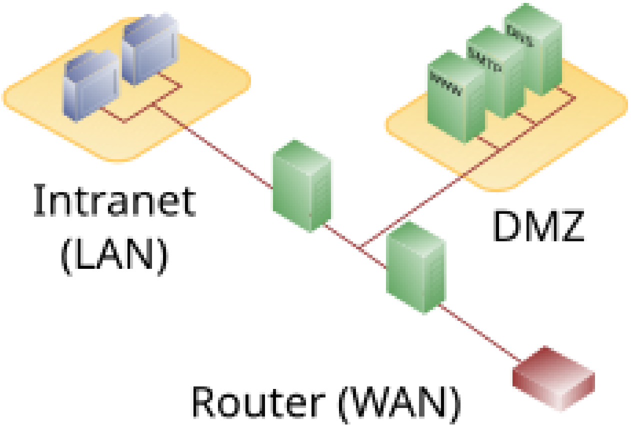
Use a screened subnet when you care about layered defense. Use a screened host when you're on a budget—but harden the hell out of it.

Screened Subnet (DMZ) vs. Screened Host

Screened Subnet (DMZ – Demilitarized Zone)

- A network segment isolated from both the internal network and the internet.
- Used to host public-facing services (like web servers, mail servers, DNS) in a way that limits access and exposure.
- Protected by two firewalls or a tri-homed firewall:
  - One between the internet and DMZ
  - One between the DMZ and internal network
- Minimizes risk to internal systems if a DMZ system is compromised.

Think of it as a "buffer zone" between your castle (internal network) and the outside world.



2025 CISSP MENTOR PROGRAM

CHAPTER 11

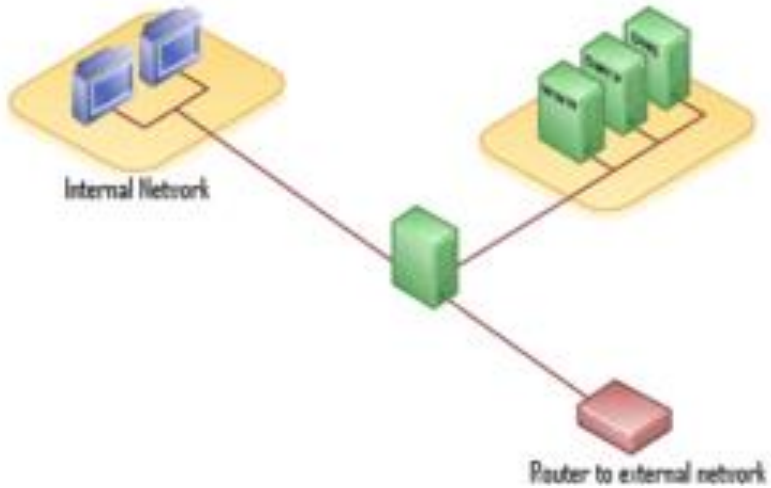
Screened Subnet (DMZ) vs. Screened Host

Screened Host Architecture

Use a screened subnet when you care about layered defense. Use a screened host when you're on a budget—but harden the hell out of it.

- A simpler architecture where a single firewall (or screening router) filters traffic and a bastion host (a hardened system) handles all communications between the external and internal networks.
- One layer of filtering, usually less secure than a DMZ.
- The bastion host is the key control point and must be very secure.
- Simpler and cheaper, but not as resilient to attacks as a DMZ.

Like having a guard at the gate who speaks for everyone inside.



2025 CISSP MENTOR PROGRAM

CHAPTER 11

Screened Subnet (DMZ) vs. Screened Host

Screened Host Architecture

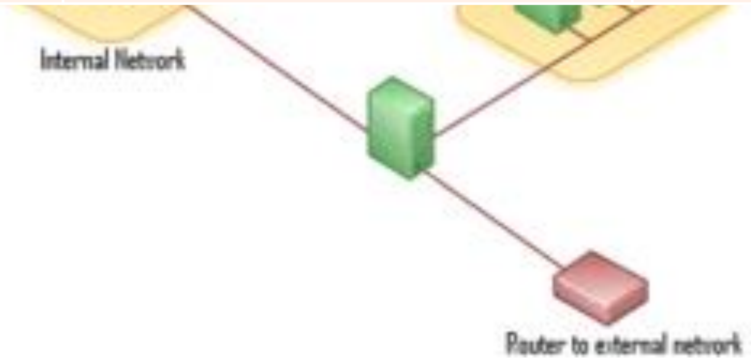
Use a screened subnet when you care about layered defense. Use a screened host when you're on a budget—but harden the hell out of it.

- A simpler architecture where a single firewall (or screening router) filters traffic and a bastion hos ernal net
- One
- The
- Sim

at the gate who inside.

Key Differences:

Feature	Screened Subnet (DMZ)	Screened Host
Layers of Defense	Multiple (2+ firewalls)	Single firewall/router
Internal Isolation	Stronger (via DMZ)	Weaker (host closer to LAN)
Complexity	Higher	Lower
Security Level	More secure	Less secure



FRSECURE

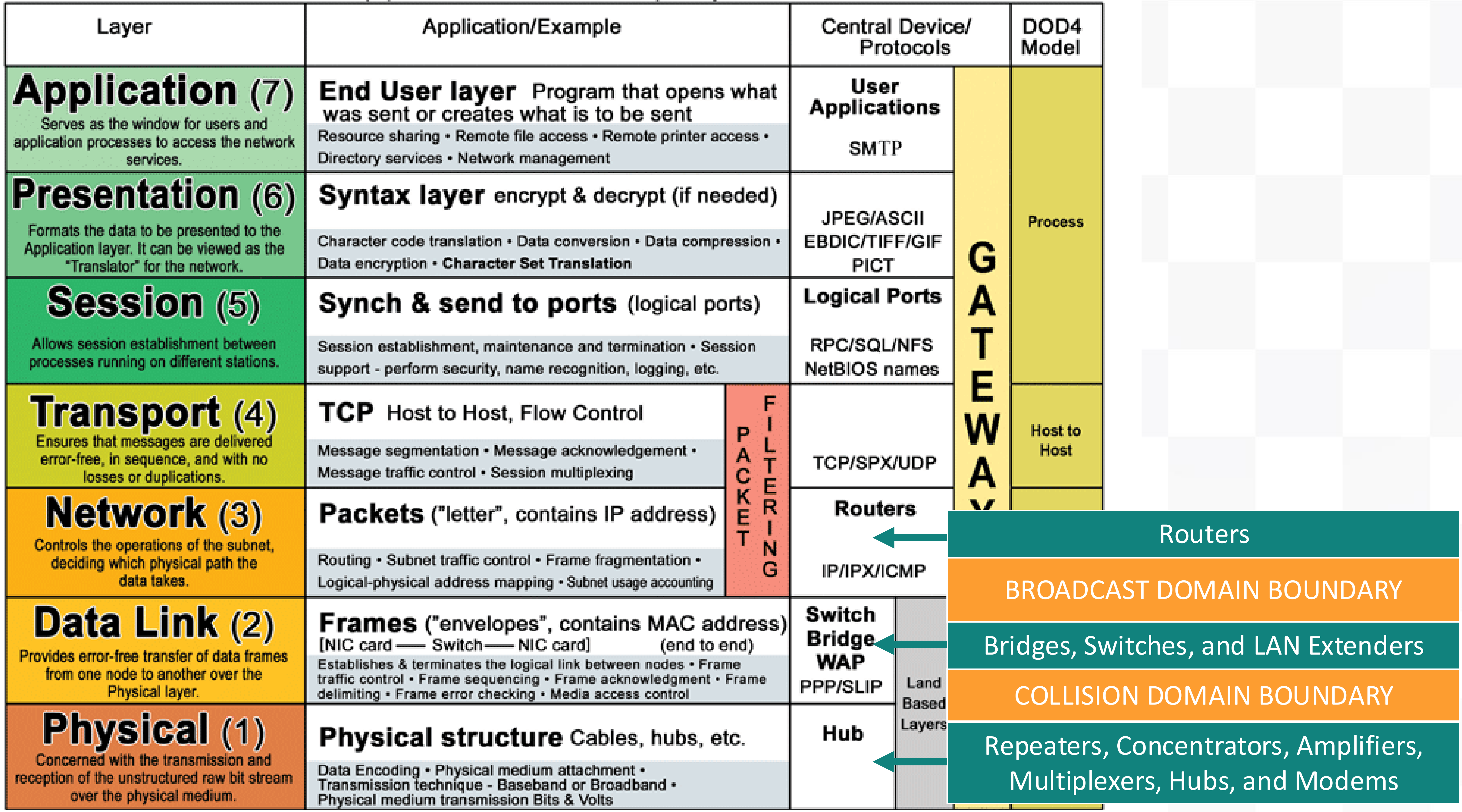
We’re almost done, I promise!

CHAPTER 11

Screened Subnet (DMZ) vs. Screened Host

Screened Host Architecture

- A simpler architecture where a single firewall (or screening router) filters traffic and a bastion host (a hardened system) handles all communications between the external and internal networks.
- One layer of filtering, usually less secure than a DMZ.
- The bastion host is the key control point and must be very secure.
- Simpler and cheaper, but not as resilient to attacks as a DMZ.



Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP		
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card —— Switch —— NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch** **Bridge** **WAP** PPP/SLIP	Land Based Layers	
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

Routers

BROADCAST DOMAIN BOUNDARY

Bridges, Switches, and LAN Extenders

COLLISION DOMAIN BOUNDARY

Repeaters, Concentrators, Amplifiers, Multiplexers, Hubs, and Modems

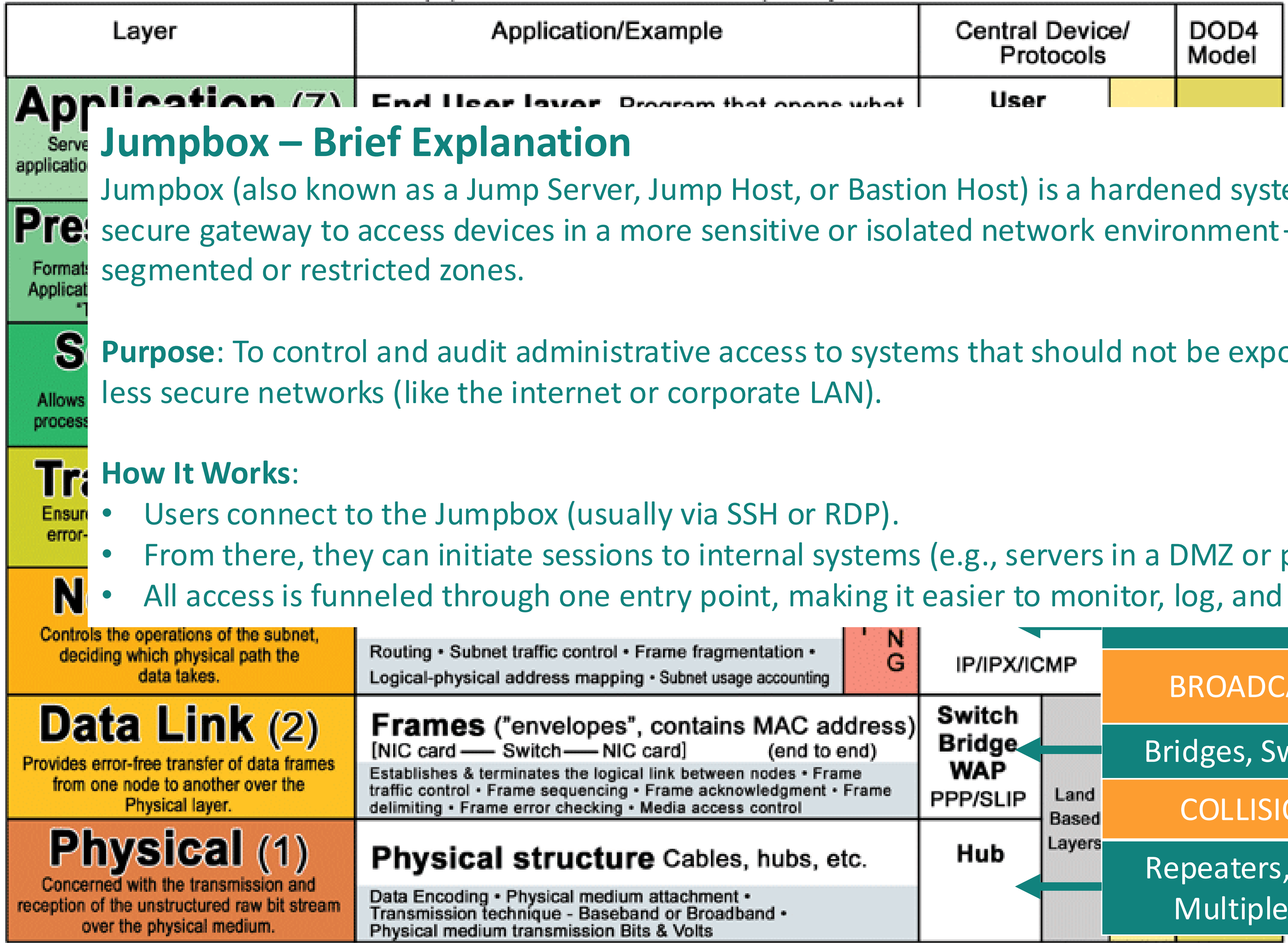
Jumpbox – Brief Explanation

Jumpbox (also known as a Jump Server, Jump Host, or Bastion Host) is a hardened system used as a secure gateway to access devices in a more sensitive or isolated network environment—especially in segmented or restricted zones.

Purpose: To control and audit administrative access to systems that should not be exposed directly to less secure networks (like the internet or corporate LAN).

How It Works:

- Users connect to the Jumpbox (usually via SSH or RDP).
- From there, they can initiate sessions to internal systems (e.g., servers in a DMZ or private subnet).
- All access is funneled through one entry point, making it easier to monitor, log, and secure.



Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serve… applicatio…	**End User layer** Program that opens what		**User**		
Pre… Format… Applicat… "T…					
S… Allows… process…					
Tr… Ensur… error-…					
N… Controls the operations of the subnet, deciding which physical path the data takes.	Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	N G	IP/IPX/ICMP		
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card —— Switch —— NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers	
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

Routers

BROADCAST DOMAIN BOUNDARY

Bridges, Switches, and LAN Extenders

COLLISION DOMAIN BOUNDARY

Repeaters, Concentrators, Amplifiers, Multiplexers, Hubs, and Modems

System on a Chip – Brief Explanation

An integrated circuit that combines all the essential components of a computer or electronic system onto a single chip.

What It Includes:

- CPU (central processing unit)
- GPU (graphics processing unit)
- Memory controllers
- I/O interfaces (USB, Wi-Fi, Bluetooth)
- Sometimes includes AI accelerators, DSPs, or secure enclaves

All tightly packed into a compact, power-efficient package.

Where It's Used:

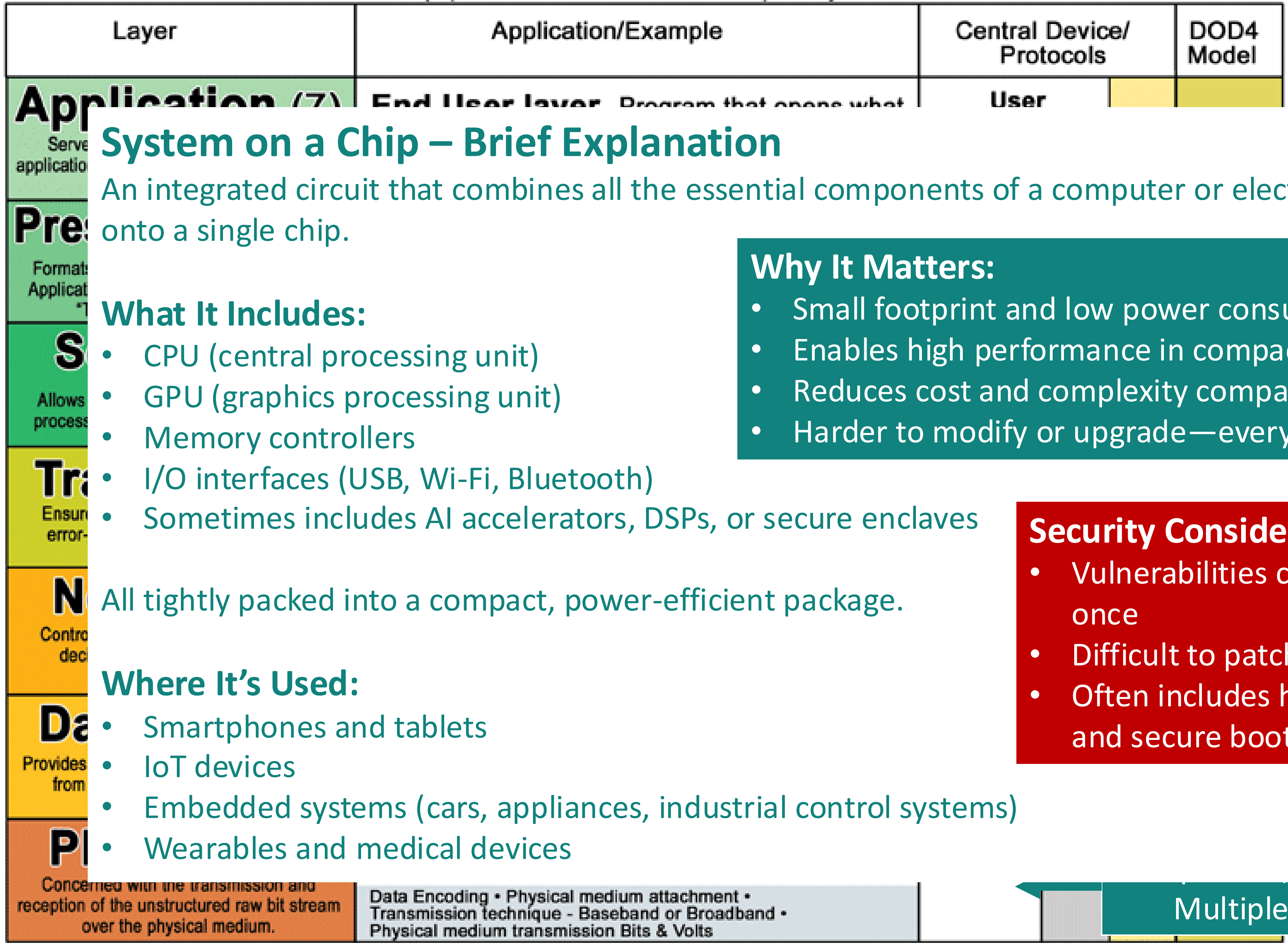
- Smartphones and tablets
- IoT devices
- Embedded systems (cars, appliances, industrial control systems)
- Wearables and medical devices

Why It Matters:

- Small footprint and low power consumption
- Enables high performance in compact form factors
- Reduces cost and complexity compared to multi-chip designs
- Harder to modify or upgrade—everything is baked in

Security Considerations:

- Vulnerabilities can affect all subsystems at once
- Difficult to patch or segment if compromised
- Often includes hardware-based encryption and secure boot features



Layer	Application/Example	Central Device/ Protocols	DOD4 Model
Application (7) Serve applicatio	End User layer Program that opens what	User	
Pres Format Applicat "1			
S Allows process			
Tra Ensur error-			
N Contro dec			
Da Provides from			
Pl Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		

NDARY

mplifiers, Multiplexers, Hubs, and Modems

CHAPTER 11

Secure Network Components

Network Access Control

NAC is like a bouncer at the network's front door—no clean credentials, no entry. And even if you're in, you're still being watched.

A security solution that enforces policies to control access to a network based on device identity, health, user credentials, or context.

CHAPTER 11

Secure Network Components

NAC is like a bouncer at the network's front door—no clean credentials, no entry. And even if you're in, you're still being watched.

Network Access Control (NAC)

A security solution that enforces policies to control access to a network based on device identity, health, user credentials, or context.

What NAC Does:

- Authenticates and authorizes users and devices before granting network access
- Assesses device posture (e.g., antivirus status, patch level, OS version)
- Allows, limits, or denies access based on compliance with defined policies
- Can quarantine or redirect non-compliant devices to remediation zones

CHAPTER 11

Secure Network Components

NAC is like a bouncer at the network's front door—no clean credentials, no entry. And even if you're in, you're still being watched.

Network Access Control (NAC)

A security solution that enforces policies to control access to a network based on device identity, health, user credentials, or context.

What NAC Does:

- Authenticates and authorizes users and devices before granting network access
- Assesses device posture (e.g., antivirus status, patch level, OS version)
- Allows, limits, or denies access based on compliance with defined policies
- Can quarantine or redirect non-compliant devices to remediation zones

Common NAC Capabilities:

- Pre-admission control – Checks a device before it joins the network
- Post-admission monitoring – Continues checking device behavior after access is granted
- Guest access management – Temporary and limited access for visitors
- Integration with identity providers, SIEMs, and EDRs for context-aware decisions

CHAPTER 11

Secure Network Components

Network Access Control (NAC)

NAC is like a bouncer at the network's front door—no clean credentials, no entry. And even if you're in, you're still being watched.

A security solution that enforces policies to control access to a network based on device identity, health, user credentials, or context.

What NAC Does:

- Authenticates and authorizes users and devices before granting network access
- g., antivirus status, patch level, OS version)
- ss based on compliance with defined policies
- on-compliant devices to remediation zones
- Pre-admission control
- Post-admission monit
- Guest access management – Temporary and limited access for visitors
- Integration with identity providers, SIEMs, and EDRs for context-aware decisions

Examples of NAC Solutions:

- Cisco Identity Services Engine (ISE)
- Aruba ClearPass
- FortiNAC
- Microsoft NPS (with 802.1X)

Benefits:

- Reduces risk of unauthorized or infected devices joining the network
- Enforces zero trust and least privilege models
- Helps with compliance (HIPAA, PCI-DSS, etc.)

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Secure Network Components

Network Access Control (NAC) - Agent-based NAC vs. Agentless NAC

Use agent-based NAC when you own the endpoints and need deep control.
Use agentless NAC when you need coverage across a messy, diverse network.

CHAPTER 11

Use agent-based NAC when you own the endpoints and need deep control.
Use agentless NAC when you need coverage across a messy, diverse network.

Secure Network Components

Network Access Control (NAC) - Agent-based NAC vs. Agentless NAC

Agent-Based NAC

- Requires software (agent) to be installed on each endpoint.
- The agent performs deep posture assessment:
  - Patch levels
  - Running services
  - Antivirus status
  - Firewall settings
  - OS version and configuration
- Often used in managed environments (corporate-issued devices).
- Can continuously monitor device health and enforce policy in real-time.

Pros:

- Granular control and visibility
- Better for ongoing policy enforcement
- Can work even when the device moves across network segments

Cons:

- Requires deployment and maintenance of agents
- May not be compatible with all device types (BYOD, IoT, etc.)
- Agents can introduce overhead or conflict with other software

Use agent-based NAC when you own the endpoints and need deep control.
Use agentless NAC when you need coverage across a messy, diverse network.

Secure Network Components

Network Access Control (NAC) - Agent-based NAC vs. Agentless NAC

Agentless NAC

- No software installation required on the endpoint.
- Uses network-based methods like:
  - SNMP
  - DHCP fingerprinting
  - Active/passive scanning
  - Directory services (e.g., AD)
  - Switch or firewall integrations
- Good for guest devices, BYOD, and IoT environments.

Pros:

- Quick to deploy
- No user involvement or endpoint change required
- Works with a wide range of devices, including unmanaged ones

Cons:

- Limited visibility into device posture
- Less effective for ongoing monitoring
- Can’t enforce some policies (e.g., antivirus, OS patch level)

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Secure Network Components

Use agent-based NAC when you own the endpoints and need deep control. Use agentless NAC when you need coverage across a messy, diverse network.

Network Access Control (NAC) - Agent-based NAC vs. Agentless NAC

Agentless NAC

- No software installation required on the endpoint

Feature	Agent-Based NAC	Agentless NAC
Software required	Yes	No
Visibility (device posture)	High	Limited
Suitable for BYOD/IoT	Often no	Yes
Deployment complexity	Higher	Lower
Policy enforcement depth	Deep & continuous	Shallow & snapshot

- Good for guest devices, BYOD, and IoT environments.

Pros:

ploy

olvement or endpoint

uired

a wide range of devices,

nmanaged ones

Cons:

- Limited visibility into device posture
- Less effective for ongoing monitoring
- Can’t enforce some policies (e.g., antivirus, OS patch level)

CHAPTER 11

Secure Network Components

Firewalls

Firewalls aren’t just walls—they’re filters, inspectors, and guards. Layer your defenses, and don’t trust a single gate to protect the whole kingdom.

CHAPTER 11

Firewalls aren’t just walls—they’re filters, inspectors, and guards. Layer your defenses, and don’t trust a single gate to protect the whole kingdom.

Secure Network Components

Firewalls

- A firewall is a network security device or software that monitors, filters, and controls incoming and outgoing network traffic based on predetermined security rules.
- At its core, a firewall’s job is to enforce what is allowed or denied, acting as a barrier between trusted and untrusted networks.

CHAPTER 11

Secure Network Components

Firewalls aren't just walls—they're filters, inspectors, and guards. Layer your defenses, and don't trust a single gate to protect the whole kingdom.

Firewalls

- A firewall is a network security device or software that monitors, filters, and controls incoming and outgoing network traffic based on predetermined security rules.
- At its core, a firewall's job is to enforce what is allowed or denied, acting as a barrier between trusted and untrusted networks.

1. **Static Packet-Filtering Firewalls (Layer 3)**
    - Operate at the Network Layer (OSI Layer 3)
    - Inspect IP headers and TCP/UDP ports
    - Filter packets based on simple rules: source/destination IP, protocol, and port number

Think of it like a bouncer who only checks ID and not behavior

Pros: Fast, low overhead

Cons: No awareness of connection state or application context

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Secure Network Components

Firewalls

Firewalls aren't just walls—they're filters, inspectors, and guards. Layer your defenses, and don't trust a single gate to protect the whole kingdom.

- A firewall is a network security device or software that monitors, filters, and controls incoming and outgoing network traffic based on predetermined security rules.
- At its core, a firewall's job is to enforce what is allowed or denied, acting as a barrier between trusted and untrusted networks.

2. **Stateful Inspection Firewalls (Layer 3–4)**
    - Maintain a state table to track active connections
    - Only allow packets that are part of a known valid session
    - Inspects headers and state information

A smarter bouncer who remembers who came in and what they're doing.

Pros: More secure than static filtering, blocks unsolicited packets

Cons: Still can't inspect the contents of application data

CHAPTER 11

Firewalls aren't just walls—they're filters, inspectors, and guards. Layer your defenses, and don't trust a single gate to protect the whole kingdom.

Secure Network Components

Firewalls

- A firewall is a network security device or software that monitors, filters, and controls incoming and outgoing network traffic based on predetermined security rules.
- At its core, a firewall's job is to enforce what is allowed or denied, acting as a barrier between trusted and untrusted networks.

3. **Circuit-Level Gateways (Layer 5 – Session Layer)**
    - Monitor TCP handshakes and sessions, but not the content of traffic
    - Often used in SOCKS proxies
    - Validate that sessions are legitimate before allowing data flow

Pros: Efficient for session control

Cons: No application layer inspection

Like a doorman who verifies you're in a valid conversation but doesn't care what you're saying.

CHAPTER 11

Firewalls aren't just walls—they're filters, inspectors, and guards. Layer your defenses, and don't trust a single gate to protect the whole kingdom.

Secure Network Components

Firewalls

- A firewall is a network security device or software that monitors, filters, and controls incoming and outgoing network traffic based on predetermined security rules.
- At its core, a firewall's job is to enforce what is allowed or denied, acting as a barrier between trusted and untrusted networks.

4. **Application-Level Gateways (Layer 7 – Proxy Firewalls)**
   - Inspect application data (HTTP, FTP, SMTP, etc.)
   - Often work as proxies, terminating and forwarding connection

Pros: Deep content inspection, can block malicious payloads

Cons: Slower, resource-intensive, protocol-specific

A guard who reads your messages before passing them on.

CHAPTER 11

Secure Network Components

Firewalls aren't just walls—they're filters, inspectors, and guards. Layer your defenses, and don't trust a single gate to protect the whole kingdom.

Firewalls

- A firewall is a network security device or software that monitors, filters, and controls incoming and outgoing network traffic based on predetermined security rules.
- At its core, a firewall's job is to enforce what is allowed or denied, acting as a barrier between trusted and untrusted networks.

5. **Next-Generation Firewalls (NGFWs)**
    - Combine stateful inspection, application-layer inspection, IDS/IPS, URL filtering, SSL decryption, and threat intelligence
    - Can identify users, applications, and behaviors, not just ports/IPs

Pros: High security with granular control

Cons: Expensive, complex configuration

Like a security team that knows your name, what app you're using, and whether you're acting sketchy.

CHAPTER 11

Firewalls aren’t just walls—they’re filters, inspectors, and guards. Layer your defenses, and don’t trust a single gate to protect the whole kingdom.

Secure Network Components

Firewalls

- A firewall is a network security device or software that monitors, filters, and controls incoming and outgoing network traffic based on predetermined security rules.
- At its core, a firewall’s job is to enforce what is allowed or denied, acting as a barrier between trusted and untrusted networks.

6. **Internal Segmentation Firewalls (ISFWs)**
   - Deployed inside the network to segment internal systems (east-west traffic)
   - Useful for limiting lateral movement in case of breach

Pros: Protects against internal threats

Cons: Adds complexity, may require re-architecting traffic flows

Walls within the castle to stop attackers from roaming freely once inside.

CHAPTER 11

Secure Network Components

Firewalls

Firewalls aren't just walls—they're filters, inspectors, and guards. Layer your defenses, and don't trust a single gate to protect the whole kingdom.

- A firewall is a network security device or software that monitors, filters, and controls incoming and outgoing network traffic based on predetermined security rules.
- At its core, a firewall's job is to enforce what is allowed or denied, acting as a barrier between trusted and untrusted networks.

7. **Proxy Servers**
   - Act as an intermediary between users and the internet
   - Can anonymize, cache, and filter web traffic
   - May be transparent or explicit

A translator and gatekeeper between your network and the outside world.

Pros: Hide internal systems, enforce policies, reduce bandwidth

Cons: Can become a bottleneck, not a full replacement for a firewall

URL filtering is like putting blinders on your network—users only see what they’re supposed to. But make sure you’re not flying blind yourself—log and review what’s being blocked.

CHAPTER 11

Secure Network Components

Content/URL Filter

A security control that monitors and restricts access to specific websites, URLs, or web content types based on predefined policies.

CHAPTER 11

Secure Network Components

Content/URL Filter

URL filtering is like putting blinders on your network—users only see what they're supposed to. But make sure you're not flying blind yourself—log and review what's being blocked.

A security control that monitors and restricts access to specific websites, URLs, or web content types based on predefined policies.

What It Does:

- Blocks or allows access to websites based on:
  - URL categories (e.g., gambling, adult content, social media)
  - Specific domain names or keywords
  - Malicious or phishing sites (often using threat intelligence feeds)
- Can operate at various levels:
  - Network-level (via firewall, proxy, or DNS filter)
  - Host-level (via endpoint security agent or browser extension)

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Secure Network Components

Content/URL Filter

URL filtering is like putting blinders on your network—users only see what they're supposed to. But make sure you're not flying blind yourself—log and review what's being blocked.

Why It Matters:

- Prevents accidental or intentional access to risky or inappropriate content
- Helps enforce corporate policies and productivity standards
- Reduces exposure to malware, phishing, and C2 infrastructure
- Assists with compliance (e.g., CIPA, HIPAA, PCI-DSS)

bsites, URLs, or web content

- URL categories (e.g., gambling, adult content, social media)
- Specific domain names or keywords

Types of Filtering

Filter Type	Description
URL Filtering	Blocks based on domain or URL pattern (e.g., badsite.com)
Keyword Filtering	Blocks pages with flagged words in the content or URL
Category Filtering	Uses threat intel to block entire categories (e.g., porn)
DNS Filtering	Blocks DNS resolution for malicious or unwanted domains

CHAPTER 11

Secure Network Components

Endpoint Security

If your firewall is the front door, your endpoint security is the deadbolt on every room inside. Don’t rely on just the perimeter—defend every endpoint.

The practice of protecting end-user devices—like laptops, desktops, smartphones, tablets, and servers—from cyber threats, unauthorized access, and data breaches

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Secure Network Components

Endpoint Security

If your firewall is the front door, your endpoint security is the deadbolt on every room inside. Don’t rely on just the perimeter—defend every endpoint.

The practice of protecting end-user devices—like laptops, desktops, smartphones, tablets, and servers—from cyber threats, unauthorized access, and data breaches

What Endpoint Security Includes:

- Antivirus/Antimalware
- Host-based firewalls
- Endpoint Detection & Response (EDR)
- Disk encryption (e.g., BitLocker, FileVault)
- Data Loss Prevention (DLP)
- Patch management
- Device control (e.g., blocking USBs)
- Zero Trust enforcement and MFA

Why It’s Important:

- Endpoints are where users interact with data
- They are frequent vectors for:
  - Phishing
  - Ransomware
  - Credential theft
- They leave the safety of the corporate network (e.g., remote work, travel)
- BYOD and IoT devices complicate visibility and control

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Secure Network Components

Endpoint Security

If your firewall is the front door, your endpoint security is the deadbolt on every room inside. Don’t rely on just the perimeter—defend every endpoint.

es—like laptops, desktops, smartphones, tablets, and
d access, and data breaches

Modern Endpoint Security Tools:

- EDR/XDR (like CrowdStrike, SentinelOne, Microsoft Defender) for behavior-based threat detection
- Mobile Device Management (MDM) and Unified Endpoint Management (UEM) for enforcing policies across devices

- Disk encryption (e.g., BitLocker, FileVault)
- Data Loss Prevention (DLP)
- Patch management
- Device control (e.g., blocking USBs)
- Zero Trust enforcement and MFA

Why It’s Important:

- Endpoints are where users interact with data
- They are frequent vectors for:
  - Phishing
  - Ransomware
  - Credential theft
- They leave the safety of the corporate network (e.g., remote work, travel)
- BYOD and IoT devices complicate visibility and control

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Cabling, Topology, and Transmission Media Technology

LANs vs. WANs

LANs are fast and local; WANs are broad and complex—and securing the link between them is where things often go wrong.

CHAPTER 11

Cabling, Topology, and Transmission Media Technology

LANs vs. WANs

LANs are fast and local; WANs are broad and complex—and securing the link between them is where things often go wrong.

Quick Comparison Table:

Feature	LAN	WAN
Area Covered	Small/local	Large/regional/global
Ownership	Organization-owned	ISP or telecom-managed
Speed	High	Varies (generally slower)
Cost	Lower	Higher
Examples	Home network, office LAN	Internet, corporate interlinks

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Understanding transmission media is foundational—security is pointless if the signal doesn't arrive correctly or securely. Choose your media with reliability and risk in mind.

Cabling, Topology, and Transmission Media Technology

Transmission Media

Refers to the physical or logical paths used to carry data between devices in a network.

CHAPTER 11

Cabling, Topology, and Transmission Media Technology

Transmission Media

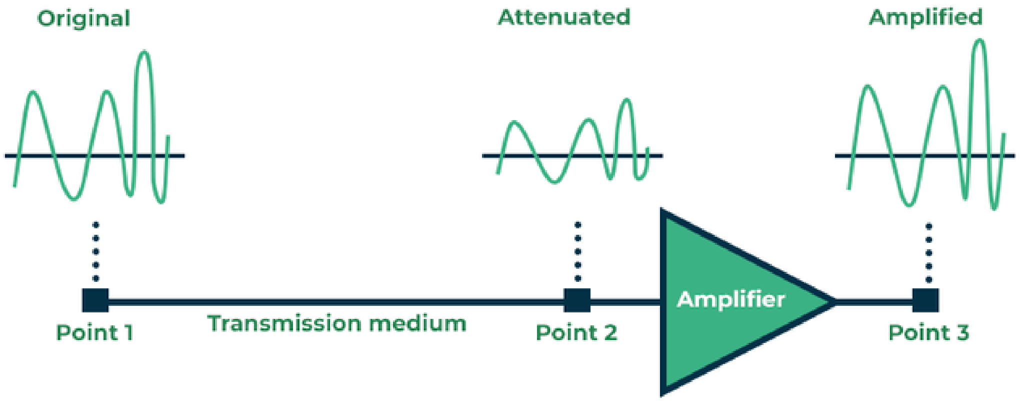
Understanding transmission media is foundational—security is pointless if the signal doesn't arrive correctly or securely. Choose your media with reliability and risk in mind.

Key Transmission Concepts to Know:

Attenuation

- Definition: The weakening of signal strength as it travels through a medium.
- Impact: Longer distances = weaker signals.
- Mitigation: Use repeaters, amplifiers, or fiber optics.

Like yelling across a canyon—eventually, your voice fades.



CHAPTER 11

Cabling, Topology, and Transmission Media Technology

Transmission Media

Understanding transmission media is foundational—security is pointless if the signal doesn't arrive correctly or securely. Choose your media with reliability and risk in mind.

Key Transmission Concepts to Know:

Attenuation

Like yelling across a canyon—eventually, your voice fades.

- Definition: The weakening of signal strength as it travels through a medium.
- Impact: Longer distances = weaker signals.
- Mitigation: Use repeaters, amplifiers, or fiber optics.

Interference

- Definition: Disruption caused by external signals (like electrical devices, EMI, RFI).
- Impact: Corrupted or lost data.
- Mitigation: Shielded cables, proper grounding, and frequency separation

Think of someone using a hairdryer while you're on a call.

CHAPTER 11

Cabling, Topology, and Transmission Media Technology

Transmission Media

Understanding transmission media is foundational—security is pointless if the signal doesn't arrive correctly or securely. Choose your media with reliability and risk in mind.

Key Transmission Concepts to Know:

Noise = static in your data conversation.

Noise

- Definition: Unwanted signals that interfere with data transmission.
- Types: Crosstalk, white noise, impulse noise.
- Mitigation: Error detection/correction, better cables, shielding.

CHAPTER 11

Understanding transmission media is foundational—security is pointless if the signal doesn't arrive correctly or securely. Choose your media with reliability and risk in mind.

Cabling, Topology, and Transmission Media Technology

Transmission Media

Key Transmission Concepts to Know:

Noise = static in your data conversation.

Noise

- Definition: Unwanted signals that interfere with data transmission.
- Types: Crosstalk, white noise, impulse noise.
- Mitigation: Error detection/correction, better cables, shielding.

Jitter

- Definition: The variation in packet arrival times.
- Impact: Causes choppy voice/video in real-time apps.
- Mitigation: Buffering, QoS settings, stable connections.

Like a stuttering video stream during a Zoom call.

CHAPTER 11

Cabling, Topology, and Transmission Media Technology

Transmission Media

Understanding transmission media is foundational—security is pointless if the signal doesn't arrive correctly or securely. Choose your media with reliability and risk in mind.

Key Transmission Concepts to Know:

Bandwidth

Think of it as the width of a highway—the wider it is, the more cars (data) can travel.

- Definition: The maximum rate of data transfer a medium can support, typically measured in Mbps or Gbps.
- Higher bandwidth = more data, faster speeds.

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Cabling, Topology, and Transmission Media Technology

Transmission Media

Understanding transmission media is foundational—security is pointless if the signal doesn't arrive correctly or securely. Choose your media with reliability and risk in mind.

Key Transmission Concepts to Know:

Bandwidth

Think of it as the width of a highway—the wider it is, the more cars (data) can travel.

- Definition: The maximum rate of data transfer a medium can support, typically measured in Mbps or Gbps.
- Higher bandwidth = more data, faster speeds.

Propagation Delay / Latency

- Definition: The time it takes for a signal to travel from source to destination.
- Measured in milliseconds (ms).
- Higher over long distances or slower mediums (like satellites).

Like how long it takes for your voice to reach someone across the country.

CHAPTER 11

Coax was once the king of networking, but it’s now mostly a legacy or niche medium—still solid for short, shielded runs or specialized applications.

Cabling, Topology, and Transmission Media Technology

Transmission Media

Coaxial Cable

A coaxial cable (or coax cable) is a type of guided transmission medium used to carry high-frequency electrical signals with minimal interference and signal loss.

CHAPTER 11

Coax was once the king of networking, but it's now mostly a legacy or niche medium—still solid for short, shielded runs or specialized applications.

Cabling, Topology, and Transmission Media Technology

Transmission Media

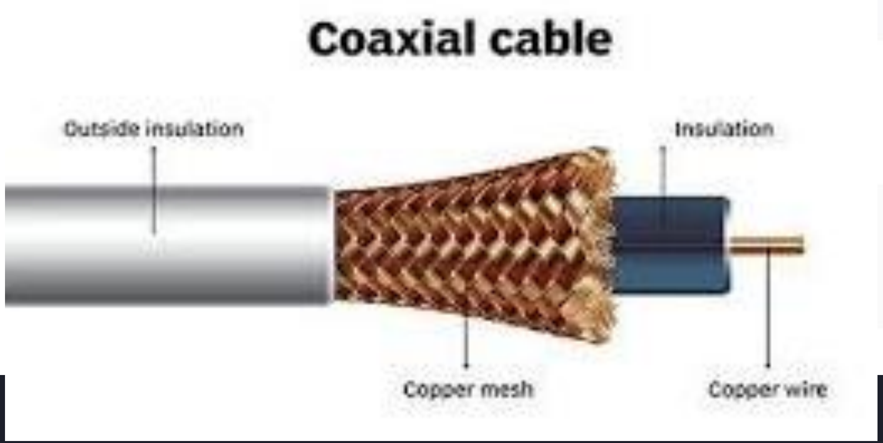
Coaxial Cable

A coaxial cable (or coax cable) is a type of guided transmission medium used to carry high-frequency electrical signals with minimal interference and signal loss.

Coaxial cable consists of four layers:

- Inner conductor – Carries the signal (usually copper)
- Insulating layer – Separates the core from shielding
- Metal shield (braid/foil) – Blocks electromagnetic interference (EMI)
- Outer jacket – Protects the cable physically

The term "coaxial" refers to the shared axis of the conductor and shield.



CHAPTER 11

Cabling, Topology, and Transmission Media Technology

Transmission Media

Coax was once the king of networking, but it's now mostly a legacy or niche medium—still solid for short, shielded runs or specialized applications.

Coaxial Cable

A coaxial cable (or coax cable) i rry high-frequency electrical signals with

Common Uses:

- Cable TV and internet (e.g., DOCSIS)
- Radio transmitters
- CCTV security cameras
- Legacy Ethernet networks (10Base2, 10Base5 – now mostly obsolete)

Pros:

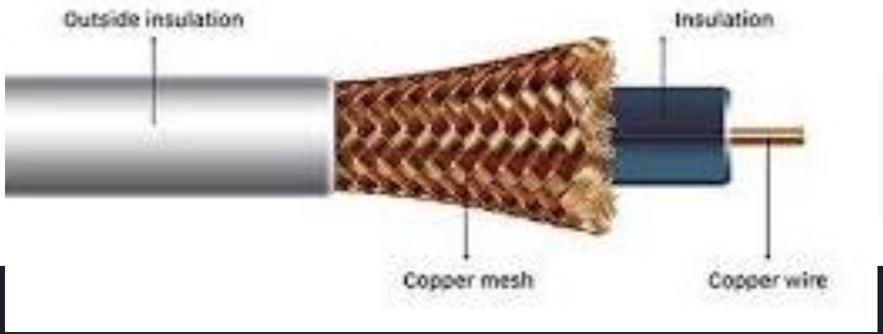
- Better shielding than twisted pair cables
- Higher bandwidth capacity (compared to unshielded alternatives)
- Resistant to EMI and external noise

nal (usually copper)

to the shared axis of the conductor and shield.

Cons:

- Thicker and less flexible than twisted pair
- More expensive and harder to install
- Lower bandwidth and distance capacity than fiber optics



CHAPTER 11

Baseband is for digital simplicity, perfect for local networks. Broadband is built for scale, ideal when you need to cram more signals into one pipe.

Cabling, Topology, and Transmission Media Technology

Transmission Media

Baseband vs. Broadband Cabling

Both baseband and broadband describe methods of transmitting signals over cabling, but they do so in very different ways—especially in how they allocate bandwidth and handle multiple signals.

CHAPTER 11

Cabling, Topology, and Transmission Media Technology

Baseband is for digital simplicity, perfect for local networks. Broadband is built for scale, ideal when you need to cram more signals into one pipe.

Transmission Media

Baseband vs. Broadband Cabling

Both baseband and broadband describe methods of transmitting signals over cabling, but they do so in very different ways—especially in how they allocate bandwidth and handle multiple signals.

Baseband Transmission

- Definition: Transmits a single signal over the entire bandwidth of the cable at one time.
- Uses digital signals (binary 1s and 0s).
- Common in LANs, especially with Ethernet (e.g., 10Base-T).

Like a one-lane road: only one car (signal) moves at a time.

Pros:

- Simple, cost-effective
- Low signal interference
- High performance over short distances

Cons:

- One channel at a time—no simultaneous transmissions
- Not suitable for long-distance or multiple service types

CHAPTER 11

Baseband is for digital simplicity, perfect for local networks. Broadband is built for scale, ideal when you need to cram more signals into one pipe.

Cabling, Topology, and Transmission Media Technology

Transmission Media

Baseband vs. Broadband Cabling

Both baseband and broadband describe methods of transmitting signals over cabling, but they do so in very different ways—especially in how they allocate bandwidth and handle multiple signals.

Broadband Transmission

- Definition: Divides the cable into multiple frequency channels, allowing simultaneous transmission of multiple signals.
- Uses analog signals, often modulated into different frequency ranges.
- Common in cable TV, Internet via DOCSIS, and some metropolitan networks

Pros:

- Can transmit multiple data streams at once
- Supports long-distance and multi-service environments

Like a highway with many lanes—multiple cars (signals) traveling side by side

Cons:

- More complex and expensive
- Requires modulation/demodulation (e.g., via modem)

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Cabling, Topology, and Transmission Media Technology

Transmission Media

Twisted-pair cabling is the workhorse of local networks—simple, cheap, and everywhere. But know your categories—Cat 5e won’t cut it for high-speed backbones.

Twisted-Pair Cable

- One of the most common types of network cabling, especially for LANs and telephone systems.

CHAPTER 11

Twisted-pair cabling is the workhorse of local networks—simple, cheap, and everywhere. But know your categories—Cat 5e won't cut it for high-speed backbones.

Cabling, Topology, and Transmission Media Technology

Transmission Media

Twisted-Pair Cable

- One of the most common types of network cabling, especially for LANs and telephone systems.
- Consists of pairs of insulated copper wires twisted together to reduce electromagnetic interference (EMI) and crosstalk.
- Each cable contains two wires twisted into a pair.
- Multiple pairs (usually 4) are bundled in a single cable.
- The twisting helps cancel out noise from external sources and neighboring pairs.

Types of Twisted-Pair Cable:

Type	Shielding	Use Case
UTP (Unshielded Twisted Pair)	No shielding	Common in Ethernet LANs (Cat 5e, Cat 6)
STP (Shielded Twisted Pair)	Individual or overall shielding	Better EMI protection, used in industrial or noisy environments

2025 CISSP MENTOR PROGRAM

CHAPTER 11

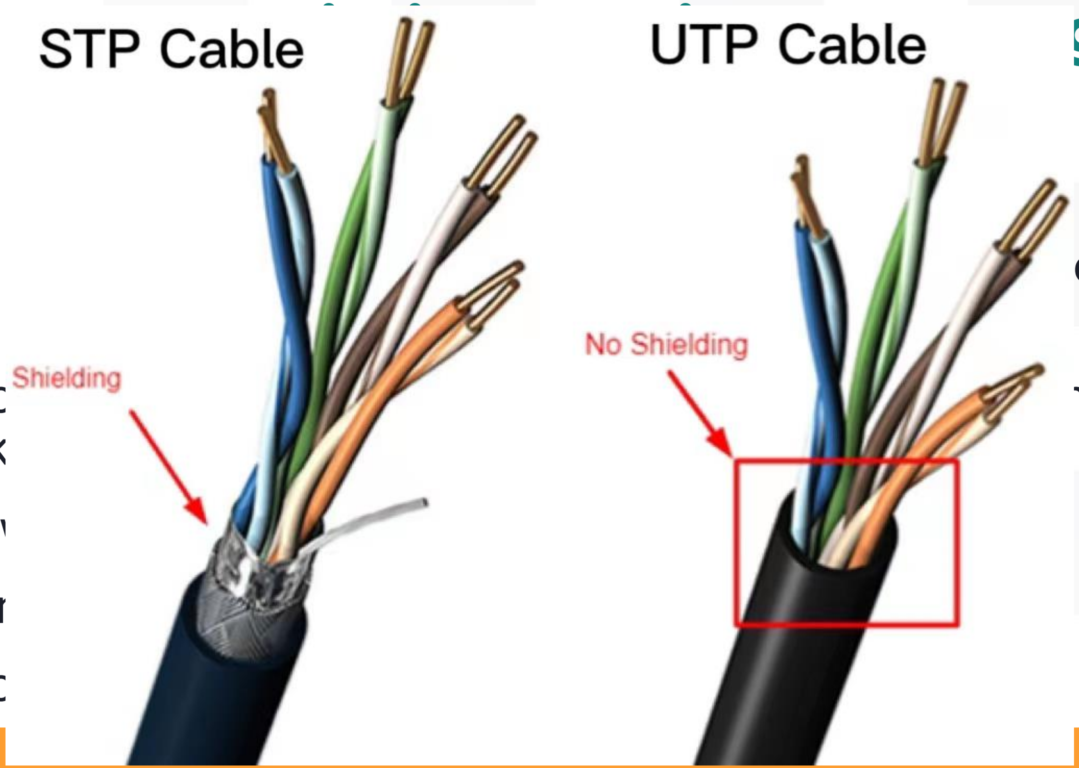
Cabling, Topology, an gy

Twisted-pair cabling is the workhorse of local networks—simple, cheap, and everywhere. But know your categories—Cat 5e won't cut it for high-speed backbones.

Transmission Media

Twisted-Pair Cable

- One of the most common types one systems.
- Consists of pairs of insulated cc netic interference (EMI) and crosstalk
- Each cable contains two wires t
- Multiple pairs (usually 4) are bur
- The twisting helps cancel out nc



Types of Twisted-Pair Cable:

Type	Shielding	Use Case
UTP (Unshielded Twisted Pair)	No shielding	Common in Ethernet LANs (Cat 5e, Cat 6)
STP (Shielded Twisted Pair)	Individual or overall shielding	Better EMI protection, used in industrial or noisy environments

Cat 5e is still the LAN standard, but if you're planning for the future or deploying backbone links, go Cat 6a or higher. Cat 8 is overkill for most environments unless you're building a data center.

CHAPTER 11

Cabling, Topology, and Transmission Media Technology

Transmission Media

Unshielded Twisted-Pair (UTP) Cable Comparison Table

Category	Max Throughput	Max Frequency	Use Case / Notes
Cat 1	<1 Mbps	N/A	Voice only (analog phones); obsolete
Cat 2	4 Mbps	1 MHz	Old Token Ring networks; obsolete
Cat 3	10 Mbps	16 MHz	Early Ethernet (10Base-T); rarely used today
Cat 4	16 Mbps	20 MHz	Token Ring; outdated
Cat 5	100 Mbps	100 MHz	100Base-TX Ethernet; obsolete
Cat 5e	1 Gbps	100 MHz	Enhanced Cat 5; standard for modern Ethernet
Cat 6	1 Gbps (10 Gbps <55m)	250 MHz	Better shielding; good for short 10G links
Cat 6a	10 Gbps	500 MHz	Improved Cat 6; suitable for 10G up to 100m
Cat 7	10 Gbps	600 MHz	Shielded; less common, proprietary connectors
Cat 8	25–40 Gbps (≤30m)	2000 MHz	Data centers; very short, high-speed runs

Know the 5-4-3 rule as a historical reference. Today's Ethernet networks are switched, not shared, so collision domains are gone — but the exam might still ask.

The 5-4-3 Rule for Ethernet – Brief Explanation

The 5-4-3 rule is a design guideline from the early days of Ethernet networking, specifically for 10Base5 and 10Base2 bus topology networks using coaxial cable and repeaters.

The Rule:

In a collision domain, you can have:

- **5** network segments
- Connected by **4** repeaters
- With only **3** segments populated (i.e., with devices attached)

The other 2 segments must be link-only (used just to connect repeaters).

Why the Rule Exists:

It was designed to ensure signal timing and collision detection worked correctly in CSMA/CD (Carrier Sense Multiple Access with Collision Detection) networks. If signals took too long to travel across the cable, devices wouldn't detect collisions properly, breaking Ethernet's core logic.

Is It Still Relevant?

Nope — not for modern switched Ethernet networks. This rule applied to shared Ethernet with hubs, coaxial cable, and repeaters, which are now obsolete. Switches and full-duplex Ethernet made the rule unnecessary.

CHAPTER 11

Cabling, Topology, and Transmission Media Technology

Transmission Media

Fiber is the gold standard for high-speed, long-range communication. Copper is cheap and easy—fiber is fast and future-proof.

Fiber-Optic Cables

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Cabling, Topology, and Transmission Media Technology

Fiber is the gold standard for high-speed, long-range communication. Copper is cheap and easy—fiber is fast and future-proof.

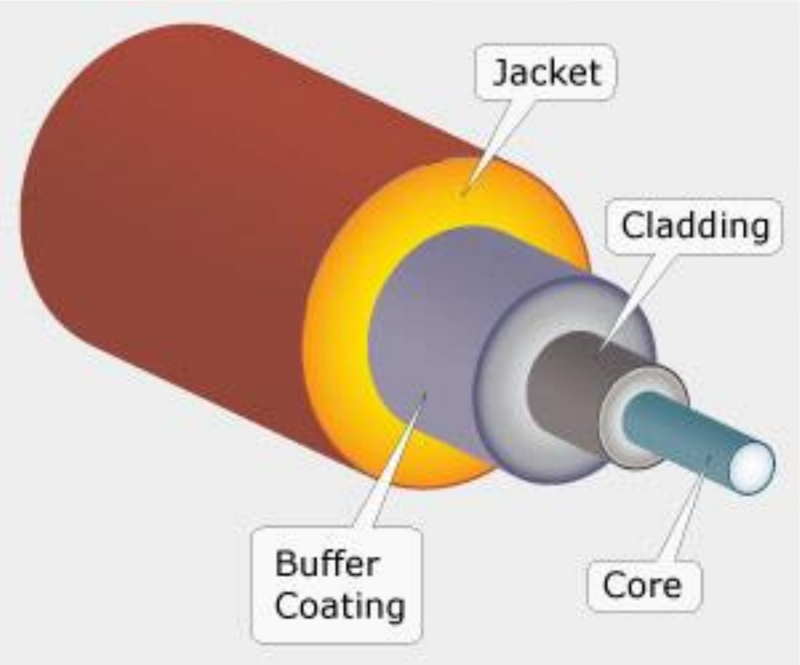
Transmission Media

Fiber-Optic Cables

- Transmit data using light signals rather than electrical ones.
- High bandwidth, long-distance, and interference-resistant

How It Works:

- Data is transmitted as pulses of light, usually from LI
- Light travels through a core made of glass or plastic.
- A cladding layer reflects the light inward, keeping it t internal reflection.



Core Components:

- Core: Carries the light signal.
- Cladding: Reflects light back into the core.
- Buffer Coating: Protects the fiber from moisture and
- Outer Jacket: Provides physical protection.

CHAPTER 11

Cabling, Topology, and Transmission Media Technology

Fiber is the gold standard for high-speed, long-range communication. Copper is cheap and easy—fiber is fast and future-proof.

Transmission Media

Fiber-Optic Cables

Types of Fiber:

Type	Description	Use Case
Single-Mode (SMF)	Very thin core; carries one light signal over long distances	Long-haul, telco, WAN links
Multi-Mode (MMF)	Thicker core; multiple light paths; shorter distances	LANs, data centers, shorter runs

Advantages:

- Immune to EMI/RFI (electromagnetic/radio interference)
- Extremely high bandwidth
- Long-distance capability (many kilometers)
- More secure (difficult to tap undetected)

Disadvantages:

- More expensive than copper
- Fragile and harder to install
- Requires specialized connectors and tools

CHAPTER 11

Cabling, Topology, and Transmission Media Technology

Coax is aging, twisted-pair is everywhere, and fiber is the future—use the right medium for the right mission.

Cable Type Comparison Table

Feature	Coaxial Cable	Twisted-Pair Cable	Fiber-Optic Cable
Transmission Type	Electrical signals	Electrical signals	Light signals
Speed/Bandwidth	Medium (up to ~1 Gbps with DOCSIS 3.1)	Varies: up to 10–40 Gbps (Cat 6a–8)	Very high (100 Gbps+ possible)
Distance	Medium (~500m max)	Short (up to 100m typical)	Long (tens of km without repeaters)
Interference Resistance	Good (due to shielding)	Fair (STP > UTP)	Excellent (immune to EMI/RFI)
Security	Moderate	Moderate	High (difficult to tap without detection)
Cost	Moderate	Low (Cat 5e, Cat 6 are inexpensive)	High (but dropping)
Flexibility	Less flexible	Very flexible	Least flexible (glass core is fragile)
Use Cases	Cable TV, broadband, CCTV	LANs, phones, Ethernet	Backbone networks, data centers, WANs
Installation	Moderate complexity	Easy	Complex (requires specialized tools)
Connector Types	BNC, F-type	RJ-45, GG45	SC, LC, ST, MTP, etc.

CHAPTER 11

Star topology dominates modern networks (especially Ethernet), but mesh rules in high-availability environments. Know ring and bus as legacy designs—and how their weaknesses shaped today's networks.

Cabling, Topology, and Transmission Media Technology

Network Topology

Refers to the physical or logical layout of how devices (nodes) are connected in a network. It impacts performance, fault tolerance, cost, and scalability.

CHAPTER 11

Star topology dominates modern networks (especially Ethernet), but mesh rules in high-availability environments. Know ring and bus as legacy designs—and how their weaknesses shaped today's networks.

Cabling, Topology, and Transmission Media Technology

Network Topology – Ring Topology

- Devices are connected in a circular loop; each device connects to two others.
- Data travels in one direction (or both, in dual-ring).
- Token passing is often used to avoid collisions.
- Predictable data flow
- A single break can disrupt the entire network unless dual-ring or with redundancy.

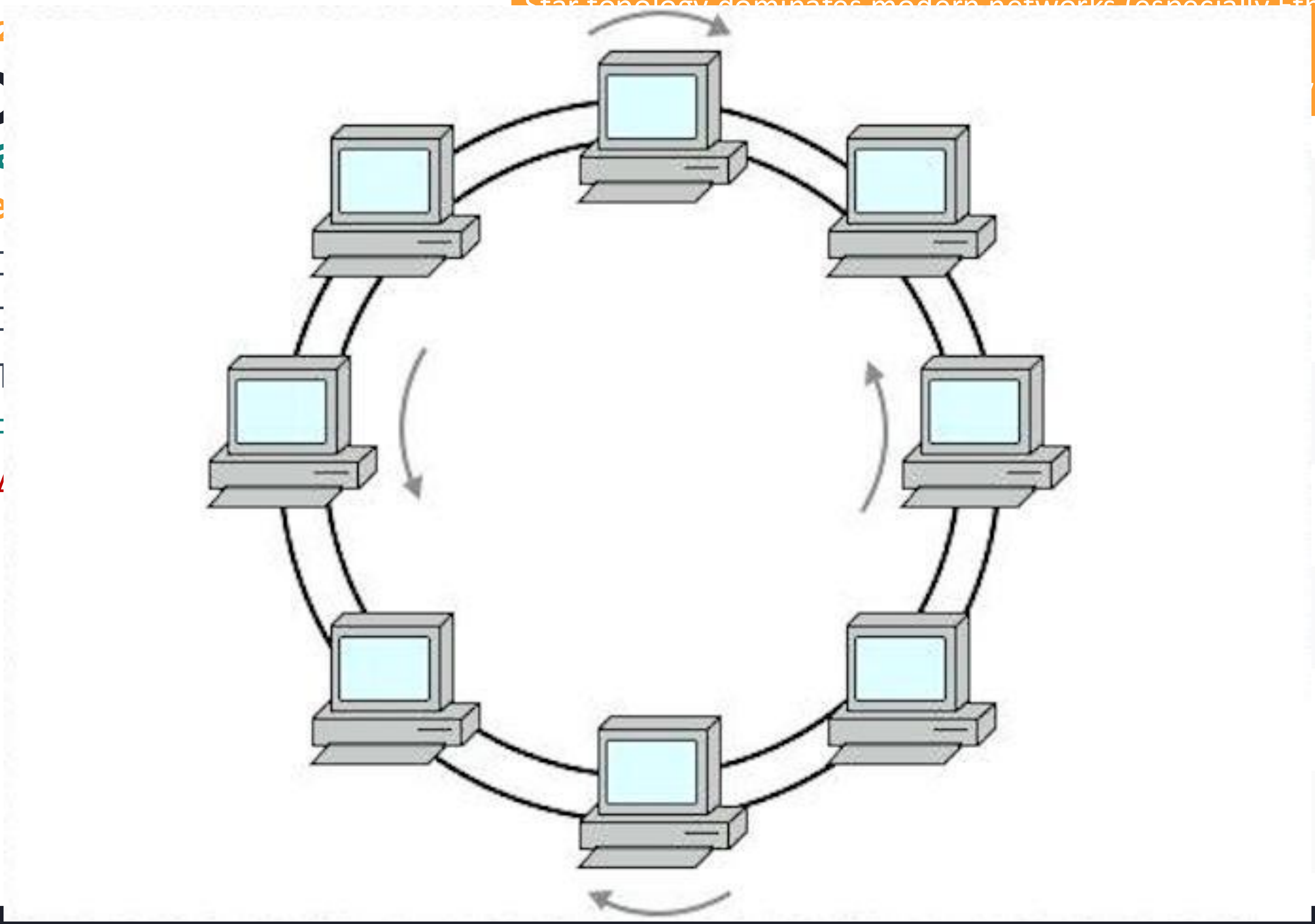
202

C

Ca

Ne

- [
- [
- T
- F
- A



Star topology dominates modern networks (especially Ethernet), but

nd bus as

’s networks.

Star topology dominates modern networks (especially Ethernet), but mesh rules in high-availability environments. Know ring and bus as legacy designs—and how their weaknesses shaped today’s networks.

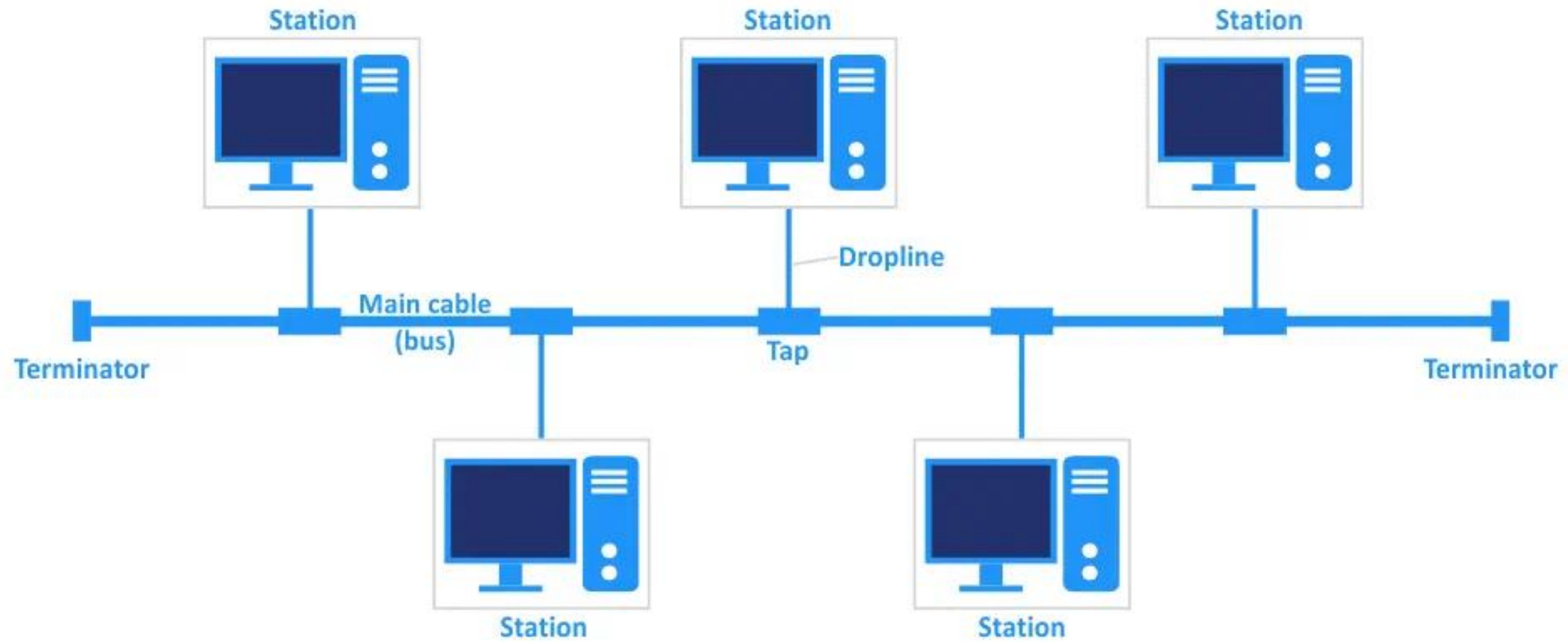
Cabling, Topology, and Transmission Media Technology

Network Topology – Bus Topology

- All devices share a single central cable (the bus).
- Terminators are placed at both ends.
- Devices communicate via the bus, taking turns.
- Easy to set up and cheap
- Only one device can transmit at a time; a cable fault can bring the whole thing down.

Star topology dominates modern networks (especially Ethernet), but mesh rules in high-availability environments. Know ring and bus as

Bus Topology



CHAPTER 11

Star topology dominates modern networks (especially Ethernet), but mesh rules in high-availability environments. Know ring and bus as legacy designs—and how their weaknesses shaped today's networks.

Cabling, Topology, and Transmission Media Technology

Network Topology – Star Topology

- All devices connect to a central hub or switch.
- Each device has a dedicated cable to the center.
- Failure of one device doesn't affect others
- Easy to manage and scale
- If the central hub fails, everything goes down.

2025 CISSP MENTOR PROGRAM

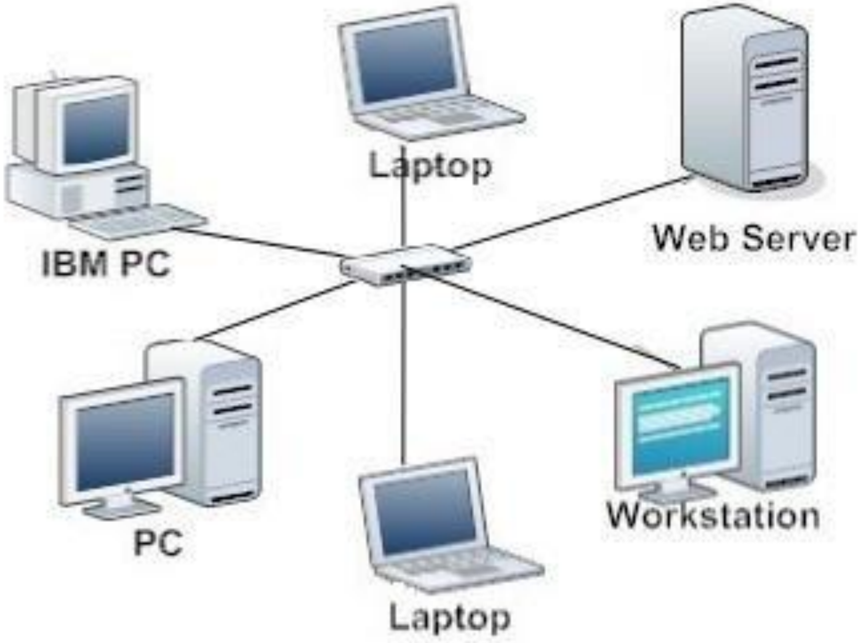
CHAPTER 11

Star topology dominates modern networks (especially Ethernet), but mesh rules in high-availability environments. Know ring and bus as legacy designs—and how their weaknesses shaped today’s networks.

Cabling, Topology, and Transmission Media Technology

Network Top

- All devices c
- Each device
- Failure of or
- Easy to mar
- If the centra



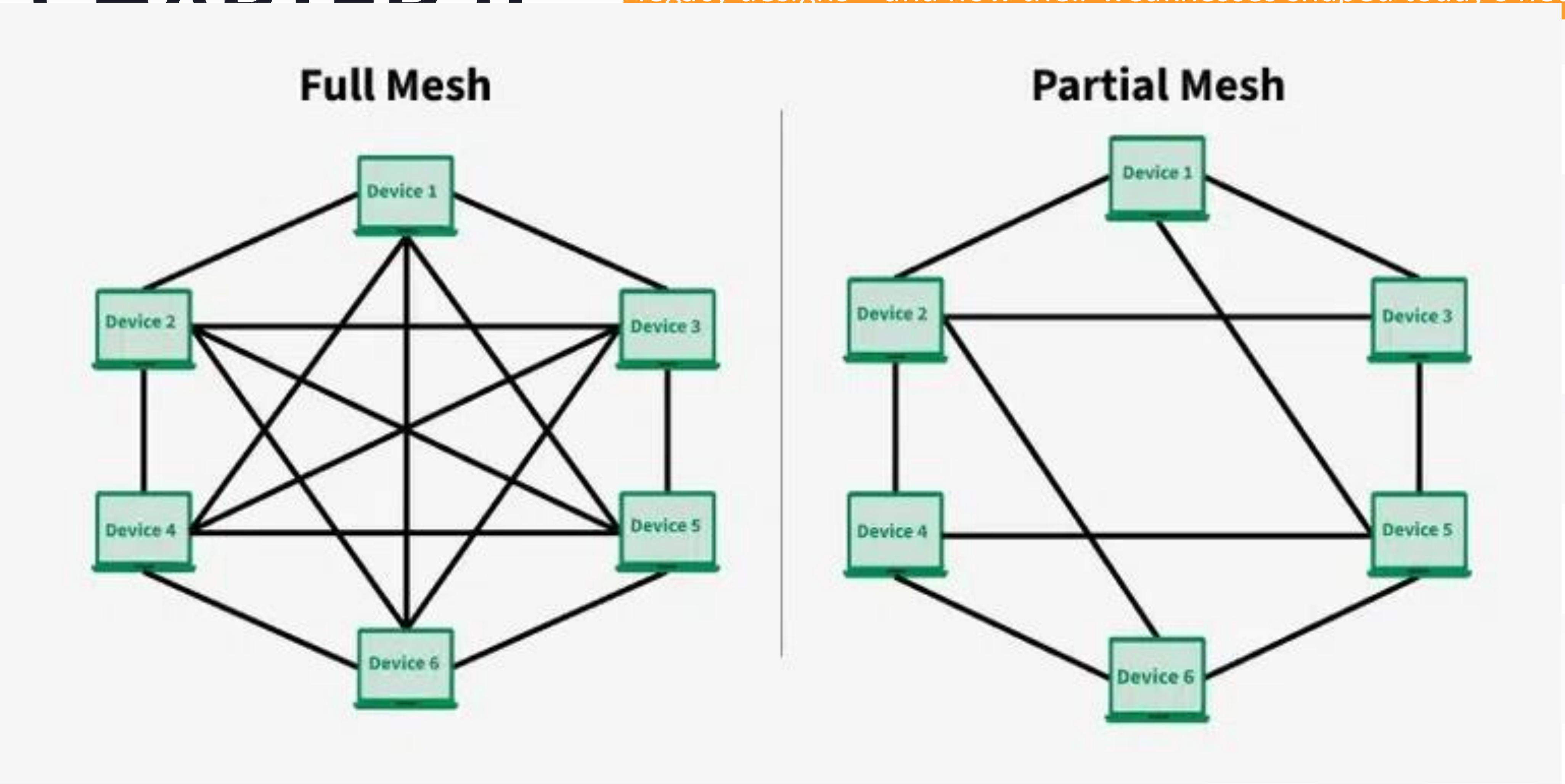
Star topology dominates modern networks (especially Ethernet), but mesh rules in high-availability environments. Know ring and bus as legacy designs—and how their weaknesses shaped today's networks.

Cabling, Topology, and Transmission Media Technology

Network Topology – Mesh Topology

- Every device connects to every other device (full mesh), or to some (partial mesh).
- Provides high redundancy and fault tolerance.
- Highly reliable and resilient
- Expensive and complex to cable and manage

Star topology dominates modern networks (especially Ethernet), but mesh rules in high-availability environments. Know ring and bus as legacy designs—and how their weaknesses shaped today’s networks.



CHAPTER 11

Ethernet is more than a cable—it's a protocol suite, a switching method, and a power delivery system. It's the foundation of modern LANs and continues to evolve with higher speeds and broader capabilities.

Cabling, Topology, and Transmission Media Technology

Ethernet

- The most widely used LAN (Local Area Network) technology in the world.

CHAPTER 11

Ethernet is more than a cable—it's a protocol suite, a switching method, and a power delivery system. It's the foundation of modern LANs and continues to evolve with higher speeds and broader capabilities.

Cabling, Topology, and Transmission Media Technology

Ethernet

- The most widely used LAN (Local Area Network) technology in the world.
- Defines how devices communicate over a physical medium using frames and follows standards from the IEEE 802.3 family.

Key Features of Ethernet:

- Frame-based communication using MAC addresses
- Uses CSMA/CD (Carrier Sense Multiple Access with Collision Detection) in older half-duplex systems
- Operates at Layer 1 (Physical) and Layer 2 (Data Link) of the OSI Model
- Can run over twisted-pair, fiber-optic, or coaxial media
- Modern Ethernet is full-duplex and switched, eliminating collisions

2025 CISSP MENTOR PROGRAM

CHAPTER 11

Ethernet is more than a cable—it's a protocol suite, a switching method, and a power delivery system. It's the foundation of modern LANs and continues to evolve with higher speeds and broader capabilities.

Cabling, Topology, and Transmission Media Technology

Ethernet (Common Sub-Technologies)

Standard	Name	Speed	Media	Notes
10Base-T	Ethernet	10 Mbps	Twisted-pair (Cat 3)	Obsolete; early standard
100Base-TX	Fast Ethernet	100 Mbps	Twisted-pair (Cat 5)	Still found in older infrastructure
1000Base-T	Gigabit Ethernet	1 Gbps	Twisted-pair (Cat 5e+)	Most common standard today
1000Base-LX/SX	Gigabit Ethernet	1 Gbps	Fiber	Long/short distance links
10GBase-T	10-Gig Ethernet	10 Gbps	Twisted-pair (Cat 6a+)	Data centers and high-speed LANs
10GBase-SR/LR	10-Gig Ethernet	10 Gbps	Fiber	Short/long-range fiber networks
40G/100G/400G	High-speed Ethernet	40–400 Gbps	Fiber (QSFP, etc.)	Used in enterprise backbones, data centers
Power over Ethernet (PoE)	IEEE 802.3af/at/bt	N/A	Twisted-pair	Powers devices (IP cameras, phones) via cable

CHAPTER 11

In networking, digital wins because of its resilience, accuracy, and compatibility with computing systems—but analog still rules in areas like radio and legacy voice systems.

Cabling, Topology, and Transmission Media Technology

Analog and Digital

Analog and digital refer to two different methods of representing and transmitting information, especially in electronics and communication systems.

CHAPTER 11

In networking, digital wins because of its resilience, accuracy, and compatibility with computing systems—but analog still rules in areas like radio and legacy voice systems.

Cabling, Topology, and Transmission Media Technology

Analog and Digital

Analog and digital refer to two different methods of representing and transmitting information, especially in electronics and communication systems.

Analog

- Continuous signals that vary smoothly over time
- Can represent any value within a range
- Common in natural phenomena (sound, light, temperature)
- Example: A vinyl record or FM radio

- **Pros**:
  - Can carry more subtle detail
  - Good for real-world signal capture (like sound)
- **Cons**:
  - More prone to noise and degradation
  - Harder to store and replicate perfectly

CHAPTER 11

In networking, digital wins because of its resilience, accuracy, and compatibility with computing systems—but analog still rules in areas like radio and legacy voice systems.

Cabling, Topology, and Transmission Media Technology

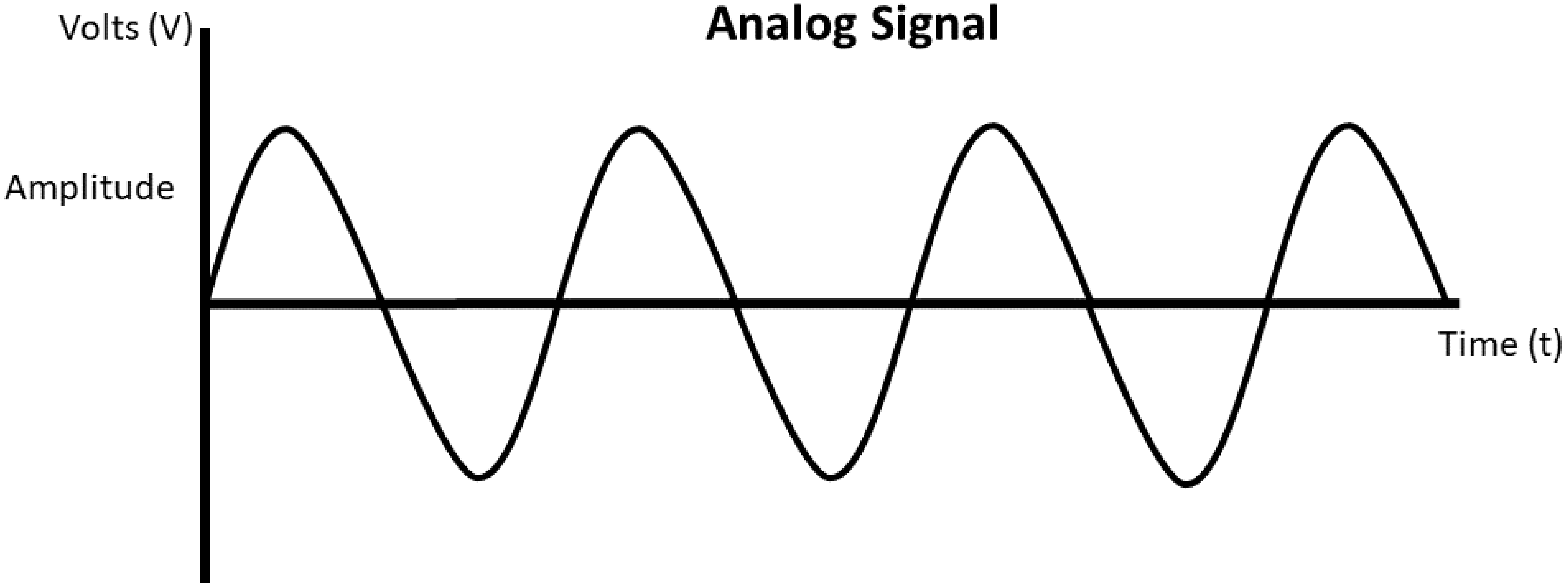
Analog and Digital

Analog and digital refer to two different methods of representing and transmitting information, especially in electronics and communication systems.

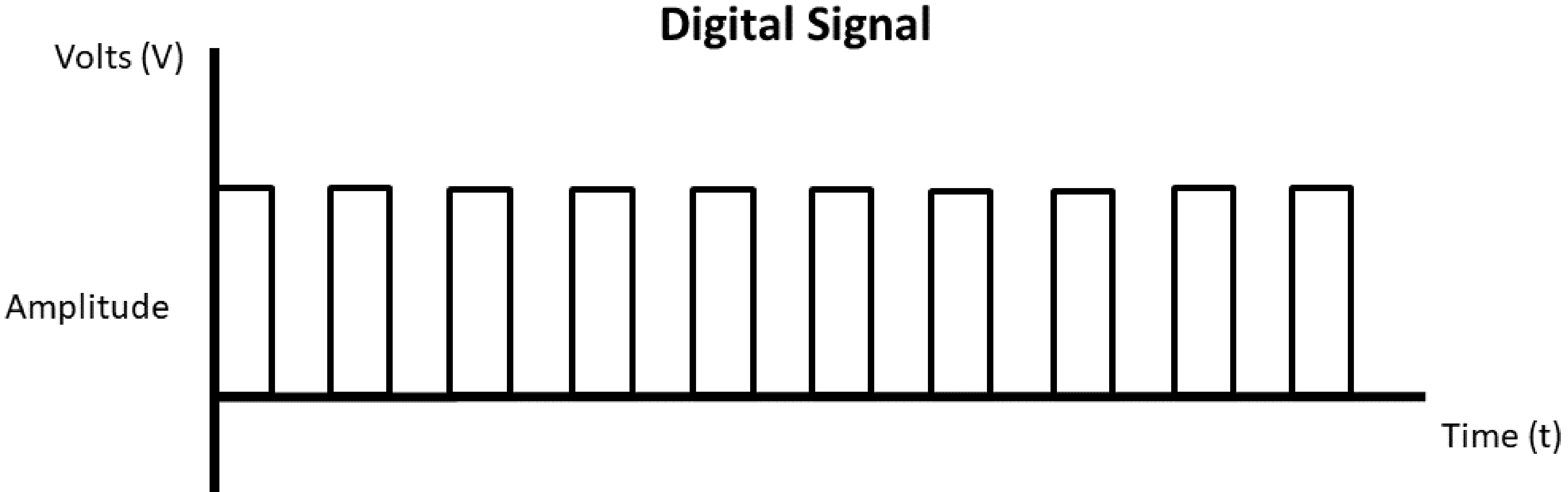
Digital

- Discrete signals (usually binary: 0s and 1s)
- Information is quantized into fixed steps
- Common in computers, networking, storage
- Example: MP3 files, digital watches, Ethernet

- **Pros**:
  - Less noise, easier to store and process
  - Exact copies are easy to make
  - Enables encryption, compression, and error detection
- **Cons**:
  - May lose nuance due to quantization
  - Requires more processing to represent analog inputs



Analog Signal



Digital Signal

CHAPTER 11

CSMA/CD is for old-school Ethernet. Modern Ethernet is switched—no collisions. But Wi-Fi still relies on CSMA/CA to avoid interference in shared airspace.

Cabling, Topology, and Transmission Media Technology

LAN Media Access

- LAN Media Access Control (MAC) determines how devices on a network share the communication channel and avoid talking over each other.

CHAPTER 11

CSMA/CD is for old-school Ethernet. Modern Ethernet is switched—no collisions. But Wi-Fi still relies on CSMA/CA to avoid interference in shared airspace.

Cabling, Topology, and Transmission Media Technology

LAN Media Access

- LAN Media Access Control (MAC) determines how devices on a network share the communication channel and avoid talking over each other.
- In shared media (like early Ethernet or Wi-Fi), multiple devices may attempt to transmit at the same time — so we need rules.

Carrier Sense Multiple Access (CSMA)

"Is someone else talking? If not, I'll speak."

- "Carrier Sense": A device listens to the channel before sending data.
- "Multiple Access": Multiple devices can access the same channel.
- It's the core concept behind both CSMA/CD and CSMA/CA.

CHAPTER 11

CSMA/CD is for old-school Ethernet. Modern Ethernet is switched—no collisions. But Wi-Fi still relies on CSMA/CA to avoid interference in shared airspace.

Cabling, Topology, and Transmission Media Technology

LAN Media Access

- LAN Media Access Control (MAC) determines how devices on a network share the communication channel and avoid talking over each other.
- In shared media (like early Ethernet or Wi-Fi), multiple devices may attempt to transmit at the same time — so we need rules.

CSMA/CD (Collision Detection)

- Used in wired Ethernet (especially older, half-duplex networks).
- Device listens before sending (carrier sense).
- If collision occurs, devices detect it and back off for a random time (collision detection).
- Efficient when traffic is low.
- Collisions increase as network gets busy.

"I'll talk if it's quiet, but if someone else talks at the same time, I'll pause and try again later."

CHAPTER 11

Cabling, Topology, and Transmission Media Technology

LAN Media Access

“You can only talk when you’re holding the talking stick.”

Token Passing

How it works:

- A special data packet called a “token” circulates around the network.
- Only the device holding the token is allowed to transmit data.
- After transmitting, the token is released to the next device in line.
- Used in:
  - Token Ring networks (IEEE 802.5)
  - FDDI (Fiber Distributed Data Interface)
- **Pros**:
  - Deterministic: You know when your turn is coming
  - No collisions
  - Works well under high traffic loads

Cons:

- Slower under low loads
- Token loss can disrupt communication
- More complex and expensive to implement

Token passing and polling aren't widely used anymore, but they're worth knowing for historical context, industrial systems, and understanding the evolution of deterministic networking.

Cabling, Topology, and Transmission Media Technology

LAN Media Access

“The teacher asks each student in turn if they have anything to say.”

Polling

How it works:

- A central controller (master) queries each device (slave) one at a time:
- “Do you have anything to send?”
- If yes, the device responds with data; if not, the master moves on.
- Used in:
  - Mainframe terminal systems
  - Some industrial or proprietary networks
- **Pros**:
  - Simple control
  - Avoids collisions
  - Good in **centralized** environments

Cons:

- Central controller is a single point of failure
- Inefficient when many devices are idle

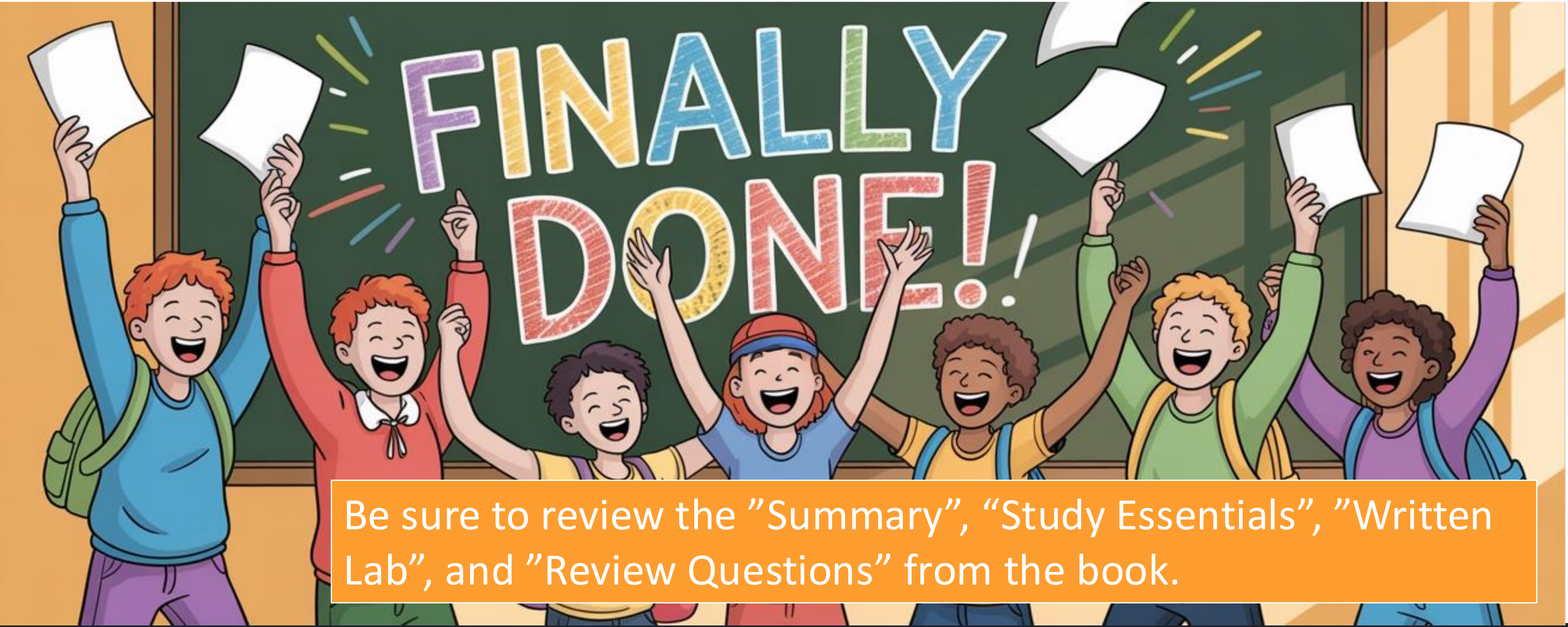
2025 CISSP MENTOR PROGRAM

CHAPTER 11

Secure Network Architecture and Components

CONGRATULATIONS!

You stuck it out. (266 slides later)



Be sure to review the ”Summary”, “Study Essentials”, ”Written Lab”, and ”Review Questions” from the book.