Protecting Information Assets
- Unit# 10 -

Network Security

Agenda

- Open Systems Interconnection Model: Foundation for understanding networks
- Concept of Perimeter (Boundary Protection)
- Defense-in-Depth and Layered Architectures (Tiers)
- Role of Network Segmentation (Compartmentalize)
- Security Information and Event Management (SIEM)
- Quiz

Telecommunication Models

Help understand electromagnetic transmission of data among systems

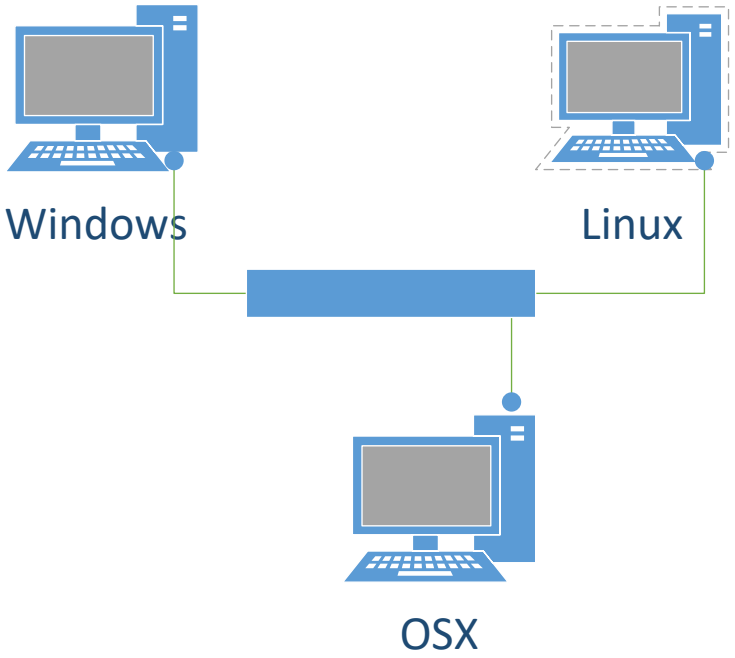
- Through digital, wireless and analog transmission networks

- **Models** and standards of the following organizations have shaped our IT communication technology today
  - International Telecommunication Union (ITU)
  - International Standards Organization (ISO)

Information and Communications Technologies (ICT)

Network protocol

- Standard set of rules that determines how systems communicate across networks
- Different systems can use the same protocol to communicate and understand each other despite their differences.



Open Systems Interconnection(OSI) Reference Model – ISO Standard 7498-1

OSI Model

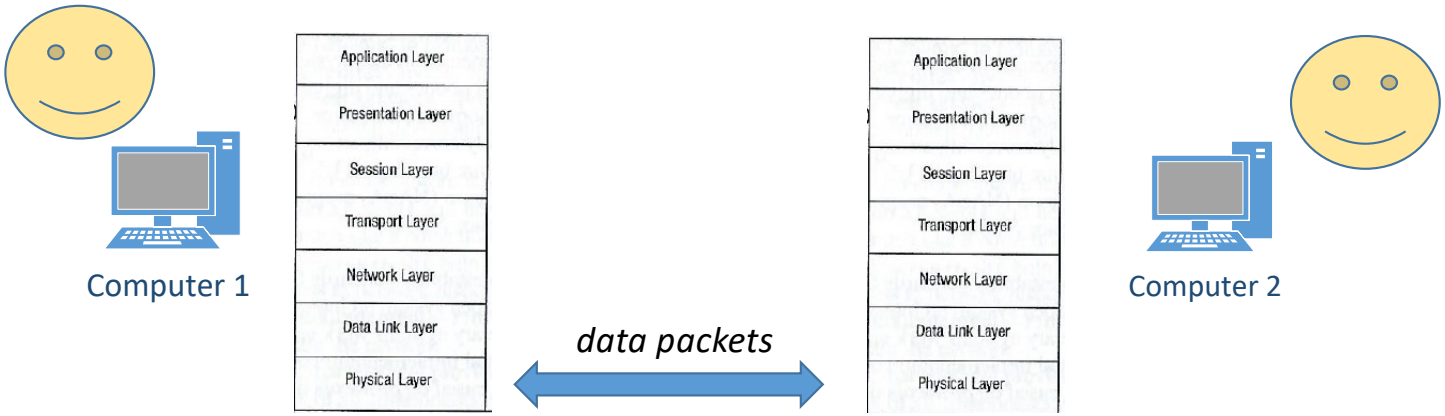
- Guidelines used by vendors, engineers, developers to develop products that enable computer systems to interoperate
- **Open network architecture is**
  - Not owned by vendors and not proprietary
  - Can easily integrate various technologies and vendor implementation of those technologies

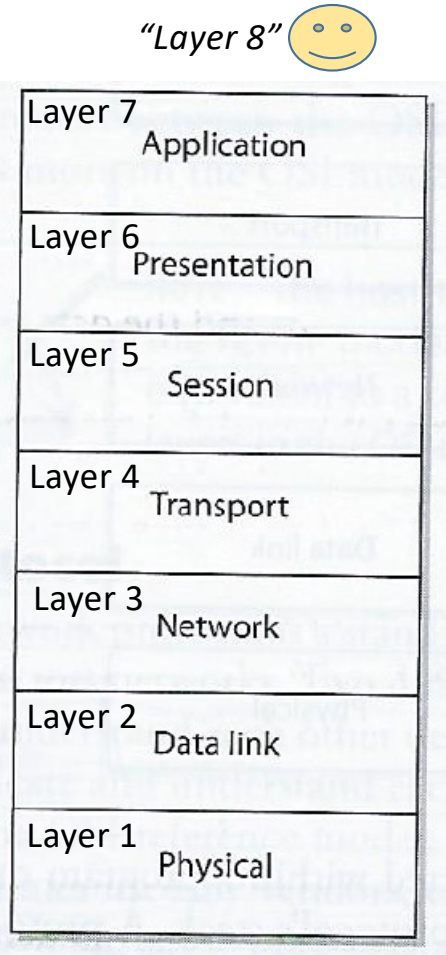
Graphics on the following slides come from Harris S. and Maymi F. (2016) All in One CISSP Exam Guide, Seventh Edition

Open Systems Interconnection(OSI) Reference Model – ISO Standard 7498-1

OSI Model

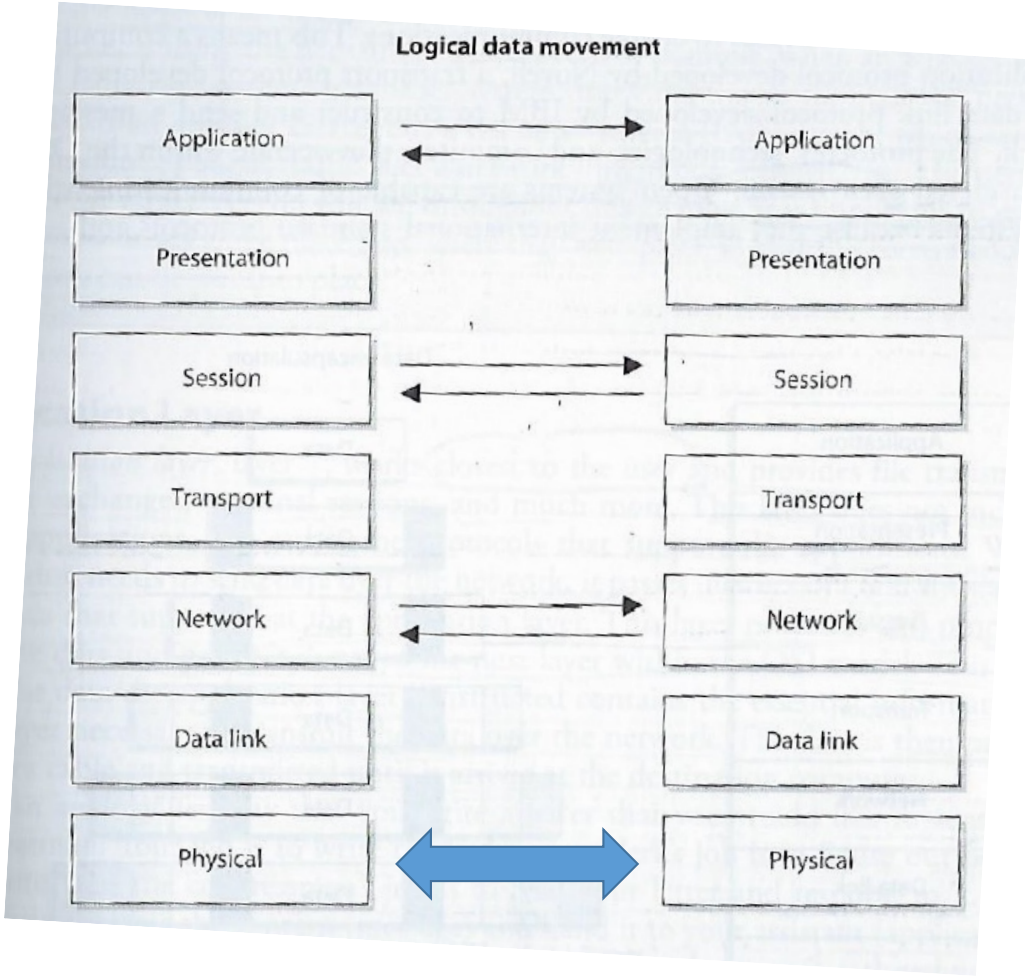
- Guidelines used by vendors, engineers, developers to enable their systems to interoperate
- Layers networking tasks, protocols and services into different layers
- Each layer has its own responsibilities regarding how two computers communicate over a network





Computers communicate via network

- Protocols function in specific OSI layers
- Each protocol on one computer communicates with the same corresponding protocol within the same OSI layer on another computer
- Via logical channels
- At the physical layer electronic/light signals are passed from one computer over a wire/fiber optic cable to the other computer

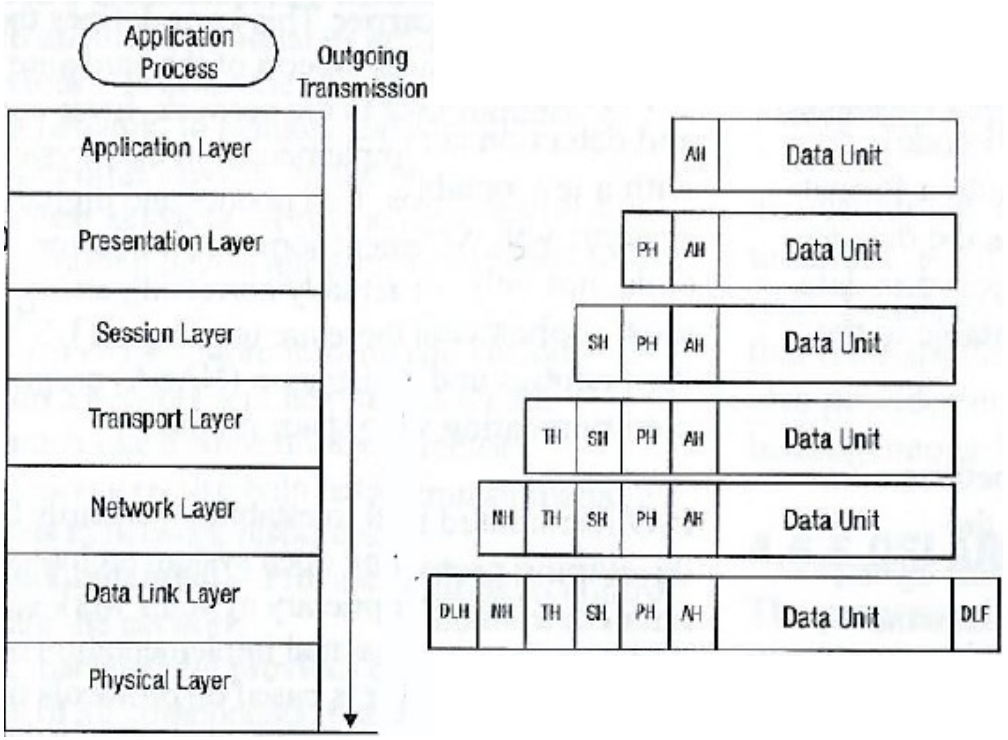


Encapsulation

- Process by which a protocol is used to enable two computers to communicate with each other within a specific OSI layer on each

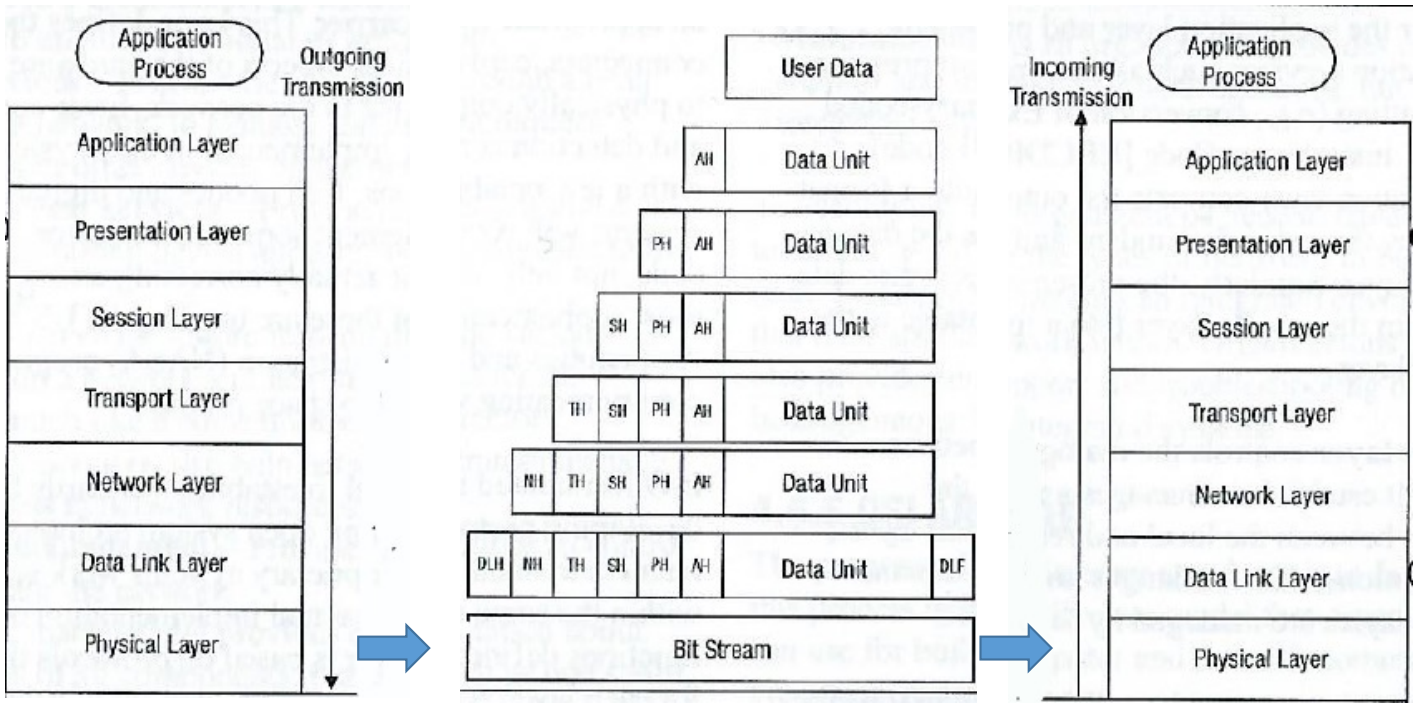
1. A message is constructed within a program on one computer and passed down through a stack of network protocols…

   A protocol at each layer adds its own information to the message, and the message grows in size as it goes down the protocol stack & is prepared for transfer over the network



Encapsulation

2. At the physical layer of the network the message is passed by the sending computer as bits via electronic or light pulses (on/off) across the network to the destination computer

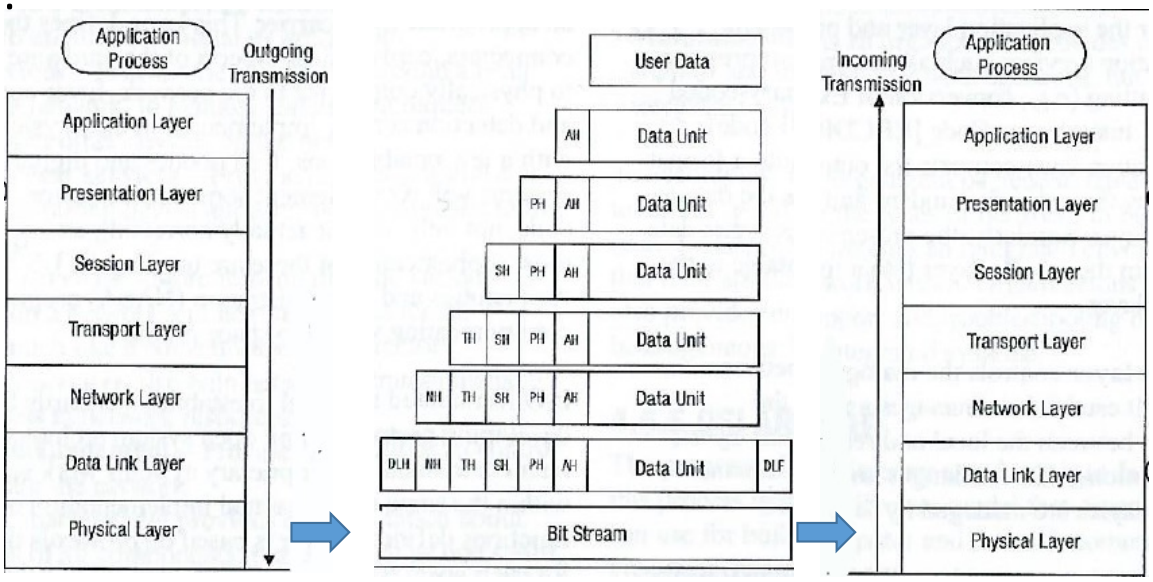


3. At the destination computer the encapsulation is reversed taking the message apart via the protocols of each layer until the data is ready for the application processing

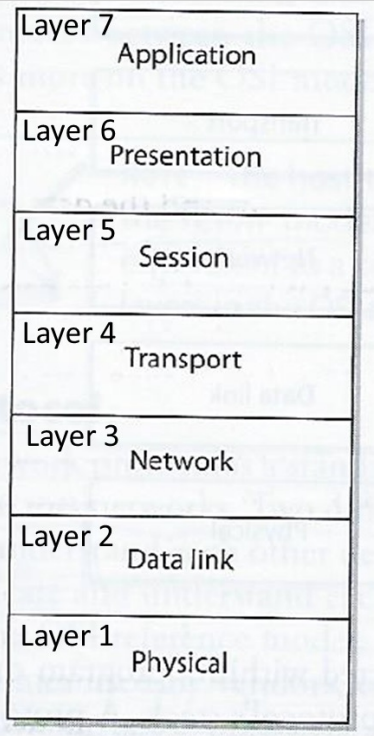
OSI Network Model

- A protocol at each layer expects the data in a particular format (“syntax”) and performs specific control functions on the data
- Data for control functions are added by the protocols at each layer in the form of headers and trailers of the datagram/packet/frame
- Each layer has a connection point (“interface”) that allows it to communicate with 3 other layers, communications with:

1. Interface of the layer above
2. Interface of the layer below it
3. Communications with the same layer in the interface of the destination computer



OSI Layers

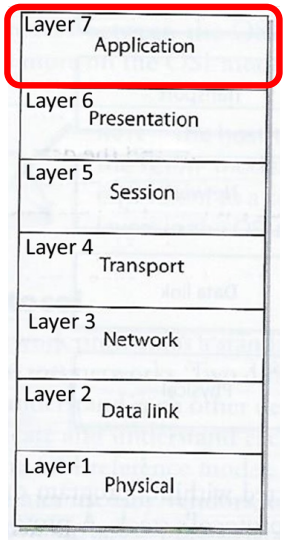


- Specifications for each layer's interface is very structured
- Implementing international standard protocols and interfaces within different vendors' technologies makes them part of an "open system" in which computers can communicate with one another
- Being part of an open system of protocols makes the different layers of a common network stack vulnerable and targets of attack

A network can be:

1. Used as a channel of an attack – i.e. as a resource for an attacker
   - For example: *Attacker sends a virus via a network channel from one system to another*
2. The target of an attack
   - For example: *Attacker carries out a denial-of-service (DoS) attack which sends a large volume of badly formed protocol message traffic over a network link to bog it down*

Layer 7: Application Layer



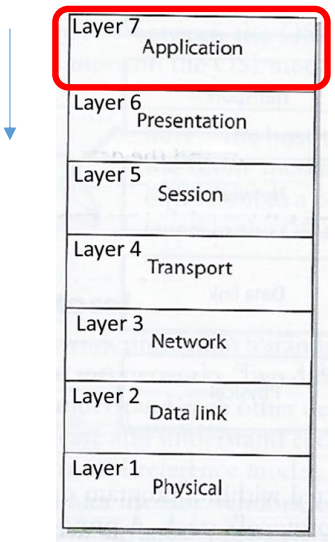
Works closest to the user – providing protocols that support the user's applications

For example: File transmissions, message exchanges, terminal sessions…

- When an application needs to send data over the network, it passes instructions and data through the protocols that support it at the application layer

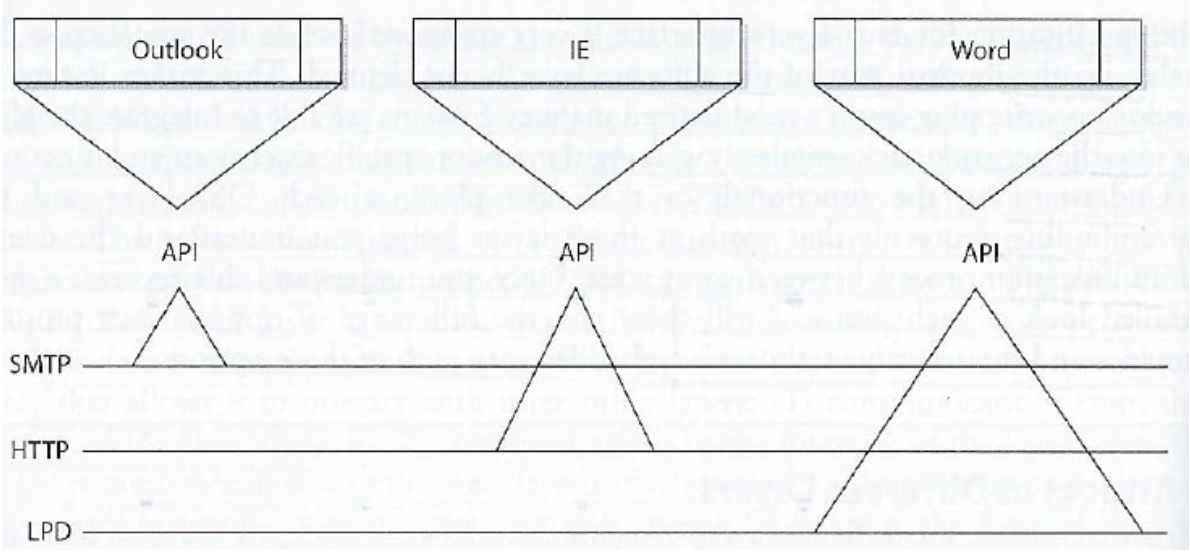
Application layer properly formats the data and sends it down to the presentation layer… (after data makes it through all the layers it has all the information needed to transmit it over the network)

Layer 7: Application Layer

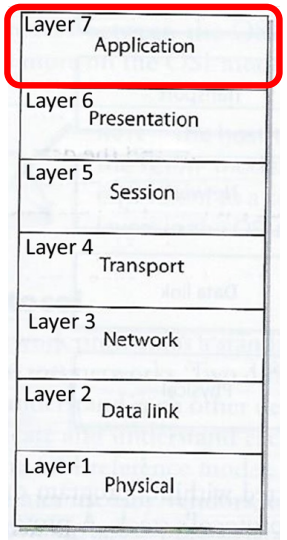


Applications communicate with Layer 7 protocols by sending requests using Application Program Interface (API) libraries

E.g. Outlook user clicks send, and the email client sends this information to SMTP (Simple Mail Transfer Protocol) which adds information to the user's message and passes it down to the Presentation Layer



Layer 7: Application Layer



Many application service-specific protocols are available within Layer 7, including:

Running Commands and Applications

- **Telnet** – A terminal emulation network application that supports remote connectivity for executing commands and running applications. It does not support transfer of files
- **X Window** – A graphical user interface (GUI) application programming interface (API) for command-line operating systems

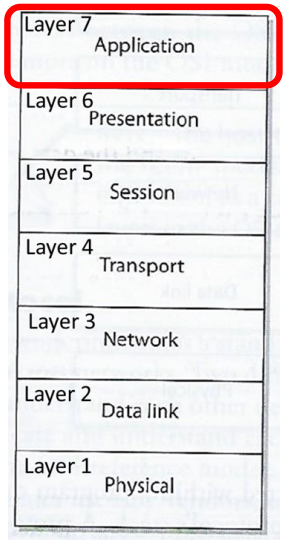
File Transfer:

- **File Transfer Protocol (FTP)** – A network application that supports exchange of files which supports either anonymous and specific authentication
- **Trivial File Transfer Protocol (TFTP)** – A network application that supports exchange of files that does not require authentication
- **Network File System (NFS)** – A network service used to support file sharing between different systems

Email:

- **Simple Mail Transfer Protocol (SMTP)** – A protocol for transmitting email messages from a client to an email server and from one email server to another
- **Post Office Protocol (POP3)** – A protocol for pulling email messages from an inbox on an email server down to an email client
- **Internet Message Access Protocol (IMAP)** – More secure than POP3. A protocol for: pulling email messages from an inbox on an email server down to an email client; pulling email message headers from the email server and deleting messages from the email server (without pulling the entire message to the local client)

Layer 7: Application Layer



Many application service-specific protocols are available within the Application Layer, including:

Network Addressing

- **Dynamic Host Configuration Protocol (DHCP)** – Enables centralized control of network addressing, used to assign TCP/IP configuration settings to systems when booted up

Web Pages

- **Hypertext Transfer Protocol (HTTP**) – A protocol used to transmit web page contents from web server to web browsers

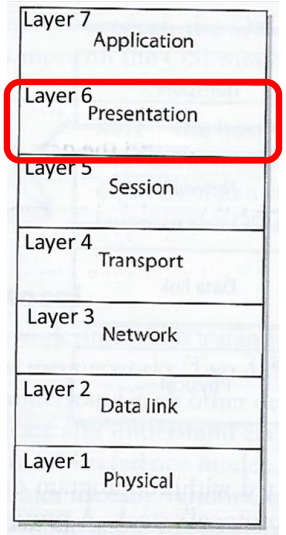
Printing

- **Line Print Daemon (LPD)** – A network service used to send print jobs to printers, and to spool print jobs

Network Monitoring

- **Simple Network Management Protocol (SNMP)** – A protocol used to collect network status and health information by polling devices (routers, switches, wireless access points, firewalls, printers, …) from a central monitoring station. SNMP v3 supports encryption and authentication

Layer 6: Presentation Layer



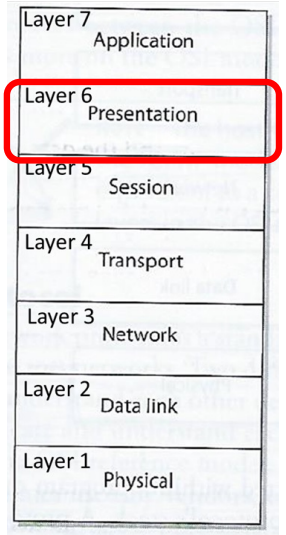
Receives data from the application layer protocol and puts it in a standard format with annotation that enables understanding by the processes operating at Layer 6 on destination computer

Presentation layer

1. Translates the format of data an application is using into a standard format used for passing messages over a network
2. Adds file type data to tell destination computer the file type and how to process and present it
3. Handles compression and encryption requests and adds data that enables the receiving computer to know how to decompress and decrypt the data

Application layer properly formats the data and sends it down to the presentation layer… (after data makes it through all the layers it has all the information needed to transmit it over the network)

Layer 6: Presentation Layer

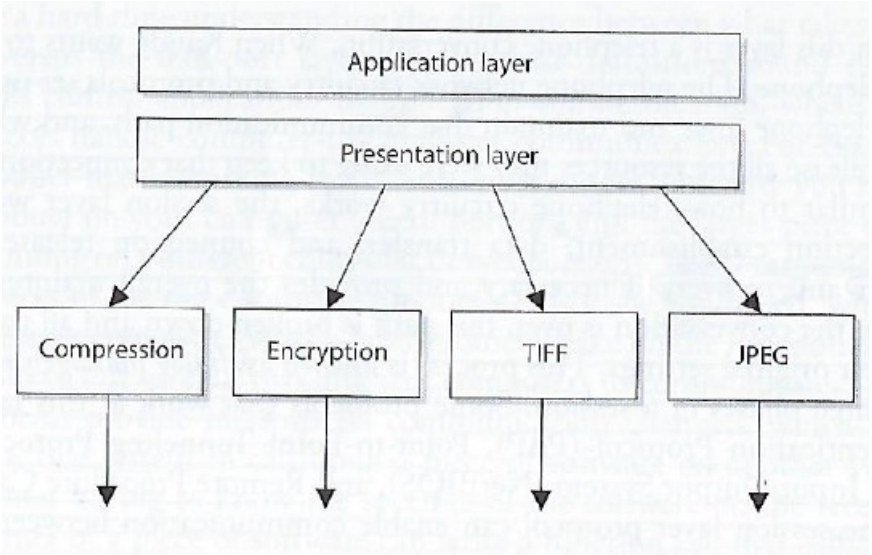


Protocols functioning at this layer communicate include:

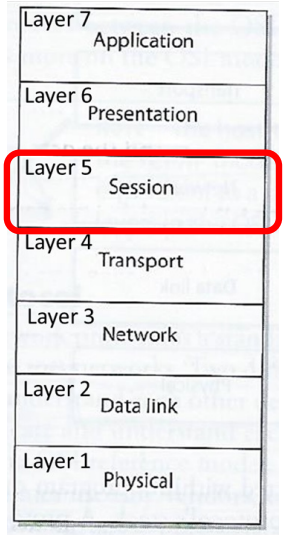
- ASCII – American Standard Code for Information Interchange
- MIME – Multipurpose Internet Main Extensions standards
- TIFF - Tagged Image File Format
- GIF – Graphic Interchange Format
- JPEG – Joint Photographic Experts Group
- MPEG – Moving Picture Experts Group
- MIDI – Musical Instrument Digital Interface

For example,

1. *User compresses file on Windows computer sends it to someone on Linux computer*
2. *Linux computer receives the file, it looks at the file header, interprets the header's MIME type (Content-Type: application/zip) and knows what application to use to decompress the file*
3. *If systems does not have a program that understands the compression/decompression instructions, the file is displayed to the user with an unassociated icon*



Layer 5: Session Layer



When two applications need to communicate or transfer data between themselves, Layer 5 is responsible for:

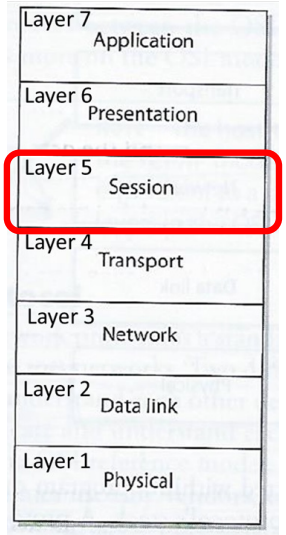
1. Establishing a connection between two applications
2. Dialog management to maintain the connection during the transfer of data
   - *Restarts and recovers the session to maintain the connection if needed*
3. Controlling release of the connection

- Provides inter-process communication channels, enables one software module on a local system to call a second software module running on a remote system. The results of the second module are retuned to the first system over the same session protocol channel

The session layer protocol enables 3 different modes of communications between 2 applications running on different computers across the network:

1. ***Simplex:*** *Communication takes place in one direction (very seldom used)*
2. ***Half-duplex:*** *Communication takes place in both directions, but only one application can send information at a time*
3. ***Full-duplex:*** *Communication takes place in both directions , and both applications can send information at the same time*

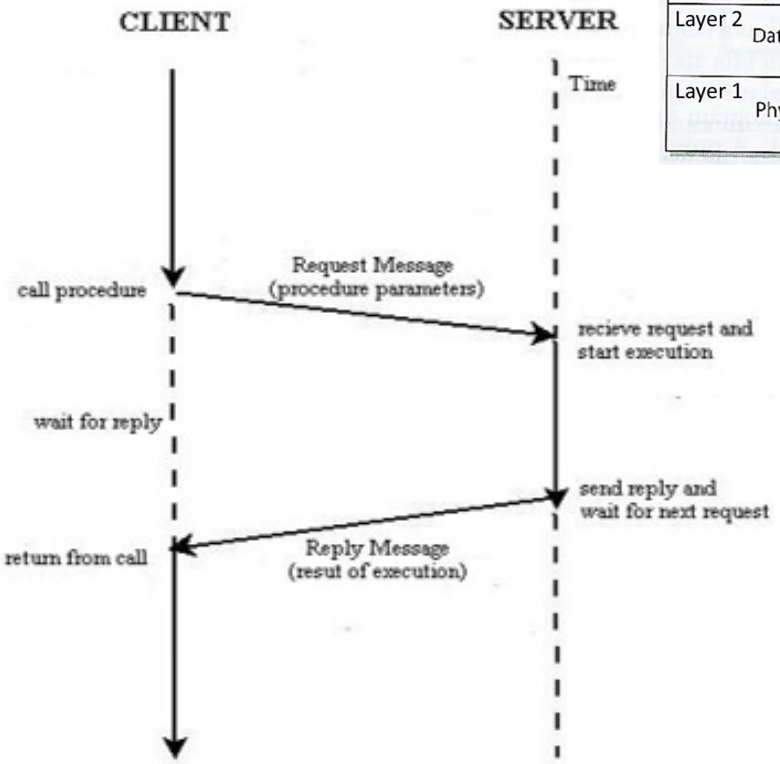
Layer 5: Session Layer



Provides inter-process communication channels, enables one software module on a local system to call a second software module running on a remote system. The results of the second module are retuned to the first system over the same session protocol channel

Protocols include:

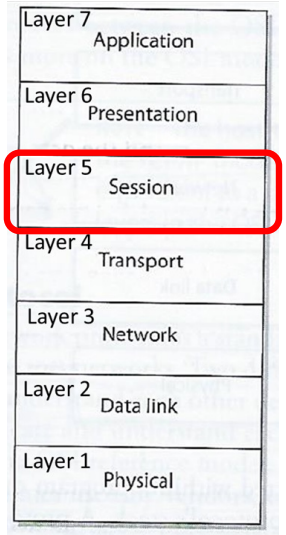
- PAP – Password Authentication Protocol
- PPTP – Point to Point Tunneling Protocol
- SQL – Structured Query Language
- RPC – Remote Procedure Call



Session layer protocols provide the middleware functionality that connects and maintains the connection between software applications on different computers as they communicate (i.e. application to application communication)

- Client-server model
- Service oriented architecture (SOA)

Layer 5: Session Layer



One security issue affecting the session layer common to inter-process communication software (e.g. RPC) is the lack of authentication or use of weak authentication

Example mitigation:

- *Use SRPC – Secure RPC*

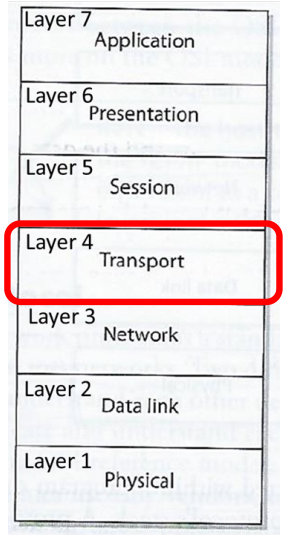
  Requires authentication to take place before two computers located in different locations are able to communicate with each other

  Session layer protocols need to secure authentication capabilities, however, which use shared secret keys, public keys, or Kerberos tickets

Unused Session Layer protocols should be identified and disabled on systems to decrease the chance of them getting exploited

RPC and NetBIOS and similar distributed processing calls usually only take place within a single organization's network, thus firewalls should be configured to filter this dangerous traffic and prevent it from moving into or out of the network

Layer 4: Transport Layer

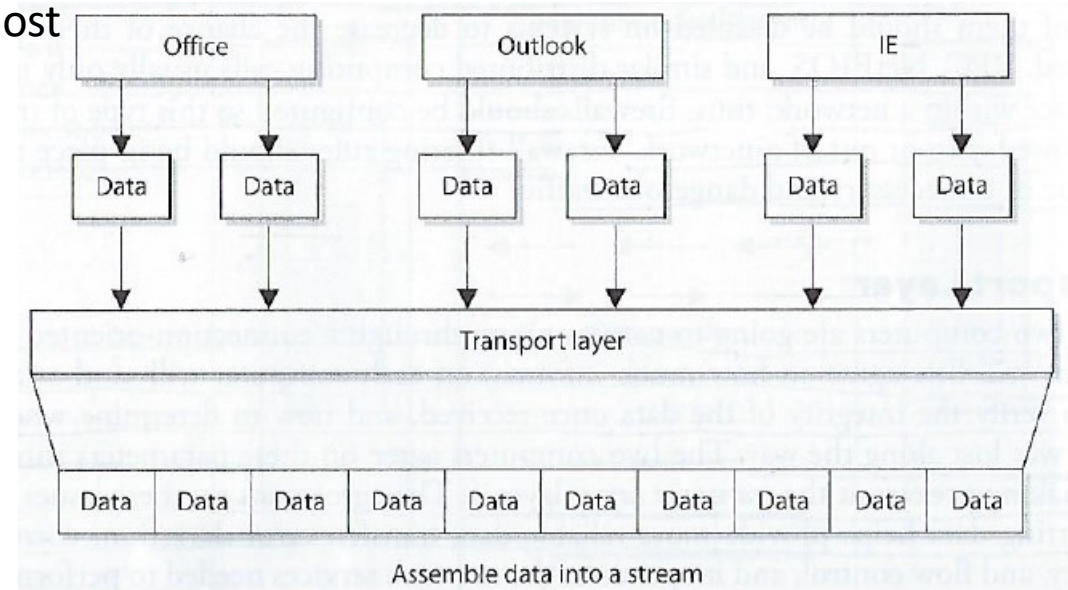


Establishes a logical connection between two computer systems and provides end-to-end data transport services

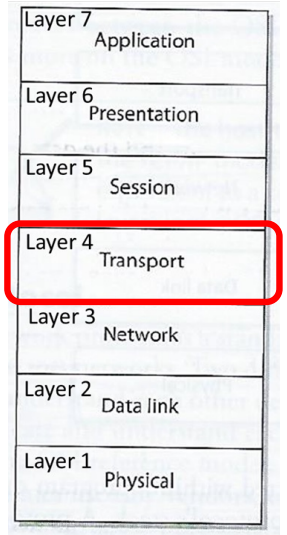
Provides connection level protocols for two computers to engage in a "handshaking process" and agree on parameters for:

1. How much data each computer will send at a time
2. How to verify data integrity once received
3. How to determine if a data packet was lost

Receives data from different applications and assembles their data into a stream for transmission over the network



Layer 4: Transport Layer

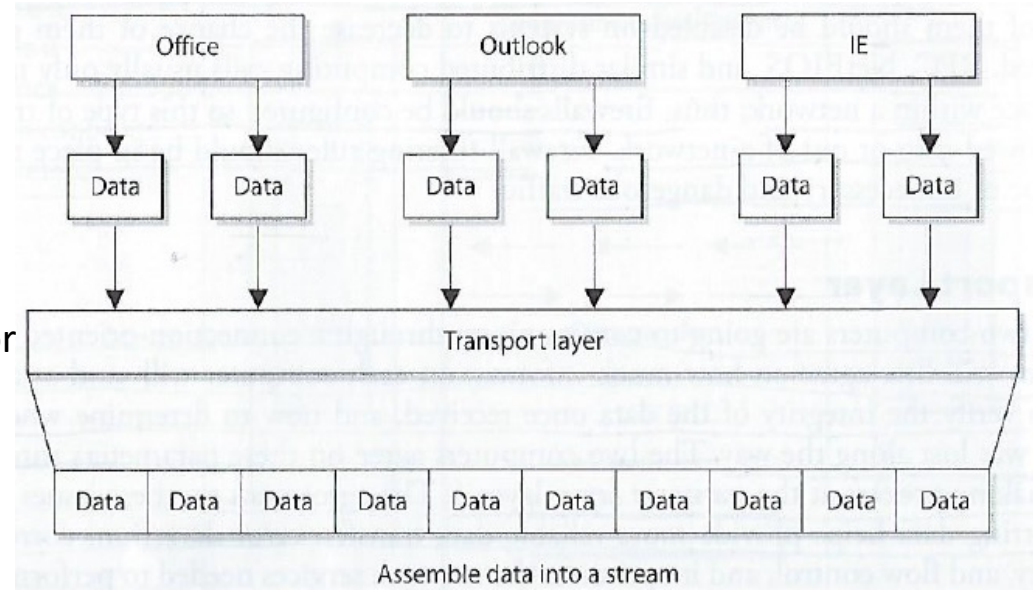


Transport layer protocol controls data flow across computer to computer connections without tracking connections between individual pairs of applications communicating across the network

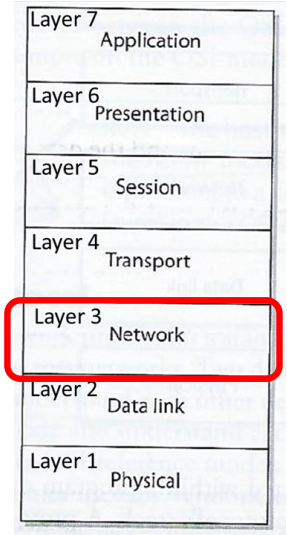
Protocols include:

- **TCP – Transmission Control Protocol,** *Connection-oriented provides reliable data transmission*
- **UDP – User Datagram Protocol**, *Connectionless*
- **SSL - Secure Sockets Layer (SSL) –** Originally designed for secure web communications (HTTPS)
- **TLS – Transport Layer Security protocol**, straddles both Session and Transport layers, is capable of securing communications supporting other Application Layer protocols

After the Transport Layer appends it's information to the data message, it is called either a TCP "segment" or a UDP "Packet"



Layer 3: Network Layer's



Routing protocols

- Build and maintain routing tables
  Routing tables are maps of the network
- Determine best route to send packet from source computer to destination computer
- Inserts information into the data packet's header consisting of addresses (source and destination) and routes to their destination
- Do not guarantee delivery of packets
  Transport layer protocols catch problems and resend packets as needed (TCP not UDP)

Protocols include:

- ICMP – Internet Control Message Protocol
- IP – Internet Protocol
- Internet Protocol Security (IPSec)
- IPX – Internet Packet Exchange
- RIP – Routing Information Protocol
- OSPF – Open Shortest Path First
- BGP – Border Gateway Protocol
- NAT –Network Address Translation
- SKIP –Simple Key Management for Internet Protocols

Routers operate on OSI Layer 3

After the Network Layer appends it's information to the data message, it converts it to binary format and the unit of data is called a "packet"

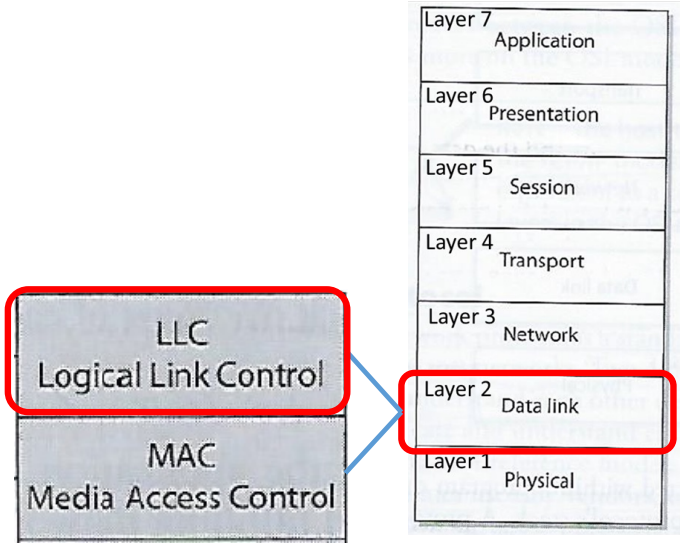
Layer 2: Data Link Layer

Translates the data packet with header/footer information accumulated from layers above into

- LAN (Local Area Network) or WAN (Wide Area Network) binary format for transmission over the network transmission line

After the network layer adds its routing information into the data packet, it passes the packet to the Data Link Layer's LCC sublayer

- LCC sublayer takes care of flow of control and error checking and passes it to the MAC sublayer



"Framing" is the name of the process when the data link layer applies its header and trailer to the data message

The unit of data is called a "frame"

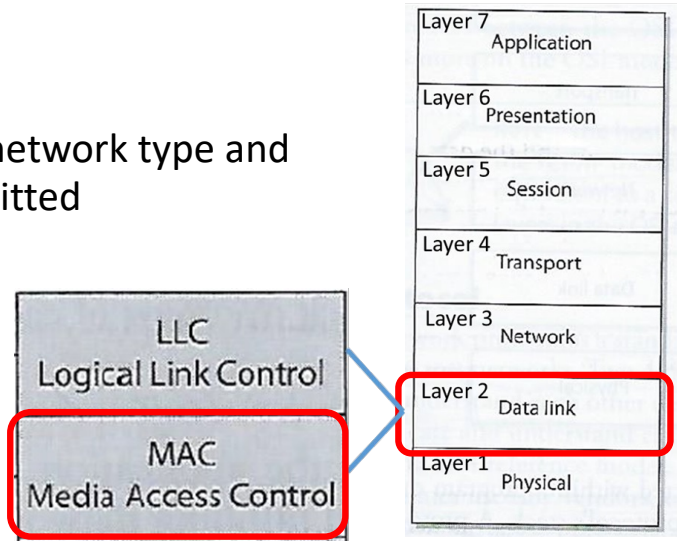
Switches operation on OSI Layer 2

Layer 2: Data Link Layer

The MAC sublayer determines if data will be transmitted over a LAN or WAN, network type and protocols and puts the last header and trailer on the packet before it is transmitted

- Each network type uses different protocols, NICs (network interface cards), cables, and transmission methods
- The MAC sublayer determines the format of the data frame for transmission over the particular type network the computer's NIC is attached to the following protocols:

  Ethernet (IEEE 802.3)
  Token Ring (IEEE 802.3)
  FDDI – Fiber Distributed Data Interface
  Wireless Ethernet (IEEE 802.11)



Other protocols at this layer include:

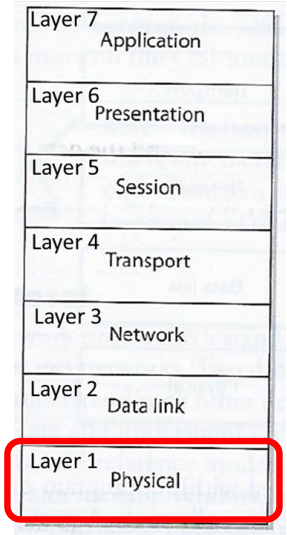
- ARP – Address Resolution Protocol
- RARP – Reverse Address Resolution Protocol
- SLIP – Serial Line Internet Protocol
- PPP – Point-to-Point Protocol
- PPTP – Point-to-Point Tunneling Protocol
- L2F – Layer 2 Forwarding
- L2TP –Layer 2 Tunneling Protocol

Each component has a different:

- *Header data format structure*
- *Protocol for physical transmission across the network type (coaxial, twisted pair, fiber optic cable; or wireless)*

The computer's network card bridges the data link and physical layers, takes data passed down from the user's application through the 6 layers above and its network card driver encodes the bits at the data link layer

Layer 1: Physical Layer



The Network Interface Card (NIC)

- Produces and interprets electromagnetic signals
- Converts bits into signals or voltages suitable for transmission across the LAN or WAN technology it is connected
- Determines synchronization, data transfer rates, line noise and transmission techniques based on the physical connection to electrical, optical or mechanical equipment

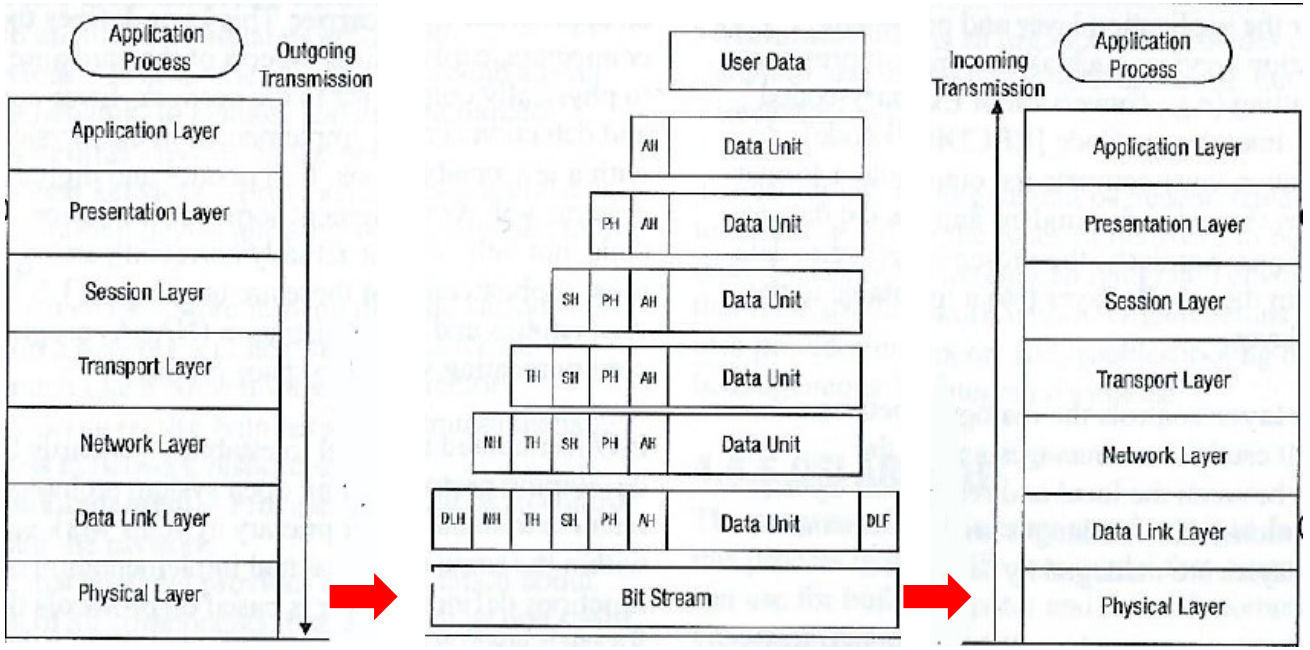
E.g. A '1' bit transmitted via Ethernet would be translated by the NIC to +0.5-volt electric signal, and '0' bit would be transmitted as 0-volts

TIA – Telecommunications Industry Association
EIA – Electronic Industry Alliance

Standard interfaces at this layer include:

- RS/EIA/TIA-422, RS/EIA/TIA-423, RS/EIA/TIA-429, RS/EIA/TIA-449, RS/EIA/TIA-485
- 10Base-T, 10Base2, 10Base5, 100Base-TX, 100Base-FX, 100Base-T, 1000Base-T, 1000-Base-SX
- X.21
- HSSI – High-Speed Serial Interface
- SONET – Synchronous Optical Networking
- V.24 and V.35

Layer 1: Physical Layer



Data/file requests and terminals

Standard formats, encryption, compression

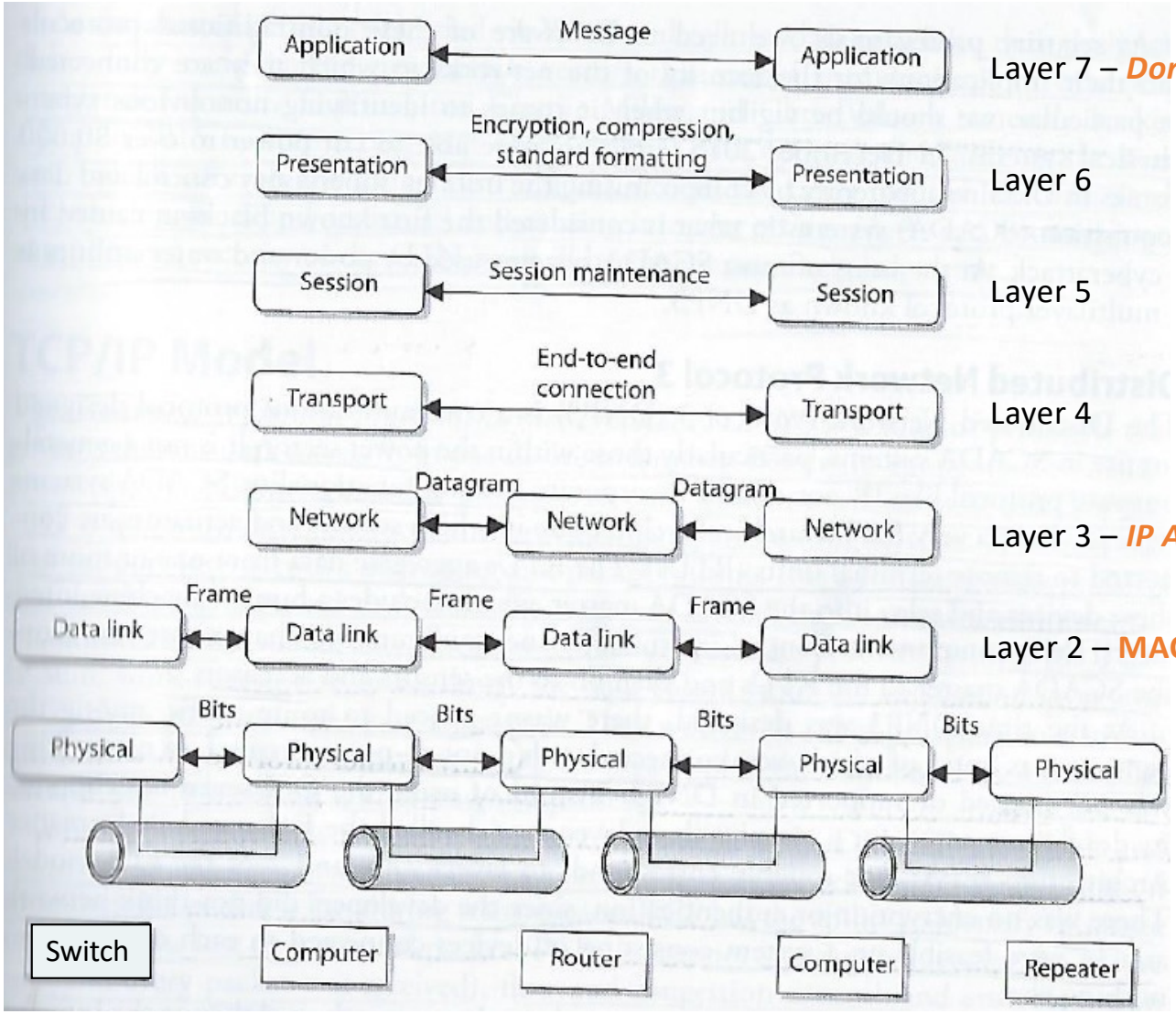
Applications communicating data

Computers communicating

Routing packets formed

Data frames ready for transfer

Signal processing



Layer 7 – ***Domain Name e.g. mycomputer.temple.edu***

Layer 6

Layer 5

Layer 4

Layer 3 – ***IP Address e.g. xxx.xxx.xxx.xxx***

Layer 2 – **MAC (Media Access Control) Address**

Layer 1

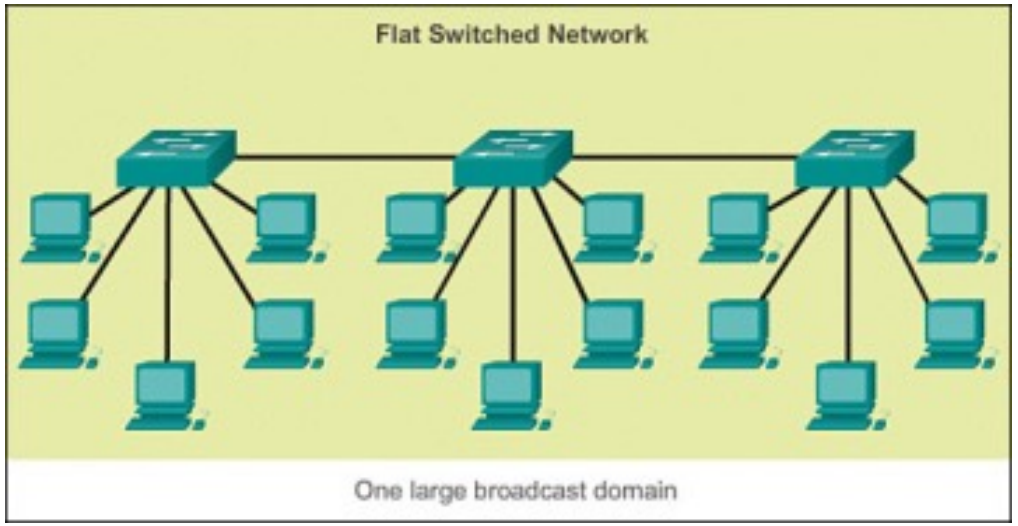
Note: Synonyms for host computer across the OSI Model

Agenda

- ✓Open Systems Interconnection Model: Foundation for understanding networks
- Concept of **Perimeter** (Boundary Protection)
- Defense-in-Depth and Layered Architectures (Tiers)
- Role of Network Segmentation (Compartmentalize)
- Security Information and Event Management (SIEMs)
- Quiz

Flat Networks

- Flat networks (single vlan) do not have defense-in-depth.
- No network level inspections
- Events on flat networks propagate on entire vlan



VLAN = Virtual LAN

Network Security is about controlling access to who can ....

see packets (**C**onfidentiality)

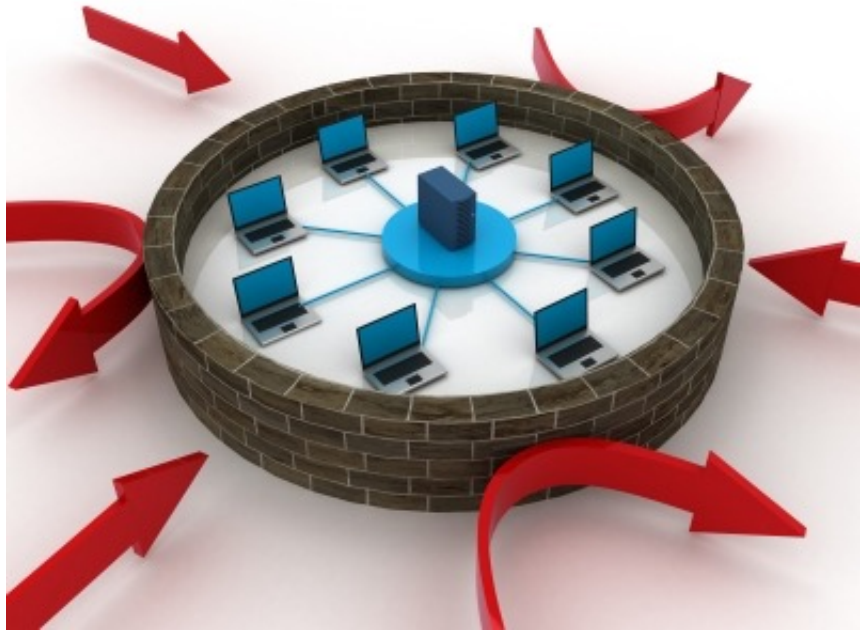
change packets (**I**ntegrity)

interrupt packets (**A**vailability)

Perimeter

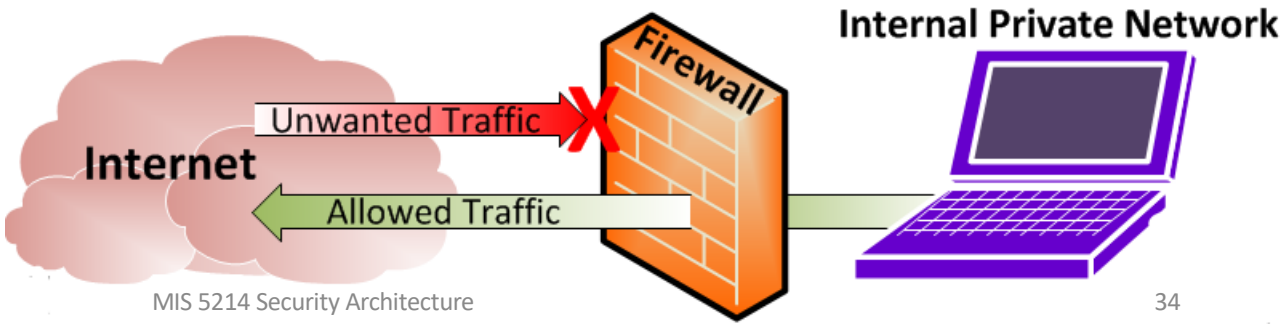
Perimeter

- Boundary between the private and locally managed-and-owned side of a network.
- Requires necessary safeguards
  - Firewalls
- What is the exposure?
  - Vulnerability scanning (Nmap)



Firewalls used to Implement Network Security Policy

- Support and enforce an organization's network security policy
- Implement high-level directives on acceptable an unacceptable actions to protect critical assets
- Firewall security policy:
  - What services can be accessed
  - What IP addresses and ranges are restricted
  - What ports can be accessed



Firewalls are security architecture “choke points” in an IT network

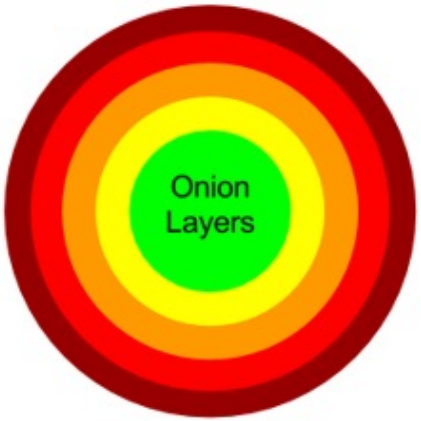
- All communication should flow through, be inspected by, and restricted by firewalls

- Firewalls are used to restrict access from one network to another network
  - From the internet to access corporate networks
  - Between internal network segments

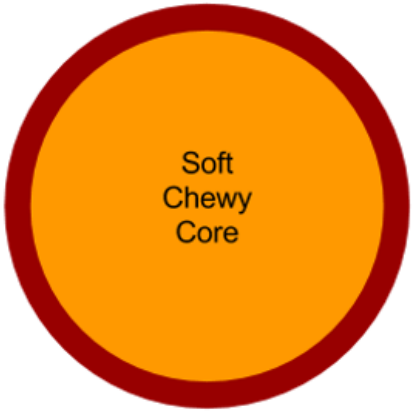
- Restrict access
  - Between origin and destination
  - Based on determination of acceptable traffic type(s)

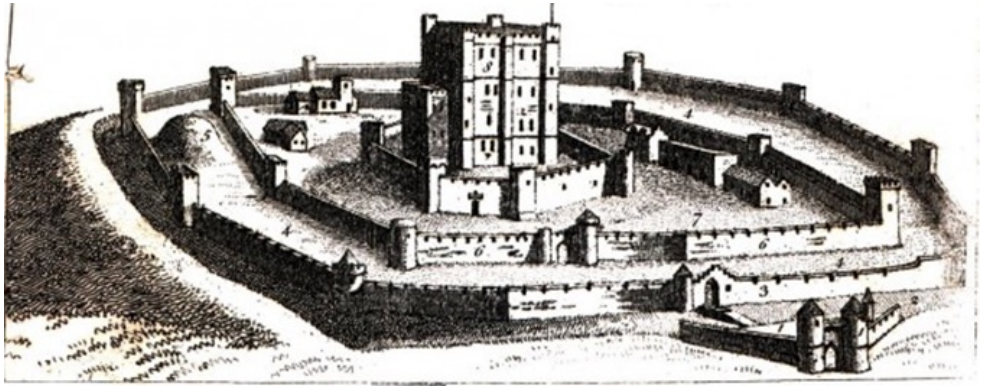
Perimeter security only takes care of the outer layer of security

For better security, however, we seek…

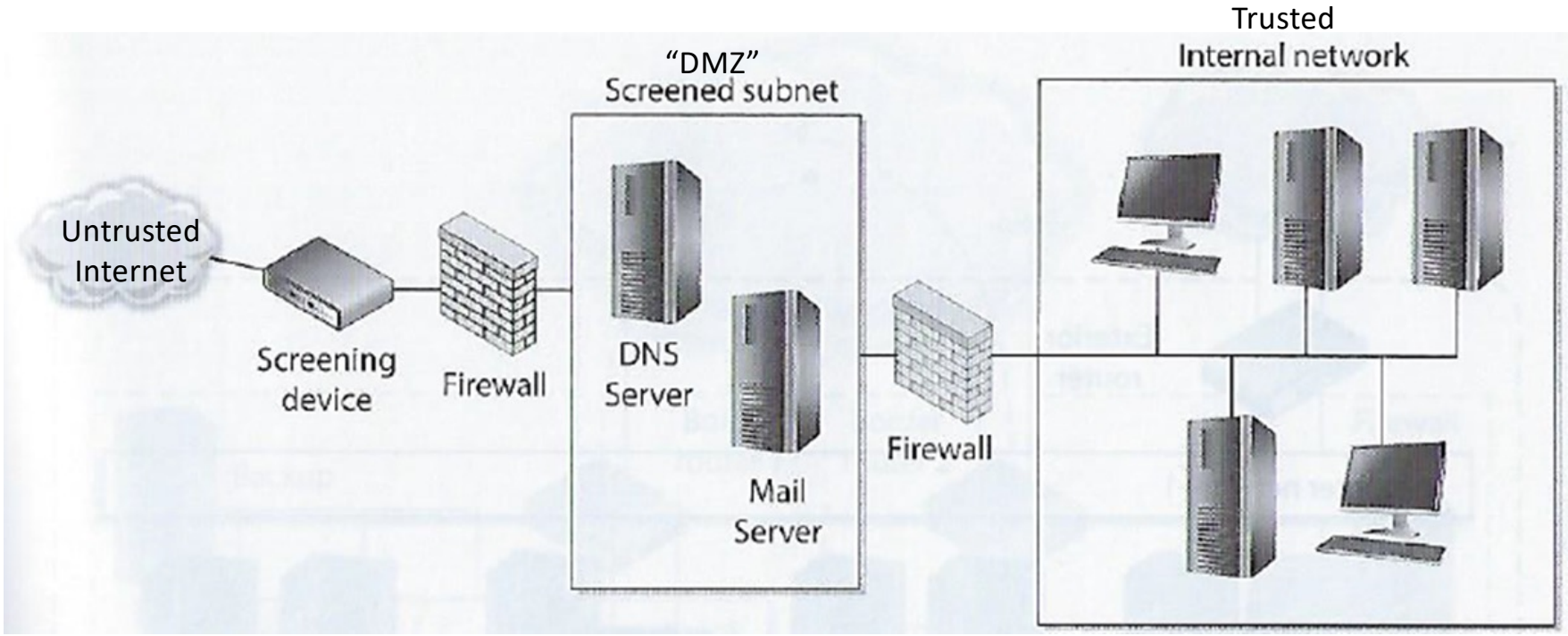


“Layered Security” = “Defense in Depth”





Layered Security Architecture at Perimeter



Firewall Technology

- May be implemented as a
  - Software product running on a server
  - Specialized hardware appliance
- Monitors data packets coming into and out of the network it is protecting
- Packets are filtered by:
  - Source and destination addresses and ports
  - Header information
  - Protocol type
  - Packet type
  - Service
  - Data content – i.e. application and file data content

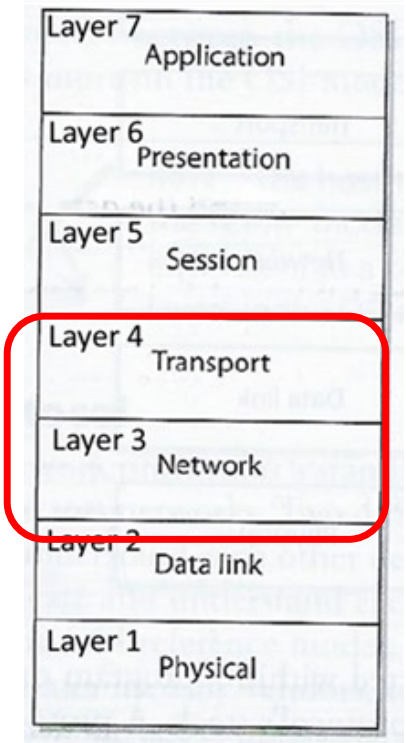
Different types of firewalls work at different OSI Layers

1. Static Packet filtering firewalls (OSI Network Layer 3)
2. Dynamic packet filtering firewalls (OSI Network & Transport Layers 3 & 4)
3. Stateful inspection firewalls (OSI Transport Layer 4)
4. Deep Packet Inspection or Application-Level firewalls (OSI Application Layer 7)
5. Next-Generation firewalls (OSI Layers 3 through 7 + IDS or IPS)

Static packet-filtering firewalls

"First-generation" firewall technology – most basic and primitive

- Operate on Network Layer 3 of the OSI model
- Also known as "*screening routers*"



Capabilities built into most firewalls and routers

- Configured with access control list (ACL) rules which dictate the sources or destinations of permitted traffic into and out of the network
- Filters compare protocol header information from network and transport layers with ACLs
  - ACL black-listing allows all traffic by default but specifically identifies IP addresses of packets associated with prohibited origins or destinations
  - ACL white-listing denies all traffic by default but specifically identifies IP address of packets associated with permitted origins or destinations

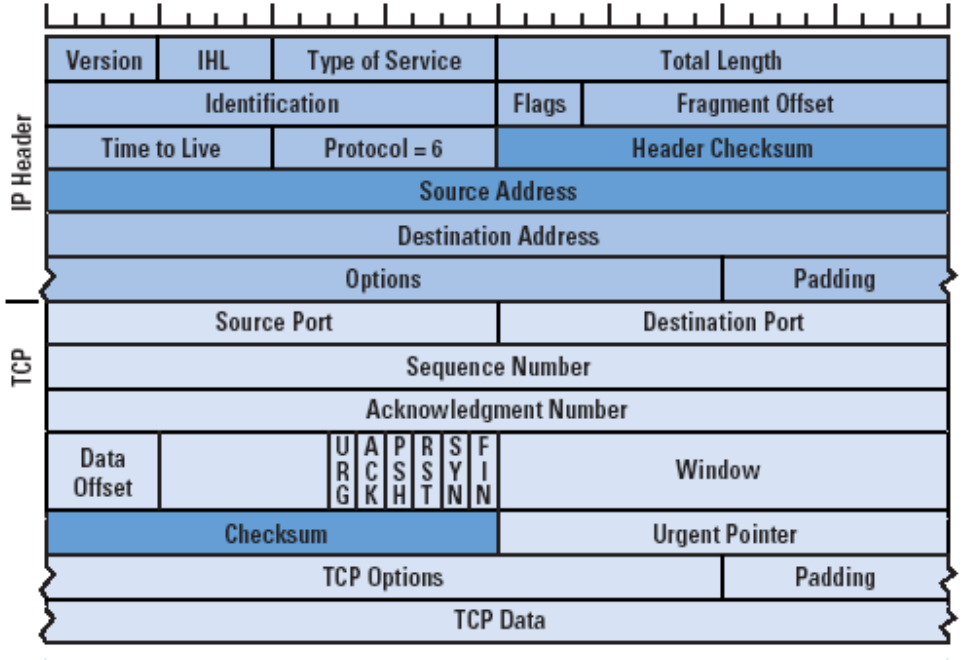
Packet-filtering Firewalls

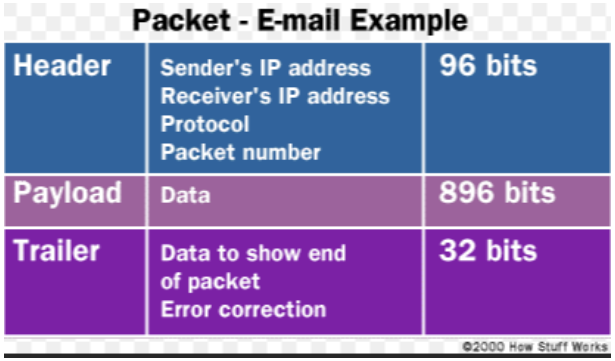
Compares ACLS with network protocol header values to determine permit/deny network access based on:

1. Source and destination IP addresses
2. Source and destination port numbers
3. Protocol types
4. Inbound and outbound traffic direction

Network Layer 3

Transport Layer 4





Agenda

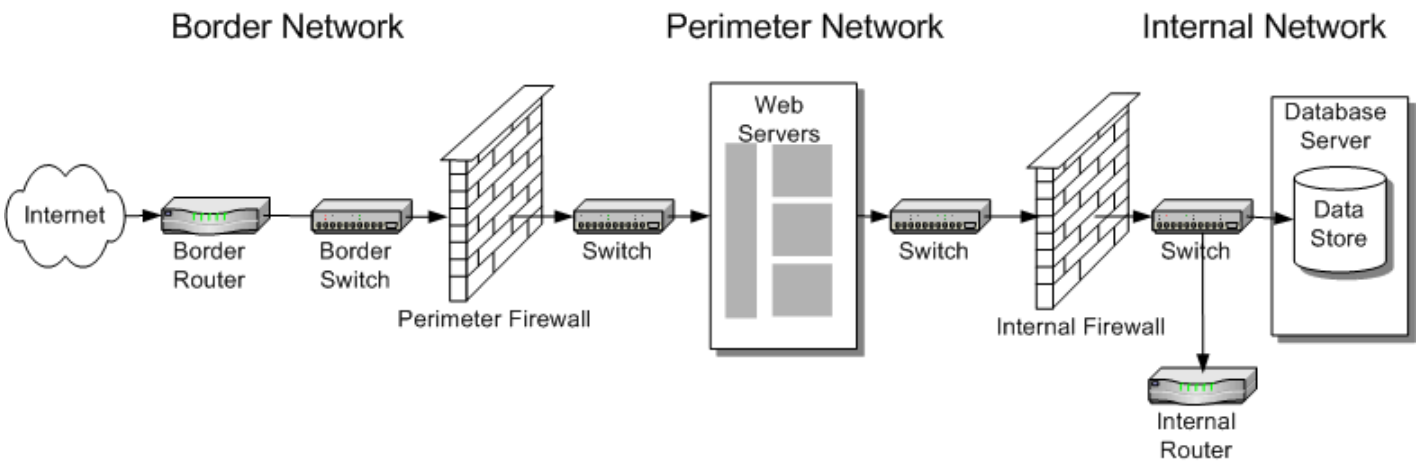
- ✓Open Systems Interconnection Model: Foundation for understanding networks
- ✓Concept of **Perimeter** (Boundary Protection)
- ✓Defense-in-Depth and Layered Architectures (Tiers)
- Role of Network Segmentation (Compartmentalize)
- Security Information and Event Management (SIEMs)
- Quiz

Network Segmentation:

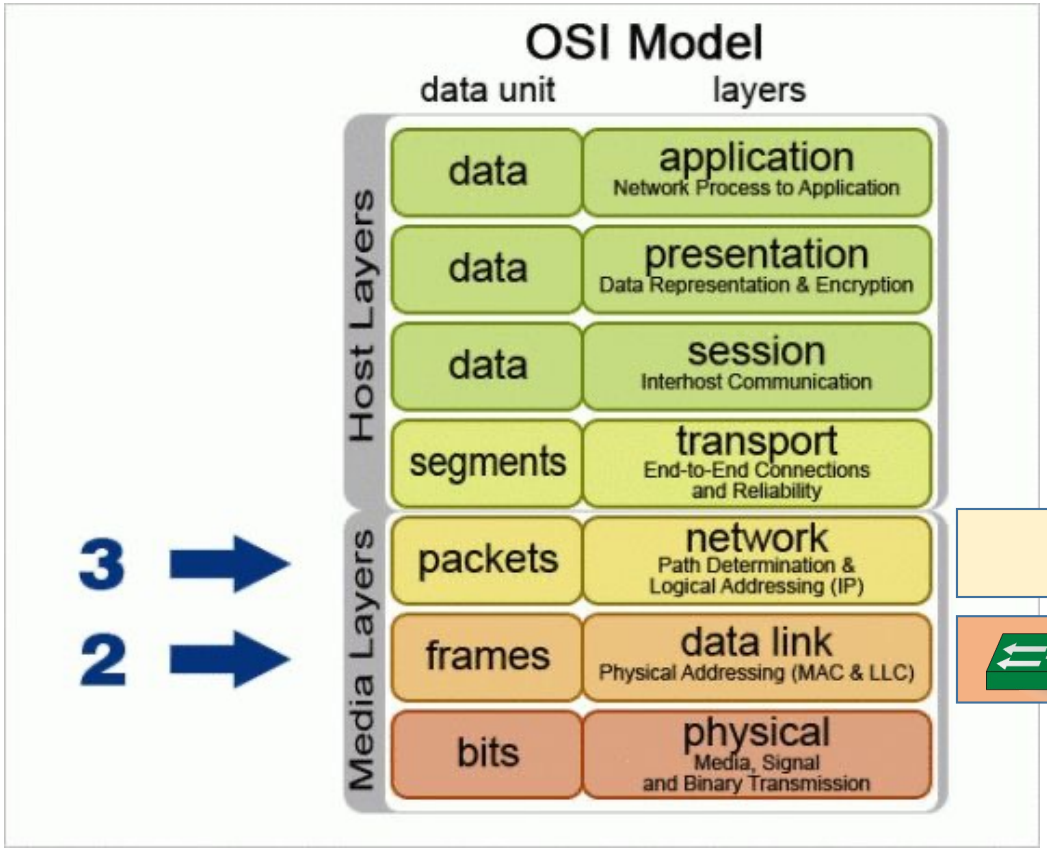
What is it?

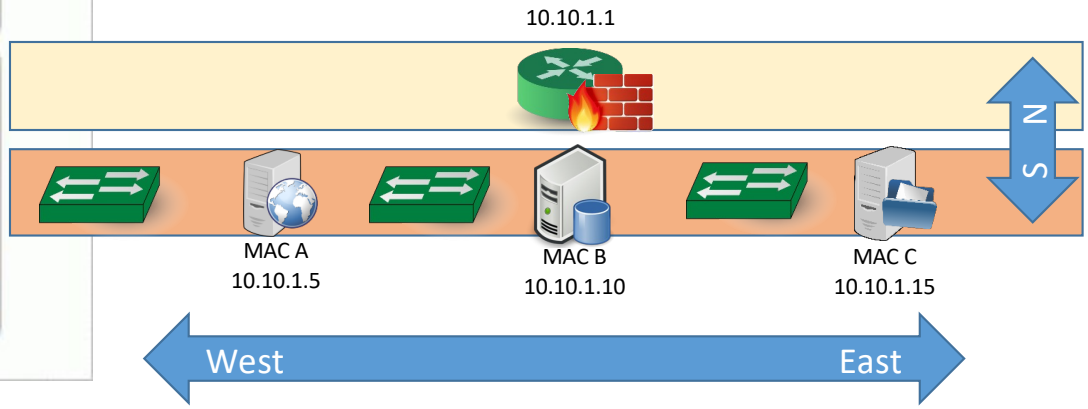
Example Segmented Architecture at Perimeter

"Internet" *"Extranet"* *"Intranet"*



Layer 2: Flat Networks

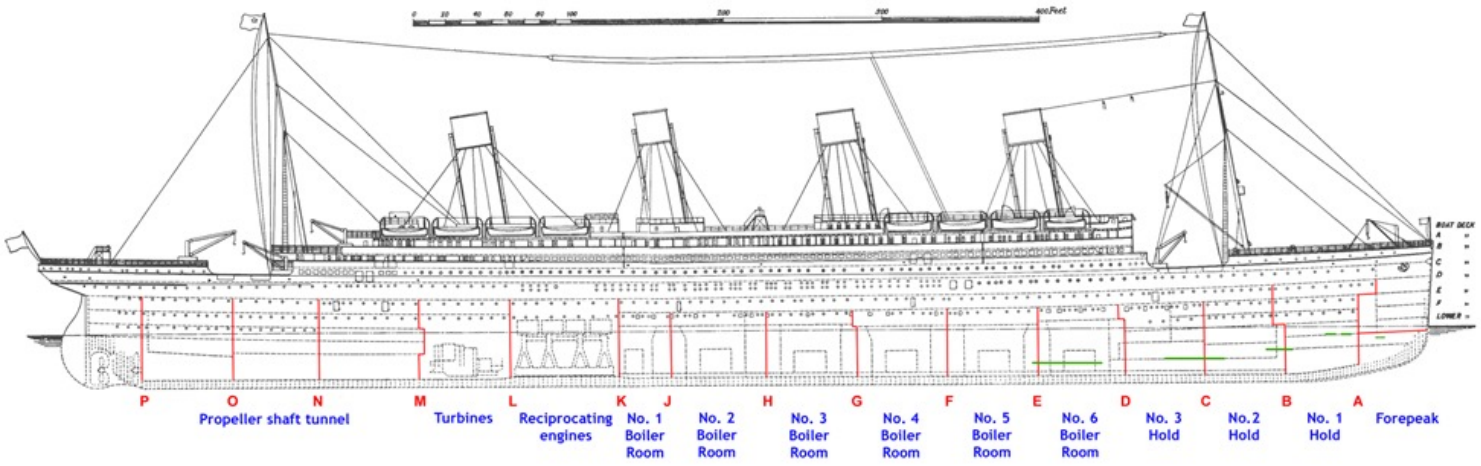




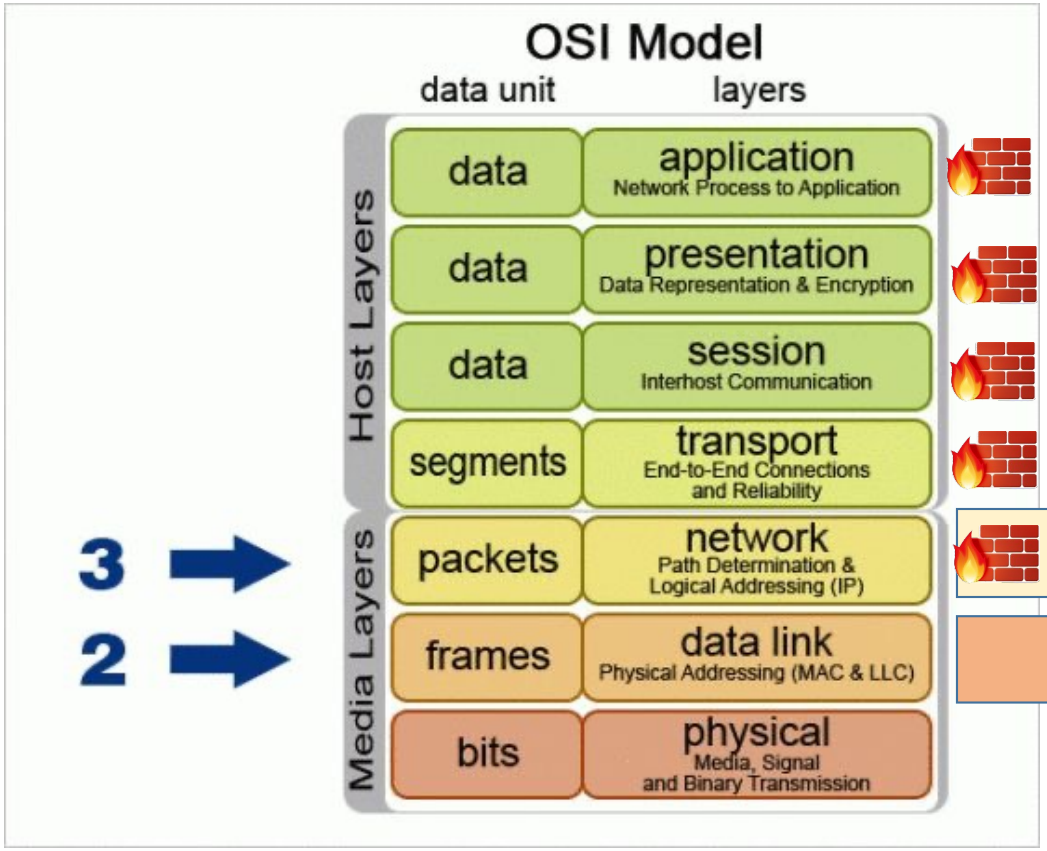
Segmentation

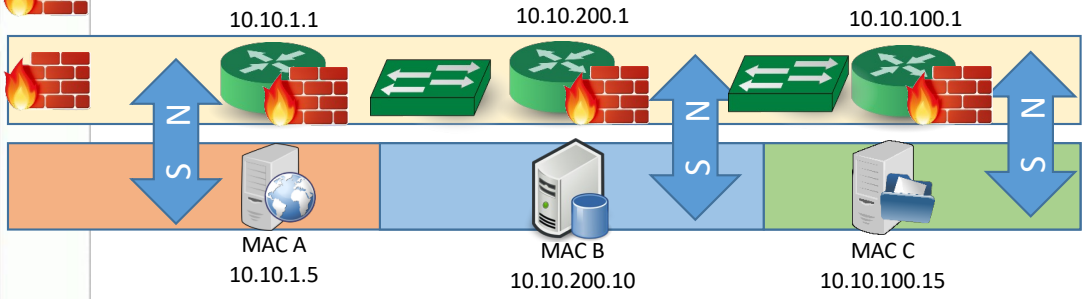
- Network attacks are “multi-vector”, a single safeguard is not enough to see it and stop it. Therefore, defense-in-depth.

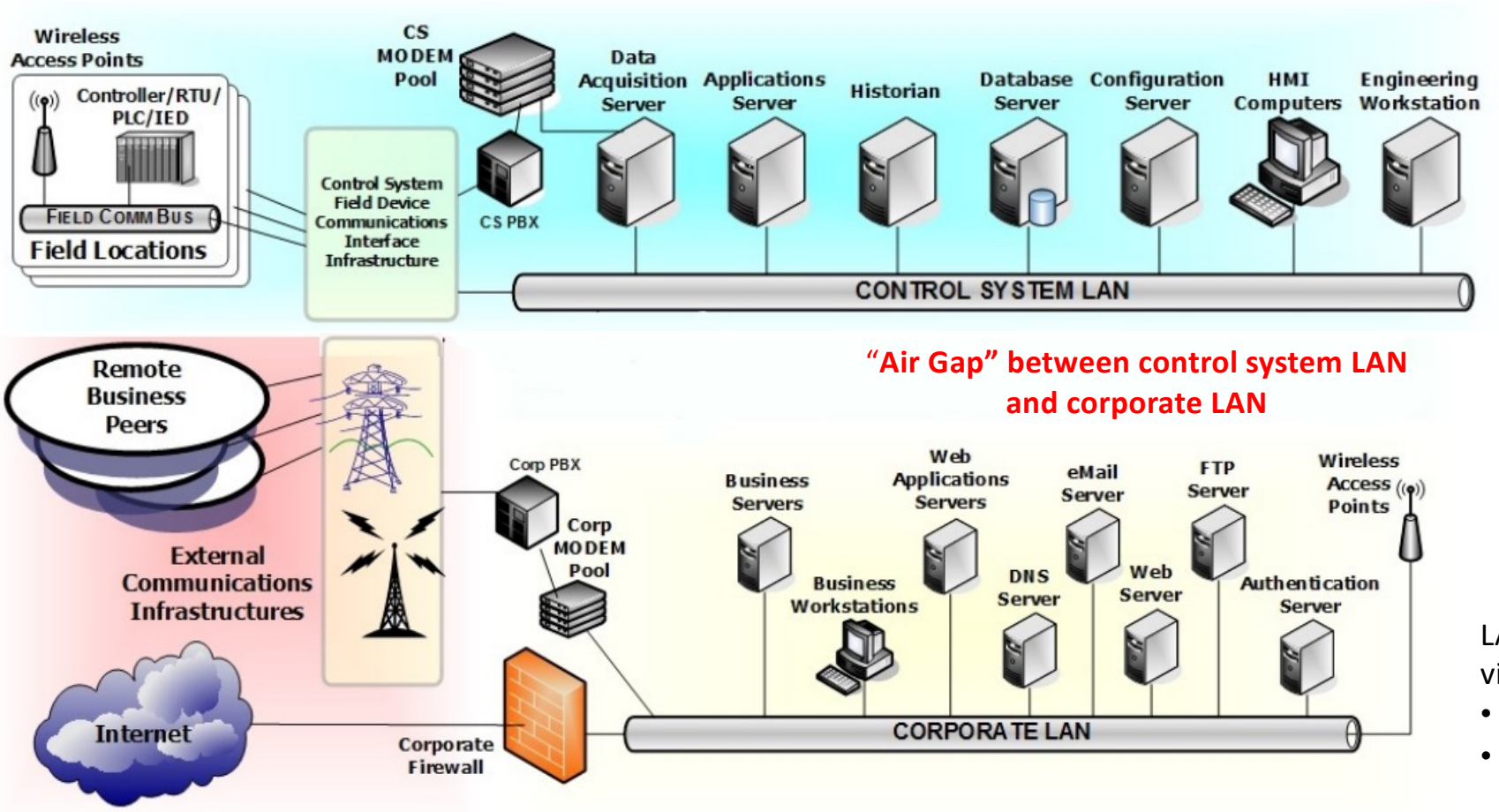
- Golden rule of secure architecture. No compromise of a single element should compromise the whole application stream or network. (compartmentalize)



Layer 3: Tiered Networks



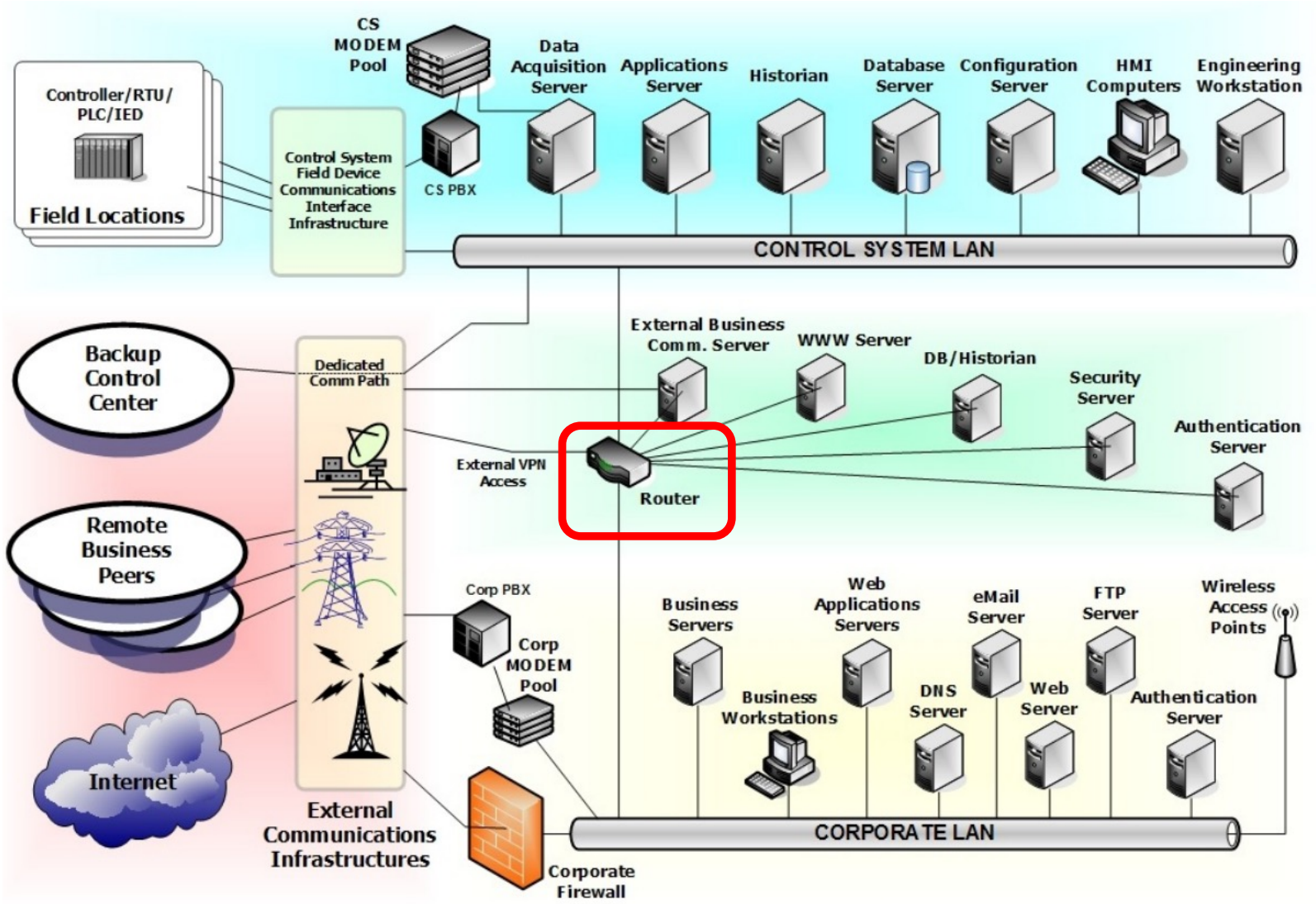




LAN 1 – connected via
- layer 2 switches
- PBX

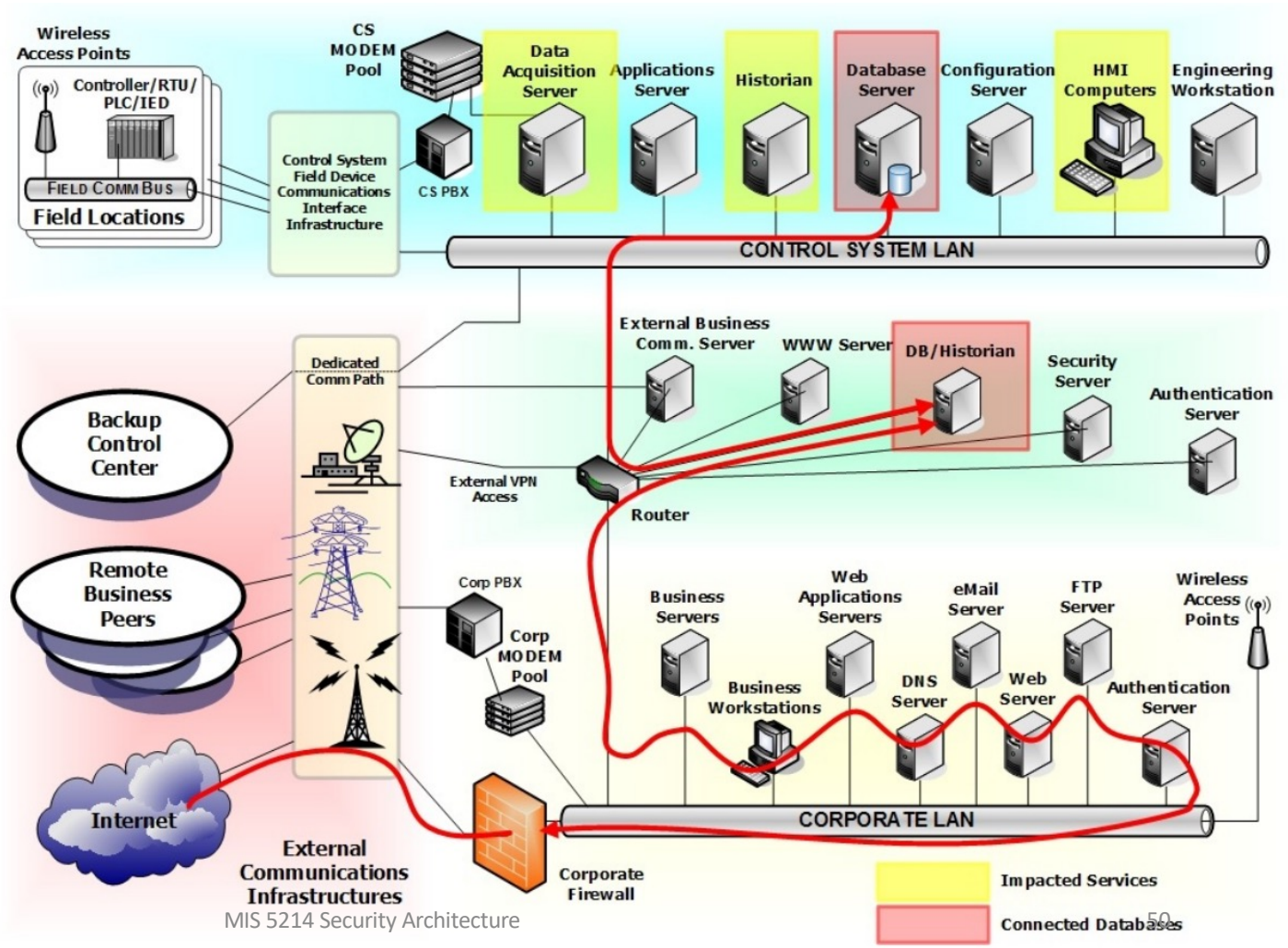
LAN 2 – connected via
- layer 2 switch
- PBX

HMI = Human Machine Interface
CS = Control System
PBX = Private Branch Exchange telephone system switches between users on local lines while allowing users to use a fixed # of external phone lines
RTU = Remote Terminal Unit is a computer controlled device that connects physical machines to distributed control systems
PLC = Programmable Logic Controller
IED = Intelligent End device



Integrated networks

Attack begins at some point outside the control zone, after initial intrusion attacker pries deeper and deeper into the network architecture

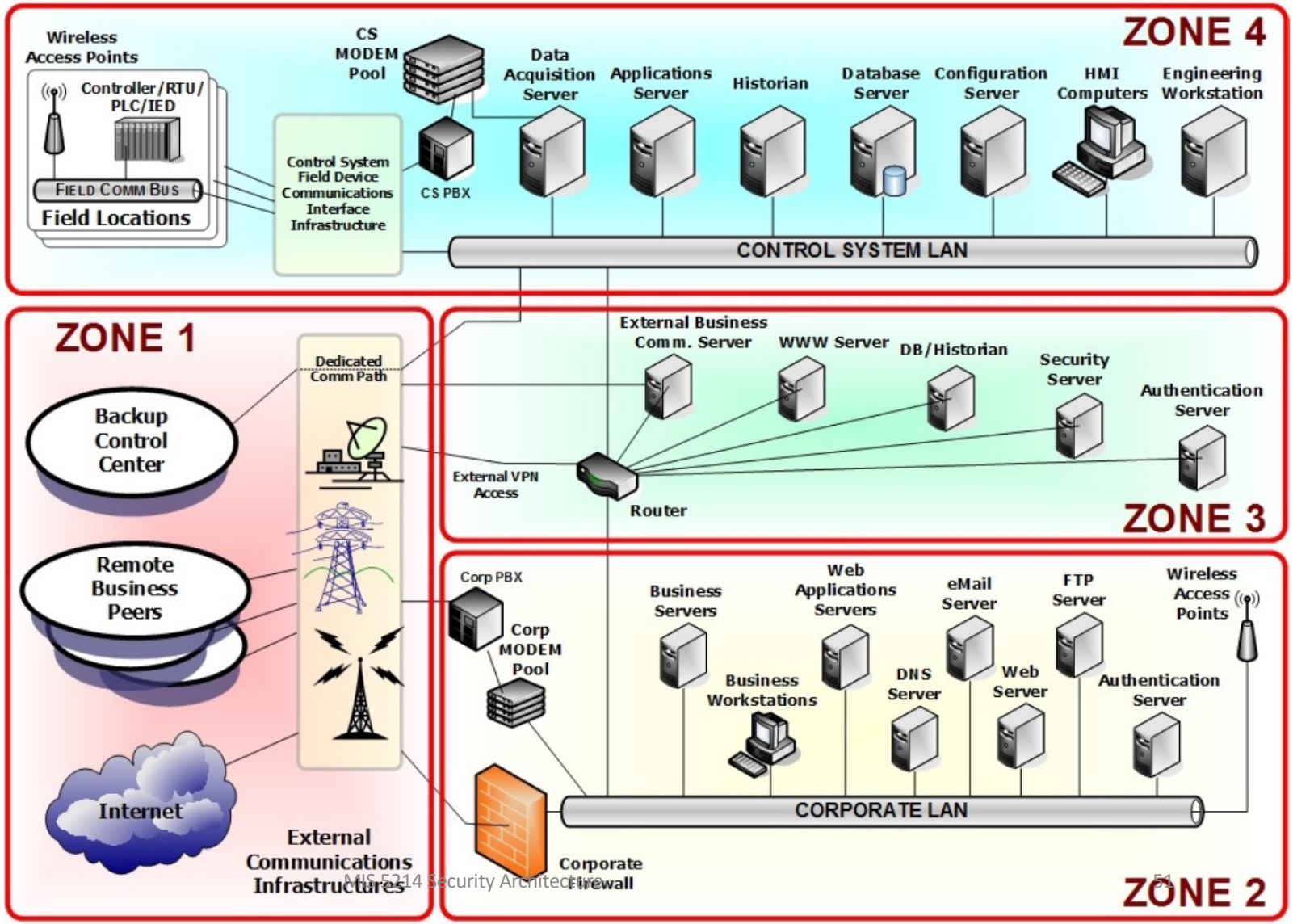


Zone 1: External connectivity to the Internet, peer locations, and back- up facilities

Zone 2: External connectivity for corporate communications

Zone 3: Control systems communications from external services

Zone 4: Control systems operations

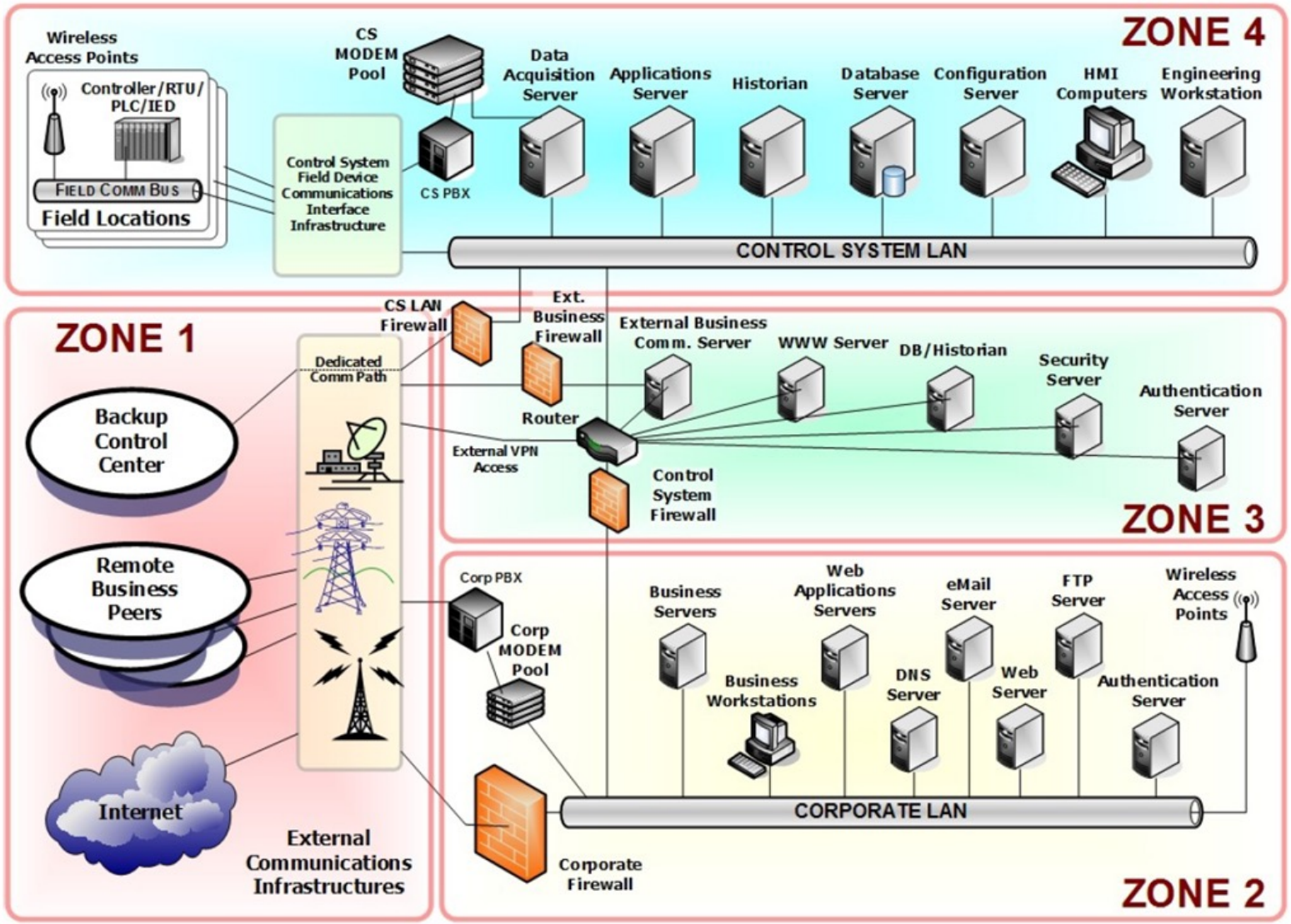


Zone 1: External connectivity to the Internet, peer locations, and back- up facilities

Zone 2: External connectivity for corporate communications

Zone 3: Control systems communications from external services

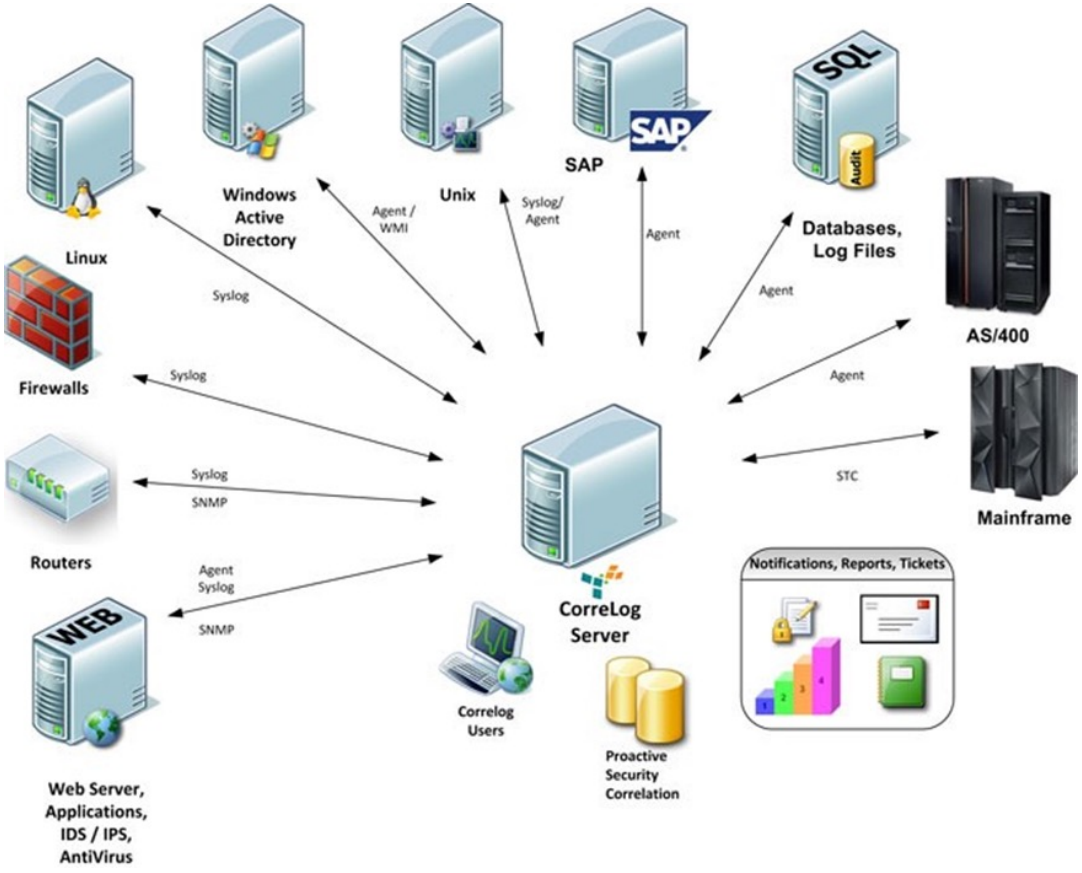
Zone 4: Control systems operations



Agenda

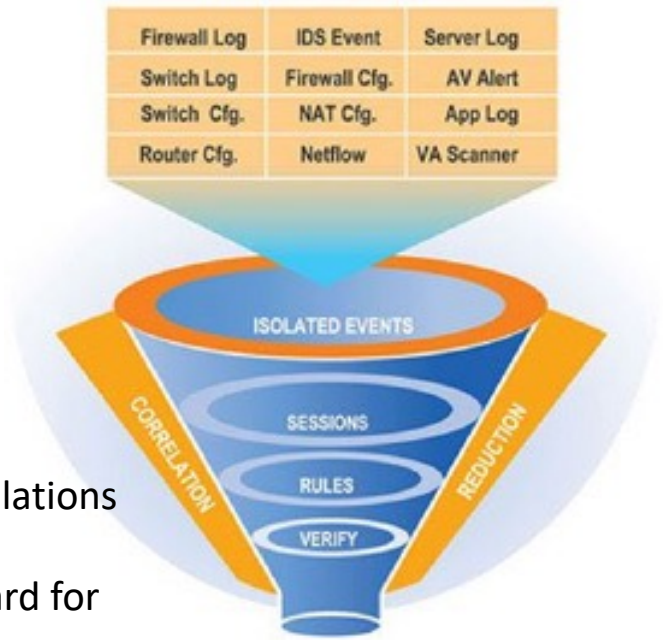
- ✓Open Systems Interconnection Model: Foundation for understanding networks
- ✓Concept of **Perimeter** (Boundary Protection)
- ✓Defense-in-Depth and Layered Architectures (Tiers)
- ✓Role of Network Segmentation (Compartmentalize)
- Security Information and Event Management (SIEMs)
- Quiz

Security Information and Event Management (SIEM)



For continuous monitoring

Data Analysis and Correlation



- Bring raw data events into one database via
  - System logging protocol
  - Monitoring agents
  - Application Programming Interfaces (APIs)

- Program the database software to look for “Notable events” or Correlations

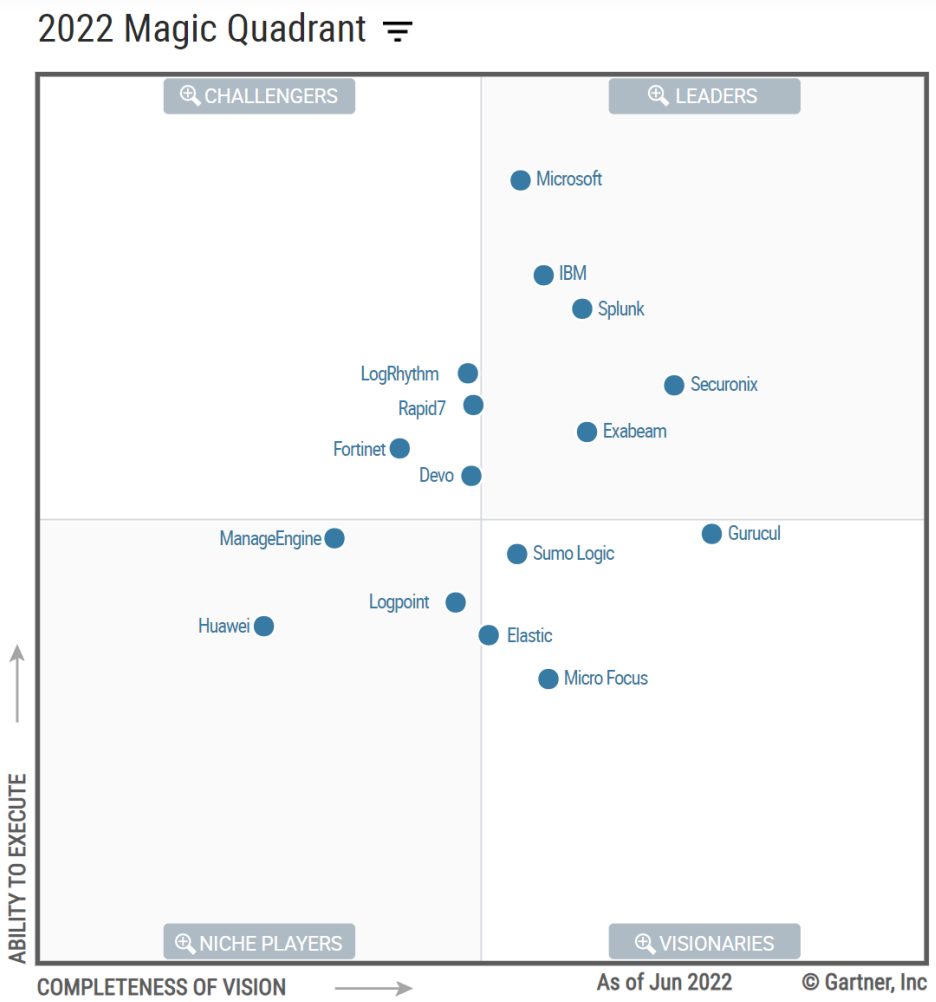
- Correlations will take seemingly isolated events and bring them forward for review/action:
  - **Windows Log:** Employee denied windows login (unknown user account)

  - **Identity Management System:** notes the user account was deleted because employee was terminated last month.

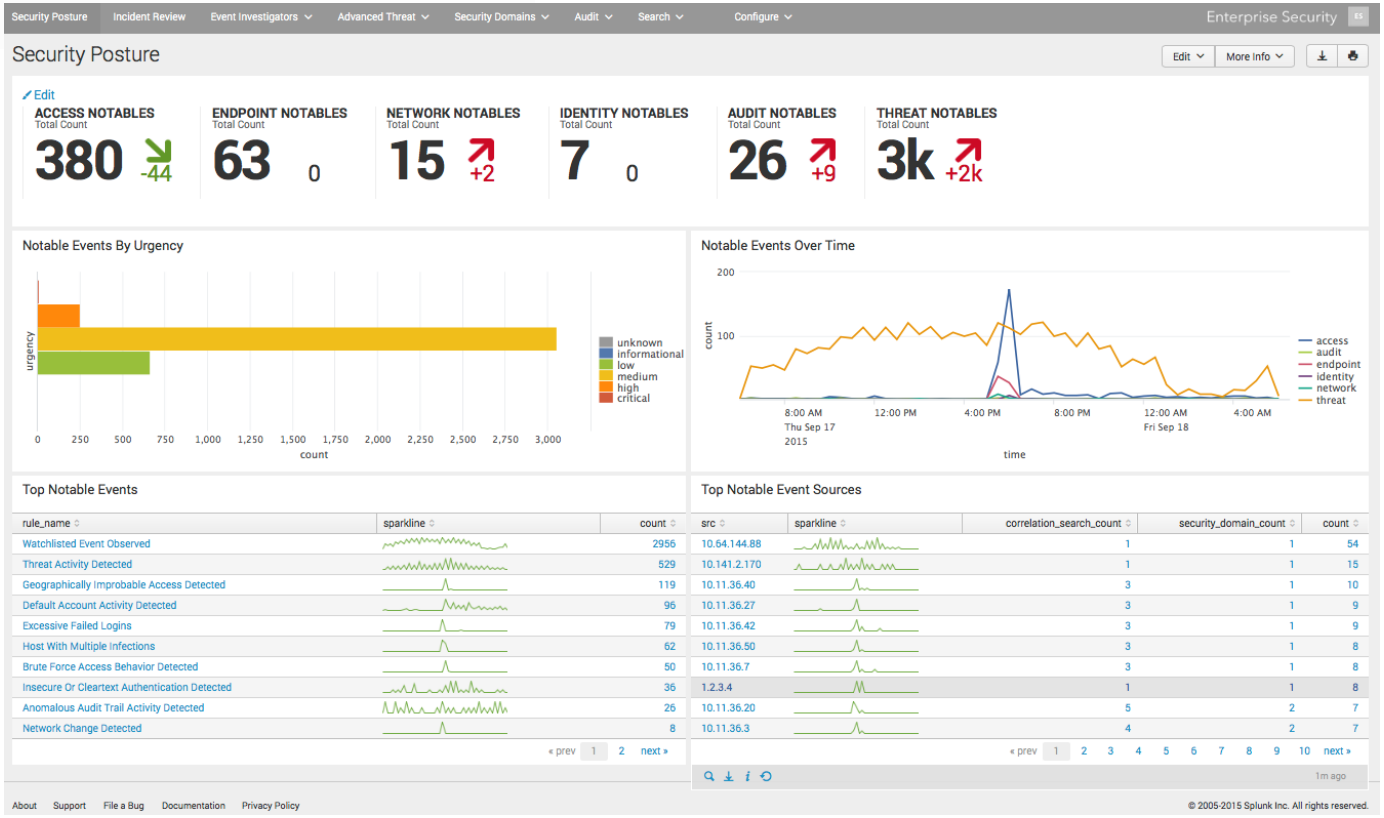
- Security Domains: Endpoints, Networks, Identity, Access

SIEM

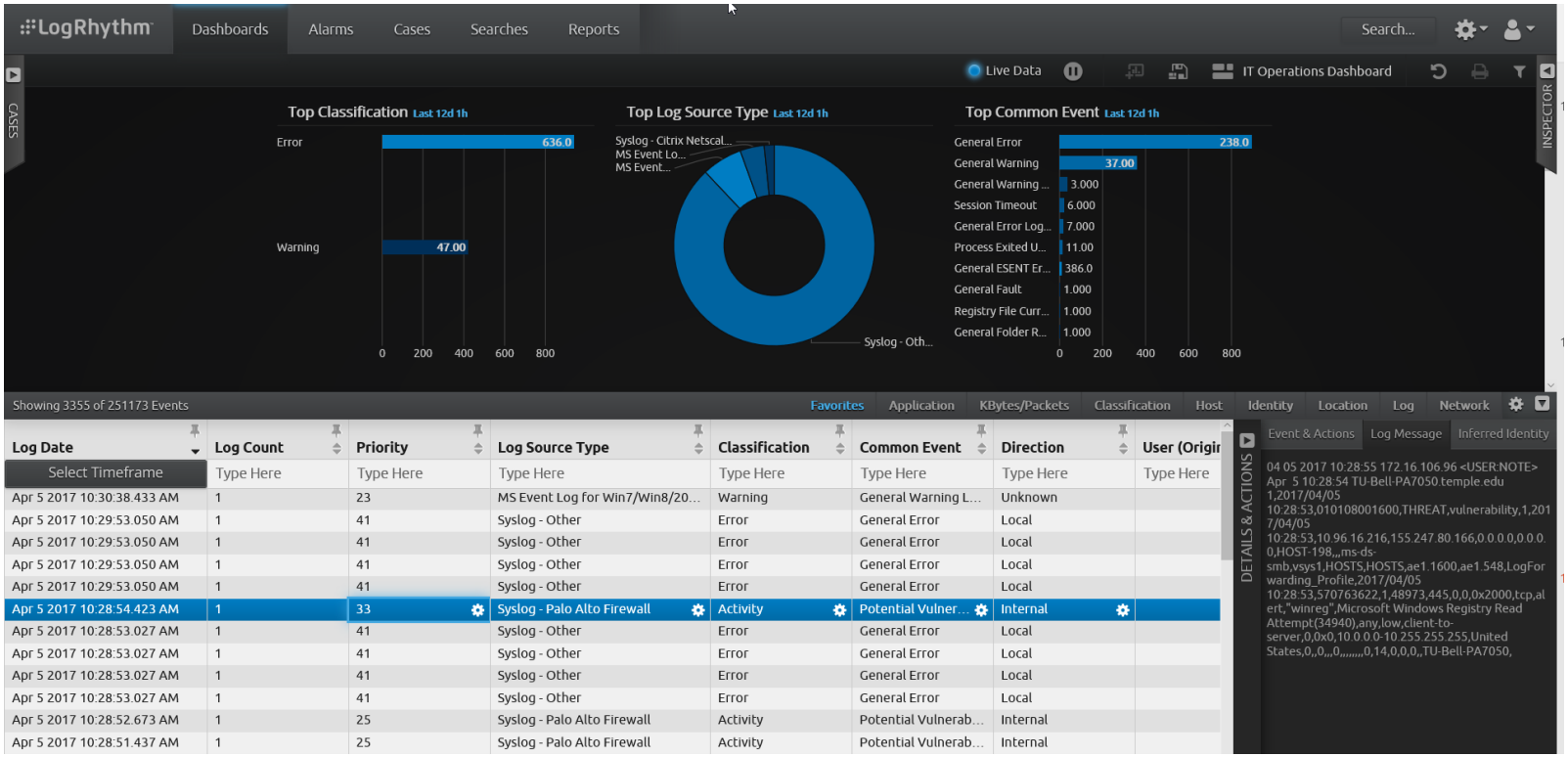
- ***Security Information and Event Management (SIEM)*** market is defined by the customer's need to analyze event data in real time
- Allows for the early detection of targeted attacks and data breaches
- Collect, store, investigate and report on log data for incident response, forensics and regulatory compliance.
- Aggregates event data (logs) produced by security devices, network infrastructure, systems and applications



splunk>

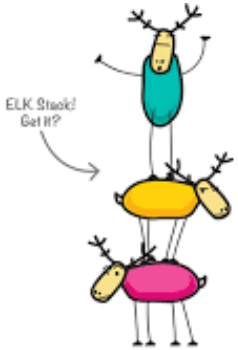

Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Security Posture
Edit
More Info
Edit
ACCESS NOTABLES
Total Count
380
-44
ENDPOINT NOTABLES
Total Count
63
0
NETWORK NOTABLES
Total Count
15
+2
IDENTITY NOTABLES
Total Count
7
0
AUDIT NOTABLES
Total Count
26
+9
THREAT NOTABLES
Total Count
3k
+2k
Notable Events By Urgency
urgency
unknown
informational
low
medium
high
critical
0
250
500
750
1,000
1,250
1,500
1,750
2,000
2,250
2,500
2,750
3,000
count
Notable Events Over Time
200
100
count
access
audit
endpoint
identity
network
threat
8:00 AM
Thu Sep 17
2015
12:00 PM
4:00 PM
8:00 PM
12:00 AM
Fri Sep 18
4:00 AM
time
Top Notable Events
rule_name
sparkline
count
Watchlisted Event Observed 2956
Threat Activity Detected 529
Geographically Improbable Access Detected 119
Default Account Activity Detected 96
Excessive Failed Logins 79
Host With Multiple Infections 62
Brute Force Access Behavior Detected 50
Insecure Or Cleartext Authentication Detected 36
Anomalous Audit Trail Activity Detected 26
Network Change Detected 8
« prev 1 2 next »
Top Notable Event Sources
src
sparkline
correlation_search_count
security_domain_count
count
10.64.144.88 1 1 54
10.141.2.170 1 1 15
10.11.36.40 3 1 10
10.11.36.27 3 1 9
10.11.36.42 3 1 9
10.11.36.50 3 1 8
10.11.36.7 3 1 8
1.2.3.4 1 1 8
10.11.36.20 5 2 7
10.11.36.3 4 2 7
« prev 1 2 3 4 5 6 7 8 9 10 next »
1m ago
About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2015 Splunk Inc. All rights reserved.

LogRhythm™


LogRhythm
Dashboards
Alarms
Cases
Searches
Reports
Search...
Live Data
IT Operations Dashboard
CASES
INSPECTOR
Top Classification Last 12d 1h
Error
636.0
Warning
47.00
0
200
400
600
800
Top Log Source Type Last 12d 1h
Syslog - Citrix Netscal...
MS Event Lo...
MS Event...
Syslog - Oth...
Top Common Event Last 12d 1h
General Error
238.0
General Warning
37.00
General Warning ...
3.000
Session Timeout
6.000
General Error Log...
7.000
Process Exited U...
11.00
General ESENT Er...
386.0
General Fault
1.000
Registry File Curr...
1.000
General Folder R...
1.000
0
200
400
600
800
Showing 3355 of 251173 Events
Favorites
Application
KBytes/Packets
Classification
Host
Identity
Location
Log
Network
Log Date
Log Count
Priority
Log Source Type
Classification
Common Event
Direction
User (Origi
Select Timeframe
Type Here
Apr 5 2017 10:30:38.433 AM 1 23 MS Event Log for Win7/Win8/20... Warning General Warning L... Unknown
Apr 5 2017 10:29:53.050 AM 1 41 Syslog - Other Error General Error Local
Apr 5 2017 10:29:53.050 AM 1 41 Syslog - Other Error General Error Local
Apr 5 2017 10:29:53.050 AM 1 41 Syslog - Other Error General Error Local
Apr 5 2017 10:29:53.050 AM 1 41 Syslog - Other Error General Error Local
Apr 5 2017 10:28:54.423 AM 1 33 Syslog - Palo Alto Firewall Activity Potential Vulner... Internal
Apr 5 2017 10:28:53.027 AM 1 41 Syslog - Other Error General Error Local
Apr 5 2017 10:28:53.027 AM 1 41 Syslog - Other Error General Error Local
Apr 5 2017 10:28:53.027 AM 1 41 Syslog - Other Error General Error Local
Apr 5 2017 10:28:53.027 AM 1 41 Syslog - Other Error General Error Local
Apr 5 2017 10:28:52.673 AM 1 25 Syslog - Palo Alto Firewall Activity Potential Vulnerab... Internal
Apr 5 2017 10:28:51.437 AM 1 25 Syslog - Palo Alto Firewall Activity Potential Vulnerab... Internal
DETAILS & ACTIONS
Event & Actions
Log Message
Inferred Identity
04 05 2017 10:28:55 172.16.106.96 <USER:NOTE>
Apr 5 10:28:54 TU-Bell-PA7050.temple.edu
1,2017/04/05
10:28:53,0101080001600,THREAT,vulnerability,1,2017/04/05
10:28:53,10.96.16.216,155.247.80.166,0.0.0.0,0.0.0.0,HOST-198,,,ms-ds-
smb,vsys1,HOSTS,HOSTS,ae1.1600,ae1.548,LogForwarding_Profile,2017/04/05
10:28:53,570763622,1,48973,445,0,0,0x2000,tcp,alert,"winreg",Microsoft Windows Registry Read
Attempt(34940),any,low,client-to-server,0,0x0,10.0.0.0-10.255.255.255,United
States,0,,0,,,0,,,,,,,,0,14,0,0,0,,TU-Bell-PA7050,

Hybrid – “ELK Stack”

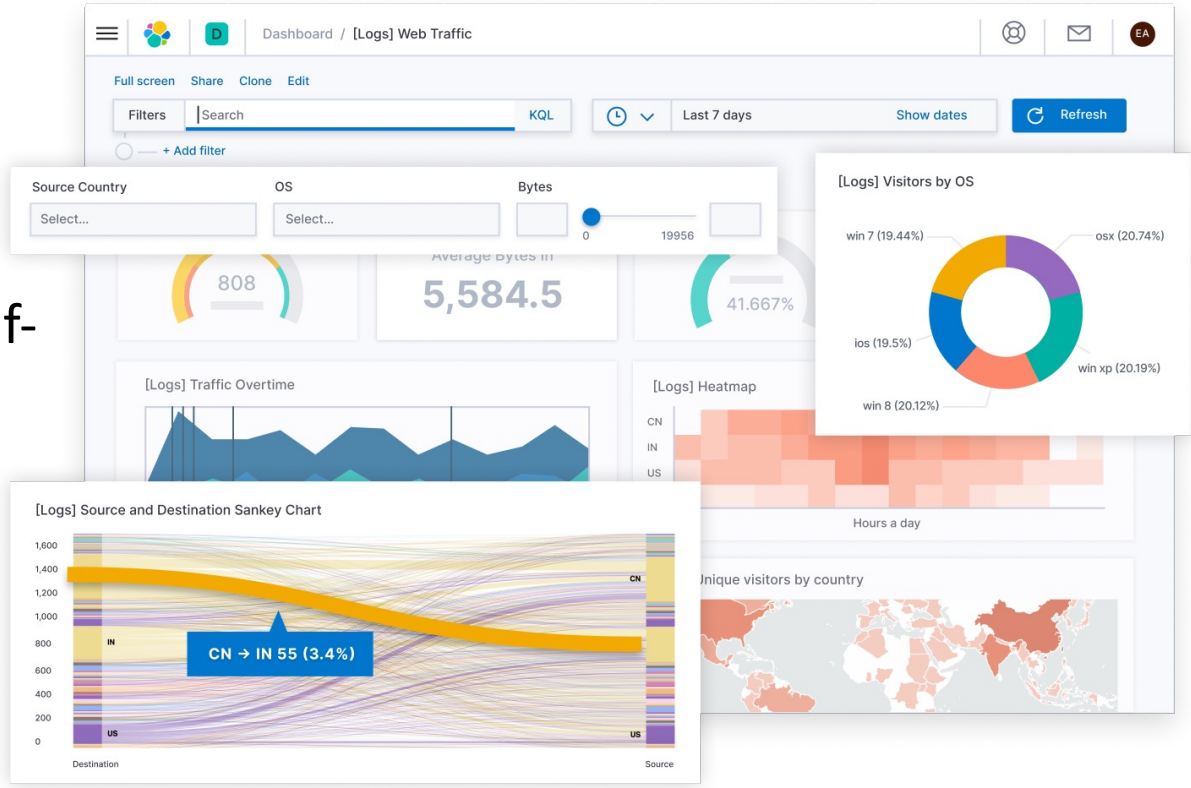
- On-Prem
- Cloud (hosted)
- Kubernetes
- Connectors (Maps for self-managed or air-gapped, Tableau, Hadoop)



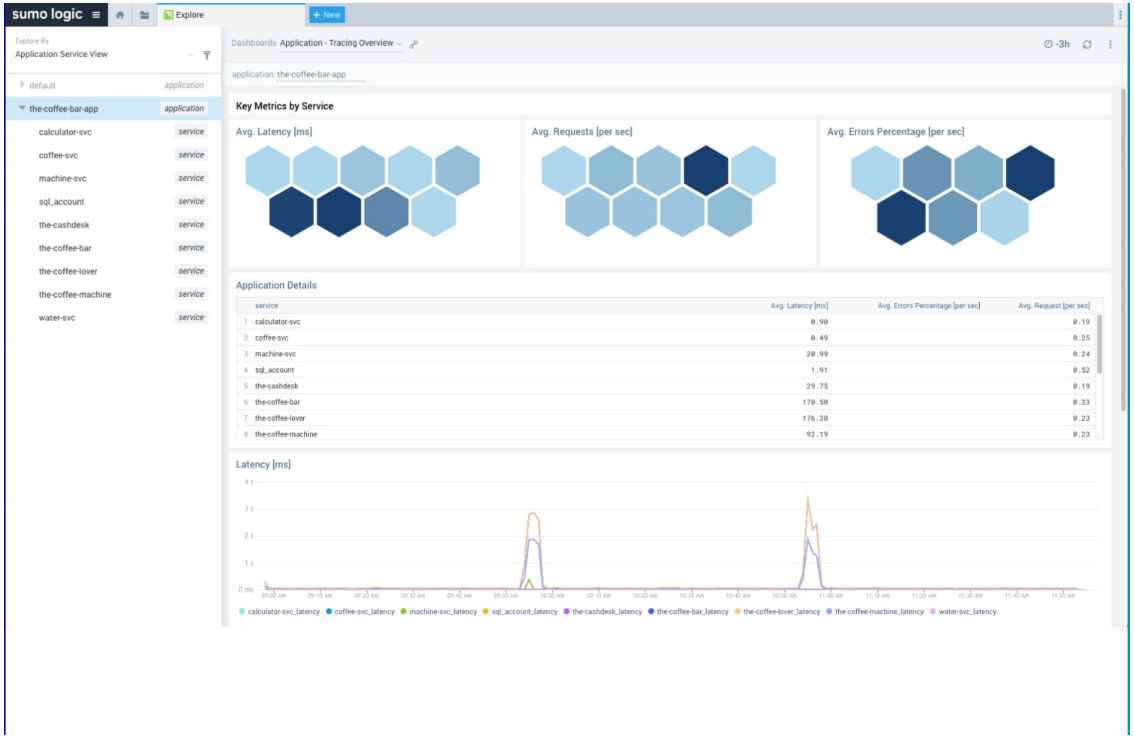
E Elasticsearch

L Logstash

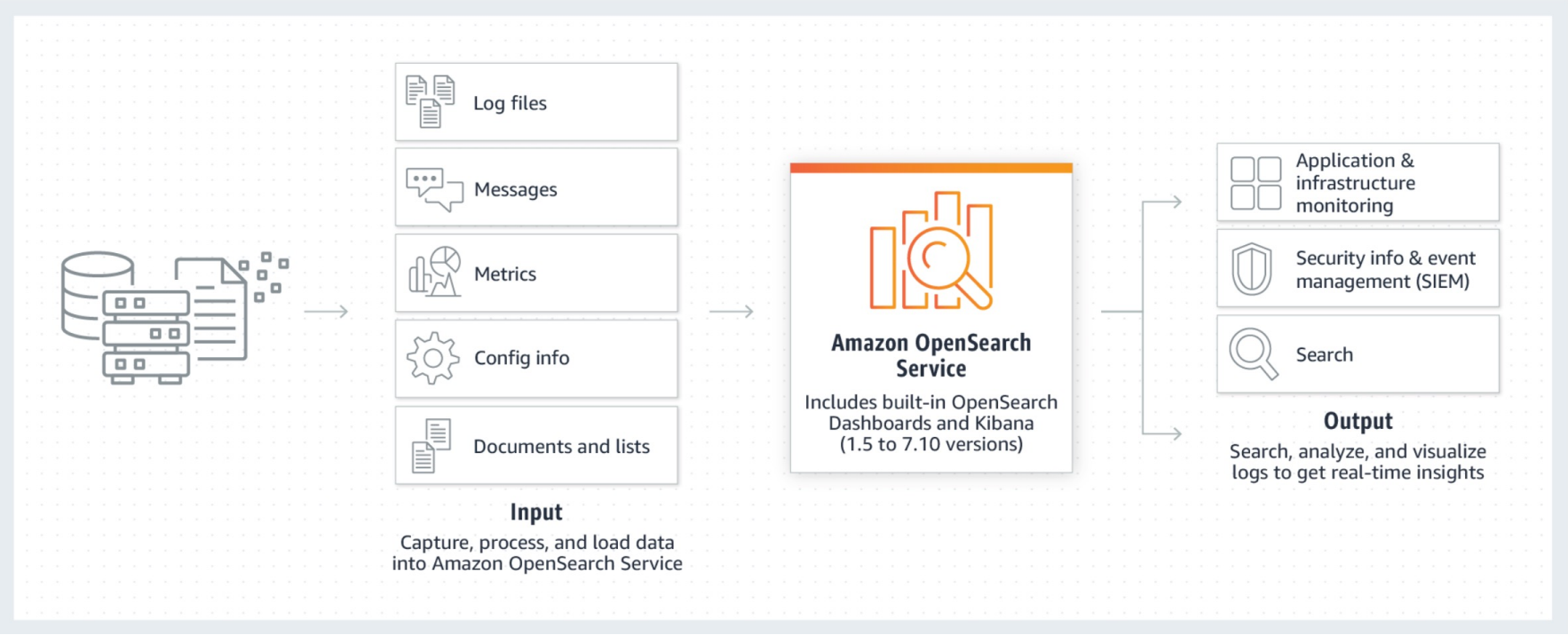
K Kibana



Cloud Based Example - Sumologic



Open-Source Cloud Example – Amazon OpenSearch



Agenda

- ✓Open Systems Interconnection Model: Foundation for understanding networks
- ✓Concept of **Perimeter** (Boundary Protection)
- ✓Defense-in-Depth and Layered Architectures (Tiers)
- ✓Role of Network Segmentation (Compartmentalize)
- ✓Security Information and Event Management (SIEMs)
- Quiz

QUIZ

1. Which of the following best reduces the ability of one device to capture the packets that are meant for another device
   A. Hubs
   B. Switches
   C. Routers
   D. Firewalls

1. Which of the following best reduces the ability of one device to capture the packets that are meant for another device
   A. Hubs
   B. Switches
   C. Routers
   D. Firewalls

QUIZ

2. When reviewing the configuration of network devices, an IS auditor should first identify:
   A. the good practices for the types of network devices deployed.
   B. whether components of the network are missing.
   C. the importance of the network devices in the topology.
   D. whether subcomponents of the network are being used appropriately.

2. When reviewing the configuration of network devices, an IS auditor should first identify:
   A. the good practices for the types of network devices deployed.
   B. whether components of the network are missing.
   C. the importance of the network devices in the topology.
   D. whether subcomponents of the network are being used appropriately.

QUIZ

3. Which of the following network components is primarily set up to serve as a security measure by preventing unauthorized traffic between different segments of the network?
   A. Firewalls
   B. Routers
   C. Layer 2 switches
   D. Virtual local area networks (VLANS)

3. Which of the following network components is primarily set up to serve as a security measure by preventing unauthorized traffic between different segments of the network?
   A. Firewalls
   B. Routers
   C. Layer 2 switches
   D. Virtual local area networks (VLANS)

QUIZ

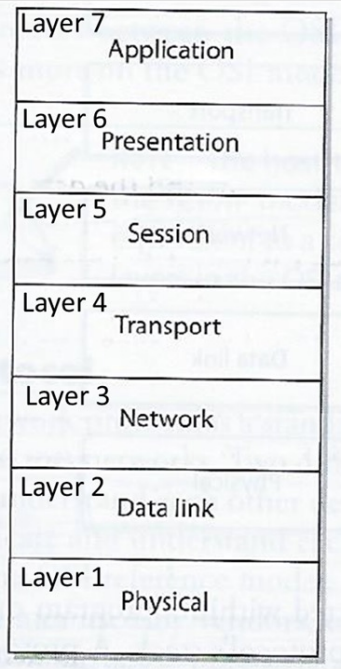
4. During a review of intrusion detection logs, an IS auditor notices traffic coming from the Internet, which appears to originate from the internal IP address of the company payroll server. Which of the following malicious activities would most likely cause this type of result?
   A. A denial-of-service (DoS) attack
   B. Spoofing
   C. Port scanning
   D. A man-in-the middle attack

4. During a review of intrusion detection logs, an IS auditor notices traffic coming from the Internet, which appears to originate from the internal IP address of the company payroll server. Which of the following malicious activities would most likely cause this type of result?
   A. A denial-of-service (DoS) attack
   B. Spoofing
   C. Port scanning
   D. A man-in-the middle attack

QUIZ

5. Which of the following shows the layer sequence as layers 2, 5, 7, 4, and 3
   A. Data link, session, application, transport, and network
   B. Data link, transport, application, session, and network
   C. Network, session, application, network, and transport
   D. Network, transport, application, session, and presentation

5. Which of the following shows the layer sequence as layers 2, 5, 7, 4, and 3
   A. Data link, session, application, transport, and network
   B. Data link, transport, application, session, and network
   C. Network, session, application, network, and transport
   D. Network, transport, application, session, and presentation



QUIZ

6. Systems that are built on the OSI framework are considered open systems. What does this mean?
   A. They do not have authentication mechanisms configured by default.
   B. They have interoperability issues.
   C. They are built with internationally accepted protocols and standards so they can easily communicate with other systems.
   D. They are built with international protocols and standards so they can choose what types of systems they will communicate with.

6. Systems that are built on the OSI framework are considered open systems. What does this mean?
   A. They do not have authentication mechanisms configured by default.
   B. They have interoperability issues.
   C. They are built with internationally accepted protocols and standards so they can easily communicate with other systems.
   D. They are built with international protocols and standards so they can choose what types of systems they will communicate with.

QUIZ

7. What takes place at the session layer?
   A. Dialog control
   B. Routing
   C. Packet sequencing
   D. Addressing

7. What takes place at the session layer?
   A. Dialog control
   B. Routing
   C. Packet sequencing
   D. Addressing

Agenda

- Open Systems Interconnection Model: Foundation for understanding networks
- Concept of Perimeter (Boundary Protection)
- Defense-in-Depth and Layered Architectures (Tiers)
- Role of Network Segmentation (Compartmentalize)
- Security Incident and Event Management (SIEMs)
- Quiz

Protecting Information Assets
- Unit# 10 -

Network Security