CISSP EXAM CRAM

THE COMPLETE COURSE

DOMAIN 4

Communication and Network Security

INSIDE CLOUD AND SECURITY

Exam Outline

4.1 Implement secure **design principles** in network architectures

4.2 Secure **network components**

4.3 Implement secure **communication channels** according to design

WHAT'S NEW IN DOMAIN 4?

4.1 Assess and implement secure design principles in network architectures

Micro-segmentation

- Software Defined Networks (**SDN**)
- Virtual eXtensible Local Area Network (**VXLAN**)
- Encapsulation
- Software-Defined Wide Area Network (**SD-WAN**)

Wireless Networks

- Li-fi
- Zigbee
- Satellite

Cellular Networks

- 4G, 5G

- Content Distribution Networks (CDN)

NETWORK ARCHITECTURES

VXLAN

Virtual
Extensible
LAN

network virtualization enabling network segmentation at high scale.

overcomes VLAN scale limitations – limit is 4096 VLANs versus millions of VXLANs

tunneling protocol that encapsulates an Ethernet frame (layer 2) in a UDP packet.

explained in rfc7348, the VXLAN RFC

layer 2 can generally only be attacked from within (e.g. MAC spoofing, or flooding to cause DoS), such as by a rogue host.

NETWORK ARCHITECTURES

SDN

Software Defined Networks

a network architecture approach that enables the network to be intelligently and centrally controlled, or 'programmed,' using software

and has capacity to reprogram the data plane at any time.

use cases include **SD-LAN** and **SD-WAN**

Separating the control plane from the data plane opens up a number of security challenges

SDN vulnerabilities can include man-in-the-middle attack (MITM) and a service denial (DoS) secure with TLS!

NETWORK ARCHITECTURES

SD-WAN

Software Defined Wide-Area Networks

enables users in branch offices to remotely connect to an enterprise's network

enables use of many network services –MPLS, LTE, and broadband internet, etc. – to securely connect users to applications..

security is based largely on IP security (IPsec), VPN tunnels, next-gen firewalls (NGFWs), and the micro-segmentation of application traffic

uses a centralized control function for intelligent routing and secure access service edge (SASE) to decentralize connectivity

NETWORK ARCHITECTURES

LiFi

Light Fidelity

uses the modulation of light intensity to transmit data (uses LED).

can safely function in areas otherwise susceptible to electromagnetic interference

can theoretically transmit at speeds of up to 100 Gbit/s

✓ LI-FI only requires working LED lights

X visible light is that it cannot penetrate opaque walls.

NETWORK ARCHITECTURES

LiFi

Light Fidelity

uses the modulation of light intensity to transmit data (uses LED).

can safely function in areas otherwise susceptible to electromagnetic interference

can theoretically transmit at speeds of up to 100 Gbit/s

✓ LI-FI only requires working LED lights

✓ visible light is that it cannot penetrate opaque walls.

NETWORK ARCHITECTURES

Zigbee

Personal Area Network (PAN)

IoT smart home hub

A short-range wireless PAN (Personal Area Network) technology developed to support automation, machine-to-machine communication, remote control and monitoring of IoT devices.

supports both **centralized** and **distributed security models,** and **mesh** topology

assumes that symmetric keys used are transmitted securely (encrypted in-transit)

During pre-configuration of a new device, in which a single key might be sent unprotected, creating a brief vulnerability.

CELLULAR NETWORKING

5G

5th Generation Cellular

- Faster speeds and lower latency
- Unlike 4G, 5G doesn't identify each user through their SIM card. Can assign identities to each device.
- Some air interface threats, such as session hijacking, are dealt with in 5G.
- Standalone (SA) version of 5G will be more secure than the non-standalone (NSA) version

NSA anchors the control signaling of 5G networks to the 4G Core

CELLULAR NETWORKING

5G

5th Generation Cellular

Diameter protocol, which provides authentication, authorization, and accounting (AAA), will be a target.

Because 5G has to work alongside older tech (3G/4G), old vulnerabilities may be targeted.

Because scale of IoT endpoint counts on 5G is exponentially greater, **DDoS** is a concern.

Some carriers originally launched an NSA version of 5G, which continues to rely on availability of the 4G core.

CONTENT DELIVERY NETWORKS (CDN)

a geographically distributed network of proxy servers and their data centers.

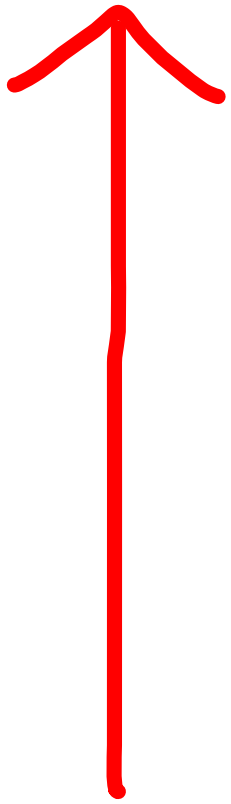
goal is fast and highly available content delivery by distributing content **spatially relative (close to)** users.

CDN networks serving JavaScript have been targeted to inject malicious content into pages.

examples: video and audio streaming, software downloads, etc.

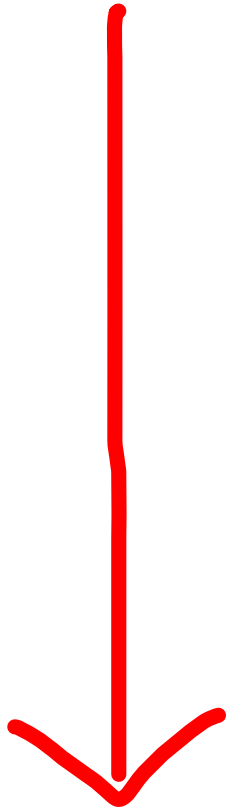
Vendors in CDN space offer **DDoS protection** and **web application firewalls (WAF)**

THE OSI MODEL



Away
Pizza
Sausage
Throw
Not
Do
Please

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical



All
People
Seem
To
Need
Data
Processing

THE OSI MODEL

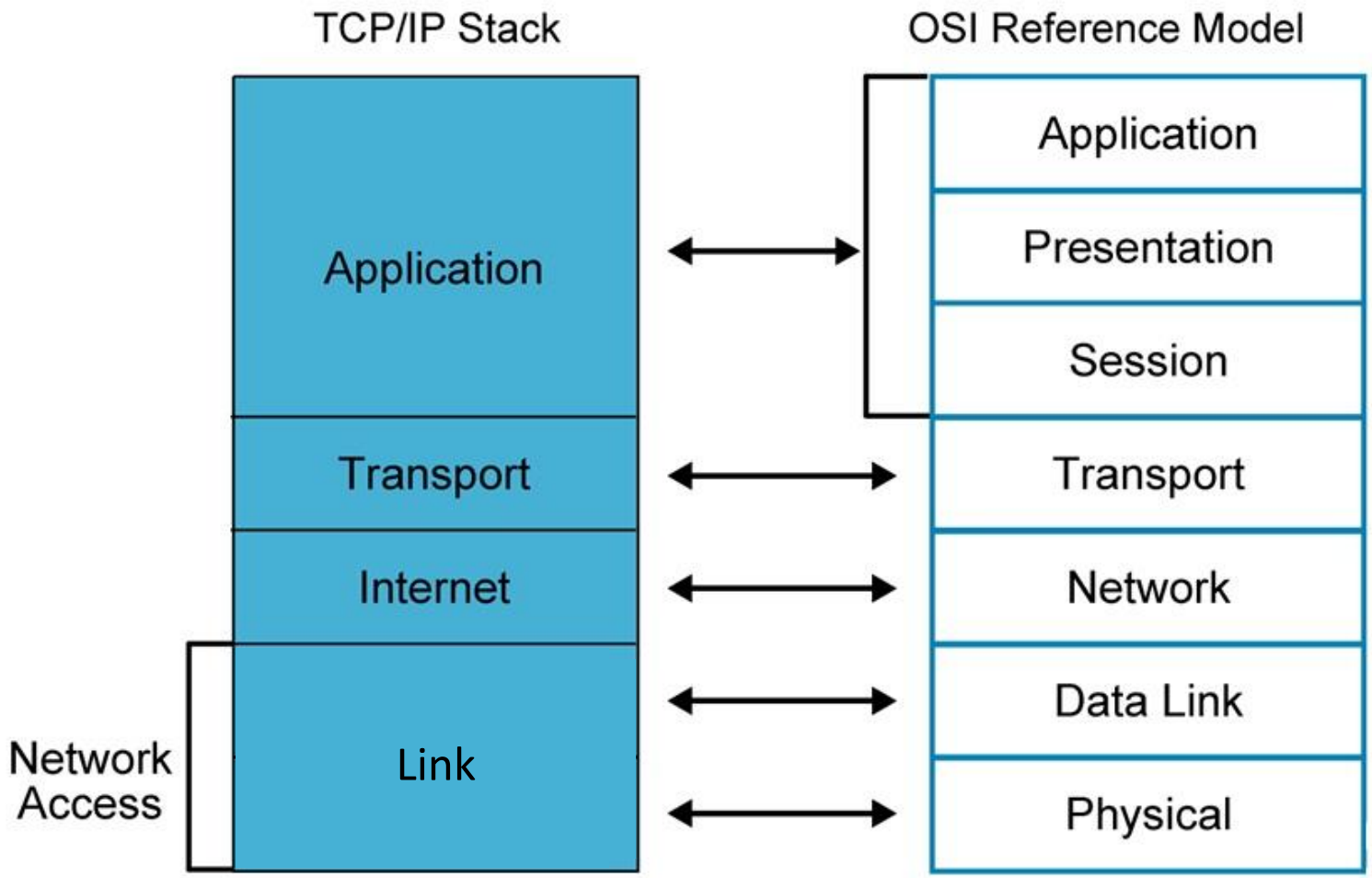
7	Application	SSH, HTTP, FTP, LPD, SMTP, Telnet, TFTP, EDI, POP3, IMAP, SNMP, NNTP, S-RPC, and SET
6	Presentation	Encryption protocols and format types, such as ASCII, EBCDICM, TIFF, JPEG, MPEG, MIDI
5	Session	SMB, RPC, NFS, and SQL
4	Transport	SPX, SSL, TLS, TCP, and UDP
3	Network	ICMP, RIP, OSPF, BGP, IGMP, IP, IPSec, IPX, NAT, and SKIP
2	Data Link	ARP, SLIP, PPP, L2F, L2TP, PPTP, FDDI, ISDN
1	Physical	EIA/TIA-232, EIA/TIA-449, X.21, HSSI, SONET, V.24, V.35, Bluetooth, 802.11 - Wifi, and Ethernet

COMMON TCP/UDP PORTS

PROTOCOL	TCP/UDP	Port
File Transfer Protocol (FTP)	TCP	20/21
Secure Shell (SSH)	TCP	22
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name System (DNS)	TCP/UDP	53
Dynamic Host Configuration Protocol (DHCP)	UDP	67/68
Trivial File Transfer Protocol (TFTP)	UDP	69
Hypertext Transfer Protocol (HTTP)	TCP	80
Post Office Protocol (POP3)	TCP	110
Network Time Protocol (NTP)	UDP	123

PROTOCOL	TCP/UDP	Port
NetBIOS	TCP/UDP	137/138/139
Internet Message Access Protocol (IMAP)	TCP	143
Simple Network Mgmt Protocol (SNMP)	TCP/UDP	161/162
Border Gateway Protocol (BGP)	TCP	179
Lightweight Directory Access Protocol (LDAP)	TCP/UDP	389
HTTP over SSL/TLS (HTTPS)	TCP	443
LDAP over TLS/SSL	TCP/UDP	636
FTP over TLS/SSL	TCP	989/990

TCP vs OSI


TCP/IP Stack
OSI Reference Model
Application
Transport
Internet
Link
Network Access
Application
Presentation
Session
Transport
Network
Data Link
Physical

TCP vs UDP

No.	TCP	UDP
1	**Connection oriented**	Connection-less protocol
2	**Byte** stream	**Message** stream
3	No support for multicasting/broadcasting	Supports **multicasting/broadcasting**
4	Supports **full duplex** transmission	No support for full duplex transmission
5	**Reliable** service of data transmission	Unreliable service of data transmission
6	TCP packet is called a **segment**	UDP packet is called a **datagram**
7	Provides **error detection** and **flow control**	No support for error detection and flow control

CABLING TYPES & THROUGHPUT

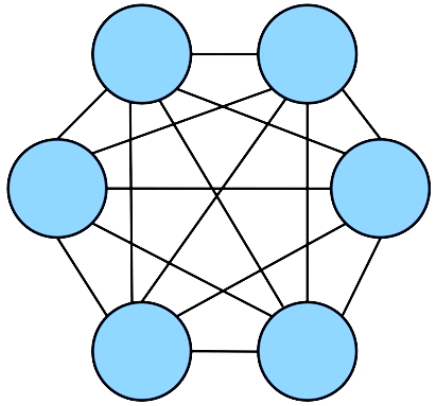
UTP Categories - Copper Cable				
UTP Category	**Data Rate**	**Max. Length**	**Cable Type**	**Application**
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

CABLING TYPES & THROUGHPUT

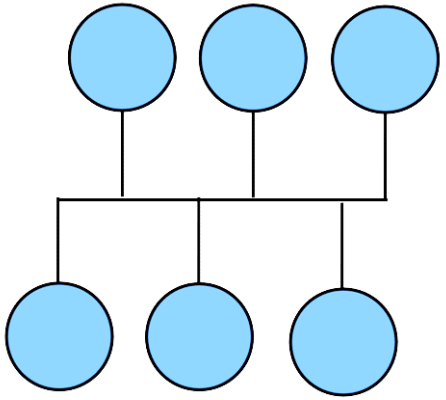
Type	Max speed	Distance	Difficulty of installation	Susceptibility to EMI
10Base2	10 Mbps	185 meters	Medium	Medium
10Base5	10 Mbps	500 meters	High	Low
10BaseT (UTP)	10 Mbps	100 meters	Low	High
STP	155 Mbps	100 meters	Medium	Medium
100BaseT/100BaseTX	100 Mbps	100 meters	Low	High
1000BaseT	1 Gbps	100 meters	Low	High
Fiber-optic	2+ Gbps	2+ kilometers	High to medium	None

UTP = unshielded twisted pair

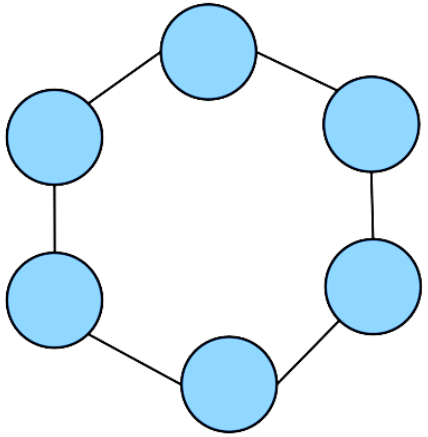
STANDARD NETWORK TOPOLOGIES



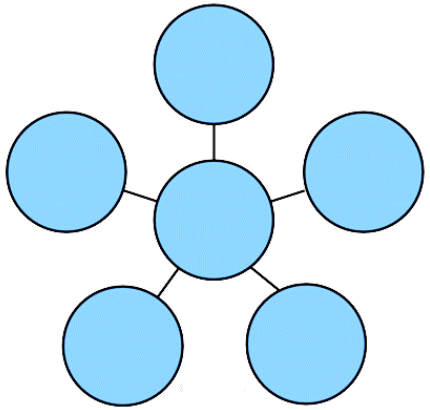
MESH



BUS

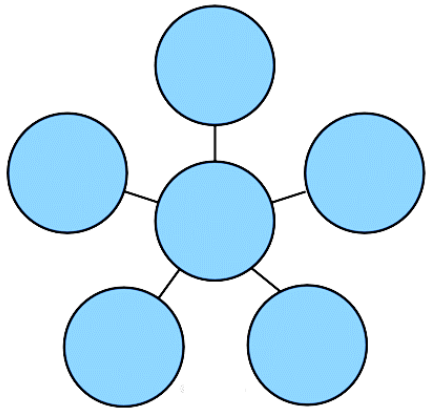


RING



STAR

STANDARD NETWORK TOPOLOGIES



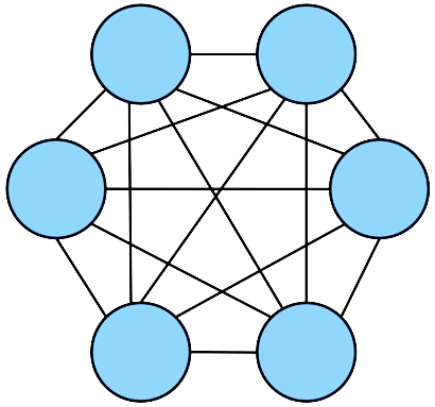
STAR

Employs a centralized connection device.

Can be a simple hub or switch.

Each system is connected to the **central hub** by a dedicated segment

STANDARD NETWORK TOPOLOGIES



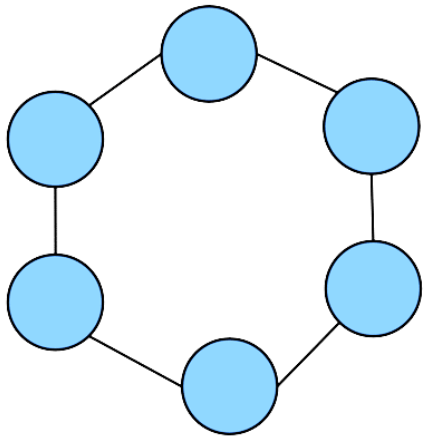
MESH

Connects systems to all other systems using numerous paths.

A partial mesh topology connects many systems to many other systems.

Provides **redundant connections** to systems, allowing multiple segment failures without seriously affecting connectivity.

STANDARD NETWORK TOPOLOGIES



RING

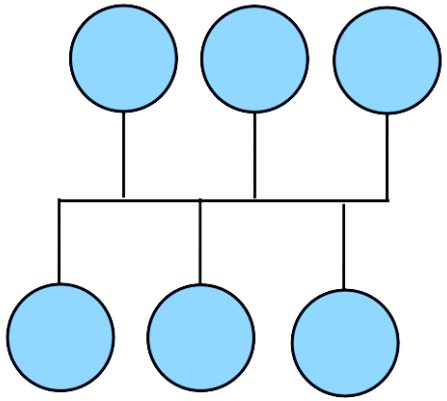
Connects each system as points on a circle.

The connection medium acts as a unidirectional transmission loop.

Only one system can transmit data at a time. Traffic management is performed by a token.

Token ring is a ring-based network

STANDARD NETWORK TOPOLOGIES



BUS

Connects each system to a trunk or backbone cable.

All systems on the bus can transmit data simultaneously, which can result in collisions.

A collision occurs when two systems transmit data at the same time; the signals interfere with each other.

Ethernet is a bus network

ANALOG vs DIGITAL

Analog

Communications occur with a continuous signal that varies in frequency, amplitude, phase, voltage, and so on.

The variances in the continuous signal produce a wave shape (as opposed to the square shape of a digital signal).

The actual communication becomes altered and corrupted because of attenuation over long distances and interference.

Digital

Communications occur through the use of a discontinuous electrical signal and a state change or on-off pulses.

More reliable than analog signals over long distances or when interference is present because of a digital signal's definitive information storage method

Uses current voltage where voltage on represents a value of 1 and voltage off represents a value of 0. These on-off pulses create a stream of binary data.

SYNCHRONOUS vs ASYNCHRONOUS

Some communications are synchronized with some sort of clock or timing activity, and are **synchronous** or **asynchronous**:

Synchronous

Communications rely on a timing or clocking mechanism based on either an independent clock or a time stamp embedded in the data stream.

Are typically able to support very high rates of data transfer. example: networking

Asynchronous

Communications rely on a stop and start delimiter bit to manage the transmission of data.

Best suited for smaller amounts of data.

example: public switched telephone network (PSTN) modems

BASEBAND vs BROADBAND

Baseband

can support only a single communication channel.

it uses a direct current applied to the cable. A current that is at a higher level represents the binary signal of 1, and a lower level is binary signal of 0

is a form of digital signal. example: ethernet

Broadband

can support multiple simultaneous signals. uses frequency modulation to support numerous channels,

each supporting a distinct communication session. suitable for high throughput rates, especially when several channels are multiplexed.

is a form of analog signal. TV, cable modem, ISDN, DSL, T1, T3

BROADCAST, MULTICAST, UNICAST

Broadcast, Multicast, and Unicast

Broadcast, multicast, and unicast technologies determine how many destinations a single transmission can reach:

Broadcast technology supports communications to all possible recipients.

Multicast technology supports communications to multiple specific recipients.

Unicast technology supports only a single communication to a specific recipient.

CARRIER SENSE MULTIPLE ACCESS (CSMA)

Developed to decrease the chances of collisions when two or more stations start sending their signals over the datalink layer. Requires that each station first **check the state of the medium** before sending.

CSMA, CSMA/CA, CSMA/CD

CSMA variations and collisions

CSMA
does not directly address collisions.

CSMA/CA (collision avoidance)
attempts to avoid collisions by granting only a single permission to communicate at any given time.

CSMA/CD (collision detection)
responds to collisions by having each member of the collision domain wait for a short but random period of time before starting the process over.

CSMA, CSMA/CA, CSMA/CD

NO.	CSMA/CD detection	CSMA/CA avoidance
1	CSMA / CD is effective **after a collision**.	Whereas CSMA / CA is effective **before a collision**.
2	CSMA / CD is used in **wired** networks.	Whereas CSMA / CA is commonly used in **wireless** networks.
3	It only reduces the **recovery time**.	Whereas CSMA/ CA minimizes the **possibility of collision**.
4	CSMA / CD resends the data frame whenever a conflict occurs.	Whereas CSMA / CA will first transmit the intent to send for data transmission.
5	CSMA / CD is **used in 802.3** standard.	While CSMA / CA is **used in 802.11** standard.
6	It is more efficient than simple CSMA(Carrier Sense Multiple Access).	Is similar to simple CSMA (Carrier Sense Multiple Access) in terms of efficiency.

TOKEN PASSING, POLLING

Token passing

Prevents collisions in ring networks

Performs communications using a **digital token**. Once its transmission is complete, it releases the token to the next system.

Polling

used by SDLC

Performs communications using a **master-slave configuration**. The primary system polls each secondary system in turn whether they have a need to transmit data.

NETWORK SEGMENTATION

Intranet

a private network that is designed to host the same information services found on the Internet.

Extranet

a cross between Internet & intranet

a section of an organization's network that has been sectioned off to act as an intranet for the private network but also serves information to the public Internet.

DMZ

perimeter

an extranet for public consumption is typically labeled a demilitarized zone **(DMZ)** or **perimeter network**.

used to control traffic and isolate static/sensitive environments

NETWORK SEGMENTATION

Reasons for segmentation

Boosting Performance

can improve performance through an organizational scheme in which systems that often communicate are located in the same segment, while systems that rarely or never communicate are located in other segments.

Reducing Communication Problems

reduces congestion and contains communication problems, such as broadcast storms, to individual subsections of the network.

Providing Security

can also improve security by isolating traffic and user access to those segments where they are authorized.

BLUETOOTH

Bluetooth

(IEEE 802.15)

Bluetooth, or IEEE 802.15, personal area networks (PANs) are another area of wireless security concern.

Connects headsets for cell phones, mice, keyboards, GPS, and other devices

Connections are set up using pairing, where primary device scans the 2.4 GHz radio frequencies for available devices

Pairing uses a 4-digit code (often 0000) to reduce accidental pairings but is not actually secure.

MOBILE SYSTEM ATTACKS

BLUEJACKING (annoyance)

Think of it as a high-tech version of ding-dong-ditch, where savvy pranksters push unsolicited messages to engage or annoy other nearby Bluetooth users by taking advantage of a loophole in the technology's messaging options.

BLUESNARFING (data theft)

With bluesnarfing, thieves wirelessly connect to some early Bluetooth-enabled mobile devices without the owner's knowledge to download and/or alter phonebooks, calendars or worse.

BLUEBUGGING

An attack that grants hackers remote control over the feature and functions of a Bluetooth device. This could include the ability to turn on the microphone to use the phone as an audio bug.

WIRELESS TECHNOLOGIES (CONT)

Version	Speed	Frequency
★ 802.11	2 Mbps	2.4 GHz
802.11a	54 Mbps	5 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	54 Mbps	2.4 GHz
802.11n	200+ Mbps	2.4 GHz
802.11ac	1 Gbps	5 GHz

802.11 standard also defines WEP

SSID BROADCAST

SSID
Broadcast

Wireless networks traditionally announce their SSID on a regular basis with a beacon frame

When the SSID is broadcast, any device with automatic detect and connect to the network

Hiding the SSID is considered "**security through obscurity**" - it's detectable through client traffic

SSID = service set identifier

TKIP

TKIP

Temporal Key Integrity Protocol

was designed as the replacement for WEP without the need to replace legacy hardware

implemented into 802.11 wireless networking under the name WPA (Wi-Fi Protected Access).

CCMP

CCMP

Counter Mode with **C**ipher Block Chaining
Message Authentication Code **P**rotocol

created to replace WEP and TKIP/WPA

uses AES (Advanced Encryption Standard)
with a 128-bit key

used with WPA2, which replaced WEP and WPA

WPA2

WPA2

a new **encryption scheme** known as the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP),

CCMP is based on the AES encryption scheme

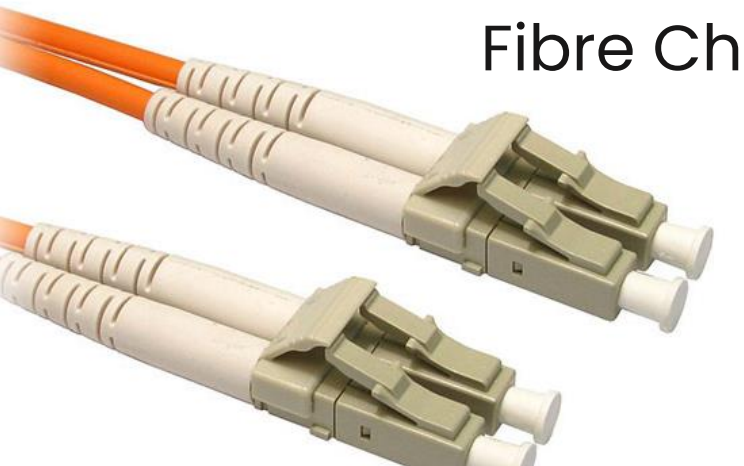
FIBRE CHANNEL & FCoE

Fibre Channel

a form of network data storage solution (i.e., SAN (storage area network) or NAS (network-attached storage)) that allows for high-speed file transfers.

Understand FCoE

FCoE (**F**ibre **C**hannel **o**ver **E**thernet) is used to encapsulate Fibre Channel communications over Ethernet networks.



iSCSI

iSCSI (Internet Small Computer System Interface) is a networking storage standard based on IP.

SITE SURVEY

The process of investigating the presence, strength, and reach of wireless access points deployed in an environment.

SITE SURVEY

usually involves walking around with a portable wireless device, taking note of the wireless signal strength, and mapping this on a plot or schematic of the building.

EAP, PEAP, LEAP

LEAP
Lightweight...

a Cisco proprietary alternative to TKIP for WPA. developed to address deficiencies in TKIP before the 802.11i/WPA2 system was ratified as a standard.

PEAP
Protected...

encapsulates EAP methods within a TLS tunnel that provides authentication and potentially encryption.

EAP
extensible authentication protocol

an authentication framework. allows for new authentication technologies to be compatible with existing wireless or point-to-point connection technologies

MAC FILTERING

MAC Filtering

a list of authorized wireless client interface MAC addresses

used by a wireless access point to block access to all nonauthorized devices.

CAPTIVE PORTALS

portal is an authentication technique that redirects a newly connected wireless web client to a portal access control page.

ANTENNA TYPES

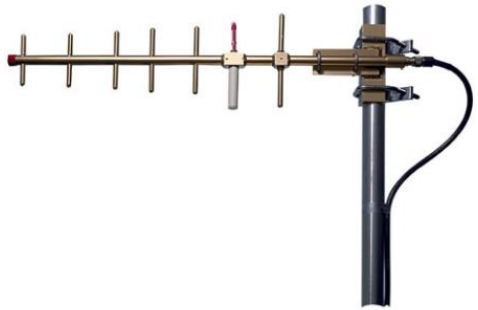
Monopole

Panel

Dipole.

Loop

Cantenna



Yagi

Parabolic

ANTENNA TYPES

Loop

Reaches multiple frequencies and is more commonly used for TV and RFID systems. Omnidirectional if horizontally mounted.

ANTENNA TYPES

Monopole

an omnidirectional antenna that can send and receive signals in all directions perpendicular to the line of the antenna itself.

ANTENNA TYPES

Dipole.

an omnidirectional antenna essentially composed of two monopoles. Generate powerful signal in restricted space

ANTENNA TYPES

Panel

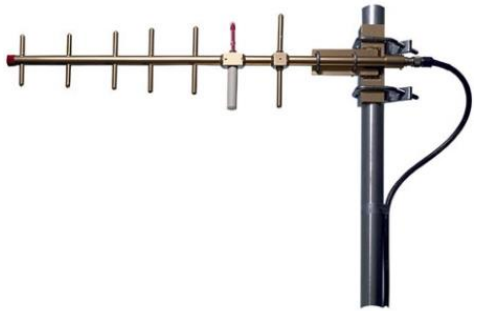
flat devices that focus from only one side of the panel.

ANTENNA TYPES

Parabolic

are used to focus signals from very long distances or weak sources.

ANTENNA TYPES



Yagi

crafted from a straight bar with cross sections to catch specific radio frequencies in the direction of the main bar.

ANTENNA TYPES

Cantenna

constructed from tubes with one sealed end. They focus along the direction of the open end of the tube.

NETWORK DEVICES

Firewalls

Firewalls are essential tools in managing and controlling network traffic. A firewall is a network device used to filter traffic.

Switch

repeats traffic only out of the port on which the destination is known to exist. Switches offer greater efficiency for traffic delivery, create separate collision domains, and improve the overall throughput of data. usually layer 2, sometimes layer 3

Routers

used to control traffic flow on networks and are often used to connect similar networks and control traffic flow between the two. They can function using statically defined routing tables, or they can employ a dynamic routing system. layer 3

Gateways

a gateway connects networks that are using different network protocols. also known as protocol translators, can be stand-alone hardware devices or a software service.

network gateways work at layer 3.

NETWORK DEVICES

Repeaters, **Concentrators**, and **Amplifiers**
used to strengthen the communication signal over a cable segment as well as connect network segments that use the same protocol. layer 1

Bridges
used to connect two networks (even networks of different topologies, cabling types, and speeds) in order to connect network segments that use the same protocol. layer 2

Hubs
Hubs were used to connect multiple systems and connect network segments that use the same protocol. A hub is a multiport repeater. Hubs operate at OSI layer 1. layer 1

LAN Extenders
a remote access, multilayer switch used to connect distant networks over WAN links.

LAN & WAN TECHNOLOGIES

WAN connections and communication links can include **private circuit** technologies and **packet-switching** technologies.

Private circuit technologies use dedicated physical circuits.

Private circuit technologies
— dedicated or leased lines
— PPP (point-to-point protocol
— SLIP (serial line internet protocol)
— ISDN (integrated services digital network)
— DSL (digital subscriber line)

LAN & WAN TECHNOLOGIES

WAN connections and communication links can include **private circuit** technologies and **packet-switching** technologies.

Packet-switching technologies use **virtual circuits** instead of dedicated physical circuits. efficient and cost effective

Packet switching technologies
- X.25, Frame Relay
- Asynchronous transfer mode (ATM),
- Synchronous Data Link Control (SDLC)
- High-Level Data Link Control (HDLC)

FIREWALLS

Types of firewalls

Static Packet-Filtering Firewalls Operate at layer 3 and up
filters traffic by examining data from a message header.

Application-Level Firewalls Operate at layer 7 of OSI model
filters traffic based on a single internet service, protocol, or application

Circuit-Level Firewalls
used to establish communication sessions between trusted partners.
They operate at the Session layer (layer 5) of the OSI model.

SOCKS is an example of a circuit-level firewall

FIREWALLS

Types of firewalls

Stateful Inspection Firewalls
evaluate the state, session, or the context of network traffic.

Deep Packet Inspection Firewalls
a filtering mechanism that operates typically at the application layer in order to filter the payload contents of a communication rather than only on the header values.

FIREWALL AND STATE

Stateless

Watch network traffic and restrict or block packets based on source and destination addresses or other static values.

Not 'aware' of traffic patterns or data flows.

Typically, faster and perform better under heavier traffic loads.

Stateful

Can watch traffic streams from end to end.

Are aware of communication paths and can implement various IP security functions such as tunnels and encryption.

Better at identifying unauthorized and forged communications.

MODERN FIREWALLS

Firewalls
Web Application
aka "WAF"

protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet.

typically protects web applications from common attacks like XSS, CSRF, and SQL injection.

Some come pre-configured with OWASP rulesets

Firewalls
Next Generation
aka "NGFW"

a deep-packet inspection firewall that moves beyond port/protocol inspection and blocking.

adds application-level inspection, intrusion prevention, and brings intelligence from outside the firewall.

TYPES OF FIREWALLS

Deep Packet Inspection

packet inspection inspects and filters both the header and payload of a packet that is transmitted through an inspection point.

can detect protocol non-compliance, spam, viruses, intrusions

Unified Threat Management

aka "UTM"

a multifunction device (MFD) composed of several security features in addition to a firewall;

may include IDS, IPS, a TLS/SSL proxy, web filtering, QoS management, bandwidth throttling, NAT, VPN anchoring, and antivirus.

More common in small and medium businesses (SMB)

TYPES OF FIREWALLS

NAT

Network Address Translation Gateway

allows private subnets to communicate with other cloud services and the Internet but hides the internal network from Internet users.

The NAT gateway has the Network Access Control List (NACL) for the private subnets. .

Content / URL Filter

Looks at the content on the requested web page and blocks request depending on filters.

Used to block inappropriate content in the context of the situation.

Associated with "deep packet inspection"

OPEN-SOURCE vs PROPRIETARY FIREWALLS

Open Source

one in which the vendor makes the license freely available and allows access to the source code, though it might ask for an optional donation.

There is no vendor support with open source, so you might pay a third party to support in a production environment

One of the more popular open-source firewalls is **pfsense**, the details for which can be found at https://www.pfsense.org/.

Proprietary

are more expensive but tend to provide more/better protection and more functionality and support (at a cost).

many vendors in this space, including Cisco, Checkpoint, Pal Alto, Barracuda. but "no source code access"

HARDWARE vs SOFTWARE

Hardware

A piece of purpose-built network hardware.

May offer more configurable support for LAN and WAN connections.

Often has superior throughput versus software because it is hardware designed for the speeds and connections common to an enterprise network.

Software

Software based firewalls that you might install on your own hardware.

Provide flexibility to place firewalls anywhere you'd like in your organization.

On servers and workstations, you can run a host-based firewall.

Host-based (software) are more vulnerable in some aspects due to attack vectors

APPLICATION vs HOST-BASED vs VIRTUAL

Application

Typically catered specifically to application communications.
Often that is HTTP or Web traffic.
An example is called a next generation firewall (NGFW)

Host-based

An application installed on a host OS, such as Windows or Linux, both client and server operating systems.

Virtual

In the cloud, firewalls are implemented as virtual network appliances (VNA).
Available from both the CSP directly and third-party partners (commercial firewall vendors)

IDS and IPS

Intrusion Detection System

analyzes whole packets, both header and payload, looking for known events. When a known event is detected, a **log message is generated.**

Reports and/or alerts

Intrusion Prevention System

analyzes whole packets, both header and payload, looking for known events. When a known event is detected, **packet is rejected**.

Takes action!

TYPES OF IDS SYSTEMS

Behavior based

creates a baseline of activity to identify normal behavior and then measures system performance against the baseline to detect abnormal behavior.

can detect previously unknown attack methods

Knowledge based

uses signatures similar to the signature definitions used by anti-malware software.

only effective against known attack methods

Both host-based (HIDS) and network-based (NIDS) systems can be knowledge based, behavior based, or a combination of both.

HOST-BASED IDS AND IPS

IDS/IPS in software form, installed on a host (often a server)

HIDS

Host-based Intrusion Detection System

analyzes whole packets, both header and payload, looking for known events. When a known event is detected, a **log message is generated**.

HIPS

Host-based Intrusion Prevention System

analyzes whole packets, both header and payload, looking for known events. When a known event is detected, **packet is rejected**.

NETWORK-BASED IDS AND IPS

IDS/IPS at the network level, often in hardware form

NIDS

Network-based Intrusion Detection System

analyzes whole packets, both header and payload, looking for known events. When a known event is detected, a **log message is generated**.

NIPS

Network-based Intrusion Prevention System

analyzes whole packets, both header and payload, looking for known events. When a known event is detected, **packet is rejected**.

MODES OF OPERATION

Inline
aka "in-band"

NIDS/NIPS placed on or near the firewall as an additional layer of security.

Passive
aka "out-of-band"

traffic does not go through the NIPS/NIDS.

sensors and collectors forward alerts to the NIDS.

NETWORK APPLIANCES

Sensors and Collectors

can be placed on a network to alert NIDS of any changes in traffic patterns on the network.

If you place a sensor on the Internet side of the network, it can scan all of the traffic from the Internet.

SECURE NETWORK DESIGN

Bastion Host

hardened

computer or appliance that is exposed on the Internet and has been hardened by removing all unnecessary elements, such as services, programs, protocols, and ports.

Screened Host

MOST SECURE

is a firewall-protected system logically positioned just inside a private network.

Screened Subnet

similar to the screened host in concept, except a subnet is placed between two routers or firewalls and the bastion host(s) is located within that subnet.

A **proxy server** functions on behalf of the client requesting service, masking the true origin of the request to the resource.

SECURE NETWORK DESIGN

Honeypot

Lure bad people into doing bad things. Lets you watch them.

Only ENTICE, not ENTRAP. you are not allowed to let them download items with “Enticement”.

For example, allowing download of a fake payroll file would be entrapment.

remember this difference!

Goal is to **distract** from real assets and **isolate** in a padded cell until you can track them down.

NETWORK ATTACKS

Teardrop Attack

is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device.

Fraggle Attack

is a denial-of-service (DoS) attack that involves sending a large amount of spoofed UDP traffic to a router's broadcast address within a network. It is very similar to a **Smurf Attack**, which uses spoofed ICMP traffic using a 3rd party network rather than UDP traffic to achieve the same goal.

Land Attack

is a Layer 4 Denial of Service (DoS) attack in which, the attacker sets the source and destination information of a TCP segment to be the same. A vulnerable machine will crash or freeze due to the packet being repeatedly processed by the TCP stack

NETWORK ATTACKS

SYN FlooD

is a form of denial-of-service attack in which an attacker sends a succession of **SYN** requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

Ping of Death

Employs an oversized ping packet. Max allowed ping packet size is 65,536 bytes. Ping of death sends package 65,537 bytes or larger.

1) SYN 2) SYN-ACK 3) ACK

Know the **TCP 3-way handshake**, a process used in a TCP/IP network to make a connection between the server and client.