Communications and Network Security

Cybersecurity Bootcamp 2024

Disclaimer

This learning material is addressed and used only for Cybersecurity Bootcamp 2024 and should not be used or relied upon for any other purposes. Our learning material is not to be disseminated to or used by any third party in whole or in part without prior consent and permission from Kasikorn Technology Group Secretariat Company Limited (KBTGSec). Accordingly, we will not accept or take any responsibility or liability for any party or any person, whether or not such material is shown, disseminated, obtained, or possessed to such party or person since such material is only for educational purposes. We reserve all of our rights, including but not limited to intellectual property rights in our learning material, such as presentations, spreadsheets, system techniques, ideas, concepts, information, forms, electronic tools, forming parts of the materials, etc.

Topics overview

1. Introduction to OSI model
2. 7 Layers of OSI model
3. OSI vs TCP
4. Network security technology

Key objectives

1. To understand what the OSI Model and how data is transported over a network, from the application layer to the physical layer.
2. To understand the purpose and functionality of various networking protocols, such as HTTP, FTP, TCP, IP, and Ethernet.
3. To help learners in identifying and addressing network problems by assessing each layer.
4. To assist learners in effectively and securely designing networks infrastructure.
5. To know Network Security Technology, such as security zone, WAN, Firewall Best Practices, NAT/PAT etc.,

01

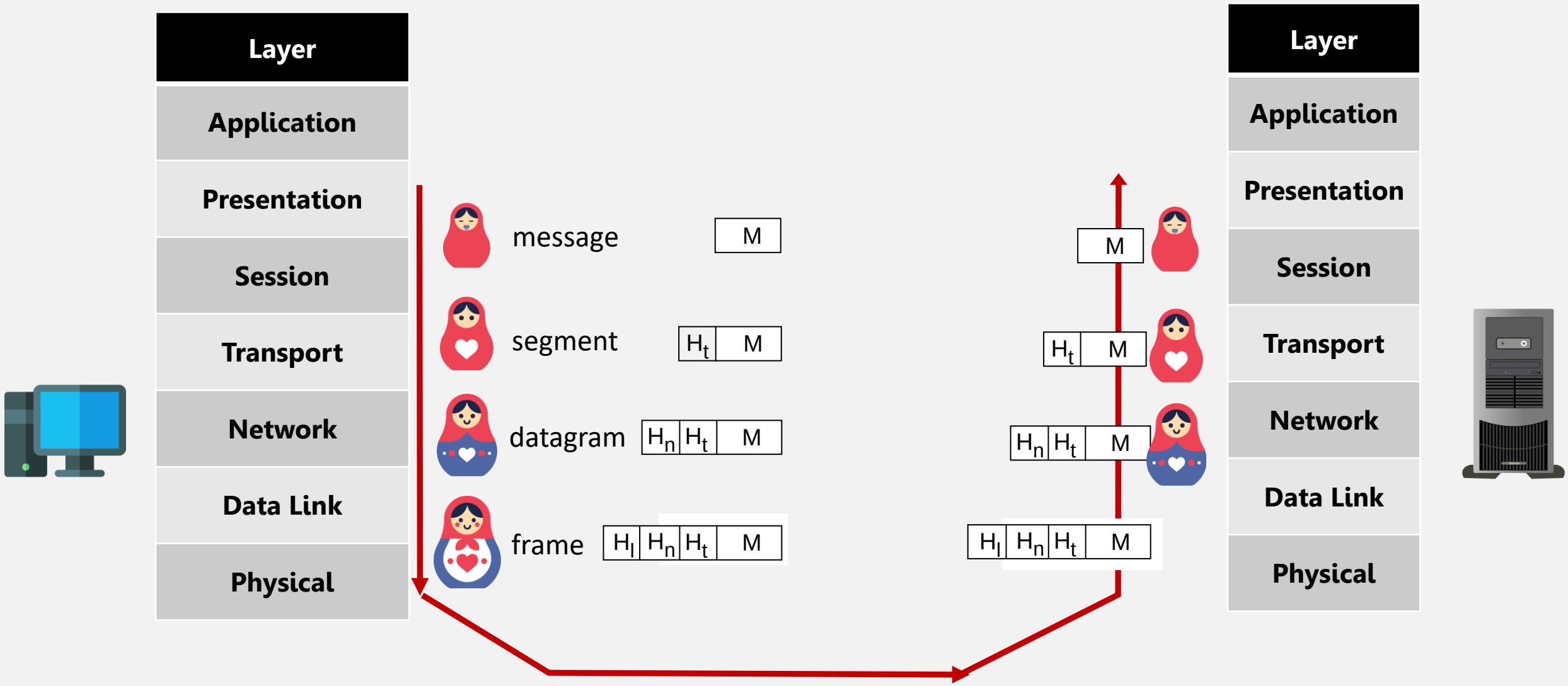
Overview and The OSI Reference Model

Open Systems Interconnection (OSI)

- The Open Systems Interconnection (OSI) reference model is used to explains how devices communicate with each other
- The model consis7 layers, each layer providing services to the layers above and below

Layer	Definitions
Layer 7 – Application Layer	Enables users and applications to access network services
Layer 6 – Presentation Layer	Translates data into a common format
Layer 5 – Session Layer	Establishes a communication session between devices
Layer 4 – Transport Layer	Manages message fragmentation and reassembly
Layer 3 – Network Layer	Manages data routing and creating sub networks
Layer 2 – Data Link Layer	Provides error-free transfer of data frames
Layer 1 – Physical Layer	Physical network media and signal methods

OSI Model Layers



02

The OSI Model
Part 1 - Physical Layer

Layer 1 – Physical Layer

Defines the physical and electrical medium for data transfer

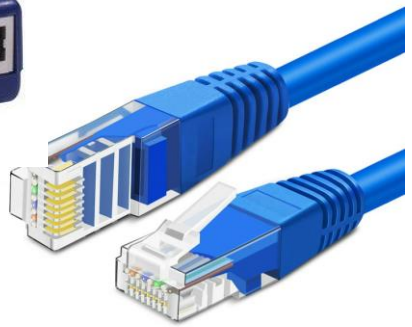
Physical layer components: cables, jacks, patch panels, punch blocks, hubs, and MAUs

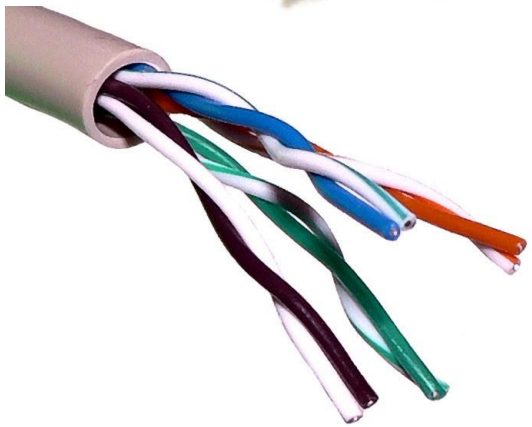
Physical layer concepts: topologies, analog versus digital encoding, bit synchronization, baseband versus broadband, multiplexing, and serial data transfer

Unit of measurement: Bits

Hardware components

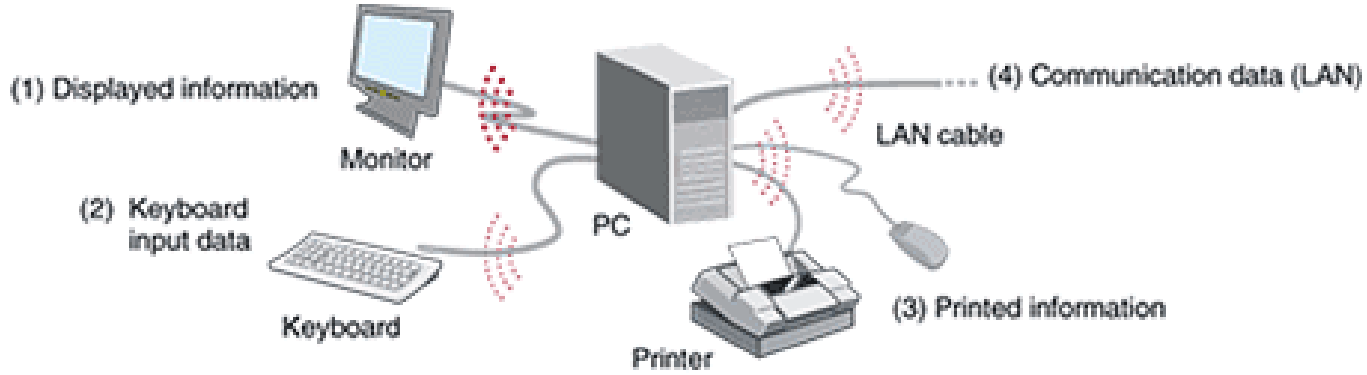
- Hub
- CAT5
- Network interface card
- Fiber optic wire
- Ethernet copper cable
- Wireless Access point





Threats

- Theft
- Unauthorized access
- DDoS
- Sniffing
- Interference
- Data emanation



Information hidden in leaking emissions	Importance and quantity of the information	Difficulty of regenerating original information	Strength of emissions	Total threat of information leakage
(1) Displayed information	High (displayed information)	Easy	Strong	High
(2) Keyboard input data	Low to medium (only text)	Hard (need to decipher code assigned to each key)	Weak	Low to medium
(3) Printed information	Low (only printed information)	Hard (need to demodulate printer interface signal)	Weak	Low
(4) Communication data	Medium to high (communicated information)	Hard (need to demodulate LAN interface signal)	Weak	Medium

LAN: local area network

Src pic: https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200810sf2.html

03

The OSI Model: Part 2 – Data Link Layer

Layer 2 – Data Link Layer

Establishes, maintains, and decides how transfer is accomplished over the physical layer and ensures error-free transmission over the physical layer

MAC addresses, which are unique hexadecimal addresses burned into the ROM of the NIC, identify each hardware device at the Data Link Layer

Data Link Layer components: network interface cards and bridges

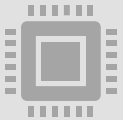
Unit of measurement: frames

Ethernet Standards (IEEE 802.3)

- LAN standard facilitating high-speed data exchange among devices
- Defined Physical and Data Link Layer
- Examples
  - 100BASE-T (100 Mbps, Baseband, and Twisted-pair cabling)
  - 1000Base-T (IEEE 802.3ab)
  - 10GBase-T (802.3.an)
- Baseband refers to the fact that devices on the network use digital signaling over a single frequency
- Broadband systems use analog signaling over a range of frequencies enabling multiple channels over the same physical medium

Media Access Control Address

Network adapters on an Ethernet network have unique Media Access Control (MAC) addresses



MAC addresses are unique identifiers assigned to network adapters by the manufacturer

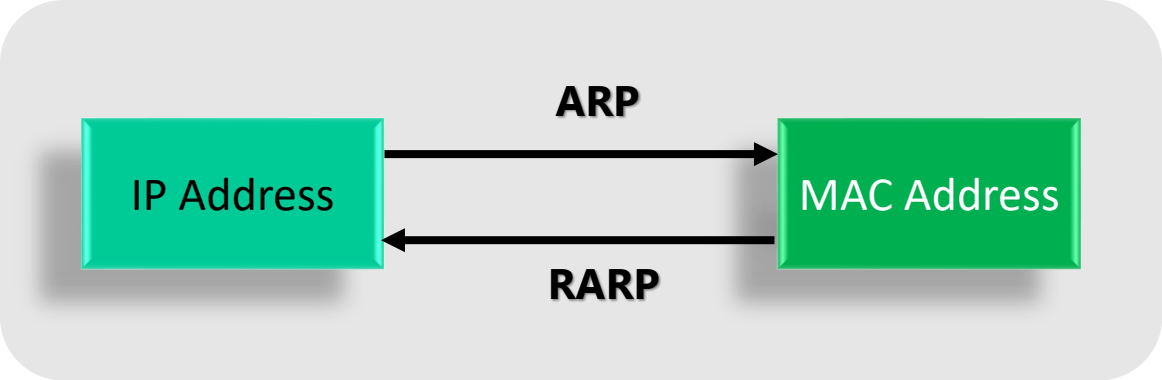
MAC address is six octets in length written in hexadecimal

Ipconfig command

```
D:\Users\kitisak.j>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : [redacted]
   Primary Dns Suffix  . . . . . . . : [redacted]
   Node Type . . . . . . . . . . . . : Peer-Peer
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : [redacted]

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : [redacted]
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (6) I219-V
   Physical Address. . . . . . . . . : F8-75-A4-B7-EA-30
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

ARP and RARP

Parameter	ARP	RARP
Abbreviation for	Address resolution protocol	Reverse Address Resolution Protocol
Broadcast MAC/IP	Nodes use ARP broadcast in LAN by using broadcast MAC address	RARP uses Broadcast IP address
Mapping	Maps IP address of node to its MAC Address	Maps 48 bit MAC address to IP address
Usage	Used by host or Router to find physical address of another host/Router in LAN.	Used by thin clients with limited facilities
Table maintained by	Local Host maintains ARP table	RARP Server maintains RARP table
Reply information	ARP reply is used to update ARP table	RARP reply is used to configure IP address in local host




```
D:\Users\kitisak.j>arp -a

Interface: 192.168.1.158 --- 0x15
  Internet Address      Physical Address      Type
  192.168.1.1           f0-63-f9-3e-ce-3d     dynamic
  192.168.1.123         20-df-b9-0e-9d-80     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

04

The OSI Model: Part 3 - Network Layer

Layer 3 – Network Layer

- Controls the operations of routing and switching information to different networks
- Translates logical addresses or names to physical addresses
- Internet Protocol (IP) is a Network Layer protocol
- Devices that work at the network layer are routers and IP switches
- Network Layer components: IP addresses, subnets
- Unit of measurement: packets

Layer 3 Protocols - Examples

IP (Internet Protocol) stands for Internet Protocol. It is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries.

ICMP (Internet Control Message Protocol) is a protocol used by network devices, including routers, to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached.

IGMP (Internet Group Management Protocol) is a communications protocol used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of IP multicast.

IGRP (Interior Gateway Routing Protocol) is a proprietary distance-vector routing protocol used by Cisco routers to exchange routing data within an autonomous system.

IPSEC (IP Security) is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet in a communication session. It provides security at the network layer.

IKE (Internet Key Exchange) is a key management protocol used by IPsec to establish security associations (SAs) and negotiate cryptographic keys between two parties.

ISAKMP (Internet Security Association and Key Management Protocol) is a protocol for establishing Security Associations (SAs) and cryptographic keys in an Internet environment. It is used in conjunction with IKE for key exchange and security association negotiation in IPsec VPNs

ICMP Attack - Examples

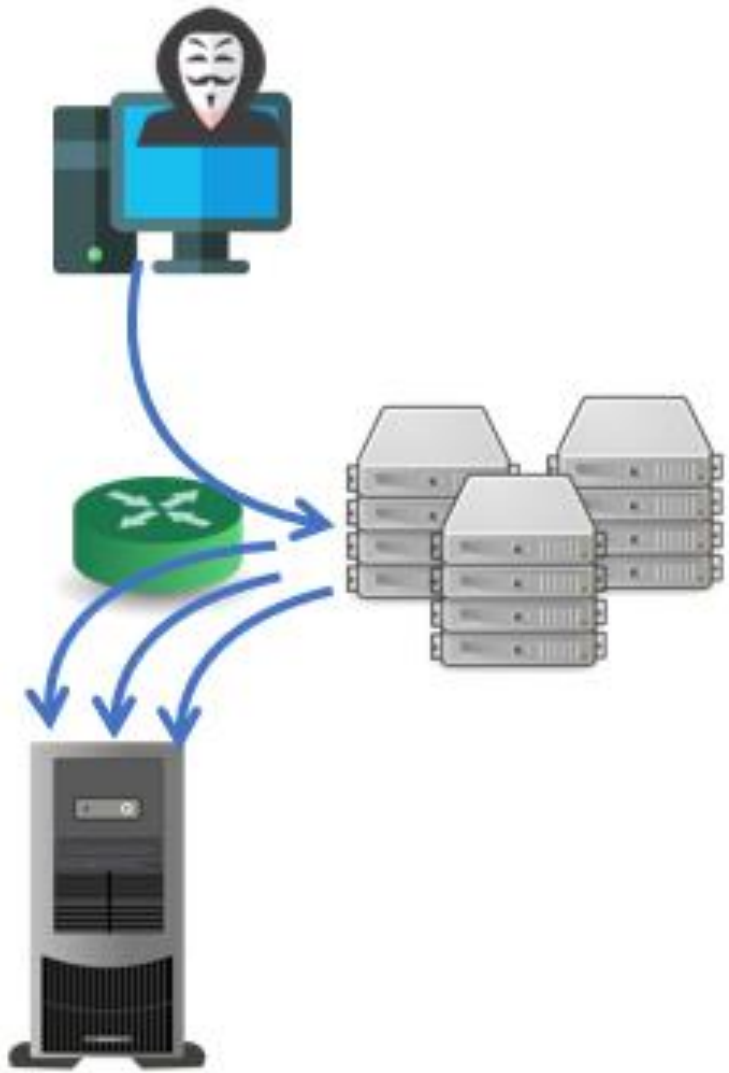
ICMP (Internet Control Message Protocol) attacks exploit vulnerabilities or weaknesses in the ICMP protocol to disrupt network operations or compromise systems.

Ping Flood: Also known as an ICMP flood, the attacker sends a massive number of ICMP Echo Request (ping) packets to a target system.

ICMP Flood: Similar to a Ping Flood, but involves flooding the target with various types of ICMP packets, not just ping request

Ping of Death: The attacker sends an oversized or malformed ICMP packet to the target system.

Smurf Attack: The attacker sends ICMP Echo Request packets to IP broadcast addresses, spoofing the source IP address to appear as the victim's IP address. Then all hosts reply to the victim's IP address, overwhelming it with responses and causing denial of service.



05

The OSI Model: Part 4 - Transport Layer

Layer 4 – Transport Layer

This layer ensures messages are delivered error-free, in sequence and with no losses or duplications

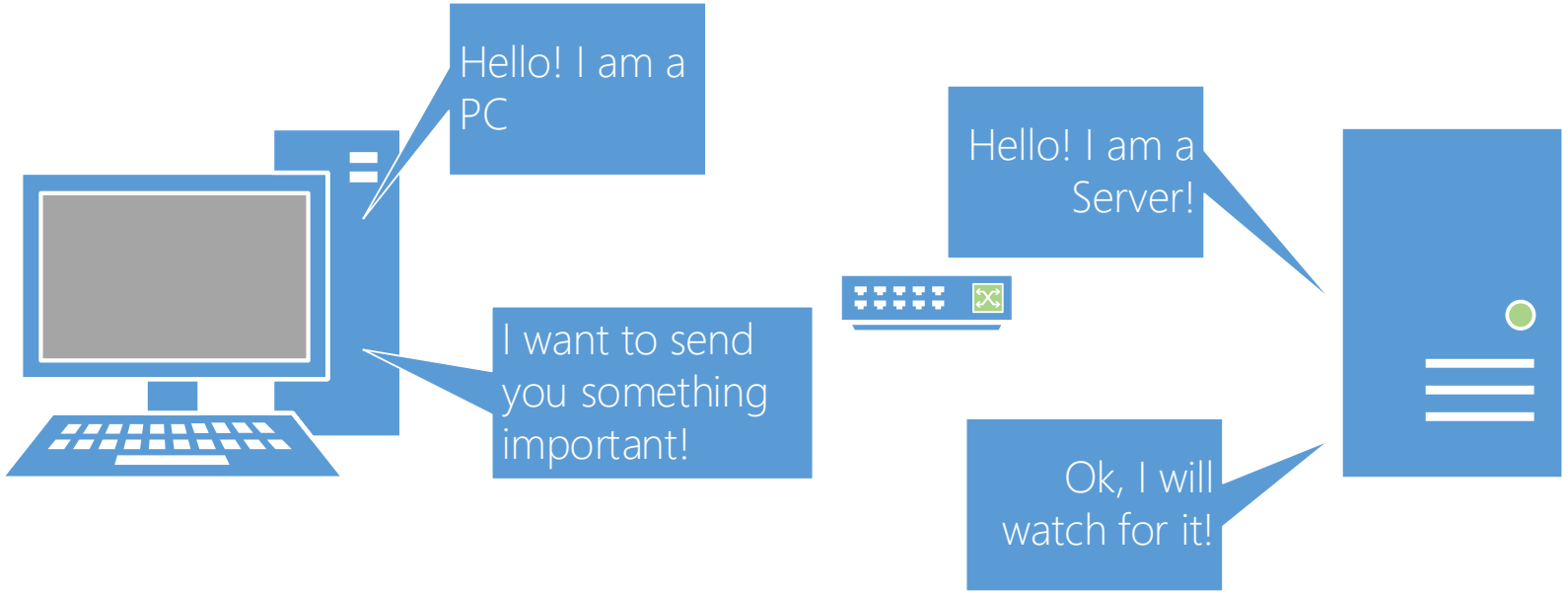
Protocols that work at this layer segment messages, ensure correct reassembly at the receiving end, perform message acknowledgement and message traffic control

The Transport Layer contains both connection-oriented and connectionless protocols

Unit of measurement: segments or messages

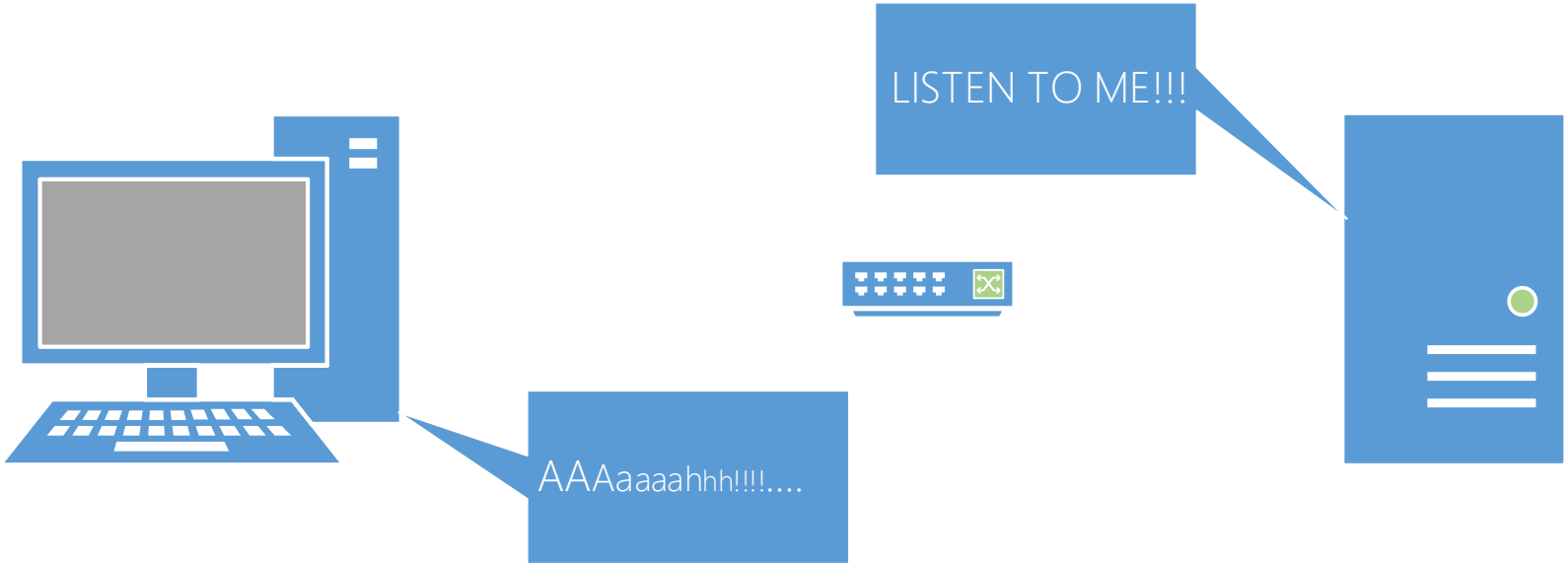
Connection Oriented Communications

- Require both devices involved in the communication establish an end-to-end logical connection before data can be sent
- These communications are considered reliable network services
- Packets not received by the destination device can be resent by the sender



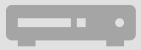
Connectionless Communications

- End-to-end connection is not necessary before data is sent
- Every packet that is sent has the destination address in the header
- Sufficient to move independent packets, such as in streaming media
- Datagram delivery is not guaranteed, and lost packets cannot be resent



Connection-based Protocols

The Transport Layer contains both connection-oriented and connectionless protocols



Transmission Control Protocol (TCP) provides a connection-based, reliable, byte-stream service to programs

User Datagram Protocol (UDP) provides a connectionless, unreliable transport service

TCP and UDP

- TCP transport is used for logging on, file and print sharing, replication of information between domain controllers, transfer of browse lists, and other common functions. TCP can only be used for one-to-one communications.
- UDP is often used for one-to-many communications, using broadcast or multicast IP datagrams

Protocol	Type	Example
Transmission Control Protocol (TCP)	Connection-oriented	Web browser
User Datagram Protocol (UDP)	Connectionless	Streaming media

Ports

- Ports are a Layer 4 protocol that a computer uses for data transmission
- Ports act as logical communications endpoint for specific program on computers for delivery of data sent
- There are a total of 65,536 ports, numbering between 0 and 65,535
- Ports are defined by the Internet Assigned Numbers Authority or IANA and divided into categories

Ports

Port Number	Associated Protocol	Full Name
21	FTP	File Transfer Protocol
22	SSH	Secure Shell
23	Telnet	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name System
80	HTTP	Hypertext Transfer Protocol
88	Kerberos	Kerboros
110	POP3	Post Office Protocol Version 3
119	NNTP	Network New Transfer Protocol
137-139	NetBIOS	NetBIOS Name, Datagram, and Session Service, respectively
143	IMAP	Internet Access Message Protocol
161	SNMP	Simple Network Management Protocol
389	LDAP	Lightweight Directory Access Protocol
443	HTTPS	Hypertext Transfer Protocol Secure (uses TLS or SSL)
445	SMB	Server Message Block
1701	L2TP	Layer 2 Tunneling Protocol
1723	PPTP	Point-to-Point Tunneling Protocol
3389	RDP	Remote Desktop Protocol (Microsoft Terminal Server)

06

The OSI Model: Part 5 - Session Layer

Layer 5 – Session Layer

- The Session Layer manages session establishment, maintenance and termination between network devices
- Example: when you log on and log off
- This layer controls the name and address database for the OS
- NetBIOS (Network Basic Input Output System) is a protocol that works at this layer

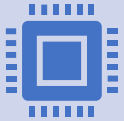
NetStat Command

```
D:\Users\kitisak.j>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2701           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8005           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8081           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9000           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49703          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:61534          0.0.0.0:0              LISTENING
  TCP    10.213.210.239:139     0.0.0.0:0              LISTENING
  TCP    10.213.210.239:49159   161.69.88.140:8080     TIME_WAIT
  TCP    10.213.210.239:49162   161.69.88.140:8080     TIME_WAIT
  TCP    10.213.210.239:49250   161.69.88.140:8080     TIME_WAIT
```

07

The OSI Model: Part 6 - Presentation Layer

Layer 6 – Presentation Layer



This layer translates the data format from sender to receiver in the various OSes that may be used

Presentation Layer concepts include: character code conversion, data compression, and data encryption

Redirectors work on this layer, such as mapped network drives that enable a computer to access file shares on a remote computer

08

The OSI Model: Part 7 - Application Layer

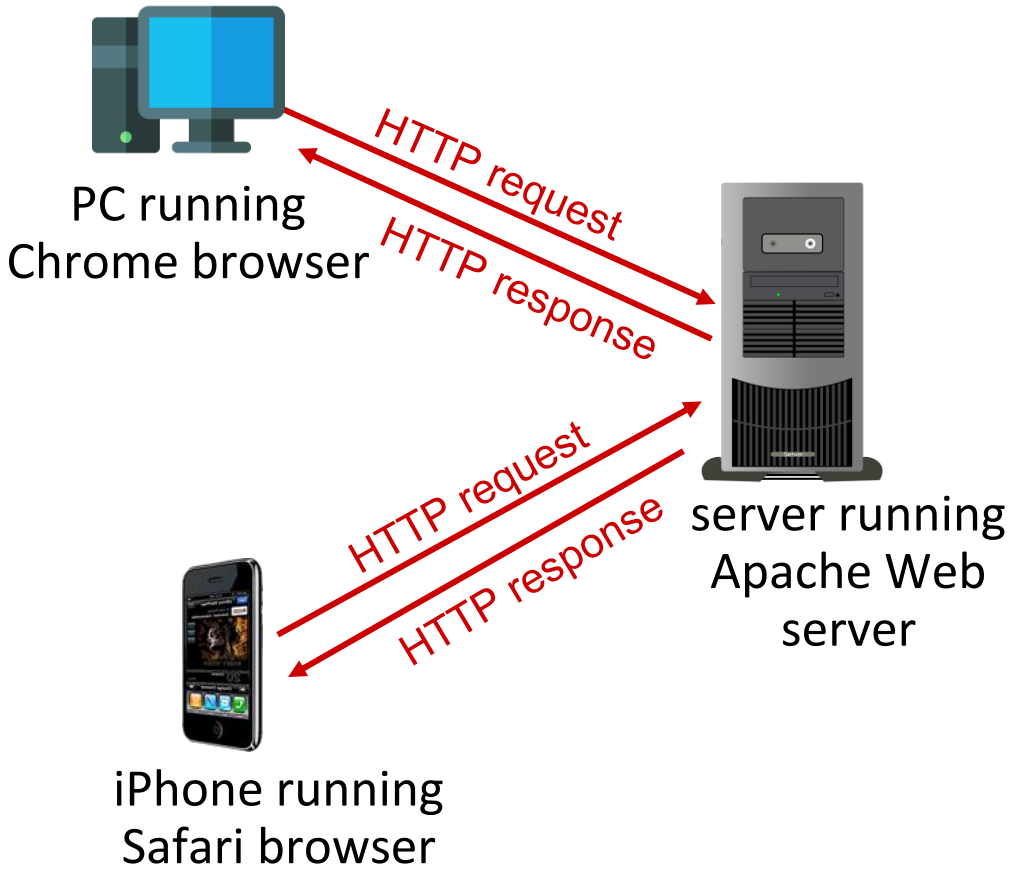
Layer 7 – Application Layer

- Serves as a the window for users and application processes to access network services
- This layer is where message creation begins
- End-user protocols such as HTTP, FTP, SMTP, Telnet, and RAS work at this layer
- This layer is not the application itself, but the protocols that are initiated by this layer

Example - HTTP overview

HTTP: hypertext transfer protocol

- client/server model:
  - client: browser that requests, receives, (using HTTP protocol) and “displays” Web objects
  - server: Web server sends (using HTTP protocol) objects in response to requests



HTTP overview (continued)

HTTP uses TCP:

- client initiates TCP connection to server, port 80
- server accepts TCP connection from client
- HTTP messages (Application layer protocol messages) exchanged between browser (HTTP client) and Web server (HTTP server)
- TCP connection closed

OSI Model Revisited

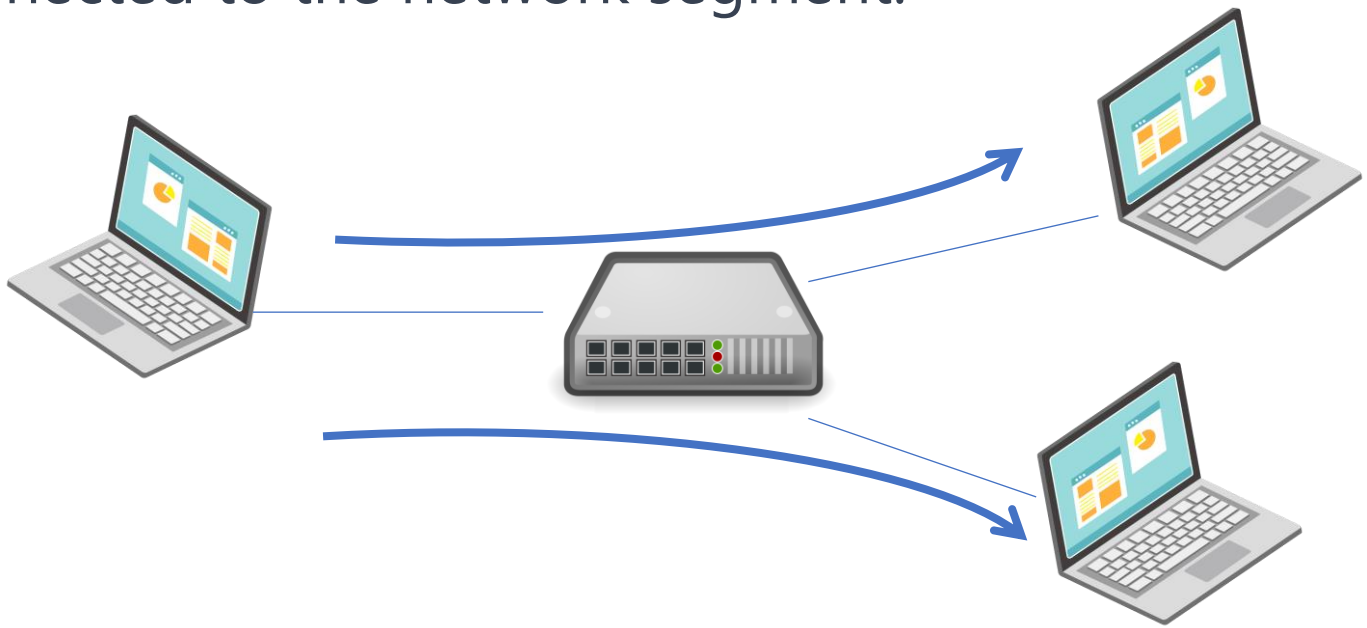
Layer	Protocol	Device
7 – Application	FTP, HTTP, POP3, SMTP	Gateway
6 – Presentation	Compression, Encryption	N/A
5 – Session	Logon/Logoff	N/A
4 – Transport	TCP, UDP	N/A
3 – Network	IP, ICMP, ARP, RIP	Routers
2 – Data Link	802.3, 803.5	NICs, Switches, Bridges, WAPs
1 – Physical	100BASE-T, 1000BASE-X	Hubs, Patch Panels, RJ45 Jacks

09

Network Devices at Layers 1, 2, and 3

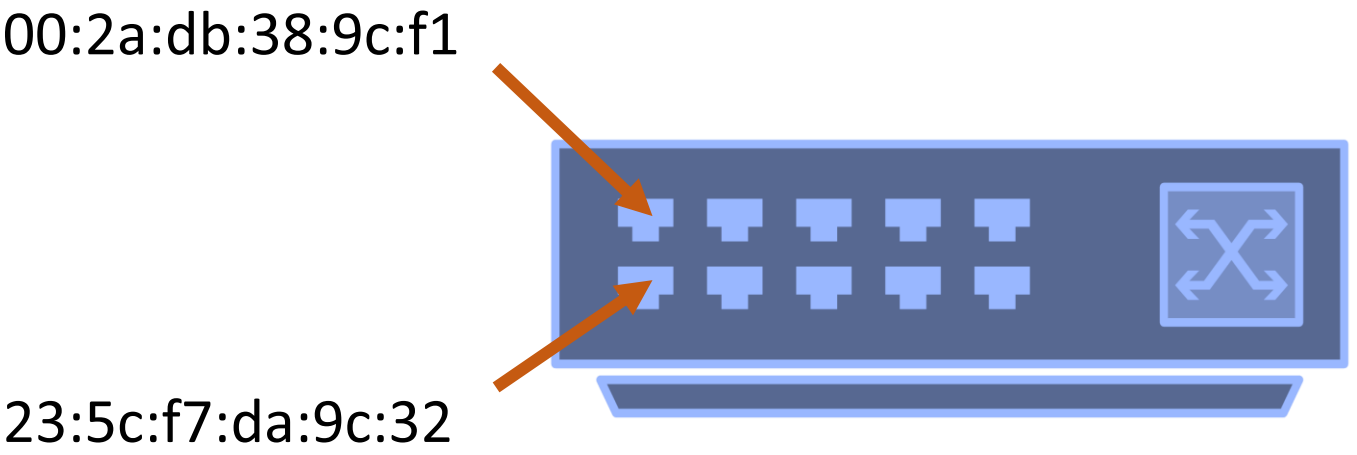
Layer 1 HUB

- Layer 1 hub handles the physical connection between devices and sends data bits over a communication channel.
- This type of hub forwards data at the electrical or optical signal level without understanding the actual data.
- It works like a multi-port repeater, sending incoming data packets to all devices connected to the network segment.



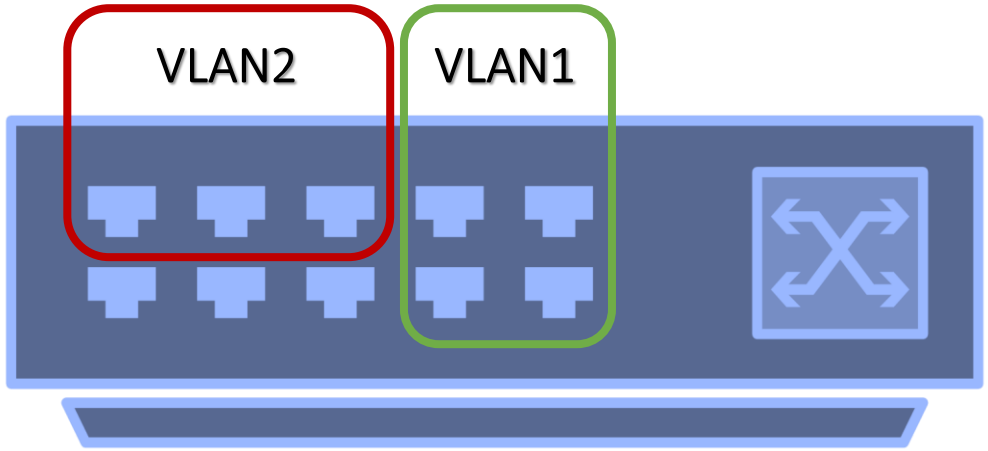
Layer 2 Switches

- Layer 2 switches are hardware-based and use MAC addresses to forward data frames between devices within the same local area network (LAN)
- Ports on the switch are mapped to the specific MAC address of the device attached
- This allows the switch to intelligently forward data frames only to the intended destination device, improving network efficiency and reducing unnecessary network traffic.



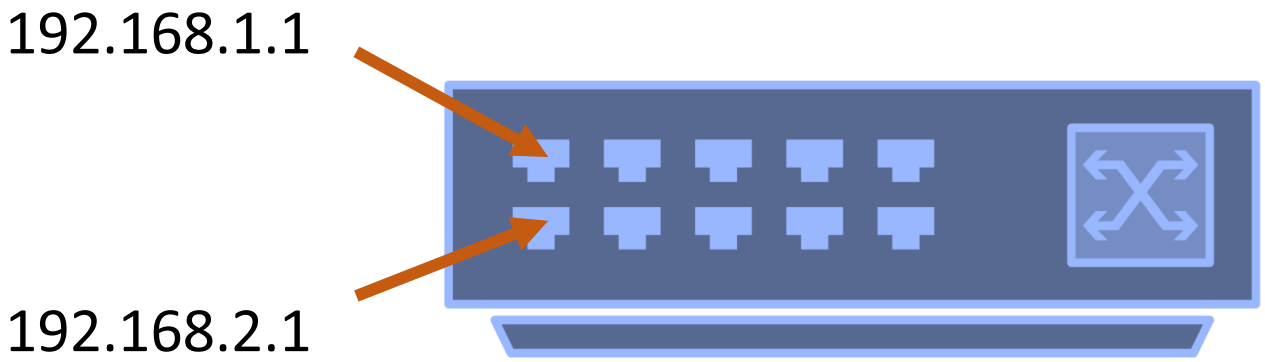
Virtual LAN (VLAN)

- Layer 2 switching can also allow for a virtual LAN (VLAN) to be implemented.
- A VLAN is implemented to segment and organize the network, to reduce collisions, boost performance
- IEEE 802.1Q is the standard that supports VLANs
- A tag is added to the data frame to identify the VLAN
- VLANs are commonly used to improve network security, optimize performance, and simplify network management.



Layer 3 Switches

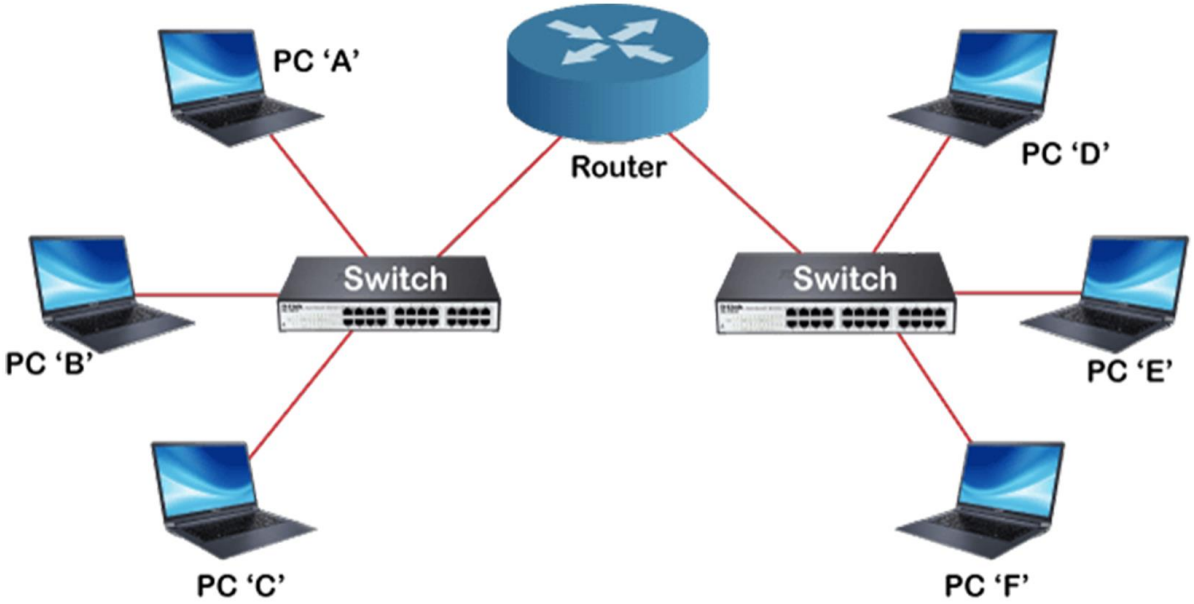
- Switches can also reside on the network layer
- A layer 3 switch determines paths for data using logical addressing (IP addresses) instead of physical addressing (MAC addresses for a layer 2 switch)
- Layer 3 switches forward packets, whereas layer 2 switches forward frames



Switches vs Routers

both are store-and-forward:

- Routers: Network layer devices
- Switches: Data link layer devices



SRC PIC: https://www.lightoptics.co.uk/blogs/news/how-to-connect-a-switch-to-a-router

both have forwarding tables:

- Routers: compute tables using routing algorithms, IP addresses
- Switches: learn forwarding table using flooding, learning, MAC addresses

Key Takeaways

- OSI model consists of 7 layers
- Communication protocol between each layer
- Network threats in each layer depends on charactoristics
- Network devices such as HUB, L2 Switch, and L3 Switch

10

TCP Model and OSI Review

TCP Model

- The TCP/IP model is similar to the OSI model
- This model is composed of only four layers

Layer	Description	Protocols
Application Layer	Defines TCP/IP application protocols	HTTP, Telnet, FTP, SMNP, DNS
Transport Layer	Provides communication session management	TCP, UDP, RTP
Internet Layer	Packages and routes data	IP, ICMP, ARP, RARP
Network Interface	Details how data is physically sent through the network	Ethernet, Token Ring, Frame Relay

OSI Model Compared to TCP Model

OSI Model	TCP Model
Application Layer	Application Layer
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer
Network Layer	Internet Layer
Data Link Layer	Network Access Layer
Physical Layer	

- **Layers**: The OSI model has seven layers, while the TCP/IP model has four layers.
- **Complexity**: The OSI model is more complex and detailed, whereas the TCP/IP model is simpler and more streamlined.
- **Standardization**: The OSI model is a formal standard, while the TCP/IP model is more of a practical implementation used in real-world networking.
- **Usage**: The OSI model is used more as a conceptual framework and reference model, while the TCP/IP model is directly implemented in most modern networking environments, especially the Internet.

Topics key takeaways

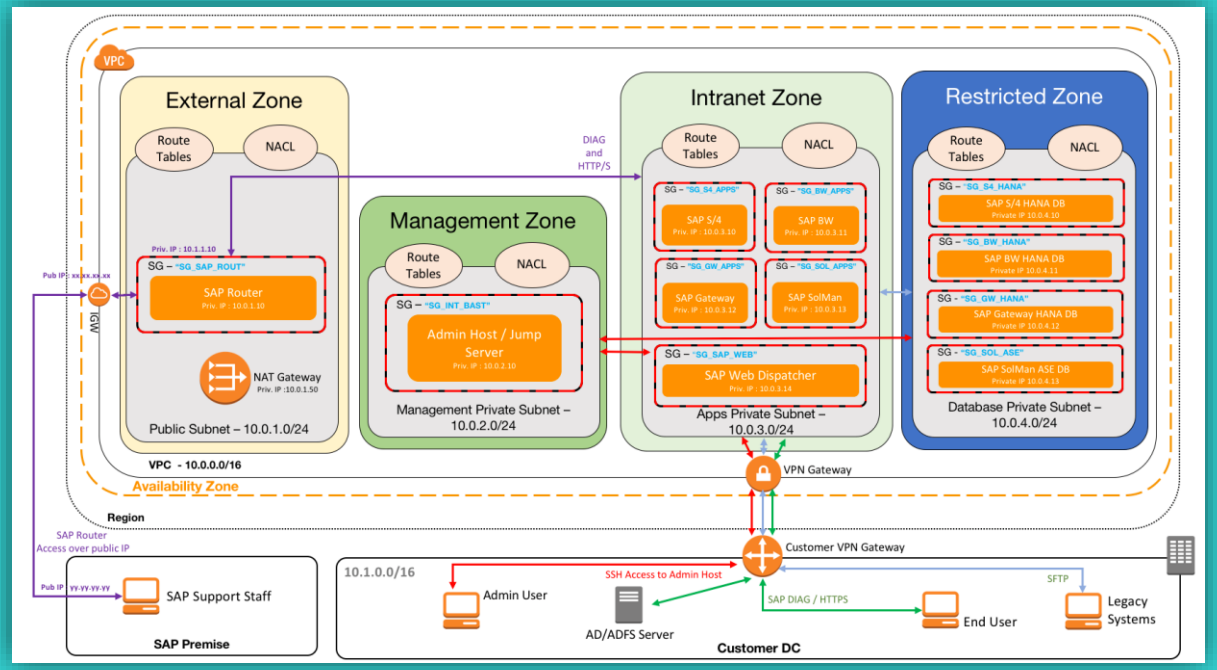
- Understand the OSI model by defining each of the layers from a theory perspective
- Be able to separate the functions of the lower levels of the OSI model, from the upper levels where message creation begins.
- Understand the differences between layer 2 and layer 3 switches, and gain a basic understanding of how they operate.
- Differentiate between the OSI model and the TCP model.

11

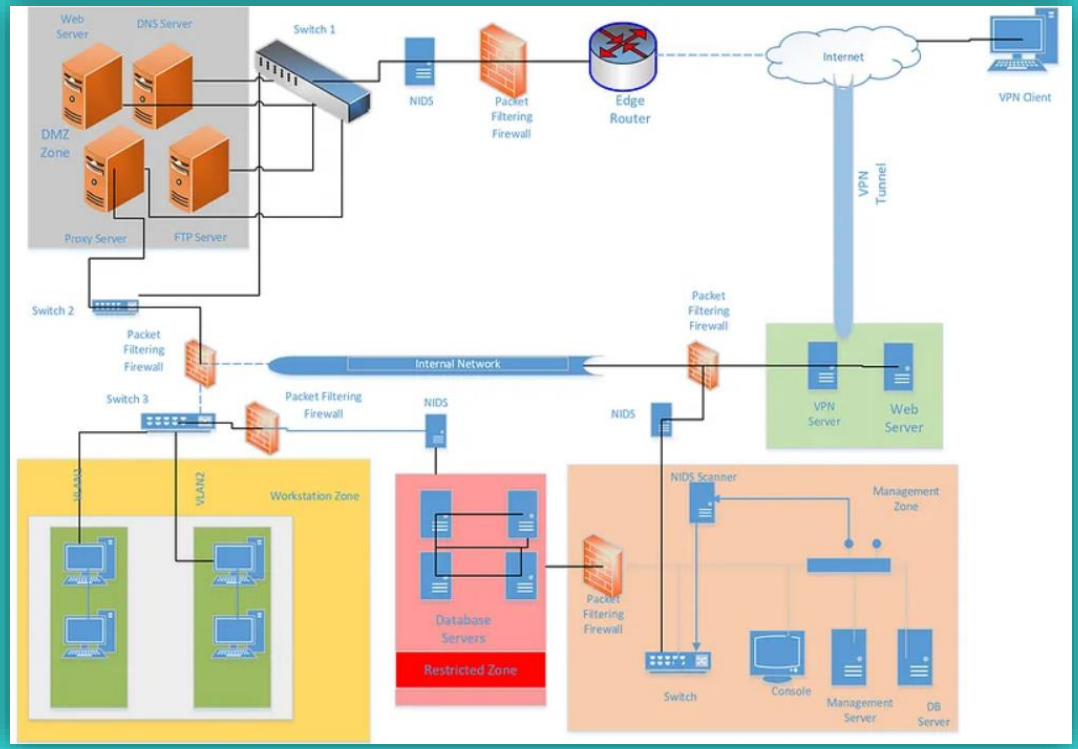
Security Zone

Security Zone

DMZ Zone /Web, App, DB Zone/ Intranet/ Client Zone

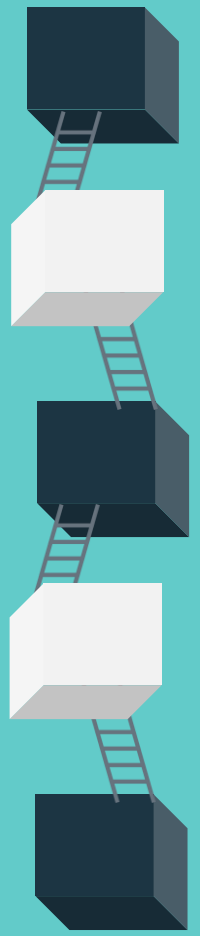


Management Zone /Restricted Zone /VPN Zone Trusted – Untrusted/ Semi-Trusted Zone



Security Zone

Why ?



01	Risk Segmentation	Isolation of Critical Assets, Critical Inventory
02	Containment of Threats	Malware, Virus, Ransomware, Phishing, etc.
03	Layered security control	WAF, IPS, FW, NextGen FW, DDOS, AV, FIM, DLP
04	Monitoring and Logging	Incident Response plan, Post Incident Activity
05	Regulatory Compliance	PCI-DSS, ISO27001, PDPA, GDPR, HIPAA, etc.

12

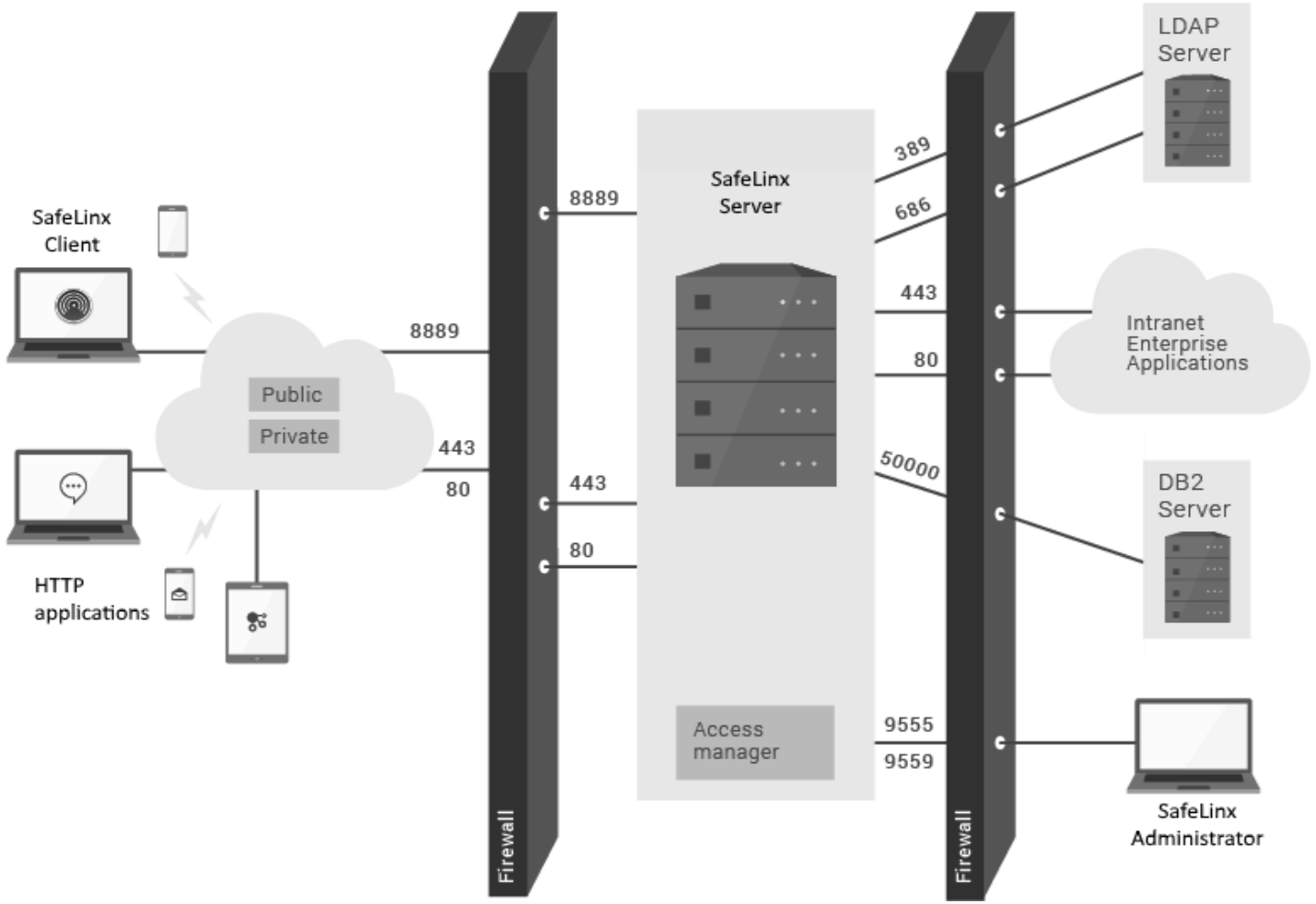
Firewalls and the OSI Model

Firewalls and the OSI Model

Firewall -> Layer 3

Packet Filtering

- Source IP Address
- Destination IP Address
- Source Port
- Destination Port
- Protocol

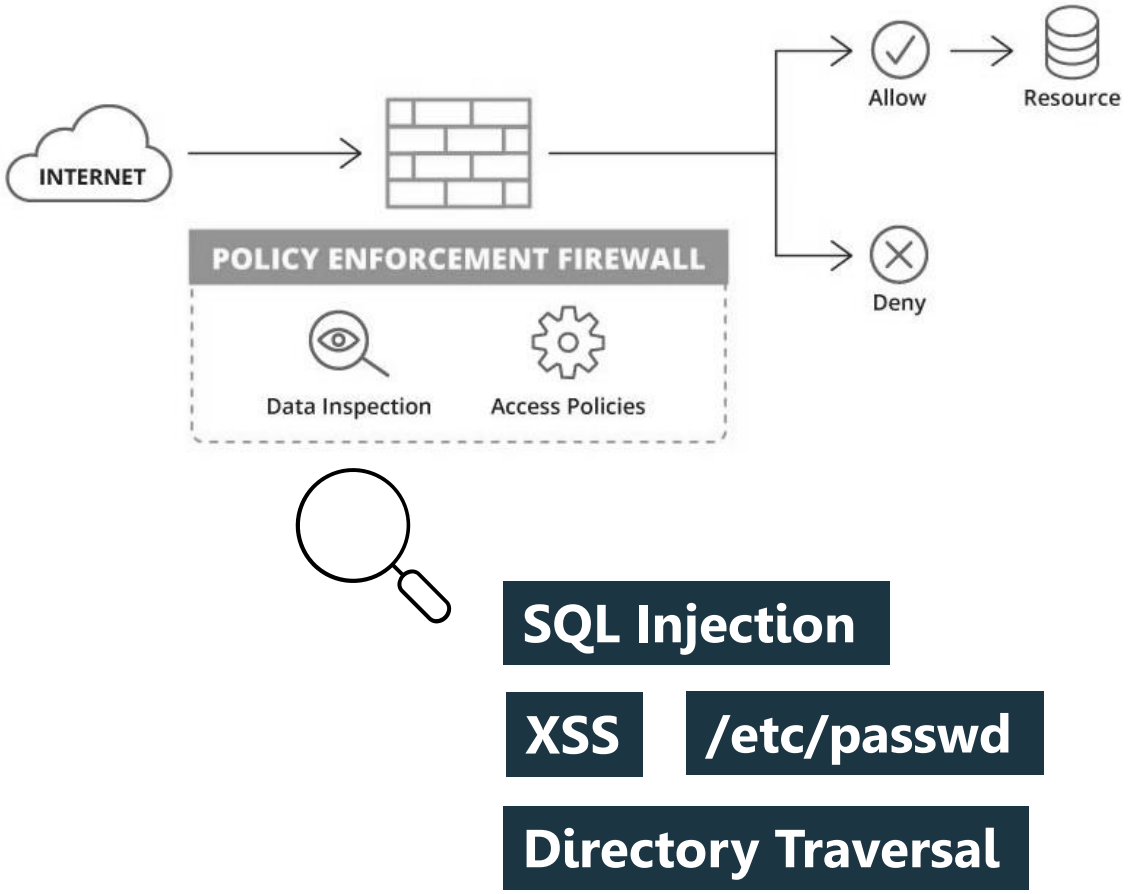


Firewalls and the OSI Model

Next Gen Firewall -> Layer 7

Inspect content, traffic

- Application
- Proxy
- VPN Module
- IPS Module
- Threat Intelligence Module



13

Firewall Best Practices

Firewall Best Practices (1/2)

1. Understand Network Traffic

Understand the types of network traffic in your environment. Identify the applications, services, and protocols that should be allowed or blocked.

2. Use a Deny by Default Rule

Only explicitly allowed traffic is permitted, reducing the attack surface.

3. Create Specific Allow Rules

Only open the ports and protocols necessary for the required services, applications, and communication.

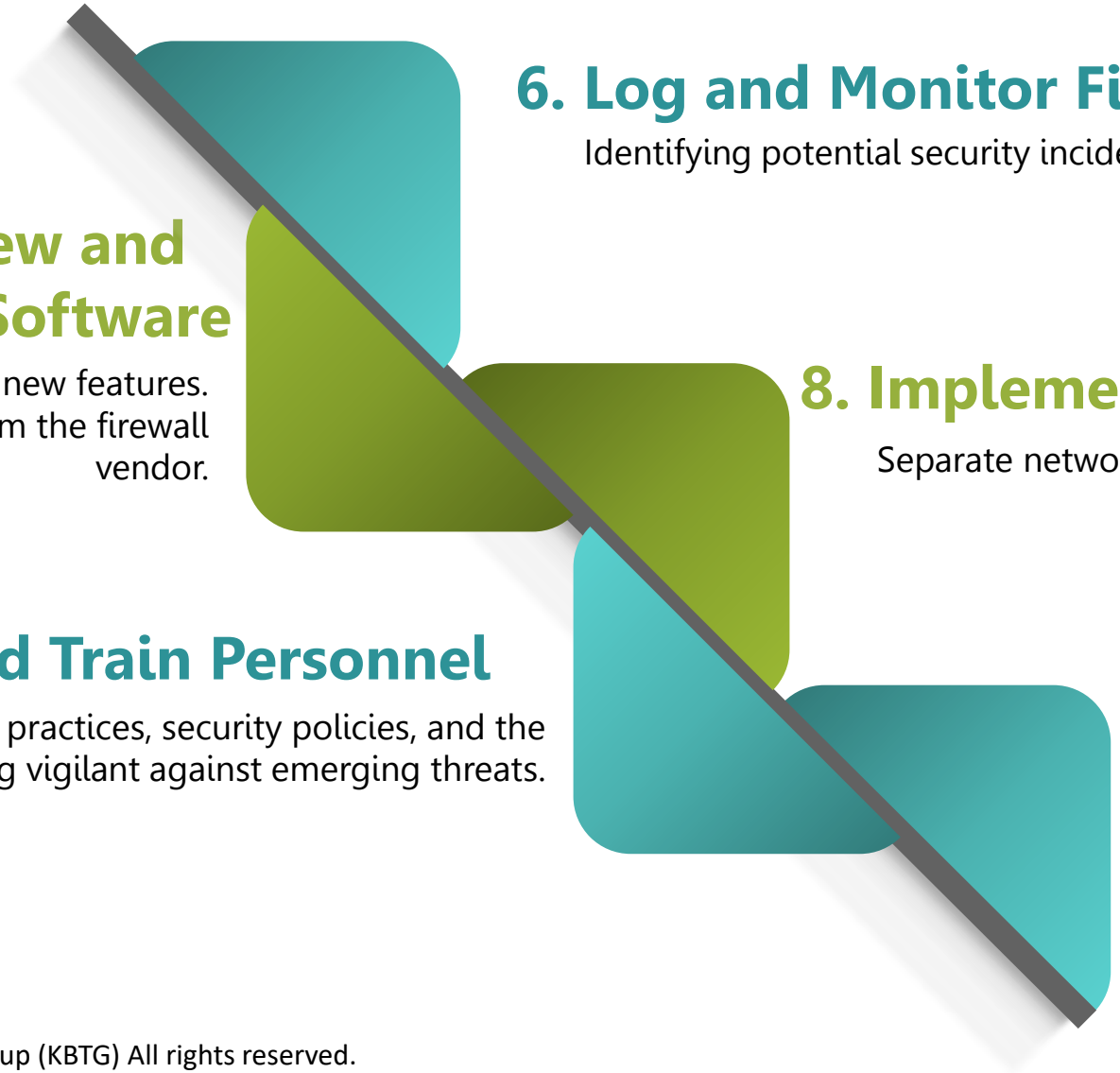
4. Regularly Update Rule Sets

Regularly review and update firewall rule sets

5. Filtering Outbound Traffic

Prevent malicious software from communicating with command-and-control servers.

Firewall Best Practices (2/2)



6. Log and Monitor Firewall Events

Identifying potential security incidents and policy violations.

7. Regularly Review and Update Firmware/Software

Security patches, bug fixes, and new features. Regularly check for updates from the firewall vendor.

8. Implement Virtual LANs (VLANs)

Separate network zone or network segmentation.

9. Educate and Train Personnel

Training firewall best practices, security policies, and the importance of staying vigilant against emerging threats.

10. Backup Firewall Configurations

Regularly back up firewall configurations to facilitate quick recovery in case of firewall failures.

14

Network Address Translation

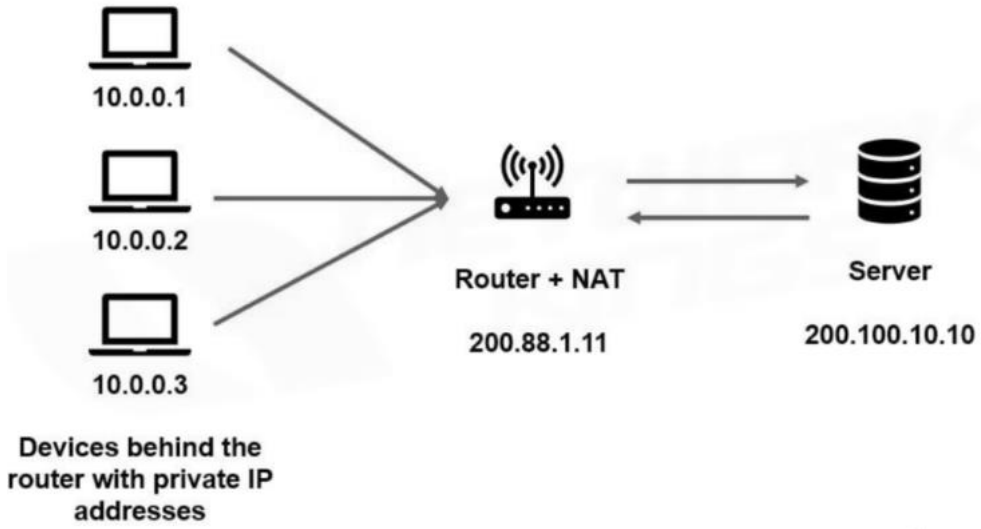
Port Address Translation

(NAT / PAT)

Network Address Translation and Port Address Translation (NAT, PAT)

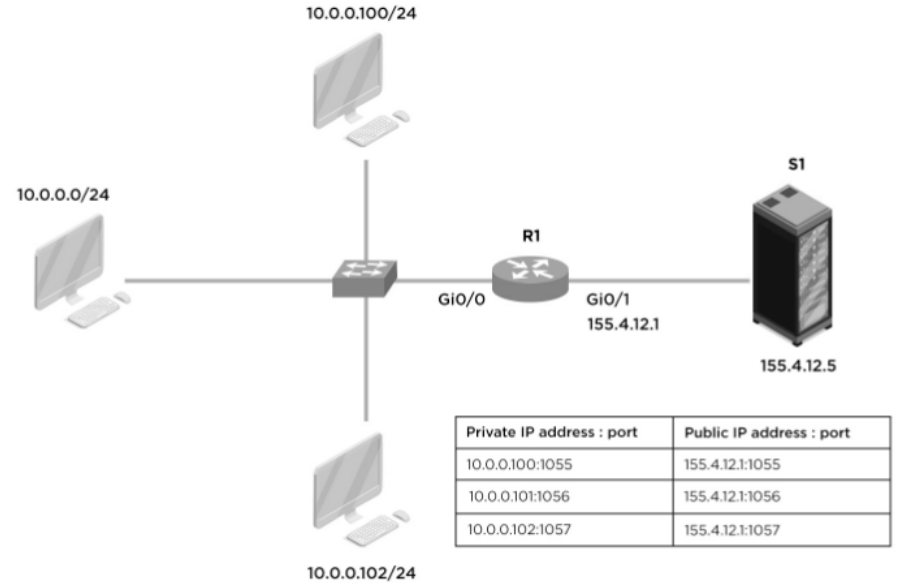
Network Address Translation

NAT allows multiple devices within a private network to share a **single public IP address** when communicating with external networks/Internet



Port Address Translation

PAT is a variation of NAT that allows multiple devices in a private network to share a single public IP address. It achieves this by **using unique port numbers to distinguish between services**.



Private IP address : port	Public IP address : port
10.0.0.100:1055	155.4.12.1:1055
10.0.0.101:1056	155.4.12.1:1056
10.0.0.102:1057	155.4.12.1:1057

Pros

- Conserves public IP addresses.
- Enhances security by hiding internal network structure.
- Facilitates the use of private IP addresses within organizations.

Cons

- Configuring and managing policies can be complex, especially in larger networks
- Single point of failure

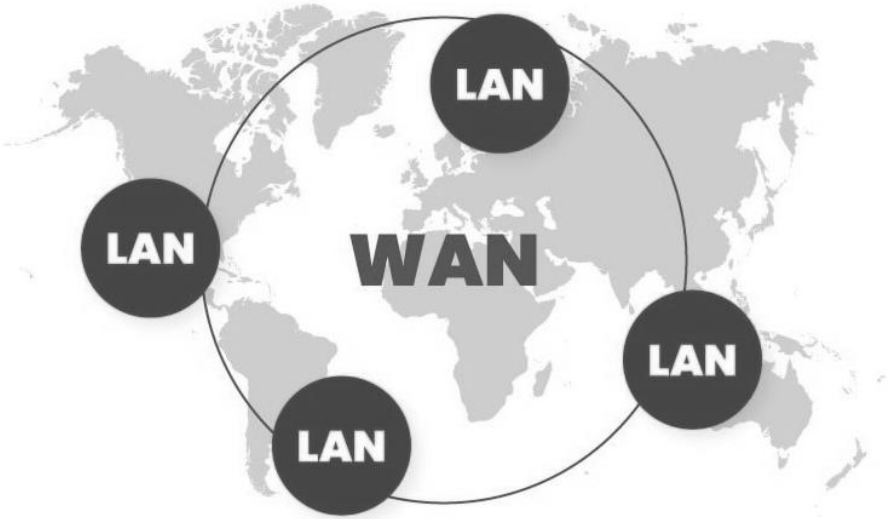
15

WAN Technology

LAN and WAN

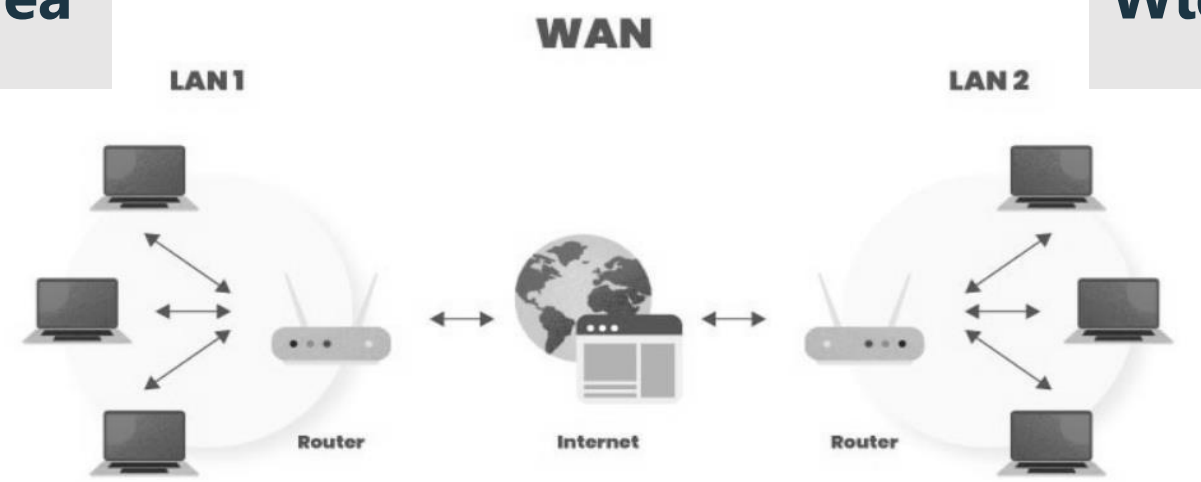
Local Area Network (LAN)

High Speed
Small Physical Area

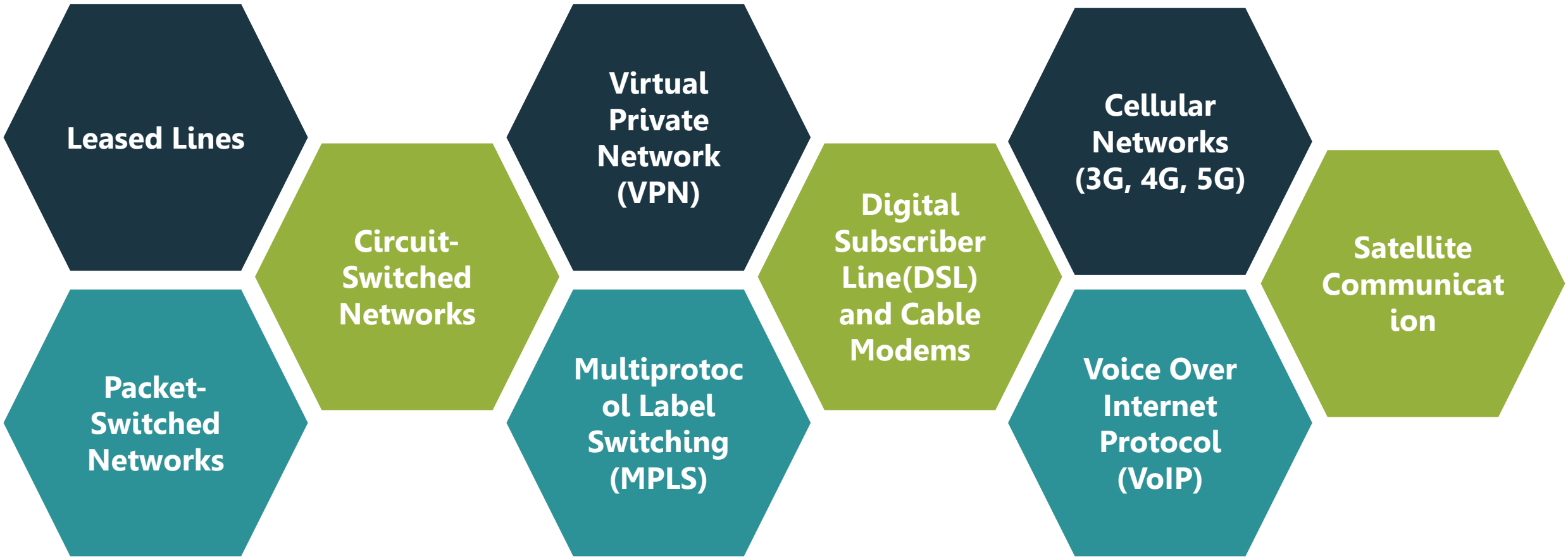


Wide Area Network (WAN)

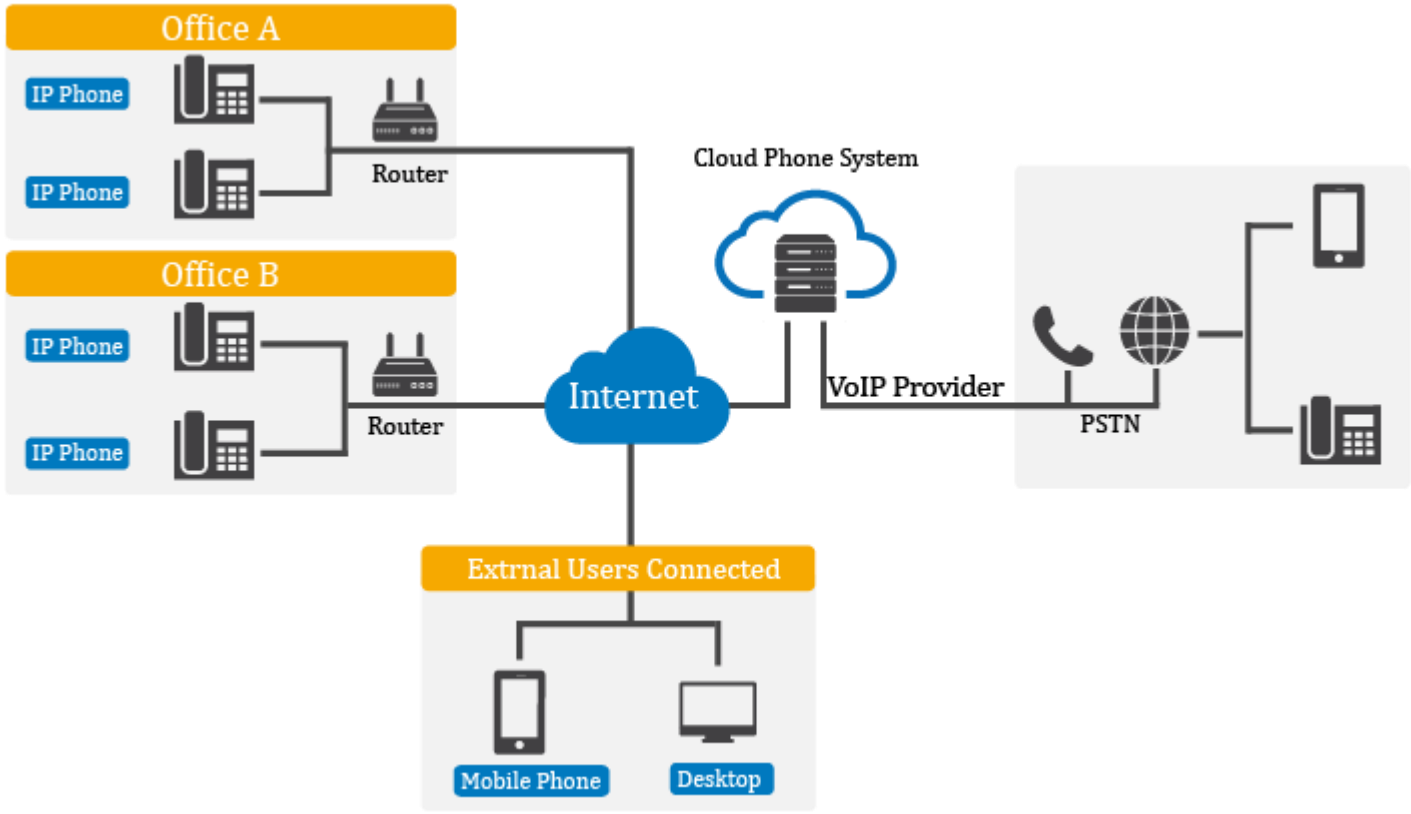
Slow Speed
Wide Geolocation Area



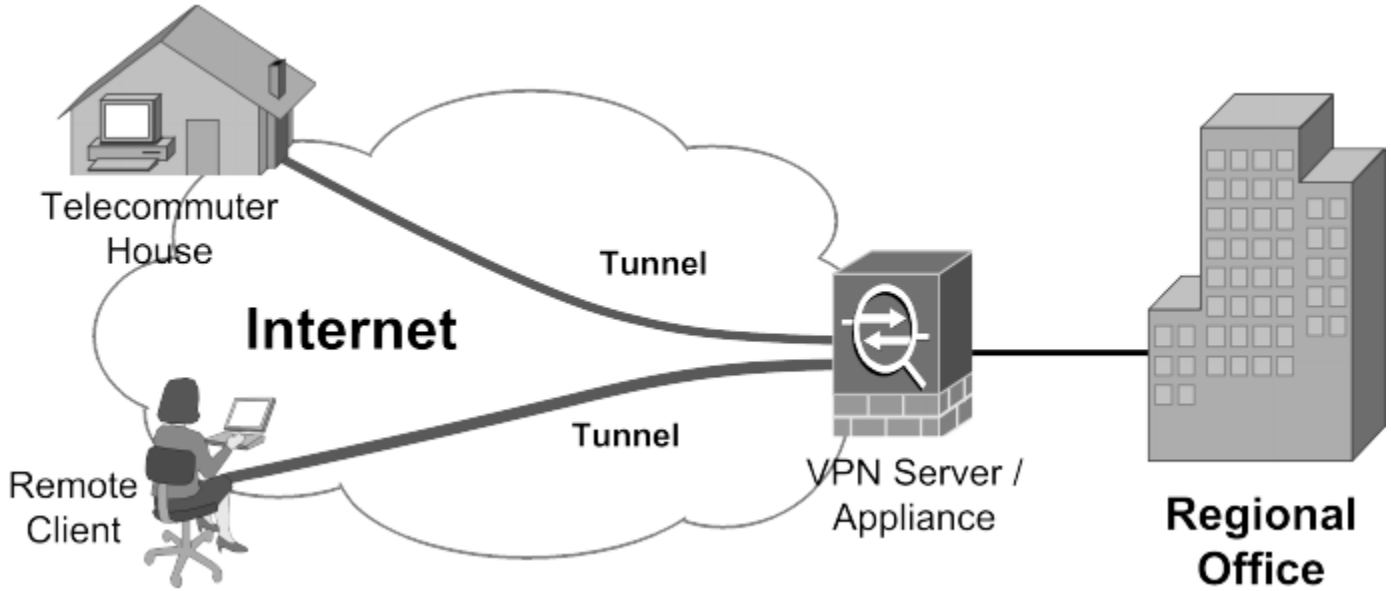
WAN Technology



WAN Technology - VoIP



WAN Technology - VPN



NordVPN®

Surfshark®

Pulse Secure

OPENVPN

Private Internet ACCESS®

16

Remote Access Protocol

Remote Access Protocol

Tunneling

- SSL/TLS (Secure Sockets Layer/Transport Layer Security)
- IPsec (Internet Protocol Security)
- VPN (Virtual Private Network)
- WPA (Wi-Fi Protected Access)

Remote Access Tools

- Remote Desktop Connection
- Secure Shell (SSH)
- TeamViewer

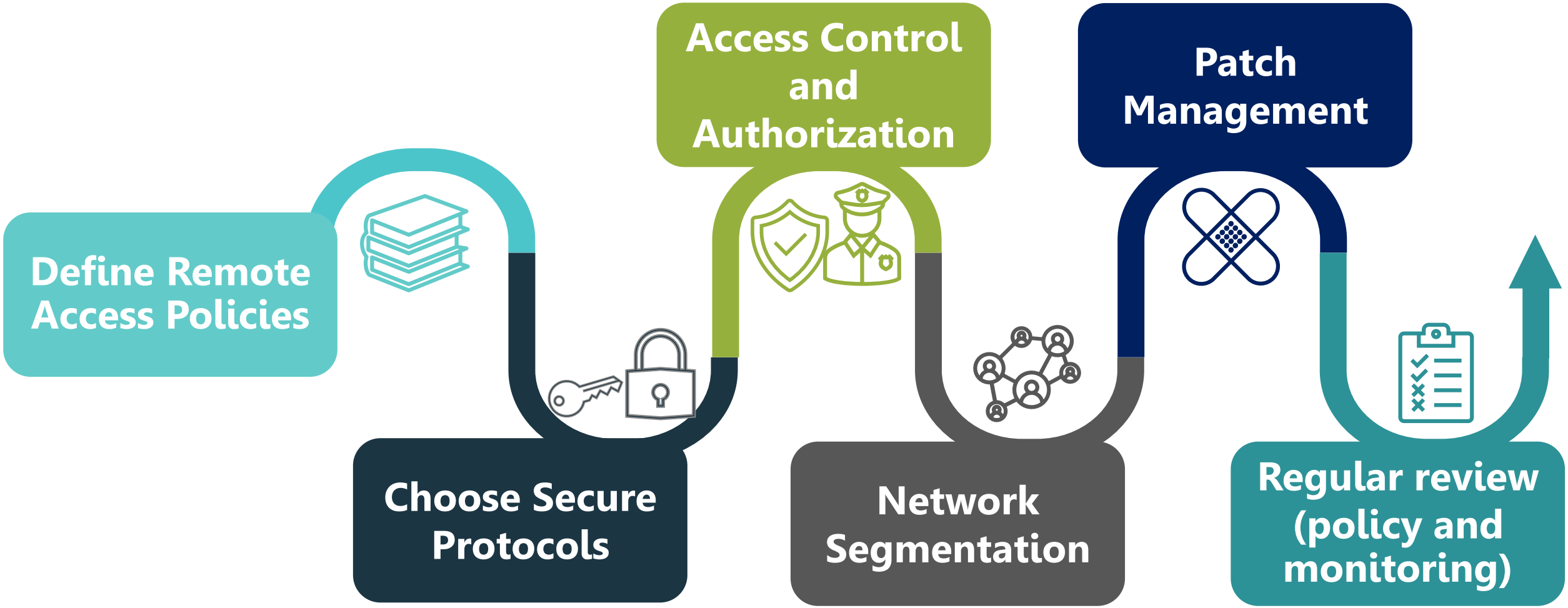
Authentication

- Password
- Multi factor authentication (MFA)
- Certificate
- Device
- Biometric

17

Managing Remote Desktop

Managing Remote Desktop



18

Tunneling Protocols

Tunneling Protocols

Objective

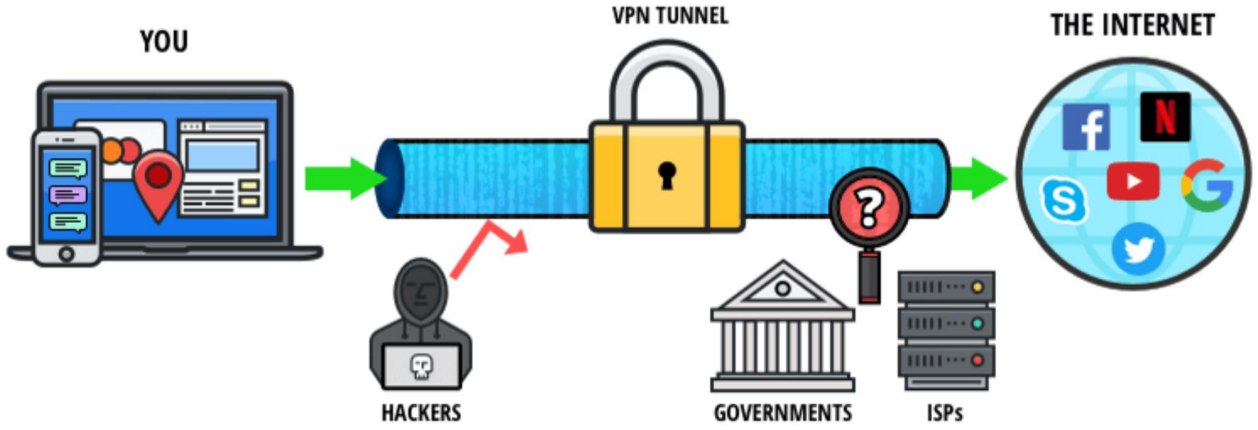
01 Privacy and Confidentiality

02 Data Integrity

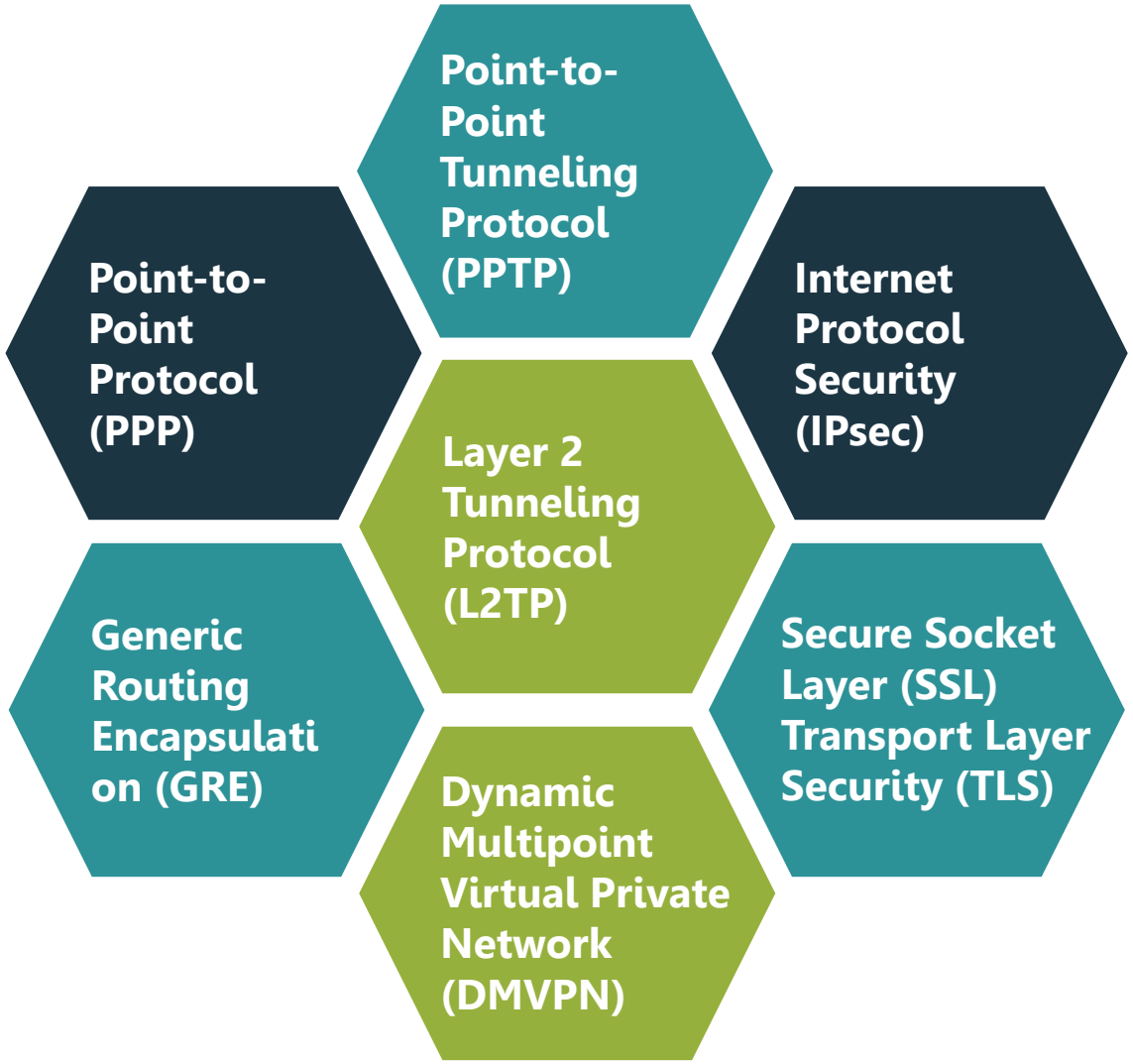
03 Authentication

04 Secure Data Transmission Across Untrusted Networks

05 Network Segmentation



Tunneling Protocols



Samples

- VPN Services
- Secure Online Transactions
- Secure Communication Apps
- Video Conferencing Security
- Secure Email Access

19

Wireless Networking And Wireless Security

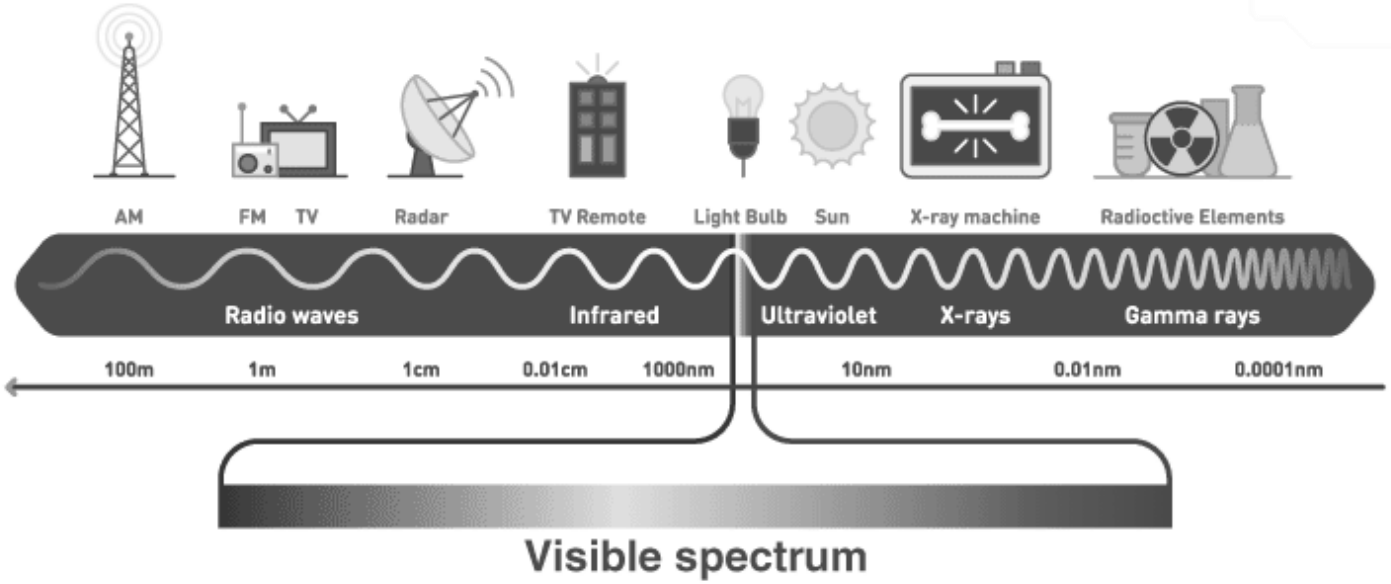
Wireless Networking

Infrared

Bluetooth

Wi-Fi

Radio Signal



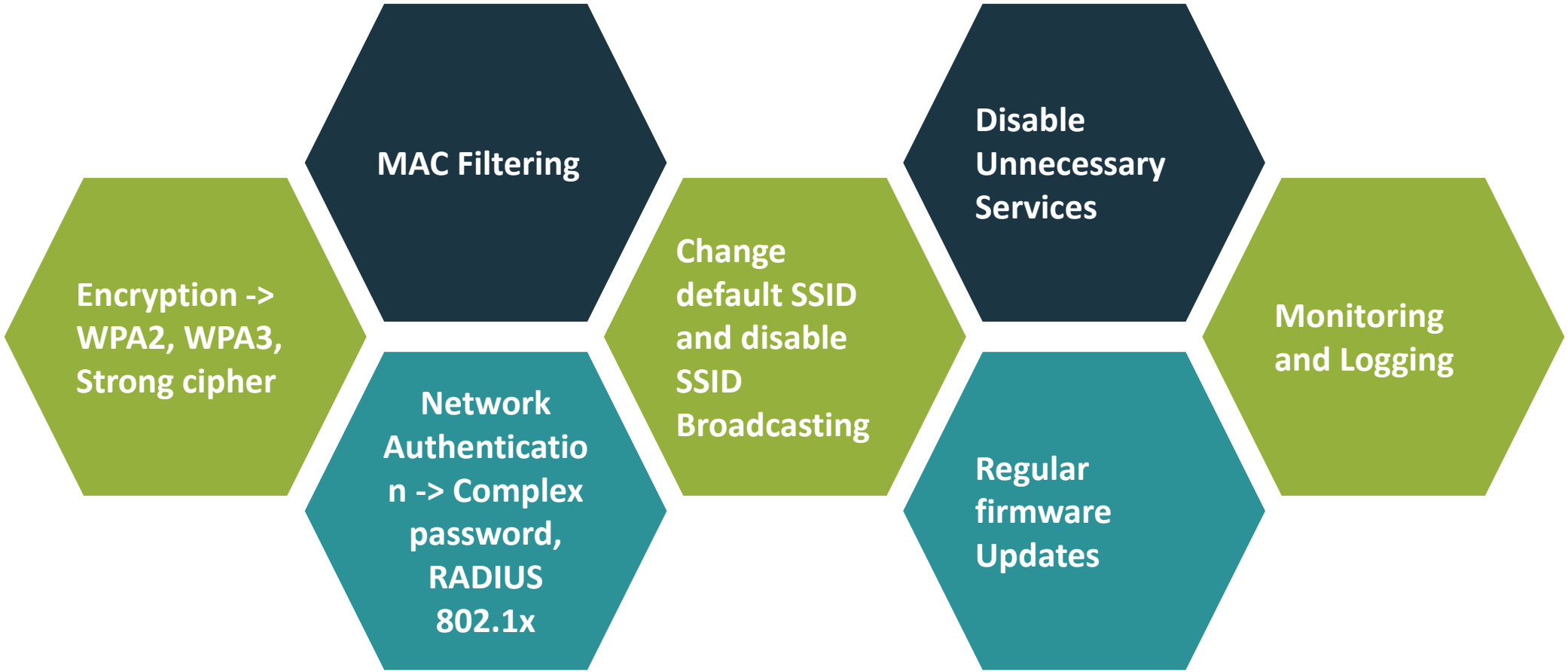
Pros

- Low cost -> Low cost to deploy and implementation
- Mobility and simplicity -> easy and fast to deploy without cabled network
- Maintainability -> easy to maintenance

Cons

- Latency and Speed -> Depend on locations within the coverage
- Wi-Fi signals that exceed the intended range. -> Unauthorized access, Sniffing, War Driving

Wireless Security



END

Summary

Implementation!!
Risk management
Monitoring and measurement

What do we protect?
Why we do that ?