ECE/CS230
Computer Systems Security

Charalambos (Harrys) Konstantinou

https://sites.google.com/view/ececs230kaust

Network security

Overview

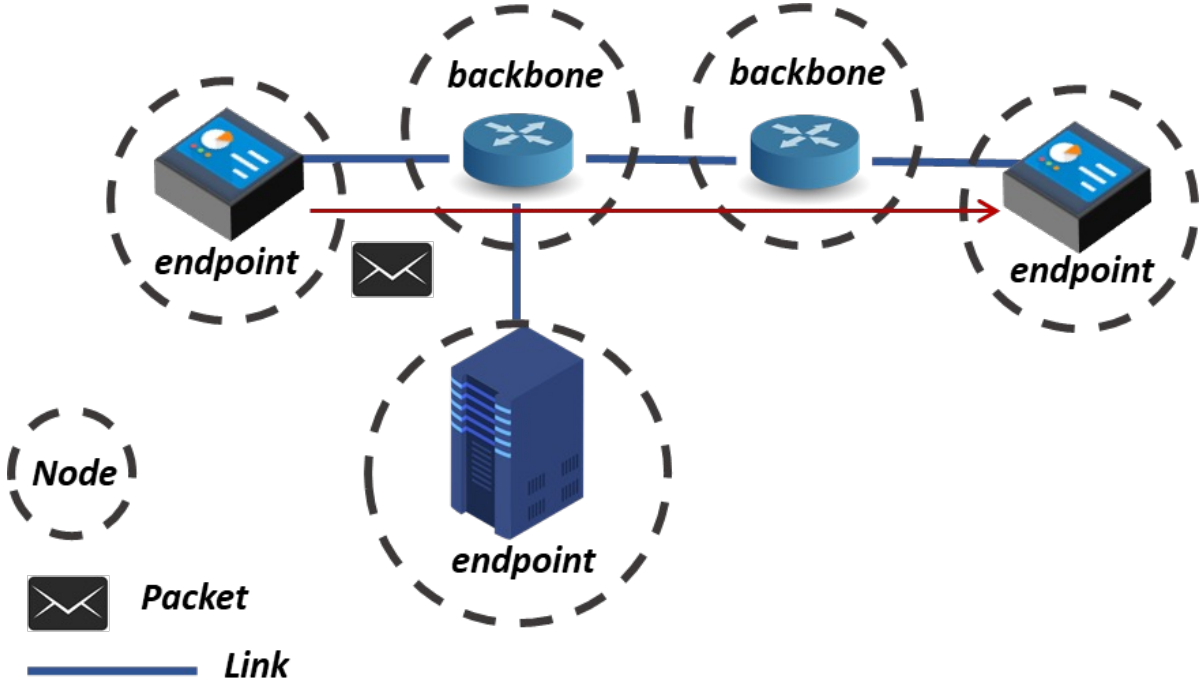
1. Network Basics
2. Threats on Communication Networks
3. Example Threats in Communication Networks
4. Methods to Secure Communication Networks

Network Basics: Nomenclature

- **Nodes:** A point used for redistribution or endpoint.
- **Links (Medium):** A communication channel that connects two or more devices for data transmission.
- **Protocols:** A system of rules to transmit messages between two/more computational entities.
- **Packets:** A small segment of a larger message
  - - Names for ‘packets’ at different layers
    - Segments (Transport Layer)
    - Datagram (Network Layer)/Packet
    - Frames (Link Layer)

Network Basics: Nomenclature

- **Nodes**
- **Links**
- **Protocols**
- **Packets**



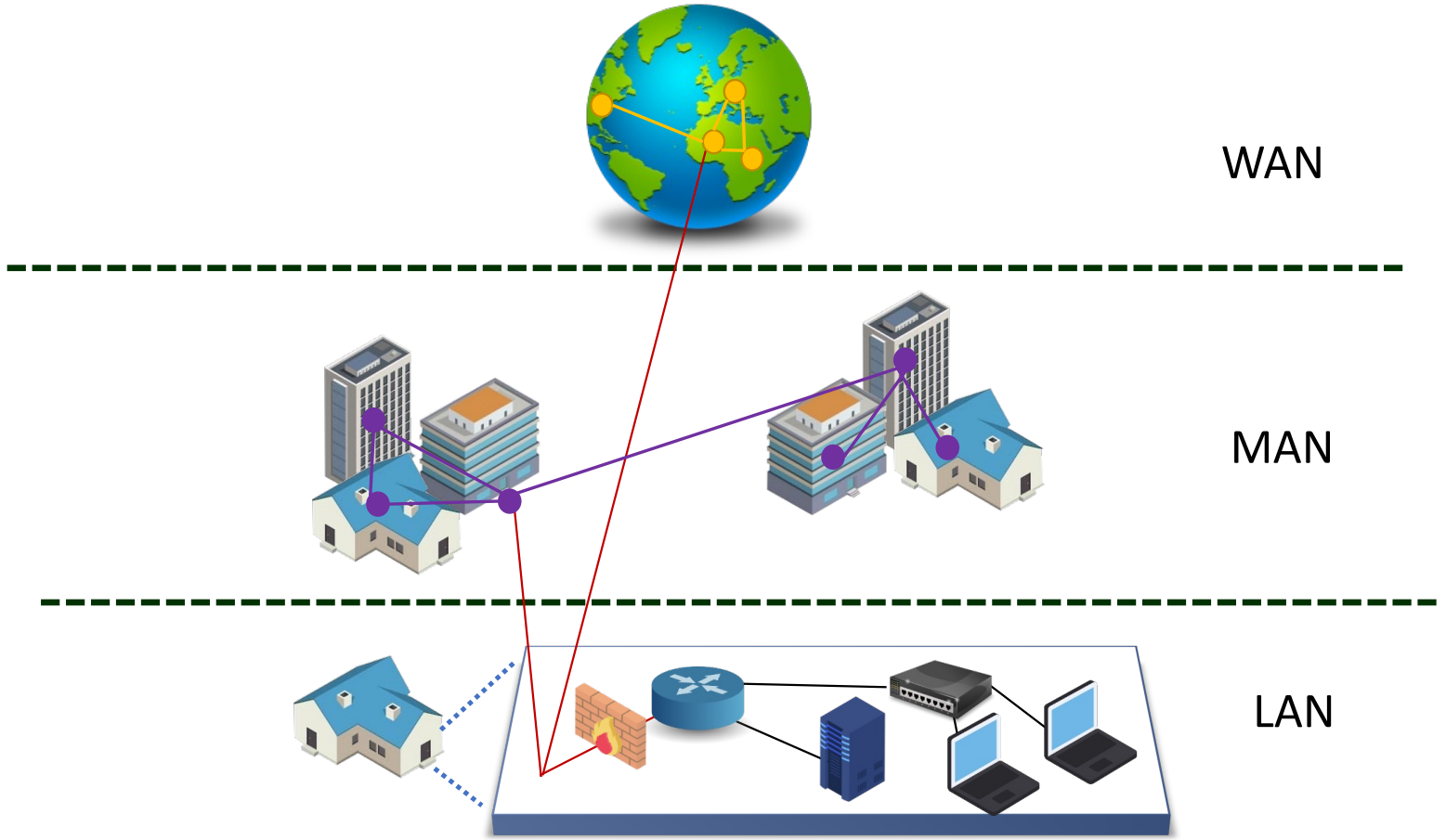
Network Basics: Types of Comm. Networks

- **Local Area Networks (LAN):** Private for buildings, houses, etc.
- **Municipal Area Networks (MAN**): Larger network that may span several buildings in cities.
- **Wide Area Networks (WAN): Not restricted to geographical location & connects several LANs.**

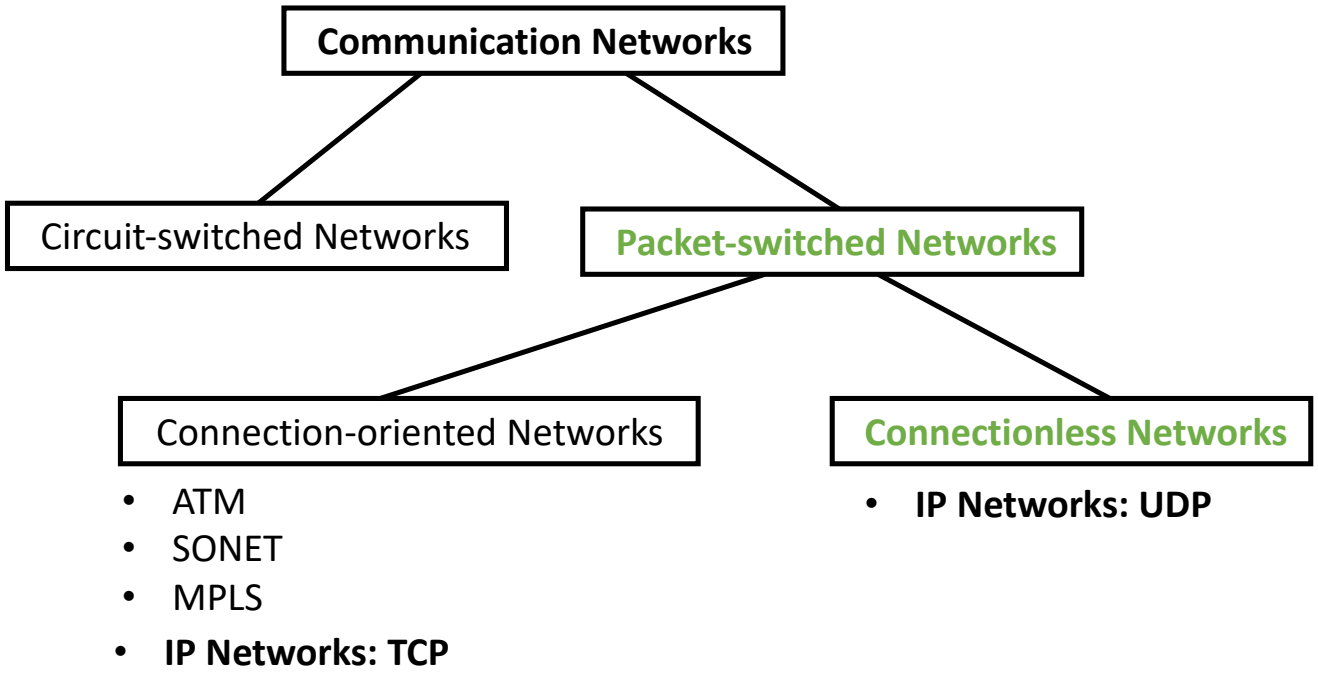
Internet: Combination of two or more types of networks (mostly WANs & LANs).

https://www.studytonight.com/computer-networks/types-of-networks

Network Basics: Types of Comm. Networks

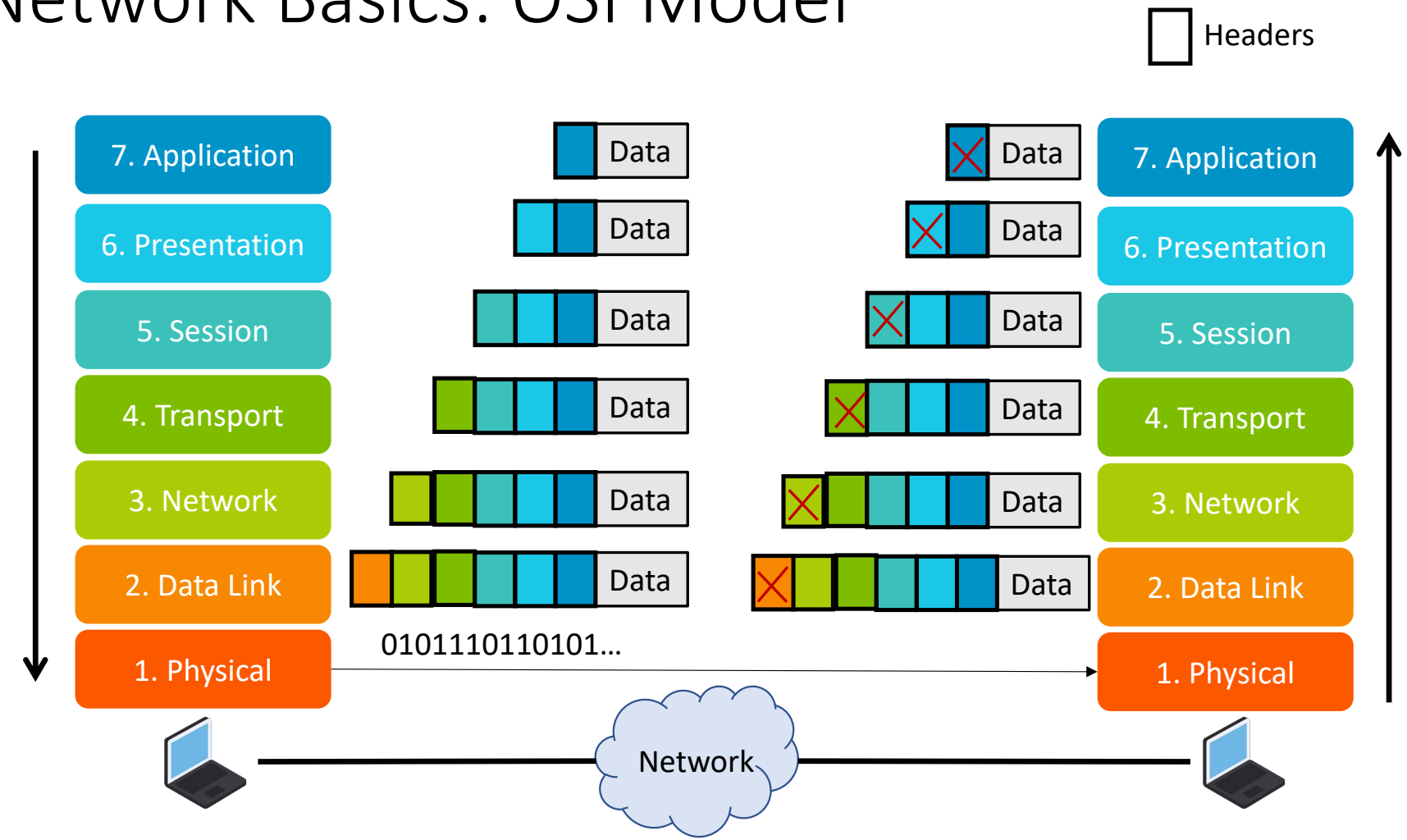


Network Basics: Connection-oriented vs. Connectionless networks



Perros, Harry G. *Connection-oriented networks: SONET/SDH, ATM, MPLS and optical networks*. John Wiley & Sons, 2005.

Network Basics: OSI Model



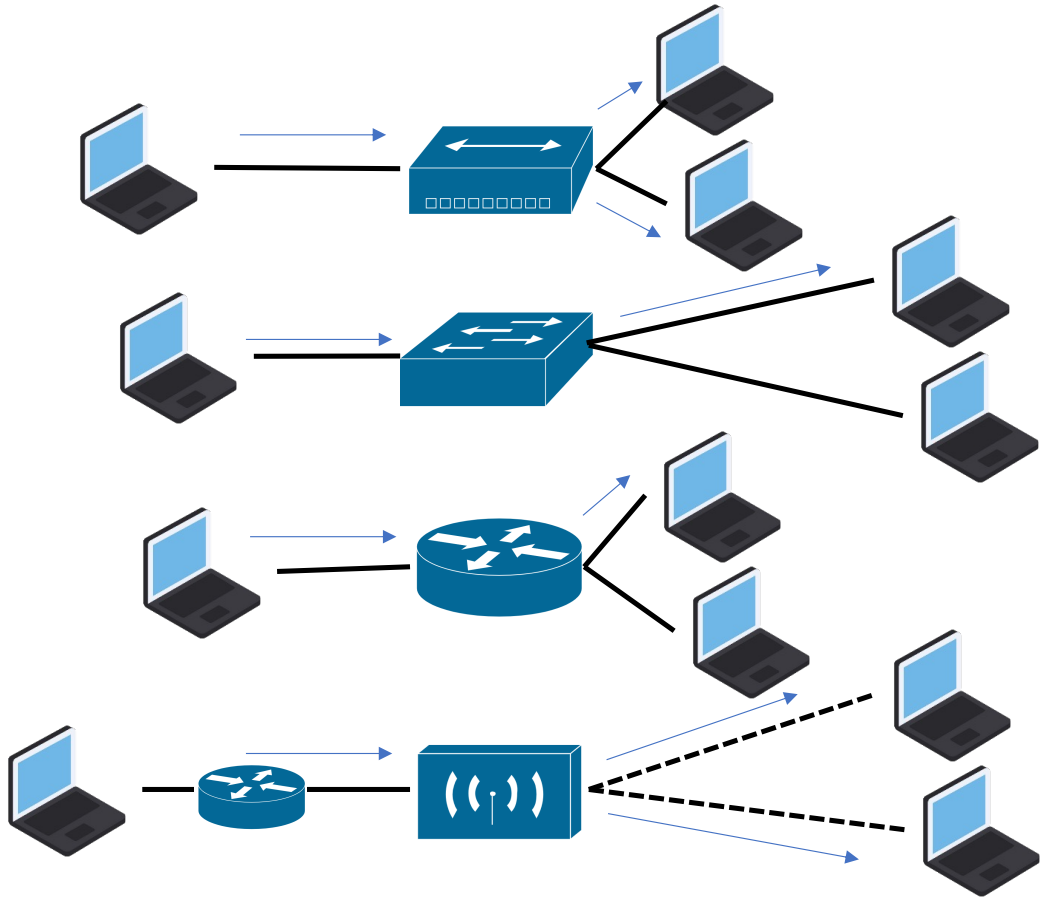
Network Basics: Communication Network Elements

Layer 1
- **Hubs:** *Packets received at port are copied to **other ports.***

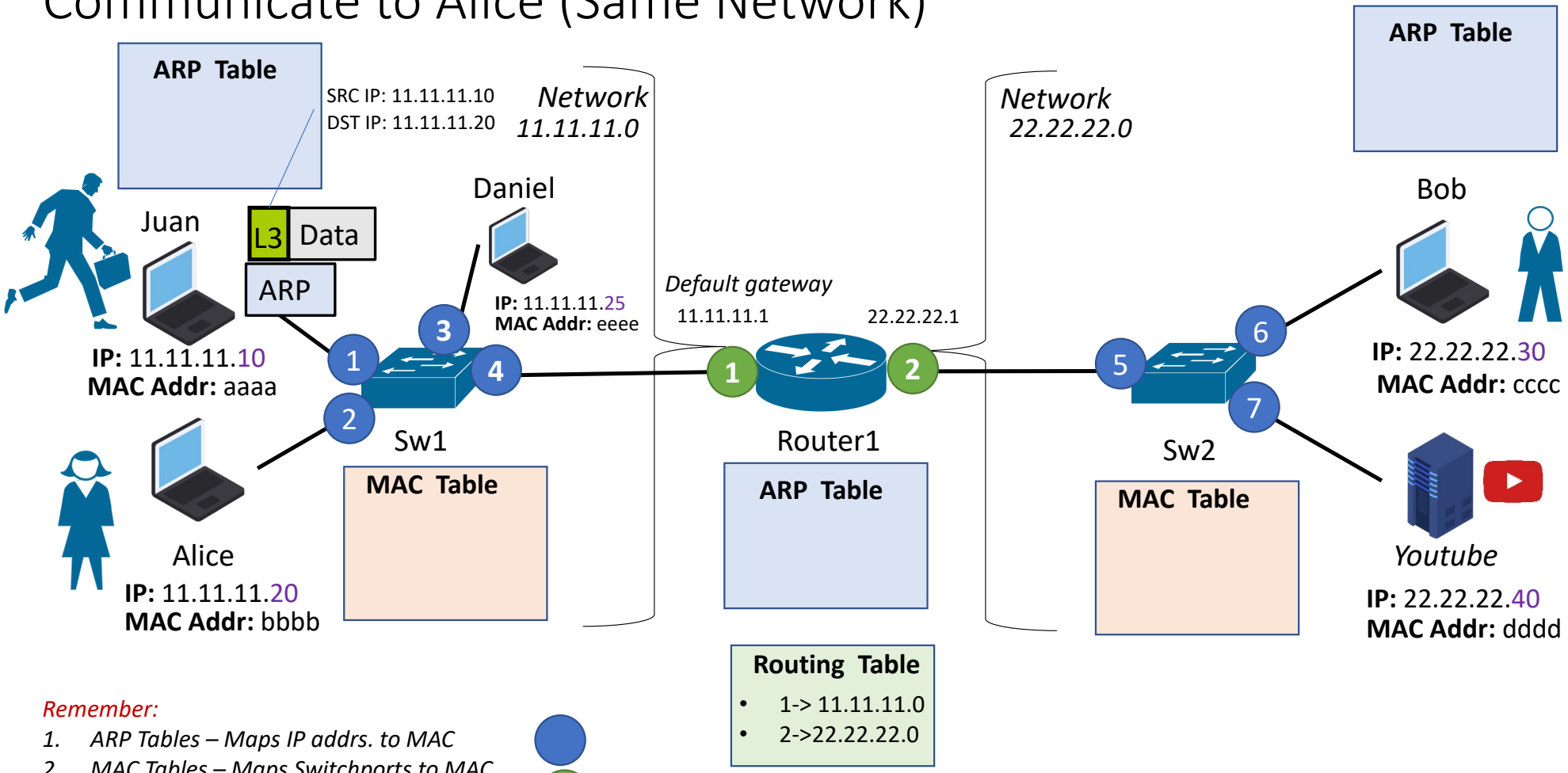
Layer 2
- **Switches:** *Forward packets along same networks.*

Layer 3
- **Routers:** *Forward packets along different networks.*

- **Access Points (Wireless):** *Relays data between wired network and wireless devices.*



Network Basics: How a Packet Travels through a Network – Communicate to Alice (Same Network)

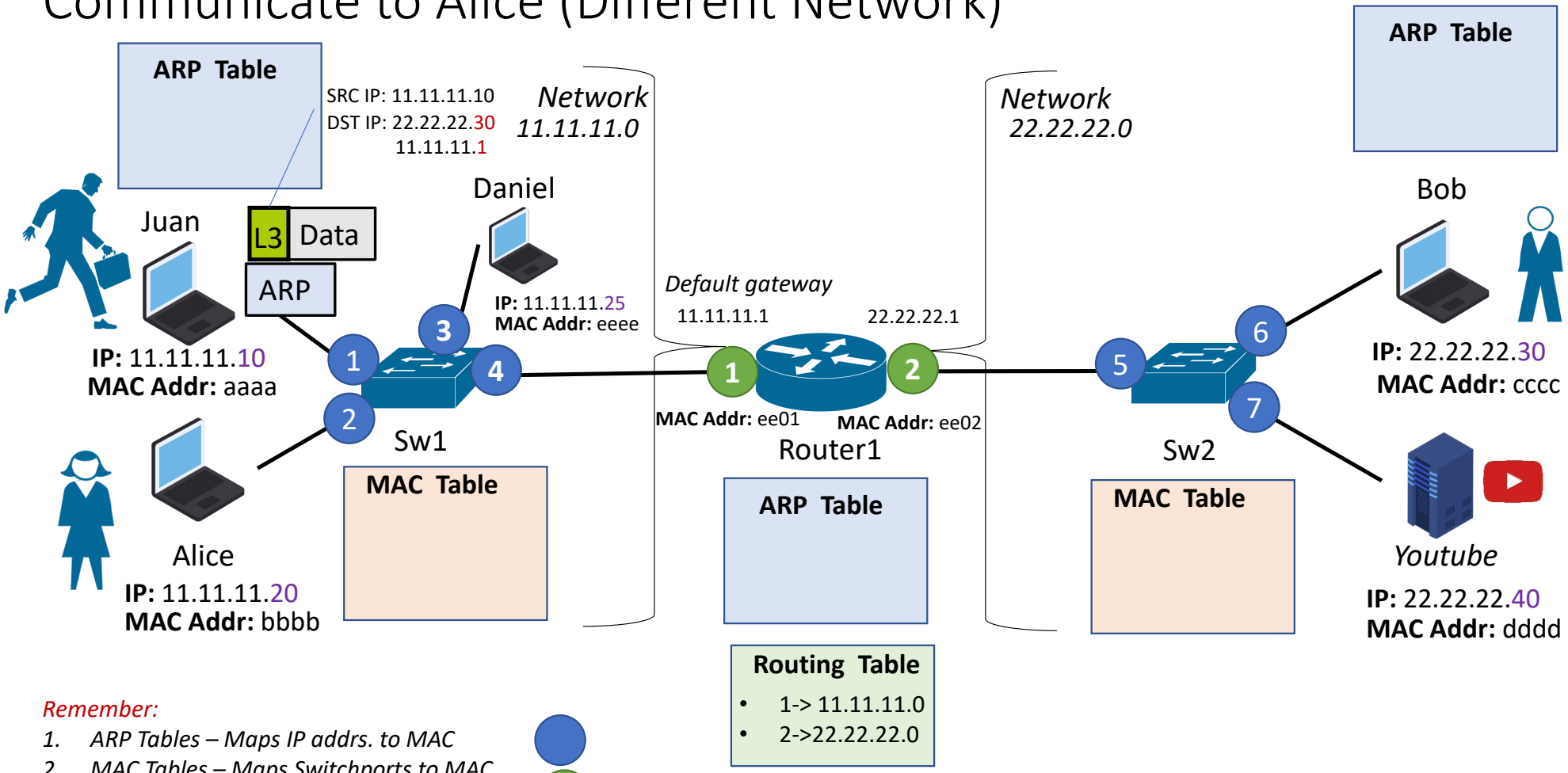


Remember:

1. *ARP Tables – Maps IP addrs. to MAC*
2. *MAC Tables – Maps Switchports to MAC*
3. *Routing Tables – Map IP addrs. to Interfaces*

https://www.practicalnetworking.net/series/packet-traveling/packet-traveling/

Network Basics: How a Packet Travels through a Network – Communicate to Alice (Different Network)



Remember:

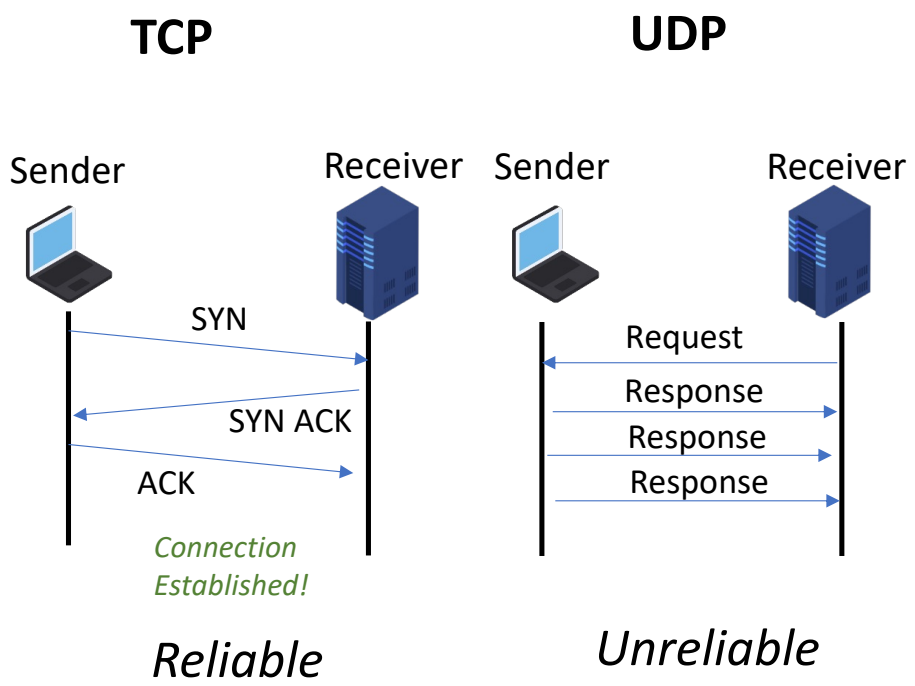
1. *ARP Tables – Maps IP addrs. to MAC*
2. *MAC Tables – Maps Switchports to MAC*
3. *Routing Tables – Map IP addrs. to Interfaces*

https://www.practicalnetworking.net/series/packet-traveling/packet-traveling/

Network Basics: TCP vs. UDP

- What is TCP?
  - Transmission Control Protocol (TCP)
  - Connection-oriented protocol
  - With error checking & guarantees data delivery (if nor retries)
  - **EX: File transfers, Email**

- What is UDP?
  - User Datagram Protocol (UDP)
  - Connectionless protocol
  - No error checking & not guarantee data delivery
  - **EX: Videos, Online games**



Network Basics: Communication Media

TABLE 6-1 Communications Media Strengths and Weaknesses

Medium	Strengths	Weaknesses
Wire	• Widely used • Inexpensive to buy, install, maintain	• Susceptible to emanation • Susceptible to physical wiretapping
Optical fiber	• Immune to emanation • Difficult to wiretap	• Potentially exposed at connection points
Microwave	• Strong signal, not seriously affected by weather	• Exposed to interception along path of transmission • Requires line of sight location • Signal must be repeated approximately every 30 miles (50 kilometers)
Wireless (radio, WiFi)	• Widely available • Built into many computers	• Signal degrades over distance; suitable for short range • Signal interceptable in circular pattern around transmitter
Satellite	• Strong, fast signal	• Delay due to distance signal travels up and down • Signal exposed over wide area at receiving end

Threats on Communication Networks: Terminology

Threats: Set of circumstances that has the potential to cause loss or harm.

- *interception*, or unauthorized viewing (confidentiality)
- *modification*, or unauthorized change (integrity failures)
- *fabrication*, or unauthorized creation (integrity failures)
- *interruption*, or preventing authorized access (accessibility)

Vulnerability: A weakness in the system.

Attack: Exploiting a vulnerability; by person or computer system.

Control: A protective measure.

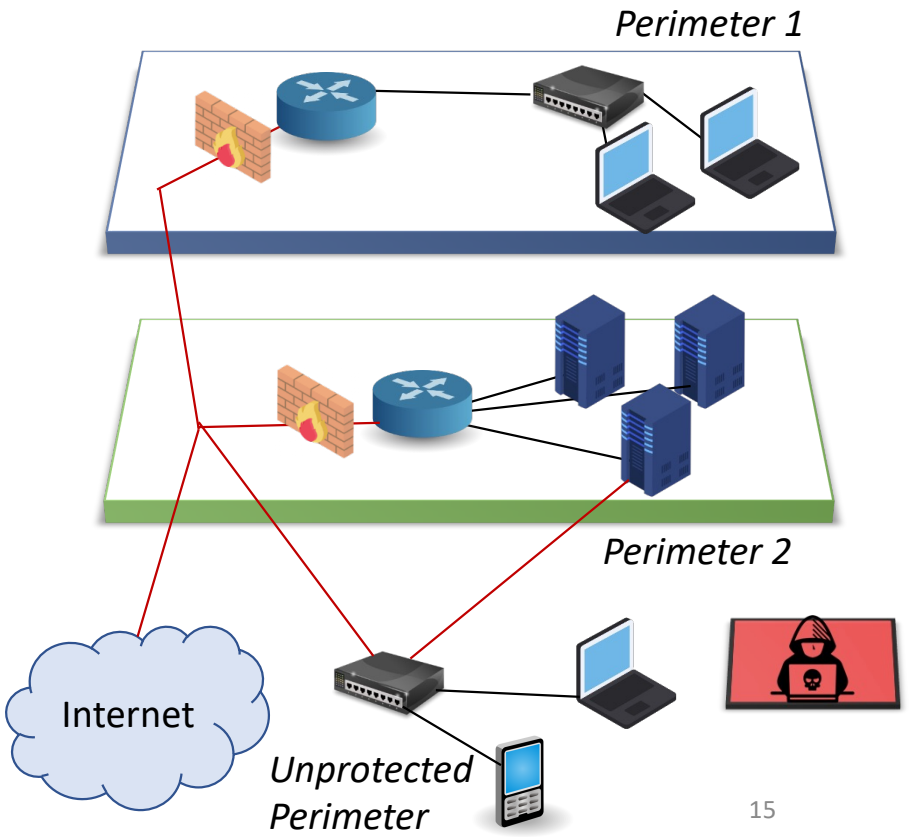
- A technique that removes or reduces a vulnerability

A *threat* is blocked by *control* of a *vulnerability*.

Threats on Communication Networks: What Makes a Network Vulnerable?

What Makes a Network Vulnerable?

- **Anonymity** (An attacker can attempt many attacks, anonymously, from thousands of miles away)
- **Large networks** mean **many points of potential entry** (Many points of attack)
- **Sharing** (Share resources may expose vulnerabilities)
- **Network complexity** (Hard to protect diverse systems with different OS, vulnerabilities)
- **Unknown perimeter** (Complex networks change all the time so may open up potential access vulnerabilities)
- **Unknown path** (There may be many paths, including untrustworthy ones, from one host to another)



Threats on Communication Networks: Security Goals & Threats to the Triad

CIA (Confidentiality, Integrity, Accessibility) Triad

- Confidentiality:
  - Only authorized people or computers can access the data.
  - Known as in networking community as Wiretapping (even if no physical wire involved)
- Integrity:
  - The data can only be modified by authorized people or computers.
  - Known as in networking community as Data Corruption
- Accessibility:
  - The data is accessible to authorized people or computer when they need it.
  - Related to attacks such as Denial of Service (DoS)

A successful attack violates one or more of these goals.

Threats on Communication Networks: Interception/Wiretapping (Confidentiality)

Wiretapping is the name given to data **interception**, often covert and unauthorized.

- The name wiretap refers to the **original mechanism**, which was a device that was attached to a wire to split off a second pathway that data.
- Users generally have little control over the routing of a signal.
  - In an internet call example, a call from New York to Sydney might travel west by satellite, transfer to an undersea cable, and reach the ultimate destination on conventional wire.
  - Along the way, the signal could pass through different countries, as well as international regions of the oceans and sky.
  - Along the way may be people with method, opportunity, and motive to obtain your data.
- That is why a WAN can be far **riskier** than a well-controlled LAN.
- Encryption is the **strongest and most commonly used countermeasure** against **interception**.
- Others:
  - physical security (protecting the communications lines themselves)
  - dedicated lines
  - controlled routing (ensuring that a communication travels only along certain paths)

Threats on Communication Networks: Modification & Fabrication (Integrity)

- **Data corruption**
  - May be intentional or unintentional, malicious or non-malicious, directed or random
- **Sequencing**
  - Permuting the order of data, such as packets arriving in sequence
- **Substitution**
  - Replacement of one piece of a data stream with another
- **Insertion**
  - A form of substitution in which data values are inserted into a stream
- **Replay**
  - Legitimate data are intercepted and reused

Threats on Communication Networks: Interruption/DoS (Accessibility)

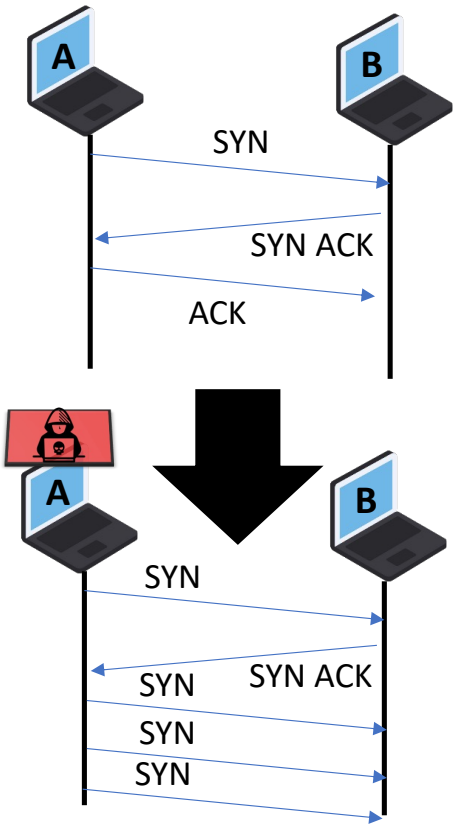
- **Routing**
  - Internet routing protocols are complicated, and one misconfiguration can poison the data of many routers
- **Excessive demand**
  - Network capacity is finite and can be exhausted; an attacker can generate enough demand to overwhelm a critical part of a network
- **Component failure**
  - Component failures tend to be sporadic and unpredictable, and will cause loss of service if not planned for

Example Attacks on Communication Networks: Major Cyber-Attacks in Networks

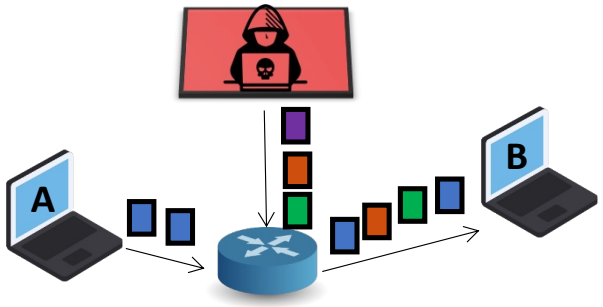
	Protocol attacks:	**Routing attacks:**	**Intrusions:**
	• Exploits a weakness in the **layer 3** and **4** of the **OSI model**.	• Network layer attacks such as **spoofing**, **replay**, and **selective forwarding** attacks.	• **Unauthorized** activity, execution or access to unauthorized information.
Affects	1. Controllers 2. Routers 3. Switches 4. Network equipment	1. Controllers 2. Routers 3. Switches 4. Network equipment 5. Operator workstations	1. HMI 2. Access control systems 3. Applications servers 4. ICS comm. networks
Examples:	TCP SYN Flooding Attack UDP Flooding Ping Flooding ‘’DoS’’	IP Spoofing Replay	Unauthorized access Rootkits Worms Malware

Example Attacks on Communication Networks: Major Cyber-Attacks in Networks

TCP SYN Flooding Attack

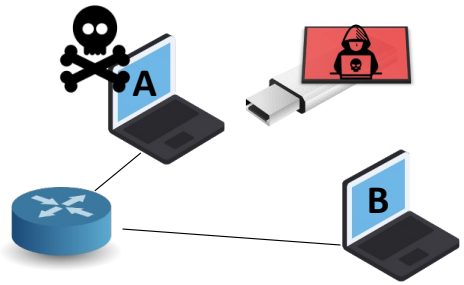


IP Spoofing

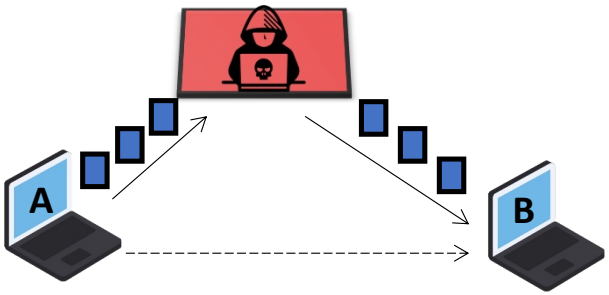


Malware/Rootkits

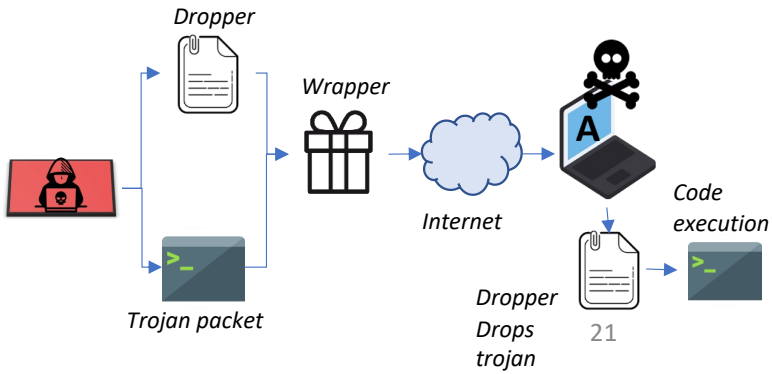
(Could be Insider threats)



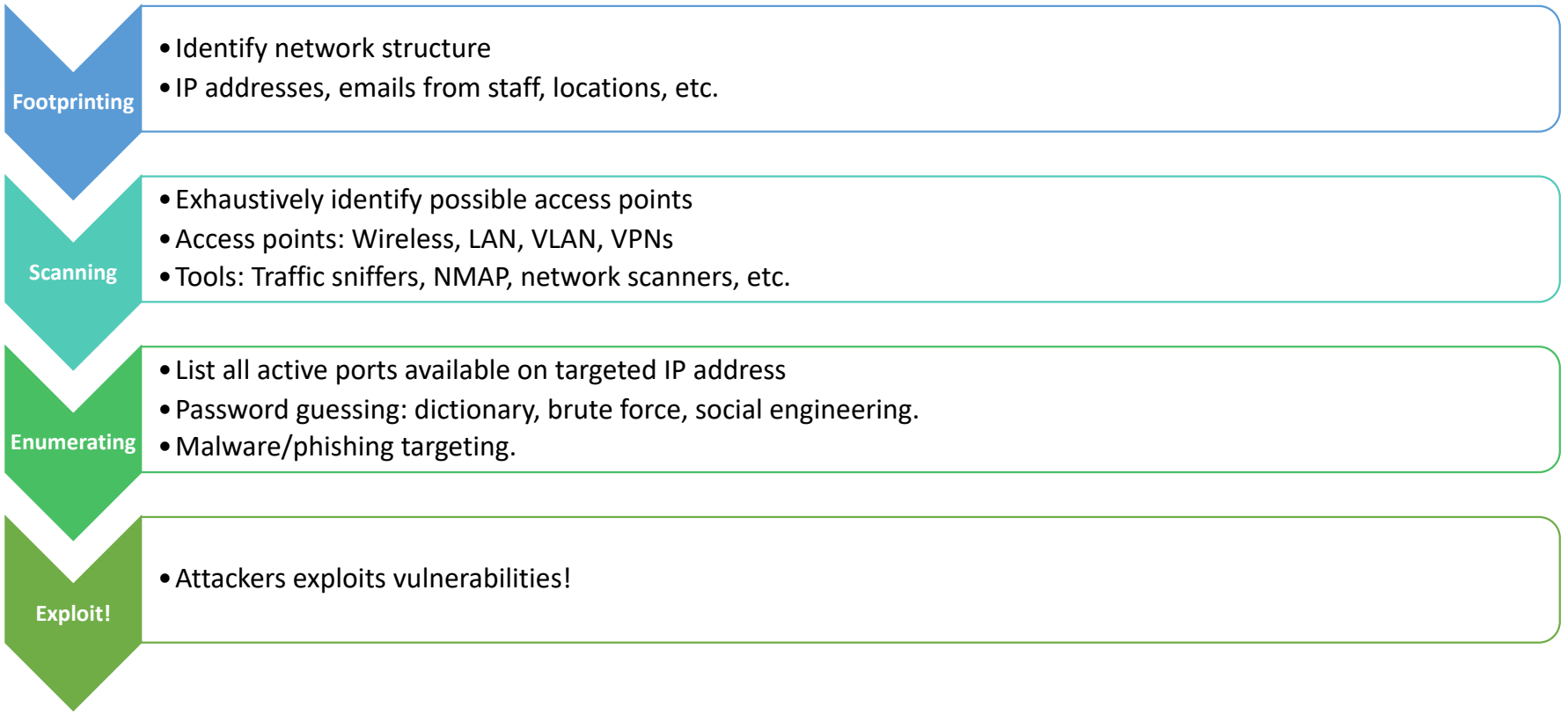
Replay (MiTM)



Trojans



Example Attacks on Communication Networks: Cyber Intrusion Process



Methods to Secure Communication Networks: How to achieve them?

Confidentiality

- Message content should be accessed by authorized users only
- Achieved by **Encryption**

Integrity

- Making sure message was not altered during transit or later
- Achieved by using **Hashing**

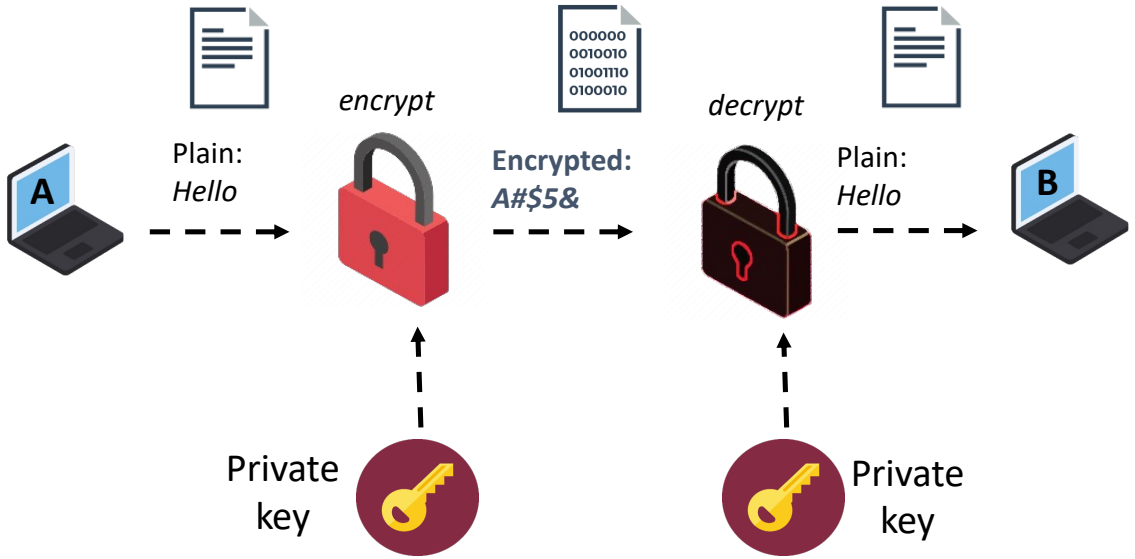
Availability

- Services must be accessible and available to authorize users
- Achieved by **Protections**: Firewalls, IDS, VPNs

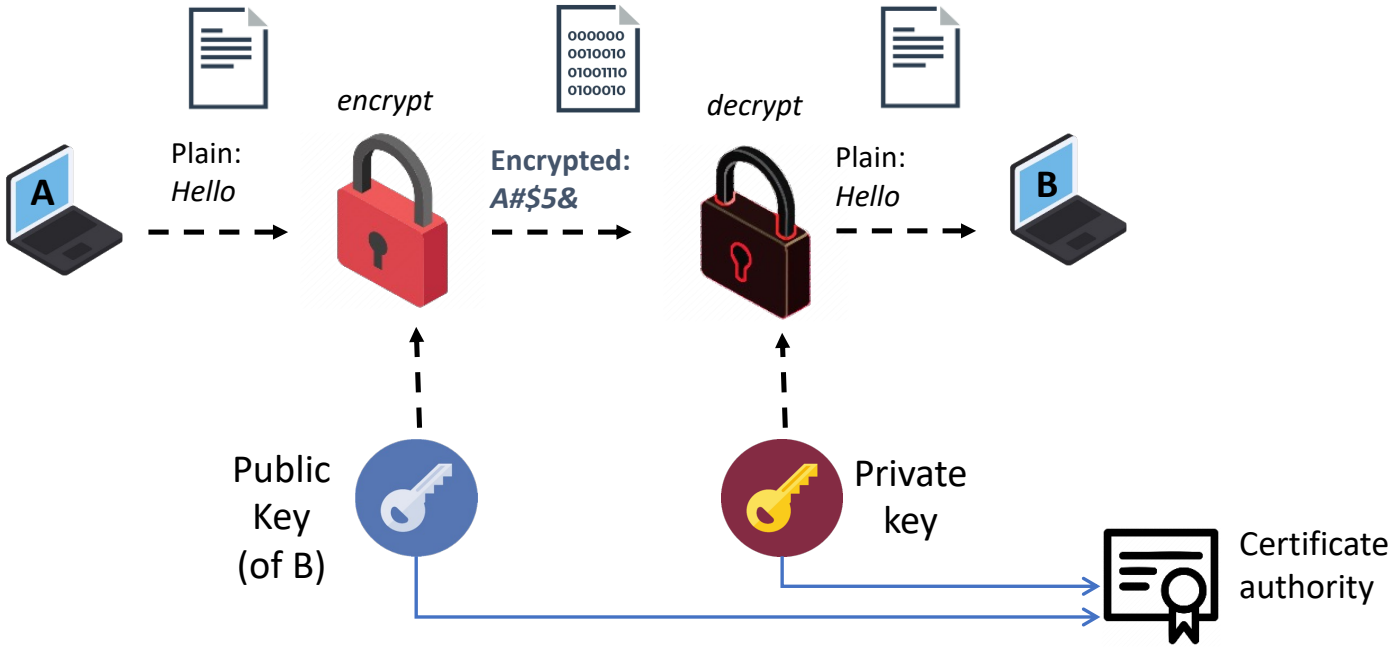
Authentication

- Sender & receiver need to confirm identity of each other
- Achieved by the use of **Digital Signatures**

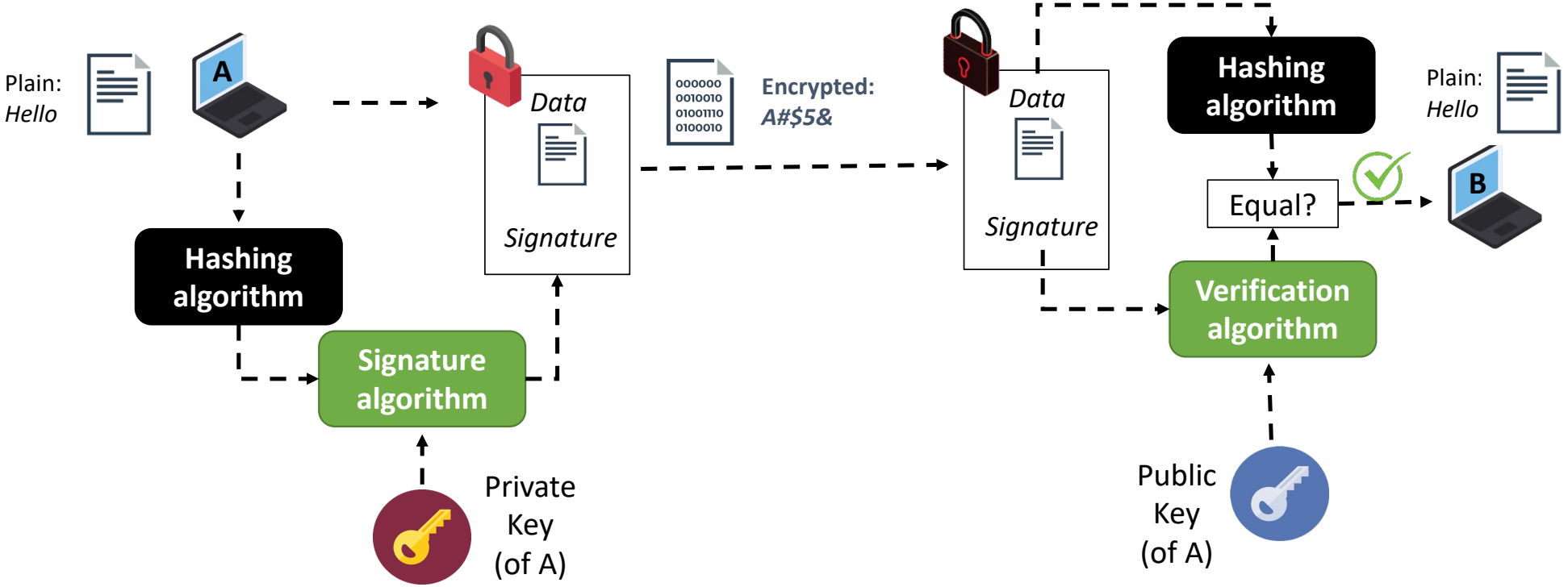
Methods to Secure Communication Networks: Symmetric Key Encryption



Methods to Secure Communication Networks: Asymmetric Key Encryption



Methods to Secure Communication Networks: Digital Signatures



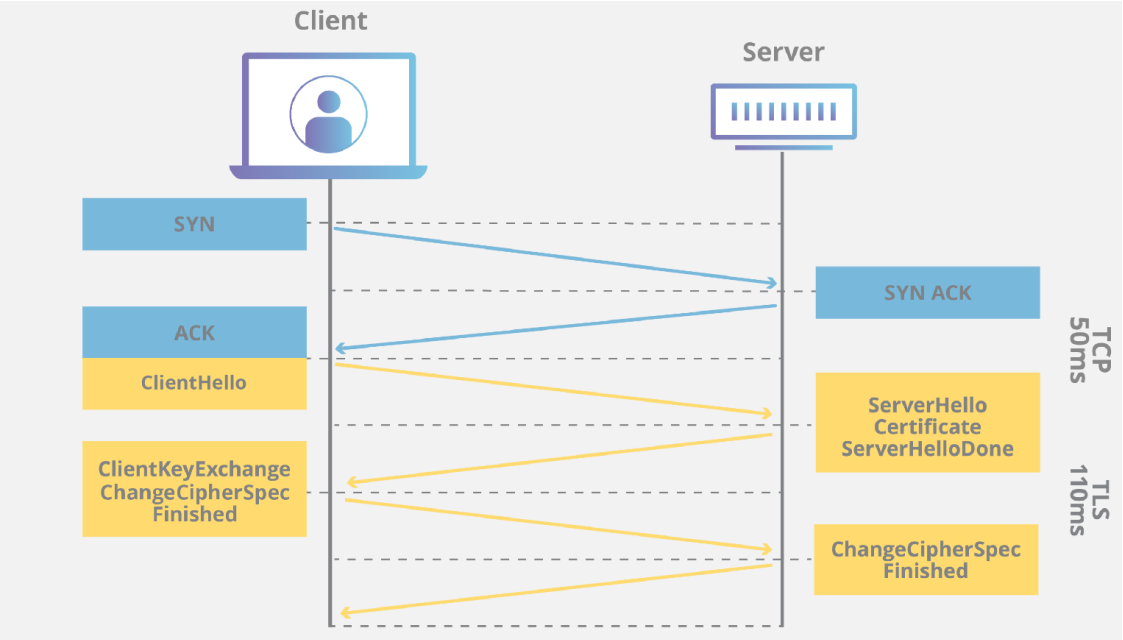
Methods to Secure Communications Networks: SSL & TLS

Transport Secure Layer (TLS) is an encryption protocol designed to secure Internet communications.

- Secure Socket Layer (SSL) was the original implementation.
- TLS makes use of Asymmetric encryption

TLS has a few drawbacks:

- TLS will **add latency** to your site's traffic.
- The handshake is **resource-intensive**. It uses asymmetric encryption to establish a session key, which then allows the client and server to switch to a faster symmetric encryption.
- TLS will add **complexity** to your server management. You will need to get a certificate installed on your web server and maintain the validity of that certificate.

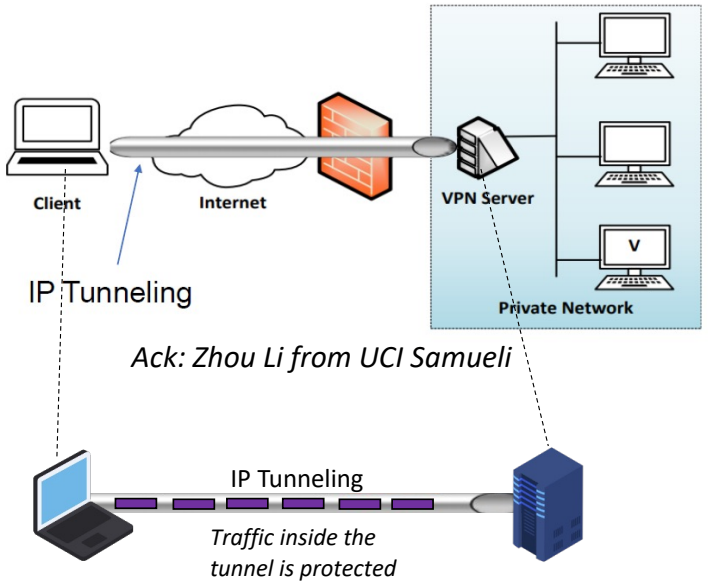


https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/

Methods to Secure Communications Networks: VPN

Virtual Private Network (VPN) allows users to create a secure, private network, using public networks.

- Needs a VPN server on the network.
- External computers go through the VPN server to reach computers inside via **authentication**.
- Internal computers are protected by firewalls, etc., while VPN server is exposed to outside.



2 Types of IP tunneling:

1. **Internet Protocol Security (IPSec):** *encapsulates packet not a new packet with additional packet headers.*
2. **TLS**

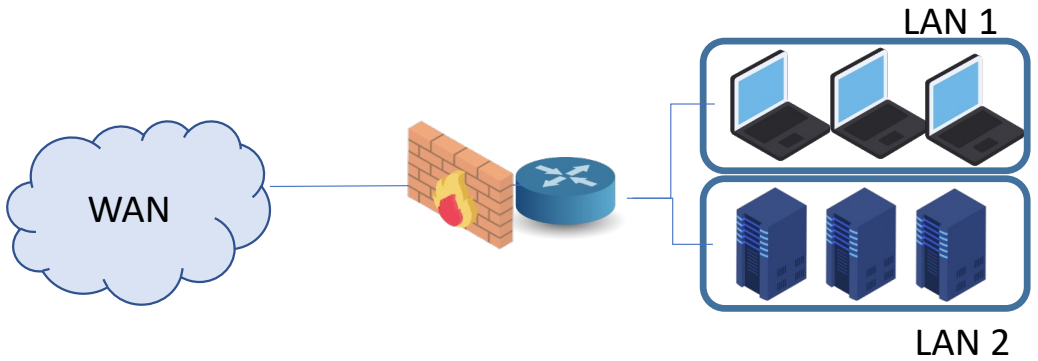
Methods to Secure Communications Networks: Firewalls

Firewall: controls the flow of network traffic between networks or hosts.

- Started as simple packet inspectors but have evolved to very sophisticated devices.
- Standalone or (more commonly) integrated with a router, gateway, or computer (OS)
- Provides a **"first level of defense"** to a network, a.k.a. **electronic security perimeter**

- Create policies that handle **inbound** and **outbound** network traffic.

- Identify requirements for firewall rules.



Methods to Secure Communications Networks: IDS/IPS

Intrusion Detection System (IDS) / Intrusion Prevention System(IPS): Monitors network data traffic with the aim of detecting and reporting unauthorized activity.

- An IPS has the ability to take action on detection
- Can be based on predefined rules or predefined anomalies

Types of Intrusion Detection & Prevention Systems:

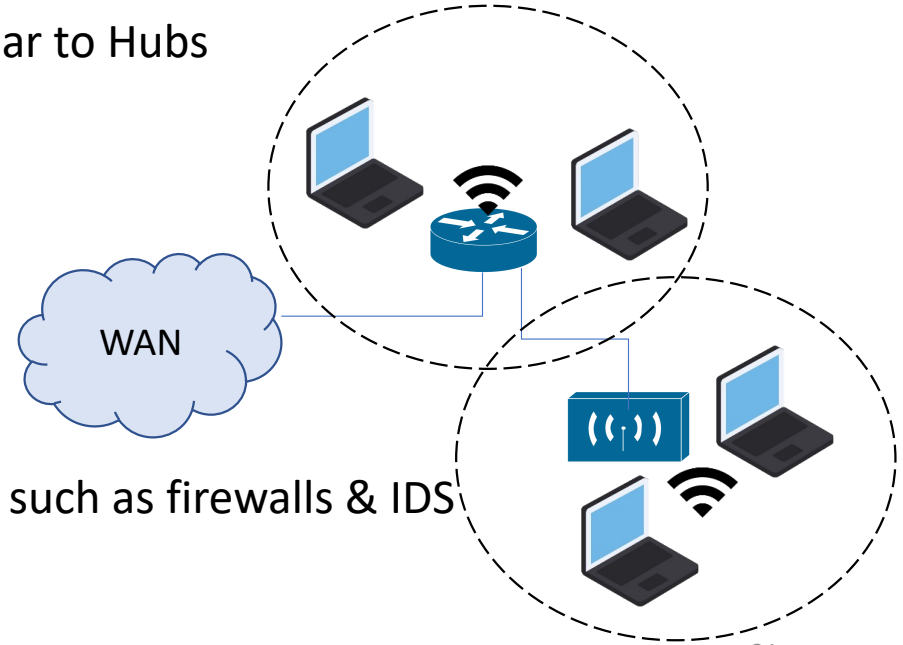
- **Network-based**: Monitor network traffic for suspicious activity.
- **Wireless:** Monitors wireless traffic for suspicious activity.
- **Network Behavior Analysis**: Examines traffic to identify threats that generate unusual traffic , e.g., DoS attacks.
- **Host-Based:** Monitors characteristics of single host and suspicious activity.

Detection Methodologies

- Signature-Based Detection
- Anomaly-Based Detection
- Stateful Protocol Analysis

Methods to Secure Communications Networks: WLANs

- Wireless LANs are extensions to wired LANs based on **IEEE 802.11** standard.
- Wireless networks are, by design, more vulnerable than wired networks.
  - Wireless **Access points** and **Routers** work similar to Hubs
- **<u>Steps to minimize risks:</u>**
  1. Password policies & management
  2. Encrypt data using standards such as WPA2
  3. Restrict access using security controls:
     1. MAC address filtering
     2. Disable not-used network interfaces
  4. Configure host-based network security tools such as firewalls & IDS



How to Detect Anomalies?

Suspicious ‘exception’ event detection?

- Network traffic detected from a foreign IP address within a secure zone.
- Industrial protocol used in nonindustrial zone.
- Unauthorized user performing admin functions.
- Authentication logs indicate non-admin users.

What items are typically monitored for network flows?

- Flow start time and flow end time.
- The number of bytes/packets being transmitted/received.
- Source and destination IP addresses.

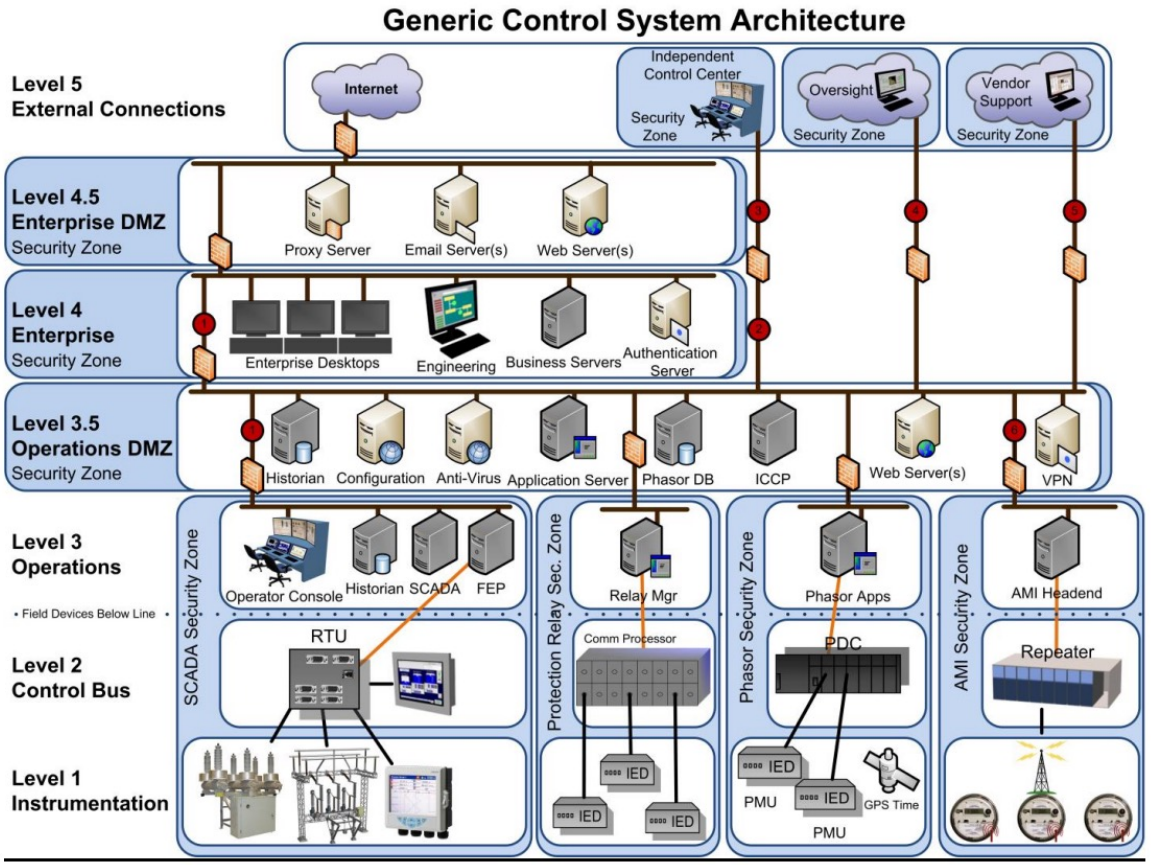
Best Practices for Securing Networks

1. Identifying systems that need to be protected
2. Separation of the systems into functional groups
3. Implementation of a layered defense strategy for each group
4. Access control into and between each group:
    1. identification
    2. authentication
    3. authorization.
5. Monitor the activities that occur within and between groups
6. Limiting the actions that can be executed within and between groups

Apply the the principle of "least route":

- R/ The principle of least route states that in **purpose-built networks** a **node** should only be given the **connectivity necessary to perform its function**. In other words, a node should only possess the minimum level of network access that it requires.

Best Practices for Securing Networks



Mahan, Robert E., et al. Secure data transfer guidance for industrial control and SCADA systems. No. PNNL-20776. Pacific Northwest National Lab.(PNNL), Richland, WA (United States), 2011.

Example Real Cyber-Attack: Ukraine Grid Dec. 2015

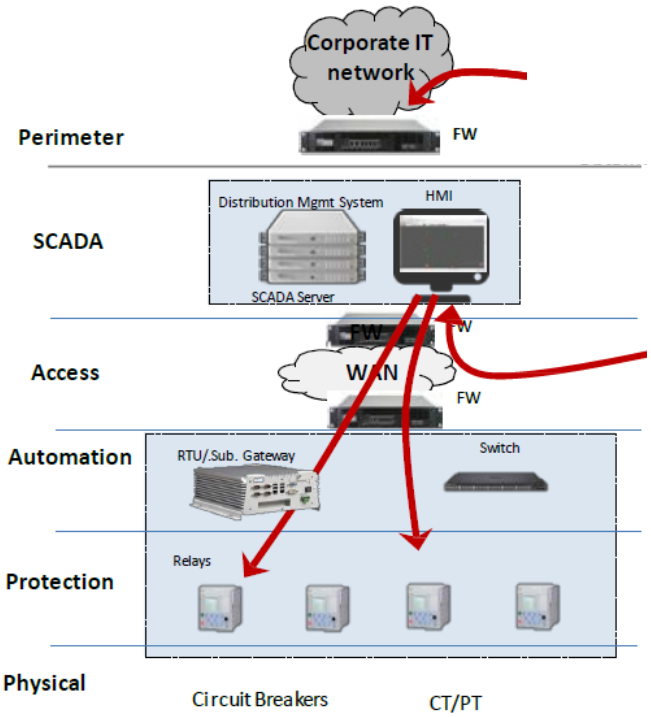
Attack Description & Impacts:

- Coordinated cyber attack to 3 distribution (electric) companies (around 30 substations)

- 225k customers suffered outages
- Blackouts in multiple regions throughout the country

Attack Path:

1. Spear phishing
2. Stolen VPN credentials
3. VPN login
4. Open breakers in the system



Ack: Adam Hahn, Washington State University

IT

1. Phishing email to IT network

2. Privilege escalation

OT Pre-Impact

3. OT VPN login from stolen credentials

4. Install malware (BlackEnergy)

5. Unauthorized remote HMI session access to SCADA

6. Trip the Breakers (Blackout)

OT Post-Impact

7. Disable systems, wipe info., brick controllers

8. Telephone DDOS preventing customers to inform.