SNA Labs (Mids) - Jaish Khan

1. Network Administration

Network administration involves **configuring, managing, and maintaining networks.**
Key Responsibilities

- Configuring network devices
- Monitoring network traffic
- Managing user access
- Troubleshooting network issues
- Implementing security policies

Types of Networks → Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN), Personal Area Network (PAN).

1.1 Networking Models

- OSI Model (7 Layers)
- TCP/IP Model (4 Layers)

Networking Devices

1. **Router** → Directs data between networks.
2. **Switch** → Operates within LAN, directing data between devices.
3. **Firewall** → Protects network by controlling traffic.
4. **Access Point** → Connects wireless devices to a wired network.

Network Protocols → Set of rules that *allow communication between devices on a network.* Protocols define format, timing, sequencing, and error checking for data transmission. SNA Labs (Mids) - Jaish Khan > Networking Protocols

2. Network Monitoring

SNA Labs (Mids) - Jaish Khan > Network Monitoring Tools

Why monitor networks?

- **Performance Monitoring**: Ensures that the network is operating efficiently, detecting bottlenecks or failures.
- **Security**: Identifies suspicious or unauthorized activity on the network.
- **Troubleshooting**: Helps to pinpoint and resolve network issues quickly.
- **Capacity Planning**: Helps in forecasting network needs and preventing overload.

2.1 VLAN (Virtual Local Area Network)

> A technology that allows network administrators to create logically separate networks on the same physical switch.

We can define the "type" of the port of the switch to be either `access port` or `trunk port`.

1. **Access Port** → Used for intra-vlan communication. (with devices on the same VLAN)
2. **Trunk Port** → User for inter-vlan communication. (with devices on other VLANs)

SNA Labs (Mids) - Jaish Khan > VLAN(Extra Information)

2.2 Basic Router/Switch Configuration

Basic Router Configuration: Assign IP addresses, Static/Dynamic Routing Configuration and SSH Configuration for remote access.
Basic Switch Configuration: Configuring VLANs, Disable unused ports for security

---

3. Network Security

> It refers to practices and policies for preventing and monitoring unauthorized access, misuse, modification, or denial of a computer network and its resources.

The 3 Objectives of Security (CIA):

1. **Confidentiality:** Ensuring only authorized users can access data.
2. **Integrity:** Data should not be altered or tampered with.
3. **Availability:** Network services and resources must be available to authorized users.

3.1 Types of Network Threats

Passive Threats	Active Threats
Eavesdropping on network communications without altering the data.	Intentional actions that alter or disrupt data.
Examples: Packet sniffing, traffic analysis.	*Examples:* Man-in-the-Middle attacks, Denial-of-Service and Malware.

3.1.1 Types of Active Threats

1. **MitM** (Man-in-the-Middle) → An attacker secretly intercepts and potentially alters communication between two parties who believe they are directly communicating.
    1. *Eavesdropping* → Intercepting and reading unencrypted data.
    2. *Session Hijacking* → Stealing a user's session token to impersonate them.
    3. *SSL Stripping* → Downgrading an HTTPS connection to HTTP, allowing data to be read in plaintext.
    4. *DNS Spoofing* → Altering DNS responses to redirect users to malicious sites.
2. **DoS** (Denial of Service) & **DDoS** (Distributed Denial of Service) → Attacks that aim to make a network service unavailable by overwhelming it with illegitimate requests.
    6. *Volume-Based Attacks* → Techniques like ICMP floods and UDP floods that overwhelm bandwidth.
    7. *Protocol Attacks* → Exploits weaknesses in the network protocol stack, such as SYN floods and Ping of Death.
    8. *Application Layer Attacks* → Targets specific web applications (e.g., HTTP flood) to exhaust server resources.
3. **Phishing** → Attackers pose as a trustworthy entity to trick individuals into revealing sensitive information. Broad attempts using emails, fake websites, or messages.

    1. *Spear Phishing* → Targeted phishing, often directed at specific individuals or organizations using personal information.
    2. *Whaling* → Spear phishing targeting high-profile individuals (e.g., CEOs, CFOs).
4. **Malware Attacks** → Software designed to disrupt, damage, or gain unauthorized access.
    1. *Viruses* → Malicious code that attaches to files and programs, spreading to others.
    2. *Worms* → Standalone malware that replicates itself to spread across networks.
    3. *Trojan Horses* → Malicious software disguised as legitimate software; may create a backdoor.
    4. *Ransomware* → Encrypts data and demands a ransom for decryption.
    5. *Spyware* → Secretly monitors user activity to steal sensitive information.
    6. *Adware* → Displays or downloads unwanted advertising material.
5. **Brute Force Attacks** → Trying multiple combinations of usernames and passwords until the correct one is found.
    1. *Dictionary Attack* → Uses a list of common passwords or words.
    2. *Credential Stuffing* → Uses leaked credentials from one service to gain access to another.
6. **Spoofing Attack** → An attacker masquerades as a legitimate entity by falsifying data to gain unauthorized access or steal information. Things like IP Spoofing, Email Spoofing, DNS Spoofing or MAC Spoofing.
7. **XSS** (Cross-Site Scripting) → Attackers inject malicious scripts into websites viewed by other users. Things like Stored XSS, Reflected XSS or DOM-Based XSS.
8. **Insider Threats** → Threats that come from within the organization. The insider can malicious, negligent or compromised.
9. **APT** (Advanced Persistent Threats) → Prolonged and targeted cyberattacks in which an intruder remains undetected for an extended period.

3.2 Components of Network Security

- **Authentication** → Verifying the identity of a user or device.
- **Authorization** → Ensuring authenticated entities have permission to access specific resources.
- **Access Control** → Policies that restrict access to the network.
- **Security Protocols** → SSL/TLS, IPsec, HTTPS.
- **Network Policies**

3.3 Firewall

A security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Used to establish a barrier between a trusted internal network and untrusted external networks (like the internet).

Non-Intrusive Firewalls
Intrusive Firewalls

3.3.1 Firewall Configurations

- **Perimeter Firewall** → Placed at the network's boundary to filter external traffic.
- **Internal Firewall** → Deployed within the network to provide internal segmentation and protection.
- **DMZ (Demilitarized Zone)** → A network segment for exposing external services while isolating them from the internal network. Commonly used for public-facing servers (web, email).

3.4 VPN (Virtual Private Network)

A technology that creates a secure, encrypted connection ("tunnel") over a less secure network, such as the internet.It provides secure access to private network resources and maintains confidentiality and integrity of transmitted data.

Remote Access VPN	Site-to-Site VPN
Connects individual users to a remote network. Commonly used for telecommuting or accessing company resources from outside the office.	Connects entire networks to each other (like a branch office to headquarters). Can be Intranet-based or Extranet-based.

3.4.1 VPN Protocols

1. **IPsec** (Internet Protocol Security) → Operates at Layer 3 and provides confidentiality, integrity, and authentication. Protocols Used: AH (Authentication Header), ESP (Encapsulating Security Payload).
2. **SSL/TLS VPN** → Uses the SSL/TLS protocol to secure VPN traffic, operating at Layer 4 (Transport). Ideal for remote access as it can be used via a web browser.
3. **PPTP** (Point-to-Point Tunneling Protocol) → Older protocol, fast but with security limitations. Rarely used due to vulnerabilities.
4. **L2TP** (Layer 2 Tunneling Protocol) with IPsec → Combines L2TP for tunneling and IPsec for encryption. Offers a secure and reliable connection.

VPN Configuration

- *Authentication*: Users are authenticated using credentials (username/password, certificates, or multi-factor authentication).
- *Encryption*: Select strong encryption algorithms (e.g., AES-256).
- *Network Configuration*: Ensure that the VPN gateway is properly configured to route traffic securely through the tunnel.

3.5 Network Intrusion Detection and Prevention

> **IDS** (Intrusion Detection System) → Monitors network traffic for suspicious activity and alerts administrators.

> **IPS** (Intrusion Prevention System) → Similar to IDS but also takes proactive measures to block or prevent detected threats.

Types of IDS/IPS

1. **Network-Based IDS/IPS** → Monitors and protects the entire network by analyzing network traffic. Deployed at strategic points in the network (like behind a firewall).
2. **Host-Based IDS/IPS** → Monitors and protects individual hosts (like servers, workstations). Inspects system files, logs, and running processes.

3.5.1 Detection Methods

- **Signature-Based Detection** → Uses predefined attack patterns (signatures) to detect known threats.
  - *Pros*: Effective against known threats.
  - *Cons*: Unable to detect new (zero-day) attacks.
- **Anomaly-Based Detection** → Establishes a baseline for normal network behavior and detects deviations from this baseline.
  - *Pros*: Can detect unknown threats.
  - *Cons*: May generate false positives if the baseline is not well-defined.
- **Hybrid Detection** → Combines both signature-based and anomaly-based techniques for comprehensive detection.

3.5.2 Configuration and Placement

Place NIDS outside the firewall to monitor all incoming traffic, and consider placing another NIDS inside the network for internal monitoring. Set up alerts and logging to notify administrators in real-time. Regularly update signatures, adjust anomaly detection baselines, and fine-tune alerts to reduce false positives.

4. Network Optimization & Diagnosis

4.1 Network Diagnosis Tools

1. **Ping** → Tests connectivity between two devices. It sends ICMP echo requests and listens for responses.
   Usage: Checking network availability, measuring latency, diagnosing packet loss.
   Example: `ping google.com`
2. **Traceroute** → Traces the path packets take from source to destination. It sends packets with increasing TTL values and records the route.
   Usage: Identifying slow network segments, diagnosing routing issues or loops.
   Example: `traceroute google.com`
3. **Netstat** → Displays network connections, routing tables, interface statistics, and more. Shows current active connections and network statistics.
   Usage: Identifying active TCP/UDP connections, monitoring network traffic, detecting unusual connections or port activity.
   Example: `netstat -an`
4. **Nslookup/dig** → Queries DNS to resolve domain names to IP addresses.
   Usage: Troubleshooting DNS issues, checking if a DNS server is working correctly.
   Example: `nslookup google.com` / `dig google.com`

Third-Party Apps: Wireshark, speedtest.net, Nmap, Crystal eye

4.2 Network Performance Metrics

Network Performance Metric	Description	Measurement	Optimization
Latency	*Time it takes for data to travel from source to destination and back.*	Using Ping or Wireshark to measure round-trip time (RTT).	Reduce network hops. Improve hardware (routers, switches).
Bandwidth	*Maximum data transfer rate of a network connection.*	Tools like speedtest.net or network monitoring software.	Prioritize traffic using QoS. Upgrade internet service or networking equipment.
Throughput	*Actual amount of data transferred*	Using network monitoring tools like	Avoid congestion by load balancing.

Network Performance Metric	Description	Measurement	Optimization
	successfully over the network.	Wireshark or SolarWinds.	Upgrade network hardware.
Packet Loss	*Percentage of data packets lost during transmission.*	Ping or network monitoring tools.	Improve connection reliability. Use redundancy.

4.3 Common Network Issues

1. Connectivity Issue	2. Slow Network Speed	3. High Latency	4. IP Address Conflict
Symptoms: No network access, unable to connect to the internet.	*Symptoms*: Slow downloads/uploads, buffering during streaming.	*Symptoms*: Delays in response times during communications.	*Symptoms*: Devices unable to connect to the network, "IP address conflict" error.
Causes: Faulty cables, misconfigured devices, DNS issues, or firewall blocking traffic.	*Causes*: Bandwidth bottlenecks, congestion, high latency, or packet loss.	*Causes*: Long routes, overloaded devices, or inefficient routing.	*Causes*: Two devices on the network using the same IP.
Solutions 1. Check cables and ports. 2. Restart modems and routers. 3. Verify IP and DNS settings.	*Solutions* 1. Optimize bandwidth usage. 2. Identify high traffic devices or applications. 3. Upgrade equipment.	*Solutions* 1. `traceroute` to identify latency sources. 2. Reroute traffic through better paths. 3. Reduce the no of network hops.	*Solutions* 1. Ensure DHCP is configured correctly. 2. Assign static IP addresses to critical devices. 3. Expand the DHCP IP range.

4.4 Optimizing Network Performance

- **Load Balancing** → Distribute traffic evenly across multiple servers or paths.
  - Tools: Load balancers (e.g., HAProxy, NGINX) to ensure high availability and avoid bottlenecks.
- **QoS** → Prioritize critical traffic over less important data.

    - Implementation: Set QoS rules on routers to allocate more bandwidth to high-priority applications.
- **Network Segmentation** → Reduce network congestion by segmenting traffic (e.g., VLANs).
    - Benefits: Limits broadcast domains, improving performance and security.
- **Monitoring and Proactive Measures** → Continuously monitor network performance.
    - Tools: SNMP-based network monitoring (e.g., SolarWinds, Zabbix).
- **Regular Firmware and Software Updates** → Ensure all network devices have the latest updates for performance improvements and security fixes.

Less Important

1. Networking Protocols

Protocol	Description	Features	Notes
TCP (Transmission Control Protocol)	**Connection-oriented protocol** ensuring reliable, ordered, and error-checked delivery of data.	Connection establishment (3-way handshake), sequencing, error detection and correction.	*Uses* Web browsing (HTTP/HTTPS), email (SMTP), file transfers (FTP).
UDP (User Datagram Protocol)	**Connectionless protocol** used when fast transmission is more important than error correction.	No handshake or connection establishment, faster but less reliable.	*Uses* Video streaming, online gaming, VoIP.
IP (Internet Protocol)	Delivers packets from source to destination based on IP addresses.	Defines IP addressing and routing, fragmentation, reassembly of packets.	*Versions* IPv4 (32-bit) IPv6 (128-bit)
ARP (Address Resolution Protocol)	Resolves IP addresses to MAC addresses in a local network.	ARP requests are broadcast to discover MAC addresses.	
ICMP (Internet Control Message Protocol)	Used by network devices to send error messages and operational information.		*Uses* Ping, Traceroute, error reporting.
DHCP (Dynamic Host Configuration Protocol)	Automatically assigns IP addresses and other network configuration parameters.	Simplifies IP address management, reduces manual configuration errors.	
DNS (Domain Name System)	Translates human-readable domain names into IP addresses.	User enters domain name; DNS resolver queries servers.	*Command* nslookup

1.1 IP Addressing

- **IPv4 Addressing** → *32-bit addresses* divided into four octets (192.168.1.1).
  - Address Classes: A, B, C, D, E for different network sizes.
- **IPv6 Addressing** → *128-bit addresses* (2001:0db8:85a3:0000:0000:8a2e:0370:7334).
  - Advantages over IPv4: increased address space, simplified header structure.

Subnetting	Supernetting
Dividing a network into smaller subnets for improved management and efficiency. Subnet Mask defines the network and host portions of an IP address.	Aggregating multiple networks into a larger network to reduce routing table size.

NAT (Network Address Translation) → Modifies network address information in IP headers during transit. Allows multiple devices to share a single public IP address.

- *Types* → Static NAT, Dynamic NAT, PAT.

2. Network Monitoring Tools

Tool	Description	Features	Usage
Wireshark	A widely used, open-source packet analyzer that captures network traffic in real-time, enabling deep visibility into data packets being transmitted.	Captures and inspects packets at a granular level then provides details such as IP addresses, port numbers, and protocols and supports filtering.	Troubleshooting, Security, Network Analysis.
SolarWinds NPM	SolarWinds Network Performance Monitor is a comprehensive tool for monitoring network performance across distributed environments.	Monitors network traffic, device status, and performance metrics. Supports real-time alerts and graphs. Automatically discovers and maps network devices.	Centralized Monitoring, Alerting, Network Mapping.
Nagios	An open-source network monitoring tool used for	Monitors host and service status. Sends alerts via email, SMS,	Server and Device Monitoring, Custom Alerting.

Tool	Description	Features	Usage
	monitoring the health of networks, servers, and applications.	or other methods when network problems occur.	
PRTG Network Monitor	An all-in-one network monitoring tool that can track bandwidth usage, traffic, and the availability of various network services.	Monitors LAN, WAN, VPN, and Cloud services. Provides sensor-based monitoring of devices, applications, and traffic.	Bandwidth Monitoring, Network Uptime Monitoring, Network Traffic Analysis.

2.1 Monitoring and Management Protocols

Protocol	Description	Usage
Simple Network Management Protocol	SNMP is used for monitoring network devices' performance and faults.	Performance Monitoring, Fault Detection, Capacity Planning.
NetFlow	Developed by Cisco to collect IP traffic information for monitoring purposes.	Analyze network traffic, understand which devices are generating the most traffic, and detect anomalies.
Syslog	Used to send system log messages to a central server for monitoring and analysis.	Centralized log collection for troubleshooting and security auditing.

3. Network Routing

The process of choosing a path across one or more networks. Directing a data packet from one node to another.

There are limits to how many hop counts a packet can do; if it is exceeded, the packet is considered to be lost.

It works by finding the shortest path from the source node to the destination node across a network. Steps involved in Routing:

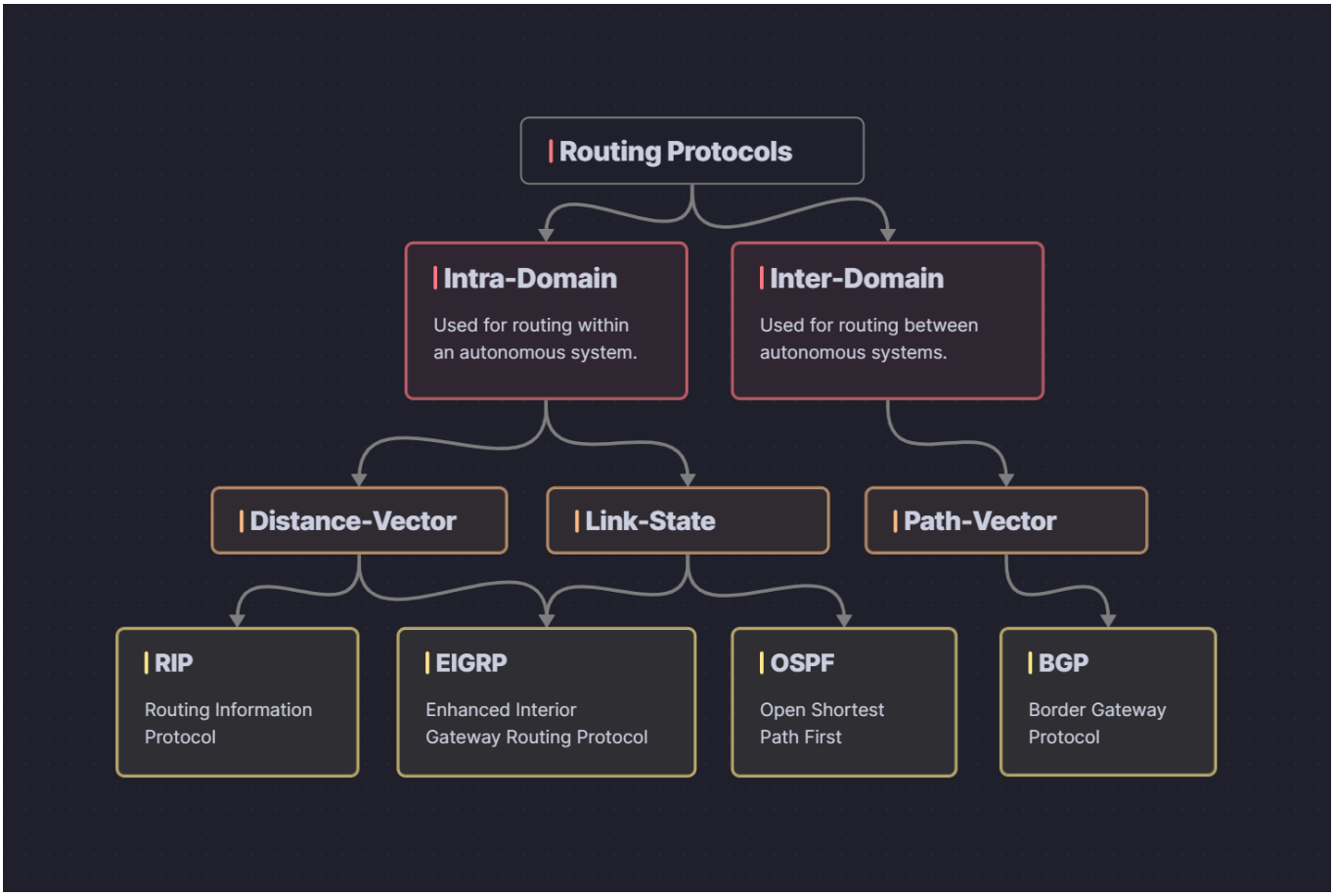
1. *Communication initiation* → One node initiates communication across a network.

2. *Data Packets* → The source device breaks information into small data packets, each labeled with the destination node's IP address.
3. *Routing Table* → The source node uses the routing table to select the shortest path and routes the data packet accordingly.
4. *Hopping procedure* → The data packet undergoes many hops across various nodes until it reaches the destination node.
5. *Reaching the destination node* → The data packets re-assemble at the destination node, transforming into the complete information.

3.1 Types of Routing

Static Routing	Dynamic Routing
Also called "non-adaptive routing". Routing configuration is done manually by the network administrator.	Works automatically without any human intervention. Packets are sent using various shortest-path algorithms and metrics.
Advantages 1. Minimal CPU and memory resource usage. 2. Easy implementation in small networks. 3. Predictability because the next-hop is always the same.	*Advantages* 1. Best for larger networks as it can handle many routes. 2. Can reroute traffic around failed links which improves reliability and uptime. 3. Calculates optimal routes based on metrics such as link speed.
Disadvantages 1. Configuration complexity in large networks. 2. Needs manual intervention is required to reroute traffic. 3. Prone to configuration errors.	*Disadvantages* 1. Requires more CPU, memory, and bandwidth. 2. Setting up dynamic routing protocols can be complex. 3. Routes can change due to fluctuations in network conditions, which may lead to unpredictable routing paths if not configured with clear policies.

3.2 Routing Protocols



Distance-Vector	Link-State
Each router maintains a table of distances to other routers in the network.	Each router has a complete map of the network topology.
Based on distance (hop count)	Based on entire network map
Information Sharing → only with neighbors	**Information Sharing** → With all routers in the network
Updates → Periodic and full routing table	**Updates** → Triggered updates with topology change
Simple Implementation and Low Resource Usage	Complex Implementation and High Resource Usage
Less Accurate and Slower to converge.	Efficient Path Selection and Faster to converge

- A maximum of 15 hops (16 is unreachable).

4. VLAN(Extra Information)

> **Why use VLANs?**
>
> Network Segmentation, Improved Security, Simplified Management, Broadcast Domain Control, Flexibility

4.1 802.1Q Encapsulation

A network standard used for **VLAN tagging** on Ethernet frames.

4.1.1 VLAN Tagging

Process of adding a tag to Ethernet frames to identify which VLAN they belong to. When a frame is tagged, switches and routers that support VLANs can forward it based on its VLAN ID.

- **Tagged frames**: These carry a VLAN ID, enabling them to traverse network segments designated for specific VLANs.
- **Untagged frames**: Frames without VLAN tags are usually treated as part of the *native VLAN* (default, untagged VLAN).

It allows network administrators to enforce segmentation, access control, and traffic isolation without separate physical networks.

Components:

- **TPID** (Tag Protocol Identifier) → A *2-byte* field with a fixed value which tells if the tagging is set or not.
- **TCI** (Tag Control Information) → A *2-byte* field with 3 subfields:
  - **PCP** (Priority Code Point) → A *3-bit* field for specifying the **frame's priority level** (0-7). PCP is used in **Quality of Service (QoS)** to prioritize network traffic, with higher numbers indicating higher priority.
  - **DEI** (Drop Eligible Indicator) → A *1-bit* field which tells if the frame can be dropped under network congestion.
  - **VID** (VLAN Identifier) → A *12-bit* field that specifies the **VLAN ID** (0-4095), identifying the VLAN the frame belongs to.

4.1.2 Native VLAN

The "default" VLAN that carries untagged traffic on a trunk link. By default, VLAN "default" is set as the native VLAN.

4.1.3 ROAS (Router-on-a-Stick)

A technique for enabling **inter-VLAN routing** using a single physical router interface.

4.2 VLAN Creation in Packet Tracer

1. `interface` command → used to specify ports.
2. `switchport mode` command → tells which mode the port is going to be (can be `access` or `trunk`).
3. `switchport access vlan` command → allows us to create a new VLAN by specifying the id (`10`, `20`, `30`).
4. `show vlan brief` command → shows VLAN configuration information.
5. `vlan <id>` into `name <name>` → to change the name of the VLAN.

```
interface range g1/0-3
switchport mode access
switchport access vlan 10

interface range g2/0-2
switchport mode access
switchport access vlan 20

interface range g3/0-3
switchport mode access
switchport access vlan 30

do show vlan brief

vlan 10
name ENGINEERING

vlan 20
name HR

vlan 30
name SALES
```

Other Random Things

1. We only require a single primary and a single backup connection (having more than that is a waste of resources).
2. If all connections break then it is called a *Network Outage*.
3. **Broadcast Domain** → The scope within which broadcast frames are forwarded. A single VLAN or LAN (Router) is 1 broadcast domain.
4. **Collision Domain** → The network segment where data collisions can occur. A 32-port switch has 32 collision domains.