# LAN

LAN stands for Local Area Network:

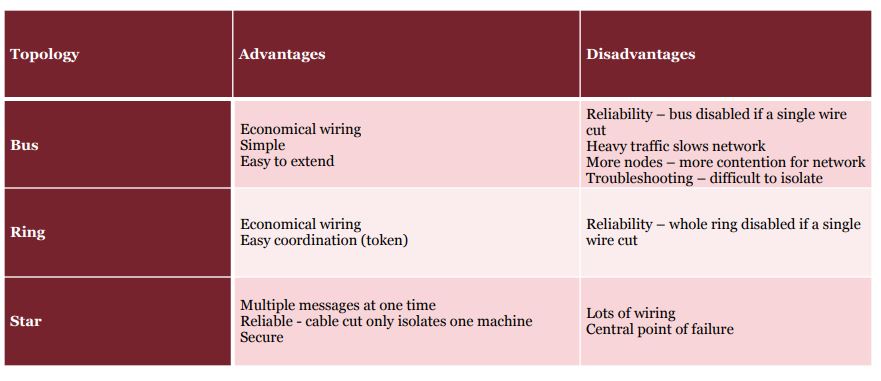
* Typically covers a geographically small area
* Owned and managed by one organization
* Simple physical and logical topologies
* Predictable, fast, and reliable

**Why use LAN?**

* Information sharing locally between devices of an organization in close physical proximity
* Improves productivity
* Service sharing among all devices
* Reduces costs

**LAN Topologies**

*Logical Topologies* → How the data flows in a network  
*Physical Topologies* → How devices of a network are physically connected to one another

1. **Bus** Topology
   1. Only one transmitter at a time
   2. Messages go to all other nodes in the network
   3. If cables/lines are cut, it affects all other devices on the network
2. **Ring** Topology
   1. Messages travel around a ring, unidirectionally
   2. Minimises packet collisions (in a half-duplex network)
   3. Very little redundancy, if one station disconnects, then entire ring disconnects, and the network stops
3. **Star** Topology
   1. Multiple messages can be sent at the same time
   2. Messages only seen by the destination
   3. Localized point of failure at central node (single point of failure)
   4. Most common LAN topology
   5. Very cost effective and efficient
   6. Given that physical LAN connections with cables is full-duplex (can transmit and receive data at the same time), has the best efficiency as all nodes can talk at once
4. **Full Mesh** Topology
   1. All nodes are connected to all other nodes of a network
   2. This is the topology of the internet
   3. Has very high redundancy, if one node goes down, the network will still work
   4. Very complicated as the number of nodes increases
   5. Very expensive
   6. Difficult to manage

**Connecting a LAN**

* Fiber cabling (very fast, great bandwidth, great distance, expensive)
* Twisted pair cabling (not quite as fast, cannot travel as far in distance, much cheaper)
* Can use WLAN (802.11x access point) to wireless connect to a LAN

**Media access strategies**

* Point-to-point
  + Exclusive access to the network
  + Can transmit at any time
  + No need for access control
  + No need to addresses (only 1 possible destination)
* Multipoint Network
  + Shared access of network
  + Can only transmit when clear
  + Access control required
  + Need for addresses to identify recipient

# Subnetting

**Advantages of subnetting:**

* It is inefficient to assign every device to the same network
* Subnetting is used to subdivide a network into logical pieces
* Subdivision of a network can be used to align the network to the logical business functions
* Subdividing a network with subnetting allows the creation of a clear networking hierarchy

**Standard terminologies**

* Class A (8 bit netmask → 24 host bits)
* Class B (16 bit netmask → 16 host bits)
* Class C (24 bit netmask → 8 host bits)

**Subnetting Question with a table format**

1. **Network address / netmask provided by ISP → (137.111.0.0/22)**
2. **Identify the network address range (137.111.0.0 → 137.111.3.255)**
3. **Identify the broadcast address (137.111.3.255)**
4. **Raw netmask → (255.255.11111100.0) [yellow is decimal, green is binary]**
5. **Identify the total number of host bits (32 - 22 = 10 host bits)**
6. **Identify the total number of hosts using these host bits (2^10 = 1024)**
7. **Using the case study / question provided, ask yourself the 2 below questions**
   1. How many subnets are required? Why?
   2. How many hosts are required for each subnet? Why?
   3. Use this information to determine the number of subnets
8. **The total number of subnets created will be a 2^(number of used host bits) [E.g., 2^2 = 4)**
9. **From this number, subnet 0 and the highest subnet are not usable**

**Example**

**Provided network: 190.11.40.0/23**

**Network range: 190.11.40.0 → 190.11.41.255**

**Broadcast address: 190.11.41.255**

**Netmask: 255.255.11111110.0 [decimal in yellow, binary in green]**

**Host bits: 9**

**Max no. hosts: 512 (510 not including 0s and 1s)**

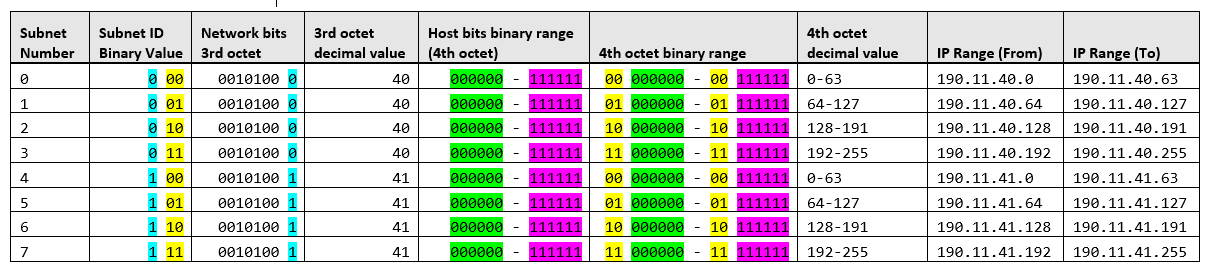
**How many subnets? (THIS IS MOST LIKELY WHAT THE QUESTION WILL BE ABOUT)**

**We want to create as many subnets as possible that can support a minimum of 50 hosts each. Therefore, we want to use 6 hosts bits to allow for 64 hosts per subnet (62 usable). This means we have 3 bits remaining in our netmask, allowing us to create 8 subnets (6 usable).**

**Netmask (after subnetting): 255.255.255.11000000**

**Host bits (after subnetting): 6**

**Max no. hosts (after subnetting): 64 (62 not including 0s and 1s)**



(**Use font consolas**)

# Application Layer

**Application architectures**:

1. Host-based architecture (thin-client)
2. Client-based architecture (thick-client)
3. Client-server architecture (distributed-client)

**Multi-tier architecture**

The involving of more than 1 computer in the distribution of application logic

1. 2-tier architecture (2 computers [server + client])
2. 3-tier architecture (3 computers [most often database + server + client])
3. N-tier architecture (Many computers managing different aspects of application logic)

**Easy way to understand it**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Data Logic** | **Application Logic** | **Presentation** | **Example** |
| **Host-based** | Server | Server | Client | Salesforce.com |
| **Client-based** | Server | Client | Client | Printing |
| **Client-server** | Server | Server + Client | Client | Outlook |

**Multi-tier architecture continued**:

**Advantages**:

* Better load balancing of processing logic
* Able to distribute workload (which is load balancing)
* More scalable

**Disadvantages**:

* Heavier on the network
* More data exchanges
* Difficult to program and test
* Increases complexity

**Choosing an architecture** (major factors):

1. Infrastructure costs
2. Development costs
3. Scalability
4. Is there an existing system (factor in migration)

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Host-based** | **Client-based** | **Client-server** |
| **Infrastructure cost** | High | Medium | Low |
| **Development cost** | Low | Medium | Medium |
| **Scalability** | Low | Medium | High |

# Security

Security mitigates risk from threats and attacks that exploit vulnerabilities in systems.

**Key Definitions**:

* Vulnerability: A weakness or potential point of exploitation.
* Threat: The possibility of harmful events occurring, i.e. Attacks, Human Error, Disasters, Data Loss.
* Attack: Intentional activity undertaken with the intention to cause harm or damage to a system.

Vulnerabilities can be classed as Software, Hardware or procedural vulnerabilities.

**Software vulnerabilities include**:

* Bugs/Errors in Software
* Insecure encryption or connections
* Misconfiguration of systems.

**Hardware vulnerabilities include**:

* Lack of physical security, i.e. Leaving sensitive paperwork outside a locked and secure cabinet.
* Failing to monitor devices with access to sensitive information. Can be used to intrude without exploiting a software vulnerability.
* Stolen devices.

**Procedural vulnerabilities include**:

* Lack of password or very weak password.
* Insufficient user authentication.

**Threats to a network include**:

* Disruptions to service
* Destruction of Data
* Disasters
* Unauthorised access

Threats are realised through the exploitation of vulnerabilities.

**Exploits include**:

* Attacks (Hacking into a system, can be active or passive)
* Malware (Viruses, trojans, spyware, etc)
* Web exploits (Cross-site scripting, injection attacks, etc)
* Social Engineering (Phishing, Pharming, etc)
* Denial of service, distributed denial of service.

**Attack Types**:

* Active attacks aim to damage, alter or impede the operation of a system.
* Passive attacks attempt to steal information but do not impede the operation of a system.

Attacks can be conducted from “inside”, that is someone who is authorised to access the system abuses their access to attack the system. Otherwise, attacks are considered to be from the outside, in which an external entity attempts to breach the network and gain unauthorised access for their own motives.

**Assets**:

* Assets should be protected to reduce the likelihood of a successful attack, or the resultant damage of an attack that does succeed.
* Structured Assets include bank information, business accounting information (inventory, etc.), Customer information, HR and Payroll information.
* Unstructured information includes Intellectual property, marketing plans/strategies, Acquisition or merger planes.
* Other assets could include email or similar information.

**Risk Control Measures**:

Administrative controls:

* Legal policies
* Background checks/screening
* Job rotation
* Segregation of duties
* Principle of least privilege

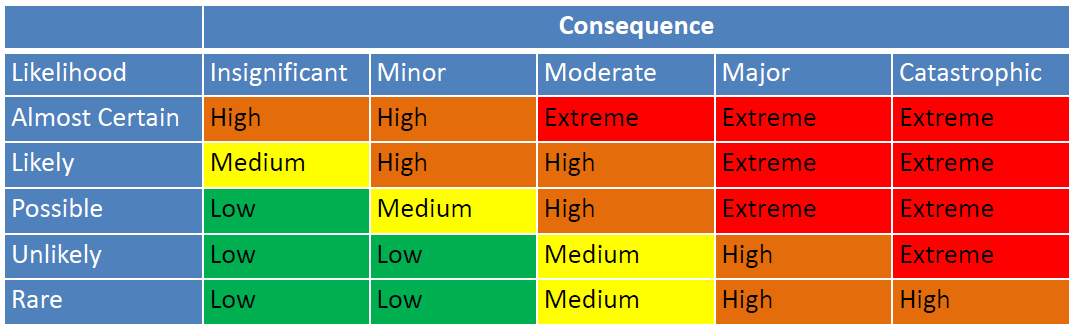
Technical Controls:

* Identity management
* Access control systems
* Cryptographic controls
* Network Controls (Firewalls, NAC/NAP, etc.)
* Intrusion detection/prevention systems
* Logging, security/event incident and management

Physical controls

* Perimeter protection (lighting, fences, gates)
* Locks, Badge Access

**Risk Matrix**:



**Risk assessment steps**:

1. Prioritise assets that are most important/likely vulnerable.
2. Determine what the threats to these assets are as well the possible consequences of an attack.
3. Assign controls to mitigate the risk and consequences of an attack.

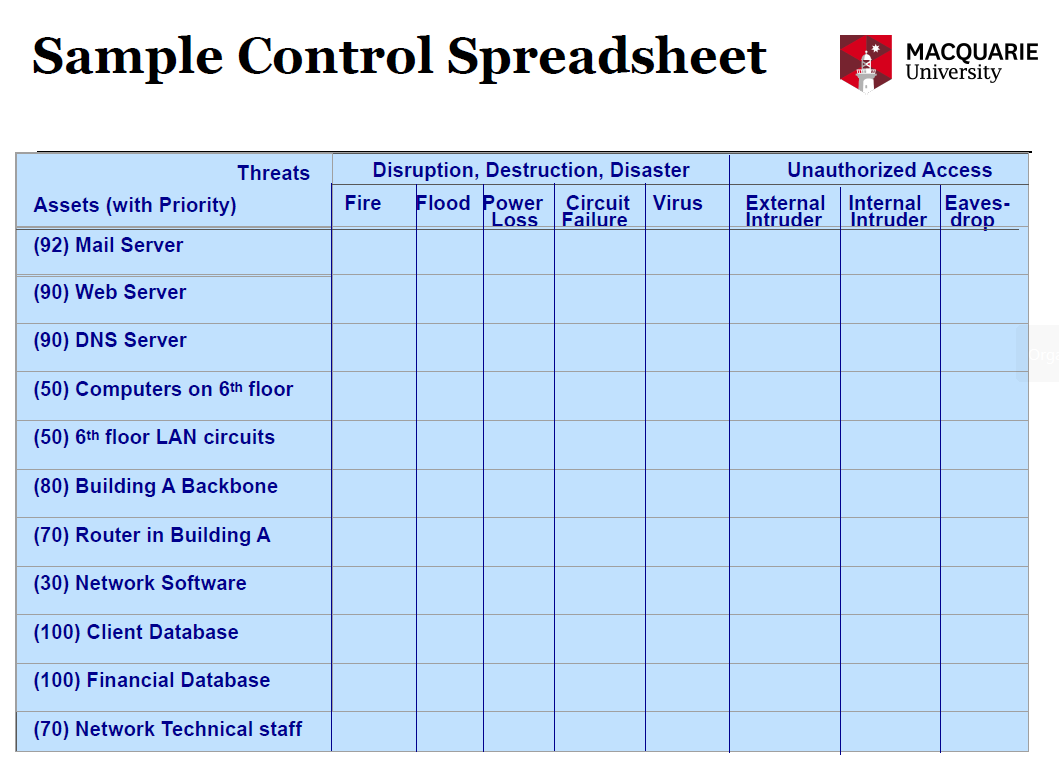
**Risk Assessment Framework**:

Just use - **Operationally Critical Threat, Asset, and Vulnerability Evaluation** (**OCTAVE**) from the Computer Emergency Readiness Team:

1. **Develop risk measurement criteria - Following are most common impact areas:**
   1. Financial (revenue and expenses)
   2. Productivity (business operations)
   3. Reputation (customer perceptions)
   4. Safety (health of customers and employees)
   5. Legal (potential for fines and litigation)
2. **Inventory IT assets - Identify the following:**
   1. Mission critical applications (if they go down, business cannot operate)
   2. Organization’s data (loss, corruption, or destruction of critical data)
   3. NOW RATE THEM BY IMPORTANCE
      1. Confidentiality
      2. Integrity
      3. Accessibility
3. **Identify threats**
4. **Document existing controls**
   1. Risk control strategy
   2. Accept a risk
   3. Mitigate a risk
   4. Share a risk (insurance)
   5. Defer a risk (need to collect additional information)
5. **Identify improvements**

Spreadsheets can aid the identification of risk for network components.

E.g. Make a table that lists network assets on the Left Hand side, and lists the threats across the top of the table. In the corresponding cells, list the controls currently existing to control the risk of that threat.



Assess whether the current controls are adequate or whether security should be improved as the system would be vulnerable to attack.

**List of controls to be considered for implementation**:

* Disaster Recovery Plan
* Fire extinguishing systems (Normal for most rooms, Halon for server rooms)
* Not on or below ground level.
* Uninterruptible Power Supply for all major network servers.
* Contract guarantees from interexchange carriers.
* Extra backbone fibre cable laid in different conduits.
* Virus screening software for networks and hosts.
* User training on cyber security, and updates for the most common threats.
* Strong authentication/Password Software.
* Application Layer firewall.

Additional considerations should include users working from home. Employees' home network may not be secure and could act as a point of vulnerability if a user’s home network and devices are breached. E.g. Spyware could record passwords and thus enable unauthorised access to company assets. This could be controlled with encryption.

**Cryptography**:

Used to verify data is not publicly available, it is not corrupt or altered, it can be verified and makes the creator of the data responsible for it.

This **provides confidentiality, integrity, authenticity** and non-repudiation.

**Encryption**:

* Makes intercepted data unreadable
* Usually requires two different keys for encryption and decryption. These keys use algorithms to convert the data back to a readable format.
* Public key for encryption, private key for decryption. Allows messages to be sent but only the recipient to decrypt it.
* Also authenticates the user as only an encryption key holder can encrypt the data in the first place. This additionally makes the sender accountable for the data sent.
* Can use session only keys.

**Encryption works by**:

* Encryption Algorithm used to convert Plaintext into Cipher Text.
* Cipher Text is sent to the recipient.
* Recipient poses a key to decrypt the message and convert back into Plaintext.

The main weakness of encryption is interception of the encryption key during distribution. Longer keys are stronger to break.

**Encryption can be broken by**:

* Brute force (trying all combinations)
* Cryptanalysis (Identifies weakness in the algorithm to use less combinations when trying to brute force.

**Integrity checksums**:

* Sender sends checksum, receiver verifies it.
* Can be done with Parity or CRC.
* If checksums agree, it can be said that the message was not damaged or modified in transit.

**Authentication**:

* Method of proving identity.
* Authentication is the basis for authorisation, cannot authorise someone until you know who they are.
* Identity can be proven via password, access card or biometric information or a one time token (used in two-factor authentication commonly).
* Limits access of users within a network to the absolute minimum required to perform their duties.
* Blocks users if they are not authorised or authenticated.

It is important to delete old accounts (former employees) or add an expiration period. Network authentication should also occur on a per session basis. That is every time the employee arrives at the site.

**Two-Factor authentication**:

* ID and password
* Issued temporary token.

**Intruders and types of intruders**:

* Casual (Limited knowledge, pre built hacking tools or techniques usually)
* Hackers (Security experts, cause damage)
* Professional Hackers (Conduct espionage and fraud)
* Employees (Exceeding legitimate access and abusing privilege)

**Preventing intrusion**:

* Use of air gapped computers for extremely sensitive information. (Air gapped means completely offline and isolated from the network. No connections means no chance of external hack)
* Implement controls scaling with the potential risk of the asset.
* Employee training and rules.
* Conduct tests/audits of security.

**Access Control Models**:

Models that decide when subjects (entities performing actions) can control or access objects (resources).

**Discretionary Access Control (DAC)**:

* File and Data ownership (Who created the object).
* Access rights and permissions (Which subjects can access the object).

Determined by policy as to who can access what.

**Mandatory Access Control (MAC)**:

* Sensitivity level assigned to subjects and objects.
* Access granted if subject sensitivity is greater than or equal to object sensitivity.

Additionally, rules are put into place so that only necessary files can be accessed using this method.

**Role Based Access Control (RBAC)**:

* Access is granted based on the subject's role.
* Every subject has a role.
* Each object can only be accessed by certain roles.

**Network Controls**:

* Access points of a network are the modem, Internet and the Internal LAN.
* Access points controlled by Firewalls, NAT proxies and Intrusion Detection Systems (IDS).
* The Internet is the most frequent attack point.

**Firewalls**:

* Control traffic (Inspect to see if traffic complies with ruleset, block disallowed connections).
* Usually a packet filter or application level firewall is used.
* Prevents DOS attacks
* Used on all Internet connections
* Packet Filters inspect source and destination IP, port numbers and some check data content to verify the packet data does not contain viruses or spam, or track connections.
* Application Level firewalls require user login, restricts applications and separates private networks from the internet. It requires more processing power than a packet firewall. Acts as a middle man between internet and internal servers which requires authentication.

**IP spoofing (THIS IS A THREAT)**:

* Changes a packet source address to one from inside the network i.e. an allowed traffic IP.
* Some firewalls can recognise this and block incoming traffic with an IP from on the network.

**Network Address translation (NAT)**:

* Assigns public address to a group of computers on the internal network.
* Limits the number of public IP addresses the company must use.
* Can be temporary IP (per computer) or Ported using a shared public IP. (Basic vs Port translation)
* Intruders cannot access except through NATs

Important to secure the inside of a network too. It's often ignored.

**Intrusion Detection Systems**:

* Monitor network and server traffic for suspicious behaviour and report.
* Types are Network based, server based and application based.

**IDS Techniques**:

* Signatures of known attacks (to help recognise). Alerts upon a match. Have to keep the database current.
* Monitors for abnormal activity patterns.
* Sometimes triggers false alarms.

**Denial of Service**:

* Attacks which prevent legitimate users from obtaining the service.
* Flood network with packets to cause congestion
* Flood of TCP SYN Handshake requests prevent servers from establishing connections.
* DDOS is similar but harder to prevent as requests do not all come from one source.
* Can be prevented by filtering for Valid IPs (expensive), Slowing traffic or using IDS/IPS.

**Malware**:

* Virus (Attaches to exe files, spreads when the files run).
* Macro virus (Like a virus but can run out of a data file not an executable).
* Worm (Attacks other computers through the network. Can spread without human interaction).
* Trojan (Malicious code hidden in a useful program or file).
* Spyware (Collects personal information)
* Scareware (False virus warnings, asks user to purchase non functional anti virus)
* Adware (Displays unwanted advertisements).

**Preventing Malware**:

* Scans disk, files, email
* Email is the most common source of malware.

**Where to secure?**:

* Layer 2 and Layer 3 should use link encryption (encrypted and decrypted at each hop).
* Layers 4 and above should feature end to end encryption (encrypted by sender, decrypted by intended recipient).
* Both can be used in a network protocol stack.

**Traffic Analysis**:

* Lower level tends to be more vulnerable.
* Quantity, Direction, Frequency, Message Sizes, Sender, Receiver, port and protocol information are not encrypted.

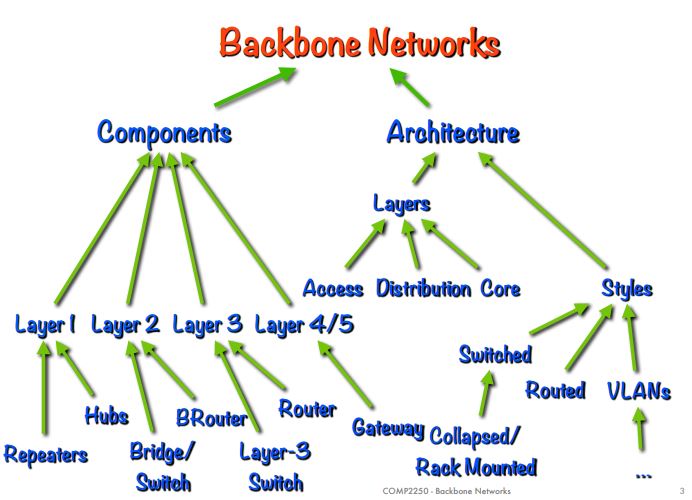
**Secure Sockets Layer (SSL)**:

* Between transport and application layer.
* Negotiate key usings PKI (Public key and the encryption for this session are sent, a session key is generated and sent to the server. Both parties can use this key to communicate.

**IP Security protocol (IPSec)**:

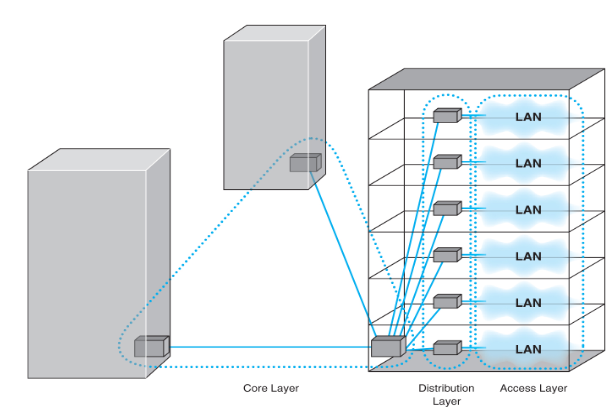
* A and B communicate and send a key each, this key is combined into one key, forming the session key.
* An encryption method is negotiated between the clients.
* Encrypted packages can be sent.
* Modes can be Transport mode (encrypt IP payload), Tunnel mode (encrypt IP packet, encapsulate in new packet).

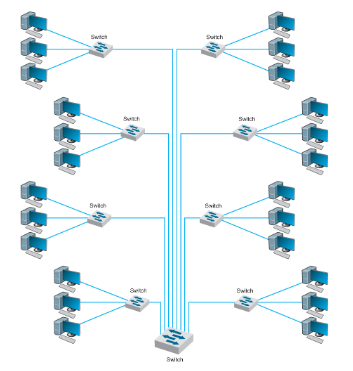
# Backbone Networks

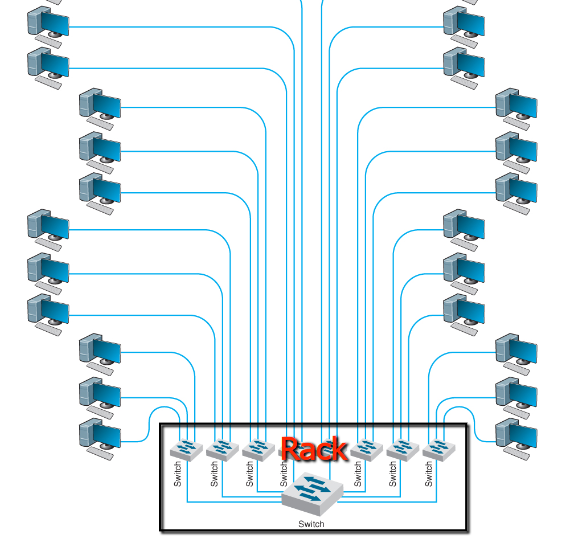
Backbone networks are used to connect multiple LANs together.

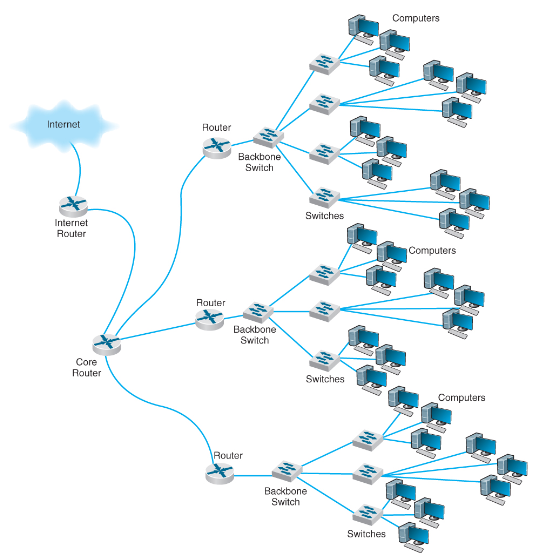
**Architecture**

**Layers**

1. Access Layer
   1. This is just the LAN that a client will connect to with their device
   2. For example, this could be the ethernet cable plugged into your computer, or your phone connected to an access point
   3. This IS NOT part of a backbone network
   4. A backbone network is used to connect multiple access layer LANs
2. Distribution Layer
   1. This IS part of a backbone network
   2. Connects multiple access layer lans together
   3. Most commonly used to connect all of the LANs of a single building
3. Core Layer
   1. This IS part of a backbone network
   2. Connects multiple distribution layer backbone networks together
   3. As distribution layer backbone networks are used to connect LANs within a single building, core layer backbone networks are used to connect multiple buildings together
   4. Most common for large enterprise networks

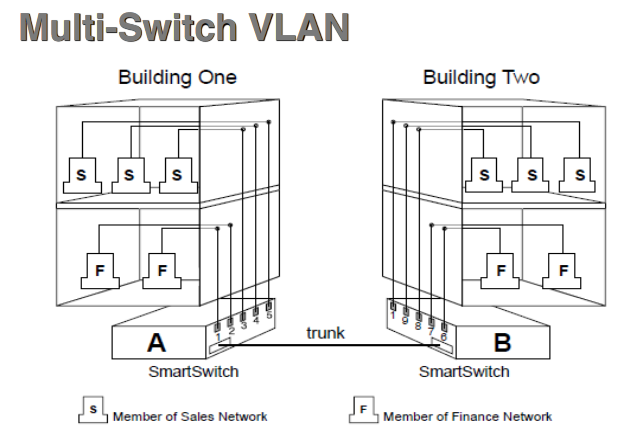
**Styles (Different ways to create a backbone network)**

1. Switched backbone
   1. Uses switches, so it operates at layer 2 of the OSI model (data link layer [MAC Addresses])
   2. Moves packets between LAN networks based on data link layer addresses (MAC)
   3. Cheap and easy to install (just uses switches)
   4. More cabling, but less devices
   5. This makes the network more simple and easier to manage
   6. Has improved performance
   7. **PERFORMS WELL FOR SMALL NETWORKS**  
      
2. Switched collapsed backbone
   1. Exactly the same as a switched backbone, but all switches are together in a cabinet (single location)
   2. Just makes it a bit easier to manage and move devices / people around as needed
   3. Longer cabling again, but improved simplicity, and administration of the network (as everything is one place)
   4. Since everything is in one rack, uses a star topology



1. Routed backbone
   1. Operates at the network layer (uses routers too)
   2. Moves packets using network layer addresses (IP addresses)
   3. Commonly uses a bus topology
   4. Each lane uses a separate subnet
   5. Commonly used at the core layer (connecting building together)
   6. LANs operate as separate entities
   7. Excellent LAN segmentation
   8. Can cause time delays
   9. Not as simple to manage as a switch
2. VLAN backbone
   1. Uses software rather than hardware
   2. Cheaper
   3. Software often has better UI and admin management platforms
   4. Flexible
   5. Scalable
   6. With this flexibility, we can create LANs based on a business functions and requirements
   7. Frees the network from physical constraints
   8. Often faster
   9. More secure, as the flow of traffic is defined by software and can be clearly defined
   10. Easier to assign devices to specific LAN networks
   11. With use of software, LANs are no longer defined by their geographical location

**There are 2 types of VLAN architectures**

1. **Single Switch** → VLANs are created on, managed on, and only exist no a single switch (**BEST FOR MOST MODERN BACKBONE NETWORKING**)
2. **Multi-Switch** → Connecting of multiple switches, creating a larger LAN to work with, then subdividing the network using VLANs software - also allows for the connecting of multiple buildings with this method (**BEST FOR MOST MODERN LARGER ORGANISATIONS**)  
     
   

# WLAN (Wireless Local Area Network)

* WLAN stands for Wireless Local Area Network
* **Uses the electromagnetic spectrum (radio waves)** to transmit and receive data in the form of electromagnetic waves between a Network Interface Card (NIC) and an Access Point (AC)
* Data will be encoded and used to **manipulate the waves transmitted**
* Antennas are used to send and receive electromagnetic waves in the air
* **Waves can collide** with each other, causing disruptions in communication and loss of / corruption of data
* **Half-duplex** networking technology - data can only flow in a single direction
  + Cannot both transmit and receive data at the same time
  + Uses Carrier-Sense Multiple Access (CSMA) and CA (Collision Avoidance) to manage the challenges caused by half-duplex communication
  + This pauses communication when collisions occur and allows clients to retry data transmission to reduce dropped packets
* CSMA / CA consumes most of the bandwidth of WLAN, slows down download and upload speeds, increases response times due to collisions, and worsens as the number of devices increases
* **Logical bus topology** (logical meaning the way data flows - this explains the collisions)
* **Physical star topology**

**802.11x**

This represents the standards created by the IEEE for networking wirelessly over-the-air in a LAN (WLAN). This family of standards can be broken down further into each generation, each with their own specifications. Also known as Wireless Ethernet or Wi-Fi.

**Modern and most commonly used 802.11x generations**

|  |  |  |  |
| --- | --- | --- | --- |
| **802.11x Generation** | **Frequency Bands** | **Theoretical Speeds** | **Theoretical Max Distance** |
| 802.11n | 2.4 GHz & 5 GHz | 450Mbps \* 3 channels | 100m (2.4 GHz) |
| 802.11ac | 2.4 GHz & 5 GHz (SIMULTANEOUS) | 433Mbps \* 8 channels  4.9Gbps \* 1 channel | 100m (2.4GHz)  30m (5 GHz) |

*2.4 GHz travels farther and penetrates walls better than 5 GHz.*

**Multiple Input - Multiple Output (MIMO)**

Simply put, **using more antennas**, increases bandwidth and signal transmission and receiving efficiency.

**WLAN Topologies**

1. Independent Basic Service Set **(IBSS)** - Wireless version of mesh topology, devices communicate directly with each other
2. Infrastructure Basic Service Set **(BSS)** - Wireless version of star topology, devices all communicate with a single access point
3. Extended Service Set **(ESS)** - Connecting multiple BSS WLAN networks with a distribution network (like a backbone network) - ESS is similar to SSID (Service Set IDentifier - allowing you to separate a WLAN)

**WLAN Design Choices**

* Close-by networks should use different channels to reduce collision
* Recommended channels 1, 6, and 11
* Allowed channels vary by country
* Allow for roughly 15% overlap of wireless coverage between APs

**WLAN Security**

* **SSID** (Service Set IDentifier)
  + Required by all clients to include in every packet
  + Plain text
  + Not secure
* **WEP** (Wired Equivalent Privacy)
  + Users must enter a key manually
  + Communication is encrypted using this key
  + Good for small office / home office networks
  + Easy to break with brute force
* **WPA-2 (Wi-Fi Protected Access) [current WLAN security standard]**
  + Longer key is used for encryption
  + Master key obtained through EAP (connecting to WLAN)
  + Master key used to establish a secret key for communication for the session
  + Keys used to create new keys for encrypted communication
  + Key is different for every password, the master and secret key are used to decrypt
  + Session key (secret key) has a limited lifetime

# MAN + WAN

These types of networks exist to allow for network communication over long distances. Often, MAN and WAN solutions are used to connect multiple LANs which are not near each other (e.g., a Sydney, Melbourne, and Brisbane office).

**MANs** **(Metropolitan Area Network)** → Used to connect backbone networks between 5 kms - 50 kms

**WANs (Wide Area Network)** → Used to connect MANs, backbone networks, and LANs and much longer distances, usually > 100 kms

**Circuits (purchasing / renting a dedicated connection line to premises)**

**Circuit-Switched services**:

* Simplest approach
* Circuit is established only when data is being transferred (similar to the phone network)
* Pay for use
* Uses the public switched telephone network (PSTN)
* “Connect, Data, Disconnect”
* Pros: No routing delay, no congestion, packets are ordered, no packet analysis at hops, is a dedicated line
* Cons: Has connection delay, not efficient with capacity, can be expensive, no visibility as to what happens to data during transmission, slow speed

**Dedicated Circuits Networks**:

* Point-to-point links
* Flat fee, unlimited traffic
* Permanent lease (vs switched circuit), this connection is just for you
* **Topologies**:
  + Ring → Reliable, data usually flows in a single direction (can flow in both direction with slower speeds), messages travel around the ring, hitting many nodes before reaching destination
  + Star → Easy management, single point of failure (central location), performance bottleneck
  + Mesh → High redundancy, best performance, (full-mesh very expensive, partial-mesh much more practical)
* **Services**:
  + SONET → Very fast, very expensive, leased lines by companies
  + T-Carrier → Fast, expensive, leased lines by companies

**Connection Types Matrix** (use appropriate connection based on requirements)

|  |  |
| --- | --- |
| **Connection-oriented** | **Connectionless** |
| Voice calls | Internet |
| Continuous data streams (video streaming) | Bursts |
| Constant data rate | Different data rates |

**Packet-Switched Networks (Sharing circuits / non-dedicated circuits)**

Circuits waste networking resources and capacity (for data). Packet switching shares a circuit and has a massively reduced cost. Pay for connection to circuit and traffic sent over the network. Connection can be both leased or owned.

**Methods**:

Datagrams (Connectionless)

* No connection or circuit is set up
* Address in the packet
* Path between two nodes can change
* Packets can be out of order
* Packets can be dropped (missing)
* Each packet handled independently
* Pros: Fast, minimal overhead, cheap
* Cons: The recipient must try and detect dropped, corrupted, or out of order packets

Virtual Circuits (Creating a connection using connectionless datagrams) [sort of like tcp]

* Packets follow same route (faster, more efficient)
* Permanent (PVC)
  + Long-term (lasts days or weeks)
  + Managed by network manager
  + Common
  + Behaves like a dedicated circuit
* Switched (SVC)
  + Establish on demand
  + Disconnect when done

**Services**:

* **MPLS (Multi Protocol Label Switching)**
  + Runs over the internet (does not need new expensive hardware to work)
  + Best of connectionless and connection-oriented worlds
  + Sends packets over established paths
  + MPLS Header inserted into the packet (between layer 2 and 3)
  + Packet path is forwarded using this established Label
  + Forwarding uses a simple table lookup, faster than general packet routing
  + MPLS works over any existing type of WAN connection
  + MPLS is more complex as it adds another layer to packets
  + Very commonly used
  + Very expensive
* **Ethernet services**
  + Much cheaper than other services
  + No translations required (typically packets have been translated from ethernet packets to something else to assist with transferring over longer distances)
  + Fast
  + Kind of like a standard broadband cable
* **VPN (Virtual Private Networks)**
  + Encrypt, encapsulates, and sends packets through a tunnel
  + Operated over the standard public internet
  + VERY low cost
  + VERY easy to set up
  + Unpredictable QoS (Quality of Service - measuring the performance of the network communication)
  + Transparent to everyone (uses the public internet) - but is encrypted
  + Very redundant
  + If no internet connection, no VPN connection either
  + Potential for eavesdropping as uses public internet (handles with encryption)