Enterprise Network Architecture

INFO-6078 – Managing Enterprise Networks

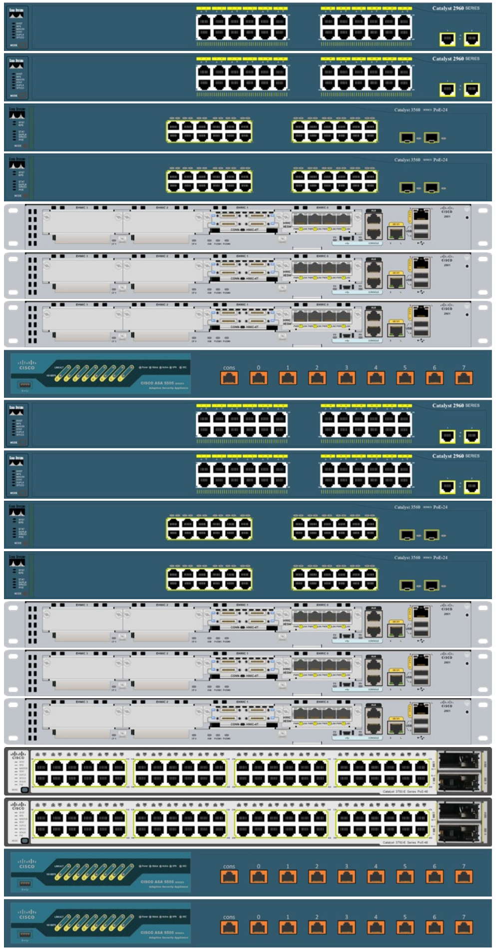
FANSHAWE

Network Topologies

- Topologies describe the arrangement of network elements (end-devices, network links, network hardware, etc.), and how they create the network as a whole
- Most networks can be described by their **Physical Topology** and their **Logical Topology;** however, most networks can be categorized as having more than one logical topology

Physical Topologies

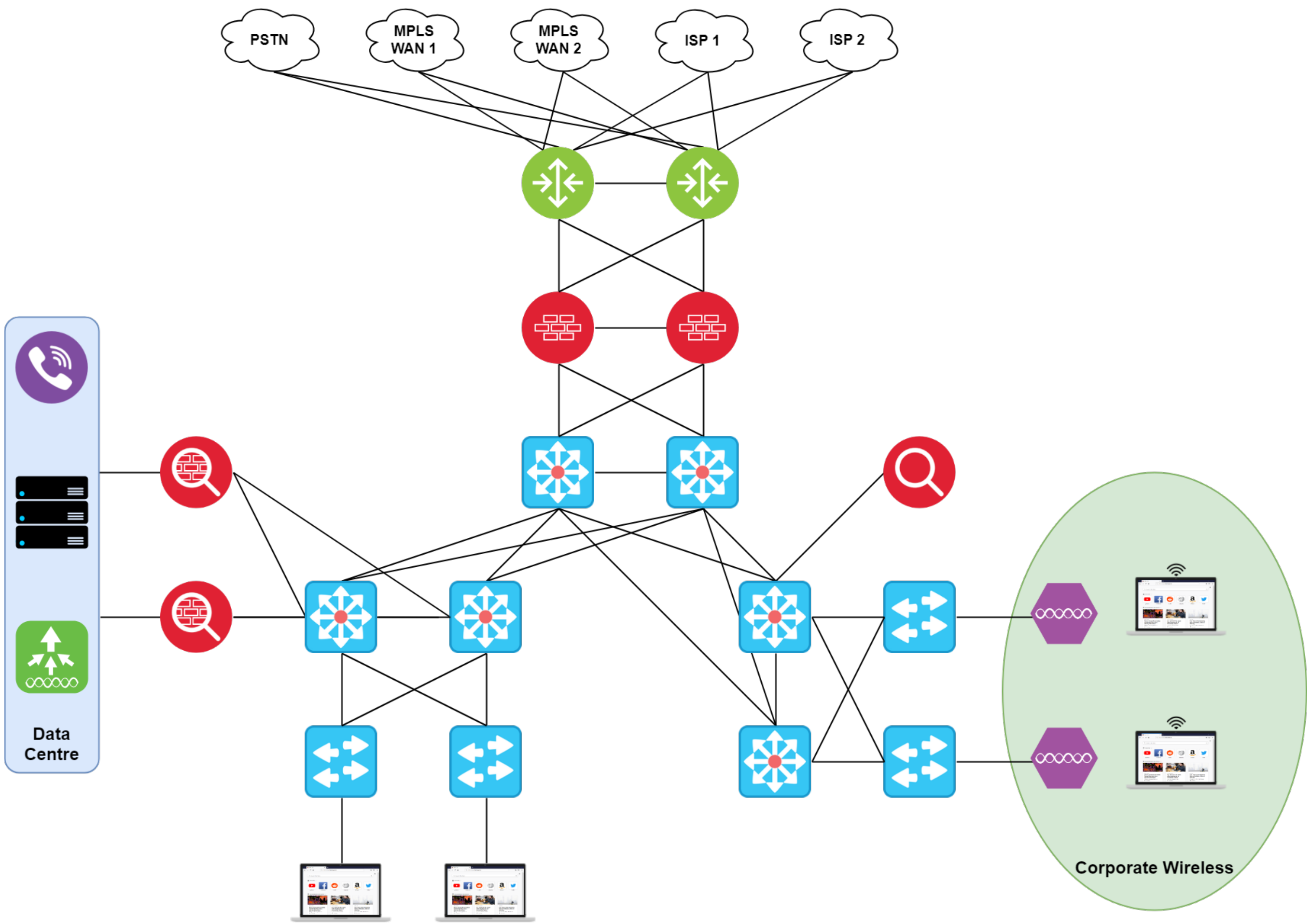
- A physical topology describes the physical structure of the network, and details the devices that are being connected, as well as the connection type and specifications of such
- Physical topologies can include items such as:
  - Device models
  - Software revision
  - Cabling positions
  - Cable specifications
  - Cabling endpoints



Logical Topologies

- A logical topology describes the logical connections between various network nodes, and identifies how information is moved across the network
- Logical topologies can include items such as:
  - Devices
  - VLANS
  - Link speeds
  - Virtual connections
  - Routing domains

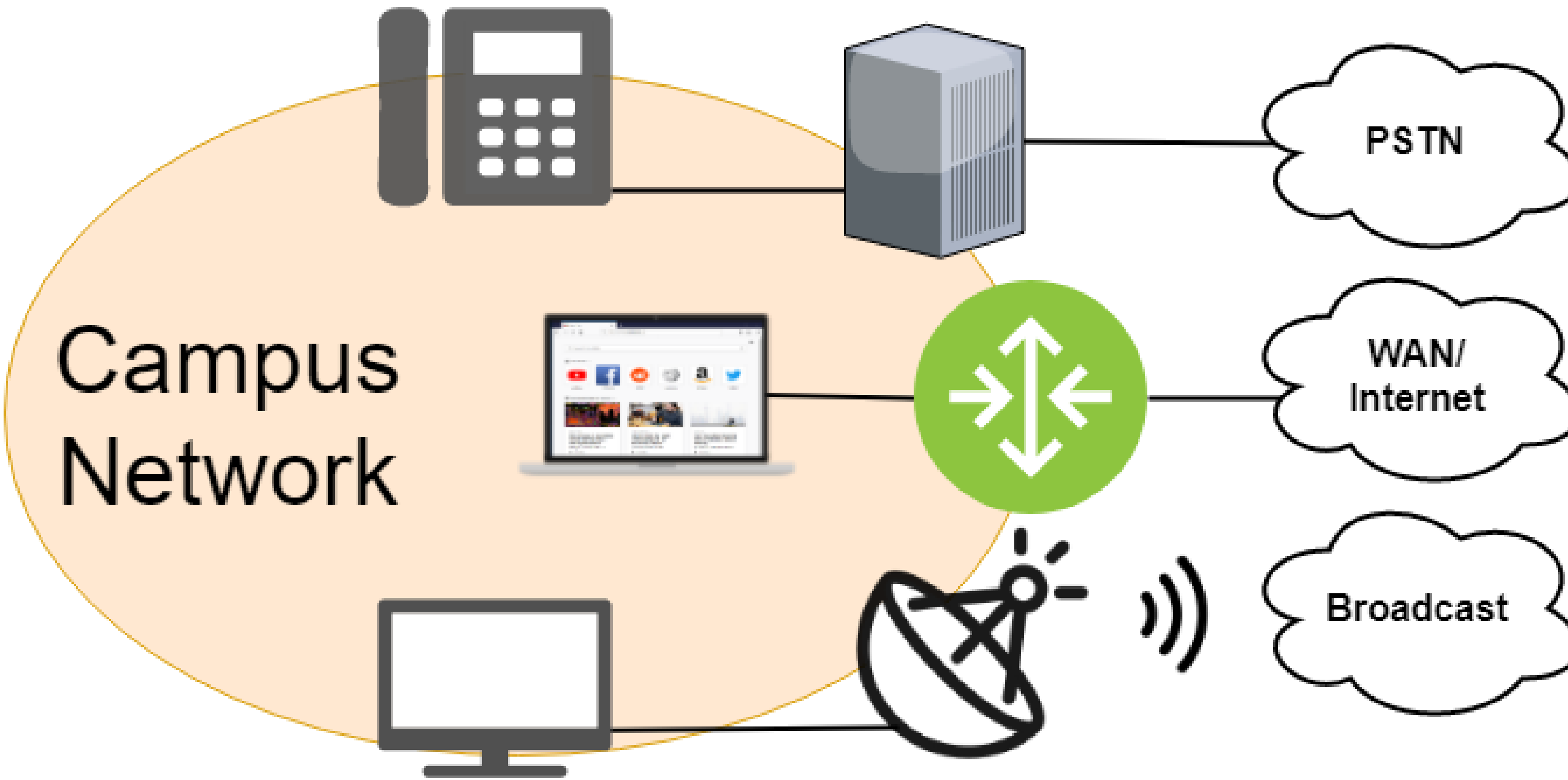
Logical Topologies



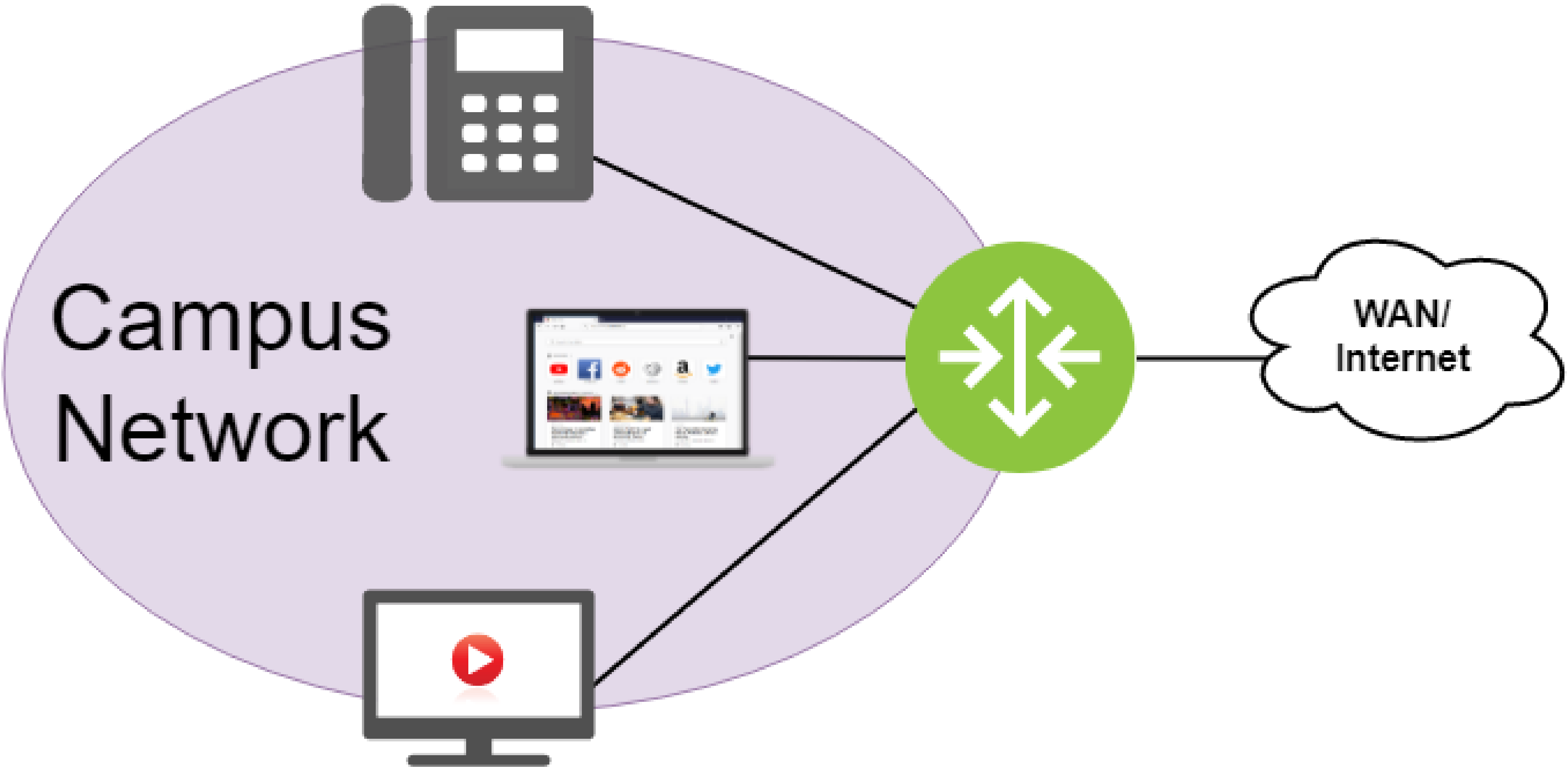
Network Convergence

- Traditionally, a separate network was required for each media type, and buildings would have separate cable runs for data, telephone/intercom systems, as well as television or CCTV services
- Modern networks are capable of providing multiple "converged" services across a single network platform
- As each of these services have unique requirements, network hardware and protocol requirements have evolved to meet the demands of these networks

Network Convergence – Traditional Networks



Network Convergence – Converged Networks



Network Reliability

- Enterprise networks must meet and exceed the needs of the organization, even during a partial outage
- Additionally, an organizations network should be able to grow as the requirements of the organization changes
- The four underlying concepts related to the provision of network reliability are:
  - Fault Tolerance
  - Scalability
  - Service Quality
  - Security

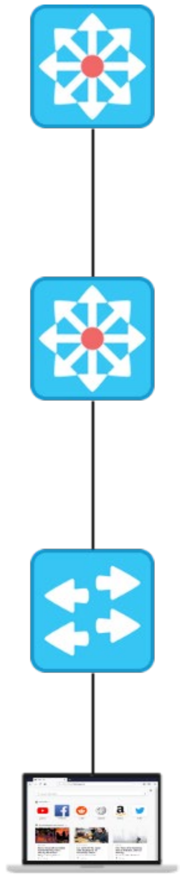
FANSHAWE

Fault Tolerance

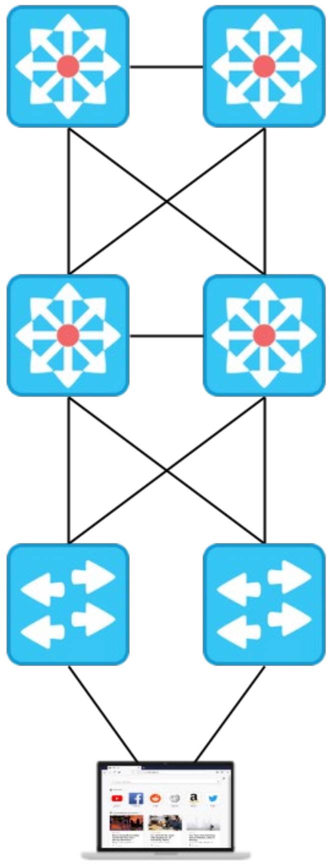
- In organizations, it is the expectation that the network is a basic service that business functions utilize
- Many organizations are also migrating core business functions to the cloud, which makes access to these services critical to business continuity
- Fault Tolerance describes how the network will behave should an outage occur
- A crucial element in designing a fault tolerant network is designing one that avoids any possible single points of failure.

Fault Tolerance

Single Point of Failure



No Single Point of Failure



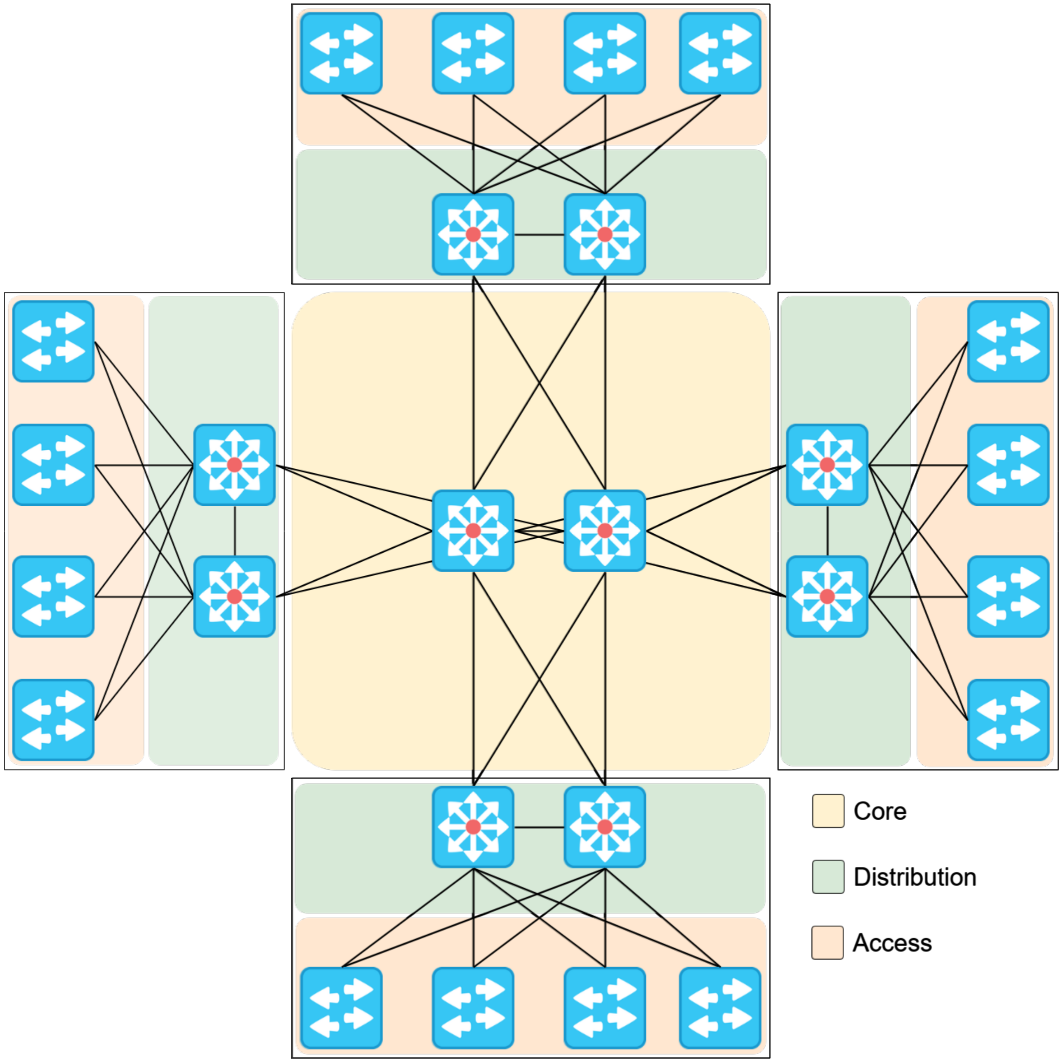
Fault Tolerance

- Fault tolerant networks utilize redundancy to provide alternative paths, should a failure occur.
- In addition to providing redundant paths to user services, the following should be taken into account:
  - Service provider connections
  - Connection media
  - Power supply/backups
  - Cooling
  - Phone systems

FANSHAWE

Scalability

- A scalable network can be expanded to provide service to new users with minimal impact to users and services currently operating on the network.



Service Quality

- As more business functions rely on services provided across the network, service quality becomes an important topic
- Congestion occurs when demand for the network exceeds the available bandwidth
- The result of congestion on the network includes dropped packets, retransmissions, or delay
- On converged networks, congestion would occur if a user downloading a file using BitTorrent is allowed to saturate a connection that is also used for customer telephone calls

Service Quality

- Services like voice over IP (VoIP) calling or video conferencing make higher demands on the network, as they are almost always sensitive to dropped packets or delay
- Quality of Service (QoS) can provide increased priority to services that have higher expectations of the network such as VoIP and video conferencing

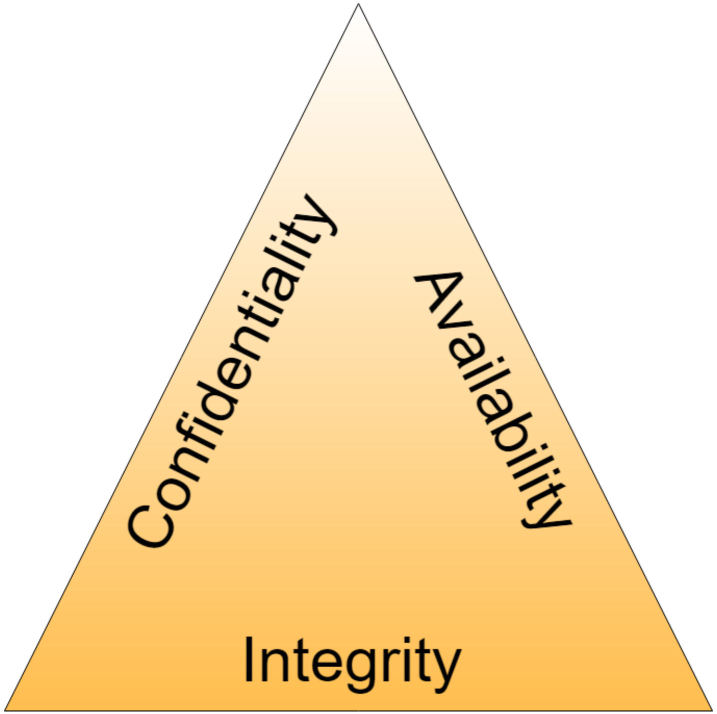
Security

- Confidential and personal information is often transmitted over data networks
- Network security provides safeguards to protect this information in the following ways:
  - **Infrastructure security** – ensuring that only authorized users have access to the network infrastructure
    - Examples of infrastructure security include user logins for network devices
  - **Information Security** – ensuring that the information being transmitted over the network arrives intact and is delivered only to the recipient

Confidentiality, Integrity and Availability

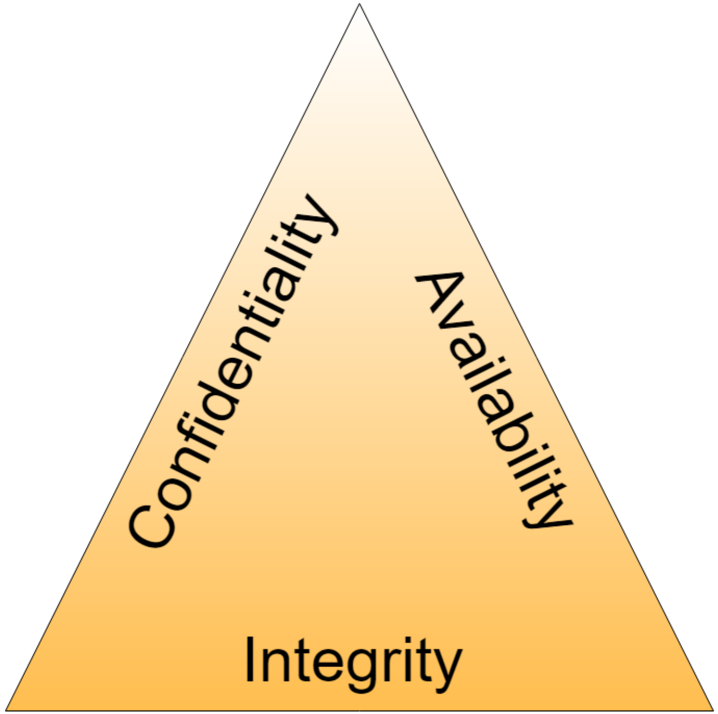
When considering information security, we relate most tasks to preserving one of the tenants of Confidentiality, Integrity and Availability (CIA)

- **Confidentiality**
  - Refers to safeguarding information, keeping it away from those that should not have access
  - Controls that preserve confidentiality are permissions and encryption



Confidentiality, Integrity and Availability

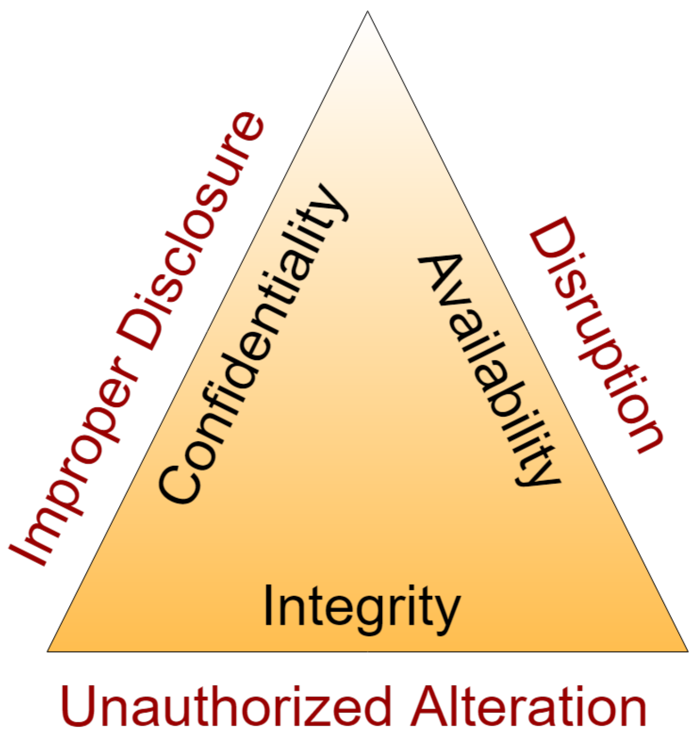
- **Integrity**
  - Deals with keeping information in a format that retains its original purpose
  - The receiver opens the data and it is as the creator intended
- **Availability**
  - Keeping information and resources available to those that need them, when they need them



Confidentiality, Integrity and Availability

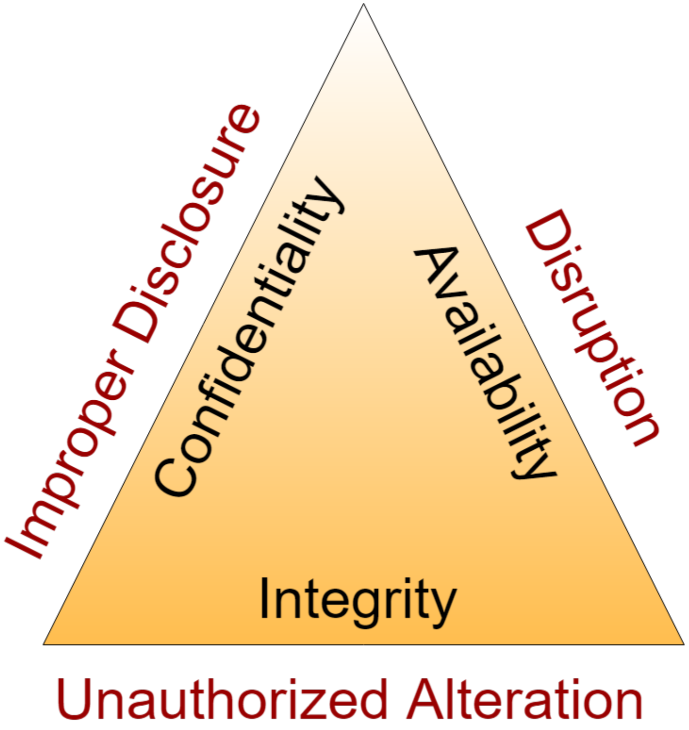
Another way of looking at this is to consider the consequences when CIA has been compromised:

- **Improper Disclosure**
  - Inadvertent, accidental, or malicious revealing or accessing of information or resources to an outside party.



Confidentiality, Integrity and Availability

- **Unauthorized Alteration**
  - Unauthorized or unintended modification of information.
  - Examples include corruption, accidental access, or malicious access.
- **Disruption (loss)**
  - Access to information or resources has been lost when it should have been available.
  - Information is useless if it is not available when needed.



Network Segmentation

- Network segmentation is the practice of splitting a computer network into smaller subnetworks (subnets, VLANS)
- Segmentation provides the following benefits:
  - **Reduced Congestion**
    - Network performance is improved as fewer hosts are contending for network resources
  - **Improved Security**
    - The network surface is reduced, and any host trying to spy on network traffic may not be on the correct segment
- Segmentation may be required to meet regulatory standards

Service-Level Agreement

- A service-level agreement (SLA) is a contract between a service provider and a client that defines the level of service the client can expect in terms of availability and reliability
- An SLA includes two distinct areas:
  - **Services** – Defines metrics of the service provided including:
    - **Percentage of Uptime**
      - How often the client can expect outages to occur
    - **Responsiveness**
      - Metrics that govern how the service should perform under regular conditions
    - **Mean time to recover**
      - If an outage occurs, how quickly can the service be restored

Service-Level Agreement

- **Management** – Defines additional details including:
  - A description of the service provided
  - The procedure for reporting problems
  - Performance monitoring guidelines
  - Consequences of not meeting service levels
  - When and how the agreement can be updated
  - Escape clauses
- Service availability is usually express terms of percentage of uptime and the class of nines

Service-Level Agreement

Number of Nines	Availability Percentage	Downtime per year
Two Nines	99%	3.65 days
Three Nines	99.9%	8.77 hours
Four Nines	99.99%	52.6 minutes
Five Nines	99.999%	5.26 minutes
Six Nines	99.9999%	31.56 seconds

- The cost of providing a service increases exponentially as the availability percentage increases

Hierarchical Design

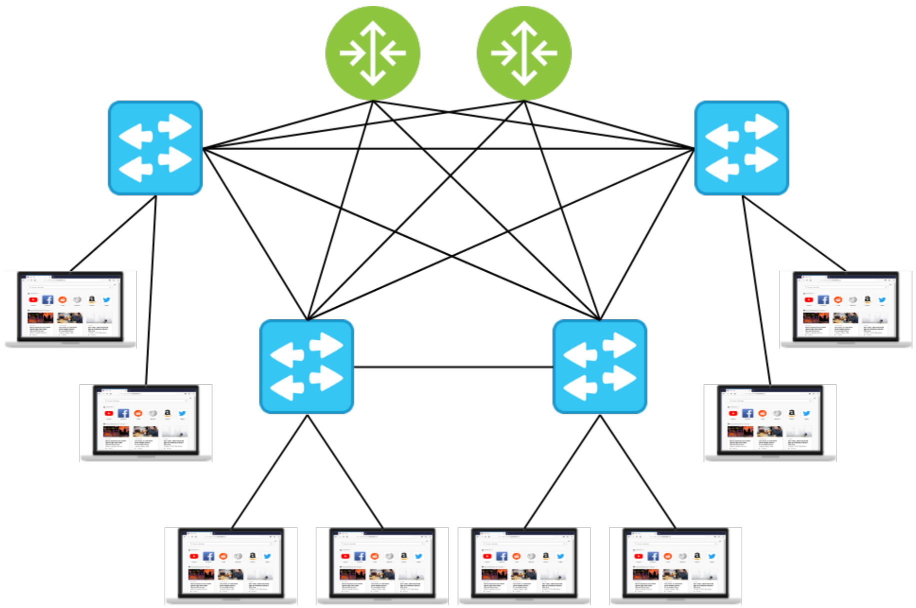
- Most enterprise networks follow the principles of a 3 or 2 layer hierarchical design
- Initially developed by Cisco, hierarchical design can provide the following benefits to an organization:
  - It allows network architects to minimize the size of broadcast domains, thus decreasing the amount of broadcast traffic that each host must process
  - It allows for segmentation, as well as filtering and access control at specific layers

Hierarchical Design

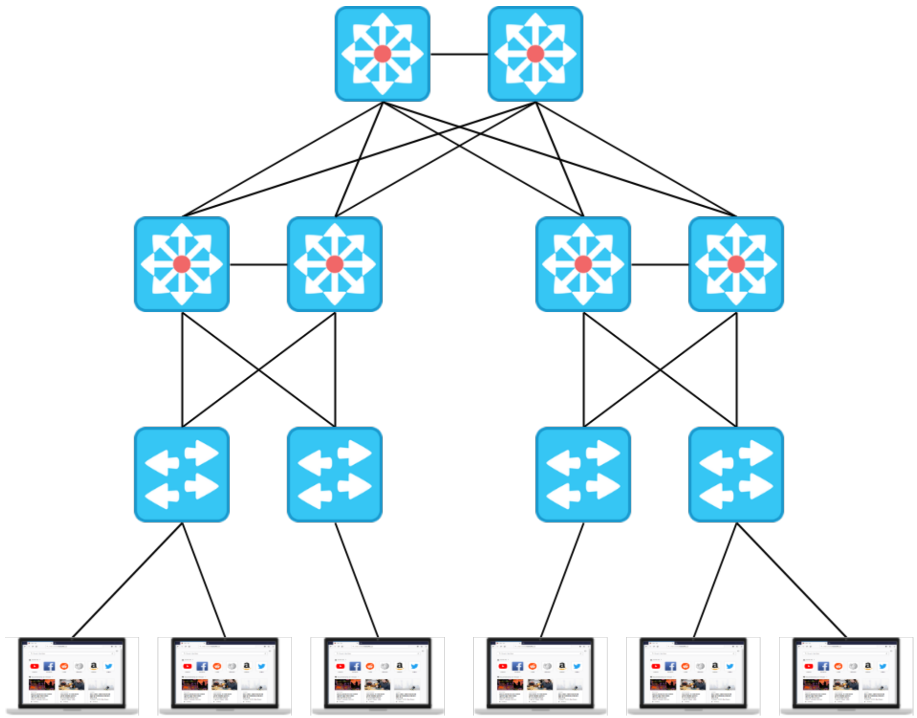
- It standardizes the equipment required for each layer of the network, potentially saving money for the organization
- The modular nature of hierarchical design allows for more accurate capacity planning
- Incorporates simplicity into network design, as each layer has a predetermined set of functions
- Testing and fault isolation are improved
- Upgrade costs can be limited to a section of the network

Mesh Design vs Hierarchical-Mesh Topologies

Mesh Network Design



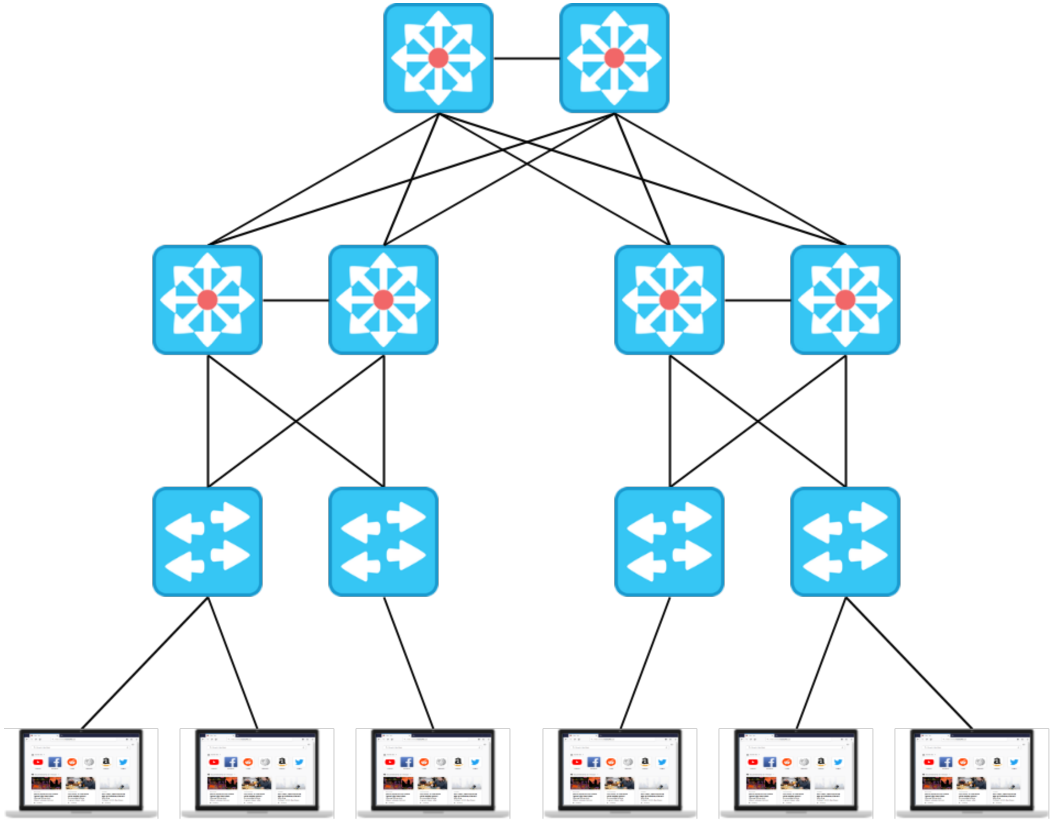
Hierarchical Network Design



FANSHAWE

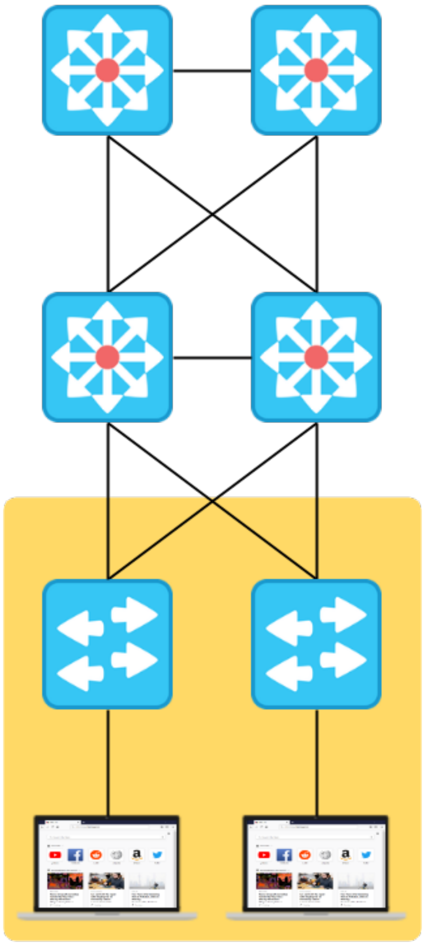
Three-Layer Hierarchical Networks

- Three layer hierarchical networks are split into the following layers:
  - Access
  - Distribution
  - Core



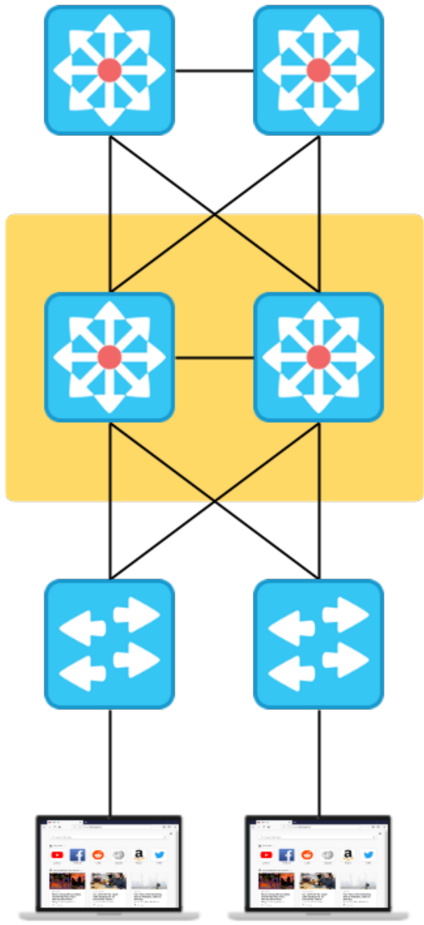
Access Layer

- As its name suggests, the access layer provides access to network resources for end-devices
- Traditionally, the access layer provides layer 2 connections to devices
- Characteristics of the access layer include:
  - Power over Ethernet (PoE)
  - QoS Classifications
  - Port Security
  - Loop Prevention



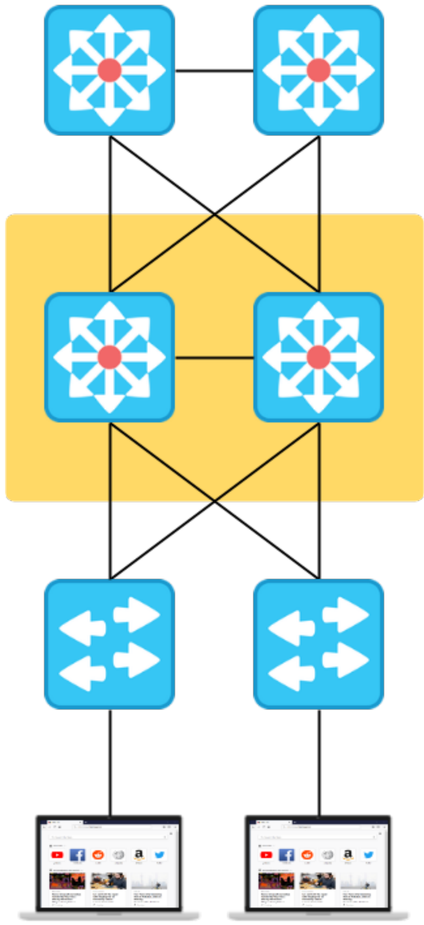
Distribution Layer

- The distribution layer is the intermediary between the access layer and the network core
- The distribution layer is almost always comprised of devices running at layer 3 of the OSI model
- Characteristics of the distribution layer include:
  - Boundary definition
  - Routing



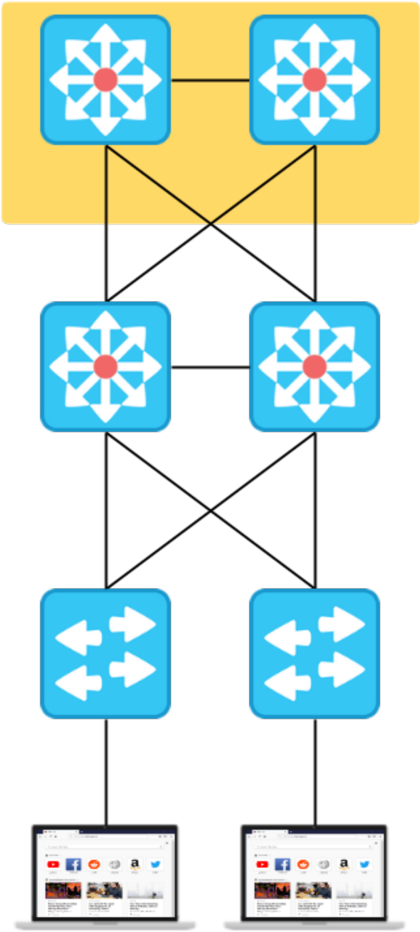
Distribution Layer

- Traffic filtering and ACLs
- QoS Policy management
- Broadcast Domain Control
- Load Balancing



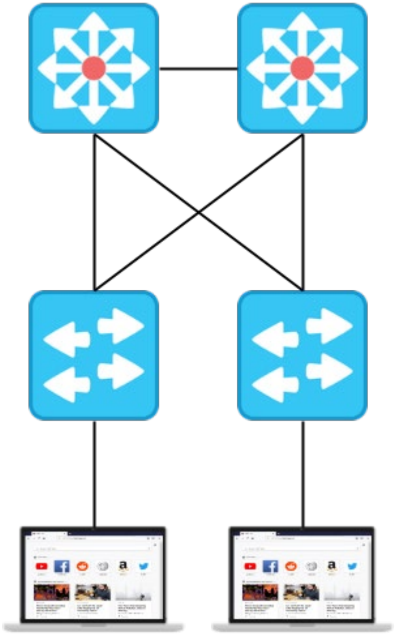
Core Layer

- The core layer is the high-speed backbone of the network
- The primary function of the core is to move information as fast as possible to it’s destination
- The core will also connect geographically separate areas of the network
- As the purpose of the core is to deliver information quickly, it is not recommended to inspect traffic in the core



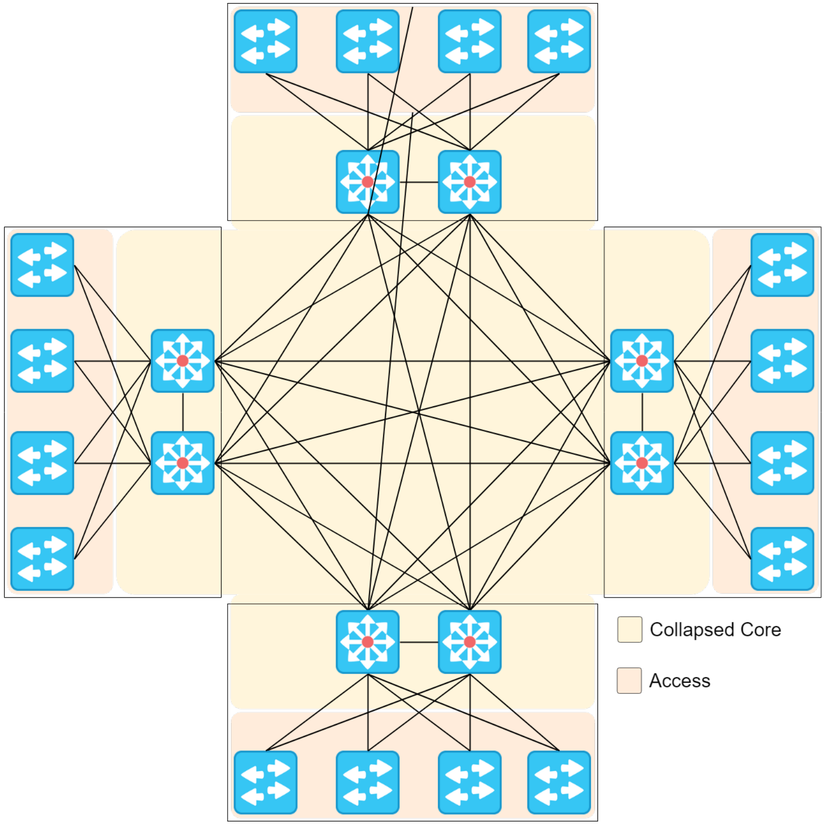
Two-Layer Hierarchical Networks

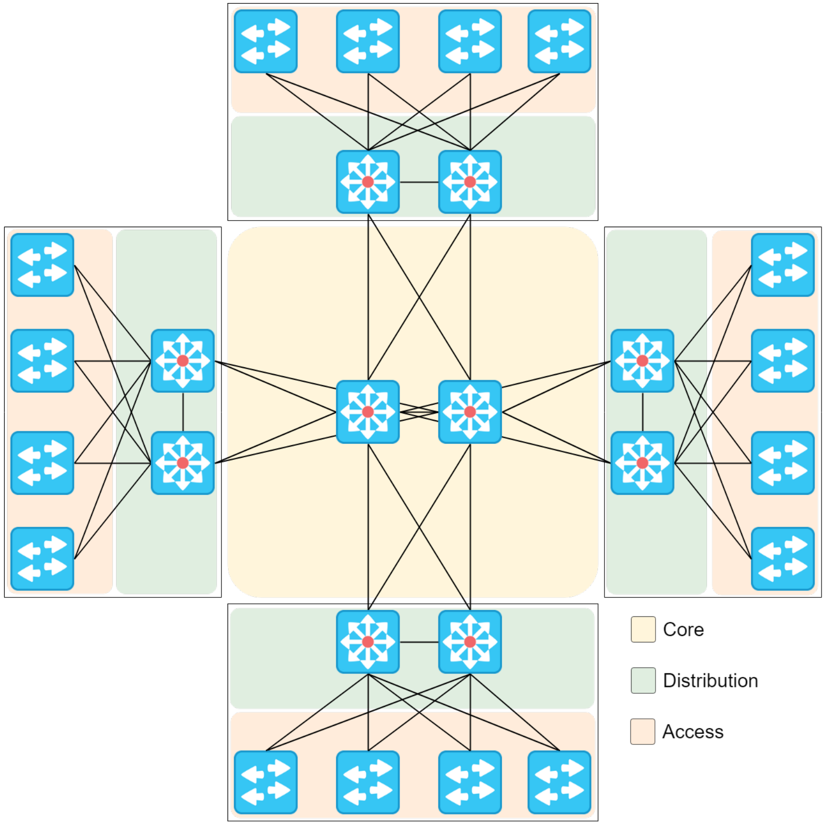
- Also known as the collapsed-core design, the two-layer hierarchical design combines the functions of the distribution and core layers into a single layer
- A two-layer design is suitable for smaller organizations that have no plans for significant growth
- The primary motivation for choosing a two-layer design is the financial savings associated with the model



FANSHAWE

Two-Layer vs Three-Layer





FANSHAWE

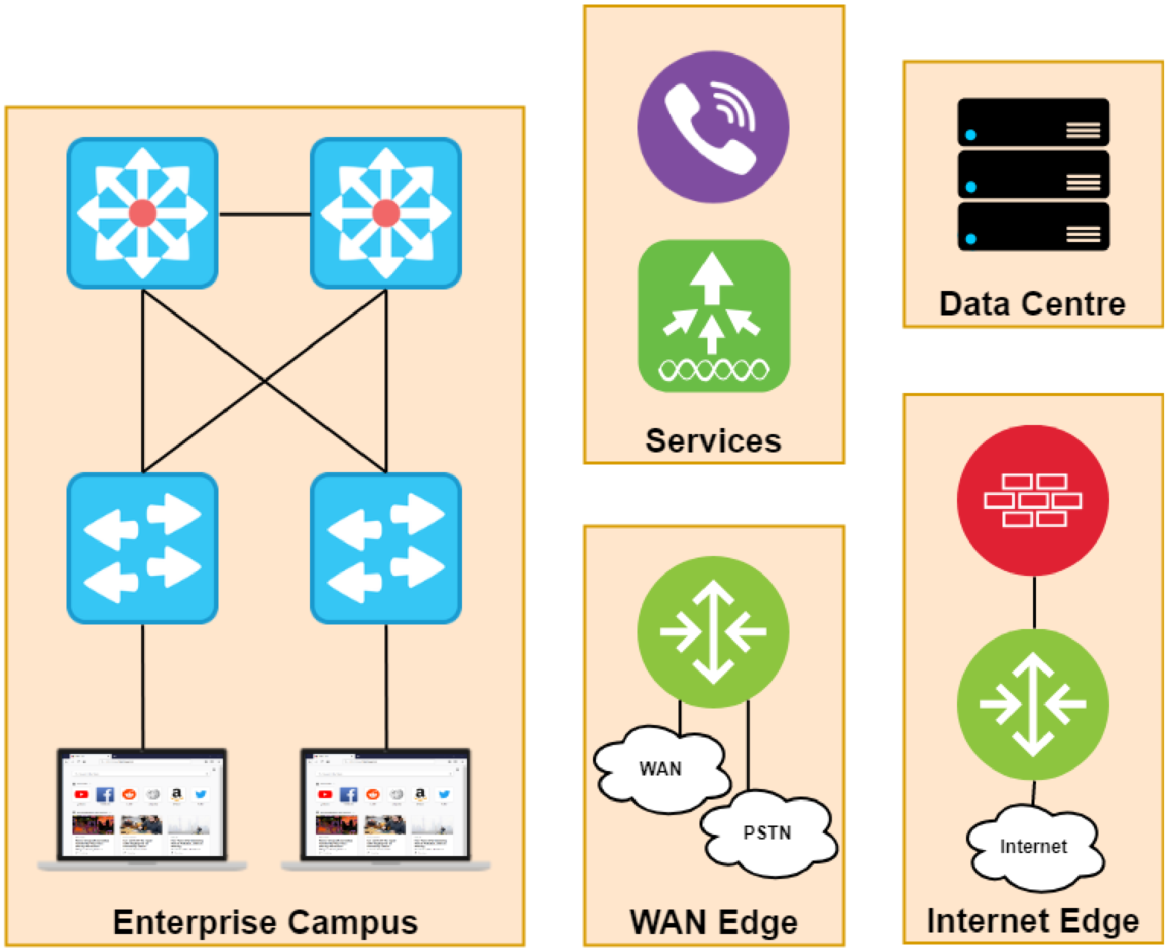
Modular Network Design

- Incorporating modular network design improves scalability and fault tolerance, as well as simplifying troubleshooting
- When discussing modular network design, Cisco uses the term Enterprise Composite Network Model to describe the various modules
- The Enterprise Composite Network Model is comprised of three main sections, the **Enterprise Campus**, **Enterprise Edge** and the **Service Provider Edge,** as well as optional sections such as **Enterprise Branch**, **Enterprise Data Center** and **Enterprise Teleworker**

Modular Network Design

- Enterprise campus includes the access, distribution and core layers that allow users to connect to the network
- The Service Provider Edge is not managed by the organization, but refers to the infrastructure maintained by the service provider

Modular Network Design



Edge Connections

- Today, many organizations are built around the tools and services provided on the internet
- Additionally, more software vendors are moving their business applications to the cloud
- Internet is now considered an essential service for organizations to make money
- The terms single/multi-homing describe the number any type of internet connections organizations can use to support their business

Single-homing vs Multi-homing

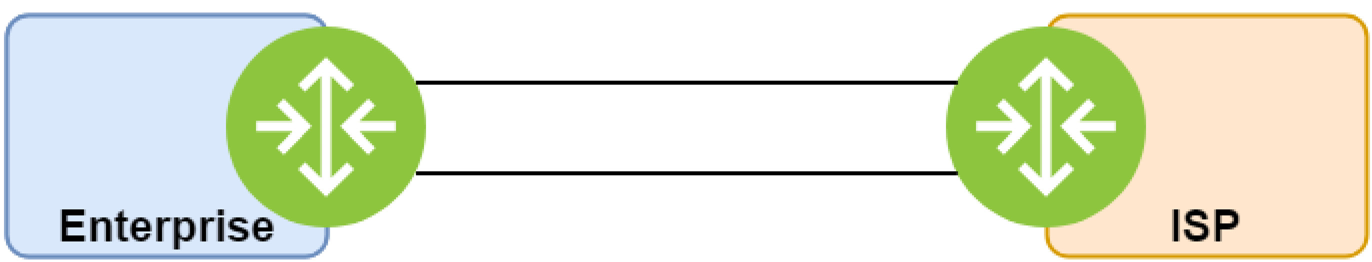
- **Single-homed:**
  - Provides the best cost savings at the expense of reliability
  - Can often utilize static routing for simplification of device management
  - BGP setup is not required
- **Multi-homed:**
  - Redundant connections protect the network against upstream failures
  - Often takes advantage of dynamic routing and the ability to provide automatic best-path selection
  - BGP setup is preferred

Edge Connections – Single Homed

- A single connection to a single ISP
- Simplest setup to deploy
- Lowest overall cost to the organization
- Provides no redundancy

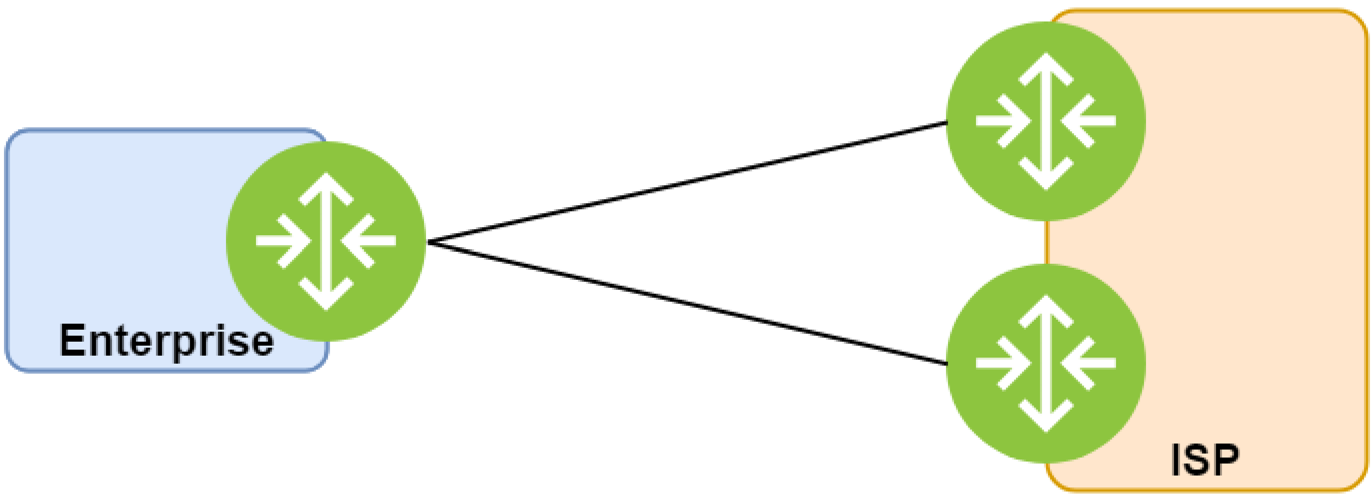
Edge Connections – Dual Homed

- The enterprise is still connected via a single ISP, but utilizes two connections to the ISP
- Provides some redundancy
- Lower overall cost
- Simple management for organization



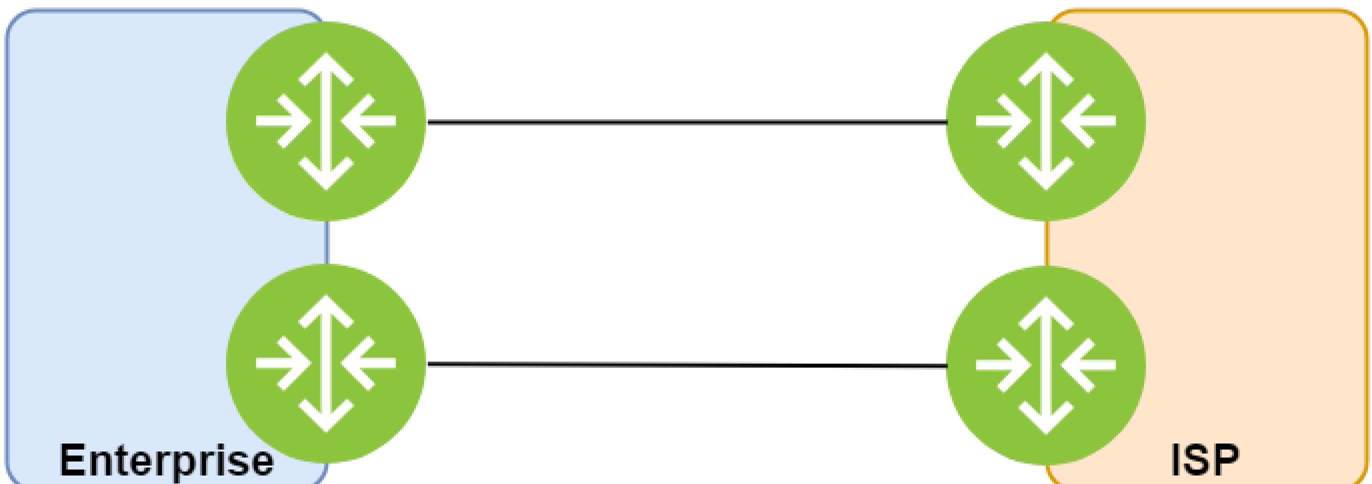
Edge Connections – Dual Homed

- The enterprise is still connected via a single ISP, but utilizes two connections to the ISP
- The ISP provides connections from different routers
- Lower overall cost
- Simple management for organization



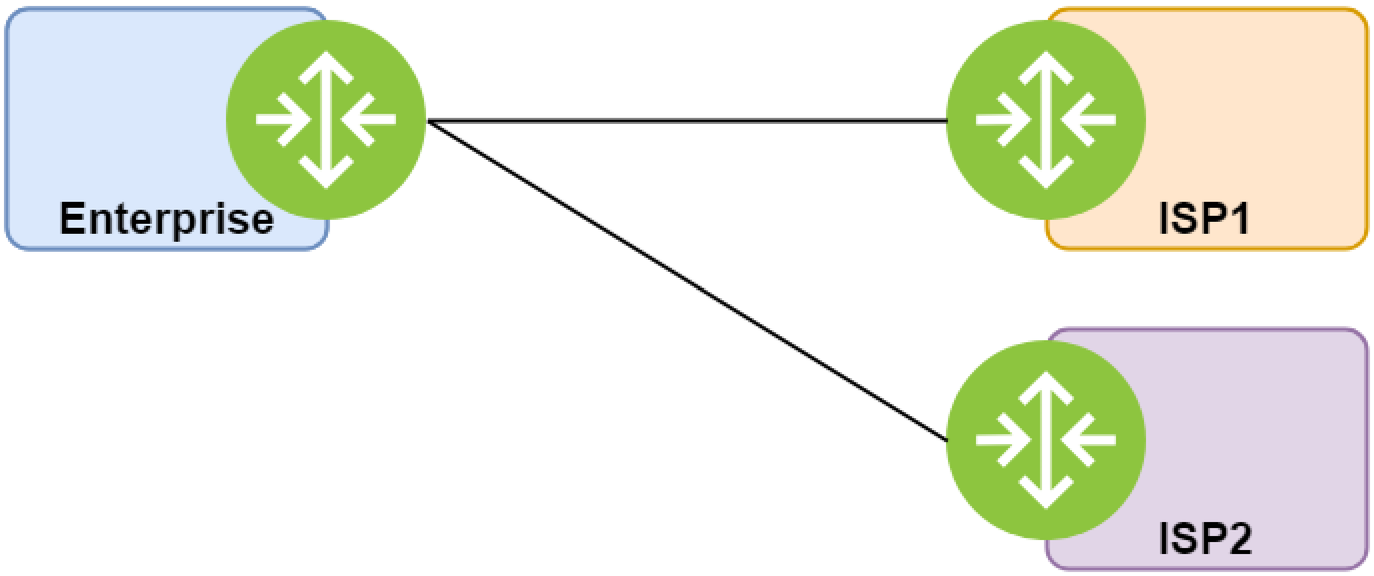
Edge Connections – Dual Homed

- The enterprise is still connected via a single ISP, but utilizes two connections to the ISP
- Each connection uses a different router to provide redundancy (this is the most reliable connection to a single ISP)
- Simple management for organization



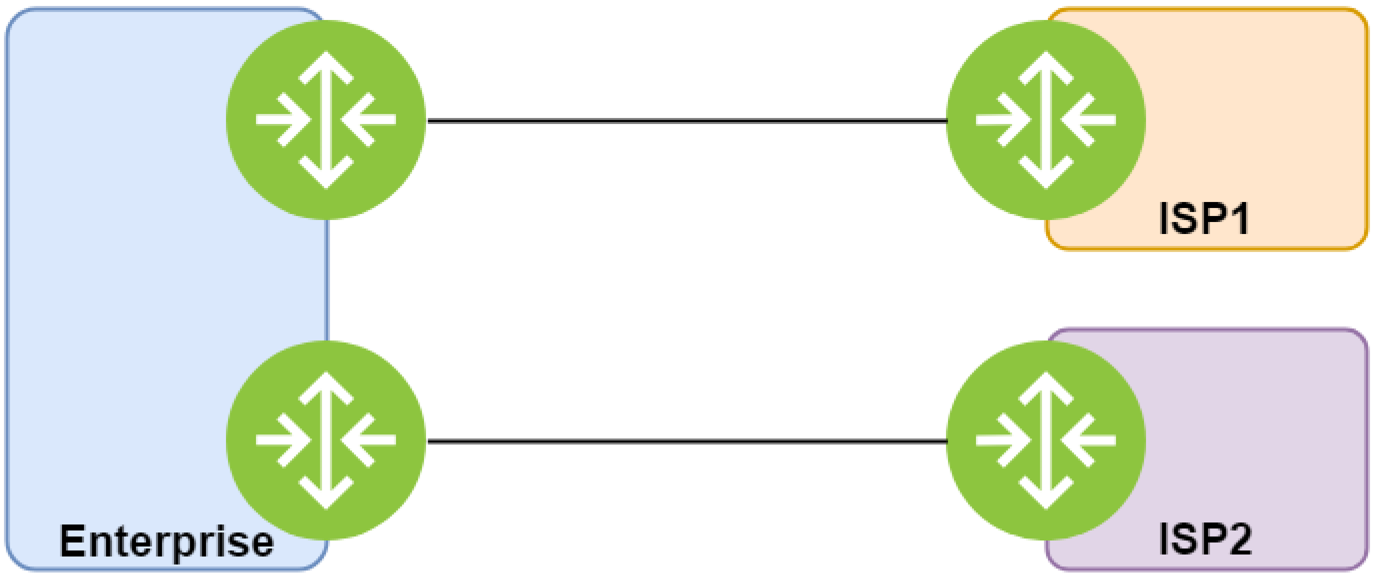
Edge Connections – Single Multihomed

- The enterprise is connected to at least two different ISPs
- Moderate cost to organization
- Provides some redundancy
- The enterprise router creates a single point of failure



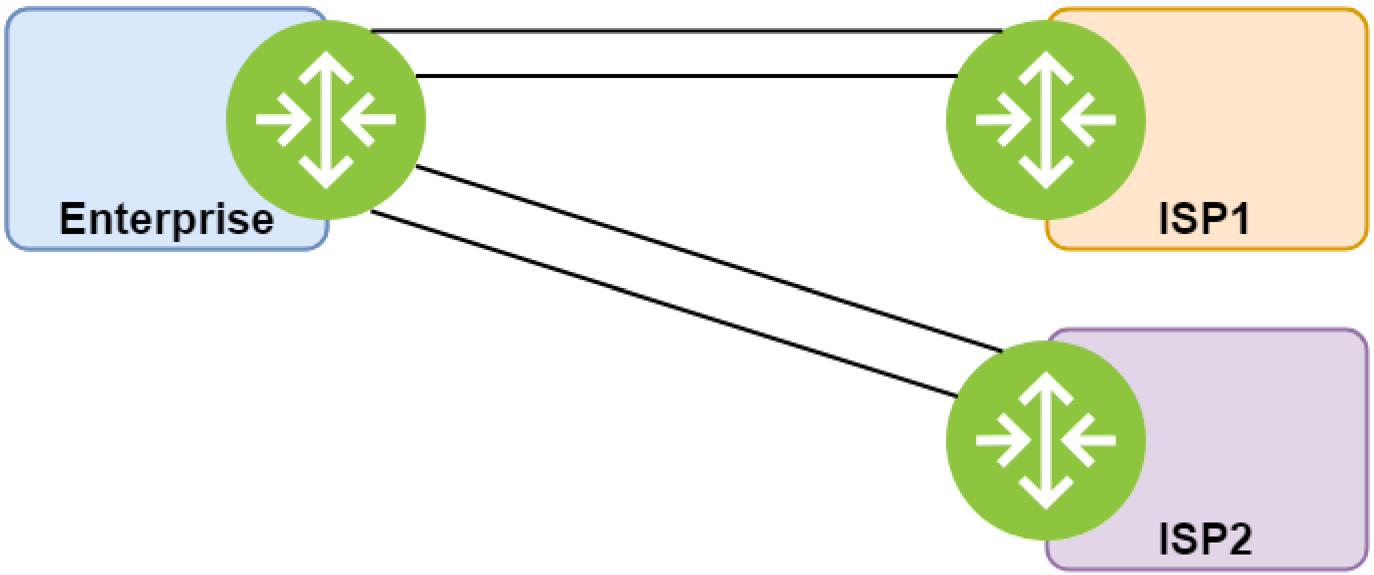
Edge Connections – Single Multihomed

- The enterprise is connected to at least two different ISPs using independent routers
- Moderate cost to organization
- Provides moderate redundancy



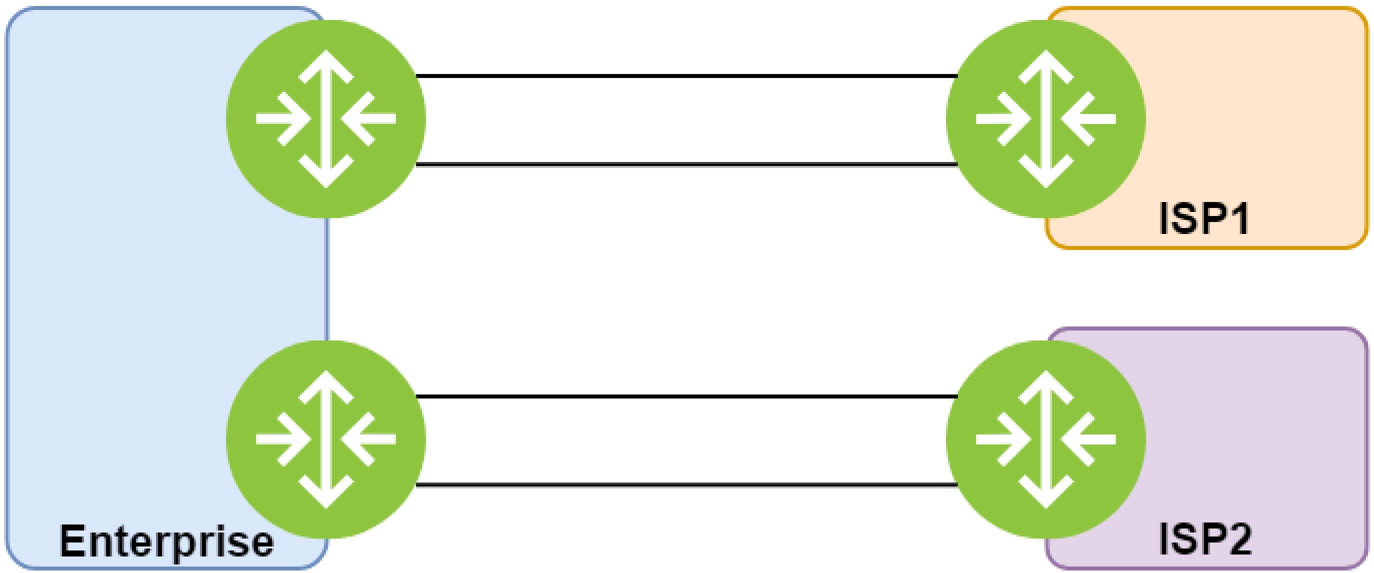
Edge Connections – Dual Multihomed

- The enterprise is connected to at least two different ISPs using redundant connections
- Moderate to high cost to organization
- Provides moderate redundancy



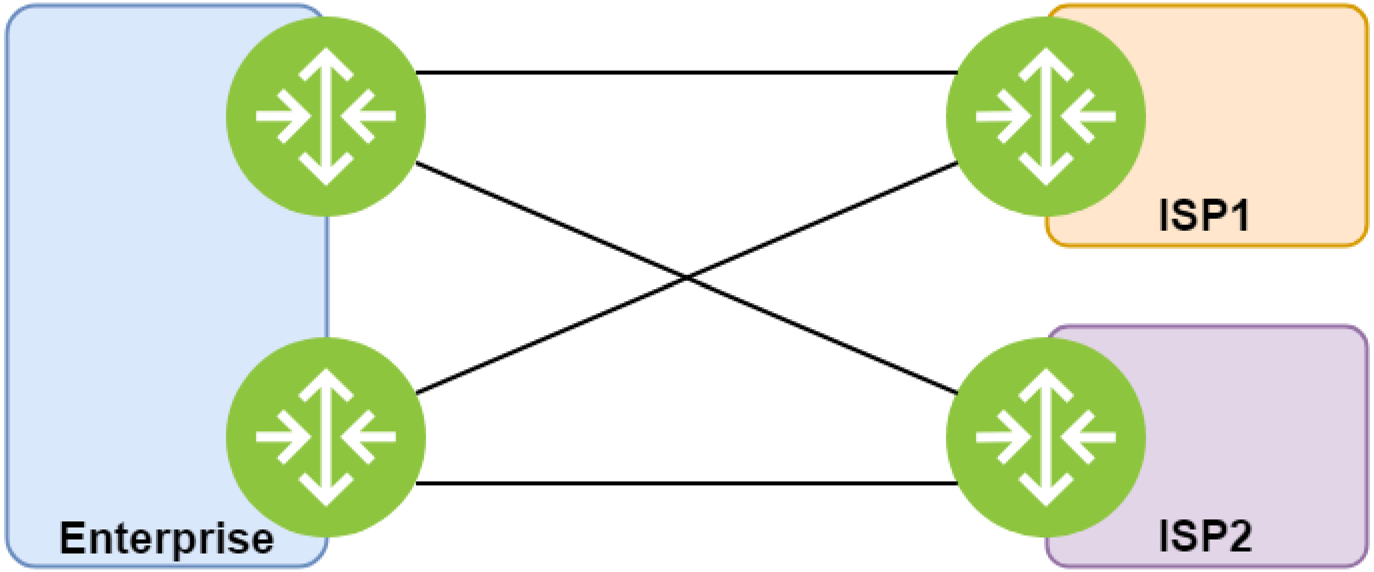
Edge Connections – Dual Multihomed

- The enterprise is connected to at least two different ISPs using multiple routers and redundant connections
- High cost to the organization
- Provides moderate redundancy



Edge Connections – Dual Multihomed

- The enterprise is connected to at least two different ISPs using multiple routers and redundant connections
- High cost to the organization
- Provides highest level of redundancy, but is the most complex setup



WAN Connections

- When organizations span cities, provinces or across the world, private communication across locations is important
- The public internet does not provide a suitable environment for communication that requires privacy or Quality-of-Service
- Wide Area Networks (WANs) can provide a solution that allows organizations to communicate both securely and provide traffic prioritization from source to destination
- Many WAN technologies exist and provide various levels of privacy, reliability, and the ability to provide QoS

WAN Connection Types

- Some (mostly) legacy WAN technologies:
  - **Frame Relay**
    - Provides a permanent virtual circuit (PVC), which appears to be a dedicated connection from the customers standpoint, but is actually a shared connection from a service provider perspective
  - **Asynchronous Transfer Mode (ATM)**
    - Designed to integrate telecommunications networks, ATM was designed to handle real-time, low-latency communications such as IP telephony
    - ATM utilized 53 byte “cells” to provide reduced latency for time-sensitive transfers

WAN Connection Types

- Some current WAN technologies:
  - **Dedicated Leased Line**
    - While an aging technology, dedicated leased lines are still found in organizations due to the increased level of privacy they provide, as well as guaranteed bandwidth and support for QoS
    - The main disadvantage of leased lines is the expense of connecting all required nodes in an redundant manner
    - Another disadvantage of leased lines is the limited bandwidth of connections:
      - **T1 (1.544 Mbps)** – 24 (64 Kbps) channels (DS0)
      - **E1 (2.048 Mbps)** – 32 (64 Kbps) channels
      - **T3 (44.736 Mbps)** – 672 (64 Kbps) channels (28 T1 connections)
      - **E3 (34.368 Mbps)** – 480 (64 Kbps) channels (16 E1 connections)

WAN Connection Types

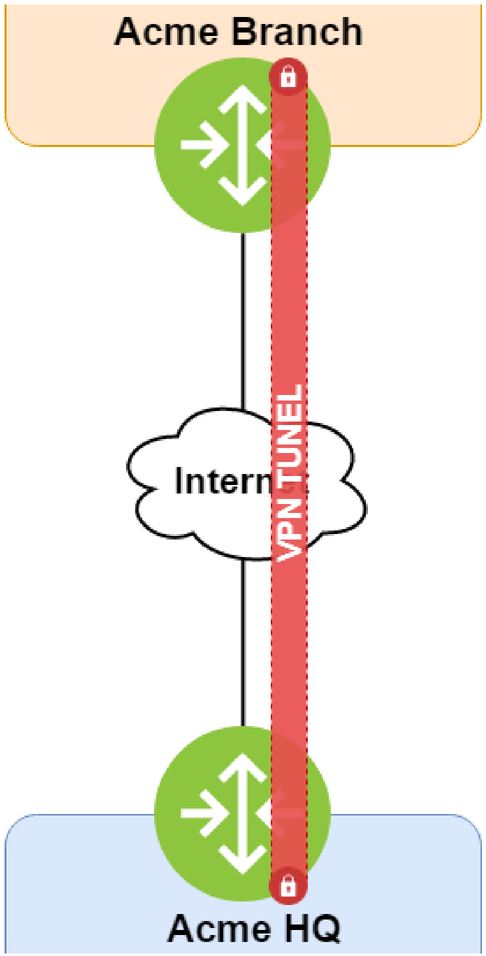
- **Multiprotocol Label Switching (MPLS)**
  - Forwards packets based on path labels instead of route destinations
  - MPLS packets have a label assigned when leaving the customers network
  - This label is used to move the packet through the carrier network, without inspecting the packet further
  - QoS is supported and makes MPLS a popular choice for modern WAN connections
  - MPLS is normally one of the most expensive types of WAN connection for organizations

WAN Connection Types

- **Metro Ethernet**
  - Metro Ethernet was developed to offer Ethernet services for enterprise customers to connect their LANs over high-bandwidth optical Metropolitan networks
  - The success of Metro Ethernet led to the development of Carrier Ethernet
- **Carrier Ethernet**
  - Carrier Ethernet has expanded Metro Ethernet to traverse national and international networks
  - It promises QoS, lower latency, higher throughput and increased flexibility when compared to MPLS
  - CE makes use of VLANs to provide internet access and private network access over a single connection

WAN Connection Types

- **Virtual Private Network (VPN)**
  - VPNs utilize encapsulation and encryption to create “private” tunnels that connect sites and users over the public internet
  - While cheap to deploy, VPNs increase network latency between sites due to processing time for encryption
  - As VPNs traverse the public internet, QoS information is not retained and makes VPNs unsuitable for real-time applications



WAN Connection Types

- **Software-defined WAN (SD-WAN)**
  - While inherently not a type of WAN connection itself, SD-WAN promises to make WAN architectures with diverse connection types easier for organizations to deploy operate and manage.
  - SD-WAN includes WAN optimization by aggregating public and private WAN connections to deliver the optimal path for traffic based on the needs of the application
  - SD-WAN connects remote sites via a central controller to determine how traffic will flow

Voice Connections - PSTN

- Converged networks provide voice services to users in addition to data services
- As a result, modern networks require connections to the public switched telephone network (PSTN)
- Although many organizations incorporate VoIP systems on their networks, most still have connections to the PSTN to provide emergency services (911), and potentially as a backup service should the VoIP system fail

Voice Connections - VoIP

- Voice over Internet Protocol (VoIP) is a key component in modern converged networks
- Providing voice services from networking devices allows organizations to remove outdated Private Branch Exchange (PBX) systems and provide additional benefits to end users such as integration into business systems
- VoIP is normally more cost effective than deploying a separate telephony solution
- Session Initiation Protocol (SIP) Trunks connect enterprise VoIP systems to VoIP service providers for fully VoIP solutions

References

- https://www.edrawsoft.com/Hierarchical-Network-Design.php
- https://www.edrawsoft.com/Modular-Network-Design.php
- https://networklessons.com/cisco/ccna-routing-switching-icnd2-200-105/singledual-homed-and-multi-homed-designs/
- http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=5
- http://www.ciscopress.com/articles/article.asp?p=1073230
- https://datapacket.com/blog/multihomed-network-vs-single-homed-network/

FANSHAWE

References

- Edge Connections –
  - https://datapacket.com/blog/multihomed-network-vs-single-homed-network/
  - https://networklessons.com/cisco/ccna-routing-switching-icnd2-200-105/singledual-homed-and-multi-homed-designs/
- Service-Level Agreement –
  - https://www.paloaltonetworks.com/cyberpedia/what-is-a-service-level-agreement-sla
  - https://www.cio.com/article/2438284/outsourcing/outsourcing-sla-definitions-and-solutions.html

FANSHAWE

References

- WAN Connections –
  - https://searchnetworking.techtarget.com/definition/WAN-wide-area-network
  - https://searchnetworking.techtarget.com/tip/SD-WAN-vs-VPN-How-do-they-compare
- Voice Connections –
  - https://www.nextiva.com/blog/pstn-vs-voip-vs-pots.html