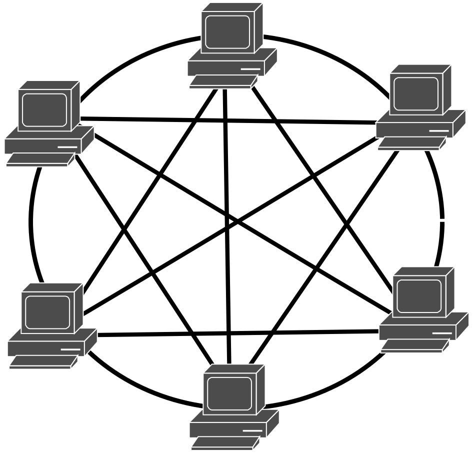
Network Design Models

Redes de Comunicações II

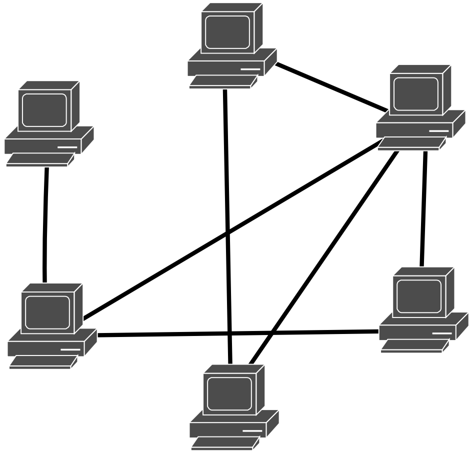
Licenciatura em
Engenharia de Computadores e Informática
DETI-UA

universidade de aveiro
deti.ua.pt

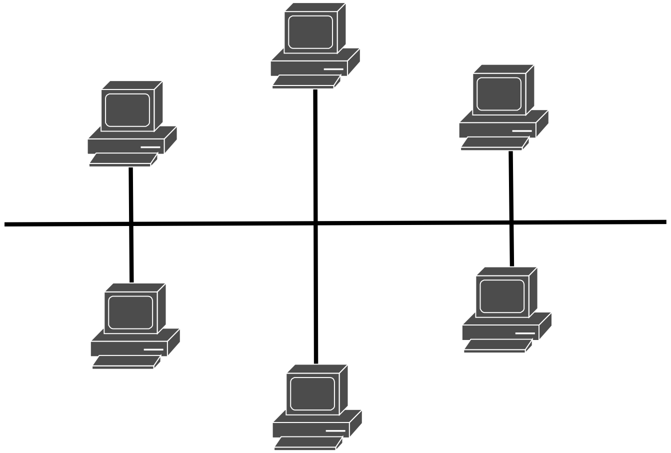
Types of Network Topology



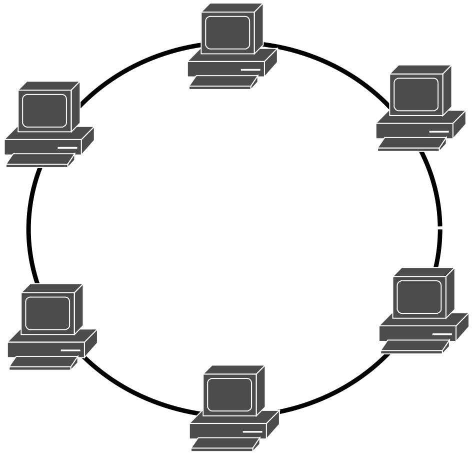
Fully Connected



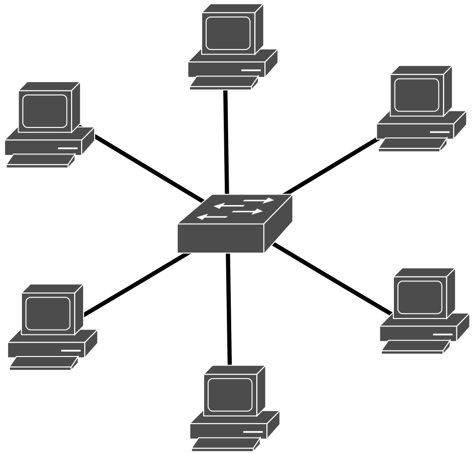
Mesh



Common Bus



Ring

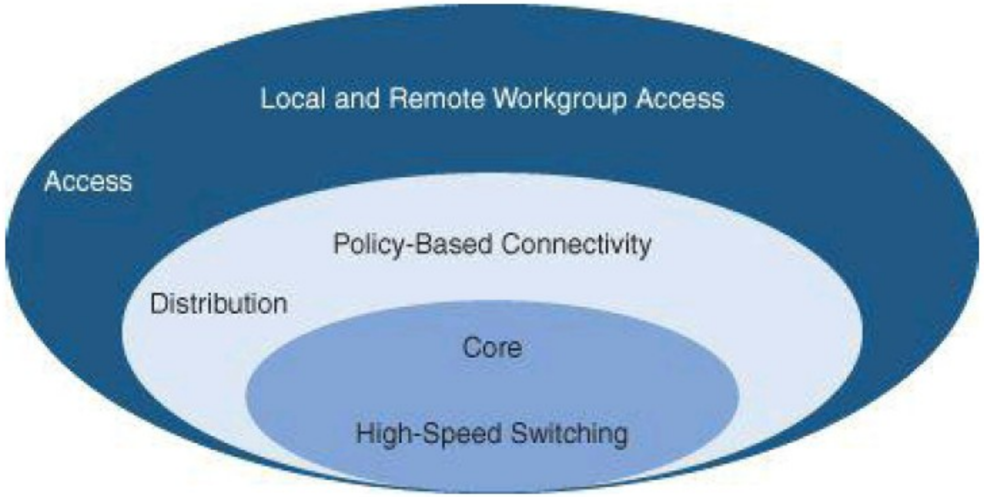


Star

Objectives of Network Design

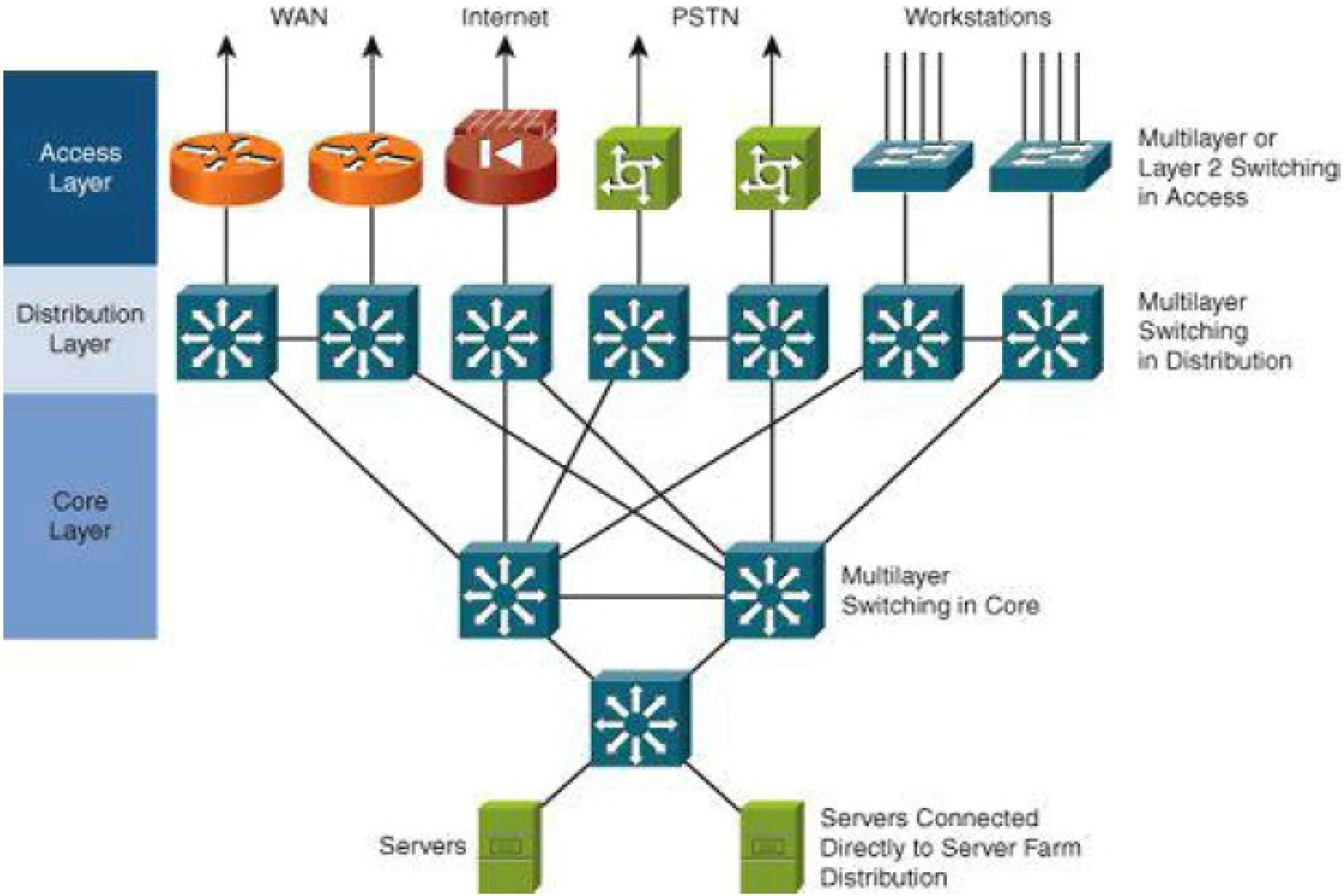
- Network should be **Modular**
  - Support growth and change.
  - Scaling the network is eased by adding new modules instead of complete redesigns.
- Network should be **Resilient**
  - Up-time close to 100 percent.
    - If network fails in some companies (e.g. financial), even for a second, may represent millions of lost revenue.
    - If network fails in a modern hospital, this may represent lost of lives.
  - Resilience has costs.
    - Resilience level should be a trade-off between available budget and acceptable risk.
- Network should have **Flexibility**
  - Businesses change and evolve.
  - Network should adapt quickly.

Hierarchical Network Model

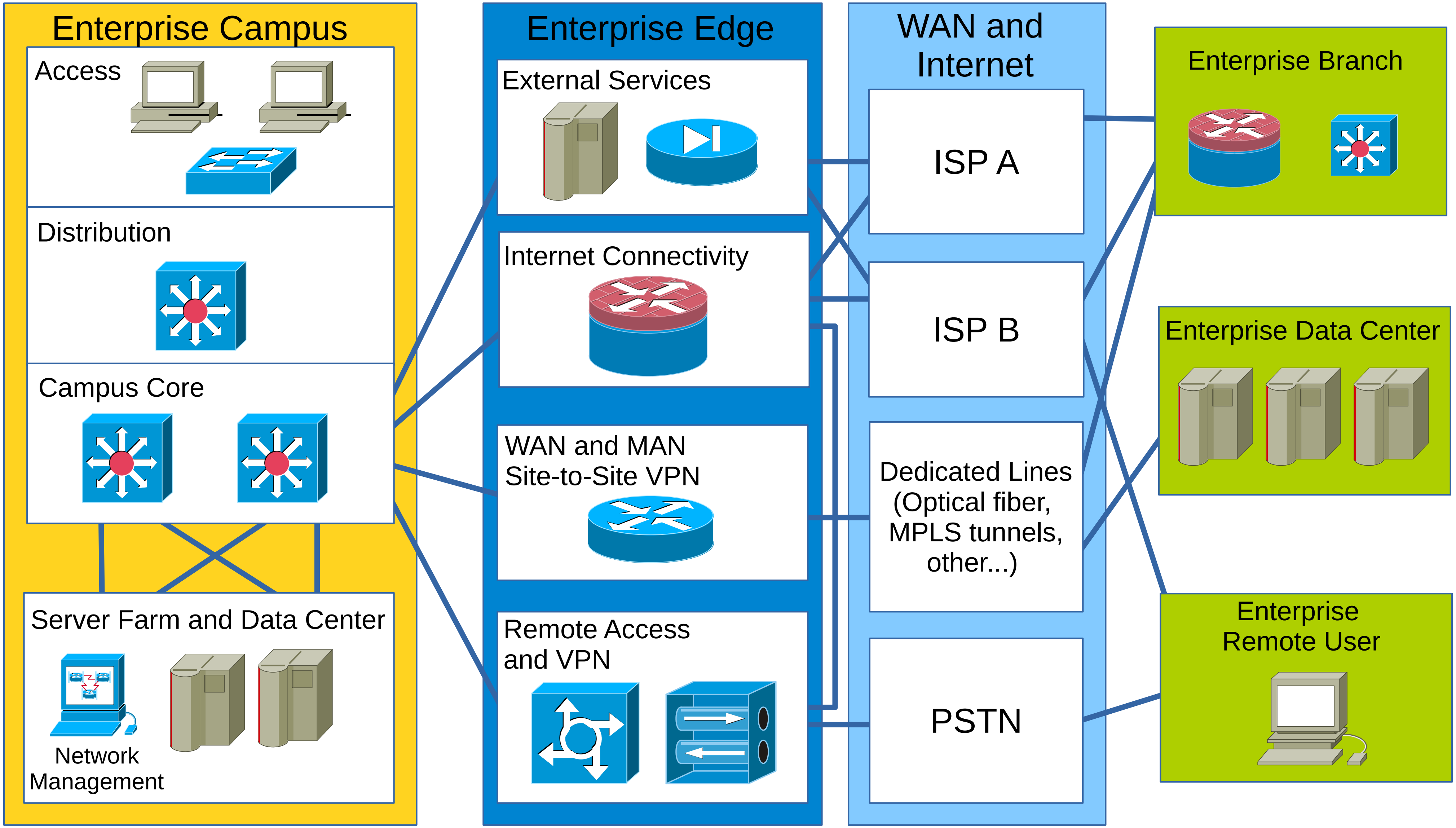


- Access layer
  - Provides user access to network.
  - Generally incorporates switched LAN devices that provide connectivity to workstations, IP phones, servers, and wireless access points.
  - For remote users or remote sites provide an entry to the network across WAN technology.
- Distribution layer
  - Aggregates LAN devices.
  - Segments work groups and isolate network problems.
  - Aggregates WAN connections at the edge of the campus and provides policy-based connectivity.
  - Implements QoS policies.
- Core layer
  - A high-speed backbone.
  - Core is critical for connectivity, must provide a high level of availability and adapt quickly to changes.
  - Should provide scalability and fast convergence.
  - Should provide an integration point for data center.

A Hierarchical Network



Modular Network Design



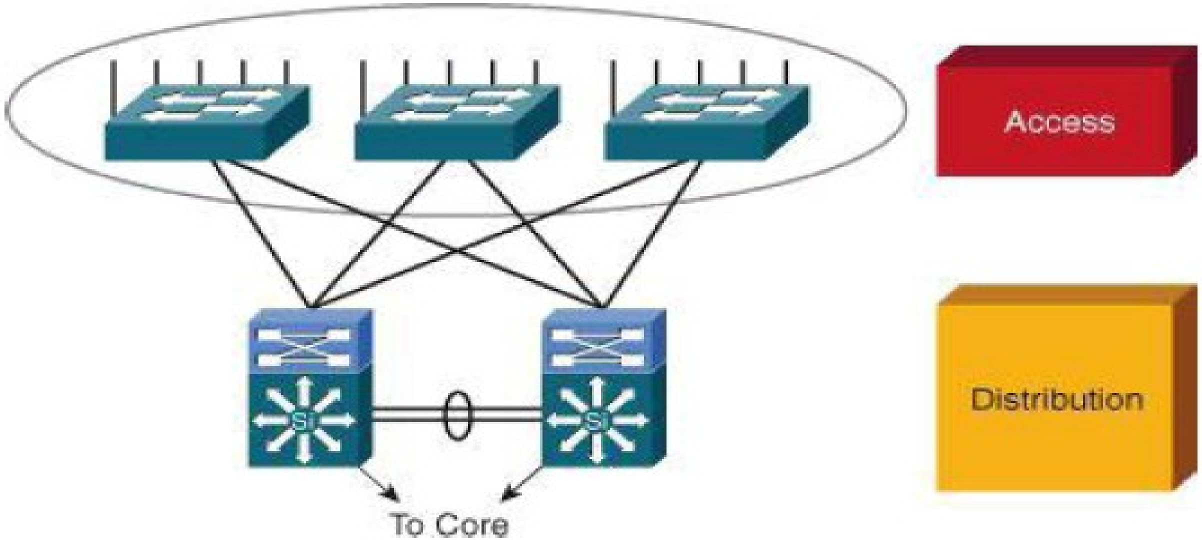
Network Modules (1)

- Campus
  - Operating center of an enterprise.
  - This module is where most users access the network.
  - Combines a core infrastructure of intelligent switching and routing with mobility, and advanced security.
- Data Center
  - Redundant data centers provide backup and application replication.
  - Network and devices offer server and application load balancing to maximize performance.
  - Allows the enterprise to scale without major changes to the infrastructure.
  - Can be located either at the campus as a server farm and/or at a remote facility.
- Branch
  - Allows enterprises to extend head-office applications and services to remote locations and users or to a small group of branches.
  - Provides secure access to voice, mission-critical data, and video applications.
  - Should provide a robust architecture with high levels of resilience for all the branch offices.

Network Modules (2)

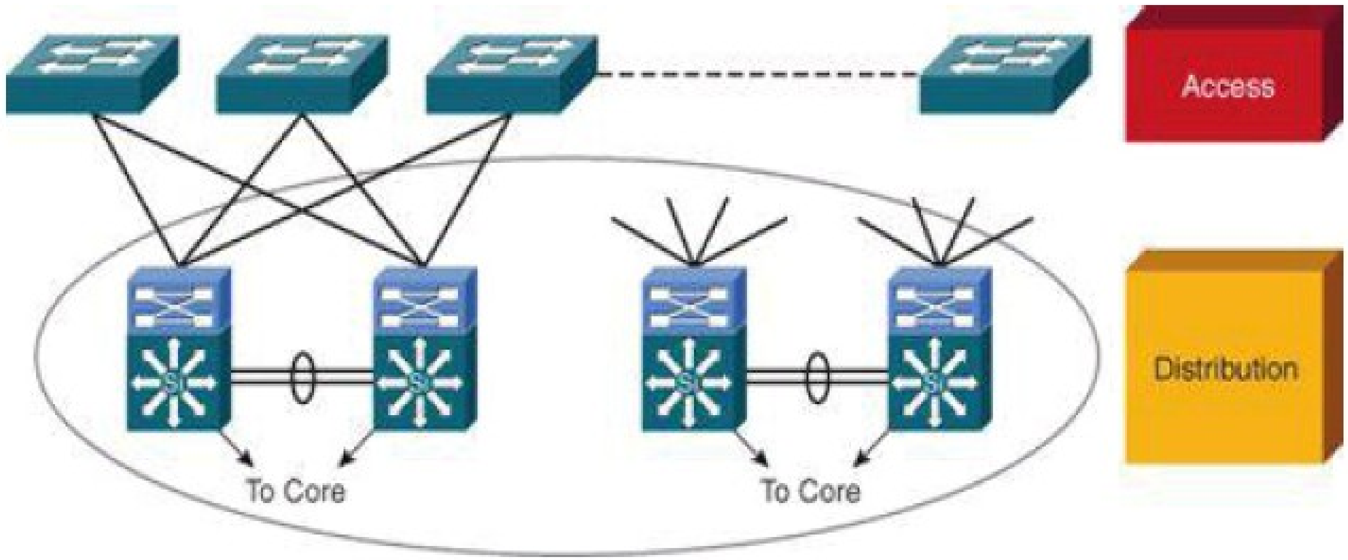
- WAN and MAN
  - Offers the convergence of voice, video, and data services.
  - Enables the enterprise a cost-effectively presence in large geographic areas.
  - QoS, granular service levels, and comprehensive encryption options help ensure the secure delivery to all sites.
  - Security is provided with multiservice VPNs (IPsec and MPLS) over Layer 2 or Layer 3 communications.
- Remote User
  - Allows enterprises to securely deliver voice and data services to a remote small office/home office (SOHO) over a standard broadband access service.
  - Allows a secure log in to the network over a VPN and access to authorized applications and services.

Designing the Access Layer



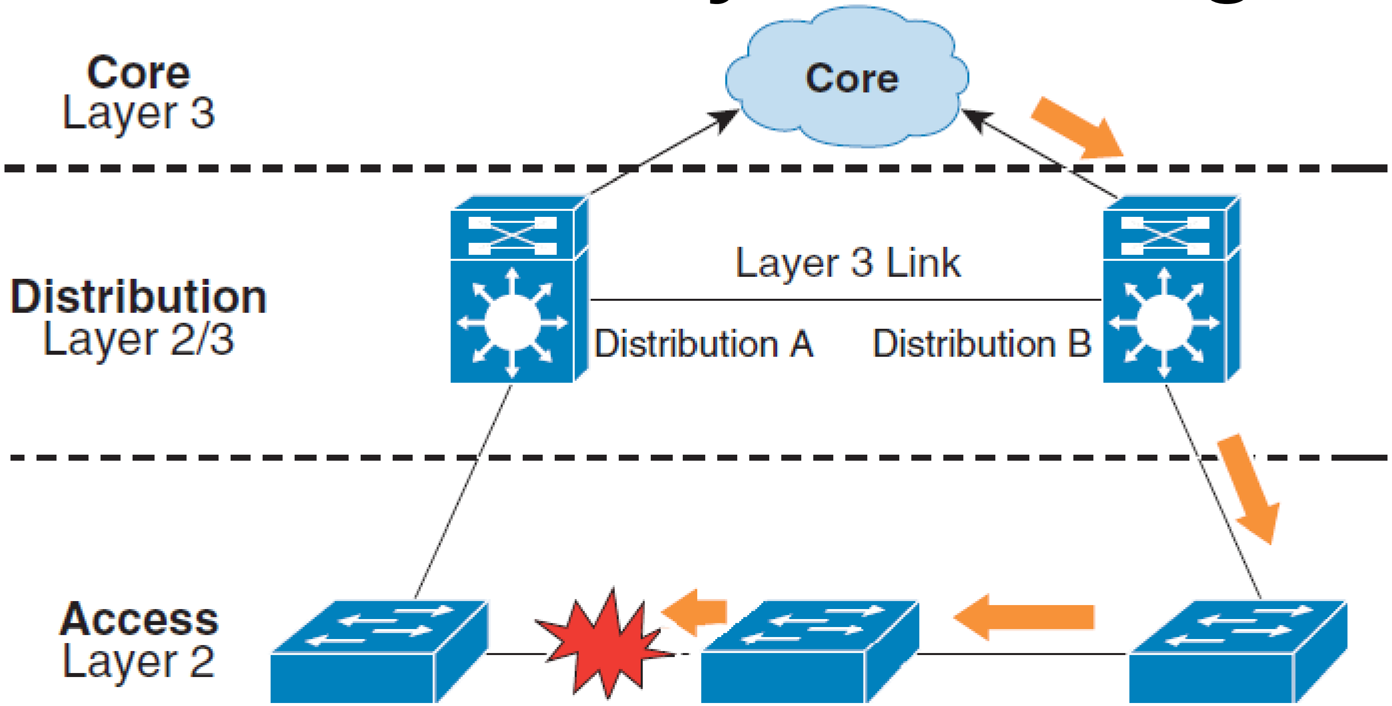
- High availability
  - Default gateway redundancy using multiple connections from access switches to redundant distribution layer switches.
  - Redundant power supplies.
- Other considerations
  - Convergence: the access layer should provide seamless convergence of voice into data network and providing roaming wireless LAN (WLAN).
  - Security: for additional security against unauthorized access to the network, the access layer should provide tools such as IEEE 802.1X, port security, DHCP snooping and dynamic ARP inspection (DAI).
  - Quality of service (QoS): The access layer should allow prioritization of critical network traffic using traffic classification and queuing as close to the ingress of the network as possible.
  - IP multicast: the access layer should support efficient network and bandwidth management using features such as Internet Group Management Protocol (IGMP) snooping.

Designing the Distribution Layer



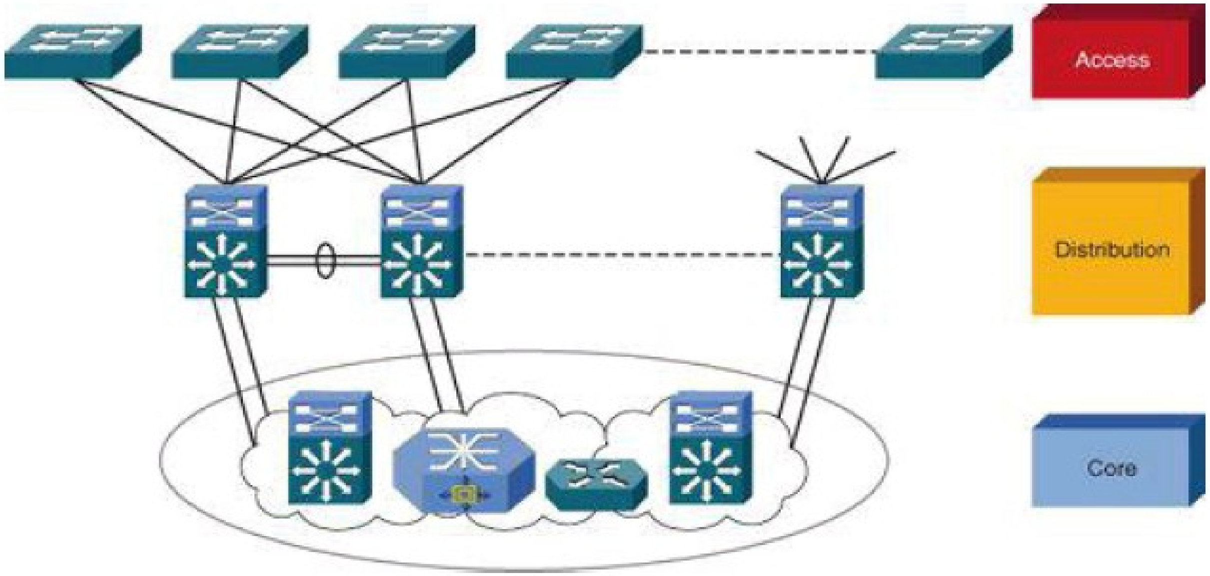
- Uses a combination of Layer 2 and multilayer switching to segment workgroups and isolate network problems, preventing them from impacting the core layer.
- Connects network services to the access layer and implements QoS, security, traffic loading balancing, and implements routing policies.
- Major design concerns: high availability, load balancing, QoS, and provisioning.
- In some networks, offers a default route to access layer routers and runs dynamic routing protocols when communicating with core routers.
- The distribution layer it is usually used to terminate VLANs from access layer switches.
- To further improve routing protocol performance, summarizes routes from the access layer.
- To implement policy-based connectivity, performs tasks such as controlled routing and filtering and QoS.

Avoid Daisy Chaining



- When using a L3 link between Distribution layer switches
  - In Access layer, any path from a switch should not require another switch from the Access layer.
  - In Distribution layer, any path between Distribution layer switches should not require a switch from the Access layer.
- When using a L2 link between Distribution layer switches
  - Daisy chain is acceptable, however
    - Could overload some Access layer switches.
    - Could increase STP convergence in case of failure.

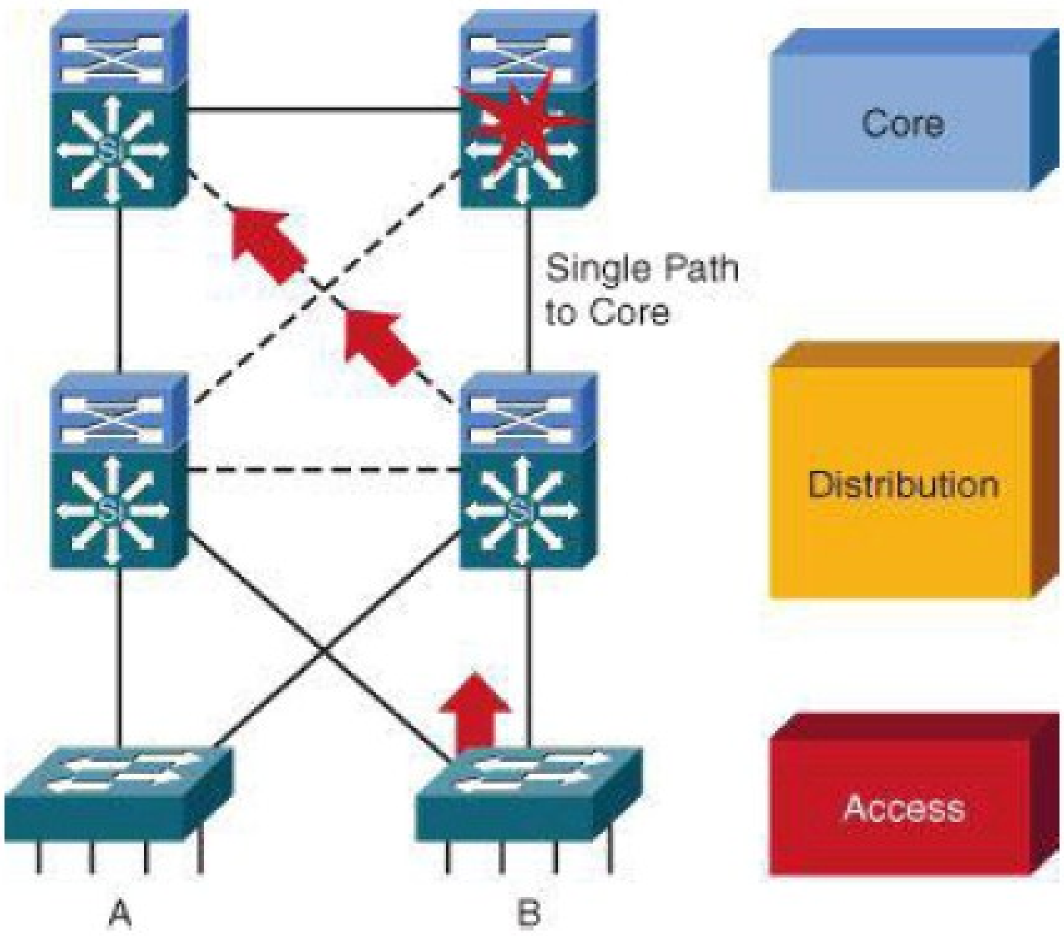
Designing the Core Layer



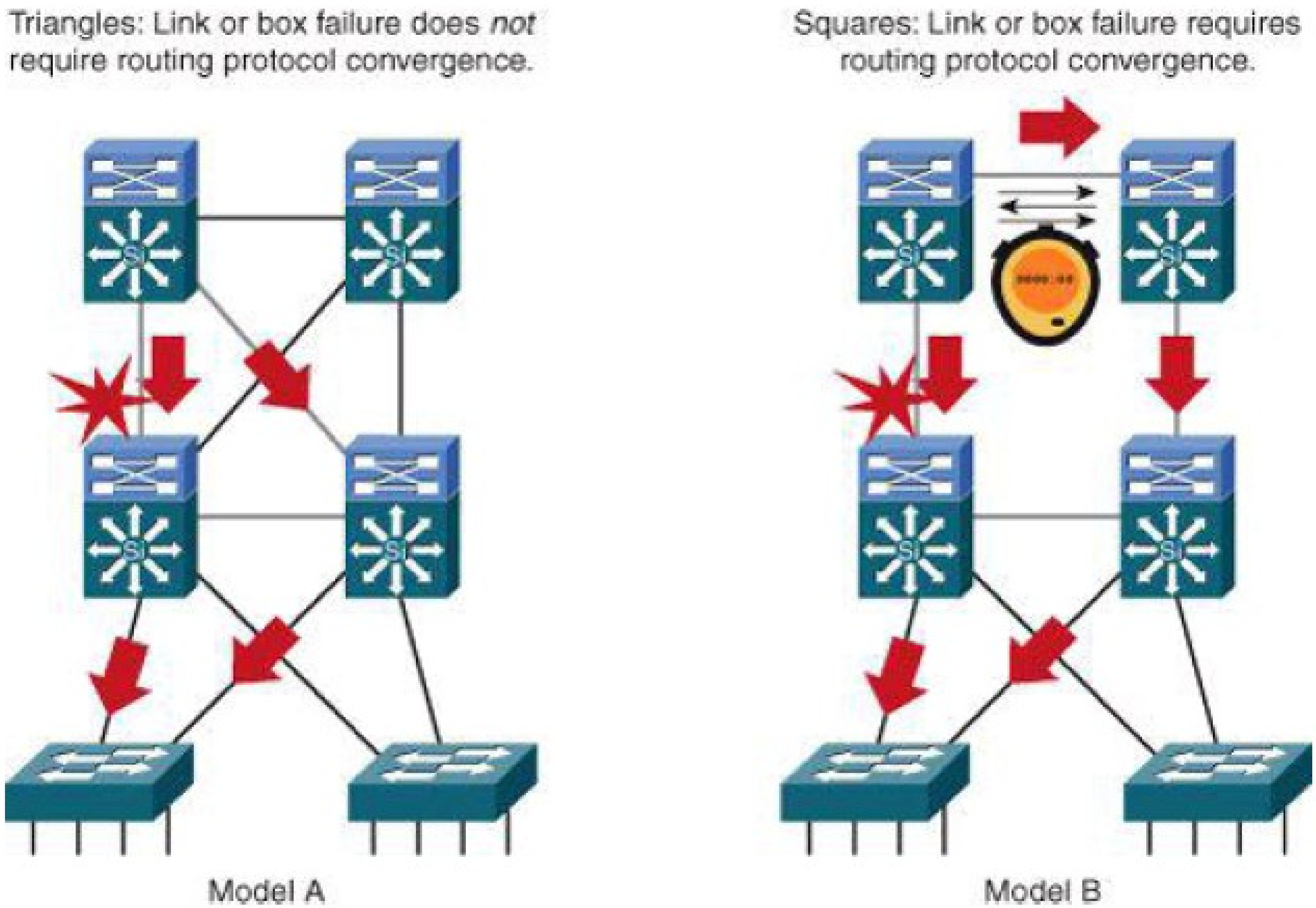
- Backbone for campus connectivity and is the aggregation point for the other layers.
- Should provide scalability, high availability, and fast convergence to the network.
  - The core layer should scale easily.
  - High-speed environment that should use hardware-acceleration, if possible.
  - The core should provide a high level of redundancy and adapt to changes quickly.
    - Core devices should be more reliable
    - Accommodate failures by rerouting traffic and respond quickly to changes in the network topology.
  - Implements scalable protocols and technologies.
  - Provides alternate paths and load balancing.
  - Packet manipulation should be avoided, such as checking access lists and filtering, which could slow down the switching of packets.
- Not all campus implementations require a campus core.
- The core and distribution layer functions can be combined at the distribution layer for a smaller campus.

Provide Alternate Paths

- An additional link providing an alternate path to a second core switch from each distribution switch offers redundancy to support a single link or node failure.

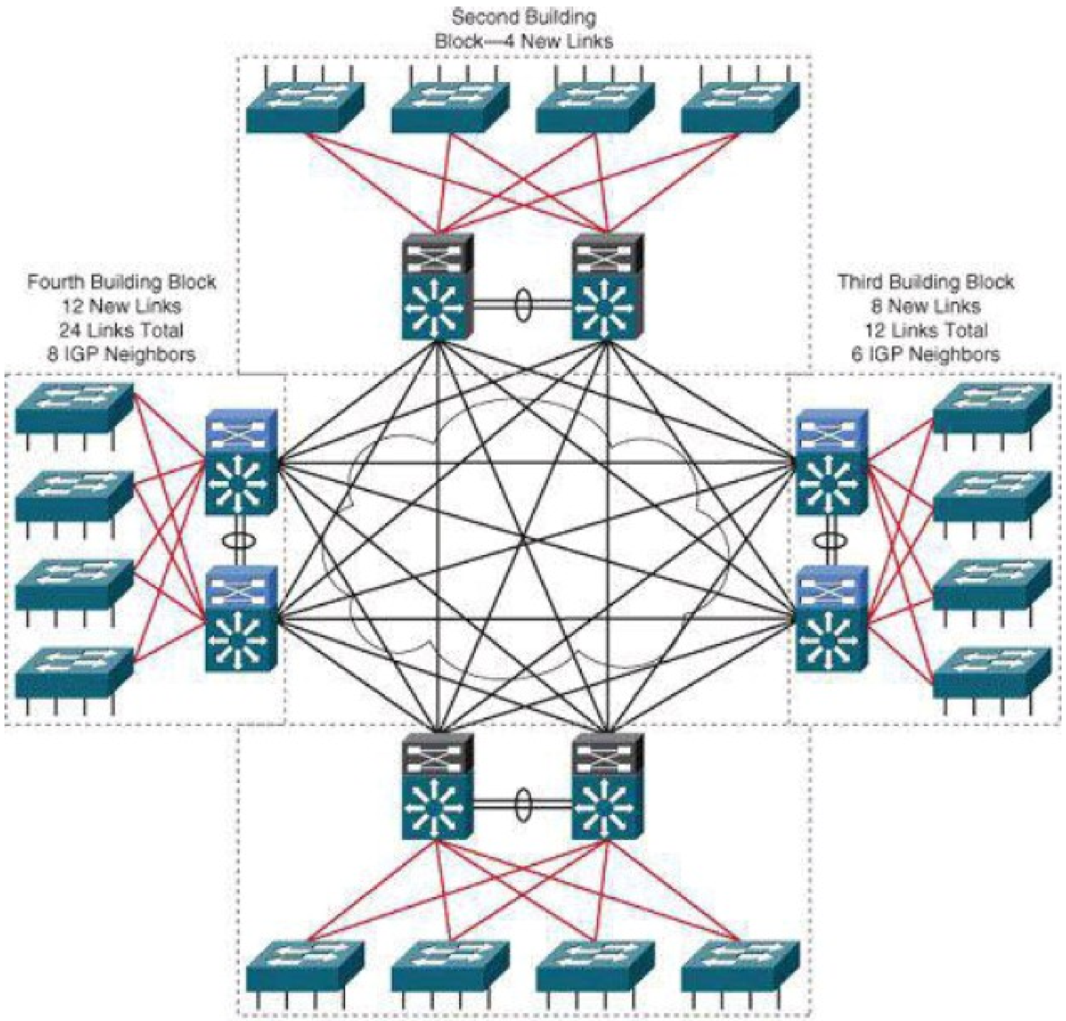


Core Redundant Triangles

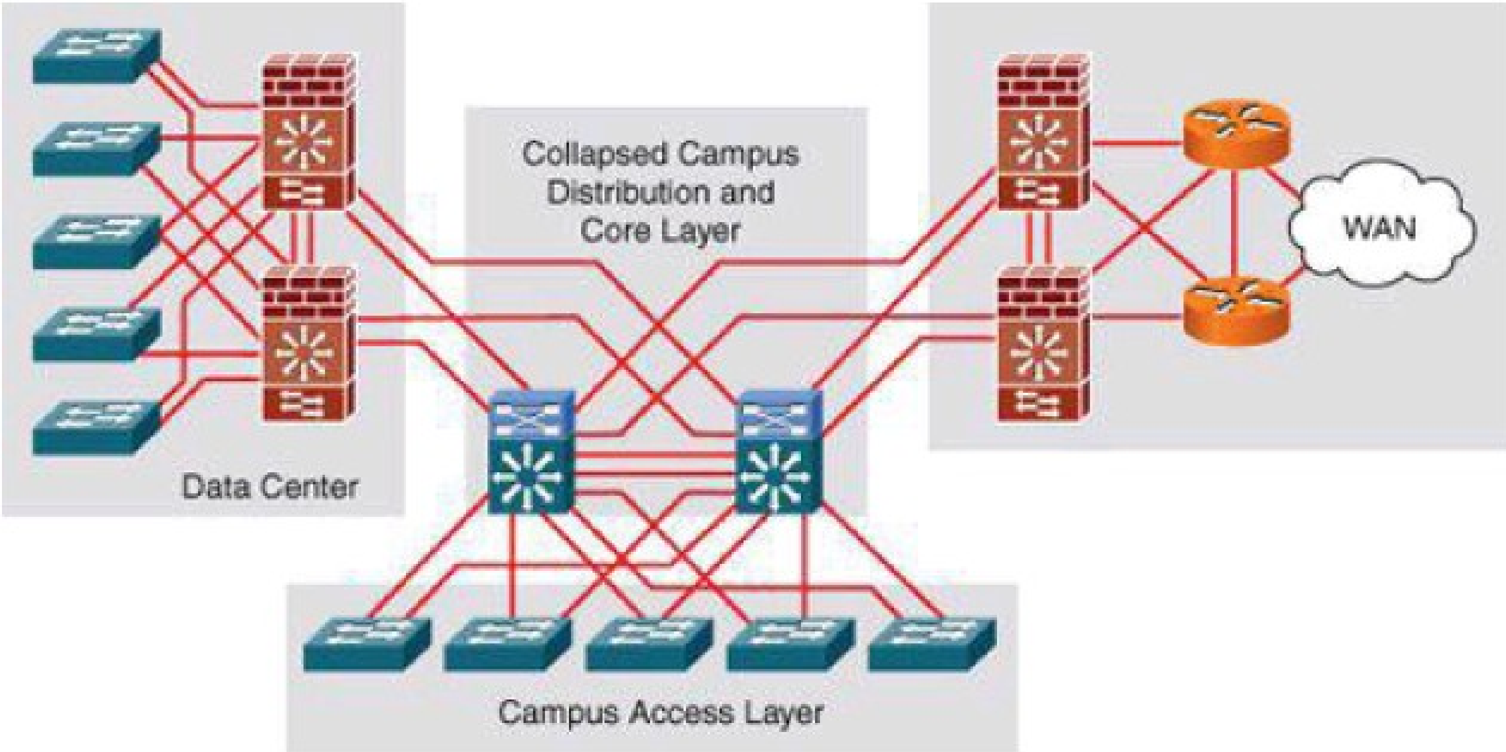


Without a Core Layer

- The distribution layer switches need to be fully meshed.
- Can be difficult to scale.
- Increases the cabling requirements.
- Routing complexity of a full-mesh design increases as new neighbors are added.
- Can be used in small campus <u>with no perspective of growing</u>.

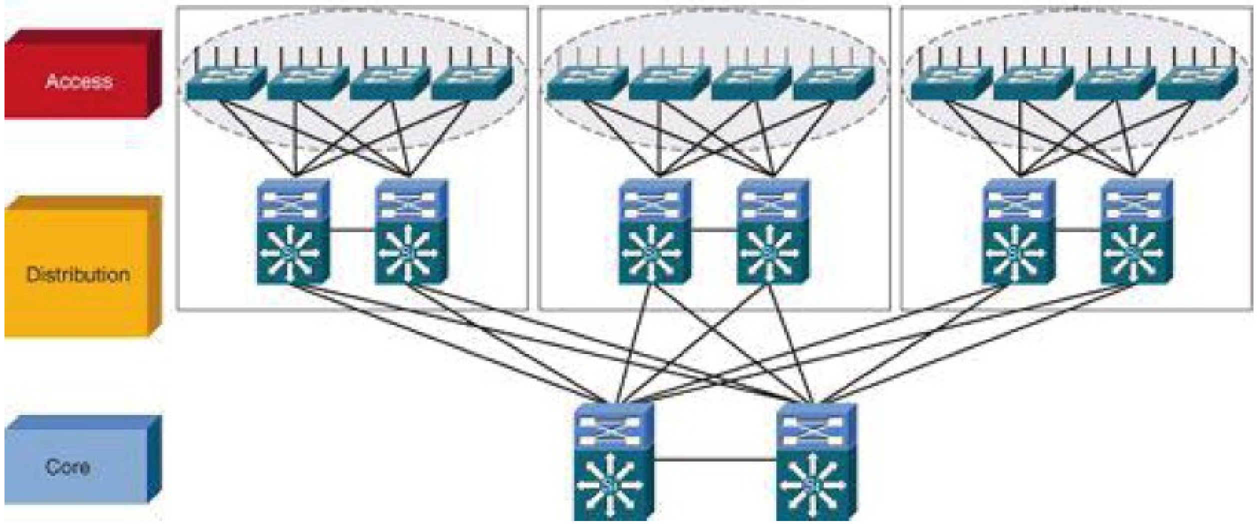


Collapsed Core Layer Architecture



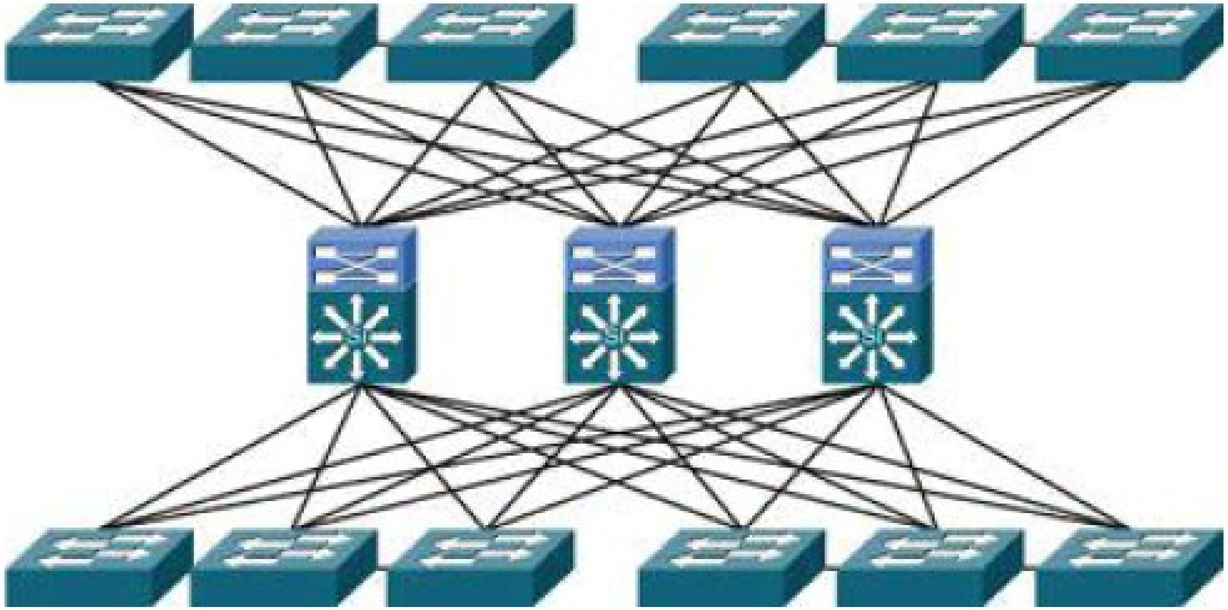
- In smaller networks, the core and the distribution layer can be only one,
  - Eliminates the need for extra switching hardware and simplifies the network implementation.
- However, eliminates the advantages of the multilayer architecture, specifically fault isolation.

Avoid Single Points of Failure



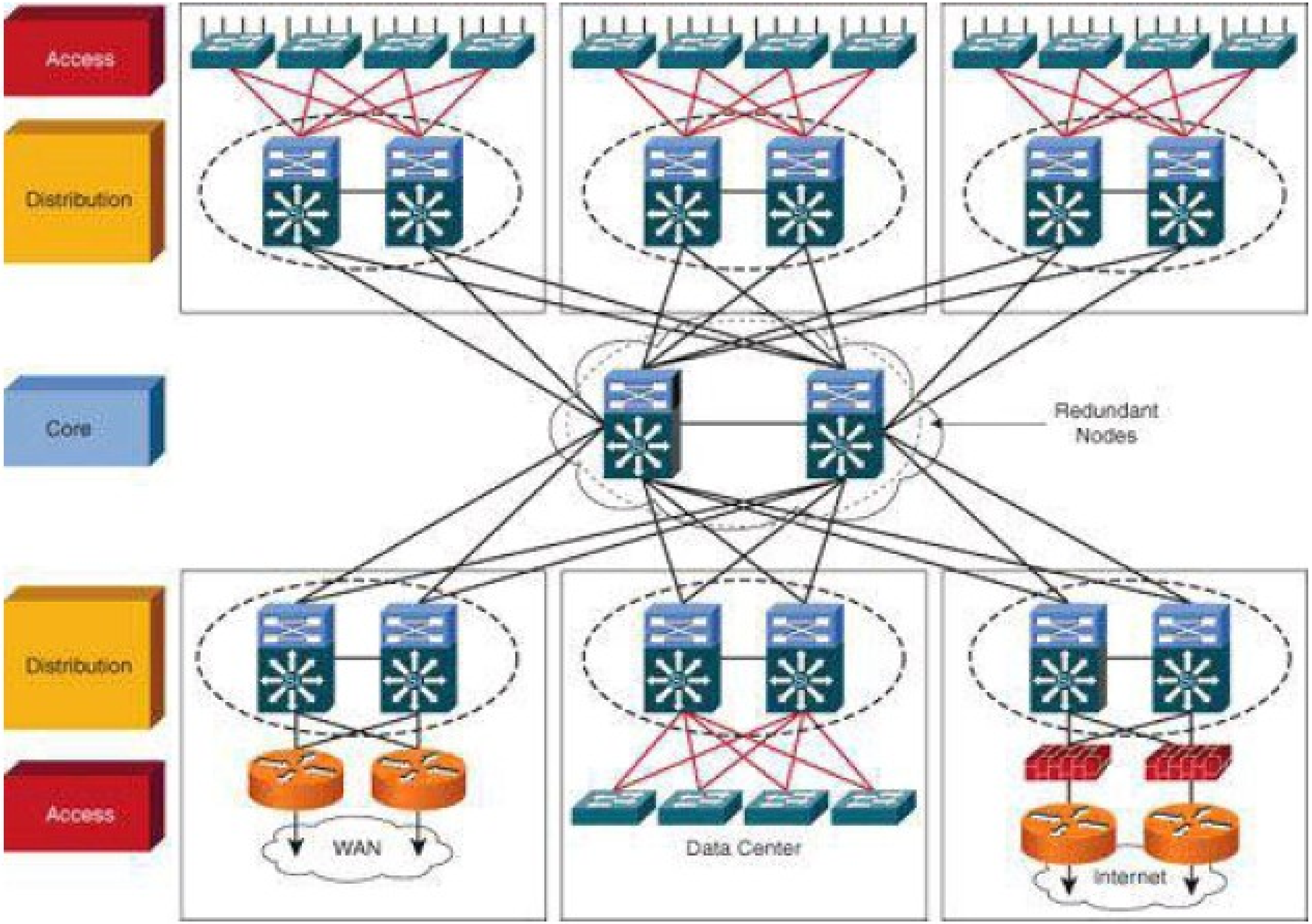
- With an hierarchical design,
  - In Distribution and Core Layers the single points of failure are easy to avoid with redundant links.
    - Don't forget redundant power and cooling!
  - In Access Layer, all L2 switches are single points of failure (only) to the user connected to them,
    - Solution 1, redundant backup hardware activated by a (proprietary) supervision mechanism to “replace” faulty equipment.
      - Copies full configuration and state to backup hardware.
    - Solution 2, have multiple connections between each user terminal and different access switches
      - Requires multiple network cards in user terminals and more plugs/wiring.
      - Cheaper?

Avoid Too Much Redundancy

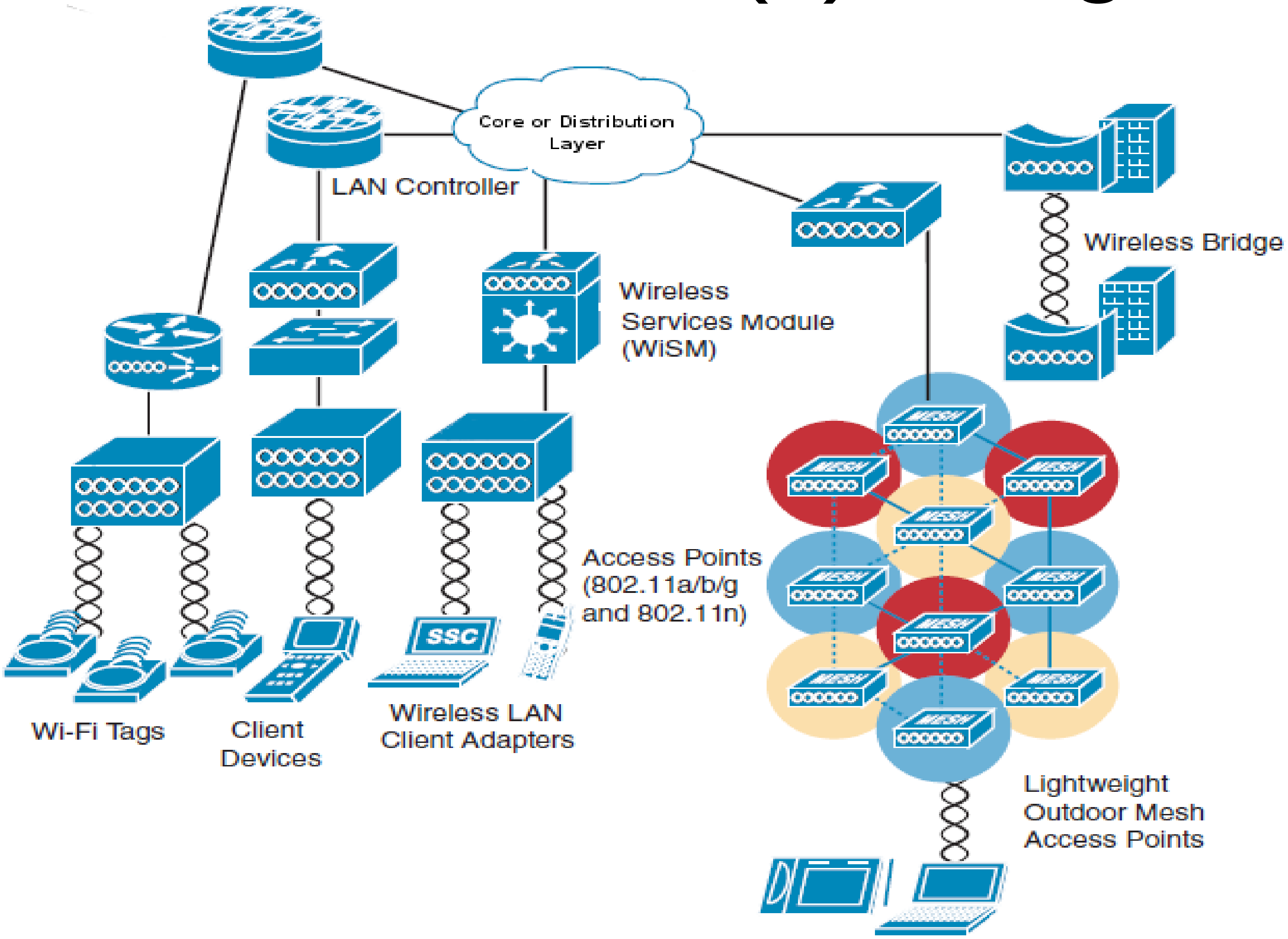


- Increases,
  - Routing complexity
  - Number of ports used
  - Wiring

Optimal Redundancy



Wireless Network(s) Integration



- Wireless networking technologies should have an integration point at core or distribution layers.
- In terms of network architecture a WLAN can be seem as any LAN.
  - Except that we have mobility and must have seamless roaming while moving.
- A large number of AP can be managed by a (Wireless) LAN Controller.

VLANs on Access Points

- AP have trunk ports to distribution/core switches.
- “Wired” VLANs must/can be extended to the wireless domain.
  - e.g., VLAN 30 “Green” and VLAN 10 “Red”.
- Each SSID can be mapped to a VLAN.
  - Different SSID/VLAN can have different security policies.
- Wireless VLANs should be configured as end-to-end.
  - Mobility and AP roaming should not break Layer 3 connectivity.
  - IP address should be the same → same VLAN with campus.
- A Native VLAN is required to provide management capability and client authentications.
  - Never extended to the wireless domain!!
    - e.g., VLAN 1.

Datacenter CLOS Topology

- With large-scale data center deployments, three-tier topologies have become scale bottlenecks.
- The classic three-tier topology evolved to a CLOS topology.
  - Original designed by Charles Clos in 1950 to find a more efficient way to handle telephonic call transfers.
- Eliminating the need for STP the network evolved to greater stability and scalability.
- Layer 3 moves to the Access Layer.
- Usually called Spine-and-Leaf Architecture.