

Enterprise Network Design Topics

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 tradeoff between available budget and acceptable risk.
- Network should have **Flexibility**
 - Businesses change and evolve.
 - Network should adapt quickly.

Equipments

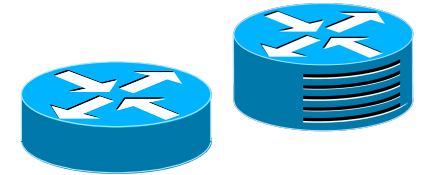
- Switch

- OSI Layer 2 inter-connection
- Implements VLAN
- Spanning-tree based routing
 - STP, RSTP, MSTP
- Wireless Access Points



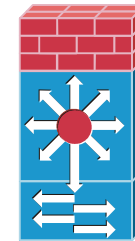
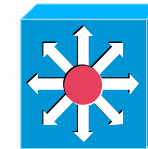
- Router

- OSI Layer 3 inter-connection
- Have extra functionalities like QoS, Security, VPN gateway, network monitoring, etc...



- L3 Switch

- Switch+Router
- Low-end and mid-end range routing functionalities are limited
- High-end have full routing functionalities
- Many have dedicated L2 routing hardware

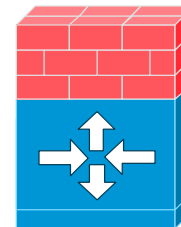
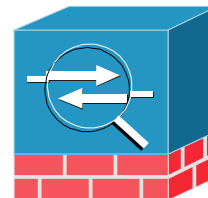


- Router with switching modules

- L3 Switch with full routing capabilities

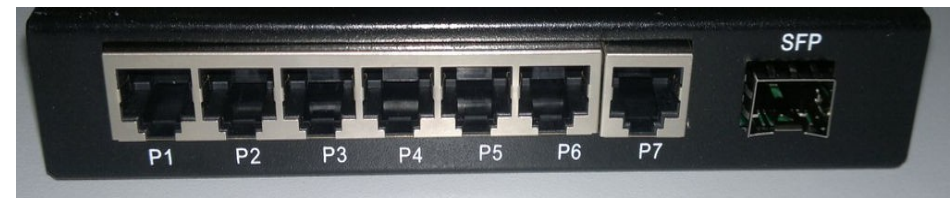
- Security Appliance

- Firewall
- IDS/IPS (Intrusion Detection/Prevention System)
- NAT/PAT
- VPN Gateway
- Services proxy



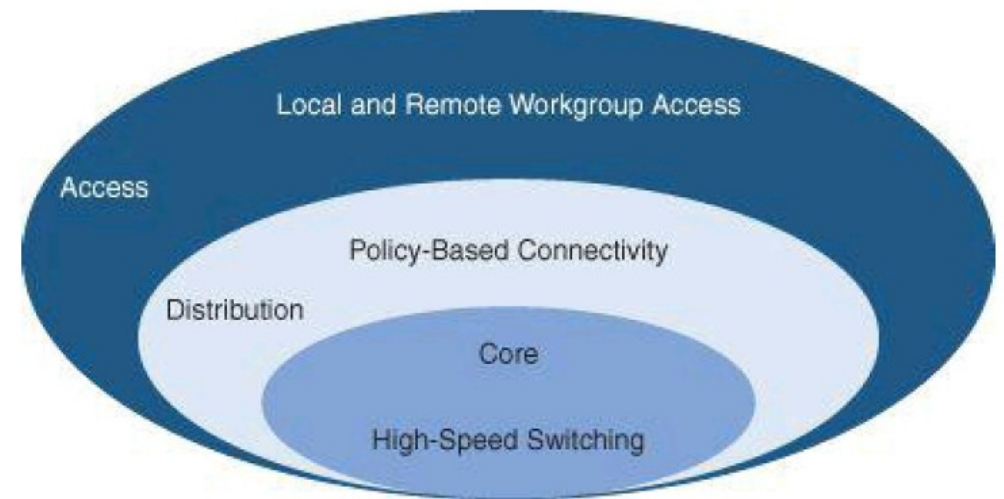
How to Choose the Equipments

- Type
 - L2 Switch, L3 Switch, Router + Switching module, Router, ...
- Manufacturer
 - Reliability
 - (Expected) Maximum MTBF (mean time between failures) as possible.
 - Depends on multiple factors:
 - Hardware/Electronics redundant architectures, inherent quality, environmental constraints, etc...
 - Price
 - Usually (not always), a lower price means lower reliability.
 - Assistance
- Range/Model
 - Processing/Commutation speed
 - Number of bytes/packets processed/commuted per second.
 - Lower than the sum of all ports speed.
 - Software version
 - Supported protocols and functionalities.
 - Determines also memory requirements.
 - Number of ports (and speed of ports)
 - Ethernet (10 Mbps, 100 Mbps, 1Gbps, 10Gbps, ...)
 - Connectors
 - To copper or to fiber.
 - RJ-45, Small form-factor pluggable (SFP), Enhanced small form-factor pluggable (SFP+)
 - With or without PoE (Power over Ethernet)
 - For VoIP phones, Access Points, etc...
- Number of slots
 - For additional port/processing modules.



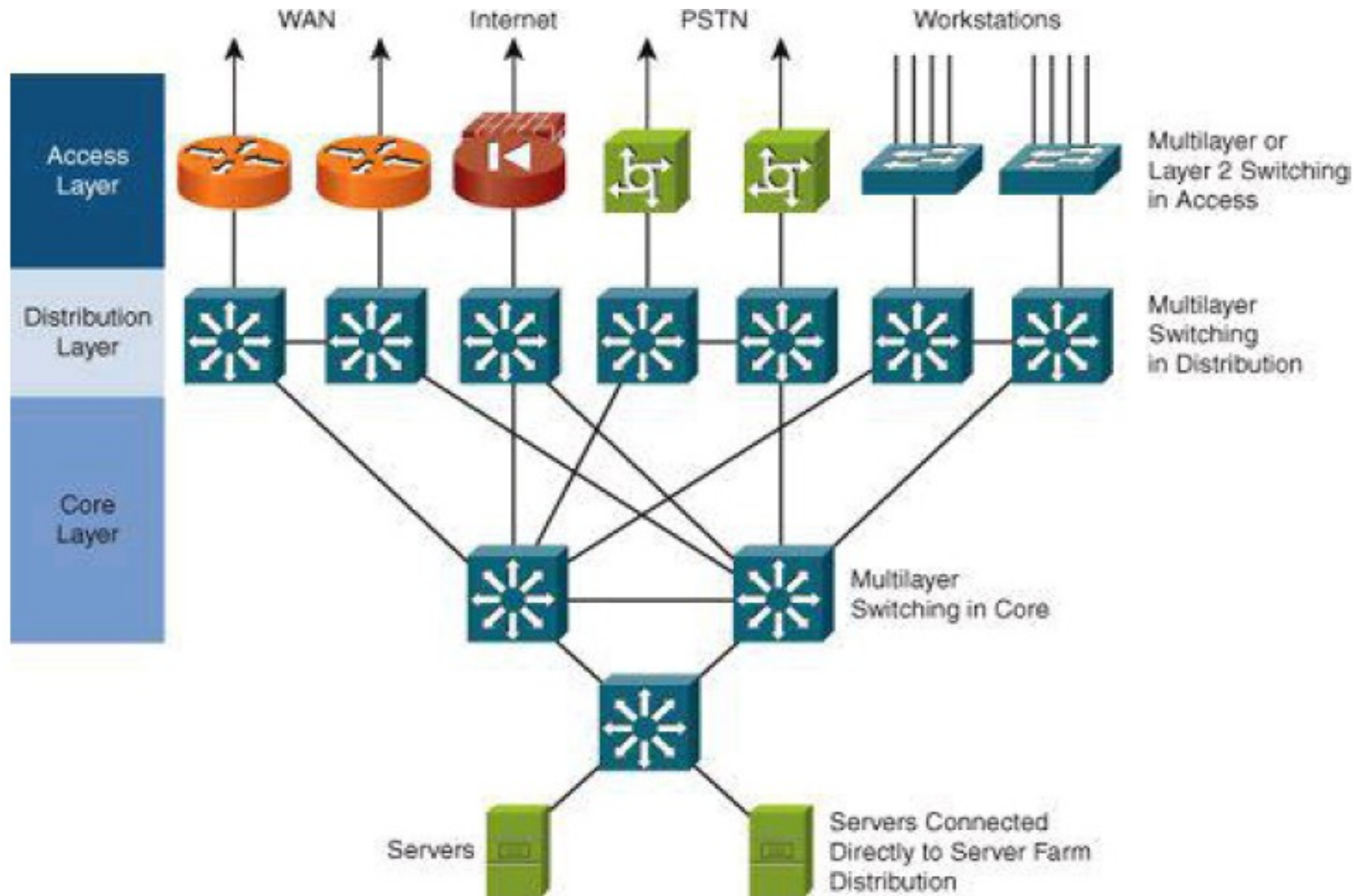
Hierarchical Network Model

Hierarchical Network Model

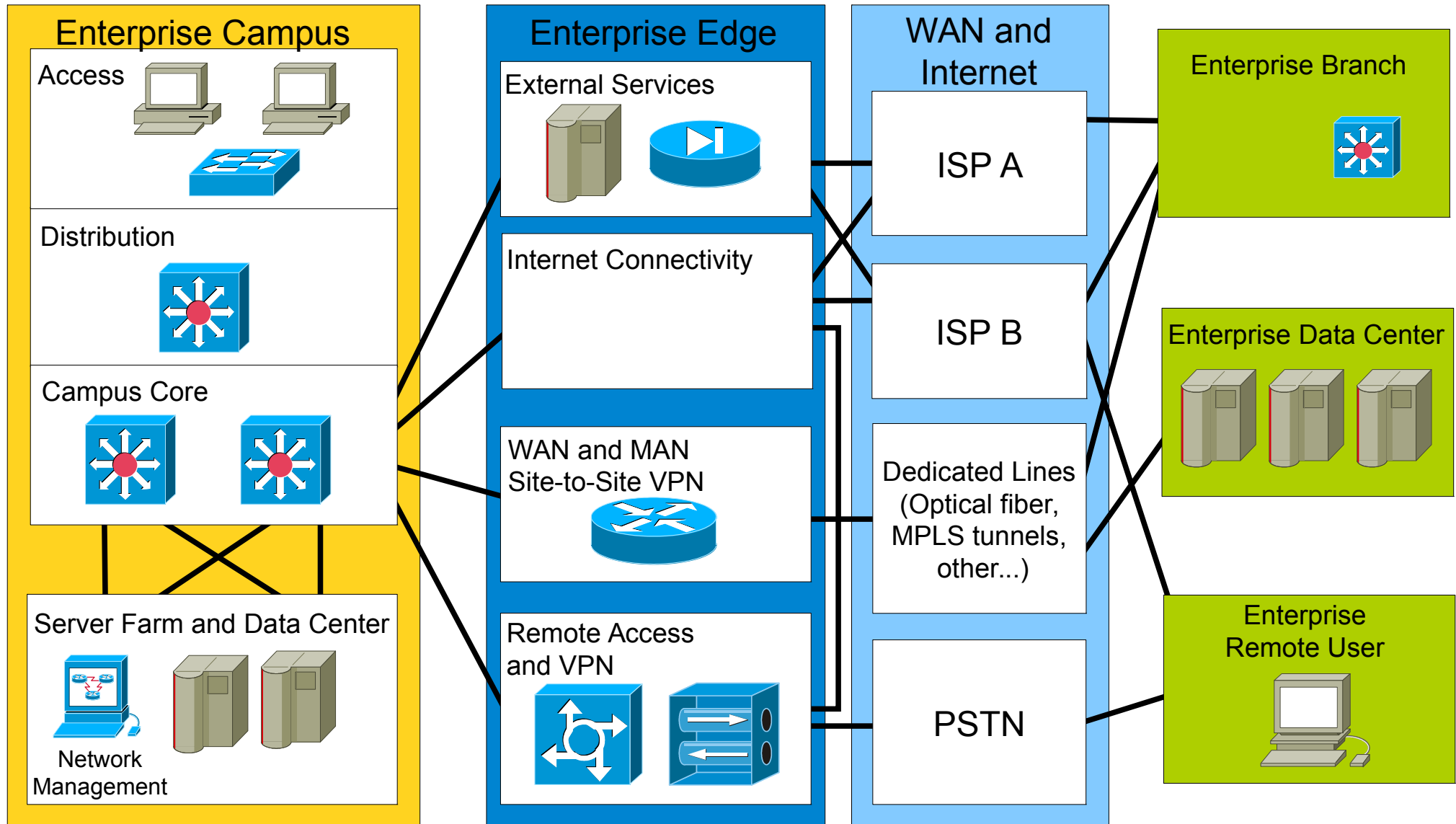


- Access layer
 - Provides user access to network.
 - Generally incorporates switched LAN devices that provide connectivity to workstations, IP phones, servers, and wireless access points.
 - For remote users or remote sites provide an entry to the network across WAN technology.
- Distribution layer
 - 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.

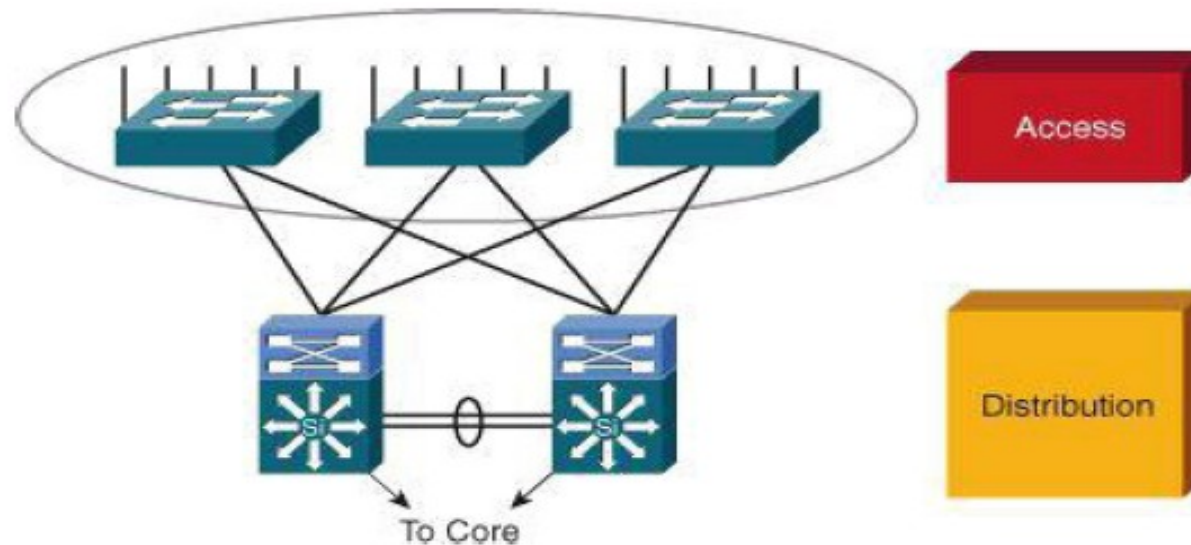
- Branch

- 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)

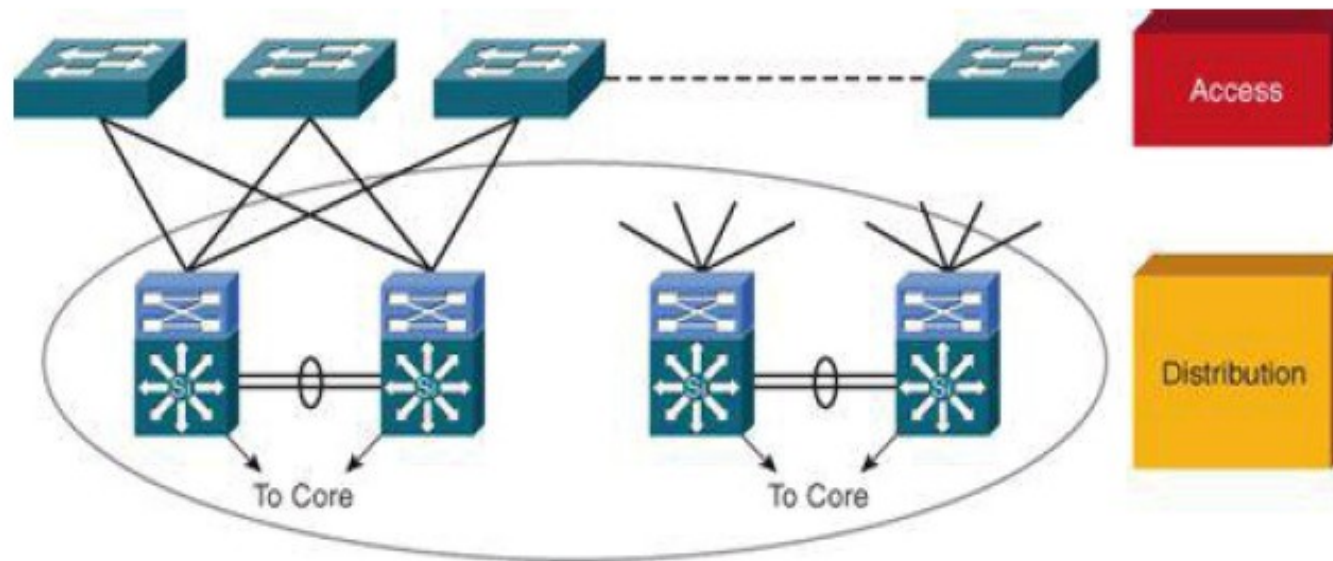
- WAN and MAN
 - Offers the convergence of voice, video, and data services.
 - Enables the enterprise a cost-effectively presence in large geographic areas.
 - QoS, granular service levels, and comprehensive encryption options help ensure the secure delivery to all sites.
 - Security is provided with 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



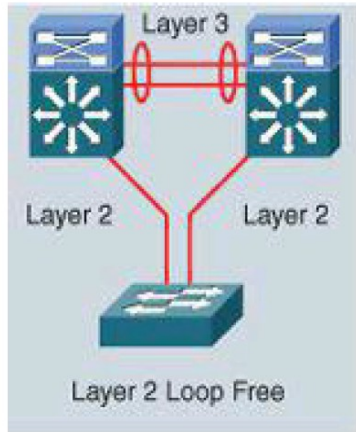
- High availability
 - Default gateway redundancy using multiple connections from access switches to redundant distribution layer switches.
 - Redundant power supplies.
- Other considerations
 - Convergence: the access layer should provide seamless convergence of voice into data network and providing 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.

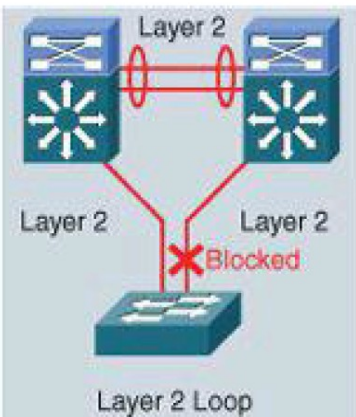
Access-Distribution Block Designs



- Layer 2 loop-free design
 - The links between the access and distribution layers are configured as Layer 2 trunks (inter-switch ports).
 - The link between the distribution switches is configured as a Layer 3 routed link.
 - The Spanning Tree Protocol is not involved in network convergence and load balancing.

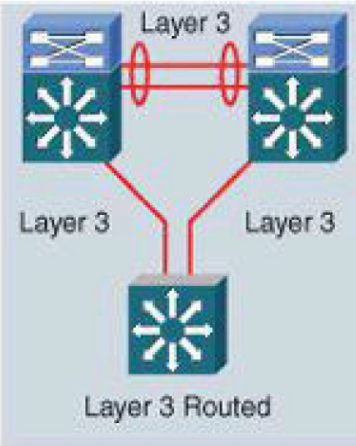
- Layer 2 looped design

- The links between the access and distribution switches are all configured as Layer 2 trunks (inter-switch ports).
 - This configuration introduces a Layer 2 loop between the distribution switches and the access switches. To eliminate this loop from the topology, the Spanning Tree Protocol must be active.
 - A drawback is that network convergence in the case of failure is now dependent on spanning-tree convergence.
 - Another downside is limited load balancing.

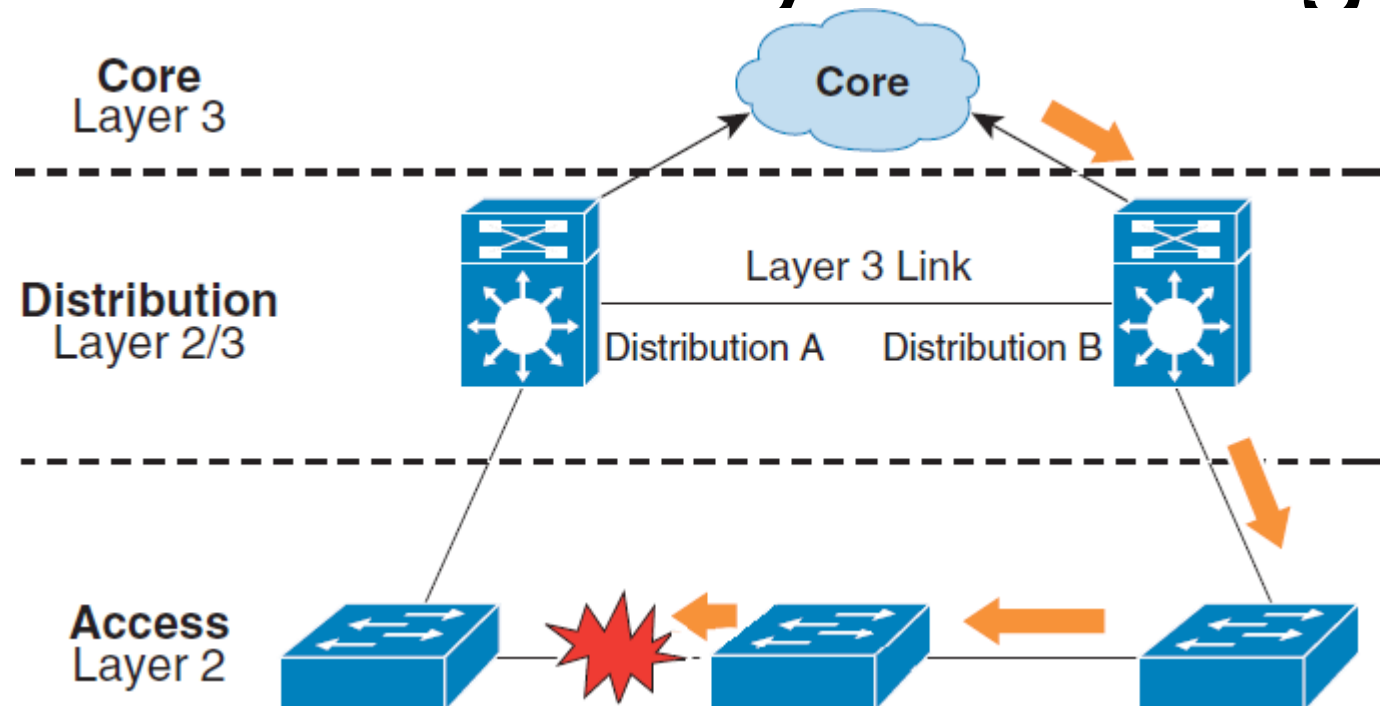


- Layer 3 routed design

- All links between switches are configured as Layer 3 routed links.
 - The advantage of this design is that it eliminates the Spanning Tree Protocol from the inter-switch links.
 - It is still enabled on edge ports to protect against user-induced loops, but it does not play a role in the network re-convergence in the access-distribution block.
 - Network re-convergence behavior is determined solely by the routing protocol being used.
 - The Layer 3 routed design constrains VLANs to a single access switch.
 - It requires more sophisticated hardware for the access switches.

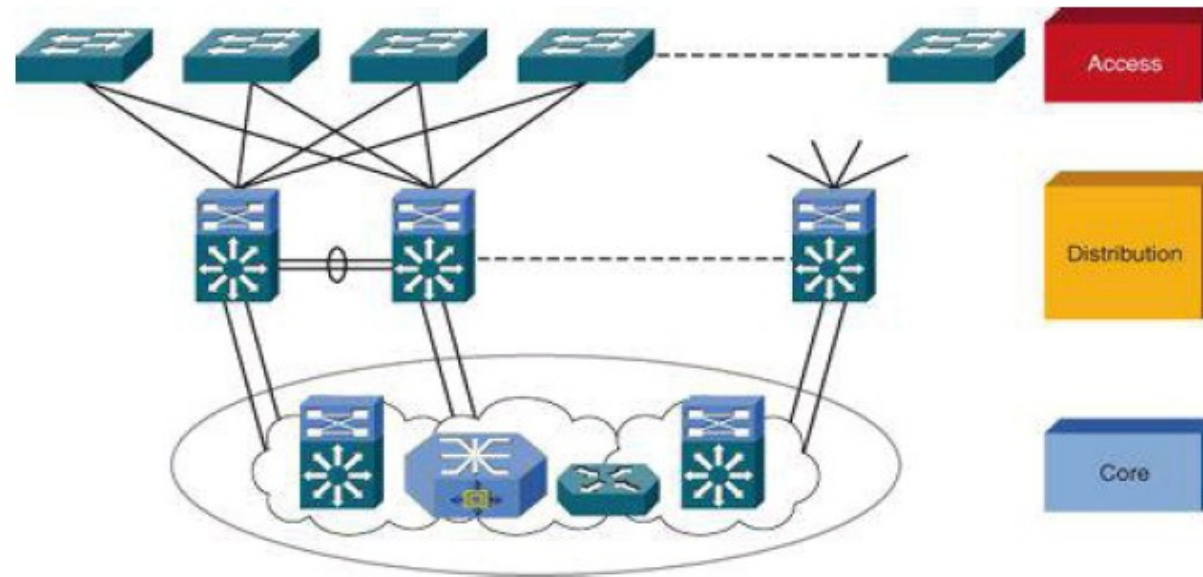


Avoid Daisy Chaining



- 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.

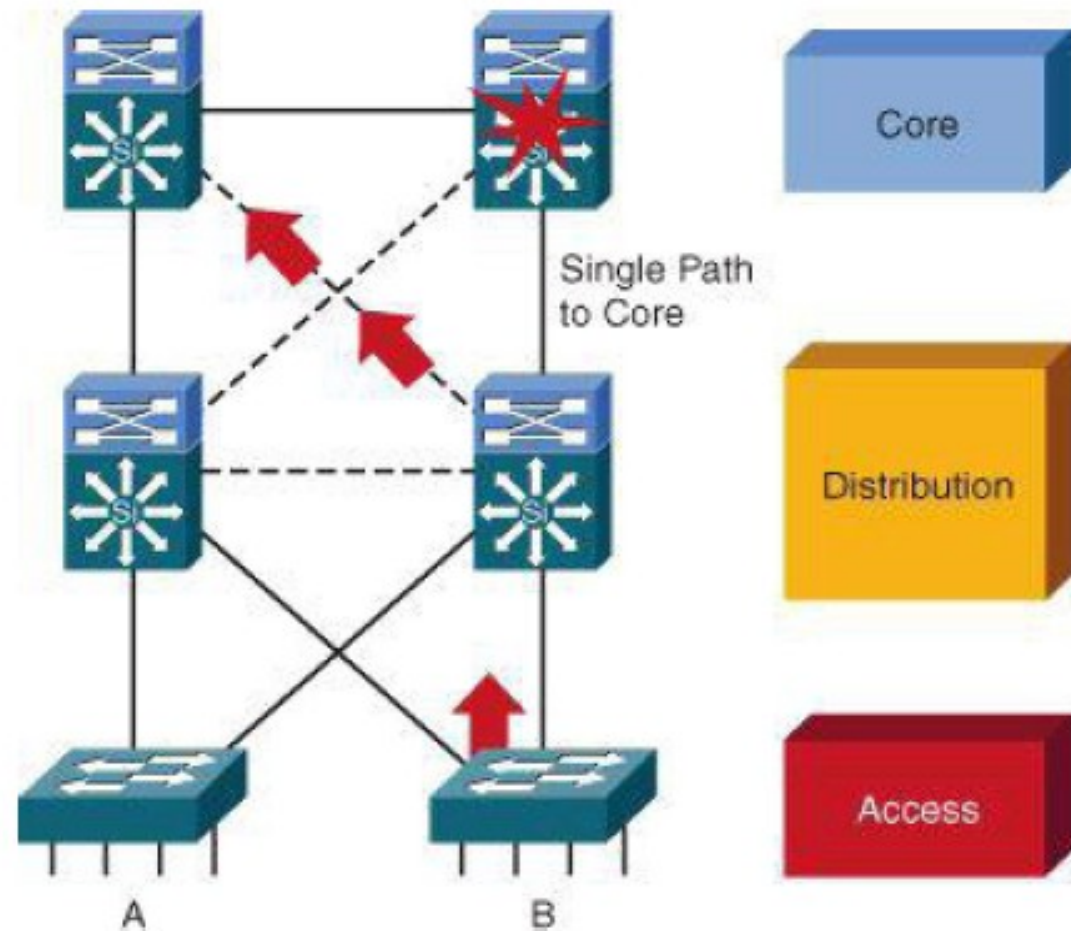
Designing the Core Layer



- 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.

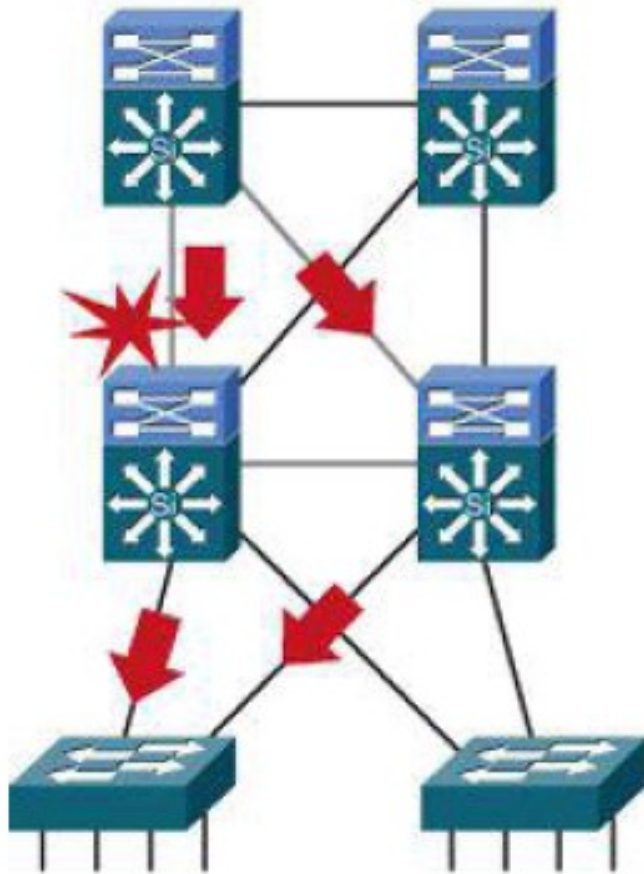
Provide Alternate Paths

- 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.



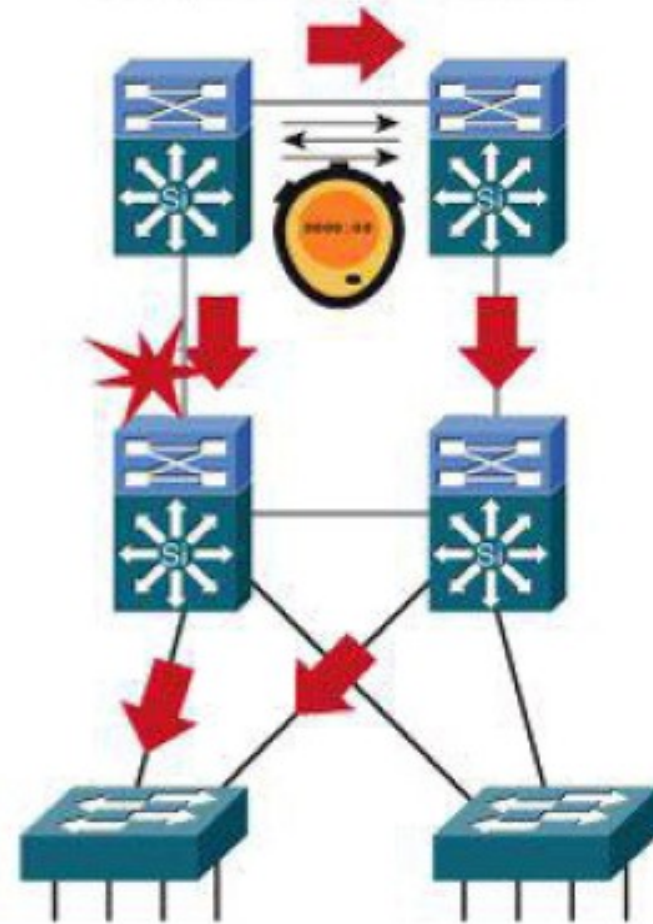
Core Redundant Triangles

Triangles: Link or box failure does *not* require routing protocol convergence.



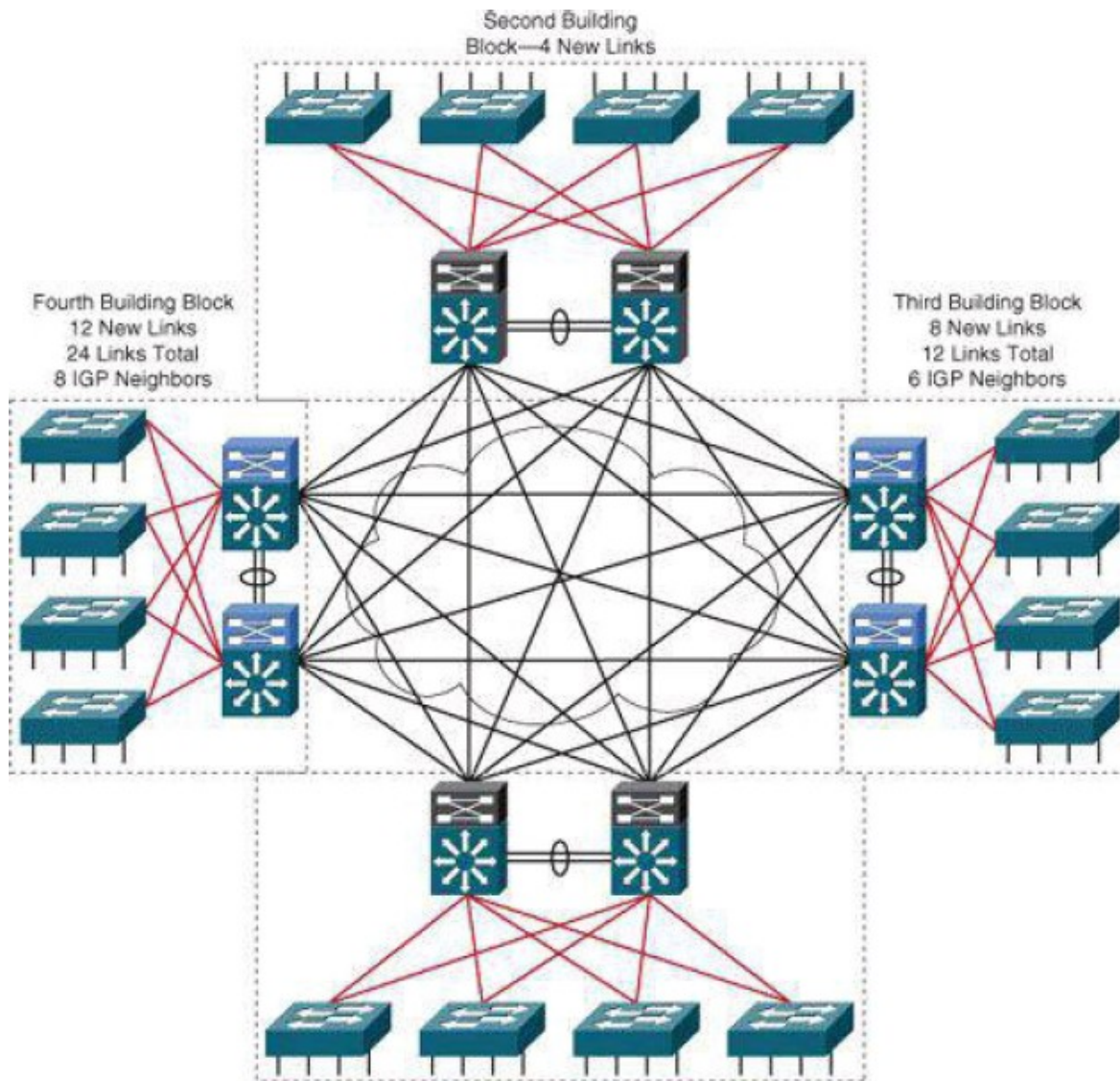
Model A

Squares: Link or box failure requires routing protocol convergence.



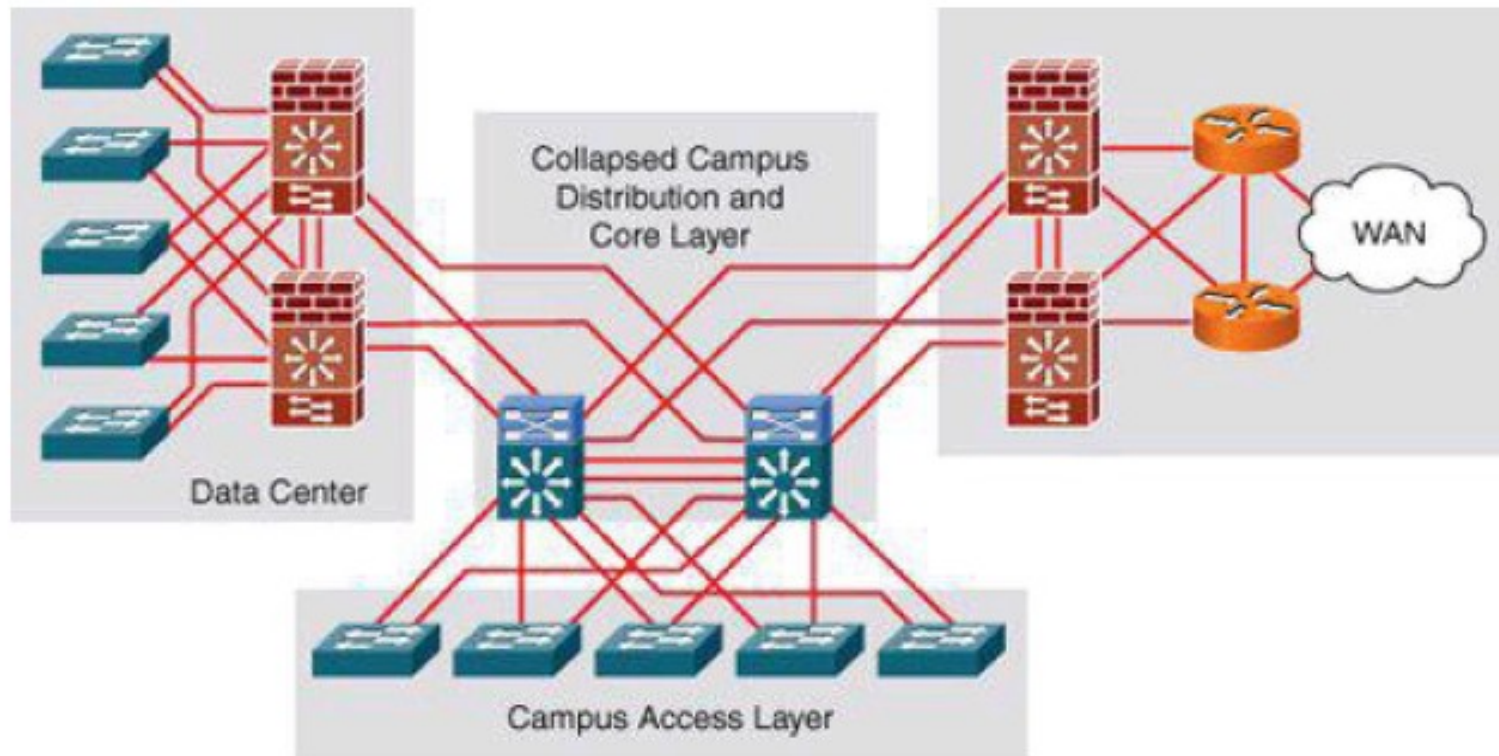
Model B

Without a Core Layer



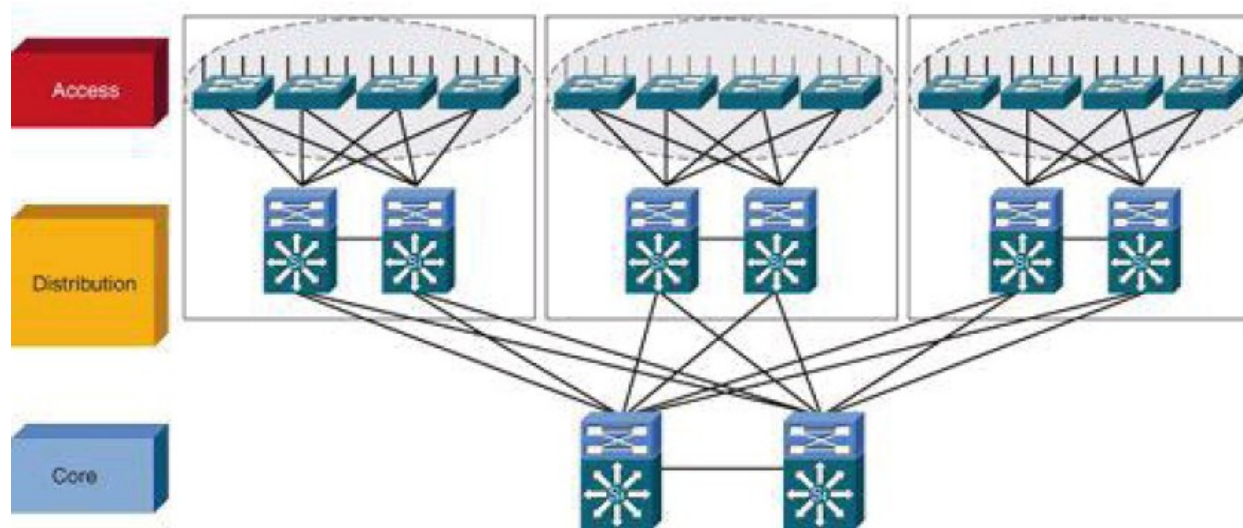
- The distribution layer switches need to be fully meshed.
- Can be difficult to scale.
- Increases the cabling requirements.
- Routing complexity of a full-mesh design increases as new neighbors are added.
- Can be used in small campus with no perspective of growing.

Collapsed Core Layer Architecture



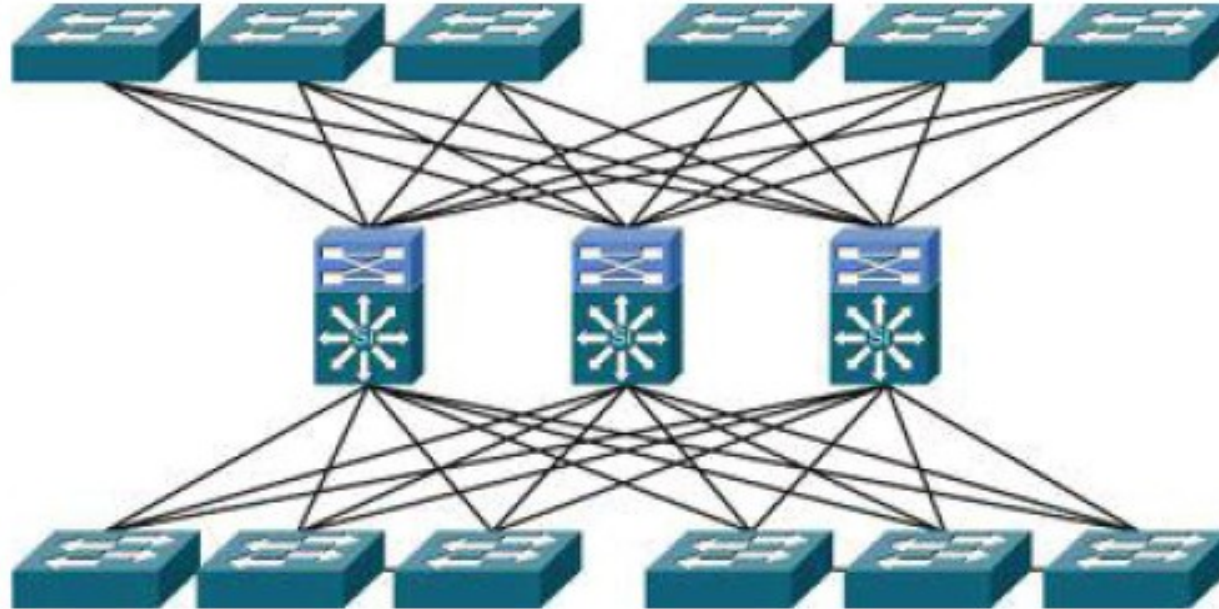
- In smaller networks, the core and the distribution layer can be only one,
 - Eliminates the need for extra switching hardware and simplifies the network implementation.
- However, eliminates the advantages of the multilayer architecture, specifically fault isolation.

Avoid Single Points of Failure



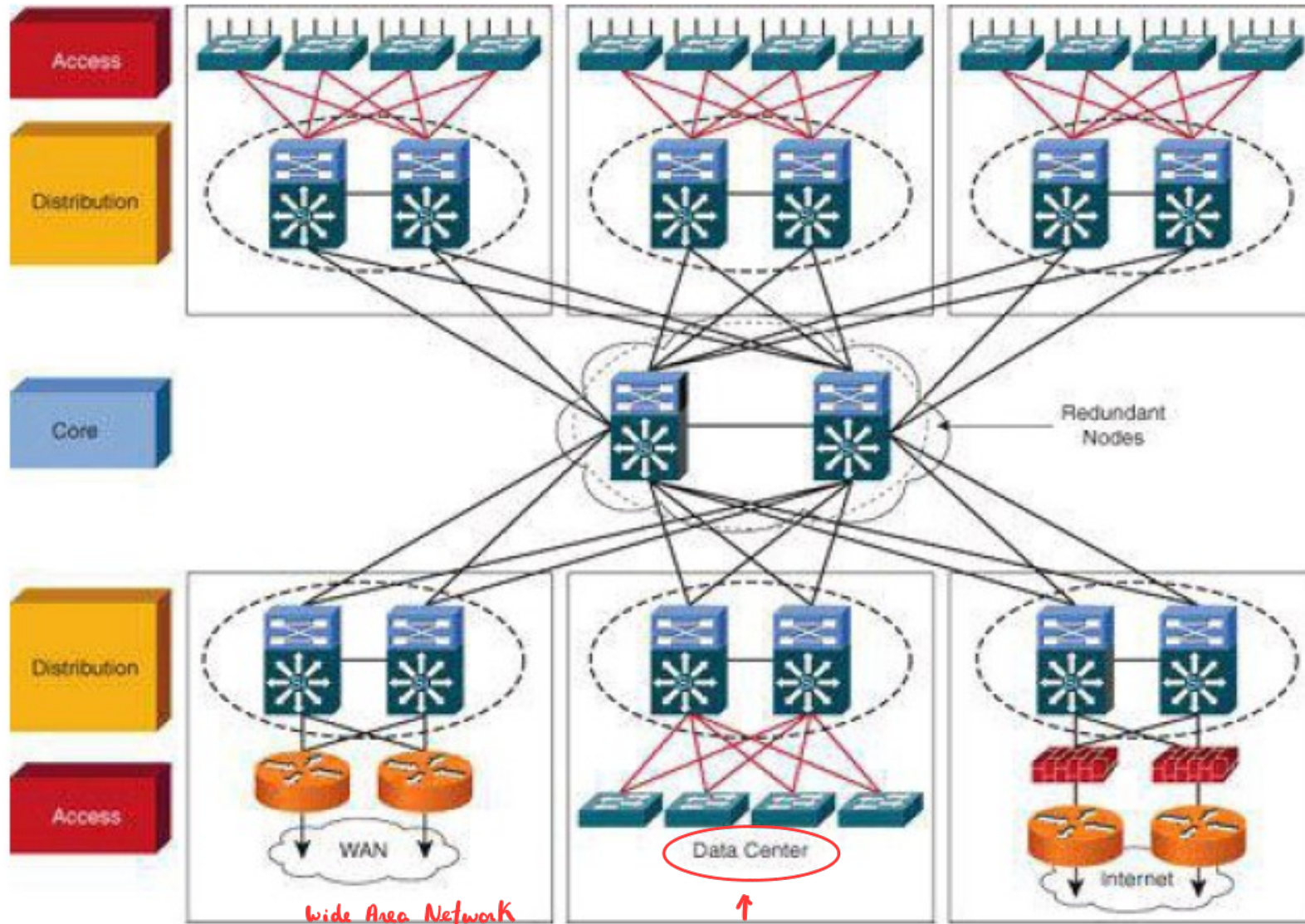
- With an hierarchical design,
 - In Distribution and Core Layers the single points of failure are easy to avoid with redundant links.
 - Don't forget redundant power and cooling!
 - In Access Layer, all L2 switches are single points of failure (only) to the user connected to them,
 - Solution 1, redundant 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



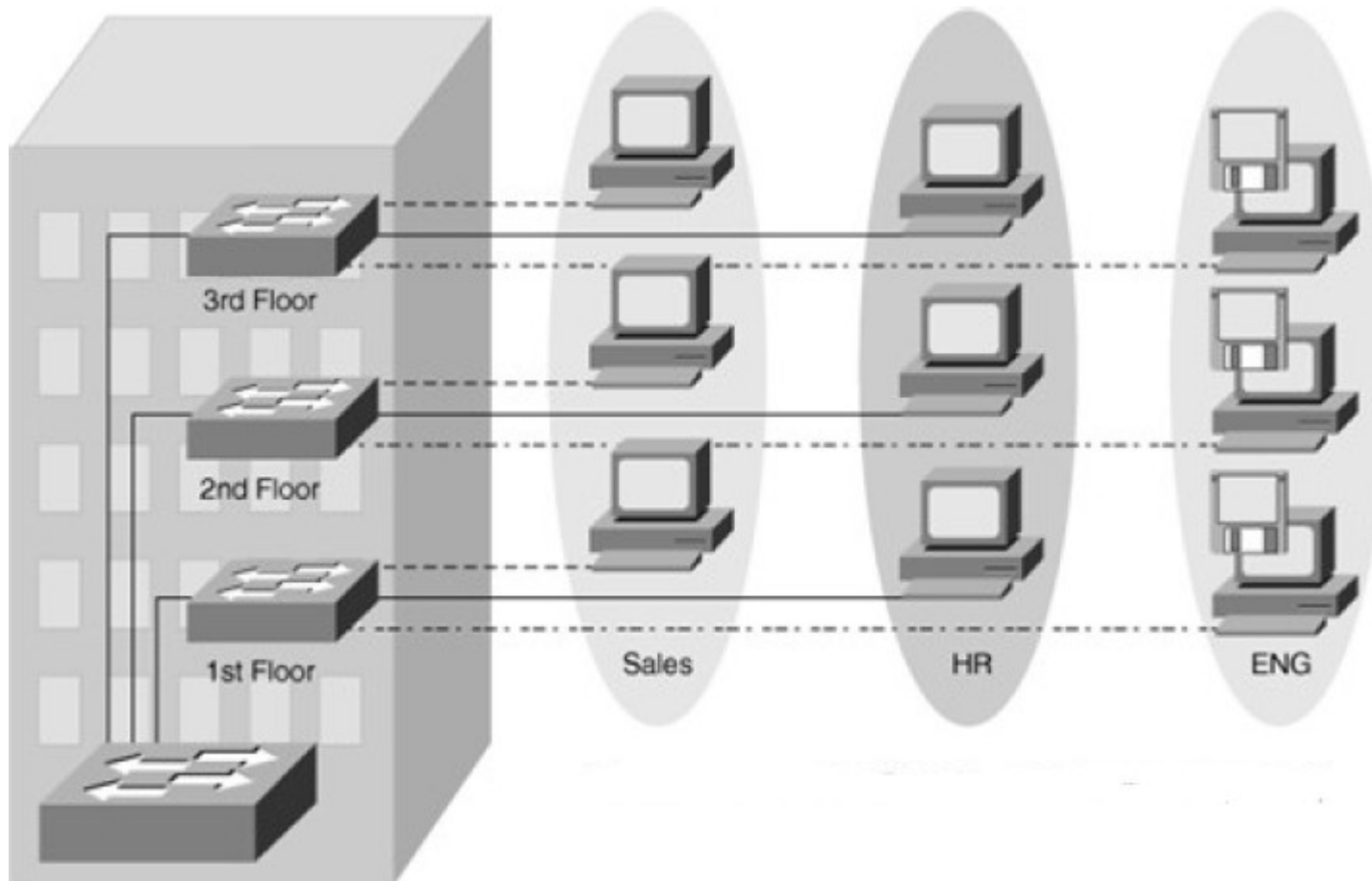
Access Layer Partitions (V)LAN

Virtual LANs

- Group of individual switch ports into switched logical *workgroup*
 - Restrict the broadcast domain to designated VLAN member ports
 - Communication between VLANs requires a router.
- Solves the scalability problems of large flat networks
 - By breaking a single broadcast domain into several smaller broadcast domains.

Implementing VLANs

- VLAN is a logical group of end devices with a common set of requirements independent of their physical location.



VLAN Segmentation Models

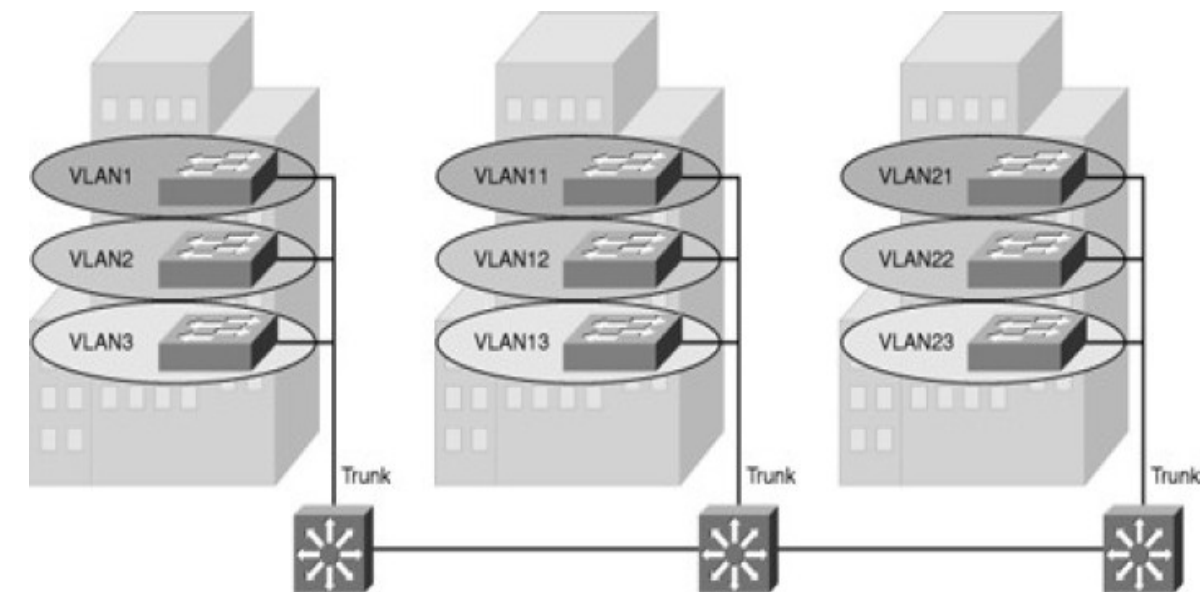
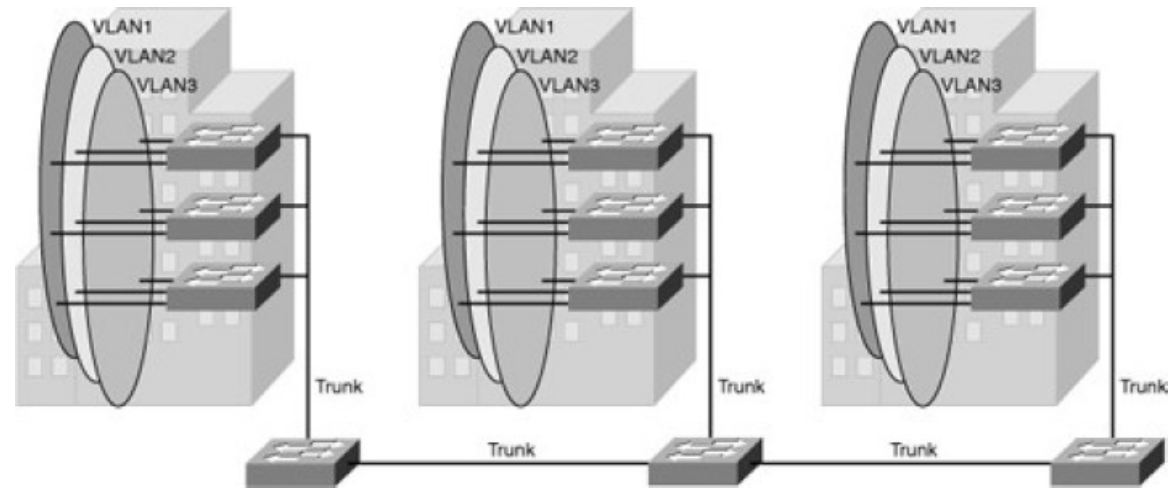
→ mesma VLAN mas longe...

➤ End-to-End VLAN

- VLAN are associated with switch ports widely dispersed over the network

➤ Local VLAN

- Local VLANs are generally confined to a wiring closet.



VLAN Segmentation (examples)

- Local VLANs
 - Per service/function
 - VoIP phones, Video conference, printers, cameras, PCs, servers, ...
 - Per user role
 - Engineers I, engineers II, technicians, administrators, ...
 - Per location
 - Building I, floor 4, right wing, etc...
 - Mixture of service/function, role, location
 - e.g.: VLAN of VoIP phones, of the Engineers in Building I.
- End-to-end VLANs
 - Services/roles that have a global scope within the network.
 - Wireless network
 - Same IP network (same IP address) independently of location.
 - To avoid IP changes when moving from location to location.
 - Administration VLAN (optional)
 - VLAN used by the network administrator to remotely access network equipments.
 - Same administrator of (all) equipments independent of location.

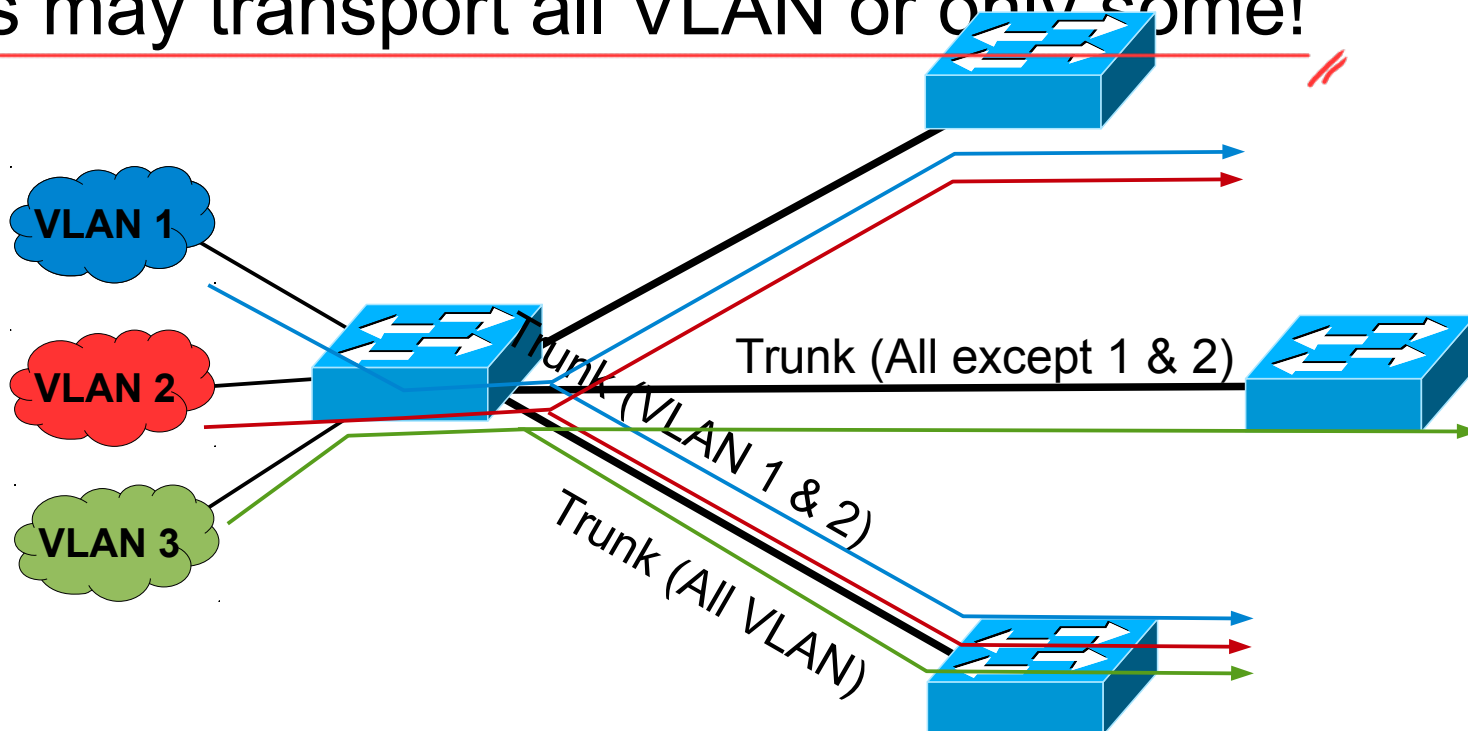
VLAN Segmentation Purpose

- Joint in the same logical network services/terminals/users with same traffic/security/QoS policies.
 - Each VLAN must have an unique IP (sub-)network.
 - May have more than one IP (sub-)network.
 - Including IPv4 public and IPv4 private networks.
 - And, IPv6 networks.
- Neighbor (local) VLANs with similar traffic/security/QoS policies should have IP (sub-)networks that can be summarized/aggregated.
 - E.g.: VLAN of VoIP phones in Building 1 (VLAN 21: 200.0.0.0/24)
 - VLAN of VoIP phones in Building 2 (VLAN 22: 200.0.1.0/24)
 - Summarized/aggregated address of VLAN21+VLAN22: 200.0.0.0/23.

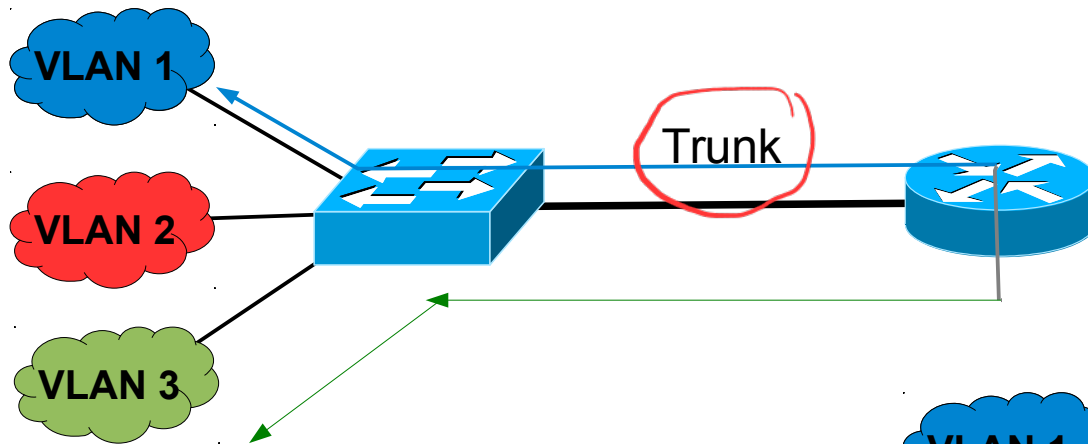
Trunk Links

Multiples VLANs

- A VLAN trunk carries traffic for multiple VLANs by using IEEE 802.1Q.
- Inter-Switch Link (ISL) encapsulation is an alternative but it getting obsolete.
- Trunks may transport all VLAN or only some!

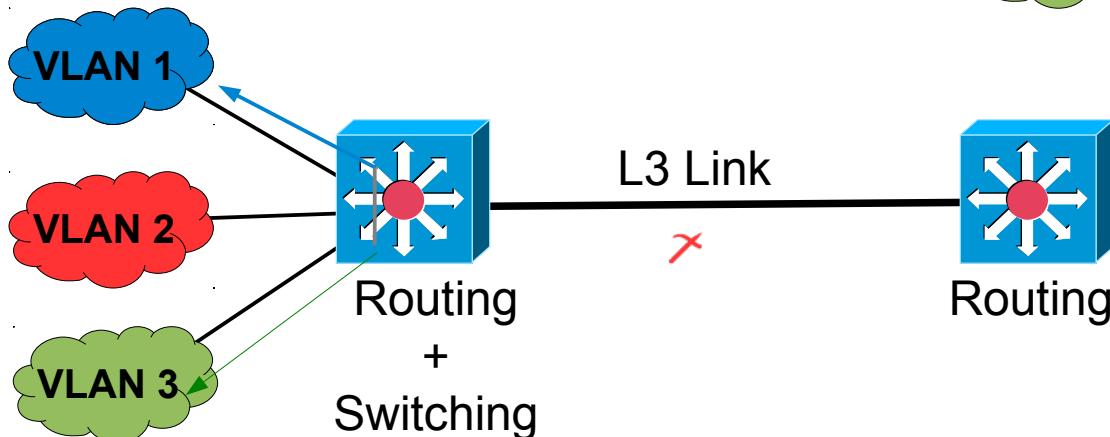
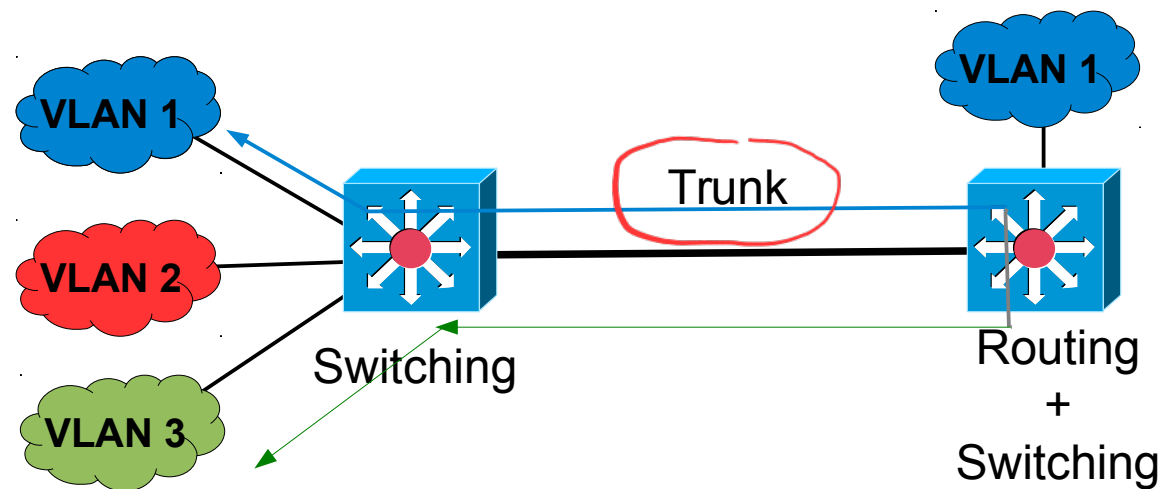


Inter-(V)LAN Routing



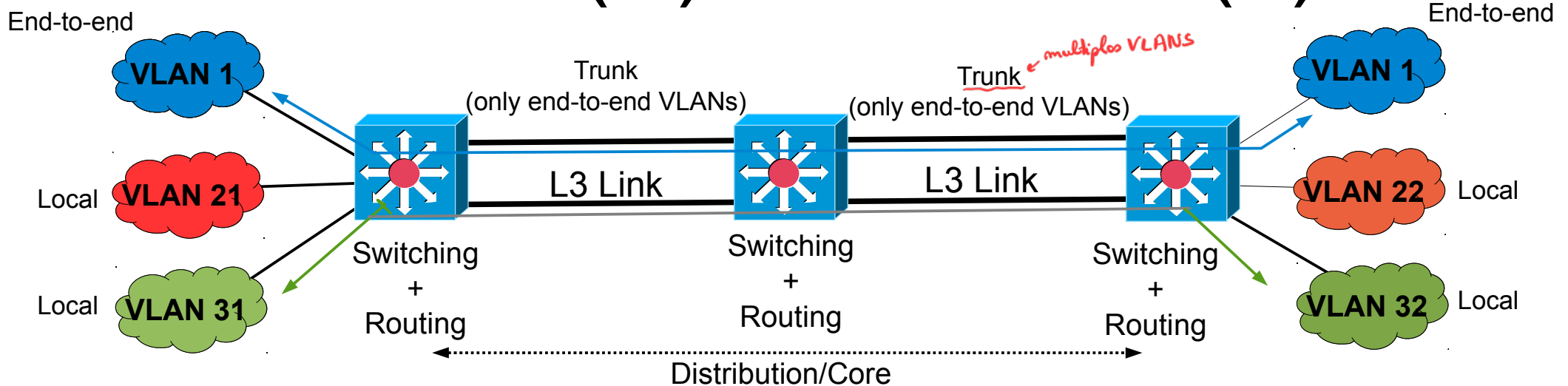
- L2 Switch + Router
- Does not allow end-to-end VLANs.

- L3 Switch + L3 Switch
- Traffic between VLANs must “travel” until the first L3 Switch performing Routing.



- L3 Switch + L3 Switch
- The same ID VLAN may exist, while there are trunks to transport L2 traffic.

Inter-(V)LAN Traffic (1)

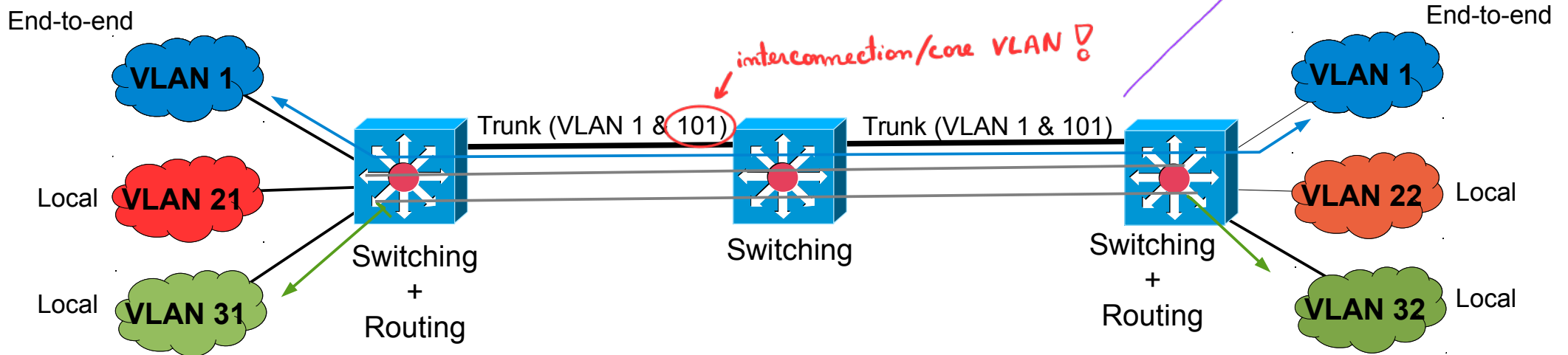


- End-to-end VLANs traffic should be **switched** over the Distribution/Core layers
 - ↳ É como se estivessem encostados ? ?
- Using a trunk (for end-to-end VLANs only).
- Local VLANs traffic should be **routed** over the Distribution/Core layers
 - ↳ entre VLANs iguais sem end-to-end o tráfego é routed,,
- Using standard layer 3 Links.

ESTE CONCEITO
É IMPORTANTE

Inter-(V)LAN Traffic (2)

- Layer 2 and Layer 3 traffic should share the same physical link!
 - The layer 3 link is replaced by an Interconnection/Core VLAN.
- Interconnection/Core VLANs
 - VLAN used only for interconnection between local-VLANs.
 - Allows the mixture of VLAN segmentation models.
- **Interconnection trunks should allow ONLY:**
 - Ends-to-end VLANS *f entre a VLAN 1*
 - Interconnection/Core VLANs *→ Para fazer routing entre VLANs*



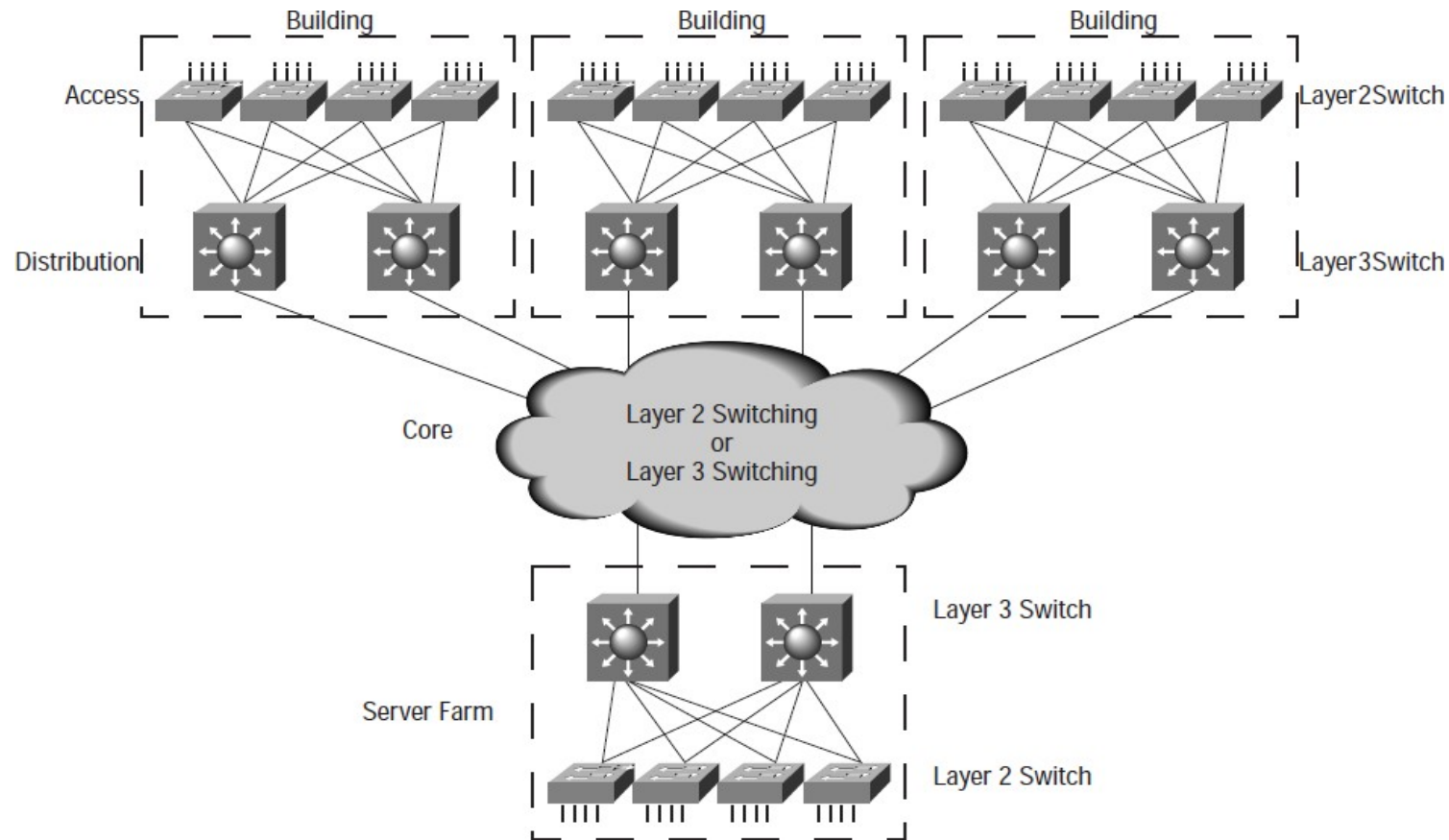
VLAN 101 is the interconnection VLAN.

Spanning Tree Protocol

- STP enables the network to deterministically block interfaces and provide a loop-free topology in a network with redundant links.
- There are several STP Standards and Features:
 - STP is the original IEEE 802.1D version (802.1D-1998) that provides a loop-free topology in a network with redundant links.
 - RSTP, or IEEE 802.1W, is an evolution of STP that provides faster convergence of STP.
 - Multiple Spanning Tree (MST) is an IEEE standard. MST maps multiple VLANs into the same spanning-tree instance.
 - Per VLAN Spanning Tree Plus (PVST+) is a Cisco enhancement of STP that provides a separate 802.1D spanning-tree instance for each VLAN configured in the network.
 - RPVST+ is a Cisco enhancement of RSTP that uses PVST+. It provides a separate instance of 802.1W per VLAN.
- Recommended Practices for STP
 - Define by configuration (using STP priority) the root bridge/switch.
 - Use the same cost in all interfaces (if possible).

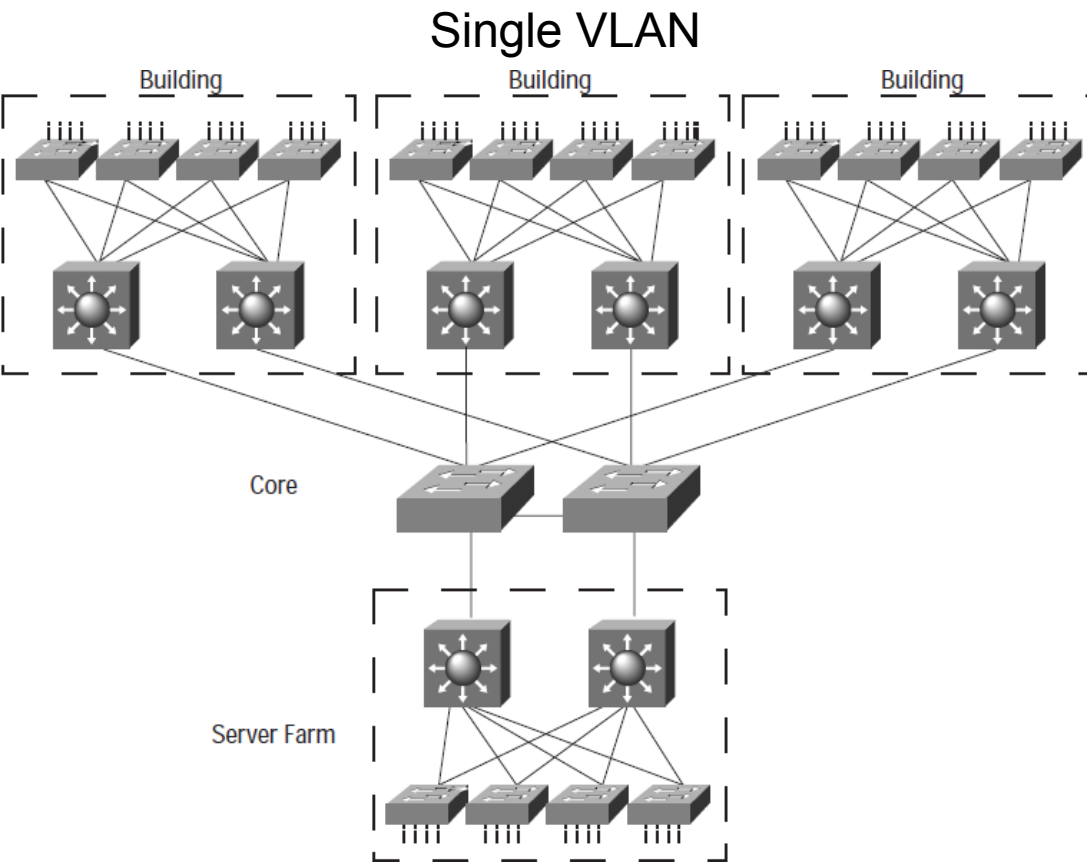
Core Types

Layer 2 vs. Layer 3 Core

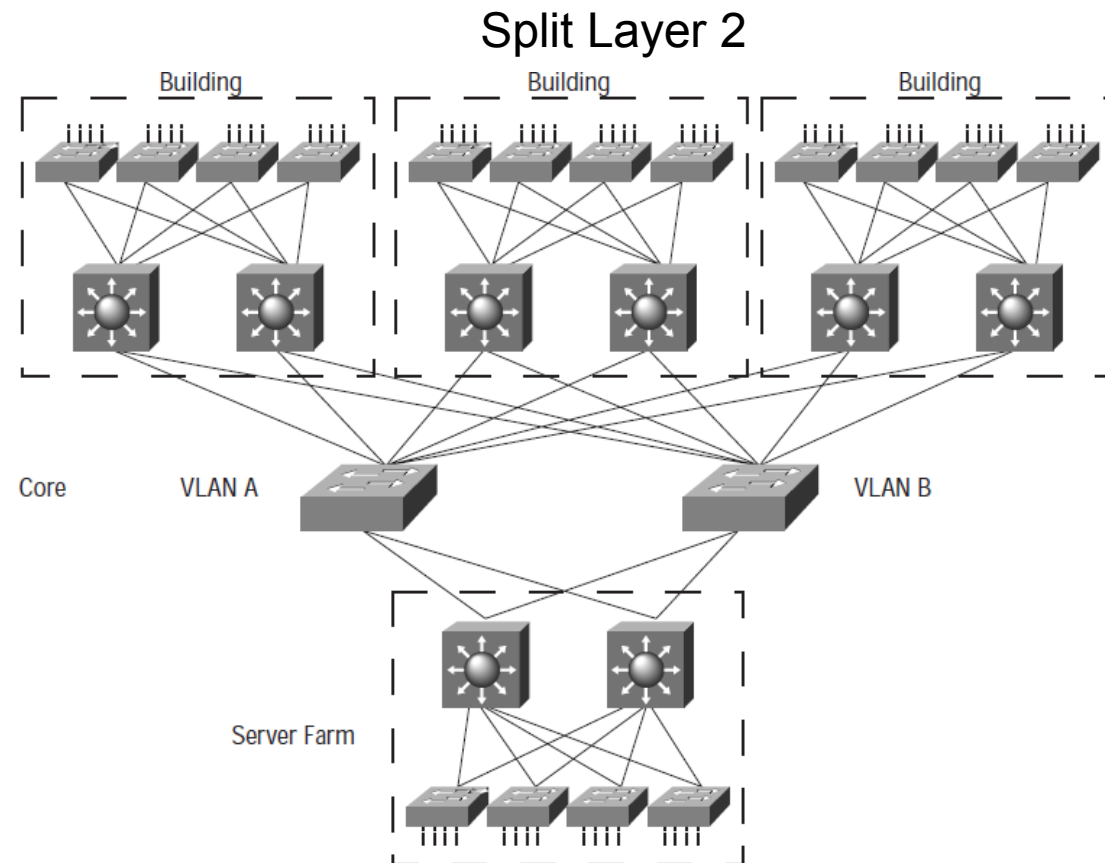


- Layer 3 switched backbones have several advantages:
 - Reduced router peering.
 - Flexible topology with no spanning-tree loops.
 - Multicast and broadcast control in the backbone.
 - Scalability to arbitrarily large size.

Layer 2 Switched Core



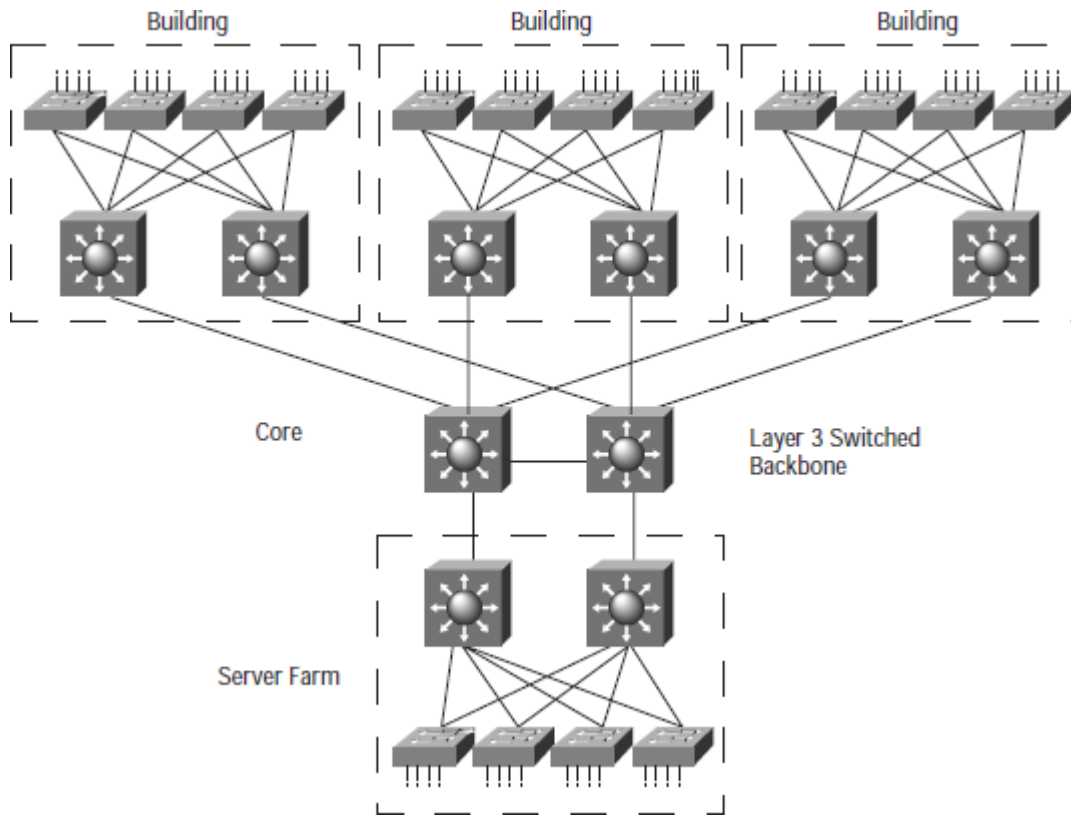
- The core is a single Layer 2 switched domain VLAN with a star topology.
 - A single IP subnet is used in the core.
- Because there are no loops, spanning-tree protocol does not put any links in blocking mode.
 - Spanning-tree protocol convergence will not affect the core.
 - To prevent spanning-tree protocol loops, the links into the core should be defined as routed interfaces, not as VLAN trunks/inter-switch ports.
- All broadcasts and multicasts packets flood the core.



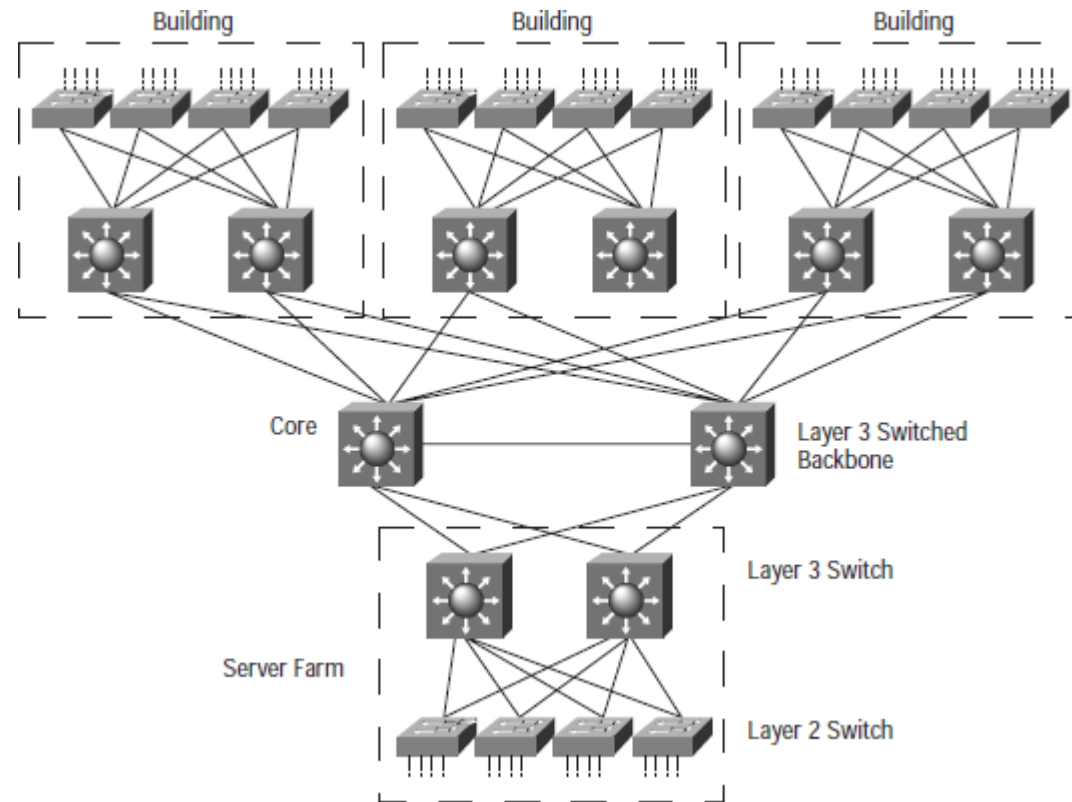
- The core is two Layer 2 switched VLANs that form two totally separate redundant cores.
 - There is no trunk linking the VLANs
- Each Layer 3 switch in the distribution layer now has two distinct equal-cost paths to every other distribution-layer switch.
 - If the VLAN A path is disconnected, the Layer 3 switch will immediately route all traffic over VLAN B.
- The advantage of the Split Layer 2 backbone design is that two equal-cost paths provide fast convergence.
- The extra cost of the dual-core design is associated with the extra links from each distribution switch to each backbone switch.

Layer 3 Switched Core

Without Dual Paths

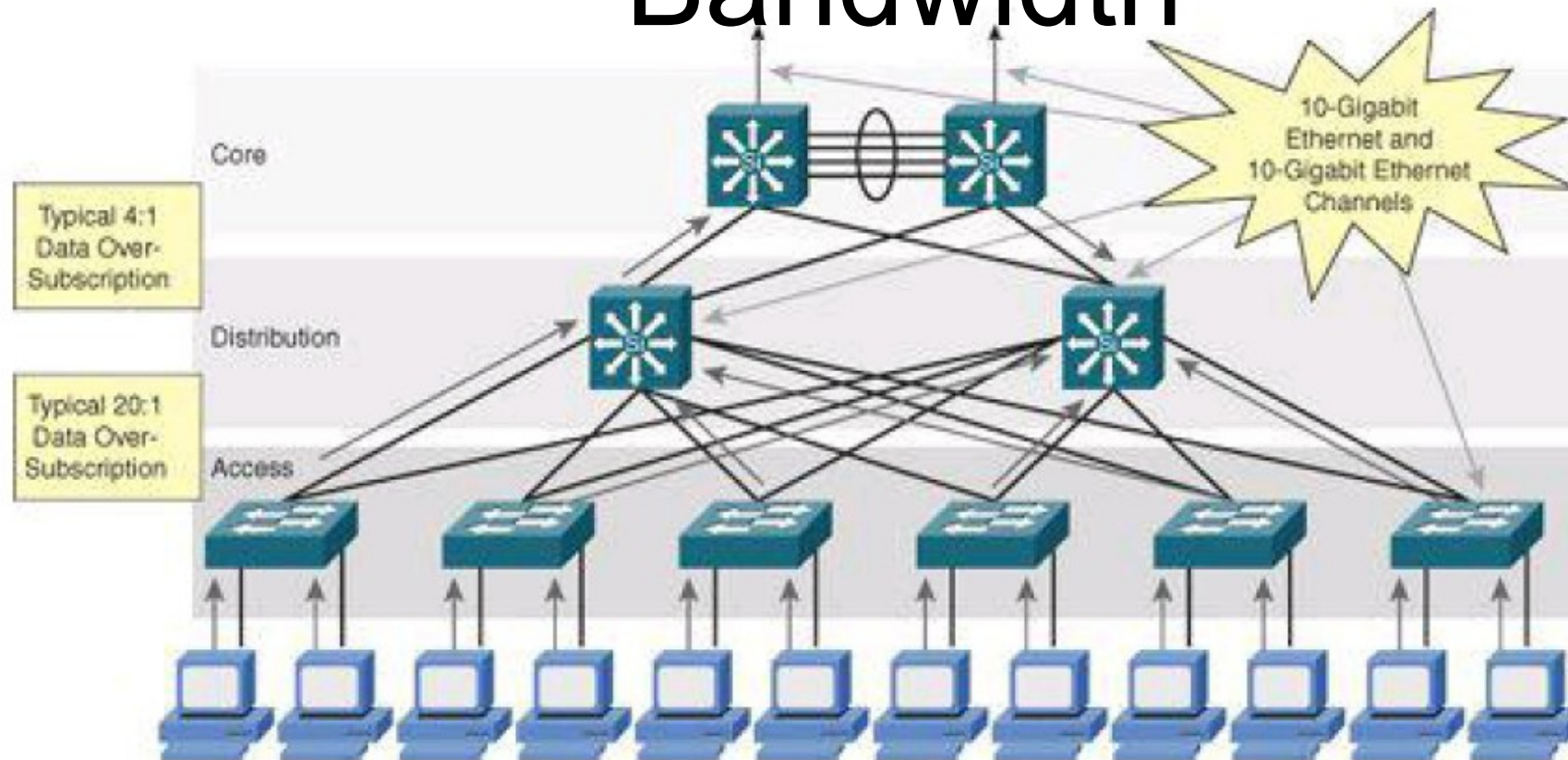


With Dual Paths



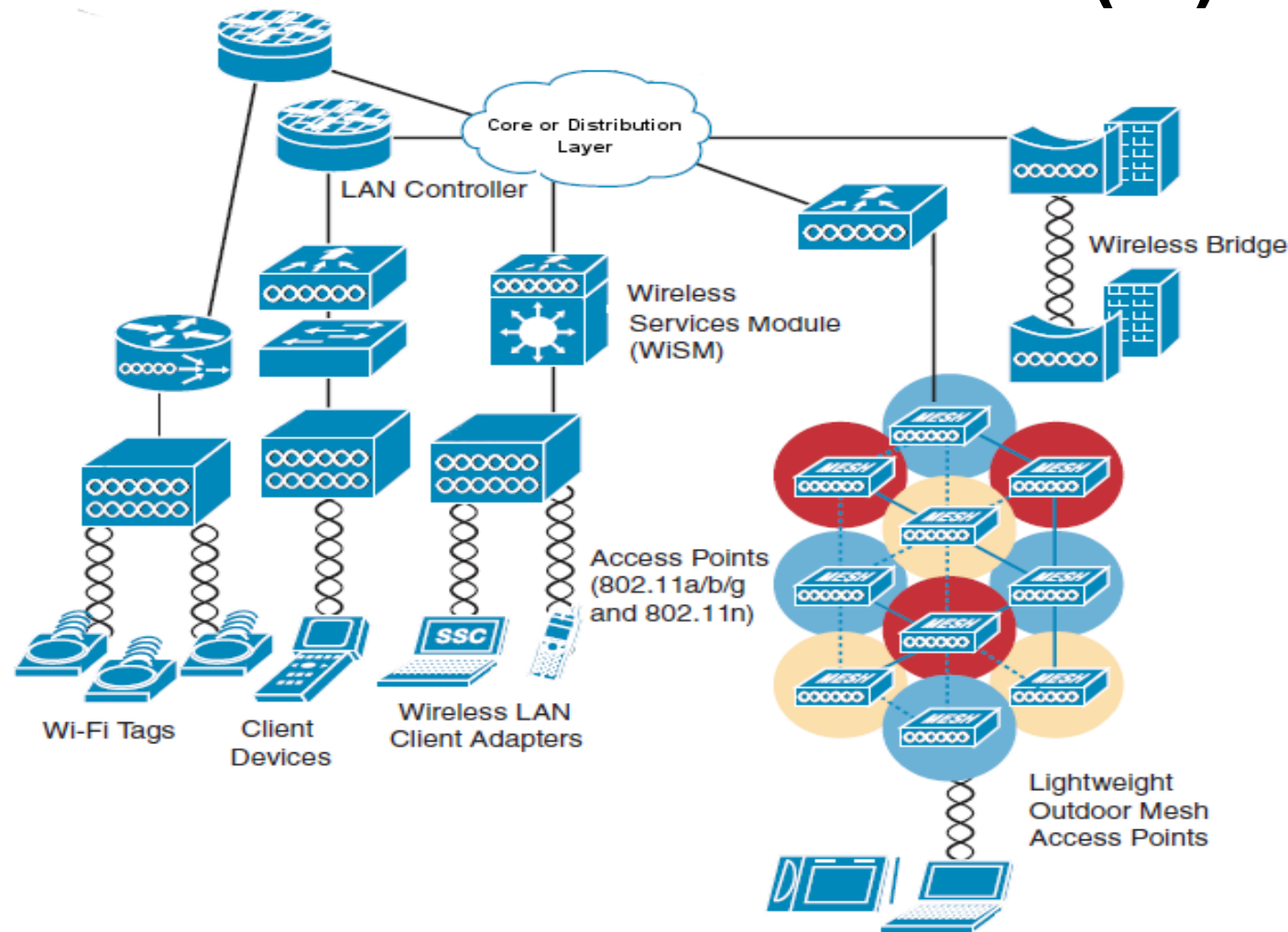
- The main advantage of a Layer 3 Core with dual paths design is that each distribution-layer switch maintains two equal-cost paths to every destination network.
 - Recovery from any link failure is fast.
 - Provides double the bandwidth capacity into the core.
- The inter-connection between the access layer and the Layer 3 switched core can be done using a split Layer 2 (dual VLAN) approach.

Managing Over-subscription and Bandwidth



- The rule-of-thumb recommendation for data oversubscription is:
 - 20:1 for access ports on the access-to-distribution uplink,
 - 4:1 for the distribution-to-core links.
- When you use these oversubscription ratios, you may make congestion on the uplinks an infrequent occurrence.
 - QoS is needed for these occasions.
- If congestion is occurring frequently, the design does not have sufficient uplink bandwidth.

Wireless Network(s)



- Wireless networking technologies should have an integration point at core or distribution layers.
- In terms of network architecture a WLAN can be seen as any LAN.
 - Except that we have mobility and must have seamless roaming while moving.
- We will get back to this later!

Recommended Reading

- [Chapters 1 and 2] - A Practical Approach to Corporate Networks Engineering, António Nogueira, Paulo Salvador, River Publishers, ISBN-13: 978-8792982094, 2013.
- [Chapters 1 and 2] - Designing Cisco Network Service Architectures (ARCH), John Tiso, Cisco Press, ISBN-13: 978-1587142888, 3rd Edition, 2011.
- Cisco's White Paper, "Gigabit Campus Network Design Principles and Architecture". (Available at moodle.ua.pt)