# Enterprise Network Design Topics

**Arquitetura de Redes**

**Mestrado Integrado em**
**Engenharia de Computadores e Telemática**
**DETI-UA**

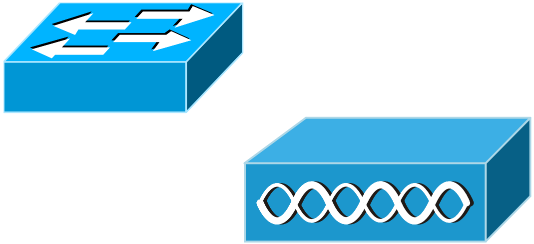
universidade de aveiro
deti.ua.pt

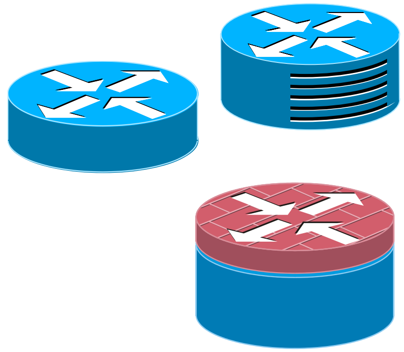
# Objectives of Network Design

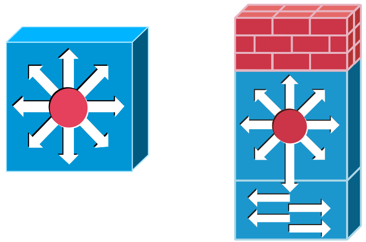
- Network should be **Modular**
  - Support growth and change.
  - Scaling the network is eased by adding new modules instead of complete redesigns.
- Network should be **Resilient**
  - Up-time close to 100 percent.
    - If network fails in some companies (e.g. financial), even for a second, may represent 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.

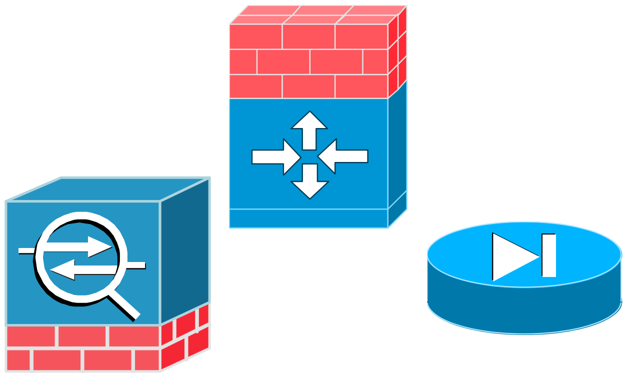
# Equipments

- 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



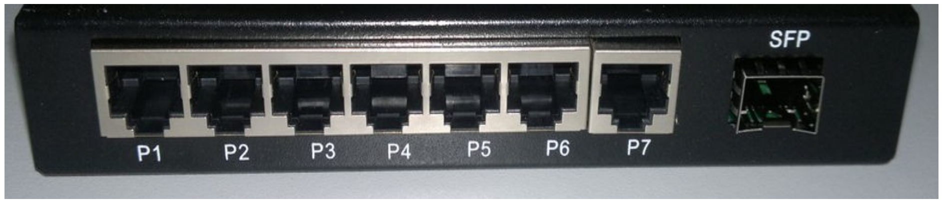


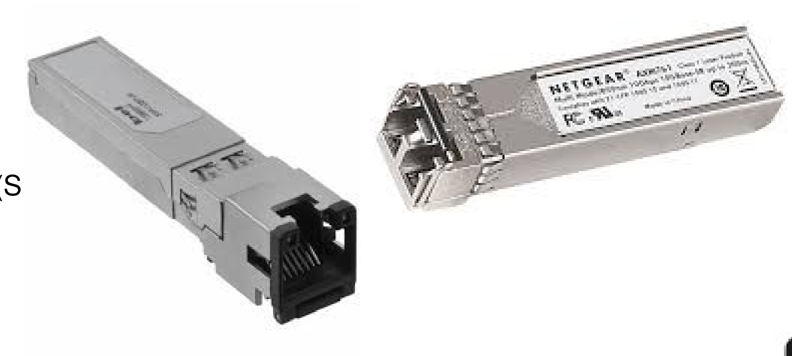




# How to Choose the Equipments

- 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 constrains, 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 (S
    - With or without PoE (Power over Ethernet)
      - For VoIP phones, Access Points, etc...
  - Number of slots
    - For additional port/processing modules.



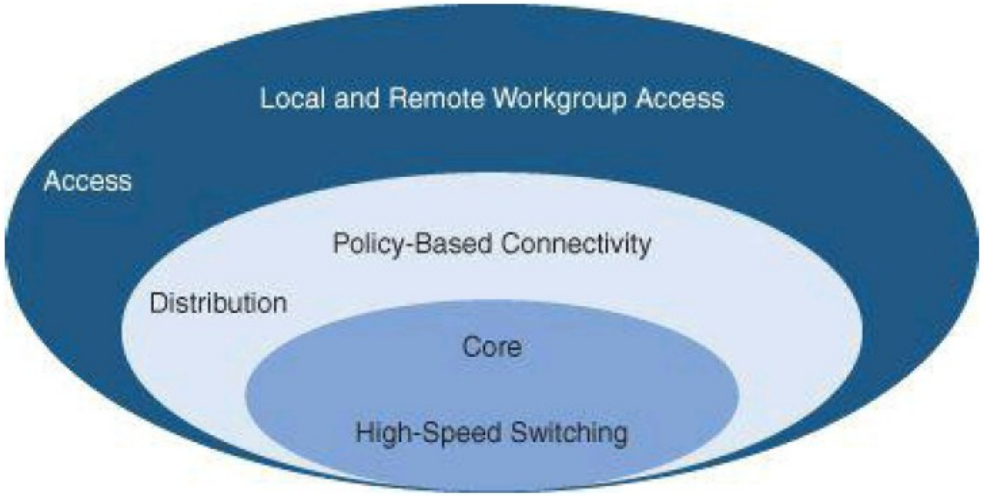



# Hierarchical Network Model

universidade de aveiro

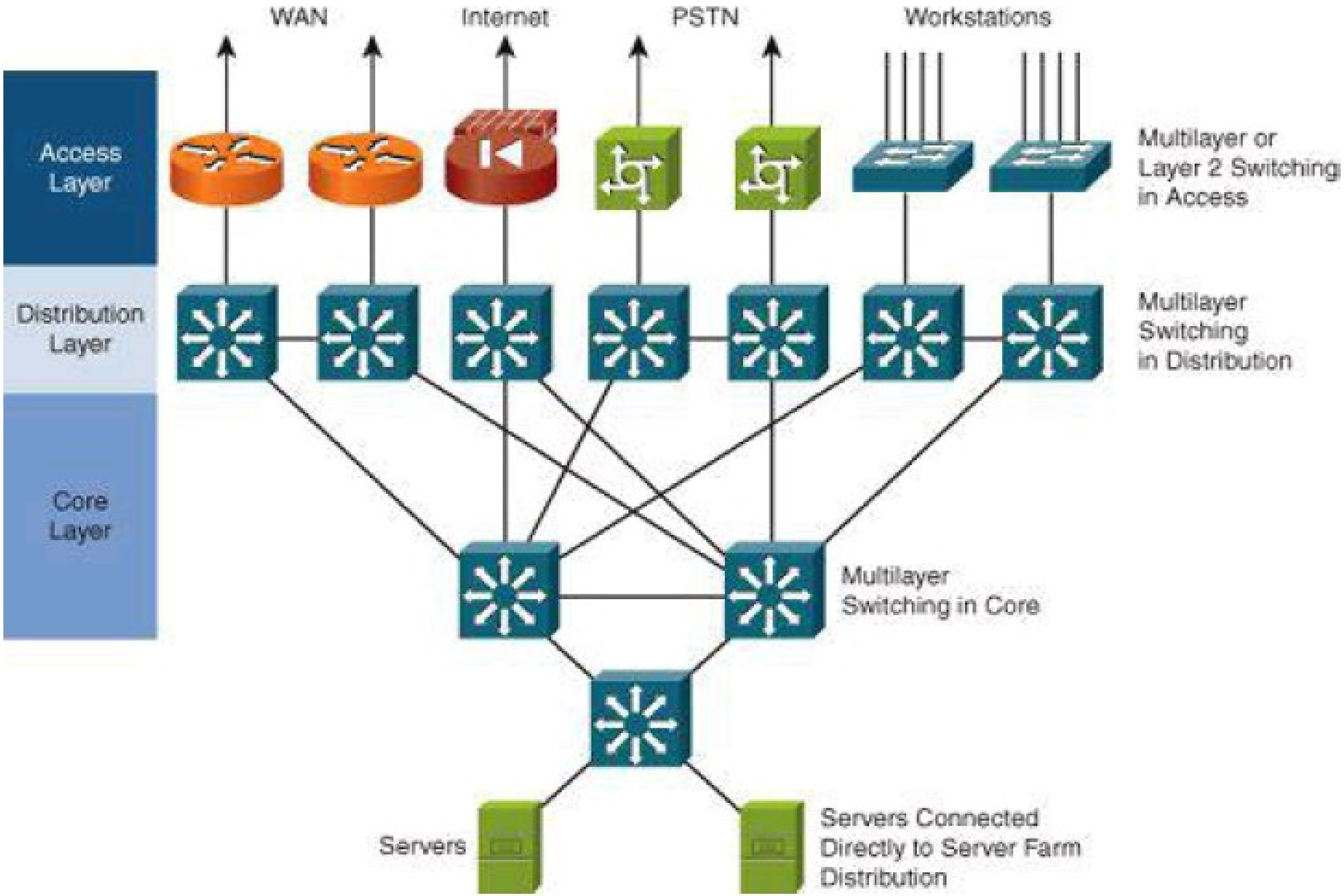
deti.ua.pt

# Hierarchical Network Model

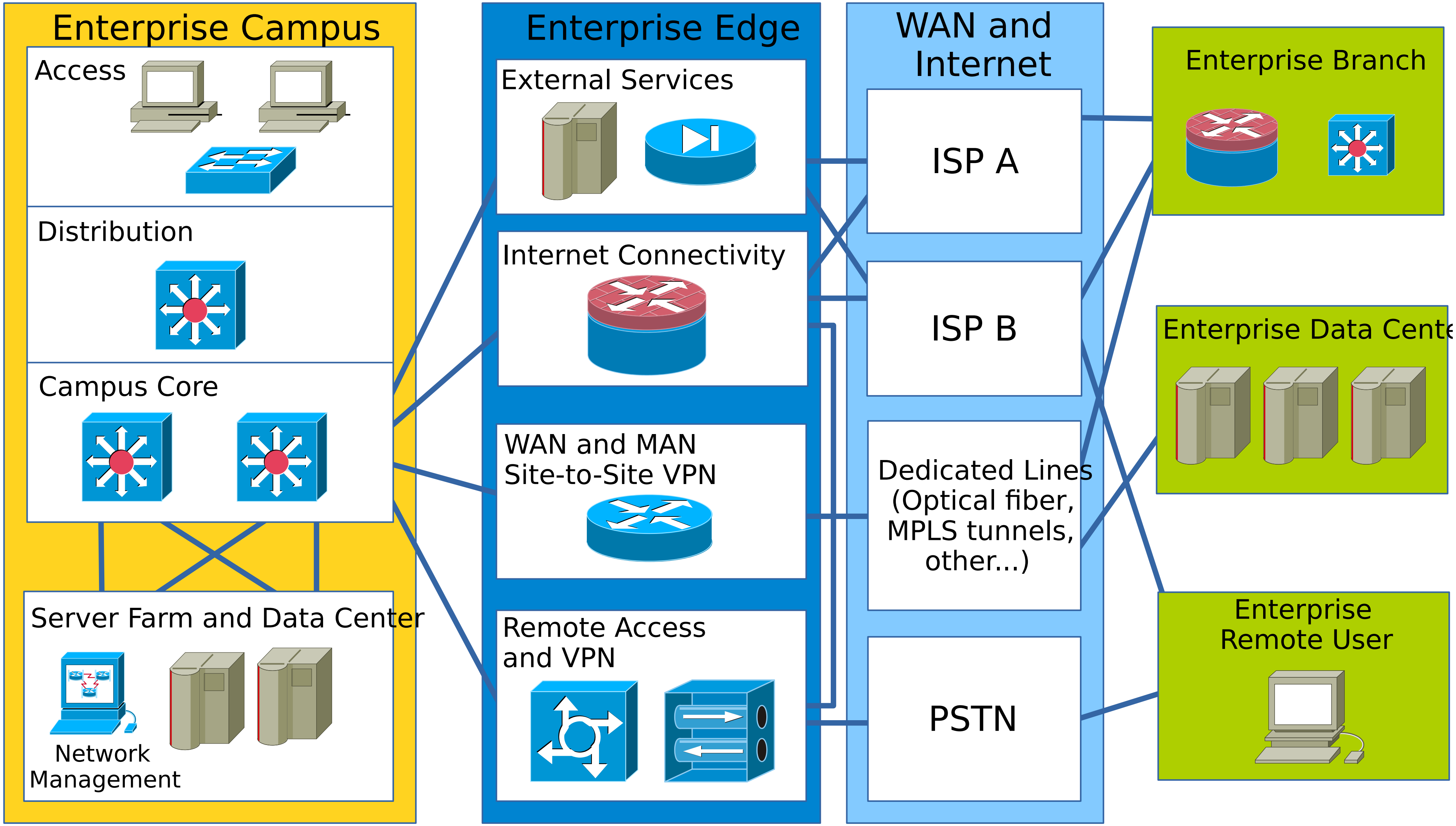



- Access layer
  - Provides user access to network.
  - Generally incorporates switched LAN devices that provide connectivity to workstations, IP phones, servers, and wireless access points.
  - For remote users or remote sites provide an entry to the network across WAN technology.
- Distribution layer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



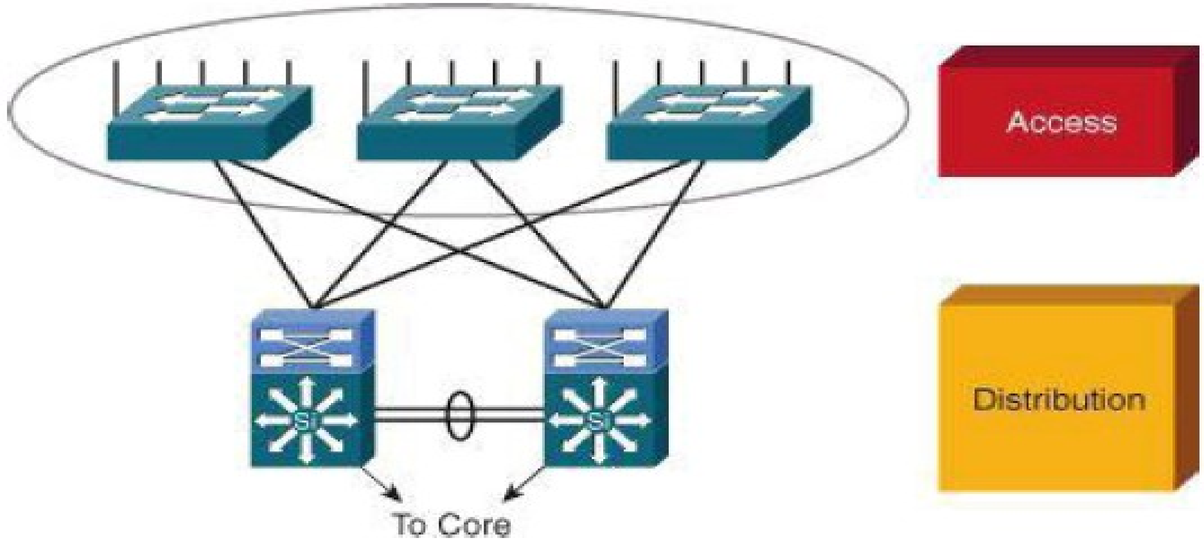
# Network Modules (1)

- 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)

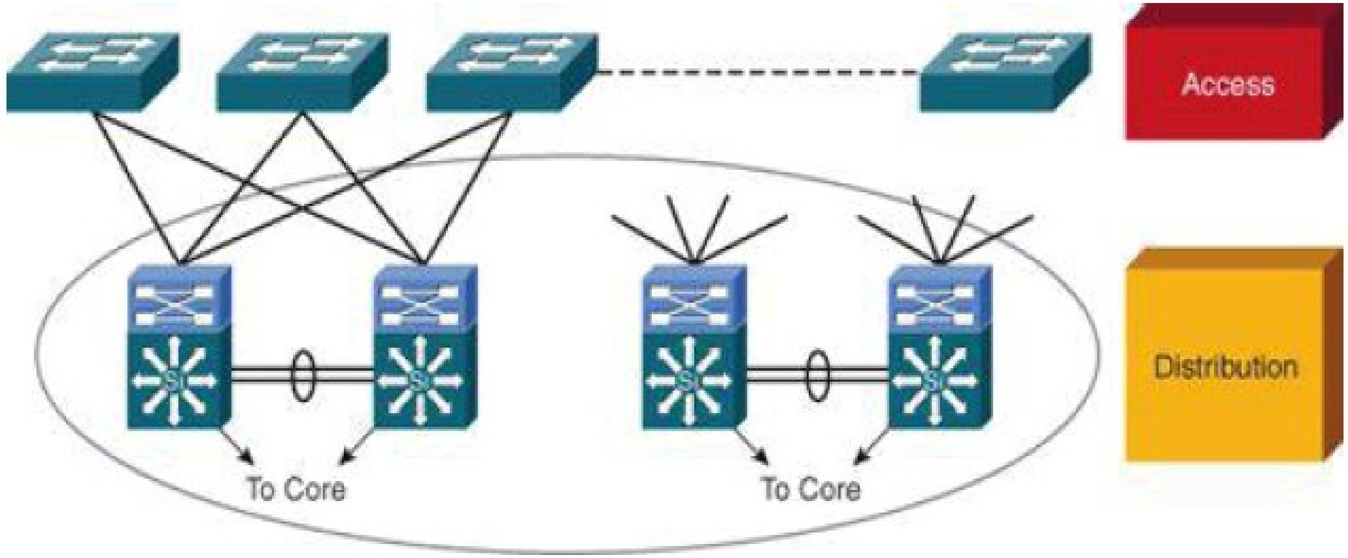
- WAN and MAN
  - Offers the convergence of voice, video, and data services.
  - Enables the enterprise a cost-effectively presence in large geographic areas.
  - QoS, granular service levels, and comprehensive encryption options help ensure the secure delivery to all sites.
  - Security is provided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



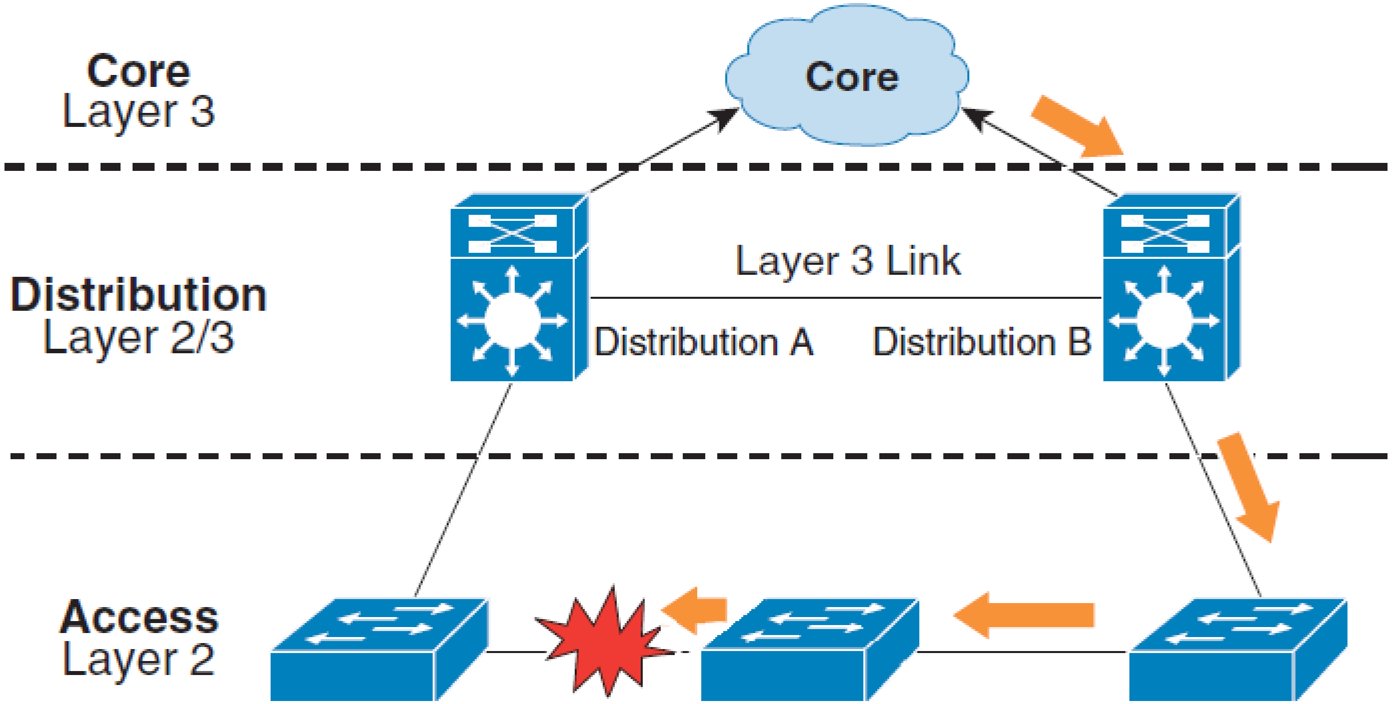

- High availability
  - Default gateway redundancy using multiple connections from access switches to redundant distribution layer switches.
  - Redundant power supplies.
- Other considerations
  - Convergence: the access layer should provide seamless convergence of voice into data network and providing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



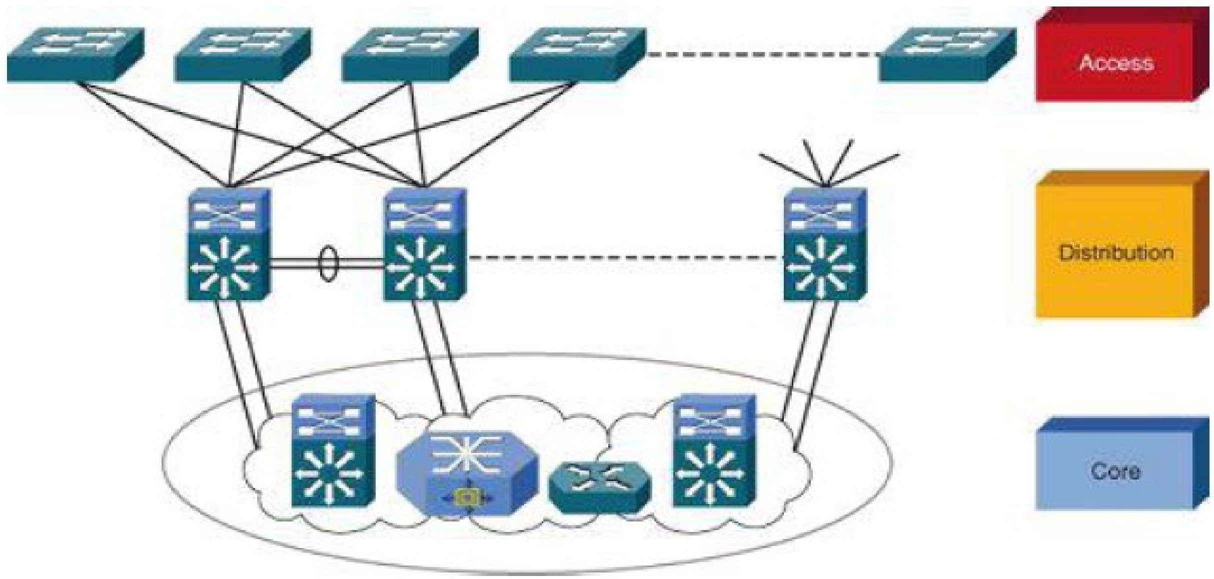

- Uses a combination of Layer 2 and multilayer switching to segment workgroups and isolate network problems, preventing them from impacting the core layer.
- Connects network services to the access layer and implements QoS, security, traffic loading balancing, and implements routing policies.
- Major 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.

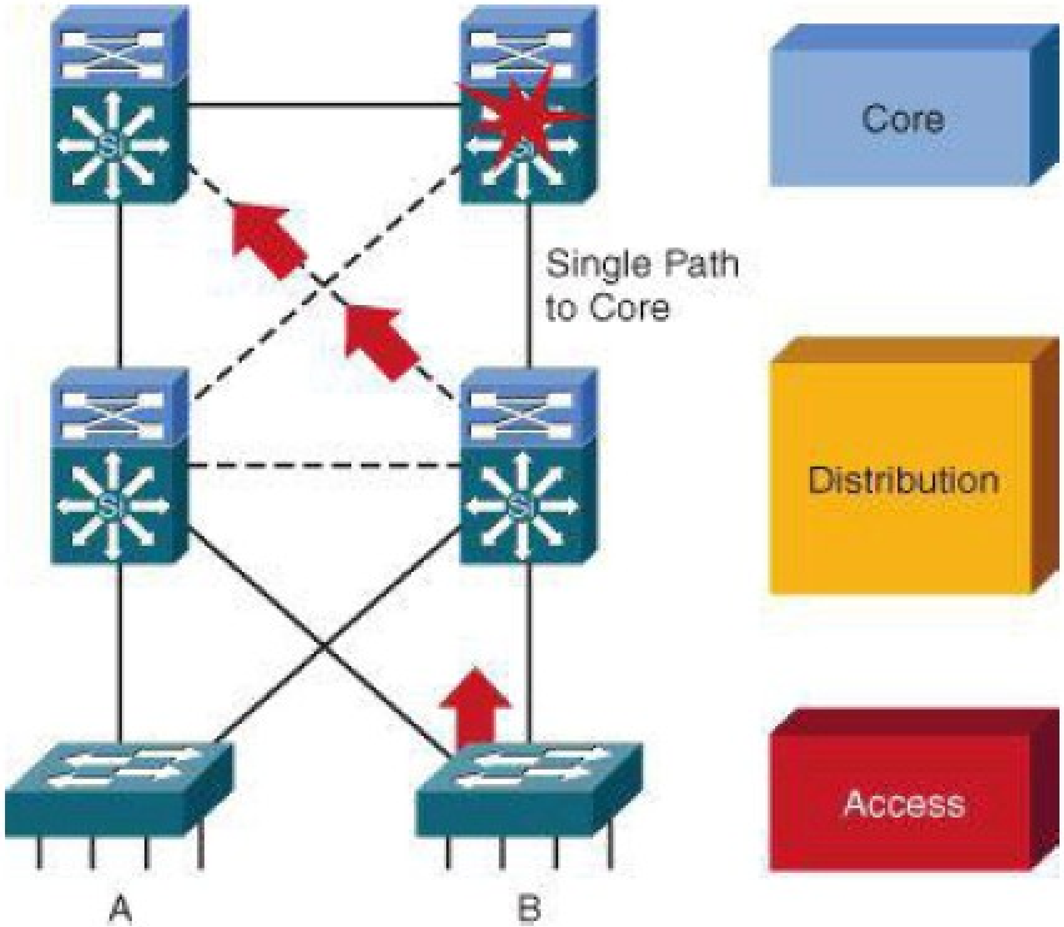
# Designing the Core Layer



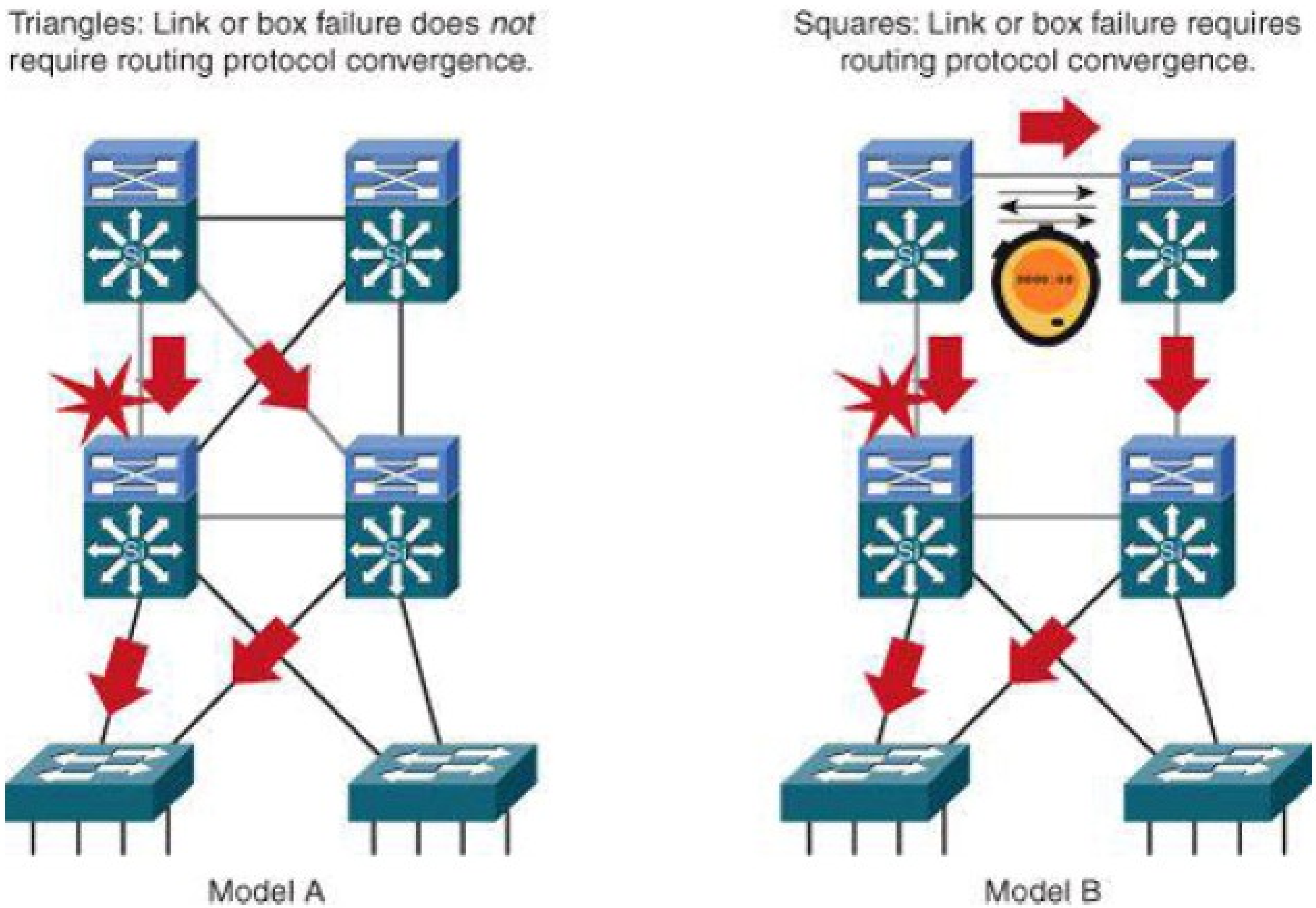

- Backbone for campus connectivity and is the aggregation point for the other layers.
- Should provide scalability, high availability, and fast convergence to the network.
  - The core layer should scale easily.
  - High-speed environment that should use hardware-acceleration, if possible.
  - The core 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

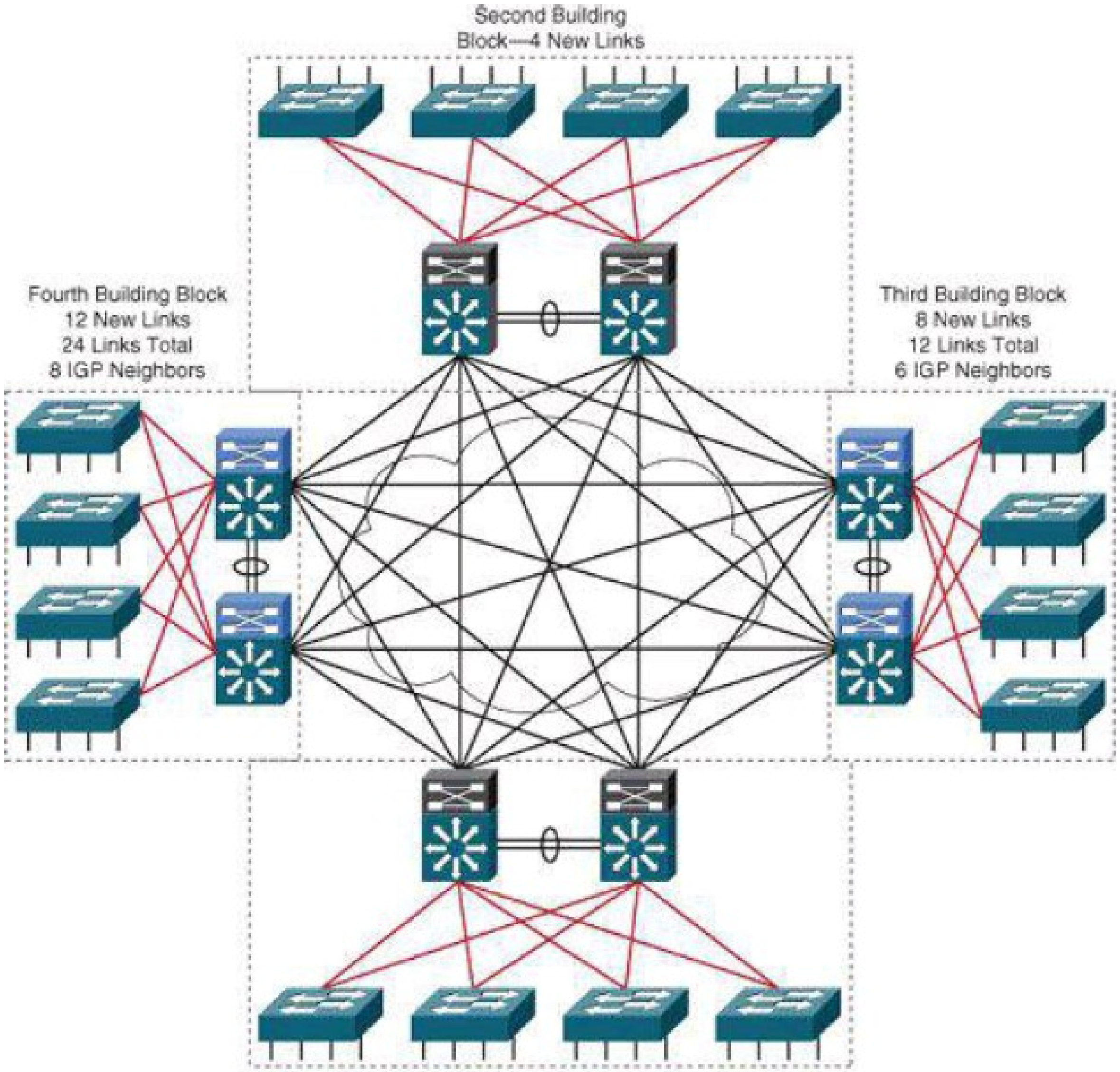
- An additional link providing an alternate path to a second core switch from each distribution switch offers redundancy to support a single link or node failure.



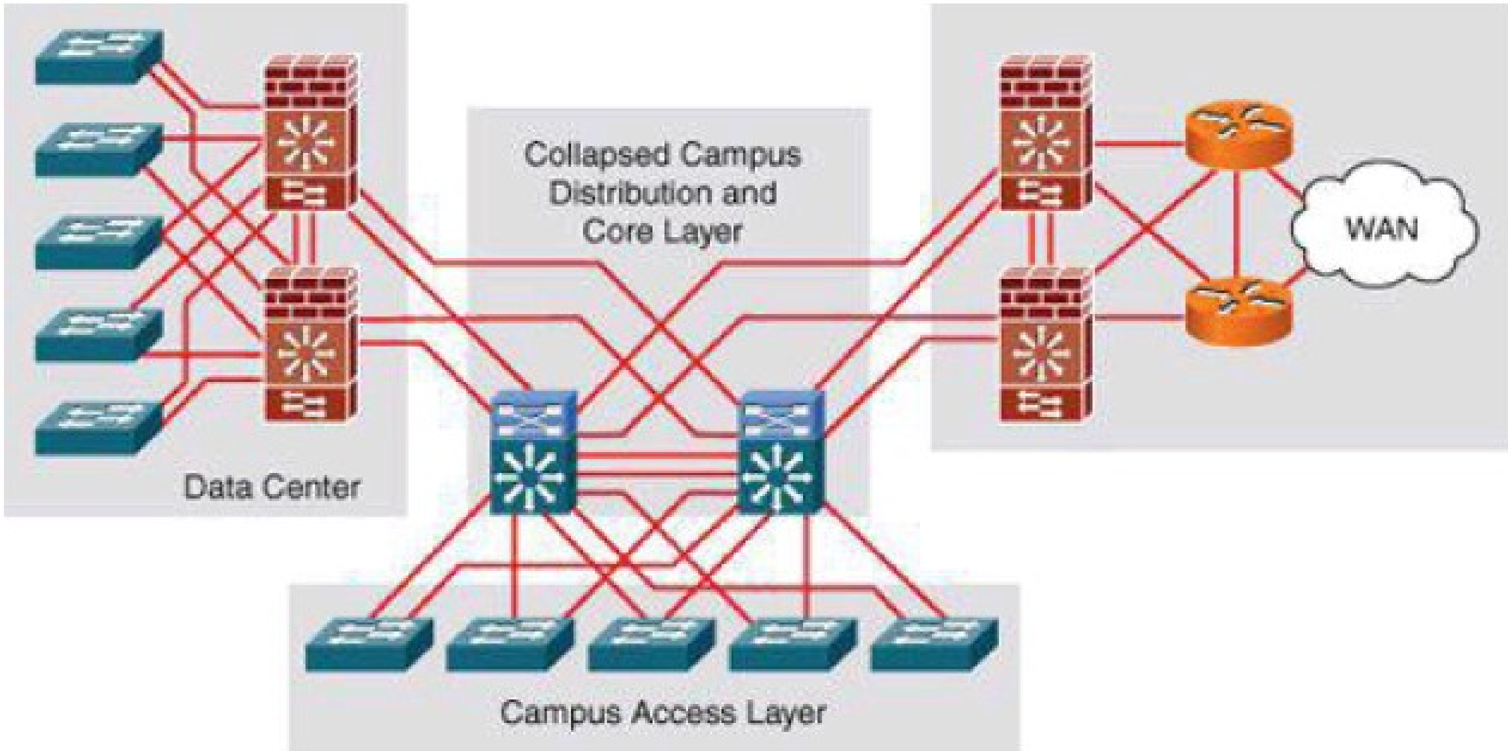
# Core Redundant Triangles



# Without a Core Layer

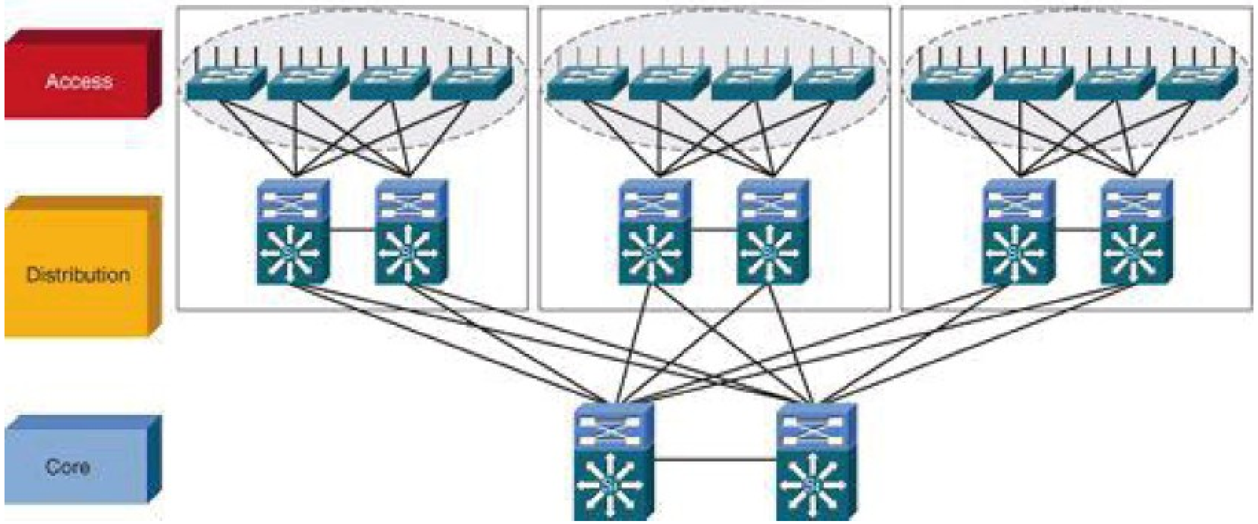


# Collapsed Core Layer Architecture



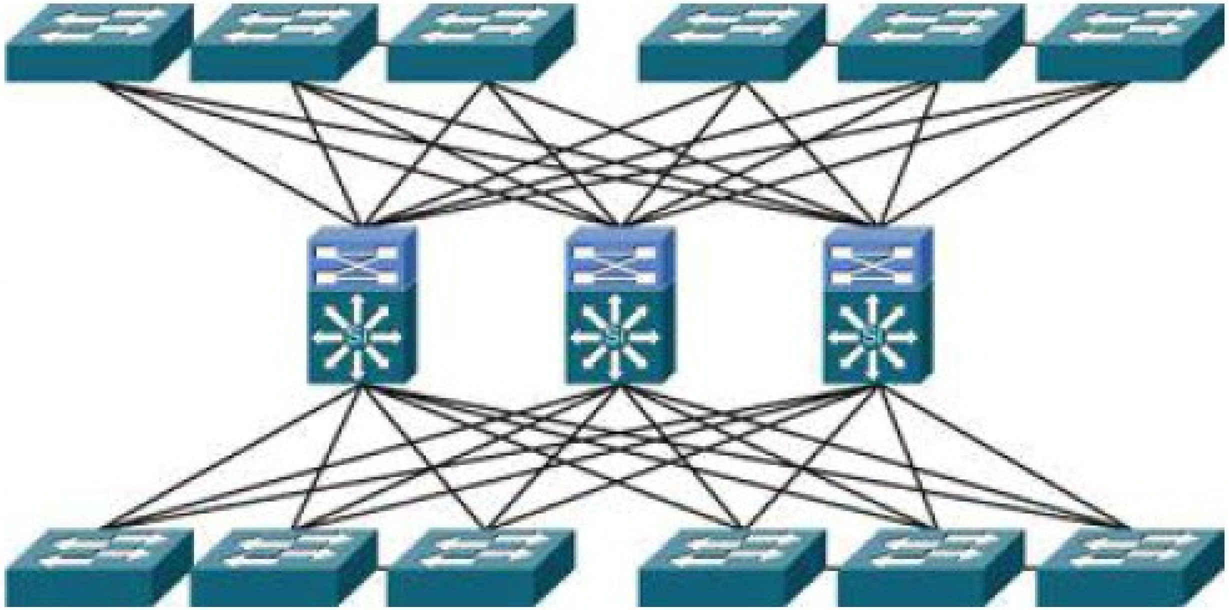

- In smaller networks, the core and the distribution layer can be only one,
  - Eliminates the need for extra switching hardware and simplifies the network implementation.
- However, eliminates the advantages of the multilayer architecture, specifically fault isolation.

# Avoid Single Points of Failure



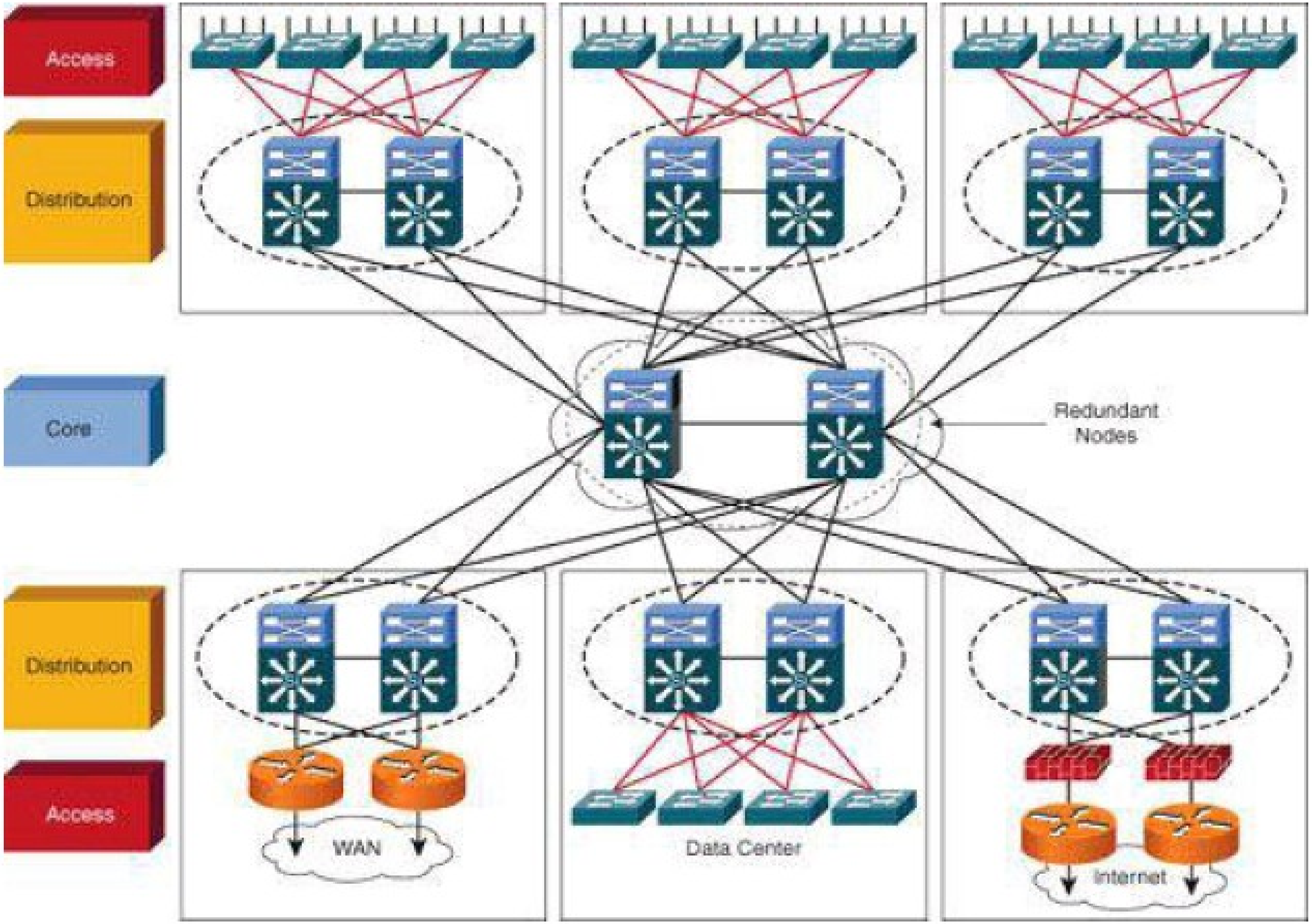

- With an hierarchical design,
  - In Distribution and Core Layers the single points of failure are easy to avoid with redundant links.
    - Don't forget redundant power and cooling!
  - In Access Layer, all L2 switches are single points of failure (only) to the user connected to them,
    - Solution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

universidade de aveiro

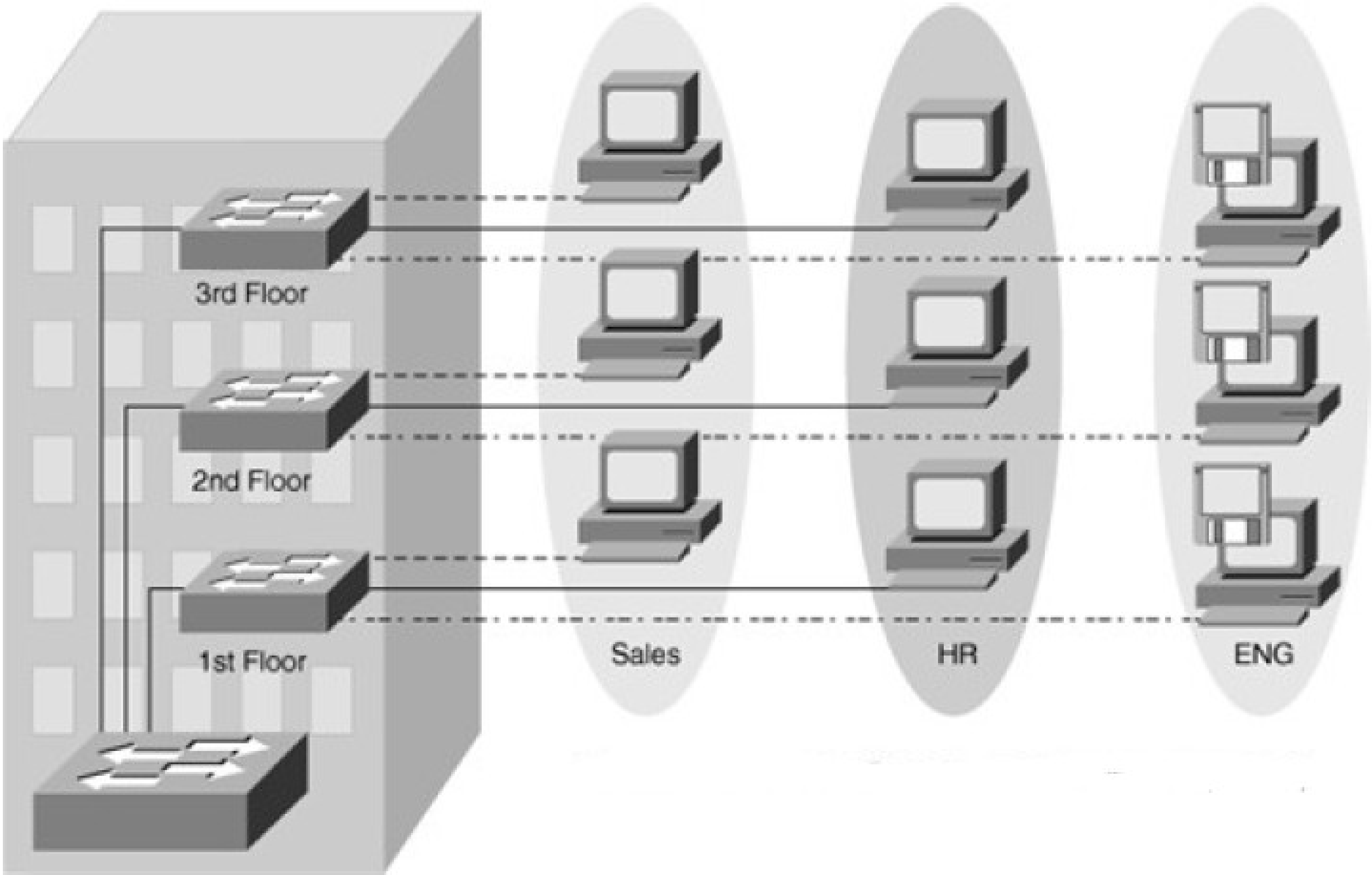
deti.ua.pt

# Virtual LANs

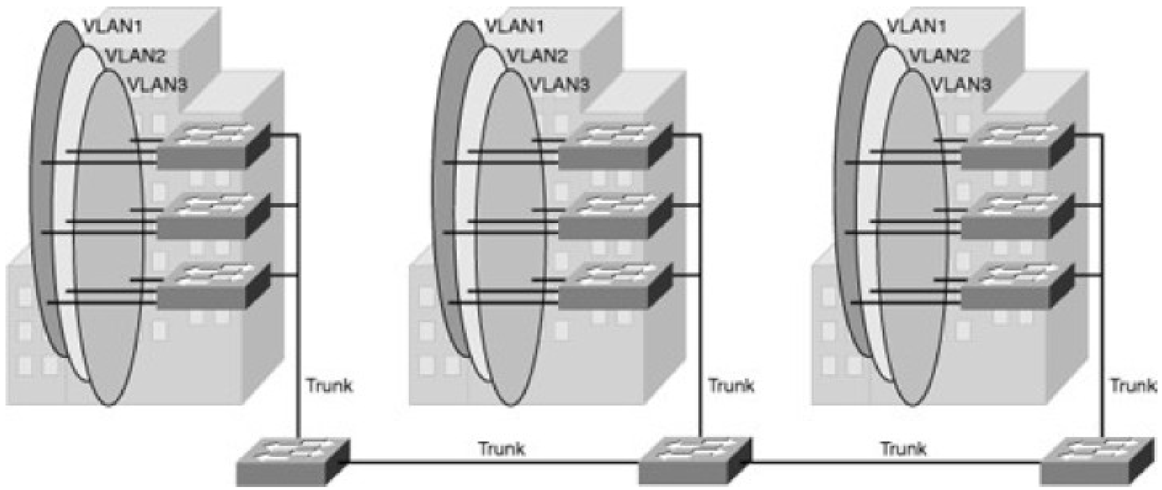
- Group of individual switch ports into switched logical *workgroup*
  - Restrict the broadcast domain to designated VLAN member ports
  - Communication between VLANs requires a router.
- Solves the scalability problems of large flat networks
  - By breaking a single broadcast domain into several smaller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

# Implementing VLANs

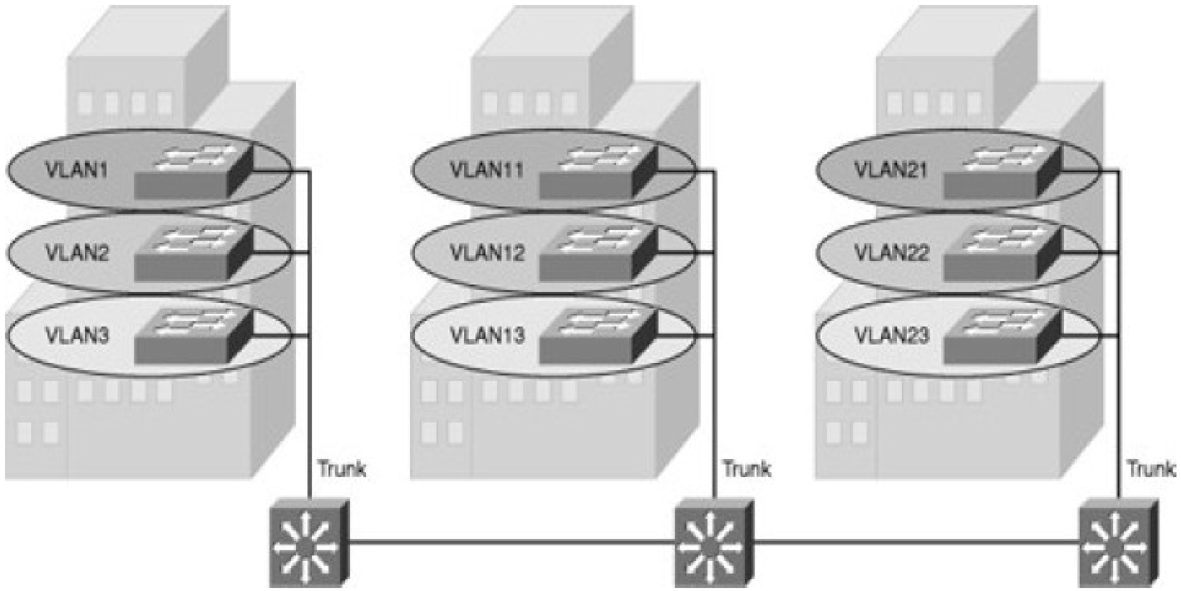
- VLAN is a logical group of end devices with a common set of requirements independent of their physical location.



# VLAN Segmentation Models




- 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

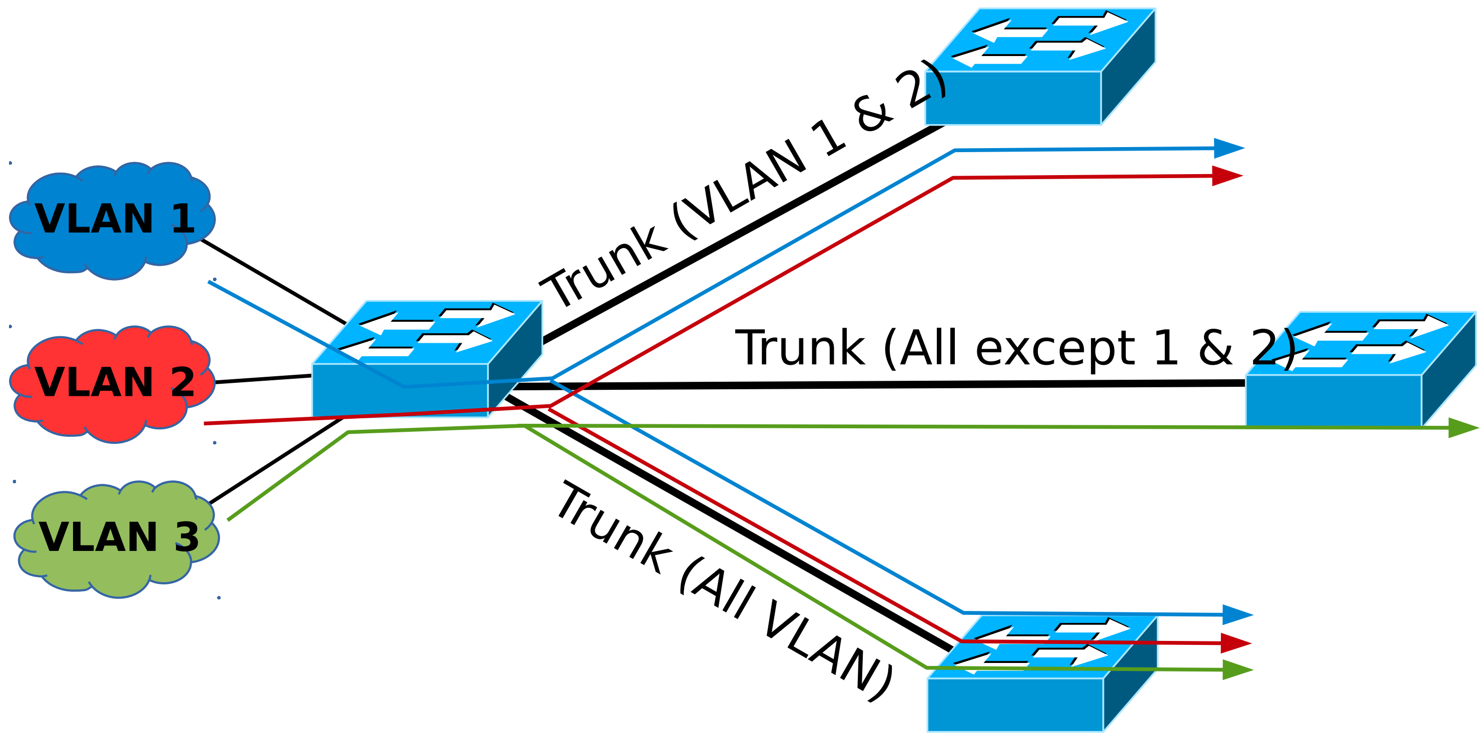
- Joint in the same logical network services/terminals/users with same traffic/security/QoS policies.
  - Each VLAN must have an unique IP (sub-)network.
  - May have more than one IP (sub-)network.
    - Including IPv4 public and IPv4 private networks.
    - And, IPv6 networks.
- Neighbor (local) VLANs 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.

# Special Services Considerations

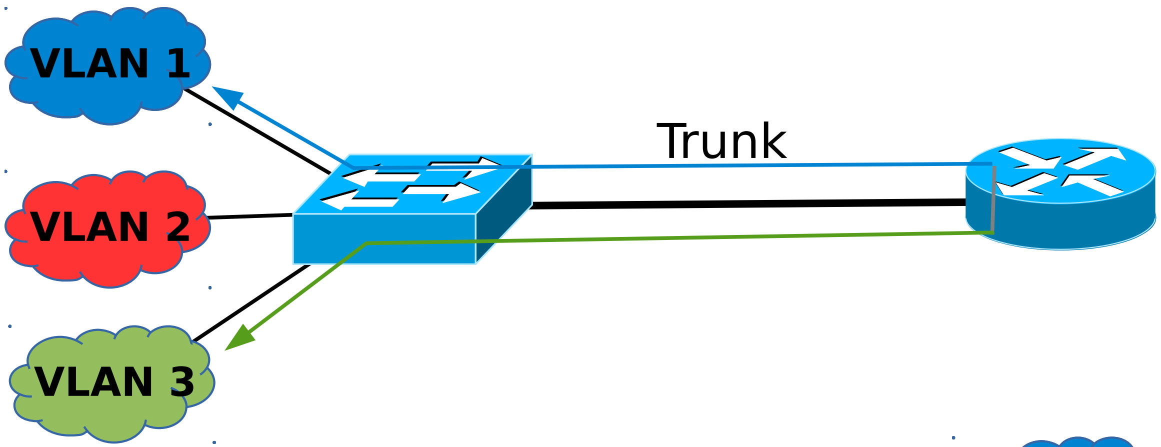
- VoIP (SIP / H.323)
  - Uses a proxy server to establish connections.
    - Communication over NAT/PAT have multiple functional issues.
  - Proxy may rely also multimedia data.
  - Local VLANs, no public IPv4 addresses required.
- Video conference
  - Similar to VoIP, however is common to establish direct conference calls to the exterior or through external servers.
  - NAT issues (SIP) → Requires IPv4 public addresses.
- Corporate TV.
  - Constant traffic from a central internal server to several equipments.
  - May use multicast routing.
  - No public IP addresses required.
- Video-surveillance
  - Constant traffic from several equipments to a central internal server.
- Authentication services.
  - Isolated core VLAN just for isolated secure communications (not common, but good idea).
- Management VLAN
  - A end-to-end VLAN used to perform management actions in equipments.

# Trunk Links

- 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!

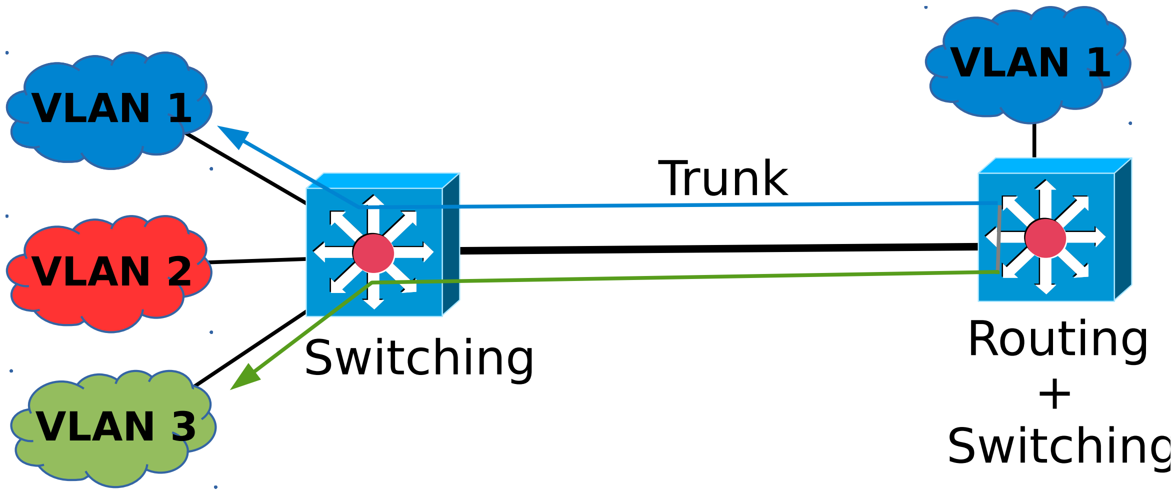


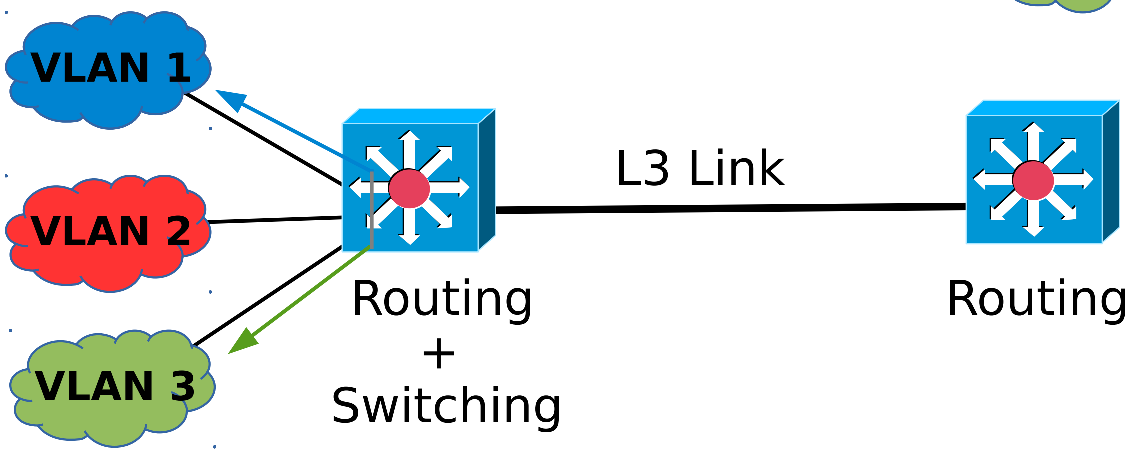
# Inter-(V)LAN Routing




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

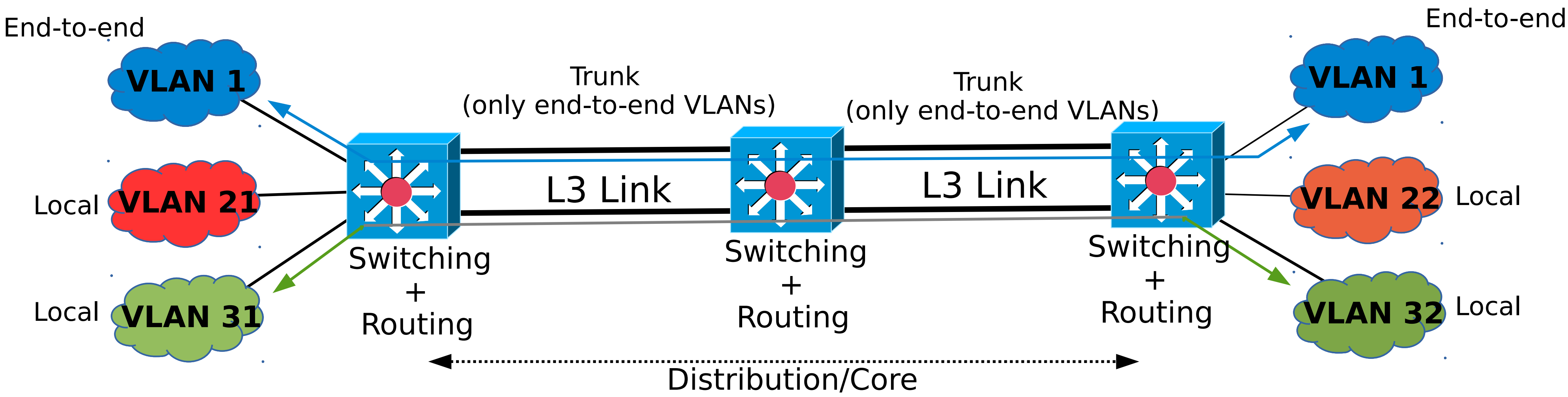
- L3 Switch + L3 Switch
  - Traffic between VLANs must “travel” until the first L3 Switch performing Routing.




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

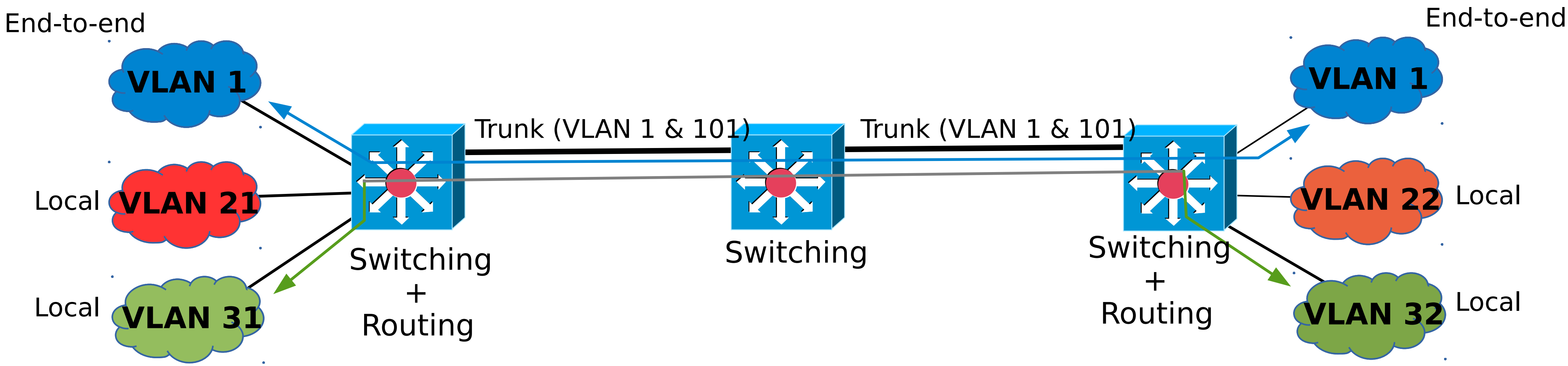
# Inter-(V)LAN Traffic (1)




- End-to-end VLANs traffic **<u>should be switched</u>** over the Distribution/Core layers
  - Using a trunk (for end-to-end VLANs only).
- Local VLANs traffic **<u>should be routed</u>** over the Distribution/Core layers
  - Using standard layer 3 Links.
  - Using static routing (not the best solution!).
  - Exchange the routing information only through the L3 links
    - End-to-end VLAN should be passive interfaces for the routing processes.
      - Routes are not exchanged → Traffic is not routed!

# Inter-(V)LAN Traffic (2)

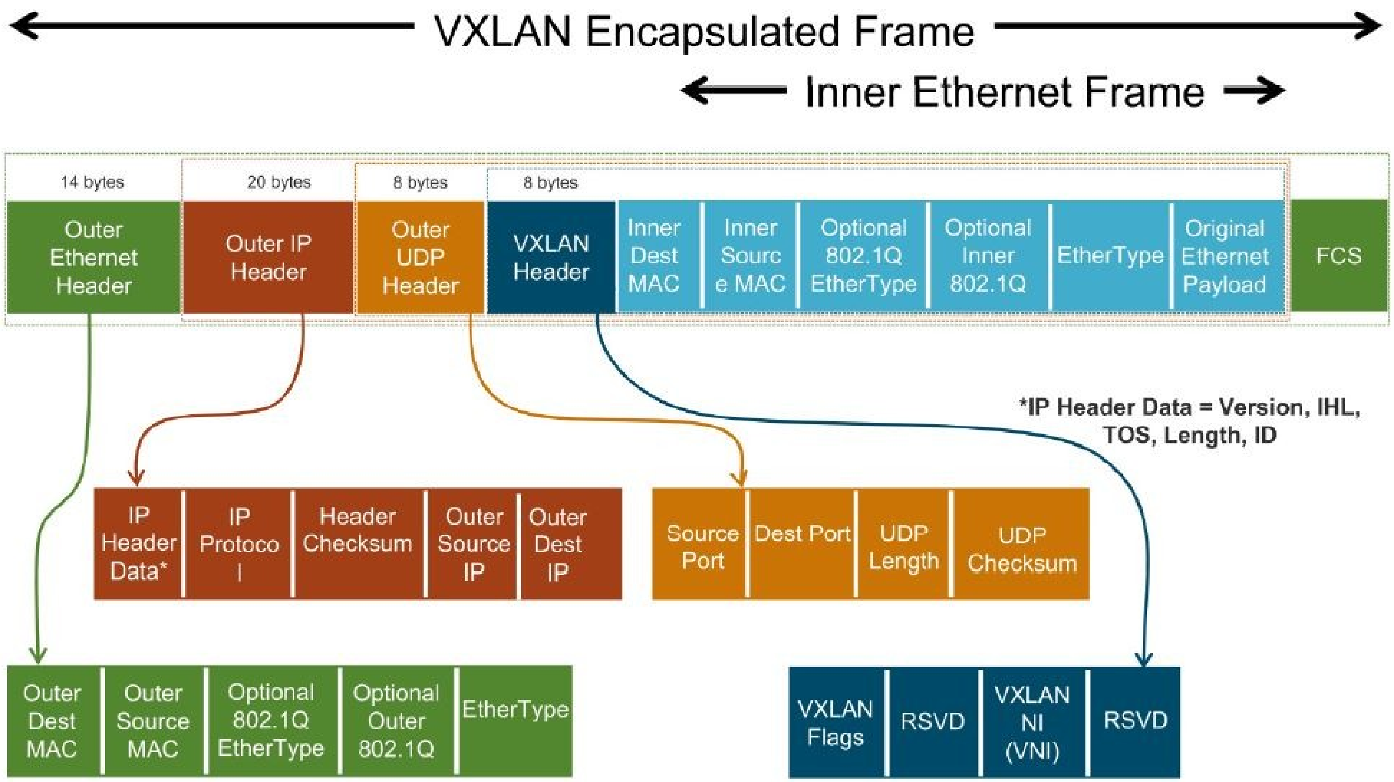
- Layer 2 and Layer 3 traffic should share the same physical link!
  - The layer 3 link is replaced by an Interconnection/Core VLAN.
- Interconnection/Core VLANs
  - VLAN used only for interconnection between local-VLANs.
  - Allows the mixture of VLAN segmentation models.
- Interconnection trunks should allow ONLY:
  - Ends-to-end VLANS
  - Interconnection/Core VLANs
- Exchange of routing information **<u>should</u>** only be done through the interconnection VLAN.
  - Other VLAN should be *passive-interfaces* for the routing processes.




VLAN 101 is the interconnection VLAN.

# Virtual Extensible LAN (VXLAN)

- Encapsulates OSI Layer 2 Ethernet frames within Layer 4 UDP datagrams.
  - Default port 4789.
- Alternative to 802.1Q.



# Spanning Tree Protocol

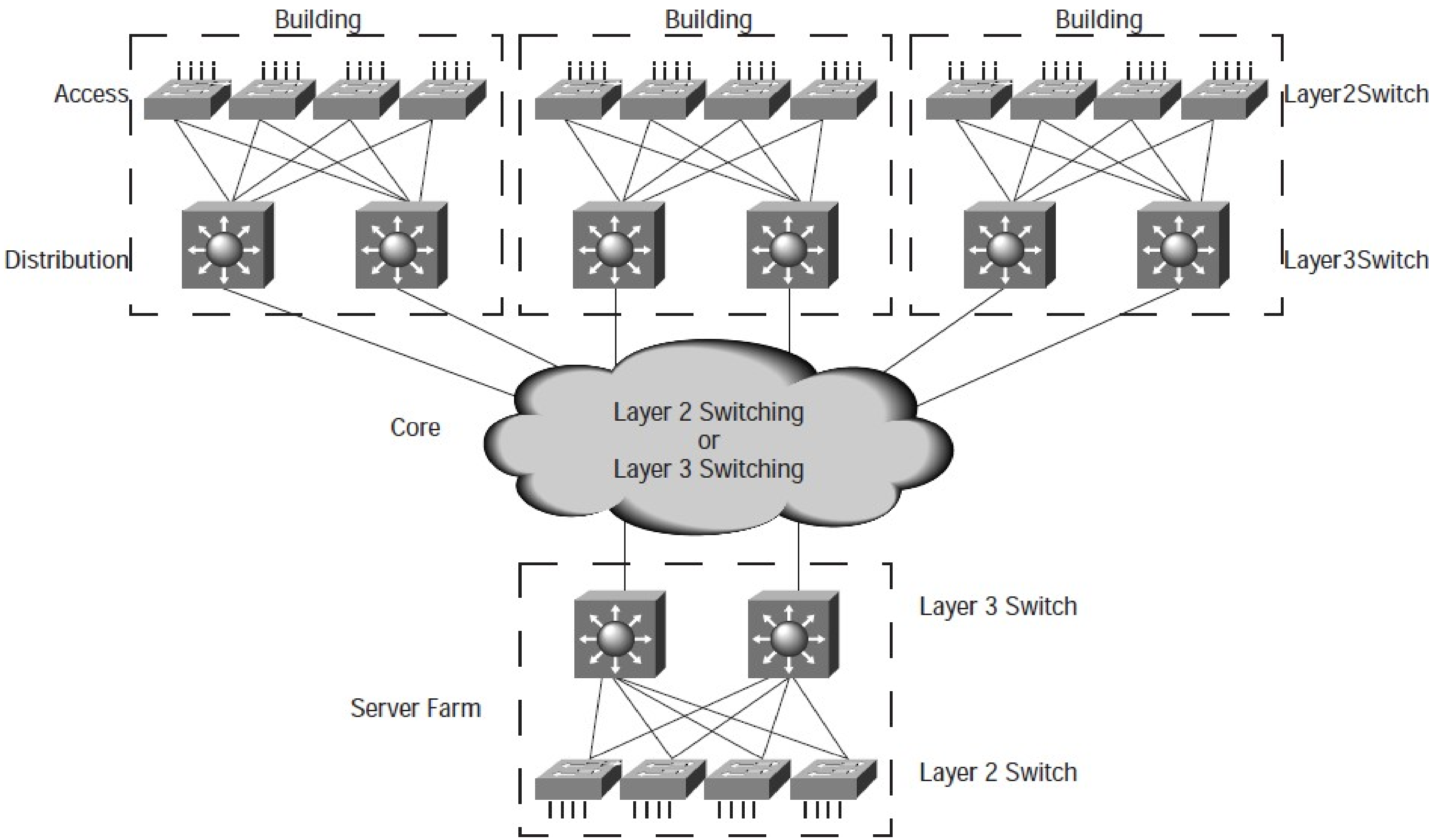
- STP enables the network to deterministically block interfaces and provide a loop-free topology in a network with redundant links.
- There are several STP Standards and Features:
  - STP is the original IEEE 802.1D version (802.1D-1998) that provides a loop-free topology in a network with redundant 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

universidade de aveiro

deti.ua.pt

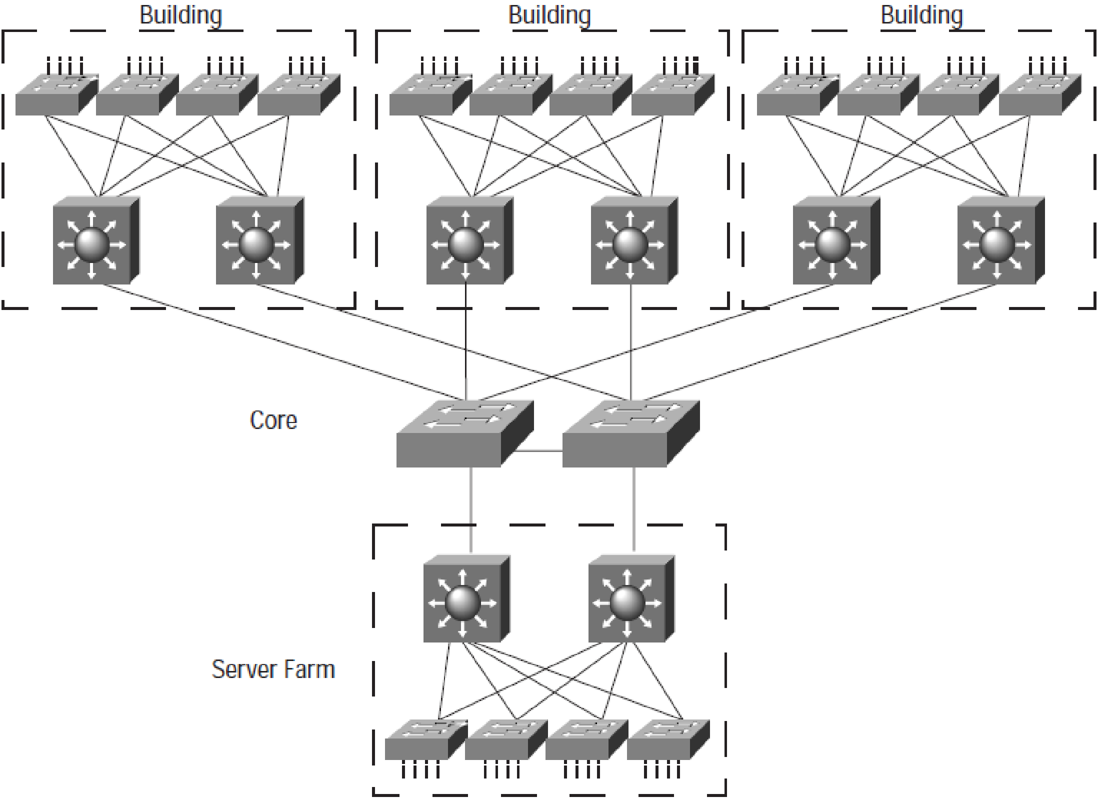
# Layer 2 vs. Layer 3 Core



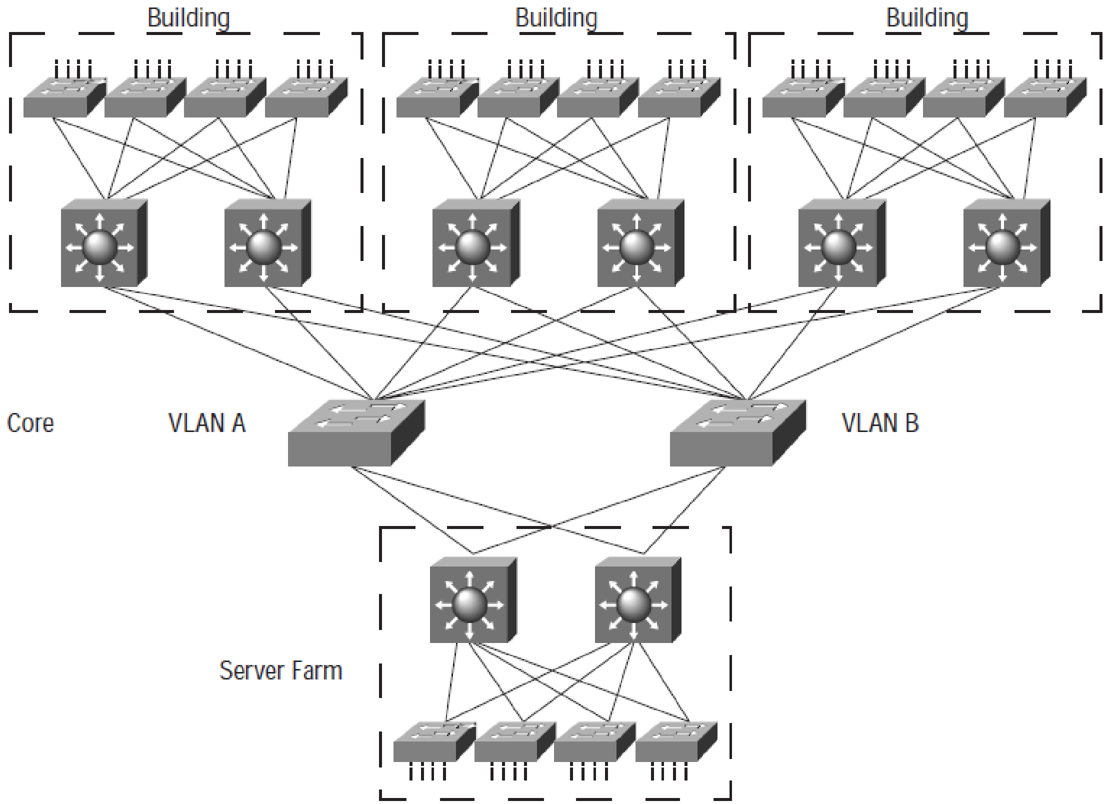

- Layer 3 switched backbones have several advantages:
  - Reduced router peering.
  - Flexible topology with no spanning-tree loops.
  - Multicast and broadcast control in the backbone.
  - Scalability to arbitrarily large size.

# Layer 2 Switched Core

## Single VLAN



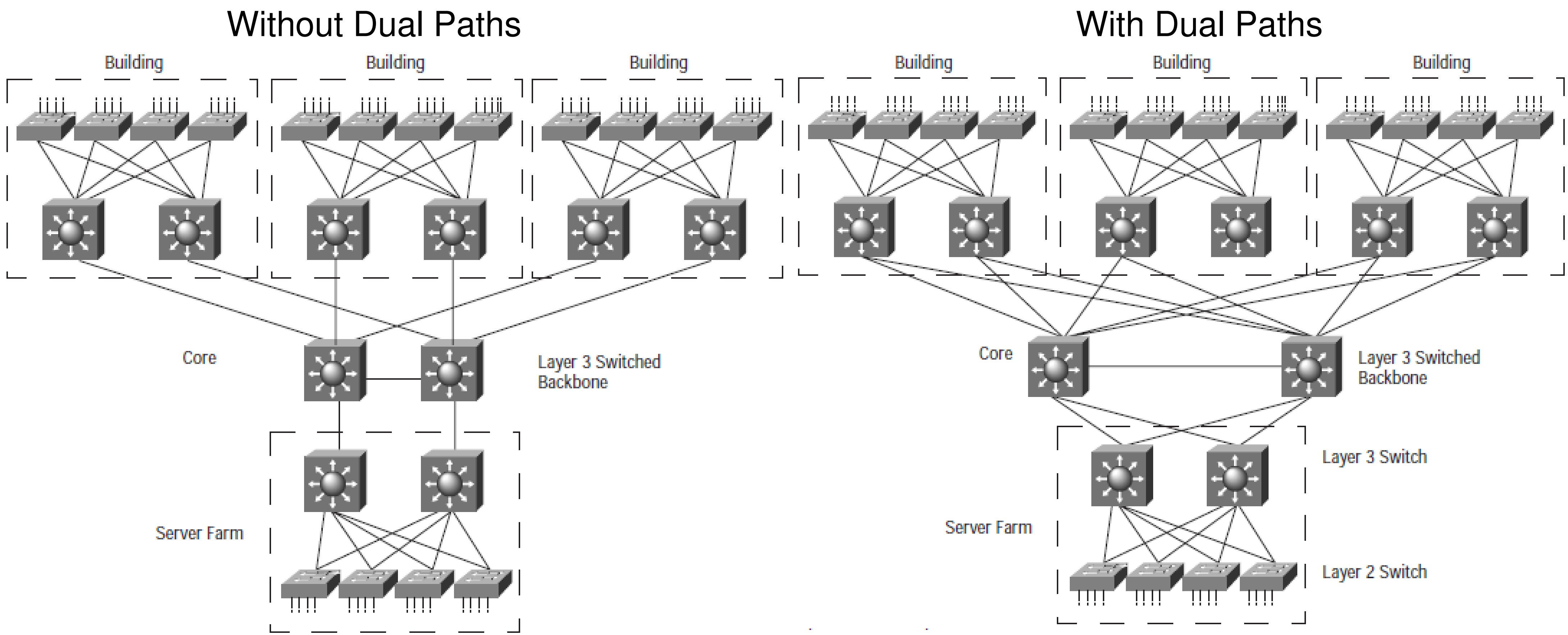

## Split Layer 2




- 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



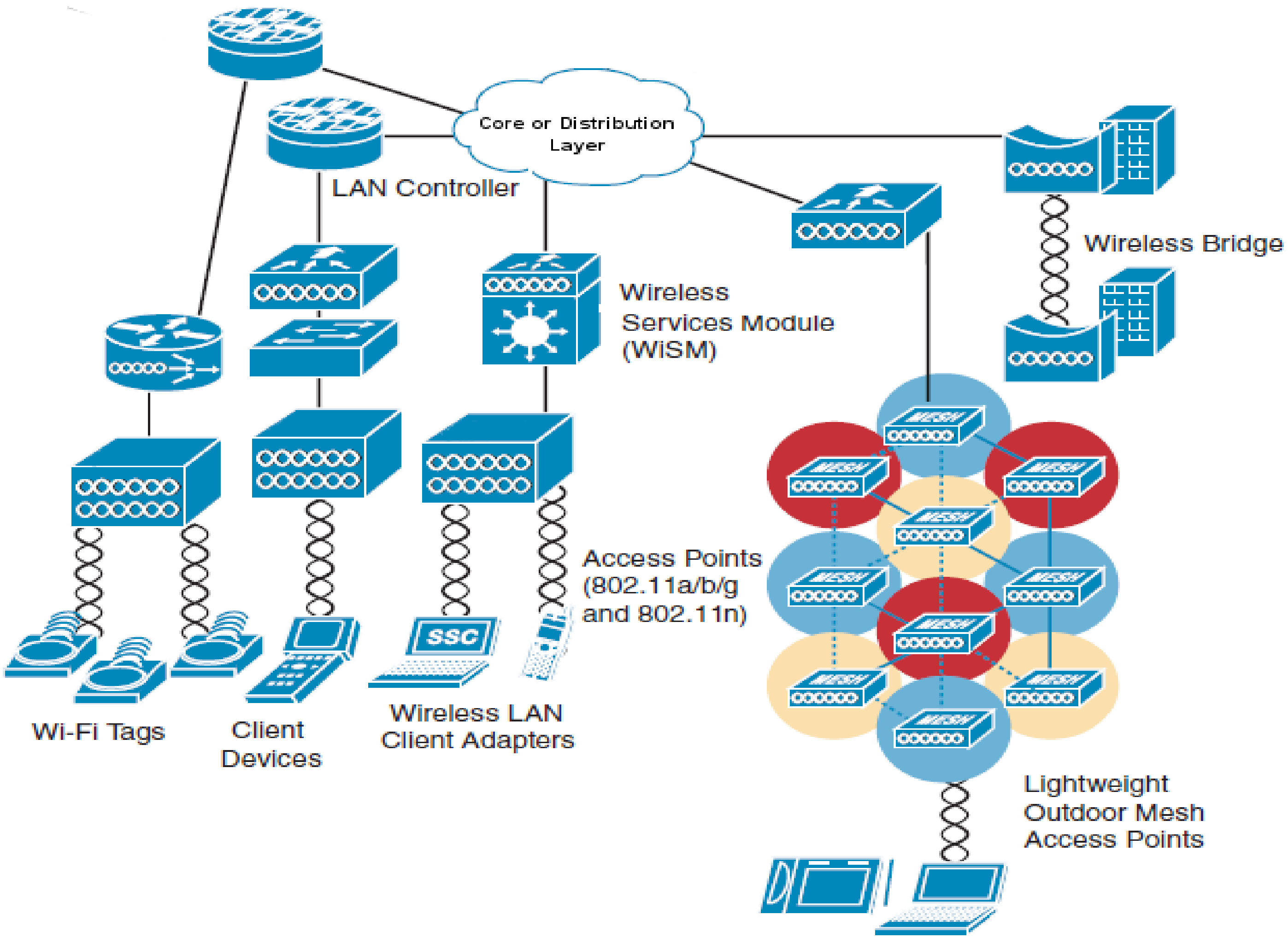

- The main advantage of a Layer 3 Core with dual paths design is that each distribution-layer switch maintains two equal-cost paths to every destination network.
  - Recovery from any link failure is fast.
  - Provides double the bandwidth capacity into the core.
- The inter-connection between the access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

# Implementation of Local and End-to-End VLANs

- End-to-End VLANs are switched at Layer 3 Distribution and Core Switches.
  - Allowed over core trunks.
  - Routing protocol “should be passive” in end-to-end VLANs.
    - Announces network, does not provide routing path.
- Local VLAN are routed over Core (Interconnection) VLANs.
  - Local VLANs are not allowed over core trunks.
  - Core (Interconnection) VLANs are allowed over core trunks and run routing protocol.

# Wireless / Wired Networks Interconnection

# Wireless Network(s)

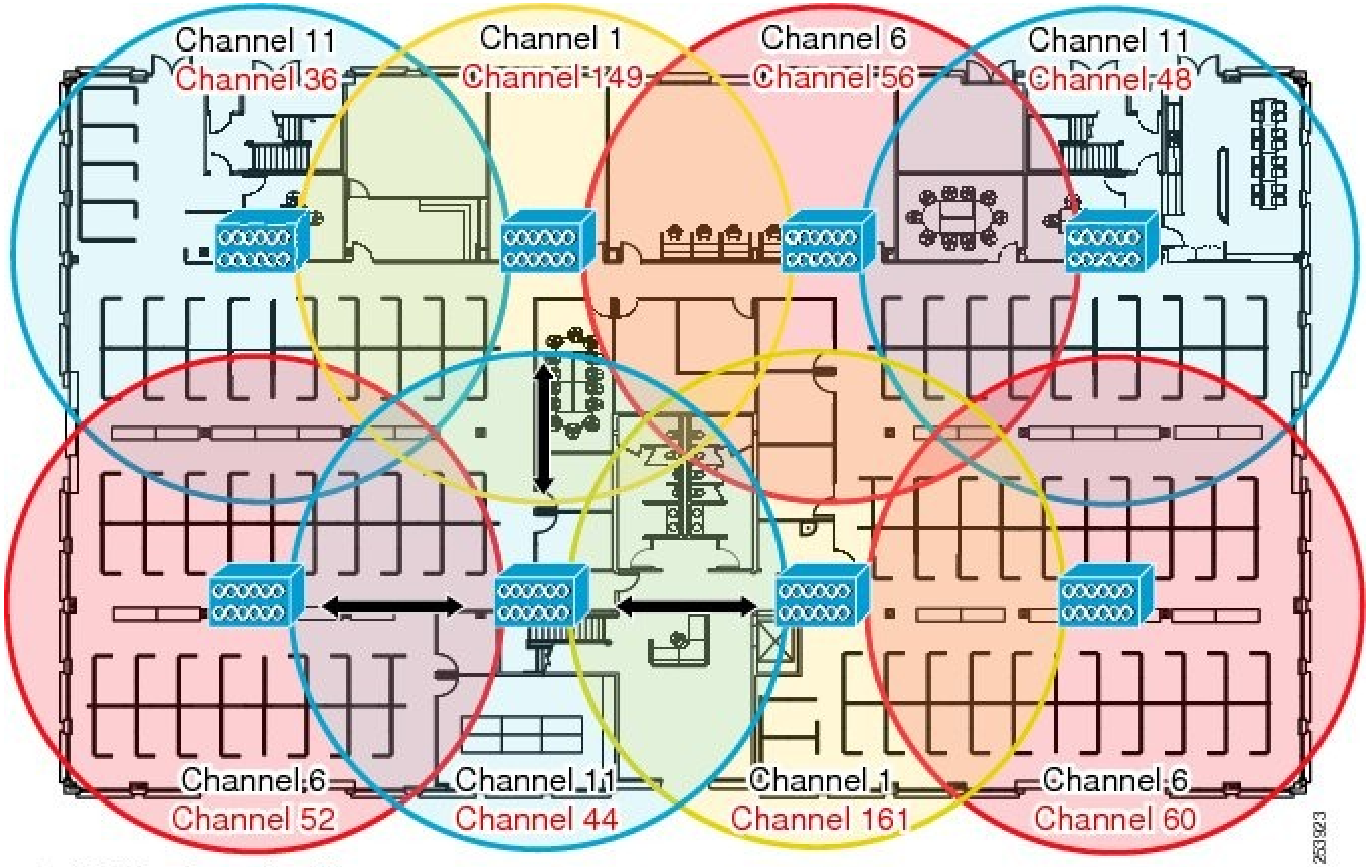



- Wireless networking technologies should have an integration point at core or distribution layers.
- In terms of network architecture a WLAN can be seem as any LAN.
  - Except that we have mobility and must have seamless roaming while moving.
- A large number of AP can be managed by a (Wireless) LAN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

# VLANs on Access Points

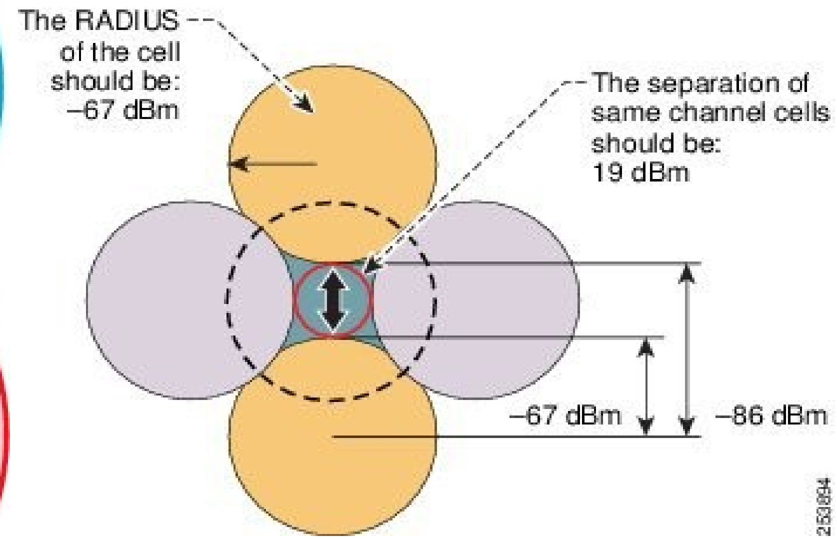
- AP have trunk ports to distribution/core switches.
- “Wired” VLANs must/can be extended to the wireless domain.
  - e.g., VLAN 30 “Green” and VLAN 10 “Red”.
- Each SSID can be mapped to a VLAN.
  - Different SSID/VLAN can have different  security policies.
- Wireless VLANs should be configured as end-to-end.
  - 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.

# AP Placement and Channel Allocation




2.4 GHz channel cells
5 GHz channel cells

Minimum of 20% Overlap




- 802.11n or 802.11ac 5GHz deployment does not have the overlap or collision domain issues of 2.4GHz.

# Equipment/Network
# High-level Dimensioning

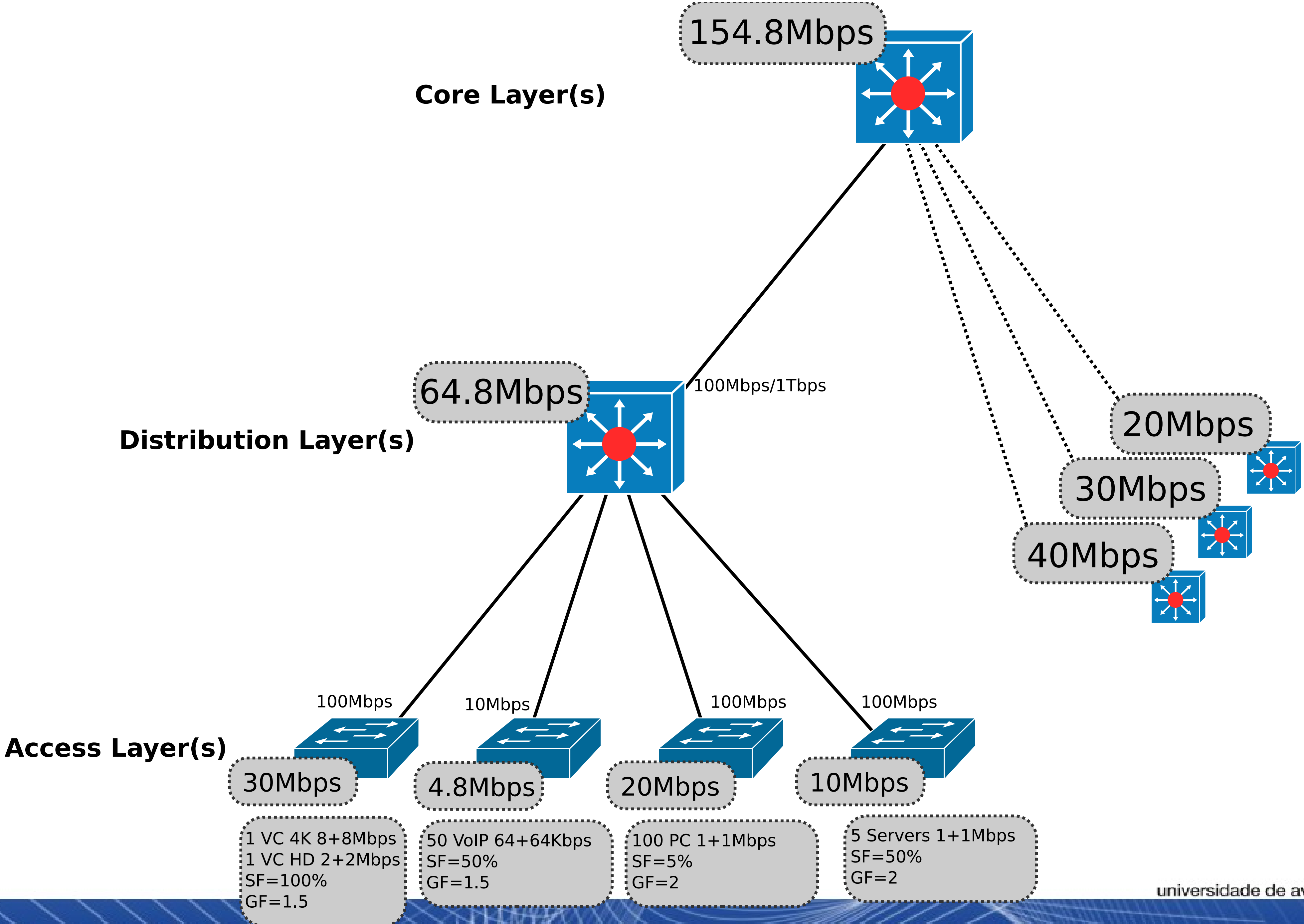
# Traffic Bandwidth Requirements (1)

- Determination of minimum equipment performance in terms of forwarding/routing speed.
  - Usually, express in terms of bits per second (bps) or packets per second (pps)
  - $P_{pps}=P_{bps}/MPS$
    - MPS→ Mean Packet Size in bits.
- Aggregated traffic requirements: $A_{bps}=N*F_{bps}*SF*GF$
  - N → Number of terminals.
  - $F_{bps}$ → Upload+Download traffic requirements (bps)
  - SF → Simultaneity Factor (or diversity factor)
    - Probability that a particular equipment/user will generate traffic coincidentally (in time) with another equipment/user.
  - GF → Growing Factor (or slack factor)
    - Factor by which the traffic may grow at medium-term.
      - May depend on number of users, user behavior, and application protocols/behaviors

# Traffic Bandwidth Requirements (2)

- At each layer, an equipment must be ablr to process all traffic from all equipment connected to him in the lower layers.
  - May be considered an additional Slack Factor.
- Aggregated traffic requirements for layer i, section j:
  - $A_{i,j}$=sum($A_{i-1,j'}$), for all lower layer j' sections connected to section j of the upper layer.
- Most parameters are subjective (and result mainly from empirical analysis) and depend on many technical and management factors.
  - In networks with a monitoring history may be possible to infer/extrapolate current and future values/behaviors more accurately.

# Example


154.8Mbps
Core Layer(s)
64.8Mbps
100Mbps/1Tbps
Distribution Layer(s)
20Mbps
30Mbps
40Mbps
100Mbps
10Mbps
100Mbps
100Mbps
Access Layer(s)
30Mbps
4.8Mbps
20Mbps
10Mbps
1 VC 4K 8+8Mbps
1 VC HD 2+2Mbps
SF=100%
GF=1.5
50 VoIP 64+64Kbps
SF=50%
GF=1.5
100 PC 1+1Mbps
SF=5%
GF=2
5 Servers 1+1Mbps
SF=50%
GF=2

# 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)