Chapter 2: Network Design Fundamentals

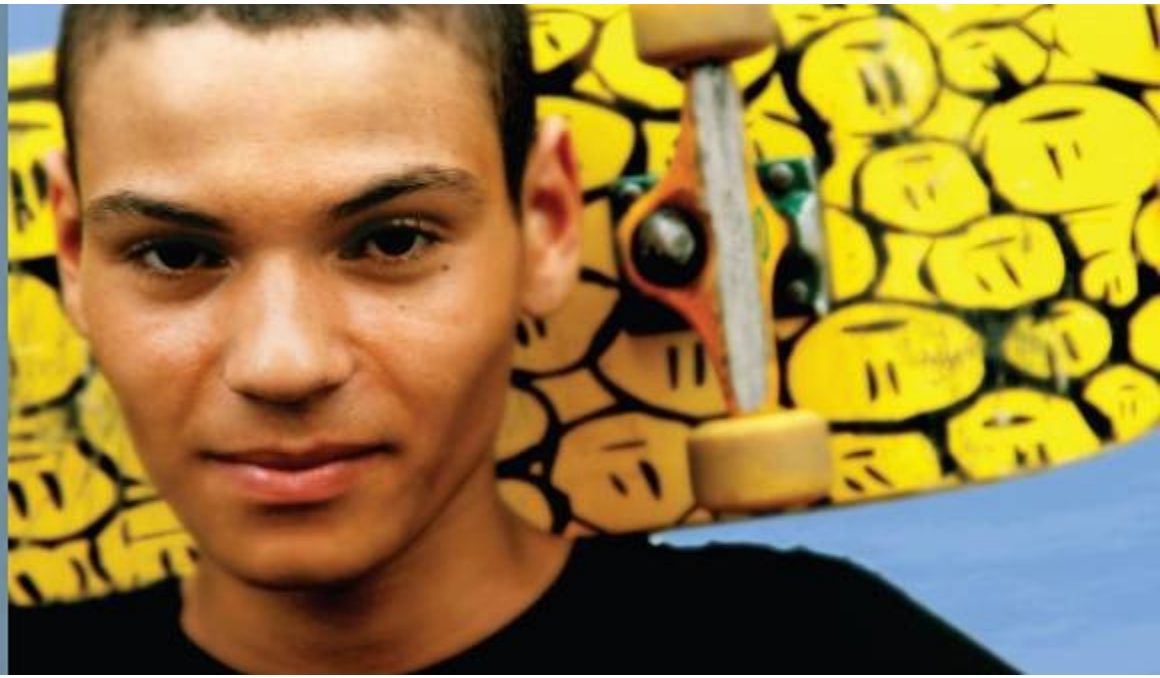
CCNP SWITCH: Implementing Cisco IP Switched Networks

Cisco | Networking Academy®
Mind Wide Open™

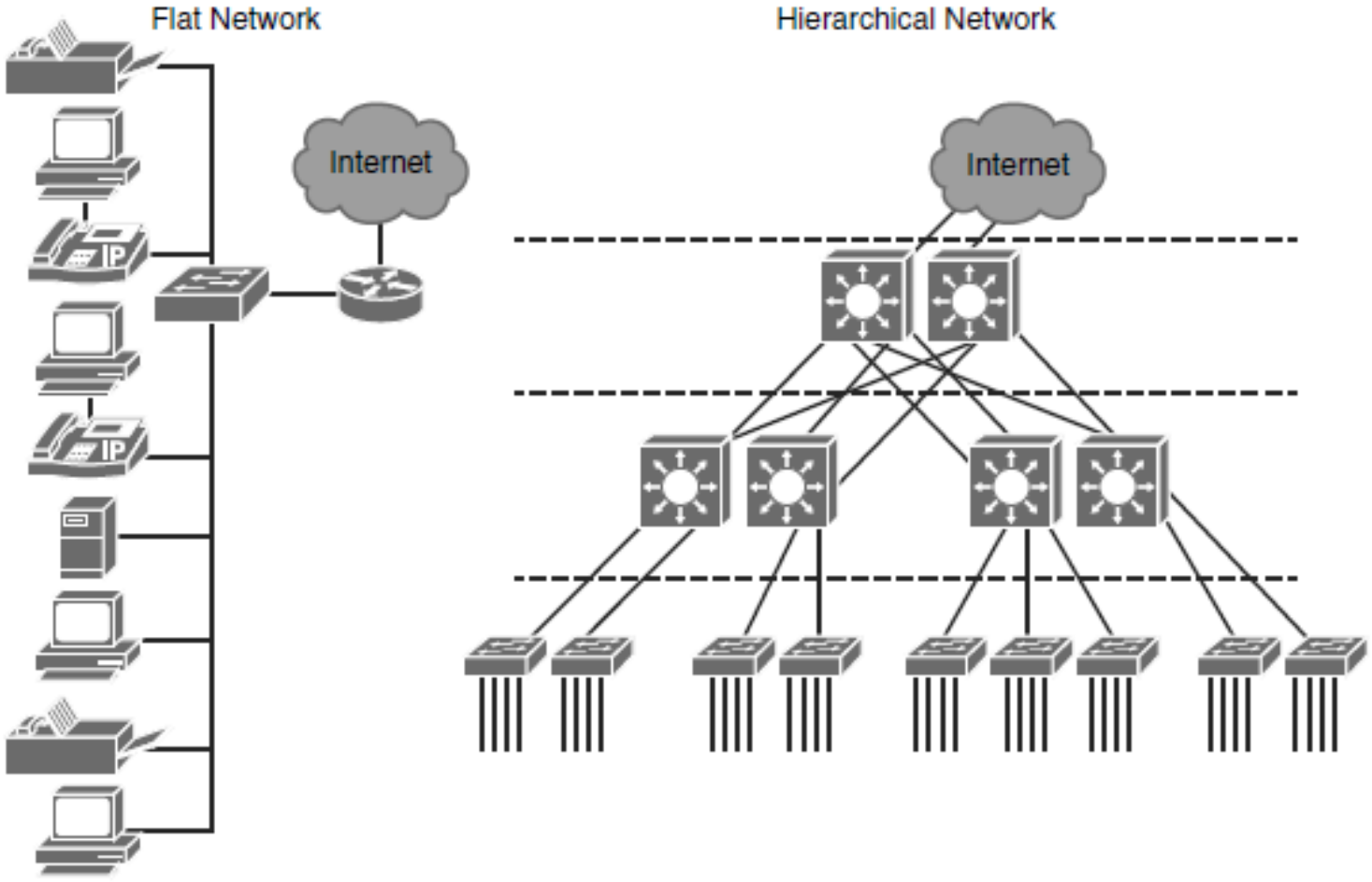
Chapter 2 Objectives

- Campus network structure
- Introduction to Cisco switches and their associated architecture

Campus Network Structure



Hierarchical Network Design

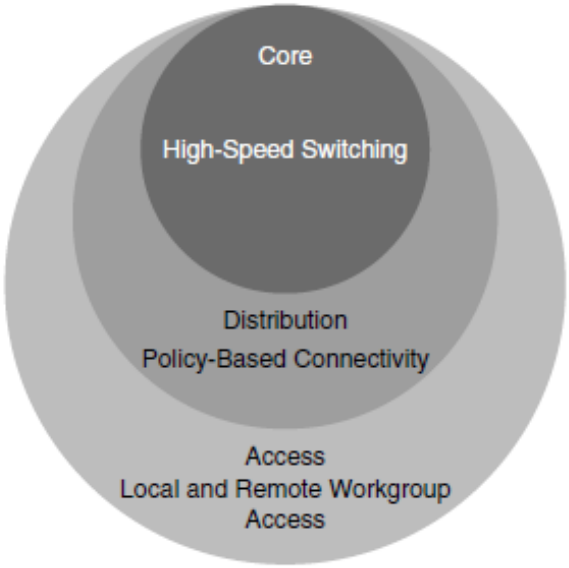


Flat Network Design

- A flat enterprise campus network is where all PCs, servers, and printers are connected to each other using Layer 2 switches.
- A flat network does not use subnets for any design purposes. In addition, all devices on this subnet are in the same broadcast domain, and broadcasts will be flooded to all attached network devices.
- Wasting bandwidth and computational resources.
- Flat networks do not scale to meet the needs of most enterprise networks or of many small and medium-size businesses.

Hierarchical Network Design

- Hierarchical Model

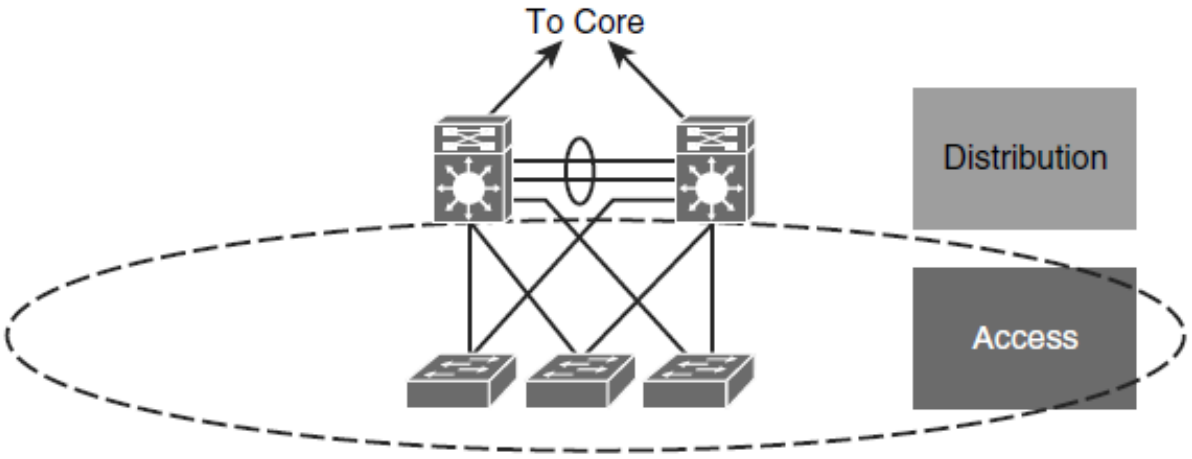


- Hierarchical models for network design allow you to design any networks in layers.
- Leveraging the hierarchical model also simplifies campus network design by allowing focus at different layers that build on each other.
- The layers of the hierarchical model are divided into specific functions categorized as **core**, **distribution**, and **access layers**.
- This categorization provides for modular and flexible design, with the ability to grow and scale the design without major modifications or reworks.

Hierarchical Model Layers

- **Access layer**
  - The access layer is used to grant the user access to network applications and functions. In a campus network, the access layer generally incorporates switched LAN devices with ports that provide connectivity to workstations, IP phones, access points, and printers. In a WAN environment, the access layer for teleworkers or remote sites may provide access to the corporate network across WAN technologies.
- **Distribution layer**
  - The distribution layer aggregates the access layer switches wiring closets, floors, or other physical domain by leveraging module or Layer 3 switches.
  - Similarly, a distribution layer may aggregate the WAN connections at the edge of the campus and provides policy-based connectivity.
- **Core layer (also referred to as the backbone)**
  - The core layer is a high-speed backbone, which is designed to switch packets as fast as possible. In most campus networks, the core layer has routing capabilities.
  - Because the core is critical for connectivity, it must provide a high level of availability and adapt to changes quickly. It also provides for dynamic scalability to accommodate growth and fast convergence in the event of a failure.

Access Layer



- Describes the logical grouping of the switches that interconnect end devices such as PCs, printers, cameras, and so on.
- It is also the place where devices that extend the network out one more level are attached.
- Two such prime examples are IP phones and wireless APs, both of which extend the connectivity out one more layer from the actual campus access switch.

Access Layer Capabilities

- **High availability**
  - The access layer supports high availability via default gateway redundancy using dual connections from access switches to redundant distribution layer switches when there is no routing in the access layer. This mechanism behind default gateway redundancy is referred to as *first-hop redundancy protocol* (FHRP).
- **Convergence**
  - The access layer generally supports inline Power over Ethernet (PoE) for IP telephony, thin clients, and wireless access points (APs).
  - In addition, the access layers allow support for converged features that enable optimal software configuration of IP phones and wireless APs, as well.
- **Security**
  - The access layer also provides services for additional security against unauthorized access to the network by using tools such as **port security**, **QoS, DHCP snooping, DAI, and IP Source Guard**.

Dynamic ARP inspection (DAI)

- DAI je bezpečnostní funkce, která odmítá neplatné a škodlivé pakety ARP. Tato funkce zabraňuje třídě útoků typu MitM, kde nepřátelská stanice zachycuje provoz na jiných stanicích tím, že otráví paměť ARP svých nic netušících sousedů a chytá pakety s cizí IP adresou na svoji MAC adresu.

- DAI se spoléhá na DHCP snooping. DHCP snooping naslouchá výměnám zpráv DHCP a sestavuje databázi vazeb platných trojic (MAC adresa, IP adresa, rozhraní VLAN).

- Je-li zapnutá funkce DAI, přepínač přeruší paket ARP, pokud adresa MAC odesílatele a adresa IP odesílatele neodpovídají položce v databázi vazeb **DHCP snooping**.

- Nicméně, to může být překonáno **statickým mapováním**. Statické mapování je užitečné např. tehdy, když jiné přepínače v síti nevykonávají DARP.

DHCP snooping – arp inspection trust

(SW1) (Config)# ip dhcp snooping

(SW1) (Config)# ip dhcp snooping vlan

(SW1) (Config)# interface 1/0/1
(SW1) (Interface 1/0/1)# ip dhcp snooping trust
(SW1) (Interface 1/0/1)# sh ip dhcp snooping bind

MAC Address	IP Address	VLAN	Interface	Type	Lease (Secs)
00:16:76:A7:88:CC	192.168.10.86	1	1/0/2	DYNAMIC	86400

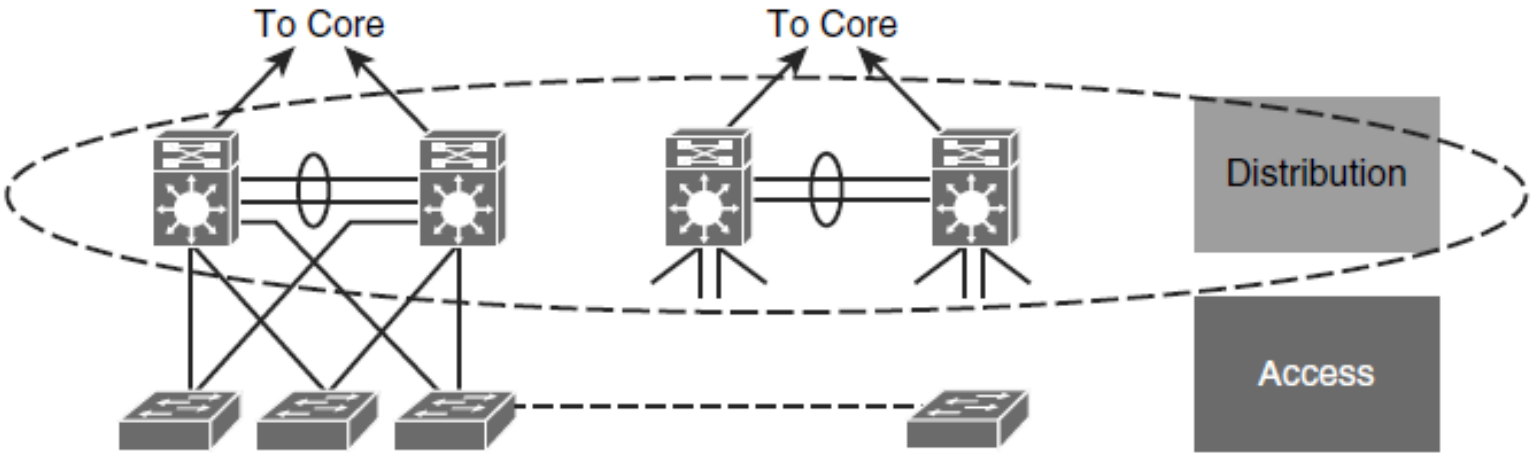
(SW1) (Config)# ip arp inspection vlan 1

(SW1) (Config)# interface 1/0/1
(SW1) (Interface 1/0/1)# ip arp inspection trust

ARP spoofing

```
root@kali:~# arpspoof -i eth0 -t 192.168.10.100 192.168.10.250
0:c:29:c8:11:e aa:bb:cc:0:9:0 0806 42: arp reply 192.168.10.250 is-at 0:c:29:c8:11:e
0:c:29:c8:11:e aa:bb:cc:0:9:0 0806 42: arp reply 192.168.10.250 is-at 0:c:29:c8:11:e
0:c:29:c8:11:e aa:bb:cc:0:9:0 0806 42: arp reply 192.168.10.250 is-at 0:c:29:c8:11:e
0:c:29:c8:11:e aa:bb:cc:0:9:0 0806 42: arp reply 192.168.10.250 is-at 0:c:29:c8:11:e
0:c:29:c8:11:e aa:bb:cc:0:9:0 0806 42: arp reply 192.168.10.250 is-at 0:c:29:c8:11:e
0:c:29:c8:11:e aa:bb:cc:0:9:0 0806 42: arp reply 192.168.10.250 is-at 0:c:29:c8:11:e
0:c:29:c8:11:e aa:bb:cc:0:9:0 0806 42: arp reply 192.168.10.250 is-at 0:c:29:c8:11:e
0:c:29:c8:11:e aa:bb:cc:0:9:0 0806 42: arp reply 192.168.10.250 is-at 0:c:29:c8:11:e
0:c:29:c8:11:e aa:bb:cc:0:9:0 0806 42: arp reply 192.168.10.250 is-at 0:c:29:c8:11:e
0:c:29:c8:11:e aa:bb:cc:0:9:0 0806 42: arp reply 192.168.10.250 is-at 0:c:29:c8:11:e
0:c:29:c8:11:e aa:bb:cc:0:9:0 0806 42: arp reply 192.168.10.250 is-at 0:c:29:c8:11:e
0:c:29:c8:11:e aa:bb:cc:0:9:0 0806 42: arp reply 192.168.10.250 is-at 0:c:29:c8:11:e
0:c:29:c8:11:e aa:bb:cc:0:9:0 0806 42: arp reply 192.168.10.250 is-at 0:c:29:c8:11:e
0:c:29:c8:11:e aa:bb:cc:0:9:0 0806 42: arp reply 192.168.10.250 is-at 0:c:29:c8:11:e
0:c:29:c8:11:e aa:bb:cc:0:9:0 0806 42: arp reply 192.168.10.250 is-at 0:c:29:c8:11:e
0:c:29:c8:11:e aa:bb:cc:0:9:0 0806 42: arp reply 192.168.10.250 is-at 0:c:29:c8:11:e
0:c:29:c8:11:e aa:bb:cc:0:9:0 0806 42: arp reply 192.168.10.250 is-at 0:c:29:c8:11:e
0:c:29:c8:11:e aa:bb:cc:0:9:0 0806 42: arp reply 192.168.10.250 is-at 0:c:29:c8:11:e
```

Distribution Layer



- The distribution layer in the campus design has a unique role in which it acts as a services and control boundary between the access layer and the core.
- Availability, fast path recovery, load balancing, and QoS are all important considerations at the distribution layer.
- Generally, high availability is provided through Layer 3 redundant paths from the distribution layer to the core, and either Layer 2 or Layer 3 redundant paths from the access layer to the distribution layer.

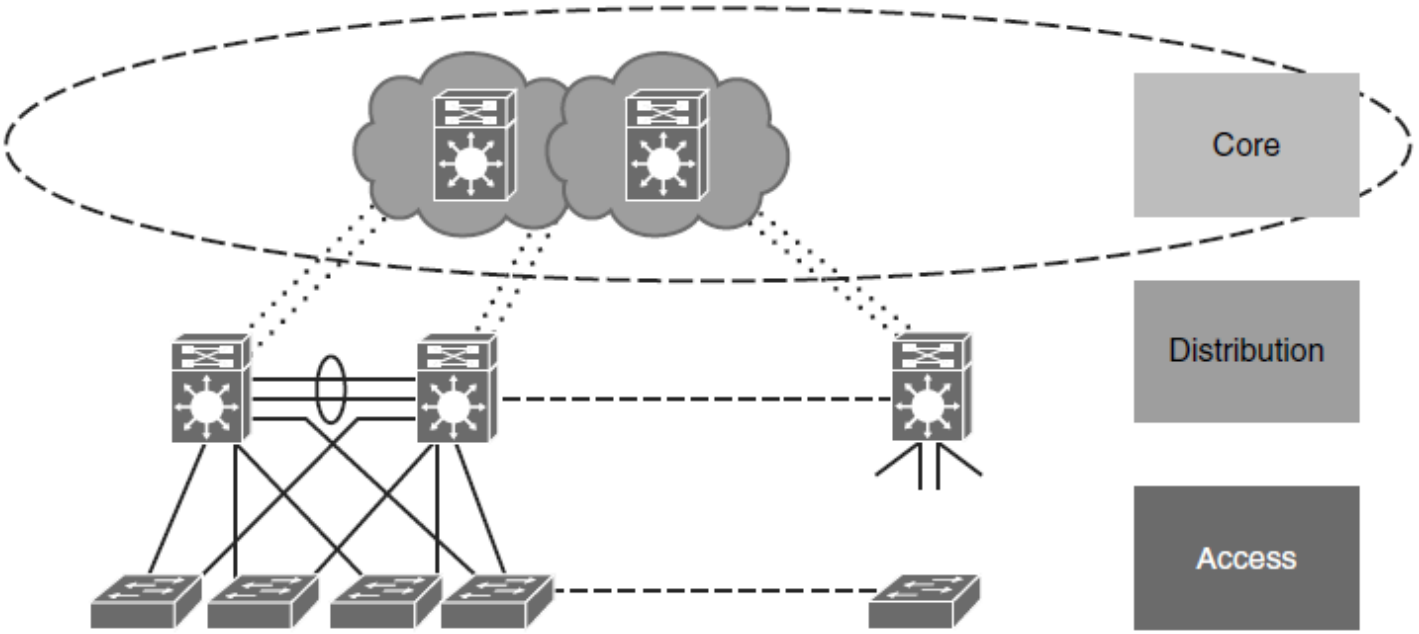
Distribution Layer

- With a Layer 2 design in the access layer, the distribution layer generally serves as a routing boundary between the access and core layer by terminating VLANs.
- The distribution layer may perform tasks such as controlled routing decision making and filtering to implement policy-based connectivity, security, and QoS.
- These features allow for tighter control of traffic through the campus network.
- To improve routing protocol performance further, the distribution layer is generally designed to summarize routes from the access layer.
- In addition, the distribution layer optionally provides default gateway redundancy by using a first-hop routing protocol (**FHRP**) such as HSRP, GLBP, or VRRP.

Distribution Layer Functions

- Provides high availability and equal-cost load sharing by interconnecting the core and access layer via at least dual paths
- Generally terminates a Layer 2 domain of a VLAN
- Routes traffic from terminated VLANs to other VLANs and to the core
- Summarizes access layer routes
- Implements policy-based connectivity such as traffic filtering, QoS, and security
- Provides for an FHRP

Core Layer (Backbone)

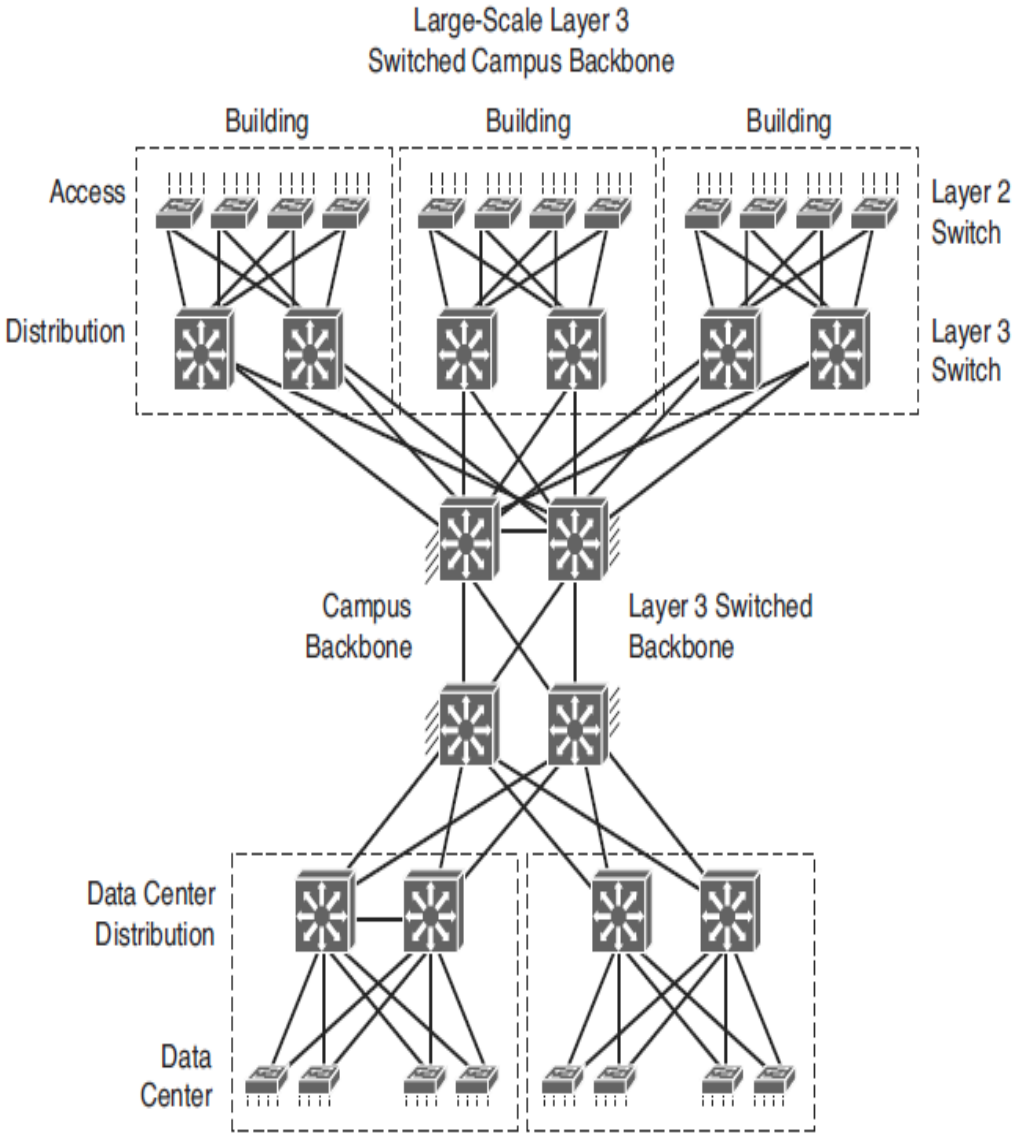


- From a design point-of-view, the campus core is in some ways the simplest yet most critical part of the campus.
- It provides a **limited set of services** and is designed to be highly available and requires 100 percent uptime.
- In large enterprises, the core of the network must operate as a nonstop, always-available service.

Core Layer (Backbone)

- The key design objectives for the campus core are based on providing the appropriate level of redundancy to allow for near-immediate data-flow recovery in the event of the failure of any component (switch, supervisor, line card, or fiber interconnect, power, and so on).
- The network design must also permit the occasional, but necessary, hardware and software upgrade or change to be made without disrupting any network applications.
- The core of the network should not implement any complex policy services, nor should it have any directly attached user or server connections.
- The core should also have the minimal control plane configuration that is combined with highly available devices that are configured with the correct amount of physical redundancy to provide for this nonstop service capability.

Core Layer (Backbone)

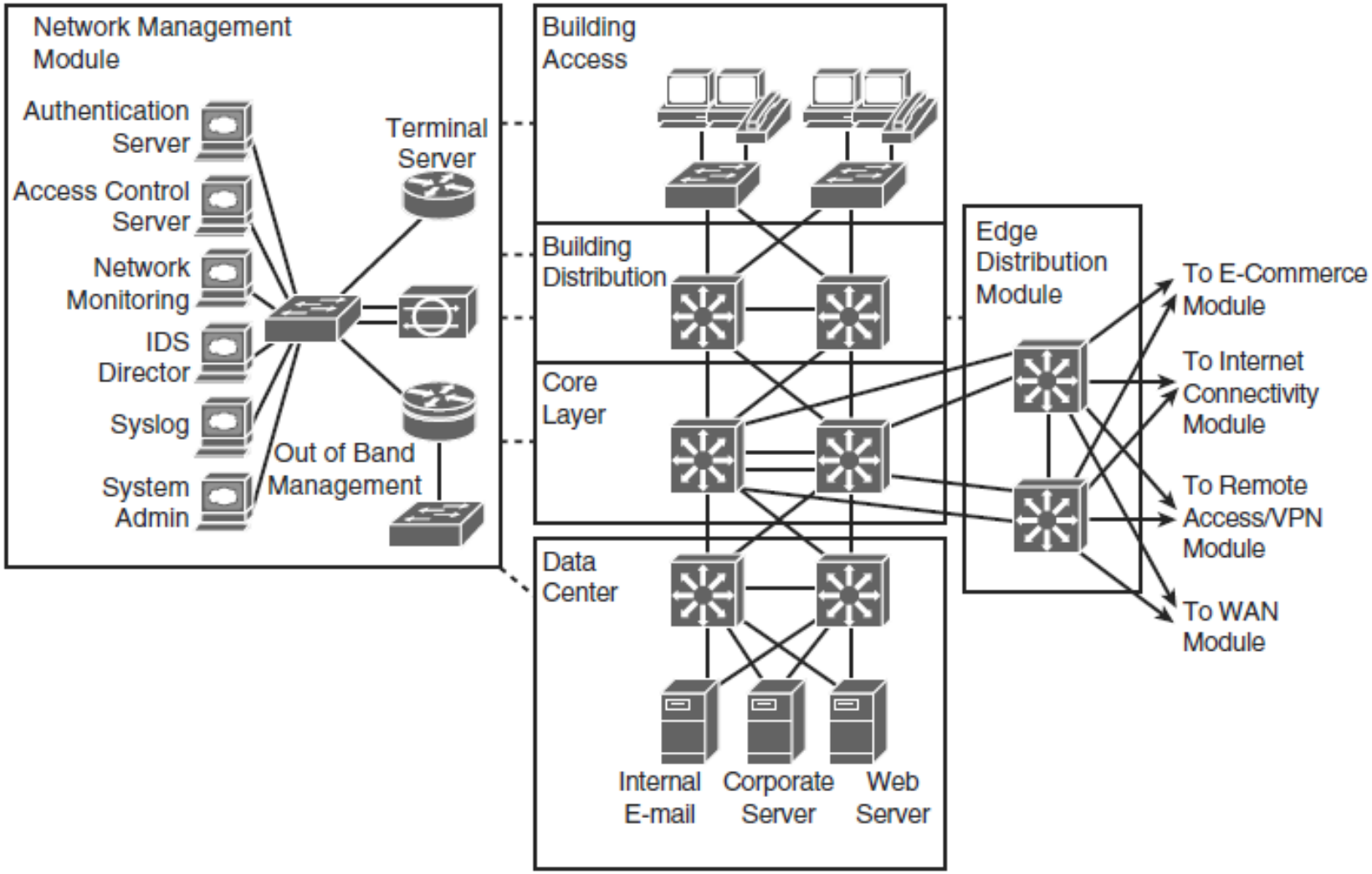


- From an enterprise architecture point-of-view, the campus core is the backbone that binds together all the elements of the campus architecture to include the WAN, the data center, and so on. In other words, the core layer is the part of the network that provides for connectivity between end devices, computing, and data storage services that are located within the data center, in addition to other areas and services within the network.

Core Layer Functions

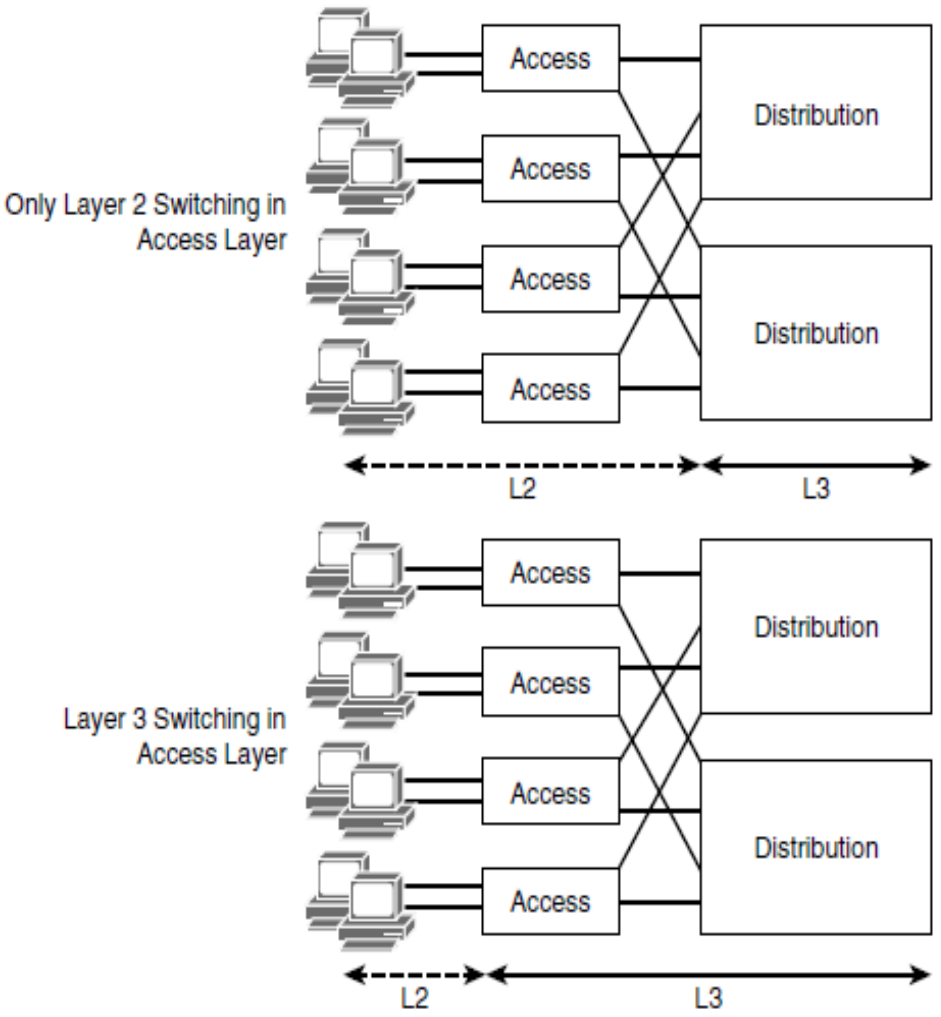
- Aggregates the campus networks and provides interconnectivity to the data center, the WAN, and other remote networks
- Requires high availability, resiliency, and the ability to make software and hardware upgrades without interruption
- Designed without direct connectivity to servers, PCs, access points, and so on
- Requires core routing capability
- Architected for future growth and scalability
- Leverages Cisco platforms that support hardware redundancy such as the Catalyst 4500 and the Catalyst 6800

Core Layer Interconnecting with the Enterprise Network



Layer 3 in the Access Layer

- Because of the reduced cost and a few inherit benefits, Layer 3 switching in the access layer has become more common over typical Layer 2 switching in the access layer.
- Using Layer 3 switching or traditional Layer 2 switching in the access layer has benefits and drawbacks.

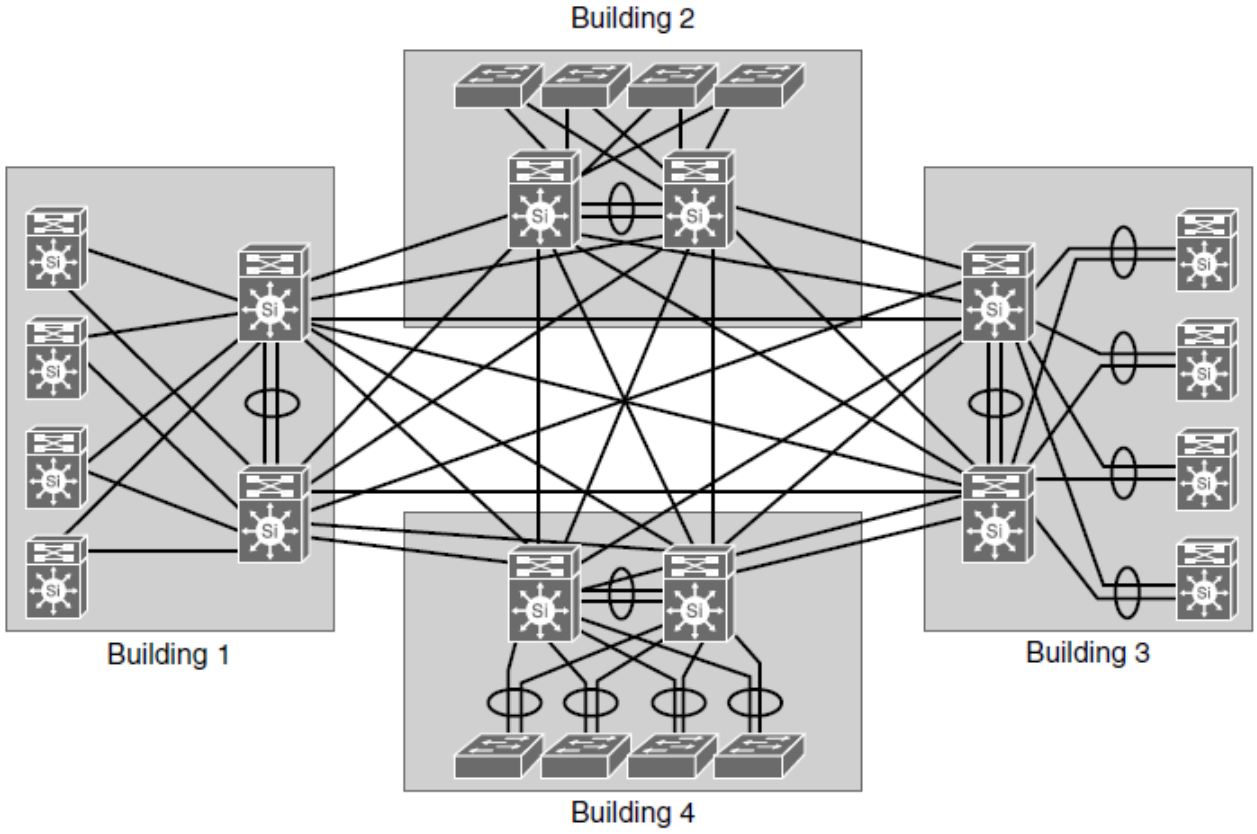


Layer 3 in the Access Layer

- **Benefits**
  - Using a design that leverages Layer 3 switching to the access layer VLANs scales better than Layer 2 switching designs because VLANs get terminated on the access layer devices.
  - Specifically, the links between the distribution and access layer switches are routed links; all access and distribution devices would participate in the routing scheme.
  - The Layer 2-only access design is a traditional, slightly cheaper solution, but it suffers from optimal use of links between access and distribution due to spanning tree
- **Drawbacks**
  - Layer 3 designs introduce the challenge of how to separate traffic.
  - Layer 3 designs also require careful planning with respect to IP addressing.
  - A VLAN on one Layer 3 access device cannot be on another access layer switch in a different part of your network because each VLAN is globally significant.
  - Traditionally, mobility of devices is limited in the campus network of the enterprise in Layer 3 access layer networks. without using an advanced mobility networking features .

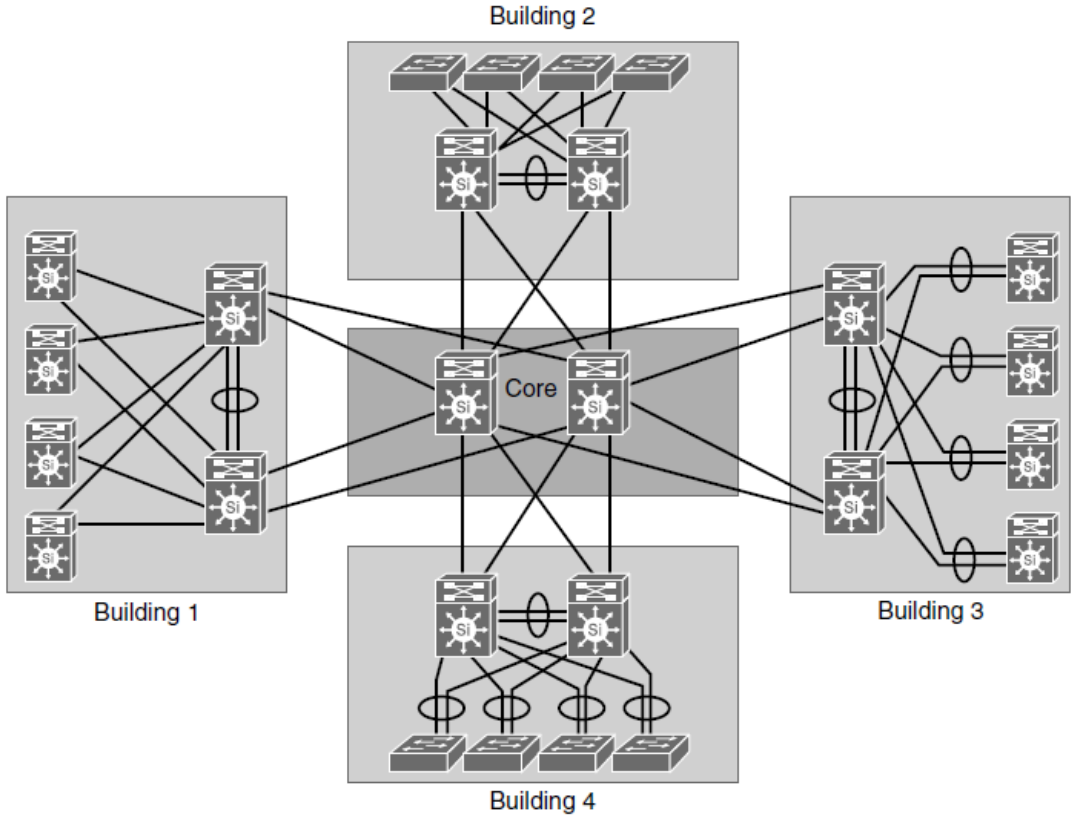
The Need for a Core Layer

- In a campus network contained with a few buildings or a similar physical infrastructure, collapsing the core into the distribution layer switches may save on initial cost because an entire layer of switches is not needed.



The Need for a Core Layer

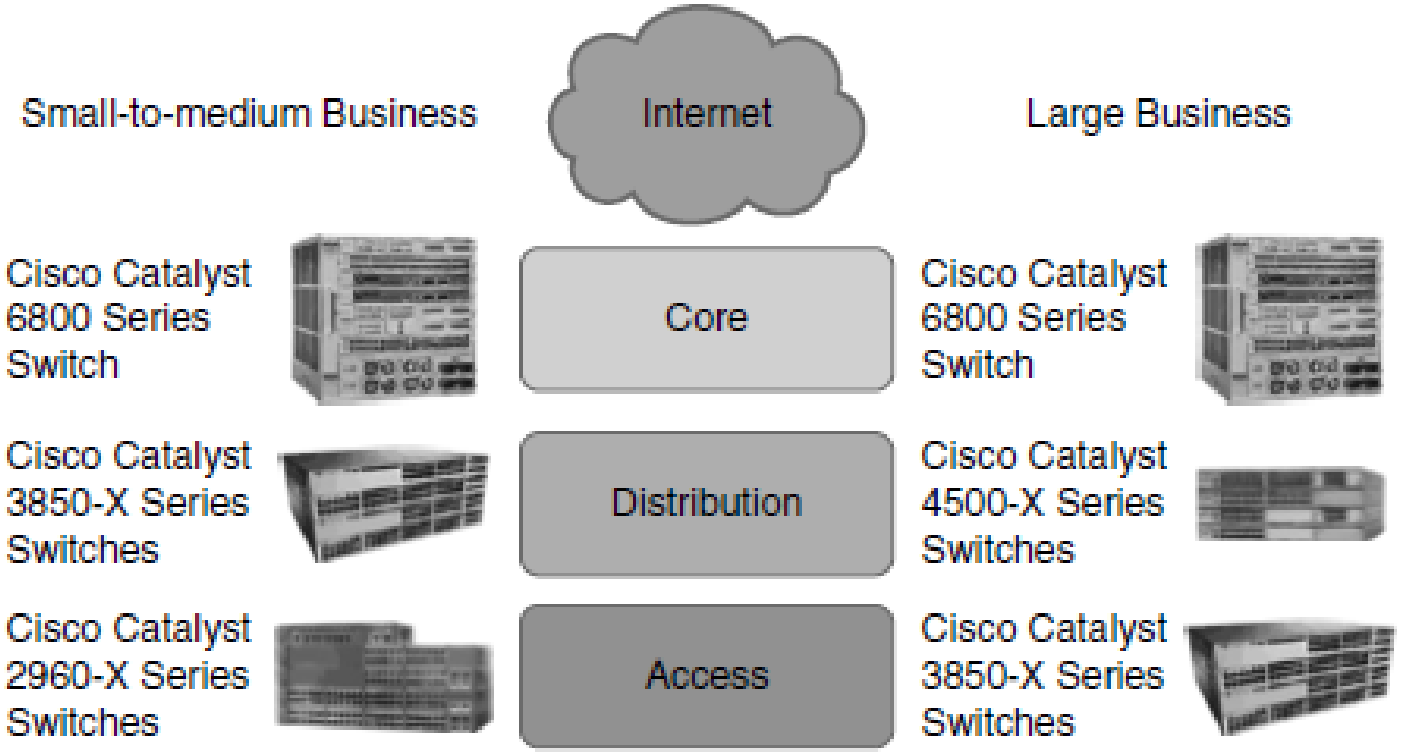
- Despite a possible lower cost to the initial build, this design is difficult to scale. In addition, cabling requirements increase dramatically with each new building because of the need for full-mesh connectivity to all the distribution switches. The routing complexity also increases as new buildings are added because additional routing peers are needed.



Types of Cisco Switches

Types of Cisco Switches

- Cisco designs the Catalyst switches for campus networks and Nexus switches for data centers. The context of CCNP will focus mostly on Catalyst switches.



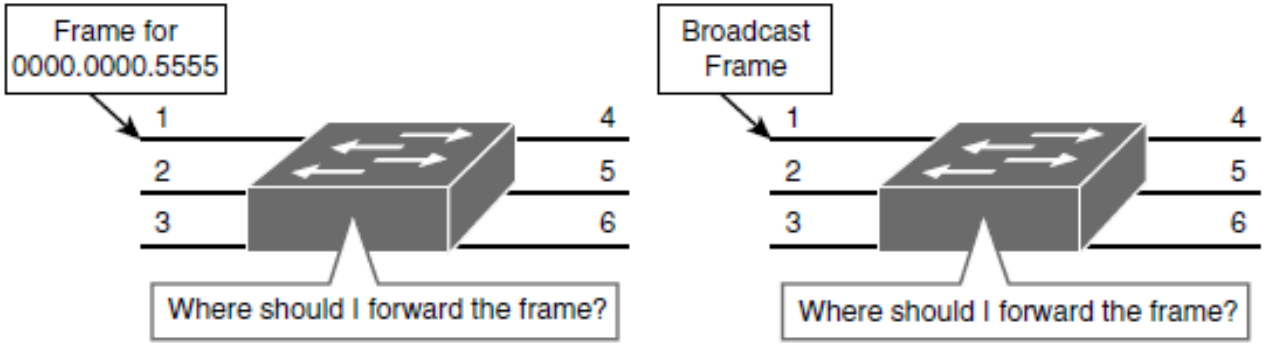
Comparing Layer 2 and Multilayer Switches

- L2 switches make decisions about forwarding frames based on the destination MAC addresses found within the frame.
- When a switch receives in **store-and-forward mode**, the frame is checked for errors, and frames with a valid cyclic redundancy check (CRC) are regenerated and transmitted.
- Some models of switches, mostly Nexus switches, opt to switch frames based only on reading the Layer 2 information and bypassing the CRC check.
- This bypass, referred to as **cut-through switching**, lowers the latency of the frame transmission as the entire frame is not stored before transmission to another port.
- Lower switching latency is beneficial for low-latency applications such as algorithm trading programs found in the data center. The assumption is that the end device network interface card (NIC) or an upper-level protocol will eventually discard the bad frame.
- Most Catalyst switches are store-n-forward.

MAC Address Forwarding

CAM Table

MAC Address	Port	VLAN
0000.0000.1111	1	1
0000.0000.2222	2	1
0000.0000.6666	6	1
0000.0000.5555	5	1
0000.0000.3333	3	20
0000.0000.4444	4	1



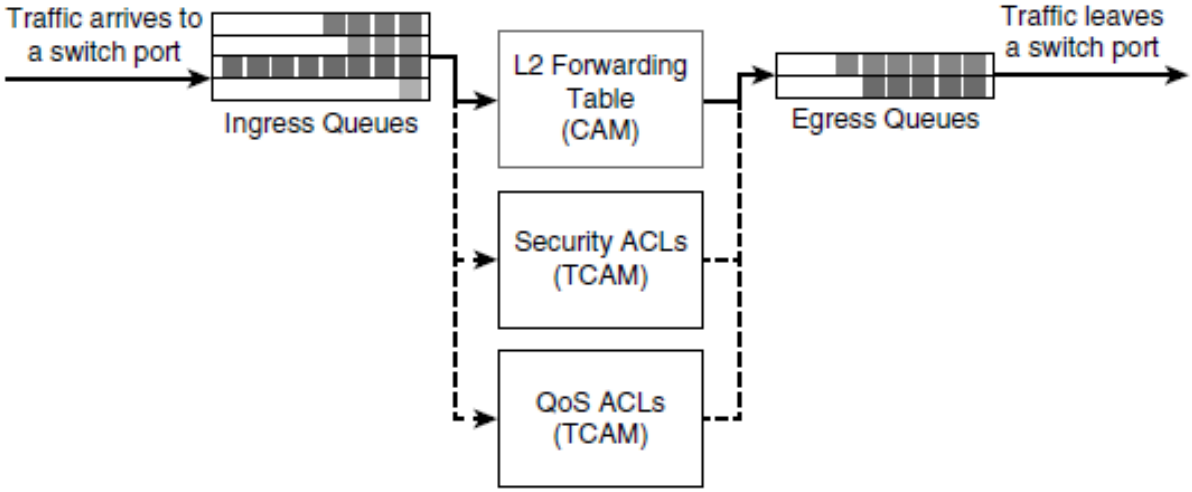
- Where should the frame be forwarded?
- Are there restrictions preventing the forwarding of the frame?
- Is there any prioritization or marking that needs to be applied to the frame?

Layer 2 Switch Operation

- **Layer 2 forwarding table**
  - The Layer 2 forwarding table, also called the *MAC table* , contains information about where to forward the frame. Specifically, it contains MAC addresses and destination ports. The switches reference the destination MAC address of the incoming frame in the MAC table and forward the frames to the destination ports specified in the table. If the MAC address is not found, the frame is flooded through all ports in the same VLAN.
- **ACLs**
  - Access control lists (ACLs) do not only apply to routers. Switches can also apply ACLs based on MAC and IP addresses. Generally only higher-end switches support ACLs based on both MAC and IP addresses, whereas Layer 2 switches support ACLs only with MAC addresses.
- **QoS**
  - Incoming frames can be classified according to QoS parameters. Traffic can then be marked, prioritized, or rate-limited.

Layer 2 Switch Operation

- CAM and TCAM are extremely fast access and allow for line-rate switching performance. CAM supports only two results: 0 or 1.
- Therefore, CAM is useful for Layer 2 forwarding tables.
- TCAM provides three results: 0, 1, and don't care. TCAM is most useful for building tables for searching on longest matches, such as IP routing tables organized by IP prefixes.
- The TCAM table stores ACL, QoS, and other information generally associated with upper-layer processing. As a result of using TCAM, applying ACLs does not affect the performance of the switch.

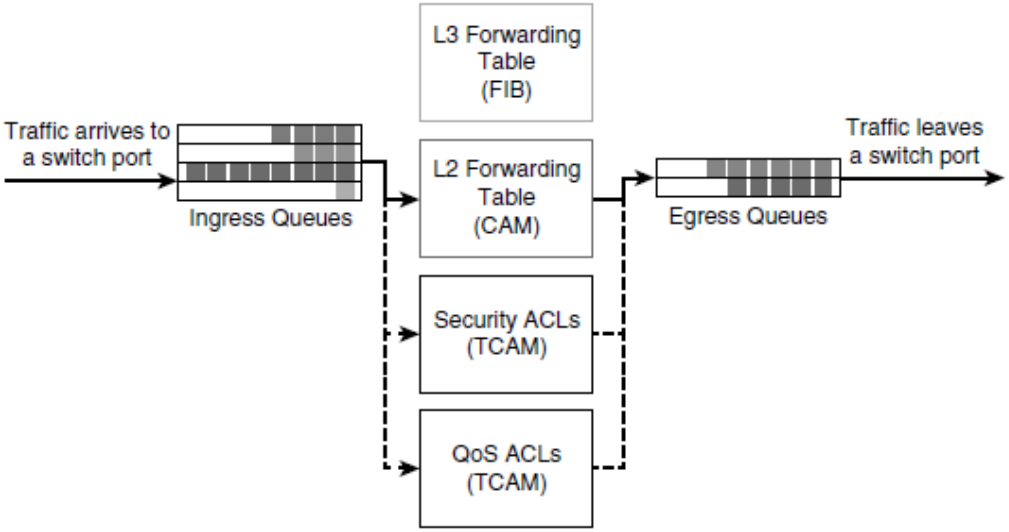


CAM Table

MAC Address	Egress Port	VLAN

Layer 3 (Multilayer) Switch Operation

- Multilayer switches not only perform Layer 2 switching but also forward frames based on Layer 3 and 4 information.
- Multilayer switches not only combine the functions of a switch and a router but also add a flow cache component.



FIB Table

IP Address	Next-Hop IP Address	Next-Hop MAC Address

CAM Table

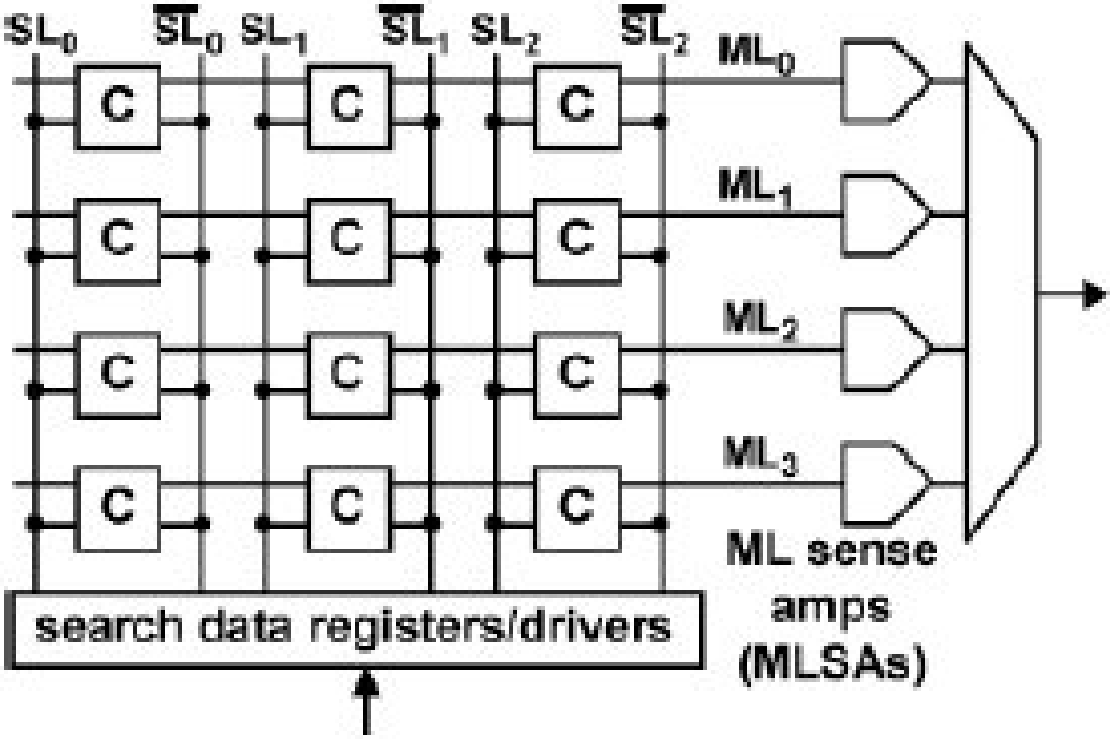
Egress Port	MAC Address	Egress Port	VLAN

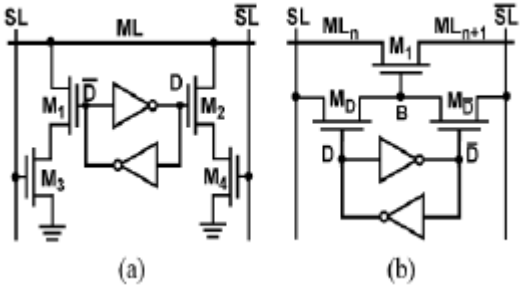
Commands for Viewing and Editing Catalyst Switch MAC Address Tables

```
Switch1# show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0000:0c00.9001    DYNAMIC     Et0/1
   1    0000.0c00.9002    DYNAMIC     Et0/2
   1    0000.0c00.9002   DYNAMIC     Et0/3
Total Mac Addresses for this criterion: 3

Switch1# show mac address-table interface ethernet 0/1
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0000:0c00.9001    DYNAMIC     Et0/1
Total Mac Addresses for this criterion: 1

Switch1# show mac address-table | include 9001
   1    0000:0c00.9001    DYNAMIC     Et0/1
```

Operace vyhledávání v TCAM s (a) globálním maskováním a (b) lokálním maskováním.

Buňka CAM slouží dvěma základním funkcím: bitové paměti (jako v RAM) .

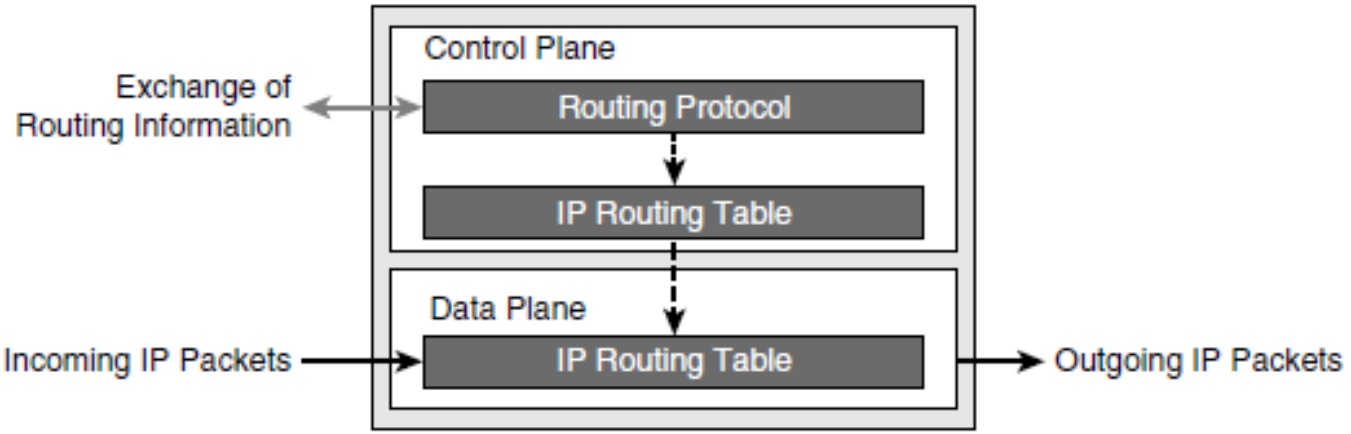




10-T NOR-type CAM and (b) 9-T NAND-type CAM

Distributed Hardware Forwarding

- Network devices contain at least three planes of operation:
  - Management plane
  - Control plane
  - Forwarding plane



Distributed Hardware Forwarding

- The **management plane** is responsible for the network management, such as SSH access and SNMP, and may operate over an out-of-band (OOB) port.
- The **control plane** is responsible for protocols and routing decisions, and the **forwarding plane** is responsible for the actual routing (or switching) of most packets.
- Multilayer switches must achieve high performance at line rate across a large number of ports. To do so, multilayer switches deploy independent control and forwarding planes.
- The control plane will program the forwarding plane on how to route packets.
- Multilayer switches may also employ multiple forwarding planes. For example, a Catalyst 6800 uses forwarding planes on each line module, with a central control plane on the supervisor module.
- To continue the example of the Catalyst 6800, each line module includes a microcoded processor that handles all packet forwarding.
- For the control plane on the supervisor to communicate with the line module, a control layer communication protocol exists.

Cisco Switching Methods

A Cisco IOS-based routers uses one of three methods to forward packets:

- Process Switching
  - Process switching is the slowest form of routing because the processor must route and rewrite using software.
- Fast Switching
  - Is a faster method by which the first packet in a flow is routed and rewritten by a route processor using software, and each subsequent packet is then handled by hardware.
- Cisco Express Forwarding (CEF)
  - The CEF method uses hardware forwarding tables for most common traffic flows, with only a few exceptions. If you use CEF, the route processor spends its cycles mostly on other tasks.

Cisco Switching Methods

- The architecture of the Cisco Catalyst and Nexus switches both focus primarily on the Cisco router equivalents of CEF.
- The absolute last-resort switching method for Cisco Catalyst or Nexus switches is process switching.
- The route processors of these switches were never designed to switch or route packets, and by doing so, this will have an adverse effect on performance.
- Fortunately, the default behavior of these switches is to use fast switching or CEF, and process switching occurs only when necessary.

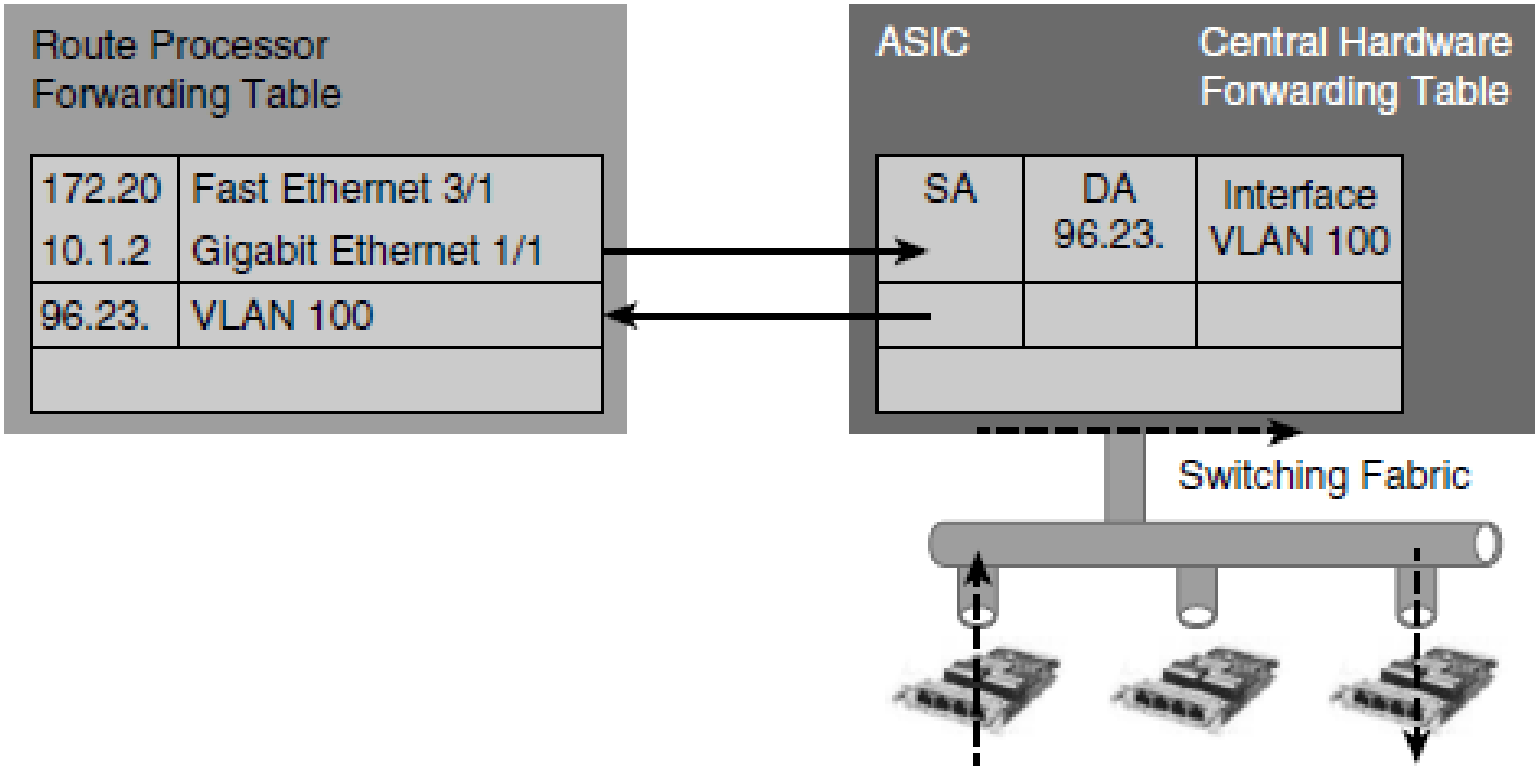
Cisco Switching Methods

With Cisco Catalyst switching terminology, fast switching is referred to as *route caching* , and the application of CEF with distributed hardware forwarding is referred to as *topology-based switching*.

As a review, the following list summarizes route caching and topology-based forwarding on Cisco Catalyst switches:

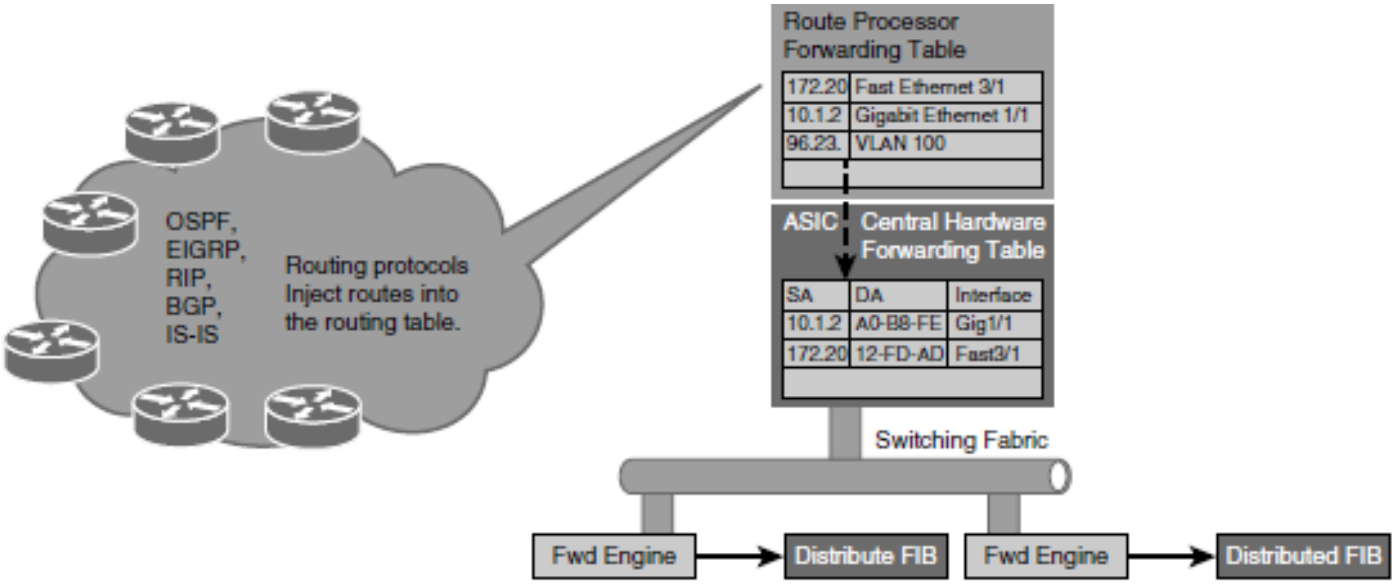
- **Route caching**
  - Also known as *flow-based* or *demand-based switching* , route caching describes a Layer 3 route cache that is built within the hardware functions as the switch detects traffic flow into the switch.
- **Topology-based switching**
  - Information from the routing table is used to populate the route cache, regardless of traffic flow. The populated route cache is the FIB, and CEF is the facility that builds the FIB.

Route Caching



- The first packet in a stream is switched in software by the route processor, because no cache entry exists yet for the new flow.

Topology-Based Switching



- CEF uses information in the routing table to populate a route cache (known as an FIB), without traffic flows being necessary to initiate the caching process.
- In addition, CEF adds enhanced support for parallel paths and thus optimizes load balancing at the IP layer.
- In most current-generation Catalyst switches, CEF supports both load balancing based on source IP address and destination IP address combination and source and destination IP plus TCP/UDP port number.

Hardware Forward Details

- The actual Layer 3 switching of packets occurs at two possible different locations on Catalyst switches.
- These possible locations are in a **centralized** manner, such as on a supervisor module, or in **distributed** fashion, where switching occurs on individual line modules.
- These methods are referred to as *centralized switching* and *distributed switching* , respectively.
- The Catalyst 6500 was a perfect example where there was an option to centralize switch everything on the supervisor or place specific hardware versions of line modules in the chassis to gain distributed switching capability.
- The benefits of centralized switching include lower hardware cost and lower complexity.
- For scaling and large enterprise core networks, distributed switching is optimal. Most small form-factor switches leverage centralized switching.

Chapter 2 Summary

- Flat Layer 2 networks are extremely limited in scale and in most cases will only scale to 10 to 20 end users before adverse conditions may occur.
- Despite its age, the hierarchical model continues to be a key design fundamental of any network design, including campus network designs.
- The hierarchical model consists of an access, distribution, and core layer, thus allowing for scalability and growth of a campus network in a seamless manner.
- The different models of Cisco Catalyst switches provide for a range of capabilities depending on need and placement within the hierarchical model.
- Cisco Catalyst switches leverage CAM for Layer 2 forwarding tables and TCAM for Layer 3 forwarding tables to achieve line-rate performance.
- Cisco Catalyst switches leverage CEF (topology-based switching) for routing, utilizing a distributed hardware forwarding model that is centralized or distributed per line card.

Chapter 2 Labs

- **None**

Acknowledgment

- *Some of the images and texts are from Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: (CCNP SWITCH 300-115)* by Richard Froom and Erum Frahim (1587206641)

- Special Thanks to *Bruno Silva*