

# **11W NET3011**

## **CCNP SWITCH – Chapter 1**

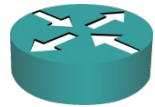
# **Enterprise Campus Architecture**

**David Bray**

**brayd@algonquincollege.com**

**with contributions obtained from Rick Graziani & Cisco**

# Cisco Icons and Symbols



Router



Network Cloud



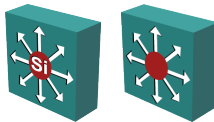
IP Phone



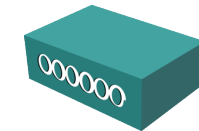
End Users



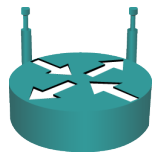
Voice-Enabled Router



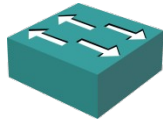
Multilayer Switch



Access Point



Wireless Router



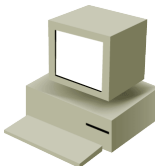
Workgroup Switch



Lightweight Single-Radio Access Point



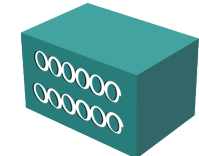
Ethernet



PC



Workgroup Switch: Voice-Enabled



Autonomous Dual-Band Access Point



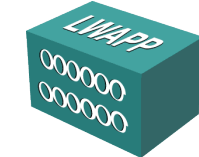
Wireless Link



Laptop



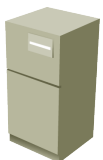
100BASE-T Hub



Lightweight Dual-Band Access Point



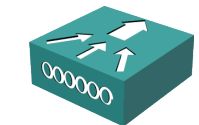
Route/Switch Processor



File Server

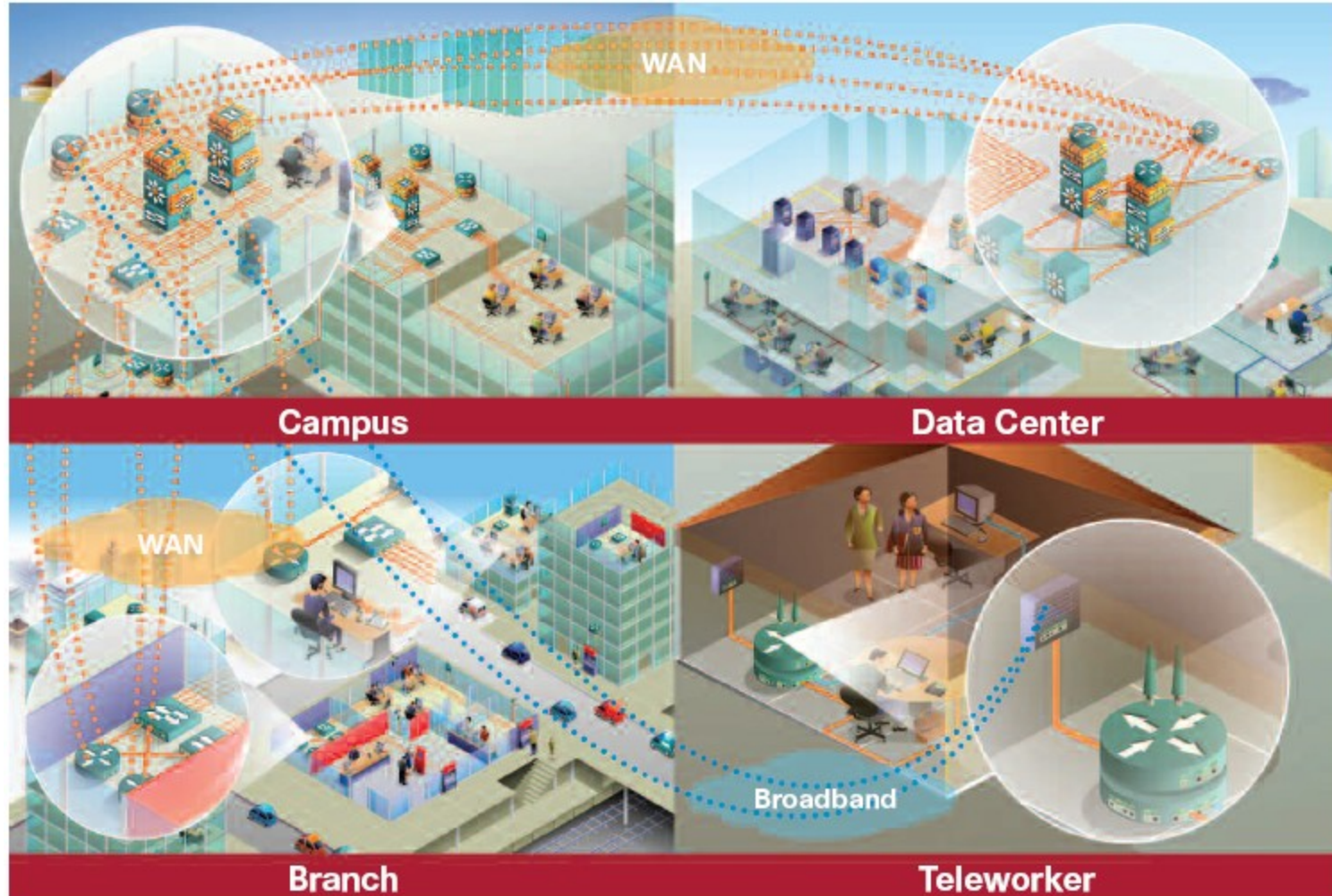


Bridge



Wireless LAN Controller

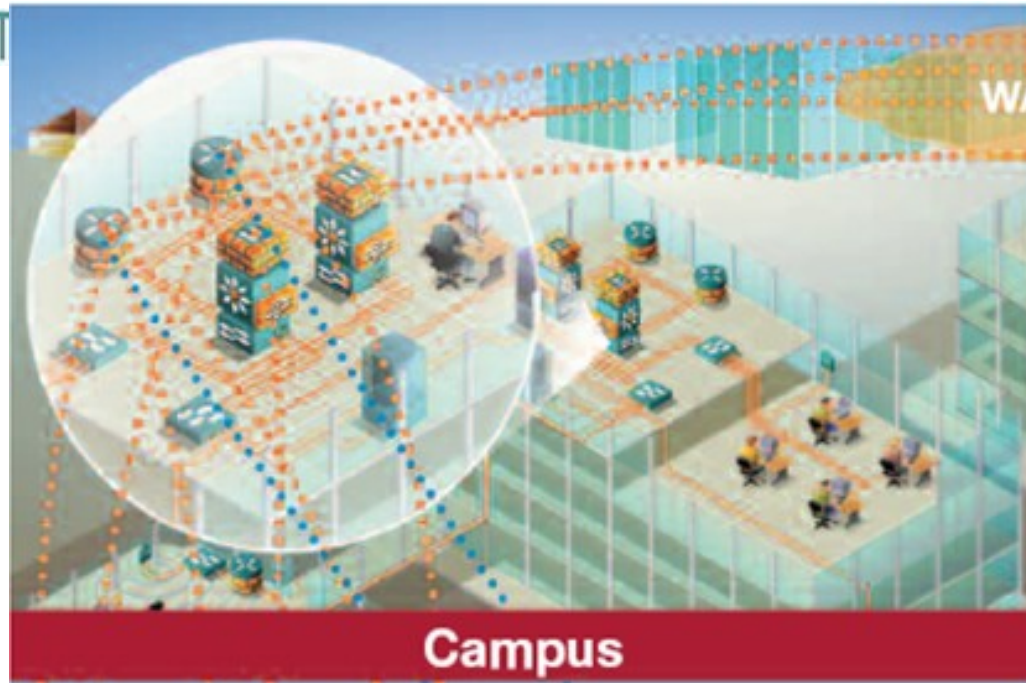
# Cisco Enterprise Architecture



**Four key components of the architecture**

# Campus

- Campus combines a core **infrastructure** of intelligent switching and routing, including:
  - **IP Communications**
  - **mobility**, and
  - **advanced security**
- Provides **high availability**.
- **Quality of service (QoS)** prevents oversubscription to ensure that real-time traffic, such as voice and video, or critical data is not dropped or delayed.
- **Integrated security** protects against and mitigates the impact of worms, viruses, and other attacks on the network, even at the port level.
- Provides the **flexibility** to add IP Security (IPSec) and Multiprotocol Label Switching Virtual Private Networks (MPLS VPNs), identity and access management, and VLANs to compartmentalize access.



# Data Center

ALGONQUIN  
COLLEGE

- Provide data access that is:
  - **integrated**
  - **secure**
  - **high performance**
  - **geared to business continuance**



- Cohesive, adaptive network architecture.
- Provides departmental staff, suppliers, or customers with **secure, access to applications and resources.**
- Streamlines network management, thereby reducing overhead.
- Redundant data centers provide backup.
- The network and devices offer server and application load balancing to maximize fault tolerance and performance.

# Branch

- Provide data access that is:
  - **ubiquitous**
  - **secure**
  - **scalable**

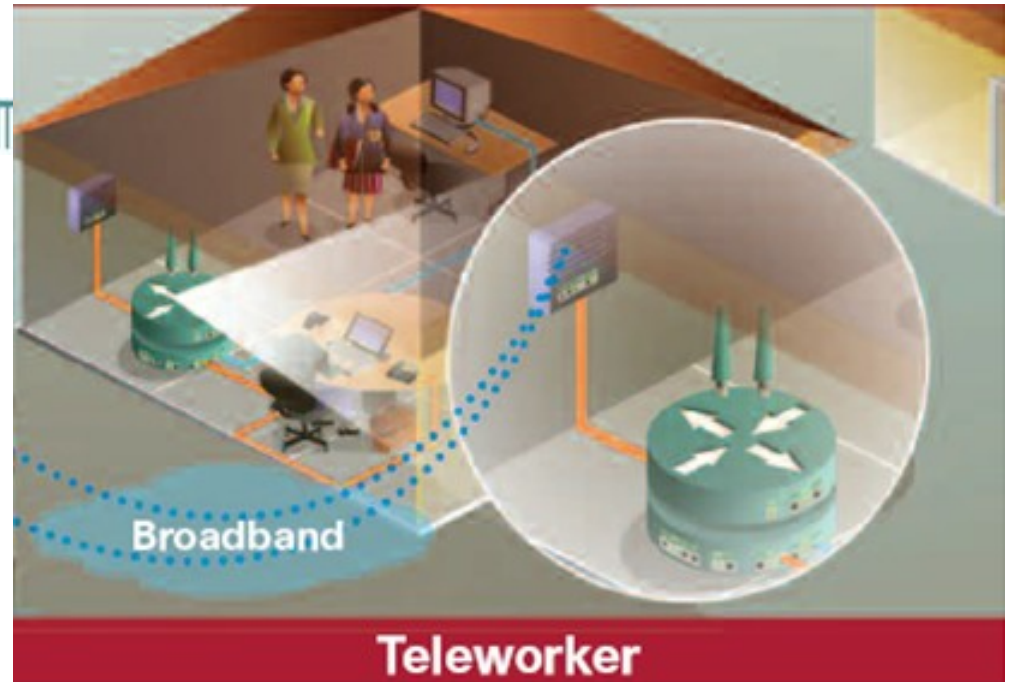


- Extends head-office applications and services, such as security, IP Communications, and advanced application performance, to remote locations, users, or branches.
- Integrates security, switching, network analysis, caching, and converged voice and video services into a series of integrated services routers
  - Can deploy new services when they are ready without buying new equipment.

# Teleworker

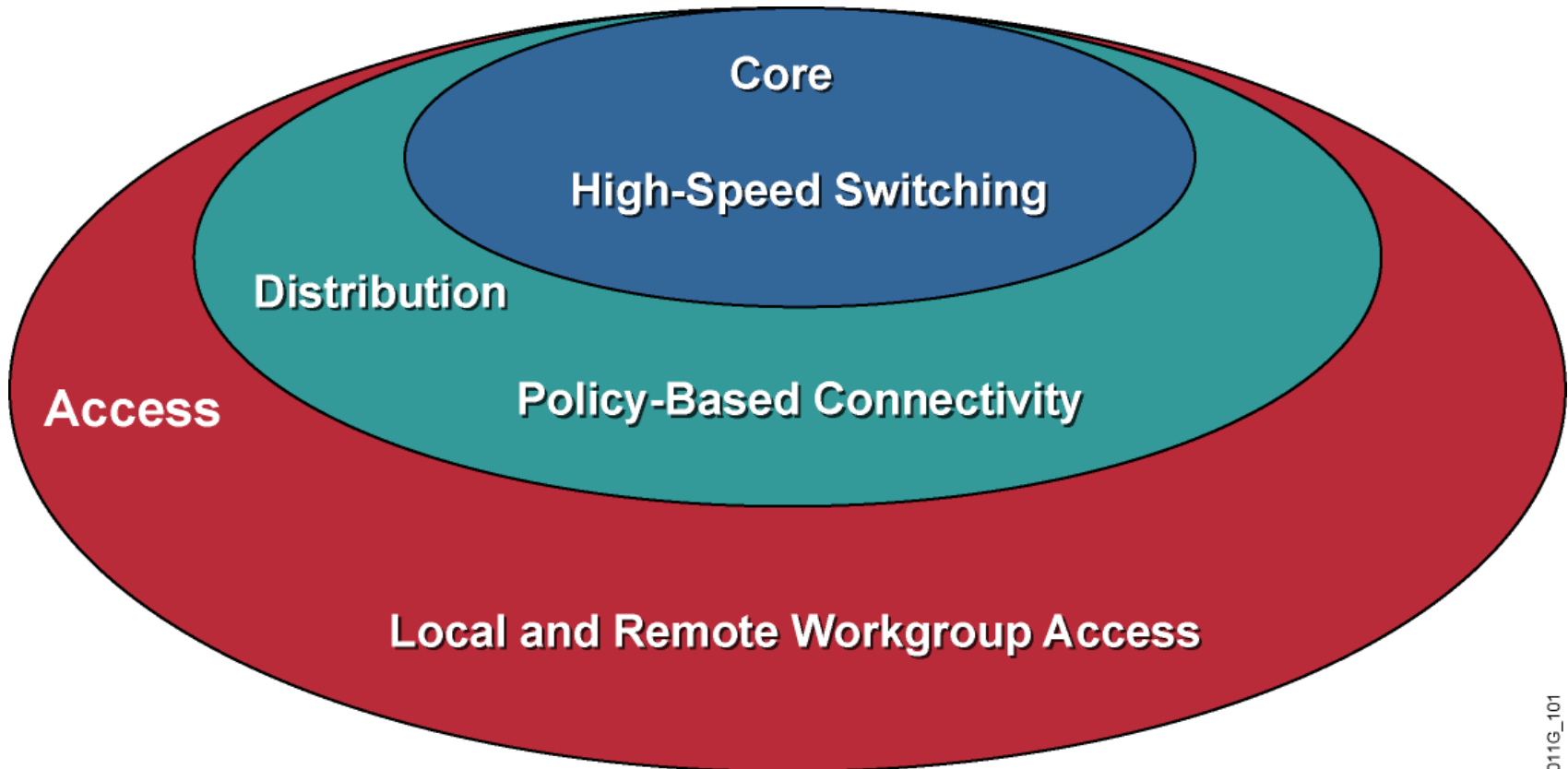
- Provide data access that is:
  - **ubiquitous**
  - **secure**
  - **scalable**

(same access that a Branch has, but at a distance)



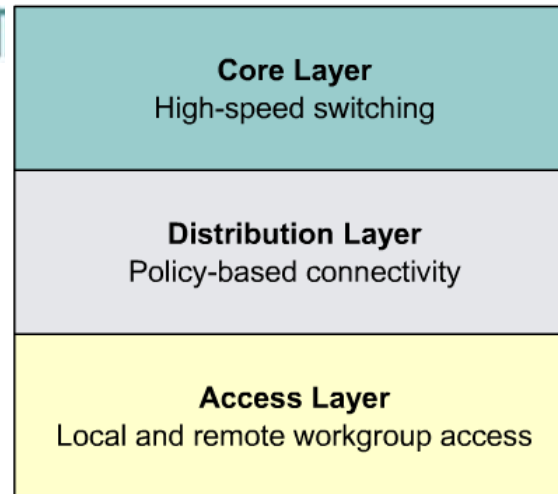
- Allows enterprises to securely deliver voice and data services to remote small or home offices over a standard broadband access service.
- Flexible work environment for employees.
- Extend campus security policies to the teleworker.
- “Always-on” VPN and gain access to authorized applications and services, including IP phone.

# Cisco Hierarchical Network Model



011G\_101

# Core Layer



## The Core Layer:

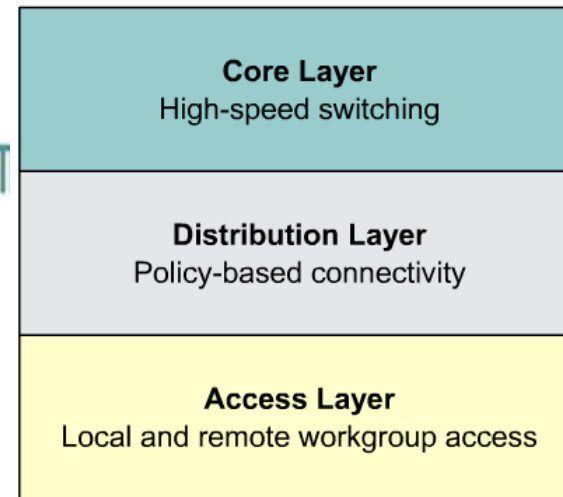
- Is an optimized and reliable transport structure, with the sole aim of forwarding traffic.
- Switches packets as fast as possible.

Devices at the core layer should not be burdened with any processes that impede packet switching at top speed.

Core devices are characterized by:

- *No Access-list checking*
- *No Data encryption*
- *No Address translation*

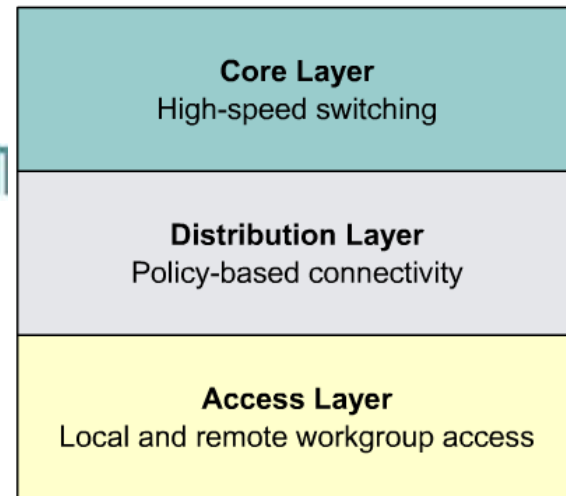
# Distribution Layer



## The Distribution Layer

- Provides *boundary definition* using access lists and other strategies to limit what enters the core.
- Defines policy for the network.
- A policy is an *approach* to handling certain kinds of traffic, including the following:
  - Routing updates
  - Route summaries
  - VLAN traffic
  - Address aggregation

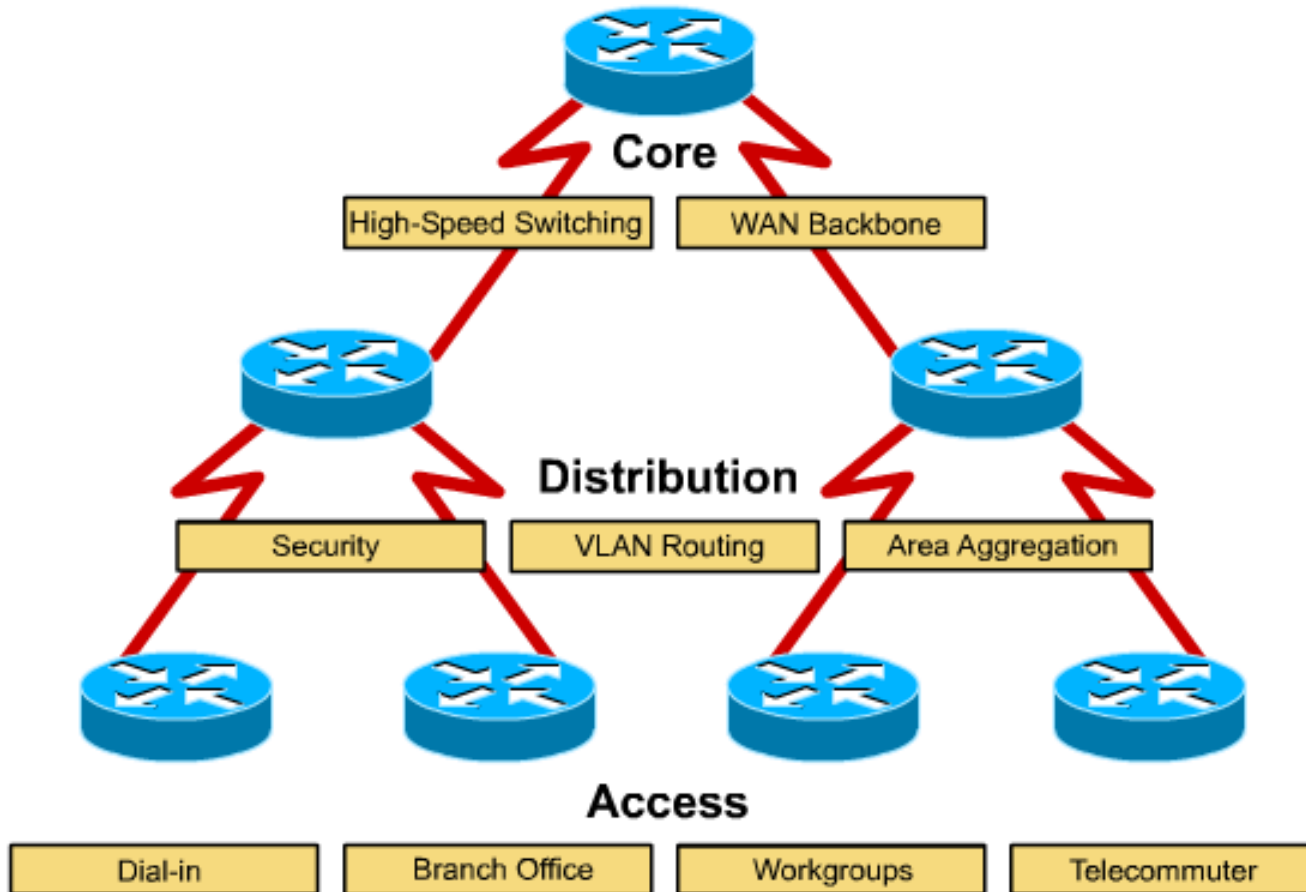
# Access Layer



## The Access Layer

- The access layer provides end user access to the network and performs network admission control.
- Acting as the front door to a network, the access layer can employ access lists designed to prevent unauthorized users from gaining entry.
- Facilitates QoS by classifying traffic entering the network.
- The access layer can also give remote sites access to the network by way of a wide-area technology such as Frame Relay, dedicated lines or other broadband technologies.

# Three-layer Design Template



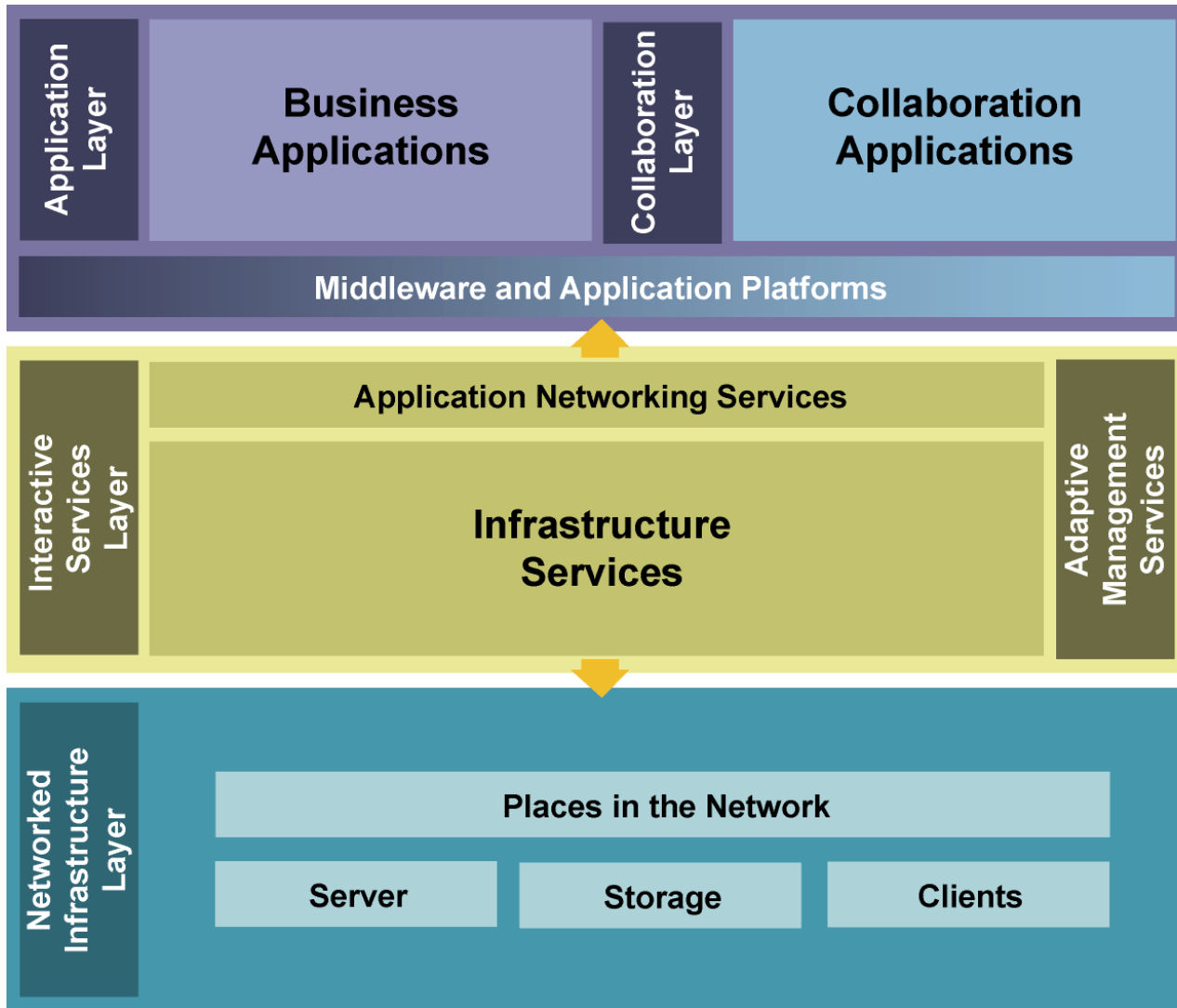
# Traffic Mix in Today's Networks

- **Converged network traffic mix:**
  - Voice and video traffic
  - Voice applications traffic
  - Mission critical applications traffic
  - Transactional traffic
  - Routing update traffic
  - Network management traffic
- **Key requirements:**
  - Performance (bandwidth, delay, jitter)
  - Security (access, transmission)

# Cisco SONA Framework

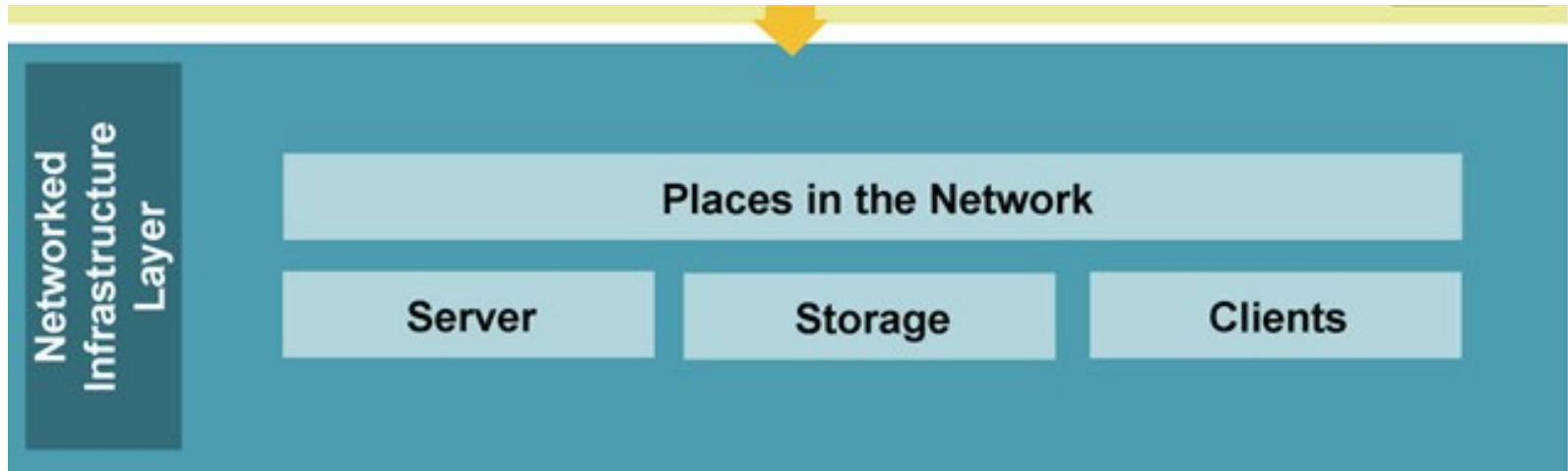
- The Cisco **Service-Oriented Network Architecture** (SONA) is an *architectural framework*.
- **SONA** brings several advantages to enterprises including how to:
  - Evolve towards the Intelligent Information Network (IIN)
  - Build integrated systems across a fully converged intelligent network
  - Improve flexibility and increase efficiency
  - Optimize applications, processes, and resources

# Cisco SONA Framework Layers



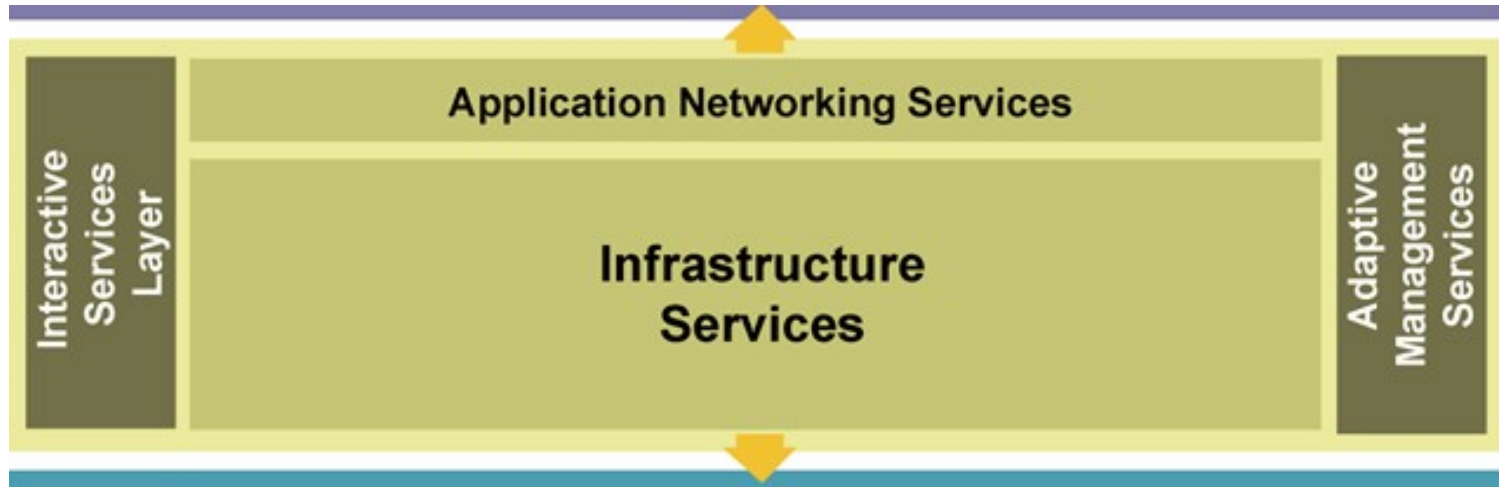
310P\_152

# SONA—Networked Infrastructure Layer



- The goal is **ubiquitous access**:  
“anywhere/anytime connectivity to devices and data”

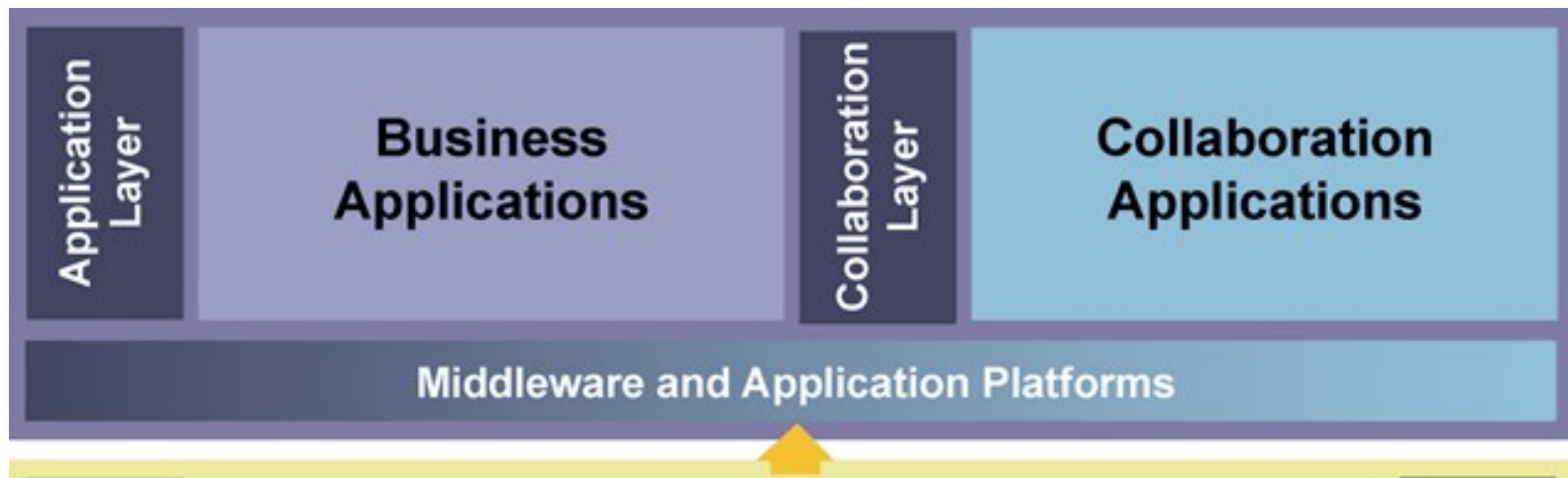
# SONA—Interactive Services Layer



## Interactive services includes:

- voice and collaboration services
- mobility services
- security and identity services
- storage services
- computer services
- application networking services
- network infrastructure virtualization
- services management
- adaptive management services

# SONA—Application Layer

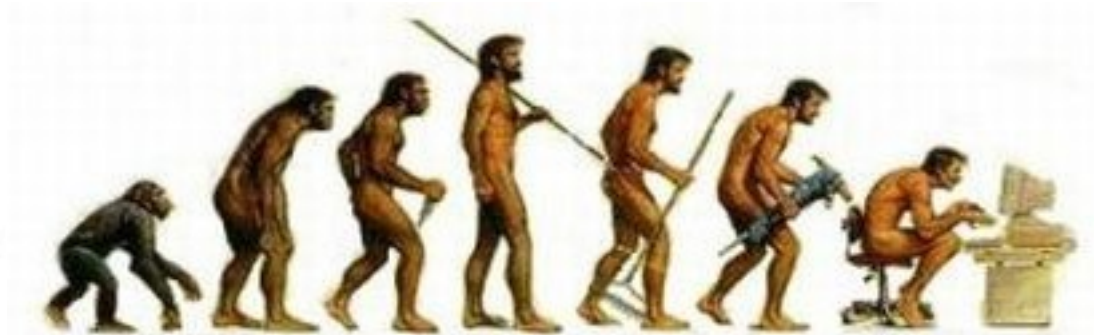


Application Layer includes:

- business applications
- collaboration applications

# Intelligent Information Network

- **IIN**
  - Integrates networked resources and information assets
  - Extends intelligence across multiple products and infrastructure layers
  - Actively participates in the delivery of services and applications
- **Three phases in building an IIN are:**
  - Integrated transport – of all data types
  - Integrated services – allows pooling, virtualization
  - Integrated applications – optimizes appl'n performance
    - network is application-aware
    - applications are network-aware



Evolution of

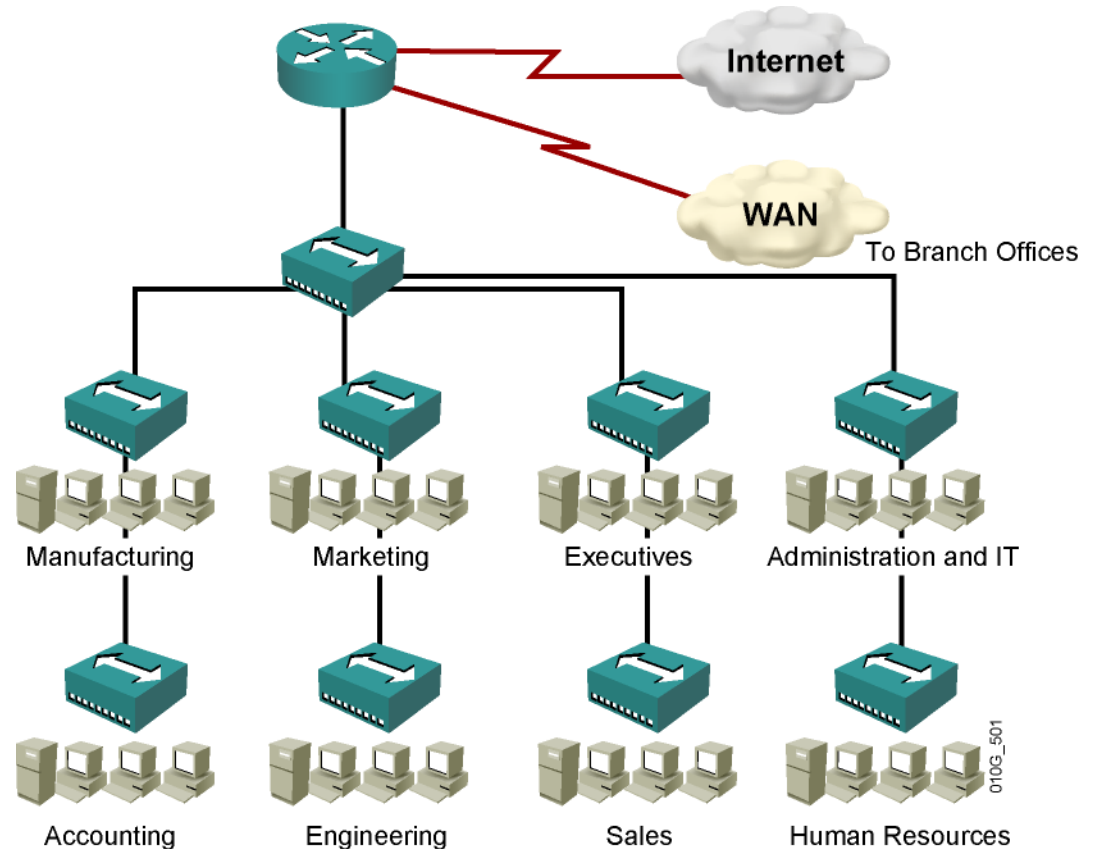
# Network designs



# Nonhierarchical Networks and Devices

## Characterized by:

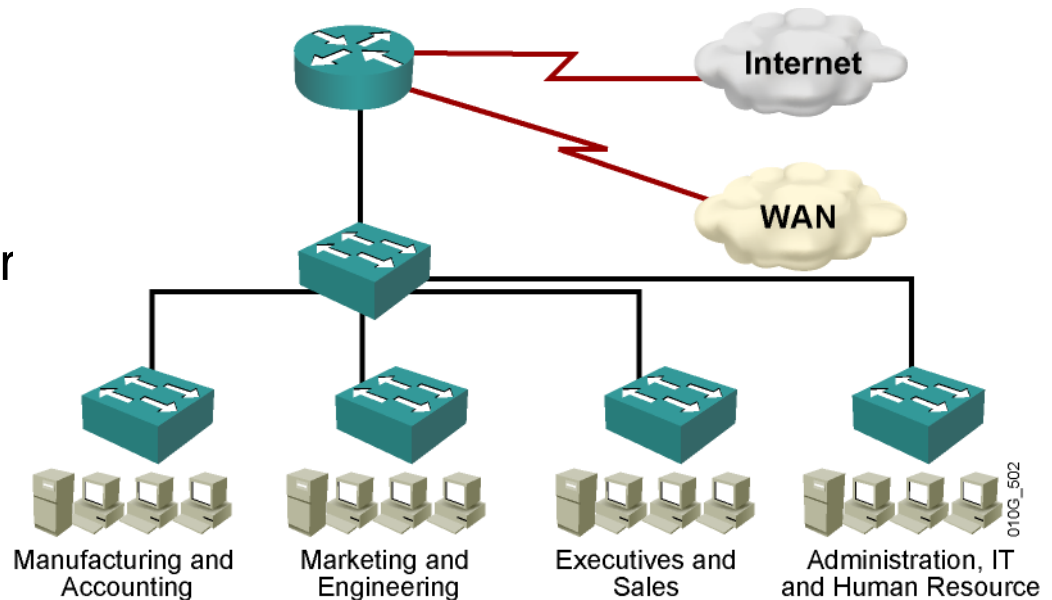
- Large collision domains
- Large broadcast domains
- High latency
- Difficult to troubleshoot



# Layer 2 Switching and Nonhierarchical Issues

## Layer 2 Switching benefits

- Hardware-based bridging
- Wire-speed performance
- Single collision domain per port
- Traffic containment based on MAC address



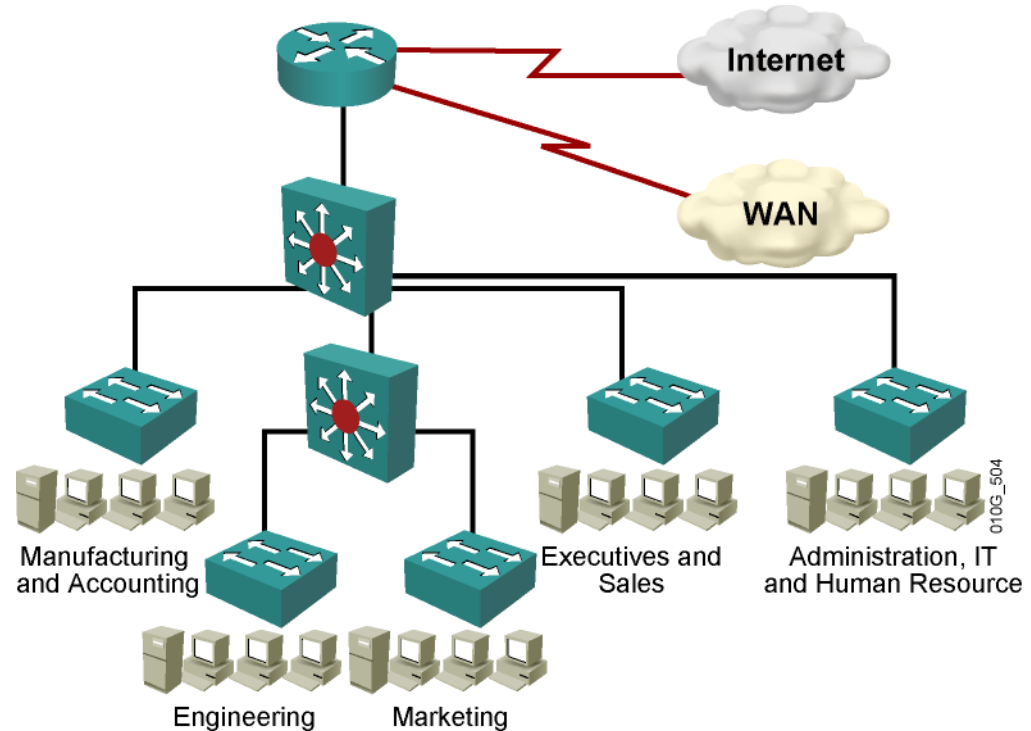
## Issues

- Without VLANs, large unbounded broadcast domain.
- No traffic between VLANs without layer 3 routing.
- Increases potential for bridge loops and therefore, the use of Spanning Tree Protocol (STP) becomes imperative.
- Servers not centrally located (no advantage).



# Multilayer Switching

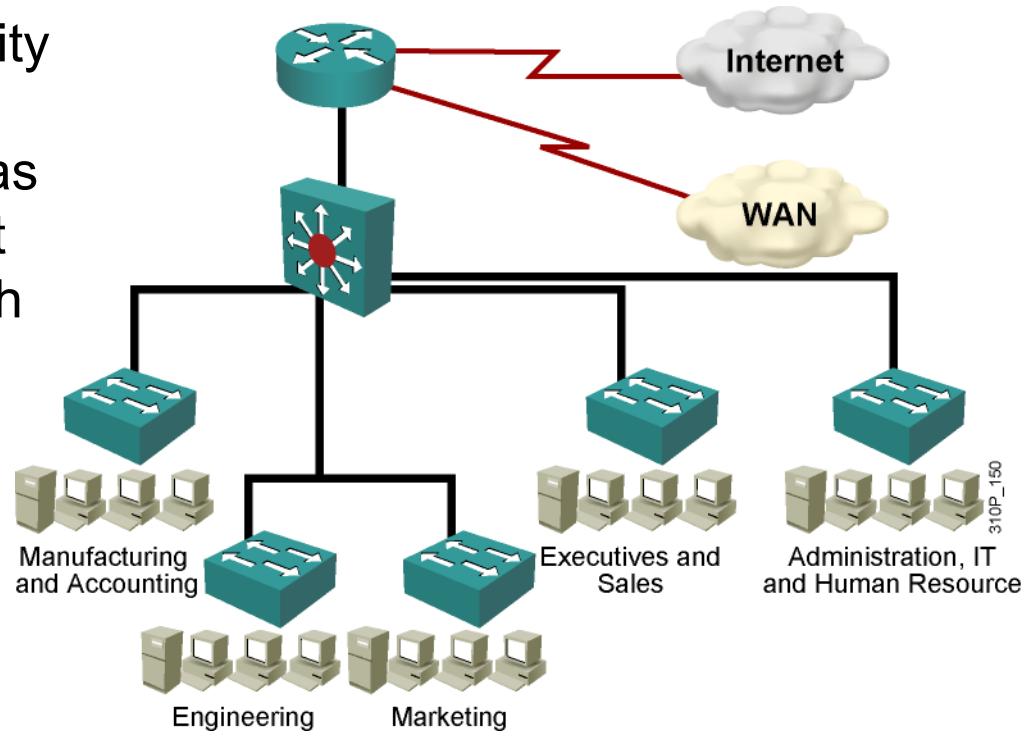
- **Multilayer switching** is hardware-based switching and routing integrated into a single platform.
- A multilayer switch does everything at the frame and packet level that a traditional switch or router does, including the following:
  - Layer 2 switching
  - Layer 3 switching
  - Layer 4 switching
  - Low latency
  - High-speed scalability



- Supports QoS
- Supports VoIP

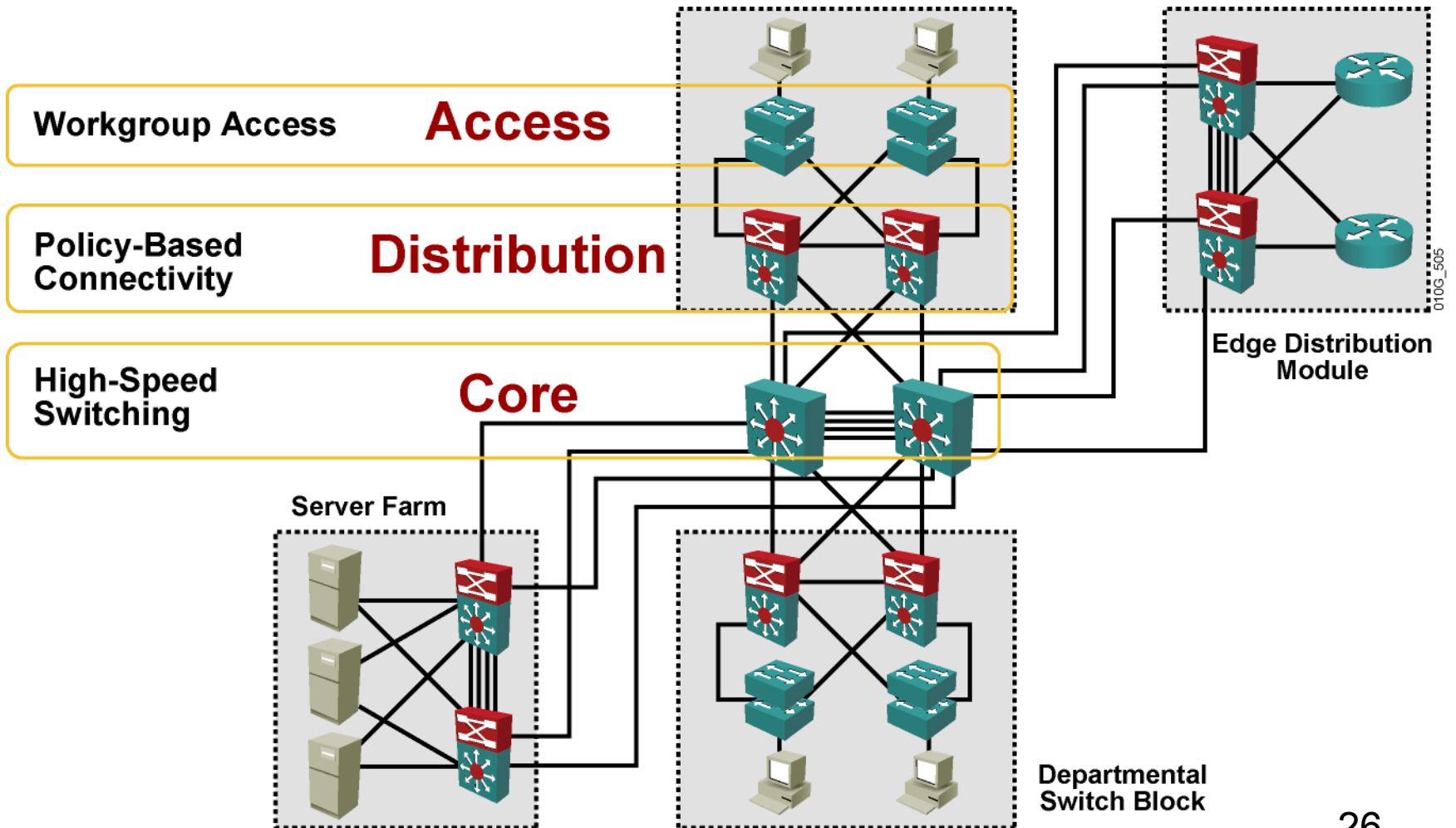
# Issues with Multilayer Switches in a Nonhierarchical Network

- Single point of failure for Layer 2 and Layer 3 devices
- Multilayer switching functionality may be under-utilized if a multilayer switch is deployed as a simple physical replacement for a traditional router or switch without any network re-design
- Increases Spanning Tree complexity
- Servers not centrally located



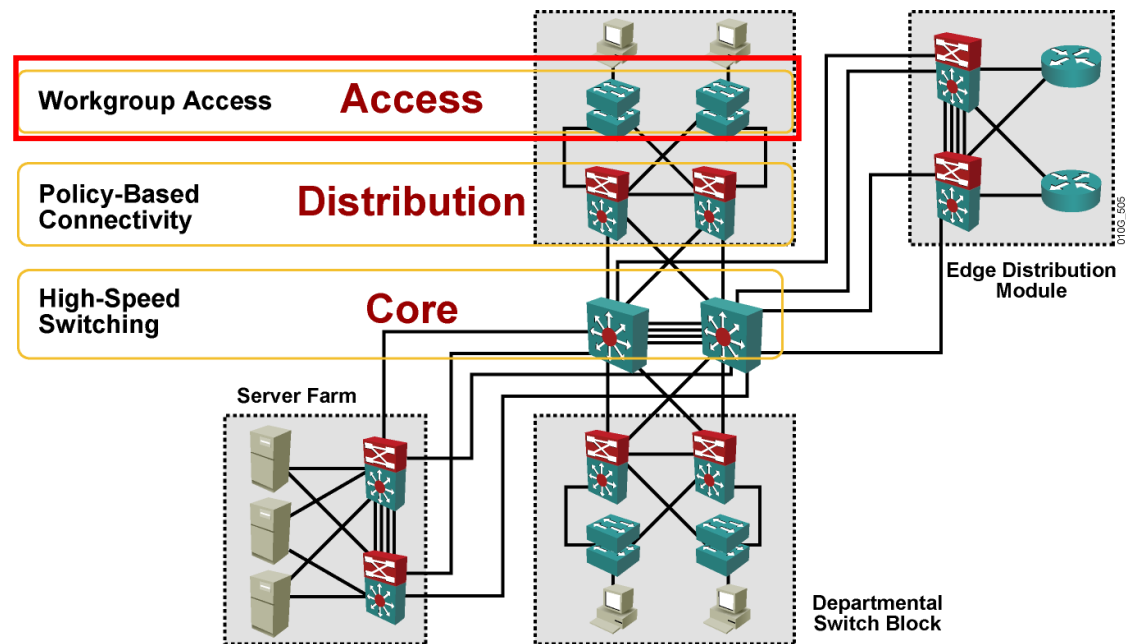
# Hierarchical Campus Model

- Allows flexibility in network design and facilitates ease of implementation and troubleshooting.



# Building Access layer

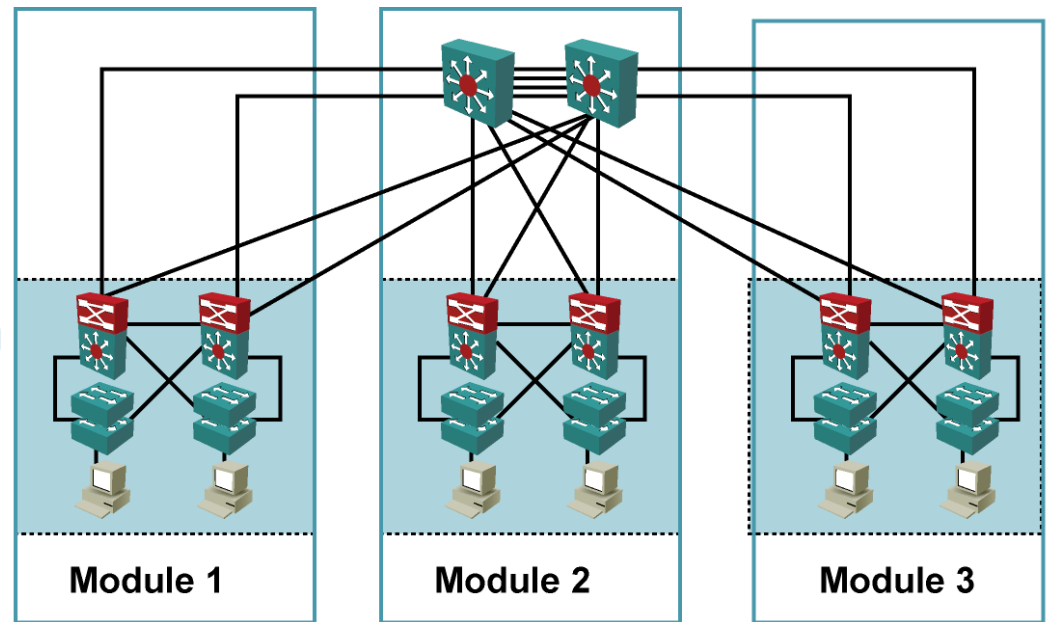
- User access to network devices.
- Layer 2 and 3 broadcast multicast management, QoS, and access control.
- **Network campus**, incorporates switched LAN devices with ports that provide connectivity to workstations and servers.
- **WAN environment**, provides access to the corporate network across various WAN technologies.



# Building Access submodule



Core  
Distribution  
Access

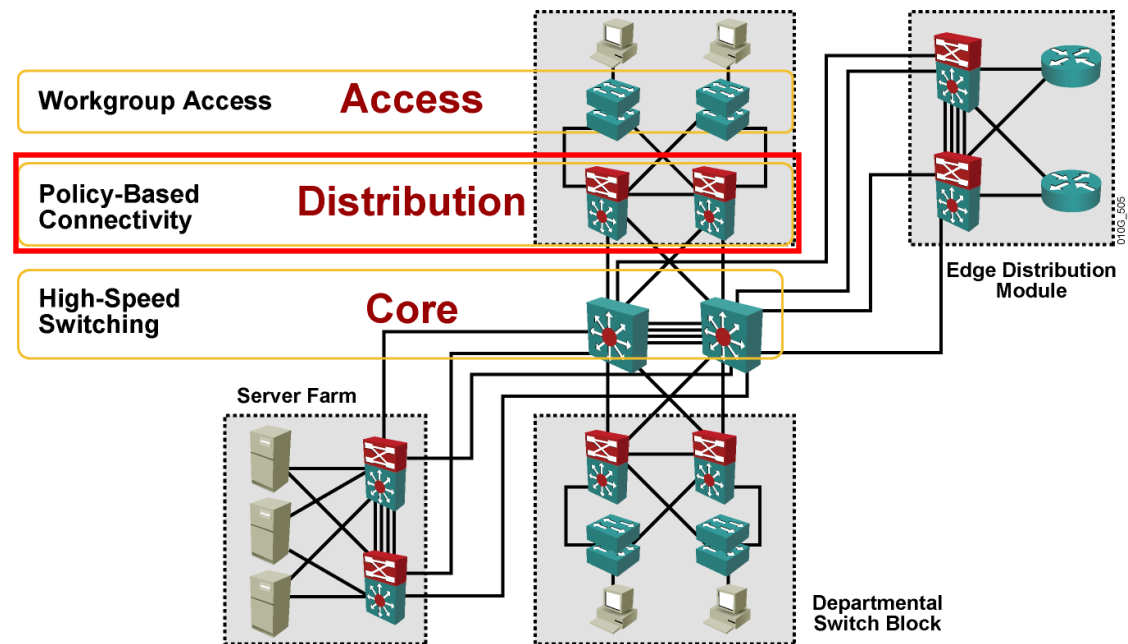


## Building Access submodule (also known as Building Access layer):

- Contains:
  - end-user workstations,
  - IP phones
  - Layer 2 access switches
- Connects devices to the Building Distribution submodule.
- The Building Access submodule performs services such as:
  - support for multiple VLANs
  - private VLANs
  - establishment of trunk links to the Building Distribution layer
  - IP telephony

# Building Distribution layer

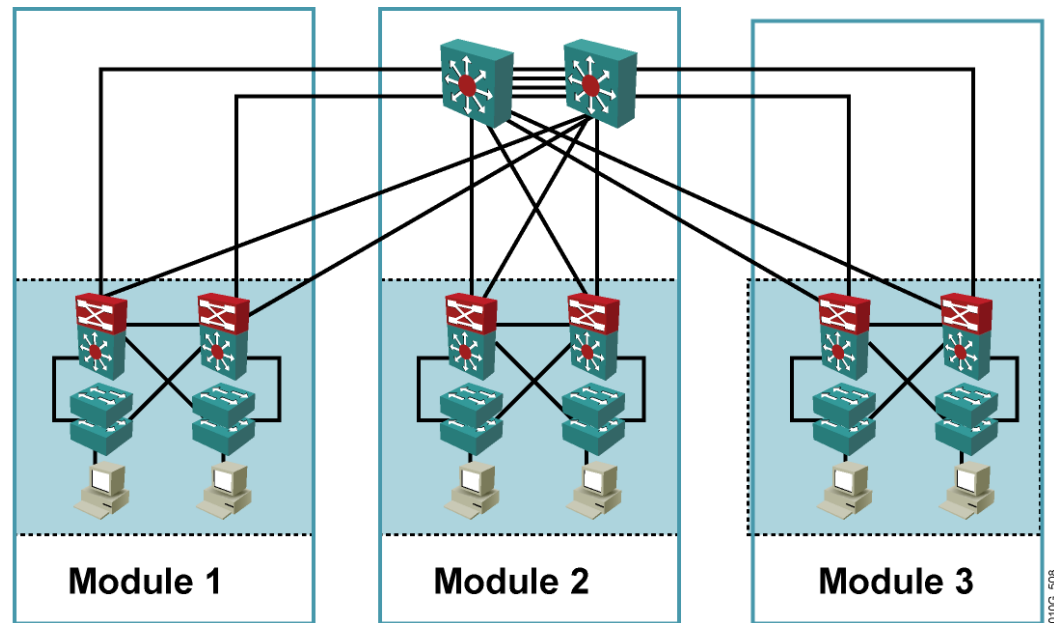
- Aggregates the wiring closets and uses switches to segment workgroups and isolate network problems.
- Generally performs IP routing and implements QoS and access control.



# Building Distribution submodule



Core  
Distribution  
Access

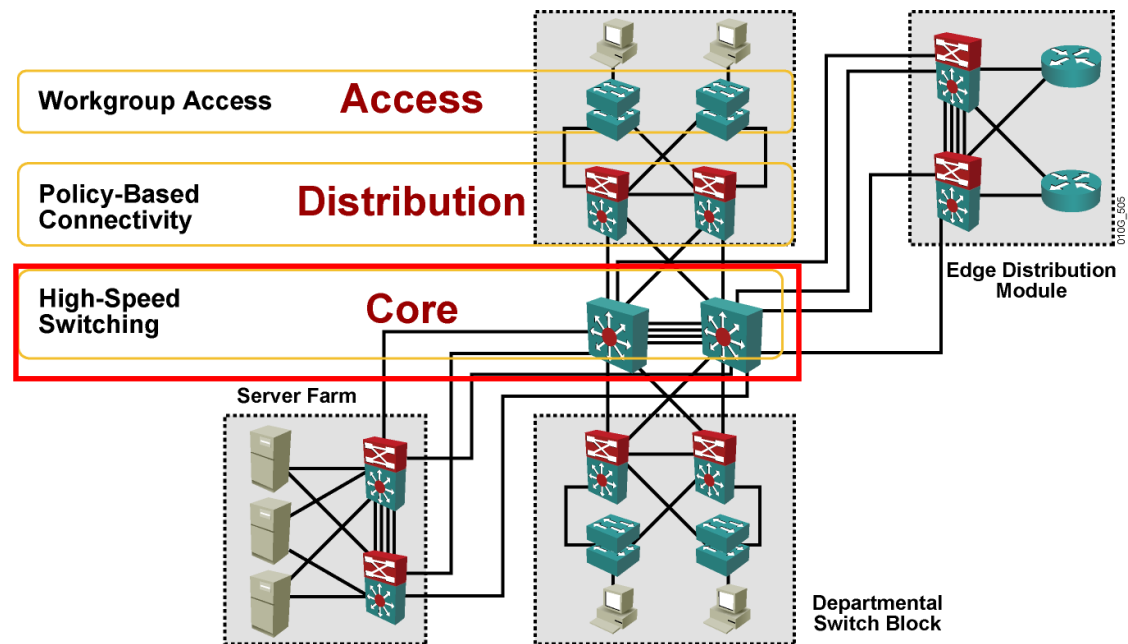


## Building Distribution submodule (also known as Building Distribution layer):

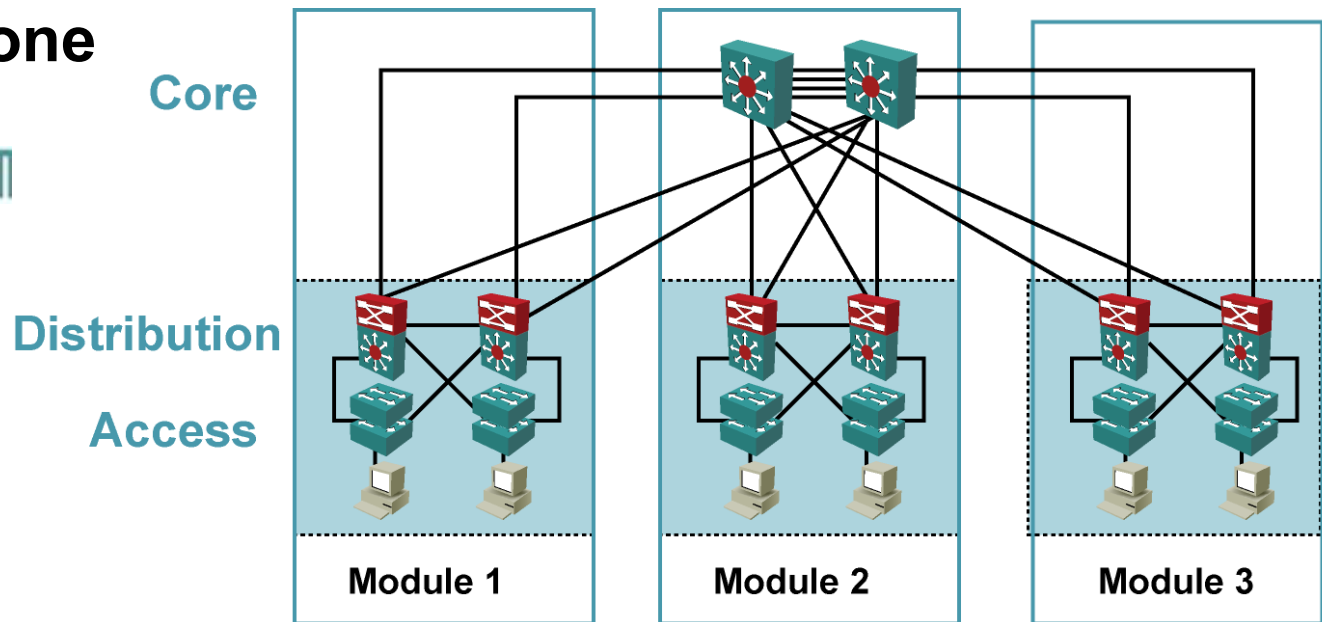
- Provides aggregation of building access devices, often using Layer 3 switching.
- Performs routing, QoS, and policy control.
- Traffic generally flows through the building distribution switches and onto the campus core or backbone.
- Provides fast failure recovery because each building distribution switch maintains two equal-cost paths in the routing table for every Layer 3 network number.
- Each building distribution switch has connections to redundant switches in the core.

# Building Core layer

- High-speed backbone
- Designed to switch packets as fast as possible.
- Because the core is critical for connectivity, it must provide a high level of availability and adapt to changes very quickly
- Also known as the Campus Backbone
- Generally uses Layer 3 switches with added routing, QoS and security features.



# Campus Backbone submodule

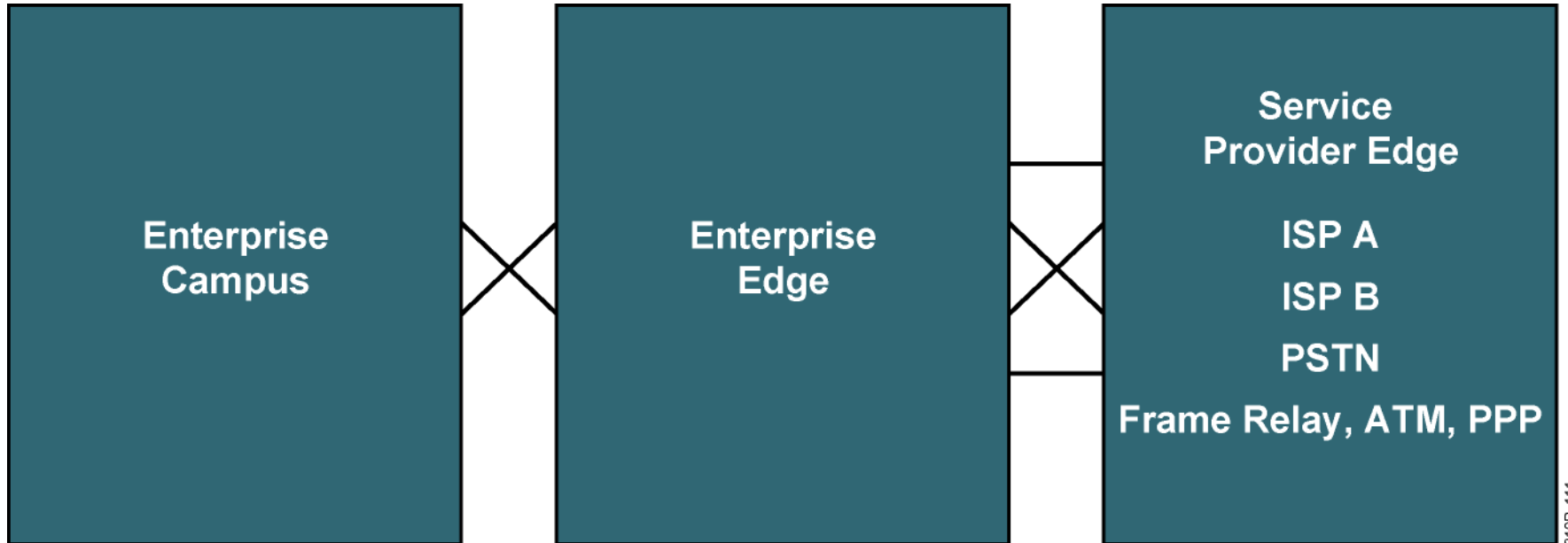


## Campus Backbone submodule (also known as Building Core layer):

- Provides redundant and fast-converging connectivity between buildings and the Server Farm and Edge Distribution modules.
- The purpose is to switch traffic as fast as possible between Campus Infrastructure submodules and destination resources.
- Forwarding decisions made at the ASIC level whenever possible.
- Routing, ACLs, and processor-based forwarding decisions should be avoided at the core and implemented at building distribution devices whenever possible.
- High-end Layer 2 or Layer 3 switches are used at the core for high throughput, with optimized routing, QoS, and security capabilities available when needed.

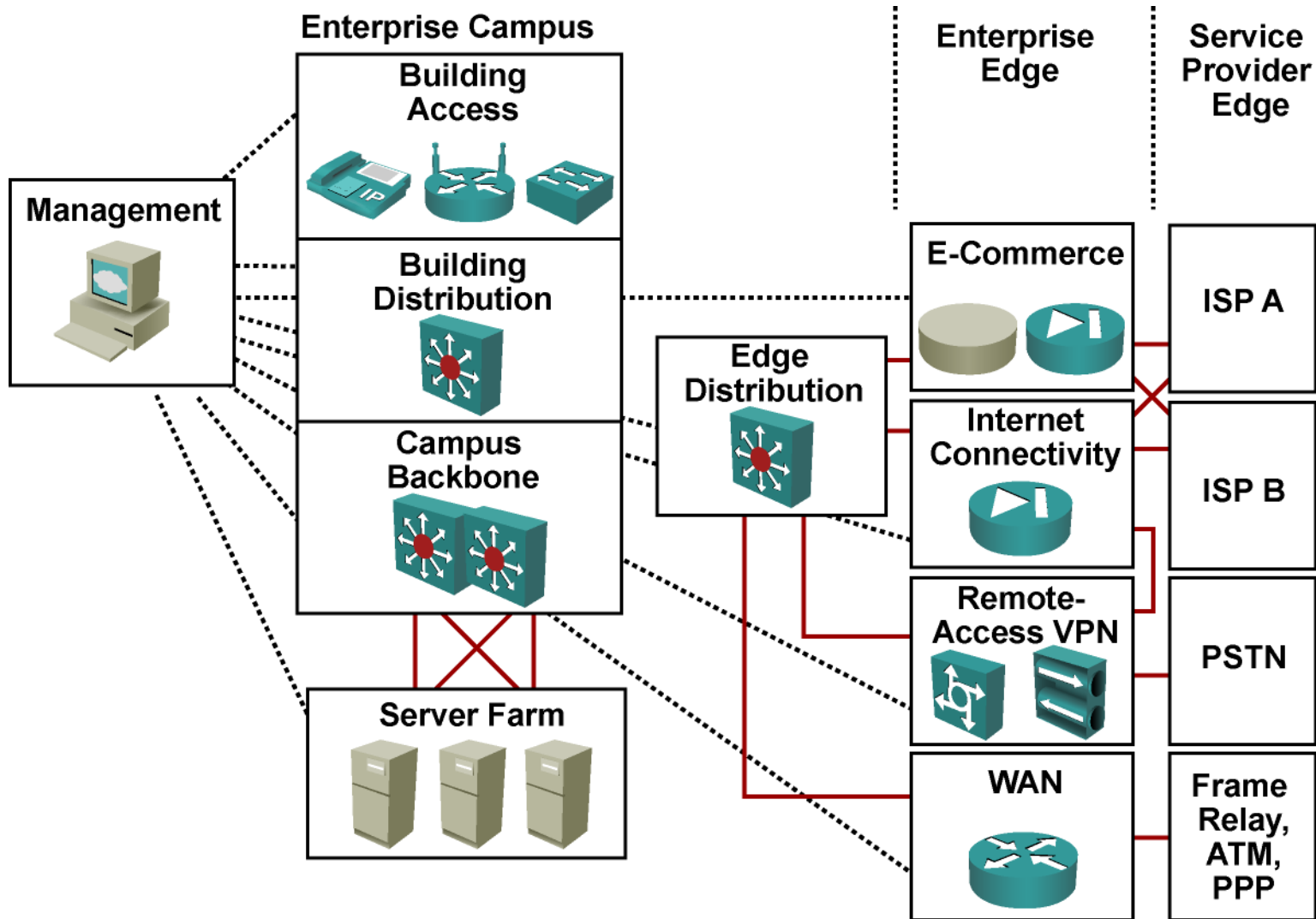
# Enterprise Composite Network Model (ECNM)

## Functional Areas



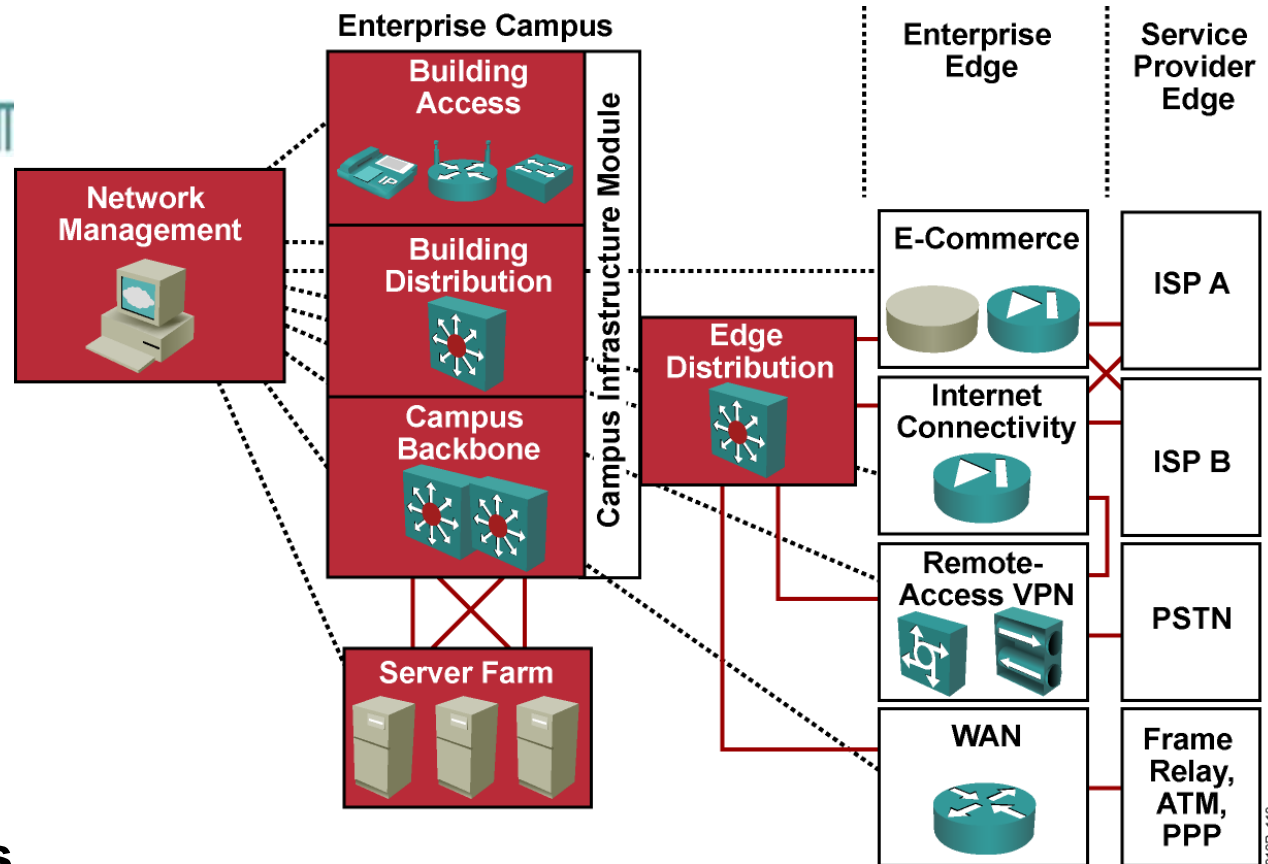
- The ECNM introduces modularity by dividing the network into functional areas that ease design, implementation, and troubleshooting tasks.
- An enterprise campus is defined as one or more buildings, with multiple virtual and physical networks, connected across a high-performance, multilayer-switched backbone.

# Enterprise Composite Network Model



310P\_112

# ECNM



## Enterprise Campus.

- Hierarchical, highly robust campus network that offers performance, scalability, and availability.
- Network elements required for independent operation within a single campus, such as access from all locations to central servers.
- Does not offer remote connections or Internet access.

# ECNM

ALGONQUIN  
COLLEGE

## Enterprise Campus:

- **Campus Infrastructure module:**

- connects users within the campus to the Server Farm and Edge Distribution modules.
- one or more floors or buildings connected to the Campus Backbone

- **Network Management module:**

- Performs system logging and authentication as well as network monitoring and general configuration management functions.

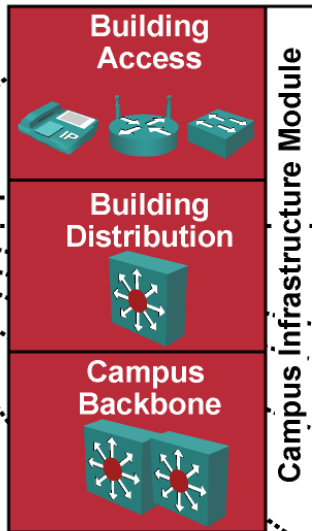
- **Server Farm module:**

- Contains e-mail and corporate servers providing application, file, print, e-mail, and Domain Name System (DNS) services to internal users.

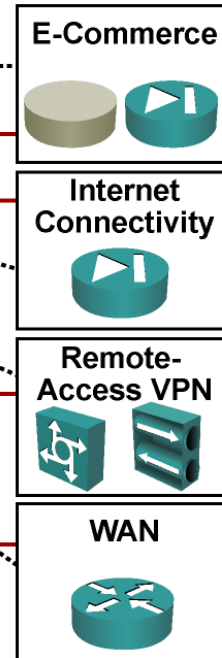
- **Edge Distribution module:**

- Aggregates the connectivity Enterprise Edge and routes the traffic into the Campus Backbone.

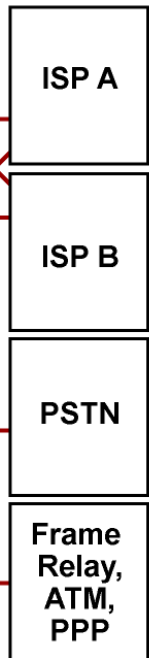
### Enterprise Campus



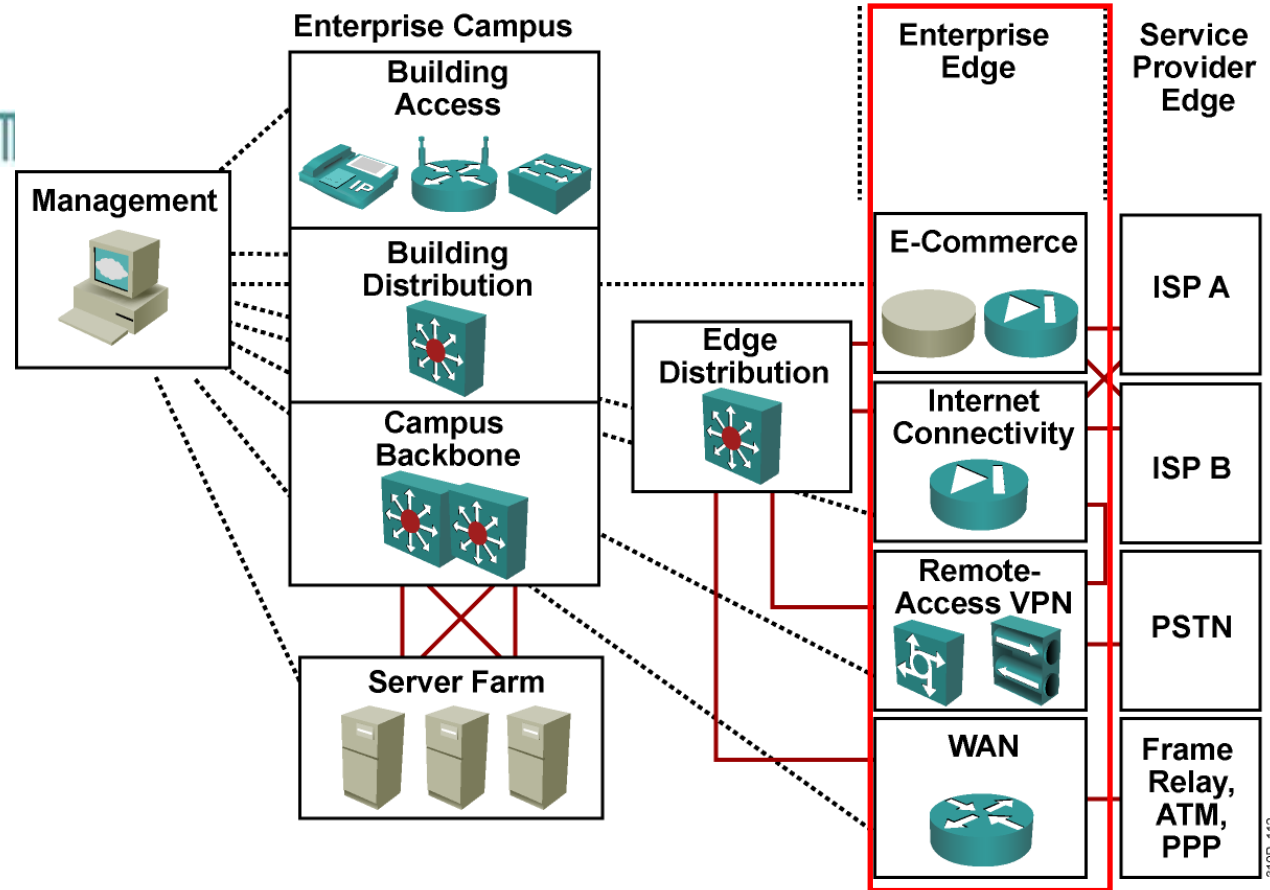
### Enterprise Edge



### Service Provider Edge



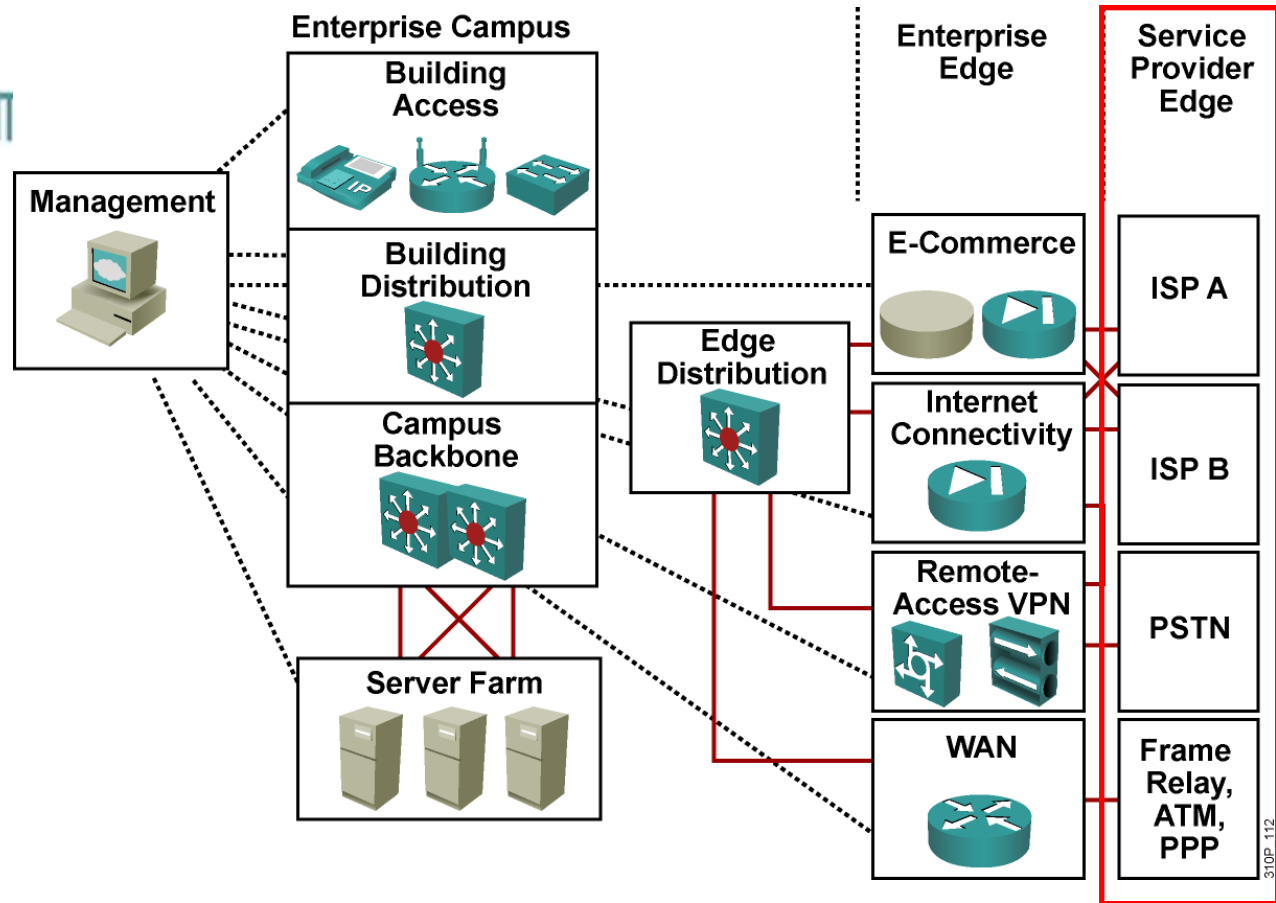
# ECNM



## Enterprise Edge:

- Aggregates connectivity external to the enterprise network.
- As traffic comes into the campus, this area filters traffic from the external resources and routes it into the Enterprise Campus functional area.
- It contains all of the network elements for efficient and secure communication between the enterprise campus and remote locations, remote users, and the Internet.
- The Enterprise Edge would replace the traditional Demilitarized Zone (DMZ) that still exists in many networks.

# ECNM



## Service Provider Edge:

- This functional area represents connections to resources external to the campus.
- This area facilitates communication to WAN and Internet service provider technologies.



A last word about

# cisco switching platforms

# Switch Configuration Interfaces

- In the era of the early high-end Cisco Catalyst switches, the Cisco Catalyst operating system (CatOS) and the command interface were significantly different from the Cisco IOS mode navigation interfaces available on all newer Cisco Catalyst platforms.
- The two interfaces have different features and a different prompt and CLI syntax.
- Two interfaces are used to configure Cisco Catalyst switches
  - Cisco CatOS
  - Cisco IOS
- Cisco CatOS was traditionally used to configure Layer 2 parameters on the modular switches
  - Cisco Catalyst 4000, 5500, 6500 Series
  - These switches now support Cisco IOS (native IOS)
- Cisco IOS is standard software for most other switches and for Layer 3 configuration on the modular switches .

# Cisco Catalyst Operating System (CatOS)

- CatOS is used to configure Layer 2 parameters.
- CatOS configuration commands are prefaced with the keyword **set**.
  - **Console(enable) set port enable 3/5**
- Layer 3 configuration is implemented on MSFC (Multilayer Switching Feature Card) with Cisco IOS.
- Some platforms can now use Cisco IOS to configure both Layer 2 and Layer 3 (native IOS).



**Cisco Catalyst 4000, 5500,  
and 6500 switches**

# Cisco IOS Interface

- On virtually all current Catalyst switches, Cisco IOS is the standard interface for
  - Layer 2 configuration
  - Layer 3 configuration on multilayer switch

