Chapter 1: Routing Services

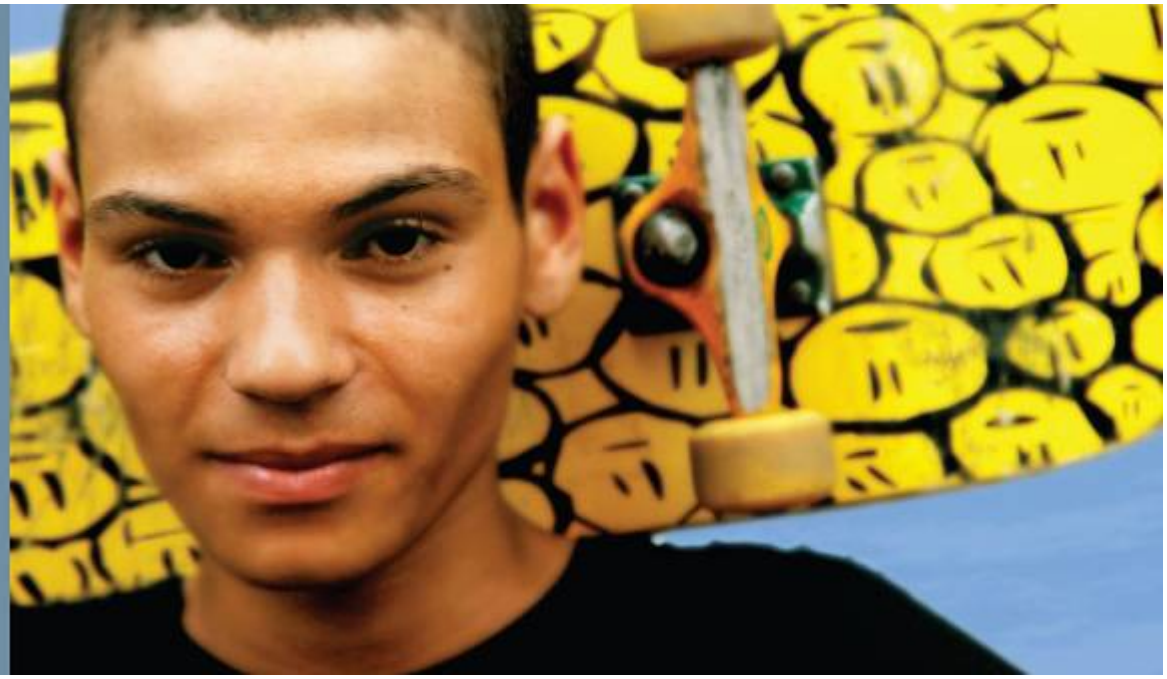
CCNP ROUTE: Implementing IP Routing

Cisco | Networking Academy®
Mind Wide Open™

Chapter 1 Objectives

- Describe common enterprise traffic requirements and network design models.
- Describe how to create a plan for implementing routing services in an enterprise network.
- Review the fundamentals of routing and compare various routing protocols.

Complex Enterprise Network Frameworks, Architectures, and Models



Traffic Conditions in a Converged Network

- Modern networks must support various types of traffic:
  - Voice and video traffic
  - Voice applications traffic
  - Mission-critical traffic
  - Transactional traffic
  - Network management traffic
  - Routing protocol traffic
- This mix of traffic greatly impacts the network requirements such as security and performance.
- To help enterprises, Cisco has developed the Intelligent Information Network (IIN).

Cisco Intelligent Information Network

- The 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.
- The IIN technology vision consists of 3 three phases in which functionality can be added to the infrastructure as required:
  - Integrated transport
  - Integrated services
  - Integrated applications

3 Phases of the IIN

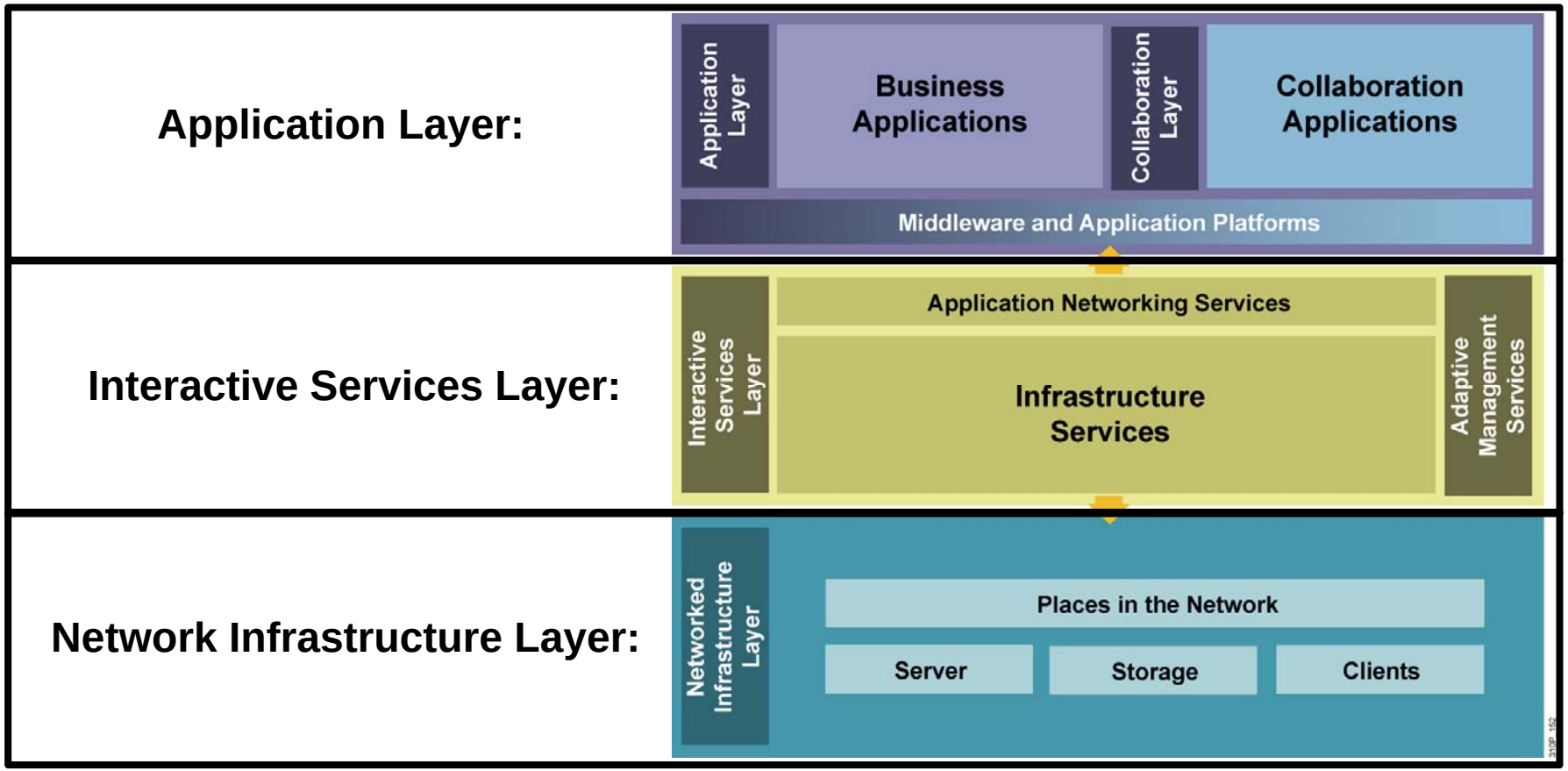
- **Phase 1: Integrated transport**
  - Integrates data, voice, and video transport into a single, standards-based, modular network simplifying network management and generating enterprise-wide efficiencies.
- **Phase 2: Integrated services**
  - Integrated services help to unify common elements, such as storage and data center server capacity.
  - IT resources can now be pooled and shared, or virtualized, to address the changing needs of the organization.
  - Business continuity is also enhanced in the event of a local systems failure because shared resources across the IIN can provide needed services.
- **Phase 3: Integrated applications**
  - This phase focuses on making the network application-aware so that it can optimize application performance and more efficiently deliver networked applications to users.

Cisco SONA Framework

- The Cisco Service-Oriented Network Architecture (SONA) is an architectural framework to create a dynamic, flexible architecture and provide operational efficiency through standardization and virtualization.
  - SONA provides guidance, best practices, and blueprints for connecting network services and applications to enable business solutions.
  - In this framework, the network is the common element that connects and enables all components of the IT infrastructure.
- SONA help enterprises achieve their goals by leveraging:
  - The extensive Cisco product-line services
  - The proven Cisco architectures
  - The experience of Cisco and its partners

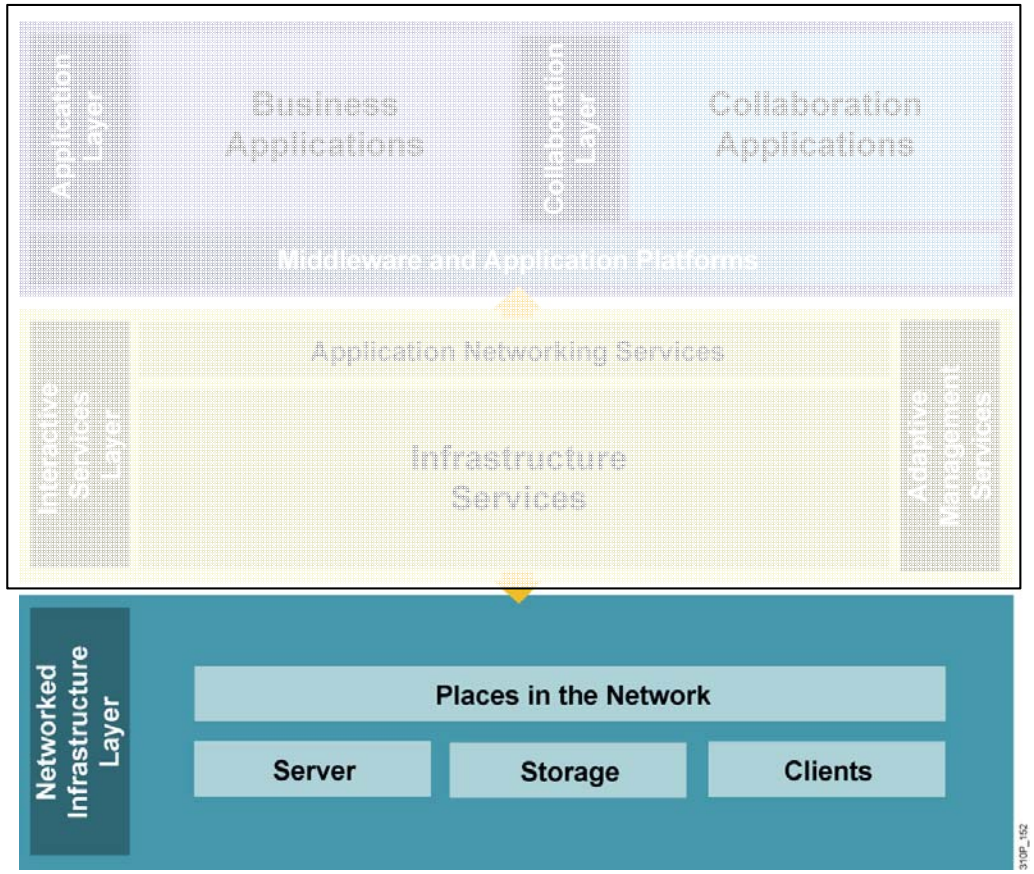
Cisco SONA Framework Layers

The SONA framework outlines three layers:



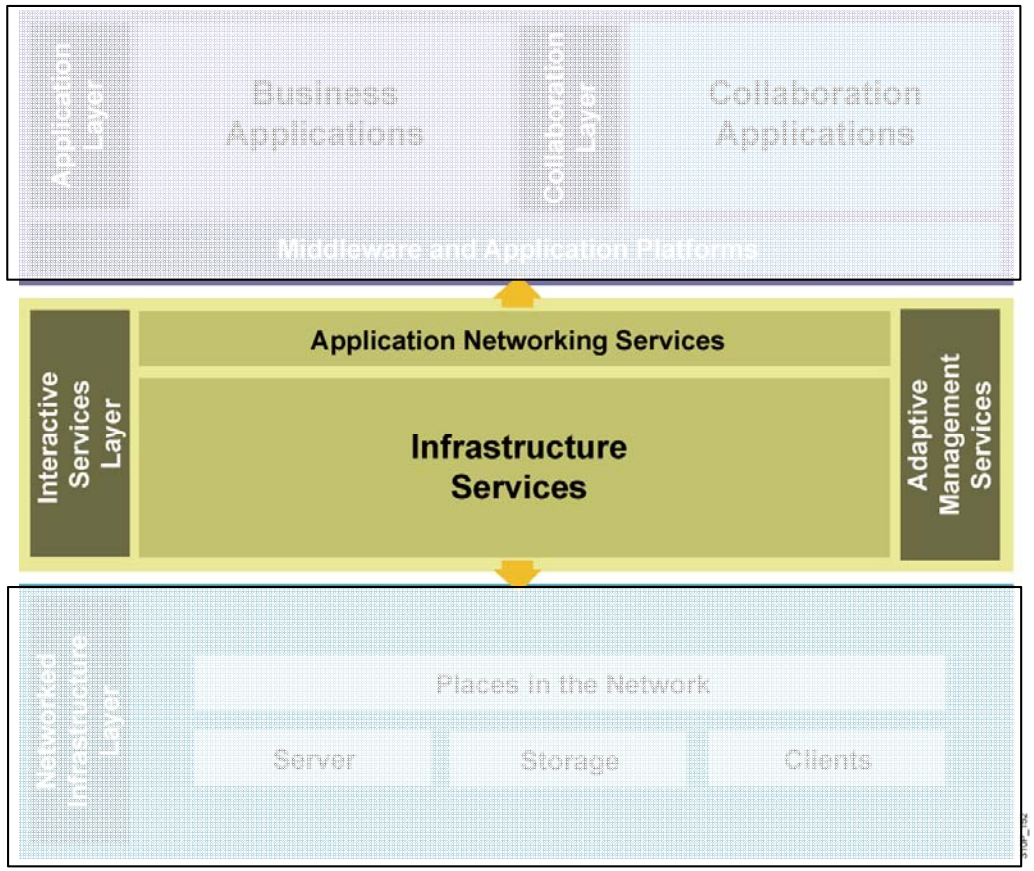
SONA: Network Infrastructure Layer

- This layer provides connectivity anywhere and anytime.
- All the IT resources (servers, storage, and clients) are interconnected across a converged network foundation.
- This layer represents how these resources exist in different places in the network (campus, branch, data center, WAN, MAN and with the teleworker).



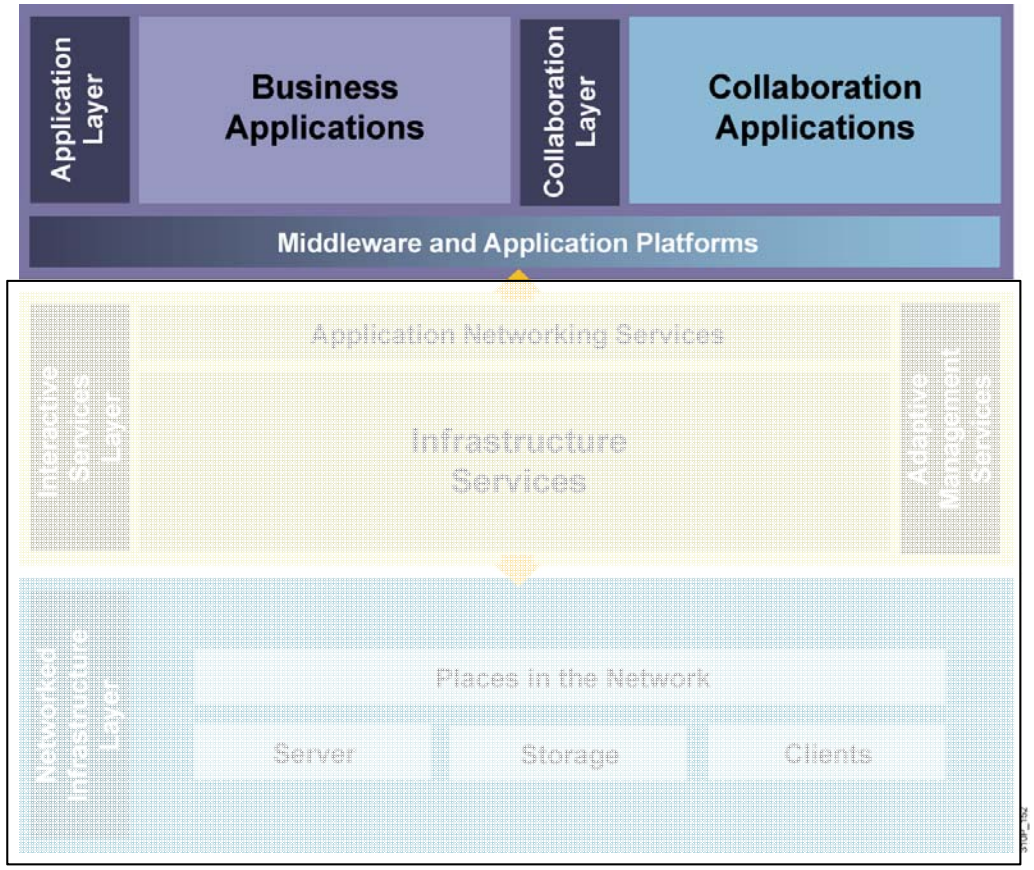
SONA: Interactive Services Layer

- Enables efficient allocation of resources to applications and business processes delivered through the networked infrastructure.
- Application and business processes include:
  - 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



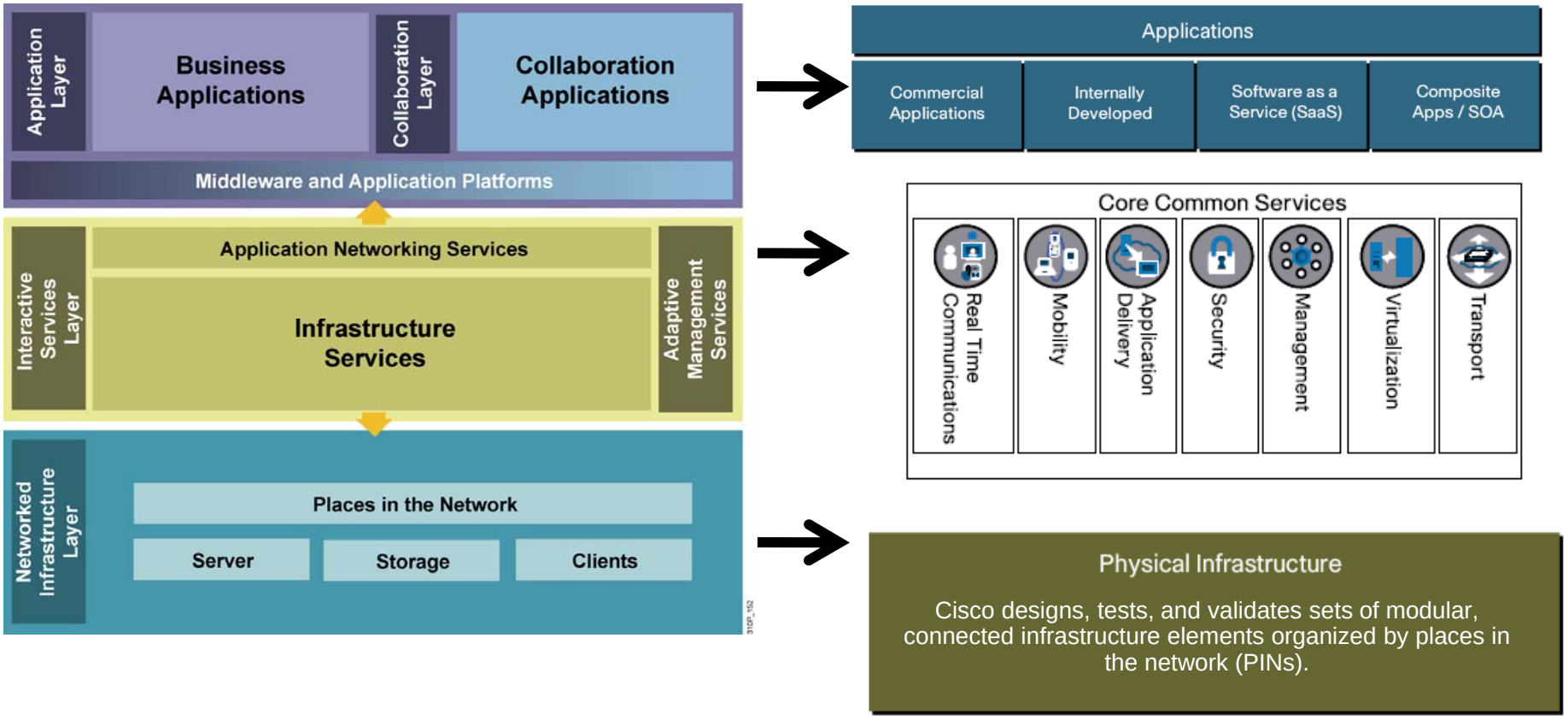
SONA: Application Layer

- This layer's objective is to meet business requirements and achieve efficiencies by leveraging the interactive services layer.
- Includes business applications and collaboration applications such as:
  - Commercial applications
  - Internally developed applications
  - Software as a Services (SaaS)
  - Composite Apps/SOA

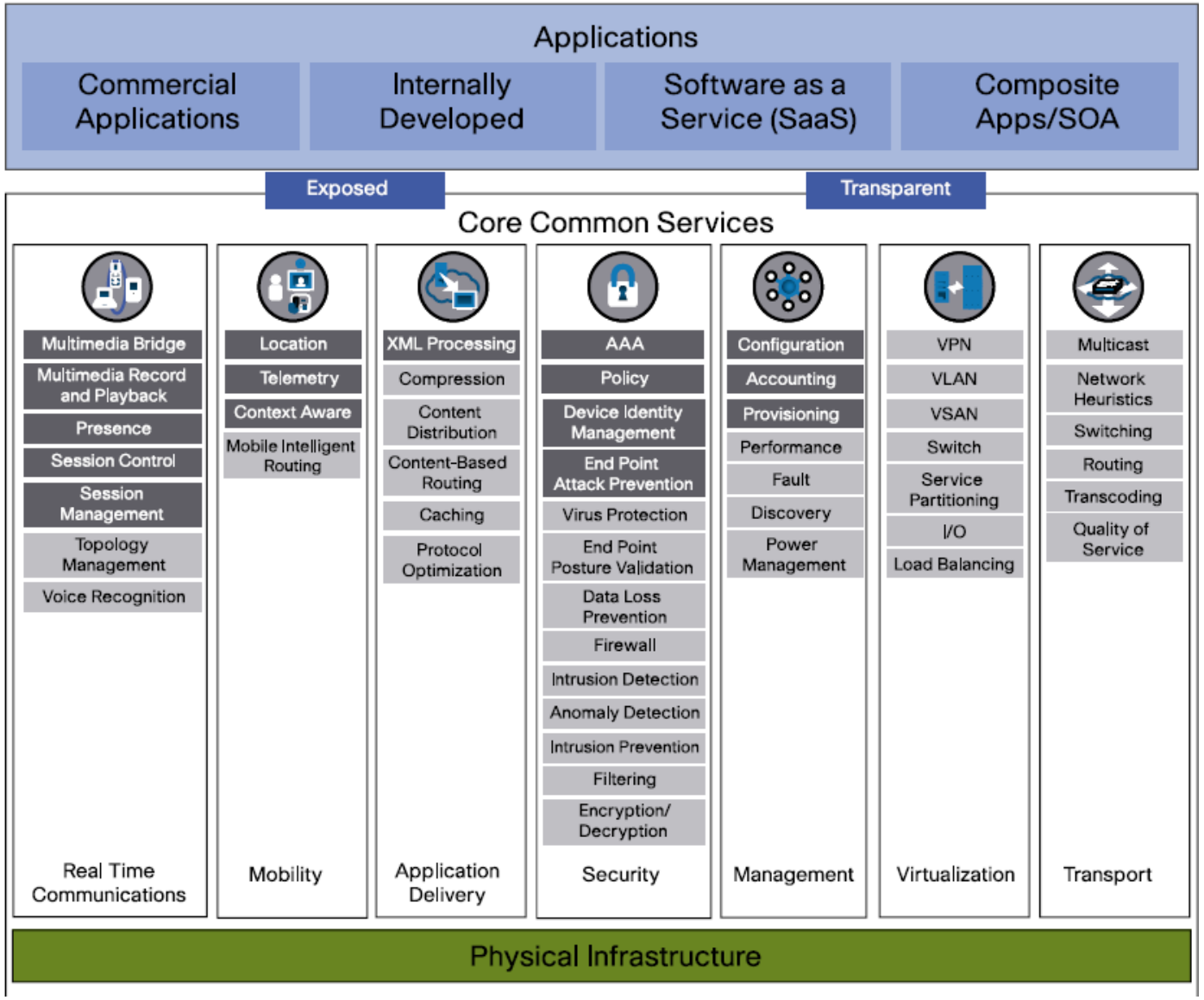


Updated SONA Framework

Cisco Systems has recently updated the SONA framework:

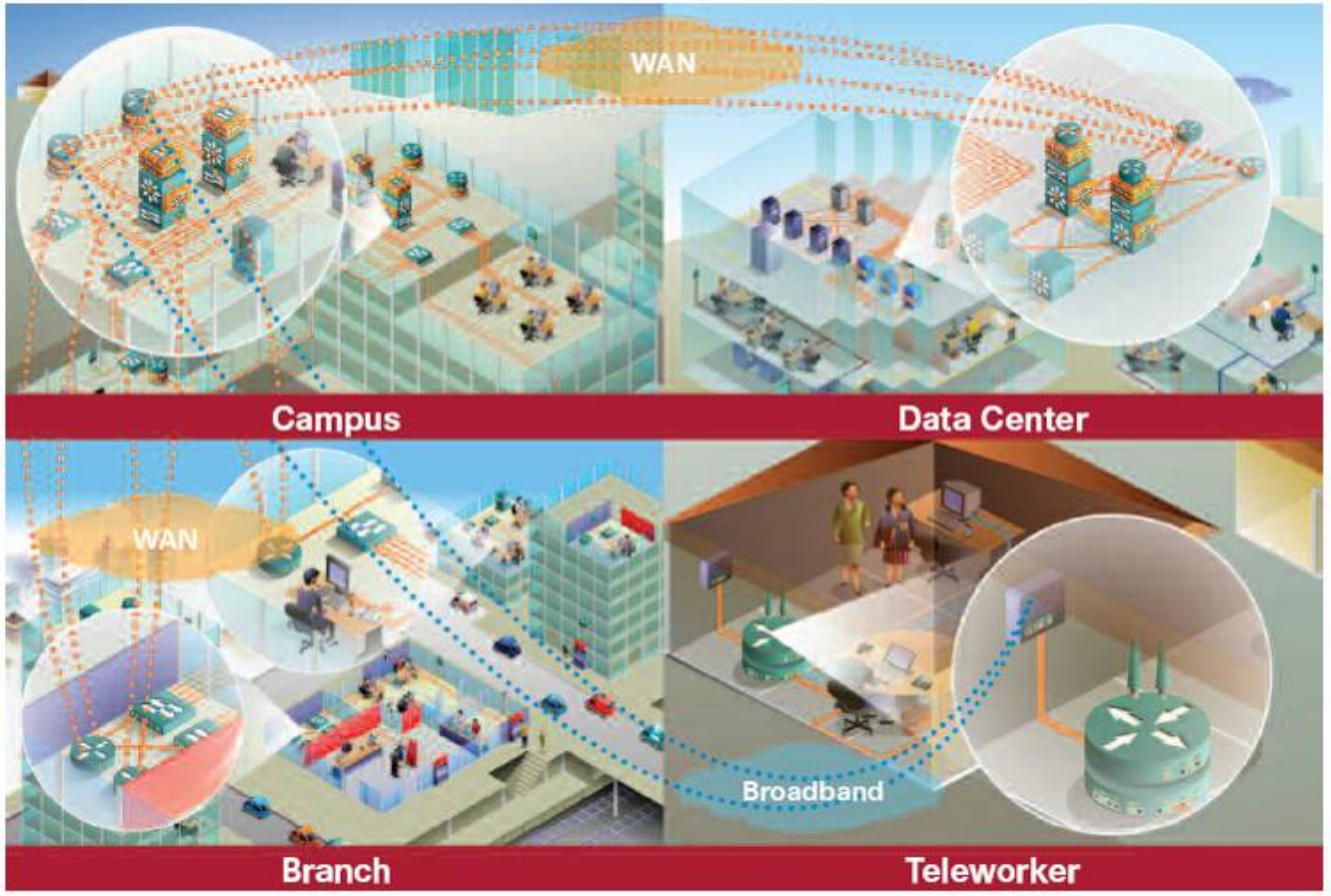


Updated SONA Framework

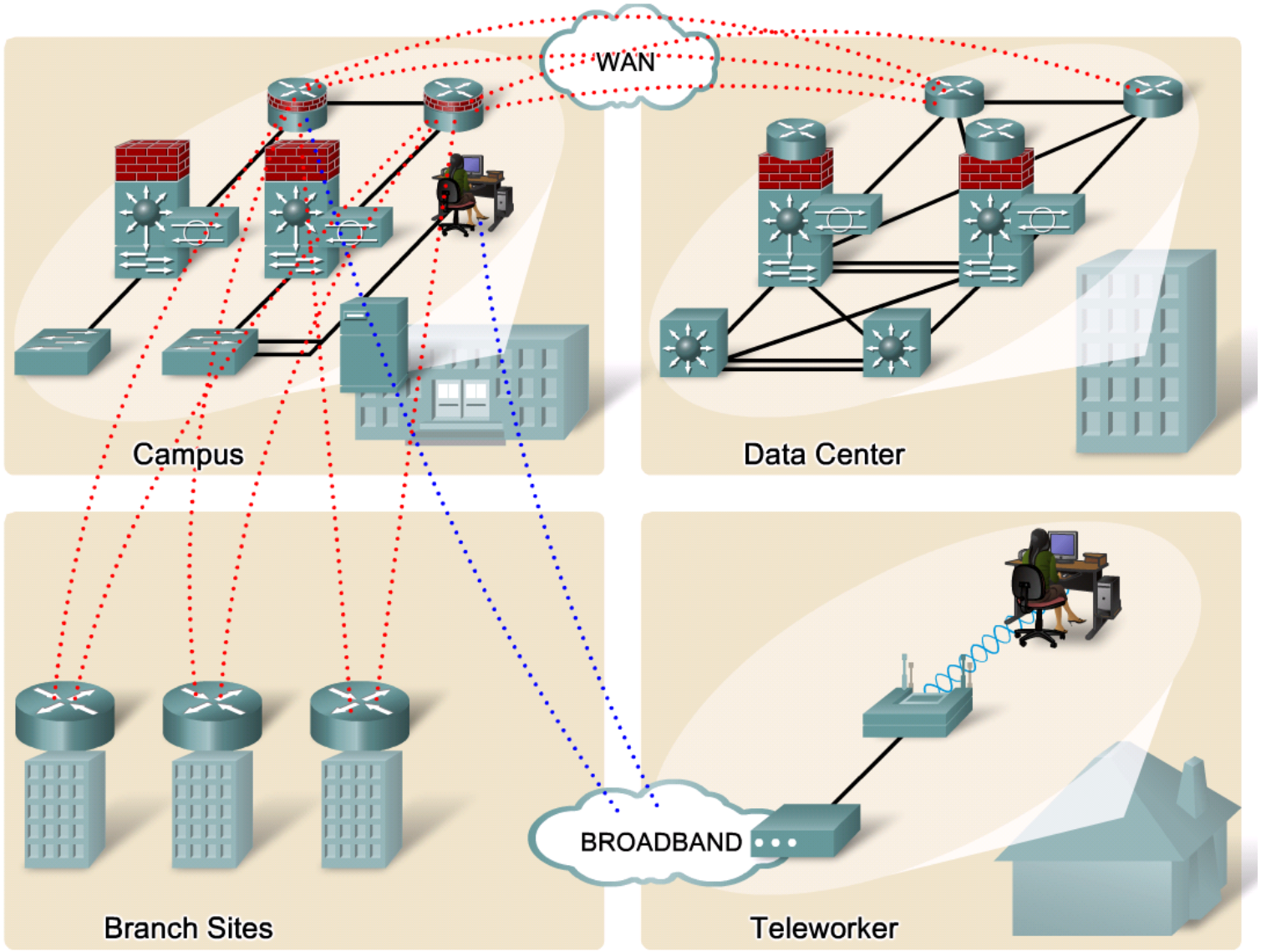


Cisco Enterprise Architecture

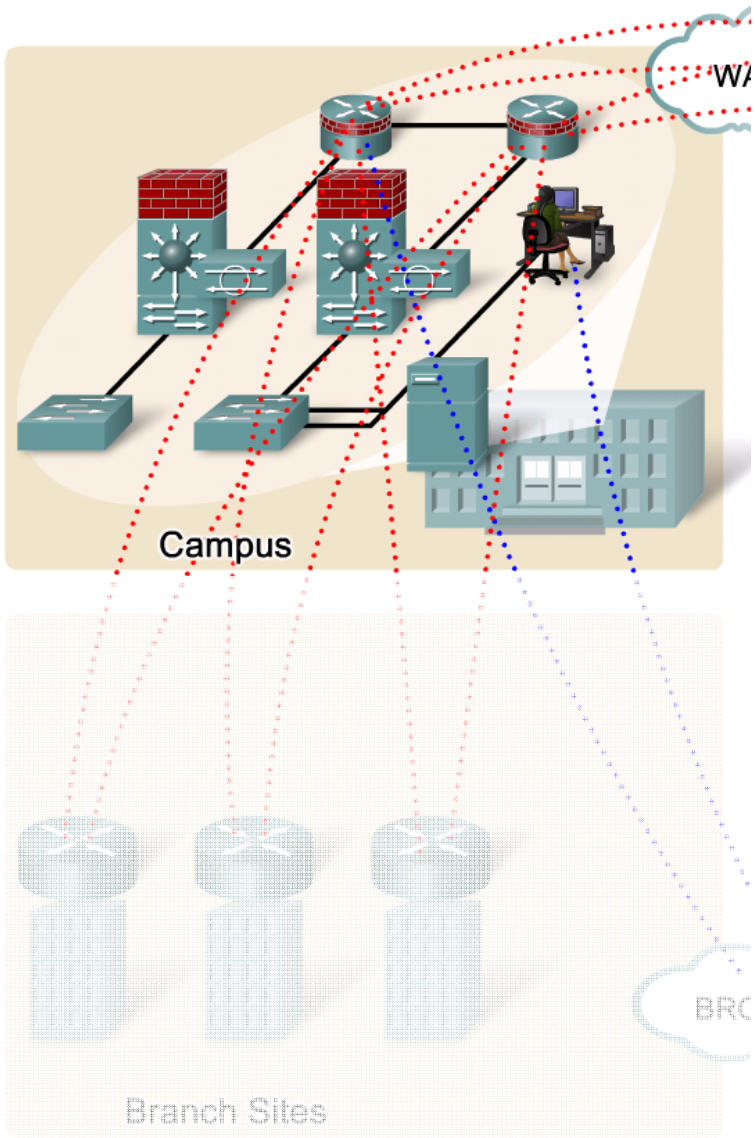
The places in the network in the SONA Network Infrastructure Layer have been identified as follows:



The Cisco Enterprise Architecture



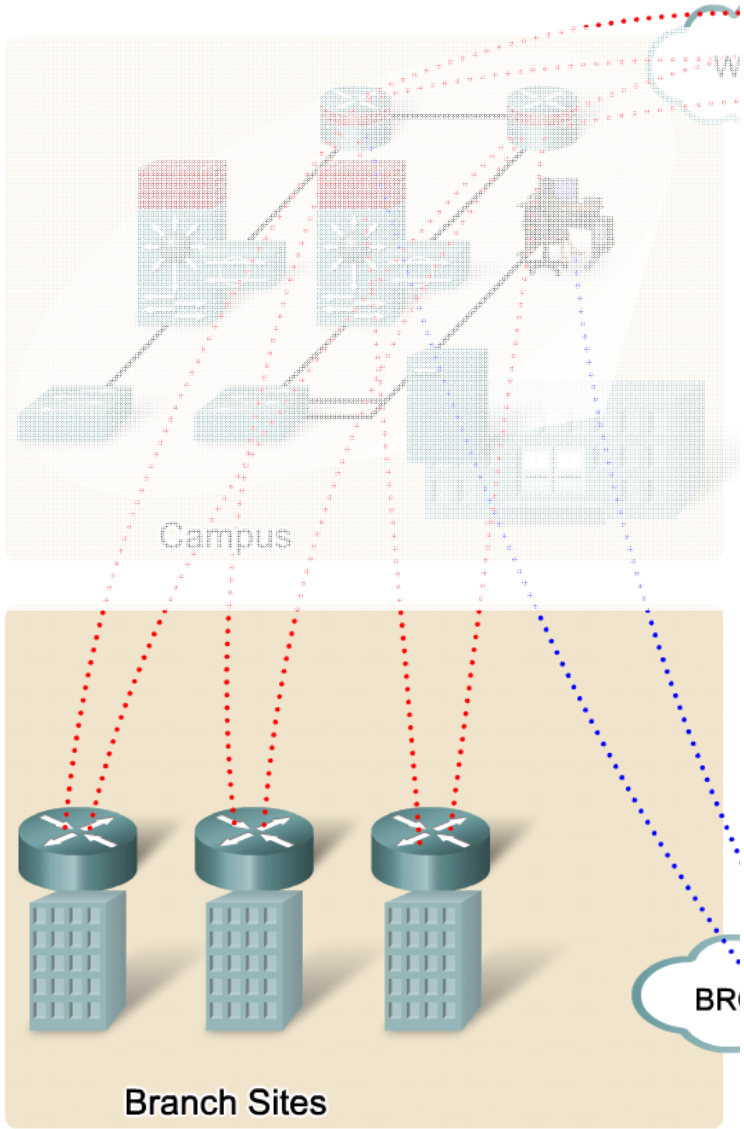
Campus Architecture



Provides:

- High availability with a resilient multilayer design and redundant hardware and software features.
- Automatic procedures for reconfiguring network paths when failures occur.
- Multicast to provide optimized bandwidth consumption.
- Quality of Service (QoS).
- Integrated security.
- Flexibility to add IP security (IPsec) and MPLS VPNs, identity and access management, and VLANs to compartmentalize access.

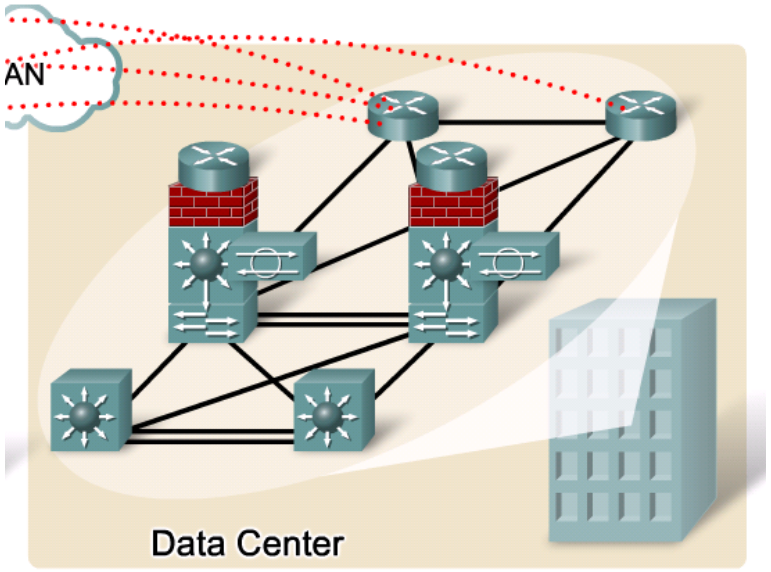
Branch Architecture

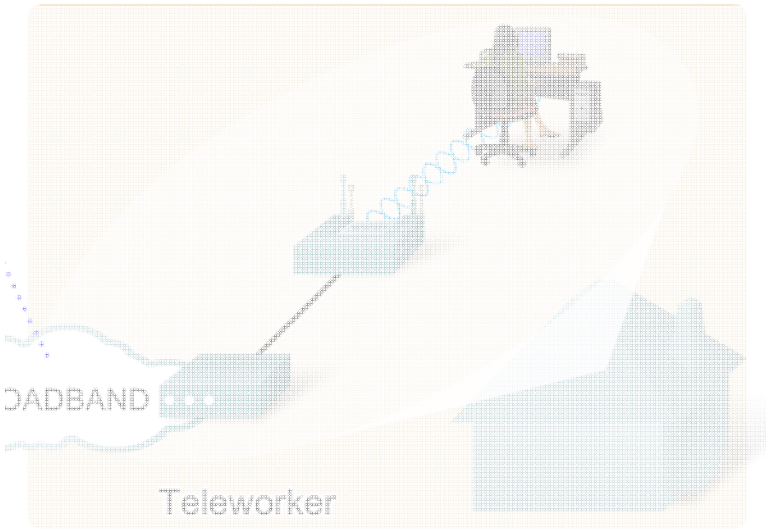


- Provides head-office applications and services, such as security, Cisco IP Communications, and advanced application performance.
- Integrates security, switching, network analysis, caching, and converged voice and video services into a series of integrated services routers in the branch.
- Enterprises can centrally configure, monitor, and manage devices that are located at remote sites.

Data Center Architecture

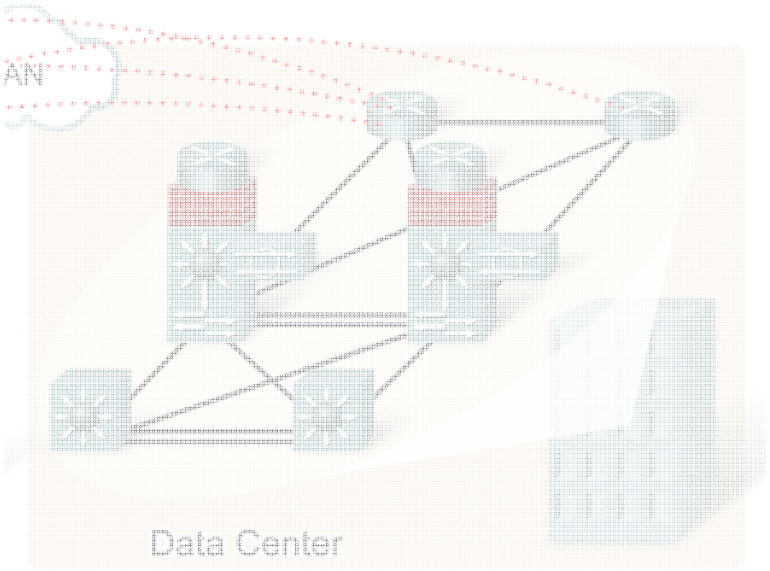
- Adaptive network architecture that supports the requirements for consolidation, business continuance, and security.
- Redundant data centers provide backup services using synchronous and asynchronous data and application replication.
- The network and devices offer server and application load balancing to maximize performance.
- This solution allows the enterprise to scale without major changes to the infrastructure.

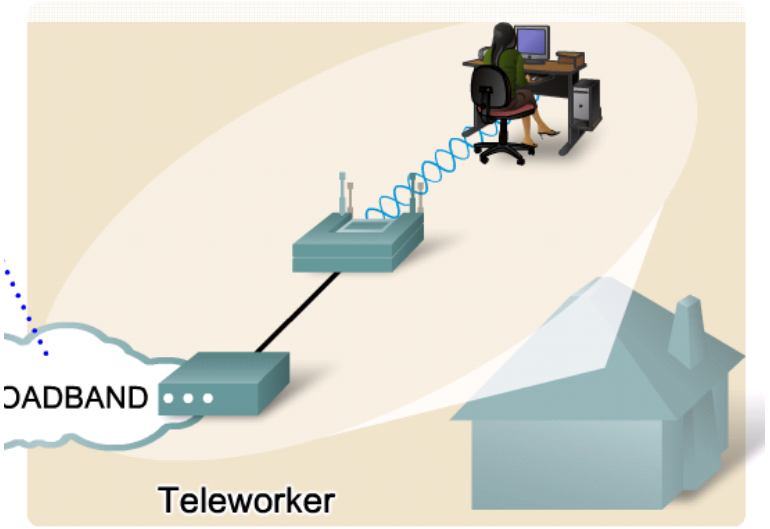




Teleworker Architecture

- Also called the Enterprise Branch-of-One, it allows enterprises to deliver secure voice and data services to remote SOHO offices over a broadband access service.
- Centralized management minimizes the IT support costs.
- Campus security policies are implemented using robust integrated security and identity-based networking services.
  - Staff can securely log on to the network over an always-on VPN and gain access to authorized applications and services.

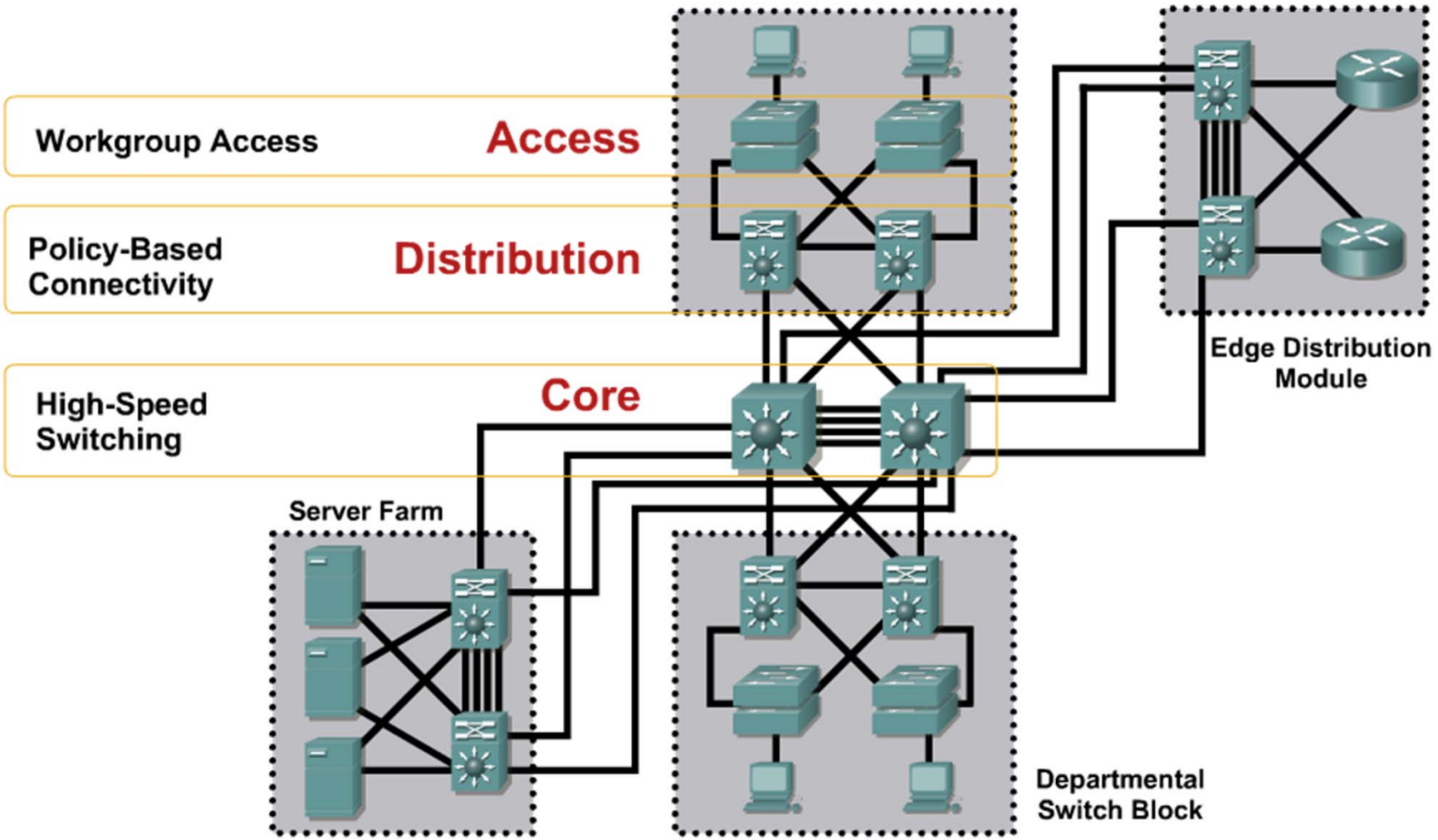




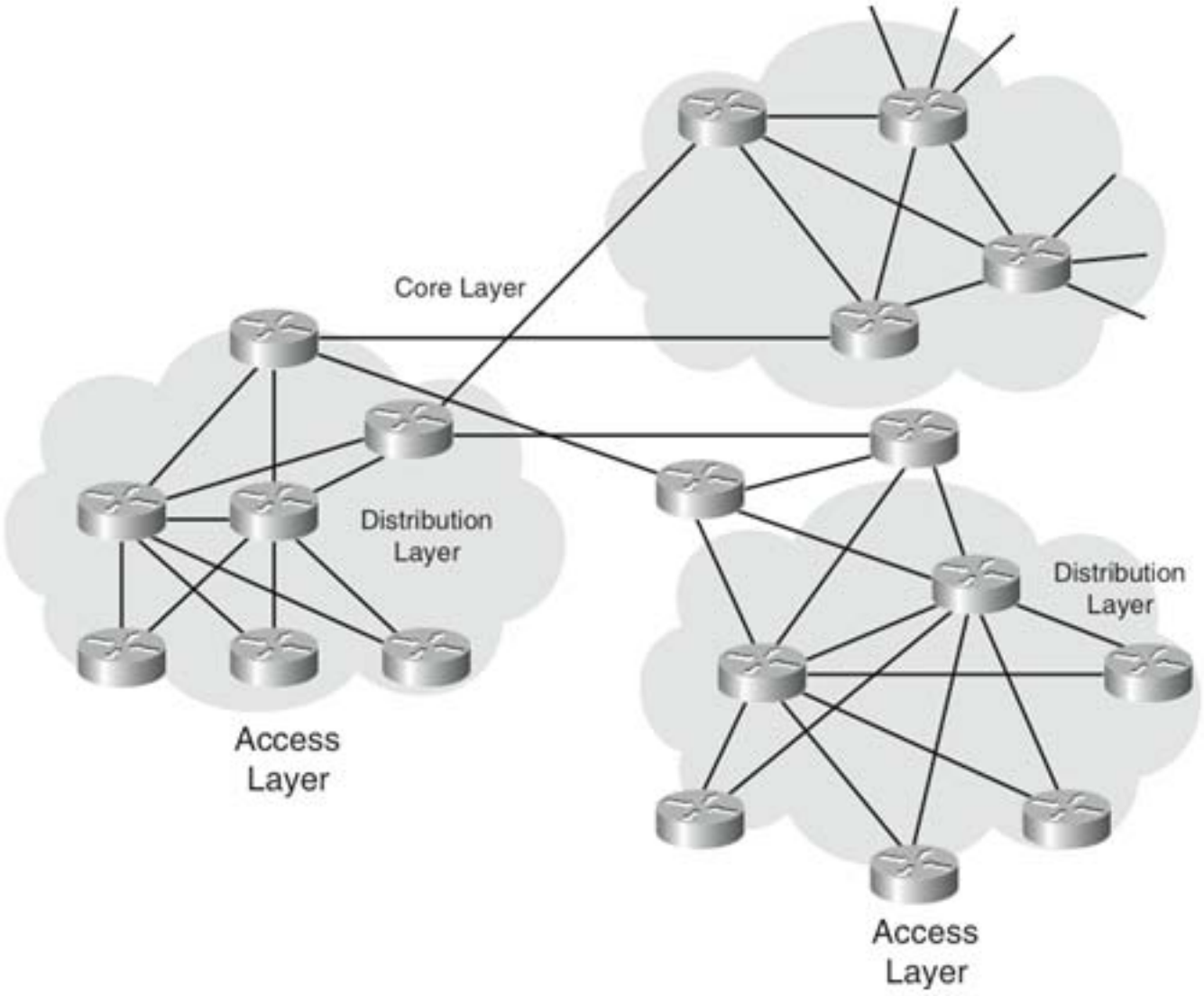
Cisco Hierarchical Network Model

- The three-layer hierarchical model is used extensively in network design.
- The hierarchical model consists of the:
  - Access layer
  - Distribution layer
  - Core layer
- It provides a modular framework that allows design flexibility and facilitates implementation and troubleshooting.
  - The hierarchical model is useful for smaller networks, but does not scale well to today's larger, more complex networks.

Hierarchical Campus Model

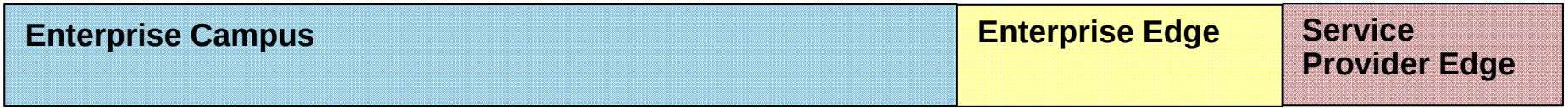


Hierarchical Model Applied to a WAN

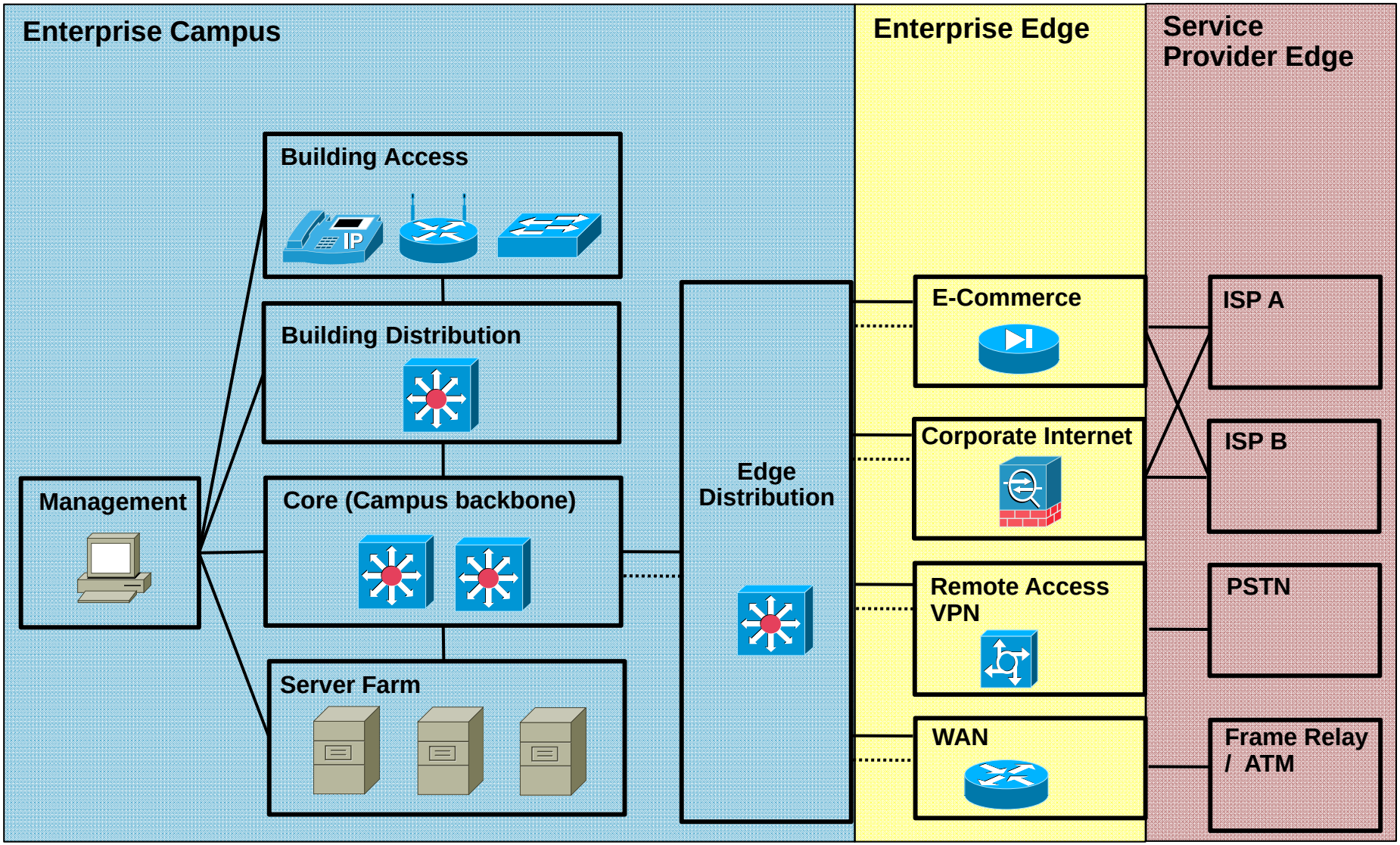


Enterprise Composite Network Model

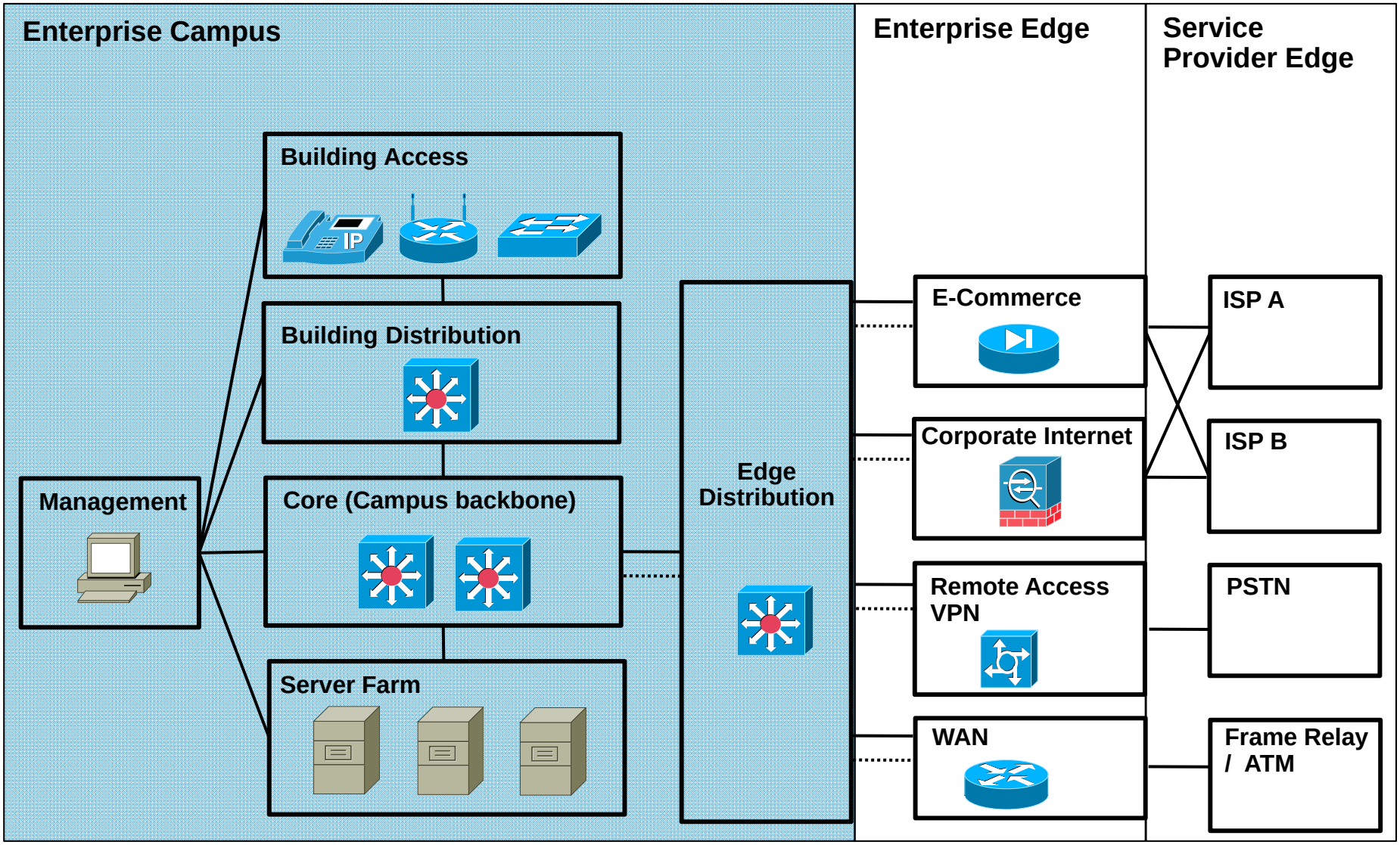
- The Enterprise Composite Network Model divides the network into three functional areas:



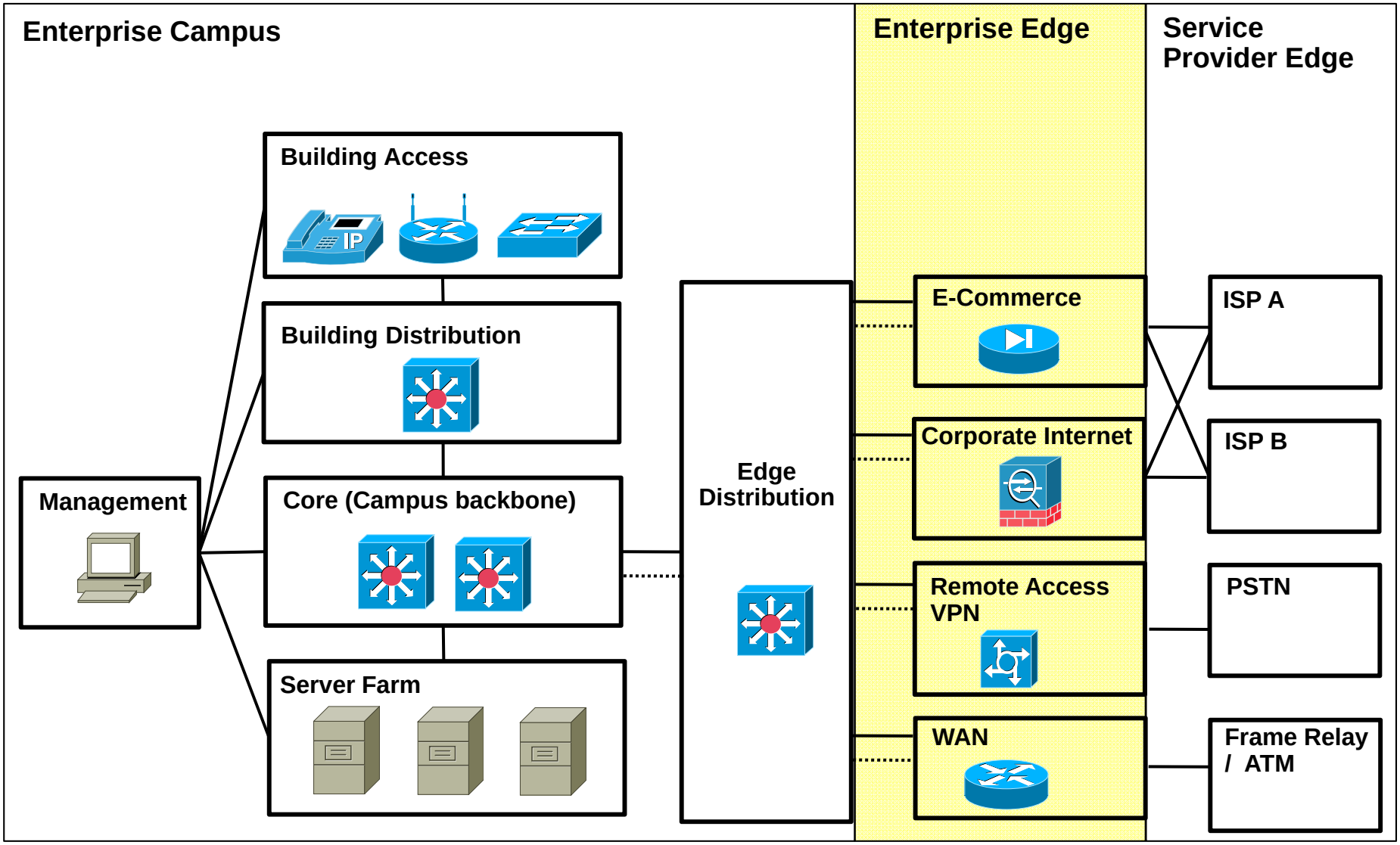
Enterprise Composite Network Model



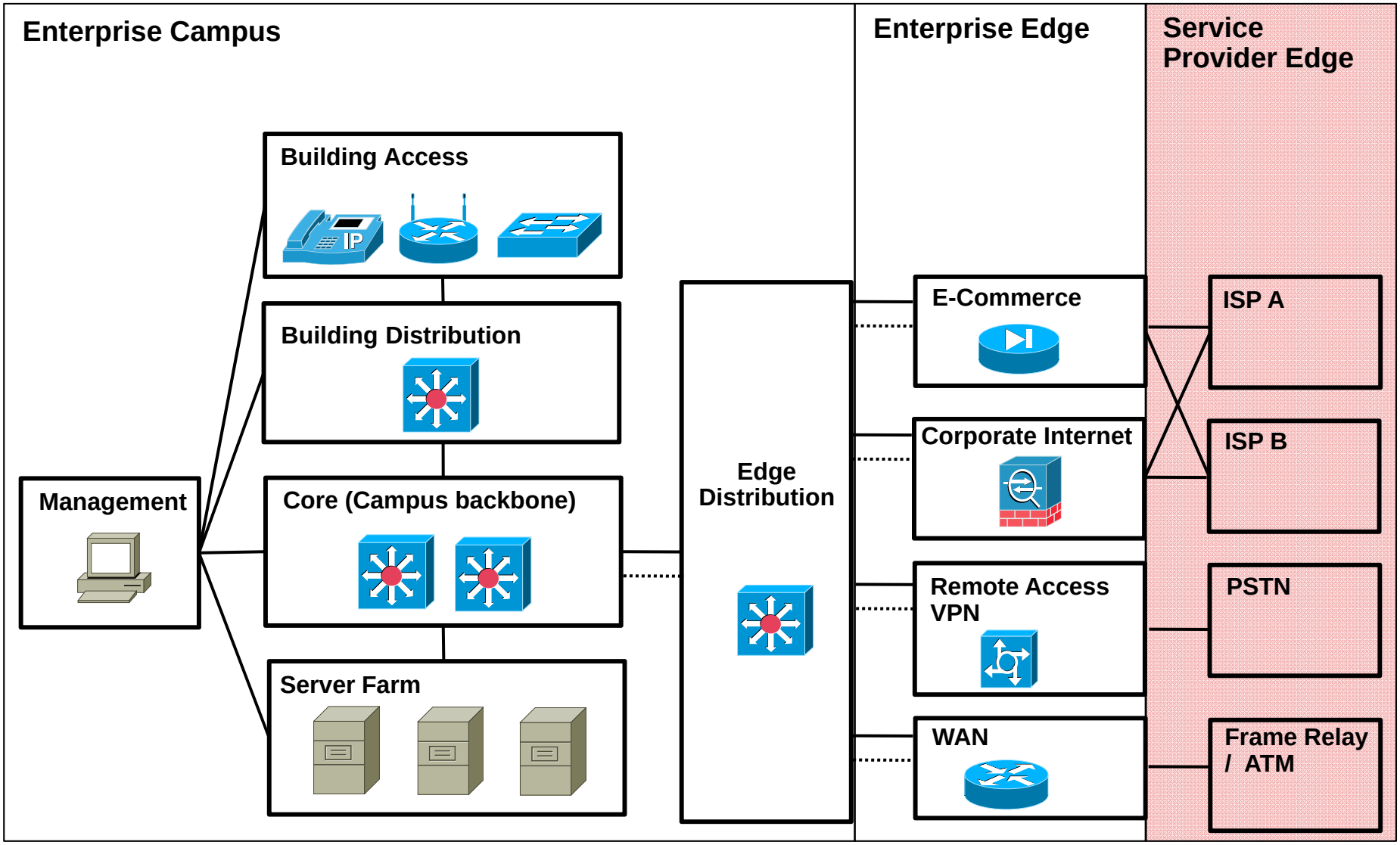
Modules in the Enterprise Campus



Modules in the Enterprise Edge



Modules in the Service Provider Edge



Creating, Documenting, and Executing an Implementation Plan

Creating an Implementation Plan

- An effective, documented implementation plan is a result of good processes and procedures during network design, implementation, and performance testing.
- There are two approaches to implementing changes to a network.
  - Ad-hoc approach
  - Structured approach

Ad-hoc Approach

- The many tasks such as deploying new equipment, connectivity, addressing, routing, and security are implemented and configured as required without planning any of the tasks.
- With such an approach, it is more likely that scalability issues, suboptimal routing, and security issues can occur.
- A good implementation plan is required to avoid such difficulties.

Structured Approach

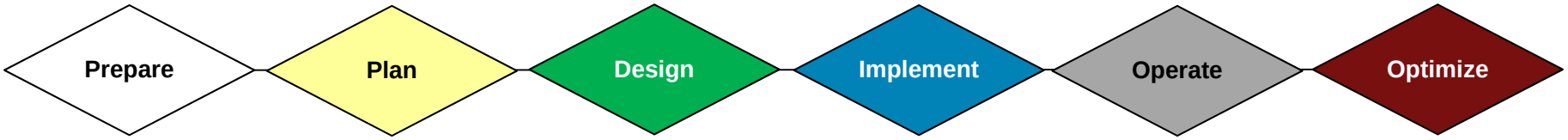
- Prior to implementing a change many considerations are taken into account.
- The design and implementation plan are completed, and may include a new topology, an IP addressing plan, a solution to scalability issues, a link utilization upgrade, remote network connectivity, and changes to other network parameters.
- The design and implementation plan must meet both technical and business requirements.
- All details are documented in the implementation plan prior to the implementation.
  - After successful implementation, the documentation is updated to include the tools and resources used, and the implementation results.

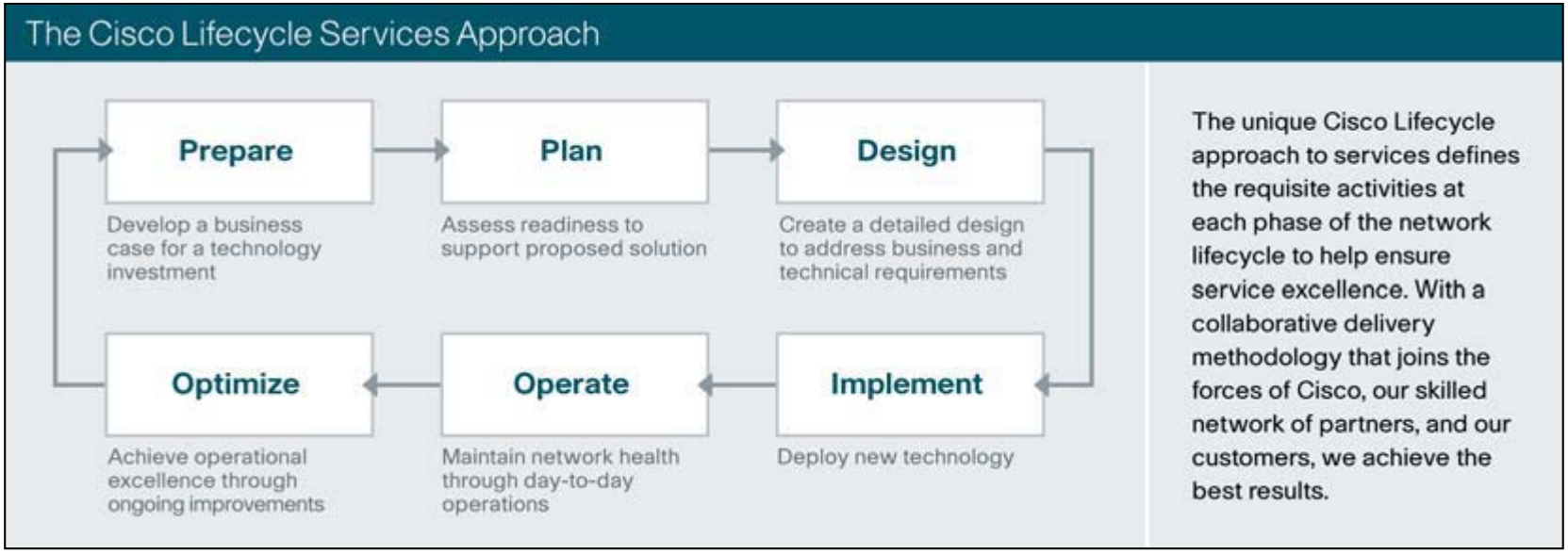
Models and Methodologies

- There are there are many models and methodologies used in IT that define a lifecycle approach using various processes to help provide high quality IT services.
  - No need to reinvent the wheel.
- Examples of these models:
  - The Cisco Lifecycle Services (PPDIOO) model
  - IT Infrastructure Library (ITIL)
  - The Fault, Configuration, Accounting, Performance, and Security (FCAPS) model
    - International Organization for Standardization (ISO)
  - The Telecommunications Management Network (TMN) model
    - Telecommunications Standardization Sector (ITU-T)

Cisco Lifecycle Services (PPDIOO) Model

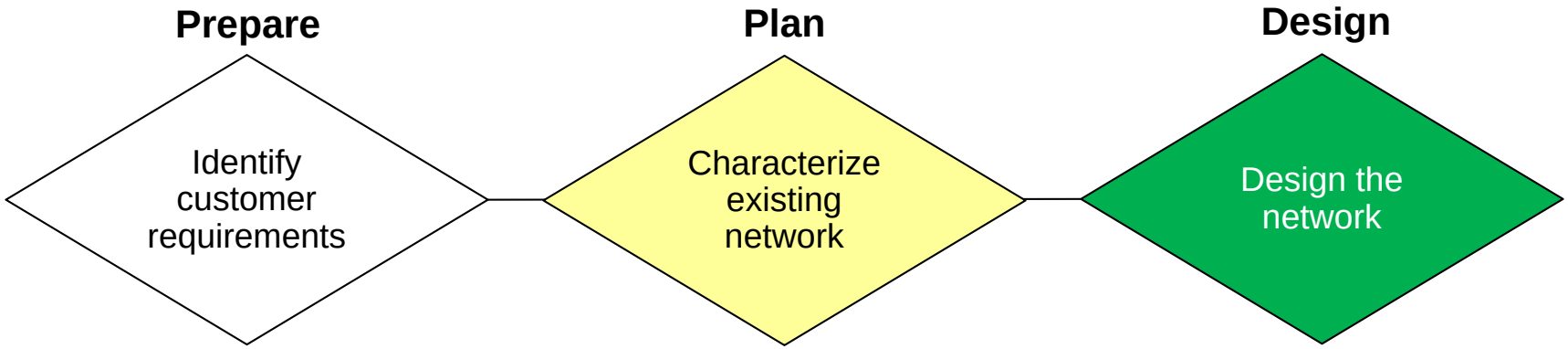
The Cisco Lifecycle Services approach defines six phases in the network lifecycle and is referred to as the PPDIOO model:





PPDIOO – Prepare, Plan, and Design

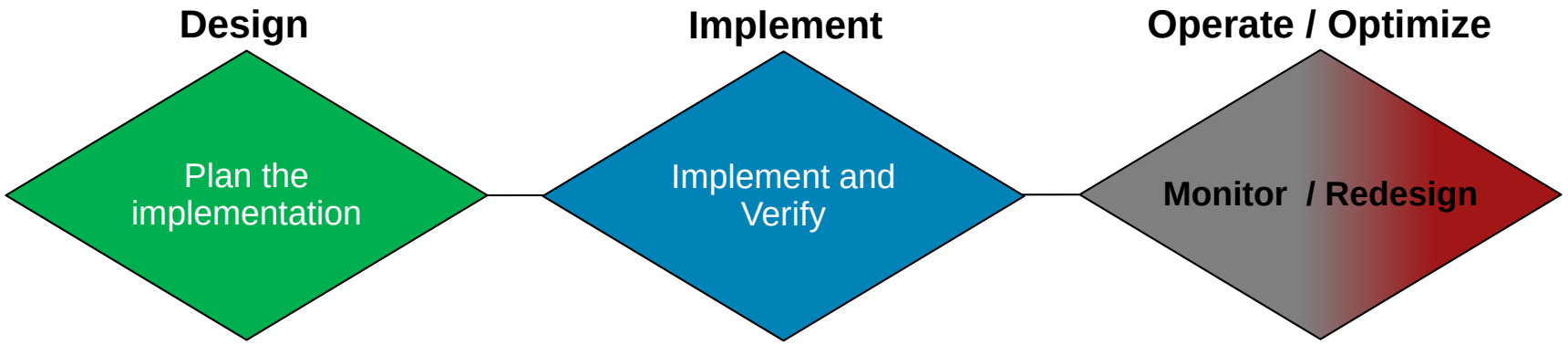
- The PPDIOO methodology begins with these three basic steps:
  - **Step 1: Identify customer requirements**
  - **Step 2: Characterize the existing network and sites**
  - **Step 3: Design the network topology and solutions**



- Once the design is defined, the implementation plan can be executed.

PPDIOO – Implement, Operate, Optimize

- The next three steps include:
  - **Step 4: Plan the implementation**:
  - **Step 5: Implement and verify the design**:
  - **Step 6: Monitor and optionally redesign**:



Implementation Plan documentation

- The implementation plan documentation should include the following:
  - Network information
  - Tools required
  - Resources required
  - Implementation plan tasks
  - Verification tasks
  - Performance measurement and results
  - Screen shots and photos, as appropriate
- The documentation creation process is not finished until the end of the project, when the verification information is added to it.

Sample Implementation Plan

- Project contact list and statements of work, to define all of the people involved and their commitments to the project
- Site and equipment location information and details of how access to the premises is obtained
- Tools and resources required
- Assumptions made
- Tasks to be performed, including detailed descriptions
- Network staging plan

Project Contact List (sample)

Cisco Project Team	<Customer> Project Team
Project Manager: Telephone: Email:	Project Manager: Telephone: Email:
Project Engineer: Telephone: Email:	Project Engineer: Telephone: Email:
Design Engineer: Telephone: Email:	Design Engineer: Telephone: Email:
Account Manager: Telephone: Email:	Account Manager: Telephone: Email:
Systems Engineer: Telephone: Email:	Systems Engineer: Telephone: Email:

Equipment Floor Plan (sample)

Location	Details
Floor	
Room	
Suite	
Position	
Rack No.	

Tools Required (sample)

Item No.	Item
1.	PC with Teraterm, 100BaseT interface, FTP Server and TFTP client applications
2.	Console port cable
3.	Ethernet cable

Implementation Task List (sample)

Step No.	Task
1.	Connect to the router
2.	Verify the current installation and create backup file
3.	Change IOS version (on all routers)
4.	Update IP address configuration (on distribution routers)
5.	Configure EIGRP routing protocol
6.	Verify configuration and record the results

IP Routing Overview

Routing

- This section addresses the ways in which routers learn about networks and how routers can incorporate static and dynamic routes.
- A router can be made aware of remote networks in two ways:
  - An administrator can manually configure the information (static routing)
  - The router can learn from other routers (dynamic routing).
- A routing table can contain both static and dynamically recognized routes.

Static Routes

- A static route can be used in the following circumstances:
  - To have absolute control of routes used by the router.
  - When a backup to a dynamically recognized route is necessary.
  - When it is undesirable to have dynamic routing updates forwarded across slow bandwidth links.
  - To reach a stub network.

Static Routing

- Configure a static route with the `ip route` command.

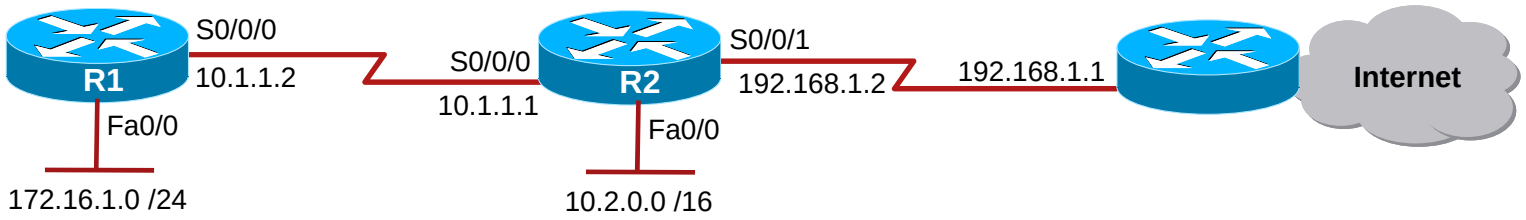
```
Router(config)#
ip route prefix mask address interface dhcp distance name
  next-hop-name permanent track number tag tag
```

Parameter	Description
prefix mask	The IP network and subnet mask for the remote network to be entered into the IP routing table.
address	The IP address of the next hop that can be used to reach the destination network.
interface	The local router outbound interface to be used to reach the destination network.
dhcp	(Optional) Enables a Dynamic Host Configuration Protocol (DHCP) server to assign a static route to a default gateway (option 3).
distance	(Optional) The administrative distance to be assigned to this route.
name *next-hop-name*	(Optional) Applies a name to the specified route.
permanent	(Optional) Specifies that the route will not be removed from the routing table even if the interface associated with the route goes down.
track *number*	(Optional) Associates a track object with this route. Valid values for the number argument range from 1 to 500.
tag *tag*	(Optional) A value that can be used as a match value in route maps.

Configuring a Default Static Route

- R2 is configured with a static route to the R1 LAN and a default static route to the Internet.
- R1 is configured with a default static route.

```
R2(config)# ip route 172.16.1.0 255.255.255.0 S0/0/0
R2(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1
```




```
R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.1
R1(config)# exit
R1# show ip route

<output omitted>
Gateway of last resort is not set
C    172.16.1.0 is directly connected, FastEthernet0/0
C    10.1.1.0 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 10.1.1.1
R1#
```

Dynamic Routing

- Dynamic routing (RIPv1, RIPv2, EIGRP, OSPF, and IS-IS) allows the network to adjust to changes in the topology automatically, without administrator involvement.
- The information exchanged by routers includes the metric or cost to each destination (this value is sometimes called the distance).
  - Different routing protocols base their metric on different measurements, including hop count, interface speed, or more-complex metrics.

On-Demand Routing

- Static routes must be manually configured and updated when the network topology changes.
- Dynamic routing protocols use network bandwidth and router resources.
  - Resource usage of dynamic routing can be considerable.
- A third option is to use the Cisco On-Demand Routing (ODR) feature.
  - ODR uses minimal overhead compared to a dynamic routing protocol and requires less manual configuration than static routes.

ODR

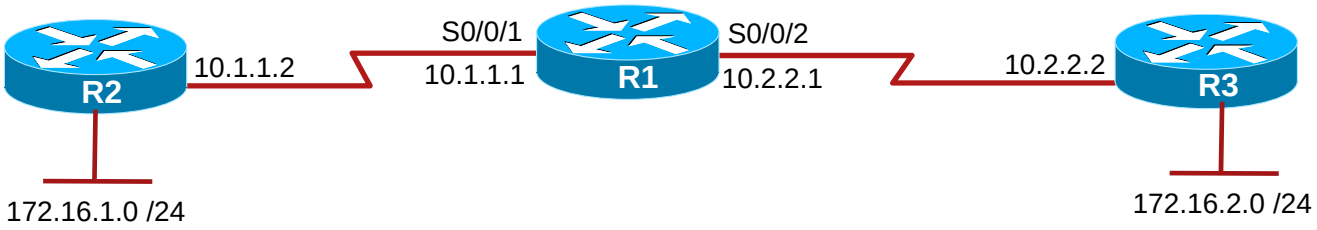
- ODR is applicable in a hub-and-spoke topology only.
- ODR works with the Cisco Discovery Protocol (CDP) to carry network information between spokes and hub router.
- The hub router sends a default route to the spokes that points back to itself and installs the stub networks reported by ODR in its routing table.
  - The hub router can then be configured to redistribute the ODR learned routes into a dynamic routing protocol.

Configuring ODR

- ODR is configured:
  - On all routers, CDP must be enabled.
  - On the hub router using the **`router odr`** global config command.
  - On the stub routers, no IP routing protocol can be configured.
- ODR learned routes appear in the hub router routing table with an entry of “o” and an administrative distance of 160.
  - On each spoke router, the routing table contains only its connected networks and a static default route injected by ODR from the hub.

Configuring ODR

- R1 is a hub router while R2 and R3 are stub routers.
- All routers have CDP enabled.




```
R1(config)# router odr
R1(config)# exit
R1# show ip route

<output omitted>

172.16.0.0/16 is subnetted, 2 subnets
o 172.16.1.0/24 [160/1] via 10.1.1.2, 00:00:23, Serial0/0/1
o 172.16.2.0/24 [160/1] via 10.2.2.2, 00:00:03, Serial0/0/2
<output omitted>
R1#
```

Additional ODR commands.

- ODR can also be tuned with optional commands, including:
  - a distribute list to filter routing updates
  - **`timers basic`** router configuration command to adjust ODR timers
  - **`cdp timer`** global configuration command to adjust the timers and improve convergence time (default is every 60 seconds).

Distance Vector Versus Link-State

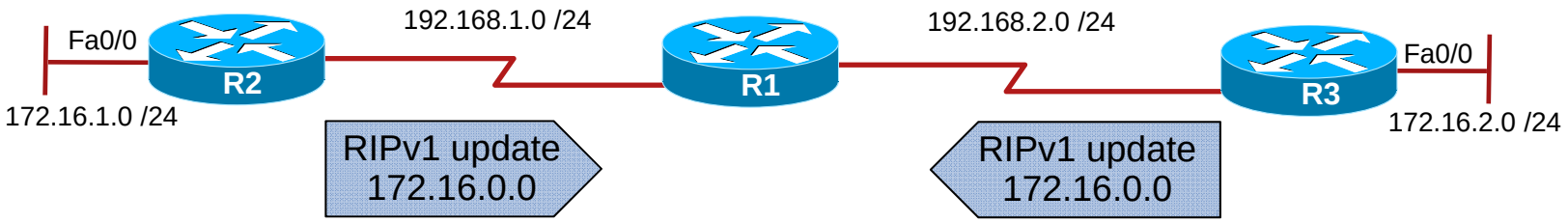
- **Distance vector:**
  - All the routers periodically send their routing tables (or a portion of their tables) to only their neighboring routers.
  - Routers use the received information to determine whether any changes need to be made to their own routing table.
- **Link-state routing protocol:**
  - Each router sends the state of its own interfaces (links) to all other routers in an area only when there is a change.
  - Each router uses the received information to recalculate the best path to each network and then saves this information in its routing table.

Classful Versus Classless Routing

- **Classful Routing Protocol:**
  - Does not support VLSM.
  - Routing updates sent do not include the subnet mask.
  - Subnets are not advertised to a different major network.
  - Discontiguous subnets are not visible to each other.
  - RIP Version 1 (RIPv1) is a classful routing protocol.
- **Classless Routing Protocol:**
  - Supports VLSM.
  - Routing updates sent include the subnet mask.
  - Subnets are advertised to a different major network.
  - Discontiguous subnets are visible to each other.
  - RIPv2, EIGRP, OSPF, IS-IS, and BGP are classless routing protocols.

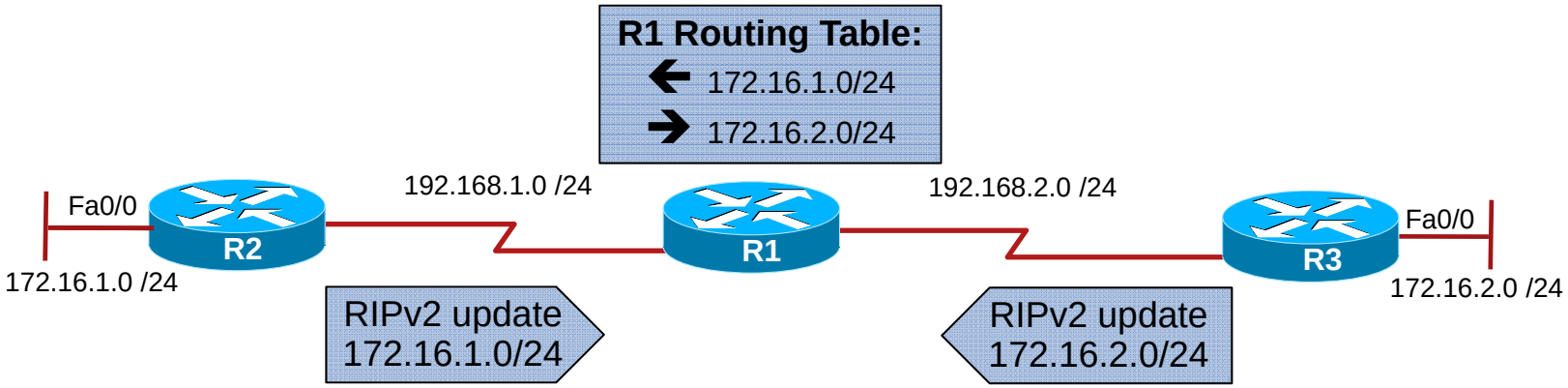
Discontiguous Subnets - Classful Routing

- Classful routing protocols do not support discontiguous networks.
- Discontiguous subnets are subnets of the same major network that are separated by a different major network.
  - For example, RIPv1 has been configured on all three routers.
  - Routers R2 and R3 advertise 172.16.0.0 to R1.
    - They cannot advertise the 172.16.1.0 /24 and 172.16.2.0 /24 subnets across a different major network because RIPv1 is classful.
  - R1 therefore receives routes about 172.16.0.0 /16 from two different directions and it might make an incorrect routing decision.



Discontiguous Subnets - Classless Routing

- Classless routing protocols support discontiguous networks.
  - For example, RIPv2 has been configured on all three routers.
  - Because of RIPv2, routers R2 and R3 can now advertise the 172.16.1.0 /24 and 172.16.2.0 /24 subnets across a different major network.
  - R1 therefore receives routes with valid subnet information and can now make a correct routing decision.



ip classless Command

- The behavior of a classful routing protocol changes when the **`ip classless`** global config command is used.
- Classful protocols assume that if the router knows some of the subnets of a classful network (e.g. 10.0.0.0), then it must know all that network's existing subnets.
  - If a packet arrives for an unknown destination on the 10.0.0.0 subnet and:
    - **`ip classless`** is *not* enabled, the packet is dropped.
    - **`ip classless`** is enabled, then the router will follow the best supernet route or the default route.
- Since IOS release 12.0, **`ip classless`** is enabled by default and should not be disabled.

Automatic Route Summarization

- Classful routing automatically summarize to the classful network boundary at major network boundaries.
- Classless routing protocols either do not automatically summarize or automatically summarize but this feature can be disabled.
  - OSPF or IS-IS do not support automatic network summarization.
  - RIPv2 and EIGRP perform automatic network summarization to maintain backward compatibility with RIPv1 and IGRP.
  - However, automatic summarization can be disabled in RIPv2 and EIGRP by using the **`no auto-summary`** router config command.

Characteristics of Routing Protocols

Characteristics	RIPv1	RIPv2	EIGRP	IS-IS	OSPF	BGP
Distance vector	✓	✓	✓			✓
Link-state				✓	✓	
Classless		✓	✓	✓	✓	✓
VLSM support		✓	✓	✓	✓	✓
Automatic route summarization	✓	✓ (can be disabled using **`no auto-summary`**)	✓ (can be disabled using **`no auto-summary`**)			✓
Manual route summarization		✓	✓	✓	✓	✓
Hierarchical topology required				✓	✓	
Size of network	Small	Small	Large	Large	Large	Very large
Metric	Hops	Hops	Composite metric	Metric	Cost	Path attributes
Convergence time	Slow	Slow	Very fast	Fast	Fast	Slow

Routing Protocol Specifics

Routing Protocol	Protocol Number	Port Number	Admin Distance
RIP	--	UDP 520	120
IGRP	9	--	100
EIGRP	88	--	90 Summary Routes – 5 Redistributed Routes – 170
OSPF	89	--	110
IS-IS	124	--	115
BGP	--	TCP 179	eBGP – 20 iBGP – 200

Routing Table Criteria

- The best route selected from various routing protocols for a specific destination is chosen by considering the following four criteria:
  - Valid next-hop IP address.
  - Administrative distance
  - Metric
  - Prefix

Administrative Distance

- Cisco routers use a value called administrative distance to select the best path when they learn of two or more routes to the same destination with the same prefix from different routing protocols.
- Administrative distance rates a routing protocol's *believability*.
- Cisco has assigned a default administrative distance value to each routing protocol supported on its routers.
  - Each routing protocol is prioritized in the order of most to least believable.

Administrative Distances

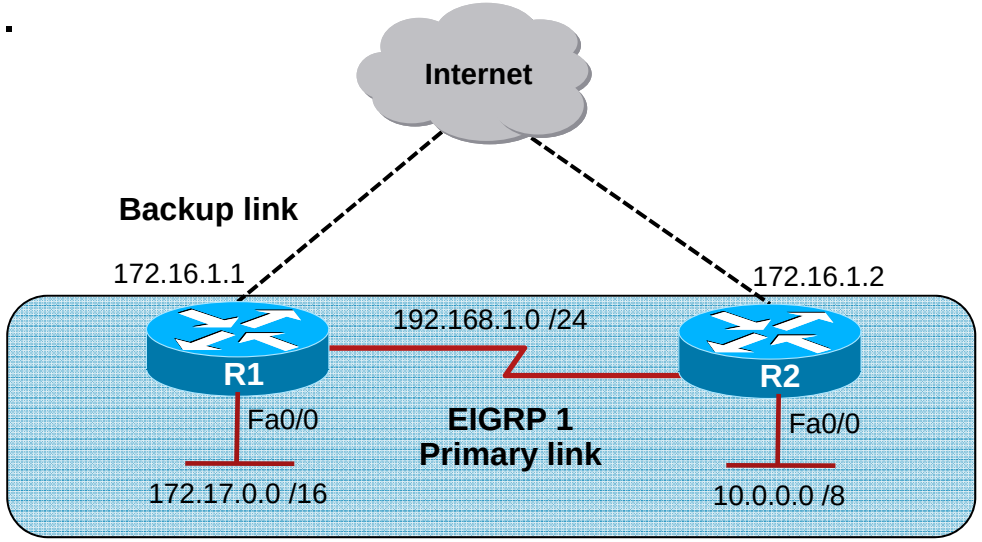
Route Source	Default Distance	Routing Table Entry
Connected interface	0	C
Static route out an interface	0	S
Static route to a next-hop address	1	S
EIGRP summary route	5	D
External BGP	20	B
Internal EIGRP	90	D
IGRP	100	I
OSPF	110	O
IS-IS	115	i
RIPv1, RIPv2	120	R
Exterior Gateway Protocol (EGP)	140	E
ODR	160	O
External EIGRP	170	D EX
Internal BGP	200	B
Unknown	255	

Floating Static Route

- Routers believe static routes over any dynamically learned route.
- To change this default behavior and make a static route appear in the routing table only when the primary route goes away, create a **floating static** route.
  - The administrative distance of the static route is configured to be higher than the administrative distance of the primary route and it "floats" above the primary route, until the primary route fails.
- To configure a static route use the **`ip route`** command with the *distance* parameter.

Configuring a Floating Static Route

- Create floating static routes on R1 and R2 that floats above the EIGRP learned routes.




```
R1(config)# ip route 10.0.0.0 255.0.0.0 172.16.1.2 100
R1(config)# router eigrp 1
R1(config-router)# network 172.17.0.0
R1(config-router)# network 192.168.1.0
```

```
R2(config)# ip route 172.17.0.0 255.255.0.0 172.16.1.1 100
R2(config)# router eigrp 1
R2(config-router)# network 10.0.0.0
R2(config-router)# network 192.168.1.0
```

Routing Within the ECNM

- Routing protocols are an integral part of any network.
  - When designing a network routing protocol, selection and planning are among the design decisions to be made.
- Although the best practice is to use one IP routing protocol throughout the enterprise if possible, in some cases multiple routing protocols might be required.

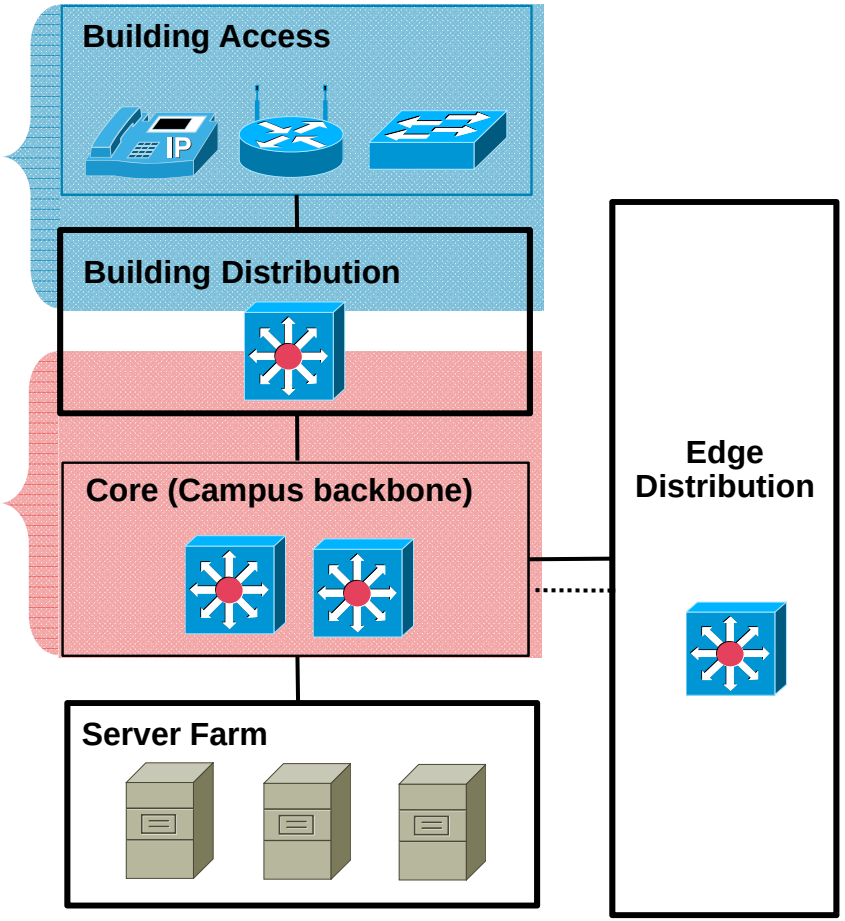
Suggested Routing Protocols Used

Between Building Access and Building Distribution:

RIPv2, OSPF, EIGRP, Static routes

Between Building Distribution and Core:

OSPF, EIGRP, IS-IS and BGP



Routing Within the ECNM

- The Enterprise Composite Network Model can assist in determining where each routing protocol is implemented, where the boundaries between protocols are, and how traffic flows between them will be managed.

Chapter 1 Summary

- Traffic in converged networks includes voice and video, voice applications, mission-critical, transactional, routing protocol, and network management.
- The three phases of the Cisco IIN: integrated transport, integrated services, and integrated applications.
- The three layers of the Cisco SONA architectural framework: networked infrastructure, interactive services, application.
- The components of the Cisco Enterprise Architecture for integration of the entire network: campus, data center, branches, teleworkers, and WAN.
- The traditional hierarchical network model with its three layers: core, distribution, and access.
- The Cisco Enterprise Composite Network Model with its three functional areas and their associated modules:
  - Enterprise Campus: Building, Building Distribution, Core, Edge Distribution, Server Farm, Management
  - Enterprise Edge: E-commerce, Corporate Internet, VPN and Remote Access, WAN
  - Service Provider Edge: ISP, PSTN, Frame Relay/ATM.

Chapter 1 Summary (continued)

- The two approaches to implementing changes to a network: using an ad-hoc approach or using a structured approach.
- Four models used in IT services lifecycles: Cisco Lifecycle Services (PPDIOO), ITIL, FCAPS, and TMN.
- Creating an implementation plan, as part of the network Design phase, that includes:
  - Network information
  - Tools required
  - Resources required
  - Implementation plan tasks
  - Verification tasks
  - Performance measurement and results}

Chapter 1 Summary (continued)

- Static routing characteristics and configuration.
- Characteristics and configuration of ODR, which uses CDP to carry network information between spoke (stub) routers and the hub router.
- Dynamic routing protocol characteristics, including:
  - The metric, a value (such as path length) that routing protocols use to measure paths to a destination.
  - Configuration, using the **router** *protocol* global configuration command.
  - Distance vector routing, in which all the routers periodically send their routing tables (or a portion of their tables) to only their neighboring routers.
  - Link-state routing, in which each of the routers sends the state of its own interfaces (its links) to all other routers (or to all routers in a part of the network, known as an area) only when there is a change.
  - Hybrid routing, in which routers send only changed information when there is a change (similar to link-state protocols) but only to neighboring routers (similar to distance vector protocols).
  - Classful routing protocol updates, which do not include the subnet mask. Classful protocols do not support VLSM or discontiguous subnets and must automatically summarize across the network boundary to the classful address.
  - Classless routing protocol updates, which do include the subnet mask. Classless protocols do support VLSM and discontiguous subnets, and do not have to summarize automatically across network boundaries.
- The process that Cisco routers use to populate their routing tables includes a valid next-hop IP address, Administrative distance, metric, and prefix.

Chapter 1 Labs

- **Lab 1-1 Tcl Script Reference and Demonstration**