CHAPTER 4

Solution Implementation

Overview

Cisco customers have asked Cisco to provide insight into how Cisco products can be used to address PCI DSS 2.0 requirements. To fully accomplish this goal, Cisco hired an auditor and went through the same process as organizations. To audit Cisco products for the capability to address compliance, they had to be installed and configured within a representative design.

This chapter demonstrates how the Cisco PCI solution was installed and configured to address the specifications of PCI 2.0. Cisco partnered with RSA, HyTrust, EMC, VCE, and Verizon Business to create a comprehensive design that reflected the framework and architectural principles discussed in earlier chapters.

The Cisco PCI solution was validated in the Cisco Lab in San Jose, California. The branches, data center, WAN, and Internet edge network infrastructures were built using Cisco best practice design guides, as represented by the Cisco enterprise architecture (http://www.cisco.com/go/designzone). The individual components were installed and configured to adhere to PCI 2.0 specifications. Verizon Business then conducted an assessment of the design and advised on remediation for specific configurations of individual components. After the remediation was complete, Verizon Business provided a detailed reference architecture report (see Appendix C, "Verizon Business Reference Architecture Report—Cisco PCI Solution.")

Tip An ***architecture*** is a strategic structure for the consistent design, construction, and operation of systems to achieve a desired set of outcomes.

A ***design*** is a tactical implementation of an architectural strategy, using specific configurations of products to satisfy business requirements.

Chapter 3, "Solution Architecture," describes the enterprise architecture with regards to compliance. This chapter demonstrates a design or, in other words, a specific implementation of components to achieve these principles. Various designs can result from the solution architecture. The design that was implemented is not intended to represent the only way that Cisco and partner products can be installed to address PCI. It is intended to provide an example showing how and what was used to achieve the principles described in Chapter 3, "Solution Architecture."

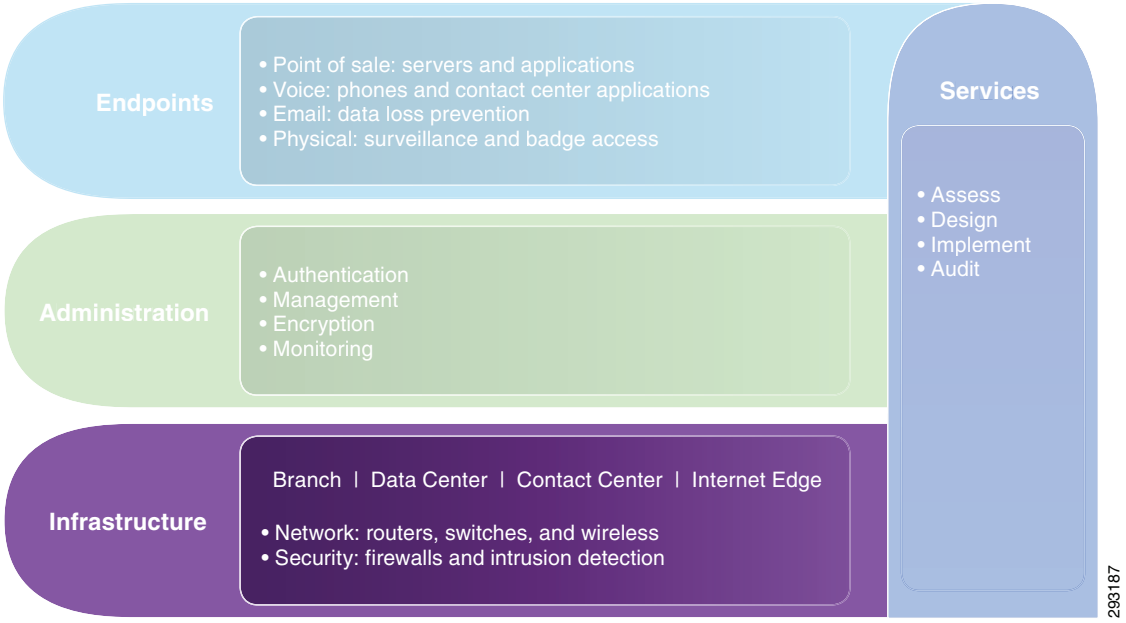
Although every company has specific considerations that vary from this implementation, these designs and the configurations of the components in Appendix E, "Detailed Full Running Configurations," provide an instructive example of what is needed to secure credit card data. Each component selected was audited for its capabilities, and that assessment is covered in the next chapter.

In each section, the reference architecture is shown with the corresponding design that was implemented and validated within the Cisco PCI laboratories. The full configurations of each individual component are available in Appendix E, "Detailed Full Running Configurations."

Infrastructure

The infrastructure layer of the solution framework addresses the components such as routers, switches, firewalls, and security components, as shown in Figure 4-1.

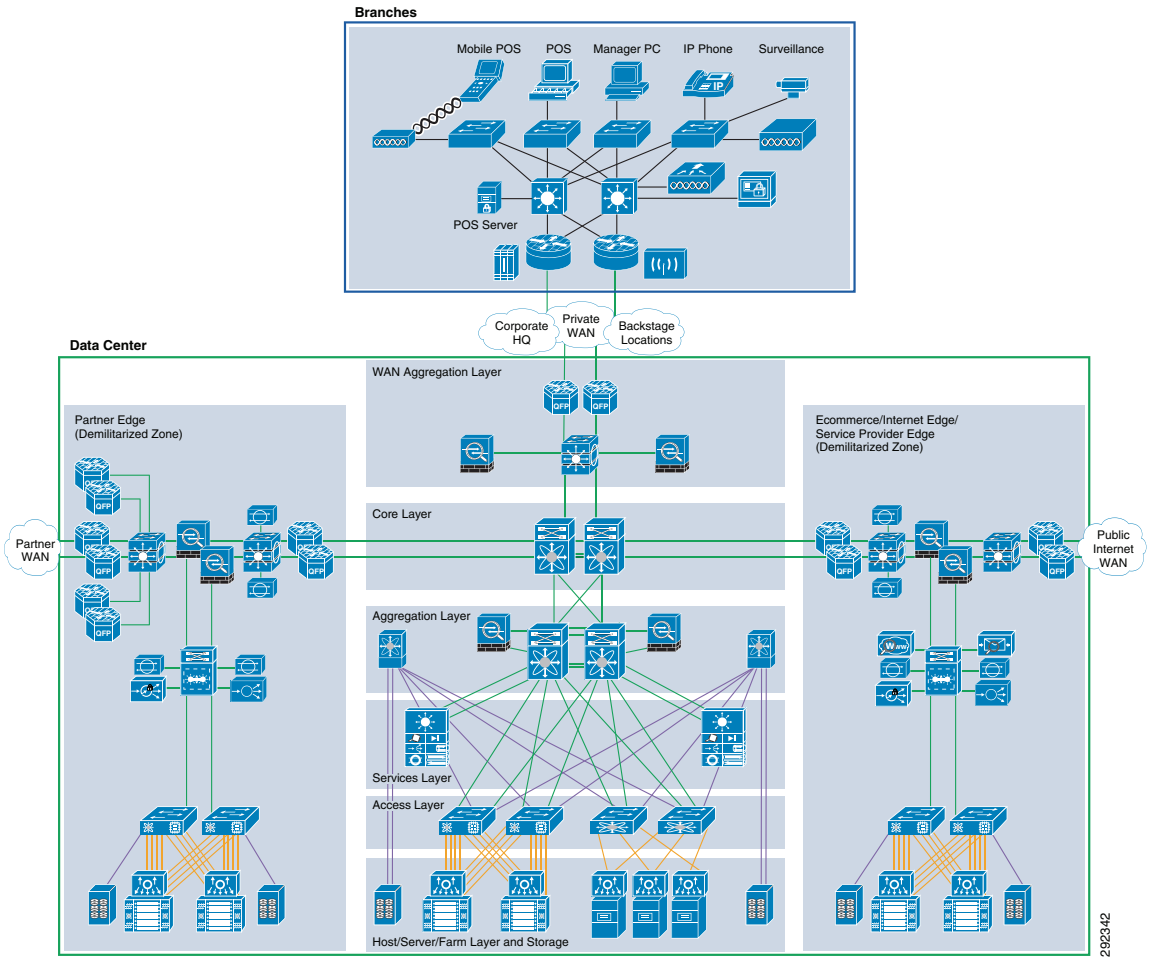
Figure 4-1 Infrastructure Layer of the Solution Framework



The following sections describe the designs that were implemented from the reference architecture.

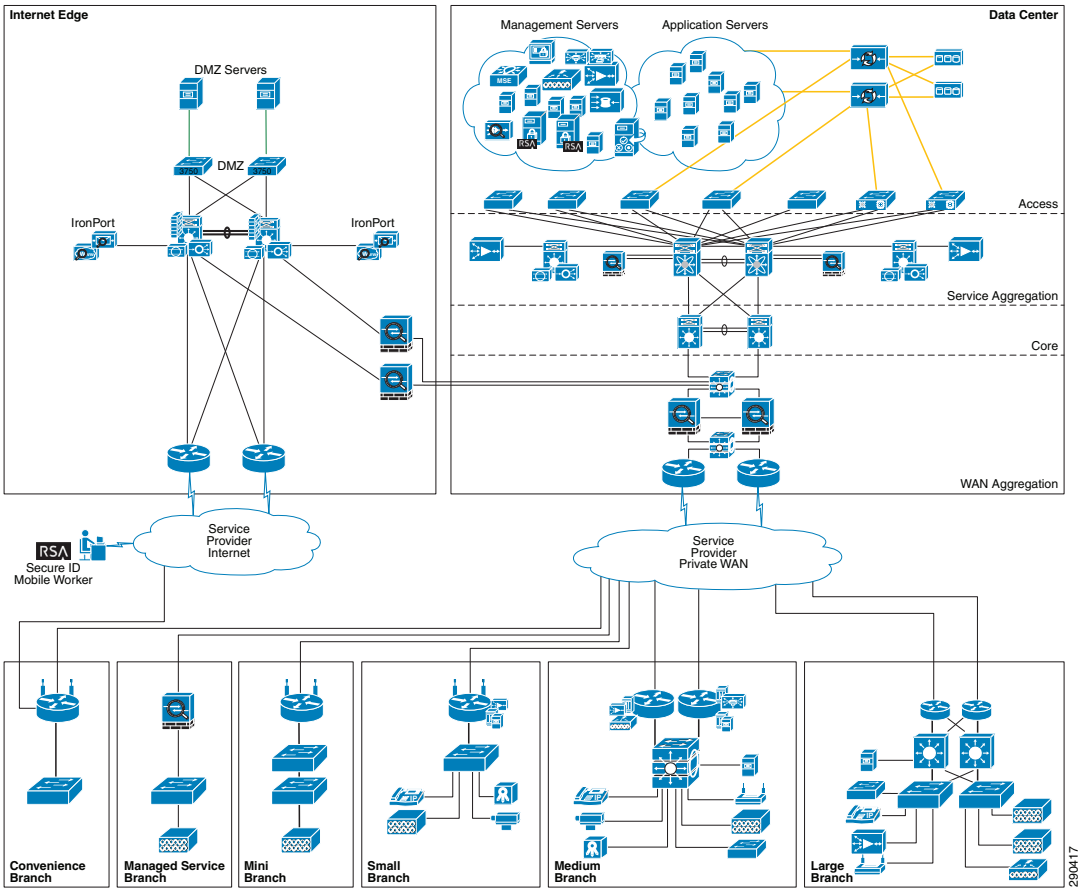
Figure 4-2 shows the enterprise-wide reference architecture.

Figure 4-2 Enterprise-Wide Reference Architecture



Referencing the enterprise-wide architecture shown in Figure 4-2, the design shown in Figure 4-3 was created in the Cisco Lab.

Figure 4-3 Cisco PCI Solution Lab Architecture



Note the following:

- Six branch designs were selected to represent Cisco and partner products.
- The data center consists of a single aggregation block based on the Data Center 3.0 architecture.
- The Internet edge is representative of both the e-commerce and partner edge for the purposes of validation.

The following sections describe this enterprise-wide design in more detail, and demonstrate what was implemented within the lab.

Branches

Multiple branch footprints were implemented that address a variety of business objectives. Each branch footprint section contains designs that were extracted from the reference architecture. Each design contains the following:

- Reference architecture
- Branch design
  - Logical topology
  - Addressing plan
  - Components selected

For component compliance functionality, see Chapter 5, "Component Assessment.". For full device configurations, see Appendix E, "Detailed Full Running Configurations."

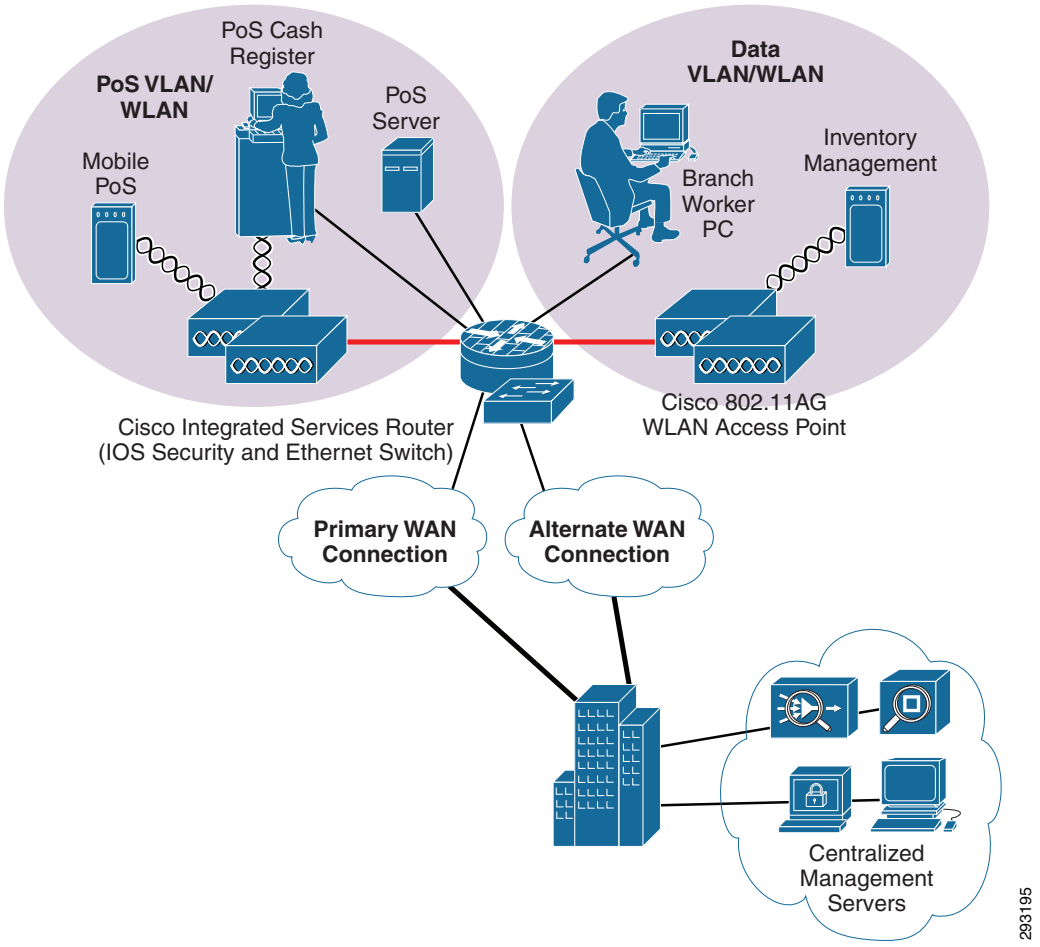
Note Each of these branch designs includes a variety of components that can be interchangeably used between them, depending on business requirements. For validation purposes, it was not necessary to implement all possible components in each design.

Small Branch Architecture

The small branch network scenario, shown in Figure 4-4, meets the following design requirements:

- Branch size averages between 2000–6000 square feet
- Fewer than 25 devices requiring network connectivity
- Single router with firewall/IPS, integrated Ethernet switch, compact switch, and power-over-Ethernet (PoE)
- Preference for integrated services within fewer network components because of physical space requirements
- Wireless connectivity

Figure 4-4 Small Branch Architecture



The small branch reference architecture is a powerful platform for running an enterprise that requires simplicity and a compact form factor. This combination appeals to many formats that can include the following:

- Small branch—Specialty shops, discount businesses
- Mini branches—Fuel stations, mall outlet
- Convenience branches—Pop-up stores, health centers, mall kiosks
- Managed service provider branch—WAN access controlled by service provider

This network architecture is widely used and consolidates many services into fewer infrastructure components. The small branch also supports a variety of business application models because an integrated Ethernet switch supports high-speed LAN services. In addition, an integrated content engine supports centralized application optimization requirements such as Web Cache Communications Protocol (WCCP)-based caching, pre-positioning of data, local media streaming, and other application velocity services.

Advantages include the following:

- Lower cost per branch
- Fewer parts to spare
- Fewer software images to maintain
- Lower equipment maintenance costs

Limitations include the following:

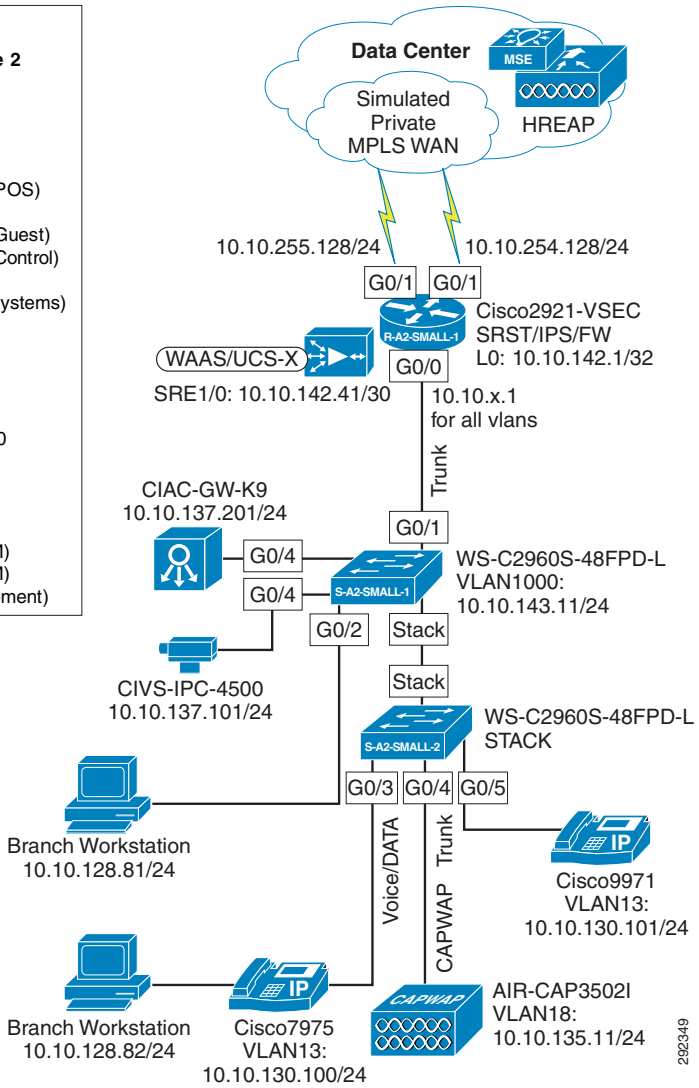
- Decreased levels of network resilience
- Greater potential downtime because of single points of failure

Small Branch—Small Design

Figure 4-5 shows the small branch network design.

Figure 4-5 Small Branch Network Design

Small Branch IP Addressing	
10.10.128.0 255.255.240.0	**Small Branch Aisle 2**
10.10.128.0 /24	VLAN11 (POS)
10.10.129.0 /24	VLAN12 (Data)
10.10.130.0 /24	VLAN13 (Voice)
10.10.131.0 /24	VLAN14 (Wireless)
10.10.132.0 /24	VLAN15 (Wireless POS)
10.10.133.0 /24	VLAN16 (Partner)
10.10.134.0 /24	VLAN17 (Wireless Guest)
10.10.135.0 /24	VLAN18 (Wireless Control)
10.10.136.0 /24	VLAN19 (WAE)
10.10.137.0 /24	VLAN20 (Security Systems)
10.10.138.0 /24	(Future)
10.10.139.0 /24	(Future)
10.10.140.0 /24	(Future)
10.10.141.0 /24	(Future)
10.10.142.0 /24	Other- (Misc)
10.10.142.1 /32	R-A2-Small-1 Loop 0
10.10.142.16 /30	(Future)
10.10.142.20 /30	(Future)
10.10.142.24 /30	(Future)
10.10.142.28 /30	(Future)
10.10.142.32 /29	VLAN 110 (SRE-SM)
10.10.142.40 /30	VLAN 111 (SRE-SM)
10.10.143.0 /24	VLAN1000 (Management)



Components Selected

- Cisco 2921 Integrated Services Router (ISR)
- Cisco Catalyst 2960S 48-port PoE Switch
- Cisco Aironet 3502i Access Points
- Cisco Video Surveillance 4500 Series IP Cameras
- Cisco Physical Access Gateway

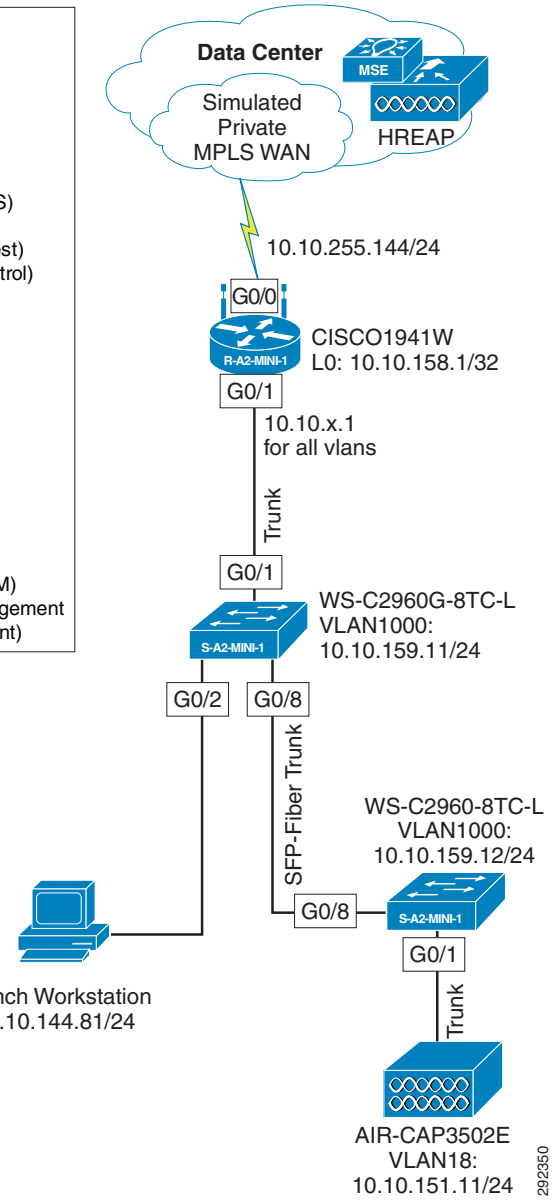
Small Branch—Mini Design

The mini branch represents an alternate design for the small branch architecture, using different components.

Figure 4-6 shows the mini branch network design.

Figure 4-6 Mini Branch Network Design

Mini Branch IP Addressing	
10.10.144.0 255.255.240.0	**Mini Branch Aisle 2**
10.10.144.0 /24	VLAN11 (POS)
10.10.145.0 /24	VLAN12 (Data)
10.10.146.0 /24	VLAN13 (Voice)
10.10.147.0 /24	VLAN14 (Wireless)
10.10.148.0 /24	VLAN15 (Wireless POS)
10.10.149.0 /24	VLAN16 (Partner)
10.10.150.0 /24	VLAN17 (Wireless Guest)
10.10.151.0 /24	VLAN18 (Wireless Control)
10.10.152.0 /24	VLAN19 (WAE)
10.10.153.0 /24	(Future)
10.10.154.0 /24	(Future)
10.10.155.0 /24	(Future)
10.10.156.0 /24	(Future)
10.10.157.0 /24	(Future)
10.10.158.0 /24	Other- (Misc)
10.10.158.1 /32	R-A2-Mini-1 Loop 0
10.10.158.16 /30	(Future)
10.10.158.20 /30	(Future)
10.10.158.24 /30	(Future)
10.10.158.28 /30	(Future)
10.10.158.32 /29	VLAN 110 (Wireless NM)
10.10.158.40 /30	VLAN 111 (WAE Management
10.10.159.0 /24	VLAN1000 (Management)



Components Selected

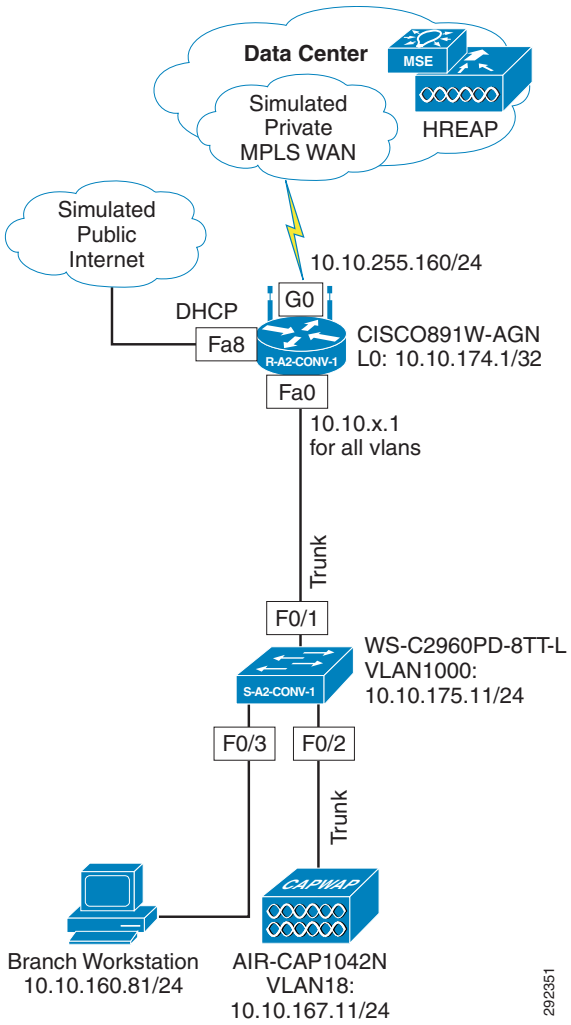
- Cisco 1941 Integrated Services Router (ISR)
- Cisco Catalyst 2960 Switch
- Cisco Aironet 3502e Access Point

Small Branch—Convenience Design

The convenience branch represents an alternate design for the small branch architecture. Figure 4-7 shows the convenience branch network design.

Figure 4-7 Convenience Branch Network Design

Convenience Branch IP Addressing	
10.10.160.0 255.255.240.0	**Convenience Branch Aisle 2**
10.10.160.0 /24	VLAN11 (POS)
10.10.161.0 /24	VLAN12 (Data)
10.10.162.0 /24	VLAN13 (Voice)
10.10.163.0 /24	VLAN14 (Wireless)
10.10.164.0 /24	VLAN15 (Wireless POS)
10.10.165.0 /24	VLAN16 (Partner)
10.10.166.0 /24	VLAN17 (Wireless Guest)
10.10.167.0 /24	VLAN18 (Wireless Control)
10.10.168.0 /24	VLAN19 (WAE)
10.10.169.0 /24	(Future)
10.10.170.0 /24	(Future)
10.10.171.0 /24	(Future)
10.10.172.0 /24	(Future)
10.10.173.0 /24	(Future)
10.10.174.0 /24	Other- (Misc)
10.10.174.1 /32	R-A2-Conv-1 Loop 0
10.10.174.16 /30	(Future)
10.10.174.20 /30	(Future)
10.10.174.24 /30	(Future)
10.10.174.28 /30	(Future)
10.10.174.32 /29	(Future)
10.10.174.40 /30	(Future)
10.10.175.0 /24	VLAN1000 (Management)



Components Selected

- Cisco 891 Series Integrated Services Router (ISR)
- Cisco Catalyst 2960 Series Switch
- Cisco Aironet 1042N Access Point

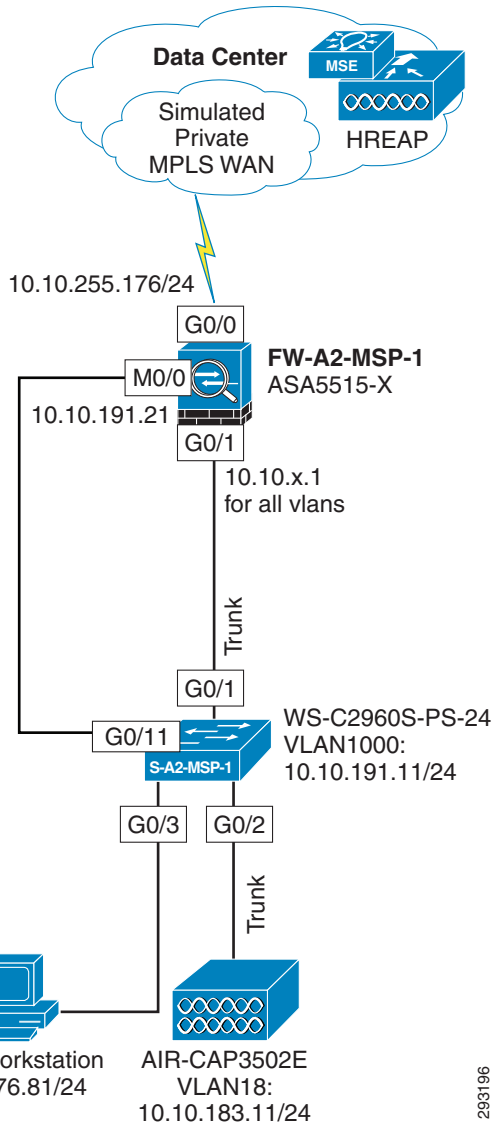
Small Branch—Managed Service Provider Design

The managed service provider branch represents an alternate design for the small branch architecture. Figure 4-8 shows the managed service provider network design.

Figure 4-8 Managed Service Provider Branch Network Design

Managed Service Provider Branch IP Addressing

10.10.176.0 255.255.240.0	MSP Branch Aisle 2
10.10.176.0 /24	VLAN11 (POS)
10.10.177.0 /24	VLAN12 (Data)
10.10.178.0 /24	VLAN13 (Voice)
10.10.179.0 /24	VLAN14 (Wireless)
10.10.180.0 /24	VLAN15 (Wireless POS)
10.10.181.0 /24	VLAN16 (Partner)
10.10.182.0 /24	VLAN17 (Wireless Guest)
10.10.183.0 /24	VLAN18 (Wireless Control)
10.10.184.0 /24	VLAN19 (WAE)
10.10.185.0 /24	(Future)
10.10.186.0 /24	(Future)
10.10.187.0 /24	(Future)
10.10.188.0 /24	(Future)
10.10.189.0 /24	(Future)
10.10.190.0 /24	Other- (Misc)
10.10.190.1 /32	R-A2-MSP-1 Loop 0
10.10.190.16 /30	SP to FW link
10.10.190.20 /30	(Future)
10.10.190.24 /30	(Future)
10.10.190.28 /30	(Future)
10.10.190.32 /29	(Future)
10.10.190.40 /30	(Future)
10.10.191.0 /24	VLAN1000 (Management)



Components Selected

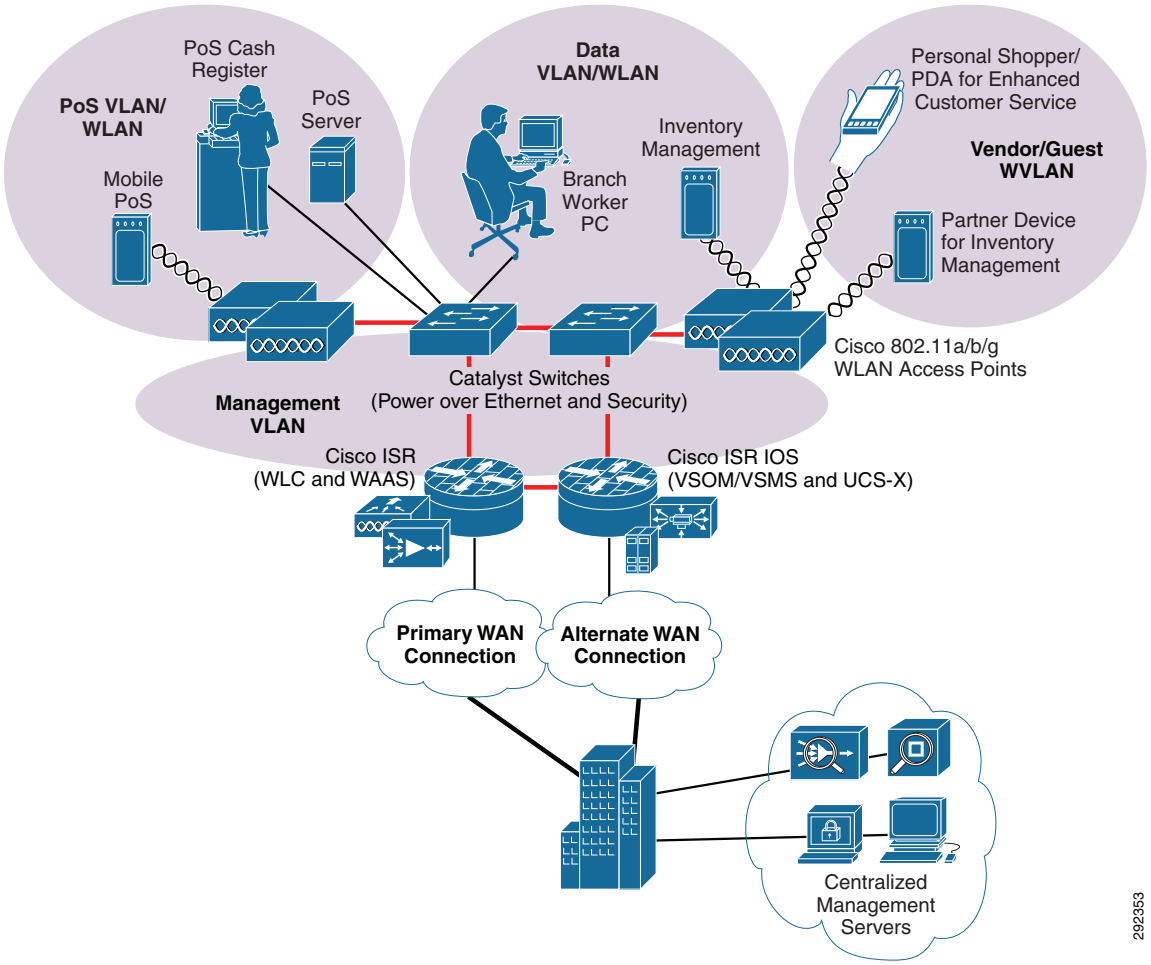
- Cisco ASA 5510 Firewall with SSM-10
- Cisco Catalyst 3560E Switch
- Cisco Aironet 3502e Access Points

Medium Branch Architecture

The medium branch network scenario, shown in Figure 4-9, meets the following design requirements:

- Branch size averages between 6,000–18,000 square feet
- The physical size of the branch is smaller than a large branch, so a distribution layer of network switches is not required
- Number of devices connecting to the network averages 25–100 devices
- Redundant LAN and WAN infrastructures with firewall/IPS
- Wireless connectivity

Figure 4-9 Medium Branch Architecture



The medium branch reference architecture is designed for enterprise businesses that require network resilience and increased levels of application availability over the small branch architecture and its single-threaded, simple approach. As more mission-critical applications and services converge onto the IP infrastructure, network uptime and application availability are more important. The dual-router and dual-LAN switch design of the medium branch supports these requirements. Each of the Cisco ISR routers can run Cisco IOS Software security services and other branch communication services

simultaneously. Each of the Cisco ISR routers is connected to a dedicated WAN connection. Hot Standby Routing Protocol (HSRP) is used to ensure network resilience in the event that the network connection fails.

The access layer of the network offers enhanced levels of flexibility and more access ports compared to the small branch. Up to 12 wireless access points can be installed in the branch, supported by the Cisco Wireless Control System (WCS) controller as tested and without adding more controllers. The distributed Cisco Catalyst switches can support a combination of larger physical buildings or a larger number of endpoints than the small branch.

Advantages include the following:

- More adaptive access layer with support for a greater number of endpoints and more diverse building requirements (multiple floors, sub-areas, and so on)
- Improved network resilience through parallel device design
- Improved network and application availability through parallel paths

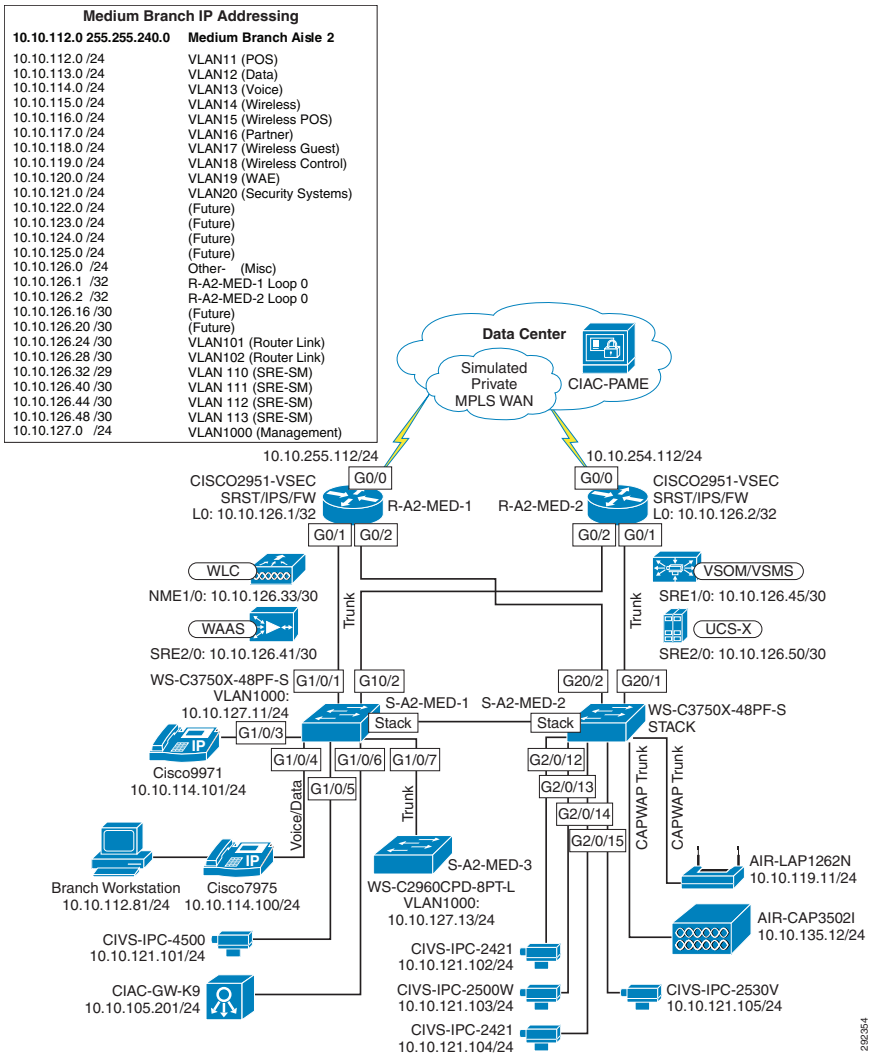
Limitations include the following:

- No distribution layer between core layer (the ISR) and the access layer switches
- Single WCS Controller decreases in-branch resilience of the wireless network; the recommendation is to have branch APs fallback to the central WCS controller if the local WCS controller fails, or to install dual-local WCS controllers.

Medium Branch—Design

Figure 4-10 shows the medium branch network design.

Figure 4-10 Medium Branch Network Design



Components Selected

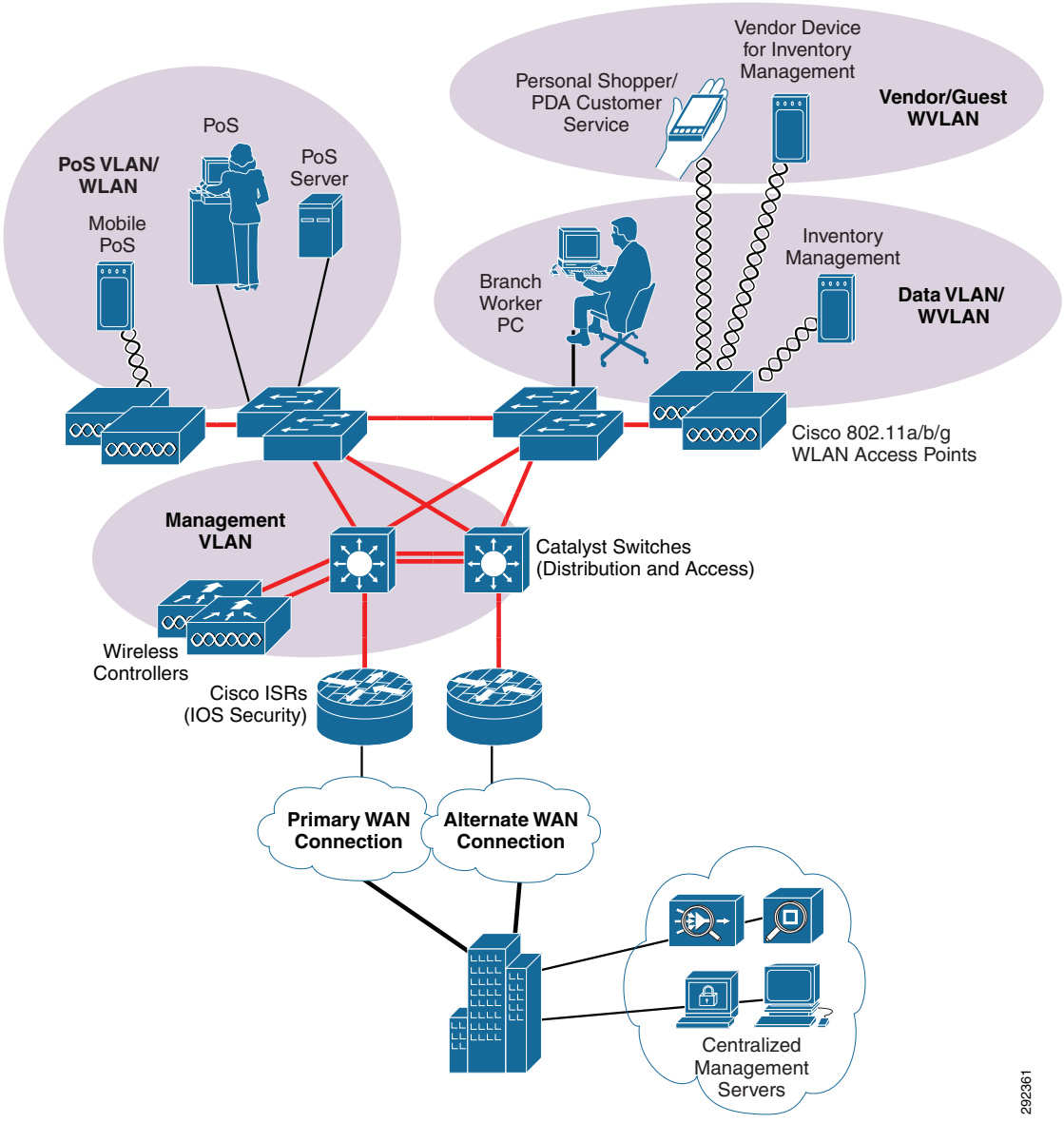
- Cisco 2951 Integrated Services Router (ISR)
- Cisco Catalyst 3750X 48-port PoE Switch
- Cisco Catalyst 2960 Compact Switch
- Cisco Aironet 3502e and 1262N Access Points
- Cisco Video Surveillance 2421 IP Dome Camera
- Cisco Video Surveillance 2500 Series IP Camera
- Cisco Operations Manager v4.1
- Cisco Physical Access Gateway

Large Branch Architecture

The large branch network scenario, shown in Figure 4-11, meets the following design requirements:

- Branch size averages between 15,000–150,000 square feet
- More than 100 devices per branch requiring network connectivity
- Multiple routers with firewall/IPS for primary and backup network requirements
- Preference for a combination of network services distributed within the branch to meet resilience and application availability requirements
- Tiered network architecture within the branch; distribution layer switches are employed between the central network services core and the access layer connecting to the network endpoints (POS, wireless APs, servers)

Figure 4-11 Large Branch Architecture



The large branch reference architecture takes some of the elements of Cisco campus network architecture recommendations and adapts them to a large branch environment. Network traffic can be better segmented (logically and physically) to meet business requirements. The distribution layer of the large branch architecture can greatly improve LAN performance while offering enhanced physical media connections (that is, fiber and copper for connection to remote access layer switches and wireless access points). A larger number of endpoints can be added to the network to meet business requirements. This type of architecture is widely used by large format organizations globally. Dual routers and distribution layer media flexibility greatly improve network serviceability because the network is highly available and scales to support the large branch requirements. Routine maintenance and upgrades can be scheduled and performed more frequently or during normal business hours because of parallel path design.

Advantages include the following:

- Highest network resilience based on highly available design
- Port density and fiber density for large locations
- Increase segmentation of traffic
- Scalable to accommodate shifting requirements in large branches

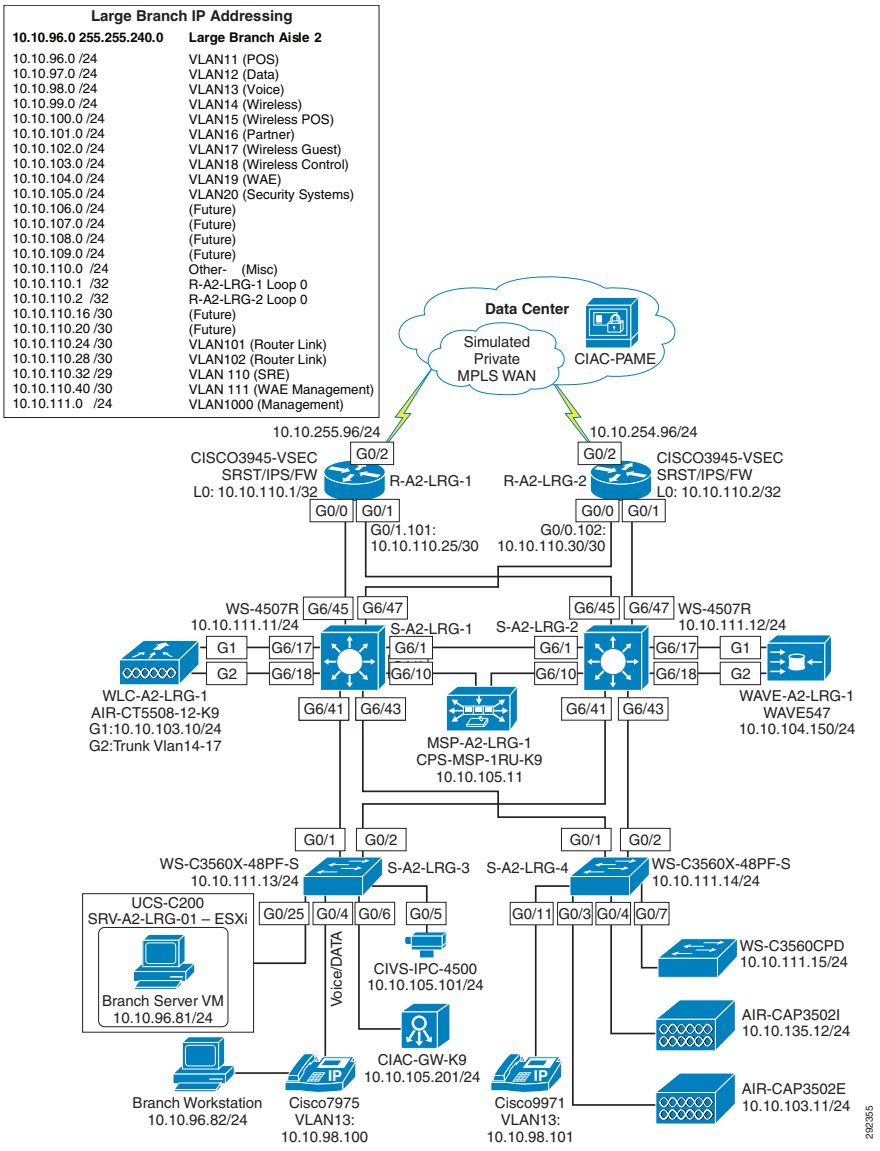
Limitations include the following:

- Higher cost because of network resilience based on highly available design
- These branch network designs are capable of helping an organization achieve PCI compliance, and also serve as the scalable platform for new services and applications

Large Branch Design

Figure 4-12 shows the large branch network design.

Figure 4-12 Large Branch Network Design



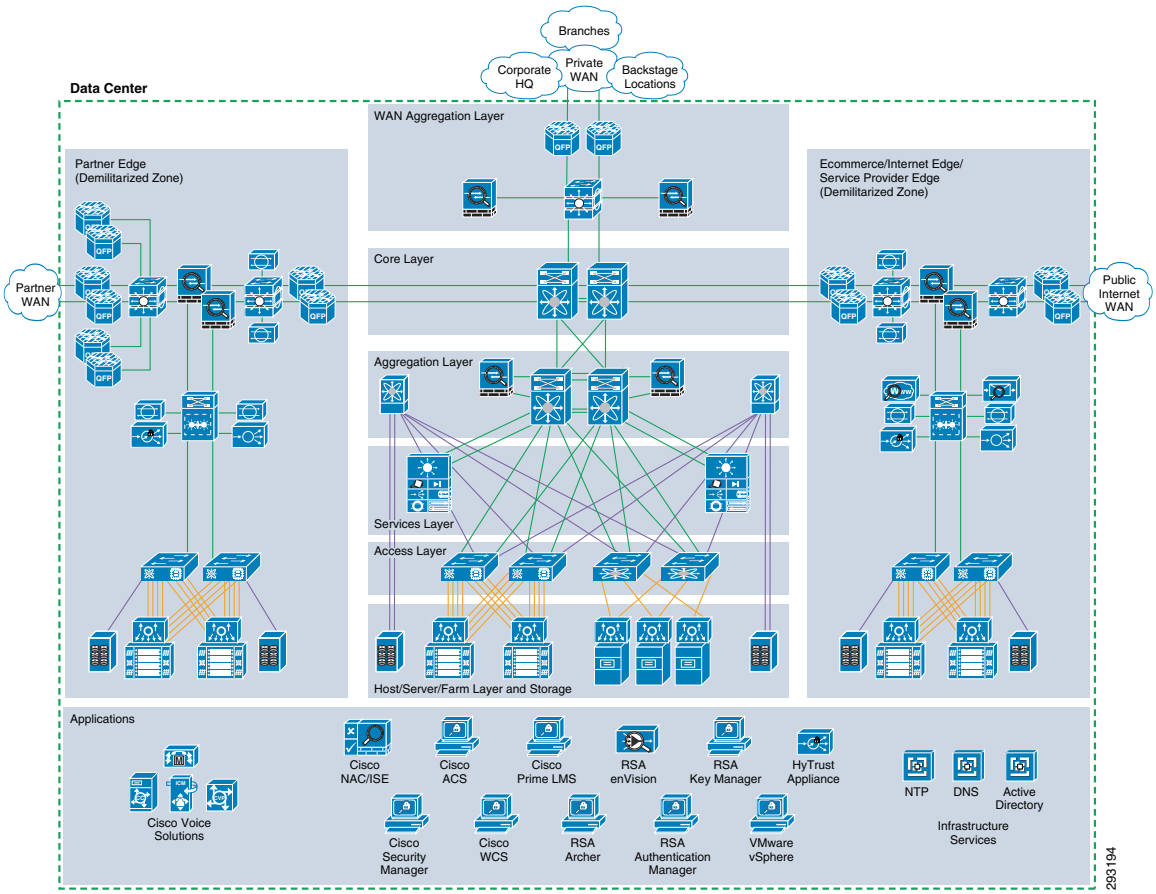
Components Selected

- Cisco 3945 Integrated Services Router (ISR)
- Cisco Catalyst 3560X and 4500 switches
- Cisco Aironet 3502e and 3502i Access Points
- Cisco 5508 Wireless Controller
- Cisco 4500 Video Surveillance Camera
- Cisco Physical Access Gateway

Data Center

The data center is where centralized data processing, data storage, and data communications take place (see Figure 4-13). The data center is also the place where management systems are deployed. The data center provides centralized control from an administrative perspective because it is typically where the tools that are used to monitor and enforce compliance are deployed.

Figure 4-13 Data Center Architecture



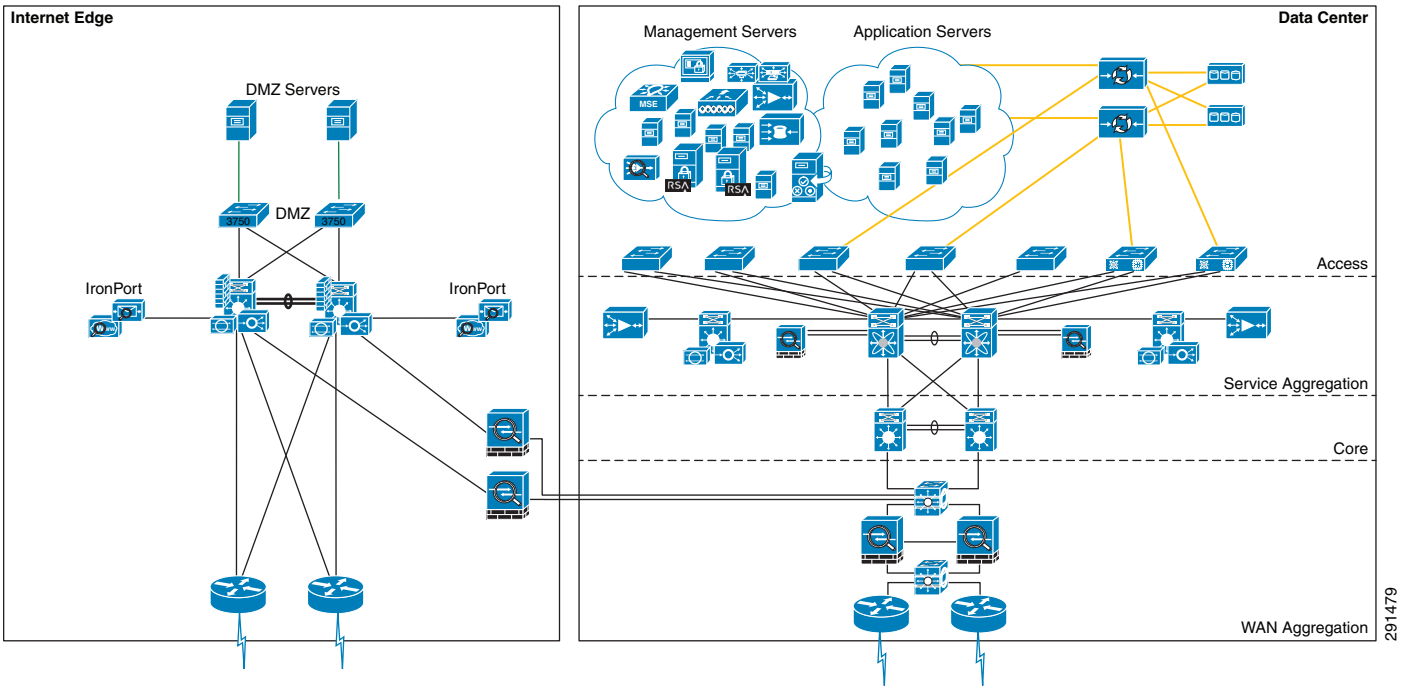
Design considerations are as follows:

- Centralized solution management supports all aspects of network, security, and systems management; and supports remote access from anywhere on the network.
- Standardized equipment and software images, deployed in a modular, layered approach, simplify configuration management and increase the systems availability.
- The highly available data center design permits highly resilient access from branches to core data and storage services.
- WAN aggregation alternatives allow flexible selection of service provider network offerings.
- The service aggregation design allows for a modular approach to adding new access layers and managing shared network services (for example, firewall, IPS, application networking, wireless management)

- Firewall, IPS, and application networking services are available at the service and aggregation layers of the data center.
- Scalability to accommodate shifting requirements in data center compute and storage requirements.
- WAN access speeds are typically the limiting factor between the branch network systems and the WAN aggregation layer.
- It is typical for organizations to over-subscribe the WAN circuits between the branches and the WAN edge aggregation router. Over-subscription can cause inconsistent results and packet loss of payment card information in the event that more traffic enters the WAN circuit simultaneously.
- Backup network connections from branch networks to the data center are recommended when payment card information is transported via the WAN.

Figure 4-14 shows the data center design.

Figure 4-14 Data Center Design



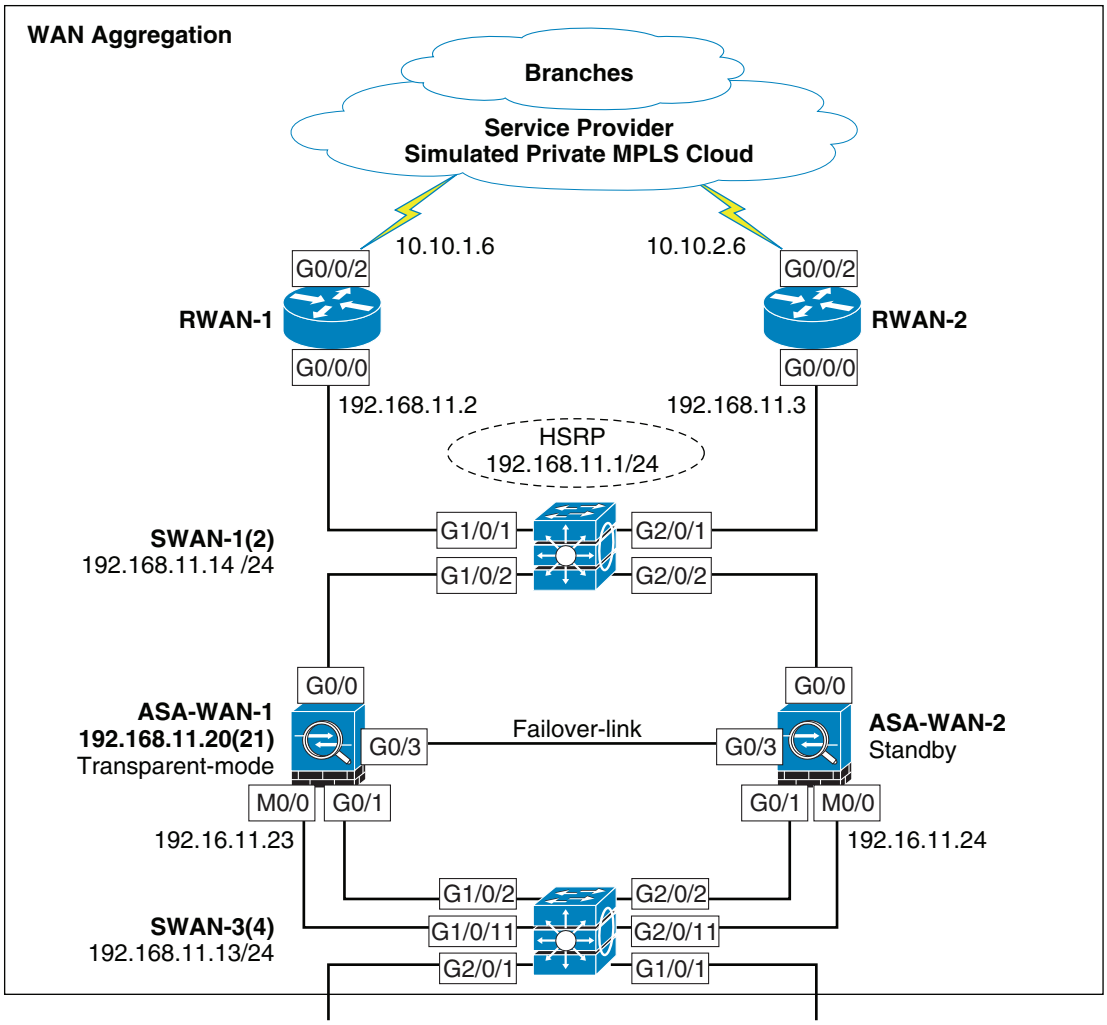
Data centers can house many types of functions and the term itself can encompass narrow and broad aspects. For the purposes of this guide, data centers include the following functions:

- WAN aggregation layer—Aggregates the branch and backstage WAN connections to the core
- Core layer—Highly available, high-speed area that is the central point of connectivity to all data center areas
- Aggregation block—Aggregates the services of one area and connects that area to the core, including Vblock1 design
- Internet edge—Secure connectivity to the Internet

WAN Aggregation Layer Design

Figure 4-15 shows the WAN aggregation layer design.

Figure 4-15 WAN Aggregation Layer Design



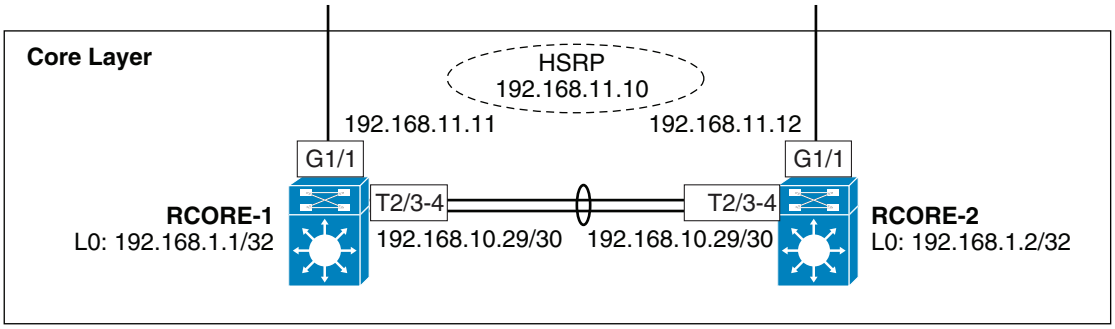
Components Selected

- Cisco ASR 1002-Fixed Router
- Cisco ASA 5540 Adaptive Security Appliance
- Cisco Catalyst 3750X Switch

Core Layer Design

Figure 4-16 shows the core layer design.

Figure 4-16 Core Layer Design



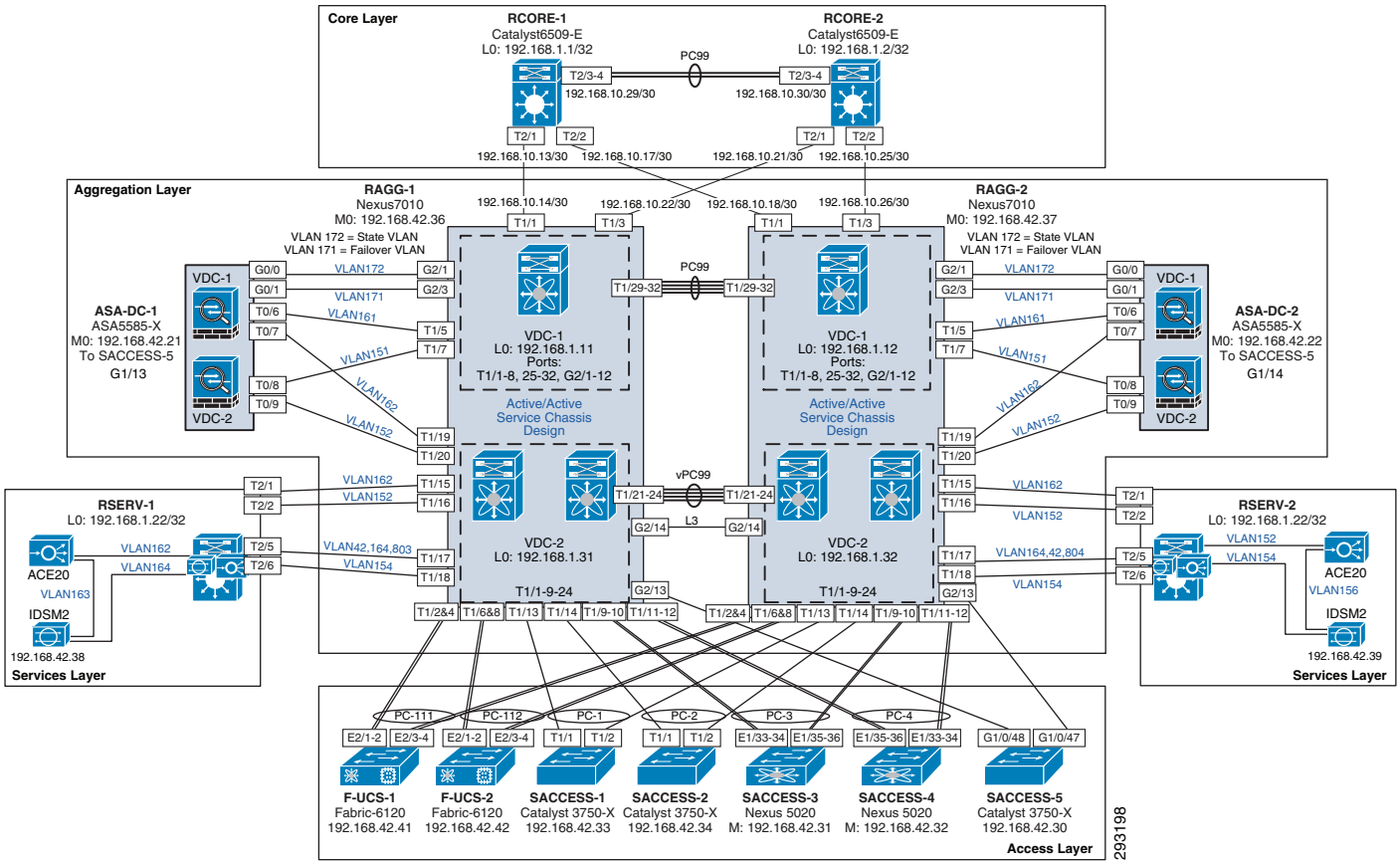
Components Selected

- Cisco Catalyst 6500-E Switch

Aggregation Block Design

Figure 4-17 shows the aggregation block design.

Figure 4-17 Aggregation Block Design



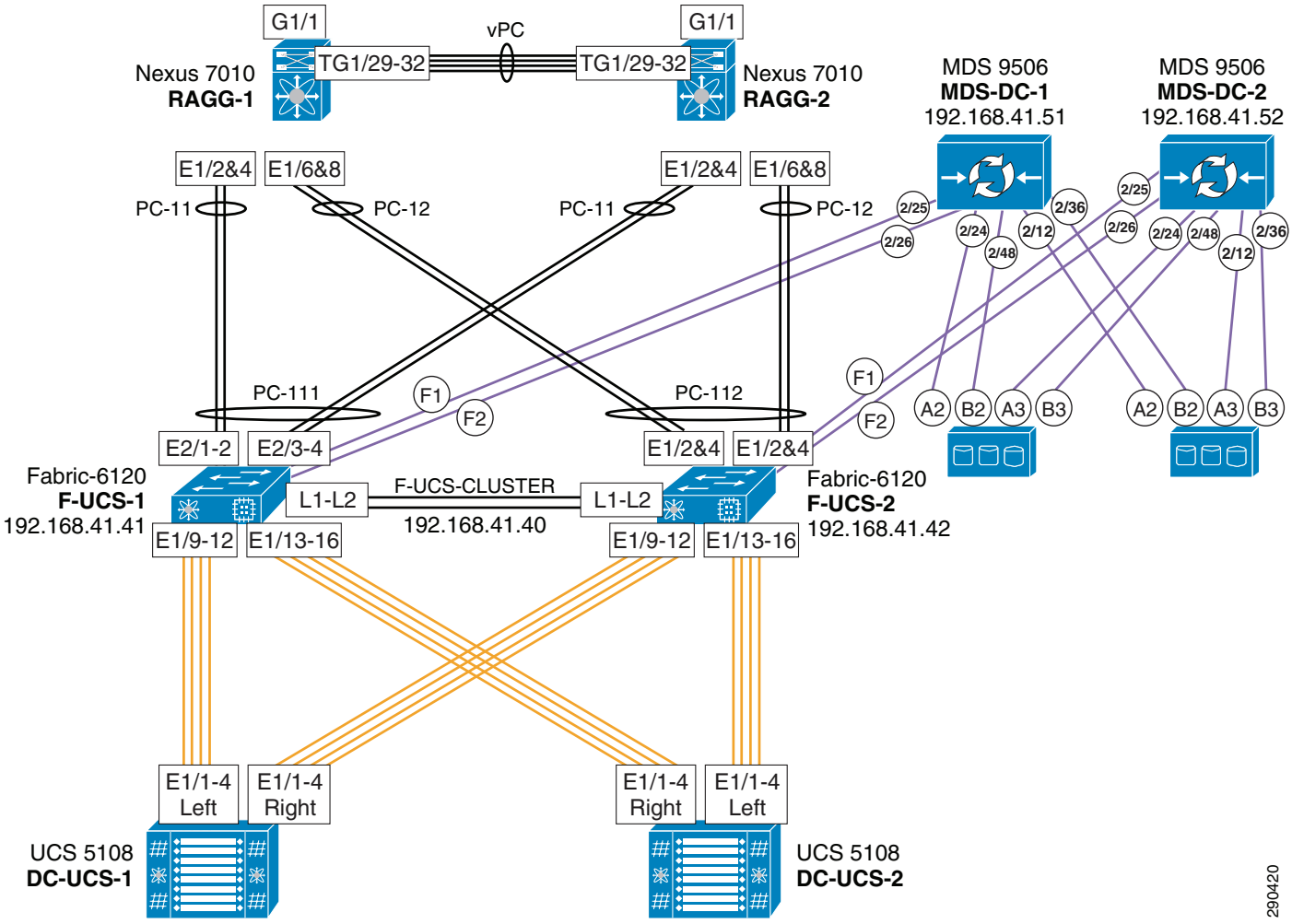
Components Selected

- Cisco ASA 5585-X Adaptive Security Appliance
- Cisco Nexus 7010 Switch
- Cisco Catalyst 6500-E Switch
  - Cisco ACE 20
  - Cisco IDSM-2
- Cisco Nexus 5020 Switch
- Cisco Catalyst 4948 Switch

Vblock Design

Figure 4-18 shows the Vblock design.

Figure 4-18 Vblock Design



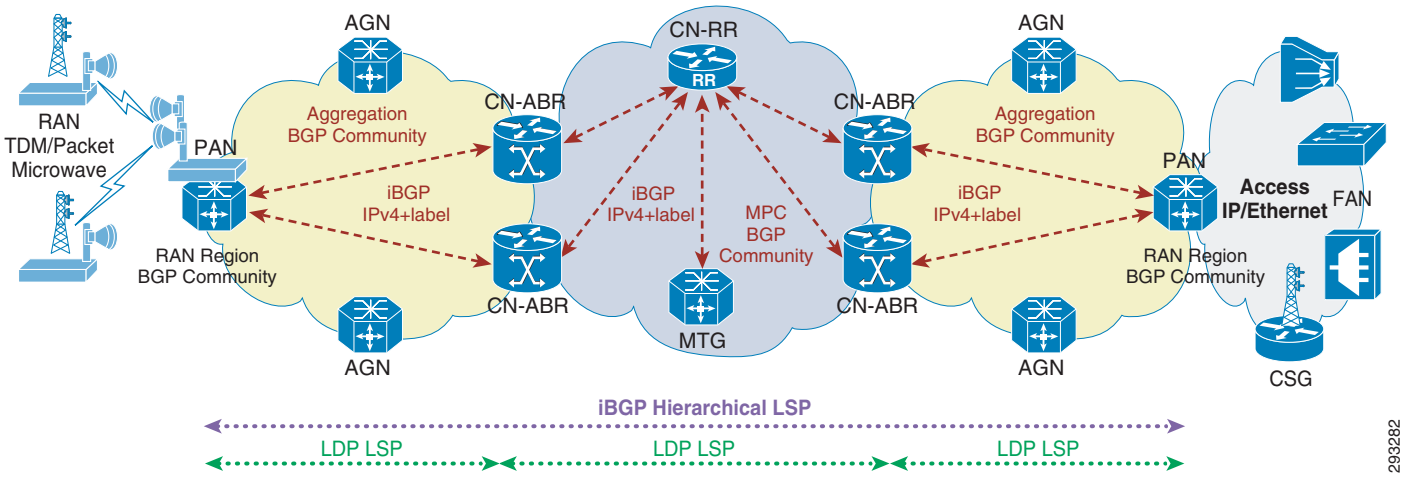
Components Selected

- Cisco UCS 5108 Blade Server Chassis
  - Cisco UCS B200 Blade Server
- Cisco UCS 6120 Fabric Interconnect
- Cisco MDS 9506 Multilayer Director
- EMC CLARiion CX4 Model 240

Internet Edge Design

Figure 4-19 shows the Internet edge network design.

Figure 4-19 Internet Edge Network Design



Components Selected

- Cisco 7200 Series Router
- Cisco Catalyst 6500-E Switch
  - Cisco ACE 20
  - Cisco IDSM-2
- Cisco Catalyst 3750X Switch
- Cisco MDS 9204i Switch
- Cisco IronPort C670

Addressing and Routing Disclosure

PCI requirement 1.3.8 states that merchants must not disclose private addressing and routing information. An enterprise contains two segments:

- Public—Where Internet services are hosted
- Private—Where internal systems reside that are not directly accessible from outside the company

Both may be deployed internally within an enterprise data center or other PIN. The private information must be protected and not propagated out to untrusted parties.

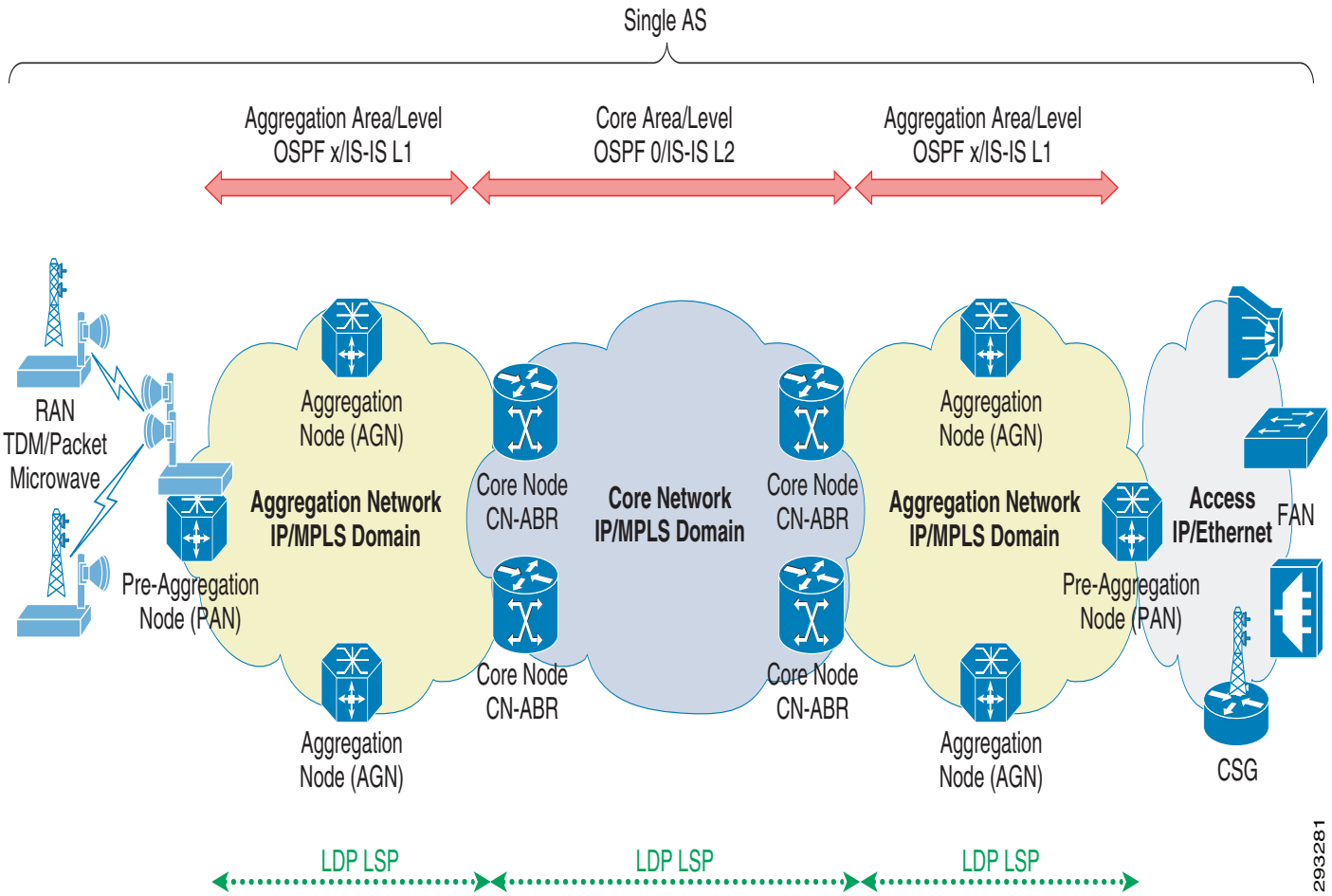
In 2013, it is common for enterprises to deploy an IPv6 Internet presence by using the Server Load Balancing (SLB) to do protocol family translation; that is, when the SLB receives an IPv6 inbound connection from the Internet, the SLB translates this connection on the fly into an IPv4 connection to the real servers.

In this solution, PCI 1.3.8 was met because all the security pieces for IPv4 are also used for IPv6 connections. Moreover, the servers where the information resides have no IPv6 addresses and cannot be reached over IPv6. The attack surface of the servers is strictly the IPv4 attack surface.

Note For more information on the Cisco ACE Application Control Engine Module, see the following URL: http://www.cisco.com/en/US/products/ps6906/index.html.

A best practice when implementing IPv6 is a phased approach. Figure 4-20 illustrates the scenario described above as the first phase of an IPv6 deployment.

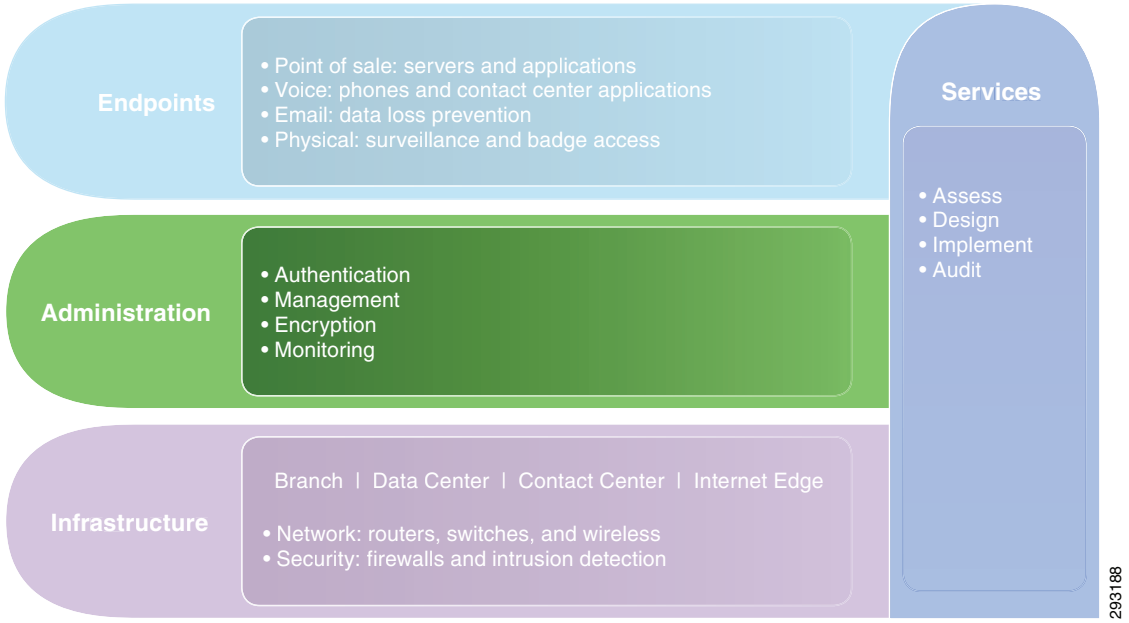
Figure 4-20 IPv6 Phased Approach



Administration

The administration layer of the solution framework addresses the components such as authentication, encryption, management, and monitoring, as shown in Figure 4-21.

Figure 4-21 Administration Layer of the Solution Framework



Authentication

Components Selected

- Cisco Secure Access Control Server (ACS)
- Cisco Identity Services Engine (ISE)
- RSA Authentication Manager
- Windows Active Directory

Encryption

Components Selected

- Cisco Security Manager
- Cisco Key Manager
- RSA Data Protection Manager

Management

Components Selected

- Cisco Prime LAN Management Solution (LMS)

- Cisco Security Manager
- Cisco Wireless Control Server Manager
- EMC Unified Infrastructure Manager
- VMware vSphere vCenter
- Cisco Video Surveillance Manager
- Cisco Physical Access Manager
- RSA Archer

Monitoring

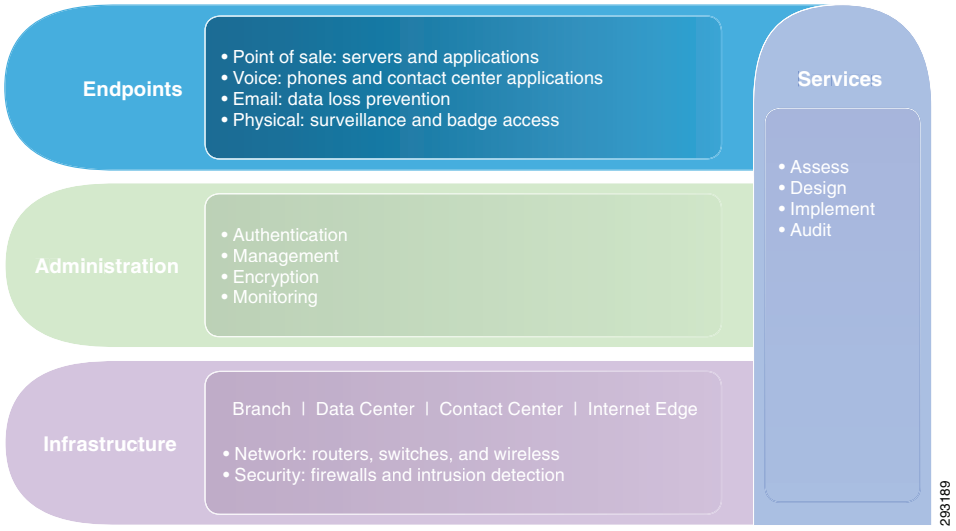
Components Selected

- RSA enVision
- HyTrust

Endpoints

The endpoints layer of the solution framework addresses the components such as voice, e-mail, and physical security, as shown in Figure 4-22.

Figure 4-22 Endpoints Layer of the PCI Solution Framework



Voice

Components Selected

- Cisco Unified Communications Manager

- Cisco IP Phones (9971, 7975)
- Cisco Survivable Remote Site Telephony (SRST)

E-mail

Components Selected

- Cisco IronPort Email Security Appliance with Data Loss Prevention
- Microsoft Exchange Server 2008

Physical

Components Selected

- Cisco Physical Access Gateway
- Cisco Video Surveillance Cameras (2421, 2500, 4500)

Note For a complete Bill of Materials, see Appendix A, "Bill Of Material." For assessment of components selected for PCI compliance, see Chapter 5, "Component Assessment." For complete running configurations of components, see Appendix E, "Detailed Full Running Configurations."

PCI Solution Result Summary

Cisco Compliance Solution Components

This solution combines components to create an end-to-end solution conforming to the requirements of the PCI 2.0 guidelines. The result is a set of branch, data center, and Internet edge architectures and designs that simplify the process of achieving and maintaining compliance.

Endpoints	Primary PCI Function
Cisco IronPort Email Security	DLP
Cisco Physical Access Control	9.1
Cisco UCS and UCS Express	Servers
Cisco Unified CM and IP Phones	9.1.2
Cisco Video Surveillance	9.1.1

Administration	Primary PCI Function
Cisco ACS	7.1
Cisco Identity Services Engine	7.1, 11.1b, 11.1d
Cisco Prime LMS	1.2.2
Cisco Security Manager	1.2
Hytrust Appliance	10.5
RSA Authentication Manager	8.3
RSA Data Protection Manager	3.5
RSA enVision	10.5

Infrastructure	Primary PCI Function
Cisco ASA-Branch	1.3, 11.4
Cisco ASA-Data Center	1.3, 11.4
Cisco Branch Routers	1.3, 11.4
Cisco Branch Switches	Segmentation
Cisco Data Center Routers	1.2, 1.3
Cisco Data Center Switches	Segmentation
Cisco Data Center IDSM	11.4
Cisco MDS Switches	3.4
Cisco Nexus 1000V Series Switch	Segmentation
Cisco Nexus Data Center Switches	Segmentation
Cisco Nexus VSG	Virtual Firewall
Cisco Wireless	4.1, 11.1
EMC CLARiioN SAN	Storage