Enterprise Branch Architecture Design Overview

This design guide provides an overview of the Enterprise Branch Architecture, which is one component in the overall Cisco Service-Oriented Network Architecture (SONA). SONA is a comprehensive framework to provide guidelines to accelerate applications, business processes, and profitability. Based on the Cisco SONA framework, the Enterprise Branch Architecture incorporates networked infrastructure services, integrated services, and application networking services across typical branch networks. This design guide provides an overview of the entire Enterprise Branch Architecture as it applies to the SONA framework. This Enterprise Branch Architecture framework is evolving. Cisco has adopted a phased approach to help meet customer needs accordingly. Individual proven design guides provide more detailed design and implementation descriptions for each of the major services.

Cisco Enterprise Systems Engineering (ESE) is dedicated to producing high-quality tested design guides that are intended to help deploy the system of solutions more confidently and safely. This design overview is part of an ongoing series that addresses enterprise branch solutions using the latest advanced services technologies from Cisco and based on best practice design principles that have been tested in an Enterprise Systems environment.

Contents

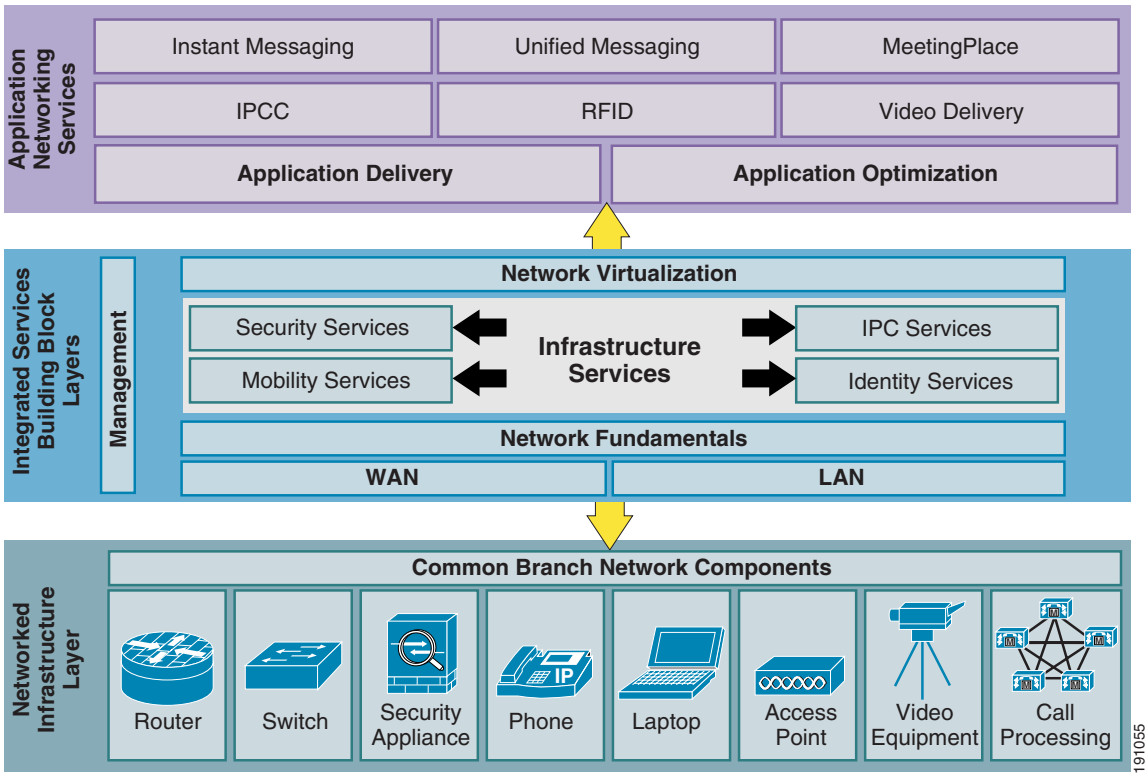
Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

This document provides an overview of the Enterprise Branch Architecture as a part of the Cisco SONA framework. This document describes the overall strategy of the Enterprise Branch Architecture framework. This framework is based on a phased approach that will result in a series of documents to support the evolution of Enterprise Branch network designs with various integrated services.

Figure 1 shows the Enterprise Branch Architecture framework.

Figure 1 Enterprise Branch Architecture Framework



This architecture framework comprises three layers, each with their own components. The foundation of the framework is the networked infrastructure layer, which comprises all the common physical network elements residing in a branch. All other layers in this architecture framework are built upon these components. Next is the integrated services building block layer. This layer organizes the key services that are embedded within the fabric of the network infrastructure at the branch, regardless of which branch components are used. These services include the following:

- WAN services
- LAN services
- Network fundamentals
- Security services
- Identity services
- Mobility services
- Cisco IP Communications (IPC) services
- Network virtualization

These services are described in more detail in this document. The top layer in this architecture framework is the application networking services layer. Business applications used to facilitate collaboration and communication such as video, messaging, and Cisco Unified Contact Center Enterprise are increasingly becoming a requirement at a branch.

These applications leverage the efficiencies gained from the interactive services found in the integrated services layer. Application-oriented networking allows for centralized management and consistent enforcement of policies across a distributed network. By deeply integrating with the network fabric, solutions do not require additional client installation or provisioning while maintaining application visibility and security. This results in reduced latency and simplified policy management.

Each layer in the Enterprise Branch Architecture builds upon itself to provide a complete solution for branches. The design overview is the overall strategy of an ongoing series of design chapters that will create a comprehensive solution for enterprise branch networks.

Target Audience

This design guide is targeted at Cisco systems engineers and customer support engineers to provide guidelines and best practices for customer deployments.

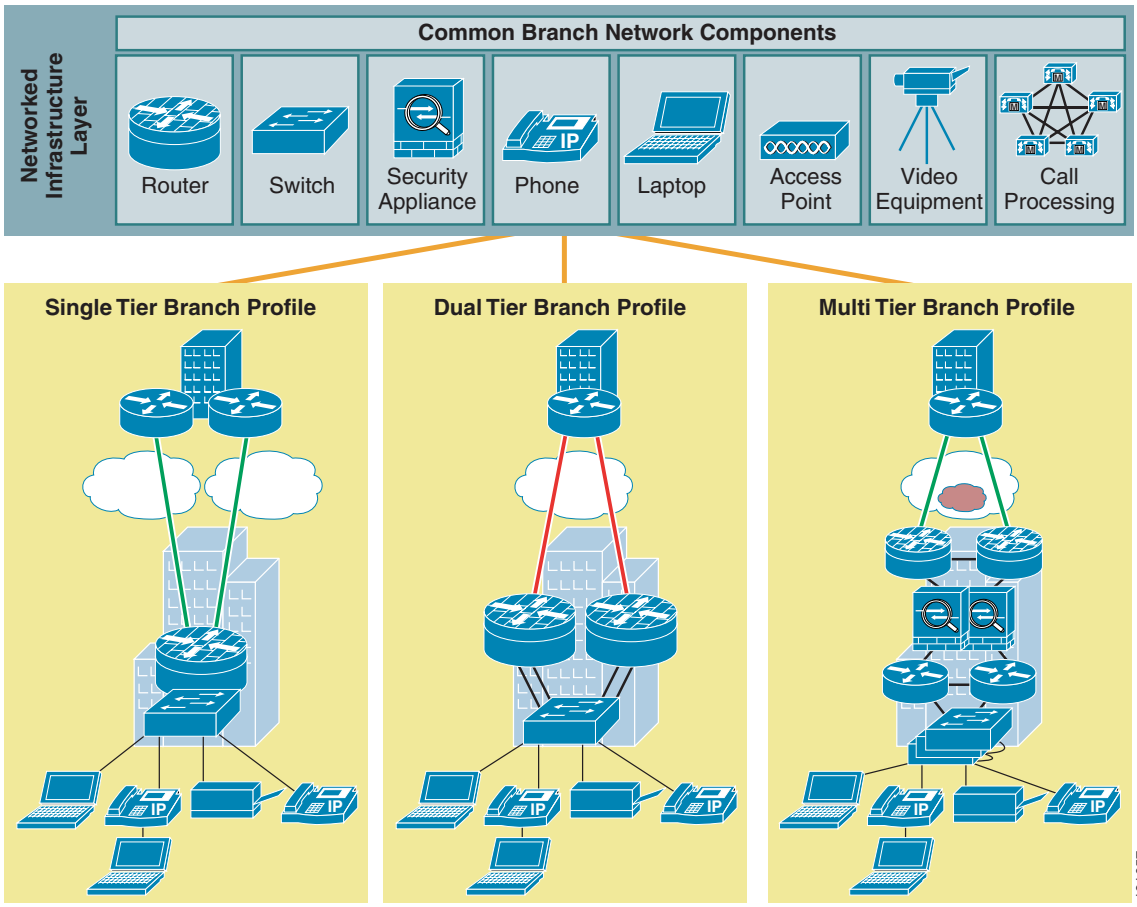
Networked Infrastructure Layer

The networked infrastructure layer is the bottom layer of the Enterprise Branch Architecture framework. This layer provides the foundation upon which all services and applications are applied. The networked infrastructure layer comprises common branch network elements to which all branch architectures can be based. The Enterprise Branch Architecture has defined three profiles to showcase branch architectures. These three profiles will be used to build out all of the layers in the entire framework. The three profiles tested are as follows:

- Single-tier branch profile
- Dual-tier branch profile
- Multi-tier branch profile

These three profiles are shown in Figure 2.

Figure 2 Networked Infrastructure Layer—Three Profiles



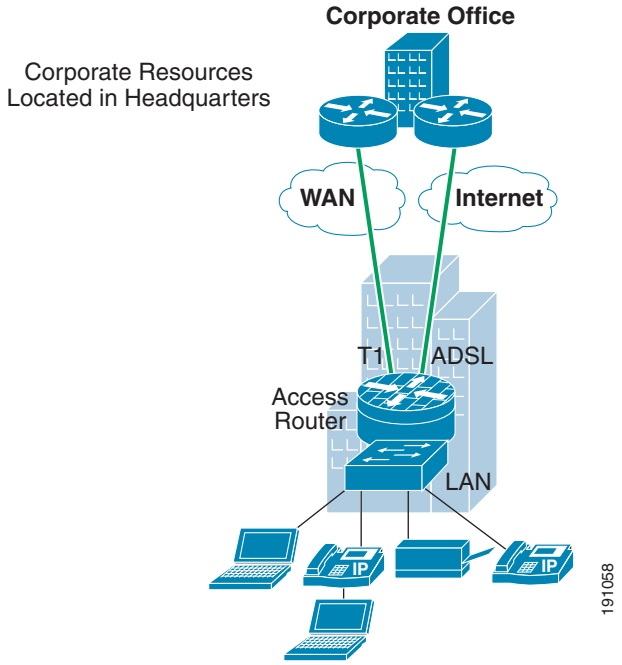
Common Branch Network Components

There is not a single or typical branch network across the entire enterprise customer space. Depending on size, marketing vertical, location, or cost, each branch has its own network design. Regardless of network architecture, there are a set of common branch networking elements. Branch networks require routers, switches, and, optionally, security appliances to provide network connectivity. Users at each branch contain a combination of phones, laptops, and video equipment to run various applications. Access points and call processing equipment might be required in branches that require mobility and centralized voice in their network. The Enterprise Branch Architecture introduces the concept of three branch profiles that incorporate the common branch network components. These three profiles are not intended to be the *only* architectures recommended for branch networks, but rather a representation of various aspects that branch network need to include. These profiles are used as the baseline foundation with which all the integrated services building blocks and application networking services are built. The design guides documented in the Enterprise Branch Architecture suite are written as such to provide guidelines and modularity between each profile.

Single-Tier Branch Profile Overview

Figure 3 shows the single-tier branch profile.

Figure 3 Single-Tier Branch Profile

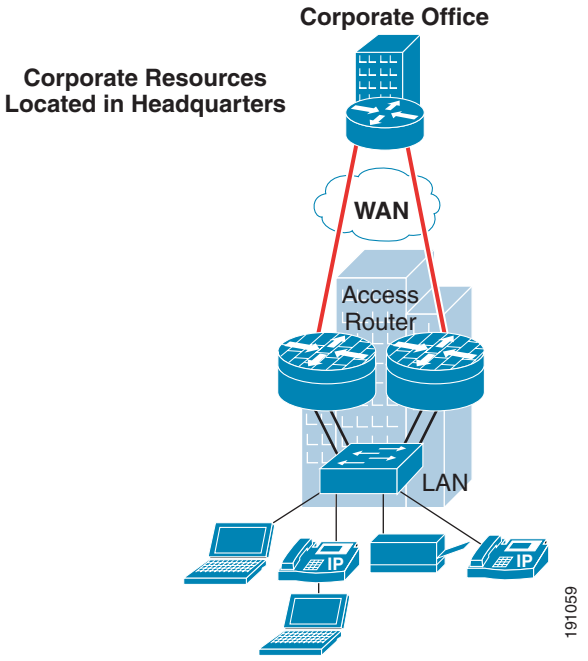


This profile is recommended for smaller enterprise branches that do not require platform redundancy and a large user base. This profile consists of an Integrated Services Router (ISR) as the access router with an Integrated EtherSwitch network module for LAN and WAN connectivity. High availability is achieved through a T1 link with an ADSL backup. This profile is intended for branch networks that want to incorporate as many services as possible into a single platform solution. This profile is also very cost effective and contains the least number of devices to manage at the branch. The drawback to this profile is network resiliency and capacity planning. By having a single platform solution, there is a common point of failure. There is no platform redundancy, so a network can affect users. User capacity is also limited in this design to the number of LAN ports that the ISR platforms can support. For future growth, either an external desktop switch must be used, or another router platform is needed for additional slot capacity.

Dual-Tier Branch Profile Overview

Figure 4 shows the dual-tier branch profile.

Figure 4 Dual-Tier Branch Profile

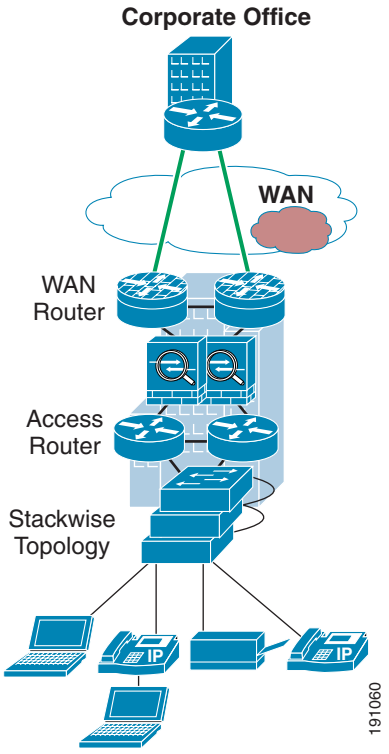


This profile is based on legacy branch networks that exist today. The intent of this profile is to illustrate how to apply advanced services within a branch network without requiring a forklift upgrade or the redesign of a current network. This profile consists of two ISR access routers connected to an external switch. Dual WAN links and box redundancy provide a greater level of high availability compared to the single-tier branch profile, at the expense of additional equipment costs and more components to manage at the branch. This branch is typical of most branches in traditional enterprise branch networks. WAN and LAN services are not integrated in this profile. The ISRs serve to terminate WAN connections and the LAN connectivity is performed by a desktop switch. For additional user capacity, an additional switch may be added via an EtherChannel. This profile exists in many legacy branch networks and is intended to serve as a migration profile to show customers how to upgrade their branch to new WAN transport such as Metro Ethernet or advanced services listed in the Integrated Services Building Block layer in the overall Enterprise Branch Architecture framework.

Multi-Tier Branch Profile Overview

Figure 5 shows the multi-tier branch profile.

Figure 5 Multi-Tier Branch Profile



This profile consists of dual ISRs for WAN termination, dual ASA appliances for security, dual ISRs for services integration, and several desktop switches in a Stackwise topology. This profile has the most network gear but produces the greatest amount of high availability and redundancy. The top ISR routers provide WAN termination, the ASA appliances provide security services, the middle ISRs provide integrated services termination and LAN connectivity is provided by external desktop switches in a Stackwise deployment model. Some services are not integrated in this profile, but redundancy and high availability are provided at every device. The multi-tier branch profile closely resembles a small campus and large enterprise branches. Additional switch port expansion can be easily achieved by simply adding more external desktop switches into the stack. This profile provides the most expansion capability, performance, and availability but requires the most management resources of devices.

In summary, the three profiles incorporate the common branch network elements into three architectures of varying cost, availability, size, expandability, and functionality. These three profiles provide the basis for all services such as security and mobility. The intent of using these three profile architectures is to determine functionality of integrated services with various high availability requirements into branch networks with various levels of services integration in a platform. The single-tier profile provides the most integration of services into a single platform at the expense of high availability. The dual-tier profile incorporates some high availability with distributed LAN connectivity via desktop switches and WAN connectivity via branch routers. The multi-tier profile offers the most availability but offers no integration of services in a single platform.

Integrated Services Building Block Layer

The integrated services building block layer provides the key technologies that branch architecture need to operate. These technologies can be used separately or together. The goal of the Enterprise Branch Architecture is to layer each technology with each other in a phased approach. Ultimately, all the key infrastructure services will function together on the three platforms established in the network infrastructure layer. The key infrastructure services are the following:

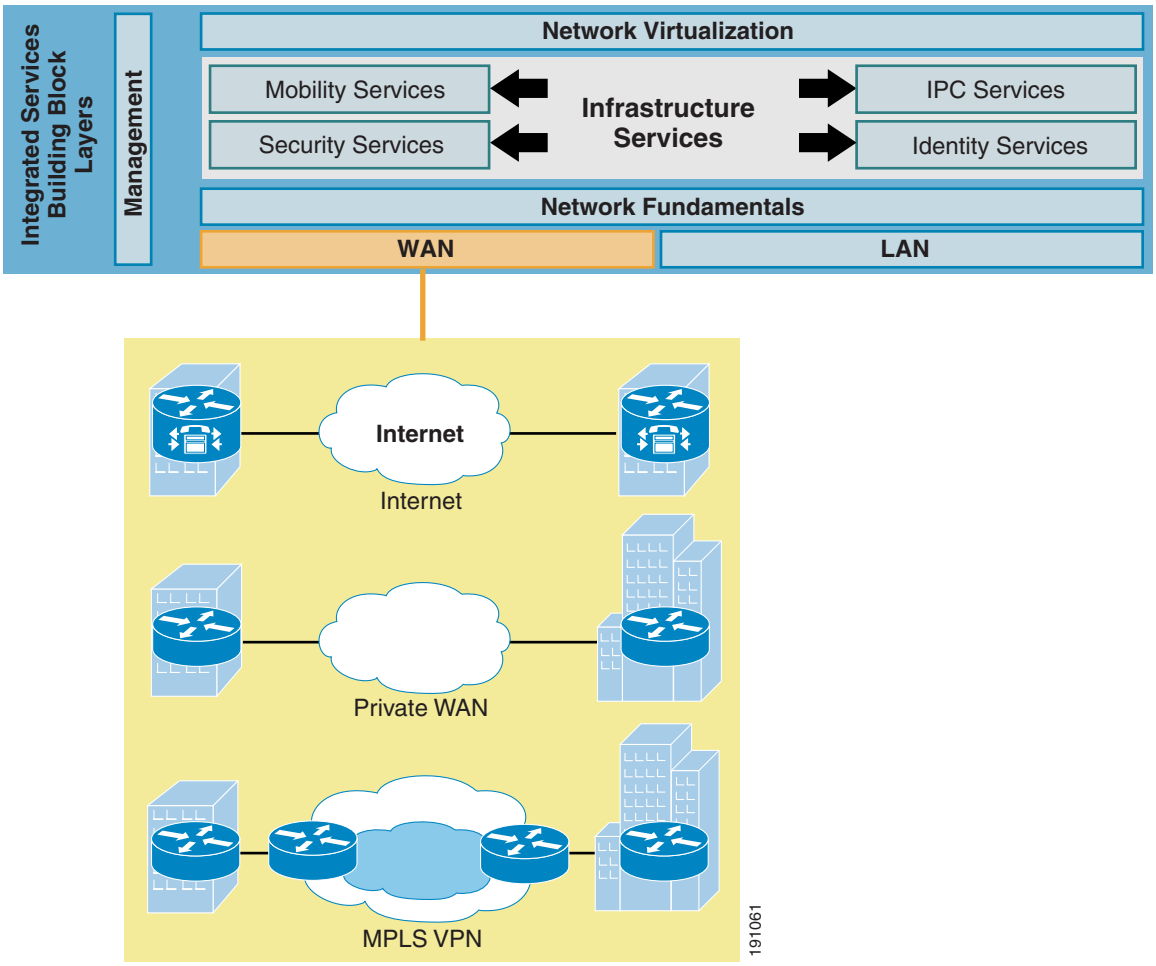
- WAN services—Foundation for branch architectures to connect to the campus core via a public or private ISP network
- LAN services—Provide end device connectivity to the corporate network within the branch
- Network fundamentals—Basic services required for network connectivity
- Security services —Enhance the device and network security from intrusion, data theft, secure data transport, and denial of service
- Identity services—Allow specific users to access specific resources. A network device interrogates the user for their identity and grants access privileges and enforces policies to them. These policies govern the user interaction with applications, as well as apply to network permissions and VLAN assignment
- Mobility services—Allows users to access network resources regardless of their physical location
- Cisco IP Communications (IPC) services—Deliver a foundation that carries voice and video across the network
- Network infrastructure virtualization—Makes one network resource appear as many instances (or many as one) and provides the ability to deal with resources on a logical rather than physical basis

Each of these key services will be explored in the three profiles established for a branch network in a phased approach. In this overview, all the above technologies are discussed at a high level to give the reader an overview of the entire Enterprise Branch Architecture roadmap. More details will be added as future testing is completed.

WAN Services

WAN services provide the foundation for the Enterprise Branch Architecture to connect to the campus or data center core via an ISP public or private network, potentially also Internet access. The WAN services building block consists of three fundamental deployment options, each with its own set of associated attributes, as shown in Figure 6.

Figure 6 WAN Deployment Models



The Internet WAN deployment model provides no data privacy and requires a secure connectivity mechanism for secured traffic. With this deployment model, all traffic traverses through an ISP cloud. The routing control is determined by the ISP and, as such, only IP protocol is supported through the cloud. Although this deployment model may provide the most cost savings, this deployment model is the least secure of the three deployment models.

The private WAN deployment model is the traditional hub-and-spoke model that has been deployed in enterprise networks for decades. The traditional Frame Relay or ATM networks would be categorized in the private WAN deployment model. Data privacy is provided through traffic separation such as Frame Relay DLCIs or ATM VCs. The routing is controlled by the enterprise routing protocol across the private WAN and both IP and non-IP protocols are supported. This deployment model is most commonly used.

The MPLS deployment uses MPLS as the WAN transport mechanism. As with the Internet deployment model, routing control is held by the ISP, and only IP protocol is supported through the cloud. However, unlike the Internet deployment model, there is data privacy through traffic separation as in the private WAN deployment model. Traffic separation is provided through labels, and traffic is placed inside a virtual route forwarding (VRF) table.

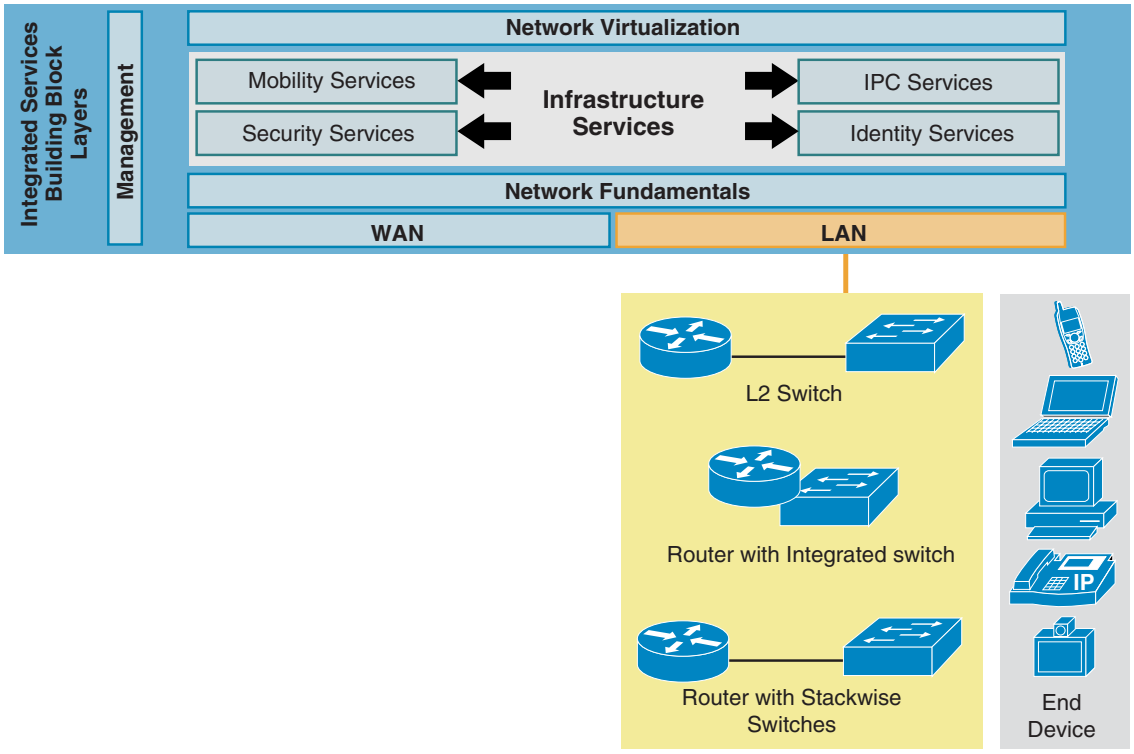
All three WAN deployment models will be tested in the Enterprise Branch Architecture. The single-tier profile uses the Internet deployment model. The dual-tier profile uses the private WAN deployment model, and the multi-tier profile uses the MPLS WAN deployment model.

For more information regarding WAN and MAN architectures, see the Enterprise WAN at the following URL: http://www.cisco.com/go/wanandman.

LAN Services

LAN services provide end device connectivity to the corporate network within the branch office. With the convergence of services onto a single network infrastructure, devices such as computers, telephones, video cameras, and so on, all require the connection to the corporate network over the LAN. Figure 7 shows the three physical configurations that may be used for LAN connectivity.

Figure 7 LAN Deployment Models



The three configurations for LAN connectivity are as follows:

- Access router connected to a physically separate Cisco Catalyst switch as a Layer 2 only switch
- Access router with an integrated switch
- Access router integrated with Cisco Catalyst switches in a Stackwise topology

An access router connected to a separate Catalyst switch provides scaling, extensive feature support, and end devices may be electrically powered inline by connecting to a Power over Ethernet (PoE) enabled switch. The access router with an integrated switch provides a one-box solution: a single device with single manageability. End devices may still receive PoE by connecting to a powered switch. The access router in a Stackwise topology provides high availability for the LAN and fault tolerance. Another issue of LAN connectivity is where to place Layer 3 routing decisions. In the past, switches were considered Layer 2-only devices, but the line between Layer 2 and Layer 3 devices has blurred. Routers may now have integrated switch ports incorporated into them, and modern switches may have Layer 3 interfaces.

All three LAN deployment models are tested in either Layer 2 or Layer 3 topology. The single-tier profile uses the access router with an integrated switch deployment model. The switches are Layer 2 devices in this profile. The dual-tier profile uses the access router connected to a physically separate Cisco Catalyst switch as a Layer 2-only device. The multi-tier profile uses the Stackwise topology and the switches all serve as Layer 3 devices.

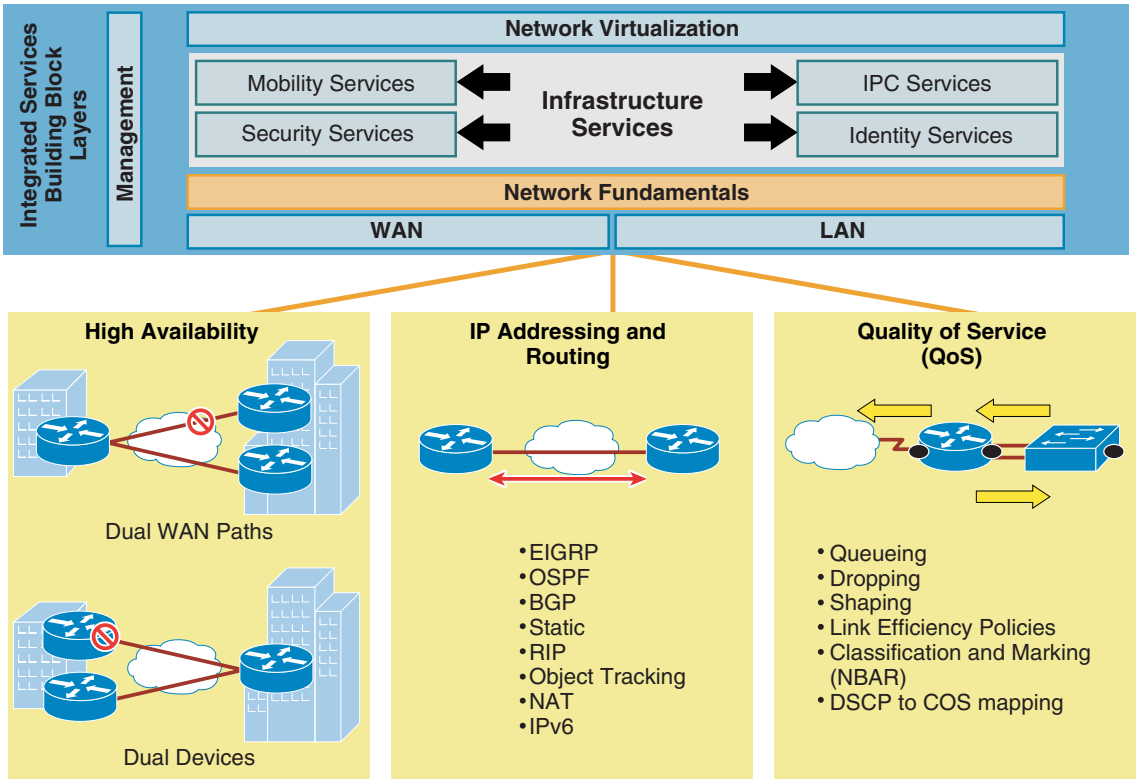
For more information on LAN deployment models, see the following documents at http://www.cisco.com/go/srnd under the Branch Office heading:

- *LAN Baseline Architecture Overview Branch Office Network* (EDCS-488184)
- *LAN Baseline Architecture Branch Office Network Reference Design Guide* (EDCS-488185).

Network Fundamentals

Network fundamentals refer to the basic services that are required for network connectivity. These services include high availability, IP addressing and routing, and QoS, as shown in Figure 8.

Figure 8 Network Fundamentals



High availability is crucial for modern branch architectures. Regardless of which technology a branch incorporates from those in the integrated services building block Layer, remaining up during a failure or outage is crucial. Branch networks cannot afford to have network downtime. In a branch office, there are several methods to achieve high availability that are explored in the three profiles. Branches can have dual WAN links to their headquarters in case of WAN failure. In addition to dual WAN links, a branch can also provide dual devices at each branch in case of a router failure or outage. For complete high availability, a branch can provide both a dual WAN link and a dual device high availability model.

The single-tier profile explores dual WAN link high availability with a T1 as the primary WAN type with ADSL as the backup link. The dual-tier profile uses the dual device model leveraging Hot Standby Routing Protocol (HSRP) for device failover. The multi-tier profile uses the combination of both high availability deployment models. Each device in the profile is replicated for device failover, and there are dual WAN links to the headquarters. In addition, the multi-tier profile adds another layer of high availability by providing the external Cisco Catalyst switches in a Stackwise topology for LAN fault tolerance.

For more information on Stackwise topology, see the Cisco Stackwise Technology White Paper at the following URL:

http://www.cisco.com/en/US/partner/products/hw/switches/ps5023/products_white_paper09186a00801b096a.shtml.

IP addressing and choice of routing protocol is vital in setting up a network and allowing connectivity. Currently, only IP is used in the Enterprise Branch Architecture; specifically IPv4. IPv6 is being scoped and will be added in future phases.

The choice of routing protocols is as unique as branch architecture. There are advantages and disadvantages to each routing protocol available. Unless otherwise noted, the Enterprise Branch Architecture uses EIGRP as the routing protocol choice. Cisco developed EIGRP, and this protocol is widely used across branch networks. OSPF, BGP, RIP, and static routing are all valid protocols; however, EIGRP was chosen for the initial phases of testing.

QoS is being regarded as a network fundamental. Maintaining high quality voice or video within the LAN or through the WAN is required on branch networks. QoS includes defining the trust on ports to prohibit unauthorized use of QoS for preferential treatment on a branch network. Access routers and switches require the following QoS policies:

- Appropriate (endpoint dependent) trust policies
- Classification and marking policies
- Policing and markdown policies
- Queuing policies

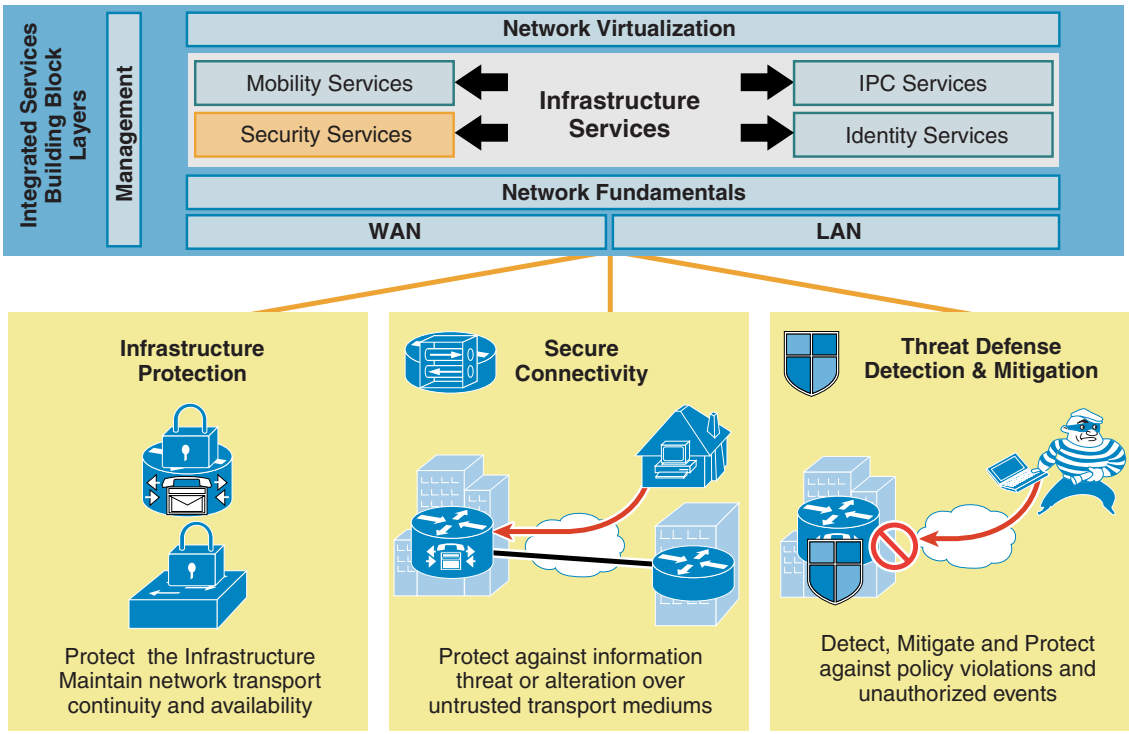
Scavenger class QoS does assist in maintaining high quality voice or video, but it can be used for abnormal network conditions such as DoS and worm attacks through the use of Network-Based Application Recognition (NBAR). NBAR classification is required to classify and mark traffic to identify and immediately drop known worm traffic.

For more in depth knowledge of QoS, see the *Enterprise QoS Solution Reference Network Design Guide Version 3.3* at the following URL:
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/ccmigration_09186a008049b062.pdf

Security Services

Security services enhance the device and network security from intrusion, data theft, secure data transport, and denial of service. Figure 9 shows the key areas of security services.

Figure 9 Security Services



These three areas of security services are as follows:

- Infrastructure protection
- Secure connectivity
- Threat defense detection and mitigation

Infrastructure protection provides proactive measures to protect the infrastructure devices; in this case, Cisco IOS Software-based routers, switches and appliances, from direct attacks as well as indirect attacks. Infrastructure protection assists in maintaining network transport continuity and availability. Turning off unnecessary services, password and login management, and SSH are all examples of Infrastructure protection services.

Secure connectivity protects against information theft or alteration of the end user data over untrusted transport mediums. The level of network security that is deployed in a branch depends on the WAN type and deployment model chosen. In a typical enterprise branch, the WAN types are generally cable/DSL for smaller branches, T1/E1 for medium branches, and T3/E3 for larger branches. The typical WAN deployment models for these WAN types are Internet, private WAN (Frame Relay), and MPLS deployment models as discussed in WAN Services, page 9.

Both Frame Relay and MPLS provide a level of secure connectivity through the use of traffic separation achieved through FR DLCIs, or MPLS VRFs. Traffic is separated from each user; however, the data is not encrypted. The Internet deployment model requires a layer of encryption to be applied. Frame Relay and MPLS can run encryption as an additional layer of secure connectivity. The fundamental aspect of encrypting network traffic is through the use of the standard encryption method, such as IP Security (IPsec). The IPsec standard provides a method to manage authentication and data protection between multiple crypto peers engaging in a secure data transfer. The four following ways to use the IPsec standard to provide secure connectivity across the WAN:

- Direct IPsec encapsulation

- Point-to-point Generic Routing Encapsulation (p2p GRE) over IPsec
- Dynamic multipoint GRE (DMVPN)
- Virtual tunnel interface (VTI)

When used alone, a direct IPsec encapsulation design provides a private, resilient network for IP unicast only, where support is not required for IP multicast, dynamic IGP routing protocols, or non-IP protocols. When dynamic routing and IP multicast (IPmc) are required, the p2p GRE over IPsec, DMVPN, or VTI may be used. If non-IP protocol support is required, only p2p GRE over IPsec is applicable. For more information on these four secure connectivity designs using IPsec, see the SRNDs under the Wide Area Network and Metropolitan Area Network at the following URL: http://www.cisco.com/en/US/partner/netsol/ns656/networking_solutions_design_guidances_list.html#anchor9

Other tunneling protocols that can be used for secure connectivity include the following:

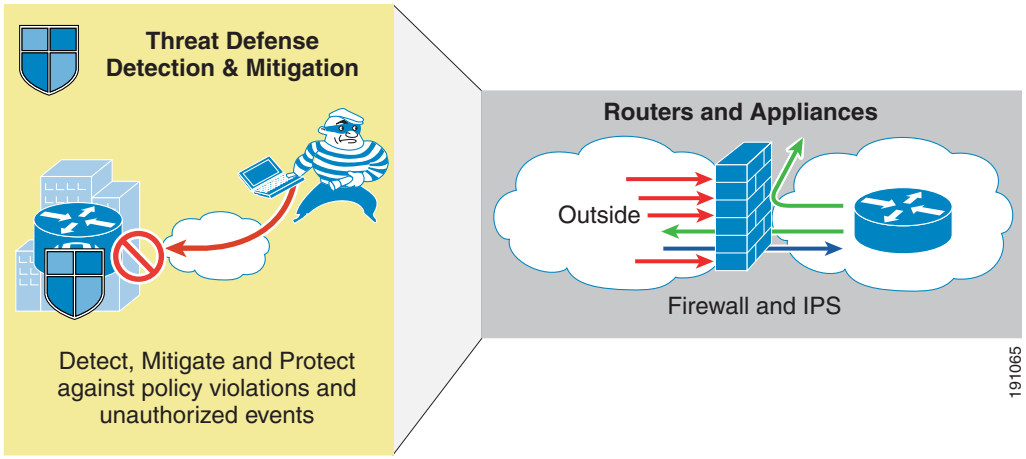
- Secure Sockets Layer/Transport Layer Security (SSL/TLS)
- VPN (WebVPN)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)

These protocols are based on user or client-to-gateway VPN connections, commonly called remote access solutions, and are not implemented in the initial phase of this solution. The single-tier profile uses DMVPN as the secure connectivity mechanism. No encryption is used for the dual-tier or multi-tier profiles. The secure connectivity mechanisms for these protocols are Frame Relay and MPLS, respectively. Plans to integrate IPsec encryption over these two profiles as well as SSL are being scoped for a future phase of testing.

Secure connectivity can be applied at the switch level as well. Although the IPsec standard is not used, traffic separation can be accomplished through virtual LANs (VLANs) and VRF in a MPLS environment. VLANs provide isolation at Layer 2 of different broadcast domains. VLANs provide a very basic level of secure connectivity by preventing cross-VLAN hopping and snooping between users on the same LAN segment. As a result, a network manager can create small Layer 2 domains for secure connectivity and addressing, which can then map into the Layer 3 routed network for enterprise-wide scalability. In conjunction with a MPLS network, VRFs provide a private forwarding table per VLAN on a LAN switch. This feature is known as VRF-lite and can map a single LAN user into a MPLS VPN as defined in RFC-2547. Through VLANs and VRFs, LAN traffic can be separated to ensure secure connectivity.

Threat defense detection and mitigation encompasses the mechanisms to detect, mitigate, and protect devices against violations and unauthorized events including perimeter and endpoint security. For router and appliances, two of these mechanisms are through firewalls and an intrusion protection system (IPS), as shown in Figure 10.

Figure 10 Threat Defense Mechanisms for Routers and Appliances



Firewalls provide stateful security and application inspection for each protocol entering or leaving a branch network. A stateful inspection firewall uses a combination of access control with application inspection to ensure that only approved responses get through the firewall. Firewalls can be used through an external appliance such as the ASA in the multi-tier profile, or in conjunction with the Cisco IOS feature set, can be used for Cisco IOS routers as in the single-tier and dual-tier profiles.

For more information on the Cisco IOS Firewall Feature Set and the ASA firewall appliance, see the Cisco IOS Firewall feature set and the Cisco ASA 5500 Series Adaptive Security Appliances at the following URLs:

- http://www.cisco.com/en/US/partner/products/sw/secursw/ps1018/index.html
- http://www.cisco.com/en/US/partner/products/ps6120/index.html

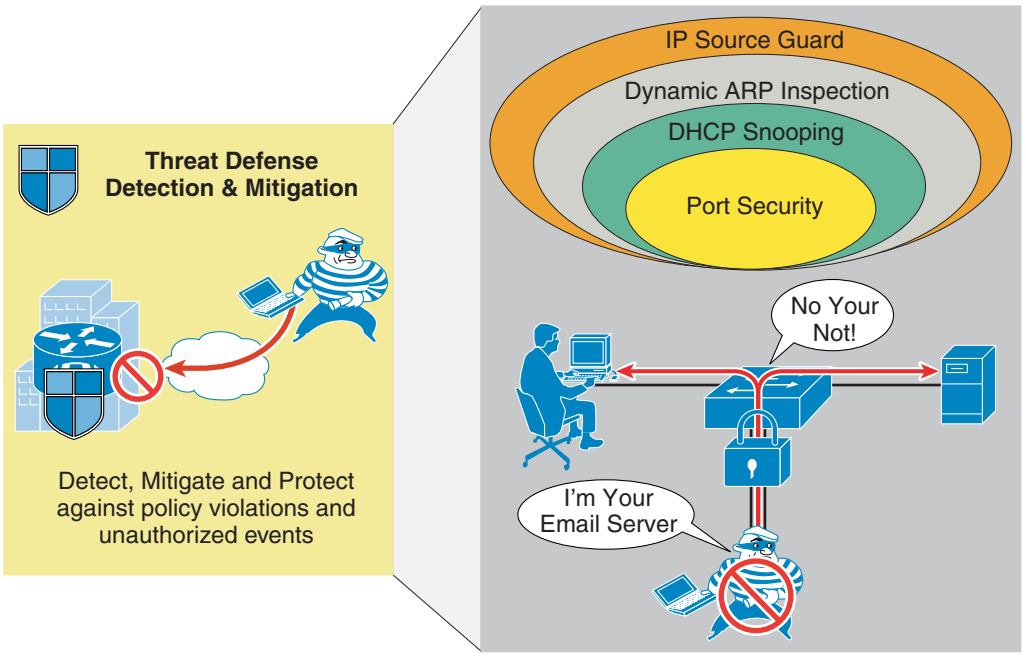
Intrusion protection monitors packets and sessions as they flow through the branch, and scans each packet to match any of the IPS signatures. When a device running IPS, either an access router with the Cisco IOS IPS feature set or an external ASA with the IPS feature set loaded or a standalone IPS sensor, detects suspicious activity, it may respond before network security can be compromised. When an IPS signature is matched, one or more of the following actions are taken

- Sends an alarm to a syslog server or a centralized management interface
- Drops the packet
- Resets the connection
- Takes no action

For more information on the Cisco IPS feature set, see Cisco IOS Intrusion Prevention System (IPS) at the following URL:
http://www.cisco.com/en/US/partner/products/ps6634/products_ios_protocol_group_home.html

Catalyst switches have additional mechanisms for threat defense that are applied on a per-port basis. These mechanisms include Port Security, DHCP Snooping, Dynamic ARP inspection, and IP Source Guard, as shown in the Figure 11.

Figure 11 Threat Defense Mechanisms for Switches



Port Security limits the number of MAC addresses that are able to connect to a switch, and ensures only approved MAC addresses are able to access the switch. This feature prevents MAC address flooding and ensures only approved users can log onto the network. With the DHCP Snooping feature enabled, a switch port forwards only DHCP requests from untrusted access ports, and drops all other types of DHCP traffic. DHCP Snooping eliminates rogue devices from behaving as the DHCP server.

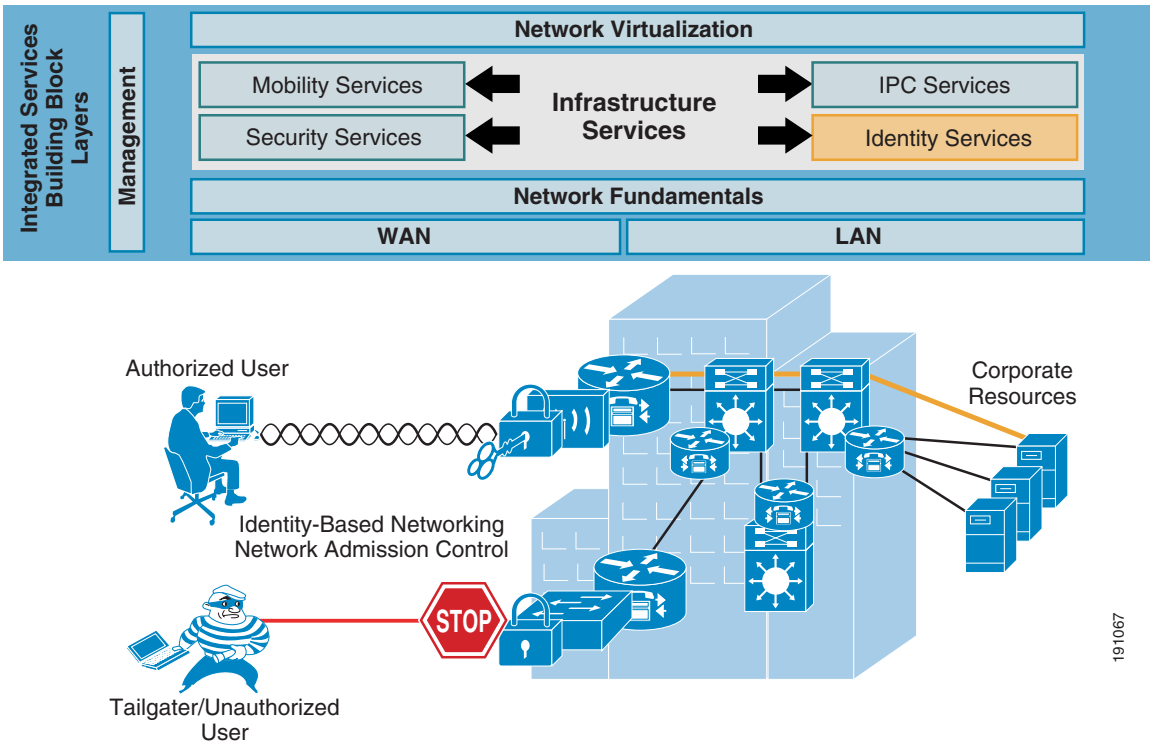
Dynamic ARP Inspection (DAI) maintains a binding table containing IP and MAC address associations dynamically populated using DHCP Snooping. This feature ensures the integrity of user and default gateway information such that traffic cannot be captured. ARP spoofing or ARP poisoning attacks are mitigated through this feature.

IP Source Guard automatically configures a port ACL for an IP address and adds a MAC address to the port security list for the port. DHCP Snooping uses the port ACL defined by IP Source Guard to assist in building the DHCP binding table. When the ACL or MAC entry lease expires, DHCP Snooping removes these entries from the table. These two features working in conjunction help to prevent snooping of data or anonymous launching of attacks. The entire Catalyst switch threat defense mechanisms are used in the three profiles defined because each profile contains a user base connecting to a Catalyst switch.

Identity Services

Identity services allow specific users to access specific resources. A network device interrogates the user for their identity and grants access privileges and enforces policies to them. The policy governs the user interaction with applications, as well as applies to network permissions and VLAN management. Identity services can be divided into two major areas: Identity-based Networking and Network Access Control (NAC). Figure 12 illustrates the main concern with identity services.

Figure 12 Identity Services



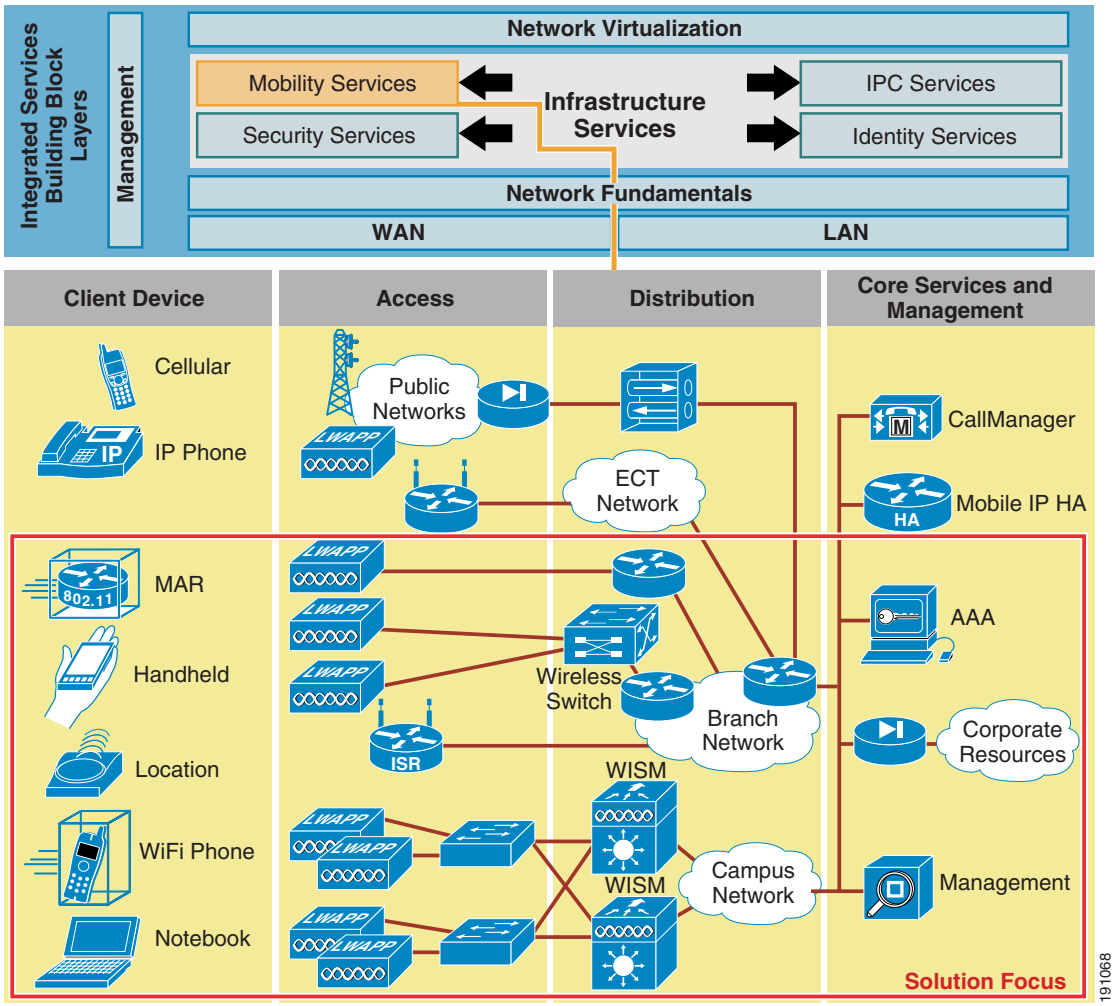
Identity-based Networking identifies the user or device on the network and ensures access to correct network resources. A branch network can authenticate and grant privileges based (authorize) on user logon information, regardless of the user location or device based on the 802.1x feature, MAC auth-bypass, WebAuth, or static assignment. The 802.1x feature, in conjunction with a RADIUS server, authenticates each user entering a network. Each user receives authorization based on their personal username and password. Identity-based networking ensures that users get only their designated privileges, no matter how they are logged onto the network, and reports unauthorized access.

NAC restricts network access by interrogating endpoint devices for policy compliance. NAC checks the endpoint device on whether it has the correct virus software and protection or operation system/application program version or patch level. NAC improves the network ability to identify, prevent, and adapt to threats.

Mobility Services

Mobility services allow users to access network resources regardless of their physical location. Mobility services provide solutions that can enable connectivity to the corporate intranet from anywhere in the world through either internal (as compared to public) wireless LAN (WLAN), cellular, or public WLAN. Figure 13 illustrates the components, such as access points, wireless controllers, and wireless end devices, needed for mobility services in a branch network.

Figure 13 Mobility Services



Unlike wired users who remain in a static location within the branch network, wireless users can connect to the branch network from anywhere inside or outside of a branch network. Providing VPN connectivity through the use of clientless SSL VPN or IPsec VPN client software to establish IPsec tunnels between corporate headquarters is based on the Identity-based Networking Identity Services discussed in the previous section, allows trusted mobile users to connect to a network from anywhere.

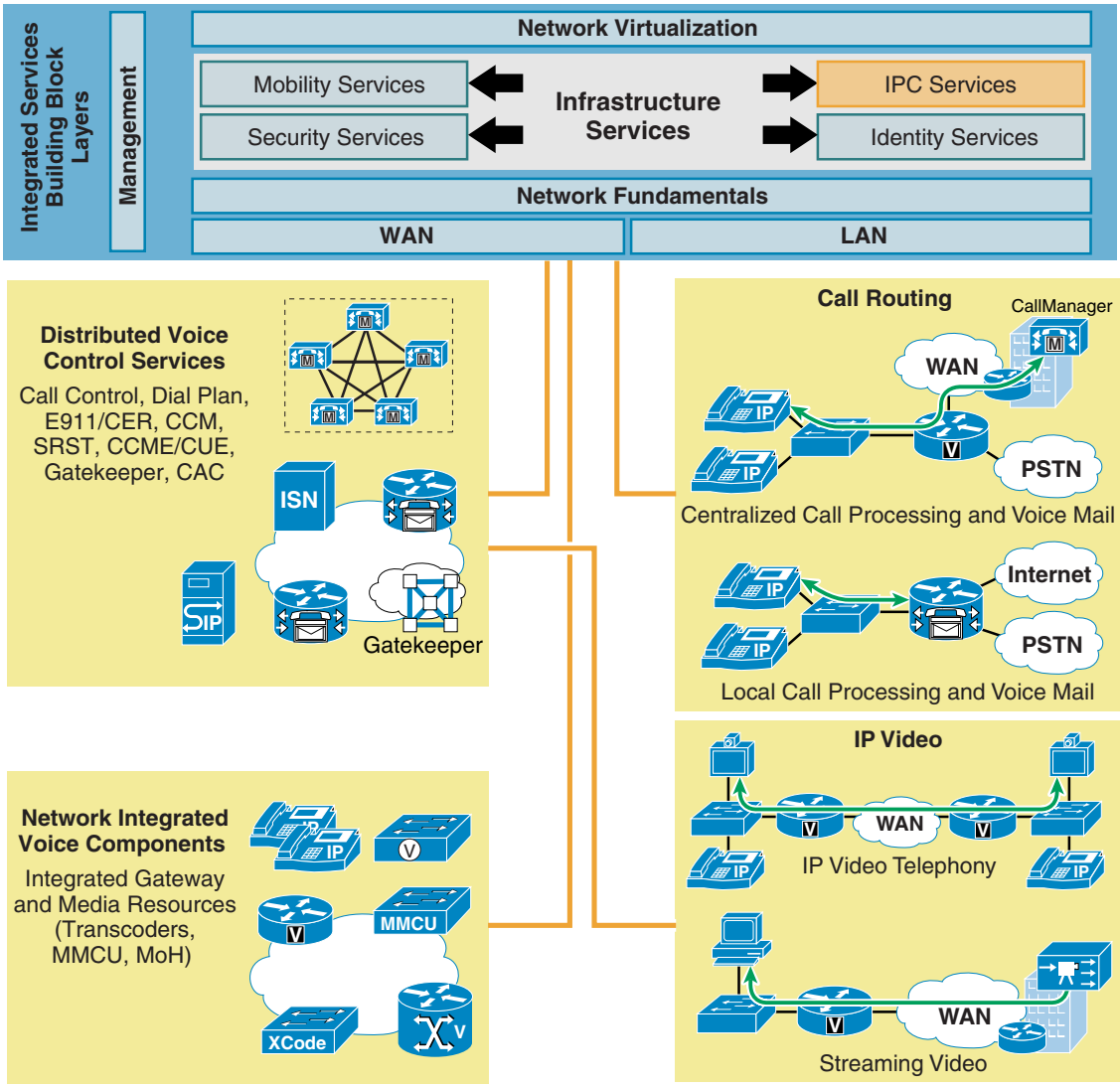
The *Enterprise Mobility 3.0 Design Guide* discusses how to provide wireless connectivity to branch locations. Sections include using Remote Edge Access Point (REAP) and Hybrid REAP (H-REAP) to address unique challenges introduced by branch locations. This design guide provides recommendations on how to offer common applications such as guest access, which segments (isolates) guest user traffic from other branch office traffic, and roaming.In addition, the "Branch Deployment" section describes scenarios where the main corporate campus comprises only a minority presence in terms of installed wireless infrastructure within the enterprise. In these cases, the majority of wireless infrastructure as well as mission-critical wireless usage are located in remote branch offices.

For more information regarding mobility designs, see the *Enterprise Mobility 3.0 Design Guide* at the following URL: www.cisco.com/go/srnd.

Cisco IP Communications (IPC) Services

IPC services encompass all services that deliver a foundation that carries voice and video across the network. Transmitting data, voice, and video over a single network infrastructure using IP while maintaining a high level of QoS, availability, and security comprise IPC services. There are numerous features and services that fall under IPC. Figure 14 summarizes the major aspects when designing a branch network for data, voice, and video.

Figure 14 IPC Services



Call routing refers to where the call processing is located: centrally or locally. Centralized call processing is primarily used to serve branches where a centralized CallManager cluster and Unity VoiceMail System reside in the headquarters and provides all the call processing and voice-mail services for the remote IP phones located in the branch. Local processing is used in branches where CallManager Express, a software feature in the access router, provides the local call processing and the Cisco Unity Express hardware module, NM-CUE, provides the local voice-mail and auto-attendant services.

Aside from call routing, IPC services for voice can also be divided into two areas: network integrated voice components, and distributed voice control components. Network integrated voice components comprise the integrated gateways and media resources. A voice over IP (VoIP) gateway is a network device that is the interface between a telephony (PSTN) network and an IP network (such as the Internet). Among other tasks, a VoIP gateway digitizes analog voice signals into digital packets. A Cisco access router can function as a voice gateway using voice IOS images, voice interfaces, and DSP resources. Media resources are the conferencing and transcoding DSPs as well as applications such as Music on Hold (MoH).

Distributed voice control services include the call control and dial plans needed for call routing. Failover mechanisms such as Survivable Remote Site Telephony (SRST) and call congestion mechanisms such as Call Admission Control (CAC) are some of these services.

Video can be transmitted either over a branch network through streaming video, as in distant learning applications, or IP video telephony using Cisco VT Advantage products. In either case, maintaining a high level of QoS is required to produce high quality video to remote branch networks.

A collection of UC design guides are available that discuss branch deployments:

The *Cisco Unified Communications SRND Based on Cisco Unified CallManager 5.x* discusses branch considerations including using a centralized or distributed call processing models, remote survivability, bandwidth recommendations, multicast music on hold, and call admission control.

Cisco Unified Contact Center Enterprise (Unified CCE) is part of the Cisco Unified Communications application suite, which delivers intelligent call routing, network-to-desktop Computer Telephony Integration (CTI), and multi-channel contact management to contact center agents over an IP network. It combines software IP automatic call distribution (ACD) functionality with Cisco Unified Communications in a unified solution that enables companies to rapidly deploy an advanced, distributed contact center infrastructure. *Cisco Unified Contact Center Enterprise 7.x Solution Reference Network Design (SRND)* provides recommendation for implementation in both single-site and multi-site contact centers. An existing Cisco IP network is used to lower administrative expenses and extend the boundaries of the contact center enterprise to include branch offices, home agents, and knowledge workers.

Cisco IP Contact Center (IPCC) Express provides a reliable and flexible voice processing and contact center solution for the enterprise. Cisco IPCC Express is a tightly integrated contact center solution providing three primary functions: interactive voice response (IVR), ACD, and CTI. Consult the *Cisco IPCC Express 4.5 Solution Reference Network Design (SRND)* for details on deploying this solution.

Cisco Unified Customer Voice Portal (CVP) is a VoiceXML-based solution that provides carrier-class IVR and IP switching services on voice over IP (VoIP) networks. The Unified CVP feature set includes the following:

- IP-based IVR services
- IP-based queuing treatment
- Integration with Cisco Unified Contact Center
- IP-based call switching
- Unified CVP Operations Console
- Voice response unit (VRU) reporting

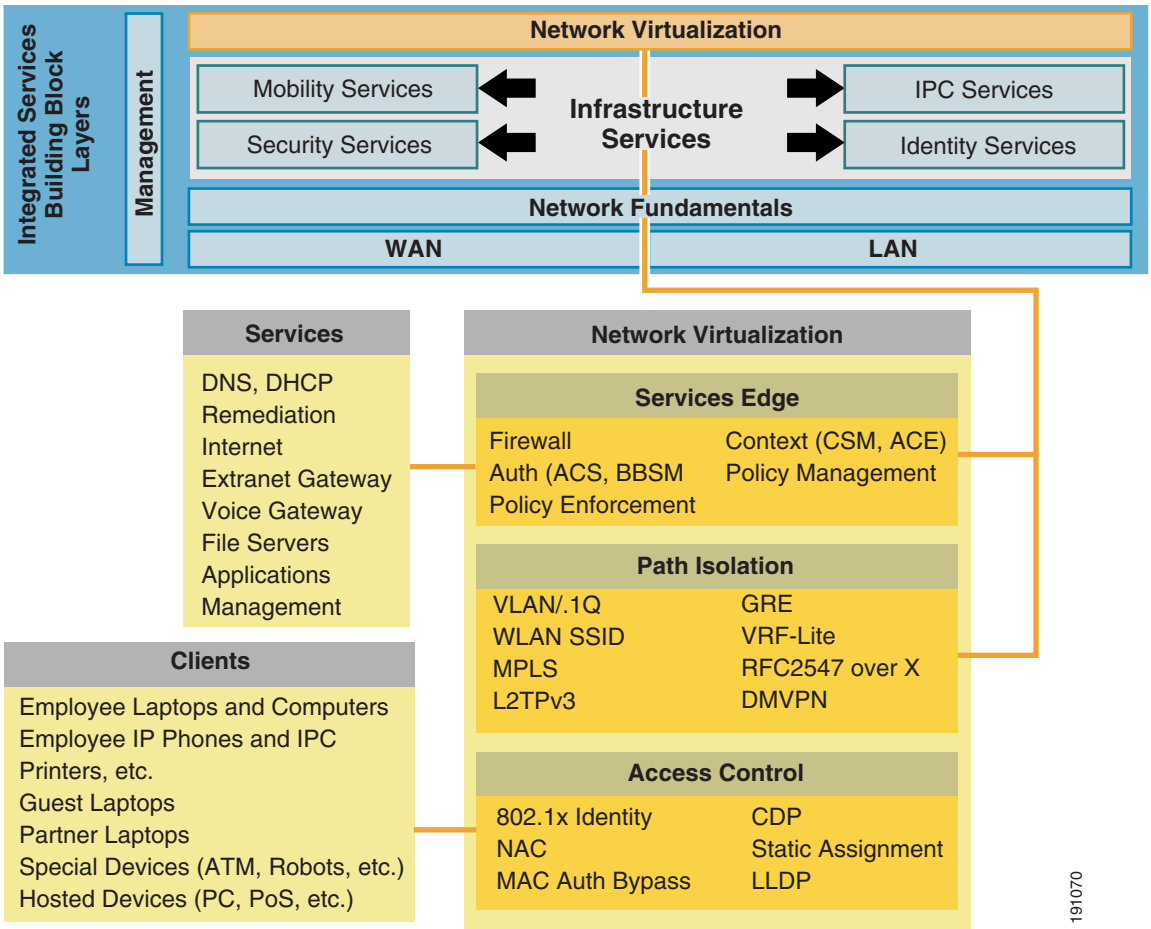
The *Cisco Unified Customer Voice Portal (CVP) 4.0 Solution Reference Network Design (SRND)* describes deployment models where the CVP components reside in the branch.

For more information regarding branch designs with Cisco IP Communications (IPC) Services, refer to the Unified Communications section at www.cisco.com/go/srnd.

Network Virtualization Services

Network virtualization is the ability to make many resources look like one (or one to look like many), and the ability to deal with resources on a logical rather than physical basis. Figure 15 summarizes the key areas of network virtualization: access control, path isolation, and services edge.

Figure 15 Network Virtualization



For branch architectures, currently only access control and path isolation of the clients listed in the above slide are required. Services edge is mainly a requirement for campus or data center and the services listed are virtualized between user groups. Access control identifies and authenticates users and devices that are attempting to access the network. Similar to identity services, now users are classified into a segment completely isolated from other users not in the same group (segment). Path isolation ensures the traffic from each segment defined is separated from each other, end-to-end across the network. Services edge provides key services as each segment enters a campus or data center environment. Allowing converged services over segmented traffic is the challenge with services edge.

Network virtualization incorporates *all* the integrated services building block layers into a completely integrated, virtualized network. Much work across Cisco is being performed on how to achieve this across all places in an enterprise network, including enterprise branch networks.

Application Networking Services

Application networking services contain the collaborative applications that take advantage of the efficiencies from the integrated services building block layer and the network infrastructure layer. Application delivery such as Cisco Wide Area Application Services (WAAS), and Application-Oriented Networking (AON) add value and can accelerate applications over an integrated network that are crucial to increasing productivity at branch sites. WAAS software incorporates WAN optimizations and application-specific acceleration techniques to enable enterprises to consolidate remote office infrastructure, optimize WAN utilization, and improve application responsiveness. AON helps to reduce the complexity of enterprise application deployment, integration, and management by providing common infrastructure capabilities directly within the network. Both AON and WAAS help to run the collaborative applications such as Instant Messaging, Unified Messaging, Cisco MeetingPlace, IPCC, RFID, and Video Delivery.

The *Enterprise Branch Wide Area Application Services Design Guide* provides guidelines and best practices when implementing WAAS in enterprise architectures. This document gives an overview of WAAS technology and then explores how WAAS operates in branch architectures with the three profiles. Design considerations and complete tested topologies and configurations are provided.

For more information regarding WAAS Designs, see *Enterprise Branch Wide Area Application Services (WAAS)* at www.cisco.com/go/srnd.

Design Selection

This section gives a high-level overview of the phases of testing incorporated in the Enterprise Branch Architecture Framework. These design guides will be published separately on http://www.cisco.com/go/srnd. This section is a roadmap of the work that will be tested going forward for an enterprise branch.

Enterprise Branch Security Design Chapter

This design chapter focuses on building the three branch profiles in the network infrastructure layer: single-tier profile, dual-tier profile, and multi-tier profile. All three LAN and WAN deployment models are investigated. Network fundamentals and security services are discussed in detail. This design chapter focuses on laying the foundation of the three profiles to start integrating other integrated services building block layer services during future testing of the Enterprise Branch Architecture Framework.

Summary

This design guide provides an overview of the entire Enterprise Branch Architecture as it applies to the SONA framework. Accomplishing the entire Enterprise Branch Architecture framework will require several phases. Individual design guides provide more detailed design and implementation descriptions for each of the major services tested.

Appendix A—Cisco Platforms Evaluated

Table 1 shows the Cisco platforms evaluated for each profile.

Table 1 Evaluated Cisco Platforms

Single-Tier Profile	
Access router	Cisco Integrated Services Routers—2800 and 3800 Series
LAN	EtherSwitch Service Module
WAN	T1—Multiflex Trunk Voice/WAN Interface Card
	ADSL—ADSLoPOTs WIC with Dying Gasp
Dual-Tier Profile	
Access router	Cisco Integrated Services Routers—2800 and 3800 Series
LAN	Catalyst 3750
WAN	T1—Multiflex Trunk Voice/WAN Interface Card
Multi-Tier Profile	
Access router	Cisco Integrated Services Routers—2800 and 3800 Series
LAN	Catalyst 3750
WAN	T1—Multiflex Trunk Voice/WAN Interface Card
Security	ASA5510

Appendix B—Cisco IOS Releases Evaluated

Table 2 Cisco IOS Releases Evaluated

Cisco Platform	Cisco IOS Release Evaluated
Access routers	Cisco IOS Release 12.4(7.7)T, Advanced IP Services Feature Set
Cisco Catalyst switches	Cisco IOS Release 12.2(25)SEE, Advanced IP Services Feature Set
ASA Security Appliances	Cisco Adaptive Security Appliance Software Version 7.0(4)

Appendix C—References and Recommended Reading

This section provides the following references and additional information related to the subjects covered in this design guide:

- Branch design—http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html#anchor1
  - Enterprise Branch Architecture Design Overview

  - LAN Baseline Architecture Overview--Branch Office Network
  - LAN Baseline Architecture Branch Office Network Reference Design Guide
  - Enterprise Branch Security Design Guide
  - Deploying IPv6 in Branch Networks
  - Enterprise Branch Wide Area Application Services (WAAS)
- WAN and MAN—
http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html#anchor10
  - IPsec VPN WAN Design Overview
  - IPsec Direct Encapsulation Design Guide
  - Point-to-Point GRE over IPSec Design Guide
  - Virtual Tunnel Interface (VTI) Design Guide
  - Dynamic Multipoint VPN (DMVPN) Design Guide
  - IPsec VPN Redundancy and Load Sharing Design Guide
  - Voice and Video Enabled IPsec VPN (V3PN) SRND
  - Multicast over IPsec VPN Design Guide
  - Digital Certificates/PKI for IPsec VPN Design Guide
  - Next Generation Enterprise MPLS VPN-Based MAN Design and Implementation Guide
  - Layer 3 MPLS VPN Enterprise Consumer Guide Version 2
  - Infrastructure Protection and Security Service Integration Design for the Next Generation WAN Edge v2.0
- Network virtualization designs—
http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html#anchor7
  - Network Virtualization—Guest Internet Access Deployment Guide
  - Network Virtualization—Access Control Design Guide
  - Network Virtualization—Path Isolation Design Guide
  - Network Virtualization—Services Edge Design Guide
- Unified Communications designs—
http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html#anchor10
  - Cisco Unified Communications SRND Based on Cisco Unified CallManager 5.x
  - Cisco Unified Contact Center Enterprise 7.x Solution Reference Network Design (SRND)
  - Cisco IPCC Express 4.5 Solution Reference Network Design (SRND)
  - Cisco Unified Customer Voice Portal (CVP) 4.0 Solution Reference Network Design (SRND)
- End to-end network services—
http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html#anchor4
  - Enterprise QoS Solution Reference Network Design Guide Version 3.3
  - Cisco AVVID Network Infrastructure IP Multicast Design (SRND)

- Mobility—
http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html#anchor6
  - Enterprise Mobility 3.0 Design Guide
- Request For Comment (RFC) papers
  - RFC-2547—BGP/MPLS VPNs
- Web sites
  - Cisco Stackwise Technology White Paper—
http://www.cisco.com/en/US/partner/products/hw/switches/ps5023/products_white_paper09186a00801b096a.shtml
  - Wireless/Mobility Solutions for Large Enterprise—
http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/networking_solutions_packages_list.html
  - Enterprise QoS Solution Reference Network Design Guide Version 3.3—
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/ccmigration_09186a008049b062.pdf
  - Cisco IOS Firewall Feature Set—
http://www.cisco.com/en/US/partner/products/sw/securesw/ps1018/index.html
  - Cisco ASA 5500 Series Adaptive Security Appliances—
http://www.cisco.com/en/US/partner/products/ps6120/index.html
  - Cisco IOS IPS Feature Set—
http://www.cisco.com/en/US/partner/products/ps6634/products_ios_protocol_group_home.html
  - Identify-Based Networking Systems Configuration Guide—
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns75/c654/cdccont_0900aecd803fab62.pdf
  - Implementing Network Admission Control Phase One Configuration and Deployment—
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd80217e26.pdf

Appendix C—Acronyms

Term	Definition
ATM	Asynchronous Transfer Mode
DHCP	Dynamic Host Configuration Protocol
DMVPN	Dynamic Multipoint Virtual Private Network
DSL	Digital Subscriber Line
EIGRP	Enhanced Interior Gateway Routing Protocol
FR	Frame Relay
FTP	File Transfer Protocol
GRE	Generic Route Encapsulation

HSRP	Hot Standby Router Protocol
IOS	Internetwork Operating System
IPsec	IP Security
ISP	Internet Service Provider
MPLS	Multi-Protocol Label Switching
OSPF	Open Shortest Path First
p2p GRE	Point-to-Point GRE
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User System
VoIP	Voice over IP
V3PN	Voice and Video Enabled IPsec VPN
VPN	Virtual Private Network
VTI	Virtual Tunnel Interface
WAN	Wide Area Network