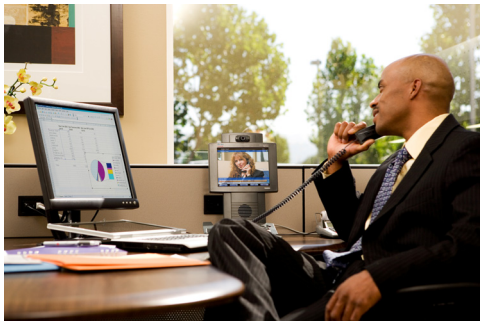


Streamlined Medium Branch Network Overview

Revised: December 21, 2009

This chapter describes the Streamlined Medium Branch Network design and components.

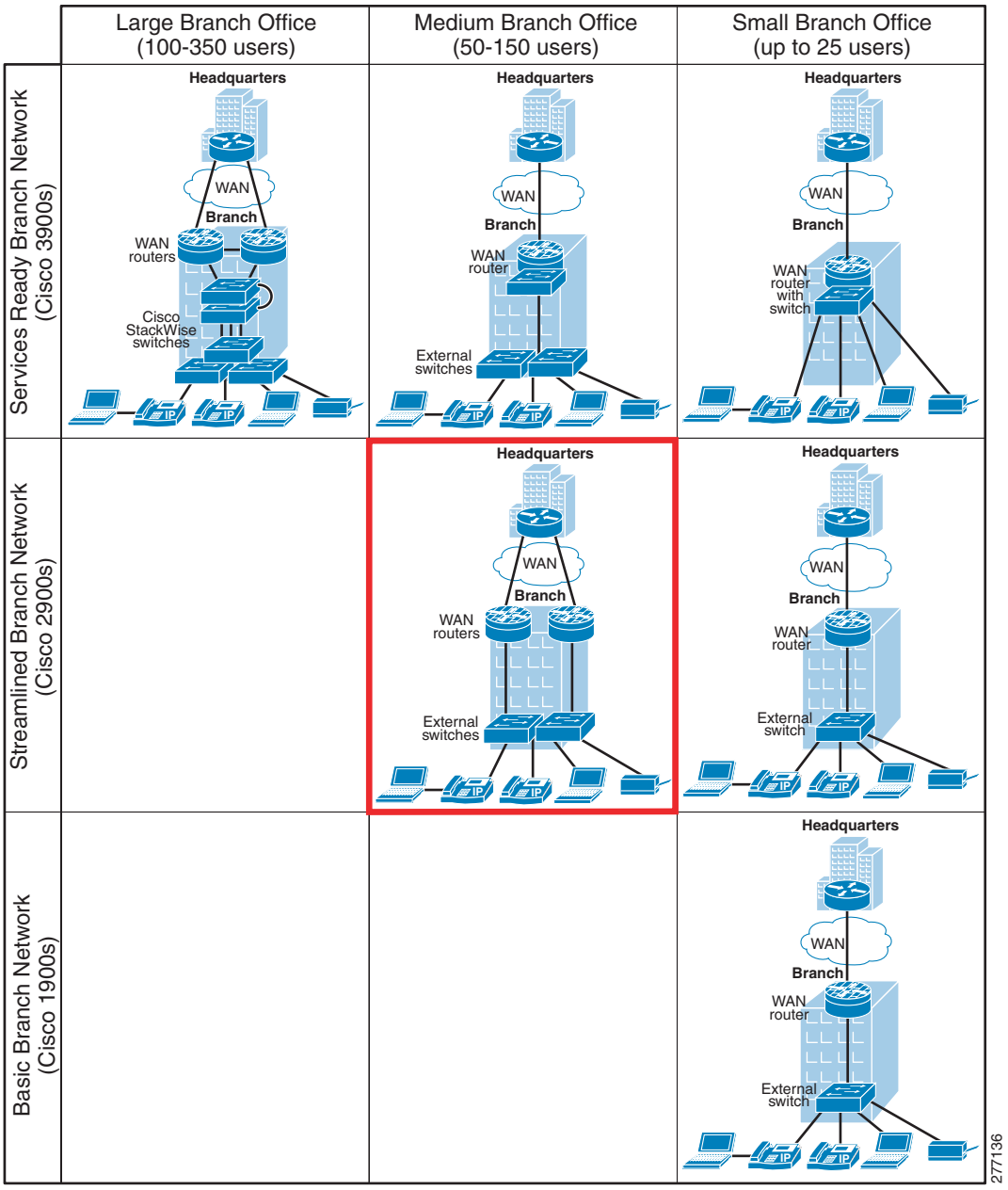
Contents

Introduction

The Streamlined Medium Branch Network enables enterprises with branch offices of 50 to 100 users to deploy high-value network services such as unified communication and application optimization on top of a secure branch network infrastructure that is connected to a campus or data center core (central site) over a variety of WAN technologies. The goal of the Streamlined Medium Branch Network is to make deployment of these services fast, simple, and predictable.

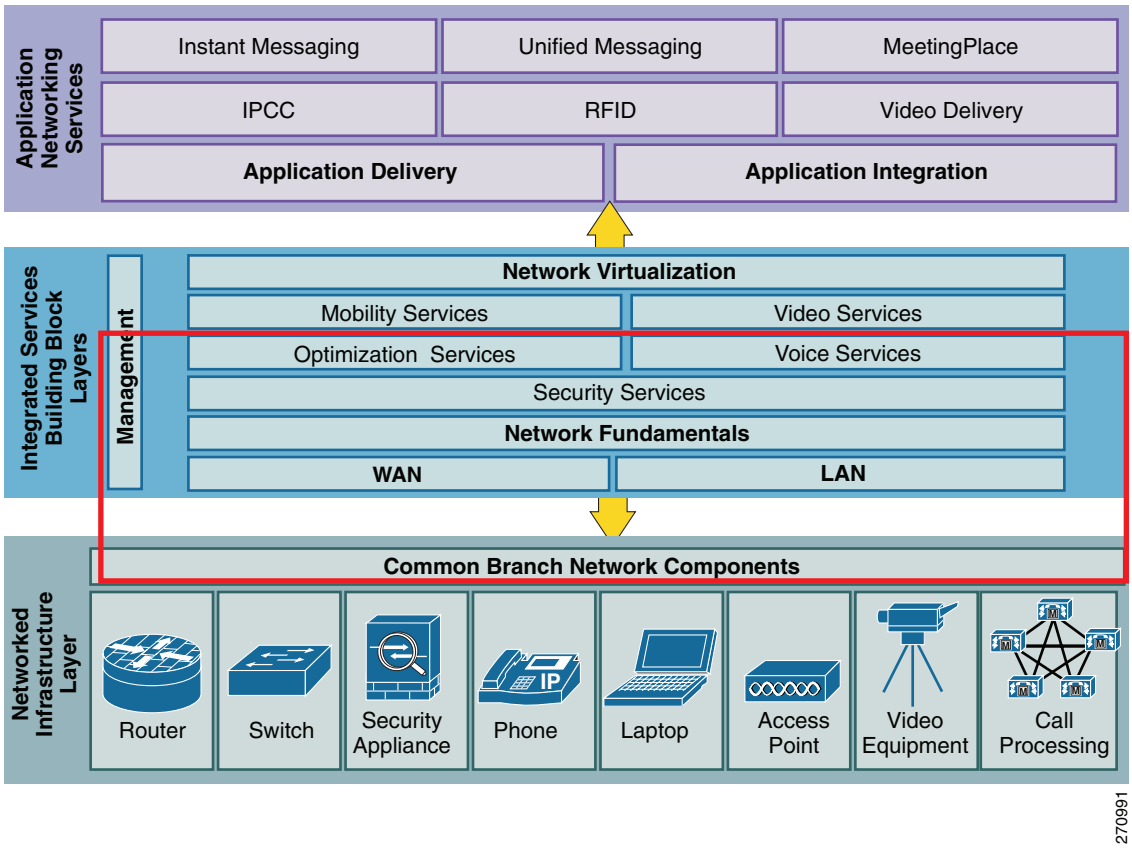
The Streamlined Medium Branch Network is one of the Cisco Integrated Services Networks for the branch office. These networks focus on providing branch office deployment blueprints for connectivity, security, voice, and application optimization services integrated into the branch router. Integrated Services Branch Networks consist of three Services Ready Branch Networks, two Streamlined Branch Networks, and one Basic Branch Network, each corresponding to a different size branch office and branch router platform, as shown in Figure 1.

Figure 1 Integrated Services Branch Networks



The Integrated Services Branch Networks are implementations of the Cisco Enterprise Branch Architecture framework and focus on networking services directly integrated into the branch office router. The Framework is one component in the overall Cisco Service Oriented Network Architecture (Cisco SONA), which provides guidelines for designing advanced network capabilities into enterprise IT infrastructure. Leveraging elements of the Cisco Enterprise Branch Architecture Framework, the Cisco Integrated Services Branch Networks incorporate networking infrastructure components and the most common integrated services found in a typical branch office, as shown in the red box in Figure 2. All Integrated Services Networks have undergone an intensive system assurance test program and will be tested on an ongoing basis as individual components continue to evolve.

Figure 2 Common Integrated Services in Enterprise Branch Networks



This guide focuses on deployment of the Streamlined Medium Branch Network. It provides design, implementation, and testing guidelines for the following features for a medium branch network:

- WAN services
- LAN services
- Network fundamentals
  - IP routing and addressing
  - Quality of service (QoS)
  - High availability
- Security services
  - Infrastructure protection
  - Access control
  - Secure connectivity
  - Threat prevention, detection, and mitigation
- Network management
- Voice services
  - IP telephony with centralized call control
  - IP telephony with local call control
  - Traditional telephony and fax

- Optimization services
  - WAN optimization
  - Application optimization

The blueprint begins with a list of design criteria for a secure medium branch office network optimized for unified communication and access to centrally hosted enterprise applications. The "System Design" section on page 7 describes the network topology and network services that address these design criteria. The "System Implementation" chapter provides a step-by-step implementation of the topology and configuration of each service. Finally, testing methodology for the system is provided along with test cases and test results in the "System Testing" chapter. The "References and Recommended Reading" section on page 13 lists additional detailed documents on the various technologies used in the Streamlined Medium Branch Network.

For a list of tested platforms, interface cards, modules, and software versions, see the "Cisco Platforms and Versions Evaluated" section on page 12.

Medium Branch Design Considerations

Today most enterprise resources are typically located at the corporate headquarters and accessed from a branch office over a private WAN. However, certain types of applications and services continue to be deployed in the branch office. To support them, a branch network must meet additional requirements beyond basic connectivity. For the medium branch office, these requirements typically include high availability, security, manageability, telephony, and application optimization. The Streamlined Medium Branch Foundation has been designed to meet such requirements. The following are its main design criteria:

Branch Network Components

- 50 to 100 active users within the branch office
- Multiple integrated network services deployed in the branch router
- Converged data, voice, and video network
- Minimal carbon footprint
- Majority of corporate resources are centrally located
- Telephony that supports the following use cases:
  - Moderate call volume user
  - Heavy call volume user
  - Decision maker

  - Video-conferencing user
  - Conference room

WAN Services

- Dedicated bandwidth ranging from 3 to 6 Mb/s to handle data, voice, and video traffic
- Gigabit Ethernet or multiple T1 dedicated lines to WAN service providers network
- Traditional Layer 2 private WAN with various encapsulation options to guarantee privacy and reliability

  or

  Layer 3 Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) for increased flexibility and reduced bandwidth cost

  or

  Layer 2 Ethernet or MPLS VPN for greater control and simplified connectivity

LAN Services

- Hierarchical network design to simplify deployment, troubleshooting, and management
- Connectivity to branch devices at Fast Ethernet or Gigabit Ethernet speeds
- Near-wire-speed performance between all devices
- Networking device redundancy without traffic loops
- Power-over-Ethernet (PoE)

Network Fundamentals

- High availability, rapid recovery, and disaster recovery
  - Prolonged uptime and availability, to keep the branch productive
  - Rapid recovery in case of non-redundant component failure
  - Automatic switchover to backup WAN link that has a minimum one-quarter of the bandwidth of the primary WAN link
  - Elimination of all single points of failure between all networking devices
  - Ability to restore service within 24 hours in the event of a disaster
  - Maximum use of backup, standby, and spare links and devices
- Quality of service (QoS)
  - Application-specific traffic prioritization both within the branch office and across the enterprise WAN
  - Bandwidth management for WAN-based traffic
  - Provisions for IP telephony, business video, critical and bulk data applications
  - Provisions to mitigate denial of service (DoS) and worm attacks
  - Identification and classification of critical application flows for QoS
- IP routing and addressing
  - Routing within the enterprise and between the branch and the service provider network
  - Direct Internet access from the branch
  - Support for multicast applications

  - Translation of private addresses and ports in order to access the Internet
  - Dynamic allocation of IP addresses for end devices

Security Services

- Infrastructure protection
  - Physical securing of access to networking devices
  - Disabling of unused services that may be used to exploit the network
  - Authentication of routing protocol updates
- Access control
  - Authentication and authorization services for controlling access to network resources
  - Logging capabilities for auditing access to network devices and resources
  - Integration with global access management system to enforce access privileges
- Secure connectivity
  - Secure interoffice connectivity for full-mesh and hub-and-spoke WAN topologies
  - Secure access into the branch network for remote or home office workers
  - Voice, video, and data separation on the LAN
  - Separation of network management traffic
  - Access to the server in the branch by home office users
- Threat protection, detection, and mitigation
  - Blocking of unauthorized traffic from entering or leaving the branch
  - Access to servers in the branch by home office users
  - Verification of source addresses for incoming traffic
  - Identification and mitigation of common DoS attacks and worms
  - Prevention of malicious attacks on the branch office network from outside
  - Prevention of attacks and security breaches from within the branch office

Network Management

- Monitoring of networking services through a unified management console
- Analysis of IP services and generation of data needed for verification of service level agreements
- Ability to synchronize network time to accurately analyze network performance
- Traffic monitoring and accounting
- Common infrastructure for collecting and logging events generated by network devices
- Ability to automate initial software installation and configuration of all network devices
- Ability to automate reconfiguration of all network devices

Voice Services

- Ability to use IP-based and traditional analog telephones in the branch network
- Support for WAN-based (Toll Bypass), LAN-based (Private Exchange), and PSTN (Traditional) calling
- Ability to regulate quantity of calls placed over the WAN

- Support for direct dial to extension, caller ID, and calling number identification
- Support for voice and video calls
- Local voice mail and auto attendant
- Ability to use traditional analog fax devices
- Support for conference calling
- Transcoding of various voice codecs
- Connectivity to emergency services
- Support for multiple dial peers and plans
- Music on hold for waiting callers
- Capacity to support:
  - 5:1 user-to-active call ratio
  - 4:1 WAN-to-PSTN call ratio
  - 4:1 WAN-to-LAN call ratio
  - 2 percent of calls to be video
  - 5 percent of calls to be conferencing calls
  - 10 percent of calls resulting in a transcoding session
- Survivable central-site call control

  or

  Local call control

Optimization Services

- Maximize WAN link bandwidth utilization and throughput
- Improve response time of typical enterprise client/server applications

System Design

Branch network design varies greatly from one enterprise to another. Each design reflects the size, location, cost constraints, and business requirements of the corresponding branch office. However, regardless of the network architecture, a set of common branch networking elements provides:

- Network connectivity within the branch, to the Internet, and to the rest of the enterprise
- Security for data residing in the branch or crossing the network
- Unified network management and configuration
- Voice and fax services to support reliable, converged VoIP and POTS communication
- Response time or data throughput acceleration for centrally located enterprise applications

To help enterprises address these common connectivity, security, management, voice, and optimization needs, the Streamlined Medium Branch Network assembles the most important and common of these elements in a single, rigorously tested design. The goals of this design are to provide assurance that the various features interoperate and to provide a starting point for customization. The design focuses only on the services that integrate directly into the branch office router. Alternative designs that feature external appliances and provide the same functionality as the Streamlined Medium Branch Network are equally viable.

For guidance on implementation of such designs, see the Cisco enterprise branch architecture documents at:

http://www.cisco.com/en/US/netsol/ns656/networking_solutions_program_home.html.

The following components and fundamental connectivity, security, and management services were tested in the Streamlined Medium Branch Network:

Branch Network Components

- Cisco 2951 and Cisco 2921 Integrated Services Routers (ISRs)
- Cisco Catalyst 3560 Switches
- Cisco Unified IP Phones 7942G, 7945G, 7961G, 7962G, 7965G, 7971G, and 7985G
- Cisco Unified IP Conference Station 7936

WAN Services

- Dedicated leased lines through service provider network
  - Four T1 lines with Multilink Frame Relay (MLFR), Multilink Point-to-Point Protocol (MLPPP) encapsulation
  - Two T1 lines with Multilink Frame Relay, MLPPP encapsulation
  - Gigabit Ethernet line shaped to 6 Mb/s
- Virtual lines through service provider network provisioned at provider edge (PE) devices
  - Frame Relay service

    Connectivity to service provider's PE device

    Four T1 lines with MLFR encapsulation

    Two T1 lines with MLFR encapsulation
  - Layer 3 Virtual Private Network (L3VPN)

    Connectivity to service provider's PE device

    Four T1 lines with MLPPP encapsulation

    Two T1 lines with MLPPP encapsulation
  - Layer 2 Virtual Private Wire Service (VPWS)

    Connectivity to service provider's PE device:

    Four T1 lines with MLPPP encapsulation

    Two T1 lines with MLFR encapsulation

Four T1 lines with MLFR encapsulation

Gigabit Ethernet line shaped to 6 Mb/s

LAN Services

- Access switches with EtherChannel configuration
- Power-over-Ethernet (PoE)
- Fast Ethernet and Gigabit Ethernet connectivity

Network Fundamentals

- High availability, rapid recovery, and disaster recovery
  - Redundant edge routers and links among networking devices
  - Backup WAN link with Symmetric High-Speed Digital Subscriber Line (SHDSL)
  - Hot Standby Router Protocol (HSRP) for routers
  - EtherChannel configuration for switches
  - Routers and switches with modular, field-replaceable components
- IP addressing and routing
  - Network Address Translation (NAT)/Port Address Translation (PAT)
  - Open Shortest Path First (OSPF)
  - Enhanced Interior Gateway Routing Protocol (EIGRP)
  - Border Gateway Protocol (BGP)
  - Routing Information Protocol (RIP) Version 2
  - Dynamic Host Configuration Protocol (DHCP)
  - Multicast
- QoS
  - Hierarchical 8-class QoS Model using Low Latency Queuing (LLQ), Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), and Differentiated Services Code Point (DSCP)-WRED on the router
  - Policing of voice and video traffic on the egress WAN interface
  - Shaping on the egress WAN interface
  - Class of service (CoS) to DSCP mapping with Weighted Round Robin (WRR) queuing on LAN switches
  - DSCP re-marking on LAN switches
  - Rate policing on LAN switches
  - Congestion-only queuing on LAN switches
  - Network Based Application Recognition (NBAR)

Security Services

- Infrastructure protection
  - Disabling of unused services
  - Console timeouts

  - Password protection
  - Secure Shell (SSH) access
  - Routing protocol security
- Access control
  - Authentication, Authorization, and Accounting (AAA) with RADIUS and TACACS+
  - Syslog
- Secure connectivity
  - Encryption with 3 DES (Data Encryption Standard) and 256-bit Advanced Encryption Standard (AES)
  - Key exchange with Diffie-Hellman Group 2
  - Data integrity with Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1)
  - Preshared key (PSK)
  - IP Security (IPsec) Dynamic Multipoint VPN (DMVPN)
  - IPsec Group Encrypted Transport VPN (GETVPN)
  - 802.1Q virtual LANs (VLANs)
  - WebVPN (SSL VPN)
- Threat Protection, Detection, and Mitigation
  - Cisco IOS Intrusion Prevention System (IPS) with advanced signature set
  - Zone-based Cisco IOS firewall
  - 802.1x
  - Port security
  - IP source guard
  - PortFast bridge protocol data unit (BPDU) guard
  - DHCP snooping
  - Dynamic Address Resolution Protocol (ARP) inspection
  - Standard and extended Access Control Lists (ACLs)
  - Unicast Reverse Path Forwarding (uRPF)
  - DoS attack and worm detection and mitigation with NBAR

Management Services

- Simple Network Management Protocol (SNMPv3)
- Cisco Configuration Professional (CCP)
- Network Time Protocol (NTP)
- IP service level agreements (SLAs)
- NetFlow version 5
- Syslog
- Cisco Configuration Engine

Voice Services

- Cisco Unified Communications Manager (Cisco Unified CM)
- Survivable Remote Site Telephony (Cisco Unified SRST)
- Cisco Unified Communications Manager Express (Cisco Unified CME)
- Voice Gateway
- Cisco Unity Express
- Resource Reservation Protocol (RSVP) agent
- Digital trunk line for PSTN connectivity
- Analog device connectivity
- Emergency services
- Packet voice digital signal processing modules (PVDM)
- Fax pass-through
- Fax T.38 relay
- Transcoding
- Conferencing
- G.711 and G.729a codecs
- cRTP
- Music on hold (MOH)

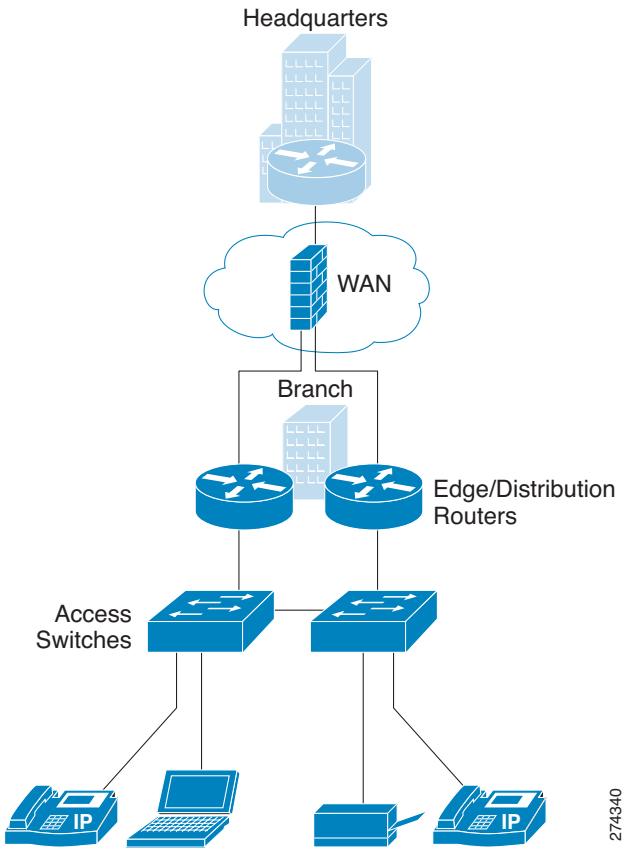
Optimization Services

- Cisco Wide Area Application Services (Cisco WAAS)

Topology

The Streamlined Medium Branch Network provides performance, availability, security, and network manageability for the medium branch, and integrates the various network services into the branch office router. As Figure 3 shows, it consists of dual Cisco 2900 series ISRs (either Cisco 2951 or Cisco 2921 ISRs) for WAN termination and services aggregation, and an access layer with two Catalyst 3560 switches for LAN connectivity. Access layer switches provide connectivity to end devices and provide control of access to the network. Redundancy and high availability are provided between all networking devices. This topology meets the criteria highlighted in the "Medium Branch Design Considerations" section on page 4.

Figure 3 Streamlined Medium Branch Network Topology



Cisco Platforms and Versions Evaluated

The information in this document is based on the hardware and software listed in Table 1 and Table 2.

Table 1 Hardware Configurations

Platform	Configuration
Cisco 2951	EHWIC, 256MB flash , 512MB DRAM Cisco IOS Release 15.0(1)M–Advanced Enterprise Services Image
Cisco 2921	EHWIC, 256MB flash , 512MB DRAM Cisco IOS Release 15.0(1)M–Advanced Enterprise Services Image
Catalyst 3560	WS-C3560G-48PS-S WS-C3560G-48TS-S 128 MB DRAM, 32 MB flash Cisco IOS Release 12.2(25)SEE4—IP Services Image

Table 2 Hardware and Software Versions

Component	Version
AIM2-CUE	3.1
NME-WAE-502	4.0.19
Cisco Unified IP Phones 7942G, 7945G, 7961G, 7962G, 7965G, 7971G, 7985G	8.3.x
Cisco Unified Conference Station 7936	1.2(1)
Cisco Unified Communications Manager Express (Cisco Unified CME)	4.1
Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST)	4.1
Cisco IOS Intrusion Prevention System (Cisco IOS IPS)	5.0
Cisco Configuration Engine	3.0

References and Recommended Reading

For more information on topics described in this guide, see the following documents:

- *Cisco WAFS Benchmark Tool for Microsoft Office Applications Installation and Configuration Note*
- *High Availability Campus Network Design—Routed Access Layer Using EIGRP or OSPF*
- *LAN Baseline Architecture Branch Office Network Reference Design Guide*
- *Enterprise QoS Solution Reference Network Design Guide*
- *Business Ready Teleworker Design Guide*
- *Enterprise Branch Security Design Guide*
- *Enhanced IP Resiliency Using Cisco Stateful Network Address Translation*
- *Stateful Failover for IPSec*

The following information is referenced in this guide:

- Cisco Design Zone for Security
- *Cisco IOS Configuration Fundamentals Command Reference*
- *Cisco IOS Debug Command Reference*
- *Cisco IOS IP Addressing Services Command Reference*
- *Cisco IOS IP Application Services Command Reference*
- *Cisco IOS IP Multicast Command Reference*
- *Cisco IOS IP Routing Protocols Command Reference*
- *Cisco IOS LAN Switching Command Reference*
- *Cisco IOS NetFlow Command Reference*
- *Cisco IOS Quality of Service Solutions Command Reference*
- *Cisco IOS Security Command Reference*

- *Cisco IOS Voice Command Reference*
- Cisco Solution Reference Network Design Guides
- *Streamlined Medium Branch Network Quick Start Guide*
- Support–Cisco Systems