

Basic Small Branch Network Overview

Revised: December 21, 2009

This chapter describes the Basic Small Branch Network design and components.

Contents

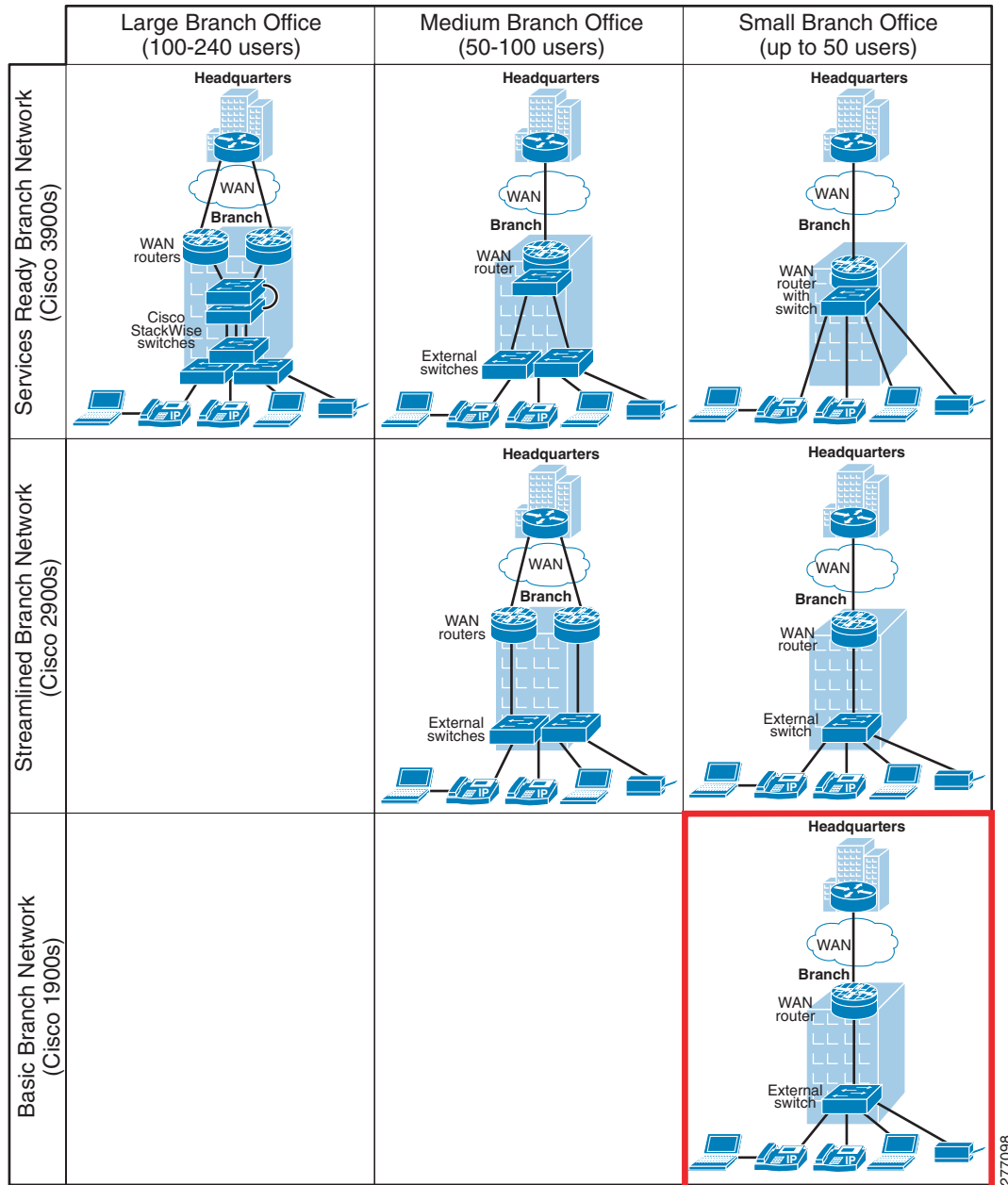
- [Introduction, page 1](#)
- [Small Branch Design Considerations, page 4](#)
- [System Design, page 7](#)
- [Topology, page 11](#)
- [Cisco Platforms and Versions Evaluated, page 13](#)
- [References and Recommended Reading, page 14](#)

Introduction

The Basic Small Branch Network enables enterprises with branch offices of up to 25 users to deploy high-value network services such as unified communication 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 Basic Small Branch Network is to make deployment of these services fast, simple, and predictable.

The Basic Small 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 Basic Branch Networks, and one Basic Branch Network, each corresponding to a different size branch office and branch router platform, as shown in [Figure 1](#).

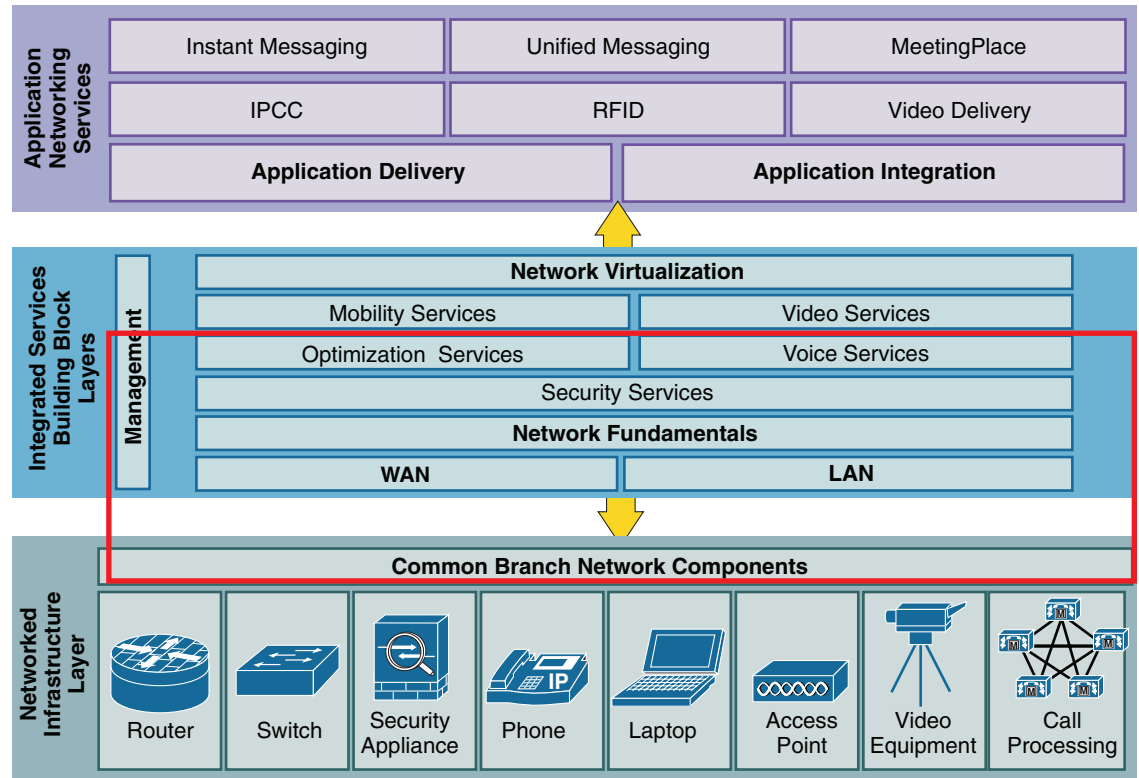
Figure 1 *Integrated Services Branch Networks*



277098

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



270991

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

- WAN services
- LAN services
- Network fundamentals
 - IP routing and addressing
 - Quality of service (QoS)
- 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

The blueprint begins with a list of design criteria for a secure small branch office network that can be optimized for unified communications. 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 14](#) lists additional detailed documents on the various technologies used in the Basic Small Branch Network.

For a list of tested platforms, interface cards, modules, and software versions, see the [“Cisco Platforms and Versions Evaluated” section on page 13](#).

Small 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 small branch office, these requirements typically include security, manageability, and telephony. The Basic Small Branch Network has been designed to meet such requirements and offers two deployment options. One provides security services for a branch office of up to 25 users. The other provides security and voice services for a branch office of up to 15 users. The following are its main design criteria:

- [Branch Network Components, page 4](#)
- [Branch Network Components for Voice-Enabled Basic Branch, page 4](#)
- [WAN Services, page 5](#)
- [LAN Services, page 5](#)
- [Network Fundamentals, page 5](#)
- [Security Services, page 6](#)
- [Network Management, page 6](#)
- [Voice Services, page 6](#)

Branch Network Components

- Up to 25 active users within the branch office
- Multiple integrated network services deployed in the branch router
- Minimal carbon footprint
- Majority of corporate resources are centrally located

Branch Network Components for Voice-Enabled Basic Branch

- Up to 15 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 0.75 to 1.5 Mb/s to handle data, voice, and video traffic
- Fast Ethernet, single T1, or fractional 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
- Power-over-Ethernet (PoE)

Network Fundamentals

- High availability, rapid recovery, and disaster recovery
 - 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
 - Ability to restore service within 24 hours in the event of a disaster
- Quality of service (QoS)
 - Automatic application-specific traffic prioritization both within the branch office and across the enterprise WAN
 - Bandwidth management for WAN-based traffic
 - Provisions to mitigate denial of service (DoS) and worm attacks
 - Identification and classification of critical application flows for QoS
- Additional Quality of Service (QoS) for the voice-enabled branch
 - Manual application-specific traffic prioritization both within the branch office and across the enterprise WAN
 - Provisions for IP telephony, business video, critical and bulk data applications
- 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 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

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

To help enterprises address these common connectivity, security, management, and voice needs, the Basic Small 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 Basic Small 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 Basic Small Branch Network:

- [Branch Network Components, page 8](#)
- [Branch Network Components for Voice-Enabled Basic Branch, page 8](#)
- [WAN Services, page 8](#)
- [LAN Services, page 9](#)
- [Network Fundamentals, page 9](#)
- [Security Services, page 9](#)
- [Management Services, page 10](#)
- [Voice Services, page 10](#)

Branch Network Components

- Cisco 1941 Integrated Services Router (ISR)
- Cisco Catalyst 2960 Switch

Branch Network Components for Voice-Enabled Basic Branch

- Cisco 1861 ISR
- Cisco Catalyst 2960 Switch
- 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
 - A T1 lines with Multilink Frame Relay, Multilink Point-to-Point Protocol (MLPPP) encapsulation
 - A ½ T1 line with PPP or Frame Relay (FR) encapsulation
 - Fast Ethernet line shaped to 1.5 Mb/s
- Virtual lines through service provider network provisioned at provider edge (PE) devices
 - Frame Relay service
 - Connectivity to service provider's PE device
 - A ½ T1 line with Frame Relay (FR) encapsulation
 - Layer 3 Virtual Private Network (L3VPN)
 - Connectivity to service provider's PE device
 - A T1 line with PPP encapsulation
 - A ½ T1 line with PPP encapsulation
 - Layer 2 Virtual Private Wire Service (VPWS)
 - Connectivity to service provider's PE device:
 - A T1 line with PPP encapsulation
 - A ½ T1 line with PPP encapsulation
 - A T1 line with Frame Relay (FR) encapsulation

A ½ T1 line with Frame Relay (FR) encapsulation
Fast Ethernet line shaped to 1.5 Mb/s

LAN Services

- Power-over-Ethernet (PoE)
- Fast Ethernet connectivity

Network Fundamentals

- High availability, rapid recovery, and disaster recovery
 - Backup WAN link with Symmetric High-Speed Digital Subscriber Line (SHDSL)
 - 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)
 - Routing Information Protocol (RIP) Version 2
 - Dynamic Host Configuration Protocol (DHCP)
 - Multicast
- QoS
 - Automatic QoS (AutoQoS)
 - 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)
- Additional QoS for the voice-enabled branch
 - 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

Security Services

- Perimeter 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 (CCE)

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
- Analog lines 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)

Topology

The Basic Small Branch Network provides security, and network manageability for the small branch, and integrates the various network services into the branch office router. As [Figure 3](#) shows, there are two topologies.

One topology consists of a single Cisco 1861 series ISR for WAN termination, services aggregation, and LAN connectivity, and a Catalyst 2960 access switch for additional LAN connectivity. This topology features security and voice services.

The other topology consists of a single Cisco 1941 series ISR for WAN termination, services aggregation, and a Catalyst 2960 access switch for LAN connectivity. This topology only features security but supports a larger number of users.

Both topologies meet the criteria highlighted in the “[Small Branch Design Considerations](#)” section on [page 4](#).

Figure 3 Basic Small Branch Network Topology for Security and Voice Services

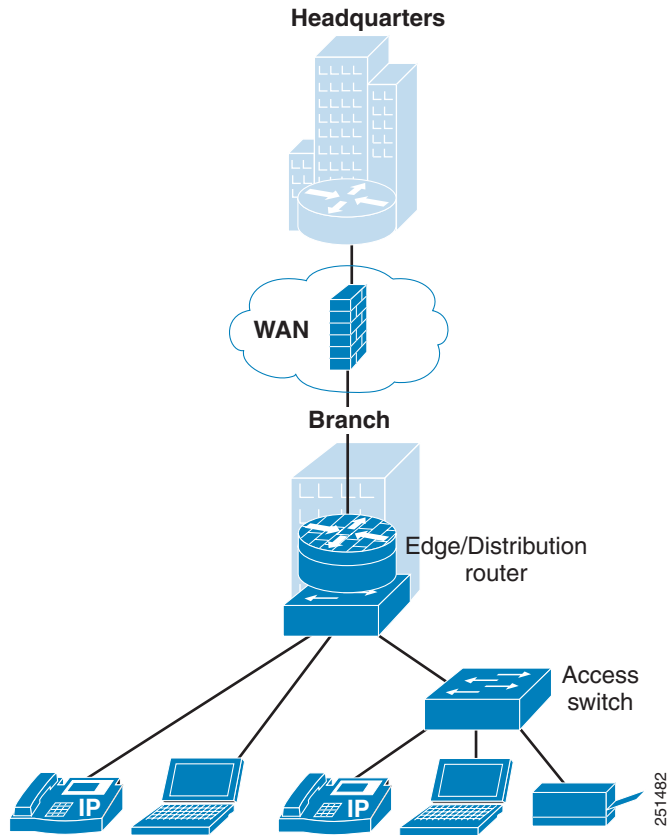


Figure 4 *Basic Small Branch Network Topology for Security Services*



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 1861	HWIC-1T1/E1, PVDM3-32, 128 MB DRAM, 64 MB flash Cisco IOS Release 12.4(20)T2–Advanced Enterprise Services Image
Cisco 1941	EHWIC, 512MB DRAM, 256MB flash Cisco IOS Release 15.0(1)M–Advanced Enterprise Services Image

Table 1 Hardware Configurations (continued)

Platform	Configuration
Catalyst 2960	WS-C2960G-24-TC-L, 64 MB DRAM, 32 MB flash Cisco IOS Release 12.2(25)SEE4 - IP Services Image
Catalyst 2960	WS-C2960PD-8TT-L, WS-C2960-8TC-L, 64 MB DRAM, 32 MB flash Cisco IOS Release 12.2(25)SEE4 - IP Services Image

Table 2 Hardware and Software Versions

Component	Version
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 (CCE)	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
- *Basic Small Branch Network Quick Start Guide*
- Support–Cisco Systems

