SMART Designs

Cisco Hosted Small Business Communications 2.0

Design Guide

October, 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Cisco SMART Designs

The Cisco SMART Designs consists of solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit www.cisco.com/go/partner/smartdesigns.

CONTENTS

Cisco Hosted Small Business Communications 2.0 Design Guide

This design guide is part of Cisco SMART Designs, which help Cisco partners serve small business customers with a broad range of Cisco products. Cisco SMART Designs are simple, efficient, and include the most commonly used Cisco-validated solutions for quick and effective deployment. These designs facilitate the phased deployment of solutions to provide investment protection for small business customers.

Cisco SMART Designs reduce overall system complexity and help service provider partners with various levels of technical knowledge deploy the Cisco Hosted Small Business Communications (HSB) Communications solution effectively. This design guide and the accompanying implementation guides provide a Cisco-validated reference for designing and implementing the HSB solution. Implementation guides and application notes provide pre-validated and easy-to-follow configuration steps. This design guide explains the features, underlying technologies, and guidelines for selecting products best suited for customer-specific deployments. It includes the following sections:

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

Design Overview

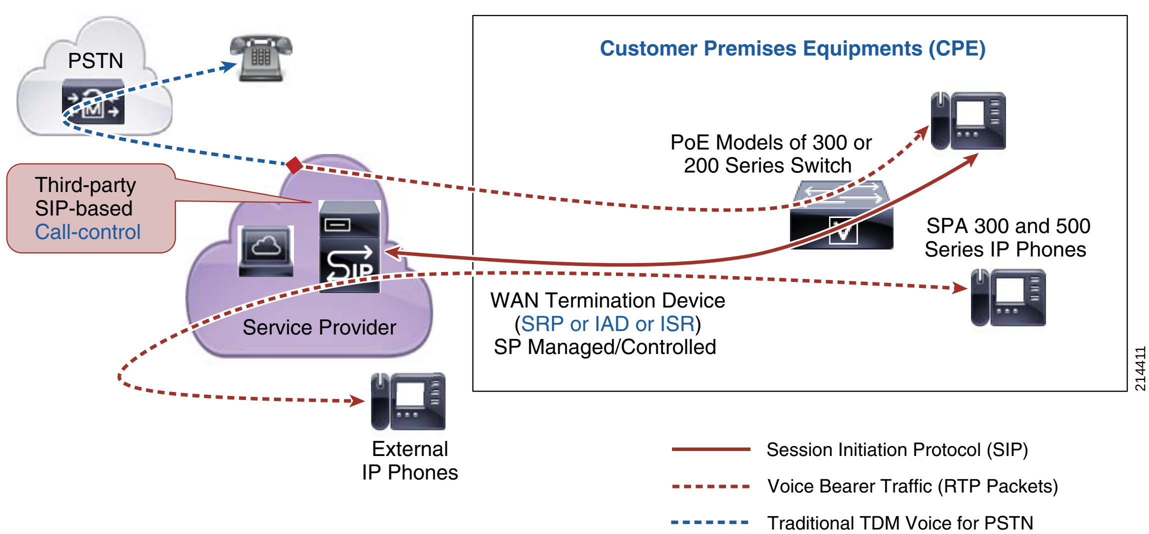
Cisco Hosted HSB Communications is a complete customer premises equipment (CPE) solution that equips SPs with a fully-tested communications infrastructure that consists of Cisco routers, switches, and IP phones, along with proven, documented deployment scenarios with major third-party call control platforms. The HSB solution supports standards-based provisioning and management, including TR-069, XML, and DCHP Option 66, 159, and 160. The efficiency of this solution reduces time to market and lowers operating expenses for service providers, allowing the deployment of hosted communication services for small businesses with confidence and ease.

Small businesses have multiple options for obtaining communications services, including hosted and premises-based solutions. For those businesses who choose a hosted solution, service providers can deploy a complete Cisco solution that helps them achieve economies in deployment and service delivery. This solution includes the following:

- One of the following WAN termination edge devices:
  - Cisco SRP52x, and SRP54x Series Services Ready Platform
  - Cisco IAD88x, and IAD243x Series Integrated Access Device
  - Cisco Integrated Service Router (ISR): 8xx Series, 19xx Series, 2901 and 2911
- Voice-ready LAN infrastructure using Cisco Small Business 300 or 200 Series switches
- Cisco Small Business IP Phones:
  - Cisco SPA300 Series IP Phones
  - Cisco SPA500 Series IP Phones

The WAN connection on the SRP, IAD, or ISR has a direct physical connection to the SP aggregation device. Both data traffic to the Internet and voice traffic to the PSTN and to other VoIP endpoints traverse through the SP infrastructure. Voice service is provided using SIP proxy devices and SIP servers. Figure 1 shows a deployment scenario, with a single SP providing both data and voice services by using a Cisco SRP52x/54x, Cisco IAD88x/243x, or Cisco ISR router.

Figure 1 Hosted Bundled Data and Voice Service Provided Using CPE



The Cisco HSB Communications solution provides the following capabilities and features:

- WAN termination device—Cisco SRP52x/54x, Cisco IAD88x/243x, or Cisco 8xx/19xx/2901/2911 ISR with the following capabilities and features:
  - Industry-leading SIP stack to support interoperability with popular soft switches and SIP servers.
  - Various types of WAN interfaces—Fast Ethernet, ADSL, G.SHDSL, and T1/E1 to provide Internet connectivity.
  - Network security services such as Network Address Translation (NAT), Intrusion Prevention System (IPS), Stateful Packet Inspection (SPI) firewall, and high-speed IPSec VPN.
  - 3G wireless WAN readiness (SRP and ISR onbly.
  - TR-069 and XML-based provisioning for near zero-touch deployment.
- Voice-ready LAN infrastructure—Design and implementation of a LAN infrastructure using Cisco Small Business 300 or 200 Series switches. Preferred switches are 300 series and have following key capabilities:
  - Switches with 8, 24, or 48 Power over Ethernet (PoE) FastEthernet ports and 8 or 24 PoE ports of GigabitEthernet to directly connect IP phones and other network-attached devices.
  - High reliability for demanding business applications, including optional redundant power supply.
  - Advanced network security to protect sensitive business information, including IEEE 802.1x, port security, access control lists (ACLs), VLANs, and MAC address notification features.
  - Network design flexibility with small form-factor pluggable (SFP) expansion slots that support fiber optic or Gigabit Ethernet uplink connectivity.
  - Integrated quality of service (QoS) intelligence to ensure high quality for real-time traffic of delay-sensitive applications such as voice and video.
  - Simple configuration and management through a browser-based device manager.
  - Cisco Discovery Protocol (CDP), Voice Service Discovery Protocol (VSDP), and Auto Smartport features.
- Cisco Small Business IP Phones—Cisco SPA300 and 500 Series IP Phones with the following capabilities and features:
  - Connect directly to a hosted IP telephony service using SIP.
  - Wideband audio codec to enhance voice quality.
  - Applications to enhance employee productivity.
  - Easy installation and highly secure remote provisioning, as well as menu-based and browser-based configuration.
  - PoE-powered, intuitive, easy-to-use, feature-rich IP phones.
  - Cisco SPA525G is a 5-line IP phone with Bluetooth and Wi-Fi capability.

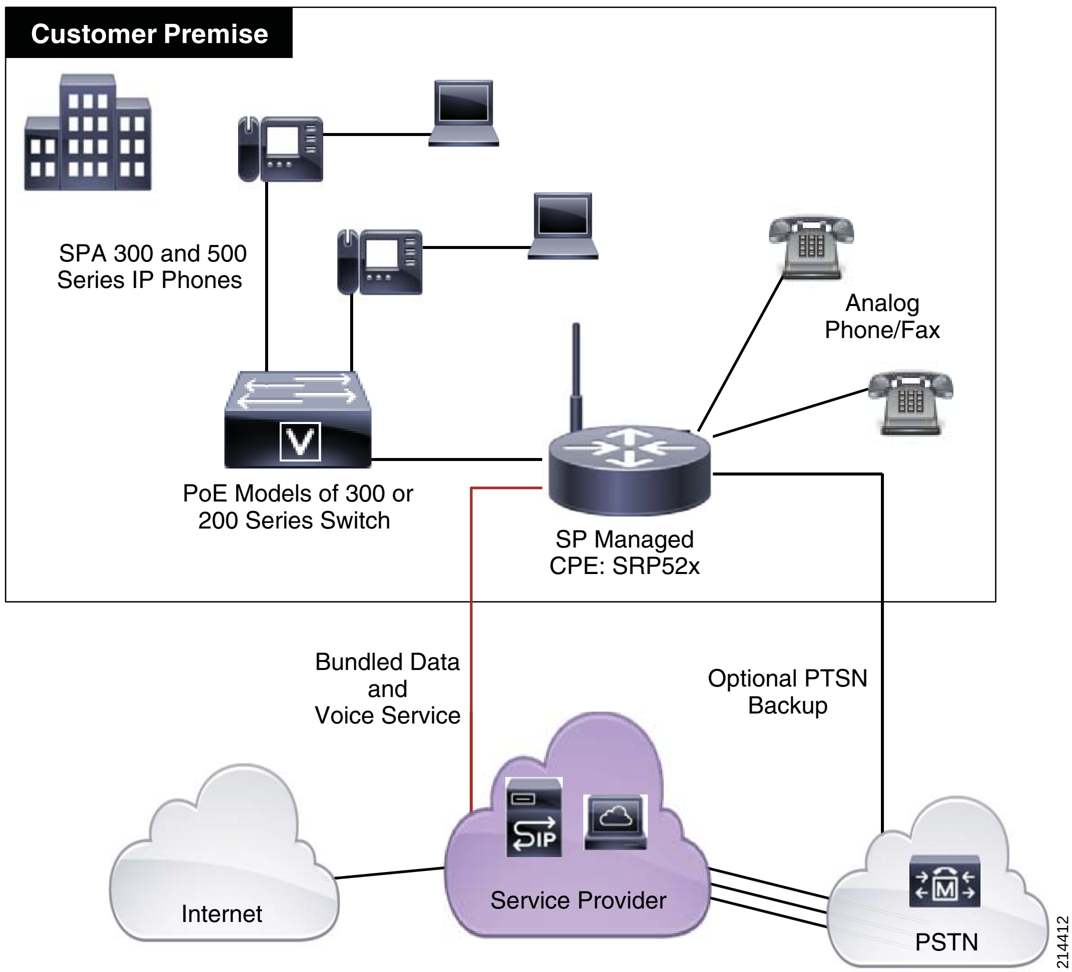
Deployment Options

This section describe three deployment options for HSB Communications solutions. These options are primarily based on the number of phones. Other factors to consider are PSTN backup, data WAN backup, wireless, and so on. This section includes the following topics:

For 10 or Less Phones

Figure 2 shows the Cisco HSB Communications solution for 10 or less phones, which is deployed using a Cisco SRP52x device and a Cisco Small Business 300 Series PoE switch with a minimum of eight ports. The Cisco SRP52x is controlled and managed by the SP.

Figure 2 HSB Communications Solution for 10 or Less Phones

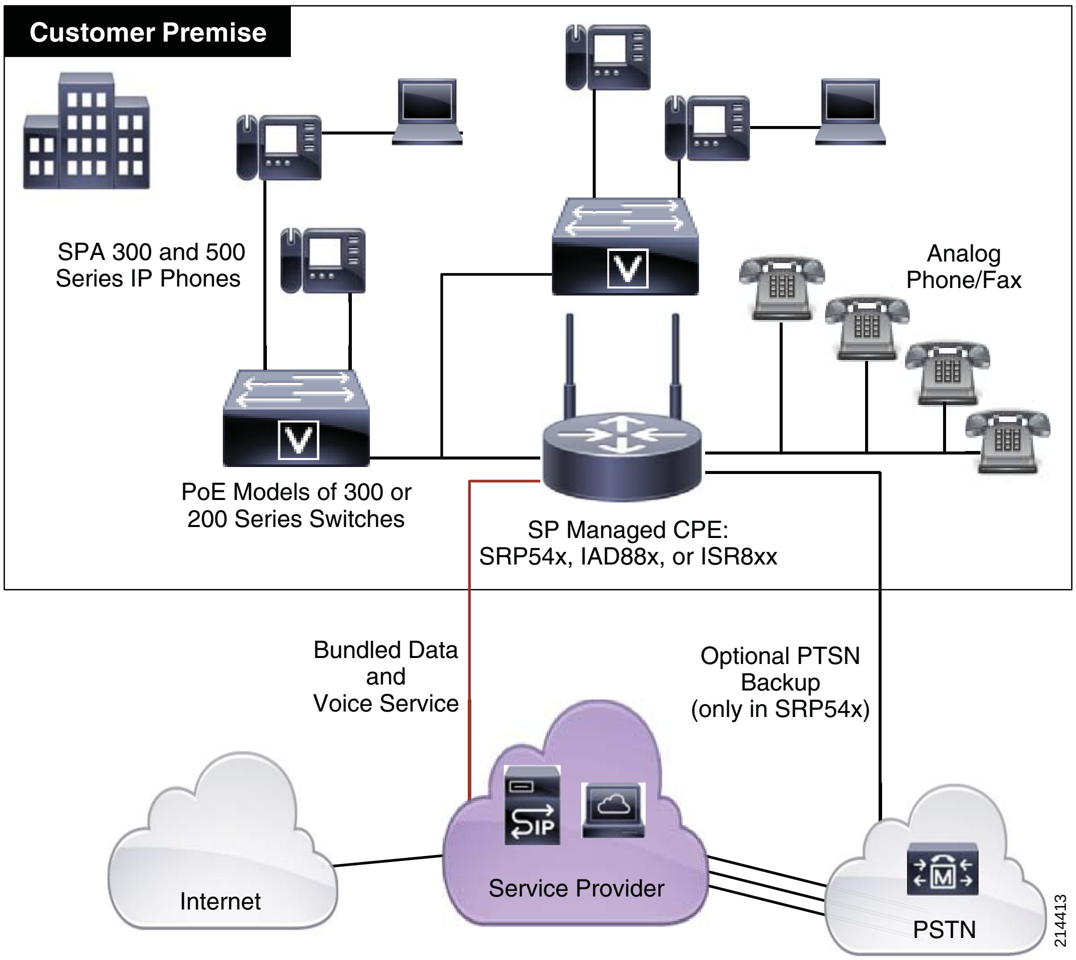


Note Cisco SRP52x platforms have one FXO port to provide PSTN backup for only one analog station.

For 11 to 50 Phones

Figure 3 shows the HSB Communications solution for 50 or less phones, which is deployed using a Cisco SRP54x Series device, IAD88x Series device, or a Cisco ISR8xx series router and one or two Cisco Small Business 300 Series PoE switches with the appropriate number of ports. The SPR54x, IAD88x, or ISR8xx is managed and controlled by the SP.

Figure 3 HSB Communications Solution for 50 or Less Phones



Note SRP54x platforms have one FXO port to provide PSTN backup for only one analog station.

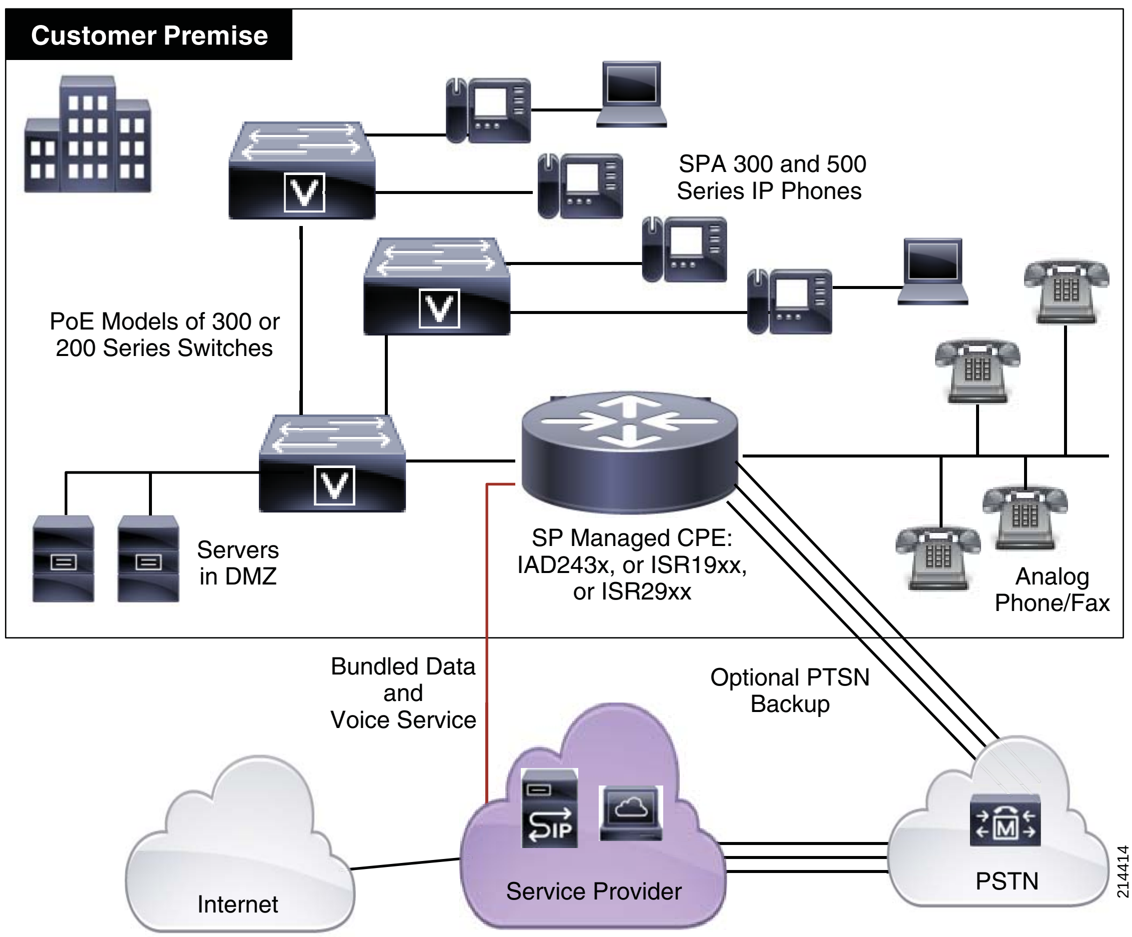
For 51 to 100 Phones Including Reliable PSTN Backup

If customers require reliable PSTN backup, if there is a need to use a T1/E1 as the WAN connection, or if the customer wants to deploy more than 50 phones, the HSB Communications solution with the Cisco IAD243x Series device or Cisco ISR19xx/29xx series router is recommended. The ISR19xx/29xx and Cisco IAD243x Series have a VIC slot option. One VIC slot can be used to provide PSTN backup using either four FXO lines, two BRI lines, or one to two T1/E1 PRI lines.

Note For IAD243x series, the VIC slot for PSTN backup is available only in the Cisco IAD2431 and IAD2432.

Figure 4 shows the HSB Communications solution for more than 50 phones, which is deployed using a Cisco IAD243x Series device and two to three Cisco Small Business 300 Series PoE switches. Because this is a large deployment, a two-layer LAN infrastructure with an aggregation switch and two or more access switches is recommended.

Figure 4 HSB Communications Solution for More than 50 Phones with Reliable PSTN Backup



This concludes the broad overview of deployment options. The next section provides the details of the components of the Cisco HSB Communications solution, to help SPs select the right models of each component.

Solution Provisioning Options

Cisco SPA Series IP Phones are provisioned by receiving an XML-formatted configuration file from the provisioning server located in the SP network. This mechanism provides the SP with centralized control and easy mass provisioning. It is accomplished by the DHCP server hosted on the WAN termination device. The following DHCP options are available:

- DHCP Option 66—Provides the TFTP server address
- DHCP Option 159—URL based on the IP address of the provisioning server, which is hosted in the SP network
- DHCP Option 160—URL based on the hostname of the provisioning server, which is hosted in the SP network

For more details about these options, which enable SPs to easily execute mass provisioning of Cisco SPA IP Phones, see DHCP Options for Voice VLAN.

Solution Components

The Cisco HSB Communications solution has three major hardware components:

- WAN termination CPE device
- Voice-ready LAN infrastructure using Cisco 300 or 200 Series switches
- Cisco SPA Series IP Phones

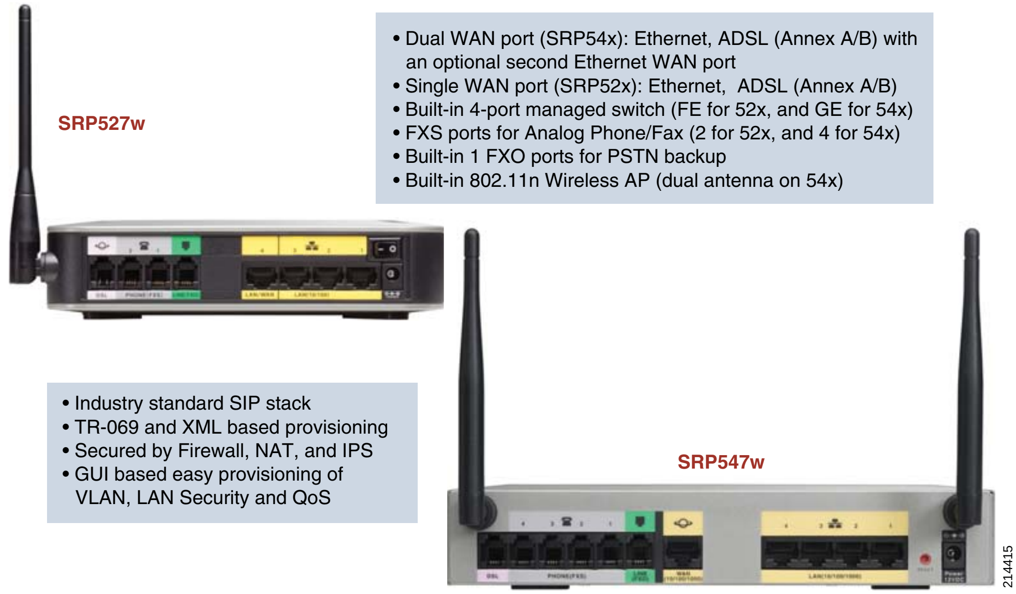
This section describes the various models available for each component to help the SP select the best option for a specific deployment:

- WAN Termination CPE, page 7
- LAN Infrastructure, page 10
- IP Phones, page 12

WAN Termination CPE

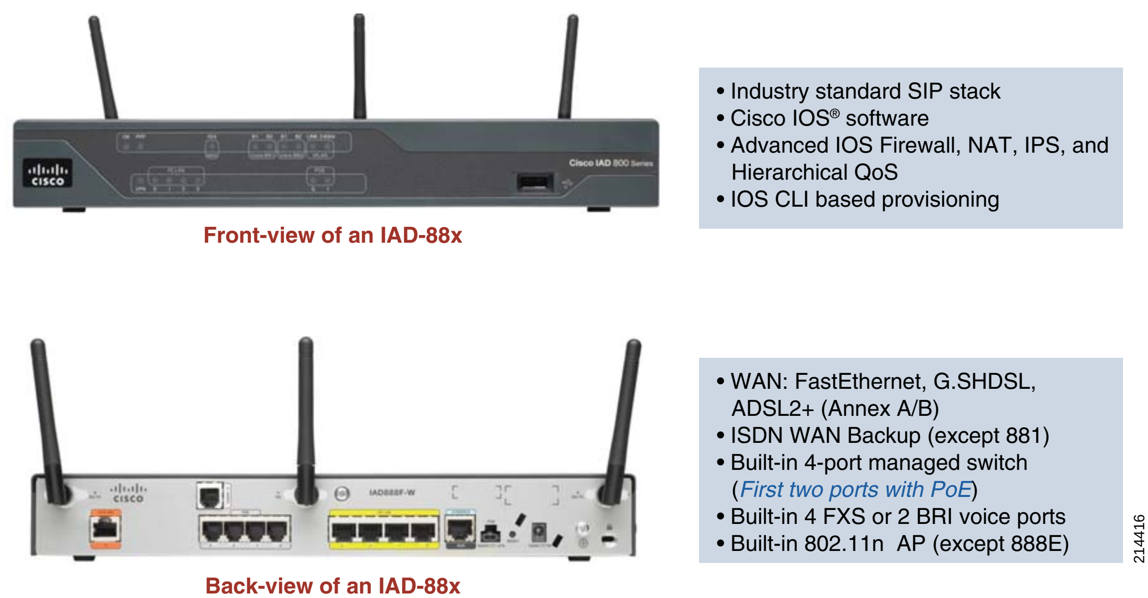
The selection of the WAN termination edge device (Cisco SRP, IAD or ISR) is based on the number of phone lines required, the WAN connection type, and the PSTN backup requirement. Figure 5 summarizes the key features and capabilities of a Cisco SRP Series CPE.

Figure 5 Cisco Small Business CPE SRP500 Series



Both IADs are and ISRs are Cisco IOS Software-based routers. IAD88x and ISR8xx are fixed hardware configuration platforms. Figure 6 summarizes the key features and capabilities of the Cisco IAD88x Series.

Figure 6 Cisco IAD88x Series devices

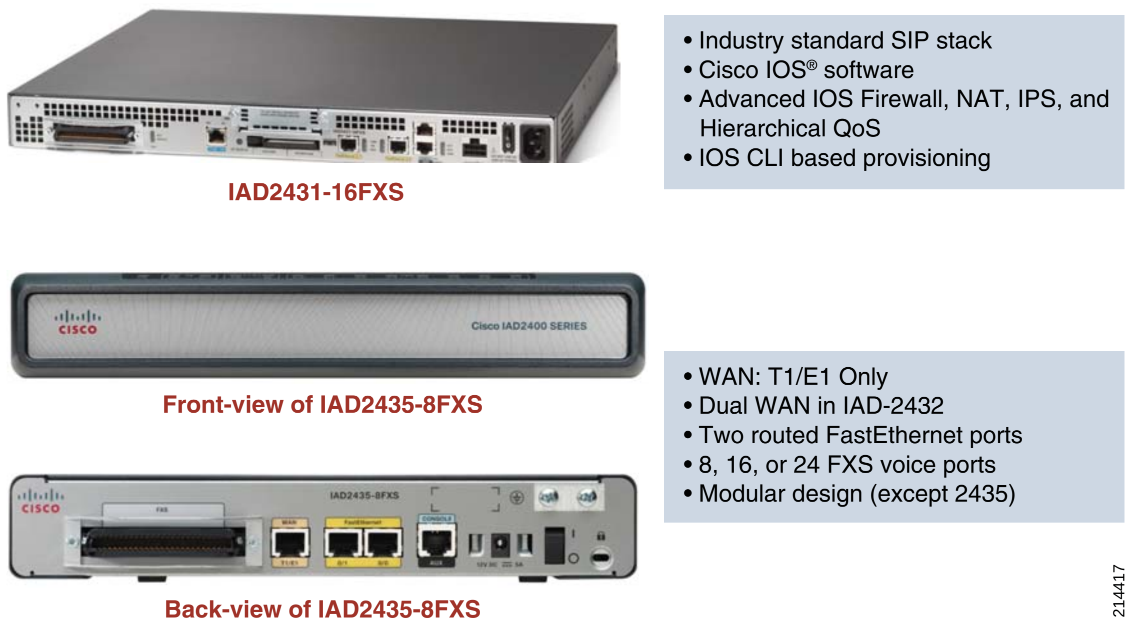


The Cisco ISR8xx Series provides multiple fixed configuration options depending on the choice of LAN switchports, primary WAN, and backup WAN and so forth. For details see the following website: http://www.cisco.com/go/isr.

Note Although the Cisco SRP52x, IAD88x Series and ISR8xx series are capable of providing 802.11n wireless LAN services, this document does not focus on wireless deployments and therefore does not describe these features.

The Cisco IAD243x and ISR19xx/29xx Series are modular platforms with one or more VWIC slots to add either a WAN or PSTN connection. In the HSB Communications solution, at least one VWIC slot is used to provide a PSTN backup connection by using either a four-FXO, two-BRI voice or one to two T1/E1 cards. Figure 7 summarizes key features of the Cisco IAD243x Series.

Figure 7 Cisco IAD243x Series for 51 to 100 Phones



Cisco ISR19xx series, ISR2901, and ISR2911 are modular platforms with multiple hardware configuration options. For details, see the following website: http://www.cisco.com/go/isr

Note For IADs, the VIC slot for PSTN backup is available only with the IAD2431 and 2432 Series.

Table 1 lists various customer scenarios and suggests appropriate WAN termination devices for the HSB Communications solution. Note that these are broad guidelines only. Hardware configuration may change because of specific customer requirements. For configurations of ISR routers, visit www.cisco.com/go/isr

Table 1 Selecting WAN Termination Device for the HSB Communications Solution

Number of Phones	Analog Stations	PSTN Backup	WAN Connection	CPE Device
0–10	2 FXS	1 FXO (relay)	10/100 Mbps Fast Ethernet	Cisco SRP521W
0–10	2 FXS	1 FXO (relay)	ADSL2+ (Annex B)	Cisco SRP526W

Table 1 Selecting WAN Termination Device for the HSB Communications Solution

Number of Phones	Analog Stations	PSTN Backup	WAN Connection	CPE Device
0–10	2 FXS	1 FXO (relay)	ADSL2+ (Annex A)	Cisco SRP527W
11–50	4 FXS	1 FXO (relay)	10/100/1000 Mbps Gigabit Ethernet	Cisco SRP541W
11–50	4 FXS	1 FXO (relay)	ADSL2+ (Annex B)	Cisco SRP546W
11–50	4 FXS	1 FXO (relay)	ADSL2+ (Annex A)	Cisco SRP547W
11–50	4 FXS	None	10/100 Mbps Fast Ethernet	Cisco IAD881F-K9
11–50	4 FXS	None	ADSL2+ (Annex B)	Cisco IAD886F-K9
11–50	4 FXS	None	ADSL2+ (Annex A)	Cisco IAD887F-K9
11–50	4 FXS	None	G.SHDSL	Cisco IAD888F-K9
11–50	4 FXS	None	Ethernet over Copper	Cisco IAD888EF-K9
51–100	8 FXS	None	One T1/E1	Cisco IAD2435-8FXS
51–100	8 FXS	4 FXO/2 BRI	One T1/E1	Cisco IAD2431-8FXS
51–100	16 FXS	4 FXO/2 BRI	One T1/E1	Cisco IAD2431-16FXS
51–100	24 FXS	4 FXO/2 BRI	Two T1/E1	Cisco IAD2432-24FXS

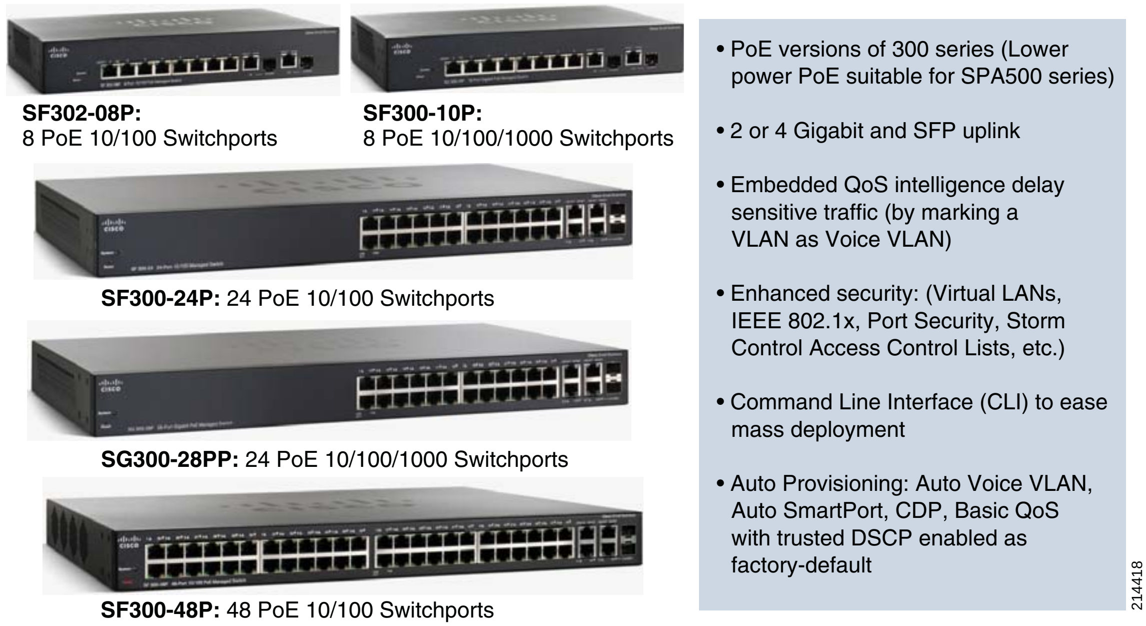
Note All Cisco IAD88x Series devices have BRI options instead of FXS. To order an IAD88x with two BRI ports for digital stations instead of four analog stations, replace the *F* by a *B* in the part number.

Note ISR routers have multiple options from which to choose. The 800 Series ISRs have fixed hardware configurations, and only the ISR88x-SRST has FXO ports for PSTN backup. The ISR19xx and ISR29xx Series are modular platforms, which can be configured using hosts of available voice and data modules. To learn more, and to configure an ISR hardware configuration for your customer, visit http://www.cisco.com/go/isr.

LAN Infrastructure

The LAN infrastructure of the HSB Communications solution is based on the Cisco Small Business 300 or 200 Series PoE switches. Figure 7 shows the recommended 300 Series switch models:

Figure 8 Cisco Small Business 300 Series PoE Switches



Cisco Small Business 300 and 200 Series switches provide CDP, Auto Voice VLAN using VSDP, and Auto Smartport features, which greatly reduce the configuration time. The switch comes with CDP, Auto Smartport mode, Auto Voice VLAN, and Basic QoS with trusted DSCP enabled, by default. This makes it very easy to configure complex QoS and security settings.

Note Among the 200 Series Small Business switches, the SG200-08P, SF200E-24P, and SF200E-48P do not support the VSDP and Auto Smart Port features but may be manually configured to be voice ready.

Selection of the switch for a Cisco HSB Communications solution is affected by the number of users and type of phones. Cisco recommends using Cisco Small Business switches that come with inline power. PoE is a 48-volt DC power supply capability provided over standard Ethernet. PoE switch selection is determined by the number of users and type of phones. The PoE budget plays an important role in selection.

Cisco Small Business PoE switches support the IEEE 802.3af PoE standard. An IEEE 802.3af standard PoE port can supply up to 15.4 watts maximum. Cisco SPA IP Phones are class-2 PoE devices, which require less than 7 watts of power. Table 2 shows the PoE budget (Total PoE power in Watts) for all SBCS-supported PoE switches.

Table 2 PoE Budget (in Watts) and Number of PoE Ports for Cisco Small Business PoE Switches

PoE Ports	FastEthernet Models (PoE Budget)	GigabitEthernet Models (PoE Budget)
8	SF302-08P (62W) SF302-08MP (124W)	SG300-10P (62W) SG300-10MP (124W)
12	SF200-24P (100W)	SG200-26P (100W)

Table 2 PoE Budget (in Watts) and Number of PoE Ports for Cisco Small Business PoE Switches (continued)

PoE Ports	FastEthernet Models (PoE Budget)	GigabitEthernet Models (PoE Budget)
24	SF300-24P (180W) SF200-48P (180W)	SG300-28P (180W) SG200-50P (180W)
48	SF300-48P (375W)	n/a

As shown in Table 2, only half of the switch ports on the Cisco 200 Series Smart Switches provide PoE. On a 24-port Cisco 200 Series, switch ports 1–6 and 13–18 are PoE ports. On a 48-port Cisco 200 Series switch, 1–12 and 25–36 are PoE ports. Cisco recommends using these switches with only class-2 PoE devices because of their low PoE budget, so that all the PoE switchports can be simultaneously used to connect IP phones. When using class-3 PoE devices, such as access points, either use fewer ports on these switches or use Max-Power (MP) models. Please note that switches supplying a higher PoE budget and/or with Gigabit Ethernet ports are more expensive than those providing lower budget PoE and FastEthernet ports.

IP Phones

The HSB Communications solution uses the Cisco Small Business SPA IP Phones. Phones range from single-line utilitarian models to multi-line models with high-resolution color displays capable of displaying low-motion video with BlueTooth support. All phone models support up to two 32-button attendant consoles (also known as sidecars). Table 3 compares the features provided by Cisco Small Business IP Phones.

Table 3 Cisco Small Business SPA300 and SPA500 Series IP Phones

IP Phone	Line Keys	Color Display	Attendant Console	PoE 802.3af	PC Switch Port	Wideband Audio G.722
Cisco SPA301	1	n/a	Y	N	N	Y
Cisco SPA303	3	N	Y	N	Y	Y
Cisco SPA501G	8	n/a	Y	Y	Y	Y
Cisco SPA502G	1	N	Y	Y	Y	Y
Cisco SPA504G	4	N	Y	Y	Y	Y
Cisco SPA508G	8	N	Y	Y	Y	Y
Cisco SPA509G	12	Y	Y	Y	Y	Y
Cisco SPA525G	5	Y	Y	Y	Y	Y

Note the following:

- The Cisco SPA501G uses paper labels to mark speed dials or extensions.
- All SPA500 Series IP Phones can be powered by PoE. If connected to a non-PoE switchport, use a 5V/2A power adapter; part number *PA100-XX*, where *XX* stands for the specific region (NA, UK, EU, and AU). This part is included and shipped with the SPA300 Series IP Phone.
- Even though the SPA525G2 is capable of Wi-Fi and Bluetooth, this document does not focus on wireless deployments and therefore does not describe these wireless features.

LAN Design

The HSB network design addresses the small business requirements for a secure network infrastructure. The concepts presented in this document are intended to provide a general understanding of the following topics:

The network design implements the LAN, WAN, and integrated security services, and lays the foundation for secure data and robust voice communication services. The components of the Cisco HSB Communications solution have built-in capabilities for a secure network, with factory-default configuration appropriate for many small businesses. If additional configuration is required, it can be easily accomplished using smart configuration techniques with the browser-based provisioning tool provided.

This section describes recommended design for the LAN in an HSB solution, and includes the following topics:

- General Design, page 13
- VLAN Design, page 13
- Spanning Tree Protocol, page 15
- SmartPort Roles, page 15
- Power over Ethernet, page 15

General Design

For larger deployments, LAN designs consist of core, distribution, and access layers. Each layer has a different set of switches to serve a distinct purpose. For smaller deployments, the core and distribution layers are often collapsed into one layer, known as the aggregation layer, which can be a separate switch or an integrated switch in a router device. LAN designs are typically deployed in one of the three following ways:

- Layer 2 switching between all layers
- Layer 3 routing between core and distribution layers, and Layer 2 switching between distribution and access layers
- Layer 3 routing between all layers

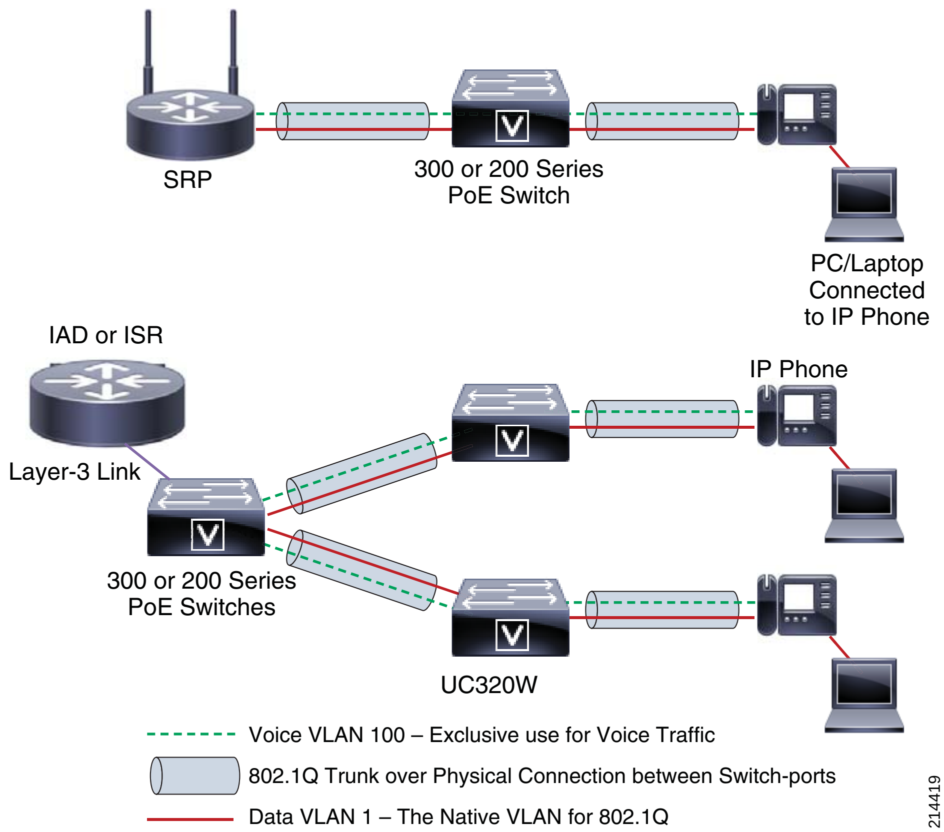
The LAN design used in the HSB Communications solution consists of Layer 2 switching, mainly because of its simplicity. This design, regardless of the number of users supported, contains no redundant components, and uses a loop-free Layer 2 topology. For ten or less users using the Cisco SRP52x Series, Cisco recommends using one switch connected to one of the integrated switchports. For 11 to 50 users using the Cisco IAD88x or ISR8xx Series, one to two switches can be connected to integrated non-PoE switchports (the other two switchports are PoE ports). For 51 to 100 users using the Cisco IAD243x Series or ISR19xx/29xx series, one small aggregation switch and two to three access switches are used.

VLAN Design

All components used in the HSB Communications solution support VLANs, which are logical connections that enable groups of devices, such as PCs, desktops, and IP phones, to communicate as if they were connected to the same physical wire even though they might be connected to completely different LAN switches. In the HSB Communications solution, VLANs are used to group voice devices on the voice VLAN (assigned the value of 100, by default) and to group data devices on the data VLAN (assigned the value of 1, by default).

In contrast to large Unified Communications network designs, the HSB Communications design uses only two VLANs. This makes it simplifies separation of the two types of devices, as well as other tasks, such as Dynamic Host Configuration Protocol (DHCP) server administration and IP addressing. Figure 9 shows the Layer 2 characteristics of the LAN design.

Figure 9 Layer 2 LAN in the HSB Communications Network Design



One benefit of using IEEE 802.1q trunking on Cisco IP phones is that it permits PC access via an IP phone port. Cisco SPA Series IP phones with a PC port have a built-in three-port switch and the function of each port is as follows:

- One port is invisible and is used internally for IP phones using the voice VLAN
- One port is used to connect a PC using the data VLAN
- One port is used to connect the IP phone to a switch using an IEEE 802.1q trunk.

With this setup, no switchport is lost when an IP phone is added to a switch. The PC that is to be connected to the switch can be connected to the network using the access port provided by the IP phone.

Spanning Tree Protocol

Layer 2 devices use the Spanning Tree Protocol (STP) to help them dynamically discover loops in the network and block them. STP is not strictly required in the HSB Communications design because no physical loops exist. However, STP is used as a precautionary measure to prevent any issues if two switches are connected together with two separate cables. STP provides the following capabilities:

- Fast convergence using IEEE 802.1w or Rapid STP (RSTP), which is enabled by default
- PortFast or fast-start feature, supported for all SmartPort roles, as described later in this document

SmartPort Roles

SmartPort roles are Cisco-verified feature templates based on the type of device (such as desktops, IP phones, servers, and switches) that are connected to the switchports. These templates require only minimal effort and expertise to consistently and reliably configure essential Layer 2 switching, security, PoE for IP phones, and Quality of Service (QoS), which is explained later in this document. These templates also simplify the configuration process by reducing redundant command entries and preventing problems caused by switchport misconfiguration. SmartPort roles can be selected from a drop-down menu in a GUI-based provisioning application. The SmartPort role reflects the type of device to be connected, such as switch, router, desktop, IP Phone+Desktop, access point, and so on.

Power over Ethernet

Cisco Small Business 300 and 200 series PoE switches support the IEEE 802.3af PoE standard. PoE is a 48-volt DC power supply capability provided over standard Ethernet unshielded twisted pair (UTP) cable. Instead of using wall power, IP phones and other inline-powered devices, such as wireless access points, can receive power via an Ethernet connection. PoE is delivered on the same wire pairs used for data connectivity (pins 1, 2, 3, and 6). Deploying inline power-capable switches that are powered with an uninterruptible power supply (UPS) helps ensure that all devices remain operational during power failures and that IP phones can still make and receive calls. The HSB Communications design described in this document recommends Cisco 300 and 200 switches with inline power. A PoE port can supply up to 15 watts (IEEE 802.3af standard) maximum, though many SPA Series IP Phones require no more than 7 watts.

WAN Design

WANs are based on various access technologies and provide various levels of services. Some WAN connections provide guaranteed bandwidth and quality based on service-level agreements (SLAs), such as MPLS VPN, Metro Ethernet, and T1/E1 access. Other WAN options are comparatively cost-effective, but provide only best-effort services, such as cable and xDSL.

The WAN termination device is selected based on the available WAN access method at the customer premises. In a small deployment, basic WAN design is entirely dependent on the service parameters provided by the Internet service provider. QoS on the WAN connection, as well as other parameters to preserve voice call quality such as Call Admission Control (CAC) and Link Fragmentation and Interleaving (LFI) are discussed later in this document.

Layer 3 Design

The Layer 3 design for an HSB solution provides the capabilities necessary to forward traffic between Layer 2 switching segments or VLANs, and between the LAN and WAN. Layer 3 designs consist of several components, including IP addressing, NAT, and IP routing. The following topics cover each of these components and describes how they are deployed:

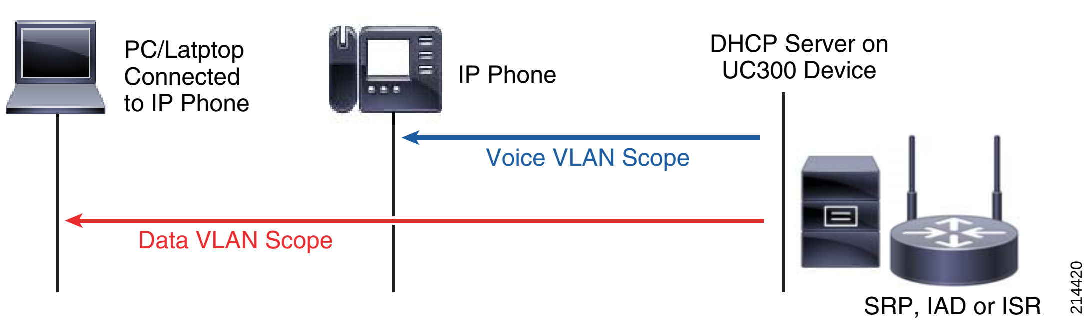
- IP Addressing, page 16
- DHCP Options for Voice VLAN, page 17
- Domain Name System, page 19
- Network Address Translation, page 19
- IP Routing, page 21
- Network Time Protocol, page 21

IP Addressing

The Cisco HSB Communications solution uses IPv4 addressing. IP addresses can be assigned by either a static or a dynamic method. If the static method is used, a network administrator or service provider assigns specific addresses to devices. This method is recommended for a network resource (for example, an e-mail server or a switch) that must maintain a consistent address because it is offering services to other devices.

If the dynamic method is used, DHCP assigns IP addresses to devices as they are needed. This simplifies the administration of IP addresses because they do not need to be statically assigned to endpoints. For example, DHCP allows users to move their devices, such as laptops, to different locations without having to manually change the IP address of the device. DHCP also helps conserve IP addresses because they can be reallocated if an endpoint no longer needs an IP address. In addition to IP addresses, DHCP can deliver other network information, such as a default gateway, a subnet mask, and server addresses, to reduce configuration effort and time. Figure 10 shows the DHCP server running on the Cisco CPE device.

Figure 10 DHCP Server Running on the Cisco SRP, IAD or ISR



LAN interfaces, switchports, and servers are assigned static IP addresses because other devices rely on them for services such as e-mail, Internet access, and default gateway routing. The remaining endpoints, such as PCs, desktops, and IP phones, are assigned dynamic IP addresses from the DHCP pools on the data or voice VLAN.

The Cisco SRP, IAD or ISR device provides the DHCP service in the IP addressing design. The DHCP server running on the SRP, IAD or ISR is configured with the address ranges for the data VLAN and voice VLAN. The DHCP server also provides a default gateway IP address to the endpoints. Some addresses are excluded from the dynamic address range of the DHCP server, because they are statically assigned to the SRP, IAD or ISR itself, additional switches, and servers, and therefore must not be assigned to other devices.

Table 4 provides the IP addressing scheme used in this design. IP addresses under data VLAN 1 and voice VLAN 100 are preconfigured on the Cisco SRP500 Series devices, and the same are configured manually on the IAD devices and ISR.

Table 4 IP Addressing Scheme in the HSB Communications Solution

Description	IP Address	Assignment Method
WAN interface of the CPE device	Dynamic or static	From ISP
Data VLAN (1)	192.168.15.1/24	Static
Voice VLAN (100)	192.168.100.1/24	Static
Servers and Cisco 300 or 200 series switches	192.168.15.1–192.168.15.99	Static
Data endpoints	192.168.15.100–192.168.15.254	Dynamic
Voice endpoints	192.168.100.100–192.168.100.254	Dynamic

DHCP Options for Voice VLAN

Cisco SPA IP Phones are provisioned by receiving an XML-formatted configuration file from the provisioning server. This file is unique to an IP Phone, with its name based on the MAC address of the IP Phone. There are two ways to receive the XML-formatted phone configuration file:

- Using an intermediate CFG file from the WAN termination device. This file contains the information about how to get the phone configuration file from a provisioning server. One CFG file is required for each phone model in the customer network. DHCP option 66 is used to provide the TFTP server address running on the WAN termination device.
- Using the URL of a provisioning server hosted in the SP network. The WAN termination device provides either an IP address based on this URL using DHCP option 159, or a hostname based on this URL using DHCP option 160.

Using DHCP Option 66

To use DHCP option 66, the following files are required:

- XML-formatted phone configuration files for each phone on the provisioning server in the SP network
- CFG files for each phone type, provided by the TFTP server on the WAN termination device

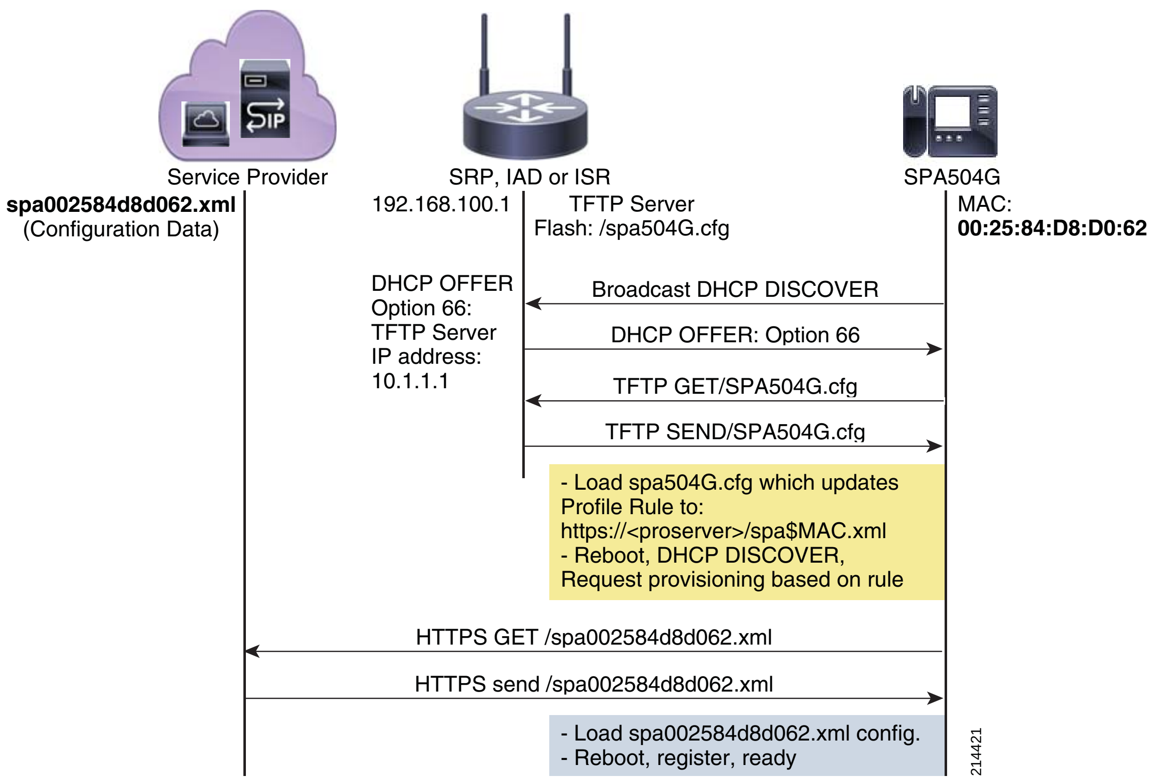
Cisco SPA IP phones rely on a TFTP server to acquire configuration information, which is in a configuration file that is unique to each IP phone. In the HSB Communications solution, the files for Cisco SPA IP phones are assigned a name based on the MAC address of the SPA IP phone. For example, an SPA IP phone with the MAC address *ABCDEF123456* would be associated with a file named *spaABCDEF123456.xml*. This file resides in the provisioning server located in the SP data center. The system administrator at the SP data center creates this file as part of service provisioning.

When a SPA IP Phone is powered up by connecting to the HSB Communications network at the customer location, it gets its IP address from the SRP, IAD, or ISP device with option 66 (TFTP server address) for the SRP, IAD or ISR device itself. Configuration files specific to the SPA IP Phone model are stored in the SRP, IAD or ISR.

For example, for the Cisco SPA501G, the name of this file will be spa501.cfg. This file provides the IP address of the provisioning server and authentication details. Phones get this file from the SRP, IAD, or ISR, and then send the request to the provisioning server for its unique configuration file in XML format.

Figure 11 shows the mechanism of the SPA IP Phone provisioning using DHCP option 66 for TFTP.

Figure 11 SPA IP Phone Provisioning with DHCP Option 66 for TFTP

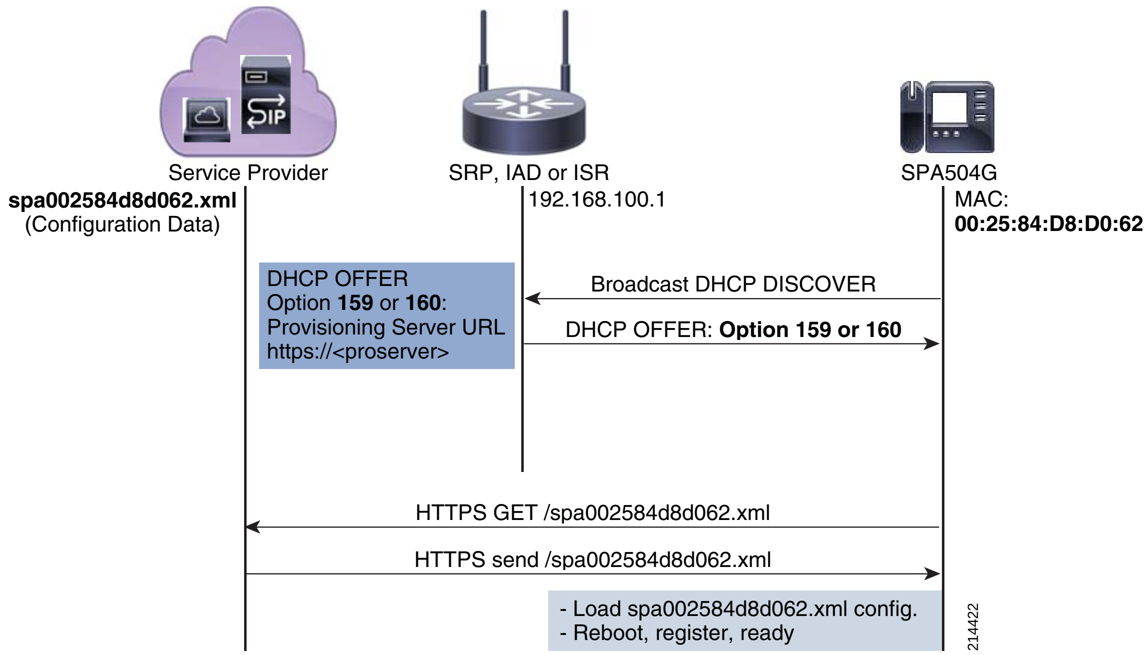


Using DHCP Option 159 or 160

To use DHCP option 159 or 160, XML-formatted phone configuration files for each phone on the provisioning server in the SP network are required.

When a SPA IP Phone is powered up by connecting to the HSB Communications network at the customer location, it gets its IP address from the SRP, IAD. or ISR device with option 159 or 160 (IP address or hostname) for the provisioning server. The IP Phone then sends a request to the provisioning server for its unique configuration file, which is in XML format. This is an efficient provisioning mechanism that will be the preferred method for future releases of the HSB Communications solution. Figure 12 shows the mechanism of the SPA IP Phone provisioning using DHCP option 159.

Figure 12 SPA IP Phone Provisioning with DHCP Option 159



Domain Name System

The domain name system (DNS) is used on the Internet and in intranets for translating host names of network devices into IP addresses. Host names, such as *www.cisco.com*, are typically easier to remember than IP addresses. In the HSB design, as in many other small business networks, an ISP provides the DNS service. The factory defaults for SRP500 Series devices configures DHCP for the data VLAN to import DNS services from an ISP-provided DNS server. The HSB design also uses this DNS/DHCP configuration on Cisco IOS software-based IAD and ISR Series, assuming that no DNS server is installed on the small business premises.

Network Address Translation

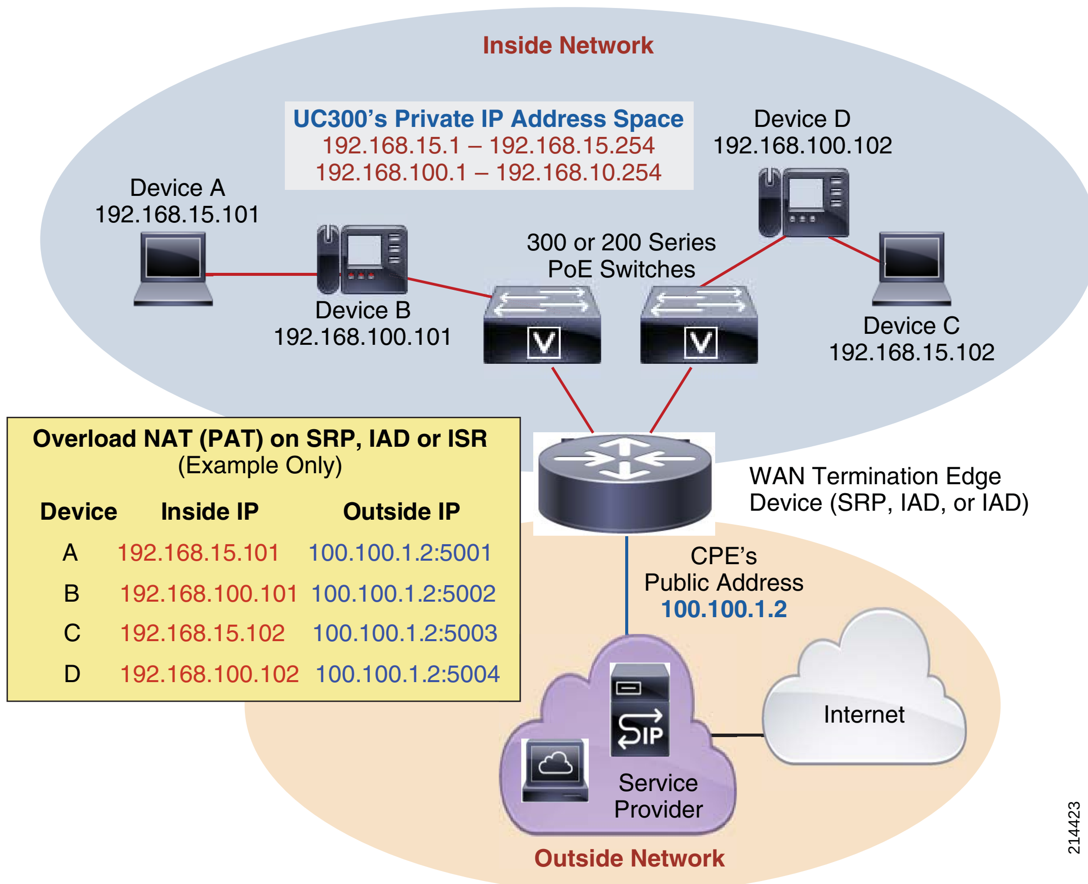
Network Address Translation (NAT) converts a private IP address (defined by RFC 1918) to a public IP address that is recognized and routable on the public Internet. NAT allows devices connected to private (inside) IP networks to communicate with the public (outside) Internet.

The three types of NAT are as follows:

- Static NAT—Static one-to-one mapping
- Dynamic NAT—Dynamic one-to-one mapping using address pools
- Overload NAT, often referred to as Port Address Translation (PAT)—Dynamic one-to-many mapping of multiple private IP addresses to one public IP address

NAT can be used on any device that connects two networks to translate the private address space into the public address space. For example, if a customer uses the IP address range 192.168.15.0/24 for devices on a private network, for external communication, the customer must use NAT to translate these addresses into an IP address or range of IP addresses that are registered for use on the public Internet. The HSB Communications solution uses overload NAT to simplify addressing and conserve addresses and reduces the customer requirement for a large number of publicly registered IP addresses. Figure 13 shows NAT operations in the HSB Communications solution.

Figure 13 Network Address Translation in the HSB Communications Solution



Typically, the customer is given a single public IP address, assigned to the WAN interface of the edge device (SRP, IAD or ISR), and is unique on the Internet. When devices on the private network access the Internet, the edge device translates the IP address of the internal device into this external IP address and assigns a specific port number to this translation. The port number helps the edge device identify which translation is mapped to the internal device.

Note Static NAT is required if a customer has a DMZ that provides host servers for external users. Although DMZs can be provisioned on the edge device, they are not discussed in this document.

IP Routing

The HSB Communications design is intended for small deployments without redundant paths to the Internet, so routing protocols are not necessary for this design. Because there is a single entry and exit point to the SP via the designated WAN interface of the CPE device, a simple static default route is sufficient to forward traffic to the Internet. For internal traffic, routing protocols are not necessary because the CPE device is directly connected to every Layer 2 VLAN within the design, and serves as the default gateway for each VLAN.

Network Time Protocol

Network Time Protocol (NTP) is a standard protocol built on top of TCP/IP that helps ensure accurate local time synchronization within a network that consists of routers, switches, and other devices. A master source maintains the time and is typically a radio or atomic clock located on the Internet.

NTP can synchronize distributed clocks within milliseconds over long time periods. NTP is critical in any network because it helps ensure that all devices have accurate and synchronized time stamps. This is especially important if the network contains IP communications components, which require time synchronization to function properly. NTP also helps ensure that network events and error messages, as well as security logs, traces, and system reports, contain accurate time information that helps when troubleshooting and managing the network. Additionally, NTP is important for collecting call detail records and generating billing reports. This guide recommends using one of the master clocks on the Internet as an NTP server. If this is not an option, use the CPE device (or SIP proxy or provision server) as the NTP master.

Quality of Service

This section describes the role that Quality of Service (Qos) plays in an HSB solution, and includes the following topics:

Basic QoS Concepts

This section introduces some fundamental QoS concepts. QoS provides the ability of a network to supply differentiated services to different types of network traffic over various underlying technologies such as DSL, cable, Frame Relay, ATM, and Ethernet. QoS delivers improved and more predictable network service by providing the following:

- Dedicated bandwidth support for specific types of traffic
- Improved traffic loss characteristics
- Network congestion avoidance and management techniques
- Traffic shaping to smooth intermittent bursts
- Traffic prioritization across a network

QoS can be used in both the LAN and the WAN. If the WAN connection sends and receives voice traffic, QoS must be configured to provide a certain amount of dedicated bandwidth and to prioritize voice over other types of traffic.

As traffic enters the network, QoS classifies and marks it for appropriate treatment. Common methods to differentiate traffic are Layer 2 class of service (CoS) or IEEE 802.1p, Layer 3 type of service (ToS), or Layer 3 differentiated services code point (DSCP). Each port on a network device has a series of input and output queues: input queues for ingress (inbound traffic), and output queues for egress (outbound traffic). Queues are temporary storage areas for data, and the amount assigned for a queue (that is, temporary storage) is known as a buffer.

Data waits in input queues before it can be taken in for switching, or it waits in output queues before it can be transmitted out. When a frame arrives at a port during congestion, it is placed into an RX (input) queue. The CoS value in the Ethernet header of the incoming frame determines into which queue the frame is placed.

On egress, a scheduling algorithm is used to empty the TX (output) queue. For each TX queue, a weighting is used to dictate how much data is emptied from the queue before moving on to the next queue. The weighting for each TX queue is assigned a number from 1 to 255.

During traffic congestion, packets may be dropped. TCP retransmission can then make congestion even worse, which results in buffer overflow. To avoid this situation, QoS assigns threshold values to each queue. Thresholds are configurable levels that define utilization points at which the congestion management algorithm can start dropping data from the queue.

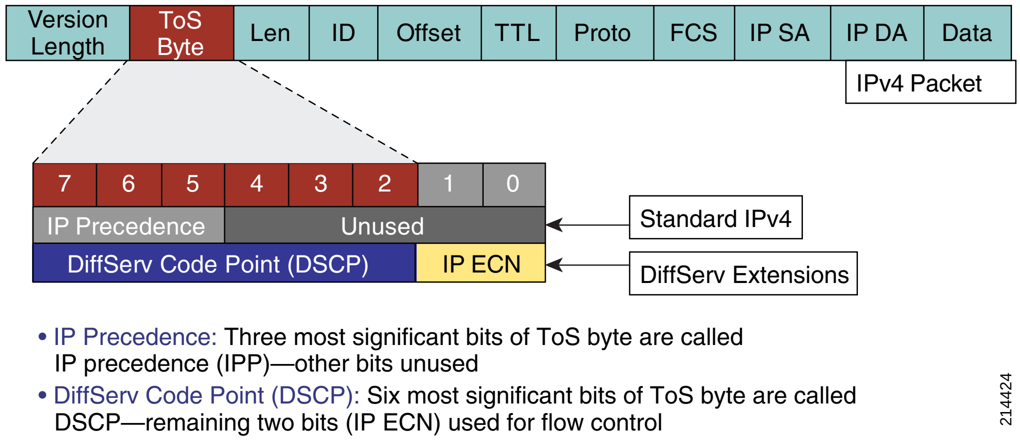
In the context of QoS, frames are assigned with different priorities based on CoS and are mapped to these thresholds. As the buffer begins to fill and thresholds are exceeded, the frames identified by CoS to threshold mapping are dropped. This mapping can be used to determine the thresholds at which frames with specific CoS values can be dropped (default), and the queue into which a frame is placed, based on its CoS value (default).

QoS policy (mapping) can override these default policies as follows:

- CoS values on an incoming frame to a DSCP value
- IP precedence values on an incoming frame to a DSCP value
- DSCP values to a CoS value for an outgoing frame
- CoS values to drop thresholds on receive queues
- CoS values to drop thresholds on transmit queues
- DSCP markdown values for frames that exceed policing statements
- CoS values to a frame with a specific destination MAC address

Figure 14 illustrates IP precedence, DSCP, which is a 5-bit value in the 1-byte ToS field in the IPv4 header, and ToS.

Figure 14 QoS Uses the Type of Service (ToS) Field of IPv4



LAN QoS

To ensure that voice traffic receives the necessary QoS, the features described in this section must be enabled and configured on each Ethernet port to which a Cisco IP Phone is connected.

- **Virtual Local Area Network (VLAN)**—A VLAN is a virtual network that segments different types of traffic and users; and is identified through a Port VLAN ID (PVID), such as 1, 10, 12, and so on. When adding voice to a network, a separate VLAN should be added to the network for the voice traffic.

  A voice VLAN has higher quality requirements than a standard data network.

- **PortFast**—Allows a device such as an IP phone to connect or disconnect to the network quickly, which helps with adding and removing devices on the network.
- **Bridge Protocol Data Unit (BPDU) Guard**—BDPU Guard prevents hackers from changing from one VLAN to another without authorization, helping to secure the network.
- **Storm Control**—Helps to prevent storms on the network; storms are an unusual burst of traffic that can impede business processes on the network, including voice.
- **Port Security**—Stops users from adding unauthorized devices to the network, which helps to keep unwanted applications off the network, including viruses, worms, and so on.
- **Quality of service (QoS)**—Helps to ensure that applications such as voice get through the network with limited interruptions. This helps to ensure the quality of the voice call being made on the network. When setting up QoS on the network, the following specific features should be enabled or customized:
  - Class of service (CoS)—Used within an Ethernet network to set the priority of the traffic traversing that network. CoS helps to ensure the quality of the voice calls on the Ethernet network.
  - Differentiated Service Code Point (DSCP) classification—Classifies packets across a network to provide guaranteed service for specific packets, such as voice packets. DSCP ensures voice quality across the entire network.

- Access control list (ACL)—Create security policies for your business; such policies may include who has access to specific servers, and securing your business from the Internet.
- Priority processing (queuing and scheduling)—Helps to manage the traffic flowing through the network by organizing which traffic has precedence, ensuring that sensitive traffic such as voice gets through the network first.

  To simplify the configuration of the necessary features, Cisco Small Business devices (ESW500, IAD, and SRP) are provided with templates for the recommended security and QoS configuration. These templates are based on the role of device in the network, such as IP phone, access point, and so on. These templates are known as macros (for Cisco IOS-based IADs) and SmartPort roles for Cisco ESW500 and SRPs.

- **Hardware queues**—The templates automatically map the CoS and DSCP values to specific queues and set the round-robin queuing allocations for the switchports. For example, if the IPPhone+Desktop SmartPort role is assigned to a switchport, voice traffic from the IP phone is always prioritized over the data traffic from the connected desktop device. The voice traffic is then sent to one of four available hardware queues within the switchport of the device. This queue is provisioned with a specific amount of dedicated bandwidth that is available only to voice traffic. The other three queues share the remaining bandwidth in a round-robin fashion for other data traffic.

WAN QoS

In most networks, the connection between the integrated switchports in the LAN is typically 10, 100, or 1000 Mbps, and the upstream bandwidth of the WAN connection generally ranges from 512 Kbps to 3.0 Mbps. As a result, the CPE device must often process more traffic from the LAN than it can send on the WAN, and the WAN interface becomes congested because it cannot handle all the traffic coming upstream from the LAN. Without QoS on the WAN of the CPE device, critical outgoing traffic such as routing, VoIP signaling, and real-time voice traffic suffers. Congestion is not an issue with downstream traffic received from the WAN because the LAN has more than enough bandwidth to handle the incoming traffic, for which WAN downstream bandwidth generally ranges from 1.5 Mbps to 10 Mbps. To prevent congestion of outgoing traffic on the WAN interface, specific traffic classes must be designed and assigned an adequate amount of bandwidth to each class to help ensure that all traffic is provided with the necessary QoS. When VoIP is used in the network, special low latency queuing (LLQ) must be provisioned. The LLQ is designed to prioritize voice-bearer traffic (RTP packets) over other types using expedited forwarding (EF) to help prevent delay, jitter, and packet retransmissions. Voice-signaling traffic (SIP packets) requires special treatment, as well, but is not as delay-sensitive as is voice-bearer traffic. Therefore, voice signaling is allocated to a class-based weighted fair queuing (CBWFQ) with assured forwarding (AF). Finally, all other data traffic is assigned to the remaining CBWFQ, but is provided with only best-effort service.

If this priority treatment is applied to the whole WAN bandwidth, other data traffic types such as e-mail, HTTP, and other business applications are unable to communicate. Therefore, a designer must allocate an appropriate amount of bandwidth for such traffic. By reserving either a percentage or a specific amount of bandwidth, the priority mechanism works within the reserved part of bandwidth, leaving the unreserved bandwidth as free for every type of data traffic. Table 5 lists the traffic classes and suggested bandwidth allocations used in this design.

Table 5 Traffic Classes and Suggested Bandwidth Provisioning for the WAN

Traffic Class	Description	IP Precedence/ DSCP	Per Hop Behavior (DSCP-Based)	Queuing Type	Bandwidth Guarantee
Real time	Voice bearer (RTP packets)	CS5/EF	Expedited forwarding	Priority queuing	Certain percentage of upstream bandwidth
Signaling	Voice signaling (SIP packets)	CS3/AF31	Assured forwarding	CBWFQ	Low amount such as 10 kbps
Routing	Routing, other critical traffic	CS6	Assured forwarding	CBWFQ	Low amount such as 10 kbps
Best-effort	Data traffic	0, 1, 4	Best-effort	CBWFQ	Remaining bandwidth after priority queue has been serviced

This design guide assumes that small business customers have a guaranteed amount of upstream bandwidth. QoS configuration is based on this assumption.

Priority treatment of real-time traffic using the WAN QoS described in this section is not a complete solution to maintain voice quality. A good designer must limit the number of voice calls over the WAN to match the allocated bandwidth that guarantees good voice quality. The next section describes this mechanism, known as Call Admission Control (CAC).

Call Admission Control

QoS can ensure the quality of the voice call only as long as voice traffic does not exceed the allocated bandwidth. If reserved bandwidth is sufficient only for a certain number of VoIP calls, and any extra calls are made over the WAN, the quality of all the voice calls deteriorates. CAC further guarantees the voice quality of calls transmitted across WAN links with limited bandwidth. CAC ensures that only a certain number of VoIP calls are placed over the WAN by blocking any extra VoIP calls. CAC accounts for the bandwidth being used for VoIP traffic used. If no bandwidth is available, the WAN call is blocked, and the caller hears a line-busy signal.

Delay and Jitter in Slower WAN Links

To prevent the annoying talkover that can be caused by excessive round-trip delays, the telephone industry standard ITU-T G.114 recommends that the maximum one-way delay for a voice packet be no more than 150 milliseconds. Although this standard is addressed in part by WAN QoS and CAC as described in the previous sections, Link Fragmentation and Interleaving (LFI) should be provisioned on slower access links to ensure that the end-to-end delay limit for voice packets is not exceeded. LFI is necessary on links of less than 768 K access speeds. Cisco CPE are appropriately configured for LFI.

The exact amount of bandwidth required for each RTP stream depends on the WAN type and its associated encapsulation method (Frame Relay, IPSec, and so on) as well as the voice sampling rate.

Cisco strongly recommends upstream bandwidth of 768 kbps or more for the HSB Communications solution.

Based on this assumption and the bandwidth consumption per call, Table 6 lists the recommended maximum voice calls for various WAN interfaces and codec types. Here it is assumed that 50 percent of upstream bandwidth is reserved for voice calls.

Table 6 Recommended Maximum Voice Calls for WAN Interfaces and Codec Types

WAN Interface	Upstream Bandwidth	G.711 (80 Kbps per call)	G.729 (24 Kbps per call)	G.722 (80 Kbps per call)
1 x T1	1.5 Mbps	10	32	10
2 x T1	3 Mbps	20	64	10
Broadband (Ethernet, DSL, or cable)	2 Mbps	12	40	12

For more information about calculating VoIP bandwidth, see *Bandwidth Calculation to Optimize VoIP Bandwidth on WAN* at the following website: http://www.cisco.com/application/pdf/paws/7934/bwidth_consume.pdf.

IP Telephony

This section describes some important concepts regarding IP telephony, and includes the following topics:

What is IP Telephony?

Traditional telephony systems are based on physical connections between analog endpoints (such as telephones and fax machines) and a circuit-switched telephony system (such as PBXs and the PSTN). These traditional telephony systems have limited capability and are expensive. The HSB Communications solution enables SPs to deliver a packet-switching-based IP telephony system. It is based on software constructs that represent IP endpoints and voice channels. These constructs provide greater flexibility when provisioning endpoints, phone numbers, and voice channels. The following section, although not required for completing installation of the HSB Communications solution, is provided for a better understanding of the underlying calling features, technology, and concepts.

Session Initiation Protocol

Session Initiation Protocol (SIP) is an application-layer protocol, which means it requires the services of transport layer protocols TCP or UDP. SIP proxy devices and servers resides in the SP data center. SIP communication happens between SIP proxy/servers and clients, known as user agent clients (UAC). UAC are simply multimedia endpoints, such as an IP Phone in the HSB Communications solution. SIP uses the format of the most popular protocols of the Internet, HTTP and SMTP, and thus has quickly become the protocol of choice for packet-voice service providers. SIP is used to control, as a signaling protocol, and to create, modify, and terminate multimedia sessions among one or more participants, such as audio sessions among one or more IP Phones in the HSB Communications solution described in this document.

Call Coverage Features

Call coverage features help ensure that all incoming calls are answered by a user or application, such as auto-attendant or voice mail, even when the originally dialed number is busy or does not answer. This is accomplished by a class of supplementary services made available by the provisioning server. Key call coverage features include the following:

- Call waiting—If a second call is delivered to a user who is already connected to a call, the user can either answer the second call or let the system forward the incoming call to auto-attendant or voice mail.
- Call forwarding—This feature diverts a call to an alternate answering point based on a specific condition, such as no answer, busy, all calls, or night service hours.
- Call hunt—When a call is placed to a specific extension, this feature sends that call to multiple phones, often in a preferred order, until the call is answered.
- Call blast—This is a special instance of a call hunt feature known as parallel hunt, where a call to a specific extension simultaneously rings multiple phones until the call is answered by any phone.
- Call pickup—This feature allows a user at one phone to answer an incoming call to another phone.

Call Handling Features

Call handling features allow users to manipulate existing calls in various ways. This is accomplished by a class of supplementary services made available by the provisioning server. The key call handling features include the following:

- Call hold—This feature places an existing call into a hold state to answer another incoming call.
- Call transfer—This feature changes the connection of a call from one destination to another without disconnecting the caller. Call transfers can be blind or consultative. In a blind transfer, the transferring extension connects the caller to a destination extension before ringback begins. In a consultative transfer, the transferring party either connects the caller to a ringing phone (ringback is heard) or speaks with the third party before connecting the caller to the third party.
- Conferencing—This feature creates calls that consist of three or more parties in a single conversation. Three-party conferencing can be hosted on an IP phone.

- Call park—This feature places a call on hold by using a special extension that functions as a temporary parking spot for the call, and then another user or phone in the system can retrieve the call.
- Call blocking—This feature prevents users from placing unauthorized outgoing calls to specific number patterns during certain periods throughout the day.

SPA IP Phone Features

Cisco HSB Communications SPA IP phone features have the appearance or operation of an IP phone. These features can be changed with a class of supplementary services available in the provisioning server. The key IP phone features are as follows:

- Speed dial—This feature allows users to associate frequently dialed numbers with phone buttons so that the system can quickly dial the number when the corresponding button is used.
- Intercom—This feature establishes a dedicated two-way audio path between two IP phones so that users can speak to each other even when one user is already connected to another call.
- Paging—This feature provides a one-way audio path to idle IP phones that have been designated to receive paging, which automatically answer the call using the speakerphone.
- Music-on-hold (MoH)—When a caller is put on hold, this feature plays an audio stream.
- Overlay/shared extensions (DN)—Multiple extension numbers on a single IP phone line.
- Monitored extensions (DN)—Monitoring status of an extension (busy or available).

Analog Devices and Fax Support

Analog devices, including traditional telephones, fax machines, and modems for credit card processing, are still widely used in various environments. These devices are accommodated by available FXS ports on the deployed CPE device. Table 1 lists the number of FXS ports available on each Cisco IAD choice for the HSB Communications solution. the Cisco ISR19xx/29xx provides even more flexibility due to its modularity. Alternatively, Cisco Small Business SPA2102 or SPA8000 devices can be deployed to add two or eight FXS ports respectively. All Cisco devices support T.38 Fax.

For More Information

For general information, see the following:

- Cisco SMART Designs—http://www.cisco.com/go/partner/smartdesigns
- Cisco Hosted Smart Business Communications—http://www.cisco.com/go/hsb
- Cisco Small Business Support Community—http://www.cisco.com/go/smallbizsupport

For product references, see the following:

- Cisco Small Business 300 Series Managed Switches—http://www.cisco.com/go/300switches
- Cisco 200 Series Smart Switches—http://www.cisco.com/go/200switches
- Cisco SPA 300 Series IP Phones—http://www.cisco.com/go/300phones
- Cisco SPA 500 Series IP Phones—http://www.cisco.com/go/500phones

- Cisco Small Business SPA Series IP Phone Administration Guide—http://www.cisco.com/en/US/docs/voice_ip_comm/csbpipp/ip_phones/administration/guide/spa500_admin.pdf

For technology references, see the following:

- Understanding Virtual LAN and VTP—http://www.cisco.com/warp/customer/473/vtp_flash/
- How NAT Works—http://www.ietf.org/rfc/rfc1918.txt