ADMINISTRATION GUIDE

Cisco SRP500 Series Services Ready Platforms (SRP520-U and SRP540 Models)

 78-20940-01

Contents

1

Introducing the SRP500 Series Services Ready Platforms

Thank you for choosing the Cisco SRP500 Series Services Ready Platforms. The SRP500 Series are flexible devices that enable small businesses to connect to a variety of services (high-quality data, hosted voice, and security services) offered by service providers.

This chapter provides information to familiarize you with the product. It includes the following sections:

- **Product Features**
- **Product Overview**

For information about how to physically install the SRP, see the Cisco SRP500 Series Services Ready Platforms Quick Start Guides at: www.cisco.com/go/srp500resources.

Product Features

The Cisco SRP500 Series provide these features:

- Intelligence to support voice, data, security, and application services.
- Industry-leading Session Initiation Protocol (SIP) stack to deliver clear, high-quality voice services.
- Interoperability with popular softswitches and voice gateways.
- Advanced security features, including SPI firewall, site to site IPSec VPN and IPSec VPN remote access server.
- 802.11n wireless access point.
- Resilient WAN connectivity.

- Support for standard USB mobile data network modems used for connectivity backup and load sharing.
- Standards-based provisioning using TR-069 and TR-104, or the Cisco XML API for streamlined deployments.
- SNMP v2/v3 management.

Product Overview

This section lists the available model numbers to help you become familiar with your SRP, and shows the front panel, back panel, and side view for each product family.

Model Numbers

SRP520-U Models

Model	Description
SRP521W-U	Fast Ethernet WAN 2 Phone (FXS) ports, 1 Line (FXO) failover port, 1 WAN (10/100) port, 4 LAN (10/100) ports, 1 USB 2.0 port, 802.11n, and WiFi Protected Setup (WPS)
SRP526W-U	ADSL2+ Annex B (ADSL over ISDN) 2 Phone (FXS) ports, 1 Line (FXO) failover port, 1 DSL port, 4 LAN (10/100) ports, 1 USB 2.0 port, 802.11n, and WiFi Protected Setup (WPS)
SRP527W-U	ADSL2+ Annex A/M (ADSL over POTS) 2 Phone (FXS) ports, 1 Line (FXO) failover port, 1 DSL port, 4 LAN (10/100) ports, 1 USB 2.0 port, 802.11n, and WiFi Protected Setup (WPS)

SRP540 Models

Model	Description
SRP541W	Gigabit Ethernet WAN 4 Phone (FXS) ports, 1 Line (FXO) port, 2 Gigabit WAN ports, 4 Gigabit LAN ports, 2 USB 2.0 ports, 802.11b/g/n, and WiFi Protected Setup (WPS)
SRP546W	ADSL2+ Annex B (ADSL over ISDN) 4 Phone (FXS) ports, 1 Line (FXO) port, 1 DSL port, 1 Gigabit WAN port, 4 Gigabit LAN ports, 2 USB 2.0 ports, 802.11b/g/n, and WiFi Protected Setup (WPS)
SRP547W	ADSL2+ Annex A/M (ADSL over POTS) 4 Phone (FXS) ports, 1 Line (FXO) port, 1 DSL port, 1 Gigabit WAN port, 4 Gigabit LAN ports, 2 USB 2.0 ports, 802.11b/g/n, and WiFi Protected Setup (WPS)

Front Panel (SRP520-U Models)

SRP521W-U Front Panel

SRP526W-U and SRP527W-U Front Panel

Front Panel Lights

The following table describes the lights on the front panel of the SRP520-U models. These lights are used for monitoring system activity.

SRP520-U Front Panel Lights

Lights	Description
POWER/SYS	Solid green when the SRP has successfully booted and is ready to use. Flashes green when the SRP is booting.
LAN ports (1–4)	Solid green when a link is established. Flashes green when there is activity on the LAN port.
WAN port (SRP521W-U only)	Solid green when an Ethernet link is established. Flashes green when there is activity on the WAN port.
PHONE (FXS) ports (1–2)	Solid green when the port is connected to a phone or fax machine and the SRP is able to make and receive calls. Flashes green when a call is in progress on the port.
DSL CD (SRP526W-U/527W-U)	Flashes green when a DSL service is detected. Lights solid green when synchronized.
DSL DATA (SRP526W-U/527W-U)	Flashes green when there is DSL activity on the line.
WLAN	Solid green when the radio is powered on and operational. Flashes green when there is wireless activity on the WLAN port.

SRP520-U Front Panel Lights (Continued)

USB port	Solid green when the connected USB device is operational. Flashes green if there is a device failure or unsupported device.
WPS	Solid green when WiFi Protected Setup (WPS) is operational. A slow green flash indicates that the setup is in progress. A fast green flash indicates a setup error.

Front Panel (SRP540 Models)

SRP541W Front Panel

SRP546W / SRP547W Front Panel

Front Panel Lights

The following table describes the lights on the front panel of the SRP540 Models. These lights are used for monitoring system activity.

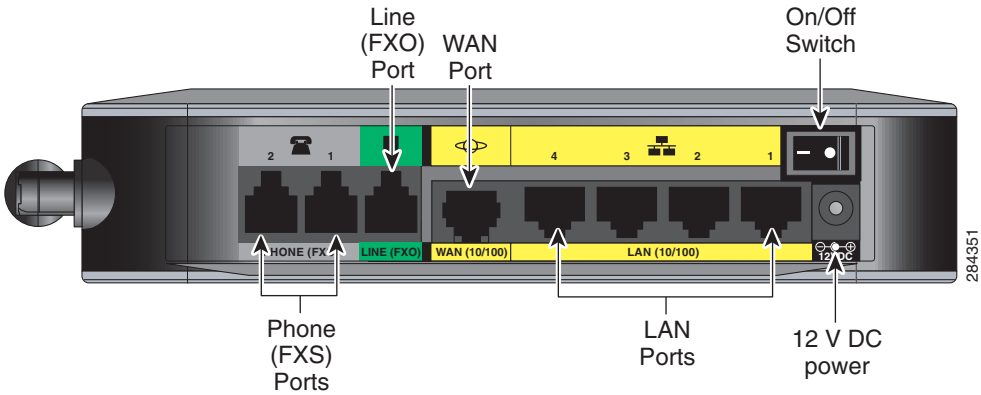
SRP540 Front Panel Lights

Lights	Description
POWER/SYS	Solid green when the SRP has successfully booted and is ready to use. Flashes green when the SRP is booting.
LAN ports (1–4)	Solid green when a link is established. Flashes green when there is activity on the LAN port.
WAN ports	Solid green when an Ethernet link is established. Flashes green when there is activity on the WAN port.
LINE port	Solid green when the port is connected to a PSTN line and the SRP is able to make and receive calls. Flashes green when a call is in progress on the port.
PHONE (FXS) ports (1–4)	Solid green when the port is connected to a phone or fax machine and the SRP is able to make and receive calls. Flashes green when a call is in progress on the port.
DSL CD (SRP546W/547W only)	Flashes green when a DSL service is detected. Lights solid green when synchronized.
DSL DATA (SRP546W/547W only)	Flashes green when there is DSL activity on the line.
WLAN	Solid green when the radio is powered on and operational. Flashes green when there is wireless activity on the WLAN port.
USB ports (1–2)	Solid green when the connected USB device is operational. Flashes green if there is a device failure or an unsupported device.
WPS button	Solid green when WiFi Protected Setup (WPS) is operational. A slow green flash indicates that the setup is in progress. A fast green flash indicates a setup error. To automatically configure wireless security for devices that support WPS, press and hold this button until the WPS light flashes. Make sure that the device is located near the SRP during setup.

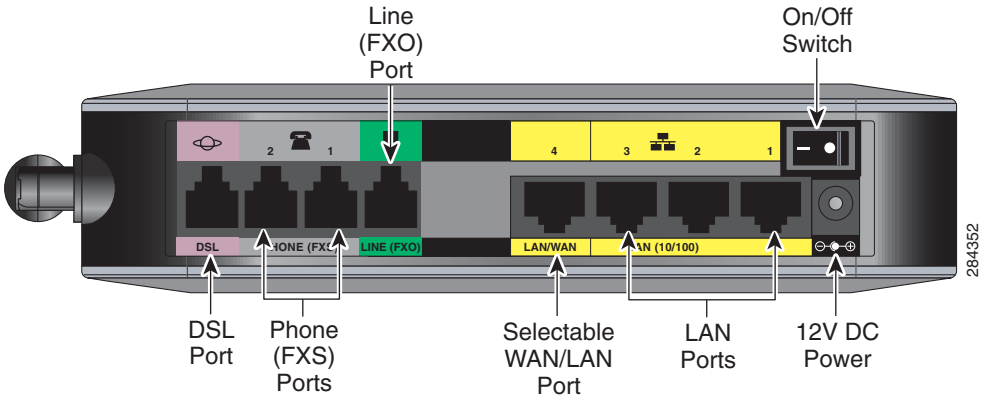
Back Panel (SRP520-U Models)

Network devices are connected to the back of the SRP. The ports on the panel vary depending on the model.

SRP521W-U Back Panel



SRP526W-U and SRP527W-U Back Panel

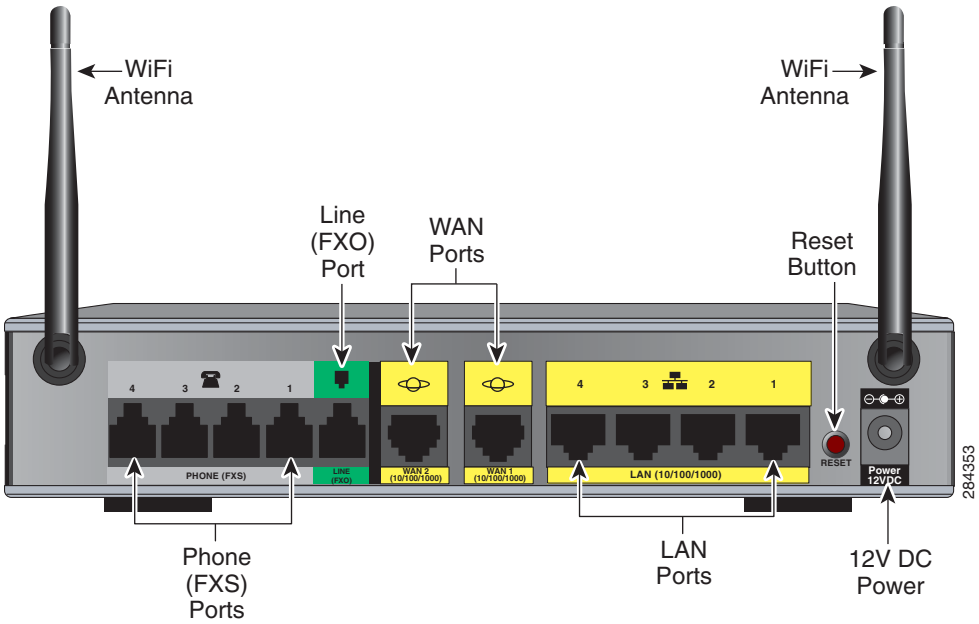


SRP520-U Back Panel Descriptions

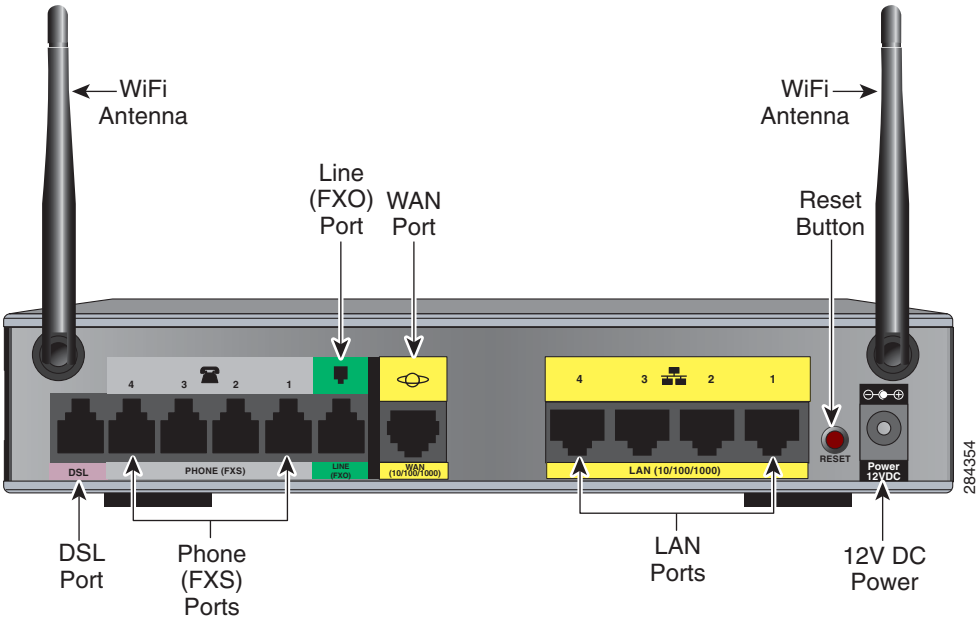
Feature	Description
DSL port SRP526W-U/SRP527W-U only	Connect to a DSL connection.
PHONE (FXS) ports (1–2)	Connect directly to an analog telephone, fax machine, or similar device. If your analog phone requires a separate bell line, you may need to connect a ring adapter between the SRP and your phone so that the phone rings when calls are presented.
LINE (FXO) port	Connect to an analog phone line.
WAN (10/100) port SRP521W-U only	Connect to an Ethernet broadband Internet connection.
LAN (10/100) ports (1–4)	Connect to a wired computer and other network devices.
Selectable WAN/LAN (10/100) port SRP526W-U/SRP527W-U only	Port can be used as a WAN Ethernet port if the ADSL interface is disabled. By default the ADSL port is enabled, allowing this port to be used for LAN connectivity. See the SRP500 Administration Guide for further information.
On/Off Switch	Powers the SRP on or off.
12V DC power	Connect to the provided power adapter.

Back Panel (SRP540 Models)

SRP541W Back Panel



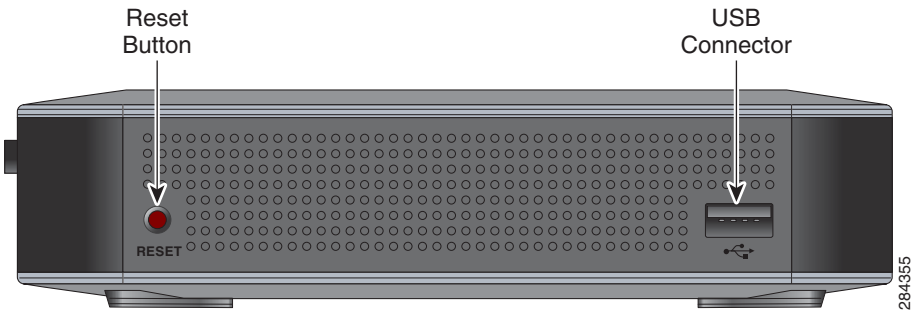
SRP546W and SRP547W Back Panel

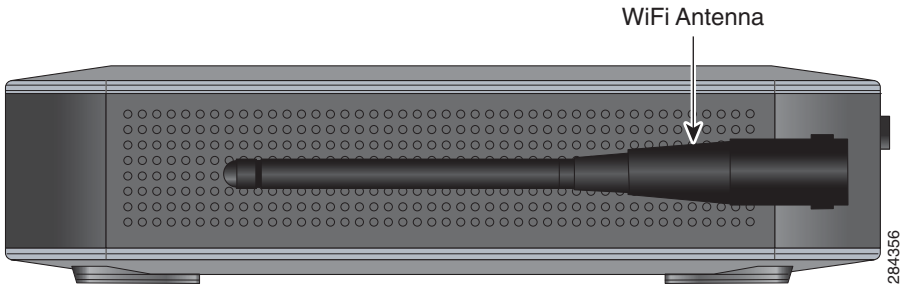


SRP540 Back Panel Descriptions

Feature	Description
DSL port SRP546W/SRP547W only	Connect to a DSL connection.
PHONE (FXS) ports (1–4)	Connect directly to an analog telephone, fax machine, or similar device. If your analog phone requires a separate bell line, you may need to connect a ring adapter between the SRP and your phone so that the phone rings when calls are presented.
LINE (FXO) port	Connect to an analog telephone line.
WAN (10/100/1000) port(s) Note. The SRP541W has 2 WAN ports.	Connect to an Ethernet broadband Internet connection.
LAN (10/100/1000) ports (1–4)	Connect to a wired computer and other network devices.
RESET button	Press and hold for 5 seconds to reset the SRP. Press and hold for 10 seconds to reset the SRP to its factory defaults. To press the button, insert a paper clip or similar object into the opening. **CAUTION** This will reset the device to its factory default settings.
Power 12VDC	Connect to the provided power adapter.
WiFi antennas	Two detachable WiFi antennas with TNC connectors.

Side View (SRP520-U Models)

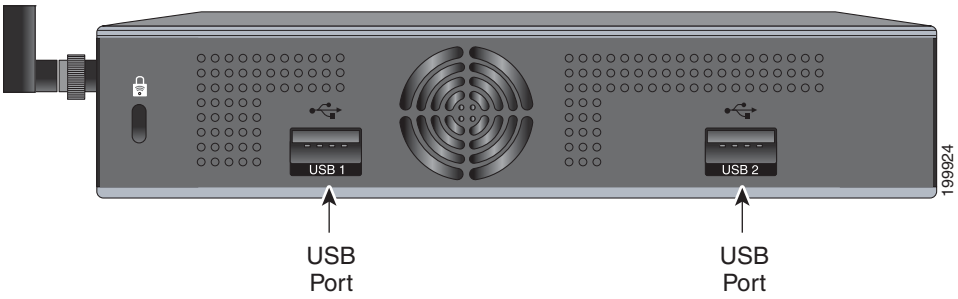




SRP520-U Side View

Feature	Description
RESET button	Press and hold for 5 seconds to reset the SRP. Press and hold for 10 seconds to reset the SRP to its factory defaults. To press the button, insert a paper clip or similar object into the opening. CAUTION This will reset the device to its factory default settings.
USB port	Connect to a compatible USB modem. For information about connecting the SRP to a USB modem, see **Mobile Network, page 46**.
WiFi antenna	Adjustable WiFi antenna.

Side View (SRP540 Models)



SRP540 Side View

Feature	Description
USB ports (1–2)	Connect to compatible USB modems. For information about connecting the SRP to a USB modem, see **Mobile Network, page 46**.

Top View (SRP520-U Models)

SRP520-U Side View

Feature	Description
WPS button	Use to automatically configure wireless security for devices that support WiFi Protected Setup (WPS). To configure WPS, press and hold this button until the WPS light flashes. Make sure that the device is located near the SRP during setup.

Default Settings

The following table lists the default settings for the Services Ready Platforms.

SRP Default Settings

Parameter	Value
Device IP	192.168.15.1
Customer username	cisco
Customer password	cisco
Administrator username	admin
Administrator password	admin
DHCP Range	192.168.15.100 to 149
Data VLAN	VLAN 1: Default data access. By default, the assigned IP subnet is 192.168.15.1/24.
Voice VLAN	VLAN 100: Advertised to Cisco VoIP phones through CDP. By default, the Voice VLAN is assigned IP subnet 192.168.100.100 to 149.

2

Getting Started with the Configuration Utility

This chapter describes how to use the Services Ready Platform Configuration Utility. This is a web-based utility you use to manage and provision your Services Ready Platform (SRP).

This chapter includes the following sections:

- **Logging In to the Configuration Utility**
- **Overview of the Configuration Utility Interface**

Logging In to the Configuration Utility

To log in to the Services Ready Platform Configuration Utility.

STEP 1 Configure your computer to use DHCP for its LAN connection.

Using an Ethernet cable, connect your computer to an available LAN port (1-4) on the SRP. Your computer will automatically obtain an IP address in the 192.168.15.x range.

STEP 2 Start a web browser. In the Address bar, enter the default IP address: **http://192.168.15.1**

STEP 3 When the login window opens, enter the default username and password to log in as the administrator.

The default username is **admin**.
The default password is **admin**.

NOTE The username and password are case sensitive.

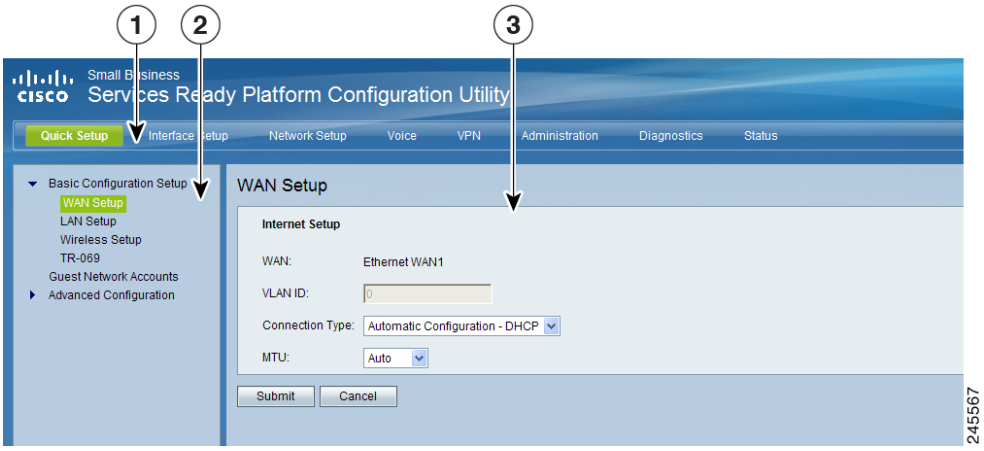
After you log in, the Configuration Utility opens.

STEP 4 Continue configuring your SRP from the Quick Setup pages. See **The Quick Setup Menu, page 29**.

Overview of the Configuration Utility Interface

This section describes the Main menu bar areas and icons that the Configuration Utility uses.

Main Menu Bar



Number	Component	Description
1	Menu Bar	Contains the major function categories. Click a menu item to change to another category.
2	Navigation Pane	Provides easy navigation through the configurable device features. The main branches expand to provide the subfeatures. Click on the triangle next to the main branch title to expand or contract its contents. Click the title of a feature or subfeature to open it.
3	Main Content	The main content of the feature appears in this area.

Icons

The Configuration Utility has icons and buttons for commonly used configuration options.

Icon		Description
	Edit Icon	Edits an existing item from a list.
	Add Item Icon	Adds an item to a list.
	Delete Item Icon	Deletes an item from a list.
	Increment Decrement Icons	Changes the numeric values. ▪ Click the “+” icon to increment a value. ▪ Click the “-” icon to decrement a value.

3

The Quick Setup Menu

This chapter describes how to use the Quick Setup Menu to set up the essential connectivity features and guest accounts for your Services Ready Platforms. It includes the following sections:

- **Basic Configuration Setup**
- **Guest Network Accounts**
- **Advanced Configuration Setup**

The Quick Setup menu is displayed by default when you first log in to the SRP. You can use these setup pages to quickly get the device up and running. This menu also provides convenient links to features found in the Configuration Utility.

Basic Configuration Setup

Use the Basic Configuration Setup to configure WAN, LAN, Wireless, and Remote Provisioning settings for your SRP. To access these pages click **Quick Setup > Basic Configuration Setup** from the Configuration Utility.

WAN Setup (Ethernet)

Use the WAN Setup page to set up your Ethernet WAN interface.

STEP 1 Click **Quick Setup > Basic Configuration Setup > WAN Setup**. The WAN Setup window opens.

STEP 2 Choose the Connection Type as required by your Internet Service Provider (ISP).

STEP 3 Specify the Connection Type Settings as defined in **Ethernet WAN Interface Settings, page 39**.

STEP 4 Click **Submit** to save your changes.

WAN Setup (ADSL)

Use the WAN Setup page to quickly set up your ADSL WAN interface.

STEP 1 Click **Quick Setup > Basic Configuration Setup > WAN Setup**. The WAN Setup/VC and IP Settings window opens.

STEP 2 Enter the VC (Virtual Connection) and IP settings as defined in **Internet Setup, page 35**.

STEP 3 Click **Submit** to save your changes.

LAN Setup

Use the LAN Setup page to quickly set up the LAN interface.

NOTE The Quick Setup assumes that you will configure the SRP to act as a DHCP server for the main local subnet. If you require alternative configurations, access the full feature set through Interfaces menu.

STEP 1 Click **Quick Setup > Basic Configuration Setup > LAN Setup**. The LAN Setup window opens.

This page shows the DHCP server (Default LAN) and voice settings. The default is DHCPRule_1 (Default LAN) and DHCPRule_voice.

STEP 2 (Optional) View, edit, or add a new DHCP entry. For more information, see **DHCP Server, page 54**.

STEP 3 Click **Submit** to save your settings.

Wireless Setup

Use the Wireless Setup page to quickly set up the Wireless network.

STEP 1 Click **Quick Setup > Basic Configuration Setup > Wireless Setup**. The Wireless Setup window opens.

STEP 2 Specify the wireless network settings as defined in **Basic Wireless Settings, page 65**.

STEP 3 Click **Submit** to save your changes.

Remote Provisioning (TR-069)

Use the TR-069 page to configure communication with an Auto-Configuration Server (ACS) through the TR-069 CPE WAN Management Protocol (CWMP).

STEP 1 Click **Quick Setup > Basic Configuration Setup > Remote Provisioning**. The Remote Provisioning window opens.

STEP 2 Click **Enabled** to enable remote provisioning. The default is disabled.

STEP 3 Specify the remote provisioning settings as defined in **TR-069, page 240**.

STEP 4 Click **Submit** to save your settings.

Guest Network Accounts

Use the Guest Network page to add guest accounts to your network.

STEP 1 Click **Quick Setup > Guest Network Accounts.** The Guest Network Accounts window opens.

STEP 2 Specify the guest account settings as defined in **Configuring the User Account, page 116**.

STEP 3 Click **Submit** to save your settings.

Advanced Configuration Setup

Use the Advanced Configuration pages to configure advanced settings for Voice, Mobile Network Setup, Firewall, NAT, and Port Range Forwarding.

To access these pages click **Quick Setup > Advanced Configuration Setup** from the Configuration Utility.

Voice

Use the Voice option to administer and view voice services and voice settings. See **Configuring Voice, on page 121**.

Mobile Network Setup

Use the Mobile Network Setup option to configure the mobile network settings. See **Mobile Network, on page 46**.

Firewall

Use the Firewall option to configure the firewall filter settings. See **Firewall, on page 100**.

NAT

Use the NAT option to configure the Network Address Translation (NAT) settings. See **Network Address Translation, on page 85**.

Port Range Forwarding

Use the Port Range Forwarding Page to forward traffic to a range of ports to the same ports on the target server in the LAN. See **Port Forwarding, page 89**.

4

Setting Up the Interfaces of the Services Ready Platforms

This chapter describes how to set up the interfaces for your SRP. It includes the following sections:

- **Setting Up the WAN Interfaces**
- **Setting Up the VLAN Interfaces and LAN Ports**
- **Setting Up the Wireless LAN**
- **Using the Management Interface**

To access these pages, click **Interface Setup** from the Configuration Utility menu bar.

Setting Up the WAN Interfaces

This section includes the following topics:

- **Internet Setup**
- **Internet Option**
- **Mobile Network**
- **Multi-WAN Configuration**

To access these pages, click **Interface Setup > WAN** from the Configuration Utility.

Internet Setup

Use the Internet Setup page to configure the settings for WAN networking.

NOTE After you configure the interface settings, we recommend that you create a new username and password for your SRP for both administrator and customer/user roles. To change it, see **User List, page 250**. Taking this precaution increases security by protecting the SRP from unauthorized changes.

STEP 1 Click **Interface Setup > WAN > Internet Setup**. The Internet Setup window opens. The WAN Interface List shows the System Default and Default Voice Route, Interface type, type of Internet connection, and IP address and subnet mask for each interface.

STEP 2 Configure the interfaces.

a. Click the interface to configure under the Interface column.

b. Configure the parameters for the physical interfaces. There are two sets of options, one for DSL and the other for Ethernet.

- For a DSL interface, choose a modulation type from the drop-down list. The default is MultiMode (recommended), which automatically detects the line modulation type.
- For an Ethernet interface, select the flow control setting (enabled by default), interface speed (the default is Auto-negotiate), or override the MAC address used by the interface. To use the MAC address from the PC being used to configure the SRP, click the **Clone Your PC's MAC** button.

c. Click **Submit** after you are finished.

STEP 3 Configure the Interface addressing.

a. From the WAN interface List, select either a DSL PVC or an Ethernet subinterface depending on your model.

- To configure a DSL PVC interface, click the **Edit** (pencil) icon next to the PVC0 interface. The *Internet Setup* settings for the PVC0 interface window opens.

  Specify the Internet Setup settings as defined in the **Virtual Channel (VC) Settings** table. The encapsulation type you choose may change the other options that appear on this page. For more information, see **Encapsulation Settings, page 41**.

- You can edit the Ethernet interface (the main one, or a subinterface, if it has already been created) by clicking the pencil icon. A subinterface may be added by clicking the add item icon, see **Adding a Subinterface, page 38**.

b. Click **Submit** to save your changes.

STEP 4 Select the default route for the interface that you are configuring from the drop-down list.

NOTE This interface default route is used to select the outbound logical interface when the failover feature switches between physical interfaces.

STEP 5 To view the interface information, select an interface from the WAN Interface Detail List. This list displays information about the selected interface as described in **WAN Interface Status Details** table.

Virtual Channel (VC) Settings

Encapsulation	Protocol used between your broadband gateway and your ISP's servers. Most of the encapsulations are defined in Internet standards called Requests for Comments (RFCs). Two are derived from the Point-to-Point Protocol (PPP): PPP over Ethernet (PPPoE) and PPP over ATM (PPPoA). The available options are IPoA, PPPoE, PPPoA, and RFC 1483 Bridged EoA encapsulation.
Multiplexing	Select the method used to route different kinds of data through different virtual circuits (VCs) in the ATM network. The choices are: ▪ Logical Link Control (LLC) encapsulation (also called LLC-SNAP). This is the default setting. ▪ Virtual Channel (VC) multiplexing (also called VC-Mux).

Virtual Channel (VC) Settings

QoS Type	DSL quality of service (QoS) method your ISP uses on your line: Unspecified Bit Rate (UBR), Constant Bit Rate (CBR), Real-Time Variable Bit Rate (RTVBR), or Non-Real-Time Variable Bit Rate (NRTVBR). CBR provides the best guarantee of low latency; UBR provides none, but is typically used for most broadband data services. ▪ **Pcr Rate**: When QoS is set to CBR, VBR_RT, or VBR_NRT, enter the Peak Cell Rate (PCR) in cells per second. ▪ **Scr Rate**: When QoS is set to VBR_NRT or VBR_RT, enter the Sustained Cell Rate (SCR) in cells per second. ▪ **MBS**: When QoS is set to VBR_NRT or VBR_RT, enter the MBS in cells per second. ▪ **CDVT**: When QoS is set to CBR, VBR_NRT or VBR_RT, enter the CDVT in cells per second.
VPI/VCI Auto Detect	Enables or disables automatic detection of the VPI and VCI values that identify your line to the ATM network. The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) are values used to identify your line to your ISP's ATM network. The SRP will automatically detect DSL services checked on the following VC pairs: 0/35, 8/35, 0/43, 0/51, 0/59, 8/43, 8/51, 8/59, 0/38.

WAN Interface Status Details

Physical and Logical Link Status	Status of the physical interface: connected or disconnected.
IP Address	IP address assigned to the interface.
Netmask	Subnet mask.
Gateway	IP address of the ISP server.
Host Name	Hostname, if applicable.
Domain Name	Domain name, if applicable.

WAN Interface Status Details

MTU Type	Auto or Custom.
MTU Size	Current MTU size. This is displayed even if Auto is selected.
DNS 1,2,3	IP addresses of the DNS servers, if configured.
Static DNS Servers 1, 2, 3	IP addresses of the Static DNS servers, if configured.
VLAN Encapsulation	If enabled, for an ADSL PVC, an IEEE 802.1q VLAN header is added to outbound traffic, allowing some Service Providers to control quality of service based on associated IEEE 802.1p priority values.
VLAN ID	VLAN ID used if VLAN Encapsulation is enabled.

Adding a Subinterface

Use the WAN interface list from the Internet Setup window to add a subinterface to the SRP. These options are the same as those for configuring a main WAN interface except you cannot configure an Ethernet subinterface for PPTP or L2TP.

The SRP supports multiple logical interfaces per physical port. For ADSL interfaces, you can configure up to 4 PVC interfaces. For Ethernet ports, VLAN interfaces are created as part of an IEEE 802.1p trunk.

Ethernet Subinterface

The SRP supports VLANs that can be used as either local area VLANs or WAN subinterfaces. The SRP520 models support up to 5 VLAN connections. The SRP540 models support up to 10.

STEP 1 To add a new logical Internet connection, select the top level WAN from the Internet Setup page and click the **Add** (page) icon. The *Internet Setup* window for the new Internet connection opens.

STEP 2 Choose the Connection Type required by your Internet Service Provider (ISP) as defined in the **Ethernet WAN Interface Settings** table below.

STEP 3 Choose an MTU option from the drop-down list. Unless a change is required by your ISP, we recommend that you set the MTU method to **Auto**, which allows the device to automatically choose the size. The default size is 1500 bytes.

To specify another MTU size, choose **Manual** from the drop-down list and enter the size in bytes. The standard size for Ethernet networks is 1500 bytes. For PPPoE connections, a typical value is 1492 bytes.

STEP 4 Click **Submit** to save your changes. The new connection is added to the WAN Interface List on the Internet Setup page.

Ethernet WAN Interface Settings

WAN	Physical interface name - either Ethernet WAN1 or Ethernet WAN2 (SRP540 only).
VLAN ID	Enter the VLAN ID for the new logical subinterface. Note that the first logical interface of an Ethernet port is assigned VLAN ID 0 (no VLAN tag). This cannot be changed.
Connection Type	Type of Internet connection that your ISP provides.
	Automatic Configuration/DCHP Connection type often used with cable modems. Choose this option if your ISP did not assign a static IP address to your account and instead use the Dynamic Host Control Protocol (DHCP) to assign an IP address dynamically. No other information is required for this selection.
	Static IP Choose this option if your ISP provides you with a static (permanent) IP address. Enter the **Internet IP Address**, **Subnet Mask**, and **Default Gateway** IP address. Optionally, you can enter the IP addresses of up to three Domain Name System (DNS) servers.

Ethernet WAN Interface Settings

	PPPoE Choose this option if your ISP uses Point-to-Point Protocol over Ethernet (PPPoE). Enter the **Username** and **Password** for your ISP account and the **Service Name** if required by your ISP. Select either the **Connect on Demand** or **Keep Alive** option. **Connect on Demand** Opens a connection only when a user attempts to connect to the Internet. The connection automatically terminates if there is a period of inactivity longer than the specified Max Idle Time (in minutes). We recommend this option if your billing is based on the time that you are connected. PCs often send information to the Internet even if email or a web browser is not being used. This may keep the session connected for longer than expected. **Keep Alive** Keeps you connected to the Internet indefinitely, even when your connection sits idle.
	PPTP Select this option if your ISP uses Point to Point Tunneling Protocol (PPTP). Enter the **PPTP Server IP** address and the **Username** and **Password** for your account. If your service provider does not dynamically assign an IP address, disable DHCP and enter the **Internet IP address**, **Subnet Mask** and **Gateway** information provided for your account. Select either the **Connect on Demand** or **Keep Alive** option.

Ethernet WAN Interface Settings

	L2TP Select this option if your ISP uses Layer 2 Tunneling Protocol (L2TP). Enter the L2TP Server IP address and the Username and Password for your account. If your service provider does not dynamically assign an IP address, disable **DHCP** and enter the **Internet IP address**, **Subnet Mask** and **Gateway** information provided for your account. Select either the **Connect on Demand** or **Keep Alive** option.
MTU (Maximum Transmission Unit)	Size, in bytes, of the largest packet that can be sent through the network. This value is typically 1500 bytes; however, it might need to be lower for some broadband services. Check with your service provider for specific requirements.
DNS 1-3	(Optional) Enter the IP addresses of up to three DNS servers, or leave the fields blank to allow a DNS server to be assigned dynamically. This option cannot be configured for a WAN subinterface.

Encapsulation Settings

This section describes the ADSL Encapsulation Settings that you can choose from in the Internet Setup page under VC settings. The available options are IPoA, PPPoE, PPPoA, and RFC 1483 Bridged EoA encapsulation.

Encapsulation is the protocol used between the SRP and your ISP's servers. Most of the encapsulations are defined in Internet standards called Requests for Comments (RFCs). Two are derived from the Point-to-Point Protocol (PPP): PPP over Ethernet (PPPoE) and PPP over ATM (PPPoA).

IPoA Settings

Choose IPoA for direct encapsulation of IP traffic over the DSL ATM virtual circuit. Enter the required information as provided by your ISP: Internet IP Address, Subnet Mask, and Default Gateway IP address. Optionally, you can enter the IP addresses of primary and secondary DNS servers.

IPoA Settings

Internet IP Address and Subnet Mask	The SRP's IP address and subnet mask as seen by external users on the Internet (including your ISP). Your ISP will provide you with this information.
Default Gateway	Your ISP will provide you with the gateway IP address.
Primary/Secondary DNS	Use to define one or two DNS servers. The SRP will use these to resolve domain names for locally configured features and may also pass these on to local clients through DHCP.

PPPoE Settings

Choose PPPoE to run Ethernet encapsulated PPP over the DSL ATM virtual circuit. Enter the username and password provided to you by your ISP. Optionally, you can also specify a PPP service name, if one is provided by your service provider.

PPPoE Settings

Username and Password	Enter the strings that your ISP has instructed you to use. The username can be called a "username," "login name," or "login."
Service Name	String required by some ISPs. Enter this information only if your ISP requires it.
Connect on Demand	Click this option if you want your broadband gateway to connect to your ISP when a connection is needed, and to disconnect when the line to your ISP has been idle for a given amount of time. Connection and disconnection are automatic. You can also adjust the maximum idle time. The default setting is 20 minutes. The alternative to Connect on Demand is Keep Alive (see next). In most cases you can choose either option without consulting your ISP.
Keep Alive	Click this option if you want the gateway to maintain the connection to your ISP all the time. If the link goes down for a given number of seconds (the "redial period"), the gateway will automatically try to reestablish it. The default redial period is 20 seconds.

PPPoE Settings

MTU	Extra header information used on PPPoE connections over ADSL typically limits the maximum packet size that can be sent to 1492 bytes. Enable this setting only if instructed to do so by your ISP.
LCP Echo-Request Interval	(SRP547W/SRP546W models only) Specify the **LCP Echo Interval** in seconds. The default is 30 seconds. This determines how often the SRP sends an LCP echo request at regular intervals to the ISP to make sure that the PPPoE connection is active.

PPPoA Settings

Choose PPPoA to run PPP directly over the DSL ATM virtual circuit. Enter the username and password provided by your ISP.

PPPoA Settings

Username and Password	Enter the strings that your ISP has instructed you to use. The username can be called a “username,” “login name,” or “logon.”
Connect on Demand	Click this option if you want your broadband gateway to connect to your ISP when a connection is needed, and to disconnect when the line to your ISP has been idle for a given amount of time. Connection and disconnection are automatic. You can also adjust the maximum idle time; the default setting is 20 minutes. The alternative to Connect on Demand is Keep Alive (see next). In most cases, you can choose either option without consulting your ISP.
Keep Alive	Click this option if you want the gateway to maintain the connection to your ISP all the time. If the link goes down for a given number of seconds (the “redial period”), the gateway will automatically try to reestablish it. The default redial period is 20 seconds.

RFC 1483 Bridged EoA

Use this encapsulation to bridge local traffic with the DSL PVC. If you are using an Ethernet over ATM service, you can choose to configure the WAN IP address either statically or dynamically.

Alternatively, if you want to bridge traffic to a device connected locally (thereby using the SRP as a DSL modem only for this PVC), create a new VLAN that includes this PVC and the Ethernet LAN port to which the device is connected. The local device will then be able to terminate the IP connection (that is, through PPPoE) directly.

RFC 1483 Bridged EoA Settings

IP Settings	Select the IP Setting. The default setting is Obtain an IP Address Automatically. If you selected manual, enter the IP address, mask, gateway, and DNS settings.

Common DSL Encapsulation Settings

The following additional settings appear when you select a DSL encapsulation setting. These settings are common to all DSL encapsulations.

DSL Encapsulation Settings

MAC Address Clone	Specify the MAC Address Clone Settings. Enable this feature if your ISP requires that you register a MAC address to access the Internet. ▪ To clone your MAC address, select **Enabled** and then enter the previously registered MAC address. ▪ If you previously registered a different MAC address and do not want to register again with your ISP, click the **Clone Your PC's MAC** button. This allows you to assign the previously registered MAC address to the SRP.
802.1Q VLAN Encapsulation	To enable 802.1Q encapsulation, select **Enabled** (the default is Disabled). Then enter a value for the VLAN ID. The range is 0 to 4079.

DSL Encapsulation Settings

MTU	Choose an MTU option from the drop-down list. Unless a change is required by your ISP, we recommend that you set the MTU method to **Auto**. The default size is 1500 bytes.

Internet Option

If necessary, use the Internet Option page to supplement the information configured for your Internet connection.

STEP 1 Click **Interface Setup > WAN > Internet Option**. The Internet Option window opens.

STEP 2 Enter the **Host Name** and **Domain Name** if provided by your ISP.

STEP 3 Enter the **IP addresses** for up to three DNS servers.

NOTE The SRP allows DNS server information to be specified in a number of different contexts, allowing you to meet your specific needs.

Each WAN interface allows either the static or dynamic configuration of primary, secondary and tertiary connection specific servers. You can also statically configure primary, secondary and tertiary servers globally.

To determine which servers to use for internal name resolution, the SRP takes the first three addresses from a list that it constructs in the following order:

- Primary servers from Internet Options, WAN1, WAN2, and then 3G.
- Secondary servers from Internet Options, WAN1, WAN2, and then 3G.
- Tertiary servers from Internet Options, WAN1, WAN2, and then 3G.

STEP 4 Enable **Schedule WAN Reconnect** if you want all WAN connections to be restarted at a certain time. If enabled, specify the **Reconnect Time** by hour and minute.

STEP 5 Click **Submit** to save your changes

Internet Options

Host Name	Hostname provided by your ISP.

Internet Options

Domain Name	Domain Name provided by your ISP.
IPv4 Static DNS 1–3	Enter the IP addresses for up to three DNS servers.
Scheduled WAN Reconnect	Enable this option to cause all WAN connections to be restarted at a specified Reconnect time.
Reconnect Time	If Scheduled WAN Reconnect is enabled, set the reconnect time by hour and minute.

Mobile Network

Use the Mobile Network page to configure your mobile network settings. You can configure your SRP to connect to a Mobile Broadband USB modem that is connected to its USB interface. For information about compatible modems, click the Technical References link at:

http://www.cisco.com/go/srp500resources

A USB modem will be automatically discovered and configured when connected to the SRP. A custom configuration for network access can be added once the modem is detected.

- If the SRP500 is configured for Connection Failover, the USB modem will only attempt to connect once higher priority interfaces fail to connect.
- If it is not using Connection Failover, the USB modem will attempt to connect immediately.

Use of the Mobile Broadband USB Modem is primarily meant for data services only. Voice quality over the mobile network cannot be guaranteed.

STEP 1 Click **Interface Setup > Mobile Network**. The Mobile Network window opens.

STEP 2 Connect to the USB Modem. If the card is supported by the SRP, it is automatically detected and appears on the Mobile Network page.

STEP 3 Select **Auto** or **Manual** connection mode. The default mode is Auto.

- To enable your modem to establish a connection automatically, select **Auto** mode.

  NOTE Ethernet Connection Recovery works only if the Connection Mode is set to Auto. If you select Auto, you must also select either **Connect on Demand** or **Keep Alive**.

- To connect or disconnect your modem connection manually, select **Manual** mode.

  NOTE If you cannot establish a connection, select **Manual** mode and enter the Access Point Name (APN), dial number, username, and password. Some mobile data services may need you to configure the APN, dial number, username, and password manually.

STEP 4 Verify that the Card Status field shows the status of your mobile card.

STEP 5 If required, select a Tunnel Protocol from the drop-down list.

STEP 6 If necessary, change any mobile network settings in the **Mobile Network Setup** area.

NOTE You must click the Manual option in the Configure Mode field to manually set up your mobile network card.

STEP 7 Click **Submit** to save your settings.

Mobile Network Settings

Global Settings	
Connect Mode	Choose **Auto** or **Manual** Mode. Select **Auto** mode for your modem to establish a connection automatically. If you are using manual mode, you will need to access the Configuration Utility to establish an Internet connection through the mobile connection. Click **Connect** to establish a connection when required. Click **Disconnect** to tear down the connection. **Connect on Demand**: Select this option to enable the SRP to terminate the Internet connection after it is inactive for a specified period of time (Max Idle Time). If your Internet connection is terminated due to inactivity, this option enables the modem to automatically reestablish a terminated connection when a user attempts to access the Internet again. In the **Max Idle Time** field, enter the number of minutes of idle time that can elapse before your Internet connection terminates. The default Max Idle Time is 5 minutes. **Keep Alive**: Select this option to enable the SRP to check your Internet connection at the specified interval (Redial Period). If you are disconnected, the SRP automatically reestablishes your connection. In the Redial Period field, specify how often you want the SRP to check the Internet connection. The default Redial Period is 30 seconds.

Mobile Network Settings

Tunnel Protocol	As with WAN Ethernet ports, you can select either PPTP or L2TP through the USB modem. See the **Ethernet WAN Interface Settings, page 39** for option details. **NOTE** Only dynamic addressing is allowed on this interface. **NONE**. Select this option to disable protocol tunneling. This is the default setting. **PPTP/L2TP**. Select PPTP or L2TP depending on the service that you want to use. You will need to provide the server IP address, username, and password.
Card Status	Displays the current modem connection status as initializing, connecting, connected, disconnecting, or disconnected. These messages might also appear: ▪ Please set APN manually (appears when the SRP is unable to determine the APN from the operator in automatic mode) ▪ Searching for service... ▪ no SIM card ▪ SIM locked ▪ SIM busy ▪ SIM ready ▪ pin code needed ▪ pincode error ▪ Card is locked ▪ Card is not activated ▪ Card initialized error ▪ error If Connect Mode is set to Manual, you can click a button to connect or disconnect your modem.

Mobile Network Settings

Mobile Network Setup	
Configure Mode	The SRP automatically detects supported modems and presents a list of appropriate default configurations. To override any of these settings (with the exception of the SIM PIN), select manual configuration mode.
Card Model	Data card model that is inserted into the USB drive. Unsupported cards are reported as unrecognized.
Access Point Name (APN)	Internet network to which the mobile device is connecting to. Enter the access point name provided by your mobile network service provider. This field is only displayed for GSM cards.
Dial Number	Dial number for the Internet connection. Enter the number required for your modem.
Username/ Password	(Optional) Enter the **username** and **password** provided by your mobile network service provider.
SIM PIN	(Optional) PIN code associated with your SIM card. Enter your SIM PIN number here. This field is only displayed for GSM cards.
Server Name	(Optional) Name of the server for the Internet connection if provided by your service provider.
Authentication	Type of authentication used by your service provider. Choose your authentication type from the drop-down list. The default is Auto. If you do not know which type of authentication to use, keep the default setting.
Service Type	Select the most commonly available type of mobile data service connection based on your area service signal. Choices are HSDPA/3G/UMTS Preferred, HSDPA/3G/UMTS Only, and GPRS Only. If your location supports only one mobile data service, you can set up an enhanced build-up connection. The first selection will always search for HSPDA/3G/UMTS service or switch to GPRS automatically only when it is available.

Mobile Network Settings

LTE Service	Choose an LTE wireless service from the drop-down menu. Choices are 3G only, 4G only, or Auto. The default is Auto.

Multi-WAN Configuration

An Internet connection can be established though an Ethernet cable (connected to the WAN port), through ADSL (connected to the ADSL port), or through a compatible USB modem (connected to the USB port). When you enable connection failover, you can connect these at the same time, but only one of them can be used to establish a link at a time.

Whenever the Internet connection fails on the interface that is in use, the SRP automatically attempts to bring up another connection on the other interface according to the priority. Whenever the Internet connection recovers on a WAN interface that has higher priority, the SRP automatically attempts to bring back and recover the Internet connection through that WAN.

When connection failover is disabled, the SRP tries to use all available WAN interfaces. In this case, the routing protocols or policy-based routing is used to direct traffic if configured. Otherwise, all traffic is routed through the highest priority interface. Alternatively, traffic can be balanced across connected interfaces in accordance with a predefined weighting scheme. In addition to policy-based routing, static routes can also be used to direct traffic.

STEP 1 Click **Interface Setup > Multi-WAN Config**. The Multi-WAN Config window opens.

STEP 2 To enable Connection Failover, select **Enabled**. When enabled, the SRP sets the interface to the highest priority.

NOTE Mobile Connection Mode must be set to **Auto** to use Connection Recovery. See **Mobile Network, page 46**.

STEP 3 Enter the **Failover Check Interval**, **Failover Ping Timeout**, and **Failover Retry** values.

STEP 4 Choose a site on which to perform failover validation. Select either **Gateway** (the default gateway for the interface) or enter the IP address for a **Custom** site.

STEP 5 To enable WAN Load Balancing, select **Enabled**. Load Balancing cannot be used if interface failover is enabled.

STEP 6 Specify the WAN interface priority and weight values as specified in the **Multi-WAN Configuration Settings** table.

STEP 7 Click **Submit** to save your settings.

Multi-WAN Configuration Settings

Failover	
Connection Failover	Ensures that the Internet connection is always connected through a stable WAN link. **Enabled**: When enabled, the SRP first establishes the highest priority WAN interface. If the validation site associated with the WAN is unreachable, the SRP tries to establish the interface default route for the next priority WAN if available, and changes the system default route to that WAN. Once the validation site associated with the higher priority WAN interface is reachable, the SRP changes the system default route back to the higher priority WAN interface and stops the lower priority WAN connection. **Disabled**: When disabled, all WAN interfaces try to establish the connection and the system default route is set to the highest priority WAN interface. During this time, WAN Load Balancing is configurable.
Failover Values	▪ **Failover Check Interval**: How often the SRP checks the status of the Internet connection. The is default is 60 seconds. ▪ **Failover Ping Timeout**: Maximum time allowed for verification response. The default is 5 seconds. ▪ **Failover Ping Retries**: Number of verification checks missed before failing over to the next available interface. The default is 1 second. ▪ **Failback after Check Interval Successes**: Number of successful verifications required on a restored interface, before traffic is rerouted back to it.

Multi-WAN Configuration Settings

Connection Validation Site	IP address used as a ping target for the SRP that detects the status of the Internet connection. Select either **Gateway** (interface default gateway) or enter the IP address for a **Custom** site.
WAN Interface	Shows information on the current status of the wired mobile network connections. Click the **Status** link to view the interface details or configure the interface priority by using the Priority drop-down list for each interface.
WAN Interface Detail	Shows detailed information about the WAN interfaces including Interface name, IP Address, Netmask, and Gateway IP address.
Load Balance	
WAN Load Balancing	Select **Enable** to enable WAN Load Balancing.The default is Disabled. When enabled, we recommend that you disable NAT. See **Network Address Translation, page 85**. Failover and Load Balancing cannot be enabled at the same time. Enabling Failover will overwrite Load Balancing.
Health Check	Select **Enable** to determine the health of the WAN interfaces. The default setting is Disabled. The SRP can monitor the validity of a link by sending ICMP packets to either the interface default gateway or custom remote gateway.
Health Check Time Interval	Enter the period that the SRP checks the health of the WAN interfaces. The default is 60 seconds.
Load Balance Control	Multi-WAN weights used by the WAN interface to balance outcoming traffic. The range is between 0 to 99. All WAN interfaces are given a default of one. If the value is zero, load balancing is not used.

Setting Up the VLAN Interfaces and LAN Ports

This section describes how to set up the SRP VLAN and LAN ports. It includes the following sections:

- **DHCP Server**
- **VLAN Settings**
- **Port Settings**
- **Spanning Tree Protocol**

To access these pages, click **Interface Setup > LAN** from the Configuration Utility.

DHCP Server

Use the DHCP Server page to create DHCP lease pools, reserve leases for specific hosts, define the default routing, and set the DHCP option values.

To configure the SRP as a DHCP server, you must first create a DHCP server from the DHCP Server page and then enable it by assigning it to a VLAN interface.

NOTE When creating a DHCP server, specify the IP address and subnet mask for the VLAN interface it is assigned to. Otherwise, the IP addressing options are configured directly through the VLAN settings.

STEP 1 Click **Interface Setup > LAN > DHCP Server**. The DHCP Server window opens.

STEP 2 From this page you can view, edit, or add a new DHCP entry.

- To view details for a DHCP entry, click the entry in the **DHCP List**. The information displays in the **DHCP Server Settings** table.
- To edit or delete a DHCP entry from the DHCP list, click the **Edit** (pencil) or **Delete** (x) icon.
- To create a new DHCP Server Pool, click **Add Entry**. The *DCHP Server* window for the new entry opens.

STEP 3 Configure the DHCP Server Settings as defined in the **DHCP Server Settings** table.

STEP 4 Click **Submit** to save your settings.

DHCP Server Settings

Router IP	
DHCP Name	Identifies this DHCP Server configuration and is used to assign the service to a VLAN interface.
Local IP Address/ Subnet Mask	IP address and subnet mask (8–32 bits), used to configure the VLAN interface to which this DHCP rule is applied.
DHCP Server Setting	
DHCP Mode	Choose the DHCP mode from the drop-down list. Select either **DHCP Server** or **DHCP Relay** mode. The DHCP Relay agent relays DHCP messages between DHCP servers on different IP networks. If you select this option, enter the **Remote DHCP Server** IP address where the DHCP messages will be sent. **NOTE** If you selected DHCP Relay mode, manually disable NAT for the VLAN being configured. Selecting DHCP Relay does not disable NAT automatically. To disable NAT entirely, see **Global Settings, page 86**. To disable NAT for specific VLANs, see **NAT Bypass, page 88**.
Remote DHCP Server	(DHCP Relay mode only) Sets the DHCP Server IP address that DHCP messages are relayed to.
IP Reservation	Shows or hides the DHCP Reservation information. Click this button to view or modify the reservations. Click it again to hide the reservations.
Select Clients from DHCP Tables	(option only appears if IP Reservations are shown) Shows the clients currently receiving IP addresses from the DHCP Server. To reserve the currently assigned IP address for exclusive use by a client, check the **Select** box and click the **Add Clients** button. The client appears in the Clients Already Reserved table.

DHCP Server Settings

Manually Adding Client	(option only appears if IP Reservations are shown) To reserve an IP address for a client, enter the client name and the IP address you want to reserve. Then enter the client MAC address and click **Add**. The client appears in the Clients Already Reserved table.
WAN Interface	Choose the WAN Interface from which the related DHCP information, specifically DNS, is obtained.
Default Gateway	Enter the IP address of the default gateway to be used by clients of this pool. If the field is 0.0.0.0. the VLAN Local IP Address is used as the default gateway.
Option 66	Provides provisioning server address information to hosts requesting this option. Server information is defined in one of three ways: ▪ **Local TFTP Server**: The SRP uses its own TFTP server to source provisioning files so it returns its own local IP address to the client. ▪ **Remote TFTP Server**: If the SRP was configured by using this method, it uses the server information it received through Option 66 on its WAN interface in response to local client requests. ▪ **Manual TFTP Server**: Allows the manual configuration of a configuration server address. While this option is typically used to provide either an IP address or a fully qualified hostname, the SRP can also accept and offer a full URL (protocol, path and filename) to meet the requirements of specific clients.
Option 67	Configuration/bootstrap filename. Used in conjunction with Option 66 to allow the client to form an appropriate TFTP request for the file.
Option 159	Configuration URL that defines the protocol and path information by using an IP address for clients that cannot use DNS. For example: **https://10.1.1.1:888/configs/bootstrap.cfg**

DHCP Server Settings

Option 160	Configuration URL that defines the protocol and path information by using a Fully Qualified Domain Name (FQDN) for clients that can use DNS. For example: **https://myconfigs.cisco.com:888/configs/bootstrap.cfg**
DNS Proxy	When enabled, local clients are offered the SRP Local IP Address to use for DNS requests. The SRP then proxies these requests to the DNS servers that it was configured with. See the note about DNS in **Internet Option, page 45**. When disabled, DHCP clients are offered DNS server information based on the following: ▪ If the Static DNS field is configured, then that server alone is offered to clients. ▪ If the Static DNS field is not configured, up to three servers are offered, first from the global Internet Options static configuration and then from the WAN interface nominated above.
Starting IP Address	IP address of the first address in this pool.
Maximum DHCP Users	Maximum number of devices that you want the DHCP server to assign IP addresses to. This number is affected by the subnet mask and starting IP address and cannot be greater than 1024. The default is 50.
Client Lease Time	Amount of time that an address is leased to a client. Enter the amount of time, in minutes, for the lease. The default is 0 minutes, which means one day. Enter **9999** to assign an infinite lease.
Static DNS	DNS server address that DHCP clients use directly for name resolution. This option is only required when DNS proxy is disabled for this DHCP server. This field is hidden when DNS proxy is enabled.
WINS (Window Internet Naming Service)	Manages the window's hostname to address resolution. When using a WINS server, enter the IP address of the server. Otherwise, leave this field blank.

NOTE The SRP DHCP server also offers domain information to clients, if available. Where multiple domain names are available to the SRP, the statically configured value (Internet Options) is used in preference to that learned from the system default route interface. Domain names learned on other WAN interfaces are not used for DHCP.

VLAN Settings

Use this page to configure the Virtual LAN (VLAN) interface settings.

STEP 1 Click **Interface Setup > LAN > VLAN Settings**. The VLAN Settings window opens. From this page you can view the list of configured VLANs, add or delete a VLAN, and view the details for a selected VLAN.

- To edit or delete a VLAN entry from the VLAN List, click the **Edit** (pencil) or **Delete** (x) icon.
- To view information for a VLAN (DHCP Server Pool) entry, click the entry in the VLAN List. Detailed information for the entry appears in the **VLAN Settings** table.
- To create a new VLAN, click **Add Entry**. The VLAN Settings window for the new VLAN opens.

STEP 2 Specify the VLAN settings for the new entry as defined in the **VLAN Settings** table.

STEP 3 Click **Submit** to save your settings.

VLAN Settings

VLAN List	▪ **Name**: The default is data_Lan and voice_Lan. ▪ **ID**: The default is data_Lan : 1 and voice_Lan : 100. ▪ **Address Type**: The default is data_Lan and voice_Lan : DHCP Server Pool. ▪ **Voice**: The default is data_Lan : disabled and voice_Lan : enabled. ▪ **Membership**: The default is data_Lan : LAN Port 1-4 and SSID1, 3, 4, voice_Lan : LAN Port 1-4 and SSID2.
VLAN Name	Enter a name for the VLAN.
VLAN ID	Enter an identification number for the VLAN.
Voice VLAN	Check this box if you want voice applications to use this VLAN. The default is data_Lan : disabled and voice_Lan : enabled. All traffic from a voice VLAN follows the voice default route specified in WAN interface configuration unless there is policy-based routing configured for the voice VLAN. Policy-based routing takes precedence over the default route. There are no implicit QoS settings for voice VLAN. You will need to create these accordingly.
Role	When bridging LAN ports with a WAN interface, the VLAN role will control how the associated IP interface is created. ▪ **LAN role**: Creates the IP interface, if required, as a LAN VLAN. VLANs created without WAN interfaces are automatically created with the LAN role. ▪ **WAN role**: Creates the IP interface as a subinterface of the selected Ethernet WAN. The resulting VLAN will be a Layer 2 broadcast domain on the outside of the firewall.

VLAN Settings

IPv4 Address Type	Determines the way that the VLAN IP interface is configured. ▪ Choose **None** if an IP interface is not required. This typically is the case when bridging ports only. ▪ Choose **Static IP Address** to manually define an address for the interface. ▪ Choose **Dynamic IP Address** to request an address from a DHCP server on the local network. ▪ Choose **DHCP server** to enable a previously configured DHCP Server service on this interface. In this case, the VLAN IP address is derived from the DHCP Server configuration.
Available Interface	Interfaces that are available to be added to the VLAN. To move an interface to the Added Interface list, click the interface, and then click the **right-arrow button (>)**. To move all of the interfaces at once, click the **double right-arrow button (>>)**.
Added Interface	Interfaces that were selected as members of the VLAN bridge. To remove an interface from this list, click the interface and then click the **left arrow button (<)**. To remove all of the interfaces at once, click the **double left-arrow button (<<)**.

Port Settings

Use the Port Settings page to set the VLAN port attributes, edit the port settings, or view the port settings.

STEP 1 Click **Interface Setup > LAN > Port Settings**. The Port Settings window opens.

STEP 2 Specify the flow control and speed duplex settings for LAN ports 1–4 as defined in the **Port Settings** table.

STEP 3 To view the port information, click any of the items in the Port List. Detailed information for the port displays in the **Port Settings** table.

STEP 4 To edit a port entry, click the **Edit** (pencil) icon. The VLAN Port Settings window opens.

STEP 5 Specify the port settings as defined in the **Port Settings** table.

STEP 6 Click **Submit** to save your settings.

Port Settings

Mode	The currently configured behavior of the port. ▪ **Desktop mode**: Provides attached devices with access to a single data VLAN for which the SRP provides services. All traffic will be untagged. ▪ **IP Phone + Desktop mode**: The port is configured with a data VLAN for native access and a voice VLAN for use with an attached IP phone. CDP is used to communicate voice VLAN information to the phone. This implies that there are only two VLANs associated with this port - one for data, which is the native VLAN, and the voice VLAN which is tagged only. ▪ **Switch/AP mode**: The port is configured to be part of multiple VLANs (any combination other than 1 data and 1 voice VLAN) for the purposes of trunking to either a switch or wireless access point. ▪ **Generic**: The port is configured for Layer 2 bridging mode only.
Enabled Flow Control	Mechanism for temporarily stopping the transmission of data on this physical interface. For example: A situation might arise where a sending station (computer) is transmitting data faster than some other part of the network (including the receiving station) can accept. The overwhelmed network element will send a PAUSE frame, which halts the transmission of the sender for a specified period of time. To enable this feature, check the **Enabled Flow Control** box. The default setting is Disabled.

Port Settings

Speed Duplex	Choose the duplex mode from the drop-down list. Select either **Auto-negotiate**, **10 Half**, **10 Full**, **100 Half** **100 Full**, **1000 Half**, or **1000 Full**. The default is Auto-negotiate.
Port Details	Shows detailed information for each configured port.

VLAN Port Settings

Port	Specify the quality of service trust settings for the port. The default setting is untrusted. ▪ **Untrusted**: If the port is not trusted, Ethernet traffic class of service will be re-marked with the configured priority setting. ▪ **Trust**: If the port is trusted, the incoming class of service markings are retained for queuing (which may or may not happen later on the packet's path through the router).
Port/Access VLAN	Select the native VLAN (PVID) for this port. The drop-down list includes all VLAN IDs that were configured on the VLAN Settings page.
Priority	Set a priority for unmarked, or untrusted traffic received on this port. By default, the priority is set to 0. A higher number indicates a higher priority.
Voice VLAN	When the VLAN mode is IP Phone + Desktop, the voice VLAN ID is shown. This value is informational only.

Spanning Tree Protocol

Use the STP page to configure settings for the Spanning Tree Protocol (STP). STP is a link-layer network protocol that ensures a loop-free topology for any bridged LAN. The basic function of STP is to prevent bridge loops and to ensure broadcast radiation.

STEP 1 Click **Interface Setup > LAN > STP**. The STP window opens.

STEP 2 To enable STP, select **Enabled**. The default is Disabled.

STEP 3 Specify the STP settings for LAN Ports 1-4 as follows:

- **Enabled STP**: Select which ports will participate in STP. Ensure that this setting is enabled for connections to switch trunks.
- **Path Cost**: If set to auto-detect, the SRP uses a path cost for the port based on its speed configuration. To override this value, uncheck the auto detect option and enter a value between 0 and 240.

STEP 4 If necessary, configure the STP advanced settings as defined in the **STP Settings** table.

STEP 5 Click **Submit** to save your changes.

NOTE Forward Delay, Hello Time, and Max Age are configuration settings sent by the root bridge to all other bridges to define the current STP configuration. If the SRP is not elected as the root, the active timer values might be different from those configured here. The time calculations are based on the IEEE 802.1D Standard that provides interoperability with legacy bridges. This is because timers are learned from the root bridge. A bridge will enforce the following relationship:

2 x (Forward_Delay - 1.0 seconds) >= Max_Age
Max_Age >= 2 x (Hello_Time + 1.0 seconds

STP Settings

Advanced Settings	
Bridge Priority	Used to influence which bridge becomes the STP root. The bridge with the lowest value in the network will be elected as the root. Valid Bridge Priorities range from 0 through 61440, in steps of 4096. The default value is 32768.
Forward Delay	Time spent in the listening and learning state. This time is equal to 15 seconds by default, but you can adjust the time to be between 4 and 30 seconds.
Hello Time	Time between each Bridge Protocol Data Unit (BPDU) that is sent by a bridge. This time is equal to 2 seconds by default, but you can adjust the time to be between 1 and 10 seconds.
Max Age	Timer that defines how long bridges will wait after receiving the last hello message before assuming that the Layer 2 topology has changed. At this point, the current spanning tree configuration is discarded and the new topology is discovered. This time is 20 seconds by default, but you can adjust the time to be between 6 and 40 seconds.

Setting Up the Wireless LAN

This section describes how to configure the wireless LAN settings for the SRP. It includes the following sections:

- **Basic Wireless Settings**
- **Wi-Fi Protected Setup**
- **Wireless MAC Filter**
- **Advanced Wireless Settings**
- **Wi-Fi Multimedia Setting**

To access these pages, click **Interface Setup > Wi-Fi Settings** from the Configuration Utility.

Basic Wireless Settings

Use the Basic Wireless Settings page to configure the SRP's integrated wireless access point and up to four wireless networks.

STEP 1 Click **Interface Setup > Wi-Fi Settings > Basic Wireless Settings**. The Basic Wireless Settings window opens.

STEP 2 Configure the wireless network settings as defined in the **Basic Wireless Settings** table. When you are finished, click **Submit** to save your settings.

STEP 3 Select the network mode to turn the radio on and click **Apply**.

NOTE The radio must be enabled to use the Wi-Fi Protected setup (WPS) feature.

STEP 4 Configure the network security settings for each SSID. In the Wireless Table area, click the **Edit** button in the Security column. The Wireless Security window opens.

STEP 5 Choose the security mode setting from the drop-down list. The default is Disabled.

When you enable security mode, a window opens that defines the security settings for that mode (authentication type, encryption, passphrase, and so on). Enter the security settings as defined in the **Basic Wireless Settings** table and then click **Submit** to save your settings.

> **NOTE** The default algorithm for both WPA and WAP2 security mode settings (Personal and Enterprise) is AES. Because AES is a stronger encryption method, we recommend that you use AES instead of TKIP whenever possible.

Basic Wireless Settings

Network Mode	Choose the wireless mode based on the type of devices in your network. **NOTE** The wireless access point is disabled by default to ensure network security. You must select an active network mode to enable it before configuring further. ▪ **Mixed:** Choose this option if you have Wireless-N, Wireless-G, and Wireless-B devices in your network. ▪ **BG-Mixed**: Choose this option if you have only Wireless-G and Wireless-B devices in your network. ▪ **Wireless-N Only:** Choose this option if you have only Wireless-N devices. ▪ **Wireless-G Only**: Choose this option if you have only Wireless-G devices. ▪ **Wireless-B Only**: Choose this option if you have only Wireless-B devices. ▪ **Disabled:** Choose this option if you don't want to use the integrated wireless access point.
Radio Band	Select the wireless bandwidth for your network. There are three options: Auto, Standard–20MHz Channel, and Wide-40MHz Preferred. The default is Standard–20MHz Channel. Wide channel band configuration is available for Wireless-N networks and clients only. If wide channel mode is selected for mixed networks, standard channel usage is still available for Wireless -B and -G clients.
Wide Channel	If you selected the Wide-40MHz channel for the Radio Band setting, then this setting will be available for your primary Wireless-N channel. Select a channel (3-9 for -A- models, 3-11 for -E- models) from the drop-down list. If radio band is selected automatically, the wide channel is also chosen automatically.

Basic Wireless Settings

Standard Channel	If you selected Wide-40MHz Preferred or Standard -20MHz Channel for the Radio Band setting, then this setting will be available. Select the channel for Wireless-N, Wireless-G, and Wireless-B networking. If you selected Wide-40MHz Preferred for the Radio Band setting, then the Standard Channel will be a secondary channel for Wireless-N. The default is Standard Channel 11 - 2.462 GHZ (Wide Channel 9). If radio band is selected automatically, the standard channel will also be chosen automatically.
Wireless Table	
Wireless Network Name (SSID)	Name of the network that clients use when connecting to the network. By default the wireless network is named “cisco-data” and is connected to the default VLAN. To rename the default wireless network, enter a unique Wireless Network Name, which is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). The second default wireless network has the default name “cisco-voice” and is bridged to the voice VLAN. To create a second wireless network, enter a unique Wireless Network Name in the SSID2 setting. To activate this network, select **Enabled Network**. **NOTE** Your ISP or ITSP may be responsible for controlling the SSID2 settings. Contact your ISP or ITSP for more information.
SSID1/2/3/4	Network name shared among all devices in a wireless network. The SRP can support up to four wireless networks. By default, the first and second wireless networks are enabled. For each wireless network, configure the Wireless Network Name (SSID), Broadcast Network Name, and Enable Network option. **NOTE** Guest Network uses SSID3. Do not use SSID3 if you intend to use this feature.

Basic Wireless Settings

Broadcast Network Name	When wireless clients survey the local area for available wireless networks, they detect the SSIDs that are broadcast by nearby wireless networks. To broadcast the SSID, keep the box checked. If you do not want to broadcast the SSID, uncheck the box. In this case, wireless users would have to know the SSID to associate with the network.
Enabled Network	To enable the wireless network, check the box. To disable the wireless network, uncheck the box.
WPS Hardware Button	Press the Wi-Fi Protected Setup button on the SRP front panel to associate the currently selected SSID. To use this this feature, the SSID must be enabled. Otherwise, it is grayed out. To enable WPS, see **Wi-Fi Protected Setup, page 71**. **NOTE** Wi-Fi Protected Setup does not support WPA and WPA2 Enterprise security modes.

Wireless Security Settings

To access, click the **Edit Security** button for any configured SSIDs.	
Security Mode	Choose a **Security Mode** for your wireless network. The SRP supports the WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, and WEP security modes. Wi-Fi Protected Access (WPA) is a stronger security standard than Wired Equivalent Privacy (WEP) encryption. If you do not want to use wireless security, keep the default setting, Disabled. We recommend that you use the highest level of security that is supported by your client wireless devices.
WEP Security Mode Settings	
WEP	Basic encryption method, which is not as secure as WPA. WEP may be required if your network devices do not support WPA.

Wireless Security Settings

Authentication Type	Choose **Auto** or **Shared Key** from the drop-down list. With the Auto setting, the network is open and any device can join the network with or without a shared key. Shared Key authentication requires that the client provides the key that you specify on this page.
Encryption	Select a level of WEP encryption, **64-bit 10 hex digits or 5 ASCII characters** (default) or **128-bit 26 hex digits or 13 ASCII characters**. Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance.
Passphrase	Enter a passphrase to automatically generate the WEP keys. Then click the **Generate** button. Valid keys appear.
Key 1-4	If you did not enter a passphrase, enter the WEP key(s) manually. If you chose 64-bit WEP encryption, the key must be exactly 5 ASCII or 10 hexadecimal characters in length. If you chose 128-bit WEP encryption, the key must be exactly 13 ASCII or 26 hexadecimal characters in length. Valid hexadecimal characters are “0” to “9” and “A” to “F”. **NOTE** The SRP supports a single WEP key for the access point. If multiple SSIDs are configured with WEP, they must share the same key.
TX Key	Select which TX (Transmit) Key to use. The default is 1.
WPA Personal Mode Settings	
WPA Personal	Provides stronger wireless security with advanced encryption (TKIP or AES).
WPA Algorithms	Supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **AES** or **TKIP**. The default is AES.
WPA Shared Key	Enter a passphrase of 8 to 63 characters.
Group Key Renewal	Enter an interval in seconds to specify how often the SRP changes the encryption keys. The default Group Key Renewal period is 3600 seconds, which is 1 hour.

Wireless Security Settings

WPA2 Personal Mode Settings	
WPA2 Personal	Provides strong wireless security with advanced encryption (AES or TKIP + AES).
WPA Algorithms	Supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **AES** or **TKIP + AES**. The default is AES.
WPA Shared Key	Enter a passphrase of 8 to 63 characters.
Group Key Renewal	Enter an interval in seconds to specify how often the SRP changes the encryption keys. The default Group Key Renewal period is 3600 seconds, which is 1 hour.
WPA and WPA2 Enterprise Settings **NOTE** Wi-Fi Protected Setup does not support WPA and WPA2 Enterprise security modes.	
WPA Enterprise	This option features WPA used in conjunction with a reachable RADIUS server. If you have two RADIUS servers, select one to be the primary server and specify a secondary server to use as a backup.
WPA2 Enterprise	This option features WPA2 used in conjunction with a reachable RADIUS server. If you have two RADIUS servers, select one to be the primary server and use the secondary server as a backup.
WPA Algorithms	WPA and WPA2 support two encryption methods, TKIP and AES, with dynamic encryption keys. Select the algorithm you want to use, **TKIP** or **AES**. The default is AES.
Primary RADIUS Server	**RADIUS Server:** Enter the IP address of the RADIUS server. **RADIUS Port:** Enter the port number of the RADIUS server. The default value is 1812. **Shared Secret:** Enter the key shared between the SRP and the server. The key can include 8 to 63 ASCII characters or 64 hexadecimal characters.

Wireless Security Settings

Secondary RADIUS Server	**RADIUS Server Address:** Enter the IP address of the RADIUS server. **RADIUS Port:** Enter the port number of the RADIUS server. **Shared Secret:** Enter the key shared between the SRP and the server. The key can include 8 to 63 ASCII characters or 64 hexadecimal characters.
Key Renewal Timeout	Enter an interval in seconds to specify how often the SRP changes the encryption keys. The default Group Key Renewal period is 3600 seconds, which is 1 hour. The range is 600 to 7200 seconds.

Wi-Fi Protected Setup

Use the Wi-Fi Protected Setup (WPS) page to automatically configure wireless security for your wireless networks.

NOTE Make sure that the WPS client device is located near the SRP during setup.

STEP 1 Click **Interface Setup > Wi-Fi Settings > Wi-Fi Protected Setup**. The Wi-Fi Protected Setup window opens.

STEP 2 To enable Wi-Fi Protected Setup for an individual SSID, choose the name of the wireless network that you want configure from the drop-down list. The default data SSID is cisco-data. The default voice SSID is cisco-voice.

NOTE Wi-Fi Protected Setup is disabled by default.

STEP 3 Choose a Wi-Fi Protected Setup method. For method descriptions, see **Wi-Fi Methods, page 72**. Use the method that applies to the client device that you are configuring.

STEP 4 After the setup is complete, the current Wi-Fi Protected status appears at the bottom of the page.

Wi-Fi Methods

There are three methods to configure Wi-Fi Protected Setup.

Wi-Fi Protected Setup Method 1

Use this method if your client device has a WPS button.

STEP 1 Click or press the **WPS** button on the client device.

STEP 2 Click the **WPS** icon on this page or press the WPS button on the SRP front panel, if it was associated with the currently selected SSID. See **Basic Wireless Settings, page 65**.

STEP 3 After the client device is configured, click **OK**. Then refer to your client device or its documentation for further instructions.

Wi-Fi Protected Setup Method 2

Use this method if your client device has a WPS PIN number.

STEP 1 Enter the PIN number in the field on this page and then click the **Register** button.

STEP 2 After the client device is configured, click **OK**. Then refer to your client device or its documentation for further instructions.

Wi-Fi Protected Setup Method 3

Use this method if your client device asks for the SRP's PIN number.

STEP 1 Enter the PIN number listed on this page. (It is also listed on the label on the bottom of the SRP).

STEP 2 After the client device is configured, click **OK**. Then refer to your client device or its documentation for further instructions.

Wireless MAC Filter

Use the Wireless MAC filter page to specify the MAC addresses of the wireless devices that are permitted access or are blocked by the SRP. Up to 32 permit/deny rules may be configured.

STEP 1 Click **Interface Setup > Wi-Fi Settings > Wireless MAC Filter**. The Wireless MAC Filter window opens.

STEP 2 From the Select a SSID drop-down list, choose the MAC filter settings to apply to the SSID. The default data SSID is cisco-data. The default voice SSID is cisco-voice.

STEP 3 To filter wireless users by MAC Address, either permitting or blocking access, select **Enable**. The default is Disable.

STEP 4 In the Access Restriction area, select either **Prevent** or **Permit**.

STEP 5 If Wireless MAC Filter is enabled, click the **Show Client List** button to open the Wireless Client List page. This page shows computers and other devices currently associated with the wireless network. The list can be sorted by Client Name, IP Address, MAC Address, and Status.

STEP 6 Select **Save to MAC Address Filter List** for any device you want to add to the list and click **Add**. To retrieve the most up-to-date information, click **Refresh**. To exit this page and return to the Wireless MAC Filter page, click **Close**.

NOTE You can filter wireless access by using the MAC addresses of the wireless devices transmitting within your network radius.

STEP 7 Click **Submit** to save your settings.

Wireless MAC Filter Settings

Wireless MAC Filter	
Select a SSID	Name of the wireless network that you want to configure. The default data SSID is cisco-data. The default voice SSID is cisco-voice.
Wireless MAC Filter	To filter wireless users by MAC Address, either permitting or blocking access, select **Enabled**. The default is Disable.
Access Restriction	
Prevent	Blocks wireless access from the clients listed in the MAC Address Table. This is the default setting.
Permit	Permits wireless access only from the clients listed in the MAC Address table.
Show Client List	Displays a list of computers and other devices that are connected to this wireless network. To add a client to the MAC Address Table, check the **Save to MAC Address Filter List** box and click **Add**. To hide the client list, click **Hide Client List**.
MAC Address Table	
01-32	Enter the MAC addresses of the devices whose wireless access that you want to block or allow.

Advanced Wireless Settings

Use the Wireless Settings page to configure advanced wireless functions for the SRP.

NOTE These settings should only be configured by an experienced administrator. Before you configure these settings, make sure that wireless is enabled on the SRP. See **Basic Wireless Settings, page 65**.

STEP 1 Click **Interface Setup > Wi-Fi Settings > Advanced Wireless Settings**. The Advanced Wireless window opens.

STEP 2 To configure the RTS Threshold, select an SSID from the drop-down list.

STEP 3 Enter a value in the RTS Threshold field. If you encounter inconsistent data flow, enter only minor reductions. The recommended default value is 2347.

STEP 4 Change any settings in the Global Settings area as defined in the **Advanced Wireless Settings** table.

STEP 5 Click **Submit** to save your settings.

Advanced Wireless Settings

Advanced Wireless Setup	
Select a SSID	Name of the wireless network that you want to configure. The default data SSID is cisco-data. The default voice SSID is cisco-voice.
RTS Threshold	The SRP sends Request to Send (RTS) frames to a receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. If you encounter inconsistent data flow, you can adjust this threshold. Only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The RTS Threshold value should remain at its default value of 2347.

Advanced Wireless Settings

Global Settings	
AP Isolation	Isolates all wireless clients and wireless devices from one another. Wireless devices will be able to communicate with the SRP but not with other wireless devices on the network. To use this function, select **Enabled**. AP Isolation is disabled by default.
Basic Rate	Series of rates at which the SRP can transmit. The SRP advertises its Basic Rate to the other wireless devices in your network so they know which rates will be used, and automatically selects the best rate for transmission. The default setting is Default, which allows the SRP to transmit at all standard wireless rates (1-2Mbps, 5.5Mbps, 11Mbps, 18Mbps, and 24Mbps). Other options are 1-2Mbps, for use with older wireless technology, and All, which allows the SRP to transmit at all wireless rates. The Basic Rate is not the actual rate of data transmission. To specify the SRP's rate of data transmission, configure the Transmission Rate setting.
Transmission Rate	Set the data transmission rate depending on the speed of your wireless network. Select from a range of transmission speeds, or select **Auto** for the SRP to automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback negotiates the best possible connection speed between the SRP and a wireless client. The default is Auto.
CTS Protection Mode	The SRP automatically uses CTS (Clear-To-Send) Protection Mode when your Wireless-N and Wireless-G products are experiencing severe problems and are not able to transmit to the SRP in an environment with heavy 802.11b traffic. This function boosts the SRP's ability to catch all Wireless-N and Wireless-G transmissions but can impact performance. The default is Auto.

Advanced Wireless Settings

DTIM Interval	Indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field that informs clients of the next window for listening to broadcast and multicast messages. When the SRP buffers these messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The range is 1 to 255, the default value is 1.
Fragmentation Threshold	Specifies the maximum size for a packet before data is fragmented into multiple packets. If a high packet error rate occurs, you can slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of 2346.
Beacon Interval	Indicates the frequency interval of the beacon. A beacon is a packet broadcast by the SRP to synchronize the wireless network. Enter a value between 40 and 3500 milliseconds. The default value is 100.
Power Control	Choose **high**, **middle**, or **low** to specify the range of the wireless network. The default is high, which is a normal power level.

Wi-Fi Multimedia Setting

Use the WMM Setting page to configure support for Wi-Fi Multimedia (WMM) devices on your network.

STEP 1 Click **Interface Setup > Wi-Fi Settings > WMM Setting**. The WMM Setting window opens.

STEP 2 If you have other devices on your network that support WMM, keep the default setting **Enabled**.

STEP 3 In the No Acknowledgement option, select **Enabled** to disable the acknowledgement feature, so that the SRP will not resend data if an error occurs. The default is Disabled.

STEP 4 Click **Submit** to save your settings.

Using the Management Interface

Use the Management Interface page to set the Loopback Interfaces, which can be used for routing updates and some protocols. You can set up to two loopback interfaces.

STEP 1 Click **Interface Setup > Management Interface**. The Management Interface window opens.

From this page you can view or edit the currently configured loopback interfaces.

STEP 2 To edit an interface, click the **Edit** (pencil) icon. The Manually Adding Loopback window opens.

STEP 3 Enter the IP address to use for the loopback interface. The address must not overlap with any other interface configured on the SRP.

NOTE The IP address used for the loopback interface assumes a subnet mask of 255.255.255.255.

STEP 4 Click **Submit** to save your settings.

5

Configuring the Network

This chapter describes how to configure the network settings for the Services Ready Platforms. It includes the following sections:

- **Routing**
- **Network Address Translation**
- **Quality of Service**
- **Firewall**
- **PPPoE Relay**
- **Dynamic DNS (IPv4)**
- **DMZ Configuration**
- **Internet Group Management Protocol**
- **Universal Plug and Play**
- **Cisco Discovery Protocol**
- **Guest Network**
- **DNS Spoofing**

To access these pages, click **Network Setup** from the Configuration Utility menu bar.

Routing

This section describes how to configure various types of routing on the SRP including:

- **Static Routes**
- **Routing Information Protocol**
- **Intervlan Routing**
- **Policy Routing (IPv4)**

To access these pages, click **Network Setup > Routing** from the Configuration Utility.

Static Routes

Use the Static Routes page to configure static routes for network traffic.

IPv4

STEP 1 Click **Network Setup > Routing > Static Routes > IPv4**. The Static Routes window opens. From this page you can add a route, edit a route, or view the existing routes from the Routing table.

STEP 2 To add a static route, Click **Add Entry.**

STEP 3 Enter the **Route Name**, **Destination**, and **Subnet Mask** for the specified network or host to which you want to assign a static route.

STEP 4 Enter the **Gateway** IP address that allows for contact between the SRP and the specified network or host, or choose the **Interface** for this route from the drop-down list.

STEP 5 Click **Submit** to save your changes.

NOTE To see the routing table for all specified routes, click the **Show Routing Table** button. To hide this information, click the button again.

Static Route IPv4 Settings

Enter Route Name	Name of the static route.
Destination	IP address of the network or host to which you want to assign a static route.
Subnet Mask	Determines which portion of an IP address is the network portion and which portion is the host portion.
Gateway	IP address of the gateway device that allows for contact between the SRP and the network or host.
Interface	Determines if the Destination IP Address is on the LAN and Wireless (internal wired and wireless networks), or on the Internet (WAN).
Show Routing Table	Displays the routing table for all specified routes.

Routing Information Protocol

Use the Routing Information Protocol (RIP) pages to configure dynamic routing on the SRP. You can enable this protocol to allow the specified interfaces to automatically adjust to physical changes in the network's layout and to exchange routing tables with other routers. The SRP determines the network packets' route based on the fewest number of hops between the source and destination.

Routing Information Protocol Next Generation (RIPng) is used for dynamic routing supporting for IPv6. You can enable this protocol to allow the specified interfaces to automatically adjust to physical changes in the network's layout and to exchange routing tables with other router. The router determines the network packets route based on the fewest number of hops between the source and destination. To enable the Dynamic Routing feature, select Enabled then enter the RIP settings, and enable RIP on the interfaces where you want to use this feature. To disable the Dynamic Routing feature for all data transmissions, use the default setting, Disabled.

RIP IPv4

STEP 1 Click **Network Setup > Routing > RIP > IPv4**. The IPv4 window opens.

STEP 2 To enable RIP (Dynamic Routing), select **Enabled**. The default is Disabled.

STEP 3 If RIP is enabled, select the RIP version and timeout values.

STEP 4 Select which networks will participate in the routing protocol either by **Interface** or by **Network** (IP address and subnet mask).

- If you selected RIP By Interface, specify the interface settings as defined in the **RIP IPv4 Settings** table below.
- If you selected RIP By Network, click the **Add Network** button and enter the **Network Address** and mask for the new entry.

STEP 5 Click **Submit** to save your settings.

RIP IPv4 Settings

RIP Version	To limit the types of packets that can be transmitted, choose **Version 1** or **Version 2**. Alternatively, choose **RIP v1/v2** to allow both Version 1 and Version 2 packets to be transmitted.

RIP IPv4 Settings

RIP Timer	Timers that regulate RIP performance. These include a routing-update timer, a route-timeout timer, and a route-flush timer. **Update**: Enter the rate at which the SRP sends routing updates. The default is 30 seconds. **Timeout**: Enter the rate at which the SRP expects to receive routing updates from each router in the routing table. The default is 180 seconds. If this value is exceeded, the route is declared unreachable. The route is not removed from the routing table until the route-flush timer expires. **Flush**: Enter the maximum period that the SRP waits for an update before removing a route from the routing table. The default is 120 seconds.
RIP By	Select either enable **RIP by Interface** or **RIP by Network**.
RIP List	Shows the RIP settings of all the SRP interfaces. If you selected RIP by Interface you can edit an interface by clicking the **Edit** (pencil) icon next to interface you want to change. **Interface:** Shows the type of interface. **RIP Enabled**: Indicates if RIP is enabled or disabled on the interface. Check the box to enable RIP. **Passive Mode**: All receiving packets are processed as normal and only sends multicast or unicast RIP packets to RIP neighbors. To select this mode, select **Enabled** from the RIP Config Edit window. **Authentication**: If you are sending and receiving RIP Version 2 packets, select a RIP authentication on an interface. The SRP supports two modes of authentication on an interface: Simple Password Authentication and MD5 Authentication. A simple or MD5 password can be any string up to 15 characters. You can use ASCII letters and numbers in addition to the . , -_ characters. **NOTE** RIP Version 1 does not support authentication.
RIP Network	If you enabled “RIP By Network” click the **Add Network** button and enter the IP address and subnet mask for the entry.

Intervlan Routing

Configuring VLANs helps control the size of the broadcast domain and keeps local traffic local. However, when an end station in one VLAN needs to communicate with an end station in another VLAN, intervlan communication is required. This communication is enabled by Intervlan Routing.

NOTE Intervlan Routing does not apply to the Guest VLAN if you configured wireless guest access.

STEP 1 Click **Network Setup > Routing > Intervlan Routing.** The Intervlan Routing window opens.

STEP 2 Intervlan Routing is enabled by default. To disable it, select **Disabled**.

STEP 3 Click **Submit** to save your changes if required.

Policy Routing (IPv4)

Use the Policy Routing page to route traffic according to the matching criteria. Traffic arriving at selected LAN interfaces is classified based on a set of prioritized rules and are routed to a chosen WAN interface accordingly.

STEP 1 Click **Network Setup > Routing > Policy Routing**. The Policy Routing window opens. From this page you can view, add, edit and prioritize routing rules.

STEP 2 To add a policy route, click **Add Entry**. The Policy Routing Rule add window for the new rule opens.

STEP 3 Define the matching criteria as defined in **Policy Routing Settings** table. Only configure the fields that are sufficient to classify the traffic correctly.

STEP 4 To disable this rule if the interface goes down, check the **Disable Rule** box. Disabling a rule allows the matching algorithm to select an alternative route in the event of a link failure. If you leave the rule enabled and a link failure occurs, matched traffic is discarded.

STEP 5 If required, adjust the priority of each rule to meet your specific matching requirements.

STEP 6 Click **Submit** to save your changes.

Policy Routing Settings

Incoming Interface	Specify which LAN interfaces will receive the incoming traffic from the Incoming Interface drop-down list. Select **Any** or one of the currently defined VLAN interfaces.
Source IP Address and Destination IP Address/Subnet Mask	Enter the **Source and Destination IP address** and corresponding subnet mask for which the rule will apply.
Port	Select the destination port that this rule will apply to. Any is the default setting. If you choose **Single** or **Range**, enter the port number or range of numbers in the appropriate fields.
Protocol	Restrict the IP protocol (**TCP** or **UDP**) for traffic matching, if required.
DSCP	Specify the **DSCP number** to match for this rule.
Route	Specify the WAN route to which matching traffic will be sent. Choose any configured **IPSec Tunnel**, **GRE Tunnel**, or **WAN Interface**.

Network Address Translation

This section describes how to configure the Network Address Translation (NAT) settings for the SRP. It includes the following sections:

- **Global Settings**
- **NAT Bypass**
- **Port Forwarding**
- **Port Range Triggering**

To access these pages, click **Network Setup > NAT** from the Configuration Utility.

Global Settings

Use the NAT page to enable or disable NAT routing, which allows the SRP to host your network connection to the Internet.

STEP 1 Click **Network Setup > NAT> NAT Setting**. The NAT Setting window opens.

STEP 2 NAT is enabled by default and applied to all traffic passing between LAN and WAN interfaces. To disable NAT entirely, click **Disabled**.

STEP 3 Specify the ALG Control settings as defined in the **ALG Settings** table. To enable an ALG, click **Enabled** next to the ALG that you want to use.

NOTE All ALGs (Application Level Gateways) are enabled by default.

STEP 4 Click **Submit** to save your settings.

ALG Settings

NAT	NAT is enabled by default (this is the recommended setting for an Internet access device). Select **Disabled** if the SRP will be used in a private network with other routers.
SIP ALG	When enabled, the ALG allows SIP traffic to pass through NAT by translating the embedded address and port information from the private inside network to the device's public IP address.
NetMeeting	Provides support for Microsoft Netmeeting and other H.323 applications through NAT by translating embedded address and port information.
RTSP ALG	Ensures that RTSP and RTP UDP streams pass through the NAT process.

ALG Settings

IRC ALG	Commonly-used extension to call Direct Client-to-Client Protocol (DCC). This enables users to send files to each other, and also chat to each other without the need of a server. DCC Sending is used anywhere that you send files over IRC. DCC Chat is most commonly used by Eggdrop bots. If you are using NAT, this extension enables you to send files and initiate chats. **NOTE:** You do not need this extension to retrieve files, initiate chats, or perform other tasks in IRC.

NAT Bypass

In many cases, using NAT for all LAN-to-WAN traffic is sufficient. In some cases, where multiple services are delivered via different logical or physical wide area connections, it may be necessary to translate addressing for some connections and route without translation for others.

The NAT bypass feature allows you to define exceptions to the global NAT function (see **Global Settings, page 86**), ensuring that traffic meeting specified criteria is routed without address translation.

STEP 1 Click **Network Setup > NAT> NAT Bypass**. The NAT Bypass window opens.

From this page you can view an existing policy, edit a policy, or add a new policy.

STEP 2 To add a new Policy, click **Add Policy**. The NAT Bypass window opens.

STEP 3 Enter a name for the new policy.

STEP 4 Select **Enabled** to activate the policy. The default is Disabled.

STEP 5 Specify the rule criteria by defining where the traffic to be routed is coming from (Inside Interface) and going to (Outside Interface).

NOTE Local traffic is matched when it comes from either a locally defined VLAN, a specific host IP address, or a local Indirect Network (an IP network reachable through another router connected to an SRP LAN).

STEP 6 Click **Submit** to save your settings.

STEP 7 The new policy appears in the Policy List table on the NAT Bypass page. Click the policy to see the policy details.

NAT Bypass Settings

Policy Details	
Policy Name	Enter a name for the new policy.
Enabled	Click **Enabled** to activate the policy.
Inside Interface	
VLAN Interface	Choose the **VLAN Interface** from which traffic to be routed will originate.

NAT Bypass Settings

Host IP Address	Define traffic by the source Host IP Address.
Indirect Network	Enter the source **IP Address** and **Subnet Mask** associated with the Indirect Network.
Outside Interface	
WAN Interface	Choose an available **WAN Interface** for the outside interface from the drop-down menu.
IP Address/Subnet Mask	Specify the destination **IP Address** and **Subnet Mask** to which traffic must be routed and not translated.

Port Forwarding

Use the Port Forwarding page if your local network hosts network services (Internet applications) such as web, email, FTP, video conferencing or gaming. For each service, Internet traffic is forwarded by application (IP port) to the Local servers that host these services.

Port Forwarding enables the SRP to route packets addressed to a WAN IP address for a specific application port or port range, to a device on the local area network. For example, if you have a web server on the SRP LAN, you can set up port forwarding for all requests to port 80 to be translated and sent to the internal web server IP address.

NOTE To ensure correct forwarding of traffic, local servers must either be configured with a static IP address, or be assigned a reserved IP address through DHCP. Use the **Interface Setup > LAN > DHCP Server** page to reserve IP addresses. See **DHCP Server, page 54**.

STEP 1 Click **Network Setup > NAT > Port Forwarding**. The Port Forwarding window opens. From this page you can view an entry, edit an entry, or add an entry for another network service.

STEP 2 To add a new entry, click **Add Entry**. The Manually Adding Port Forwarding window opens.

STEP 3 Enter the port forwarding settings as defined in **Port Forwarding Settings** table.

STEP 4 Click **Submit** to save your settings.

Port Forwarding Settings

Port Forwarding Type	Choose the type of port forwarding from the drop-down list. **Single Port Forwarding**: Forwards traffic for a specified port to the same port or to an alternative port on the target server in the LAN. **Port Range Forwarding:** Forwards traffic to a range of ports to the same ports on the target server in the LAN. Refer to the Internet application's documentation for the required ports or ranges.
Application Name	(Single port forwarding only) Choose a common application from the drop-down list, such as Telnet or DNS. To enter an application that is not on the list, choose **Add a new name**, and then enter the name of the new application.
Enter a Name	(Single port forwarding only) Enter the name of the new application.
WAN Interface Name	Select the WAN interface to which the traffic is initially addressed.
External Port	(Single port forwarding only) Enter the port number that external clients will use to set up a connection with the internal server.
Internal Port	(Single port forwarding only) Enter the port number that the SRP uses when forwarding traffic to the internal server. For simplicity, internal and external port numbers will often be the same, however, different external port numbers can be used to differentiate traffic of the same application type intended for different internal servers, or to promote privacy through the use of non-standard ports.

Port Forwarding Settings

Start-End Port	(Port range forwarding only) Enter the range of ports used by the server or Internet application. Enter the first port in the first box, and enter the final port in the second box to specify the range. Check the Internet application's documentation for more information. In this case, port numbers are not changed when forwarded to the internal server.
Protocol	Protocol(s) to be forwarded: **TCP**, **UDP**, or **Both**.
IP Address	IP address of the local server that will receive the forwarded traffic.
Enabled	Click **Enabled** to activate this forwarding rule. The default setting is unchecked (Disabled).

Port Range Triggering

Use the Port Range Triggering page to allow the SRP to monitor outgoing data for specific port numbers and to dynamically create a forwarding rule to direct returning traffic to the requesting local client.

Port Range Triggering does not require the local client to use a fixed IP address. Traffic for any given port can only be forwarded to one local client at a time.

STEP 1 Click **Network Setup > NAT> Port Range Triggering**. The Port Range Triggering window opens. From this page you can view the existing entries from the Port Range Triggering List and the view the details about a selected entry.

STEP 2 To add a new entry for port range triggering, Click **Add Entry**. The Port Range Triggering window for the new entry opens.

STEP 3 Enter the settings for port range triggering as defined in the **Port Range Triggering Status** table.

STEP 4 Click **Submit** to save your settings.

Port Range Triggering Status

Application Name	Enter a name to identify the application in the Port Range Triggering List.
WAN	Choose the **WAN** Interface through which the trigger ports will be detected.
LAN	Choose the **LAN** where the host computer is located and to which forwarded traffic will be directed.
Triggered Range	Enter the **starting** and **ending** port numbers of the triggered port range. When a local client makes an outbound connection to a port in this range, the SRP opens the ports that are specified in the Forwarded Range fields back to the originating client. Refer to the Internet application's documentation for the appropriate port numbers.
Forwarded Range	Enter the **starting** and **ending** port numbers of the forwarded port range. These ports are opened when an outbound connection is made to one of the ports specified in the Triggered Range fields. Refer to the Internet application documentation for the appropriate port numbers.
Protocol	Choose a protocol type from the down list (**TCP**, **UDP**, or **both**).
Enabled	Click **Enabled** to enable the applications that you defined. The default is disabled.

Quality of Service

This section describes how to configure quality of service (QoS) settings for the SRP. It includes the following sections:

- **QoS Bandwidth Control**
- **QoS Policy (IPv4)**
- **CoS To Queue**
- **DSCP To Queue**

To access these pages, click **Network Setup > QoS** from the Configuration Utility menu bar.

QoS Bandwidth Control

Use the QoS Bandwidth Control page to allow the SRP to rate limit upstream data transmissions to suit the broadband service.

STEP 1 Click **Network Setup > QoS > Bandwidth Control**. The QoS Bandwidth Control window opens.

STEP 2 Click **Enabled** next to the interface on which you want to enable bandwidth control. Uncheck the box to disable it. The default setting is Disabled.

STEP 3 To configure the available bandwidth for each physical interface, click the **Edit** (pencil) icon. The Bandwidth Shaping Control window opens.

STEP 4 Specify the bandwidth shaping control values as defined in the **Bandwidth Shaping Control Settings** table below.

STEP 5 Click **Submit** to save your settings.

Bandwidth Shaping Control Settings

Upstream Bandwidth	Enter the maximum available **Upstream Bandwidth** value for the connected broadband service. The default values are 100000 kbps for Ethernet interfaces, 1000 kbps for ADSL_PVC0/1/2/3 interfaces, 2000 kbps for 3G interfaces, and 100000 kbps for GE WAN interfaces. **NOTE** Setting this value higher than the available service bandwidth can result in traffic being dropped arbitrarily in the service provider's network.
Strict High Priority Queue	Enter the bandwidth required for strict priority traffic. Traffic from the strict queue within this rate is transmitted before that from any other queue. The range is 1–70000 kbps. The default is 128 kbps.
High, Medium, Normal, Low	Specify the relative priority, or weighting, of the high, medium, normal and low priority queues. The queue weighting determines the relative amount of bandwidth that traffic from each queue will be assured during busy periods. The bandwidth column provides an indication of this value allowing for the strict priority bandwidth. To adjust the relative weighting of the queues, click the plus **(+)** button and minus **(-)** buttons. The priority range is 1–99. In the absence of strict priority traffic, data from these queues are handled on a weighted round robin basis. The bandwidth values on this page indicate the minimum assured throughput available per queue under load. Higher rates of traffic are seen, when other queues are under utilized.

QoS Policy (IPv4)

Quality of service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as video conferencing.

Use the QoS Policy page to configure rules to classify, queue, and mark traffic passing from LAN to WAN interfaces. Various classification methods are provided to ensure that traffic can be prioritized appropriately.

STEP 1 Click **Network Setup > QoS > QoS Policy**. The QoS Policy window opens.

From this page you can view, add, and edit the QoS Policies. Click on any rule to see the detailed information about the policy.

STEP 2 To add a new policy, click **Add Entry**. The QoS Priority Setting window opens.

STEP 3 Choose the QoS category from the drop-down list (**Application**, **MAC Address**, **Ethernet Port**, **VLAN**, or **IP Address**).

STEP 4 Specify the policy settings for the particular category as defined in the **QoS Policy Settings: Classification** table below.

STEP 5 Choose the Queuing and Marking settings for this rule.

NOTE When setting the priority, do not set all applications to High. This defeats the purpose of allocating the available bandwidth.

STEP 6 Click **Submit** to save your settings.

QoS Policy Settings: Classification

Application Category	
Applications/ Name	Choose a standard application from the drop-down list. To enter an application not listed, choose **Add a New Application**, and then enter the name of the new application.
LAN	Choose the source LAN. Select **All** or one of the currently defined LAN interfaces.

QoS Policy Settings: Classification

Port Range	Enter the port, or range of ports, and protocol (**TCP**, **UDP**, or **both**) that define the required application. You can specify up to three port ranges per rule. Single ports can be defined by entering the same value for range start and end fields. Check the Internet application's documentation for more information.
MAC Address Category	
Name	Enter a name to describe this rule.
LAN	Choose the source LAN. Select **All** or one of the currently defined LAN interfaces.
MAC Address	Enter the **MAC Address** of the originating device in the following format: xx:xx:xx:xx:xx:xx
Ethernet Port Category	
Name	Enter a name to describe this rule.
LAN	Choose the source LAN.
Ethernet	Choose the source Ethernet port.
VLAN Category	
Name	Enter a name to describe this rule.
VLAN	Choose the source VLAN.
IP Address Category (IPv4)	
Name	Enter a name to describe this rule.
Destination IP Address	Enter the destination IP address that must be used to classify traffic.
Destination Mask	Enter the subnet mask for the destination address IP range.

QoS Policy Settings: Queuing

Priority	Choose the queuing priority for matched traffic: Strict, High, Medium, Normal, or Low.

QoS Policy Settings: Marking

Marking	Modifies the DiffServ or CoS field of the packet classified by this QoS policy rule (by Application port range, MAC, Ethernet port, VLAN and IP Address). To set or override QoS marking for traffic satisfying this rule, select **Enabled**. The default setting is Disabled which leaves the QoS markings unchanged. **CoS**: Enter the Ethernet Class of Service value between 0 and 7. This value is only valid for Ethernet WAN interfaces and ADSL PVCs configured for 802.1Q tagging. **DiffServ**: Enter the DiffServ Code Point (DSCP) values in hex. Values must be between 0x00 and 0xfc in multiples of 0x04 and are valid for all IP WAN interfaces. See the DiffServe mapping table.

DSCP Mappings

Hex	Decimal	DSCP Bits		Suggested Queue Map
0x00	0	000000	Default	Normal
0x20	8	001000	CS1	Low
0x28	10	001010	AF11	Low
0x30	12	001100	AF12	Low
0x38	14	001110	AF13	Low
0x40	16	010000	CS2	Low
0x48	18	010010	AF21	Normal
0x50	20	010100	AF22	Normal
Ox58	22	010110	AF23	Normal
0x60	24	011000	CS3	Normal
0x68	26	011010	AF31	Medium
0x70	28	011100	AF32	Medium

DSCP Mappings (Continued)

0x78	30	011110	AF33	Medium
0x80	32	100000	CS4	Medium
0x88	34	100010	AF41	Medium
0x90	36	100100	AF42	Medium
0x98	38	100110	AF43	Medium
0xa0	40	101000	CS5	Medium
0xB8	46	101110	EF	Strict
0xc0	48	110000	CS6	High
Oxe0		111000	CS7	High

CoS To Queue

Use the CoS To Queue page to queue traffic based on Ethernet Class of Service (CoS) settings.

STEP 1 Click **Network Setup > QoS > CoS To Queue**. The CoS To Queue window opens.

The priority values (0-7) are mapped to SRP's queue, where zero is the lowest and 7 is the highest. These numbers define the different type of services, such as video or voice.

The services are expressed through the 3-bit PCP field in an IEEE 802.1Q header added to the frame. The way traffic is treated when assigned to any particular class is undefined and left to the implementation. The IEEE has made some broad recommendations as defined in the **CoS to Queue Priority Values** table.

STEP 2 Change the priority for each VLAN CoS as necessary. Choose a **priority level** (Strict, High, Medium, Normal, or Low) from the drop-down list.

STEP 3 Click **Submit** to save your settings.

CoS to Queue Priority Values

PCP	Network Priority	Traffic Characteristics

CoS to Queue Priority Values

1	0 (Lowest)	Background
0	1	Best Effort
2	2	Excellent Effort
3	3	Critical Applications
4	4	Video, < 100 ms latency
5	5	Voice, < 10 ms latency
6	6	Internetwork Control
7	7 (Highest)	Network Control

DSCP To Queue

Use the DSCP to Queue page to queue traffic based on the Differentiated Services Code Point (DSCP) value in the incoming packet.

STEP 1 Click **Network Setup > QoS > DSCP To Queue**. The *DSCP To Queue* window opens.

STEP 2 Change the priority settings for each IP DiffServ value as necessary. Choose a **priority level** (Strict, High, Medium, Normal, or Low) from the drop-down list. The priority defines the traffic forwarding queue to which traffic with the given DSCP is mapped.

STEP 3 Click **Submit** to save your settings.

Firewall

This section describes how to configure the firewall settings for the SRP. It includes the following sections:

- **Firewall Filter**
- **IPv4 Internet Access Control**
- **IPv4 Advanced Firewall Settings**
- **PPPoE Relay**

To access these pages, click **Network Setup > Firewall** from the Configuration Utility.

Firewall Filter

Use the Firewall Filter page to enable WAN-to-LAN firewall protection filtering on the SRP. The firewall enhances network security and uses Stateful Packet Inspection (SPI) to analyze data packets entering your network.

STEP 1 Click **Network Setup > Firewall > Firewall Filter**. The Firewall window opens.

STEP 2 SPI firewall protection is enabled by default. To disable it, click **Disabled**.

STEP 3 Specify the Internet and Web Filter Options as specified in the **Firewall Filter Settings** table.

STEP 4 Click **Submit** to save your settings.

Firewall Filter Settings

SPI Firewall Protection	SPI firewall protection is enabled by default. To disable it, click **Disabled**.
Internet Filter Options	
Filter Anonymous Internet Requests	Prevents your network from being pinged or detected by other Internet users. It also hides your network ports. Both make it more difficult for outside users to enter your network. This filter is enabled by default. Select **Disabled** to allow anonymous Internet requests.
Filter Internet NAT Redirection	Prevents local clients from accessing local services through active port forwarding rules (that is, local clients cannot use the router's public IP address to access local services, as they might if they were connected through the Internet). This feature does not prevent a local client from accessing a local service directly by using private addressing. This filter is disabled by default. Select **Enabled** to filter Internet NAT redirection.
Filter IDENT (Port 113)	Prevents port 113 from being scanned by devices outside of your local network. Select **Enabled** to filter port 113, or **Disabled** to disable it.
Filter DoS Attack	Protects the SRP from Denial-of-Service attacks.
Web Filter Settings	
Proxy	Use of WAN proxy servers can compromise your network security. Enabling the proxy filter blocks access to any WAN proxy servers. To enable proxy filtering, check the **Proxy** box. This filter is disabled by default.
Java	Java is a programming language for websites. Filtering Java prevents access to Internet sites created by using this programming language. To enable Java filtering, check the **Java** box. This filter is disabled by default.
ActiveX	ActiveX is a programming language for websites. Filtering ActiveX prevents access to Internet sites that use this programming language. To enable ActiveX filtering, check the **ActiveX** box. This filter is disabled by default.

Firewall Filter Settings

Cookies	Cookies are blocks of data stored on your computer and used by Internet sites when you interact with them. To filter cookies, check the **Cookies** box. This filter is disabled by default.
Filter Port	Enter the HTTP port number that will be scanned when using any of the above filters. By default, this is set to port 80.

IPv4 Internet Access Control

Use the Internet Access Control page to configure rules for controlling user access to the Internet (LAN to WAN).

STEP 1 Click **Network Setup > Firewall > IPv4 > Internet Access Control**. The Internet Access Control window opens. From this window you can add a policy, edit a policy, and view an existing policy.

STEP 2 To add an Internet Access policy, click **Add Entry**. The Internet Access Control settings window for the new policy opens.

STEP 3 Enter a name for the Internet access policy.

STEP 4 Click **Enabled** to activate Internet Access Control. The default is Disabled.

STEP 5 You can apply the rule to all traffic by choosing **From All**, **To All**, or you can limit the rule to apply only to particular interfaces, such as From VLAN1 to WAN1

STEP 6 (Optional) Click **Show Edit List** to display the MAC Address, IP Address, and IP Address Range policies.

STEP 7 Under the Schedule area, select the days and times when you want this policy to be enforced. Select the individual days, or select **Everyday**. Enter a range of hours by specifying the start time (**From**) and the end time (**To**), or select **24 Hours**.

STEP 8 Select other blocking options as necessary as defined in the **Internet Access Control Settings** table.

STEP 9 Click **Submit** to save your settings.

Internet Access Control Settings

Enter Policy Name	Enter a name for the policy.
Status	To enable this policy, click **Enabled**. The default setting is Disabled
From, To	You can apply the rule to all traffic by choosing **From All**, **To All**, or you can limit the rule so that it applies only to particular interfaces, such as From VLAN1 to WAN1.
Applied PCs (Optional)	To apply the policy only to specified PCs, click the **Show Edit List** button. Then specify the individual PCs by entering the MAC address or the IP address. You can specify groups of PCs by entering up to two ranges of IP addresses.
Schedule	
Days	Choose the days when you want this policy to be enforced. Select either individual days (**Sun–Sat**) or **Everyday**. Enter a range of hours by specifying the start time (**From**) and the end time (**To**), or select **24 Hours**.
Times	Choose the times when you want this policy to be enforced. Enter a range of hours by specifying the start time (**From**) and the end time (**To**), or select **24 Hours**.
Action	
Blocking Everything	Check this box to block all Internet traffic that meets the criteria that you specified on this page. Uncheck it to choose one or more of the other filtering options.
Blocking by URL and Keyword	Check this box to prevent users from accessing specified URLs or URLs that contain specified keywords. You can enter up to four URLs and up to six keywords.
Blocking by Destination IP Address	Check this box to prevent users from accessing specified IP addresses. You can enter up to four IP addresses.

Internet Access Control Settings

Blocking by Application	Check this box to prevent users from accessing specified Internet services, such as FTP or Telnet (You can block up to three applications per policy.) From the Applications list, click the application that you want to block. Then click the right-arrow button **(>>)** to move the application to the Blocked List. To remove an application from the Blocked List, click it and then click the button left-arrow button **(<<)**.
Modify Application	If the application you want to block is not listed or you want to edit a service's settings, enter the application's name in the Application Name field. Enter its port range in the Port Range fields. Select its protocol from the Protocol drop-down list. Then click **Add Entry**. To modify a service, select it from the Application list. Change its name, port range, and/or protocol setting and then click the **Edit** (pencil) icon. To delete a service, select it from the Application list. Then click the **Delete** (x) icon.

IPv4 Advanced Firewall Settings

Use the Advanced Firewall Settings page to configure rules for controlling access from the Internet (WAN to LAN).

NOTE Up to 20 IPv4 Advanced Firewall rules may be configured.

STEP 1 Click **Network Setup > Firewall > IPv4 > Advanced Firewall Settings**. The Advanced Firewall Settings window opens. From this page you can add, edit, view and prioritize the existing rules from the Advanced Firewall Policy List. Click on any rule to see detailed information about the policy.

STEP 2 To add a new firewall rule, click **Add Entry**. The Advanced Firewall settings window for the rule opens

STEP 3 Enter the name for the new rule.

STEP 4 Click **Enabled** to activate the rule.

STEP 5 Specify the Interface settings, Source and Destination port information, Action, and Scheduling information as defined in the **Advanced Firewall Settings** table.

STEP 6 Click **Submit** to save your changes. The new rule is added to the Advanced Firewall Policy List on the Advanced Firewall Settings page.

Advanced Firewall Settings

Advanced Firewall Policy List	Lists the existing firewall rules and corresponding policy name, status, inside and outside interface, and priority status of each rule. Select the priority level for a rule from the Priority drop-down list to set the order that the rules are applied. The SRP will use the first rule matched to determine what action to take. When finished, click **Submit** to save your changes.
Policy Details	Shows the policy information for the selected rule.
Rule Name	Enter a name for the rule. You can enter up to 31 characters.
Status	Select **Enabled** to enable the rule. The default is Disabled.
IN Interface	Choose the incoming WAN interface **(IN Interface)** for this rule from the drop-down list. ALL WAN means that this rule is applied to traffic arriving on any WAN interface.
OUT Interface	Choose the outgoing LAN interface (**Out Interface)** for the firewall rule from the drop-down list. ALL LAN means that this rule is applied to traffic arriving on any LAN interface.
Source IP Address	Specifies a source IP address to match.
Source Subnet Mask	Defines the source IP address wildcard mask. Masks specify which bits are used and which bits are ignored. A mask of 255.255.255.255 indicates that all bits are important. A mask of 0.0.0.0 indicates that all bits will be ignored. This means that if you specify a destination IP address but the destination subnet mask is set to 0.0.0.0, the rule will regards it as a 0.0.0.0/0 (all) address.

Advanced Firewall Settings

Destination IP Address	Specifies a destination IP address to match.
Destination Subnet Mask	Defines the destination IP address wildcard mask. Masks specify which bits are used and which bits are ignored. A subnet mask of 255.255.255.255 indicates that all bits are important. A mask of 0.0.0.0 indicates that all bits will be ignored. This means that if you specify a destination IP address but the destination subnet mask is set to 0.0.0.0, the rule will regard it as a 0.0.0.0/0 (all) address.
Protocol	Specify the protocol for the firewall rule. Choose from **TCP**, **UP**, **ICMP**, or **Any**. The default is Any.
Source Port	Choose the TCP/UDP source port for the firewall from the drop-down list. The default is Any that means that the port will not be inspected. Choose from **Single** or **Range** to define the required port(s).
Destination Port	Choose the TCP/UDP destination port for the firewall rule from the drop-down list. The default is Any. Choose from **Single** or **Range** to define the required port(s).
Action	Choose **Deny** or **Permit** from the drop-down list to deny or permit traffic associated with the rule.
Schedule	Check **Everyday** to apply the firewall rule to all days of the week. Uncheck it to disable it.
Times	Specify the times when the rule will be applied. The default is 24 hours. To enter a specific time, select **Range** and enter the time (in 24-hour format) in the range fields.

PPPoE Relay

Use the PPPoE Relay page to set the PPPoE relay settings. The PPPoE Relay feature listens for PPP traffic on nominated LAN interfaces and forwards them to the nominated WAN. Frames received on the WAN are relayed back to the client that originated the session in the LAN.

STEP 1 Click **Network Setup > PPPoE Relay**. The PPPoE Relay window opens. From this page you view, edit, or add a new relay.

STEP 2 To add a PPPoE Relay, click **Add Entry**. The PPPoE Relay Add window opens.

STEP 3 To enable PPPoE Relay for the Internet side, click **Enabled**. The default is Disabled.

STEP 4 Select the **WAN Interface** for this rule. For example: WAN1 or WAN2.

STEP 5 Select the **LAN Interface** for this rule. For example: VLAN1 or VLAN100.

STEP 6 Click **Submit** to save your settings.

PPPoE Relay Settings

WAN interface	Select the **WAN Interface** for this rule.
LAN interface	Select the **LAN Interface** for this rule.
PPPoE Relay Status	Enables an L2TP Access Concentrator (LAC) to relay active discovery and service selection functionality for PPP over Ethernet (PPPoE over a Layer 2 Tunneling Protocol (L2TP) control channel, to an L2TP Network Server (LNS) or tunnel switch (multihop node). The relay functionality of this feature allows the LNS or tunnel switch to advertise the services it offers to the client, which provides end-to-end control of services between the LNS and a PPPoE client.

Dynamic DNS (IPv4)

Use the Dynamic DNS (DDNS) page to specify an Internet service that allows routers with nonstatic public IP addresses to be located by using Internet domain names. When assigned a new IP address, the SRP updates the DDNS service to ensure that its associated domain name resolves to this new value, which facilitates remote access.

NOTE To use DDNS, you must set up an account with either DynDNS.com or TZO.com.

STEP 1 Click **Network Setup > DDNS**. The DDNS window opens.

STEP 2 Choose a DDNS service from the drop-down list. Select either **DynDNS.org** or **TZO.com.** The window for the DDNS Service opens.

STEP 3 Enter the information for the service that you chose as specified in the **DDNS Service Settings** table.

STEP 4 Click **Submit** to save your settings.

DDNS Service Settings

DDNS Service	Choose the provider for your DDNS service from the drop-down list. Select either **DynDNS.org** or **TZO.com**. DDNS service is disabled by default. **NOTE** You must sign up for an account with either one of these providers before you can use this service.
DynDNS.org Settings	
User Name	Enter the username from DynDNS.org.
Password	Enter the password from DynDNS.org.
Host Name	Enter your hostname. For example: name.dyndns.org.
System	Select the DynDNS service that you use. Choose either **Dynamic**, **Static**, or **Custom**.
Mail Exchange (Optional)	Enter the address of your mail exchange server, so that email to your DynDNS address goes directly to your mail server.

DDNS Service Settings

Mail Exchange (Backup MX)	Allows the mail exchange server to be used as a backup. To enable this feature, select **Enabled**. If you are not sure which setting to use, keep the default setting, **Disabled**.
Wildcard	Allows you to use a wildcard value in the DDNS address. For example, if your DDNS address is *myplace.dyndns.org* and you enable a wildcard, you can also use *x.myplace.dyndns.org*, where *x* is the wildcard. To enable wildcards, select **Enabled**. If you have not subscribed to this service, or are unsure, keep the default setting, Disabled.
Internet IP Address	Displays your current IP address.
Status	Displays your DDNS status.
Update	To manually trigger an update, click the **Update** button
TZO.org Settings	
E-mail Address	Enter the email address for your TZO account.
TZO Key	Enter the key for your TZO account.
Domain Name	Enter your hostname. For example: name.dyndns.org.
Internet IP Address	Displays your current IP address.
Status	Displays your DDNS status.
Update	To manually trigger an update, click the **Update** button.

DMZ Configuration

Use the DMZ (Demilarized Zone) pages to set up full external access to local servers that run Internet services. The SRP offers two types of DMZ configuration: Software (or hosted) DMZ, which maps traffic for a public IPv4 address to a local privately addressed host, or Hardware DMZ, which uses a dedicated Layer 2 interface/network for IPv4 DMZ hosts to maximize protection for private LAN clients.

To access these pages click **Network Setup > DMZ** from the Configuration Utility.

Software DMZ

STEP 1 Click **Network Setup > DMZ > Software DMZ**. The Software DMZ window opens. From this page you can view any currently installed software DMZ's, view the DMZ status, edit a DMZ, and add a DMZ.

STEP 2 To add a software DMZ, click **Add Entry.** The DMZ Setting window for the new DMZ opens.

STEP 3 Software DMZ is enabled on creation by default. To disable it, select **Disabled**.

STEP 4 Specify the DMZ settings as defined in the **Software DMZ Settings** table.

STEP 5 Click **Submit** to save your settings.

Software DMZ Settings

Status	Software DMZ rule is enabled by default when created.
Public IP	Enter the Public IP address through which the DMZ server will be accessed. If the SRP WAN address will be used and this address is assigned dynamically by the service provider, enter 0.0.0.0 in this field. If using more than one WAN connection, create a separate DMZ host rule for each interface.
Private IP	Enter the **Private IP** address. This is the server's private IP address on the LAN that corresponds to the Public IP address.

Software DMZ Settings

WAN Interface	Choose a **WAN interface** type from the drop-down list. This is the WAN interface that this DMZ matching will bind to.

Hardware DMZ

Use the Hardware DMZ page to configure LAN port 4 for public access to the customer's web and other servers that are accessible from the Internet. The other LAN network ports on the SRP will continue to be used for private internal traffic.

NOTE This feature can only be used with Ethernet encapsulated WAN interfaces (that is, Ethernet or EoA), PPP, PPTP, L2TP, or IPoA WAN interfaces cannot be used.

STEP 1 Click **Network Setup > DMZ > Hardware DMZ**. The Hardware DMZ window opens. From this page you can enable the Hardware DMZ feature, and add, view, or modify public addresses that will be passed in to the hardware DMZ.

Click **Add Entry** to create public IP addresses that will be forwarded to the DMZ.The DMZ Setting page for the new Hardware DMZ appears.

NOTE The Hardware DMZ feature itself is disabled by default. Individual address entries are enabled on creation by default.

STEP 2 Click **Submit** to save your settings.

Hardware DMZ Settings

Status	DMZ entries are enabled by default. When enabled, LAN port 4 will act as DMZ port. When disabled, it acts as a normal LAN port for private internal traffic and the hardware DMZ feature is disabled.
Public IP	Enter a **Public IP** address equal to the server IP address that is the behind the hardware DMZ port.
WAN Interface	From the WAN interface drop-down list, choose the **WAN interface** that this address will bind to

Internet Group Management Protocol

Use the IGMP page to configure settings for the Internet Group Management Protocol (IGMP) protocol. IGMP is a signaling protocol that supports IP multicasting for IPTV. For example, use IGMP if you have Internet Protocol Television (IPTV) with multiple setup boxes on the same local network that have different video streams running simultaneously.

STEP 1 Click **Network Setup > IGMP**. The IGMP window opens.

STEP 2 To allow multicast traffic through the SRP for your multimedia application devices, use the default setting, **Enabled**.

STEP 3 Select the version you want to support, **IGMP v1** or **IGMP v2.** If you are not sure which version to select, use the default setting, IGMP v2.

STEP 4 Choose the **WAN interface** that IGMP service will bind to (Auto, Ether_WAN1, USB_3G, or Ether_WAN2).

STEP 5 Enable **Immediate Leave** if you use IPTV applications and want to allow channel swapping or flipping without lag or delays. Otherwise, keep the default setting, Disabled.

STEP 6 Click **Submit** to save your settings.

IGMP Settings

IGMP Proxy	To Enable the IGMP Proxy, select **Enabled**. This allows multicast traffic to pass through the SRP for multimedia application devices.
Support IGMP Version	Choose the IGMP version from the drop-down list. Select either **IGMP v1** or **IGMP v2**. If you are not sure which version to select, keep the default setting, IGMP v2.
WAN Interface	Choose the **WAN interface** that the IGMP service will bind to. IGMP only can support one dedicated WAN interface at a time. The default AUTO setting allows the SRP to follow the current system default route for multicast forwarding.

IGMP Settings

Immediate Leave	Select **Enabled** if you use IPTV applications and want to allow channel swapping or flipping without lag or delays. Otherwise, keep the default setting, Disabled.

Universal Plug and Play

Use the UPnP page to enable the UPnP protocol. The Universal Plug and Play (UPnP) protocol allows local devices to discover the SRP to control certain configurations.

STEP 1 Click **Network Setup > UPnP**. The UPnP window opens.

STEP 2 UPnP is enabled by default. To disable it, select **Disabled**.

STEP 3 Configure the UPnP settings as defined in the **UPnP Settings** table.

STEP 4 Click **Submit** to save your settings.

UPnP Settings

UPnP	UPnP is enabled by default. To disable it, select **Disabled**.
Allow Users to Configure	When enabled (default), local clients can use UPnP to change the SRP configuration and behavior. If you only want to allow clients to discover the SRP using UPnP, select **Disabled**.
Keep UPnP Configurations After System Reboot	When enabled, the SRP saves the configuration changes made by clients over a system reboot. The default is Disabled.

Cisco Discovery Protocol

Use the CDP page to specify the Cisco Discovery Protocol (CDP) settings on your network. CDP is a link-level device discovery protocol available on many Cisco products. Each CDP-enabled device sends periodic messages to a multicast address and also listens to the periodic messages sent by others to learn about neighboring devices.

STEP 1 Click **Network Setup > CDP Setting**. The CDP Setting window opens.

You can enable CDP on some, all, or none of the SRP Ethernet interfaces. We recommend the default setting, Per Port, that enables CDP on LAN ports only. Enabling CDP is not recommended on the WAN port because it is connected to an insecure network.

STEP 2 Specify the CDP Timer values and port participation as defined in the **Cisco Discovery Protocol** table.

STEP 3 Click **Submit** to save your settings.

CDP Settings

CDP	Enables or disables CDP. You can enable CDP on some, all, or none of the SRP Ethernet interfaces. CDP per port is the default setting (recommended).
CDP Timer	Specify the interval at which successive CDP packets can be sent. Enter a value between 5 and 900 seconds. The default is 60 seconds.
CDP Hold Timer	Use the CDP Hold Timer to specify the amount of time the receiving device should hold a Cisco Discovery Protocol (CDP) packet from your router before discarding it. Enter a value between 10 to 255 seconds. The default value is 80 seconds and should be set to a value higher than the CDP transmit timer.
Interface List	Check the **Enable** box to select which interfaces will run CDP.

Guest Network

Use the Guest Network settings pages to configure a guest network on the SRP. A guest network allows users to securely connect to the Internet without accessing your private network.

This section includes the following topics:

- **Basic Configuration**
- **Configuring the User Account**
- **Customizing the Welcome Page**

Basic Configuration

Use the Basic Configuration page to configure the network settings for the guest network.

Before you configure the Guest Network, do the following:

Enable the wireless network. Wireless is disabled by default. To enable it, go to the **Interface Setup > Wi-Fi Settings > Basic Wireless Settings** page and configure the security settings for private access. We recommend using WPA2 security with AES encryption because it is more secure and less vulnerable to attacks. For configuration information, see **Basic Wireless Settings, page 65**.

Verify that SSID3 is not in use. When Guest Network is enabled, SSID3 is associated automatically with the Guest Network VLAN. If SSID3 is currently being used you will need to reassign it to a different SSID.

STEP 1 Click **Network Setup > Guest Network > Basic Configuration**. The Basic Configuration window opens.

The first time you configure the Guest Network, a precheck is performed to verify that all conditions are met to create a guest network. Before continuing, make sure that you back up your current configuration and then click **Yes** to proceed.

STEP 2 Select **Enabled** to enable the Guest Network. The default is Disabled.

STEP 3 Specify the network settings as defined in the **Guest Network Basic Configuration** table below.

STEP 4 Click **Submit** to save your settings.

.

Guest Network Basic Configuration

Feature	Click **Enabled** to create a Guest Network.The default is Disabled.
Network	Specify the Guest Network subnet address.
Default Lease Time	Enter the amount of time (global setting) that the user can be connected to the Guest Network. The range is 1 to 168 hours. The default is 24 hours.
Start lease from	Specify the time when the lease begins. You can choose from when the guest first logs in (**First Login**), or when the guest account is first created (**Account Creation**).
Auto Redirect URL	Click **Enabled** to automatically redirect the guest to the URL specified in the Redirect URL field (next field below)
Redirect URL	Specify the URL of the web page that the client first sees when logging into the guest network, such as their company home page.

Configuring the User Account

Use the User Account page to configure a Guest Network user account on the SRP. You can configure up to 50 guest user accounts, with each user being able to connect up to three devices using a single account.

The maximum number of active guest sessions depend on the SRP model. The SRP520W-U models will allow up to 25 guest devices to be associated at any time. The SRP540W models support up to 50 concurrent devices.

STEP 1 Click **Network Setup > Guest Network > User Account**. The User Account window opens.

From this page, you can add a new guest account, edit, or delete an account, or export a list of your existing accounts to a text file.

STEP 2 To add a guest account, click **Add Account**. The Guest Network Account window opens.

STEP 3 Specify the guest account settings as defined in the **Guest Network User Account** table below.

STEP 4 Click **Submit** to save your changes

Guest Network User Account

Account	Enter a name for the guest account. This name is case sensitive and can only contain letters, numbers, "@", or ".".
Password	Click the **Generate** button to create a random password for this user. This is a 6-digit numeric password that must be generated.
Lease Time	Specify how long the user can access the Internet through the guest network. To enter another time, click **Other**. The range is 1 to 168 hours. **NOTE:** After the lease time expires, the user account is deleted and any associated devices will be dropped from the wireless network.

Customizing the Welcome Page

You can customize a user's login page in any language by configuring the Welcome page from the Guest Network portal.

STEP 1 Click **Network Setup > Guest Network > Welcome Page.** The Welcome Page window opens.

Specify the welcome page settings as defined in the **Guest Network Welcome Page** table below. This is the page that the user will see when they log into the guest network.

STEP 2 After you are finished, click **Submit** to save your changes.

When the user logs into to their Welcome page, their custom Welcome page opens.

- If Auto Redirect URL is enabled, the guest's browser is directed to the URL specified in the Basic Configuration Settings window.

- If Auto Direct URL is disabled, the Guest Network Login Information window opens that shows the guest username and remaining lease time.

Guest Network Welcome Page

Company Title	Company name that appears on the left side of the Guest Network user login page.
Welcome Title	Welcome message that appears on left side of the Guest Network user login page
Username Title	Label for the username field that appears on right side of the Guest Network login page. The default title is Username.
Password Title	Label for the password field that appears on the right side of the Guest Network login page. The default title is Password.
Login Button Title	Label for the button that appears on the Guest Network login page, used to log into the guest network. The default title is Login.
Agree Title	Agree text used in the declaration statement that appears on the Guest Network login page. The default text is "I agree to the conditions of use."
Logout Info Title	Descriptive title for the Guest Network Information Logout page.
Logout Button Title	Label for the button that appears on the Guest Network Login Information page, used to log out of the guest network. The default title is Logout.
Time Left Title	Shows the remaining time that the user has left on the guest network before being disconnected (appears on the Guest Network Login Information page).
Copyright	Copyright that appears on the bottom left of the Guest Network login page.
Title Font Color	Font color that appears on the Guest Network login and logout pages. Select either **White** or **Black**.

Guest Network Welcome Page

Error 1, Error 2, and Error 3	Messages that appear on the Guest Network if an error occurs. To change a message, enter the new text under the applicable error field and then click **Submit**.
Upload Files	Allows you to upload and change the background image and logo that appear on the Guest Network login page. Only JPEG and GIF image files are allowed. The maximum file size for the background image is 256 KB. The maximum size for the logo is 10 KB Click **Browse** to locate the file and then click **Upload** to to add the new image. **NOTE** If you upload a graphic file, the image status changes from Default to Customize.
Declaration	Click **Enabled** to display the declaration (legal) statement and agree check box on the Guest Network login page. The default is Disabled. When enabled, the declaration appears in the scrolling text box underneath. To add a carriage return to text, use the HTML tag. For example: aaabr >bbbb

DNS Spoofing

Use the DNS Spoofing to set up DNS Spoofing service on the SRP. DNS spoofing is a service that supplements the DNS proxy feature, by allowing the SRP to intercept DNS requests from local clients, and to respond directly by using locally configured hostname to address mapping information.

IPv4

STEP 1 Click **Network Setup > DNS Spoofing > IPv4**. The IPv4 window opens. From this window you can view existing entries from the DNS Spoofing List and add a new DNS spoofing entry.

STEP 2 Click **Enabled** to enable DNS spoofing.

STEP 3 To add a new entry, click **Add Entry**. The DNS Spoofing Add window opens.

STEP 4 Enter the Host Name and IPv4 address.

STEP 5 Click **Submit** to save your changes.

6

Configuring Voice

This chapter describes how to configure voice settings and voice services for the Services Ready Platforms. It includes the following sections:

- **Configuring Voice Services**
- **Configuring Voice Settings**

NOTE The voice feature only supports IPv4 and the voice services must be bound to an IPv4 WAN interface.

Configuring Voice Services

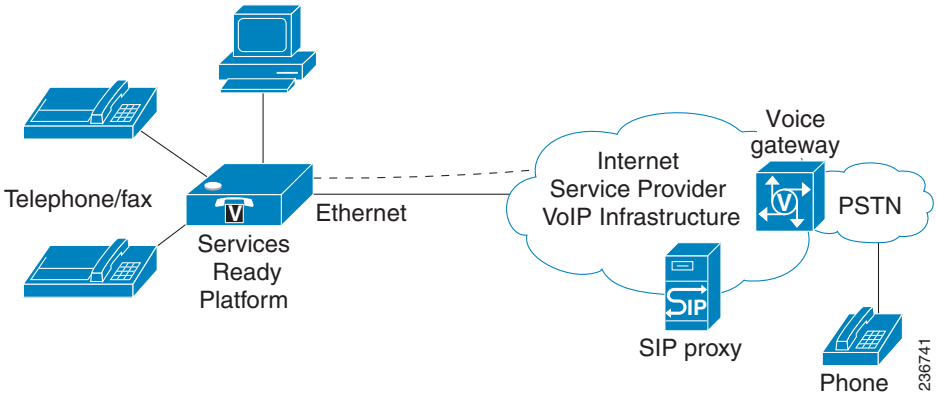
This section describes how to configure your SRP to meet the customer's requirements for voice services. It includes the following topics:

- **Understanding Voice Port Operations**
- **Managing Caller ID Services**
- **Configuring Dial Plans**
- **Secure Call Implementation**

Understanding Voice Port Operations

The SRP has a number of voice ports that allow calls to be made from locally connected analog handsets or fax machines by using SIP-based Internet phone services. In addition to the handset (FXS) ports, the SRP also has a single line (FXO) port that can be used to place calls to the telephone network in the event of broadband or even SRP failure.

The SRP's FXO port is mainly used as a backup if a registration failure occurs, if the network is disconnected, or if the SRP power is down. For the SRP520 Models, calls cannot be routed dynamically to this interface under normal operating conditions but can for the SRP540 Models. See settings on the **Voice> PSTN** page.



The SRP maintains the state of each call made through the FXS interface and makes the proper reaction to user input events (such as on/off hook or hook flash). Because the SRP uses the Session Initiation Protocol (SIP), it is compatible with most Internet Telephony Service Provider offerings.

SRP Voice Features

The SRP is equipped with fully featured, programmable voice ports that can be custom provisioned within a wide range of configuration parameters. The following sections describe the factors that contribute to voice quality:

- **Supported Codecs**
- **SIP Proxy Redundancy**
- **Other SRP Voice Features**

Supported Codecs

The SRP voice ports support the following codecs:

Codec	Description

G.711 (A-law and mu-law)	Very low complexity codecs that support uncompressed 64 kbps digitized voice transmissions at one through ten 5 ms voice frames per packet. These codecs provide the highest narrow-band voice quality and uses the most bandwidth of any of the available codecs.
G.726-32	Low complexity codec that supports compressed 32 kbps digitized voice transmission at one through ten 10 ms voice frames per packet. This codec provides high voice quality.
G.729a	ITU G.729 voice coding algorithm used to compress digitized speech. G.729a is a reduced complexity version of G.729 requiring about half the processing power of G.729. The G.729 and G.729a bit streams are compatible and interoperable, but not identical.

The administrator can select the preferred codecs to be used for each line. See **Audio Configuration, page 205**.

In addition, negotiation of the optimal voice codec sometimes depends on the ability of a device to match a codec name with the codec used by the far-end device. You can individually name the various codecs so that the SRP can successfully negotiate the codec with the far-end equipment. For more information, see **Audio Configuration, page 205.**

SIP Proxy Redundancy

In typical commercial IP telephony deployments, all calls are established through a SIP proxy server. A typical SIP proxy server can handle thousands of subscribers. It is important that a backup server be available so that an active server can be temporarily switched out for maintenance. The SRP supports the use of backup SIP proxy servers (through DNS SRV) so that service disruption is minimized.

An easy way to support proxy redundancy is to configure your DNS server with a list of SIP proxy addresses. The SRP can be instructed to contact a SIP proxy server in a domain named in the SIP message. The SRP consults the DNS server to get a list of hosts in the given domain that provides SIP services. If an entry exists, the DNS server returns an SRV record that contains a list of SIP proxy servers for the domain, with their host names, priority, listening ports, and so on. The SRP tries to contact the list of hosts in the order of their stated priority.

If the SRP is currently using a lower priority proxy server, it periodically probes the higher priority proxy to see whether it is back on line, and switches back to the higher priority proxy when possible. SIP Proxy Redundancy is configured in the Line pages (1–4) in the Services Ready Platform Configuration Utility. See **Line Pages (1–4), page 191**.

Other SRP Voice Features

The following table summarizes other voice features provided by the SRP.

Feature	Description
Silence Suppression	Voice Activity Detection (VAD) with Silence Suppression is a means of increasing the number of calls supported by the network by reducing the average bandwidth required for a single call. VAD uses a sophisticated algorithm to distinguish between speech and non-speech signals. Based on the current and past statistics, the VAD algorithm decides whether or not speech is present. If the VAD algorithm decides speech is not present, the silence suppression and comfort noise generation is activated. This is accomplished by removing and not transmitting the natural silence that occurs in normal two-way connection. The IP bandwidth is used only when someone is speaking. During the silent periods of a telephone call, additional bandwidth is available for other voice calls or data traffic because the silence packets are not being transmitted across the network. Comfort Noise Generation provides artificially-generated background white noise (sounds), designed to reassure callers that their calls are still connected during silent periods. If Comfort Noise Generation is not used, the caller may think the call has been disconnected because of the “dead silence” periods created by the VAD and Silence Suppression feature.

Feature	Description
Modem and Fax Pass-Through	Modem passthrough mode can be triggered only by predialing the number set in the Modem Line Toggle Code. See **Regional Page, page 170**. **FAX pass-through mode** is triggered by the detection of a CED/CNG tone or an NSE event. **Echo canceller** is automatically disabled for Modem passthrough mode. **Echo canceller** is disabled for fax passthrough if the parameter FAX Disable ECAN (Line 1 or 2 tab) is set to "yes" for that line (in that case FAX passthrough is the same as modem pass-through). **Call waiting and silence suppression** is automatically disabled for both fax and modem passthrough. In addition, out-of-band DTMF transmission is disabled during modem or fax passthrough.
Adaptive Jitter Buffer	The SRP can buffer incoming voice packets to minimize the impact of variable network delays. This process is known as jitter buffering. The size of the jitter buffer adapts reactively to suit changing network conditions. The SRP has a Network Jitter Level control setting for each line of service. The jitter level determines how aggressively the SRP tries to shrink the jitter buffer over time to achieve a lower overall delay. If the jitter level is higher, it shrinks more gradually. If jitter level is lower, it shrinks more quickly. Adaptive Jitter Buffer is configured in the Line pages. See **Line Pages (1–4), page 191**.

Feature	Description
International Caller ID Delivery	In addition to support of the Bellcore (FSK) and Swedish/ Danish (DTMF) methods of Caller ID (CID) delivery, the SRP provides a large subset of ETSI-compliant methods to support international CID equipment. International CID is configured from the PSTN page. See **PSTN Page (SRP540 Models Only), page 212**.
Secure Calls	A user (if enabled by service provider or administrator) has the option to make an outbound call secure in the sense that the audio packets in both directions are encrypted.
Adjustable Audio Frames Per Packet	This feature allows the user to set the number of audio frames contained in one RTP packet. Packets can be adjusted to contain from 1–10 audio frames. Increasing the number of packets decreases the bandwidth utilized, but it also increases delay and may affect voice quality. RTP packets are configured in the SIP page. See **SIP Page, page 153**.
DTMF Relay	The SRP may relay DTMF digits as out-of-band events to preserve the fidelity of the digits. This can enhance the reliability of DTMF transmission required by many IVR applications such as dial-up banking and airline information. DTMF Relay is configured in the DTMF TX Mode parameter in the Line pages. See **Line Pages (1–4), page 191**.
Call Progress Tones	The SRP has configurable call progress tones. Call progress tones are generated locally on the SRP so that an end user is advised of status (such as ringback). Parameters for each type of tone (for instance a dial tone played back to an end user) may include frequency and amplitude of each component, and cadence information. The Call Progress tones are configured in the Regional page, See **Regional Page, page 170**.
Call Progress Tone Pass Through	This feature allows the user to hear the call progress tones (such as ringing) that are generated from the far-end network.

Feature	Description
Echo Cancellation	Impedance mismatch between the telephone and the IP Telephony gateway phone port can lead to near-end echo. The SRP has a near-end echo canceller that compensates for impedance match. The SRP also implements an echo suppressor with Comfort Noise Generator (CNG) so that any residual echo is not noticeable. Echo Cancellation is configured from the Line pages. See **Line Pages (1–4), page 191**.
Signaling Hook Flash Event	The SRP can signal hook flash events to the proxy during a connected call. This feature can be used to provide advanced mid-call services with third-partycall control. Depending on the features that the service provider offers using third-party call control, the following ATA features may be disabled to correctly signal a hookflash event to the softswitch: **Call Waiting Service**: Refers to the call waiting serv parameter in the Line pages) **Three Way Conference Service**: Refers to the three-way conf serv parameter in the Line pages) **Three Way Call Service**: Refers to the three-way call serv parameter in the Line pages) You can configure the length of time allowed for detection of a hook flash using the Hook Flash Timer parameter on the Regional page. See **Regional Page, page 170**.

Feature	Description
Configurable Dial Plan with Interdigit Timers	The SRP has three configurable interdigit timers: **Initial timeout (T)**: Signals that the handset is off the hook and that no digit has been pressed yet. **Long timeout (L)**: Signals the end of a dial string; that is, no more digits are expected. **Short timeout (S)**: Used between digits; that is after a digit is pressed a short timeout prevents the digit from being recognized a second time. See **Configuring Dial Plans, page 135** for more information.
Polarity Control	The SRP allows the polarity to be set when a call is connected and when a call is disconnected. This feature is required to support some pay phone system and answering machines. Polarity Control is configured in the Line pages. See **Line Pages (1–4), page 191**.
Calling Party Control	Calling Party Control (CPC) signals to the called party equipment that the calling party has hung up during a connected call by removing the voltage between the tip and ring momentarily. This feature is useful for auto answer equipment, which then knows when to disengage. CPC is configured in the Regional page. See **Regional Page, page 170.**
Report Generation and Event Logging	The SRP reports a variety of status and error reports to assist service providers to diagnose problems and evaluate the performance of their services. The information can be queried by an authorized agent, using HTTP with digest authentication, for instance. The information may be organized as an XML page or HTML page. Report Generation and Event Logging are configured from the System page. See **System Page, page 152**.

Feature	Description
Syslog and Debug Server Records	Syslog and Debug Sever Records list more details than Report Generation and Event Logging. Using the configuration parameters, the SRP allows you to select which type of activity/ events should be logged. Syslog and Debug Server allow the information captured to be sent to a Syslog Server. Syslog and Debug Server Records are configured from the System page. See **System Page, page 152.**
SIP Over TLS	The SRP allows the use of SIP over Transport Layer Security (TLS). SIP over TLS is designed to eliminate the possibility of malicious activity by encrypting the SIP messages between the service provider and the end user. SIP over TLS relies on the widely-deployed and standardized TLS protocol. SIP Over TLS encrypts only the signaling messages and not the media. A separate secure protocol such as Secure Real-Time Transport Protocol (SRTP) can be used to encrypt voice packets. SIP over TLS is configured in the SIP Transport parameter configured in the Line pages. See **Line Pages (1–4), page 191.**

Registering to the Service Provider

To use an Internet phone service, you must register your SRP to the Internet Telephony Service Provider (ITSP).

NOTE Each line tab must be configured separately. Each line tab can be configured for a different ITSP.

STEP 1 Log in to the Configuration Utility. If prompted, enter the administrative logon provided by the Service Provider. The default username and password are both **admin**.

STEP 2 Under the Voice menu, select the **Line** Interface that you want to modify.

STEP 3 In the Proxy and Registration section, enter the Proxy.

STEP 4 In the Subscriber Information section, enter the User ID and Password.

These are the minimum settings for most ITSP connections. Enter the account information as required by your ITSP.

STEP 5 Click **Submit** to save your settings. The voice service will restart.

STEP 6 To verify your progress, perform the following tasks:

a. From the Voice navigation pane, click **Info**. Scroll down to the **Line** section of the page for the line you configured. Verify that the line is registered.

b. Use an external phone to place an inbound call to the telephone number that was assigned by your ITSP. Assuming that you have left the default settings in place, the phone should ring and you can pick up the phone to get two-way audio.

c. If the line is not registered, you may need to refresh the browser several times because it can take a few seconds for the registration to complete. Also verify that DNS is configured properly.

Managing Caller ID Services

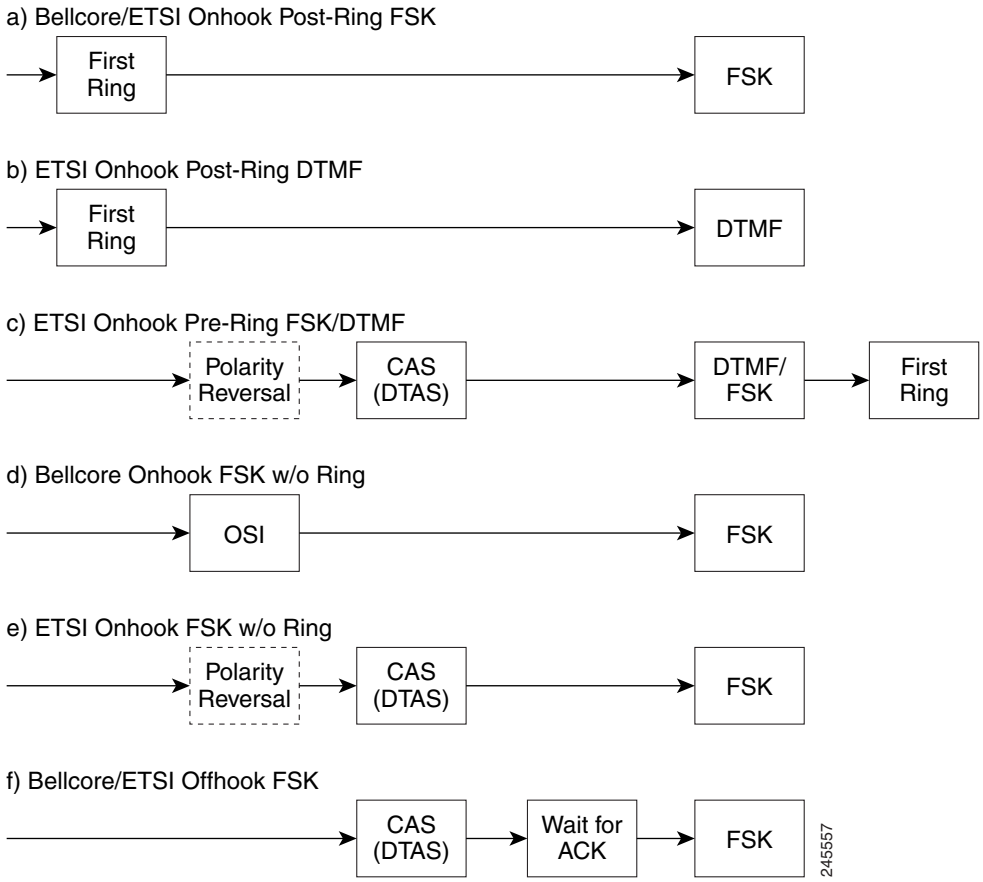
The choice of Caller ID (CID) method is dependent on your area/region. This option is located on the **Voice > Regional** page under the Miscellaneous area. To configure CID, use the following parameters.

Caller ID Method
Bellcore (North America, China)—CID, CIDCW, and VMWI. FSK sent after first ring (same as ETSI FSK sent after first ring) (no polarity reversal or DTAS). This is the default setting.
DTMF (Finland, Sweden)—CID only. DTMF sent after polarity reversal (and no DTAS) and before first ring.
DTMF (Denmark)—CID only. DTMF sent before first ring with no polarity reversal and no DTAS.
ETSI DTMF—CID only. DTMF sent after DTAS (and no polarity reversal) and before first ring.

Caller ID Method
ETSI DTMF With PR—CID only. DTMF sent after polarity reversal and DTAS and before first ring.
ETSI DTMF After Ring—CID only. DTMF sent after first ring (no polarity reversal or DTAS).
ETSI FSK—CID, CIDCW, and VMWI. FSK sent after DTAS (but no polarity reversal) and before first ring. Waits for ACK from CPE after DTAS for CIDCW.
ETSI FSK With PR (UK)—CID, CIDCW, and VMWI. FSK is sent after polarity reversal and DTAS and before first ring. Waits for ACK from CPE after DTAS for CIDCW. Polarity reversal is applied only if equipment is on hook.
DTMF (Denmark) With PR—CID only. DTMF sent after polarity reversal (and no DTAS) and before first ring.
Caller ID FSK Standard
The SRP supports bell 202 and v.23 standards for caller ID generation. Select the FSK standard that you want to use, bell 202 or v.23. The default is bell 202.

There are three types of Caller IDs:

- **On Hook Caller ID Associated with Ringing**—Type of Caller ID is used for incoming calls when the attached phone is on hook. See the following figure (a) – (c). All CID methods can be applied for this type of CID.
- **On Hook Caller ID Not Associated with Ringing**—Used to send VMWI signal to the phone to turn the message waiting light on and off (see the figure). This is available only for FSK-based CID methods: (Bellcore, ETSI FSK, and ETSI FSK with PR).
- **Off Hook Caller ID**—Used to deliver caller ID on incoming calls when the attached phone is off hook (see the following figure). This can be call-waiting caller ID (CIDCW), or to notify the user that the far end party identity has changed or been updated (such as due to a call transfer). This is available only for FSK-based CID methods: (Bellcore, ETSI FSK, and ETSI FSK with PR).


a) Bellcore/ETSI Onhook Post-Ring FSK
First Ring
FSK
b) ETSI Onhook Post-Ring DTMF
First Ring
DTMF
c) ETSI Onhook Pre-Ring FSK/DTMF
Polarity Reversal
CAS (DTAS)
DTMF/ FSK
First Ring
d) Bellcore Onhook FSK w/o Ring
OSI
FSK
e) ETSI Onhook FSK w/o Ring
Polarity Reversal
CAS (DTAS)
FSK
f) Bellcore/ETSI Offhook FSK
CAS (DTAS)
Wait for ACK
FSK
245557

Optimizing Fax Completion Rates

Issues can occur with fax transmissions over IP networks, even with the T.38 standard, which is supported by the SRP. You can adjust several settings on your SRP to optimize your fax completion rates.

STEP 1 Ensure that you have enough bandwidth for the uplink and the downlink.

- For G.711 fallback, it is recommend to have approximately 100 kbps.
- For T.38, allocate at least 50 kbps.

STEP 2 To optimize G.711 fallback fax completion rates, set the following on the Line tab of your SRP:

- **Network Jitter Buffer**: very high
- **Jitter buffer adjustment**: disable
- **Call Waiting**: no
- **3 Way Calling**: no
- **Echo Canceller**: no
- **Silence suppression**: no
- **Preferred Codec**: G.711
- **Use pref. codec only**: yes

NOTE If you are using a Cisco media gateway for PSTN termination, disable T.38 (fax relay) and enable the fax using modem pasthrough. For example:

```
modem passthrough nse payload-type 110 codec g711ulaw
fax rate disable
fax protocol pass-through g711ulaw
```

STEP 3 Enable T.38 fax on the SRP by configuring the following parameter on the Line tab for the FXS port to which the FAX machine is connected:

```
FAX_Passthru_Method: ReINVITE
```

If a T.38 call cannot be setup, then the call automatically reverts to G.711 fallback.

STEP 4 If you are using a Cisco media gateway use the following settings. Make sure that the Cisco gateway is correctly configured for T.38 with the SRP dialpeer. For example:

```
fax protocol T38
```

```
fax rate voice
fax-relay ecm disable
fax nsf 000000
no vad
```

Fax Troubleshooting

If you have problems sending or receiving faxes, complete the following steps:

STEP 1 Verify that your fax machine is set to a speed between 7200 and 14400.

STEP 2 Send a test fax in a controlled environment between two SPRs.

STEP 3 Determine the success rate.

STEP 4 Monitor the network and record the statistics for Jitter, Loss, and Delay.

STEP 5 If faxes fail consistently, capture a copy of the SRP configuration by downloading the following file. You can then send this file to Technical Support.

```
http://<SRP_IP_Address>/admin/
config.xml&xuser=admin&xpassword=<admin_password>
```

If you are using a web browser, choose the option to **view source** for the resulting page and save this file locally.

STEP 6 Enable and capture the debug list.

NOTE You can also capture data using a sniffer trace.

STEP 7 Identify the type of fax machine connected to the device.

STEP 8 Contact technical support:

- If you are an end user of VoIP products, contact the reseller or Internet telephony service provider (ITSP) that supplied the equipment.
- If you are an authorized Cisco partner, contact Cisco technical support at: www.cisco.com/support.

Configuring Dial Plans

Dial plans determine how dialed digits are interpreted and transmitted. They also determine whether the dialed number is accepted or rejected. You can use a dial plan to facilitate dialing or to block certain types of calls such as long distance or international. This section includes information that you need to understand dial plans, as well as procedures for configuring your own dial plans.

This section includes the following topics:

- **About Dial Plans**
- **Editing Dial Plans**

About Dial Plans

This section provides information to help you understand how dial plans are implemented. See the following topics:

- **Digit Sequences**
- **Digit Sequence Examples**
- **Acceptance and Transmission the Dialed Digits**
- **Dial Plan Timer (Off-Hook Timer)**
- **Interdigit Long Timer (Incomplete Entry Timer)**
- **Interdigit Short Timer (Complete Entry Timer)**

Digit Sequences

A dial plan contains a series of digit sequences, separated by the quote character. The entire collection of sequences is enclosed within parentheses. Each digit sequence within the dial plan includes a series of elements, which are individually matched to the keys that the user presses.

NOTE White space is ignored, but may be used for readability.

Digit Sequence	Function
0 1 2 3 4 5 6 7 8 9 0 * #	Enter any of these characters to represent a key that the user must press on the phone keypad.

Digit Sequence	Function
x	Enter `x` to represent any character on the phone keypad.
[sequence]	Enter characters within square brackets to create a list of accepted key presses. The user can press any one of the keys in the list. Numeric range: For example, you would enter `[2-9]` to allow the user to press any one digit from 2 through 9. Numeric range with other characters: For example, you would enter `[35-8*]` to allow the user to press 3, 5, 6, 7, 8, or *.
. (period)	Enter a period for element repetition. The dial plan accepts zero or more entries of the digit. For example, `01.` allows users to enter 0, 01, 011, 0111, and so on.
<dialed:substituted>	Use this format to indicate that certain dialed digits are replaced by other characters when the sequence is transmitted. The dialed digits can be zero or more characters. **EXAMPLE 1**: `<8:1650>xxxxxxx` When the user presses 8 followed by a seven digit number, the system automatically replaces the dialed 8 with 1650. If the user dials **85550112**, the system transmits **16505550112**. **EXAMPLE 2**: `<:1>xxxxxxxxxx` In this example, no digits are replaced. When the user enters a 10-digit string of numbers, the number 1 is added at the beginning of the sequence. If the user dials **9725550112**, the system transmits **19725550112.**

Digit Sequence	Function
, (comma)	Enter a comma between digits to play an “outside line” dial tone after a user-entered sequence. **EXAMPLE:** `9, 1xxxxxxxxxx` An “outside line” dial tone is sounded after the user presses 9, and the tone continues until the user presses 1.
! (exclamation point)	Enter an exclamation point to prohibit a dial sequence pattern. **EXAMPLE:** `1900xxxxxxx!` The system rejects any 11-digit sequence that begins with 1900.
*xx	Enter an asterisk to allow the user to enter a 2-digit star code.
S0 or L0	Enter S0 to reduce the short inter-digit timer to 0 seconds, or enter L0 to reduce the long inter-digit timer to 0 seconds.

Digit Sequence Examples

The following examples show digit sequences that you can enter in a dial plan.

In a complete dial plan entry, sequences are separated by a pipe character (|), and the entire set of sequences is enclosed within parentheses.

EXAMPLE: `([1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

Extensions on your system

`EXAMPLE: ( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

[1-8]xx Allows a user dial any three-digit number that starts with the digits 1 through 8. If your system uses four-digit extensions, you would instead enter the following string: **[1-8]xxx**

Local dialing with seven-digit number

```
EXAMPLE: ( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx |
9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]111)
```

9, xxxxxxx After a user presses 9, an external dial tone sounds. The user can then dial any seven-digit number, as in a local call.

Local dialing with 3-digit area code and a 7-digit local number

EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

9, <:1>[2-9]xxxxxxxxx This example is useful where a local area code is required. After a user presses 9, an external dial tone sounds. The user must enter a 10-digit number that begins with a digit 2 through 9. The system automatically inserts the 1 prefix before transmitting the number to the carrier.

Local dialing with an automatically inserted 3-digit area code

EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

8, <:1212>xxxxxxx This example is useful where a local area code is required by the carrier but the majority of calls go to one area code. After the user presses 8, an external dial tone sounds. The user can enter any seven-digit number. The system automatically inserts the 1 prefix and the 212 area code before transmitting the number to the carrier.

U.S. long distance dialing

EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

9, 1 [2-9] xxxxxxxxx After the user presses 9, an external dial tone sounds. The user can enter any 11-digit number that starts with 1 and is followed by a digit 2 through 9.

Blocked number

EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

9, 1 900 xxxxxxx ! This digit sequence is useful if you want to prevent users from dialing numbers that are associated with high tolls or inappropriate content, such as 1-900 numbers in the U.S. After the user press 9, an external dial tone sounds. If the user enters an 11-digit number that starts with the digits 1900, the call is rejected.

U.S. international dialing

EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

9, 011xxxxxx. After the user presses 9, an external dial tone sounds. The user can enter any number that starts with 011, as in an international call from the U.S.

Informational numbers

EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

0 | [49]11 This example includes two digit sequences, separated by the pipe character. The first sequence allows a user to dial 0 for an operator. The second sequence allows the user to enter 411 for local information or 911 for emergency services.

Acceptance and Transmission the Dialed Digits

When a user dials a series of digits, each sequence in the dial plan is tested as a possible match. The matching sequences form a set of candidate digit sequences. As more digits are entered by the user, the set of candidates diminishes until only one or none are valid. When a terminating event occurs, the SRP either accepts the user-dialed sequence and initiates a call, or else rejects the sequence as invalid. The user hears the reorder (fast busy) tone if the dialed sequence is invalid.

The following table explains how terminating events are processed.

Terminating Event	Processing
The dialed digits do not match any sequence in the dial plan.	The number is rejected.

Terminating Event	Processing
The dialed digits exactly match one sequence in the dial plan.	If the sequence is allowed by the dial plan, the number is accepted and is transmitted according to the dial plan. If the sequence is blocked by the dial plan, the number is rejected.
A timeout occurs.	The number is rejected if the dialed digits are not matched to a digit sequence in the dial plan within the time specified by the applicable interdigit timer. The Interdigit Long Timer applies when the dialed digits do not match any digit sequence in the dial plan. The default value is 10 seconds. The Interdigit Short Timer applies when the dialed digits match one or more candidate sequences in the dial plan. The default value is 3 seconds.
The user presses the # key.	If the sequence is complete and is allowed by the dial plan, the number is accepted and is transmitted according to the dial plan. If the sequence is incomplete or is blocked by the dial plan, the number is rejected.

Dial Plan Timer (Off-Hook Timer)

You can think of the Dial Plan Timer as the “off-hook timer.” This timer starts counting when the phone goes off hook. If no digits are dialed within the specified number of seconds, the timer expires and the null entry is evaluated. Unless you have a special dial plan string to allow a null entry, the call is rejected. The default value is 5.

Syntax for the Dial Plan Timer

SYNTAX: `(Ps<:n> | dial plan )`

- s: The number of seconds; if no number is entered after `P`, the default timer of 5 seconds applies.
- n: (optional): The number to transmit automatically when the timer expires; you can enter a valid number. No wildcard characters are allowed because the number will be transmitted as shown. If you omit the number

substitution, <:n>, then the user hears a reorder (fast busy) tone after the specified number of seconds.

Examples for the Dial Plan Timer

- **Allow more time for users to start dialing after taking a phone off hook.**

  EXAMPLE: `(P9 | (9,8<:1408>[2-9]xxxxxx | 9,8,1[2 9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)`

  `P9` After taking a phone off hook, a user has 9 seconds to begin dialing. If no digits are pressed within 9 seconds, the user hears a reorder (fast busy) tone. By setting a longer timer, you allow more time for users to enter the digits.

- **Create a hotline for all sequences on the System Dial Plan**

  EXAMPLE: `(P9<:23> | (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)`

  `P9<:23>` After taking the phone off hook, a user has 9 seconds to begin dialing. If no digits are pressed within 9 seconds, the call is transmitted automatically to extension 23.

- **Create a hotline on a line button for an extension**

  EXAMPLE: `(P0 <:1000>)`

  With the timer set to 0 seconds, the call is transmitted automatically to the specified extension when the phone goes off hook. Enter this sequence in the Phone Dial Plan for Ext 2 or higher on a client station.

Interdigit Long Timer (Incomplete Entry Timer)

You can think of this timer as the “incomplete entry” timer. This timer measures the interval between dialed digits. It applies as long as the dialed digits do not match any digit sequences in the dial plan. Unless the user enters another digit within the specified number of seconds, the entry is evaluated as incomplete, and the call is rejected. The default value is 10 seconds.

NOTE This section explains how to edit a timer as part of a dial plan. Alternatively, you can modify the Control Timer that controls the default interdigit timers for all calls. See **Resetting the Control Timers, page 143**.

Syntax for the Interdigit Long Timer

SYNTAX: `L:s, ( dial plan )`

s: The number of seconds; if no number is entered after `L:`, the default timer of 5 seconds applies. The timer sequence appears to the left of the initial parenthesis for the dial plan.

Example for the Interdigit Long Timer

EXAMPLE: `L:15, (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)`

`L:15,` This dial plan allows the user to pause for up to 15 seconds between digits before the Interdigit Long Timer expires.

Interdigit Short Timer (Complete Entry Timer)

You can think of this timer as the "complete entry" timer. This timer measures the interval between dialed digits. It applies when the dialed digits match at least one digit sequence in the dial plan. Unless the user enters another digit within the specified number of seconds, the entry is evaluated. If it is valid, the call proceeds. If it is invalid, the call is rejected. The default value is 3 seconds.

Syntax for the Interdigit Short Timer

SYNTAX 1 : `S:s, ( dial plan )`

Use this syntax to apply the new setting to the entire dial plan within the parentheses.

SYNTAX 2 : *sequence* `Ss`

Use this syntax to apply the new setting to a particular dialing sequence.

s: The number of seconds; if no number is entered after `S`, the default timer of 5 seconds applies.

Examples for the Interdigit Short Timer

- Set the timer for the entire dial plan.

  EXAMPLE: `S:6,(9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)`

  `S:6,` While entering a number with the phone off hook, a user can pause for up to 15 seconds between digits before the Interdigit Short Timer expires.

- Set an instant timer for a particular sequence within the dial plan.

  EXAMPLE: `(9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxS0 | 9,8,011xx. | 9,8,xx.|[1-8]xx)`

  `9,8,1[2-9]xxxxxxxxxS0` With the timer set to 0, the call is transmitted automatically when the user dials the final digit in the sequence.

Editing Dial Plans

You can edit dial plans and can modify the control timers.

Entering the Line Interface Dial Plan

This dial plan is used to strip steering digits from a dialed number before it is transmitted out to the carrier.

STEP 1 Log in to the Configuration Utility. If prompted, enter the administrative logon provided by the Service Provider. The default username and password are both **admin**.

STEP 2 Under the Voice menu, select the Line interface that you want to modify.

STEP 3 Scroll down to the Dial Plan section.

STEP 4 Enter the digit sequences in the **Dial Plan** field. For more information, see **About Dial Plans, page 135**.

STEP 5 Click **Submit** to save your settings.

Resetting the Control Timers

You can use the following procedure to reset the default timer settings for all calls.

NOTE To edit a timer setting only for a particular digit sequence or type of call, you can edit the dial plan. See **About Dial Plans, page 135**.

STEP 1 Log in to the Configuration Utility. If prompted, enter the administrative logon provided by the Service Provider. The default username and password are both **admin**.

STEP 2 Under the Voice menu, click **Regional**.

STEP 3 Scroll down to the Control Timer Values section.

STEP 4 Enter the desired values in the Interdigit Long Timer field and the Interdigit Short Timer field. Refer to the definitions at the beginning of this section.

Secure Call Implementation

This section describes secure call implementation with the SRP. It includes the following sections:

- **Enabling Secure Calls**
- **Secure Call Details**
- **Using a Mini-Certificate**
- **Generating a Mini-Certificate**

NOTE This is an advanced topic only meant for experienced installers.

Enabling Secure Calls

A secure call is established in two stages. The first stage is no different from a normal call setup. The second stage starts after the call is established in the normal way with both sides ready to stream RTP packets.

In the second stage, the two parties exchange information to determine if the current call can switch over to the secure mode. The information is transported by base64 encoding embedded in the message body of SIP INFO requests, and responses using a proprietary format. If the second stage is successful, the SRP plays a special Secure Call Indication Tone for a short time to indicate to both parties that the call is secured and that RTP traffic in both directions is being encrypted.

If the user has a phone that supports Call Waiting Caller ID (CIDCW) and that service is enabled, the CID will be updated with the information extracted from the Mini-Certificate received from the remote party. The Name field of the CID will be prepended with a '$' symbol. Both parties can verify the name and number to ensure the identity of the remote party.

The signing agent is implicit and must be the same for all devices that communicate securely with each other. The public key of the signing agent is pre-configured into the SRP by the administrator and is used by the SRP to verify the Mini-Certificate of its peer. The Mini-Certificate is valid if it has not expired, and it has a valid signature.

The SRP can be configured so that, by default, all outbound calls are either secure or not secure. If secure by default, the user has the option to disable security when making a call by dialing *19 before dialing the target number. If not secure by default, the user can make a secure outbound call by dialing *18 before dialing the target number. However, the user cannot force inbound calls to be secure or not secure; that depends on whether the caller has security enabled or not.

The SRP will not switch to secure mode if the CID of the called party from its Mini-Certificate does not agree with the user-id used in making the outbound call. The SRP performs this check after receiving the Mini-Certificate of the called party.

Secure Call Details

Looking at the second stage of setting up a secure call in greater detail, this stage can be further divided into two steps.

STEP 1 The caller sends a Caller Hello message (base64 encoded and embedded in the message body of a SIP INFO request) to the called party with the following information:

- Message ID (4B)
- Version and flags (4B)
- SSRC of the encrypted stream (4B)
- Mini-Certificate (252B)

Upon receiving the Caller Hello, the called party responds with a Callee Hello message (base64 encoded and embedded in the message body of a SIP response to the caller's INFO request) with similar information, if the Caller Hello message is valid. The caller then examines the Callee Hello and proceeds to the next step if the message is valid.

STEP 2 The caller sends the Caller Final message to the called party with the following information:

- Message ID (4B)
- Encrypted Master Key (16B or 128b)
- Encrypted Master Salt (16B or 128b)

Using a Mini-Certificate

The Master Key and Master Salt are encrypted with the public key from the called party Mini-Certificate. The Master Key and Master Salt are used by both ends for deriving session keys to encrypt subsequent RTP packets. The called party then responds with a Callee Final message (which is an empty message).

The Mini-Certificate (MC) contains the following information:

- User Name (32B)
- User ID or Phone Number (16B)
- Expiration Date (12B)
- Public Key (512b or 64B)
- Signature (1024b or 512B)

The MC has a 512-bit public key used for establishing secure calls. The administrator must provision each subscriber of the secure call service with an MC and the corresponding 512-bit private key. The MC is signed with a 1024-bit private key of the service provider, which acts as the Certificate Authority (CA) of the MC. The 1024-bit public key of the CA signing the MC must also be provisioned for each subscriber.

The CA public key is used to verify the MC received from the other end. If the MC is invalid, the call will not switch to secure mode. The MC and the 1024-bit CA public key are concatenated and base64 encoded into the single parameter Mini-Certificate. The 512-bit private key is base64 encoded into the SRTP Private Key parameter, which should be kept secret, like a password. (Mini-Certificate and SRTP Private Key are configured in the Line pages (1-4).

Because the secure call establishment relies on exchange of information embedded in message bodies of SIP INFO requests/responses, the service provider must ensure that the network infrastructure allows the SIP INFO messages to pass through with the message body unmodified.

Generating a Mini-Certificate

Cisco provides a Mini-Certificate Generator for the generation of Mini-Certificates and private keys. Contact your Cisco representative to access this tool.

The Mini-Certificate Generator uses the following syntax:

`gen_mc` *`ca-key user-name user-id expire-date`*

Where:

- *ca-key* is a text file with the base64 encoded 1024-bit CA private/public key pairs for signing/verifying the MC, such as the following:


```
9CC9aYU1X5lJuU+EBZmi3AmcqE9U1LxEOGwopaGyGOh3VyhKgi6JaVtQZt87PiJINKW8XQj3B9Qq
e3VgYxWCQNa335YCnDsenASeBxuMIEaBCYd1l1fVEodJZOGwXwfAde0MhcbD0kj7LVlzcsTyk2TZ
YTccnZ75TuTjj13qvYs=5nEtOrkCa84/mEwl3D9tSvVLyliwQ+u/
Hd+C8u5SNk7hsAUZaA9TqH8Iw0J/
IqSrsf6scsmundY5j7Z5mK5J9uBxSB8t8vamFGD0pF4zhNtbrVvIXKI9kmp4vph1C5jzO9gDfs3M
F+zjyYrVUFdM+pXtDBxmM+fGUfrpAuXb7/k=
```


- *user-name* is the name of the subscriber, such as Joe Smith. Maximum length is 32 characters.
- *user-id* is the user ID of the subscriber, which must match exactly the user id used in the INVITE when making the call, such as 14083331234. The maximum length is 16 characters.
- *expire-date* is the expiration date of the MC, such as “00:00:00 1/1/34” 34=2034). Internally the date is encoded as a fixed 12B string: 000000010134

The tool generates the Mini-Certificate and SRTP Private Key parameters that can be provisioned.

Example:

```
gen_mc ca_key “Joe Smith” 14085551234 “00:00:00 1/1/34”
```

This example produces the following Mini-Certificate and SRTP Private Key:


```
<Mini Certificate>
Sm9lIFNtaXRoAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAxNDA4NTU1MTIzNAAAAAAAMDAwMDAwMDEw
MTM00OvJakde2vVMF3Rw4pPXL7lAgIagMpbLSAG2+++YlSqt198Cp9rP/
xMGFfoPmDKGx6JFtkQ5sxLcuwgxpxpxkeXvpZKlYlpsb28L4Rhg5qZA+Gqj1hDFCmG6dffZ9SJhx
ES767G0JIS+N8lQBLr0AuemotknSjjjOy8c+1lTCd2t44Mh0vmwNg4fDck2YdmTMBR516xJt4/
uQ/
LJQlni2kwqlm7scDvll5k232EvvvVtCK0AYa4eWd6fQOpiESCO9CC9aYU1X5lJuU+EBZmi3AmcqE
9U1LxEOGwopaGyGOh3VyhKgi6JaVtQZt87PiJINKW8XQj3B9Qqe3VgYxWCQNa335YCnDsenASeBx
uMIEaBCYd1l1fVEodJZOGwXwfAde0MhcbD0kj7LVlzcsTyk2TZYTccnZ75TuTjj13qvYs=
<SRTP Private Key>
b/DWc96X4YQraCnYzl5en1CIUhVQQqrvcr6Qd/8R52IEvJjOw/
e+Klm4XiiFEPaKmU8UbooxKG36SEdKusp0AQ==
```

Configuring Voice Settings

Use the Voice pages to view and configure the voice settings for your SRP. These pages are described in the following sections:

- **Info Page**
- **System Page**
- **SIP Page**
- **Provisioning Page**
- **Regional Page**
- **Line Pages (1–4)**
- **PSTN Page (SRP540 Models Only)**
- **User Pages**

NOTE To access the voice settings pages, click **Voice** on the tab and then click the page you want to access in the navigation pane.

Info Page

Use the Info page to view information about the SRP voice application. This page includes the following sections:

- **Product Information**
- **System Status**
- **Line Status**

Product Information

Voice > Info > Product Information

Product Name	Model number/name.
Software Version	Software version number.
Voice Module Version	Voice Module version number.
Client Certificate	Status of the client certificate, which can indicate if the SRP was authorized by your ITSP.

Serial Number	Product serial number.
Hardware Version	Hardware version number.
MAC Address	MAC Address. For example, 8843E1657936.
Customization	Feature not used.

System Status

Voice > Info > System Status

Current Time	Current date and time of the system; for example, 10/3/2003 16:43:00. Set the system time by using the **Administration > Time Setup** page.
RTP Packets Sent	Total number of RTP packets sent (including redundant packets).
RTP Packets Recv	Total number of RTP packets received (including redundant packets).
SIP Messages Sent	Total number of SIP messages sent (including retransmissions).
SIP Messages Recv	Total number of SIP messages received (including retransmissions).
External IP	External IP address used for NAT mapping.
Elapsed Time	Total time elapsed since the last reboot of the system; for example, 25 days and 18:12:36.
RTP Bytes Sent	Total number of RTP bytes sent.
RTP Bytes Recv	Total number of RTP bytes received.
SIP Bytes Sent	Total number of bytes of SIP messages sent (including retransmissions).
SIP Bytes Recv	Total number of bytes of SIP messages received (including retransmissions)

Line Status

Voice > Info > Line 1 Status (similar information also provided for Line 2, 3, and 4)

Hook State	Hook state of the FXO port. Lines are either On or Off.
Last Registration At	Last date and time the line was registered.
Message Waiting	States are either Yes or No. The value automatically is set to Yes when a message is received. You also can clear or set the flag manually from the user menu.
Last Called Number	The last number called from the FXO Line.
Registration State	Indicates if the line has registered with the SIP proxy.
Next Registration In	Number of seconds before the next registration renewal. Indicates whether you have new voice mail waiting.
Call Back Active	Indicates whether a call back request is in progress. Options are either Yes or No.
Last Caller Number	Number of the last caller.
Mapped SIP Port	Port number of the SIP port mapped by NAT.
Call 1 and 2 State	Can take one of the following values: ▪ Idle ▪ Collecting PSTN Pin ▪ Invalid PSTN PIN ▪ PSTN Caller Accepted ▪ Connected to PSTN
Call 1 and 2 Tone	Type of tone used by the call.
Call 1 and 2 Encoder	Codec used for encoding.
Call 1 and 2 Decoder	Codec used for decoding.
Call 1 and 2 FAX	Status of the fax pass-through mode.

Call 1 and 2 Type	Direction of the call. May take one of the following values: ▪ PSTN Gateway Call = VoIP-To-PSTN Call ▪ VoIP Gateway Call = PSTN-To-VoIP Call ▪ PSTN To Line 1 = PSTN call ring through and answered by Line 1 ▪ Line 1 Forward to PSTN Gateway = VoIP calls Line 1, then forwarded to PSTN GW ▪ Line 1 Forward to PSTN Number = VoIP calls Line 1, then forwarded to PSTN number ▪ Line 1 To PSTN Gateway ▪ Line 1 Fallback To PSTN Gateway
Call 1 and 2 Remote Hold	Indicates whether the far end has placed the call on hold.
Call 1 and 2 Callback	Indicates whether the call was triggered by a call back request.
Call 1 and 2 Peer Name	Name of the peer phone.
Call 1 and 2 Peer Phone	Phone number of the peer phone.
Call 1 and 2 Duration	Duration of the call.
Call 1 and 2 Packets Sent	Number of packets sent
Call 1 and 2 Packets Recv	Number of packets received.
Call 1 and 2 Bytes Sent	Number of bytes sent.
Call 1 and 2 Bytes Recv	Number of bytes received.
Call 1 and 2 Decode Latency	Number of milliseconds for decoder latency.
Call 1 and 2 Jitter	Number of milliseconds for receiver jitter
Call 1 and 2 Round Trip Delay	Number of milliseconds for delay.
Call 1 and 2 Packets Lost	Number of packets lost.

Call 1 and 2 Packet Error	Number of invalid packets received.
Call 1 and 2 Mapped RTP Port	The port mapped for Real Time Protocol traffic for Call 1/2.
Call 1 and 2 Media Loopback	Media loopback is used to quantitatively and qualitatively measure the voice quality experienced by the end user.

PSTN Line Status (SRP540 Only)

(PSTN) Hook State	Hook state of the FXO port. Values are either On or Off.
(PSTN) Line Voltage	Voltage existing on the PSTN line.
(PSTN) Loop Current	The current (milliamperes) existing on the local loop.

System Page

Use the System page to configure settings for your system and network. This page includes the following sections:

- **System Configuration**
- **Miscellaneous Settings**

System Configuration

Voice > System > System Configuration

Restricted Access Domains	Feature not currently used by the SRP.
IVR Admin Password	Password for the administrator to manage the SRP using the built-in IVR through a connected handset. The default is **1234**.
IVR User Password	Password for the phone user to manage their line using the built-in IVR through their handset. The default is **no password**.

Miscellaneous Settings

Voice > System > Miscellaneous Settings

Syslog Server	Enter the IP address of the syslog server, to which system messages will be sent.
Debug Server	Enter the IP address of the syslog server, to which system messages will be sent.
Debug Level	Determines the level of debug information that will be generated. Select 0, 1, 2, 3 or 3+Router from the drop-down list. The higher the debug level, the more debug information will be generated. The default is 0, which indicates that no debug information will be generated. Levels 1, 2 & 3 generate messages related to the voice ports only. 3+Router generates debug content for both voice and router components. To configure the logging options, go to the **Administration > Log** pages.

SIP Page

Use the SIP page to configure numerous SIP parameters and values. This page includes the following sections:

- **SIP Parameters**
- **SIP Timer Values**
- **Response Status Code Handling**
- **RTP Parameters**
- **SDP Payload Types**
- **NAT Support Parameters**

SIP Parameters

Voice > SIP > SIP Parameters

Max Forward	Max Forward value, which can range from 1 to 255. The default is 70.
Max Redirection	Number of times an invite can be redirected to avoid an infinite loop. The default is 5.
Max Auth	Maximum number of times (from 0 to 255) a request may be challenged. The default is 2.
SIP User Agent Name	User-Agent header used in outbound requests. If empty, the header is not included. Macro expansion of $A to $D corresponding to GPP_A to GPP_D allowed. The default is $VERSION.
SIP Server Name	Server header used in responses to inbound responses. The default is $VERSION.
SIP Reg User Agent Name	User-Agent name to be used in a REGISTER request. If this value is not specified, the SIP User Agent Name parameter is also used for the REGISTER request. The default is blank.
SIP Accept Language	Accept-Language header used. There is no default (this indicates that the SRP does not include this header). If empty, the header is not included.
DTMF Relay MIME Type	MIME Type used in a SIP INFO message to signal a DTMF event. The default is application/dtmf-relay.

Remove Last Reg	Lets you remove the last registration before registering a new one if the value is different. Select yes or no from the drop-down list. The default is no.
Use Compact Header	Lets you use compact SIP headers in outbound SIP messages. Select yes or no from the drop-down list. If set to yes, the SRP uses compact SIP headers in outbound SIP messages. If set to no, the SRP uses normal SIP headers. If inbound SIP requests contain compact headers, the SRP reuses the same compact headers when generating the response regardless of the settings of the Use Compact Header parameter. If inbound SIP requests contain normal headers, the SRP substitutes those headers with compact headers (if defined by RFC 261) if Use Compact Header parameter is set to yes. The default is no.
Escape Display Name	Lets you keep the Display Name private. Select yes if you want the SRP to enclose the string (configured in the Display Name) in a pair of double quotes for outbound SIP messages. If the display name includes " or \, these will be escaped to \" and \\ within the double quotes. Otherwise, select no. The default is no.
RFC 2543 Call Hold	Configures the type of call hold: a:sendonly or 0.0.0.0. The default is no; do not use the 0.0.0.0 syntax in a HOLD SDP; use the a:sendonly syntax. Mark All AVT Packets If set to yes, all AVT tone packets (encoded for redundancy) have the marker bit set. If set to no, only the first packet has the marker bit set for each DTMF event. The default is yes.

Mark all AVT Packets	If set to yes, all AVT tone packets (encoded for redundancy) have the marker bit set. If set to no, only the first packet has the marker bit set for each DTMF event. The default is yes.
SIP TCP Port Min	Specifies the lowest TCP port number that can be used for SIP sessions. The default value is 5060.
SIP TCP Port Max	Specifies the highest TCP port number that can be used for SIP sessions. The default value is 5080.

SIP Timer Values

Voice > SIP > SIP Timer Values

SIP T1	RFC 3261 T1 value (RTT estimate), which can range from 0 to 64 seconds. The default is 0.5.
SIP T2	RFC 3261 T2 value (maximum retransmit interval for non- INVITE requests and INVITE responses), which can range from 0 to 64 seconds. The default is 4.
SIP T4	RFC 3261 T4 value (maximum duration a message remains in the network), which can range from 0 to 64 seconds. The default is 5.
SIP Timer B	INVITE time-out value, which can range from 0 to 64 seconds. The default is 32.
SIP Timer F	Non-INVITE time-out value, which can range from 0 to 64 seconds. The default is 32.

SIP Timer H	H INVITE final response, time-out value, which can range from 0 to 64 seconds. The default is 32.
SIP Timer D	ACK hang-around time, which can range from 0 to 64 seconds. The default is 32.
SIP Timer J	Non-INVITE response hang-around time, which can range from 0 to 64 seconds. The default is 32.
INVITE Expires	INVITE request Expires header value. If you enter 0, the Expires header is not included in the request. The default is 240. Range: 0–(2^{31}-1).
ReINVITE Expires	ReINVITE request Expires header value. If you enter 0, the Expires header is not included in the request. The default is 30. Range: 0–(2^{31}-1).
Reg Min Expires	Minimum registration expiration time allowed from the proxy in the Expires header or as a Contact header parameter. If the proxy returns a value less than this setting, the minimum value is used. The default is 1.
Reg Max Expires	Maximum registration expiration time allowed from the proxy in the Min-Expires header. If the value is larger than this setting, the maximum value is used. The default is 7200.
Reg Retry Intvl	Interval to wait before the SRP retries registration after failing during the last registration. The default is 30.

Reg Retry Long Intvl	When registration fails with a SIP response code that does not match Retry Reg RSC, the SRP waits for the specified length of time before retrying. If this interval is 0, the SRP stops trying. This value should be much larger than the Reg Retry Intvl value, which should not be 0. The default is 1200.

Response Status Code Handling

Voice > SIP > Response Status Code Handling

SIT1 RSC	SIP response status code for the appropriate Special Information Tone (SIT). For example, if you set the SIT1 RSC to 404, when the user makes a call and a failure code of 404 is returned, the SIT1 tone is played. Reorder or Busy tone is played by default for all unsuccessful response status code for SIT 1 RSC through SIT 4 RSC.
SIT2 RSC	SIP response status code to INVITE on which to play the SIT2 Tone.
SIT3 RSC	SIP response status code to INVITE on which to play the SIT3 Tone.
SIT4 RSC	SIP response status code to INVITE on which to play the SIT4 Tone.
Try Backup RSC	SIP response code that retries a backup server for the current request.
Retry Reg RSC	Interval to wait before the SRP retries registration after failing during the last registration.

RTP Parameters

Voice > SIP > RTP Parameters

RTP Port Min	Minimum port number for RTP transmission and reception. The RTP Port Min and RTP Port Max parameters should define a range that contains at least 4 even-number ports, such as 100–106. The default is 16384.
RTP Port Max	Maximum port number for RTP transmission and reception. The default is 16482.
RTP Packet Size	Packet size in seconds, which can range from 0.01 to 0.16. Valid values must be a multiple of 0.01 seconds. The default is 0.030.
Max RTP ICMP Err	Number of successive ICMP errors allowed when transmitting RTP packets to the peer before the SRP terminates the call. If value is set to 0, the SRP ignores the limit on ICMP errors. The default is 0.

RTCP Tx Interval	Interval for sending out RTCP sender reports on an active connection. It can range from 0 to 255 seconds. During an active connection, the SRP can be programmed to send out compound RTCP packet on the connection. Each compound RTP packets except the last one contains a SR (Sender Report) and a SDES (Source Description). The last RTCP packet contains an additional BYE packet. Each SR except the last one contains exactly 1 RR (Receiver Report); the last SR carries no RR. The SDES contains CNAME, NAME, and TOOL identifiers. The CNAME is set to <User ID>@<Proxy>, NAME is set to <Display Name> (or Anonymous if user blocks caller ID), and TOOL is set to the Vendor/Hardware-platform-software-version (such as Cisco/srp5201.0.31(b) or Cisco/srp5401.0.31(b)). The NTP timestamp used in the SR is a snapshot of the SRP's local time, not the time reported by an NTP server. If the SRP receives a RR from the peer, it attempts to compute the round-trip delay and show it as the <Call Round Trip Delay> value (ms) on the Voice > Info page. The default is 0.
No UDP Checksum	Select yes if you want the SRP to calculate the UDP header checksum for SIP messages. Otherwise, select no. The default is no.
Stats In BYE	Determines whether the SRP includes the P-RTP-Stat header or response in a BYE message. The header contains the RTP statistics of the current call. Select yes or no from the drop-down list. The format of the P-RTP-Stat header is: P-RTP-State: PS=<packets sent>,OS=<octets sent>,PR=<packets received>,OR=<octets received>,PL=<packets lost>,JI=<jitter in ms>,LA=<delay in ms>,DU=<call duration ins>,EN=<encoder>,DE=<decoder>. The default is yes.

SDP Payload Types

Voice > SIP > SDP Payload Types

NSE Dynamic Payload	NSE dynamic payload type. The valid range is 96-127. The default is 100.
AVT Dynamic Payload	AVT dynamic payload type. The valid range is 96-127. The default is 101.
INFOREQ Dynamic Payload	INFOREQ dynamic payload type. There is no default.
G726r32 Dynamic Payload	G726r32 dynamic payload type. The default is 2.
G729b Dynamic Payload	G.729b dynamic payload type. The valid range is 96-127. The default is 99.
EncapRTP Dynamic Payload	EncapRTP Dynamic Payload type. The default is 112.
RTP-Start-Loopback Dynamic Payload	RTP-Start-Loopback Dynamic Payload type. The default is 113.
RTP-Start-Loopback Codec	RTP-Start-Loopback Codec. Select one of the following: G711u, G711a, G726-32, G729a. The default is G711u.
NSE Codec Name	NSE codec name used in SDP. The default is NSE.
AVT Codec Name	AVT codec name used in SDP. The default is telephone-event.
G711u Codec Name	G.711u codec name used in SDP. The default is PCMU.

G711a Codec Name	G.711a codec name used in SDP. The default is PCMA.
G726r32 Codec Name	G.726-32 codec name used in SDP. The default is G726-32.
G729a Codec Name	G.729a codec name used in SDP. The default is G729a.
G729b Codec Name	G.729b codec name used in SDP. The default is G729ab.
EncapRTP Codec Name	EncapRTP codec name used in SDP. The default is EncapRTP.

NAT Support Parameters

Voice > SIP > NAT Support Parameters

Handle VIA received	If you select yes, the SRP processes the received parameter in the VIA header (this value is inserted by the server in a response to anyone of its requests). If you select no, the parameter is ignored. Select **yes** or **no** from the drop-down menu. The default is no.
Handle VIA rport	If you select yes, the SRP processes the rport parameter in the VIA header (this value is inserted by the server in a response to anyone of its requests). If you select no, the parameter is ignored. Select **yes** or **no** from the drop-down menu. The default is no.
Insert VIA received	Inserts the received parameter into the VIA header of SIP responses if the received-from IP and VIA sent-by IP values differ. Select yes or no from the drop-down menu. The default is no.

Insert VIA rport	Inserts the parameter into the VIA header of SIP responses if the received-from IP and VIA sent-by IP values differ. Select **yes** or **no** from the drop-down menu. The default is no.
Substitute VIA Addr	Lets you use NAT-mapped IP:port values in the VIA header. Select yes or no from the drop-down menu. The default is no.
Send Resp To Src Port	Sends responses to the request source port instead of the VIA sent-by port. Select yes or no from the drop-down menu. The default is no.
STUN Enable	Enables the use of STUN to discover NAT mapping. Select yes or no from the drop-down menu. The default is no.
STUN Test Enable	If the STUN Enable feature is enabled and a valid STUN server is available, the SRP can perform a NAT-type discovery operation when it powers on. It contacts the configured STUN server, and the result of the discovery is reported in a Warning header in all subsequent REGISTER requests. If the SRP detects symmetric NAT or a symmetric firewall, NAT mapping is disabled. The default is no.
STUN Server	IP address or fully-qualified domain name of the STUN server to contact for NAT mapping discovery.

EXT IP	External IP address to substitute for the actual IP address of the SRP in all outgoing SIP messages. If 0.0.0.0 is specified, no IP address substitution is performed. If this parameter is specified, the SRP assumes this IP address when generating SIP messages and SDP (if NAT Mapping is enabled for that line). However, the results of STUN and VIA received parameter processing, if available, supersede this statically configured value. **NOTE** This option requires that you have (1) a static IP address from your Internet Service Provider and (2) an edge device with a symmetric NAT mechanism. If the SRP is the edge device, the second requirement is met. The default is 0.0.0.0.
EXT RTP Port Min	External port mapping number of the RTP Port Min. number. If this value is not zero, the RTP port number in all outgoing SIP messages is substituted for the corresponding port value in the external RTP port range. There is no default value.
NAT Keep Alive Intvl	Interval between NAT-mapping keepalive messages. The default is 15.

Provisioning Page

Use the Provisioning page to configure various profiles and parameters. This page includes the following sections:

- **Configuration Profile**
- **Firmware Upgrade**
- **General Purpose Parameters**

Configuration Profile

Voice > Provisioning > Configuration Profile

Provision Enable	Controls all resync actions independently of firmware upgrade actions. Set to Yes to enable remote provisioning. The default is Yes.
Resync On Reset	Triggers a resync after every reboot except for reboots caused by parameter updates and firmware upgrades. The default is Yes.
Resync Random Delay	The maximum value for a random time interval that the device waits before making its initial contact with the provisioning server. This delay is effective only on the initial configuration attempt following device power-on or reset. The delay is a pseudo-random number between zero and this value. This parameter is in units of 20 seconds; the default value of 2 represents 40 seconds. This feature is disabled when this parameter is set to zero. This feature can be used to prevent an overload of the provisioning server when a large number of devices power-on simultaneously. The default is 2 (40 seconds).

Resync Periodic	The time interval between periodic resyncs with the provisioning server. The associated resync timer is active only after the first successful sync with the server. Set this parameter to zero to disable periodic resyncing. The default is 3600 seconds.
Resync Error Retry Delay	Resync retry interval (in seconds) applied in case of resync failure. The device has an error retry timer that activates if the previous attempt to sync with the provisioning server fails. The device waits to contact the server again until the timer counts down to zero. This parameter is the value that is initially loaded into the error retry timer. If this parameter is set to zero, the device immediately retries to sync with the provisioning server following a failed attempt. The default is 3600 seconds.
Forced Resync Delay	Maximum delay (in seconds) the SPA waits before performing a resync. The device does not resync while one of its phone lines is active. Because a resync can take several seconds, it is desirable to wait until the device has been idle for an extended period before resyncing. This allows a user to make calls in succession without interruption. The device has a timer that begins counting down when all of its lines become idle. This parameter is the initial value of the counter. Resync events are delayed until this counter decrements to zero. The default is 14,400 seconds.
Resync From SIP	Enables a resync to be triggered via a SIP NOTIFY message. The default is Yes.
Resync After Upgrade Attempt	Triggers a resync after every firmware upgrade attempt. The default is Yes.

Resync Trigger 1 Resync Trigger 2	Configurable resync trigger conditions. A resync is triggered when the logic equation in these parameters evaluates to TRUE. The default is (empty).
Resync Fails On FNF	Determines whether a file-not-found response from the provisioning server constitutes a successful or a failed resync. A failed resync activates the error resync timer. The default is Yes.
Profile Rule	This parameter is a profile script that evaluates to the provisioning resync command. The command is a TCP/IP operation and an associated URL. The TCP/IP operation can be TFTP, HTTP, or HTTPS. If the command is not specified, TFTP is assumed, and the address of the TFTP server is obtained through DHCP option 66. In the URL, either the IP address or the FQDN of the server can be specified. The file name can have macros, such as $MA, which expands to the device MAC address. The default is /srp$PSN.cfg.
Profile Rule B: Profile Rule C: Profile Rule D:	Defines second, third, and fourth resync commands and associated profile URLs. These profile scripts are executed sequentially after the primary Profile Rule resync operation has completed. If a resync is triggered and Profile Rule is blank, Profile Rule B, C, and D are still evaluated and executed. The default is (empty).
Profile Name and Profile Region	A provisioning server can store string data in this parameter, and subsequently read this data back when querying the device. It performs no other internal function.
Log Resync Request Msg	This parameter contains the message that is sent to the Syslog server at the start of a resync attempt. The default is $PN $MAC – Requesting resync $SCHEME://$SERVIP:$PORT$PATH.

Log Resync Success Msg	Syslog message issued upon successful completion of a resync attempt. The default is $PN $MAC – Successful resync $SCHEME://$SERVIP:$PORT$PATH -- $ERR.
Log Resync Failure Msg	Syslog message issued after a failed resync attempt. The default is $PN $MAC – Resync failed: $ERR.
Report Rule	The target URL to which configuration reports are sent. This parameter has the same syntax as the Profile_Rule parameter, and resolves to a TCP/IP command with an associated URL. A configuration report is generated in response to an authenticated SIP NOTIFY message, with Event: report. The report is an XML file containing the name and value of all the device parameters. This parameter may optionally contain an encryption key. For example: [--key $K] tftp://ps.callhome.net/$MA/rep.xml.enc The default is (empty).

Firmware Upgrade

Voice > Provisioning > Firmware Upgrade

Upgrade Enable	Enables firmware upgrade operations independently of resync actions. The default is Yes.
Upgrade Error Retry Delay	The upgrade retry interval (in seconds) applied in case of an upgrade failure. The device has a firmware upgrade error timer that activates after a failed firmware upgrade attempt. The timer is initialized with the value in this parameter. The next firmware upgrade attempt occurs when this timer counts down to zero. The default is 3600 seconds.

Downgrade Rev Limit	Enforces a lower limit on the acceptable version number during a firmware upgrade or downgrade. The device does not complete a firmware upgrade operation unless the firmware version is greater than or equal to this parameter. The default is (empty).
Upgrade Rule	This parameter is a firmware upgrade script with the same syntax as Profile_Rule. Defines upgrade conditions and associated firmware URLs. The default is (empty).
Log Upgrade Request Msg	Syslog message issued at the start of a firmware upgrade attempt. The default is $PN $MAC -- Requesting upgrade $SCHEME://$SERVIP:$PORT$PATH.
Log Upgrade Success Msg	Syslog message issued after a firmware upgrade attempt completes successfully. The default is $PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR.
Log Upgrade Failure Msg	Syslog message issued after a failed firmware upgrade attempt. The default is $PN $MAC -- Upgrade failed: $ERR.
License Keys	This field is not currently used by the SRP500.

General Purpose Parameters

Voice > Provisioning > General Purpose Parameters

GPP A to GPP P	General purpose provisioning parameters. These parameters can be used as variables in provisioning and upgrade rules. They are referenced by prepending the variable name with a '$' character, such as $GPP_A. The default is (empty).

Regional Page

Use the Regional page to localize your system with the appropriate regional settings. The following sections appear on the **Voice > Regional** page.

- **Call Progress Tones**
- **Distinctive Ring Patterns**
- **Distinctive Call Waiting Tone Patterns**
- **Distinctive Ring/CWT Pattern Names**
- **Control Timer Values**
- **Vertical Service Activation Codes**
- **Vertical Service Announcement Codes**
- **Outbound Call Codec Selection Codes**
- **Miscellaneous**

Defining Ring and Cadence and Tone Scripts

To define ring and tone patterns, the SRP uses the concept of scripts. The following defines how to create Cadence Scripts (CadScripts), Frequency Scripts (FreqScripts) and Tone Scripts (ToneScripts).

CadScript

A mini-script of up to 127 characters that specifies the cadence parameters of a signal.

Syntax: S_1[;S_2], where:
S_i=D_i(on_i, 1/off_i, 1[,$on_{i,2}$/$off_{i,2}$[,$on_{i,3}$/$off_{i,3}$[,$on_{i,4}$/$off_{i,4}$[,$on_{i,5}$/$off_{i,5}$,$on_{i,6}$/$off_{i,6}$]]]]]) and is known as a section, $on_{i,j}$ and $off_{i,j}$ are the on/off duration in seconds of a *segment* and i = 1 or 2, and j = 1 to 6. D_i is the total duration of the section in seconds. All durations can have up to three decimal places to provide 1 ms resolution. The wildcard character "*" represents infinite duration. The segments within a section are played in order and repeated until the total duration is played.

Example 1: 60(2/4)

```
Number of Cadence Sections = 1
Cadence Section 1: Section Length = 60 s
Number of Segments = 1
Segment 1: On=2s, Off=4s
Total Ring Length = 60s
```

Example 2—Distinctive ring (short,short,short,long): 60(.2/.2,.2/.2,.2/.2,1/4)

```
Number of Cadence Sections = 1
Cadence Section 1: Section Length = 60s
Number of Segments = 4
Segment 1: On=0.2s, Off=0.2s
Segment 2: On=0.2s, Off=0.2s
Segment 3: On=0.2s, Off=0.2s
Segment 4: On=1.0s, Off=4.0s
Total Ring Length = 60s
```

FreqScript

A mini-script of up to 127 characters that specifics the frequency and level parameters of a tone.

Syntax: F_1@L_1[,F_2@L_2[,F_3@L_3[,F_4@L_4[,F_5@L_5[,F_6@L_6]]]]
Where F_1–F_6 are frequency in Hz (unsigned integers only) and L_1–L_6 are corresponding levels in dBm (with up to 1 decimal places). White spaces before and after the comma are allowed (but not recommended).

Example 1—Call Waiting Tone: 440@-10

```
Number of Frequencies = 1
   Frequency 1 = 440 Hz at -10 dBm
```

Example 2—Dial Tone: 350@-19,440@-19

```
Number of Frequencies = 2
   Frequency 1 = 350 Hz at -19 dBm
   Frequency 2 = 440 Hz at -19 dBm
```

ToneScript

A mini-script of up to 127 characters that specifies the frequency, level and cadence parameters of a call progress tone. This may contain up to 127 characters.

Syntax: FreqScript;Z_1[;Z_2].
The section Z_1 is similar to the S_1 section in a CadScript except that each on/off segment is followed by a frequency components parameter: $Z_1 = D_1(on_{i,1}/off_{i,1}/f_{i,1}[,on_{i,2}/off_{i,2}/f_{i,2}[,on_{i,3}/off_{i,3}/f_{i,3}[,on_{i,4}/off_{i,4}/f_{i,4}[,on_{i,5}/off_{i,5}/f_{i,5}[,on_{i,6}/off_{i,6}/f_{i,6}]]]]])$, where fi,j

= $n_1[+n_2]+n_3[+n_4[+n_5[+n_6]]]]]$ and $1 < n_k < 6$ indicates which of the frequency components given in the FreqScript are used in that segment; if more than one frequency component is used in a segment, the components are summed together.

Example 1—Dial tone: 350@-19,440@-19;10(*/0/1+2)

```
Number of Frequencies = 2
   Frequency 1 = 350 Hz at -19 dBm
   Frequency 2 = 440 Hz at -19 dBm
Number of Cadence Sections = 1
   Cadence Section 1: Section Length = 10 s
   Number of Segments = 1
      Segment 1: On=forever, with Frequencies 1 and 2
Total Tone Length = 10s
```

Example 2—Stutter tone: 350@-19,440@-19;2(.1/.1/1+2);10(*/0/1+2)

```
Number of Frequencies = 2
   Frequency 1 = 350 Hz at -19 dBm
   Frequency 2 = 440 Hz at -19 dBm
Number of Cadence Sections = 2
   Cadence Section 1: Section Length = 2s
      Number of Segments = 1
         Segment 1: On=0.1s, Off=0.1s with Frequencies 1 and 2
   Cadence Section 2: Section Length = 10s
      Number of Segments = 1
         Segment 1: On=forever, with Frequencies 1 and 2
Total Tone Length = 12s
```

Call Progress Tones

Voice > Regional > Call ProgressTones

Dial Tone	Prompts the user to enter a phone number. Reorder Tone is played automatically when Dial Tone or any of its alternatives times out. The default is 350@-19,440@-19;10(*/0/1+2).
Second Dial Tone	Alternative to the Dial Tone when the user dials a three-way call. The default is 420@-19,520@-19;10(*/0/1+2).

Outside Dial Tone	Alternative to the Dial Tone. It prompts the user to enter an external phone number, as opposed to an internal extension. It is triggered by a "," (comma) character encountered in the dial plan. The default is 420@-19;10(*/0/1).
Prompt Tone	Prompts the user to enter a call forwarding phone number. The default is 520@-19,620@-19;10(*/0/1+2).
Busy Tone	Played when a 486 RSC is received for an outbound call. The default is 480@-19,620@-19;10(.5/.5/1+2).
Reorder Tone	Played when an outbound call has failed, or after the far end hangs up during an established call. Reorder Tone is played automatically when Dial Tone or any of its alternatives times out. The default is 480@-19,620@-19;10(.25/.25/1+2).
Off Hook WarningTone	Played when the caller has not properly placed the handset on the cradle. Off Hook Warning Tone is played when the Reorder Tone times out. The default is 480@10,620@0;10(.125/.125/1+2).
Ring Back Tone	Played during an outbound call when the far end is ringing. The default is 440@-19,480@-19;*(2/4/1+2).
Ring Back 2 Tone	Your SRP plays this ringback tone instead of Ring Back Tone if the called party replies with a SIP 182 response without SDP to its outbound INVITE request. The default value is the same as Ring Back Tone, except the cadence is 1s on and 1s off. The default is 440@-19,480@-19;*(1/1/1+2).
Confirm Tone	Brief tone to notify the user that the last input value has been accepted. The default is 600@-16; 1(.25/.25/1).

SIT1 Tone	Alternative to the Reorder Tone played when an error occurs as a caller makes an outbound call. The RSC to trigger this tone is configurable on the SIP screen. The default is 985@-16,1428@-16,1777@ 16;20(.380/0/1,.380/0/2,.380/0/3,0/4/0).
SIT2 Tone	Alternative to the Reorder Tone played when an error occurs as a caller makes an outbound call. The RSC to trigger this tone is configurable on the SIP screen. The default is 914@-16,1371@-16,1777@ 16;20(.274/0/1,.274/0/2,.380/0/3,0/4/0).
SIT3 Tone	Alternative to the Reorder Tone played when an error occurs as a caller makes an outbound call. The RSC to trigger this tone is configurable on the SIP screen. The default is 914@-16,1371@-16,1777@-16;20(.380/0/1,.380/0/2,.380/0/3,0/4/0).
SIT4 Tone	Alternative to the Reorder Tone played when an error occurs as a caller makes an outbound call. The RSC to trigger this tone is configurable on the SIP screen. The default is 985@-16,1371@-16,1777@-16;20(.380/0/1,.274/0/2,.380/0/3,0/4/0).
MWI Dial Tone	Played instead of the Dial Tone when there are unheard messages in the caller's mailbox. The default is: 350@-19,440@-19;2(.1/.1/1+2);10(*/0 1+2).
Cfwd Dial Tone	Played when all calls are forwarded. The default is: 350@-19,440@-19;2(.2/.2/1+2);10(*/0/1+2).
Holding Tone	Informs the local caller that the far end has placed the call on hold. The default is 600@-19*(.1/.1/1,.1/.1/1,.1/9.5/1).
Conference Tone	Played to all parties when a three-way conference call is in progress. The default is 350@-19;20(.1/.1/1,.1/9.7/1).

Secure Call Indication Tone	Played when a call has been successfully switched to secure mode. It should be played only for a short while (less than 30 seconds) and at a reduced level (less than -19 dBm) so it does not interfere with the conversation. The default is 397@-19,507@-19;15(0/2/0,.2/.1/1,.1/2.1/2).
Feature Invocation Tone	Played when a feature is implemented. The default is 350@-16;*(.1/.1/1).

Distinctive Ring Patterns

Voice > Regional > Distinctive Ring Patterns

Ring1 Cadence	Cadence script for distinctive ring 1. The default is 60(2/4).
Ring2 Cadence	Cadence script for distinctive ring 2. The default is 60(.8/.4,.8/4).
Ring3 Cadence	Cadence script for distinctive ring 3. The default is 60(.4/.2,.4/.2,.8/4).
Ring4 Cadence	Cadence script for distinctive ring 4. The default is 60(.3/.2,1/.2,.3/4).
Ring5 Cadence	Cadence script for distinctive ring 5. The default is 1(.5/.5).
Ring6 Cadence	Cadence script for distinctive ring 6. The default is 60(.2/.4,.2/.4,.2/4).
Ring7 Cadence	Cadence script for distinctive ring 7. The default is 60(.4/.2,.4/.2,.4/4).
Ring8 Cadence	Cadence script for distinctive ring 8. The default is 60(0.25/9.75).

Distinctive Call Waiting Tone Patterns

Voice > Regional > Distinctive Call Waiting Tone Patterns

CWT1 Cadence	Cadence script for distinctive CWT 1. The default is 30(.3/9.7).
CWT2 Cadence	Cadence script for distinctive CWT 2. The default is 30(.1/.1, .1/9.7).
CWT3 Cadence	Cadence script for distinctive CWT 3. The default is 30(.1/.1, .1/.1, .1/9.7).
CWT4 Cadence	Cadence script for distinctive CWT 4. The default is 30(.1/.1, .3/.1, .1/9.3).
CWT5 Cadence	Cadence script for distinctive CWT 5. The default is 1(.5/.5).
CWT6 Cadence	Cadence script for distinctive CWT 6. The default is 30(.3/.1,.3/.1,.1/9.1).
CWT7 Cadence	Cadence script for distinctive CWT 7. The default is 30(.3/.1,.3/.1,.1/9.3).
CWT8 Cadence	Cadence script for distinctive CWT 8. The default is 2.3(.3/2).

Distinctive Ring/CWT Pattern Names

IMPORTANT. Ring and Call Waiting tones do not work the same way on all phones. When setting ring tones, consider the following recommendations:

- Begin with the default Ring Waveform, Ring Frequency, and Ring Voltage.
- If your ring cadence does not sound right, or your phone does not ring, change your Ring Waveform, Ring Frequency, and Ring Voltage to the following:
  - Ring Waveform: Sinusoid
  - Ring Frequency: 25

- Ring Voltage: 80Vc

Voice > Regional > Distinctive Ring/CWT Pattern Name*s*

Ring1 Name	Name in an INVITE's Alert-Info Header to pick distinctive ring/CWT 1 for the inbound call. The default is Bellcore-r1.
Ring2 Name	Name in an INVITE's Alert-Info Header to pick distinctive ring/CWT 2 for the inbound call. The default is Bellcore-r2.
Ring3 Name	Name in an INVITE's Alert-Info Header to pick distinctive ring/CWT 3 for the inbound call. The default is Bellcore-r3.
Ring4 Name	Name in an INVITE's Alert-Info Header to pick distinctive ring/CWT 4 for the inbound call. The default is Bellcore-r4.
Ring5 Name	Name in an INVITE's Alert-Info Header to pick distinctive ring/CWT 5 for the inbound call. The default is Bellcore-r5.
Ring6 Name	Name in an INVITE's Alert-Info Header to pick distinctive ring/CWT 6 for the inbound call. The default is Bellcore-r6.
Ring7 Name	Name in an INVITE's Alert-Info Header to pick distinctive ring/CWT 7 for the inbound call. The default is Bellcore-r7.
Ring8 Name	Name in an INVITE's Alert-Info Header to pick distinctive ring/CWT 8 for the inbound call. The default is Bellcore-r8.
Ring Waveform	Waveform for the ringing signal. Choices are Sinusoid or Trapezoid. The default is Trapezoid.

Ring Frequency	Frequency of the ringing signal. Valid values are 10–100 (Hz). The default is 20.
Ring Voltage	Ringing voltage. Choices are **60–90** (V). The default is 85.
CWT Frequency	Frequency script of the call waiting tone. All distinctive CWTs are based on this tone. The default is 440@-10.
Synchronized Ring	If this is set to Yes, when the SRP is called, all lines ring at the same time (similar to a regular PSTN line). After one line answers, the others stop ringing. The default is no.

Control Timer Values

Voice > Regional > Control Timer Values (sec)

Hook Flash Timer Min	Minimum on-hook time before off-hook qualifies as hookflash. If less than the minimum time the on-hook event is ignored. Range: 0.1–0.4 seconds. The default is 0.1.
Hook Flash Timer Max	Maximum on-hook time before off-hook qualifies as hookflash. If more than the maximum time the on-hook event is treated as on-hook (no hook-flash event). Range: 0.4–1.6 seconds. The default is 0.9.
Callee On Hook Delay	Phone must be on-hook for at this time in seconds before the SRP will tear down the current inbound call. It does not apply to outbound calls. Range: 0–255 seconds. The default is 0.
Reorder Delay	Delay after far end hangs up before reorder tone is played. 0 = plays immediately, inf = never plays. Range: 0–255 seconds. The default is 5.

Call Back Expires	Expiration time in seconds of a call back activation. Range: 0–65535 seconds. The default is 1800.
Call Back Retry Intvl	Call back retry interval in seconds. Range: 0–255 seconds. The default is 30.
Call Back Delay	Delay after receiving the first SIP 18x response before declaring the remote end is ringing. If a busy response is received during this time, the SRP still considers the call as failed and keeps on retrying. The default is 0.5.
VMWI Refresh Intvl	Interval between VMWI refresh to the CPE. The default is 0.
Interdigit Long Timer	Long timeout between entering digits when dialing. The interdigit timer values are used as defaults when dialing. The Interdigit_Long_Timer is used after any one digit, if all valid matching sequences in the dial plan are incomplete as dialed. Range: 0–64 seconds. The default is 10.
Interdigit Short Timer	Short timeout between entering digits when dialing. The Interdigit_Short_Timer is used after any one digit, if at least one matching sequence is complete as dialed, but more dialed digits would match other as yet incomplete sequences. Range: 0–64 seconds. The default is 3.

CPC Delay	Delay in seconds after caller hangs up when the SRP starts removing the tip-and-ring voltage to the attached equipment of the called party. The range is 0–255 seconds. This feature is generally used for answer supervision on the caller side to signal to the attached equipment when the call has been connected (remote end has answered) or disconnected (remote end has hung up). This feature should be disabled for the called party (in other words, by using the same polarity for connected and idle state) and the CPC feature should be used instead. Without CPC enabled, reorder tone is played after a configurable delay. If CPC is enabled, dial tone is played when tip-to-ring voltage is restored. Resolution is 1 second. The default range is 2.
CPC Duration	Duration in seconds for which the tip-to-ring voltage is removed after the caller hangs up. After that, tip-to-ring voltage is restored and dial tone applies if the attached equipment is still off-hook. CPC is disabled if this value is set to 0. Range: 0 to 1.000 second. Resolution is 0.001 second. The default is 0 (CPC disabled).

Vertical Service Activation Codes

Vertical Service Activation Codes are automatically appended to the dial-plan. There is no need to include them in dial-plan, although no harm is done if they are included.

Voice > Regional > Vertical Service Activation Codes

Call Return Code	Calls the last caller. The default is *69.
Call Redial Code	Redials the last number called. The default is *07.
Blind Transfer Code	Begins a blind transfer of the current call to the extension specified after the activation code. The default is *98.
Call Back Act Code	Starts a callback when the last outbound call is not busy. The default is *66.
Call Back Deact Code	Cancels a callback. The default is *86.
Call Back Busy Act Code	Starts a callback when the last outbound call is busy. The default is *05
Cfwd All Act Code	Forwards all calls to the extension specified after the activation code. The default is *72.
Cfwd All Deact Code	Cancels call forwarding of all calls. The default is *73.
Cfwd Busy Act Code	Forwards busy calls to the extension specified after the activation code. The default is *90.
Cfwd Busy Deact Code	Cancels call forwarding of busy calls. The default is *91.

Cfwd No Ans Act Code	Forwards no-answer calls to the extension specified after the activation code. The default is *92.
Cfwd No Ans Deact Code	Cancels call forwarding of no-answer calls. The default is *93.
Cfwd Last Act Code	Forwards the last inbound or outbound calls to the extension specified after the activation code. The default is *63.
Cfwd Last Deact Code	Cancels call forwarding of the last inbound or outbound calls. The default is *83.
Block Last Act Code	Blocks the last inbound call. The default is *60.
Block Last Deact Code	Cancels blocking of the last inbound call. The default is *80.
Accept Last Act Code	Accepts the last outbound call. It lets the call ring through when do not disturb or call forwarding of all calls are enabled. The default is *64.
Accept Last Deact Code	Cancels the code to accept the last outbound call. The default is *84.
CW Act Code	Enables call waiting on all calls. The default is *56.
CW Deact Code	Disables call waiting on all calls. The default is *57.
CW Per Call Act Code	Enables call waiting for the next call. The default is *71.

CW Per Call Deact Code	Disables call waiting for the next call. The default is *70.
Block CID Act Code	Blocks caller ID on all outbound calls. The default is *67.
Block CID Deact Code	Removes caller ID blocking on all outbound calls. The default is *68.
Block CID Per Call Act Code	Blocks caller ID on the next outbound call. The default is *81.
Block CID Per Call Deact Code	Removes caller ID blocking on the next inbound call. The default is *82.
Block ANC Act Code	Blocks all anonymous calls. The default is *77.
Block ANC Deact Code	Removes blocking of all anonymous calls. The default is *87.
DND Act Code	Enables the do not disturb feature. The default is *78.
DND Deact Code	Disables the do not disturb feature. The default is *79.
CID Act Code	Enables caller ID generation. The default is *65.
CID Deact Code	Disables caller ID generation. The default is *85.
CWCID Act Code	Enables call waiting, caller ID generation. The default is *25.
CWCID Deact Code	Disables call waiting, caller ID generation. The default is *45.

Dist Ring Act Code	Enables the distinctive ringing feature. The default is *26.
Dist Ring Deact Code	Disables the distinctive ringing feature. The default is *46.
Speed Dial Act Code	Assigns a speed dial number. The default is *74.
Paging Code	Used for paging other clients in the group. The default is *96.
Secure All Call Act Code	Makes all outbound calls secure. The default is *16.
Secure No Call Act Code	Makes all outbound calls not secure. The default is *17.
Secure One Call Act Code	Makes the next outbound call secure. (It is redundant if all outbound calls are secure by default.) The default is *18.
Secure One Call Deact Code	Makes the next outbound call not secure. (It is redundant if all outbound calls are not secure by default.) The default is *19.
Conference Act Code	If this code is specified, the user must enter it before dialing the third party for a conference call. Enter the code for a conference call.
Attn-Xfer Act Code	If the code is specified, the user must enter it before dialing the third party for a call transfer. Enter the code for a call transfer.
Modem Line Toggle Code	Toggles the line to a modem. The default is *99. Modem pass-through mode can be triggered only by pre-dialing this code.
FAX Line Toggle Code	Toggles the line to a fax machine. The default is #99.

Media Loopback Code	Use for media loopback. The default is *03.
Referral Services Codes	These codes tell the SRP what to do when the user places the current call on hold and is listening to the second dial tone. One or more *codes can be configured into this parameter, such as *98, or *97|*98|*123, etc. Maximum total length is 79 characters. This parameter applies when the user places the current call on hold (by Hook Flash) and is listening to second dial tone. Each *code (and the following valid target number according to current dial plan) entered on the second dial tone triggers the SRP to perform a blind transfer to a target number that is prepended by the service *code. For example, after the user dials *98, the SRP plays a special dial tone called the Prompt Tone while waiting for the user the enter a target number (which is checked according to dial plan as in normal dialing). When a complete number is entered, the SRP sends a blind REFER to the holding party with the Refer-To target equals to *98 target_number. This feature allows the SRP to hand off a call to an application server to perform further processing, such as call park. The *codes should not conflict with any of the other vertical service codes internally processed by the SRP. You can empty the corresponding *code that you do not want the SRP to process.

Feature Dial Services Codes	These codes tell the SRP what to do when the user is listening to the first or second dial tone. One or more *code can be configured into this parameter, such as *72, or *72|*74|*67|*82, etc. Maximum total length is 79 characters. This parameter applies when the user has a dial tone (first or second dial tone). Enter *code (and the following target number according to current dial plan) entered at the dial tone triggers the SRP to call the target number prepended by the *code. For example, after user dials *72, the SRP plays a special tone called a Prompt tone while awaiting the user to enter a valid target number. When a complete number is entered, the SRP sends a INVITE to *72 target_number as in a normal call. This feature allows the proxy to process features like call forward (*72) or Block Caller ID (*67). The *codes should not conflict with any of the other vertical service codes internally processed by the SRP. You can empty the corresponding *code that you do not want to the SRP to process. You can add a parameter to each *code in Features Dial Services Codes to indicate what tone to play after the *code is entered, such as *72‘c‘|*67‘p‘. This is a list of allowed tone parameters (note the use of open quotes surrounding the parameter w/o spaces): ‘c‘ = <Cfwd Dial Tone> ‘d‘ = <Dial Tone> ‘m‘ = <MWI Dial Tone> ‘o‘ = <Outside Dial Tone> ‘p‘ = <Prompt Dial Tone> ‘s‘ = <Second Dial Tone> ‘x‘ = No tones are place, x is any digit not used above If no tone parameter is specified, the SRP plays Prompt tone by default. If the *code is not to be followed by a phone number, such as *73 to cancel call forwarding, do not include it in this parameter. In that case, simply add that *code in the dial plan and the SRP send INVITE *73@..... as usual when user dials *73.’

Vertical Service Announcement Codes

Voice > Regional > Vertical Service Announcement Codes

Service Annc Base Number	Base number for service announcements. The default is blank.
Service Annc Extension Codes	Extension codes for service announcements. The default is blank.

Outbound Call Codec Selection Codes

Voice > Regional > Outbound Call Codec Selection Codes

Prefer G711u Code	Dial prefix to make G.711u the preferred codec for the call. The default is *017110.
Force G711u Code	Dial prefix to make G.711u the only codec that can be used for the call. The default is *027110.
Prefer G711a Code	Dial prefix to make G.711a the preferred codec for the call. The default is *017111.
Force G711a Code	Dial prefix to make G.711a the only codec that can be used for the call. The default is *027111.
Prefer G726r32 Code	Dial prefix to make G.726r32 the preferred codec for the call. The default is *0172632.
Force G726r32 Code	Dial prefix to make G.726r32 the only codec that can be used for the call. The default is *0272632.

Prefer G729a Code	Dial prefix to make G.729a the preferred codec for the call. The default is *01729.
Force G729a Code	Dial prefix to make G.729a the only codec that can be used for the call. The default is *02729.

Miscellaneous

Voice > Regional > Miscellaneous

Set Local Date (mm/dd)	Sets the local date (mm stands for months and dd stands for days). The year is optional and uses two or four digits. **NOTE:** You do not generally need to set this value because the voice application date and time is synchronized with the SRP. See the **Administration > Time Setup** page.
Set Local Time (HH/mm)	Sets the local time (hh stands for hours and mm stands for minutes). Seconds are optional. **NOTE:** You do not generally need to set this value because the voice application date and time is synchronized with the SRP. See the **Administration > Time Setup** page.
FXS Port Impedance	Sets the electrical impedance of the FXS port. Choices are: 600, 900, 600+2.16uF, 900+2.16uF, 270+750‖150nF, 220+850‖120nF, 220+820‖115nF, or 200+600‖100nF. The default is 600. **NOTE** For New Zealand impedance (370+620‖310nF), use 270+750‖150nF.
FXS Port Input Gain	Input gain in dB, up to three decimal places. The range is 6.000 to -12.000. The default is -3.

FXS Port Output Gain	Output gain in dB, up to three decimal places. The range is 6.000 to -12.000. The Call Progress Tones and DTMF playback level are not affected by the FXS Port Output Gain parameter. The default is -3.
DTMF Playback Level	Local DTMF playback level in dBm, up to one decimal place. The default is -16.0.
DTMF Playback Twist	The loudness difference between high and low tone frequencies. The default s 1.3.
DTMF Playback Length	Local DTMF playback duration in milliseconds. The default is .1.
Detect ABCD	To enable local detection of DTMF ABCD, select yes. Otherwise, select no. The default is yes. This setting has no effect if DTMF Tx Method is INFO; ABCD is always sent OOB regardless in this setting.
Playback ABCD	To enable local playback of OOB DTMF ABCD, select yes. Otherwise, select no. The default is yes.

Caller ID Method	The following choices are: **Bellcore (N.Amer,China)**: CID, CIDCW, and VMWI. FSK sent after first ring (same as ETSI FSK sent after first ring) (no polarity reversal or DTAS). **DTMF (Finland, Sweden)**: CID only. DTMF sent after polarity reversal (and no DTAS) and before first ring. **DTMF (Denmark)**: CID only. DTMF sent before first ring with no polarity reversal and no DTAS. **ETSI DTMF:** CID only. DTMF sent after DTAS (and no polarity reversal) and before first ring. **ETSI DTMF With PR**: CID only. DTMF sent after polarity reversal and DTAS and before first ring. **ETSI DTMF After Ring**: CID only. DTMF sent after first ring (no polarity reversal or DTAS). **ETSI FSK: CID, CIDCW, and VMWI**. FSK sent after DTAS (but no polarity reversal) and before first ring. Waits for ACK from CPE after DTAS for CIDCW. **ETSI FSK With PR (UK)**: CID, CIDCW, and VMWI. FSK is sent after polarity reversal and DTAS and before first ring. Waits for ACK from CPE after DTAS for CIDCW. Polarity reversal is applied only if equipment is on hook. The default is Bellcore(N.Amer, China).
FXS Port Power Limit	The choices are from 1 to 8. The default is 3.
Caller ID FSK Standard	The SRP supports bell 202 and v.23 standards for caller ID generation. The default is bell 202.
Feature Invocation Method	Select the method you want to use, Default or Sweden default. The default is Default.

Line Pages (1–4)

Use the Line pages to configure the lines for voice services.

NOTE Depending on your model number, the number of available lines may be different. The SRP520-U models only support 2 lines (Line 1 and Line 2), while the SRP540 models support 4 lines (Line 1–4).

These pages include the following sections:

- **Line Enable**
- **Streaming Audio Server**
- **NAT Settings**
- **Network Settings**
- **SIP Settings**
- **Call Feature Settings**
- **Proxy and Registration**
- **Subscriber Information**
- **Supplementary Service Subscription**
- **Audio Configuration**
- **Dial Plan**
- **FXS Port Polarity Configuration**

In a configuration profile, the Line parameters must be appended with the appropriate numeral (for example, [1] or [2]) to identify the line to which the setting applies.

Line Enable

Voice > Line 1–4 > Line Enable

Line Enable	To enable this line for service, select **yes**. Otherwise, select no. The default is yes.

Streaming Audio Server

Voice > Line 1–4 > Streaming Audio Server (SAS)

SAS Enable	To enable the use of the line as a streaming audio source, select yes. Otherwise, select no. If enabled, the line cannot be used for outgoing calls. Instead, it auto-answers incoming calls and streams audio RTP packets to the caller. The default is no.
SAS DLG Refresh Intvl	If this value is not zero, it is the interval at which the streaming audio server sends out session refresh (SIP re-INVITE) messages to determine whether the connection to the caller is still active. If the caller does not respond to the refresh message, the SRP ends this call with a SIP BYE message. The range is 0 to 255 seconds (0 means that the session refresh is disabled.) The default is 30.

SAS Inbound RTP Sink	This setting works around devices that do not play inbound RTP if the streaming audio server line declares itself as a send-only device and tells the client not to stream out audio. Enter a Fully Qualified Domain Name (FQDN) or IP address of an RTP sink; this value is used by the streaming audio server line in the SDP of its 200 response to an inbound INVITE message from a client. The purpose of this parameter is to work around devices that do not play inbound RTP if the SAS line declares itself as a send-only device and tells the client not to stream out audio. This parameter is a FQDN or IP address of a RTP sink to be used by the SAS line in the SDP of its 200 response to inbound INVITE from a client. It will appear in the c = line and the port number and, if specified, in the m = line of the SDP. If this value is not specified or equal to 0, then c = 0.0.0.0 and a=sendonly will be used in the SDP to tell the SAS client to not to send any RTP to this SAS line. If a non-zero value is specified, then a=sendrecv and the SAS client will stream audio to the given address. Special case: If the value is $IP, then the SAS line's own IP address is used in the c = line and a=sendrecv. In that case the SAS client will stream RTP packets to the SAS line. The default value is empty.

NAT Settings

Voice > Line 1–4 > NAT Settings

NAT Mapping Enable	Used to externally map IP addresses and SIP/RTP ports in SIP messages. The default is no. **NOTE** Typically, you will not need to change this as voice ports are bound to the WAN interface (and are therefore not subjected to NAT).

NAT Keep Alive Enable	To send the configured NAT keep alive message periodically, select yes. Otherwise, select no. The default is no.
NAT Keep Alive Msg	Enter the keep alive message that should be sent periodically to maintain the current NAT mapping. If the value is $NOTIFY, a NOTIFY message is sent. If the value is $REGISTER, a REGISTER message without contact is sent. The default is $NOTIFY.
NAT Keep Alive Dest	Destination that should receive NAT keep alive messages. If the value is $PROXY, the messages are sent to the current proxy server or outbound proxy server. The default is $PROXY.

Network Settings

Voice > Line 1–4 > Network Settings

SIP ToS/DiffServ Value	TOS/DiffServ field value in UDP IP packets carrying a SIP message. The default is 0x68.
SIP CoS Value [0-7]	CoS value for SIP messages. The default is 3.
RTP ToS/DiffServ Value	ToS/DiffServ field value in UDP IP packets carrying RTP data. The default is 0xb8.
RTP CoS Value [0- 7]	CoS value for RTP data. The default is 6.

Network Jitter Level	Determines how jitter buffer size is adjusted by the SRP. Jitter buffer size is adjusted dynamically. The minimum jitter buffer size is 30 milliseconds or (10 milliseconds + current RTP frame size), whichever is larger, for all jitter level settings. However, the starting jitter buffer size value is larger for higher jitter levels. This setting controls the rate at which the jitter buffer size is adjusted to reach the minimum. Select the appropriate setting: **low**, **medium**, **high**, **very high**, or **extremely high**. The default is high.
Jitter Buffer Adjustment	Controls how the jitter buffer should be adjusted. Select the appropriate setting: **up and down**, **up only**, **down only**, or **disable**. The default is up and down.
Auto PSTN Fallback	To enable the Line router to call the FXO port when the IP service is unavailable, select **yes**. Otherwise, select **no**. The default is yes.

SIP Settings

Voice > Line 1–4 > SIP Settings

SIP Transport	The TCP choice provides “guaranteed delivery,” which assures that lost packets are retransmitted. TCP also guarantees that the SIP packages are received in the same order that they were sent. As a result, TCP overcomes the main disadvantages of UDP. In addition, for security reasons, most corporate firewalls block UDP ports. With TCP, new ports do not need to be opened or packets dropped, because TCP is already in use for basic activities such as Internet browsing or e-commerce. Options are: **UDP**, **TCP**, **TLS**. The default is UDP.

SIP Port	Port number of the SIP message listening and transmission port. The default is 5060.
SIP 100REL Enable	To enable the support of 100REL SIP extension for reliable transmission of provisional responses (18x) and use of PRACK requests, select **yes**. Otherwise, select **no**. The default is no.
EXT SIP Port	The external SIP port number.
Auth Resync-Reboot	If this feature is enabled, the SRP authenticates the sender when it receives the NOTIFY resync reboot (RFC 2617) message. To use this feature, select **yes**. Otherwise, select **no**. The default is yes.
SIP Proxy-Require	The SIP proxy can support a specific extension or behavior when it sees this header from the user agent. If this field is configured and the proxy does not support it, it responds with the message, unsupported. Enter the appropriate header in the field provided.
SIP Remote-Party-ID	To use the Remote-Party-ID header instead of the From header, select **yes**. Otherwise, select **no**. The default is yes.
SIP GUID	The Global Unique ID is generated for each line for each device. When it is enabled, the SRP adds a GUID header in the SIP request. The GUID is generated the first time the unit boots up and stays with the unit through rebooting and even factory reset. This feature was requested by Bell Canada (Nortel) to limit the registration of SIP accounts. The default is no.

SIP Debug Option	SIP messages are received at or sent from the proxy listen port. This feature controls which SIP messages to log. The choices are: ▪ **none**—No logging. ▪ **1-line**—Logs the start-line only for all messages. ▪ **1-line excl. OPT**—Logs the start-line only for all messages except OPTIONS requests/responses. ▪ **1-line excl. NTFY**—Logs the start-line only for all messages except NOTIFY requests/responses. ▪ 1-**line excl. REG**—Logs the start-line only for all messages except REGISTER requests/responses. ▪ **1-line excl. OPT|NTFY|REG**—Logs the start-line only for all messages except OPTIONS, NOTIFY, and REGISTER requests/responses. ▪ **full**—Logs all SIP messages in full text. ▪ **full excl. OPT**—Logs all SIP messages in full text except OPTIONS requests/responses. ▪ **full excl. NTFY**—Logs all SIP messages in full text except NOTIFY requests/responses. ▪ **full excl. REG**—Logs all SIP messages in full text except REGISTER requests/responses. ▪ **full excl. OPT|NTFY|REG**—Logs all SIP messages in full text except for OPTIONS, NOTIFY, and REGISTER requests/responses. The default is none.

RTP Log Intvl	The interval for the RTP log. The default is 0.
Restrict Source IP	If Lines 1 and 2 use the same SIP Port value and the Restrict Source IP feature is enabled, the proxy IP address for Lines 1 and 2 is treated as an acceptable IP address for both lines. To enable the Restrict Source IP feature, select yes. Otherwise, select no. If configured, the SRP will drop all packets sent to its SIP Ports originated from an untrusted IP address. A source IP address is untrusted if it does not match any of the IP addresses resolved from the configured Proxy (or Outbound Proxy if Use Outbound Proxy is yes). The default is no.
Referor Bye Delay	Controls when the SRP sends BYE to terminate stale call legs upon completion of call transfers. Multiple delay settings (Referor, Refer Target, Referee, and Refer-To Target) are configured on this screen. For the Referor Bye Delay, enter the appropriate period of time in seconds. The default is 4.
Refer Target Bye Delay	For the Refer Target Bye Delay, enter the appropriate period of time in seconds. The default is 0.
Referee Bye Delay	For the Referee Bye Delay, enter the appropriate period of time in seconds. The default is 0.
Refer-To Target Contact	To contact the refer-to target, select yes. Otherwise, select no. The default is no.

Sticky 183	If this feature is enabled, the SRP ignores further 180 SIP responses after receiving the first 183 SIP response for an outbound INVITE. To enable this feature, select yes. Otherwise, select no. The default is no.
Use Anonymous With RPID	When set to yes, use "anonymous" in the SIP message. The default is yes.
Use Local Addr In From	Use the local SRP IP address in the SIP FROM message. The default is no.
Auth INVITE	When enabled, authorization is required for initial incoming INVITE requests from the SIP proxy.
Reply 182 On Call Waiting	When enabled, the SRP replies with a SIP182 response to the caller if it is already in a call and the line is off-hook. To use this feature select **yes**. The default is no.

Call Feature Settings

Voice > Line 1–4 > Call Feature Settings

Blind Attn-Xfer Enable	Enables the SRP to perform an attended transfer operation by ending the current call leg and performing a blind transfer of the other call leg. If this feature is disabled, the SRP performs an attended transfer operation by referring the other call leg to the current call leg while maintaining both call legs. To use this feature, select **yes**. Otherwise, select **no**. The default is no.
MOH Server	User ID or URL of the auto-answering streaming audio server. When only a user ID is specified, the current or outbound proxy is contacted. Music-on-hold is disabled if the MOH Server is not specified.

Xfer When Hangup Conf	Makes the SRP perform a transfer when a conference call has ended. Select **yes** or **no** from the drop-down menu. The default is yes.
Conference Bridge URL	This feature supports external conference bridging for n-way conference calls (n>2), instead of mixing audio locally. To use this feature, set this parameter to that of the server's name. For example: conf@mysefver.com:12345 or conf (which uses the Proxy value as the domain).
Conference Bridge Ports	Select the maximum number of conference call participants. The range is 3 to 10. The default is 3.

Proxy and Registration

Voice > Line 1–4 > Proxy and Registration

Proxy	SIP proxy server for all outbound requests.
Outbound Proxy SIP	SIP Outbound Proxy Server where all outbound requests are sent as the first hop.
Use Outbound Proxy	Enables the use of an Outbound Proxy. If set to no, the Outbound Proxy and Use OB Proxy in Dialog parameters are ignored. The default is no.
Use OB Proxy In Dialog	Whether to force SIP requests to be sent to the outbound proxy within a dialog. Ignored if the parameter Use Outbound Proxy is no, or the Outbound Proxy parameter is empty. The default is yes.
Register	Enable periodic registration with the Proxy parameter. This parameter is ignored if Proxy is not specified. The default is yes.

Make Call Without Reg	Allow making outbound calls without successful (dynamic) registration by the unit. If No, dial tone will not play unless registration is successful. The default is no.
Register Expires	Expires value (in seconds) in a REGISTER request. The SRP will periodically renew registration shortly before the current registration expired. This parameter is ignored if the Register parameter is no. Range: 0 – (2^{31} – 1) sec. The default is 3600.
Ans Call Without Reg	Allow answering inbound calls without successful (dynamic) registration by the unit. The default is no.
Use DNS SRV	Whether to use DNS SRV lookup for Proxy and Outbound Proxy. The default is no.
DNS SRV Auto Prefix	If enabled, the SRP will automatically prepend the Proxy or Outbound Proxy name with _sip._udp when performing a DNS SRV lookup on that name. The default is no.
Proxy Fallback Intvl	This parameter sets the delay (sec) after which the SRP will retry from the highest priority proxy (or outbound proxy) servers after it has failed over to a lower priority server. This parameter is useful only if the primary and backup proxy server list is provided to the SRP via DNS SRV record lookup on the server name. (Using multiple DNS A record per server name does not allow the notion of priority and so all hosts will be considered at the same priority and the SRP will not attempt to fall back after a fail over). The default is 3600.

Proxy Redundancy Method	Select Normal or Based on SRV Port. The SRP creates an internal list of proxies returned in the DNS SRV records. If you select Normal, the list contains proxies ranked by weight and priority. If you select Based on SRV Port, the SRP uses Normal, the inspects the port number based on the first listed proxy port. The default is Normal.
Voice Mail Server	Enter the URL or IP address of the server.
Mailbox Subscribe Expires	Sets subscription interval for voicemail message waiting indication.

Subscriber Information

Voice > Line 1–4 > Subscriber Information

Display Name	Display name for caller ID.
User ID	User ID for this line.
Password	Password for this line.
Use Auth ID	To use the authentication ID and password for SIP authentication, select yes. Otherwise, select no to use the user ID and password. The default is no.
Auth ID	Authentication ID for SIP authentication.
Directory Number	Enter the number for this line.
Mini Certificate	Base64 encoded of Mini-Certificate concatenated with the 1024-bit public key of the CA signing the MC of all subscribers in the group. The default is empty.
SRTP Private Key	Base64 encoded of the 512-bit private key per subscriber for establishment of a secure call. The default is empty.

Supplementary Service Subscription

The SRP provides native support of a large set of enhanced or supplementary services. All of these services are optional. The parameters listed in the following table are used to enable or disable a specific supplementary service. A supplementary service should be disabled if a) the user has not subscribed for it, or b) the Service Provider intends to support similar service using other means than relying on the SRP.

Voice > Line 1–4 > Supplementary Service Subscription

Call Waiting Serv	Enable Call Waiting Service. The default is yes.
Block CID Serv	Enable Block Caller ID Service. The default is yes.
Block ANC Serv	Enable Block Anonymous Calls Service The default is yes.
Dist Ring Serv	Enable Distinctive Ringing Service The default is yes.
Cfwd All Serv	Enable Call Forward All Service The default is yes.
Cfwd Busy Serv	Enable Call Forward Busy Service The default is yes.
Cfwd No Ans Serv	Enable Call Forward No Answer Service The default is yes.
Cfwd Sel Serv	Enable Call Forward Selective Service The default is yes.
Cfwd Last Serv	Enable Forward Last Call Service The default is yes.
Block Last Serv	Enable Block Last Call Service The default is yes.

Accept Last Serv	Enable Accept Last Call Service The default is yes.
DND Serv	Enable Do Not Disturb Service The default is yes.
CID–Serv	Enable Caller ID Service The default is yes.
CWCID Serv	Enable Call Waiting Caller ID Service The default is yes.
Call Return Serv	Enable Call Return Service The default is yes.
Call Redial Serv	Enable Call Redial Service.
Call Back Serv	Enable Call Back Service.
Three Way Call Serv	Enable Three Way Calling Service. Three Way Calling is required for Three Way Conference and Attended Transfer. The default is yes.
Three Way Conf Serv	Enable Three Way Conference Service. Three Way Conference is required for Attended Transfer. The default is yes.
Attn Transfer Serv	Enable Attended Call Transfer Service. Three Way Conference is required for Attended Transfer. The default is yes.
Unattn Transfer Serv	Enable Unattended (Blind) Call Transfer Service. The default is yes.
MWI Serv	Enable MWI Service. MWI is available only if a Voice Mail Service is set-up in the deployment. The default is yes.

VMWI Serv	Enable VMWI Service (FSK). The default is yes.
Speed Dial Serv	Enable Speed Dial Service. The default is yes.
Secure Call Serv	Enable Secure Call Service. The default is yes.
Referral Serv	Enable Referral Service. See the Referral Services Codes parameter for more details. The default is yes.
Feature Dial Serv	Enable Feature Dial Service. See the Feature Dial Services Codes parameter for more details. The default is yes.
Service Announcement Serv	Enable Service Announcement Service. The default is yes.

Audio Configuration

Voice > Line 1–4 > Audio Configuration

Preferred Codec	Preferred codec for all calls. (The actual codec used in a call still depends on the outcome of the codec negotiation protocol.) Select one of the following: **G711u, G711a, G726-32,** or **G729a.** The default is G711u.
Second Preferred Codec	Second preferred codec for all calls. (The actual codec used in a call still depends on the outcome of the codec negotiation protocol.) Select one of the following:.**Unspecified**, **G711u, G711a, G726-32,** or **G729a.** The default is Unspecified.

Third Preferred Codec	Third preferred codec for all calls. (The actual codec used in a call still depends on the outcome of the codec negotiation protocol.) Select one of the following: **Unspecified, G711u, G711a, G726-16, G726-24, G726-32, G726-40, G729a,** or **G723.** The default is Unspecified.
Use Pref Codec Only	To use only the preferred codec for all calls, select **yes**. (The call fails if the far end does not support this codec.) Otherwise, select **no**. The default is no.
Silence Supp Enable	To enable silence suppression so that silent audio frames are not transmitted, select **yes**. Otherwise, select **no**. The default is no.
Silence Threshold	Select the appropriate setting for the threshold: high, medium, or low. The default is medium.
G729a Enable	To enable the use of the G.729a codec at 8 kbps, select yes. Otherwise, select **no**. The default is yes.
Echo Canc Enable	To enable the use of the echo canceller, select **yes**. Otherwise, select **no**. The default is yes.
Echo Canc Adapt Enable	To enable the echo canceller to adapt, select **yes**. Otherwise, select **no**. The default is yes.
Echo Supp Enable	To enable the use of the echo suppressor, select **yes**. Otherwise, select **no**. The default is yes.
Echo Cancel Delay	To enable the use of echo cancel delay select **yes**. Otherwise, select **no**. The default is yes.

Echo Cancel Tail	To enable the use of echo cancel tail select **yes**. Otherwise, select **no**. The default is yes.
FAX V21 Detect Enable	To enable detection of V21 fax tones, select **yes**. Otherwise, select **no**. The default is yes.
G726-32 Enable	To enable the use of the G.726 codec at 32 kbps, select **yes**. Otherwise, select **no**. The default is yes.
FAX CNG Detect Enable	To enable detection of the fax Calling Tone (CNG), select **yes**. Otherwise, select **no**. The default is yes.
FAX Passthru Codec	Select the codec for fax passthrough, G711u or G711a. The default is G711u.
DTMF Process INFO	To use the DTMF process info feature, select yes. Otherwise, select **no**. The default is yes.
FAX Codec Symmetric	To force the SRP to use a symmetric codec during fax passthrough, select **yes**. Otherwise, select **no**. The default is yes.
DTMF Process AVT	To use the DTMF process AVT feature, select **yes**. Otherwise, select **no**. The default is yes.
FAX Passthru Method	Select the fax passthrough method: None, NSE, or ReINVITE. The default is NSE.

DTMF Tx Method	Select the method to transmit DTMF signals to the far end: **InBand, AVT, INFO,** or **Auto**. InBand sends DTMF using the audio path. AVT sends DTMF as AVT events. INFO uses the SIP INFO method. Auto uses InBand or AVT based on the outcome of codec negotiation. The default is Auto.
DTMF Tx Mode	**DTMF Detection Tx Mode** is available for SIP information and AVT. Options are **Strict** or **Normal**. The default is Strict for which the following are true: A **DTMF digit** requires an extra hold time after detection. The **DTMF level** threshold is raised to -20 dBm. The minimum and maximum duration thresholds are: ▪ strict mode for AVT: 70 ms ▪ normal mode for AVT: 40 ms ▪ strict mode for SIP info: 90 ms ▪ normal mode for SIP info: 50 ms
FAX Process NSE	To use the fax process NSE feature, select **yes**. Otherwise, select **no**. The default is yes.
Hook Flash Tx Method	Select the method for signaling hook flash events: None, AVT, or INFO. None does not signal hook flash events. AVT uses RFC2833 AVT (event = 16). INFO uses SIP INFO with the single line signal=hf in the message body. The MIME type for this message body is taken from the Hook Flash MIME Type setting. The default is None.
FAX Disable ECAN	If enabled, this feature automatically disables the echo canceller when a fax tone is detected. To use this feature, select **yes**. Otherwise, select **no**. The default is no**.**

Release Unused Codec	This feature allows the release of codecs not used after codec negotiation on the first call, so that other codecs can be used for the second line. To use this feature, select **yes**. Otherwise, select **no**. The default is yes.
FAX Enable T38	To enable the use of ITU-T T.38 standard for FAX Relay, select **yes**. Otherwise, select **no**. The default is yes.
FAX T38 Redundancy	Select the appropriate number to indicate the number of previous packet payloads to repeat with each packet. Choose 0 for no payload redundancy. The higher the number, the larger the packet size and the more bandwidth consumed. The default is 1.
FAX T38 ECM Enable	Select **yes** to enable T.38 Error Correction Mode. Otherwise, select **no**.
FAX Tone Detect Mode	This parameter has three possible values: **caller or callee**: The SRP will detect FAX tone whether it is callee or caller. **caller only:** The SRP detects FAX tone only if it is the caller. **callee only**: The SRP detects FAX tone only if it is the callee. The default is caller or callee.
Auto Dump Option1/ Option2	Parameters used by cusomter support to capture audio on the line.

Dial Plan

The default dial plan script for each line is as follows: (*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxx|xxxxxxxxxxxx.). The syntax for a dial plan expression is described in the table.

Voice > Line 1–4 > Dial Plan

Dial Plan Entry	Functionality
*xx	Allow arbitrary 2 digit star code
[3469]11	Allow x11 sequences
0	Operator
00	Int'l Operator
[2-9]xxxxxx	US local number
1xxx[2-9]xxxxxx	US 1 + 10-digit long distance number
xxxxxxxxxxxx.	Everything else (Int'l long distance, FWD, ...)

Dial Plan	Dial plan script for this line. The default is (*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxxS0|xxxxxxxxxxxx.) Each parameter is separated by a semi-colon (;). Example 1: *1xxxxxxxxxx<:@fwdnat.pulver.com:5082;uid=jsmith;pwd=xy z Example 2: *1xxxxxxxxxx<:@fwd.pulver.com;nat;uid=jsmith;pwd=xyz Example 3: [39]11<:@gw0>
PSTN Fallback Dial Plan	Dial plan script for routing calls to the FXO port when the IP service is unavailable. The default script is (S0<:@gw0>).

Enable IP Dialing	Enable or disable IP dialing. If IP dialing is enabled, one can dial [user-id@]a.b.c.d[:port], where '@', '.', and ':' are dialed by entering *, user-id must be numeric (like a phone number) and a, b, c, d must be between 0 and 255, and port must be larger than 255. If port is not given, 5060 is used. Port and User-Id are optional. If the user-id portion matches a pattern in the dial plan, then it is interpreted as a regular phone number according to the dial plan. The INVITE message, however, is still sent to the outbound proxy if it is enabled. The default is no.
Emergency Number	Comma separated list of emergency number patterns. If outbound call matches one of the pattern, the SRP will disable hook flash event handling. The condition is restored to normal after the call ends. Blank signifies no emergency number. Maximum number length is 63 characters. The default is blank.

FXS Port Polarity Configuration

Voice > Line 1–4 > FXS Port Polarity Configuration

Idle Polarity	Polarity before a call is connected: Forward or Reverse. The default is Forward.
Caller Conn Polarity	Polarity after an outbound call is connected: Forward or Reverse. The default is Forward.
Callee Conn Polarity	Polarity after an inbound call is connected: Forward or Reverse. The default is Forward.

PSTN Page (SRP540 Models Only)

Use the PSTN pages to configure the PSTN (Public Switched Telephone Network) line on the SRP.

These pages include the following sections:

- **PSTN Line Enable**
- **SIP Settings**
- **Ring Settings**
- **PSTN Timer Values**
- **PSTN Disconnect Detection**
- **International Settings**

PSTN Line Enable

Voice > PSTN > PSTN Line Enable

PSTN Line Enable	To enable this line for service, select yes. Otherwise, select no. The default is yes.
PSTN Contact List	List the phone ports that should be alerted to incoming calls. List the required port numbers separated by '+'. The default setting alerts all ports using the list 1+2+3+4.

SIP Settings

Voice > PSTN > SIP Settings

SIP Debug Option	SIP messages are received at or sent from the proxy listen port. This feature controls which SIP messages to log. Choices are as follows: **none**—No logging. **1-line**—Logs the start-line only for all messages. **full**—Logs all SIP messages in full text. The default is none.

Ring Settings

Voice > PSTN > Ring Settings

Default Ring	Set the default ring for calls from the PSTN. Select 1–8 or follow the line-specific configurations.

PSTN Timer Values

Voice > PSTN > PSTN Timer Values (sec)

PSTN Ring Thru Delay	Delay in seconds before starting to ring through Line 1 after the PSTN starts ringing. In order for Line 1 to have the caller-id information, the delay should be set to larger than the delay required to complete the PSTN caller-id delivery (such as 5s). The range is 0-255. The default is 1.
PSTN Dialing Delay	Delay after going off hook before the SRP dials a PSTN number. The range is 0-255. The default is 1.
PSTN Ring Timeout	Delay after a ring burst before the SRP decides that PSTN ring has ceased. The range is 0-255. The default is 5.
PSTN Dial Digit Len	Determines the on/off time when transmitting digits through the FXO port. The syntax is *on-time/off-time*, where *on-time* and *off-time* are expressed in seconds with up to two decimal places, within the permitted range, which is from .05 to 3.00. The default is .2/.2. If this value is blank, the default is used.
PSTN Hook Flash Len	The length of the hook flash in seconds. During a PSTN-to-VoIP gateway call, the SRP processes the out-of-band hook flash signal sent from the VoIP peer through a hook-flash (momentary on-hook signal) on the FXO port. This allows the VoIP peer to initiate a three-way conference call and subsequent call transfer. The duration of the on-hook signal can be configured using this parameter. The default is 0.25. The permitted range is limited to 0.02 to 1.6 seconds.

PSTN Ring Thru CWT Delay	Specify the delay before incoming PSTN calls will ring Line 1 using a Call Waiting Tone. The default is 3.

PSTN Disconnect Detection

Voice > PSTN > PSTN Disconnect Detection

Detect CPC	CPC is a brief removal of tip-and-ring voltage. If enabled, the SRP will disconnect both call legs when this signal is detected. The default is yes.
Detect Polarity Reversal	If enabled, SPA will disconnect both call legs when this signal is detected during a gateway call. If it is a PSTN gateway call, the 1st polarity reversal is ignored and the 2nd one triggers the disconnection. For VoIP gateway call, the 1st polarity reversal triggers the disconnection. The default is yes.
Detect PSTN Long Silence	If enabled, SRP will disconnect both call legs when the PSTN side has no voice activity for a duration longer than the length specified in the PSTN Long Silence Duration parameter during a gateway call. The default is no.
Detect VoIP Long Silence	If enabled, SRP will disconnect both call legs when the VoIP side has no voice activity for a duration longer than the length specified in the VoIPnLong Silence Duration parameter during a gateway call. The default is no.
PSTN Long Silence Duration	This value is minimum length of PSTN silence (or inactivity) in seconds to trigger a gateway call disconnection if Detect PSTN Long Silence is yes. The default is 30.
VoIP Long Silence Duration	This value is minimum length of VoIP silence (or inactivity) in seconds to trigger a gateway call disconnection if Detect VoIP Long Silence is yes. The default is 30.

PSTN Silence Threshold	This parameter adjusts the sensitivity of PSTN silence detection. Choose from {very low, low, medium, high, very high}. The higher the setting, the easier to detect silence which is easier to trigger a disconnection. The default is medium.
Min CPC Duration	Specify the minimum duration of a low tip-and-ring voltage (below 1V) for the Gateway to recognize it as a CPC signal or PSTN line removal. The default is 0.2.
Detect Disconnect Tone	If enabled, SRP will disconnect both call legs when it detects the disconnect tone from the PSTN side during a gateway call. Disconnect tone is specified in the Disconnect Tone parameter, which depends on the region of the PSTN service. The default is yes.

Disconnect Tone	This value is the tone script, which describes to the SPA the tone to detect as a disconnect tone. The syntax follows a standard Tone Script with some restrictions. Default value is standard US reorder (fast busy) tone, for 4 seconds. Restrictions: ▪ Two frequency components must be given. If single frequency is desired, the same frequency is used for both ▪ The tone level value is not used. –30 (dBm) should be used for now. ▪ Only one segment set is allowed ▪ Total duration of the segment set is interpreted as the minimum duration of the tone to trigger detection ▪ Six segments of on/off time (seconds) can be specified. A 10% margin is used to validated cadence characteristics of the tone. The Disconnect Tone Script values for various countries are as follows: **US** (default)—480@-30,620@-30;4(.25/.25/1+2) **UK**—400@-30,400@-30; 2(3/0/1+2) **France**—440@-30,440@-30; 2(0.5/0.5/1+2) **Germany**—425@-10; 10(0.48/0.48/1) **Netherlands**—425@-30,425@-30; 2(0.5/0.5/1+2) **Sweden**—425@-10; 10(0.25/0.25/1) **Norway**—425@-10; 10(0.5/0.5/1) **Italy**—425@-30,425@-30; 2(0.2/0.2/1+2) **Spain**—425@-10; 10(0.2/0.2/1,0.2/0.2/1,0.2/0.6/1) **Portugal**—425@-10; 10(0.5/0.5/1) **Poland**—425@-10; 10(0.5/0.5/1) **Denmark**—425@-10; 10(0.25/0.25/1) **New Zealand**—400@-15; 10(0.25/0.25/1) **Australia**—425@-13; 10(0.375/0.375/1)

International Settings

Voice > PSTN > International Settings

FXO Country Setting	Select the country of deployment from the drop-down list.
FXO Port Impedance	Desired impedance of the FXO Port. Choices are: {**600**, **900, 270+750||150nF, 220+820||120nF**, **370+620||310nF**, **320+1050|| 230nF**, **370+820||110nf**, **275+780||115nF**, **120+820||110nF**, **350+100 || 210nF**, **0 + 90 ||130nF**}, **600+2.16uF**, **900+1uF, 900+2.16uF, 6001uF,** or **Global**. The default is 600. The impedance values for various countries follows: ▪ **US**—600 ▪ **EU (UK, France, Germany, Netherlands, Sweden, Norway, Italy, Spain, Portugal, Poland, and Denmark)**—270+750||150nF ▪ **Australia**—220+820||120nF ▪ **New Zealand**—370+620||310nF
CO (Device) Termination	Specify the device termination value. Choices are: **Unknown**, **900+2.16uF**, **600**,**1200+376 ||112nf**, **150+510||150nF, 600||15uF**, **220+120||115nF**, **220+820||115nF**, **370 + 620||310nF**, **220+820||120nF**, **300+1000|| 270+750||150nF, 200+560||100nF**
Line Type	Specify the line type. Choices are EIA (0-7), 2000 ft., and 22, 24, or 26 awg.
Impedance Match	Determines the best match impedance setting for the FXO or FXS port. The default is no.
Ring Frequency Min	Specify the lower limit of the ring frequency used to detect the ring signal. The default is **10**.
SRP To PSTN Gain	dB of digital gain (or attenuation if negative) to be applied to the signal sent from the SRP to the PSTN. The range is 15 to 12. The default is 0.

Ring Frequency Max	Specify the higher limit of the ring frequency used to detect the ring signal. The default is 100.
PSTN To SRP Gain	dB of digital gain (or attenuation if negative) to be applied to the signal sent from the PSTN to the SRP. The range is - 15 to 12. The default is 0.
Ring Validation Time	Specify the minimum signal duration required by the SRP for recognition as a ring signal. The default is 256 ms.
Tip/Ring Voltage Adjust	Choices are {3.1V, 3.2V, 3.35V, 3.5V}. The default is 3.5V.
Ring Indication Delay	Choose from {0, 256, 512, 768, 1024, 1280, 1536, 1792} (ms). The default is 512ms.
Operational Loop Current Min	Choices for mA are {10, 12, 14, 16). The default is 10.
Ring Timeout	Choose from {0, 128, 256, 384, 512, 640, 768, 896, 1024, 1152, 1280, 1408, 1536, 1664, 1792, 1920} (ms). The default is 640 ms.
On-Hook Speed	Choose from {Less than 0.5ms, 3ms (ETSI), 26ms (Australia)}. The default is Less than 0.5ms.
Ring Threshold	Choose from {13.5–16.5, 19.35–23.65, 40.5–49.5} (Vrms). The default is 13.5-16.5 Vrms.
Current Limiting Enable	Enable or disable current limiting. The default is no.
Ringer Impedance	Choose from {High, Synthesized (Poland, S.Africa, Slovenia)}. The default is high.
Line-In-Use Voltage	Determines the voltage threshold at which the SRP assumes the PSTN is in use by another handset sharing the same line (and will declare PSTN gateway service not available to incoming VoIP callers). The default value is 30v.

User Pages

Use these pages to configure the caller user settings.

NOTE Depending on your model number, the number of available user pages may be different. Because the SRP520-U models only support 2 lines (Line 1 and Line 2), only two user pages will appear (User 1 and User 2).

These pages include the following sections:

- **Call Forward Settings**
- **Selective Call Forward Settings**
- **Speed Dial Settings**
- **Supplementary Service Settings**
- **Distinctive RIng Settings**
- **Ring Settings**

When a call is made from one of the available lines, the SRP uses the user and line settings for that line; there is no user login support. Per user parameter tags must be appended with [1] [2][3] or [4] (corresponding to appropriate line) in the configuration profile. It is omitted for readability.

Call Forward Settings

Voice > User 1–4 > Call Forward Settings

Cfwd All Dest	Forward number for Call Forward All Service. The default is blank.
Cfwd Busy Dest	Forward number for Call Forward Busy Service. The default is blank.
Cfwd No Ans Dest	Forward number for Call Forward No Answer Service. The default is blank.
Cfwd No Ans Delay	Delay in sec before Call Forward No Answer triggers. The default is 20.

Selective Call Forward Settings

Voice > User 1-4 > Selective Call Forward Settings

Cfwd Sel1- 8 Caller	Caller number pattern to trigger Call Forward Selective 1, 2, 3, 4, 5, 6, 7, or 8. The default is blank.
Cfwd Sel1 - 8 Dest	Forward number for Call Forward Selective 1, 2, 3, 4, 5, 6, 7, or 8. The default is blank.
Cfwd Last Caller	The Caller number that is actively forwarded to Cfwd Last Dest by using the Call Forward Last activation code. The default is blank.
Cfwd Last Dest	Forward number for the Cfwd Last Caller parameter. The default is blank.
Block Last Caller	ID of caller blocked via the Block Last Caller service. The default is blank.
Accept Last Caller	ID of caller accepted via the Accept Last Caller service. The default is blank.

Speed Dial Settings

Voice > User 1-4 > Speed Dial Settings

Speed Dial 2-9	Target phone number (or URL) assigned to speed dial 2, 3, 4, 5, 6, 7, 8, or 9. The default is blank.

Supplementary Service Settings

The SRP provides native support of a large set of enhanced or supplementary services. All of these services are optional. The parameters listed in the following table are used to enable or disable a specific supplementary service. A supplementary service should be disabled if a) the user has not subscribed for it, or b) the Service Provider intends to support similar service using other means than relying on the SRP.

Voice > User 1-4 > Supplementary Service Settings

CW Setting	Call Waiting on/off for all calls. The default is yes.
Block CID Setting	Block Caller ID on/off for all calls. The default is no.
Block ANC Setting	Block Anonymous Calls on or off. The default is no.
DND Setting	DND on or off. The default is no.
CID Setting	Caller ID Generation on or off. The default is yes.
CWCID Setting	Call Waiting Caller ID Generation on or off. The default is yes.
Dist Ring Setting	Distinctive Ring on or off. The default is yes.
Secure Call Setting	If yes, all outbound calls are secure calls by default. The default is no.
Message Waiting	The user can also manually modify it to clear or set the flag. Setting this value to yes can activate stutter tone and VMWI signal. This parameter is stored in long term memory and will survive after reboot or power cycle. The default is no.

Accept Media Loopback Request	Controls how to handle incoming requests for loopback operation. Choices are **Never**, **Automatic**, and **Manual**, where: **Never**—Never accepts loopback calls; reply 486 to the caller **Automatic**—Automatically accepts the call without ringing **Manual**—Rings the phone first, and the call must be picked up manually before loopback starts. The default is Automatic.
Media Loopback Mode	The loopback mode to assume locally when making call to request media loopback. Choices are **Source** and **Mirror.** The default is Source. If the SRP answers the call, the mode is determined by the caller.
Media Loopback Type	The loopback type to use when making a call to request media loopback operation. Choices are **Media** and **Packet**. The default is Media. **NOTE** If the SRP answers the call, then the loopback type is determined by the caller (the SRP always picks the first loopback type in the offer if it contains multiple type).

Distinctive RIng Settings

Caller number patterns are matched from Ring 1 to Ring 8. The first match (not the closest match) will be used for alerting the subscriber.

Voice > User > Distinctive Ring Settings

Ring1 - 8 Caller	Caller number pattern to play Distinctive Ring/CWT 1, 2, 3, 4, 5, 6, 7, or 8. The default is blank.

Ring Settings

Voice > User 1-4 > Ring Settings

Default Ring	Default ringing pattern, 1–8, for all callers. The default is 1.
Default CWT	Default CWT pattern, 1–8, for all callers. The default is 1.
Hold Reminder Ring	Ring pattern for reminder of a holding call when the phone is on-hook. The default is 8.
Call Back Ring	Ring pattern for call back notification. The default is 7.

7

Configuring VPN (IPv4)

This chapter describes how to configure VPN policies and settings for the SRP. It includes the following sections:

- **Site-to-Site IPsec VPN**
- **GRE Tunnel**
- **VPN Passthrough**
- **Cisco VPN Server**

To access these pages, click **VPN** from the Configuration Utility menu bar.

Site-to-Site IPsec VPN

This section describes how to configure the VPN settings to allow other sites to connect to your network. It includes the following topics:

- **NAT Traversal**
- **IKE Policy**
- **IPSec Policy**

NAT Traversal

If the SRP or any IPsec peer is located behind a network address translation device, enable IPsec NAT Traversal to detect and locate the translation. Keepalive traffic is then generated in accordance with RFC3947 to maintain the tunnel.

STEP 1 Click **VPN > Site-to-Site IPSec VPN > NAT Traversal**. The NAT Traversal window opens.

STEP 2 To enable NAT Traversal, select **Enabled**. The default is disabled.

STEP 3 Click **Submit** to save your changes.

IKE Policy

Use the IKE Policy page to configure a VPN IKE policy. Each IKE policy contains the parameters for setting IKE authentication rules. These IKE policies can be used in different VPN policies.

STEP 1 Click **VPN > Site to Site IPSec VPN > IKE Policy**. The IKE Policy window opens. From this window you can view the existing policies, edit a policy, and add a new IKE policy.

STEP 2 To add an IKE policy, click **Add Entry**. The IKE Policy configuration window for the new policy opens.

STEP 3 In the **Policy Name** field, enter a unique name for the VPN policy.

STEP 4 Choose an exchange mode from the drop-down list. Select **Main** mode if you want higher security, but a slower connection. Select **Aggressive** mode if you want a faster connection, but lowered security.

STEP 5 Set the IKE SA parameters as needed as defined in the **IKE Policy Settings** table.

STEP 6 If connected to a XAUTH server, enter a **Username** and **Password**. When enabled, the SRP can authenticate users from an external authentication server such as a RADIUS server.

STEP 7 Click **Submit** to save your settings.

IKE Policy Settings

General	
Policy Name	Enter a unique name for the VPN policy.
Exchange Mode	Choose the mode based on your requirements for security and speed. **Main**: Provides higher security, but a slower connection. Main Mode relies upon a two-way key exchange between the initiator and the receiver. The key-exchange process slows down the connection but increases security. **Aggressive**: Provides a faster connection, but lowered security. In Aggressive Mode there are fewer key exchanges between the initiator and the receiver. Both sides exchange information even before there is a secure channel.
Local ID and Remote ID	Enter the Local and Remote identifiers to use in IKE Phase 1 negotiation or leave these fields blank to omit the identify setting. Choices are: ▪ IP address (For example: 1.1.1.1) ▪ User Specified Name: FQDN (prefixed by the "**at sign** @) that signifies that it should not be resolved. For example: @www.cisco.com
IKE SA Parameters	
Encryption Algorithm	Encryption mode. Select from **DES**, **3DES**, **AES128**, **AES192**, and **AES256**.
Authentication Algorithm	Authentication algorithm for the IKA SA. Select from **MD5** or **SHA1**.
Diffie-Hellman (DH) Group	DH group used to set the strength of the algorithm in bits. Select from **Group 1 (768 bit)** or **Group 2 (1024 bit).**
Pre Shared Key	Enter an alphanumeric key to be shared with the IKE peer.

IKE Policy Settings

Enable Dead Peer (DPD) Detection	To enable DPD, select **Enable**. The default is Disable. DPD is not required for an IKE rule, but if enabled, helps keep the connection alive during times when there is no traffic.
DPD Interval	Enter an interval for DPD. This packet is sent periodically in interval seconds during no data traffic.
DPD Timeout	Enter a timeout (in seconds) for Dead Peer Detection.
Extended Authentication	
XAUTH Client Enable	Select **Enable** if the VPN peer requires Extended Authentication credentials. The default is Disable.
Username/ Password	Enter the credentials that the SRP uses to connect with the remote peer.

IPSec Policy

Use the IPSec Policy page to configure a VPN IPSec policy. The IPSec VPN policy contains the IPSec Security Association parameters that define the connection type and key type.

STEP 1 Click **VPN > Site to Site IPSec VPN > IPSec Policy**. The IPSec Policy window opens. From this page you can view the existing IPSec policies, edit an IPSec policy and add an IPSec policy. You can also view the details for each policy from the IPSec Details table.

STEP 2 To add an IPSec policy, click **Add Entry**. The new window for the IPSec Policy window opens.

STEP 3 To enable the new policy, select **Enable**.

STEP 4 Choose a **Policy Number** (identification) from the drop-down list.

STEP 5 In the **Policy Name** field, enter a unique name for the IPSec policy.

STEP 6 Choose a policy type from the drop-down list. Select either **Auto Policy** or **Manual Policy**.

STEP 7 Enter the IPSec Policy settings as defined in the **IPSec Policy Settings** table below.

STEP 8 Click **Submit** to save your settings.

The IKE policy appears in the List of IKE policies table on the IKE Policy Add Entry page. To view the policies, click the **View IKE Table** button.

IPSec Policy Settings

General Settings	
Enable	Check the box to activate the policy.
Policy Number	Enter an identification number for the policy.
Policy Name	Enter a unique name for the policy.
Policy Type	Choose the policy type. Select either **Auto Policy** or **Manual** Policy. The Auto Policy uses the IKE protocol to negotiate random keys for more security. If you choose this option, you must also set an IKE policy on the **Site to Site IPSec VPN > IKE Policy** page. The Manual Policy does not use IKE, which makes this policy more simple, but less secure.
Remote Endpoint	Choose how you want to identify the remote gateway for this site-to-site VPN tunnel. Select **IP Address** to enter an IP address, select **FQDN** to enter a Fully Qualified Domain Name, or select **Any** (available only for an Auto Policy). Be aware that an FQDN requires that the SRP can connect to a DNS server to resolve the address before establishing the VPN tunnel.
Encryption Algorithm	Choose the encryption algorithm. Select from **DES**, **3DES**, **AES128, AES192,** and **AES256**.
Integrity Algorithm	Choose an authentication algorithm. Select from **MD5** or **SHA-1**.
WAN Interface Name	Choose which WAN interface should be used to connect to the remote gateway for this site-to-site VPN tunnel. The default is System Default.
Auto Policy Parameters **(these options only appear if Auto Policy is selected)**	

IPSec Policy Settings

PFS	Select **Enable** to enable Perfect Forward Secrecy (PFS). The default is disabled. This feature requires a new Diffie-Hellman exchange for each phase-2 negotiation. While this process is slower, it ensures that no keys are dependent on any other previously used keys.
SA Lifetime	Enter the IPsec SA life time in seconds. The default is 7800 sec. (130 min.) The range is 60 to 28800 sec.
Manual Policy Parameters (these options only appear if Manual Policy is selected)	
SPI Incoming	Enter a hexidecimal value, for the incoming *Security Parameters Index* between 0x100 and 0xffffffff.
SPI Outgoing	Enter a hexdicimal value, for the outgoing *Security Parameters Index* between 0x100 and 0xffffffff.
Encryption Algorithm Key	Enter a hexidecimal value for the encryption algorithm key. The length depends on the Encryption Algorithm that you selected. Choices are DES:16 characters, 3DES: 48 characters, AES-128: 32 characters, AES-192: 48 characters, AES-256: 64 characters.
Integrity Algorithm Key	Enter a hexadecimal value for the integrity algorithm key. The length of the key depends on the Integrity Algorithm selected. Choices are MD5: 32 characters, SHA-1: 40 characters.
Local Traffic Selection	
Local IP	Determines which local hosts will be allowed to use the VPN. Select either a single **IP Address** or a **subnet** (IP Address and Subnet Mask).
Remote Traffic Selection	
Remote IP	Traffic from permitted local hosts to the remote IP address or subnet will be routed via the VPN tunnel. Select either a **single IP Address** or a **subnet** (IP Address and Subnet Mask).
Select IKE Policy	Choose an IKE Policy to associate with this IPSec Policy. To view all IKE policies, click the **View IKE Table** button.

GRE Tunnel

Use the GRE Tunnel page to configure Generic Routing Encapsulation (GRE). GRE is a tunneling protocol developed by Cisco that can encapsulate network layer protocol packet types inside IP tunnels, creating a virtual point-to-point link to the SRP at remote points over an IP internetwork.

STEP 1 Click **VPN > Site to Site IPSec VPN > GRE Tunnel**. The GRE Tunnel window opens. From this page you can view the existing GRE tunnels, edit a GRE tunnel and add a new GRE tunnel. You can also view the details for each tunnel from the GRE Details table.

STEP 2 To add a GRE tunnel, click **Add Entry**. The GRE IP Tunnel window opens.

STEP 3 Choose a Tunnel Number and enter a Tunnel Name.

STEP 4 To enable the tunnel, click the **Enable** box.

STEP 5 Specify the parameters for Checksum, Sequence, and Key as defined in the **GRE Tunnel Settings** table.

STEP 6 Choose the WAN interface through which the tunnel should be connected. For example: WAN1 or WAN2. System Default Route is the default.

STEP 7 Enter the destination IP address of the remote device that will terminate the new tunnel.

STEP 8 Enter the IP address and subnet mask of the remote host. Click the **Add** button to add additional IP addresses or click **Delete** to remove one.

STEP 9 Click **Submit** to save your settings.

GRE Tunnel Settings

Tunnel Number	Choose an identification number for this tunnel. You can create up to 10 tunnels.
Tunnel Name	Enter a name to describe this tunnel.
Enable	Check the box to enable the tunnel, or uncheck the box to disable it.
Checksum	Choose **Input**, **Output**, **Both**, or **None**. The default is None. Input requires that all inbound packets have the correct checksum. Output requires the checksums for outbound packets. Both requires the checksum for all inbound and outbound packets.
Sequence	Choose **None**, **Both**, **Input**, or **Output**. The default is None. Output requires a sequence number for outbound packets. Input requires a sequence number for inbound packets. Both requires a sequence number for inbound and outbound packets.
Key	Choose **None**, **Both**, **Input** and **Output** value. The default is None. Input parameter sets the key for input. Output parameter sets the key for output. Both sets the key to use in both directions.
Key value	If you chose a key, enter the key value between 0 and 4294967295.
WAN Interface Name	Choose the WAN interface used to create the GRE Tunnel with the remote host.
Destination IP or HostName	IP address or FQDN of the remote device that will terminate the tunnel.
Remote IP Address/ Subnet Mask	Lists the remote hosts and networks available through the tunnel.

GRE Tunnel Settings

Modify Remote IP Address/Subnet Mask	To define a host or network that is reachable through the tunnel, enter the address and subnet mask and click **Add**. To remove an address, select it in the Remote IP Address list and click **Delete**.

VPN Passthrough

Use the VPN Passthrough page to configure VPN passthrough for IPSec, PPTP, and L2TP protocols. Use this feature if there are devices behind the SRP that need IPsec tunnels to be set up independently, such as connecting to another router on the WAN.

STEP 1 Click **VPN > Site to Site IPSec VPN > VPN Passthrough**. The VPN Passthrough window opens.

STEP 2 IPsec, PPTP, and L2TP Passthrough are enabled by default. Click **Disabled** to disable any of these passthrough options.

STEP 3 Click **Submit** to save your settings.

VPN Passthrough Settings

IPSec Passthrough	Internet Protocol security (IPsec) is a suite of protocols used to implement secure exchange of packets at the IP layer. IPSec Passthrough is enabled by default. To disable it, select **Disabled**.
PPTP Passthrough	Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. PPTP Passthrough is enabled by default. To disable it, select **Disabled**.
L2TP Passthrough	Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions through the Internet on the Layer 2 level. L2TP Passthrough is enabled by default. To disable it, select **Disabled**.

Cisco VPN Server

This section describes how to configure the server polices. settings and users for the Cisco VPN Server. The Cisco VPN Server allows remote users to access Intranet resources through an encrypted IPSec VPN tunnel by using the Cisco VPN Client. See www.cisco.com/go/vpnclient.

NOTE Only the VPN Server or a site-to- site VPN can be used at a time on the SRP. If you enable VPN Server, site-to-site VPN is disabled.

Configuring Groups

Use the group page to configure the settings that control the Cisco VPN Server and the IPsec policies for communication with remote users.

STEP 1 Click **VPN > Cisco VPN Server > Group**. The Group window opens.

STEP 2 Click **Enable** to activate the VPN Server. The default is Disable.

STEP 3 Under Identity, specify the **Group Name** and **Password**.

STEP 4 If necessary make changes to the **IKE Phase 1** and **IKE Phase 2** settings to match the desired IPsec policies.

STEP 5 Specify the Mode Configuration settings.

NOTE The SRP520 models support up 5 concurrent connections /IP address assignments. The SRP540 models can support up to 10.

a. Set the **DNS1** field to the primary DNS server address. A backup DNS Server may optionally be specified in the **DNS2** field.

b. If necessary, specify the WINS servers to use.

c. (Optional) Enter a welcome message in the Banner field if desired. This message will be displayed to the VPN client user once the VPN session is established.

STEP 6 Click **Submit** to save your settings.

Cisco VPN Server Settings

Group	
Enable	Click **Enable** to activate the VPN Server. The default is Disable. **NOTE** Enabling the VPN Server will deactivate any site-to-site VPN tunnels that have been defined.
Identity	
Group Name	Enter the Cisco VPN Group name that will be used as an identifier for the VPN Server. This name must match the group name specified the VPN Client profile. The length can contain up to 32 characters and is case sensitive.
Password	Enter the Cisco VPN Group password. This password must match the group password specified the VPN Client profile. The length can contain up to 32 characters is case sensitive.
IKE Phase 1	
Aggressive Mode	Aggressive mode is applied by default and cannot be changed. This mode is used for negotiating phase one ISAKMP Security Associations (SAs) when using preshared keys for authentication.
ESP Algorithm	Enter an encryption algorithm for the ISAKMP SA. Choices are AES, DES, and 3DES. The default is AES.
AH Algorithm	Hash algorithm for the ISAKMP SA. Choices are MD5 and SHA1. The default is MD5.
Auth Method	Method used to authenticate the remote user. Choices are **PSK** or **PSK+XAUTH**. If PSK is selected, then the client will be authenticated if it specifies the correct group name and password. If PSK+XAUTH is selected, then an additional username and password is required.
DH Group	Diffie-Hellman (DH) group used to set the strength of the algorithm in bits. 2 [modp 1024] is the only available option.

Cisco VPN Server Settings

IKE Phase 2P	
PFS Group	Diffie-Hellman group options for PFS in phase 2. Choices are 1 [modp 768], 2 [modp 1024], 5 [modp 1536], 14 [modp 2048], or 15 [modp 3072].
SA Lifetime	Defines how long an IPsec SA (security association) will be used. The default is 30 minutes.
Mode Configuration	
IP Pool	**Starting IP Addres**s: Starting IP address of the range of addresses that are assigned to the remote client. This range must not be in the same subnet as any VLAN. **Subnet Mask**: Mask for the address range assigned to remote clients. The defined mask must be large enough to accommodate the maximum number of connections supported by your SRP.
DNS1	Primary DNS server to be used by remote clients.
DNS2	Secondary DNS server to be used by remote clients.
WINS1	Primary WINS server to be used by remote clients.
WINS2	Secondary WINS server to be used by remote clients
Banner	Message displayed to the remote user after they log on. The banner allows up to 500 printable ASCII characters on 1 line.

Configuring Users

The Users page contains a list of usernames that can be used to log in to the SRP VPN Server. Up to 25 unique users can be defined.

STEP 1 Click **VPN > Cisco VPN Server > Users**. The Users window opens.

From this page you can add, edit, or delete a user account.

STEP 2 To add a user, click **Add Entry**. The User Account page opens.

STEP 3 Enter a **Username** for the new user.

STEP 4 Specify a **Password** and reenter it in the **Confirm Password** field.

STEP 5 Click **Submit** to save your settings.

The user is added to the List of VPN Server Users table on the Users page.

STEP 6 Repeat steps 2 through 5 for each user who requires VPN access.

User Account Settings

Username	Username to be provided by the VPN client when using PSK+XAUTH as the authentication method.
Password	Password to be provided by the VPN client when using PSK+XAUTH as the authentication method.
Confirm Password	The contents of this field must match the Password field.

8

Administration Settings

This chapter describes the Administration settings for the Services Ready Platforms. It includes the following sections:

- **Web Access Management**
- **Remote Support**
- **Remote Management**
- **Time Setup**
- **User Management**
- **Certificate Management**
- **User Privilege Control**
- **Logging**
- **Factory Defaults**
- **Firmware Upgrade**
- **Backup & Restore**
- **Reboot**
- **Switch Settings**
- **Status**

To access these pages, click **Administration** from the Configuration Utility menu bar.

Web Access Management

Use the Web Access management page to configure the web access settings and remote access rules for the SRP.

STEP 1 Click **Administration > Web Access Management**. The Web Access Management window opens.

STEP 2 If desired, enter the **Banner Text**. This is the text that the user will see when they log into the SRP. You can enter a maximum of 1024 characters.

STEP 3 Configure the Remote Access settings as defined in the **Web Access Management Settings** table.

STEP 4 Click **Submit** to save your settings.

Web Access Management Settings	
Web Access	
Web Utility Access	Select **HTTP** and/or **HTTPS**. For secure Internet access, select **HTTPS**. If you select HTTPS, you must include https in the URL when you connect to the utility. For example https://xxx.xxx.xxx.xxx, where the x's represent the gateway's Internet IP address.
Web Utility Access via Wireless	Allows the web user interface to be accessed by devices associated with the SRP wireless access point. The default is Disabled.
Login Banner	
Banner Text	Text that the user sees when they access the SRP login page. You can enter a maximum of 1024 characters.
Remote Access	
Remote Management	Used to manage your SRP from a remote location through the Internet. The default is Disabled.

Web Access Management Settings	
Web Utility Access	Select **HTTP** or **HTTPS**. For secure Internet access, select **HTTPS**. For HTTPS, enter https://xxx.xxx.xxx.xxx (the x's represent the Gateway's Internet IP address) in your web browser's address field.
Remote Upgrade	If enabled, the firmware for the SRP can be upgraded from the Internet. **NOTE** You can only change this setting when connecting to the web interface from the LAN.
Allowed Remote IP Address	To access the SRP from any external IP address, select **Any IP Address**. To specify an external IP address or range of IP addresses, select the second radio button and enter the desired IP address(es).
Remote Management Port	Enter the remote access port number. The default port number is 8080.

Remote Support

Use the Remote Support page to assist Cisco support engineers in diagnosing product issues.

STEP 1 Click **Administration > Remote Support**. The Remote Support window opens.

STEP 2 Click the **Collect Device Status Information** button to generate a snapshot of the SRP's operational state in a file called debug_info.tgz. Provide this file directly to Cisco support for further analysis.

STEP 3 If your Cisco support engineer requests remote access to the SRP to diagnose an issue, check **Enable Remote Support**.

STEP 4 Enter an **Access Port** number for the remote access shell.

STEP 5 Enter a **Remote Support Password** that you agree on with your support engineer. You will also need to provide the support engineer with the MAC address of the device to enable access (see Status > Router).

STEP 6 Click **Submit** to activate the remote support session. This opens the SSH access on the specified port for approximately 30 minutes. Afterwards, remote access will be disabled.

Remote Support Settings	
Enable Remote Support	Check this box to turn on the remote debug shell. Once enabled, it is only valid for 30 minutes.
Access Port	The debug shell's port number, the default value is 22.
Remote Support Password	The remote support password.

Remote Management

Use the Remote Management pages to configure settings for the following:

- **TR-069**
- **SNMP**
- **Local TFTP**

To access these pages click **Administration > Remote Management** from the Configuration Utility.

TR-069

Some service providers can automatically provision your customer premises equipment from a central server. Use the TR-069 page to set up communication with an Auto-Configuration Server (ACS).

STEP 1 Click **Administration > Remote Management > TR-069**. The TR-069 window opens.

STEP 2 Select **Enabled** to allow auto-configuration of the SRP from a central server. The default is Disabled.

STEP 3 Specify the TR-069 settings as defined in the **TR-069 Settings** table.

STEP 4 Click **Submit** to save your settings.

TR-069 Settings	
Status	Select **Enabled** to allow auto-configuration of your router from a central server. The default is Disabled.
ACS URL	ACS URL provided by your service provider. The ACS URL uses the following format: **Protocol://host:port/path** ▪ Protocol can be either HTTP or HTTPS. ▪ Host can be a fully qualified domain name, or IP address. ▪ Port is optional. ▪ Path is dependant on ACS configuration.
ACS Username	Enter a **Username** the SRP to use if the ACS requests authentication. The default username is OUI-Serial Number.
ACS Password	Enter a **Password** for the SRP to use if the ACS requests authentication.
Connection Request Port	Enter the **Connection Request Port** number that the ACS will use to contact the SRP.
Connection Request Username	(Optional) Enter the authentication **Username** that the ACS must use when initiating a connection request.
Connection Request Password	(Optional) Enter the authentication **Password** that the ACS must use when initiating a connection request.
Periodic Inform Enable	Select **Enabled** to allow the router to periodically send inform messages to the ACS. Otherwise, select Disabled.
Periodic Inform Interval	Enter an **Interval** (in seconds) when the SRP will send an inform message to the ACS. The default value is 86400 seconds (24 hours).

TR-069 Settings	
Binding with Loopback Interface	By default, all TR-069 messages are bound to the default WAN IP address. Alternatively, one of the two SRP Loopback Interfaces can be used for TR-069 communications. The SRP will also define its Connection Request URL using the loopback address if selected.
Request Download	Click the **Apply** button to immediately initiate a connection to the ACS. The ACS calls the Download RPC when it receives the request.
Provisioning Code	Enter the code that will be used by the ACS to determine provider-specific custom and provisioning parameters.

SNMP

The SRP500 supports SNMP which allows you to monitor a variety of availability and performance metrics. SNMP versions 1, 2, and 3 are supported for read only access of supported MIBs. SNMP traps are also supported for selected management objects.

STEP 1 Click **Administration > Remote Management > SNMP**. The SNMP window opens.

STEP 2 To enable SNMP, click **Enabled**. The default is Disabled.

STEP 3 Enter the SNMP Settings as defined in the **SNMP Settings** table.

STEP 4 Click **Submit** to save your settings.

SNMP Settings	
SNMP Enable/ Disable	Select **Enabled** to enable SNMP. The default is Disabled.
Trusted IP	Enter the IP address and subnet mask of a management server or network that allows access to the SRP through SNMP, or choose **Any** to allow access from any IP address (not recommended).
Get Community	Enter a public password that allows read-only access to the SRP's SNMP information.
Set Community	Enter a private password that allows read access to the SRP's SNMP information.
SNMPv3	
SNMPv3 Enable/ Disable	Select **Enabled** to enable SNMPv3. The default is Disabled, which means that SNMPv2 will be used.
R/W User	Enter a username for SNMPv3.
Auth-Protocol	SNMPv3 authentication protocol. Choose either **HMAC-MD5** or **HMAC-SHA** from the drop-down list.
Auth-Password	The authentication password.
PrivProtocol	Privacy authentication protocol. Choose **None** or **CBC-DES** from the drop-down list. If you select CBC-DES, the Privacy Password is used to encrypt the data portion of the message that is being sent.
Privacy Password	The encryption key that the PrivProtocol uses.

SNMP Port Descriptions

The following tables list the internal Linux interface labels used by SNMP when listing interfaces.

SRP500 IP Interfaces	
br0	WAN Ethernet 1
br*n*	LAN VLAN *n*, where *n* = 1–4079
br4080 through br4083	ADSL PVC1–4
br4088	WAN Ethernet 2
lo	Loopback interface. Hosts management addresses configured in the Configuration Utility and the internal loopback (127.0.0.1).
ppp10	3G Modem PPP Interface
gre0 through gre9	GRE Tunnel Interface 1–10
ipsec0 through ipsec4	IPSec Tunnel Interface 1–5
ath0 through ath3	Wireless SSID1–4

SRP500 Internal Interfaces	
eth0	WAN Ethernet Interface
eth1	Internal connection to LAN switch
eth1.*n*	Internal subinterface connection to LAN VLANs. (Where *n* is the VLAN number 1 - 4079)
eth0.4080 through eth0.4083	Internal bridged connections to ADSL PVC1–4
eth0.4093	Internal connection to ADSL modem
wifi0	Internal connection to wireless access point
ifb0	Not currently used
ifb1	Not currently used
mast0	Not currently used

Supported MIBs

The following table lists the supported MIBs for the SRP500.

SRP500 Supported MIBs		
ADSL-LINE-MIB	CISCO-CLASS-BASED-QOS-MIB	CISCO-CONFIG-COPY-MIB
CISCO-FLASH-MIB	CISCO-MEMORY-POOL-MIB	CISCO-IETF-DHCP-SERVER-MI
CISCO-IETF-NAT-MIB	CISCO-IPSEC-MIB	CISCO-PROCESS-MIB
CISCO-SMI	CISCO-WAN-3G-MIB	DISMAN-EVENT-MIB
ENTITY-MIB	HOST-RESOURCES-MIB	IF-MIB
IP-MIB	IEEE80211-MIB	NET-SNMP-AGENT-MIB
NET-SNMP-MIB	NOTIFICATION-LOG-MIB	RFC1158-MIB
RFC1213-MIB	SNMP-FRAMEWORK-MIB	SNMP-MPD-MIB
SNMP-TARGET-MIB	SNMP-USER-BASED-SM-MIB	SNMP-VIEW-BASED-ACM-MIB
SNMPv2-MIB	TCP-MIB	UCD-DLMOD-MIB.mib
UCD-SNMP-MIB.mib	UDP-MIB	

Local TFTP

Use the Local TFTP page to enable the SRP to be a TFTP server. When you enable TFTP, you can upload files to the SRP remotely and then use it as a local server to serve small files to hosts on the LAN, such as bootstrap configuration files for IP phones. The SRP local storage space for TFTP is 1MB.

STEP 1 Click **Administration > Remote Management > Local TFTP**. The Local TFTP Control window opens.

STEP 2 TFTP is enabled by default. To disable it, select **Disabled** and then click **Submit**.

STEP 3 Specify the Get Remote File Settings as defined in the **Local TFTP Settings** table to upload your files.

Local TFTP Settings	
TFTP	TFTP is enabled by default. To disable it, select **Disabled**.
Get Remote File Settings	
URL	Enter the URL where the remote file resides. For example: http://www.yoursite.com:port/path/filename or ftp://username:password@yoursite:port/path/filename.
Save As	Enter the filename for the file you are saving.
Session Timeout	Maximum time allowed for a connection session. Enter the **Session Timeout** value (in seconds). The default is 10 seconds. ▪ The timeout for HTTP and FTP sessions is 3 seconds. ▪ The timeout for TFTP sessions is 1 second. **NOTE** For HTTP and FTP, a TCP reset response message will terminate a session.
Retry Sessions	Number of sessions that will retry if a transient problem occurs in a session.
Get File	Click this button to upload the desired file to the File List.
Status	Status of the processing remote file.
File List table	Shows the name and size of the remote file.

Time Setup

Use the Time Setup page to set the time zone parameters for your network. You can configure the time automatically by using the Network Time Protocol (NTP) server or configure it manually.

STEP 1 Click **Administration > Time Setup**. The Time Setup window opens.

STEP 2 Choose your region's time zone from the Time Zone drop-down list. Time zone is often referred to as the local time.

STEP 3 To set up the system clock manually, under Manual Setting choose the **Date** and **Time**.

STEP 4 To set the time using the Network Time Protocol (NTP) server, select **NTP**. Specify the NTP settings, as defined in the **Time Setup Settings** table.

STEP 5 To recover the system time after a system reboot, check the **Auto Recovery After Reboot** box. The default (unchecked) is disabled.

STEP 6 Click **Submit** to save your settings.

Time Setup Settings	
Time Zone	
Enter your region's time zone from the drop-down list. For example: (GMT-8:00) Pacific Time (USA & Canada).	
Manual Setting	
Use to set the system clock manually. Enter the date as "Year/Month/Day" and the time as "Hour:Min:Sec."	
NTP	
Time Server Address	Sets the time by using a Network Time Protocol (NTP) server. ▪ To automatically set the time using the SRP's default NTP servers, choose **Auto.** This is the default setting. ▪ To specify a particular NTP server, select **Manual** and enter the hostname or IP address of the NTP server.
Resync Timer	Enter how often the SRP will resync with the NTP server. The default setting is 3600 seconds.

Time Setup Settings	
Enable Daylight Saving	Daylight savings time is enabled by default. To disable it, uncheck the box. When enabled, one of these options can be selected: ▪ Automatically: Automatically set daylight savings time. ▪ Manually: Manually set daylight savings time. - Start/End Month: The start/end month value in the range 1-12 (January-December) - Start/End Date: The start/end day value in the range 1-31. If the value is -1, the time will change on the weekday on or before the end of the month; the last occurrence of a weekday in that month. - Start/End Weekday: The start/end weekday value in the range of -7 to 7 (Monday to Sunday). If the weekday value is 0, the date to start of end daylight savings is exactly the month and day. If the weekday value is -7 to 7, daylight savings starts or ends on the weekday value on or after the month and day. If the value is not negative or 0, then daylight saving starts or ends on the weekday value on or before the month and day. - Start/End Hour: The start/end hour of daylight saving time. - Start/End Minute: The start/end minute of daylight saving time. - Adjust time: The number of hours, minutes, and/or seconds to add to the current time during DST.
Auto Recovery After Reboot	
Check this box to recover the system time after a system reboot. The default (unchecked) is disabled. This feature attempts to start the system clock as close to the current time as possible after reboot.	

User Management

The section describes how to configure the User Management settings to authenticate and control all users that log in to the SRP. It includes the following sections:

- **Password Complexity Settings**
- **User List**

Password Complexity Settings

Use the Password Complexity Settings page to enforce password complexity requirements when one is created or changed. Using a strong password is the first line of defense against unauthorized access to your network.

STEP 1 Click **Administration > User Management > Password Complexity Settings**. The Password Complexity Settings window opens.

STEP 2 This feature is disabled by default. To enable it, click **Enabled**.

STEP 3 Enter a password with a strong password strength.

The password must contain a minimum of eight characters and at least three of these character classes:

- A through Z (uppercase)
- a though z (lowercase)
- 0 through 9 (alphanumeric)
- special characters (for example, ! $ # %)

STEP 4 Click **Submit** to save your settings.

User List

Use the User List page to manage the users who have access to the Configuration Utility.

NOTE The SRP supports two user accounts, one for administrator use and the other for a restricted user. By default these accounts are named "admin" and "cisco," respectively.

STEP 1 Click **Administration > User Management > User List**. The *User List* window opens.

STEP 2 Click the **Edit** (pencil) icon for the account that you want to change. The User Account window opens.

STEP 3 Specify the user settings as defined in the **User List Settings** table.

STEP 4 Click **Submit** to save your settings.

User List Settings	
Username	Enter a new username.
Old Password (Admin account only)	Enter your old password. You will be asked for this when changing your password.

User List Settings	
New Password/Confirm New Password	Enter and confirm a new password. The maximum number of characters is 32. The default administrator password is **admin**. The default guest password is **cisco**. You will be asked for your password when you log into the Configuration Utility. For security purposes, we strongly recommend changing it. **NOTE** If the password complexity feature is enabled, you will be required to enter a strong password consisting of a minimum of eight characters and at least three of these character classes: ▪ A through Z (uppercase) ▪ a though z (lowercase) ▪ 0 through 9 (alphanumeric) ▪ special characters (for example, ! $ # %).
Level	Shows the level of permissions for this user. The Admin account has access to all settings, while the User account has access only to those features defined by the User Privilege page.

Certificate Management

When TR-069 and XML provisioning is secured using HTTPS, use the Certificate Management page to install the public certificates required to authenticate the provisioning servers.

Digital certificates (also known as PKI X.509 certificates), are used to authenticate the identity of users and systems, and are issued by Certification Authorities (CAs) such as VeriSign or Thawte. Each certificate file can include multiple certificates, provided that the total file size remains less that 8 KB.

STEP 1 Click **Administration > Certificate Management.** The Certificate Management window opens.

This page lists the certificate files currently installed for use with TR-069 and XML provisioning servers. From this page you can add, delete, or enable a certificate file.

- To add a certificate file, enter a descriptive name in the CA Name box, then click **Choose File** or **Browse** to select the certificate file (.pem). Click the **Upload** button to install the certificate file. You can upload up to 3 certificate files for use with a TR-069 ACS, however, only one can be active at a time.
- To delete a currently installed certificate file, click the **Delete** (x) icon next to the certificate you want to remove.
- To activate an existing certificate file, check the **Enable** box next to the applicable certificate.

STEP 2 Click **Submit** to save your settings.

Certificate Management Settings	
TR-069 Root CA File List	Lists the certificate file available to authenticate to a TR-069 ACS.
Provision File List	Shows the certificate available for authenticating an XML provisioning server.
Enabled	Check the **Enable** box to activate a certificate. Uncheck the box to disable it.
CA Name	Enter a descriptive name for the certificate.
Select Certificate	Uploads a certificate from the client's PC. To upload it, click **Choose File** or **Browse**, find and select the certificate file (.pem), and then click the **Upload** button. To remove an installed certificate, click the **Delete** (x) icon next to the certificate you want to remove.

User Privilege Control

Use the Privilege Control page to specify privileges for the User account.

STEP 1 Click **Administration > User Privilege Control**. The User Privilege Control window opens.

STEP 2 Choose one of these access types for each feature:

- **Read/Write**: Allows the User account to view and configure the web page.
- **Read Only**: Allows the User account to only view the web page.
- **Hidden**: Hides the page from the User account.

STEP 3 Click **Apply** to save your settings.

Logging

This section describes the logging options for the SRP. It includes the following sections:

- **Log Setting**
- **Log Module**
- **Log Viewer**
- **Firewall Log**

To access these pages, click **Administration > Log** from the Configuration Utility menu bar.

Log Setting

STEP 1 Click **Administration > Log > Log Setting**. The Log window opens.

STEP 2 Enter the log size that will be saved in the memory of the SRP. The allowed range is 128–1024 KB.

NOTE If you reboot the SRP, these log messages will not be saved.

STEP 3 To save system messages to a USB memory card that is connected to the SRP, enter the filename to be saved to the USB device. The allowed range is 1–512 MB. If a USB is not connected, "USB disconnect" is displayed.

STEP 4 Enter the **IP Address** and **Port** number of the of the remote syslog server. Port 514 is the default port. The range is 1–65535.

STEP 5 Specify the email log parameters for logs to be sent a specific email address as defined in the **Log Settings** table.

STEP 6 Click **Submit** to save your settings.

Log Settings	
Local	Log size that will be saved in the memory of the SRP. The allowed range is 128–1024 KB.
USB	To save list messages to a USB memory card that is connected to the SRP, enter the filename. The allowed log range is 1–512 MB. If a USB is not connected, the message "USB disconnect" is displayed.
Syslog Server	IP address and port number of the of the remote syslog server. Port 514 is the default port. The range is 1–65535.
Email	
Sender and Receiver	Enter the **Sender** and **Receiver** email address.
SMTP Server	Enter the **SMTP Mail Server** address.
SMTP Port	Enter the **SMTP Port** address that the mail server listens on. Port 25 is the default.
Subject	Specify an email **Subject** for the logs.
Number of Logs	Enter the **Number of Logs** to be collected in the email. The range is 10–200 logs.

Log Settings	
Interval	Enter the amount of time that forces email to be sent if the amount of logs does not reach the number of logs that you specified. The range is 1–1440 minutes.
User Name and Password	Enter the **User Name** and **Password** for mail server authentication.

Log Module

Use the Log Module settings to select the level of logging detail that be collected and where it must be sent.

STEP 1 Click **Administration > Log > Log Module**. The Log Module window opens.

STEP 2 To collect the activity logs, select **Enabled**. The default is Disabled. With logging enabled, you can choose to collect system and/or kernel messages.

STEP 3 To enable logging for a particular service, check the **Enable** box.

STEP 4 Choose a **Priority level** from the drop-down list. These are described in the Logging Severity Settings table on page 107. Initially no logs are displayed until one of these options is selected.

STEP 5 Click **Submit** to save your changes.

Log Module Settings

Log Level	
Status	To collect the activity logs, select **Enabled**. The default is Disabled.
Log	▪ **Local**: Saves the log to system memory. ▪ **USB**: Saves the log to a USB device. ▪ **Email**: Sends the log through email. ▪ **Syslog Server**: Sends the log to a specific log server. To set up the server address, see Log Setting, page 253.

Log Viewer

STEP 1 Click **Administration > Log > Log Viewer**. The Log Viewer window opens.

STEP 2 Click the **Download All Log** button to download logging messages to a file on a local PC.

STEP 3 Click the **Clear Log** button to clear all log messages saved in memory.

STEP 4 Choose the type of logs you want to view on the web page from the Display drop-down list. You can select from **All** logs, **kernel** logs, or **system** logs. Initially, no logs are displayed until one of these options is selected.

STEP 5 To filter log messages with a specific pattern, enter a suitable string in the Filter field and then click the **Filter** button to view all messages containing that pattern.

For example, enter [TR-069] to show all TR-069 messages in the log list. In this case, you must configure the log to capture these messages on the Log Module window and also configure the Log Viewer to **All** to show all messages. See **Log Module, page 256**.

Firewall Log

Use the firewall log page to select firewall event logging preferences.

NOTE A firewall DoS attack log message will be generated if ICMP Echo Request or TCP sync packets are detected at a rate of 100 packets per second or more at the WAN interface. To generate the log, the firewall has to be configured to filter DoS attacks and the firewall filter has to be enabled for DoS.

STEP 1 Click **Administration > Log > Firewall Log**. The Firewall Log window opens.

STEP 2 Click **Enabled** to enable firewall logging. The default is Disabled.

STEP 3 Choose a severity level from the Log Level drop-down list as defined in **Logging Severity Settings** table. All events of this level and higher will be logged.

STEP 4 Select the firewall module that you want to log (**SPI** or **DoS** attack), and enter the number of events to be generated per log.

STEP 5 Click **Submit** to save your changes.

Logging Severity Settings

Log Level	
Emergency (level 0)	System unusable. Syslog definition is LOG_EMERG.
Alert (level 1)	Immediate action needed. Syslog definition is LOG_ALERT.

Logging Severity Settings

Critical (level 2)	Syslog definition is LOG_CRIT.
Error (level 3)	Error conditions. Syslog definition is LOG_ERR.
Warning (level 4)	Warning conditions. Syslog definition is LOG_WARNING.
Notification (level 5)	Normal but significant condition. Syslog definition is LOG_NOTICE.
Information (level 6)	Informational messages only. Syslog definition is LOG_INFO.
Debugging (level 7	Debugging messages. Syslog definition is LOG_DEBUG.
Log Category	
SPI and DoS Attack	Select the firewall module that you want to log (Stateful Packet Inspection (SPI), DoS attack, or both) and enter how many events to be generated per log.

Factory Defaults

Use the Factory Default page to set the SRP to the settings it was configured with when it was shipped from the factory.

NOTE If the Service Provider used the SP Defaults feature, then the configuration will be reset to those values rather than the Cisco factory default.

STEP 1 Click **Administration > Factory Defaults**. The Factory Defaults window opens.

STEP 2 To restore the SRP or voice settings to its factory defaults, select **Yes**.

CAUTION Back up any custom data (SRP) or voice settings that you saved. These settings will be lost when the default settings are restored.

STEP 3 Click **Submit** to apply the reset.

Firmware Upgrade

Use the Firmware Upgrade page to upgrade the firmware on the SRP.

NOTE It is not necessary to upgrade unless you are experiencing problems with the device or if the new firmware has a feature that you want to use. Before upgrading, we recommend that you back up your data first. For more information, see **Backup Configuration, page 260**.

To download the firmware upgrade file go to: www.cisco.com/go/srp500. Click the Download Software link to download the latest software.

STEP 1 Click **Administration > Firmware Upgrade**. The Firmware Upgrade window opens.

STEP 2 Click **Choose File** or **Browse**, and select the location of the firmware upgrade file that you downloaded.

STEP 3 Click the **Upgrade** button.

CAUTION Upgrading the firmware may take several minutes. Until the process is complete, DO NOT turn off the power, press the hardware reset button, or click the Back button in your current browser.

Backup & Restore

This section describes how to backup and restore the configuration settings for the SRP. It includes the following sections:

- **Default Configuration**
- **Backup Configuration**
- **Restore Configuration**
- **XML Configuration**

To access these pages, click **Administration > Backup & Restore** from the Configuration Utility.

Default Configuration

Use the Default Configuration page to specify the SRP default configuration settings.

NOTE The Service Provider defaults are a specific set of configuration parameters applied to the SRP during initial deployment to define the behavior of the device following reset by the user account. This setting defines whether the Service Provider defaults are used or not (allowing the administrator to restore to Cisco factory defaults).

STEP 1 Click **Administration > Backup & Restore > Default Configuration.** The Default Configuration window opens.

STEP 2 Select **Yes** to load the Service Provider's default configuration. Select **No** to restore the Cisco factory default settings to the SRP.

STEP 3 Click **Submit** to save your changes.

Backup Configuration

Use the Backup Configuration page to back up the SRP configuration settings to a file. You can later restore these same settings to the SRP.

STEP 1 Click **Administration > Backup & Restore > Backup Configuration**. The Backup Configuration window opens.

STEP 2 Click the **Backup** button to save the configuration information of the SRP.

Restore Configuration

User the Restore Configuration page to restore the SRP configuration settings from a previous backup.

STEP 1 Click **Administration > Backup & Restore > Restore Configuration**. The Restore Configuration window opens.

STEP 2 Click **Choose File** or **Browse,** locate the backup file, and then click **Restore**.

XML Configuration

For security purposes, when backing up or restoring the system configuration through XML, it is important that all passwords are protected. Use the XML Configuration page to enable encryption to protect the password in the XML profile.

STEP 1 Click **Administration > Backup & Restore > XML Configuration**. The XML Configuration window opens.

STEP 2 Password encryption is enabled by default. To disable it, uncheck **Encrypt Password Text**.

STEP 3 Enter the **Encryption Key**. This key is used to encrypt all password text in XML. It can contain up to 32 characters and at least three of these character classes:

- A through Z (uppercase)
- a though z (lowercase)
- 0 through 9 (alphanumeric)
- special characters (for example, ! $ # %) .

NOTE If this field is left blank, the device console password is used. To obtain the console password, please contact your service provider.

STEP 4 Click **Submit** to save your changes.

Reboot

Use the Reboot page to restart the SRP (if necessary) from the Configuration Utility.

STEP 1 Click **Administration > Reboot**. The Reboot window opens.

STEP 2 Click the **Reboot** button to power cycle the SRP.

Switch Settings

This section describes how to configure the switch settings for the SRP. It includes the following sections:

- **Jumbo Setting**
- **Port Status**
- **DSL Switch Setting**
- **MAC Filtering (SRP540 Models Only)**

To access these pages, click **Administration > Switch Setting** from the Configuration Utility.

Jumbo Setting

Use the Jumbo Setting page to set an interface to Jumbo Mode. Jumbo frames are Ethernet frames with more than 1500 bytes of payload.

STEP 1 Click **Administration > Switch Setting > Jumbo Setting**. The Jumbo Setting window opens. This page lists the interfaces (wired physical Ethernet ports) that support jumbo mode.

STEP 2 To change the size of the packet, choose a mode from the Jumbo Mode drop-down list. The default packet size is 2048 bytes. Alternatively, you can choose from 1552, 2048, or 10240 bytes.

NOTE The SRP520-U models only support 1552 and 2048 bytes.

STEP 3 Click **Submit** to save your settings.

Port Status

Use the Port Status page to enable or disable an Ethernet interface.

STEP 1 Click **Administration > Switch Setting > Port Status**. The Port Status window opens.

STEP 2 To enable an interface, click **Enabled**. This option is not available for Wireless or ADSL interfaces.

STEP 3 Click **Submit** to save your settings.

DSL Switch Setting

Use the DSL Switch Setting page to manage use of the DSL interface.

STEP 1 Click **Administration > Switch Setting > DSL Switch Setting**. The DSL Switch Setting window opens.

STEP 2 To disable the ADSL interface and convert LAN port 4 to WAN mode, click **Disabled**.

STEP 3 Click **Submit** to save your settings.

MAC Filtering (SRP540 Models Only)

You can control access to your network by specifying the MAC addresses of the devices that are permitted access or are blocked. Up to 16 filter rules may be configured per port.

NOTE Only wired Ethernet interfaces support MAC filtering. See wireless MAC filter for controlling access through WiFi.

STEP 1 Click **Administration > Switch Setting > MAC Filter**. The MAC Filter (Allowed list) window opens.

From this page you can enable MAC filtering to permit network access to the SRP and view all MAC addresses assigned to LAN ports 1-4. You can also enable a MAC address (if disabled), and add a new MAC address entry that will allow traffic to pass.

STEP 2 To add a MAC address, choose the LAN Port from the drop-down list, enter the corresponding MAC address, and click the **Add** button.

STEP 3 Select **Enabled** to turn on MAC filtering for LAN ports 1–4.

STEP 4 Click **Submit** to save your changes.

Status

Use the Status page to view the CPU and memory status for the SRP. The status information is displayed in real time.

To access this page, click **Administration > Status.**

From this page you can view the following:

- **CPU**–MIBS, Loads, and Uptime.
- **Memory**–Memory's Total size (KB), Free size (%), Used size (%), Buffer size (%), Cached size (%), Active size (%), and Inactive size(%).

9

Using Services Ready Platforms Diagnostics

This chapter describes how to use diagnostic features for the Services Ready Platforms. It includes the following sections:

- **Ping Test**
- **Traceroute Test**
- **Detect Active LAN Clients**
- **TCP Dump**
- **ATM OAM Ping**

To access these pages, click **Diagnostics** from the Configuration Utility menu bar.

Ping Test

Use the Ping Test page to test connectivity between the SRP and a connected device on the network.

IPv4

STEP 1 Click **Diagnostics > Ping Test > IPv4**. The Ping Test window opens.

STEP 2 Enter the IPv4 address or fully qualified domain name that you want to ping.

STEP 3 Enter a packet size in bytes. The range is 32 to 65500 bytes.

STEP 4 Choose the number of times to ping from the drop-down list (**5**, **10**, or **Unlimited**).

STEP 5 Click the **Start to Ping** button to start the test. After the test is complete, the test results appear on the page.

STEP 6 To return to the previous window, click **Close**.

Traceroute Test

Use the IPv4 Traceroute pages to view the route between the SRP and a destination.

IPv4

STEP 1 Click **Diagnostics > Traceroute Test > IPv4**. The Traceroute Test window opens.

STEP 2 Enter the IPv4 address or fully qualified domain name to run the trace route to.

STEP 3 Click the **Start to Traceroute** button to start the test. The results appear on the page and are refreshed every 5 seconds.

STEP 4 To return to the previous window, click **Close**.

Detect Active LAN Clients

Use the Detect Active LAN Client(s) page to discover which client devices are active on the SRP networks.

STEP 1 Click **Diagnostics > Detect Active LAN Client(s)**. The Detect Active LAN Client(s) window opens.

STEP 2 Choose the LAN interface that you want to detect from the drop-down list. For example: VLAN1.

STEP 3 Choose how long that you want to perform this search (**5**, **10**, or **15** seconds).

STEP 4 Click the **Start to Search** button to start the test. A new window opens and displays the test results.

STEP 5 To run the scan again, click the **Retry** button. To return to the previous window, click **Close**.

TCP Dump

Use the TCP Dump page to capture packets on an interface by using the tcpdump command.

TCP Dump can be used to capture some or all packets received by a network interface. Captured packets are stored in a pcap file on an attached USB memory device. From here, the file can be downloaded through the SRP interface, or taken using the memory device, for analysis using an application such as Wireshark.

NOTE You can execute the tcpdump command with the “no option” to capture the packet flow through all interfaces. Specify the -i option to filter on a particular Ethernet interface. For example: # tcpdump -i eth1.

STEP 1 Plug the USB device into the specified USB port on the SRP. For USB port locations, see **Product Overview, page 13**.

STEP 2 Click **Diagnostics > TCP Dump**. The TCP dump window opens.

STEP 3 Select an external USB storage from the drop-down list. This is where the raw packet file will be saved. Choose either **USB Stick 1** or **USB Stick 2**. These correspond to the USB devices connected to the USB ports on the SRP.

STEP 4 Choose an interface to use for capturing the packets from the drop-down list.

STEP 5 Adjust the -w filename if required. For example: tcpdump.pcap.

STEP 6 Enter the **Run Time** (in seconds) to run tcpdump. The range is 0-86400 seconds. The default is 60 seconds. Enter 0 to run the trace indefinitely. If you use this option, you must stop the trace manually when required.

STEP 7 If required, adjust the **Advanced Command String** input to tune tcpdump using standard command options. For example: -i br0 -w /home/usb_storage_1/tcpdump.pcap.

> **NOTE** By default, the SRP only captures the first 60 bytes of each packet. If more detail is required, this limitation may be lifted by adding "-s 0". The performance of the SRP may be degraded if the traffic capture rate is very high. For more information on TCP Dump options, see: http://www.tcpdump.org/tcpdump_man.html.

STEP 8 Click the **Start** button to run the TCP Dump daemon. Click the **Stop** button to end it. To save the file, click the **Download dump file to PC** button.

ATM OAM Ping

Use the ATM Ping page to send an Operation, Administration, and Maintenance (OAM) packet to confirm the connectivity of a specific Permanent Virtual Circuit (PVC), and to facilitate ATM network troubleshooting

STEP 1 Click **Diagnostics > ATM OAM Ping**. The ATM OAM window opens.

STEP 2 Choose the WAN interface you want to ping from the drop-down list. For example: PVC0.

STEP 3 Choose the OAM Type (**F4 End Loopback**, **F4 Segment Loopback**, **F5 End Loopback**, and **F5 Segment Loopback**) from the drop-down list.

STEP 4 Click the **Start to Ping** button to start the test. A new window opens and displays the test results.

STEP 5 To return to the previous window, click **Close**.

10

Viewing the Services Ready Platforms Status

This chapter describes how to view the status of Services Ready Platforms from the Configuration Utility. It includes the following sections:

- **Router Status**
- **Firewall Status**
- **Interface Information**
- **Port Statistics**
- **Wireless Network Status**
- **Wireless Client Information**
- **Guest Network Information**
- **Mobile Network Status**
- **DHCP Server Information**
- **QoS Status**
- **Routing Table**
- **ARP**
- **RIP Status**
- **IGMP Status**
- **VPN Status**
- **VPN Server Status**
- **CDP Neighbor Information**
- **Status ADSL**
- **STP Status**

To access these pages, click **Status** from the Configuration Utility menu bar.

Router Status

Use the **Status > Router** page to view information about the SRP and its firmware status.

Router Status

Model	Product name and features.
Version ID	Product version ID.
Hardware Version	Hardware version number.
Boot Version	Boot firmware version number.
Firmware Version	Current firmware version.
ADSL Firmware Version	Current ADSL firmware version.
Recovery Firmware	Version number of the recovery firmware.
Setup Wizard Version	Version number of the Setup Wizard.
WAN MAC Address	MAC address of the WAN interface.
Current Time	Time that the page was loaded; the page does not update.
Wireless	Number of Wireless SSIDs that are enabled.

Firewall Status

Use the **Status > Firewall** page to view the SRP firewall information.

Firewall Status

Internet Access Policy	
No	The index number of the Internet Access Policy list.
Policy Name	The name of the Internet Access Policy.

Firewall Status

Status	Status of the Internet Access Policy. Click on the link to access the policy configuration.
Passed (pkts)	Number of packets passed by this rule.
Passed (bytes)	Traffic volume passed by this rule, in bytes.
Blocked (pkts)	Number of packets blocked by this rule.
Blocked (bytes)	Traffic volume blocked by this rule, in bytes.
Port Forwarding	Status of the currently active port forwarding rules. Rules that are not enabled, or that are associated with disconnected WAN interfaces are not shown.
Type	Indicates single port or port range forwarding.
Protocol	Port being forwarded.
Port	Port being forwarded.
Host	LAN host IP address to forward to.
Packets	Number of packets forwarded.
Traffic (bytes)	Traffic volume forwarded, in bytes.
Statistics	General traffic measurements through the firewall.
Name	IP Table name associated with firewall packet processing. **INPUT**: Traffic destined for the SRP. **OUTPUT**: Traffic originating from the SRP. **FORWARD**: Traffic passed between the public/external and private/internal networks.
Accept PKT	Number of packets accepted by this firewall path.
Accept Volume (bytes)	Volume of traffic, in bytes, processed by this firewall path.
Drop PKT	Number of packets filtered/blocked by this firewall path.
Drop Volume (bytes)	Volume of traffic, in bytes, filtered/blocked by this firewall path.

Interface Information

Use the **Status > Interface** Information page to view information for the various interfaces.

NOTE To view additional status information, click an item in the WAN List. The detail of Interface table displays the WAN information for the selected interface.

Interface Information

Interface List	
Interface	Shows all currently configured LAN and WAN layer three (IP) interfaces. An Ethernet WAN interface is shown as Ether_WAN and an ADSL WAN interface is shown as ADSL_PVC. Interface numbering is derived as follows: ▪ **Primary Interfaces**: Numbering follows physical port labelling (that is, WAN1 and WAN2). ▪ **Ethernet WAN Sub-interfaces**: Numbering reflects configured VLAN index. ▪ **ADSL PVCs**: Numbered serially from 0 to 3. ▪ **VLAN Interfaces**: Numbering reflects the configured VLAN index.
Connect Type	Protocol in use by the interface.
IP Address	IP address of the interface.
Subnet Mask	Subnet mask of the interface.
MAC Address	MAC address of the interface.
Disconnect button	Click this button to disconnect the interface, if the interface is a VPN tunnel.
Port List	
Interface	Lists all currently configured LAN and WAN physical (Ethernet, WiFi SSID, DSL PVC) interfaces.
TX (pkts)	Number of packets transmitted from this port.

Interface Information

RX (pkts)	Number of packets received by this port.
Status	Port connectivity status.
Clear TX & RX button	Resets to 0 the count of TX and RX packets.

Port Statistics

Use the **Status > Port Statistics** page to view statistics for physical port activity.

Port Statistics

Port LIst	
Port	Displays the current MIB counters for a single physical port, Ether_WAN1, 4 LAN ports (LAN Port 1, LAN Port 2, LAN Port 3, LAN Port 4), and Ether_WAN2.
Columns	▪ **Port**: Physical port. ▪ **Input Bytes**: Number of bytes received by the port. ▪ **Output Bytes**: Number of bytes transmitted by the port. ▪ **Input Errors**: Number of receive errors seen for incoming traffic. ▪ **Input Broadcasts**: Number of Ethernet broadcast messages received by the interface. ▪ **Output Broadcasts**: Number of Ethernet broadcast messages sent by the interface. ▪ **Input Multicasts**: Number of Ethernet Multicast messages received by the interface. ▪ **Output Multicasts**: Number of Ethernet multicast messages sent by the interface.

Wireless Network Status

Use the **Status > Wireless Network** page to view status information about your wireless networks.

Wireless Network Status

Network Mode	Operating mode configured for the embedded wireless access point. See **Setting Up the Wireless LAN, page 64** for more information.
Radio Band	Channel bandwidth in use by the wireless network.
Channel	Wireless channel currently in use.
Wireless List	Current SSID configuration. Columns in the Wireless List include: ▪ **SSID Name:** Configured SSID name. ▪ **Status**: SSID enabled or disabled. ▪ **Broadcast**: SSID broadcast enabled or disabled. ▪ **Security**: Current security settings. ▪ **WPS:** Indicates whether WPS is enabled for this SSID.

Wireless Client Information

Use the **Status > Wireless Client** information page to view information for the wireless clients connected by an SSID.

.

Wireless Client Information

MAC Address	Client MAC address.
Tx-Rate	Current transmission data rate of the client.
Rx-Rate	Current receive data rate of the client.

Wireless Client Information

RSSI	Signal strength of the last received packet.
IDLE	Current setting of the station inactivity timer. This is the time in milliseconds when the station goes into power save if no activity occurs on the link.

Guest Network Information

Use the **Status > Guest Network** page to view information for a guest network client.

Guest Network User List Status

Account	User's authenticated name.
IP Address	User's assigned network DHCP IP address.
MAC	User's network card MAC address
Remain Lease Time	Remaining time available before the user session ends.
Disconnect	Click this button to terminate the session.

Mobile Network Status

Use the **Status > Mobile Network Status** page to view information for the Broadband USB modem that is installed in the SRP.

NOTE This page will differ depending on the type of USB modem that you installed.

Mobile Network Modem Status

Connection	Displays the modem status; Connected or Unable to Detect USB Mobile Modem (shows if no modem is installed).
Internet IP Address	IP address assigned to the USB modem.

Mobile Network Modem Status

Subnet Mask	Subnet mask of the mobile network.
Default Gateway	Gateway IP address assigned by the ISP.
DNS	DNS server IP address assigned by the ISP
Connection Up Time	Duration of the current connection session.
Current Session Usage	Receive and Transmit traffic volume.
Data Card Status	
Manufacturer	Manufacturer of the connected USB modem.
Card Model	Model name of the connected USB modem.
Card Firmware	Firmware revision currently installed on the USB modem.
SIM Status	SIM card status. (SIM ready or pin code needed).
IMSI	International Mobile Subscriber Identity (IMSI) number of this USB modem. This is a unique number stored in the Subscriber Identity Module (SIM) associated with all GSM and Universal Mobile Telecommunications System (UMTS) network mobile phone users.
Carrier	Network service provider used for the Internet connection.
Service Type	USB modem service type.
Signal Strength	Signal strength of the current UMTS/GPRS/EVDO service.
Card Status	Status of the card: Connecting, Connected, Disconnecting, Disconnected or Card is not activated. If no card is attached, the status page says that the SRP is “Unable to Detect USB Mobile Modem.”

USB CDMA2000 EVDO Card Settings

Connection	Displays the modem status. Connected or Unable to Detect USB Mobile Modem (shows if no modem is installed).
IP Address	IP address assigned to the USB modem.
Connection Up Time	Duration of the current connection session.
Current Session Usage	Receive and Transmit traffic volume.
Manufacturer	Manufacturer of the connected USB modem.
Card Model	Model name of the connected USB modem.
Card Firmware	Firmware revision currently installed on the USB modem.
ESN	ESN number of this USB modem.
PRL Version	PRL Version of this USB modem.
Phone Number	Phone number associated with the account of this USB modem.
Carrier	Carrier name associated to the USB modem service.
Signal Strength	Signal strength.
Card Status	Status of the card: Connecting, Connected, Disconnecting, Disconnected or Card is not activated. If no card is attached, the status page says that the SRP is “Unable to Detect USB Mobile Modem.”

DHCP Server Information

Use the **Status > DHCP Server Information** page to view DHCP Server lease information by rule.

DHCP Pool Information

Client Name	Host name of the DHCP client.
IP Address	IP address leased to the client.
MAC Address	MAC address of the DHCP client.
Expires Time	Expiration time of the current DHCP lease.
Interface	Interface through which the client is connected.

QoS Status

Use the **Status > QoS** page to view traffic queuing statistics. The SRP supports 5 queues: One strict queue and four weighted round robin queues.

NOTE To view this page, you must enable one of the interfaces from the **Network Setup > QoS > QoS Bandwidth Control** page. See **QoS Bandwidth Control, page 93**.

QoS Status

Queue Name	Lists the five queues used by the SRP (Strict High, High, Medium, Normal, and Low).
Config Rate	Nominal amount of traffic that each queue can handle under balanced and loaded conditions. Bandwidth not used by a queue may be used by any other, implying that the configured queuing bandwidth may be exceeded.

QoS Status

Allow Maximum Rate	Maximum permitted traffic rate in kbps for each queue. Weighted Round Robin queues are allowed to use all of the shaped bandwidth, whereas Priority Queue traffic is limited to 70% of the total to ensure reliable handling of real time media.
Send (bytes)	Number of bytes sent from this queue.
Send (pkts)	Number of packets sent from this queue.
Drop	Number of packets dropped when total traffic rate exceeds Allow Maximum rate.
Overlimits	Number of packets that have been dropped when traffic rate is higher than the Allow Maximum rate.
Requeues	If a packet cannot be sent, it is put back into the original queue allowing another attempt. This event increases the Requeue counter.
Current Rate (bps)	Current throughput rate for this queue in bits per second.

Routing Table

Use the **Status > Routing Table** page to view routing information.

Routing Table Status

Destination LAN IP	Address of the network or host to which the static route is assigned.
Subnet Mask	Determines which portion of an IP address is the network portion, and which portion is the host portion.
Gateway	IP address of the gateway device that allows for contact between the gateway and the network or host.
Interface	Determines if the Destination IP Address is on the LAN & Wireless (internal wired and wireless networks), or the Internet (WAN).

ARP

Use the **Status > ARP/ND Table** page to view Address Resolution Protocol (ARP) information.

ARP Table Status

IP Address	IP address of the device.
HW Address	MAC address of the device.
Device	Interface through which the address was learned.

RIP Status

Use the **Status > RIP** page to view information for all Routing Information Protocol activity (RIP). This page dumps all RIP-related messages for the associated RIP daemon. For each route received through RIP, it displays the time the packet was sent and the tag information. It also displays current RIP status such as RIP timer, filtering, version, RIP enabled interface, and RIP peer information.

IGMP Status

Use the **Status > IGMP Status** page to view Internet Group Management (IGMP) Information.

IGMP Status

IP Address	Multicast group that the LAN clients have joined.
Port	Lists the ports joined to the multicast address group.

VPN Status

Use the **Status > VPN Status** page to view the VPN status information.

VPN Status

Tunnel Name	Name of the VPN tunnel.
Remote Policy	The remote network policy.
Local Policy	The local network policy.
IKE Algorithm	Final result of the IKE algorithm after ISAKMP. Only applies to AUTO mode.
IPSec Algorithm	IPsec algorithm this tunnel is currently using.
TX Bytes	Number of transmitted bytes of this tunnel.
RX Bytes	Number of received bytes of this tunnel.
Connect Status	Only applies to AUTO mode.

VPN Server Status

Use the **Status > VPN Server Status** page to view information about IPsec VPN clients connected to the VPN server. The VPN server can support up to 5 VPN client connections on the SRP520 models and up to 10 on the SRP540 models.

VPN Server Status

WAN IP Address	IP address used by the VPN client to establish a tunnel with the VPN server.
IP Address	IP address assigned by the VPN server. This address is specified on the **VPN > Cisco VPN Server > Group** page, under Mode Configuration.
XAUTH Name	Account name used by the VPN client to authenticate to the VPN server which is using the PSK+XAUTH method. **NOTE** If the VPN server is using PSK Authentication only, this field shows a "--" symbol that indicates XAUTH is not used.

CDP Neighbor Information

Use the **Status > CDP Neighbor Information** page to view CDP Neighbor information.

CDP Neighbor Information

Neighbor Information	
Device ID	The neighbor's device ID number.
Local Interface	The SRP interface to which the CDP neighbor is connected.
Hold Time	Hold time before CDP will throw away packets.
Capability	The neighbor's class.
IP Address	10.52.204.254

To view additional status information, click an item in the Neighbor information list. The CDP Details table displays information about the selected device.
For example:

```
Name: Value
Device ID: SBTG-4948
Local Interface: LAN Port 1
Hold Time: 30 sec.
Capability: R, S, I
Platform: cisco WS-C4948
Port ID: GigabitEthernet1/31
IP address: 10.52.204.254
```

Status ADSL

Use the **Status > ADSL Status** page to view the ADSL and PVC status settings for the SRP.

ADSL Status

This page shows ADSL information about the SRP. This information will vary depending on the Internet Connection type specified on the **Internet Setup > WAN > Internet Setup** page.

ADSL Status Settings

DSL Status	Current DSL line status. Possible states are: ▪ **Idle**: Line is disconnected. ▪ **G.994 training**: Modem is training to the DSL service. ▪ **G.992 Started**: An ADSL service has been detected and the service is starting. ▪ **G.922 Channel Analysis**: Modem is assessing DSL channel usage. ▪ **G.992 Message Exchange**: Modem is establishing the ADSL connection. ▪ **Showtime**: ADSL modem has trained successfully and is running normally.
DSL Modulation Mode	Current modulation mode in use by the ADSL modem.
Downstream Rate	Current downstream data rate in kbps. This figure indicates the maximum throughput of the ADSL PVC. Network congestion or throughput policies imposed by your service provider may mean that lower rates are seen in practice.
Upstream Rate	Current upstream data rate in kbps. This figure indicates the maximum throughput of the ADSL connection. Network congestion or throughput policies imposed by your service provider may mean that lower rates are seen in practice.
Downstream Noise Margin	Downstream Noise Margin/Signal to Noise Ratio in dB.
Upstream Noise Margin	Measured Upstream Noise Margin/Signal to Noise Ratio in dB.
Downstream Line Attenuation	Downstream Line Attenuation in dB.
Upstream Line Attenuation	Upstream Line Attenuation in dB.

ADSL Status Settings

Downstream Transmit Power	Downstream transmit power in dBm.
Upstream Transmit Power	Upstream transmit power in dBm.

PVC Status

Use the **Status > PVC Status** page to view connectivity information for each of the PVCs configured on the DSL interface.

PVC Status

Interface	PVC interface name.
Encapsulation	Encapsulation type configured for the PVC.
VPI	PVC Virtual Path Identifier. This value can be manually configured or automatically detected.
VCI	PVC Virtual Circuit Identifier. The value can be manually configured or automatically detected.
PVC Status	Current configuration status of the PVC (applied).

STP Status

Use the **Status > STP** page to view information for all Spanning Tree Protocol (STP) activity. This page dumps all STP-related messages for the associated STP daemon and displays status information such as bridging, forward delay, hello time, and age time information.

A

Specifications

This appendix lists the specifications for the Services Ready Platforms.

SRP520-U Specifications

Feature	Model
WAN	▪ SRP521W-U: Fast Ethernet ▪ SRP526W-U: ADSL2+ Annex B ▪ SRP527W-U: ADSL2+ Annex A
LAN	4 Fast Ethernet ports
Wireless	802.11b/g/n access point with single captive antenna
Voice Ports	2 phone (FXS) ports, 1 line (FXO) port used for lifeline relay mode only
USB Ports	1 USB 2.0 port
Operating Temperature	-32° F to 140° F (0° C to 40° C)
Non-operating temperature	-22° F to 158° F (-30° C to 70° C)
Operating humidity	5 to 95% RH (noncondensing)
Voltage Range	100-240 V 50/60 Hz AC
Dimensions	(W x D x H): 170 mm (6.69 inches) x 170 mm (6.69 inches) x 42 mm (1.65 inches)
Weight	400 g (0.89 lbs)

SRP540 Specifications

Feature	Model
WAN	▪ SRP541W: 2 Gigabit Ethernet WAN ports ▪ SRP546W: ADSL2+ Annex B (ADSL over ISDN) /1 Gigabit Ethernet WAN port ▪ SRP547W: ADSL2+ Annex A/M (ADSL over POTS)/1 Gigabit Ethernet WAN port
LAN	4 Gigabit Ethernet LAN ports
Wireless	802.11b/g/n access point with two removable (TNC) antennae
Voice Ports	4 phone (FXS) ports, 1 line (FXO) port
USB Ports	2 USB 2.0 ports
Operating Temperature	-32° F to 140° F (0° C to 40° C)
Non-operating temperature	-22° F to 158° F (-30° C to 70° C)
Operating humidity	5 to 95% RH (noncondensing)
Voltage Range	100-240 V 50/60 Hz AC
Dimensions	(W x D x H): 220 mm (8.66 inches) x 170 mm (6.69 inches) x 44 mm (1.73 inches)
Weight	▪ SRP541W: 930 g (2.05 lbs) ▪ SRP546W/SRP547W: 962 g (2.12 lbs)

B

Where to Go From Here

Cisco provides a wide range of resources to help you and your customers obtain the full benefits of the Services Ready Platforms.

Product Resources

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport For information about the SRP, click Small Business Routers from the Community page.
Online Technical Support and Documentation (Login Required)	www.cisco.com/support
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/go/sbsc
Software	
Software Downloads (Login Required)	www.cisco.com/go/srp500 Click the Download Software link.
Open Source Documentation	www.cisco.com/en/US/products/ps10500/prod_release_notes_list.html
Product Documentation	
Cisco Services Ready Platform 500 Series for Small Business	www.cisco.com/go/srp500resources
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb
Marketplace	www.cisco.com/go/marketplace

B