



## ADMINISTRATION GUIDE

### Cisco SRP500 Series Services Ready Platforms (SRP520 Models)

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

<b>Chapter 1: Introducing the SRP500 Series Services Ready Platform (SRP520 Models)</b>	<b>10</b>
Feature Overview	10
Product Overview	11
Model Numbers	11
Front Panel	11
SRP521W Front Panel	11
SRP526W / SRP527W Front Panel	12
Front Panel Lights	12
Back Panel	13
SRP521W Back Panel	13
SRP526W / SRP527W Back Panel	13
Back Panel Descriptions	14
Side View	15
Top View	16
Default Settings	17
<b>Chapter 2: Getting Started with the Configuration Utility</b>	<b>18</b>
Logging In to the Configuration Utility	18
Overview of the Configuration Utility	19
Main Window Areas	19
Configuration Utility Icons	20
<b>Chapter 3: The Quick Setup Menu</b>	<b>21</b>
Basic Configuration Setup	21
WAN Setup (Ethernet)	21
WAN Setup (ADSL)	26
LAN Setup	28
Wireless Setup	30
Remote Provisioning	36
Advanced Configuration	38
Voice	38
Mobile Network Setup	38

Firewall	38
NAT	38
<b>Chapter 4: Setting up the Interfaces of the Services Ready Platforms</b>	<b>39</b>
Setting up the WAN Interface	39
Internet Setup	40
VC Settings	42
IPOA Settings / Static IP Setting	42
PPPoE Settings	43
PPPoA Settings	44
Mobile Network	45
Failover and Recovery (SRP521W)	49
Failover and Recovery (SRP526W, SRP527W)	51
Setting up the VLAN Interfaces and WAN Ports	53
DHCP Server	53
VLAN Setting	56
Port Settings	58
Setting up the Wireless LAN	59
Basic Wireless Settings	60
Wireless Protected Setup	69
WPS Method 1	69
WPS Method 2	69
WPS Method 3	70
Wireless MAC Filter	70
Advanced Wireless Settings	72
WMM Setting	75
Using the Management Interface	75
<b>Chapter 5: Configuring the Network</b>	<b>76</b>
Routing	77
Static Routes	77
RIP	78
Intervlan Routing	80

NAT	80
NAT Setting	80
Port Forwarding	81
Port Range Triggering	83
QoS	85
QoS Bandwidth Control	85
QoS Policy	86
CoS To Queue	88
DSCP To Queue	89
Firewall	89
Firewall Filter	89
Internet Access Control	92
PPPoE Relay	94
DDNS	95
DMZ	97
IGMP	98
UPnP	99
CDP Setting	100

## **Chapter 6: Configuring Voice** **102**

Configuring Voice Services	102
Understanding Voice Port Operations	102
SRP Voice Features	103
Supported Codecs	103
SIP Proxy Redundancy	104
Other SRP Voice Features	105
Registering to the Service Provider	110
Managing Caller ID Services	112
Optimizing Fax Completion Rates	114
Fax Troubleshooting	115
Silence Suppression and Comfort Noise Generation	116
Configuring Dial Plans	117

About Dial Plans	117
Digit Sequences	117
Digit Sequence Examples	119
Acceptance and Transmission the Dialed Digits	121
Dial Plan Timer (Off-Hook Timer)	122
Syntax for the Dial Plan Timer	122
Examples for the Dial Plan Timer	123
Interdigit Long Timer (Incomplete Entry Timer)	123
Syntax for the Interdigit Long Timer	124
Example for the Interdigit Long Timer	124
Interdigit Short Timer (Complete Entry Timer)	124
Syntax for the Interdigit Short Timer	124
Examples for the Interdigit Short Timer	124
Editing Dial Plans	125
Entering the Line Interface Dial Plan	125
Resetting the Control Timers	125
Secure Call Implementation	126
Enabling Secure Calls	126
Secure Call Details	127
Using a Mini-Certificate	128
Generating a Mini Certificate	129
Configuring Voice Settings	130
Info Page	130
Product Information	130
System Status	131
Line Status	132
System Page	134
System Configuration	134
Miscellaneous Settings	134
SIP Page	135
SIP Parameters	135
SIP Timer Values	138
Response Status Code Handling	140
RTP Parameters	140
SDP Payload Types	142
NAT Support Parameters	143
Provisioning Page	146
Configuration Profile	146
Firmware Upgrade	149

General Purpose Parameters	150
Regional Page	151
Defining Ring and Cadence and Tone Scripts	151
Call Progress Tones	153
Distinctive Ring Patterns	156
Distinctive Call Waiting Tone Patterns	156
Distinctive Ring/CWT Pattern Names	157
Voice > Regional > Distinctive Ring/CWT Pattern Names	157
Ring and Call Waiting Tone Spec	159
Control Timer Values (sec)	159
Vertical Service Activation Codes	162
Vertical Service Announcement Codes	168
Outbound Call Codec Selection Codes	168
Miscellaneous	<b>169</b>
Line Pages (1–2)	171
Line Enable	172
Streaming Audio Server (SAS)	172
NAT Settings	173
Network Settings	174
SIP Settings	175
Call Feature Settings	179
Voice > Line 1–2 > Call Feature Settings	179
Proxy and Registration	181
Subscriber Information	183
Supplementary Service Subscription	184
Audio Configuration	186
Dial Plan	191
FXS Port Polarity Configuration	192 192
User Pages (1–2)	193
Call Forward Settings	193
Selective Call Forward Settings	194
Speed Dial Settings	194
Supplementary Service Settings	195
Distinctive Ring Settings	197
Ring Settings	197

<b>Chapter 7: Configuring VPN</b>	<b>198</b>
IKE Policy	198
IPSec Policy	200
GRE Tunnel	203
VPN Passthrough	205
<b>Chapter 8: Administration Settings</b>	<b>206</b>
Web Access Management	206
Remote Management	208
TR069	208
SNMP	210
Local TFTP	211
Time Setup	212
Setup Wizard	213
User List	213
User Privilege Control	214
Logging	215
Factory Defaults	215
Firmware Upgrade	216
Backup & Restore	216
Backup Configuration	217
Restore Configuration	217
Reboot	217
Status	218
Switch Setting	218
<b>Chapter 9: Using Services Ready Platform Diagnostics</b>	<b>220</b>
Ping Test	220
Traceroute Test	221
Detect Active LAN Clients	221



<b>Chapter 10: Viewing the Services Ready Platforms Status</b>	<b>222</b>
Router Settings	223
Firewall Status	224
Interface Information	226
Wireless Network Status	227
Wireless Client Information	228
Mobile Network Status	228
DHCP Server Information	230
QoS Status	231
Routing Table	232
ARP Table	232
RIP Status	233
IGMP Status	233
VPN Status	234
CDP Neighbor Information	235
<b>Appendix A: Specifications</b>	<b>236</b>
<b>Appendix B: Where to Go From Here</b>	<b>238</b>

# Introducing the SRP500 Series Services Ready Platform (SRP520 Models)

Thank you for choosing the Cisco SRP500 Series Services Ready Platforms (SRP520 Models). 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 consists of these sections:

- **Feature Overview**
- **Product Overview**

For information about how to physically install the SRP and how to use the Setup Wizard to initially configure it, see the Cisco SRP500 Series Services Ready Platforms Quick Start Guide (SRP520 Models) at: [www.cisco.com/go/srp500/](http://www.cisco.com/go/srp500/)

## Feature Overview

Thank you for choosing the Cisco Services Ready Platform SRP 500 Series (SRP520 Models).

The SRP 500 Series platforms includes these features:

- Intelligence to support voice, data, security, and application services.
- Industry-leading Session Initiation Protocol (SIP) stack to deliver clear, high-quality voice service.
- Interoperability with popular soft switches and voice gateways.
- Integrated security, VPN capabilities, and an 802.11n wireless access point.
- Standards-based provisioning for streamlined deployments.

## 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 of the unit.

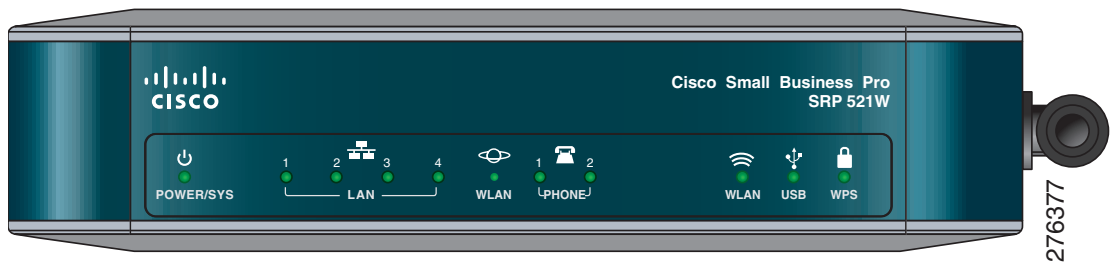
### Model Numbers

The following table describes the SRP520 Model numbers:

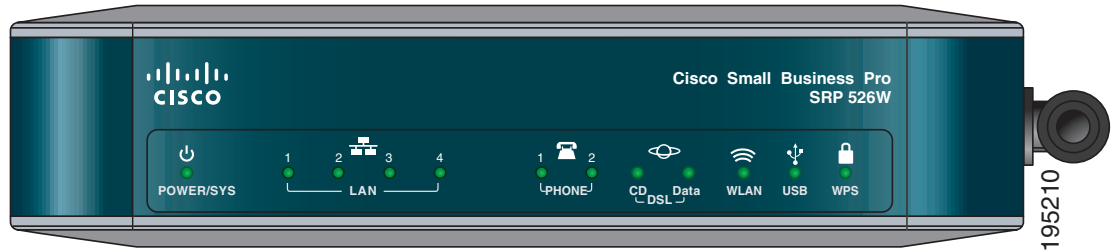
Model	Description
<b>SRP521W</b>	Fast Ethernet WAN  2 Phone (FXS) ports, 1 Line (FXO) port, 1 WAN (10/100) port, 4 LAN (10/100) ports, 1 USB 2.0 port, 802.11n, and WiFi Protected Setup (WPS)
<b>SRP526W</b>	ADSL2+ Annex B (ADSL over ISDN)  2 Phone (FXS) ports, 1 Line (FXO) port, 1 DSL port, 4 LAN (10/100)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

### Front Panel

#### SRP521W Front Panel



## SRP526W / SRP527W Front Panel



### Front Panel Lights

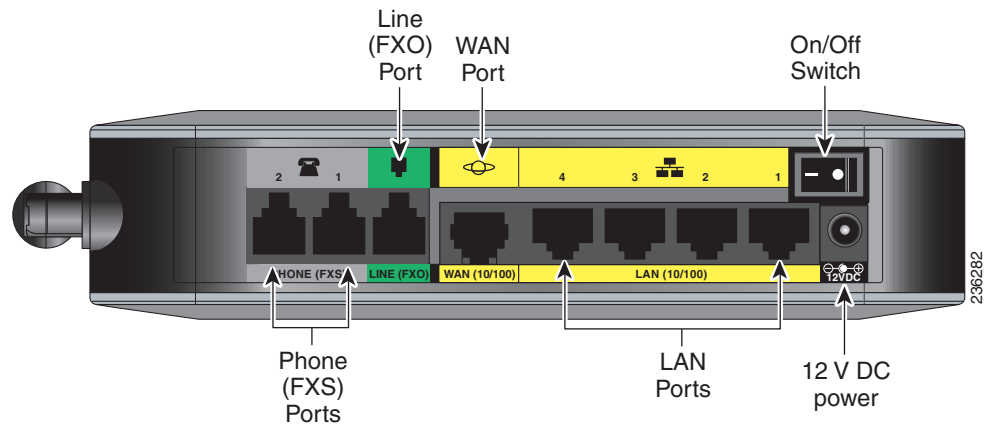
The following table describes the lights on the front panel of the SRP. These lights are used for monitoring system activity.

Lights (Green)	Description
POWER/SYS	Lights when the SRP has successfully booted and is ready to use. Flashes when the SRP is booting.
LAN ports (1–4)	Lights when a link is established. Flashes when there is activity on the LAN port.
WAN port (SRP521W only)	Lights when a link established. Flashes when there is activity on the WAN port.
Phone (FXS) ports (1–2)	Lights when a link is established. Flashes when there is activity on the Phone port.
DSL CD	Flashes when a DSL service is detected. Lights solid green when synchronized.
DSL Data (SRP 526W/527W only)	Flashes when there is DSL activity on the line.
WLAN	Lights when the radio is powered on and operational. Flashes when there is wireless activity on the WLAN port.
USB port	Lights when the connected USB device is operational. Flashes if there is a device failure or unsupported device.
WPS button	Lights 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.

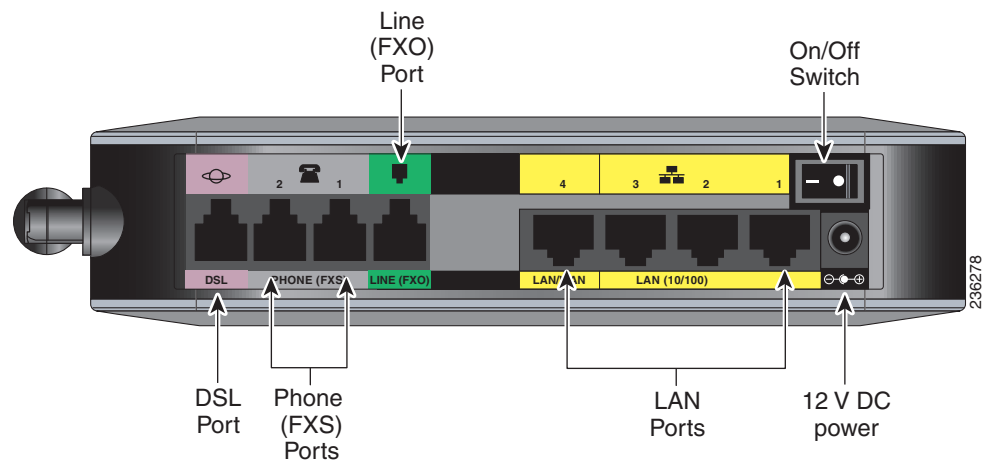
## Back Panel

The back panel is where you connect the network devices. The ports on the panel vary depending on the model.

### SRP521W Back Panel



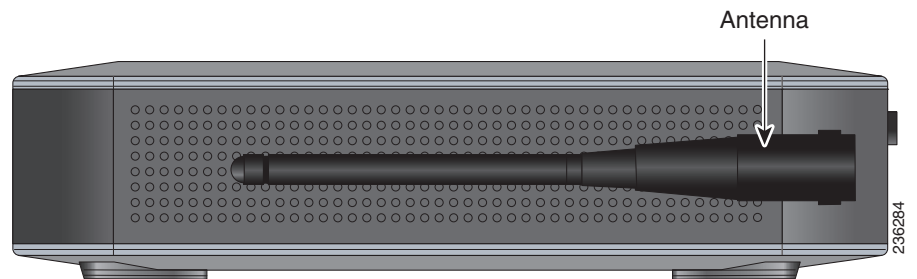
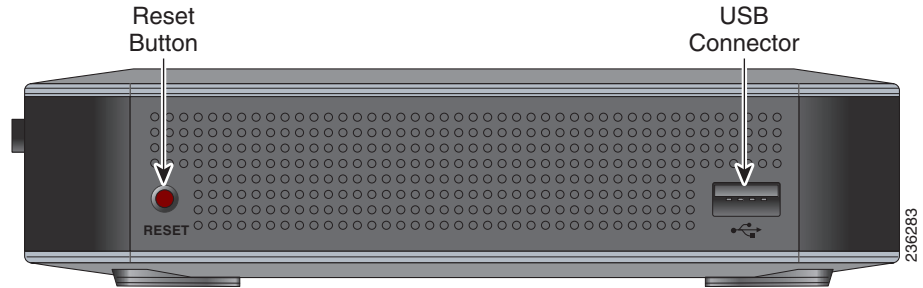
### SRP526W / SRP527W Back Panel



## Back Panel Descriptions

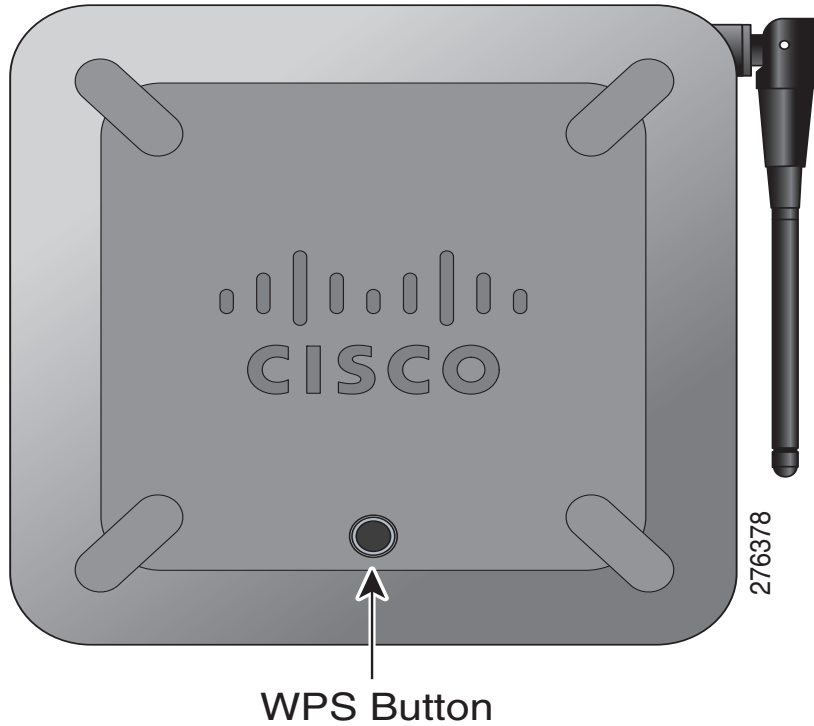
Feature	Description
DSL port SRP526/SRP527W only	Connects the SRP to your DSL connection.
Phone (FXS) ports (1–2)	Connect directly to an analog telephone, fax machine, or similar device.  If your analog phone requires a separate bell line (as is often the case in the UK), you might need to connect a ring adapter between the SRP and your phone so that the phone rings when calls are presented.
Line (FXO) port	Connects to a PSTN, which is the analog telephone service network that a traditional telephone service uses.
WAN (10/100) port SRP521W only	Connects the SRP to your Wide-Area-Network (WAN).
LAN (10/100) ports (1–4)	Connects to a wired computer and other network devices.
On/Off Switch	Powers the SRP on or off.
12 V DC power	Connects to the provided power adapter.

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.
USB port	Connects to a compatible USB Modem. For information about connecting the SRP to a USB see <a href="#">Mobile Network, page 45</a> .
Antenna	The WiFi antenna.

Top 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

Parameter	Value
Device IP	192.168.15.1
Username	cisco
Password	cisco
Admin Username	admin
Admin Password	admin
DHCP Range	192.168.15.100 to 149
Data VLAN	VLAN 1
Voice VLAN	VLAN 100, published to the Cisco VOIP phones via CDP

## Getting Started with the Configuration Utility

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

This chapter includes the following sections:

- [Logging In to the Configuration Utility](#)
- [Overview of the Configuration Utility](#)

### Logging In to the Configuration Utility

This section describes how to log in to Services Ready Platform Configuration Utility.

- 
- STEP 1** Connect a computer to an available LAN port of your SRP. By default, your PC will become a DHCP client of the SRP and will receive an IP address in the 192.168.15.x range.
- STEP 2** Start a web browser.
- In the Address bar, enter **http://192.168.15.1**. This is the default address of the SRP.
- STEP 3** When the login window opens, enter the username and password to login as the administrator.
- The default username is **admin**.  
The default password is **admin**.
- NOTE** Passwords are case sensitive.
- NOTE** If you log in as **cisco** (with password of **cisco**), the Setup Wizard will automatically begin. If you log in as **admin**, you can start the Setup Wizard by clicking **Administration > Setup Wizard**.

**STEP 4** Click **Log In**. The Services Ready Platform Configuration Utility opens.

## Overview of the Configuration Utility

### Main Window Areas

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







Number	Component	Description
1	Menu Bar	Contains the major function categories. Click a menu item to change to another category.

Number	Component	Description
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 on the title of a feature or subfeature to open it.
3	Main Content	The main content of the feature appears in this area.

## Configuration Utility Icons

The Configuration Utility has icons and buttons for commonly used configuration options. The following table describes these icons:

Icon	Description
 Edit Icon	The Edit icon lets you edit an existing item from a list. After making your changes, click the <b>Submit</b> button to save your changes.
 Add Item Icon	The Add Item icon lets you add an item to a list. After you have created a new item, click the <b>Submit</b> button to save the new item.
 Delete Item Icon	The Delete Item icon lets you delete an item from a list. After you have deleted an item, click the <b>Submit</b> button to save your changes.
 Increment Decrement Icons	The Increment and Decrement icons let you change numeric values. Click the “+” icon to increment a value; click the “-” icon to decrement a value. Click the <b>Submit</b> button to save your changes.

## The Quick Setup Menu

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

- **Basic Configuration Setup**
- **Advanced Configuration**

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

To access these pages click **Quick Setup > Basic Configuration Setup** from the Configuration Utility menu bar.

### Basic Configuration Setup

The features in Basic Configuration Setup lets you setup your WAN, LAN, Wireless, and Remote Provisioning.

#### WAN Setup (Ethernet)

Use the WAN Setup page to quickly setup your Ethernet WAN interface.

- 
- STEP 1** Click **Quick Setup > WAN Setup**. The *WAN Setup* window opens.
  - STEP 2** Enter your Internet connection type and any optional WAN settings as necessary.
  - STEP 3** Click **Submit** to save your settings.
-

Field	Description
WAN	The WAN interface.
VLAN ID	The VLAN ID.
Connection Type	The type of Internet connection your ISP provides from the drop-down menu.
	<p><b>Automatic Configuration - DHCP</b></p> <p>By default, the Router's Internet Connection Type is set to <b>Automatic Configuration - DHCP</b>, which should be kept only if your ISP supports DHCP or you are connecting through a dynamic IP address.</p>
	<p><b>Static IP</b></p> <p>If you are required to use a permanent IP address to connect to the Internet, select Static IP.</p> <ul style="list-style-type: none"> <li>▪ <b>Internet IP Address and Subnet Mask</b> This is the Router's IP Address and Subnet Mask as seen by external users on the Internet (including your ISP). If your Internet connection requires a static IP address, then your ISP will provide you with a Static IP Address and Subnet Mask.</li> <li>▪ <b>Default Gateway</b> Your ISP will provide you with the Gateway IP Address.</li> <li>▪ <b>DNS 1-3</b> The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. If you wish to use another, type that IP Address in one of these fields. You can type up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.</li> </ul>

Field	Description
	<p data-bbox="748 354 1062 388"><b>PPPoE (For ADSL user)</b></p> <p data-bbox="748 417 1458 596">Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet Connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE.</p> <ul style="list-style-type: none"> <li data-bbox="748 627 1495 741"> <p data-bbox="748 627 1114 655">▪ User Name and Password</p> <p data-bbox="792 678 1495 741">Enter the User Name and Password you use when logging onto your ISP through a PPPoE connection.</p> </li> <li data-bbox="748 764 1377 846"> <p data-bbox="748 764 971 791">▪ Service Name</p> <p data-bbox="792 814 1377 846">If provided by your ISP, enter the Service Name.</p> </li> <li data-bbox="748 869 1495 1241"> <p data-bbox="748 869 1045 896">▪ Connect on Demand</p> <p data-bbox="792 919 1495 1241">You can configure the Router to disconnect your Internet connection after a specified period of inactivity (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. If you want your Internet connection to remain active at all times. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.</p> </li> <li data-bbox="748 1264 1479 1503"> <p data-bbox="748 1264 927 1291">▪ Keep Alive</p> <p data-bbox="792 1314 1479 1503">This option keeps you connected to the Internet indefinitely, even when your connection sits idle. To use this option, click the radio button next to Keep Alive. The default Redial Period is 30 seconds (in other words, the Router will check the Internet connection every 30 seconds).</p> </li> </ul>

Field	Description
	<p><b>PPTP</b></p> <p>Point-to-Point Tunneling Protocol (PPTP), is a service that applies to tunneling connections.</p> <ul style="list-style-type: none"> <li>▪ <b>Internet IP Address and Subnet Mask</b> The IP Address and Subnet Mask as seen by external users on the Internet (including your ISP). If your Internet connection requires a static IP address, then your ISP will provide you with a Static IP Address and Subnet Mask.</li> <li>▪ <b>Gateway</b> Your ISP will provide you with the Gateway IP Address.</li> <li>▪ <b>DNS 1-3</b> Your ISP will provide you with at least one DNS Server IP Address. If you wish to use another, type that IP Address in one of these fields. You can type up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.</li> <li>▪ <b>PPTP Server IP</b> This is the IP address of the PPTP Server. Enter the IP address provided by your ISP.</li> <li>▪ <b>User Name and Password</b> Enter the User Name and Password you use when logging onto your ISP through a PPTP connection.</li> <li>▪ <b>Connect on Demand</b> If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. If you want your Internet connection to remain active at all times. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.</li> <li>▪ <b>Keep Alive</b> This option keeps you connected to the Internet indefinitely, even when your connection sits idle. Click the radio button next to Keep Alive. The default Redial Period is 30 seconds (in other words, the Router will check the Internet connection every 30 seconds).</li> </ul>



Field	Description
	<p data-bbox="748 359 821 386"><b>L2TP</b></p> <p data-bbox="748 422 1463 489">Layer Two Tunneling Protocol (L2TP) is a service that applies to tunneling connections.</p> <ul data-bbox="748 520 1498 1850" style="list-style-type: none"><li data-bbox="748 520 1498 632">▪ DHCP To Keep only if your ISP supports DHCP or you are connecting through a dynamic IP address.</li><li data-bbox="748 657 1498 831">▪ Internet IP Address and Subnet Mask The IP Address and Subnet Mask as seen by external users on the Internet (including your ISP). If your Internet connection requires a static IP address, then your ISP will provide you with a Static IP Address and Subnet Mask.</li><li data-bbox="748 856 1498 940">▪ Gateway Your ISP will provide you with the Gateway IP Address.</li><li data-bbox="748 966 1498 1171">▪ DNS 1-3 Your ISP will provide you with at least one DNS Server IP Address. If you wish to use another, type that IP Address in one of these fields. You can type up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.</li><li data-bbox="748 1197 1498 1308">▪ Server IP Address This is the IP address of the L2TP Server. Enter the IP address provided by your ISP.</li><li data-bbox="748 1333 1498 1417">▪ User Name and Password Enter the User Name and Password provided by your ISP.</li><li data-bbox="748 1442 1498 1617">▪ Connect on Demand: Max Idle Time If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again.</li><li data-bbox="748 1642 1498 1850">▪ Keep Alive This option keeps you connected to the Internet indefinitely, even when your connection sits idle. The default Redial Period is 30 seconds (in other words, the Router will check the Internet connection every 30 seconds).</li></ul>

Field	Description
Host Name	Your host name. This should be in the format of name.dyndns.org.
Domain Name	Your domain name. This should be in the format of name.tzo.org.
MTU	The Maximum Transmission Unit (MTU) size.
Static DNS 1 to 3	Static Domain Name System (DNS) entries 1 to 3. The DNS is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS server IP address. If you wish to use another, type that IP address.

## WAN Setup (ADSL)

Use the WAN Setup page to quickly setup your ADSL WAN interface.

- STEP 1** Click **Quick Setup > WAN Setup**.
- STEP 2** The *WAN Setup* window opens.
- STEP 3** Enter your VC and IP settings as necessary.
- STEP 4** Click **Submit** to save your settings.

Field	Description
Encapsulation	Encapsulation is the 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).
Multiplexing	Select the method used to route different kinds of data through different virtual circuits (VCs) in the ATM network: Logical Link Control (LLC) encapsulation (also called LLC-SNAP) or Virtual Channel (VC) multiplexing (also called VC-Mux).

Field	Description
QoS Type	<p>Select the 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.</p> <ul style="list-style-type: none"> <li>▪ Pcr Rate—When QoS is set to CBR, VBR_RT, or VBR_NRT, the Peak Cell Rate (PCR) in cells per second must be entered here.</li> <li>▪ Scr Rate—When QoS is set to VBR_NRT or VBR_RT, the Sustained Cell Rate (SCR) in cells per second must be entered here.</li> <li>▪ MBS—When QoS is set to VBR_NRT or VBR_RT, the MBS in cells per second must be entered here.</li> <li>▪ CDVT—When QoS is set to CBR, VBR_NRT or VBR_RT, the CDVT in cells per second must be entered here.</li> </ul>
VPI/VCI Auto Detect	<p>You can enable or disable automatic detection of the VPI and VCI values (see next) that identify your line to the ATM network.</p>
Virtual Circuit	<p>The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) are values used to identify your line to your ISP's ATM network.</p>
Static IP Setting	<p>Select this option if your ISP provides you with a static IP address. Enter the following 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 up to three Domain Name System (DNS) servers, or leave the fields blank to allow a DNS server to be chosen dynamically.</p>

## LAN Setup

Use the LAN Setup page to quickly setup the LAN interface.

- STEP 1** Click **Quick Setup > LAN Setup**. The *LAN Setup* window opens.
- STEP 2** Enter your Internet connection type and any optional LAN settings as necessary.
- STEP 3** Click **Submit** to save your settings.

Field	Description
DHCP Name	The DHCP Name.
Local IP Address / Subnet Mask	The DHCP IP address and subnet mask as seen by external users on the Internet (including your ISP).
DHCP Server	The DHCP server settings. Click the <b>Show DHCP Reservation</b> button to change DHCP server settings.
WAN Interface	The WAN Interface.
Option 66	Option to user a TFTP server. Choices are None, Local TFTP Server, or Remote TFTP Server. The default value is None. <ul style="list-style-type: none"><li>▪ The Local TFTP Server option indicates that the Services Ready Platform is used as the TFTP server for that LAN subnet.</li><li>▪ The Remote TFTP Server option indicates that the TFTP server is obtained on the Services Ready Platform WAN interface.</li><li>▪ The Manual TFTP Server option indicates an IP address is entered manually for the TFTP server (other than the Services Ready Platform).</li></ul>
Option 67	The name of the configuration file to be requested from the TFTP server.

Field	Description
DNS Proxy	The DNS proxy relays DNS requests to the current public network DNS server for the proxy, and replies as a DNS resolver to the client device on the network. To enable the DNS Proxy feature, select <b>Enabled</b> . The default setting is <b>Disabled</b> .
Starting IP Address	Enter a value for the DHCP server to start with when issuing IP addresses. Because the default IP address is 192.168.15.1, the starting IP address must be 192.168.15.2 or greater, but smaller than 192.168.15.149. The default starting IP address is 192.168.15.100.
Maximum DHCP Users	Enter the maximum number of PCs that you want the DHCP server to assign IP addresses. This number cannot be greater than 253. The default is 50.
IP Address Range	The range of DHCP addresses is displayed here.
Client Lease Time	Amount of time a network user will be allowed connection to the gateway with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be “leased” this dynamic IP address. After the time is up, the user will be automatically assigned a new dynamic IP address. The default is 0 minutes, which means one day.
Static DNS	The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS server IP address. If you wish to use another, type that IP address.
WINS	The Windows Internet Naming Service (WINS) manages PCs interaction with the Internet. If you use a WINS server, enter the IP address of the server here. Otherwise, leave this field blank.

## Wireless Setup

Use the Wireless Setup page to quickly setup the Wireless network.

- STEP 1** Click **Quick Setup > Wireless Setup**. The *Wireless Setup* window opens.
- STEP 2** In the Network Mode field, select a wireless network mode.
- If you have Wireless-N, Wireless-G, and Wireless-B devices in your network, use the default setting, **Mixed**.
  - If you have only Wireless-G and Wireless-B devices in your network, select BG-Mixed. If you have only Wireless-N devices, select **Wireless-N Only**.
  - If you have only Wireless-G devices, select **Wireless-G Only**.
  - If you have only Wireless-B devices, select **Wireless-B Only**.
  - If you do not have any wireless devices in your network, select **Disabled**.
- STEP 3** In the Radio Band field, select a bandwidth for the wireless network.
- STEP 4** If necessary, select a channel that pertains to the type of bandwidth that you selected in the previous step.
- STEP 5** If necessary, add or edit the wireless network name (SSID).
- STEP 6** Click **Edit** to enable security for the SSID. Cisco strongly recommends that you enable security for each SSID.
- STEP 7** Click **Submit** to save your settings.

Field	Description
Network Mode	The network mode. the default mode is <b>Mixed</b> .
Radio Band	The bandwidth of the radio channel. The default is <b>Standard - 20MHz Channel</b> .
Wide Channel	If you selected <b>Wide - 40MHz Channel</b> for the Radio Band setting, this setting will be available for your primary Wireless-N channel. Select any channel from the drop-down menu.

Field	Description
Standard Channel	If you selected <b>Wide - 40MHz Channel</b> or <b>Standard - 20MHz Channel</b> 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 <b>Wide - 40MHz Channel</b> for the Radio Band setting, then the Standard Channel will be a secondary channel for Wireless-N. The default value is channel 11.
Wireless Network Name (SSID)	The first default wireless network uses the name "cisco_data" which is connected to the default VLAN. The second default wireless network uses the name "cisco_voice" which is connected to the voip 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).
Broadcast Network Name	When wireless clients survey the local area for wireless networks to associate, they detect the SSID broadcast by the gateway. If you want to broadcast the SSID, keep the check box selected. If you do not want to broadcast the SSID, deselect the check box.
Enabled Network	To enable the wireless network, select the check box. To disable the wireless network, deselect the check box.
WPS Hardware Button	To enable the WPS hardware button on the top of SRP, select the check box.
Edit	Click the Edit button to set the security mode for the SSID. Each mode is described below.

Field	Description
Standard Channel	If you selected <b>Wide - 40MHz Channel</b> or <b>Standard - 20MHz Channel</b> 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 <b>Wide - 40MHz Channel</b> for the Radio Band setting, then the Standard Channel will be a secondary channel for Wireless-N. The default value is channel 11.
Wireless Network Name (SSID)	The first default wireless network uses the name "cisco_data" which is connected to the default VLAN. The second default wireless network uses the name "cisco_voice" which is connected to the voip 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).
Broadcast Network Name	When wireless clients survey the local area for wireless networks to associate, they detect the SSID broadcast by the gateway. If you want to broadcast the SSID, keep the check box selected. If you do not want to broadcast the SSID, deselect the check box.
Enabled Network	To enable the wireless network, select the check box. To disable the wireless network, deselect the check box.
WPS Hardware Button	To enable the WPS hardware button on the top of SRP, select the check box.
Edit	Click the Edit button to set the security mode for the SSID. Each mode is described below.



Field	Description
Edit (continued)	<ul style="list-style-type: none"> <li>▪ WEP—basic encryption method offering two levels of encryption: 128-bit is stronger than 64-bit encryption.                             <ul style="list-style-type: none"> <li>- Authentication Type—The default is Auto, which allows either Open System or Shared Key authentication. With Open System authentication, the sender and the recipient do NOT use a WEP key for authentication. With Shared Key authentication, the sender and recipient use a WEP key for authentication. Select Shared Key only use Shared Key authentication.</li> <li>- Encryption—Select the appropriate level of encryption, 64-bit (10 hex digits) or 128-bit (26 hex digits).</li> <li>- Passphrase—To automatically generate keys, enter a passphrase and click the Generate button.</li> <li>- Key 1-4—If you want to manually enter the WEP keys, then enter them in the Key 1-4 fields.</li> <li>- TX Key—To indicate which WEP key to use, select a transmit key number.</li> </ul> </li> </ul>

Field	Description
Edit (continued)	<ul style="list-style-type: none"> <li>▪ WPA Personal—Wi-fi Protected Access (WPA) is a newer security standard for securing wireless communications.                             <ul style="list-style-type: none"> <li>- WPA Algorithms—Select the algorithm you want to use, TKIP or AES. (AES is a stronger encryption method than TKIP)</li> <li>- WPA Shared key—Enter the key shared by the Router and your other network devices. It must have 8-63 ASCII characters or 64 hex characters.</li> <li>- Group Key Renewal—Enter the Key Renewal period, which tells the Router how often it should change encryption keys.</li> </ul> </li> </ul>
Edit (continued)	<ul style="list-style-type: none"> <li>▪ WPA2 Personal                             <ul style="list-style-type: none"> <li>- WPA Algorithms—Select the algorithm(s) you want to use, AES or TKIP + AES. (AES is a stronger encryption method than TKIP)</li> <li>- WPA Shared Key—Enter the key shared by the Router and your other network devices. It must have 8-63 ASCII characters or 64 hex characters.</li> <li>- Group Key Renewal—Enter the Key Renewal period, which tells the Router how often it should change encryption keys.</li> </ul> </li> </ul>

Field	Description
Edit (continued)	<ul style="list-style-type: none"><li data-bbox="792 359 1500 611">▪ WPA Enterprise—This option features WPA used in coordination with a 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 server. (This option should only be used when a RADIUS server is reachable from the Router.)</li><li data-bbox="792 642 1500 747">- WPA Algorithms—Select the algorithm(s) you want to use, TKIP or AES. (AES is a stronger encryption method than TKIP.)</li><li data-bbox="792 779 1500 884">- RADIUS Server Address (Primary and Secondary)—Enter the IP address of your RADIUS server.</li><li data-bbox="792 915 1500 978">- RADIUS Port—Enter the port number of your RADIUS server.</li><li data-bbox="792 1010 1500 1157">- Shared Secret—Enter the key shared by the Router and RADIUS server. The key can include 8 to 63 ASCII characters or 64 hexadecimal characters.</li><li data-bbox="792 1188 1500 1293">- Key Renewal Timeout—Enter the Key Renewal period, which tells the Router how often it should change encryption keys.</li></ul>

Field	Description
Edit (continued)	<ul style="list-style-type: none"> <li>▪ WPA2 Enterprise—This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) <ul style="list-style-type: none"> <li>- WPA Algorithms—Select the algorithm(s) you want to use, AES or TKIP + AES. (AES is a stronger encryption method than TKIP.)</li> <li>- RADIUS Server Address (Primary and Secondary)—Enter the IP address of your RADIUS server.</li> <li>- RADIUS Port—Enter the port number of your RADIUS server.</li> <li>- Shared Secret—Enter the key shared by the Router and RADIUS server. The key can include 8 to 63 ASCII characters or 64 hexadecimal characters.</li> <li>- Key Renewal Timeout—Enter the Key Renewal period, which tells the Router how often it should change encryption keys.</li> </ul> </li> </ul>
Edit (continued)	Disabled—No security is set for the SSID. This option is not recommended by Cisco.

## Remote Provisioning

This feature lets you configure communication with an Access Control Server (ACS) via TR-069 CPE WAN Management Protocol (CWMP).

- STEP 1** Click **Quick Setup > Remote Provisioning**. The *Remote Provisioning* window opens.
- STEP 2** Click **Enabled** to enable remote provisioning.
- STEP 3** Enter the URL for ACS. The format should be `http(s)://xxx.xxx.xxx.xxx:port` or `xxx.xxx.xxx.xxx:port`. The `xxx.xxx.xxx.xxx` is domain name or IP of ACS server; and after “:” is port. Both IP and port must be filled.
- STEP 4** Enter the ACS username and password.

**STEP 5** Optionally, enter the Connection request username and password.

**STEP 6** Optionally, enter the periodic inform interval.

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

Field	Description
Status	Select an option to enable or disable remote provisioning.
ACS URL	The URL for ACS. The format should be http(s)://xxx.xxx.xxx.xxx:port or xxx.xxx.xxx.xxx:port. The xxx.xxx.xxx.xxx is domain name or IP of ACS server; and after “:” is port. Both IP and port must be filled.
ACS Username	The username for ACS. The default username is OUI Serial Number; this should be the same as configured at ACS side and must be filled.
ACS Password	The password for ACS. This should be the same as configured at ACS side and must be filled.
Connection Request URL	This field will be auto-filled and does not need to be filled manually. The format is http://xxx.xxx.xxx.xxx:port. The xxx.xxx.xxx.xxx is WAN IP of CPE.
Connection Request Username	Connection request username. This should be the same as configured at ACS side.
Connection Request Password	Connection request password. This should be the same as configured at ACS side.
Periodic Inform Interval	The periodic inform interval. The default value is 86400 seconds.
Periodic Inform Enable	To enable or disable periodic inform.
Request Download	If applied, ACS may call the Download RPC after it receives the request from CPE.

---

## Advanced Configuration

The features in Advanced Configuration Setup lets you configure advanced settings with Voice, Mobile Network Setup, the Firewall, and NAT.

To access this page click **Quick Setup > Advanced Configuration Setup** from the Configuration Utility.

### Voice

The Voice option lets you administer and view voice settings. For more details, refer to [Configuring Voice, on page 102](#).

### Mobile Network Setup

The Mobile Network Setup option lets you administer the mobile network settings. For more details, refer to [Mobile Network, on page 45](#).

### Firewall

The Firewall option lets you administer the firewall filter settings. For more details, refer to [Firewall, on page 89](#).

### NAT

The NAT option lets you administer the NAT settings. For more details, refer to [NAT, on page 80](#).

## 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 Interface](#)
- [Setting up the VLAN Interfaces and WAN 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 Interface

This section describes how to configure the WAN interface settings for the SRP including:

- [Internet Setup](#)
- [Mobile Network](#)
- [Failover and Recovery \(SRP521W\)](#)
- [Failover and Recovery \(SRP526W, SRP527W\)](#)

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 password for your SRP. To change it, see [User List, page 213](#). 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.
- STEP 2** To add or edit interfaces in the WAN Interface List, click the add or edit icons.
- STEP 3** Adjust the **Port Settings** as necessary.
- STEP 4** To clone a MAC address to the SRP, click **Enabled** and then enter a MAC address. To clone the MAC address of your computer, click the **Clone Your PC's MAC** button.
- STEP 5** Click **Submit** to save your settings.
- 

Field	Description
WAN Interface List	The WAN Interface list which shows the physical link, its protocol, and its IP address if one exists. In each entry, you can create new sub-interface by clicking the Add Subinterface button or the Edit button.  If you have more than one sub-interface, you can choose either one as the default routing interface by selecting the Default Route radio button.
Flow Control	WAN flow control. To set flow control for the WAN, select Enabled and click Submit. The default setting is Disabled.
Speed Duplex	WAN Speed Duplex mode. Selections are Auto-negotiate, 10 Half, 10 Full, 100 Half and 100 Full. To set WAN speed duplex mode, choose the mode and click Submit. The default setting is Auto-negotiate.



Field	Description
MAC Address Clone	A MAC address is a 12-digit code assigned to a unique piece of hardware for identification purposes. Some ISPs require that you to register a MAC address in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you may assign the MAC address that you have currently registered with your ISP to the SRP with the MAC Address Clone feature. To clone your MAC address, select Enabled, click Clone Your PC's MAC, and click Submit. The default value is Disabled.
WAN Interface Detail	The Details of WAN area shows information about your WAN.

When a new interface is chosen or edited by using the Add or Edit icons, one of the following VC options may be available.

## VC Settings

Field	Description
Multiplexing	Multiplexing defines the way in which different protocols are handled within a DSL virtual circuit. You can choose between Logical Link Control (LLC) encapsulation (also called LLC-SNAP) or Virtual Channel (VC) multiplexing (also called VC-Mux).
QoS Type	<p>Select the 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.</p> <ul style="list-style-type: none"> <li>▪ <b>Pcr Rate</b>—When QoS is set to CBR, VBR_RT, or VBR_NRT, enter the Peak Cell Rate (PCR) in cells per second.</li> <li>▪ <b>Scr Rate</b>—When QoS is set to VBR_NRT or VBR_RT, enter the Sustained Cell Rate (SCR) in cells per second.</li> <li>▪ <b>MBS</b>—When QoS is set to VBR_NRT or VBR_RT, enter the MBS in cells per second.</li> <li>▪ <b>CDVT</b>—When QoS is set to CBR, VBR_NRT or VBR_RT, enter the CDVT in cells per second.</li> </ul>
VPI/VCI Auto Detect	You can enable or disable 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 offered on the following VC pairs: 0/35, 8/35, 0/43, 0/51, 0/59, 8/43, 8/51, 8/59, 0/38

## IPOA Settings / Static IP Setting

Select the IPOA Settings / Static IP Setting option if your ISP provides you with a static IP address. 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 up to three Domain Name System (DNS) servers, or leave the fields blank to allow a DNS server to be chosen dynamically.

Field	Description
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.
Primay/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 user name 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.

Field	Description
Service Name	(PPPoE only.) A Service Name is a string required by some ISPs. Fill this in only if your ISP requires it.
User name and Password	Enter the strings that your ISP has instructed you to use. The user name may be called a "username," "login name," or "login."
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.

Field	Description
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 re-establish it. The default redial period is 20 seconds.
Enable MTU/MRU greater than 1492	Extra header information used on PPPoE connections over ADSL that limits the maximum packet size that can be sent to 1492 bytes. Enable this setting only if instructed to do so by your ISP.

### PPPoA Settings

Field	Description
User name and Password	Enter the strings that your ISP has instructed you to use. The user name may be called a “username,” “login name,” or “login.”
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 re-establish it. The default redial period is 20 seconds.

## 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 see: [www.cisco.com/go/srp500](http://www.cisco.com/go/srp500).

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

**STEP 2** If necessary, change any global settings in the Global Settings area. The **Card Status** field shows the status of your mobile card.

**STEP 3** 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 setup your mobile network card.

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

Field	Description
Connect Mode	<p>Choose <b>Auto</b> or <b>Manual</b> Mode. If using are using manual mode, you will need to access the Configuration Utility to establish an Internet connection through the mobile connection. Click <b>Connect</b> to establish a connection when required. Click <b>Disconnect</b> to tear down the connection.</p> <p><b>NOTE</b> On the SRP521W, the Ethernet Connection Recovery and Interface Connection Failover works only if the Connection Mode is set to Auto. If you select Auto, you must select <b>Connect on Demand</b> and <b>Keep Alive</b>. If you select <b>Connect on Demand</b> option, you can configure the SRP to terminate the Internet connection after it has been inactive for a specified period of time (Max Idle Time).</p>

Field	Description
Connect on Demand	<p>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, Connect on Demand enables the modem to automatically re-establish a terminated connection when a user attempts to access the Internet again.</p> <p>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.</p>
Tunnel Protocol	<p>The Tunnel Protocol (PPTP/L2TP) is supported through a USB modem by one of these methods.</p> <ul style="list-style-type: none"> <li>▪ <b>NONE.</b> Select this option to disable protocol tunneling.</li> <li>▪ <b>PPTP/L2TP.</b> Select PPTP or L2TP depending on the service you want to use. You will need to provide the server IP address, user name, and password.</li> <li>▪ <b>Follow Ethernet WAN configure.</b> Select this option to make the Tunnel Protocol follow the configuration of the Ethernet WAN.</li> </ul>

Field	Description
Card Status	<p>Displays the current modem connection status as initializing, connecting, connected, disconnecting, or disconnected.</p> <p>These messages might also appear:</p> <ul style="list-style-type: none"> <li>▪ Please set APN manually                             <p>Appears when the SRP is unable to determine the APN from the operator in automatic mode.</p> </li> <li>▪ Searching for service...</li> <li>▪ no SIM card</li> <li>▪ SIM locked</li> <li>▪ SIM busy</li> <li>▪ SIM ready</li> <li>▪ pin code needed</li> <li>▪ pincode error</li> <li>▪ Card is locked</li> <li>▪ Card is not activated</li> <li>▪ Card initialized error</li> <li>▪ error</li> </ul> <p><b>NOTE</b> If Connect Mode is set to Manual, you can click a button to connect or disconnect your modem.</p>
Configure Mode	<p>The SRP automatically detects supported modems and presents a list of appropriate default configurations. If you need to override any of these settings (with the exception of the SIM PIN), select manual configuration mode.</p>
Card Model	<p>The data card model that is inserted into the USB drive.</p>
Carrier	<p>The mobile network service provider for the Internet connection. This setting is required when you are using HSDPA/UMTS/GPRS Internet service. Select the card issue country from the first drop-down menu list, then select the card issue provider from the second drop-down list.</p>

Field	Description
Access Point Name (APN)	The Internet network to which the mobile device is connecting to. Enter the access point name provided by your mobile network service provider.
Dial Number	The dial number for the Internet connection. Enter the Dial Number provided by your mobile network service provider.
User Name/ Password	Enter the user name and password provided by your mobile network service provider.
SIM PIN	The PIN code associated with your SIM card. Enter your SIM PIN number here. This field is only displayed for GSM cards.
Server Name	The name of the server for the Internet connection if provided by your service provider.
Authentication	The type of authentication used by your service provider. Choose your authentication type from the drop-down list. The default is Auto. If you don't 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. If your location supports only one mobile data service, you may set up for enhance build up connection. The first selection will always search for HSPDA/3G/UMTS service or switch to GPRS automatically only when it is available.



---

## Failover and Recovery (SRP521W)

An Internet connection can be established via the WAN port or a wireless modem plugged into the USB port. Refer to [www.cisco.com/go/srp500](http://www.cisco.com/go/srp500) for more details on compatible USB modem devices.

While both Ethernet and USB modem may be connected, only one of them can be used to establish a link at a time. Whenever the Internet connection fails, the SRP automatically attempts to bring up another connection on another interface. This feature is called *Failover*. Whenever the Ethernet Internet connection recovers, the SRP automatically attempts to bring back and recover the Internet connection. This feature is called *Recovery*.

---

**STEP 1** Click **Interface Setup > Failover & Recovery**. The *Failover & Recovery* window opens.

**STEP 2** If necessary, enable the Ethernet Connection Recovery feature by clicking **Enabled**.

When this option is enabled, the SRP sets the ethernet interface to the highest priority. Enabling this feature also enables the Interface Connection Failover feature. Whenever the Internet connection fails, the SRP automatically attempts to bring up the mobile network connection on the USB interface (if available). Whenever the Ethernet Internet connection recovers, the SRP automatically attempts to bring back and recover the Ethernet Internet connection.

**NOTE** Your Mobile Connection Mode must be set to Auto to use the Ethernet Connection Recovery feature.

**STEP 3** If necessary, enter an ethernet timeout value.

**STEP 4** Choose a site on which to perform failover validation in the Failover Validation Site area. Either use the SRP or enter the IP address for a custom site.

**STEP 5** If necessary, change the priority of the WAN interfaces by clicking the **Up** or **Down** buttons.

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

---

#### Failover and Recovery Settings (SRP521W)

Field	Description
Ethernet Connection Recovery	This feature ensures that your Ethernet Internet connection is always connected when available.
Interface Connection Failover	Failover detection works by detecting the physical connection and/or presence of traffic on the Internet link. If the link is idle, the SRP attempts to ping a destination. If the ping does not reply, the SRP assumes the link is down and attempts to fail over to another interface.
Timeout	The time interval at which the SRP detects the status of the Internet connection. The default timeout interval is 60 seconds.
Connection Validation Site	A ping target for the SRP to use to detect the status of the Internet connection. By default the SRP pings the Network Time Protocol (NTP) servers. You may specify a different IP address as a target here.
WAN Interfaces	This area provides information on current status of the Ethernet Internet connection and Mobile Network connection. You can click the Status hyperlink to view the details. You may also configure the interface priority by clicking Up or Down. Note that the interface priority setting is configurable only when Ethernet Connection Recovery is disabled.

---

## Failover and Recovery (SRP526W, SRP527W)

An Internet connection can be established via the DSL port or a wireless modem plugged into the USB port. Refer to [www.cisco.com/go/srp500](http://www.cisco.com/go/srp500) for more details on compatible USB modem devices.

While both DSL and 3G USB modem may be connected, only one of them can be used to establish a link at a time. Whenever the Internet connection fails, the SRP automatically attempts to bring up another connection on another interface. This feature is called *Failover*. Whenever the DSL Internet connection recovers, the SRP automatically attempts to bring back and recover the Internet connection. This feature is called *Recovery*.

---

**STEP 1** Click **Interface Setup > Failover & Recovery**. The *Failover & Recovery* window opens.

**STEP 2** If necessary, enable the Ethernet Connection Recovery feature by clicking **Enabled**.

When this option is enabled, the SRP sets the ethernet interface to the highest priority. Enabling this feature also enables the Interface Connection Failover feature. Whenever the Internet connection fails, the SRP automatically attempts to bring up the mobile network connection on the USB interface (if available). Whenever the Ethernet Internet connection recovers, the SRP automatically attempts to bring back and recover the Ethernet Internet connection.

**NOTE** Your Mobile Connection Mode must be set to Auto to use the Ethernet Connection Recovery feature.

**STEP 3** If necessary, enter an ethernet timeout value.

**STEP 4** Choose a site on which to perform failover validation in the Failover Validation Site area. Either use the SRP or enter the IP address for a custom site.

**STEP 5** If necessary, change the priority of the WAN interfaces by clicking the **Up** or **Down** buttons.

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

---

**Failover and Recovery Settings (SRP526W/SRP527W)**

<b>Field</b>	<b>Description</b>
Connection Recovery	This feature ensures that your Internet connection is always connected when available.
Interface Connection Failover	Failover detection works by detecting the physical connection and/or presence of traffic on the Internet link. If the link is idle, the SRP attempts to ping a destination. If the ping does not reply, the SRP assumes the link is down and attempts to fail over to another interface.
Timeout	The time interval at which the SRP detects the status of the Internet connection. The default timeout interval is 60 seconds.
Connection Validation Site	A ping target for the SRP to use to detect the status of the Internet connection. By default the SRP pings the Network Time Protocol (NTP) servers. You may specify a different IP address as a target here.
WAN Interfaces	This area provides information on current status of the Internet connection and Mobile Network connection. You can click the Status hyperlink to view the details. You may also configure the interface priority by clicking Up or Down. Note that the interface priority setting is configurable only when Connection Recovery is disabled.

## Setting up the VLAN Interfaces and WAN Ports

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

- **DHCP Server**
- **VLAN Setting**
- **Port Settings**

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

### DHCP Server

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

**NOTE** When creating a DHCP server you must also specify the IP address and mask for the VLAN interface it is assigned to. If you do not assign a DHCP Server to a VLAN interface, then the IP addressing options are configured directly through the VLAN settings.

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

- 
- STEP 1** Click **Interface Setup > LAN > DHCP Server**. The *DHCP Server* window opens.
  - STEP 2** To view the information for a DHCP entry, click one of the items in the **DHCP List**. The DHCP information displays in the DHCP Details table.
  - STEP 3** To add or delete a DHCP entry from the DHCP list, click the **Edit** (pencil) or **Delete** (x) icon.
  - STEP 4** To create a new DHCP Server Pool, click **Add Entry**. The *DHCP Server* window for the new entry opens.
  - STEP 5** Under Router IP, enter the **DHCP Name** and **Local IP Address/Subnet Mask**.
  - STEP 6** Configure the DHCP Server Settings as defined in the **DHCP Server Settings** table.
  - STEP 7** Click **Submit** to save your settings.
-

DHCP Server Settings	
Field	Description
<b>Router IP</b>	
DHCP Name	A label which identifies this DHCP Server configuration and is used to assign the service to a VLAN interface.
Local IP Address/ Subnet Mask	The IP address and subnet mask used to configure the VLAN interface to which this DHCP rule is applied.
<b>DHCP Server Setting</b>	
Show DHCP Reservation button	Click this button to review and modify the DHCP reservations. Click the button again to hide the reservation tables.
WAN Interface	Choose the WAN Interface from which the related DHCP information, specifically DNS, is obtained.
Option 66	<p>Provides provisioning server address information to hosts requesting this option. Server information can be defined in one of three ways:</p> <ul style="list-style-type: none"> <li>▪ <b>Local TFTP Server:</b> The SRP uses its own TFTP server to source provisioning files so it returns its own local IP address to the client.</li> <li>▪ <b>Remote TFTP Server:</b> 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.</li> <li>▪ <b>Manual TFTP Server:</b> 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 will also accept and offer a full URL including protocol, path and filename to meet to requirements of specific clients.</li> </ul>

DHCP Server Settings	
Field	Description
Option 67	Provides a configuration/bootstrap filename to hosts requesting this option. This is used in conjunction with option 66 to allow the client to form an appropriate TFTP request for the file.
DNS Proxy	<p>If DNS proxy is 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 it was configured with. See the note about DNS in <a href="#">Internet Setup, page 40</a>.</p> <p>If DNS proxy is disabled, then DHCP clients will be offered DNS server information based on the following:</p> <ul style="list-style-type: none"> <li>▪ If the Static DNS field is configured, then that server alone will be offered to clients.</li> <li>▪ 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.</li> </ul>
Starting IP Address	Enter an IP address of the first address in this pool.
Maximum DHCP Users	Enter the 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. It cannot be greater than 1024. The default is 50.
IP Address Range	The range of DHCP addresses is displayed
Client Lease Time	Amount of time 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	Use to define a DNS server address that DHCP clients should use directly for name resolution. This option is only required when the DNS proxy feature is disabled for this DHCP server. The field is hidden when DNS proxy is enabled.

DHCP Server Settings	
Field	Description
WINS	The Window Internet Naming Service (WINS) manages the window's host name to address resolution. If you use a WINS server, enter the IP address of the server here. Otherwise, leave this field blank.

## VLAN Setting

VLAN settings are configured on this page. After clicking **Add Entry**, you can create another VLAN.

- STEP 1** Click **Interface Setup > LAN > VLAN Setting**. The *VLAN Setting* window opens. You can edit or delete a VLAN entry by clicking the edit or delete icon.  
  
From this page you can view the list of configured VLANs, add or delete a VLAN, and view the details for a selected VLAN.
- STEP 2** To edit or delete a VLAN entry from the DHCP list, click the **Edit** (pencil) or **Delete (x)** icon.
- STEP 3** To view the information for a VLAN entry, click any of the items in the **VLAN Details List**. The VLAN information for the DHCP Pool displays in the **VLAN Details** table.
- STEP 4** To create a new VLAN, click **Add Entry**. The *VLAN Settings* window for the new VLAN opens.
- STEP 5** Specify the VLAN settings for the new entry as defined in the **VLAN Settings** table.
- STEP 6** Click **Submit** to save your settings.
- STEP 7** Click **Add Entry** to open the VLAN Add page. From this page you can add a VLAN entry.
- STEP 8** Click **Submit** to save your settings.



VLAN Settings	
Field	Description
VLAN Name	Bridge or VLAN name.
VLAN ID	Bridge or VLAN ID.
Voice VLAN	Click this box if you want to use voice. Only use this option in VLAN mode.
Address Type	<p>Address type determines the way in which the VLAN IP interface is configured.</p> <ul style="list-style-type: none"> <li>Choose <b>None</b> if an IP interface is not required. This would typically be the case when bridging ports only.</li> <li>Choose <b>Static IP Address</b> to manually define an address for the interface, or Dynamic IP Address, to request an address from a DHCP server on the local network.</li> </ul> <p>Choose <b>DHCP server</b> to enable a previously configured DHCP Server service on this interface. In this case, the VLAN IP address will be derived from the DHCP Server configuration.</p>
Available Interface	The interfaces that are available to be added to the permissions for the pool members. To move an interface to the Added Interface list, click the interface, and then click the <b>right-arrow button (&gt;)</b> . To move all of the interfaces at once, click the <b>double right-arrow button (&gt;&gt;)</b> .
Added Interface	The interfaces that were selected as members of the VLAN bridge. If you want to remove an interface from this list, click the interface and then click the <b>left arrow button (&lt;)</b> . To remove all of the interfaces at once, click the <b>double left-arrow button (&lt;&lt;)</b> .

### 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 Setting**. The *Port Setting* window opens.
- STEP 2** Specify the flow control and speed duplex settings as defined in the **Port Settings** table. You can only configure these settings for LAN ports 1–4.
- STEP 3** To view the port information, click any of the items in the Port List. The port information is displayed in the Port Details 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

Field	Description
Mode	<p>Describes the currently configured behavior of the port.</p> <ul style="list-style-type: none"> <li>▪ <b>Desktop mode:</b> Provides attached devices with access to a single data VLAN for which the SRP provides DHCP services. Incoming traffic from the host can be tagged or untagged. Outgoing traffic to the host will be untagged.</li> <li>▪ <b>IP Phone + Desktop mode:</b> 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.</li> </ul>

Port Settings	
Field	Description
Enabled Flow Control	<p>Mechanism for temporarily stopping the transmission of data on this physical interface.</p> <p>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.</p> <p>To enable this feature, check the box. The default setting is Disabled.</p>
Speed Duplex	Choose the duplex mode. You can select from Auto-negotiate, 10 Half, 10 Full, 100 Half and 100 Full. The default is Auto-negotiate.
Port Details	Shows detailed information about the ports.

## Setting up the Wireless LAN

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

- **Basic Wireless Settings**
- **Wireless Protected Setup**
- **Wireless MAC Filter**
- **Advanced Wireless Settings**
- **WMM 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 the SRP's integrated wireless access point and up to four wireless networks.

Use the Basic Wireless Settings page to 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** Configure the network security settings for each SSID. In the Wireless Table area, click the **Edit** link in the Security column. The Wireless Security window opens.
  - STEP 4** Choose the security mode setting from the drop-down list. The default is Disabled.

When you enable a 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 click **Submit** to save your settings.

You are returned to the Basic Wireless page.

---

Basic Wireless Settings	
Field	Description
Network Mode	<p>From this drop-down list, choose the wireless mode based on the type of devices in your network.</p> <p><b>NOTE</b> 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.</p> <ul style="list-style-type: none"> <li>▪ If you have Wireless-N, Wireless-G, and Wireless-B devices in your network, select <b>Mixed</b>.</li> <li>▪ If you have only Wireless-G and Wireless-B devices in your network, select <b>BG-Mixed</b>.</li> <li>▪ If you have only Wireless-N devices, select <b>Wireless-N Only</b>.</li> <li>▪ If you have only Wireless-G devices, select <b>Wireless-G Only</b>.</li> <li>▪ If you have only Wireless-B devices, select <b>Wireless-B Only</b>.</li> <li>▪ If you don't want to use the integrated wireless access point, select <b>Disabled</b>.</li> </ul>
Radio Band	<p>From this drop-down list, select the wireless bandwidth for your network. There are three options: Auto, Standard-20MHz Channel, and Wide-40MHz Channel. The default is Standard-20MHz Channel.</p> <p>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.</p>
Wide Channel	<p>If you selected Wide-40MHz Channel for the Radio Band setting, then this setting will be available for your primary Wireless-N channel. Select any channel from the drop-down list. If radio band is selected automatically, the wide channel is also chosen automatically.</p>

Basic Wireless Settings	
Field	Description
Standard Channel	<p>If you selected Wide-40MHz Channel 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.</p> <p>If you selected Wide-40MHz Channel for the Radio Band setting, then the Standard Channel will be a secondary channel for Wireless-N. The default is channel 11. If radio band is selected automatically, the standard channel will also be chosen automatically.</p>
<b>Wireless Table</b>	
Wireless Network Name (SSID)	<p>The name of the network that clients use when connecting to the network.</p> <p>By default 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).</p> <p>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 <b>Enabled Network</b>.</p> <p><b>NOTE</b> Your ISP or ITSP might be responsible for controlling the SSID2 settings. Contact your ISP or ITSP for more information.</p>
SSID1/2/3/4	<p>The SSID is the 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, and you can enable two other wireless networks if needed.</p> <p>For each wireless network you need to configure the Wireless Network Name (SSID), Broadcast Network Name, and Enable Network option.</p>

Basic Wireless Settings	
Field	Description
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. If you want 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.

Field	Description
<b>Wireless Security Settings</b> (To access, click the <b>Edit Security</b> button for any configured SSIDs)	
Security Mode	Select the security method for your wireless network. The SRP supports these wireless security mode options: WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, and WEP. (WPA stands for Wi-Fi Protected Access, which is a stronger security standard than WEP encryption). WEP stands for Wired Equivalent Privacy.  If you do not want to use wireless security, keep the default setting, Disabled. Cisco recommends that you use the highest level of security that is supported by your client wireless devices.
<b>WEP Security Mode Settings</b>	
WEP	WEP is a basic encryption method, which is not as secure as WPA. WEP may be required if your network devices do not support WPA.
Authentication Type	Choose <b>Auto</b> or <b>Shared Key</b> . 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.

Field	Description
Encryption	Select a level of WEP encryption, 64-bit, 10 hex digits or 128-bit, 26 hex digits. The default is 64-bit, 10 hex digits. 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 <b>Generate</b> . Valid keys appear.
Key 1-4	<p>If you did not enter a passphrase, enter the WEP key(s) manually.</p> <p>If you chose 64-bit WEP encryption, the key must be exactly 5 ASCII or 0 hexadecimal characters in length. If you chose 13 ASCII or 128-bit WEP encryption, the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are “0” to “9” and “A” to “F”.</p> <p><b>NOTE</b> The SRP supports a single WEP key for the access point. If multiple SSIDs are configured with WEP, they must share the same key.</p>
TX Key	Select which TX (Transmit) Key to use. The default is 1.
<b>WPA Personal Mode Settings</b>	
WPA Personal	WPA Personal provides stronger wireless security with advanced encryption (TKIP or AES).
WPA Algorithms	WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, AES or TKIP. The default is TKIP.
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.
<b>WPA2 Personal Mode Settings</b>	
WPA2 Personal	Provides strong wireless security with advanced encryption (AES or TKIP + AES).



Field	Description
WPA Algorithms	WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, AES or TKIP + AES. The default is TKIP + AES.
WPA Shared Key	Enter a Passphrase of 8-63 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.
<b>WPA and WPA2 Enterprise Settings</b>	
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 type of algorithm, AES or TKIP. The default for WPA is TKIP. The default for WPA2 is AES.
Primary RADIUS Server	<ul style="list-style-type: none"> <li>▪ <b>RADIUS Server:</b> Enter the IP Address of the RADIUS server.</li> <li>▪ <b>RADIUS Port:</b> Enter the port number of the RADIUS server. The default value is 1812.</li> <li>▪ <b>Shared Secret:</b> Enter the key shared between the SRP and the server. The key can include 8 to 63 ASCII characters or 64 hexadecimal characters.</li> </ul>
Secondary RADIUS Server	<ul style="list-style-type: none"> <li>▪ <b>RADIUS Server Address:</b> Enter the IP Address of the RADIUS server.</li> <li>▪ <b>RADIUS Port:</b> Enter the port number of the RADIUS server.</li> <li>▪ <b>Shared Secret:</b> Enter the key shared between the SRP and the server. The key can include 8 to 63 ASCII characters or 64 hexadecimal characters.</li> </ul>

Field	Description
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.

Field	Description
<b>Wireless Security Settings</b> (To access, click the <b>Edit Security</b> button for any configured SSIDs)	
Security Mode	Select the security method for your wireless network. The SRP supports these wireless security mode options: WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, and WEP. (WPA stands for Wi-Fi Protected Access, which is a stronger security standard than WEP encryption). WEP stands for Wired Equivalent Privacy.  If you do not want to use wireless security, keep the default setting, Disabled. Cisco recommends that you use the highest level of security that is supported by your client wireless devices.
<b>WEP Security Mode Settings</b>	
WEP	WEP is a basic encryption method, which is not as secure as WPA. WEP may be required if your network devices do not support WPA.
Authentication Type	Choose <b>Auto</b> or <b>Shared Key</b> . 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 128-bit, 26 hex digits. The default is 64-bit, 10 hex digits. 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 <b>Generate</b> . Valid keys appear.

Field	Description
Key 1-4	<p>If you did not enter a passphrase, enter the WEP key(s) manually.</p> <p>If you chose 64-bit WEP encryption, the key must be exactly 5 ASCII or 0 hexadecimal characters in length. If you chose 13 ASCII or 128-bit WEP encryption, the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are “0” to “9” and “A” to “F”.</p> <p><b>NOTE</b> The SRP supports a single WEP key for the access point. If multiple SSIDs are configured with WEP, they must share the same key.</p>
TX Key	Select which TX (Transmit) Key to use. The default is 1.
<b>WPA Personal Mode Settings</b>	
WPA Personal	WPA Personal provides stronger wireless security with advanced encryption (TKIP or AES).
WPA Algorithms	WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, AES or TKIP. The default is TKIP.
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.
<b>WPA2 Personal Mode Settings</b>	
WPA2 Personal	Provides strong wireless security with advanced encryption (AES or TKIP + AES).
WPA Algorithms	WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, AES or TKIP + AES. The default is TKIP + AES.
WPA Shared Key	Enter a Passphrase of 8-63 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.

Field	Description
<b>WPA and WPA2 Enterprise Settings</b>	
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 type of algorithm, AES or TKIP. The default for WPA is TKIP. The default for WPA2 is AES.
Primary RADIUS Server	<ul style="list-style-type: none"> <li>▪ <b>RADIUS Server:</b> Enter the IP Address of the RADIUS server.</li> <li>▪ <b>RADIUS Port:</b> Enter the port number of the RADIUS server. The default value is 1812.</li> <li>▪ <b>Shared Secret:</b> Enter the key shared between the SRP and the server. The key can include 8 to 63 ASCII characters or 64 hexadecimal characters.</li> </ul>
Secondary RADIUS Server	<ul style="list-style-type: none"> <li>▪ <b>RADIUS Server Address:</b> Enter the IP Address of the RADIUS server.</li> <li>▪ <b>RADIUS Port:</b> Enter the port number of the RADIUS server.</li> <li>▪ <b>Shared Secret:</b> Enter the key shared between the SRP and the server. The key can include 8 to 63 ASCII characters or 64 hexadecimal characters.</li> </ul>
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.

---

## Wireless Protected Setup

Use the Wi-Fi Protected Setup 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 WPS 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.
  - STEP 3** WPS is enabled by default. Select **Disabled** if you don't want to use this feature for the selected VLAN.
  - STEP 4** Choose a Wi-Fi Protected Setup method. The current Wi-Fi Protected status is displayed at the bottom of the page.

There are three methods to configure your WiFi settings by using WPS. Use the method that applies to the client device that you are configuring.

### WPS Method 1

Use this method if your client device has a Wi-Fi Protected Setup button.

- 
- STEP 1** Click or press the **Wi-Fi Protected Setup** button on the client device, or press the Wi-Fi protected Setup button on the SRP540 front panel, if that was associated with the currently selected SSID. See [Basic Wireless Settings, page 60](#).
  - STEP 2** Click the **Wi-Fi Protected Setup** button on this page.
  - STEP 3** After the client device is configured, click **OK**. Then refer to your client device or its documentation for further instructions.

---

### WPS Method 2

Use this method if your client device has a Wi-Fi Protected Setup PIN number.

- 
- STEP 1** Enter the PIN number in the field on this page.
  - STEP 2** Click **Register**.

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

### WPS Method 3

Use this method if your client device asks for the SRP 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.

- 
- 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 is SSID is cisco-data, and 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 the Wireless MAC Filter option is enabled, you can 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, Interface, 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** Wireless access can be filtered 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	
Field	Description
<b>Wireless MAC Filter</b>	
Select a SSID	Choose the name of the wireless network that you want to configure. The default data SSID is cisco-data and the default voice SSID is cisco-voice.
Enabled/Disabled	To filter wireless users by MAC Address, either permitting or blocking access, select <b>Enabled</b> . The default is Disabled.
<b>Access Restriction</b>	
Prevent	Select this option to block wireless access from the clients that you specify in the MAC Address Table. This is the default setting.
Permit	Select this option to permit wireless access only from the clients that you specify in the MAC Address Table.
Show Client List	Click this button to display a list of computers and other devices that are connected to this wireless network. To add a listed client to the MAC Address Table, check the <b>Save to MAC Address Filter List</b> box and click <b>Add</b> . To hide the client list, click <b>Hide Client List</b> .
<b>MAC Address Table</b>	
01-32	Enter the MAC addresses of the devices whose wireless access 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 60](#).
- 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 default value of 2347 is recommended.
- STEP 4** Change any settings in the Global Settings area as defined in the [Advanced Wireless Settings](#) table.

Click **Submit** to save your settings.

Advanced Wireless Settings	
Field	Description
<b>Advanced Wireless Setup</b>	
Select a SSID	Choose the 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.
<b>Global Settings</b>	



Advanced Wireless Settings	
Field	Description
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 <b>Enabled</b> . 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. If you want to specify the SRP's rate of data transmission, configure the Transmission Rate setting.
N Transmission Rate	Set the rate of data transmission rate depending on the speed of your Wireless-N networking. Select from a range of transmission speeds, or select <b>Auto</b> 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.
Transmission Rate	Set the data transmission rate depending on the speed of your wireless network. Select from a range of transmission speeds, or select <b>Auto</b> 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.

<b>Advanced Wireless Settings</b>	
<b>Field</b>	<b>Description</b>
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.
DTIM Interval	This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the SRP has buffered broadcast or multicast 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 default value is 1.
Fragmentation Threshold	This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may 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	Enter a value between 40 and 3500 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the SRP to synchronize the wireless network. 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.

---

### WMM 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**. The default is Disabled.
  - 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.
  - STEP 2** To edit an entry in the List of Loopback Interfaces, 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.
-

# Configuring the Network

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

- **Routing**
- **NAT**
- **Port Range Triggering**
- **Firewall**
- **PPPoE Relay**
- **DDNS**
- **IGMP**
- **UPnP**
- **CDP Setting**

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

---

## Routing

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

- **Static Routes**
- **RIP**
- **Intervlan Routing**

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.

---

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

From this page you can view the current static routing list and details of the selected route, or add another route to the Static Routing List.

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

The Static Routing window for the new entry opens.

**STEP 3** Enter a name for the new route.

**STEP 4** Enter the destination IP address and subnet mask for the specified network or host to which want to assign a static route.

**STEP 5** Enter the IP address of the gateway that allows for contact between the SRP and the specified network or host.

**STEP 6** Choose the interface for this route.

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

---

Static Route Settings	
Field	Description
Enter Route Name	Enter a name for the static route.
Destination Subnet	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 the Internet (WAN).

## RIP

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 router's. The SRP determines the network packets' route based on the fewest number of hops between the source and destination.

- 
- STEP 1** Click **Network Setup > Routing > RIP**. The *RIP* 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 as defined in the **RIP Settings** table.

The SRP allows you to define which networks will participate in the routing protocol either by interface or IP address subnet.

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

RIP Settings	
Field	Description
RIP List	<p><b>Interface:</b> Displays the list of interfaces.</p> <p><b>RIP Enabled:</b> Select to enable or disable RIP on the interface.</p> <p><b>Passive Mode:</b> With the passive mode interface, all receiving packets are processed as normal and do not send either multicast or unicast RIP packets except to RIP neighbors. To select passive mode, select <b>Enabled</b> from the RIP Config Edit window.</p> <p><b>Authentication:</b> If you are sending and receiving RIP Version 2 packets, you can select a RIP authentication on an interface. The SRP supports two modes of authentication on an interface: Simple Password Authentication and MD5 Authentication.</p> <p><b>NOTE:</b> RIP Version 1 does not support authentication.</p>
RIP Version	To limit the types of packets that can be transmitted, choose <b>Version 1</b> or <b>Version 2</b> . Alternatively, choose <b>RIP v1/v2</b> to allow both Version 1 and Version 2 packets to be transmitted.
RIP Timer	<p>RIP uses timers to regulate its performance. These include a routing-update timer, a route-timeout timer, and a route-flush timer.</p> <p><b>Update:</b> Specify the rate at which the SRP sends routing updates. The default is 30 seconds.</p> <p><b>Timeout:</b> Specify the rate at which the SRP expects to receive routing updates from each router in the routing table. 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.</p> <p><b>Flush:</b> Specify the maximum period that the SRP will wait for an update before removing a route from the routing table.</p>
RIP By	Select whether you want to enable RIP by interface or by IP Subnet.
RIP List	Displays the RIP settings all SRP interfaces. To edit the settings, click the <b>Edit</b> (pencil) icon.

---

## 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 have configured wireless guest access.

- 
- STEP 1** Click **Network Setup > Routing > Intervlan Routing**. The *Intervlan Routing* window opens.
- STEP 2** To enable Intervlan Routing, select **Enabled**. This is the default setting. To disable it, select **Disabled**.
- STEP 3** Click **Submit** to save your changes if required.
- 

## NAT

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

- **NAT Setting**
- **Port Forwarding**
- **Port Range Triggering**

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

### NAT Setting

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** To enable NAT, select **Enabled**. This is the default setting. To disable NAT, click **Disabled**. All ALGs are disabled by default.



---

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

---

## Port Forwarding

Use the Port Forwarding page if your 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 internal servers that host these services.

Port Forwarding enables the SRP to route packets addressed to the WAN interface for a specific application port, or port range, to an internal 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.

After clicking **Add Entry**, you can create another entry for another network service. To edit an entry, click the **Edit** (pencil) icon.

**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 43**.

---

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

**STEP 2** To add an 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	
Field	Description
Port Forwarding Type	<p>Choose the type of port forwarding from the drop-down list</p> <p>Select <b>Single Port Forwarding</b> to forward traffic for a specified port on to the same or an alternative port on the target server in the LAN. Select <b>Port Range Forwarding</b> to forward 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.</p>
Application Name	<p>For single port forwarding, choose a common application from the drop-down list (such as Telnet, or DNS).</p> <p>To enter application that is not on the list, choose <b>Add a new name</b>, and then enter the name of a new application.</p>
Enter a Name	For single port-forwarding, enter the name of the new application.
Wan Interface Name	Select the WAN interface to which the traffic is initially addressed.
External Port	For single port forwarding, enter the port number that external clients will use to set up a connection with the internal server.
Internal Port	<p>For single port forwarding, enter the port number that the SRP uses when forwarding traffic to the internal server.</p> <p>For simplicity, internal and external port numbers will often be the same, however, different External port numbers could 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.</p>
Protocol	Select the protocol(s) to be forwarded: TCP, UDP or Both.

Port Forwarding Settings	
Field	Description
IP Address	Enter the IP address of the local server that should receive forwarded traffic.
Enabled	Click <b>Enabled</b> 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 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 port triggering entries from the Port Range Triggering List and the view the details about a selected entry.

**STEP 2** To edit an existing entry, click the **Edit** (pencil) icon.

**STEP 3** To add a new entry for port range triggering, Click **Add Entry**.

The Port Range Triggering window opens.

**STEP 4** Enter the settings for port range triggering as defined in the **Port Range Triggering Settings** table.

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

Port Range Triggering Settings	
Field	Description
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	<p>Enter the starting and ending port numbers of the triggered port range.</p> <p>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. Check with the Internet application's documentation for the appropriate port numbers.</p>
Forwarded Range	<p>Enter the starting and ending port numbers of the forwarded port range</p> <p>These ports are opened when an outbound connection is made to one of the ports specified in the Triggered Range fields. Check with the Internet application documentation for the appropriate port numbers.</p>
Protocol	Choose a protocol type from the down list (TCP, UDP, or both).
Enable	Click <b>Enable</b> to enable the applications that you have defined. The default is disabled.

---

## QoS

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

- [QoS Bandwidth Control](#)
- [QoS Policy](#)
- [CoS To Queue](#)
- [DSCP To Queue](#)

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

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

Bandwidth Shaping Control Settings	
Field	Description
Upstream Bandwidth	<p>Enter the maximum available upstream bandwidth value for the connected broadband service. The default value is 100000 Kbps for Ethernet interfaces.</p> <p><b>NOTE</b> Setting this value higher than the available service bandwidth can result in traffic being dropped arbitrarily in the service provider's network.</p>
Strict High Priority Queue	<p>Defines the bandwidth required for strict priority traffic. Traffic from the strict queue within this rate is transmitted before that from any other queue.</p>
High, Medium, Normal, Low	<p>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.</p> <p>To adjust the relative weighting of the queues, click the plus (+) button and minus (-) button.</p> <p>In the absence of strict priority traffic, data from these queues are handled on a weighted round robin basis.</p> <p><b>NOTE</b> The bandwidth values on this page indicate the minimum assured throughput available per queue under load. Higher rates of traffic may be seen, when other queues are under utilized.</p>

## QoS Policy

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.
- STEP 2** To edit an existing rule, click the **Edit** (pencil) icon.
- STEP 3** To add a new policy, click **Add Entry**.

The QoS Priority Setting window opens.

- STEP 4** Choose the QoS category from the drop-down list (Application, MAC Address, Ethernet Port, or VLAN).
- STEP 5** Specify the policy settings for the particular category as defined in the **QoS Policy Settings: Classification** table.
- STEP 6** Enter the QoS Queuing and Marking settings for the specified category.
- STEP 7** Click **Submit** to save your settings.

<b>QoS Policy Settings: Classification</b>	
<b>Application Category</b>	
Applications/ Name	Choose a standard application from the drop-down list. To enter an application that is not on the list, choose <b>Add a New Application</b> , and then enter the name of the new application.
LAN	Choose the source LAN.
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.
<b>MAC Address Category</b>	
Name	Enter a name to describe this rule.
LAN	Choose the source LAN.
MAC Address	Enter the MAC address of the originating device in the following format: xx:xx:xx:xx:xx:xx
<b>Ethernet Port Category</b>	
Name	Enter a name of the Ethernet port. For example: Ethernet port1.
LAN	Choose the source LAN.
Ethernet	Choose the source Ethernet port.

VLAN Category	
Name	Enter the name of the Ethernet port. For example: data_Lan.
VLAN	Choose the source VLAN.
IP Address	
Name	Enter a name to describe this rule.
Destination IP	Enter the target IP address or network that will classify the traffic for this rule.
Destination Mask	Enter the mask for the target IP address or network.
LAN	Choose the source LAN.
QoS Policy Settings: Queuing	
Priority	Choose the queuing priority for this traffic: Strict, High, Medium, Normal, or Low.

## 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.

**STEP 2** Change the priority settings for each VLAN CoS as necessary.

The VLAN (CoS) priority tag (0-7) values are mapped to router's queue, where zero is the lowest and 7 is the highest.

**STEP 3** Choose a priority level from the drop-down list.

The priority defines the traffic forwarding queue to which traffic the given CoS is mapped.

Click **Submit** to save your settings.



---

## 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.
  - STEP 3** Choose a priority level from the drop-down list. The priority defines the traffic forwarding queue to which traffic with the given DSCP is mapped. The available priorities are Strict, High, Medium, Normal, and Low.
  - STEP 4** 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**
- **Internet Access Control**

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

### Firewall Filter

Use the Firewall Filter page to enable 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** Select **Enabled** to enable SPI firewall protection. The firewall is enabled by default.
  - 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	
Field	Description
SPI Firewall Protection	To enable a firewall protection, select <b>Enabled</b> . The default is Enabled.
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 <b>Disabled</b> to allow anonymous Internet requests.
Filter Internet NAT Redirection	This feature prevents local clients from accessing local services through active port forwarding rules (i.e. 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 <b>Enabled</b> to filter Internet NAT redirection, or <b>Disabled</b> to disable it.
Filter IDENT (Port 113)	Prevents port 113 from being scanned by devices outside of your local network. This filter is enabled by default. Select <b>Enabled</b> to filter port 113, or <b>Disabled</b> 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 box. This filter is disabled by default.
Java	Java is a programming language for websites. If you filter Java, you will prevent access to Internet sites created using this programming language. To enable Java filtering, check the box. This filter is disabled by default.

ActiveX	ActiveX is a programming language for websites. If you filter ActiveX, you will prevent access to Internet sites that use this programming language. To enable ActiveX filtering, check the box. This filter is disabled by default.
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 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.

## 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 > Internet Access Control**. The *Internet Access Control* window opens.
- From this window you can view existing policy details, edit a policy, and add a new 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.
- STEP 5** Optionally, click **Show Edit List** to display the MAC address, IP address, and IP address range policies.
- STEP 6** Under the Schedule area, select the days and times when you want this policy to be enforced.
- STEP 7** Select other blocking options as necessary.
- STEP 8** Click **Submit** to save your settings.
-

Internet Access Control Settings	
Field	Description
Enter Policy Name	Enter a name for the policy.
Status	To enable this policy, click <b>Enabled</b> . To disable this policy, click <b>Disabled</b> . The default setting is Disabled
From, To	You can apply the rule to all traffic by choosing <b>From All, To All</b> , or you can limit the rule to apply only to particular interfaces, such as From VLAN1 to WAN1.
Applied PCs (Optional)	To apply the policy only to specified PCs, click the <b>Show Edit List</b> 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 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.
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 this box 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. 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. Enter up to four IP addresses.

Blocking by Application	<p>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 (&gt;&gt;) to move the application to the Blocked List.</p> <p>To remove an application from the Blocked List, click it and then click the button left-arrow button (&lt;&lt;).</p>
Modify Application	<p>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 <b>Add Entry</b>.</p> <p>To modify a service, select it from the Application list. Change its name, port range, and/or protocol setting and then click the <b>Modify</b> icon.</p> <p>To delete a service, select it from the Application list. Then click the <b>Delete</b> (pencil) icon.</p>

## 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 add view or edit a relay and 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**.

**STEP 4** Select the WAN and LAN interfaces for this rule.

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

PPPoE Relay Settings	
Field	Description
WAN interface	Select the WAN Interface for this rule. For example: WAN1 or WAN2.
LAN interface	Select the LAN Interface for this rule. For example: VLAN1 or VLAN100.
PPPoE Relay Status	<p>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).</p> <p>The relay functionality of this feature allows the LNS or tunnel switch to advertise the services it offers to the client, thereby providing end-to-end control of services between the LNS and a PPPoE client.</p>

## DDNS

Use the Dynamic DNS (DDNS) page to specify an Internet service that allows routers with non-static 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, thereby facilitating remote access.

**NOTE** To use DDNS, you must setup an account with a DDNS provider such as 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. You can choose from **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	
Field	Description
DDNS Service	<p>Choose the provider for your DDNS service from the drop-down list. You can choose from DynDNS.org or TZO.com. DDNS service is disabled by default.</p> <p><b>NOTE</b> You must sign up for an account with either one of these providers before you can use this service.</p>
DynDNS.org Settings	
User Name	Enter the user name from DynDNS.org.
Password	Enter the password from DynDNS.org.
Host Name	Enter your host name. For example: name.dyndns.org.
System	Select the DynDNS service that you use. You can choose from 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.
Mail Exchange (Backup MX)	Allows the mail exchange server to be used as a backup. To enable this feature, select <b>Enabled</b> . If you're not sure which setting to use, select <b>Disabled</b> (default).
Wildcard	<p>Allows you to use a wildcard value in the DDNS address. For example, if your DDNS address is myplace.dyndns.org and you enable wildcard, you can also use x.myplace.dyndns.org, where x is the wildcard.</p> <p>To enable wildcards, select <b>Enabled</b>. If you have not subscribed to this service, or are unsure, select <b>Disabled</b> (default).</p>
Internet IP Address	Displays your current IP address.
Status	Displays your DDNS status.
Update	To manually trigger an update, click this 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 host name. 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 this button.

## DMZ

DMZ allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Range Forwarding is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet.

Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

---

**STEP 1** Click **Network Setup** on the tab and then click **DMZ** in the navigation pane. The *DMZ* window opens.

---

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

From this page you can view any existing DMZ's, view the DMZ status, edit a DMZ, and add a new DMZ.

**STEP 2** To allow DMZ hosting, use the default setting, **Enabled**. Otherwise, select **Disabled**.

**STEP 3** Specify the source IP address and the destination IP address or MAC address.

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

---

Field	Description
Status	To use this feature, select Enabled. To disable DMZ hosting, select Disabled.
Source IP Address	If you want any IP address to be the source, select Any IP Address. If you want to specify an IP address or range of IP addresses as the designated source, click the second radio button, and enter the IP address(es) in the fields provided.
Destination	To specify the DMZ host by IP address, select IP Address and complete the IP address in the field provided. If you want to specify the DMZ host by MAC address, select MAC Address and enter the MAC address in the field provided. To retrieve this information, click the DHCP Client Table button.
Show DHCP Client Table	The DHCP Client Table lists computers and other devices that have been assigned IP addresses by the Router. The list can be sorted by Client Name, Interface, IP Address, MAC Address, and Expired Time (how much time is left for the current IP address). To select a DHCP client, click the Select button. To retrieve the most up-to-date information.

## IGMP

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

Field	Description
Support IGMP Version	Select the version you want to use from the drop-down list. You can choose from <b>IGMP v1</b> or <b>IGMP v2</b> . If you are not sure which version to select, keep the default setting, IGMP v2.
IGMP Proxy	To Enable the IGMP Proxy, select <b>Enabled</b> . This allows multicast traffic to pass through the SRP for your multimedia application devices.
Immediate Leave	Select <b>Enabled</b> , if you use IPTV applications and want to allow channel swapping or flipping without lag or delays. Otherwise, keep the default setting, Disabled.

## UPnP

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

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

**STEP 2** To use UPnP, use the default setting, **Enabled**.

**STEP 3** Configure how UPnP can be used with the features described in the **UPnP Settings** table.

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

UPnP Settings	
Field	Description
UPnP	To allow UPnP, keep the default setting, Enabled. Otherwise, select <b>Disabled</b> .
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 <b>Disabled</b> .
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.
Allow Users to Disable Internet Access	When enabled, local clients are allowed to enable or disable the SRP Internet connection through UPnP. The default is Disabled.

## CDP Setting

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 all Cisco equipment. 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. Cisco recommends the default setting, **Per Port**, that enables CDP on LAN ports only.

**STEP 2** Specify the CDP timer values and port participation as defined in the **CDP Settings** table.

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

---

<b>CDP Settings</b>	
<b>Field</b>	<b>Description</b>
CDP	Control whether CDP will run 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. You can enter a value between 5 to 900 seconds. The default is 60 seconds.
CDP Hold Timer	Control whether CDP will run on some, all or none of the SRP Ethernet interfaces. Enter a value between 10 to 255 seconds. The default value is 80 seconds.
Interface List	Check the enable box to select which interfaces will run CDP.

# 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](#)

## Configuring Voice Services

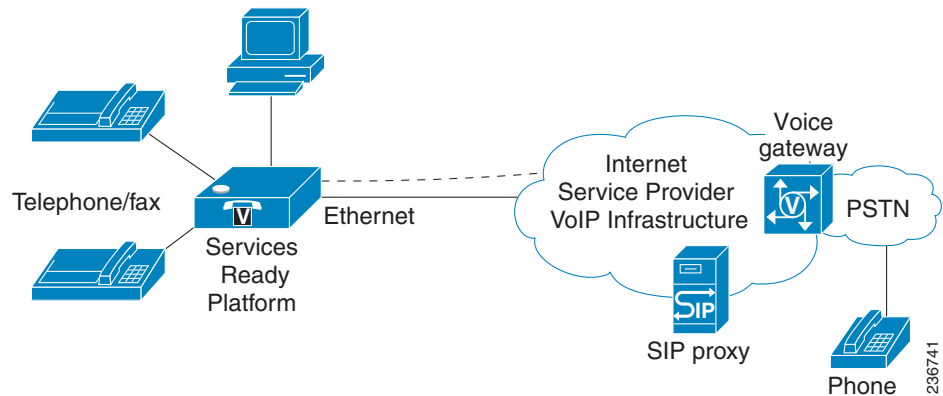
This section describes how to configure your SRP to meet the customer's requirements for voice services. It includes the following topics:

- [Understanding Voice Port Operations](#)
- [Managing Caller ID Services](#)
- [Silence Suppression and Comfort Noise Generation](#)
- [Configuring Dial Plans](#)
- [Secure Call Implementation](#)

### Understanding Voice Port Operations

The SRP520 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 four 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.

**Note:** The SRP520 line port is a passive interface that connects the PSTN line with FXS port 1 during failure conditions. Calls cannot be routed dynamically to this interface under normal operating conditions.



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 186](#).

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 186](#).

### 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 \(1–2\), page 171](#).



## Other SRP Voice Features

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

Feature	Description
Silence Suppression	<p>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.</p> <p>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.</p>

Feature	Description
<p>Modem and Fax Pass-Through</p>	<ul style="list-style-type: none"> <li>▪ Modem pass-through mode can be triggered only by predialing the number set in the Modem Line Toggle Code. See <a href="#">Regional Page, page 151</a>.</li> <li>▪ FAX pass-through mode is triggered by the detection of a CED/CNG tone or an NSE event.</li> <li>▪ Echo canceller is automatically disabled for Modem passthrough mode.</li> <li>▪ Echo canceller is disabled for FAX pass-through if the parameter FAX Disable ECAN (Line 1 or 2 tab) is set to “yes” for that line (in that case FAX pass-through is the same as Modem pass-through).</li> <li>▪ Call waiting and silence suppression is automatically disabled for both FAX and Modem pass-through. In addition, out-of-band DTMF transmission is disabled during modem or fax passthrough.</li> </ul>
<p>Adaptive Jitter Buffer</p>	<p>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.</p> <p>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.</p> <p>Adaptive Jitter Buffer is configured in the Line pages. See <a href="#">Line Pages (1–2), page 171</a>.</p>
<p>Secure Calls</p>	<p>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.</p>

Feature	Description
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 <a href="#">SIP Page, page 135</a> .
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 <a href="#">Line Pages (1–2), page 171</a> .
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 <a href="#">Regional Page, page 151</a> .
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.
Echo Cancellation	<p>Impedance mismatch between the telephone and the IP Telephony gateway phone port can lead to near-end echo.</p> <p>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 <a href="#">Line Pages (1–2), page 171</a>.</p>

Feature	Description
<p>Signaling Hook Flash Event</p>	<p>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-party-call control.</p> <p>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:</p> <ul style="list-style-type: none"> <li>▪ <b>Call Waiting Service:</b> Refers to the call waiting serv parameter in the Line pages)</li> <li>▪ <b>Three Way Conference Service:</b> Refers to the three-way conf serv parameter in the Line pages)</li> <li>▪ <b>Three Way Call Service:</b> Refers to the three-way call serv parameter in the Line pages)</li> </ul> <p>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 <a href="#">Regional Page, page 151</a>.</p>
<p>Configurable Dial Plan with Interdigit Timers</p>	<p>The SRP has three configurable interdigit timers:</p> <ul style="list-style-type: none"> <li>▪ <b>Initial timeout (T)</b>—Signals that the handset is off the hook and that no digit has been pressed yet.</li> <li>▪ <b>Long timeout (L)</b>—Signals the end of a dial string; that is, no more digits are expected.</li> <li>▪ <b>Short timeout (S)</b>—Used between digits; that is after a digit is pressed a short timeout prevents the digit from being recognized a second time.</li> </ul> <p>See <a href="#">Configuring Dial Plans, page 117</a> for more information.</p>

Feature	Description
Polarity Control	<p>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.</p> <p>Polarity Control is configured in the Line pages. See <a href="#">Line Pages (1–2), page 171</a>.</p>
Calling Party Control	<p>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.</p> <p>CPC is configured in the Regional page. See <a href="#">Regional Page, page 151</a>.</p>
Report Generation and Event Logging	<p>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.</p> <p>Report Generation and Event Logging are configured from the System page. See <a href="#">System Page, page 134</a>.</p>
Syslog and Debug Server Records	<p>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.</p> <p>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 <a href="#">System Page, page 134</a>.</p>

Feature	Description
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 <a href="#">Line Pages (1–2), page 171</a> .

## 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, click the **Line** (Line 1-2) to choose 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.

<b>Proxy and Registration</b>		
Proxy:	<input type="text"/>	
Outbound Proxy:	<input type="text"/>	
Use Outbound Proxy:	<input type="button" value="no"/>	Use OB Proxy In Dialog: <input type="button" value="yes"/>
Register:	<input type="button" value="yes"/>	Make Call Without Reg: <input type="button" value="no"/>
Register Expires:	<input type="text" value="3600"/>	Ans Call Without Reg: <input type="button" value="no"/>
Use DNS SRV:	<input type="button" value="no"/>	DNS SRV Auto Prefix: <input type="button" value="no"/>
Proxy Fallback Intvl:	<input type="text" value="3600"/>	Proxy Redundancy Method: <input type="button" value="Normal"/>
Voice Mail Server:	<input type="text"/>	Mailbox Subscribe Expires: <input type="text" value="2147483647"/>
<b>Subscriber Information</b>		
Display Name:	<input type="text"/>	User ID: <input type="text"/>
Password:	<input type="text"/>	Use Auth ID: <input type="button" value="no"/>
Auth ID:	<input type="text"/>	Directory Number: <input type="text"/>
Mini Certificate:	<input type="text"/>	
SRTP Private Key:	<input type="text"/>	

2-45578

**NOTE** 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.

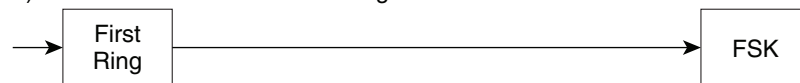
Caller ID Method
<b>Bellcore (N.Amer,China)</b> —CID, CIDCW, and VMWI. FSK sent after first ring (same as ETSI FSK sent after first ring) (no polarity reversal or DTAS). This is the default setting.
<b>DTMF (Finland, Sweden)</b> —CID only. DTMF sent after polarity reversal (and no DTAS) and before first ring
<b>DTMF (Denmark)</b> —CID only. DTMF sent before first ring with no polarity reversal and no DTAS.
<b>ETSI DTMF</b> —CID only. DTMF sent after DTAS (and no polarity reversal) and before first ring.
<b>ETSI DTMF With PR</b> —CID only. DTMF sent after polarity reversal and DTAS and before first ring.
<b>ETSI DTMF After Ring</b> —CID only. DTMF sent after first ring (no polarity reversal or DTAS).
<b>ETSI FSK</b> —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.
<b>ETSI FSK With PR (UK)</b> —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.
<b>DTMF (Denmark) With PR</b> —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 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 Figure 1 (d) and (e)). 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



b) ETSI Onhook Post-Ring DTMF



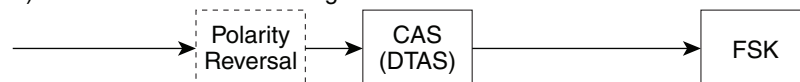
c) ETSI Onhook Pre-Ring FSK/DTMF



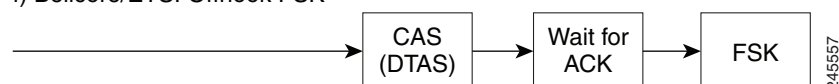
d) Bellcore Onhook FSK w/o Ring



e) ETSI Onhook FSK w/o Ring



f) Bellcore/ETSI Offhook FSK



## 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 Cancellor:** no
  - **Silence suppression:** no
  - **Preferred Codec:** G.711
  - **Use pref. codec only:** yes

If you are using a Cisco media gateway for PSTN termination, disable T.38 (fax relay) and enable fax using modem passthrough. 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
```

---

**NOTE** If a T.38 call cannot be set-up, 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 the Cisco gateway is correctly configured for T.38 with the SPA 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 ATAs.
  - 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](http://www.cisco.com/support).

## Silence Suppression and Comfort Noise Generation

Voice Activity Detection (VAD) with Silence Suppression is a means of increasing the number of calls supported by the network by reducing the required bandwidth for a single call. VAD uses a sophisticated algorithm to distinguish between speech and non-speech signals. Based on 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 suppressing the transmission of the natural silence that occurs in normal two-way connection. The IP bandwidth is therefore 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.

Silence suppression is configured from the Line (1-2) pages. tabs. See [Line Pages \(1–2\), page 171](#).

---

## 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 “|” 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.
x	Enter x to represent any character on the phone keypad.
[sequence]	<p>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.</p> <ul style="list-style-type: none"> <li>▪ Numeric range: For example, you would enter [2-9] to allow the user to press any one digit from 2 through 9.</li> <li>▪ Numeric range with other characters: For example, you would enter [35-8*] to allow the user to press 3, 5, 6, 7, 8, or *.</li> </ul>
. (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.
<dialled:substituted>	<p>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.</p> <p><b>EXAMPLE 1:</b> &lt;8:1650&gt;xxxxxxxx</p> <p>When the user presses 8 followed by a seven digit number, the system automatically replaces the dialed 8 with 1650. If the user dials <b>85550112</b>, the system transmits <b>16505550112</b>.</p> <p><b>EXAMPLE 2:</b> &lt;:1&gt;xxxxxxxxxxx</p> <p>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 <b>972550112</b>, the system transmits <b>1972550112</b>.</p>

Digit Sequence	Function
, (comma)	Enter a comma between digits to play an “outside line” dial tone after a user-entered sequence.  <b>EXAMPLE:</b> 9, 1xxxxxxxxxxx  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.  <b>EXAMPLE:</b> 1900xxxxxxxx!  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, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 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, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 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, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxxx ! | 9, 011xxxxxxx. | 0 | [49]111 )

**9, xxxxxxxx** 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, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxxx ! | 9, 011xxxxxxx. | 0 | [49]11 )

**9, <:1>[2-9]xxxxxxxxxx** 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, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxxx ! | 9, 011xxxxxxx. | 0 | [49]11 )

**8, <:1212>xxxxxxxx** This is 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, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxxx ! | 9, 011xxxxxxx. | 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, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxxx ! | 9, 011xxxxxxx. | 0 | [49]11 )



**9, 1 900 xxxxxxxx !** 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, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxxx | 9, 1 900 xxxxxxxx ! | **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, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxxx | 9, 1 900 xxxxxxxx ! | 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.	<ul style="list-style-type: none"> <li>If the sequence is allowed by the dial plan, the number is accepted and is transmitted according to the dial plan.</li> <li>If the sequence is blocked by the dial plan, the number is rejected.</li> </ul>
A timeout occurs.	<p>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.</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul>
The user presses the # key.	<ul style="list-style-type: none"> <li>If the sequence is complete and is allowed by the dial plan, the number is accepted and is transmitted according to the dial plan.</li> <li>If the sequence is incomplete or is blocked by the dial plan, the number is rejected.</li> </ul>

### 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]xxxxxxxxxx | 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]xxxxxxxxxx | 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.

### 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 125](#).

---

## 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]xxxxxxx | 9,8,1[2-9]xxxxxxxxxxx | 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]xxxxxxx | 9,8,1[2-9]xxxxxxxxxxx | 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, click the Line (Line 1–2) to choose 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 117](#).
  - 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 117](#).

---

- 
- 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 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:

```
9CC9aYU1X51JuU+EBZmi3AmcqE9U1LxEoGwopaGyGOh3VyhKgi6JaVtQZt87PiJINKW8XQj3B9Qq
e3VgYxWCQNa335YcNdsenASeBxuMIEaBCYd111fVEodJZOGwXwfAde0MhcbD0kj7LVlzcS
TYk2TZYTccnZ75TuTjj13qvYs=5nEtOrkCa84/mEw13D9tSvVlyliwQ+u/
Hd+C8u5SNk7hsAUZaA9TqH8Iw0J/
IqSrsf6scsmundY5j7Z5mK5J9uBxSB8t8vamFGD0pF4zhNtbrVvIXKI9kmp4vph1C5jzO9gDfs3M
F+zjYrVUFdM+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>
Sm9lIFNtaXRoAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAxNDA4NTU1MTIzNAAAAAAAAAMDAwMDAwMDEw
MTM000vJakde2vVMF3Rw4pPXL7lAgIagMpbLSAG2+++Y1Sqt198Cp9rP/
xMGFfoPmDKGx6JFtkQ5sxLcuwgxpXpkexVpZKlYlpsb28L4Rhg5qZA+Gqj1hDFCmG6dffZ9Sjhx
ES767G0JIS+N8lQBLr0AuemotknSjjjOy8c+11TCd2t44Mh0vmwNg4fDck2YdmTMBR516xJt4/
uQ/
LJQlni2kwqlm7scDv115k232EvvvVtCK0AYa4eWd6fQOpieSCO9CC9aYU1X51JuU+EBZmi3AmcqE
9U1LxEoGwopaGyGOh3VyhKgi6JaVtQZt87PiJINKW8XQj3B9Qqe3VgYxWCQNa335YcNdsenASeBx
uMIEaBCYd111fVEodJZOGwXwfAde0MhcbD0kj7LVlzcS
TYk2TZYTccnZ75TuTjj13qvYs=
<SRTP Private Key>
b/DWc96X4YQraCnYz15en1CIUhVQQqrvcR6Qd/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 (1–2)**
- **User Pages (1–2)**

---

**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 <b>Administration &gt; Time Setup</b> 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)

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: <ul style="list-style-type: none"> <li>▪ Idle</li> <li>▪ Collecting PSTN Pin</li> <li>▪ Invalid PSTN PIN</li> <li>▪ PSTN Caller Accepted</li> <li>▪ Connected to PSTN</li> </ul>
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	<p>Direction of the call. May take one of the following values:</p> <ul style="list-style-type: none"> <li>▪ PSTN Gateway Call = VoIP-To-PSTN Call</li> <li>▪ VoIP Gateway Call = PSTN-To-VoIP Call</li> <li>▪ PSTN To Line 1 = PSTN call ring through and answered by Line 1</li> <li>▪ Line 1 Forward to PSTN Gateway = VoIP calls Line 1 then forwarded to PSTN GW</li> <li>▪ Line 1 Forward to PSTN Number =VoIP calls Line 1 then forwarded to PSTN number</li> <li>▪ Line 1 To PSTN Gateway</li> <li>▪ Line 1 Fallback To PSTN Gateway</li> </ul>
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 Call 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.

## 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 <b>1234</b> .
IVR User Password	Password for the phone user to manage their line using the built in IVR via their handset. The default is <b>no password</b> .

### 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 <b>Administration &gt; Log</b> 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](#)
- [NSE Dynamic Payload](#)

## 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	<p>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 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.</p> <p>The default is no.</p>
Escape Display Name	<p>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.</p> <p>The default is no.</p>
RFC 2543 Call Hold	<p>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</p> <p>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.</p> <p>The default is yes.</p>
Mark all AVT Packets	<p>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.</p> <p>The default is yes.</p>

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	<p>ACK hang-around time, which can range from 0 to 64 seconds.</p> <p>The default is 32.</p>
SIP Timer J	<p>Non-INVITE response hang-around time, which can range from 0 to 64 seconds.</p> <p>The default is 32.</p>
INVITE Expires	<p>INVITE request Expires header value. If you enter 0, the Expires header is not included in the request.</p> <p>The default is 240. Range: 0–(2<sup>31</sup>-1).</p>
ReINVITE Expires	<p>ReINVITE request Expires header value. If you enter 0, the Expires header is not included in the request.</p> <p>The default is 30. Range: 0–(2<sup>31</sup>-1).</p>
Reg Min Expires	<p>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.</p> <p>The default is 1.</p>
Reg Max Expires	<p>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.</p> <p>The default is 7200.</p>
Reg Retry Intvl	<p>Interval to wait before the SRP retries registration after failing during the last registration.</p> <p>The default is 30.</p>
Reg Retry Long Intvl	<p>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.</p> <p>The default is 1200</p>

## 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	<p>Minimum port number for RTP transmission and reception.</p> <p>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.</p> <p>The default is 16384.</p>
RTP Port Max	<p>Maximum port number for RTP transmission and reception.</p> <p>The default is 16482.</p>

RTP Packet Size	<p>Packet size in seconds, which can range from 0.01 to 0.16.</p> <p>Valid values must be a multiple of 0.01 seconds. The default is 0.030.</p>
Max RTP ICMP Err	<p>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.</p> <p>The default is 0.</p>
RTCP Tx Interval	<p>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 packet 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 &lt;User ID&gt;@&lt;Proxy&gt;, NAME is set to &lt;Display Name&gt; (or Anonymous if user blocks caller ID), and TOOL is set to the Vendor/Hardware-platform-software-version (such as Cisco/srp520 1.0.31(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 &lt;Call Round Trip Delay&gt; value (ms) on the Voice &gt; Info page.</p> <p>The default is 0.</p>
No UDP Checksum	<p>Select yes if you want the SRP to calculate the UDP header checksum for SIP messages. Otherwise, select no.</p> <p>The default is no.</p>

Stats In BYE	<p>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> <p>P-RTP-State: PS=&lt;packets sent&gt;,OS=&lt;octets sent&gt;,PR=&lt;packets received&gt;,OR=&lt;octets received&gt;,PL=&lt;packets lost&gt;,Jl=&lt;jitter in ms&gt;,LA=&lt;delay in ms&gt;,DU=&lt;call duration ins&gt;,EN=&lt;encoder&gt;,DE=&lt;decoder&gt;.</p> <p>The default is yes.</p>
--------------	--

## 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 <b>telephone-event</b> .
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 <b>yes</b> or <b>no</b> from the drop-down menu.  The default is no.
---------------------	---

Handle VIA rport	<p>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 <b>yes</b> or <b>no</b> from the drop-down menu.</p> <p>The default is no.</p>
Insert VIA received	<p>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.</p> <p>The default is no.</p>
Insert VIA rport	<p>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.</p> <p>The default is no.</p>
Substitute VIA Addr	<p>Lets you use NAT-mapped IP:port values in the VIA header. Select yes or no from the drop-down menu.</p> <p>The default is no.</p>
Send Resp To Src Port	<p>Sends responses to the request source port instead of the VIA sent-by port. Select yes or no from the drop-down menu.</p> <p>The default is no.</p>
STUN Enable	<p>Enables the use of STUN to discover NAT mapping. Select yes or no from the drop-down menu.</p> <p>The default is no.</p>
STUN Test Enable	<p>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.</p> <p>The default is no.</p>



STUN Server	IP address or fully-qualified domain name of the STUN server to contact for NAT mapping discovery.
EXT IP	<p>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.</p> <p>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.</p> <p><b>NOTE:</b> 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.</p> <p>The default is 0.0.0.0.</p>
EXT RTP Port Min	<p>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.</p> <p>There is no default value.</p>
NAT Keep Alive Intvl	<p>Interval between NAT-mapping keep alive messages.</p> <p>The default is 15.</p>

## 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	<p>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.</p> <p>Set this parameter to zero to disable periodic resyncing.</p> <p>The default is 3600 seconds.</p>
Resync Error Retry Delay	<p>Resync retry interval (in seconds) applied in case of resync failure.</p> <p>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.</p> <p>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.</p> <p>The default is 3600 seconds.</p>
Forced Resync Delay	<p>Maximum delay (in seconds) the SPA waits before performing a resync.</p> <p>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.</p> <p>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.</p> <p>The default is 14,400 seconds.</p>
Resync From SIP	<p>Enables a resync to be triggered via a SIP NOTIFY message.</p> <p>The default is Yes.</p>
Resync After Upgrade Attempt	<p>Triggers a resync after every firmware upgrade attempt.</p> <p>The default is Yes.</p>

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	<p>Syslog message issued upon successful completion of a resync attempt.</p> <p>The default is \$PN \$MAC – Successful resync \$SCHEME://\$SERVIP:\$PORT\$PATH -- \$ERR.</p>
Log Resync Failure Msg	<p>Syslog message issued after a failed resync attempt.</p> <p>The default is \$PN \$MAC – Resync failed: \$ERR.</p>
Report Rule	<p>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.</p> <p>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.</p> <p>This parameter may optionally contain an encryption key.</p> <p>For example:</p> <p>[ --key \$K ] tftp://ps.callhome.net/\$MA/rep.xml.enc</p> <p>The default is (empty).</p>

## Firmware Upgrade

### *Voice > Provisioning > Firmware Upgrade*

Upgrade Enable	<p>Enables firmware upgrade operations independently of resync actions.</p> <p>The default is Yes.</p>
Upgrade Error Retry Delay	<p>The upgrade retry interval (in seconds) applied in case of 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.</p> <p>The default is 3600 seconds.</p>

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 Regional page.

- **Call Progress Tones**
- **Distinctive Ring Patterns**
- **Distinctive Call Waiting Tone Patterns**
- **Distinctive Ring/CWT Pattern Names**
- **Ring and Call Waiting Tone Spec**
- **Control Timer Values (sec)**
- **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:

$S_i = D_i(\text{on}_{i,1}/\text{off}_{i,1}[\text{on}_{i,2}/\text{off}_{i,2}[\text{on}_{i,3}/\text{off}_{i,3}[\text{on}_{i,4}/\text{off}_{i,4}[\text{on}_{i,5}/\text{off}_{i,5}, \text{on}_{i,6}/\text{off}_{i,6}]]]])$  and is known as a section,  $\text{on}_{i,j}$  and  $\text{off}_{i,j}$  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 specifies 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. May contain up to 127 characters.

Syntax:  $\text{FreqScript};Z_1[:Z_2]$ .

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:  $Z_1 = D_1(\text{on}_{i,1}/\text{off}_{i,1}/f_{i,1}[, \text{on}_{i,2}/\text{off}_{i,2}/f_{i,2} [, \text{on}_{i,3}/\text{off}_{i,3}/f_{i,3} [, \text{on}_{i,4}/\text{off}_{i,4}/f_{i,4} [, \text{on}_{i,5}/\text{off}_{i,5}/f_{i,5} [, \text{on}_{i,6}/\text{off}_{i,6}/f_{i,6}]]]]]]])$ , where  $f_{i,j} = n_1[+n_2]+n_3[+n_4[+n_5[+n_6]]]]]$  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	<p>Prompts the user to enter a call forwarding phone number.</p> <p>The default is 520@-19,620@-19;10(*0/1+2).</p>
Busy Tone	<p>Played when a 486 RSC is received for an outbound call.</p> <p>The default is 480@-19,620@-19;10(.5/5/1+2).</p>
Reorder Tone	<p>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.</p> <p>The default is 480@-19,620@-19;10(.25/.25/1+2).</p>
Off Hook WarningTone	<p>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.</p> <p>The default is 480@10,620@0;10(.125/.125/1+2).</p>
Ring Back Tone	<p>Played during an outbound call when the far end is ringing.</p> <p>The default is 440@-19,480@-19;*(2/4/1+2).</p>
Ring Back 2 Tone	<p>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.</p> <p>The default is 440@-19,480@-19;*(1/1/1+2).</p>
Confirm Tone	<p>Brief tone to notify the user that the last input value has been accepted.</p> <p>The default is 600@-16; 1(.25/.25/1).</p>
SIT1 Tone	<p>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.</p> <p>The default is 985@-16,1428@-16,1777@ 16;20(.380/0/1,.380/0/2,.380/0/3,0/4/0).</p>

SIT2 Tone	<p>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.</p> <p>The default is 914@-16,1371@-16,1777@ 16;20(.274/0/1,,274/0/2,,380/0/3,0/4/0).</p>
SIT3 Tone	<p>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.</p> <p>The default is 914@-16,1371@-16,1777@-16;20(.380/0/1,,380/0/2,,380/0/3,0/4/0).</p>
SIT4 Tone	<p>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.</p> <p>The default is 985@-16,1371@-16,1777@-16;20(.380/0/1,,274/0/2,,380/0/3,0/4/0).</p>
MWI Dial Tone	<p>Played instead of the Dial Tone when there are unheard messages in the caller's mailbox.</p> <p>The default is: 350@-19,440@-19;2(.1/.1/1+2);10(* /0 1+2).</p>
Cfwd Dial Tone	<p>Played when all calls are forwarded.</p> <p>The default is: 350@-19,440@-19;2(.2/.2/1+2);10(* /0/1+2).</p>
Holding Tone	<p>Informs the local caller that the far end has placed the call on hold.</p> <p>The default is 600@-19*(.1/.1/1,,1/.1/1,,1/9.5/1).</p>
Conference Tone	<p>Played to all parties when a three-way conference call is in progress.</p> <p>The default is 350@-19;20(.1/.1/1,,1/9.7/1).</p>
Secure Call Indication Tone	<p>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.</p> <p>The default is 397@-19,507@-19;15(0/2/0,,2/.1/1,,1/2.1/2).</p>

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,.1/9.1).
CWT8 Cadence	Cadence script for distinctive CWT 8. The default is 2.3(.3/2).

### Distinctive Ring/CWT Pattern Names

#### *Voice > Regional > Distinctive Ring/CWT Pattern Names*

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 and Call Waiting Tone Spec

**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 doesn't sound right, or your phone doesn't ring, change your Ring Waveform, Ring Frequency, and Ring Voltage to the following:
  - Ring Waveform: Sinusoid
  - Ring Frequency: 25
  - Ring Voltage: 80Vc

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 <b>60–90 (V)</b> .  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 (sec)

*Voice > Regional > Control Timer Values (sec)*

Hook Flash Timer Min	Minimum on-hook time before off-hook qualifies as hookflash. Less than this the on-hook event is ignored. Range: 0.1–0.4 seconds.  The default is 0.1.
----------------------	---

Hook Flash Timer Max	<p>Maximum on-hook time before off-hook qualifies as hookflash. More than this the on-hook event is treated as onhook (no hook-flash event). Range: 0.4–1.6 seconds.</p> <p>The default is 0.9.</p>
Callee On Hook Delay	<p>Phone must be on-hook for at this time in sec. before the SRP will tear down the current inbound call. It does not apply to outbound calls. Range: 0–255 seconds.</p> <p>The default is 0.</p>
Reorder Delay	<p>Delay after far end hangs up before reorder tone is played. 0 = plays immediately, inf = never plays. Range: 0–255 seconds.</p> <p>The default is 5.</p>
Call Back Expires	<p>Expiration time in seconds of a call back activation. Range: 0–65535 seconds.</p> <p>The default is 1800.</p>
Call Back Retry Intvl	<p>Call back retry interval in seconds. Range: 0–255 seconds.</p> <p>The default is 30.</p>
Call Back Delay	<p>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.</p> <p>The default is 0.5.</p>
VMWI Refresh Intvl	<p>Interval between VMWI refresh to the CPE.</p> <p>The default is 0.</p>
Interdigit Long Timer	<p>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.</p> <p>The default is 10.</p>



Interdigit Short Timer	<p>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.</p> <p>The default is 3.</p>
CPC Delay	<p>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.</p> <p>Without CPC enabled, reorder tone will is played after a configurable delay. If CPC is enabled, dial tone will be played when tip-to-ring voltage is restored. Resolution is 1 second.</p> <p>The default range is 2.</p>
CPC Duration	<p>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.</p> <p>The default is 0 (CPC disabled).</p>

## 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	Call Return Code This 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	<p>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.</p> <p>One or more *code can be configured into this parameter, such as *98, or *97 *98 *123, etc. Max total length is 79 chars. 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.</p> <p>For example, after the user dials *98, the SRP plays a special dial tone called the Prompt Tone while waiting for the user to 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.</p> <p>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.</p>

<p>Feature Dial Services Codes</p>	<p>These codes tell the SRP what to do when the user is listening to the first or second dial tone.</p> <p>One or more *code can be configured into this parameter, such as *72, or *72!*74!*67!*82, etc. Max total length is 79 chars. 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).</p> <p>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.</p> <p>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'. Below are a list of allowed tone parameters (note the use of open quotes surrounding the parameter w/o spaces)</p> <p>'c' = &lt;Cfwd Dial Tone&gt;</p> <p>'d' = &lt;Dial Tone&gt;</p> <p>'m' = &lt;MWI Dial Tone&gt;</p> <p>'o' = &lt;Outside Dial Tone&gt;</p> <p>'p' = &lt;Prompt Dial Tone&gt;</p> <p>'s' = &lt;Second Dial Tone&gt;</p> <p>'x' = No tones are place, x is any digit not used above</p> <p>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.</p>
------------------------------------	---

## 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.
Set Local Time (HH/mm)	Sets the local time (hh stands for hours and mm stands for minutes). Seconds are optional.
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.  <b>NOTE</b> 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 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 available: <ul style="list-style-type: none"> <li>▪ <b>Bellcore (N.Amer,China):</b> CID, CIDCW, and VMWI. FSK sent after first ring (same as ETSI FSK sent after first ring) (no polarity reversal or DTAS).</li> <li>▪ <b>DTMF (Finland, Sweden):</b> CID only. DTMF sent after polarity reversal (and no DTAS) and before first ring.</li> <li>▪ <b>DTMF (Denmark):</b> CID only. DTMF sent before first ring with no polarity reversal and no DTAS.</li> <li>▪ <b>ETSI DTMF:</b> CID only. DTMF sent after DTAS (and no polarity reversal) and before first ring.</li> <li>▪ <b>ETSI DTMF With PR:</b> CID only. DTMF sent after polarity reversal and DTAS and before first ring.</li> <li>▪ <b>ETSI DTMF After Ring:</b> CID only. DTMF sent after first ring (no polarity reversal or DTAS).</li> <li>▪ <b>ETSI FSK: CID, CIDCW, and VMWI.</b> FSK sent after DTAS (but no polarity reversal) and before first ring. Waits for ACK from CPE after DTAS for CIDCW.</li> <li>▪ <b>ETSI FSK With PR (UK):</b> 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.</li> </ul> <p>The default is Bellcore(N.Amer, China).</p>
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 (1–2)

Use the Line pages (Line 1–2) to configure the lines for voice services. These pages include the following sections:

- **Line Enable**
- **Streaming Audio Server (SAS)**
- **NAT Settings**
- **Network Settings**
- **SIP Settings**
- **Call Feature Settings**
- **Proxy and Registration**
- **Outbound Proxy SIP**
- **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 1–2 > Line Enable*

Line Enable	To enable this line for service, select <b>yes</b> . Otherwise, select no.  The default is yes.
-------------	--

## Streaming Audio Server (SAS)

### *Voice > Line 1–2 > 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	<p>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.</p> <p>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.</p> <p>The default value is empty.</p>
----------------------	--

## NAT Settings

### *Voice > Line 1-2 > NAT Settings*

NAT Mapping Enable	<p>To use externally mapped IP addresses and SIP/RTP ports in SIP messages, select yes. Otherwise, select no.</p> <p>The default is no.</p>
NAT Keep Alive Enable	<p>To send the configured NAT keep alive message periodically, select yes. Otherwise, select no.</p> <p>The default is no.</p>

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 1–2 > 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	<p>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: <b>low, medium, high, very high, or extremely high.</b></p> <p>The default is high.</p>
Jitter Buffer Adjustment	<p>Controls how the jitter buffer should be adjusted. Select the appropriate setting: <b>up and down, up only, down only, or disable.</b></p> <p>The default is up and down.</p>

## SIP Settings

### *Voice > Line 1–2 > SIP Settings*

SIP Transport	<p>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: <b>UDP, TCP, TLS.</b></p> <p>The default is UDP.</p>
SIP Port	<p>Port number of the SIP message listening and transmission port.</p> <p>The default is 5060.</p>

SIP 100REL Enable	<p>To enable the support of 100REL SIP extension for reliable transmission of provisional responses (18x) and use of PRACK requests, select <b>yes</b>. Otherwise, select <b>no</b>.</p> <p>The default is no.</p>
EXT SIP Port	<p>The external SIP port number.</p>
Auth Resync-Reboot	<p>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 <b>yes</b>. Otherwise, select <b>no</b>.</p> <p>The default is yes.</p>
SIP Proxy-Require	<p>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.</p>
SIP Remote-Party-ID	<p>To use the Remote-Party-ID header instead of the From header, select <b>yes</b>. Otherwise, select <b>no</b>.</p> <p>The default is yes.</p>
SIP GUID	<p>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.</p> <p>The default is no.</p>



SIP Debug Option	<p>SIP messages are received at or sent from the proxy listen port. This feature controls which SIP messages to log.</p> <p>Choices are as follows:</p> <ul style="list-style-type: none"> <li>▪ <b>none</b>—No logging.</li> <li>▪ <b>1-line</b>—Logs the start-line only for all messages.</li> <li>▪ <b>1-line excl. OPT</b>—Logs the start-line only for all messages except OPTIONS requests/responses.</li> <li>▪ <b>1-line excl. NTFY</b>—Logs the start-line only for all messages except NOTIFY requests/responses.</li> <li>▪ <b>1-line excl. REG</b>—Logs the start-line only for all messages except REGISTER requests/responses.</li> <li>▪ <b>1-line excl. OPTINTFYIREG</b>—Logs the start-line only for all messages except OPTIONS, NOTIFY, and REGISTER requests/responses.</li> <li>▪ <b>full</b>—Logs all SIP messages in full text.</li> <li>▪ <b>full excl. OPT</b>—Logs all SIP messages in full text except OPTIONS requests/responses.</li> <li>▪ <b>full excl. NTFY</b>—Logs all SIP messages in full text except NOTIFY requests/responses.</li> <li>▪ <b>full excl. REG</b>—Logs all SIP messages in full text except REGISTER requests/responses.</li> <li>▪ <b>full excl. OPTINTFYIREG</b>—Logs all SIP messages in full text except for OPTIONS, NOTIFY, and REGISTER requests/responses.</li> </ul> <p>The default is none.</p>
RTP Log Intvl	<p>The interval for the RTP log.</p> <p>The default is 0.</p>

Restrict Source IP	<p>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).</p> <p>The default is no.</p>
Referor Bye Delay	<p>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.</p> <p>The default is 4.</p>
Refer Target Bye Delay	<p>For the Refer Target Bye Delay, enter the appropriate period of time in seconds.</p> <p>The default is 0.</p>
Referee Bye Delay	<p>For the Referee Bye Delay, enter the appropriate period of time in seconds.</p> <p>The default is 0.</p>
Refer-To Target Contact	<p>To contact the refer-to target, select yes. Otherwise, select no.</p> <p>The default is no.</p>
Sticky 183	<p>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.</p> <p>The default is no.</p>

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 <b>yes</b> .  The default is no.

## Call Feature Settings

### *Voice > Line 1–2 > 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 <b>yes</b> . Otherwise, select <b>no</b> .  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 <b>yes</b> or <b>no</b> from the drop-down menu.  The default is yes.

Conference Bridge URL	<p>This feature supports external conference bridging for n-way conference calls (<math>n &gt; 2</math>), instead of mixing audio locally.</p> <p>To use this feature, set this parameter to that of the server's name. For example: conf@myserver.com:12345 or conf (which uses the Proxy value as the domain).</p>
Conference Bridge Ports	<p>Select the maximum number of conference call participants. The range is 3 to 10.</p> <p>The default is 3.</p>

## Proxy and Registration

### *Voice > Line 1-2 > 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 sec 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 <sup>31</sup> – 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	<p>Whether to use DNS SRV lookup for Proxy and Outbound Proxy.</p> <p>The default is no.</p>
DNS SRV Auto Prefix	<p>If enabled, the SRP will automatically prepend the Proxy or Outbound Proxy name with <code>_sip._udp</code> when performing a DNS SRV lookup on that name.</p> <p>The default is no.</p>
Proxy Fallback Intvl	<p>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).</p> <p>The default is 3600.</p>
Proxy Redundancy Method	<p>Select Normal or Based on SRV Port. The SRP creates an internal list of proxies returned in the DNS SRV records.</p> <p>If you select Normal, the list contains proxies ranked by weight and priority.</p> <p>If you select Based on SRV Port, the SRP uses Bormal, the inspects the port number based on the first listed proxy port.</p> <p>The default is Normal.</p>
Voice Mail Server	<p>Enter the URL or IP address of the server.</p>
Mailbox Subscribe Expires	<p>Sets subscription interval for voicemail message waiting indication.</p>

**Subscriber Information***Voice > Line 1–2 > 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 1-2 > 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 <b>yes</b> .
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 1–2 > 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: <b>G711u, G711a, G726-32, or G729a</b> . 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: <b>Unspecified, G711u, G711a, G726-32, or G729a</b> . The default is Unspecified.

Third Preferred Codec	<p>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: <b>Unspecified</b>, <b>G711u</b>, <b>G711a</b>, <b>G726-16</b>, <b>G726-24</b>, <b>G726-32</b>, <b>G726-40</b>, <b>G729a</b>, or <b>G723</b>.</p> <p>The default is Unspecified.</p>
Use Pref Codec Only	<p>To use only the preferred codec for all calls, select <b>yes</b>. (The call fails if the far end does not support this codec.) Otherwise, select <b>no</b>.</p> <p>The default is no.</p>
Silence Supp Enable	<p>To enable silence suppression so that silent audio frames are not transmitted, select <b>yes</b>. Otherwise, select <b>no</b>.</p> <p>The default is no.</p>
Silence Threshold	<p>Select the appropriate setting for the threshold: high, medium, or low.</p> <p>The default is medium.</p>
G729a Enable	<p>To enable the use of the G.729a codec at 8 kbps, select <b>yes</b>. Otherwise, select <b>no</b>.</p> <p>The default is yes.</p>
Echo Canc Enable	<p>To enable the use of the echo canceller, select <b>yes</b>. Otherwise, select <b>no</b>.</p> <p>The default is yes.</p>
Echo Canc Adapt Enable	<p>To enable the echo canceller to adapt, select <b>yes</b>. Otherwise, select <b>no</b>.</p> <p>The default is yes.</p>
Echo Supp Enable	<p>To enable the use of the echo suppressor, select <b>yes</b>. Otherwise, select <b>no</b>.</p> <p>The default is yes.</p>
FAX V21 Detect Enable	<p>To enable detection of V21 fax tones, select <b>yes</b>. Otherwise, select <b>no</b>.</p> <p>The default is yes.</p>

G726-32 Enable	To enable the use of the G.726 codec at 32 kbps, select <b>yes</b> . Otherwise, select <b>no</b> .  The default is yes.
FAX CNG Detect Enable	To enable detection of the fax Calling Tone (CNG), select <b>yes</b> . Otherwise, select <b>no</b> .  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 <b>yes</b> . Otherwise, select <b>no</b> .  The default is yes.
FAX Codec Symmetric	To force the SRP to use a symmetric codec during fax passthrough, select <b>yes</b> . Otherwise, select <b>no</b> .  The default is yes.
DTMF Process AVT	To use the DTMF process AVT feature, select <b>yes</b> . Otherwise, select <b>no</b> .  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: <b>InBand</b> , <b>AVT</b> , <b>INFO</b> , or <b>Auto</b> . 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	<p>DTMF Detection Tx Mode is available for SIP information and AVT. Options are: <b>Strict</b> or <b>Normal</b>. The default is Strict for which the following are true:</p> <ul style="list-style-type: none"> <li>▪ A DTMF digit requires an extra hold time after detection.</li> <li>▪ The DTMF level threshold is raised to -20 dBm.</li> </ul> <p>The minimum and maximum duration thresholds are:</p> <ul style="list-style-type: none"> <li>▪ strict mode for AVT: 70 ms</li> <li>▪ normal mode for AVT: 40 ms</li> <li>▪ strict mode for SIP info: 90 ms</li> <li>▪ normal mode for SIP info: 50 ms</li> </ul>
FAX Process NSE	<p>To use the fax process NSE feature, select <b>yes</b>. Otherwise, select <b>no</b>.</p> <p>The default is yes.</p>
Hook Flash Tx Method	<p>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.</p> <p>The default is None.</p>
FAX Disable ECAN	<p>If enabled, this feature automatically disables the echo canceller when a fax tone is detected. To use this feature, select <b>yes</b>. Otherwise, select <b>no</b>.</p> <p>The default is no.</p>
Release Unused Codec	<p>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 <b>yes</b>. Otherwise, select <b>no</b>.</p> <p>The default is yes.</p>
FAX Enable T38	<p>To enable the use of ITU-T T.38 standard for FAX Relay, select <b>yes</b>. Otherwise select <b>no</b>.</p> <p>The default is yes.</p>

FAX T38 Redundancy	<p>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.</p> <p>The default is 1.</p>
FAX T38 ECM Enable	<p>Select <b>yes</b> to enable T.38 Error Correction Mode. Otherwise select <b>no</b>.</p>
FAX Tone Detect Mode	<p>This parameter has three possible values:</p> <ul style="list-style-type: none"><li>▪ <b>caller or callee:</b> The SRP will detect FAX tone whether it is callee or caller</li><li>▪ <b>caller only:</b> The SRP will detect FAX tone only if it is the caller</li><li>▪ <b>callee only:</b> The SRP will detect FAX tone only if it is the callee</li></ul> <p>The default is caller or callee.</p>

## Dial Plan

The default dial plan script for each line is as follows: (\*xx[3469]110|00|[2-9]xxxxxx|1xxx[2-9]xxxxxx|xxxxxxxxxxxxx.). The syntax for a dial plan expression is described in the table below.

*Voice > Line 1–2 > 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
xxxxxxxxxxxxx.	Everything else (Int'l long distance, FWD, ...)
Dial Plan	<p>Dial plan script for this line.</p> <p>The default is (*xx[3469]110 00 [2-9]xxxxxx 1xxx[2-9]xxxxxxS0 xxxxxxxxxxxxx.)</p> <p>Each parameter is separated by a semi-colon (;).</p> <p>Example 1:</p> <pre>*1xxxxxxxxxx&lt;:@fwdnat.pulver.com:5082;uid=jsmith;pwd=xy z</pre> <p>Example 2:</p> <pre>*1xxxxxxxxxx&lt;:@fwd.pulver.com;nat;uid=jsmith;pwd=xyz</pre> <p>Example 3:</p> <pre>[39]11&lt;:@gw0&gt;</pre>
PSTN Fallback Dial Plan	<p>Dial plan script for routing calls to the FXO port when the IP service is unavailable.</p> <p>The default script is (S0&lt;:@gw0&gt;).</p>

<p>Enable IP Dialing</p>	<p>Enable or disable IP dialing.</p> <p>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.</p> <p>The default is no.</p>
<p>Emergency Number</p>	<p>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.</p> <p>The default is blank.</p>

### FXS Port Polarity Configuration

#### *Voice > Line 1-2 > FXS Port Polarity Configuration*

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



## User Pages (1–2)

Use these pages to configure the user settings. 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 Line 1 or Line 2, 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] or [2] (corresponding to Line 1 or 2) in the configuration profile. It is omitted below for readability.

### Call Forward Settings

*Voice > User 1–2 > 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 1–2 > 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 1–2 > 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 1–2 > 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.

<p>Message Waiting</p>	<p>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.</p> <p>The default is no.</p>
<p>Accept Media Loopback Request</p>	<p>Controls how to handle incoming requests for loopback operation. Choices are: <b>Never</b>, <b>Automatic</b>, and <b>Manual</b>, where:</p> <ul style="list-style-type: none"> <li>▪ <b>never</b>—never accepts loopback calls; reply 486 to the caller</li> <li>▪ <b>automatic</b>—automatically accepts the call without ringing</li> <li>▪ <b>manual</b>—rings the phone first, and the call must be picked up manually before loopback starts.</li> </ul> <p>The default is Automatic.</p>
<p>Media Loopback Mode</p>	<p>The loopback mode to assume locally when making call to request media loopback. Choices are: <b>Source</b> and <b>Mirror</b>. The default is Source.</p> <p><b>NOTE</b> If the SRP answers the call, the mode is determined by the caller.</p>
<p>Media Loopback Type</p>	<p>The loopback type to use when making call to request media loopback operation. Choices are <b>Media</b> and <b>Packet</b>. The default is Media.</p> <p>Note that 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).</p>

## 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 1–2 > 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 1–2 > 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.

# Configuring VPN

This chapter describes how to configure VPN policies and settings for the SRP. It includes the following sections:

- [IKE Policy](#)
- [IPSec Policy](#)
- [GRE Tunnel](#)
- [VPN Passthrough](#)

To access these pages click **VPN** from the Configuration Utility menu bar.

## 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 are used in different VPN policies

---

**STEP 1** Click **VPN > Site to Site IPSec VPN > IKE Policy**. The *IKE Policies* window opens.

From this window you can view the existing IKE policies from the List of IKE polices, edit a policy, view the policy details, and a add 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. You can choose from either **Main** or **Aggressive** mode.

Select Main mode if you want higher security, but with a slower connection. Select Aggressive this mode if you want a faster connection, but with 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	
Field	Description
<b>General</b>	
Policy Name	Enter a unique name for the VPN policy.
Exchange Mode	<p>Choose the exchange mode based on your requirements for security and speed.</p> <ul style="list-style-type: none"> <li>▪ <b>Main:</b> Choose this mode if you want higher security, but with a slower connection. Main Mode relies upon two-way key exchanges between the initiator and the receiver. The key-exchange process slows down the connection but increases security.</li> <li>▪ <b>Aggressive:</b> Choose this mode if you want a faster connection, but with 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.</li> </ul>
<b>IKE SA Parameters</b>	
Encryption Algorithm	Choose an encryption mode. Select from <b>DES</b> , <b>3DES</b> , <b>AES128</b> , <b>AES192</b> , and <b>AES256</b> .
Authentication Algorithm	Choose an authentication algorithm for the IKA SA. Select from <b>MD5</b> and <b>SHA1</b> .
Pre Shared Key	Enter an alpha-numeric key to be shared with the IKE peer.
Diffie-Hellman (DH) Group	Choose a DH group to set the strength of the algorithm in bits. Select from <b>Group 1 (768 bits)</b> and <b>Group 2 (1024bits)</b> .

IKE Policy Settings	
Field	Description
Enable Dead Peer (DPD) Detection	To enable DPD, select <b>Enable</b> . The default is disabled. <b>NOTE</b> DPD is not required for an IKE rule, but if enabled, helps to 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 (DPD).
Extended Authentication	
XAUTH Client Enable	Enable if the VPN peer requires Extended Authentication credentials. The default setting is disabled.
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, which 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 list.

**STEP 2** To add an IPSec policy, click **Add Entry**. The *IPSec Policy* window opens.

**STEP 3** To enable the new policy, select **Enable**.

**STEP 4** Choose a policy identification number 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. You can select from **Auto** or **Manual**.
- STEP 7** Enter the IPSec Policy settings as defined in the **IPSec Policy Settings** table.
- STEP 8** Click **Submit** to save your settings.

The VPN policy appears in the List of IKE policies on the IKE Policy Add Entry page.

<b>IPSec Policy Settings</b>	
<b>General Settings</b>	
Policy Name	Enter a unique name for the VPN Policy.
Policy Type	<p>Choose the policy type. Select from <b>Auto Policy</b> or <b>Manual</b> Policy.</p> <p>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 <b>Site to Site IPSec VPN &gt; IKE Policy</b> page The Manual Policy does not use IKE, which makes this policy more simple, but less secure.</p>
Remote Endpoint	<p>Choose how you want to identify the remote gateway for this site-to-site VPN tunnel.</p> <p>Select <b>IP Address</b> to enter an IP address, select <b>FQDN</b> to enter a Fully Qualified Domain Name, or select <b>Any</b> (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.</p>
Encryption Algorithm	Choose the encryption algorithm. Select from <b>DES</b> (8 characters), <b>3DES</b> (24 characters), <b>AES-128</b> (16 characters) <b>AES192</b> (24 characters) and <b>AES256</b> (32 characters).
Integrity Algorithm	Choose an integrity algorithm. Select from <b>MD5</b> (16 characters) or <b>SHA-1</b> (20 characters).
<b>Auto Policy Parameters (options only appear if Auto Policy is selected)</b>	

<b>IPSec Policy Settings</b>	
PFS	Select <b>Enable</b> 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 (130 minutes).
<b>Manual Policy Parameters (options only appear if Manual Policy is selected)</b>	
SPI Incoming	Enter a hexadecimal value, for the incoming Security Parameters Index between 0x100 and 0xffffffff.
SPI Outgoing	Enter a hexadecimal value, for the outgoing Security Parameters Index between 0x100 and 0xffffffff.
Encryption Algorithm Key	Enter a hexadecimal value for the encryption algorithm key. The length depends on the Encryption Algorithm that you selected. For example, the key length for 3DES is 48 hexadecimal digits.
Integrity Algorithm Key	Enter a hexadecimal value for the integrity algorithm key. The length of the key depends on the Integrity Algorithm selected. For example, MD5 is 32 hexadecimal digits and SHA-1 is 40 hexadecimal digits.
<b>Local Traffic Selection</b>	
Local IP/IP Address/Subnet Mask	Determine which local hosts will be allowed to use the VPN. Select either a single IP Address, or a subnet (IP Address and Subnet Mask).
<b>Remote Traffic Selection</b>	
Remote IP/IP Address/Subnet Mask	Traffic from permitted local hosts to the remote IP address or subnet will be routed via the VPN tunnel. Select either a <b>single IP Address</b> , or a <b>subnet</b> (IP Address and Subnet Mask).
Select IKE Policy	Choose an IKE Policy to associate with this IPSec Policy. To view all the IKE policies, Click <b>View IKE Table</b> .

## GRE Tunnel

Use the GRE Tunnel page to configure Generic Routing Encapsulation (GRE). GRE is a tunneling protocol developed by Cisco that can encapsulate a wide variety of 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 > GRE Tunnel** in the navigation pane. 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 list.
- STEP 2** To add a GRE tunnel, click **Add Entry**. The window for the new GRE tunnel appears.
- STEP 3** Choose an identification name for the tunnel 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 from the drop-down lists. If you choose a key value, enter its value in the Key Value field. You can enter a value from 0–4294967295.
- STEP 6** Choose the WAN interface through which the tunnel should be connected. For example: WAN1 or WAN2. The System Default Route is the default setting.
- 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	
Field	Description
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.

GRE Tunnel Settings	
Field	Description
Enable	Check the box to enable the tunnel, or uncheck the box to disable it.
Checksum	Choose <b>Input</b> , <b>Output</b> , <b>Both</b> , or <b>None</b> . The default is <b>None</b> .  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 <b>None</b> , <b>Both</b> , <b>Input</b> , or <b>Output</b> . The default is <b>None</b> .  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 <b>None</b> , <b>Both</b> , <b>Input</b> and <b>Output</b> value. The default is <b>None</b> .  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 that is 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 via the tunnel.
Modify Remote IP Address/Subnet Mask	To define a host or network that is reachable via the tunnel, enter the address and subnet mask, then click <b>Add</b> . To remove an address, select it in the Remote IP Address list and click <b>Delete</b> .

## 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	
Field	Description
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 IPsec Passthrough, select <b>Disabled</b> .
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 PPTP Passthrough, select <b>Disabled</b> .
L2TP Passthrough	Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. L2TP Passthrough is enabled by default. To disable L2TP Passthrough, select <b>Disabled</b> .

# Administration Settings

This chapter describes the Administration settings for the Services Ready Platforms. It includes the following sections:

- **Web Access Management**
- **Remote Management**
- **Time Setup**
- **User List**
- **User Privilege Control**
- **Logging**
- **Factory Defaults**
- **Firmware Upgrade**
- **Backup & Restore**
- **Reboot**

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** Configure the Remote Access settings as defined in the **Web Access Management Settings** table.

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

Web Access Management Settings	
Field	Description
<b>Web Access</b>	
Web Utility Access	Select <b>HTTP</b> and/or <b>HTTPS</b> . For secure Internet access, select <b>HTTPS</b> .  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 administrator to access the web utility from a local wireless client.
<b>Remote Access</b>	
Remote Management	Allows you to manage your SRP from a remote location through the Internet.
Web Utility Access	Select <b>HTTP</b> or <b>HTTPS</b> . For secure Internet access, select <b>HTTPS</b> .  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.  <b>NOTE</b> 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 <b>Any IP Address</b> . 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 Management

Use the Remote Management pages to configure settings for the following:

- **TR069**
- **SNMP**
- **Local TFTP**

To access these pages click **Administration > Remote Management** from the Configuration Utility.

### TR069

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** Click **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.

Click **Submit** to save your settings.

TR-069 Settings	
Field	Description
Status	Select <b>Enabled</b> to allow auto-configuration of your router from a central server. The default is Disabled.



TR-069 Settings	
Field	Description
ACS URL	Enter the ACS URL provided by your service provider. The ACS URL uses the following format: Protocol://host:port/path <ul style="list-style-type: none"> <li>▪ Protocol can be either http or https.</li> <li>▪ Host can be a fully qualified domain name, or IP address.</li> <li>▪ Port is optional.</li> <li>▪ Path is defined by the ACS.</li> </ul>
ACS Username	The username for ACS. The default username is OUI-Serial Number. This username must match the ACS server username.
ACS Password	The password for ACS. This password must match the ACS server username.
Connection Request URL	This field is automatically populated. The format is http://xxx.xxx.xxx.xxx:port. The x's represent the WAN IP address of the SRP.
Connection Request Username	This username must match the ACS server username.
Connection Request Password	This password must match the ACS server username.
Periodic Inform Interval	Specify the interval (in seconds) at which the SRP will initiate connections to the ACS. The default value is 86400 seconds (24 hours).
Periodic Inform Enable	Select <b>Enabled</b> to allow the router to periodically initiate connections to the ACS. Otherwise, select <b>Disabled</b> .
Request Download	Click <b>Apply</b> if you want to immediately initiate a connection to the ACS. The ACS calls the Download RPC when it receives the request.

## SNMP

SNMP is a network monitoring and management protocol that lets you monitor and manage your network from an SNMP manager. SNMP provides allows you to monitor and control network devices, and manage configurations, statistics collection, performance, and security. The SRP supports SNMPv2.

- 
- STEP 1** Click **Administration > Remote Management > SNMP**. The *SNMP* window opens.
- STEP 2** To enable SNMP, click **Enabled**.
- STEP 3** Select a trusted IP setting. You can select from **Any**, **Address**, or **Netmask**. Any is not recommended.
- STEP 4** Enter the Get and Set community passwords.
- The Get Community password allows read-only access to the Gateway's SNMP information. The Set Community password allows both read and write access.
- STEP 5** Click **Submit** to save your settings.
- 

SNMP Settings	
Field	Description
Enable/Disable	To enable SNMP identification, click <b>Enabled</b> . The default is Disabled.
Trusted IP	Choose <b>Any</b> to allow access from any IP address (not recommended), or enter the IP address and subnet mask of a single SNMP manager or trap agent that can access the SRP through SNMP.
Get Community	Enter the password that allows read-only access to the Gateway's SNMP information.
Set Community	Enter the password that allows read/write access to the Gateway's SNMP information.

## Local TFTP

Use the Local TFTP page to enable the SRP to be a TFTP server. When you enable TFTP, you can download files to the SRP remotely and then use it as a local TFTP server to serve files to hosts on the LAN such as IP phones.

- STEP 1** Click **Administration > Remote Management > Local TFTP**. The *Local TFTP Control* window opens.
- STEP 2** To enable TFTP, select **Enabled**.
- STEP 3** Click **Submit** to save your settings.
- STEP 4** Enter the Remote File Settings as defined in the **Local TFTP Settings** table.

Local TFTP Settings	
Field	Description
TFTP	Select <b>Enabled</b> to enable TFTP. The default is disabled.
Get Remote File Settings	
Interface	The interface used to get the remote file.
URL	Enter the URL where the remote file resides. For example: http://www.yoursite.com:port/path/filename ftp://username:password@yoursite:port/path/filename.
File	Enter the name of the remote file.
Save As	Enter the filename for the file you are saving.
User Name	Enter a user name to access the remote file
User Password	Enter a password to access the remote file.
Timeout	Specify the session timeout value (in seconds). This is the maximum time allowed for a connection session.  The connection timeout for HTTP and FTP sessions is 3 seconds. The connection timeout for TFTP is 1 second. For HTTP and FTP, a TCP reset response message will terminate a session.

Local TFTP Settings	
Field	Description
Retry	Specify the number of sessions that will retry if a transient problem occurs in a session
Status	The 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 system time manually or configure it by using the Network Time Protocol (NTP) server.

- STEP 1** Click **Administration > Time Setup**. The *Time Setup* window opens.
- STEP 2** Specify the settings for your time zone. Time zone is usually referred to as the local time.
- STEP 3** To setup the system clock manually, select **User Manual** and enter the date and time zones. Enter the date format as "Year/Month/Day" and the time format as: "Hour:Min:Sec."
- STEP 4** To automatically set the time, configure the time zone settings as defined in the **Time Setup Settings** table.
- STEP 5** Click **Submit** to save your settings.

Time Setup Settings	
Field	Description
User Manual	To setup the system clock manually, select <b>User Manual</b> and enter the date and time zones. Enter the date format as "Year/Month/Day" and the time format as: "Hour:Min:Sec."

Time Setup Settings	
<b>Time Zone</b>	
Regions	Enter your regions time zone form the drop-down list. For example: (GMT-8:00) Pacific Time (USA & Canada).
Adjust Clock for Daylight Saving Changes	Select this option for the SRP to automatically adjust for daylight savings time.
Time Server Address	To use the SRP's default Network Time Protocol (NTP) server, select <b>Auto</b> from the drop-down list. This is the default. If you want to specify the NTP server, select <b>Manual</b> , and enter the URL or IP address of the NTP server you want to use.
Resync Timer	Enter the Resync timer interval value (in seconds). This timer controls how often the SRP resyncs with the NTP server. The default setting is 3600 seconds.

## Setup Wizard

The Setup Wizard guides you through the basic steps required to configure your SRP. To start the Setup Wizard, click **Administration** on the tab and then click **Setup Wizard** in the navigation pane. The Setup Wizard appears. Follow the instructions on the Setup Wizard to continue with the installation.

## User List

Use the User List page to manage the users who have access to the Configuration Utility.

There are two default accounts, **admin** and **cisco**. The admin account has administrator-level access. The cisco account has guest-level access.

**STEP 1** Click **Administration > 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** Enter a new username.

**NOTE** The admin and cisco default usernames cannot be changed.

**STEP 4** Enter the old password (only applies to the Admin account). You will be asked for your old password when you change the password.

**STEP 5** 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**.

**NOTE** You will also be asked for your new password when you access the Configuration Utility. For security purposes, Cisco strongly recommends changing the password.

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

---

## User Privilege Control

The Privilege Control page allows the Administrator to adjust the privileges assigned to the user.

**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 you to view and configure the Web page.
- **Read Only:** allows you to view the Web page.
- **Hidden:** hides the link to the Web page.

**STEP 3** Click **Apply** to save your setting.

---

## Logging

The SRP allows you to record incoming, outgoing, and DHCP lists for various events that occur on your network. The Incoming Log displays a temporary list of the source IP addresses and destination port numbers for the incoming Internet traffic. The Outgoing Log displays a temporary list of the local IP addresses, destination URLs/IP addresses, and service/port numbers for the outgoing Internet traffic.

- STEP 1** Click **Administration > Log**. The *Log* window opens.
- STEP 2** Click **Enabled** to enable logging.
- STEP 3** Choose the log type from the Log List area.
- STEP 4** Click **Apply** to save your settings.

### Logging Settings

Field	Description
Status	To access activity logs, select Enabled. With logging enabled, you can view temporary logs. Click Disabled to disable this function.
Log List	The log type. To specify the log type, select Incoming Log, Outgoing Log, or DHCP Client 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.

- STEP 1** Click **Administration > Factory Defaults**. The *Factory Defaults* window opens.
- STEP 2** To restore the SRP to its factory defaults, select **Yes**. Any custom data (SRP) settings you have saved will be lost when the default settings are restored.

**STEP 3** To restore the voice settings to the factory defaults, select **Yes**. Any custom voice settings you have saved will be lost when the default settings are restored

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

---

## Firmware Upgrade

Use the Firmware Upgrade to upgrade the firmware on the SRP. 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 the firmware, download the firmware upgrade file for the SRP at: [www.cisco.com/go/srp500](http://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 **Browse** and select the location of the 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:

- **Backup Configuration**
- **Restore Configuration**

To access these pages, click **Administration > Backup & Restore** from the Configuration Utility.



---

## Backup Configuration

Use the Backup Configuration page to back up the SRP configuration settings to a file. You can then 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

Use the Restore Configuration page to restore the SRP configuration settings from a previous backup. Verify that you backed up the configuration settings before you restore the configuration.

- 
- STEP 1** Click **Administration > Backup & Restore > Restore Configuration**. The *Restore Configuration* window opens.
  - STEP 2** Click **Browse**, locate the backup file and then click **Restore**.
- 

## Reboot

Use the Reboot page to power cycle 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.
-

## 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**—MIPS, Loads and Uptime.
- **Memory**—Shows the memory's Total size(%), Free size(%), Used size(%), Buffer size(%), Cached size(%), active size and inactive size(%)

## Switch Setting

On DSL models SRP526W and SRP527W, Ethernet port 4 can be configured as a WAN port. You can also set the “jumbo mode” packet size on this screen.

**NOTE** When Ethernet port 4 is configured as a WAN port, the DSL port becomes inactive. When the DSL port is active, the Ethernet port 4 operates only as a LAN port.

**STEP 1** Click **Administration > Switch Setting**.

The *Switch Setting* window opens.

**STEP 2** Select **Disable** to configure Ethernet port 4 as a WAN port. Select **Enable** to enable the DSL port.

**STEP 3** Choose a Jumbo packet size.

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

### Switch Settings

Field	Description
DSL Interface	Enable or disable the DSL port. When disabled, the LAN port 4 can be used as an Ethernet WAN port.

---

**Switch Settings**

Field	Description
Jumbo Mode	The size of the jumbo packet. Choices are 1522 or 2048 bytes.

# Using Services Ready Platform Diagnostics

This chapter describes how to use diagnostic features of the Services Ready Platforms.

- **Ping Test**
- **Traceroute Test**
- **Detect Active LAN Clients**

To access these pages click *the **Diagnostics Tab*** 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.

- 
- STEP 1** Click **Diagnostics > Ping Test**. The *Ping Test* window opens.
  - STEP 2** Enter the IP address or URL address 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 **Start to Ping** to start the test. After the test is complete, the test results appear on the page.
  - STEP 6** Click **Close** to close the test results and display the form.
-

---

## Traceroute Test

Use the Traceroute page to view the route between the SRP and a destination.

- 
- STEP 1** Click **Diagnostics > Traceroute Test**. The *Traceroute Test* window opens.
  - STEP 2** Enter the IP or URL address to run the trace route on.
  - STEP 3** Click **Start to Traceroute** to start the test. The results appear on the page and are refreshed every 5 seconds.
  - STEP 4** Click **Close** to close the results and display the form.
- 

## Detect Active LAN Clients

Use the Detect Active LAN Clients page to perform a search on the active LAN clients on your SRP.

- 
- STEP 1** Click **Diagnostics > Detect Active LAN Client(s)**. The *Detect Active LAN Client(s)* window opens.
  - STEP 2** Choose the LAN interface you want to detect from the down list. For example: VLAN1.
  - STEP 3** Choose how long you want to perform this search (5, 10, or 15 seconds).
  - STEP 4** Click **Start to Search** to start the test. A new window opens and displays the test results.
-

## Viewing the Services Ready Platforms Status

This chapter describes how to view the status of Services Ready Platforms.

- **Router Settings**
- **Firewall Status**
- **Interface Information**
- **Wireless Network Status**
- **Wireless Client Information**
- **Mobile Network Status**
- **DHCP Server Information**
- **QoS Status**
- **Routing Table**
- **ARP Table**
- **RIP Status**
- **IGMP Status**
- **VPN Status**
- **CDP Neighbor Information**

To access these pages click *the **Status*** from the Configuration Utility menu bar.

## Router Settings

Use the Router page to view information about the SRP and its current settings.

### *Status > Router*

Field	Description
Model	Product name and features.
Hardware Version	Hardware version number.
Boot Version	Boot firmware version number.
Firmware Version	Current 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 is set on the SRP.
WAN	The WAN interface type and level.
LAN	The LAN interface and level.
Wireless	Number of Wireless SSIDs that are enabled.

## Firewall Status

Use the Firewall Status page to view the SRP firewall information.

### *Status > Firewall*

Firewall Status	
Field	Description
<b>Internet Access Policy</b>	
No	Number of the Internet Access Policy list.
Policy Name	Numeric identifier of the Internet Access Policy.
Status	Shows the 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.
<b>Port Forwarding</b>	
Type	Indicates single port or port range forwarding.
Protocol	Port being forwarded to.
Port	User specified port to forward.
Host	LAN host IP address to forward to.
Packets	Number of packets that were forwarded.
Traffic (bytes)	Traffic volume that was forwarded, in bytes.
<b>Statistics</b>	General traffic measurements through the firewall.



Firewall Status	
Field	Description
Name	Name associated with firewall packet processing. <ul style="list-style-type: none"><li>▪ <b>INPUT:</b> Traffic destined for the SRP.</li><li>▪ <b>OUTPUT:</b> Traffic originating from the SRP.</li><li>▪ <b>FORWARD:</b> Traffic passed between the public/external and private/internal networks.</li></ul>
Accept PKT	The number of packets accepted by this firewall path.
Accept Volume (bytes)	The volume of traffic, in bytes, processed by this firewall path.
Drop PKT	The number of packets filtered/blocked by this firewall path.
Drop Volume (bytes)	The volume of traffic, in bytes, filtered/blocked by this firewall path.

## Interface Information

Use the Interface Information page to view information for the various interfaces.

### *Status > Interface*

Interface Information	
Field	Description
<b>Interface List</b>	
Interface	<p>Lists all currently configured LAN and WAN layer three (IP) interfaces. An Ethernet WAN interface is shown as “WAN” and an ADSL WAN interface is shown as “PVC.”</p> <p>Interface numbering is derived as follows:</p> <ul style="list-style-type: none"> <li>▪ <b>Primary Interfaces:</b> Numbering follows physical port labelling (i.e. WAN1 and WAN2).</li> <li>▪ <b>Ethernet WAN Sub-interfaces:</b> Numbering reflects configured VLAN index.</li> <li>▪ <b>ADSL PVCs:</b> Numbered serially from 0 to 3.</li> <li>▪ <b>VLAN Interfaces:</b> Numbering reflects the configured VLAN index.</li> </ul>
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.
<b>Port List</b>	
Interface	Lists all currently configured LAN and WAN layer two (Ethernet, WiFi SSID, DSL PVC) interfaces.
TX (pkts)	Number of packets transmitted from this port.
RX (pkts)	Number of packets received by this port.
Status	Port connectivity status.

Interface Information	
Field	Description
Clear TX & RX	Click this button to reset to 0 the count of TX and RX packets.

## Wireless Network Status

Use the Wireless Network page to view information about your wireless networks.

*Status > Wireless*

Wireless Network Status	
Field	Description
Network Mode	Operating mode configured for the embedded wireless Access Point. See <a href="#">Setting up the Wireless LAN, page 53</a> for more information.
Radio Band	Channel bandwidth in use by the wireless network.
Channel	Wireless channel currently in use.
Wireless List	<p>Current SSID configuration.</p> <p>Columns in the Wireless List include:</p> <ul style="list-style-type: none"> <li>▪ <b>SSID Name:</b> Configured SSID name.</li> <li>▪ <b>Status:</b> SSID enabled or disabled.</li> <li>▪ <b>Broadcast:</b> SSID broadcast enabled or disabled.</li> <li>▪ <b>Security:</b> Current security settings.</li> <li>▪ <b>WPS:</b> Indicates whether WPS is enabled for this SSID.</li> </ul>

## Wireless Client Information

Use the Wireless Client Information page to view information for the wireless clients.

**Status > Wireless Client Information**

Wireless Client Information	
Field	Description
MAC Address	Client MAC address.
Tx-Rate	Current transmission data rate of the client.
Rx-Rate	Current receive data rate of the client.
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 will go into power save if no activity occurs on the link.

## Mobile Network Status

Use the Mobile Network Status page to view information for the Broadband USB modem installed in the SRP.

**NOTE** This page will differ depending on the type of USB modem that you installed

**Status > Mobile Network**

USB UMTS Card Settings	
Field	Description
IP Address	IP address assigned to the USB modem.
Connection Up Time	Duration of current connection session.
Current Session Usage	Receive and Transmit traffic volume.

USB UMTS Card Settings	
Field	Description
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	IMSI number of this USB modem.
Service Type	USB modem service type.
Signal Strength	Signal strength.
Card Status	The status of the card: Connecting, Connected, Disconnecting, Disconnected or Card is not activated. If no card is attached, the status page states that the SRP is "Unable to Detect USB Mobile Modem".

USB CDMA2000 EVDO Card Settings	
Field	Description
IP Address	IP address assigned to the USB modem.
Connection Up Time	Duration of 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.

USB CDMA2000 EVDO Card Settings	
Field	Description
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	The status of the card: Connecting, Connected, Disconnecting, Disconnected or Card is not activated. If no card is attached, the status page states that the SRP is "Unable to Detect USB Mobile Modem".

## DHCP Server Information

Use the DHCP Server status page to view DHCP Server lease information by rule.

**Status > DHCP Server Information**

DHCP Server Status	
Field	Description
Client Name	Host name of 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 QoS Status page to view traffic queuing statistics. The SRP supports 5 queues: One strict queue and four weighted round robin queues.

### *Status > QoS*

QoS Status	
Field	Description
Queue Name	Lists the five queues used by the SRP.
Config Rate	The nominal amount of traffic that each queue can handle under balanced and loaded conditions. Note that bandwidth not used by a queue may be used by any other, implying that the configured queuing bandwidth may be exceeded.
Allow Maximum Rate	The 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)	The number of bytes sent from this queue.
Send (pkts)	The number of packets sent from this queue.
Drop	The number of packets dropped when total traffic rate exceeds Allow Maximum rate.
Overlimits	The 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 Routing Table Status page to view routing information.

### *Status > Routing Table*

Routing Table Status	
Field	Description
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 Table

Use the ARP Table Status page to view information for all ARP (Address Resolution Protocol) entries.

### *Status > ARP Table*

ARP Table Status	
Field	Description
IP Address	IP address of the device.
HW Type	Hardware type of the device.
Flags	Flag type of the device.
HW Address	MAC address of the device.
Mask	Mask of the device.



ARP Table Status	
Field	Description
Device	Device interface type.

## RIP Status

Use the RIP Status page to view information for all (RIP) Routing Information Protocol activity. To access this page, click **Status > RIP** from the Configuration Utility.

This page dump 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 IGMP Status page to view IGMP information.

**Status > IGMP**

Field	Description
IP Address	IP address of the device.
Port	Port of the device.

## VPN Status

Use the VPN Status page to view VPN status information.

**Status > VPN Status**

VPN Status	
Field	Description
Tunnel Name	The name of the VPN tunnel.
Remote Policy	The remote network policy.
Local Policy	The local network policy.
IKE Algorithm	The final result of IKE algorithm after ISAKMP. Only applies to the "AUTO" mode.
Upset Algorithm	The IPsec algorithm this tunnel is currently using.
TX Bytes	The number of transmitted bytes of this tunnel.
RX Bytes	The number of received bytes of this tunnel.
Connect Status	Only applies to the "AUTO" mode.

## CDP Neighbor Information

Use the CDP Neighbor Information page to view CDP Neighbor information from the Configuration Utility.

**NOTE** To view additional status information, click an item in the Neighbor information list. The CDP Details table displays information about the selected device.

*Status > CDP Neighbor Information*

CDP Neighbor Information	
Field	Description
Device ID	The device ID of the neighbor.
Local Interface	The local SRP name.
Hold Time	The hold time before which CDP will throw away packets.
Capability	The class of the neighbor.
Platform	The neighbor's hardware system.
Port ID	The port number of the neighbor.
IP Address	The IP address of the neighbor.

## Specifications

This appendix lists the specifications for the SRP520 Models.

<b>Feature</b>	<b>SRP521W</b>
WAN	Fast Ethernet
LAN	4 Fast Ethernet Ports
Wireless	802.11b/g/n
Operating Temperature	0° C to 40° C
Storage Temperature	-20° C to 70° C
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing
Voltage Range	100-240V 50/60Hz AC
Dimensions	(W x D x H): 170mm (6.69 inches) x 170mm (6.69 inches) x 42mm (1.65 inches)
Weight	400g

<b>Feature</b>	<b>SRP526W</b>
WAN	ADSL2+ Annex B
LAN	4 Fast Ethernet Ports
Wireless	802.11b/g/n
Operating Temperature	0° C to 40° C
Storage Temperature	-20° C to 70° C

Feature	SRP526W
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing
Voltage Range	100-240V 50/60Hz AC
Dimensions	(W x D x H): 170mm (6.69 inches) x 170mm (6.69 inches) x 42mm (1.65 inches)
Weight	440g

Feature	SRP 527W
WAN	ADSL2+ Annex A
LAN	4 Fast Ethernet Ports
Wireless	802.11b/g/n
Operating Temperature	0° C to 40° C
Storage Temperature	-20° C to 70° C
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing
Voltage Range	100-240V 50/60Hz AC
Dimensions	(W x D x H): 170mm (6.69 inches) x 170mm (6.69 inches) x 42mm (1.65 inches)
Weight	440g

## Where to Go From Here

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of the Services Ready Platforms.

### Product Resources

Support	
Cisco Small Business Support Community	<a href="http://www.cisco.com/go/smallbizsupport">www.cisco.com/go/smallbizsupport</a> For information about the SRP, click Small Business Routers from the Community page.
Online Technical Support and Documentation (Login Required)	<a href="http://www.cisco.com/support">www.cisco.com/support</a>
Cisco Small Business Support and Resources	<a href="http://www.cisco.com/go/smallbizhelp">www.cisco.com/go/smallbizhelp</a>
Phone Support Contacts	<a href="http://www.cisco.com/go/sbsc">www.cisco.com/go/sbsc</a>
Software	
Software Downloads (Login Required)	<a href="http://www.cisco.com/go/srp500">www.cisco.com/go/srp500</a> Click the Download Software link.
Open Source Documentation	<a href="http://www.cisco.com/en/US/products/ps10500/prod_release_notes_list.html">www.cisco.com/en/US/products/ps10500/prod_release_notes_list.html</a>
Product Documentation	
Cisco Services Ready Platform 500 Series for Small Business	<a href="http://www.cisco.com/go/srp500">www.cisco.com/go/srp500</a>
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	<a href="http://www.cisco.com/web/partners/sell/smb">www.cisco.com/web/partners/sell/smb</a>
Cisco Small Business Home	<a href="http://www.cisco.com/smb">www.cisco.com/smb</a>
Marketplace	<a href="http://www.cisco.com/go/marketplace">www.cisco.com/go/marketplace</a>