SP200XV2 User's Manual

Version 3.2.x

SignalSys, Inc.
www.SignalSys.com

Index

SECTION I. Introduction

1.1 SP200X Production Introduction

SP200X VoIP Media-Router provides the perfect solution for broadband Internet sharing and Voice over IP. It allows multiple PCs to share one high-speed Broadband (Cable/DSL) Internet connection. It also provides one analog telephone port, which allows the user to make calls on the Internet or regular telephone line around the world.

The built-in NAT technology acts as a firewall and protects your internal network. The VPN (Virtual Private Network) pass-through protects your data when it travels on the Internet. The built-in DHCP server dynamically assigns the IP address for your LAN (local area network).

It is easy to make phone calls using SP200X. You just need to plug the standard telephone into the telephone port of SP200X. You need no sound cards, modems, speakers and microphones. None of your PCs even have to be turned on to make and receive calls.

1.2 Safety Precaution

Read these Safety Precautions carefully before you install the SP200X

- Read the User Manual before using the SP200X
- Keep your User Manual in a safe place
- Pay attention to all remarks with warning marks
- Check the power voltage in your area
- Make sure the power plug is not over burdened, which may cause equipment damage and fire
- Keep power cord standard wiring. Do not put anything on it
- Keep the equipment in a cool place
- Do not use other accessories that are not provided in your package
- Prevent thunder damage to the device. During thunderstorms, please UN-PLUG the power cord
- Do not disassemble the device
- Be careful of the adapter when un-plugging the power cord
- Make sure the power switch in turned OFF before you PLUG-IN/UNPLUG the cord
- Do not connect the SP200X to wall jacket
- Do not connect SP200X with PBX without help of technical support engineer

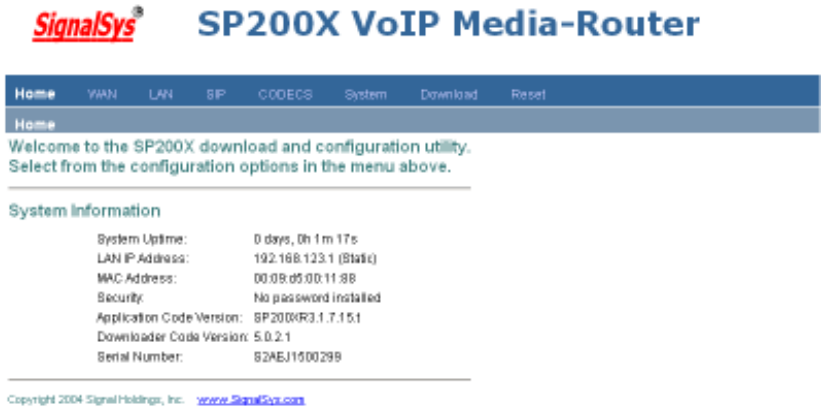
SECTION II. LAN Configuration

The device supports bridging/routing, the main menu LAN option provides sub-pages to configure the private LAN settings. There are five sub-pages to allow viewing of the LAN interface status and configuration of private internal DHCP settings, routing settings and the port

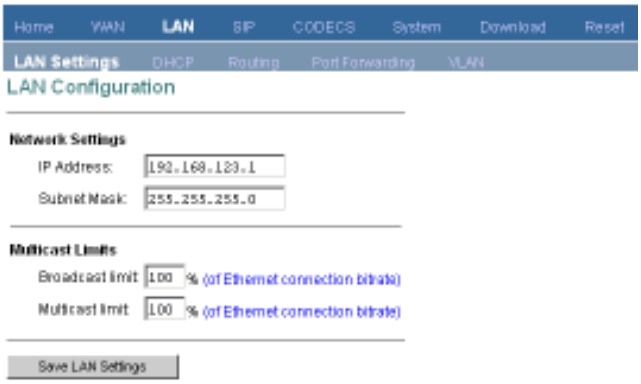
forwarding (NAPT) settings. Please note that any actions/modifications which alter the topology of the Ethernet bridge will result in the Ethernet bridge spanning tree protocol requiring to relearn. During this relearn period (may take up to one minute), HTTP access will be unavailable on all bridged interfaces (including the LAN interface).

2.1 LAN Interface Settings

This sub-page allows the user to configure the private LAN interface settings.
Assign an IP address to the LAN Ethernet port. This IP address is also the default router address for the devices on the private LAN. The default LAN interface IP address is set to **192.168.123.1**.



Enter the subnet mask for the private LAN.



If you wish to set the broadcast and multicast limits for the bridge/router, enter these values as percentages of the LAN interface Ethernet bit rate. Leaving these values blank will imply values of 100%.

Press "Save LAN Settings" to save and apply the LAN interface settings. Any new settings will take effect immediately.

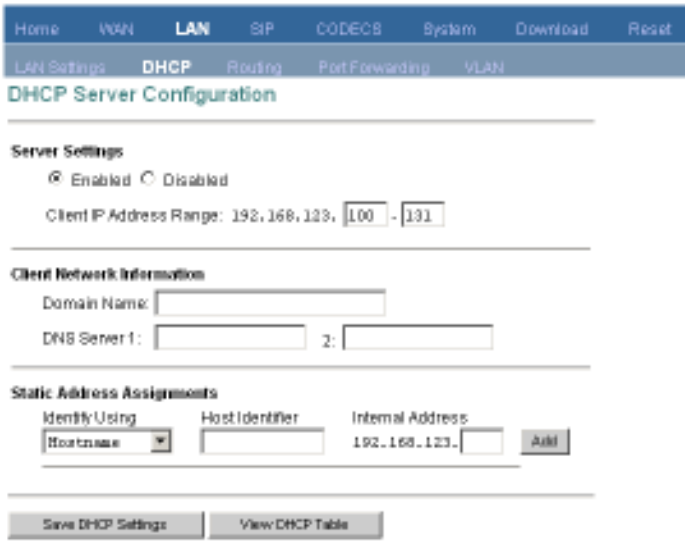
2.2 DHCP Server Settings

This sub-page allows configuration of the private LAN DHCP server. The DHCP server settings do not apply if the device is operating in bridge only mode.

Specify whether the device's internal DHCP server feature is enabled or disabled. Also indicate the IP address range to use for DHCP assignments to the LAN. Specify the domain name (optional) that is provided to LAN clients via DHCP. Two optional static DNS server IP

addresses can be entered that will be provided to LAN clients via DHCP. These are in addition to the DNS servers automatically provided by WAN connections. Press "Save DHCP Settings" to save and apply the DHCP server settings. Any new settings will take effect immediately.

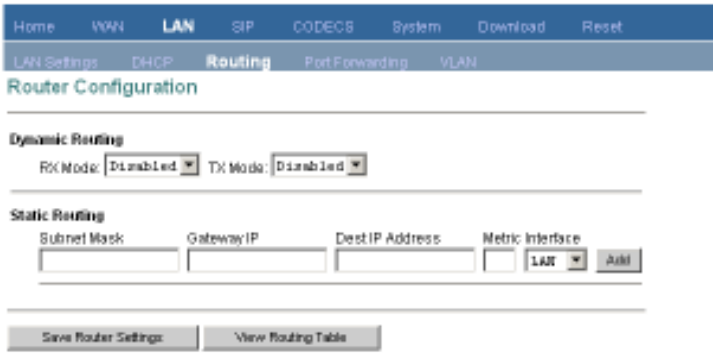
In addition, up to eight static DHCP address assignments can be configured. To add a static IP assignment, enter the LAN device's name (must be unique in the private network) and/or MAC address. Specify the static IP to be assigned and press the "Add" button. To remove an existing entry, press the "Remove" button next to the entry to be removed.



To view the current active DHCP client binding table (the internal list of devices for which the server has provided an IP address lease), press "View DHCP Table". A popup window will appear displaying the list of bindings. Press "Update" to update the binding information. Press "Close" to close the binding table window. To clear the device's internal DHCP client binding table, press "Clear client binding table". Be aware that doing this will destroy the DHCP server's knowledge of the LAN clients it has provisioned, and may result in client problems when a client tries to renew its lease.

2.3 Routing Settings

This sub-page allows configuration of the device's core router functionality. The router settings do not apply if the device is operating in bridge only mode.



If you wish for the router to dynamically update its routing tables, specify whether RIPv2 dynamic routing information is to be received or transmitted (or both). Press "Save Router Settings" to save and apply the dynamic routing settings. Any new settings will take effect immediately.

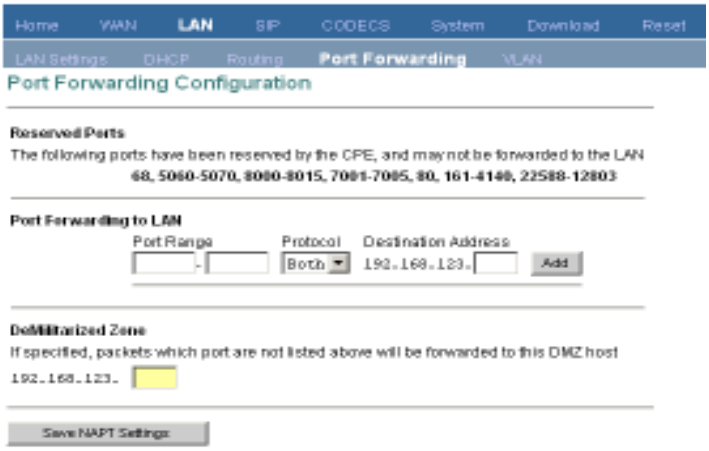
In addition, up to eight static route entries can be assigned. To add a static route, enter the static route Destination IP Address, Subnet Mask, Gateway IP Address, Metric, and Interface, and press the "Add" button. Metric is a number from 1 to 15 inclusive. To remove a static route, press the "Remove" button next to the entry you wish to remove.

To view the device's current internal routing table, press the "View Routing Table" button. A popup window will appear displaying the routing table. Press "Update" to update the route entries. Press "Close" to close the routing table window.

2.4 Port Forwarding (NAPT) Settings

This page allows the user to customize the devices port forwarding feature. The port forwarding feature does not apply if the device is operating in bridge only mode.

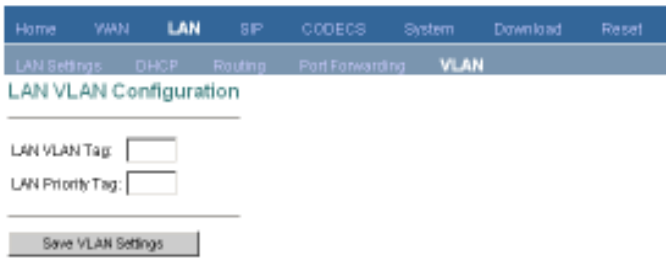
Port forwarding provides WAN access to the internal LAN, by specifying that traffic over certain ports are to be directed at particular LAN hosts. This feature is available only in router mode. Up to eight port forwarding entries ("Pinholes") can be configured. To add a port forwarding entry, configure the Port Range to be forwarded, the Protocol to be forward (TCP, UDP or both), and destination LAN IP Address. Press the "Add" button to add the entry. To remove an existing entry, click the "Remove" button next to that entry you wish to remove.



Note that certain port numbers may be reserved by the SP200X for its own internal use. These ports may not be used for port forwarding to the LAN. Ports which may be reserved by the SP200X include those used by VoIP call signaling, RTP packets, HTTP and SNMP. All reserved (unavailable) ports will be displayed on this page.

2.5 VLAN Settings

The LAN sub-page allows the user to configure general VLAN settings for all packets originating from the LAN interface. However, specific VLAN settings for VoIP call signaling and RTP packets can be separately applied (see sections 3.5), which will override the general values set on this page. If no special VoIP call signaling or RTP VLAN settings are applied, then call signaling and RTP packets will also use the general VLAN settings entered on this page.



Press "Save VLAN Settings" to save and apply the general VLAN settings. Any new settings will take effect immediately.

*DO NOT CHANGE THIS VLAN SETTINGS UNLESS YOU KNOW EXACTLY WHAT YOU WANT TO DO

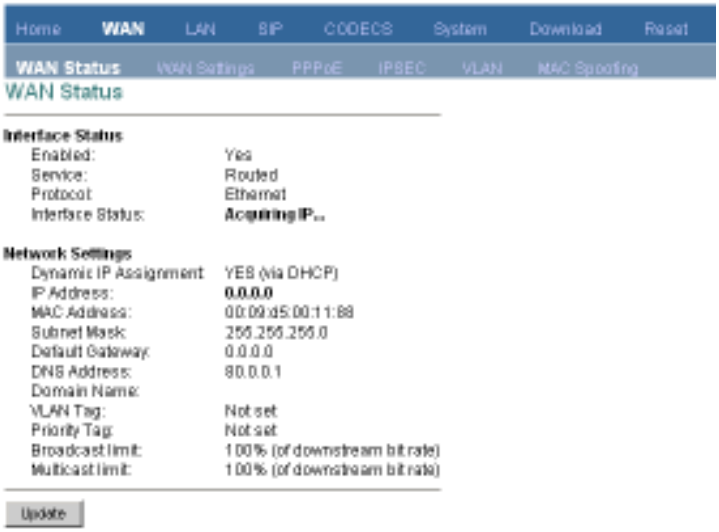
SECTION III. Ethernet WAN Configuration

This page and its sub-pages are only available on SP200X device, which support routing/bridging and allow viewing and configuration of the WAN interface status/settings.

Please note that any actions/modifications which alter the topology of the Ethernet bridge will result in the Ethernet bridge spanning tree protocol requiring to relearn. During this relearn period (may take up to one minute), HTTP access will be unavailable on all bridged interfaces (including the LAN interface).

3.1 WAN Interface Status

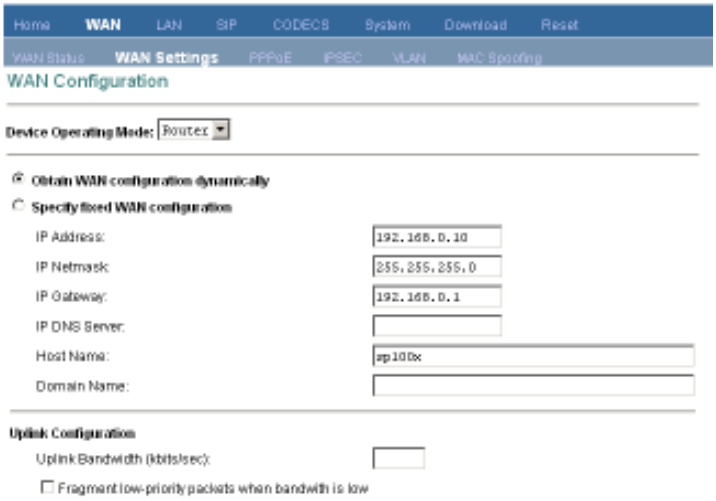
This page displays the current status of the WAN interface, including the IP address and other network settings the interface is currently using. If the interface is configured for PPPoE, a button is available to allow the administrator to DISCONNECT an active WAN PPPoE session or to initiate (CONNECT) a PPPoE session (if currently disconnected).



3.2 WAN Interface Settings

This sub-page only applies to the SP200X device. It allows the user to configure the Ethernet WAN interface. First, select whether the device is to act as a router or a bridge between the WAN and LAN interfaces.

Select whether you wish for the WAN interface to be configured dynamically (via a DHCP server on the network if Ethernet, or via PPP if using PPPoE), or statically configured. If you wish to statically assign the WAN interface settings, enter the IP address, subnet mask, default gateway IP address and DNS server IP address. It is also recommended that the network domain name be provided as well, to ensure correct DNS operation.



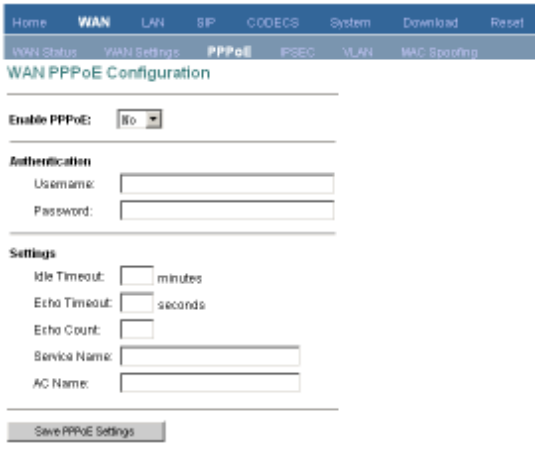
Press "Save WAN Settings" to save and apply the new values. Any new settings will take effect immediately.

3.3 Ethernet WAN PPPoE Settings

On this sub-page you can specify whether the WAN interface is to use PPPoE, and configure the PPPoE client. First, select whether PPPoE is enabled or disabled. If enabled, enter the username and password required for the login (authentication) process.

Setting the idle-timeout will result in the PPP connection being torn down if the client detects inactivity on the connection over the specified timeout period. Leaving this field blank will result in the connection being permanently up (i.e. without timeout).

If the PPPoE server (service provider) requires any special Service Name or AC Name to be set, you can specify these tags here.



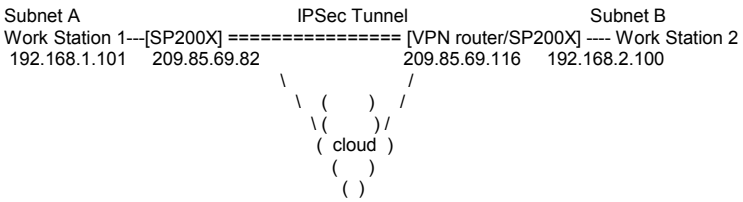
Press "Save PPPoE Settings" to save and apply the WAN interface PPPoE client settings. Any new settings will take effect immediately.

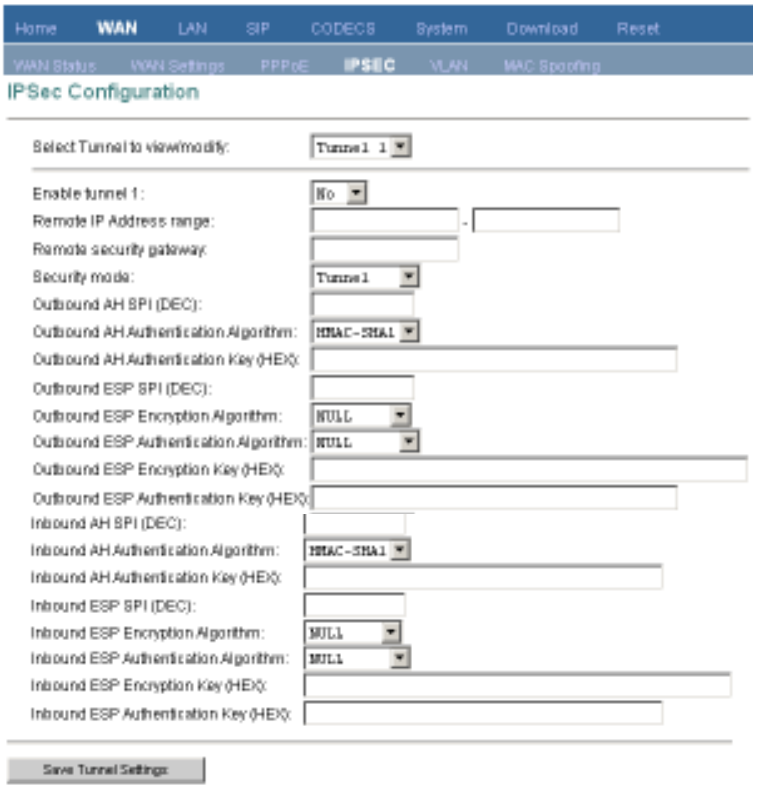
3.4 IPSEC Configuration

This sub-page allows configuration of the device's IPSec (IP Security) settings. A sample IPSec scenario is described below to aid in the configuration description. In this scenario, a SP200X router establishes a tunnel to other VPN router or another SP200X router. Both the SP200X router and the remote VPN router are configured to have private LAN subnets (Subnet A [192.168.1.x] and Subnet B [192.168.2.x] respectively). IPSec in tunneling mode can be used to establish a secure tunnel between two VPN routers. The SP200X router will send out traffic through a secure tunnel or normal internet depending on the destination address of the traffic. If a packet is to be sent through a secure tunnel, the packet will bypass NAT and will be encapsulated with the router (gateway)'s src/dest address and appropriate encryption and authentication header/trailers. This way, the packet retains its own subnet information and can be regarded as if it were originated within a private network (Virtual Private Network).

After the tunnel establishment, a work station in Subnet A should be able to access Subnet B, and vice versa.

Sample network topology:





To setup the sample IPSec tunneling configuration depicted above, use the following procedure on SP200X router. Also, the corresponding configuration should be done on the remote VPN router to complete the IPSec tunnel configuration.

1. Select the tunnel to use from "Select Tunnel to view/modify" field. For example:
```
Select tunnel 5
```
2. Enable the tunnel by selecting "YES" in the "Enable Tunnel 5" field.

3. Set the Subnet B's IP address range by specifying start and ending addresses in the "Remote IP Address range" fields. For Example:
```
192.168.2.1 ~ 192.168.2.254
```
4. Set the IP address of the remote VPN router in the "Remote security gateway" field. For example:
```
209.85.69.116
```
5. Set the security mode to "Tunnel" in the "Security mode" field. The "Transport" mode is rarely used and is not applicable in this sample network configuration.
6. Configure IPSec parameters for outbound traffic (from the SP200X router to the remote VPN router). There are two different methods to protect your packets:

- AH(Authentication Header) is used to provide authentication
- ESP(Encapsulating Security Payload) is used to keep privacy of the data by encrypting payloads. The ESP also provides limited authentication, which makes the use of ESP only secure enough in most situations.

You can enable AH and/or ESP by providing unique SPI(Security Parameter Index) numbers in the "AH SPI" and/or "ESP SPI" fields. At least one of these (ESP in most cases) must be enabled to do IPSec tunneling. In this example, we will assume only ESP is used with 3DES and MD5 for encryption and authentication.

```
Outbound AH SPI:                blank (AH is not used)
Outbound ESP SPI:               2001
```

If AH is enabled by providing a unique SPI number, you can select a message digesting algorithm from the "AH Authentication Algorithm" field, and provide the secret key value in the "AH Authentication Key" field.

```
Outbound AH Authentication Algorithm: blank (don't care)
Outbound AH Authentication Key:       blank (don't care)
```

If ESP is enabled by providing a unique ESP SPI number, you can select a message digesting algorithm from the "ESP Authentication Algorithm" field, and provide the secret key value in the "ESP Authentication Key" field. The ESP configuration also requires that the "ESP Encryption Key" by set as well.

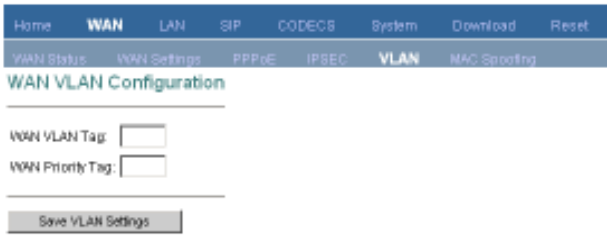
```
Outbound ESP Encryption Algorithm:              3DES-CBC
Outbound ESP Authentication Algorithm:          HMAC-MD5
Outbound ESP Encryption Key:
           157f34683a295484236593486e8d3ab5642396897ace3fbd
Outbound ESP Authentication Key:
           3587659a2f3da45c568a359f592d3ca81f326f2c
```

These parameters and algorithm selections should match those of the inbound parameters

and algorithms on the remote VPN router.

3.5 VLAN Settings

The WAN VLAN sub-page allows the user to configure general VLAN settings for all packets originating from the WAN interface.



Press "Save VLAN Settings" to save and apply the general VLAN settings. Any new settings will take effect immediately.

*DO NOT CHANGE THIS VLAN SETTINGS UNLESS YOU KNOW EXACTLY WHAT YOU WANT TO DO

3.6 MAC Spoofing

This sub-page allows the user to set the Ethernet hardware/MAC address to be used by the WAN interface. This is typically done to mimic ('spoof' or 'clone') the MAC address of one of the devices connected on the private LAN interface. Enter the 12 digit hardware address to assign to the WAN interface and press "Save MAC Spoofing Settings" to save and apply the new setting.

SECTION IV. SIP Configuration

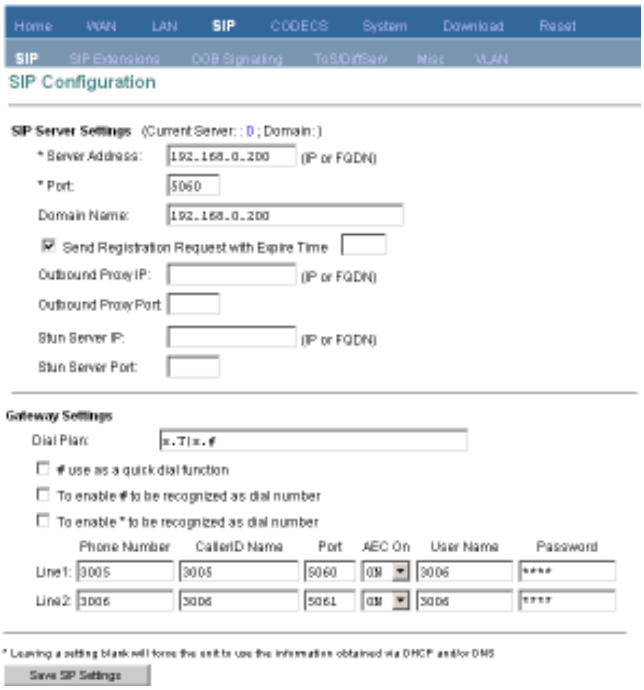
If the device is running the SIP protocol, select “SIP” from the menu on the left. This will provide sub-pages to configure: the SIP endpoint and SIP Server settings; selection of any special SIP extensions for advanced SIP features; the specification of out-of-band (OOB) DTMF signalling; the ToS/DiffServ settings for SIP and RTP packets; and the VLAN prioritization for SIP and RTP packets.

4.1 SIP Settings

This page allows configuration of the SIP server and endpoint settings.

Enter the address and port value of the SIP server. The address may be an IP address or the name of the server. If no SIP server address is entered, the device will attempt to self provision a SIP server using a DNS query. For this to be successful, ensure that the DNS settings on the device

include a DNS server address which is configured with the SIP server address and will respond to the query, and the appropriate domain name of the network.



If you wish to specify a special SIP domain name, you may enter the domain name here. If no domain name is entered, the SIP domain name will be set to that of the network.

The currently provisioned SIP Server and Domain are displayed beside “SIP Server Settings” for informational purposes.

Select whether or not to send a Registration Request to the SIP server by checking the box next to “Send Registration Request”.

If you use Outbound SIP Proxy, you may fill in the Proxy IP address and Port. Otherwise, leave them blank.

If you STUN server, you may fill in the STUN server IP address and Port. Otherwise, leave them blank.

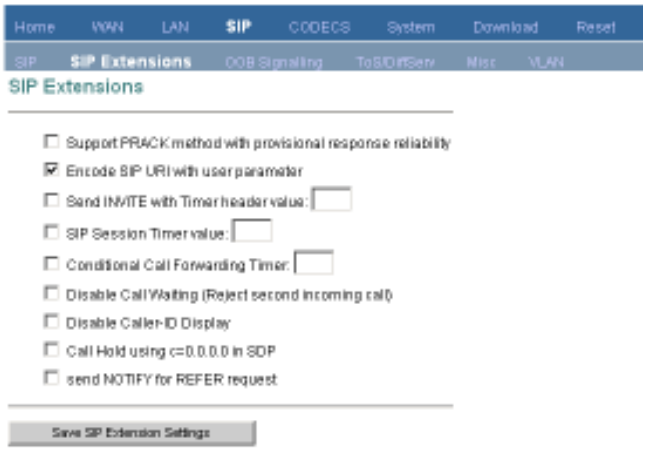
For the endpoint, set the dial plan to be used by all lines (refer to “Appendix D ” for details on the dialplan representation), and select the transport method to be used for SIP signaling (either UDP or TCP).

For each line on the endpoint (NOTE: SP200X has a single line), enter the Line Phone Number, Caller-ID Name, signaling port value, authentication Username and Password, and select if AEC is to be performed on this line.

Press “Save SIP Settings” to save the new values.

4.2 SIP Extensions

This page allows specification of the SIP signalling stack behavior under certain scenarios. If you wish for the SIP stack to implement reliable transmission of provisional responses according to RFC 3262 (using the PRACK method), check the option "Support PRACK method with provisional response reliability".



If you wish for the SIP stack to include the user parameter "user=phone" in the SIP URI header(s), check the option "Encode SIP URI with user parameter".

If you wish for the SIP stack to send INVITE messages with the "Timer" header field present, check the option "Send INVITE with Timer header value" and enter the Timer header value. If you wish for the SIP stack to implement a session timer according to "draft-sip-session-timer", select the option "SIP Session Timer value", and enter the session time-out value.

Press "Save SIP Extension Settings" to save the new values.

4.3 Out-of-band (OOB) Signaling Settings

This sub-page allows configuration of the out-of-band signaling options for SIP. Select whether OOB telephone event signaling is to be done using the SIP INFO message, or to be done via RFC2833 RTP signaling.

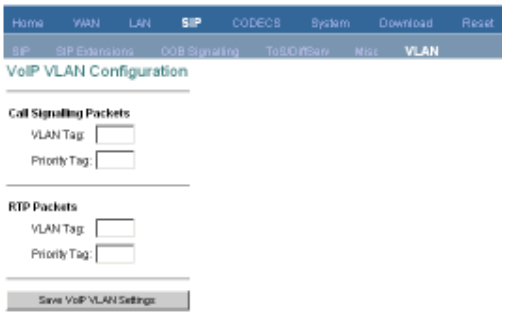
4.4 SIP ToS/DiffServ Settings

This sub-page is used to configure the Type-of-Service/Diffserv byte values which are to be used in the IP header of all transmitted SIP signaling packets and RTP packets. The ToS/DiffServ byte values are entered as two-digit hexadecimal values. If no special ToS/DiffServ value is to be used for a particular traffic type, enter "00" or leave the setting empty.

Press “Save ToS/DiffServ Settings” to save these new settings.

4.5 SIP VLAN Settings

This sub-page allows configuration of specific VLAN tags that are to be applied to all SIP signalling and RTP packets used for VoIP calls. These VLAN settings will override any general VLAN settings applied to the interface.

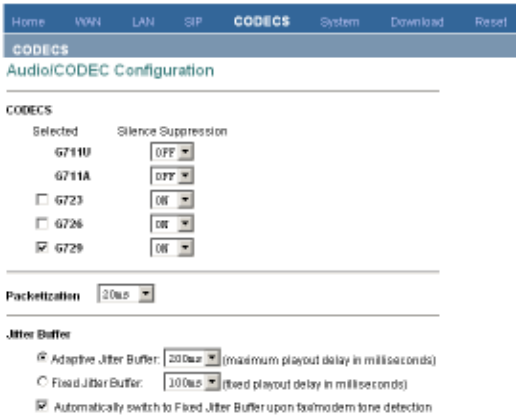


Press "Save VoIP VLAN Settings" to save the settings.

*DO NOT CHANGE THIS VLAN SETTINGS UNLESS YOU KNOW EXACTLY WHAT YOU WANT TO DO

SECTION V. CODEC Configuration

This page is available for configuring the audio CODEC parameters, as well as the Jitter Buffer settings for the CODEC decoders.



Enter which codecs are to be supported. For some protocols (e.g. SIP), the G711U and G711A protocols are always supported by default.

Select which complex codec is to be supported. Due to memory limitations, it is not possible to select more than one complex codec.

Select the packetization period to be used for each selected CODEC.

Select whether Silence Suppression is to be supported for each CODEC.

The Jitter Buffer settings apply to all active CODEC decoders. You may choose between an adaptive jitter buffer or a fixed jitter buffer. For an adaptive jitter buffer, choose the maximum allowable playout delay (in milliseconds). For a fixed jitter buffer, choose the fixed playout delay (in milliseconds).

Finally, select whether or not a decoder should automatically switch from an adaptive jitter buffer to a fixed jitter buffer upon fax/modem tone detection. Adaptive jitter buffers are sometimes detrimental to fax transmission over G711 CODECs if they have to adapt too rapidly or too extensively due to inconsistent and widespread packet delays. In these adverse network conditions, a fixed jitter buffer provides superior performance when handling incoming fax transmissions over G711 CODECs.

Press "Save CODEC Settings" to save the new CODEC parameters.

SECTION VI. System Configuration

This main menu option provides sub-pages to configure certain of the device's system level settings: the device's SNMP, security and localization settings.

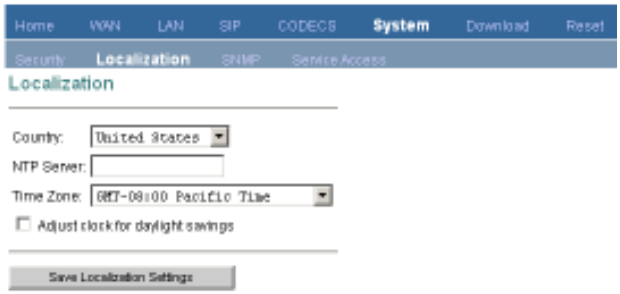
6.1 Security Settings

This sub-page allows an administrator to configure the device with an access password.

Enter the password and confirm by reentering it. Press "Save Security Settings" to apply the password protection. Effective immediately, the password will be required whenever anyone wishes to access the device's configuration web pages.

6.2 Localization / Clock Settings

This sub-page only applies to devices running a VoIP protocol, and is used to configure the localization settings of the device.



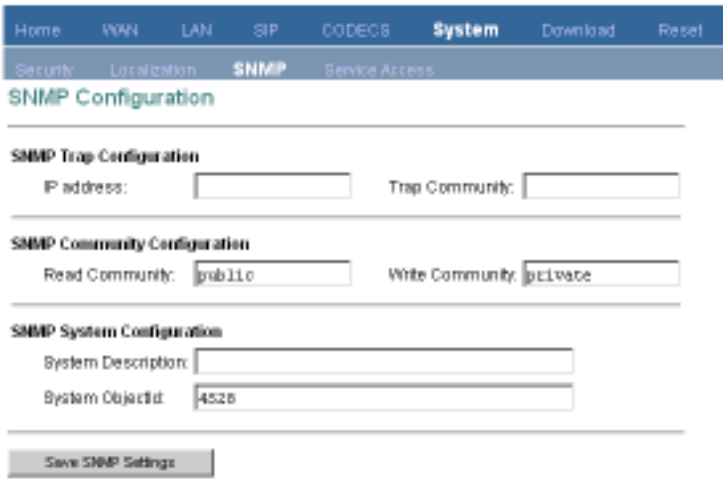
Enter the country (certain media hub devices require this information in order to communicate with analog phones which follow different international standards).

If you wish for the device to automatically obtain the time via NTP, enter the NTP server address for the network (if this address is left blank, a default public NTP server will be used, if accessible). Select the time zone and whether or not adjust for daylight savings.

Press "Save Localization Settings" to save the new values. These settings will only take effect when the device is rebooted.

6.3 SNMP Settings

This sub-page is used for configuring the device's SNMP server. Configure the SNMP Trap Host IP address and community, the SNMP read and write community parameters, and the SNMP System Description and System Object ID parameters.



Press "Save SNMP Settings" to apply the new values. These settings will only take effect when the device is rebooted.

6.4 Service Access Settings

If the device is a multi-interface device (bridge/router), then this sub-page is available to enable/

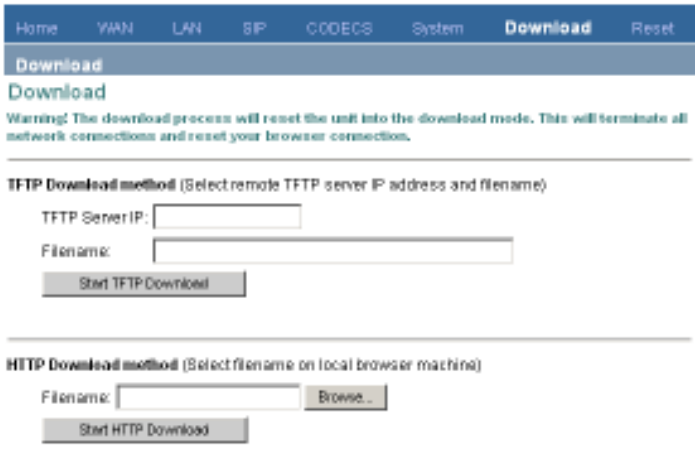
disable access to certain system level network services on the device's interfaces. From this page, an administrator can choose to allow or disallow HTTP, SNMP and VoipDiscovery access from devices on the LAN or WAN or both. Care must be taken while configuring the HTTP access, as once you have saved you will no longer be able to access the device's web pages if you have disabled HTTP on the interface you are currently accessing the device on.

For security reason, we suggest that you disable the HTTP on WAN.

Press "Save Service Access Settings" to save and apply the new access settings.

SECTION VII. Download Configuration

This page provides two options for downloading a new firmware application image to the device. If you wish to download the new firmware image using TFTP, enter the filename of the ROM image and enter the IP address of the TFTP server on which this file resides. Press "Start TFTP Download" to initiate the TFTP download process.



If the ROM image is stored on the same local machine you are using to access the device's web pages, you can choose to download the ROM file to the device using an HTTP post. Enter the filename of the ROM image or press "Browse" to help locate the file. Press "Start HTTP Download" to initiate the HTTP download process.

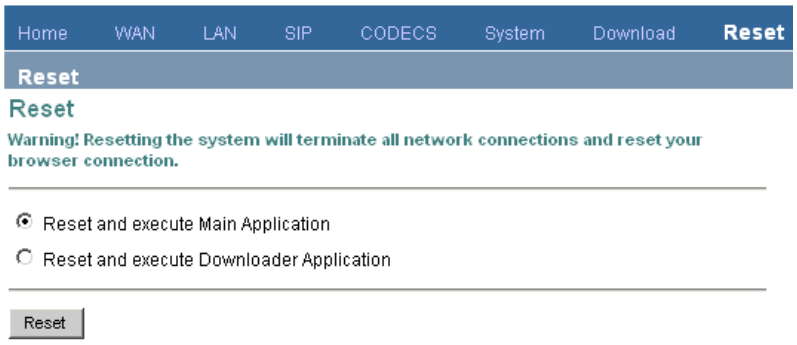
If the main application is executing at the time, the device will automatically reboot itself into

the downloader mode and begin the download process. If the downloader application is executing at the time, the download process will begin. The download status will be displayed when the image download process is complete.

IMPORTANT
Once the download is in progress, it MUST be allowed to complete in its entirety, or the main application image will be destroyed. If an irrecoverable error occurs, reboot the device. It will automatically execute the downloader application and allow you to reattempt a download of the new firmware image.

SECTION VIII. Reset Configuration

This page provides options for resetting the device. Select whether you wish to reset the device and start executing the main (default) application, or whether you wish to reset the device and start executing the internal downloader application.



Press "Reset" to reset the device.

SECTION IX. General Troubleshooting

9.1 LED
LED “Power”: ON/OFF (indicates power connection)
LED “LAN”: ON/OFF (indicates LAN connection)
LED “WAN”: ON/OFF (indicates WAN connection)
LED “L1”: ON/OFF (indicates Phone pickup)
LED “L2”: ON/OFF (indicates SIP registration)
LED “L3”: ON/OFF (indicates Message waiting)

9.2 Mass Deployment
If the “Mass Deployment” is selected, the router will take approximate **20 seconds** to startup. The LED “L1” is ON when the router is in “Mass Deployment” and the LED “L3” is ON when the router is upgrading the image software using “Mass Deployment” server.

SECTION X. Make Phone Calls

10.1 Make a call

If you have your own dial plan, just dial the phone number. If you have no dial plan or using default dial plan, dial the phone number followed by #. See Appendix C for Dial Plan setup.

10.2 3-Way Conference

While two parties are in the conversation, either party can add the third party in the 3-way conference by flash hook (hang up once while holding handset) and dial 7. After you hear a dial tone, please dial telephone number to add third party for conference. To drop the third party, flash and dial 8.

10.3 Call Waiting

During the conversation, when you hear the call waiting tone, flash and dial "*". It will switch you to the incoming call. Flash and "*" again, it will be switched to the previous conversation.

10.4 Call Forwarding

Pick up the phone and dial *2. After hearing the dial tone, dial the forwarding phone number and #. Then, hang-up the phone. The incoming calls will be forwarded.

To set call forwarding off, pick up the phone and dial *3.

APPENDIX

A. Determining the IP Address

This section provides instructions on how to determine the IP address of a unit, or how to boot up into a 'safe' mode that allows the IP address to be reconfigured. Instructions differ depending on the platform type.

A.1 General Instructions

The following general instructions can be followed to determine the IP address of a unit. Several mechanisms are available:

• If the device is thought to be using DHCP to obtain an IP address, check the DHCP server log, leases file, or binding table (if available). Look for the MAC address of the unit. The MAC address is a 6-octet string and can be found on a barcode label on the device.

• Use a packet sniffer attached to the same network as the device. Set the sniffer to filter packets based on the unit's MAC address, and initiate some data packet transfer (e.g. make a VoIP call). Analyze the captured packets to determine the device's IP address.

• If the SNMP trap destination has been previously set, check your SNMP management server for the IP address which is sent out as part of the Cold Start trap on system reset.

B. Forcing 'Safe' Modes

The SP200X can be forced into a 'safe' downloader mode by performing the following steps in order. In this description, the RESET button, which is the button at the back end of SP200X:

1. Power cycle the unit while holding down the RESET button. Count 4 seconds. **Release the RESET button immediately.**

2. To force the unit to use a fixed IP that is in the config file, press and immediately release the RESET button again **within 2 seconds** of releasing it after step 1 above. After 2 seconds of button inactivity, the device will start the downloader network stack in fixed IP mode (**LED L1 and L2 are ON**). If no fixed IP information exists in the configuration file, the device will default back to DHCP mode.

3. Finally, to force the unit to use 10.1.0.54 as the IP address, press and immediately release the RESET button again a third time **within 2 seconds** of releasing it after step 3 above. The device will now use 10.1.0.54 as the IP address (**LED L1, L2, and L3 are ON**).

REMINDER: There is a two second time-out after each press of the RESET button, after which the downloader network stack will boot into the selected mode.

1 Presses = FIXED IP
2 Presses = 10.1.0.54

If the wrong network mode is started by mistake, the process can be easily restarted by holding down the RESET button and power cycling the device again.

C. Dial Plans

The SIP code will allow provisioning (via web browser) of the dial plan. A dial plan gives the unit a map to determine when a complete number has been entered and should be passed to the SIP Server for resolution into an IP address. Dial plans are expressed using the same syntax as used by MGCP NCS specification.

The formal syntax of the dial plan is described by the following notation:

```
Digit ::= "0" | "1" | "2" | "3" | "4" | "5" | "6" | "7" | "8" | "9"
Timer ::= "T" | "t"
Letter ::= Digit | Timer | "#" | "*" | "A" | "a" | "B" | "b" | "C" | "c"
        | "D" | "d"
Range ::= "X" | "x" -- matches any digit
        | "[" Letters "]" -- matches any of the specified letters
Letters::= Subrange | Subrange Letters
Subrange::= Letter -- matches the specified letter
        | Digit "-" Digit -- matches any digit between first and last
Position::= Letter | Range
StringElement::= Position -- matches any occurrence of the position
        | Position "." -- matches an arbitrary number of occurrences
```

including 0
String ::= StringElement | StringElement String
StringList::= String | String "|" StringList
DialPlan::= String | "(" StringList ")"

A dial plan, according to this syntax, is defined either by a (case insensitive) string or by a list of strings. Regardless of the above syntax a timer is only allowed if it appears in the last position in a string (12T3 is not valid). Each string is an alternate numbering scheme. The unit will process the dial plan by comparing the current dial string against the dial plan, if the result is under qualified (partial matches at least one entry) then it will do nothing further. If the result matches or is over-qualified (no further digits could possibly produce a match) then send the string to the gatekeeper and clear the dial string.

The Timer T is activated when it is all that is required to produce a match. The period of timer T is 4 seconds. For example a dial plan of (xxxT|xxxxx) will match immediately if 5 digits are entered, it will also match after a 4 second pause when 3 digits are entered.

C.1 Sample Dial Plans

Simple Dial Plan

Allows dialing of 7 digit numbers (e.g. 5551234) or an operator on 0. Dial plan is 0T|xxxxxxx

Non-dialed Line Dial Plan

As soon as handset is lifted the unit contacts the SIP Server (used for systems where dtmf detection is done in-call). Dial plan is (x.) i.e. match against 0 (or more) digits. Note: the dot '.'

Complex Dial Plan

Local operator on 0, long distance operator on 00, four digit local extension number starting with 3,4 or 5, seven digit local numbers are prefixed by an 8, two digit star services (e.g. 69), ten digit long distance prefixed by 91, and international numbers starting with 9011+variable number of digits.

Dial plan for this is:

0T|00T|[3-5]xxx|8xxxxxxx|*xx|91xxxxxxxxxx|9011x.T