

Service Managed Gateway™

Configuring a V90 Modem on an SMG



Issue 2.1
Date 18 August 2010

1	About this document	3
1.1	Scope	3
1.2	Readership	3
1.3	More information.....	3
1.3.1	Assigned interface number	3
2	Introduction	4
3	Setting up and configuring the V90 modem.....	5
3.1	Setting up the physical port connection	5
3.2	Configuring the V90 modem.....	5
3.3	Configuring the SMG to use the V90 modem interface.....	5
3.3.1	Configure the IP default route	5
3.3.2	Configure the IP interface.....	6
3.3.3	Configure address translation.....	8
3.3.4	Configure IPCP options.....	9
3.3.5	Configure the PPP interface.....	12
3.3.6	Select asynchronous PPP operation	13
3.3.7	Configure authentication options	15
3.3.8	Set dialling options	17
3.3.9	Configure the modem interface	19
4	Saving your configurations.....	21
4.1	Reload the configuration	21
4.2	Using the modem as a backup WAN interface	22
4.3	Caller ID restrictions	22
5	Modem monitoring and diagnostics	23
5.1	Active data connections	23
5.2	Call history	23
5.3	Connection monitor	24
5.4	Modem events	24
5.5	Modem events list	25

1 About this document

1.1 Scope

This document describes how to configure and use the V90 modem.

1.2 Readership

The document is for engineers who configure and manage Service Managed Gateways (SMGs).

1.3 More information

1.3.1 Assigned interface number

Throughout this document, we have used (n) as the assigned interface number.

- modem(n), where n is the interface number, for example, modem-0
- PPP-n, where n is the interface number, for example, PPP-1

2 Introduction

The Virtual Access Service Managed Gateway 6000 series and GW7000 series product range are optionally fitted with an V90 modem.

The modem conforms to ITU V.92 specification, which is an enhancement of the V.90 modem. The V.92 modem offers two main functions over the V.90 modem:

1. Quick connect: the connection time may be reduced by 50% compared to the V.90 modem.
2. Faster upstream rate: upload speeds may reach 48kbps, compared to 31.2kbps with the V.90 modem. It is also capable of data speeds of up to 56kbps downstream.

The following standards are supported:

Data modem	V.92/V.90 V.34 V.32bis V.32 V.29 V.22bis V.22 V.22 Fast Connect V.23 V.21 Bell212a Bell103
Data compression	V.44 V.42bis and MNP5 V.42 LAPM and MNP2-4 error correction

The V90 modem interface on SMG products is available for use in several scenarios.

Scenario	Description
As a normal WAN interface	Use the V90 modem in the same way other WAN interfaces such as DSL and ISDN are used.
As a backup WAN interface	Set up the V90 modem to come into operation if the primary WAN interface becomes unusable for some reason.
As an out-of-band management interface	Use the V90modem to access the SMG management functions by dialing into the SMG, for example, using Virtual Access Activator. It is also possible for the SMG to dial out via the V90 modem interface under some conditions.

A number of low-level maintenance functions are available by dialling the SMG V90 modem interface if the SMG does not boot up correctly, or otherwise fails to start up properly.

3 Setting up and configuring the V90 modem

3.1 Setting up the physical port connection

To set up the physical modem interface, connect one end of your modem cable to your phone line wall-socket and the other end to the SMG RJ-11 modem port.



Figure 1: The physical port connection for the 6000 series

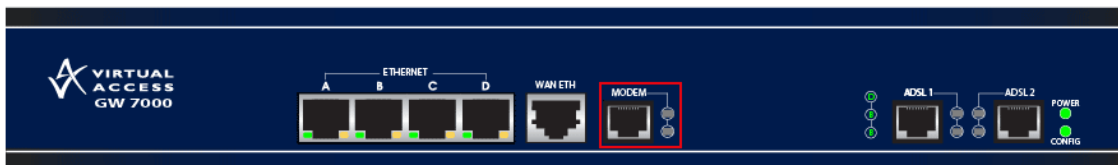


Figure 2: The physical port connection for the GW7000 series

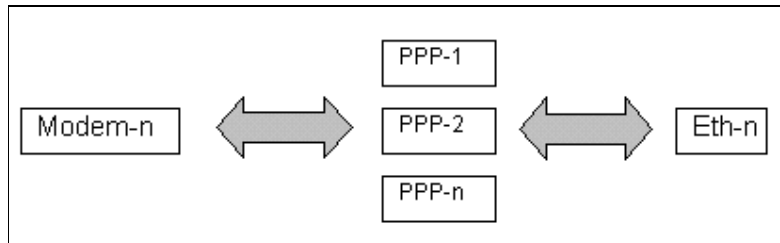
3.2 Configuring the V90 modem

The modem is configured as a logical interface modem-n, for example, modem-0.

The modem interface has the following configuration attributes:

Enabled: yes, no

The logical modem interface is connected to a PPP interface by configuring the PPP WAN interface as described in section 3.3.2 below.



3.3 Configuring the SMG to use the V90 modem interface

To configure the SMG to use the V90 modem interface, follow the steps in sections 3.3.1 to 3.3.9. When you have committed all the settings, you must save the configuration as described in section 3.3.10.

3.3.1 Configure the IP default route

In the Expert View menu, select **system -> ip -> ip routing -> default route**. The IP Default route page appears.

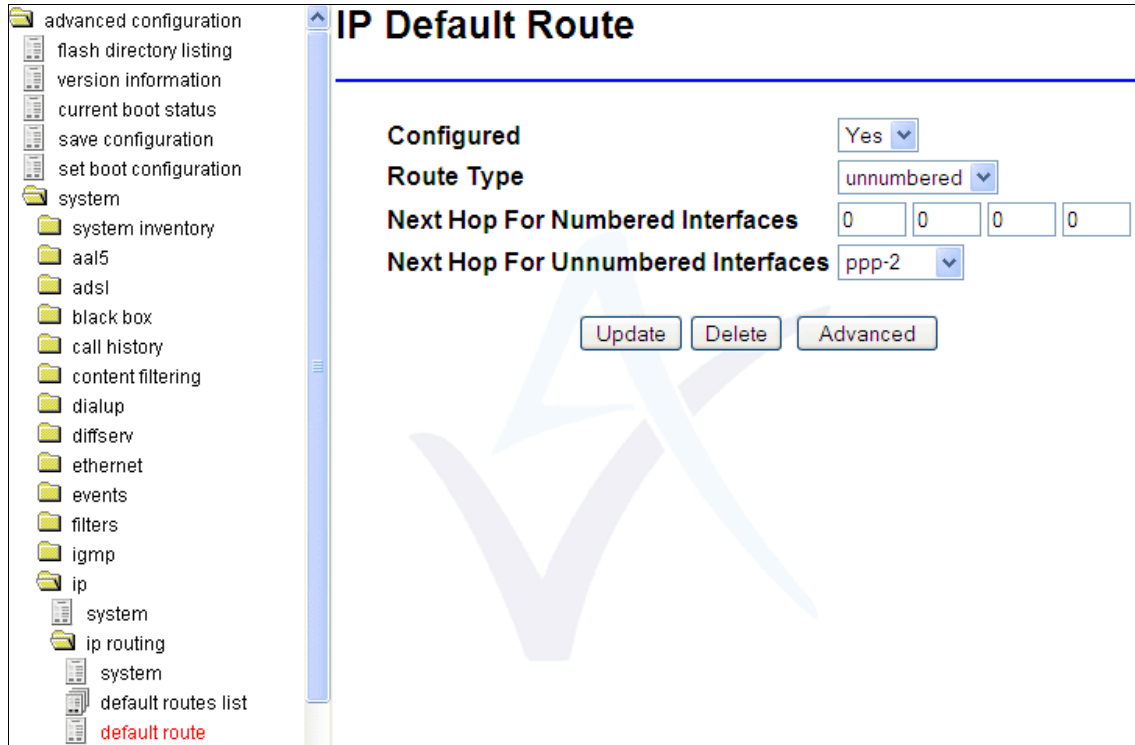


Figure 3: The IP default route page

Set the fields and drop-down lists in the IP default route page as shown in table 1.

Click **Update**. The Configuration Update Result page appears. Proceed to section 3.3.2 to set the next configuration.

Field name	Description	Command Line
Configured	Enables or disables the default route. Set Configured to Yes	Set Ip Route Default Configured
Route Type	Indicates whether the route type is over a numbered or unnumbered link. A numbered link is a link that has been assigned an IP address. Set Route Type to unnumbered	Set Ip Route Default Numbered
Next Hop For Numbered Interfaces	When Route Type is set to numbered , enter the IP address in dotted-decimal notation, of an adjacent router. The local device sends traffic to this router when a route to a destination is not known. Type in 0.0.0.0 .	Set Ip Route Default Next Hop Ip
Next Hop For Unnumbered Interfaces	Sets the interface as the default route. Select the default route to interface <portnumber> .	Ip Route Default Next Hop Interface

Table 1: The IP default route page fields and values

3.3.2 Configure the IP interface

In the Expert View menu, select **interfaces -> ppp-2 -> ip -> ip**. The IP Interface page appears.

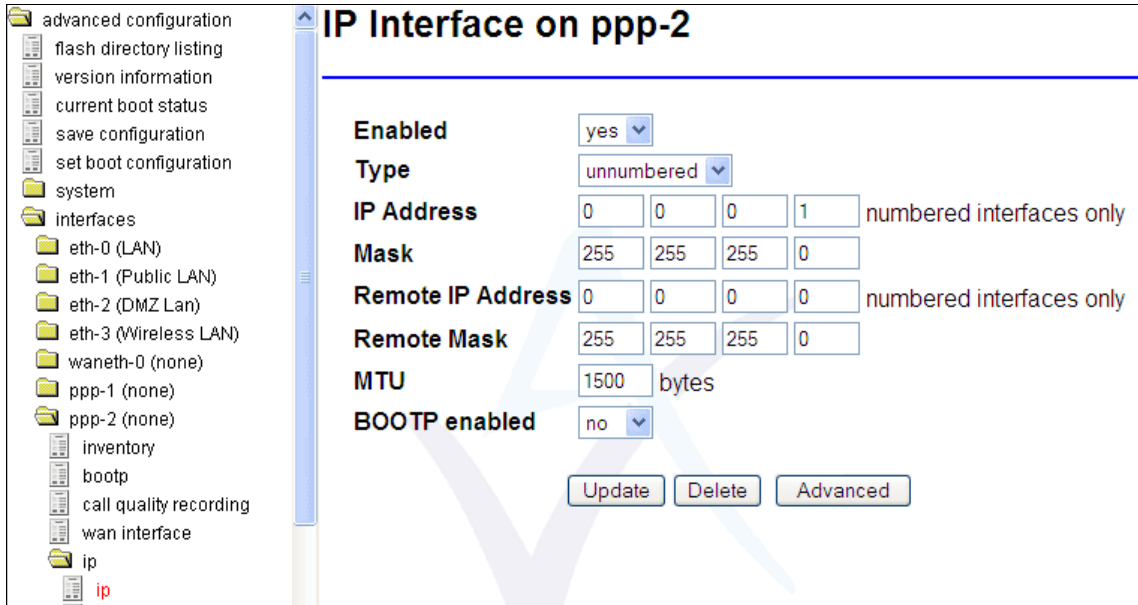


Figure 4: The IP interface on ppp-2 page

Field name	Description	Command Line		
Enabled	Use this option to enable or disable IP operation on the selected interface	Set Ip Interface Enabled		
	<table border="1"> <tr> <td>yes</td> <td>Enables IP operation on the selected interface. This is the default setting. Select yes.</td> </tr> <tr> <td>no</td> <td>Disables IP operation on the selected interface.</td> </tr> </table>		yes	Enables IP operation on the selected interface. This is the default setting. Select yes .
yes	Enables IP operation on the selected interface. This is the default setting. Select yes .			
no	Disables IP operation on the selected interface.			
Type	Select numbered or unnumbered to define the point-to-point link associated with the PPP interface operating in unnumbered IP mode or numbered IP mode.	Set Ip Interface Unnumbered Link Enabled		
	<table border="1"> <tr> <td>numbered</td> <td>Configures an IP point to point link for numbered operation. This is the default setting.</td> </tr> <tr> <td>unnumbered</td> <td>Configures an IP point to point link for numberless or unnumbered operation.</td> </tr> </table> <p>Unnumbered operation: the IP router identifies itself to IP peers across unnumbered point to point links by using the first configured IP address; that is, the IP interface with both IP Address and Mask; of the IP router. It identifies each unnumbered peer by the remote IP address for each point-to-point link. If RIP is enabled for operation across an unnumbered point-to-point link, the IP router learns routes to and through the peer dynamically, thereby eliminating the need to configure the remote IP address. Dynamic or static routes can be used under this mode of operation.</p> <p>Note: when you define an interface as</p>		numbered	Configures an IP point to point link for numbered operation. This is the default setting.
numbered	Configures an IP point to point link for numbered operation. This is the default setting.			
unnumbered	Configures an IP point to point link for numberless or unnumbered operation.			

	unnumbered, you must set the IP Address field for the interfaces(s) to 0.0.0.0 .	
IP Address	Enter the IP address, in dotted decimal notation, to be assigned to the selected interface. This field and the mask provide the network and host identification. This configuration change does not take effect until you reboot the device. Note: when the interface is defined as unnumbered, you must set this field to 0.0.0.0 .	Set Ip Interface Address
Mask	The subnet mask is used to determine the network and host ID from the IP address and is based on the network class. Enter the subnet mask, 255. 255. 255. 0 , to be assigned to the selected interface.	Set Ip Interface Address Mask
Remote IP Address	The IP router process establishes a host route to the end point of each point-to-point link based on the remote address. Enter the IP address of the peer at the opposite end of the point-to-point link associated with the selected interface. Type in 0.0.0.0 .	Set Ip Interface Remote Address
Remote Mask	Specify the subnetwork mask, in dotted decimal notation, to be associated with the remote end point of an unnumbered IP link. Type in 255.255.255.0 .	Set Ip Interface Remote Mask
MTU	Enter the size, in bytes, of the largest IP datagram that can be sent by the selected interface. The MTU value includes the data link header, IP header, and IP data field. Type in 1500 .	Set Ip Interface Mtu
BOOTP enabled	Enables or disables BOOTP on the selected interface. Select no .	Set Ip Interface Bootp Enabled

Table 2: The IP interface page fields and their descriptions

Click **Update**. The Configuration Update Result page appears. Proceed to section 3.3.3 to set the next configuration.

3.3.3 Configure address translation

In the Expert View menu, select **interfaces -> ppp-2 -> ip -> address translation -> outgoing**. The Outgoing Address Translation page appears.

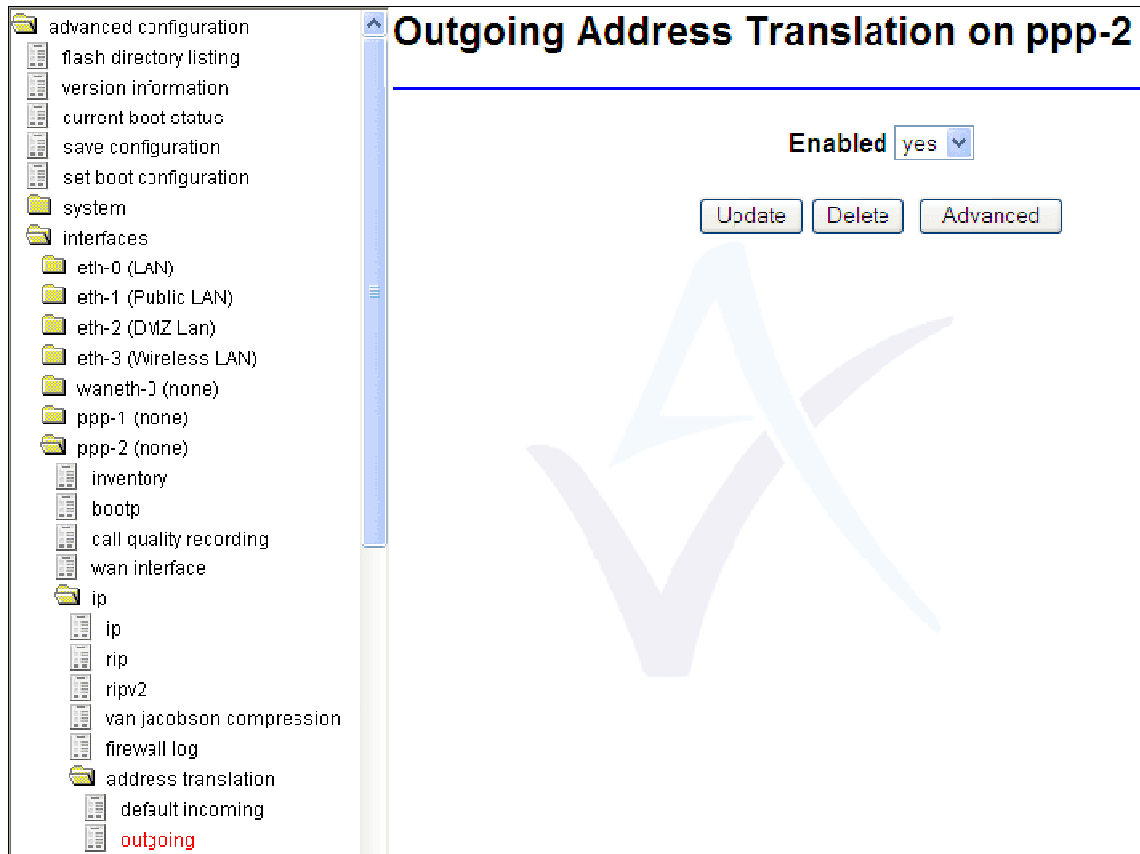


Figure 5: The outgoing address translation page

On the Outgoing Address Translation on ppp-2 page, set Enabled to **yes**.

Click **Update**. The Configuration Update Result page appears. Proceed to section 3.3.4 to set the next configuration.

3.3.4 Configure IPCP options

In the Expert View menu, select **interfaces -> ppp-2 -> ip -> ipcp options -> local address**. The Local IP Address Negotiation on ppp page appears.

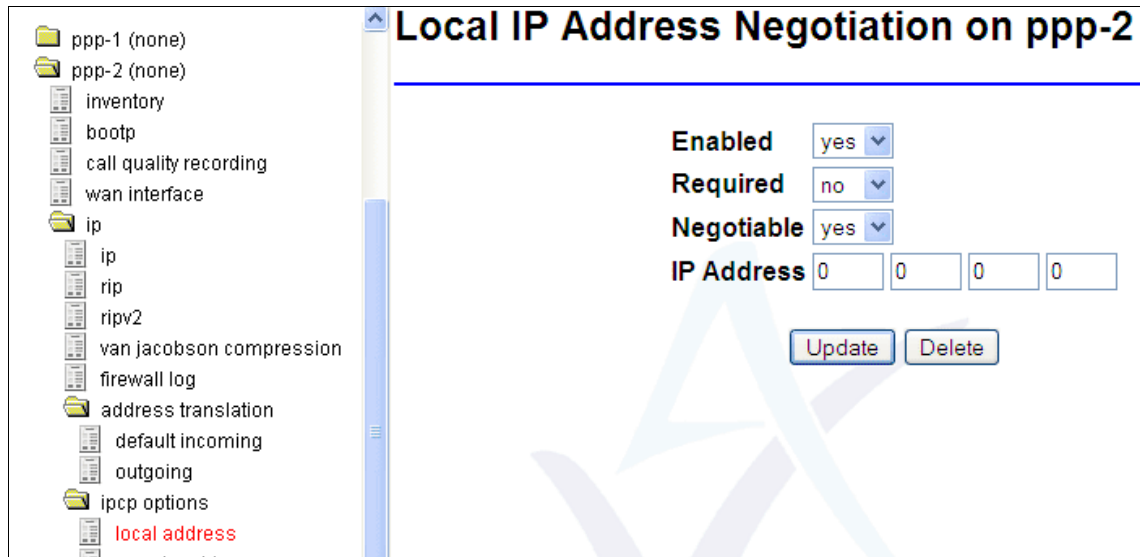


Figure 6: The local IP address page

Field name	Description	Command Line
Enabled	Enables or disables local IP address negotiation on the local end of the link. Set Enabled to yes .	Set Ppp Interface Local Option Ipcp Address Enabled
Required	Specifies whether or not negotiation of the local IP address is required. Set Required to no .	Set Ppp Interface Local Option Ipcp Address Negotiation Required Enabled
Negotiable	Indicates whether the IP address is negotiable or not negotiable. Set Negotiable to yes .	Set Ppp Interface Local Option Ipcp Address Negotiable Enabled
IP Address	If negotiation is enabled, enter the IP address to use for local IP address negotiation. Enter the IP address in dotted decimal notation: 0.0.0.0 .	Set Ppp Interface Local Option Ipcp Address Value

Table 3: The local IP address negotiation on ppp page fields and their descriptions

Click **Update**. The Configuration Update Result page appears.

In the Expert View menu, select **interfaces -> ppp-2 -> ip -> ipcp options -> local primary dns**. The Local Primary DNS Negotiation page appears.

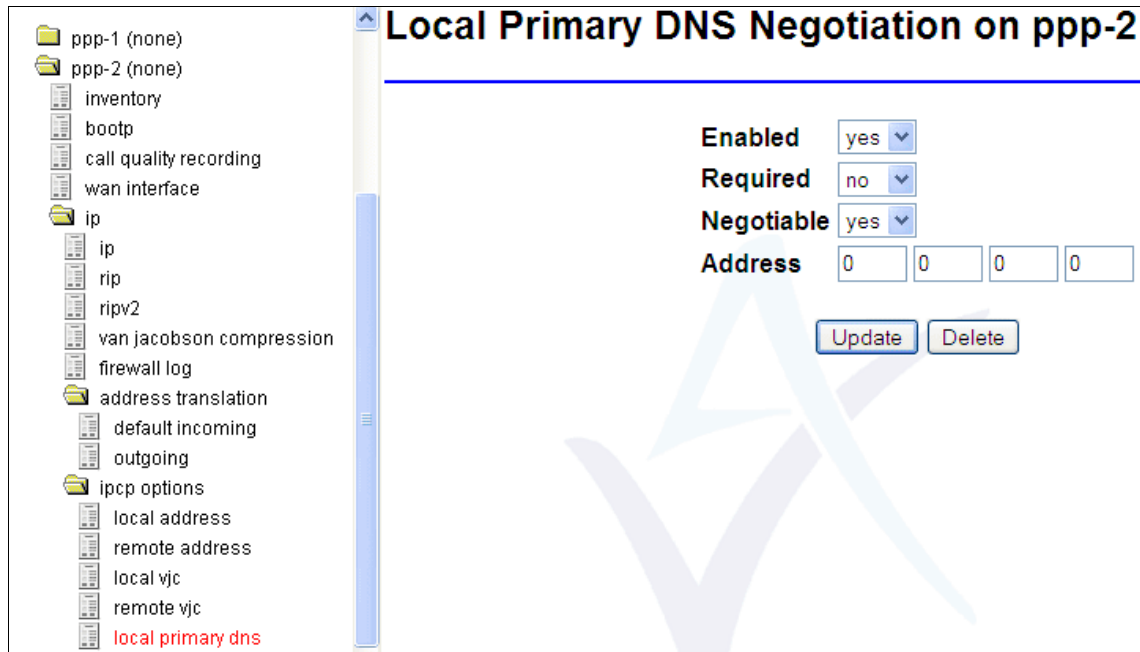


Figure 7: The local primary DNS page

Field name	Description	Command Line
Enabled	Enables or disables negotiation of the primary DNS IP address on the local end of the link. Set Enabled to yes .	Set Ppp Interface Local Option Ipcp Primary Dns Address Enabled
Required	Enables or disables primary DNS negotiation on the local end of the link. Set Required to no .	Set Ppp Interface Local Option Ipcp Primary Dns Address Negotiation Required Enabled
Negotiable	Indicates whether primary DNS negotiation is negotiable or not negotiable by the local end of the link. Set Negotiable to yes .	Set Ppp Interface Local Option Ipcp Primary Dns Address Negotiable Enabled
IP Address	Enter the IP address of the primary DNS server to be used by the local end of the link. Setting the IP address to 0.0.0.0 is an explicit request that the remote end provides the address information. Type in 0.0.0.0 .	Set Ppp Interface Local Option Ipcp Primary Dns Address Value

Table 4: Fields in the local primary DNS page

Click **Update**. The Configuration Update Result page appears.

In the Expert View menu, select **interfaces -> ppp-2 -> ip -> ipcp options -> local secondary dns**. The Local Secondary DNS page appears.

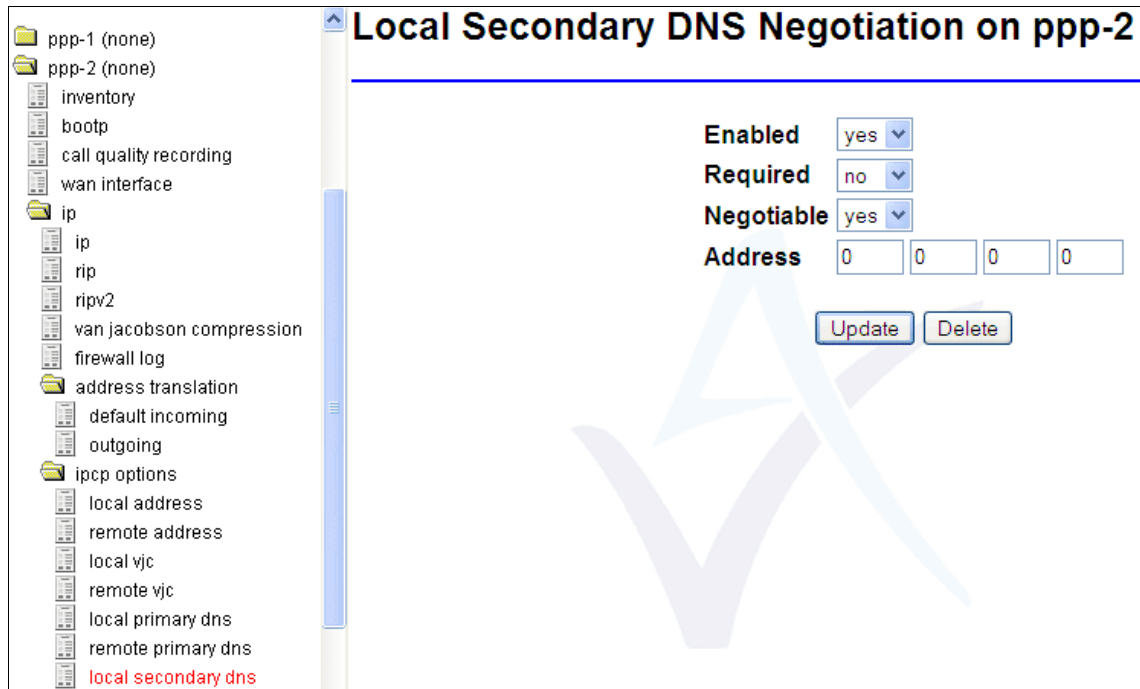


Figure 8: The local secondary DNS page

Field name	Description	Command Line
Enabled	Enables or disables negotiation of the primary DNS IP address on the local end of the link. Set Enabled to yes .	Set Ppp Interface Local Option Ipcp Secondary Dns Address Enabled
Required	Enables or disables primary DNS negotiation on the local end of the link. Set Required to no .	Set Ppp Interface Local Option Ipcp Secondary Dns Address Negotiation Required Enabled
Negotiable	Indicates whether primary DNS negotiation is negotiable or not negotiable by the local end of the link. Set Negotiable to yes .	Set Ppp Interface Local Option Ipcp Secondary Dns Address Negotiable Enabled
IP Address	Enter the IP address of the primary DNS server to be used by the local end of the link. Setting the IP address to 0.0.0.0 is an explicit request that the remote end provides the address information. Type in 0.0.0.0 .	Set Ppp Interface Local Option Ipcp Secondary Dns Address Value

Table 5: The local secondary DNS negotiation page fields and their descriptions

Click **Update**. The Configuration Update Result page appears. Proceed to section 3.3.5 to set the next configuration.

3.3.5 Configure the PPP interface

You must configure the ppp-n interface to send and receive data using the modem interface.

In the Expert View menu, select **interfaces -> ppp-n -> wan interface**. The PPP WAN interface page appears.

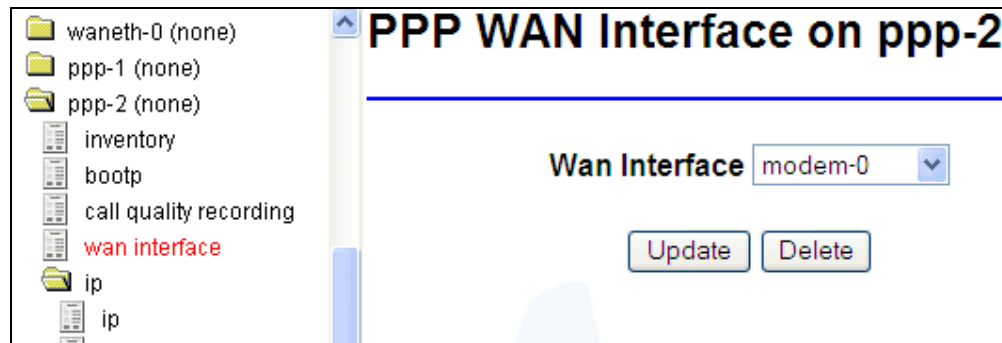


Figure 9: The WAN interface page

On the PPP WAN Interface on ppp-n page, select **modem (0)** from the Wan Interface drop-down list.

Click **Update**. The Configuration Update Result page appears. Proceed to section 3.3.6 to set the next configuration.

3.3.6 Select asynchronous PPP operation

The SMG allows asynchronous data transfer, which transfers data in both directions at different speeds.

In the Expert View menu, select **interfaces -> ppp-2 -> ppp -> ppp**. The PPP Interface page appears.

PPP Interface on ppp-2

Enabled yes

Maximum Receive Unit (MRU) 1524 bytes

Maximum Remote Receive Unit 1524 bytes

Periodic Authentication Timer 60 secs

Maximum Authentication Retries 3

IP Enabled yes

Bridging Enabled no

Time to Send LQR 0 secs

Send Time Remaining Enabled no

Send Identifier String Enabled no

Identifier String

Asynchronous Link Enabled yes

Primary DNS IP Address

Secondary DNS IP Address

ADSL Auto Disconnect Enabled no

Figure 10: The PPP interface page

To view the Asynchronous Link Enabled field, click **Advanced** to display all fields.

Field name	Configuration	Command Line
Enabled	Enables the ppp-2 interface. Set Enabled to yes .	Set Ppp Interface Enabled
Maximum Receive Unit (MRU)	The SMG sends the MRU to the end device or peer to inform it that the router can receive larger packets, or to request that the peer send smaller packets. Enter the MRU for the specified PPP interface. Minimum value is 512 bytes. Default/Maximum value is 1524 bytes.	Set Ppp Interface Maximum Receive Unit
Maximum Remote Receive Unit	The peer sends the Maximum Remote Receive Unit (MRRU) to the SMG to inform it that the remote router can receive larger packets, or to request that the peer send smaller packets. Enter the MRRU for the specified PPP interface. Minimum value is 512 bytes. Default/Maximum value is 1524 bytes.	Set Ppp Interface Maximum Remote Receive Unit
Period Authentication Time	Indicates the length of time, up to 3600 seconds, between successive attempts to authenticate the PPP peer associated with the selected PPP interface.	Set Ppp Interface Periodic Authentication Timer
Maximum Authentication	Indicates the maximum number of authentication retries after the first	Set Ppp Interface Maximum Number Of

Retries	authentication attempt fails. When the maximum number of retries is exceeded, the connection is terminated on the selected PPP interface. The maximum number of retries allowed is 64; the default is 3. Minimum value is 0 and maximum value is 64.	Authentication Retries
IP Enabled	Enables IP on the interface.	Set Ppp Interface Ip Enabled
Bridging Enabled	Enables or disables bridging negotiation and operation on the selected PPP interface.	Set Ppp Interface Stp Enabled
Time to Send LQR	Indicates the length of time in seconds to send the LQR. The maximum allowed is 3600 seconds; the default is 0 seconds.	Set Ppp Interface Time To Send Lqr
Send Time Remaining Enabled	Enables or disables the option to send a notice indicating the amount of time remaining for the connection on the selected interface.	Set Ppp Interface Send Time Remaining Enabled
Send Identifier String Enabled	Enables or disables the option to send an identifier string on the selected interface. When this option is enabled, enter the identifier string in the Identifier String field.	Set Ppp Interface Send Identifier String Enabled
Identifier String	Used to enter the identifier string when Send Identifier String Enabled is set to yes.	Set Ppp Interface Identifier String
Asynchronous Link Enabled	Enables the interface to communicate in asynchronous mode. Set Asynchronous Link Enabled to yes .	Set Ppp Interface Asynchronous Link Enabled
Primary DNS IP Address	Address of the primary DNS server.	Set Ppp Interface Dns Ip Address
Secondary DNS IP Address	Address of the secondary DNS server.	Set Ppp Interface Secondary Dns Ip Address

Table 6: The ppp interface page fields and their descriptions

On the PPP Interface on ppp-2 page, set Enabled to **yes**, and Asynchronous Link Enabled to **yes**. You can leave all other fields as the default settings.

Click **Update**. The Configuration Update Result page appears. Proceed to section 3.3.7 to set the next configuration.

3.3.7 Configure authentication options

In the Expert View menu, select **interfaces -> ppp-2 -> ppp->authentication->name and password**. The Name and Password page appears.

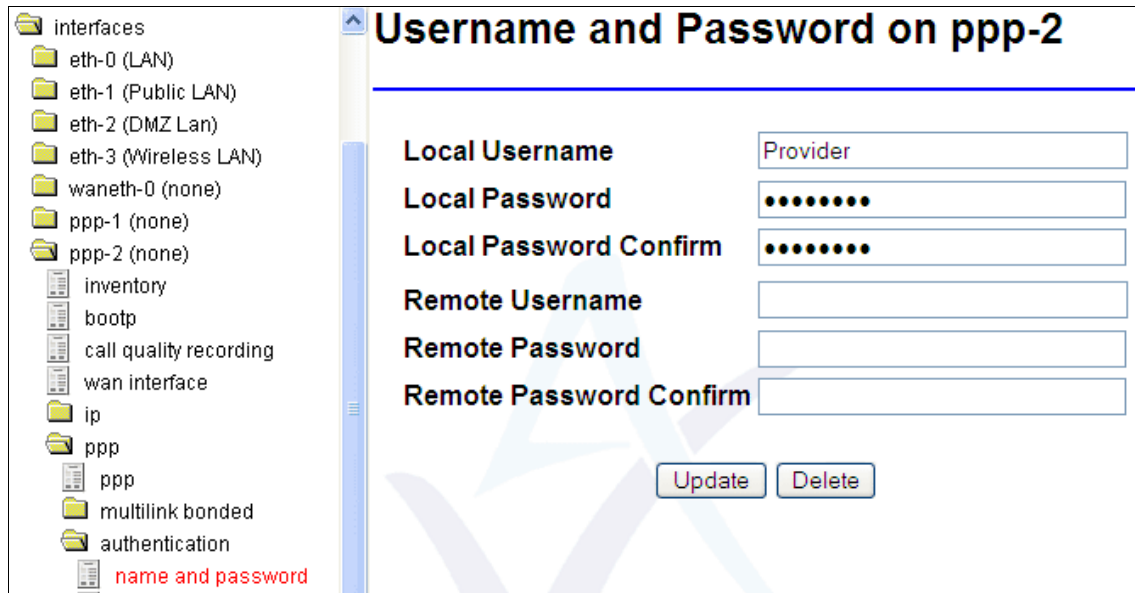


Figure 11: The username and password page

On the name and password page, set the local username and password.

Click **Update**. The Configuration Update Result page appears.

In the Expert View menu, select **interfaces -> ppp-2 -> ppp->authentication->send PAP**. The Send PAP Password page appears

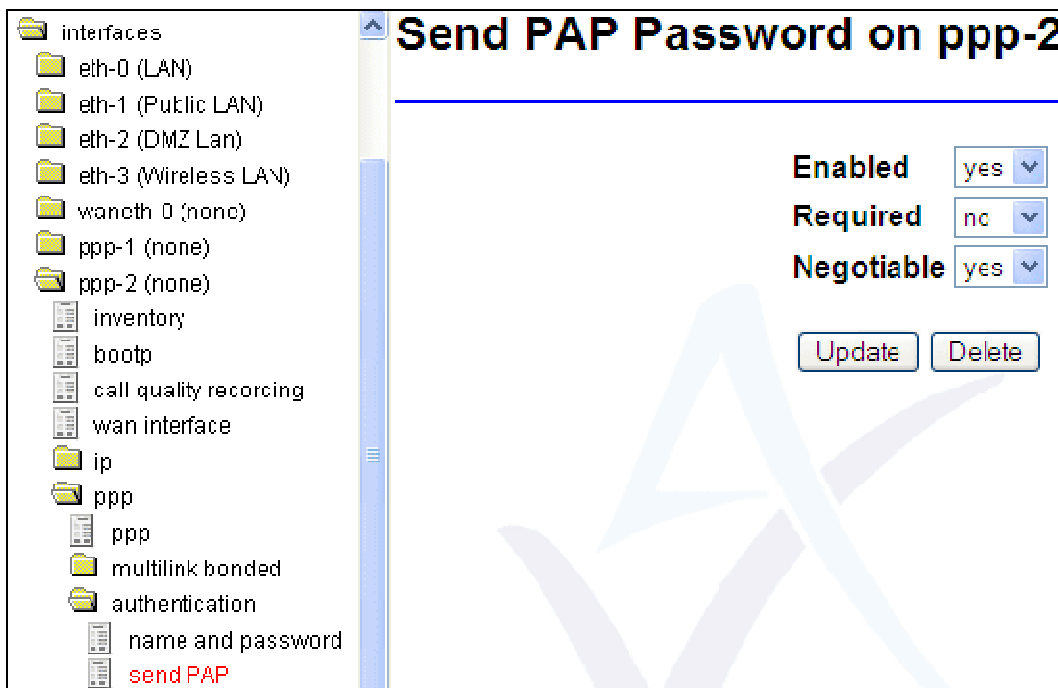


Figure 12: The send PAP password page

On the Send PAP page, set Enabled to **yes**, Required to **no**, and Negotiable to **yes**.

Click **Update**. The Configuration Update Result page appears.

In the Expert View menu, select **interfaces -> ppp-2 -> ppp->authentication->Send CHAP**. The Send CHAP Password page appears.

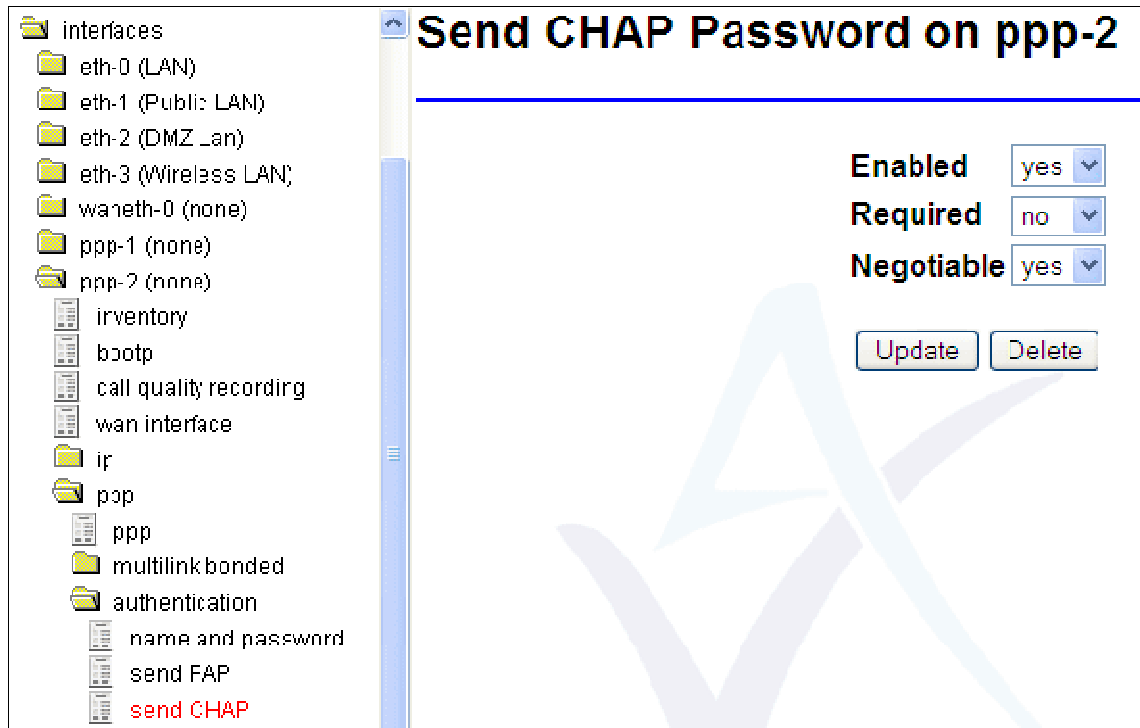


Figure 13: The send CHAP page

On the Send CHAP page, set Enabled to **yes**, Required to **no**, and Negotiable to **yes**.

Click **Update**. The Configuration Update Result page appears. Proceed to section 3.3.8 to set the next configuration.

3.3.8 Set dialling options

In the Expert View menu, select **interfaces -> ppp-2 -> call control -> call**. The Call Details page appears.

Call Details on ppp-2

Outgoing Call Destination Number

Outgoing Call Destination Subaddress

Incoming Call Remote Number

Incoming Call Local Number

ISDN Call Type

Permissions

Auto Connect Enabled

Inactivity Timer secs

Minimum Duration secs

Maximum Duration secs

Figure 14: The call details page

Field name	Configuration	Command Line
Outgoing Call Destination Number	To establish a connection to the Internet, type the phone number of your ISP.	Set Dial Neighbour Originate Address
Outgoing Call Destination Subaddress	Specifies the device's subaddress, or extension, if the call destination device has a subaddress defined. No spaces are allowed. ISDN only.	Set Dial Neighbour Originate Subaddress
Incoming Call Remote Number	Specifies the number of one of the locations that is allowed to place calls on this interface. No spaces are allowed. ISDN only.	Set Dial Neighbour Answer Address
Incoming Call Local Number	Specifies the device's local subaddress, or extension, if the call source has a subaddress defined. No spaces are allowed. ISDN only.	Set Dial Neighbour Received Called Address
ISDN Call Type	If using ISDN, defines the call type.	Set Dial Neighbour Call Type
Permissions	Assigns the SMG permissions to call, answer, call and answer, or call back. Select Call .	Set Dial Neighbour Permission
Auto Connect Enabled	Allows the V90 modem to bring up the link automatically when the SMG is restarted. Set to no .	Set Dial Neighbour Call Autoconnect
Inactivity Timer	Period of inactivity elapsed before the call connection is disconnected. Set to 0 to stay up permanently.	Set Dial Neighbour Inactivity Timer
Minimum Duration	Minimum connection time before the inactivity timer becomes active.	Set Dial Neighbour Minimum Duration
Maximum Duration	Maximum time that the connection should be maintained.	Set Dial Neighbour Maximum Duration

Table 7: The call details on ppp-2 fields and values

Click **Update**. The Configuration Update Result page appears. Proceed to section 3.3.9 to set the next configuration.

3.3.9 Configure the modem interface

In the Expert View menu, select **interfaces -> modem-0 -> modem interface**. The Modem Interface page appears.

The modem is set to US country code by default. To change the required country code, on the Modem Interface on modem-0 page, click **Advanced**.

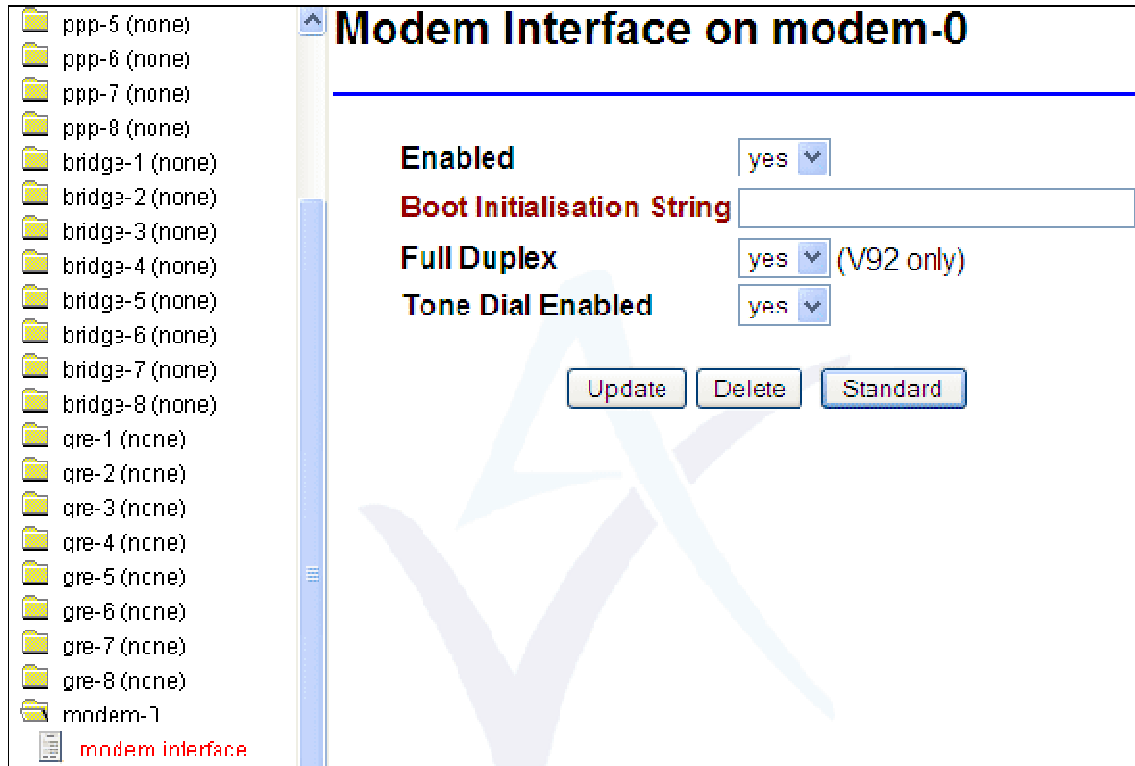


Figure 15: The modem interface on modem-0 page

Set Enabled to **yes**.

To set the appropriate country code, type in boot initialised string using the country code shown in Table 8.

Use ; (semi-colon) to separate multiple commands.

Field name	Description	Command Line	
Enabled	Specifies if the modem interface is enabled. Select yes .	Set Modem Interface Enabled	
Boot Initialisation String	Defines an initialisation string that is sent to the modem on boot. Set the field to a string with:	Set Modem Interface Boot Initialization String	
	US value		Default
	UK value		at+gci=B4;
	Japan value		at+gci=00;
	Multiple command	at+gci=B4;+vcid=1;v0w2e0	

	example	
Full Duplex	Enables full duplex mode for modem connections. Select yes .	Set Modem Interface Full duplex Enabled
Tone Dial Enabled	Enables DTMF tones for dialling otherwise pulse dial is used. Select yes .	Modem Interface Tone Dial Enabled

Table 8: The modem interface on modem-0 fields and values

Click **Update**. The Configuration Update Result page appears.

When you have committed all the necessary configurations, you can batch-save your configuration changes.

4 Saving your configurations

In the Configuration Update Result page, click **saved to flash**.

Configuration Update Result

Status Configuration committed successfully

Errors None

Save Changes will be lost unless [saved to flash](#)

Reboot? The system must be [reloaded](#) before all changes will come into effect

[Return to previous page](#)

Figure 16: The configuration update results page

The Save Configuration to Flash page appears.

Save Configuration to Flash

The last flash configuration loaded was **config1**.
When the system is next rebooted, **config1** will be loaded.

Some of your [recent changes](#) have not yet been saved to flash.

Save Committed Changes To

Config 1 ▾

Config 1

Config 2

Alternate Config

Figure 17: The save configuration to flash page

In the drop-down menu select the config you want to save changes to and click **Save**.

There are 3 options to save to:

- Config 1
- Config 2
- Alternate Config

It is good practice to save to Alternate Config in case your committed configurations are unsuccessful.

If you select a different config option to the existing config, you will need to change the boot config to reload into the correct config.

4.1 Reload the configuration

In the Expert View menu, select **set boot configuration**.

In the drop-down menu, select the config option you have chosen to save to.

Click **Select**.

Next Boot Configuration

The currently active configuration is config1.

Configuration to use at next boot

Select Reset Form

Config 1
Config 1
Config 2
Alternate Config
Factory Config

Figure 18: Next boot configuration page

4.2 Using the modem as a backup WAN interface

The V90 modem can be used as a backup WAN interface. For example, if PPP-x is configured as the primary WAN interface using ADSL and becomes un-operational for longer than a specified amount of time, an outgoing PPP connection is established on PPP-y which has been configured as backup.

For more information on configuring the modem as a backup WAN interface, read 'How to Use the Backup Script' in the SMG full reference guide.

4.3 Caller ID restrictions

It may be necessary to restrict the modem to only answer dial calls from specific phone numbers or Calling Line Identifier (CLI).

5 Modem monitoring and diagnostics

5.1 Active data connections

When a modem call is established it can be monitored using the Active Data Connections applet. To view the Active Data Connections monitor, on the SMG Start page select **Status** -> **Active Data Connections**. The following information is available for monitoring:

Field name	Field description
Interface name	Descriptive PPP interface name (e.g. "PPP-1 Testing")
Interface port	PPP-n (n – PPP interface number)
Interface address	xxx.xxx.xxx.xxx – ppp interface address
Call Direction	Incoming or outgoing call direction
Connection Type	Modem
State	
Channels in use	
Called number	Called party number for outgoing call direction
Called sub-address	
Calling number	Calling party number for incoming call direction
Calling sub-address	
Connect time	Call establishment data and time
Duration	Call current duration
Transmitted packets	Number of transmitted packets
Transmitted bytes	Number of transmitted bytes
Received packets	Number of received packets
Received bytes	Number of received bytes
Initial IP source	
Initial IP destination	

5.2 Call history

V90 modem historical usage can be monitored using the Call History applet.

On the Fast.Start page, select **Status** -> **Call History**. Click the desired day and hour, or click **zoom in** if you need to see a more detailed view of the history. The detailed call view includes the following fields:

Field name	Description
Interface	PPP interface. For example, PPP-1.
Title	Interface descriptive name. For example, Testing.
Duration	Call duration.
Connect	Date and time the connection was established.
Disconn	Date and time the connection was terminated.
Channel	Local interface. For example, modem-0.
Called no	Called number for outgoing calls
Source IP	
Destination	
Protocol	

Data In	Number of bytes and packets received
Data Out	Number of bytes and packets received
Cause	Termination cause. For example, Normal clearing.

5.3 Connection monitor

The Connection Monitor enables you to view the current status of IPCP, CHAP/PAP and LCP protocol, as well as modem data status.

On the Fast.Start page, select **Advanced** -> **Connection Monitor**. Then select **Modem Interface**.

	P1	P2	P3	P4	P5	P6	P7	P8
IPCP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CHAP/PAP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LCP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Modem

The boxes represent the current status of the monitored entities.

<input checked="" type="checkbox"/>	Active	<input type="checkbox"/>	Inactive
<input checked="" type="checkbox"/>	Error	<input type="checkbox"/>	Unconfigured

5.4 Modem events

You can use the SMG web trace applet to monitor the log of modem-related events.

To access the trace analyzer, on the Fast.Start page, select **Advanced** -> **Diagnostics**. Click **Trace Analyzer**. The Trace Analyzer pop-up window appears.

To select custom events, check Custom Events and click **Select**. The select events to trace pop-up window appears.

In the scroll-down Events Available menu, select **MODEM** to the list of selected events. Click **ADD** and then click **OK** to start the trace. The modem call events appear in the trace window.

Time	Class	Severity	Dir	Details
11:44:44	MODEM	INFO		Modem: Dial (904121288284128)
11:44:44	MODEM	DEBUG	Out	Modem Tx: atv0w2e0
11:44:44	MODEM	DEBUG	In	Modem Rx: 0
11:44:44	MODEM	DEBUG	Out	Modem Tx: ats7=30dt904128078284128
11:45:13	MODEM	DEBUG	In	Modem Rx: 64
11:45:13	MODEM	INFO		Modem: Outgoing Call Connected 28800 bps
11:45:34	MODEM	INFO		Modem: Outgoing Call Local Disconnect
11:45:35	MODEM	DEBUG	In	Modem Rx: .)#!)4)1) }\$eg.3
11:55:07	MODEM	INFO		Modem: Dial (904121288412128)
11:55:07	MODEM	DEBUG	Out	Modem Tx: atv0w2e0
11:55:08	MODEM	DEBUG	In	Modem Rx: 0
11:55:08	MODEM	DEBUG	Out	Modem Tx: ats7=30dt904128078284128
11:55:37	MODEM	DEBUG	In	Modem Rx: 64
11:55:37	MODEM	INFO		Modem: Outgoing Call Connected 28800 bps

Figure 19: The trace analyzer window

5.5 Modem events list

The following table lists common modem events.

Severity	Text	Description
INFO	Dial (<called number>)	Outgoing modem call in progress to called number.
INFO	Incoming Ring	Incoming ring signal detected by modem interface on the line.
INFO	Incoming Call Answering	SMG answered the incoming modem call, connection negotiation in progress.
INFO	<Incoming Outgoing >Call Connected <DCE speed>	Modem call connected with displayed line speed in bits per second.
NOTICE	<Incoming Outgoing >Call Failed <DCE reason>	Modem call failed to establish. DCE reason is given, for example, NO DIALTONE.
NOTICE	Dial failed (<reason>). Retrying (n)	Outgoing modem call dial failed. DCE reason is given, for example, BUSY and a dial command is being re-tried, n is the retry number.
NOTICE	Dial Failed (outgoing calls not allowed)	Outgoing dial did not proceed, because the PPP port permission is not set to make outgoing calls
NOTICE	Dial Failed (no number configured)	Outgoing dial did not proceed because the PPP port dial neighbour originate address (called number) is not configured.
INFO	<Incoming Outgoing >Call Local Disconnect	Modem call has been locally terminated.
INFO	<Incoming Outgoing >Call Remote Disconnect <reason>	Modem call remotely terminated. DCE reason is given, for example, NO CARRIER.