

**Series 5000**  
**ADSL Modem / Router**  
**Firmware Release Notes**

Document Number: 0013-001-000201

Version: 1.2 (03 February, 2011)

Firmware Version: v1.44

## **Documentation Control**

Generation Date: February 4, 2011

**Copyright © 2011 Cybertec Pty Limited**

**All rights Reserved.**

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Cybertec Pty Limited.

Cybertec Pty Limited has intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Cybertec Pty Limited, the furnishing of this document does not give you any license to this intellectual property.

## Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
<b>2</b>	<b>Version</b>	<b>4</b>
<b>3</b>	<b>Applicability</b>	<b>4</b>
<b>4</b>	<b>Version 1.44 (03/02/2011)</b>	<b>5</b>
4.1	General . . . . .	5
4.2	New Features . . . . .	5
4.3	Enhancements . . . . .	5
4.4	Bug Fixes . . . . .	5
4.5	Known Issues . . . . .	5
<b>5</b>	<b>Version 1.43 (23/11/2010)</b>	<b>6</b>
5.1	General . . . . .	6
5.2	New Features . . . . .	6
5.3	Enhancements . . . . .	6
5.4	Bug Fixes . . . . .	6
5.5	Known Issues . . . . .	6
<b>6</b>	<b>Version 1.42 (25/10/2010)</b>	<b>7</b>
6.1	General . . . . .	7
6.2	New Features . . . . .	7
6.3	Enhancements . . . . .	7
6.4	Bug Fixes . . . . .	7
6.5	Known Issues . . . . .	7
<b>7</b>	<b>Version 1.41 (25/06/2010)</b>	<b>8</b>
7.1	General . . . . .	8
7.2	New Features . . . . .	8
7.3	Enhancements . . . . .	8
7.4	Bug Fixes . . . . .	8
7.5	Known Issues . . . . .	8
<b>8</b>	<b>Version 1.40 (23/04/2010)</b>	<b>9</b>
8.1	General . . . . .	9
8.2	New Features . . . . .	9
8.3	Enhancements . . . . .	9
8.4	Bug Fixes . . . . .	11
8.5	Known Issues . . . . .	11

- 9 Version 1.32 (24/08/2009) 12**
  - 9.1 General . . . . . 12
  - 9.2 New Features . . . . . 12
  - 9.3 Enhancements . . . . . 12
  - 9.4 Bug Fixes . . . . . 12
  - 9.5 Known Issues . . . . . 12
  
- 10 Firmware Upgrade Procedure 13**
  - 10.1 Connect to the Web interface . . . . . 13
  - 10.2 System Backup and Upgrade . . . . . 14

## **1 Introduction**

This document provides a summary of the firmware changes and details the firmware upgrade procedure for the Cybertec Series 5000 ADSL Modem / Routers.

## **2 Version**

The latest version of the Series 5000 firmware is: v1.44.

The firmware file for the current release is: S5000-v144.upg

## **3 Applicability**

The firmware described in this document is applicable for all Series 5000 models

## **4 Version 1.44 (03/02/2011)**

### **4.1 General**

- This is a bug fix release.

### **4.2 New Features**

- No new features.

### **4.3 Enhancements**

- No enhancements.

### **4.4 Bug Fixes**

- Fixed issue where Openswan could not correctly identify required interfaces and would fail on start-up.
- GRE - A keepalive reply is no longer sent on start-up, it now waits for the first keep alive request.
- VRRP page now shows a blank option if the GRE tunnel previously used has been deleted.
- The dyn dns password now accepts standard character set.
- Resolved residual error messages seen when the ADSL interface was disabled on boot.
- Added PPPoE connection attempt re-try after timeout.

### **4.5 Known Issues**

- No known issues.

## **5 Version 1.43 (23/11/2010)**

### **5.1 General**

- This is a bug fix release.

### **5.2 New Features**

- No new features.

### **5.3 Enhancements**

- No enhancements.

### **5.4 Bug Fixes**

- DHCP Server
  - The DHCP server now includes the DNS search domain (DSN Suffix) in its DHCP information.
- VRRP
  - Configuration changes not correctly applied. Fixed.
- GRE
  - tunnels do not bring up static routes correctly. Fixed.
  - tunnels may change interface id when the device is rebooted. Fixed

### **5.5 Known Issues**

- No known issues.

## **6 Version 1.42 (25/10/2010)**

### **6.1 General**

- This release includes several enhancements and bug fixes.

### **6.2 New Features**

- No new features.

### **6.3 Enhancements**

- GRE Tunnels
  - Support for keep-alives added.
- VRRP and GRE integration
  - GRE tunnel status integrated with VRRP to allow for tunnel switch-over.
- Serial server
  - Enable TCP No Delay option has been added to the Serial Server.

### **6.4 Bug Fixes**

- Time change reboot.
  - A change in the system time of more than 100 seconds causes the unit to reboot. Fixed.
- Negative temperatures displayed incorrectly.
  - Negative temperature incorrectly displayed, eg -1.4C was displayed as -1.-40. Fixed.
- Web server
  - The IPsec configuration page is slow to update. Fixed.
  - Web pages do not display correctly on webkit browsers. Fixed.

### **6.5 Known Issues**

- No known issues.

## **7 Version 1.41 (25/06/2010)**

### **7.1 General**

- This release is a bug fix release.

### **7.2 New Features**

- No new features.

### **7.3 Enhancements**

- Power on/off sequence improved
  - The power on/off sequence has been enhanced.
  - Power on sequence changes improves boot time.
  - Improved power off sequence allows for faster network connection on next boot.
- IPsec
  - Allow IPsec to be configured with XAUTH and rekeying at the same time.

### **7.4 Bug Fixes**

- Serial Server
  - The pulldown options for Serial Server's (config/serial-server.asp) Immediate send character matching field were incorrect. The options presented:
    - Override
    - Follow carrierchanged to:
    - Off
    - Match any character
    - Match all characters

### **7.5 Known Issues**

- No known issues.

## 8 Version 1.40 (23/04/2010)

### 8.1 General

- This release includes new features, several enhancements and bug fixes.

### 8.2 New Features

- Capability to establish a PPP connection using an external modem added to Serial Server.
  - This feature allows a unit to establish a PPP connection using an external modem connected to a serial port.
- Ethernet MAC Address filter.
  - Filter allows MAC addresses to be accepted or rejected.
  - Default policy can be set to allow or deny.
- Alias IP address can be enabled using configuration reset switch.
  - Pressing the configuration reset switch for approximately 2 seconds will enable an aliased IP at the default IP address setting.
  - This feature enables access to the unit when the IP is not known.
  - The Ethernet ports must be enabled for this feature to work.
- Unit can be powered down using configuration reset switch.
  - Pressing and holding the configuration reset switch will cause the unit to disconnect from the network and power down.
  - This feature is provided to shutdown the network connection prior to removing power.
  - If the power is not removed from the unit it will power on again after 60 seconds. This provides a recovery mechanism should the power down be accidentally activated.
- Generic Routing Encapsulation (GRE) support added.
  - Up to 5 GRE tunnels can be configured.

### 8.3 Enhancements

- Power controller power off maximum offset added.
  - An off time offset has been added to the power controller. This value only has meaning if the unit has been powered off by the power controller and then during the off time the power to the unit is removed and then re-applied. When the power is re-applied the unit will re-boot and then check if the current time indicates the unit should be off. The previous behaviour was to shutdown if the current time was prior to the “on” time. The option adds an offset time which by default is 5 minutes. If the “on” time will be within the offset time then the modem will not turn off but will remain on.
- Web Pages
  - Status alarms for non active services are now shown in the background colour. The previous colour was to display the background in green which could indicate the service was active thus causing confusion.
- System log automatically scrolls to last entry.
  - The system log web page now automatically scrolls to the last entry. It is common for a user to be interested in the last file entries. This saves the user from scrolling to the end of the log each time it is selected.

- Serial Server
  - PPP Dial-out client added.
- IPsec Virtual Private Network (VPN) improvements.
  - The IPsec “tab” on the web page is now the first tab so it is the default VPN page.
  - The name of the IPsec tab has been changed from “IPsec VPN” to “IPsec”.
  - The default for IPsec was changed from Enabled to Disabled.
  - Check-box added to overwrite MTU on General Configuration page.
  - General IPsec Configuration defaults set to the following:
    - NAT traversal enabled
    - Overwrite MTU disabled.
  - “General Configuration” page added.
  - Tunnel can now be configured to be either an Initiator or Responder.
  - Phase 1 Encryption - IKE proposal defaults set to AES(128) SHA1 DH Group 2.
  - Phase 2 Configuration - Phase 2 Encryption defaults set to the following:
    - ESP proposal: AES(128)-SHA1
    - Perfect forward secrecy & group : Enabled with DH Group 2.
    - Key lifetime: 480 mins.
  - Dead Peer Detection (DPD) moved to “Tunnel options” configuration page.
  - Dead Peer Detection (DPD) action on failure supports the following:
    - None
    - Hold
    - Clear (Default for Responder)
    - Restart (Default for Initiator)
    - Restart by peer
  - Default to not use shared certificates. Previously the default was to use shared certificates.
  - Tunnel Network configuration moved from Phase 2 page to a separate page.
  - Tunnel Networks - Network option “None (Host only)” removed and replaced by 2 more explicit options:
    - Host only (WAN IP)
    - Host only (LAN IP)
  - Support for Xauth.
    - XAUTH provides an additional level of authentication by allowing the IPsec responder to request extended authentication from remote users. Before being allowed access to the VPN remote users are required to respond with their credentials.
  - VPN log automatically scrolls to last entry.
    - The VPN log web page now automatically scrolls to the last entry. It is common for a user to be interested in the last file entries. This saves the user from scrolling to the end of the log each time it is selected. This feature works in the same way as the System log scroll and was added for consistency.
- Firewall
  - Custom NAT - Added check box to “Drop traffic to original target”.

## 8.4 Bug Fixes

- IPsec
  - Traffic destined to be sent over the tunnel could block if a transmission attempt was made prior to the tunnel initialisation. This has been fixed for both Initiator and Responder modes.
  - Timeout problems when using Greenbow client have been resolved.
- Web Server
  - Web Server fails to respond. The Web Server was found to block under certain conditions, this has been fixed.

## 8.5 Known Issues

- No known issues.

## **9 Version 1.32 (24/08/2009)**

### **9.1 General**

- First Series 5000 production release.

### **9.2 New Features**

- No new features.

### **9.3 Enhancements**

- No enhancements.

### **9.4 Bug Fixes**

- No Bug fixes

### **9.5 Known Issues**

- No known issues.

## 10 Firmware Upgrade Procedure

The firmware upgrade procedure for the /ctpfullname / is described. The same procedure can be used for all models in the product range.

### 10.1 Connect to the Web interface

- Connect to the Web interface of the modem either via the Ethernet interface or the wireless interface if web access is enabled.
- If connecting via the Ethernet interface:
  - Connect an Ethernet cable between the modem and the PC which will be used for the upgrade.
  - Open a web browser on the PC and enter the IP address of the LAN address of the modem. Note: The IP address of the modem may be configured differently for each installation. The default IP address is 10.10.10.10
- If connecting via the wireless interface:
  - Open a web browser on the PC and enter the IP address of the wireless interface.
- When prompted supply the username and password.
- The main status page should now be displayed.
- If the main page is not shown check:
  - If using the Ethernet interface:
    - The Ethernet cable is connected correctly to the modem and the PC.
    - The IP address of the modem is correct.
    - The Ethernet ports are enabled.
  - If using the wireless interface:
    - The wireless IP address is correct and is publicly accessible.
    - The firewall rules have been set to allow wireless web access.

## 10.2 System Backup and Upgrade

- Select System ▸ Backup & Upgrade. The System Backup & Upgrade page will be displayed as shown in Figure 1.



Figure 1: The System Backup & Upgrade page.

### 10.2.1 Backup Configuration

- It is recommended to save the current configuration file.
- The configuration of the modem is forward compatible. This means the configuration of the modem will still be correct after a firmware upgrade to a later version even though the format used to store the configuration may be changed.
- The configuration of the modem is not always backward compatible. This means that if the modem firmware is replaced with an earlier version the configuration file may not be readable by the earlier version of firmware and so the configuration will revert to the default settings. If the configuration file from the earlier version was saved prior to the upgrade then this configuration can be loaded into the modem to restore the previous settings after reverting to the earlier revision of firmware.
- To save the configuration click the link in the section titled “Backup current configuration” as shown in Figure 2 and save the file to the local machine.



Figure 2: System configuration backup.

- To restore a configuration click the Browse button in the section title “Restore a saved configuration” as shown in Figure 3 then click the Upload button.

Restore a saved configuration	
Select configuration file	<input type="text"/> Browse...
Upload	

Figure 3: System configuration restore.

### 10.2.2 Firmware Upgrade

- In the section titled “UpgradeSeries 5000 firmware” click the Browse button and navigate to and select the upgrade file appropriate for the series of modem being upgraded as shown in Figure 4. The firmware file for the current release is: S5000-v144.upg
- If the incorrect file is selected the upload will fail and report an error.

Upgrade Series 5000 firmware	
Current firmware version	1.32
Select upload file	00-images/S5000-v144.upg Browse...
Upload	

Figure 4: Select the upgrade file.

- Click the Upload button. The file will now be transferred to the modem.
- When the upload is complete the Upgrade section of the page will change to be similar to that shown in Figure 5.

Upgrade Series 5000 firmware	
Status of uploaded file	Passed
Filename	series-5000-v144.img
Release	1.44
Build date	03/02/2011
Upgrade	Cancel Upgrade

Figure 5: File has been uploaded to the modem.

- Check that the information shown is correct.
- If the data is correct click the “Upgrade” button.



Once the Upgrade has started power must be maintained to the modem to prevent corruption of the Flash memory.

---

- The Upgrade section of the page will now show a message as shown in Figure 6.

<b>Upgrade Series 5000 firmware</b>	
The Series 5000 is now starting the upgrade.	
The upgrade will take several minutes to complete and the modem will be offline during this time.	
The modem will reboot once the upgrade is complete.	

Figure 6: The Upgrade page.

- During the upgrade:
  - the top two front panel LEDs will flash alternatively Red then Green.
  - the modem will disconnect from the wireless network.
  - the modem will not respond to any network traffic.
  - the modem will re-boot when the upgrade has completed
- When the Upgrade has completed and the modem has re-booted the new firmware version can be checked in the System Information page. Figure 7 is an example of the System Information page after the upgrade has completed. Note only the Application Version is shown.

### System Information

<b>Series 5000 Information</b>	
Model	5100
Serial Number	
Application Version	1.44
Bootloader Version	
<b>Hardware Addresses</b>	
LAN MAC	
DSL Software Version	

Figure 7: The System Information page after the upgrade.

Cybertec Pty Limited  
ABN 72 062 978 474  
Unit 11, 41-43 Higginbotham Road  
Gladesville NSW 2111  
Australia  
Phone: +612 9807 5911  
Fax: +612 9807 2258  
[www.cybertec.com.au](http://www.cybertec.com.au)

**CYBERTEC**