



**Efficient Networks 5800 Business Class Routers**  
**Firmware version 5.3.80 (March 11, 2002)**

**INTRODUCTION:**

Thank you for choosing **Efficient Networks** as your solution for Internet access.

The following documents are provided to help you with the setup and configuration of your product:

- Customer Release Notes (this document – supercedes the copy on the release CD)
- User Reference Guide (discusses hardware setup, Web Easy Setup application)
- Command Line Interface (CLI guide; on CD - covers console or Telnet use and advanced settings)
- Technical Reference Guide (on CD)

Important Note: Please, use the User Reference Guide. Refer to the other documents only if needed.

This document contains important information about your router and has the following sections:

- Hardware Compatibility
- Configuration Notes
- Key Changes in this Release
- Known Problems
- Documentation
- Technical Support

**HARDWARE COMPATIBILITY:**

This release note covers the following hardware models:

- 5851 SDSL (PN 120-5851-xxx)    5851 SDSL (PN 060-5851-xxx) w/ Rapid Secure HW
- 5861 ADSL (PN 120-5861-xxx)    5861 ADSL (PN 060-5861-xxx) w/ Rapid Secure HW
- 5865 ADSL / ISDN                    5871 IDSL

The software product numbers and DSLAMs supported are:

Standard	RapidSecure	DSLAM
5851-001	5851-035	SDSL ATM to the Nokia SpeedLink™ DSLAM (Covad)
5851-002	5851-038	SDSL ATM to the Nokia SpeedLink™ DSLAM
5851-004	5851-039	SDSL FR to the Copper Mountain DSLAM
5851-005	5851-031	SDSL Router pair for Point to Point to a second router
5851-006	5851-040	SDSL ATM to the Promatory/ Nortel UE IMAS DSLAM
5851-008	5851-041	SDSL ATM to the Lucent Stinger™, Lucent Anymedia™ DSLAM
5851-012	5851-042	SDSL ATM to the Newbridge Networks DSLAM
5851-015		SDSL ATM to the Paradyne DSLAM
5851-016	5851-043	SDSL ATM to the Promatory/ Nortel UE IMAS DSLAM (TMC)
5851-017	5851-044	SDSL ATM to the Lucent Stinger™ Autobaud DSLAM
5851-018	5851-045	SDSL ATM to the Nokia Stinger™ Autobaud DSLAM
5851-023	5851-037	SDSL ATM to the PairGain™ DSLAM
5851-034	5851-054	
5861-002	5861-008	ADSL G.DMT compatible DSLAMs
5861-004		ADSL G.DMT compatible DSLAMs (SBC)
5861-005		ADSL G.DMT compatible DSLAMs (SBC/Ameritech)
	5861-009	ADSL G.DMT compatible DSLAMs (Verizon)
	5861-010	ADSL G.DMT compatible DSLAMs (SBC)
	5861-012	ADSL G.DMT compatible DSLAMs (Covad)
	5861-016	ADSL G.DMT compatible DSLAMs (WorldCom)

## CUSTOMER RELEASE NOTES

	5861-017	ADSL G.DMT compatible DSLAMs (BellSouth)
	5861-018	ADSL G.DMT compatible DSLAMs (Qwest)
	5861-019	ADSL G.DMT compatible DSLAMs (Hanaro)
	5861-020	ADSL G.DMT compatible DSLAMs (Sprint)
	5861-021	ADSL G.DMT compatible DSLAMs (CE power cord)
	5861-022	ADSL G.DMT compatible DSLAMs (UK power cord)
	5861-023	ADSL G.DMT compatible DSLAMs (AU-NZ power cord)
	5861-024	ADSL G.DMT compatible DSLAMs (Danish power cord)
	5861-025	ADSL G.DMT compatible DSLAMs (Telephonica power cord)
	5861-026	ADSL G.DMT compatible DSLAMs (Swiss power cord)
	5861-027	ADSL G.DMT compatible DSLAMs (France Telecom)
5861-101	5861-108	ADSL G.DMT compatible DSLAMs (Alcatel firmware 3.6.70)
5865-001		ADSL G.DMT Annex B or ETSI compatible DSLAMS
5871-001		IDSL Adtran, AccessLAN, Cisco, Lucent, New Bridge, Nokia, Pulsecom, Promatory
5871-003		IDSL to the Copper Mountain DSLAM
5871-004		IDSL Adtran, AccessLAN, Cisco, Lucent, New Bridge, Nokia, Pulsecom, Promatory

The model and product numbers are displayed by the web GUI after connecting to the router.

### CONFIGURATION NOTES:

#### Test Light Blinking Heartbeat:

After the boot sequence is complete, the TEST LED blinks with the following pattern: 1.9 seconds "on" and 0.1 seconds "off", every 2 seconds. This feature is also known as a "heartbeat" and provides visual assurance that the router is functioning.

This device may be configured using several different methods:

- Using Easy Setup from a web browser connected to the router's default IP address of 192.168.254.254
- Using the Windows Quick Start application, which is installed from the Installation CD
- From the console port using the Command Line Interface (CLI) (requires console cable to be connected)
- From a Telnet session connected to 192.168.254.254, again using the CLI

#### Web Easy Setup GUI:

The simplest method is to use your web browser and connect to the router's built in Web Easy Setup application. Be sure to set your PC's IP driver to use DHCP to get an IP address from the router before trying to connect. If your PC is on a different LAN, type at a Window's DOS command prompt:

```
route add 192.168.254.254 x.x.x.x, where x is the PC's IP address.
```

To access the Web GUI, connect to 192.168.254.254 and use the username `login` and the password `admin`. Follow the prompts and enter the values provided by your Network Service Provider.

#### Security Caution:

DSL devices are always on by nature and can pose a data security risk if precautions are not taken. The router supports HTTP access for configuration changes and this can be a security risk if access is not controlled. The web GUI has a 'Change Access Control' button. You may wish to select 'Allowed from LAN' to stop access from the Internet (WAN). Telnet access and SNMP access can also be disabled. The CLI provides additional commands that support advanced access controls.

**An IP Packet Filter Firewall is included with your router but requires configuration.** There is a Set Firewall page on the Web GUI where you can select maximum, medium, minimum or no security from the web GUI. These filter sets are also provided in the `samples` directory on the Installation CD. Firewalls are discussed at length in the Command Line Interface document. Be sure to edit the file to fit your specific configuration and seek expert help if you are not familiar with security. IP filters only work if IP routing is enabled.

## Additional Software Tools:

A set of Microsoft Windows applications are on the Installation CD that allows you to configure the router, install new software versions, and set up other advanced options. There is also a Command Line Interface (CLI) that you may need to set up certain settings like host mapping, VRRP, IPX and optional features like L2TP.

## Sample configurations:

There are sample files with CLI configuration commands on the Installation CD in the directory called `samples`. These script files can be edited to fit your specific configuration and then copied to the router using the Quick Start application by clicking the Tools and Execute Script buttons.

## VPN Software Options:

IPSec, L2TP, DES and Triple DES are software options that can be enabled on your router. They must be purchased separately from your supplier and then activated. IPSec and the associated Internet Key Exchange (IKE) can be configured using the Web GUI or by using the CLI. L2TP is configured using the CLI. See the CLI document for details. Sample configuration files are provided in the `samples` directory.

## Network Address Translation (NAT):

This router has special feature code to support many applications through NAT.

The supported applications are: AOL chat, Cu SeeMe, Doom, FTP, L2TP, HTTP, Kali, Netbios over IP, Net Meeting, PCanywhere, PPTP, Quake, Quicktime Video, Real Audio, RTSP, SGI Media Base, SMTP, StreamWorks, Telnet, TFTP, Unix commands (finger, rcp, rshell, rlogin, whois), VDO.

Other applications that use IP or UDP protocols may have problems with NAT. You may be able to avoid this problem by running in TCP mode or by turning off NAT and running as a subnetwork to your ISP.

## KEY CHANGES IN THIS RELEASE:

### **Significant Changes in 5.3.80**

Unit replies to EOC messages in DSLAM in order based on ITU G.991.2.

-GUI Enhancements

LAN IP configuration has been added to the NAT page.

A configuration element has been added to the NAT page to enable or disable NAT passthru, for the support of multiple VPN PC clients.

A pop-up message has been added reminding users to reboot when the Ethernet LAN IP address has changed. This pop-up also states that now is a good time to change NAT settings.

We have added a text sentence to the `download.html` page that says 'Remember to rename the file after download completed.'

A new pop-up dialog appears to remind the user that a reboot is needed to establish new IKE settings.

### **Significant Changes in 5.3.71**

CERT Advisory CA-2002-03; 'Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)' has been addressed through recommended testing and found to have no vulnerabilities as identified in the CERT advisory.

### **Significant Changes in 5.3.70**

Buffer usage has been modified to support large output volumes to the system support trace web page.

When the local ID for a peer (with peer address set to 0.0.0.0) is looked up, the ID that is received in the request is compared to the peer ID stored in the aggressive mode policy. If a match is found, the corresponding local ID is returned in the reply.

IKE Phase One functionality with Cisco 3000 VPN has been augmented.

If bytes are found in the options section of a TCP/IP header that are not recognized as valid options, then an MSS option is not added. The function will simply return without modifying the packet.

The circuit re-training rate has been improved during the restoration of a DSL connection after using dial backup.

-CLI enhancements:

Multiple VPN clients can now be routed through a VPN server by using a new command:

```
system vpnpassthru <enable|disable>
```

enable- allows multiple VPN clients to route thru the box, disable (default) - only allows a single VPN client.

**Significant Changes in 5.3.60**

IPSec aggressive mode now replaces the peer address with the peer ID value in all replies to aggressive mode packets. This enhancement works with multiple tunnels.

IPSec filters are now updated after all SAs are read into memory.

In IPSec filters, the *inipsec* rule is added to the receive filter. The transmit filter has the *outipsec* rule with the source and destination address as the addresses behind that router that would get tunneled inside IPSec packets.

Password changes will now autosave, preserving the new password even if the router is turned off without a save command.

-CLI enhancements:

Added a command 'sdsl acttimer', to configure SDSL activation timeout. The timer can be set to 30 seconds, 52 seconds, or a variable value that depends upon the line rate. The slower the line rate, the longer the activation timeout interval. The command syntax is as follows:

```
sdsl acttimer [30s|52s|auto]
```

where the 30s, 52s, and auto are the valid arguments for this command.

The default value is 30 seconds. The help message and value of activation timer currently configured are displayed as shown in the below example if no argument is provided.

**Significant Changes in 5.3.50**

Copyright information has been updated.

Firmware has been upgraded to version 3.8.129 on all ADSL products except 5861-101, -108, 5865.

The opening of telnet sessions is restricted to one or fewer per second.

In addition to using the identifier and sequence number pair for NAT entry lookups, the router now stores the destination address in the NAT entry for the outgoing ICMP echo requests. This address is also used while doing the NAT entry lookup.

On model 5851 for the AnyMediaDSLAM, if Preactivation is unavailable, then autobaud post activation is turned off.

IPSec input and output filters now add only accept rules for protocol 50/51 (depending on what protocol is specified in the SA). The *inipsec* rule is added to the receive filter. The *outipsec* rule is added to the transmit filter with the source and destination address as the addresses behind that specific router that would get tunneled inside IPSec packets.

The 5851 Promatory models will now allow SDSL speeds of 256kbps and 512kbps to be selected.

- CLI enhancements:

Added a feature to the SDSL SPEED command that allows a user to enter up to three preferred speeds. Once these speeds are entered, the IAD will only attempt to train at these preferred speeds. This setting should shorten the time required by the IAD to find the correct line speed.

Usage:

```
sdsl speed <value in Kb/s> [ 192 256 384 512 768 1152 1536 1744
2320 ] | noauto
```

OR... to select up to three preferred rates:

```
sdsl speed <value1 in Kb/s> <value2 in Kb/s> [value3 in Kb/s]
```

To enable the Preferred Rate Mode, simply enter to or more valid speeds:

```
sdsl speed 256 512
```

Then to view the current selections, type the following to get the listing:

```
sdsl speed
```

To disable Preferred Rate mode just enter a single speed:

```
sdsl speed 512
```

You must type SDSL SAVE to store preferences.

-GUI enhancements:

An option to specify PPP-LLC has been added to the WAN Easy Setup and Quick.html pages.

**Significant Changes in 5.3.20**

The Phase 1 and Phase 2 delete SA messages are now handled for IPSec proposal lifetime expirations.

Added the proper if statement to allow PPPoE with bridging and the Ethernet interface.

- CLI enhancements:

Added a portscan command which is modeled on the ping command. This provides an ability to open a TCP socket for a specific TCP port to check for use.

Added one new command to make the RIP timer configurable:

```
system riptimer <seconds>
```

The default is thirty (30) seconds, the minimum value is fifteen (15) seconds.

**Significant Changes in 5.3.12**

Other features:

Telnet functionality has been improved in situations when two logical interfaces are used with NAT in a data path.

-GUI enhancements:

On SBC routers (5861-004, -005, -010) users can no longer set the password back to the default using the Web GUI. If the user tries to set the default password on the CLI or the Web GUI they will receive the same error message and the password will not be set back to the default. Additional information has been provided on the Change Password screen.

**Significant Changes in 5.3.11**

Other features:

Management data can be routed in bridge mode using a management PVC different from 0\*38 as a host.

In routing mode, management data can be routed while the primary data PVC is routed.

The PPP Retry timer has been adjusted to allow an 8 second interval for PPP configuration requests once the timer expires. After the 8 second interval has elapsed, the timer will restart with its original value.

**Significant Changes in 5.3.10**

Other features:

Upstream data transmissions have been improved to guard against data packet loss.

**Significant Changes in 5.3.8**

Other features:

- CLI enhancements:

Traffic shaping commands are now accepted during the boot sequence.

-GUI enhancements:

Dial Backup Configuration in the Web GUI no longer requires DNS or IP addresses for ping validations.

In the Dial Backup Configuration pages, the Reset to Defaults button now clears the IP addresses DNS box, if it has been checked previously.

**Significant Changes in 5.3.5**

Firewall help pages are updated.

IPSec can now be configured without IKE.

IPSec passthrough support has been added. Note: Support does not allow multiple clients to access the same server simultaneously.

IKE filters are no longer inserted if IKE policies are not defined.

A mode was added which requires the customer to change the administrator password when logging in via the console, Telnet, Web or Configuration Manager. It is not possible to change the password back to the factory default setting (5861-010 only). A problem was fixed that caused a data-only router to reboot if presented with non-AAL5 ATM cells.

The router will now stop retransmitting TCP packets (on connections terminating at the router) after three minutes and will close the connection.

Other features:

- Autoexec.bat changes

**Significant Changes in 5.3.4**

Other Features:

- GUI Enhancements:

The GUI now connects/disconnects more efficiently.

The SECURITY button has been changed to PROFILE SETUP.

Various superfluous links across pages have been removed.

A Router Administration Password button has been added.

The DONE button on the Security page returns the user to the Main page.

Minor enhancements to the Tools page.

Descriptive text has been added to the Security page.

- Security:  
IPSec will now tunnel through NAT. ESP and AH packets will be passed without modification.

### **Significant Changes in 5.3.3**

#### Other Features:

- CLI Enhancements:  
DNS addresses are shown with the <ipifs> command.
- GUI Enhancements:  
A customized Web interface for the 5861-007 and 5865-002 products has been created. The interface displays the Efficient Networks logo and guides the user through configuration of the PPP setup for connection to the ISP.  
PPP connection status is updated on the displayed web page.
- Firewall setting and reporting enhancements:  
Three firewall configurations have been provided. The firewall configurations are as follows:  
Maximum: Allows all outgoing TCP connections, PING responses from the router, NTP and DNS.  
Medium: Allows FTP data in addition to the above.  
Minimum: Does not provide packet filtering.  
A User Defined selection will run the filter script **user.txt** if it exists on the router.  
The firewall configuration can be selected from a web page added to the interface.
- DHCPDECLINE Message - Rather than removing the hostname and expiring the lease, the router will give the hostname a value of **\*\*\*Reserved\*\*\*** and keep the statically assigned address marked until the lease expires.
- DHCP default lease time (on KPN products 5861-007 and 5865-002):  
Autoexec.bat sets the default lease time to one (1) hour (minimum possible lease time).

### **Significant Changes in 5.3.2**

#### Bug Fixes:

- The Web GUI and CLI passwords are synchronized.
- Fixed a problem with Dial Backup and IDSL products.
- Firewall scripts now allow L2TP to the router.

### **Significant Changes in 5.3.1**

#### Command Line Interface enhancements:

- Alphabetized listing of command options.

#### Other Features:

- Added 3.7.121 Alcatel firmware.

#### Bug Fixes:

- AAL2 packets are handled gracefully.

### **Significant Changes in 5.3.x**

#### Web GUI enhancements:

- New DHCP page shows current active leases, setting of pool and enable/ disable.
- New NAT page allows NAT enable/ disable; and setting of in bound NAT entries (equivalent to system addserver commands) and display current values.
- New Diagnostic page can display values for: PPPoE, interface, routing table, ATM or TCP
- New Firewall filters page. Allows 4 canned filter sets to be run.  
Files maxsec.txt, medsec.txt, minsec.txt and nosec.txt must be pre-installed on router.

#### Other Features:

- MIB additions:  
New WAN types - ifType: Add values ipOverATM(114), rfc1483(159), sdsl(96)  
Set fpdownload.fpOnlineDownload = 6 allows execution of a script file on router

#### New commands:

- date MM/DD/YY - command to set date
- time HH:MM:SS - command to set time of day
- sntp enable|disable (see the CLI for sntp details)
- sntp prefServer, active, request, and server
- sntp offset <Minutes from UTC>
- ike commit [on|off|help] - sets the commit bit for traffic

- `ike start (or stop) <ipsec policy name>` - for ipsec debugging
- `remote setPPPRetryTimer <retryTimerValue> <remoteName>`  
where `<retryTimerValue>` is 0 for off (default) and 1 to 60 for random retry time

**Bug fixes**

- Prohibit script file (autoexec.bat) from running when boot recovery mode active
- Fix Interoperability issue with Netscreen 2.5.x

**Significant Changes in 5.1.5**

- For ADSL revise reset modem timer to close the WAN port in case the handshake fails. The timer is started when the modem tries to activate and is stopped after a successful activation, or expires, whichever comes first. After `<retries>` occurrences of this stuck condition (consecutive, or not), the modem is reset (and the retry count reset to 0)
- Change debug timeout command `'dmt to <seconds> min=30, max=3600, default=45'` (from 30 seconds to 1 hour per try)
- Add command: `'dmt retries <retries> min=1, max=10000, default=10'` (1 retry means reset after 1 instance of the modem being stuck)  
Changes take effect immediately and are not saved to flash.

**Significant Changes in 5.1.2**

- For ADSL add a 45 sec timer to close the WAN port in case the handshake fails to complete.
- If the above fails to work after 10 attempts, do a reset on the ADSL chip.
- Add a debug DMT timeout command - `dmt to x;` where x is 45 by default. This is not saved in flash.

**Significant Changes in 5.1.0**

- H.323 Network Address Translation support.  
This allows Microsoft NetMeeting™ and CuSeeMe to work over address translation.
  - Microsoft NetMeeting™ server support using `addserver tcp 1503` and `tcp h323` commands
  - Allow hostnames on the Ping and Traceroute commands. e.g. `ping www.yahoo.com`.  
The DNS server must be set in DHCP or learned from WAN or LAN. (`dhcp set value dns x.x.x.x`).
  - IP Filter type `Forward` has replaced the filter types `Receive` and `Transmit`
- Bug fixes:
- Fix memory leaks in Network address translation.
  - Fix memory leak when receiving a packet on an interface that needed an IP address.
  - Fix Web GUI memory leaks.
  - Do not send a bootp or DHCP requests out a stopped dod interface.
  - DSL firmware loaded by mistake in a dual-Ethernet router no longer hangs.
  - Add changes to make PPP and dial on demand processing more robust.
  - Repair problem where MLP link occasionally is stuck in the 'starting' state.

**KNOWN PROBLEMS:**

Netscape users may have trouble installing the Windows applications from the release CD from their browser. The work around is to do a Windows Start and Run `D:\dsltools\setup.exe` to run the installer, where D: is the CD rom drive.

For H.323 support the fast connect setup and the Gatekeeper (H.245) functionality are not supported. This affects Voice over IP usage for NAT configurations.

Some PPP systems do not completely support IP address negotiation. Communications with such systems can result in protocol hangs. The command: `remote setpppoptions reacqIPAddr off <remote name>` can be used to force the router to always request a new IP address whenever the PPP session is terminated, thus providing a work around until the software in the other systems has been changed.

MS Internet Explorer 4 does not honor the no cache option. Thus old values appear in the Web GUI rather than the current ones. You need to go to settings/internet options and set refresh to 'Every visit to the page' to see changed alues. This is not an issue with the Netscape browser.

## CUSTOMER RELEASE NOTES

### DOCUMENTATION:

The Command Line Reference manual, User Reference Guide and draft Release Notes are included in soft copy format on the Installation CD. Use your Browser to open file index.htm on the CD for a table of contents. You will need the freely-available Acrobat Reader to view and print these documents. If you don't have the Acrobat Reader already installed on your system, you can install it from the Installation CD or from Adobe's Web site (<http://www.adobe.com/>). The Acrobat Reader is available for a very wide range of platforms, including MS Windows, Macintosh and many Unix systems.

### TECHNICAL SUPPORT:

Should you have any difficulty installing or operating the product, feel free to contact Technical Support. Before you call, please try to gather a trace file. See if you can connect to the router with Telnet (for Windows, do a Start | Run | Telnet. Login with the administrative password and type `system support`). Copy and paste the result into a file. This will generate a file that can be used to analyze the problem.

If you can't connect to the router, but are able to use the console interface, use the Terminal or HyperTerminal applications that come with Windows (use the parameters: 9600, 8N1), type `system support` and copy and paste the result into a file.

Efficient Networks, Inc.  
4849 Alpha Road  
Dallas, TX 75244

Phone: +1(888) 286-9375  
Internet mail: [support@efficient.com](mailto:support@efficient.com)