



Release Notes for Cisco 827 Routers

This document describes new and changed information for the *Cisco 827 Routers Hardware Installation Guide* and the *Cisco 827 Routers Software Configuration Guide*.

For last-minute updates to this release note, refer to the Cisco 827 routers documentation Web site at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/index.htm.

ADSL Cable Requirements

The ADSL cable that you connect to the Cisco 827 router must be 10BaseT Category 5, unshielded twisted-pair (UTP) cable. Using regular telephone cable can introduce line errors.

DHCP Client Support

Follow these steps to configure the router for DHCP client support:

-
- Step 1** Configure the BVI interface by entering the **ip address dhcp client-id Ethernet 0** command.
- Specifying the value *client-id ethernet0* means that the MAC address of the Ethernet interface is used as the client ID when the DHCP request is sent. Otherwise, the MAC address of the BVI interface is used as the client ID.
- Step 2** Configure NAT:
- Configure the BVI interface by entering the **ip nat outside** command.
 - Configure the Ethernet interface by entering the **ip nat inside** command.
 - Create an access list under NAT by entering the **access-list 1 permit ip address** command to match all Ethernet IP addresses.
 - Configure the source list under NAT by entering the **ip nat inside source list 1 interface BVI 1 overload** command.



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2005 Cisco Systems, Inc. All rights reserved.

- Step 3** Configure the Cisco 827 router to act as a DHCP server. This step is optional.
- At the `config-if` router prompt, enter the `ip dhcp pool server name` command.
 - Enter the `import all` command to have the Cisco 827 router retrieve the Microsoft Windows nameserver (WINS) and domain name system (DNS) server addresses for name resolution.

Configuration Example

The following example shows a configuration of the DHCP client.

```
Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c827
!
!
ip subnet-zero
ip dhcp excluded-address 10.10.10.1
!
ip dhcp pool SERVER
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.1
 import all
!
bridge irb
interface Ethernet0
 ip address 10.10.10.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
!
interface ATM0
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 bundle-enable
 hold-queue 208 in
!
interface ATM0.1 point-to-point
 no ip directed-broadcast
 pvc 1/100
 encapsulation aal5snap
!
bridge-group 1
!
interface ATM0.2 point-to-point
 ip address 5.0.0.2 255.0.0.0
 no ip directed-broadcast
 pvc 1/101
 protocol ip 5.0.0.1 broadcast
 protocol ip 5.0.0.5 broadcast
 encapsulation aal5snap
!
```

```

!
interface BVI1
  ip address dhcp client-id Ethernet0
  no ip directed-broadcast
  ip nat outside
!
ip nat inside source list 1 interface BVI1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 BVI1
no ip http server
!
access-list 1 permit 10.10.10.0 0.0.0.255
bridge 1 protocol ieee
bridge 1 route ip
!
voice-port 1
timing hookflash-in 0
!
voice-port 2
timing hookflash-in 0
!
voice-port 3
timing hookflash-in 0
!
voice-port 4
timing hookflash-in 0
!
!
line con 0
exec-timeout 0 0
transport input none
stopbits 1
line vty 0 4
password lab
login
!
scheduler max-task-time 5000
end

```

Dialer Interface Configuration

The “Configuring the Dialer Interface” section in Chapter 3, “Feature-By-Feature Router Configurations,” of the *Cisco 827 Routers Software Configuration Guide* has an incorrect router prompt in Step 4. The prompt should be `Router(config-if)`.

Easy IP (Phase 1) Configuration

The “Configuring Easy IP (Phase 1)” section in Chapter 3, “Feature-By-Feature Router Configurations,” of the *Cisco 827 Routers Software Configuration Guide* has an incorrect reference in Step 2. The task should refer to the access list defined in Step 1 rather than in Step 2.

MMI Support

The Modem Management Interface (MMI) is software that enables auto-provisioning for the Cisco 827 routers. The MMI uses a fixed PVC to communicate with the Proxy Element (PE) residing on the digital subscriber line access multiplexer (DSLAM). Using MMI, the Cisco 827 router updates the running image and downloads the prescribed configuration using a configuration file or configuration values in a provisioning information database.

Configuring MMI for Auto-Provisioning

The customer premise equipment (CPE) can be automatically configured using the Cisco DSL CPE download, but it can be configured only with the image provisioning feature. The following provisioning configuration files are not supported in this release:

- profiles
- CDCM objects below the CPE level (that is, the ATM VCC objects)
- propVirtual objects and interface objects (ATMif and Ethernetif)

Follow these steps to configure the router for MMI support in configure-terminal mode:

Step 1 To set the configuration approach for MMI, enter the following command:

mmi auto-configure

no mmi auto-configure

If this parameter is enabled, the router is provisioned by the PE. By default, this parameter is enabled.

If this parameter is disabled, the router is configured by the start up configuration file.

Step 2 To set the polling interval for the router to check the PE for any updated image or configuration files, enter the following command:

mmi polling-interval *time*

where *time* is the number of seconds. The polling-interval range is from 1 to 65535, with the default set to 60 seconds.

Step 3 To set the ATM PVC so the MMI communicates with the PE, enter the following command:

mmi pvc *vpi/vci*

where *vpi/vci* is the virtual path identifier/virtual channel identifier. The default PVC for MMI is 0/16 ilmi, but if it is not available, you must set the specific PVC for the router to communicate with the PE.

Step 4 To set the timer to monitor the image file download, enter the following command in configure terminal mode:

mmi snmp-timeout *time*

where *time* is 1 to 1800 seconds, which is the allowed interval to download any two consecutive blocks. If you enter the **no mmi snmp-timeout** command, the default time is set to 180 seconds.

Step 5 To eliminate the ADSL line training delay, enter the following command:

dsl operating-mode auto

If the DSLAM is using a Cisco 4xDMT ADI-based card, enter the following command:

dsl operating-mode ansi-dmt

Step 6 To set up the debug process for MMI, enter the following command:

debug mmi

Step 7 Save the configuration file to NVRAM and reload. The router's OK LED on the front panel blinks while the image is being auto-provisioned. The PVC is set up when the reboot occurs.

MMI Configuration Example

The following example shows an MMI configuration:

```
820-voice1#sh run
Building configuration...

Current configuration :947 bytes
!
version 12.1
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 820-voice1
!
no logging buffered
no logging buffered
logging rate-limit console 10 except errors
!
mmi polling-interval 1000
no mmi auto-configure
mmi pvc 0/16
debug mmi
ip subnet-zero
no ip finger
!
!
!
interface Ethernet0
  no ip address
  shutdown
!
interface Virtual-Template1
  no ip address
!
interface ATM0
  no ip address
  pvc 0/101
!
  bundle-enable
  dsl operating-mode auto
!
```

```

ip classless
no ip http server
!
snmp-server manager
!
voice-port 1
!
voice-port 2
!
voice-port 3
!
voice-port 4
>
line con 0
  transport input none
  stopbits 1
line vty 0 4
  login
!
scheduler max-task-time 5000
end

```

Notes for the DSL Provider

To use the Cisco automated configuration solution with the Cisco 827 CPEs, follow these steps:

-
- Step 1** Enable the MMI configuration, as described in the previous section.
 - Step 2** Ping from the DSLAM to the CPE to ensure the DSLAM is a proxy element host.
 - Step 3** Store the MMI configuration file on an FTP server that acts as the proxy element's image server.
 - Step 4** Use Cisco DSL CPE Manager (CDCM) to add the configuration file to the proxy element's image table. The image file can also be added to the PE.
 - Step 5** Use CDCM to deploy the CPE. You can manually deploy it or use autodiscovery to deploy multiple CPE's.
 - Step 6** Use CDCM to provision an image for each CPE, which associates a specific configuration file to the CPE.

For more information on the Cisco DSL CPE image provisioning, refer to the following documents:

- *Cisco DSL CPE Automated Configuration Solution Guide*
 - *Cisco DSL CPE Manager*
-

Multilink PPP and Interleaving

Multilink PPP fragments large data packets so that small voice packets can be interleaved within them. However, apart from first-in-first-out (FIFO) queuing, no other kind of output queuing mechanisms are currently supported with PPP over ATM. Consequently, when multilink PPP is configured on the Cisco 827 routers, the big packets are fragmented, but interleaving of small voice packets within them does not occur.

NAT Support for H.323 Signaling

Currently, NAT does not support alerting H.225 messages. Therefore, NAT communication cannot be established between the router end points.

NAT support for H.323 signaling is limited to the Netmeeting application.

PPP over AAL5SNAP Encapsulation Support

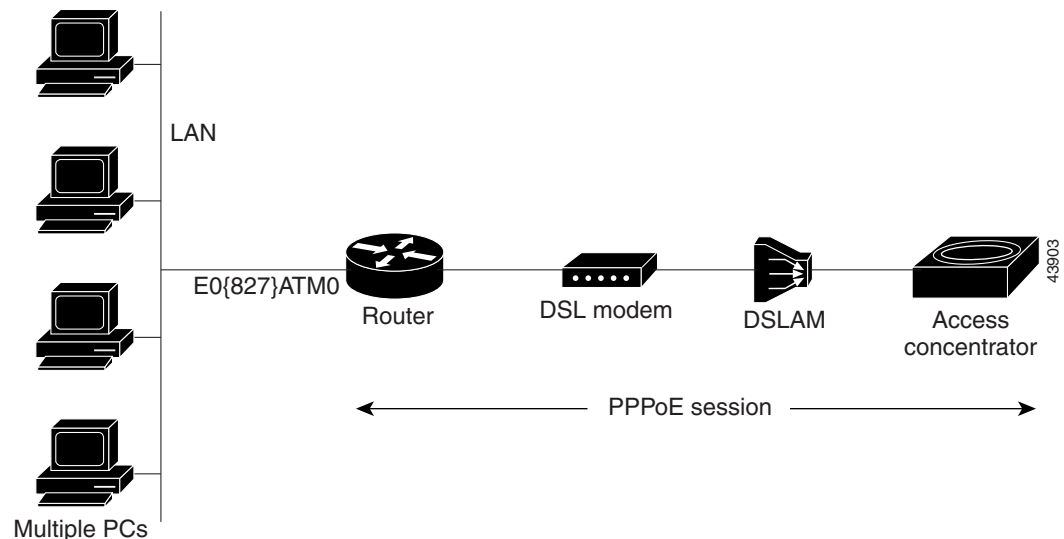
PPP over AAL5SNAP encapsulation is currently not supported, although the context-sensitive help mentions that it can be configured.

PPP over Ethernet Support

This feature supports the PPP over Ethernet (PPPoE) client on an ATM permanent virtual circuit (PVC). Only one PPPoE client on a single ATM PVC is supported. The PPPoE client over an ATM interface is supported for all 820 platforms.

The following figure depicts a typical deployment scenario for PPPoE support:

Figure 1 PPPoE Deployment Scenarios



A PPPoE session is initiated on the client side by the network described above. If the session has a timeout or is disconnected, the PPPoE client immediately attempts to reestablish the session.

Follow these steps to configure the router for PPPoE client support:

- Step 1** If your router is running a Cisco IOS release prior to Cisco IOS release 12.2(13)T, configure the virtual private dialup network (VPDN) group number. If your router is running Cisco IOS release 12.2(13)T or higher, proceed to [Step 2](#).

**Note**

Enabling VPDN is not necessary for routers running Cisco IOS release 12.2(13)T or higher.

- a. Enter the **vpdn enable** command in global configuration mode.
- b. Configure the VPDN group by entering the **vpdn group tag** command.
- c. Specify the dialing direction by entering the **request-dialin** command in the VPDN group.
- d. Specify the type of protocol in the VPDN group by entering the **protocol pppoe** command.

- Step 2** Configure the ATM interface with PPPoE support.

- a. Configure the ATM interface by entering the **interface atm 0** command.
- b. Specify the ATM PVC by entering the **pvc number** command.
- c. Configure the PPPoE client and specify the dialer interface to use for cloning by entering the **pppoe-client dial-pool-number number** command.

- Step 3** Configure the dialer interface by entering the **int dialer number** command.

- a. Configure the IP address as negotiated by entering the **ip address negotiated** command.
- b. Configure authentication for your network by entering the **ppp authentication** protocol command. This step is optional.
- c. Configure the dialer pool number by entering the **dialer pool number** command.
- d. Configure the dialer-group number by entering the **dialer-group number** command.
- e. Configure a dialer list corresponding to the dialer-group by entering the **dialer-list 1 protocol ip permit** command.

**Note**

Multiple PPPoE clients can run on a different PVCs, in which case, each client has to use a separate dialer interface and a separate dialer pool, and the PPP parameters need to be applied on the dialer interface.

If you enter the **clear vpdn tunnel pppoe** command with a PPPoE client session already established, the PPPoE client session terminates and the PPPoE client immediately tries to reestablish the session.

Configuration Example

The following example shows a configuration of a PPPoE client on a router running a Cisco IOS release prior to Cisco IOS release 12.2(13)T.

```
vpdn enable
vpdn-group 1
    request-dialin
protocol pppoe

int atm0

pvc 1/100
    pppoe-client dial-pool-number 1

int dialer 1
ip address negotiated
ppp authentication chap
dialer pool 1
dialer-group 1
```

The following example shows a configuration of a PPPoE client on a router running Cisco IOS release 12.2(13)T or higher.

```
int atm0

pvc 1/100
    pppoe-client dial-pool-number 1

int dialer 1
ip address negotiated
ppp authentication chap
dialer pool 1
dialer-group 1
```

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

Use this document in conjunction with the *Cisco 827 Routers Hardware Installation Guide*, the *Regulatory Compliance and Safety Information* document for your router, the *Cisco 827 Routers Software Configuration Guide*, and the Cisco IOS configuration guides and command references.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2005, Cisco Systems, Inc.
All rights reserved. Printed in USA