Installing the G.SHDSL ATM WIC on the Cisco 1700 Series Router

This document describes the multirate symmetric high-speed digital subscriber line (G.SHDSL) one-port wide area network (WAN) interface card (WIC). G.SHDSL is a last-mile access technology, which has a symmetrical data rate over a single copper pair. The G.SHDSL ATM WIC, the WIC-1SHDSL card, is available for, Cisco 1700, 2600, and 3600 series routers and supports ATM AAL5, raw cell, and various classes of quality of service (QoS) for both voice and data service, including the following:

- Constant bit rate (CBR)
- Variable bit rate (VBR) (real-time and non-real-time)
- Unspecified bit rate (UBR)

This card is compatible with the Cisco G.SHDSL line card in the Cisco 6015, Cisco 6130, Cisco 6160, or Cisco 6260 digital subscriber line access multiplexer (DSLAM).

This document contains the following sections:

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

Related Documentation

Use this document with the following guides:

- *Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2T* and *Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(2)XL*—provide information for running IOS images on a Cisco 1700 series router
- *Cisco 1700 Router Hardware Installation Guide*—provides procedures for physical installation
- *Cisco WAN Interface Cards Hardware Installation Guide*—also provides installation information for WICs in routers
- Cisco IOS configuration guides and command references—provide IOS software commands and configurations for your router
- *Voice, Video, and Home Applications Configuration Guide*—a Cisco IOS Release 12.2 guide that provides information about voice configuration
- *Voice, Video, and Home Applications Command Reference*—a Cisco IOS Release 12.2 guide that provides information about voice commands
- *Network Protocols Configuration Guide, Part 1*—provides information about configuring IP
- *Wide-Area Networking Configuration Guide*—provides information about configuring ATM
- *Configuration Guide for Cisco DSLAMs with NI-2*—provides information about configuring a DSLAM
- *Regulatory Compliance and Safety Information for Cisco 1600 and Cisco 1700 Routers*
- *Enhanced Voice and QoS for ADSL and G.SHDSL on Cisco 1700 Series, Cisco 2600 Series, and Cisco 3600 Series Routers*

These documents are available under Technical Documentation at http://www.cisco.com.

Features

G.SHDSL is an ATM-based, multirate, high-speed (up to 2.32 Mb), symmetric digital subscriber line digital data transfer between a single customer premises equipment (CPE) subscriber and a central office (CO).

The WIC-1SHDSL card is compatible with Cisco 6015, Cisco 6130, Cisco 6160, and Cisco 6260 DSLAMs. The DSLAM must be equipped with G.SHDSL line cards that are compatible with the DSL service to be configured.

The following are features of the WIC-1SHDSL card:

- Trellis-coded pulse amplitude modulation (TC-PAM) line coding.
- Multilink PPP for dual WIC.
- Loop reach performance for a 2.320-Mbps rate.
- Bit error rate of better than 10^{-7} for all test loops, with white noise level at -140 dBm.

The following ATM features are supported:

- PVC ATM Forum UNI 3.1 and 4.0: AAL5.
- Interim Local Management Interface (ILMI).
- Virtual channel (VC) traffic shaping (at 32 kbps granularity).

- IP QoS map to ATM class of service (CoS).
- 16-bit VPI/VCI addressability, supporting up to 65,536 virtual path identifiers (VPIs) (with one VPI) or up to 256 virtual channel identifiers (VCIs) (with 256 possible VPIs).

The following buffering is supported:

- Per virtual channel queuing (French requirement).
- Per virtual channel peak cell rate (PCR) and sustainable cell rate (SCR) enforcement.
- PPP over ATM, and PPP over Ethernet over ATM.
- Operations and maintenance cells, consisting of F4 and F5 types for ATM switch and router.
- Virtual channel support for up to 23 permanent virtual circuits (PVCs) on a WIC-1SHDSL card.

Benefits

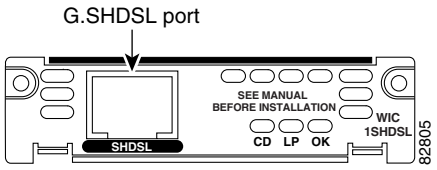
The following are benefits of the WIC-1SHDSL card:

- Enables business class broadband service with voice integration, scalable performance, flexibility, and security
- Aggregates G.SHDSL and other transport options into a single box
- Provides G.SHDSL high-speed digital data transmissions between CPE and the CO, or between routers located within a customer site
- Supports ITU G.991.2 (SHDSL)
- Supports ANSI T1.601 (BRI), ANSI T1.410 (digital data service [DDS]), and ANSI T1.403 (T1 carrier)
- Provides ATM traffic management and QoS features to enable service providers to manage their core ATM network infrastructures
- Supports Frame Relay Forum (FRF) internetworking functions FRF.5 and FRF.8

LEDs

Figure 1 shows the WIC-1SHDSL card.

Figure 1 WIC-1SHDSL Card



The WIC-1SHDSL card has three LEDs, which are shown in Figure 1 and are described in Table 1.

Table 1 WIC-1SHDSL Card LEDs

Feature	Color	Description
CD LED	Green	The unit is connected to the network. On during normal operation.
LP LED	Yellow	DSL interface is in loopback mode.
	Off	Normal operation.
OK LED	Green	Enabled when the card is detected by the router.

Requirements

This section describes the requirements and standards supported for the WIC-1SHDSL card.

Software Requirements

The WIC-1SHDSL card requires Cisco IOS Release 12.2(4)XL or later.

Memory Requirements

The memory requirements for running the full-featured Cisco 1700 router encryption images with the G.SHDSL WIC are as follows:

- 16 MB of Flash memory
- 64 MB of dynamic RAM (DRAM)

Caveats

The following are caveats concerning the use of a WIC-1SHDSL card.

- If the WIC-1SHDSL card is used with an IOS image that does not support it, an error message appears, indicating an unrecognized WIC. This does not damage the router or the WIC-1SHDSL card. The error message is “00:00:05: %PQUICC-1-UNKNOWN_WIC: PQUICC(0), WIC card has an unknown ID of 0xFF.”
- ConfigMaker does not recognize the WIC-1SHDSL card.
- The WIC-1SHDSL card does not support dual latency. When the DSL link is intended to support both voice and data traffic simultaneously, the total supported data rate must be reduced to adjust for the reduced coding gain, which is usually present with high-latency traffic.
- The WIC-1SHDSL card does not support “dying gasp” in ANSI T1.413 Issue 2.
- The WIC-1SHDSL card does not support ABR CoS.
- On Cisco 1700 series routers, the WIC should be inserted only in slot 0 or slot 1.

Data Rate Limitations

The card supports the following data rates (26 AGW) and distances:

192 kbps	22,000 feet
272 kbps	21,400 feet
400 kbps	19,900 feet
528 kbps	18,700 feet
784 kbps	17,500 feet
1040 kbps	16,600 feet
1168 kbps	15,800 feet
1552 kbps	14,200 feet (HDSL2 unframed T1)
2064 kbps	13,000 feet
2320 kbps	12,500 feet

Safety Warnings

Safety warnings appear throughout this publication in procedures that can harm you if they are performed incorrectly. A warning symbol precedes each warning statement.

Warning Conventions

Warning **This warning symbol means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Waarschuwing **Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het document *Regulatory Compliance and Safety Information* (Informatie over naleving van veiligheids- en andere voorschriften) raadplegen dat bij dit toestel is ingesloten.**

Varoitus **Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. Tässä julkaisussa esiintyvien varoitusten käännökset löydät laitteen mukana olevasta *Regulatory Compliance and Safety Information* -kirjasesta (määräysten noudattaminen ja tietoa turvallisuudesta).**

Attention **Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions d'avertissements figurant dans cette publication, consultez le document *Regulatory Compliance and Safety Information* (Conformité aux règlements et consignes de sécurité) qui accompagne cet appareil.**

Warnung **Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Dokument *Regulatory Compliance and Safety Information* (Informationen zu behördlichen Vorschriften und Sicherheit), das zusammen mit diesem Gerät geliefert wurde.**

Avvertenza **Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nel documento *Regulatory Compliance and Safety Information* (Conformità alle norme e informazioni sulla sicurezza) che accompagna questo dispositivo.**

Advarsel **Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du vare oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i dokumentet *Regulatory Compliance and Safety Information* (Overholdelse av forskrifter og sikkerhetsinformasjon) som ble levert med denne enheten.**

Aviso **Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. Para ver as traduções dos avisos que constam desta publicação, consulte o documento *Regulatory Compliance and Safety Information* (Informação de Segurança e Disposições Reguladoras) que acompanha este dispositivo.**

¡Advertencia! **Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. Para ver una traducción de las advertencias que aparecen en esta publicación, consultar el documento titulado *Regulatory Compliance and Safety Information* (Información sobre seguridad y conformidad con las disposiciones reglamentarias) que se acompaña con este dispositivo.**

Varning! **Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. Se förklaringar av de varningar som förkommer i denna publikation i dokumentet *Regulatory Compliance and Safety Information* (Efterrättelse av föreskrifter och säkerhetsinformation), vilket medföljer denna anordning.**

Power Supply Warnings

The following warnings apply when you are installing a card or working with the power supply:

Warning **Read the installation instructions before you connect the system to its power source.**

Warning **Only trained and qualified personnel should be allowed to install or replace this equipment.**

Warning **Warning: Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord.**

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.**

Electrical Warnings

The following warnings apply when you are working with electricity:

Warning **To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Both LAN and WAN ports may use RJ-45 connectors. Use caution when connecting cables.**

Warning **No operator-serviceable parts inside. Refer servicing to qualified personnel.**

Follow these guidelines when working on equipment powered by electricity:

- Locate the emergency power-off switch in the room in which you are working. Then, if an electrical accident occurs, you can quickly shut the power off.
- Before working on the router, turn off power to the router and unplug the power cord.
- Disconnect all power before doing the following:
  - Installing or removing a router chassis
  - Working near power supplies
- Do not work alone if potentially hazardous conditions exist.
- Never assume that power is disconnected from a circuit. Always check.
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, and missing safety grounds.

If an electrical accident occurs, proceed as follows:

- Use caution; do not become a victim yourself.
- Turn off power to the router.
- If possible, send another person to get medical aid. Otherwise, determine the condition of the victim and then call for help.
- Determine if the victim needs rescue breathing or external cardiac compressions; then take appropriate action.

Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. It can occur when printed circuit cards are improperly handled and can result in complete or intermittent failures. Always follow ESD prevention procedures when removing and replacing cards. Ensure that the router chassis is electrically connected to earth ground. Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the clip to an unpainted surface of the chassis frame to safely channel unwanted ESD voltages to ground. To guard against ESD damage and shocks, the wrist strap and cord must be used properly. If no wrist strap is available, ground yourself by touching the metal part of the chassis.

Caution For safety, periodically check the resistance value of the antistatic strap, which should be between 1 and 10 megohms (Mohms).

Connecting a G.SHDSL Card to the Network

Use a straight-through RJ-11 cable for this connection. The port on this interface card is color-coded lavender.

If you are connecting a DSL card to an RJ-11 wall jack that has the DSL pair wired for pins 2 and 5, you must use an RJ-11 crossover cable (lavender with blue stripe). The RJ-11 crossover cable is orderable separately as a spare.

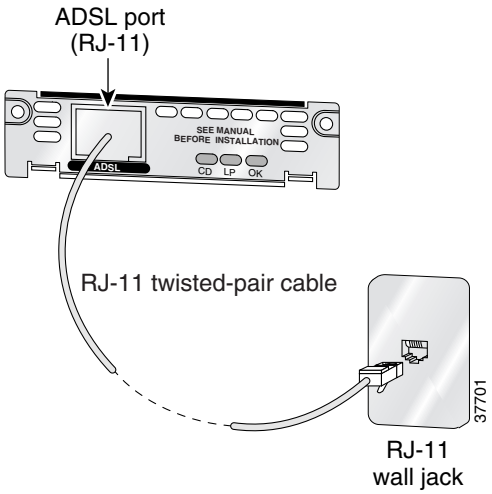
Complete the following steps to connect a 1-port G.SHDSL card to the network:

Step 1 Confirm that the router is turned off.

Step 2 Connect one end of the cable to the G.SHDSL port on the card.

Step 3 Connect the other end to the wall jack (RJ-11) at your site, as shown in Figure 2.

Figure 2 Connecting a G.SHDSL WIC to the Wall Jack



Step 4 Turn on power to the router.

Step 5 To connect the card to the network, you must configure the card in the router to the no shutdown state. Enter the **no shut** command in the router configuration. Check that the CD LED goes on, indicating that the card is connected to the network.

Configuration Modes

Whenever you install a new card, or if you want to configure an existing card, you must configure the interface. If you replace a card that was already configured, the router recognizes it and brings up the interface by using the existing configuration.

Before you configure an interface, have the following information available:

- Protocols you plan to route on the new interface
- IP addresses, subnet masks, network numbers, zones, or other information related to the routing protocol

Obtain this information from your system administrator or network plan before you begin configuring the router.

You can configure the new interface and other router parameters by using any of the following methods:

- Command-Line Configuration (manual configuration)—recommended if you are familiar with IOS commands. Enter the commands and values at the prompt.
- System Configuration Dialog (Setup facility)—recommended if you are not familiar with IOS commands. You are prompted for each value.
- AutoInstall (automatic installation)—recommended if another router running IOS software is installed on the network. This configuration method must be coordinated in advance by someone with experience using IOS software, such as the network administrator.

These procedures are explained in the following sections. To change the settings shown in the examples and to obtain further information, refer to the IOS configuration guides and command references. If you have questions or need help, see the "Obtaining Technical Assistance" section in this document.

Command-Line Configuration

You can configure the card by entering IOS commands on the command line. This method provides the greatest power and flexibility. For further information about these commands, refer to the IOS configuration guides and command references. You can display help by entering a question mark (**?**) at the prompt.

Before you begin, disconnect all WAN cables from the router to prevent it from running the AutoInstall process. The router tries to run AutoInstall whenever you power it on if there is a WAN connection on both ends and if the router does not have a valid configuration file stored in NVRAM (for instance, when you add a new interface). It can take several minutes for the router to determine that AutoInstall is not connected to a remote Transmission Control Protocol/Internet Protocol (TCP/IP) host.

To configure the card by using the command-line interface (CLI), follow this procedure:

Step 1 Connect a console or a PC running terminal emulation software, such as HyperTerminal, to the router. If you need instructions for connecting to the console port of the router, refer to the installation chapter of your router installation and configuration guide.

Step 2 Power on the router. If the startup configuration is valid, the EXEC prompt (Router>) appears. If the startup configuration is not valid, the router attempts to run Auto Install, and the following prompt appears:

```
Would you like to enter the initial dialog? [yes]:
```

Step 3 Enter **no** and press **Enter** to display the EXEC prompt.

Step 4 Enter **enable** and the password (if any) to enter enable mode. The prompt changes to the privileged mode prompt (`Router#`). Configuration changes can be made only in enable mode.

Step 5 Enter **config terminal** to enter configuration mode:

```
Router#config terminal
Router(config)#
```

The router enters global configuration mode, shown by the `Router(config)#` prompt.

If you want to change the router configuration, you can configure global parameters, passwords, network management, and routing protocols. For complete information about global configuration commands, refer to the IOS configuration guides and command references.

Step 6 Select the Ethernet interface to configure. The following uses the Cisco WIC-1ENET interface as an example:

```
Router(config)#interface Ethernet 0
Router(config-if)#
```

The prompt changes again to show that you are in interface configuration mode.

Step 7 Configure the routing protocols on the interface. (You must have previously enabled these protocols as part of global configuration.) In this example, IP and IPX are being configured:

```
Router(config-if)#ip address ipaddress subnetmask
Router(config-if)#ipx network networknumber
```

Step 8 Enter **no shutdown** to enable the port:

```
Router(config-if)#no shutdown
```

Step 9 Enter **exit** to return to the `Router(config)#` prompt.

Step 10 Exit configuration mode, and return to privileged mode by pressing **Ctrl-Z**. To see the current running configuration, including any changes you made, enter the **show running-config** command:

```
Router#show running-config
```

Step 11 To store the running configuration in NVRAM, enter the **copy running-config startup-config** command while in privileged mode:

```
Router#copy running-config startup-config
Building configuration. . .
[OK]
Router#
```

The router automatically copies the startup configuration in NVRAM to the running configuration and executes it whenever the router is powered on or the **reload** command is entered. To see the configuration stored in NVRAM, enter the **show startup-config** command:

```
Router#show startup-config
```

System Configuration Dialog

You can configure the router by using the system configuration dialog (also called the *Setup facility*). The system configuration dialog prompts you for each response.

This section shows a sample configuration using the system configuration dialog. You should enter values appropriate for your router and network. To change the settings shown in the examples and to obtain further information, refer to the IOS configuration guides and command references.

Many prompts in the system configuration dialog include default answers, shown in square brackets following the question. Enter your response, or press **Return** to accept the default answer.

You can request help at any time by entering a question mark (**?**) at the system configuration dialog prompt.

Before you begin, disconnect all WAN cables from the router to prevent it from running the AutoInstall process. The router tries to run AutoInstall whenever you power it on if there is a WAN connection on both ends, and the router does not have a valid configuration file stored in NVRAM (for instance, when you add a new interface). It can take several minutes for the router to determine that AutoInstall is not connected to a remote TCP/IP host.

Follow these steps to configure the router by using the system configuration dialog:

Step 1 Power down the router, and install the card.

Step 2 Connect a console to the router. If you need instructions for connecting a console, refer to the installation chapter of your router installation and configuration guide.

Step 3 Power on the router.

If the router does not have a valid startup configuration file, it tries to run AutoInstall. The following prompt appears:

```
Would you like to enter the initial dialog? [yes]:
```

Step 4 Enter **no**, and press **Enter** to display the EXEC prompt (`Router>`).

If the startup configuration is valid, the EXEC prompt (`Router>`) appears.

Step 5 Enter **enable** to enter privileged mode. The enable prompt (`Router#`) appears. Enter enter setup mode and display the system configuration dialog as follows:

```
Router> enable
```

Step 6 Enter Setup mode by entering the following command:

```
Router# setup
```

Step 7 Follow the prompts and change the parameters, or accept the defaults to configure global parameters, such as passwords, network management, and routing protocols. Refer to the procedures in the IOS configuration guides and command references.

The following is an example of the process.

a. Enter **yes** to start setup mode.

```
Would you like to enter the initial configuration dialog? [yes/no]: yes
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
```

b. Respond to the prompt as follows:

```
Would you like to enter basic management setup? [yes/no]: no
First, would you like to see the current interface summary? [yes]: no
```

c. Enter the host name of the router as follows:

```
Configuring global parameters:
   Enter host name [Router]: hostname
```

d. Enter the enable secret password as follows:

```
The enable secret is a password used to protect access to
   privileged EXEC and configuration modes. This password, after
   entered, becomes encrypted in the configuration.
   Enter enable secret: password
   The enable password is used when you do not specify an
   enable secret password, with some older software versions, and
   some boot images.
```

e. Enter the enable password as follows:

```
Enter enable password: password
```

f. Enter the virtual terminal password as follows:

```
The virtual terminal password is used to protect
   access to the router over a network interface.
   Enter virtual terminal password: password
```

g. Respond to the prompts as follows:

```
Configure SNMP Network Management? [yes]: no
   Configure IP? [yes]: yes
     Configure IGRP routing? [yes]: yes
       Your IGRP autonomous system number [1]: 1
   Configure bridging? [no]: no
```

h. Enter the IP address and subnet mask as follows:

```
Configuring interface parameters:
Do you want to configure Ethernet0  interface? [yes]: yes
   Configure IP on this interface? [yes]: yes
IP address for this interface: ipaddress
     Subnet mask for this interface [255.0.0.0] : netmask
     Class X network is x.x.x.x, x subnet bits; mask is /x

Do you want to configure FastEthernet0  interface? [yes]: no

The following configuration command script was created:
hostname Router
enable secret 5 $1$ANpR$LYOj7mFpk1TE7SSAXDgVA/
enable password password
line vty 0 4
password password
no snmp-server
!
!
ip routing
no bridge 1
!
interface Ethernet0
ip address x.x.x.x x.x.x.x
!
router igrp 1
redistribute connected
network x.x.x.x
network x.x.x.x
!
end
```

After the configuration you entered appears, you are asked if you want to use it.

Step 8 Enter **yes** to save the startup configuration:

```
Use this configuration? [yes/no]: yes
Building configuration...
Use the enabled mode 'configure' command to modify this configuration.

Press RETURN to get started!
```

The configuration is saved.

Enter **no** if you do not want to save the configuration. The information you entered is discarded, and you can reenter the configuration parameters.

AutoInstall

The AutoInstall process is designed to configure the router automatically after it connects to your WAN. For AutoInstall to work properly, a TCP/IP host on your network must be configured to provide the configuration files. The TCP/IP host can reside anywhere on the network if the following two conditions exist:

- The host is on the remote side of the router's synchronous serial connection to the WAN.
- User Datagram Protocol (UDP) broadcasts to and from the router and the TCP/IP host is enabled.

This functionality is coordinated by your system administrator at the TCP/IP host site. You should not try to use AutoInstall unless the required files are installed on the TCP/IP host.

Follow this procedure to prepare your router for the AutoInstall process:

Step 1 Connect the router to the WAN.

Step 2 Turn on power to the router. If the remote end of the WAN connection is connected and properly configured, the AutoInstall process begins.

Step 3 If AutoInstall succeeds, write the configuration data to NVRAM. To do this, enter the **copy running-config startup-config** command at the `Router#` prompt:

```
Router# copy running-config startup-config
Building configuration. . .
[OK]
Router#
```

This saves the configuration settings that the AutoInstall process created. If you do not do this, your configuration will be lost the next time you boot the router.

Platform Configuration

See the following sections for configuration tasks for the WIC-1SHDSL:

- Configuring G.SHDSL on a Cisco Router
- Configuring ILMI on the DSLAM Connected to the WIC-1SHDSL Card
- Configuring Quality of Service Parameters
- Configuring the SCC Clock Rate
- Configuring FRF.5 and FRF.8 Internetworking Functions

Configuring G.SHDSL on a Cisco Router

To configure G.SHDSL service on a Cisco router containing a WIC-1SHDSL card, complete the following steps, beginning in global configuration mode:

Step	Command	Purpose
Step 1	`router(config)# interface atm 1/0`	Enters ATM configuration mode for interface ATM 0 in slot 1. If a slot has two subslots for WIC modules and no ATM interface is present in subslot 0, the WIC will take ATM x/0 as its interface number even if placed in subslot 1 (ATMx/1). If a two-port ATM module is present in subslot 0, the WIC will use ATM x/2 as its interface number. This subslot number is pertinent to all interface commands such as **show interface atm** and **show dsl interface atm**.
Step 2	`router(config-if)# ip-address` *IP-address*	Assigns an IP address to the DSL ATM interface.
Step 3	`router(config-if)# atm ilmi-keepalive` *seconds*	(Optional) Enables Interim Local Management Interface (ILMI) keepalives. If you enable ILMI keepalives without specifying the seconds, the default time interval is 3 seconds.
Step 4	`router(config-if)# pvc` [*name*] *vpi/vci*	Enters atm-virtual-circuit (interface-atm-vc) configuration mode, and configures a new ATM PVC by assigning a name (optional) and VPI/VCI numbers. The default traffic shaping is UBR; the default encapsulation is AAL5+LLC/SNAP.
Step 5	`router(config-if-vc)# protocol ip` *IP-address*	(Optional) Enables IP connectivity and create a point-to-point IP address for the VC.
Step 6	`router(config-if-vc)# vbr-rt` *peak-rate average-rate burst*	(Optional) Configures the PVC for real-time variable bit rate (VBR) traffic shaping. • Peak rate = peak cell rate (PCR) in Kbps • Average rate = average cell rate in Kbps • Burst = burst size in cells
Step 7	`router(config-if-vc)# encapsulation` {**aal5autoppp** | **aal5ciscoppp** | **aal5mux** | **aal5nlpid** | **aal5snap**}	(Optional) Configures the ATM adaptation layer (AAL) and encapsulation type. • aal5autoppp for Cisco AUTO PPP over AAL5 • aal5ciscoppp for Cisco PPP over AAL5 • aal5mux for AAL5+MUX • aal5nlpid for AAL5+NLPID • aal5snap for AAL5+LLC/SNAP (the default)
Step 8	`router(config-if-vc)# exit`	Exits from interface-ATM-VC configuration mode.
Step 9	`router(config-if)# shutdown`	Ensures that the ATM interface is shut down. The following commands are not accepted if the interface is up.
Step 10	`router(config-if)# dsl operating-mode` {**gshdsl symmetric annex {A | B}**}	Configures the DSL interface to operate in a specified DSL mode, **gshdsl**—symmetrical, high-speed DSL per ITU G.991.2. The default is **gshdsl symmetric annex A**.

Step	Command	Purpose
Step 11	`router(config-if)# equipment-type {co | cpe}`	Configures the DSL interface to function as central office (CO) equipment or CPE: • **co**—The card functions as CO equipment and can interface with another G.SHDSL WIC configured as **cpe**. • **cpe**—The card functions as CPE and can interface with a DSLAM or with another G.SHDSL WIC configured as **co**. The default is **cpe**.
Step 12	`router(config-if)# dsl linerate {kbps | auto }`	Configures the DSL line rate: • *kbps*—Line rate (data transfer rate) in kilobits per second. Allowable entries are: **200, 264, 328, 392, 456, 520, 584, 648, 712, 776, 840, 904, 968, 1032, 1096, 1160, 1224, 1288, 1352, 1416, 1480, 1544, 1608, 1672, 1736, 1800, 1864, 1928, 1992, 2056, 2120, 2184, 2248, and 2312**. • **auto**—The WIC automatically trains for an optimal line rate by negotiating with the far-end DSLAM or WIC. The default is **auto**.
Step 13	`router(config-if)# exit`	Exits ATM interface configuration mode.
Step 14	`router(config)# exit`	Exits global configuration mode.
Step 15	`router> show interface atm 1/0`	Verifies the ATM interface configuration.
Step 16	`router# clear interface atm 1/0`	Permits the configuration changes to take effect.

Configuring ILMI on the DSLAM Connected to the WIC-1SHDSL Card

The Interim Local Management Interface (ILMI) protocol allows DSLAMs to be used for ATM address registration across an ATM User-Network Interface (UNI). If ILMI is configured on the WIC-1SHDSL card, the ATM PVC must be configured on the DSLAM. All switch-terminating connections use interface 0/0 to connect to the switch CPU.

For information about configuring the DSLAM, refer to the *Configuration Guide for Cisco DSLAMs with NI-2*.

Verifying ATM Configuration

Use the following commands to verify your configuration:

- Use **show running-config** to verify the current configuration and to view the status for all controllers.
- Use **show controllers atm** *slot/port* to view ATM controller statistics.
- Use **show atm vc** to verify the PVC status. Make sure that active PVCs are up.
- Use **debug atm events** to help identify ATM-related events as they are generated. Use **debug atm errors** to determine which interfaces are having trouble.

- Use **show ip route** to verify an entry for the ATM interface you configured.
- Use **show interface atm** *slot/port* to view the status of ATM interface. Make sure ATM slot/port and line protocol is up, as shown in the following example:

```
Router# sh int atm1/0
ATM1/0 is up, line protocol is up
  Hardware is DSLSAR (with Globespan G.SHDSL Module)
  MTU 4470 bytes, sub MTU 4470, BW 800 Kbit, DLY 2560 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Keepalive not supported
  Encapsulation(s):AAL5 PVC mode
  24 maximum active VCs, 256 VCs per VP, 2 current VCCs
  VC idle disconnect time:300 seconds
  Last input never, output 00:00:01, output hang never
  Last clearing of "show interface" counters 03:16:00
  Queueing strategy:fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     2527 packets input, 57116 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     10798 packets output, 892801 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out

Router# show atm vc
            VCD /                                        Peak  Avg/Min Burst
Interface   Name       VPI   VCI  Type   Encaps   SC    Kbps   Kbps   Cells  Sts
1/0.3       2            9    36   PVC    MUX      UBR     800                UP
1/0.2       1            9    37   PVC    SNAP     UBR     800                UP

Router# show controllers atm 1/0
Interface ATM1/0 is up
  Hardware is DSLSAR (with Globespan G.SHDSL Module)
IDB:    62586758  Instance:6258E054  reg_dslsar:3C810000  wic_regs:3C810080
PHY Inst:62588490  Ser0Inst:62573074  Ser1Inst: 6257CBD8  us_bwidth:800
Slot:   1         Unit:    1         Subunit:  0         pkt Size:4496
VCperVP:256       max_vp:  256       max_vc:   65536     total vc:2
rct_size:65536     vpivcibit:16        connTblVCI:8         vpi_bits:8
vpvc_sel:3         enabled: 0         throttled:0

WIC    Register   Value      Notes
---------------   ---------- ----------
FPGA Dev ID (LB)  0x44       'D'
FPGA Dev ID (UB)  0x53       'S'
FPGA Revision     0x9D
WIC Config Reg    0x45       WIC / VIC select = WIC;
                             CTRLE addr bit 8 = 1;
                             OK LED on;
                             LOOPBACK LED off;
                             CD LED on;
WIC Config Reg2   0x07       Gen bus error on bad ADSL access
Int 0 Enable Reg  0x03       ADSL normal interrupt enabled
                             ADSL error interrupt enabled
```

- Use **show dsl interface atm** *slot/port* to view the status of WIC-1SHDSL card. If the line is down, the following statement appears: `Line is not active. Some of the values may not be accurate.` You can also verify whether the equipment type and operating mode configuration are correct for your application.

Output Example

The WIC is configured as CO equipment, and the line is up.

```
Router# show dsl interface atm 0/0
Globespan G.SHDSL Chipset Information

 Equipment Type:        Central Office
 Operating Mode:        G.SHDSL
 Clock Rate Mode:       Auto rate selection Mode
 Reset Count:           2
 Actual rate:           2320 Kbps
 Modem Status:          Data
 Noise Margin:          43 dB
 Loop Attenuation:      0.0 dB
 Transmit Power:        13.5 dB
 Receiver Gain:         204.8000 dB
 Last Activation Status:No Failure
 CRC Errors:            0
 Chipset Version:       1
 Firmware Version:      R1.5

 Farend Statistics since CO boot-time:

CRC Errors:      0
Errored Seconds: 0
Severly ES:      0
Un Available S:  48
Loss Of Sync S:  0
```

Output Example

The WIC is configured as CPE, and the line is up.

```
Router# show dsl interface atm 0/0
Globespan G.SHDSL Chipset Information

 Equipment Type:        Customer Premise
 Operating Mode:        G.SHDSL
 Clock Rate Mode:       Auto rate selection Mode
 Reset Count:           1
 Actual rate:           2320 Kbps
 Modem Status:          Data
 Noise Margin:          42 dB
 Loop Attenuation:      0.0 dB
 Transmit Power:        13.5 dB
 Receiver Gain:         204.8000 dB
 Last Activation Status:No Failure
 CRC Errors:            0
 Chipset Version:       1
 Firmware Version:      R1.0
```

Configuring Quality of Service Parameters

This section describes QoS parameters that can be configured for Cisco 1700 series routers, using the WIC-1SHDSL card. The following are included:

- Low Latency Queuing (Priority Queuing with Class-Based Weighted Fair Queuing)
- DiffServ
- Committed Access Rate
- Multilink PPP over ATM with Link Fragmentation and Interleaving
- Weighted Random Early Detection
- ATM per-VC Queuing and VC Bundling
- ATM Cell Loss Priority Bit Marking
- Compressed RTP
- Tunable Transmission Ring
- MLP Bundling

Low Latency Queuing (Priority Queuing with Class-Based Weighted Fair Queuing)

Low latency queuing (LLQ) allows strict priority queuing (PQ) to class-based weighted fair queuing (CBWFQ). This priority queuing allows delay-sensitive data such as voice packets to be de-queued and sent before other packet traffic, reducing jitter in voice conversations. To configure LLQ, enter the **priority** command under the CBWFQ configuration.

Configuration Example

The following example shows a Cisco 1751 router configured with LLQ:

```
class-map match-all VOIP
 match ip dscp 32
class-map CRITICAL
 match access-group 100
!
policy-map 1751_DSL
 class CRITICAL
  priority 48
 class VOIP
  bandwidth 64
  set ip precedence 6
!
interface Loopback1
ip address 10.0.0.10 255.255.255.252
!
interface ATM0/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM0/0.1 point-to-point
 pvc 0/33
  vbr-rt 320 320 30
  tx-ring-limit 3
  protocol ppp Virtual-Template1
!
interface Virtual-Template1
 bandwidth 320
```

```
 ip unnumbered Loopback1
 service-policy output 1751_DSL
 ppp multilink
 ppp multilink fragment-delay 4
 ppp multilink interleave
!
access-list 100 permit udp any any precedence critical
!
dial-peer voice 201 voip
 destination-pattern 3640200
 session target ipv4:10.0.0.11
 ip qos dscp cs4 media
 ip qos dscp cs4 signalling
```

DiffServ

DiffServ addresses the clear need for relatively simple and coarse methods of categorizing traffic into different classes and applying QoS parameters to those classes. DiffServ supports class-based marking.

Cisco Express Forwarding (CEF) mode is required for DiffServ support. To enable CEF, enter the **ip cef** command.

Configuration Example

The following example shows a Cisco 1751 router configured with DiffServ:

```
access-list 102 permit udp host 16.0.0.4 host 15.0.0.5
access-list 103 permit udp host 16.0.0.4 host 13.0.0.5
ip cef
class-map match-all traffic-INTRA
 match access-group 102
class-map match-all traffic-INTER
 match access-group 103
class-map match-all traffic-dscp1
 match ip dscp 1
class-map match-any traffic-prec3
 match ip dscp 24
 match ip dscp 25
 match ip dscp 26
 match ip dscp 27
policy-map DSL-out
 class traffic-INTRA
  bandwidth percent 8
 class traffic-dscp1
  set ip dscp 5
 class traffic-prec3
  set ip precedence 2
 class traffic-INTER
  bandwidth percent 8
 class class-default
  fair-queue
!
interface ATM0/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM0/0.1 point-to-point
mtu 576
 ip address 1.0.0.1 255.0.0.0
 pvc 99/99
  protocol ip 2.0.0.2 broadcast
  vbr-nrt 142 142 1
```

```
  tx-ring-limit 3
  oam-pvc 0
  oam retry 5 5 1
  encapsulation aal5snap
  service-policy out DSL-out
!
dial-peer voice 201 voip
 destination-pattern 3640200
 session target ipv4:14.0.0.3
 ip qos dscp cs4 media
 ip qos dscp cs4 signaling
```

Committed Access Rate

Committed access rate (CAR) allows you to limit bandwidth transmission rates to traffic sources and destinations and allows you to specify policies for handling traffic that conforms to or breaches the specified bandwidth allocations.

CEF mode is required for CAR support. To enable CEF, enter the **ip cef** command.

To enable CAR, enter the **rate-limit** command under the atm interface.

Configuration Example

The following example shows a Cisco 1751 router configured with CAR:

```
ip cef
interface ATM0/0.1 point-to-point
 mtu 576
 ip address 10.0.0.10 255.255.255.0
 rate-limit output 368000 2000 2000 conform-action set-dscp-transmit 40 exceed-action set-
dscp-transmit 48
 pvc 0/33
  protocol ip 10.0.0.9 broadcast
  vbr-nrt 142 142 1
  encapsulation aal5snap
 !
```

Multilink PPP over ATM with Link Fragmentation and Interleaving

This feature allows multilink PPP (MLPPP) encapsulation over a single slow link to fragment and interleave (LFI) packets to a small enough size that the delay requirements of delay-sensitive traffic will be met.

Fragment size at the MLPPP bundle can be configured by using the virtual-template interface **bandwidth** command and the **ppp multilink fragment-delay** command. The ideal fragment size for MLPPP over ATM should allow the fragments to fit into an exact multiple of ATM cells. These commands calculate fragment size by using the following formula:

fragment size = bandwidth x fragment-delay / 8.

For example, if the MLPPP ATM header is 10 bytes and the AAL5 packet overhead is 8 bytes, the fragment size for MLPPP over ATM can be calculated as follows:

fragment size = 48 x the number of cells - 10 - 8.

In this case, two cells per fragment are desirable, so the fragment size is calculated at 78 bytes.

The total bandwidth usable on this interface is 75 percent of the value declared in the **bandwidth** command. To change this default value, enter the **max-reserved-bandwidth** command.

LLQ must be enabled when you configure MLPPP with link fragmentation and interleaving.

Note Cisco 1700 series routers support only PPP encapsulation for MLPPP with link fragmentation and interleaving. The dialer interface is not supported.

Configuration Example

The following example shows a Cisco 1751 router configuration with MLPPP/LFI:

```
class-map match-all VOIP
 match ip dscp 32
class-map CRITICAL
match access-group 100
!
policy-map 1751_DSL
 class CRITICAL
 priority 48
class VOIP
 priority 64
 set ip precedence 6
!
interface ATM0/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM0/0.1 point-to-point
 pvc 0/33
 vbr-rt 150 150 30
 tx-ring-limit 3
 protocol ppp Virtual-Template1
!
interface Loopback1
 ip address 10.0.0.10 255.255.255.255
interface Virtual-Template1
 bandwidth 320
 ip unnumbered Loopback1
 service-policy output 1751_DSL
 ppp multilink
 ppp multilink fragment-delay 4
 ppp multilink interleave
!
access-list 100 permit udp any any precedence critical
!
dial-peer voice 201 voip
 destination-pattern 3640200
 session target ipv4:10.0.0.11
 ip qos dscp cs4 media
 ip qos dscp cs4 signalling
```

Weighted Random Early Detection

You can set a queuing technique on a device's interface to manage how packets are handled when an interface starts to become congested. The queuing technique available for congestion avoidance is called *weighted random early detection* (WRED).

WRED allows the interface to start dropping packets from selected flows when traffic begins to exceed the interface's traffic thresholds, but before congestion occurs. If the dropped packets are TCP packets, the TCP source recognizes that packets are being dropped, and then lowers its transmission rate. The lowered transmission rate reduces the traffic to the interface, thus avoiding congestion. Because TCP retransmits dropped packets, no actual data loss occurs.

Note WRED parameters cannot be configured on a physical ATM interface or the VC-bundle level. You must create one or more WRED parameter groups and then attach the parameter group to each PVC. By using this method, you can apply the same WRED settings to multiple PVCs without needing to configure each PVC and maximum packet limit. The bandwidth assigned to a class is the guaranteed bandwidth delivered to the class during congestion.

Configuration Example

The following example shows a Cisco 1751 configured with WRED:

```
random-detect-group 1751_DSL
 exponential-weighting-constant 5
 precedence 2 96 256 100
 precedence 5 192 256 100
!
interface ATM0/0
 no ip address
 no atm ilmi-keepalive
 !
interface ATM0/0.1 point-to-point
 ip address 1.0.0.1 255.0.0.0
```

```
 pvc 88/88
  random-detect attach 1751_DSL
  protocol ip 2.0.0.2
  vbr-rt 320 320 30
  oam-pvc 40
  oam retry 3 5 1
  encapsulation aal5snap
!
```

ATM per-VC Queuing and VC Bundling

Parameters can be applied to individual VCs either by using VC classes or by directly applying them to the bundle members. Parameters applied to an individual VC supersede bundle-level parameters. Parameters applied directly to a VC take precedence over the same parameters applied within a class to the VC at the bundle-VC configuration level.

All of the QoS features are supported in per-virtual circuit (VC) and VC bundling mode. The default is per-VC queuing mode.

VC bundling allows individual VCs going to the same destination to be grouped together. Traffic mapping to each VC is based on traffic protocol criteria such as IP precedence. (VC bundling is not supported for MLPPP/LFI.)

To enable VC bundling, enter the **bundle** command under the ATM interface.

Configuration Example

The following example shows a VC bundling configuration:

```
vc-class atm atm-bundle
  broadcast
  oam-pvc manage 1
  oam retry 3 3 1
  encapsulation aal5snap
  protocol ip inarp broadcast
  oam-bundle manage 1
!
vc-class atm vip
  vbr-rt 256 256 20
  precedence 5-7
  bump implicit
  no protect vc
  no protect group
!
vc-class atm high
  vbr-rt 256 256 20
  precedence 2-4
  bump implicit
  no protect vc
  no protect group
!
vc-class atm normal
  vbr-rt 256 256 20
  precedence 0-1
  bump explicit 2
  no protect vc
  no protect group
!
interface ATM0/0
  no ip address
  no atm ilmi-keepalive
 !
```

```
interface ATM0/0.1 point-to-point
  ip address 2.0.0.2 255.255.0.0
  bundle 1751_DSL
  class-bundle atm-bundle
  pvc-bundle vip 0/33
   class-vc vip
  pvc-bundle high 0/34
   class-vc high
  pvc-bundle normal 0/35
   class-vc normal
```

ATM Cell Loss Priority Bit Marking

When congestion occurs in an ATM network, ATM cells are discarded. One way to control which cells are discarded is to use the cell loss priority (CLP) bit in the ATM header of each cell. The CLP bit may be set to either 1 or 0. Cells with the CLP bit set to 1 are always discarded before any of the cells with the CLP bit set to 0.

The ATM CLP bit marking feature allows you to control the CLP setting on Cisco routers. The marking of the CLP bit is implemented on a per-packet basis so that the CLP bit of every ATM cell that belongs to a particular packet is set to either 0 or 1.

Configuration Example

The following is an example of enabling ATM CLP Bit Marking using the **set atm-clp** command and modular QoS command-line interface. In this example, all output packets that have an IP Precedence value of 0 are sent with the CLP set to 1. Note that IP CEF must be on when using ATM CLP bit marking.

```
ip cef
class-map match-all prec0
 match ip precedence 0

policy-map ATM_OUT
 class prec0
 set atm-clp

interface ATM0/0
 pvc 0/33
 service-policy output ATM_OUT
```

Compressed RTP

The Real-Time Transport Protocol (RTP), as described in RFC 1889, is used to carry real-time data for voice and video applications. For a typical Voice over IP (VoIP) application, the payload portion of the packet can be smaller than the header. For instance, using the G.729 codec, the payload is 20 bytes, but the IP, User Data Protocol (UDP), and RTP header is 40 bytes. It is inefficient to send the IP, UDP, and RTP header across a slow link without compressing it. The Compressed Real-Time Transport Protocol (cRTP) feature, as defined in RFC 2508, addresses this inefficiency by making the VoIP packet headers smaller.

The basic premise of cRTP is that although several fields in the IP, UDP, and RTP header change from packet to packet, the differences in these fields from packet to packet are constant. The compression scheme in cRTP is to encode the header to reduce the size of information to be transmitted. With cRTP, a 40-byte IP, UDP, and RTP header of a VoIP packet can be compressed to 2 to 4 bytes per packet, yielding approximately 11.2 kbps of bandwidth for a G.729 codec call with RTP.

cRTP can be applied to an ATM link through cRTP for MLP over ATM, or through cRTP for PPP over ATM.

Configuration Example

The following are examples of cRTP for MLP over ATM, and cRTP for PPP over ATM. The **ip rtp header-compression** command sets cRTP.

cRTP Using MLP over ATM

```
interface Loopback1
 ip address 10.0.0.9 255.255.255.255
!
interface ATM0/0
 no ip address
!
dsl equipment-type CPE
dsl operating-mode GSHDSL symmetric annex A
dsl linerate AUTO
!
interface ATM0/0.1 point-to-point
 pvc 0/33
  ip 10.0.0.10
  vbr-rt 320 320 30
  tx-ring-limit 3
  protocol ppp Virtual-Template1
!
interface Virtual-Template1
 bandwidth 320
 ip unnumbered Loopback1
 ip tcp header-compression iphc-format
 service-policy output ADSL-2
 ppp multilink
 ppp multilink fragment-delay 4
 ppp multilink interleave
 ip rtp header-compression iphc-format
```

cRTP Using PPP over ATM

```
interface Loopback1
 ip address 10.0.0.9 255.255.255.255
!
interface ATM0/0
 no ip address
!
dsl equipment-type CPE
dsl operating-mode GSHDSL symmetric annex A
dsl linerate AUTO
!
interface ATM0/0.1 point-to-point
 pvc 0/33
  protocol ip 10.0.0.10
  vbr-rt 320 320 30
  tx-ring-limit 3
  protocol ppp Virtual-Template1
!
interface Virtual-Template1
 bandwidth 320
 ip unnumbered Loopback1
 ip tcp header-compression iphc-format
 service-policy output ADSL-2
 ip rtp header-compression iphc-format
```

Tunable Transmission Ring

The transmission (tx) ring is the first-in, first-out (FIFO) buffer used to hold frames before transmission at the DSL driver level. The tx ring defines the maximum number of packets that can wait for transmission at Layer 2.

The tx ring complements the ability of LLQ to minimize jitter and latency of voice packets. For maximum voice quality, a low tx ring setting should be used. For maximum data throughput, a high tx ring setting should be used.

You can configure the size of the tx ring for each permanent virtual circuit (PVC). The default value is 60. However, the value of the setting can be from 2 through 60.

Note A low tx ring setting, such as 3, is required for latency-critical traffic.

For example, when the tx ring limit is configured as 3 and LLQ is configured on the PVC, the worst-case delay for a voice packet is the time required to transmit three data packets. When the buffering is reduced by configuring the tx ring limit, the delay experienced by voice packets is reduced by a combination of the tx ring and LLQ mechanism.

Note The size of the tx ring buffer is measured in packets, not particles.

Configuration Example

The following example is a configuration of the tx ring limit on an ATM PVC interface. To enable the tx ring limit, enter the **tx-ring-limit** command.

```
class-map match-all VOIP
 match ip dscp 32
class-map CRITICAL
 match access-group 100
!
policy-map 1751_DSL
 class CRITICAL
  priority 48
 class VOIP
  bandwidth 64
  set ip precedence 6
!
interface Loopback1
ip address 10.0.0.10 255.255.255.252
!
interface ATM0/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM0/0.1
 pvc 0/33
  vbr-rt 320 320 30
  tx-ring-limit 3
  protocol ppp Virtual-Template1
!
interface Virtual-Template1
 bandwidth 320
 ip unnumbered Loopback1
 ip mroute-cache
 service-policy output 1751_DSL
 ppp multilink
```

```
 ppp multilink fragment-delay 4
 ppp multilink interleave
!
access-list 100 permit udp any any precedence critical
!
dial-peer voice 201 voip
 destination-pattern 3640200
 session target ipv4:10.0.0.11
 ip qos dscp cs4 media
 ip qos dscp cs4 signalling
```

MLP Bundling

Multilink PPP (MLP), standardized in RFC 1990, is similar to load balancing techniques in that it sends packets across the individual links in a round-robin fashion. However, MLP adds three significant capabilities:

- Because MLP works at the link layer, it makes an MLP bundle appear as one logical link to the upper layer protocols in the router. Thus, only one network address needs to be configured for the entire MLP bundle.
- MLP keeps track of packet sequencing and buffers packets that arrive early. With this ability, MLP preserves packet order across the entire MLP bundle.
- Packet fragmentation can be enabled to split large data packets into smaller packet fragments that are individually transmitted across the links. In many circumstances, fragmentation can increase the efficiency of the MLP link.

Additionally, when more bandwidth is needed, additional links can be added to the bundle by simply configuring them as members of the bundle. No reconfiguration at the network layer, such as new addressing, is needed. This is also a significant factor when considering the use of advanced router services. For example, a specific QoS can be configured once for the bundle as a whole rather than on each link in the bundle. The trade-off for the increased functionality is that MLP requires greater CPU processing than load-balancing solutions. Packet reordering, fragment reassembly, and the MLP protocol itself increase the CPU load.

Note

- The fragment delay on the multilink interface should be configured on the basis of the desired maximum delay for interleaved packets. Interleaving is useful only at low bandwidths, usually below 1 Mbps, and it is dependent on the link bandwidths, not the bundle bandwidth.
- It is recommended that IP CEF be turned on. IP CEF will result in better performance and ease of configuration.
- Virtual template (VT) should be used (instead of dialer interface) when configuring either authentication or dynamic address assignment for MLP with LFI.

Configuration Example

The following example shows a Cisco 1760 router configured with MLP Bundling:

```
!
interface Multilink1
 ip address 10.0.0.9 255.255.0.0
 load-interval 30
 keepalive 1
 max-reserved-bandwidth 100
 service-policy output CISCO
```

```
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 10
 ppp multilink interleave
 multilink-group 1
!
interface ATM0/0
 no ip address
 no atm ilmi-keepalive
 pvc 0/38
  vbr-rt 192 192 1000
  tx-ring-limit 2
  protocol ppp Virtual-Template1
 !
 dsl operating-mode auto
 no shut
!
!
interface ATM1/0
 no ip address
 no atm ilmi-keepalive
 pvc pvc 6/65
  vbr-rt 192 192 1000
  tx-ring-limit 2
  protocol ppp Virtual-Template1
 !
 !
 dsl operating-mode auto
 no shut
!
!
!
interface Virtual-Template1
 no ip address
 load-interval 30
 keepalive 1
 ppp multilink
 ppp multilink multiclass
 multilink-group 1
!
```

For information on how to verify and troubleshoot MLP Bundling, please refer to *Enhanced Voice and QoS for ADSL and G.SHDSL on Cisco 1700 Series, Cisco 2600 Series, and Cisco 3600 Series Routers.*

Configuring the SCC Clock Rate

Communciation between a DSL WIC and the host in a router takes place through a device called a *serial communications controller* (SCC). Whenever the host wants to transmit data or send any control traffic to the DSL WIC, it uses an SCC. Similarly, when a DSL WIC wants to forward incoming data from the line to the host, it also uses an SCC. Each DSL WIC installed in a router uses two SCCs. One SCC, SCC-A, is used for ATM adaptation layer 5 (AAL5) data traffic, while the other, SCC-B, is used for ATM adaptation layer 2 (AAL2) data traffic and for control traffic. The speed at which an SCC transfers data between the host and the WIC depends on the clock rate with which the SCC has been configured. This clock rate is configured by the user, and it is always synchronous. The SCC clock rate is the same whether the WIC is sending or receiving data through the SCC. For an asynchronous DSL (ADSL) WIC, the SCC clock rate should be set slightly higher than the larger of the DSL line rates (upstream or downstream). It is recommended that the SCC clock rate always be set higher than the DSL line rate to accommodate any SCC overhead.

SCC Clock Rate Configuration

The following example is a configuration of SCC clock rates on an ATM interface. Clock rates are set with the **clock rate aal5** command and the **clock rate aal2** command. On Cisco 1700 series routers, valid clock rates are from 4 Mbps to 8 Mbps. The clock rate values are entered as bits per second, as shown in the example.

```
interface ATM0/0
 no ip address
 clock rate aal5 5300000
 clock rate aal2 4000000
 no atm ilmi-keepalive
 bundle-enable
 bundle ama-bundle12
 !
 dsl operating-mode auto
end
```

Note It is strongly recommended that on Cisco 1700 series routers, the SCC clock rate be set to the default value of 8 Mbps (8000000 bps).

Note When an SCC clock rate is deconfigured on a Cisco 1700 series router by using the **no** form of the command, it is reset to the default value of 8 Mbps.

SCC Clock Rate Verification

To verify the configuration of the SCC clock rate, use the **show controller** command. SCC-A represents the clock rate for AAL5 while SCC-B represents the clock rate for AAL2.

```
Router#show controller atm0/0
Interface: ATM0/0, Hardware: DSLSAR (with Alcatel ADSL Module), State: up
IDB: 82115298 Instance: 82116A4C reg_dslsar:68030000 wic_regs: 68030080
PHY Inst:8213862C Ser0Inst: 8210F690 Ser1Inst: 8211281C us_bwidth:864
Slot: 0 Unit: 0 Subunit: 0 pkt Size: 4528
VCperVP: 256 max_vp: 256 max_vc: 65536 total vc: 1
rct_size:65536 vpivcibit:16 connTblVCI:8 vpi_bits: 8
vpvc_sel:3 enabled: 0 throttled: 0 cell drops: 0
Parallel reads to TCQ:0 tx count reset = 0, periodic safe start = 0
Serial idb(AAL5) output_qcount:0 max:40
Serial idb(RAW) output_qcount:0, max:40
Sar ctrl queue: max depth = 10, current queue depth = 0, drops = 0, urun cnt = 0, total
cnt = 99
Serial idb tx count: AAL5: 0, RAW: 0, Drop count:AAL5: 0, RAW: 0
SCC Clockrates:
    SCC-A = 5300000
    SCC-B = 4000000

WIC   Register     Value      Notes
---- ----------- ---------- ----------
FPGA Dev ID (LB)   0x44      'D'
FPGA Dev ID (UB)   0x53      'S'
FPGA Revision      0x9F
WIC  Config Reg    0x4D       WIC / VIC select = WIC;
```

Configuring FRF.5 and FRF.8 Internetworking Functions

To communicate over WANs, end-user stations and the network cloud typically must use the same type of transmission protocol. This limitation has prevented differing networks such as Frame Relay and ATM from being linked. The Frame Relay–to–ATM Service Interworking feature allows Frame Relay and ATM networks to exchange data despite differing network protocols. The functional requirements for linking Frame Relay and ATM networks are provided by the *Frame Relay/ATM PVC Service Interworking Implementation Agreement* specified in Frame Relay Forum (FRF) documents FRF.5 and FRF.8. The FRF.5 and FRF.8 interworking functions involve multiplexing PVCs between Frame Relay and ATM networks and mapping the control bits between Frame Relay frame headers and ATM cell headers. FRF.5 and FRF.8 are necessary for ATM-based features to interwork with Frame Relay–based IP class of service (CoS) features.

Configuration Examples

These examples show how to configure a mapping between a Frame Relay data-link connection identifier (To communicate over WANs, end-user stations and the network cloud typically must use the same type of transmission protocol. This limitation has prevented differing networks such as Frame Relay and ATM from being linked. The Frame Relay–to–ATM Service Interworking feature allows Frame Relay and ATM networks to exchange data despite differing network protocols. The functional requirements for linking Frame Relay and ATM networks are provided by the *Frame Relay/ATM PVC Service Interworking Implementation Agreement* specified in Frame Relay Forum (FRF) documents FRF.5 and FRF.8. The FRF.5 and FRF.8 interworking functions involve multiplexing PVCs between Frame Relay and ATM networks and mapping the control bits between Frame Relay frame headers and ATM cell headers. FRF.5 and FRF.8 are necessary for ATM-based features to interwork with Frame Relay–based IP class of service (CoS) features.

) and an ATM PVC, using the **connect** command. For a full description of the **connect** command as used in the FRF.5 and FRF.8 internetworking functions, refer to *Enhanced Voice and QoS for ADSL and G.SHDSL on Cisco 1700 Series, Cisco 2600 Series, and Cisco 3600 Series Routers.*

Note For FRF.5 and FRF.8, you may need to match the maximum transmission unit (MTU) between the ATM and Frame Relay networks for large size packets.

FRF.5

The following example shows how to create an FRF.5 connection, using the **network-interworking** keyword in the **connect** command.

```
interface serial0
 no ip address
 encapsulation frame-relay IETF
 no fair-queue
 frame-relay interface-dlci 100 switched
 frame-relay intf-type dce
!
interface atm1
 no ip address
 no atm ilmi-keepalive
 pvc 0/33
 encapsulation aal5mux frame-relay
!
```

```
dsl equipment-type CPE
dsl operating-mode GSHDSL symmetric annex A
dsl linerate AUTO
!
connect frf5 serial0 100 atm1 0/33 network-interworking
```

FRF.8

The following example shows how to create an FRF.8 connection, using the **service-interworking** keyword in the **connect** command.

```
interface serial0
 no ip address
 encapsulation frame-relay IETF
 no fair-queue
 frame-relay interface-dlci 100 switched
 frame-relay intf-type dce
!
interface atm1
 no ip address
 no atm ilmi-keepalive
 pvc 0/33
 encapsulation aal5mux fr-atm-srv
!
dsl equipment-type CPE
dsl operating-mode GSHDSL symmetric annex A
dsl linerate AUTO
!
connect frf8 serial0 100 atm1 0/33 service-interworking
```

New or Changed IOS Commands

This section gives the new or changed Cisco IOS commands for configuring the ADSL or G.SHDSL WIC features. All other commands used to configure the ADSL or G.SHDSL WIC features are documented in the following publications:

- The “Configuring ATM” section of the *Cisco IOS Wide-Area Networking Configuration Guide*
- The “ATM Commands” section of the *Cisco IOS Wide-Area Networking Command Reference*

Reference information for the following commands is provided in *Enhanced Voice and QoS for ADSL and G.SHDSL on Cisco 1700 Series, Cisco 2600 Series, and Cisco 3600 Series Routers.*

- **clock rate**
- **ppp multilink multiclass**
- **connect** (FRF.5 and FRF.8)
- **tx-ring-limit**

Reference information is provided below for configuring the card on the router, using these commands:

- **dsl equipment-type**
- **dsl linerate**

dsl equipment-type

To configure the DSL ATM interface to function as central office equipment or customer premises equipment, use the **dsl equipment-type** ATM interface command.

Use the **no** form of this command to restore the default equipment type.

dsl equipment-type {**co** | **cpe**}

no dsl equipment-type

Syntax Description

co	Configures the DSL ATM interface to function as central office equipment.
cpe	Configures the DSL ATM interface to function as customer premises equipment.

Defaults

The DSL ATM interface functions as customer premises equipment.

Command History

Release	Modification
12.2(4)T	This command was introduced for the WIC-1SHDSL.

Usage Guidelines

This configuration command applies to a specific ATM interface. You must specify the ATM interface before you enter this command.

The ATM interface must be in the shutdown state before you enter this command.

Examples

The following example configures DSL ATM interface 1/1 to function as central office equipment.

```
router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# int atm 1/1
router(config-if)# dsl equipment-type co
router(config-if)# end
router# clear interface atm 1/1
router#
```

Related Commands

Command	Description
dsl linerate	Specifies a line rate for the DSL ATM interface.

dsl linerate

To specify a line rate for the DSL ATM interface, use the **dsl linerate** ATM interface command.

Use the **no** form of this command to restore the default line rate.

dsl linerate {*kbps* | **auto**}

no dsl linerate

Syntax Description

kbps	Specifies a line rate in kilobits per second for the DSL ATM interface. Allowable entries are:**200, 264, 328, 392, 456, 520, 584, 648, 712, 776, 840, 904, 968, 1032, 1096, 1160, 1224, 1288, 1352, 1416, 1480, 1544, 1608, 1672, 1736, 1800, 1864, 1928, 1992, 2056, 2120, 2184, 2248, and 2312**.
auto	Configures the DSL ATM interface to automatically train for an optimal line rate by negotiating with the far-end DSLAM or WIC.

Defaults

The DSL ATM interface automatically synchronizes its line rate with the far-end DSLAM or WIC.

Command History

Release	Modification
12.2(4)T	This command was introduced on the WIC-1SHDSL.

Usage Guidelines

This configuration command applies to a specific ATM interface. You must specify the ATM interface before you enter this command.

The ATM interface must be in the shutdown state before you enter this command.

Examples

The following example configures DSL ATM interface 0/1 to operate at a line rate of 1040 kbps:

```
router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# int atm 0/1
router(config-if)# dsl linerate 1096
router(config-if)# end
router# clear interface atm 0/1
router#
```

Related Commands

Command	Description
dsl equipment-type	Configures the DSL ATM interface to function as central office equipment or customer premises equipment.

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.

- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.