Highlight of Changes in this Release

- **Cisco Compatible Management**:
  - ability to configure and manage the 833IS using a command structure based on Cisco IOS version 12. For Perle specific features, new commands are implemented that follow the syntax of the Cisco command set
  - configuration to be performed by a telnet session to the 833IS (IP must be used)
  - up to five concurrent telnet sessions
  - memory is organized like a disk drive with files stored under different file systems; commands are available to view file directories, copy and erase files
  - the current GUI manager is no longer needed to configure and manage the 833IS but is still available for this purpose if required
  - all new features will be implemented under both management methods

- **Re-organized screens in the GUI Manager**
  - the majority of screens have been reorganized by grouping related parameters together using Window tab folders
  - the interface is more "drag-and-drop"
  - some little-used parameters and those that could not be supported under the Cisco command structure have been eliminated
  - configurations saved in a text file format

- **Changes to 833IS defaults when using the Manager**
  - when using the Manager to configure the 833IS, the following has been changed:
    - UDP port for Radius authentication and accounting servers now default to 1645 and 1646 respectively

- **New options for installing the Manager from Diskette**

- **Factory Mode setup has been changed for IP networks**
  - to get the 833IS communicating on a IP network, the IP address and default gateway must still be entered from the front panel; however, the changes take effect immediately without requiring a reboot

- **Two configurations are stored in the 833IS – start up and running configuration**
  - the start up configuration is used after a reboot and this is the configuration the server will use after it has been booted up
  - the running configuration is often the same as the start up configuration; it changes when commands are issued in the Cisco configuration mode to modify any operating parameters; whenever possible, changes take effect immediately without a reboot. These changes are not saved after a server reboot unless they

are copied from the running configuration to the start up configuration
- when the server is in factory mode, it does not use either the start up or running configuration

- **Added Syslog Event Message support to a Syslog UNIX or Windows server**

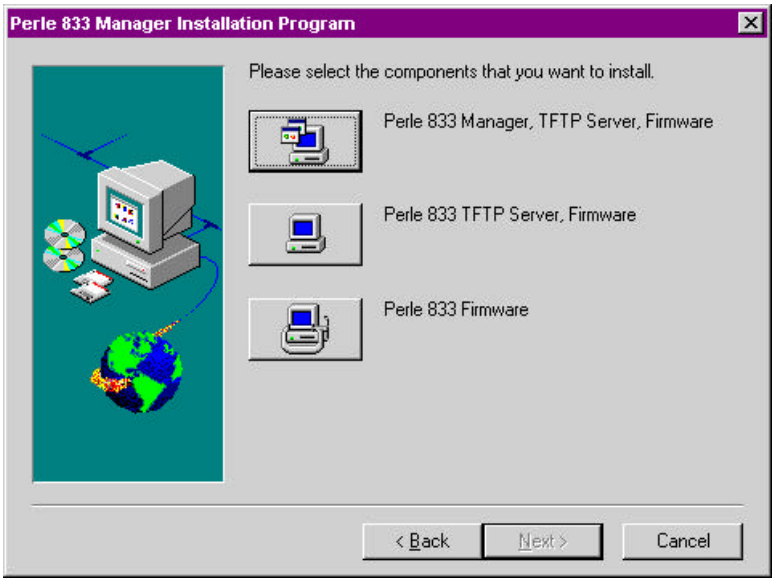
- **Added the ability to disconnect a specific user connected to the 833IS**

The ***readme.txt*** file on the Manager disks contains a full description of the changes in this release along with a list of non-conformances that were corrected in this version.

Implications of Upgrading to V7.00

- Manager V7.00 and higher cannot connect to and manage 833IS or 833AS servers running firmware V6.xx or earlier; it can read in configurations saved under earlier firmware versions and re-save them in Cisco format
- servers running IP are no longer auto-detected by the manager – they can only be detected using directed IP (need to specify the address of the server in the manager)
- when connecting to the server from the Manager in Win95, the PC must have Microsoft's Winsock2 patch installed. This update can be obtained at: www.microsoft.com/Windows95/downloads/contents/WUAdminTools/S_WUNetworkingTools/W95Sockets2/Default.asp
- CHAP and PAP parameters are no longer configurable in the user database and PPP setup screens
- the Manager is now a full 32-bit application and is no longer supported under Win 3.x – it will work under Win 9x, NT 4.0 workstation, Win 2000 Professional
- the Manager and the accompanying manuals is only available in English
- existing 833IS units require a Feature Upgrade kit in order to run the V7.00 Manager – the main hardware component of this kit is a 4M SIMM upgrade

New Options For Installing the Manager from Diskette



There is now an option to install components separately using the Manager diskette:

- Manager – this option installs the Manager application, the TFTP server application, and all the firmware
- TFTP Server – this option installs the TFTP server and all firmware files
- Firmware – this option installs just the firmware

Factory Mode Setup on IP Networks

0123F456+	On power-up, the 833IS will display this on the screen. The "F" between the 3 and the 4 indicates it is booting up in factory mode. (An "R" means it is booting up in running mode). The "+" sign will alternate with a "-" sign to show activity.
Initializing …	Just before the 833IS is ready to come up, this appears on the screen.
PERLE 833IS	The boot up process is now complete.
No Manager	After a short pause, the screen shows this to indicate it is not communicating with the Manager **Press the RIGHT arrow.**
Manager Setup	**Press the DOWN arrow.**
IP Address	**Press the ENTER and input the IP address of the server. Press ENTER when done.** **Press the DOWN arrow.**

IP Subnet Mask
255.255.255.0

A default subnet mask is automatically filled in. If this is correct, **press the DOWN** arrow. Otherwise, **press the ENTER and input the IP address of the subnet mask. Press ENTER when done.**

Press the DOWN arrow.

Default Gateway

If the PC used to configure this server is on another LAN segment, you must enter the address of the gateway here. **Press ENTER to input the gateway address and ENTER when done.**

Press the DOWN arrow.

LAN Speed
Auto Detect

For an Ethernet LAN, use the **RIGHT** arrow key to set the speed to **Auto Detected, 100 Mbits, or 10 Mbits**.

For a Token Ring LAN, use the **RIGHT** arrow to set the speed to **4 Mbps or 16 Mbps.**

Press the DOWN arrow.

Port
RJ45

If the card has an ethernet interface and it contains both a BNC and RJ45 connector, this screen will be shown. Use the **RIGHT** arrow to select the port to connect to the LAN – RJ45, BNC, or Auto Detect.

Press the DOWN arrow.

Save Config

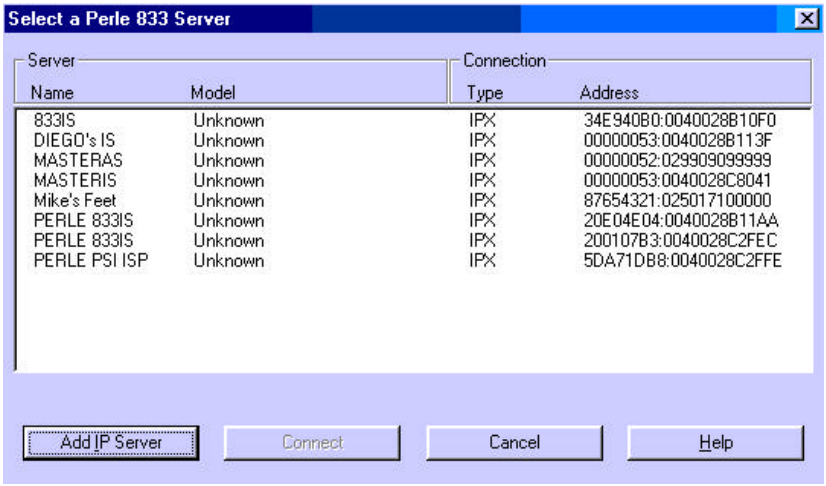
If you want to save the changes to the start-up configuration, **press ENTER.** Then press **ENTER** again to confirm.

NOTE: It is not necessary to save the changes for the configuration to take effect.

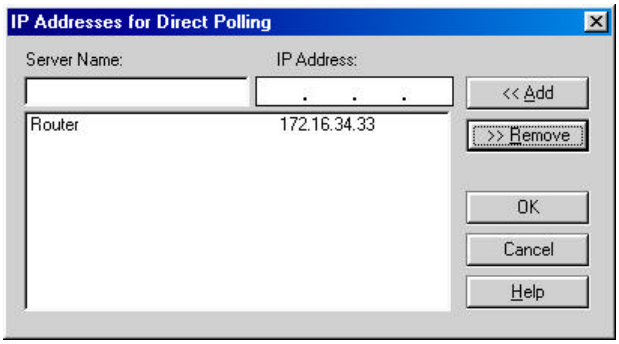
The front panel configuration is complete. **DO NOT REBOOT THE 833IS AT THIS POINT. IF YOU DO, ALL CHANGES WILL BE LOST EVEN IF YOU HAD SAVED THE CONFIGURATION BECAUSE THE START-UP CONFIG FILE IS NOT READ IN FACTORY MODE.** Connect to the 833IS using the Manager or via a telnet session if using Cisco Configuration Mode.

833IS Manager

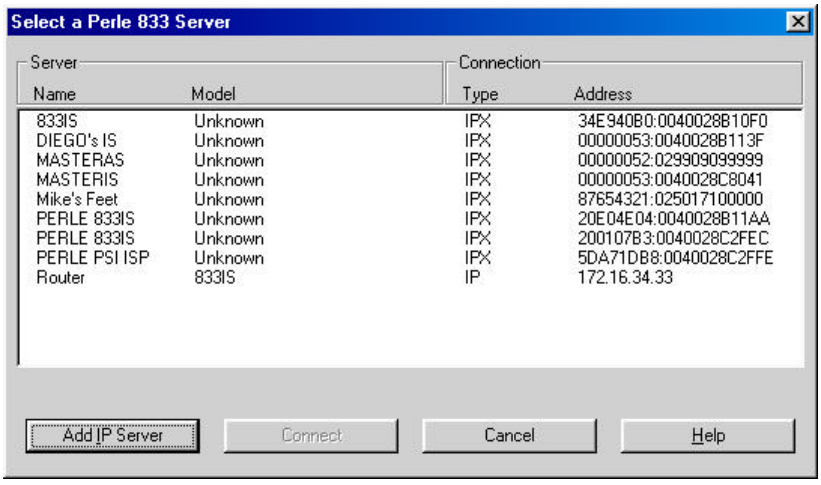
The Manager will no longer auto detect servers running on IP. This results in less IP broadcast traffic on the network. Click on the **Add IP Server** to send a directed message to the 833IS.



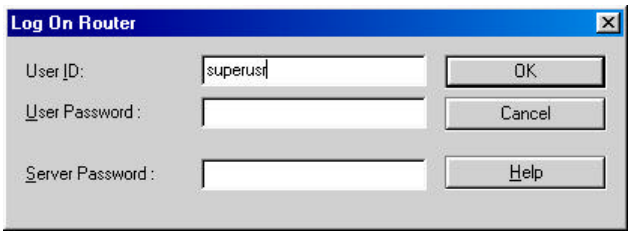
Enter any name in the **Server Name** field and the **IP Address** of the server. Click on **Add** and then **OK.**



If everything is OK, the server will show up on the list. Select it and click on **Connect.**



The default **User ID** is ***superusr.*** Leave the **User Password** and **Server Password** blank. The Manager will require a firmware download before proceeding.



If you have problems getting the Manager to detect the 833IS, try pinging it from the PC. If the 833IS received the ping, the front panel will show the IP address of the PC sending the ping request and the number of requests it received. If the front panel does not show this, the 833IS did not receive the ping request.

NOTE: This feature works only when the server boots in factory mode.

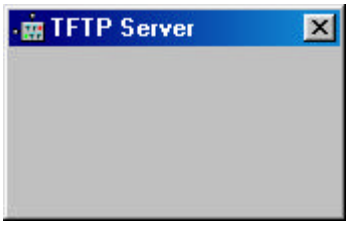
Ping 4
172.16.34.34

Cisco Configuration Mode

On the PC, run telnet and connect to the 833IS. At the **Username** prompt, enter ***superusr***. Hit **<*Enter*>** at the **Password** prompt. Notice that the system prompt is **PERLE 833IS(boot)>**. The "boot" indicates that firmware has not been downloaded to the unit. The ">" indicates we are in user mode. In order to download firmware, we must be in Privilege Exec mode. Type the command **enable** to enter this mode.

Before the firmware can be downloaded, the PC must be running a TFTP server. There is one provided on the manager disks created in the directory specified during the installation.

Execute the program Tftp_svr.exe. A small window opens.



When transferring files, make sure to specify the path to the source file from the directory where the TFTP application is executed . The firmware files can be found under the directory specified in the installation in the sub-directory:

download\833is\pcc6600s.img	for S/T interface
download\833is\pcc6600u.img	for U interface

If you have problems getting the Telnet to connect to the 833IS, try pinging it from the PC. If the 833IS received the ping, the front panel will show the IP address of the PC sending the ping request and the number of requests it received. If the front panel does not show this, the 833IS did not receive the ping request.

NOTE: This feature works only when the server boots in factory mode.

Ping **4**
172.16.34.34

Copy the firmware from the TFTP server to 833IS flash memory.

Enter the address of the TFTP server

Enter the source filename (specify a path if necessary). **Do not specify a path for the destination filename.**

```
PERLE 833IS(boot)#copy tftp: flash:
Enter IP address or IPX address? 172.16.34.34
Source filename []? pcc6600s.img
Destination filename [pcc6600s.img]?
Erase flash before copying? [confirm]
Erasing the flash file system will remove all files! Continue? [confirm]
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
TFTP copy succeeded, 1198804 bytes copied
PERLE 833IS(boot)#
```

The 833IS always prompts **Erase flash before copying**. This is to ensure there is enough room on the file system to write in the new file. If there is not enough room for the new file, the copy process will fail. Erasing the flash deletes all files in the flash first before the copy process starts. The final size of the file copied is shown when the process completes.

Enter into global configuration mode.

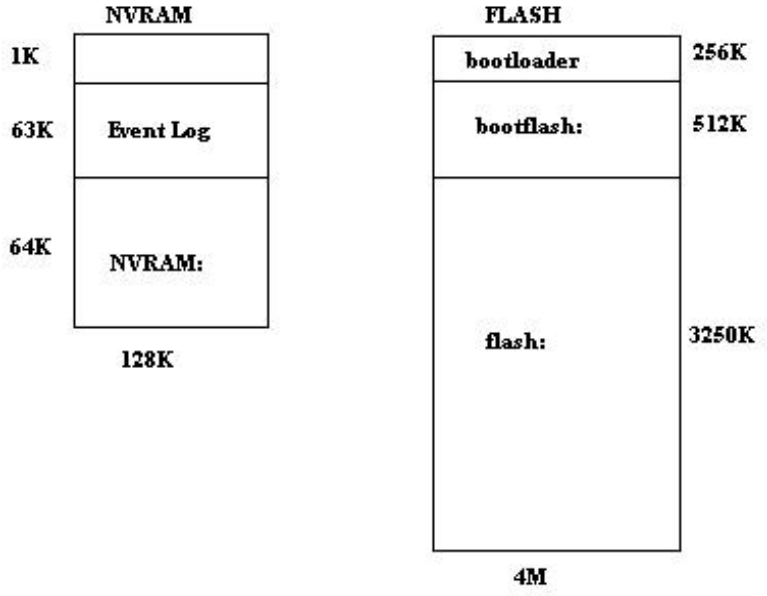
Specifies the firmware to execute on boot up.

```
PERLE 833IS(boot)#configure
PERLE 833IS(boot)(config)#boot system flash pcc6600s.img
PERLE 833IS(boot)(config)#exit
PERLE 833IS(boot)#reload
System configuration has been modified. Save? [yes/no]: y
Verifying checksum ... OK (0XA17E)
483 bytes copied
Proceed with reload? [confirm]
PERLE 833IS(boot)#
```

Command to reset the server.

Information entered from the front panel is saved to the start-up config if this had not already been done.

833IS File System and Its Configuration Files



To emulate the operation of Cisco routers, the memory on the 833IS are divided into file systems. These file systems work like logical drives like A: and C: drives in DOS. These drives are transparent to the user when using the Manager.

Event Log – this is not a logical drive. This is where the event log is stored. In previous releases, the event log occupied virtually all of NVRAM. With V7.00, it is effectively reduced in size by a half.

bootloader – this is the code called from the BIOS. It completes the startup sequence of the unit.

NVRAM: logical file system where the startup-config file is stored. No other files can be written here.

bootflash: logical file system where the factory version of firmware is stored. This file and the entire file system is read-only.

flash: logical file system where the running firmware file. This file system is read/write and any other files can be written here.

tftp: logical file system used to reference files on the TFTP server.

Configuration Files
The 833IS now maintains two configuration files – startup-config and running-config. When the 833IS boots up, it always uses the configuration saved in startup-config. Any configuration changes made using the Manager are automatically saved here. Any configurations made in Cisco mode are saved in the running-config in RAM. These changes take effect immediately (with a few exceptions) without a reboot but are lost when the 833IS is rebooted and the changes are not saved to the startup-config. When a reload is requested, the user is prompted to update the startup-config if the running-config is changed.

Deleting Files
When files are deleted from flash, they are only marked as deleted so they do not show up in a directory list. It is therefore very easy to undelete a file. However, the space occupied by deleted files are not reused so eventually the flash runs out of space even if there are no active files. The space occupied by deleted files can only be recovered by formatting the flash. However, be careful when doing this as this also deletes the firmware file. If the unit does not see a firmware file when booting, it will come up in factory mode.

Cisco Configuration Mode

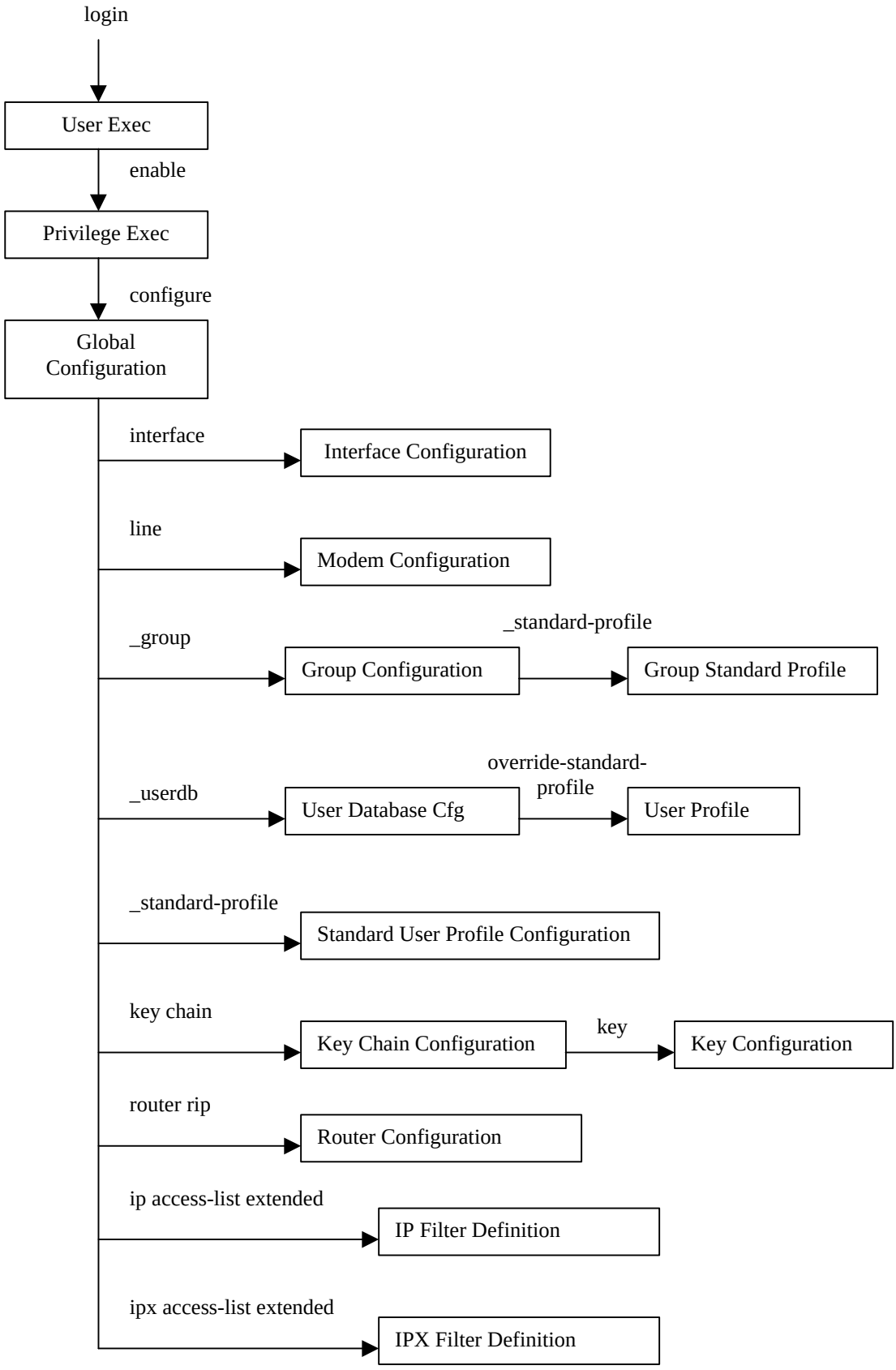
The Cisco configuration mode is designed for personnel trained and familiar with the configuration of Cisco products to manage and configure the 833IS in a similar fashion. For all other users, it is recommended that they use the GUI interface to perform these tasks. In the Cisco configuration mode, there are several important differences between the implementation on the 833IS and in the typical Cisco product:

- Initial configuration of the 833IS (factory mode) is performed through the front panel instead of a direct connection using a serial interface
- There is no equivalent Cisco "setup" script to interactively generate an initial configuration. It is recommended that the Windows-based 833IS Manager be used to create the base configuration which can then be refined afterwards using the Cisco configuration mode.
- The Cisco configuration mode of the 833IS is based on Cisco IOS version 12. Some Cisco commands support additional parameters not present in the 833IS version. If these commands are executed from a file, the additional parameters are ignored. Any error messages will be written to a log file. The contents of this file can be viewed using the "show _log" command. If the commands are entered interactively through a telnet session, errors are displayed to the user.
- The Cisco command set does not accommodate all configuration and management features available on the 833IS. As such, new Perle specific commands have been developed for this purpose. The new commands were designed to be of similar syntax and format as equivalent Cisco commands. All Perle specific commands are identified with an underscore ("_") character preceding the command or parameter keyword.
- Cisco products allow access to internal resources such as queues and buffer sizes. The Perle 833IS implementation protects these internal resources and restricts users from modifying them to maintain the server's operational integrity.

Cisco IOS Command Modes

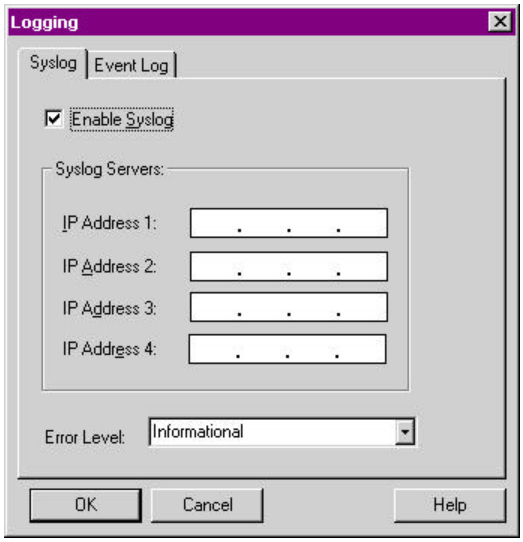
The Cisco IOS command set operate under a number of different modes. There are basically two operating modes: user and privilege. The user exec mode has minimal rights and there are severe restrictions as to what can be done in this mode. It allowsonly a basic ability to monitor the server's operation. The privilege exec mode on the other hand, allows full functionality in the ability to manage and configure the server. Because of the power available in privilege exec mode, access is protected through a password. Users must first login to get into user exec mode plus enter an additional password to enter into privilege exec mode. If no enable password is configured but the user has administrative privileges, the user is also allowed into privilege exec mode.

The configuration of the server within the privilege mode is broken further into additional modes. Each of these modes represent a configuration "area" like the LAN interface, the modem interface, group definitions, user definitions, user profiles, and filter definitions for example. It is important to know which configuration mode is currently active since commands entered only apply to that mode. Also, commands available in one mode may be invalid in a different mode. To assist the user in keeping track of what mode is currently active, the command prompt changes when entering and exiting a mode. The *exit* command is used to leave the current configuration mode returning to the mode from where it entered.


login
User Exec
enable
Privilege Exec
configure
Global Configuration
interface
Interface Configuration
line
Modem Configuration
_group
Group Configuration
_standard-profile
Group Standard Profile
_userdb
User Database Cfg
override-standard-profile
User Profile
_standard-profile
Standard User Profile Configuration
key chain
Key Chain Configuration
key
Key Configuration
router rip
Router Configuration
ip access-list extended
IP Filter Definition
ipx access-list extended
IPX Filter Definition

Mode	**Command Prompt** **(server_name = Router)**	**Command to Enter Mode**	**Function**
User Exec	Router>	login	Monitor server operation
Privileged Exec	Router#	enable	Configure and manage server
Global Configuration	Router(config)#	configure	Configure global parameters
Interface Configuration	Router(config-if)#	interface bri *n* (n=0-7)	Configure BRI ports
		interface dialer 0	Configure WAN port
		interface FastEthernet 0	Configure LAN port (ethernet)
		interface TokenRing 0	Configure LAN port (token ring)
		interface group-Async 0	Configure PPP interface
Line Configuration	Router(config-line)#	line *n* (n=1-16)	Configure modem
Group Configuration	Router(config-group)#	_group *name*	Configure group
User Database Configuration	Router(config-user)	_userdb	Configure user record
Standard Profile Configuration	Router(config-stdUser)#	_standard-profile	Configure user standard profile
	Router(config-group-stdUser)	_standard-profile	Configure group user profile
User Profile Configuration	Router(config-user-override)	override-standard-profile	Configure user profile
Key Chain	Router(config-key-chain)	key chain *name*	Configure RIP key chain
Key Configuration	Router(config-key-chain-key-id)	key *n* (n=0-255)	Configure key
Router Configuration	Router(router-rr)	router rip	Configure RIP
IP Filter Configuration	Router(config-ip-ext-na)#	ip access-list extended *name*	Define and assign IP filters
IPX Filter Configuration	Router(config-ipx-ext-na)#	ipx access-list extended *name*	

Syslog Event Message Support



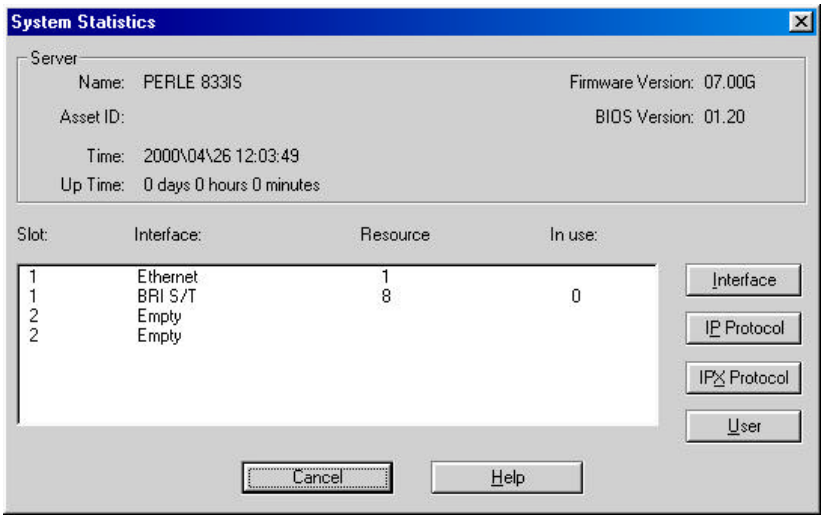
Event message has been improved with the addition of syslog message support. Syslog reporting sends an event log message in real time using UDP protocol to a syslog server. Up to four syslog servers can be configured and all servers are updated simultaneously. These syslog servers can run Windows or UNIX with a syslog daemon application installed. Messages sent to the syslog server are divided into eight severity levels with each level including those messages sent at levels below it. The default severity level is "informational" which is at level 7. The main advantages of using syslog are:

- multiple syslog servers can be configured in case of failure in one of them
- a syslog server can store messages from multiple 833IS servers and other devices using syslog on the network
- the size of the event log file is limited by the storage space on the syslog server – there is no need to worry about the event log information wrapping
- the syslog messages can be further processed and sorted based on time, host name, or other fields

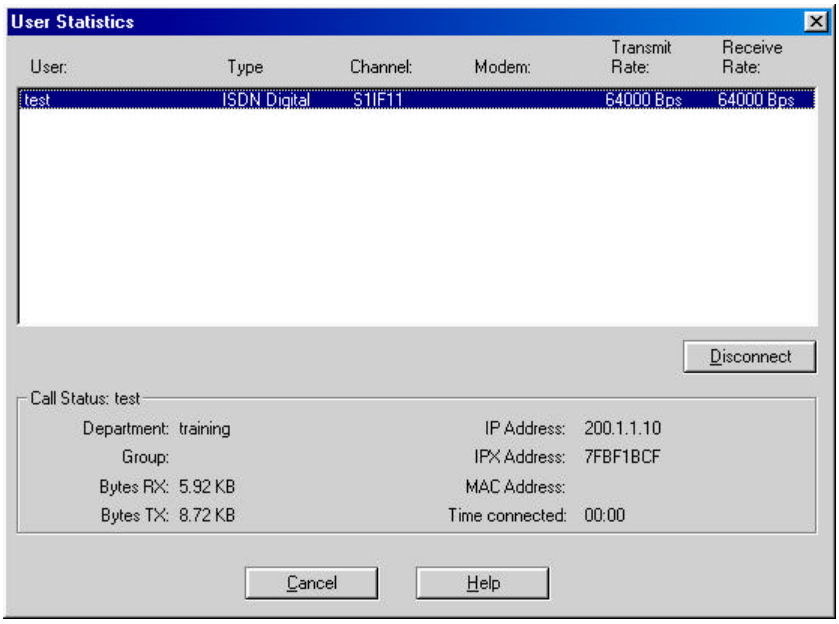
Disconnecting Specific Users

This new feature allows the administrator of the 833IS to disconnect a user that is currently connected through the RAS. If there are multiple users connected using the same user name, then all of them will be disconnected at the same time.

833IS Manager



Click on the **User** button to view users that are currently connected.



Highlight the user(s) to be disconnected then click on **Disconnect.**

Cisco Configuration Mode

clear _user *username*

Note that this command must be executed from the Privilege Exec mode.

Tech Tips

1. IP Address to use on a dial in connection

When dialed into the 833IS, to connect with the Manager, specify the WAN address port of the 833IS in the server list. If you want to use the LAN address port, be sure to add a route entry on the dial in PC with the command:

route add {local LAN network} **mask** {subnet mask of LAN} {833IS WAN port}

The static route entry is automatically removed when the call disconnects so it must be created on every connection.

To connect to the 833IS with telnet the same advice applies -- specify the WAN address port unless you wish to add a static route entry.

2. Simultaneous administration with the Manager and Cisco mode

The 833IS can be administered with one Manager session and four Cisco telnet sessions simultaneously (maximum of five administrative users in total).

3. Manager always uploads the startup-config

The upload and "get configuration" function of the Manager always retrieves the startup-config file. Any changes made from a Cisco telnet session at the same time will not appear in the configuration from the Manager but the changes will still come into effect. As a result, the configuration as seen with theManager may not necessarily be the same configuration running on the server.

4. Do not specify paths for files in the FLASH:

When performing a TFTP transfer and the destination is FLASH:, do not specify a path for the destination filename. This will cause the file transfer to fail.

5. Do not attempt to overwrite the running-config file in FLASH:

Do not attempt to overwrite the contents of the running-config file with another config file. If you try this, the result will be a new running-config file with the contents of both the old config file and the new one. You can replace the startup-config with a new config file however.

6. Clearing the configuration without re-downloading firmware

To clear the configuration without going into factory defaults and reloading the firmware, delete the startup-config file in Cisco config mode. You will need to re-enter the IP address on the front panel

7. Starting the configuration from factory defaults

When bringing up the server from factory defaults with the Manager, after the firmware has been loaded and the server is reset, re-connect with the Manager. After logging in, select **New** on the tool bar instead of uploading the configuration from the server. This will open a configuration with the same Manager defaults as in V6.x. If you upload the configuration from the server, it will use Cisco defaults. This does not enable an authentication protocol for user database security, WAN IP address selection, or the type of routing.

8. Check the error.txt file for configuration load errors.

If the manager cannot read or upload the configuration created in Cisco mode, check the contents of the file "config\error.txt". It will indicate the problems it encountered with the configuration.

9. Encrypting user passwords

To save user passwords in encrypted form, issue the command

service password-encryption

first before entering any user passwords. Then use the command

username test password testpassword

will save passwords in encrypted form. Also, any passwords in the config file that were not encrypted will be after issuing the service command. Note that you cannot decrypt a password in the config file using the command

no service password-encryption

This command will save any future passwords entered in the clear. Also, do not try to encrypt passwords by entering the command

username test password 100 testpassword

It will generate an error saying the encrypted password is not valid.