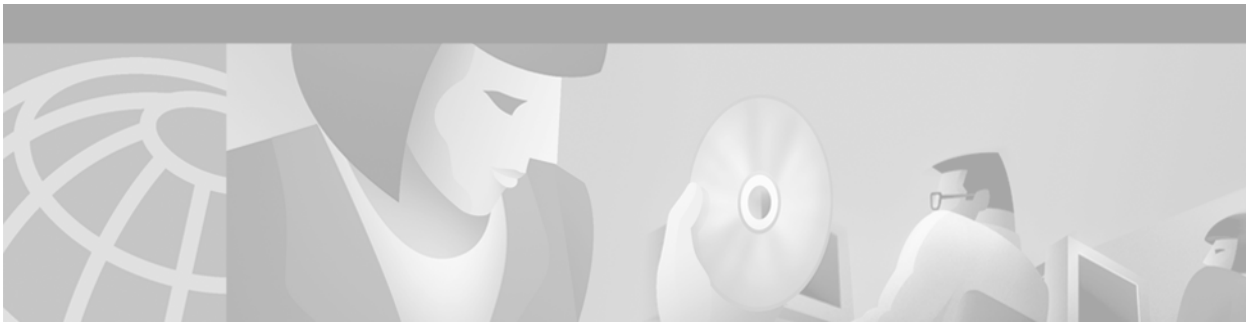


Task 4—Using Syslog, NTP, and Modem Call Records to Isolate and Troubleshoot Faults

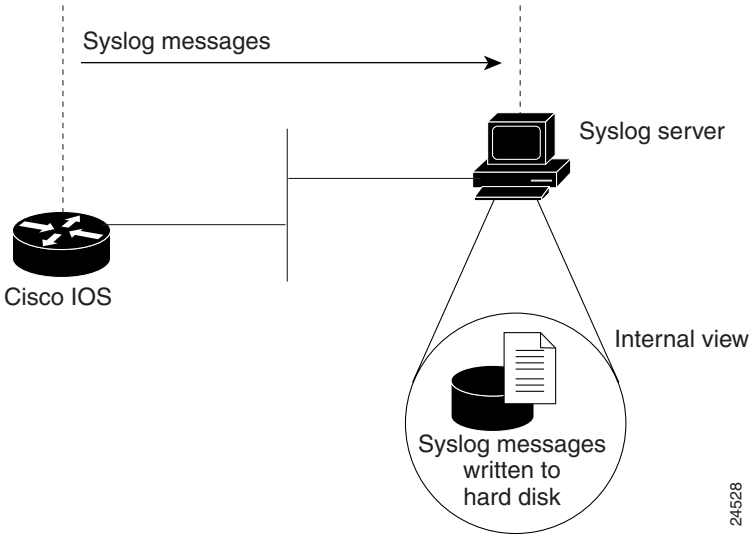
About Syslog

Syslog, Network Time Protocol (NTP), and modem call records work together to isolate and troubleshoot faults in a dial access network.

Syslog enables you to:

- Centrally log and analyze configuration events and system error messages, such as router configuration changes, interface up and down status, modem events, security alerts, environmental conditions, trace backs, and CPU process overloads.
- Capture client debug output sessions in a real-time scenario.
- Reserve telnet sessions for making configurations changes and using **show** commands. Telnet sessions that are cluttered with debug output interfere with troubleshooting procedures.
- Reduce network downtime by knowing when the network has quality problems.

Figure 16 Cisco IOS Sending Syslog Messages to a Syslog Server



You can enable syslog in any Cisco IOS device and send syslog messages to many different destinations (host, buffer, console, history, and monitor).

By using the **logging ?** command, you can see the log settings for distinct destinations:

```
travis-nas-01(config)#logging ?
  Hostname or A.B.C.D  IP address of the logging host
  buffered             Set buffered logging parameters
  console              Set console logging level
  facility             Facility parameter for syslog messages
  history              Configure syslog history table
  monitor              Set terminal line (monitor) logging level
  on                   Enable logging to all supported destinations
  rate-limit           Set messages per second limit
  source-interface     Specify interface for source address in logging
                       transactions
  trap                 Set syslog server logging level
```

There are eight levels of syslog information in the Cisco IOS software. Monitor and manage logs according to the severity level of the syslog message. By using the **logging trap ?** command, you can see the logging severity levels:

```
travis-nas-01(config)#logging trap ?
  <0-7>          Logging severity level
  alerts         Immediate action needed           (severity=1)
  critical       Critical conditions               (severity=2)
  debugging      Debugging messages                (severity=7)
  emergencies    System is unusable                (severity=0)
  errors         Error conditions                  (severity=3)
  informational  Informational messages            (severity=6)
  notifications  Normal but significant conditions (severity=5)
  warnings       Warning conditions                (severity=4)
  <cr>
```

Table 18 Logging Trap Severity Definitions

Message Type	Description	Syslog Message	Severity Level
emergencies	System unusable	LOG_EMERG	0
alerts	Immediate action needed	LOG_ALERT	1
critical	Critical conditions	LOG_CRIT	2
errors	Error conditions	LOG_ERR	3
warnings	Warning conditions	LOG_WARNING	4
notifications	Normal but significant condition	LOG_NOTICE	5
informational	Informational messages only	LOG_INFO	6
debugging	Debugging messages	LOG_DEBUG	7

In this case study, syslog is enabled on all Cisco access servers and backbone routers. Each device sends syslog messages to the same log file on the same syslog server.

The terminology in the syslog messages can vary between different versions of Cisco IOS software. To effectively manage syslog messages, ensure that wherever possible, the same version of Cisco IOS software is running on all routers.

Note For background information on syslog, go to http://www.cert.org/security-improvement/

About NTP

The Network Time Protocol (NTP):

- Provides a synchronized time base for networked routers, servers, and other devices.
- Coordinates the time of network events, which helps you understand and troubleshoot the time sequence of network events. For example, call records for specific users can be correlated within one millisecond.
- Enables you to compare time logs from different networks, which is essential for:
  - Tracking security incidents
  - Analyzing faults
  - Troubleshooting

  Without precise time synchronization between all the various logging, debug output, management, and AAA functions in the network, you cannot make time comparisons.

For a list of NTP clients, go to http://www.eecis.udel.edu/~ntp/software.html

About Modem Call Records

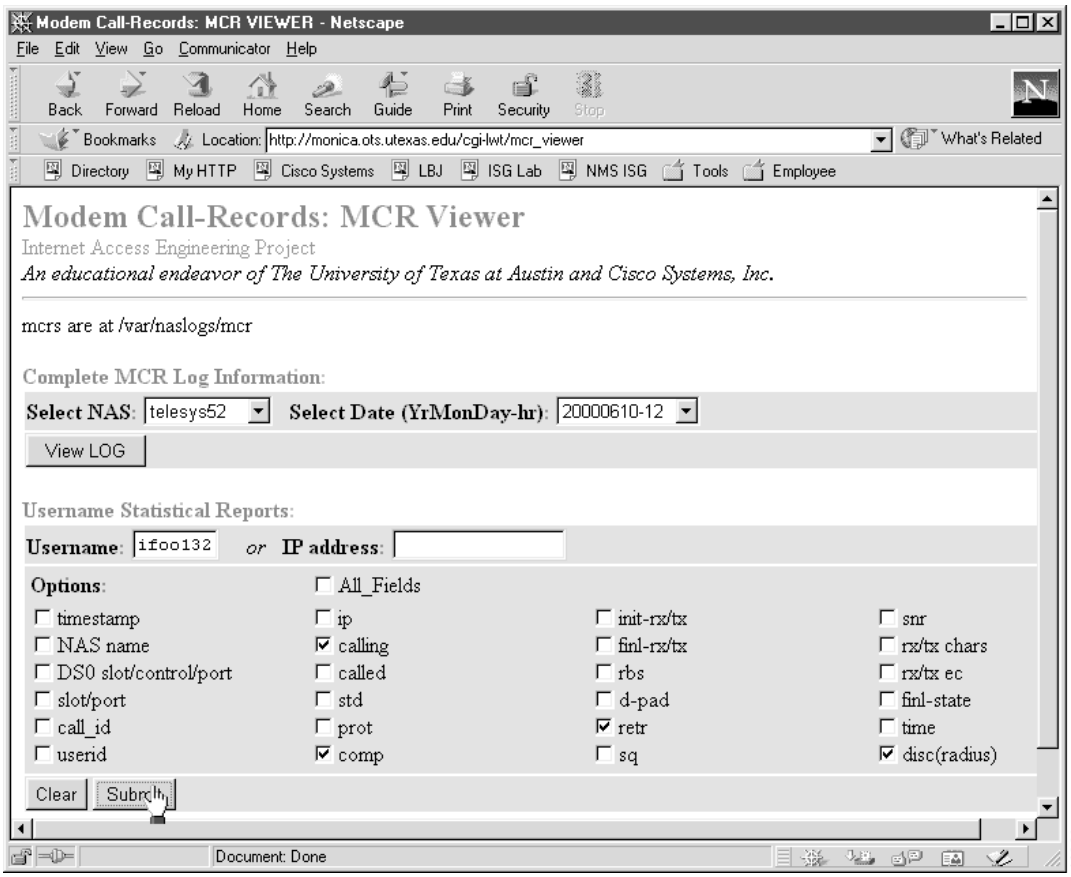
A modem call record (MCR) is a type of syslog message that is:

- Created when a user dials in and hangs up, but it is not generated until the end of the call.
- Used to gather statistics and modem-performance logs on a per-call basis, such as:
  - Modulation trends (V.90 verses V.34).
  - Call time durations (consistent short connection times on a modem, regular Lost Carrier counts).
  - Unavailable user IDs.
  - PPP negotiation or authentication failures.

In this case study, the engineers filter modem call records out of syslog and store them into flat files on a Unix host. The records are sorted by using cron jobs and perl scripts. A web-based MCR viewer facility is used to:

- Search the call records.
- Extract historical and statistical information about individual users and access servers.

Figure 17 Web-Based MCR Viewer



You can view entire log files or portions of logs in the MCR viewer. In addition, you can parse for specific users and other call attributes for a modem call (for example, modulation, error correction, compression, disconnect causes, and retrains).

Note Modem call records are available in syslog starting with Cisco IOS Releases 11.3AA and 12.0T.

Enabling NTP on a Cisco IOS Device

To enable NTP and related clocking services, follow these steps.

Step 1 From the Cisco IOS device, enter the following commands. Enable debug timestamps and include the date, time, and milliseconds relative to the local time zone:

```
!
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
!
```

Step 2 Identify the local timezone and enable recurring time adjustments for daylight savings time by entering the following commands:

```
!
clock timezone CST -6
clock summer-time CST recurring
!
```

Step 3 Locate an NTP server that can be reached by the Cisco IOS device.

Step 4 Specify the IP address for the NTP server and enable automatic-calendar updates by entering the following commands:

```
!
ntp update-calendar
ntp server 172.22.255.1
!
```

Note By default, the **ntp clock-period** command is enabled in some Cisco IOS releases. The Cisco IOS software appends an arbitrary number to the end of the command.

Step 5 Verify that the clock is synchronized with the NTP server by entering the following command:

```
travis-nas-01>show ntp status
Clock is synchronized, stratum 9, reference is 172.22.255.1
nominal freq is 250.0000 Hz, actual freq is 249.9987 Hz, precision is 2**24
reference time is BD123336.28CCF0C4 (18:09:42.159 CST Sat Jul 8 2000)
clock offset is 0.1183 msec, root delay is 61.84 msec
root dispersion is 0.93 msec, peer dispersion is 0.79 msec
travis-nas-01>
```

Inspect the status and time association. Clock sources are identified by their stratum levels. The previous display shows a stratum level nine clock.

Note If the NTP synchronization does not take place, reload the router.

Step 6 Verify that the router is receiving NTP packets from the NTP server by entering the following command:

```
travis-nas-01>show ntp association

      address         ref clock     st  when  poll reach  delay  offset    disp
*~172.22.255.1     127.127.7.1       8   984  1024  377    60.3   -0.89     0.8
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
travis-nas-01>
```

The tilde (~) next to the IP address of the NTP server means the NTP service is configured. The asterisk (*) indicates successful synchronization with the master clock.

Setting Up an NTP Client

To set up an NTP client on a Solaris v2.6 workstation, follow these steps.

Note Additional software is not required to set up NTP on the workstation if it is running Solaris v2.6 (or later).

Step 1 Locate an NTP server that can be reached by the workstation. There are many available NTP servers on the Internet. If your workstation cannot reach the Internet, locate an NTP server within your network.

Note A common practice is to configure an area border router as an NTP server for a particular subnet. The area border router then points to an external NTP server. Other equipment on that subnet uses the loopback 0 IP address on the area border router as an NTP server.

Step 2 Go to the /etc/inet directory and inspect the template file called ntp.client:

```
onionring:~$ cd /etc/inet
onionring:/etc/inet$ more ntp.client
# @(#)ntp.client        1.2     96/11/06 SMI
#
# /etc/inet/ntp.client
#
# An example file that could be copied over to /etc/inet/ntp.conf; it
# provides a configuration for a host that passively waits for a server
# to provide NTP packets on the ntp multicast net.
#

multicastclient 224.0.1.1
```

Step 3 Copy ntp.client and create the ntp.conf configuration file in the /etc/inet default directory:

```
onionring:/etc/inet$ cp ntp.client ntp.conf
onionring:/etc/inet$
```

The NTP daemon reads ntp.conf at startup to locate the NTP server.

Note You must have root-level permissions to edit or copy any files in the /etc/inet/ directory.

Step 4 Edit the ntp.conf file by changing *multicastclient* to **server** followed by the IP address of the target NTP server:

```
# @(#)ntp.client        1.2     96/11/06 SMI
#
# /etc/inet/ntp.client
#
# An example file that could be copied over to /etc/inet/ntp.conf; it
# provides a configuration for a host that passively waits for a server
# to provide NTP packets on the ntp multicast net.
#

server 172.22.255.1
```

Step 5 Go to the directory /usr/lib/inet/ and start the NTP daemon by entering the **xntpd** command. The daemon sets and maintains the time-of-day of the operating system in agreement with the master time server.

```
onionring:/etc/inet$ cd /usr/lib/inet/
onionring:/usr/lib/inet$ ls
in.dhcpd  xntpd
onionring:/usr/lib/inet$ xntpd
onionring:/usr/lib/inet$
```

Step 6 Verify that the NTP daemon is running by entering the **ntpq -p** command:

```
onionring:/usr/lib/inet$ ntpq -p
     remote           refid      st t when poll reach   delay   offset    disp
==============================================================================
*maui-rtr-01.mau CHU(1)           8 u   49   64  377     1.08   -0.131    0.08
onionring:/usr/lib/inet$
```

The following information appears:

- The remote NTP server to which the workstation is connected.
- The reference ID.
- The stratum level of the server.
- The type of NTP packet that was received by the client (local, unicast, multicast, or broadcast).
- The polling interval in seconds.
- The reachability register in octal.
- The current delay of the server in seconds.
- The current offset of the server in seconds and the dispersion of the server in seconds.
- The delay, offset, and displacement between the client and the server in seconds.

When the daemon starts, most of the time values will be zeros until there is a sufficient number of queries taken by the daemon to determine the correct offset.

Troubleshooting the NTP Client

Table 19 NTP Problems and Solutions

Problem	Solution
The ntp.client file or the xntpd daemon cannot be found in the directories shown in the examples.	Verify that the workstation is running Solaris v2.6 or a later version of Solaris. Enter the **uname -a** command to see the version. Versions earlier than Solaris v2.6 do not support NTP and must be supplemented with additional NTP software available from http://www.sunfreeware.com/
The error message "No Associations IDs Returned" when you enter the **ntpq -p** command.	There are three possible solutions: • The network traffic is slow, and the workstation has not had time to poll the NTP server. Allow the workstation enough time to issue the poll (a few seconds); then, enter the **ntpq -p** command. • The mulitcastclient line in the ntp.conf file was not replaced with the server line. • The NTP server you have chosen is down, or it is not configured correctly.

Enabling Syslog and Modem Call Records in the Cisco IOS Software

To enable syslog messages in the Cisco IOS software and send them to a syslog server, follow these steps:

Step 1 Inspect the current logging status by entering the following command:

```
travis-nas-01#show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level debugging, 42 messages logged
    Monitor logging: level debugging, 93 messages logged
    Buffer logging: level debugging, 3 messages logged
    Trap logging: level informational, 121 message lines logged

Log Buffer (8192 bytes):
travis-nas-01#
```

Step 2 Set up a basic syslog configuration by entering the following commands. See Table 20 for command descriptions.

```
!
logging buffered 10000 debugging
no logging console guaranteed
logging console informational
!

!
logging trap debugging
logging facility local0
logging 172.21.100.100
!
```

Table 20 Logging Command Descriptions

Command	Purpose
logging buffered 10000 debugging	Sets the internal log buffer to 10000 bytes for debug output. New messages overwrite old messages. You can tune buffered-logging parameters for collecting logs on a NAS when you are at a remote location. For example, turn on debugs and start logging them in the history buffer. Make your test call; then, re-connect in shell mode and inspect the debugs.
logging console informational **no logging console guaranteed**	Sends the most urgent informational logs to the console port in the event the IP network or syslog server fails. Alternatively, send messages to the console by using the commands **logging console errors** or **logging console warnings**. **Caution** Logging console can cause the router to intermittently freeze up as soon as the console port overloads with log messages. Debugs and modem call records sent to the console port are potentially destructive to the Cisco IOS software.
logging trap debugging	Enables logging up to the debug level (all eight levels).
logging 172.21.100.100	Specifies the IP address of the syslog server.
logging facility local0	Assigns a logging-facility tag (local0) to the syslog messages for this device. The tag must match the facility number configured in the syslog.conf file on the Unix host. See Step 1 in "Configuring the Syslog Daemon" section on page 76. In this case study, each device sends syslog messages to the same log file on the same syslog server.

Step 3 Enable modem call records in the Cisco IOS by entering the following command:

```
!
modem call-record terse
!
```

A modem call record, which is a syslog message, looks like this:

```
May 26 22:04:23.346 CST: %CALLRECORD-3-MICA_TERSE_CALL_REC: DS0 slot/contr/chan=
0/0/0, slot/port=2/14, call_id=26, userid=(n/a), ip=0.0.0.0, calling=4082322078,
 called=3241933, std=V.34+, prot=LAP-M, comp=V.42bis both, init-rx/tx b-rate=264
00/24000, finl-rx/tx b-rate=28800/24000, rbs=0, d-pad=None, retr=1, sq=4, snr=27
, rx/tx chars=136/6470, bad=2, rx/tx ec=134/184, bad=0, time=594, finl-state=Ste
ady, disc(radius)=(n/a)/(n/a), disc(modem)=DF03 Tx (host to line) data flushing
- OK/Requested by host/DTR dropped
```

Step 4 (Optional) To disable syslog messages and SNMP traps when dial interfaces go up and down, use the commands **no logging event link-status** and **no snmp trap link-status**. Although up and down events are legitimate events on dial interfaces, these events should not cause alarms as LAN and WAN interfaces would.

```
!
interface Serial1/0/0:4:23
 no logging event link-status
 no snmp trap link-status
!
interface Group-Async0
 no logging event link-status
 no snmp trap link-status
!
```

In this example, only the fourth T1 of a T3 card is shown.

Note In some Cisco IOS images, the **logging event link-status** command is disabled by default.

Configuring the Syslog Daemon

In this case study, all the syslog messages from the access servers are sent to a single log file. The syslog messages from the backbone routers are sent to a different log file.

To configure the syslog daemon on a Solaris syslog server, follow these steps:

Step 1 On the syslog server, edit the file syslog.conf in the /etc/ directory by using a text editor. To get syslog working, you must add the following line to the file:

```
|
local0.debug     /var/log/router.log
|
```

- The local facility number is **local0.debug**. It must match the facility number configured in the Cisco IOS device. See the **logging facility** command in Table 20.
- The log file path name is **/var/log/router.log**
- One tab exists between the facility number and the path name. Spaces are not permitted. You can define any directory location/path for the .txt log file.

In the following example, the new line is in **bold**:

```
"syslog.conf" 53 lines, 1861 characters
#ident  "@(#)syslog.conf        1.3     93/12/09 SMI"   /* SunOS 5.0 */
#
# Copyright (c) 1991-1993, by Sun Microsystems, Inc.
#
# syslog configuration file.
#
# This file is processed by m4 so be careful to quote (`') names
# that match m4 reserved words.  Also, within ifdef's, arguments
# containing commas must be quoted.
#
#
#
#
```

```
#Following is the new line. It adds a logging facility number and direcory path for the
#log file (router.log).
local0.debug    /var/log/router.log
```

Note The previous syslog.conf example has been abbreviated to fit this document. The actual file size is much larger than the example. Add the new line to the end of the file.

Step 2 Create the log file and check the read/write privileges by entering the following commands:

```
aurora:/etc ->touch /var/log/router.log
aurora:/etc ->ls -l /var/log/router.log
-rw-r--r--   1 root     other      27110 Jul  8 19:56 /var/log/router.log
aurora:/etc ->
```

Step 3 Verify the syslog daemon is running by entering the **ps -elf | grep syslog** command from the /etc directory. If the daemon is running, a process ID is returned by the system (for example, 169). If the daemon is not running, no ID is returned.

```
aurora:/etc ->ps -elf | grep syslog
 8 S     root   169     1  0  41 20 60756cc8    187 604e3156   Jun 19 ?        d
aurora:/etc ->
```

Step 4 Activate the configuration changes you made in syslog.conf by restarting the syslog daemon. Enter the start/stop S74syslog scripts from the /etc/rc2.d directory.

```
aurora:/etc ->rc2.d/S74syslog stop
Stopping the syslog service.
aurora:/etc ->rc2.d/S74syslog start
syslog service starting.
aurora:/etc ->ps -elf | grep syslog
 8 S     root  4405     1  0  44 20 6042d320    187 604e3156 09:16:35 ?        d
aurora:/etc ->
```

Confirm that a new syslog process ID was assigned (for example, 4405) after the start/stop process.

Note You must have root-level permissions to run system scripts, such as the files in /etc/rc2.d

Inspecting Syslog Messages in the Log File

To inspect syslog messages by using Cisco IOS commands, Unix commands, FTP, and a web browser, follow these steps:

Step 1 From the Cisco IOS device, create basic syslog messages by entering these commands:

```
travis-nas-01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
travis-nas-01(config)#^Z
travis-nas-01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
travis-nas-01(config)#^Z
travis-nas-01#
```

Step 2 From the syslog server, verify that the syslog messages went in to the log file. Enter the **tail -f** command to monitor the last 10 lines of an active log file. To exit tail -f mode, press **Ctrl-C**.

```
aurora:/etc ->tail -f /var/log/router.log
May 26 17:43:12 [172.21.101.20.6.122] 629: May 26 20:35:23.551 CST: %SYS-5-CONFIG_I:
Configured from console by vty0 (172.22.61.200)
May 26 17:51:15 [172.21.101.20.6.122] 630: May 26 20:43:27.068 CST: %SYS-5-CONFIG_I:
Configured from console by console
May 26 17:51:19 [172.21.101.20.6.122] 631: May 26 20:43:30.932 CST: %SYS-5-CONFIG_I:
Configured from console by console
May 26 17:54:38 [172.21.101.20.6.122] 632: May 26 20:46:50.344 CST: %SYS-5-CONFIG_I:
Configured from console by vty0 (172.22.61.200)
^C
aurora:/etc ->
```

Step 3 View the syslog messages in a web browser. Notice the wide horizontal scroll bar, which is helpful for viewing debug messages and modem call records.

Figure 18 Syslog Messages that Appear by Using FTP and a Web Browser

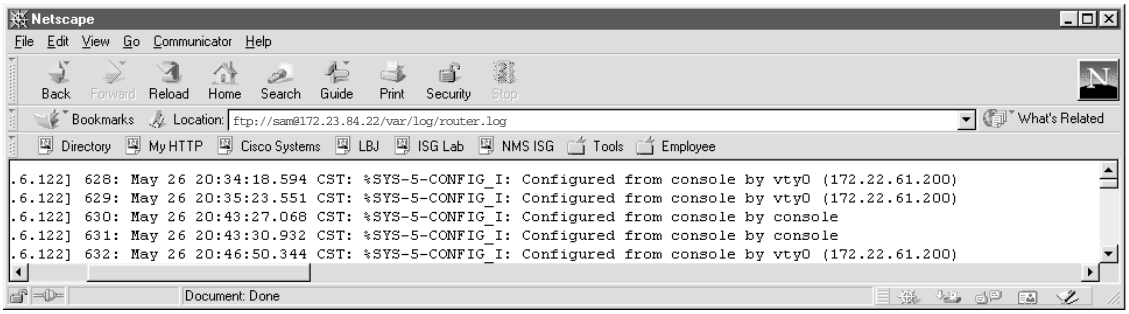


Table 21 shows the generic URL syntax to use. Be sure to replace the variables with your own information. The FTP server automatically prompts you for a login password.

Table 21 URL Syntax Descriptions and Examples

Generic URL Syntax	Description	Example
ftp://*username@host/directory-path*	Uses FTP to view logs from a remote location.	ftp://sam@172.23.84.22/var/log/router.log
file://*directory-path*	Views logs on a local host.	file://var/log/router.log