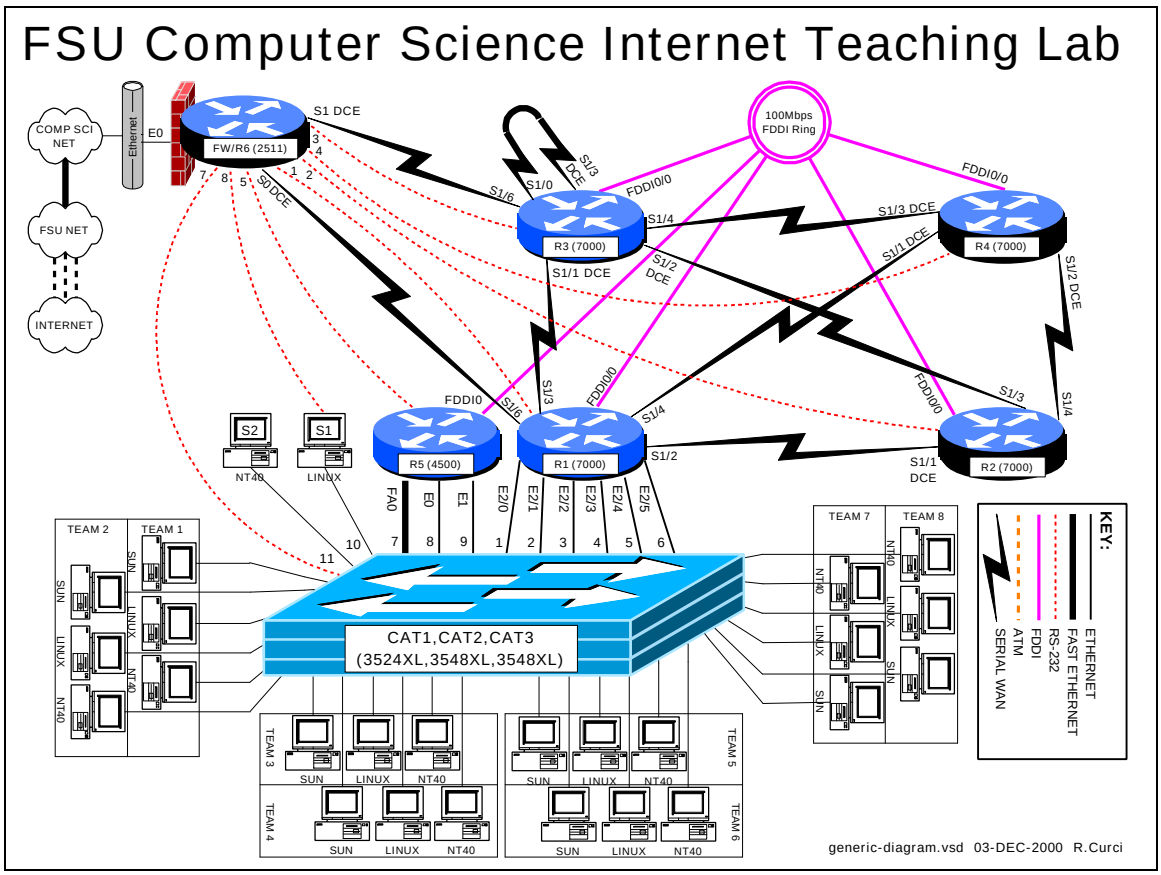
INTERNET TEACHING LAB: CISCO ROUTER DEBUGGING



OVERVIEW

Debug mode is a feature of the Cisco IOS software to locate router configuration errors and software bugs. Log messages are similar to debug messages and are generally alerts to problems. You can think of log messages as debug messages that cannot be turned off. Problems are diagnosed by reviewing descriptive messages generated by the router. There are hundreds of different debug options that can be individually turned on and off depending on what part of the system is under examination. It is possible to turn on all debug modes simultaneously, however, this is rarely appropriate as the volume of information would be too voluminous. Debug mode should generally not be used on a production network as it is easy to generate hundreds of error messages per second and cause a router to crash and reboot. We will also explore some of the "show" commands used for debugging problems. **This lab assignment assumes you have the base router configuration from the "Cisco Router Basics" loaded with the RIP routing protocol.** The following is a sample of some debug and log messages. I have removed the timestamps to fit the messages on the page.

```
(Sample of debug and log messages)
r1#term monitor
r1#debug all
This may severely impact network performance. Continue? [confirm]y
All possible debugging has been turned on

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/2, changed state to
down
%LINK-3-UPDOWN: Interface Serial1/2, changed state to up
%SYS-5-CONFIG_I: Configured from memory by console
%SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) GS Software (GS7-J-M), Version 11.1(24), RELEASE SOFTWARE (fc1)
%ENVM-2-SUPPLY: Upper Power Supply is Non-Operational
%LINK-4-FDDISTAT: Interface Fddi0/0, FDDI state c_wrap_b detected?
IP: s=192.168.16.6 (Serial1/6), d=224.0.0.10, len 64, dispose 31
SMT I: Fddi0/0, FC=SMT, DA=0000.309c.fb2d, SA=0000.309c.9e3f,
IP: s=192.168.16.6 (Serial1/6), d=255.255.255.255, len 176, rcvd 2
UDP: rcvd src=192.168.16.6(520), dst=255.255.255.255(520), length=152
RIP: received v1 update from 192.168.16.6 on Serial1/6
     0.0.0.0 in 5 hops
     192.168.13.0 in 16 hops (inaccessible)
     192.168.66.0 in 1 hops
Serial1/2: HDLC myseq 8, mineseen 8*, yourseen 11, line up
RIP: sending v1 update to 255.255.255.255 via Serial1/2 (192.168.12.1)
     default, metric 6
     network 192.168.66.0, metric 2
RIP: Update contains 21 routes
RIP: Update queued
RIP: Update sent via Serial1/2
CDP-PA: Packet received from cat1 on interface Ethernet2/0

r1#undebug all
```

PART 1 – SHOW COMMANDS:

Although not technically debug commands, there are several "show" commands that are helpful with debugging and worth mentioning. Read about the following "show" commands using either the hardcopy Cisco manuals or online manuals at www.cisco.com and try them out on your router. Include a brief description what each of these commands does for your assignment:

1. show version
2. show controller [cbus | serial]
3. show cdp neighbors [detail]
4. show interface
5. show ip interface [brief]
6. show ip protocol
7. show memory
8. show processes cpu
9. show diagbus (7000 only)
10. show tech-support

Using information gathered on your router using the above "show" commands, answer the following questions:

1. What IOS software is your router running? What is the filename of the IOS image? How much RAM? FLASH? What is the value of the configuration register? What model CPU does your router have?
2. For each of your router's serial WAN interfaces, what kind of cable is attached (DTE, DCE, or none)?
3. Which adjacent routers are sending CDP messages to your router? What IOS software version is running on the adjacent CDP routers?
4. What is the MAC address of your router's FDDI interface?
5. For each of your router's active interfaces, is IP Split-Horizon enabled?
6. For the RIP protocol running on your router, what are the values of the RIP protocol *update*, *invalid*, *holddown*, and *flush* timers?
7. How much TOTAL, USED, and FREE RAM is in your router?
8. What is the average CPU utilization for the last 5 minutes?
9. On your 7000 router, what card is physically located in slot 0? What is its hardware revision and serial number?

PART 2 – SET THE CLOCK:

Debug messages are often examined on multiple router devices to study the sequence of events. It is often very useful to configure the debug messages to include a timestamp in order to correlate events in different log files. Setting the router clock is important to make the correlation possible. The current system clock can be displayed with the "show clock" command and set with the "clock set" command. Like UNIX, the Cisco router internally maintains the time as a long integer indicating the number of seconds that have elapsed since January 1st, 1970 GMT (Greenwich Mean Time). Sometimes GMT is called UTC (Universal Time Coordinated). By setting the appropriate time zone, number of hours offset from UTC, and daylight savings time information, the router can display the correct local time. Configure your router's time zone and daylight savings time information. Configure so that your router will display the local time appropriately and adjust automatically between standard time and daylight savings time. Manually set your router's clock.

PART 3 – NETWORK TIME PROTOCOL:

In the previous section, we saw how to manually set the router clock and timezone information. Sometimes it is helpful to automatically keep the clocks in sync or synchronize them more accurately than can be done manually. Cisco routers include software that implements the NTP (Network Time Protocol) version 3. NTP can typically maintain the clock accuracy within a few milliseconds. NTP devices maintain relationships with other NTP devices such as "master", "client", and "peer". Each NTP device has a stratum number which indicates the clock's accuracy and believability. We

will configure routers R1, R2, R3, R4, and R5 as NTP clients of router R6, a stratum 4 NTP server. Configure your router to be an NTP client of NTP server R6. Verify that your clock is synchronized using the "show ntp status", "show ntp associations", and "show ntp associations detail" commands. A full discussion of NTP is beyond the scope of this document, however, additional information can be found at http://www.eecis.udel.edu/~ntp/.

PART 4 – TIMESTAMPS:

Timestamps can be prepended to debug or log messages. A timestamp can be either an indication of the uptime (how much time has elapsed since the router was booted) or the current date and time. The date and time can be in UTC or the local timezone. Optionally, the timezone and/or the number of milliseconds can be included. Configure your router so that timestamps for both DEBUG and LOG messages will display the local time including the timezone and millisecond information. Verify that it is working.

PART 5 -- OUTPUT OPTIONS:

Debug and log messages generated have three different modes of output: (1) console screen, (2) internal circular buffer, or (3) syslog server.

1. Console Screen
   Using the console screen is probably the simplest way to view messages as they are generated. The command "term monitor" enables the display of messages while "term no monitor" inhibits the messages.

2. Internal Circular Buffer
   Part of a router's RAM memory can be allocated to be a circular logging buffer using the configuration command "logging buffer XXXX" where XXXX indicates the size of the buffer. The contents of the buffer can be displayed with the "show logging" command.

3. Syslog Server
   A syslog server is a TCP/IP service that accepts log messages and appends them to log files. Both UNIX and NT server systems can be configured as syslog servers. Syslog servers can be used to centralize the collection of messages from many systems to ease system administration. Syslog uses the concepts of facility and severity level. Facility classifies the messages by subsystem to allow the server to append the proper log file. The severity level provides an indication of the importance of an error message where the system manager can set a severity level threshold on both the router and syslog server. On the router, messages with lower priority than the threshold are never sent to the syslog server. A threshold set on the syslog server indicates the minimal importance necessary for a message

to be logged to a file which is otherwise discarded. By default, Cisco routers use the syslog facility "local7" and severity "informational", but these parameters are adjustable. Severity "informational" will send more messages except those with severity "debug". In this part, we will use severity level "debug" so that all messages are important enough to be forwarded from the router to the syslog server and all will be logged by the syslog server.

Configure your router so that debug messages will be logged to three different locations (1) to the console screen, (2) to the internal circular buffer, and (3) to your Linux system using facility "local7" and "severity debug". Your Linux server should append the messages to file /var/log/cisco.log. We will work on generating messages in the next part.

PART 5 – DEBUG MODE:

The command "debug" is used to enable the various debug modes. You can see the options with "debug ?". Each debug mode can be individually enabled or disabled using "debug xxxxx" to turn on a mode or "no debug xxxxx" to turn one off. The command "show debug" displays which debug modes are currently enabled. You can use the command "debug all" to turn on all debug modes, but it is generally not useful as it can generate hundreds of messages per second. You can turn off all debug modes with the command "no debug all" or "undebug all". Turn on icmp debugging "debug ip icmp" and ping one of your router's interfaces. Turn off debugging. Review the messages on your console screen, in your circular buffer, and on your syslog server's /var/log/cisco.log file. Are the entries identical? If not, explain what is different