ISP and NSP Security Workshop

APRICOT 2013

Day 1

Core Security

PCH Packet Clearing House

Alcatel·Lucent

SUBISU

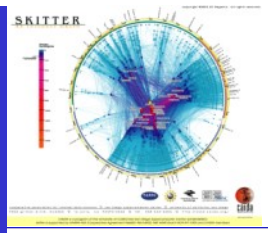
Security Workshop

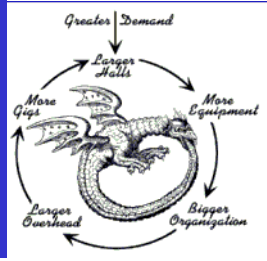
Lab Overview

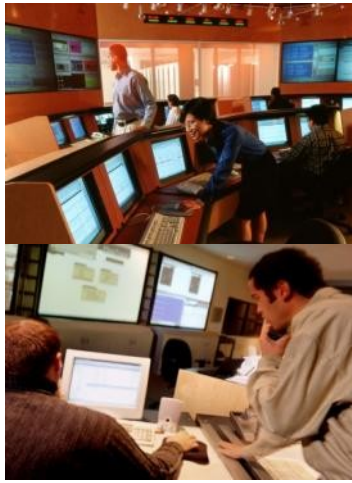
Lab OS Overview

- For this workshop we will be using Cisco IOS based platforms
- Each group of four participants will have four routers to share
- Introduction to the platform and how IOS works
- This module will contain general router configuration advice as well as IOS-specific configuration elements

Cisco IOS Configuration







Router Components

- **Bootstrap** – stored in ROM microcode – brings router up during initialisation, boots router and loads the IOS.
- **POST** – Power On Self Test - stored in ROM microcode – checks for basic functionality of router hardware and determines which interfaces are present
- **ROM Monitor** – stored in ROM microcode – used for manufacturing, testing and troubleshooting
- **Mini-IOS** – a.k.a RXBOOT/boot loader by Cisco – small IOS ROM used to bring up an interface and load a Cisco IOS into flash memory from a TFTP server; can also do a few other maintenance operations

Router Components

- **RAM** – holds packet buffers, ARP cache, routing table, software and data structure that allows the router to function; running-config is stored in RAM, as well as the decompressed IOS in later router models
- **ROM** – starts and maintains the router
- **Flash memory** – holds the IOS; is not erased when the router is reloaded; is an EEPROM [Electrically Erasable Programmable Read-Only Memory] created by Intel, that can be erased and reprogrammed repeatedly through an application of higher than normal electric voltage
- **NVRAM** – Non-Volatile RAM - holds router configuration; is not erased when router is reloaded

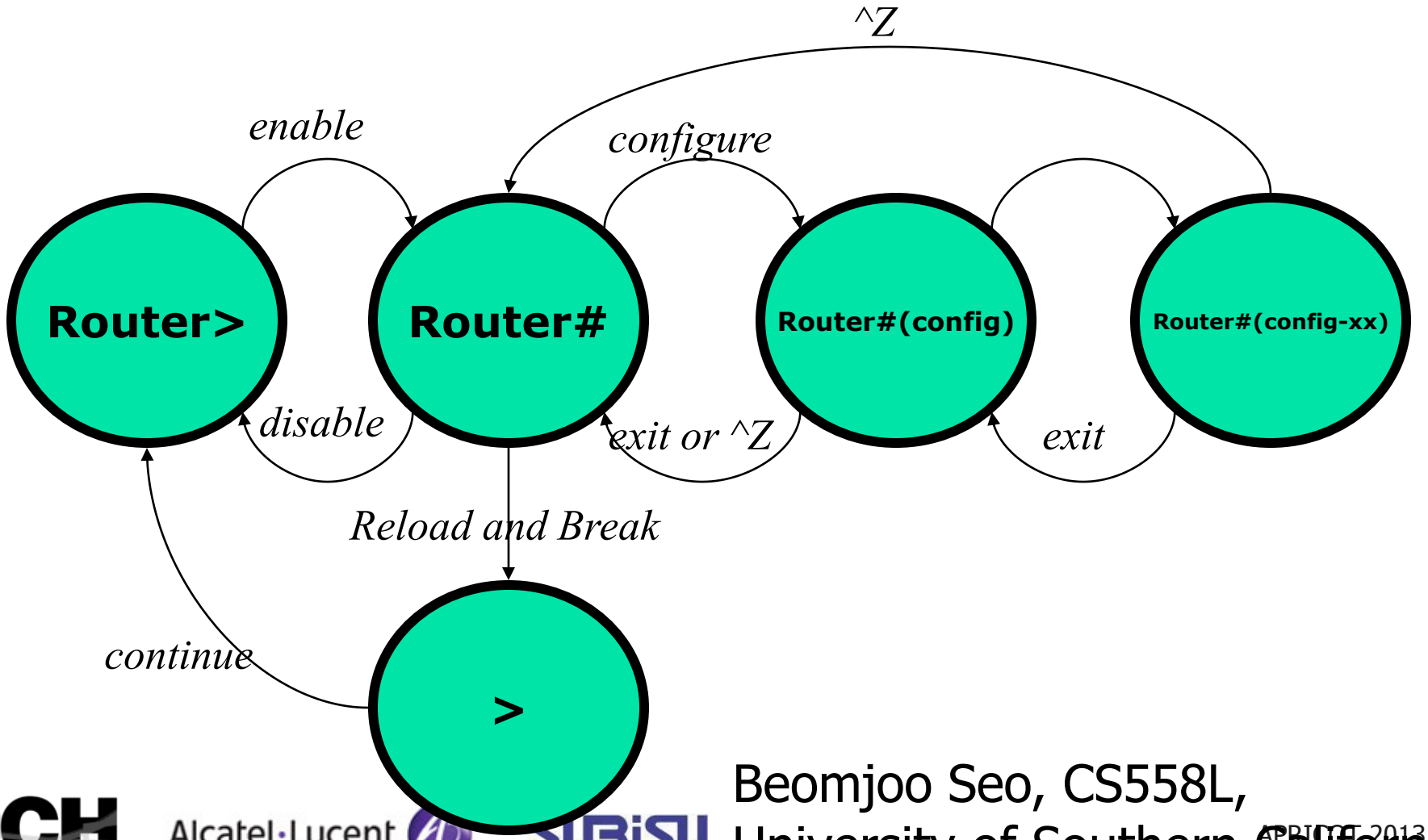
Router Components

- **Config-Register** – controls how router boots; value can be seen with "show version" command; is typically 0x2102, which tells the router to load the IOS from flash memory and the startup-config file from NVRAM

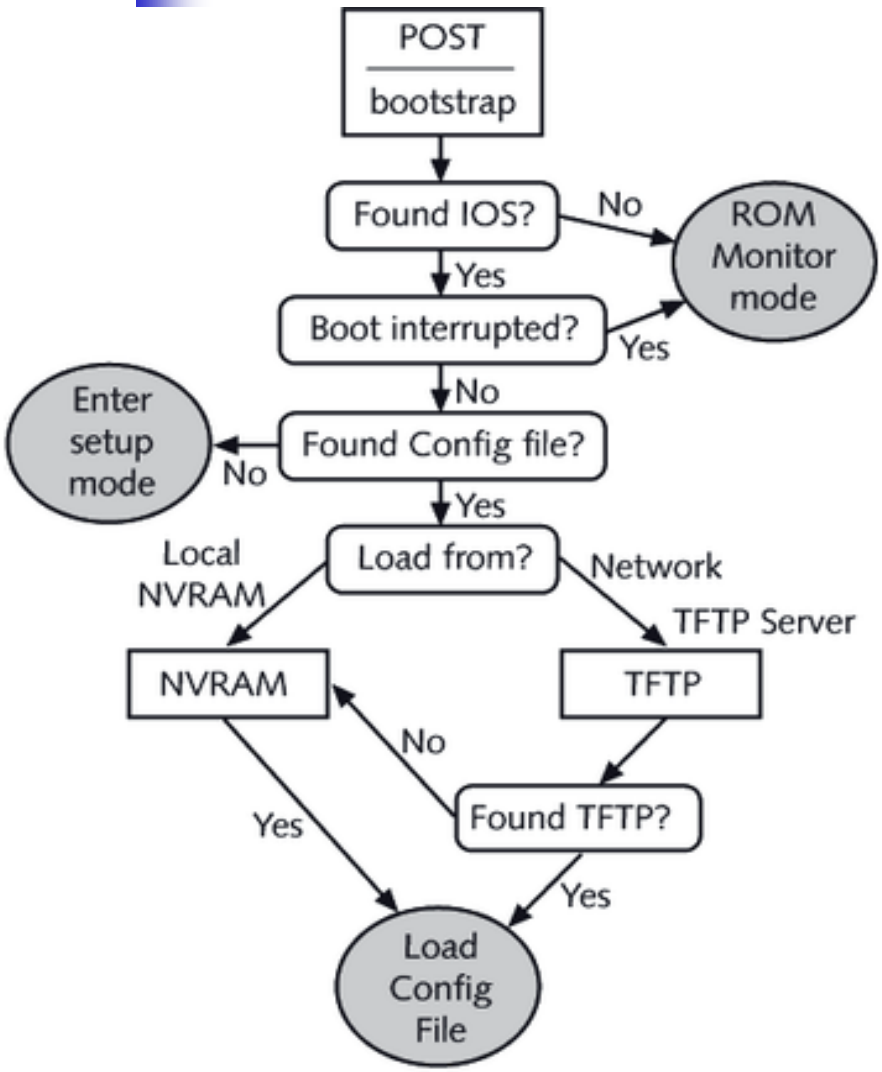
Router Modes Changed With Config-Register

- Reasons why you would want to modify the config-register:
  - Force the router into ROM Monitor Mode
  - Select a boot source and default boot filename
  - Enable/Disable the Break function
  - Control broadcast addresses
  - Set console terminal baud rate
  - Load operating software from ROM
  - Enable booting from a TFTP server

Router Modes Change and Prompts



Router Setup and Startup



POST – loaded from ROM and runs diagnostics on hardware

Bootstrap – locates and loads the IOS image; default is flash

IOS – locates and loads a valid configuration from NVRAM; from startup-config and only exists if you copy running-config to NVRAM

Startup-config – if found, router loads it and runs embedded configuration; if not found, router enters setup mode

Where is the Cisco IOS Configuration?

Command from Enable Mode	Description
copy running-config tftp	Copies the running configuration located in RAM to a TFTP server.
copy startup-config tftp	Copies the startup configuration located in NVRAM to a TFTP server.
copy tftp running-config	Copies the configuration from the TFTP server to the running configuration. The reconfiguration of the router is immediate when this command is issued. The running-config is not replaced. The files are blended.
copy tftp startup-config	Copies the configuration from the TFTP server to the startup configuration. The startup-config is replaced with the one from the TFTP server.
copy run start	Copies the working configuration file in RAM to the startup configuration file in NVRAM. Replaces the startup configuration file.
copy start run	Copies the startup configuration file in NVRAM to the running configuration in RAM. Does not replace the file in RAM; the files are blended.
copy flash tftp	Copies the IOS in flash memory to a TFTP server.
copy tftp flash	Copies the IOS from a TFTP server to flash memory.
configure terminal	Used to specify that you would like to configure your settings manually from the console terminal.
configure memory	Used to specify that you would like to pull your configuration information from NVRAM.

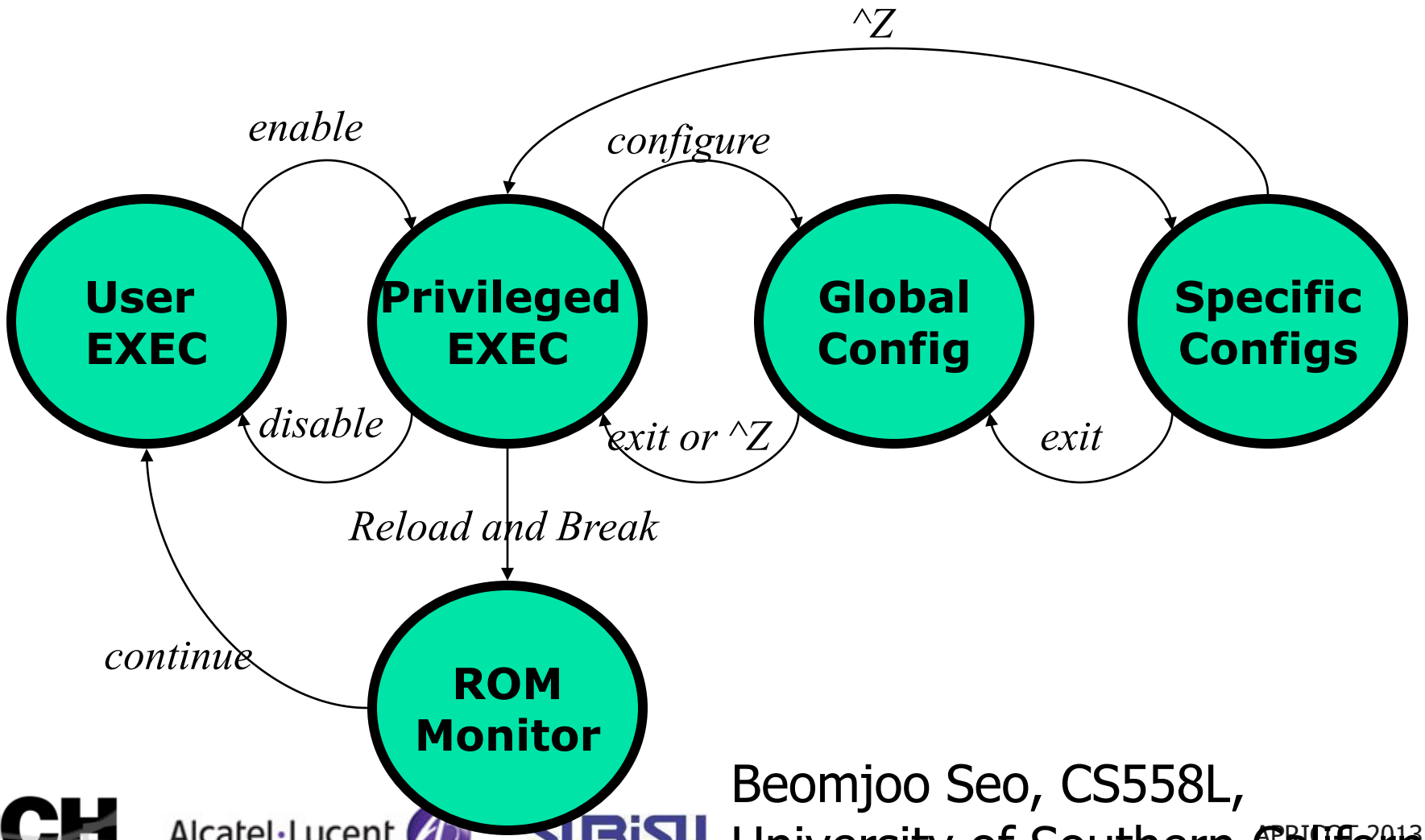
Router Access Modes

- User EXEC mode - limited examination of router
  - Router>
- Privileged EXEC mode - detailed examination of router, debugging, testing, file manipulation
  - Router#
- ROM Monitor - useful for password recovery & new IOS upload session
- Setup Mode – available when router has no startup-config file

Router Access Modes

Mode	Prompt	To enter	To exit	Used for
User EXEC	Router>	If there is a line password, enter it. Otherwise, press the Return or Enter key.	Logout or Exit	Shows the status of the router and allows network operators to manage connections
Privileged EXEC	Router#	Type enable at the prompt.	Disable Exit Logout	Copies, erases, sets up, and shows router settings
Global configuration	Router (config)#	Configure	Exit End	Allows you to configure various items, including clock, hostname, enable password, and enable secret password
Interface configuration	Router (config-if)#	Interface Ethernet0 *or* Interface Serial0	Exit End	Allows you to configure the settings, such as IP, for a specific interface
Line configuration	Router (config-line)#	Line console 0 *or* Line vty 0 4 *or* Line aux 0	Exit End	Configures lines, such as the console, virtual terminal, or auxiliary
Router configuration	Router (config-router)#	Router rip *or* Router igrp	Exit End	Adds or configures RIP, IGRP, or other routing protocols

CLI Modes for Router Access



External Configuration Sources

- Console – direct PC serial access
- Auxilliary port – Modem access
- Virtual terminals – Telnet access
- TFTP Server – copy configuration file into router RAM
- Network Management Software - CiscoWorks

Telnet

- Utility that connects at the highest layer of the OSI model
- Provides remote access to other devices
- Cisco routers allow telnet connections via their virtual terminal ports
- If you can establish telnet connectivity to a router, you have established that it is available on the network and that you have connectivity at all layers

SSH

- Replaces telnet for a protected command and control communication channel
- Privacy and integrity provided through the use of strong cryptographic algorithms
- Supports TACACS+, RADIUS and local authentication
- Secure Copy (SCP) available in new SSH enabled code
- Restrict access to ssh via "transport input ssh" command
- SSHv2 now in Cisco IOS!

IP Host Names

- When telnetting to a remote router or host, the IP address of the host must follow the telnet command
- Rather than using IP addresses, it is easier to refer to a remote host or router using a name
- Sometimes, you cannot gain connectivity because the host name that you are trying to connect with is entered in a table incorrectly
- Using a name server provides name resolution from one location, making a table configuration on each device unnecessary

Ping and Trace

- If you can't get connectivity at the Application layer, try connectivity at the Internetwork layer
- Ping and trace verify connectivity at the Internetwork layer
  - Both use ICMP messages to verify the destination host is reachable, and if not, give possible reasons for the problem
- Ping sends a packet to the destination and waits for a response
  - By default, the ping utility with Cisco routers is configured to send five packets to the target

Ping and Trace

- Extended mode ping
  - Options include:
    - The destination address of the ping
    - The protocol
    - Repeat count
    - Datagram size
  - Can only be accessed from the privileged mode prompt

Ping and Trace

- If ping indicates a problem with connectivity, using trace may provide a better clue as to the source of the connectivity problem
- Trace command is similar to ping command, except that the replies are requested at each hop along the way to the destination
- Trace sends multiple ICMP packets with progressively higher TTL counters until the packet reaches the destination

IP Route

- If you cannot get connectivity using ping or trace, you should check your routing table
- You can issue the show ip route command from the enable mode prompt
  - This command shows the routing table
- Typically, routing tables are dynamically created when routing protocols are configured on the router

Checking the Interface

- On of the biggest mistakes made when troubleshooting is not checking the interfaces on the router
- If the interfaces are down, packets cannot be delivered
- Router interfaces go down for a variety of reasons including:
  - Incorrect IP configuration
  - Cable problems

Checking the Interface

- Keepalive frames
  - Data frames sent between two hosts to ensure that the connection between those hosts remains open
- Different types of interfaces can show different types of reports
  - For example, a Token Ring interface reports down when there is no electrical carrier signal present

Checking the Interface

```
lab-a#show interfaces
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 0000.0c8e.b490 (bia 0000.0c8e.b490)
  Internet address is 192.5.5.1/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
Serial0 is down, line protocol is down
  Hardware is HD64570
  Internet address is 201.100.11.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 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
     15 packets output, 3198 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=down  RTS=down  CTS=up
Serial1 is administratively down, line protocol is down
  Hardware is HD64570
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
```

Interface E0 is fully functional. Frames can be sent and received on this interface.

S0 is not functional. In this case, the serial interface on the router attached to this router is down. If one end of a point-to-point link is down, it will "push" the attached up interface on the next router down.

The S1 interface is not functional. In this case, there is no cable attached to S1 as it is not being used.

Clear Counters

- Routers keep detailed statistics regarding the data passing across its interfaces
- Before using the show interface command, you may want to clear the existing interface information
- You can clear these statistics (**counters**) on the interface by using the clear interface or clear counters command

Debug

- Debug command
  - One of the most powerful tools you can use to obtain information from your router
  - Only available from privileged EXEC mode
  - Has numerous subcommands that allow you to troubleshoot particular protocols
  - Allows you to check for specific types of traffic on the wire

Debug

```
RouterB#debug all
This may severely impact network performance. Continue? [confirm]

All possible debugging has been turned on
RouterB#
IP: s=172.22.3.1 (Serial1), d=255.255.255.255, len 76, rcvd 2
UDP: rcvd src=172.22.3.1(520), dst=255.255.255.255(520), length=52
RIP: received v1 update from 172.22.3.1 on Serial1
     172.22.4.0 in 1 hops
     172.22.5.0 in 2 hops
RIP: Update contains 2 routes
SERVICE_MODULE(0): lxt441 interrupt 1 status A7 loop 0
SERVICE_MODULE(0): lxt441 interrupt 1 status 87 loop 0
SERVICE_MODULE(0): lxt441 interrupt 1 status A7 loop 0
SERVICE_MODULE(0): lxt441 interrupt 1 status 87 loop 0
Serial1: HDLC myseq 6631, mineseen 6631, yourseen 6580, line up
SERVICE_MODULE(0): lxt441 interrupt 1 status A7 loop 0
SERVICE_MODULE(0): lxt441 interrupt 1 status 87 loop 0
SERVICE_MODULE(0): lxt441 interrupt 1 status A7 loop 0
SERVICE_MODULE(0): lxt441 interrupt 1 status 87 loop 0
RIP: sending v1 update to 255.255.255.255 via Ethernet0 (172.22.2.1)
     subnet  172.22.3.0, metric 1
     subnet  172.22.4.0, metric 2
     subnet  172.22.5.0, metric 3
RIP: Update contains 3 routes
IP: s=172.22.2.1 (local), d=255.255.255.255 (Ethernet0), len 55, sending broad/m
ulticast
RIP: sending v1 update to 255.255.255.255 via Serial1 (172.22.3.2)
     subnet  172.22.2.0, metric 1
RIP: Update contains 1 routes
IP: s=172.22.3.2 (local), d=255.255.255.255 (Serial1), len 67, sending broad/mul
ticast
SERVICE_MODULE(0): lxt441 interrupt 1 status A7 loop 0
SERVICE_MODULE(0): lxt441 interrupt 1 status 87 loop 0
Serial0: attempting to restart
Serial1: HDLC myseq 6632, mineseen 6632, yourseen 6581, line up
IP: s=172.22.5.1 (Ethernet0), d=255.255.255.255, len 106, rcvd 2
UDP: rcvd src=172.22.5.1(520), dst=255.255.255.255(520), length=72
RIP: ignored v1 update from bad source 172.22.5.1 on Ethernet0
SERVICE_MODULE(0): lxt441 interrupt 1 status A7 loop 0
SERVICE_MODULE(0): lxt441 interrupt 1 status 87 loop 0
SERVICE_MODULE(0): lxt441 interrupt 1 status A7 loop 0
SERVICE_MODULE(0): lxt441 interrupt 1 status 87 loop 0
SERVICE_MODULE(0): lxt441 interrupt 1 status A7 loop 0
SERVICE_MODULE(0): lxt441 interrupt 1 status 87 loop 0
Serial1: HDLC myseq 6633, mineseen 6633, yourseen 6582, line up
All possible debugging has been turned off
RouterB#
```

The debug all command warns you that issuing this command could cause severe network congestion. This command should only be used for a short period of time as a troubleshooting tool.

Lab

- Follow the lab-guide to set up initial topology
- Follow the lab-guide to secure remote access

Lab Guide – Day 1