

The Cisco Router as a Hidden Troubleshooting Tool

Ryan Determan
CCIE #5276



Agenda

- Introduction
- Presentation: The Cisco Router as a Hidden Troubleshooting Tool
- Question & Answer



Outline

The Cisco Router as a Hidden Troubleshooting Tool:

- I. Individual tools and their secrets
- II. Internal router processes
- III. Using the appropriate command
- IV. What am I looking at?
- V. When the router is the problem



(I) Individual Tools and Their Secrets

1. ICMP Ping and its options
2. Cisco Telnet and its options
3. Debugging Properly
4. NBAR
5. Test command
6. Csim start command
7. SAA / RTR responders



ICMP Ping and its options

Standard Cisco ping:

```
core_router#ping 10.123.123.7
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.123.123.7, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms



ICMP Ping and its options

Extended Cisco ping:

```
core_router#ping
```

```
Protocol [ip]:
```

```
Target IP address: 10.123.123.7
```

```
Repeat count [5]:
```

```
Datagram size [100]:
```

```
Timeout in seconds [2]:
```

```
Extended commands [n]: y
```

```
Source address or interface:
```

```
Set DF bit in IP header? [no]:
```

```
Loose, Strict, Record, Timestamp, Verbose[none]:
```

```
Sending 5, 100-byte ICMP Echos to 10.123.123.7, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```



ICMP Ping and its options

Record option:

core_router#ping

Protocol [ip]:

Target IP address: 131.108.1.115

Output Omitted...

Extended commands [n]: **y**

Output Omitted...

Loose, Strict, Record, Timestamp, Verbose[none]: **r**

Number of hops [9]:



ICMP Ping and its options

Record Option (cont):

Sending 5, 100-byte ICMP Echos to 131.108.1.115, timeout is 2 seconds:

Packet has IP options: Total option bytes= 39, padded length=40

Record route: <*>

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)



ICMP Ping and its options

Record Option (cont):

The following display is a detail of the Echo packet section:

0 in 4 ms. Received packet has options

Total option bytes= 40, padded length=40

Record route: 160.89.80.31 131.108.6.10 131.108.1.7 131.108.1.115

131.108.1.115 131.108.6.7 160.89.80.240 160.89.80.31 <*> 0.0.0.0

End of list

1 in 6 ms. Received packet has options

Output Omitted...

NOTE- IP Source Routing has to be enabled on all routers in the path for the record option to work



ICMP Ping and its options

Source Interface Option:

```
core_router#ping
```

```
Protocol [ip]:
```

```
Target IP address: 10.123.123.7
```

```
Output Omitted...
```

```
Extended commands [n]: y
```

```
Source address or interface: loopback0 (or an actual local IP address)
```

```
Output Omitted...
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.123.123.7, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```



ICMP Ping and its options

MTU testing:

core_router#ping

Target IP address: 10.123.123.7

Output Omitted...

Extended commands [n]: **y**

Set DF bit in IP header? [no]: **y**

Output Omitted...

Sweep range of sizes [n]: **y**

Sweep min size [36]: **64**

Sweep max size [18024]: **1550**

Sweep interval [1]: **10**

Type escape sequence to abort.

Sending 745, [64..1550]-byte ICMP Echos to 10.123.123.7, timeout is 2 seconds:

!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!.....

Success rate is 96 percent (96/100), round-trip min/avg/max = 1/3/4 ms

MTU math= (success*interval)+min sweep value

$$(96*10)+64=1024$$



Telnet and its Options

Standard Cisco Telnet:

```
core_router#telnet 10.123.123.254
```

OR:

```
core_router#10.123.123.254
```



Telnet and its Options

Cisco Telnet Options:

core_router#telnet 10.123.123.254 ?

/debug	Enable telnet debugging mode
/ipv4	Force use of IP version 4
/ipv6	Force use of IP version 6
/line	Enable telnet line mode
/noecho	Disable local echo
/quiet	Suppress login/logout messages
/route:	Enable telnet source route mode
/source-interface	Specify source interface
/stream	Enable stream processing
/terminal-type	Set terminal type
<0-65535>	Port number



Telnet and its Options

Source Interface option:

```
core_router#telnet 10.123.123.254 /source-interface ethernet 0/0
```

Debug option:

```
core_router#telnet 10.123.123.254 /debug
```

Multiple options:

```
core_router#telnet 10.123.123.254 /source-interface ethernet 0/0 /debug
```



Using Debug Appropriately

- System messages generated by the router (ICMP, SNMP, telnet, logging, debugging) are CPU intensive.
- The system messages that are generated do not really get 'routed', they get created.
- I.E. Using debug incorrectly can lead to network latency and/or failure!



Using Debug Appropriately

Debug Usage Guidelines:

- Ensure you understand what you are looking for
- Enable debug timestamps to simplify timeframe
`core_router(config)#service timestamps debug datetime localtime`
- Never use debug from the console/aux, always telnet
`core_router#term mon`
- Use a filter whenever possible
 - Access-list debug filtering
 - Interface debug filtering



Access-list Debug Filtering

```
core_router#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
core_router(config)#access-list 10 permit 10.123.123.7
```

```
core_router(config)#^Z
```

```
core_router#debug ip packet detail ?
```

```
<1-199>   Access list
```

```
<1300-2699> Access list (expanded range)
```

```
<cr>
```

```
core_router#debug ip packet detail 10
```

IP packet debugging is on (detailed) for access list 10

```
core_router#ping 10.123.123.7
```

```
03:16:57: IP: s=10.123.123.7 (Ethernet0/0), d=10.123.123.254 (Ethernet0/0), len 100, rcvd 3
```

```
03:16:57:   ICMP type=0, code=0
```



Interface Debug Filtering

```
core_router#debug list ?
<0-2699>      access list
Dialer        Dialer interface
Ethernet      IEEE 802.3
Multilink     Multilink-group interface
Output Omitted...
<cr>
core_router#debug list ethernet 0/0
core_router#debug ip packet detail
IP packet debugging is on
      for interface: Ethernet0/0
(detailed)

03:19:32: IP: s=10.123.123.7 (Ethernet0/0), d=10.123.123.254 (Ethernet0/0), len 100, rcvd 3
03:19:32:  ICMP type=0, code=0
```



Combination Debug Filtering

```
core_router#debug list ethernet 0/0 ?
```

```
<0-2699> access list
```

```
<cr>
```

```
core_router#debug list ethernet 0/0 10
```

```
core_router#debug ip packet detail
```

```
IP packet debugging is on
```

```
for interface: Ethernet0/0 and access list: 10
```

```
(detailed)
```

```
03:21:38: IP: s=10.123.123.7 (Ethernet0/0), d=10.123.123.254 (Ethernet0/0), len 100, rcvd 3
```

```
03:21:38: ICMP type=0, code=0
```



NBAR

- NBAR - Network Based Application Recognition
- Full functionality in IOS 12.1.5(T) and greater
- Can use to evaluate, detect, and protect
- Basic NBAR supported on most models (incl 2500, 1600, etc)
- Full NBAR support for newer routers (1700, 2600, 36xx)



Enabling NBAR

- Cisco Express Forwarding must be enabled

```
core_router#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
core_router(config)#ip cef
```

```
core_router(config)#int e 0/0
```

```
core_router(config-if)#ip nbar protocol-discovery
```

```
core_router(config-if)#^Z
```

```
core_router#sh ip nbar protocol-discovery
```



NBAR for Evaluation

```
core_router#sh ip nbar protocol-discovery
Ethernet0/0      Input          Output
Protocol        Packet Count   Packet Count
                Byte Count    Byte Count
                5 minute bit rate (bps) 5 minute bit rate (bps)
-----
http            2892          3487
                427198       2930628
                0            0
secure-http    2462          2064
                854207       706349
                0            0
```



NBAR for Detection

```
core_router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
core_router(config)#class-map nbar-detect
core_router(config-cmap)#match prot napster (NBAR used for detection)
core_router(config)#policy-map napster-detect
core_router(config-pmap)#class nbar-detect
core_router(config)#int e 2/0
core_router(config-if)#service-policy input napster-detect
core_router(config-if)#service-policy output napster-detect
core_router(config-if)#^Z
core_router#sh policy-map interface ethernet 2/0
```



NBAR for Protection

```
core_router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
core_router(config)#class-map nbar-detect
core_router(config-cmap)#match prot napster (NBAR used for detection)
core_router(config)#policy-map napster-detect
core_router(config-pmap)#class nbar-detect
core_router(config-pmap)#set ip dscp 1
core_router(config)#access-list 101 deny ip any any dscp 1 log
core_router(config)#access-list 101 permit ip any any
core_router(config-if)#ip access-group 101 in
core_router(config-if)#ip access-group 101 out
core_router(config-if)#^Z
core_router#sh access-list 101
```



NBAR for Code Red

```
core_router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
core_router(config)#class-map nbar-detect
core_router(config-cmap)#match prot http url "*cmd.exe"
core_router(config-cmap)#match prot http url "*root.exe"
core_router(config-cmap)#match prot http url "*readme.eml"
core_router(config-cmap)#match prot http url "*.ida*"
core_router(config)#access-list 101 deny ip any any dscp 1 log
core_router(config)#access-list 101 permit ip any any
core_router(config-if)#ip access-group 101 in
core_router(config-if)#ip access-group 101 out
core_router(config-if)#^Z
core_router#sh access-list 101
```



Test Command

- Various different 'test' commands

core_router#test ?

aaa	AAA Authentication, Authorization and Accounting
interfaces	Network interfaces
memory	Non-volatile and/or multibus memory
pas	Port Adaptor Tests
sGBP	
cac	test the I2 cac functionality
call	Call test commands
crypto	Test crypto functions

Output Omitted...



Documented Test Command

- test crypto isakmp 63.227.15.229
63.81.254.121 esp-des
- test memory
- test voice port 1/0/0 relay ring on



U/MDocumented Test Command

- test dhcp [allocate xxx.xxx.xxx.xxx] | [release] | [renew]
- test crash [value] or <cr> to enter crash menu
- test dsp memory



CSIM Start Command

- CSIM start command was introduced in 12.0(x) code for testing voice calls / peers
- Very handy command if you aren't next to the actual phone

```
core_router#csim start 3037412284
```

```
csim: called number = 3037412284, loop count = 1 ping count = 0
```

```
csim err:csim_do_test Error peer not found
```



SAA / RTR responders

- Feature implemented in early IOS versions, <10.3
- Originally designed for SNA networks
- New capabilities allow for intricate TCP/UDP/IP testing
- Recent additions for Voice tests (latency, jitter, etc)



SAA / RTR Options

core_router(config)#rtr ?

<1-2147483647>

Entry Number

key-chain

Use MD5 authentication for RTR control message

low-memory

Configure low water memory mark

reaction-configuration

RTR Reaction Configuration

reaction-trigger

RTR Trigger Assignment

reset

RTR Reset

responder

Enable RTR Responder

restart

Restart an Active Entry

schedule

RTR Entry Scheduling



SAA / RTR Types

```
core_router(config)#rtr 1
core_router(config-rtr)#type ?
dhcp      Perform DHCP Operation
dlsw      Perform DLSw Keepalive Operation
dns       Perform DNS Query
echo      Perform Point to Point Echo Operations
frame-relay Perform frame relay operation
ftp       Perform ftp operation
http      Perform HTTP Operations
jitter    Perform Jitter Operation
pathEcho  Perform Path Discovered Echo Operations
pathJitter Perform Path Jitter Operation using ICMP
tcpConnect Perform TCP Connect Operations
udpEcho   Perform UDP Echo Operations
```



DNS SAA for www.ccti.com

```
core_router#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
core_router(config)#rtr 1
```

```
core_router(config)#type dns target-addr www.ccti.com name-server 10.123.123.7
```

```
core_router(config)#
```

```
core_router(config)#rtr schedule 1 ?
```

ageout How long to keep this Entry when inactive

life Length of time to execute in seconds

start-time When to start this entry

```
<cr>
```

```
core_router(config)#rtr schedule 1 start-time now
```



SAA / RTR States

```
core_router#sh rtr operational-state
Entry Number: 1
Modification Time: 13:49:27.000 mdt Wed Apr 4 2003
Diagnostics Text:
Last Time this Entry was Reset: Never
Connection Loss Occurred: FALSE
Timeout Occurred: FALSE
Over Thresholds Occurred: FALSE
Number of Operations Attempted: 1
Current Seconds Left in Life: 3565
Operational State of Entry: active
Latest Completion Time (milliseconds): 4
Latest Operation Start Time: 13:49:27.000 mdt Wed Apr 4 2003
Latest Operation Return Code: ok
Latest www.ccti.com
```



(II) Router Processes

- Switching Types
- IP CEF
- Examining the CPU
- Deciphering show version



Switching Types

- Process Switching (routing)
- Fast Switching (limited cache routing)
- Cisco Express Forwarding (expanded cache routing)



Process Switching

- Uses CPU to examine every packet of every data flow
- Matches destination IP address against routing table for each individual packet
- CPU intensive, but accurate
- Achieves 'true' load balancing



Fast Switching

- Uses CPU to examine first packet of every data flow
- Takes lookup information and populates an inbound cache for the interface
- Cache is made up of 3 fields:
 - Destination IP address
 - Local interface to use when forwarding
 - MAC header to place on the new frame



Fast Switching cont.

- Fast switching is less CPU intensive than Process switching
- Route lookup time is decreased due to proximity of cache
- Due to cache limitations, Fast switching will never use 2 paths to the same destination
- Result is 'destination load' balancing



Cisco Express Forwarding

- Similar to Fast switching
- Better usage of cache, more fields
- Performs recursive lookup immediately
- Cache allows for load balancing and includes QoS fields



Cisco Express Forwarding

```
core_router(config)#ip cef ?
  accounting      Enable CEF accounting
  load-sharing     Load sharing
  table           Set CEF forwarding table characteristics
  traffic-statistics Enable collection of traffic statistics
  <cr>
core_router(config)#ip cef load-sharing per-packet
core_router(config)#ip cef load-sharing per-destination
core_router(config)#ip cef distributed (note - assumes you have VIP cards
(7500,12000)
core_router(config)#ip cef
core_router(config)#int e 2/0
core_router(config-if)#no ip route-cache cef
```



Examining the CPU

- Show processes memory
- Show processes CPU
- Show processes CPU options



Examining Memory Usage

```
core_router#sh processes memory
```

```
Total: 13831296, Used: 11168180, Free: 2663116
```

PID	TTY	Allocated	Freed	Holding	Getbufs	Retbufs	Process
0	0	118804	1848	7345896	0	0	Init*
0	0	824	268852	824	0	0	*Sched*
0	0	16262020	5440428	81772	170844	0	*Dead*
1	0	284	284	3828	0	0	Load Meter
2	0	96	0	6924	0	0	CRYPTO IKMP IPC



Examining CPU Usage

```
core_router#sh processes cpu
```

```
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
```

PID	Runtime(ms)	Invoked	uSecs	5Sec	1Min	5Min	TTY	Process
1	0	3650	0	0.00%	0.00%	0.00%	0	Load Meter
2	4	8	500	0.00%	0.00%	0.00%	0	CRYPTO IKMP IPC
3	0	7	0	0.00%	0.00%	0.00%	0	fax timers
4	0	2	0	0.00%	0.00%	0.00%	0	IpSecMibTopN
5	13436	2166	6203	0.16%	0.10%	0.06%	0	Check heaps



Examining the CPU History (60s)

```
core_router#sh processes cpu history
```

```
11111
```

100

90

80

70

60

50

40

30

20

10

```
0...5...1...1...2...2...3...3...4...4...5...5...
```

```
0 5 0 5 0 5 0 5 0 5
```

CPU% per second (last 60 seconds)



Deciphering Show Version

IOS (tm) 3600 Software (**C3640-IK9O3S-M**), Version 12.2(8)T8, RELEASE SOFTWARE (fc1)

ROM: System Bootstrap, Version 11.1(20)AA2, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)

core_router uptime is 5 hours, 8 minutes

System returned to ROM by power-on

System restarted at 09:17:03 mdt Wed Apr 4 2003

System image file is "flash:**c3640-ik9o3s-mz.122-8.T8.bin**"

cisco 3640 (R4700) processor (revision 0x00) with **56320K/9216K** bytes of memory.

R4700 CPU at 100Mhz, Implementation 33, Rev 1.0

SuperLAT software (copyright 1990 by Meridian Technology Corp).

6 Ethernet/IEEE 802.3 interface(s)

DRAM configuration is 64 bits wide with parity disabled.

125K bytes of non-volatile configuration memory.

16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102



(III) Using the Appropriate Command

- Show run command is a crutch
- There is a better show command for every piece of the show run output
- You may not have level 15 access

Example of router section of show run:

```
router eigrp 2284
  passive-interface Serial0/0:0.1
  network 63.0.0.0
  network 205.229.198.0
  no auto-summary
  no eigrp log-neighbor-changes
```

- Compare this to show ip protocols



Show IP Protocols

Routing Protocol is "eigrp 2284"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Default networks flagged in outgoing updates

Default networks accepted from incoming updates

EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0

EIGRP maximum hopcount 100

EIGRP maximum metric variance 1

Redistributing: eigrp 2284

Automatic network summarization is not in effect

Maximum path: 4

Routing for Networks:

63.0.0.0

205.229.198.0

--More--



Show IP Protocols cont.

Continued from previous output:

Passive Interface(s):

Serial0/0:0.1

Ethernet1/0

Ethernet1/1

Routing Information Sources:

Gateway	Distance	Last Update
---------	----------	-------------

205.229.198.249	90	1d23h
-----------------	----	-------

Distance: internal 90 external 170



Using Show Run

- If we still have to use show run, let's use it properly
- Show run followed by the / option
- Show run using the | option
- Following the | option is a regular expression



Show Run | options

Examples of show run |

core_router#sh run | ?

begin Begin with the line that matches

exclude Exclude lines that match

include Include lines that match

core_router#sh run | incl access-list 10 **(shows any access-list that begins with the numbers 1 and 0)**

core_router#sh run | incl access-list 10_ **(shows any access-list that begins with the numbers 1 and 0 followed by a delimiter, in this case 'space')**



Other | Commands

Other commands that can utilize |

- Show access-list 109 |
- Show ip arp |
- Show ip route |
- Show ip interface |
- Basically any show command that displays filterable info



(IV) What am I looking At?

- Show controllers
- Show interface
- Show [protocol] interface
- Show tcp vty 0



Show Controllers

Show Controllers [interface]

3640_4#sh controllers serial 3/0 (or **cxbus on >=7000's**)

CD2430 Slot 3, Port 0, Controller 0, Channel 0, Revision 16

Channel mode is synchronous serial

idb 0x62781084, buffer size 1524, **V.35 DTE cable**



Show Interface E0/0

Ethernet0/0 is up, line protocol is up
Hardware is AmdP2, address is **aa00.0412.1234** (bia **0006.537b.d5c1**)
Internet address is 10.123.123.254/24
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 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
--more--



Show Interface E0/0 cont.

5 minute output rate 0 bits/sec, 0 packets/sec
26361 packets input, 3684169 bytes, **0 no buffer**
Received 2416 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, **3 ignored**
0 input packets with dribble condition detected
26254 packets output, 7407061 bytes, 0 underruns
0 output errors, 2 collisions, 0 interface resets
0 babbles, 0 late collision, 17 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out



Show [IP] interface

Ethernet0/0 is up, line protocol is up
Internet address is 10.123.123.254/24
Broadcast address is 255.255.255.255
MTU is 1500 bytes
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is 107
Proxy ARP is enabled
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
--more--



Show [IP] interface cont.

IP CEF switching is enabled

IP CEF Feature Fast switching turbo vector

IP output packet accounting is disabled

IP access violation accounting is disabled

TCP/IP header compression is disabled

RTP/IP header compression is disabled

Probe proxy name replies are disabled

Policy routing is enabled, using route map fixvpn

Network address translation is enabled, interface in domain inside

WCCP Redirect outbound is disabled

WCCP Redirect inbound is disabled

WCCP Redirect exclude is disabled

BGP Policy Mapping is disabled

IP multicast multilayer switching is disabled

Inbound inspection rule is determan.org

Inbound audit rule is outside



Show TCP VTY 0

```
core_router#sh tcp vty 0
tty130, virtual tty from host 10.123.123.11
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 10.123.123.254, Local port: 23
Foreign host: 10.123.123.11, Foreign port: 2054
Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x1386084):
Timer      Starts  Wakeups    Next
Retrans    4333     0         0x0
TimeWait   0         0         0x0
AckHold    2830    127        0x0
SendWnd    0         0         0x0
KeepAlive  0         0         0x0
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
```



(V) When the Router is the Problem

- Enabling POST Messages
- Performing a Stack Trace
- Decoding a Stack Trace
- Core Dumps
- Access-lists



Enabling POST Messages

- By default, POST messages are suppressed during boot
- POST messages can diagnose why a router isn't booting correctly, or not responding
- Enabling POST messages requires modification of the config-register
- Bit (dip-switch) 15 needs to be enabled
- Default register is 0x2102
- To add POST messages use 0xA102



Tracebacks and Stack Traces

- When a router fails it produces a traceback
- Some tracebacks cause a reboot
- We can examine the traceback with a stack trace
- After decoding, the stack trace can point to the problem

Apr 10 17:27:00: %SYS-3-CPUHOG: Task ran for 4784 msec (2/1), process = Virtual Exec, PC = 6043B208.

-Traceback= 6043B210 603833F0 60383E14 603836B0 60484644 603A4A78
603B72D0 60421 724 60421710x



Show Stacks

- Issue sh stacks:

```
core_router#sh stacks
```

```
Minimum process stacks:
```

```
Free/Size Name
5588/6000 DHCPD Receive
5576/6000 SPAN Subsystem
5412/6000 PostOfficeNet
5532/6000 CDP Protocol
1916/3000 allegro libretto init
7420/12000 Init
5268/6000 RADIUS INITCONFIG
7992/12000 Virtual Exec
5384/6000 script background loader
7132/9000 IP RTR Probe 1
--more--
```

Interrupt level stacks:

Level	Called	Unused/Size	Name
1	190442	6248/9000	Network interfaces
2	51309	8616/9000	DMA/Timer Interrupt
3	0	9000/9000	PA Management Int Handler
4	23759	8620/9000	Console Uart
5	0	9000/9000	External Interrupt
7	28968753	8604/9000	NMI Interrupt Handler

- Highlight all data, and paste into decoder



Output Interpreter

• <https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>

Cisco-Output Interpreter - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites History

Address <https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl> Go Links

1. Enter output from one or more commands. [example](#)

Paste the output into this field:

Remove passwords and other sensitive information

Or, for large outputs, save the output to file and upload it:

Enter a file name (or browse your disk):

Browse...

2. What should the analysis engine report? [example](#)

Errors requiring action

Errors, Warnings suggesting action

Errors, Warnings, Pertinent status information

Errors, Warnings, Pertinent status information, Helpful references

3. Submit for immediate analysis.

Enter one or more addresses to email a copy of the report: *optional

Send Email To

example: jsmith@company.com, team@company.com

Reset Submit

BUSINESS INDUSTRIES & SOLUTIONS | NETWORKING SOLUTIONS & PROVISIONED SERVICES | PRODUCTS & SERVICES | TECHNOLOGIES | ORDERING | TECHNICAL SUPPORT | LEARNING & EVENTS | PARTNERS & RESELLERS | ABOUT CISCO

(1 item remaining) Downloading picture https://www.cisco.com/jsa1/sitewide_text_start.gif... Unknown Zone



sunset
LEARNING



Core Dumps

- When a router crashes it can perform a core dump, if configured

`core_router(config)#exception dump 10.123.123.7` (a file called *hostname-core* will be placed on the tftp server 10.123.123.7 when a dump is performed)

- You can also manually perform a core dump for troubleshooting

`core_router#write core` (you will be prompted for a tftp-server IP address and a filename to use)



Access-lists

- Most common configuration mistake is incorrect access-lists
- Security based ACL usually are built permit>permit>deny
- Missing lines in ACL prevent desired network usage
- Implicit deny filters anything not permitted higher in the list



Deny IP Any Any Log

- Tip: turn implicit deny into explicit deny with logging

```
core_router(config)#access-list 109 deny ip any any log
core_router#term mon
core_router#
Apr 9 15:25:04: %SEC-6-IPACCESSLOGP: list 109 denied tcp
                203.115.212.147(23027) -> 63.227.15.227(80), 1 packet
core_router#
```

- Also acts as a basic IDS



Sources of Other Information

- <http://www.cisco.com>
Official Cisco Information website
- <http://boerland.com/dotu>
Document the undocumented
- <http://nitrous.digex.net>
MAE east/west/etc looking glass
- <http://cidr-report.org>
BGP website



Thank You

Ryan J. Determan

rdeterman@ccti.com (business)

ryan@determan.org (personal)

<http://www.ccti.com>

1.800.569.1894

