Cisco Routers and Switches

Phoenix Cisco User Group (PCUG)

Tools, tips, and tricks you never knew

Hello!

Jeremy D. Cioara - CCIE, MCSE, CNE

AdTEC Networks - Chief Information Officer

Cisco IP Telephony Specialist

Network Engineer, Author, and Trainer

Topic Breakdown

IOS Navigation

Remote Auto-Configuration

Network Monitoring

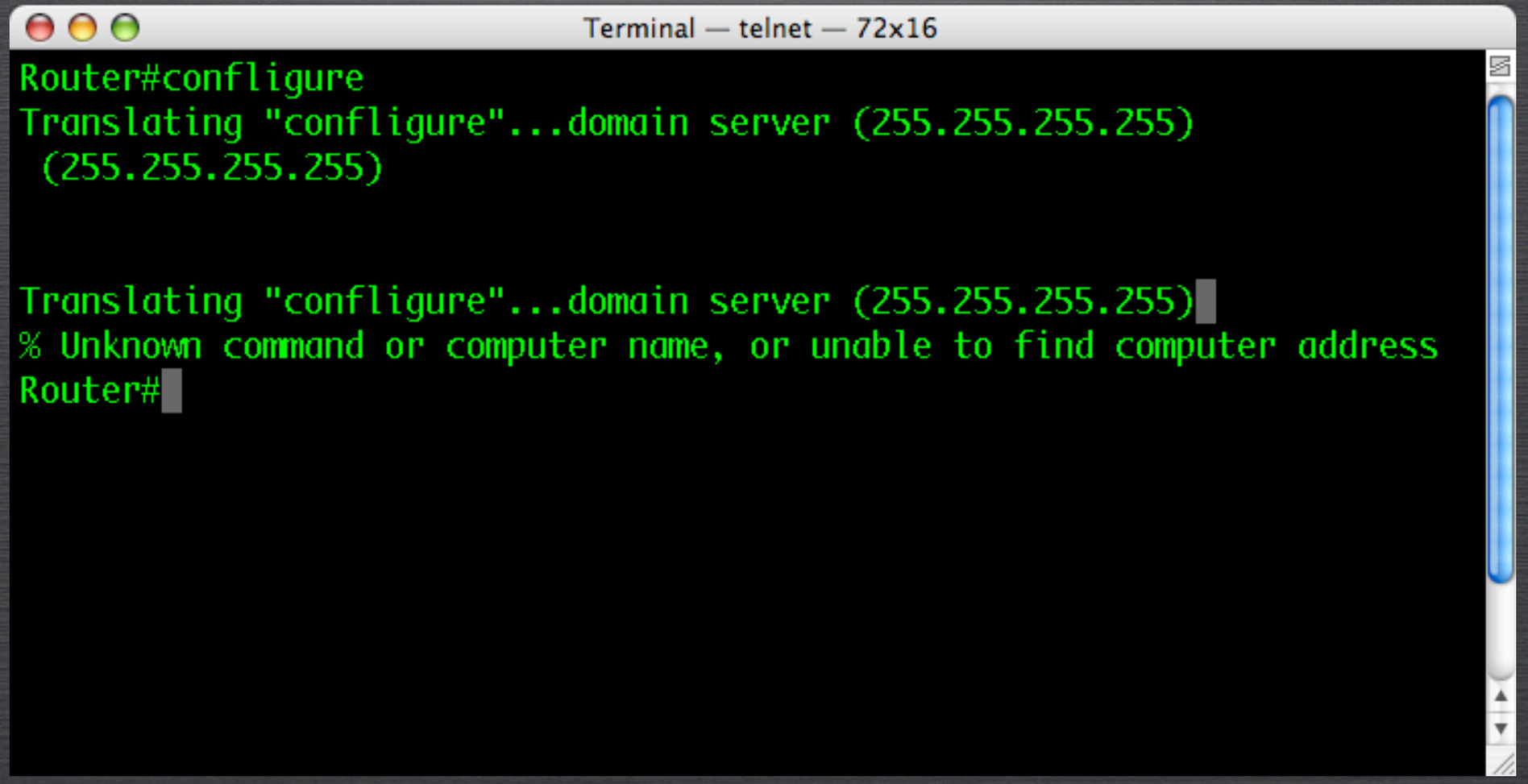
Mesmerizing Utilities

IOS Navigation

- Disabling DNS Lookup
- Limiting EXEC Interruptions
- Filtering Command Output
- Creating Aliases
- Erasing Interface Configurations
- The Wonderful “Do” Command
- Adjusting the TCP Timeout

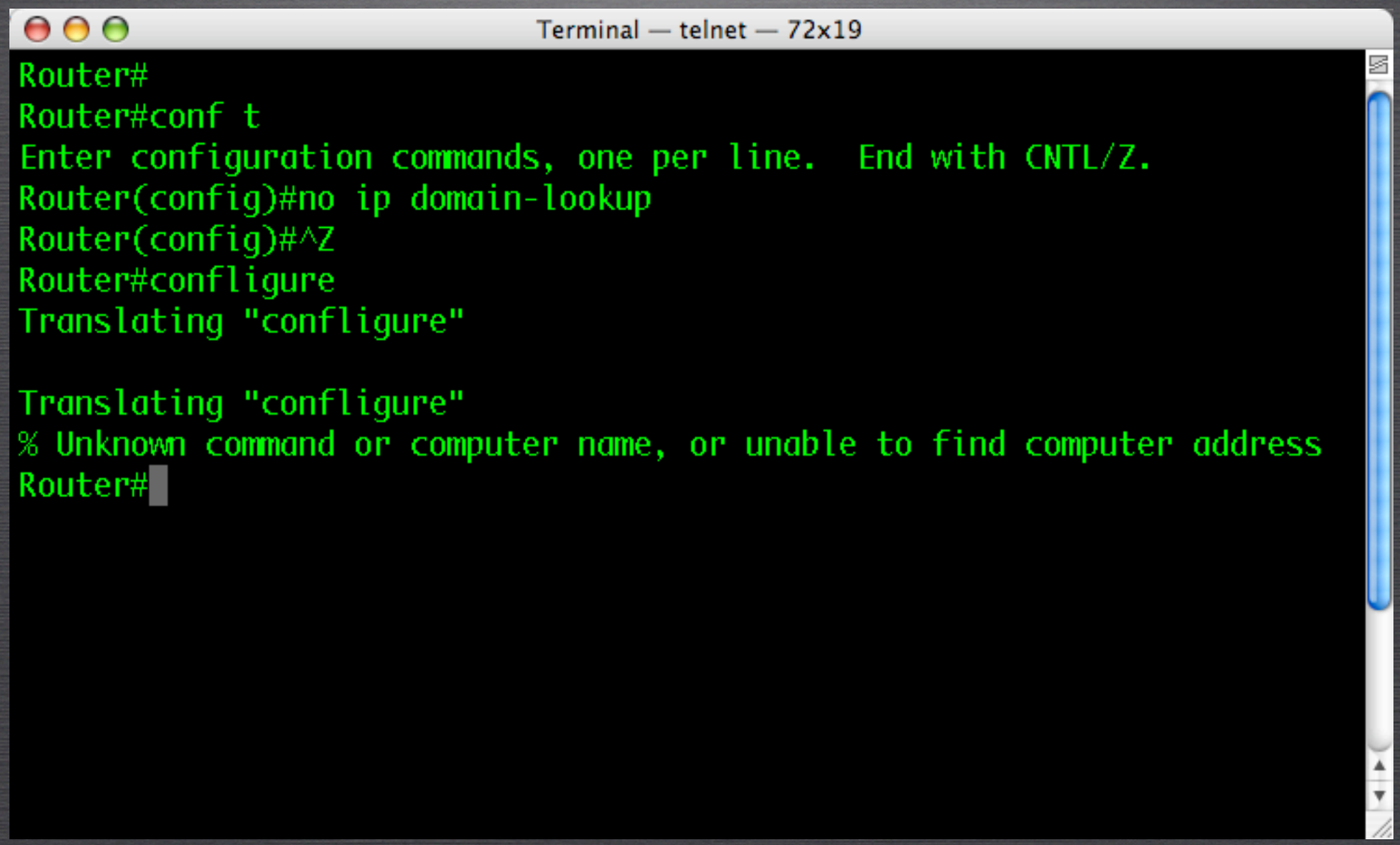
Disabling DNS Lookup

- By default, Cisco router attempts to resolve DNS hostnames to IP addresses
- The result: Any mistyped command in privileged mode causes 30-45 second delay



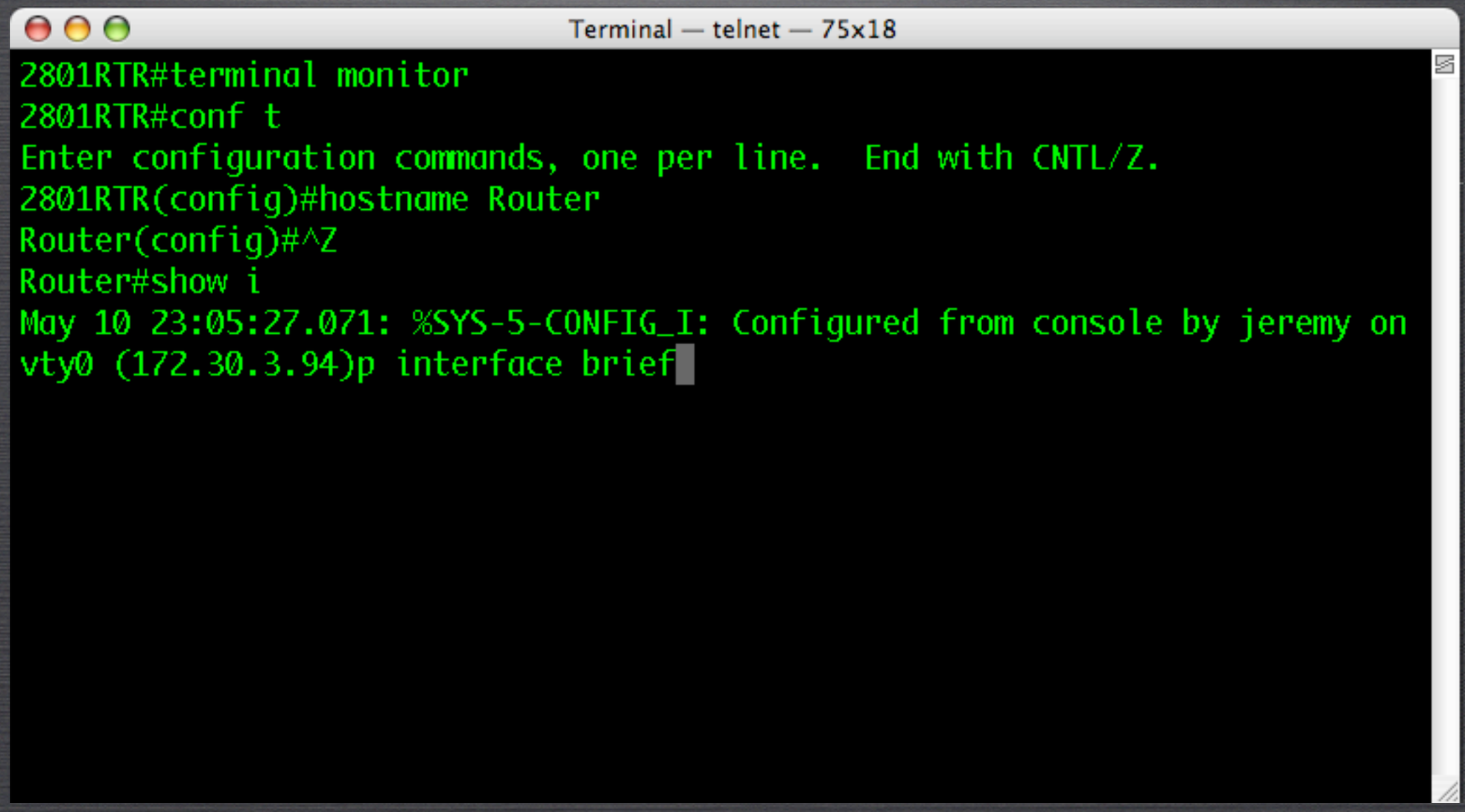
Disabling DNS Lookup (cont.)

- The Solution: Disable DNS lookups



Limiting Exec Interruptions

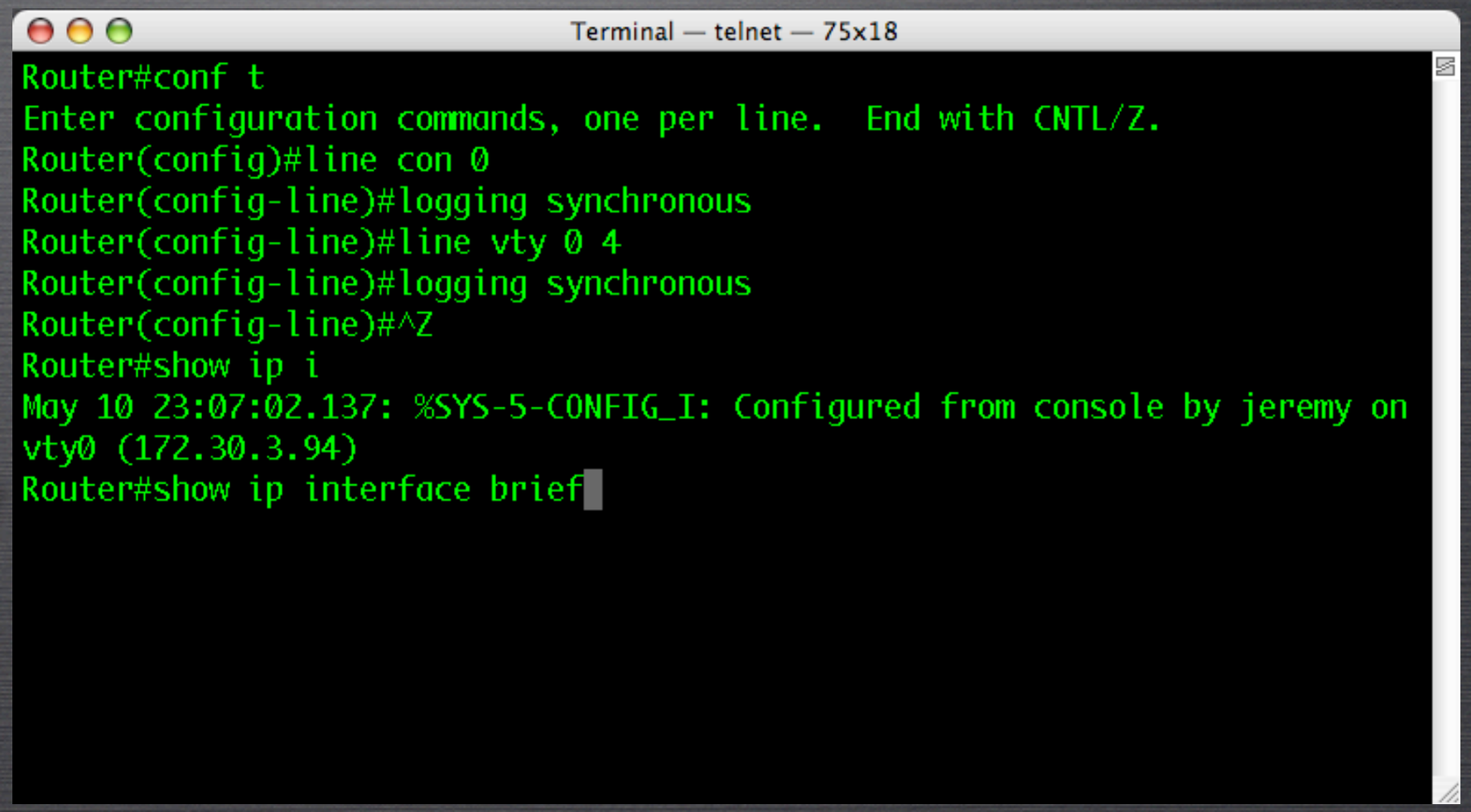
- By default, Cisco devices allow console and line messages to interrupt typed text



Limiting Exec Interruptions

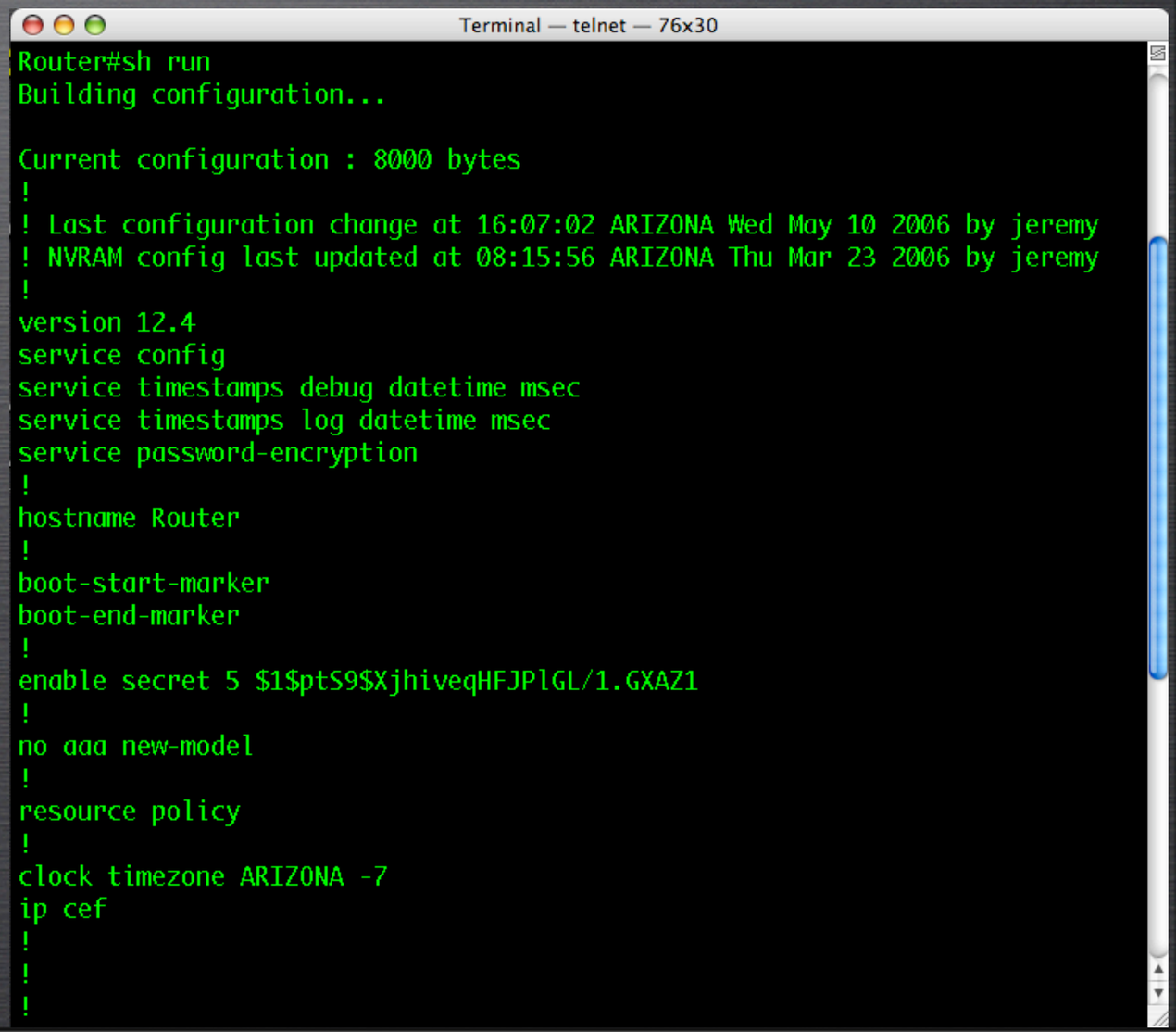
- To prevent this feature, do the following:

The line is automatically repainted



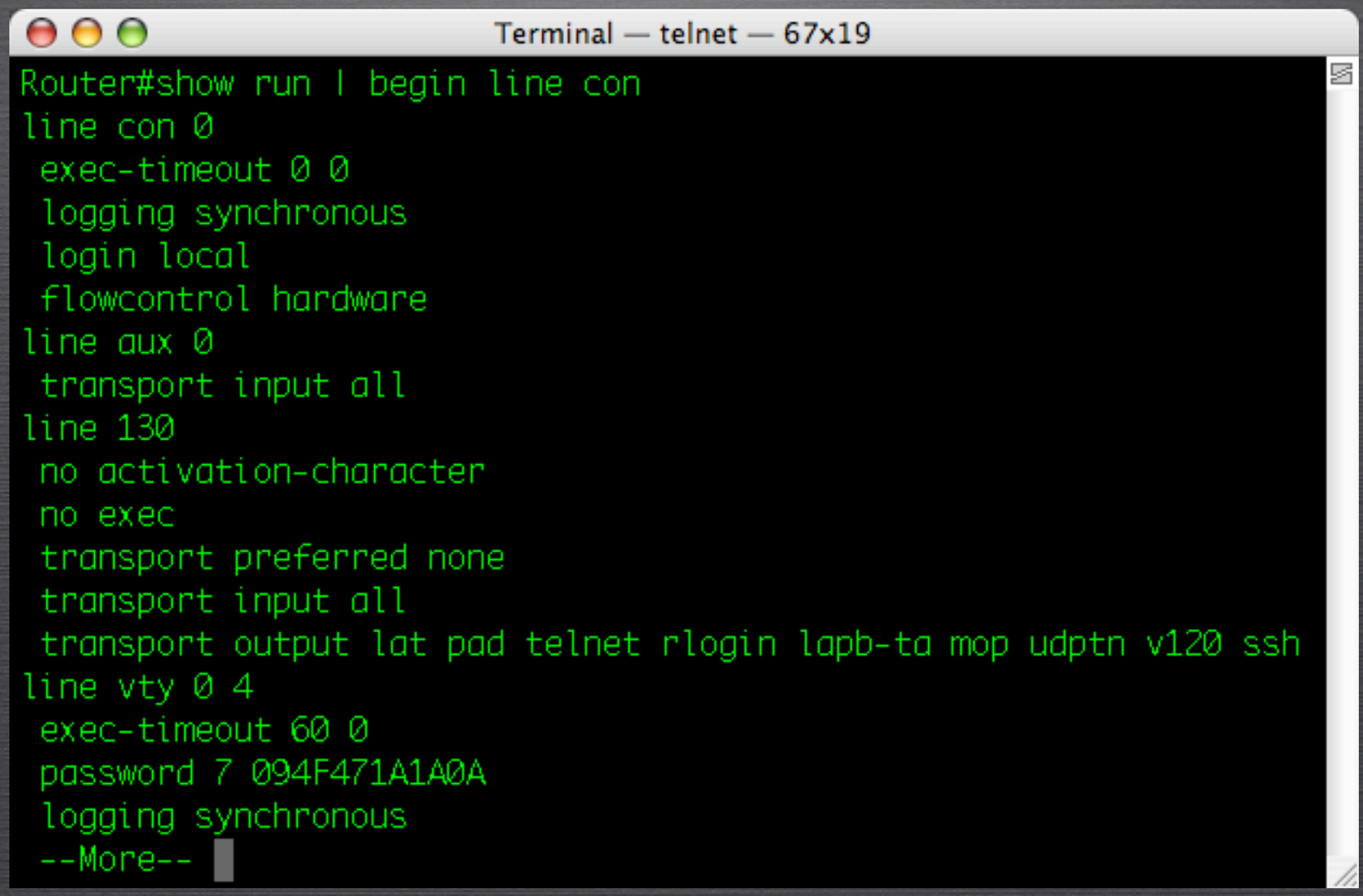
Filtering Command Output

- Many commands output excessive information to the screen.
- Unix-like filtering options can aid in device management



Filtering Command Output

- Router# show <argument> | begin <argument>



Filtering Command Output

- Router# show <argument> | include <argument>

Terminal — telnet — 84x18

```
Router#show run | include ip nat
 ip nat inside
 ip nat outside
ip nat inside source list NAT_ADDRESSES interface FastEthernet0/1 overload
ip nat inside source static tcp 172.30.2.50 3389 interface FastEthernet0/1 3389
ip nat inside source static udp 172.30.3.62 69 interface FastEthernet0/1 69
ip nat inside source static tcp 172.30.3.62 44227 interface FastEthernet0/1 44227
ip nat inside source static udp 172.30.100.11 514 interface FastEthernet0/1 514
ip nat inside source static tcp 172.30.3.62 6881 interface FastEthernet0/1 6881
ip nat inside source static tcp 172.30.100.11 21 interface FastEthernet0/1 21
ip nat inside source static tcp 172.30.3.100 8000 interface FastEthernet0/1 8000
ip nat inside source static tcp 172.30.2.29 3389 interface FastEthernet0/1 3390
Router#
```

Filtering Command Output

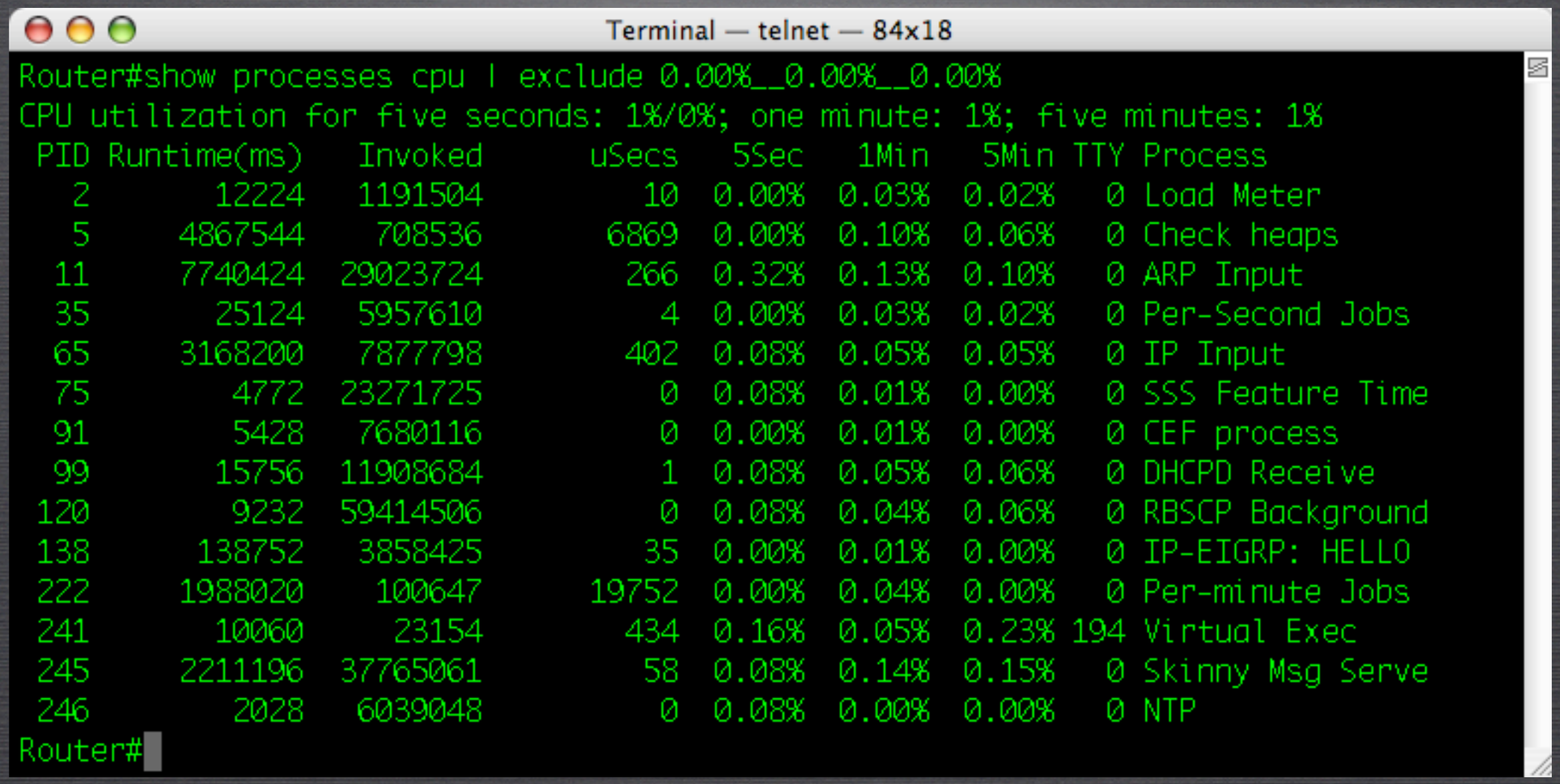
- Router# show run interface <interface>

Terminal — telnet — 84x18

```
Router#show run interface fastethernet 0/0
Building configuration...

Current configuration : 161 bytes
!
interface FastEthernet0/0
 ip address 172.30.4.2 255.255.255.0
 ip nbar protocol-discovery
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
end

Router#
```

Getting Fancy with Filtering

- Router# show process cpu | exclude 0.00%__0.00%__0.00%



The Alias Command

- In the world of Cisco, you may find yourself typing the same commands again and again
- The alias command can help alleviate a little carpal tunnel syndrome
- Commands I use all the time:
  - show ip interface brief
  - show running-config
  - show ip route
  - show ip <ospf/eigrp> neighbor
  - show ip bgp

The Alias Command

Syntax:

- Router(config)# alias <mode> <alias> <command>

Terminal — telnet — 93x23

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#alias exec s show ip int brief
Router(config)#alias exec sir show ip route
Router(config)#alias exec sr show run
Router(config)#alias exec sofn show ip ospf neighbor
Router(config)#^Z
Router#
May 11 00:12:37.824: %SYS-5-CONFIG_I: Configured from console by jeremy on vty0 (172.30.3.94)
Router#sir
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 68.3.160.1 to network 0.0.0.0

     68.0.0.0/21 is subnetted, 1 subnets
C       68.3.160.0 is directly connected, FastEthernet0/1
     172.19.0.0/32 is subnetted, 1 subnets
```

The Alias Command

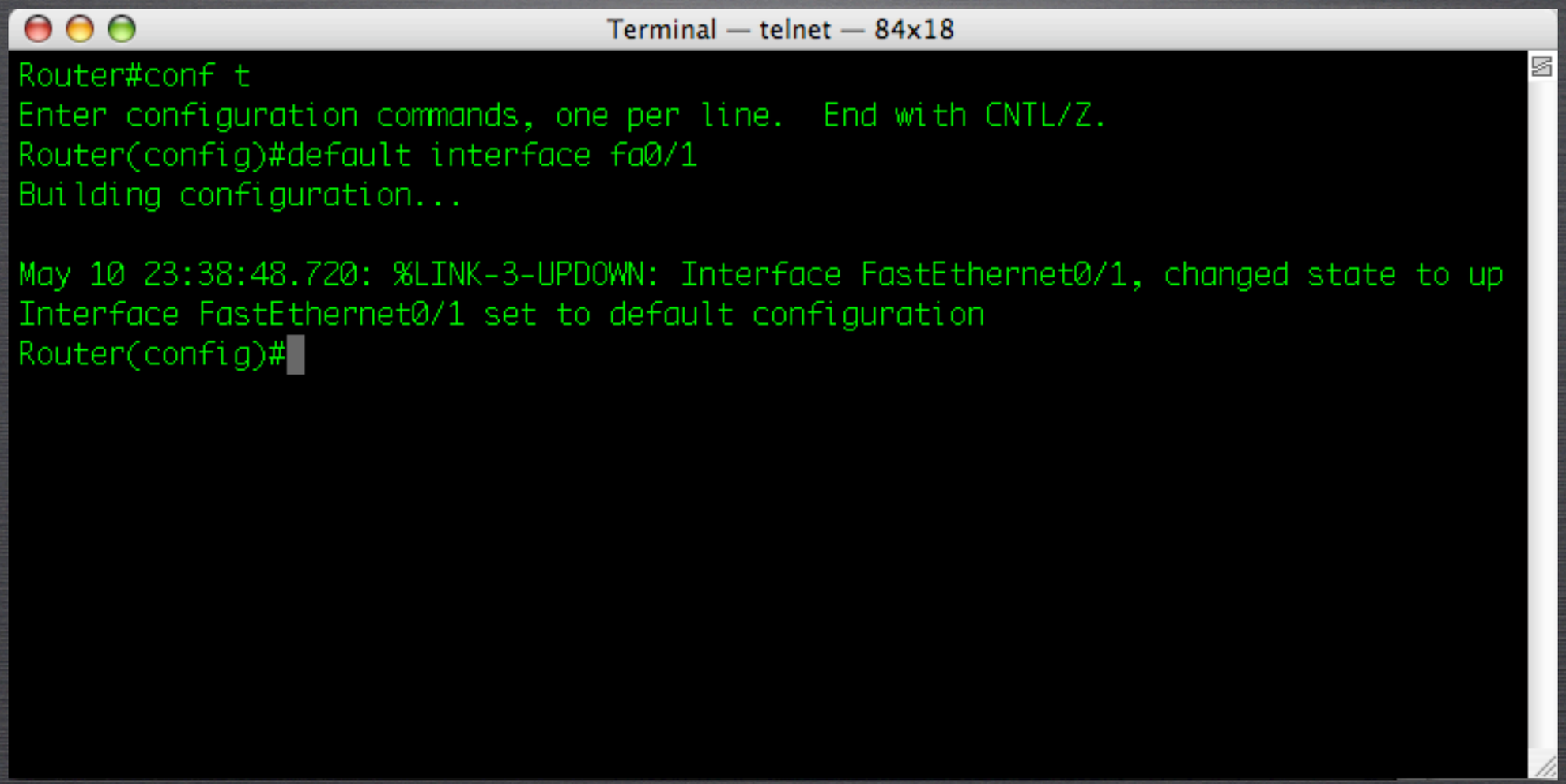
- Verifying your aliases

Terminal — telnet — 81x19

```
Router#show alias
Exec mode aliases:
  h                    help
  lo                   logout
  p                    ping
  r                    resume
  u                    undebug
  un                   undebug
  w                    where
  traffic              show ip nbar protocol-discovery st bi top 10
  sri                  show run | include
  s                    show ip int brief
  sir                  show ip route
  sr                   show run
  sofn                 show ip ospf neighbor
  proc                 show proc cpu | excl 0.00%__0.00%__0.00%

Router#
```

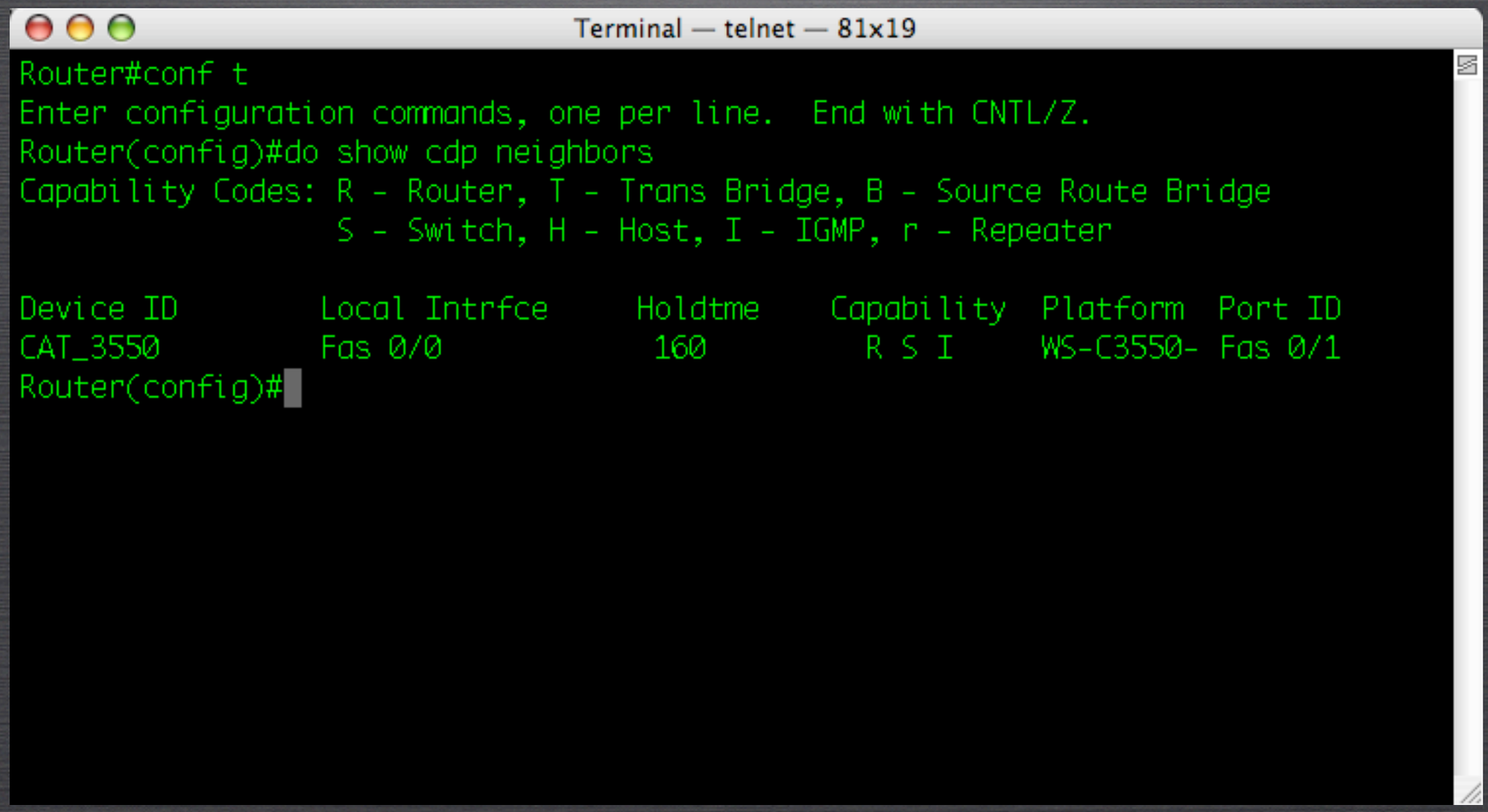
Erasing an Interface Config

- Router(config)# default interface <int>



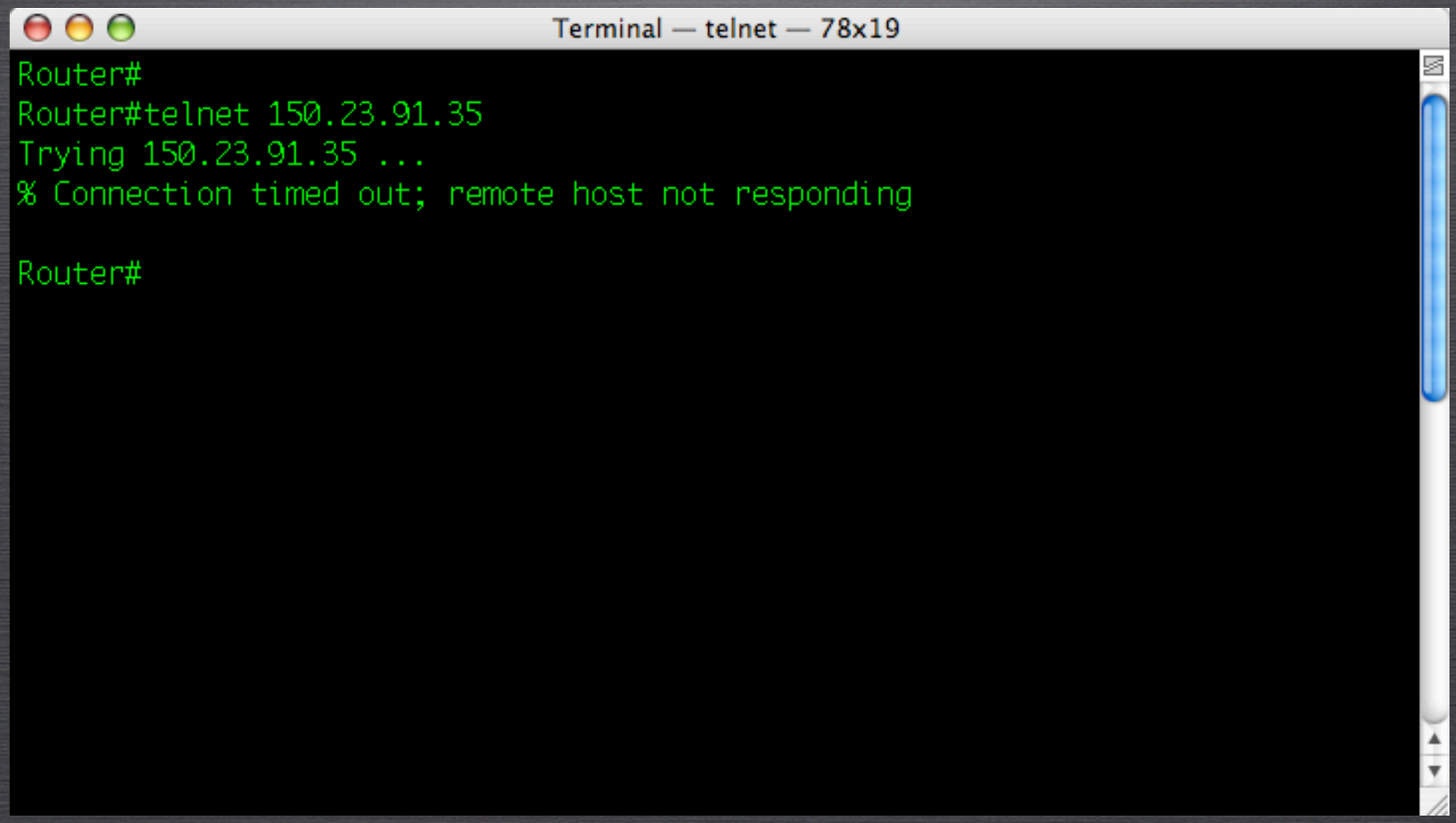
The Wonderful 'do' Command

- Allows you to execute privileged mode commands from any mode
- IOS 12.2(8)T versions and later



Shrinking the TCP Timeout

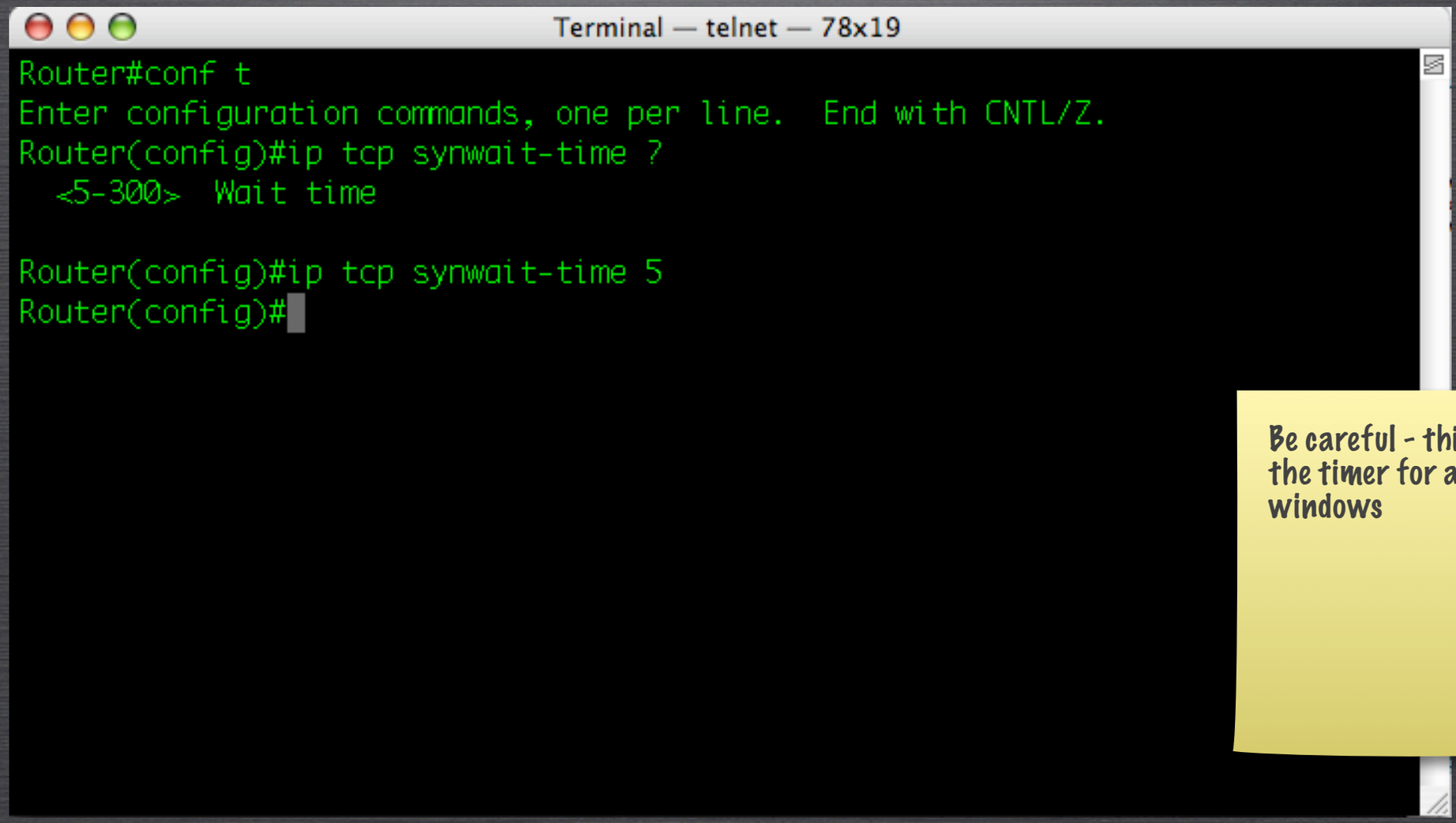
- When you telnet to a mistyped or unavailable IP address, the router hangs for 30 seconds before you can get a prompt back



Shrinking the TCP Timeout

- To adjust this timer, use the following command:

Router(config)# ip tcp synwait-time <5-300 seconds>

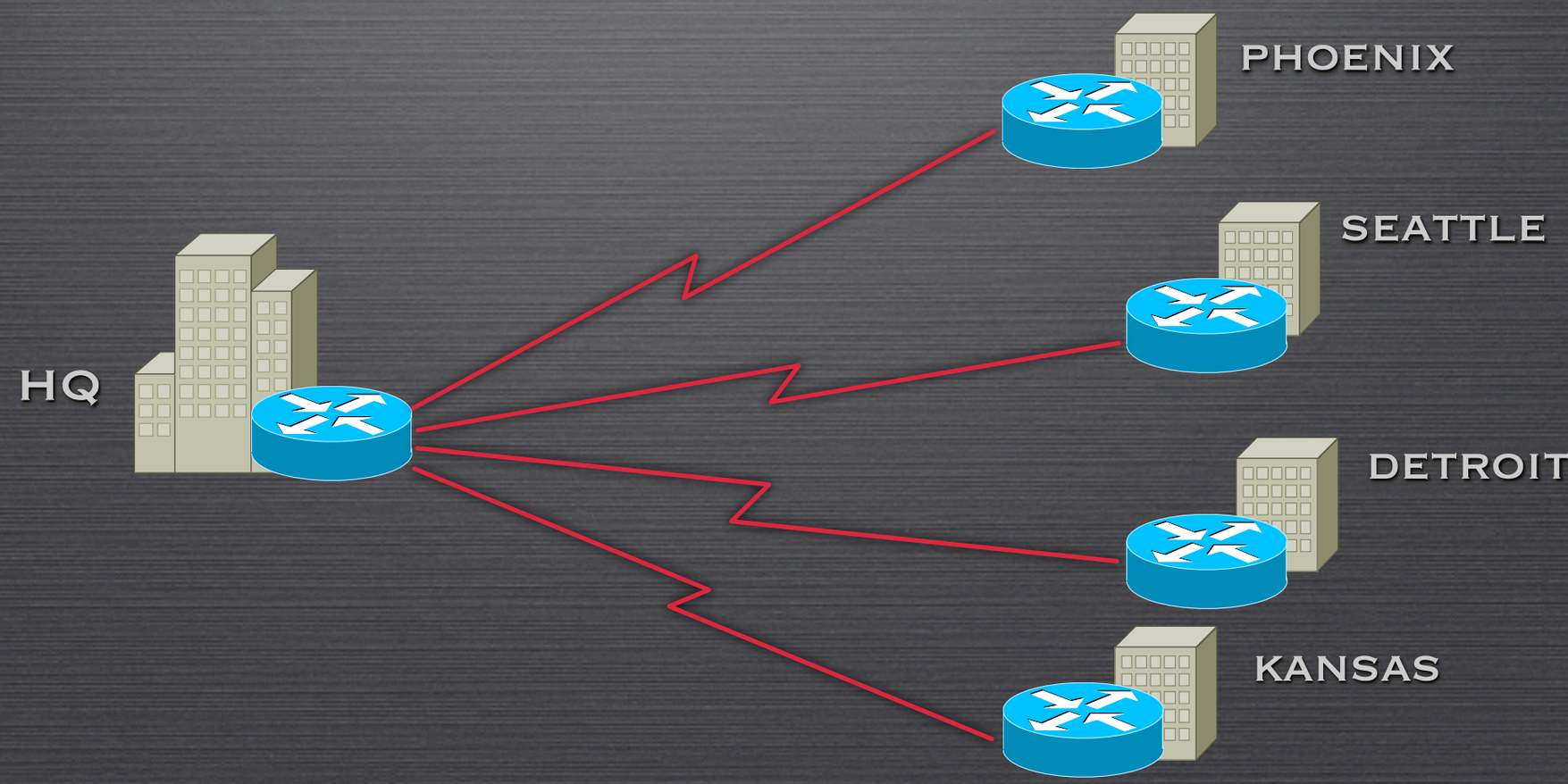


Be careful - this adjusts the timer for all TCP windows

Remote Router Auto-Configuration

Remote Router Auto-Configuration

Scenario: You are deploying four remote offices for your corporation; however, you are the only Cisco-competent employee



Remote Router Auto-Configuration

Concepts:

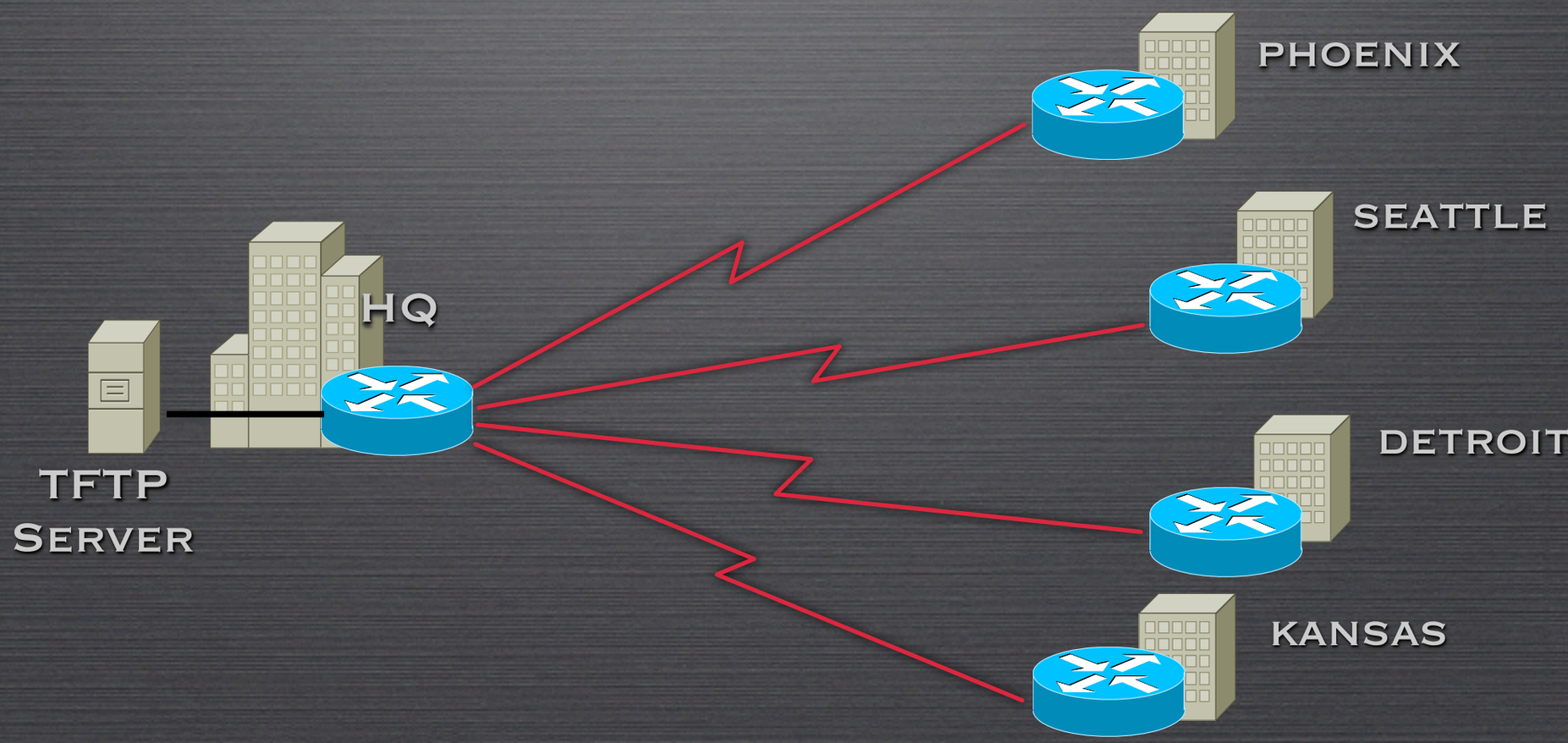
1. A router (out-of-the-box) will attempt to receive an IP address via DHCP (on LAN interfaces) or SLARP (on serial interfaces)

2. If they receive an IP address, they will begin broadcasting for a file called network.config. This file tells the router its name

3. The router will then broadcast for a file called <router_name>.config

Remote Router Auto-Configuration

Step 1: Set up a TFTP Server at the central location

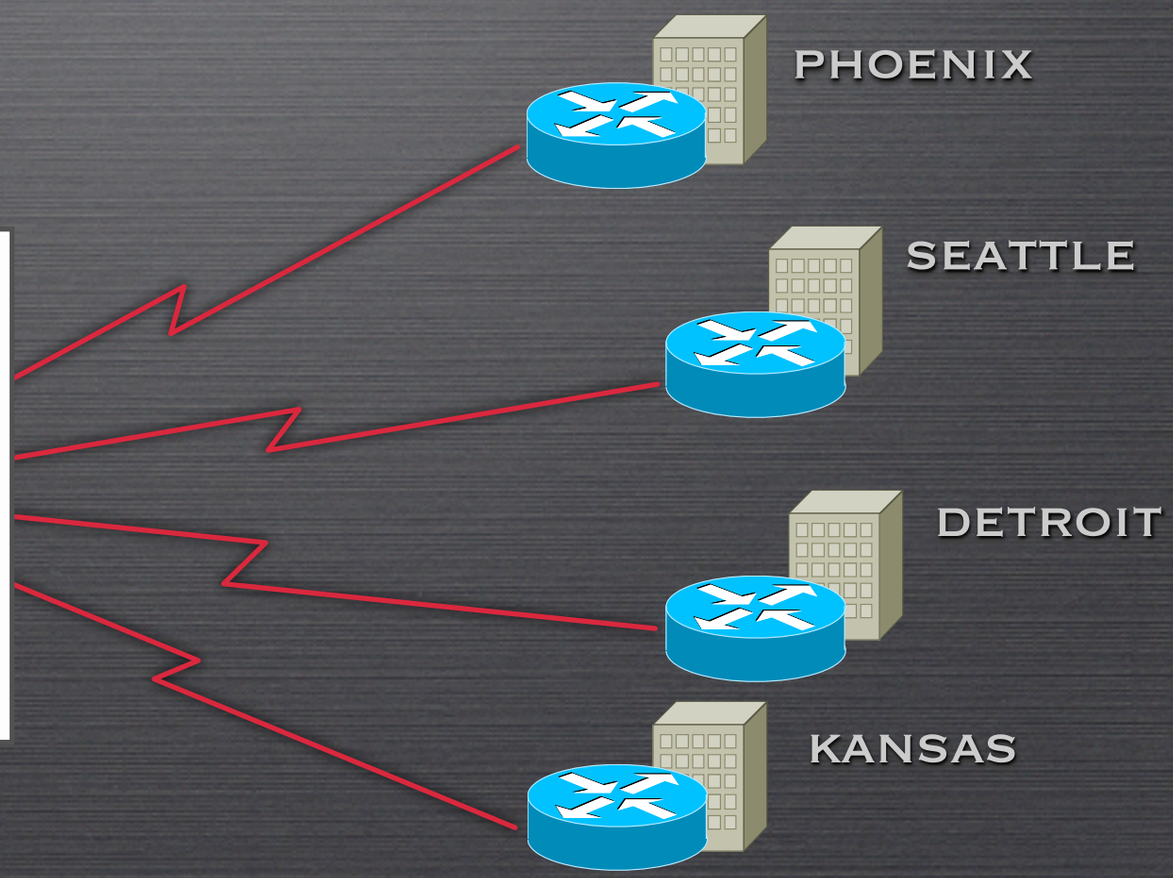


Remote Router Auto-Configuration

Step 2: Create an ASCII text file on the TFTP server called **network.config** containing the name-to-ip mappings for the new routers

network.config

```
phoenix   10.5.1.2
seattle   10.6.1.2
detroit   10.7.1.2
kansas    10.8.1.2
```

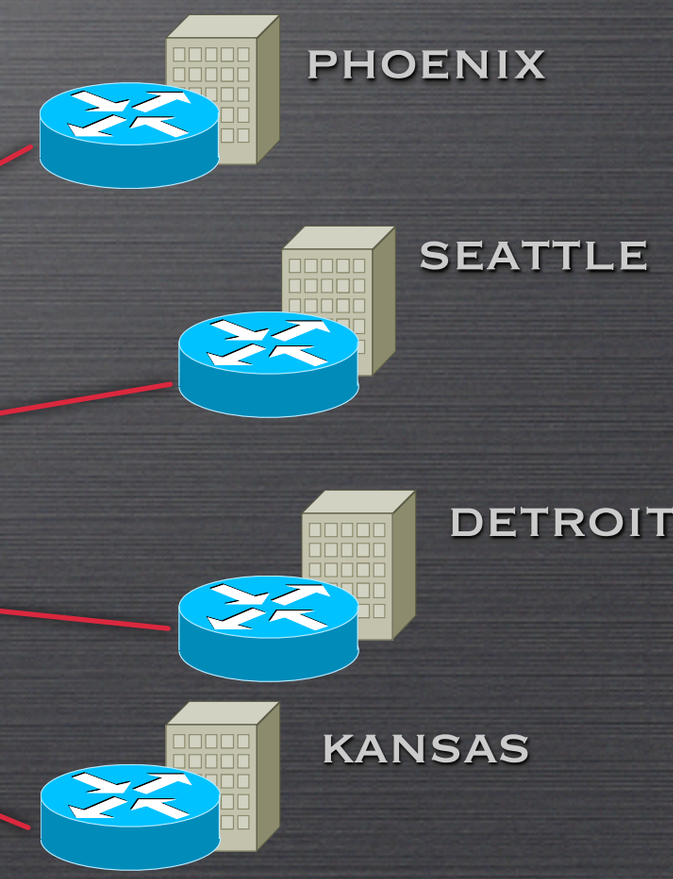


Remote Router Auto-Configuration

Step 3: Create an ASCII text file on the TFTP server for each router called <RTR_NAME>.config - routers will broadcast for this filename

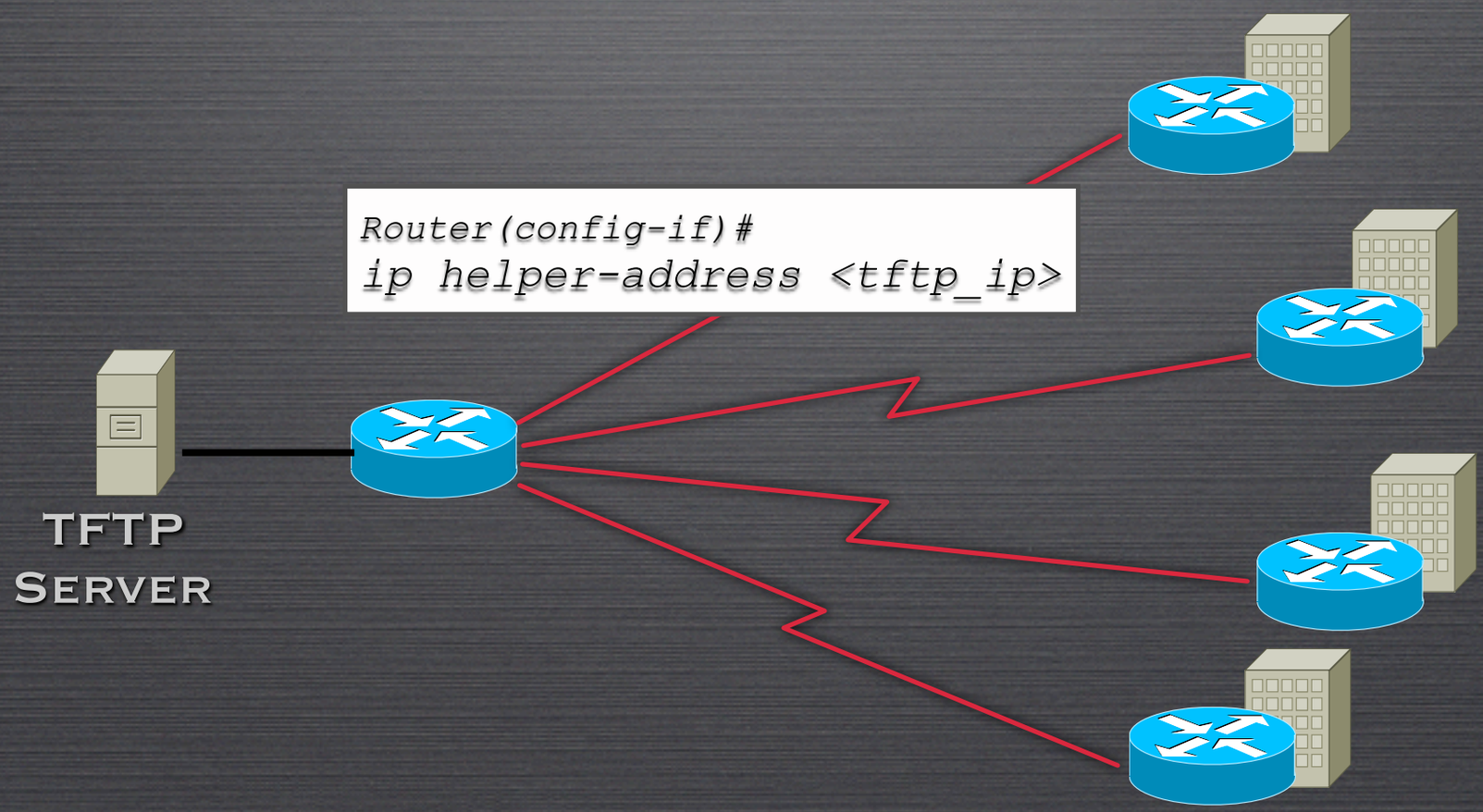
phoenix.config

```
network.config

 version 12.4
service config
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$ptS0$XjhivegHFJPlGL/1.GXAZ1
!
no aaa new-model
!
resource policy
!
clock timezone ARIZONA -7
ip cef
```



Remote Router Auto-Configuration

Step 4: Add an "ip helper-address" command on each WAN interface of the HQ router pointing to the TFTP server



Network Monitoring

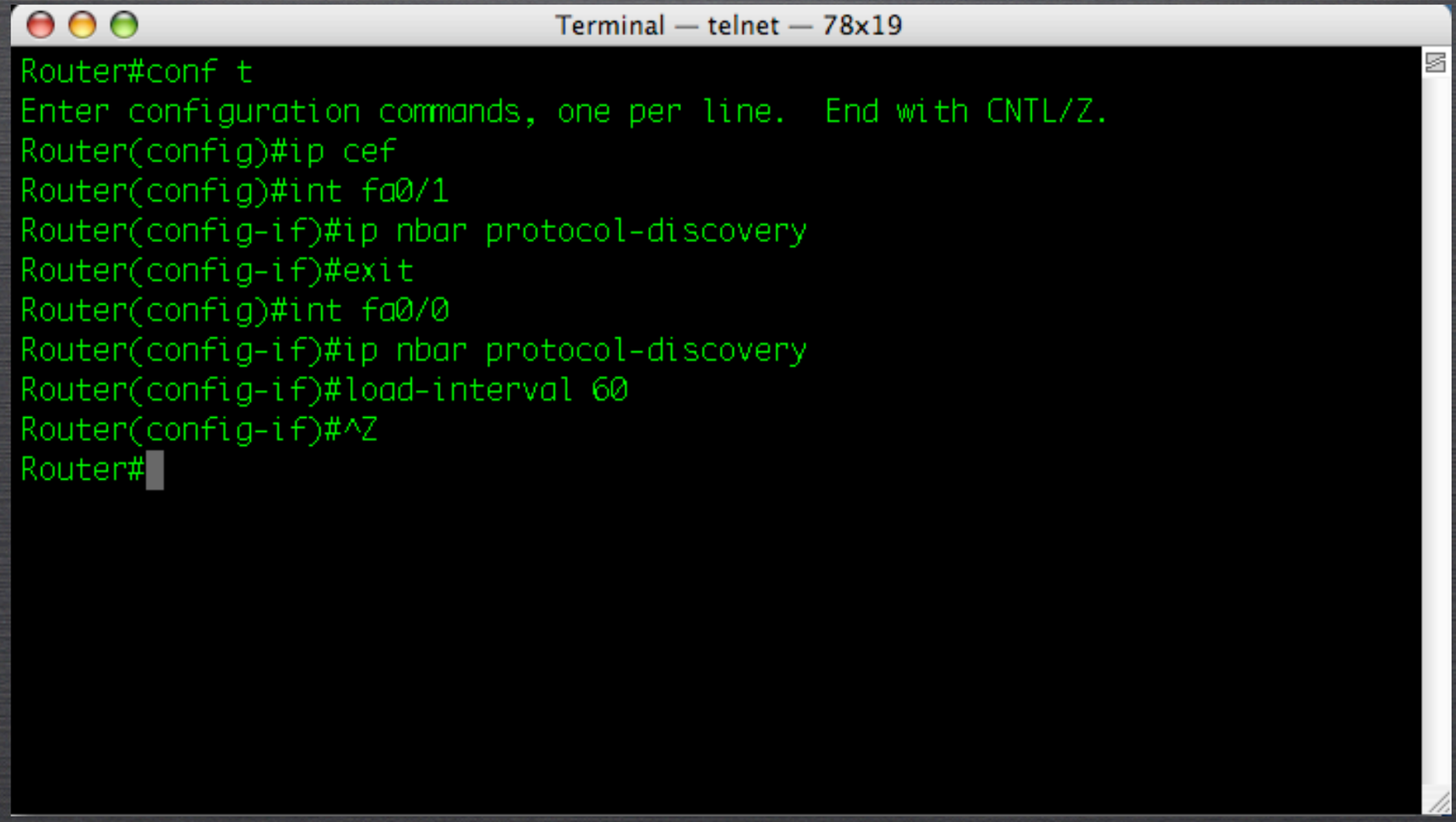
- Using Built-in Network Monitoring
  - Network-Based Application Recognition (NBAR)
  - Netflow
- Using Cool, Free SNMP Monitoring
  - Multi-Router Traffic Grapher (MRTG)
  - Paessler-Router Traffc Grapher (PRTG)

Network-Based Application Recognition (NBAR)

- NBAR is a application recognition utility originally designed for QoS
- Allows QoS mechanisms to match an manipulate:
  - VoIP traffic
  - Peer-to-Peer file sharing
  - Multiple common applications (such as ftp, http, realaudio, etc...)
- Also included in NBAR is a spiffy traffic monitoring feature

Network-Based Application Recognition (NBAR)

- Enabling NBAR
  - Requires cisco express forwarding (cef)
  - Activated on a per-interface basis



Network-Based Application Recognition (NBAR)

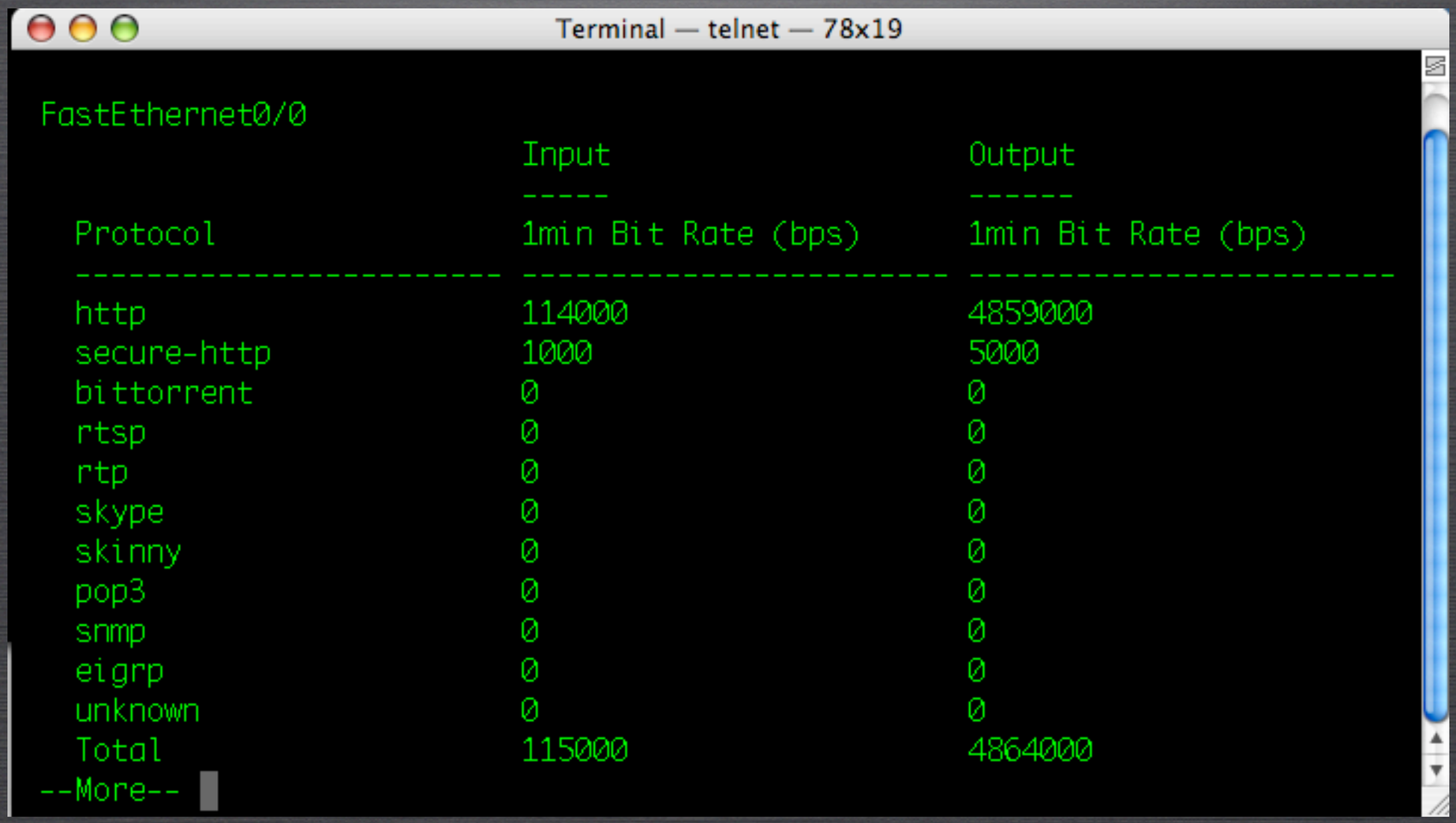
- Monitoring NBAR - many options

Terminal — telnet — 78x19

```
Router#show ip nbar protocol-discovery ?
  interface  Show for a specific interface
  protocol   Show stats about a particular protocol
  stats      Show Stats
  top-n      Show Top-N protocols by bytes
  |          Output modifiers
  <cr>

Router#show ip nbar protocol-discovery stats ?
  bit-rate      Show Bit Rates
  byte-count    Show Byte Counts
  max-bit-rate  Show Max Bit Rate
  packet-count  Show Packet Stats

Router#show ip nbar protocol-discovery stats bit-rate top-n 10
```

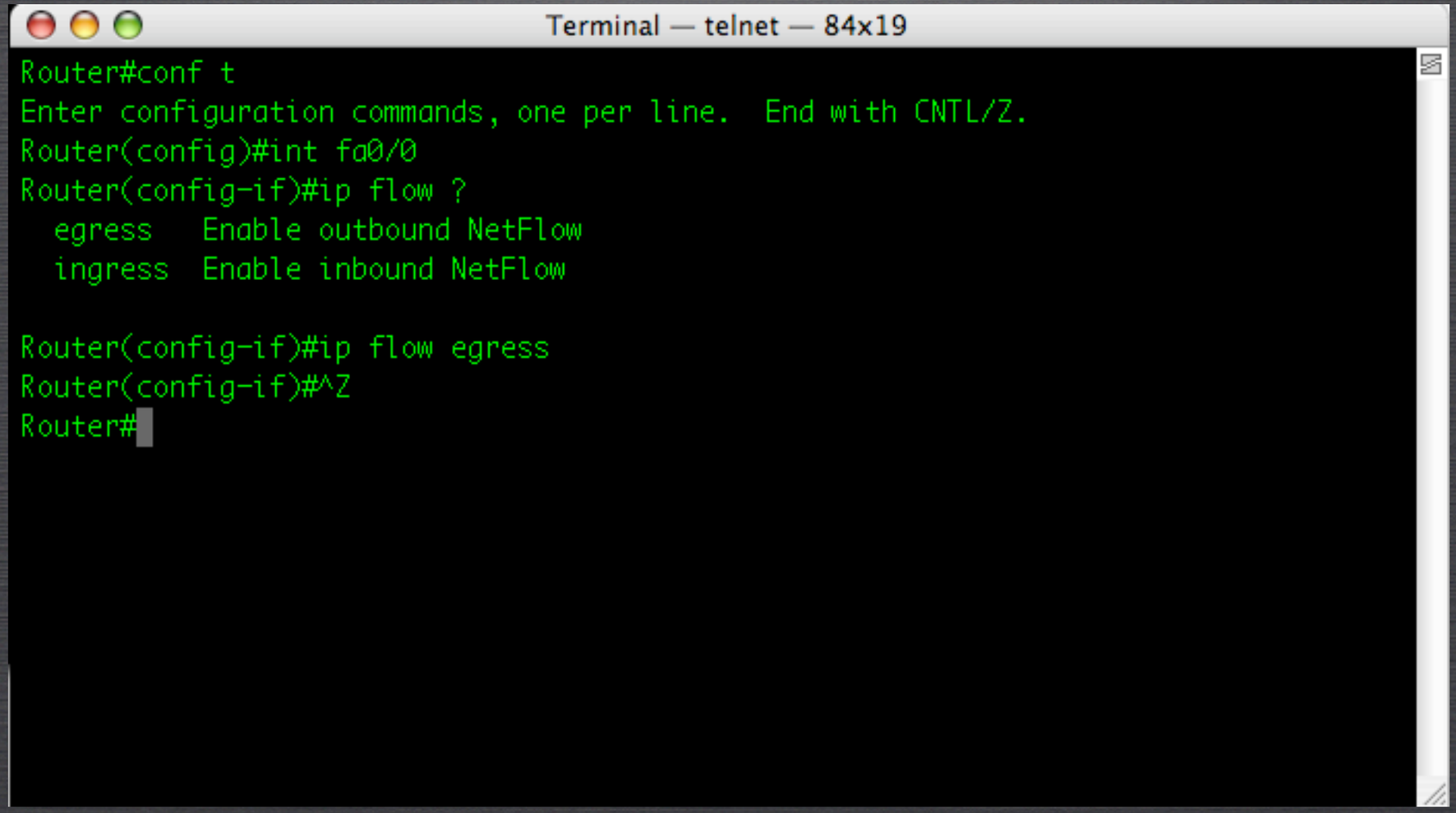
Network-Based Application Recognition (NBAR)

- Monitoring NBAR - top protocols



IP Netflow

- Netflow is an EXTREMELY advanced and complex system Cisco devices can use to track data flows
- Many commercial systems have been created to take advantage of netflow statistics



IP Netflow

Terminal — telnet — 84x32

```
Router#show ip cache flow
IP packet size distribution (297345 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .019 .483 .000 .000 .000 .009 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .483 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  6 active, 4090 inactive, 18343 added
  603698 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25736 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-WWW            224      0.0        26    47      0.0       0.0       1.6
TCP-SMTP             5      0.0         7    69      0.0       0.2       1.4
TCP-other           25      0.0         2    42      0.0       1.2       5.3
UDP-NTP          17969      0.0         8    76      0.0      17.4      15.4
UDP-other           98      0.0        31   201      0.0       1.6      15.5
ICMP                20      0.0         8   198      0.0       8.7      15.4
Total:           18341      0.0         8    77      0.0      17.0      15.3

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/1         69.59.242.82    Fa0/0*        172.30.2.26     11 2710 2710     1
Fa0/1         12.164.210.1    Fa0/0*        172.30.100.11   11 00A1 08EE     2
 --More--
```

IP Netflow

Terminal — telnet — 84x32

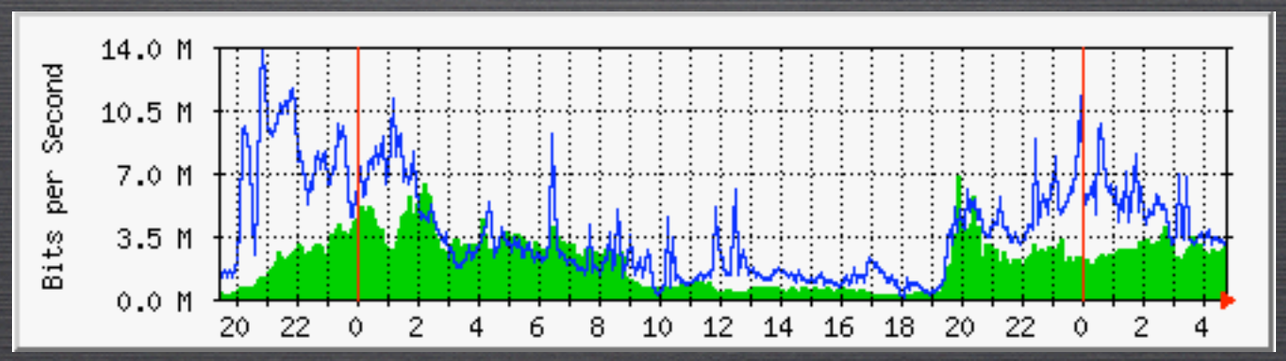
```
IP Flow Switching Cache, 278544 bytes
  6 active, 4090 inactive, 18343 added
  603698 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25736 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-WWW            224      0.0        26    47      0.0       0.0       1.6
TCP-SMTP             5      0.0         7    69      0.0       0.2       1.4
TCP-other           25      0.0         2    42      0.0       1.2       5.3
UDP-NTP          17969      0.0         8    76      0.0      17.4      15.4
UDP-other           98      0.0        31   201      0.0       1.6      15.5
ICMP                20      0.0         8   198      0.0       8.7      15.4
Total:           18341      0.0         8    77      0.0      17.0      15.3

SrcIf       SrcIPaddress    DstIf       DstIPaddress    Pr SrcP DstP  Pkts
Fa0/1       69.59.242.82    Fa0/0*      172.30.2.26     11 2710 2710     1
Fa0/1       12.164.210.1    Fa0/0*      172.30.100.11   11 00A1 08EE     2

SrcIf       SrcIPaddress    DstIf       DstIPaddress    Pr SrcP DstP  Pkts
Fa0/1       12.164.210.1    Fa0/0*      172.30.100.11   11 00A1 08ED     2
Fa0/1       208.47.130.1    Fa0/0*      172.30.100.11   11 00A1 0914     2
Fa0/1       208.47.130.1    Fa0/0*      172.30.100.11   11 00A1 0915     2
Fa0/1       216.115.21.69   Fa0/0*      172.30.2.30     11 2710 13C5     1
Fa0/1       209.133.111.21  Fa0/0*      172.30.3.94     06 0050 C6C4   188K
Router#
```

MRTG and SNMP

- The Multi-Router Traffic Grapher is a utility that has been around for eons
  - Available as a free download from www.mrtg.org
  - Creates HTML pages graphing specified SNMP counters

MRTG and SNMP

- The Multi-Router Traffic Grapher is a utility that has been around for eons
  - Available as a free download from www.mrtg.org
  - Creates HTML pages graphing specified SNMP counters



High-level View of SNMP

- SNMP is a protocol that allows you to perform GET and SET operations on Management Information Base (MIB) objects on a network device
  - GET operations retrieve information
  - SET operations change information
  - Every informational item on a Cisco device has a MIB identifier

Replacing Passwords Using SNMP

- snmpset -t 10 -r 5 -c communityname hostname .1.3.6.1.4.1.9.2.1.53.150.150.150.1 octetstring configfile.txt

Where:

- 150.150.150.150 is the address of the Trivial File Transfer Protocol (TFTP) server
- hostname is the hostname of the router (or its IP address)
- configfile.txt is the file containing the configuration commands that you wish to implement (this file must be in a directory reachable by TFTP to the TFTP server)

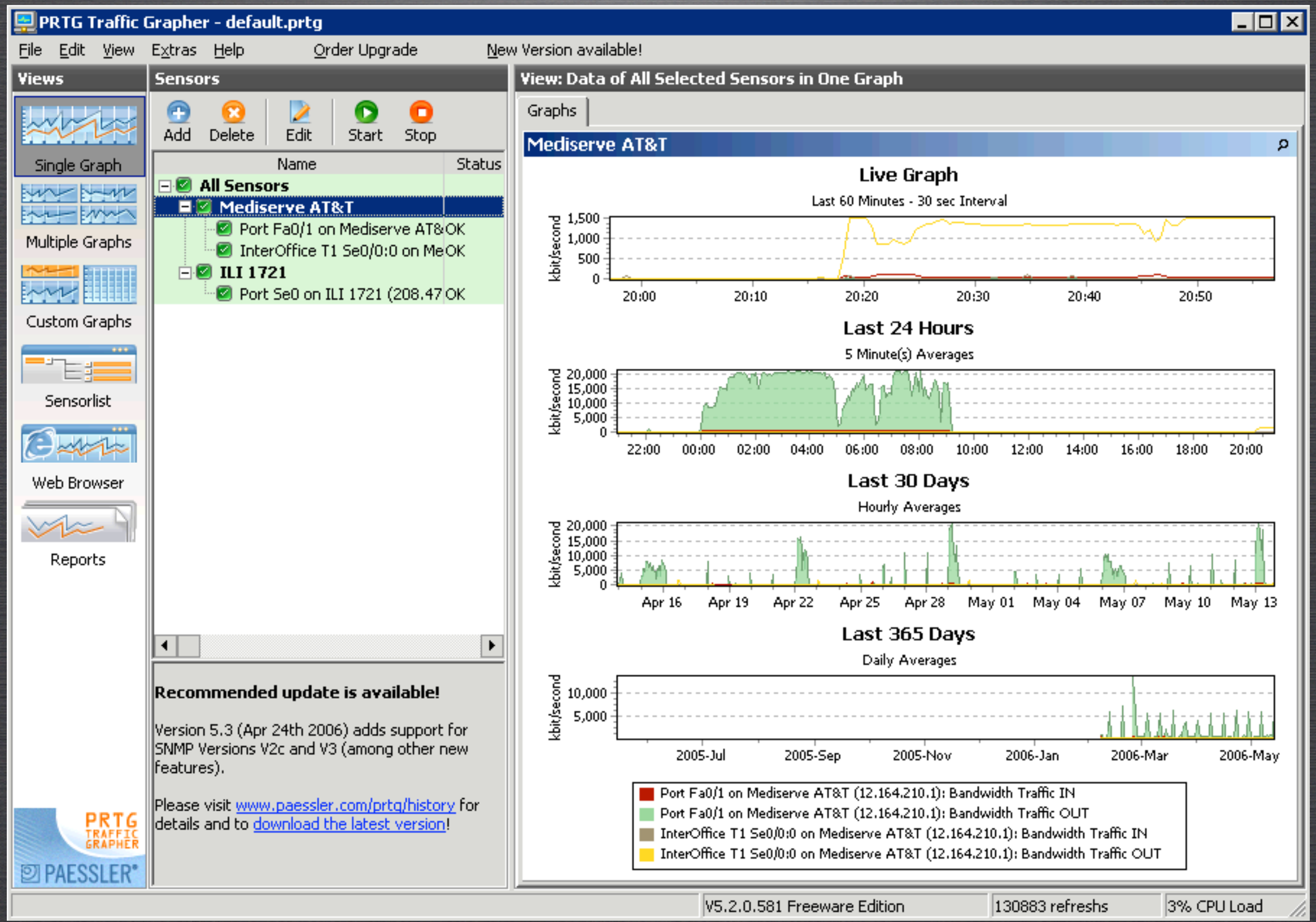
Example of configfile.txt -

```
no enable secret
enable secret newpassword
end
```

PRTG

- Freeware / Commercial MRTG-like product
  - Installs on Windows
  - Free version comes with 3 counters
  - Commercial version is relatively inexpensive
  - Automatically comes with MIB counters pre-configured for most Cisco devices
- Available at http://www.paessler.com/prtg

PRTG


PRTG Traffic Grapher - default.prtg
File Edit View Extras Help Order Upgrade New Version available!
Views
Single Graph
Multiple Graphs
Custom Graphs
Sensorlist
Web Browser
Reports
Sensors
Add Delete Edit Start Stop
Name Status
All Sensors
Mediserve AT&T
Port Fa0/1 on Mediserve AT& OK
InterOffice T1 Se0/0:0 on Me OK
ILI 1721
Port Se0 on ILI 1721 (208.47 OK
Recommended update is available!
Version 5.3 (Apr 24th 2006) adds support for SNMP Versions V2c and V3 (among other new features).
Please visit www.paessler.com/prtg/history for details and to download the latest version!
View: Data of All Selected Sensors in One Graph
Graphs
Mediserve AT&T
Live Graph
Last 60 Minutes - 30 sec Interval
kbit/second
1,500
1,000
500
0
20:00 20:10 20:20 20:30 20:40 20:50
Last 24 Hours
5 Minute(s) Averages
20,000
15,000
10,000
5,000
0
22:00 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00
Last 30 Days
Hourly Averages
Apr 16 Apr 19 Apr 22 Apr 25 Apr 28 May 01 May 04 May 07 May 10 May 13
Last 365 Days
Daily Averages
2005-Jul 2005-Sep 2005-Nov 2006-Jan 2006-Mar 2006-May
Port Fa0/1 on Mediserve AT&T (12.164.210.1): Bandwidth Traffic IN
Port Fa0/1 on Mediserve AT&T (12.164.210.1): Bandwidth Traffic OUT
InterOffice T1 Se0/0:0 on Mediserve AT&T (12.164.210.1): Bandwidth Traffic IN
InterOffice T1 Se0/0:0 on Mediserve AT&T (12.164.210.1): Bandwidth Traffic OUT
V5.2.0.581 Freeware Edition
130883 refreshs
3% CPU Load

Mesmerizing Utilities

- Get Pass
- Rip Generator
- Switch Inspector
- Kiwi Syslog / Cattools

Mesmerizing Utilities

Boson GetPass 1.1 - Crack level 7 encryption

http://www.AdTECNetworks.com/ciscoutils/get_pass.exe

```
line vty 0 4
 exec-timeout 60 0
 password 7 094F471A1A0A
 login local
 transport input all
```

Boson Rip Route Generator

http://www.AdTECNetworks.com/ciscoutils/rip_gen.exe

Mesmerizing Utilities

- Netxar SwitchInspector
  http://www.switchinspector.com/
- Allows you to identify the devices attached to each of the switch ports in your organization

Mesmerizing Utilities

Mesmerizing Utilities

Mesmerizing Utilities

Mesmerizing Utilities

SwitchInspector 1.3.1 (Not for Resale) - Netxar Technologies Inc.

SWITCH INSPECTOR
map your connected devices

Switch Port Mapping - Connected Devices

Main Menu

- Switch Information
- Switch Port Mapping
- Help
- Exit

Tasks

Switch Description
172.30.2.1

Determining SNMP Version
Done

Executing Ping Sweep
Done

Getting Switch Information
Done

Mapping Conn. Devices
Done

Looking Up Device Names
Done

Export Results

Switch Info Table | Switch Ports Table | Devices Table

MTU	Duplex Setting	Oper. Status	VLAN(s)	VLAN Description(s)	Num. Devices
1500	Full Duplex	●	400	EXIT	1
1500	Full Duplex	●	200	CLIENTS	1
1500	Auto Negotiate	●	200	CLIENTS	
1500	Full Duplex	●	300	WIRELESS	2
1500	Auto Negotiate	●	400	EXIT	
1500	Auto Negotiate	●	200	CLIENTS	
1500	Auto Negotiate	●	200	CLIENTS	
1500	Auto Negotiate	●			
1500	Auto Negotiate	●	300	WIRELESS	
1500	Full Duplex	●	600, 200	VOICE, CLIENTS	2
1500	Full Duplex	●	200	CLIENTS	2
1500	Auto Negotiate	●			
1500	Auto Negotiate	●	200	CLIENTS	
1500	Auto Negotiate	●	200	CLIENTS	
1500	Auto Negotiate	●	200	CLIENTS	
1500	Auto Negotiate	●	200	CLIENTS	
1500	Auto Negotiate	●			
1500	Auto Negotiate	●	500	DMZ	
1500	Full Duplex	●	100, 1	SERVERS, default	2
1500	Auto Negotiate	●	200	CLIENTS	
1500	Auto Negotiate	●	200	CLIENTS	
1500	Full Duplex	●	600, 200	VOICE, CLIENTS	4
1500	Undetermined	●	200	CLIENTS	1
1500	Undetermined	●	600, 200	VOICE, CLIENTS	2
1500	Auto Negotiate	●	1	default	
1500	Auto Negotiate	●	1	default	

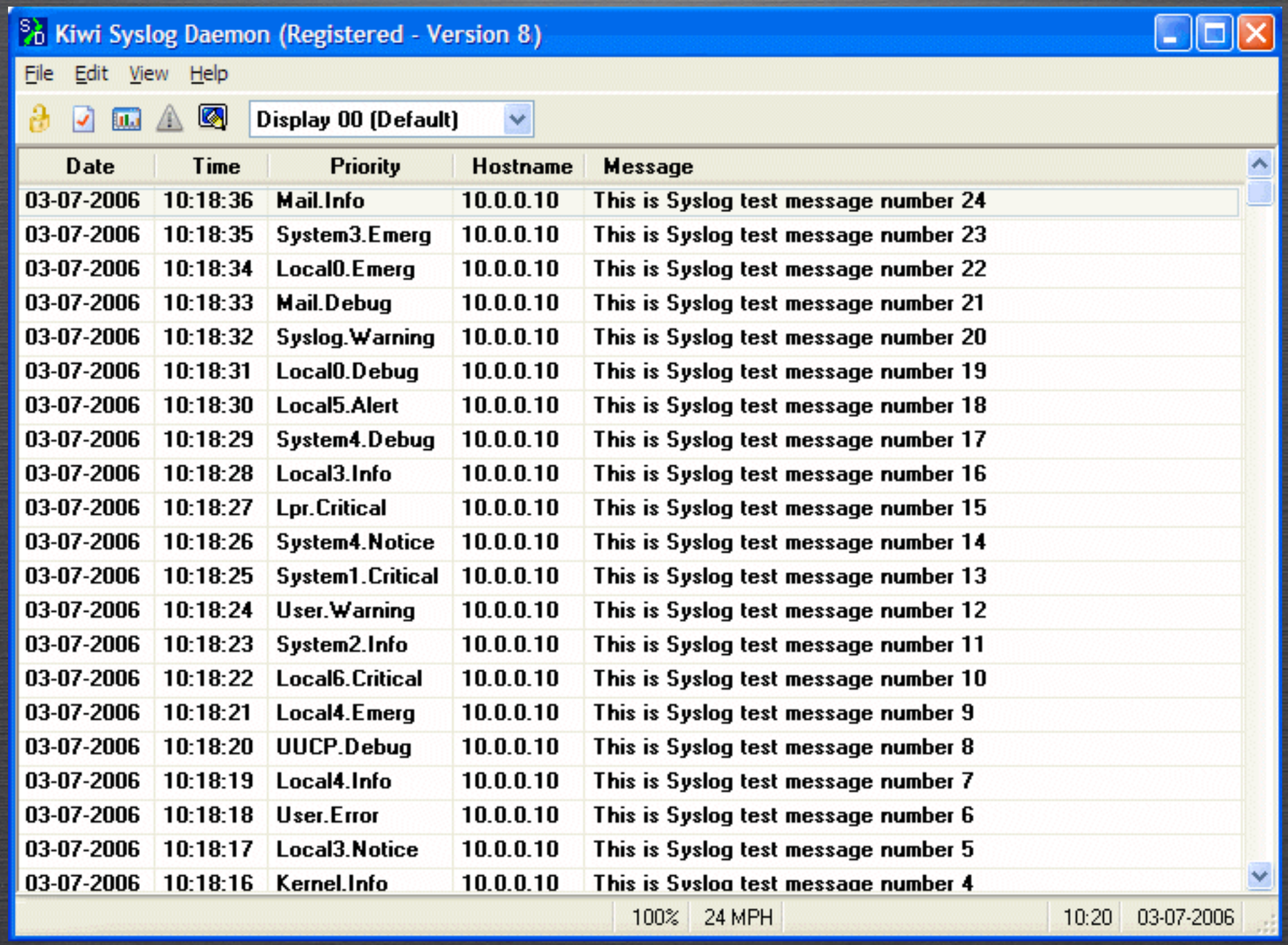
Mesmerizing Utilities

Mesmerizing Utilities

Mesmerizing Utilities

Kiwi Syslog

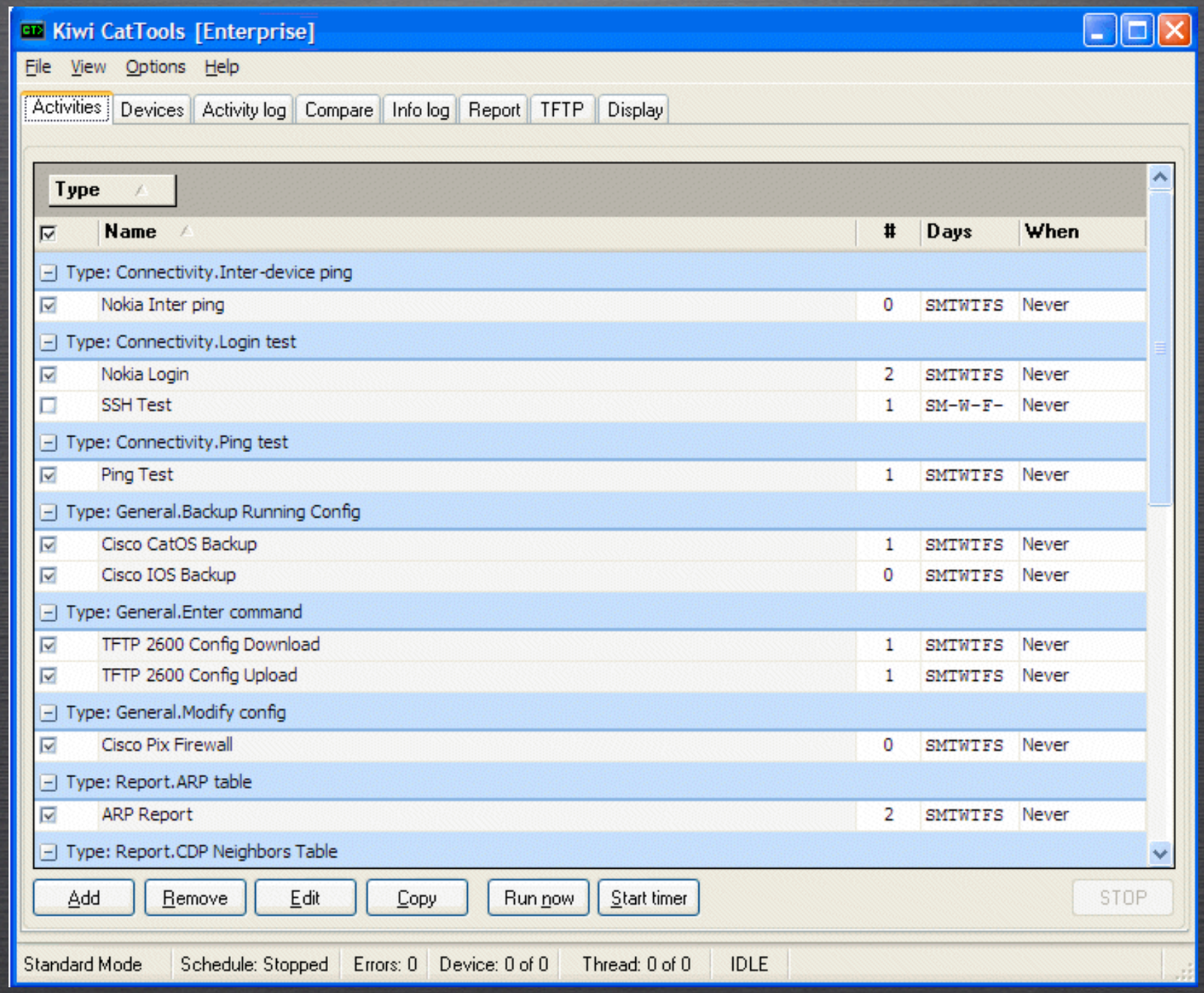
http://www.kiwisyslog.com



Mesmerizing Utilities

Kiwi Cattools - config dif, multi commands

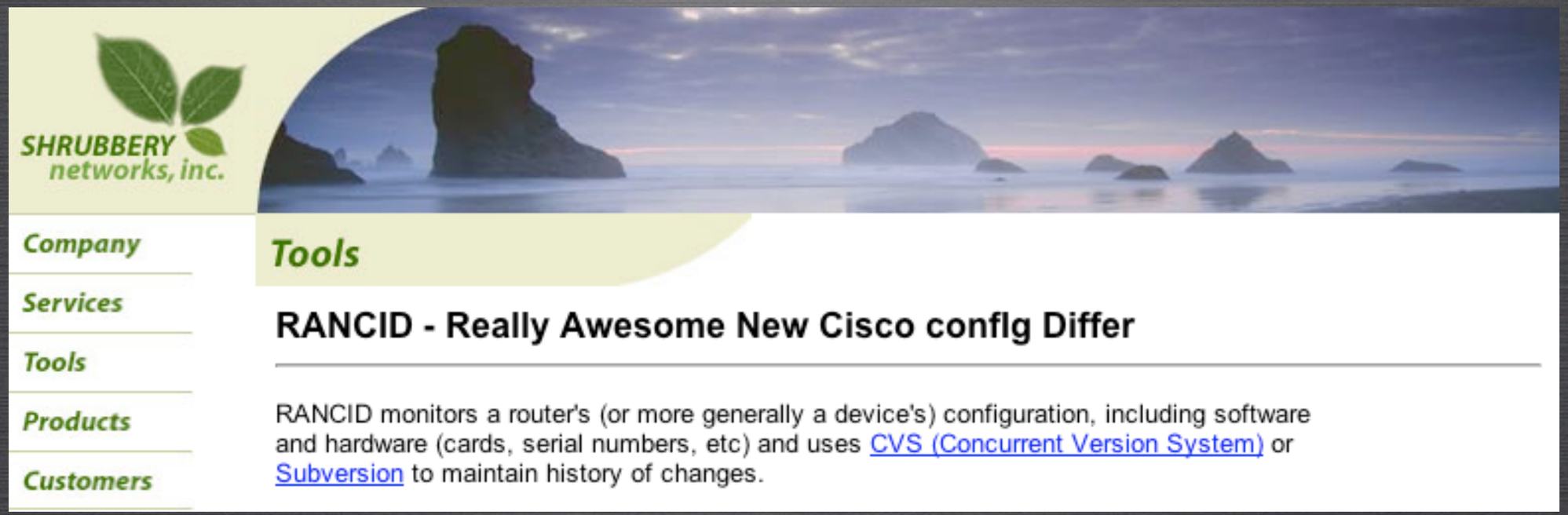
http://www.kiwisyslog.com



Mesmerizing Utilities

Really Awesome New Cisco confIg Differ (rancid)

http://www.shrubbery.net/rancid/#started



Simalr to CatTools, but completely free

Questions?

Check out:
http://www.ciscoblog.com