

# 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

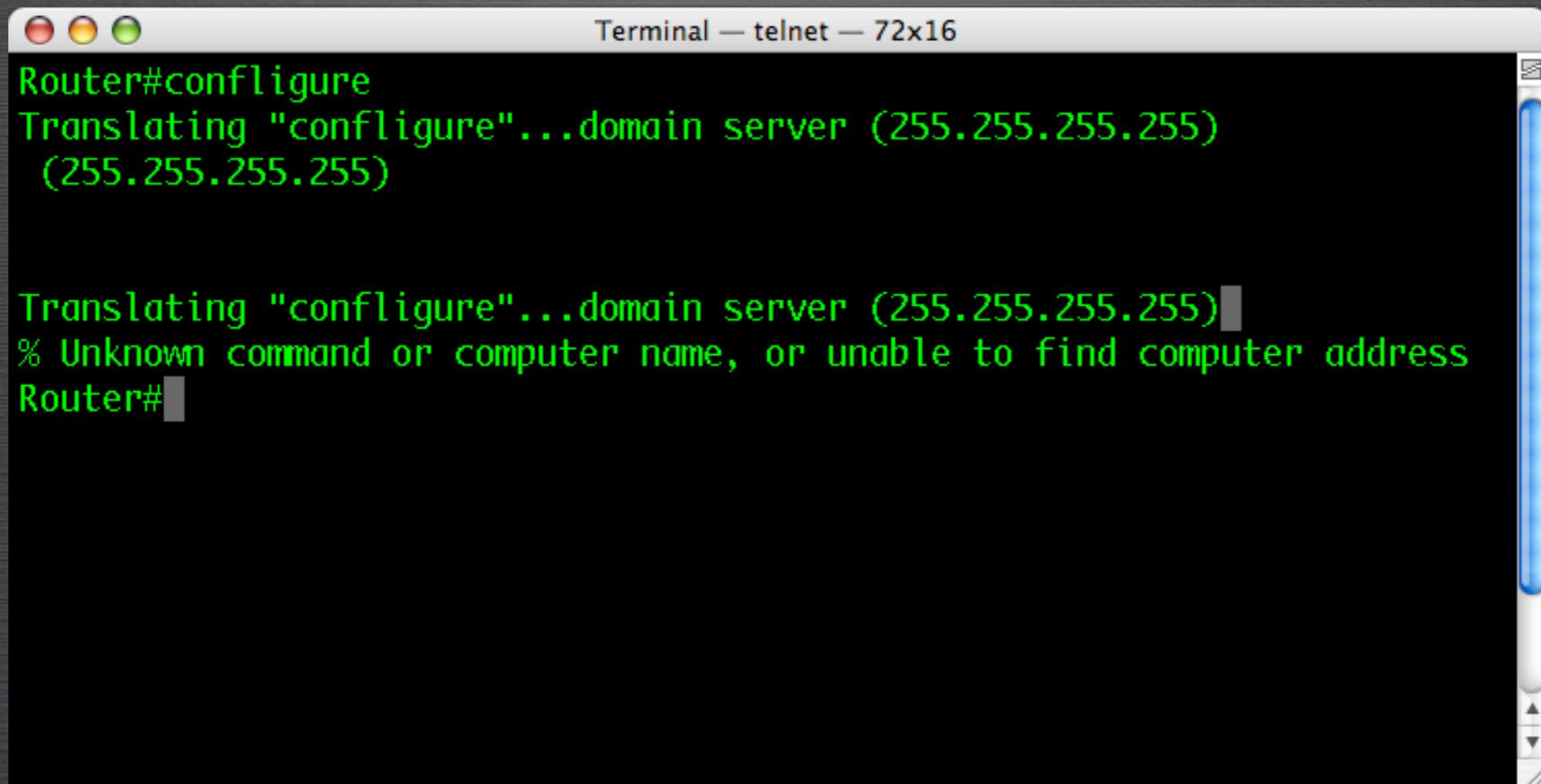
MESMERIZING UTILITIES

# 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

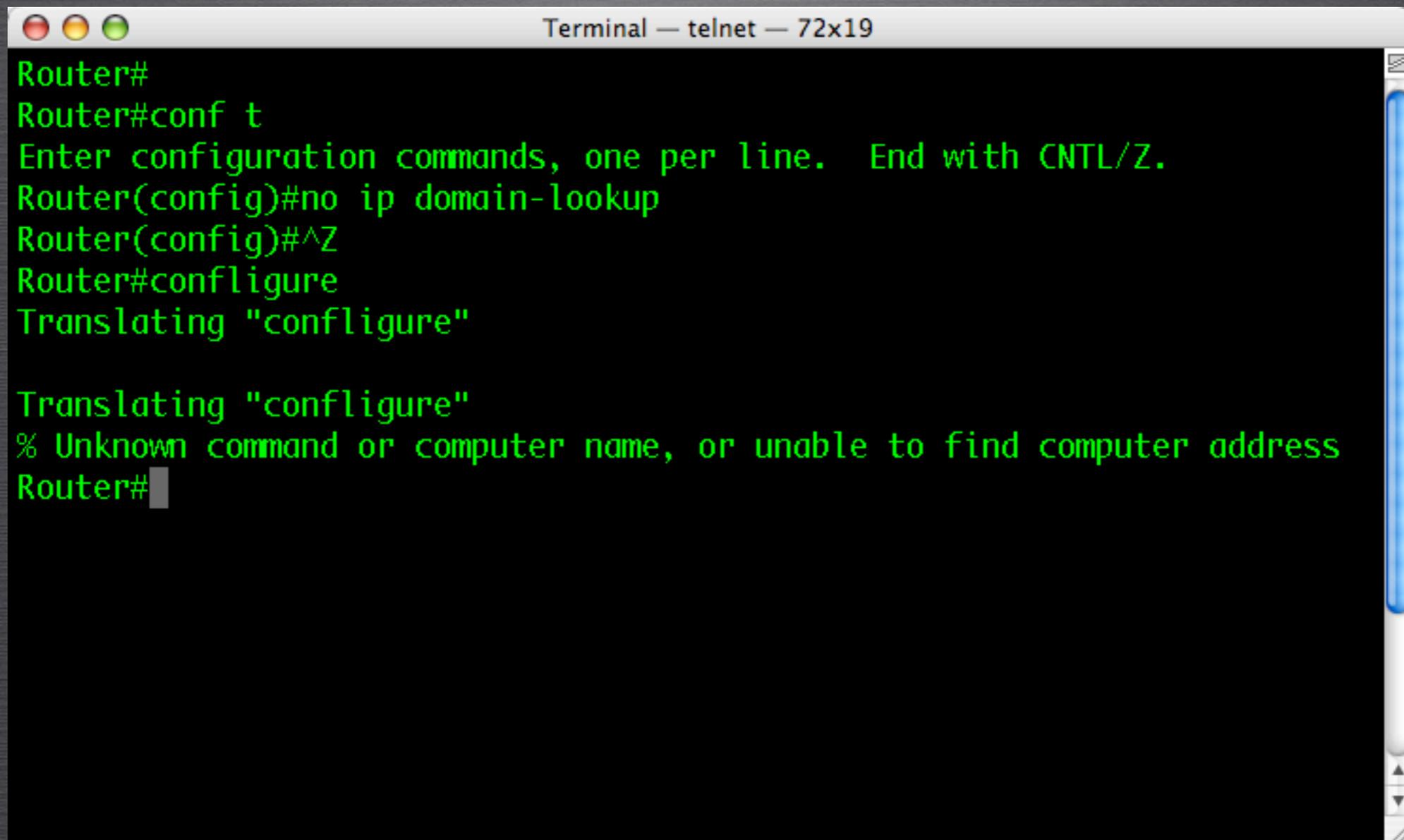


```
Terminal — telnet — 72x16
Router#configure
Translating "configure"...domain server (255.255.255.255)
(255.255.255.255)

Translating "configure"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
Router#
```

# DISABLING DNS LOOKUP (CONT.)

- THE SOLUTION: DISABLE DNS LOOKUPS

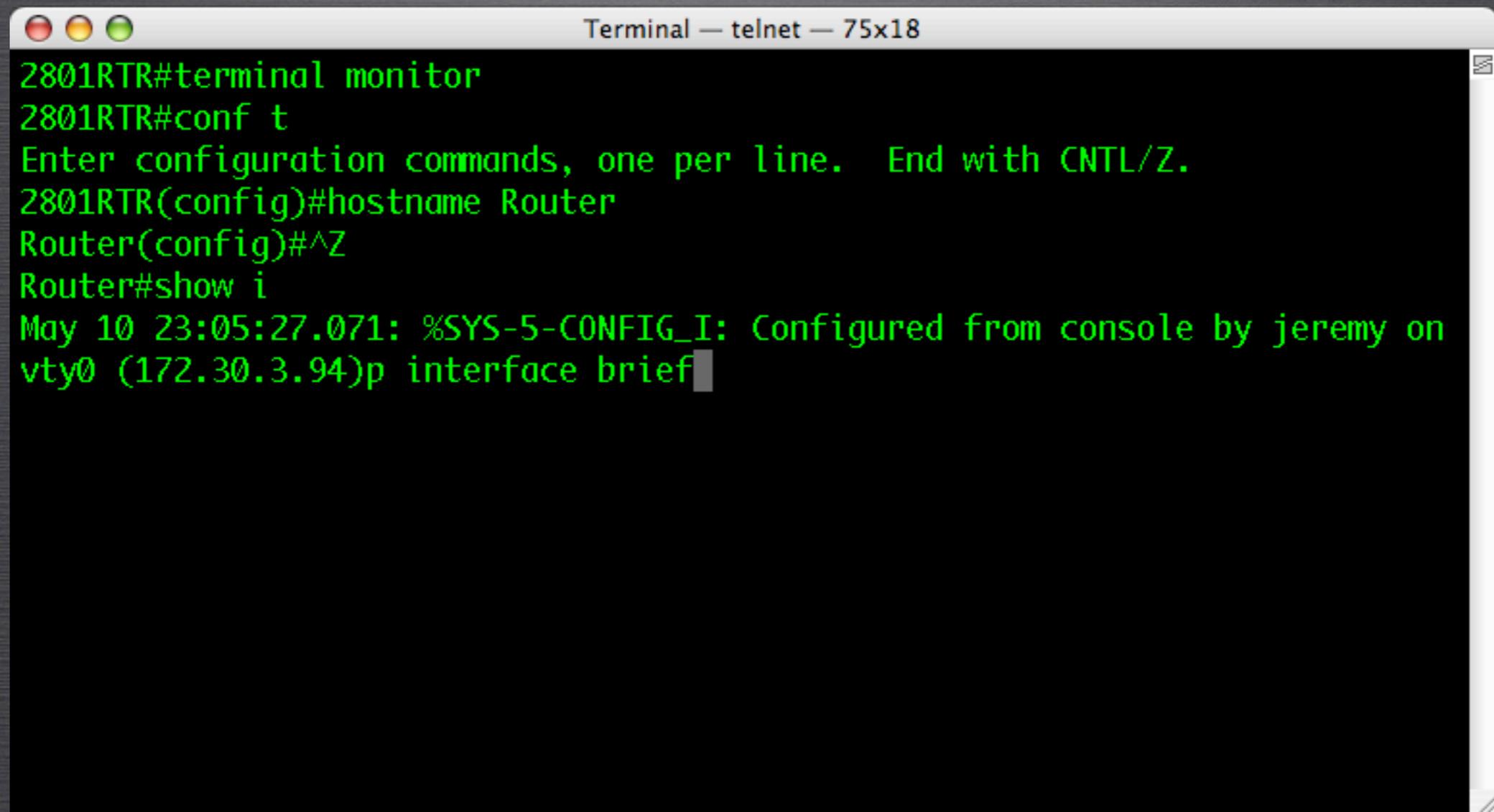


```
Terminal — telnet — 72x19
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#^Z
Router#configure
Translating "configure"

Translating "configure"
% Unknown command or computer name, or unable to find computer address
Router#
```

# LIMITING EXEC INTERRUPTIONS

- BY DEFAULT, CISCO DEVICES ALLOW CONSOLE AND LINE MESSAGES TO INTERRUPT TYPED TEXT



```
Terminal — telnet — 75x18
2801RTR#terminal monitor
2801RTR#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2801RTR(config)#hostname Router
Router(config)#^Z
Router#show i
May 10 23:05:27.071: %SYS-5-CONFIG_I: Configured from console by jeremy on
vty0 (172.30.3.94)p interface brief
```

# LIMITING EXEC INTERRUPTIONS

- TO PREVENT THIS FEATURE, DO THE FOLLOWING:

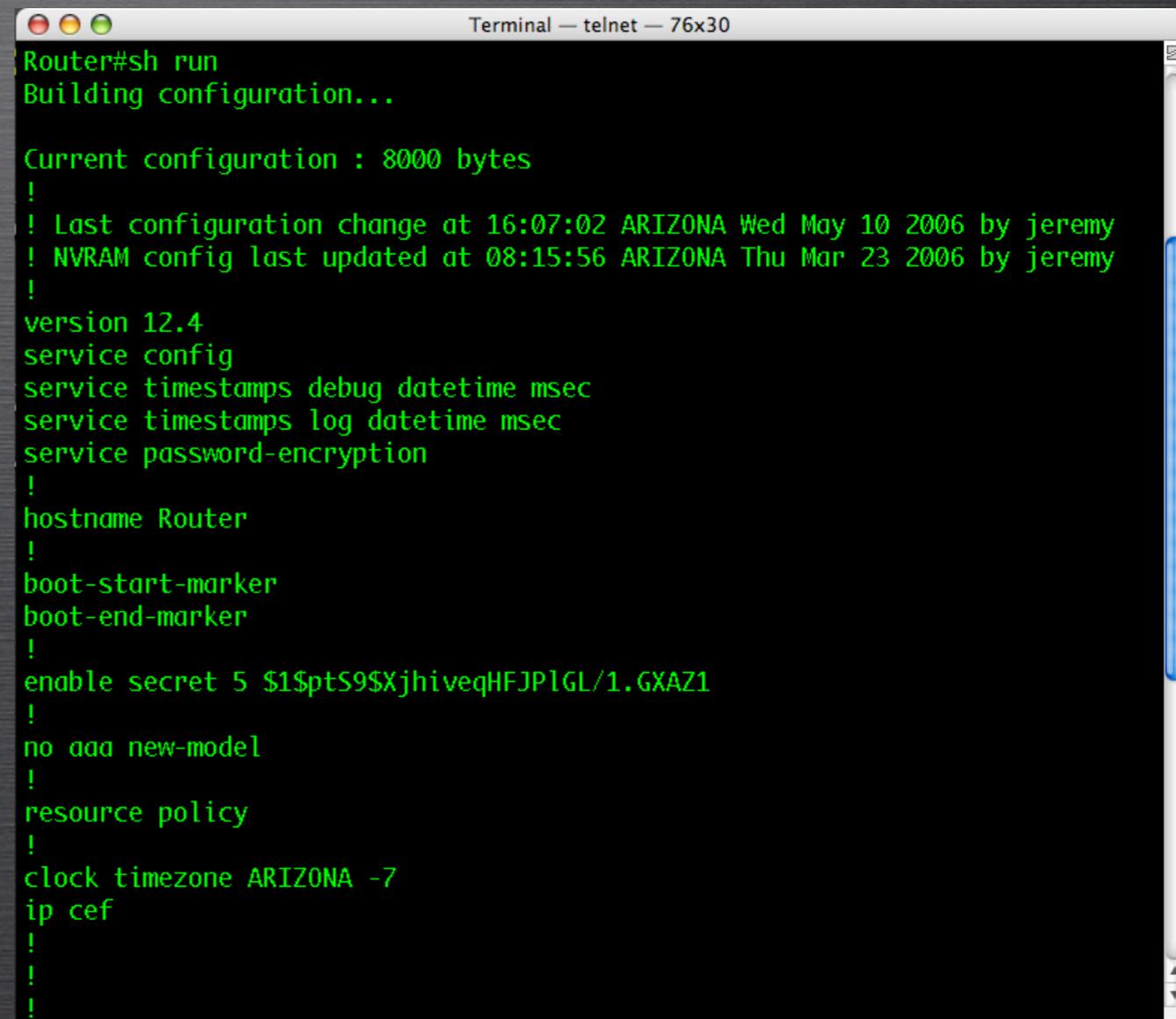
THE LINE IS  
AUTOMATICALLY  
REPAINTED



```
Terminal — telnet — 75x18
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line con 0
Router(config-line)#logging synchronous
Router(config-line)#line vty 0 4
Router(config-line)#logging synchronous
Router(config-line)#^Z
Router#show ip i
May 10 23:07:02.137: %SYS-5-CONFIG_I: Configured from console by jeremy on
vty0 (172.30.3.94)
Router#show ip interface brief
```

# FILTERING COMMAND OUTPUT

- MANY COMMANDS OUTPUT EXCESSIVE INFORMATION TO THE SCREEN.
- UNIX-LIKE FILTERING OPTIONS CAN AID IN DEVICE MANAGEMENT

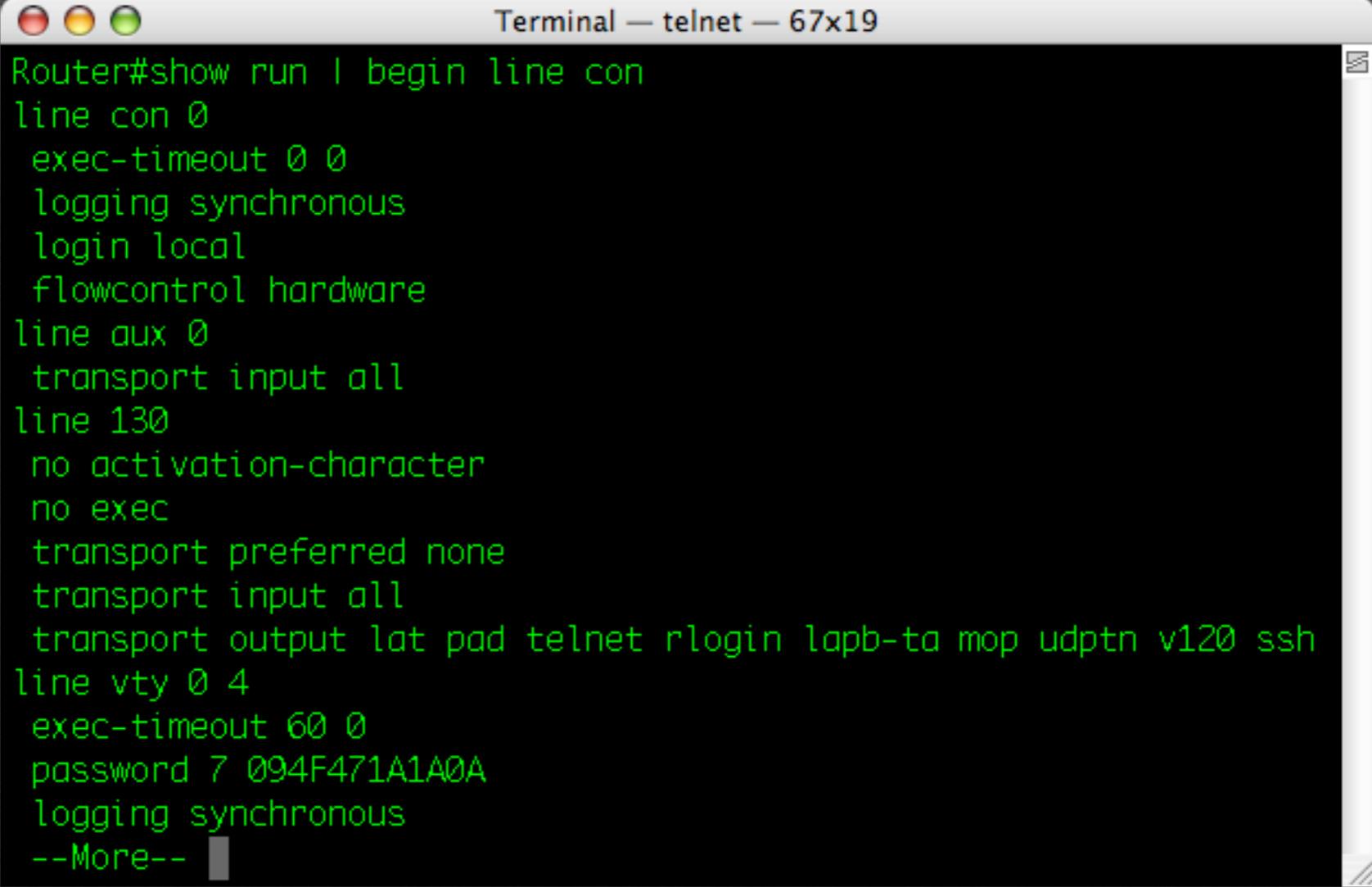
A terminal window titled "Terminal - telnet - 76x30" displays the output of the "sh run" command on a Cisco Router. The output shows the current configuration in a structured format with exclamation marks as delimiters. The configuration includes version 12.4, service timestamps, hostname Router, boot markers, enable secret, no aaa new-model, resource policy, and clock timezone ARIZONA -7.

```
Router#sh run
Building configuration...

Current configuration : 8000 bytes
!
! Last configuration change at 16:07:02 ARIZONA Wed May 10 2006 by jeremy
! NVRAM config last updated at 08:15:56 ARIZONA Thu Mar 23 2006 by jeremy
!
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 $1$ptS9$XjhiveqHFJPlGL/1.GXAZ1
!
no aaa new-model
!
resource policy
!
clock timezone ARIZONA -7
ip cef
!
!
```

# FILTERING COMMAND OUTPUT

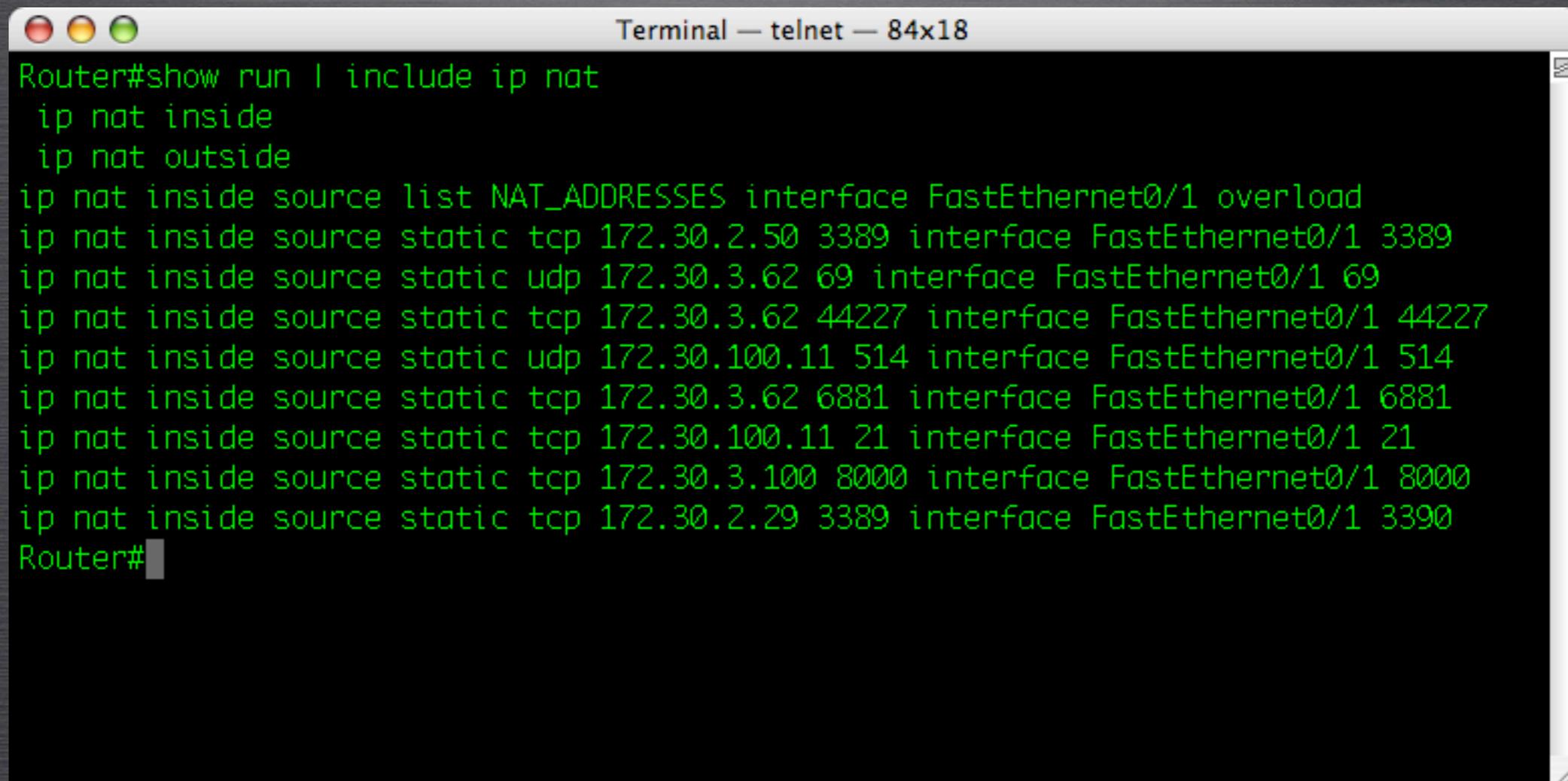
- `ROUTER# SHOW <ARGUMENT> | BEGIN <ARGUMENT>`



```
Terminal — telnet — 67x19
Router#show run | begin line con
line con 0
  exec-timeout 0 0
  logging synchronous
  login local
  flowcontrol hardware
line aux 0
  transport input all
line 130
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
  exec-timeout 60 0
  password 7 094F471A1A0A
  logging synchronous
--More--
```

# FILTERING COMMAND OUTPUT

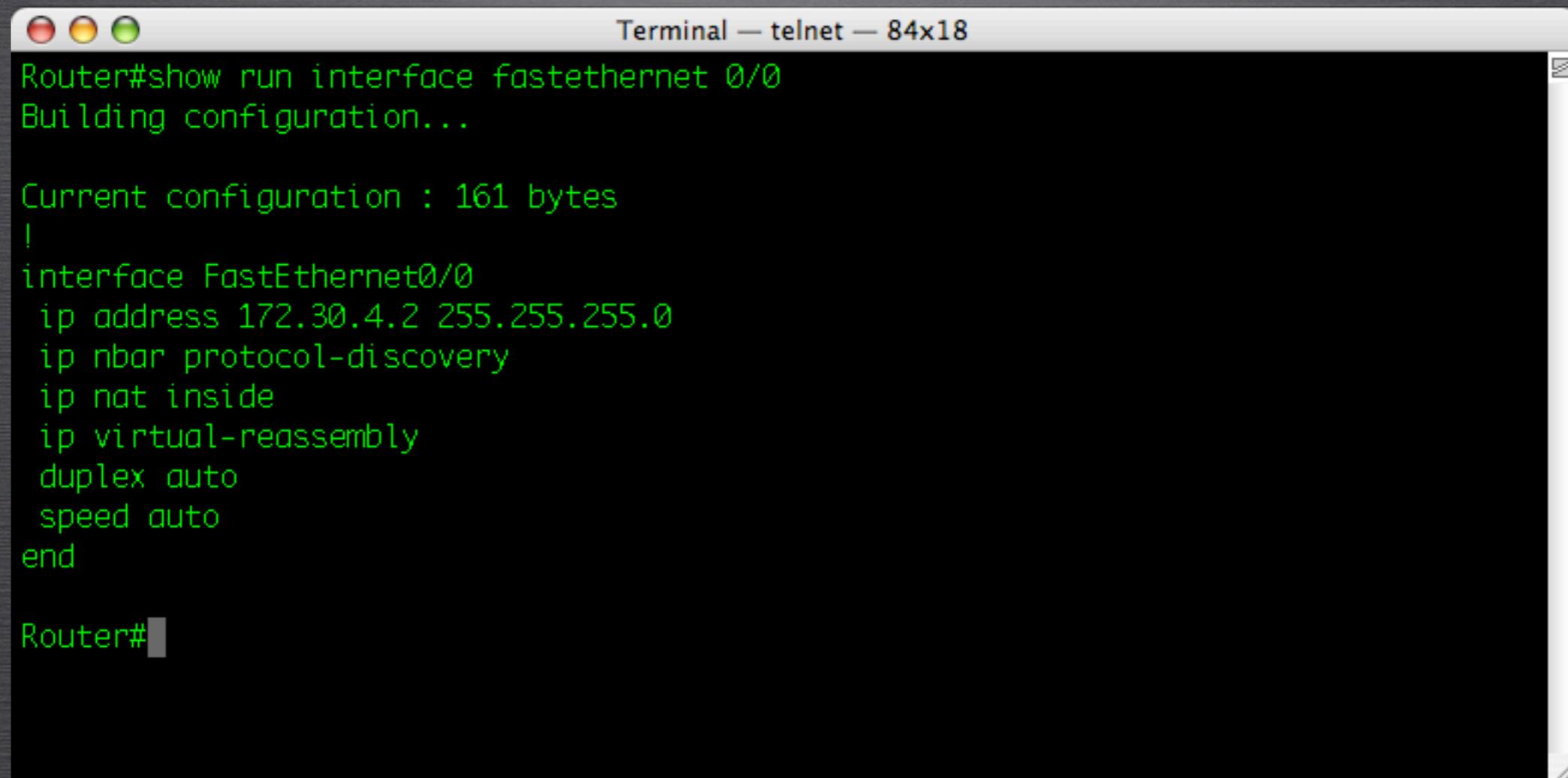
- `ROUTER# SHOW <ARGUMENT> | INCLUDE <ARGUMENT>`



```
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%

```
Terminal — telnet — 84x18
Router#show processes cpu | exclude 0.00%__0.00%__0.00%
CPU utilization for five seconds: 1%/0%; one minute: 1%; five minutes: 1%
PID Runtime(ms)   Invoked    uSecs   5Sec   1Min   5Min  TTY Process
  2      12224    1191504      10   0.00%  0.03%  0.02%  0 Load Meter
  5     4867544    708536     6869   0.00%  0.10%  0.06%  0 Check heaps
 11     7740424   29023724     266   0.32%  0.13%  0.10%  0 ARP Input
 35      25124    5957610      4   0.00%  0.03%  0.02%  0 Per-Second Jobs
 65     3168200    7877798     402   0.08%  0.05%  0.05%  0 IP Input
 75       4772   23271725      0   0.08%  0.01%  0.00%  0 SSS Feature Time
 91       5428    7680116      0   0.00%  0.01%  0.00%  0 CEF process
 99      15756   11908684      1   0.08%  0.05%  0.06%  0 DHCPD Receive
120       9232   59414506      0   0.08%  0.04%  0.06%  0 RBSCP Background
138     138752   3858425      35   0.00%  0.01%  0.00%  0 IP-EIGRP: HELLO
222    1988020    100647    19752   0.00%  0.04%  0.00%  0 Per-minute Jobs
241      10060     23154     434   0.16%  0.05%  0.23% 194 Virtual Exec
245    2211196   37765061      58   0.08%  0.14%  0.15%  0 Skinny Msg Serve
246       2028    6039048      0   0.08%  0.00%  0.00%  0 NTP
Router#
```

# 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

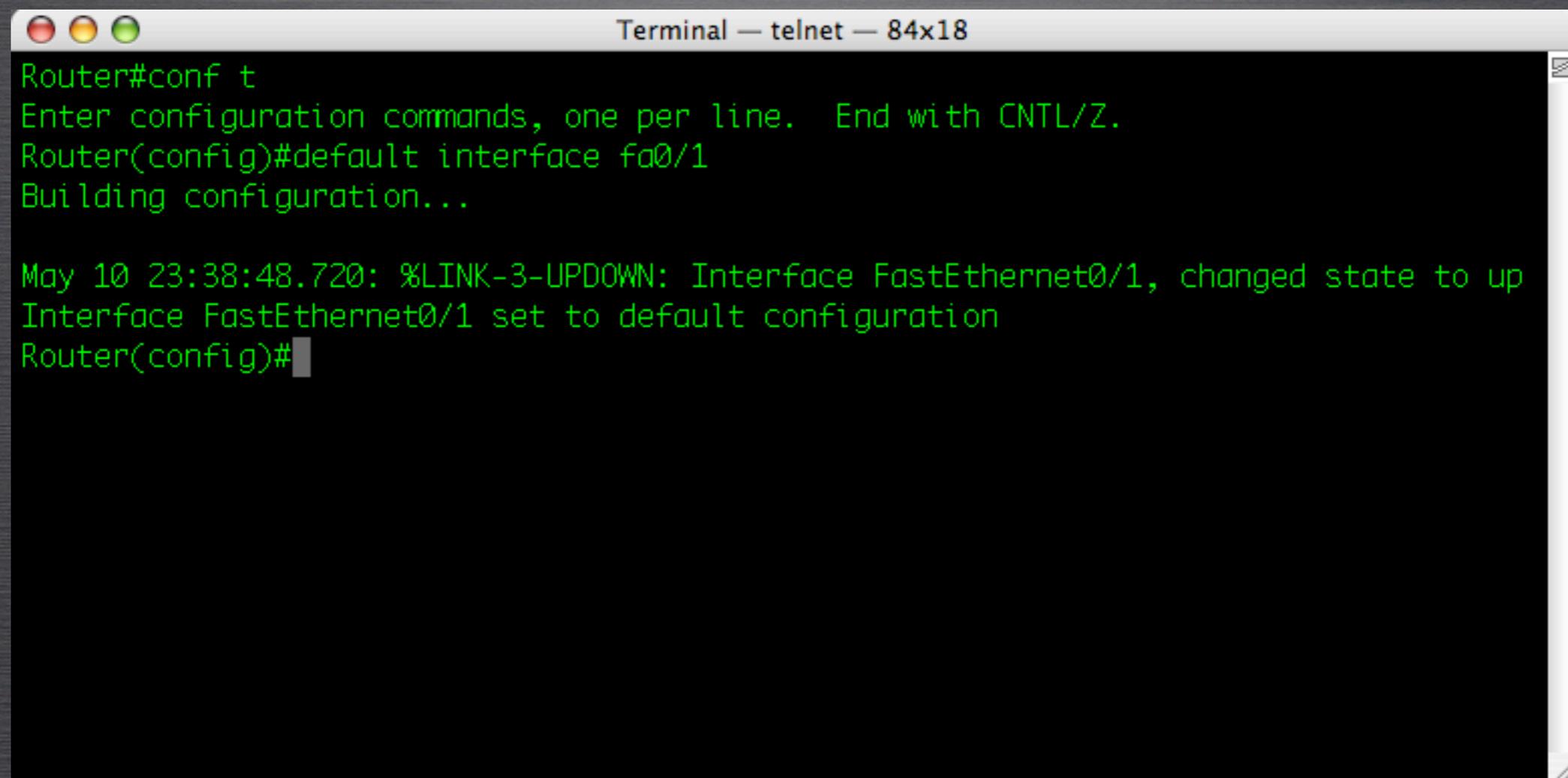
## ○ VERIFYING YOUR ALIASES

```
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>**



```
Terminal — telnet — 84x18
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#default interface fa0/1
Building configuration...

May 10 23:38:48.720: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
Interface FastEthernet0/1 set to default configuration
Router(config)#
```

# THE WONDERFUL 'DO' COMMAND

- ALLOWS YOU TO EXECUTE PRIVILEGED MODE COMMANDS FROM ANY MODE
- IOS 12.2(8)T VERSIONS AND LATER

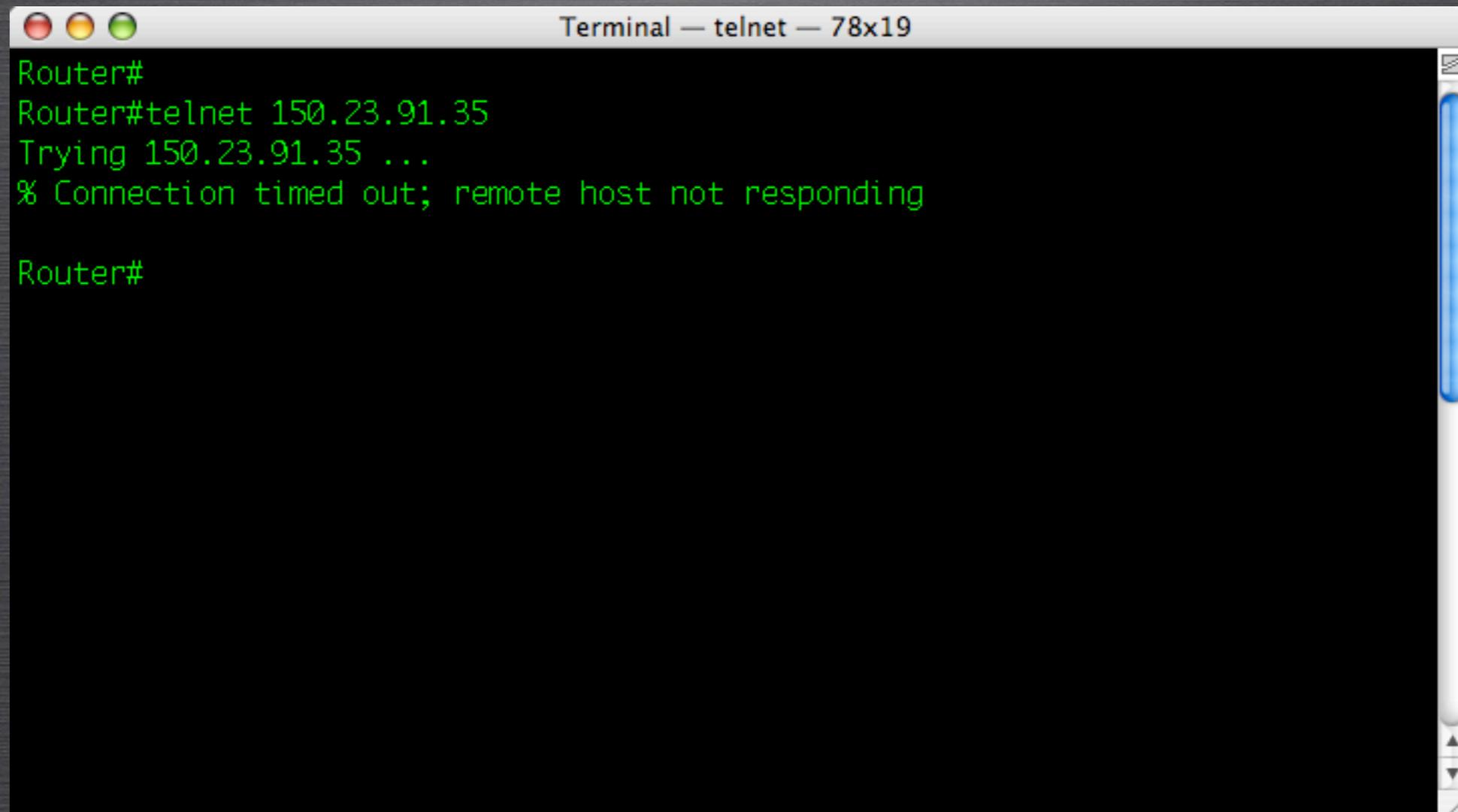


```
Terminal — telnet — 81x19
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#do show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID           Local Intrfce   Holdtme    Capability  Platform  Port ID
CAT_3550            Fas 0/0         160        R S I       WS-C3550- Fas 0/1
Router(config)#
```

# 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

A screenshot of a terminal window titled "Terminal — telnet — 78x19". The terminal shows a sequence of commands and responses from a router. The text is as follows:

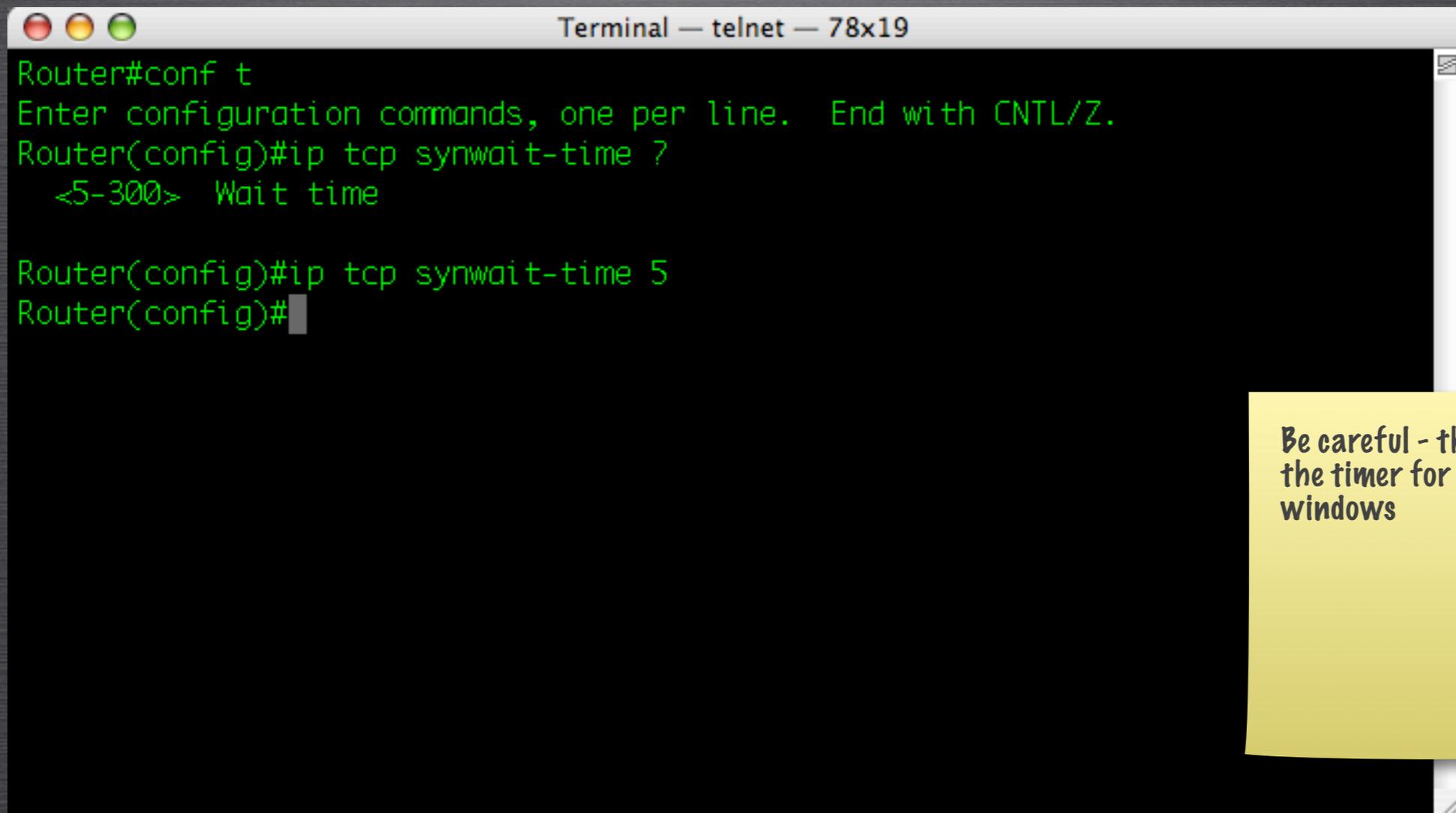
```
Router#  
Router#telnet 150.23.91.35  
Trying 150.23.91.35 ...  
% Connection timed out; remote host not responding  
  
Router#
```

The terminal window has a standard macOS-style title bar with three colored buttons (red, yellow, green) on the left and a scroll bar on the right. The text is displayed in a green monospaced font on a black background.

# SHRINKING THE TCP TIMEOUT

- TO ADJUST THIS TIMER, USE THE FOLLOWING COMMAND:

ROUTER(CONFIG)# IP TCP SYNWAIT-TIME <5-300 SECONDS>



```
Terminal — telnet — 78x19
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip tcp synwait-time ?
    <5-300>  Wait time

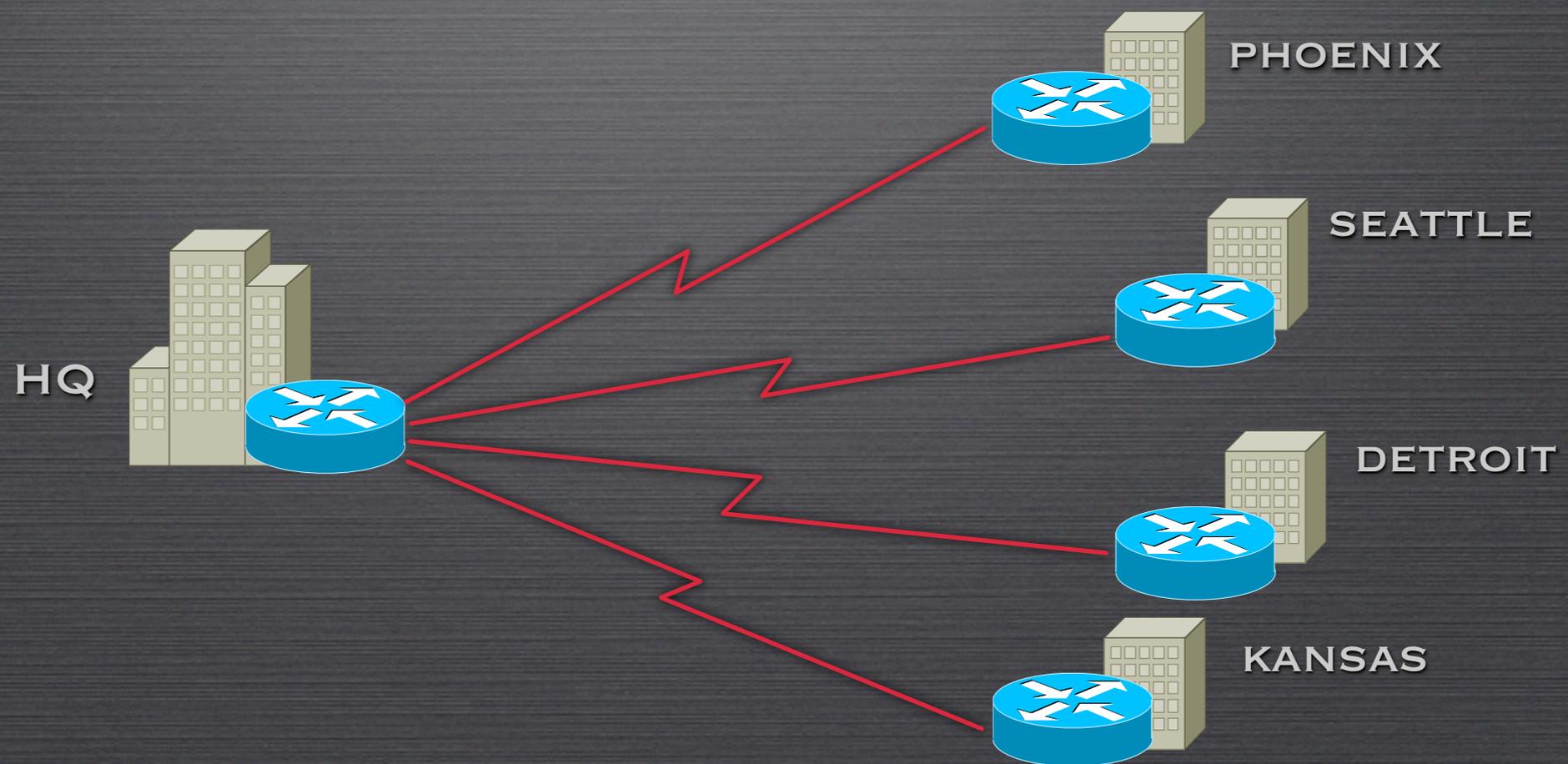
Router(config)#ip tcp synwait-time 5
Router(config)#
```

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



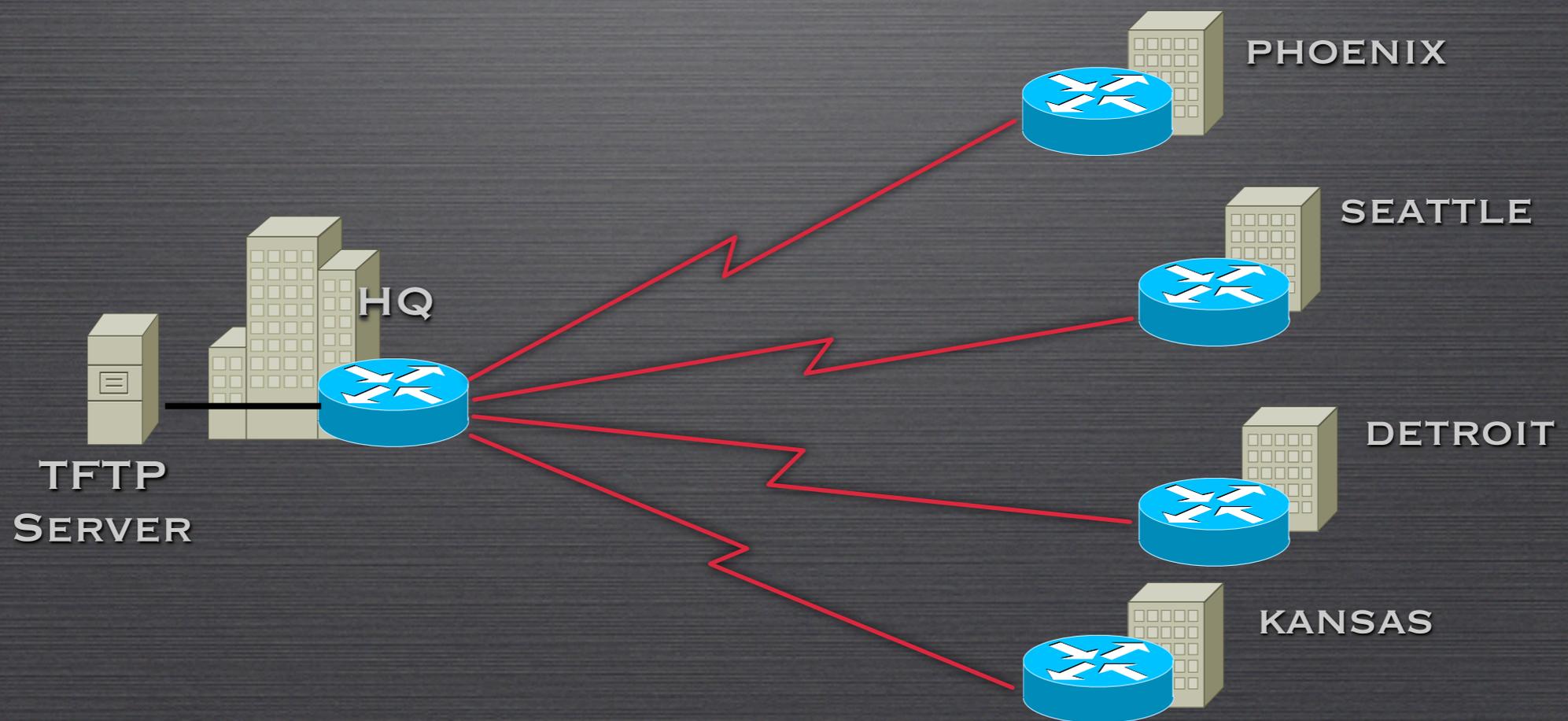
# REMOTE ROUTER AUTO-CONFIGURATION

## 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

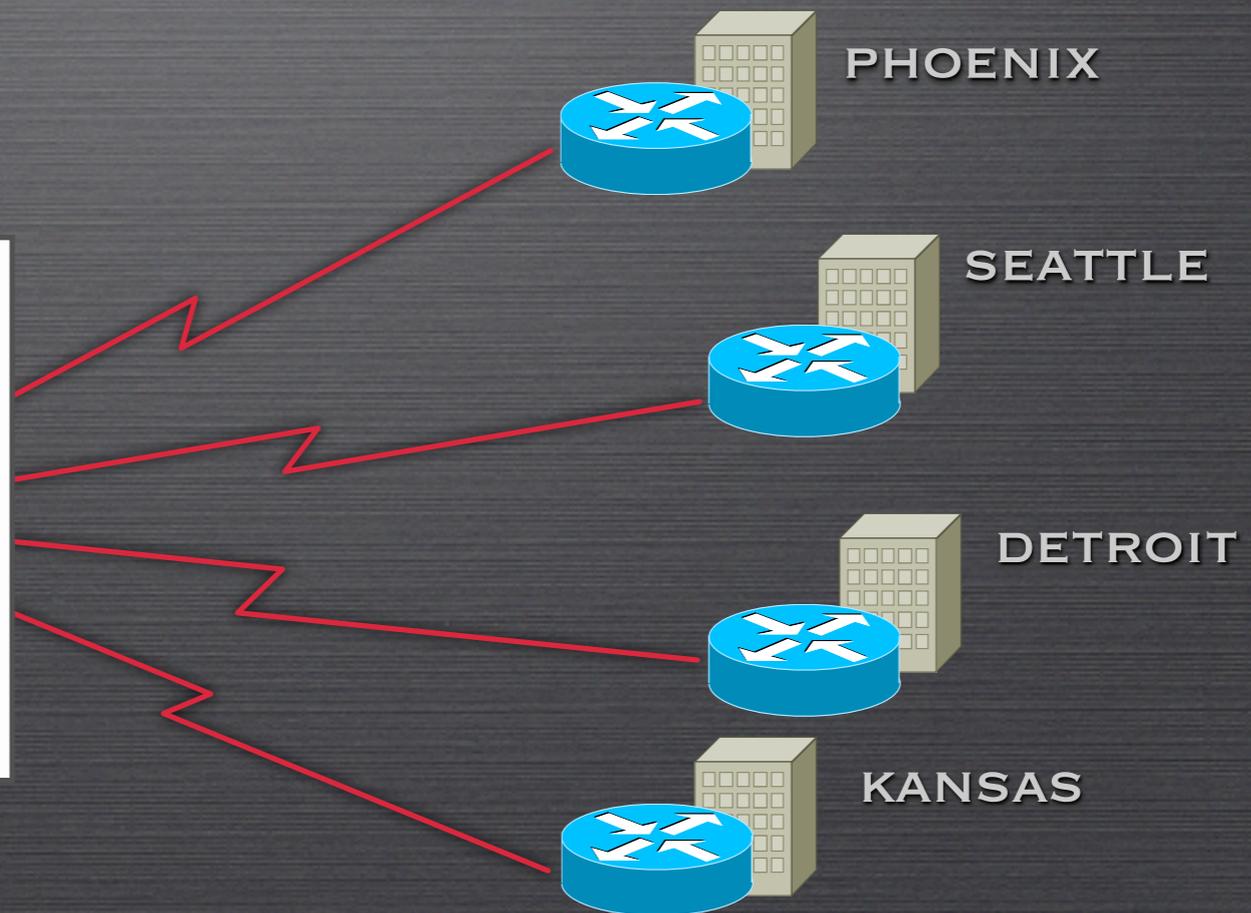


# REMOTE ROUTER AUTO-CONFIGURATION

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
```

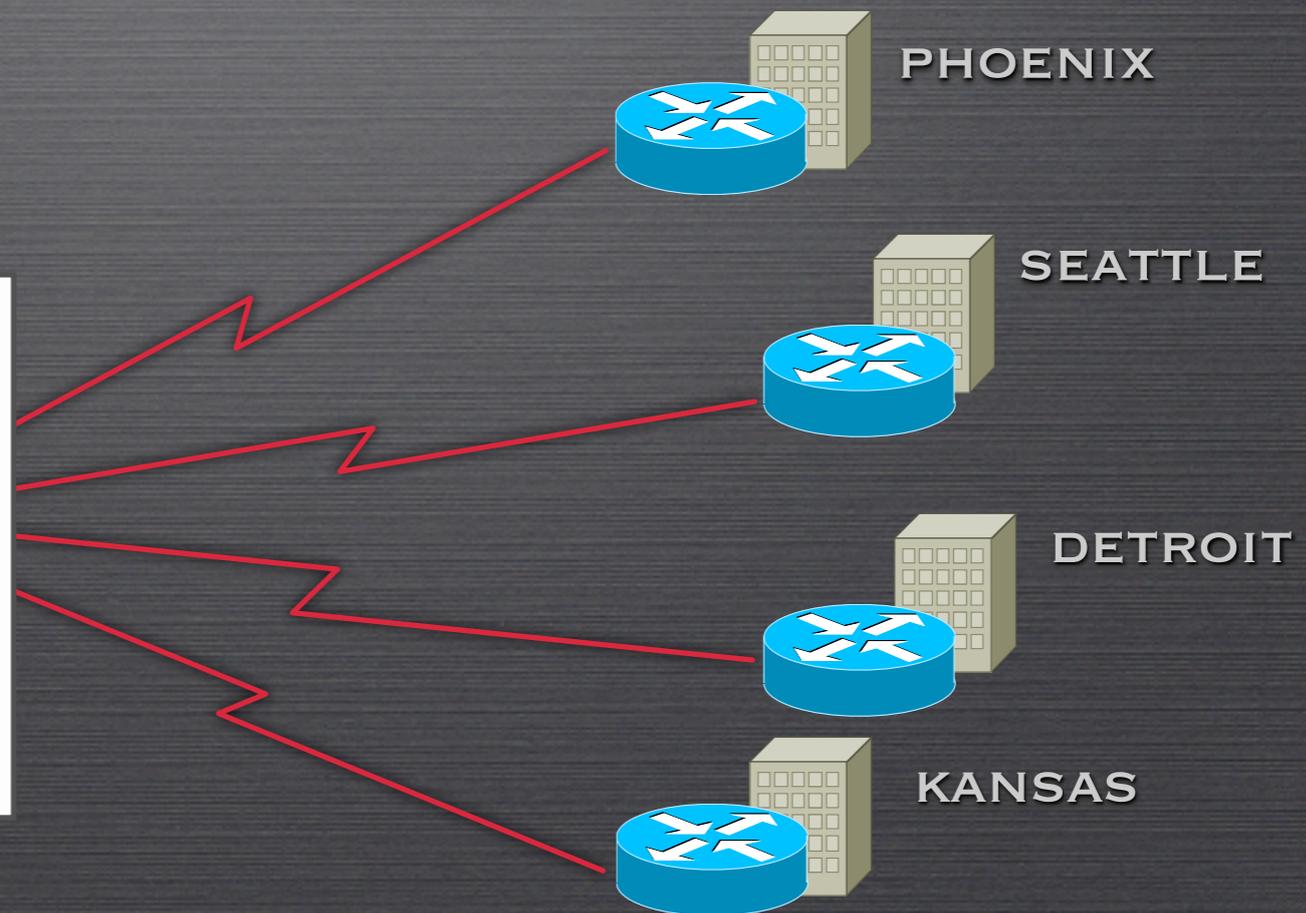


# REMOTE ROUTER AUTO-CONFIGURATION

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 $1$pt9$9$XjhiwagHFJPIGL/1.GX2Z1
!
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)

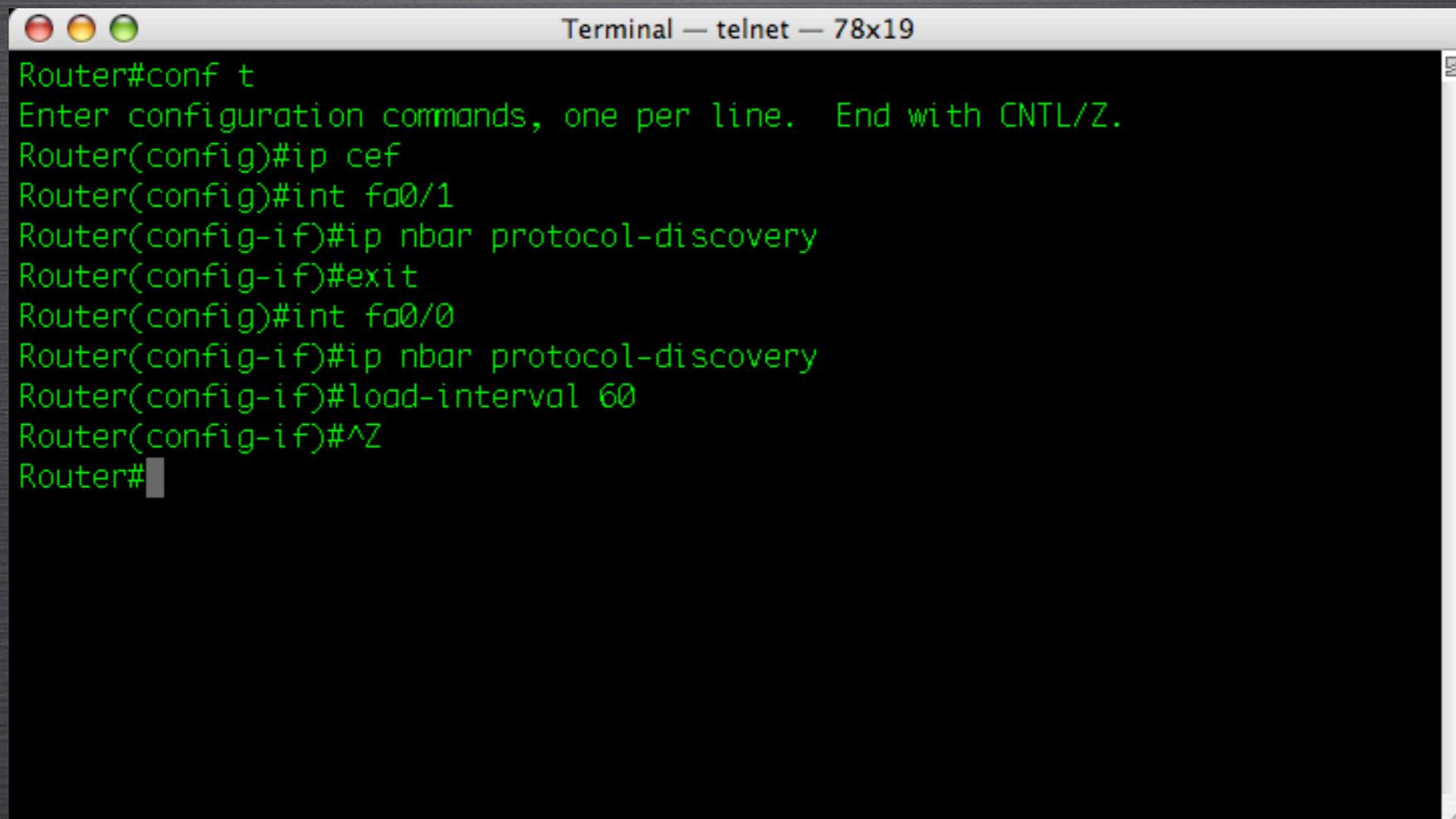
  - PAESSLER-ROUTER TRAFFIC GRAPHER (PRTG)

# 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)

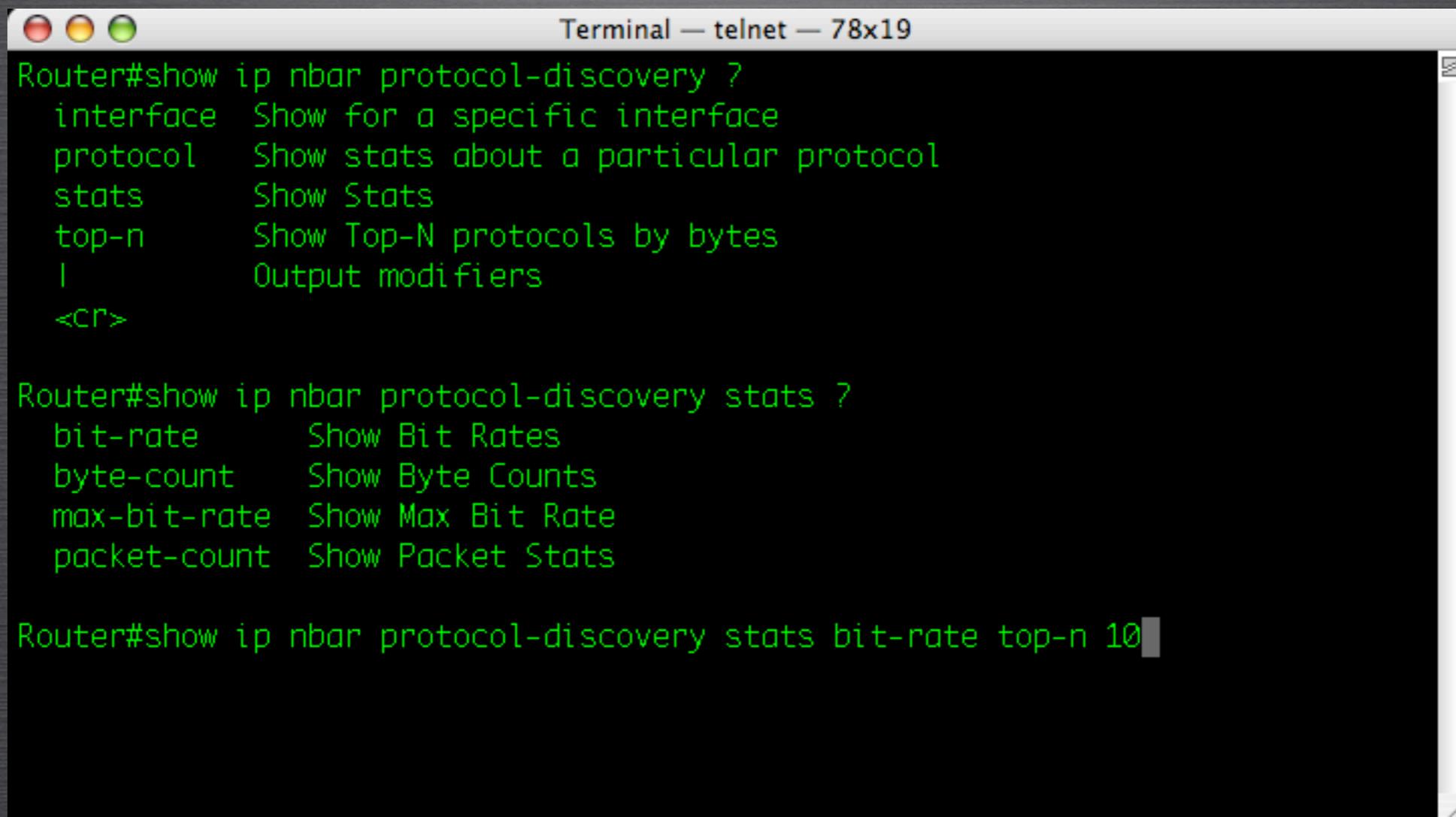
- ENABLING NBAR
  - REQUIRES CISCO EXPRESS FORWARDING (CEF)
  - ACTIVATED ON A PER-INTERFACE BASIS

A terminal window titled "Terminal — telnet — 78x19" with a standard macOS-style title bar (red, yellow, green buttons). The terminal displays the following configuration commands in green text on a black background:

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip cef
Router(config)#int fa0/1
Router(config-if)#ip nbar protocol-discovery
Router(config-if)#exit
Router(config)#int fa0/0
Router(config-if)#ip nbar protocol-discovery
Router(config-if)#load-interval 60
Router(config-if)#^Z
Router#
```

# NETWORK-BASED APPLICATION RECOGNITION (NBAR)

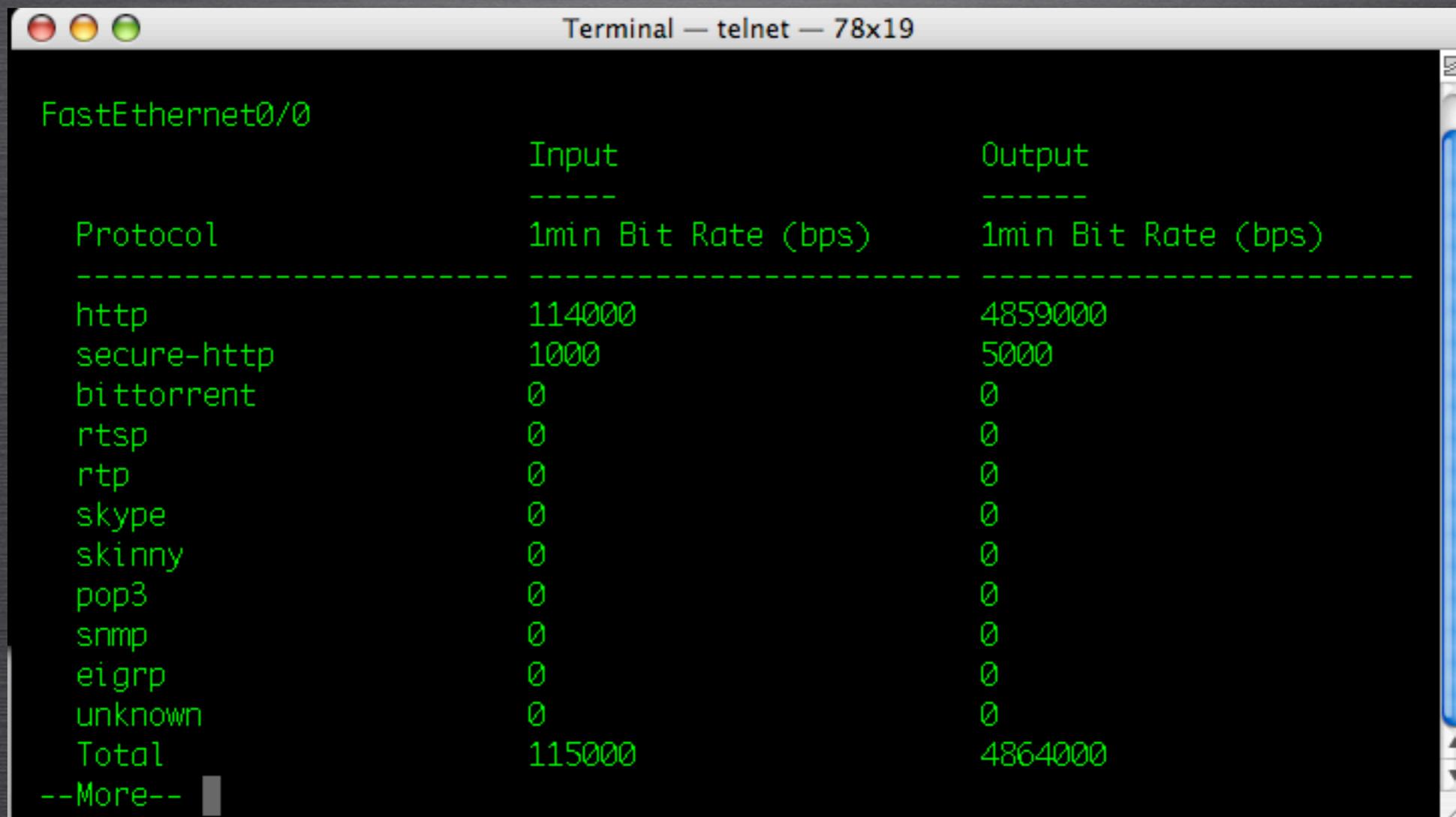
## ○ MONITORING NBAR - MANY OPTIONS

A terminal window titled "Terminal — telnet — 78x19" with a standard macOS-style title bar (red, yellow, green buttons). The terminal displays the following text in green on a black background:

```
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



Terminal — telnet — 78x19

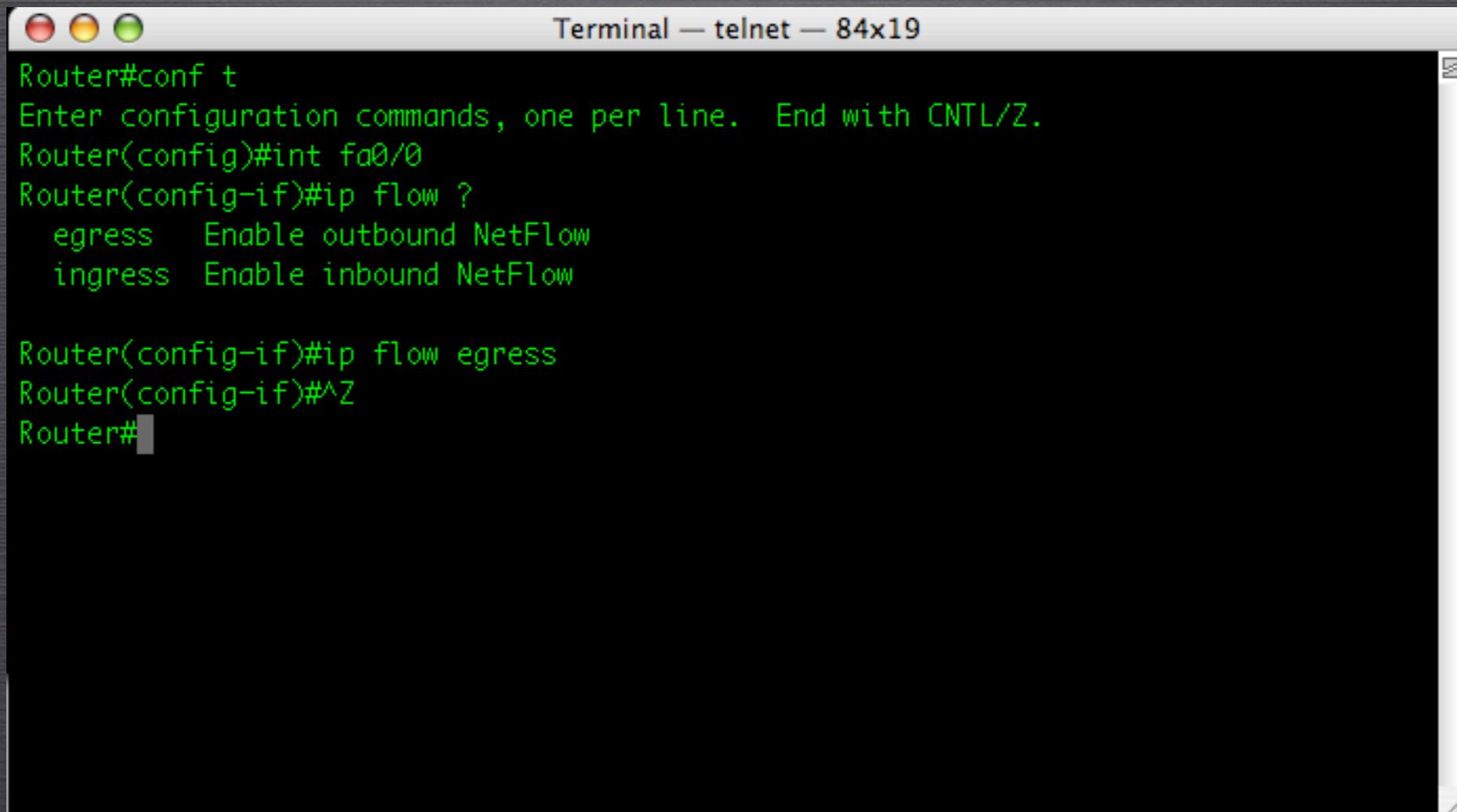
FastEthernet0/0

Protocol	Input ----- 1min Bit Rate (bps)	Output ----- 1min Bit Rate (bps)
http	114000	4859000
secure-http	1000	5000
bittorrent	0	0
rtsp	0	0
rtp	0	0
skype	0	0
skinny	0	0
pop3	0	0
snmp	0	0
eigrp	0	0
unknown	0	0
Total	115000	4864000

--More--

# 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

A terminal window titled "Terminal — telnet — 84x19" with a standard macOS-style title bar (red, yellow, green buttons). The terminal text is as follows:

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip flow ?
    egress  Enable outbound NetFlow
    ingress Enable inbound NetFlow

Router(config-if)#ip flow egress
Router(config-if)#^Z
Router#
```

# 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 age 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 age 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

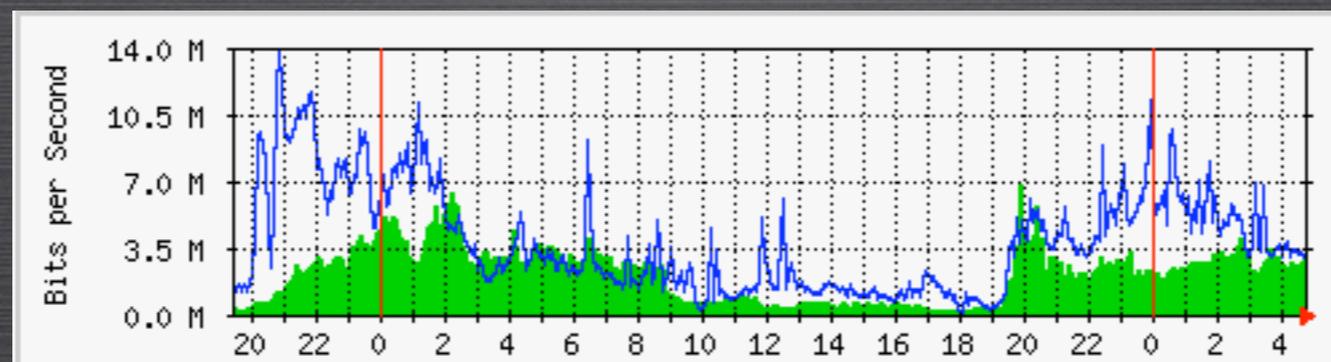
Router#
```

# 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](http://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](http://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](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
[-]	<b>All Sensors</b>	
[-]	<b>Mediserve AT&amp;T</b>	
	Port Fa0/1 on Mediserve AT&OK	OK
	InterOffice T1 Se0/0:0 on MeOK	OK
[-]	<b>ILI 1721</b>	
	Port Se0 on ILI 1721 (208.47 OK	OK

**View: Data of All Selected Sensors in One Graph**

Graphs

**Mediserve AT&T**

**Live Graph**

Last 60 Minutes - 30 sec Interval

**Last 24 Hours**

5 Minute(s) Averages

**Last 30 Days**

Hourly Averages

**Last 365 Days**

Daily Averages

■ 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

**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](http://www.paessler.com/prtg/history) for details and to [download the latest version!](#)

V5.2.0.581 Freeware Edition
130883 refreshes
3% CPU Load



# MESMERIZING UTILITIES

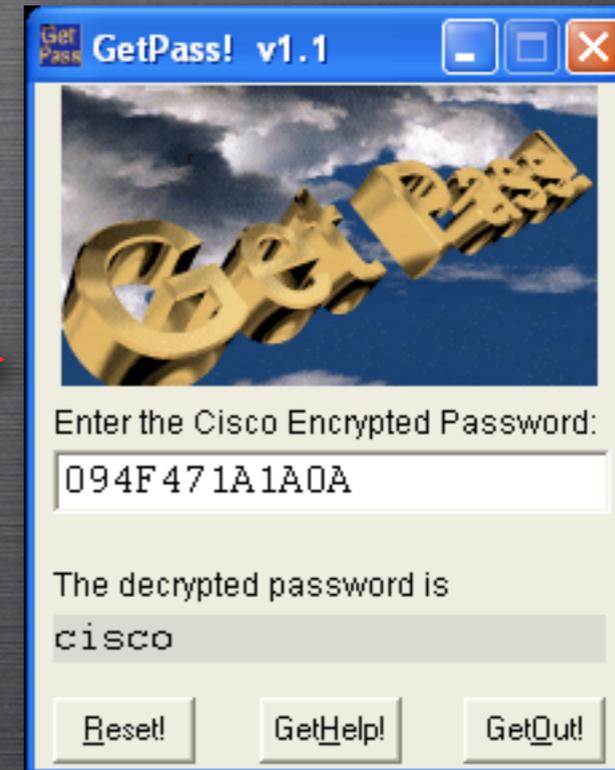
- GET PASS
- RIP GENERATOR
- SWITCH INSPECTOR
- KIWI SYSLOG / CATTOOLS

# MESMERIZING UTILITIES

## BOSON GETPASS 1.1 - CRACK LEVEL 7 ENCRYPTION

[HTTP://WWW.ADTECNETWORKS.COM/CISCOUTILS/GET\\_PASS.EXE](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](http://www.adtecnetworks.com/ciscoutils/rip_gen.exe)

# MESMERIZING UTILITIES

- NETXAR SWITCHINSPECTOR

[HTTP://WWW.SWITCHINSPECTOR.COM/](http://www.switchinspector.com/)

- ALLOWS YOU TO IDENTIFY THE DEVICES ATTACHED TO EACH OF THE SWITCH PORTS IN YOUR ORGANIZATION

# 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
Switch Property	Value	
Switch Name:	CAT_3550	
IP Address:	172.30.2.1	
Netmask:	255.255.255.0	
Model:	WS-C3550-24-PWR	
OS Description:	Cisco IOS Software, C3550 Software (C3550-I5K91L2Q3-M), Version 12.2(25)SEA, R... Copyright (c) 1986-2005 by Cisco Systems, Inc. Compiled Tue 25-Jan-05 23:50 by antonino	
Contact:		
Location:		
Uptime:	1874 hours 45 minutes 40 seconds	
Last Reload Reason:	power-on	
System Image File:	flash:c3550-i5k91l2q3-mz.122-25.SEA/c3550-i5k91l2q3-mz.122-25.5	
Processor RAM:	64 MB	
Free Processor RAM:	32.2 MB	
NVRAM:	384 KB	
NVRAM Used:	7.8 KB	
Processor Memory:	Used: 11.1 MB / Free: 32.2 MB	
I/O Memory:	Used: 2.9 MB / Free: 5.1 MB	

# 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

Port Name	Port Description	Port Mac Address	Port Speed	MTU	Duplex Setting
Fa0/1	FastEthernet0/1	00:0C:85:4C:05:01	100 Mbps	1500	Full Duplex
Fa0/2	FastEthernet0/2	00:0C:85:4C:05:02	100 Mbps	1500	Full Duplex
Fa0/3	FastEthernet0/3	00:0C:85:4C:05:03	100 Mbps	1500	Auto Negotiate
Fa0/4	FastEthernet0/4	00:0C:85:4C:05:04	100 Mbps	1500	Full Duplex
Fa0/5	FastEthernet0/5	00:0C:85:4C:05:05	100 Mbps	1500	Auto Negotiate
Fa0/6	FastEthernet0/6	00:0C:85:4C:05:06	10 Mbps	1500	Auto Negotiate
Fa0/7	FastEthernet0/7	00:0C:85:4C:05:07	100 Mbps	1500	Auto Negotiate
Fa0/8	FastEthernet0/8	00:0C:85:4C:05:08	100 Mbps	1500	Auto Negotiate
Fa0/9	FastEthernet0/9	00:0C:85:4C:05:09	100 Mbps	1500	Auto Negotiate
Fa0/10	FastEthernet0/10	00:0C:85:4C:05:0A	100 Mbps	1500	Full Duplex
Fa0/11	FastEthernet0/11	00:0C:85:4C:05:0B	100 Mbps	1500	Full Duplex
Fa0/12	FastEthernet0/12	00:0C:85:4C:05:0C	100 Mbps	1500	Auto Negotiate
Fa0/17	FastEthernet0/17	00:0C:85:4C:05:11	10 Mbps	1500	Auto Negotiate
Fa0/18	FastEthernet0/18	00:0C:85:4C:05:12	10 Mbps	1500	Auto Negotiate
Fa0/19	FastEthernet0/19	00:0C:85:4C:05:13	100 Mbps	1500	Auto Negotiate
Fa0/20	FastEthernet0/20	00:0C:85:4C:05:14	10 Mbps	1500	Auto Negotiate
Fa0/21	FastEthernet0/21	00:0C:85:4C:05:15	100 Mbps	1500	Auto Negotiate
Fa0/22	FastEthernet0/22	00:0C:85:4C:05:16	10 Mbps	1500	Auto Negotiate
Fa0/23	FastEthernet0/23	00:0C:85:4C:05:17	100 Mbps	1500	Full Duplex
Fa0/24	FastEthernet0/24	00:0C:85:4C:05:18	10 Mbps	1500	Auto Negotiate
Fa0/13	FastEthernet0/13	00:0C:85:4C:05:0D	100 Mbps	1500	Auto Negotiate
Fa0/14	FastEthernet0/14	00:0C:85:4C:05:0E	100 Mbps	1500	Full Duplex
Fa0/15	FastEthernet0/15	00:0C:85:4C:05:0F	100 Mbps	1500	Undetermined
Fa0/16	FastEthernet0/16	00:0C:85:4C:05:10	100 Mbps	1500	Undetermined
Gi0/1	GigabitEthernet0/1	00:0C:85:4C:05:19	10 Mbps	1500	Auto Negotiate
Gi0/2	GigabitEthernet0/2	00:0C:85:4C:05:1A	10 Mbps	1500	Auto Negotiate

# 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	●			
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

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

Device IP Address	Device Name	Device Mac Address	NIC Manufacturer	Port Name
172.30.4.2	172.30.4.2	00:14:1C:14:11:2C		Fa0/1
172.30.2.30	172.30.2.30	00:12:17:23:01:DA		Fa0/2
172.30.3.225	172.30.3.225	00:0F:B5:24:83:BA	NETGEAR Inc	Fa0/1
172.30.3.94	ip68-3-164-215.ph....	00:16:CB:B7:D1:C4		Fa0/1
172.30.60.29	172.30.60.29	00:14:1C:48:E7:1A		Fa0/1
172.30.60.29	172.30.60.29	00:14:1C:48:E7:1A		Fa0/1
172.30.2.48	172.30.2.48	00:14:A8:9E:F8:45		Fa0/1
172.30.2.50	jerwks.cioara.org	00:0F:EA:30:BC:71	Giga-Byte Technology Co.,LTD.	Fa0/1
172.30.1.100	172.30.1.100	00:0B:AC:AE:4F:00	3Com Europe Ltd.	Fa0/2
172.30.100.11	WIN2003	00:0F:EA:30:45:96	Giga-Byte Technology Co.,LTD.	Fa0/2
172.30.2.26	172.30.2.26	00:12:17:FC:A3:DB		Fa0/1
172.30.60.31	172.30.60.31	00:14:1C:48:E6:D1		Fa0/1
172.30.2.220	172.30.2.220	00:0C:41:97:BF:9A	The Linksys Group,Inc.	Fa0/1
172.30.60.31	172.30.60.31	00:14:1C:48:E6:D1		Fa0/1
172.30.2.47	172.30.2.47	00:14:6A:16:C2:DA		Fa0/1
172.30.60.27	172.30.60.27	00:14:6A:9C:33:09		Fa0/1
172.30.60.27	172.30.60.27	00:14:6A:9C:33:09		Fa0/1

# 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

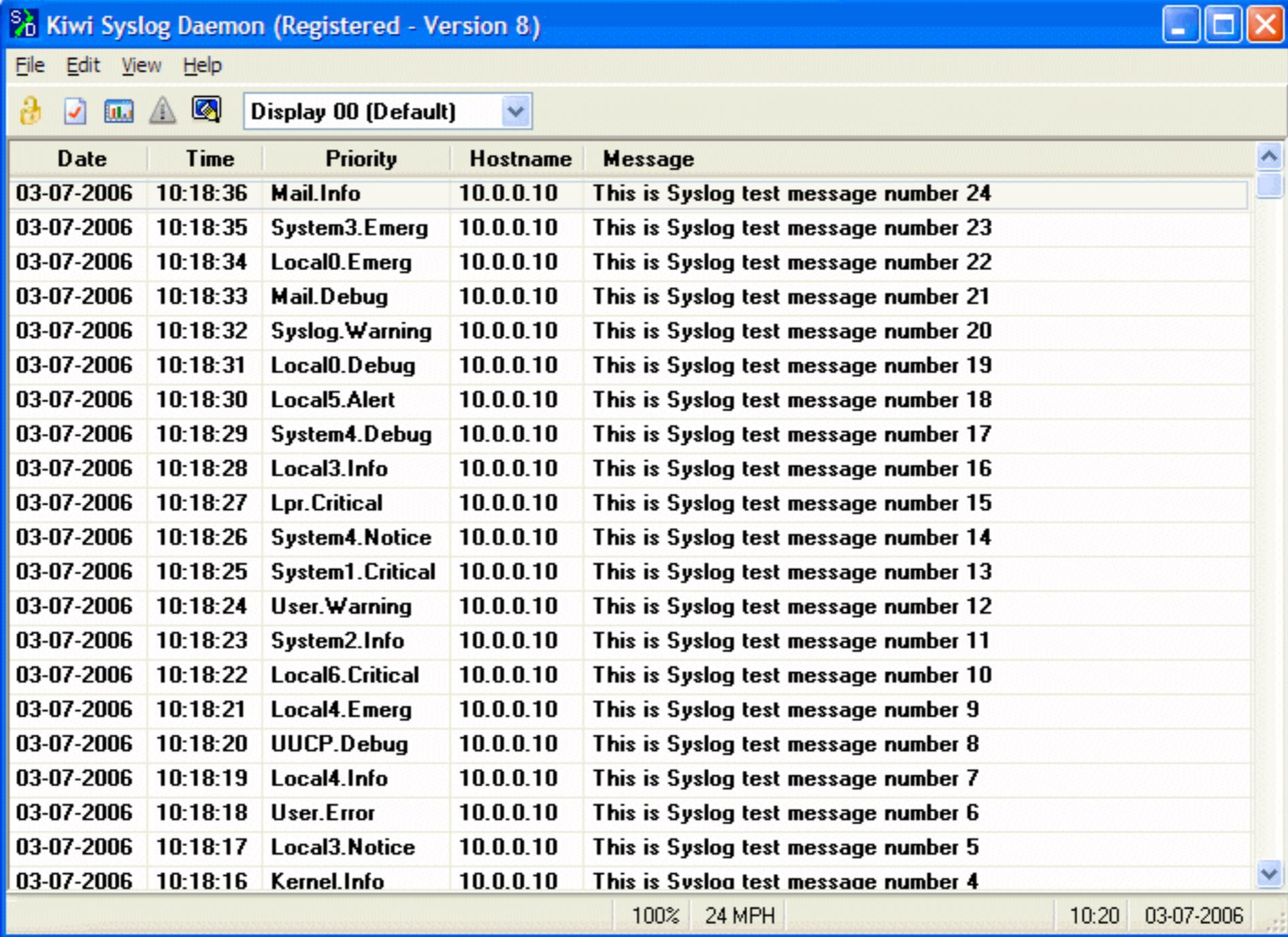
Export Results

Switch Info Table	Switch Ports Table	Devices Table			
Manufacturer	Port Name	VLAN	VLAN Description	Win User(s)	Windows Workgroup
	Fa0/1	400	EXIT		
	Fa0/2	200	CLIENTS		
Inc	Fa0/4	300	WIRELESS		
	Fa0/4	300	WIRELESS		
	Fa0/10	600	VOICE		
	Fa0/10	200	CLIENTS		
	Fa0/11	200	CLIENTS		
gy Co.,LTD.	Fa0/11	200	CLIENTS		CIOARA
e Ltd.	Fa0/23	1	default		
gy Co.,LTD.	Fa0/23	100	SERVERS		CIOARA
	Fa0/14	200	CLIENTS		
	Fa0/14	200	CLIENTS		
up,Inc.	Fa0/14	200	CLIENTS		
	Fa0/14	600	VOICE		
	Fa0/15	200	CLIENTS		
	Fa0/16	200	CLIENTS		
	Fa0/16	600	VOICE		

# MESMERIZING UTILITIES

## KIWI SYSLOG

[HTTP://WWW.KIWISYSLOG.COM](http://www.kiwisyslog.com)



The screenshot shows the 'Kiwi Syslog Daemon (Registered - Version 8)' application window. The window has a menu bar with 'File', 'Edit', 'View', and 'Help'. Below the menu bar is a toolbar with several icons and a dropdown menu set to 'Display 00 (Default)'. The main area contains a table of log messages with columns for Date, Time, Priority, Hostname, and Message. The messages are numbered 4 through 24 and all originate from the hostname 10.0.0.10. The status bar at the bottom shows '100%' zoom, '24 MPH' speed, and the time '10:20' on '03-07-2006'.

Date	Time	Priority	Hostname	Message
03-07-2006	10:18:36	Mail.Info	10.0.0.10	This is Syslog test message number 24
03-07-2006	10:18:35	System3.Emerg	10.0.0.10	This is Syslog test message number 23
03-07-2006	10:18:34	Local0.Emerg	10.0.0.10	This is Syslog test message number 22
03-07-2006	10:18:33	Mail.Debug	10.0.0.10	This is Syslog test message number 21
03-07-2006	10:18:32	Syslog.Warning	10.0.0.10	This is Syslog test message number 20
03-07-2006	10:18:31	Local0.Debug	10.0.0.10	This is Syslog test message number 19
03-07-2006	10:18:30	Local5.Alert	10.0.0.10	This is Syslog test message number 18
03-07-2006	10:18:29	System4.Debug	10.0.0.10	This is Syslog test message number 17
03-07-2006	10:18:28	Local3.Info	10.0.0.10	This is Syslog test message number 16
03-07-2006	10:18:27	Lpr.Critical	10.0.0.10	This is Syslog test message number 15
03-07-2006	10:18:26	System4.Notice	10.0.0.10	This is Syslog test message number 14
03-07-2006	10:18:25	System1.Critical	10.0.0.10	This is Syslog test message number 13
03-07-2006	10:18:24	User.Warning	10.0.0.10	This is Syslog test message number 12
03-07-2006	10:18:23	System2.Info	10.0.0.10	This is Syslog test message number 11
03-07-2006	10:18:22	Local6.Critical	10.0.0.10	This is Syslog test message number 10
03-07-2006	10:18:21	Local4.Emerg	10.0.0.10	This is Syslog test message number 9
03-07-2006	10:18:20	UUCP.Debug	10.0.0.10	This is Syslog test message number 8
03-07-2006	10:18:19	Local4.Info	10.0.0.10	This is Syslog test message number 7
03-07-2006	10:18:18	User.Error	10.0.0.10	This is Syslog test message number 6
03-07-2006	10:18:17	Local3.Notice	10.0.0.10	This is Syslog test message number 5
03-07-2006	10:18:16	Kernel.Info	10.0.0.10	This is Syslog test message number 4

# MESMERIZING UTILITIES

KIWI CATTOOLS - CONFIG DIF, MULTI COMMANDS

[HTTP://WWW.KIWISYSLOG.COM](http://www.kiwisyslog.com)

The screenshot displays the Kiwi CatTools [Enterprise] application window. The interface includes a menu bar (File, View, Options, Help) and a toolbar with buttons for Activities, Devices, Activity log, Compare, Info log, Report, TFTP, and Display. The main area shows a list of tasks with columns for Name, #, Days, and When. The tasks are grouped by type, such as Connectivity, General, and Report. At the bottom, there are buttons for Add, Remove, Edit, Copy, Run now, Start timer, and STOP. The status bar at the very bottom indicates 'Standard Mode', 'Schedule: Stopped', 'Errors: 0', 'Device: 0 of 0', 'Thread: 0 of 0', and 'IDLE'.

Type	Name	#	Days	When
Type: Connectivity.Inter-device ping	Nokia Inter ping	0	SMTWTFS	Never
Type: Connectivity.Login test	Nokia Login	2	SMTWTFS	Never
	SSH Test	1	SM-W-F-	Never
Type: Connectivity.Ping test	Ping Test	1	SMTWTFS	Never
Type: General.Backup Running Config	Cisco CatOS Backup	1	SMTWTFS	Never
	Cisco IOS Backup	0	SMTWTFS	Never
Type: General.Enter command	TFTP 2600 Config Download	1	SMTWTFS	Never
	TFTP 2600 Config Upload	1	SMTWTFS	Never
Type: General.Modify config	Cisco Pix Firewall	0	SMTWTFS	Never
Type: Report.ARP table	ARP Report	2	SMTWTFS	Never
Type: Report.CDP Neighbors Table				

# MESMERIZING UTILITIES

REALLY AWESOME NEW CISCO CONFIG DIFFER (RANCID)

[HTTP://WWW.SHRUBBERY.NET/RANCID/#STARTED](http://www.shrubbery.net/rancid/#started)



<b>Company</b>	<b>Tools</b>
<b>Services</b>	<b>RANCID - Really Awesome New Cisco conflg Differ</b>
<b>Tools</b>	
<b>Products</b>	RANCID monitors a router's (or more generally a device's) configuration, including software and hardware (cards, serial numbers, etc) and uses <a href="#">CVS (Concurrent Version System)</a> or <a href="#">Subversion</a> to maintain history of changes.
<b>Customers</b>	

SIMALR TO CATTOOLS, BUT COMPLETELY FREE

# QUESTIONS?

Check out:

<http://www.ciscoblog.com>



