Introduction to Routing Techniques and Theory (CCNA 2)

Lab Portfolio
Spring 2006

Rich Simms
May 12, 2006
CIS 82
Cabrillo College

Table of Contents

Lab 1: Introduction to using the router
Lab 2: Router configuration
Lab 3: Password Recovery and TFTP
Lab 4: Static Routes
Lab 5: RIP
Lab 6: IGRP
Lab 7: ACL
Case Study
Example Commands
Worksheets (additional lab work)

CIS 82 - LAB 1: Introduction To Using The Router
Rich Simms
February 21, 2006

Teammates:

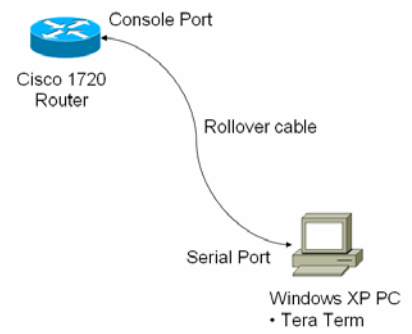
- Louis Arbanas
- Eric Jett
- Alf Popp

---

1 – Scenario

We used one Cisco Model 1720 Router attached to one Windows XP PC console. On the console PC we used the TeraTerm terminal emulation software. The objective of this lab was to learn how to cable a console to the router and explore some basic IOS commands.

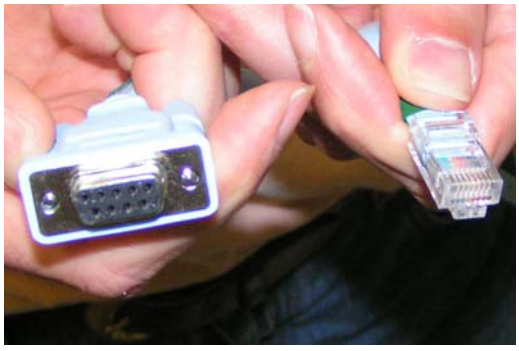
2 – Diagram



Lab 1 scenario

Cisco models 1720 (upper) and 1721 (lower)

"Cape Town" pod



Flat rollover cable

3 – Running Configurations

```
Router#show running-config
Building configuration...

Current configuration : 513 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!!
memory-size iomem 15
ip subnet-zero
!
!!
interface Serial0
 no ip address
 shutdown
!
interface Serial1
 no ip address
 shutdown
!
interface BRI0
 no ip address
 shutdown
!
interface FastEthernet0
 no ip address
 shutdown
 speed auto
!
ip classless
no ip http server
!
!
line con 0
line aux 0
line vty 0 4
!
no scheduler allocate
end

Router#
```

4 – Troubleshooting/Reflections

This lab went smoothly without any real problems. It took a little while to become familiar with the pods, the router backplanes, the various cables and how to power up everything. We started with HyperTerminal then switched to TeraTerm. We had to increase the number of lines TeraTerm would save so we could record everything. We copy and pasted console output from TeraTerm into a Word document and transferred that to a USB memory stick. We created an online collaboration website and data repository using Yahoo Groups to keep our lab data.

5 – Questions from the lab

Router Interface/Port	Cable Type	Connector	Device And Port To Which The Cable Is Connected
Console	Rollover	RJ-45	PC COM port 1 (with DB-9 connector)

Serial1	Serial (v.35)	Smart Serial Connector	Another router or WAN device
Serial0	Serial (v.35)	Smart Serial Connector	Another router or WAN device
Aux	Rollover	RJ-45	Modem
10/100 Ethernet	Straight	RJ-45	Switch
ISDN BRI U		RJ-45	ISDN device

Regarding Show Interface

- What does this command show you? (Shows detailed information and status for each router interface)
- Lots if information is shown, some of which we will discuss this semester. Is there any information you recognize? (Port names, MTUs, Ethernet parameters).
- How many interfaces does your router have and what are there names? (BRI0, BRI0:1, BRI0:2, FastEthernet0, Serial0, Serial1)
- How would you show a specific interfaces? (show interface serial 0)

Regarding show ip interface brief

- What kind of information does this command give you? (concise summary of interfaces)
- What is the state of the interfaces? (all down)
- Do they have IP addresses configured yet? (no, all unassigned)
- No is correct, but why not? That's right you have not configured them yet.

Match the interfaces displayed in the previous commands with the physical interfaces on the router.

BRI0, BRI0:1, BRI0:2 all go with ISDN BRI port
Serial0 goes with Serial0 port
Serial1 goes with Serial1 port
FastEthernet goes with 10/100 Ethernet port

Question: What do each of the following features do? (Short-term CCNA v2 exam knowledge.)

- CTRL-B = go "Back One Character". (can also use LEFT Arrow key)
- CTRL-F = go "Forward One Character". (can also use RIGHT Arrow key)
- CTRL-A = goes to the "Beginning" of the Line.
- CTRL-E = goes to the "End" of the Line.
- ESCAPE and B = go "Backward to the Beginning of the Next Word".

- ESCAPE and F = go "Forward to the Beginning of the Next Word".

6 – Example Commands

Erasing NVRAM

```
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
```

The penalty for making a typo

```
Router#confirm
Translating "confirm"...domain server (255.255.255.255)

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

Power router off and on

```
System Bootstrap, Version 12.0(3)T, RELEASE SOFTWARE (fc1)
Copyright (c) 1999 by cisco Systems, Inc.
C1700 platform with 20480 Kbytes of main memory

program load complete, entry point: 0x80008000, size: 0x3d7e44
Self decompressing the image : ##################################################
################################################################################################
################################################################################################
################################################################################################
################################################################################################
################################### [OK]

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-SY-M), Version 12.1(19), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Tue 04-Mar-03 16:01 by kellythw
Image text-base: 0x80008088, data-base: 0x807A62C8

cisco 1720 (MPC860) processor (revision 0x501) with 17408K/3072K bytes of memory
.
Processor board ID JAD04170G6P (2336786490), with hardware revision 0000
M860 processor: part number 0, mask 32
Bridging software.
X.25 software, Version 3.0.0.
Basic Rate ISDN software, Version 1.1.
```

```
1 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no

Would you like to terminate autoinstall? [yes]: yes


Press RETURN to get started!


00:00:03: %LINK-3-UPDOWN: Interface FastEthernet0, changed state to up
00:00:07: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0, changed
 state to up
00:00:08: %LINK-3-UPDOWN: Interface Serial0, changed state to down
00:00:08: %LINK-3-UPDOWN: Interface Serial1, changed state to down
00:00:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state
 to down
00:00:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed state
 to down
00:00:12: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0, changed
 state to down
00:00:36: %LINK-5-CHANGED: Interface BRI0, changed state to administratively dow
n
00:00:37: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0, changed state to
 down
00:00:38: %LINK-5-CHANGED: Interface Serial0, changed state to administratively
down
00:00:38: %LINK-5-CHANGED: Interface FastEthernet0, changed state to administrat
ively down
00:00:38: %LINK-5-CHANGED: Interface Serial1, changed state to administratively
down
00:00:45: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-SY-M), Version 12.1(19), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Tue 04-Mar-03 16:01 by kellythw
Router>
```

STEP 4 – Basic Commands

Help (non-privileged level)

```
Router>?
Exec commands:
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  clear            Reset functions
  connect          Open a terminal connection
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
  exit             Exit from the EXEC
  help             Description of the interactive help system
  lock             Lock the terminal
  login            Log in as a particular user
  logout           Exit from the EXEC
  mrinfo           Request neighbor and version information from a multicast
                   router
  mstat            Show statistics after multiple multicast traceroutes
  mtrace           Trace reverse multicast path from destination to source
  name-connection  Name an existing network connection
  pad              Open a X.29 PAD connection
```

```
  ping             Send echo messages
  ppp              Start IETF Point-to-Point Protocol (PPP)
  resume           Resume an active network connection
  rlogin           Open an rlogin connection
  show             Show running system information
  slip             Start Serial-line IP (SLIP)
  systat           Display information about terminal lines
  telnet           Open a telnet connection
  terminal         Set terminal line parameters
  traceroute       Trace route to destination
  tunnel           Open a tunnel connection
  where            List active connections
  x28              Become an X.28 PAD
  x3               Set X.3 parameters on PAD

Router>
```

Help (privileged level)

```
Router>enable
Router#?
Exec commands:
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  access-template  Create a temporary Access-List entry
  archive          manage archive files
  bfe              For manual emergency modes setting
  cd               Change current directory
  clear            Reset functions
  clock            Manage the system clock
  configure        Enter configuration mode
  connect          Open a terminal connection
  copy             Copy from one file to another
  debug            Debugging functions (see also 'undebug')
  delete           Delete a file
  dir              List files on a filesystem
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  elog             Event-logging control commands
  enable           Turn on privileged commands
  erase            Erase a filesystem
  exit             Exit from the EXEC
  help             Description of the interactive help system
  isdn             Make/disconnect an isdn data call on a BRI interface
  lock             Lock the terminal
  login            Log in as a particular user
  logout           Exit from the EXEC
  more             Display the contents of a file
  mrinfo           Request neighbor and version information from a multicast
                   router
  mrm              IP Multicast Routing Monitor Test
  mstat            Show statistics after multiple multicast traceroutes
  mtrace           Trace reverse multicast path from destination to source
  name-connection  Name an existing network connection
  no               Disable debugging functions
  pad              Open a X.29 PAD connection
  ping             Send echo messages
  ppp              Start IETF Point-to-Point Protocol (PPP)
  pwd              Display current working directory
  reload           Halt and perform a cold restart
  resume           Resume an active network connection
  rlogin           Open an rlogin connection
  rsh              Execute a remote command
  send             Send a message to other tty lines
  setup            Run the SETUP command facility
  show             Show running system information
  slip             Start Serial-line IP (SLIP)
  start-chat       Start a chat-script on a line
  systat           Display information about terminal lines
  telnet           Open a telnet connection
```

```
  terminal         Set terminal line parameters
  test             Test subsystems, memory, and interfaces
  traceroute       Trace route to destination
  tunnel           Open a tunnel connection
  undebug          Disable debugging functions (see also 'debug')
  verify           Verify a file
  where            List active connections
  write            Write running configuration to memory, network, or terminal
  x28              Become an X.28 PAD
  x3               Set X.3 parameters on PAD

Router#
```

More Help showing drill down to sub-level commands

```
Router>show ?
  backup          Backup status
  c1700           Show c1700 information
  cca             CCA information
  cdapi           CDAPI information
  cef             Cisco Express Forwarding
  class-map       Show QoS Class Map
  clock           Display the system clock
  compress        Show compression statistics
  controllers     Interface controller status
  dialer          Dialer parameters and statistics
  exception       exception informations
  flash:          display information about flash: file system
  history         Display the session command history
  hosts           IP domain-name, lookup style, nameservers, and host table
  isdn            ISDN information
  location        Display the system location
  modemcap        Show Modem Capabilities database
  policy-map      Show QoS Policy Map
  ppp             PPP parameters and statistics
  queue           Show queue contents
  queueing        Show queueing configuration
  radius          Shows radius information
  rmon            rmon statistics
  rtr             Response Time Reporter (RTR)
  sessions        Information about Telnet connections
  snmp            snmp statistics
  tacacs          Shows tacacs+ server statistics
  template        Template information
  terminal        Display terminal configuration parameters
  traffic-shape   traffic rate shaping configuration
  users           Display information about terminal lines
  version         System hardware and software status
  vpdn            VPDN information


Router>show interface ?
  BRI              ISDN Basic Rate Interface
  FastEthernet     FastEthernet IEEE 802.3
  Null             Null interface
  Serial           Serial
  accounting       Show interface accounting
  crb              Show interface routing/bridging info
  fair-queue       Show interface Weighted Fair Queueing (WFQ) info
  irb              Show interface routing/bridging info
  mac-accounting   Show interface MAC accounting info
  precedence       Show interface precedence accounting info
  random-detect    Show interface Weighted Random Early Detection (WRED) info
  rate-limit       Show interface rate-limit info
  type             Show vlan types
  |                Output modifiers
  <cr>
```

Help system

```
Router>help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
```

Privilege Mode

```
Router>
Router>enable
Router#disable
Router>enable
```

Ending session

```
Router#exit


Router con0 is now available


Press RETURN to get started.
```

Setting the date and Time

```
Router#clock set 18:00:00 9 Feb 2006
Router#show clock
18:00:09.619 UTC Thu Feb 9 2006
Router#
```

```
Router#show running-config
Building configuration...

Current configuration : 560 bytes
!
! No configuration change since last restart
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
!
!
!
!
!
memory-size iomem 15
ip subnet-zero
!
```

```
!
!
!
interface Serial0
 no ip address
 shutdown
!
interface Serial1
 no ip address
 shutdown
!
interface BRI0
 no ip address
 shutdown
!
interface FastEthernet0
 no ip address
 shutdown
 speed auto
!
ip classless
no ip http server
!
!
line con 0
line aux 0
line vty 0 4
!
no scheduler allocate
end

Router#


Router#show startup-config
%% Non-volatile configuration memory is not present
Router#
```

Copy

```
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#

Router#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router#


Router#show startup-config
Using 620 out of 29688 bytes
!
! No configuration change since last restart
! NVRAM config last updated at 02:12:25 UTC Fri Feb 10 2006
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
!
!
!
!
```

```
!
memory-size iomem 15
ip subnet-zero
!
!
!
!
interface Serial0
 no ip address
 shutdown
!
interface Serial1
 no ip address
 shutdown
!
interface BRI0
 no ip address
 shutdown
!
interface FastEthernet0
 no ip address
 shutdown
 speed auto
!
ip classless
no ip http server
!
!
line con 0
line aux 0
line vty 0 4
!
no scheduler allocate
end

Router#
```

Reload (without clearing startup-config)

```
Router#reload
Proceed with reload? [confirm]

00:43:29: %SYS-5-RELOAD: Reload requested
System Bootstrap, Version 12.0(3)T, RELEASE SOFTWARE (fc1)
Copyright (c) 1999 by cisco Systems, Inc.
C1700 platform with 20480 Kbytes of main memory

program load complete, entry point: 0x80008000, size: 0x3d7e44
Self decompressing the image : ########################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
######################### [OK]

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706
```

```
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-SY-M), Version 12.1(19), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Tue 04-Mar-03 16:01 by kellythw
Image text-base: 0x80008088, data-base: 0x807A62C8

cisco 1720 (MPC860) processor (revision 0x501) with 17408K/3072K bytes of memory
.
Processor board ID JAD04170G6P (2336786490), with hardware revision 0000
M860 processor: part number 0, mask 32
Bridging software.
X.25 software, Version 3.0.0.
Basic Rate ISDN software, Version 1.1.
1 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)



Press RETURN to get started!


00:00:03: %LINK-3-UPDOWN: Interface FastEthernet0, changed state to up
00:00:07: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0, changed
 state to up
00:00:07: %LINK-5-CHANGED: Interface BRI0, changed state to administratively dow
n
00:00:08: %SYS-5-CONFIG_I: Configured from memory by console
00:00:08: %LINK-5-CHANGED: Interface Serial0, changed state to administratively
down
00:00:08: %LINK-5-CHANGED: Interface Serial1, changed state to administratively
down
00:00:08: %LINK-5-CHANGED: Interface FastEthernet0, changed state to administrat
ively down
00:00:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0, changed state to
 down
00:00:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state
 to down
00:00:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed state
 to down
00:00:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0, changed
 state to down
00:00:10: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-SY-M), Version 12.1(19), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Tue 04-Mar-03 16:01 by kellythw
Router>enable
Router#
```

Reload (after clearing startup-config)

```
Router#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#reload
Proceed with reload? [confirm]

00:04:15: %SYS-5-RELOAD: Reload requested
System Bootstrap, Version 12.0(3)T, RELEASE SOFTWARE (fc1)
Copyright (c) 1999 by cisco Systems, Inc.
C1700 platform with 20480 Kbytes of main memory

program load complete, entry point: 0x80008000, size: 0x3d7e44
Self decompressing the image : ################################################
################################################################################################
################################################################################################
```

```
###############################################################################################
###############################################################################################
################################### [OK]

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-SY-M), Version 12.1(19), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Tue 04-Mar-03 16:01 by kellythw
Image text-base: 0x80008088, data-base: 0x807A62C8

cisco 1720 (MPC860) processor (revision 0x501) with 17408K/3072K bytes of memory
.
Processor board ID JAD04170G6P (2336786490), with hardware revision 0000
M860 processor: part number 0, mask 32
Bridging software.
X.25 software, Version 3.0.0.
Basic Rate ISDN software, Version 1.1.
1 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no

Would you like to terminate autoinstall? [yes]: yes


Press RETURN to get started!


00:00:03: %LINK-3-UPDOWN: Interface FastEthernet0, changed state to up
00:00:07: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0, changed
 state to up
00:00:08: %LINK-3-UPDOWN: Interface Serial0, changed state to down
00:00:08: %LINK-3-UPDOWN: Interface Serial1, changed state to down
00:00:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state
 to down
00:00:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed state
 to down
00:00:12: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0, changed
 state to down
00:00:31: %LINK-5-CHANGED: Interface BRI0, changed state to administratively dow
n
00:00:32: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0, changed state to
 down
00:00:32: %LINK-5-CHANGED: Interface Serial0, changed state to administratively
down
00:00:32: %LINK-5-CHANGED: Interface FastEthernet0, changed state to administrat
ively down
00:00:32: %LINK-5-CHANGED: Interface Serial1, changed state to administratively
down
00:00:35: %SYS-5-RESTART: System restarted --
```

```
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-SY-M), Version 12.1(19), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Tue 04-Mar-03 16:01 by kellythw


Router>setup
Translating "setup"...domain server (255.255.255.255)

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


         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no
Router#


Router#show interface
BRI0 is administratively down, line protocol is down
  Hardware is PQUICC BRI with U interface
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Last input never, output never, 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: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/16 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  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
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
BRI0:1 is administratively down, line protocol is down
  Hardware is PQUICC BRI with U interface
  MTU 1500 bytes, BW 64 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
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/16 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  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
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
BRI0:2 is administratively down, line protocol is down
  Hardware is PQUICC BRI with U interface
  MTU 1500 bytes, BW 64 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
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/16 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  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
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
 FastEthernet0 is administratively down, line protocol is down
  Hardware is PQUICC_FEC, address is 00b0.c289.49b2 (bia 00b0.c289.49b2)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 252/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, 10Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:31:32, 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
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     9 packets output, 1104 bytes, 0 underruns
     9 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     9 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Serial0 is administratively down, line protocol is down
  Hardware is PowerQUICC Serial
  MTU 1500 bytes, BW 128 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 00:31:21
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/32 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  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
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=down  DSR=down  DTR=down  RTS=down  CTS=down

Serial1 is administratively down, line protocol is down
  Hardware is PowerQUICC Serial
  MTU 1500 bytes, BW 128 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
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/32 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  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
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=down  DSR=down  DTR=down  RTS=down  CTS=down

Router#

Router#show ip interface brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
BRI0                       unassigned      YES unset  administratively down down

BRI0:1                     unassigned      YES unset  administratively down down

BRI0:2                     unassigned      YES unset  administratively down down

FastEthernet0              unassigned      YES unset  administratively down down

Serial0                    unassigned      YES unset  administratively down down

Serial1                    unassigned      YES unset  administratively down down

Router#

Router#show int serial 0
Serial0 is administratively down, line protocol is down
  Hardware is PowerQUICC Serial
  MTU 1500 bytes, BW 128 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 00:02:13
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/32 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  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
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=down  DSR=down  DTR=down  RTS=down  CTS=down



Router#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete
```

```
Router#
```

CIS 82 LAB 2: Router Configuration
Rich Simms
February 28, 2006

Teammates:

- Louis Arbanas
- Eric Jett
- Alf Popp

---

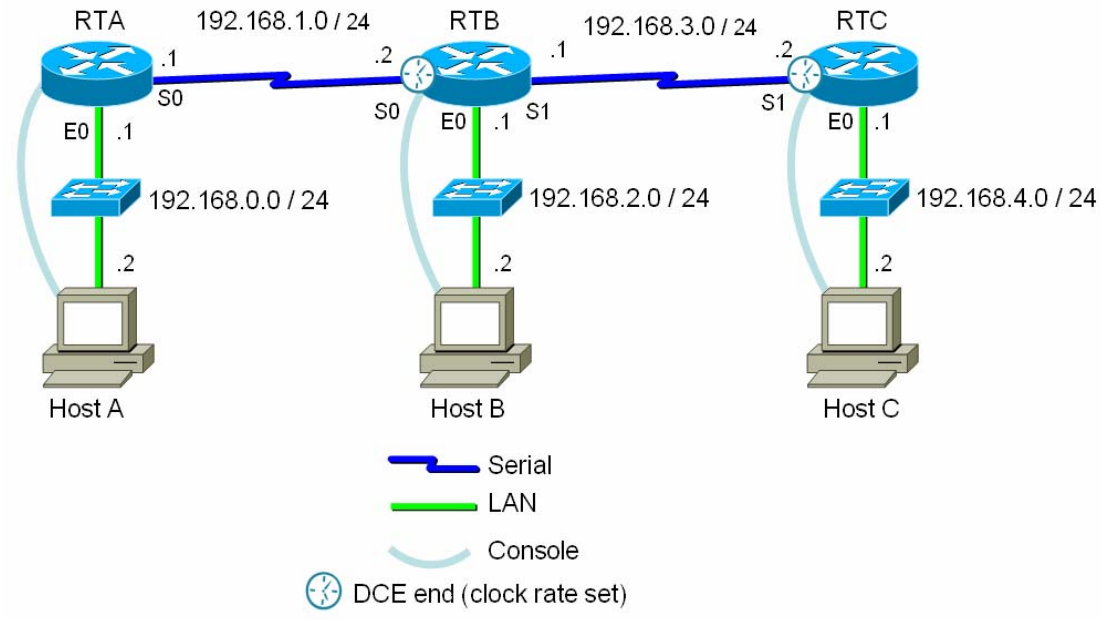
1 – Scenario

For this lab we used three Cisco routers, one switch and three PC's acting as both hosts and consoles. The routers were connected using the serial interfaces and the hosts were attached to the Ethernet interfaces. The switch was used between the hosts and the routers which allowed us to use all straight LAN cables.

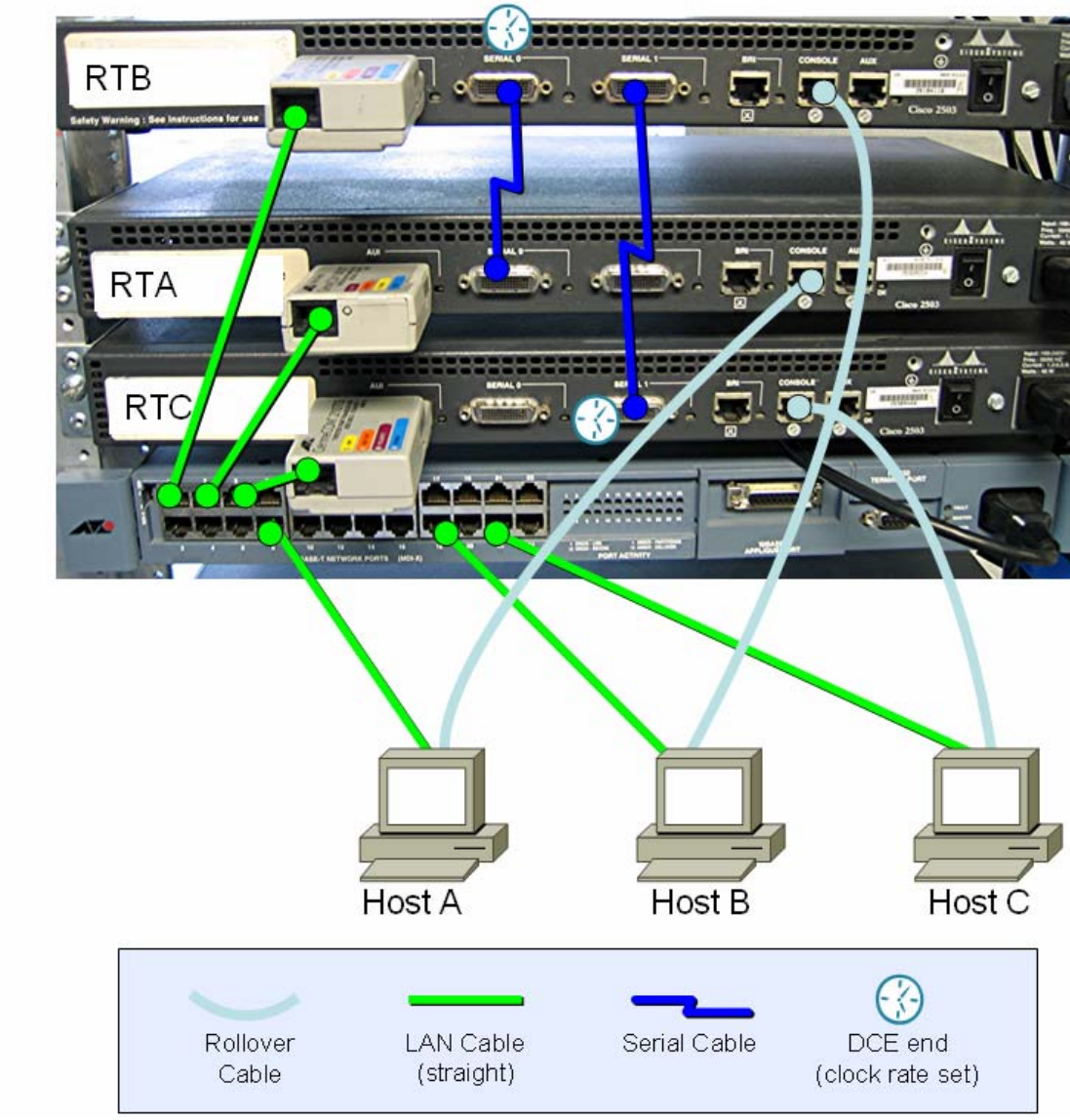
The objective of this lab was to learn how to configure interfaces, use telnet, set passwords & banners, explore CDP and debug capabilities.

2 – Diagram

Logical view:



Physical view:



3 – Running Configurations

```
RTA#show running-config
Building configuration...
< output omitted >
!
hostname RTA
!
enable secret 5
$1$ckL4$pSY1fZN8awVfqyUPXBDeN0
!
< output omitted >
!
no ip domain-lookup
ip host RTB 192.168.1.2
ip host RTA 192.168.1.1
ip name-server 192.168.0.50
!
< output omitted >
!
interface FastEthernet0
 description Blue LAN
 ip address 192.168.0.1
255.255.255.0
 speed auto
!
!
!
interface Serial0
 description Serial Link to
RTB
 ip address 192.168.1.1
255.255.255.0
!
interface Serial1
 no ip address
 shutdown
!
ip classless
no ip http server
ip pim bidir-enable
!
!
!
banner motd ^C
Warning! Authorized Access
Only ^C
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
!
no scheduler allocate
end

RTA#
```

```
RTB#show running-config
Building configuration...
< output omitted >
!
hostname RTB
!
enable secret 5
$1$X3KC$M9zTojEIrd7En5c34OuN8.
!
ip subnet-zero
no ip domain-lookup
ip host RTA 192.168.1.1
ip host RTC 192.168.3.2
ip host RTB 192.168.3.1
ip name-server 192.168.2.50
!
!< output omitted >
!
interface Ethernet0
 description White LAN
 ip address 192.168.2.1
255.255.255.0
 no ip directed-broadcast
!
!< output omitted >
!
interface Serial0
 description Serial link to
RTA
 ip address 192.168.1.2
255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 clockrate 64000
!
interface Serial1
 description Serial link to
RTC
 ip address 192.168.3.1
255.255.255.0
 no ip directed-broadcast
!
ip classless
!
banner motd ^C
WARNING KEEP OFF THE ROUTER ^C
!
line con 0
 password cisco
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end

RTB#
```

```
RTC#show running-config
Building configuration...
< output omitted >
!
hostname RTC
!
enable secret 5
$1$4KBP$4.icrRsYHXx5nx5cYgx/6.
!
memory-size iomem 15
ip subnet-zero
no ip domain-lookup
ip host RTC 192.168.3.2
ip host RTB 192.168.3.1
ip name-server 192.168.4.50
!
!< output omitted >
!
interface FastEthernet0
 description Red LAN
 ip address 192.168.4.1
255.255.255.0
 speed auto
!
!< output omitted >
!
interface Serial1
 description Serial link to
RTB
 ip address 192.168.3.2
255.255.255.0
 clockrate 64000
!
< output omitted >
!
ip classless
no ip http server
!
banner motd ^C
Warning!
Authorized Access Only ^C
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
!
no scheduler allocate
end

RTC#
```

4 – Troubleshooting /Reflections

Probably the most trouble with this lab was getting the cabling correct and understanding which end of the serial cables were DCE or DTE. Cabling required a slow, systematic and methodical

approach. The `ping` command was absolutely invaluable for making sure each connection worked. The `show ip int brief` was very helpful to make sure the interfaces were up and configured correctly.

5 – Questions from the lab

Regarding

Regarding clock rate command:

- Do you need to include this command on this serial interface? It is always needed for the DCE interface.

Regarding interface status:

- What might cause your Ethernet interface to be down? Unconnected cable, forgetting the no shut command.
- What might cause your Serial interface to be down? Unconnected, faulty or incorrect cabling, forgetting the no shut command, no clock rate set on the DCE end.
- What might cause your Serial or Ethernet interface to be administratively down? Forgetting the no shut command.

Regarding Show interface:

- Do you see your interface description? yes
- Do you see the ip address information? yes
- What else do you notice? There is a great deal of information about each interface including encapsulation, MTU, bandwidth, reliability, timers, traffic statistics etc.

Issue an extended ping command. How did you do that?

An extended ping lets you specify both source and destination IP addresses as well as other options. To run an extended ping just type ping and then you get prompted for the rest. The extended ping command works only in privileged EXEC mode while the normal ping works both in the user and privileged EXEC modes.

Regarding Telnet:

- What is the difference between telnetting into a device and accessing it via the console port? Telnet sessions access routers on the network from anywhere on the network. The console port requires a physical connection to the router using the special rollover cable from the serial COM port on a PC.
- What must you have configured before telnetting into the router? A password.

6 – Example Commands

Ping

```
RTA#ping rta

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 162.168.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)


RTA#ping rta

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
RTA#rtb

RTA#ping 192.168.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

RTA#config term
Enter configuration commands, one per line.  End with CNTL/Z.
RTA(config)#ip host rta 192.168.1.2
RTA(config)#ip host rta 192.168.1.1
RTA(config)#exit
```

Interfaces

```
RTB#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0              192.168.2.1     YES manual up                    up
Ethernet1              unassigned      YES unset  administratively down down
Serial0                192.168.1.2     YES manual up                    up
Serial1                192.168.3.1     YES manual up                    up
RTB#

RTA#show hosts
Default domain is not set
Name/address lookup uses static mappings

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined

Host                   Port  Flags      Age Type   Address(es)
rtb                    None  (perm, OK)  0   IP    192.168.1.2
rta                    None  (perm, OK)  0   IP    192.168.1.1
RTA#

RTA#show interface serial 0
Serial0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Description: Serial Link to RTB
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

```
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:05, output 00:00:01, output hang never
  Last clearing of "show interface" counters 01:34:06
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/2/32 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 96 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     193 packets input, 12224 bytes, 0 no buffer
     Received 193 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     226 packets output, 22896 bytes, 0 underruns
     0 output errors, 0 collisions, 73 interface resets
     0 output buffer failures, 0 output buffers swapped out
     33 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

RTA#show interface fastethernet 0
FastEthernet0 is up, line protocol is up
  Hardware is PQUICC_FEC, address is 000b.5f70.e2d0 (bia 000b.5f70.e2d0)
  Description: Blue LAN
  Internet address is 192.168.0.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:01, 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
  5 minute output rate 0 bits/sec, 0 packets/sec
     424 packets input, 155778 bytes
     Received 424 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     347 packets output, 43219 bytes, 0 underruns
     18 output errors, 0 collisions, 14 interface resets
     0 babbles, 0 late collision, 0 deferred
     18 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
RTA#
```

CDP

```
RTA#show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is  enabled

RTC#show cdp neighbor
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
Switch           Fas 0              151         S I       WS-C2950-2Fas 0/12
RTB              Ser 1              152          R        2500      Ser 1
RTC#

RTA#show cdp entry RTB
-------------------------
Device ID: RTB
Entry address(es):
  IP address: 192.168.1.2
Platform: cisco 2500,  Capabilities: Router
Interface: Serial0,  Port ID (outgoing port): Serial0
Holdtime : 126 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(5), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 15-Jun-99 20:08 by phanguye

advertisement version: 1

RTA#show cdp interface
BRI0 is administratively down, line protocol is down
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
BRI0:1 is administratively down, line protocol is down
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
   Holdtime is 180 seconds
   BRI0:2 is administratively down, line protocol is down
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
FastEthernet0 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial0 is up, line protocol is up
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial1 is administratively down, line protocol is down
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
   Holdtime is 180 seconds


RTA#show cdp neighbor detail
-------------------------
Device ID: Switch
Entry address(es):
Platform: cisco WS-C2950-24,  Capabilities: Switch IGMP
Interface: FastEthernet0,  Port ID (outgoing port): FastEthernet0/11
Holdtime : 143 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(19)EA1c, RELEASE SOFTWARE
 (fc2)
Copyright (c) 1986-2004 by cisco Systems, Inc.
```

```
Compiled Mon 02-Feb-04 23:29 by yenanh

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27, value=0000000
0FFFFFFFF010231FF00000000000000115CD1BC00FF0000
VTP Management Domain: 'group1'
Native VLAN: 1
Duplex: full

-------------------------
Device ID: RTB
Entry address(es):
  IP address: 192.168.1.2
Platform: cisco 2500,  Capabilities: Router
Interface: Serial0,  Port ID (outgoing port): Serial0
Holdtime : 139 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(5), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 15-Jun-99 20:08 by phanguye

advertisement version: 1
```

Debug

```
RTC#debug ip packet
IP packet debugging is on
RTC#
02:42:24: IP: s=192.168.4.2 (FastEthernet0), d=192.168.4.1 (FastEthernet0), len 60, rcvd 3
02:42:24: IP: s=192.168.4.1 (local), d=192.168.4.2 (FastEthernet0), len 60, sending
02:42:25: IP: s=192.168.4.2 (FastEthernet0), d=192.168.4.1 (FastEthernet0), len 60, rcvd 3
02:42:25: IP: s=192.168.4.1 (local), d=192.168.4.2 (FastEthernet0), len 60, sending
02:42:26: IP: s=192.168.4.2 (FastEthernet0), d=192.168.4.1 (FastEthernet0), len 60, rcvd 3
02:42:26: IP: s=192.168.4.1 (local), d=192.168.4.2 (FastEthernet0), len 60, sending
02:42:27: IP: s=192.168.4.2 (FastEthernet0), d=192.168.4.1 (FastEthernet0), len 60, rcvd 3
02:42:27: IP: s=192.168.4.1 (local), d=192.168.4.2 (FastEthernet0), len 60, sending
02:42:34: IP: s=0.0.0.0 (FastEthernet0), d=255.255.255.255, len 604, rcvd 2
02:42:48: IP: s=0.0.0.0 (FastEthernet0), d=255.255.255.255, len 604, rcvd 2
RTC#undebug ip packet
```

CIS 82 Lab 3 – WebCT submittal

Rich Simms
March 8, 2006

The objective of Lab 3 was to learn how to do password recovery and utilize an TFTP server. This abbreviated WebCT write-up contains the following sections:

1) Post password recovery configuration files.
2) Step-by-Step instructions for doing a password recovery.
3) Step-by-Step instructions for backing up and restoring configuration files with TFTP.

1) Post Password Recovery Configuration Files

Router: Cisco 2503 (Carmel in pod Istanbul)
Date: 03-Mar-2007
Time: 4:00 PM

```
simms#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(5), RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 15-Jun-99 20:08 by phanguye
Image text-base: 0x030380DC, data-base: 0x00001000

ROM: System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-RXBOOT), Version 10.2(8a),
RELEASE SOFTW
ARE (fc1)

simms uptime is 4 minutes
System restarted by power-on
System image file is "flash:c2500-d-l_120-5.bin"
```

(The image file the router booted from)

Interpretation of image filename "c2500-d-l_120-5.bin":

- Platform "C2500" = Cisco core router model 2500 platform
- Feature set "d" = Desktop subset (SNMP, IP, Bridging, WAN, Remote Node, Terminal Services, IPX, Atalk, ARAP)
- File format "l" = relocatable (runs from RAM)
- Version "120-5" = version 12.0, revision 5

```
cisco 2500 (68030) processor (revision D) with 8192K/2048K bytes of
memory.
Processor board ID 01730642, with hardware revision 00000000
Bridging software.
X.25 software, Version 3.0.0.
Basic Rate ISDN software, Version 1.1.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-volatile configuration memory.
```

```
8192K bytes of processor board System flash (Read ONLY)

Configuration register is 0x42 (will be 0x2102 at next reload)
```
(this is the configuration register, we are leaving it at 0x2102)

```
simms#show flash

System flash directory:
File  Length   Name/status
  1   6830452  c2500-d-l_120-5.bin
[6830516 bytes used, 1558092 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)
```
(size of image in flash)

```
simms#show start
Using 693 out of 32762 bytes
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname simms
!
enable secret 5 $1$8ubm$MMdf0mrVS7PxV6z8nqiLK0
!
ip subnet-zero
no ip domain-lookup
ip host CON 10.1.1.2
!
!
process-max-time 200
!
interface Ethernet0
 ip address 10.1.1.1 255.255.255.0
 no ip directed-broadcast
 shutdown
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
interface BRI0
 no ip address
 no ip directed-broadcast
 shutdown
!
ip classless
```

```
!
!
line con 0
 password cisco
 login
 transport input none
line aux 0
line vty 0 4
 login
!
end

simms#
```

2) Step-by-Step Password Recovery Instructions

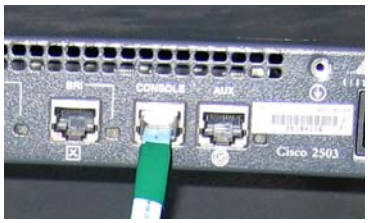
The passwords for a router are stored in the startup-config file in NVRAM. Recovering the password involves "breaking-in" during the router bootup process and configuring the configuration register so that the startup-config file is bypassed. This allows the router to start in an un-configured state with no password. From that point the network administrator has control again of the router and can both recover configuration information as well as reset the password

The instructions below apply to the Cisco router model 2503. For specific instructions relating to other routers models see:

http://www.cisco.com/warp/public/474/

Step 1 – Attach a PC console to the router

- Connect a flat rollover cable from the router's console port to the Serial COM port on a PC that will act as the console.



- Insure TeraTerm terminal emulation software is installed on the console PC.
  http://hp.vector.co.jp/authors/VA002416/teraterm.html
- Configure TeraTerm to connect using the serial COM 1 port with 9600 baud, no parity, 8 databits, 1 stop bit, no flow control. Other COM ports can be used as well if COM 1 is not available.

Step 2 – Record current configuration register setting

- If you still have access to the router, enter a `show version` command and record the setting of the configuration register at the end of the version information:

```
Configuration register is 0x2102
```

  We will use this later to restore the routers configuration register after changing it.

Step 3 – Reboot and "break in" into the router.

- Note, if this is a production router you will need to schedule this operation accordingly and notify users the network will be down.
- Reboot - power off the router, then power it back on using the router's power switch.
- Break in - send a break sequence within 60 seconds of powering on the router. With TeraTerm this is done by typing **Alt-b** (pressing alt and b keys at the same time)
- If you hit the **alt-b** enough times during the 60 second window you will enter ROMmon mode which looks as follows:

```
System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
Copyright (c) 1986-1995 by cisco Systems
2500 processor with 8192 Kbytes of main memory

Abort at 0x10EA82E (PC)
>
```

  If you don't get into ROMmon mode the first time, keep rebooting and entering multiple Alt-b's till you hit the right time window.

Step 4 – In ROMmon mode, reconfigure router boot to bypass startup-config and reboot again

- Use the following commands to reset the configuration register and reboot:

```
>o/r 0x42
>i
```

- When the router comes up type `no` to the setup prompt or `ctrl-c`

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog?
[yes/no]: no
```

Step 5 – Perform password recovery

- Enter privileged mode

```
Router>enable
Router#
```

- Restore previous startup configuration:

```
Router#copy startup-config running-config
Destination filename [running-config]?
683 bytes copied in 4.784 secs (170 bytes/sec)
simms#
```

- Set new password:

```
simms#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
simms(config)#enable secret class
```

- Restore the configuration register to the value recorded in Step 2:

```
simms(config)#config-register 0x2102
simms(config)#exit
simms#
```

- Save new configuration (with reset password):

```
simms#copy running-config startup-config
```

- Verify configuration register change by issuing show version command and looking at the end of the output for the restored setting of the configuration register:

```
Configuration register is 0x42 (will be 0x2102 at next
reload)
```

- Reboot the router now and check that your new password is correct.

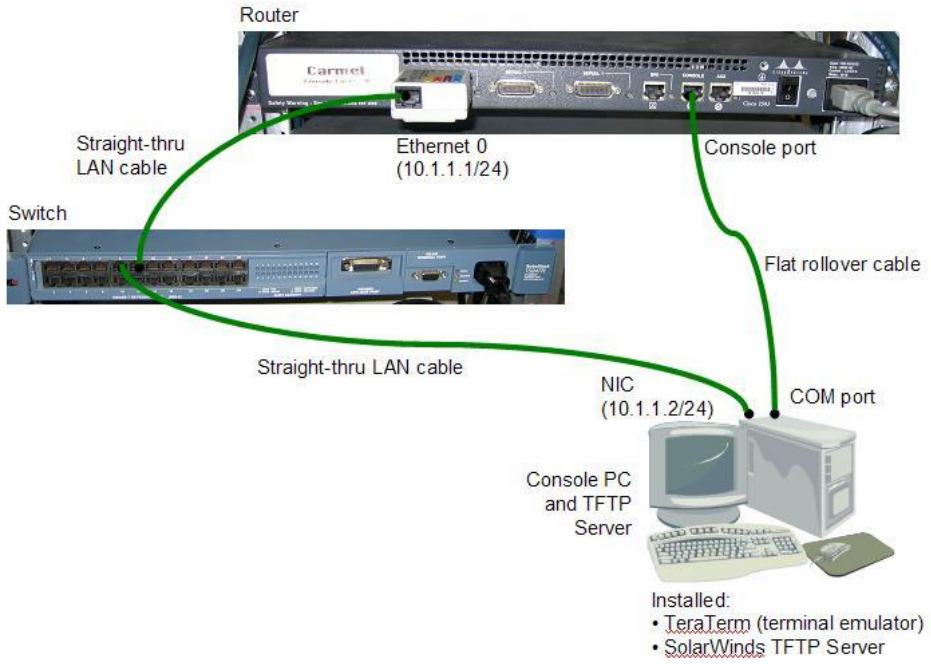
3) Step-by-Step instructions for backing up and restoring configuration files with TFTP.

IOS can copy files to and from a TFTP server. TFTP stands for trivial File Transfer Protocol and is a way to transfer files over a network. In this case we will use the SolarWinds TFTP server software on the console PC to act as the TFTP server.

The following instructions show how to backup and restore files. The example shows a particular configuration which has the TFTP server running on the console PC. This is for this example only as the TFTP server could be elsewhere on the network.

Step 1 – Connect console (and TFTP server) to the router

- Make the following connections



- Insure TeraTerm terminal emulation software is installed on the console PC.
  http://hp.vector.co.jp/authors/VA002416/teraterm.html
- Configure TeraTerm to connect using the serial COM 1 port with 9600 baud, no parity, 8 databits, 1 stop bit, no flow control. Other COM ports can be used as well if COM 1 is not available.
- Insure SolarWinds TFTP server is installed and running.
  http://www.solarwinds.net/FreeTools.htm

Step 2 – Configure the interfaces

- Note: for this example we will configure a 10.1.1.0/24 network for the router and TFTP server to use for file transfer. This does not have to be this specific network for TFTP transfers and other correctly configured networks can be used instead.
- On the Console PC (which is also the TFTP server) configure the LAN interface as follows:

```
IP 10.1.1.2
```

```
Subnet mask: 255.255.255.0
Default gateway: 10.1.1.1
```

- On the router, configure the Ethernet interface.

```
simms#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
simms(config)#interface ethernet 0
simms(config)#ip address 10.1.1.1 255.255.255.0
simms(config)#no shut
simms(config)#end
```

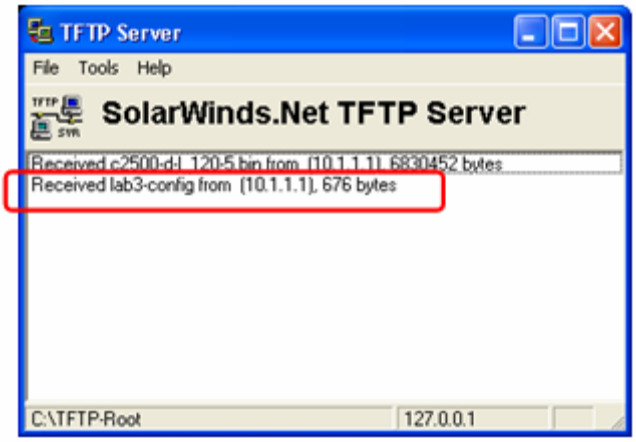
- At this time it is a good idea to check all interfaces with the ping command on the router and on the Console PC. From the router ping the PC and from the PC ping the router.
- Make sure the TFTP server is running on the Console PC.

Step 3 – Backup a configuration file to the TFTP server

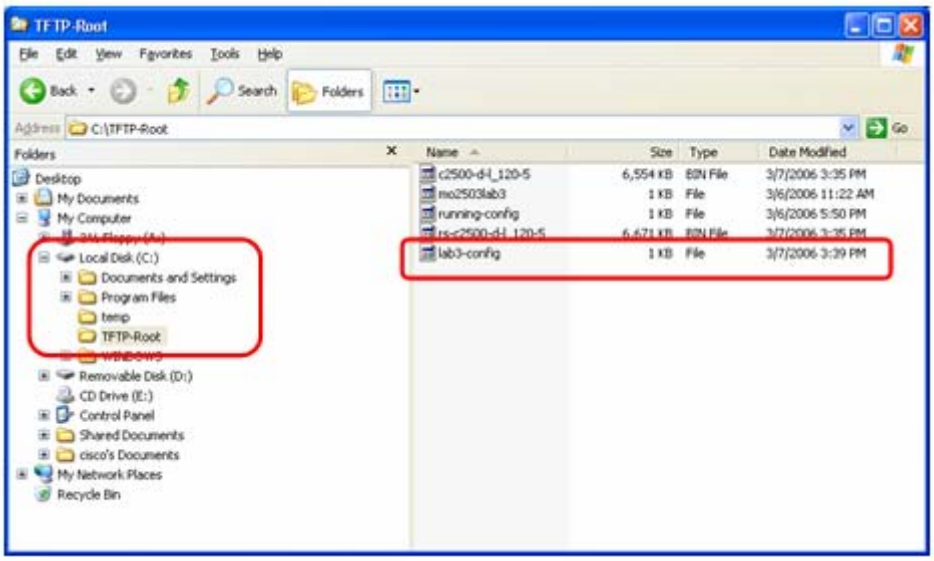
- Use the copy command to back up running-config or startup-config file. In this example we will backup the startup-config file and name it lab3-config on the TFTP server:

```
simms#
simms#copy startup-config tftp
Address or name of remote host []? 10.1.1.2
Destination filename [startup-config]? lab3-config
!!
676 bytes copied in 0.240 secs
simms#
```

- Look at SolarWinds TFTP server to verify the transfer. In this example the startup-config file on the router was copied to a file named lab3-config on the TFTP server:



- The files on the TFTP server (Console PC) are placed in the TFTP-Root directory on the C: drive by default. Use Windows Explorer to view and manage these files as needed. Best practices include adding your initials and dates to the names of these files.

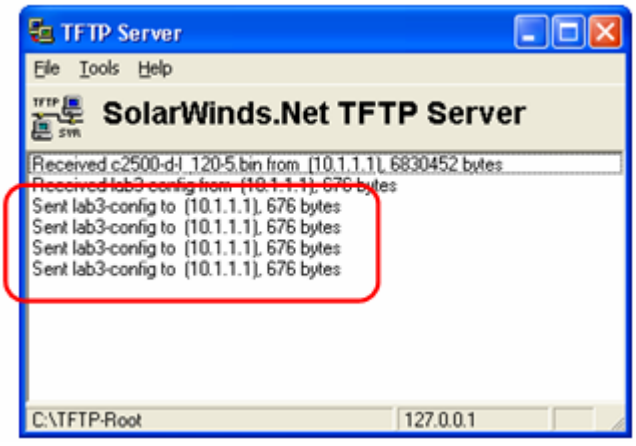


Step 4 - Restore a configuration file from the TFTP server

- Use the copy command as follows to restore the startup-config file:

```
oops#copy tftp startup-config
Address or name of remote host []? 10.1.1.2
Source filename []? lab3-config
Destination filename [startup-config]?
Accessing tftp://con/lab3-config...
Loading lab3-config from 10.1.1.2 (via Ethernet0): !
[OK - 676/1024 bytes]
```

- Look at SolarWinds TFTP server to verify it sent the file. In this example we transferred the file named lab3-config on the TFTP server back to startup-config file on the router. Note, this overwrites the file on the router.



- At this point you can view the new startup configuration file using `show startup-config` to insure it is what you wanted.
- Note the copy command could just as easily be used to backup or restore other configuration files such as running-config. It is also capable of backing up and restoring image files in flash.

CIS 82 LAB 3: Password Recovery and TFTP
Rich Simms
March 7, 2006

Teammates:

- Louis Arbanas
- Eric Jett
- Alf Popp

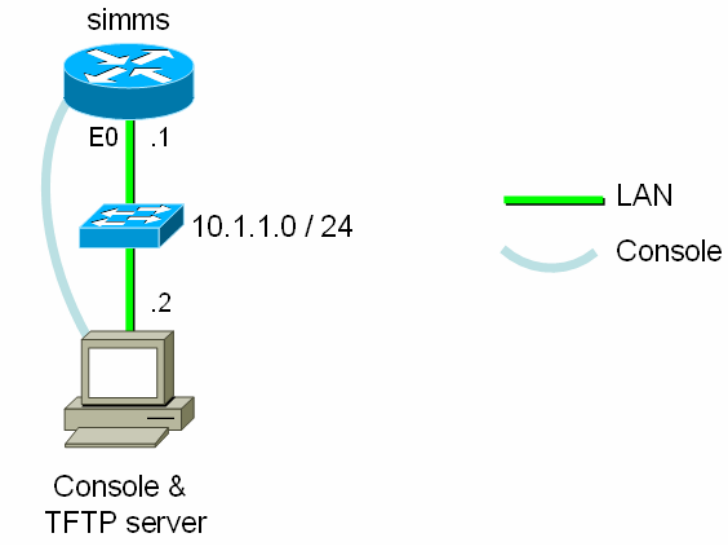
---

1 – Scenario

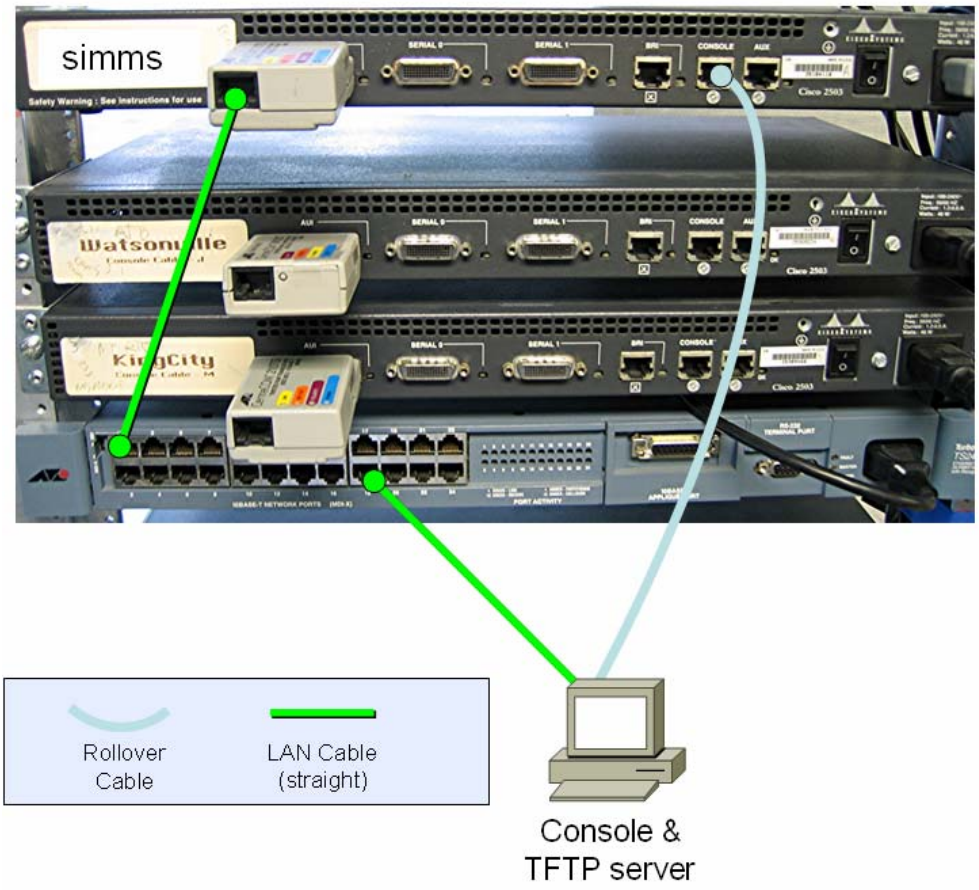
The objective of this lab was to learn how to perform password recovery, utilize a TFTP server to backup and to boot up form a TFTP server. For this lab we used one Cisco router, one switch and one PC. The PC played the role of both console and TFTP server.

2 – Diagram

Logical view:



Physical view:



3 – Running Configurations

```
simms#show start
Using 693 out of 32762 bytes
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname simms
!
enable secret 5
$1$8ubm$MMdf0mrVS7PxV6z8nqiLK0
!
ip subnet-zero
no ip domain-lookup
ip host CON 10.1.1.2
!
!
process-max-time 200
!
interface Ethernet0
 ip address 10.1.1.1 255.255.255.0
 no ip directed-broadcast
 shutdown
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
interface BRI0
 no ip address
 no ip directed-broadcast
 shutdown
!
ip classless
!
!
line con 0
 password cisco
 login
 transport input none
line aux 0
line vty 0 4
 login
!
end

simms#
```

4 – Troubleshooting/Reflection

The most time consuming problem was trying to get the router to boot from the TFTP server. Instead of booting it would time out with the following message:

```
%SYS-6-READ_BOOTFILE_FAIL: tftp://255.255.255.255/rs-c1700-k9o3sy7-mz.122-8.T5.b
in File read failed -- Timed out.
```

Note that normal TFTP file copies worked fine and it was only the boot from TFTP that had a problem.

The Cisco web site recommended:

%SYS-6-READ_BOOTFILE_FAIL : [chars] [chars].
Explanation A configured boot system command has failed.

Recommended Action If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

And the Cisco site also recommended:

Q. Why do I get "Timeout" error messages?

A. Verify that the TFTP server is open on your PC. Also, make sure the file is in the root directory (from the TFTP application software menu bar, choose View > Options).

Try to eliminate extraneous networking complexities between the router and the TFTP server, such as hubs and switches, or reduce the hop count between the router and server. This may involve moving the TFTP server or setting up a new server on a network segment topologically closer to the router, or on the same LAN segment as the router.

Finally, if these actions fail to resolve the problem, try using different TFTP server software.

Trying different routers did not resolve the problem. Only when trying a different host PC did everything work properly.

Many weeks later, one of the lab techs also looked into this problem. He was able to reproduce the same boot failure. He discovered another work-around which entailed replacing the switch between the TFTP server and the router with a cross-over cable.

5 – Lab Questions

After breaking in during boot and changing the configuration register to x42 from x2102

- What does the running-config look like? Clean (no password set)
- What does the startup-config look like? Has configured settings including password
- Why is the startup-config still there? not erased, just ignored
- What happens the next time you reboot the router if you do not reset the configuration register to x2102? will bypass startup-config again

Regarding TFTP

- What is the difference between copying the running-config to the TFTP server or the startup-config to the TFTP server? Running-config will have any unsaved changes
- When does it matter which one you choose? Should save whichever one you wish to later restore from
- After copying the old startup-config file from the TFTP server, when will this version take effect?

Regarding booting from TFTP

- Where did the router boot from? Booted from tftp server
- Now, from the TFTP server's directory delete the IOS image. Reboot the router. Where do you think it will boot from now? From Flash
- Does it make a difference if the TFTP server is on? Fails if tftp server is not available
- What is the command to prevent the router from attempting to boot from the image on the TFTP server? Just use boot system flash and delete commands to boot from tftp server

6 – Example Commands

```
Router>
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname simms
simms(config)#

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
simms(config)#int e0
simms(config-if)#ip add 10.1.1.1 255.255.255.0
simms(config-if)#no shut
simms(config-if)#
00:03:44: %LINK-3-UPDOWN: Interface Ethernet0, changed state to up
00:03:45: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed sta
te to up
simms(config-if)#ip host CON 10.1.1.2
simms(config)#enable secret class
simms(config)#line console 0
simms(config-line)#login
simms(config-line)#password cisco
simms(config-line)#end
simms#
00:05:37: %SYS-5-CONFIG_I: Configured from console by consolecopy run
simms#

simms#show flash

System flash directory:
File  Length   Name/status
  1   6830452  c2500-d-l_120-5.bin
[6830516 bytes used, 1558092 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)

simms#copy flash tftp
Source filename []? c2500-d-l_120-5.bin
Address or name of remote host []? con
Destination filename [c2500-d-l_120-5.bin]?
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
            cisco Systems, Inc.
            170 West Tasman Drive
            San Jose, California 95134-1706


Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(5), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 15-Jun-99 20:08 by phanguye
Image text-base: 0x0000144C, data-base: 0x00637308

cisco 2500 (68030) processor (revision D) with 8192K/2048K bytes of memory.
Processor board ID 01730642, with hardware revision 00000000
Bridging software.
X.25 software, Version 3.0.0.
Basic Rate ISDN software, Version 1.1.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)



Press RETURN to get started!




simms#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(5), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 15-Jun-99 20:08 by phanguye
Image text-base: 0x030380DC, data-base: 0x00001000

ROM: System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-RXBOOT), Version 10.2(8a), RELEASE SOFTW
ARE (fc1)

simms uptime is 4 minutes
System restarted by power-on
System image file is "flash:c2500-d-l_120-5.bin"

cisco 2500 (68030) processor (revision D) with 8192K/2048K bytes of memory.
Processor board ID 01730642, with hardware revision 00000000
Bridging software.
X.25 software, Version 3.0.0.
Basic Rate ISDN software, Version 1.1.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)

Configuration register is 0x42 (will be 0x2102 at next reload)

simms#
```

CIS 82 LAB 4: Static Routing
Rich Simms
March 14, 2006

Teammates:

- Louis Arbanas
- Eric Jett
- Alf Popp

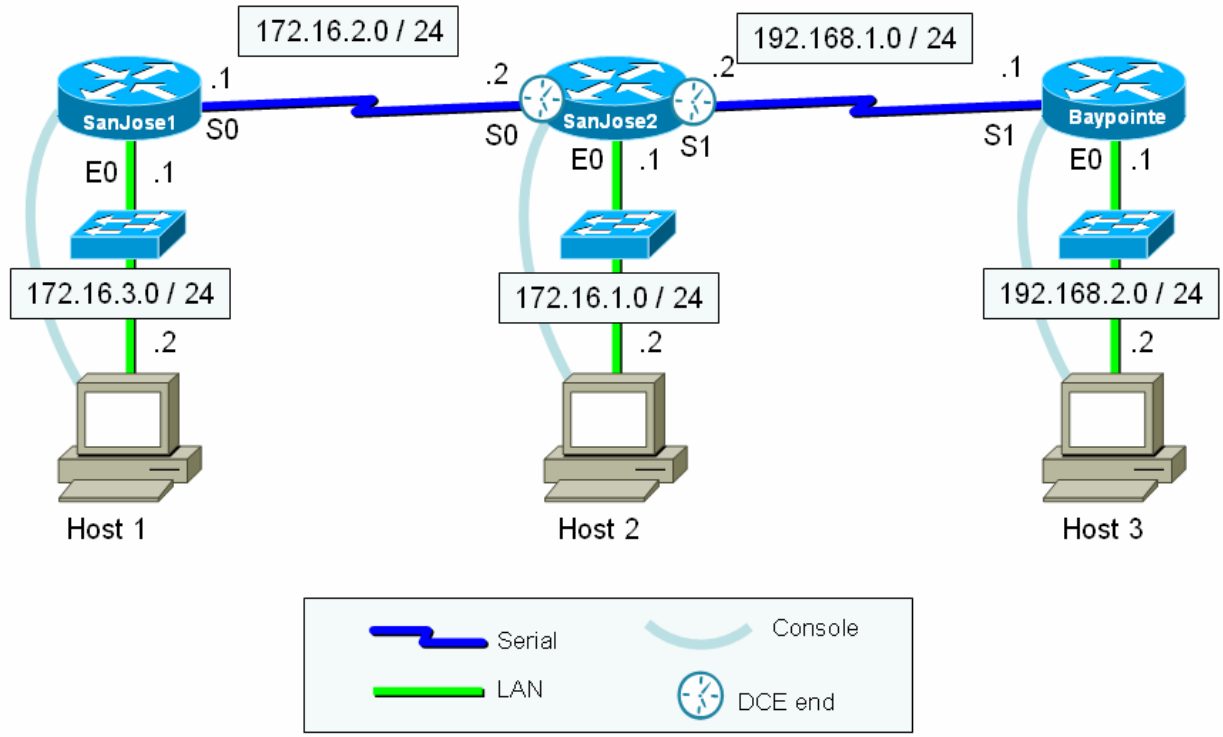
---

1 – Scenario

The objective of this lab is to learn how to configure static routing including default gateways. The scenario will include three routers configured as shown in the diagram below. Serial links are used between the routers and the Ethernet interfaces are used for LANs of single hosts.

2 – Diagram

Logical view:



3 – Running Configurations

SanJose 1	SanJose2	Baypointe
SanJose1#show run Building configuration... Current configuration : 1081 bytes ! version 12.2 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname SanJose1 ! enable secret 5 1eNrg$EWI.Yra3mZ16gZBiHFRj0. ! mmi polling-interval 60 no mmi auto-configure no mmi pvc mmi snmp-timeout 180 ip subnet-zero ! ! no ip domain-lookup ip host host1 172.16.1.10 ip host host2 172.16.3.10 ip host host3 192.168.2.10 ip host Baypointe 192.168.1.1 ip host SanJose2 172.16.2.1 ! ip audit notify log ip audit po max-events 100 ! ! ! ! interface BRI0 no ip address shutdown ! interface FastEthernet0 ip address 172.16.1.1 255.255.255.0 speed auto ! interface Serial0 ip address 172.16.2.2 255.255.255.0 no fair-queue clockrate 64000 ! interface Serial1 ip address 192.168.1.2 255.255.255.0 clockrate 64000 ! ip classless ip route 172.16.3.0 255.255.255.0 172.16.2.1 ip route 192.168.2.0 255.255.255.0 192.168.1.1 no ip http server ip pim bidir-enable ! !	SanJose2#show run Building configuration... Current configuration : 963 bytes ! version 12.2 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname SanJose2 ! enable secret 5 1GGV/$tNV7xIUARYha1Hs1cVnt0. ! mmi polling-interval 60 no mmi auto-configure no mmi pvc mmi snmp-timeout 180 ip subnet-zero ! ! no ip domain-lookup ip host baypointe 192.168.1.1 ip host host1 172.16.1.10 ip host host2 172.16.3.10 ip host host3 192.168.2.10 ip host SanJose1 172.16.2.2 ! ip audit notify log ip audit po max-events 100 ! ! ! ! interface BRI0 no ip address shutdown ! interface FastEthernet0 ip address 172.16.3.1 255.255.255.0 speed auto ! interface Serial0 ip address 172.16.2.1 255.255.255.0 ! interface Serial1 no ip address shutdown ! ip classless ip route 0.0.0.0 0.0.0.0 172.16.2.2 no ip http server ip pim bidir-enable ! ! ! banner motd ^C Warning - Authorized users only! ^C !	Baypointe# show run Building configuration... Current configuration : 966 bytes ! version 12.2 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname Baypointe ! enable secret 5 1Deop$sNWseKt9g6hb27y.Ac0Tw0 ! mmi polling-interval 60 no mmi auto-configure no mmi pvc mmi snmp-timeout 180 ip subnet-zero ! ! no ip domain-lookup ip host SanJose2 172.16.2.1 ip host host2 172.16.3.10 ip host host1 172.16.1.10 ip host SanJose1 192.168.1.2 ip host host3 192.168.2.10 ! ip audit notify log ip audit po max-events 100 ! ! ! ! interface BRI0 no ip address shutdown ! interface FastEthernet0 ip address 192.168.2.1 255.255.255.0 speed auto ! interface Serial0 no ip address shutdown ! interface Serial1 ip address 192.168.1.1 255.255.255.0 ! ip classless ip route 0.0.0.0 0.0.0.0 192.168.1.2 no ip http server ip pim bidir-enable ! ! ! banner motd ^C Warning - authorized users only! ^C !

! banner motd ^C Warning - authorized users only! ^C ! line con 0 password cisco login line aux 0 line vty 0 4 password cisco login ! no scheduler allocate end	line con 0 password cisco login line aux 0 line vty 0 4 password cisco login ! no scheduler allocate end	line con 0 password cisco login line aux 0 line vty 0 4 password cisco login ! no scheduler allocate end

SanJose1	SanJose1#show ip route Codes: C - connected, S - static, I - IGRP, 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, E - EGP i - IS-IS, 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 not set 172.16.0.0/24 is subnetted, 3 subnets C 172.16.1.0 is directly connected, FastEthernet0 C 172.16.2.0 is directly connected, Serial0 S 172.16.3.0 [1/0] via 172.16.2.1 C 192.168.1.0/24 is directly connected, Serial1 S 192.168.2.0/24 [1/0] via 192.168.1.1 SanJose1#
SanJose2	SanJose2# show ip route Codes: C - connected, S - static, I - IGRP, 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, E - EGP i - IS-IS, 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 172.16.2.2 to network 0.0.0.0 172.16.0.0/24 is subnetted, 2 subnets C 172.16.2.0 is directly connected, Serial0 C 172.16.3.0 is directly connected, FastEthernet0 S* 0.0.0.0/0 [1/0] via 172.16.2.2 SanJose2#
Baypointe	Baypointe#show ip route Codes: C - connected, S - static, I - IGRP, 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, E - EGP i - IS-IS, 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 192.168.1.2 to network 0.0.0.0 C 192.168.1.0/24 is directly connected, Serial1 C 192.168.2.0/24 is directly connected, FastEthernet0 S* 0.0.0.0/0 [1/0] via 192.168.1.2 Baypointe#

4 – Troubleshooting/Reflection

This lab went quite smoothly (unlike the last lab!). I can see how static routes would allow precise routing flow control. I also see that on large networks they would be very tedious and network changes could lead to both large and subtle routing problems.

5 – Lab Questions

What are the different classful networks?

172.16.0.0/16
192.168.2.0/24
192.168.1.0/24

Are there any subnets? If so, what are they?

172.16.1.0/24
172.16.2.0/24
172.16.3.0/24

Regarding initial static route configuration

- What routes to networks do you see?

SanJose2
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 3 subnets
S 172.16.1.0 [1/0] via 172.16.2.2
C 172.16.2.0 is directly connected, Serial0
C 172.16.3.0 is directly connected, FastEthernet0
S 192.168.1.0/24 [1/0] via 172.16.2.2
S 192.168.2.0/24 [1/0] via 172.16.2.2

SanJose1
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 3 subnets
C 172.16.1.0 is directly connected, FastEthernet0
C 172.16.2.0 is directly connected, Serial0
S 172.16.3.0 [1/0] via 172.16.2.1
C 192.168.1.0/24 is directly connected, Serial1
S 192.168.2.0/24 [1/0] via 192.168.1.1

Baypointe
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 3 subnets
S 172.16.1.0 [1/0] via 192.168.1.2
S 172.16.2.0 [1/0] via 192.168.1.2
S 172.16.3.0 [1/0] via 192.168.1.2
C 192.168.1.0/24 is directly connected, Serial1
C 192.168.2.0/24 is directly connected, FastEthernet0

- Which routes are static and which routes are directly connected?

SanJose2
- Static:
  - S 172.16.1.0 [1/0] via 172.16.2.2
  - S 192.168.1.0/24 [1/0] via 172.16.2.2
  - S 192.168.2.0/24 [1/0] via 172.16.2.2
- Directly connected:
  - C 172.16.2.0 is directly connected, Serial0
  - C 172.16.3.0 is directly connected, FastEthernet0

SanJose1
- Static:
  - S 172.16.3.0 [1/0] via 172.16.2.1
  - S 192.168.2.0/24 [1/0] via 192.168.1.1
- Directly connected:
  - C 172.16.1.0 is directly connected, FastEthernet0
  - C 172.16.2.0 is directly connected, Serial0
  - C 192.168.1.0/24 is directly connected, Serial1

Baypointe
- Static:
  - S 172.16.1.0 [1/0] via 192.168.1.2
  - S 172.16.2.0 [1/0] via 192.168.1.2
  - S 172.16.3.0 [1/0] via 192.168.1.2
- Directly connected:
  - C 192.168.1.0/24 is directly connected, Serial1
  - C 192.168.2.0/24 is directly connected, FastEthernet0

What is the administrative distance for a static route? 1
What is the administrative distance for a directly connected network? 0

How does the next-hop-ip-address help with the routing process?
It identifies the specific destination to send the packet for the next portion of the journey through the routers.
Does it give the entire route?

Not necessarily, the next-hop-ip-address only indicates the path to the next router. This could be an intermediate hop and the routing process would have to continue through each router along the path to the final destination network.

What is it actually doing regarding the routing of the packet?

The next-hop-ip-address is used if the packet's destination network in not on one of the local interfaces. The basic routing algorithm and use of the next-hop-ip-address operates as follows:

- Compute the destination network number of the destination IP address
- If the destination network matches a local interface, then the packet is forwarded out that interface.
- Otherwise if the destination network matches an entry in the routing table, then the packet is forwarded to the next-hop/interface specified in the routing table.

How does a packet get from Host 2 to Host 3?

When a framed packet arrives at a router interface, the data-link identifies in the frame destination and the address field is examined. If it contains either the identifier of the routers interface or a broadcast identifiers. The router strips off the frame and passes the enclosed packet to the network layer. At the network layer, the destination address of the packet is examined. If the destination addresses is either the I.P. address of the router's interface or all-hosts broadcast address, the protocol field of the packet is examined and the enclosed data is sent to the appropriate process. Any other destination address calls for routing of the packet is routable, the router will do a route table lookup for the correct address

Instead of a next-hop-ip-address, what else could you have used?

The alternative to using the next-hop address would be to specify one of the router interfaces instead.

What would you need to do if you added new networks or deleted/modified existing networks?

The routing tables would have to be updated to reflect the changes in the topology

Is there any way to summarize several static routes to multiple subnets into a single static route?

You can "supernet" individual subnets together by using a mask that applies to multiple subnets. For example you could specify all three 17.16.x.x subnets with a 255.255.0.0 mask.

Regarding summary static routes

- What routes to networks do you see?

SanJose2 (blue)
Gateway of last resort is not set

```
    172.16.0.0/24 is subnetted, 3 subnets
S      172.16.1.0 [1/0] via 172.16.2.2
C      172.16.2.0 is directly connected, Serial0
C      172.16.3.0 is directly connected, FastEthernet0
S    192.168.1.0/24 [1/0] via 172.16.2.2
```

S 192.168.2.0/24 [1/0] via 172.16.2.2

SanJose1 (white)
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 3 subnets
C 172.16.1.0 is directly connected, FastEthernet0
C 172.16.2.0 is directly connected, Serial0
S 172.16.3.0 [1/0] via 172.16.2.1
C 192.168.1.0/24 is directly connected, Serial1
S 192.168.2.0/24 [1/0] via 192.168.1.1

Baypointe (white)
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 3 subnets
S 172.16.1.0 [1/0] via 192.168.1.2
S 172.16.2.0 [1/0] via 192.168.1.2
S 172.16.3.0 [1/0] via 192.168.1.2
C 192.168.1.0/24 is directly connected, Serial1
C 192.168.2.0/24 is directly connected, FastEthernet0

- Which routes are static and which routes are directly connected?
  SanJose2 (blue)
  - Static:
    - S 172.16.1.0 [1/0] via 172.16.2.2
    - S 192.168.1.0/24 [1/0] via 172.16.2.2
    - S 192.168.2.0/24 [1/0] via 172.16.2.2
  - Directly connected:
    - C 172.16.2.0 is directly connected, Serial0
    - C 172.16.3.0 is directly connected, FastEthernet0

  SanJose1 (white)
  - Static:
    - S 172.16.3.0 [1/0] via 172.16.2.1
    - S 192.168.2.0/24 [1/0] via 192.168.1.1
  - Directly connected:
    - C 172.16.1.0 is directly connected, FastEthernet0
    - C 172.16.2.0 is directly connected, Serial0
    - C 192.168.1.0/24 is directly connected, Serial1

  Baypointe (red)
  - Static:
    - S 172.16.1.0 [1/0] via 192.168.1.2

    - S 172.16.2.0 [1/0] via 192.168.1.2
    - S 172.16.3.0 [1/0] via 192.168.1.2
- Directly connected:
    - C 192.168.1.0/24 is directly connected, Serial1
    - C 192.168.2.0/24 is directly connected, FastEthernet0

What is the administrative distance for a static route? 1
What is the administrative distance for a directly connected network? 0

How does the next-hop-ip-address help with the routing process?

It identifies the specific destination to send the packet for the next portion of the journey through the routers.

Does it give the entire route?

Not necessarily, the next-hop-ip-address only indicates the path to the next router. This could be an intermediate hop and the routing process would have to continue through each router along the path to the final destination network.

What is it actually doing regarding the routing of the packet?

The next-hop-ip-address is used if the packet's destination network in not on one of the local interfaces. The basic routing algorithm and use of the next-hop-ip-address operates as follows:

- Compute the destination network number of the destination IP address
- If the destination network matches a local interface, then the packet is forwarded out that interface.
- Otherwise if the destination network matches an entry in the routing table, then the packet is forwarded to the next-hop/interface specified in the routing table.

How does a packet get from Host 2 to Host 3?

When a framed packet arrives at a router interface, the data-link identifies in the frame destination and the address field is examined. If it contains either the identifier of the routers interface or a broadcast identifiers. The router strips off the frame and passes the enclosed packet to the network layer. At the network layer, the destination address of the packet is examined. If the destination addresses is either the I.P. address of the router's interface or all-hosts broadcast address, the protocol field of the packet is examined and the enclosed data is sent to the appropriate process. Any other destination address calls for routing of the packet is routable, the router will do a route table lookup for the correct address

Instead of a next-hop-ip-address, what else could you have used?

The alternative to using the next-hop address would be to specify one of the router interfaces instead.

What would you need to do if you added new networks or deleted/modified existing networks?

The routing tables would have to be updated to reflect the changes in the topology

Is there any way to summarize several static routes to multiple subnets into a single static route?

Yes all subnets can be summarized into their classful networks.

Do you think static routes still used even with dynamic routing (RIP, OSPF, etc.)?

Yes, It is common to use a static route where using a dynamic routing protocols would have disadvantages or where it just not needed. Static routes can be preferable for security, performance or administrative reasons. For example, stub networks are like dead-end streets with only one link to the main network.

Do you think default static routes still used even with dynamic routing (RIP, OSPF, etc.)?

Yes, default static routers are useful for connecting stub networks.

What is the disadvantage of doing this? How would a default static route be properly used in a real world network? (How would a company's network use a default route when connecting to the Internet?)

As with other summary routes, the trade off with default routes is a loss of routing detail. The stub routers have no way of knowing if a destination is unreachable. All packets are forwarded to hub router, and only then is the reachability determined. Some example real world scenarios of networks that would benefit from default static routes are branch offices and home networks. The branch offices all connect back into the larger corporate network. Home networks will have a single connection to their ISP's router to get internet access.

6 – Example Commands

```
!**********************
! Create static routes
!**********************

!set route using net hop address
conf t
  ip route 172.16.1.0 255.255.255.0 192.168.1.2
  no ip route 172.16.1.0 255.255.255.0 192.168.1.2

!Setup default routes
conf t
  ip route 0.0.0.0 0.0.0.0 192.168.1.2
  no ip route 0.0.0.0 0.0.0.0 192.168.1.2
  ip route 0.0.0.0 0.0.0.0 s1
  exit

!Alternate default GW that works with RIP and IGRP advertisements
conf t
  ip default-network 10.0.0.0
  exit

! to verify routes
show ip route
show run
```

CIS 82 LAB 5: RIP
Rich Simms
March 21, 2006

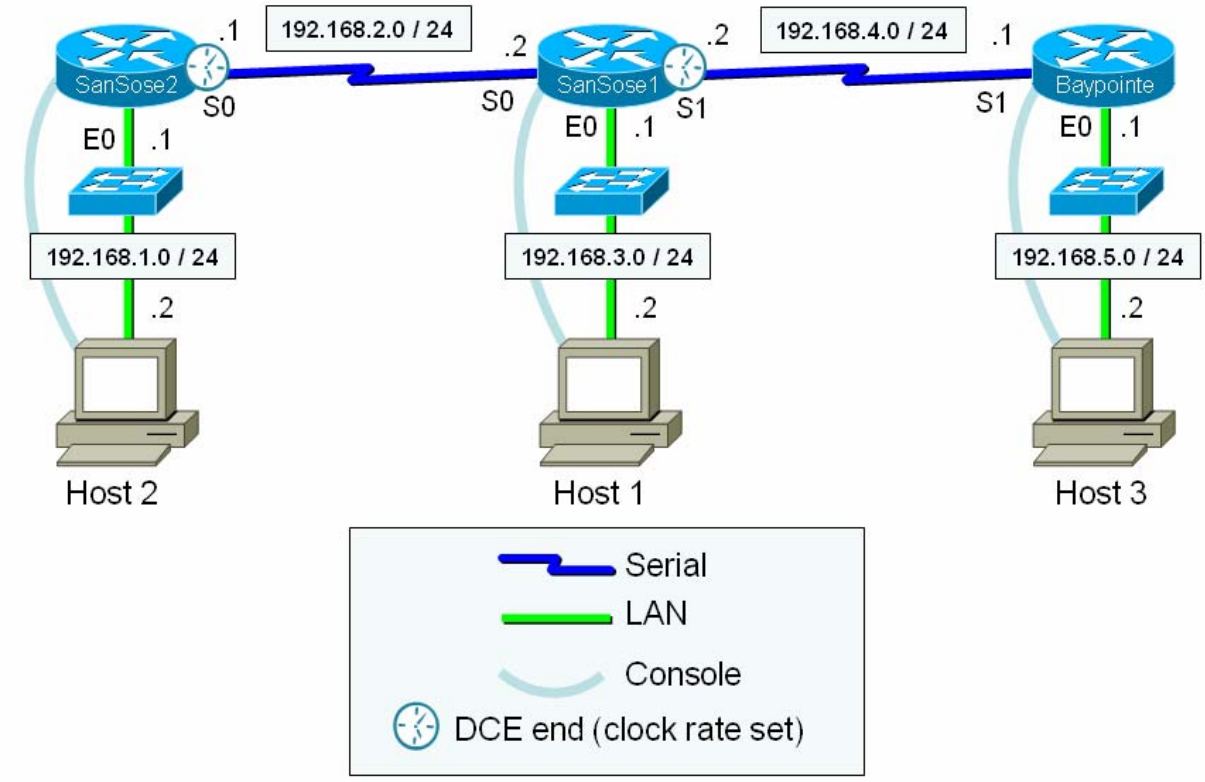
Teammates:

- Louis Arbanas
- Eric Jett
- Alf Popp

Scenario 1

Scenario 1 examines RIPv1 running on classful networks. This scenario uses three routers and three hosts as shown below. All five networks are classful. RIP v1 is configured on each router. There are no static routes required for convergence.

Scenario 1 Diagram



Scenario 1 Running Configurations

SanJose2	SanJose1	Baypointe

```
SanJose2#show run
Building configuration...

Current configuration : 671
bytes
!
version 12.1
no service single-slot-reload-
enable
service timestamps debug
uptime
service timestamps log uptime
no service password-encryption
!
hostname SanJose2
!
!memory-size iomem 15
ip subnet-zero
no ip domain-lookup
ip host Baypointe 192.168.4.1
ip host SanJose1 192.168.2.2
!
!
!
!
interface Serial0
 ip address 192.168.2.1
255.255.255.0
 no fair-queue
 clockrate 64000
!
interface Serial1
 no ip address
 shutdown
!
!
interface FastEthernet0
 ip address 192.168.1.1
255.255.255.0
 speed auto
!
router rip
 network 192.168.1.0
 network 192.168.2.0
!
!
ip classless
no ip http server
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
End
```

```
SanJose1#show run
Building configuration...

Current configuration : 705
bytes
!
version 12.1
no service single-slot-reload-
enable
service timestamps debug
uptime
service timestamps log uptime
no service password-encryption
!
hostname SanJose1
!
memory-size iomem 15
ip subnet-zero
no ip domain-lookup
ip host Baypointe 192.168.4.1
ip host SanJose2 192.168.2.1
!
!
!
!
interface Serial0
 ip address 192.168.2.2
255.255.255.0
 no fair-queue
!
!
interface Serial1
 ip address 192.168.4.2
255.255.255.0
 clockrate 64000
!
interface FastEthernet0
 ip address 192.168.3.1
255.255.255.0
 speed auto
!
router rip
 network 192.168.2.0
 network 192.168.3.0
 network 192.168.4.0
!
ip classless
no ip http server
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
End
```

```
Baypointe#show run
Building configuration...

Current configuration : 634
bytes
!
version 12.1
no service single-slot-reload-
enable
service timestamps debug
uptime
service timestamps log uptime
no service password-encryption
!
hostname Baypointe
!
!memory-size iomem 15
ip subnet-zero
ip host SanJose1 192.168.4.2
ip host SanJose2 192.168.2.1
!
!
!
!
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
!
!
interface Serial1
 ip address 192.168.4.1
255.255.255.0
!
!
interface FastEthernet0
 ip address 192.168.5.1
255.255.255.0
 speed auto
!
router rip
 network 192.168.4.0
 network 192.168.5.0
!
!
ip classless
no ip http server
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
End
```

Scenario 1 Routing Table Updates (Debug Traces)

SanJose2

```
00:15:47: RIP: build update entries
00:15:47:       network 192.168.2.0 metric 1
00:15:47:       network 192.168.3.0 metric 2
00:15:47:       network 192.168.4.0 metric 2
00:15:47:       network 192.168.5.0 metric 3
   . . .
00:15:47: RIP: sending v1 update to 255.255.255.255 via FastEthernet0 (192.168.1.1)
00:15:47: RIP: sending v1 update to 255.255.255.255 via Serial0 (192.168.2.1)
```

	. . . 00:16:03: RIP: received v1 update from 192.168.2.2 on Serial0 00:16:03: 192.168.3.0 in 1 hops 00:16:03: 192.168.4.0 in 1 hops 00:16:03: 192.168.5.0 in 2 hops
SanJose1	00:15:06: RIP: build update entries 00:15:06: network 192.168.1.0 metric 2 00:15:06: network 192.168.2.0 metric 1 00:15:06: network 192.168.4.0 metric 1 00:15:06: network 192.168.5.0 metric 2 . . . 00:15:06: RIP: sending v1 update to 255.255.255.255 via Serial0 (192.168.2.2) 00:15:06: RIP: sending v1 update to 255.255.255.255 via Serial1 (192.168.4.2) 00:15:35: RIP: sending v1 update to 255.255.255.255 via FastEthernet0 (192.168.3.1) . . . 00:15:33: RIP: received v1 update from 192.168.4.1 on Serial1 00:15:33: 192.168.5.0 in 1 hops 00:15:47: RIP: received v1 update from 192.168.2.1 on Serial0 00:15:47: 192.168.1.0 in 1 hops
Baypointe	00:15:25: RIP: build update entries 00:15:25: network 192.168.1.0 metric 3 00:15:25: network 192.168.2.0 metric 2 00:15:25: network 192.168.3.0 metric 2 00:15:25: network 192.168.4.0 metric 1 . . . 00:15:25: RIP: sending v1 update to 255.255.255.255 via FastEthernet0 (192.168.5.1) 00:15:25: RIP: sending v1 update to 255.255.255.255 via Serial1 (192.168.4.1) . . . 00:15:27: RIP: received v1 update from 192.168.4.2 on Serial1 00:15:27: 192.168.1.0 in 2 hops 00:15:27: 192.168.2.0 in 1 hops 00:15:27: 192.168.3.0 in 1 hops

Scenario 1 Routing Tables

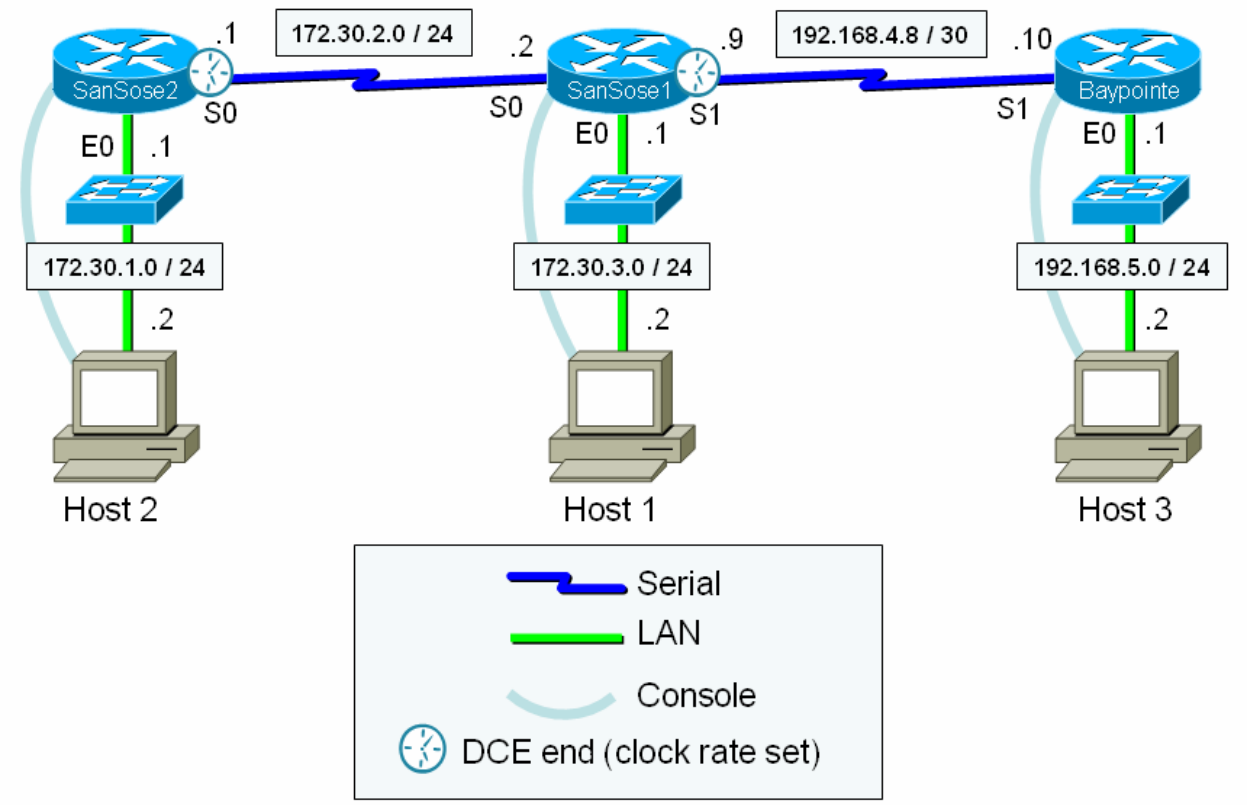
SanJose2	SanJose2#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, 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 not set R 192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:06, Serial0 R 192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:06, Serial0 C 192.168.1.0/24 is directly connected, FastEthernet0 C 192.168.2.0/24 is directly connected, Serial0 R 192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:06, Serial0 SanJose2#
SanJose1	SanJose1#show ip route Codes: C - connected, S - static, I - IGRP, 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, E - EGP i - IS-IS, 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 not set C 192.168.4.0/24 is directly connected, Serial1 R 192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial1

	R 192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:17, Serial0 C 192.168.2.0/24 is directly connected, Serial0 C 192.168.3.0/24 is directly connected, FastEthernet0 SanJose1#
Baypointe	Baypointe#show ip route Codes: C - connected, S - static, I - IGRP, 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, E - EGP i - IS-IS, 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 not set C 192.168.4.0/24 is directly connected, Serial1 C 192.168.5.0/24 is directly connected, FastEthernet0 R 192.168.1.0/24 [120/2] via 192.168.4.2, 00:00:19, Serial1 R 192.168.2.0/24 [120/1] via 192.168.4.2, 00:00:19, Serial1 R 192.168.3.0/24 [120/1] via 192.168.4.2, 00:00:19, Serial1 Baypointe#

Scenario 2

Scenario 2 examines RIPv1 running on subnets and between classful networks. This scenario uses three routers and three hosts as shown below. Now there are only three classful networks (172.30.0.0, 192.168.4.0 and 192.168.5.0) and some are subnetted. RIP v1 is configured on each router. This scenario is pushing RIP v1 to its limits because it is passing subnets in its routing advertisements but it is **not** including subnet masks. The router is applying it's own subnet mask to these subnets based on how its own matching interface is configured. There are no static routes required for convergence.

Scenario 2 Diagram



Scenario 2 Running Configurations

SanJose2	SanJose1	Baypointe
SanJose2#show run Building configuration... Current configuration : 632 bytes ! version 12.1 no service single-slot-reload- enable service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname SanJose2 ! ! ! ! ! ! memory-size iomem 15 ip subnet-zero no ip domain-lookup ip host SanJose1 172.30.2.2 ip host Baypointe 192.168.4.10 ! ! ! !	**SanJose1#show run** **Building configuration...** **Current configuration : 668** **bytes** **!** **version 12.1** **no service single-slot-reload-** **enable** **service timestamps debug** **uptime** **service timestamps log uptime** **no service password-encryption** **!** **hostname SanJose1** **!** **!** **!** **!** **!** **!** **memory-size iomem 15** **ip subnet-zero** **no ip domain-lookup** **ip host SanJose2 172.30.2.1** **ip host Baypointe 192.168.4.10** **!** **!** **!** **!** **interface Serial0**	Baypointe#show run Building configuration... Current configuration : 641 bytes ! version 12.1 no service single-slot-reload- enable service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname Baypointe ! ! ! ! ! ! memory-size iomem 15 ip subnet-zero no ip domain-lookup ip host SanJose1 192.168.4.9 ip host SanJose2 172.30.2.1 ! ! ! ! interface Serial0

```
interface Serial0
 ip address 172.30.2.1
255.255.255.0
 clockrate 64000
!
interface Serial1
 no ip address
 shutdown
!
interface FastEthernet0
 ip address 172.30.1.1
255.255.255.0
 speed auto
!
router rip
 network 172.30.0.0
!
ip classless
no ip http server
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

```
 ip address 172.30.2.2
255.255.255.0
!
interface Serial1
 ip address 192.168.4.9
255.255.255.252
 clockrate 64000
!
interface FastEthernet0
 ip address 172.30.3.1
255.255.255.0
 speed auto
!
router rip
 network 172.30.0.0
 network 192.168.4.0
!
ip classless
no ip http server
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

```
 no ip address
 shutdown
!
interface Serial1
 ip address 192.168.4.10
255.255.255.252
!
interface FastEthernet0
 ip address 192.168.5.1
255.255.255.0
 speed auto
!
router rip
 network 192.168.4.0
 network 192.168.5.0
!
ip classless
no ip http server
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

Scenario 2 Routing Table Updates (Debug Traces)

SanJose2

```
00:11:09: RIP: build update entries
00:11:09:       subnet 172.30.2.0 metric 1
00:11:09:       subnet 172.30.3.0 metric 2
00:11:09:       network 192.168.4.0 metric 2
00:11:09:       network 192.168.5.0 metric 3
   . . .
00:11:09: RIP: sending v1 update to 255.255.255.255 via Serial0 (172.30.2.1)
00:11:35: RIP: sending v1 update to 255.255.255.255 via FastEthernet0 (172.30.1.1)
   . . .
00:11:28: RIP: received v1 update from 172.30.2.2 on Serial0
00:11:28:      172.30.3.0 in 1 hops
00:11:28:      192.168.4.0 in 1 hops
00:11:28:      192.168.5.0 in 2 hops
```

SanJose1

```
00:11:25: RIP: build update entries
00:11:25:       subnet 172.30.1.0 metric 2
00:11:25:       subnet 172.30.2.0 metric 1
00:11:25:       network 192.168.4.0 metric 1
00:11:25:       network 192.168.5.0 metric 2
   . . .
00:11:25: RIP: sending v1 update to 255.255.255.255 via FastEthernet0 (172.30.3.1)
00:11:55: RIP: sending v1 update to 255.255.255.255 via Serial0 (172.30.2.2)
00:11:25: RIP: sending v1 update to 255.255.255.255 via Serial1 (192.168.4.9)
   . . .
00:12:00: RIP: received v1 update from 172.30.2.1 on Serial0
00:12:00:      172.30.1.0 in 1 hops
00:11:55: RIP: received v1 update from 192.168.4.10 on Serial1
00:11:55:      192.168.5.0 in 1 hops
```

Baypointe

```
00:12:20: RIP: build update entries
00:12:20:       network 172.30.0.0 metric 2
00:12:20:       network 192.168.4.0 metric 1
   . . .
00:12:20: RIP: sending v1 update to 255.255.255.255 via FastEthernet0 (192.168.5.1)
00:12:20: RIP: sending v1 update to 255.255.255.255 via Serial1 (192.168.4.10)
   . . .
```

	00:12:20: RIP: received v1 update from 192.168.4.9 on Serial1 00:12:20: 172.30.0.0 in 1 hops

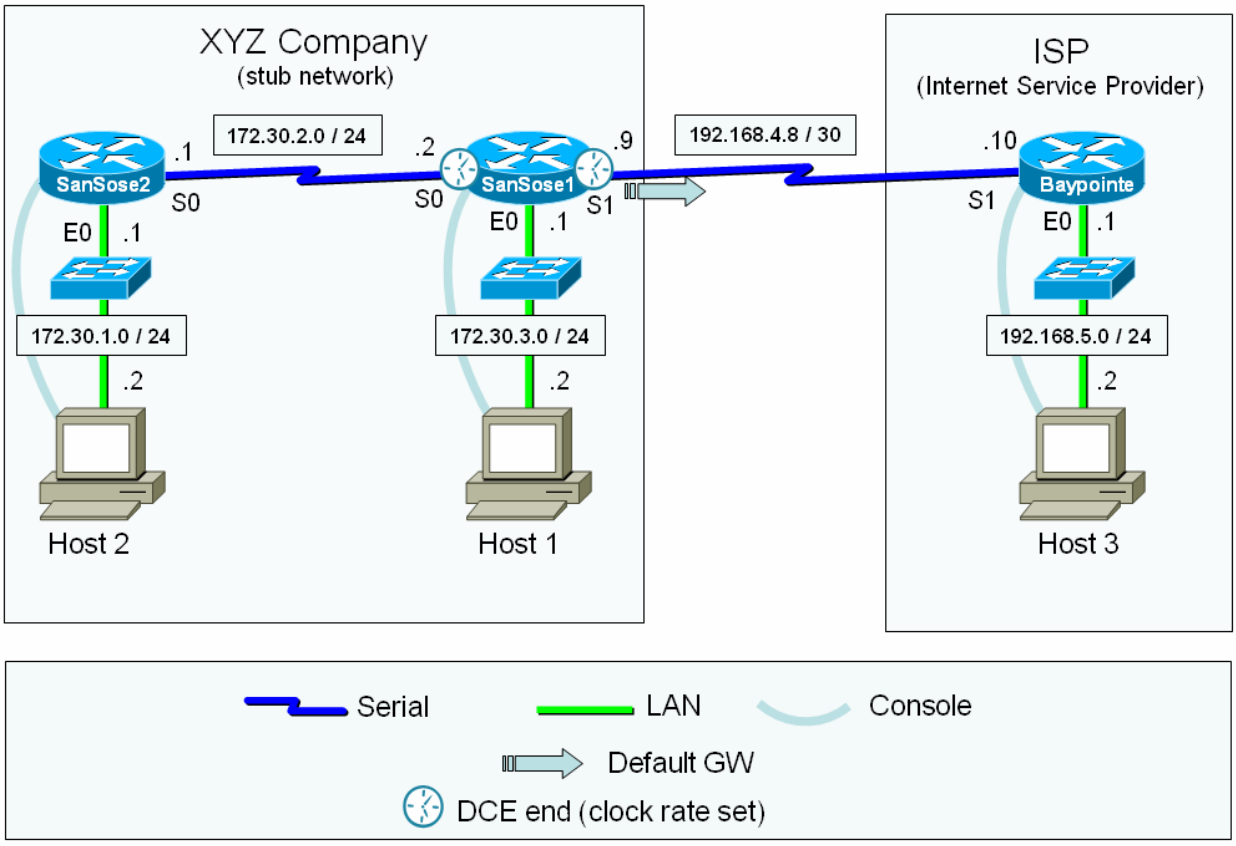
Scenario 2 Routing Tables

SanJose2	SanJose2#show ip route Codes: C - connected, S - static, I - IGRP, 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, E - EGP i - IS-IS, 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 not set 172.30.0.0/24 is subnetted, 3 subnets C 172.30.2.0 is directly connected, Serial0 R 172.30.3.0 [120/1] via 172.30.2.2, 00:00:01, Serial0 C 172.30.1.0 is directly connected, FastEthernet0 R 192.168.4.0/24 [120/1] via 172.30.2.2, 00:00:01, Serial0 R 192.168.5.0/24 [120/2] via 172.30.2.2, 00:00:01, Serial0 SanJose2#
SanJose1	**SanJose1#show ip route** **Codes: C - connected, S - static, I - IGRP, 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, E - EGP** **i - IS-IS, 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 not set** **172.30.0.0/24 is subnetted, 3 subnets** **C 172.30.2.0 is directly connected, Serial0** **C 172.30.3.0 is directly connected, FastEthernet0** **R 172.30.1.0 [120/1] via 172.30.2.1, 00:00:04, Serial0** **192.168.4.0/30 is subnetted, 1 subnets** **C 192.168.4.8 is directly connected, Serial1** **R 192.168.5.0/24 [120/1] via 192.168.4.10, 00:00:11, Serial1** **SanJose1#**
Baypointe	Baypointe#show ip route Codes: C - connected, S - static, I - IGRP, 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, E - EGP i - IS-IS, 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 not set R 172.30.0.0/16 [120/1] via 192.168.4.9, 00:00:17, Serial1 192.168.4.0/30 is subnetted, 1 subnets C 192.168.4.8 is directly connected, Serial1 C 192.168.5.0/24 is directly connected, FastEthernet0 Baypointe#

Scenario 3

Scenario 2 examines RIPv1 running on a stub network. SanJose1 and SanJose2 make up the "stub network" of the small XYZ Company as shown below. This company has an internet connection via their ISP which uses the Baypointe router. XYZ company uses the 172,30.00 classful network which is subnetted into 172.30.1.0 / 24, 172.30.2.0 / 24 and 172.30.3.0 / 24. The ISP has a static route to the 172.30.0.0 network on Baypointe. A default route to the ISP is put on the SanJose1 router. This default route gets propagated to SanJose2 using the `default-information originate` command.

Scenario 3 Diagram



Scenario 3 Running Configurations

SanJose2	SanJose1	Baypointe
version 12.0 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname SanJose2 ! enable secret 5 1BkJ2$cfWJnrCeH9BBU3hENDIfx1	version 12.0 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname SanJose1 ! enable secret 5 1tRct$QYX8VqJsUuzvBPD.9Kwfa/	version 12.0 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname Baypointe ! enable secret 5 1zuER$SILetB1cWiwXIPuW.KsyC1

```
!
ip subnet-zero
ip host Baypointe 192.168.4.10
ip host SanJose1 172.30.2.2
!
!
!
process-max-time 200
!
interface Ethernet0
 ip address 172.30.1.1
255.255.255.0
 no ip directed-broadcast
!
interface Serial0
 ip address 172.30.2.1
255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 no fair-queue
!
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
!
interface BRI0
 no ip address
 no ip directed-broadcast
 shutdown
!!
router rip
 network 172.30.0.0
!
!
ip classless
!
!
!
banner motd ^C
Long live old reliable
routers! ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

```
!
ip subnet-zero
no ip domain-lookup
ip host SanJose2 172.30.2.1
ip host Baypointe 192.168.4.10
!
!
process-max-time 200
!
interface Ethernet0
 ip address 172.30.3.1
255.255.255.0
 no ip directed-broadcast
!
interface Serial0
 ip address 172.30.2.2
255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 no fair-queue
 clockrate 64000
!
interface Serial1
 ip address 192.168.4.9
255.255.255.252
 no ip directed-broadcast
 clockrate 64000
!
interface BRI0
 no ip address
 no ip directed-broadcast
 shutdown
!
router rip
 network 172.30.0.0
 default-information originate
!
ip classless
ip route 0.0.0.0 0.0.0.0
Serial1
!
banner motd ^C
Long live old reliable
routers! ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

```
!
ip subnet-zero
no ip domain-lookup
ip host SanJose1 192.168.4.9
ip host SanJose2 172.30.2.1
!
!
process-max-time 200
!
interface Ethernet0
 ip address 192.168.5.1
255.255.255.0
 no ip directed-broadcast
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
!
!
!
interface Serial1
 ip address 192.168.4.10
255.255.255.252
 no ip directed-broadcast
!
!
interface BRI0
 no ip address
 no ip directed-broadcast
 shutdown
!
!
!
!
!
ip classless
ip route 172.30.0.0
255.255.0.0 Serial1
!
banner motd ^C
Long live reliable old
routers! ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Scenario 3 Routing Table Updates (Debug Traces)

SanJose2	00:48:20: RIP: sending v1 update to 255.255.255.255 via Serial0 (172.30.2.1) 00:48:20: subnet 172.30.1.0, metric 1 . . . 00:49:01: RIP: received v1 update from 172.30.2.2 on Serial0 00:49:01: 172.30.3.0 in 1 hops 00:49:01: 0.0.0.0 in 1 hops 00:48:32: RIP: ignored v1 update from bad source 172.30.3.1 on Ethernet0
SanJose1	00:49:24: RIP: sending v1 update to 255.255.255.255 via Serial0 (172.30.2.2) 00:49:24: subnet 172.30.3.0, metric 1 00:49:24: default, metric 1 . . . 00:49:39: RIP: received v1 update from 172.30.2.1 on Serial0 00:49:39: 172.30.1.0 in 1 hops
Baypointe	RIP not enabled

Scenario 3 Routing Tables

SanJose2	SanJose2#show ip route Codes: C - connected, S - static, I - IGRP, 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, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default U - per-user static route, o - ODR Gateway of last resort is 172.30.2.2 to network 0.0.0.0 172.30.0.0/24 is subnetted, 3 subnets C 172.30.2.0 is directly connected, Serial0 R 172.30.3.0 [120/1] via 172.30.2.2, 00:00:03, Serial0 C 172.30.1.0 is directly connected, Ethernet0 R* 0.0.0.0/0 [120/1] via 172.30.2.2, 00:00:03, Serial0 SanJose2#
SanJose1	SanJose1#show ip route Codes: C - connected, S - static, I - IGRP, 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, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default U - per-user static route, o - ODR Gateway of last resort is 0.0.0.0 to network 0.0.0.0 172.30.0.0/24 is subnetted, 3 subnets C 172.30.2.0 is directly connected, Serial0 C 172.30.3.0 is directly connected, Ethernet0 R 172.30.1.0 [120/1] via 172.30.2.1, 00:00:20, Serial0 192.168.4.0/30 is subnetted, 1 subnets C 192.168.4.8 is directly connected, Serial1 S* 0.0.0.0/0 is directly connected, Serial1 SanJose1#
Baypointe	Baypointe#show ip route Codes: C - connected, S - static, I - IGRP, 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, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default U - per-user static route, o - ODR Gateway of last resort is not set S 172.30.0.0/16 is directly connected, Serial1 192.168.4.0/30 is subnetted, 1 subnets C 192.168.4.8 is directly connected, Serial1 C 192.168.5.0/24 is directly connected, Ethernet0 Baypointe#

4 – Troubleshooting/Reflection

I did scenarios 1 & 2 on NetLab. However it was not possible to complete scenario 3 on NetLab because the `default-information originate` command did not result in propagating the default route via RIP. So for Scenario 3 I used the older routers (Istanbul Pod) in the lab and it worked fine.

NetLab uses IOS v12.0 and I noticed the debug trace output differs slightly from the examples in the original lab. With v12.0 you can see the "build update entries" but you don't see the actual entries that are being sent out each interface.

5 – Lab Questions

No unanswered questions in this lab.

6 – Example Commands

```
! Configuring RIP v1
conf t
  router rip
    ! add only directly connected classful network for RIP to advertise
    network 192.168.4.0
    network 172.30.0.0
    ! undo any mistakes
    no network 172.30.0.0

    !propogate default GW (worked on lab routers, not on NetLAb)
    default-information originate

    !propogate default GW (works on NetLab & lab)
    redistribute static

    !suppress announcements to stub networks
    passive-interface e0

! tracing RIP updates
debug ip rip
undebug ip rip
undebug all

! Disabling RIP
conf t
  no router rip

! Suppressiong IOS annoyances
```

```
line con 0
  login
  password cisco
  logging synchronous
  exec-timeout 0 0
  exit
```

CIS 82 LAB 6: IGRP
Rich Simms
March 28, 2006

Teammates:

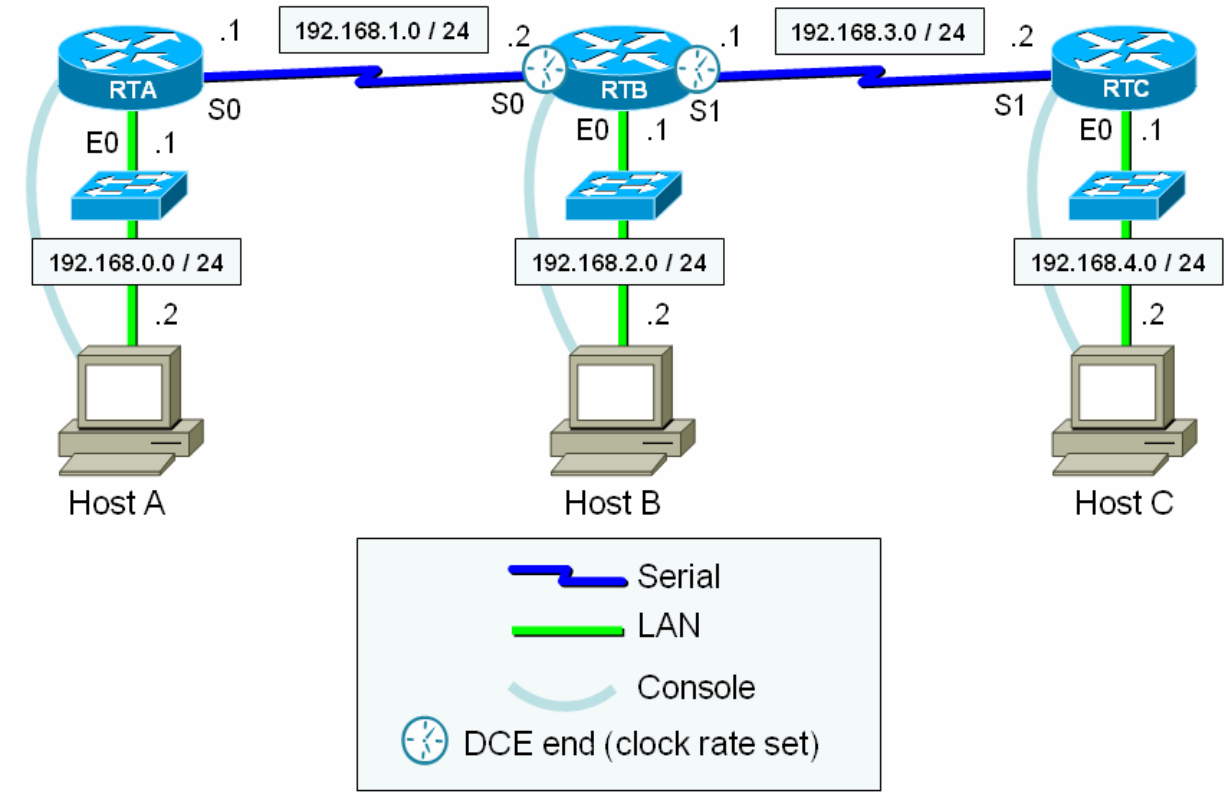
- Louis Arbanas
- Eric Jett
- Alf Popp

---

1 - Scenario

The objective for this lab is to learn how to configure IGRP. IGRP is classful like RIPv1. RIP's metric is based on number of hops. IGRP uses instead a composite metric based on bandwidth, delay, reliability, and load. The scenario below uses the standard three router setup we have been using in the other labs. All networks configured are classful.

2 - Diagram



3 - Running Configurations

RTA

```
RTA#show run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug
uptime
service timestamps log uptime
no service password-encryption
!
hostname RTA
!
enable secret 5
$1$XgEF$gXHkoRSkZAePlVe.8eO8u.
!
ip subnet-zero
no ip domain-lookup
ip host RTC 192.168.3.2
ip host RTB 192.168.1.2
!
process-max-time 200
!
interface Ethernet0
 ip address 192.168.0.1
255.255.255.0
 no ip directed-broadcast
!
interface Serial0
 ip address 192.168.1.1
255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 no fair-queue
!
!
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
!
interface BRI0
 no ip address
 no ip directed-broadcast
 shutdown
!
router igrp 364
 timers basic 15 45 0 60
 network 192.168.0.0
 network 192.168.1.0
 no metric holddown
 metric maximum-hops 50
!
!
ip classless
!
banner motd ^C
Long live old reliable
routers! ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
```

RTB

```
RTB#show run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug
uptime
service timestamps log uptime
no service password-encryption
!
hostname RTB
!
enable secret 5
$1$ot4Q$VyS3wAfJXb//d/RRETwVG.
!
ip subnet-zero
no ip domain-lookup
ip host RTA 192.168.1.1
ip host RTC 192.168.3.2
!
process-max-time 200
!
interface Ethernet0
 ip address 192.168.2.1
255.255.255.0
 no ip directed-broadcast
!
interface Serial0
 bandwidth 128
 ip address 192.168.1.2
255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 no fair-queue
 clockrate 64000
!
interface Serial1
 ip address 192.168.3.1
255.255.255.0
 no ip directed-broadcast
 clockrate 64000
!
interface BRI0
 no ip address
 no ip directed-broadcast
 shutdown
!
router igrp 364
 timers basic 15 45 0 60
 network 192.168.1.0
 network 192.168.2.0
 network 192.168.3.0
 no metric holddown
 metric maximum-hops 50
!
ip classless
!
banner motd ^C
Long live old reliable
routers! ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
```

RTC

```
RTC#show run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug
uptime
service timestamps log uptime
no service password-encryption
!
hostname RTC
!
enable secret 5
$1$VT6C$EdTUXwXfnA0si4tSgBTOt/
!
ip subnet-zero
no ip domain-lookup
ip host RTB 192.168.3.1
ip host RTA 192.168.1.1
!
process-max-time 200
!
interface Ethernet0
 ip address 192.168.4.1
255.255.255.0
 no ip directed-broadcast
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 no fair-queue
!
!
!
interface Serial1
 ip address 192.168.3.2
255.255.255.0
 no ip directed-broadcast
!
!
interface BRI0
 no ip address
 no ip directed-broadcast
 shutdown
!
router igrp 364
 timers basic 15 45 0 60
 network 192.168.3.0
 network 192.168.4.0
 no metric holddown
 metric maximum-hops 50
!
!
ip classless
!
banner motd ^CC
Long live reliable old
routers! ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
```

```
line vty 0 4
 password cisco
 login
!
end

RTA#
```

```
line vty 0 4
 password cisco
 login
!
end

RTB#
```

```
line vty 0 4
 password cisco
 login
!
end

RTC#
```

Routing Tables

RTA

```
RTA#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

I    192.168.4.0/24 [100/10576] via 192.168.1.2, 00:00:23, Serial0
C    192.168.0.0/24 is directly connected, Ethernet0
C    192.168.1.0/24 is directly connected, Serial0
I    192.168.2.0/24 [100/8576] via 192.168.1.2, 00:00:23, Serial0
I    192.168.3.0/24 [100/10476] via 192.168.1.2, 00:00:23, Serial0
RTA#
```

RTB

```
RTB#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

I    192.168.4.0/24 [100/8576] via 192.168.3.2, 00:00:08, Serial1
I    192.168.0.0/24 [100/8576] via 192.168.1.1, 00:00:25, Serial0
C    192.168.1.0/24 is directly connected, Serial0
C    192.168.2.0/24 is directly connected, Ethernet0
C    192.168.3.0/24 is directly connected, Serial1
RTB#
```

RTC

```
RTC#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

C    192.168.4.0/24 is directly connected, Ethernet0
I    192.168.0.0/24 [100/10576] via 192.168.3.1, 00:00:18, Serial1
I    192.168.1.0/24 [100/10476] via 192.168.3.1, 00:00:18, Serial1
I    192.168.2.0/24 [100/8576] via 192.168.3.1, 00:00:18, Serial1
C    192.168.3.0/24 is directly connected, Serial1
RTC#
```

IGRP debug tracing (on RTB)

```
RTB#debug ip igrp events
IGRP event debugging is on
RTB#debug ip igrp transactions
IGRP protocol debugging is on
```

```
   . . .
00:30:53: IGRP: received update from invalid source 192.168.0.1 on Ethernet0
00:31:08: IGRP: received update from invalid source 192.168.4.1 on Ethernet0
```
(note: using one switch for multiple logical networks and these updates are broadcasts)
```
   . . .
00:30:53: IGRP: received update from 192.168.1.1 on Serial0
00:30:53:       network 192.168.0.0, metric 8576 (neighbor 1100)
00:30:53: IGRP: Update contains 0 interior, 1 system, and 0 exterior routes.
00:30:53: IGRP: Total routes in update: 1
   . . .
00:31:08: IGRP: received update from 192.168.3.2 on Serial1
00:31:08:       network 192.168.4.0, metric 8576 (neighbor 1100)
00:31:08: IGRP: Update contains 0 interior, 1 system, and 0 exterior routes.
00:31:08: IGRP: Total routes in update: 1
   . . .
00:31:24: IGRP: sending update to 255.255.255.255 via Ethernet0 (192.168.2.1)
00:31:24:       network 192.168.4.0, metric=8576
00:31:24:       network 192.168.0.0, metric=8576
00:31:24:       network 192.168.1.0, metric=8476
00:31:24:       network 192.168.3.0, metric=8476
00:31:24: IGRP: Update contains 0 interior, 4 system, and 0 exterior routes.
00:31:24: IGRP: Total routes in update: 4
   . . .
00:31:24: IGRP: sending update to 255.255.255.255 via Serial0 (192.168.1.2)
00:31:24:       network 192.168.4.0, metric=8576
00:31:24:       network 192.168.2.0, metric=1100
00:31:24:       network 192.168.3.0, metric=8476
00:31:24: IGRP: Update contains 0 interior, 3 system, and 0 exterior routes.
00:31:24: IGRP: Total routes in update: 3
   . . .
00:31:24: IGRP: sending update to 255.255.255.255 via Serial1 (192.168.3.1)
00:31:24:       network 192.168.0.0, metric=8576
00:31:24:       network 192.168.1.0, metric=8476
00:31:24:       network 192.168.2.0, metric=1100
00:31:24: IGRP: Update contains 0 interior, 3 system, and 0 exterior routes.
00:31:24: IGRP: Total routes in update: 3
   . . .
00:32:07: IGRP: received update from 192.168.1.1 on Serial0
00:32:07:       network 192.168.0.0, metric 8576 (neighbor 1100)
00:32:07: IGRP: Update contains 0 interior, 1 system, and 0 exterior routes.
00:32:07: IGRP: Total routes in update: 1
   . . .
00:32:38: IGRP: received update from 192.168.3.2 on Serial1
00:32:38:       network 192.168.4.0, metric 8576 (neighbor 1100)
00:32:38: IGRP: Update contains 0 interior, 1 system, and 0 exterior routes.
00:32:38: IGRP: Total routes in update: 1
00:32:46:       network 192.168.3.0, metric=8476

RTB#undebug all
All possible debugging has been turned off
```

4 – Troubleshooting/Reflection

This lab took the least amount of time of all the labs. I built and tested the basic router configurations using PacketTracer then "pasted" the these configurations into the actual lab consoles. Once the basic configurations were completed I did the IGRP configuration manually.

I can see how IGRP would address RIP limitations in larger networks. The metrics used would result in better path selection and the limit of 15 hops gets extended to 255.

Gerlinde showed me how to use IOS help command (shown below) to determine the maximum number of hops for IGRP. The allowable range gets printed with the "?" after `metric maximum-hops.`

I also see now why we get "invalid source" routing updates. This is due to updates being broadcast by the routers out their Ethernet interfaces into a common switch. The broadcasts are flooded by the switch to all ports which are then picked up as inputs to the other routers Ethernet interfaces.

5 – Lab Questions

Use the command show ip protocols

```
RTB#show ip protocols
Routing Protocol is "igrp 364"
  Sending updates every 90 seconds, next due in 31 seconds
  Invalid after 270 seconds, hold down 280, flushed after 630
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  IGRP maximum hopcount 100
  IGRP maximum metric variance 1
  Redistributing: igrp 364
  Routing for Networks:
    192.168.1.0
    192.168.2.0
    192.168.3.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.1.1          100      00:00:04
    192.168.3.2          100      00:00:52
  Distance: (default is 100)
```

1. How often are IGRP updates being sent? 90 seconds
2. When is the next update due? 31 seconds
3. How long will it take for a route to become invalid? 270 seconds
4. How long will the route remain in hold down, or wait to accept a new route? 280 seconds
5. What is the value of the K-1 and the K-2 constants? K1=1, K2=0
6. What is the default maximum hop count? 100
7. What is the maximum hop count? 255

```
RTC(config-router)#metric maximum-hops ?
```

```
        <1-255>  Hop count
```

6 – Example Commands

```
!*******************
! Configuring IGRP
!*******************

config t
  router igrp 10
    network 192.15.25.0
    network 172.30.0.0

! Trace IGRP updates
debug ip igrp events
debug ip igrp transactions
! Changing bandwidth
conf t
  int s0
    bandwidth 128

! Configure IGRP timers for fast convergence
conf t
  router igrp 364
    timers basic 15 45 0 60
    no metric holddown
    metric maximum-hop 50
```

CIS 82 LAB 7: Access Control Lists
Rich Simms
May 2, 2006

Teammates:

- Louis Arbanas
- Eric Jett
- Alf Popp

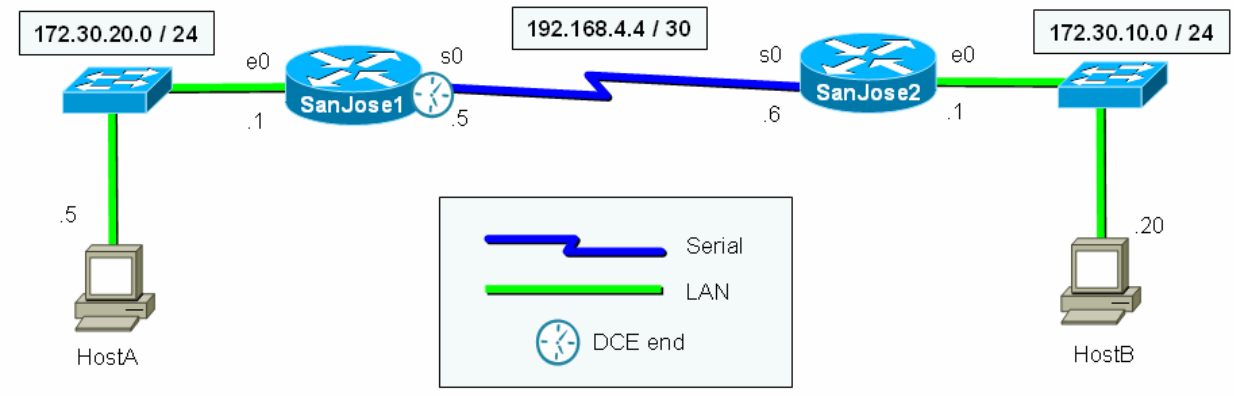
---

1 – Scenario

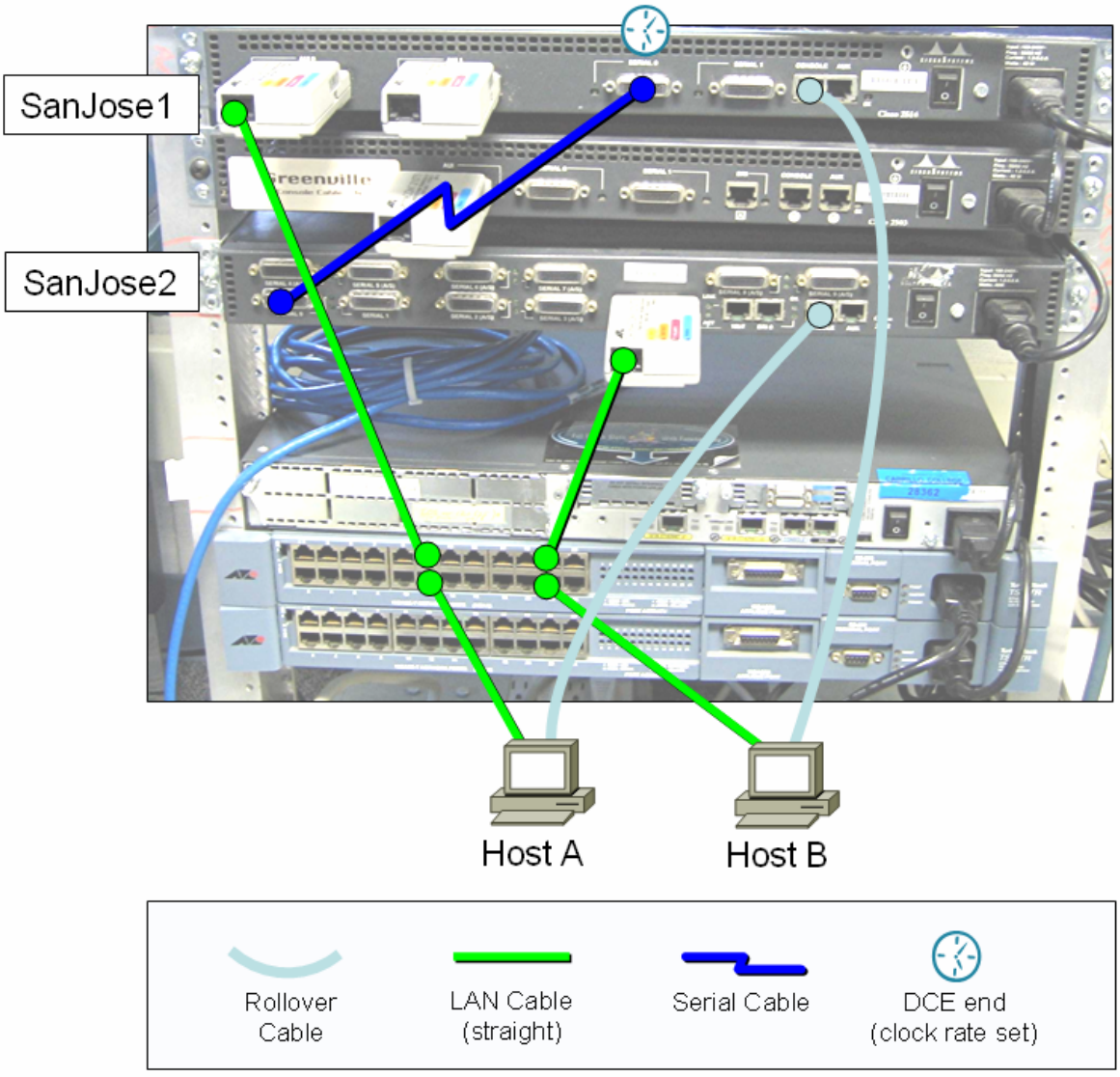
The objective of this lab was to learn how to implement access control lists. This lab utilizes two routers and two hosts as shown in the diagram below. The routers were connected by a serial link. A variety of access control lists are applied including standard, extended and named.

2 – Diagram

Logical view:



Physical view:



3 – Running Configurations

Task 1: Create a standard ACL that will deny all packets from HostB from reaching the 172.30.20.0/24 network.

```
SanJose1#show run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SanJose1
!
enable secret 5 $1$UcCf$ScmX8KHd5iSLgZWXM3iuH.
!
ip subnet-zero
no ip domain-lookup
ip host SanJose1-s0 192.168.4.5
ip host SanJose1-e0 172.30.20.1
ip host HostA 172.30.20.5
ip host SanJose2-s0 192.168.4.6
ip host SanJose2-e0 172.30.10.1
ip host HostB 172.30.10.20
!
!
process-max-time 200
!
interface Ethernet0
 description Connection to SanJose1 LAN
 ip address 172.30.20.1 255.255.255.0
 no ip directed-broadcast
!
   < output omitted >
!
interface Serial0
 description Connection to SanJose2
 ip address 192.168.4.5 255.255.255.252
 ip access-group 1 in
 no ip directed-broadcast
 no ip mroute-cache
 no fair-queue
 clockrate 64000
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
!
!
router rip
 version 2
 network 172.30.0.0
 network 192.168.4.0
 no auto-summary
!
ip classless
!
access-list 1 deny   172.30.10.20
access-list 1 permit any
```

```
SanJose2#show run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SanJose2
!
enable secret 5 $1$RuW.$yihlCP4TiysBmhJtRSPjc0
!
ip subnet-zero
no ip domain-lookup
ip host SanJose1-s0 192.168.4.5
ip host SanJose1-e0 172.30.20.1
ip host HostA 172.30.20.5
ip host SanJose2-s0 192.168.4.6
ip host SanJose2-e0 172.30.10.1
ip host HostB 172.30.10.20
!
!
process-max-time 200
!
interface Ethernet0
 description Connection to SanJose2 LAN
 ip address 172.30.10.1 255.255.255.0
 no ip directed-broadcast
!
!
!
interface Serial0
 description Connection to SanJose1
 ip address 192.168.4.6 255.255.255.252
 no ip directed-broadcast
 no ip mroute-cache
 no fair-queue
!
!
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
   < output omitted >
!
router rip
 version 2
 network 172.30.0.0
 network 192.168.4.0
 no auto-summary
!
ip classless
!
!
!
```

```
banner motd ^C
Warning!
Authorized Access Only ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

```
banner motd ^C
Warning!
Authorized Access Only ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

```
SanJose1#show access-lists
Standard IP access list 1
    deny   172.30.10.20
    permit any
SanJose1#
```

```
SanJose2#show access-lists
SanJose2#
```

Task 2: Moving the same ACL closer to the source.

```
SanJose1#show run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SanJose1
!
enable secret 5 $1$ycLF$wNCjZmHNmGSsnb0HdBcaH.
!
ip subnet-zero
no ip domain-lookup
ip host SanJose1-s0 192.168.4.5
ip host SanJose1-e0 172.30.20.1
ip host HostA 172.30.20.5
ip host SanJose2-s0 192.168.4.6
ip host SanJose2-e0 172.30.10.1
ip host HostB 172.30.10.20
!
!
process-max-time 200
!
interface Ethernet0
 description Connection to SanJose1 LAN
 ip address 172.30.20.1 255.255.255.0
 no ip directed-broadcast
!
interface Ethernet1
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial0
 description Connection to SanJose2
 ip address 192.168.4.5 255.255.255.252
```

```
SanJose2#show run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SanJose2
!
enable secret 5 $1$PL1q$ymqQyirafZb4jYO1kUT3F/
!
ip subnet-zero
no ip domain-lookup
ip host SanJose1-s0 192.168.4.5
ip host SanJose1-e0 172.30.20.1
ip host HostA 172.30.20.5
ip host SanJose2-s0 192.168.4.6
ip host SanJose2-e0 172.30.10.1
ip host HostB 172.30.10.20
!
!
process-max-time 200
!
interface Ethernet0
 description Connection to SanJose2 LAN
 ip address 172.30.10.1 255.255.255.0
 ip access-group 1 in
 no ip directed-broadcast
!
!
!
!
!
interface Serial0
 description Connection to SanJose1
 ip address 192.168.4.6 255.255.255.252
```

```
 no ip directed-broadcast
 no ip mroute-cache
 no fair-queue
 clockrate 64000
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
router rip
 version 2
 network 172.30.0.0
 network 192.168.4.0
 no auto-summary
!
ip classless
!
!
!
banner motd ^C
Warning!
Authorized Access Only ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

```
 no ip directed-broadcast
 no ip mroute-cache
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
!   < output omitted >
!
router rip
 version 2
 network 172.30.0.0
 network 192.168.4.0
 no auto-summary
!
ip classless
!
access-list 1 deny   172.30.10.20
access-list 1 permit any
banner motd ^C
Warning!
Authorized Access Only ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

```
SanJose1#show access-lists
SanJose1#
```

```
SanJose2#show access-lists
Standard IP access list 1
    deny   172.30.10.20
    permit any
SanJose2#
```

Task 3: Deny an entire network

```
SanJose1#show run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SanJose1
!
enable secret 5 $1$UPQS$mdOzGv0EEVic0IFEgtg2V1
!
ip subnet-zero
no ip domain-lookup
ip host SanJose1-s0 192.168.4.5
ip host SanJose1-e0 172.30.20.1
ip host HostA 172.30.20.5
ip host SanJose2-s0 192.168.4.6
ip host SanJose2-e0 172.30.10.1
```

```
SanJose2#show run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SanJose2
!
enable secret 5 $1$LRI/$EUUdMU1Nghf9n91CemHGJ1
!
ip subnet-zero
no ip domain-lookup
ip host SanJose1-s0 192.168.4.5
ip host SanJose1-e0 172.30.20.1
ip host HostA 172.30.20.5
ip host SanJose2-s0 192.168.4.6
ip host SanJose2-e0 172.30.10.1
```

```
ip host HostB 172.30.10.20
!
!
process-max-time 200
!
interface Ethernet0
 description Connection to SanJose1 LAN
 ip address 172.30.20.1 255.255.255.0
 no ip directed-broadcast
!
!  < output omitted >
!
interface Serial0
 description Connection to SanJose2
 ip address 192.168.4.5 255.255.255.252
 ip access-group 1 in
 no ip directed-broadcast
 no ip mroute-cache
 clockrate 64000
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
router rip
 version 2
 network 172.30.0.0
 network 192.168.4.0
 no auto-summary
!
ip classless
!
access-list 1 deny   172.30.10.0 0.0.0.255
access-list 1 permit any
banner motd ^C
Warning!
Authorized Access Only ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

```
ip host HostB 172.30.10.20
!
!
process-max-time 200
!
interface Ethernet0
 description Connection to SanJose2 LAN
 ip address 172.30.10.1 255.255.255.0
 no ip directed-broadcast
!
!
!
interface Serial0
 description Connection to SanJose1
 ip address 192.168.4.6 255.255.255.252
 no ip directed-broadcast
 no ip mroute-cache
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
!  < output omitted >
!
router rip
 version 2
 network 172.30.0.0
 network 192.168.4.0
 no auto-summary
!
ip classless
!
!
!
banner motd ^C
Warning!
Authorized Access Only ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

```
SanJose1#show access-lists
Standard IP access list 1
    deny   172.30.10.0, wildcard bits 0.0.0.255
    permit any
SanJose1#
```

```
SanJose2#show access-lists
SanJose2#
```

Task 4a: Deny all Telnets

```
SanJose1#show run
Building configuration...
```

```
SanJose2#show run
Building configuration...
```

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SanJose1
!
enable secret 5 $1$D1Jv$Jqnm7uFCtH4GCGC3qew31/
!
ip subnet-zero
no ip domain-lookup
ip host SanJose1-s0 192.168.4.5
ip host SanJose1-e0 172.30.20.1
ip host HostA 172.30.20.5
ip host SanJose2-s0 192.168.4.6
ip host SanJose2-e0 172.30.10.1
ip host HostB 172.30.10.20
!
!
process-max-time 200
!
interface Ethernet0
 description Connection to SanJose1 LAN
 ip address 172.30.20.1 255.255.255.0
 no ip directed-broadcast
!
  < output omitted >
!
interface Serial0
 description Connection to SanJose2
 ip address 192.168.4.5 255.255.255.252
 ip access-group 101 in
 no ip directed-broadcast
 no ip mroute-cache
 clockrate 64000
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
router rip
 version 2
 network 172.30.0.0
 network 192.168.4.0
 no auto-summary
!
ip classless
!
access-list 101 deny   tcp any any eq telnet
access-list 101 permit ip any any
banner motd ^C
Warning!
Authorized Access Only ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SanJose2
!
enable secret 5 $1$nMNT$thk.iufDLX790NDg9nxR8.
!
ip subnet-zero
no ip domain-lookup
ip host SanJose1-s0 192.168.4.5
ip host SanJose1-e0 172.30.20.1
ip host HostA 172.30.20.5
ip host SanJose2-s0 192.168.4.6
ip host SanJose2-e0 172.30.10.1
ip host HostB 172.30.10.20
!
!
process-max-time 200
!
interface Ethernet0
 description Connection to SanJose2 LAN
 ip address 172.30.10.1 255.255.255.0
 no ip directed-broadcast
!
!
!
interface Serial0
 description Connection to SanJose1
 ip address 192.168.4.6 255.255.255.252
 no ip directed-broadcast
 no ip mroute-cache
 no fair-queue
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
! <output omitted >
router rip
 version 2
 network 172.30.0.0
 network 192.168.4.0
 no auto-summary
!
ip classless
!
!
!
banner motd ^C
Warning!
Authorized Access Only ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

SanJose1#show access-lists
Extended IP access list 101
    deny tcp any any eq telnet (28 matches)
    permit ip any any (36 matches)
SanJose1#
	SanJose2#show access-lists
	SanJose2#

Task 4b: Deny all Telnets from specific host

SanJose1#show run Building configuration... Current configuration: ! version 12.0 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname SanJose1 ! enable secret 5 1OCjL$Vj0BrGWxUDSGn64mJo61D1 ! ip subnet-zero no ip domain-lookup ip host SanJose1-s0 192.168.4.5 ip host SanJose1-e0 172.30.20.1 ip host HostA 172.30.20.5 ip host SanJose2-s0 192.168.4.6 ip host SanJose2-e0 172.30.10.1 ip host HostB 172.30.10.20 ! ! process-max-time 200 ! interface Ethernet0 description Connection to SanJose1 LAN ip address 172.30.20.1 255.255.255.0 no ip directed-broadcast ! < output omitted > ! interface Serial0 description Connection to SanJose2 ip address 192.168.4.5 255.255.255.252 ip access-group 101 in no ip directed-broadcast no ip mroute-cache clockrate 64000 ! interface Serial1 no ip address no ip directed-broadcast shutdown ! router rip version 2 network 172.30.0.0 network 192.168.4.0 no auto-summary ! ip classless ! access-list 101 deny tcp host 172.30.10.20 any eq telnet	San SanJose2#show run Building configuration... Current configuration: ! version 12.0 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname SanJose2 ! enable secret 5 1c6E2$8MWHRVqsxUcyww3fx9xEJ1 ! ip subnet-zero no ip domain-lookup ip host SanJose1-s0 192.168.4.5 ip host SanJose1-e0 172.30.20.1 ip host HostA 172.30.20.5 ip host SanJose2-s0 192.168.4.6 ip host SanJose2-e0 172.30.10.1 ip host HostB 172.30.10.20 ! ! process-max-time 200 ! interface Ethernet0 description Connection to SanJose2 LAN ip address 172.30.10.1 255.255.255.0 no ip directed-broadcast ! interface Serial0 description Connection to SanJose1 ip address 192.168.4.6 255.255.255.252 no ip directed-broadcast no ip mroute-cache ! interface Serial1 no ip address no ip directed-broadcast shutdown ! ! < output omitted > ! ! router rip version 2 network 172.30.0.0 network 192.168.4.0 no auto-summary ! ip classless ! ! !

```
access-list 101 permit ip any any
banner motd ^C
Warning!
Authorized Access Only ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

```
!
banner motd ^C
Warning!
Authorized Access Only ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

```
SanJose1#show access-lists
Extended IP access list 101
    deny tcp host 172.30.10.20 any eq telnet (6
matches)
    permit ip any any (212 matches)
SanJose1#
```

```
SanJose2#show access-lists
SanJose2#
```

Task 5: Deny Telnet based on source and destination IP address

```
SanJose1#show run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SanJose1
!
enable secret 5 $1$rOmp$piUUwswkzfHwXvxxK.IZo/
!
ip subnet-zero
no ip domain-lookup
ip host SanJose1-s0 192.168.4.5
ip host SanJose1-e0 172.30.20.1
ip host HostA 172.30.20.5
ip host SanJose2-s0 192.168.4.6
ip host SanJose2-e0 172.30.10.1
ip host HostB 172.30.10.20
!
!
process-max-time 200
!
interface Ethernet0
 description Connection to SanJose1 LAN
 ip address 172.30.20.1 255.255.255.0
 no ip directed-broadcast
!
   < output omitted >
!
interface Serial0
 description Connection to SanJose2
 ip address 192.168.4.5 255.255.255.252
 ip access-group 101 in
```

```
SanJose2#show run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SanJose2
!
enable secret 5 $1$IKi1$nnFVVnbh/jWgE/nhxv2yI/
!
ip subnet-zero
no ip domain-lookup
ip host SanJose1-s0 192.168.4.5
ip host SanJose1-e0 172.30.20.1
ip host HostA 172.30.20.5
ip host SanJose2-s0 192.168.4.6
ip host SanJose2-e0 172.30.10.1
ip host HostB 172.30.10.20
!
!
process-max-time 200
!
interface Ethernet0
 description Connection to SanJose2 LAN
 ip address 172.30.10.1 255.255.255.0
 no ip directed-broadcast
!
!
!
interface Serial0
 description Connection to SanJose1
 ip address 192.168.4.6 255.255.255.252
 no ip directed-broadcast
```

```
 no ip directed-broadcast
 no ip mroute-cache
 clockrate 64000
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
router rip
 version 2
 network 172.30.0.0
 network 192.168.4.0
 no auto-summary
!
ip classless
!
access-list 101 deny   tcp host 172.30.10.20
host 192.168.4.5 eq telnet
access-list 101 permit ip any any
banner motd ^C
Warning!
Authorized Access Only ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

```
 no ip mroute-cache
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
  < output omitted>
!
router rip
 version 2
 network 172.30.0.0
 network 192.168.4.0
 no auto-summary
!
ip classless
!
!
!
!
banner motd ^C
Warning!
Authorized Access Only ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

```
SanJose1#show access-lists
Extended IP access list 101
    deny tcp host 172.30.10.20 host 192.168.4.5
eq telnet (12 matches)
    permit ip any any (76 matches)
SanJose1#
```

```
SanJose2#show access-lists
SanJose2#
```

Task 6: Named access lists

```
SanJose1#show run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SanJose1
!
enable secret 5 $1$h3MA$iD3XYMu/hvn/npYz5Hvor/
!
ip subnet-zero
no ip domain-lookup
ip host SanJose1-s0 192.168.4.5
ip host SanJose1-e0 172.30.20.1
```

```
SanJose2#show run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SanJose2
!
enable secret 5 $1$z1D2$BTtimhgC.IyAap6VFed/K/
!
ip subnet-zero
no ip domain-lookup
ip host SanJose1-s0 192.168.4.5
ip host SanJose1-e0 172.30.20.1
```

```
ip host HostA 172.30.20.5
ip host SanJose2-s0 192.168.4.6
ip host SanJose2-e0 172.30.10.1
ip host HostB 172.30.10.20
!
!
process-max-time 200
!
interface Ethernet0
 description Connection to SanJose1 LAN
 ip address 172.30.20.1 255.255.255.0
 no ip directed-broadcast
!
  < output omitted >
!
interface Serial0
 description Connection to SanJose2
 ip address 192.168.4.5 255.255.255.252
 ip access-group Restrict-172.30.10.0/24-Access
in
 no ip directed-broadcast
 no ip mroute-cache
 clockrate 64000
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
router rip
 version 2
 network 172.30.0.0
 network 192.168.4.0
 no auto-summary
!
ip http server
ip classless
!
!
ip access-list extended Restrict-
172.30.10.0/24-Access
 deny   icmp 172.30.10.0 0.0.0.255 any echo
 permit tcp 172.30.10.0 0.0.0.255 host
172.30.20.1 eq telnet
 deny   tcp 172.30.10.0 0.0.0.255 any eq telnet
 permit ip any any
banner motd ^C
Warning!
Authorized Access Only ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

```
ip host HostA 172.30.20.5
ip host SanJose2-s0 192.168.4.6
ip host SanJose2-e0 172.30.10.1
ip host HostB 172.30.10.20
!
!
process-max-time 200
!
interface Ethernet0
 description Connection to SanJose2 LAN
 ip address 172.30.10.1 255.255.255.0
 no ip directed-broadcast
!
!
!
interface Serial0
 description Connection to SanJose1
 ip address 192.168.4.6 255.255.255.252
 no ip directed-broadcast
 no ip mroute-cache
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
  < output omitted >
!
!
router rip
 version 2
 network 172.30.0.0
 network 192.168.4.0
 no auto-summary
!
!
ip classless
!
!
!
!
!
!
!
!
!
banner motd ^C
Warning!
Authorized Access Only ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

```
SanJose1#show access-lists
Extended IP access list Restrict-
172.30.10.0/24-Access
    deny icmp 172.30.10.0 0.0.0.255 any echo
(24 matches)
    permit tcp 172.30.10.0 0.0.0.255 host
172.30.20.1 eq telnet (48 matches)
```

```
SanJose2#show access-lists
SanJose2#
```

```
    deny tcp 172.30.10.0 0.0.0.255 any eq
telnet (6 matches)
    permit ip any any (340 matches)
SanJose1#
```

4 – Troubleshooting/Reflection

This lab required a number of different configurations and reloads. Instead of typing in each command I created a complete set of commands for each task and router ahead of time and verified them on NetLab. Once I had the physical lab cabled and powered on I just copied and pasted into the TeraTerm console. I noticed TeraTerm is not fully compliant with standard Windows UI conventions. For example it used the right mouse key to do the paste operation and it lacks a "select all" under the Edit menu. In several previous labs I had mistakenly pasted the clipboard into the console by accident by clicking on the right mouse key.

The following tools were used to test ACL's:

Ping from router:

Success	Fail
SanJose2#ping 172.30.20.1	SanJose2#ping 172.30.20.1
Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.30.20.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms SanJose2#	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.30.20.1, timeout is 2 seconds: U.U.U Success rate is 0 percent (0/5) SanJose2#

Extended ping from router:

Success	Fail
SanJose2#ping Protocol [ip]: Target IP address: 172.30.20.1 Repeat count [5]: Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: y Source address or interface: 172.30.10.1 Type of service [0]: Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes [n]:	SanJose2#ping Protocol [ip]: Target IP address: 172.30.20.5 Repeat count [5]: Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: y Source address or interface: 172.30.10.1 Type of service [0]: Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes [n]:
Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.30.20.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms SanJose2#	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.30.20.5, timeout is 2 seconds: U.U.U Success rate is 0 percent (0/5)

Ping form host:

Success	Fail
C:\Documents and Settings\cisco>ping 192.168.4.6	C:\Documents and Settings\cisco>ping 192.168.4.5

Pinging 192.168.4.6 with 32 bytes of data:
 	
Reply from 192.168.4.6: bytes=32 time=2ms TTL=255
Reply from 192.168.4.6: bytes=32 time=2ms TTL=255
Reply from 192.168.4.6: bytes=32 time=2ms TTL=255
Reply from 192.168.4.6: bytes=32 time=2ms TTL=255
 	
Ping statistics for 192.168.4.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
	Pinging 192.168.4.5 with 32 bytes of data:
	
	Reply from 192.168.4.5: Destination net unreachable.
	Reply from 192.168.4.5: Destination net unreachable.
	Reply from 192.168.4.5: Destination net unreachable.
	Reply from 192.168.4.5: Destination net unreachable.
	
	Ping statistics for 192.168.4.5:
	    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
	Approximate round trip times in milli-seconds:
	    Minimum = 0ms, Maximum = 0ms, Average = 0ms

Telnet from host:

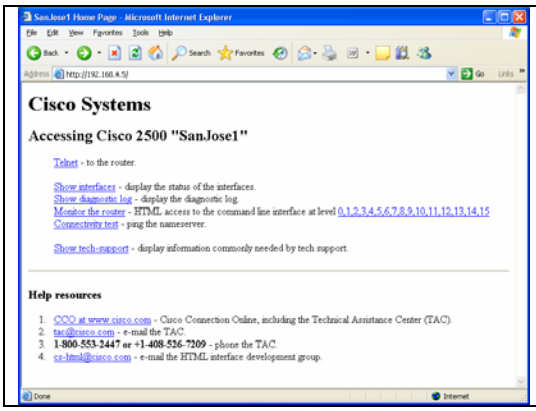
Success	Fail
C:\Documents and Settings\cisco>telnet 192.168.4.5	C:\Documents and Settings\cisco>telnet 192.168.4.5
Warning! Authorized Access Only User Access Verification Password: SanJose1>	Connecting To 192.168.4.5...Could not open connection to the host, on port 23: Connect failed

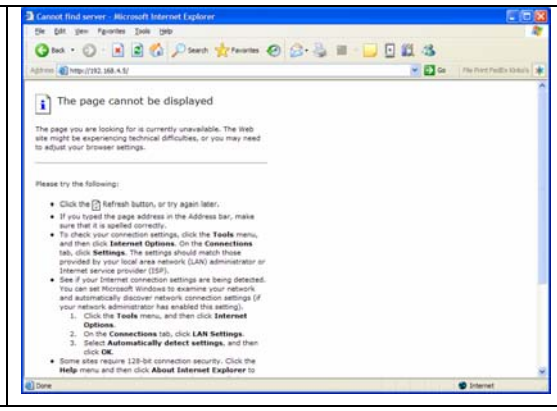
Telnet from router:

Success	Fail
SanJose2#telnet sanjose1-s0	SanJose2#telnet sanjose1-s0
Trying SanJose1-s0 (192.168.4.5)... Open Warning! Authorized Access Only User Access Verification Password:	Trying SanJose1-s0 (192.168.4.5)... % Destination unreachable; gateway or host down SanJose2#

Browser:

Success	Fail
http://192.168.4.5	http://192.168.4.5

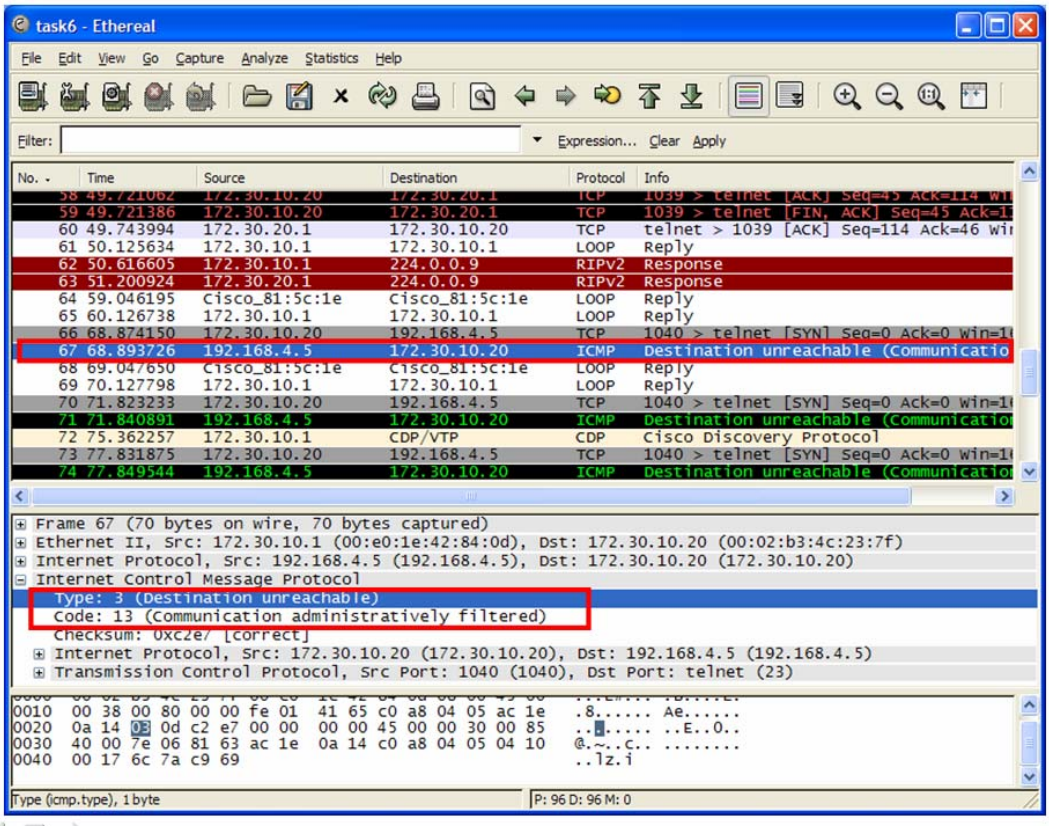




5 – Lab Questions

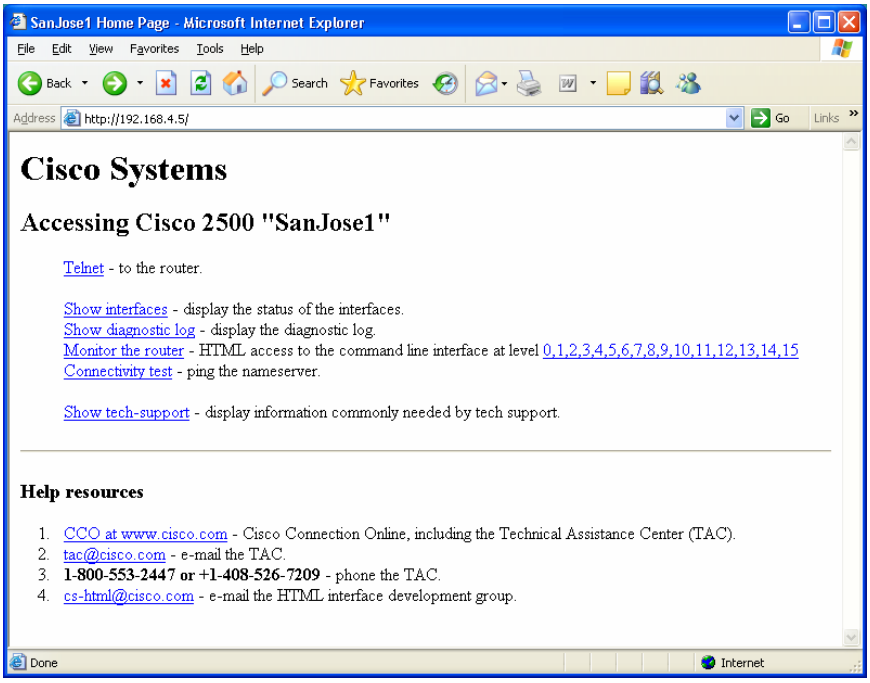
Regarding Task 6 ICMP packets captured on Ethereal when attempting to connect to 192.168.4.5

What is the type and code? Type 3, Code 13



6 – Example Commands

```
! Enable router's web UI
Router#ip http server
```




```
! Standard access list example
interface Serial0
  ip access-group 1 in
!
access-list 1 deny   172.30.10.20
access-list 1 permit any

! Extended access list example
interface Serial0
  ip access-group 101 in
access-list 101 deny   tcp host 172.30.10.20 host 192.168.4.5 eq telnet
access-list 101 permit ip any any

! Named access control list example
interface Serial0
  ip access-group Restrict-172.30.10.0/24-Access in
!
ip access-list extended Restrict-172.30.10.0/24-Access
 deny   icmp 172.30.10.0 0.0.0.255 any echo
 permit tcp 172.30.10.0 0.0.0.255 host 172.30.20.1 eq telnet
 deny   tcp 172.30.10.0 0.0.0.255 any eq telnet
 permit ip any any

SanJose1#show access-lists
Extended IP access list Restrict-172.30.10.0/24-Access
    deny icmp 172.30.10.0 0.0.0.255 any echo (24 matches)
    permit tcp 172.30.10.0 0.0.0.255 host 172.30.20.1 eq telnet (48 matches)
```

CIS 82 - Case Study

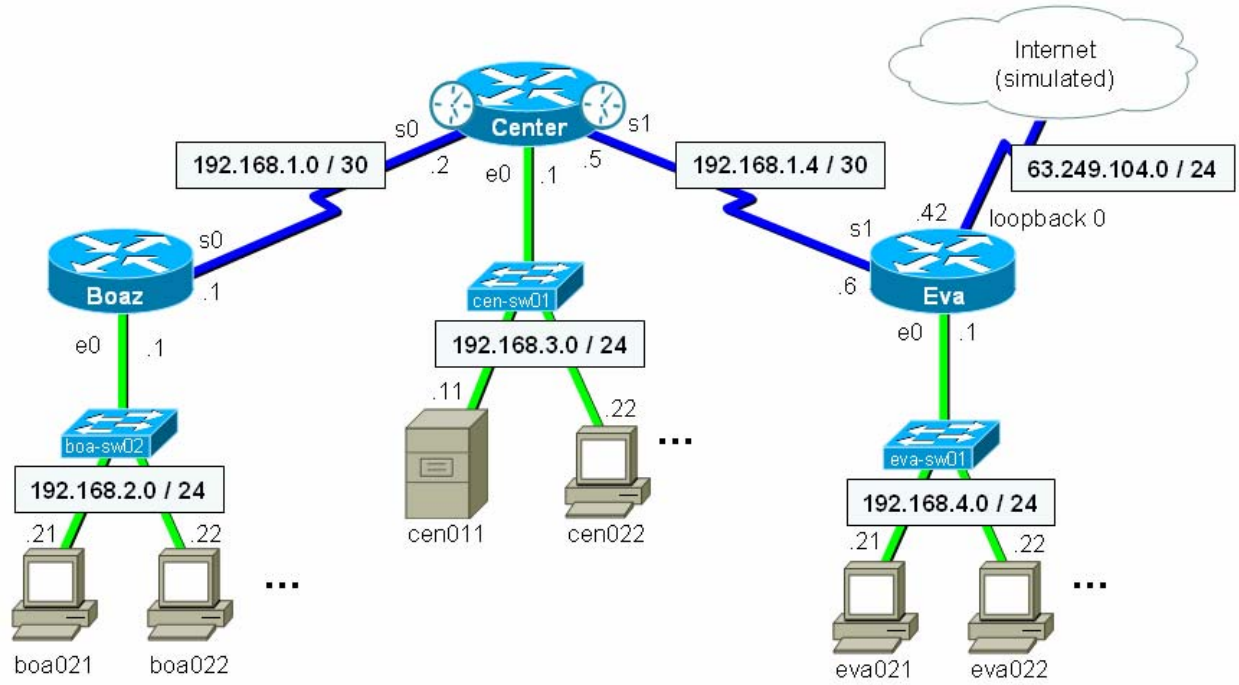
Rich Simms
May 12, 2006

Objective

The objective of this case study is to design and implement a multi-site network from scratch. There will be three sites and one connection to the Internet. Each site will have 50 to 80 hosts. The network will need to be secured using Access Control Lists.

Diagram

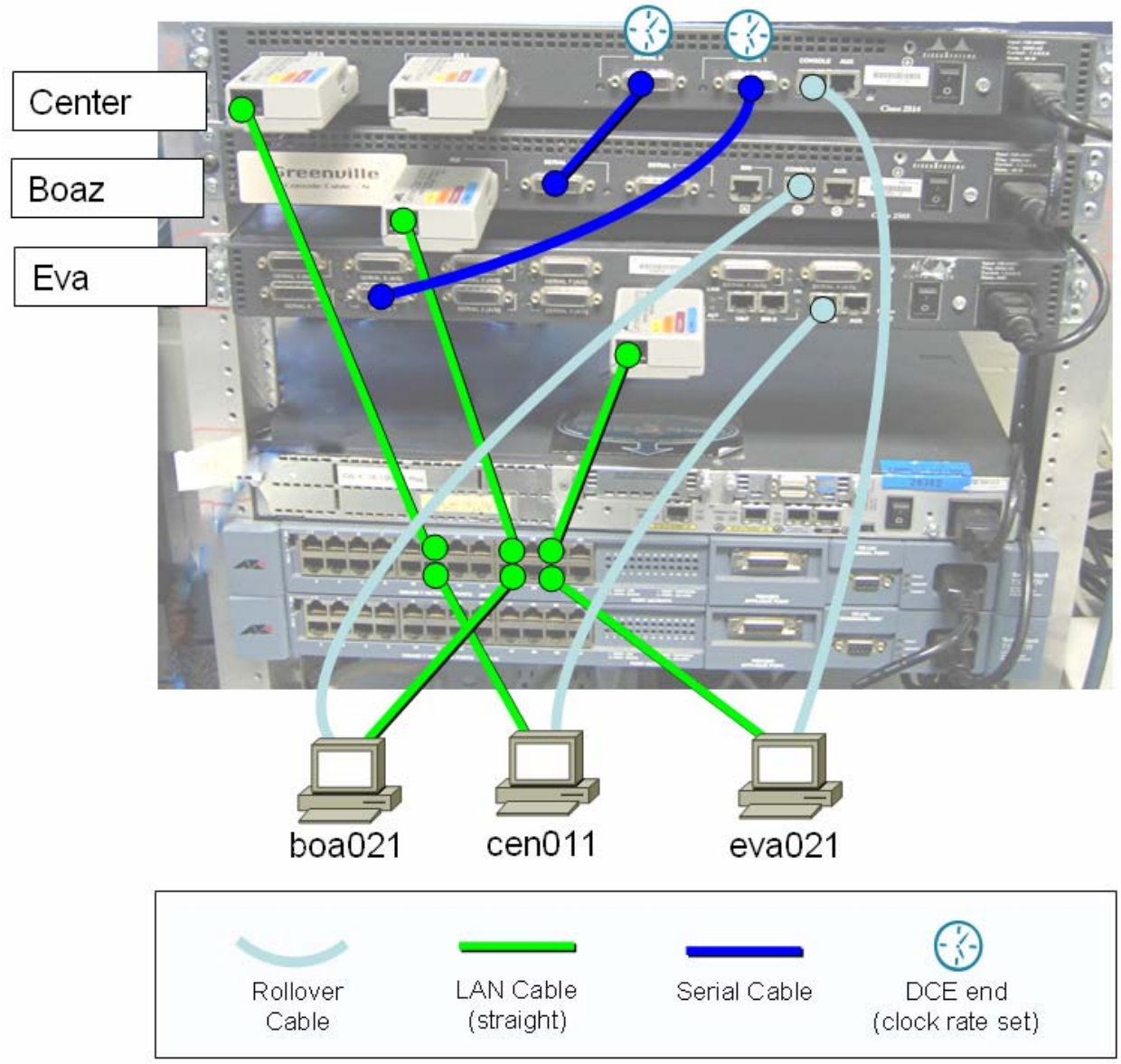
Logical view



Classful networks and subnets (indented):
192.168.1.0
    192.168.1.0 / 30
    192.168.1.4 / 30
192.168.2.0
192.168.3.0
192.168.4.0
63.0.0.0
    63.249.104.0 / 24

Serial
LAN
DCE end

Physical view



IP Addressing Scheme

We have three sites Boaz, Center, and Eva. We will be using the 192.168.0.0 private network and subnet it into multiple class C networks for each site. These networks will all have a /24 mask. In addition the 192.168.1.0 network will be further subnetted into multiple /30 subnets to use for serial links which only need two host addresses for each end of the serial connection.

Currently each site only has 50-80 hosts but with the Class C networks they have room for growth. Each class C network can have up to 254 hosts. The IP addressing scheme for the sites will be to have the ending .1 address always assigned to the router interface. The addresses ending in .2 to .20 will be reserved for non-clients (printers, servers, switches, etc.) The

remaining addresses up to the one ending with .254 will be used for client desktops and workstations. The hostnames for the routers will be the same as the site names. All other hostnames will be based on the first three letters of the site name plus the last portion of the IP address. For example boa022 will be the hostname for a client on the Boaz site which has an IP address of 192.168.2.22.

Subnet table

Subnet	Network address	Mask	Classful	Host range	Broadcast address	Usable	Status
0	192.168.0.0	/24	Yes (C)	192.168.0.1 to 192.168.0.254	192.168.0.255	yes	available
1	192.168.1.0	/24	Yes (C)	192.168.1.1 to 192.168.1.254	192.168.1.255	yes	Serial links
2	192.168.2.0	/24	Yes (C)	192.168.2.1 to 192.168.2.254	192.168.1.255	yes	Boaz LAN
3	192.168.3.0	/24	Yes (C)	192.168.3.1 to 192.168.3.254	192.168.1.255	yes	Center LAN
4	192.168.4.0	/24	Yes (C)	192.168.4.1 to 192.168.4.254	192.168.1.255	yes	Eva LAN
...	...	...	...	...	...	...	available
254	192.168.254.0	/24	Yes (C)	192.168.254.1 to 192.168.254.254	192.168.254.255	yes	available
255	192.168.255.0	/24	Yes (C)	192.168.255.1 to 192.168.255.254	192.168.255.255	no	unusable

In addition the 192.168.1.0 network above will be further subnetted for multiple serial links

Subnet	Network address	Mask	Classful	Host range	Broadcast address	Usable	Status
0	192.168.1.0	/30	No (CIDR)	192.168.0.1 to 192.168.0.2	192.168.0.3	yes	Boaz-Center WAN
1	192.168.1.4	/30	No (CIDR)	192.168.0.5 to 192.168.0.6	192.168.0.7	yes	Center-Eva WAN
2	192.168.1.8	/30	No (CIDR)	192.168.0.9 to 192.168.0.10	192.168.0.11	yes	available
...	...	...	...	...	...	...	available
62	192.168.1.248	/30	No (CIDR)	192.168.1.249 to 192.168.1.250	192.168.1.251	yes	available
63	192.168.1.252	/30	No (CIDR)	192.168.1.253 to 192.168.1.254	192.168.1.255	no	unusable

Host Configuration table

Hostname	LAN	IP	Mask	Default Gateway	Device Type
...					
boa021	boaz	192.168.2.21	255.255.255.0	192.168.2.1	PC
boa022	boaz	192.168.2.22	255.255.255.0	192.168.2.1	PC
...					
cen011	center	192.168.3.11	255.255.255.0	192.168.3.1	server
cen022	center	192.168.3.22	255.255.255.0	192.168.3.1	PC
...					
eva021	eva	192.168.4.21	255.255.255.0	192.168.4.1	PC
eva022	eva	192.168.4.22	255.255.255.0	192.168.4.1	PC
...					

Subnet Details Table

Network Address				Mask	Address (blue host bits)	Address Type	Address	Allocation
192	168	0	0	/24	192.168.0.0000 0000	network	192.168.0.0	available
192	168	1	0	/30	192.168.1.0000 0000	network	192.168.1.0	Boaz-Center Serial WAN
192	168	1	0	/30	192.168.1.0000 0001	host	192.168.1.1	Boaz S0
192	168	1	0	/30	192.168.1.0000 0010	host	192.168.1.2	Center S0
192	168	1	0	/30	192.168.1.0000 0011	broadcast	192.168.1.3	
192	168	1	4	/30	192.168.1.0000 0100	network	192.168.1.4	Center-Eva WAN
192	168	1	4	/30	192.168.1.0000 0101	host	192.168.1.5	Center S1
192	168	1	4	/30	192.168.1.0000 0110	host	192.168.1.6	Eva S1
192	168	1	4	/30	192.168.1.0000 0111	broadcast	192.168.1.7	
192	168	1	8	/30	192.168.1.0000 1000	network	192.168.1.8	3rd subnet available
192	168	1	...	/30	...	networks	192.168.1.16 to 192.168.1.248	4th to 63rd subnets available
192	168	1	252	/30	192.168.1.1111 1100	network	192.168.1.252	64th subnet unusable
192	168	2	0	/24	192.168.2.0000 0000	network	192.168.2.0	Boaz LAN
192	168	2	0	/24	192.168.2.0000 0001	host	192.168.2.1	Boaz LAN host 1
192	168	2	0	/24	192.168.2.0000 0010	host	192.168.2.2	Boaz LAN host 2
192	168	2	0	/24	...	networks	192.168.2.3 to 192.168.2.254	Boaz LAN hosts (3 to 254)
192	168	2	0	/24	192.168.2.1111 1111	broadcast	192.168.2.255	Boaz LAN broadcast
192	168	3	0	/24	192.168.3.0000 0000	network	192.168.3.0	Center LAN
192	168	3	0	/24	192.168.3.0000 0001	host	192.168.3.1	Center LAN host 1
192	168	3	0	/24	192.168.3.0000 0010	host	192.168.3.2	Center LAN host 2
192	168	3	0	/24	...	hosts	192.168.3.3 to 192.168.3.254	Center LAN hosts (3 to 254)
192	168	3	0	/24	192.168.3.1111 1111	broadcast	192.168.3.255	Center LAN broadcast
192	168	4	0	/24	192.168.4.0000 0000	network	192.168.4.0	Eva LAN
192	168	4	0	/24	192.168.4.0000 0001	host	192.168.4.1	Eva LAN host 1
192	168	4	0	/24	192.168.4.0000 0010	host	192.168.4.2	Eva LAN host 2
192	168	4	0	/24	...	hosts	192.168.4.3 to 192.168.4.254	Eva LAN hosts 3 to 254
192	168	4	0	/24	192.168.4.1111 1111	broadcast	192.168.4.255	Eva LAN broadcast
192	168	5	0	/24	192.168.5.0000 0000	network	192.168.5.0	available
192	168	...	0	/24	...	networks	192.168.6.0 to 192.168.254.0	available
192	168	255	0	/24	192.168.255.0000 0000	network	192.168.255.255	unusable

Routing Protocol and default gateway

The routers will be configured with the RIP v2 protocol to exchange routing table information. V2 is necessary since the serial link networks are not classful. A default gateway will be configured on Eva to the "Internet" (loopback interface). To propagate this route via RIP advertisements the `redistribute static` command is used.

Access Control Lists

The server cen011 (192.168.3.11) on the Center LAN is running a restricted access web server. Access to this server is restricted to Center and Eva LAN users. Eva LAN users are further restricted to port 80 (HTTP) access only on this server. No other users may access is server. Access control will be implemented as follows:

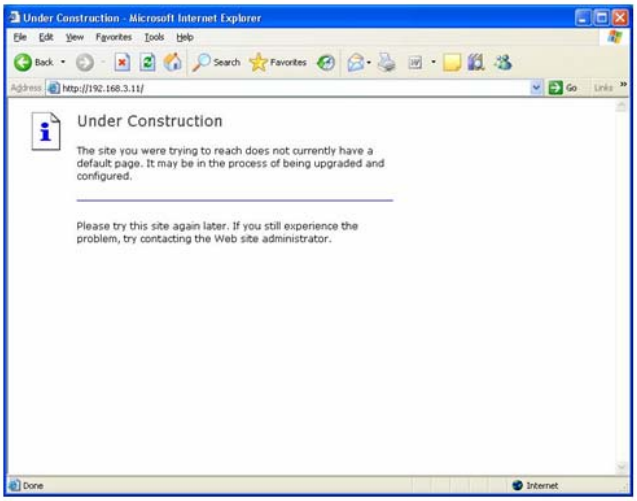
On Center:

```
access-list 101 permit tcp 192.168.4.0 0.0.0.255 host 192.168.3.11 eq 80
access-list 101 deny ip any host 192.168.3.11
access-list 101 permit ip any any
```

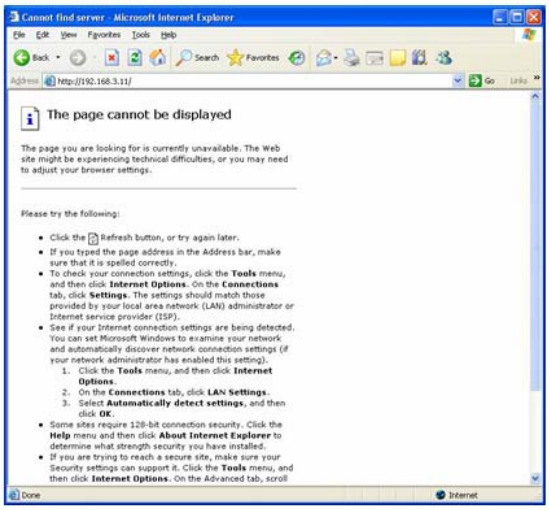
On Center's e0 interface:

```
ip access-group 101 out
```

e0 (out)	Extended IP access list 101 permit tcp 192.168.4.0 0.0.0.255 host 192.168.3.11 eq www (10 matches) deny ip any host 192.168.3.11 (62 matches) permit ip any any (275 matches)



Showing web server access from Eva LAN



Showing restricted access from Boaz LAN

Router Details

Hostname: Boaz
Pod: Sydney Australia
Platform: Cisco 2503
IOS Version: 12.0(5)

Interface	DCE/DTE	Speed	Description	Network	IP Address	Mask
e0	na	10000 Kbit	Boaz lan	192.168.2.0 /24	192.168.2.1	255.255.255.0
s0	DTE	1544 Kbit	Serial link to Center	192.168.1.0 /30	192.168.1.1	255.255.255.252

Hostname: Center
Pod: Sydney Australia
Platform: Cisco 2514
IOS Version: 12.0(5)

Interface	DCE/DTE	Speed	Description	Network	IP Address	Mask
e0	na	10000 Kbit	Center lan	192.168.3.0 /24	192.168.3.1	255.255.255.0
s0	DCE	1544 Kbit	Serial link to Boaz	192.168.1.0 /30	192.168.1.2	255.255.255.252
s1	DCE	1544 Kbit	Serial link to Eva	192.168.1.4 /30	192.168.1.5	255.255.255.252

Hostname: Eva
Pod: Sydney Australia
Platform: Cisco 2522
IOS Version: 12.0(5)

Interface	DCE/DTE	Speed	Description	Network	IP Address	Mask
e0	na	10000 Kbit	Eva lan	192.168.3.0 /24	192.168.4.1	255.255.255.0
s1	DTE	1544 Kbit	Serial link to Center	192.168.1.4 /30	192.168.1.6	255.255.255.252
loopback	na	na	Simulated Internet	63.249.104.0 /24	63.249.104.42	255.255.255.0

Convergence

To verify convergence all nodes were checked to be able to ping all other nodes successfully. This utilized the ping commands on both the routers and the Windows hosts. To make use of the loopback "internet" address as a source address the extended ping command was used.

With the ACL activated, access to the web server on Center LAN was only successful using a web browser from the Center or Eva LANs. All other source IP packets were dropped.

Running Configs

```
boaz#show run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug
uptime
service timestamps log uptime
no service password-encryption
!
hostname boaz
!
enable secret 5
$1$gVgy$5m1ccDgj2aq5HSh1ZMwLY0
!
ip subnet-zero
no ip domain-lookup
ip host eva-s1 192.168.1.6
ip host eva-e0 192.168.4.1
ip host center-s1 192.168.1.5
ip host center-s0 192.168.1.2
ip host center-e0 192.168.3.1
ip host boaz-s0 192.168.1.1
ip host boaz-e0 192.168.2.1
ip host internet 63.249.104.42
ip host boa021 192.168.2.21
ip host cen011 192.168.3.11
ip host cen022 192.168.3.22
ip host eva021 192.168.4.21
!
!
process-max-time 200
!
!
!
!
!
!
!
!
interface Ethernet0
 description Boaz LAN
 ip address 192.168.2.1
255.255.255.0
 no ip directed-broadcast
!
!
!
```

```
center#show run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug
uptime
service timestamps log uptime
no service password-encryption
!
hostname center
!
enable secret 5
$1$/SQz$445vOYSvFPZx8kgRI/6QT1
!
ip subnet-zero
no ip domain-lookup
ip host eva-s1 192.168.1.6
ip host eva-e0 192.168.4.1
ip host center-s1 192.168.1.5
ip host center-s0 192.168.1.2
ip host center-e0 192.168.3.1
ip host boaz-s0 192.168.1.1
ip host boaz-e0 192.168.2.1
ip host internet 63.249.104.42
ip host boa021 192.168.2.21
ip host cen011 192.168.3.11
ip host cen022 192.168.3.22
ip host eva021 192.168.4.21
!
!
process-max-time 200
!
!
!
!
!
!
!
!
interface Ethernet0
 description Connection to
Center LAN
 ip address 192.168.3.1
255.255.255.0
 ip access-group 101 out
 no ip directed-broadcast
!
```

```
eva#show run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug
uptime
service timestamps log uptime
no service password-encryption
!
hostname eva
!
enable secret 5
$1$81BX$ZlpBWwtYFHlYbspyRQYgB0
!
ip subnet-zero
no ip domain-lookup
ip host eva-s1 192.168.1.6
ip host eva-e0 192.168.4.1
ip host center-s1 192.168.1.5
ip host center-s0 192.168.1.2
ip host center-e0 192.168.3.1
ip host boaz-s0 192.168.1.1
ip host boaz-e0 192.168.2.1
ip host internet 63.249.104.42
ip host boa021 192.168.2.21
ip host cen011 192.168.3.11
ip host cen022 192.168.3.22
ip host eva021 192.168.4.21
!
!
process-max-time 200
!
interface Loopback0
 description Loopback
Interface on Eva
 ip address 63.249.104.42
255.255.255.0
 no ip directed-broadcast
!
interface Ethernet0
 description Connection to Eva
LAN
 ip address 192.168.4.1
255.255.255.0
 no ip directed-broadcast
!
!
```

```
interface Serial0
 description Connection to
Center
 ip address 192.168.1.1
255.255.255.252
 no ip directed-broadcast
 no ip mroute-cache
 no fair-queue
!
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
!
!
interface BRI0
 no ip address
 no ip directed-broadcast
 shutdown
!
router rip
 version 2
 passive-interface Ethernet0
 network 192.168.1.0
 network 192.168.2.0
 no auto-summary
!
!
ip classless
!
!
!
!
!
!
!
!
banner motd ^C
Warning!
Authorized Access Only ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

```
interface Serial0
 description Connection to
Boaz
 ip address 192.168.1.2
255.255.255.252
 no ip directed-broadcast
 no ip mroute-cache
 no fair-queue
 clockrate 64000
!
interface Serial1
 description Connection to Eva
 ip address 192.168.1.5
255.255.255.252
 no ip directed-broadcast
 clockrate 64000
!
interface BRI0
 no ip address
 no ip directed-broadcast
 shutdown
!
router rip
 version 2
 passive-interface Ethernet0
 network 192.168.1.0
 network 192.168.3.0
 no auto-summary
!
!
ip classless
!
access-list 101 permit tcp
192.168.4.0 0.0.0.255 host
192.168.3.11 eq www
access-list 101 deny   ip any
host 192.168.3.11
access-list 101 permit ip any
any
banner motd ^C
Warning!
Authorized Access Only ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

```
interface Serial0
 no ip address
 no ip directed-broadcast
 shutdown
!
!
!
!
!
!
interface Serial1
 description Connection to
Center
 ip address 192.168.1.6
255.255.255.252
 no ip directed-broadcast
!
interface BRI0
 no ip address
 no ip directed-broadcast
 shutdown
!
router rip
 version 2
 redistribute static
 passive-interface Ethernet0
 network 192.168.1.0
 network 192.168.4.0
 no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0
Loopback0
!
!
!
!
!
!
banner motd ^C
Warning!
Authorized Access Only ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Routing Tables

```
boaz#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is 192.168.1.2 to network 0.0.0.0
```

```
R    192.168.4.0/24 [120/2] via 192.168.1.2, 00:00:25, Serial0
     192.168.1.0/30 is subnetted, 2 subnets
C       192.168.1.0 is directly connected, Serial0
R       192.168.1.4 [120/1] via 192.168.1.2, 00:00:25, Serial0
C    192.168.2.0/24 is directly connected, Ethernet0
R    192.168.3.0/24 [120/1] via 192.168.1.2, 00:00:25, Serial0
R*   0.0.0.0/0 [120/2] via 192.168.1.2, 00:00:25, Serial0
boaz#
```

```
center#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is 192.168.1.6 to network 0.0.0.0

R    192.168.4.0/24 [120/1] via 192.168.1.6, 00:00:27, Serial1
     192.168.1.0/30 is subnetted, 2 subnets
C       192.168.1.0 is directly connected, Serial0
C       192.168.1.4 is directly connected, Serial1
R    192.168.2.0/24 [120/1] via 192.168.1.1, 00:00:21, Serial0
C    192.168.3.0/24 is directly connected, Ethernet0
R*   0.0.0.0/0 [120/1] via 192.168.1.6, 00:00:27, Serial1
```

```
eva#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

C    192.168.4.0/24 is directly connected, Ethernet0
     63.0.0.0/24 is subnetted, 1 subnets
C       63.249.104.0 is directly connected, Loopback0
     192.168.1.0/30 is subnetted, 2 subnets
R       192.168.1.0 [120/1] via 192.168.1.5, 00:00:20, Serial1
C       192.168.1.4 is directly connected, Serial1
R    192.168.2.0/24 [120/2] via 192.168.1.5, 00:00:20, Serial1
R    192.168.3.0/24 [120/1] via 192.168.1.5, 00:00:20, Serial1
S*   0.0.0.0/0 is directly connected, Loopback0
eva#
```

Troubleshooting/Reflection

I had a problem with the serial connection between Center and Eva. I used ping, show ip int brief, and show controllers to see the line was not up. I looked at my cables and saw the serial cable was not connected correctly.

I had setup and tested the route configurations previously on NetLab so that part went quite fast. I brought edited config files that I just "pasted" into TeraTerm consoles. This saved a lot of time.

Successful propagation of the default gateway varied across different routers. It was discovered that using the alternative `default-information originate` or the `default-network x.x.x.x` commands also worked on the older Sydney pod routers running v12.0. However the `default-information originate` command did not propagate the default route on the NetLab pod.

For the fake Internet address configured on Eva's loopback interface I used the actual settings I found on my home network's DSL connection to Cruzio. I don't have a static IP with this ISP so that is probably why they use a /24 network rather than a /30 network.

CIS 82 Lab - SBA Practice – Paper Handout
Rich Simms
May 15, 2006

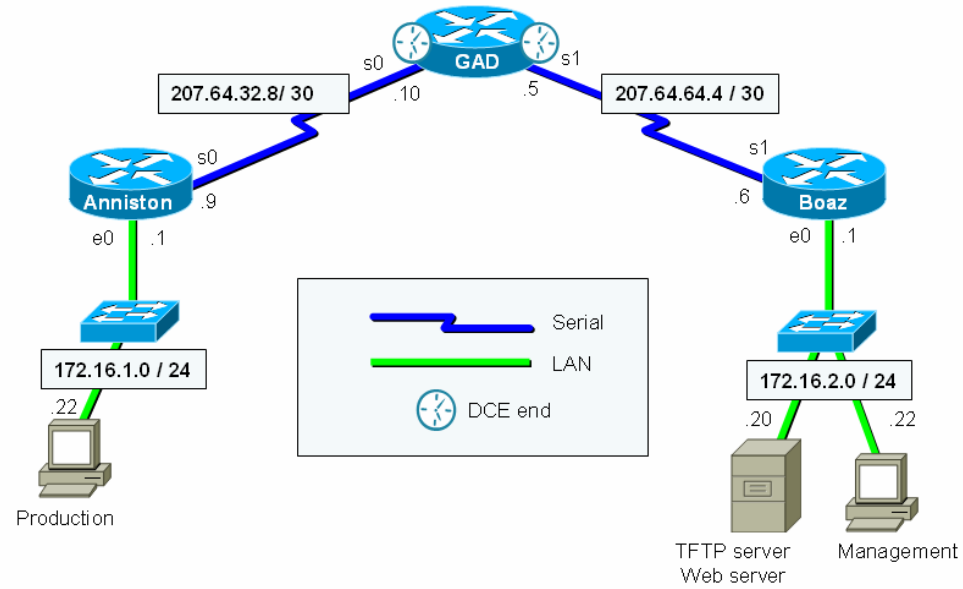
---

1 – Scenario

The objective of this exercise was to practice setting up three routers in anticipation of the skills based assessment. The objective was to take the practice SBA handout from class and implement it. The access control requirements are:

"… denies the production network PC access to the web server. Access to the tftp server needs to be allowed … Deny all telnet access to the Boaz router. You should always be able to telnet and ping to the other routers in your network"

2 – Diagram



3 – Running Configurations

Anniston	Gad	Boaz
anniston#show run Building configuration... Current configuration : 1192 bytes ! version 12.2 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname anniston ! enable secret 5	gad#show run Building configuration... Current configuration : 1177 bytes ! version 12.2 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname gad ! enable secret 5	boaz#show run Building configuration... Current configuration : 1613 bytes ! version 12.2 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname boaz ! enable secret 5

```
$1$MXfT$uHGxPzTRFcJBZp/uPHw4p0
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
no ip domain-lookup
ip host tftp-server
172.16.2.20
ip host web-server 172.16.2.20
ip host boaz-s1 207.64.64.6
ip host boaz-e0 172.16.2.1
ip host gad-s1 207.64.64.5
ip host gad-s0 207.64.32.10
!
!
!
!
ip audit notify log
ip audit po max-events 100
!
!
!
!
interface BRI0
 no ip address
 shutdown
!
interface FastEthernet0
 description Anniston LAN
 ip address 172.16.1.1
255.255.255.0
 speed auto
!
!
!
interface Serial0
 description Connection to GAD
 ip address 207.64.32.9
255.255.255.252
 no fair-queue
!
!
!
interface Serial1
 no ip address
 shutdown
!
!
!
!
router rip
 version 2
 network 172.16.0.0
 network 207.64.32.0
 no auto-summary
!
!
ip classless
no ip http server
ip pim bidir-enable
!
!
!
!
!
!
!
```

```
$1$DDCU$3auQhexIzWo7TA3YESkCv1
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
no ip domain-lookup
ip host boaz-e0 172.16.2.1
ip host boaz-s1 207.64.64.6
ip host anniston-s0
207.64.32.9
ip host anniston-e0 172.16.1.1
!
!
!
!
!
ip audit notify log
ip audit po max-events 100
!
!
!
!
interface BRI0
 no ip address
 shutdown
!
interface FastEthernet0
 no ip address
 shutdown
 speed auto
!
!
!
!
interface Serial0
 description Connection to
Anniston
 ip address 207.64.32.10
255.255.255.252
 no fair-queue
 clockrate 64000
!
interface Serial1
 description Connection to
Boaz
 ip address 207.64.64.5
255.255.255.252
 clockrate 64000
!
router rip
 version 2
 network 207.64.32.0
 network 207.64.64.0
 no auto-summary
!
!
ip classless
no ip http server
ip pim bidir-enable
!
!
!
!
!
!
!
```

```
$1$cKkN$BTgVK48RfBZjFOusTTgKc/
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
no ip domain-lookup
ip host web-server 172.16.2.20
ip host boaz-e0 172.16.2.1
ip host boaz-s1 207.64.64.6
ip host production 172.16.1.22
ip host gad-e0 172.16.2.1
ip host gad-s1 207.64.64.5
ip host gad-s0 207.64.32.10
ip host anniston-s0
207.64.32.9
ip host anniston-e0 172.16.1.1
!
ip audit notify log
ip audit po max-events 100
!
!
!
!
interface BRI0
 no ip address
 shutdown
!
interface FastEthernet0
 description Boaz LAN
 ip address 172.16.2.1
255.255.255.0
 ip access-group 102 in
 ip access-group 101 out
 speed auto
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
!
!
!
!
interface Serial1
 description connection to GAD
 ip address 207.64.64.6
255.255.255.252
 ip access-group 102 in
!
!
router rip
 version 2
 redistribute static
 network 172.16.0.0
 network 207.64.64.0
 no auto-summary
!
ip classless
no ip http server
ip pim bidir-enable
!
!
access-list 101 deny   tcp
host 172.16.1.22 host
172.16.2.20 eq www
access-list 101 permit ip any
any
```

```
!
!
!
!
!

!
banner motd ^C
Welcome to Anniston
Authorized users only! ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
no scheduler allocate
end

anniston#
```

```
!
!
!
!
!
!
!
banner motd ^C
Welcome to GAD
Authorized users only! ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
no scheduler allocate
end

gad#
```

```
access-list 102 deny   tcp any
host 207.64.64.6 eq telnet
access-list 102 deny   tcp any
host 172.16.2.1 eq telnet
access-list 102 permit ip any
any
!
banner motd ^C
Welcome to Boaz
Authorized users only! ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
no scheduler allocate
end

boaz#
```

4- Troubleshooting / Reflection

This practice session was implemented on the smaller C1700 models in the Singapore pod. I learned from Eric that there is a simpler way to deny telnet access with the line vty 0 4 command. I googled this and found four alternatives for denying router telnet access posted by "BillW" at Cisco:

> *How would I disable telnet access to a Cisco 2500 router with v9.1? Any clues?*
>
> *There are a couple of methods:*
>
> *1) require an impossible login:*
> *line vty 0 4*
> *login*
> *no password*
>
> *This results in a "password required, but none set" message when you try to telnet to the router. This is the "virgin" state of a cisco router - in the absence of any configuration, this is how it behaves.*
>
> *2) Line access lists:*
>
> *access-list 77 deny 0.0.0.0 0.0.0.0*
> *! (implied deny everything else)*
> *line vty 0 4*
> *access-class 77 in*
>
> *This will result in a tcp rst packet in response to connection requests (usually shown as "connection refused".) Of course, you may use a more complex access list and allow some hosts to connect, but not others.*

3) Transport command:

```
line vty 0 4
transport input none
```

This will also result in connection refused commands. "transport" is generally used to allocate different vty ranges to different protocols (ie, on a protocol translator.)

4) autocommand:

```
line vty 0 4
autocommand quit
```

In this case the connection is accepted, but as soon as the resulting exec is ready to execute a command, it will execute the "quit" autocommand instead, which immediately closes the connection again. This has the advantage (?) that any banner that is configured will be displayed before disconnecting the user. So if you want to write nasty messages about unathorized access and so on, you get a chance..

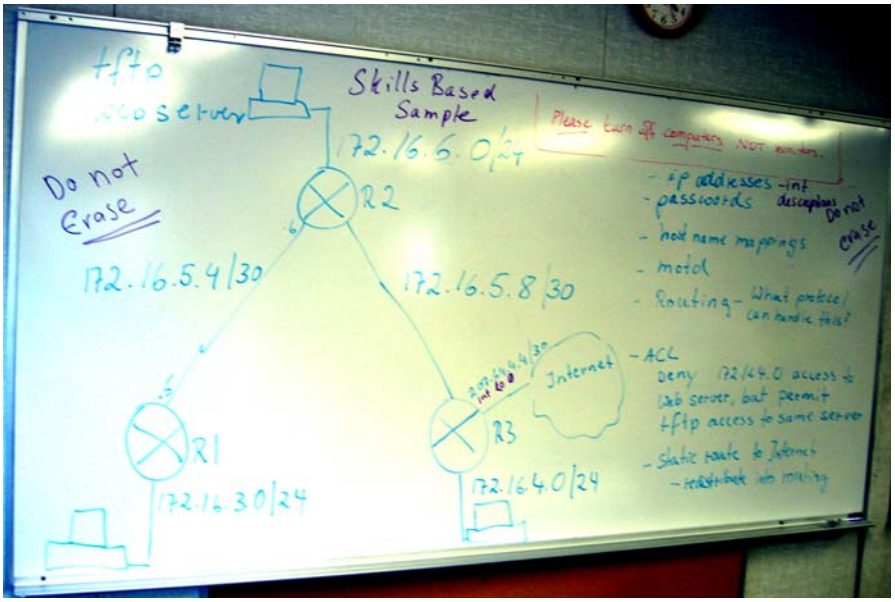
BillW
cisco

CIS 82 Lab - SBA Practice – White Board "A"
Rich Simms
May 12, 2006

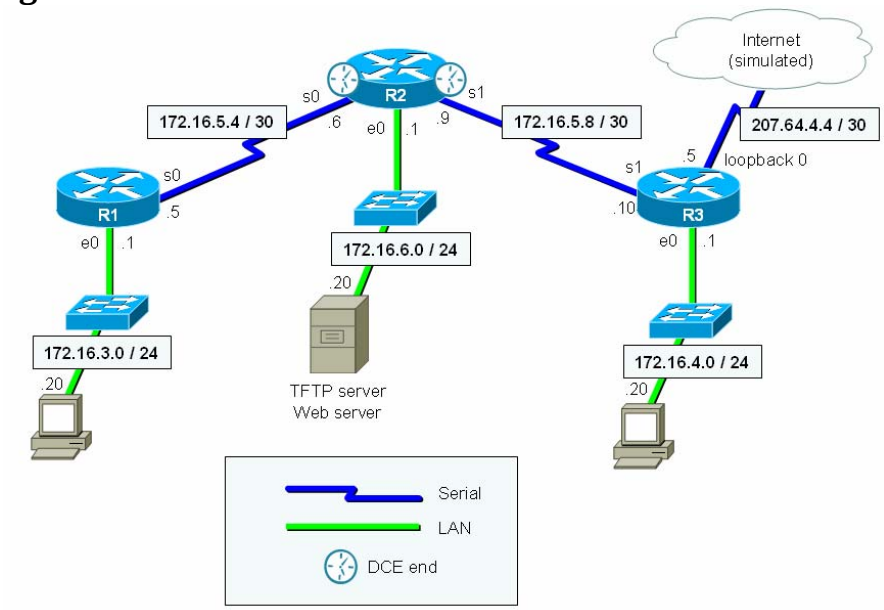
---

1 – Scenario

The objective of this exercise was to practice setting up three routers in anticipation of the skills based assessment. The objective was to take the diagram on the whiteboard and implement it.



2 – Diagram



3 – Running Configurations

R1

```
!
version 12.1
no service single-slot-reload-
enable
service timestamps debug
uptime
service timestamps log uptime
no service password-encryption
!
hostname r1
!
enable secret 5
$1$ss66$Jspc4jx8NSm2V/XwDFOFk/
!
!
!
!
!
memory-size iomem 15
ip subnet-zero
no ip domain-lookup
ip host server 172.16.6.20
ip host internet 207.64.4.5
ip host r3-e0 172.16.4.1
ip host r3-s1 172.16.5.10
ip host r2-s1 172.16.5.9
ip host r2-s0 172.16.5.6
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 description R1 LAN
 ip address 172.16.3.1
255.255.255.0
 duplex auto
 speed auto
!
!
interface Serial0/0
 description Connection to R2
 ip address 172.16.5.5
255.255.255.252
 no fair-queue
!
< snipped >
!
interface Serial0/1
 no ip address
 shutdown
!
!
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
!
```

R2

```
!
version 12.1
no service single-slot-reload-
enable
service timestamps debug
uptime
service timestamps log uptime
no service password-encryption
!
hostname r2
!
enable secret 5
$1$YE2U$GxCO3Rf9.m/2.0fF3itPl0
!
!
!
!
!
memory-size iomem 15
ip subnet-zero
no ip domain-lookup
ip host r3-e0 172.16.4.1
ip host r3-s1 172.16.5.10
ip host r1-e0 172.16.3.1
ip host r1-s0 172.16.5.5
ip host internet 207.64.4.5
ip host server 172.16.6.20
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 description R2 LAN
 ip address 172.16.6.1
255.255.255.0
 ip access-group 102 out
 duplex auto
 speed auto
!
interface Serial0/0
 description Connection to R1
 ip address 172.16.5.6
255.255.255.252
 clockrate 64000
!
< snipped >
!
interface Serial0/1
 description Connection to R3
 ip address 172.16.5.9
255.255.255.252
 clockrate 64000
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
!
```

R3

```
!
version 12.2
service timestamps debug
uptime
service timestamps log uptime
no service password-encryption
!
!
!
hostname r3
!
enable secret 5
$1$J/gb$ihYhMvIChnZP25TaMlyS41
!
memory-size iomem 10
ip subnet-zero
!
!
!
!
no ip domain-lookup
ip host r2-s1 172.16.5.9
ip host r2-e0 172.16.6.1
ip host r2-s0 172.16.5.6
ip host r1-e0 172.16.3.1
ip host r1-s0 172.16.5.5
ip host internet 207.64.4.5
ip host server 172.16.6.20
!
call rsvp-sync
!
interface Loopback0
 description Internet
Simulation
 ip address 207.64.4.5
255.255.255.252
!
interface FastEthernet0/0
 description R3 LAN
 ip address 172.16.4.1
255.255.255.0
 duplex auto
 speed auto
!
!
interface Serial0/0
 no ip address
 shutdown
!
< snipped >
!
!
!
interface Serial0/1
 description Connection to R2
 ip address 172.16.5.10
255.255.255.252
!
!
router rip
 version 2
 redistribute static
 network 172.16.0.0
 no auto-summary
!
```

```
ip classless
ip http server
!
!
!
!
!
!
banner motd ^C
Welcome to R1
Authorized users only! ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end
```

```
ip classless
ip http server
!
access-list 102 deny   tcp
172.16.4.0 0.0.0.255 host
172.16.6.20 eq www
access-list 102 permit ip any
any
banner motd ^C
Welcome to R2
Authorized users only! ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end
```

```
ip classless
ip route 0.0.0.0 0.0.0.0
Loopback0
ip http server
!
!
dial-peer cor custom
!
banner motd ^C
Welcome to R3
Authorized users only! ^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end
```

4- Troubleshooting / Reflection

I wanted to try out the new routers Kevin installed in the lab. They were rack mounted 2600 family routers and with the smaller smart serial interface connectors. As they were modular you had to specify both the slot and the interface number for the interface commands

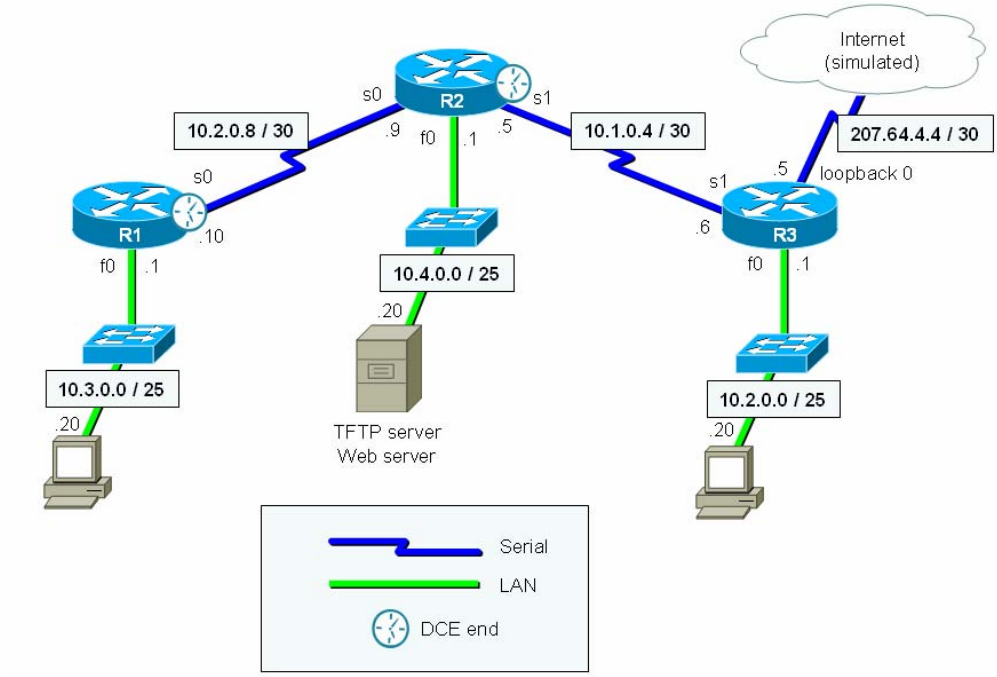
CIS 82 Lab - SBA Practice – White Board "B"
Rich Simms
May 16, 2006

---

1 – Scenario

The objective of this exercise was to practice setting up three routers in anticipation of the skills based assessment. The objective was to take the newly modified diagram on the whiteboard and implement it. The IP addresses and masks changed since the "A" version.

2 – Diagram



3 – Running Configurations

R1	R2	R3

`r1#show run`
`Building configuration...`
 	
`Current configuration : 1033 bytes`
`!`
`version 12.1`
`no service single-slot-reload-enable`
`service timestamps debug uptime`
`service timestamps log uptime`
`no service password-encryption`
	`r2#show run`
	`Building configuration...`
	
	`Current configuration : 1126 bytes`
	`!`
	`version 12.1`
	`no service single-slot-reload-enable`
	`service timestamps debug uptime`
	`service timestamps log uptime`
	`no service password-encryption`
		`r3#show run`
		`Building configuration...`
		
		`Current configuration : 1155 bytes`
		`!`
		`version 12.1`
		`no service single-slot-reload-enable`
		`service timestamps debug uptime`
		`service timestamps log uptime`
		`no service password-encryption`

```
!
hostname r1
!
enable secret 5
$1$rRCh$l/gq45mnz8zue7YbHMCA0.
!
!
!
!
!
memory-size iomem 15
ip subnet-zero
no ip domain-lookup
ip host web-server 10.4.0.20
ip host internet 207.64.4.5
ip host r3-e0 10.2.0.1
ip host r3-s1 10.1.0.6
ip host r2-e0 10.4.0.1
ip host r2-s1 10.1.0.5
ip host r2-s0 10.1.0.9
!
!
!
!
!
!
!
!
interface Serial0
 description Connection to R2
 ip address 10.1.0.10
255.255.255.252
 no fair-queue
 clockrate 64000
!
interface Serial1
 no ip address
 shutdown
!
!
!
interface FastEthernet0
 description R1 LAN
 ip address 10.3.0.1
255.255.255.128
 speed auto
!
!
router rip
 version 2
 network 10.0.0.0
 no auto-summary
!
!
ip classless
no ip http server
!
!
!
!
!
!
!
banner motd ^C
Welcome to R1
Authorized users only! ^C
!
line con 0
 exec-timeout 0 0
 password cisco
```

```
!
hostname r2
!
enable secret 5
$1$j9pi$ZLY1Mx5pnwtKkwHA3D85x1
!
!
!
!
!
memory-size iomem 15
ip subnet-zero
no ip domain-lookup
ip host web-server 10.4.0.20
ip host internet 207.64.4.5
ip host r3-s1 10.1.0.6
ip host r3-e0 10.2.0.1
ip host r1-s0 10.1.0.10
ip host r1-e0 10.3.0.1
!
!
!
!
!
!
!
!
interface Serial0
 description Connection to R1
 ip address 10.1.0.9
255.255.255.252
 no fair-queue
!
!
interface Serial1
 description Connection to R3
 ip address 10.1.0.5
255.255.255.252
 clockrate 64000
!
interface FastEthernet0
 description R2 LAN
 ip address 10.4.0.1
255.255.255.128
 ip access-group 101 out
 speed auto
!
router rip
 version 2
 network 10.0.0.0
 no auto-summary
!
!
ip classless
no ip http server
!
access-list 101 deny   tcp
10.3.0.0 0.0.0.127 host
10.4.0.20 eq www
access-list 101 permit ip any
any
!
banner motd ^C
Welcome to R2
Authorized users only! ^C
!
line con 0
 exec-timeout 0 0
 password cisco
```

```
!
hostname r3
!
enable secret 5
$1$FE0y$FwHFQE3TE1ZPBqG.tlP6V1
!
!
!
!
!
memory-size iomem 15
ip subnet-zero
no ip domain-lookup
ip host internet 207.64.4.5
ip host web-server 10.4.0.20
ip host r2-s1 10.1.0.5
ip host r2-e0 10.4.0.1
ip host r2-s0 10.1.0.9
ip host r1-s0 10.1.0.10
ip host r1-e0 10.3.0.1
!
!
!
!
!
interface Loopback0
 description Internet
 ip address 207.64.4.5
255.255.255.252
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
!
!
!
interface Serial1
 description Connection to R2
 ip address 10.1.0.6
255.255.255.252
!
!
interface FastEthernet0
 description R3 LAN
 ip address 10.2.0.1
255.255.255.128
 speed auto
!
!
router rip
 version 2
 redistribute static
 network 10.0.0.0
 no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0
Loopback0
no ip http server
!
!
!
!
!
banner motd ^C
Welcome to R3
Authorized users only! ^C
!
line con 0
 exec-timeout 0 0
 password cisco
```

logging synchronous login line aux 0 password cisco login line vty 0 4 password cisco login ! no scheduler allocate end	logging synchronous login line aux 0 password cisco login line vty 0 4 password cisco login ! no scheduler allocate end	logging synchronous login line aux 0 password cisco login line vty 0 4 password cisco login ! no scheduler allocate end

Routing Tables

R1

```
r1#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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 10.1.0.9 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.1.0.8/30 is directly connected, Serial0
R       10.2.0.0/25 [120/2] via 10.1.0.9, 00:00:04, Serial0
C       10.3.0.0/25 is directly connected, FastEthernet0
R       10.4.0.0/25 [120/1] via 10.1.0.9, 00:00:04, Serial0
R       10.1.0.4/30 [120/1] via 10.1.0.9, 00:00:04, Serial0
R*   0.0.0.0/0 [120/2] via 10.1.0.9, 00:00:04, Serial0
r1#
```

R2

```
r2#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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 10.1.0.6 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.1.0.8/30 is directly connected, Serial0
R       10.2.0.0/25 [120/1] via 10.1.0.6, 00:00:14, Serial1
R       10.3.0.0/25 [120/1] via 10.1.0.10, 00:00:20, Serial0
C       10.4.0.0/25 is directly connected, FastEthernet0
C       10.1.0.4/30 is directly connected, Serial1
R*   0.0.0.0/0 [120/1] via 10.1.0.6, 00:00:14, Serial1
r2#
```

R3

```
r3#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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 0.0.0.0 to network 0.0.0.0

     207.64.4.0/30 is subnetted, 1 subnets
C       207.64.4.4 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
R       10.1.0.8/30 [120/1] via 10.1.0.5, 00:00:23, Serial1
C       10.2.0.0/25 is directly connected, FastEthernet0
R       10.3.0.0/25 [120/2] via 10.1.0.5, 00:00:23, Serial1
R       10.4.0.0/25 [120/1] via 10.1.0.5, 00:00:23, Serial1
C       10.1.0.4/30 is directly connected, Serial1
S*   0.0.0.0/0 is directly connected, Loopback0
r3#
```

4- Troubleshooting / Reflection

I implemented these configurations on NetLab so could not fully test the ACL's.

Example IOS commands

☐ Develop IP address plan
☐ Draw map – label interfaces, DCE, IP networks, IP addresses, host names
☐ Notepad ACL's

Global Config

☐ clock set (optional)
```
[clock set 18:00:00 9 Feb 2006]
```
☐ router hostname
```
hostname boaz
```
☐ privilege mode PW
```
enable secret class
```
☐ no dns timeouts
```
no ip domain-lookup
```
☐ banner
```
banner motd #
```
☐ ip hosts
```
ip host boaz-e0 192.168.1.1
ip host internet 207.64.4.5
ip host web-server 192.168.3.20
```

Lines

☐ console
```
line con 0
 login
 password cisco
 logging synchronous
 exec-timeout 0 0
```
☐ aux
```
line aux 0
 login
 password cisco
```
☐ vty
```
line vty 0 4
 login
 password cisco
```

Interfaces

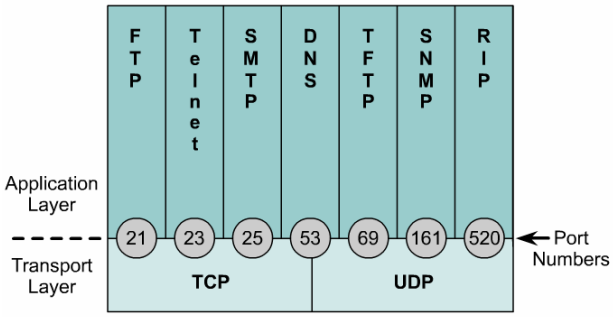
☐ int (s, l, e, f)
☐ ip
```
ip add 192.168.2.1 255.255.255.0
```
☐ description
```
description Connection to Boaz LAN
```
☐ clock rate
```
clock rate 64000
```
☐ enable
```
no shut
```

☐ **Static routes**
```
ip route 172.16.1.0 255.255.255.0 192.168.1.2
```

☐ **Default gateway**
```
ip route 0.0.0.0 0.0.0.0 192.168.1.2
ip route 0.0.0.0 0.0.0.0 l0
```
☐ **Routing protocols**
```
router rip
 version 2
  no auto-summary
  network 192.168.2.0
 network 192.168.3.0
  redistribute static
```
(only on router with static default GW)

☐ **convergence**
```
ping, extended ping
```
☐ **ACLs (use notepad)**

Class A: 0-127 (255.0.0.0) Class B: 128-191 (255.255.0.0) Class C: 192-223 (255.255.255.0) Class D: 224-239		/25 255.255.255.128 0.0.0.127 1000 0000 /26 255.255.255.192 0.0.0.63 1100 0000 /27 255.255.255.224 0.0.0.31 1110 0000 /28 255.255.255.240 0.0.0.15 1111 0000 /29 255.255.255.248 0.0.0.7 1111 1000 /30 255.255.255.252 0.0.0.3 1111 1100




```
1-99 standard IP
100-199 extended IP


More TCP:  www = 80

host n.n.n.n = n.n.n.n 0.0.0.0
any = 0.0.0.0 255.255.255.255

!verify ACL's
show access-lists
show running-config
show ip int s0
```

Anatomy Of An Access List

List No.	Rule	Pattern Definition						
access-list xxx (100-199)	permit or deny	IP or ICMP (TCP or UDP)	Source IP address xxx.xxx.xxx.xxx	Source IP address mask xxx.xxx.xxx.xxx 255=ignore 0=apply	Destination IP address xxx.xxx.xxx.xxx	Destination IP address mask xxx.xxx.xxx.xxx 255=ignore 0=apply	eq=equal gt=greater than lt=less than neq=not equal	TCP or UDP destination port no.
1	2	3	4	5	6	7	8	9

1) Every extended access list has a number from 100 to 199, which identifies the list in two places. When building the list, every line must be labeled with the same access list number. When you apply the list to an interface on the router, you must reference it by the same number. Version 11.2 of the IOS allows you to use a name for the list instead of a number.

2) A permit or deny rule has to be applied to every line or statement on the list.

3) If you are only filtering on IP address, you will specify IP (or ICMP for pings and trace routes) as the protocol. This means that only the IP address is considered for a match. If you are also filtering on UDP or TCP port, you must specify TCP or UDP.

4) Every line in the list must have a source address.

Required Optional

5) Every IP source address in the list must have a mask. The mask lets you determine how much of the preceding IP address to apply to the filter. In most cases, you will simply want to put a 255 corresponding to every octet in the IP address that you want to ignore, and 0 for every octet that you want the packet match to apply to.

6) Every line in the list must have a destination address.

7) Every IP destination address in the list must have a mask. See 5 above.

8) This applies to the TCP or UDP port that you are filtering on. In most cases, you will use the eq, which means equals. This gives you the ability to permit or deny TCP or UDP ports equal to the port specified. There are cases, however, where you will want to apply a range of port numbers, which is where the gt, greater than, or lt, less than, will come in handy.

9) If you have defined the pattern as a TCP or UDP packet, you will have to have an associated port number.

From: p118 Network Computing - *April 15, 1998* - www.networkcomputing.com

```
config t
  access-list 101 permit tcp 192.168.4.0
0.0.0.255 host 192.168.3.11 eq 80
  access-list 101 deny ip any host 192.168.3.11
  access-list 101 permit ip any any

  int e0
    ip access-group 101 out

  !removing ACL's
  no access-list 101
  int e0
    no ip access-list 101 out

!Named ACL example
config t
  ip access-list extended server-access
    permit TCP any host 131.108.101.99 eq smtp
    permit UDP any host 131.108.1.1.99
    deny ip any any log
    ^z

  int fa 0/0
  ip access-group server-access out
  ^z
! Corporate outgoing to Internet must be legit
access-list 101 permit ip 10.10.10.0 0.0.0.255
any
access-list 101 deny ip any any

! Corporate incoming from Internet
access-list 102 permit tcp any any established
access-list 102 permit icmp any any echo-reply
access-list 102 permit icmp any any unreachable
```

```
! protect web-server in DMZ
access-list 112 permit tcp any host 10.1.1.10
eq www
access-list 112 permit icmp 10.10.10.0
0.0.0.255 host 10.1.1.10

! prevent spoofing from Internet
access-list 121 deny ip 10.10.10.0 0.0.0.255
any
access-list 121 deny ip 127.0.0.0 0.255.255.255
any
access-list 121 deny ip 224.0.0.0
31.255.255.255 any
access-list 121 permit ip any any

!Disable telnet access to a router (
BillW@Cisco)
1) require an impossible login:
        line vty 0 4
        login
        no password

2) Line access lists:
        access-list 77 deny 0.0.0.0 0.0.0.0
        ! (implied deny everything else)
        line vty 0 4
        access-class 77 in

3) Transport command:
        line vty 0 4
        transport input none

4) autocommand:
        line vty 0 4
        autocommand quit
```

```
!Anything after the ! is a comment and ignored by IOS

!Classful networks
!
!  Class A:   0-127   255.0.0.0
!  Class B: 128-191   255.255.0.0
!  Class c: 192-223   255.255.255.0
!  Class D: 224-239


!*****************
! Privilege Mode
!*****************
enable
disable


!************************************
! global configuration mode
!************************************
clock set 18:00:00 9 Feb 2006
config t

  hostname SanJose1

  !Suppress dns lookup delays
  no ip domain lookup

  !enable privileged mode password
  enable secret class

  !not really secure
  service password-encryption

  !configure console password & suppress annoyances
  line con 0
    login
    password cisco
    logging synchronous
    exec-timeout 0 0
    exit

  !configure console password & suppress annoyances
  line aux 0
    login
    password cisco
    exit

  !configure telnet password
  line vty 0 4
    login
    password cisco

  !configure message of the day
  banner motd #
  Warning!
  Authorized Access Only #

  !To create local host names to reference IP addresses
  ip host boaz 192.168.1.1
```

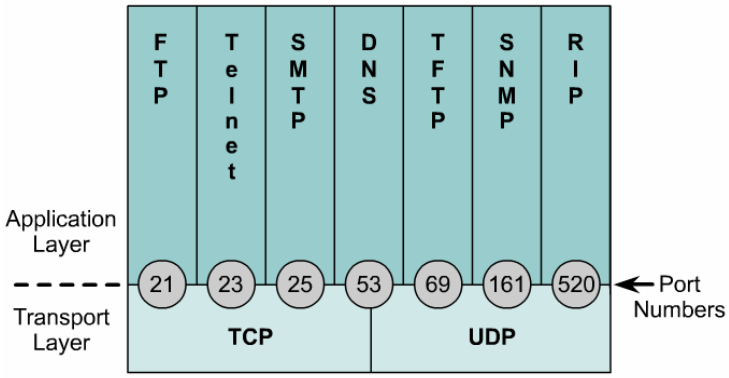
```
  ip host center 192.168.1.2
  no ip host center 192.168.1.2

!to verify
shows hosts
show run

!*****************************
!  Configure router interfaces
!*****************************

conf t
  int fa0
  int e0
    ip add 192.168.2.1 255.255.255.0
    no ip add 192.168.2.1 255.255.255.0
    description Connection to Boaz LAN
    no shut

  int s0
  int s1
    ip add 192.168.2.1 255.255.255.0
    no ip add 192.168.2.1 255.255.255.0
    !DCE end needs clock rate
    clock rate 64000
    description Connection to Boaz
    no shut

  interface loopback 0
    description Loopback Interface of CORE-GW3
    ip address 215.18.3.34 255.255.255.255

!to verify
show ip int brief
show int s0
show ip int s0
show run

!***********************
! Create static routes
!***********************

!set route using net hop address
conf t
  ip route 172.16.1.0 255.255.255.0 192.168.1.2
  no ip route 172.16.1.0 255.255.255.0 192.168.1.2

!Setup default routes
conf t
  ip route 0.0.0.0 0.0.0.0 192.168.1.2
  no ip route 0.0.0.0 0.0.0.0 192.168.1.2
  ip route 0.0.0.0 0.0.0.0 s1
  exit

!Alternate default GW that works with RIP and IGRP advertisements
conf t
  ip default-network 10.0.0.0
  exit

! to view routing table
show ip route
```

```
!******************
! Configuring RIP
!******************


!RIP v1
conf t
  router rip
    ! add only directly connected classful network for RIP to advertise
    network 192.168.4.0
    network 172.30.0.0

    !propogate default GW (worked on older lab routers)
    default-information originate

    !propogate default GW (for NetLab & lab)
    redistribute static

    !suppress announcements to stub networks
    passive-interface e0

  !alternative way to specify & propagate default route
  ip default-network  10.0.0.0

!RIP v2
conf t
  router rip
    version 2
    no auto-summary
    network 192.168.2.0
    network 192.168.3.0
```

	d-n	rs	d-io
2500 (Sydney/Istanbul)	yes	yes	yes
1700 (Singapore)		yes	
1700 (NetLab)		yes	no

```
show ip protocols
debug ip rip
undebug ip rip
undebug all

clear arp-cache
clear ip route *

!******************
! Configuring IGRP
!******************

config t
  router igrp 10
    network 192.15.25.0
    network 172.30.0.0

! Trace IGRP updates
debug ip igrp events
debug ip igrp transactions
! Changing bandwidth
conf t
```

```
  int s0
    bandwidth 128

! Configure IGRP timers for fast convergence
conf t
  router igrp 364
    timers basic 15 45 0 60
    no metric holddown
    metric maximum-hop 50

!***********************
! access control lists
!***********************

1-99 standard IP
100-199 extended IP
```




```
More TCP:  www = 80
```

Anatomy Of An Access List

List No.	Rule	Pattern Definition						
access-list xxx (100-199)	permit or deny	IP or ICMP TCP or UDP	Source IP address xxx.xxx.xxx.xxx	Source IP address mask xxx.xxx.xxx.xxx 255=ignore 0=apply	Destination IP address xxx.xxx.xxx.xxx	Destination IP address mask xxx.xxx.xxx.xxx 255=ignore 0=apply	eq=equal gt=greater than lt=less than neq=not equal	TCP or UDP destination port no.
1	2	3	4	5	6	7	8	9

1) Every extended access list has a number from 100 to 199, which identifies the list in two places. When building the list, every line must be labeled with the same access list number. When you apply the list to an interface on the router, you must reference it by the same number. Version 11.2 of the IOS allows you to use a name for the list instead of a number.

2) A permit or deny rule has to be applied to every line or statement on the list.

3) If you are only filtering on IP address, you will specify IP (or ICMP for pings and trace routes) as the protocol. This means that only the IP address is considered for a match. If you are also filtering on UDP or TCP port, you must specify TCP or UDP.

4) Every line in the list must have a source address.

5) Every IP source address in the list must have a mask. The mask lets you determine how much of the preceding IP address to apply to the filter. In most cases, you will simply want to put a 255 corresponding to every octet in the IP address that you want to ignore, and 0 for every octet that you want the packet match to apply to.

6) Every line in the list must have a destination address.

7) Every IP destination address in the list must have a mask. See 5 above.

8) This applies to the TCP or UDP port that you are filtering on. In most cases, you will use the eq, which means equals. This gives you the ability to permit or deny TCP or UDP ports equal to the port specified. There are cases, however, where you will want to apply a range of port numbers, which is where the gt, greater than, or lt, less than, will come in handy.

9) If you have defined the pattern as a TCP or UDP packet, you will have to have an associated port number.

Required Optional

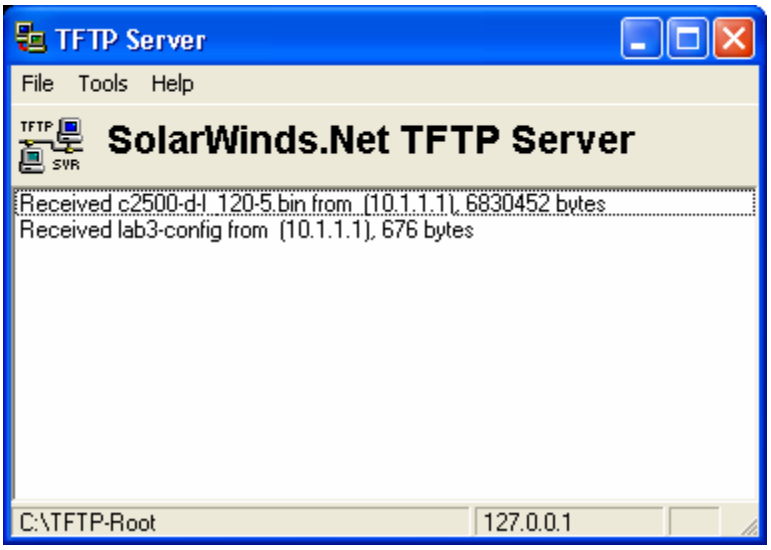
From: p118 Network Computing - *April 15, 1998* - www.networkcomputing.com

```
config t
  access-list 101 permit tcp 192.168.4.0 0.0.0.255 host 192.168.3.11 eq 80
  access-list 101 deny ip any host 192.168.3.11
  access-list 101 permit ip any any

  int e0
```

```
    ip access-group 101 out

  !removing ACL's
  no access-list 101
  int e0
    no ip access-list 101 out

!Named ACL example
config t
  ip access-list extended server-access
    permit TCP any host 131.108.101.99 eq smtp
    permit UDP any host 131.108.1.1.99
    deny ip any any log
    ^z

  int fa 0/0
  ip access-group server-access out
  ^z

!advanced ACL's
access-list 102 permit tcp any any established
access-list 102 permit icmp any any echo-reply
access-list 102 permit icmp any any unreachable


!verify ACL's
show access-lists
show running-config
show ip int s0

!Disable telnet access to a router (from BillW@Cisco)
1) require an impossible login:
        line vty 0 4
        login
        no password

2) Line access lists:
        access-list 77 deny 0.0.0.0 0.0.0.0
        ! (implied deny everything else)
        line vty 0 4
        access-class 77 in

3) Transport command:
        line vty 0 4
        transport input none

4) autocommand:
        line vty 0 4
        autocommand quit



!********
! debug
!********

debug ip packet
undebug ip packet
undebug all

debug ip rip
```

```
undebug ip rip
undebug all

clear arp-cache
clear ip route *

!to monitor debug on telnet sessions
terminal monitor
terminal no monitor

ping 192.168.3.1

!extended ping
R1#ping
Protocol [ip]:
Target IP address: 12.1.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 11.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.1.1.1, timeout is 2 seconds:
!!!!!

!*****************************
! manage configuration files
!*****************************

show running-config
show run

show startup-config
show start

copyt running-config startup-config
copy start run
wr


!*********************************************
! document router configuration and operation
!*********************************************

show running-config
show startup-config

show ip interface brief
show ip route
show ip protocol
show cdp neighbors
show version

show interfaces
show controllers
```

```
show cdp interface
show cdp neighbor
show cdp neighbor detail
show cdp entry Baypoint


!*******
! TFTP
!*******

simms#copy startup-config tftp
Address or name of remote host []? con
Destination filename [startup-config]? lab3-config
!!
676 bytes copied in 0.240 secs
simms#
```




```
oops#copy tftp startup-config
Address or name of remote host []? 10.1.1.2
Source filename []? lab3-config
Destination filename [startup-config]?
Accessing tftp://con/lab3-config...
Loading lab3-config from 10.1.1.2 (via Ethernet0): !
[OK - 676/1024 bytes]

676 bytes copied in 10.892 secs (67 bytes/sec)

!*********************************************************
! Password recovery
!
! Break in during boot, change config register to bypass
! startup-config then reset password
!*********************************************************

conf t
  !normal boot
  configure-register 0x2102
  !boot into ROM code
  configure-register 0x42
```

```
! to recover password
<< reboot  – enter multiple alt-b's >>

System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
Copyright (c) 1986-1995 by cisco Systems
2500 processor with 8192 Kbytes of main memory

Abort at 0x10EA82E (PC)
>
>o/r 0x42
>i

System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
Copyright (c) 1986-1995 by cisco Systems
2500 processor with 8192 Kbytes of main memory

F3: 6741816+88604+453712 at 0x3000060

             Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

          cisco Systems, Inc.
          170 West Tasman Drive
          San Jose, California 95134-1706


Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(5), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 15-Jun-99 20:08 by phanguye
Image text-base: 0x030380DC, data-base: 0x00001000

cisco 2500 (68030) processor (revision D) with 8192K/2048K bytes of memory.
Processor board ID 01730642, with hardware revision 00000000
Bridging software.
X.25 software, Version 3.0.0.
Basic Rate ISDN software, Version 1.1.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!


simms(config)#enable secret correct password
simms(config)#config-register 0x2102


!
! Boot from TFTP server
!
Router#copy flash tftp
Source filename []? c2500-d-l_120-5.bin
Address or name of remote host []? 10.1.30.2
Destination filename [c2500-d-l_120-5.bin]?

! Change the boot order commands
Router# configure terminal
Router(config)# boot system tftp ma-c2500-d-l_120-5.bin 10.1.30.2
Router(config)# boot system flash
Router(config)# end
Router# copy running-config startup-config
Router# show startup-config
```

```
!**********
! Cleanup
!**********

erase startup-config
erase nvram
```