Introduction

This document is a tutorial related to the Router Emulator which is available at:

http://www.dcs.napier.ac.uk/~bill/router.html

A demo is also available at:

http://www.dcs.napier.ac.uk/~bill/router_demo.htm

The requirements for it are:

- Macromedia Flash 6.

Please note that this version is for demonstration purposes only, and the full version is available by registering from the above page. The full version has the following features:

- EXE program.
- Full implementation of commands.
- No time limitation.
- Multiple routers, which are interconnected.
- Fault simulation.
- Cisco Switch, Wireless and UNIX networking emulations.

User and Privileged EXEC mode

The router has two main modes:

- **User mode**. This is the initial mode that the user goes into when they log onto the router. In this mode it is not possible to configure the router, and it is only possible to perform simple commands such as telnet and ping.
- **Executive mode**. In this mode the full range of commands can be used, and the router can be programmed.

The command which is used to go from user mode into executive mode is `enable`. If a password is set for the executive mode, the user must enter this before they can enter into the executive mode. The prompt should change from a '>' to a '#'. The following gives an example:

1 Enter ? command to show the commands in the User Exec mode.
Outline some of the commands that are listed?

2 Enter Priv. Exec mode with the enable command.

3 Enter ? command to show the commands in the Priv. Exec mode.
Outline some of the commands that are listed?

Setting the host name

The hostname is set using the `hostname` command. This name is reflected in the prompt of the router, and makes it easier to identify the current router.

1 Go into the privileged mode by typing enable.
How does the prompt change?

2 Use the ? command to view the commands in this mode.
What commands are available in Privileged Exec mode?

3 Configure the device using by typing config t.
How does the prompt change?

4 Set the hostname by typing hostname myhost.

5 Go back to the user executive mode with the command exit.

6 Show the main system configuration with show running-config.
What are the parameters displayed?

Using show

1 Go into Priv. Exec. mode.

2 Use the show buffers command.

3 Use the show memory command.

4 Use the show stacks command.

5 Use the show hosts command.

6 Use the show arp command.

7 Use the show flash command.

8 Use the show version command.

9 Use the show protocols command.

10 Use the show interface e0 command.

11 Use the show interface s0 command.

12 Use the show interface s1 command.

Using CDP (Cisco Discovery Protocol)

The CDP allows the discovery of the other devices which connect to the local device.

1 Enter show cdp neighbors command.
Which devices are connected to yours?

2 Enter show cdp neighbors details command.

Saving the configuration

The changes that are made are made only to the running configuration (running-configuration). Once the user has verified that the new changes are okay, they should copy the running configuration into the startup configuration (startup-configuration). Once this is done, the router will startup with the updated changes. To do this the copy running-config startup-config command is used.

1 Go to the configuration mode (that is, with the (config) # prompt).

2 Use the copy running-config startup-config command.

Other methods include:

copy running-config tfp which copies the running config to the TFTP server.
copy tftp running-config which copies from the TFTP server to the current running config.

Showing your commands

The router stores all the previous commands, which can be recalled with the show history command.

1 Use the show history to display the previous commands.

Scrolling through previous commands

The UP and DOWN arrow keys can be used to scroll through the previous command, of which the user can select any of them, as required.

1 Use the UP and DOWN arrows to scroll through the command.

Setting Line Console parameters

The console password is set by using the line con 0 command from the Privileged Exec mode, and then using the password command.

1 Go to the privileged interface mode (that is, with the (config) # prompt). Next configure the third Ethernet port with the line con 0 (which is the short form of line console 0)

2 Use the password fred command to set the password to fred.

3 Go back to the privileged mode (#) and run show running-config, and check that the parameters have been set.

Adding passwords

There are two main passwords. The first is for the EXEC level, and the second is for the Privileged EXEC level.

1 Go into privileged EXEC level (config)#, and enter enable password level 1 fred, to change the EXEC password to fred.

2 Go into privileged EXEC level (config)#, and enter enable password level 15 bert, to change the privileged EXEC password to bert.

3 Show running-config, and prove that the passwords have been set.

Programming the ports

The router has three ports (e0, s0 and s1). One of the most important things to set on the router is the IP address of each of the ports. These ports will be used as gateways out of the network segment to which they connect to. The `interface` command (or `int` for short) programs each of the interfaces. In the following example, the three ports on the router are programmed with the required IP addresses, and subnet masks. The ports will not automatically come on-line, and will start in a shutdown mode. Thus the no shutdown command is used to start them up. They are programmed with:

1 Go to Priv Exec mode

2 Enter config t command.

3 Enter interface e0 command to program the ethernet 0 port.

4 Enter ip address 192.5.5.1 255.255.255.0 command.

5 Enter no shutdown command.

6 Enter exit command.

7 Enter interface s0 command to program the serial 0 port.

8 Enter ip address 205.7.5.1 255.255.255.0 command.

9 Enter no shutdown command.

10 Enter exit command.

11 Enter interface s1 command to program the serial 1 port.

12 Enter ip address 201.100.11.1 255.255.255.0 command.

13 Enter clock rate 56000 command to set the clock rate of the serial port to 56kbps.

14 Enter no shutdown command.

15 Enter exit command.

16 Enter show protocols command to see if the IP addresses have been changed.

Other interface commands include:

keepalive 10 - Set the time interval for the keepalive signal (in this case to 10 seconds).
bandwidth 64 - Set the bandwidth on the port (in this case to 64 kbps).

Ping'ing the ports

The show protocols command shows if the ports are UP, but the best way to really test them is to use the ping command.

1 Go to Priv Exec mode

2 Enter ping 192.5.5.1 and prove that the port is alive.

3 Enter ping 205.7.5.1 and prove that the port is alive.

4 Enter ping 201.100.11.1 and prove that the port is alive.

5 Enter interface e0 command to program the serial 0 port.

6 Enter shutdown command.

7 Enter exit command.

8 Enter interface s0 command to program the serial 0 port.

9 Enter shutdown command.

10 Enter exit command.

11 Enter interface s1 command to program the serial 0 port.

12 Enter shutdown command.

13 Enter exit command.

14 Enter ping 192.5.5.1 and prove that the port is not alive.

15 Enter ping 205.7.5.1 and prove that the port is not alive.

16 Enter ping 201.100.11.1 and prove that the port is not alive.

Setting a routing protocol to RIP

RIP is one of the most widely used routing protocols, and measures the best route by the number of hops that it takes to get to a destination.

1 Go to Priv Exec mode

2 Enter config t command.

3 Enter router rip command to define the RIP protocol.

4 Enter network 192.5.5.0 command.

5 Enter network 205.7.5.0 command.

6 Enter network 201.100.11.0 command.

7 Enter exit command.

8 Enter exit command.

9 Enter show running-config command to see if the networks have been added.

Removing a network

Often it is not required that the routing table is broadcast into some of the connected networks, thus to remove a network:

1 Go to Priv Exec mode

2 Enter config t command.

3 Enter router rip command, where 111 is the AS number.

4 Enter no network 205.7.5.0 command.

5 Enter exit command.

6 Enter exit command.

7 Enter show running-config command to see if the networks have been deleted.

Setting a routing protocol to IGRP

IGRP is an improvement on RIP, and it based on an AS (Autonomous System) number.

1 Go to Priv Exec mode.

2 Enter config t command.

3 Enter router igrp 111 command, where 111 is the AS number.

4 Enter network 192.5.5.0 command.

5 Enter network 205.7.5.0 command.

6 Enter network 201.100.11.0 command.

7 Enter exit command.

8 Enter exit command.

9 Enter show running-config command to see if the networks have been added.

Setting the name server

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 From the config mode,set the domain-name is mycomp.com, the name-server to 192.168.0.10, using:

```
(config)# ip domain-name mycomp.com
(config)# ip name-server 192.168.0.10
```

4 Go back to the user executive mode with the command exit.

5 Show the main system configuration with show running-config.

Setting up host names

Apart from setting up a name server, it is also possible to assign names locally in a hosts table. These map domain names to associated IP addresses.

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 From the config mode, set the host names with:

```
(config)# ip host LAB_A 192.5.5.1 205.7.5.1 201.100.11.1
```

```
(config)# ip host LAB_B 201.100.11.2 219.17.100.1 199.6.13.1
(config)# ip host LAB_C 223.8.151.1 204.204.7.1
(config)# ip host LAB_D 210.93.105.1 204.204.7.2
(config)# ip host LAB_E 210.93.105.2
```

4 Go back to the user executive mode with the command exit.

5 Show the main system configuration with show running-config.

6 Show the hosts configuration with show hosts.

Defining encapsulation

Encapsulation allows data packets to be wrapped in a defined protocol, and send over an Internet connection. One of the most popular encapsulation techniques is PPP (which is the standard used to connect users to the Internet from a modem). This is achieved with:

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 Define the encapsulation on s0 with:

```
(config)# interface s0
(config-if)# encapsulation ppp
```

4 Go back to the user executive mode with the command exit, followed by exit

5 Show the main system configuration with show running-config.

Defining authentication

Along with encapsulation, there is normally an authentication for the connection. In the following the authentication is defined as chap (which is more secure than pap).

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 Define the authentication technique with:

```
(config)# interface s0
(config-if)# ppp authentication chap
```

4 The CHAP protocol continually challenges the remote router for a user name and a password. Thus we must define a username and password (in this case a username of fred with a password of mypass):

```
(config)# username fred password mypass
```

5 Finally on the required interface we set the hostname and the password for the remote router:

```
(config)# interface s0
(config-if)# ppp chap hostname fred
(config-if)# ppp chap password mypass
```

6 Go back to the user executive mode with the command exit, followed by exit

7 Show the main system configuration with show running-config.

Defining ACLs

Access Control Lists (ACLs) allow for incoming and outgoing data to be filtered, and are used to implement firewalls. A simple example is:

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 To deny access from the incoming E0 port to every host on the 156.1.1.0 subnet:

```
(config)# access-list 1 deny 156.1.1.0 0.0.0.255
(config)# interface e0
(config-if)# ip access-group 1 in
```

4 Go back to the user executive mode with the command exit, followed by exit

5 Show the main system configuration with show running-config.

At this point the running-config should look something like:

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
Hostname Router
!
!
ip subnet-zero
!
ip domain-name mycomp.com
ip name-server 192.168.0.10
!
interface ethernet 0
 ip address 219.17.100.1 255.255.255.0
 no shutdown
 ip access-group 1 in
!
interface serial 0
 ip address 199.6.13.1 255.255.255.0
 no shutdown
```

```
 encapsulation ppp
 ppp authentication chap
!
interface serial 1
 ip address 201.100.11.2 255.255.255.0
 no shutdown
 encapsulation ppp
 ppp authentication chap
!
router rip
 network 199.6.13.0
 network 201.100.11.0
 network 219.17.100.0
!
access-list 1 deny 156.1.1.0 0.0.0.255
!
ip host LAB_A 192.5.5.1 205.7.5.1 201.100.11.1
ip host LAB_B 210.100.11.2 219.17.100.1 199.6.13.1
ip host LAB_C 223.8.151.1 204.204.7.1 199.6.13.1
ip host LAB_D 210.93.105.1 204.204.7.2
ip host LAB_E 210.93.105.2
!
end
```

Defining ACLs using Named ACLs

It is also possible to define an ACL by a name. For example, the following permits accesses from the 10.11.12.0 and 20.31.42.0 subnets, and disallows all other subnets:

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 To deny access from the incoming E0 port to every host on the 156.1.1.0 subnet:

```
(config)# access-list standard myacl
(config-std-nacl)# permit 10.11.12.0 0.0.0.255
(config-std-nacl)# permit 20.31.42.0 0.0.0.255
(config-std-nacl)# exit
(config)# int e0
(config-if)# ip access-group myacl out
(config-if)# exit
```

4 Go back to the user executive mode with the command exit

5 Show the main system configuration with show running-config.

An extended NACL is defined with access-list extended myextacl.

IP unnumbered

An IP unnumbered approach allows a port to borrow an IP address from an unused address on a connected network. For example to assign an address from the network which connects to EO to S1:

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 Then:

```
(config)# interface s1
(config-if)# ip unnumbered e0
```

4 Go back to the user executive mode with the command exit, followed by exit.

5 Show the main system configuration with show running-config.

Implementing NAT

NAT (Network Address Translation) allows the mapping of internal private addresses to one or more public addresses. For NAT, the internal addresses are defined as inside, and the public interface is outside. This to define the addresses on EO as internal, and S0 as external:

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 Then:

```
(config)# interface e0
(config-if)# ip nat inside
(config-if)# exit
(config)# interface s0
(config-if)# ip nat outside
```

4 Go back to the user executive mode with the command exit, followed by exit

5 Show the main system configuration with show running-config.

Defining SNMP

The SNMP-server command is used to enable SNMP monitoring, such as:

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 The snmp-server community command is used to initialise SNMP. For example to define the read-only string to public:

```
(config)# snmp-server community public RO
```

or for read-write access use RW instead of RO. The community access string (in this case, public) acts as a password for the access to the SNMP information. To setup the SNMP contact:

```
(config)# snmp-server contact fred smith
```

and to set the location:

```
(config)# snmp-server location room c27
```

To enable SNMP traps so that all the data is monitored:

```
(config)# snmp-server enable traps
```

and to send these traps to a remote host (to www.myhost.com):

```
(config)# snmp-server host www.myhost.com public
```

4 Go back to the user executive mode with the command exit

5 Show the main system configuration with show running-config.

6 To show SNMP event values:

```
# show management event
```

and to determine the status of the SNMP communications:

```
# show snmp
```

and to display the SNMP engine and remote engines:

```
# show snmp engine
```

and to display the SNMP group:

```
# show snmp group
```

SNMP uses an MIB database to store its values. To display its contents:

```
# show snmp mib
```

To show the currently pending SNMP requests:

```
# show snmp pending
```

To show the SNMP sessions:

```
# show snmp sessions
```

7 Show the main system configuration with show running-config.

Adding a description to the interface

The description command can be added to the interface, such as:

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 Then:

```
(config)# interface e0
(config-if)# description Bert's Port
```

4 Go back to the user executive mode with the command exit, followed by exit

5 Show the main system configuration with show running-config.

Defining SNTP

The SNTP (Simple Network Time Protocol) can be used to allow the router to listen to Time Servers. This achieved with:

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 Then to enable the router to receive broadcasted NTP packets from a time server:

```
# config t
(config) # sntp broadcast client
```

4 Go back to the user executive mode with the command exit.
5 For the SNTP (Simple Network Time Protocol):

```
# show sntp
```

Showing other statistics

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 Then:

```
# show tcp
```

4 For the reload details:

```
# show reload
```

5 For the boot details:

```
# show boot
```

6 For the aliases:

```
# show aliases exec
```

7 For system crashes

```
# show context
```

8 or:

```
# show context summary
```

9 To show debugging:

```
# show debugging
```

10 To show environment details:

```
# show environment
```

Defining a MOTD

The Message of the Day (motd) is show when someone logs into the router, and is setup by:

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 Then:

```
(config)# banner motd # This is my router #
```

4 Go back to the user executive mode with the command exit, followed by exit

5 Show the main system configuration with show running-config. Also apply a SLIP/PPP banner, with:

```
(config)# banner slip-ppp # Welcome to the SLIP/PPP login #
```

IP interface options

There are many IP options which can be applied to an interface:

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 Then:

```
(config)# interface e0
(config-if)# ip ?
```

4 You can also view the commands available from each mode with the ? key.

5 Then:

```
> ?
> enable
# ?
# config t
(config)# ?
(config)# interface e0
(config-if)# ?
```

Configuring DHCP

Routers can run DHCP, which grants IP addresses to hosts.

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 Then:

```
(config)# ip dhcp pool pool1
(config-dhcp)# network 192.5.5.0/24
(config-dhcp)# exit
```

4 Go back to the user executive mode with the command exit, followed by exit

5 Show the main system configuration with show running-config. To get rid of DHCP, use:

```
(config)# no ip dhcp pool pool1
```

Static route

A static route can be setup which does not require the transmission of routing tables:

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 Then:

```
(config)# ip route 192.168.0.0 255.255.255.0 140.10.20.30
(config)# ip default-network 192.168.0.0
(config)# exit
```

4 Go back to the user executive mode with the command exit

5 Show the main system configuration with show running-config.

Enabling IPX routing

Cisco routers can also be used to route IPX networks (such as those used in Novel Netware).

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 Then:

```
(config)# ipx routing
(config)# interface e0
(config-if)# ipx network 5
(config-if)# exit
(config)# exit
```

4 Go back to the user executive mode with the command exit

5 Show the main system configuration with show running-config. To get rid of IPX routing, use:

```
(config)# no ipx routing
```

Enabling AppleTalk routing

Cisco routers can also be used to route AppleTalk networks (such as those used in Apple-based systems).

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 Then:

```
(config)# appletalk routing
(config)# interface e0
(config-if)# appletalk zone Sales_Dept
```

```
(config-if)# appletalk cable-range 1-1
(config-if)# exit
(config)# exit
```

4 Go back to the user executive mode with the command exit

5 Show the main system configuration with show running-config. To get rid of AppleTalk routing, use:

```
(config)# no appletalk routing
```

Enabling DECnet routing

Cisco routers can also be used to route DECnet networks (such as those which use VAX/DEC-type equipment).

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 Then:

```
(config)# decnet routing
(config)# exit
```

4 Go back to the user executive mode with the command exit

5 Show the main system configuration with show running-config. To get rid of DECnet routing, use:

```
(config)# no decnet routing
```

Context-based Access Control

Context-based Access Control is used to implement firewall options, such as limiting the number of open connections. A typical attack is the DoS (Denial of Service) attack, where the external party open up multiple connections. To overcome this the router can be setup to detect a minimum threshold for half-open sessions. This can be achieved with:

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 Then to limit the maximum open sessions at any time to between 900 and 1100:

```
(config)# ip inspect max-incomplete low 900
(config)# ip inspect max-incomplete high 1100
```

and for the maximum open sessions for one-minute:

```
(config)# ip inspect one-minute low 900
(config)# ip inspect one-minute high 1100
(config)# exit
```

4 Go back to the user executive mode with the command exit, followed by exit

5 Show the main system configuration with show running-config. To get rid of IP inspect, use:

```
(config)# no ip inspect one-minute low
```

To limit the DNS-timeout to 10 seconds:

```
(config)# ip inspect dns-timeout 10
```

Defining a Syslog server

The router can be setup to sent system logging information to a remote server which supports Syslog (which is UDP port 514). For example to send it to 192.168.0.20:

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 Then:

```
(config)# logging 192.168.0.20
```

4 Go back to the user executive mode with the command exit

5 Show the main system configuration with show running-config.

IDS (Intrusion Detection System)

An IDS can be used to detect intruders into the system. This is normally applied at the perimeter of the network. To setup a SPAM filter which sets a threshold of 30 users receiving the same email message:

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 Then:

```
(config)# ip audit log
(config)# ip audit smtp spam 30
```

4 Go back to the user executive mode with the command exit

5 Show the main system configuration with show running-config.

Alarm interface

The alarm interface gives access to alarm interface. For example for the alarm interface in Slot 5:

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 Then:

```
(config)# alarm-interface 5
(config-aic)# ip address 192.10.0.10
(config-aic)# reset
Alarm Interface Card in slot 5 restarted
(config)# exit
```

4 Go back to the user executive mode with the command exit, followed by exit

5 Show the main system configuration with show running-config. To get rid of DHCP, use:

```
(config)# no ip dhcp pool pool1
```

Authentication, authorization and accounting (AAA)

The main elements of security are AAA. These allows for enhanced security for who is allowed to log into a network, and what they are allowed to do, and logs the things that they have done. Typically this security is applied at the edge of a network, using a network access server (NAS). This server contains a database of users and their associated passwords, and any other configuration. On routers there are three main security protocols: TACACS+, RADIUS and Kerberos. On a router, AAA is enabled with:

1 Go into the privileged mode by typing enable.

2 Configure the device using by typing config t.

3 Then a model is defined with:

```
(config)# aaa new-model
```

4 For TACACS+, the IP address of the TACACS+ server is specified with:

```
(config)# tacacs-server host 192.168.0.10
```

5 Next the encryption key is specified with:

```
(config)# tacacs-server key mypass
```

6 For RADIUS, the IP address of the RADIUS server is specified with:

```
(config)# radius-server host 192.168.0.10
```

7 Next the encryption key is specified with:

```
(config)# radius-server key mypass
```

8 Go back to the user executive mode with the command exit

9 Show the main system configuration with show running-config.

Other commands implemented

# help	
# show ip aliases	to enable the usage of the .0 subnet (use no ip subnet-zero to disable it).
# show ip idrp	to display details of IDRP (ICMP Discovery Routing Protocol).
# show ip netmasks	to display details of netmasks used on a given subnet address.
# show ip nat statistics	to display details of NAT (Network Address Translation).
# show ip nat translations	to display details of NAT translations.
# show ip nat translations verbose	to display details of port translations in NAT.
# show ip snat	to display active SNAT (Stateful Network Address Translation) translations.
# clear counters	clear counters on interfaces.
# show ip nhrp	to display NHRP details.
# show ip nhrp traffic	to display NHRP traffic.
# show ip rip database	to display rip database.
# show ip route summary	show summmary details of a route.
# show ip route	show details of a route.
# show flash: chips	show details of Flash devices.
# show flash: filesys	show details of file system on the Flash devices.
# show flash: all	show all the details of the Flash.
# show flash: detailed	show detailed information of the Flash.
# show memory scan	show if there are any memory errors.
# show ip http server all	show HTTP server details.
# show ip http server status	show HTTP server status.
(config)# ip http max-connections 5	set the maximum connections to 5 for the HTTP server.
(config)# ip default-gateway w.x.y.z	which defaults the default gateway when routing is disabled
(config)# ip classless	defines classless IP addresses

(config)# ip directed-broadcast	enable the translation of directed broadcasts to physical broadcasts
(config)# ip domain-list	define list of default domain names for unqualified host names
(config)# ip domain-lookup	enable DNS lookup service
(config)# ip forward-protocol	specify the ports which forwards broadcasts
(config)# ip netmask-format bitcount	display netmask in bit count format (such as 192.168.0.10/24).
(config)# ip netmask-format decimal	display netmask in decimal format (such as 255.255.255.0).
(config)# ip netmask-format hexadecimal	display netmask in hexadecimal format (such as 0xFFFFFF00).
(config)# no ip routing	disable routing (use ip routing to enable it).
(config)# ip subnet-zero	to enable the usage of the .0 subnet (use no ip subnet-zero to disable it).
(config)# router odr	enable ODR (On-demand routing) routing (use no router odr to disable it).
(config)# cdp run	enable CDP on router
(config)# no cdp run	disable CDP on router (recommended for security purposes).
(config-if)# cdp enable	enable CDP on an interface.
(config-if)# no cdp enable	disable CDP on an interface.
(config-if)# carrier-delay 5	defines carrier-delay on a serial port (in this case 5 seconds).
(config-if)# cut-through	defines cut-through switching on an Ethernet port (cut-through forwards the data frame before it has been fully received on the incoming port).
(config-if)# duplex full	defines full duplex on an Ethernet port.
(config-if)# duplex half	defines half duplex on an Ethernet port.
(config-if)# duplex auto	defines auto duplex on an Ethernet port.
(config-if)# speed 10	defines 10Mbps rate on an Ethernet port.
(config-if)# speed 100	defines 100Mbps rate on an Ethernet port.
(config-if)# ip split-horizon	enables split-horizon on the interface.
(config-if)#ip nhrp	enables NHRP (Next Hop Resolution Protocol).
(config-if)# ip proxy-arp	enable proxy Address Resolution Protocol on an interface.
(config-router)# neighbor w.x.y.z	defines the router (w.x.y.z) in which to broadcast the routing information to.
(config-router)# version 2	defines RIP Version 2 (or Version 1 can be used).

Additional:

ACLs can also be extended ACL, such as, to block Napster traffic destined for port 8888:

```
(config)# access-list 100 deny tcp 192.5.5.0 0.0.0.255 any eq 8888 log
(config)# access-list 100 deny udp 192.5.5.0 0.0.0.255 any eq 8888 log
(config)# interface e0
(config-if)# ip access-group 100 in
```

or Kazaa (on port 1214):

```
(config)# access-list 101 deny tcp 192.5.5.0 0.0.0.255 any eq 1214 log
(config)# access-list 101 deny udp 192.5.5.0 0.0.0.255 any eq 1214 log
(config)# interface e0
(config-if)# ip access-group 101 in
```

Gnutella can be blocked with ports 6346 and 6347, while ICQ is blocked with 5190.

Note. If you want to see the completed configuration, please type the command **complete** at any point, and the configuration should be set, to the configuration defined in the previous sections.

W.Buchanan, 15 July 2003.

If you have any questions, please contact w.buchanan@napier.ac.uk