Basic Router Configuration

Our building network consists of a distribution (aggregation) router and two edge routers. Each building distribution router connects to the core router of our campus network and serve as aggregation points for all the edge routers. Edge routers serve the end users.

Each router will be named according to the table above: core1.campus1, dist1-b1.campus1, edge2-b1.campus5, etc

Device	Interface	Remote Device	Remote Interface
dist1-bY.campusX	GigabitEthernet1/0	edge1-bY.campusX	GigabitEthernet0/0
	GigabitEthernet1/1	edge1-bY.campusX	GigabitEthernet0/1
	GigabitEthernet2/0	edge2-bY.campusX	GigabitEthernet0/0
core1.campusX	GigabitEthernet0/0	bdr1.campusX	GigabitEthernet0/1
	GigabitEthernet0/1	dist1-b1.campusX	GigabitEthernet0/0
	GigabitEthernet0/2	dist1-b2.campusX	GigabitEthernet0/0
	GigabitEthernet0/3	srv1.campusX	ens3
bdr1.campusX	GigabitEthernet0/0	transit1-nren	GigabitEthernet0/X
	GigabitEthernet0/2	transit2-nren	GigabitEthernet0/X

Replace **Y** with your building number and **X** with your campus/group number.

Your group should share out the seven routers amongst the team members and configure each one using the example shown below.

Hostname

Your routers should be given a basic configuration as follows:

Router> enable
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname bdr1.campusX
bdr1.campusX(config)#

Turn Off Domain Name Lookups

Cisco devices will always try to look up the DNS for any name or address specified in the command line. You can see this when doing a trace on a router with no DNS server or a DNS server with no in-addr.arpa

entries for the IP addresses. We will turn this lookup off for the labs for the time being to speed up traceroutes.

bdr1.campusX(config)# no ip domain lookup

Set the Domain Name

We will now set the domain name of our campus devices, for future use in this workshop.

bdr1.campusX(config)# ip domain name ws.nsrc.org

Configure console and other ports

By default, Cisco devices will try all transports available if they don't recognise what is typed into the command line. This behaviour is annoying especially if making a typo during configuration work, so we will disable the behaviour completely. We will also set the idle-timeout on the console and other ports to 30 minutes - after 30 minutes of no activity on the port, the device will disconnect the connection.

bdr1.campusX(config)# line con 0
bdr1.campusX(config-line)# transport preferred none
bdr1.campusX(config-line)# exec-timeout 30 0
bdr1.campusX(config-line)# line aux 0
bdr1.campusX(config-line)# transport preferred none
bdr1.campusX(config-line)# exec-timeout 30 0
bdr1.campusX(config-line)# line vty 0 4
bdr1.campusX(config-line)# transport preferred none
bdr1.campusX(config-line)# exec-timeout 30 0

Usernames and Passwords

All router usernames should be **cndlab** with password being **lab-PW**. The enable password (which takes the operator into configuration mode) needs to be **lab-EN**[1].

Please do not change the username or password to anything else, or leave the password unconfigured (access to vty ports is not possible if no password is set). It is essential for a smooth operating lab that all participants have access to all routers.

bdr1.campusX(config)# username cndlab secret lab-PW
bdr1.campusX(config)# enable secret lab-EN
bdr1.campusX(config)# service password-encryption

The service password-encryption directive tells the router to encrypt all passwords stored in the router's configuration (apart from enable secret[2] which is already encrypted).

Enabling login access for other devices

In order to let you telnet into your device in future modules of this workshop, you need to configure a password for all virtual terminal lines.

bdr1.campusX(config)# aaa new-model
bdr1.campusX(config)# aaa authentication login default local
bdr1.campusX(config)# aaa authentication enable default enable

This series of commands tells the router to look locally for standard user login (the username password pair set earlier), and to the locally configured enable secret for the enable login. By default, login will be enabled on all vtys for other teams to gain access.

Configure system logging

A vital part of any Internet operational system is to record logs. The router by default will display system logs on the router console. However, this is undesirable for Internet operational routers, as the console is a 9600 baud connection, and can place a high processor interrupt load at the time of busy traffic on the network. However, the router logs can also be recorded into a buffer on the router – this takes no interrupt load and it also enables to operator to check the history of what events happened on the router.

bdr1.campusX(config)# no logging console
bdr1.campusX(config)# logging buffer 8192 debug

which disables console logs and instead records all logs in a 8192 byte buffer set aside on the router. To see the contents of this internal logging buffer at any time, the command show log should be used at the command prompt.

And we also want to set up improved time-stamping for the log messages as well:

service timestamps debug datetime msec localtime show-timezone year
service timestamps log datetime msec localtime show-timezone year

which will give resolution down to milliseconds, and include the year as well.

Save the Configuration.

With the basic configuration in place, save the configuration. To do this, exit from enable mode by typing end or <ctrl>Z, and at the command prompt enter write memory. If you are prompted [confirm] hit enter again.

bdr1.campusX(config)# end
bdr1.campusX# write memory
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 3788 bytes to 1832 bytes[OK]

[OK]
bdr1.campusX#

It is highly recommended that the configuration is saved quite frequently to NVRAM. If the configuration is not saved to NVRAM, any changes made to the running configuration will be lost after a power cycle or virtual machine failure

Log off the router:

bdr1.campusX# exit

and then log back in again. Notice how the login sequence has changed, prompting for a username and password from the user, like this:

bdr1.campusX con0 is now available

Press RETURN to get started.

User Access Verification

Username:

Note that at each checkpoint in the workshop, you should save the configuration to memory – remember that powering the device off will result in it reverting to the last saved configuration in NVRAM.

IP Addressing

For the lab exercises, each group has been allocated the following address space for their campus:

Campus	Public IPv4	Private IPv4	IPv6 Campus	AS Number
1	100.68.1.0/24	172.21.0.0/16	2001:DB8:1::/48	10
2	100.68.2.0/24	172.22.0.0/16	2001:DB8:2::/48	20
3	100.68.3.0/24	172.23.0.0/16	2001:DB8:3::/48	30
4	100.68.4.0/24	172.24.0.0/16	2001:DB8:4::/48	40
5	100.68.5.0/24	172.25.0.0/16	2001:DB8:5::/48	50
6	100.68.6.0/24	172.26.0.0/16	2001:DB8:6::/48	60

The following IPv4 address ranges have been assigned by the NREN for the links to the Border routers:

Campus	NREN Link Subnet	NREN Router Address	Campus Border Router Address
1	100.68.0.0/30	100.68.0.1	100.68.0.2
2	100.68.0.4/30	100.68.0.5	100.68.0.6
3	100.68.0.8/30	100.68.0.9	100.68.0.10

4	100.68.0.12/30	100.68.0.13	100.68.0.14
5	100.68.0.16/30	100.68.0.17	100.68.0.18
6	100.68.0.20/30	100.68.0.21	100.68.0.22

The following IPv6 address ranges have been assigned by the NREN for the links to the Border routers:

Campus	NREN Link Subnet	NREN Router Address	Campus Border Router Address
1	2001:DB8:100:1::/127	2001:DB8:100:1::0	2001:DB8:100:1::1
2	2001:DB8:100:2::/127	2001:DB8:100:2::0	2001:DB8:100:2::1
3	2001:DB8:100:3::/127	2001:DB8:100:3::0	2001:DB8:100:3::1
4	2001:DB8:100:4::/127	2001:DB8:100:4::0	2001:DB8:100:4::1
5	2001:DB8:100:5::/127	2001:DB8:100:5::0	2001:DB8:100:5::1
6	2001:DB8:100:6::/127	2001:DB8:100:6::0	2001:DB8:100:6::1

For completeness, the following addresses are used within the NREN itself. Note that the NREN's IPv4 backbone addressing is shared with the classroom backbone.

	IPv4	IPv6
TR1 Loopback	100.68.0.251	2001:DB8:100:FF::251
TR2 Loopback	100.68.0.252	2001:DB8:100:FF::252
TR1 Ethernet Backbone	192.168.122.2/24	2001:DB8::2/64
TR2 Ethernet Backbone	192.168.122.3/24	2001:DB8::3/64

The NREN is running inside AS 65534.

You will be given details the addresses to use for the routers and switches as we work through the exercises but they will be allocated from these blocks:

Network	IPv4	IPv6
Router core	100.68.X.0/28	2001:DB8:X:0::/64
NAT Pool	100.68.X.32/28	N/A
Servers	100.68.X.128/28	2001:DB8:X:1::/64
Loopbacks	100.68.X.240/28	2001:DB8:X:2::/64
Building 1 Management	172.2X.10.0/24	2001:DB8:X:10::/64
Building 1 Staff	172.2X.11.0/24	2001:DB8:X:11::/64
Building 1 Student	172.2X.12.0/24	2001:DB8:X:12::/64
Building 2 Management	172.2X.20.0/24	2001:DB8:X:20::/64
Building 2 Staff	172.2X.21.0/24	2001:DB8:X:21::/64
Building 2 Student	172.2X.22.0/24	2001:DB8:X:22::/64