# Static Routing Lab

## Accessing the routers

The overall architecture and the full address plan can be found in the IP Address Plan

See the Layer 2 Network Design Lab for details of how to login. The routers have the same username and passwords as the switches.

The console details are:

| Router Name | Console |
|---|---|
| r1-bdr-campus1 | telnet s1.ws.nsrc.org 2101 |
| r1-bdr-campus2 | telnet s1.ws.nsrc.org 2201 |
| r1-bdr-campus3 | telnet s1.ws.nsrc.org 2301 |
| r1-bdr-campus4 | telnet s1.ws.nsrc.org 2401 |
| r1-bdr-campus5 | telnet s1.ws.nsrc.org 2501 |
| r1-bdr-campus6 | telnet s1.ws.nsrc.org 2601 |
| r1-core-campus1 | telnet s1.ws.nsrc.org 2102 |
| r1-core-campus2 | telnet s1.ws.nsrc.org 2202 |
| r1-core-campus3 | telnet s1.ws.nsrc.org 2302 |
| r1-core-campus4 | telnet s1.ws.nsrc.org 2402 |
| r1-core-campus5 | telnet s1.ws.nsrc.org 2502 |
| r1-core-campus6 | telnet s1.ws.nsrc.org 2602 |

## Basic Router Configuration
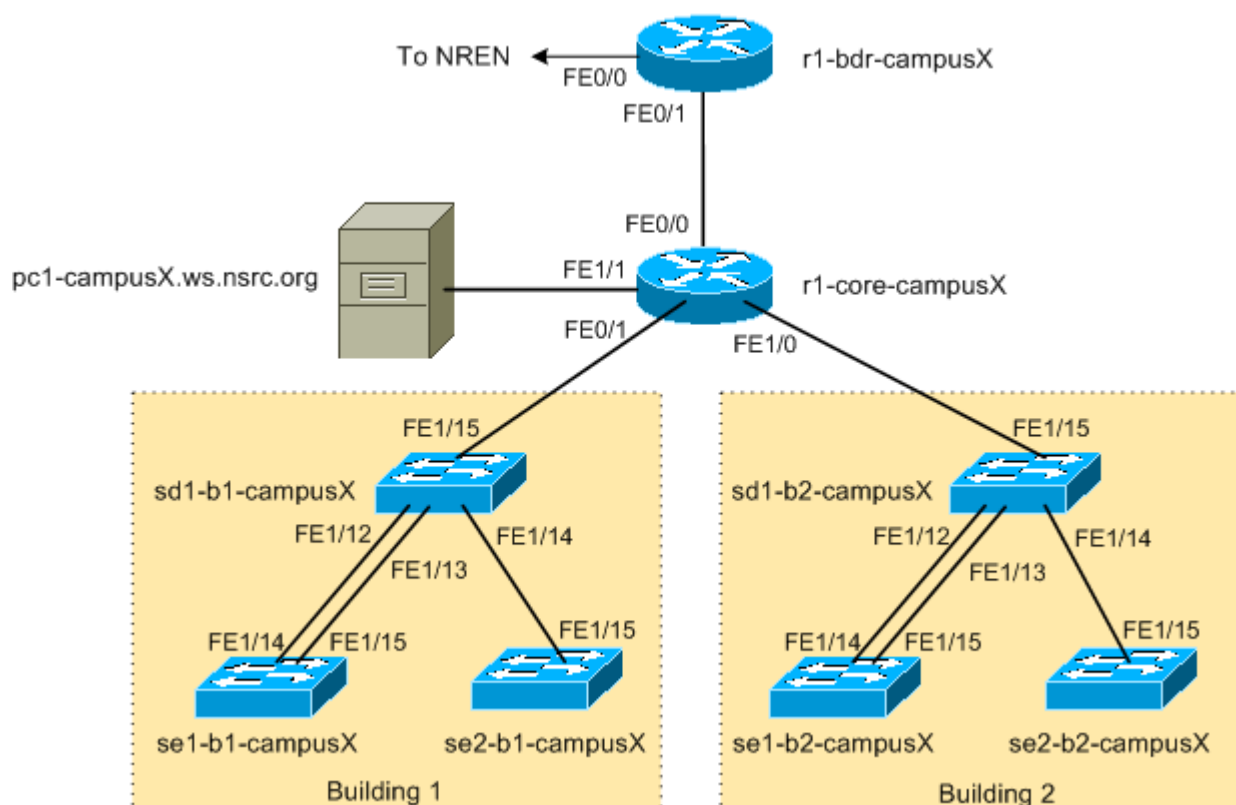
Our campus network consists of two routers, r1-bdr-campusX and r1-core-campusX as well as six switches that we've already configured.

The following table shows the connections between each device in the campus:

| Device | Interface | Remote Device | Remote Interface |
|---|---|---|---|
| sd1-bN-campusX | FastEthernet1/12 | se1-bN-campusX | FastEthernet1/14 |
| | FastEthernet1/13 | se1-bN-campusX | FastEthernet1/15 |
| | FastEthernet1/14 | se2-bN-campusX | FastEthernet1/15 |
| r1-core-campusX | FastEthernet0/0 | r1-bdr-campusX | FastEthernet0/1 |
| | FastEthernet0/1 | sd1-b1-campusX | FastEthernet1/15 |
| | FastEthernet1/0 | sd1-b2-campusX | FastEthernet1/15 |
| | FastEthernet1/1 | pc1-campusX | |

Replace **N** with your building number and **X** with your campus number.

**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 r1-bdr-campusX
r1-bdr-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.

```
r1-bdr-campusX (config)# no ip domain-lookup
```

## Configure console and other ports

```
r1-bdr-campusX (config)# line con 0
r1-bdr-campusX (config-line)# transport preferred none
r1-bdr-campusX (config-line)# line vty 0 4
r1-bdr-campusX (config-line)# transport preferred none
```

## 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**.

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.

```
r1-bdr-campusX (config)# username cndlab secret lab-PW
r1-bdr-campusX (config)# enable secret lab-EN
r1-bdr-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 which is already encrypted).

**Note A:** There is the temptation to simply have a username of cisco and password of cisco as a lazy solution to the username/password problem. Under no circumstances must any service provider operator ever use easily guessable passwords as these on their live operational network.

**IMPORTANT: This sentence cannot be emphasized enough. It is quite common for attackers to gain access to networks simply because operators have used familiar or easily guessed passwords.**

**Note B:** for IOS releases prior to 12.3, the username/secret pair is not available, and operators will have to configure username/password instead. The latter format uses type-7 encryption, whereas the former is the more secure md5 based encryption.

## Enabling login access for other machines

In order to let you telnet into your router in future modules of this workshop, you need to configure a

password for all virtual terminal lines.

```
r1-bdr-campusX (config)# aaa new-model
r1-bdr-campusX (config)# aaa authentication login default local
r1-bdr-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. In a future module, the lab will configuration the router to send the log messages to a SYSLOG server.

```
r1-bdr-campusX (config)# no logging console
r1-bdr-campusX (config)# logging buffered 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.

**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".

```
r1-bdr-campusX(config)#^Z
r1-bdr-campusX# write memory
Building configuration...
[OK]
r1-bdr-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 by typing exit, and then log back in again. Notice how the login sequence has changed, prompting for a "username" and "password" from the user. Note that at each checkpoint in the workshop, you should save the configuration to memory – remember that powering the router off will result in it reverting to the last saved configuration in NVRAM.

# Configure the Core Router

## Configure the interface to the Border router

Make sure you change the X below to the correct value for your campus:

```
interface FastEthernet0/0
 description CAMPUS CORE to BORDER
 ip address 100.68.X.2 255.255.255.240
 ipv6 address 2001:db8:X:0::2/64
 no ip redirects
 no ip proxy-arp
 no shutdown
```

## Configure the Management VLAN interfaces

In the VLAN lab we moved the Management address of the switches into a dedicated vlan for each building. We used vlan 41 in Building 1 and vlan 42 in Building 2. Now we'll configure our core router so that it can talk to these vlans (and the switches).

On r1-core-campusX add the following for Building 1:

```
interface FastEthernet0/1
 no ip address
 no shutdown
!
interface FastEthernet0/1.41
 description Building 1 Management - vlan 41
 encapsulation dot1Q 41
 ip address 172.2X.0.1 255.255.255.240
 ipv6 address 2001:db8:X:3::1/64
 no ip redirects
 no ip proxy-arp
 no shutdown
```

And for Building 2:

```
interface FastEthernet1/0
 no ip address
 no shutdown
!
interface FastEthernet1/0.42
 description Building 2 Management - vlan 42
 encapsulation dot1Q 42
 ip address 172.2X.0.17 255.255.255.240
 ipv6 address 2001:db8:X:4::1/64
```

```
 no ip redirects
 no ip proxy-arp
 no shutdown
```

Exit configuration mode and save your changes!

Test that you can ping all six switches from the core router. You should also test that you can ping the Building 1 switches from the Building 2 switches.

# Configure the STAFF and STUDENT interfaces

We've configured STAFF and STUDENT ports on our edge switches and any device plugged into those ports should be able to talk to others in the same vlan. If we want to allow those devices to get to the wider campus network and the Internet we need to add interfaces on the core router.

For Building 1 we need to add:

```
interface FastEthernet0/1.51
 description Building 1 STAFF - vlan 51
 encapsulation dot1Q 51
 ip address 172.2X.51.1 255.255.255.0
 ipv6 address 2001:db8:X:51::1/64
 no ip redirects
 no ip proxy-arp
 no shutdown
!
interface FastEthernet0/1.61
 description Building 1 STUDENT - vlan 61
 encapsulation dot1Q 61
 ip address 172.2X.61.1 255.255.255.0
 ipv6 address 2001:db8:X:61::1/64
 no ip redirects
 no ip proxy-arp
 no shutdown
```

For Building 2 we need to add:

```
interface FastEthernet1/0.52
 description Building 2 STAFF - vlan 52
 encapsulation dot1Q 52
 ip address 172.2X.52.1 255.255.255.0
 ipv6 address 2001:db8:X:52::1/64
 no ip redirects
 no ip proxy-arp
 no shutdown
!
interface FastEthernet1/0.62
 description Building 2 STUDENT - vlan 62
```

```
 encapsulation dot1Q 62
 ip address 172.2X.62.1 255.255.255.0
 ipv6 address 2001:db8:X:62::1/64
 no ip redirects
 no ip proxy-arp
 no shutdown
```

If we had a real physical network, we'd be able to connect a device to the switch ports we set up earlier, configure an IP address and ping the router at this stage.

# Configure the Network Management and Monitoring interface

Our network management and monitoring server, pc1-campusX.ws.nsrc.org, is connected to FastEthernet1/1 on the core router. We'll configure the router, r1-core-campusX, so that we can start to use that server to manage and monitor our network:

```
interface FastEthernet1/1
 description Network Management and Monitoring
 ip address 100.68.X.129 255.255.255.240
 ipv6 address 2001:db8:X:1::1/64
 no ip redirects
 no ip proxy-arp
```

At this stage you should be able to **ssh** to pc1-campusX.ws.nsrc.org as sysadm and ping the core router on this address.

If that works, try using telnet to connect to the router.

# Set up SNMP access on the Core router

Later in the week we're going to start using SNMP to manage the routers and switches. We'll add the necessary commands at this stage:

```
access-list 99 permit 100.68.X.130
!
snmp-server community NetManage RO 99
snmp ifmib ifindex persist
```

The access-list only allows SNMP queries from the NMM server.

If your router doesn't take the above snmp commands, try the following instead. Even though Cisco IOS is one operating system, the implementation details on different platforms can well be different:

```
access-list 99 permit 100.68.X.130
!
snmp-server community NetManage RO 99
```

```
snmp-server ifindex persist
```

# Configure the Border Router

## Configure the NREN interface

The full address plan for the lab can be found in the IP Address Plan. Consult the address plan for the addresses of the point to point links between the Campus Border Router and the NREN Router.

Make sure you change the **X** and **Y** below to the correct value from address plan mentioned above:

```
interface FastEthernet0/0
 description NREN
 ip address 100.68.0.Y 255.255.255.252
 ipv6 address 2001:db8:0:X::1/127
 no ip redirects
 no ip proxy-arp
 no shutdown
```

Test that you can ping the NREN end of the link. Test both IPv4 and IPv6 connectivity.

## Configure the Core interface

Make sure you change the **X** below to the correct value for your campus:

```
interface FastEthernet0/1
 description CAMPUS CORE
 ip address 100.68.X.1 255.255.255.240
 ipv6 address 2001:db8:X:0::1/64
 no ip redirects
 no ip proxy-arp
 no shutdown
```

Test that you can ping your Core router at the other end this link.

## Set up SNMP access on the Border router

Later in the week we're going to start using SNMP to manage the routers and switches. We'll add the necessary commands at this stage:

```
access-list 99 permit 100.68.X.130
!
```

```
snmp-server community NetManage RO 99
snmp ifmib ifindex persist
```

The access-list only allows SNMP queries from the NMM server.

If your router doesn't take the above snmp commands, try the following instead. Even though Cisco IOS is one operating system, the implementation details on different platforms can well be different:

```
access-list 99 permit 100.68.X.130
!
snmp-server community NetManage RO 99
snmp-server ifindex persist
```

# Configure Static Routing

At this stage you should be able to ping each of the devices in your campus network from their immediate neighbours. If you try to ping the Border router from one of the switches or the NMM server you'll have less success. We need to add some additional routing information to the routers so that we can pass packets successfully.

Let's look at the routing information on the Core router:

```
r1-core-campus1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
Gateway of last resort is not set

      100.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C        100.68.1.0/28 is directly connected, FastEthernet0/0
L        100.68.1.2/32 is directly connected, FastEthernet0/0
C        100.68.1.128/28 is directly connected, FastEthernet1/1
L        100.68.1.129/32 is directly connected, FastEthernet1/1
C        100.68.1.242/32 is directly connected, Loopback0
      172.21.0.0/16 is variably subnetted, 4 subnets, 2 masks
C        172.21.0.0/28 is directly connected, FastEthernet0/1.41
L        172.21.0.1/32 is directly connected, FastEthernet0/1.41
C        172.21.0.16/28 is directly connected, FastEthernet1/0.42
L        172.21.0.17/32 is directly connected, FastEthernet1/0.42
```

and on the Border router:

```
r1-bdr-campus1>sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      100.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
C        100.68.0.0/30 is directly connected, FastEthernet0/0
L        100.68.0.2/32 is directly connected, FastEthernet0/0
C        100.68.1.0/28 is directly connected, FastEthernet0/1
L        100.68.1.1/32 is directly connected, FastEthernet0/1
```

Each of the routers knows about the **local** and **connected** networks but no other routes.

What about IPv6? What routes do you see for IPv6 destinations? Is there a similarity with what you see for IPv4?

# Turn on IPv6 Routing

Cisco IOS routers have IPv6 Routing turned off by default. So while we can reach our directly attached neighbours, we cannot get anywhere beyond, nor can we turn on any IPv6 routing protocols. We now need to turn on IPv6 routing, and to do that we use the following command:

```
ipv6 unicast-routing
```

# Static routes on the Core router

The Core router needs a default route added to it so that we can forward IPv4 and IPv6 traffic from the Campus network to the wider Internet via the NREN. We add this route to send traffic to the border router:

```
ip route 0.0.0.0 0.0.0.0 100.68.X.1
ipv6 route ::/0 2001:db8:X:0::1
```

# Static routes on the Border router

The Border needs a default route added to it so that we can forward traffic from the Campus network

to the wider Internet via the NREN. We add this route to send traffic to the NREN router:

```
ip route 0.0.0.0 0.0.0.0 100.68.0.Y
ipv6 route ::/0 2001:db8:0:X::0
```

Choose the correct value for **X** and **Y** from the table we used when we set up the interface.

**IMPORTANT: You have added a number of subnets on your core router and building switches for the NMM subnet and VLAN 41, 42, 51, 52, 61, 62. Your Border router needs to be able to send packets to those subnets.**

Which networks should you add routes for?

**HINT**: You need routes for all the IPv4 and IPv6 networks assigned to your Campus. See the IP Address Plan for details.

**Add these routes.**

# Testing the routing setup

The two NREN routers are connected to the same workshop subnet as your laptops, 10.10.0.0/24. They have the IPv4 addresses, 10.10.0.201 and 10.10.0.202.

You should be able to ping these addresses from your Core router if your setup is correct. You should also be able to ping your Core router from your laptop.

Now try pinging 8.8.8.8 - does this work?

***Checkpoint***: *call the lab assistant to verify the connectivity.*

From:
https://workshops.nsrc.org/dokuwiki/ - **Workshops**

Permanent link:
**https://workshops.nsrc.org/dokuwiki/doku.php?id=2016:nsrc-tein-mmren:static-routing**

Last update: **2016/06/08 10:28**