Lab Guide 1 - Basic Configuration and Interface Configuration

Objective: All the workshop lab routers are set to the default configuration and cabling requirements are prebuild according to the following topology diagram. Participants will be required to do the necessary configurations as part of a team according to the lab design specification explained in the presentation section. Workshop instructor will explain how the team will be organized, router will be allocated and IP address detail to access the lab routers.

Prerequisites: Cisco router CLI, Telnet/SSH software etc.

The following will be the common topology and IP address plan used for the labs.

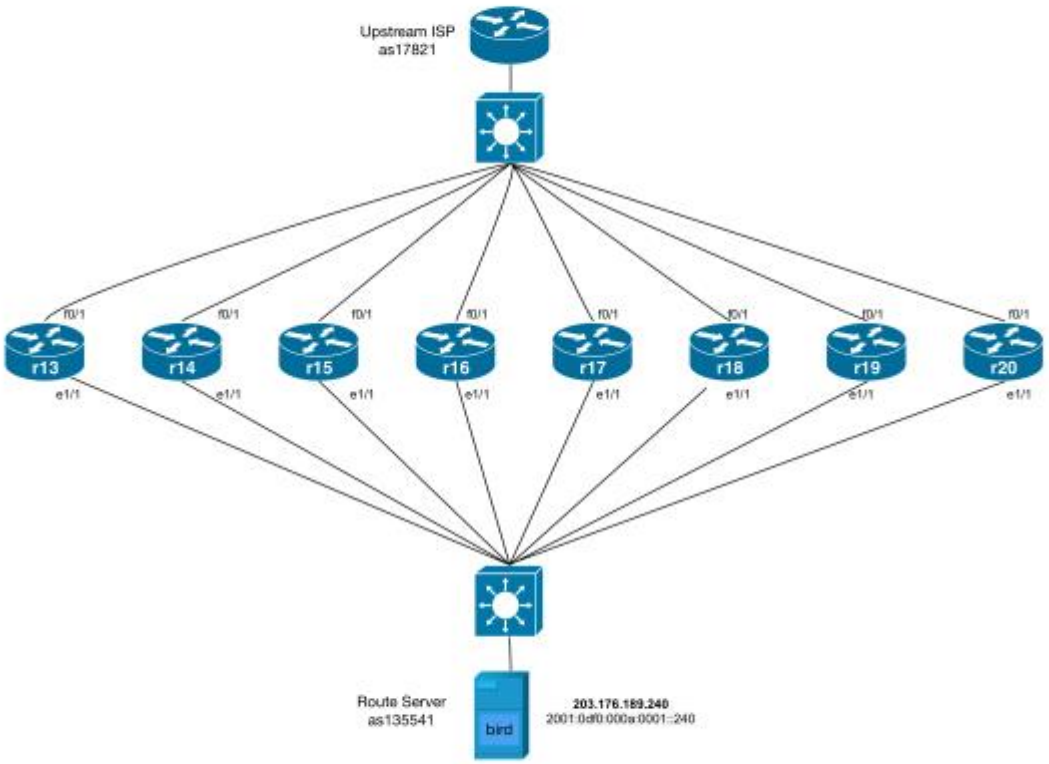


Figure 1 – IXP Lab Topology

Lab Notes

This workshop is intended to be run on real cisco routers or Dynamips server with the above lab topologies set up. The routers are using both IPv4 and IPv6 supported IOS software. There will be one route server (running on BIRD) will be configured by the instructors.

Address Plannings

	Io0	f0/1 Connected with upstream	e1/1 Connected with IX	Prefixes
r13 AS135533	172.16.16.254/32 2406:6400:8000:0000::1/128	172.16.11.2/30 2406:6400:0010:0000::2/64	203.176.189.13/24 2001:0df0:000a:0001::13/64	172.16.16.0/23 2406:6400:8000::/48
r14 AS135534	172.16.18.254/32 2406:6400:9800:0000::1/128	172.16.11.34/30 2406:6400:0014:0000::2/64	203.176.189.14/24 2001:0df0:000a:0001::14/64	172.16.18.0/23 2406:6400:9800::/48
r15 AS135535	172.16.20.254/32 2406:6400:A000:0000::1/128	172.16.11.66/30 2406:6400:0018:0000::2/64	203.176.189.15/24 2001:0df0:000a:0001::15/64	172.16.20.0/23 2406:6400:a000::/48
r16 AS135536	172.16.22.254/32 2406:6400:B800:0000::1/128	172.16.11.98/30 2406:6400:001C:0000::2/64	203.176.189.16/24 2001:0df0:000a:0001::16/64	172.16.22.0/23 2406:6400:b800::/48
r17 AS135537	172.16.24.254/32 2406:6400:C000:0000::1/128	172.16.11.130/30 2406:6400:0020:0000::2/64	203.176.189.17/24 2001:0df0:000a:0001::17/64	172.16.24.0/23 2406:6400:c000::/48
r18 AS135538	172.16.26.254/32 2406:6400:D800:0000::1/128	172.16.11.162/30 2406:6400:0024:0000::2/64	203.176.189.18/24 2001:0df0:000a:0001::18/64	172.16.26.0/23 2406:6400:d800::/48
r19 AS135539	172.16.28.254/32 2406:6400:E000:0000::1/128	172.16.11.194/30 2406:6400:0028:0000::2/64	203.176.189.19/24 2001:0df0:000a:0001::19/64	172.16.28.0/23 2406:6400:e000::/48
r20 AS135540	172.16.30.254/32 2406:6400:F800:0000::1/128	172.16.11.226/30 2406:6400:002C:0000::2/64	203.176.189.20/24 2001:0df0:000a:0001::20/64	172.16.30.0/23 2406:6400:f800::/48

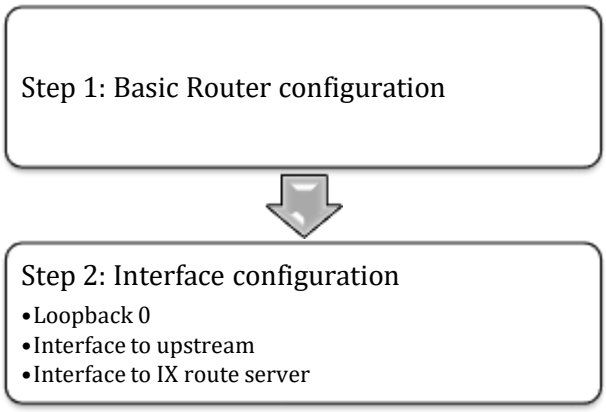
This workshop is intended to be run on real cisco routers or Dynamips server with the above lab topologies set up. The routers are using both IPv4 and IPv6 supported IOS software. Participants should do their workshop module one configuration in several steps as explained below:

1. Standard basic router configuration.
2. Standard interface related configuration for IPv4.
3. Do necessary verification to make sure you can ping your neighbouring router point-to-point interface and satisfy the requirement to go to the next step.

Please notice that some Cisco commands are case sensitive, already enable by default in some recent IOS version and some are not a mandatory command for router functionality. But for lab troubleshooting and verification purpose it is strongly recommended that please do all necessary configuration exactly as it is explained in the instruction. Our objective after the exercise is to build a template for each participant so that it can be re-used after you go back to your work environment.

Lab Exercise

Every team will be assigned one router, tasks for each team:



1. **Basic Router Configuration:** This will set the router with necessary basic configuration used in a real production router for both enterprise and service provider network. In this basic configuration, we add IPv6 too.

   Example Config on a Router:

```
enable
config t
```

   To enter into a cisco router global configuration mode.

```
hostname Router13
```

   Router host name which is an FQDN name mapped into a DNS server. There is a common practice about router hostname which is domain name then 3 digit airline city code then region/pop then a name etc. Example: router1.pop1reg1.BNE.apnic.net. Please use your router name according the topology diagram.

```
ip routing
```

   It recent IOS this command is enable by default. So it can act as a router and start routing IP packet. To be safe add this command in your template. Need to look for equivalent IPv6 command if any command read IP/L3 header

```
ipv6 unicast-routing
```

   Even in recent IOS [15.1(4)M3] this command is not enable by default. We must use this command so that router starts routing IPv6 packet. To be safe add this command in your template.

```
ip cef
```

   Enable Cisco (Proprietary) Express Forwarding to process IPv4 packet faster.

```
ipv6 cef
```

   Enable Cisco (Proprietary) Express Forwarding to process IPv6 packet faster. Some high end cisco router process packet using line card. Use `ipv6 cef distributed` instead on those routers.

```
no ip domain-lookup
```

To disable DNS resolver functionality on router if you do not use it. If yes then specify DNS server IP. There is no equivalent command for IPv6 yet [15.1(4)M3].

```
no ip http server
```

To disable HTTP server functionality on a router. Otherwise router is accessible from a browser and it consumes CPU and memory resources. We normally access router from a CLI. There is no equivalent command for IPv6 yet [15.1(4)M3].

```
no ip http secure-server
```

To disable HTTPS server functionality on a router. Otherwise router is accessible from a browser and it consumes router CPU and memory resources. We normally access router from CLI. There is no equivalent command for IPv6 yet [15.1(4)M3].

```
no ip finger
```

Finger service can be used to find out which users are logged into a router. Also a special DoS attack named “Finger of death” uses the finger service to continuously transmit finger requests to a given device consuming great amounts of processing resources. Depending of your IOS version it could be disable by default. To be safe add it in your command template. There is no equivalent command for IPv6 yet [15.1(4)M3].

```
no service pad
```

To disable Packet Assembler/Disassembler (PAD) service, which is used for X.25 networks in early days. If you do not use it now please disable it.

```
no service udp-small-servers
no service tcp-small-server
```

Depending on your cisco IOS version it offer by default small tcp/udp services that are basically a set of simple services that are used for diagnostic purposes. An attacker could maliciously use these services to gain system information and even launch Denial of Service (DoS) attacks to your router.

```
no ip bootp server
```

A Cisco router can be configured to act as a BOOTP server and provide IOS software image to another Cisco network devices. This service could be used by an attacker to download a copy of a network device’s IOS software. There is no equivalent command for IPv6 yet [15.1(4)M3].

```
no ip source-route
no ipv6 source-route
```

An IP source routing function allows the sender of an IP packet to control the route that the packet will take towards its final destination. Source routing should be disabled when it’s not needed because it could be used for various malicious attacks and also very CPU intensive function.

```
logging source-interface loopback 0
```

We need the router use the loopback address as the "source interface" for traffic that is generated by the router, such as syslog packets, SNMP traps, security related packets. Also DNS is mapped with the loopback address and FQDN name of the router.

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

Router will show either uptime or current date and time on the log it will generate based on the configuration on your router. We would like to record current date and time in msec unit for both log and debug messages to facilitate the log analysis if required.

```
clock timezone AEST 10
```

Set your router clock according to your local time zone. We used AEST 10 to reflect APNIC office where it is located and corresponding time zone.

```
ip subnet-zero
```

Under old IP subnetting rules, the all 0's subnet was reserved for the network, and the all 1's subnet was reserved for the broadcast. Over time this idea has been changed and we can use all 0's and all 1's subnet. Depending on your IOS version you might need to enable this on your cisco router. To be safe add this command in your template. IP subnet-zero concept is not applicable for IPv6 address family

```
ip classless
```

In old days routers are by default classful. Now we are in CIDR era. Depending on your cisco IOS version this command can be there by default. To be safe add this command in your template. IP classless concept is not applicable for IPv6 address family.

```
Line console 0
transport preferred none
exit
```

By default telnet is the preferred protocol and when we mistyping a command the router will try to telnet the "name" we typed. If we set the transport preferred to none the router won't try to telnet when mistyping and we still can have DNS resolver enabled.

```
line console 0
logging synchronous
exit
```

Before the command:

```
SW1(config)#int vlan 1
SW1(config-if)#^Z
SW1#sh
*Mar  4 21:50:27.949: %SYS-5-CONFIG_I: Configured from console by consolerunn
```

After the command:

```
SW1(config-line)#logging synchronous
SW1(config-line)#exit
SW1(config)#int vlan
SW1(config)#int vlan 1
SW1(config-if)#^Z
SW1#sh
*Mar  4 21:53:24.890: %SYS-5-CONFIG_I: Configured from console by console
SW1#sh
```

```
ip tcp synwait-time 15
```

An attacker could flood a router with a high volume of TCP connection requests for which it does not return back an acknowledgement causing connection queues to fill up at the receiving host. Setting the TCP Synwait time to 15 seconds for example, will instruct the router to shut down any incomplete connections after 15 seconds. There is no equivalent command for IPv6 yet [15.1(4)M3].

```
security authentication failure rate 3 log
```

Configuring a router to lock access (for about 15 seconds) after three unsuccessful login attempts. This method protects a router from malicious attack (brute-force attack) and at the same time a log message is generated warning about the unsuccessful login attempts.

```
exit
wr
```

[wr] is an abbreviation or write command. Which will eventually copy (Save) the running configuration (From RAM) in to the startup-configuration (NVRAM) of cisco router.

END OF STEP ONE……

2. **Interface Related Configuration:** This will set the router with necessary interface related configuration (IPv4) used in a real production router for both enterprise and service provider network.

Example IPv4 Config on a Router:

2.1 Configure Loopback Interface

```
config t

interface Loopback0
```

To go to an interface configuration mode of a cisco router

```
description LAN r13
```

It is very important to add a meaningful description of a router interface to explain where this interface is connected. Otherwise we might be lost finding which interface connects where on a large data centre and need to jump behind the rack to look for a clue.

```
no ip redirects
```

This disables ICMP redirect messages. Redirects function happen when a router recognizes a packet arriving on an interface and the best route is out that same interface. In that case the router sends an ICMP redirect back to the source telling them about a better router on the same subnet. Subsequent packets take the redirected path. This function can be abused by an attacker who has got access to your layer 2 network to initiate man in the middle attack.

```
no ip unreachables
```

From a security point of view someone can initiate reconnaissance attack on a device and if you want to minimize the amount of information that the device can provides about itself to others this command is very useful. It also protects the router from the un wanted resource utilization on the device.

```
ip address 172.16.16.254 255.255.255.255
```

Assign IP address on a cisco router interface.

```
exit
```

2.2 Configure the interface connected to upstream router

```
interface FastEthernet0/1

description Upstream WAN r13-UR

ip address 172.16.11.2 255.255.255.252

no ip redirects

no ip unreachables

speed auto

duplex auto

no shut

exit
```

Cisco router interface is disable by default. Use this command to activate the interface to start processing IP packet.

Verify the neighboring interface configuration:

Ping the IPv4 address on the upstream router interface (IPv4 address on your own upstream router are different from other groups):

```
Example on Router13:

Ping 172.16.11.1           [!!!!!]
```

2.3 Configure the interface connected to IX router

```
interface Ethernet1/1

description IX Router
```

```
no ip redirects

no ip unreachables

ip address 203.176.189.13 255.255.255.0

duplex full

no shut

exit
exit
wr
```

Verify the neighboring interface configuration:

Ping the IPv4 address on the IXP router server which is 203.176.189.240 in this lab:

```
Example on Router13:

Ping 203.176.189.240       [!!!!!]
```

END OF STEP TWO……