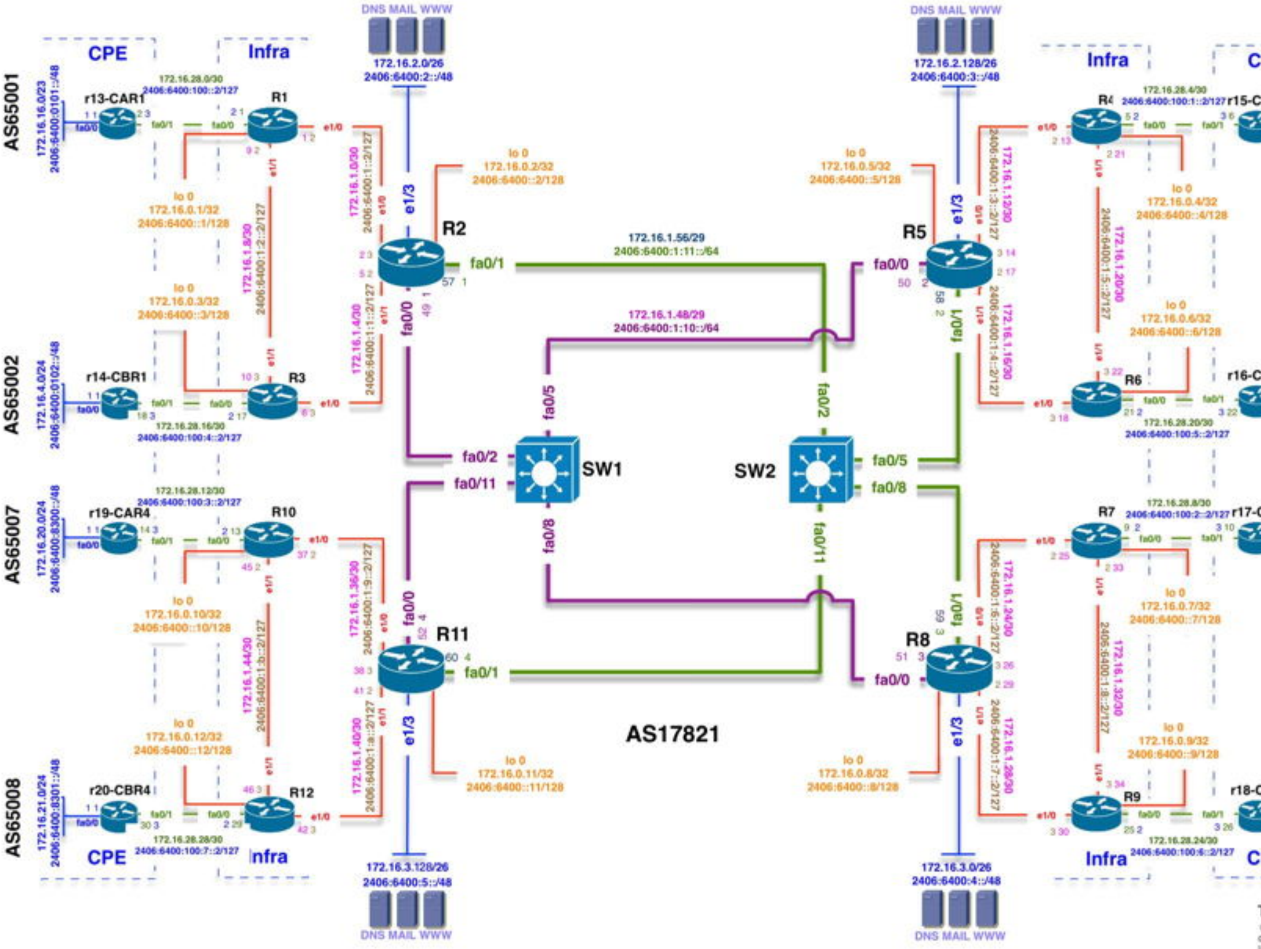
Module 1 - Basic and Interface Configuration

Topology introduction:

- The topology below shows 4 regional networks comprised of a core POP and 2 aggregation POPs (edge routers).
- Edge routers aggregate downstream customers.
- The regional networks are interconnected with redundant transport links.



Training Lab Topology
© APNIC Training
Created: 25/09/2009
Last update: 15/10/2018

Lab Tasks

- Participants should complete the following tasks for this module:
  1. Basic best practice configuration
  2. Interface address (IPv4/v6) configuration
  3. Verify reachability of directly connected interfaces

Lab Exercise

Step 1 - Basic best practice Configuration:

Example Configuration on a R1:

Assuming the router did not have a configuration file stored in NVRAM, you will be at the user EXEC mode prompt on the router. The prompt will be `Router>`. Enter privileged EXEC mode by typing `enable`. `Router> enable Router#` 1. To enter into a Cisco router global configuration mode.

```
    config t
```

1. configure the hostname

   ```
   hostname R1
   ```

2. Enable IPv6 routing

   ```
   ipv6 unicast-routing
   ```

3. Enable hardware switching

   ```
   ip cef
   ipv6 cef
   ```

4. Disable resolver functionality

   ```
   no ip domain-lookup
   ```

5. Disable router management through the web interface

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

6. Disable finger service. 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.

   ```
   no ip finger
   ```

7. Disable tcp/udp ports 13 and below (generally called small-servers) 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 service udp-small-servers
   no service tcp-small-servers
   ```

8. Disable BOOTP server Cisco routers 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.

   ```
   no ip bootp server
   ```

9. Disable source routing. Source routing allows the sender of an IP packet to control the route that the packet will take towards its final destination (could bypass your security nodes).

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

10. To disable the Cisco Discovery Protocol on all interfaces. Cisco Discovery Protocol (CDP) is enabled by default. The CDP messages are not encrypted and it is recommended that it is disabled on any external interfaces, for security reasons.

    ```
    no cdp run
    ```

11. By default, when we mistype a command the router will try to connect to the “name” we typed through every possible transport sessions.

    ```
    line console 0
    transport preferred none
    ```

12. Sync the console messages from bothering you while typing in your commands.

    ```
    line console 0
    logging synchronous
    ```

    OR, if you want to totally disable console messages, use the following

```
no logging console
```

13. Exit the configuration mode by using `exit` and save the configuration by using `wr`. Please remember to save it after we have changed the configuration.

    ```
    exit
    exit
    wr
    ```

Typing `end` will take you back to the privileged EXEC mode, no matter where in IOS hierarchy you are.

Step 2 - Interface Configuration:

This will set the router with necessary interface related configuration (IPv6 and IPv4)

1. Example IPv4 Configuration on a Router:

   To go to an interface configuration mode of a cisco router

   ```
   config t
   interface e1/0
   ```

   Add a meaningful description of a router interface to explain where this interface is connected.

   ```
   description ||WAN R3-R2||
   ```

   To disable ICMP redirect messages.

   ```
   no ip redirects
   ```

   Every subnet in IPv4 has a broadcast address. If any packet arrives on a router with broadcast address as destination the router will amplify L2 frame on that interface. Any network attacker can initiate a traffic amplification attack in your LAN if directed broadcast is not disable on that Interface.

   ```
   no ip directed-broadcast
   ```

   From a security point of view some one can initiate reconnaissance attack on a device.

   ```
   no ip unreachables
   ```

2. Example IPv4/v6 Configuration on R1:

   as following:

```
config t
interface loopback 0
ip address 172.16.0.1 255.255.255.255
ipv6 address 2406:6400:0000:0000::1/128
no shut

interface e1/0
ip address 172.16.1.1 255.255.255.252
ipv6 address 2406:6400:0001:0000::2/127
no shut

interface e1/1
ip address 172.16.1.9 255.255.255.252
ipv6 address 2406:6400:0001:0002::2/127
no shut
```

Please remember to save the configuration.

Step 3 - Verify the neighbouring interface configuration:

1. Ping directly connected neighbours

   R1 as an example:

   ```
   R1#ping 172.16.1.2
   [!!!!!]

   R1#ping 2406:6400:1::3
   [!!!!!]
   ```

2. Issue the `show ip interface brief` or `show ipv6 interface brief` to see the addresses configured on each interface.