Module 6 – Device and Infrastructure Security Lab

Objective: All the routers are pre-configured with basic (No security) interface, OSPF and BGP configuration according to the following topology diagram. Create a basic AAA, Device security BCP, OSPF, BGP password on the lab routers. After finishing the configuration ensure that you can telnet/SSH to all routers with proper password. OSPF, BGP neighbours are all up and running (Both IPv4 and IPv6).

Prerequisites: Knowledge of Huawei router CLI, previous hands on experience.

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

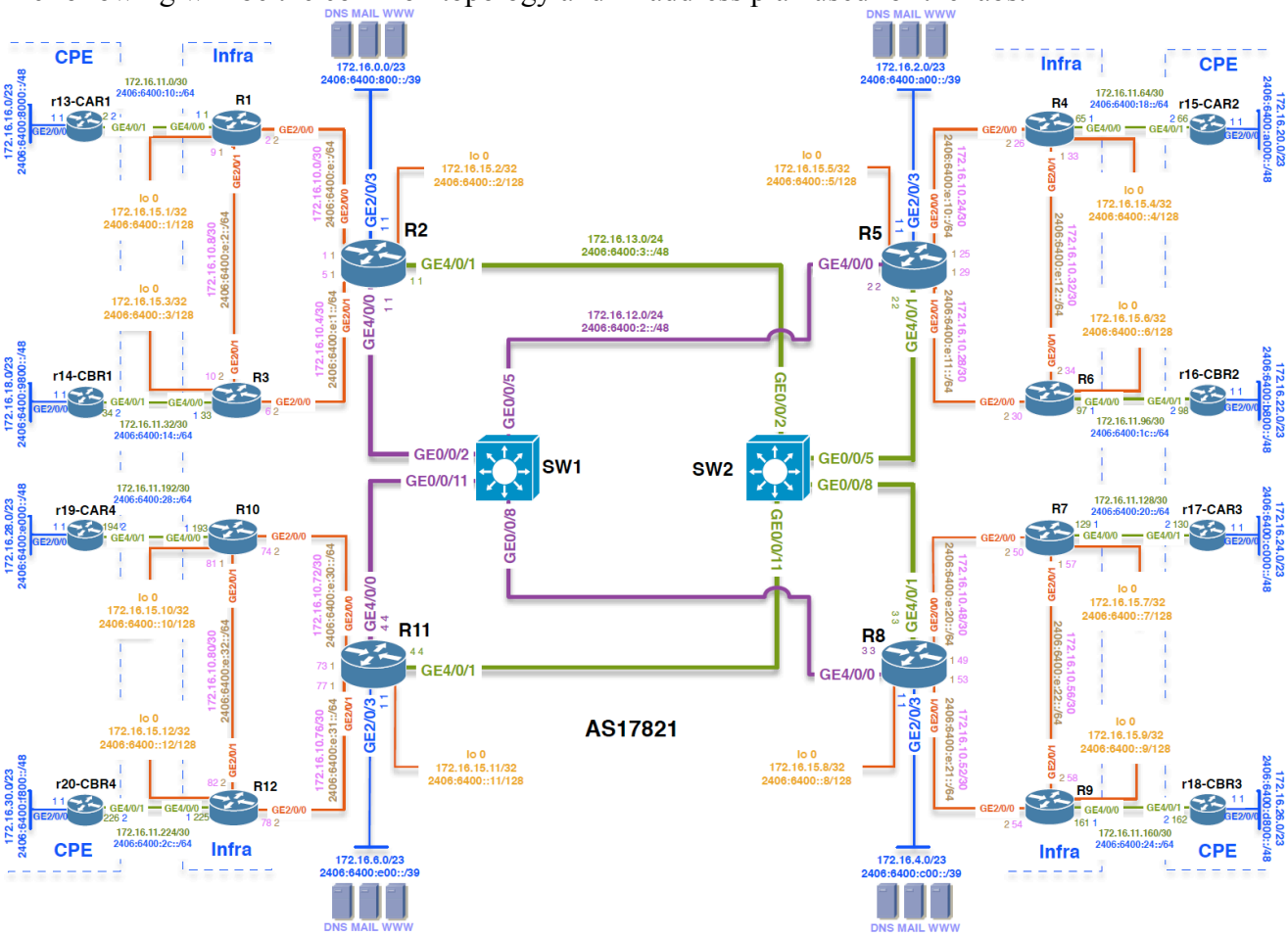

Figure 1 – ISP Lab Basic Configuration

Lab Notes

This workshop is intended to be run on a real Huawei routers or eNSP (Enterprise Network Simulation Platform) with the above lab topologies set up. The routers are using both IPv4 and IPv6 supported Huawei VRP software (VRP software, Version 5.130) and basic routing configurations are pre loaded. Participants are only needed to configure the security related configuration throughout the workshop days. Before you start the security configuration it is advisable to spend some time to be familiar with the lab topology and IP (Both IPv4 & IPv6) addressing plan.

Lab Exercise

1. **Usernames and Passwords.** All router usernames should be ***training*** and all passwords should be ***apnic***. Please do **not** change the username or password to anything else, or leave the password un-configured (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.

```
system-view
aaa
local-user training password cipher apnic
local-user training privilege level 3
local-user training service-type telnet
quit
quit
```

2. **Enabling login access for other teams.** In order to let other teams telnet into your router you need to configure a password for all virtual terminal lines.

```
system-view
user-interface vty 0 4
authentication-mode aaa
quit
quit
save
```

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

a. Try to telnet to other lab router

```
<Router1> telnet 172.16.15.2
```

3. **Enabling SSH remote login to the router.** In order to let other teams to login your router using secure SSH remote access the lab routers need to configure following set of commands.

```
system-view
rsa local-key-pair create
y
512
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
quit
aaa
local-user training password cipher apnic
local-user training privilege level 3
quit
ssh user training authentication-type password
stelnet server enable
```

"`rsa local-key-pair create`" command will generate private and public key pair on the router and the key length will be the default: 512 bytes.

a. Try to ssh to other lab router

```
[Router1]ssh client first-time enable
```

Enable the first authentication function on the SSH client upon the first login.

```
[Router1]stelnet 172.16.15.2
```

4. **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.

```
system-view
undo info-center console channel
info-center logbuffer size 1024
```

which disables console logs and instead records all logs in a buffer set aside on the router. Set the maximum number of logs in the log buffer. To see the contents of this internal logging buffer at any time, the command "`display logbuffer`" should be used at the command prompt.

5. **Controlling Access to a Virtual Terminal Line.** Each router Team should enable access control to their router and allow in/out telnet only from the loopback address aggregated block which is 172.16.15.0/24.

   a. IPv6 prefix list configuration to match prefix permitted

```
system-view
acl name IPV4-VTY-ALLOW 3000
rule 0 permit ip source 172.16.15.0 0.0.0.255 destination any
rule 5 deny ip source any destination any
quit
quit
save
```

   b. Attach the access list to your router VTY line

```
system-view
user-interface vty 0 4
acl 3000 inbound
quit
quit
save
```

c. Try to telnet to other lab router by specifying loopback as source interface

```
telnet –a 172.16.15.3 172.16.15.1
```

The deny statement in IP access-list is only required if we need to see the log of the matching traffic which are denied by this access-list.

Need to specify the source interface loopback 0 so that telnet packet source will be from IP address range 172.16.15.0/24. By default telnet source IP address will be the outgoing interface IP address configured.

6. **Activating OSPF area based authentication.** OSPF authentication can be done under Interface level or Area boundary. In our lab we will enable authentication for the area. Please note that on regional core routers (ABR) we need to enable authentication for both internal area plus the backbone area.

   a. Enable authentication for OSPF neighbour adjacency:

```
system-view
ospf 17821
area 1
authentication-mode md5 1 cipher security
quit
area 0
authentication-mode md5 1 cipher security [Regional core routers only]
```

   b. Verify OSPF adjacency status after the authentication has been setup:

```
[Router2]display ospf peer brief

 OSPF Process 17821 with Router ID 172.16.15.2
        Peer Statistic Information
 ----------------------------------------------------------------------------
 Area Id          Interface                       Neighbor id      State
 0.0.0.0          GigabitEthernet4/0/0            172.16.15.5      Full
 0.0.0.0          GigabitEthernet4/0/0            172.16.15.8      Full
 0.0.0.0          GigabitEthernet4/0/0            172.16.15.11     Full
 0.0.0.0          GigabitEthernet4/0/1            172.16.15.5      Full
 0.0.0.0          GigabitEthernet4/0/1            172.16.15.8      Full
 0.0.0.0          GigabitEthernet4/0/1            172.16.15.11     2-Way
 0.0.0.1          GigabitEthernet2/0/0            172.16.15.1      Full
 0.0.0.1          GigabitEthernet2/0/1            172.16.15.3      Full
 ----------------------------------------------------------------------------
```

   If your OSPF neighbours are not up then you might need to discuss with your neighbouring routers to find out the authentication problem and solve it.

7. **Activating BGP peer authentication for peer group:** BGP authentication can be useful because it will make it difficult for un-authorized or malicious user to disrupt your BGP peering session with the neighbour. BGP protocol can be configured for MD5-based authentication system for authenticating peers relationship. It can be configured under both peer-group or individual peering.

a. Configuration of BGP peer authentication under peer group. Please note in our lab exercise authentication need to be configured for all peer-group used on the router.

```
system-view
bgp 17821
peer IPV4-iBGP-REG1 password cipher security
peer IPV4-eBGP-CUSTOMER-REG1-POP1 password cipher security[POP routers
only]
peer IPV4-iBGP-TRCORE password cipher security[Regional core routers
only]
```

b. Verify BGP adjacency status after the authentication has been setup:

```
[Router1]display bgp peer

 BGP local router ID : 172.16.15.1
 Local AS number : 17821
 Total number of peers : 3          Peers in established state : 3

  Peer            V       AS  MsgRcvd  MsgSent  OutQ  Up/Down     State PrefRcv

  172.16.11.2     4    65001        3       22     0 00:00:06 Established     1
  172.16.15.2     4    17821       25        7     0 00:03:04 Established    18
  172.16.15.3     4    17821        7        7     0 00:03:04 Established     2
```

If the BGP peers are not up then you might need to discuss with your neighbouring routers to find out the authentication problem and solve it.

END OF MODULE SIX……