



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

ENTERPRISE CORE(ACCA7029)

Checkpoint Activity

 **Networking**
CISCO™ **Academy**

Objectives

Task 1: Build the Topology (15 Mins)

Task 2: Complete Basic Configurations (15 Mins)

Task 3: Configure Network (45 Mins)

Task 4: Troubleshoot and Test (15 Mins)

Task 5: Document and Submit (20 Mins)

Task 6: Erase and Initialize (10 Mins)

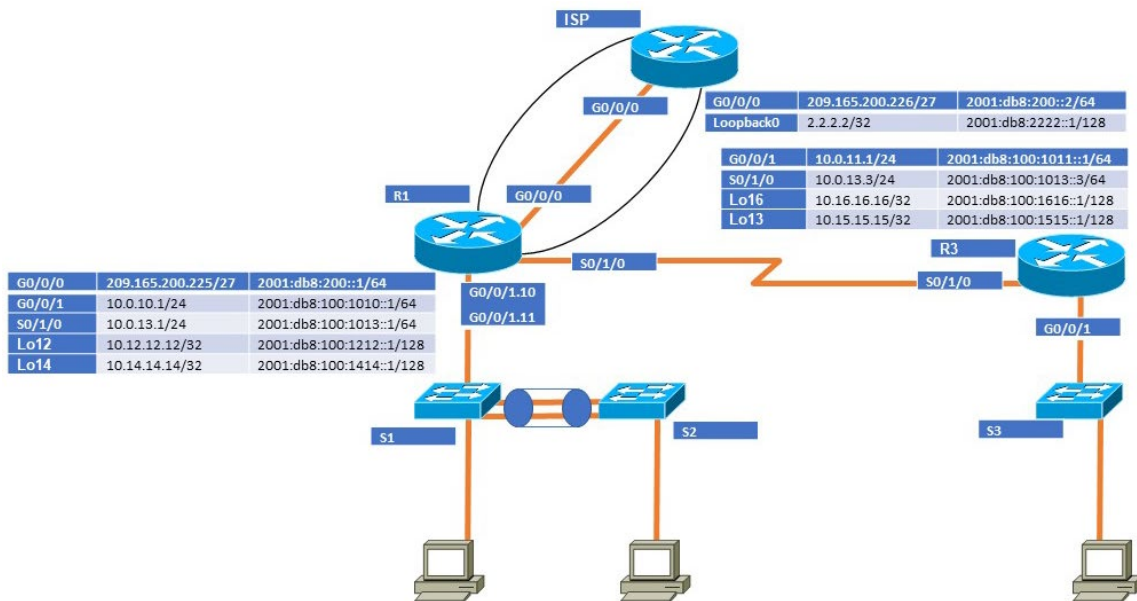
Required Resources

✓ 3 Cisco Routers and Switches

Optional:

✓ Packet Tracer (Latest version)

Topology



1. Configure hostnames on each device.
2. Disable DNS lookup on all routers
3. Enable ipv6 unicast routing
4. Configure all devices with IP address shown in the network topology.
5. On R1, R3 configure single-area OSPFv2 in area 0. Use OSPF Process ID 4.
 - a. Assign the following router-IDs. R1: 0.0.4.1, R3: 0.0.4.3
 - b. On R1, and R3, advertise all directly connected networks in Area 0. On R1, do not advertise the R1 – ISP network.
 - c. On R1, propagate a default route. Note that the default route will be provided by BGP.
6. On R1, R3, configure classic single-area OSPFv3 in area 0. Use OSPF Process ID 6
 - a. Assign the following router-IDs. R1: 0.0.6.1, R3: 0.0.6.3
 - b. On R1, R3, advertise all directly connected networks in Area 0. On R1, do not advertise the R1 – ISP network.
 - c. On R1, propagate a default route. Note that the default route will be provided by BGP.
7. On R1 in the “ISP Network”, configure MP-BGP.
 - a. Configure R1 in BGP ASN 200 and use the router-id 1.1.1.1.
 - b. Configure an IPv4 and IPv6 neighbor relationship with ISP in ASN 500.
 - c. In IPv4 address family:
 - i. Disable the IPv6 neighbor relationship.
 - ii. Enable the IPv4 neighbor relationship.
 - iii. Advertise the 10.0.0.0/8 network.
 - d. In IPv6 address family
 - i. Disable the IPv4 neighbor relationship.
 - ii. Enable the IPv6 neighbor relationship.
 - iii. Advertise the 2001:db8:100::/48 network.
 - e. Configure two static summary routes to interface Null 0:
 - i. A summary IPv4 route for 10.0.0.0/8.
 - ii. A summary IPv6 route for 2001:db8:100::/48.
8. ISP in the “ISP Network”, configure MP-BGP.
 - a. Configure ISP in BGP ASN 500 and use the router-id 2.2.2.2.
 - b. Configure and enable an IPv4 and IPv6 neighbor relationship with R1 in ASN 200
 - c. In IPv4 address family:
 - i. The Loopback 0 IPv4 network (/32).
 - ii. The default route 0.0.0.0/0.
 - d. In IPv6 address family
 - i. The Loopback 0 IPv0 network (/128).
 - ii. The default route (::/0).
 - e. Configure two static summary routes to interface Loopback 0:
 - i. An IPv4 default static route.
 - ii. An IPv6 default static route.
9. On switches S1, S2, configure VLANs as shown in the table:

VLAN number	Name
100	Management
101	UserA

102	UserB
999	NATIVE

configure IEEE 802.1Q trunk interfaces on interconnecting switch links.
Configure VLANs as shown in the table.
Set Switch Interfaces appropriately as Trunk and Access ports as per the scenario enabling a successful and feasible network connectivity.
On switches S1 and S2, configure Rapid PVST+ as spanning tree mode.
Configure PortFast and BPDU Guard on the interfaces connected to PCs.
Shutdown all unused ports.

10. On all switches, configure an LACP EtherChannel as shown in the topology. Make sure you modify your configuration according to the request.
11. On all devices, set the local clock to the current UTC time.
12. Configure ISP as NTP master at stratum level 3. Other Networks to synchronize with ISP
13. Enable port security on ports connected to end devices. Set the maximum so that only one device can access the Fast Ethernet ports.
14. Secure the ports so that the MAC address of a device is dynamically learned and added to the running configuration. Set the violation mode so that the Fast Ethernet ports are not disabled when a violation occurs, but a notification of the security violation is generated and packets from the unknown source are dropped.
15. Test Connectivity. Troubleshoot if required

16. Submission Requirement

Copy running configuration of all devices. It must be saved as “studentname_id” and uploaded onto Moodle.

All documentation for your solution should be submitted electronically on Moodle. It is your responsibility that you submit all the outputs and files correctly.