



Proyek Uji Lomba Kompetensi Siswa Nasional 2026

SMA/MA/SMK/MAK/Sederajat



Cabang Ajang

**Teknologi Informasi Sistem Administrasi Jaringan
(IT Network System Administration)**

ACTUAL TEST PROJECT

MODUL B – NETWORK SYSTEMS

IT NETWORK SYSTEMS ADMINISTRATION

**LOMBA KOMPETENSI SISWA DIKMEN
TINGKAT NASIONAL 2026**

Contents

- Contents 3
- Introduction..... 4
- Description of project and tasks..... 4
- Physical Topology..... 1
- Instructions to the Competitor..... 4
- Basic Configuration 6
- Switching..... 7
- Routing..... 8
- Services 9
- Security 9

Introduction

Network technology knowledge is becoming essential nowadays for people who want to build a successful career in any IT engineering field. This test project contains a lot of challenges from real life experience, primarily IT integration and IT outsourcing. If you are able to complete this project with the high score, you are definitely ready to service the network infrastructure for any multi-branch enterprise.

Description of project and tasks

This test project is designed using a variety of network technologies that should be familiar from the Cisco certification tracks. Tasks are broken down into following configuration sections:

- Basic Configuration
- Switching
- Routing
- Services
- Security

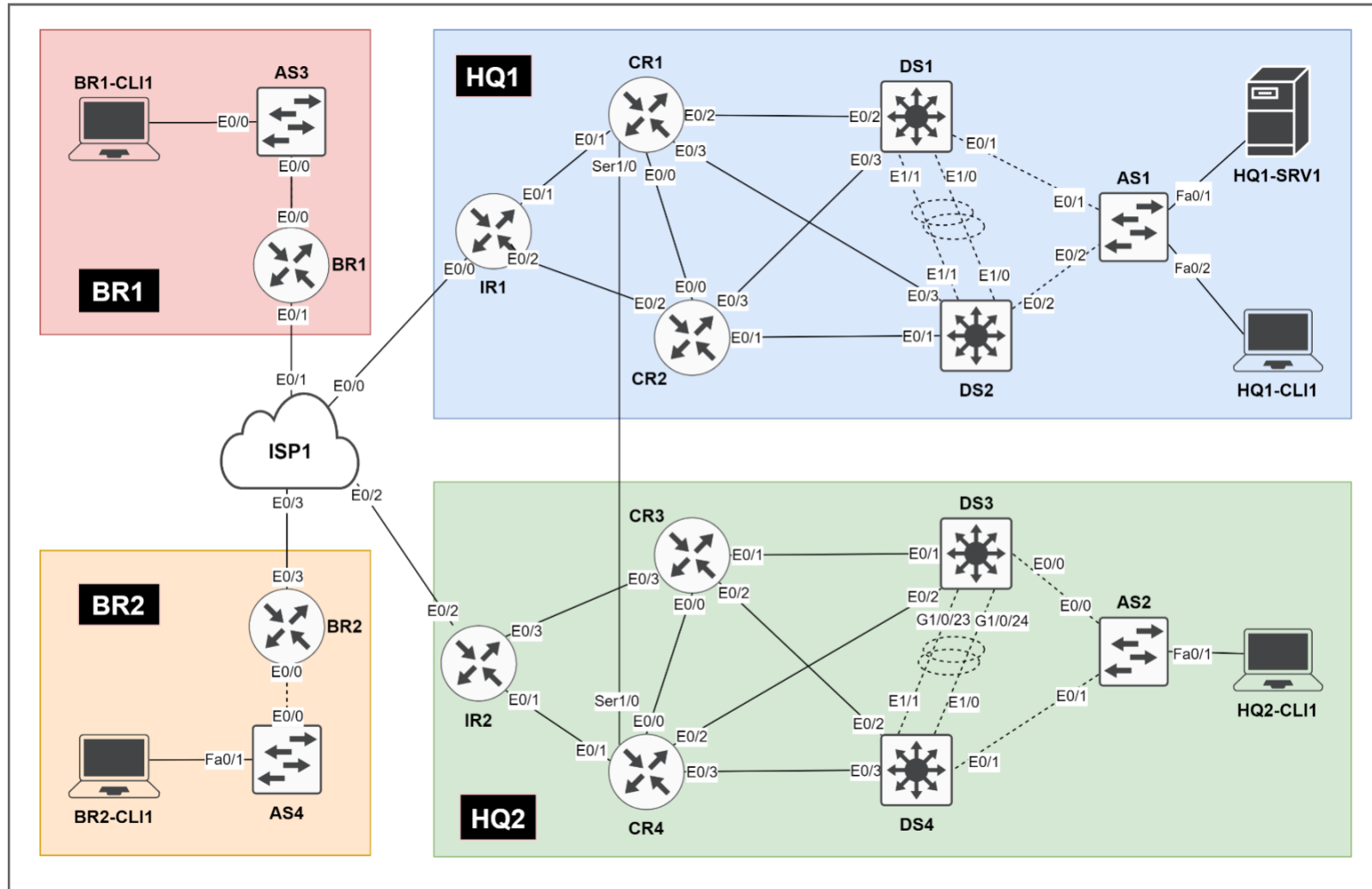
It is very important to read the whole test project first. However, be aware that not all tasks are written in chronological order. Some sections may require configuration from other sections below them. Do not waste your time if you're stuck with some tasks. You can use temporary solution (if you have technology stack dependency) and continue to work with other tasks, this may allow you to go back afterwards and fix things that are not working properly if you still have time.

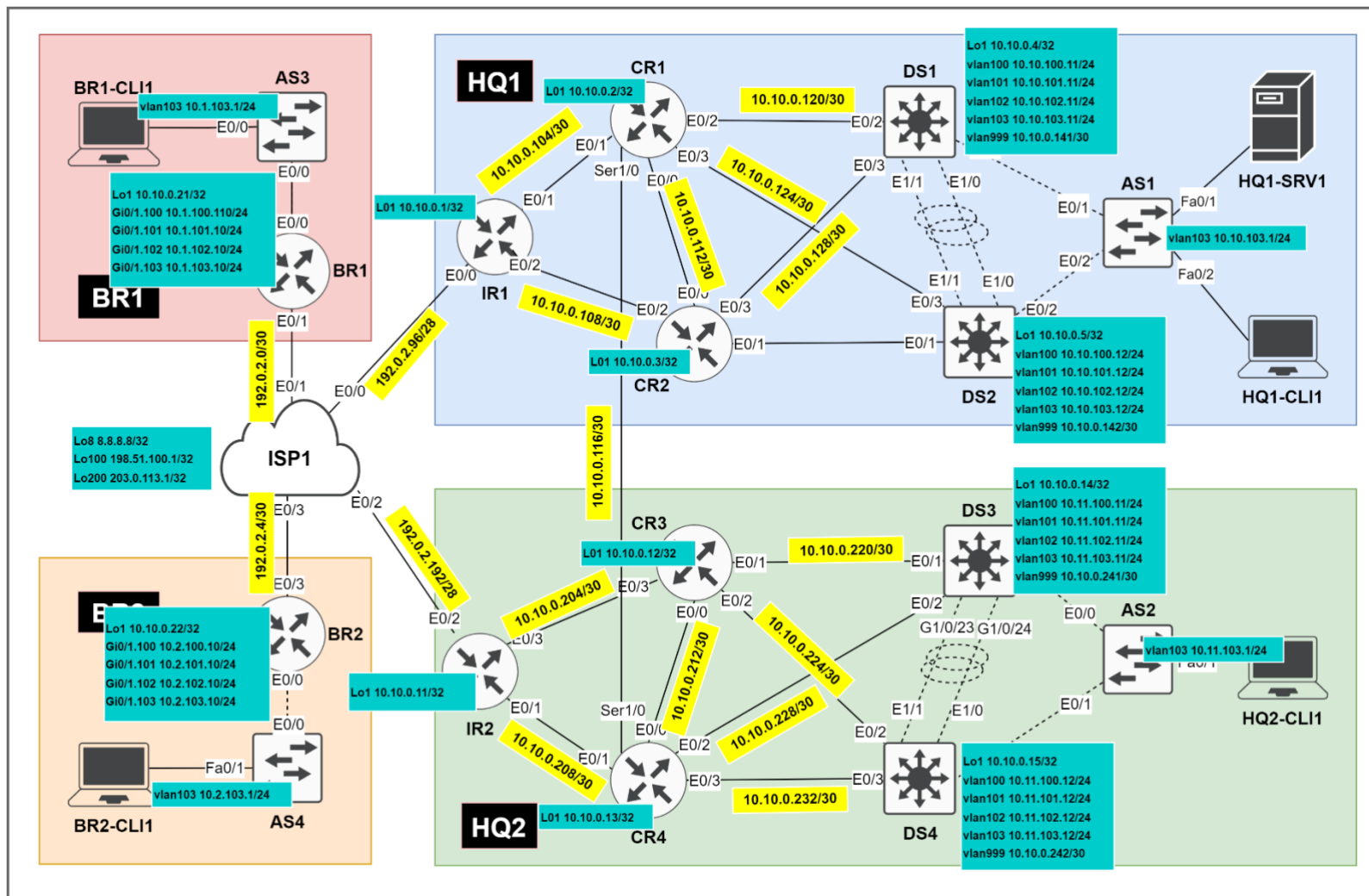
Login Hosts

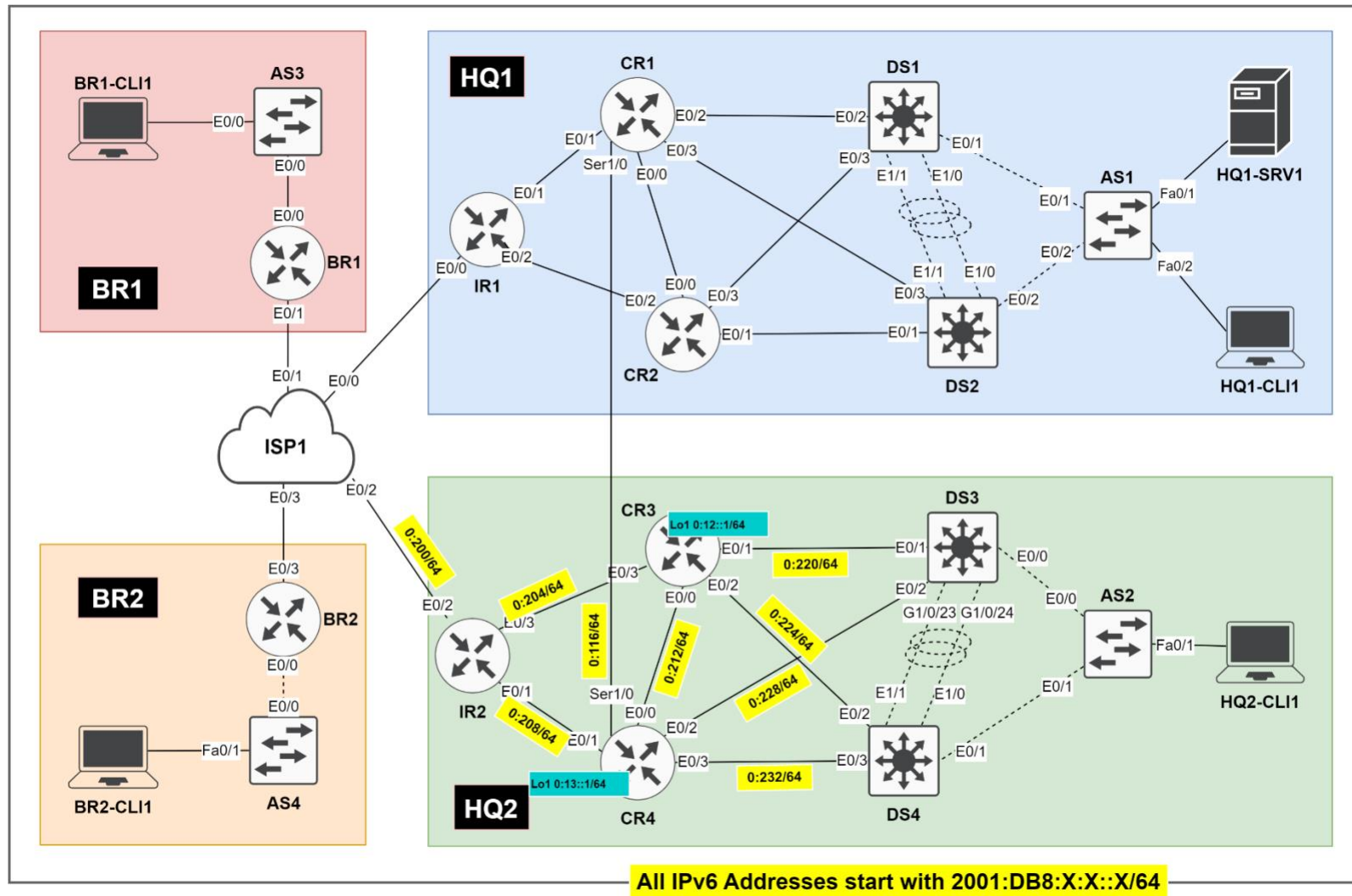
Username : cisco
Password : cisco

Physical Topology

Below is the physical topology of the Test Project.







Instructions to the Competitor

Please carefully read below instruction.

1. Please do not modify ISP1's configuration. All ISP1 configurations are completed, and you are not supposed to touch that device.
2. Read all tasks in each section before proceeding with any configuration. The completion of any item may require the completion of any previous or later item.
3. If you need to add a command to ensure the service functions, there will be no point deduction. You are free to add commands, the most important thing is that the main objective of the task can function properly.
4. Save your configurations frequently; accidents do and will happen.
5. **All Router and Switch IP Addresses configuration already done for you EXCEPT IP ADDRESS OF INTERFACE VLAN.**

DEVICE	INTERFACE	IPV4 ADDRESS	NEIGHBOR
ISP1	Ethernet 0/0	192.0.2.101/28	IR1
ISP1	Ethernet 0/2	192.0.2.201/28	IR2
ISP1	Ethernet 0/1	192.0.2.1/30	BR1
ISP1	Ethernet 0/3	192.0.2.5/30	BR2
ISP1	Loopback100	198.51.100.1/24	N/A
ISP1	Loopback200	203.0.113.1/24	N/A
IR1	Ethernet 0/1	10.10.0.105/30	CR1
IR1	Ethernet 0/2	10.10.0.109/30	CR2
IR1	Ethernet 0/0	192.0.2.102/28	ISP1
IR1	Loopback1	10.10.0.1/32	N/A
IR2	Ethernet 0/3	10.10.0.205/30	CR3
IR2	Ethernet 0/1	10.10.0.209/30	CR4
IR2	Ethernet 0/2	192.0.2.202/28	ISP1
IR2	Loopback1	10.10.0.11/32	N/A
CR1	Ethernet 0/0	10.10.0.113/30	CR2
CR1	Ethernet 0/2	10.10.0.121/30	DS1
CR1	Ethernet 0/3	10.10.0.125/30	DS2
CR1	Ethernet 0/1	10.10.0.106/30	IR1
CR1	Serial1/0	10.10.0.117/30	CR4
CR1	Loopback1	10.10.0.2/32	N/A
CR2	Ethernet 0/0	10.10.0.114/30	CR1
CR2	Ethernet 0/1	10.10.0.133/30	DS2
CR2	Ethernet 0/3	10.10.0.129/30	DS1

DEVICE	INTERFACE	IPV4 ADDRESS	NEIGHBOR
CR2	Ethernet 0/2	10.10.0.110/30	IR1
CR2	Loopback1	10.10.0.3/32	N/A
CR3	Ethernet 0/0	10.10.0.213/30	CR4
CR3	Ethernet 0/1	10.10.0.221/30	DS3
CR3	Ethernet 0/2	10.10.0.225/30	DS4
CR3	Ethernet 0/3	10.10.0.206/30	IR2
CR3	Loopback1	10.10.0.12/32	N/A
CR4	Ethernet 0/0	10.10.0.214/30	CR3
CR4	Ethernet 0/3	10.10.0.233/30	DS4
CR4	Ethernet 0/2	10.10.0.229/30	DS3
CR4	Ethernet 0/1	10.10.0.210/30	IR2
CR4	Serial1/0	10.10.0.118/30	CR1
CR4	Loopback1	10.10.0.13/32	N/A
DS1	Ethernet 0/2	10.10.0.122/30	CR1
DS1	Ethernet 0/3	10.10.0.130/30	CR2
DS1	Loopback1	10.10.0.4/32	N/A
DS2	Ethernet 0/1	10.10.0.134/30	CR2
DS2	Ethernet 0/3	10.10.0.126/30	CR1
DS2	Loopback1	10.10.0.5/32	N/A
DS3	Ethernet 0/1	10.10.0.222/30	CR3
DS3	Ethernet 0/2	10.10.0.230/30	CR4
DS3	Loopback1	10.10.0.14/32	N/A
DS4	Ethernet 0/3	10.10.0.234/30	CR4
DS4	Ethernet 0/2	10.10.0.226/30	CR3
DS4	Loopback1	10.10.0.15/32	N/A
AS1	Vlan33	10.10.103.1/24	N/A
AS2	Vlan33	10.11.103.1/24	N/A
BR1	Ethernet 0/1	192.0.2.2/30	ISP1
BR1	Ethernet 0/0.30	10.1.100.10/24	N/A
BR1	Ethernet 0/0.31	10.1.101.10/24	N/A
BR1	Ethernet 0/0.32	10.1.102.10/24	N/A
BR1	Ethernet 0/0.33	10.1.103.10/24	N/A

DEVICE	INTERFACE	IPV4 ADDRESS	NEIGHBOR
BR1	Loopback1	10.10.0.21/32	N/A
AS3	Vlan33	10.1.103.1/24	N/A
BR2	Ethernet 0/3	192.0.2.6/30	ISP1
BR2	Ethernet 0/0.30	10.2.100.10/24	N/A
BR2	Ethernet 0/0.31	10.2.101.10/24	N/A
BR2	Ethernet 0/0.32	10.2.102.10/24	N/A
BR2	Ethernet 0/0.33	10.2.103.10/24	N/A
BR2	Loopback1	10.10.0.22/32	N/A
AS4	Vlan33	10.2.103.1/24	N/A

Basic Configuration

1. Configure device hostname according to the topology.
2. Configure domain name to "cloud.id" on all devices.
3. Create user "admin" with secret "Pa\$\$word" with maximum privilege.
4. Display banner motd "Unauthorized Access is Strictly Prohibited" before user authentication on all devices.
5. Configure device timezone to GMT+7 on all devices.
6. Configure IPv4/IPv6 address according to the addressing table. Only HQ2 requires IPv6 configuration.

DEVICE	INTERFACE	IPV4 ADDRESS	NEIGHBOR
DS1	VLAN30	10.10.100.11/24	N/A
	VLAN31	10.10.101.11/24	N/A
	VLAN32	10.10.102.11/24	N/A
	VLAN33	10.10.103.11/24	N/A
	VLAN99	10.10.0.141/30	DS2
DS2	VLAN30	10.10.100.12/24	N/A
	VLAN31	10.10.101.12/24	N/A
	VLAN32	10.10.102.12/24	N/A
	VLAN33	10.10.103.12/24	N/A
	VLAN99	10.10.0.142/30	DS2
DS3	VLAN30	2001:DB8:11:100::11/64	N/A
		10.11.100.11/24	N/A
	VLAN31	2001:DB8:11:101::11/64	N/A
		10.11.101.11/24	N/A

DEVICE	INTERFACE	IPV4 ADDRESS	NEIGHBOR
	VLAN32	2001:DB8:11:102::11/64	N/A
		10.11.102.11/24	N/A
	VLAN33	10.11.103.11/24	N/A
	VLAN99	2001:DB8:0:240::1/64	DS4
		10.10.0.241/30	DS4
DS4	VLAN30	2001:DB8:11:100::12/64	N/A
		10.11.100.12/24	N/A
	VLAN31	2001:DB8:11:101::12/64	N/A
		10.11.101.12/24	N/A
	VLAN32	2001:DB8:11:102::12/64	N/A
		10.11.102.12/24	N/A
	VLAN33	10.11.103.12/24	N/A
	VLAN99	2001:DB8:0:240::2/64	DS3
		10.10.0.242/30	DS3

Switching

- Configure VTP Version 3 on DS1, DS2, DS3, DS4, AS1 and AS2 only with domain "LKSN2026". Configure DS1 and DS3 as VTP Server and other switches as clients.
 - AS3 and AS4 are standalone switches and must not participate in the VTP domain.
- Configure following VLANs across all distribution (DSx) and access switches (ASx) in this topology.

VLAN ID	VLAN NAME	DEVICES
30	SERVER	DS1, DS2, DS3, AS1, AS2, AS3, AS4
31	USER1	DS1, DS2, DS3, AS1, AS2, AS3, AS4
32	USER2	DS1, DS2, DS3, AS1, AS2, AS3, AS4
33	MGT	DS1, DS2, DS3, AS1, AS2, AS3, AS4
99	L3_P2P	DS1, DS2, DS3, DS4

- Configure link aggregation on DC switches refer to the list below. The distribution switches (DSx) must act as a negotiator to perform link aggregation if using negotiation protocol, meanwhile other switch must be configured as the responder.
 - DS1 (channel 2) <=> DS2 (channel 2) using LaCP with port E1/0 & E1/1
 - DS3 (channel 3) <=> DS4 (channel 3) using PaGP with port E1/0 & E1/1

4. Configure all distribution switches (DS1-4) ports connect to AS1 and AS2 as trunk ports. Configure vlan 88 as native vlan across these trunk ports and allow all VLANs in the table. Don't forget to configure both AS1-2 devices. Also configure AS3 and AS4 E0/0 interface as trunk ports. You can leave vlan 1 as native vlan for these trunk ports
5. Configure HSRP for the 4 vlans (30-33) to meet following conditions.
 - a In each subnet, default gateway IP address needs to be .10 in each /24 subnet. Use vlan number as HSRP group number when configuring.
 - b DS1 should be the HSRP active for HQ1 and DS3 should be the HSRP active for HQ2 with priority 110 and leave the default value for non priority.
 - c In case of active device (DS1 or DS3) goes down DS2 or DS4 should act as active device in each site. When DS1 or DS3 comes back after failure, it should take over HSRP active role once it is operational.
6. Configure port connected to the end device as the access port and enable portfast feature on the port.

Routing

1. Configure BGP peering.
 - a. Configure each router using the autonomous system number specified below:
 - ISP1 : AS 65000 (preconfigured)
 - IR1 : AS 65101
 - IR2 : AS 65102
 - BR1 : AS 65103
 - BR2 : AS 65104
 - b. Configure eBGP peering between ISP1 and IR1, IR2, BR1, and BR2.
 - c. Configure full-mesh eBGP peering between IR1, IR2, BR1, and BR2.
 - d. Establish all BGP peering sessions using loopback interfaces as the update source.
Note: Static host routes and default routes required to ensure bidirectional reachability between the BGP loopback addresses have been preconfigured. These routes are used only as the underlying reachability mechanism for loopback-based eBGP peering and must not be modified.
 - e. Enable BGP neighbor authentication using the password Pa\$\$worD.
 - f. Advertise each router's Loopback1 IPv4 address and all required directly connected public IPv4 networks into BGP.
 - g. Do not use route redistribution to advertise the required BGP networks.
2. Configure EIGRP in COR2.
 - a. Configure EIGRP for IPv4 using autonomous system number 100 on IR2, CR3, CR4, DS3, and DS4.
 - b. Use the Loopback1 IPv4 address as the EIGRP router ID on each device.
 - c. Advertise all Loopback1 and /30 point-to-point networks on IR2, CR3, CR4, DS3, and DS4.
 - d. Advertise VLAN 30, VLAN 31, VLAN 32, and VLAN 33 networks on DS3 and DS4.
 - e. Disable automatic route summarization.
3. Configure OSPF in COR1.
 - a. Configure OSPF process 100 on IR1, CR1, CR2, DS1, and DS2.
 - b. Use the Loopback1 IPv4 address as the OSPF router ID on each device.
 - c. Advertise all Loopback1 and /30 point-to-point networks into OSPF area 0.
 - d. Advertise VLAN 30, VLAN 31, VLAN 32, and VLAN 33 networks on DS1 and DS2 into OSPF area 0.
4. Configure inter-domain routing between COR1 and COR2.
 - a. Configure EIGRP AS100 on CR1 for the serial link between CR1 and CR4.
 - b. Configure mutual redistribution between OSPF process 100 and EIGRP AS100 on CR1.
 - c. Configure an explicit EIGRP seed metric.
 - d. Ensure all internal IPv4 networks are mutually reachable. Do not redistribute BGP routes into OSPF or EIGRP.

Services

You have been asked to configure following IP services.

1. When vlan 31-32 users (~400 in total users and require simultaneous internet access) in HQ1 and HQ2 communicate with internet (You can use 8.8.8.8 IP for testing) their addresses should be translated to following addresses depend on the internet router it goes through.
 - a. Traffic goes via IR1 -> 192.0.2.104 -192.0.2.110
 - b. Traffic goes via IR2 -> 192.0.2.193 -192.0.2.199
2. When HQ1-SRV1 with IP address 10.10.100.101 goes to internet it should appear as 192.0.2.99 IR1.
 - a. HQ1-SRV1 has already configured with 10.10.100.101 statically.
3. Configure DHCP services on DS1 and DS3 to meet requirements below.
 - a. on DS1
 - a. VL31 DHCP address scope 10.10.101.101-10.10.101.254 with default router of 10.10.101.10
 - b. VL32 DHCP address scope 10.10.102.101-10.10.102.254 with default router of 10.10.102.10
 - a. on DS3
 - a. (c) VL31 DHCP address scope 10.11.101.101-10.11.101.254 with default router of 10.11.101.10
 - b. (d) VL32 DHCP address scope 10.11.102.101-10.11.102.254 with default router of 10.11.102.10
4. Configure DHCP services BR1 and BR2 in a way clients BR1-CLI1 get IP address from vlan31 and BR2-CLI1 get IP address from vlan32.
 - a. BR1-VL31 DHCP address scope 10.1.101.101-10.1.101.254 with default-gateway 10.1.101.10.
 - b. BR2-VL32 DHCP address scope 10.2.102.101-10.2.102.254 with default-gateway 10.2.102.10.

Security

1. Configure SSH version 2 on all network devices in IR1, IR2, BR1 and BR2 routers.
 - a. Use local authentication
 - b. Telnet should not be allowed when accessing network devices.
2. Configure DHCP snooping for VLAN31 and VLAN32 on HQ1 & HQ2 sites. Ensure AS1 and AS2 only forwarding packet sourced from IP that has been registered in DHCP snooping database.
3. Limit only HQ1-SRV1 (10.10.100.101/24) can SSH into IR1 and IR2 with the name ACL: SSH_ONLY.
4. Configure port security on HQ site on both SW switch that is connected to the client. Permit maximum 2 MAC Address and save those MAC address on running-config. In case of policy violation, security message should be displayed on the console and port should not go to err-disabled state.
5. Configure BPDU feature on DC switches.
 - a. Access switch must not forward BPDU to the port that is connected to the client. Disable port if port receive BPDU