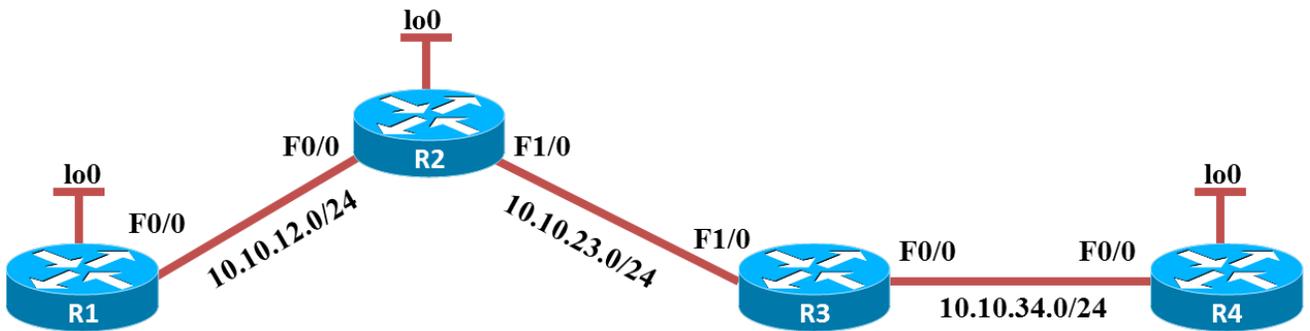


CNS – Skill Based Test

1 Topology



2 Important notices:

- Addresses on router physical interfaces **are already configured**.
 - For each router, the last octet is going to be represented by the number of the router in the above topology (Example: 10.10.12.1 for R1 and 10.10.12.2 for R2)
- Not all configurations required to achieve the objectives are explicitly stated. If there are multiple ways of achieving an objective, any one of them is valid, provided it is not explicitly prohibited
- CCO (cisco.com) access is permitted. Google searches that led to cisco.com are also permitted. No other Internet access is allowed.
 - **If you access any other site you will fail the exam**
- No written notes / curriculum / reference book access is allowed.
- Do not use IP addresses other than the ones in the diagram and/or text.
- Grading will be done for each sub-task that is completed
- There are some tasks that are dependent upon each other, so we recommend you solve the tasks **in order**.
- The completion of a sub-task requires:
 - The actual technical solving of the task
 - Knowledge required to verify that specific task.
- The solving of a specific task **MUST NOT** invalidate the functionality of previously solved tasks
- Save your configurations often!

3 Tasks

1. IP Addressing

- a. Configure the IP addresses on router interfaces according to the table below.

| Router | Interface | IP address |
|--------|-----------|---------------|
| R1 | Lo0 | 10.10.1.1 /24 |
| R2 | Lo0 | 10.10.2.1 /24 |
| R4 | Lo0 | 10.10.4.1 /24 |

Task total: 10 points

2. Static routing

- a. Routing is already enabled on the links between R1, R2, R3 and R4 using OSPF. Configure the missing static routes so that each router will see every loopback in the topology.

Hint: default routes are also permitted

Task total: 10 points

3. Securing Network Devices – all the following configurations will be done on router R1.

- a. Configure the password “cns” to secure the console and the vty lines.
 - i. Make sure the password will be required when connecting via Telnet.
 - ii. Make sure the password is being stored in an encrypted form

10 points

- b. Configure SSH access to router R1 using authentication through AAA with the local user **cns** and the password **cns**. Do not disable telnet as a remote access method.

15 points

- c. Create the user **monitor** at privilege level 10 and allow this user to issue the *show running-config* command.

10 points

Task total: 35 points

4. ACLs

- a. Configure the network so that only the hosts residing on the Lo0 of R2 can have remote access to R1 (either to Lo0 or to the Fa0/0 interface) through SSH.

10 points

- b. Configure the network so that telnet to Lo0 of R1 is only allowed from R2's F0/0 interface address.

10 points

- c. Configure the network so that:
 - i. R1(F0/0) can initiate HTTP connections to R3(F1/0)
 - ii. The return HTTP traffic from R3(F1/0) to R1(F0/0) is permitted
 - iii. R3(F1/0) cannot initiate HTTP connections to R1(F0/0)

Hint: test this by issuing the **"ip http server"** command on R3 and the **"telnet 10.10.23.3 80"** command from R1.

5 points

Task total: 25 points

5. IPsec and CBAC

- a. Configure an IPsec VPN tunnel between R2 and R4 that should accomplish the following requirements:
 - i. The IPsec tunnel will encrypt all ICMP traffic between R4(Lo0) and R2(Lo0)
 - ii. The ISAKMP security association must use 3DES encryption, the pre-shared key **cns** and an MD5 hash.
 - iii. The IPsec transform set must use ESP 256 bits encryption with MD5-HMAC.

Note: Call your assistant to grade this subject before attempting CBAC

10 points

- b. Implement a CBAC firewall on R3 following the below rules:
 - i. R4 should be able to initiate any traffic from any of its interfaces to any network beyond R3.
 - ii. Return traffic for traffic initiated at the above sub-point should be allowed back to R4
 - iii. Traffic initiated by R2 or R1 to R4 should be dropped.

10 points

- c. Configure the CBAC firewall to allow R2(Lo0) to initiate a ping to R4(Lo0) through the IPsec tunnel.

10 points

Task total: 30 points

Exam total: 110 points