CCIE Security v3.0 Configuration Practice Labs,

Second Edition

Yusuf Bhaiji

ciscopress.com

About the Author

Yusuf Bhaiji, CCIE No. 9305 (R&S and Security), has been with Cisco Systems for 9 years and is currently the product manager for the Cisco CCIE Security certification and CCIE Proctor in Cisco Dubai Lab. Prior to this, he was technical lead for the Sydney TAC Security and VPN team.

Yusuf's passion for security technologies and solutions has played dominant a role in his 19 years of industry experience, from as far back as his initial master's degree in computer science and since reflected in his numerous certifications.

Yusuf prides himself in his knowledge sharing abilities, evident in the fact that he has mentored many successful candidates, as well as having designed and delivered a number of network security solutions around the globe.

Yusuf is advisory board member of several non-profit organizations for the dissemination of technologies and promoting indigenous excellence in the field of internetworking through academic and professional activities. Yusuf chairs the Networkers Society of Pakistan (NSP) and IPv6 Forum Pakistan chapter.

Yusuf has previously authored two Cisco Press books: *Network Security Technologies and Solutions* and *CCIE Security Practice Labs First Edition*. In addition to authoring these, he has also been a technical reviewer for several Cisco Press publications and written articles, white papers, and presentations on various security technologies. He is a frequent lecturer and well-known speaker presenting at several conferences and seminars worldwide.

About the Technical Editor

Aun Raza, CCIE No. 23580 (Security), is a seasoned IT professional, with almost 10 years of experience in the industry, with top multi-national companies including Dow Jones & Co, Rockwell, KPMG and currently Cisco. At Cisco, Aun has been working with the world-renowned TAC for the past 2½ years, specializing in VPN and Security technologies.

Aun's passion for technology is apparent from the various certifications he holds, including CISSP, MCSE and Sun's SCSA and SCNA amongst other Cisco Professional certifications. When he's not working or engrossed in learning about some new exciting technology, he's either busy entertaining his little ones, hassling his wife, or playing ping pong.

 Please see page 474 for more details.

Dedication

I dedicate this book to my beloved wife Farah. Thank you for being my pillar of strength and empowering my success.

And,

I dedicate this book to my daughter Hussaina (my angel) and my son Abbas (my chi), for being the joy in my life that makes everything else worthwhile.

Foreword

As networks become increasingly complex, so does the job of securing those networks. This evolution has moved security-focused engineers from an isolated role to a distinct cross-functional strategic player responsible for the protection of highly sensitive organizational and individual data and assets. IT Security professionals are not only accountable for protecting the network and its data, but also troubleshooting, monitoring threats, and managing risks, all while maintaining constant availability to business-critical functions.

With the network security marketplace escalating at double-digit growth, IT Security professionals continue to be in high demand and CCIE certification sets apart those engineers with proven expert-level knowledge and skills. The CCIE program continues to be the most prestigious IT certification program, differentiating experts through rigorous hands-on assessments, which differentiates experts through hands-on assessments.

CCIE Security Practice Labs offers an invaluable mix of instruction and practice labs, approximating the level of complexity and difficulty of the real CCIE labs. These labs will allow candidates to practice their configuration and troubleshooting skills on real-world network security scenarios. Candidates will receive invaluable feedback on their performance as well as instruction in key areas. Proficiency in these labs will provide candidates with experience and confidence that will benefit their CCIE lab taking experience.

Yusuf Bhaiji is the Program Manager for the CCIE Security track and has also served as a CCIE proctor in the Cisco Dubai lab. Yusuf's passion and expertise has led to international recognition and he is a globally sought-after speaker and author in the areas of security technologies and solutions. Yusuf's experiences in combination with his numerous successful mentoring programs, give him a unique insight into taking candidates through a hands-on preparation process that will result in expanded expert-level skills in network security.

Sarah DeMark, Ph. D. Sr. Manager, Learning & Certifications

 Please see page 474 for more details.

CHAPTER 1

Practice Lab 1

Overview

Practice Labs in this book are based on the CCIE Security v3.0 Lab Exam blueprint. All sections in these labs closely mimic the real lab exam, providing candidates with a comprehensive mock lab scenario with greater complexity to prepare you for the real lab exam.

Labs in this book are multiprotocol, multitechnology, testing you in all areas as outlined in the CCIE Security Lab blueprint v3.0.

To assist you, initial configurations and final solution configurations are provided for the entire lab, including common **show** command outputs from all the devices in the topology.

In addition, an "Ask the Proctor" section is provided at the end of the lab. It provides assistance and common answers to ensure that you are following the correct solution path. Try to avoid referring to this section too often, though, because this luxury is not available on the real lab exam.

Furthermore, a "Lab Debrief" section is provided, which gives you a comprehensive analysis of what is required and how the desired result is achieved. The "Lab Debrief" also provides verification and solution tips, troubleshooting hints, and highlights of the integrated complexities, if any.

NOTE

Hardware cabling, IP addressing, and IP routing are preconfigured in the real CCIE Lab, except for the security appliances, ASA firewall, and IPS sensor (candidates are required to configure the ASA and IPS).

Each Practice Lab lasts 8 hours and is worth 100 points. You must score at least 80 to pass. The lab has been designed such that you should be able to complete all the questions in eight hours, excluding prelab setup such as initial configuration, IP addressing, IP routing, and hardware cabling.

Initial configurations are provided, including basic IP addressing and IP routing. You can copy and paste the initials to your devices before you start the Practice Lab. You may want to allow an additional hour for prelab setup and cabling your rack. Use the cabling instructions shown in Figures 1-1 and 1-2 to cable all devices in your topology, and observe the instructions in the general guidelines that follow.

You can use any combination of devices, as long as you fulfill the lab topology diagram shown in Figure 1-3. You are not required to use the same model used in this lab.

You will now be guided through the equipment requirements and prelab setup in preparation for completing Practice Lab 1.

Equipment List

You need the hardware and software components listed in Table 1-1 to mount Practice Lab 1.

TABLE 1-1 Equipment list

Device	Model	Software	Interfaces
R1 R2 R3 R4 R5 R6	Six Cisco ISRs (Integrated Services Routers), any model	Cisco Router IOS Version 12.4(15)T or above(Advanced Enterprise Services K9 image)	Two Gigabit Ethernet interfaces and two serial (sync/async) interfaces on each router
Sw1 Sw2	Two Cisco 3560 Catalyst Switches	Cisco Catalyst IOS Version 12.2(44)SE1 or above (Advanced IP Services K9 image)	24 ports on each switch
ASA1 ASA2	Two Cisco ASA 5510 (or above) Firewall Appliances	Cisco ASA Software Version 8.0(3) (Security Plus license)	Four Ethernet interfaces and one Management interface on each ASA Firewall
IPS	One Cisco IPS 4240 (or above) Sensor Appliance	Cisco IPS Sensor Software Version 6.1(1)E2 or above with latest Signature Update	Four Gigabit Ethernet Sensing interfaces One Management interface
Server PC	One desktop PC	Microsoft Windows 2003 Server (Service Pack 2) with Cisco Secure ACS server software version 4.1	One Ethernet
Test PC	One desktop PC	Microsoft Windows XP with Cisco AnyConnect VPN Client version 2.3.x and Cisco Secure VPN client version 5.x	One Ethernet

General Guidelines

- Read the entire Practice Lab document before you start.
- Knowledge of configuration and troubleshooting techniques is part of the lab exam.
- You are allowed to add, remove, and modify any static/default routes as required.
- Use "cisco" as the password for any authentication string, enable-password, and TACACS+/RADIUS key, or for any other purpose during this Practice Lab.
- You can add additional loopbacks as specified during this Practice Lab.
- You must time yourself to complete this Practice Lab exam in 8 hours.
- The Practice Lab has 100 points total, and you must score at least 80 to pass. Each section head says how many points that section is worth.
- Do not configure any AAA authentication and authorization on the console and aux ports.

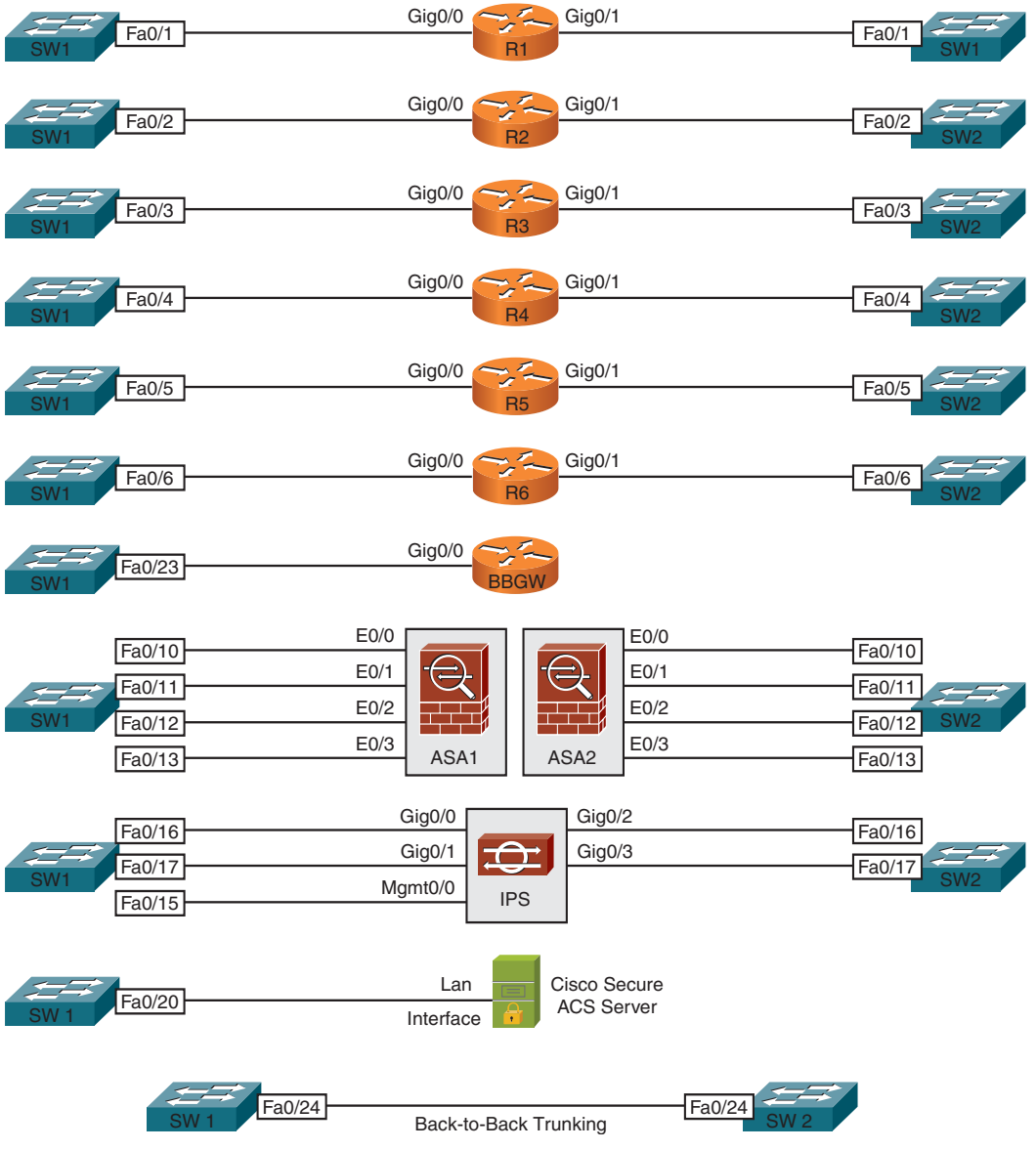
Prelab Setup and Cabling Instructions

You can use any combination of routers, as long as you fulfill the topology diagram outlined in Figure 1-3. You are not required to use the same model of routers. You need to set up the devices using the following cabling instructions to start Practice Lab 1. Use Figures 1-1 and 1-2 to cable all devices in your topology. It is not a requirement to use the same type or sequence of interface. You may use any combination of interface(s) as long as you fulfill the requirement.

Catalyst Switchport Cabling Diagram

Figure 1-1 illustrates the complete details of how to cable all your devices to both of the Catalyst switches before starting this lab as part of the prelab setup. You are not required to use the same type or sequence of interface. You may use any combination of interface(s), as long as you fulfill the requirement. However, it will be much easier for you to copy and paste the initial configuration and refer to the final solutions if you use the same cabling schema.

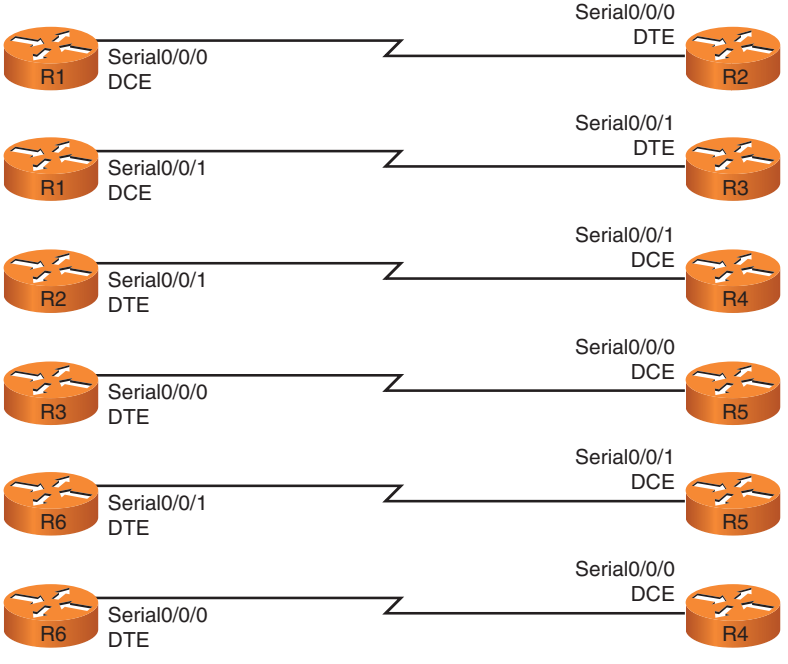
FIGURE 1-1
Catalyst switchport cabling diagram



Serial WAN Interface Cabling Diagram

Figure 1-2 illustrates the complete details of how to cable all your serial WAN interfaces back-to-back. Again, you are not required to use the same type or sequence of interface. You may use any combination of interface(s) as long as you fulfill the requirement. However, it will be much easier for you to copy and paste the initial configuration and refer to the final solutions if you use the same cabling schema.

FIGURE 1-2
Serial WAN interface cabling diagram



NOTE
All serial interfaces are connected to each other back-to-back.

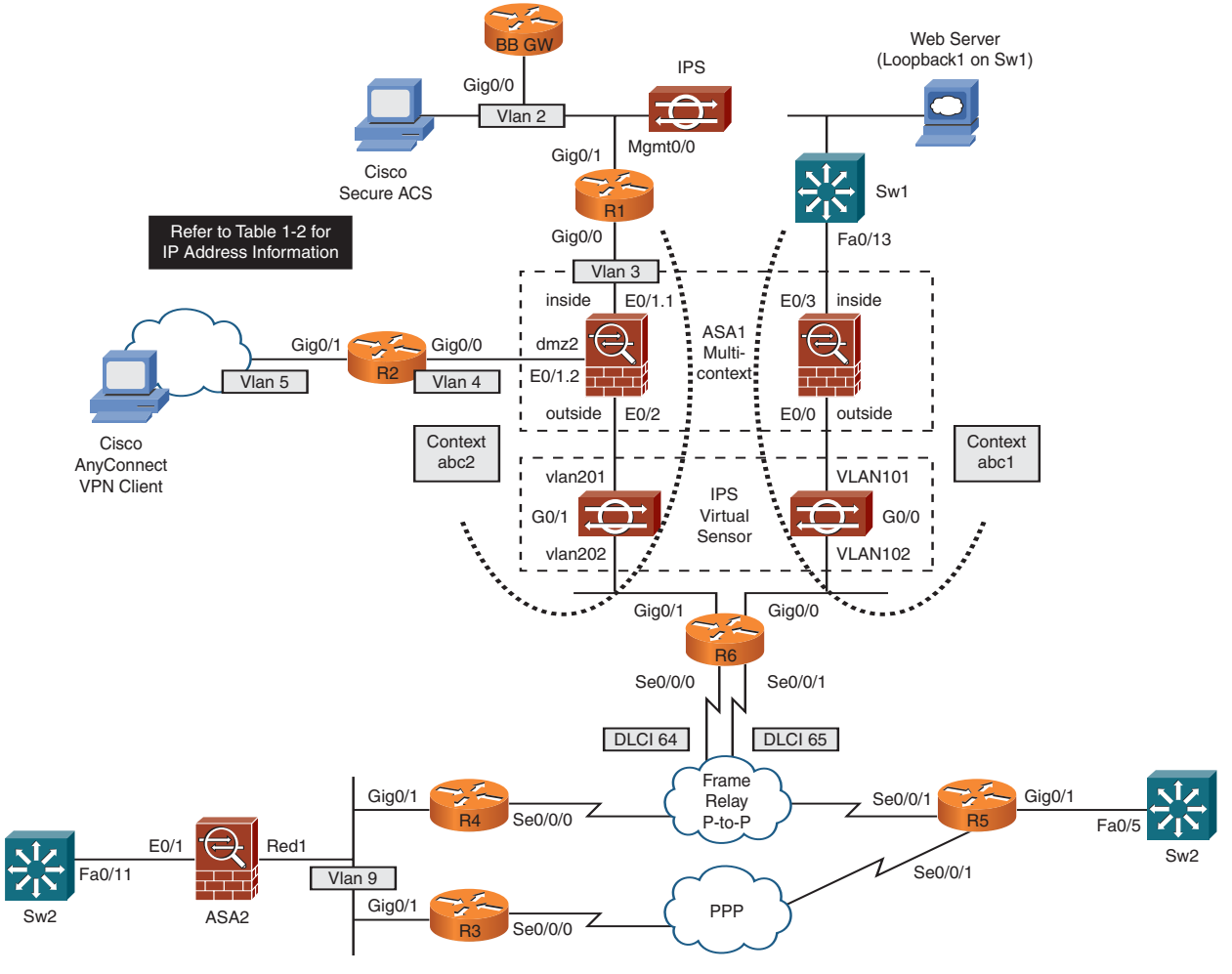
Clock rate and Frame Relay switching are preconfigured in the initial configuration provided.

Lab Topology Diagram

Figure 1-3 illustrates the logical lab exam topology. This diagram is very important and perhaps is the most referenced item throughout the exam. It is highly recommended that you spend a few minutes focusing on how the logical setup is

done (mind mapping). Also redraw the entire diagram by yourself. This will help reinforce the setup and will make it easier for you to navigate through the topology while working on the questions. Take note of Table 1-2, which provides comprehensive details that map this diagram.

FIGURE 1-3
Lab topology diagram



NOTE

The BB GW router shown in the diagram is not compulsory. It's OK if you cannot arrange for this router; it is used for default GW purposes only in this lab. In your scenario, it could be your service provider or upstream router. However, if you can arrange a spare router, any low-end router will do, such as the 2500 series or above, with any Cisco IOS Software version with the basic IP Plus image. Additionally, you can use this router as a terminal/CommServer for console connections to all devices.

IP Address Details

Table 1-2 is a complete list of IP addresses, relevant VLAN numbers, and DLCI information for all devices used in this lab. All of them have been preconfigured in the initial configuration files provided. You can simply copy and paste the initial configuration if you use the same cabling schema.

TABLE 1-2 IP address information

Device	Interface	IP Address	Mask	VLAN/DLCI
R1	GigabitEthernet0/0	192.168.3.11	255.255.255.0	Vlan 3
	GigabitEthernet0/1	192.168.2.11	255.255.255.0	Vlan 2
	Loopback0	10.1.1.1	255.255.255.0	—
R2	GigabitEthernet0/0	192.168.4.11	255.255.255.0	Vlan 4
	GigabitEthernet0/1	192.168.5.11	255.255.255.0	Vlan 5
	Loopback0	10.2.2.2	255.255.255.0	—
R3	Serial0/0/0	192.168.35.3	255.255.255.0	—
	GigabitEthernet0/1	192.168.9.3	255.255.255.0	Vlan 9
	Loopback0	10.3.3.3	255.255.255.0	—
R4	Serial0/0/0	192.168.64.4	255.255.255.0	DLCI 64
	GigabitEthernet0/1	192.168.9.4	255.255.255.0	Vlan 9
	Loopback0	10.4.4.4	255.255.255.0	—
R5	Serial0/0/0	192.168.35.5	255.255.255.0	—
	Serial0/0/1	192.168.65.5	255.255.255.0	DLCI 65
	GigabitEthernet0/1	192.168.11.10	255.255.255.0	—
	Loopback0	10.5.5.5	255.255.255.0	—

TABLE 1-2 *Continued*

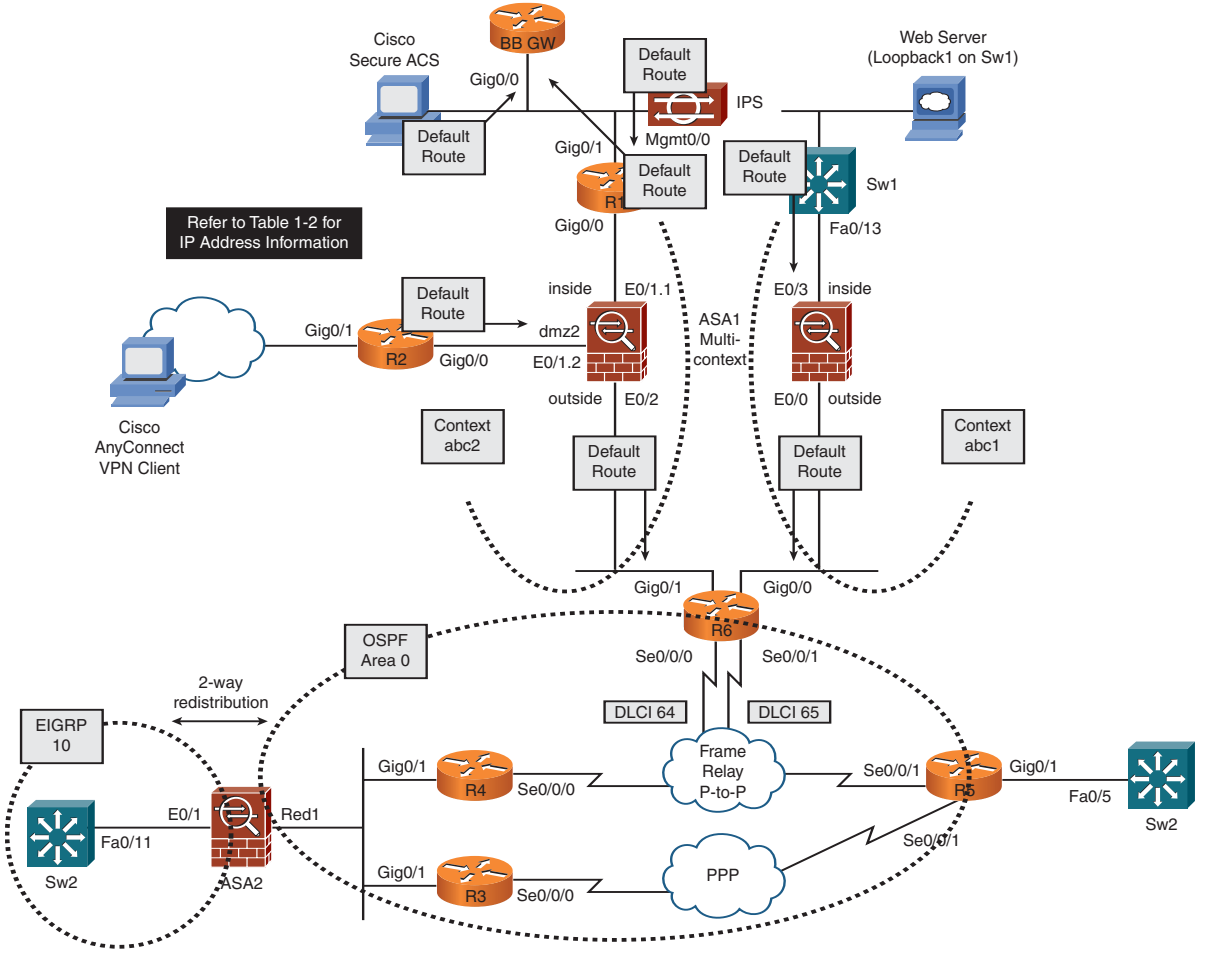
Device	Interface	IP Address	Mask	VLAN/DLCI
R6	Serial0/0/0	192.168.64.6	255.255.255.0	DLCI 64
	Serial0/0/1	192.168.65.6	255.255.255.0	DLCI 65
	GigabitEthernet0/0	192.168.7.11	255.255.255.0	Vlan 102
	GigabitEthernet0/1	192.168.6.11	255.255.255.0	Vlan 202
	Loopback0	10.6.6.6	255.255.255.0	—
Sw1	Loopback0	10.7.7.7	255.255.255.0	—
	Loopback1	172.16.1.1	255.255.255.0	—
	FastEthernet0/13	192.168.8.11	255.255.255.0	—
Sw2	Loopback0	10.8.8.8	255.255.255.0	—
	FastEthernet0/5	192.168.11.11	255.255.255.0	—
	FastEthernet0/11	192.168.10.11	255.255.255.0	—
ASA1 context “abc1”	Ethernet0/0	192.168.7.10	255.255.255.0	Vlan 101
	Ethernet0/3	192.168.8.10	255.255.255.0	—
ASA1 context “abc2”	Ethernet0/2	192.168.6.10	255.255.255.0	Vlan 201
	Ethernet0/1.1	192.168.3.10	255.255.255.0	Vlan 3
	Ethernet0/1.2	192.168.4.10	255.255.255.0	Vlan 4
ASA2	Redundant1 (Ethernet0/0, Ethernet0/2)	192.168.9.10	255.255.255.0	Vlan 9
ASA2	Ethernet0/1	192.168.10.10	255.255.255.0	—
BB GW	GigabitEthernet0/0	192.168.2.1	255.255.255.0	Vlan 2
IPS	Management0/0	192.168.2.12	255.255.255.0	Vlan 2
Cisco Secure ACS	LAN interface	192.168.2.14	255.255.255.0	Vlan 2
Test PC	LAN interface	192.168.5.10	255.255.255.0	Vlan 5

IP Routing Protocol Diagram

Figure 1-4 illustrates the IP routing protocol setup in this exam topology. It shows which protocols are used in this exam, including static and default routes. Table 1-3 provides comprehensive details that map this diagram.

FIGURE 1-4
Routing protocol information

NOTE
Security appliances shown in this diagram (ASA firewall and IPS sensor) are not preconfigured in this Practice Lab. You are required to configure the ASA firewall and IPS sensor accordingly, as stated in the Practice Lab questions.



 Please see page 474 for more details.

IP Routing Details

Table 1-3 provides complete details of IP routing for all devices used in this lab. All of them have been preconfigured in the initial configuration files provided, except for the security appliances—ASA firewall and IPS sensor (candidates are required to configure the ASA and IPS). For all remaining devices, you can simply copy and paste the initial configuration if you are using the same cabling schema.

TABLE 1-3 IP routing information

Device	Route Type	Protocol	Network/Mask	Other Details
R1	Default	—	0.0.0.0/0	Next hop 192.168.2.1 (BB GW router)
	Static	—	10.0.0.0/8 192.168.0.0/16	Next hop 192.168.3.10 (ASA1/abc2/inside interface)
R2	Default	—	0.0.0.0/0	Next hop 192.168.4.10 (ASA1/abc2/dmz2 interface)
R3	Dynamic	OSPF Process 1	Advertise 10.3.3.0/24 192.168.9.0/24 192.168.35.0/24	Area 0
R4	Dynamic	OSPF Process 1	Advertise 10.4.4.0/24 192.168.9.0/24 192.168.64.0/24	Area 0
R5	Dynamic	OSPF Process 1	Advertise 10.5.5.0/24 192.168.35.0/24 192.168.65.0/24	Area 0
R6	Dynamic	OSPF Process 1	Advertise 10.6.6.0/24 192.168.64.0/24 192.168.65.0/24	Area 0 and redistribute connected and static into OSPF
	Static	—	10.1.1.0/24 10.2.2.0/24 192.168.2.0/24 192.168.3.0/24	Next hop 192.168.6.10 (ASA1/abc2/outside interface)

 Please see page 474 for more details.

TABLE 1-3 *Continued*

Device	Route Type	Protocol	Network/Mask	Other Details
	Static	—	192.168.4.0/24 192.168.5.0/24 10.7.7.0/24 172.16.1.0/24 192.168.8.0/24	Next hop 192.168.7.10 (ASA1/abc1/outside interface)
Sw1	Default	—	0.0.0.0/0	Next hop 192.168.8.10 (ASA1/abc1/inside interface)
Sw2	Dynamic	EIGRP AS 10	Advertise 10.8.8.0/24 192.168.10.0/24	Disable autosummary
ASA1 context "abc1"	Default route on outside interface	—	0.0.0.0/0	Next hop 192.168.7.11 (R6)
	Static routes on inside interface	—	10.7.7.0/24 172.16.1.0/24	Next hop 192.168.8.11 (Sw1)
ASA1 context "abc2"	Default route on outside interface	—	0.0.0.0/0	Next hop 192.168.6.11 (R6)
	Static routes on inside interface	—	10.1.1.0/24 192.168.2.0/24	Next hop 192.168.3.11 (R1)
	Static routes on dmz2 interface	—	10.2.2.0/24 192.168.5.0/24	Next hop 192.168.4.11 (R2)
ASA2	Default	—	0.0.0.0/0	Next hop 192.168.9.4 (R4)
	Dynamic	OSPF Process 1	Advertise 192.168.9.0/24	Area 0 and redistribute EIGRP AS 10 into OSPF Process 1
	Dynamic	EIGRP AS 10	Advertise 192.168.10.0/24	Disable autosummary and redistribute OSPF Process 1 into EIGRP AS 10
IPS	Default	—	0.0.0.0/0	Next hop 192.168.2.11 (BB GW router)
Cisco Secure ACS	Default	—	0.0.0.0/0	Next hop 192.168.2.11 (R1)
Test PC	Default	—	0.0.0.0/0	Next hop 192.168.5.11 (R2)

Practice Lab 1
Section 1.0: Core Configuration (20 Points)

Question 1.1: Initializing the ASA1 firewall (5 points)

Initialize the ASA1 firewall, meeting all the following requirements:

- Configure the ASA1 firewall in multicontext routed mode, as shown in Figure 1-3.
- Configure hostname “ASA1” and enable password “cisco.”
- Create three contexts, as shown in Tables 1-4 through 1-8.
- Context names are case-sensitive. Use exact names and numbers, as shown in the tables.
- Assign context “admin” as the admin-context.
- Assign interfaces as shown in the tables. Map physical interface names to logical names.
- Configure IP addresses and all other initialization parameters as shown in the tables.
- Configure static and default routes within context as shown in the tables. You can also refer to Figure 1-4 and Table 1-3 for more information.
- To perform basic verification using ping tests throughout this Practice Lab, you are allowed to permit **icmp any any** in your ACL in both contexts on ASA1.
- Ensure that you can ping all the interfaces, including loopbacks on Sw1 from context abc1.
- Ensure that you can ping all the interfaces, including loopbacks on R1 and R2 from context abc2.

 Please see page 474 for more details.

TABLE 1-4 Context name **admin**

Assign Physical Interface	Logical Name	VLAN	Save Config
Management0/0	mgmt	—	disk0:/admin

TABLE 1-5 Context name **abc1**

Assign Physical Interface	Logical Name	VLAN	Save Config
Ethernet0/0	outside	101	disk0:/abc1
Ethernet0/3	inside	—	

TABLE 1-6 Context name **abc2**

Assign Physical Interface	Logical Name	VLAN	Save Config
Ethernet0/2	outside	201	disk0:/abc2
Ethernet0/1.1	inside	3	
Ethernet0/1.2	dmz2	4	

TABLE 1-7 Context initialization details

Context	Interface	IP Address/Mask	Nameif	Security Level
admin	mgmt	None	mgmt	100
abc1	outside	192.168.7.10/24	outside	0
	inside	192.168.8.10/24	inside	100
abc2	outside	192.168.6.10/24	outside	0
	inside	192.168.3.10/24	inside	100
	dmz2	192.168.4.10/24	dmz2	50

TABLE 1-8 IP routing initialization details

Context	Route Type	Network Prefix(es)	Next Hop
abc1	Configure Default route on outside interface	0.0.0.0/0	192.168.7.11 (R6)
	Configure Static routes on inside interface	10.7.7.0/24 172.16.1.0/24	192.168.8.11 (Sw1)
abc2	Configure Default route on outside interface	0.0.0.0/0	192.168.6.11 (R6)
	Configure Static routes on inside interface	10.1.1.0/24 192.168.2.0/24	192.168.3.11 (R1)
	Configure Static routes on dmz2 interface	10.2.2.0/24 192.168.5.0/24	192.168.4.11 (R2)

Question 1.2: Initializing the ASA2 firewall (5 points)

Initialize the ASA2 firewall, meeting all the following requirements:

- Configure the ASA2 firewall in single-routed mode, as shown in Figure 1-3.
- Configure hostname "ASA2" and enable password "cisco."
- Configure a redundant interface on ASA2 as shown in Tables 1-9 and 1-10. Ensure that interface Ethernet0/0 is the active member interface.
- Configure IP addresses and all other initialization parameters as shown in Tables 1-9 through 1-11.
- Configure static and default routes as shown in the tables. You can also refer to Figure 1-4 and Table 1-3 for more information.
- Ensure that OSPF and EIGRP adjacencies are established (as per Figure 1-4) after you complete the ASA2 initialization. R3, R4, and Sw2 have been preconfigured for IP routing.
- To perform basic verification using ping tests throughout this Practice Lab, you are allowed to permit **icmp any any** in your ACL on ASA2.
- Ensure that you can ping all the interfaces, including loopbacks on R3, R4, and Sw2 from ASA2.

TABLE 1-9 Redundant interface details

Interface	Member-Interface
Redundant 1	Ethernet0/0 (active)
Ethernet0/2	

TABLE 1-10 ASA2 initialization details

Interface	Nameif	Security Level	IP Address/Mask
Redundant 1	outside	0	192.168.9.10/24
Ethernet0/1	inside	100	192.168.10.10/24

TABLE 1-11 IP Routing initialization details

Interface	Route Type	Protocol	Network Prefix(es)	Other
Outside	Configure the default route on the outside interface	—	0.0.0.0/0	Next hop 192.168.9.4 (R4)
Outside	Configure dynamic routing on the outside interface	OSPF Process 1 Area 0	Advertise 192.168.9.0/24	Redistribute EIGRP AS 10 into OSPF Process 1
Inside	Configure dynamic routing on the inside interface	EIGRP AS 10	Advertise 192.168.10.0/24	Disable autosummary and redistribute OSPF Process 1 into EIGRP AS 10

Question 1.3: Secure IP routing (3 points)

Configure strong authentication for OSPF and EIGRP routing protocols using the information in Table 1-12. You can also refer to Figure 1-4.

- Ensure that OSPF and EIGRP adjacencies are established on all devices after you complete this task.
- Repeat all the pings from Question 1.2, and ensure that they are successful.

TABLE 1-12 IP routing authentication details

Device	Link Authentication	Interface	Protocol	Authentication
R3	192.168.9.0	GigabitEthernet0/1	OSPF Process 1	Strong authentication
R4	192.168.9.0	GigabitEthernet0/1		
ASA2	192.168.9.0	Redundant1		
Sw2	192.168.10.0	FastEthernet0/11	EIGRP AS 10	Strong authentication
ASA2	192.168.10.0	Ethernet0/1		

Question 1.4: Initializing IPS Sensor (4 points)

Initialize Cisco IPS Sensor, meeting all the following requirements:

- Configure the IPS sensor appliance in virtual sensor mode, as shown in Figure 1-3.
- Configure hostname "IPS," and allow Telnet sessions to the IPS sensor from VLAN 2.
- Configure the Command and Control (Management 0/0) interface IP address 192.168.2.12/24 with default gateway 192.168.2.11.
- Catalyst switches have been preconfigured for this question.
- Configure the integrated web server on the sensor appliance to accept HTTPS connections on port 8000 for managing the sensor. Users in VLAN 2 should be able to browse the IPS Device Manager (IDM) using https://192.168.2.12:8000 from their web browser.

- Configure the IPS sensor for inline VLAN pairing using the information in Table 1-13. Refer to Figure 1-3 for more information.
- You can also refer to Figure 1-1 for physical port connections.
- Verify that the virtual sensors are passing traffic. Ensure that you can ping all interfaces, including loopbacks of R1, R2, and Sw1 from R6.

TABLE 1-13 Inline VLAN pairing information

Sensor Placement Policy	Physical Interface	Inline VLAN Pair Number	Virtual Sensor Number	Assign Signature
Inline VLAN pair between ASA1 context abc1 and R6	GigabitEthernet0/0	Vlan1 = 101 Vlan2 = 102	vs0	sig0
Inline VLAN pair between ASA1 context abc2 and R6	GigabitEthernet0/1	Vlan1 = 201 Vlan2 = 202	vs2	sig2

Question 1.5: Configuring NTP (3 points)

Configure Network Time Protocol (NTP) on R1, R5, and ASA2 using the following information:

- Configure R1 as the NTP server using source Loopback0 and stratum 5.
- Configure strong authentication to protect NTP sessions between server and client using password "cisco."
- Configure ASA2 and R5 as NTP clients to synchronize its clock with R1.
- Configure access control on the R1 NTP server such that it allows full access from specific hosts ASA2 outside interface and R5 Loopback0 interfaces only. No other device should be able to sync clock with R1.
- Configure Sw2 to synchronize its clock with R5. Do not use any NTP server/peer commands on Sw2. There should be no NTP commands in global configuration mode on Sw2.

Section 2.0: Cisco Firewall (10 Points)

Question 2.1: Network Address Translation (NAT) (3 points)

Configure Network Address Translation (NAT) on ASA1 and ASA2, meeting all the following requirements:

- Do not enable NAT control on ASA1 and ASA2.
- Configure static identity NAT on ASA1/abc1 context for the web server (Sw1 Loopback1). Permit HTTP and HTTPS ports to allow connections from any host to this web server. Verify that you can establish a Telnet connection to this web server on HTTP and HTTPS ports from R6.
- Configure address translation on ASA1/abc2 context such that when R1 establishes a Telnet session to R6 Loopback0 using its source Loopback0, the source address gets translated to 192.168.6.61. However, when R1 establishes the same Telnet session to R6 Loopback0 without using its source Loopback0 (that is, using any other source), it should get translated to 192.168.6.62. Do not use a **static** NAT command to perform this task.
- Configure static NAT on ASA2 such that Sw2 can reach destination R6 Loopback0 interface using local address 192.168.10.6. Ensure that you can ping and telnet to R6 Loopback0 from Sw2 using IP address 192.168.10.6. Verify the connections table on ASA2 to confirm that your Telnet session to destination R6 Loopback0 (10.6.6.6) is translated to 192.168.10.6.

Question 2.2: High-availability (HA) default route (3 points)

Configure the high-availability (HA) default route on ASA2, meeting the following requirement:

- ASA2 has a default route configured to R4 Gig0/1 (192.168.9.4) in Question 1.2. Configure a backup default route to R3 Gig0/1 (192.168.9.3) such that it will be installed in the routing table of ASA2 only if Loopback0 on R4 (10.4.4.4) is unreachable. Ensure that the primary default route to 192.168.9.4 is preferred and always installed, unless 10.4.4.4 becomes unreachable by polling it every five seconds and sending three packets with each poll before declaring it unreachable. The backup default route should be installed only when 10.4.4.4 is unreachable.

Question 2.3: Cisco IOS Zone Based Policy Firewall (ZFW) (4 points)

Configure Cisco IOS Zone Based Policy Firewall (ZFW) on R5, meeting all the following requirements:

- Configure two zones and security policies for traffic traversing between zones, as shown in Tables 1-14 through 1-16.
- Ensure that you can ping and telnet 192.168.35.3 and .5 from R6.
- Ensure that you can ping and telnet 192.168.65.5 and .6 from R3.

TABLE 1-14 Zone initialization details

Zone Name	Zone Member Interface
CENTRAL	Serial0/0/1
REMOTE	Serial0/0/0

TABLE 1-15 Zone-pair information for traffic from the CENTRAL to REMOTE zone

Zone-Pair Name	Policy Name	Traffic	Action
central_remote	central_remote	All IP traffic	Inspect all IP traffic.

TABLE 1-16 Zone-pair information for traffic from the REMOTE to CENTRAL zone

Zone-Pair Name	Policy Name	Protocol	Traffic Actions
remote_central	remote_central	ICMP	Inspect ICMP protocol, and apply rate-limit policing to 20000 bps with a burst of 2000 bytes.
		HTTP	Inspect SMTP protocol, and reset connections that misuse the HTTP port for tunneling applications.
		SMTP	Inspect SMTP protocol, and drop (reset connections) emails from specific email sender joe@myemail.com, who is sending large file attachments of 10000000 bytes (10MB) and greater.
		Telnet and SSH	Inspect all Telnet and SSH sessions.

Section 3.0: Cisco VPN (16 Points)

Question 3.1: Configuring Cisco IOS CA server (3 points)

Configure a Cisco IOS Certificate Authority (CA) server on R1, meeting all the following requirements:

- Configure R1 as the Cisco IOS CA server using the information provided in the following **show** command output:

```
R1# show crypto pki server myCA
Certificate Server myCA:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=myCA.cisco.com
    CA cert fingerprint: DCB2B525 0E99785C 0770EE49 722BDB63
    Granting mode is: auto
    Last certificate issued serial number (hex): 1
    CA certificate expiration timer: 08:56:42 UTC Jun 8 2010
    CRL NextUpdate timer: 14:56:43 UTC Jun 8 2009
    Current primary storage dir: flash:
    Database Level: Complete - all issued certs written as <serialnum>.cer
```

- Configure the lifetime of the certificate server and the certificate issued by the server to one year.
- After the CA server is up, configure ASA2 and R5 as the CA clients, and obtain the certificates on both devices.

 Please see page 474 for more details.

Question 3.2: Configuring a LAN-to-LAN IPsec tunnel using digital certificates (4 points)

Configure a LAN-to-LAN (L2L) IPsec tunnel using certificates between ASA2 and R5, meeting all the following requirements:

- Configure the IPsec tunnel on ASA2 and R5, protecting host-to-host IPsec interesting traffic between Loopback0 of both Sw2 and R5.
- Use the certificates obtained in the preceding question to perform ISAKMP authentication.
- Configure ISAKMP profile configuration on R5, and associate this profile to the crypto map. Configure a certificate attribute map that performs two validation checks: the certificate issuer-name contains string "myCA," and the subject name contains string "ASA2." The ISAKMP authentication should fail if either condition is mismatched.
- Configure high-availability IPsec peering in such a way that it should continue to work if either WAN link on R5 (Serial0/0/0 or Serial0/0/1) goes down. You are not allowed to configure multiple crypto maps or multiple peer statements. Only one crypto map with one peer statement is allowed on both sides.

Question 3.3: Troubleshooting DMVPN (3 points)

Dynamic Multipoint VPN (DMVPN) has been preconfigured in this question. Your task is to troubleshoot and identify the injected faults and bring up the DMVPN tunnels, meeting all the following requirements:

- DMVPN is preconfigured between R1, R2, and R4 in a single DMVPN cloud with a static hub-to-spoke and dynamic spoke-to-spoke scenario. R1 is Hub1, with R2 and R4 being the spokes connecting to the hub.
- A single multipoint GRE (mGRE) tunnel interface is preconfigured on each router.
- Five faults are injected into your preconfiguration. Identify these faults, and verify that tunnels are established. Note that the faults injected could be either related to incorrect preconfiguration or missing commands to complete the configuration.

 Please see page 474 for more details.

- Open the ACL on the ASA1/abc2 context, allowing IPsec traffic entering the outside interface. This task excludes the five faults.
- Ensure that each spoke has a permanent IPsec tunnel to the hub. Also ensure that spoke-to-spoke tunnels will be established on demand when traffic between the spokes will traverse directly, bypassing the hub using the dynamically established spoke-to-spoke tunnel.
- While fixing this issue, you are allowed to alter the preconfiguration and add, modify, or remove part of the preconfiguration. However, you need to ensure that altering the preconfiguration does not impede any other question.
- For verification, perform the following ping test, and ensure that the following routing table outputs match your result:

```
R1# ping 22.22.22.22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 22.22.22.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms

R1# ping 44.44.44.44
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 44.44.44.44, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

R2# ping 44.44.44.44
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 44.44.44.44, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
```

```
R4# ping 22.22.22.22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 22.22.22.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1# show ip route eigrp 100
     22.0.0.0/24 is subnetted, 1 subnets
D       22.22.22.0 [90/2969600] via 172.1.0.2, 00:03:44, Tunnel1
     44.0.0.0/24 is subnetted, 1 subnets
D       44.44.44.0 [90/2969600] via 172.1.0.4, 00:03:44, Tunnel1

R2# show ip route eigrp 100
     11.0.0.0/32 is subnetted, 1 subnets
D       11.11.11.11 [90/2969600] via 172.1.0.1, 00:03:23, Tunnel1
     44.0.0.0/24 is subnetted, 1 subnets
D       44.44.44.0 [90/3251200] via 172.1.0.4, 00:03:23, Tunnel1

R4# show ip route eigrp 100
     22.0.0.0/24 is subnetted, 1 subnets
D       22.22.22.0 [90/3251200] via 172.1.0.2, 00:03:34, Tunnel1
     11.0.0.0/32 is subnetted, 1 subnets
D       11.11.11.11 [90/2969600] via 172.1.0.1, 00:03:34, Tunnel1
```

Question 3.4: Configuring Group Encrypted Transport VPN (GETVPN) (3 points)

Configure Group Encrypted Transport VPN (GETVPN) on R1, R3, and R6, meeting all the following requirements:

- Configure GETVPN using preshared keys on R1, R3, and R6 using the information in Tables 1-17 and 1-18.
- Use "cisco" for the preshared key on all devices.
- R1 will be the Key Server (KS), and R3 and R6 will be the Group Members (GM).
- Interface Loopback10 in subnet 172.17.0.0/16 has been preconfigured on R3 and R6 GMs.
- Use the information in the tables to complete this task.

TABLE 1-17 Configuration information for the key server (KS)

ISAKMP Policy	☐ Preshared key authentication ☐ Advanced Encryption Standard (AES) encryption algorithm ☐ Message Digest 5 (MD5) hash algorithm ☐ Diffie-Hellman group 2
IPsec Policy	☐ ESP transform using AES cipher ☐ ESP transform using HMAC-SHA authentication ☐ IPsec profile name = gdoi_profile ☐ Set IPsec SA lifetime to 10 hours
GDOI Parameters	☐ Group name = lab1getvpn ☐ Group identity number 123 ☐ Unicast Rekey transport with two retransmits at 30-second intervals ☐ Rekey lifetime to 24 hours ☐ Enable time-based antireplay check to 10 seconds
Access List Policies	☐ Traffic to be encrypted between 172.17.0.0/16 network address range to communicate using GETVPN

 Please see page 474 for more details.

TABLE 1-18 Configuration information for the group members (GM)

ISAKMP Policy	☐ Preshared key authentication ☐ AES encryption algorithm ☐ MD5 hash algorithm ☐ Diffie-Hellman group 2
GDOI Parameters	☐ Group name = lab1getvpn ☐ Group identity number 123 ☐ Key server IP address 192.168.3.11

Question 3.5: Configuring the remote-access VPN using Cisco AnyConnect (3 points)

Configure the remote-access VPN connection using the Cisco AnyConnect SSLVPN client, meeting all the following requirements:

- Configure the remote-access VPN on ASA2 using the information in Table 1-19.
- Establish a remote-access VPN connection to the ASA2 firewall from the host PC behind R2 in VLAN 5 (as shown in Figure 1-3) using Cisco AnyConnect SSLVPN client software.
- Use the information in the table to complete this task.

TABLE 1-19 Configuration information for ASA2

Policies for SSLVPN Connection	☐ Specify the group alias for this connection profile as "lab1." Allow the remote users to select a connection profile group identified by this alias, "lab1," on their login page and on their AnyConnect client connection panel. ☐ Configure a username "lab1user" and password "cisco." The user should be restricted to remote-access VPN sessions only; these cannot be used for Telnet/SSH/ASDM access to ASA2. ☐ IP pool range for VPN clients 192.168.111.1/24 through 192.168.111.50/24 ☐ Domain name cisco.com ☐ DNS server IP address 192.168.2.14

TABLE 1-19 *Continued*

VPN Test PC	☐ The VPN test PC is located in VLAN 5 behind R2 (refer to Figure 1-3). ☐ Assign IP address 192.168.5.10/24 to the Test PC with a gateway to 192.168.5.11. Ensure that you can ping your network, including the ASA2 outside interface. ☐ Verify the solution by establishing an SSLVPN connection using the Cisco AnyConnect client to ASA2.

Section 4.0: Cisco IPS (Intrusion Prevention System) (6 Points)

Question 4.1: Configuring IPS signatures (4 points)

Configure the Cisco IPS sensor appliance, meeting both of the following requirements:

- Configure signature tuning and custom signatures in both sig0 and sig2, which were applied to the virtual sensors earlier.
- Use the information in Table 1-20 to complete this task.

TABLE 1-20 IPS signature configuration information

Signature Definition	Tuning Signature	Custom Signature
sig0	Enable ICMP echo and ICMP echo reply signatures. Set the action to produce an alert for both signatures. Set the alert to medium level for both signatures.	Create custom Sig# **60000** named **kazaa** to drop all connections used by a custom peer-to-peer (P2P) networking application called Kazaa (case-insensitive) using UDP port 1214. Set its alert to high level and its fidelity rating 100.
sig2	Enable ICMP echo and ICMP echo reply signatures. Set the action to produce an alert for both signatures. Set the alert to medium level for both signatures.	Enable HTTP application policy enforcement, allowing a maximum of five HTTP requests to the server at any given time.

 Please see page 474 for more details.

Question 4.2: Configuring NTP on IPS Sensor (2 points)

To have an accurate timestamp on signature alerts and to have a consistent time source, configure NTP on the Cisco IPS sensor appliance, meeting all the following requirements:

- Configure the sensor to synchronize its clock with the NTP server on R1.
- Use the MD5 password "cisco."
- Ensure that the sensor clock has NTP as its time source.

Section 5.0: Implement Identity Authentication (12 Points)

Question 5.1: User-level access control (4 points)

Configure AAA authentication on Sw1 and Cisco Secure ACS server, meeting all the following requirements:

- Enable AAA authentication on Sw1 using TACACS+ protocol using the shared secret key "cisco." Do not use the default method list.
- Add Sw2 IP address 192.168.8.11 as the AAA client on the Cisco Secure ACS server (192.168.2.14) located in VLAN 2.
- Configure two new users on the Cisco Secure ACS server, "user1" and "user2," using the password "cisco" for both users. Both users must be assigned to the Default group.
- Configure user-level access restriction on the Cisco Secure ACS server to control network device access as follows. User1 should always be allowed access to Sw1 from any source IP address (within your network). However, user2 should only be allowed access to Sw1 from any Loopback0 (within your network) source IP address. Do not configure any settings within the user2 profile to complete the latter task.

- Do not use Network Access Filtering (NAF) or Network Access Restriction (NAR) from the Shared Profile components to complete this task.
- Verify the Failed Reports on the Cisco Secure ACS server to ensure that user2 is failing due to the user access filter implementation.
- Ensure that the console port is unaffected by this task.

Question 5.2: Role-based access control (4 points)

Configure role-based access control using AAA authentication on R2 and Cisco Secure ACS server, meeting all the following requirements:

- Enable AAA authentication on R2 using TACACS+ protocol using the shared secret key "cisco." Do not use the default method list.
- Add R2 IP address 192.168.4.11 as the AAA client on Cisco Secure ACS server (192.168.2.14) located in VLAN 2.
- Configure role-based CLI views using the information in Tables 1-21 and 1-22.
- Configure Cisco Secure ACS user profiles using the information in the tables.
- Verify functionality by establishing a Telnet session to R2, and ensure that both users get dynamic assignment from the AAA server to their respective user roles.
- Ensure that the console port is unaffected by this task.
- Use the information in the tables to complete this task.

TABLE 1-21 Role-based CLI configuration information on R2

Network Operator Role	☐ Configure a CLI view called "netop" with password "netop." ☐ Users in this view should be able to configure any dynamic routing protocols and static routes. ☐ Users should also be able to apply any interface specific commands. ☐ Users in this view should be able to execute any show commands.
Security Operator Role	☐ Configure a CLI view called "secop" with password "secop." ☐ Users in this view should be able to configure any VPN-related configuration (crypto), plus AAA, CBAC, and zone-based firewall configuration. ☐ Users should be able to configure any TACACS+ and RADIUS-related parameters. ☐ Users should be able to apply any interface-specific commands. ☐ Users in this view should be able to execute any show commands.

TABLE 1-22 Cisco Secure ACS server configuration information

Network Operator Role	☐ Configure a new user called "netop" with password "netop," and assign it to a group called "Role-Based CLI group." ☐ Upon successful authentication, this user should dynamically map to the Network Operator role CLI view configured on R2.
Security Operator Role	☐ Configure a new user called "secop" with password "secop," and assign it to a group called "Role-Based CLI group." ☐ Upon successful authentication, this user should dynamically map to the Security Operator role CLI view configured on R2.

Question 5.3: Port-based authentication (4 points)

Configure port-based authentication using 802.1x on Sw2, meeting all the following requirements:

- A wireless LAN access point (AP) not supporting 802.1x will be connected in the future to Sw2 FastEthernet0/7. Prepare to implement 802.1x-based authentication on Sw2 interface FastEthernet0/7 (with traffic in both directions) to authenticate all the wireless clients connected to the AP.

- Enable periodic reauthentication, set the guest VLAN assignment to VLAN 5, and set the maximum number of times that the switch sends an EAP-request to the client to three (assuming that no response is received) before restarting the authentication process.
- Ensure that the port is set to shut down in the event of a violation.
- Do not configure any AAA and RADIUS configuration on Sw2 yet. This will be done at a later stage, when AP is ready for deployment.

Section 6.0: Implement Control and Management Plane Security (12 Points)

Question 6.1: Control plane protection (4 points)

Configure Control Plane Policing (CoPP) on R2, meeting all the following requirements:

- Configure CoPP protection on R2, allowing ICMP pings sourced from the RFC 1918 address space only. Any ICMP packets sourced from nonprivate address space to R2 should be dropped.
- Do not configure any parameters under the default class that matches any packet.
- You are allowed to configure only one class-map and one policy-map to complete this task.

Question 6.2: Storm control protection (2 points)

Configure Storm Control Protection on Sw1, meeting all the following requirements:

- Configure Storm Control Protection on Sw1 interface FastEthernet0/13 to block all broadcast traffic using the following criteria.

 Please see page 474 for more details.

- Broadcast traffic should be blocked when the rising threshold reaches 80%, and traffic resumes forwarding when the falling threshold reaches 60% of the available bandwidth.
- Do not configure any ACL on interface FastEthernet0/13 to complete this task.

Question 6.3: Management plane protection (3 points)

Configure Management Plane Protection (MPP) on R2, meeting all the following requirements:

- Configure MPP on R4 to protect device access using the following criteria.
- Only Telnet protocol is allowed to access R4 through the Serial0/0/0 interface. However, both Telnet and HTTP protocols are allowed to access R4 through the GigabitEthernet0/1 interface.
- Do not configure any ACL to complete this task.

Question 6.4: Router system management (3 points)

Configure router system management parameters on R5, meeting all the following requirements:

- Configure R5 to generate a SYSLOG message when the CPU exceeds 75% within a 5-second window.
- Configure R5 to store all SYSLOG messages on the router buffer for all levels up to severity level 7.
- Additionally, configure R5 such that a network administrator can get a list of users currently using this router without having to console to it. The information displayed includes the processes running on the router, line number, connection name, idle time, and terminal location.

Section 7.0: Advanced Security (12 Points)

Question 7.1: Web server protection (4 points)

Configure web server protection on the ASA1/abc1 context, meeting all the following requirements:

- A web server (Sw1 Loopback1) is hosted behind the ASA1/abc1 context, which was configured for address translation in Question 2.1, with HTTP and HTTPS connections allowed from any host to this web server.
- The web server has limited resources. Therefore, configure the ASA1/abc1 context to protect this web server from TCP synchronization (SYN) flood denial-of-service (DoS) attacks by limiting the maximum number of TCP embryonic (half-open) connections to 50 (per protocol). Of these, only five can be from a single host at any given time.
- Do not change the static identity translation configured in Question 2.1 to complete this task.
- Do not use ACL to complete this task.
- Do not configure any parameters under the global default policy.

Question 7.2: Troubleshooting Cisco IOS NAT (3 points)

Network Address Translation (NAT) has been preconfigured on R5 in this question. Your task is to troubleshoot and identify the injected faults and ensure that NAT is functional, meeting all the following requirements:

- Cisco IOS NAT has been preconfigured on R5 in a multihomed scenario. R5 has two WAN uplinks (Serial0/0/0 and Serial0/0/1); assume that these are the two redundant ISP uplinks.
- A Loopback5 with IP address 10.55.55.55/32 has been preconfigured and advertised into OSPF Area 0.

- The NAT objective is to perform source address translation for Loopback5 to the respective egress WAN interface when the packet leaves this router (R5). For example, if R3 tries to ping Loopback5, the return packet should have a source address of Serial0/0/0. However, when R6 tries to ping the same Loopback5, the return packet should have a source address of Serial0/0/1.
- Three faults are injected into your preconfiguration. Identify these faults, and verify that NAT is functional as per the requirement. Note that the faults injected could be related to either incorrect preconfiguration or missing commands to complete the configuration.
- While fixing this issue, you are allowed to alter the preconfiguration and add to, modify, or remove part of the preconfiguration. However, you need to ensure that altering the preconfiguration does not impede any other question.
- For verification, perform the following ping test, and ensure that the inside global address in the NAT table from the following **show** output matches your result:

```
R3# ping 10.55.55.55
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.55.55.55, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R6# ping 10.55.55.55
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.55.55.55, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R5# show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
icmp 192.168.35.5:33   10.55.55.55:33     192.168.35.3:33    192.168.35.3:33
icmp 192.168.65.5:85   10.55.55.55:85     192.168.65.6:85    192.168.65.6:85
```

 Please see page 474 for more details.

Question 7.3: Configuring source IP address validation (2 points)

Configure source IP address validation on R6, meeting all the following requirements:

- Configure R6 WAN links to protect from forged (spoofed) IP source addresses by discarding IP packets that lack a verifiable source IP address. R6 should prevent any attack using spoofing techniques by forwarding only packets that have source addresses that are valid and found in the IP routing table.
- The solution should check the source addresses of each ingress packet without regard for the specific interface on which it was received, as long as it has a valid route found in the IP routing table.
- Do not configure ACL to complete this task.

Question 7.4: Spanning-Tree Protocol protection (3 points)

Configure spanning-tree protection on Sw1, meeting all the following requirements:

- Configure Sw1 globally to enable the Port Fast feature on all nontrunking interfaces (all access ports) by default.
- Configure Sw1 to prevent any interface that is Port Fast-enabled from participating in the spanning tree. If Sw1 receives a bridge protocol data unit (BPDU) packet on any interface that is in Port Fast operational state, it should put the interface in the error-disabled state when it receives a BPDU.
- Ensure that Sw1 will put the interface back in service automatically after 60 seconds, only (conditionally) if this interface was put in the error-disabled state due to a BPDU issued explicitly, and not others.
- Additionally, configure Sw1 globally to prevent alternate and root ports from becoming designated ports (DP) because of a failure that leads to a unidirectional link.

Section 8.0: Network Attacks (12 Points)

Question 8.1: Filtering instant messaging (3 points)

Configure Instant Messaging (IM) filtering on the ASA1/abc2 context, meeting all the following requirements:

- An end user of the MSN Instant Messaging (IM) application is transferring infected files over the application, propagating a worm that exploits a known vulnerability, thus causing a threat to the corporate network. The end user's MSN login ID is yusuf@hotmail.com.
- Configure the ASA1/abc2 context to drop all connections that explicitly match the parameters. All other normal MSN services, such as regular chat services, except file transferring, should continue to work for the user.
- All other end users should be unaffected by this task, and their MSN services should continue to work, including file transferring.
- Do not use ACL to complete this task.
- The solution must be applied to the global default policy.

Question 8.2: Preventing unauthorized connections (2 points)

Configure the ASA1/abc1 context to prevent unauthorized connections, meeting all the following requirements:

- Configure the ASA1/abc1 context to send TCP resets (the TCP RST flag in the TCP header) to the denied host for any inbound TCP sessions that are denied by the firewall.
- In addition, configure the ASA1/abc1 context to disable the proxy ARP function and stop responding to any ARP request with its own MAC address, thus limiting exposure of its MAC address.
- Do not use ACL to complete this task.

 Please see page 474 for more details.

Question 8.3: Restricting unauthorized access (4 points)

Configure R1 to restrict unauthorized TCP connections, meeting all the following requirements:

- An intruder has gained illegitimate access to some of the devices in your network, has established a Telnet session to the R1 Loopback0 IP address, and is making unauthorized changes to the router configuration.
- Configure R1 to prevent the unauthorized TCP session by matching explicit parameters, thus restricting any source from being able to establish a Telnet session to the R1 Loopback0 IP address.
- Apply the solution to the R1 control plane.
- Ensure that you open the ACL on the ASA1/abc2 context, permitting any source to any destination on TCP port 23, thus ensuring that your solution is responsible for blocking the Telnet session, and not the ASA/abc2 context.
- Do not use ACL to complete this task.
- Do not use ZFW or CBAC to complete this task.
- Verify functionality by establishing a Telnet session from any device in your network to the R1 Loopback 0 IP address. Telnet session to R1 Loopback 0 IP address should fail to connect. However, establishing Telnet session to any other IP address on R1 should be successful (as shown in verification section below).

Question 8.4: ARP spoofing attack (3 points)

Configure Sw2 to protect against ARP spoofing attacks, meeting all the following requirements:

- An intruder is attempting to poison ARP table entries of critical devices in VLAN 50.
- Configure a countermeasure on Sw2 to protect against ARP spoofing attacks. Check the source MAC addresses and IP address fields of all ARP entering packets to see if the ARP requester is valid in the snooping binding. If it isn't, traffic should be blocked.
- Additionally, configure rate limiting for all incoming ARP packets to 10 packets per second.
- The DHCP server resides on Sw2 interface FastEthernet0/15. Ensure that this port is the trusted port to reply to DHCP requests on the network.

Ask the Proctor

This section provides basic questions and answers. You can use it if you need any clarification to complete the Practice Lab questions. In the real CCIE lab, the proctor will not discuss with you the questions or solutions, except for basic clarifications. The proctor will be present only to ensure that you do not have problems with the lab environment and to maintain the timing element of the lab exam.

Section 1.0: Core Configuration (20 Points)

Question 1.1: Initializing the ASA1 firewall (5 points)

Question: Do I have to be exact in naming the interfaces, such as Inside versus inside versus INSIDE?

Answer: Yes. You have to use exact names and numbers, as mentioned in the question. Context names also are case-sensitive, so use the exact names mentioned in the tables.

Question: Can I add static routes on the ASA1 firewall?

Answer: Yes, you can add static and default routes as required throughout this Practice Lab unless restricted explicitly.

Question: Why is my Interface Management0/0 showing down?

Answer: The Management0/0 interface is physically not connected and will remain down; ignore it.

Question: Do I need to configure the VLANs on Catalyst Switches?

Answer: Only if required. All VLAN information has been preconfigured in the initial configuration provided. However, if there is a scenario where you feel you want to modify the VLAN information, you are allowed to do so.

Question 1.2: Initializing the ASA2 firewall (5 points)

Question: Do I have to be exact in naming the interfaces, such as Inside versus inside versus INSIDE?

Answer: Yes. You have to use exact names and numbers, as mentioned in the question. Context names are also case-sensitive, so use the exact names mentioned in the tables.

Question: Can I add static routes on the ASA2 firewall?

Answer: Yes, you can add static and default routes as required throughout this Practice Lab unless restricted explicitly.

Question: Which VLAN must the two physical interfaces be in for redundant interface 1?

Answer: The two physical member interfaces Ethernet0/0 and Ethernet0/2 must be in VLAN 9, as shown in Table 1-2.

Question: Do I need to create subinterfaces for the redundant interface?

Answer: No, do not create subinterfaces. Configure an IP address and other basic initialization parameters under the Redundant 1 logical interface.

Question: What metric should I use when redistributing on ASA2 between OSPF and EIGRP?

Answer: You can use any metric.

Question 1.3: Secure IP routing (3 points)

Question: What password string should I use?

Answer: Use password “cisco.” The general guidelines clearly state that you must use “cisco” as the password for any authentication string, enable-password, and TACACS+/RADIUS key or for any other purpose during this Practice Lab.

 Please see page 474 for more details.

Question: The table says to enable authentication on the physical interface of R3, R4, and Sw2. Do I need to enable it on loopback interfaces as well?

Answer: No. Enable only the authentication shown in the table.

Question: What happens if I can't get the authentication to work? Will I lose points from Question 1.2 as well?

Answer: If you are unable to get authentication working, I advise you to skip this question and move to next one. In this case, you will not lose points for Question 1.2, because they are not interconnected if not attempted. However, if you attempt to configure Question 1.3, and it fails to work, you will lose points on both Questions 1.2 and 1.3.

Question: How do I determine if the question requires MD5 or clear-text authentication?

Answer: The question offers a hint by using the term "strong" authentication, which implies a strict type of authentication mechanism. Often, strong authentication is associated with two-factor or multifactor authentication. However, in this case, the choice is between clear-text and the MD5 type only, which is why you must choose MD5 authentication. If you configure clear-text, the solution is considered incorrect.

Question 1.4: Initializing IPS Sensor (4 points)

Question: Do I need to permit all hosts in VLAN 2 or specific hosts in VLAN 2?

Answer: Permitting all hosts in VLAN 2 means any host. Permit the /24 subnet in your sensor ACL.

Question: What subinterface number should I use when configuring inline VLAN pairs?

Answer: The default range is 1 to 255, and you can use any number. Usually candidates use the first logical number available—1.

Question: What are the default username and password for sensor console login?

Answer: The default username and password are usually "cisco" (without the quotation marks). However, the default password may have been reset and can be different. Generally, the password is set to "cisco" or "123cisco123" or "cisco123," to name few.

Question 1.5: Configuring NTP (3 points)

Question: What number should I use for the authentication key and trusted key?

Answer: The default range is 1 to 4294967295, and you can use any number. Usually candidates use the first logical number available—1.

Question: Do I need to permit NTP (UDP port 123) for any hosts in the ACL on the ASA1/abc2 context or specific hosts?

Answer: Because the question does not restrict or mention anything about this ACL, you can permit UDP port 123 from any source to any destination. However, as a best practice, I recommend that you write a specific ACL, because you know the source and destination IP address in this task. Again, this is just a recommendation, not a requirement.

Question: Can I use the **broadcast** command or any NTP-related commands in interface configuration mode on R5 and Sw2?

Answer: Yes, you can enter NTP-related commands in interface configuration mode, because the question disallows entering commands in global configuration mode.

Section 2.0: Cisco Firewall (10 Points)

Question 2.1: Network Address Translation (NAT) (3 points)

Question: Can I enable NAT control for testing on ASA1 or ASA2?

Answer: The requirement is clear: do not enable NAT control. However, if you want to test some functionality, you can enable it, but be sure to disable it before completing this task.

Question: If I miss one small requirement, will I get partial credit?

Answer: All three requirements must be met to earn the points. There is no partial credit on the CCIE lab exam.

Question: Do I need to allow HTTP and HTTPS ports from a specific host/destination for the first task?

Answer: You are allowed to permit connections from any host to the web server on Sw1.

Question: The third task says not to use a **static** command. Does this mean the use of the **static** command or NAT translation in general?

Answer: It means the **static** NAT command from a syntax perspective.

Question: For the third task, are you saying to configure address translation for the destination IP address?

Answer: Yes.

Question: Do I need to permit return traffic on the outside interface for the second and third tasks?

Answer: There is no need to configure ACL, because traffic is traversing from a higher-security (inside) interface to a lower-security (outside) interface.

Question 2.2: High-availability (HA) default route (3 points)

Question: What monitor ID number should I use when configuring the SLA monitoring process on ASA2?

Answer: The default range is 1 to 2147483647, and you can use any number. Usually candidates use the first logical number available—1—or sometimes 123, whichever is more convenient.

Question: What tracking ID number should I use when configuring the route tracking object on ASA2?

Answer: The default range is 1 to 500, and you can use any number. Usually candidates use the first logical number available—1.

Question: Can I configure or tune my dynamic routing protocol to control the default route injection when the primary default route fails on ASA2?

Answer: No. The question explicitly requires configuring a static backup default route.

Question: What administrative distance should I use for the secondary (backup) default route?

Answer: You can use any administrative distance number that is higher than the primary default route's administrative distance.

Question: Is there an alternative solution if I do not use the SLA monitoring and route tracking feature?

Answer: Not that I can think of.

Question: What monitoring protocol do I use for tracking the target network?

Answer: The only option available on the Cisco ASA firewall to track route objects is using ipIcmpEcho (ICMP echo protocol). There is no other option.

Question 2.3: Cisco IOS Zone Based Policy Firewall (ZFW) (4 points)

Question: The question says to use specific zone, zone-pair, and policy-map names. What about the class-map names?

Answer: If not specified, you can use any naming convention to complete the configuration task.

Question: How many class-maps and policy-maps are required to be configured?

Answer: Careful planning is required for the number of class-maps and policy-maps required to fulfill all the requirements. The best approach is to take each protocol and draft its own class-map matching the protocol and policy-map, applying inspection and any other action (optional) required to apply this traffic.

Question: Can I configure additional class-maps, policy-maps, or ACLs to complete the task?

Answer: Yes, you can configure any number of class-maps, policy-maps, or any other configuration as long as it is directly related to completing this task.

Question: Can I configure **parameter-map** to complete this task?

Answer: Yes, some parts of the question may require configuring **parameter-map** for deep packet inspection, pattern matching regex, or other advanced filters.

Question: When matching protocols for inspection in **class-map**, can I use match protocol or match using ACL?

Answer: If not mentioned, you can use any method. However, best practice is to use match protocol, because it covers all variations of the specific protocol inspection and also allows deep packet inspection parameters. On some occasions, you may have to use both to fulfill all the criteria.

Question: When configuring rate-limit, can I round the KB and MB parameters to 1000 instead of 1024?

Answer: Yes, you can use rounding to 1000. For example, 1 MB = 1000 KB, and 1 KB = 1000 bytes.

Section 3.0: Cisco VPN (16 Points)

Question 3.1: Configuring Cisco IOS CA server (3 points)

Question: Do I have to be exact in naming the server?

Answer: Yes. You must use the exact names shown in the output; they are case-sensitive.

 Please see page 474 for more details.

Question: What name should I use to configure the trustpoint?

Answer: If not mentioned in the question requirement, you can use any name. Candidates generally use "cisco" because it is easy to remember.

Question: What if I am unable to get the CA server working or clients authenticating with the server?

Answer: You will lose points for this question and the later question that is linked with the CA server.

Question: Do I need to be explicit when opening ACL on the ASA1/abc2 context for CA enrollment traffic or any host?

Answer: Because the question does not restrict or mention anything about this ACL, you can permit from any source to any destination. However, as a best practice, I recommend that you write a specific ACL, because you know the source and destination IP address in this task. Again, this is just a recommendation, not a requirement.

Question 3.2: Configuring a LAN-to-LAN IPsec tunnel using digital certificates (4 points)

Question: What name should I use for configuring the crypto map, transform set, trustpoint, and so on?

Answer: If not mentioned in the question requirement, you can use any name. Candidates generally use "cisco" because it is easy to remember.

Question: For the high-availability function, can I create a new loopback interface on R5? If so, what IP address subnet should I use?

Answer: Yes, you can configure a new Loopback1 interface on R5 (for peering) using any IP address and advertise this Loopback1 into OSPF area 0 so that it is routable throughout the network. Ensure that ASA2 can ping this Loopback1 address.

Question: If my certificates are not populated and are having trouble with the CA, can I skip the certificate part and configure this task using the preshared key?

Answer: No. You will lose points, because the question clearly requires configuring this task using certificates.

Question: When I initiate a ping test to bring up the tunnel, usually I lose one or two pings when the tunnel is establishing, so the success rate is not always 100%. Is that OK, or will the proctor check for 100%?

Answer: The success rate can be any percentage greater than 0, as long as the ping works.

Question: This question seems long and has a lot of requirements. If I skip some of them, will I get partial credit?

Answer: No. The CCIE lab exam has no concept of partial credit. If you miss any item, you lose all points. The grading system is all or none.

Question 3.3: Troubleshooting DMVPN (3 points)

Question: Can you clarify the nature of injected faults?

Answer: Faults can be on any device within the DMVPN configuration or within the network topology around it. They also could be related to any of the non-VPN technologies, such as switching, routing, WAN link, IOS features, NAT, and ACL filtering, to name few. Secondly, faults injected could be related to either incorrect preconfiguration or missing commands to complete the configuration.

Question: Must I find the injected faults, or can I delete all DMVPN configurations and start fresh?

Answer: You cannot remove the DMVPN preconfiguration and start over. The faults injected must be found within the existing preconfiguration.

Question: If I can't find all the faults, do I get partial credit for the ones I found?

Answer: All faults must be found to earn the total points. The CCIE lab exam offers no partial credit.

Question: Are all the faults on one device, or are they spread across multiple devices?

Answer: Faults are injected on multiple devices across the topology to create a more challenging scenario.

Question: Are all the faults related to DMVPN configuration only?

Answer: No. As mentioned earlier, faults can be anywhere within the DMVPN configuration or within the network topology around it. Faults also could be related to any of the non-VPN technologies.

Question: Do I need to be explicit when opening ACL on the ASA1/abc2 context for DMVPN traffic?

Answer: Because the question does not restrict or mention anything about this ACL, you can permit from any source to any destination. However, as a best practice, I recommend that you write a specific ACL, because you know the source and destination IP address in this task. Again, this is just a recommendation, not a requirement.

Question 3.4: Configuring Group Encrypted Transport VPN (GETVPN) (3 points)

Question: Do I need to be explicit when opening the ACL on the ASA1/abc2 context for GETVPN traffic?

Answer: Because the question does not restrict or mention anything about this ACL, you can permit from any source to any destination. However, as a best practice, I recommend that you write a specific ACL, because you know the source and destination IP address in this task. Again, this is just a recommendation, not a requirement.

Question: What protocol and port number does the GETVPN traffic use during the Group Domain of Interpretation (GDOI) registration process?

Answer: GDOI uses User Datagram Protocol (UDP) port number 848 to establish its IKE sessions between the key server and the group members.

Question: Do I need to configure a host-specific preshared key or for any host using 0.0.0.0/0?

Answer: Because the question does not clearly mention anything about this, you can use any host key 0.0.0.0/0. However, from a GDOI protocol requirement perspective, a preshared key is required on each GM to authenticate the KS only. You are not required to define a preshared key on a GM to authenticate other GMs.

Question 3.5: Configuring the remote-access VPN Using Cisco AnyConnect (3 points)

Question: Do I need to preinstall the Cisco AnyConnect VPN client software on the remote PC?

Answer: It is not compulsory. You have two options. Either preinstall the Cisco AnyConnect VPN client on the test PC, or dynamically install it during your connection to ASA2. If you choose the latter, you must have the appropriate package file flashed on ASA2 (review the following flash output). When you use a web browser to browse using HTTPS to the ASA2 outside interface IP address, the firewall automatically deploys the Cisco AnyConnect VPN client to the remote host upon successful login.

```
ASA2# show flash:
--#--  --length--  -----date/time------  path
   75  4096        Jan 18 2009 20:03:48  log
  142  14137344    Jan 08 2009 02:11:08  asa804-k8.bin
   79  4096        Jan 08 2009 02:16:18  crypto_archive
  147  3032497     Jun 11 2009 06:29:46  anyconnect-win-2.3.0254-k9.pkg
62947328 bytes total (45387776 bytes free)
```

Question: What naming convention should I use for configuring SSLVPN tunnel, groups, pool, and other SSLVPN-related configuration?

Answer: Because the question does not restrict or mention anything about this, you can use any naming convention convenient for you.

Question: Will I have similar access to a test PC for verifying remote connections in the real lab?

Answer: Yes. The CCIE lab exam uses a similar test PC with preinstalled client software required for verification. You will have full access to it.

Section 4.0: Cisco IPS (Intrusion Prevention System) (6 Points)

Question 4.1: Configuring IPS signatures (4 points)

Question: What is the signature ID number for ICMP echo request and echo reply packets?

Answer: ICMP echo request is sig ID 2000, and echo reply is 2004. You need to know some of the common built-in signature ID numbers on the IPS sensor appliance.

Question: How do I verify the functionality of this task?

Answer: You cannot verify the functionality of this custom signature, because no live traffic is traversing the sensor, which can trigger the alert. However, on other occasions, you may be able to verify some custom signatures.

Question 4.2: Configuring NTP on IPS Sensor (2 points)

Question: After configuring the NTP on IPS sensor, I am still seeing the dot before the timestamp.

Answer: After you configure NTP on the sensor, the display on **show clock detail** keeps showing a dot before the timestamp, indicating NTP synchronization is in progress. This may take some time.

Question: The IPS management interface and R1 NTP server are both in the same VLAN 2. Do I still need to configure the NTP ACL on R1?

Answer: Yes. Opening the NTP ACL is still required. You need to open the ACL on NTP server R1 to allow NTP connections from the sensor.

 Please see page 474 for more details.

Section 5.0: Implement Identity Authentication (12 Points)

Question 5.1: User-level access control (4 points)

Question: The question says not to use the default method list. How many named method lists can be used?

Answer: It does not matter how many, as long as you fulfill the requirement. However, two named methods should do and will fulfill all the requirements.

Question: Do I need to configure an explicit named method list for console line authentication?

Answer: Yes. Because the question clearly says "Ensure that the console port is unaffected by this task," this must be fulfilled by configuring a separate named method list with **none** to exempt the console line from any form of authentication. This also protects you from locking out of the router because of any unforeseen errors during the configuration.

Question: What name should be used when configuring the named method list?

Answer: Because the question does not restrict or mention anything about this, you can use any naming convention convenient to you.

Question: Do I need to be explicit when opening the ACL on the ASA1/abc1 context for Telnet sessions (TCP/23)?

Answer: Because the question does not restrict or mention anything about this ACL, you can permit from any source to any destination. However, as a best practice, I recommend that you write the best possible specific ACL, because you know the destination IP address in this task. Permit any source IP address to destination Sw1 192.168.8.11 on TCP port 23. Again, this is just a recommendation, not a requirement.

Question: The question says that both users must be assigned to the Default group. Can they be in any group, as long as they are in the same group, or must I use the built-in Default group?

Answer: Both users must be in the system Default group.

 Please see page 474 for more details.

Question: When I browse the User Setup in Cisco Secure ACS, I am unable to see the user-level Network Access Restriction (NAR) option.

Answer: To enable the user-level NAR option, go to the Interface Configuration menu and select Advanced Options. Then select the checkbox User-Level Network Access Restrictions.

Question 5.2: Role-based access control (4 points)

Question: The question says not to use the default method list. How many named method lists can be used?

Answer: It does not matter how many, as long as you fulfill the requirement. However, two named methods should do and will fulfill all the requirements.

Question: Do I need to configure an explicit named method list for console line authentication?

Answer: Yes. Because the question clearly says "Ensure that the console port is unaffected by this task," this must be fulfilled by configuring a separate named method list with **none** to exempt the console line from any form of authentication. This also protects you from locking out of the router because of any unforeseen errors during the configuration.

Question: What name should I use when configuring the named method list?

Answer: Because the question does not restrict or mention anything about this, you can use any naming convention convenient to you.

Question: Do I need to be explicit when opening the ACL on the ASA1/abc2 context for Telnet sessions (TCP/23)?

Answer: Because the question does not restrict or mention anything about this ACL, you can permit from any source to any destination. However, as a best practice, I recommend that you write the best possible specific ACL, because you know the destination IP address in this task. Permit any source IP address to destination R2 192.168.4.11 on TCP port 23. Again, this is just a recommendation, not a requirement.

Question: Do I need to be explicit when opening the ACL on the ASA1/abc2 context for TACACS+ sessions (TCP/49)?

Answer: Because the question does not restrict or mention anything about this ACL, you can permit from any source to any destination. However, as a best practice, I recommend that you write the best possible specific ACL, because you know the source and destination IP address in this task. Permit any source R2 (192.168.4.11) to destination Cisco Secure ACS server (192.168.2.14) on TCP port 49. Again, this is just a recommendation, not a requirement.

Question: When I browse the User Setup in Cisco Secure ACS, I am unable to see the custom TACACS+ attribute option.

Answer: By default, the TACACS+ custom attribute box under the User setup is not visible. Figure 1-13 shows how to enable it from TACACS+ (Cisco IOS) on the Interface Configuration menu on Cisco Secure ACS server. Select the checkbox Display a window for each service selected in which you can enter customized TACACS+ attributes.

Question 5.3: Port-based authentication (4 points)

Question: The question requires configuring 802.1x on Sw2 Fa0/7, but my switch shows the interface is down/down.

Answer: The interface is down/down because nothing is connected yet. A wireless LAN access point (AP) will be connected to this port in the future.

Question: What is the IP address of the RADIUS server?

Answer: The question clearly states that there is no need to configure AAA and RADIUS-related configuration at this point, because the access point (AP) is not ready for deployment yet. At this point, you are only required to configure the switch port, in preparation for the AP deployment.

Section 6.0: Implement Control and Management Plane Security (12 Points)

Question 6.1: Control plane protection (4 points)

Question: What naming convention do I use when configuring **class-map** and **policy-map**?

Answer: Because the question does not restrict or mention anything about this, you can use any naming convention convenient to you.

Question: Can I use a named ACL or numbered only?

Answer: Because the question does not restrict or mention anything about this, you can use either a named or numbered ACL.

Question: The question says to use only one class-map and policy-map. Can I use multiple ACLs within one class-map?

Answer: Yes. This is allowed and is the required solution.

Question 6.2: Storm control protection (2 points)

Question: Can I configure a service policy to complete this task?

Answer: No. Only storm-control broadcast configuration is allowed.

Question 6.3: Management plane protection (3 points)

Question: Can I configure an ACL on VTY lines?

Answer: No. The question clearly says not to use any type of ACL to complete this task.

Question: Can I modify the protocol list under VTY lines to allow or disallow Telnet sessions?

Answer: You can. However, this will not fulfill the requirement of restricting the protocol for traffic arriving on a particular interface. Only MPP supports this function.

Question 6.4: Router system management (3 points)

Question: When configuring CPU thresholds, do I need to configure both process and total type levels?

Answer: No. Only the total type level is required.

Question: Do I need to disable the automatic CPUhog profiling that is enabled by default?

Answer: No. Do not change the default settings.

Question: Should I enable SYSLOG messaging to a specific server for all notifications?

Answer: Because the question does not specify any IP address for the SYSLOG server, it is not required. You only need to enable buffer logging on the router system.

Section 7.0: Advanced Security (12 Points)

Question 7.1: Web server protection (4 points)

Question: How do I know if Modular Policy Framework (MPF) is the only solution to this question?

Answer: This question can be configured using various methods, such as the **static** command or ACL. However, because the question clearly restricts their use, the only option available is using MPF. Another important differentiator is the requirement to set the per-host embryonic limit to 5. This can only be achieved using MPF. The **static** command syntax can only set the total maximum limit of embryonic connections, not per-host.

Question: Can I apply the policy to the inside interface?

Answer: No. The question requires protecting the web server from traffic entering the firewall. Therefore, the best scenario is protecting at the ingress point on the outside interface.

Question: How can I validate the functionality of this question?

Answer: You can use the **show service-policy flow** command to validate the policy configuration for any specific type of traffic flow. This command verifies the policy trigger without your having to send real-time traffic through the firewall to test your policy.

Question 7.2: Troubleshooting Cisco IOS NAT (3 points)

Question: If I can't find all the faults, do I get partial credit for the ones I found?

Answer: You must find all the faults to earn the total points. The CCIE lab exam offers no partial credit.

Question: Are all the faults on one device, or are they spread across multiple devices?

Answer: Faults are injected on multiple devices across the topology to create a more challenging scenario.

Question: Are all the faults related to NAT related to configuration only?

Answer: No. As mentioned earlier, faults can be anywhere within the NAT configuration or within the network topology around it. Faults could also be related to any of the non-NAT technologies.

Question: Can I create a new ACL for NAT configuration?

Answer: Yes. However, NAT ACL number 102 has been preconfigured and has been referenced in the **route-map**. You can either remove and re-create ACL number 102 or create a new ACL number and change the respective reference in **route-map**, whichever works for you.

Question 7.3: Configuring source IP address validation (2 points)

Question: Can I configure an IP source tracking solution?

Answer: No. This will not fulfill the question's requirements. The question clearly states that the solution should use the routing table for source IP address validation.

Question: Do I need to configure ACL with a Unicast Reverse Path Forwarding (uRPF) solution?

Answer: No. The question does not require it.

Question: If I apply the uRPF solution on one WAN interface only, will I get credit?

Answer: The question clearly requires protection for both WAN links. Configuring one WAN link is considered incomplete, and you will lose all points. No partial credit is given.

Question 7.4: Spanning-Tree Protocol protection (3 points)

Question: Can I configure all interfaces in Port Fast using the **interface range** command?

Answer: No. The question requires enabling Port Fast globally using global configuration mode.

Question: Is it OK to set the BPDU Guard and Loop Guard on each interface?

Answer: No. Your solution should not be interface-specific. The question requires enabling this using global configuration mode.

Section 8.0: Network Attacks (12 Points)

Question 8.1: Filtering instant messaging (3 points)

Question: Can I configure multiple **class-map**s and/or **policy-map**s to complete this task?

Answer: Yes. Because the question does not restrict this, you can configure any number of these as long as you fulfill the criteria.

Question: What naming convention should I use for the **class-map** and **policy-map** configuration?

Answer: Because the question does not restrict or mention anything about this, you can use any naming convention convenient to you.

Question: Can I use protocol and port numbers to match the MSN Instant Messaging application within the **class-map**?

Answer: You could, but the question requires deep packet inspection. Also, a built-in Instant Messaging inspection engine can be used to match MSN and Yahoo-based Instant Messaging services on the Cisco ASA firewall. Another concern is that MSN port numbers can change in different versions or future releases. Therefore, it is safe to use the inspection engine instead, which does not rely on port numbers.

Question: For the **drop-connection** action parameter within the policy-map, can I configure **reset** instead?

Answer: Yes, but note that the **drop-connection** action closes the connection and the **reset** action closes the connection and sends a TCP reset to the client. Because the question does not mention anything about the **reset** function, the best choice is to select the **drop-connection** action.

Question 8.2: Preventing unauthorized connections (2 points)

Question: Is the ACL allowed to match in the class-map and be used in the service-policy?

Answer: The question clearly states not to use ACL in any fashion to complete this task.

Question: Do I need to reset TCP connections in both directions?

Answer: The question requires sending a TCP reset to any unauthorized inbound connections entering the firewall.

Question: When disabling Proxy ARP on the firewall, do I need to create static ARP entries for connected devices?

Answer: This isn't required. Proxy ARP does not affect these.

Question 8.3: Restricting unauthorized access (4 points)

Question: Can I use an ACL to match the traffic in the class-map within the Flexible Packet Matching (FPM) solution?

Answer: The question clearly says not to use ACL in any fashion to complete this task.

Question: What naming convention should I use for the **class-map** and **policy-map** configuration?

Answer: Because the question does not restrict or mention anything about this, you can use any naming convention convenient to you.

Question: When trying to configure the stack type and access-control type **class-map**, I am unable to see the FPM options. Am I missing something?

Answer: Before you can configure FPM, you need to load the Protocol Header Definition File (PHDF) files into the router flash and enable it from global configuration mode. FPM provides ready-made definitions for these standard protocols (IP, TCP, UDP, ICMP), which can be loaded onto the router with the **load protocol** command: ip.phdf, tcp.phdf, udp.phdf, and icmp.phdf. Ensure that the files are in the flash, and then enable them as shown here:

```
R1# config term
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# load protocol flash:ip.phdf
R1(config)# load protocol flash:tcp.phdf
```

 Please see page 474 for more details.

Question 8.4: ARP spoofing attack (3 points)

Question: Do I need to configure DHCP Snooping feature on the switch to complete this task?

Answer: Yes, DHCP Snooping feature must be enabled as it is a prerequisite for DAI functionality to work and DAI depends on the snooping binding table which is built and populated dynamically when DHCP snooping feature is enabled. You can also populate static entries into this table.

Question: The question requires configuring DAI on Sw2 Fa0/15; however, my switch shows interface is down/down?

Answer: Yes, interface is down/down as there is nothing connected yet. A DHCP server will be connected to this port in the future.

Lab Debrief

As mentioned in the Overview, this section is primarily important when verifying the outcome and functionality of the Practice Lab questions. You can use this section primarily to understand how to verify and compare your work. This section also provided some useful hints needed to complete the respective exercises. Sometimes, it is easy to misinterpret the question requirements having integral and complex elements.

This section shows outputs using the most common **show** and **debug** command(s) used for verification and troubleshooting. Analyze and study these outputs carefully.

The following outputs also have some important parts highlighted that require your attention. Focus on those highlights, and match your outputs to ensure absolute accuracy.

This section analyzes each question, showing you what was required and how to achieve the desired results. Each question also highlights the skills tested in each question. You should use this section to produce an overall score for your test.

Section 1.0: Core Configuration (20 Points)

Question 1.1: Initializing the ASA1 firewall (5 points)

Initialize the ASA1 firewall, meeting all the following requirements:

- Configure the ASA1 firewall in multicontext routed mode, as shown in Figure 1-3.
- Configure hostname “ASA1” and enable password “cisco.”
- Create three contexts, as shown in Tables 1-4 through 1-8.
- Context names are case-sensitive. Use exact names and numbers, as shown in the tables.
- Assign context “admin” as the admin-context.

- Assign interfaces as shown in the tables. Map physical interface names to logical names.
- Configure IP addresses and all other initialization parameters as shown in the tables.
- Configure static and default routes within context as shown in the tables. You can also refer to Figure 1-4 and Table 1-3 for more information.
- To perform basic verification using ping tests throughout this Practice Lab, you are allowed to permit **icmp any any** in your ACL in both contexts on ASA1.
- Ensure that you can ping all the interfaces, including loopbacks on Sw1 from context abc1.
- Ensure that you can ping all the interfaces, including loopbacks on R1 and R2 from context abc2.

Skills tested

- ☐ Initializing the Cisco ASA1 firewall in multicontext mode
- ☐ Configuring basic IP address and IP routing initialization tasks

Functionality and solution verification

- ☐ This question is one of the core configuration tasks. You need to be very careful when attempting this question. If you get even one item wrong, it can potentially impede a lot of other questions and functionality for later questions.
- ☐ It is strongly recommended that you practice the ASA multicontext configuration during your study sessions several times to ensure perfection and accuracy in this area.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

Check that the hostname is ASA1:

```
ASA1# show run hostname
hostname ASA1
```

Check if the ASA1 is configured in multicontext mode:

```
ASA1# show mode
Security context mode: multiple
```

Check if the ASA1 is configured in routed mode:

```
ASA1# show firewall
Firewall mode: Router
```

Check the context details and interface allocations for each context on ASA1. Also check that the context name is case-sensitive, as per the requirement.

```
ASA1# show context
Context Name      Class      Interfaces                    URL
*admin            default    Management0/0                 disk0:/admin
 abc1             default    Ethernet0/0,Ethernet0/3       disk0:/abc1
 abc2             default    Ethernet0/1.1,2,Ethernet0/2   disk0:/abc2

Total active Security Contexts: 3
```

Check that the logical VLAN is assigned on the subinterfaces on Ethernet0/1 on the ASA1 system context:

```
ASA1# show running-config interface
!
interface Ethernet0/0
!
```

 Please see page 474 for more details.

```
interface Ethernet0/1
!
interface Ethernet0/1.1
 vlan 3
!
interface Ethernet0/1.2
 vlan 4
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Management0/0
 shutdown


ASA1# show running-config context
!
admin-context admin
context admin
  allocate-interface Management0/0 mgmt
  config-url disk0:/admin
!
context abc1
  allocate-interface Ethernet0/0 outside
  allocate-interface Ethernet0/3 inside
  config-url disk0:/abc1
!
context abc2
  allocate-interface Ethernet0/1.1 inside
```

 Please see page 474 for more details.

```
  allocate-interface Ethernet0/1.2 dmz2
  allocate-interface Ethernet0/2 outside
  config-url disk0:/abc2
!
ASA1#
```

Check for admin context assigned as admin-context:

```
ASA1# show admin-context
Admin: admin disk0:/admin
```

Change the context to "abc1":

```
ASA1# changeto context abc1
```

Check that the interface is UP on the ASA1/abc1 context, and ensure that the interface name is masked with logical names and displays "Interface inside" and not "Interface Ethernet0/3":

```
ASA1/abc1# show interface
Interface inside "inside", is up, line protocol is up
        MAC address 0021.a049.4c27, MTU 1500
        IP address 192.168.8.10, subnet mask 255.255.255.0
  Traffic Statistics for "inside":
        182 packets input, 13448 bytes
        182 packets output, 11936 bytes
        0 packets dropped
Interface outside "outside", is up, line protocol is up
        MAC address 0021.a049.4c24, MTU 1500
        IP address 192.168.7.10, subnet mask 255.255.255.0
  Traffic Statistics for "outside":
        199 packets input, 46126 bytes
        112 packets output, 8536 bytes
        88 packets dropped
```

 Please see page 474 for more details.

Check the nameif and security levels assigned to each interface on the ASA1/abc1 context. Also check that the nameif is case-sensitive, as per the requirement:

```
ASA1/abc1# show nameif
Interface                Name                    Security
Ethernet0/3              inside                  100
Ethernet0/0              outside                 0
```

Check the IP address/mask assigned to each interface on the ASA1/abc1 context:

```
ASA1/abc1# show ip
System IP Addresses:
Interface                Name                    IP address      Subnet mask     Method
inside                   inside                  192.168.8.10    255.255.255.0   manual
outside                  outside                 192.168.7.10    255.255.255.0   manual
Current IP Addresses:
Interface                Name                    IP address      Subnet mask     Method
inside                   inside                  192.168.8.10    255.255.255.0   manual
outside                  outside                 192.168.7.10    255.255.255.0   manual
```

Check the static and default routes according to Table 1-3:

```
ASA1/abc1# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

 Please see page 474 for more details.

```
Gateway of last resort is 192.168.7.11 to network 0.0.0.0

C    192.168.8.0 255.255.255.0 is directly connected, inside
S    172.16.1.0 255.255.255.0 [1/0] via 192.168.8.11, inside
S    10.7.7.0 255.255.255.0 [1/0] via 192.168.8.11, inside
C    192.168.7.0 255.255.255.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 192.168.7.11, outside
```

Ensure that you can ping all the interfaces, including loopbacks of Sw1 from the ASA1/abc1 context. Your success rate percentage should be greater than 0 for all the ping outputs. The question clearly states that you are allowed to permit **icmp any any** in your ACL in both contexts.

```
ASA1/abc1# ping 192.168.8.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.8.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA1/abc1# ping 10.7.7.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.7.7.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA1/abc1# ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

 Please see page 474 for more details.

Now, change the context to abc2:

```
ASA1# changeto context abc2
```

Check that the interface is UP on the ASA1/abc2 context, and ensure that the interface name is masked with logical names and displays “Interface outside” and not “Interface Ethernet0/2”:

```
ASA1/abc2# show interface
Interface outside "outside", is up, line protocol is up
        MAC address 0021.a049.4c26, MTU 1500
        IP address 192.168.6.10, subnet mask 255.255.255.0
  Traffic Statistics for "outside":
        387 packets input, 38732 bytes
        310 packets output, 28120 bytes
        70 packets dropped
Interface inside "inside", is up, line protocol is up
        MAC address 0021.a049.4c25, MTU 1500
        IP address 192.168.3.10, subnet mask 255.255.255.0
  Traffic Statistics for "inside":
        232 packets input, 21256 bytes
        249 packets output, 21252 bytes
        0 packets dropped
Interface dmz2 "dmz2", is up, line protocol is up
        MAC address 0021.a049.4c25, MTU 1500
        IP address 192.168.4.10, subnet mask 255.255.255.0
  Traffic Statistics for "dmz2":
        145 packets input, 12826 bytes
        146 packets output, 12296 bytes
        10 packets dropped
```

 Please see page 474 for more details.

Check the nameif and security levels assigned to each interface on the ASA1/abc2 context. Also see if the nameif is case-sensitive, as per the requirement:

```
ASA1/abc2# show nameif
Interface                Name                    Security
Ethernet0/2              outside                   0
Ethernet0/1.1            inside                  100
Ethernet0/1.2            dmz2                     50
```

Check the IP address/mask assigned to each interface:

```
ASA1/abc2# show ip
System IP Addresses:
Interface                Name                    IP address      Subnet mask     Method
outside                  outside                 192.168.6.10    255.255.255.0   manual
inside                   inside                  192.168.3.10    255.255.255.0   manual
dmz2                     dmz2                    192.168.4.10    255.255.255.0   manual
Current IP Addresses:
Interface                Name                    IP address      Subnet mask     Method
outside                  outside                 192.168.6.10    255.255.255.0   manual
inside                   inside                  192.168.3.10    255.255.255.0   manual
dmz2                     dmz2                    192.168.4.10    255.255.255.0   manual
```

Check the static and default routes according to Table 1-3:

```
ASA1/abc2# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

 Please see page 474 for more details.

```
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.6.11 to network 0.0.0.0

C    192.168.4.0 255.255.255.0 is directly connected, dmz2
S    192.168.5.0 255.255.255.0 [1/0] via 192.168.4.11, dmz2
S    10.1.1.0 255.255.255.0 [1/0] via 192.168.3.11, inside
S    10.2.2.0 255.255.255.0 [1/0] via 192.168.4.11, dmz2
C    192.168.6.0 255.255.255.0 is directly connected, outside
S    192.168.2.0 255.255.255.0 [1/0] via 192.168.3.11, inside
C    192.168.3.0 255.255.255.0 is directly connected, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 192.168.6.11, outside
```

Ensure that you can ping all the interfaces, including loopbacks of R1 and R2 from the ASA1/abc2 context. Your success rate percentage should be greater than 0 for all the ping outputs.

```
ASA1/abc2# ping 192.168.2.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA1/abc2# ping 192.168.3.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA1/abc2# ping 192.168.4.11
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA1/abc2# ping 192.168.5.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA1/abc2# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA1/abc2# ping 10.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Change the context to admin:

```
ASA1# changeto context admin
```

Because the Management0/0 interface is physically not connected and will remain down, you are allowed to shut down manually:

```
ASA1/admin# show interface
Interface mgmt "mgmt", is administratively down, line protocol is down
        MAC address 0021.a049.4c23, MTU 1500
        IP address unassigned
  Traffic Statistics for "mgmt":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
        Management-only interface. Blocked 0 through-the-device packets
```

Check the nameif and security levels assigned on the ASA1/admin context:

```
ASA1/admin# show nameif
Interface                 Name                      Security
Management0/0             mgmt                      100
```

Question 1.2: Initializing the ASA2 firewall (5 points)

Initialize the ASA2 firewall, meeting all the following requirements:

- Configure the ASA2 firewall in single-routed mode, as shown in Figure 1-3.
- Configure hostname "ASA2" and enable password "cisco."
- Configure a redundant interface on ASA2, as shown in Tables 1-9 and 1-10. Ensure that interface Ethernet0/0 is the active member interface.
- Configure IP addresses and all other initialization parameters as shown in Tables 1-9 through 1-11.
- Configure static and default routes as shown in the tables. You can also refer to Figure 1-4 and Table 1-3 for more information.

- Ensure that OSPF and EIGRP adjacencies are established (as per Figure 1-4) after you complete the ASA2 initialization. R3, R4, and Sw2 have been preconfigured for IP routing.
- To perform basic verification using ping tests throughout this Practice Lab, you are allowed to permit **icmp any any** in your ACL on ASA2.
- Ensure that you can ping all the interfaces, including loopbacks on R3, R4, and Sw2 from ASA2.

Skills tested

- ☐ Initializing the Cisco ASA2 firewall in single-routed mode
- ☐ Configuring basic IP address and IP routing initialization tasks
- ☐ Configuring high-availability features using interface redundancy

Functionality and solution verification

- ☐ Similar to the preceding question, this question is also one of the core configuration tasks. If you get any item wrong in this question, it can potentially impede later questions and their functionality.
- ☐ This question requires configuring the high-availability (HA) feature using interface redundancy.
- ☐ Interface redundancy is compatible with all firewall modes (routed/transparent and single/multiple) and all HA deployment (Active/Active and Active/Standby) modes. When the active physical interface fails, traffic fails to the standby physical interface, and routing adjacencies, active connections, and auth state do not have to be relearned. The interface redundancy feature is available on Cisco ASA 5510 models and above.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

Check that the hostname is ASA2:

```
ASA2# show run hostname
hostname ASA2
```

Check if ASA2 is configured in single mode:

```
ASA1# show mode
Security context mode: single
```

Check if ASA2 is configured in routed mode:

```
ASA1# show firewall
Firewall mode: Router
```

Check that the interfaces are UP on ASA2, and ensure that Ethernet0/0 and Ethernet0/2 are members of interface Redundant 1. Also ensure that Ethernet0/0 is the current active member:

```
ASA2# show interface ¦ include Ethernet0/0 ¦ Ethernet0/2 ¦ Redundant1
Interface Ethernet0/0 "", is up, line protocol is up
        Active member of Redundant1
Interface Ethernet0/2 "", is up, line protocol is up
        Standby member of Redundant1
Interface Redundant1 "outside", is up, line protocol is up
        Member Ethernet0/0(Active), Ethernet0/2
```

Check the nameif and security levels assigned to each interface on ASA2. Also check that the nameif is case-sensitive, as per the requirement:

```
ASA2# show nameif
Interface                 Name                      Security
Ethernet0/1               inside                    100
Redundant1                outside                     0
```

 Please see page 474 for more details.

Check the IP address/mask assigned to each interface on ASA2:

```
ASA2# show ip
System IP Addresses:
Interface                Name                IP address      Subnet mask     Method
Ethernet0/1              inside              192.168.10.10   255.255.255.0   manual
Redundant1               outside             192.168.9.10    255.255.255.0   manual
Current IP Addresses:
Interface                Name                IP address      Subnet mask     Method
Ethernet0/1              inside              192.168.10.10   255.255.255.0   manual
Redundant1               outside             192.168.9.10    255.255.255.0   manual
```

Check the OSPF and EIGRP adjacencies on ASA2:

```
ASA2# show ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.3.3.3          1   FULL/BDR        0:00:39     192.168.9.3     outside
10.4.4.4          1   FULL/DROTHER    0:00:36     192.168.9.4     outside

ASA2# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.10.11           Et0/1            10     3d23h 1    200  0   50
```

Check that ASA2 is an Autonomous System Boundary Router (ASBR), because it is running both OSPF and EIGRP processes. Also ensure that EIGRP is being redistributed into OSPF.

```
ASA2# show ospf 1
 Routing Process "ospf 1" with ID 192.168.10.10 and Domain ID 0.0.0.1
 Supports only single TOS(TOS0) routes
 Does not support opaque LSA
 It is an autonomous system boundary router
 Redistributing External Routes from,
    eigrp 10 with metric mapped to 1, includes subnets in redistribution
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 24. Checksum Sum 0x bc908
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm executed 49 times
        Area ranges are
        Number of LSA 10. Checksum Sum 0x 2d798
        Number of opaque link LSA 0. Checksum Sum 0x     0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Check that autosummary is disabled and that OSPF is being redistributed into EIGRP 10 on ASA2:

```
ASA2# show run router eigrp
!
router eigrp 10
 no auto-summary
 network 192.168.10.0 255.255.255.0
 redistribute ospf 1 metric 1 1 1 1 1
```

Check the default route, and dynamic OSPF and EIGRP routes, on ASA2:

```
ASA2# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.9.4 to network 0.0.0.0

O E2 192.168.8.0 255.255.255.0 [110/1] via 192.168.9.4, 93:36:28, outside
C    192.168.9.0 255.255.255.0 is directly connected, outside
C    192.168.10.0 255.255.255.0 is directly connected, inside
O E2 172.16.1.0 255.255.255.0 [110/1] via 192.168.9.4, 93:36:28, outside
O    192.168.64.0 255.255.255.0 [110/74] via 192.168.9.4, 93:36:28, outside
O E2 192.168.4.0 255.255.255.0 [110/1] via 192.168.9.4, 93:36:28, outside
O    192.168.65.0 255.255.255.0 [110/138] via 192.168.9.4, 93:36:28, outside
                                [110/138] via 192.168.9.3, 93:36:28, outside
```

 Please see page 474 for more details.

```
O E2 192.168.5.0 255.255.255.0 [110/1] via 192.168.9.4, 93:36:28, outside
O    10.3.3.3 255.255.255.255 [110/11] via 192.168.9.3, 93:36:28, outside
D    10.8.8.0 255.255.255.0 [90/130816] via 192.168.10.11, 95:16:12, inside
O E2 10.7.7.0 255.255.255.0 [110/1] via 192.168.9.4, 93:36:28, outside
O E2 10.2.2.0 255.255.255.0 [110/1] via 192.168.9.4, 93:36:28, outside
O E2 10.1.1.0 255.255.255.0 [110/1] via 192.168.9.4, 93:36:28, outside
O    10.6.6.6 255.255.255.255 [110/75] via 192.168.9.4, 93:36:29, outside
O    10.4.4.4 255.255.255.255 [110/11] via 192.168.9.4, 93:36:29, outside
O    10.5.5.5 255.255.255.255 [110/75] via 192.168.9.3, 93:36:29, outside
O E2 192.168.6.0 255.255.255.0 [110/1] via 192.168.9.4, 93:36:29, outside
O E2 192.168.7.0 255.255.255.0 [110/1] via 192.168.9.4, 93:36:29, outside
O    192.168.35.0 255.255.255.0 [110/74] via 192.168.9.3, 93:36:29, outside
O E2 192.168.2.0 255.255.255.0 [110/1] via 192.168.9.4, 93:36:29, outside
O E2 192.168.3.0 255.255.255.0 [110/1] via 192.168.9.4, 93:36:29, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 192.168.9.4, outside
```

Ensure that you can ping all the interfaces, including loopbacks of R3, R4, and Sw2 from ASA2. Your success rate percentage should be greater than 0 for all the ping outputs. The question clearly states that you are allowed to permit **icmp any any** in your ACL on ASA2.

```
ASA2# ping 192.168.9.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA2# ping 192.168.35.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.35.3, timeout is 2 seconds:
!!!!!
```

 Please see page 474 for more details.

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA2# ping 10.3.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA2# ping 192.168.9.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA2# ping 192.168.64.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.64.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA2# ping 10.4.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA2# ping 192.168.10.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.11, timeout is 2 seconds:
!!!!!
```

 Please see page 474 for more details.

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA2# ping 10.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Question 1.3: Secure IP routing (3 points)

Configure strong authentication for OSPF and EIGRP routing protocols using the information in Table 1-12. You can also refer to Figure 1-4.

- Ensure that OSPF and EIGRP adjacencies are established on all devices after you complete this task.
- Repeat all the pings from Question 1.2, and ensure that they are successful.

Skills tested

☐ Configuring MD5 authentication (link-based) for OSPF and EIGRP protocols on Cisco Routers, Catalyst Switches, and Cisco ASA firewall

Functionality and solution verification

☐ This question builds on the initial configuration provided in Question 1.2. Note that OSPF and EIGRP are preconfigured on R3, R4, and Sw2. And Question 1.2 required configuring the OSPF and EIGRP on ASA2.

☐ By using the term "strong" authentication, the question implies a strict type of authentication mechanism. Often, strong authentication is associated with two-factor or multifactor authentication. However, in this case, the choice is between clear-text and MD5 type only, which is why you must choose MD5 authentication. If you configure clear-text, the solution will be considered incorrect.

- ☐ The objective of this question is to configure strong MD5 authentication on all devices (R3, R4, Sw2, and ASA2) for OSPF and EIGRP AS 10, as per Figure 1-4.
- ☐ Note that the question requires configuring link-based authentication, not area-wide. Therefore, solutions will be primarily configured under the interface(s) on each device.
- ☐ Ensure that OSPF and EIGRP adjacencies are established (as per Figure 1-4) after you complete this task.
- ☐ After completing the configuration, you need to reverify all pings from Question 1.2 and ensure that they are successful.
- ☐ You will see several **show** command outputs that help you check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

Check that R3 area 0 has no authentication (area-wide authentication is not allowed):

```
R3# show ip ospf
 Routing Process "ospf 1" with ID 10.3.3.3
 Start time: 3w0d, Time elapsed: 5d00h
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
```

 Please see page 474 for more details.

```
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 13. Checksum Sum 0x13B372
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
   Area BACKBONE(0)
        Number of interfaces in this area is 3 (1 loopback)
        Area has no authentication
        SPF algorithm last executed 18:18:43.968 ago
        SPF algorithm executed 12 times
        Area ranges are
        Number of LSA 6. Checksum Sum 0x08232D
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

 Please see page 474 for more details.

Check that R3 interface Gi0/1 has link-based authentication configuration:

```
R3# show ip ospf interface GigabitEthernet 0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet Address 192.168.9.3/24, Area 0
  Process ID 1, Router ID 10.3.3.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 192.168.10.10, Interface address 192.168.9.10
  Backup Designated router (ID) 10.3.3.3, Interface address 192.168.9.3
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 6
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 10.4.4.4
    Adjacent with neighbor 192.168.10.10  (Designated Router)
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

 Please see page 474 for more details.

Check that R4 area 0 has no authentication (area-wide authentication is not allowed):

```
R4# show ip ospf
 Routing Process "ospf 1" with ID 10.4.4.4
 Start time: 3w1d, Time elapsed: 5d00h
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 13. Checksum Sum 0x0DCEF5
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
 IETF NSF helper support enabled
 Cisco NSF helper support enabled
    Area BACKBONE(0)
        Number of interfaces in this area is 3 (1 loopback)
```

```
Area has no authentication
SPF algorithm last executed 18:19:20.792 ago
SPF algorithm executed 17 times
Area ranges are
Number of LSA 6. Checksum Sum 0x05975F
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
```

Check that R4 interface Gi0/1 has link-based authentication configuration:

```
R4# show ip ospf interface GigabitEthernet 0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet Address 192.168.9.4/24, Area 0
  Process ID 1, Router ID 10.4.4.4, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.10.10, Interface address 192.168.9.10
  Backup Designated router (ID) 10.3.3.3, Interface address 192.168.9.3
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:03
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 6, maximum is 6
  Last flood scan time is 0 msec, maximum is 4 msec
```

```
 Neighbor Count is 2, Adjacent neighbor count is 2
   Adjacent with neighbor 10.3.3.3  (Backup Designated Router)
   Adjacent with neighbor 192.168.10.10  (Designated Router)
 Suppress hello for 0 neighbor(s)
 Message digest authentication enabled
   Youngest key id is 1
```

Check that ASA2 area 0 has no authentication (area-wide authentication is not allowed):

```
ASA2# show ospf 1
 Routing Process "ospf 1" with ID 192.168.10.10 and Domain ID 0.0.0.1
 Supports only single TOS(TOS0) routes
 Does not support opaque LSA
 It is an autonomous system boundary router
 Redistributing External Routes from,
    eigrp 10 with metric mapped to 1, includes subnets in redistribution
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 24. Checksum Sum 0x da29a
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm executed 49 times
        Area ranges are
        Number of LSA 10. Checksum Sum 0x 4694e
```

```
        Number of opaque link LSA 0. Checksum Sum 0x     0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Check that ASA2 interface outside has link-based authentication configuration:

```
ASA2# show ospf 1 interface
outside is up, line protocol is up
  Internet Address 192.168.9.10 mask 255.255.255.0, Area 0
  Process ID 1, Router ID 192.168.10.10, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.10.10, Interface address 192.168.9.10
  Backup Designated router (ID) 10.3.3.3, Interface address 192.168.9.3
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 0:00:04
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 7, maximum is 7
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 10.3.3.3  (Backup Designated Router)
    Adjacent with neighbor 10.4.4.4
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

 Please see page 474 for more details.

Check that ASA2 interface Redundant 1 has link-based authentication configuration:

```
ASA2# show run interface Redundant 1
!
interface Redundant1
 member-interface Ethernet0/0
 member-interface Ethernet0/2
 nameif outside
 security-level 0
 ip address 192.168.9.10 255.255.255.0
 ospf message-digest-key 1 md5 <removed>
 ospf authentication message-digest
!
```

Check that interface Sw2 Fa0/11 has link-based authentication configuration:

```
Sw2# show run interface fastEthernet 0/11
Building configuration...

Current configuration : 170 bytes
!
interface FastEthernet0/11
 no switchport
 ip address 192.168.10.11 255.255.255.0
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 cisco
end
```

Check the EIGRP adjacencies on Sw2:

```
Sw2# show ip eigrp neighbors
EIGRP-IPv4:(10) neighbors for process 10
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.10.10           Fa0/11            13 18:21:47    1   200  0  72
```

Check that the OSPF and EIGRP adjacencies on ASA2 are established after configuring authentication:

```
ASA2# show ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.3.3.3          1   FULL/BDR        0:00:32     192.168.9.3     outside
10.4.4.4          1   FULL/DROTHER    0:00:30     192.168.9.4     outside

ASA2# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.10.11           Et0/1             12  18:20:48 2    200   0   70
```

Finally, you need to reverify all the pings from Question 1.2. Ensure that you can ping all the interfaces, including loopbacks of R3, R4, and Sw2 from ASA2. Your success rate percentage should be greater than 0 for all the ping outputs.

```
ASA2# ping 192.168.9.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA2# ping 192.168.35.3
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.35.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA2# ping 10.3.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA2# ping 192.168.9.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA2# ping 192.168.64.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.64.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA2# ping 10.4.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA2# ping 192.168.10.11
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA2# ping 10.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Question 1.4: Initializing IPS Sensor (4 points)

Initialize Cisco IPS Sensor, meeting all the following requirements:

- Configure the IPS sensor appliance in virtual sensor mode, as shown in Figure 1-3.
- Configure hostname "IPS," and allow Telnet sessions to the IPS sensor from VLAN 2.
- Configure the Command and Control (Management 0/0) interface IP address 192.168.2.12/24 with default gateway 192.168.2.11.
- Catalyst switches have been preconfigured for this question.
- Configure the integrated web server on the sensor appliance to accept HTTPS connections on port 8000 for managing the sensor. Users in VLAN 2 should be able to browse the IPS Device Manager (IDM) using https://192.168.2.12:8000 from their web browser.
- Configure the IPS sensor for inline VLAN pairing using the information in Table 1-13. Refer to Figure 1-3 for more information.

- You can also refer to Figure 1-1 for physical port connections.
- Verify that the virtual sensors are passing traffic. Ensure that you can ping all interfaces, including loopbacks of R1, R2, and Sw1 from R6.

Skills tested

- ☐ Configuring basic initialization for the Cisco IPS sensor appliance
- ☐ Configuring virtual sensors, enabling the virtualization of both the configuration and the sensor state
- ☐ Configuring inline VLAN pairing for two virtual sensors
- ☐ Tuning the sensor to use a nonstandard web server port
- ☐ Securing access control using ACL

Functionality and solution verification

- ☐ Again, this question is one of the core configuration tasks, so you need to be very careful when attempting it. If you get any item wrong in this question, it can potentially impede the functionality of later questions.
- ☐ It is strongly recommended that you practice the IPS virtual sensor several times using inline mode configuration during your study sessions to ensure perfection and accuracy in this area. There are several types of inline configuration: inline VLAN pair, inline interface pair, inline VLAN group. Practice all the varying combinations.
- ☐ The Catalyst switches have been preconfigured for this Practice Lab. However, during the real CCIE lab exam, you might have to configure the switches as well. Practice this task during your study sessions, and verify your configuration with the final switch solutions provided. Refer to Figure 1-1 for the physical port connections.
- ☐ This question can be divided into two subsections. The first is the basic initial configuration of the sensor, which involves basic IP addressing, Telnet, and ACL. The second is the inline VLAN pairing, which is a critical piece of this task.

- After the sensor is configured, you need to verify that the virtual sensors using inline VLAN pairing are passing traffic. Ensure that you can ping all interfaces, including loopbacks of R1, R2, and Sw1 from R6. The success of these ping verifications provides evidence that inline VLAN pairing is configured correctly and functioning as required.
- You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

Check the IPS basic initial parameters first:

```
IPS(config)# service host
IPS(config-hos)# show settings
   network-settings
   ------------------------------------------------
      host-ip: 192.168.2.12/24,192.168.2.11 default: 192.168.1.2/24,192.168.1.1
      host-name: IPS default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      ------------------------------------------------
         network-address: 192.168.2.0/24
         ------------------------------------------
      ------------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text:  <defaulted>
   ------------------------------------------------
   time-zone-settings
   ------------------------------------------------
<snip>
```

Check that the IPS management interface is UP:

```
IPS# show interfaces Management0/0
MAC statistics from interface Management0/0
   Interface function = Command-control interface
   Description =
   Media Type = TX
   Default Vlan = 0
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 27910
   Total Bytes Received = 5058593
   Total Multicast Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 8830
   Total Bytes Transmitted = 12101507
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
```

Verify if hosts in VLAN 2 can ping and telnet the IPS sensor:

```
R1# ping 192.168.2.12 source GigabitEthernet 0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.12, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.11
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R1# telnet 192.168.2.12 /source-interface GigabitEthernet 0/1
```

 Please see page 474 for more details.

```
Trying 192.168.2.12 ... Open
login: cisco
Password: 123cisco123
Last login: Sun May 31 06:27:14 on ttyS0
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the IPS-4240.
The system will continue to operate with the currently installed
signature set.  A valid license must be obtained in order to apply
signature updates.  Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
IPS# exit
[Connection to 192.168.2.12 closed by foreign host]
R1#
```

 Please see page 474 for more details.

If this is successful, verify whether IPS is accepting connections only from VLAN 2 hosts. For example, when pinging from a non-VLAN 2, the interface on R1 should fail, because the IPS drops the pings due to the sensor ACL.

```
R1# ping 192.168.2.12 source GigabitEthernet 0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.12, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.11
.....
Success rate is 0 percent (0/5)
```

Now, verify if the IPS management port is accepting connections on port 8000 and not 80:

```
R1# telnet 192.168.2.12 8000 /source-interface GigabitEthernet 0/1
Trying 192.168.2.12, 8000 ... Open

^C
[Connection to 192.168.2.12 closed by foreign host]
R1#

R1# telnet 192.168.2.12 80 /source-interface GigabitEthernet 0/1
Trying 192.168.2.12, 80 ...
% Connection refused by remote host
```

When everything is OK, move on to verifying the second part of the question, which requires configuring inline VLAN pairing.

Check the settings under the interface service to ensure that Gig0/0 and Gig0/1 are enabled and that the inline VLAN pair and VLAN numbers are configured as per the requirement:

```
IPS(config)# service interface
IPS(config-int)# show settings
   physical-interfaces (min: 0, max: 999999999, current: 5)
```

```
-----------------------------------------------
   <protected entry>
   name: GigabitEthernet0/0
   -----------------------------------------------
      media-type: tx <protected>
      description:  <defaulted>
      admin-state: enabled default: disabled
      duplex: auto <defaulted>
      speed: auto <defaulted>
      default-vlan: 0 <defaulted>
      alt-tcp-reset-interface
      -----------------------------------------------
         none
         -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      subinterface-type
      -----------------------------------------------
         inline-vlan-pair
         -----------------------------------------------
            subinterface (min: 1, max: 255, current: 1)
            -----------------------------------------------
               subinterface-number: 1
               -----------------------------------------------
                  description:  <defaulted>
                  vlan1: 101
                  vlan2: 102
               -----------------------------------------------
            -----------------------------------------------
```

 Please see page 474 for more details.

```
      ------------------------------------------------
   ---------------------------------------------
---------------------------------------------
<protected entry>
name: GigabitEthernet0/1
---------------------------------------------
   media-type: tx <protected>
   description:  <defaulted>
   admin-state: enabled default: disabled
   duplex: auto <defaulted>
   speed: auto <defaulted>
   default-vlan: 0 <defaulted>
   alt-tcp-reset-interface
   ---------------------------------------------
      none
      ---------------------------------------------
      ---------------------------------------------
   ---------------------------------------------
   subinterface-type
   ---------------------------------------------
      inline-vlan-pair
      ---------------------------------------------
         subinterface (min: 1, max: 255, current: 1)
         ---------------------------------------------
            subinterface-number: 1
            ---------------------------------------------
               description:  <defaulted>
               vlan1: 201
               vlan2: 202
            ---------------------------------------------
```

 Please see page 474 for more details.

```
                  -------------------------------------------
               -------------------------------------------
            -------------------------------------------
         -------------------------------------------
         <protected entry>
         name: GigabitEthernet0/2 <defaulted>
         -------------------------------------------
<snip>
```

Now check the settings under the analysis-engine, and ensure that two virtual sensors are configured—namely, vs0 and vs2—and have the sig0 and sig2 signature definitions assigned, respectively:

```
IPS(config)# service analysis-engine
IPS(config-ana)# show settings
   global-parameters
   -------------------------------------------
      ip-logging
      -------------------------------------------
         max-open-iplog-files: 20 <defaulted>
      -------------------------------------------
   -------------------------------------------
   virtual-sensor (min: 1, max: 255, current: 2)
   -------------------------------------------
      <protected entry>
      name: vs0
      -------------------------------------------
         description: default virtual sensor <defaulted>
         signature-definition: sig0 <protected>
         event-action-rules: rules0 <protected>
         anomaly-detection
```

 Please see page 474 for more details.

```
   ------------------------------------------------
      anomaly-detection-name: ad0 <protected>
      operational-mode: detect <defaulted>
   ------------------------------------------------
   physical-interface (min: 0, max: 999999999, current: 1)
   ------------------------------------------------
      name: GigabitEthernet0/0
      subinterface-number: 1 default: 0
      ------------------------------------------------
   ------------------------------------------------
   logical-interface (min: 0, max: 999999999, current: 0)
   ------------------------------------------------
   ------------------------------------------------
   inline-TCP-session-tracking-mode: virtual-sensor <defaulted>
   inline-TCP-evasion-protection-mode: strict <defaulted>
------------------------------------------------
name: vs2
------------------------------------------------
   description:  <defaulted>
   signature-definition: sig2 default: sig0
   event-action-rules: rules0 <defaulted>
   anomaly-detection
   ------------------------------------------------
      anomaly-detection-name: ad0 <defaulted>
      operational-mode: detect <defaulted>
   ------------------------------------------------
   physical-interface (min: 0, max: 999999999, current: 1)
   ------------------------------------------------
      name: GigabitEthernet0/1
      subinterface-number: 1 default: 0
```

 Please see page 474 for more details.

```
            ------------------------------------------
          ------------------------------------------
          logical-interface (min: 0, max: 999999999, current: 0)
          ------------------------------------------
          ------------------------------------------
          inline-TCP-session-tracking-mode: virtual-sensor <defaulted>
          inline-TCP-evasion-protection-mode: strict <defaulted>
        ------------------------------------------
      ------------------------------------------
```

When the inline VLAN pairing configuration looks OK, you need to verify if the virtual sensors are passing traffic. You also need to verify the functionality using ping tests through these virtual sensors all the way across the ASA1 contexts.

The question clearly states that R6 should be able to ping all interfaces, including the loopbacks of R1, R2, and Sw1. The success of these ping verifications provides evidence that inline VLAN pairing is configured correctly and passing traffic as required.

On a side note, another test you could perform to ensure that virtual sensors are passing traffic correctly is changing the preconfigured VLANs and putting them in an incorrect, dummy VLAN. This should break the traffic flow, and pings would fail.

```
R6# ping 192.168.3.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R6# ping 192.168.2.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.11, timeout is 2 seconds:
!!!!!
```

 Please see page 474 for more details.

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R6# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R6# ping 192.168.4.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R6# ping 192.168.5.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R6# ping 10.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms

R6# ping 192.168.8.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.8.11, timeout is 2 seconds:
!!!!!
```

 Please see page 474 for more details.

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R6# ping 10.7.7.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.7.7.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

R6# ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Question 1.5: Configuring NTP (3 points)

Configure Network Time Protocol (NTP) on R1, R5, and ASA2 using the following information:

- Configure R1 as the NTP server using source Loopback0 and stratum 5.
- Configure strong authentication to protect NTP sessions between server and client using password “cisco.”
- Configure ASA2 and R5 as NTP clients to synchronize its clock with R1.
- Configure access control on the R1 NTP server such that it allows full access from specific hosts ASA2 outside interface and R5 Loopback0 interfaces only. No other device should be able to sync clock with R1.
- Configure Sw2 to synchronize its clock with R5. Do not use any NTP server/peer commands on Sw2. There should be no NTP commands in global configuration mode on Sw2.

Skills tested

- ☐ Configuring Network Time Protocol (NTP) on Cisco routers, switches, and ASA firewall in client/server mode, including broadcast mode
- ☐ Configuring NTP to use a specific source address for all NTP packets
- ☐ Securing NTP sessions using MD5 authentication and specifying trusted hosts using ACL

Functionality and solution verification

- ☐ The reason this question is part of the core configuration is that later sections in this Practice Lab may build upon this question. For example, when configuring the Cisco IOS CA server, the clock must be synchronized on all devices. Therefore, the NTP solution ensures that clocks are synchronized before you can configure CA server parameters.
- ☐ The objective of this question is very basic—to synchronize clocks. However, you should be aware of a few embedded challenges to complete all the requirements.
- ☐ R1 is designated as the NTP server using stratum number 5, with ASA2 and R5 being the NTP clients.
- ☐ The question also requires configuring Loopback0 as the source IP address on R5 for all NTP packets.
- ☐ The question also requires configuring strong MD5 authentication using the "cisco" password.
- ☐ In addition to MD5 authentication, the question requires strict access control on R1 to specify trusted clients—ASA2 outside interface and R5 Loopback0 interfaces only. This task requires that you configure a standard access control list (ACL) allowing ASA2 outside interface and R5 Loopback0 explicitly, and that you apply this ACL using the NTP **access-group** command on the R1 server.
- ☐ Also note that you need to open the ACL on the ASA1/abc2 context to allow an NTP session (UDP port 123) entering the outside interface from the source ASA2 outside interface and R5 Loopback0 to destination R1 Loopback0. Because the question does not restrict or mention anything about this ACL, you can permit UDP port 123 from any source to any destination. However, as a best practice, I recommend that you write a specific ACL, because you know the source and destination IP address in this task. Again, this is just a recommendation, not a requirement.

 Please see page 474 for more details.

- The most challenging part of this question lies in the last item, which requires Sw2 to synchronize its clock with R5 without using any NTP commands in Sw2 global configuration mode. The solution is to configure R5 as NTP broadcast mode under the GigabitEthernet0/1 interface and to configure Sw2 as NTP broadcast listen mode under the FastEthernet0/5 interface. Sw2 and R5 are connected back-to-back on these interfaces. This will meet the requirement.
- You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

Check that R1 is configured as the NTP server and that its clock is synchronized using NTP with stratum 5:

```
R1# show ntp status
Clock is synchronized, stratum 5, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is CDD1074D.F9C12F96 (14:29:33.975 UTC Wed Jun 3 2009)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 14 sec ago.

R1# show ntp associations detail
127.127.1.1 configured, our_master, sane, valid, stratum 4
ref ID .LOCL., time CDD1075D.F9C07383 (14:29:49.975 UTC Wed Jun 3 2009)
our mode active, peer mode passive, our poll intvl 16, peer poll intvl 16
root delay 0.00 msec, root disp 0.00, reach 377, sync dist 0.00
delay 0.00 msec, offset 0.0000 msec, dispersion 0.23
precision 2**24, version 4
org time CDD1075D.F9C07383 (14:29:49.975 UTC Wed Jun 3 2009)
rec time CDD1075D.F9C0D4F2 (14:29:49.975 UTC Wed Jun 3 2009)
```

 Please see page 474 for more details.

```
xmt time CDD1075D.F9C035E7 (14:29:49.975 UTC Wed Jun 3 2009)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
minpoll = 4, maxpoll = 4

R1# show clock detail
14:29:57.935 UTC Wed Jun 3 2009
Time source is NTP
```

Ensure that MD5 authentication is configured, along with update source IP address using Loopback0. Also ensure that the access control list (ACL) is allowing specific hosts ASA2 outside interface and R5 Loopback0 only:

```
R1# show run ¦ section ntp
ntp authentication-key 1 md5 045802150C2E 7
ntp authenticate
ntp trusted-key 1
ntp source Loopback0
ntp access-group peer 1
ntp master 5
R1#

R1# show ip access-lists 1
Standard IP access list 1
    10 permit 10.5.5.5 (83 matches)
    20 permit 192.168.9.10 (99 matches)
```

Now check NTP client configuration on ASA2 and ensure that the clock is synchronized with R1 Loopback0 and that authentication is OK:

```
ASA2# show ntp status
Clock is synchronized, stratum 6, reference is 10.1.1.1
nominal freq is 99.9984 Hz, actual freq is 99.9984 Hz, precision is 2**6
reference time is cdd75f12.3b31499c (09:57:38.231 UTC Mon Jun 8 2009)
clock offset is 0.6172 msec, root delay is 2.15 msec
root dispersion is 16.65 msec, peer dispersion is 15.81 msec

ASA2# show ntp associations detail
10.1.1.1 configured, authenticated, our_master, sane, valid, stratum 5
ref ID 127.127.1.1, time cdd75f10.f26b45f7 (09:57:36.946 UTC Mon Jun 8 2009)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 0.00 msec, root disp 0.23, reach 377, sync dist 17.105
delay 2.15 msec, offset 0.6172 msec, dispersion 15.81
precision 2**24, version 3
org time cdd75f12.3b12f429 (09:57:38.230 UTC Mon Jun 8 2009)
rcv time cdd75f12.3b31499c (09:57:38.231 UTC Mon Jun 8 2009)
xmt time cdd75f12.3a9e2ea2 (09:57:38.228 UTC Mon Jun 8 2009)
filtdelay =     2.15    2.21    2.14    2.11    2.04    2.20    2.15    2.11
filtoffset =    0.62    0.41    0.49    0.38    0.34    0.45    0.39    0.34
filterror =    15.63   16.60   17.26   18.23   19.21   20.19   21.16   22.14

ASA2# show clock detail
09:58:23.478 UTC Mon Jun 8 2009
Time source is NTP
```

 Please see page 474 for more details.

As mentioned earlier, for clients to be able to successfully synchronize their clock with R1, you need to open the ACL on the ASA1/abc2 context to allow the NTP session (UDP port 123) entering the outside interface:

```
ASA1/abc2# show run access-group
access-group 100 in interface outside
access-group 100 in interface dmz2

ASA1/abc2# show run access-list 100
access-list 100 extended permit icmp any any
access-list 100 extended permit udp host 10.5.5.5 host 10.1.1.1 eq ntp
access-list 100 extended permit udp host 192.168.9.10 host 10.1.1.1 eq ntp
```

Now repeat similar steps on R5 to check NTP client configuration and to ensure that the clock is synchronized with R1 Loopback0 and that authentication is OK:

```
R5# show ntp status
Clock is synchronized, stratum 6, reference is 10.1.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0009 Hz, precision is 2**24
reference time is CDD109EC.9D7804BE (14:40:44.615 UTC Wed Jun 3 2009)
clock offset is -0.0555 msec, root delay is 0.00 msec
root dispersion is 0.06 msec, peer dispersion is 0.00 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000003551 s/s
system poll interval is 64, last update was 198 sec ago.

R5# show ntp associations detail
10.1.1.1 configured, authenticated, our_master, sane, valid, stratum 5
ref ID 127.127.1.1   , time CDD10AAC.F9BC7A9B (14:43:56.975 UTC Wed Jun 3 2009)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.21, reach 377, sync dist 0.00
delay 0.00 msec, offset -55.5902 msec, dispersion 4.60
```

 Please see page 474 for more details.

```
precision 2**24, version 4
org time CDD10AAD.8C795DF9 (14:43:57.548 UTC Wed Jun 3 2009)
rec time CDD10AAD.9ADC3B81 (14:43:57.604 UTC Wed Jun 3 2009)
xmt time CDD10AAD.9A3D4243 (14:43:57.602 UTC Wed Jun 3 2009)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =   -0.05   -0.05   -0.05   -0.05   -0.05   -0.05   -0.05   -0.05
filterror =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
minpoll = 6, maxpoll = 10

R5# show clock detail
14:44:12.537 UTC Wed Jun 3 2009
Time source is NTP
```

One important verification on R5 is to check whether it was configured as NTP broadcast mode to advertise NTP packets out the Gig0/1 interface:

```
R5# show run interface GigabitEthernet 0/1
Building configuration...
Current configuration : 133 bytes
!
interface GigabitEthernet0/1
 ip address 192.168.11.10 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 ntp broadcast
end
```

If this was configured correctly, Sw2 will synchronize its clock with R5 if it was configured as NTP broadcast listen mode. Verify FastEthernet0/5 on Sw2:

```
Sw2# show run interface FastEthernet 0/5
Building configuration...
Current configuration : 110 bytes
!
interface FastEthernet0/5
 no switchport
 ip address 192.168.11.11 255.255.255.0
 ntp broadcast client
end
```

Ensure that no NTP server/peer commands are configured under global configuration mode as restricted:

```
Sw2# show run ¦ include ntp
 ntp broadcast client
ntp clock-period 36028965
```

If all these configurations are correct, you will see that the Sw2 clock is synchronized with R5 using broadcast mode:

```
Sw2# show ntp associations detail
192.168.11.10 dynamic, our_master, sane, valid, stratum 6
ref ID 10.1.1.1, time CDD10AEF.9A0226C0 (14:45:03.601 UTC Wed Jun 3 2009)
our mode bdcast client, peer mode bdcast, our poll intvl 64, peer poll intvl 64
root delay 2.12 msec, root disp 64.71, reach 377, sync dist 67.581
delay 1.04 msec, offset -0.9759 msec, dispersion 1.30
precision 2**24, version 4
org time CDD10C8E.9453107A (14:51:58.579 UTC Wed Jun 3 2009)
rcv time CDD10C8E.94D004B0 (14:51:58.581 UTC Wed Jun 3 2009)
xmt time CDD0F673.7C9842F3 (13:17:39.486 UTC Wed Jun 3 2009)
```

 Please see page 474 for more details.

```
filtdelay =     1.04    1.04    1.04    1.04    1.04    1.04    1.04    1.04
filtoffset =   -0.98   -1.02   -0.93   -1.82   -3.54   -1.24   -0.53   -0.31
filterror =     0.98    1.98    2.94    3.92    4.88    5.87    6.84    7.81

Sw2# show clock detail
14:52:51.610 UTC Wed Jun 3 2009
Time source is NTP
```

Section 2.0: Cisco Firewall (10 Points)

Question 2.1: Network Address Translation (NAT) (3 points)

Configure Network Address Translation (NAT) on ASA1 and ASA2, meeting all the following requirements:

- Do not enable NAT control on ASA1 and ASA2.
- Configure static identity NAT on the ASA1/abc1 context for the web server (Sw1 Loopback1). Permit HTTP and HTTPS ports to allow connections from any host to this web server. Verify that you can establish a Telnet connection to this web server on HTTP and HTTPS ports from R6.
- Configure address translation on the ASA1/abc2 context such that when R1 establishes a Telnet session to R6 Loopback0 using its source Loopback0, the source address gets translated to 192.168.6.61. However, when R1 establishes the same Telnet session to R6 Loopback0 without using its source Loopback0 (that is, using any other source), it should get translated to 192.168.6.62. Do not use a **static** NAT command to perform this task.
- Configure static NAT on ASA2 such that Sw2 can reach destination R6 Loopback0 interface using local address 192.168.10.6. Ensure that you can ping and telnet to R6 Loopback0 from Sw2 using IP address 192.168.10.6. Verify the connections table on ASA2 to confirm that your Telnet session to destination R6 Loopback0 (10.6.6.6) is translated to 192.168.10.6.

 Please see page 474 for more details.

Skills tested

- ☐ Configuring Network Address Translation (NAT) on Cisco ASA Firewall
- ☐ Configuring static identity NAT
- ☐ Configuring policy NAT
- ☐ Configuring destination NAT
- ☐ Tuning ACL on the Cisco ASA Firewall to allow legitimate connections
- ☐ Establishing HTTP and HTTPS connections from a router to verify web server connectivity through the firewall

Functionality and solution verification

- ☐ This question is divided into three parts, requiring you to configure static identity NAT, policy NAT, and destination NAT. All three requirements must be met to earn the points. The CCIE lab exam offers no partial credit.
- ☐ The question clearly says not to enable NAT control on both ASA1 and ASA2.
- ☐ The first task in this question requires configuring static identity NAT on the ASA1/abc1 context. Static identity NAT is similar to static NAT, but it creates a fixed 1-to-1 translation of the real address, keeping the same original address. The NAT engine on the firewall does not perform address translation for the internal hosts, and the source address remains the same. Outside users can initiate an inbound connection to this untranslated address as long as the address is routable. In addition, you are required to open ACL on the ASA1/abc1 context to allow HTTP (TCP port 80) and HTTPS (TCP port 443) connections from any host to the web server IP address (172.16.1.1). The most important part of this question is the verification and functionality testing. This can be performed from R6 by establishing a Telnet session to the web server on TCP ports 80 and 443, accordingly. Sample **show** outputs are shown next to illustrate this test. They verify the connections table on the ASA1/abc1 context to ensure that the sessions are correct. More sample **show** outputs are shown next to illustrate the identity NAT feature.

- The second task in this question requires configuring policy NAT on the ASA1/abc2 context. Policy NAT is also similar to static NAT. However, it allows for defining conditional criteria to check the pairing of source address and destination address (or ports) combined. With this feature, source address translation can vary, subject to destination. In summary, regular NAT uses source IP addresses/ports only, whereas policy NAT uses both source and destination IP addresses/ports to identify real addresses for translation. The question clearly says not to use static NAT commands, which means that the only other way to configure the solution is to use the dynamic **nat/global** command set. Again, this question is verifiable, and functionality can be tested by establishing specific Telnet sessions from R1 to R6, as shown next. These sample **show** outputs illustrate the policy NAT feature.
- The third task in this question requires configuring destination NAT on ASA2. As the name implies, destination NAT is used to translate the destination IP address in the connection, not the source. All regular NAT functions are mostly about source address translation; however, with certain scenarios in the network you must configure destination NAT. Again, this question is verifiable, and functionality can be tested by establishing Telnet sessions from Sw2 to R6, as shown next. These sample **show** outputs illustrate the destination NAT feature.
- You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

The following steps illustrate verification for the first task in this question, requiring static identity NAT configuration on the ASA1/abc1 context.

Verify if NAT control is disabled on the ASA1/abc1 context. Then verify that static identity NAT and ACL are configured correctly:

```
ASA1# changeto context abc1
ASA1/abc1# show run nat-control
no nat-control

ASA1/abc1# show run static
static (inside,outside) 172.16.1.1 172.16.1.1 netmask 255.255.255.255

ASA1/abc1# show run access-group
access-group 100 in interface outside

ASA1/abc1# show run access-list 100
access-list 100 extended permit icmp any any
access-list 100 extended permit tcp any host 172.16.1.1 eq www
access-list 100 extended permit tcp any host 172.16.1.1 eq https
```

When this configuration is OK, you can perform verification steps to check its functionality by establishing Telnet sessions from R6 to the web server IP address on ports 80 and 443:

```
R6# telnet 172.16.1.1 80
Trying 172.16.1.1, 80 ... Open
^C
HTTP/1.1 400 Bad Request
Date: Tue, 30 Mar 1993 22:14:22 GMT
Server: cisco-IOS
Accept-Ranges: none
400 Bad Request
[Connection to 172.16.1.1 closed by foreign host]

R6# telnet 172.16.1.1 443
Trying 172.16.1.1, 443 ... Open
^C
[Connection to 172.16.1.1 closed by foreign host]
R6#
```

When the Telnet connection is successful, you can simultaneously check the connections table on the ASA1/abc1 context to verify that the connection is indeed established through the firewall on the desired address/port. The following **show conn** output shows TCP sessions on ports 80 and 443 to the web server IP address from R6:

```
ASA1/abc1# show conn
1 in use, 4 most used
TCP outside 192.168.7.11:34707 inside 172.16.1.1:80, idle 0:00:03, bytes 0, flags UB

ASA1/abc1# show conn
1 in use, 4 most used
TCP outside 192.168.7.11:21622 inside 172.16.1.1:443, idle 0:00:02, bytes 0, flags UB
```

The following steps illustrate verification for the second task in this question—requiring policy NAT configuration on the ASA1/abc2 context.

Verify if NAT control is disabled on the ASA1/abc2 context. Also verify if static NAT commands are not used to complete this task. Then, verify that policy NAT and the ACL are configured correctly using the **nat/global** command set.

There is no need to configure ACL on the outside interface, because traffic is traversing from a higher-security (inside) interface to a lower-security (outside) interface.

```
ASA1# changeto context abc2
ASA1/abc2# show run nat-control
no nat-control

ASA1/abc2# show run static
<null output>

ASA1/abc2# show run nat
nat (inside) 1 access-list 101
nat (inside) 2 access-list 102
```

 Please see page 474 for more details.

```
ASA1/abc2# show run global
global (outside) 1 192.168.6.61
global (outside) 2 192.168.6.62

ASA1/abc2# show run access-list 101
access-list 101 extended permit tcp host 10.1.1.1 host 10.6.6.6 eq telnet

ASA1/abc2# show run access-list 102
access-list 102 extended permit tcp any host 10.6.6.6 eq telnet
```

When this configuration is OK, you can perform verification steps to check its functionality by establishing Telnet sessions from R1 to R6 Loopback0 using two scenarios, with and without source Loopback0. The important verification is using the **who** command after establishing the Telnet session to verify the translated IP address in both scenarios.

In the first Telnet session, when using source Loopback0, the source IP address should be translated to 192.168.6.61. However, in the second Telnet session, without using source Loopback0, the source IP address should be translated to 192.168.6.62:

```
R1# telnet 10.6.6.6 /source-interface Loopback 0
Trying 10.6.6.6 ... Open

User Access Verification

Password: cisco
R6> who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:11:32
*578 vty 0                 idle                 00:00:00 192.168.6.61

  Interface    User               Mode         Idle     Peer Address
```

 Please see page 474 for more details.

```
R6> exit
[Connection to 10.6.6.6 closed by foreign host]
R1#
R1#
R1# telnet 10.6.6.6
Trying 10.6.6.6 ... Open

User Access Verification

Password: cisco
R6> who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:11:42
*578 vty 0                 idle                 00:00:00 192.168.6.62

  Interface    User               Mode         Idle     Peer Address

R6> exit
[Connection to 10.6.6.6 closed by foreign host]
R1#
```

When the Telnet connection is successful, you can simultaneously check the xlate table on the ASA1/abc1 context to verify that the connection is indeed established through the firewall and that the source IP address is translated, as per the requirement. The following **show xlate detail** output shows outbound Telnet sessions being translated to the different IP address when matching the ACL in parentheses.

The first output was captured during the first Telnet session (when using source Loopback0) matching ACL 101. The second output was captured during the second Telnet session (without using source Loopback0) matching ACL 102.

```
ASA1/abc2# show xlate detail
1 in use, 2 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
       r - portmap, s - static
TCP PAT from inside:10.1.1.1/45388 to outside(101):192.168.6.61/2902 flags ri

ASA1/abc2# show xlate detail
2 in use, 2 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
       r - portmap, s - static
TCP PAT from inside:192.168.3.11/21305 to outside(102):192.168.6.62/58597 flags ri
```

The following steps illustrate verification for the third task in this question—requiring destination NAT configuration on ASA2.

Verify if NAT control is disabled on ASA2. Then, verify that destination NAT is configured correctly using the **static** command.

There is no need to configure the ACL, because traffic is traversing from a higher-security (inside) interface to a lower-security (outside) interface.

```
ASA2# show run nat-control
no nat-control

ASA2# show run static
static (outside, inside) 192.168.10.6 10.6.6.6 netmask 255.255.255.255

ASA2# show xlate
1 in use, 1 most used
Global 192.168.10.6 Local 10.6.6.6
```

 Please see page 474 for more details.

When this configuration is OK, you can perform verification steps to check its functionality by establishing Telnet sessions from Sw2 to R6 Loopback0 using local IP address 192.168.10.6:

```
Sw2# telnet 192.168.10.6
Trying 192.168.10.6 ... Open

User Access Verification

Password: cisco
R6> exit

[Connection to 192.168.10.6 closed by foreign host]
Sw2#
```

When the Telnet connection is successful, you can simultaneously check the connections table on ASA2 to verify that the connection is indeed established through the firewall and that the Telnet session to destination Loopback0 on R6 IP address 10.6.6.6 (in parentheses) is translated to 192.168.10.6, as per the requirement. The following **show conn** output shows outbound Telnet sessions from Sw2 to R6 Loopback0 being translated. The flags UIO indicate this is an outbound connection.

```
ASA2# show conn
7 in use, 16 most used
TCP outside 192.168.10.6(10.6.6.6):23 inside 192.168.10.11:35199, idle 0:00:15, bytes 111, flags UIO
```

Question 2.2: High-Availability (HA) default route (3 points)

Configure the high-availability (HA) default route on ASA2, meeting the following requirement:

 Please see page 474 for more details.

- ASA2 has a default route configured to R4 Gig0/1 (192.168.9.4) in Question 1.2. Configure a backup default route to R3 Gig0/1 (192.168.9.3) such that it will be installed in the routing table of ASA2 only if Loopback0 on R4 (10.4.4.4) is unreachable. Ensure that the primary default route to 192.168.9.4 is preferred and always installed, unless 10.4.4.4 becomes unreachable by polling it every 5 seconds and sending three packets with each poll before declaring it unreachable. The backup default route should be installed only when 10.4.4.4 is unreachable.

Skills tested

- ☐ Configuring the high-availability (HA) default route using the route-tracking feature on the Cisco ASA firewall

Functionality and solution verification

- ☐ This question can initially seem challenging, because it does not provide any hint that you have to use the route-tracking feature to complete this task. The only clue you may derive from reading the question is when it talks about checking the reachability of 10.4.4.4 every 5 seconds and sending three packets with each poll. This is perhaps the only giveaway in the question that can lead you to configure the route-tracking feature.
- ☐ The static route-tracking feature provides a method for tracking the availability of a static/default route and installing a backup route if the primary route should fail. This allows you to define a default route to gateway1 and a backup default route to a secondary gateway2 in case the primary gateway1 becomes unavailable.
- ☐ First, configure a secondary (backup) default route 0.0.0.0/0 to 192.168.9.3 (R3) with a higher administrative distance of 2 (anything greater than the primary default route). This will ensure that it does not get installed until the primary default 0.0.0.0/0 to 192.168.9.4 (which has a lower administrative distance of 1) is removed from the routing table.
- ☐ Then, configure SLA monitoring with the object-tracking feature to monitor the primary default route using the SLA reachability feature to track the 10.4.4.4 host. If this host is unreachable, the primary default 0.0.0.0/0 is conditionally removed, and the backup default is automatically installed, having the next-best administrative distance of 2.

- To verify the question, shut down Loopback0 on R4 (10.4.4.4), which will trigger the solution to work. Review the outputs shown next.
- You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

First, check that the primary default route is installed on ASA2 to 192.168.9.4 (R4) with an administrative distance of 1:

```
ASA2# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.9.4 to network 0.0.0.0

O E2 192.168.8.0 255.255.255.0 [110/1] via 192.168.9.4, 70:37:17, outside
C    192.168.9.0 255.255.255.0 is directly connected, outside
C    192.168.10.0 255.255.255.0 is directly connected, inside
O E2 172.16.1.0 255.255.255.0 [110/1] via 192.168.9.4, 70:37:17, outside
O    192.168.64.0 255.255.255.0 [110/74] via 192.168.9.4, 70:37:17, outside
O E2 192.168.4.0 255.255.255.0 [110/1] via 192.168.9.4, 70:37:17, outside
O    192.168.65.0 255.255.255.0 [110/138] via 192.168.9.4, 70:37:17, outside
```

 Please see page 474 for more details.

```
                                [110/138] via 192.168.9.3, 70:37:17, outside
O E2 192.168.5.0 255.255.255.0 [110/1] via 192.168.9.4, 70:37:17, outside
O    10.3.3.3 255.255.255.255 [110/11] via 192.168.9.3, 70:37:17, outside
D    10.8.8.0 255.255.255.0 [90/130816] via 192.168.10.11, 70:35:59, inside
O E2 10.7.7.0 255.255.255.0 [110/1] via 192.168.9.4, 70:37:17, outside
O E2 10.2.2.0 255.255.255.0 [110/1] via 192.168.9.4, 70:37:17, outside
O E2 10.1.1.0 255.255.255.0 [110/1] via 192.168.9.4, 70:37:17, outside
O    10.6.6.6 255.255.255.255 [110/75] via 192.168.9.4, 70:37:19, outside
O    10.4.4.4 255.255.255.255 [110/11] via 192.168.9.4, 70:37:19, outside
O    10.5.5.5 255.255.255.255 [110/75] via 192.168.9.3, 70:37:19, outside
O E2 192.168.6.0 255.255.255.0 [110/1] via 192.168.9.4, 70:37:19, outside
O E2 192.168.7.0 255.255.255.0 [110/1] via 192.168.9.4, 70:37:19, outside
O    192.168.35.0 255.255.255.0 [110/74] via 192.168.9.3, 70:37:19, outside
O E2 192.168.2.0 255.255.255.0 [110/1] via 192.168.9.4, 70:37:19, outside
O E2 192.168.3.0 255.255.255.0 [110/1] via 192.168.9.4, 70:37:19, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 192.168.9.4, outside
```

Then, check the ASA2 configuration and verify two default routes (primary and backup) with varying distances. The primary default (with a lower administrative distance) should be configured with the route-tracking feature.

Verify the route-tracking configuration and status using the following commands:

```
ASA2# show run route
route outside 0.0.0.0 0.0.0.0 192.168.9.4 1 track 1
route outside 0.0.0.0 0.0.0.0 192.168.9.3 2

ASA2# show track 1
Track 1
  Response Time Reporter 444 reachability
  Reachability is Up
  9 changes, last change 2d23h
```

```
  Latest operation return code: OK
  Latest RTT (millisecs) 1
  Tracked by:
    STATIC-IP-ROUTING 0

ASA2# show sla monitor configuration 444
IP SLA Monitor, Infrastructure Engine-II.
Entry number: 444
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.4.4.4
Interface: outside
Number of packets: 3
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 5
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

This is how the basic configuration looks:

```
ASA2# show run track
track 1 rtr 444 reachability

ASA2# show run sla monitor
sla monitor 444
 type echo protocol ipIcmpEcho 10.4.4.4 interface outside
 num-packets 3
 frequency 5
sla monitor schedule 444 life forever start-time now
```

When this configuration is OK, you can perform verification steps to check its functionality by shutting down the Loopback0 on R4. Verify that the backup default route to 192.168.9.3 having the next best administrative distance of 2 is installed on ASA2.

You will also notice that network 10.4.4.0/24 is absent from the ASA2 routing table as we shut down Loopback0 on R4.

Also check the operational status of the route-tracking feature on ASA2 using **show sla monitor operational-state**. This will say "Timeout occurred: TRUE," which indicates that the tracked route is unreachable.

```
R4# config term
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)# interface Loopback0
R4(config-if)# shutdown
R4(config-if)#

ASA2# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

 Please see page 474 for more details.

```
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is 192.168.9.3 to network 0.0.0.0

O E2 192.168.8.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:14, outside
C    192.168.9.0 255.255.255.0 is directly connected, outside
C    192.168.10.0 255.255.255.0 is directly connected, inside
O E2 172.16.1.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:14, outside
O    192.168.64.0 255.255.255.0 [110/74] via 192.168.9.4, 0:00:14, outside
O E2 192.168.4.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:14, outside
O    192.168.65.0 255.255.255.0 [110/138] via 192.168.9.4, 0:00:14, outside
                                [110/138] via 192.168.9.3, 0:00:14, outside
O E2 192.168.5.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:14, outside
O    10.3.3.3 255.255.255.255 [110/11] via 192.168.9.3, 0:00:14, outside
D    10.8.8.0 255.255.255.0 [90/130816] via 192.168.10.11, 70:44:19, inside
O E2 10.7.7.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:14, outside
O E2 10.2.2.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:14, outside
O E2 10.1.1.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:14, outside
O    10.6.6.6 255.255.255.255 [110/75] via 192.168.9.4, 0:00:16, outside
O    10.5.5.5 255.255.255.255 [110/75] via 192.168.9.3, 0:00:16, outside
O E2 192.168.6.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:16, outside
O E2 192.168.7.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:16, outside
O    192.168.35.0 255.255.255.0 [110/74] via 192.168.9.3, 0:00:16, outside
O E2 192.168.2.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:16, outside
O E2 192.168.3.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:16, outside
S*   0.0.0.0 0.0.0.0 [2/0] via 192.168.9.3, outside
```

```
ASA2# show sla monitor operational-state 444
Entry number: 444
Modification time: 04:50:22.226 UTC Thu May 28 2009
Number of Octets Used by this Entry: 1480
Number of operations attempted: 119471
Number of operations skipped: 66
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 02:51:32.227 UTC Thu Jun 4 2009
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

Now, unshut the Loopback0 on R4 and check the default route on ASA2. You will notice that it has reverted to the primary default route to 192.168.9.4.

Also check the operational status of route tracking on ASA2 using **show sla monitor operational-state**. This will say "Timeout occurred: FALSE," which indicates that the tracked route is reachable.

```
R4# config term
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)# interface Loopback0
R4(config-if)# no shutdown
R4(config-if)#
```

```
ASA2# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.9.4 to network 0.0.0.0

O E2 192.168.8.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:13, outside
C    192.168.9.0 255.255.255.0 is directly connected, outside
C    192.168.10.0 255.255.255.0 is directly connected, inside
O E2 172.16.1.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:13, outside
O    192.168.64.0 255.255.255.0 [110/74] via 192.168.9.4, 0:00:13, outside
O E2 192.168.4.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:13, outside
O    192.168.65.0 255.255.255.0 [110/138] via 192.168.9.4, 0:00:13, outside
                                [110/138] via 192.168.9.3, 0:00:13, outside
O E2 192.168.5.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:13, outside
O    10.3.3.3 255.255.255.255 [110/11] via 192.168.9.3, 0:00:13, outside
D    10.8.8.0 255.255.255.0 [90/130816] via 192.168.10.11, 70:46:18, inside
O E2 10.7.7.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:13, outside
O E2 10.2.2.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:13, outside
O E2 10.1.1.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:13, outside
O    10.6.6.6 255.255.255.255 [110/75] via 192.168.9.4, 0:00:14, outside
O    10.4.4.4 255.255.255.255 [110/11] via 192.168.9.4, 0:00:14, outside
O    10.5.5.5 255.255.255.255 [110/75] via 192.168.9.3, 0:00:14, outside
```

```
O E2 192.168.6.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:14, outside
O E2 192.168.7.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:14, outside
O    192.168.35.0 255.255.255.0 [110/74] via 192.168.9.3, 0:00:14, outside
O E2 192.168.2.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:14, outside
O E2 192.168.3.0 255.255.255.0 [110/1] via 192.168.9.4, 0:00:14, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 192.168.9.4, outside

ASA2# show sla monitor operational-state 444
Entry number: 444
Modification time: 04:50:22.227 UTC Thu May 28 2009
Number of Octets Used by this Entry: 1480
Number of operations attempted: 119472
Number of operations skipped: 67
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 02:51:52.228 UTC Thu Jun 4 2009
Latest operation return code: OK
RTT Values:
RTTAvg: 1       RTTMin: 1       RTTMax: 1
NumOfRTT: 3     RTTSum: 3       RTTSum2: 3
```

Question 2.3: Cisco IOS Zone Based Policy Firewall (ZFW) (4 points)

Configure Cisco IOS Zone Based Policy Firewall (ZFW) on R5, meeting all the following requirements:

- Configure two zones and security policies for traffic traversing between zones, as shown in Tables 1-14 through 1-16.
- Ensure that you can ping and telnet 192.168.35.3 and .5 from R6.
- Ensure that you can ping and telnet 192.168.65.5 and .6 from R3.

Skills tested

- ☐ Configuring Cisco IOS Zone Based Policy Firewall (ZFW) using advanced protocol inspection
- ☐ Configuring deep packet inspection for application protocols such as HTTP and SMTP and tuning advanced inspection parameters
- ☐ Configuring nested policies

Functionality and solution verification

- ☐ This question is based on the new Cisco IOS Firewall feature called Zone Based Policy Firewall (ZFW), introduced in Cisco IOS Software release 12.4(6)T. ZFW is the new configuration model for the Cisco IOS Firewall feature set. This new configuration model offers intuitive policies for multiple-interface routers and increased granularity of firewall policy application.
- ☐ The basic initial step in this task is to configure the two zones (REMOTE and CENTRAL) and assign the member interfaces as per the table information.
- ☐ The question can then be divided into two subsections. The first is configuration for zone-pair information for traffic traversing from the CENTRAL to REMOTE zone. The second is configuration for zone-pair information for traffic from the REMOTE to CENTRAL zone.

- The major component of this task is configuring security policies for traffic traversing between the zones. Careful planning is required for the number of **class-map**s and **policy-map**s required to fulfill all the requirements. The best approach is to take each protocol and draft its own **class-map** matching the protocol and **policy-map**, applying inspection and any other action (optional) required to apply this traffic.
- Note that ZFW has a default implicit deny policy that prohibits traffic between security zones until an explicit policy is applied to allow desirable traffic. If your configured traffic policies are incorrect, it can impede the functionality of other questions.
- The final step is to configure the zone-pair that ties the security policy to traffic traversing between the zones.
- The question requires you to verify several **ping** tests and establish Telnet sessions to verify the functionality of the ZFW configuration. Review the outputs shown next.
- You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

Before you start verifying the ZFW configuration, ensure that the following ping and Telnet sessions are working successfully. If the verification is OK, proceed to verify the following configuration:

```
R6# ping 192.168.35.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.35.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R6# ping 192.168.35.5
Type escape sequence to abort.
```

 Please see page 474 for more details.

```
Sending 5, 100-byte ICMP Echos to 192.168.35.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R6# telnet 192.168.35.3
Trying 192.168.35.3 ... Open
User Access Verification
Password: cisco
R3>
R3>
R3> exit
[Connection to 192.168.35.3 closed by foreign host]
R6#

R6# telnet 192.168.35.5
Trying 192.168.35.5 ... Open
User Access Verification
Password: cisco
R5>
R5>
R5> exit
[Connection to 192.168.35.5 closed by foreign host]
R6#

R3# ping 192.168.65.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.65.5, timeout is 2 seconds:
!!!!!
```

 Please see page 474 for more details.

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R3# ping 192.168.65.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.65.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R3# telnet 192.168.65.5
Trying 192.168.65.5 ... Open
User Access Verification
Password: cisco
R5>
R5>
R5> exit
[Connection to 192.168.65.5 closed by foreign host]
R3#

R3# telnet 192.168.65.6
Trying 192.168.65.6 ... Open
User Access Verification
Password: cisco
R6>
R6>
R6> exit
[Connection to 192.168.65.6 closed by foreign host]
R3#
```

 Please see page 474 for more details.

When this configuration is OK, you can perform verification steps to check the configuration of ZFW on R5. In summary, two zones, two zone-pairs, and several class-maps and policy-maps are required to fulfill all the requirements in the question.

The following outputs provide further details.

First, check that two zones called REMOTE and CENTRAL are created, and member interfaces Serial0/0/0 and Serial0/0/1 are assigned, respectively:

```
R5# show zone security
zone self
  Description: System defined zone

zone REMOTE
  Member Interfaces:
    Serial0/0/0

zone CENTRAL
  Member Interfaces:
    Serial0/0/1
```

Next, check that the two zone-pair policies have been created for traffic traversing between the zones and applied to the zones just created. The zone names and zone-pair names were provided in the question. Be sure that you use exactly the same naming convention to avoid losing points.

```
R5# show zone-pair security
Zone-pair name central_remote
    Source-Zone CENTRAL  Destination-Zone REMOTE
    service-policy central_remote
Zone-pair name remote_central
    Source-Zone REMOTE  Destination-Zone CENTRAL
    service-policy remote_central
```

As mentioned earlier, the core of this task is configuring the various policies (inspection and action) for traffic traversing between the zones. Next is the main piece of this task.

The first subsection is the configuration for zone-pair information for traffic traversing from the CENTRAL to REMOTE zone. The following outputs illustrate the various class-maps, policy-maps, and actions configured for this subsection.

TABLE 1-23 Requirement: zone pair information for traffic from the CENTRAL to REMOTE zone

Zone-Pair Name	Policy Name	Traffic Action	
central_remote	central_remote	All IP traffic	Inspect all IP traffic.

Only one **policy-map** is configured for this subsection, because the question requires inspection for "all" IP traffic traversing from the CENTRAL to REMOTE zone. This is the most basic and straightforward scenario. Using an IP extended ACL, match all IP traffic, classify it under a **class-map**, and apply the **class-map** to the **policy-map** to inspect all the matched IP traffic. An important note is to remember the naming convention. If the question did not specify, you can use any combination of names to develop your **zone-pair**, **class-map**, and **policy-map**. However, in this task, **policy-map** and **zone-pair** names are provided and must be used in exactly the same manner, or you will lose points. You are free to use any name for **class-map** and any name or number for the ACL.

Also note that the default class-default will always have a drop action. Do not change or modify this unless the question says to, or you will lose points.

```
R5# show policy-map type inspect central_remote
  Policy Map type inspect central_remote
    Class central_remote
      Inspect
    Class class-default
      Drop

R5# show class-map type inspect central_remote
```

```
 Class Map type inspect match-any central_remote (id 1)
   Match access-group  101

R5# show ip access-lists 101
Extended IP access list 101
    10 permit ip any any (126 matches)
```

The second subsection is more complex. You must configure the zone-pair information for traffic traversing from the REMOTE to CENTRAL zone. The following outputs illustrate the various class-maps, policy-maps, and actions configured for this subsection.

TABLE 1-24 Requirement: zone pair information for traffic from the REMOTE to CENTRAL zone

Zone-Pair Name	Policy Name	Protocol	Traffic Actions
remote_central	remote_central	ICMP	Inspect ICMP protocol and apply rate-limit policing to 20000 bps with a burst of 2000 bytes.
		HTTP	Inspect SMTP protocol, and reset connections that misuse the HTTP port for tunneling applications.
		SMTP	Inspect SMTP protocol, and drop (reset connections) emails from a specific email sender, joe@myemail.com, who is sending large file attachments of 10000000 bytes (10MB) and above.
		Telnet and SSH	Inspect all Telnet and SSH sessions.

Three policy-maps are configured in this subsection, because the question requires inspection of varying traffic traversing from the REMOTE to CENTRAL zone. This part of the task is complex and requires some planning.

Five protocols are inspected in this subsection: ICMP, HTTP, SMTP, Telnet, and SSH. Also notice that each protocol has a specific set of requirements. Some require enabling deep packet inspection and actions to be taken in the event of protocol exploit. You can put Telnet and SSH into one group because there is no special requirement except for inspection.

Therefore, you need to create a total of six class-maps: four class-maps to match each individual protocol (ICMP, HTTP, SMTP, and one combined for Telnet and SSH), plus two separate class-maps for deep packet classification. One of these is for HTTP web tunneling abuse (webtunneling), and the other is for SMTP large email abuse (largemail).

Table 1-25 illustrates the six class-maps configured for traffic traversing from the REMOTE to CENTRAL zone.

TABLE 1-25 Class-map configuration for traffic from the REMOTE to CENTRAL zone

Class-Map Name	Traffic	Matching	What It Will Be Called in the Policy-Map
icmp	ICMP	Matching protocol for all ICMP traffic	remote_central
web	HTTP	Matching protocol for all HTTP (TCP port 80) traffic	remote_central
smtp	SMTP	Matching protocol for all SMTP (TCP port 25) traffic	remote_central
other	Telnet and SSH	Matching protocol for all Telnet (TCP port 23) and SSH (TCP port 22) traffic	remote_central
webtunneling	HTTP	Matching HTTP request for port misuse and violation of HTTP port for tunneling applications	dropwebtunneling
largemail	SMTP	Matching email address (using regex) and payload length for deep packet inspection	droplargemail

Here are the six class-maps just mentioned that classify the individual protocols for this subsection:

```
R5# show class-map type inspect
 Class Map type inspect match-all icmp (id 19)
   Match protocol icmp

 Class Map type inspect match-all smtp (id 32)
   Match protocol smtp
```

```
 Class Map type inspect match-any other (id 10)
   Match protocol telnet
   Match protocol ssh

 Class Map type inspect match-any web (id 11)
   Match protocol http

R5# show class-map type inspect http
 Class Map type inspect http match-any webtunneling (id 40)
   Match  request port-misuse tunneling

R5# show class-map type inspect smtp
 Class Map type inspect smtp match-all largemail (id 33)
   Match  sender address regex emailid
   Match  data-length gt 10000000
```

Here is the regex **parameter-map** to classify the email address used for the SMTP deep packet inspection class-map (largemail) just referenced:

```
R5# show parameter-map type regex
parameter-map type regex emailid
 pattern joe@myemail.com
```

When the class-maps are configured, you focus on creating the policy-maps. Three policy-maps are required to complete this subsection. The first policy-map (remote_central) is the parent policy, which is the most important and will be applied to the zone-pair. The other two policy-maps are nested policies used for deep packet inspection—one for HTTP abuse (dropwebtunneling) and another for SMTP abuse (droplargemail). The nested policies are like child policy-maps—those that are referenced under the parent policy-map when enabling deep packet inspection for a given protocol, such as HTTP and SMTP.

Table 1-26 illustrates the three policies configured for traffic traversing from the REMOTE to CENTRAL zone.

TABLE 1-26 Policy-map configuration for traffic from the REMOTE to CENTRAL zone

Policy-Map Name	Traffic	Function	Optional Parameters
remote_central	ICMP, HTTP, SMTP, Telnet, and SSH	Protocol inspection for all traffic matched in the respective class-maps	Apply rate-limit for ICMP traffic to police to 20000 bps with a burst of 2000 bytes. Apply two nested policy-maps to perform deep packet inspection for HTTP and SMTP parameters.
dropwebtunneling	HTTP	Deep packet inspection for HTTP protocol	Reset HTTP connections that misuse the HTTP port for tunneling applications.
droplargemail	SMTP	Deep packet inspection for SMTP protocol	Reset SMTP connections, emails from email sender joe@myemail.com sending large file attachments of 10000000 bytes (10MB) and above.

The following are the three policy-maps just described. As you can see, each policy-map calls its respective class-map configured earlier, and the action is applied accordingly, such as performing inspection and rate limiting and resetting the connection for protocol abuse.

```
R5# show policy-map type inspect remote_central
  Policy Map type inspect remote_central
    Class web
      Inspect
      Service Policy: http dropwebtunneling
    Class icmp
      Inspect
      Police rate 20000 burst 2000
    Class other
      Inspect
    Class smtp
```

```
      Inspect
      Service Policy: smtp droplargemail
    Class class-default
      Drop

R5# show policy-map type inspect http
  Policy Map type inspect http dropwebtunneling
    Class webtunneling
      Reset

R5# show policy-map type inspect smtp
  Policy Map type inspect smtp droplargemail
    Class largemail
      Reset
```

As you can see, ZFW configuration can be quite complex and lengthy to fulfill all requirements laid out in the information table. If you miss one small requirement, you can potentially lose all the points. I strongly recommend practicing ZFW initially with two interfaces, and then three interfaces as things get even more complicated, along with deep packet inspection for each application protocol.

Section 3.0: Cisco VPN (16 Points)

Question 3.1: Configuring Cisco IOS CA Server (3 points)

Configure a Cisco IOS Certificate Authority (CA) server on R1, meeting all the following requirements:

- Configure R1 as the Cisco IOS CA server using the information provided in the following **show** command output:

```
R1# show crypto pki server myCA
Certificate Server myCA:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=myCA.cisco.com
    CA cert fingerprint: DCB2B525 0E99785C 0770EE49 722BDB63
    Granting mode is: auto
    Last certificate issued serial number (hex): 1
    CA certificate expiration timer: 08:56:42 UTC Jun 8 2010
    CRL NextUpdate timer: 14:56:43 UTC Jun 8 2009
    Current primary storage dir: flash:
    Database Level: Complete - all issued certs written as <serialnum>.cer
```

- Configure the lifetime of the certificate server and the certificate issued by the server to one year.
- After the CA server is up, configure ASA2 and R5 as the CA clients, and obtain the certificates on both devices.

Skills tested

☐ Configuring Cisco IOS Certificate Authority Server and obtaining certificates on the Cisco router and ASA firewall

Functionality and solution verification

☐ The objective of this question is pretty straightforward. It requires you to configure the Cisco IOS CA server on R1 and clients R5 and ASA2 to obtain certificates from the server.

☐ An important aspect of this question is how to determine what parameters need to be configured to enable the Cisco IOS CA server on R1. The question provides sample **show** command output and requires you to reverse-engineer the output to configure the server using the information from this output. There are four important things to note in this

output: CA server name (case-sensitive), issuer name, grant mode is set to auto, and complete database storage of all certificate information. Ensure that these four items match the same in your solution. Other parameters can be variable.

- ☐ The question also requires configuring a lifetime of one year for the CA server certificate.
- ☐ When the server setup is done, configure the client devices, and perform the authentication and enrollment steps shown in the following sample output.
- ☐ Remember to open the ACL on the ASA1/abc2 context for CA authentication and enrollment traffic (SCEP using HTTP on TCP port 80) arriving on the outside interface.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

First, check if the CA server is configured correctly and if the server status and state are enabled. If not, you will lose all points.

In addition, check the four parameters mentioned earlier—CA server name, issuer name, grant mode, and database level.

Also check that the validity of the certificate is set to 1 year, and check the start and end dates.

```
R1# show crypto pki server
Certificate Server myCA:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=myCA.cisco.com
    CA cert fingerprint: DCB2B525 0E99785C 0770EE49 722BDB63
    Granting mode is: auto
```

```
    Last certificate issued serial number (hex): 1
    CA certificate expiration timer: 08:56:42 UTC Jun 8 2010
    CRL NextUpdate timer: 14:56:43 UTC Jun 8 2009
    Current primary storage dir: flash:
    Database Level: Complete - all issued certs written as <serialnum>.cer

R1# show crypto pki certificates
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=myCA.cisco.com
  Subject:
    cn=myCA.cisco.com
  Validity Date:
    start date: 08:56:42 UTC Jun 8 2009
    end   date: 08:56:42 UTC Jun 8 2010
  Associated Trustpoints: myCA
  Storage: nvram:myCAciscocom#1CA.cer
```

If the server state is disabled, this means you have not enabled it manually. Similar to the router interface, you need to unshut the server engine to bring it up. This is done in PKI server mode by issuing a **no shutdown** command:

```
R1(config)# crypto pki server myCA
R1(cs-server)# no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password: cisco123
```

 Please see page 474 for more details.

```
Re-enter password: cisco123
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
% Exporting Certificate Server signing certificate and keys...
% Certificate Server enabled.
```

Ensure that you permit TCP port 80 (HTTP) for the certificate enrollment process from client devices to the R1 server. This is a common mistake that candidates make—forgetting to open the firewall ACL. CA authentication fails without the proper error message, resulting in expensive troubleshooting steps during the lab. Be careful with this task.

NOTE
Ensure that you have domain-name and RSA keys generated on both clients before enrolling with the server using the following commands:
ip domain-name cisco.com
crypto key generate rsa

```
ASA1/abc2# show run access-list 100
access-list 100 extended permit icmp any any
access-list 100 extended permit udp host 10.5.5.5 host 10.1.1.1 eq ntp
access-list 100 extended permit udp host 192.168.9.10 host 10.1.1.1 eq ntp
access-list 100 extended permit tcp any host 10.1.1.1 eq www
```

The following outputs show the authentication and enrollment steps on client devices, demonstrating how to obtain a certificate from the server:

```
R5(config)# crypto pki authenticate cisco
Certificate has the following attributes:
       Fingerprint MD5: DCB2B525 0E99785C 0770EE49 722BDB63
      Fingerprint SHA1: 42742DE9 26D9C893 A028CBD6 C314113D 27023BB4

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

R5(config)# crypto pki enroll cisco
%
```

```
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password: cisco123
Re-enter password: cisco123

% The subject name in the certificate will include: R5.cisco.com
% The serial number in the certificate will be: FTX0911C0TD
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate cisco verbose' command will show the fingerprint.

Jun  8 12:23:11.019: CRYPTO_PKI:  Certificate Request Fingerprint MD5: BD10BA21 90F71835 5532A5CA A839AC61
Jun  8 12:23:11.019: CRYPTO_PKI:  Certificate Request Fingerprint SHA1: 13A9DE1F 93FA96F1 7262A704 B4F6713F
ECDED9CA
Jun  8 12:23:12.674: %PKI-6-CERTRET: Certificate received from Certificate Authority
R5(config)# exit
R5#

ASA2(config)# crypto ca authenticate cisco
INFO: Certificate has the following attributes:
Fingerprint:     dcb2b525 0e99785c 0770ee49 722bdb63
Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

 Please see page 474 for more details.

```
ASA2(config)# crypto ca enroll cisco
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password: cisco123
Re-enter password: cisco123

% The fully-qualified domain name in the certificate will be: ASA2.cisco.com
% The serial number in the certificate will be: JMX0947K0SW

Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
ASA2(config)#
ASA2(config)# The certificate has been granted by CA!
ASA2(config)#
```

Check both client devices, ASA2 and R5, to ensure that they have received a certificate from the CA server. Each device has two certificates: one from the CA server itself for CA Signature purposes, and a general-purpose certificate issued to this specific device. Also note that the duration (lifetime) of these certificates is one year.

```
ASA2# show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 03
  Certificate Usage: General Purpose
  Public Key Type: RSA (1024 bits)
  Issuer Name:
```

```
    cn=myCA.cisco.com
  Subject Name:
    serialNumber=JMX0947K0SW+hostname=ASA2.cisco.com
  Validity Date:
    start date: 10:19:25 UTC Jun 8 2009
    end   date: 08:56:42 UTC Jun 8 2010
  Associated Trustpoints: cisco

CA Certificate
  Status: Available
  Certificate Serial Number: 01
  Certificate Usage: Signature
  Public Key Type: RSA (1024 bits)
  Issuer Name:
    cn=myCA.cisco.com
  Subject Name:
    cn=myCA.cisco.com
  Validity Date:
    start date: 08:56:42 UTC Jun 8 2009
    end   date: 08:56:42 UTC Jun 8 2010
  Associated Trustpoints: cisco


ASA2# show crypto key mypubkey rsa
Key pair was generated at: 10:18:13 UTC Jun 8 2009
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 1024
 Key Data:
```

 Please see page 474 for more details.

```
  30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00b6c056
  75ff65ed 70a65c30 4196aef4 89e00b87 f286ad93 90a0d845 de16c535 a84fcbab
  f99b3be9 240b7268 95c75c74 072f0471 566df202 6333c306 9378cdb7 676e1c47
  7fbc9f14 b42003b1 17fd8b38 eeab5b2a 0bdd673d 66fe3103 ae2c9a14 b28f1e23
  7472344a a8bc86e1 fc1fcddc 926ef6eb aebff06a 1c8c9908 1826151a d7020301 0001


R5# show crypto pki certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 02
  Certificate Usage: General Purpose
  Issuer:
    cn=myCA.cisco.com
  Subject:
    Name: R5.cisco.com
    Serial Number: FTX0911C0TD
    serialNumber=FTX0911C0TD+hostname=R5.cisco.com
  Validity Date:
    start date: 10:16:43 UTC Jun 8 2009
    end   date: 08:56:42 UTC Jun 8 2010
  Associated Trustpoints: cisco
  Storage: nvram:myCAciscocom#2.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=myCA.cisco.com
```

```
  Subject:
    cn=myCA.cisco.com
  Validity Date:
    start date: 08:56:42 UTC Jun 8 2009
    end   date: 08:56:42 UTC Jun 8 2010
  Associated Trustpoints: cisco
  Storage: nvram:myCAciscocom#1CA.cer

R5# show crypto key mypubkey rsa
% Key pair was generated at: 10:15:49 UTC Jun 8 2009
Key name: R5.cisco.com
 Storage Device: private-config
 Usage: General Purpose Key
 Key is exportable.
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00B21A49 381946E7
  9C25D6E1 209DD7D6 773E60C2 101AA063 DAA6963E B57C0EA0 29AE2664 CBA21B6A
  5A2BD509 2F08BB27 7259D731 A5FA8228 20F901E3 34050D3A FF020301 0001
% Key pair was generated at: 11:15:50 UTC Jun 8 2009
Key name: R5.cisco.com.server
Temporary key
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00B10F19 7F61CD71
  1FB0CA3B 38EDD91B EBE6681D 1CFF229F 516A2FD2 EC6391E1 718C4BF9 A93AC7C6
  7528A5EF E1A554BE D017B919 2A4F0670 DA008A8C 2CDFA66C AD4156D7 49B694BA
  BF5977FB 3BCBE0BE 8E10CCDD D5EA52B5 39C3A2BF E570B95A 79020301 0001
```

 Please see page 474 for more details.

Question 3.2: Configuring a LAN-to-LAN IPsec tunnel using digital certificates (4 points)

Configure a LAN-to-LAN (L2L) IPsec tunnel using certificates between ASA2 and R5, meeting all the following requirements:

- Configure the IPsec tunnel on ASA2 and R5, protecting host-to-host IPsec interesting traffic between Loopback0 of both Sw2 and R5.
- Use the certificates obtained in the preceding question to perform ISAKMP authentication.
- Configure ISAKMP profile configuration on R5, and associate this profile to the crypto map. Configure a certificate attribute map that performs two validation checks: the certificate issuer-name contains string "myCA," and the subject name contains string "ASA2." The ISAKMP authentication should fail if either condition is mismatched.
- Configure high-availability IPsec peering in such a way that it should continue to work if either WAN link on R5 (Serial0/0/0 or Serial0/0/1) goes down. You are not allowed to configure multiple crypto maps or multiple peer statements. Only one crypto map with one peer statement is allowed on both sides.

Skills tested

- ☐ Configuring a LAN-to-LAN IPsec tunnel using CA issued certificates between the Cisco router and Cisco ASA firewall
- ☐ Configuring an ISAKMP profile for Phase 1 authentication
- ☐ Configuring a certificate attribute map to perform validation checks using parameters from the certificate, such as issuer name, subject name, and so on
- ☐ Designing high-availability IPsec peering without creating multiple crypto maps and multiple peer statements using the local-address feature

Functionality and solution verification

- ☐ This question may seem straightforward in configuring a basic LAN-to-LAN IPsec tunnel. However, some important requirements laid out in the question need careful attention.
- ☐ The first and most important requirement is to use CA issued certificates from Question 3.1. If you are unable to get the CA setup working, you may end up losing points for both Questions 3.1 and 3.2.
- ☐ The second important requirement is to use an ISAKMP profile. Again, this may seem straightforward in a regular preshared key-type scenario, but when you use certificates, additional steps must be followed.
- ☐ The third special requirement is to perform some validation checks on the recipient certificate to ensure that the certificate match is correct using the issuer name and subject name data from the ISAKMP authentication process. This can be achieved using a certificate map on R5 to match the specified attributes applied in the ISAKMP profile.
- ☐ The fourth and perhaps most important requirement is to design a high-availability peering configuration. IPsec tunnel peers should be seamless and should always continue to work if either of the WAN links on R5 (Serial0/0/0 or Serial0/0/1) goes down. You cannot use multiple crypto maps or multiple peer statements on both sides; only one crypto map with one peer statement is allowed on both sides. You can use the local-address feature on R5 and configure a loopback address on R5. On ASA2, the IPsec peering IP address and tunnel-group configuration should use the new loopback of R5 instead of the physical link.
- ☐ The question also clearly says to encrypt traffic between Loopback0 of both R5 and Sw2. Therefore, the IPsec interesting traffic ACL should be a host-to-host /32 ACL, not a /24.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

As mentioned earlier, the first core requirement is to use CA issued certificates from Question 3.1. If you are unable to get the CA setup working, you may end up losing points for both Questions 3.1 and 3.2. Ensure that both sides, ASA2 and R5, have the required certificates.

Then check the configuration on R5 to ensure that all the following requirements are met:

- The ISAKMP policy is configured to use certificates (rsa-sig).
- The ISAKMP profile is configured and applied in the crypto map.
- Only one crypto map is found using one peer statement.
- The crypto map is using the local-address feature for high availability. This requires configuring a new Loopback1 interface on R5 (for peering) using any IP address. Advertise this Loopback1 into OSPF area 0 so that it is routable throughout the network. Ensure that ASA2 can ping this Loopback1 address.
- The IPsec ACL is matching host-to-host for traffic between Loopback0 on R5 and Sw2.
- The IPsec peer is set to ASA2 outside interface IP address 192.168.9.10.
- The crypto map is applied to both WAN interfaces (Serial0/0/0 and Serial0/0/1).
- The certificate attribute map is configured to perform a validation check that the issuer name contains string "myCA" and that the subject name contains the string "ASA2."
- The CA trustpoint name and certificate attribute map are both referenced in the ISAKMP profile.

NOTE
If any one parameter of these requirements is mismatched or incorrect, you will lose all points.

The following **show** outputs from R5 can be used to verify all the preceding requirements:

```
R5# show run ¦ sec crypto pki trustpoint
crypto pki trustpoint cisco
 enrollment url http://10.1.1.1:80
 serial-number
 revocation-check none
```

```
R5# show crypto isakmp policy
Global IKE policy
Protection suite of priority 10
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit

R5# show crypto isakmp profile
ISAKMP PROFILE isakmpprofile
Ref Count = 2
   Identities matched are:
   Certificate maps matched are:
      mycert
   keyring(s): <none>
   trustpoint(s): cisco

R5# show crypto map
Crypto Map: "cisco" idb: Loopback1 local address: 192.168.55.5
Crypto Map "cisco" 10 ipsec-isakmp
        Peer = 192.168.9.10
        ISAKMP Profile: isakmpprofile
        Extended IP access list 109
            access-list 109 permit ip host 10.5.5.5 host 10.8.8.8
        Current peer: 192.168.9.10
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
```

```
        cisco:  { esp-3des esp-sha-hmac  } ,
    }
    Interfaces using crypto map cisco:
        Serial0/0/0
        Serial0/0/1

ASA2# ping 192.168.55.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.55.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms

R5# show run ¦ sec crypto pki certificate map
crypto pki certificate map mycert 10
 issuer-name co myca
 subject-name co asa2

R5# show run ¦ sec crypto isakmp profile
crypto isakmp profile isakmpprofile
   ca trust-point cisco
   match certificate mycert
```

TIP

An important point to remember is that you need to configure R5 for the ISAKMP identity to use the **dn** keyword using the **crypto isakmp identity dn** command. This is one of the major reasons for certificate-based authentication not working on the router. However, on ASA2, you need to enable the **crypto isakmp identity auto** command, which is also the default on the Cisco ASA firewall. This sets the identity to be automatically determined by the connection type: IP address for the preshared key, and Cert DN for Cert-based connections.

Then check the configuration on ASA2 to ensure the following:

- The ISAKMP policy is configured to use certificates (rsa-sig).
- Only one crypto map is found using one peer statement.
- The IPsec ACL is matching host-to-host for traffic between Loopback0 on R5 and Sw2.
- The IPsec peer is set to the new Loopback1 interface 192.168.55.5 (not the physical serial WAN IP address).

- The crypto map is applied to the outside interface.
- The CA trustpoint name is applied to both the tunnel-group and crypto map.

NOTE
If any of these parameters are mismatched or even slightly incorrect, you will lose all points.

The following **show** outputs from R5 can be used to verify all the preceding requirements:

```
ASA2# show run crypto ca trustpoint
crypto ca trustpoint cisco
 enrollment url http://10.1.1.1:80
 serial-number
 crl configure

ASA2# show run crypto isakmp
crypto isakmp enable outside
crypto isakmp policy 10
 authentication rsa-sig
 encryption 3des
 hash md5
 group 2
 lifetime 86400

ASA2# show run crypto map
crypto map cisco 10 match address 101
crypto map cisco 10 set peer 192.168.55.5
crypto map cisco 10 set transform-set cisco
crypto map cisco 10 set security-association lifetime seconds 28800
crypto map cisco 10 set security-association lifetime kilobytes 4608000
crypto map cisco 10 set trustpoint cisco
crypto map cisco interface outside
```

```
ASA2# show access-list 101
access-list 101; 1 elements
access-list 101 line 1 extended permit ip host 10.8.8.8 host 10.5.5.5 (hitcnt=209)

ASA2# show run tunnel-group
tunnel-group 192.168.55.5 type ipsec-l2l
tunnel-group 192.168.55.5 ipsec-attributes
 trust-point cisco
```

When this configuration is OK, you can perform a ping test to verify if the IPsec tunnel comes up.

Initiate a ping test from Sw2 to Loopback0 of R5 (10.5.5.5) using source address Loopback0 (10.8.8.8).

NOTE
You can also enable ISAKMP debugging to see the packet flow and troubleshoot any problems.

If the ping is successful, check the ISAKMP and IPsec SA outputs on both devices to ensure that the tunnel is working properly.

The following outputs provide verification:

```
Sw2# ping 10.5.5.5 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.5.5, timeout is 2 seconds:
Packet sent with a source address of 10.8.8.8
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/4/9 ms

R5# ping 10.8.8.8 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 10.5.5.5
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
```

NOTE

Sometimes you will notice that the src and dst addresses are flipped from the context of R5. R5 should show the src as 192.168.55.5 and dst as 192.168.9.10. This is a cosmetic issue; do not worry about it. This cosmetic error is seen only in this output; the following IPsec SA output is OK.

```
R5# show ip access-lists 109
Extended IP access list 109
    10 permit ip host 10.5.5.5 host 10.8.8.8 (1450 matches)

R5# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.55.5    192.168.9.10    QM_IDLE           1071 ACTIVE
R5# show crypto ipsec sa
     PFS (Y/N): N, DH group: none
     PFS (Y/N): N, DH group: none

interface: Serial0/0/0
    Crypto map tag: cisco, local addr 192.168.55.5

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.5.5.5/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.8.8.8/255.255.255.255/0/0)
   current_peer 192.168.9.10 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 209, #pkts encrypt: 209, #pkts digest: 209
    #pkts decaps: 209, #pkts decrypt: 209, #pkts verify: 209
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.55.5, remote crypto endpt.: 192.168.9.10
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x174FD227(391107111)
```

 Please see page 474 for more details.

```
     inbound esp sas:
      spi: 0x91ECAA94(2448206484)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2067, flow_id: Onboard VPN:67, sibling_flags 80000046, crypto map: cisco
        sa timing: remaining key lifetime (k/sec): (4507980/3428)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x174FD227(391107111)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2068, flow_id: Onboard VPN:68, sibling_flags 80000046, crypto map: cisco
        sa timing: remaining key lifetime (k/sec): (4507980/3428)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

interface: Serial0/0/1
    Crypto map tag: cisco, local addr 192.168.55.5
```

```
protected vrf: (none)
local  ident (addr/mask/prot/port): (10.5.5.5/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.8.8.8/255.255.255.255/0/0)
current_peer 192.168.9.10 port 500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 209, #pkts encrypt: 209, #pkts digest: 209
 #pkts decaps: 209, #pkts decrypt: 209, #pkts verify: 209
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0

  local crypto endpt.: 192.168.55.5, remote crypto endpt.: 192.168.9.10
  path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
  current outbound spi: 0x174FD227(391107111)

  inbound esp sas:
   spi: 0x91ECAA94(2448206484)
     transform: esp-3des esp-sha-hmac ,
     in use settings ={Tunnel, }
     conn id: 2067, flow_id: Onboard VPN:67, sibling_flags 80000046, crypto map: cisco
     sa timing: remaining key lifetime (k/sec): (4507980/3428)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE

  inbound ah sas:

  inbound pcp sas:
```

 Please see page 474 for more details.

```
     outbound esp sas:
      spi: 0x174FD227(391107111)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2068, flow_id: Onboard VPN:68, sibling_flags 80000046, crypto map: cisco
        sa timing: remaining key lifetime (k/sec): (4507980/3428)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

R5# show crypto engine connections active
Crypto Engine Connections

   ID  Type    Algorithm           Encrypt  Decrypt IP-Address
 1071  IKE     MD5+3DES                  0        0 192.168.55.5
 2067  IPsec   3DES+SHA                  0      209 192.168.55.5
 2068  IPsec   3DES+SHA                209        0 192.168.55.5

ASA2# show crypto isakmp sa

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.55.5
    Type    : L2L             Role    : initiator
```

 Please see page 474 for more details.

```
    Rekey   : no                State   : MM_ACTIVE

ASA2# show crypto ipsec sa
interface: outside
    Crypto map tag: cisco, seq num: 10, local addr: 192.168.9.10

      access-list 101 permit ip host 10.8.8.8 host 10.5.5.5
      local ident (addr/mask/prot/port): (10.8.8.8/255.255.255.255/0/0)
      remote ident (addr/mask/prot/port): (10.5.5.5/255.255.255.255/0/0)
      current_peer: 192.168.55.5

      #pkts encaps: 209, #pkts encrypt: 209, #pkts digest: 209
      #pkts decaps: 209, #pkts decrypt: 209, #pkts verify: 209
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 209, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.9.10, remote crypto endpt.: 192.168.55.5

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 91ECAA94

    inbound esp sas:
      spi: 0x174FD227 (391107111)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 237568, crypto-map: cisco
         sa timing: remaining key lifetime (kB/sec): (4373979/3446)
```

 Please see page 474 for more details.

```
         IV size: 8 bytes
         replay detection support: Y
Anti replay bitmap:
        0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0x91ECAA94 (2448206484)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 237568, crypto-map: cisco
         sa timing: remaining key lifetime (kB/sec): (4373979/3446)
         IV size: 8 bytes
         replay detection support: Y
Anti replay bitmap:
        0x00000000 0x00000001
```

The next step is to verify the high-availability IPsec peering, as discussed earlier.

If all configurations are OK, you can test this simply by shutting down the PPP link between R3 and R5 (shut down R3 Serial0/0/0).

Wait a few seconds for routing to converge via the Frame Relay link, and ensure that R5 has the route (for Loopback0 of Sw2) via R6.

Similarly, ASA2 should have the route (for Loopback0 of R5) via R4 now.

Clear the ISAKMP and IPsec tunnel on R5 to ensure that no tunnel exists in the DB.

Initiate another ping test from Sw2 to Loopback0 of R5 (10.5.5.5) using source address Loopback0 (10.8.8.8).

If the ping is successful, check the ISAKMP and IPsec SA outputs on both devices to ensure that the tunnel is working properly.

The following outputs provide verification:

```
R3# conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# interface Serial 0/0/0
R3(config-if)# shutdown
R3(config-if)# end
R3#

R5# show ip route ¦ inc 10.8.8.
O E2    10.8.8.0/24 [110/1] via 192.168.65.6, 00:00:15, Serial0/0/1

ASA2# show route ¦ inc 10.5.5.
O    10.5.5.5 255.255.255.255 [110/139] via 192.168.9.4, 0:00:25, outside

Sw2# ping 10.5.5.5 source loopback 0 repeat 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 10.5.5.5, timeout is 2 seconds:
Packet sent with a source address of 10.8.8.8
.!!!!!!!!!
Success rate is 90 percent (9/10), round-trip min/avg/max = 1/5/9 ms

R5# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.55.5    192.168.9.10    QM_IDLE           1002 ACTIVE

R5# show crypto engine connections active
Crypto Engine Connections
```

```
  ID  Type    Algorithm          Encrypt  Decrypt IP-Address
1002  IKE     MD5+3DES                 0        0 192.168.55.5
2003  IPsec   3DES+SHA                 0        9 192.168.55.5
2004  IPsec   3DES+SHA                 9        0 192.168.55.5
```

Remember to unshut the R3 interface Serial0/0/0 when done:

```
R3# conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# interface Serial 0/0/0
R3(config-if)# no shutdown
R3(config-if)# end
R3#
```

Question 3.3: Troubleshooting DMVPN (3 points)

Dynamic Multipoint VPN (DMVPN) has been preconfigured in this question. Your task is to troubleshoot and identify the injected faults and bring up the DMVPN tunnels, meeting all the following requirements:

- DMVPN is preconfigured between R1, R2, and R4 in a single DMVPN cloud with a static hub-to-spoke and dynamic spoke-to-spoke scenario. R1 is Hub1, with R2 and R4 being the spokes connecting to the hub.
- A single multipoint GRE (mGRE) tunnel interface is preconfigured on each router.
- Five faults are injected into your preconfiguration. Identify these faults, and verify that tunnels are established. Note that the faults injected could be either related to incorrect preconfiguration or missing commands to complete the configuration.
- Open the ACL on the ASA1/abc2 context, allowing IPsec traffic entering the outside interface. This task excludes the five faults.

 Please see page 474 for more details.

- Ensure that each spoke has a permanent IPsec tunnel to the hub. Also ensure that spoke-to-spoke tunnels will be established on demand when traffic between the spokes will traverse directly bypassing the hub using the dynamically established spoke-to-spoke tunnel.
- While fixing this issue, you are allowed to alter the preconfiguration and add, modify, or remove part of the preconfiguration. However, you need to ensure that altering the preconfiguration does not impede any other question.
- For verification, perform the following ping test, and ensure that the following routing table outputs match your result:

```
R1# ping 22.22.22.22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 22.22.22.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms

R1# ping 44.44.44.44
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 44.44.44.44, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

R2# ping 44.44.44.44
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 44.44.44.44, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

R4# ping 22.22.22.22
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 22.22.22.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1# show ip route eigrp 100
     22.0.0.0/24 is subnetted, 1 subnets
D       22.22.22.0 [90/2969600] via 172.1.0.2, 00:03:44, Tunnel1
     44.0.0.0/24 is subnetted, 1 subnets
D       44.44.44.0 [90/2969600] via 172.1.0.4, 00:03:44, Tunnel1

R2# show ip route eigrp 100
     11.0.0.0/32 is subnetted, 1 subnets
D       11.11.11.11 [90/2969600] via 172.1.0.1, 00:03:23, Tunnel1
     44.0.0.0/24 is subnetted, 1 subnets
D       44.44.44.0 [90/3251200] via 172.1.0.4, 00:03:23, Tunnel1

R4# show ip route eigrp 100
     22.0.0.0/24 is subnetted, 1 subnets
D       22.22.22.0 [90/3251200] via 172.1.0.2, 00:03:34, Tunnel1
     11.0.0.0/32 is subnetted, 1 subnets
D       11.11.11.11 [90/2969600] via 172.1.0.1, 00:03:34, Tunnel1
```

NOTE

As mentioned in the CCIE lab exam blueprint, "Knowledge of troubleshooting is an important skill, and candidates are expected to diagnose and solve issues as part of the CCIE lab exam." The new v3.0 lab exam strongly enforces this aspect. The new lab exam will be just as challenging and will validate both configuration and troubleshooting skills. Candidates must practice troubleshooting methods and techniques as an important skill set to be successful.

Skills tested

- ☐ Troubleshooting DMVPN technology in a real-time environment
- ☐ Identifying network-related issues within an existing topology that has been preconfigured

Functionality and solution verification

- ☐ This new format of questions is very different from the traditional configuration-based questions. The objective is to test the candidate's analytical skills in a complex environment where an engineer applies his or her troubleshooting skills to fix networking-related problems using a methodological approach with the aid of various tools. Extensive knowledge of **show** and **debug** commands is very important in these scenarios.
- ☐ A basic approach to solving this type of question is to break it into layers, such as IP connectivity, routing, switching, ISAKMP phase 1, ISAKMP phase 2, and NHRP-related issues, to name a few. As just mentioned, use a methodological approach. Also important is breaking the issue into smaller parts. For example, in this question you should check the functionality between spoke1 and the hub, between spoke2 and the hub, between spoke1 and spoke2, and so on. Start by reviewing the current preconfiguration using **show** commands. If you cannot find anything unusual, enable relevant **debugs** to get more details.
- ☐ The issues that were injected into the preconfiguration are discussed next.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

You can use several methods and varying techniques to start troubleshooting. There is no perfect method. Every person has different methodologies and uses a different approach. As long as the main objective is met, it is OK to use your own method. Earlier I described a basic approach and how to use it to your advantage.

Here is a list of five faults injected into your preconfiguration:

- Fault 1 can be found on Sw1. A VLAN access control list (VACL) has been preconfigured and applied to VLAN 4 (R2 GigabitEthernet0/0 is in VLAN 4). It drops all IP packets sourced from R2 GigabitEthernet0/0 to destination R1 GigabitEthernet0/0 and destination R4 Serial0/0/0. These are essentially the IPsec tunnel endpoints for establishing the DMVPN tunnel. To fix this issue, simply remove the VACL using the **no vlan filter abc vlan-list 4** command.

- Fault 2 can be found on R2. The tunnel key under Interface Tunnel 1 is incorrect; it should be **tunnel key 11**, not 1. You can fix this by changing the tunnel key to 11.
- Fault 3 can be found on R4. The **ip nhrp network-id 11** command is missing under Interface Tunnel 1 on R4. Add this command to match the hub network-id.
- Fault 4 can also be found on R4. The static map **ip nhrp map 192.168.3.11 172.1.0.1** for destination IP addresses to NBMA addresses under Interface Tunnel 1 is incorrect. Remove this using the **no** command and replace it with **ip nhrp map 172.1.0.1 192.168.3.11**. The IP addresses were swapped in this fault.
- Fault 5 can be found on R1. The **no ip next-hop-self eigrp 100** command is missing under Interface Tunnel 1 on R1. This command is important for the EIGRP next-hop IP address on the spokes. The question clearly shows the routing table outputs for EIGRP AS 100, which shows that spokes subnets have their next hop to the spoke IP address, not the hub. This fault directly impacts one of the requirements laid out in the question. It says to ensure that spoke-to-spoke tunnels should be established on demand when traffic between the spokes will directly bypass the hub using the dynamically established spoke-to-spoke tunnel. Also note that this fault does not impede the functionality of DMVPN. If you are unable to find this fault, the tunnels would still work. However, the next hop for the spoke subnets would show the hub IP address, and spoke-to-spoke traffic would traverse indirectly via the hub, making a U-turn. And this would not satisfy the question's requirement.

As soon as all five faults are found and fixed, perform the following ping tests and verify the routing table accordingly on all three routers—R1, R2, and R4.

```
R1# ping 22.22.22.22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 22.22.22.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms

R1# ping 44.44.44.44
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 44.44.44.44, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

R2# ping 44.44.44.44
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 44.44.44.44, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

R4# ping 22.22.22.22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 22.22.22.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1# show ip route eigrp 100
     22.0.0.0/24 is subnetted, 1 subnets
D       22.22.22.0 [90/2969600] via 172.1.0.2, 00:03:44, Tunnel1
     44.0.0.0/24 is subnetted, 1 subnets
D       44.44.44.0 [90/2969600] via 172.1.0.4, 00:03:44, Tunnel1

R2# show ip route eigrp 100
     11.0.0.0/32 is subnetted, 1 subnets
D       11.11.11.11 [90/2969600] via 172.1.0.1, 00:03:23, Tunnel1
     44.0.0.0/24 is subnetted, 1 subnets
D       44.44.44.0 [90/3251200] via 172.1.0.4, 00:03:23, Tunnel1

R4# show ip route eigrp 100
     22.0.0.0/24 is subnetted, 1 subnets
```

 Please see page 474 for more details.

```
D       22.22.22.0 [90/3251200] via 172.1.0.2, 00:03:34, Tunnel1
     11.0.0.0/32 is subnetted, 1 subnets
D       11.11.11.11 [90/2969600] via 172.1.0.1, 00:03:34, Tunnel1
```

In addition, check the ISAKMP SA using the **show crypto isakmp sa** output and IPsec SA using the **show crypto ipsec sa** output to ensure that tunnels are established properly. Verify that encrypt and decrypt counters are incrementing using the **show crypto engine connections active** command on all three devices.

Question 3.4: Configuring Group Encrypted Transport VPN (GETVPN) (3 points)

Configure Group Encrypted Transport VPN (GETVPN) on R1, R3, and R6, meeting all the following requirements:

- Configure GETVPN using preshared keys on R1, R3, and R6 using the information in Tables 1-17 and 1-18.
- Use “cisco” for the preshared key on all devices.
- R1 will be the Key Server (KS), and R3 and R6 will be the Group Members (GM).
- Interface Loopback10 in subnet 172.17.0.0/16 has been preconfigured on R3 and R6 GMs.

Skills tested

- ☐ Configuring Group Encrypted Transport VPN (GETVPN) using preshared keys
- ☐ Understanding the Group Domain of Interpretation (GDOI) protocol and how it works
- ☐ Enabling ISAKMP and IPsec parameters to support GETVPN

Functionality and solution verification

- ☐ Group Encrypted Transport VPN (GETVPN) is a debut technology in the new CCIE Security v3.0 lab blueprint. GETVPN is one of the important technologies, so candidates should be well-prepared.
- ☐ The objective is to configure GETVPN on three routers: R1 as the KS, and R3 and R6 as the GMs.
- ☐ Configure ISAKMP and IPsec policy as per the table information using preshared keys (PSK) using "cisco." IPsec transform sets and profile configurations are not required on GMs. These parameters are pushed down by the KS as part of GDOI registration. Only ISAKMP configurations are required to enable a GM and KS to authenticate each other.
- ☐ Remember that, when using the preshared key authentication method, you only need to configure the preshared key on each GM to authenticate the KS. You don't need to define the preshared key to authenticate other GMs.
- ☐ Ensure that the GDOI group name, number, and profile name match, as required in the information table. When configuring GMs, remember to use the same group identity defined on the KS and the IP address of the KS, as mentioned in the information table.
- ☐ The **crypto map** command has a new type called **gdoi** that is tied to the GDOI group on the GM; refer to the following GM sample output from R3 and R6.
- ☐ Finally, don't forget to apply the **crypto map** (not required on KS) on the GMs R3 Gig0/1 and R6 (Se0/0/0) interfaces. The important decision is which interface you should apply the **crypto map** to on R6 (whether Gig0/1, which is facing the KS, or Se0/0/0, which is facing the GM). The fundamental of choosing where to apply **crypto map** is to apply it on the interface where encrypted traffic is arriving/departing (as per the routing table). In other words, apply **crypto map** on the interface where the encrypt/decrypt process will occur. Therefore, you must apply **crypto map** on R6 Se0/0/0, which is facing the GM.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

Table 1-27 provides information that needs to be configured on the KS (R1). Use the following sample outputs from R1 to ensure that all requirements have been met.

TABLE 1-27 Configuration information for the key server (KS)

ISAKMP Policy	☐ Preshared key authentication ☐ AES (Advanced Encryption Standard) encryption algorithm ☐ MD5 (Message Digest 5) hash algorithm ☐ Diffie-Hellman group 2
IPsec Policy	☐ ESP transform using AES cipher ☐ ESP transform using HMAC-SHA authentication ☐ IPsec profile name is gdoi_profile. ☐ Set IPsec SA lifetime to 10 hours
GDOI Parameters	☐ Group name is lab1getvpn. ☐ Group identity number is 123. ☐ Unicast Rekey transport with two retransmits at 30-second intervals ☐ Rekey lifetime to 24 hours. ☐ Enable time-based antireplay check to 10 seconds.
Access List Policies	☐ Traffic to be encrypted between 172.17.0.0/16 network address range to communicate using GETVPN

```
R1# show crypto isakmp policy
Global IKE policy
Protection suite of priority 10
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 20
```

```
        encryption algorithm:    AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:          Message Digest 5
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #2 (1024 bit)
        lifetime:                86400 seconds, no volume limit

R1# show crypto gdoi ks policy
Key Server Policy:
For group lab1getvpn (handle: 2147483650) server 192.168.3.11 (handle: 2147483650):

  # of teks : 1  Seq num : 0
  KEK POLICY (transport type : Unicast)
    spi : 0xE81D1709EE0A3F3FD0FC0C931D7AB035
    management alg     : disabled    encrypt alg       : 3DES
    crypto iv length   : 8           key size          : 24
    orig life(sec): 86400       remaining life(sec): 82572
    sig hash algorithm : enabled     sig key length    : 162
    sig size           : 128
    sig key name       : gdoikeys

  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0x86305AEB    access-list           : 101
    # of transforms    : 0             transform             : ESP_AES
    hmac alg           : HMAC_AUTH_SHA
    alg key size       : 16            sig key size          : 20
    orig life(sec)     : 36000         remaining life(sec)   : 32173
    override life (sec): 0             antireplay window size: 10
  Replay Value 4322.95 secs
```

 Please see page 474 for more details.

```
R1# show run ¦ section crypto ipsec transform-set
crypto ipsec transform-set cisco esp-3des esp-md5-hmac
 mode transport
crypto ipsec transform-set gdoitrans esp-aes esp-sha-hmac

R1# show crypto ipsec profile gdoi_profile
IPSEC profile gdoi_profile
        Security association lifetime: 4608000 kilobytes/36000 seconds
        PFS (Y/N): N
        Transform sets={
                gdoitrans:  { esp-aes esp-sha-hmac  } ,
        }

R1# show run ¦ section crypto gdoi
crypto gdoi group lab1getvpn
 identity number 123
 server local
  rekey retransmit 30 number 2
  rekey authentication mypubkey rsa gdoikeys
  rekey transport unicast
  sa ipsec 1
   profile gdoi_profile
   match address ipv4 101
   replay time window-size 10
  address ipv4 192.168.3.11

R1# show crypto gdoi ks acl
Group Name: lab1getvpn
 Configured ACL:
   access-list 101 permit ip 172.17.0.0 0.0.255.255 172.17.0.0 0.0.255.255
```

 Please see page 474 for more details.

```
R1# show crypto gdoi ks rekey
Group lab1getvpn (Unicast)
    Number of Rekeys sent               : 0
    Number of Rekeys retransmitted      : 0
    KEK rekey lifetime (sec)            : 86400
        Remaining lifetime (sec)        : 82510
    Retransmit period                   : 30
    Number of retransmissions           : 2
    IPSec SA 1  lifetime (sec)          : 36000
        Remaining lifetime (sec)        : 32111

R1# show crypto gdoi ks members
Group Member Information :
Number of rekeys sent for group lab1getvpn : 0

Group Member ID   : 192.168.6.11
Group ID          : 123
Group Name        : lab1getvpn
Key Server ID     : 192.168.3.11
Rekeys sent       : 0
Rekeys retries    : 0
Rekey Acks Rcvd   : 0
Rekey Acks missed : 0
Sent seq num :    0    0    0    0
Rcvd seq num :    0    0    0    0

Group Member ID   : 192.168.9.3
Group ID          : 123
Group Name        : lab1getvpn
Key Server ID     : 192.168.3.11
```

```
Rekeys sent       : 0
Rekeys retries    : 0
Rekey Acks Rcvd   : 0
Rekey Acks missed : 0
Sent seq num :    0    0    0    0
Rcvd seq num :    0    0    0    0
```

Table 1-28 provides information that needs to be configured on the GMs (R3 and R6). Use the following sample outputs from R3 and R6 to ensure that all the requirements have been met.

TABLE 1-28 Configuration information for the group members (GM)

ISAKMP Policy	☐ Preshared key authentication ☐ AES (Advanced Encryption Standard) encryption algorithm ☐ MD5 (Message Digest 5) hash algorithm ☐ Diffie-Hellman group 2
GDOI Parameters	☐ Group name is lab1getvpn. ☐ Group identity number is 123. ☐ Key Server IP address is 192.168.3.11.

```
R3# show crypto map
Crypto Map "gdoi" 10 gdoi
        Group Name: lab1getvpn
            identity number 123
            server address ipv4 192.168.3.11
        Interfaces using crypto map gdoi:
                GigabitEthernet0/1

R3# show crypto isakmp policy
Global IKE policy
```

 Please see page 474 for more details.

```
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit

R6# show crypto map
Crypto Map "gdoi" 10 gdoi
        Group Name: lab1getvpn
            identity number 123
            server address ipv4 192.168.3.11
        Interfaces using crypto map gdoi:
                Serial0/0/0

R6# show crypto isakmp policy
Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

Next, verify the GMs to ensure that they have successfully registered with the KS and download the policies:

```
R3# show crypto gdoi
GROUP INFORMATION
    Group Name               : lab1getvpn
    Group Identity           : 123
```

 Please see page 474 for more details.

```
    Rekeys received          : 0
    IPSec SA Direction       : Both
    Active Group Server      : 192.168.3.11
    Group Server list        : 192.168.3.11

    GM Reregisters in        : 29833 secs
    Rekey Received           : never


    Rekeys received
         Cumulative          : 0
         After registration  : 0
    Rekey Acks sent          : 0

 ACL Downloaded From KS 192.168.3.11:
   access-list  permit ip 172.17.0.0 0.0.255.255 172.17.0.0 0.0.255.255

KEK POLICY:
    Rekey Transport Type     : Unicast
    Lifetime (secs)          : 86400
    Encrypt Algorithm        : 3DES
    Key Size                 : 192
    Sig Hash Algorithm       : HMAC_AUTH_SHA
    Sig Key Length (bits)    : 1024

TEK POLICY:
  GigabitEthernet0/1:
    IPsec SA:
        sa direction:inbound
```

```
        spi: 0x86305AEB(2251315947)
        transform: esp-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (31632)
        Anti-Replay(Time Based) : 10 sec interval

    IPsec SA:
        sa direction:outbound
        spi: 0x86305AEB(2251315947)
        transform: esp-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (31632)
        Anti-Replay(Time Based) : 10 sec interval

R3# show crypto gdoi ipsec sa
SA created for group lab1getvpn:
  GigabitEthernet0/1:
    protocol = ip
      local ident  = 172.17.0.0/16, port = 0
      remote ident = 172.17.0.0/16, port = 0
      direction: Both, replay(method/window): Time/10 sec

R6# show crypto gdoi
GROUP INFORMATION
    Group Name               : lab1getvpn
    Group Identity           : 123
    Rekeys received          : 0
    IPSec SA Direction       : Both
    Active Group Server      : 192.168.3.11
    Group Server list        : 192.168.3.11
```

```
    GM Reregisters in        : 29762 secs
    Rekey Received           : never


    Rekeys received
         Cumulative          : 0
         After registration  : 0
    Rekey Acks sent          : 0

 ACL Downloaded From KS 192.168.3.11:
   access-list  permit ip 172.17.0.0 0.0.255.255 172.17.0.0 0.0.255.255

KEK POLICY:
    Rekey Transport Type     : Unicast
    Lifetime (secs)          : 86388
    Encrypt Algorithm        : 3DES
    Key Size                 : 192
    Sig Hash Algorithm       : HMAC_AUTH_SHA
    Sig Key Length (bits)    : 1024

TEK POLICY:
  GigabitEthernet0/1:
    IPsec SA:
        sa direction:inbound
        spi: 0x86305AEB(2251315947)
        transform: esp-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (31560)
        Anti-Replay(Time Based) : 10 sec interval
```

 Please see page 474 for more details.

```
    IPsec SA:
        sa direction:outbound
        spi: 0x86305AEB(2251315947)
        transform: esp-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (31560)
        Anti-Replay(Time Based) : 10 sec interval

R6# show crypto gdoi ipsec sa
SA created for group lab1getvpn:
  GigabitEthernet0/1:
    protocol = ip
      local ident  = 172.17.0.0/16, port = 0
      remote ident = 172.17.0.0/16, port = 0
      direction: Both, replay(method/window): Time/10 sec
```

Both GMs R3 and R6 have been preconfigured with Interface Loopback10 in subnet 172.17.0.0/16 and are advertised into the OSPF routing protocol. Ensure that you have routes on the GMs as follows:

```
R3# show ip route ¦ include 172.17.
     172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
O       172.17.6.6/32 [110/66] via 192.168.9.4, 01:26:41, GigabitEthernet0/1
C       172.17.3.0/24 is directly connected, Loopback10

R6# show ip route ¦ include 172.17.
     172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.17.6.0/24 is directly connected, Loopback10
O       172.17.3.3/32 [110/66] via 192.168.64.4, 01:26:48, Serial0/0/0
```

Finally, ensure that traffic between GM Loopback10 is getting encrypted via GETVPN tunnel. You can verify this using the following ping tests and by checking the **show crypto engine connections active** command to verify that encrypt and decrypt counters are incrementing accordingly.

```
R3# ping 172.17.6.6 source Loopback 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.6.6, timeout is 2 seconds:
Packet sent with a source address of 172.17.3.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R3# show crypto engine connections active
Crypto Engine Connections
   ID  Type    Algorithm           Encrypt  Decrypt IP-Address
 1015  IKE     MD5+AES                   0        0 192.168.9.3
 1016  IKE     SHA+3DES                  0        0
 2015  IPsec   AES+SHA                   0       30 172.17.0.0
 2016  IPsec   AES+SHA                  30        0 172.17.0.0

R6# ping 172.17.3.3 source Loopback 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.3.3, timeout is 2 seconds:
Packet sent with a source address of 172.17.6.6
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

R6# show crypto engine connections active
Crypto Engine Connections
   ID  Type    Algorithm           Encrypt  Decrypt IP-Address
 1036  IKE     MD5+AES                   0        0 192.168.64.6
 1037  IKE     SHA+3DES                  0        0
 2039  IPsec   AES+SHA                   0       35 172.17.0.0
 2040  IPsec   AES+SHA                  35        0 172.17.0.0
```

Question 3.5: Configuring the remote-access VPN using Cisco AnyConnect (3 points)

Configure the remote-access VPN connection using the Cisco AnyConnect SSLVPN client, meeting all the following requirements:

- Configure the remote-access VPN on ASA2 using the information in Table 1-19.
- Establish a remote-access VPN connection to the ASA2 firewall from the host PC behind R2 in VLAN 5 (as shown in Figure 1-3) using Cisco AnyConnect SSLVPN client software.
- Use the information in the table to complete this task.

Skills tested

- ☐ Configuring the remote-access SSLVPN connection on the Cisco ASA firewall using SSLVPN technology
- ☐ Understanding and installing the Cisco AnyConnect SSLVPN client on the remote host PC

Functionality and solution verification

- ☐ Similar to the GETVPN technology in the earlier question, the Cisco AnyConnect SSLVPN client is also a debut technology in the new CCIE Security v3.0 lab blueprint.
- ☐ The objective is to configure a basic remote-access configuration on ASA2 using the information in the table.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

 Please see page 474 for more details.

Table 1-29 provides information that needs to be configured on ASA2. Use the following sample outputs from ASA2 to ensure that all requirements have been met.

TABLE 1-29 Configuration information for ASA2

Policies for SSLVPN Connection	☐ Specify the group alias for this connection profile as "lab1." Allow the remote user to select a connection profile group identified by this alias "lab1" on his or her login page and on his or her AnyConnect client connection panel. ☐ Configure username "lab1user" and password "cisco." The user should be restricted to remote-access VPN sessions only; these cannot be used for Telnet/SSH/ASDM access to ASA2. ☐ IP pool range for VPN clients 192.168.111.1/24 through 192.168.111.50/24 ☐ Domain name is cisco.com. ☐ DNS server IP address is 192.168.2.14.
VPN Test PC	☐ The VPN test PC is located in VLAN 5 behind R2 (refer to Figure 1-3). ☐ Assign IP address 192.168.5.10/24 to the Test PC with a gateway to 192.168.5.11. Ensure that you can ping your network, including the ASA2 outside interface. ☐ Verify the solution by establishing an SSLVPN connection using a Cisco AnyConnect client to ASA2.

```
ASA2# sh run webvpn
webvpn
 enable outside
 svc image disk0:/anyconnect-win-2.3.0254-k9.pkg 1
 svc enable
 tunnel-group-list enable

ASA2# show run group-policy
group-policy SSLclient internal
group-policy SSLclient attributes
 dns-server value 192.168.2.14
 vpn-tunnel-protocol svc
```

```
 default-domain value cisco.com
 address-pools value SSLpool

ASA2# show run tunnel-group svc
!
tunnel-group svc type remote-access
tunnel-group svc general-attributes
 default-group-policy SSLclient
!
tunnel-group svc webvpn-attributes
 group-alias lab1 enable

ASA2# show run username
username lab1user password cisco
username lab1user attributes
 service-type remote-access

ASA2# show run ip local pool
ip local pool SSLpool 192.168.111.1-192.168.111.50 mask 255.255.255.0
```

```
ASA2# show flash:
--#--  --length--  -----date/time------  path
   75  4096        Jan 18 2009 20:03:48  log
  142  14137344    Jan 08 2009 02:11:08  asa804-k8.bin
   79  4096        Jan 08 2009 02:16:18  crypto_archive
  147  3032497     Jun 11 2009 06:29:46  anyconnect-win-2.3.0254-k9.pkg
62947328 bytes total (45387776 bytes free)
```

NOTE

Before testing the remote-access VPN connection, ensure that you have either preinstalled the Cisco AnyConnect VPN client on the test PC or that you will dynamically install it during your connection to ASA2. If the latter, you must have the appropriate package file flashed on ASA2 (review the following flash output). When you use a web browser to browse using HTTPS to the ASA2 outside interface IP address, the firewall automatically deploys the Cisco AnyConnect VPN client to the remote host upon successful login.

 Please see page 474 for more details.

Finally, using the test PC behind R2, establish an SSLVPN connection to ASA2 using the Cisco AnyConnect SSLVPN client, as shown in Figure 1-5. When it is successfully connected, verify the following output on ASA2:

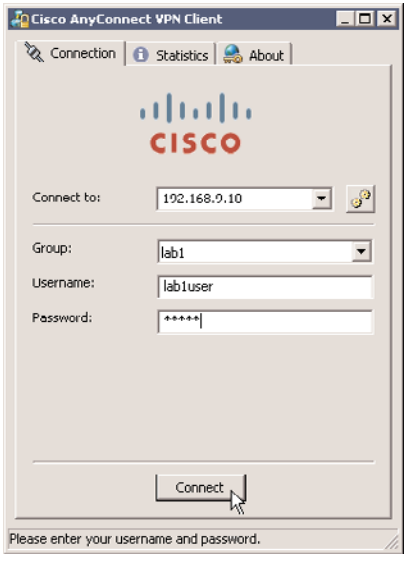
```
ASA2# show vpn-sessiondb svc

Session Type: SVC

Username     : lab1user              Index        : 78
Assigned IP  : 192.168.111.1         Public IP    : 192.168.2.14
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : SSL VPN
Encryption   : RC4 AES128            Hashing      : SHA1
Bytes Tx     : 141732                Bytes Rx     : 179936
Group Policy : SSLclient             Tunnel Group : svc
Login Time   : 06:56:43 UTC Thu Jun 11 2009
Duration     : 0h:27m:24s
NAC Result   : Unknown
VLAN Mapping : N/A                   VLAN         : none
```

Figure 1-5 shows a screen capture of the Cisco AnyConnect SSLVPN client from the test PC. The figure also shows the group connection profile "lab1" alias, as per the requirement.

FIGURE 1-5
Cisco AnyConnect SSLVPN client



Section 4.0: Cisco IPS (Intrusion Prevention System) (6 Points)

Question 4.1: Configuring IPS signatures (4 points)

Configure the Cisco IPS sensor appliance, meeting both of the following requirements:

- Configure signature tuning and custom signatures in both sig0 and sig2, which were applied to the virtual sensors earlier.
- Use the information in Table 1-30 to complete this task.

 Please see page 474 for more details.

TABLE 1-30 IPS signature configuration information

Signature Definition	Tuning Signature	Custom Signature
sig0	Enable ICMP echo and ICMP echo reply signatures. Set the action to produce an alert for both signatures. Set the alert to medium level for both signatures.	Create custom Sig# **60000** named **kazaa** to drop all connections used by a custom Peer-to-Peer (P2P) networking application called Kazaa (case-insensitive) using UDP port 1214. Set its alert to high level and its fidelity rating 100.
sig2	Enable ICMP echo and ICMP echo reply signatures. Set the action to produce an alert for both signatures. Set the alert to medium level for both signatures.	Enable HTTP application policy enforcement, allowing a maximum of five HTTP requests to the server at any given time.

Skills tested

- ☐ Configuring basic signature tuning and modifying parameters to the existing signatures available on the sensor database
- ☐ Configuring a new custom signature to specific user-defined parameters
- ☐ Enabling advanced HTTP packet inspection and application policy enforcement on the signature engine

Functionality and solution verification

- ☐ This question is divided into two parts. The first is signature tuning, which requires modifying parameters to the existing signatures that are already populated on the sensor. The second part is defining a new custom signature based on user-defined parameters to match a specific attack or application.
- ☐ Remember an important point about the new sensor appliance software release 6.0. There is a default "Event action override policy" for each signature definition (sig0 and sig2), which has a default deny packet inline set for all HIGHRISK risk rating signatures. This means that if any signature (existing or custom) falls into the HIGHRISK risk rating, they are denied by default (unless an event exception filter is configured). If you need a particular signature not to be dropped, you need to write an event action filter rule to make an exception to this parent policy.

- You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

As mentioned earlier, this question can be attempted in two parts.

The first part is straightforward, requiring tuning of the existing ICMP signatures (Sig# 2000 for echo request and Sig# 2004 for echo reply) as per the information in the preceding table.

The following output verifies that all requirements have been met:

```
IPS# show configuration
<snip>
! ------------------------------
service signature-definition sig0
signatures 2000 0
alert-severity medium
engine atomic-ip
event-action produce-alert
exit
status
enabled true
exit
exit
signatures 2004 0
alert-severity medium
engine atomic-ip
event-action produce-alert
exit
```

 Please see page 474 for more details.

```
status
enabled true
exit
exit
<snip>
! ----------------------------
service signature-definition sig2
<snip>
signatures 2000 0
alert-severity medium
engine atomic-ip
event-action produce-alert
exit
status
enabled true
exit
exit
signatures 2004 0
alert-severity medium
engine atomic-ip
event-action produce-alert
exit
status
enabled true
exit
exit
exit
! ----------------------------
<snip>
```

The second part is defining custom signature and enabling of advanced HTTP application policy enforcement as per the information in the preceding table.

Ensure that the custom signature for KaZaa is using the string-udp signature engine on UDP port 1214. The regex should be written to cater to case-insensitivity, as required, plus other parameters as per the preceding table.

Also ensure that if the question provides a specific signature name and number, they must be used exactly, or you may lose points.

The following output verifies that all the requirements have been met:

```
IPS# show configuration
<snip>
! ------------------------------
service signature-definition sig0
<snip>
signatures 60000 0
alert-severity high
sig-fidelity-rating 100
sig-description
sig-name kazaa
exit
engine string-udp
event-action produce-alert¦deny-attacker-inline
regex-string [Kk][Aa][Zz][Aa][Aa]
service-ports 1214
direction to-service
exit
status
enabled true
exit
```

 Please see page 474 for more details.

NOTE
Sometimes the custom signatures cannot be verified because there is no live traffic to run through the sensor to trigger the alerts. However, on other occasions, you may be able to verify some custom signatures.

```
exit
exit
! ----------------------------
service signature-definition sig2
application-policy
http-policy
http-enable true
max-outstanding-http-requests-per-connection 5
exit
exit
<snip>
```

Question 4.2: Configuring NTP on IPS Sensor (2 points)

To have an accurate timestamp on signature alerts and to have a consistent time source, configure NTP on the Cisco IPS sensor appliance, meeting all the following requirements:

- Configure the sensor to synchronize its clock with the NTP server on R1.
- Use the MD5 password "cisco."
- Ensure that the sensor clock has NTP as its time source.

Skills tested

- ☐ Configuring NTP on the Cisco IPS Sensor appliance to synchronize its clock

 Please see page 474 for more details.

Functionality and solution verification

- ☐ The objective of this question is to configure basic NTP parameters on the sensor appliance to synchronize its clock with the NTP server on R1.
- ☐ Remember to open the ACL on NTP server R1, which is used to secure NTP connections to the server.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

Use the following outputs to verify NTP settings on the sensor appliance:

```
IPS(config)# service host
IPS(config-hos)# ntp-option enabled
IPS(config-hos-ena)# show settings
   enabled
   -----------------------------------------------
      ntp-keys (min: 1, max: 1, current: 1)
      -----------------------------------------------
         key-id: 1
         -----------------------------------------------
            md5-key: cisco
         -----------------------------------------------
      -----------------------------------------------
      ntp-servers (min: 1, max: 1, current: 1)
      -----------------------------------------------
         ip-address: 10.1.1.1
```

 Please see page 474 for more details.

```
        key-id: 1
      ---------------------------------------------
   ------------------------------------------------
IPS(config-hos-ena)# exit
IPS(config-hos)# exit
IPS(config)# exit
IPS#

IPS# show clock detail
10:11:41 UTC Thu Jun 11 2009
Time source is NTP

R1# show ip access-lists 1
Standard IP access list 1
    10 permit 10.5.5.5 (1146 matches)
    30 permit 192.168.2.12 (57 matches)
    20 permit 192.168.9.10 (108 matches)
```

The system clock maintains a unique flag that indicates whether the time on the clock is authoritative (believed to be accurate). Table 1-31 explains the three types of flags in the **show clock detail** output and their sample **show** outputs from the sensor, respectively.

TABLE 1-31 Authoritative flag details

Symbol	Meaning
* (asterisk)	Time is not authoritative
. (dot)	Time is authoritative, but NTP is not synchronized
(blank)	Time is authoritative

Review the three **show clock detail** outputs shown next from the sensor console, illustrating each category mentioned in Table 1-31.

The following output was captured before NTP was configured on the sensor. The asterisk before the timestamp indicates that the time is not authoritative and that NTP has not been configured:

```
IPS# show clock detail
*09:37:22 UTC Thu Jun 11 2009
No time source
```

The following output was captured seconds after NTP was configured on the sensor. The dot before the timestamp indicates that NTP synchronization is in progress:

```
IPS# show clock detail
.09:50:16 UTC Thu Jun 11 2009
Time source is NTP
```

The following output was captured after a few minutes of NTP configuration. The blank before the timestamp indicates that NTP synchronization was successful and that the time is authoritative:

```
IPS# show clock detail
10:11:41 UTC Thu Jun 11 2009
Time source is NTP
```

Section 5.0: Implement Identity Authentication (12 Points)

Question 5.1: User-level access control (4 points)

Configure AAA authentication on Sw1 and Cisco Secure ACS server, meeting all the following requirements:

- Enable AAA authentication on Sw1 using TACACS+ protocol using the shared secret key "cisco." Do not use the default method list.
- Add Sw2 IP address 192.168.8.11 as the AAA client on the Cisco Secure ACS server (192.168.2.14) located in VLAN 2.
- Configure two new users on the Cisco Secure ACS server, "user1" and "user2," using the password "cisco" for both users. Both users must be assigned to the Default group.
- Configure user-level access restriction on the Cisco Secure ACS server to control network device access as follows. User1 should always be allowed access to Sw1 from any source IP address (within your network). However, user2 should only be allowed access to Sw1 from any Loopback0 (within your network) source IP address. Do not configure any settings within the user2 profile to complete the latter task.
- Do not use Network Access Filtering (NAF) or Network Access Restriction (NAR) from the Shared Profile components to complete this task.
- Verify the Failed Reports on the Cisco Secure ACS server to ensure that user2 is failing due to the user access filter implementation.
- Ensure that the console port is unaffected by this task.

Skills tested

- ☐ Configuring AAA authentication on the Cisco Catalyst Switch using named method lists
- ☐ Configuring the Cisco Secure ACS server for NAS settings and user profiles
- ☐ Configuring advanced user profile settings on Cisco Secure ACS server to control network device access

Functionality and solution verification

- ☐ This question can be divided into two parts. The first enables AAA authentication using the named method list on Sw1. The second part is the configuration on the Cisco Secure ACS server.
- ☐ The main objective of this question is to enable per-user-level access restriction to enforce device access control.
- ☐ The question requires you to configure two users. User1 has full access, and user2 has access subject to specific source IP address.
- ☐ Several other restrictions are laid out in this question. You can't use a default method list. Only a named method list is allowed, which is then applied explicitly to VTY lines. Furthermore, you cannot use Network Access Filtering (NAF) and Network Access Restriction (NAR) from the Shared Profile components. You are only allowed to use the NAR section from within the user and group settings.
- ☐ Also note that you need to open the ACL on the ASA1/abc1 context to allow a Telnet session (TCP port 23) entering the outside interface from any source to destination Sw1 IP address 192.168.8.11. Because the question does not restrict or mention anything about this ACL, you can permit TCP port 23 from any source to any destination. However, as a best practice, I recommend that you write the best possible specific ACL to allow any source to destination 192.168.8.11 on TCP port 23. Again, this is just a recommendation, not a requirement.
- ☐ Additionally, you need to open the ACL on the ASA1/abc2 context to allow the TACACS+ authentication session entering the outside interface from source Sw1 (192.168.8.11) to destination Cisco Secure ACS server (192.168.2.14) on TCP port 49. Because the question does not restrict or mention anything about this ACL, you can

permit TCP port 49 from any source to any destination. However, as a best practice, I recommend that you write the best possible specific ACL to allow from source Sw1 (192.168.8.11) to destination Cisco Secure ACS server (192.168.2.14) on TCP port 49. Again, this is just a recommendation, not a requirement.

- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

Use the following outputs to verify that AAA authentication is working, as per the question requirement.

User1 should have full access to Sw1 from any source IP address. We will establish Telnet sessions from different devices within the network to ensure that this works:

```
R6# telnet 192.168.8.11
Trying 192.168.8.11 ... Open
User Access Verification
Username: user1
Password: cisco
Sw1>
Sw1> exit
[Connection to 192.168.8.11 closed by foreign host]
R6#

R5# telnet 192.168.8.11
Trying 192.168.8.11 ... Open
User Access Verification
Username: user1
Password: cisco
Sw1> exit
```

 Please see page 474 for more details.

```
[Connection to 192.168.8.11 closed by foreign host]
R5#

R1# telnet 192.168.8.11
Trying 192.168.8.11 ... Open
User Access Verification
Username: user1
Password: cisco
Sw1>
Sw1> exit
[Connection to 192.168.8.11 closed by foreign host]
R1#
```

User2 should only be allowed access to Sw1 from any Loopback0 (within your network) source IP address. The following output shows that user2 could establish a successful Telnet session when sourcing from the Loopback0 IP address, and it fails when sourcing from any other source IP address:

```
R6# telnet 192.168.8.11 /source-interface Loopback 0
Trying 192.168.8.11 ... Open
User Access Verification
Username: user2
Password: cisco
Sw1> exit
[Connection to 192.168.8.11 closed by foreign host]
R6#

R6# telnet 192.168.8.11 /source-interface Serial 0/0/0
Trying 192.168.8.11 ... Open
User Access Verification
```

 Please see page 474 for more details.

```
Username: user2
Password: cisco
% Authentication failed
User Access Verification
Username: user1
Password: cisco
Sw1> exit
[Connection to 192.168.8.11 closed by foreign host]
R6#

R1# telnet 192.168.8.11 /source-interface Loopback 0
Trying 192.168.8.11 ... Open
User Access Verification
Username: user2
Password: cisco
Sw1> exit
[Connection to 192.168.8.11 closed by foreign host]
R1#

R1# telnet 192.168.8.11 /source-interface GigabitEthernet 0/0
Trying 192.168.8.11 ... Open
User Access Verification
Username: user2
Password: cisco
% Authentication failed
User Access Verification
Username: user1
Password: cisco
Sw1> exit
[Connection to 192.168.8.11 closed by foreign host]
R1#
```

Verify AAA client configuration on Sw1 to ensure that all conditions and restrictions are met. A default method list is not allowed; you must use a named method list only. Two named method lists are configured in this task—one for applying to VTY lines, and another for the console line. The question clearly says to ensure that the console line should be unaffected. Therefore, an explicit exemption from any authentication is required.

```
Sw1# show run ¦ inc aaa
aaa new-model
aaa authentication login vtyauthen group tacacs+
aaa authentication login conauthen none
aaa session-id common

Sw1# show run ¦ inc tacacs
tacacs-server host 192.168.2.14
tacacs-server directed-request
tacacs-server key cisco

Sw1# show run ¦ begin line con
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login authentication conauthen
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login authentication vtyauthen
 transport input telnet
!
end
```

NOTE

This **test** command utility should be used before you perform any Telnet connections shown here.

Cisco IOS provides a very useful **test** command utility that can be used to verify protocol-level connectivity from the client device (router or switch) to the Cisco Secure ACS server. It validates if the client can establish connectivity with the server using TACACS+/RADIUS ports. This is particularly helpful if the Cisco Secure ACS server is behind a firewall, to ensure that the appropriate ports are opened within the ACL on the firewall. The following output shows the **test** command utility to ensure that protocol connectivity to the server is good:

```
Sw1# test aaa group tacacs+ user1 cisco legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.

Sw1# test aaa group tacacs+ user2 cisco legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

In addition to all the preceding testing and verification steps, verify that the Cisco Secure ACS server was configured correctly.

The following figures illustrate output from the Cisco Secure ACS server that meets all the requirements.

Figure 1-6 shows Sw1 IP address 192.168.8.11 configured as an AAA client using the TACACS+ authentication protocol.

Figure 1-7 shows that both users are in the Default group.

Figure 1-8 shows the User1 setup profile with per-user level Network Access Restriction (NAR) configured.

 Please see page 474 for more details.

FIGURE 1-6
AAA client configuration

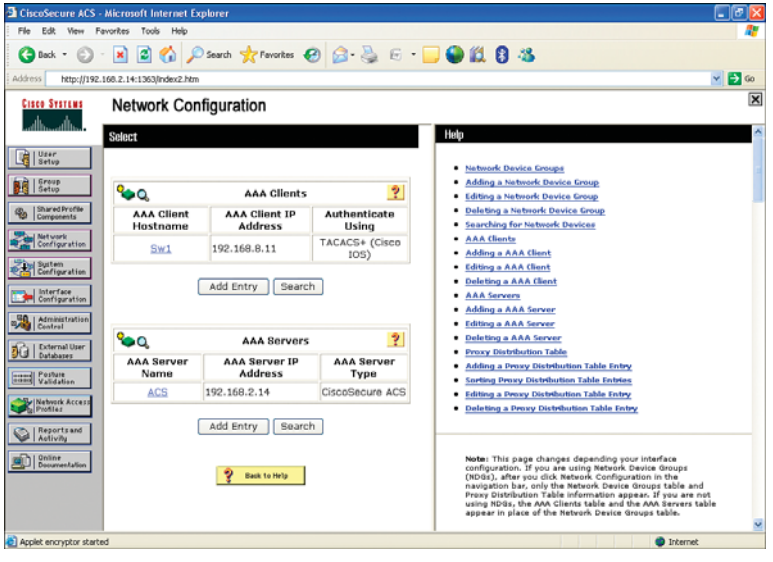


FIGURE 1-7
Both users are in the default group

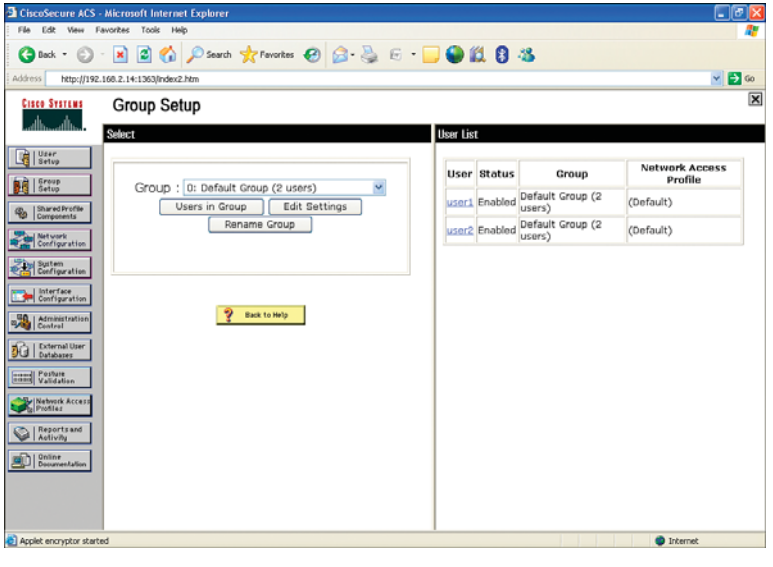
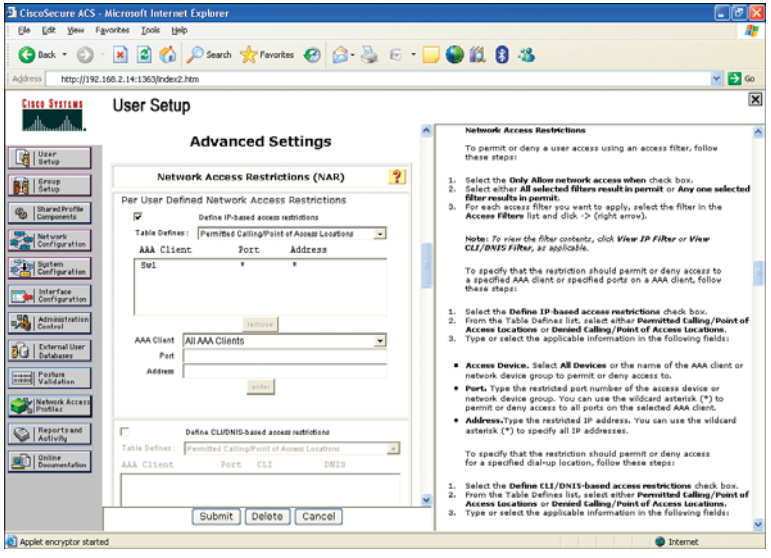


FIGURE 1-8
User1 profile configuration

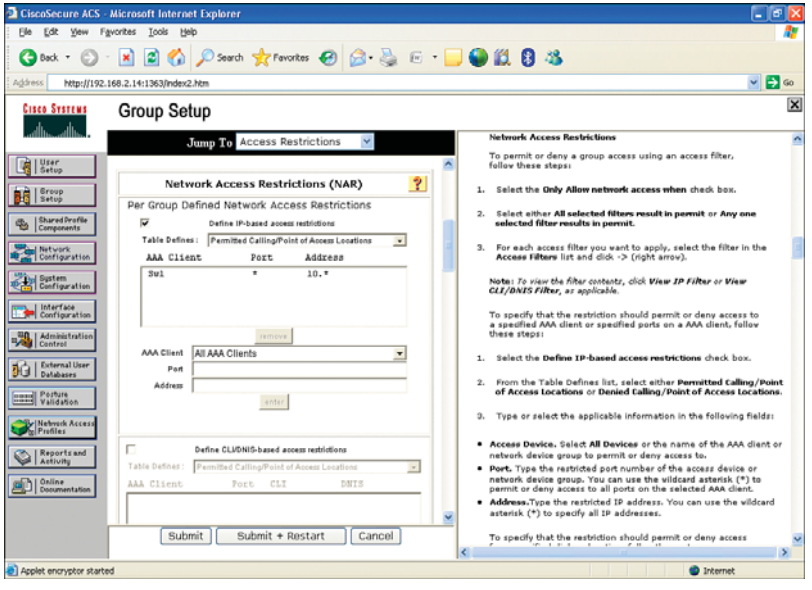


There was also an explicit requirement in the question not to configure any settings within the user2 profile to complete the second task of the user2 profile restriction. The only workaround to that was to configure the group-level settings instead. Ensure that no NAR is configured under user2 profile settings.

Figure 1-9 shows the Default group setup (because both users are in the Default group) with group-level NAR configured. User2 will inherit these settings. Note that user1 will also inherit these restrictions. However, the user-level profile always overwrites the group-level profile. Therefore, the previous user1 profile setup supersedes these settings.

 Please see page 474 for more details.

FIGURE 1-9
Default group profile configuration



Another restriction was to avoid using the NAF and NAR from the Shared Profile components.

Figures 1-10 and 1-11 show that NAF and NAR, respectively, in the Shared Profile component are blank.

FIGURE 1-10
Network Access Filtering (NAF)

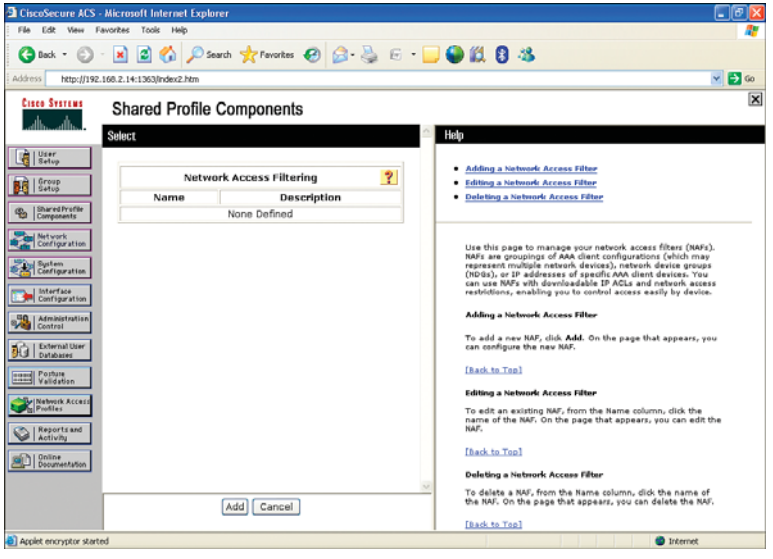
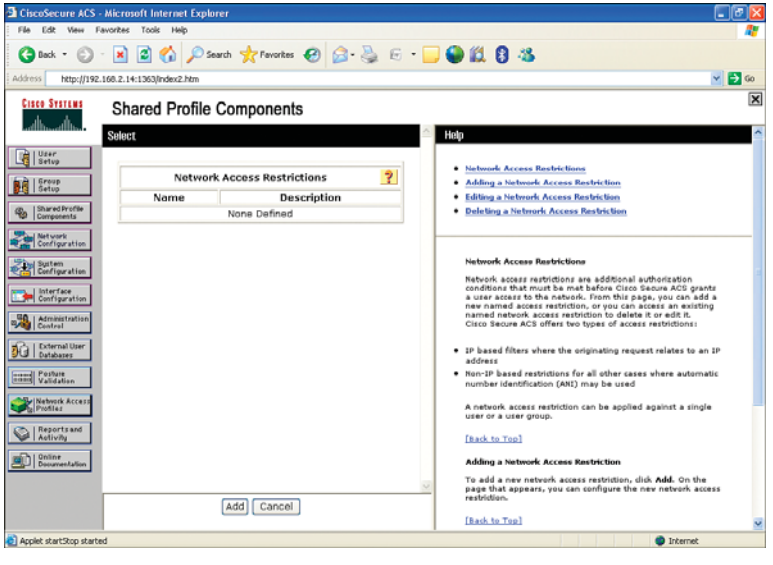
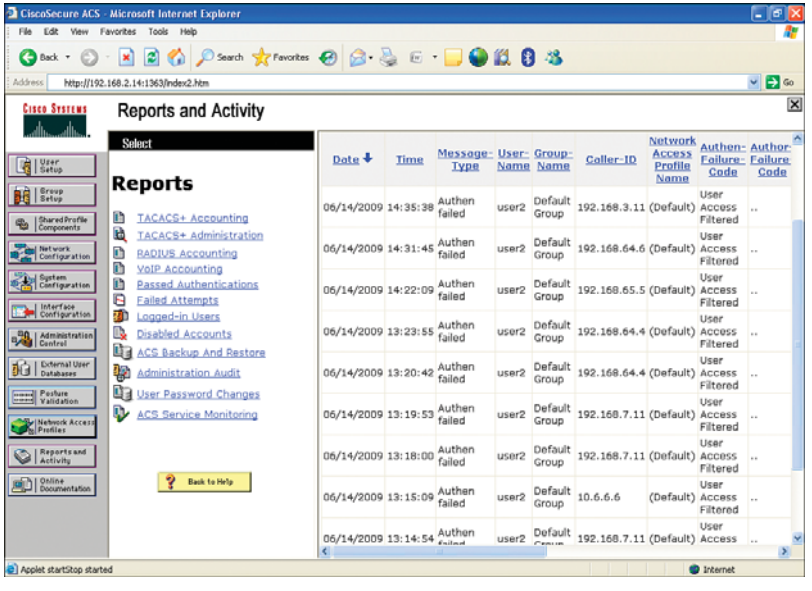


FIGURE 1-11
Network Access Restriction (NAR)



Finally, check Figure 1-12 from Failed Reports to ensure that user2 is failing due to the filter implementation. Check the Authen-Failure-Code column in this output, which shows User Access Filtered.

FIGURE 1-12
Failed reports



Question 5.2: Role-based access control (4 points)

Configure role-based access control using AAA authentication on R2 and Cisco Secure ACS server, meeting all the following requirements:

- Enable AAA authentication on R2 using TACACS+ protocol using the shared secret key “cisco.” Do not use the default method list.
- Add R2 IP address 192.168.4.11 as the AAA client on Cisco Secure ACS server (192.168.2.14) located in VLAN 2.
- Configure role-based CLI views using the information in Tables 1-21 and 1-22.

- Configure Cisco Secure ACS user profiles using the information in the tables.
- Verify functionality by establishing a Telnet session to R2, and ensure that both users get dynamic assignment from the AAA server to their respective user roles.
- Ensure that the console port is unaffected by this task.
- Use the information in the tables to complete this task.

Skills tested

- ☐ Configuring Role-Based CLI access control to define "views" providing selective or partial access to Cisco IOS EXEC and configuration (Config) mode commands
- ☐ Configuring AAA configuration on the router using named method lists
- ☐ Configuring the Cisco Secure ACS server for NAS settings and user profiles
- ☐ Configuring advanced user profile settings on Cisco Secure ACS server using the new TACACS+ custom attribute called **cli-view-name** to map CLI views to user roles configured on the router

Functionality and solution verification

- ☐ This question can be divided into three parts. The first is to enable AAA authentication using a named method list on R2 and applying to VTY lines (the console port should be explicitly configured for none authentication). The second part is most important—configuring CLI views on R2 according to the roles requirement defined in the information table. The third part is configuration on the Cisco Secure ACS server to create the user and groups. It also involves assigning the CLI views using the new TACACS+ custom attribute called **cli-view-name** to dynamically map CLI views to user roles configured on the router upon successful authentication using the TACACS+ protocol.
- ☐ The main objective of this question is to enable per-user-level access restriction based on each person's role and function within the organization. This question gives an example of two roles: network operator and security

operator. This feature is very useful when you want to delegate varying responsibilities to different user groups within the organization. For example, managing and configuring routing protocols and infrastructure configuration should be assigned to the network operations team. Responsibility for managing the VPN, IOS firewall, and AAA functionality should be assigned to the security operations team.

- CLI views allow per-user per-device CLI-based policy control that is applied by the local device (router) after the specified view (using the new TACACS+ attribute **cli-view-name**) of the authenticated user is received from the AAA server.
- The question requires configuring two users—netop and secop—mapped to their corresponding CLI views.
- The question clearly says not to use a default method list. Only a named method list is allowed, which is then applied explicitly to VTY lines.
- Also note that you need to open the ACL on the ASA1/abc2 context to allow a Telnet session (TCP port 23) entering the outside interface from any source to destination R2 IP address 192.168.4.11. Because the question does not restrict or mention anything about this ACL, you can permit TCP port 23 from any source to any destination. However, as a best practice, I recommend that you write the best possible specific ACL to allow from any source to destination 192.168.4.11 on TCP port 23. Again, this is just a recommendation, not a requirement.
- Additionally, you need to open the ACL on the ASA1/abc2 context to allow a TACACS+ authentication session entering the dmz2 interface from source R2 (192.168.4.11) to destination Cisco Secure ACS server (192.168.2.14) on TCP port 49. Because the question does not restrict or mention anything about this ACL, you can permit TCP port 49 from any source to any destination. However, as a best practice, I recommend that you write the best possible specific ACL to allow from source R2 (192.168.4.11) to destination Cisco Secure ACS server (192.168.2.14) on TCP port 49. Again, this is just a recommendation, not a requirement.
- You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

As mentioned earlier, this question can be divided into three parts.

The first part is to enable AAA authentication using a named method list on R2 and applying to VTY lines. Note that the question clearly states that the console port should be unaffected. Hence, an explicit named method list should be configured to exempt console authentication:

NOTE

You cannot begin configuring CLI views until you have configured AAA configuration and root view; both are a prerequisite.

If AAA is not configured, you will receive the error message "% AAA must be configured."

After AAA is configured (as just shown), you need to go into root view before you can start configuring the required CLI views.

```
R2# show run ¦ section aaa authentication
aaa authentication login vtyauthen group tacacs+
aaa authentication login conauthen none

R2# show run ¦ section tacacs-server
tacacs-server host 192.168.2.14
tacacs-server key cisco

R2# show run ¦ begin line con
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login authentication conauthen
!
line vty 0 4
 exec-timeout 0 0
 password cisco
 authorization exec vtyexec
 logging synchronous
 login authentication vtyauthen
 transport input telnet
!
```

NOTE
When this is done, you can enter global configuration mode and begin CLI view configuration.

```
R2# enable view
Password: cisco
Jun 14 17:47:34.763: %PARSER-6-VIEW_SWITCH: successfully set to view 'root'.
R2#
R2# show parser view
     Current view is 'root'
```

The second and perhaps most important part is configuring the CLI views on R2 according to the roles requirements defined in Table 1-32.

TABLE 1-32 Role-based CLI configuration information on R2

Network Operator Role	☐ Configure a CLI view called "netop" with password "netop." ☐ Users in this view should be able to configure any dynamic routing protocols and static routes. ☐ Users should also be able to apply any interface-specific commands. ☐ Users in this view should be able to execute any show commands.
Security Operator Role	☐ Configure a CLI view called "secop" with password "secop." ☐ Users in this view should be able to configure any VPN-related configuration (crypto), plus AAA, CBAC, and Zone-based firewall configuration. ☐ Users should also be able to configure any TACACS+ and RADIUS-related parameters. ☐ Users should be able to apply any interface-specific commands. ☐ Users in this view should be able to execute any show commands.

```
R2# show run ¦ section view
parser view netop
 secret netop
 commands configure include all ip route
 commands configure include all router
 commands configure include all interface
 commands configure include ip
 commands exec include configure terminal
```

 Please see page 474 for more details.

```
 commands exec include configure
 commands exec include all show
parser view secop
 secret secop
 commands configure include all radius-server
 commands configure include all tacacs-server
 commands configure include all interface
 commands configure include all zone-pair
 commands configure include all zone
 commands configure include all policy-map
 commands configure include all class-map
 commands configure include all crypto
 commands configure include all aaa
 commands exec include configure terminal
 commands exec include configure
 commands exec include all show
```

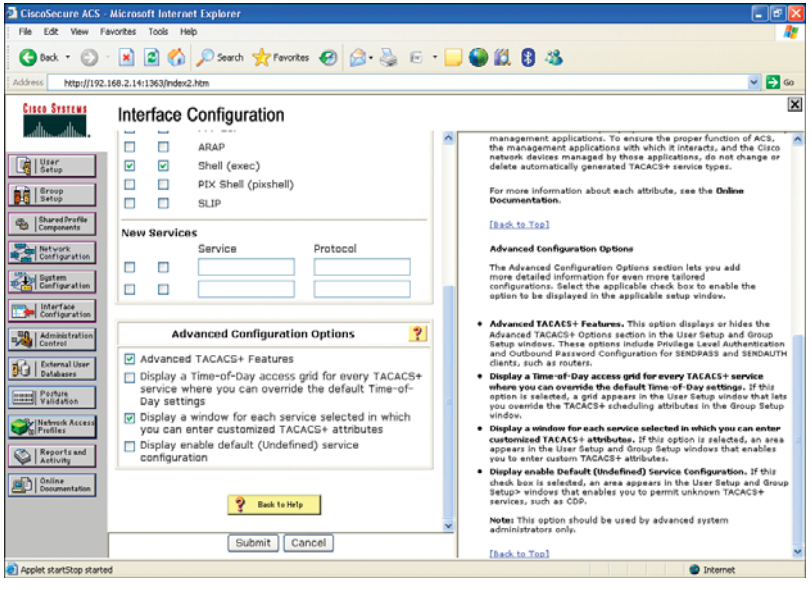
The third and final part is configuring the Cisco Secure ACS server to create the users and groups. You also assign the CLI views using the new TACACS+ custom attribute called **cli-view-name** to dynamically map CLI views to user roles configured on the router upon successful authentication using the TACACS+ protocol.

TABLE 1-33 Cisco Secure ACS server configuration information

Network Operator Role	☐ Configure a new user called "netop" with password "netop," and assign it to a group called "Role-Based CLI group." ☐ Upon successful authentication, this user should dynamically map to the Network Operator role CLI view configured on R2.
Security Operator Role	☐ Configure a new user called "secop" with password "secop," and assign it to a group called "Role-Based CLI group." ☐ Upon successful authentication, this user should dynamically map to the Security Operator role CLI view configured on R2.

By default, the new TACACS+ custom attribute box under the User setup will not be visible. Figure 1-13 shows how to enable it from the TACACS+ (Cisco IOS) option under the Interface Configuration menu on Cisco Secure ACS server. Then you select the checkbox titled Display a window for each service selected in which you can enter customized TACACS+ attributes.

FIGURE 1-13
Enabling the custom TACACS+ attribute from the advanced configuration options



The following figures illustrate outputs from the Cisco Secure ACS server that meet all the requirements.

Figure 1-14 shows R2 IP address 192.168.4.11 configured as an AAA client using the TACACS+ authentication protocol.

Figure 1-15 shows that both users are in the Default group.

Figure 1-16 shows the user “netop” profile with the TACACS+ custom attribute to map the NetOp CLI view.

Figure 1-17 shows the user “secop” profile with the TACACS+ custom attribute to map the SecOp CLI view.

FIGURE 1-14
AAA client configuration

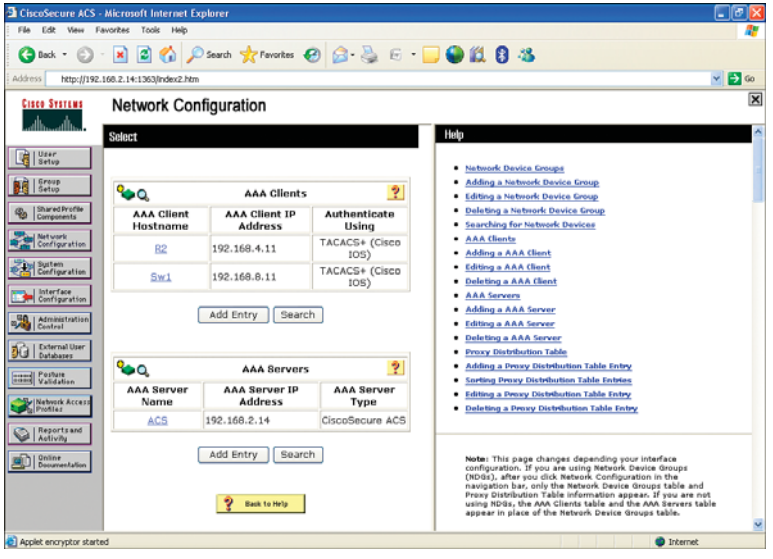


FIGURE 1-15
Both users are in the Role-Based CLI group

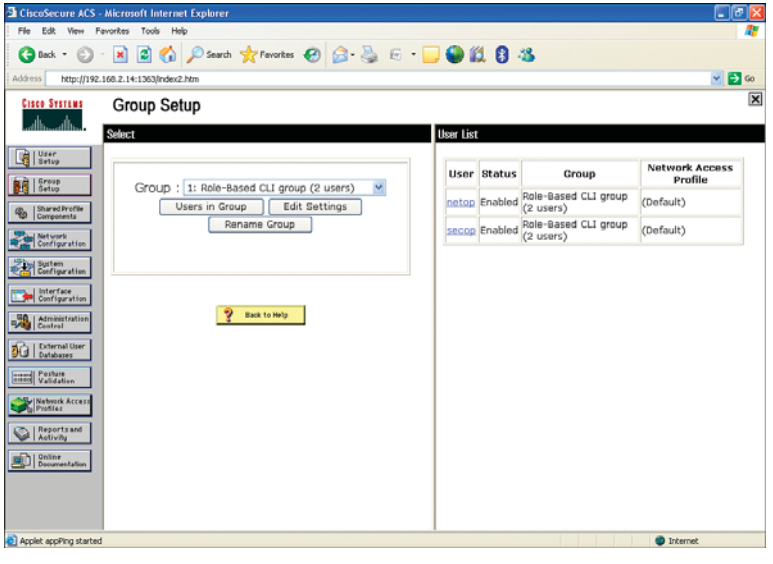


FIGURE 1-16
User netop profile configuration

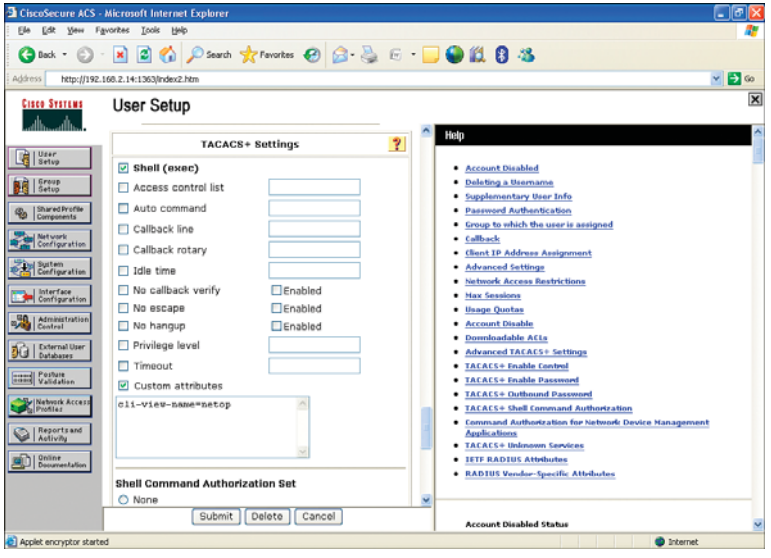
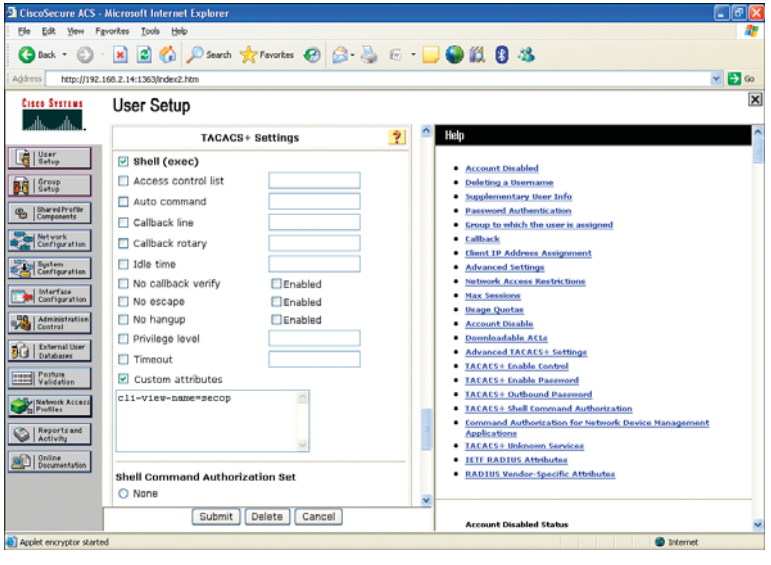


FIGURE 1-17
User secop profile configuration



NOTE

The Shell (exec) check-box must also be selected to perform EXEC-level authorization, as shown in Figure 1-17.

Finally, ensure that role-based CLI view is working as per the requirement by establishing the following Telnet sessions to R2 and performing user authentication.

The following outputs verify user netop authentication. The output shows that, after being authenticated, this user is dynamically mapped to CLI view NetOp and is can perform all the commands as per the information table. The ? illustrates the commands available in EXEC and configuration (config) modes.

```
R6# telnet 192.168.4.11
Trying 192.168.4.11 ... Open
User Access Verification
Username: netop
Password: netop
R2#
R2# ?
Exec commands:
  <1-99>      Session number to resume
  configure   Enter configuration mode
  credential  load the credential info from file system
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  show        Show running system information

R2#
R2# show parser view
Current view is 'netop'
R2#
R2# conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# ?
Configure commands:
```

 Please see page 474 for more details.

```
  do          To run exec commands in config mode
  exit        Exit from configure mode
  interface   Select an interface to configure
  ip          Global IP configuration subcommands
  router      Enable a routing process
R2(config)# router ?
  bgp         Border Gateway Protocol (BGP)
  eigrp       Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis        ISO IS-IS
  iso-igrp    IGRP for OSI networks
  mobile      Mobile routes
  odr         On Demand stub Routes
  ospf        Open Shortest Path First (OSPF)
  rip         Routing Information Protocol (RIP)
R2(config)# ^Z
R2# exit
[Connection to 192.168.4.11 closed by foreign host]
R6#
R6#
```

The following outputs verify user secop authentication. The output shows that, after being authenticated, this user is dynamically mapped to CLI view SecOp and can perform all the commands as per the information table. The ? illustrates the commands available in EXEC and configuration (config) modes.

```
R6# telnet 192.168.4.11
Trying 192.168.4.11 ... Open
User Access Verification
Username: secop
Password: secop
R2#
```

 Please see page 474 for more details.

```
R2# ?
Exec commands:
  <1-99>      Session number to resume
  configure   Enter configuration mode
  credential  load the credential info from file system
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  show        Show running system information

R2# show parser view
Current view is 'secop'
R2#
R2# conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# ?
Configure commands:
  aaa            Authentication, Authorization and Accounting.
  class-map      Configure Class Map
  crypto         Encryption module
  do             To run exec commands in config mode
  exit           Exit from configure mode
  interface      Select an interface to configure
  policy-map     Configure Policy Map
  radius-server  Modify RADIUS query parameters
  tacacs-server  Modify TACACS query parameters
  zone           FW with zoning
  zone-pair      Zone pair command
R2(config)# crypto ?
  ca            Certification authority
  call          Configure Crypto Call Admission Control
```

```
  ctcp          Configure cTCP encapsulation
  dynamic-map   Specify a dynamic crypto map template
  engine        Enter a crypto engine configurable menu
  gdoi          Configure GDOI policy
  identity      Enter a crypto identity list
  ipsec         Configure IPSEC policy
  isakmp        Configure ISAKMP policy
  key           Long term key operations
  keyring       Key ring commands
  logging       logging messages
  map           Enter a crypto map
  mib           Configure Crypto-related MIB Parameters
  pki           Public Key components
  provisioning  Secure Device Provisioning
  wui           Crypto HTTP configuration interfaces
  xauth         X-Auth parameters
R2(config)# ^Z
R2# exit
[Connection to 192.168.4.11 closed by foreign host]
R6#
```

Question 5.3: Port-based authentication (4 points)

Configure port-based authentication using 802.1x on Sw2, meeting all the following requirements:

- A wireless LAN access point (AP) not supporting 802.1x will be connected in the future to Sw2 FastEthernet0/7. Prepare to implement 802.1x-based authentication on Sw2 interface FastEthernet0/7 (with traffic in both directions) to authenticate all the wireless clients connected to the AP.

- Enable periodic reauthentication, set the guest VLAN assignment to VLAN 5, and set the maximum number of times that the switch sends an EAP-request to the client to three (assuming that no response is received) before restarting the authentication process.
- Ensure that the port is set to shut down in the event of a violation.
- Do not configure any AAA and RADIUS configuration on Sw2 yet. This will be done at a later stage, when AP is ready for deployment.

Skills tested

- ☐ Configuring port authentication on a Cisco Catalyst Switch using 802.1x port-based access control on a Layer 2 port
- ☐ Enabling advanced 802.1x parameters

Functionality and solution verification

- ☐ The objective of this question is straightforward. You must enable 802.1x port-based authentication on Sw2 interface FastEthernet0/7.
- ☐ The question requires tuning some additional 802.1x parameters such as guest VLAN number, enable periodic reauthentication, maximum request, and port violation mode.
- ☐ An important observation to note is that the question mentions that the access point (AP) that will be connected to the switch port does not support 802.1x. Also, the switch needs to act as the authenticating device for all the wireless clients connected to the AP. This means the switch port must be configured as a multihost port for the 802.1x authentication. See the following sample output.
- ☐ The question clearly states that there is no need to configure AAA and RADIUS-related configuration at this point, because the access point (AP) is not ready for deployment yet. At this point, you are only required to configure the switch port, in preparation for the AP deployment.

 Please see page 474 for more details.

- Also note that if RADIUS configuration is required, you also need to open ACL on the ASA1/abc2 context to allow a RADIUS authentication session entering the outside interface from source Sw2 to destination RADIUS server (Cisco Secure ACS) in VLAN 2. Because the question does not require configuring RADIUS at this point, this task is not required, but do remember this for the future.
- You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

As mentioned in the question, the wireless LAN access point (AP) currently is not connected, and we are configuring the 802.1x as presetup in preparation for the AP deployment.

The objective of this question is enabling 802.1x port-based authentication on Sw2 interface FastEthernet0/7.

The following outputs illustrate configuration and 802.1x verification:

```
Sw2# show dot1x Interface FastEthernet 0/7
Dot1x Info for FastEthernet0/7
----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
Violation Mode            = SHUTDOWN
ReAuthentication          = Enabled
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
```

```
ReAuthPeriod             = 3600 (Locally configured)
ReAuthMax                = 2
MaxReq                   = 3
TxPeriod                 = 30
RateLimitPeriod          = 0
Guest-Vlan               = 5

Sw2# show run interface FastEthernet 0/7
Building configuration...
Current configuration : 227 bytes
!
interface FastEthernet0/7
 switchport mode access
 dot1x pae authenticator
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x violation-mode shutdown
 dot1x max-req 3
 dot1x reauthentication
 dot1x guest-vlan 5
end
```

 Please see page 474 for more details.

Section 6.0: Implement Control and Management Plane Security (12 Points)

Question 6.1: Control plane protection (4 points)

Configure Control Plane Policing (CoPP) on R2, meeting all the following requirements:

- Configure CoPP protection on R2, allowing ICMP pings sourced from the RFC 1918 address space only. Any ICMP packets sourced from nonprivate address space to R2 should be dropped.
- Do not configure any parameters under the default class that matches any packet.
- You are allowed to configure only one class-map and one policy-map to complete this task.

Skills tested

- ☐ Configuring Control Plane Policing (CoPP) using Modular QoS CLI (MQC) to define traffic classification criteria and to specify the policy actions for the classified traffic
- ☐ Understanding CoPP features and capabilities
- ☐ Knowledge of the MQC configuration model
- ☐ Understanding the private address space (RFC 1918)

Functionality and solution verification

- ☐ This question seems basic, but an important restriction might create complexity in how you configure the class-map in MQC to complete this task.
- ☐ The question clearly says not to use the default class-map and permits only one class-map and one policy-map to complete this task.

- You could easily do this by configuring separate classes to match the private address space (RFC 1918) and all other remaining traffic. Because you are allowed to use only one class-map, the best way to achieve the result is to configure two ACLs. The first matches any ICMP packets from any source to any destination, and the second matches RFC 1918 source to any destination.
- Within the **class-map**, you can match the first ACL (any ICMP). You can use the **match not** option, which is used to negate the match to match the second ACL, and apply the **drop** action keyword in the **policy-map** for traffic matching this criterion. This way, you are permitting all ICMP traffic sourced from RFC 1918 and dropping all other remaining ICMP packets.
- You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

The following outputs illustrate the configuration:

```
R2# show policy-map control-plane
 Control Plane

  Service-policy input: copp

    Class-map: copp (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 101
      Match: not access-group 102
      drop

    Class-map: class-default (match-any)
```

```
        877 packets, 113617 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
        Match: any

R2# show ip access-lists
Extended IP access list 101
    10 permit icmp any any (274 matches)
Extended IP access list 102
    10 permit icmp 10.0.0.0 0.255.255.255 any (96 matches)
    20 permit icmp 172.16.0.0 0.15.255.255 any (33 matches)
    30 permit icmp 192.168.0.0 0.0.255.255 any (110 matches)
```

NOTE

An important point to remember in the preceding configuration is that your **class-map** must use the **match-all** keyword to ensure that it uses the logical-AND operation for all matching statements under this **class-map**. If **match-any** is used, you will lose all points.

Verify that CoPP is working as per the requirement by sending ICMP ping packets legitimate private source address space from RFC 1918 (the ping should succeed):

```
R6# ping 192.168.4.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R6# ping 192.168.4.11 source Loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.11, timeout is 2 seconds:
Packet sent with a source address of 10.6.6.6
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R6# ping 192.168.4.11 source Loopback 10
Type escape sequence to abort.
```

 Please see page 474 for more details.

```
Sending 5, 100-byte ICMP Echos to 192.168.4.11, timeout is 2 seconds:
Packet sent with a source address of 172.17.6.6
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Finally, to verify that CoPP is dropping all the nonprivate source address space, create a dummy loopback interface on R6, and assign any random IP address using the nonprivate address range. Then send ICMP packets to R2 sourced from this Loopback (the ping should be dropped). Verify the result on R2 using the **show policy-map control-plane** command.

```
R6# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         192.168.7.11    YES NVRAM  up                    up
GigabitEthernet0/1         192.168.6.11    YES NVRAM  up                    up
Serial0/0/0                192.168.64.6    YES NVRAM  up                    up
Serial0/0/1                192.168.65.6    YES NVRAM  up                    up
SSLVPN-VIF0                unassigned      NO  unset  up                    up
Loopback0                  10.6.6.6        YES NVRAM  up                    up
Loopback10                 172.17.6.6      YES NVRAM  up                    up
Loopback20                 50.50.50.50     YES manual up                    up

R6# ping 192.168.4.11 source Loopback 20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.11, timeout is 2 seconds:
Packet sent with a source address of 50.50.50.50
.....
Success rate is 0 percent (0/5)

R2# show policy-map control-plane
 Control Plane
```

```
  Service-policy input: copp

    Class-map: copp (match-all)
      5 packets, 570 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 101
      Match: not access-group 102
      drop

    Class-map: class-default (match-any)
      1023 packets, 133249 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
R2#
```

Question 6.2: Storm control protection (2 points)

Configure Storm Control Protection on Sw1, meeting all the following requirements:

- Configure Storm Control Protection on Sw1 interface FastEthernet0/13 to block all broadcast traffic using the following criteria.
- Broadcast traffic should be blocked when the rising threshold reaches 80%, and traffic resumes forwarding when the falling threshold reaches 60% of the available bandwidth.
- Do not configure any ACL on interface FastEthernet0/13 to complete this task.

Skills tested

- ☐ Configuring Storm Control Protection using the port-based traffic control feature on a Cisco Catalyst switch
- ☐ Understanding broadcast storms

Functionality and solution verification

- ☐ This question is very easy and straightforward. This task isn't too complex.
- ☐ Configure basic Storm Control Protection on Sw1 using the port-based traffic control using the rising and falling threshold provided.
- ☐ You will see **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

The following outputs illustrate configuration and verification:

```
Sw1# show storm-control FastEthernet 0/13
Interface  Filter State   Upper        Lower        Current
---------  ------------  -----------  -----------  ----------
Fa0/13     Forwarding       80.00%       60.00%        0.00%

Sw1# show run interface FastEthernet 0/13
Building configuration...
Current configuration : 131 bytes
!
interface FastEthernet0/13
 no switchport
 ip address 192.168.8.11 255.255.255.0
 storm-control broadcast level 80.00 60.00
end
```

 Please see page 474 for more details.

Verify the restriction in the question not to use any ACL on interface FastEthernet 0/13:

```
Sw1# show ip interface FastEthernet 0/13 ¦ inc access list
  Outgoing access list is not set
  Inbound  access list is not set
```

Question 6.3: Management plane protection (3 points)

Configure Management Plane Protection (MPP) on R2, meeting all the following requirements:

- Configure MPP on R4 to protect device access using the following criteria.
- Only Telnet protocol is allowed to access R4 through the Serial0/0/0 interface. However, both Telnet and HTTP protocols are allowed to access R4 through the GigabitEthernet0/1 interface.
- Do not configure any ACL to complete this task.

Skills tested

- ☐ Configuring Management Plane Protection (MPP) using extended CoPP features
- ☐ Understanding MPP features and capabilities

Functionality and solution verification

- ☐ The objective of this question is to restrict the interfaces on which network management packets are allowed to enter a device. The MPP feature lets you assign one or more router interfaces as designated management interfaces.
- ☐ The question requires allowing Telnet traffic entering Serial0/0/0 and allowing both Telnet and HTTP entering GigabitEthernet0/1.

- You could also configure an ACL and apply it to the physical interface or VTY lines. However, use of ACL is not allowed to complete this task.
- You will see **show** command outputs so that you can check and verify the requirements laid out in the question.
- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

The following outputs illustrate configuration and verification:

```
R4# show management-interface
Management interface GigabitEthernet0/1
        Protocol        Packets processed
            http                18
          telnet                46

Management interface Serial0/0/0
        Protocol        Packets processed
          telnet                120

R4# show run ¦ section control-plane host
control-plane host
 management-interface GigabitEthernet0/1 allow http telnet
 management-interface Serial0/0/0 allow telnet
```

Verify the restriction in the question not to use any ACL to complete this task:

NOTE
No ACL (**access-class** command) is under VTY lines.

```
R4# show ip interface Serial 0/0/0 ¦ inc access list
  Outgoing access list is not set
  Inbound  access list is not set

R4# show ip interface GigabitEthernet 0/1 ¦ inc access list
  Outgoing access list is not set
  Inbound  access list is not set

R4# show run ¦ section vty
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input telnet
```

Verify that MPP is working as per the requirement by establishing Telnet and HTTP sessions to R4, as shown next. Only the Telnet connection works for traffic entering R4 Serial0/0/0, whereas the HTTP connection fails:

```
R6# telnet 192.168.64.4
Trying 192.168.64.4 ... Open
User Access Verification
Password: cisco
R4> exit
[Connection to 192.168.64.4 closed by foreign host]

R6# telnet 192.168.64.4 80
Trying 192.168.64.4, 80 ...
% Connection timed out; remote host not responding
R6#
```

 Please see page 474 for more details.

Both the Telnet and HTTP connections work for traffic entering R4 GigabitEthernet0/1:

```
Sw2# telnet 192.168.9.4
Trying 192.168.9.4 ... Open
User Access Verification
Password: cisco
R4> exit
[Connection to 192.168.9.4 closed by foreign host]
Sw2#

Sw2# telnet 192.168.9.4 80
Trying 192.168.9.4, 80 ... Open
/
HTTP/1.1 400 Bad Request
Date: Mon, 15 Jun 2009 11:33:14 GMT
Server: cisco-IOS
Accept-Ranges: none
400 Bad Request
[Connection to 192.168.9.4 closed by foreign host]
Sw2#
```

Question 6.4: Router system management (3 points)

Configure router system management parameters on R5, meeting all the following requirements:

- Configure R5 to generate a SYSLOG message when the CPU exceeds 75% within a 5-second window.
- Configure R5 to store all SYSLOG messages on the router buffer for all levels up to severity level 7.
- Additionally, configure R5 such that a network administrator can get a list of users currently using this router without having to console to it. The information displayed includes the processes running on the router, line number, connection name, idle time, and terminal location.

Skills tested

- ☐ Configuring router system management features complementing router security
- ☐ Understanding SYSLOG, CPU thresholds, and system notification parameters

Functionality and solution verification

- ☐ The objective of this question is to configure some basic router system management parameters.
- ☐ The question requires you to configure the CPU threshold and to notify via SYSLOG when the total CPU threshold rises above 75% within a 5-second interval window. All SYSLOG messages must be stored locally on the router buffer. The question requires you to enable buffer logging at severity level 7 (debugging). This is the highest level, and it includes all lower levels' notifications.
- ☐ The question also requires enabling the Finger service (port 79) on the router. This allows any user on the network to get a list of the users currently connected to this router and other process-level information.
- ☐ You will see **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

CAUTION

Enabling the Finger service can be very dangerous, because it provides valuable user information that can be instrumental in hacking. It is highly recommended that you disable this service. The purpose of this task is for informational purposes only.

The following outputs illustrate configuration and verification that meet all the requirements:

```
R5# show run ¦ sec process cpu
process cpu threshold type total rising 75 interval 5

R5# show log
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)
```

 Please see page 474 for more details.

```
No Active Message Discriminator.

No Inactive Message Discriminator.

    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 3 messages logged, xml disabled,
                     filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped

    Trap logging: level informational, 143 message lines logged

Log Buffer (4096 bytes):

Jun 15 13:59:00.548: %SYS-5-CONFIG_I: Configured from console by console
R5#
```

The Finger service is disabled by default. To enable Finger, you can use either the **service finger** or **ip finger** command from global configuration mode:

```
R5# show run ¦ section finger
ip finger
```

After it is enabled, you can run the Finger service from any device (the example shown is from R3) to establish a Finger session using the Telnet protocol. As you can see, you can get valuable information without actually connecting or consoling to router R5:

```
R3# telnet 192.168.35.5 finger
Trying 192.168.35.5, 79 ... Open

    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:00:50
 578 vty 0                 idle                 00:00:05 192.168.9.4
*579 vty 1                 idle                 00:00:00 192.168.35.3

  Interface    User               Mode         Idle     Peer Address
  Se0/0/0                         Sync PPP     00:00:00 192.168.35.3

[Connection to 192.168.35.5 closed by foreign host]
R3#
```

Section 7.0: Advanced Security (12 Points)

Question 7.1: Web server protection (4 points)

Configure web server protection on the ASA1/abc1 context, meeting all the following requirements:

- A web server (Sw1 Loopback1) is hosted behind the ASA1/abc1 context, which was configured for address translation in Question 2.1, with HTTP and HTTPS connections allowed from any host to this web server.

- The web server has limited resources. Therefore, configure the ASA1/abc1 context to protect this web server from TCP synchronization (SYN) flood denial-of-service (DoS) attacks by limiting the maximum number of TCP embryonic (half-open) connections to 50 (per protocol). Of these, only five can be from a single host at any given time.
- Do not change the static identity translation configured in Question 2.1 to complete this task.
- Do not use ACL to complete this task.
- Do not configure any parameters under the global default policy.

Skills tested

- ☐ Configuring TCP SYN flood and DoS protection using various proactive techniques
- ☐ Understanding TCP three-way handshake and embryonic (half-open) connections
- ☐ Knowledge of the Modular Policy Framework (MPF) configuration model on the Cisco ASA Firewall

Functionality and solution verification

- ☐ The objective of this question is to configure a proactive solution to prevent TCP SYN flood-type DoS attacks.
- ☐ You can use several techniques to configure this task. However, the question clearly says not to use the **static** command and ACL. The only option left is to use the MPF feature on the ASA1/abc1 context.
- ☐ The question mentions several restrictions; ensure that each of them is observed accordingly.
- ☐ Another important requirement to note in this question is that you need prevention for both protocols (HTTP and HTTPS). Because ACL is not allowed, you need to create two separate **class-maps** to match TCP port 80 and TCP port 443, respectively. (Multiple **match** commands under one **class-map** are not supported, which is why you need to create two separate **class-maps**.)

- The question restricts the use of ACL. Therefore, you need to use the **match port** command in the **class-map** to classify the HTTP and HTTPS traffic.
- The question requires configuring the embryonic (half-open) connections limit to a maximum of 50 embryonic connections per protocol. Also note that the question requires that out of these 50 half-open connections, only five embryonic connections can be from a single host at any given time.
- Another restriction laid out in the question is not to use the default global policy. Therefore, the solution must be applied to the outside interface on the ASA1/abc1 context.
- You will see **show** command outputs so that you can check and verify the requirements laid out in the question.
- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

The following outputs illustrate configuration and verification that meet all the requirements:

```
ASA1/abc1# show service-policy interface outside
Interface outside:
  Service-policy: webserver
    Class-map: webserver443
      Set connection policy: embryonic-conn-max 50 per-client-embryonic-max 5
        current embryonic conns 0, drop 0
    Class-map: webserver80
      Set connection policy: embryonic-conn-max 50 per-client-embryonic-max 5
        current embryonic conns 0, drop 0

ASA1/abc1# show run class-map ¦ ex default
!
```

 Please see page 474 for more details.

```
class-map webserver443
 match port tcp eq https
class-map webserver80
 match port tcp eq www
!
```

You can use the **show service-policy flow** command to validate the policy configuration for any specific type of traffic flow (such as HTTP) and what action has been applied to this flow. This command is very useful to verify configuration without having to send real-time traffic through the firewall to test your policy.

The following output shows which security policy and action will be matched and applied if a packet arrives on the outside interface from any source to the destination web server (172.16.1.1) on TCP port 80:

```
ASA1/abc1# show service-policy flow tcp host 0.0.0.0 host 172.16.1.1 eq 80
Global policy:
  Service-policy: global_policy
    Class-map: class-default
      Match: any
      Action:
        Output flow:
Interface outside:
  Service-policy: webserver
    Class-map: webserver80
      Match: port tcp eq www
      Action:
        Input flow:  set connection embryonic-conn-max 50 per-client-embryonic-max 5
    Class-map: class-default
<..>
```

 Please see page 474 for more details.

Finally, check the restriction; the existing static identity translation should not be altered from Question 2.1. If it is altered, you will see **tcp 0 50** at the end of this syntax, and you will lose all points.

```
ASA1/abc1# show run static
static (inside,outside) 172.16.1.1 172.16.1.1 netmask 255.255.255.255
```

Question 7.2: Troubleshooting Cisco IOS NAT (3 points)

Network Address Translation (NAT) has been preconfigured on R5 in this question. Your task is to troubleshoot and identify the injected faults and ensure that NAT is functional, meeting all the following requirements:

- Cisco IOS NAT has been preconfigured on R5 in a multihomed scenario. R5 has two WAN uplinks (Serial0/0/0 and Serial0/0/1); assume that these are the two redundant ISP uplinks.
- A Loopback5 with IP address 10.55.55.55/32 has been preconfigured and advertised into OSPF Area 0.
- The NAT objective is to perform source address translation for Loopback5 to the respective egress WAN interface when the packet leaves this router (R5). For example, if R3 tries to ping Loopback5, the return packet should have a source address of Serial0/0/0. However, when R6 tries to ping the same Loopback5, the return packet should have a source address of Serial0/0/1.
- Three faults are injected into your preconfiguration. Identify these faults, and verify that NAT is functional as per the requirement. Note that the faults injected could be related to either incorrect preconfiguration or missing commands to complete the configuration.
- While fixing this issue, you are allowed to alter the preconfiguration and add to, modify, or remove part of the preconfiguration. However, you need to ensure that altering the preconfiguration does not impede any other question.
- For verification, perform the following ping test, and ensure that the inside global address in the NAT table from the **show** output matches your result.

NOTE

As mentioned on the CCIE lab exam blueprint, "Knowledge of troubleshooting is an important skill, and candidates are expected to diagnose and solve issues as part of the CCIE lab exam." The new v3.0 lab exam strongly enforces this aspect. The new lab exam will be just as challenging and will validate both configuration and troubleshooting skills. Candidates must practice troubleshooting methods and techniques as an important skill set to be successful.

Skills tested

- ☐ Troubleshooting Cisco IOS NAT technology. Knowledge of troubleshooting IOS NAT is very important, as you've seen several times. You must see when VPN scenarios are not working and broken due to the NAT application in between the path of VPN packets.
- ☐ Identifying network-related issues within an existing topology that has been preconfigured

Functionality and solution verification

- ☐ As seen in the previous VPN section, this is another troubleshooting series question. These new format questions are different from the traditional configuration-based questions. The objective is to identify candidates' analytical skills in a complex environment where an engineer applies his or her troubleshooting skills to fix networking-related problems using a methodological approach with the aid of various tools. Extensive knowledge of **show** and **debug** commands is very important in these scenarios.
- ☐ A basic approach to solving this type of question is to break it into layers, such as basic IP connectivity, routing, switching, and any other network-related issues. As mentioned earlier, use a methodological approach. Also important is to break the issue into smaller parts. For example, in this question you should check basic IP reachability without the NAT function applied (between R3-and-R5 and R6-and-R5). This ensures that all routing and switching are working properly. When you are done, you can apply the NAT function and start troubleshooting the NAT-related configuration. Start by reviewing the current preconfiguration using **show** commands. If you cannot find anything unusual, enable relevant **debug**s to get more details.
- ☐ The issues that were injected into the preconfiguration are described next, with elaborations.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

 Please see page 474 for more details.

You can use several methods and varying techniques to start troubleshooting. There is no perfect method. Every person has different methodologies and uses a different approach. As long as the main objective is met, it is OK to use your own method. Earlier I described a basic approach and how to use it to your advantage.

Here is a list of three faults injected into your preconfiguration:

- Fault 1 can be found on R5. The NAT **access-list** number 102 referenced in both **route-maps** is incorrect. The source and destination are swapped. The correct ACL should have source address as Loopback5 (10.55.55.55) to any destination **access-list 102 permit ip host 10.55.55.55 any**.
- Fault 2 can be found on R6. An **access-list** number 101 is applied on interface Serial0/0/1 on R6, which is blocking ingress ICMP packets arriving from Loopback5 (blocking both real and NATed addresses). Remove this ACL 101 from the interface.
- Fault 3 can be found on R5. The **ip nat outside** command is missing under the Interface Serial0/0/1 on R5. Although ICMP pings will work from R6, the source address in the return packet will not be translated as required, and it will be the original 10.55.55.55 address.

When all three faults have been found and fixed, perform the following ping tests and verify that the inside global address in the NAT table from the following **show** output matches your result.

The sample output also provides a **debug ip icmp** capture. You can use this to be certain that the return ICMP packet has the source address translated to the corresponding egress interface.

```
R3# show debug
Generic IP:
  ICMP packet debugging is on
R3# ping 10.55.55.55
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.55.55.55, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R3#
*Jun 16 11:43:33.608: ICMP: echo reply rcvd, src 192.168.35.5, dst 192.168.35.3
*Jun 16 11:43:33.612: ICMP: echo reply rcvd, src 192.168.35.5, dst 192.168.35.3
*Jun 16 11:43:33.612: ICMP: echo reply rcvd, src 192.168.35.5, dst 192.168.35.3
*Jun 16 11:43:33.616: ICMP: echo reply rcvd, src 192.168.35.5, dst 192.168.35.3
*Jun 16 11:43:33.616: ICMP: echo reply rcvd, src 192.168.35.5, dst 192.168.35.3
R3#

R6# show debug
Generic IP:
  ICMP packet debugging is on
R6# ping 10.55.55.55
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.55.55.55, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R6#
*Jun 16 11:38:14.432: ICMP: echo reply rcvd, src 192.168.65.5, dst 192.168.65.6
*Jun 16 11:38:14.436: ICMP: echo reply rcvd, src 192.168.65.5, dst 192.168.65.6
*Jun 16 11:38:14.436: ICMP: echo reply rcvd, src 192.168.65.5, dst 192.168.65.6
*Jun 16 11:38:14.440: ICMP: echo reply rcvd, src 192.168.65.5, dst 192.168.65.6
*Jun 16 11:38:14.440: ICMP: echo reply rcvd, src 192.168.65.5, dst 192.168.65.6

R5# show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
icmp 192.168.35.5:33   10.55.55.55:33     192.168.35.3:33    192.168.35.3:33
icmp 192.168.65.5:85   10.55.55.55:85     192.168.65.6:85    192.168.65.6:85
```

Question 7.3: Configuring source IP address validation (2 points)

Configure source IP address validation on R6, meeting all the following requirements:

- Configure R6 WAN links to protect from forged (spoofed) IP source addresses by discarding IP packets that lack a verifiable source IP address. R6 should prevent any attack using spoofing techniques by forwarding only packets that have source addresses that are valid and found in the IP routing table.
- The solution should check the source addresses of each ingress packet without regard for the specific interface on which it was received, as long as it has a valid route found in the IP routing table.
- Do not configure ACL to complete this task.

Skills tested

- ☐ Configuring Unicast Reverse Path Forwarding in loose mode
- ☐ Understanding source IP address validation techniques
- ☐ Understanding asymmetric routing
- ☐ Knowledge of attacks employing spoofed (forged) source IP addresses

Functionality and solution verification

- ☐ You can use several techniques to combat source IP address spoofing. This question requires configuring a Unicast Reverse Path Forwarding (uRPF) solution.
- ☐ This question also requires configuring uRPF in loose mode to accommodate asymmetric routing (if any).
- ☐ Also note that the question requires protection for WAN links (plural). Therefore, you need to configure uRPF on both WAN links (Serial0/0/0 and Serial0/0/1).

- ☐ The question clearly says not to use ACL, which leaves your choice as the uRPF solution only.
- ☐ You will see **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

The following outputs verify uRPF configuration and meeting the requirement:

```
R6# show ip interface Serial 0/0/0 ¦ inc verify
  IP verify source reachable-via ANY

R6# show ip interface Serial 0/0/1 ¦ inc verify
  IP verify source reachable-via ANY
```

Question 7.4: Spanning-Tree Protocol protection (3 points)

Configure spanning-tree protection on Sw1, meeting all the following requirements:

- Configure Sw1 globally to enable the Port Fast feature on all nontrunking interfaces (all access ports) by default.
- Configure Sw1 to prevent any interface that is Port Fast-enabled from participating in the spanning tree. If Sw1 receives a bridge protocol data unit (BPDU) packet on any interface that is in Port Fast operational state, it should put the interface in the error-disabled state when it receives a BPDU.
- Ensure that Sw1 will put the interface back in service automatically after 60 seconds, only (conditionally) if this interface was put in the error-disabled state due to a BPDU issued explicitly, and not others.
- Additionally, configure Sw1 globally to prevent alternate and root ports from becoming designated ports (DP) because of a failure that leads to a unidirectional link.

Skills tested

- ☐ Configuring Spanning-Tree Protocol (STP) protection using BPDU Guard and Loop Guard features on Cisco Catalyst Switches
- ☐ Understanding basic STP operation and how STP attacks work, and knowledge of attacks exploiting STP
- ☐ Understanding switch ports in error-disabled state and how to recover them automatically

Functionality and solution verification

- ☐ This question is about configuring proactive measures to prevent attacks surrounding Spanning-Tree Protocol (STP). STP has several weaknesses and possible exploits and issues if STP is not protected properly.
- ☐ The objective of this question is to prevent STP issues using BPDU Guard and Loop Guard features on Sw1. Both these features can be enabled globally or per-interface. The question requires configuring these features globally.
- ☐ The question also requires a switch to recover the bad port (error-disabled state) automatically after 60 seconds. Pay attention to the **conditionally** statement. The switch can be configured to automatically recover any error-disabled port within 60 seconds regardless of the original cause, or you can explicitly mention the recovery cause linked to BPDU Guard. The latter is required to fulfill the requirement.
- ☐ Additionally, the question also requires enabling all nontrunking (access ports) to Port Fast mode using global configuration.
- ☐ You will see **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

The following outputs verify that BPDU Guard and Loop Guard have been enabled globally, error-disabled recovery configuration, and all other requirements:

```
Sw1# show spanning-tree summary totals
Switch is in pvst mode
Root bridge for: VLAN0001-VLAN0005, VLAN0009, VLAN0101, VLAN0201
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is enabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short
Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
10 vlans                       0         0        0         35         35

Sw1# show errdisable recovery
ErrDisable Reason            Timer Status
-----------------            --------------
arp-inspection               Disabled
bpduguard                    Enabled
channel-misconfig            Disabled
dhcp-rate-limit              Disabled
dtp-flap                     Disabled
gbic-invalid                 Disabled
inline-power                 Disabled
l2ptguard                    Disabled
```

 Please see page 474 for more details.

```
link-flap                   Disabled
mac-limit                   Disabled
loopback                    Disabled
pagp-flap                   Disabled
port-mode-failure           Disabled
psecure-violation           Disabled
security-violation          Disabled
sfp-config-mismatch         Disabled
small-frame                 Disabled
storm-control               Disabled
udld                        Disabled
vmps                        Disabled

Timer interval: 60 seconds

Interfaces that will be enabled at the next timeout:
Sw1#
```

You can also verify individual interfaces (access ports) to check if Port Fast mode, BPDU Guard, and Loop Guard have also been enabled by default. For example, the following output is a sample capture from FastEthernet0/1 and FastEthernet0/2 both being access ports:

```
Sw1# show spanning-tree interface FastEthernet0/1 detail
 Port 3 (FastEthernet0/1) of VLAN0003 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.3.
   Designated root has priority 32771, address 0014.a811.3600
   Designated bridge has priority 32771, address 0014.a811.3600
   Designated port id is 128.3, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
```

 Please see page 474 for more details.

```
   The port is in the portfast mode by default
   Link type is point-to-point by default
   Bpdu guard is enabled by default
   Loop guard is enabled by default on the port
   BPDU: sent 265366, received 0

Sw1# show spanning-tree interface FastEthernet0/2 detail
 Port 4 (FastEthernet0/2) of VLAN0004 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.4.
   Designated root has priority 32772, address 0014.a811.3600
   Designated bridge has priority 32772, address 0014.a811.3600
   Designated port id is 128.4, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   The port is in the portfast mode by default
   Link type is point-to-point by default
   Bpdu guard is enabled by default
   Loop guard is enabled by default on the port
   BPDU: sent 303302, received 0
```

Section 8.0: Network Attacks (12 Points)

Question 8.1: Filtering instant messaging (3 points)

Configure Instant Messaging (IM) filtering on the ASA1/abc2 context, meeting all the following requirements:

- An end user of the MSN Instant Messaging (IM) application is transferring infected files over the application, propagating a worm that exploits a known vulnerability, thus causing a threat to the corporate network. The end user's MSN login ID is yusuf@hotmail.com.

- Configure the ASA1/abc2 context to drop all connections that explicitly match the parameters. All other normal MSN services, such as regular chat services, except file transferring, should continue to work for the user.
- All other end users should be unaffected by this task, and their MSN services should continue to work, including file transferring.
- Do not use ACL to complete this task.
- The solution must be applied to the global default policy.

Skills tested

- ☐ Configuring Instant Messaging (IM) filtering using deep packet inspection on the Cisco ASA firewall
- ☐ Understanding basic IM operation and knowledge of attacks exploiting IM
- ☐ Knowledge of the Modular Policy Framework (MPF) configuration model on the Cisco ASA Firewall

Functionality and solution verification

- ☐ The objective of this question is to protect the network from a worm exploiting a known vulnerability using an MSN IM application.
- ☐ The solution can be achieved using the MPF using deep packet inspection (inspect types **class-map** and **policy-map**).
- ☐ The question clearly says to configure the solution to prevent file transferring only from the end user yusuf@hotmail.com, while ensuring that all other MSN services continue to work. This requires configuring an inspect type **class-map** (deep packet inspection) for IM and matching three parameters: protocol MSN, end user login ID, and MSN service of file transferring. An important point is that the **class-map** must have a **match-all** to ensure that all three criteria match explicitly before the connection is dropped. If any one condition does not match, the traffic is permitted normally via the inspection engine and thus does not affect all other end users.

- ☐ The question says not to use an ACL to complete this task.
- ☐ The solution must be applied under the default global policy.
- ☐ You will see **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

The following outputs verify the MPF solution preventing the IM from file-transferring any files using the MSN application based on the three criteria mentioned earlier.

The output also shows that the solution was applied under the default global policy. The way to complete this task is to create an inspect type **policy-map** and apply it under the default global policy inspecting IM protocol.

The output also shows the inspect type **policy-map** and **class-map** matching the three criteria, including a **regex** to match the login-ID.

There is no usage of ACL, as per the restriction in the question.

```
ASA1/abc2# show service-policy global
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 19, drop 0, reset-drop 0
      Inspect: ftp, packet 0, drop 0, reset-drop 0
      Inspect: h323 h225 _default_h323_map, packet 0, drop 0, reset-drop 0
      Inspect: h323 ras _default_h323_map, packet 0, drop 0, reset-drop 0
      Inspect: netbios, packet 0, drop 0, reset-drop 0
      Inspect: rsh, packet 0, drop 0, reset-drop 0
```

 Please see page 474 for more details.

```
      Inspect: rtsp, packet 0, drop 0, reset-drop 0
      Inspect: skinny , packet 0, drop 0, reset-drop 0
      Inspect: esmtp _default_esmtp_map, packet 0, drop 0, reset-drop 0
      Inspect: sqlnet, packet 0, drop 0, reset-drop 0
      Inspect: sunrpc, packet 0, drop 0, reset-drop 0
      Inspect: tftp, packet 19526, drop 0, reset-drop 0
      Inspect: sip , packet 0, drop 0, reset-drop 0
      Inspect: xdmcp, packet 0, drop 0, reset-drop 0
      Inspect: im filterIMpolicy, packet 0, drop 0, reset-drop 0

ASA1/abc2# show run policy-map type inspect im
!
policy-map type inspect im filterIMpolicy
 parameters
 class filterIMclassmap
  drop-connection
!

ASA1/abc2# show run class-map type inspect im
!
class-map type inspect im match-all filterIMclassmap
 match protocol msn-im
 match login-name regex filterIMregex
 match service file-transfer
!
ASA1/abc2#

ASA1/abc2# show run regex
regex filterIMregex "yusuf@hotmail.com"
ASA1/abc2#
```

Question 8.2: Preventing unauthorized connections (2 points)

Configure the ASA1/abc1 context to prevent unauthorized connections, meeting all the following requirements:

- Configure the ASA1/abc1 context to send TCP resets (the TCP RST flag in the TCP header) to the denied host for any inbound TCP sessions that are denied by the firewall.
- In addition, configure the ASA1/abc1 context to disable the proxy ARP function and stop responding to any ARP request with its own MAC address, thus limiting exposure of its MAC address.
- Do not use ACL to complete this task.

Skills tested

- ☐ Preventing unauthorized TCP connections from causing performance degradation and unwanted TCP SYN flooding, using a TCP Reset function with the **service resetinbound** command
- ☐ Limiting MAC address exposure by disabling the Proxy ARP feature using the **sysopt noproxyarp outside** command
- ☐ Understanding TCP SYN flooding and MAC spoofing attacks

Functionality and solution verification

- ☐ This question has two objectives. The first is to reset inbound TCP sessions that attempt to traverse the Cisco ASA firewall and that are denied by the firewall based on access lists or AAA settings. The second is to disable the proxy ARP function on the Cisco ASA firewall.
- ☐ Both of these functions have a unique role. In rare circumstances, you might want to disable them, because they could potentially conflict or cause irregularities.

- These features also have advantages. For example, the TCP reset function (TCP RST flag) to the denied host also terminates the identity request (IDENT) connections, stopping outside hosts from retransmitting the SYN by resetting the IDENT process. This prevents any potential TCP SYN flooding.
- Similarly, disabling proxy ARP can limit the exposure of MAC addresses to external users that can potentially be used during a MAC spoofing attack. However, this is not a best practice and should be carefully evaluated before you use it.
- The question says not to use an ACL to complete this task.
- You will see **show** command outputs so that you can check and verify the requirements laid out in the question.
- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

The following outputs verify the required prevention techniques on the ASA/abc1 context:

```
ASA1/abc1# show run service
service resetinbound

ASA1/abc1# show run sysopt
sysopt noproxyarp outside
```

Question 8.3: Restricting unauthorized access (4 points)

Configure R1 to restrict unauthorized TCP connections, meeting all the following requirements:

- An intruder has gained illegitimate access to some of the devices in your network, and has established a Telnet session to the R1 Loopback0 IP address, and is making unauthorized changes to the router configuration.

 Please see page 474 for more details.

- Configure R1 to prevent the unauthorized TCP session by matching explicit parameters, thus restricting any source from being able to establish a Telnet session to the R1 Loopback0 IP address.
- Apply the solution to the R1 control plane.
- Ensure that you open the ACL on the ASA1/abc2 context, permitting any source to any destination on TCP port 23, thus ensuring that your solution is responsible for blocking the Telnet session, and not the ASA/abc2 context.
- Do not use ACL to complete this task.
- Do not use ZFW or CBAC to complete this task.
- Verify functionality by establishing a Telnet session from any device in your network to the R1 Loopback 0 IP address. Telnet session to R1 Loopback 0 IP address should fail to connect. However, establishing Telnet session to any other IP address on R1 should be successful (as shown in verification section below).

Skills tested

- ☐ Preventing unauthorized TCP connections using the new Cisco IOS Flexible Packet Matching (FPM) feature
- ☐ Understanding the CoPP feature
- ☐ Knowledge of the MQC configuration model using extended FPM capabilities
- ☐ Loading the Protocol Header Definition File (PHDF) files into the router flash and enable it from global configuration mode.
- ☐ Configuring nested policy-maps

Functionality and solution verification

- ☐ Cisco IOS Flexible Packet Matching (FPM) is another new technology in the new CCIE Security v3.0 lab blueprint. FPM is one of the important technologies, so candidates should be well-prepared.

- The objective of this question is to configure CoPP protection with the MQC configuration model using extended FPM capabilities. FPM can be used in a variety of scenarios, performing deep packet inspection with its ability to perform granular Layer 2 through 7 matching.
- The reason for using simplified Telnet session blocking in this question is to ensure that you can verify your FPM solution by passing the Telnet traffic. If complex parameters were to be defined, you wouldn't be able to validate the FPM solution without real-time traffic. Therefore, this question will provide complete functionality verification and a clear understanding of how FPM deep packet inspection works.
- This question could be easily configured using a regular extended ACL to match the restrictive Telnet sessions and using the traditional MQC model and applying it to the CoPP. However, the question clearly says not to use an ACL to complete this task. Therefore, using FPM is the only other option.
- You need to configure two FPM (deep packet inspection) class-maps. The first class-map should be of type stack to match the TCP packet in the IP header. The second class-map should be of type access-control, matching additional parameters such as destination-port and destination-IP-address.
- Configure two policy-maps, both access-control types. The first policy-map should match the attributes (destination-port and destination-IP) and define the drop action to it. The second policy-map should match the stack-type class-map and apply the first policy-map as a child in a nested fashion. Review the solution shown next.
- All other Telnet sessions except those matching the previous requirement should work flawlessly.
- Note that a stack-type class-map in a policy-map cannot be applied directly to the CoPP. This is why you need to configure the nested approach.
- Ensure that you open the ACL on the ASA1/abc2 context, permitting any source to any destination on TCP port 23. This ensures that your previous solution is responsible for blocking the Telnet session and not the ASA/abc2 context.
- You will see **show** command outputs so that you can check and verify the requirements laid out in the question.
- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

Before you can configure FPM, you need to load the Protocol Header Definition File (PHDF) files into the router flash and enable it from global configuration mode.

FPM provides ready-made definitions for these standard protocols (IP, TCP, UDP, ICMP) that can be loaded onto the router with the **load protocol** command: ip.phdf, tcp.phdf, udp.phdf, and icmp.phdf.

Ensure that the PHDF files are copied in the flash, and then enable them as shown here:

```
R1# config term
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# load protocol flash:ip.phdf
R1(config)# load protocol flash:tcp.phdf
```

After the PHDF modules are loaded, you can start configuring the relevant FPM configuration.

The following outputs verify the FPM configuration using the extended MQC nested configuration model. Note that an ACL is not used to complete this task.

```
R1# show policy-map type access-control control-plane
 Control Plane

  Service-policy access-control input: blockTCP23

    Class-map: matchTCPstack (match-all)
      2 packets, 120 bytes
      5 minute offered rate 0 bps
     Match: field IP protocol eq 6 next TCP

     Service-policy access-control : dropTCP23

       Class-map: TCP23classmap (match-all)
```

 Please see page 474 for more details.

```
          2 packets, 120 bytes
          5 minute offered rate 0 bps
          Match: field TCP dest-port eq 23
          Match: field IP dest-addr eq 10.1.1.1
      drop

        Class-map: class-default (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any

    Class-map: class-default (match-any)
      1540 packets, 236261 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any

R1# show run ¦ section class-map
class-map type access-control match-all TCP23classmap
 match field TCP dest-port eq 23
 match field IP dest-addr eq 10.1.1.1
class-map type stack match-all matchTCPstack
 match field IP protocol eq 6 next TCP

R1# show run ¦ section policy-map
policy-map type access-control dropTCP23
 class TCP23classmap
   drop
policy-map type access-control blockTCP23
 class matchTCPstack
  service-policy dropTCP23
```

 Please see page 474 for more details.

```
R1# show run ¦ section control-plane
control-plane
 service-policy type access-control input blockTCP23

ASA1/abc2# show access-list 100
access-list 100; 13 elements
access-list 100 line 1 extended permit icmp any any (hitcnt=212) 0x94aa4719
access-list 100 line 2 extended permit udp host 10.5.5.5 host 10.1.1.1 eq ntp (hitcnt=1711) 0x7daffffc
access-list 100 line 3 extended permit udp host 192.168.9.10 host 10.1.1.1 eq ntp (hitcnt=779) 0x27805571
access-list 100 line 4 extended permit tcp any host 10.1.1.1 eq www (hitcnt=0) 0xe9b170c0
access-list 100 line 5 extended permit esp any any (hitcnt=516) 0x81ecd498
access-list 100 line 6 extended permit udp any any eq isakmp (hitcnt=554) 0x02e4ad13
access-list 100 line 7 extended permit udp host 192.168.9.3 host 192.168.3.11 eq 848 (hitcnt=10) 0x35937c04
access-list 100 line 8 extended permit udp host 192.168.6.11 host 192.168.3.11 eq 848 (hitcnt=14) 0x240b0a27
access-list 100 line 9 extended permit udp host 192.168.64.6 host 192.168.3.11 eq 848 (hitcnt=2) 0x6a0b93f3
access-list 100 line 10 extended permit tcp host 192.168.4.11 host 192.168.2.14 eq tacacs (hitcnt=12)
0x40b74674
access-list 100 line 11 extended permit tcp any host 192.168.4.11 eq telnet (hitcnt=6) 0xeeaa659a
access-list 100 line 12 extended permit tcp host 192.168.8.11 host 192.168.2.14 eq tacacs (hitcnt=8)
0xf4abf98f
access-list 100 line 13 extended permit tcp any any eq telnet (hitcnt=10) 0x1b0c68e7
```

When this configuration is OK, you can perform verification steps to check its functionality by establishing Telnet sessions from any device (the example is from R6) to the R1 Loopback0 IP address is unsuccessful as per requirement, as shown next. However, the Telnet session to the other IP address on R1 is successful.

```
R6# telnet 10.1.1.1
Trying 10.1.1.1 ...
% Connection timed out; remote host not responding
```

```
R6# telnet 192.168.3.11
Trying 192.168.3.11 ... Open
User Access Verification
Password: cisco
R1> exit
[Connection to 192.168.3.11 closed by foreign host]
R6#
```

Question 8.4: ARP spoofing attack (3 points)

Configure Sw2 to protect against ARP spoofing attacks, meeting all the following requirements:

- An intruder is attempting to poison ARP table entries of critical devices in VLAN 50.
- Configure a countermeasure on Sw2 to protect against ARP spoofing attacks. Check the source MAC addresses and IP address fields of all ARP entering packets to see if the ARP requester is valid in the snooping binding. If it isn't, traffic should be blocked.
- Additionally, configure rate limiting for all incoming ARP packets to 10 packets per second.
- The DHCP server resides on Sw2 interface FastEthernet0/15. Ensure that this port is the trusted port to reply to DHCP requests on the network.

Skills tested

- ☐ Configuring a countermeasure technique on Cisco Catalyst switches to prevent an ARP spoofing attack using the Dynamic ARP Inspection (DAI) feature
- ☐ Understanding ARP spoofing and DHCP attacks
- ☐ Knowledge of both DAI and DHCP snooping features using the DHCP snooping binding table and its capabilities

Functionality and solution verification

- The objective of this question is to protect VLAN 50 devices from ARP poisoning attacks using the DAI feature. This prevents ARP spoofing attacks by intercepting all ARP requests and responses.
- This task has an important point to remember: the DHCP snooping feature is a prerequisite for DAI functionality to work. It depends on the snooping binding table, which is built and populated dynamically when the DHCP snooping feature is enabled. You can also populate static entries into this table.
- When DHCP snooping is enabled, all ports by default in the VLAN are "untrusted" for DHCP replies, except for the port that is explicitly configured as "trusted." With this port, the DHCP server is connected and is the only authorized port to send DHCP replies out of the switch (interface FastEthernet0/15 in this case). Then, enable DAI on Sw2 for validating source MAC and IP addresses of all incoming ARP packets. When both DAI and DHCP snooping are enabled, all ARP packets must match the IP/MAC binding table entries. If the entries do not match, the switch discards those packets in the bit bucket.
- You will see **show** command outputs so that you can check and verify the requirements laid out in the question.
- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all devices.

The following outputs verify that the DHCP snooping and DAI features are both enabled on VLAN 50 and meet all other requirements:

```
Sw2# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
50
DHCP snooping is operational on following VLANs:
50
```

 Please see page 474 for more details.

```
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id format: vlan-mod-port
    remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
FastEthernet0/15             yes         unlimited
Sw2#

Sw2# show ip arp inspection vlan 50
Source Mac Validation      : Enabled
Destination Mac Validation : Disabled
IP Address Validation      : Enabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
   50     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
   50     Deny             Deny              Off

Sw2# show ip arp inspection interfaces FastEthernet 0/15
 Interface        Trust State     Rate (pps)    Burst Interval
 --------------   -----------     ----------    --------------
 Fa0/15           Trusted                 10                 1
```

 Please see page 474 for more details.

Overview

Practice Labs in this book are based on the CCIE Security v3.0 Lab Exam blueprint. All sections in these labs closely mimic the real lab exam, providing candidates with a comprehensive mock lab scenario with greater complexity to prepare you for the real lab exam.

Labs in this book are multiprotocol, multitechnology, testing you in all areas as outlined in the CCIE Security Lab blueprint v3.0.

To assist you, initial configurations and final solution configurations are provided for the entire lab, including common **show** command outputs from all the devices in the topology.

In addition, an "Ask the Proctor" section is provided at the end of the lab. It provides assistance and common answers to ensure that you are following the correct solution path. Try to avoid referring to this section too often, though, because this luxury is not available on the real lab exam.

Furthermore, a "Lab Debrief" section is provided, which gives you a comprehensive analysis of what is required and how the desired result is achieved. The "Lab Debrief" also provides verification and solution tips, troubleshooting hints, and highlights of the integrated complexities, if any.

Each Practice Lab lasts 8 hours and is worth 100 points. You must score at least 80 to pass. The lab has been designed such that you should be able to complete all the questions in 8 hours, excluding prelab setup such as initial configuration, IP addressing, IP routing, and hardware cabling.

NOTE

Hardware cabling, IP addressing, and IP routing are preconfigured in the real CCIE Lab, except for the security appliances, the ASA firewall, and IPS sensor. (Candidates are required to configure the ASA and IPS.)

Initial configurations are provided, including basic IP addressing and IP routing. You can copy and paste the initials to your devices before you start the Practice Lab. You may want to allow an additional hour for prelab setup and cabling your rack. Use the cabling instructions shown in Figures 2-1 and 2-2 to cable all devices in your topology, and observe the instructions in the general guidelines that follow.

You can use any combination of devices, as long as you fulfill the lab topology diagram shown in Figure 2-3. You are not required to use same model used in this lab.

You will now be guided through the equipment requirements and prelab setup in preparation for completing Practice Lab 2.

NOTE

The equipment list used for both Practice Labs in this book is the same.

Equipment List

You need the hardware and software components listed in Table 2-1 to mount Practice Lab 2.

TABLE 2-1 Equipment list

Device	Model	Software	Interfaces
R1 R2 R3 R4 R5 R6	Six Cisco ISR (Integrated Services Routers) any model	Cisco Router IOS Version 12.4(15)T or above (Advanced Enterprise Services K9 image)	2 Gigabit Ethernet interfaces and 2 Serial (sync/async) interfaces on each Router
Sw1 Sw2	Two Cisco 3560 Catalyst Switches	Cisco Catalyst IOS Version 12.2(44)SE1 or above (Advanced IP Services K9 image)	24 ports on each Switch
ASA1 ASA2	Two Cisco ASA 5510 (or above) Firewall Appliance	Cisco ASA Software Version 8.0(3) (Security Plus license)	4 Ethernet interfaces and 1 Management interface on each ASA Firewall
IPS	One Cisco IPS 4240 (or above) Sensor Appliance	Cisco IPS Sensor Software Version 6.1(1)E2 or above with latest Signature Update	4 Gigabit Ethernets Sensing interfaces 1 Management interface
Server PC	One Desktop PC	Microsoft Windows 2003 Server (Service Pack 2) with Cisco Secure ACS server software version 4.1	1 Ethernet
Test PC	One Desktop PC	Microsoft Windows XP with Cisco AnyConnect VPN Client version 2.3.*x* and Cisco Secure VPN client version 5.*x*	1 Ethernet

General Guidelines

- Read the entire Practice Lab document before you start.
- Knowledge of configuration and troubleshooting techniques is part of the lab exam.
- You are allowed to add to, remove, and modify any static/default routes as required.
- Use "cisco" as the password for any authentication string, enable-password, and TACACS+/RADIUS key, or for any other purpose during this Practice Lab.
- You can add loopbacks as specified during this Practice Lab.
- You must time yourself to complete this Practice Lab exam in 8 hours.
- The Practice Lab has 100 points total, and you must score at least 80 to pass. Each section head says how many points that section is worth.
- Do not configure any AAA authentication and authorization on the console and aux ports.

NOTE
The prelab physical cabling of all devices used for both Practice Labs in this book remains the same with no changes in the wiring diagram.

Prelab Setup and Cabling Instructions

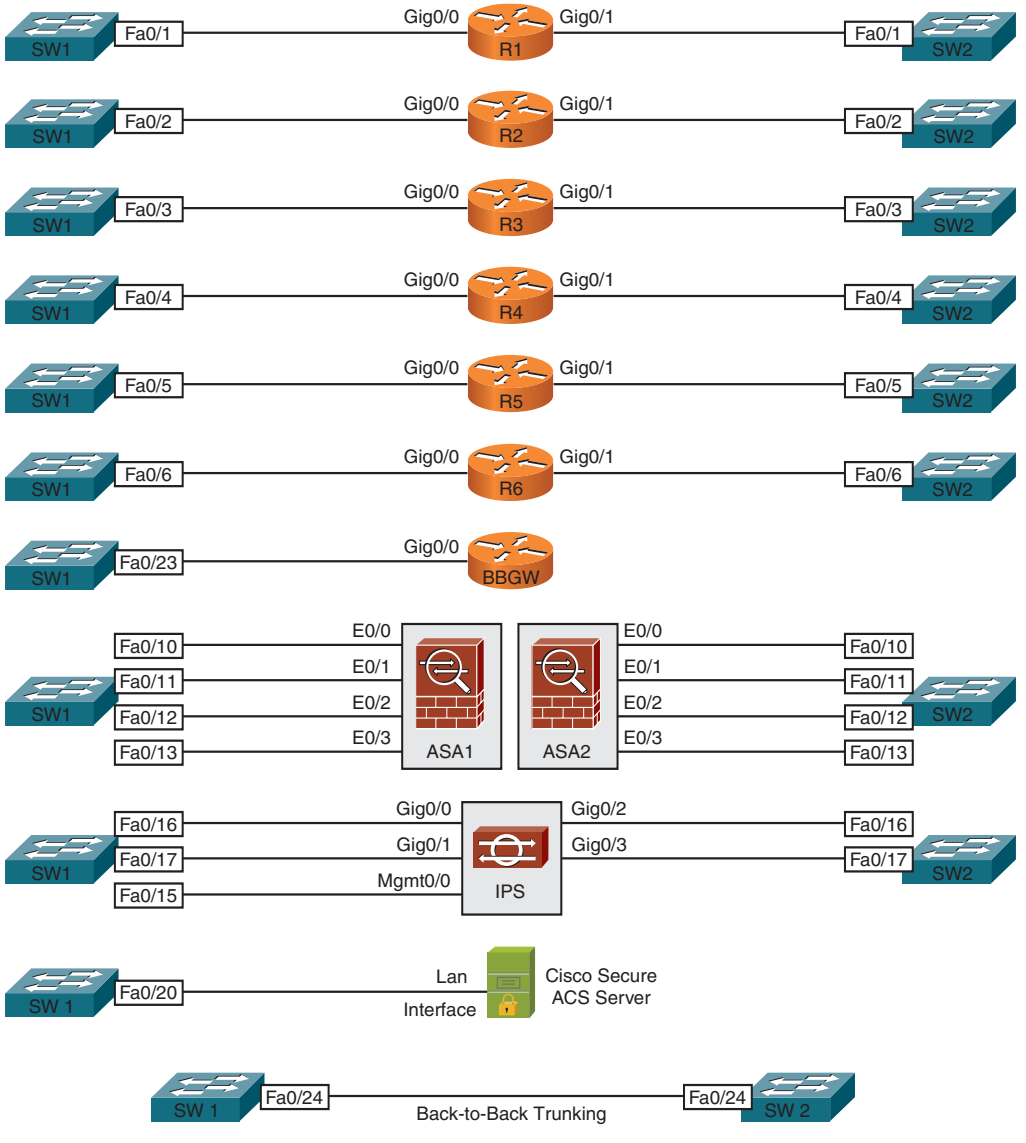
You can use any combination of routers, as long as you fulfill the topology diagram outlined in Figure 2-3. You are not required to use the same model of routers. You need to set up the devices using the following cabling instructions to start Practice Lab 2. Use Figures 2-1 and 2-2 to cable all devices in your topology. It is not a requirement to use the same type or sequence of interface. You may use any combination of interface(s) as long as you fulfill the requirement.

Catalyst Switchport Cabling Diagram

Figure 2-1 illustrates the complete details of how to cable all your devices to both of the Catalyst switches before starting this lab as part of the prelab setup. You are not required to use the same type or sequence of interface. You may use any combination of interface(s), as long as you fulfill the requirement. However, it will be much easier for you to copy and paste the initial configuration and refer to the final solutions if you use the same cabling schema.

 Please see page 474 for more details.

FIGURE 2-1
Catalyst switchport cabling diagram

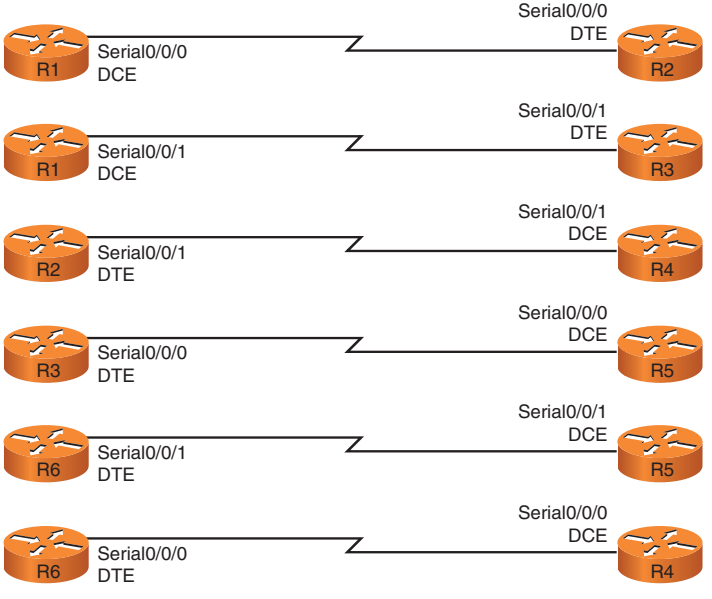


 Please see page 474 for more details.

Serial WAN Interface Cabling Diagram

Figure 2-2 illustrates the complete details of how to cable all your serial WAN interfaces back-to-back. Again, you are not required to use the same type or sequence of interface. You may use any combination of interface(s) as long as you fulfill the requirement. However, it will be much easier for you to copy and paste the initial configuration and refer to the final solutions if you use the same cabling schema.

FIGURE 2-2
Serial WAN interface cabling diagram



NOTE

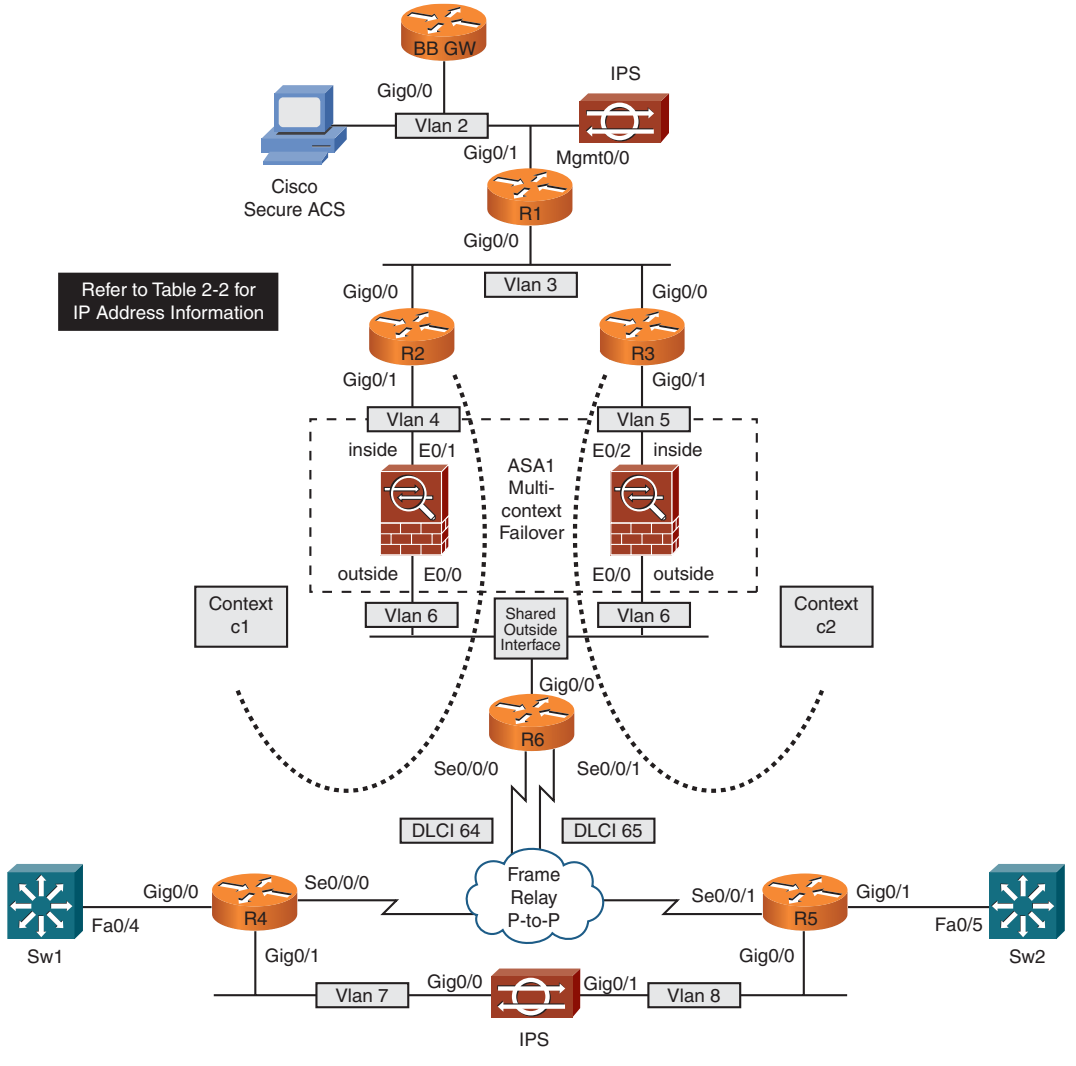
All Serial interfaces are connected to each other back-to-back.

Clock rate and Frame Relay switching are preconfigured in the initial configuration provided.

Lab Topology Diagram

Figure 2-3 illustrates the logical lab exam topology. This diagram is very important and perhaps is the most referenced item throughout the exam. It is highly recommended that you spend a few minutes focusing on how the logical setup is done (mind mapping). Also redraw the entire diagram by yourself. This will help reinforce the setup and will be much easier for you navigating through the topology while working on the questions. Take note of Table 2-2, which provides comprehensive details that map this diagram.

FIGURE 2-3
Lab topology diagram



NOTE

The BB GW router shown in Figure 2-3 is not compulsory. It's OK if you cannot arrange to use this router; it is used for default GW purposes only in this lab. In your scenario, it could be your service provider or upstream router. However, if you can use a spare router, any low-end router will do, such as the 2500 series or above, with any Cisco IOS software version with the basic IP Plus image. Additionally, you can use this router as a terminal/CommServer for console connections to all devices.

IP Address Details

Table 2-2 is a complete list of IP addresses, relevant VLAN numbers, and DLCI information for all devices used in this lab. All of them have been preconfigured in the initial configuration files provided. You can simply copy and paste the initial configuration if you use same cabling schema.

TABLE 2-2 IP address information

Device	Interface	IP Address	Mask	VLAN/DLCI
R1	GigabitEthernet0/0	192.168.3.11	255.255.255.0	Vlan 3
	GigabitEthernet0/1	192.168.2.11	255.255.255.0	Vlan 2
	Loopback0	10.1.1.1	255.255.255.0	—
R2	GigabitEthernet0/0	192.168.3.2	255.255.255.0	Vlan 3
	GigabitEthernet0/1	192.168.4.2	255.255.255.0	Vlan 4
	Loopback0	10.2.2.2	255.255.255.0	—
R3	GigabitEthernet0/0	192.168.3.3	255.255.255.0	Vlan 3
	GigabitEthernet0/1	192.168.5.3	255.255.255.0	Vlan 5
	Loopback0	10.3.3.3	255.255.255.0	—
R4	Serial0/0/0	192.168.64.4	255.255.255.0	DLCI 64
	GigabitEthernet0/0	192.168.41.1	255.255.255.0	—
	GigabitEthernet0/1	192.168.45.4	255.255.255.0	Vlan 7
	Loopback0	10.4.4.4	255.255.255.0	—
R5	Serial0/0/1	192.168.65.5	255.255.255.0	DLCI 65
	GigabitEthernet0/0	192.168.45.5	255.255.255.0	Vlan 8
	GigabitEthernet0/1	192.168.52.1	255.255.255.0	—
	Loopback0	10.5.5.5	255.255.255.0	—
R6	Serial0/0/0	192.168.64.6	255.255.255.0	DLCI 64
	Serial0/0/1	192.168.65.6	255.255.255.0	DLCI 65
	GigabitEthernet0/0	192.168.6.6	255.255.255.0	Vlan 6
	Loopback0	10.6.6.6	255.255.255.0	—

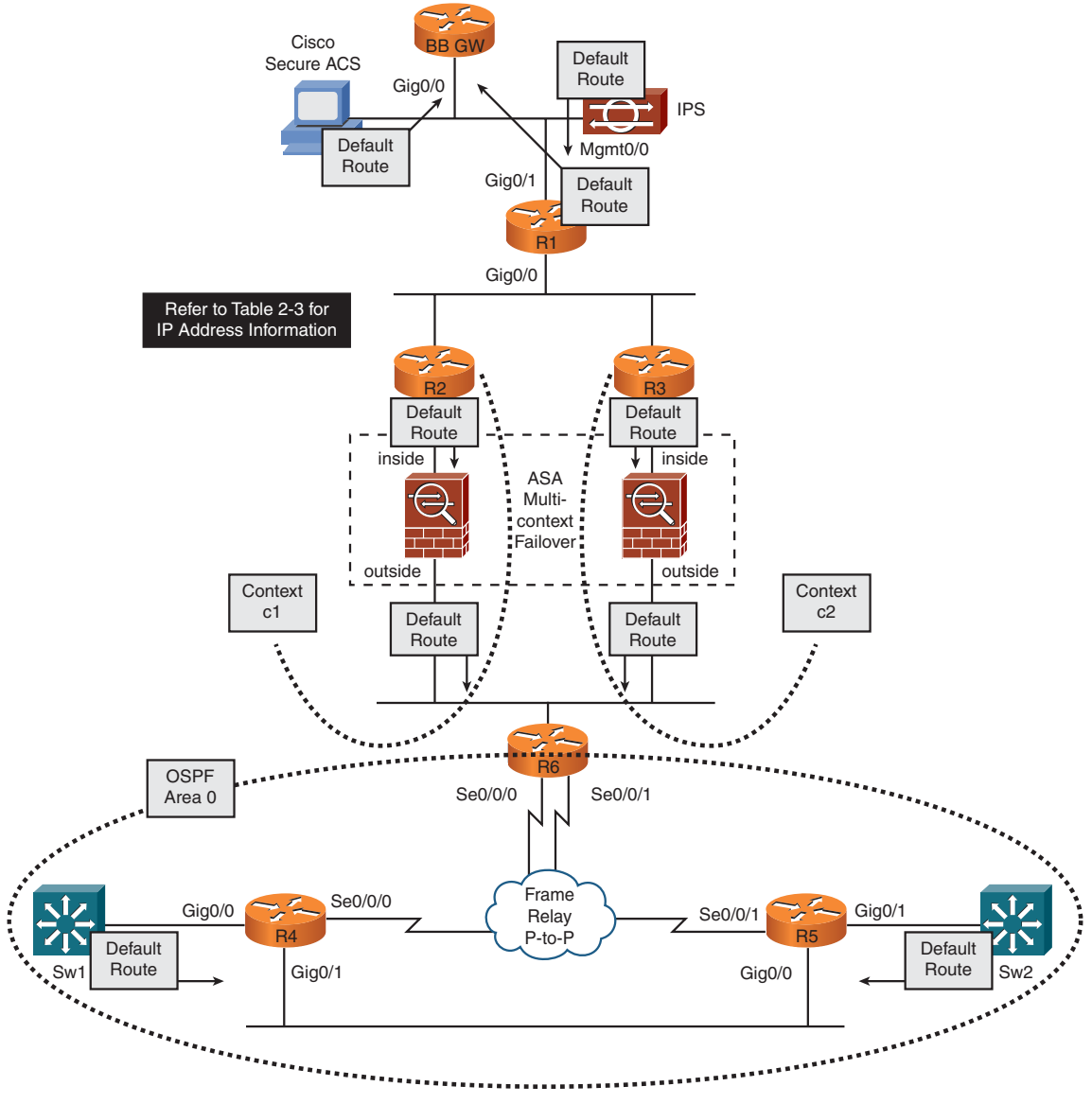
TABLE 2-2 *Continued*

Device	Interface	IP Address	Mask	VLAN/DLCI
Sw1	Loopback0	10.7.7.7	255.255.255.0	—
	FastEthernet0/4	192.168.41.2	255.255.255.0	—
Sw2	Loopback0	10.8.8.8	255.255.255.0	—
	FastEthernet0/5	192.168.52.2	255.255.255.0	—
ASA1 context c1	Ethernet0/0	192.168.6.10	255.255.255.0	Vlan 6
	Ethernet0/1	192.168.4.10	255.255.255.0	Vlan 4
ASA1 context c2	Ethernet0/0	192.168.6.11	255.255.255.0	Vlan 6
	Ethernet0/2	192.168.5.10	255.255.255.0	Vlan 5
BB GW	GigabitEthernet0/0	192.168.2.1	255.255.255.0	Vlan 2
IPS	Management0/0	192.168.2.12	255.255.255.0	Vlan 2
Cisco Secure ACS	LAN Interface	192.168.2.14	255.255.255.0	Vlan 2

IP Routing Protocol Diagram

Figure 2-4 illustrates the IP routing protocol setup in this exam topology. It shows which protocols are used in this exam, including static and default routes. Table 2-3 provides comprehensive details that map this diagram.

FIGURE 2-4
Routing protocol information



NOTE
Security appliances shown in this diagram (the ASA firewall and IPS sensor) are not preconfigured in this Practice Lab. You are required to configure the ASA firewall and IPS sensor accordingly, as stated in the Practice Lab questions.

IP Routing Details

Table 2-3 provides complete details of IP Routing for all devices used in this lab. All of them have been preconfigured in the initial configuration files provided, except for the security appliances—the ASA firewall and IPS sensor (candidates are required to configure the ASA and IPS). For all remaining devices, you can simply copy and paste the initial configuration if you are using same cabling schema.

TABLE 2-3 IP routing information

Device	Route Type	Protocol	Network/Mask	Other Details
R1	Default	—	0.0.0.0/0	Next hop 192.168.2.1 (BB GW router)
	Static	—	10.2.2.0/24 10.4.4.0/24 10.6.6.0/24 10.7.7.0/24 192.168.0.0/16	Next hop 192.168.3.2 (R2)
	Static	—	10.3.3.0/24 10.5.5.0/24 10.8.8.0/24	Next hop 192.168.3.3 (R3)
R2	Default	—	0.0.0.0/0	Next hop 192.168.4.10 (ASA/c1/inside interface)
	Static	—	10.1.1.0/24	Next hop 192.168.3.11 (R1)
R3	Default	—	0.0.0.0/0	Next hop 192.168.5.10 (ASA/c2/inside interface)
R4	Dynamic	OSPF Process 1	Advertise 10.4.4.0/24 192.168.41.0/24 192.168.45.0/24 192.168.64.0/24	Area 0
R5	Dynamic	OSPF Process 1	Advertise 10.5.5.0/24 192.168.45.0/24 192.168.52.0/24 192.168.65.0/24	Area 0

TABLE 2-3 *Continued*

Device	Route Type	Protocol	Network/Mask	Other Details
R6	Dynamic	OSPF Process 1	Advertise 10.6.6.0/24 192.168.64.0/24 192.168.65.0/24	Area 0 and, Redistribute Connected and Static into OSPF
	Static	—	10.1.1.0/24 10.2.2.0/24 192.168.2.0/24 192.168.3.0/24 192.168.4.0/24	Next hop 192.168.6.10 (ASA/c1/outside interface)
	Static	—	10.3.3.0/24 192.168.5.0/24	Next hop 192.168.6.11 (ASA/c2/outside interface)
Sw1	Default	—	0.0.0.0/0	Next hop 192.168.41.1 (R4)
	Dynamic	OSPF Process 1	Advertise 10.7.7.0/24 192.168.41.0/24	Area 0
Sw2	Default	—	0.0.0.0/0	Next hop 192.168.52.1 (R5)
	Dynamic	OSPF Process 1	Advertise 10.8.8.0/24 192.168.52.0/24	Area 0
ASA1 context 'c1'	Default route on outside interface	—	0.0.0.0/0	Next hop 192.168.6.6 (R6)
	Static routes on inside interface	—	10.1.1.0/24 10.2.2.0/24 192.168.2.0/24 192.168.3.0/24	Next hop 192.168.4.2 (R2)
ASA1 context 'c2'	Default route on outside interface	—	0.0.0.0/0	Next hop 192.168.6.6 (R6)
	Static routes on inside interface	—	10.1.1.0/24 10.3.3.0/24	Next hop 192.168.5.3 (R3)
IPS	Default	—	0.0.0.0/0	Next hop 192.168.2.11 (BB GW router)
Cisco Secure ACS	Default	—	0.0.0.0/0	Next hop 192.168.2.11 (R1)

Practice Lab 2

Section 1.0: Core Configuration (14 Points)

Question 1.1: Initializing the ASA1 firewall (5 points)

Initialize the ASA1 firewall, meeting all the following requirements:

- Configure the ASA1 firewall in multicontext routed mode, as shown in Figure 2-3.
- Configure hostname "ASA1" and enable password "cisco."
- Create three contexts as shown in Tables 2-4 through 2-8.
- Context names are case-sensitive. Use the exact names and numbers shown in the tables.
- Assign context "admin" as the admin-context.
- Assign interfaces as shown in the tables. Do not map physical interface names to logical names.
- Both contexts must use shared outside interface Ethernet0/0.
- Enable automatic assignment of unique MAC addresses to each shared context interface. Do not use manual MAC addresses for this task.
- Configure IP addresses and all other initialization parameters as shown in the tables.
- Configure static and default routes within context as shown in the tables. You can also refer to Figure 2-4 and Table 2-3 for more information.
- To perform basic verification using ping tests throughout this Practice Lab, you are allowed to permit **icmp any any** in your ACL in both contexts on ASA1.
- Ensure that you can ping all the interfaces including Loopback0 on Sw1 and Sw2 from context c1.

TABLE 2-4 Context name **admin**

Assign Physical Interface	Logical Name	VLAN	Save Config
Management0/0	mgmt	—	disk0:/admin

TABLE 2-5 Context name **c1**

Assign Physical Interface	Logical Name	VLAN	Save Config
Ethernet0/0	outside	6	disk0:/c1
Ethernet0/1	inside	4	

TABLE 2-6 Context name **c2**

Assign Physical Interface	Logical Name	VLAN	Save Config
Ethernet0/0	outside	6	disk0:/c2
Ethernet0/2	inside	5	

TABLE 2-7 Context initialization details

Context	Interface	IP Address/Mask	Nameif	Security Level
admin	mgmt	none	mgmt	100
c1	outside inside	192.168.6.10/24 192.168.4.10/24	outside inside	0 100
c2	outside inside	192.168.6.11/24 192.168.5.10/24	outside inside	0 100

TABLE 2-8 IP routing initialization details

Context	Route Type	Network Prefix(es)	Next Hop
c1	Configure Default route on outside interface Configure Static routes on inside interface	0.0.0.0/0 10.1.1.0/24 10.2.2.0/24 192.168.2.0/24 192.168.3.0/24	192.168.6.6 (R6) 192.168.4.2 (R2)
c2	Configure Default route on outside interface Configure Static routes on inside interface	0.0.0.0/0 10.1.1.0/24 10.3.3.0/24	192.168.6.6 (R6) 192.168.5.3 (R3)

Question 1.2: Configuring Active-Active Stateful Failover (5 points)

Configure the ASA1 and ASA2 firewalls with Active-Active Stateful Failover, meeting all the following requirements:

- Initialize the ASA2 firewall in multicontext routed mode.
- Configure LAN-based failover on both firewalls with ASA1 as the primary device and ASA2 as the secondary device.
- Configure failover parameters and IP addresses as shown in Tables 2-9 and 2-10 and Listings 2-1 and 2-2.
- Secure the failover communication sent over the failover and Stateful Failover links between the units with a failover key "cisco."
- For verification, ensure that your output matches the listings.

TABLE 2-9 Failover initialization details

Interface	Nameif	Primary IP Address/Mask	Standby IP Address/Mask
Ethernet0/3	failint	192.168.50.10/24	192.168.50.11/24

TABLE 2-10 Failover Active-Active details

Context	Failover Group Policy
c1	Group 1 ASA1 Primary and ASA2 Secondary
c2	Group 2 ASA2 Primary and ASA1 Secondary

LISTING 2-1 Failover verification output from ASA1

```
ASA1# show failover
Failover On
Failover unit Primary
Failover LAN Interface: failint Ethernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 5 of 250 maximum
Version: Ours 8.0(4), Mate 8.0(4)
Group 1 last failover at: 03:54:49 UTC Aug 5 2009
Group 2 last failover at: 03:54:48 UTC Aug 5 2009

  This host:    Primary
  Group 1       State:          Active
                Active time:    248146 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)

                slot 0: ASA5510 hw/sw rev (2.0/8.0(4)) status (Up Sys)
                  admin Interface mgmt (0.0.0.0): No Link (Waiting)
```

```
                    c1 Interface outside (192.168.6.10): Normal
                    c1 Interface inside (192.168.4.10): Normal
                    c2 Interface outside (192.168.6.15): Normal
                    c2 Interface inside (192.168.5.15): Normal
                  slot 1: empty

  Other host:    Secondary
  Group 1        State:          Standby Ready
                 Active time:    0 (sec)
  Group 2        State:          Active
                 Active time:    248138 (sec)

                 slot 0: ASA5510 hw/sw rev (1.0/8.0(4)) status (Up Sys)
                   admin Interface mgmt (0.0.0.0): No Link (Waiting)
                   c1 Interface outside (192.168.6.15): Normal
                   c1 Interface inside (192.168.4.15): Normal
                   c2 Interface outside (192.168.6.11): Normal
                   c2 Interface inside (192.168.5.10): Normal
                 slot 1: empty

Stateful Failover Logical Update Statistics
        Link : failint Ethernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         33196      0          33159      0
        sys cmd         33122      0          33122      0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        36         0          0          0
        ARP tbl         38         0          37         0
```

```
        Xlate_Timeout   0          0          0          0
        SIP Session     0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       33159
        Xmit Q:         0       1       33196
ASA1#
```

LISTING 2-2 Failover verification output from ASA2

```
ASA1# show failover
Failover On
Failover unit Secondary
Failover LAN Interface: failint Ethernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 5 of 250 maximum
Version: Ours 8.0(4), Mate 8.0(4)
Group 1 last failover at: 03:55:31 UTC Aug 5 2009
Group 2 last failover at: 03:55:31 UTC Aug 5 2009

  This host:    Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Active
                Active time:    248264 (sec)
```

```
                slot 0: ASA5510 hw/sw rev (1.0/8.0(4)) status (Up Sys)
                  admin Interface mgmt (0.0.0.0): No Link (Waiting)
                  c1 Interface outside (192.168.6.15): Normal
                  c1 Interface inside (192.168.4.15): Normal
                  c2 Interface outside (192.168.6.11): Normal
                  c2 Interface inside (192.168.5.10): Normal
                slot 1: empty

 Other host:    Primary
 Group 1        State:          Active
                Active time:    248272 (sec)
 Group 2        State:          Standby Ready
                Active time:    0 (sec)

                slot 0: ASA5510 hw/sw rev (2.0/8.0(4)) status (Up Sys)
                  admin Interface mgmt (0.0.0.0): No Link (Waiting)
                  c1 Interface outside (192.168.6.10): Normal
                  c1 Interface inside (192.168.4.10): Normal
                  c2 Interface outside (192.168.6.15): Normal
                  c2 Interface inside (192.168.5.15): Normal
                slot 1: empty

Stateful Failover Logical Update Statistics
        Link : failint Ethernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         33176      0          33213      0
        sys cmd         33139      0          33139      0
        up time         0          0          0          0
        RPC services    0          0          0          0
```

```
        TCP conn        0          0          0          0
        UDP conn        0          0          36         0
        ARP tbl         37         0          38         0
        Xlate_Timeout   0          0          0          0
        SIP Session     0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       33213
        Xmit Q:         0       1       33176
ASA1#
```

Question 1.3: Initializing IPS Sensor (4 points)

Initialize Cisco IPS Sensor, meeting all the following requirements:

- Configure IPS sensor appliance between R4 and R5 as shown in Figure 2-3.
- Configure hostname "IPS" and allow Telnet sessions to IPS sensor from VLAN 2.
- Configure the Command and Control (Management0/0) interface IP address 192.168.2.12/24 with default gateway 192.168.2.11.
- Configure Catalyst switches as appropriate to complete this question.
- Configure IPS sensor for inline interface pairing using information in Table 2-11. Refer to Figure 2-3 for more information.
- You can also refer to Figure 2-1 for physical port connections.
- Verify that the virtual sensor is passing traffic in inline mode. Ensure that you can ping all interfaces, including Loopback0 of R5 and Sw2 from R4.

 Please see page 474 for more details.

NOTE

You can use IPS Device Manager (IDM) from the Cisco Secure ACS server PC to complete the remaining tasks on the sensor.

TABLE 2-11 Inline interface pairing information

Sensor Placement Policy	Name	Physical Interfaces	Virtual Sensor	Signature Policy
Inline Physical Pair between R4 and R5 GigabitEthernet	mypair	Interface1=GigabitEthernet0/0 Interface2=GigabitEthernet0/1	vs0	sig0

Section 2.0: Cisco Firewall (13 Points)

Question 2.1: Network Address Translation (NAT) (3 points)

Configure Network Address Translation (NAT) on ASA, meeting all the following requirements:

- Enable NAT control on context c2. Do not enable NAT control on context c1.
- Configure static address translation on context c1 such that when R1 establishes a Telnet session to R4 Loopback0 using its source Loopback0, the source address gets translated to 192.168.6.61. However, when R1 establishes the same Telnet session to R4 Loopback0 without using its source Loopback0 (using any other source), the source address should not get translated and should retain the original IP address.
- Configure dynamic address translation on context c2 for any hosts on the inside to get translated using dynamic pool of 192.168.6.150 through 192.168.6.155. Configure a backup pool with a PAT address using the outside interface in the event the primary pool runs out. Do not use IP addresses in the PAT pool.

Question 2.2: Asymmetric routing support (3 points)

Configure asymmetric routing support on ASA, meeting the following requirement:

- Configure the outside interface in both contexts to support for asymmetrically routed packets, preventing the return packets from being dropped in case a context does not have any session information for the packet.

Question 2.3: Time-based access control (3 points)

Configure time-based access control on the Cisco ASA Firewall in context c1, meeting all the following requirements:

- The network administrator on R2 (with source IP address 10.2.2.2) is provided a one-hour downtime window for a scheduled maintenance to update router configuration of R6 (on IP address 10.6.6.6) between 9 p.m. and 10 p.m. on July 1, 2009.
- Configure the ASA1/c1 context to explicitly permit the specified IP traffic during the specified time.
- Do not use an inbound ACL to complete this task.
- Ensure that you can ping and telnet to R6 (10.6.6.6) from R2 (using source 10.2.2.2) during the downtime window. Ensure that the ping and Telnet fail outside the downtime window.

Question 2.4: Cisco IOS Firewall using CBAC (4 points)

Configure IOS Firewall using Context-Based Access Control (CBAC) on R4, meeting all the following requirements:

- Enable CBAC inspection on R4 to protect networks in your topology. Ensure that CBAC protection continues to function in the event of WAN link down, when rerouting traffic via alternate GigabitEthernet0/1 link. Do not enable CBAC inspection on GigabitEthernet0/1 link. Your solution must have CBAC inspection applied to any one interface only.
- Enable TCP, UDP, HTTP, and ICMP protocols for CBAC inspection.
- Allow Java packets from a trusted site at 198.168.10.25 while implicitly denying Java from all other sites.
- Adjust the firewall settings to delete any half-open sessions when the maximum number of half-open sessions reaches 300. The firewall should stop deleting when the number falls below 200. Additionally, adjust the maximum number of half-open TCP sessions per host to 100.
- Enable HTTP server on Sw1 using nonstandard HTTP port 8080. Verify that you can ping and telnet to Sw1 IP address 192.168.41.2 from R6 upon completion of this task.
- Ensure that all IP connectivity including IP routing and ICMP traffic used for verification for other sections of this lab continues to work. You are allowed to permit ICMP traffic from any source to any destination explicitly in this ACL.

Section 3.0: Cisco VPN (15 Points)

Question 3.1: Configuring Group Encrypted Transport VPN (GETVPN) (4 points)

Configure Group Encrypted Transport VPN (GETVPN) on R1, R3, R5, and R6, meeting all the following requirements:

- Configure GETVPN using preshared keys on R1, R3, R5, and R6 using information in Tables 2-12 and 2-13.
- Use "cisco" for the preshared key on all devices.
- R6 will be the Key Server (KS), and R3, R5, and R6 will be the Group Members (GM).
- You are allowed to update the firewall ACL in context c1 and c2 to complete this task.
- Use the information in the tables to complete this task.

TABLE 2-12 Configuration information for the key server (KS)

ISAKMP Policy	☐ Preshared Key Authentication ☐ 3DES encryption algorithm ☐ Secure Hash Standard (SHA) Hash algorithm ☐ Diffie-Hellman group 2
IPsec Policy	☐ ESP transform using 3DES cipher ☐ ESP transform using HMAC-SHA auth ☐ IPsec profile name = dmvpn_using_gdoi ☐ Set IPsec SA lifetime to 10 hours ☐ Peering using Loopback 0 address
GDOI Parameters	☐ Group name = dmvpn ☐ Group identity number 2 ☐ Unicast Rekey transport with 2 retransmits at 10 seconds interval ☐ Rekey lifetime to 24 hours
Access List Policies	☐ Traffic to be encrypted between any host to any destination for GRE protocol to communicate using GETVPN

 Please see page 474 for more details.

TABLE 2-13 Configuration information for the group members (GM)

ISAKMP Policy	☐ Preshared Key Authentication ☐ 3DES encryption algorithm ☐ Secure Hash Standard (SHA) Hash algorithm ☐ Diffie-Hellman group 2
GDOI Parameters	☐ Group name = dmvpn_gdoi ☐ Group identity number 2 ☐ Key Server IP address 10.6.6.6

Question 3.2: Configuring Dynamic Multipoint VPN (DMVPN) using GDOI (4 points)

Configure Dynamic Multipoint VPN (DMVPN) using GDOI on R1, R3, and R5, meeting all the following requirements:

- Configure DMVPN using GETVPN integration on R1, R3, and R5 using information in Tables 2-14 and 2-15.
- R1 will be the DMVPN Hub router, and R3 and R5 will be the DMVPN spoke routers.
- You are allowed to update the firewall ACL in context c1 and c2 to complete this task.
- Use the information in the tables to complete this task.

TABLE 2-14 Configuration information for the DMVPN hub (R1)

Tunnel Policy	☐ Tunnel number 0 ☐ IP address 172.16.1.1/24 ☐ Peer using Loopback 0 address ☐ Tunnel destination not allowed ☐ NHRP authentication password “cisco” ☐ NHRP Network ID 2 ☐ Secure Tunnel key 2
Routing Policy	☐ Advertise Tunnel 0 and private network Loopback 11 into EIGRP AS 2

TABLE 2-15 Configuration information for the DMVPN spokes (R3 and R5)

Tunnel Policy	☐ Tunnel number 0 ☐ IP address 172.16.1.*X*/24 (where *X* is the spoke router number) ☐ Peer using Loopback 0 address ☐ Tunnel destination not allowed ☐ NHRP authentication password "cisco" ☐ NHRP Network ID 2 ☐ Secure Tunnel key 2
Routing Policy	☐ Advertise Tunnel 0 and private network Loopback 11 into EIGRP AS 2

Question 3.3: Troubleshooting Easy VPN using DVTI (4 points)

Enhanced Easy VPN using the IPsec Dynamic Virtual Tunnel Interface (DVTI) has been preconfigured on R2 and R4 in this question. Your task is to troubleshoot and identify the injected faults and bring up the Easy VPN tunnel, meeting all the following requirements:

- Easy VPN is preconfigured using preshared keys "cisco" on R2 and R4 using information in Tables 2-16 and 2-17.
- R2 is the Easy VPN Hub router, and R4 is the Easy VPN spoke router.
- Five faults are injected into your preconfiguration. Identify these faults, and verify that the tunnel comes up. Note that the faults injected could be related to either incorrect preconfiguration or missing commands to complete the configuration.
- You are allowed to modify the ACL on the ASA/c1 context to complete this task. This excludes the five faults.
- Use the information in the tables to complete this task.

TABLE 2-16 Information for the Easy VPN hub router (R2)

AAA Policy	☐ Named Login Authentication using local database (name = ezvpn) ☐ Named Network Authorization using local database (name = ezvpn) ☐ Local username "cisco" password "cisco"
ISAKMP Policy	☐ Preshared Key Authentication ☐ 3DES encryption algorithm ☐ Secure Hash Standard (SHA) Hash algorithm ☐ Diffie-Hellman group 2 ☐ ISAKMP profile name = ezvpn_dvti
IPsec Policy	☐ Transform set name = ezvpn_trans ☐ ESP transform using 3DES cipher ☐ ESP transform using HMAC-SHA auth ☐ IPsec profile name = ezvpn_dvti
Easy VPN Policy	☐ Group name = cisco ☐ Group password = cisco ☐ Domain name = cisco.com ☐ IP pool = 10.20.20.1 through 10.20.20.100
DVTI Policy	☐ Virtual-Template 1 ☐ IP unnumbered using Loopback0 address ☐ Tunnel Source using Loopback0 address

TABLE 2-17 Information for the Easy VPN spoke router (R4)

Easy VPN Policy	☐ EzVPN profile name = ezvpn_dvti ☐ Group name = cisco ☐ Group password = cisco ☐ Connect type = auto ☐ Mode = client ☐ Xauth mode interactive on console ☐ Peer using R2 Loopback0 address
Apply	☐ Inside interface = GigabitEthernet0/0 ☐ Outside interface = Serial0/0/0

Question 3.4: Troubleshooting L2L IPsec VPN using VTI (3 points)

LAN-to-LAN (L2L) IPsec VPN using the Virtual Tunnel Interface (VTI) has been preconfigured between R4 and R5 in this question. Your task is to troubleshoot and identify the injected faults and bring up the IPsec L2L VPN tunnel, meeting all the following requirements:

- L2L VPN is preconfigured using preshared keys "cisco" on R4 and R5 using information in Table 2-18.
- Four faults are injected into your preconfiguration. Identify these faults, and verify that the tunnel comes up. Note that the faults injected could be related to either incorrect preconfiguration or missing commands to complete the configuration.
- Use the information in the table to complete this task.

TABLE 2-18 Configuration information

ISAKMP Policy	☐ Preshared Key Authentication ☐ 3DES encryption algorithm ☐ Secure Hash Standard (SHA) Hash algorithm ☐ Diffie-Hellman group 2
IPsec Policy	☐ Transform set name = L2L_trans ☐ ESP transform using 3DES cipher ☐ ESP transform using HMAC-SHA auth ☐ IPsec profile name = L2L_VTI
VTI Policy	☐ VTI Tunnel Number 45 ☐ Tunnel IP address on R4 and R5 (100.1.1.1/24 and 100.1.1.2/24), respectively ☐ Tunnel Source = GigabitEthernet (192.168.45.0)
Routing Policy	☐ Dynamic routing using RIP version 2 ☐ Disable autosummarization ☐ Advertise subnets Loopback 45 and Tunnel 45

Section 4.0: Cisco IPS (Intrusion Prevention System) (8 Points)

Question 4.1: Configuring IPS signatures (4 points)

Configure Cisco IPS sensor appliance, meeting both of the following requirements:

- Configure signature tuning and custom signatures in sig0 using information in Table 2-19 to complete this task.

TABLE 2-19 IPS signature configuration information

Signature Tuning	☐ Enable ICMP echo and echo-reply signatures. ☐ Set the alert severity to medium level and action to produce alert.
Custom Signature	☐ Create a custom Sig# **65000** named "Large ICMP attack" that inspects all ICMP packets with its IP payload size ranging between 5000 and 6000 bytes. ☐ This signature should trigger only when ICMP traffic is destined for any RFC 1918 address range. ☐ Set the alert severity to medium level and action to produce alert.

- Ensure that a signature is triggered when sending large ICMP ping packets to RFC 1918 address. For example, ping from R4 as follows.

```
R4# ping 10.8.8.8 size 5500
```

Question 4.2: Configuring Cisco IOS IPS (4 points)

Configure Cisco IOS IPS version 5.0 format signature on R1, meeting both of the following requirements:

- Configure R1 for inline intrusion prevention sensor, monitoring packets as they flow through R1.
- Use the information in Table 2-20 to complete this task.

TABLE 2-20 Cisco IOS IPS configuration information

Signature Category Policy	☐ Generate an RSA crypto key and load the Cisco public signature on your router for signature decryption (given below). ☐ Retire all category signatures except IOS_IPS basic category.
IPS Configuration Policy	☐ Config location = flash:ips5/ ☐ IOS IPS name = myIOSipsV5 ☐ Enable SDEE protocol for event notification. ☐ Apply IOS IPS in both directions to GigabitEthernet0/0.
Loading Signature Package File	☐ Load the Cisco IOS IPS file IOS-S416-CLI.pkg from TFTP server 192.168.2.14 onto IDCONF.

Note

Generate an RSA crypto key and load the Cisco public key signature on your router for signature decryption (given next). You can copy and paste this directly into your router configuration:

```
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
  key-string
   30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
   00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
   17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
   B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
   5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
   FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
   50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
   006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
   2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
   F3020301 0001
  quit
  exit
exit
```

NOTE
Download the latest Cisco IOS IPS files to your TFTP server from http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup. This Practice Lab uses IOS-S416-CLI.pkg, but you can use another file.

Section 5.0: Implement Identity Authentication (12 Points)

Question 5.1: Proxy authentication access control (4 points)

Configure proxy authentication and authorization-based access control on the ASA1/c1 context, meeting all the following requirements:

- Enable AAA solution on the ASA1/c1 context to authenticate and authorize Telnet traffic crossing the firewall.

 Please see page 474 for more details.

- The ASA firewall should perform proxy authentication for specific Telnet traffic from host 10.5.5.5 (R5) to host 10.1.1.1 (R1) crossing the ASA1/c1 context. All other traffic should go uninterrupted.
- Complete this task using information in Tables 2-21 and 2-22.

TABLE 2-21 AAA configuration information

AAA Configuration	☐ Configure AAA server parameters on the ASA1/c1 context. Ensure that you can ping the Cisco Secure ACS server. ☐ Use the TACACS+ protocol. ☐ AAA server tag = myACSserver ☐ AAA server IP address 192.168.2.14 using shared secret password "cisco" ☐ Configure maximum number of failed attempts to 2 before TACACS+ server is deemed unavailable. ☐ Enable AAA authentication and authorization using access lists to identify Telnet traffic from host 10.5.5.5 (R5) to host 10.1.1.1 (R1).

TABLE 2-22 ACS configuration information

ACS Configuration	☐ Add the ASA/c1 context inside interface as the AAA client on Cisco Secure ACS server (192.168.2.14). ☐ Configure a new user with privilege 15 on Cisco Secure ACS server "user1" using password "cisco," and assign it to the Default group. ☐ Enable shell EXEC and other parameters necessary to complete authorization. Configure the user1 profile to download idle-timeout set to 5 minutes. ☐ Configure Shell Command Authorization set under the user1 setup explicitly. The profile should allow the Telnet traffic to host 10.1.1.1 (R1).

- Verify the Pass Reports on Cisco Secure ACS server to ensure that user1 is successfully authenticated.
- Ensure that the following output is achieved on the ASA1/c1 context upon successful authentication:

```
ASA1/c1# show uauth
                        Current    Most Seen
Authenticated Users       1          1
Authen In Progress        0          1
user 'user1' at 10.5.5.5, authorized to:
   port 10.1.1.1/telnet
   absolute   timeout: 0:05:00
   inactivity timeout: 0:05:00
ASA1/c1#
```

Question 5.2: Privilege level access control (4 points)

Configure AAA authentication and authorization on R5 and Cisco Secure ACS server, meeting all the following requirements:

- Enable AAA authentication and authorization on R5 using TACACS+ protocol.
- Configure Cisco Secure ACS user profiles using information in Tables 2-23 and 2-24.
- Verify functionality by establishing a Telnet session to R5 from Sw2 and ensure that users get into Privilege level 5 and can execute only the restricted commands specified in the authorization set.
- Ensure that the console port is unaffected by this task.
- Use the information in the tables to complete this task.

TABLE 2-23 AAA configuration information

AAA Configuration	☐ Configure AAA server parameters on R5. Ensure that you can ping the Cisco Secure ACS server. ☐ Use TACACS+ protocol. ☐ AAA server IP address 192.168.2.14 using shared secret password "cisco." ☐ Enable AAA authentication using named method list. ☐ Enable AAA EXEC and command authorization using named method lists. ☐ Do not use a default method list in this task.

TABLE 2-24 ACS configuration information

NAS, User, and Group Setup Policies	☐ Add R5 Serial0/0/1 interface as the AAA client on Cisco Secure ACS server (192.168.2.14). ☐ Configure a new user with privilege level 5 called "netop" using password "cisco," and assign it to a group called "netop." ☐ Enable shell EXEC, privilege level, and other parameters necessary to complete authorization. ☐ Configure the netop group such that it allows network access on Sundays only (24 hour access).

TABLE 2-24 *Continued*

Shell Command Authorization Policy	☐ Configure Shell Command Authorization set under the Shared Profile components called netop. ☐ Users in this group should be able to configure any dynamic routing protocols. ☐ Users should also be able to apply any **interface** specific commands. ☐ Users in this group should be able to execute any **show** commands. ☐ Assign this set to netop group level.

- Verify the Pass Reports on Cisco Secure ACS server to ensure that the netop user is successfully authenticated.
- Perform verification steps by establishing a Telnet session to R5 from Sw2 and ensure that it gets into privilege level 5 with appropriate attributes.

Question 5.3: MAC-based authentication profile (4 points)

Configure MAC-based authentication using Network Access Profile (NAP) on Cisco Secure ACS server, meeting all the following requirements:

- Your network is enabled with Network Admission Control (NAC) setup and some agentless hosts require authentication using ACS.
- Configure MAC authentication bypass (MAB) using NAP to authenticate the agentless client using the host's MAC address to identify and authenticate it.
- Use the information in Table 2-25 to complete this task.

TABLE 2-25 ACS configuration information

NAP Policy	☐ NAP policy name = MAC_bypass ☐ Use RADIUS IETF protocol ☐ Do not configure any posture validation

 Please see page 474 for more details.

TABLE 2-25 *Continued*

MAB Authentication Bypass Policy	☐ Allow MAC-Authentication-Bypass ☐ Use ACS internal database for MAB ☐ MAC address 00-11-22-9F-01-7E should be assigned to Group 5 ☐ MAC address 00-11-22-4A-2D-0F should be assigned to Group 6 ☐ All other unknown MAC addresses should be assigned to the Default group

Section 6.0: Implement Control and Management Plane Security (13 Points)

Question 6.1: Control plane protection (4 points)

Configure control plane protection using Control Plane Policing (CoPP) on R3, meeting all the following requirements:

- Configure CoPP protection using a port-filter policy on R3 to drop all traffic destined to "closed" or nonlistened TCP/UDP ports trying to access this router.
- Do not configure any parameters under the default class that matches any packet.
- You are allowed to configure only one class-map and one policy-map to complete this task.

Question 6.2: Cisco IOS image and configuration protection (3 points)

Configure Cisco IOS image and configuration protection on R2, meeting the following requirements:

- R2 recently experienced a downtime due to malicious intrusion where an intruder erased the IOS image and configuration from the router causing extended downtime of services due to the delay in recovery process.

 Please see page 474 for more details.

- Configure R2 for resilient IOS image and configuration protection such that it maintains a secure copy of the router image and the configuration, hence withstanding any malicious attempts to erase the contents of persistent storage (NVRAM and flash). These secure files cannot be removed by the intruder.
- Do not use any ACL or Cisco IOS Firewall (CBAC or ZFW) configuration to complete this task.

Question 6.3: Router CPU protection (3 points)

Configure router CPU protection on R4, meeting all the following requirements:

- When a packet is forwarded to R4 from Sw1 (directly connected default gateway) and the router has no path to the destination host, R4 generates a Destination Unreachable, Code 1 (Host Unreachable) ICMP message back to Sw1. This can potentially be a target of ICMP-based DoS attack affecting the router CPU.
- Configure R4 to stop generating ICMP Destination Unreachable (Type 3) messages.
- Do not configure any ACL to complete this task.
- Ensure that when Sw1 sends any packet to its default gateway R4 to an unknown destination, R4 should silently discard without replying back to Sw1.

Question 6.4: Secure device access control (3 points)

Configure secure management access control on Sw2, meeting all the following requirements:

- Configure Sw2 to allow management access using SSH protocol only.
- Use local username cisco with password cisco for SSH connections.
- Tune the SSH timeout to 5 seconds and 2 authentication retries.
- Ensure that you can SSH from any device in your network to Sw2 using the SSH protocol.

Section 7.0: Advanced Security (12 Points)

Question 7.1: MAC flooding protection (3 points)

Configure MAC flooding protection on Sw2, meeting both of the following requirements:

- Configure MAC flooding protection and prevention of CAM table (Content Addressable Memory) attacks on Sw2 using information in Table 2-26.
- You are allowed to add new VLANs to complete this task.

TABLE 2-26 Switch configuration information

MAC Flooding Protection Policy	☐ Configure Sw2 interface FastEthernet0/20 using the following parameters. ☐ Assign Data VLAN = 101 ☐ Assign Voice VLAN = 102 ☐ Ensure that the interface is allowed to learn a maximum of ten dynamic MAC addresses of which maximum of eight addresses can be from Data VLAN and two addresses can be from Voice VLAN. ☐ Ensure that all dynamically learned MAC addresses are added to the running configuration. After you save the Sw2 configuration, and if the switch is rebooted for any reason, the interface does not need to relearn these addresses. ☐ When the number of secure MAC addresses reaches the maximum limit, packets with unknown source addresses should be dropped, and the security violation counter should increment. ☐ Do not configure the port to shut down.

Question 7.2: Troubleshooting NBAR (3 points)

Traffic filtering using Network-Based Application Recognition (NBAR) has been preconfigured on R2 and R6 in this question. Your task is to troubleshoot and identify the injected faults and ensure that legitimate traffic is forwarded, meeting all the following requirements:

- Cisco IOS NBAR classification engine using MQC configuration has been preconfigured on routers R2 and R6.
- Four faults are injected into your preconfiguration.
- Open the ACL on the ASA1/c1 context allowing Telnet traffic entering outside interface (ACL 100) from any host to any destination. This excludes the four faults.
- Identify these faults and verify that Telnet traffic using Frame Relay DLCI 65 path (such as traffic from R5/Sw2 to destination R2) with IP precedence bit set to 1 is dropped. All other Telnet traffic to R2 should be functional.
- While fixing this issue, you are allowed to alter the preconfiguration and add, modify, or remove part of the preconfiguration. However, you need to ensure that altering the preconfiguration does not impede any other question.
- Do not configure any parameters under the default class that matches any packet.
- Do not use an ACL to complete this task.
- Do not use CoPP to complete this task.
- For verification, ensure that the Telnet session from R4 to R2 (10.2.2.2) should be successful; however, the telnet from R5 to R2 (10.2.2.2) should fail.

Question 7.3: Configuring ESMTP server protection (3 points)

Configure advanced application layer protocol inspection on the Cisco ASA firewall to protect the ESMTP server, meeting the following requirement:

- Configure the ASA/c1 context to protect the ESMTP mail server preventing malformed message attacks using information in Table 2-27.

TABLE 2-27 ASA1/c1 context configuration information

ESMTP Inspection Policy	☐ Configure advanced ESMTP inspection to match and drop email connections from a specific sender email address joe@myemail.com. ☐ Additionally, drop email connections if the maximum number of email addresses in the To: field exceeds 5. ☐ Also drop email connections if any special characters are detected within the sender or receivers email address such as pipe (|), backquote (`), or null space, to name a few. ☐ Do not apply the policy to the inside or outside interface. The policy must be applied globally. ☐ Do not configure an ACL to complete this task.

Question 7.4: IKE resource exhaustion protection (3 points)

Configure IKE resource exhaustion denial-of-service (DoS) protection on R1, meeting all the following requirements:

- An intruder is attempting to exploit limitations of the IKE protocol to deplete available resources to negotiate IKE SAs (Security Associations) and block legitimate IPsec peers from establishing new IKE SAs or rekey existing IKE SAs.
- Configure R1 to rate-limit inbound UDP/500 traffic from any source to destination R1 Loopback0 preventing CPU processing power and memory resources from being fully consumed by incoming IKE requests.
- Traffic at rates below 32,000 bits per second (bps) with normal burst of 6,000 bytes should be forwarded normally; however, traffic above 32,000 bps packets with twice the normal burst must be dropped. (32,000 bps is loosely equivalent to 35 IKE messages per second.)
- Do not configure Modular QoS CLI (MQC) to complete this task.

Section 8.0: Network Attacks (13 Points)

Question 8.1: Web server attack (3 points)

Configure a mitigation solution to respond to the web server attack, meeting all the following requirements:

- Users are complaining of intermittent access to the web server located in VLAN 2 with IP address 192.168.2.100. Most external clients are cannot load the company's web page hosted on this server.
- Review the outputs that were captured on the ASA1/c1 context during the investigation and troubleshooting of this issue, and configure the ASA1/c1 context to mitigate this problem.
- The solution must be applied to the c1 context outside interface.
- Do not configure or modify network address translation to complete this task.
- Do not use an ACL to complete this task.

```
ASA1/c1# show perfmon
Context: c1
PERFMON STATS:                      Current      Average
Xlates                                0/s          0/s
Connections                        2236/s        321/s
TCP Conns                          2236/s        321/s
UDP Conns                             0/s          0/s
URL Access                            0/s          0/s
URL Server Req                        0/s          0/s
TCP Fixup                             0/s          0/s
TCP Intercept Established Conns       0/s          0/s
TCP Intercept Attempts                0/s          0/s
TCP Embryonic Conns Timeout        1012/s          4/s
HTTP Fixup                            0/s          0/s
```

 Please see page 474 for more details.

```
FTP Fixup                              0/s          0/s
AAA Authen                             0/s          0/s
AAA Author                             0/s          0/s
AAA Account                            0/s          0/s
VALID CONNS RATE in TCP INTERCEPT:     Current      Average
                                        N/A         95.00%

ASA1/c1# show conn
52121 in use, 52121 most used
TCP outside 17.24.101.118:26093 inside 192.168.2.100:80, idle 0:00:23, bytes 0, flags aB
TCP outside 111.76.36.109:23598 inside 192.168.2.100:80, idle 0:00:13, bytes 0, flags aB
TCP outside 24.185.110.202:32729 inside 192.168.2.100:80, idle 0:00:25, bytes 0, flags aB
TCP outside 130.203.2.204:56481 inside 192.168.2.100:80, idle 0:00:29, bytes 0, flags aB
TCP outside 39.142.106.205:18073 inside 192.168.2.100:80, idle 0:00:02, bytes 0, flags aB
TCP outside 75.27.223.63:51503 inside 192.168.2.100:80, idle 0:00:03, bytes 0, flags aB
TCP outside 121.226.213.239:18315 inside 192.168.2.100:80, idle 0:00:04, bytes 0, flags aB
TCP outside 66.187.75.192:23112 inside 192.168.2.100:80, idle 0:00:06, bytes 0, flags aB
TCP outside 13.50.2.216:3496 inside 192.168.2.100:80, idle 0:00:13, bytes 0, flags aB
TCP outside 99.92.72.60:47733 inside 192.168.2.100:80, idle 0:00:27, bytes 0, flags aB
TCP outside 30.34.246.202:20773 inside 192.168.2.100:80, idle 0:00:02, bytes 0, flags aB
TCP outside 95.108.110.131:26224 inside 192.168.2.100:80, idle 0:00:02, bytes 0, flags aB
TCP outside 76.181.105.229:21247 inside 192.168.2.100:80, idle 0:00:06, bytes 0, flags aB
TCP outside 82.210.233.230:44115 inside 192.168.2.100:80, idle 0:00:02, bytes 0, flags aB
TCP outside 134.195.170.77:28138 inside 192.168.2.100:80, idle 0:00:12, bytes 0, flags aB
TCP outside 70.133.128.41:22257 inside 192.168.2.100:80, idle 0:00:15, bytes 0, flags aB
TCP outside 124.82.133.172:27391 inside 192.168.2.100:80, idle 0:00:27, bytes 0, flags aB
TCP outside 26.147.236.181:37784 inside 192.168.2.100:80, idle 0:00:07, bytes 0, flags aB
TCP outside 98.137.7.39:20591 inside 192.168.2.100:80, idle 0:00:13, bytes 0, flags aB
TCP outside 37.27.115.122:24542 inside 192.168.2.100:80, idle 0:00:12, bytes 0, flags aB
<snip>
```

Question 8.2: Preventing unauthorized connections (3 points)

Configure R3 to prevent unauthorized connections, meeting all the following requirements:

- A new virus is propagating through your network from the Internet. Upon investigation, you find the virus traffic is entering your network via the R3 GigabitEthernet0/0 interface.
- Configure R3 to prevent the propagation of this virus by matching explicit parameters using the information in Table 2-28.
- Ensure that your solution does not impede any traffic and that all other traffic flows uninterrupted through R3.

TABLE 2-28 R3 configuration information

Virus Pattern Specification	☐ Configure policy-based packet matching using the following criteria. ☐ TCP Protocol ☐ TCP port 4444 ☐ Random source and destination IP address ☐ IP packet length 100 ☐ Redirect infected packets matching these criteria to router bit bucket blackholing the packets. ☐ Do not configure ZFW, CBAC, NBAR, MQC, or CAR to complete this task.

Question 8.3: W32.Blaster worm attack (4 points)

Configure a mitigation solution to respond to the W32.Blaster worm attack, meeting all the following requirements:

- Configure R1 to prevent the W32.Blaster worm propagation on UDP port 69 by matching explicit parameters using the information in Table 2-29.
- Ensure that your solution does not break existing TFTP functionality which also uses UDP port 69.
- Apply the solution inbound to R1 GigabitEthernet0/1 interface.
- Do not use ACLs to complete this task.
- Do not use ZFW or CBAC to complete this task.

TABLE 2-29 R1 configuration information

W32.Blaster Worm Specification	☐ Configure deep packet inspection to match a custom pattern using the following match criteria. ☐ UDP Protocol ☐ UDP port 69 ☐ IP packet length exceeding 402 bytes ☐ Pattern match 0x20a29010 at 50 bytes from start of IP header, to match on 4 bytes. ☐ Do not configure an ACL to complete this task.

Question 8.4: IP spoofing attack (3 points)

Configure Sw1 to protect against IP spoofing attacks, meeting all the following requirements:

- An intruder is sending a SYN flood spoofing trusted IP addresses of devices in VLAN 10 employing the source IP spoofing technique.
- Configure a countermeasure on Sw1 to protect against IP spoofing attacks by checking the source IP address field with the binding table. Packets not validated should be blocked.
- Additionally, configure a static binding entry in the DHCP snooping binding table for a trusted host (non-DHCP) with MAC address 0000.0000.0001 and IP address 10.10.1.1 in VLAN 10 connected to Sw1 interface FastEthernet0/18.
- A new DHCP server will be deployed in the future on Sw1 interface FastEthernet0/19. Ensure that this port is the trusted port to reply DHCP requests on the network.

Ask the Proctor

This section provides questions and answers. You can use it if you need any clarification to complete the Practice Lab questions. With the real CCIE lab, the proctor will not discuss with you the questions or solutions, except for basic clarifications. The proctor will be present only to ensure that you do not have problems with the lab environment and to maintain the timing element of the lab exam.

Section 1.0: Core Configuration (14 Points)

Question 1.1: Initializing the ASA1 firewall (5 points)

Question: Do I have to be exact in naming the interfaces, such as Inside versus inside versus INSIDE?

Answer: Yes. You have to use exact names and numbers, as mentioned in the question. Context names also are case-sensitive, so use the exact names mentioned in the tables.

Question: Can I add static routes on the ASA firewall?

Answer: Yes, you can add static and default routes as required throughout this Practice Lab unless restricted explicitly.

Question: Am I allowed to manually assign a MAC address on the shared context interfaces?

Answer: No. The question clearly requires configuring an automatic virtual unique MAC address to each shared context interface.

Question: Why is my Interface Management0/0 showing down?

Answer: The Management0/0 interface is physically not connected and will remain down; ignore it.

Question: Do I need to configure the VLANs on Catalyst Switches?

Answer: Only if required. All VLAN information has been preconfigured in the initial configuration provided. However, if there is a scenario where you feel you want to modify the VLAN information, you are allowed to do so.

Question 1.2: Configuring Active-Active Stateful Failover (5 points)

Question: Do I have to be exact in naming the failover interface to failint and the IP addresses?

Answer: Yes. You have to use exact names, numbers, and IP addresses, as mentioned in the question and in sample outputs. Use this approach throughout the exam, ensuring the use of exact names and numbers, as mentioned in the question requirements.

Question: Do I need to configure the ASA2 device hostname as ASA1 or ASA2?

Answer: After you enable the failover configuration on both devices, ASA1, which is the primary unit, will automatically synchronize all configurations to the ASA2 standby unit.

Question: My failover interfaces are not appearing in (Normal) state. Is this a hardware issue?

Answer: Check your configuration carefully; you must have forgotten some task. A common mistake is that candidates forget to unshut interface Ethernet0/3 on ASA2, which is used for failover and stateful communication. Ensure that Ethernet0/3 is unshut on both devices. Another common mistake is that candidates forget to configure the Catalyst switch configuration (such as VLANs) for interfaces connecting ASA2. Ensure that you configure the appropriate VLAN mappings on Sw2 FastEthernet0/10, 0/11, and 0/12 that connect the ASA2 interfaces E0/0, E0/1, and E0/2, respectively. If this is not done, your failover output will always show the interfaces in (Waiting) state.

Question: Do I need to configure the VLANs on Sw2 for interfaces connecting ASA2?

Answer: Yes, if required. As just mentioned, a common mistake is that candidates forget to configure the Catalyst switch configuration (such as VLANs) for interfaces connecting the secondary unit.

Question 1.3: Initializing IPS Sensor (4 points)

Question: Do I need to permit all hosts or specific hosts in VLAN 2?

Answer: Permitting all hosts in VLAN 2 means any host. Permit the /24 subnet in your sensor ACL.

Question: What are the default username and password for sensor console login?

Answer: The default username and password is usually “cisco” (without the quotation marks). However, the default password may have been reset and can be different. Generally, the password is set to “cisco” or “123cisco123” or “cisco123,” to name a few.

Section 2.0: Cisco Firewall (13 Points)

Question 2.1: Network Address Translation (NAT) (3 points)

Question: Can I enable nat-control for testing on ASA?

Answer: The requirement is very clear: do not enable nat-control in context c1. The requirement is to enable nat-control in context c2 only.

Question: What if I miss one small requirement? Will I get partial credit?

Answer: All requirements must be met to earn the points. The CCIE lab exam offers no partial credit.

Question: What NAT ID number should I use when configuring the **nat/global** statements on context c2?

Answer: The default range is 1 to 2147483647, and you can use any number. Usually candidates use the first logical number available—1 or sometimes 2, whichever is convenient.

Question: Do I need to permit return traffic on the outside interface for this task?

Answer: There is no need to configure an ACL, because traffic is traversing from a higher-security (inside) interface to a lower-security (outside) interface. However, permitting ICMP from any host to any destination for testing purposes is allowed in the question.

Question 2.2: Asymmetric routing support (3 points)

Question: What **asr-group** ID number should I use when configuring the asymmetric routing support on the outside interface?

Answer: The default range is 1 to 32, and you can use any number. Usually candidates use the first logical number available—1—or whichever is convenient.

Question: Do I need to configure asymmetric routing support to the inside interface as well?

Answer: No. The question clearly requires configuring the outside interface only.

Question: Is there an alternative solution if I do not use the **asr-group** feature?

Answer: Not that I can think of.

 Please see page 474 for more details.

Question 2.3: Time-based access control (3 points)

Question: The question requires setting a specific one-hour downtime window to August 1, 2009, 9 to 10 p.m. My system clock is showing the current date, and I can't change it from the c1 context prompt.

Answer: You need to change the system clock from the system context to set it to the specified range. The context inherits the clock from the system context. For testing, you can change the clock back and forth.

Question: Can I configure a named or numbered ACL to complete this task?

Answer: Because the question does not restrict or mention anything about the type of ACL, you can use either.

Question: Do I need to permit all hosts (all IP addresses) from R2 to R6 or specific hosts?

Answer: The question clearly requires allowing IP traffic from specific host 10.2.2.2 to 10.6.6.6 during the specified timeslot.

Question 2.4: Cisco IOS Firewall using CBAC (4 points)

Question: When configuring the CBAC solution, can I enable the CBAC inspection to the WAN link Serial0/0/0?

Answer: Yes. However, this does not meet an important requirement laid out in the question. The question clearly says to ensure that CBAC protection continues to function in in case the Frame Relay WAN link goes down when rerouting traffic via the alternate GigabitEthernet0/1 link. The question also says not to enable CBAC inspection on the GigabitEthernet0/1 link. Therefore, the only option left is the GigabitEthernet0/0 link, where you can apply the CBAC inspection. The question also states that your solution must have CBAC inspection applied to one interface only.

Question: The question says to configure java-list. Should I configure a **permit** statement to permit the trusted site, or a **deny** statement?

Answer: To allow the trusted site for Java traffic, you need to use a **permit** statement in the java-list ACL. It is a common misconception to use a **deny** statement. The implicit **deny** statement drops Java packets from any other site automatically.

Question: When configuring the filtering ACL, do I need to configure specific OSPF packets between Sw1 and R4 or any to any?

Answer: Because the question does not restrict or mention anything about this ACL, you can permit from any source to any destination. However, as a best practice, I recommend that you write a specific ACL whenever possible. Again, this is just a recommendation, not a requirement.

 Please see page 474 for more details.

Section 3.0: Cisco VPN (15 Points)

Question 3.1: Configuring Group Encrypted Transport VPN (GETVPN) (4 points)

Question: What name should I use for configuring the crypto map, transform set, profile, and so on?

Answer: Follow the question requirement and review the tables. If it's not mentioned in the question requirement, you can use any name. Candidates generally use "cisco" because it is easy to remember.

Question: Do I have to be exact when using the naming conventions?

Answer: Yes. You have to use exact names, numbers, and IP addresses, as mentioned in the question. Use this approach throughout the exam, ensuring the use of exact names and numbers, as mentioned in the question requirements. Failure to do so will result in loss of all points for the task.

Question: What protocol and port number does the GETVPN traffic use during the Group Domain of Interpretation (GDOI) registration process?

Answer: GDOI uses User Datagram Protocol (UDP) port number 848 to establish its IKE sessions between the key server and the group members.

Question: Which multicast address should I use for GDOI rekey?

Answer: The question clearly requires using Unicast rekey. Therefore, there is no need for a multicast address for the rekeying process.

Question: What label should I use when generating RSA keys, and what modulus?

Answer: Because the question does not clearly mention anything about this, you can use any label and modulus. The important thing to remember is to follow the instructions in the question. If a question does not provide a particular detail, you can safely assume any parameter.

Question: Do I need to configure a host-specific preshared key or for any host using 0.0.0.0/0?

Answer: Because the question does not clearly mention anything about this, you can use any host key 0.0.0.0/0. However, from a GDOI protocol requirement perspective, a preshared key is required on each GM to authenticate the KS only. It is not required to define a preshared key on a GM to authenticate other GMs.

Question: My group members (GM) are registering with the key server (KS). However, I can't get Question 3.2 (DMVPN) to work. Will I lose points for this task?

Answer: You will not lose points as long as devices register with the key server (KS), which satisfies the requirement of this task thus far. However, if it is the other way around, you will lose points for both questions.

Question 3.2: Configuring Dynamic Multipoint VPN (DMVPN) using GDOI (4 points)

Question: Do I need to redistribute routes into EIGRP AS 2?

Answer: No. Do not redistribute any protocol/routes into EIGRP AS 2. Only advertise the specific networks mentioned in the question.

Question: Do I need to permit DMVPN traffic for specific host-to-host or any-to-any?

Answer: Because the question does not restrict anything, you can permit UDP/500 and ESP any-to-any host in both contexts.

Question: If my group members (GM) are not registering with the key server (KS), can I skip the GDOI part and complete the DMVPN task with tunnel protection profile?

Answer: No. You will lose points, because the question clearly requires configuring this task using GETVPN integration.

Question: This question seems very long and has a lot of requirements. Can I skip some of them and still get partial credit?

Answer: No. The CCIE Lab exam offers no partial credit. If you miss any item, you lose all the points.

Question 3.3: Troubleshooting Easy VPN using DVTI (4 points)

Question: Can you clarify the nature of injected faults?

Answer: Faults can be on any device within the Easy VPN configuration or within the network topology around it. They could also be related to any of the non-VPN technologies, such as switching, routing, WAN link, IOS features, NAT, and ACL filtering, to name a few. Second, faults injected can be related to either incorrect preconfiguration or missing commands to complete the configuration.

Question: Must I find the injected faults, or can I delete all Easy VPN configurations and start fresh?

Answer: No, you cannot remove the Easy VPN preconfiguration to start fresh. The faults injected must be found within the existing preconfiguration.

Question: If I can't find all the faults, will I get partial credit for the ones I found?

Answer: You must find all the faults to earn the total points. There is no partial credit on the CCIE lab exam.

Question: Are all the faults on one device, or are they spread across multiple devices?

Answer: Faults are injected on multiple devices across the topology to create a more challenging scenario.

Question: Are all the faults related to the Easy VPN configuration only?

Answer: No. As mentioned earlier, faults can be anywhere within the Easy VPN configuration or within the network topology around it. They can also be related to any of the non-VPN technologies.

Question: Do I need to be explicit when opening an ACL on the ASA1/c1 context for Easy VPN traffic?

Answer: Because the question does not restrict or mention anything about this ACL, you can permit from any source to any destination. However, as a best practice, I recommend that you write a specific ACL, because you know the source and destination IP address in this task. Again, this is just a recommendation, not a requirement.

Question 3.4: Troubleshooting L2L IPsec VPN using VTI (3 points)

Question: Are all the faults on one device, or are they spread across multiple devices?

Answer: Faults are injected on multiple devices across the topology to create a more challenging scenario.

Question: Are all the faults related to VTI configuration only?

Answer: No. As mentioned earlier, faults can be anywhere within the VPN configuration or within the network topology around it. They can also be related to any of the non-VPN technologies.

Question: If I can't find all the faults, will I get partial credit for the ones I found?

Answer: All faults must be found to earn the total points. There is no partial credit on the CCIE lab exam.

Question: Do I need to configure a host-specific preshared key or for any host using 0.0.0.0/0?

Answer: Because the question does not clearly mention anything about this, you can use any host key 0.0.0.0/0.

Section 4.0: Cisco IPS (Intrusion Prevention System) (8 Points)

Question 4.1: Configuring IPS signatures (4 points)

Question: What is the signature ID number for ICMP echo-request and echo-reply packets?

Answer: ICMP echo-request is sig ID 2000, and echo-reply is 2004. You need to know some of the common built-in signature ID numbers on the IPS sensor appliance.

Question: Do I need to verify the functionality of the custom signature?

Answer: Yes. Functionality is important. If a signature is configured but not triggering, you will lose points. You can verify the functionality of the custom signature by sending large ICMP packets from R4 to an RFC 1918 address, as shown in the question example.

Question 4.2: Configuring Cisco IOS IPS (4 points)

Question: Do I need to download the same signature file S416 as used in this Practice Lab?

Answer: Not necessarily. You can download the latest Cisco IOS IPS signature package file from the following URL to complete this task:
http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup

 Please see page 474 for more details.

Question: There are several file types, and I am confused about which file to download to enable Cisco IOS IPS v5.0 support on the router.

Answer: Download the .pkg file with a naming convention of IOS-S*xxx*-CLI.pkg. (The IPS version 4.*x*-based SDF files will not load under the Cisco IOS IPS version 5.*x* version.)

Question: What if my router IOS version is below version 12.4(11)T? Can I still download the .pkg file to flash?

Answer: No, you cannot load the IPS version 5.0 .pkg file on IOS earlier than 12.4(11)T. The new file format is only supported from 12.4(11)T or above images. Ensure that you upgrade your IOS. Cisco IOS IPS version 5.0 format signatures are not backward-compatible with Cisco IOS IPS version 4.0 SDF format.

Question: Where can I find the Cisco public key for Cisco IOS IPS configuration?

Answer: You can download this information from the URL mentioned on the previous page.

Question: What if I fulfill the requirements for this task using Cisco IOS IPS v4.0 format signatures?

Answer: You will lose all points for this task, because the question clearly mentions using version 5.0 format signatures.

Section 5.0: Implement Identity Authentication (12 Points)

Question 5.1: Proxy authentication access control (4 points)

Question: What name or number should I use when configuring an access list for classifying authentication traffic for AAA?

Answer: Because the question does not restrict or mention anything about this, you can use any name/number convention convenient to you.

Question: Do I need to be explicit when opening the ACL on the ASA1/c1 context for Telnet sessions (TCP/23)?

Answer: Because the question does not restrict or mention anything about this ACL, you can permit from any source to any destination. However, as a best practice, I recommend that you write the best possible specific host-to-host ACL, because you know the destination IP address in this task. Permit source 10.5.5.5 (R5) to destination 10.1.1.1 (R1) on TCP port 23. Again, this is just a recommendation, not a requirement.

Question: The question states that the user must be assigned to the Default group. Can it be in any group, or must I use the built-in Default group?

Answer: The user must be in the system Default group.

Question: Can I add static routes if my Telnet traffic is not working?

Answer: Yes, you are allowed to add any number of additional static routes on any device to ensure that your session works. There is no restriction.

Question 5.2: Privilege level access control (4 points)

Question: The question says not to use the default method list. How many named method lists can be used?

Answer: It does not matter how many, as long as you fulfill the requirement. However, two named methods for authentication and two named methods for authorization should do and will fulfill all the requirements. Review the solution output provided.

Question: What name should I use when configuring the named method list?

Answer: Because the question does not restrict or mention anything about this, you can use any naming convention convenient to you.

Question: Do I need to configure an explicit named method list for console line authentication?

Answer: Yes. Because the question clearly says "Ensure that the console port is unaffected by this task," this must be fulfilled by configuring a separate named method list with **none** to exempt the console line from any form of authentication. This also protects you from locking out of the router because of any unforeseen errors during the configuration.

Question: Do I need to be explicit when opening the ACL on the ASA1/c1 context for TACACS+ communication between R5 and ACS?

Answer: Because the question does not restrict or mention anything about this ACL, you can permit from any source to any destination. However, as a best practice, I recommend that you write the best possible specific ACL, because you know the source and destination IP address in this task. Permit source 192.168.65.5 to destination 192.168.2.14 on TCP port 49 explicitly. Again, this is just a recommendation, not a requirement.

Question: When I browse the Group Setup in Cisco Secure ACS, I am unable to see the Time-of-Day Access settings option.

Answer: By default, the Time-of-Day Access settings option under the Group setup is not visible. Figure 2-8 shows how to enable it from the Interface Configuration menu on Cisco Secure ACS server. Go to Advanced Options, select the checkbox Default Time-of-Day / Day-of-Week Specification, and recheck the Group setup; it will appear now.

Question 5.3: MAC-based authentication profile (4 points)

Question: Do I need to configure NAC profiles and NAC settings?

Answer: No, you don't have to configure NAC profile postures for this task.

Question: What is the IP address of the RADIUS (IETF) server?

Answer: Because the question does not mention anything about this, you can use any dummy IP address.

Section 6.0: Implement Control and Management Plane Security (13 Points)

Question 6.1: Control plane protection (4 points)

Question: What naming convention do I use when configuring **class-map** and **policy-map**?

Answer: Because the question does not restrict or mention anything about this, you can use any naming convention convenient to you.

Question: Can I use an ACL to match all the closed ports?

Answer: No, this is practically impossible. There are hundreds of ports, and you cannot list them using an ACL. This is why a new **match closed-ports** option is given under the new port-filter type class-map.

Question: The question says to use only one class-map and policy-map. Can I use multiple **match** statements within one class-map?

Answer: Technically, you can; however, you won't need more than one **match** statement to complete this task.

Question: If I don't use a port-filter type class-map, can I complete this task with a regular class-map?

Answer: No, this is not possible. The new **match closed-ports** command is only available under a port-filter type class-map.

Question: The question does not specify in which direction I should apply the service-policy.

Answer: There is only one option. The new port-filter type policy-map can only be applied in the inbound direction to the control-plane host subinterface.

Question 6.2: Cisco IOS image and configuration protection (3 points)

Question: Can I configure a service policy to complete this task?

Answer: No. Only the Cisco IOS Resilient Configuration feature is allowed to enable the IOS image and configuration protection. The question clearly says not to use an ACL, ZFW, or CBAC to complete this task.

Question 6.3: Router CPU protection (3 points)

Question: Can I configure an ACL on VTY lines?

Answer: No. The question clearly says not to use any type of ACL to complete this task.

Question: Can I configure CoPP to complete this task?

Answer: You can if you can find a way to use CoPP without using an ACL and still block the ICMP Destination Unreachable (Type 3) messages going out of R4.

Question 6.4: Secure device access control (3 points)

Question: When configuring the solution, is it OK to apply under line vty 0 through 4 only?

Answer: No. You must apply the solution to all the lines, 0 through 15. The requirement is to disable Telnet and enable SSH on the entire switch, not just selective lines.

Question: Do I need to create RSA keys using 512 or 1024 modulus?

Answer: Because the question does not specify anything in this regard, you are allowed to choose any option.

Question: Do I need to enable AAA for this task?

Answer: No. The question does not require enabling AAA-based authentication. You can configure a local username and password for SSH authentication.

Question: Do I need to configure a VTY ACL to restrict topology users only?

Answer: No. The question does not require enabling a VTY ACL. However, if you choose to configure it, it should be OK.

Section 7.0: Advanced Security (12 Points)

Question 7.1: MAC flooding protection (3 points)

Question: How do I know if Port Security is the only solution to this question?

Answer: Several hints in this question lead you to enable Port Security. For example, the question says to set the maximum dynamically learned MAC addresses and violation mode.

Question: Can I enable sticky learning?

Answer: Yes, sticky learning is required as part of the solution, because the question clearly requires storing the dynamically learned MAC addresses into the configuration.

 Please see page 474 for more details.

Question: The question requires configuring Port Security on Sw2 Fa0/20. However, my switch shows that the interface is down/down.

Answer: The interface is down/down because nothing is connected yet. A secure host will be connected to this port in the future.

Question 7.2: Troubleshooting NBAR (3 points)

Question: If I can't find all the faults, will I get partial credit for the ones I found?

Answer: All faults must be found to earn the total points. There is no partial credit on the CCIE lab exam.

Question: Are all the faults on one device, or are they spread across multiple devices?

Answer: Faults are injected on multiple devices across the topology to create a more challenging scenario.

Question: Are all the faults related to NBAR configuration only?

Answer: Not necessarily. As mentioned earlier, faults can be anywhere within the NBAR or MQC configurations or within the network topology around them.

Question: Can I create a new ACL for matching Telnet traffic?

Answer: No. The question clearly says not to use an ACL on any device to complete this task.

Question: Can I change the preconfigured service-policy to apply on the control-plane interface on R2?

Answer: No. The question clearly says not to use CoPP to complete this task.

Question 7.3: Configuring ESMTP Server protection (3 points)

Question: What naming convention should I use when configuring the **policy-map** and **regex** names?

Answer: Because the question does not restrict or mention anything about this, you can use any naming convention convenient to you.

Question: How do I know if Modular Policy Framework (MPF) is the only solution to this question?

Answer: Because the question clearly states that the solution is configured on the Cisco ASA firewall, there is no other option than using the MPF. It provides a wide range of inspection parameters for all application layer protocols.

Question: Can I apply the policy to the global policy?

Answer: Yes. The question requires protecting the ESMTP server from traffic entering the firewall in any direction; therefore, the best option is protecting using a global policy. The question also clearly says not to apply the policy to the inside or outside interface explicitly.

Question: How can I validate the functionality of this question?

Answer: This question is configuration-based only; there is no live traffic that you can use to validate the functionality. You have to rely on your configuration only.

Question 7.4: IKE resource exhaustion protection (3 points)

Question: How do I determine in which direction to apply the CAR?

Answer: The question clearly says to rate-limit inbound UDP/500 traffic from any source to destination R1 Loopback0. This leads you to applying the CAR on R1 GigabitEthernet0/0 in the inbound direction.

Question: Can I use an ACL to match the traffic in the rate-limit solution?

Answer: Yes. The question clearly says to match explicit UDP/500 (IKE) traffic from any source to destination R1 Loopback0.

Question: Do you want me to configure a named or numbered ACL to complete this task?

Answer: CAR supports only numbered ACLs. Because the question does not specify the ACL number, you can use any number convention convenient to you.

 Please see page 474 for more details.

Section 8.0: Network Attacks (13 Points)

Question 8.1: Web server attack (3 points)

Question: Can I use any technique other than MPF to complete this task?

Answer: Yes. However, the question says not to use a network address translation (**static**) command where you could set the embryonic (half-open) connections limit. The only other option left on the firewall is to use the MPF feature on the ASA1/c1 context.

Question: Can I configure multiple **class-map**s and/or **policy-map**s to complete this task?

Answer: Yes. Because the question does not restrict this, you can configure any number of these as long as you fulfill the criteria.

Question: What naming convention should I use for the **class-map** and **policy-map** configuration?

Answer: Because the question does not restrict or mention anything about this, you can use any naming convention convenient to you.

Question: Is the ACL allowed to match within the **class-map**?

Answer: The question clearly says not to use an ACL in any fashion to complete this task. You need to use the **match port** command in the **class-map** to classify the HTTP (TCP/80) traffic.

Question: What number should I use to set the maximum number of embryonic (half-open) connections?

Answer: Because the question does not mention anything about this, you can set the embryonic (half-open) connections limit to any number. 100 is used in this example.

Question 8.2: Preventing unauthorized connections (3 points)

Question: Is the ACL allowed to match in the class-map and be used in the service-policy?

Answer: Yes. You can use the ACL to match virus traffic on TCP port 4444 from any source to any destination.

Question: What naming convention should I use when configuring the **route-map** and ACL configuration?

Answer: Because the question does not restrict or mention anything about this, you can use any naming convention convenient to you.

Question: Do I need to apply the policy to global mode?

Answer: No. The question clearly says to apply the solution to the R3 GigabitEthernet0/0 interface.

Question 8.3: W32.Blaster worm attack (4 points)

Question: Can I use an an ACL to match the traffic in the class-map within the Flexible Packet Matching (FPM) solution?

Answer: The question clearly says not to use an ACL in any fashion to complete this task.

Question: What naming convention should I use for the **class-map** and **policy-map** configuration?

Answer: Because the question does not restrict or mention anything about this, you can use any naming convention convenient to you.

Question: When trying to configure the stack type and access-control type **class-map**, I am unable to see the FPM options. Am I missing something?

Answer: Before you can configure FPM, you need to load the Protocol Header Definition File (PHDF) files into the router flash and enable it from global configuration mode. FPM provides ready-made definitions for these standard protocols (IP, TCP, UDP, ICMP), which can be loaded onto the router with the **load protocol** command: ip.phdf, tcp.phdf, udp.phdf, and icmp.phdf. Ensure that the files are in the flash, and then enable them as shown here:

```
R1# config term
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# load protocol flash:ip.phdf
R1(config)# load protocol flash:udp.phdf
```

Question 8.4: IP spoofing attack (3 points)

Question: Do I need to configure DHCP Snooping on the switch to complete this task?

Answer: Yes, DHCP Snooping must be enabled. It is a prerequisite for IP Source Guard (IPSG) functionality to work. IPSG depends on the snooping binding table, which is built and populated dynamically when DHCP snooping is enabled. You can also populate static entries into this table as required in this question.

Question: The question requires configuring IPSG and a DHCP trusted port on Sw1 Fa0/18 and Fa0/19. However, my switch shows that both interfaces are down/down.

Answer: The interfaces are down/down because nothing is connected yet. A DHCP server and trusted host will be connected to these ports in the future.

Lab Debrief

As mentioned in the Overview, this section is primarily important when you're verifying the outcome and functionality of the Practice Lab questions. You can use this section primarily to understand how to verify and compare your work. This section also provides some useful hints needed to complete the respective exercises. Sometimes it is easy to misinterpret question requirements that have integral and complex elements.

This section shows outputs using the most common **show** and **debug** command(s) used for verification and troubleshooting. Analyze and study these outputs carefully.

The following outputs also have some important parts highlighted that require your attention. Focus on those highlights, and match your outputs to ensure absolute accuracy.

This section analyzes each question, showing you what was required and how to achieve the desired results. Each question also highlights the skills tested in each question. You should use this section to produce an overall score for your test.

Section 1.0: Core Configuration (14 Points)

Question 1.1: Initializing the ASA1 firewall (5 points)

Initialize the ASA1 firewall, meeting all the following requirements:

- Configure the ASA1 firewall in multicontext routed mode as shown in Figure 2-3.
- Configure hostname "ASA1" and enable password "cisco."
- Create three contexts as shown in the tables.
- Context names are case-sensitive. Use exact names and numbers as shown in the tables.
- Assign context "admin" as the admin-context.
- Assign interfaces as shown in the tables. Do not map physical interface names to logical names.

- Both contexts must use shared outside interface Ethernet0/0.
- Enable automatic assignment of unique MAC addresses to each shared context interface. Do not use manual MAC addresses for this task.
- Configure IP addresses and all other initialization parameters as shown in the tables.
- Configure static and default routes within context as shown in the tables. You can also refer to Figure 2-4 and Table 2-3 for more information.
- To perform basic verification using ping tests throughout this Practice Lab, you are allowed to permit **icmp any any** in your ACL in both contexts on ASA1.
- Ensure that you can ping all the interfaces, including Loopback0 on Sw1 and Sw2 from context c1.

Skills tested

- ☐ Initializing the Cisco ASA1 firewall in multicontext mode
- ☐ Understanding packet classification in multicontext mode
- ☐ Configuring shared interfaces between contexts and assigning a unique MAC address to a shared interface
- ☐ Configuring basic IP address and IP routing initialization tasks

Functionality and solution verification

- ☐ This question is one of the core configuration tasks, so you need to be very careful when attempting it. If you get any item wrong in this question, it can potentially impede the functionality required to complete the later questions.
- ☐ It is strongly recommended that you practice the ASA multicontext configuration often during your study sessions to ensure perfection and accuracy in this area.
- ☐ Also ensure that you understand how the packet classification function works in multicontext mode.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.

- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatcheded item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

Check that the hostname is ASA1:

```
ASA1# show run hostname
hostname ASA1
```

Check if ASA1 is configured in multicontext mode:

```
ASA1# show mode
Security context mode: multiple
```

Check if ASA1 is configured in routed mode:

```
ASA1# show firewall
Firewall mode: Router
```

Check the context details and interface allocations for each context on ASA1. Also check that the context name is case-sensitive, as per the requirement:

```
ASA1# show context
Context Name      Class      Interfaces                      URL
*admin            default    Management0/0        disk0:/admin
 c1               default    Ethernet0/0,Ethernet0/1 disk0:/c1
 c2               default    Ethernet0/0,Ethernet0/2 disk0:/c2

Total active Security Contexts: 3
```

Check the context parameters and interface allocations. Ensure that Ethernet0/0 is allocated to both contexts (shared interface):

```
ASA1# show running-config context
!
admin-context admin
context admin
  allocate-interface Management0/0
  config-url disk0:/admin
!
context c1
  allocate-interface Ethernet0/0
  allocate-interface Ethernet0/1
  config-url disk0:/c1
  join-failover-group 1
!
context c2
  allocate-interface Ethernet0/0
  allocate-interface Ethernet0/2
  config-url disk0:/c2
  join-failover-group 2
!
ASA1#
```

Check for admin context assigned as admin-context:

```
ASA1# show admin-context
Admin: admin disk0:/admin
```

Check for MAC address auto-assignment:

```
ASA1# show run mac-address
mac-address auto
```

 Please see page 474 for more details.

Change the context to c1:

```
ASA1# changeto context c1
```

Check that the interface is UP on the ASA1/c1 context. Note that masking physical interface names to logical names is not allowed.

You will also note that due to the auto-mac-address command just enabled, physical interfaces will now have a unique "virtual" MAC address for each interface:

```
ASA1/c1# show interface
Interface Ethernet0/0 "outside", is up, line protocol is up
        MAC address 1200.0000.0200, MTU 1500
        IP address 192.168.6.10, subnet mask 255.255.255.0
  Traffic Statistics for "outside":
        51011 packets input, 5500988 bytes
        50949 packets output, 5498108 bytes
        2 packets dropped
Interface Ethernet0/1 "inside", is up, line protocol is up
        MAC address 1200.0100.0200, MTU 1500
        IP address 192.168.4.10, subnet mask 255.255.255.0
  Traffic Statistics for "inside":
        50938 packets input, 5497504 bytes
        50926 packets output, 5496496 bytes
        0 packets dropped
```

Check the nameif and security levels assigned to each interface on the ASA1/c1 context. Also check that the nameif is case-sensitive, as per the requirement:

```
ASA1/c1# show nameif
Interface                 Name                      Security
Ethernet0/1               inside                    100
Ethernet0/0               outside                     0
```

 Please see page 474 for more details.

Check the IP address/mask assigned to each interface on the ASA1/c1 context:

```
ASA1/c1# show ip
System IP Addresses:
Interface                Name                IP address      Subnet mask     Method
Ethernet0/0              outside             192.168.6.10    255.255.255.0   manual
Ethernet0/1              inside              192.168.4.10    255.255.255.0   manual
Current IP Addresses:
Interface                Name                IP address      Subnet mask     Method
Ethernet0/0              outside             192.168.6.10    255.255.255.0   manual
Ethernet0/1              inside              192.168.4.10    255.255.255.0   manual
```

Check the static and default routes as per the table on the ASA1/c1 context:

```
ASA1/c1# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.6.6 to network 0.0.0.0

C    192.168.4.0 255.255.255.0 is directly connected, inside
S    10.2.2.0 255.255.255.0 [1/0] via 192.168.4.2, inside
S    10.1.1.0 255.255.255.0 [1/0] via 192.168.4.2, inside
C    192.168.6.0 255.255.255.0 is directly connected, outside
S    192.168.2.0 255.255.255.0 [1/0] via 192.168.4.2, inside
S    192.168.3.0 255.255.255.0 [1/0] via 192.168.4.2, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 192.168.6.6, outside
```

 Please see page 474 for more details.

Ensure that you can ping all interfaces, including Loopbacks of Sw1 from the ASA1/c1 context. Your success rate percentage should be greater than 0 for all the ping outputs. The question clearly states that you are allowed to permit **icmp any any** in your ACL in both contexts.

```
ASA1/c1# ping 192.168.6.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.6.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA1/c1# ping 192.168.64.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.64.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA1/c1# ping 192.168.65.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.65.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA1/c1# ping 192.168.41.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.41.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA1/c1# ping 192.168.52.2
Type escape sequence to abort.
```

 Please see page 474 for more details.

```
Sending 5, 100-byte ICMP Echos to 192.168.52.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA1/c1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA1/c1# ping 10.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA1/c1# ping 10.3.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA1/c1# ping 10.4.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA1/c1# ping 10.5.5.5
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.5.5.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA1/c1# ping 10.6.6.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.6.6.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA1/c1# ping 10.7.7.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.7.7.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA1/c1# ping 10.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Now, change the context to c2:

```
ASA1# changeto context c2
```

Check that the interface is UP in the c2 context. Note that context c2 should be Active on the failover Standby unit (ASA2). You have to check the following output from ASA2. Verify that the IP addresses on ASA2 are the current addresses, and not standby IP addresses.

You will also note that due to the auto-mac-address command enabled earlier, the physical interfaces now have a unique "virtual" MAC address for each interface:

```
ASA1/c2# show interface
Interface Ethernet0/0 "outside", is up, line protocol is up
        MAC address 1200.0000.0300, MTU 1500
        IP address 192.168.6.11, subnet mask 255.255.255.0
  Traffic Statistics for "outside":
        50950 packets input, 5497332 bytes
        50901 packets output, 5494956 bytes
        0 packets dropped
Interface Ethernet0/2 "inside", is up, line protocol is up
        MAC address 1200.0200.0300, MTU 1500
        IP address 192.168.5.10, subnet mask 255.255.255.0
  Traffic Statistics for "inside":
        50934 packets input, 5498258 bytes
        50909 packets output, 5495828 bytes
        16 packets dropped
```

Check the nameif and security levels assigned to each interface on the c2 context. Also check that the nameif is case-sensitive, as per the requirement:

```
ASA1/c2# show nameif
Interface               Name                    Security
Ethernet0/0             outside                   0
Ethernet0/1             inside                  100
```

Check the IP address/mask assigned to each interface:

```
ASA1/c2# show ip
System IP Addresses:
Interface               Name                IP address      Subnet mask     Method
```

 Please see page 474 for more details.

```
Ethernet0/0             outside             192.168.6.11    255.255.255.0   CONFIG
Ethernet0/2             inside              192.168.5.10    255.255.255.0   CONFIG
Current IP Addresses:
Interface               Name                IP address      Subnet mask     Method
Ethernet0/0             outside             192.168.6.11    255.255.255.0   CONFIG
Ethernet0/2             inside              192.168.5.10    255.255.255.0   CONFIG
```

Check the static and default routes as per the table on the ASA1/c2 context:

```
ASA1/c2# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.6.6 to network 0.0.0.0

C    192.168.5.0 255.255.255.0 is directly connected, inside
S    10.1.1.0 255.255.255.0 [1/0] via 192.168.5.3, inside
S    10.3.3.0 255.255.255.0 [1/0] via 192.168.5.3, inside
C    192.168.6.0 255.255.255.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 192.168.6.6, outside
```

Ensure that you can ping all interfaces, including Loopbacks from context c2. Your success rate percentage should be greater than 0 for all the ping outputs.

```
ASA1/c2# ping 192.168.6.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.6.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA1/c2# ping 192.168.64.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.64.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA1/c2# ping 192.168.64.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.64.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA1/c2# ping 10.6.6.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.6.6.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA1/c2# ping 10.4.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

```
ASA1/c2# ping 10.5.5.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.5.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA1/c2# ping 10.3.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Now, change the context to admin:

```
ASA1# changeto context admin
```

Because the Management0/0 interface is physically not connected and will remain down, you are allowed to shut down manually:

```
ASA1/admin# show interface
Interface Management0/0 "mgmt", is administratively down, line protocol is down
        MAC address 1200.0000.0100, MTU 1500
        IP address unassigned
  Traffic Statistics for "mgmt":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
        Management-only interface. Blocked 0 through-the-device packets
```

 Please see page 474 for more details.

Check the nameif and security levels assigned on the ASA1/admin context:

```
ASA1/admin# show nameif
Interface                  Name                       Security
Management0/0              mgmt                       100
```

Question 1.2: Configuring Active-Active Stateful Failover (5 points)

Configure the ASA1 and ASA2 firewalls with Active-Active Stateful Failover, meeting all the following requirements:

- Initialize the ASA2 firewall in multicontext routed mode.
- Configure LAN-based failover on both firewalls with ASA1 as the primary device and ASA2 as the secondary device.
- Configure failover parameters and IP addresses as shown in Tables 2-30 and 2-31 and the failover output below.
- Secure the failover communication sent over the failover and Stateful Failover links between the units with a failover key "cisco."
- For verification, ensure that your output matches the failover output shown below.

TABLE 2-30 Failover initialization details

Interface	Nameif	Primary IP Address/Mask	Standby IP Address/Mask
Ethernet0/3	failint	192.168.50.10/24	192.168.50.11/24

TABLE 2-31 Failover Active-Active details

Context	Failover Group Policy
c1	Group 1 ASA1 Primary and ASA2 Secondary
c2	Group 2 ASA2 Primary and ASA1 Secondary

Skills tested

- ☐ Configuring high availability using Active-Active Stateful Failover using the shared interface context

Functionality and solution verification

- ☐ This question requires configuring high availability (HA) using an Active-Active Stateful Failover setup.
- ☐ Before you start configuring the failover parameters, ensure that you initialize the ASA2 firewall in multicontext routed mode.
- ☐ A common mistake is that candidates forget to unshut interface Ethernet0/3 on ASA2, which is used for failover and Stateful communication. Ensure that Ethernet0/3 is unshut on both devices.
- ☐ Another common and costly mistake is that candidates forget to configure the Catalyst switch configuration (such as VLANs) for interfaces connecting ASA2. Ensure that you configure the appropriate VLAN mappings on Sw2 FastEthernet0/10, 0/11, and 0/12 that connect the ASA2 interfaces E0/0, E0/1, and E0/2, respectively. If this is not done, your failover output will always show the interfaces in (Waiting) state.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the the solution configurations provided for all the devices.

Ensure that context c1 is in failover group 1 and that context c2 is in failover group 2:

```
ASA1# show run context
<snip>
context c1
  allocate-interface Ethernet0/0
  allocate-interface Ethernet0/1
  config-url disk0:/c1
```

 Please see page 474 for more details.

```
  join-failover-group 1
!
context c2
  allocate-interface Ethernet0/0
  allocate-interface Ethernet0/2
  config-url disk0:/c2
  join-failover-group 2
!
ASA1#
```

Ensure that your failover output matches Listing 2-3 on both ASA1 and ASA2. In particular, check that failover group 1 is active on the Primary unit and that group 2 is active on the Secondary unit.

LISTING 2-3 Failover verification output from ASA1

```
ASA1# show failover
Failover On
Failover unit Primary
Failover LAN Interface: failint Ethernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 5 of 250 maximum
Version: Ours 8.0(4), Mate 8.0(4)
Group 1 last failover at: 03:54:49 UTC Aug 5 2009
Group 2 last failover at: 03:54:48 UTC Aug 5 2009

  This host:    Primary
  Group 1       State:          Active
                Active time:    248146 (sec)
  Group 2       State:          Standby Ready
```

```
                Active time:    0 (sec)

                slot 0: ASA5510 hw/sw rev (2.0/8.0(4)) status (Up Sys)
                  admin Interface mgmt (0.0.0.0): No Link (Waiting)
                  c1 Interface outside (192.168.6.10): Normal
                  c1 Interface inside (192.168.4.10): Normal
                  c2 Interface outside (192.168.6.15): Normal
                  c2 Interface inside (192.168.5.15): Normal
                slot 1: empty

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Active
                Active time:    248138 (sec)

                slot 0: ASA5510 hw/sw rev (1.0/8.0(4)) status (Up Sys)
                  admin Interface mgmt (0.0.0.0): No Link (Waiting)
                  c1 Interface outside (192.168.6.15): Normal
                  c1 Interface inside (192.168.4.15): Normal
                  c2 Interface outside (192.168.6.11): Normal
                  c2 Interface inside (192.168.5.10): Normal
                slot 1: empty

Stateful Failover Logical Update Statistics
        Link : failint Ethernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         33196      0          33159      0
        sys cmd         33122      0          33122      0
        up time         0          0          0          0
```

 Please see page 474 for more details.

```
        RPC services    0           0           0           0
        TCP conn        0           0           0           0
        UDP conn        36          0           0           0
        ARP tbl         38          0           37          0
        Xlate_Timeout   0           0           0           0
        SIP Session     0           0           0           0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       33159
        Xmit Q:         0       1       33196
ASA1#
```

Note that context c2 should be Active on the Secondary unit (ASA2). Verify that the IP addresses are current on ASA2, and not the standby addresses (192.168.*X*.15) (see Listing 2-4).

LISTING 2-4 Failover verification output from ASA2

```
ASA1# show failover
Failover On
Failover unit Secondary
Failover LAN Interface: failint Ethernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 5 of 250 maximum
Version: Ours 8.0(4), Mate 8.0(4)
Group 1 last failover at: 03:55:31 UTC Aug 5 2009
Group 2 last failover at: 03:55:31 UTC Aug 5 2009
```

```
This host:    Secondary
Group 1       State:          Standby Ready
              Active time:    0 (sec)
Group 2       State:          Active
              Active time:    248264 (sec)

              slot 0: ASA5510 hw/sw rev (1.0/8.0(4)) status (Up Sys)
                admin Interface mgmt (0.0.0.0): No Link (Waiting)
                c1 Interface outside (192.168.6.15): Normal
                c1 Interface inside (192.168.4.15): Normal
                c2 Interface outside (192.168.6.11): Normal
                c2 Interface inside (192.168.5.10): Normal
              slot 1: empty

Other host:   Primary
Group 1       State:          Active
              Active time:    248272 (sec)
Group 2       State:          Standby Ready
              Active time:    0 (sec)

              slot 0: ASA5510 hw/sw rev (2.0/8.0(4)) status (Up Sys)
                admin Interface mgmt (0.0.0.0): No Link (Waiting)
                c1 Interface outside (192.168.6.10): Normal
                c1 Interface inside (192.168.4.10): Normal
                c2 Interface outside (192.168.6.15): Normal
                c2 Interface inside (192.168.5.15): Normal
              slot 1: empty

Stateful Failover Logical Update Statistics
       Link : failint Ethernet0/3 (up)
```

```
        Stateful Obj    xmit       xerr       rcv        rerr
        General         33176      0          33213      0
        sys cmd         33139      0          33139      0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          36         0
        ARP tbl         37         0          38         0
        Xlate_Timeout   0          0          0          0
        SIP Session     0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       33213
        Xmit Q:         0       1       33176
ASA1#
```

Question 1.3: Initializing IPS Sensor (4 points)

Initialize Cisco IPS Sensor, meeting all the following requirements:

- Configure IPS sensor appliance between R4 and R5 as shown in Figure 2-3.
- Configure hostname "IPS" and allow Telnet sessions to IPS sensor from VLAN 2.
- Configure the Command and Control (Management0/0) interface IP address 192.168.2.12/24 with default gateway 192.168.2.11.
- Configure Catalyst switches as appropriate to complete this question.
- Configure IPS sensor for inline interface pairing using information in Table 2-32. Refer to Figure 2-3 for more information.

- You can also refer to Figure 2-1 for physical port connections.
- Verify that the virtual sensor is passing traffic in inline mode. Ensure that you can ping all interfaces, including Loopback0 of R5 and Sw2 from R4.

TABLE 2-32 Inline interface pairing information

Sensor Placement Policy	Name	Physical Interfaces	Virtual Sensor	Signature Policy
Inline Physical Pair between R4 and R5 GigabitEthernet	mypair	Interface1=GigabitEthernet0/0 Interface2=GigabitEthernet0/1	vs0	sig0

Skills tested

- ☐ Configuring basic initialization for the Cisco IPS sensor appliance
- ☐ Configuring inline interface pairing
- ☐ Securing access control using an ACL

Functionality and solution verification

- ☐ Again, this question is one of the core configuration tasks. If you get any item wrong in this question, it can potentially impede the functionality required for later questions.
- ☐ It is strongly recommended that you practice the IPS sensor using inline mode configuration often during your study sessions to ensure perfection and accuracy in this area. There are several types of inline configuration, such as inline VLAN pair, inline interface pair, and inline VLAN group. Practice all the varying combinations.
- ☐ You are also required to configure the Catalyst switches (VLAN mappings) to complete this question. Refer to Figure 2-1 for physical port connections.
- ☐ This question can be divided into two subsections. The first is the basic initial configuration of the sensor that involves basic IP addressing, Telnet, and an ACL. The second is the inline interface pairing, which is a critical piece in this task.

- After the sensor is configured, you need to verify that the virtual sensor using inline interface pairing is passing traffic. Ensure that you can ping all interfaces, including Loopback0 of R5 and Sw2 from R4. The success of these pings provides evidence that inline interface pairing is configured correctly and functioning as required.
- You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

Check the IPS basic initial parameters first:

```
IPS(config)# service host
IPS(config-hos)# show settings
   network-settings
   ------------------------------------------------
      host-ip: 192.168.2.12/24,192.168.2.11 default: 192.168.1.2/24,192.168.1.1
      host-name: IPS default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      ------------------------------------------------
         network-address: 192.168.2.0/24
         ------------------------------------------------
      ------------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text:  <defaulted>
   ------------------------------------------------
   time-zone-settings
   ------------------------------------------------
<snip>
```

Check that the IPS management interface is UP:

```
IPS# show interfaces Management0/0
MAC statistics from interface Management0/0
   Interface function = Command-control interface
   Description =
   Media Type = TX
   Default Vlan = 0
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 443126
   Total Bytes Received = 46989094
   Total Multicast Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 415537
   Total Bytes Transmitted = 252395330
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
```

Verify if the hosts in VLAN 2 can ping and telnet the IPS sensor:

```
R1# ping 192.168.2.12 source GigabitEthernet 0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.12, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.11
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R1# telnet 192.168.2.12 /source-interface GigabitEthernet 0/1
```

 Please see page 474 for more details.

```
Trying 192.168.2.12 ... Open
login: cisco
Password: 123cisco123
Last login: Sat Aug  8 10:16:13 on pts/0
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the IPS-4240.
The system will continue to operate with the currently installed
signature set.  A valid license must be obtained in order to apply
signature updates.  Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
IPS# exit
[Connection to 192.168.2.12 closed by foreign host]
R1#
```

If this is successful, verify if IPS is accepting connections only from hosts in VLAN 2. For example, a ping from a non-VLAN 2 interface on R1 should fail, because the IPS drops the pings due to the sensor ACL.

```
R1# ping 192.168.2.12 source GigabitEthernet 0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.12, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.11
.....
Success rate is 0 percent (0/5)
```

Similarly, when you try to establish a Telnet session from a non-VLAN 2 interface on R1, it should fail:

```
R1# telnet 192.168.2.12 /source-interface GigabitEthernet 0/0
Trying 192.168.2.12 ...
% Connection timed out; remote host not responding
```

Now let's move on to verifying the second part of the question, which requires configuring inline interface pairing.

Check the settings under the interface service to ensure that GigabitEthernet0/0 and GigabitEthernet0/1 are enabled and that the inline interface pair is configured as per the requirement:

```
IPS(config)# service interface
IPS(config-int)# show settings
   physical-interfaces (min: 0, max: 999999999, current: 5)
   ----------------------------------------------
      <protected entry>
      name: GigabitEthernet0/0
      ----------------------------------------------
         media-type: tx <protected>
         description:  <defaulted>
         admin-state: enabled default: disabled
         duplex: auto <defaulted>
```

```
   speed: auto <defaulted>
   default-vlan: 0 <defaulted>
   alt-tcp-reset-interface
   ---------------------------------------------
      none
      ---------------------------------------------
      ---------------------------------------------
   ---------------------------------------------
   subinterface-type
   ---------------------------------------------
      none
      ---------------------------------------------
      ---------------------------------------------
   ---------------------------------------------
-------------------------------------------
<protected entry>
name: GigabitEthernet0/1
-------------------------------------------
   media-type: tx <protected>
   description:  <defaulted>
   admin-state: enabled default: disabled
   duplex: auto <defaulted>
   speed: auto <defaulted>
   default-vlan: 0 <defaulted>
   alt-tcp-reset-interface
   ---------------------------------------------
      none
      ---------------------------------------------
      ---------------------------------------------
   ---------------------------------------------
```

 Please see page 474 for more details.

```
            subinterface-type
            ------------------------------------------------
               none
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
<snip>
   inline-interfaces (min: 0, max: 999999999, current: 1)
   ------------------------------------------------
      name: mypair
      ------------------------------------------------
         description:  <defaulted>
         interface1: GigabitEthernet0/0
         interface2: GigabitEthernet0/1
         subinterface-type
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   bypass-mode: auto <defaulted>
   interface-notifications
   ------------------------------------------------
      missed-percentage-threshold: 0 percent <defaulted>
      notification-interval: 30 seconds <defaulted>
      idle-interface-delay: 30 seconds <defaulted>
   ------------------------------------------------
   cdp-mode: drop-cdp-packets <defaulted>
```

Now check the settings under analysis-engine, and ensure that virtual sensor vs0 has the logical interface "mypair" and sig0 signature definition assigned to vs0:

```
IPS(config)# service analysis-engine
IPS(config-ana)# show settings
   global-parameters
   -----------------------------------------------
      ip-logging
      -----------------------------------------------
         max-open-iplog-files: 20 <defaulted>
      -----------------------------------------------
   -----------------------------------------------
   virtual-sensor (min: 1, max: 255, current: 1)
   -----------------------------------------------
      <protected entry>
      name: vs0
      -----------------------------------------------
         description: default virtual sensor <defaulted>
         signature-definition: sig0 <protected>
         event-action-rules: rules0 <protected>
         anomaly-detection
         -----------------------------------------------
            anomaly-detection-name: ad0 <protected>
            operational-mode: detect <defaulted>
         -----------------------------------------------
         physical-interface (min: 0, max: 999999999, current: 0)
         -----------------------------------------------
         -----------------------------------------------
         logical-interface (min: 0, max: 999999999, current: 1)
         -----------------------------------------------
```

 Please see page 474 for more details.

```
            name: mypair
            subinterface-number: 0 <defaulted>
            ------------------------------------------
          ------------------------------------------
          inline-TCP-session-tracking-mode: virtual-sensor <defaulted>
          inline-TCP-evasion-protection-mode: strict <defaulted>
        ------------------------------------------
      ------------------------------------------
```

When the inline interface pairing configuration looks OK, you need to see whether the virtual sensor is passing traffic and verify the functionality using ping tests.

The question clearly states that R4 should be able to ping all interfaces, including the loopbacks of R5 and Sw2. The success of these pings provides evidence that inline interface pairing is configured correctly and passing traffic as required.

As a side note, another test you could perform to verify that the virtual sensor is passing traffic correctly is changing the VLAN assignments of sensing interfaces and putting them in a dummy VLAN. This should break the traffic flow, and pings would fail:

```
R4# ping 192.168.45.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.45.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R4# ping 192.168.52.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.52.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
R4# ping 10.5.5.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.5.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R4# ping 10.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Section 2.0: Cisco Firewall (13 Points)

Question 2.1: Network Address Translation (NAT) (3 points)

Configure Network Address Translation (NAT) on ASA, meeting all the following requirements:

- Enable NAT control on context c2. Do not enable NAT control on context c1.
- Configure static address translation on context c1 such that when R1 establishes a Telnet session to R4 Loopback0 using its source Loopback0, the source address gets translated to 192.168.6.61. However, when R1 establishes the same Telnet session to R4 Loopback0 without using its source Loopback0 (using any other source), the source address should not get translated and should retain the original IP address.
- Configure dynamic address translation on context c2 for any hosts on the inside to get translated using dynamic pool of 192.168.6.150 through 192.168.6.155. Configure a backup pool with a PAT address using the outside interface in the event the primary pool runs out. Do not use IP addresses in the PAT pool.

Skills tested

- ☐ Understanding NAT control on the Cisco ASA Firewall and how it works
- ☐ Configuring Network Address Translation (NAT) on the Cisco ASA Firewall
- ☐ Configuring Static Policy NAT using an ACL
- ☐ Configuring Dynamic NAT/PAT using NAT/global policy

Functionality and solution verification

- ☐ This question is divided into two parts, requiring you to configure Static Policy NAT and Dynamic NAT/PAT using NAT/global policy. You must meet both requirements to earn the points. The CCIE lab exam offers no partial credit.
- ☐ The question clearly says not to enable NAT control on context c1, only on context c2.
- ☐ The first task in this question requires configuring Static Policy NAT on the ASA1/c1 context. Policy NAT is similar to static NAT. However, it allows for defining conditional criteria to check the pairing of source address and destination address (or ports). With this feature, source address translation can vary, subject to a different destination. In summary, regular NAT uses source IP addresses/ports only, whereas policy NAT uses both source and destination IP addresses/ports to identify real addresses for translation. The question requires using static commands using an ACL to complete this task. The most important part of this question is the verification and functionality testing by establishing Telnet sessions from R1 to R4, as shown in the output. Sample **show** outputs illustrate the Static Policy NAT feature.
- ☐ The second task in this question requires configuring Dynamic NAT on the ASA1/c2 context. The question clearly says to enable NAT control on context c2. The NAT engine on the firewall will perform address translation for all internal hosts, and the source address must be translated using a dynamic pool, as mentioned. In addition, a backup PAT pool is required using the "interface" keyword. Outside users cannot initiate an inbound connection to these internal hosts due to dynamic NAT. Again, you can perform verification and functionality testing for this task by establishing Telnet sessions from R3 to R6, as shown in the following sample **show** outputs that illustrate Dynamic NAT.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.

- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

The following steps illustrate verification for the first task in this question, requiring Static Policy NAT configuration on the ASA1/c1 context.

Verify if NAT control is disabled on the ASA1/c1 context. Then, verify that Static Policy NAT using an ACL is configured correctly:

```
ASA1# changeto context c1
ASA1/c1# show run nat-control
no nat-control

ASA1/c1# show run static
static (inside,outside) 192.168.6.61  access-list policyNAT

ASA1/c1# show run access-list policyNAT
access-list policyNAT extended permit ip host 10.1.1.1 host 10.4.4.4
```

When this configuration is OK, you can perform verification steps to check its functionality by establishing Telnet sessions from source R1 Loopback0 to destination R4 Loopback0. You can issue the **who** command to validate that the source address is translated to 192.168.6.61:

```
R1# telnet 10.4.4.4 /source-interface loopback 0
Trying 10.4.4.4 ... Open
User Access Verification
Password: cisco
R4> who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 20:05:11
```

 Please see page 474 for more details.

```
*578 vty 0                idle                 00:00:00 192.168.6.61
  Interface    User               Mode         Idle     Peer Address
R4> exit
[Connection to 10.4.4.4 closed by foreign host]
R4#
```

Now, establish a Telnet session from R1 to destination R4 Loopback0 (without using source). You can issue the **who** command to validate that the source address is untranslated and remains the same, 192.168.3.11 (the original source IP address):

```
R1# telnet 10.4.4.4
Trying 10.4.4.4 ... Open
User Access Verification
Password: cisco
R4> who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 20:05:18
*578 vty 0                 idle                 00:00:00 192.168.3.11
  Interface    User               Mode         Idle     Peer Address
R4> exit
[Connection to 10.4.4.4 closed by foreign host]
R1#
```

The following steps illustrate verification for the second task in this question, requiring Dynamic NAT configuration on the ASA1/c2 context.

Verify if NAT control is enabled on the ASA1/c2 context. Also verify if static NAT commands are not used to complete this task. Then, verify that Dynamic NAT is configured correctly using the **nat/global** command set.

There is no need to configure an ACL on the outside interface, because traffic is traversing from a higher-security (inside) interface to a lower-security (outside) interface:

 Please see page 474 for more details.

```
ASA1# changeto context c2
ASA1/c2# show run nat-control
nat-control

ASA1/c2# show run static
<null output>

ASA1/c2# show run nat
nat (inside) 1 0.0.0.0 0.0.0.0

ASA1/c2# show run global
global (outside) 1 192.168.6.150-192.168.6.155
global (outside) 1 interface
```

When this configuration is OK, you can perform verification steps to check its functionality by establishing Telnet sessions from R3 to R6 Loopback0. You can issue the **who** command to validate that the source address is translated using a dynamic pool IP, such as 192.168.6.151:

```
R3# telnet 10.6.6.6
Trying 10.6.6.6 ... Open
User Access Verification
Password: cisco
R6> who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 20:44:46
*578 vty 0                 idle                 00:00:00 192.168.6.151
  Interface    User               Mode         Idle     Peer Address
R6> exit
[Connection to 10.6.6.6 closed by foreign host]
R3#
```

 Please see page 474 for more details.

Question 2.2: Asymmetric routing support (3 points)

Configure asymmetric routing support on ASA, meeting the following requirement:

- Configure the outside interface in both contexts to support for asymmetrically routed packets, preventing the return packets from being dropped in case a context does not have any session information for the packet.

Skills tested

- ☐ Configuring support for asymmetrically routed packets using the **asr-group** feature on the Cisco ASA firewall

Functionality and solution verification

- ☐ When the Cisco ASA firewall is configured for high-availability using Active/Active Failover, a device may receive a return packet for a connection that originated through its other peer unit. The packet could potentially be dropped when received on the ASA that does not have any connection information for the packet. This can be prevented using the **asr-group** command on interfaces where this is likely to occur.
- ☐ When an interface configured with the **asr-group** command receives a packet for which it has no session information, it checks the session information for the other interfaces that are in the same group. If it does not find a match, the packet is dropped. If it finds a match, one of the following actions occurs. If the incoming traffic originated on a peer unit, some or all of the Layer 2 header is rewritten, and the packet is redirected to the other unit. This redirection continues as long as the session is active. On the other hand, if the incoming traffic originated on a different interface on the same unit, some or all of the Layer 2 header is rewritten, and the packet is reinjected into the stream.
- ☐ Configure the outside interface in both contexts with the **asr-group** command to enable the asymmetric routing support. You can use any group ID to complete this task.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

Enable the **asr-group** command on the outside interface to participate in asymmetric routing support. You must enter the command on the unit where the context is in the active state so that the command is replicated to the standby failover group. For context c1, enter this command on the ASA1 unit; for context c2, enter this command on the ASA2 unit:

```
ASA1/c1# show run interface Ethernet0/0
interface Ethernet0/0
 nameif outside
<snip>
 asr-group 1
```

When this configuration is OK, you can also verify the asymmetric routing statistics using the following commands:

```
ASA1/c1# show interface outside detail
Interface Ethernet0/0 "outside", is up, line protocol is up
        MAC address 1200.0000.0200, MTU 1500
        IP address 192.168.6.10, subnet mask 255.255.255.0
  Traffic Statistics for "outside":
        67982 packets input, 7314227 bytes
        67902 packets output, 7307503 bytes
        14 packets dropped
  Control Point Interface States:
        Interface number is 1
        Interface config status is active
        Interface state is active
        Asymmetrical Routing Statistics:
                Received 0 packets
                Transmitted 0 packets
                Dropped 0 packets
```

 Please see page 474 for more details.

Question 2.3: Time-based access control (3 points)

Configure time-based access control on the Cisco ASA Firewall in context c1, meeting all the following requirements:

- The network administrator on R2 (with source IP address 10.2.2.2) is provided a one-hour downtime window for a scheduled maintenance to update router configuration of R6 (on IP address 10.6.6.6) between 9 p.m. and 10 p.m. on July 1, 2009.
- Configure the ASA1/c1 context to explicitly permit the specified IP traffic during the specified time.
- Do not use an inbound ACL to complete this task.
- Ensure that you can ping and telnet to R6 (10.6.6.6) from R2 (using source 10.2.2.2) during the downtime window. Ensure that ping and telnet fail outside the downtime window.

Skills tested

- ☐ Configuring network access control using a time-based ACL on the Cisco ASA firewall
- ☐ Configuring an outbound (egress) ACL on the Cisco ASA firewall

Functionality and solution verification

- ☐ This question is pretty straightforward, requiring you to enable network access control from a specific host to a specific destination during a specific window of time using time-based ACL on ASA.
- ☐ Additionally, the question clearly restricts the use of an inbound ACL, so using an outbound (egress) ACL is the only alternative solution.
- ☐ The first step is to configure a **time-range** for the specified time for a one-hour downtime window.
- ☐ The next step is to configure an extended ACL, carefully planning the **permit** and **deny** statements. As shown in the solution output, ACL 101 has three lines. The first line allows the specified traffic using the **time-range** keyword, thus permitting the traffic during the scheduled one-hour timeslot only. The second line of the ACL is required to deny the

same host-to-host traffic outside the one-hour timeslot (without the time-range). The third line permits all other IP traffic from any host to any destination. If you forget the third line, this can potentially impact a lot of other questions by blocking virtually all traffic passing through context c1. You could lose substantial points on the exam, so be very careful.

- ☐ The final step is to apply ACL 101 in the outbound direction to the outside interface in context c1.
- ☐ The question can be easily verified using a **ping** test and establishing a Telnet session from R2 to R6 to verify the functionality of the time-range configuration. For legitimate traffic to be successful, you need to change the system clock on ASA1 (in system context) to August 1, 2009, anytime between 9 p.m. and 10 p.m. Review the verification outputs shown next.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

Verify the time-range configuration on the ASA1/c1 context to ensure that all items are configured as per the requirement:

```
ASA1/c1# show time-range
time-range entry: abc (inactive)
   absolute start 21:00 01 August 2009 end 22:00 01 August 2009
   used in: IP ACL entry

ASA1/c1# show run access-group
access-group 100 in interface outside
access-group 101 out interface outside

ASA1/c1# show run access-list 101
access-list 101 extended permit ip host 10.2.2.2 host 10.6.6.6 time-range abc
access-list 101 extended deny ip host 10.2.2.2 host 10.6.6.6
access-list 101 extended permit ip any any
```

As you can see from the output, the **time-range** is currently in the (inactive) state because the system clock is out of the range specified.

You need to change the system clock (from the system context) to set it to the specified range so that the **time-range** becomes active and traffic is permitted:

```
ASA1# clock set 21:00:00 1 August 2009

ASA1# show clock
21:00:01.649 UTC Sat Aug 1 2009
ASA1#

ASA1/c1# show time-range
time-range entry: abc (active)
   absolute start 21:00 01 August 2009 end 22:00 01 August 2009
   used in: IP ACL entry
```

When this configuration is OK, you can perform verification steps to check the functionality of time-based network access control by establishing ping and Telnet sessions from R2 (10.2.2.2) to R6 (10.6.6.6):

```
R2# ping 10.6.6.6 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.6.6.6, timeout is 2 seconds:
Packet sent with a source address of 10.2.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R2#

R2# telnet 10.6.6.6 /source-interface Loopback 0
Trying 10.6.6.6 ... Open
User Access Verification
Password: cisco
```

 Please see page 474 for more details.

```
R6>
R6> exit
[Connection to 10.6.6.6 closed by foreign host]
R2#
```

To verify that the specified traffic is being blocked and not allowed when outside the specific time-range, change the clock to any time outside the specific time-range, and reverify ping and Telnet sessions from R2 (10.2.2.2) to R6 (10.6.6.6):

```
ASA1# clock set 6:00:00 5 August 2009

ASA1# show clock
06:00:06.339 UTC Wed Aug 5 2009

R2# ping 10.6.6.6 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.6.6.6, timeout is 2 seconds:
Packet sent with a source address of 10.2.2.2
.....
Success rate is 0 percent (0/5)

R2# telnet 10.6.6.6 /source-interface Loopback 0
Trying 10.6.6.6 ...
% Connection refused by remote host
```

Question 2.4: Cisco IOS Firewall using CBAC (4 points)

Configure IOS Firewall using Context-Based Access Control (CBAC) on R4, meeting all the following requirements:

- Enable CBAC inspection on R4 to protect networks in your topology. Ensure that CBAC protection continues to function in event of Frame Relay WAN link down, when rerouting traffic via alternate GigabitEthernet0/1 link. Do not enable CBAC inspection on GigabitEthernet0/1 link. Your solution must have CBAC inspection applied to any one interface only.

- Enable TCP, UDP, HTTP, and ICMP protocols for CBAC inspection.
- Allow Java packets from a trusted site at 198.168.10.25 while implicitly denying Java from all other sites.
- Adjust the firewall settings to delete any half-open sessions when the maximum number of half-open sessions reaches 300. The firewall should stop deleting when the number falls below 200. Additionally, adjust the maximum number of half-open TCP sessions per host to 100.
- Enable HTTP server on Sw1 using nonstandard HTTP port 8080. Verify that you can ping and telnet to Sw1 IP address 192.168.41.2 from R6 upon completion of this task.
- Ensure that all IP connectivity including IP routing and ICMP traffic used for verification for other sections of this lab continues to work. You are allowed to permit ICMP traffic from any source to any destination explicitly in this ACL.

Skills tested

- ☐ Configuring Cisco IOS Firewall using Context-Based Access Control (CBAC)
- ☐ Configuring HTTP protocol application inspection with Java filtering
- ☐ Configuring CBAC tuning using advanced inspection parameters
- ☐ Configuring Port Mapping (PAM) for CBAC inspection using nonstandard ports
- ☐ Enabling HTTP server on Cisco IOS and modifying the default HTTP port to use a nonstandard port

Functionality and solution verification

- ☐ This question is based on the legacy Cisco IOS Firewall Context-Based Access Control (CBAC) feature set. Although the new Zone Based Policy Firewall (ZFW) feature is more important in the lab exam, the legacy CBAC is still part of the lab blueprint and may appear on your lab exam.
- ☐ The first step in this task is to enable the protocols (TCP, UDP, HTTP, and ICMP) for CBAC inspection. Then you apply the inspection to the GigabitEthernet0/0 interface in the outbound direction to monitor all traffic from your topology going out of the router. The reason to choose the GigabitEthernet0/0 is that the question clearly says not to

apply CBAC on GigabitEthernet0/1. It also requires CBAC redundancy in case Serial0/0/0 goes down, which means the only option left is to apply CBAC on GigabitEthernet0/0. Note that when enabling HTTP inspection, you also need to configure Java filtering to allow Java packets coming from a trusted site only (198.168.10.25). This can be achieved using the java-list ACL option in the HTTP inspection.

- The second step is to configure an ACL to permit OSPF and ICMP traffic. Then you apply it to the GigabitEthernet0/0 interface in the inbound direction (the opposite of CBAC) so that dynamic ACL entries open a hole for the return traffic.
- Additional CBAC parameters need to be tuned to protect from half-open embryonic connections, adjusting high and low parameters.
- Finally, you must enable HTTP on Sw1 using nonstandard port 8080. You need to do two things. First, enable HTTP server on Sw1 and change its default port to use 8080. Second, enable Port Mapping (PAM) on R4 for CBAC inspection to be able to inspect HTTP traffic arriving on nonstandard ports.
- The question can be verified using several **ping** tests and by establishing Telnet sessions to verify the functionality of the CBAC configuration. Review the outputs shown next.
- You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- The highlighted portions are of the utmost importance. Grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

Verify the CBAC configuration on R4 to ensure that all items are configured as per the requirement:

```
R4# show ip inspect all
Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [unlimited : unlimited] connections
max-incomplete sessions thresholds are [200 : 300]
max-incomplete tcp connections per host is 100. Block-time 0 minute.
```

```
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
tcp reassembly queue length 16; timeout 5 sec; memory-limit 1024 kilo bytes
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name mycbac
    tcp alert is on audit-trail is off timeout 3600
    udp alert is on audit-trail is off timeout 30
    icmp alert is on audit-trail is off timeout 10
    http java-list 1 alert is on audit-trail is off timeout 3600

Interface Configuration
 Interface GigabitEthernet0/0
  Inbound inspection rule is not set
  Outgoing inspection rule is mycbac
    tcp alert is on audit-trail is off timeout 3600
    udp alert is on audit-trail is off timeout 30
    icmp alert is on audit-trail is off timeout 10
    http java-list 1 alert is on audit-trail is off timeout 3600
  Inbound access list is 101
  Outgoing access list is not set

R4# show ip access-lists 101
Extended IP access list 101
    10 permit icmp any any (310 matches)
    20 permit ospf any any (474 matches)

R4# show ip access-lists 1
Standard IP access list 1
    10 permit 198.168.10.25
```

Then verify that Port Mapping (PAM) is enabled on R4 for CBAC inspection so that you can inspect HTTP traffic arriving on nonstandard ports. Additionally, ensure that the HTTP server is enabled on Sw1 using the nonstandard 8080 port:

```
R4# show ip port-map http
Default mapping:  http                tcp port 80                    system defined
Default mapping:  http                tcp port 8080                  user defined

Sw1# show ip http server status
HTTP server status: Enabled
HTTP server port: 8080
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path: flash:html
HTTP server help root:
Maximum number of concurrent server connections allowed: 16
Server idle time-out: 180 seconds
Server life time-out: 180 seconds
Maximum number of requests allowed on a connection: 25
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-128-sha
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:
HTTP secure server active session modules: ALL
```

When this configuration is OK, you can perform verification steps to check the functionality of CBAC inspection by establishing ping and Telnet sessions from R6 to Sw1:

```
R6# ping 192.168.41.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.41.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R6# telnet 192.168.41.2 8080
Trying 192.168.41.2, 8080 ... Open
/
HTTP/1.1 400 Bad Request
Date: Fri, 05 Mar 1993 02:41:43 GMT
Server: cisco-IOS
Accept-Ranges: none
400 Bad Request
[Connection to 192.168.41.2 closed by foreign host]
R6#
```

While the HTTP connection is in progress, you can verify the CBAC session table on R4 and the HTTP connection table on Sw1 to validate the HTTP connection from R6 being inspected by CBAC:

```
R4# show ip inspect sessions
Established Sessions
 Session C047B340 (192.168.64.6:62819)=>(192.168.41.2:8080) http SIS_OPEN
R4#

Sw1# show ip http server connection
HTTP server current connections:
local-ipaddress:port  remote-ipaddress:port in-bytes   out-bytes
   192.168.41.2:8080     192.168.64.6:62819 0          0
```

 Please see page 474 for more details.

Section 3.0: Cisco VPN (15 Points)

Question 3.1: Configuring Group Encrypted Transport VPN (GETVPN) (4 points)

Configure Group Encrypted Transport VPN (GETVPN) on R1, R3, R5, and R6, meeting all the following requirements:

- Configure GETVPN using preshared keys on R1, R3, R5, and R6 using information in the table.
- Use "cisco" for the preshared key on all devices.
- R6 will be the Key Server (KS), and R3, R5, and R6 will be the Group Members (GM).
- You are allowed to update the firewall ACL in context c1 and c2 to complete this task.
- Use the information in the table to complete this task.

Skills tested

- ☐ Understanding the Group Domain of Interpretation (GDOI) protocol
- ☐ Understanding and implementing KS and GM
- ☐ Configuring Cisco GETVPN technology using a preshared key on routers
- ☐ Configuring IPsec Profiles

Functionality and solution verification

- ☐ This question covers one of the latest and most innovative methods of implementing VPN technology using a tunnel-free approach.
- ☐ GDOI is a newly developed group key protocol used in the implementation of GETVPN technology provisioning registration capability for all GMs registering with a KS. GDOI uses UDP port 848.
- ☐ This question is linked with the next one, in which GDOI will be used to protect the DMVPN traffic (GRE).

 Please see page 474 for more details.

- Both DMVPN hub and spoke routers are configured as GDOI GMs. An important point to remember is that a separate router must be used to configure the GDOI KS. Do not use the DMVPN hub router as the key server.
- One of the main advantages of using GDOI to encrypt DMVPN traffic is that after the GDOI KS is configured, no additional configuration is required on the KS for any newly added spokes within the same group/dmvpn. Only respective spokes need to be configured for GDOI.
- Note that GDOI does not support IPsec profiles; therefore, GDOI is enabled by applying a crypto map to the physical interface. Tunnel protection is no longer required in DMVPN configuration and hence is removed from the tunnel interface.
- Another important point to remember is that you need to apply **crypto map** on R3 on two interfaces: GigabitEthernet0/0 and GigabitEthernet0/1. The fundamental of choosing where to apply **crypto map** is to apply it on the interface where encrypted traffic is arriving/departing (as per the routing table). In other words, apply **crypto map** on the interface where the encrypt/decrypt process will occur. Therefore, you must apply **crypto map** on R3 Gig0/0 and Gig0/1, which is facing the two GMs upstream and downstream (R1 and R5).
- When the GDOI KS and GM setup is done, ensure that both DMVPN hub and spoke routers register with the KS and download the policies. Verification steps are shown next.
- A common mistake is that candidates forget to generate RSA keys on all routers. Ensure that you generate RSA keys with a label.
- You will see several **show** command outputs so that you can check and verify the requirement laid out in the question.
- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

Table 2-33 provides information that needs to be configured on the KS (R6). Use the following sample outputs from R6 to ensure that all requirements have been met.

TABLE 2-33 Configuration information for the key server (KS)

ISAKMP Policy	☐ Preshared Key Authentication ☐ 3DES encryption algorithm ☐ Secure Hash Standard (SHA) Hash algorithm ☐ Diffie-Hellman group 2
IPsec Policy	☐ ESP transform using 3DES cipher ☐ ESP transform using HMAC-SHA authentication ☐ IPsec profile name = dmvpn_using_gdoi ☐ Set IPsec SA lifetime to 10 hours ☐ Peering using Loopback 0 address
GDOI Parameters	☐ Group name = dmvpn ☐ Group identity number 2 ☐ Unicast Rekey transport with 2 retransmits at 10-second intervals ☐ Rekey lifetime to 24 hours
Access List Policies	☐ Traffic to be encrypted between any host to any destination for GRE protocol to communicate using GETVPN

Here are the verification outputs from the key server (R6):

```
R6# show crypto isakmp policy
Global IKE policy
Protection suite of priority 1
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit

R6# show crypto gdoi ks policy
```

```
Key Server Policy:
For group dmvpn (handle: 2147483650) server 10.6.6.6 (handle: 2147483650):

  # of teks : 1  Seq num : 0
  KEK POLICY (transport type : Unicast)
    spi : 0x2996E4B4437400E215D195A2D44ED89F
    management alg     : disabled    encrypt alg       : 3DES
    crypto iv length   : 8           key size          : 24
    orig life(sec): 86400       remaining life(sec): 85317
    sig hash algorithm : enabled     sig key length    : 94
    sig size           : 64
    sig key name       : dmvpn_gdoi

  TEK POLICY (encaps : ENCAPS_TRANSPORT)
    spi                : 0x65F6DF0D    access-list           : 101
    # of transforms    : 0             transform             : ESP_3DES
    hmac alg           : HMAC_AUTH_SHA
    alg key size       : 24            sig key size          : 20
    orig life(sec)     : 36000         remaining life(sec)   : 34918
    override life (sec): 0             antireplay window size: 64

R6# show crypto ipsec profile
IPSEC profile dmvpn_using_gdoi
        Security association lifetime: 4608000 kilobytes/36000 seconds
        PFS (Y/N): N
        Transform sets={
                dmvpn_trans:  { esp-3des esp-sha-hmac  } ,
        }
```

 Please see page 474 for more details.

```
R6# show crypto key mypubkey rsa
% Key pair was generated at: 07:38:41 UTC Aug 10 2009
Key name: dmvpn_gdoi
 Storage Device: private-config
 Usage: General Purpose Key
 Key is exportable.
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00B2563D 4A12F7E7
  339CDD50 3D9109B5 03652B4E 28F915C7 C58FC741 69ED8F40 BD4423FA 65A5FDFB
  2DA28CC6 B8F6B89A 5C4480FA DB630162 52EFB527 31269A69 7D020301 0001
% Key pair was generated at: 06:31:45 UTC Aug 11 2009
Key name: dmvpn_gdoi.server
Temporary key
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00C1CEBE 8226E21F
  FDE7C837 297B2AB4 45F1A896 563979B7 C060A737 79E77A36 690C5636 64699507
  574870F5 8D8D2632 0F7C6454 CA3E97C0 47B0020D 24E5CCE7 6800DB04 5EF77787
  BC45FE34 3959FEDC 62AAB603 B346D7FD CAA6F354 9C252987 CF020301 0001

R6# show run ¦ section crypto gdoi
crypto gdoi group dmvpn
 identity number 2
 server local
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa dmvpn_gdoi
  rekey transport unicast
  sa ipsec 1
   profile dmvpn_using_gdoi
```

```
    match address ipv4 101
    replay counter window-size 64
   address ipv4 10.6.6.6

R6# show crypto gdoi ks acl
Group Name: dmvpn
 Configured ACL:
   access-list 101 permit gre any any

R6# show crypto gdoi ks rekey
Group dmvpn (Unicast)
    Number of Rekeys sent               : 0
    Number of Rekeys retransmitted      : 0
    KEK rekey lifetime (sec)            : 86400
        Remaining lifetime (sec)        : 85272
    Retransmit period                   : 10
    Number of retransmissions           : 2
    IPsec SA 1  lifetime (sec)          : 36000
        Remaining lifetime (sec)        : 34873

R6# show crypto gdoi ks members
Group Member Information :
Number of rekeys sent for group dmvpn : 0

Group Member ID   : 10.1.1.1
Group ID          : 2
Group Name        : dmvpn
Key Server ID     : 10.6.6.6
Rekeys sent       : 0
Rekeys retries    : 0
```

 Please see page 474 for more details.

```
Rekey Acks Rcvd   : 0
Rekey Acks missed : 0
Sent seq num :    0    0    0    0
Rcvd seq num :    0    0    0    0

Group Member ID   : 10.3.3.3
Group ID          : 2
Group Name        : dmvpn
Key Server ID     : 10.6.6.6
Rekeys sent       : 0
Rekeys retries    : 0
Rekey Acks Rcvd   : 0
Rekey Acks missed : 0
Sent seq num :    0    0    0    0
Rcvd seq num :    0    0    0    0

Group Member ID   : 10.5.5.5
Group ID          : 2
Group Name        : dmvpn
Key Server ID     : 10.6.6.6
Rekeys sent       : 0
Rekeys retries    : 0
Rekey Acks Rcvd   : 0
Rekey Acks missed : 0
Sent seq num :    0    0    0    0
Rcvd seq num :    0    0    0    0

R6# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
```

```
10.6.6.6        10.3.3.3        GDOI_IDLE          1002 ACTIVE
10.6.6.6        10.1.1.1        GDOI_IDLE          1003 ACTIVE
10.6.6.6        10.5.5.5        GDOI_IDLE          1001 ACTIVE
```

Table 2-34 provides information that needs to be configured on the GMs (R1, R3, and R5). Use the following sample outputs to ensure that all requirements have been met.

TABLE 2-34 Configuration information for the group members (GM)

ISAKMP Policy	☐ Preshared Key Authentication ☐ 3DES encryption algorithm ☐ Secure Hash Standard (SHA) Hash algorithm ☐ Diffie-Hellman group 2
GDOI Parameters	☐ Group name = dmvpn_gdoi ☐ Group identity number 2 ☐ Key Server IP address 10.6.6.6

Here are the verification outputs from group member R3. Repeat these steps on other GMs (R1 and R5):

```
R3# show crypto map
Crypto Map: "dmvpn_using_gdoi" idb: Loopback0 local address: 10.3.3.3
Crypto Map "dmvpn_using_gdoi" 10 gdoi
        Group Name: dmvpn_gdoi
            identity number 2
            server address ipv4 10.6.6.6
        Interfaces using crypto map dmvpn_using_gdoi:
                GigabitEthernet0/0
                GigabitEthernet0/1

R3# show crypto isakmp policy
Global IKE policy
```

```
Protection suite of priority 1
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit

R3# show run ¦ sec crypto gdoi
crypto gdoi group dmvpn_gdoi
 identity number 2
 server address ipv4 10.6.6.6
```

Then, verify the GMs to ensure that they have successfully registered with the KS and downloaded the KEK and TEK policies.

Here is the verification output from group member R3. Repeat these steps on other GMs (R1 and R5):

```
R3# show crypto gdoi
GROUP INFORMATION

    Group Name               : dmvpn_gdoi
    Group Identity           : 2
    Rekeys received          : 0
    IPsec SA Direction       : Both
    Active Group Server      : 10.6.6.6
    Group Server list        : 10.6.6.6

    GM Reregisters in        : 32481 secs
    Rekey Received           : never
```

 Please see page 474 for more details.

```
    Rekeys received
         Cumulative          : 0
         After registration  : 0
    Rekey Acks sent          : 0

 ACL Downloaded From KS 10.6.6.6:
   access-list  permit gre any any

KEK POLICY:
    Rekey Transport Type     : Unicast
    Lifetime (secs)          : 86337
    Encrypt Algorithm        : 3DES
    Key Size                 : 192
    Sig Hash Algorithm       : HMAC_AUTH_SHA
    Sig Key Length (bits)    : 512

TEK POLICY:
  GigabitEthernet0/0:
  GigabitEthernet0/1:
    IPsec SA:
        sa direction:inbound
        spi: 0x65F6DF0D(1710677773)
        transform: esp-3des esp-sha-hmac
        sa timing:remaining key lifetime (sec): (34272)
        Anti-Replay :  Disabled

    IPsec SA:
        sa direction:outbound
        spi: 0x65F6DF0D(1710677773)
        transform: esp-3des esp-sha-hmac
        sa timing:remaining key lifetime (sec): (34272)
        Anti-Replay :  Disabled
```

TIP

Remember that NAT control is enabled on context c2. You need to add a static NAT translation for R3's Loopback0 in context c2, or you will get inconsistent results. Add static NAT as follows: **static (inside,outside) 10.3.3.3 10.3.3.3**.

NOTE

If your group members (GM) are registering with the key server (KS), but you are unable to get the next question (DMVPN) working, you will *not* lose points for this task, simply because you have satisfied the requirement of this task thus far. However, if it is the other way around, you will lose points for both questions.

Question 3.2: Configuring Dynamic Multipoint VPN (DMVPN) using GDOI (4 points)

Configure Dynamic Multipoint VPN (DMVPN) using GDOI on R1, R3, and R5, meeting all the following requirements:

- Configure DMVPN using GETVPN integration on R1, R3, and R5 using the information in Tables 2-35 and 2-36.
- R1 will be the DMVPN Hub router, and R3 and R5 will be the DMVPN spoke routers.
- You are allowed to update the firewall ACL in context c1 and c2 to complete this task.
- Use the information in the tables to complete this task.

TABLE 2-35 Configuration information for the DMVPN hub (R1)

Tunnel Policy	☐ Tunnel number 0 ☐ IP Address 172.16.1.1/24 ☐ Peer using Loopback 0 address ☐ Tunnel destination not allowed ☐ NHRP authentication password "cisco" ☐ NHRP Network ID 2 ☐ Secure Tunnel key 2
Routing Policy	☐ Advertise Tunnel 0 and private network Loopback 11 into EIGRP AS 2

TABLE 2-36 Configuration information for the DMVPN spokes (R3 and R5)

Tunnel Policy	☐ Tunnel number 0 ☐ IP address 172.16.1.*X*/24 (where *X* is the spoke router number) ☐ Peer using Loopback 0 address ☐ Tunnel destination not allowed ☐ NHRP authentication password "cisco" ☐ NHRP Network ID 2 ☐ Secure Tunnel key 2
Routing Policy	☐ Advertise Tunnel 0 and private network Loopback 11 into EIGRP AS 2

 Please see page 474 for more details.

NOTE

For more information, review a whitepaper on implementing GDOI in a DMVPN solution: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/ps6811/prod_white_paper0900aecd804c363f.html.

Skills tested

- ☐ Configuring Dynamic Multipoint VPN (DMVPN) using GDOI protocol and GETVPN integration
- ☐ Understanding DMVPN and NHRP components and how they work
- ☐ Designing highly scalable VPN networks without creating multiple tunnels by combining the DMVPN and GETVPN technology

Functionality and solution verification

- ☐ This question may seem straightforward in configuring DMVPN, but it can be challenging when integrating with the GETVPN technology.
- ☐ As mentioned earlier, this question is linked with Question 3.1, because GDOI will be used to protect the DMVPN traffic (GRE).
- ☐ DMVPN is implemented using IPsec tunnel protection (installing policies dynamically during tunnel negotiation) on the mGRE tunnel interfaces of both hub and spoke routers. Each spoke maintains a permanent IPsec tunnel with the hub, and any spoke-to-spoke connectivity requires the spoke to send an NHRP resolution request to the hub. Upon receiving an NHRP resolution reply, the spoke dynamically creates another IPsec tunnel directly with the destination spoke. A new set of pairwise keys is negotiated between spokes directly, and a point-to-point tunnel is created, introducing a delay in setting up direct tunnels. By integrating GDOI within the DMVPN, the delay can be reduced by eliminating this creation of direct tunnels between spokes.
- ☐ With GDOI, both the hub and spoke routers are group members (part of the GETVPN solution). Group keys can be distributed to the hub and spokes, eliminating the need for point-to-point IPsec sessions between them. Any group member can talk to any other group member using the same key. This means that the spoke changes the destination address to forward traffic directly to other spokes when NHRP resolution is completed. This reduces the delay between spoke-to-spoke connections by eliminating the creation of dynamic IPsec tunnels between them. By using GDOI technology, the delay caused by IPsec negotiation is eliminated, which is the major contributor to the overall delay. GDOI is not a replacement for DMVPN.

- This design provides a major advantage. Each spoke router maintains a GDOI session only with the key server, and there is no permanent tunnel between the hub and spoke. The spoke maintains NHRP entries for the hub; the spoke still needs to contact the hub first whenever spoke-to-spoke connectivity is required. The key server can push **gre any any** to all group members to achieve the same result as DMVPN using tunnel protection. Note that GDOI does not support IPsec profiles; therefore, GDOI is enabled by applying a crypto map to the physical interface. Tunnel protection is no longer required in the DMVPN configuration and hence is removed from the tunnel interface.
- Another major advantage of using GDOI to encrypt DMVPN traffic is that after the GDOI KS is configured, no additional configuration is required on KS for any newly added spokes within the same group/DMVPN. Only respective spokes need to be configured for GDOI.
- Before starting to configure DMVPN, ensure that all devices (DMVPN hub and spokes) are registered with the key server (GDOI KS) and have successfully downloaded the policies.
- Remember that NAT control is enabled on context c2. You need to add a static NAT translation for R3's Loopback0 in context c2, or you will get inconsistent results. Add static NAT as follows: **static (inside,outside) 10.3.3.3 10.3.3.3**.
- Also remember to update the ACL on context c1 and c2 to permit ISAKMP and ESP for spoke routers to send encrypted traffic to the R1 hub, and between spokes. Because the question does not restrict, you can permit UDP/500 and ESP any-to-any in both contexts.
- Configure the DMVPN hub and spoke routers using the information provided in the tables. Remember, configuring the **tunnel protection ipsec profile** command on the tunnel interface is no longer required. The GDOI ACL defines the policies to be pushed to all group members (**gre any any**), which is used to encrypt all traffic seen in the DMVPN tunnel interface. This achieves the same result as DMVPN with tunnel protection.
- You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

NOTE
Multicast traffic is forwarded to the hub router for any spoke-to-spoke communication.

TIP
The point just mentioned (not using an IPsec profile on the tunnel interface) is the key requirement for the DMVPN integration with GETVPN solution to work.

The following summarizes the packet flow in the DMVPN network using GDOI:

1. The DMVPN hub and all spokes are configured as group members and register with the GDOI key server.
2. The key server distributes the group key and IPsec policy to all group members; the IPsec policy defines the traffic selectors. For DMVPN, **gre any any** secures all tunnel traffic.
3. A spoke-to-hub tunnel is established using NHRP. All packets traveling via the DMVPN tunnel are now encrypted using the group key.
4. The spoke sends an NHRP resolution request to the hub for any spoke-to-spoke communication.
5. Upon receiving an NHRP resolution reply from the hub, the spoke sends traffic directly to other spokes with group key encryption. Until the NHRP resolution reply is received, spoke-to-spoke traffic continues via the hub with group key encryption.

First, verify the DMVPN hub configuration. Also ensure that the **tunnel protection ipsec profile** command is *not* applied to the DMVPN Tunnel 0 interface.

```
R1# show run interface Tunnel 0
Building configuration...
Current configuration : 420 bytes
!
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 no ip next-hop-self eigrp 2
 ip pim dr-priority 10
 ip pim nbma-mode
 ip pim sparse-dense-mode
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
```

 Please see page 474 for more details.

```
 ip nhrp network-id 2
 ip nhrp server-only
 no ip split-horizon eigrp 2
 no ip mroute-cache
 delay 1500
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 2
!<"tunnel protection" command should NOT be applied>
end

R1# show ip protocols
Routing Protocol is "eigrp 2"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 2
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    10.11.11.11/32
    172.16.1.0/24
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.1.3           90       00:59:56
```

 Please see page 474 for more details.

```
    Distance: internal 90 external 170

  Routing Protocol is "nhrp"
    Maximum path: 0
    Routing Information Sources:
      Gateway         Distance      Last Update
    Distance: (default is 0)
```

TIP
The point just mentioned (not using IPsec profile on the tunnel interface) is the key requirement for the DMVPN integration with GETVPN solution to work.

Now, verify that the DMVPN spokes are configured correctly, as per the table.

Also ensure that spokes are not configured with IPsec profiles and that the **tunnel protection ipsec profile** command is *not* applied to the DMVPN Tunnel 0 interface.

Here is the verification output from group member spoke R3. Repeat these steps on spoke R5:

```
R3# show crypto ipsec profile
!<no output, blank>
R3#

R3# show run interface Tunnel 0
Building configuration...
Current configuration : 484 bytes
!
interface Tunnel0
 ip address 172.16.1.3 255.255.255.0
 no ip redirects
 ip mtu 1400
 no ip next-hop-self eigrp 2
 ip pim sparse-dense-mode
 ip nhrp authentication cisco
 ip nhrp map 172.16.1.1 10.1.1.1
```

 Please see page 474 for more details.

```
 ip nhrp map multicast 10.1.1.1
 ip nhrp network-id 2
 ip nhrp nhs 172.16.1.1
 ip nhrp registration no-unique
 no ip split-horizon eigrp 2
 no ip mroute-cache
 load-interval 30
 delay 2000
 qos pre-classify
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 2
!<"tunnel protection" command should NOT be applied>
end
R3#
```

All GMs R1, R3, and R5 have been preconfigured with interface Loopback11 in subnet 10.*xx*.*xx*.0/24 (where *xx* is the router number), and you are required to advertise them into the EIGRP AS 2 routing protocol. Ensure that you have these networks on each GM in EIGRP AS 2. Verify that each DMVPN router has routes to Loopback11 for each other.

Here is the verification output from group member spoke R3. Repeat these steps on spoke R5:

```
R3# show ip protocols
Routing Protocol is "eigrp 2"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
```

 Please see page 474 for more details.

```
  Redistributing: eigrp 2
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    10.33.33.33/32
    172.16.1.0/24
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.1.1            90      00:53:23
  Distance: internal 90 external 170

Routing Protocol is "nhrp"
  Maximum path: 0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 0)

R3# show ip route eigrp 2

     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
D       10.11.11.11/32 [90/26240000] via 172.16.1.1, 00:08:54, Tunnel0
D       10.55.55.55/32 [90/26624000] via 172.16.1.5, 00:08:54, Tunnel0
```

TIP

Remember to add the ACL on context c1 and c2 to permit ISAKMP and ESP for DMVPN routers to send encrypted traffic to the R1 hub, and between spokes. Because the question does not restrict, you can permit UDP/500 and ESP any-to-any in both contexts.

Finally, ensure that traffic between GMs Loopback11 is getting encrypted via the GETVPN tunnel. You can verify this using the following ping tests and by checking the **show crypto engine connections active** command to verify that the encrypt and decrypt counters are incrementing accordingly.

Here is the verification output from group member spoke R3. Repeat these steps on spoke R5:

NOTE
If your DMVPN hub and spoke routers are *not* registering with the key server (KS) and are unable to download the TEK and KEK policies, your ISAKMP and IPsec tunnels won't come up, and you will lose points for both this question and the preceding one.

```
R3# ping 10.11.11.11 repeat 20
Type escape sequence to abort.
Sending 20, 100-byte ICMP Echos to 10.11.11.11, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (20/20), round-trip min/avg/max = 1/1/4 ms

R3# show crypto engine connections active
Crypto Engine Connections
   ID  Type    Algorithm           Encrypt  Decrypt IP-Address
 1001  IKE     SHA+3DES                  0        0 10.3.3.3
 1002  IKE     SHA+3DES                  0        0
 2001  IPsec   3DES+SHA                  0      458 0.0.0.0
 2002  IPsec   3DES+SHA                462        0 0.0.0.0
```

Question 3.3: Troubleshooting Easy VPN using DVTI (4 points)

Enhanced Easy VPN using the IPsec Dynamic Virtual Tunnel Interface (DVTI) has been preconfigured on R2 and R4 in this question. Your task is to troubleshoot and identify the injected faults and bring up the Easy VPN tunnel, meeting all the following requirements:

- Easy VPN is preconfigured using preshared keys "cisco" on R2 and R4 using information in Tables 2-37 and 2-38.
- R2 is the Easy VPN Hub router, and R4 is the Easy VPN spoke router.
- Five faults are injected into your preconfiguration. Identify these faults, and verify that the tunnel comes up. Note that the faults injected can be related to either incorrect preconfiguration or missing commands to complete the configuration.
- You are allowed to modify the ACL on the ASA/c1 context to complete this task. This excludes the five faults.
- Use the information in the tables to complete this task.

TABLE 2-37 Information for the Easy VPN hub router (R2)

AAA Policy	☐ Named Login Authentication using local database (name = ezvpn) ☐ Named Network Authorization using local database (name = ezvpn) ☐ Local username "cisco" password "cisco"
ISAKMP Policy	☐ Preshared Key Authentication ☐ 3DES encryption algorithm ☐ Secure Hash Standard (SHA) Hash algorithm ☐ Diffie-Hellman group 2 ☐ ISAKMP profile name = ezvpn_dvti
IPsec Policy	☐ Transform set name = ezvpn_trans ☐ ESP transform using 3DES cipher ☐ ESP transform using HMAC-SHA auth ☐ IPsec profile name = ezvpn_dvti
Easy VPN Policy	☐ Group name = cisco ☐ Group password = cisco ☐ Domain name = cisco.com ☐ IP pool = 10.20.20.1 through 10.20.20.100
DVTI Policy	☐ Virtual-Template 1 ☐ IP unnumbered using Loopback0 address ☐ Tunnel Source using Loopback0 address

TABLE 2-38 Information for the Easy VPN spoke router (R4)

Easy VPN Policy	☐ EzVPN profile name = ezvpn_dvti ☐ Group name = cisco ☐ Group password = cisco ☐ Connect type = auto ☐ Mode = client ☐ Xauth mode interactive on console ☐ Peer using R2 Loopback0 address

NOTE
As mentioned on the CCIE lab exam blueprint, "Knowledge of troubleshooting is an important skill, and candidates are expected to diagnose and solve issues as part of the CCIE lab exam." The new v3.0 Lab exam strongly enforces this aspect. The new lab exam will be just as challenging and will validate both configuration and troubleshooting skills. Candidates must practice troubleshooting methods and techniques as an important skill set to be successful.

NOTE
For more information, review a whitepaper on configuring Enhanced Easy VPN with IPsec Dynamic Virtual Tunnel Interface (DVTI): http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/prod_white_paper0900aecd803645b5.html.

TABLE 2-38 *Continued*

Apply	☐ Inside interface = GigabitEthernet0/0 ☐ Outside interface = Serial0/0/0

Skills tested

- ☐ Troubleshooting Easy VPN technology in a real-time environment
- ☐ Identifying network-related issues within an existing topology that has been preconfigured

Functionality and solution verification

- ☐ This new format question is very different from the traditional configuration-based questions. The objective is to identify candidates' analytical skills in a complex environment where an engineer applies his or her troubleshooting skills to fix networking-related problems using a methodological approach with the aid of various tools. Extensive knowledge of **show** and **debug** commands is very important in these scenarios.
- ☐ A basic approach to solving this type of question is to break it into layers, such as IP connectivity, routing, switching, ISAKMP phase 1, and ISAKMP phase 2 related issues, to name a few. As just mentioned, you should use a methodological approach. Start by reviewing the current preconfiguration using **show** commands, but if you cannot find anything unusual, enable relevant **debugs** to get more details.
- ☐ The issues that were injected into the preconfiguration are discussed next.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

You can use several methods and varying techniques to start troubleshooting; there is no perfect method. Every person has different methodologies and uses a different approach. As long as the main objective is met, it is OK to use your own method. However, earlier I described a basic approach and how to use it effectively to your advantage.

Here is a list of five faults injected into your preconfiguration:

- Fault 1 can be found on Sw2. An ACL has been preconfigured and applied to FastEthernet0/2 (connecting R2 GigabitEthernet0/1 in VLAN 4) and is dropping all UDP/500 packets for ISAKMP communication. To fix this issue, simply remove the ACL using the **no ip access-group 101 in** command.
- Fault 2 can be found on R2. The Group password/key is missing under the **crypto isakmp client configuration group** section. You can fix this by adding the group password using the **key cisco** command under the ISAKMP client configuration section.
- Fault 3 can also be found on R2. The **virtual-template 1** command is missing under the **crypto isakmp profile** section. Add this command to match the Virtual-Template interface ID.
- Fault 4 can be found on R4. The **crypto ipsec client ezvpn ezvpn_dvti inside** command is missing under the GigabitEthernet0/0 interface. Add it.
- Fault 5 can also be found on R4. The peer address is incorrect; it should be 10.2.2.2, not 192.168.4.2. Replace the current peer under **crypto ipsec client ezvpn ezvpn_dvti** by removing **no peer 192.168.4.2** and adding **peer 10.2.2.2**.

After all five faults have been found and fixed, perform the following verification to ensure that the Easy VPN tunnel comes up.

Note that when you check the tunnel's status, it does not come up automatically, because it requires the XAUTH authentication and authorization process. The **show crypto ipsec client ezvpn** command output shows that the state is in the XAUTH_REQ stage, requiring you to manually input the username and password interactively via the console:

```
R4# show crypto ipsec client ezvpn
Easy VPN Remote Phase: 8
Tunnel name : ezvpn_dvti
Inside interface list: GigabitEthernet0/0
Outside interface: Serial0/0/0
Current State: XAUTH_REQ
Last Event: XAUTH_REQUEST
Save Password: Disallowed
Current EzVPN Peer: 10.2.2.2
```

Perform the following steps to initiate XUATH, verify that the Easy VPN tunnel comes up, and ensure that the current state changes to IPSEC_ACTIVE, confirming that the tunnel is active:

```
R4# crypto ipsec client ezvpn xauth
Username: cisco
Password: cisco
R4#

R4# show crypto ipsec client ezvpn
Easy VPN Remote Phase: 8
Tunnel name : ezvpn_dvti
Inside interface list: GigabitEthernet0/0
Outside interface: Serial0/0/0
Current State: IPSEC_ACTIVE
Last Event: MTU_CHANGED
Address: 10.20.20.3 (applied on Loopback10000)
Mask: 255.255.255.255
Default Domain: cisco.com
Save Password: Disallowed
Current EzVPN Peer: 10.2.2.2
```

In addition, check the ISAKMP SA using **show crypto isakmp sa** command output and IPsec SA using **show crypto ipsec sa** command output to ensure that tunnels are established properly.

Question 3.4: Troubleshooting L2L IPsec VPN using VTI (3 points)

LAN-to-LAN (L2L) IPsec VPN using the Virtual Tunnel Interface (VTI) has been preconfigured between R4 and R5 in this question. Your task is to troubleshoot and identify the injected faults and bring up the IPsec L2L VPN tunnel, meeting all the following requirements:

- L2L VPN is preconfigured using preshared keys "cisco" on R4 and R5 using information in Table 2-39.
- Four faults are injected into your preconfiguration. Identify these faults, and verify that the tunnel comes up. Note that the faults injected could be related to either incorrect preconfiguration or missing commands to complete the configuration.
- Use the information in the table to complete this task.

TABLE 2-39 Configuration information

ISAKMP Policy	☐ Preshared Key Authentication ☐ 3DES encryption algorithm ☐ Secure Hash Standard (SHA) Hash algorithm ☐ Diffie-Hellman group 2
IPsec Policy	☐ Transform set name = L2L_trans ☐ ESP transform using 3DES cipher/ ☐ ESP transform using HMAC-SHA auth ☐ IPsec profile name = L2L_VTI
VTI Policy	☐ VTI Tunnel Number 45 ☐ Tunnel IP address on R4 and R5 (100.1.1.1/24 and 100.1.1.2/24) respectively ☐ Tunnel Source = GigabitEthernet (192.168.45.0)
Routing Policy	☐ Dynamic routing using RIP version 2 ☐ Disable auto summarization ☐ Advertise subnets Loopback 45 and Tunnel 45

NOTE

As mentioned on the CCIE lab exam blueprint, "Knowledge of troubleshooting is an important skill, and candidates are expected to diagnose and solve issues as part of the CCIE lab exam." The new v3.0 Lab exam strongly enforces this aspect. The new lab exam will be just as challenging and will validate both configuration and troubleshooting skills. Candidates must practice troubleshooting methods and techniques as an important skill set to be successful.

NOTE

For more information, review a whitepaper on configuring site-to-site IPsec using the Virtual Tunnel Interface (VTI) solution:http://www.cisco.com/en/US/technologies/tk583/tk372/technologies_white_paper0900aecd8029d629_ps6635_Products_White_Paper.html.

Skills tested

- ☐ Troubleshooting LAN-to-LAN (L2L) IPsec VPN using the Virtual Tunnel Interface (VTI) technology
- ☐ Identifying network-related issues within an existing topology that has been preconfigured

Functionality and solution verification

- ☐ This is another troubleshooting-oriented question, similar to the previous one. The objective is to identify candidates' skills in both legacy and emerging technologies by applying troubleshooting skills to fix networking-related problems using a methodological approach with the aid of various tools. Extensive knowledge of **show** and **debug** commands is very important in these scenarios.
- ☐ As mentioned earlier, use a methodological approach. Start by reviewing the current preconfiguration using **show** commands, but if you cannot find anything unusual, enable relevant **debugs** to get more details.
- ☐ IPsec Virtual Tunnel Interface (VTI) is a new technology used to configure IPsec-based LAN-to-LAN (L2L) VPN between site-to-site routers.
- ☐ One of the major advantages of using IPsec VTI is that it can be used to transfer multicast traffic, control traffic, or data traffic. IPsec VTI does not require a static mapping of IPsec sessions to a physical interface, thus eliminating the need to define a static peer command. Traffic is encrypted when it is forwarded from or to the logical tunnel interface. Dynamic or static IP routing can be used to route VPN interesting traffic to the encryption engine (tunnel interface), thus eliminating the need to use the IPsec ACL (legacy mechanism) to define VPN interesting traffic.
- ☐ The issues that were injected into the preconfiguration are discussed next.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

 Please see page 474 for more details.

You can use several methods and varying techniques to start troubleshooting; there is no perfect method. Every person has different methodologies and uses different approach. As long as the main objective is met, it is OK to use your own method. However, earlier I described a basic approach and how to use it effectively.

Here is a list of four faults injected into your preconfiguration:

- Fault 1 can be found on R4. An ACL has been preconfigured and applied to GigabitEthernet0/1 and is explicitly dropping all UDP/500 packets for ISAKMP communication between the peer endpoints in this task. To fix this issue, simply remove the ACL using the **no ip access-group 102 in** command.
- Fault 2 can also be found on R4. The **tunnel mode ipsec ipv4** command is missing under the **interface Tunnel45** section. Add this command under tunnel interface 45. By default, the tunnel interface mode is GRE. You can check this using the **show interface tunnel** command. One of the fundamental requirements of the VTI configuration is using the tunnel interface with IPsec mode.
- Fault 3 can be found on R5. The **tunnel protection** command is not applied under the **interface Tunnel45** section. Add the **tunnel protection ipsec profile L2L_VTI** command under the tunnel interface to encrypt L2L traffic using IPsec profile.
- Fault 4 can also be found on R5. The private subnet Loopback 45 is not advertised under RIP protocol. Advertise Loopback 45 using the **network 45.45.5.0** command under the **router rip** section.

When all four faults have been found and fixed, perform the following verification to ensure that the IPsec VPN tunnel comes up.

Check the ISAKMP SA using **show crypto isakmp sa** command output and IPsec SA using **show crypto ipsec sa** command output to ensure that tunnels are established properly. Check that the RIP routing table is showing the advertised routes and that you can ping Loopback 45 on both devices.

Here are the verification steps on R4:

```
R4# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.45.4    192.168.45.5    QM_IDLE           1036 ACTIVE
10.2.2.2        10.4.4.4        QM_IDLE           1031 ACTIVE

R4# show crypto ipsec sa interface Tunnel 45
     PFS (Y/N): N, DH group: none

interface: Tunnel45
    Crypto map tag: Tunnel45-head-0, local addr 192.168.45.4

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 192.168.45.5 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 54, #pkts encrypt: 54, #pkts digest: 54
    #pkts decaps: 52, #pkts decrypt: 52, #pkts verify: 52
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 192.168.45.4, remote crypto endpt.: 192.168.45.5
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0xAA78098D(2859993485)

     inbound esp sas:
      spi: 0x298D2A65(697117285)
```

```
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2025, flow_id: Onboard VPN:25, sibling_flags 80000046, crypto map: Tunnel45-head-0
        sa timing: remaining key lifetime (k/sec): (4595260/3173)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xAA78098D(2859993485)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2026, flow_id: Onboard VPN:26, sibling_flags 80000046, crypto map: Tunnel45-head-0
        sa timing: remaining key lifetime (k/sec): (4595260/3173)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

R4# show ip route rip
     45.0.0.0/24 is subnetted, 2 subnets
R       45.45.5.0 [120/1] via 100.1.1.2, 00:00:07, Tunnel45
```

```
R4# ping 45.45.5.1 repeat 20
Type escape sequence to abort.
Sending 20, 100-byte ICMP Echos to 45.45.5.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (20/20), round-trip min/avg/max = 1/3/32 ms

R4# show crypto engine connections active
Crypto Engine Connections
   ID  Type    Algorithm           Encrypt  Decrypt IP-Address
 1031  IKE     SHA+3DES                  0        0 10.4.4.4
 1036  IKE     SHA+3DES                  0        0 192.168.45.4
 2013  IPsec   3DES+SHA                  0        0 10.4.4.4
 2014  IPsec   3DES+SHA                  0        0 10.4.4.4
 2025  IPsec   3DES+SHA                  0       42 192.168.45.4
 2026  IPsec   3DES+SHA                 43        0 192.168.45.4
R4#
```

Here are the verification steps on R5:

```
R5# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.45.4    192.168.45.5    QM_IDLE           1008 ACTIVE

R5# show crypto ipsec sa interface Tunnel 45
     PFS (Y/N): N, DH group: none

interface: Tunnel45
    Crypto map tag: Tunnel45-head-0, local addr 192.168.45.5
```

```
protected vrf: (none)
local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 192.168.45.4 port 500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 48, #pkts encrypt: 48, #pkts digest: 48
 #pkts decaps: 49, #pkts decrypt: 49, #pkts verify: 49
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0

  local crypto endpt.: 192.168.45.5, remote crypto endpt.: 192.168.45.4
  path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
  current outbound spi: 0x298D2A65(697117285)

  inbound esp sas:
   spi: 0xAA78098D(2859993485)
     transform: esp-3des esp-sha-hmac ,
     in use settings ={Tunnel, }
     conn id: 2091, flow_id: Onboard VPN:91, sibling_flags 80000046, crypto map: Tunnel45-head-0
     sa timing: remaining key lifetime (k/sec): (4563153/3109)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE

  inbound ah sas:

  inbound pcp sas:
```

```
     outbound esp sas:
      spi: 0x298D2A65(697117285)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2092, flow_id: Onboard VPN:92, sibling_flags 80000046, crypto map: Tunnel45-head-0
        sa timing: remaining key lifetime (k/sec): (4563153/3109)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

R5# show ip route rip
     45.0.0.0/24 is subnetted, 2 subnets
R       45.45.4.0 [120/1] via 100.1.1.1, 00:00:05, Tunnel45

R5# ping 45.45.4.1 repeat 20
Type escape sequence to abort.
Sending 20, 100-byte ICMP Echos to 45.45.4.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (20/20), round-trip min/avg/max = 1/1/4 ms

R5# show crypto engine connections active
Crypto Engine Connections

   ID  Type    Algorithm           Encrypt  Decrypt IP-Address
 1008  IKE     SHA+3DES                  0        0 192.168.45.5
 2073  IPsec   3DES+SHA                  0     4621 0.0.0.0
```

 Please see page 474 for more details.

```
2074   IPsec    3DES+SHA              3611        0 0.0.0.0
2075   IPsec    3DES+SHA                 0        0 0.0.0.0
2076   IPsec    3DES+SHA                 0        0 0.0.0.0
2091   IPsec    3DES+SHA                 0       70 192.168.45.5
2092   IPsec    3DES+SHA                69        0 192.168.45.5
R5#
```

Section 4.0: Cisco IPS (Intrusion Prevention System) (8 Points)

Question 4.1: Configuring IPS signatures (4 points)

Configure Cisco IPS sensor appliance, meeting both of the following requirements:

- Configure signature tuning and custom signatures in sig0 using information in Table 2-40 to complete this task.

TABLE 2-40 IPS signature configuration information

Signature Tuning	☐ Enable ICMP echo and echo-reply signatures. ☐ Set the alert severity to medium level and action to produce alert.
Custom Signature	☐ Create a custom Sig# **65000** named "Large ICMP attack" that inspects all ICMP packets with its IP payload size ranging between 5000 and 6000 bytes. ☐ This signature should trigger only when ICMP traffic is destined to any RFC 1918 address range. ☐ Set the alert severity to medium level and action to produce alert.

- Ensure that a signature is triggered when sending large ICMP ping packets to RFC 1918 address. For example, ping from R4 as follows.

```
R4# ping 10.8.8.8 size 5500
```

 Please see page 474 for more details.

Skills tested

- ☐ Configuring basic signature tuning and modifying parameters to the existing signatures available on the sensor database
- ☐ Configuring a new custom signature to specific user-defined parameters
- ☐ Understanding ATOMIC.IP signature engine parameters

Functionality and solution verification

- ☐ This question is divided into two parts. The first is signature tuning, which requires modifying parameters to the existing signatures that are already populated on the sensor. The second is defining a new custom signature based on user-defined parameters to match a specific attack or application.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any one incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

As mentioned, the question can be attempted in two parts.

The first part is straightforward, requiring tuning of the existing ICMP signatures (Sig# 2000 for echo-request and Sig# 2004 for echo-reply), as per the information in the table.

The following output verifies that all requirements are met:

```
IPS# show configuration
<snip>
! ------------------------------
service signature-definition sig0
signatures 2000 0
alert-severity medium
engine atomic-ip
```

 Please see page 474 for more details.

```
event-action produce-alert
exit
status
enabled true
exit
exit
signatures 2004 0
alert-severity medium
engine atomic-ip
event-action produce-alert
exit
status
enabled true
exit
exit
<snip>
```

TIP
If the question provides a specific signature name and number, it must be used exactly, or you will lose points.

The second parts defines a custom signature, as per the information in the table.

Ensure that the custom signature for this ICMP traffic is using the atomic-ip engine, checking the IP payload length range between 5000 and 6000 bytes, and ensuring that it triggers only when sending packets to the RFC 1918 address range. All these parameters are configurable under the atomic-ip signature engine subcommand.

The following output verifies that all requirements are met:

```
IPS# show configuration
<snip>
! ------------------------------
service signature-definition sig0
<snip>
signatures 65000 0
```

```
sig-description
sig-name Large ICMP attack
exit
engine atomic-ip
event-action produce-alert
specify-l4-protocol yes
l4-protocol icmp
exit
exit
specify-ip-payload-length yes
ip-payload-length 5000-6000
exit
specify-ip-addr-options yes
ip-addr-options rfc-1918-address
exit
exit
exit
exit
<snip>
```

Now verify that the signature is triggered when sending the large ICMP packets to the RFC 1918 address range, as shown in the verification outputs. The output is also captured from the sensor console, which shows the signature triggered.

You will see three signatures being triggered with this ping test: the custom Sig ID 65000, plus the two regular Sig ID 2000 and 2004 that were enabled earlier, because the ping packet matches all three signature parameters:

```
R4# ping 10.8.8.8 size 5500
Type escape sequence to abort.
Sending 5, 5500-byte ICMP Echos to 10.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms
```

NOTE
Sometimes the custom signatures cannot be verified because there is no live traffic to run through the sensor to trigger the alerts. However, on other occasions, like this task, you can verify the custom signature.

```
R4#

IPS# show events alert medium
<snip>
evIdsAlert: eventId=1243792144740119961 severity=medium vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 380
  time: 2009/08/11 12:01:06 2009/08/11 12:01:06 UTC
  signature: description=Large ICMP attack id=65000 version=custom
    subsigId: 0
    sigDetails: My Sig Info
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.168.45.4
    target:
      addr: locality=OUT 10.8.8.8
      os: idSource=unknown relevance=relevant type=unknown
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 66
  threatRatingValue: 66
  interface: ge0_1
  protocol: icmp
<snip>
```

 Please see page 474 for more details.

Question 4.2: Configuring Cisco IOS IPS (4 points)

Configure Cisco IOS IPS version 5.0 format signature on R1, meeting both of the following requirements:

- Configure R1 for inline intrusion prevention sensor, monitoring packets as they flow through R1.
- Use the information in Table 2-41 to complete this task.

TABLE 2-41 Cisco IOS IPS configuration information

Signature Category Policy	☐ Generate an RSA crypto key and load the Cisco public signature on your router for signature decryption (given below). ☐ Retire all category signatures except IOS_IPS basic category.
IPS Configuration Policy	☐ Config location = flash:ips5/ ☐ IOS IPS name = myIOSipsV5 ☐ Enable SDEE protocol for event notification. ☐ Apply IOS IPS in both directions to GigabitEthernet0/0.
Loading Signature Package File	☐ Load the Cisco IOS IPS file IOS-S416-CLI.pkg from TFTP server 192.168.2.14 onto IDCONF.

Note

Generate an RSA crypto key, and load the Cisco public key signature on your router for signature decryption. You can copy and paste this directly into your router configuration:

```
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
  key-string
   30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
   00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
   17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
   B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
   5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
   FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
```

 Please see page 474 for more details.

```
  50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
  006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
  2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
  F3020301 0001
quit
exit
exit
```

NOTE
Download the latest Cisco IOS IPS files to your TFTP server from http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup. This Practice Lab uses IOS-S416-CLI.pkg; however, but you can use another file.

NOTE
Beginning with Cisco IOS Release 12.4(11)T, Cisco IOS IPS v4.0 format signatures are replaced by the v5.0 format signatures that are used by all other Cisco IPS devices. CCIE candidates must prepare Cisco IOS IPS using v5.0 format. To check whether your router is using v4.0 or v5.0 format, use the **show subsys name ips** command. In this output, version 2.*xxx*.*xxx* indicates that the router supports IPS 4.0 format, and version 3.*xxx*.*xxx* indicates that the router supports IPS 5.0 format.

Skills tested

- ☐ Configuring Cisco IOS IPS version 5.0 format signatures in inline mode
- ☐ Understanding the new Cisco IOS IPS version 5.0 format signatures
- ☐ Understanding the prerequisites and how to load the signature package file onto the router

Functionality and solution verification

- ☐ The objective of this question is to configure Cisco IOS IPS version 5.0 format signatures in inline mode.
- ☐ Cisco IOS IPS v5.*x* is a new format that has some changes to the file structure, signature format, and loading signature files onto the router. Carefully review the following steps on how to configure the new Cisco IOS IPS and understand the prerequisites.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

The following summarizes the configuration steps and ensures that prerequisites are met before you can implement Cisco IOS IPS.

Use the following detailed steps with sample outputs to understand and verify your Cisco IOS IPS configuration on R1:

 Please see page 474 for more details.

1. Download the latest Cisco IOS IPS signature package file to your TFTP server from the following URL (you need your Cisco userid and password to access this URL): http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup. This Practice Lab uses IOS-S416-CLI.pkg, but you can use another file.
2. You must have one of the following Cisco IOS software on your router to implement Cisco IOS IPS version 5.*x* format signature: adventerprisek9, advsecurityk9, or advipservicesk9. You can verify this using the **show version** or **show flash** command:

```
R1# show version
Cisco IOS Software, 3800 Software (C3825-ADVENTERPRISEK9-M), Version 12.4(22)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 10-Oct-08 06:43 by prod_rel_team
ROM: System Bootstrap, Version 12.3(11r)T2, RELEASE SOFTWARE (fc1)
R1 uptime is 2 days, 55 minutes
System returned to ROM by reload at 07:45:02 UTC Tue Aug 11 2009
System image file is "flash:c3825-adventerprisek9-mz.124-22.T.bin"
```

3. Generate an RSA crypto key, and load the Cisco public signature on your router for signature decryption (just given). You can also download the public key configuration from the URL mentioned in Step 1.

```
R1# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# crypto key pubkey-chain rsa
R1(config-pubkey-chain)# named-key realm-cisco.pub signature
Translating "realm-cisco.pub"
R1(config-pubkey-key)# key-string
Enter a public key as a hexidecimal number ....

R1(config-pubkey)# 30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
R1(config-pubkey)# 00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
R1(config-pubkey)# 17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
R1(config-pubkey)# B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
```

 Please see page 474 for more details.

```
R1(config-pubkey)# 5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
R1(config-pubkey)# FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
R1(config-pubkey)# 50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
R1(config-pubkey)# 006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
R1(config-pubkey)# 2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
R1(config-pubkey)# F3020301 0001
R1(config-pubkey)# quit
R1(config-pubkey-key)# exit
R1(config-pubkey-chain)# exit
R1(config)# exit
R1#
```

4. Router memory and resource constraints prevent a router from loading all Cisco IOS IPS signatures. Thus, it is recommended that you load only a selected set of signatures that are defined by the categories. Retire and/or unretire signature categories as mentioned in the information table requirement. Retired signatures are not scanned by Cisco IOS IPS, so they do not fire alarms.

```
R1# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip ips signature-category
R1(config-ips-category)# category all
R1(config-ips-category-action)# retired true
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# exit
R1(config-ips-category)# exit
Do you want to accept these changes? [confirm]
R1(config)# exit
R1#
*Aug 11 16:22:58.549: Applying Category configuration to signatures ...
R1#
```

5. After you have configured the basic IOS IPS category, you can start configuring the Cisco IOS IPS parameters on your router, such as creating a directory for which Cisco IOS IPS will save signature information, defining the location where Cisco IOS IPS will save the signature information, enabling SDEE protocol for event notification, and creating the IPS rule/name:

```
R1# mkdir ips5
Create directory filename [ips5]?
Created dir flash:ips5
R1#
R1# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip ips config location flash:ips5 retries 1
R1(config)# ip ips notify SDEE
R1(config)# ip ips name myIOSipsV5
```

6. Apply the Cisco IOS IPS rule/name at an interface, which automatically loads the signatures and builds the signature engines. The question requires configuring it on GigabitEthernet0/0 in both directions for traffic flowing through the router. Verify the final configuration output using the **show ip ips configuration** command:

```
R1# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface GigabitEthernet0/0
R1(config-if)# ip ips myIOSipsV5 in
R1(config-if)# ip ips myIOSipsV5 out

R1# show ip ips configuration
IPS Signature File Configuration Status
    Configured Config Locations: flash:ips5/
    Last signature default load time: 16:29:06 UTC Aug 11 2009
    Last signature delta load time: -none-
    Last event action (SEAP) load time: -none-
```

 Please see page 474 for more details.

```
    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 301
    Total Inactive Signatures: 2761

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name myIOSipsV5
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Interface Configuration
      Interface GigabitEthernet0/0
        Inbound IPS rule is myIOSipsV5
        Outgoing IPS rule is myIOSipsV5

IPS Category CLI Configuration:
    Category all:
        Retire: True
    Category ios_ips basic:
        Retire: False
```

7. Prepare to load the Signature package file to your router from the TFTP server, downloaded in Step 1. Note that you must complete the Cisco IOS IPS configuration and all other previous steps before loading this file. After the package file is loaded, all signature information is saved to the location specified via the **ip ips config location** command. You can verify that the signature is loaded using the **show ip ips signature count** command:

```
R1# copy tftp://192.168.2.14/IOS-S416-CLI.pkg idconf
Loading IOS-S416-CLI.pkg from 192.168.2.14 (via GigabitEthernet0/1): !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 9553609 bytes]
*Aug 11 16:28:59.525: %IPS-6-ENGINE_BUILDS_STARTED:  16:28:59 UTC Aug 11 2009
*Aug 11 16:28:59.525: %IPS-6-ENGINE_BUILDING: multi-string - 17 signatures - 1 of 13 engines
*Aug 11 16:28:59.557: %IPS-6-ENGINE_READY: multi-string - build time 32 ms - packets for this engine will be
scanned
*Aug 11 16:28:59.565: %IPS-6-ENGINE_BUILDING: service-http - 721 signatures - 2 of 13 engines
*Aug 11 16:29:00.657: %IPS-6-ENGINE_READY: service-http - build time 1092 ms - packets for this engine will be
scanned
*Aug 11 16:29:00.685: %IPS-6-ENGINE_BUILDING: string-tcp - 1658 signatures - 3 of 13 engines
*Aug 11 16:29:05.189: %IPS-6-ENGINE_READY: string-tcp - build time 4504 ms - packets for this engine will be
scanned
*Aug 11 16:29:05.193: %IPS-6-ENGINE_BUILDING: string-udp - 78 signatures - 4 of 13 engines
*Aug 11 16:29:05.249: %IPS-6-ENGINE_READY: string-udp - build time 56 ms - packets for this engine will be
scanned
*Aug 11 16:29:05.253: %IPS-6-ENGINE_BUILDING: state - 34 signatures - 5 of 13 engines
*Aug 11 16:29:05.349: %IPS-6-ENGINE_READY: state - build time 96 ms - packets for this engine will be scanned
*Aug 11 16:29:05.369: %IPS-6-ENGINE_BUILDING: atomic-ip - 342 signatures - 6 of 13 engines
*Aug 11 16:29:05.781: %IPS-6-ENGINE_READY: atomic-ip - build time 412 ms - packets for this engine will be
scanned
*Aug 11 16:29:05.793: %IPS-6-ENGINE_BUILDING: string-icmp - 3 signatures - 7 of 13 engines
*Aug 11 16:29:05.793: %IPS-6-ENGINE_READY: string-icmp - build time 0 ms - packets for this engine will be
scanned
*Aug 11 16:29:05.793: %IPS-6-ENGINE_BUILDING: service-ftp - 3 signatures - 8 of 13 engines
*Aug 11 16:29:06.225: %IPS-6-ENGINE_READY: service-smb-advanced - build time 320 ms - packets for this engine
will be scanned
```

```
*Aug 11 16:29:06.225: %IPS-6-ENGINE_BUILDING: service-msrpc - 33 signatures - 13 of 13 engines
*Aug 11 16:29:06.345: %IPS-6-ENGINE_READY: service-msrpc - build time 120 ms - packets for this engine will be
scanned
*Aug 11 16:29:06.345: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 6820 ms
R1#

R1# show ip ips signature count
Cisco SDF release version S416.0
Trend SDF release version V0.0

Signature Micro-Engine: multi-string: Total Signatures 17
      multi-string enabled signatures: 13
      multi-string retired signatures: 13
      multi-string compiled signatures: 4

Signature Micro-Engine: service-http: Total Signatures 721
      service-http enabled signatures: 145
      service-http retired signatures: 665
      service-http compiled signatures: 56
      service-http obsoleted signatures: 2

Signature Micro-Engine: string-tcp: Total Signatures 1658
      string-tcp enabled signatures: 650
      string-tcp retired signatures: 1531
      string-tcp compiled signatures: 127
      string-tcp obsoleted signatures: 22

Signature Micro-Engine: string-udp: Total Signatures 78
      string-udp enabled signatures: 2
      string-udp retired signatures: 72
```

```
      string-udp compiled signatures: 6
      string-udp obsoleted signatures: 1

Signature Micro-Engine: state: Total Signatures 34
      state enabled signatures: 17
      state retired signatures: 23
      state compiled signatures: 11

Signature Micro-Engine: atomic-ip: Total Signatures 342
      atomic-ip enabled signatures: 90
      atomic-ip retired signatures: 321
      atomic-ip compiled signatures: 21

Signature Micro-Engine: string-icmp: Total Signatures 3
      string-icmp enabled signatures: 0
      string-icmp retired signatures: 3

Signature Micro-Engine: service-ftp: Total Signatures 3
      service-ftp enabled signatures: 1
      service-ftp retired signatures: 2
      service-ftp compiled signatures: 1

Signature Micro-Engine: service-rpc: Total Signatures 76
      service-rpc enabled signatures: 44
      service-rpc retired signatures: 52
      service-rpc compiled signatures: 24

Signature Micro-Engine: service-dns: Total Signatures 39
      service-dns enabled signatures: 27
      service-dns retired signatures: 16
```

```
      service-dns compiled signatures: 23
      service-dns obsoleted signatures: 1

Signature Micro-Engine: normalizer: Total Signatures 9
      normalizer enabled signatures: 8
      normalizer retired signatures: 1
      normalizer compiled signatures: 8

Signature Micro-Engine: service-smb-advanced: Total Signatures 49
      service-smb-advanced enabled signatures: 42
      service-smb-advanced retired signatures: 34
      service-smb-advanced compiled signatures: 15

Signature Micro-Engine: service-msrpc: Total Signatures 33
      service-msrpc enabled signatures: 22
      service-msrpc retired signatures: 28
      service-msrpc compiled signatures: 5
      service-msrpc obsoleted signatures: 1

Total Signatures: 3062
   Total Enabled Signatures: 1061
   Total Retired Signatures: 2761
   Total Compiled Signatures: 301
   Total Obsoleted Signatures: 27
R1#

R1# show ip sdee all
Configured concurrent subscriptions: 1
No currently open subscriptions.
Alert storage:   200 alerts using 96000 bytes of memory
```

```
Message storage: 200 messages using 84800 bytes of memory
                                        SDEE Events
      Time                         Type    Description
   1: 16:25:52 UTC Aug 11 2009  STATUS  ENGINE_BUILDS_STARTED:  16:25:52 UTC Aug 11 2009
   2: 16:25:52 UTC Aug 11 2009  STATUS  ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
   3: 16:25:52 UTC Aug 11 2009  STATUS  ENGINE_READY: atomic-ip - build time 4 ms - packets for this engine
will be scanned
   4: 16:25:52 UTC Aug 11 2009  STATUS  ALL_ENGINE_BUILDS_COMPLETE: elapsed time 4 ms
   5: 16:28:59 UTC Aug 11 2009  STATUS  ENGINE_BUILDS_STARTED:  16:28:59 UTC Aug 11 2009
   6: 16:28:59 UTC Aug 11 2009  STATUS  ENGINE_BUILDING: multi-string - 17 signatures - 1 of 13 engines
   7: 16:28:59 UTC Aug 11 2009  STATUS  ENGINE_READY: multi-string - build time 32 ms - packets for this
engine will be scanned
   8: 16:28:59 UTC Aug 11 2009  STATUS  ENGINE_BUILDING: service-http - 721 signatures - 2 of 13 engines
   9: 16:29:00 UTC Aug 11 2009  STATUS  ENGINE_READY: service-http - build time 1092 ms - packets for this
engine will be scanned
  10: 16:29:00 UTC Aug 11 2009  STATUS  ENGINE_BUILDING: string-tcp - 1658 signatures - 3 of 13 engines
  11: 16:29:05 UTC Aug 11 2009  STATUS  ENGINE_READY: string-tcp - build time 4504 ms - packets for this
engine will be scanned
  12: 16:29:05 UTC Aug 11 2009  STATUS  ENGINE_BUILDING: string-udp - 78 signatures - 4 of 13 engines
  13: 16:29:05 UTC Aug 11 2009  STATUS  ENGINE_READY: string-udp - build time 56 ms - packets for this engine
will be scanned
  14: 16:29:05 UTC Aug 11 2009  STATUS  ENGINE_BUILDING: state - 34 signatures - 5 of 13 engines
  15: 16:29:05 UTC Aug 11 2009  STATUS  ENGINE_READY: state - build time 96 ms - packets for this engine will
be scanned
  16: 16:29:05 UTC Aug 11 2009  STATUS  ENGINE_BUILDING: atomic-ip - 342 signatures - 6 of 13 engines
  17: 16:29:05 UTC Aug 11 2009  STATUS  ENGINE_READY: atomic-ip - build time 412 ms - packets for this engine
will be scanned
  18: 16:29:05 UTC Aug 11 2009  STATUS  ENGINE_BUILDING: string-icmp - 3 signatures - 7 of 13 engines
  19: 16:29:05 UTC Aug 11 2009  STATUS  ENGINE_READY: string-icmp - build time 0 ms - packets for this engine
will be scanned
  20: 16:29:05 UTC Aug 11 2009  STATUS  ENGINE_BUILDING: service-ftp - 3 signatures - 8 of 13 engines
```

```
  21: 16:29:05 UTC Aug 11 2009  STATUS  ENGINE_READY: service-ftp - build time 8 ms - packets for this engine
will be scanned
  22: 16:29:05 UTC Aug 11 2009  STATUS  ENGINE_BUILDING: service-rpc - 76 signatures - 9 of 13 engines
  23: 16:29:05 UTC Aug 11 2009  STATUS  ENGINE_READY: service-rpc - build time 80 ms - packets for this engine
will be scanned
  24: 16:29:05 UTC Aug 11 2009  STATUS  ENGINE_BUILDING: service-dns - 39 signatures - 10 of 13 engines
  25: 16:29:05 UTC Aug 11 2009  STATUS  ENGINE_READY: service-dns - build time 16 ms - packets for this engine
will be scanned
  26: 16:29:05 UTC Aug 11 2009  STATUS  ENGINE_BUILDING: normalizer - 9 signatures - 11 of 13 engines
  27: 16:29:05 UTC Aug 11 2009  STATUS  ENGINE_READY: normalizer - build time 0 ms - packets for this engine
will be scanned
  28: 16:29:05 UTC Aug 11 2009  STATUS  ENGINE_BUILDING: service-smb-advanced - 49 signatures - 12 of 13
engines
  29: 16:29:06 UTC Aug 11 2009  STATUS  ENGINE_READY: service-smb-advanced - build time 320 ms - packets for
this engine will be scanned
  30: 16:29:06 UTC Aug 11 2009  STATUS  ENGINE_BUILDING: service-msrpc - 33 signatures - 13 of 13 engines
  31: 16:29:06 UTC Aug 11 2009  STATUS  ENGINE_READY: service-msrpc - build time 120 ms - packets for this
engine will be scanned
  32: 16:29:06 UTC Aug 11 2009  STATUS  ALL_ENGINE_BUILDS_COMPLETE: elapsed time 6820 ms
R1#
```

As soon as this basic configuration is done, you can tune Cisco IOS IPS signature parameters on the basis of a signature ID (for an individual signature). Or you can tune signature parameters on the basis of a category (all signatures that are within a specified category). At present, this is not required in this task.

Section 5.0: Implement Identity Authentication (12 Points)

Question 5.1: Proxy authentication access control (4 points)

Configure proxy authentication and authorization-based access control on the ASA1/c1 context, meeting all the following requirements:

- Enable AAA solution on the ASA1/c1 context to authenticate and authorize Telnet traffic crossing the firewall.
- The ASA firewall should perform proxy authentication for specific Telnet traffic from host 10.5.5.5 (R5) to host 10.1.1.1 (R1) crossing the ASA1/c1 context. All other traffic should go uninterrupted.
- Complete this task using the information in Tables 2-42 and 2-43.

TABLE 2-42 AAA configuration information

AAA Configuration	☐ Configure AAA server parameters on the ASA1/c1 context. Ensure that you can ping the Cisco Secure ACS server. ☐ Use TACACS+ protocol ☐ AAA server tag = myACSserver ☐ AAA server IP address 192.168.2.14 using shared secret password “cisco” ☐ Configure the maximum number of failed attempts to 2 before the TACACS+ server is deemed unavailable. ☐ Enable AAA authentication and authorization using access lists to identify Telnet traffic from host 10.5.5.5 (R5) to host 10.1.1.1 (R1).

 Please see page 474 for more details.

TABLE 2-43 ACS configuration information

ACS Configuration	☐ Add the ASA/c1 context inside interface as the AAA client on Cisco Secure ACS server (192.168.2.14). ☐ Configure a new user with privilege 15 on Cisco Secure ACS server "user1" using password "cisco," and assign it to the Default group. ☐ Enable shell EXEC and other parameters necessary to complete authorization. Configure the user1 profile to download idle-timeout set to 5 minutes. ☐ Configure Shell Command Authorization set under the user1 setup explicitly. The profile should allow the Telnet traffic to host 10.1.1.1 (R1).

- Verify the Pass Reports on Cisco Secure ACS server to ensure that user1 is successfully authenticated.
- Ensure that the following output is achieved on the ASA1/c1 context upon successful authentication:

```
ASA1/c1# show uauth
                        Current    Most Seen
Authenticated Users       1          1
Authen In Progress        0          1
user 'user1' at 10.5.5.5, authorized to:
   port 10.1.1.1/telnet
   absolute   timeout: 0:05:00
   inactivity timeout: 0:05:00
ASA1/c1#
```

Skills tested

- ☐ Configuring AAA authentication on the Cisco ASA firewall using access lists
- ☐ Configuring Cisco Secure ACS server for NAS settings and user profiles
- ☐ Configuring advanced user profile settings on Cisco Secure ACS server to control network device access using per-user level Shell Command Authorization sets

Functionality and solution verification

- ☐ This question can be divided into two parts. The first enables AAA authentication and authorization parameters on the ASA1/c1 context. The second part is the configuration on Cisco Secure ACS server.
- ☐ The main objective of this question is to enable proxy authentication to enforce device access control between specific host-to-host Telnet traffic.
- ☐ Note that you need to open the ACL on the ASA1/c1 context to allow a Telnet session (TCP port 23) entering the outside interface from specific host 10.5.5.5 (R5) to destination 10.1.1.1 (R1). Because the question does not restrict or mention anything about this ACL, you can permit TCP port 23 from any source to any destination. However, as a best practice, I recommend that you write the best possible specific ACL to allow specific host-to-host traffic using Layer 3 and 4 information. Again, this is just a recommendation, not a requirement.
- ☐ The question clearly says to configure the Shell command authorization set explicitly under the user1 setup. Do not use the Shared Profile components for this task.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

Verify the AAA client configuration on the ASA1/c1 context to ensure that all conditions and restrictions are met. Use the following outputs to verify that AAA authentication and authorization are configured correctly, as per the question requirement on the ASA1/c1 context:

```
ASA1/c1# show run aaa-server
aaa-server myACSserver protocol tacacs+
 max-failed-attempts 2
aaa-server myACSserver (inside) host 192.168.2.14
 key cisco
```

 Please see page 474 for more details.

```
ASA1/c1# show run aaa
aaa authentication match telnet outside myACSserver
aaa authorization match telnet outside myACSserver

ASA1/c1# show run access-list telnet
access-list telnet extended permit tcp host 10.5.5.5 host 10.1.1.1 eq telnet

ASA1/c1# show run access-list 100
access-list 100 extended permit icmp any any
access-list 100 extended permit udp any any eq 848
access-list 100 extended permit udp any any eq isakmp
access-list 100 extended permit esp any any
access-list 100 extended permit tcp host 10.5.5.5 host 10.1.1.1 eq telnet
```

The Cisco ASA firewall software provides a very useful **test** command utility that can be used to verify protocol-level connectivity from the client device to the Cisco Secure ACS server. It validates if the client can establish connectivity with the server using TACACS+/RADIUS ports. The following output shows the **test** command utility to ensure that protocol connectivity to the server is good:

NOTE
You should use this **test** command utility before performing any Telnet connections shown next.

```
ASA1/c1# test aaa-server authentication myACSserver host 192.168.2.14 username user1 password cisco
INFO: Attempting Authentication test to IP address <192.168.2.14> (timeout: 12 seconds)
INFO: Authentication Successful
ASA1/c1#
```

Assuming that the Cisco Secure ACS server is configured correctly, perform the following validation by sending Telnet traffic across the firewall from R5 source Loopback0 to destination R1 Loopback0. In addition, check the **show uauth** command output to ensure that it matches the requirement in the question:

```
R5# telnet 10.1.1.1 /source-interface loopback 0
Trying 10.1.1.1 ... Open
Username: user1
```

 Please see page 474 for more details.

```
Password: cisco
User Access Verification
Password: cisco
R1>
R1> exit
[Connection to 10.1.1.1 closed by foreign host]
R5#

ASA1/c1# show uauth
                        Current    Most Seen
Authenticated Users       1          1
Authen In Progress        0          1
user 'user1' at 10.5.5.5, authorized to:
   port 10.1.1.1/telnet
   absolute   timeout: 0:05:00
   inactivity timeout: 0:05:00
ASA1/c1#
```

In addition to all these testing and verification steps, verify that the Cisco Secure ACS server was configured correctly.

The following figures illustrate outputs from the Cisco Secure ACS server that meet all the requirements.

Figure 2-5 shows the ASA1/c1 context IP address 192.168.4.10 configured as an AAA client using the TACACS+ authentication protocol.

Figure 2-6 shows the User1 setup profile with TACACS+ settings applied.

Figure 2-7 shows the User1 setup profile with the per-user-level shell command authorization set applied.

FIGURE 2-5
AAA client configuration

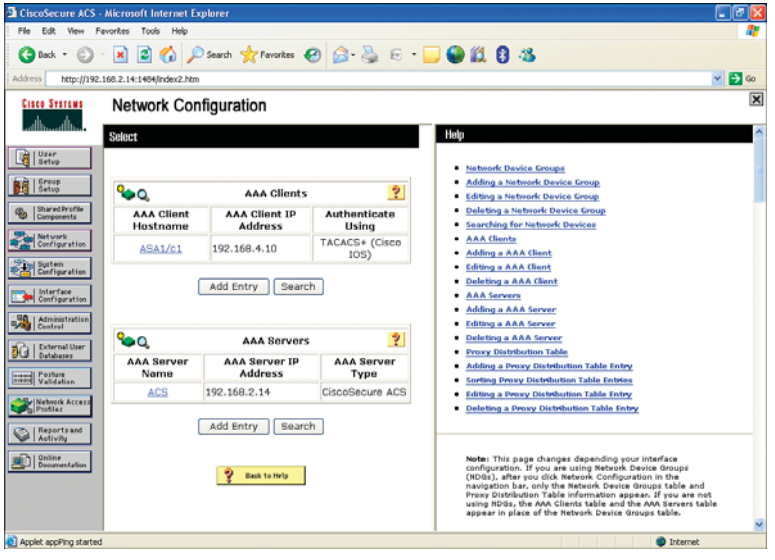
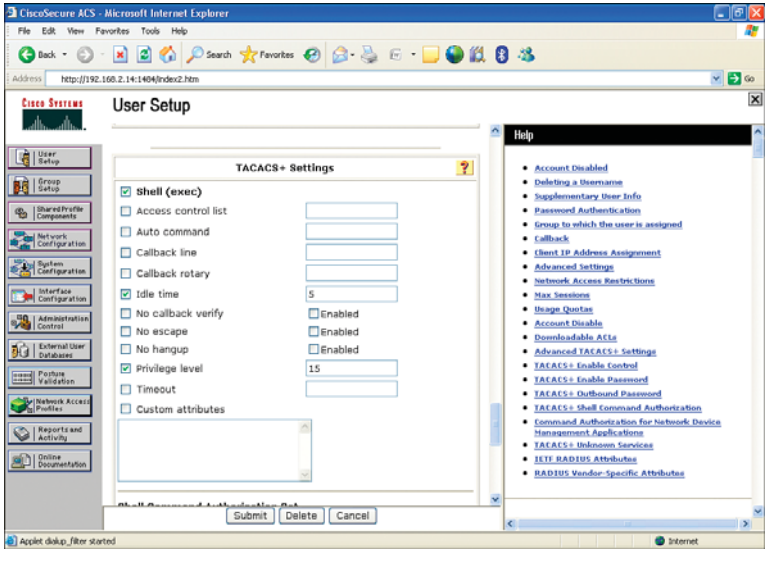
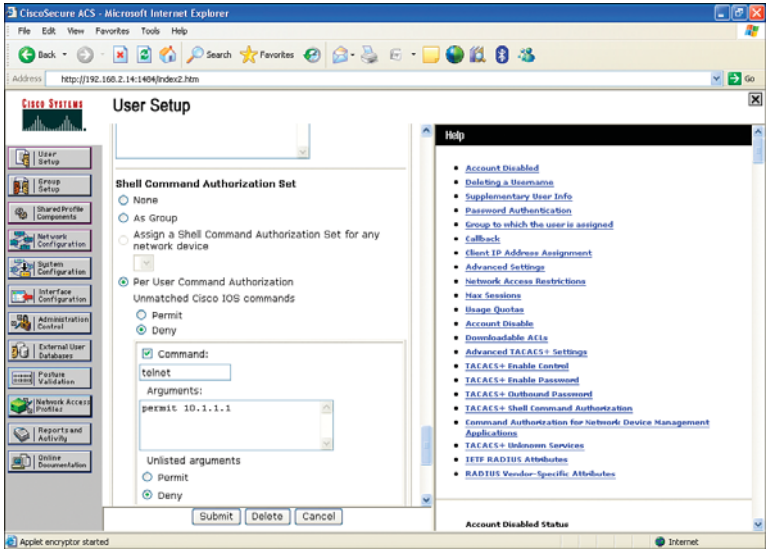


FIGURE 2-6
User1 profile configuration (TACACS+ settings)



 Please see page 474 for more details.

FIGURE 2-7
User1 profile configuration (shell command authorization set)



Question 5.2: Privilege level access control (4 points)

Configure AAA authentication and authorization on R5 and Cisco Secure ACS server, meeting all the following requirements:

- Enable AAA authentication and authorization on R5 using TACACS+ protocol.
- Configure Cisco Secure ACS user profiles using information in Tables 2-44 and 2-45.
- Verify functionality by establishing Telnet session to R5 from Sw2 and ensure that users get into Privilege level 5 and can execute only the restricted commands specified in the authorization set.
- Ensure that the console port is unaffected by this task.
- Use the information in the tables to complete this task.

TABLE 2-44 AAA configuration information

AAA Configuration	☐ Configure AAA server parameters on R5. Ensure that you can ping the Cisco Secure ACS server. ☐ Use TACACS+ protocol. ☐ AAA server IP address 192.168.2.14 using shared secret password "cisco." ☐ Enable AAA authentication using named method list. ☐ Enable AAA EXEC and command authorization using named method lists. ☐ Do not use a default method list in this task.

TABLE 2-45 ACS configuration information

NAS, User, and Group Setup Policies	☐ Add R5 Serial0/0/1 interface as the AAA client on Cisco Secure ACS server (192.168.2.14). ☐ Configure a new user with privilege level 5 called "netop" using password "cisco," and assign it to a group called "netop." ☐ Enable shell EXEC, privilege level, and other parameters necessary to complete authorization. ☐ Configure the netop group such that it allows network access on Sundays only (24 hour access).
Shell Command Authorization Policy	☐ Configure Shell Command Authorization set under the Shared Profile components called "netop." ☐ Users in this group should be able to configure any dynamic routing protocols. ☐ Users should also be able to apply any **interface** specific commands. ☐ Users in this group should be able to execute any **show** commands. ☐ Assign this set to netop group level.

- Verify the Pass Reports on Cisco Secure ACS server to ensure the netop user is successfully authenticated.
- Perform verification steps by establishing a Telnet session to R5 from Sw2 and ensure that it gets into privilege level 5 with the appropriate attributes.

Skills tested

☐ Configuring AAA configuration using named method lists

☐ Configuring Cisco Secure ACS server for NAS settings and user and group profiles

- Configuring Command Authorization sets using Shared Profile components
- Configuring advanced group level settings on Cisco Secure ACS server using TACACS+ attributes and time-based access control

Functionality and solution verification

- This question can be divided into two parts. The first part is to enable AAA authentication using a named method list on R5 and to apply it to VTY lines. (The console port should be explicitly configured for none authentication.) The second part is the configuration on Cisco Secure ACS server using the TACACS+ protocol to create the user and group, and assigning the command authorization set and time-based access settings.
- The main objective of this question is to enable per-group-level access restriction based on the privilege level and command authorization set. The question requires configuring a netop Shell command authorization set under the Shared profile and referencing it under the group setup. Additionally, the question also requires maintaining time-based restrictions, which can also be achieved under the group setup using Time-of-Day Access settings.
- The question clearly says not to use the default method list. Only a named method list is allowed, which is then applied explicitly to VTY lines.
- Also note that you need to open the ACL on the ASA1/c1 context to allow TACACS+ traffic (TCP port 49) entering the outside interface from source 192.168.65.5 (R5) to destination 192.168.2.14 (ACS). Because the question does not restrict or mention anything about this ACL, you can permit TCP port 49 from any source to any destination. However, as a best practice, I recommend that you write the best possible specific ACL to allow from specific source to specific destination on TCP port 49. Again, this is just a recommendation, not a requirement.
- You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

As mentioned, this question can be divided into two parts.

The first part is to enable AAA authentication using a named method list on R5 and applying it to VTY lines. Note that the question clearly says that the console port should be unaffected. Hence, an explicit named method list should be configured to exempt console authentication.

You also need to move the specified commands (commands set) into privilege level 5 on the router. If this isn't done, the router does not grant level 5 user access to these commands, because originally they belonged to privilege level 15. Hence, what you are doing is copying these commands into the privilege level 5 category on the router itself:

```
R5# show run ¦ section aaa
aaa authentication login myauthen group tacacs+
aaa authentication login noauthen none
aaa authorization exec myexecauthor group tacacs+
aaa authorization commands 5 mycommandauthor group tacacs+
aaa session-id common

R5# show run ¦ section tacacs-server
tacacs-server host 192.168.2.14 key cisco

R5# show run ¦ section privilege
privilege configure all level 5 router
privilege configure all level 5 interface
privilege exec level 5 configure terminal
privilege exec level 5 configure

R5# show run ¦ begin line con
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login authentication noauthen
<..>
line vty 0 4
```

 Please see page 474 for more details.

```
 exec-timeout 0 0
 password cisco
 authorization commands 5 mycommandauthor
 authorization exec myexecauthor
 logging synchronous
 login authentication myauthen
 transport input telnet
!
end
```

The second part of this task is configuring the Cisco Secure ACS server to create the users and groups. You also assign the command authorization set and time-based access control to the group level, as mentioned in the table.

By default, the Time-of-Day Access settings option under the Group setup is not visible. Figure 2-8 shows how to enable it from the Interface Configuration menu on Cisco Secure ACS server. Go to Advanced Options, select the checkbox for Default Time-of-Day / Day-of-Week Specification, and recheck the Group setup; it will appear now.

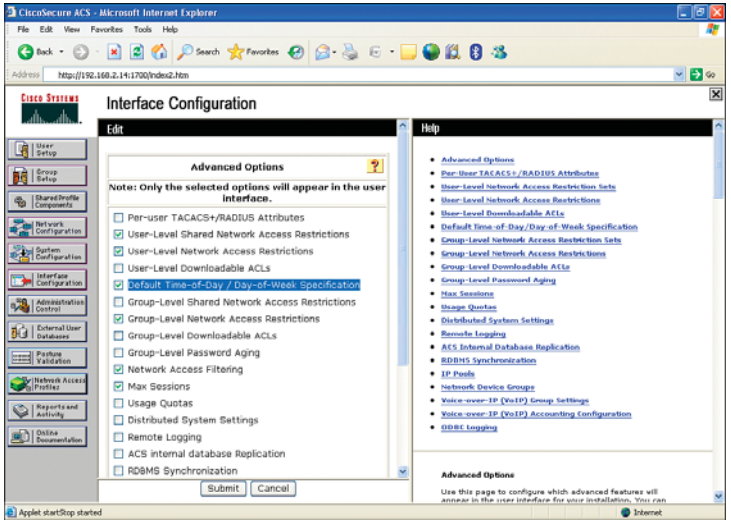


FIGURE 2-8
Enabling the Time-of-Day Access setting from the interface configuration

The following figures illustrate outputs from Cisco Secure ACS server that meet all the requirements.

Figure 2-9 shows R5 IP address 192.168.65.5 configured as an AAA client using the TACACS+ authentication protocol.

FIGURE 2-9
AAA client configuration

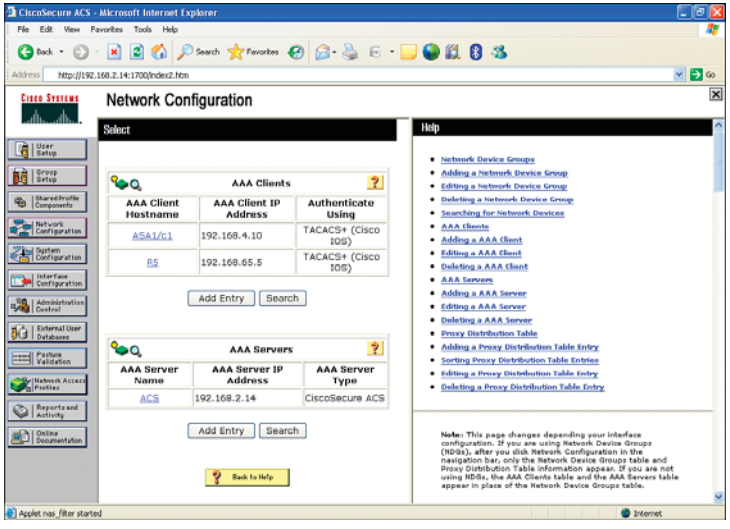


Figure 2-10 shows that user netop is assigned to group netop.

Figure 2-11 shows the Shell Command Authorization set configured under the Shared Profile components called netop.

Figure 2-12 shows group netop set up with "Time-of-Day Access Settings" allowing network access on Sundays only (24 hours).

Figure 2-13 shows group netop set up with TACACS+ attribute settings.

FIGURE 2-10
User netop in group netop

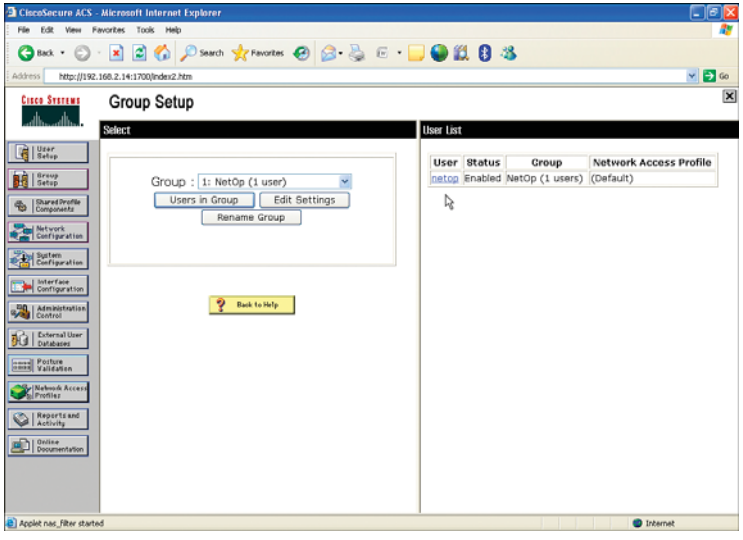


FIGURE 2-11
Shell Command Authorization set configuration

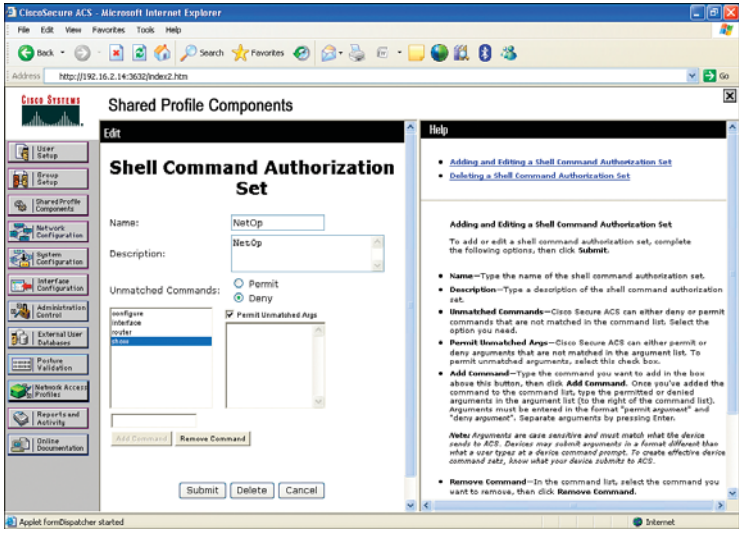


FIGURE 2-12
Group netop profile (Time-of-Day Access settings)

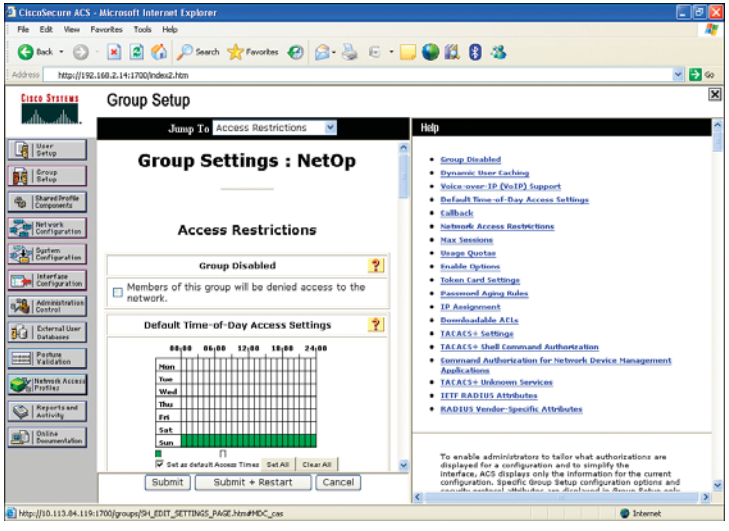
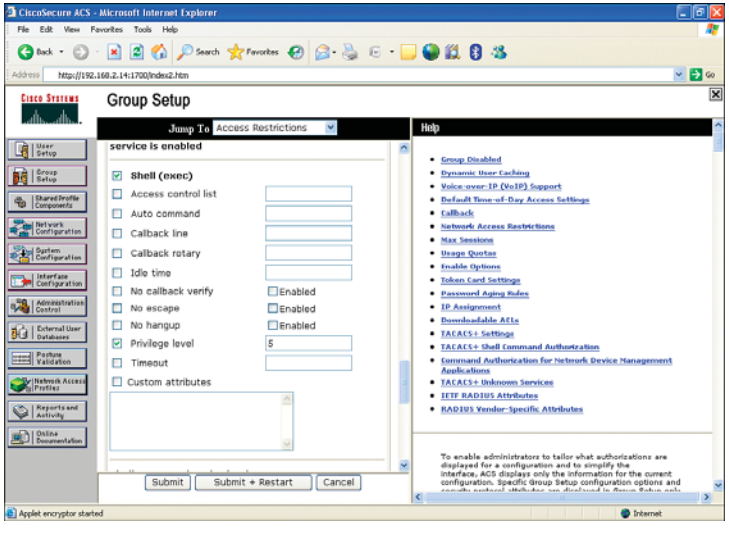


FIGURE 2-13
Group netop profile (TACACS+ settings)

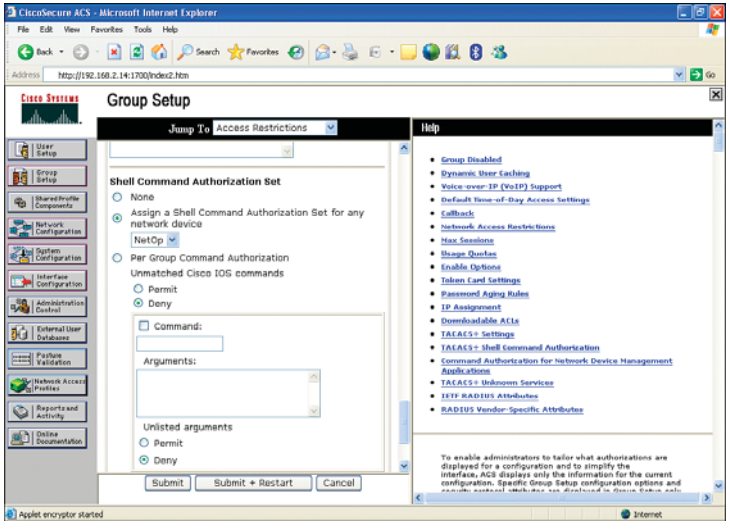


NOTE
The Shell (exec) check-box must also be selected to perform EXEC-level authorization, as shown in Figure 2-13.

 Please see page 474 for more details.

Figure 2-14 shows group netop set up with the Shell Command Authorization set applied.

FIGURE 2-14
Group netop profile (Shell Command Authorization set)



NOTE
You need to change the Clock time on the Cisco Secure ACS server to a Sunday for authentication to work due to the Time-of-Day Access restriction settings.

Finally, ensure that command authorization is working as per the requirement by establishing the following Telnet sessions to Sw2 to R5 and performing user authentication.

The following outputs verify user netop authentication. The output shows that, after being authenticated, the user is dynamically mapped to privilege 5 and can perform the commands in privilege 5 as per the information table. The ? illustrates the commands available in EXEC and configuration (config) modes:

```
Sw2# telnet 192.168.52.1
Trying 192.168.52.1 ... Open
Username: netop
Password: cisco
R5#

R5# show privilege
```

 Please see page 474 for more details.

```
Current privilege level is 5
R5#

R5# config term
Enter configuration commands, one per line.  End with CNTL/Z.
R5(config)#
R5(config)#?
Configure commands:
  beep       Configure BEEP (Blocks Extensible Exchange Protocol)
  call       Configure Call parameters
  default    Set a command to its defaults
  end        Exit from configure mode
  exit       Exit from configure mode
  help       Description of the interactive help system
  interface  Select an interface to configure
  license    Configure license features
  netconf    Configure NETCONF
  no         Negate a command or set its defaults
  oer        Optimized Exit Routing configuration submodes
  router     Enable a routing process
  sasl       Configure SASL

R5(config)# router ?
  bgp       Border Gateway Protocol (BGP)
  eigrp     Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis      ISO IS-IS
  iso-igrp  IGRP for OSI networks
  mobile    Mobile routes
  odr       On Demand stub Routes
  ospf      Open Shortest Path First (OSPF)
```

```
  rip       Routing Information Protocol (RIP)

R5(config)# interface ?
  Async               Async interface
  Auto-Template       Auto-Template interface
  BVI                 Bridge-Group Virtual Interface
  CDMA-Ix             CDMA Ix interface
  CTunnel             CTunnel interface
  Dialer              Dialer interface
  GigabitEthernet     GigabitEthernet IEEE 802.3z
  Group-Async         Async Group interface
  Lex                 Lex interface
  Loopback            Loopback interface
  MFR                 Multilink Frame Relay bundle interface
  Multilink           Multilink-group interface
  Null                Null interface
  Port-channel        Ethernet Channel of interfaces
  Serial              Serial
  Tunnel              Tunnel interface
  Vif                 PGM Multicast Host interface
  Virtual-Dot11Radio  Virtual dot11 interface
  Virtual-PPP         Virtual PPP interface
  Virtual-Template    Virtual Template interface
  Virtual-TokenRing   Virtual TokenRing
  range               interface range command
R5(config)# end
R5# exit
[Connection to 192.168.52.1 closed by foreign host]
Sw2#
```

Question 5.3: MAC-based authentication profile (4 points)

Configure MAC-Based authentication using Network Access Profile (NAP) on Cisco Secure ACS server, meeting all the following requirements:

- Your network is enabled with Network Admission Control (NAC) setup and some agentless hosts require authentication using ACS.
- Configure MAC authentication bypass (MAB) using NAP to authenticate the agentless client using the host's MAC address to identify and authenticate it.
- Use the information in Table 2-46 to complete this task.

TABLE 2-46 ACS configuration information

NAP Policy	☐ NAP policy name = MAC_bypass ☐ Use RADIUS IETF protocol ☐ Do not configure any posture validation
MAB Authentication Bypass Policy	☐ Allow MAC-Authentication-Bypass ☐ Use ACS internal database for MAB ☐ MAC address 00-11-22-9F-01-7E should be assigned to Group 5 ☐ MAC address 00-11-22-4A-2D-0F should be assigned to Group 6 ☐ All other unknown MAC addresses should be assigned to Default group

NOTE
For further information, review a whitepaper on implementing agentless support using the MAB feature: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/configuration/guide/noagent.html#wp1083361.

Skills tested

- ☐ Configuring MAC-based authentication using Network Access Profile (NAP) on the Cisco Secure ACS
- ☐ Understanding Agentless Host Support
- ☐ Enabling MAC authentication bypass (MAB) on Cisco Secure ACS server

Functionality and solution verification

- ☐ The objective of this question is straightforward, requiring enabling MAB on ACS using NAP.
- ☐ Because the question does not mention anything about the RADIUS (IETF) IP address, you can use any dummy IP address to define the AAA client.
- ☐ This question is one of the rare ones that cannot be practically verified, so the grading is configuration-based only. This task has no verification output as such, only the configuration shown from Cisco Secure ACS server.
- ☐ You will see ACS screen capture outputs to verify the requirement laid out in the question.

The following figures illustrate outputs from Cisco Secure ACS server that meet all the requirements.

Figure 2-15 shows NAP profile setup.

FIGURE 2-15
NAP profile setup

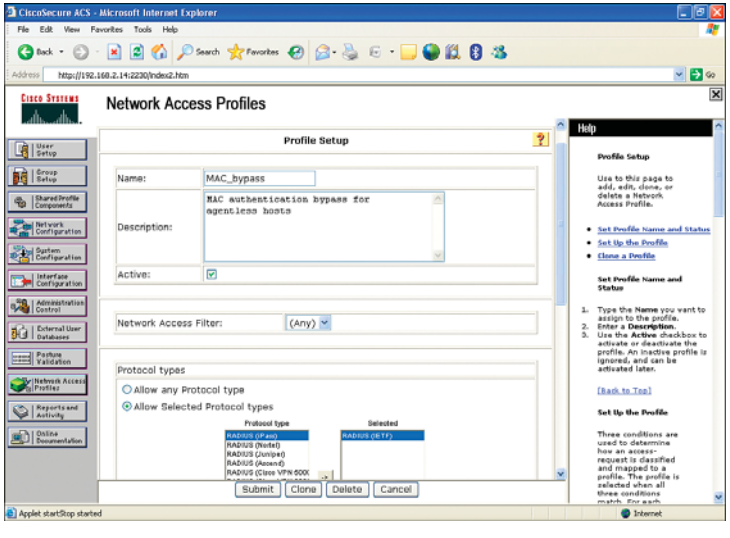
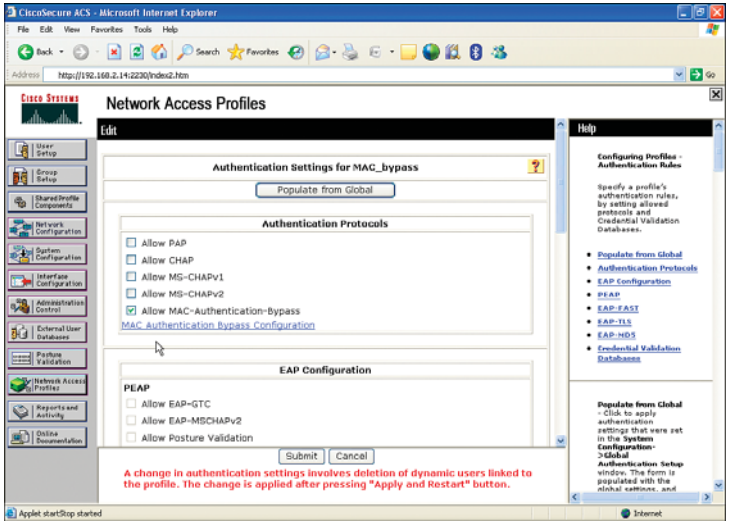


Figure 2-16 shows Authentication settings. On the Edit Network Access Profiles (NAP) page, click Authentication under the policies column.

FIGURE 2-16
Authentication setting



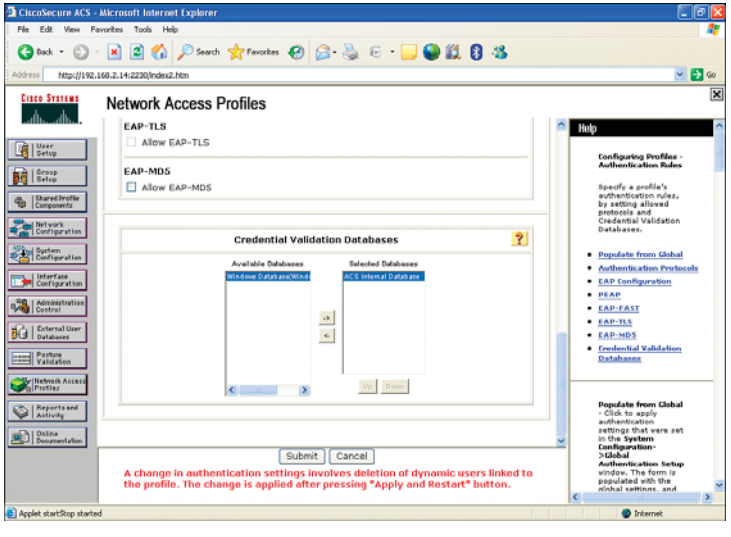
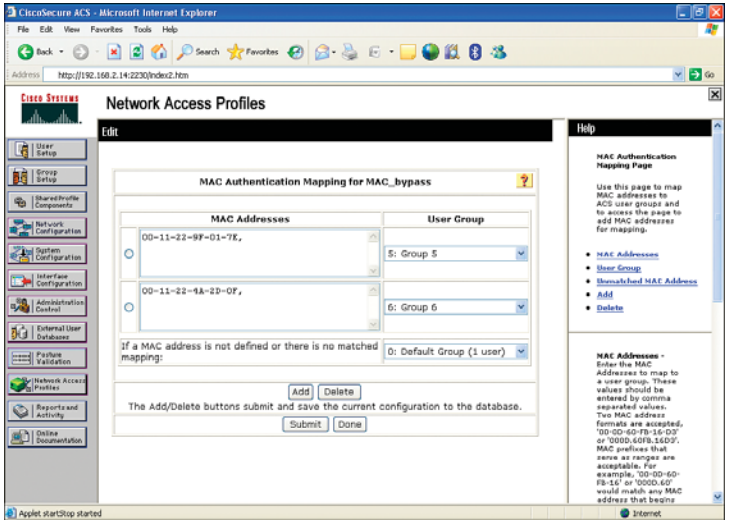


Figure 2-17 shows MAB configuration. This is done by selecting MAC Authentication Bypass Configuration from the earlier Authentication setting page.

FIGURE 2-17
MAB configuration



Section 6.0: Implement Control and Management Plane Security (13 Points)

Question 6.1: Control plane protection (4 points)

Configure control plane protection using CoPP on R3, meeting all the following requirements:

- Configure CoPP protection using a port-filter policy on R3 to drop all traffic destined to 'closed' or nonlistened TCP/UDP ports trying to access this router.
- Do not configure any parameters under the default class that matches any packet.
- You are allowed to configure only one class-map and one policy-map to complete this task.

Skills tested

- ☐ Configuring the Control Plane Policing (CoPP) host subinterface using the Modular QoS CLI (MQC) to define traffic classification criteria and to specify the policy actions for the classified traffic
- ☐ Configuring the new port-filter type class-map and policy-map
- ☐ Understanding CoPP features and capabilities
- ☐ Knowledge of the MQC configuration model

Functionality and solution verification

- ☐ This question seems very basic. However, an important requirement may add challenge initially in how you configure the class-map and policy-map in MQC to complete this task.
- ☐ The question requires configuring a port-filter type of class-map and policy-map. This new extension in the CoPP configuration is an enhanced feature to the control-plane host subinterface to block traffic destined to closed or nonlistened TCP/UDP ports. Note that you need to configure both class-map and policy-map using the same type to bind them.
- ☐ A **match closed-ports** option under this new port-filter type class-map classifies all traffic destined for the routers closed or nonlistened TCP/UDP ports.
- ☐ Then create a **port-filter** type of policy-map by referencing this class-map within, and enable the **drop** action. Defining this type of policy with a **drop** action supports early dropping of packets that are directed toward closed or nonlistened TCP/UDP ports trying to access this router.
- ☐ Finally, apply this policy-map to the **control-plane host** subinterface. The port-filter feature policy can only be attached on the control-plane host subinterface.
- ☐ The question says not to use a default class-map and permits only one class-map and one policy-map to complete this task.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

First, verify that the class-map and policy-map configured in this task are using the new **port-filter** type:

```
R3# show run ¦ section class-map
class-map type port-filter match-all myclassmap
 match  closed-ports

R3# show run ¦ section policy-map
policy-map type port-filter mypolicymap
 class myclassmap
   drop
R3#
```

Then, check that the CoPP configuration is applied to the host subinterface:

```
R3# show policy-map type port-filter control-plane host
 Control Plane Host

  Service-policy port-filter input: mypolicymap

    Class-map: myclassmap (match-all)
      2 packets, 120 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  closed-ports
      drop

    Class-map: class-default (match-any)
      51 packets, 3069 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

 Please see page 474 for more details.

Opened ports on the router can be viewed using the following command. Ports not listed in this output (called closed ports) are dropped using the CoPP configuration just shown. However, open ports (LISTEN) are allowed using the default class-map in this configuration:

```
R3# show control-plane host open-ports
Active internet connections (servers and established)
Prot              Local Address            Foreign Address                Service    State
 tcp                      *:22                      *:0               SSH-Server   LISTEN
 tcp                      *:23                      *:0                   Telnet   LISTEN
 tcp                      *:80                      *:0                HTTP CORE   LISTEN
 tcp                      *:80                      *:0                HTTP CORE   LISTEN
```

Question 6.2: Cisco IOS image and configuration protection (3 points)

Configure Cisco IOS image and configuration protection on R2, meeting the following requirements:

- R2 recently experienced a downtime due to a malicious intrusion. An intruder erased the IOS image and configuration from the router, causing extended downtime of services due to the delay in the recovery process.
- Configure R2 for resilient IOS image and configuration protection such that it maintains a secure copy of the router image and the configuration, hence withstanding any malicious attempts to erase the contents of persistent storage (NVRAM and flash). These secure files cannot be removed by the intruder.
- Do not use any ACL or Cisco IOS Firewall (CBAC or ZFW) configuration to complete this task.

Skills tested

- ☐ Configuring Cisco IOS Resilient Configuration on the router
- ☐ Understanding the consequences and procedures of an intrusion in the event of a router compromise and downtime

 Please see page 474 for more details.

Functionality and solution verification

- ☐ This question is very straightforward. There is not much complexity in this task.
- ☐ Configure the basic built-in Cisco IOS Resilient Configuration on R2 that protects the router IOS Image and configuration file by preserving these files in a secure location. Secured files will not be displayed when using the **dir** or **show flash** command, because the IFS prevents secure files in a directory from being listed. However, a user having physical access to the router can go into router ROM monitor (ROMMON) mode, which does not have any such restriction, and use ROMMON to list and boot secured files.
- ☐ Cisco IOS Resilient Configuration is intended to speed up the recovery process.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

The following outputs illustrate configuration and verification:

```
R2# show run ¦ section secure
secure boot-image
secure boot-config
R2#

R2# show secure bootset
IOS resilience router id FTX1036A0Q7

IOS image resilience version 12.4 activated at 12:04:13 UTC Thu Aug 13 2009
Secure archive flash:c3825-adventerprisek9-mz.124-22.T.bin type is image (elf) []
  file size is 60928072 bytes, run size is 61093716 bytes
  Runnable image, entry point 0x80010000, run from ram
```

 Please see page 474 for more details.

```
IOS configuration resilience version 12.4 activated at 12:04:25 UTC Thu Aug 13 2009
Secure archive flash:.runcfg-20090813-120425.ar type is config
configuration archive size 2481 bytes
R2#
```

Verify the restriction in the question not to use any ACL on interface FastEthernet 0/13:

```
Sw1# show ip interface FastEthernet 0/13 ¦ inc access list
  Outgoing access list is not set
  Inbound  access list is not set
```

Question 6.3: Router CPU protection (3 points)

Configure router CPU protection on R4, meeting all the following requirements:

- When a packet is forwarded to R4 from Sw1 (directly connected default gateway) and the router has no path to the destination host, R4 generates a Destination Unreachable, Code 1 (Host Unreachable) ICMP message back to Sw1. This can potentially be a target of ICMP-based DoS attack affecting the router CPU.
- Configure R4 to stop generating ICMP Destination Unreachable (Type 3) messages.
- Do not configure any ACL to complete this task.
- Ensure that when Sw1 sends any packet to its default gateway R4 to an unknown destination, R4 should silently discard without replying back to Sw1.

Skills tested

- ☐ Configuring a basic ICMP technique, disabling the ICMP Destination Unreachable (Type 3 Code 1, Host Unreachable) message under the interface configuration
- ☐ Understanding ICMP message types
- ☐ Understanding ICMP-based attacks that impede router CPU

Functionality and solution verification

- ☐ This question is another simple and straightforward one. Because the question clearly says not to use an ACL, using CoPP or an interface ACL is ruled out. The only option left is to use the **no ip unreachables** command.
- ☐ The lab exam at times will have questions with very short answers (from a syntax perspective). However, the importance is choosing the right solution and technology in the given circumstance. This is the key in the security field, because choosing a wrong, incompatible, or inappropriate solution may cause a lot of grief and unnecessary downtime.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

The following outputs illustrate configuration and verification:

```
R4# show ip interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.41.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5 224.0.0.6
  Outgoing access list is not set
  Inbound  access list is 101
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
```

 Please see page 474 for more details.

```
  ICMP redirects are always sent
  ICMP unreachables are never sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: Access List, MCI Check
  Output features: Firewall (NAT), Firewall (inspect)
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  Outgoing inspection rule is mycbac

R4# show run interface GigabitEthernet 0/0
Building configuration...
Current configuration : 229 bytes
interface GigabitEthernet0/0
```

```
 ip address 192.168.41.1 255.255.255.0
 ip access-group 101 in
 no ip unreachables
 ip inspect mycbac out
 duplex auto
 speed auto
 media-type rj45
 crypto ipsec client ezvpn ezvpn_dvti inside
end
R4#
```

Another way to verify is by sending a ping from Sw1 (with its default gateway set to R4) to any unknown host, knowing that this packet will be sent to R4 using the default gateway.

Without the solution applied, if you enable **debug ip icmp** on Sw1 and send the pings, you will receive an ICMP host unreachable reply packet from R4:

```
Sw1# debug ip icmp
ICMP packet debugging is on
Sw1#
Sw1# ping 10.9.9.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.9.9.9, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
*Mar  9 03:45:20.604: ICMP: dst (192.168.41.2) host unreachable rcv from 192.168.41.1
*Mar  9 03:45:22.609: ICMP: dst (192.168.41.2) host unreachable rcv from 192.168.41.1
*Mar  9 03:45:24.614: ICMP: dst (192.168.41.2) host unreachable rcv from 192.168.41.1
Sw1#
```

 Please see page 474 for more details.

Question 6.4: Secure device access control (3 points)

Configure secure management access control on Sw2, meeting all the following requirements:

- Configure Sw2 to allow management access using SSH protocol only.
- Use local username cisco with password cisco for SSH connections.
- Tune the SSH timeout to 5 seconds and 2 authentication retries.
- Ensure that you can SSH from any device in your network to Sw2 using the SSH protocol.

Skills tested

- ☐ Configuring device management to protect access control using secure SSH protocol
- ☐ Understanding how SSH works and implementation prerequisites

Functionality and solution verification

- ☐ The objective of this question is to configure SSH server-based device access control on a Cisco Catalyst Switch.
- ☐ Before you can configure SSH, ensure that your router has an IPsec (DES or 3DES) encryption software image.
- ☐ SSH requires RSA keys. Generates RSA keys on Sw2 that will automatically enable the SSH server on the switch, and tune the parameters as per the requirement.
- ☐ Configure a local username “cisco” with password “cisco.”
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

The following outputs illustrate configuration and verification that meet all the requirements.

 Please see page 474 for more details.

Ensure that you change two things under the line vty on Sw2. First, change the transport input from Telnet to SSH to explicitly permit SSH-based connections and to drop Telnet-based connections. Second, enable login local to trigger user-based authentication.

Remember, the switch has VTY lines 0 through 15, and you need to apply the solution to the entire switch. Applying your solution on VTY lines 0 through 4 only will not suffice, and you will lose points.

```
Sw2# show run ¦ include ssh
ip ssh time-out 5
ip ssh authentication-retries 2
ip ssh version 1
 transport input ssh
Sw2#

Sw2# show run ¦ include username
username cisco privilege 15 password 0 cisco

Sw2# show run ¦ begin line vty
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 exec-timeout 0 0
 password cisco
 logging synchronous
 login local
 transport input ssh
!
end
Sw2#
```

After this is enabled, verify SSH by establishing a session from R5. As you can see, you can get valuable information without actually connecting or consoling to router R5:

```
R5# ssh -l cisco 192.168.52.2
Password: cisco
Sw2#

Sw2# show ssh
Connection      Version Encryption      State                   Username
0               1.5     3DES            Session started         cisco
%No SSHv2 server connections running.
Sw2#
Sw2# exit
[Connection to 192.168.52.2 closed by foreign host]
R5#
```

Also verify that Telnet-based connections to Sw2 are denied:

```
R5# telnet 192.168.52.2
Trying 192.168.52.2 ...
% Connection refused by remote host
```

Section 7.0: Advanced Security (12 Points)

Question 7.1: MAC flooding protection (3 points)

Configure MAC flooding protection on Sw2, meeting both of the following requirements:

- Configure MAC flooding protection and prevention of CAM table (Content Addressable Memory) attacks on Sw2 using information in Table 2-47.
- You are allowed to add new VLANs to complete this task.

 Please see page 474 for more details.

TABLE 2-47 Switch configuration information

MAC Flooding Protection Policy	☐ Configure Sw2 interface FastEthernet0/20 using the following parameters: ☐ Assign Data VLAN = 101 ☐ Assign Voice VLAN = 102 ☐ Ensure that the interface is allowed to learn a maximum of ten dynamic MAC addresses of which maximum of eight addresses can be from Data VLAN and two addresses can be from Voice VLAN. ☐ Ensure that all dynamically learned MAC addresses are added to the running configuration. After you save the Sw2 configuration, if the switch is rebooted for any reason, the interface does not need to relearn these addresses. ☐ When the number of secure MAC addresses reaches the maximum limit, packets with unknown source addresses should be dropped, and the security violation counter should increment. ☐ Do not configure the port to shut down.

Skills tested

- ☐ Configuring Port-Security on a Cisco Catalyst Switch
- ☐ Understanding MAC flooding and CAM table attacks and their mitigation techniques
- ☐ Knowledge of Layer 2 and MAC addresses

Functionality and solution verification

- ☐ The objective of this question is to configure a proactive solution to prevent MAC flooding and CAM table overflow-type attacks.
- ☐ A Cisco Catalyst switch provides a security feature that is most appropriate to complete this task—Port Security.
- ☐ The question specifies several requirements and port-security parameters that can be achieved using the Port-Security feature.
- ☐ You are allowed to add the two new VLAN numbers 101 and 102 to complete this task.

- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

The following outputs illustrate configuration and verification that meet all the requirements:

```
Sw2# show run interface FastEthernet 0/20
Building configuration...
Current configuration : 385 bytes
!
interface FastEthernet0/20
 switchport access vlan 101
 switchport mode access
 switchport voice vlan 102
 switchport port-security maximum 10
 switchport port-security maximum 8 vlan access
 switchport port-security maximum 2 vlan voice
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 spanning-tree portfast
end
```

You can also use the **show port-security** command to validate the policy configuration and ensure that port security is enabled as per the requirement.

The following sample output shows port-security enabled with violation mode on Sw2 interface Fa0/20:

TIP

Ensure that you enable the Sw2 Fa0/20 port as an access port (static). Port-security can only be configured on static access ports or trunk ports. A secure port cannot be a dynamic access port.

```
Sw2# show port-security interface FastEthernet 0/20
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 10
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Table 2-48 summarizes the varying violation modes and the actions taken when the switch port is configured with port-security.

TABLE 2-48 Switch port security violation modes and actions

Violation Mode	Is Traffic Forwarded?	Sends SNMP Trap?	Sends Syslog Message?	Displays Error Message?	Violation Counter Increments?	Shuts Down Port?
Protect	No	No	No	No	No	No
Restrict	No	Yes	Yes	No	Yes	No
Shutdown	No	Yes	Yes	No	Yes	Yes
Shutdown vlan	No	Yes	Yes	No	Yes	No

Question 7.2: Troubleshooting NBAR (3 points)

Traffic filtering using Network-Based Application Recognition (NBAR) has been preconfigured on R2 and R6 in this question. Your task is to troubleshoot and identify the injected faults and ensure that legitimate traffic is forwarded, meeting all the following requirements:

- The Cisco IOS NBAR classification engine using MQC configuration has been preconfigured on routers R2 and R6.
- Four faults are injected into your preconfiguration.
- Open an ACL on the ASA1/c1 context, allowing Telnet traffic entering the outside interface (ACL 100) from any host to any destination. This excludes the four faults.
- Identify these faults, and verify that Telnet traffic using Frame Relay DLCI 65 path (such as traffic from R5/Sw2 to destination R2) with IP precedence bit set to 1 is dropped. All other Telnet traffic to R2 should be functional.
- While fixing this issue, you are allowed to alter the preconfiguration and add, modify, or remove part of the preconfiguration. However, you need to ensure that altering the preconfiguration does not impact any other question.
- Do not configure any parameters under the default class that matches any packet.
- Do not use an ACL to complete this task.
- Do not use CoPP to complete this task.
- For verification, ensure that the Telnet session from R4 to R2 (10.2.2.2) should be successful; however, the telnet from R5 to R2 (10.2.2.2) should fail.

NOTE

As mentioned on the CCIE lab exam blueprint, "Knowledge of troubleshooting is an important skill, and candidates are expected to diagnose and solve issues as part of the CCIE lab exam." The new v3.0 Lab exam strongly enforces this aspect. The new lab exam will be just as challenging and will validate both configuration and troubleshooting skills. Candidates must practice troubleshooting methods and techniques as an important skill set to be successful.

Skills tested

- ☐ Troubleshooting Cisco IOS NBAR and MQC technologies
- ☐ Understanding traffic classification using NBAR technology
- ☐ Identifying network-related issues within an existing topology that has been preconfigured

Functionality and solution verification

- ☐ As seen in the previous VPN section, this is another troubleshooting series question. These new format questions are different from the traditional configuration-based questions. The objective is to identify candidates' analytical skills in a complex environment where an engineer applies his or her troubleshooting skills to fix networking-related problems using a methodological approach with the aid of various tools. Extensive knowledge of **show** and **debug** commands is very important in these scenarios.
- ☐ A basic approach to solve this type of question is to break it into layers, such as basic IP connectivity, routing, switching, and any other network-related issues. As just mentioned, you should use a methodological approach. Also important is breaking the issue into smaller parts. For example, in this question you should check basic IP reachability without the NBAR and MQC features applied (on R2 and R6), thus ensuring that all routing and switching are working. When you're done, you can apply the NBAR and MQC features and start troubleshooting. Start by reviewing the current preconfiguration using **show** commands, but if you cannot find anything unusual, enable relevant **debugs** to get more details.
- ☐ The question states a few restrictions when completing this task. For example, you can't modify the default class-map, use an ACL, or use the control-plane (CoPP) feature. If you use any one of these, you will lose all points.
- ☐ The issues that were injected into the preconfiguration are discussed next.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

You can use several methods and varying techniques to start troubleshooting; there is no perfect method. Every person has different methodologies and uses a different approach. As long as the main objective is met, you can use your own method. However, earlier I described a basic approach and how to use it effectively.

Here is a list of four faults injected into your preconfiguration:

- Fault 1 can be found on R2. The **class-map** drop23 configured on R2 is using a Logical-OR (**match-any**) operation. The **class-map** has two **match** statements, and the Logical-OR will satisfy the classification engine if any single **match** statement is found in the arriving packet. Because you want to match Telnet traffic explicitly that is tagged with IP precedence 1, you must ensure that the **class-map** matches both the **match** statements using the Logical-AND (**match-all**) operation. To fix, remove the **class-map** and re-create it using the Logical-AND (**match-all**), with all other parameters remaining the same.
- Fault 2 can also be found on R2. The **service-policy** is applied on R2 GigabitEthernet0/1 in both directions. The requirement is to block inbound traffic to R2; therefore, the outbound policy is redundant, and you must remove it.
- Fault 3 can be found on R6. The **service-policy** is applied on R2 Serial0/0/0. However, it should be applied to Serial0/0/1, because the question requires marking and dropping traffic that uses the Frame Relay DLCI 65 path, which means any traffic coming into R2 from the DLCI 65 path. For example, traffic from R5 and Sw2 will use the DLCI 65 path. To fix this, remove the **service-policy** from R2 Serial0/0/0, and apply it to R2 Serial0/0/1 in the inbound direction.
- Fault 4 can also be found on R6. The **policy-map** on R6 has an incorrect IP precedence bit set to 2. The **policy-map** is supposed to mark all Telnet traffic arriving from the DLCI 65 path with an IP precedence set to 1. To fix this, modify the **policy-map** to set the IP precedence to 1.

After all four faults are found and fixed, perform the following Telnet sessions, and verify the functionality to meet the requirements.

Ensure that the Telnet session from R4 to R2 (10.2.2.2) is successful:

```
R4# telnet 10.2.2.2
Trying 10.2.2.2 ... Open
User Access Verification
Username: cisco
Password: cisco
R2> exit
[Connection to 10.2.2.2 closed by foreign host]
R4#
```

 Please see page 474 for more details.

However, the Telnet session from R5 to R2 (10.2.2.2) should fail:

```
R5# telnet 10.2.2.2
Trying 10.2.2.2 ...
% Connection timed out; remote host not responding
R5#

R2# show policy-map interface GigabitEthernet 0/1
 GigabitEthernet0/1

  Service-policy input: drop23

    Class-map: drop23 (match-all)
      4 packets, 240 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol telnet
      Match: ip dscp 1
      drop

    Class-map: class-default (match-any)
      650 packets, 119001 bytes
      5 minute offered rate 1000 bps, drop rate 0 bps
      Match: any
```

Question 7.3: Configuring ESMTP Server protection (3 points)

Configure advanced application layer protocol inspection on the Cisco ASA firewall to protect the ESMTP server, meeting the following requirement:

- Configure the ASA/c1 context to protect the ESMTP mail server, preventing malformed message attacks using information in Table 2-49.

 Please see page 474 for more details.

TABLE 2-49 ASA1/c1 context configuration information

ESMTP Inspection Policy	☐ Configure advanced ESMTP inspection to match and drop email connections from a specific sender email address joe@myemail.com. ☐ Additionally, drop email connections if the maximum number of email addresses in the To: field exceeds 5. ☐ Also drop email connections if any special characters are detected within the sender or receivers email address such as pipe (|), backquote (`), or null space, to name a few. ☐ Do not apply the policy to the inside or outside interface. The policy must be applied globally. ☐ Do not configure an ACL to complete this task.

Skills tested

- ☐ Configuring Application Layer Protocol inspection on the Cisco ASA firewall
- ☐ Knowledge of the Modular Policy Framework (MPF) configuration model on the Cisco ASA Firewall
- ☐ Understanding ESMTP protocol attacks
- ☐ Knowledge of the ESMTP inspection engine to mitigate attacks, including spam, phishing, malformed message attacks, and buffer overflow/underflow attacks

Functionality and solution verification

- ☐ You can use several techniques to combat ESMTP attacks. This question requires configuring the advanced application layer inspection technique on the Cisco ASA firewall using the ESMTP inspection engine, mitigating several types of malformed message attacks.
- ☐ The question clearly says not to use an ACL, which leaves your choice to an MPF solution.
- ☐ The question also says not to apply the policy to the inside or outside interface, which leaves your choice to applying the policy on the default global policy.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.

- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

The following outputs verify MPF configuration on the ASA1/c1 context, meeting the requirements:

```
ASA1/c1# show run regex
regex emailaddress "joe@myemail.com"

ASA1/c1# show run policy-map type inspect esmtp
!
policy-map type inspect esmtp blockBADemail
 parameters
  special-character action drop-connection
 match sender-address regex emailaddress
  drop-connection
 match header to-fields count gt 5
  drop-connection
!

ASA1/c1# show run policy-map global_policy
!
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
```

NOTE
This question is configuration-based only; there is no live traffic that you can use to validate the functionality. The lab exam may have a few questions of this type, where you have to rely on your configuration only.

```
  inspect rtsp
  inspect skinny
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect esmtp blockBADemail
!

ASA1/c1# show service-policy global inspect esmtp
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: esmtp blockBADemail, packet 0, drop 0, reset-drop 0
        mask-banner, count 0
        special-character, drop 0
        match sender-address regex emailaddress
          drop-connection, packet 0
        match header to-fields count gt 5
          drop-connection, packet 0
```

Question 7.4: IKE resource exhaustion protection (3 points)

Configure IKE resource exhaustion denial-of-service (DoS) protection on R1, meeting all the following requirements:

- An intruder is attempting to exploit limitations of the IKE protocol to deplete available resources to negotiate IKE SAs (Security Associations) and block legitimate IPsec peers from establishing new IKE SAs or rekey existing IKE SAs.
- Configure R1 to rate-limit inbound UDP/500 traffic from any source to destination R1 Loopback0 preventing CPU processing power and memory resources from being fully consumed by incoming IKE requests.

- Traffic at rates below 32,000 bits per second (bps) with normal burst of 6,000 bytes should be forwarded normally; however, traffic above 32,000 bps packets with twice the normal burst must be dropped. (32,000 bps is loosely equivalent to 35 IKE messages per second.)
- Do not configure Modular QoS CLI (MQC) to complete this task.

Skills tested

- ☐ Configuring Internet Key Exchange (IKE) resource exhaustion denial-of-service (DoS) protection using the Committed Access Rate (CAR)
- ☐ Understanding capabilities of the rate-limit (CAR) feature and how it works, and understanding how the values are calculated

Functionality and solution verification

- ☐ This question is about configuring proactive measures to prevent attacks surrounding Internet Key Exchange (IKE). IKE protocol version 1 has known weaknesses, with possible exploits.
- ☐ The objective of this question is to prevent IKE resource exhaustion DoS issues using the rate-limit (CAR) feature on R1.
- ☐ The question clearly says to rate-limit inbound UDP/500 traffic from any source to destination R1 Loopback0, which leaves your solution to applying the CAR on R1 GigabitEthernet0/0 in the inbound direction.
- ☐ Configure rate-limit on the R1 GigabitEthernet0/0 interface inbound using the CAR parameters.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

The following outputs verify that CAR has been enabled on the R1 GigabitEthernet0/0 interface, meeting all the requirements:

```
R1# show run interface GigabitEthernet 0/0
Building configuration...
Current configuration : 312 bytes
!
interface GigabitEthernet0/0
 ip address 192.168.3.11 255.255.255.0
 ip pim sparse-dense-mode
 ip ips myIOSipsV5 in
 ip ips myIOSipsV5 out
 rate-limit input access-group 101 32000 6000 12000 conform-action transmit exceed-action drop
 duplex auto
 speed auto
 media-type rj45
 crypto map dmvpn_using_gdoi
end

R1# show ip access-lists 101
Extended IP access list 101
    10 permit udp any host 10.1.1.1 eq isakmp
```

You can also verify CAR on the interfaces level:

```
R1# show interfaces GigabitEthernet 0/0 rate-limit
GigabitEthernet0/0
  Input
    matches: access-group 101
      params:  32000 bps, 6000 limit, 12000 extended limit
      conformed 0 packets, 0 bytes; action: transmit
      exceeded 0 packets, 0 bytes; action: drop
      last packet: 525874752ms ago, current burst: 0 bytes
      last cleared 00:02:30 ago, conformed 0 bps, exceeded 0 bps
R1#
```

 Please see page 474 for more details.

Section 8.0: Network Attacks (13 Points)

Question 8.1: Web server attack (3 points)

Configure a mitigation solution to respond to the web server attack, meeting all the following requirements:

- Users are complaining of intermittent access to the web server located in VLAN 2 with IP address 192.168.2.100. Most external clients also cannot load the company's web page hosted on this server.
- Review the outputs that were captured on the ASA1/c1 context during the investigation and troubleshooting of this issue, and configure the ASA1/c1 context to mitigate this problem.
- The solution must be applied to the c1 context outside interface.
- Do not configure or modify network address translation to complete this task.
- Do not use an ACL to complete this task.

```
ASA1/c1# show perfmon
Context: c1
PERFMON STATS:                      Current      Average
Xlates                                0/s          0/s
Connections                        2236/s        321/s
TCP Conns                          2236/s        321/s
UDP Conns                             0/s          0/s
URL Access                            0/s          0/s
URL Server Req                        0/s          0/s
TCP Fixup                             0/s          0/s
TCP Intercept Established Conns       0/s          0/s
TCP Intercept Attempts                0/s          0/s
TCP Embryonic Conns Timeout        1012/s          4/s
HTTP Fixup                            0/s          0/s
```

 Please see page 474 for more details.

```
FTP Fixup                              0/s          0/s
AAA Authen                             0/s          0/s
AAA Author                             0/s          0/s
AAA Account                            0/s          0/s
VALID CONNS RATE in TCP INTERCEPT:     Current      Average
                                        N/A         95.00%

ASA1/c1# show conn
52121 in use, 52121 most used
TCP outside 17.24.101.118:26093 inside 192.168.2.100:80, idle 0:00:23, bytes 0, flags aB
TCP outside 111.76.36.109:23598 inside 192.168.2.100:80, idle 0:00:13, bytes 0, flags aB
TCP outside 24.185.110.202:32729 inside 192.168.2.100:80, idle 0:00:25, bytes 0, flags aB
TCP outside 130.203.2.204:56481 inside 192.168.2.100:80, idle 0:00:29, bytes 0, flags aB
TCP outside 39.142.106.205:18073 inside 192.168.2.100:80, idle 0:00:02, bytes 0, flags aB
TCP outside 75.27.223.63:51503 inside 192.168.2.100:80, idle 0:00:03, bytes 0, flags aB
TCP outside 121.226.213.239:18315 inside 192.168.2.100:80, idle 0:00:04, bytes 0, flags aB
TCP outside 66.187.75.192:23112 inside 192.168.2.100:80, idle 0:00:06, bytes 0, flags aB
TCP outside 13.50.2.216:3496 inside 192.168.2.100:80, idle 0:00:13, bytes 0, flags aB
TCP outside 99.92.72.60:47733 inside 192.168.2.100:80, idle 0:00:27, bytes 0, flags aB
TCP outside 30.34.246.202:20773 inside 192.168.2.100:80, idle 0:00:02, bytes 0, flags aB
TCP outside 95.108.110.131:26224 inside 192.168.2.100:80, idle 0:00:02, bytes 0, flags aB
TCP outside 76.181.105.229:21247 inside 192.168.2.100:80, idle 0:00:06, bytes 0, flags aB
TCP outside 82.210.233.230:44115 inside 192.168.2.100:80, idle 0:00:02, bytes 0, flags aB
TCP outside 134.195.170.77:28138 inside 192.168.2.100:80, idle 0:00:12, bytes 0, flags aB
TCP outside 70.133.128.41:22257 inside 192.168.2.100:80, idle 0:00:15, bytes 0, flags aB
TCP outside 124.82.133.172:27391 inside 192.168.2.100:80, idle 0:00:27, bytes 0, flags aB
TCP outside 26.147.236.181:37784 inside 192.168.2.100:80, idle 0:00:07, bytes 0, flags aB
TCP outside 98.137.7.39:20591 inside 192.168.2.100:80, idle 0:00:13, bytes 0, flags aB
TCP outside 37.27.115.122:24542 inside 192.168.2.100:80, idle 0:00:12, bytes 0, flags aB
<snip>
```

Skills tested

- ☐ Classifying and identifying TCP SYN floods using **show** and **debug** commands on the Cisco ASA firewall
- ☐ Understanding TCP three-way handshake and embryonic (half-open) connections
- ☐ Configuring a mitigation solution to prevent SYN flood and DoS protection using TCP Intercept on the Cisco ASA Firewall
- ☐ Knowledge of the Modular Policy Framework (MPF) configuration model on the Cisco ASA Firewall

Functionality and solution verification

- ☐ The objective of this question is to configure the mitigation solution to prevent TCP SYN flood type DoS attacks.
- ☐ The most important aspect of this question is to analyze and decipher the sample outputs provided. The first output of **show perfmon** clearly shows that the TCP Embryonic Conns Timeout counter is very high. This indicates that several embryonic (half-open) connections are timing out due to no response from the final (ACK) within the TCP handshake process. Secondly, the **show conn** output also confirms this by observing multiple embryonic (half-open) connections from random source IP addresses to the web server address 192.168.2.100 on TCP/80 with flags aB. The aB flag on each entry means that a (SYN+ACK) was sent from the web server to the remote client who initiated the TCP connection. However, the final (ACK) was not received from the client back to the server, thus leaving the TCP connection incomplete. This obviously occurs because the remote client is a spoofed address (it's nonexistent or did not initiate this TCP connection). An intruder spoofs random source addresses and sends a series of TCP (SYN) packets to the web server knowing that the return (SYC+ACK) will go to the spoofed address and a response will not come back. This causes the web server to maintain a large number of the embryonic (half-open) connections occupying memory and blocking TCP connections from legitimate sources (intermittently) due to lack of memory and connection sockets.
- ☐ You can use several techniques to configure this attack. However, the question requires a solution on the Cisco ASA firewall. You also cannot use a network address translation (**static**) command where you can set the embryonic (half-open) connections limit. The only other option left on the firewall is to use MPF on the ASA1/c1 context.

 Please see page 474 for more details.

- The question restricts the use of an ACL; therefore, you need to use the **match port** command in the **class-map** to classify the HTTP (TCP/80) traffic.
- The question requires configuring MPF and setting the maximum limit for embryonic (half-open) connections. Alternatively, the same could also be achieved by setting the maximum embryonic connections limit on a per-client basis. Because the question does not restrict, both solutions are acceptable, and you can set the embryonic (half-open) connections limit to any number; 100 is used in this example.
- The question clearly says to apply the solution to the outside interface on the ASA1/c1 context.
- You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- For the final solution, refer to the solution configurations provided for all the devices.

The following outputs verify the MPF solution preventing the SYN attack to TCP port 80.

An ACL is not used, as per the restriction in the question:

```
ASA1/c1# show service-policy interface outside
Interface outside:
  Service-policy: embryonic_attack_protection
    Class-map: webport
      Set connection policy: embryonic-conn-max 100 per-client-embryonic-max 100
        current embryonic conns 0, drop 0
ASA1/c1#

ASA1/c1# show run service-policy
service-policy global_policy global
service-policy embryonic_attack_protection interface outside
```

 Please see page 474 for more details.

```
ASA1/c1# show run policy-map embryonic_attack_protection
policy-map embryonic_attack_protection
 class webport
  set connection embryonic-conn-max 100 per-client-embryonic-max 100

ASA1/c1# show run class-map webport
!
class-map webport
 match port tcp eq www
!
ASA1/c1#
```

Question 8.2: Preventing unauthorized connections (3 points)

Configure R3 to prevent unauthorized connections, meeting all the following requirements:

- A new virus is propagating through your network from the Internet. Upon investigation, you find the virus traffic is entering your network via the R3 GigabitEthernet0/0 interface.
- Configure R3 to prevent the propagation of this virus by matching explicit parameters using the information in Table 2-50.
- Ensure that your solution does not impede any traffic, and all other traffic flows uninterrupted through R3.

TABLE 2-50 R3 configuration information

Virus Pattern Specification	☐ Configure policy-based packet matching using the following criteria. ☐ TCP Protocol ☐ TCP port 4444 ☐ Random source and destination IP address ☐ IP packet length 100 ☐ Redirect infected packets matching the above criteria to router bit bucket blackholing the packets. ☐ Do not configure ZFW, CBAC, NBAR, MQC, and CAR to complete this task.

Skills tested

- ☐ Preventing unauthorized TCP connections from causing performance degradation and unwanted TCP SYN flooding using Policy-Based Routing (PBR)
- ☐ Ability to configure route-maps
- ☐ Knowledge of router bit bucket (Null0 interface) to black hole matching packets

Functionality and solution verification

- ☐ The objective of this question is to configure virus mitigation with Policy-Based Routing (PBR) using the route-map configuration model.
- ☐ The question provides virus specification using TCP port 4444 with a fixed packet length of 100. Generally, TCP port 4444 is used by Kerberos authentication and Oracle9i communication. A host infected with the virus opens a command shell on this port, allowing machines to be controlled remotely (zombies).
- ☐ The question says not to use traditional mitigation approaches, including ZFW, CBAC, NBAR, MQC, and CAR to complete this task.
- ☐ The important hint to note in this question that leads you to the PBR (route-map) solution is to set the router bit bucket to Null0 and where the requirement table says to configure policy-based packet matching.
- ☐ To mitigate the virus traffic, you need to configure PBR (**route-map**)—one **route-map** to match the TCP traffic based on the virus criteria, and a second **route-map** with no parameters (without **match/set** commands). This is similar to a default policy that matches all other traffic to pass through uninterrupted. A **route-map** configuration model has no default policy. Therefore, you need to explicitly configure the second **route-map** to mimic default policy, allowing all remaining traffic.
- ☐ Then, apply the policy (PBR) to the R3 GigabitEthernet0/0 interface. Review the solution shown.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

The following outputs verify the PBR solution on R3. Ensure that the second **route-map** policy is configured without **match/set** commands (to mimic the default policy) as mentioned:

```
R3# show ip interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.3.3/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
```

 Please see page 474 for more details.

```
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is enabled, using route map drop4444-pbr
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: IPSec input classification, Policy Routing, MCI Check
  Output features: IPSec output classification, IPSec: to crypto engine, Post-encryption output features
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled

R3# show run interface GigabitEthernet 0/0
Building configuration...
Current configuration : 179 bytes
interface GigabitEthernet0/0
 ip address 192.168.3.3 255.255.255.0
 ip policy route-map drop4444-pbr
 duplex auto
 speed auto
 media-type rj45
 crypto map dmvpn_using_gdoi
end

R3# show run ¦ section route-map
route-map drop4444-pbr permit 10
 match ip address 101
 match length 100 100
 set interface Null0
route-map drop4444-pbr permit 20
```

 Please see page 474 for more details.

```
R3# show ip policy
Interface      Route map
Gi0/0          drop4444-pbr

R3# show route-map drop4444-pbr
route-map drop4444-pbr, permit, sequence 10
  Match clauses:
    ip address (access-lists): 101
    length 100 100
  Set clauses:
    interface Null0
  Policy routing matches: 0 packets, 0 bytes
route-map drop4444-pbr, permit, sequence 20
  Match clauses:
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
R3#

R3# show ip access-list 101
Extended IP access list 101
    10 permit tcp any any eq 4444
```

NOTE
Policy-Based Routing (PBR) is applicable for inbound traffic when configured on the specified interface. By default, packets generated by the local router are not subject to this policy. To enable PBR for locally generated packets on this router, use the **ip local policy route-map** *map-name* command from global configuration mode.

Question 8.3: W32.Blaster worm attack (4 points)

Configure a mitigation solution to respond to the W32.Blaster worm attack, meeting all the following requirements:

- Configure R1 to prevent W32.Blaster worm propagation on UDP port 69 by matching explicit parameters using the information in Table 2-51.
- Ensure that your solution does not break existing TFTP functionality, which also uses UDP port 69.

 Please see page 474 for more details.

- Apply the solution inbound to R1 GigabitEthernet0/1 interface.
- Do not use an ACL to complete this task.
- Do not use ZFW or CBAC to complete this task.

TABLE 2-51 R1 configuration information

W32.Blaster Worm Specification	☐ Configure deep packet inspection to match a custom pattern using the following match criteria: ☐ UDP Protocol ☐ UDP port 69 ☐ IP packet length exceeding 402 bytes ☐ Pattern match 0x20a29010 at 50 bytes from start of IP header, to match on 4 bytes ☐ Do not configure an ACL to complete this task.

Skills tested

- ☐ Configuring work mitigation using the new Cisco IOS Flexible Packet Matching (FPM) feature
- ☐ Knowledge of the MQC configuration model using extended FPM capabilities
- ☐ Loading the Protocol Header Definition File (PHDF) files into the router flash and enabling it from global configuration mode
- ☐ Ability to configure nested policy-maps

Functionality and solution verification

- ☐ Cisco IOS Flexible Packet Matching (FPM) is another technology that makes its debut in the new CCIE Security v3.0 lab blueprint. FPM is one of the important technologies, and candidates should be well-prepared.
- ☐ The objective of this question is to configure W32.Blaster worm mitigation with the MQC configuration model using extended FPM capabilities. FPM can be used in a variety of scenarios performing deep packet inspection with its ability to perform granular Layer 2 through 7 matching.

- ☐ The W32.Blaster worm uses UDP port 69. Generally, UDP port 69 is used by TFTP protocol, which is used to load new software images or configurations to networked devices. A host infected with the W32.Blaster worm opens this port to transfer the msblast.exe file from an infected machine to a newly exploited machine.
- ☐ To mitigate the worm, you need to configure two FPM (deep packet inspection) **class-maps**. The first **class-map**, of **type stack**, matches the UDP packet in the IP header. The second **class-map**, of **type access-control**, matches additional parameters such as destination-port and IP packet length.
- ☐ Ensure that the **class-map** matches all the **match** statements using the Logical-AND (**match-all**) operation. Otherwise, it will drop legitimate UDP/69 (TFTP) packets too if using a Logical-OR (**match-any**) operation by matching a single **match** criterion.
- ☐ Then, configure two **policy-maps**, both access-control types. The first **policy-map** should match the attributes (destination-port and IP packet length) and define the drop action to it. The second **policy-map** should match the stack-type class-map and apply the first policy-map as a child in a nested fashion. Review the solution shown.
- ☐ All other UDP/69 (TFTP) sessions except those matching the preceding requirement should work flawlessly using the default class.
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

Before you can configure FPM, you need to load the Protocol Header Definition File (PHDF) files into the router flash and enable it from global configuration mode.

FPM provides ready-made definitions for these standard protocols (IP, TCP, UDP, ICMP) that can be loaded onto the router with the **load protocol** command: ip.phdf, tcp.phdf, udp.phdf, and icmp.phdf.

Ensure that the PHDF files are copied in the flash, and then enable them as shown here:

```
R1# config term
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# load protocol flash:ip.phdf
R1(config)# load protocol flash:udp.phdf
```

As soon as the PHDF modules are loaded, you can start configuring the relevant FPM configuration.

The following outputs verify the FPM configuration using the extended MQC nested configuration model. Note that an ACL is not used to complete this task:

```
R1# show run ¦ sec class-map
class-map type access-control match-all W32-Blaster
 description "Match W32.Blaster worm packets"
 match field UDP dest-port eq 0x45
 match field IP length gt 0x192
 match start l3-start offset 50 size 4 eq 0x20A29010
class-map type stack match-all udp_protocol
 description "Match UDP over IP packets"
 match field IP protocol eq 0x11 next UDP

R1# show run ¦ sec policy-map
policy-map type access-control drop-W32-Blaster
 description "Policy for UDP based W32.Blaster worm attack"
 class W32-Blaster
   drop
policy-map type access-control fpm-policy
 description "drop W32.Blaster worm packets"
 class udp_protocol
  service-policy drop-W32-Blaster

R1# show run interface GigabitEthernet0/1
```

 Please see page 474 for more details.

```
Building configuration...
Current configuration : 170 bytes
!
interface GigabitEthernet0/1
 ip address 192.168.2.11 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 service-policy type access-control input fpm-policy
end
R1#

R1# show policy-map type access-control interface GigabitEthernet 0/1
 GigabitEthernet0/1

  Service-policy access-control input: fpm-policy

    Class-map: udp_protocol (match-all)
      247 packets, 47523 bytes
      5 minute offered rate 0 bps
      Match: field IP protocol eq 0x11 next UDP

      Service-policy access-control : drop-W32-Blaster

        Class-map: W32-Blaster (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps
          Match: field UDP dest-port eq 0x45
          Match: field IP length lt 0x192
          Match: start l3-start offset 50 size 4 eq 0x20A29010
```

 Please see page 474 for more details.

```
        drop

          Class-map: class-default (match-any)
            247 packets, 47523 bytes
            5 minute offered rate 0 bps, drop rate 0 bps
            Match: any

      Class-map: class-default (match-any)
        0 packets, 0 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
        Match: any
R1#
```

Question 8.4: IP spoofing attack (3 points)

Configure Sw1 to protect against IP spoofing attacks, meeting all the following requirements:

- An intruder is sending a SYN flood spoofing trusted IP addresses of devices in VLAN 10 employing the source IP spoofing technique.
- Configure a countermeasure on Sw1 to protect against IP spoofing attacks by checking the source IP address field with the binding table. Packets not validated should be blocked.
- Additionally, configure a static binding entry in the DHCP snooping binding table for a trusted host (non-DHCP) with MAC address 0000.0000.0001 and IP address 10.10.1.1 in VLAN 10 connected to Sw1 interface FastEthernet0/18.
- A new DHCP server will be deployed in the future on Sw1 interface FastEthernet0/19. Ensure that this port is the trusted port to reply DHCP requests on the network.

 Please see page 474 for more details.

Skills tested

- ☐ Configuring a countermeasure technique on Cisco Catalyst switches to prevent an IP spoofing attack using IP Source Guard (IPSG) coupled with DHCP Snooping
- ☐ Understanding SYN attacks employing IP spoofing techniques
- ☐ Knowledge of both IPSG and DHCP snooping using binding table and its capabilities

Functionality and solution verification

- ☐ The objective of this question is to protect VLAN 10 devices from IP spoofing attacks using IP Source Guard (IPSG), which prevents IP spoofing attacks by intercepting all IP packets and validating them with the entries in the binding table.
- ☐ An important thing to remember in this task is that DHCP Snooping is a prerequisite for IPSG functionality to work. It depends on the snooping binding table, which is built and populated dynamically when DHCP snooping is enabled. You can also populate static entries into this table.
- ☐ When DHCP snooping is enabled, all ports by default in the VLAN are "untrusted" for DHCP replies, except for the port that is explicitly configured as "trusted," where the DHCP server is connected and is the only authorized port to send DHCP replies out of the switch (interface FastEthernet0/19 in this task). Then, enable IP Source Guard (IPSG) on Sw1 for validating source IP addresses of all incoming IP packets. When both IPSG and DHCP snooping are enabled, all packets must match the IP binding table entries. If the entries do not match, the switch discards those packets in the bit bucket.
- ☐ The question also requires configuring a static binding entry for a trusted host (non-DHCP).
- ☐ You will see several **show** command outputs so that you can check and verify the requirements laid out in the question.
- ☐ The highlighted portions are of the utmost importance. The grading for this question is strongly based on these highlighted items. Any incorrect or mismatched item will result in a null score for this question.
- ☐ For the final solution, refer to the solution configurations provided for all the devices.

The following outputs verify that the DHCP snooping and IP Source Guard (IPSG) features are both enabled on VLAN 10 and meet all other requirements:

```
Sw1# show run ¦ include dhcp
ip dhcp snooping vlan 10
no ip dhcp snooping information option
ip dhcp snooping
 ip dhcp snooping trust
Sw1#

Sw1# show run interface FastEthernet 0/18
Building configuration...
Current configuration : 103 bytes
!
interface FastEthernet0/18
 switchport access vlan 10
 switchport mode access
 ip verify source
end

Sw1# show run interface FastEthernet 0/19
Building configuration...
Current configuration : 109 bytes
!
interface FastEthernet0/19
 switchport access vlan 10
 switchport mode access
 ip dhcp snooping trust
end
```

```
Sw1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
DHCP snooping is operational on following VLANs:
10
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is disabled
   circuit-id format: vlan-mod-port
    remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
FastEthernet0/19             yes         unlimited

Sw1# show ip source binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:00:00:00:00:01   10.10.1.1        infinite    static          10    FastEthernet0/18
Total number of bindings: 1

Sw1# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----------
Fa0/18     ip           inactive-no-snooping-vlan
Sw1#
```

 Please see page 474 for more details.

CCIE Security v3.0 Configuration Practice Labs, Second Edition

Yusuf Bhaiji

Published by:
Cisco Press
800 East 96th Street
Indianapolis, Indiana 46240 USA

First Release November 2009

ISBN-13: 978-1-58714-026-6

ISBN-10: 1-58714-026-8

Warning and Disclaimer

This eBook is designed to provide information about the networking exam. Every effort has been made to make this eBook as complete and accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this eBook.

The opinions expressed in this eBook belong to the authors and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this eBook that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this eBook should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members of the professional technical community.

Reader feedback is a natural continuation of this process. If you have any comments on how we could improve the quality of this eBook, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please be sure to include the eBook title and ISBN in your message.

We greatly appreciate your assistance.

Corporate and Government Sales

The publisher offers excellent discounts on this eBook when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com.

For sales outside the United States, please contact: **International Sales** international@pearsoned.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**