

**ASSESSMENT**

**ICTNWK506 Configure, verify and troubleshoot WAN links and IP services in a medium enterprise network**

|  |  |
| --- | --- |
| **Student Name** |  |
| **Student ID** |  |
| **Unit commenced (Date)** |  |
| **Unit Completed (Date)** |  |
| I hereby certify that I have undertaken these assessment tasks utilising my own work without assistance from any other parties. I have not knowingly plagiarised any work in completing these assessment activities.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **Student Signature** |  |

**Knowledge Assessment (Written Tasks)**

#### 1. How do you configure an IPv6 address on a Cisco router interface?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

**2. What is HDLC?**

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

**3. In the light of Network Address Translation (NAT) working well and correctly, what is the business case for service providers to upgrade their networks to support IPv6?**

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

**4. For security reasons, you want to disable the CDP protocol on a router. Your router has multiple interfaces. The issuance of which single command will completely disable CDP?**

(a) cdp disable

(b) no cdp enable

(c) no cdp run

(d) shutdown cdp

(e) no ip routing

**5. Which two pieces of information are typically found on a logical network diagram? (Choose two.)**

(a) cable types

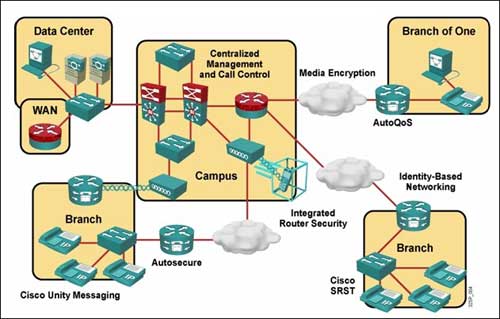
(b) connector types

(c) interface identifiers

(d) DLCI for virtual circuits

(e) operating system versions

**6. Refer to the exhibit. Which two steps should be taken during the process of creating network documentation? (Choose two.)**



(a) Record the information about the devices discovered in the Campus network only.

(b) Record the information about the devices discovered in the entire network, including the remote locations.

(c) Transfer any information about the devices from the network configuration table that corresponds to a component of the topology diagram.

(d)Transfer only the Layer 2 and Layer 3 information about the devices from the network configuration table that corresponds to a component of the topology diagram.

(e) Transfer the recorded information about the devices from the network configuration table gathered during peak network utilization that corresponds to a component of the topology diagram.

**7. Clients across the company are reporting poor performance across all corporate applications running in the data center. Internet access and applications running across the corporate WAN are performing normally. The network administrator observes a continual broadcast of random meaningless traffic (jabber) on the application server LAN in the data center on a protocol analyzer. How should the administrator start troubleshooting?**

(a) The jabber in the data center indicates a local physical layer problem. Use the protocol analyzer to determine the source of the jabber, and then check for a recent NIC driver update or bad cabling.

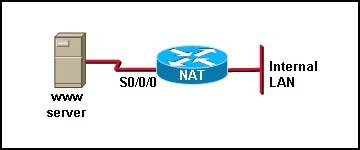
(b) Because all clients are experiencing application problems, the administrator should use a top-down approach with the

(c) application servers in the data centre.

(d)The scope of the problem indicates a likely routing or spanning-tree problem. Begin by checking routing tables, and follow up using appropriate STP show commands to find a loop if routing is working normally.

(e) Poll the staff to determine if any recent changes have been made. Back out all the changes one by one until the error condition is fixed.

**8. Refer to the exhibit. Users on the Internal LAN are unable to connect to the www server. The network administrator pings the server and verifies that NAT is functioning correctly. Which OSI layer should the administrator begin to troubleshoot next?**



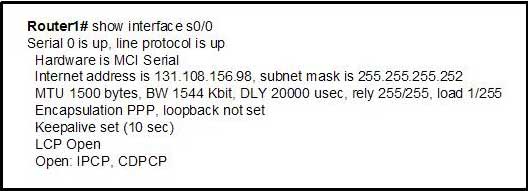
(a) physical

(b) data link

(c) network

(d) application

**9. Refer to the exhibit. Which three pieces of information can be determined by analyzing the output shown? (Choose three.)**



(a) A carrier detect signal is present.

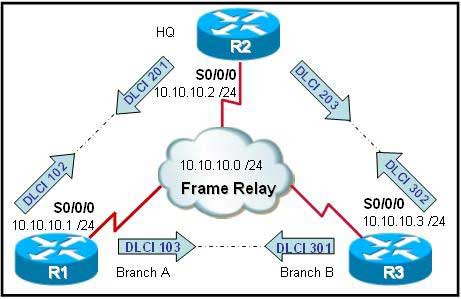
(b) Keepalives are being received successfully. (Missed)

(c) Default encapsulation is used on this serial link.

(d) The reliability of this link is very low.

(e) The LCP negotiation phase is complete.

**10. Refer to the exhibit. Users at Branch B are reporting trouble accessing a corporate website running on a server that is located at HQ. HQ and Branch A users can access the website. R3 is able to ping 10.10.10.1 successfully but not 10.10.10.2. The users at Branch B can access servers at Branch A. Which two statements are true about the troubleshooting efforts? (Choose two.)**



(a) The web server should be tested for an application layer problem.

(b) Frame Relay at R3 and R2 should be tested to narrow the scope of the problem.

(c) The fact that users at Branch A are working normally proves that there is no problem at R2.

(d) An ACL entry error could cause the failure at Layer 4 in either R3 or R2.

(e) The successful ping from R3 to R1 proves that the WAN is functioning normally. Therefore, the problem has to be in the upper layers.

**11. Which of the following statements accurately describe differences between a LAN and a WAN? (Choose two.)**

(a) A LAN makes data connections across a broad geographic area, and a WAN makes a local connection in a building.

(b) Companies can use WAN to connect remote locations, and a LAN can make a local connection in a building.

(c) WANS are usually faster than LAN's.

(d) Only WANS require a CSU/DSU to be used on the ends of a cable.

**12. Which of the following are true about a router? (Choose three.)**

(a) Routers enable different IP networks or IP subnets to communicate with each other.

(b) Routers choose paths between networks using MAC address information.

(c) Path selection is one of the main functions of a router.

(d) Protocols are specialized chips on a router's motherboard to store routing tables.

(e) Routers have a central processing unit and memory.

**13. Encapsulation errors from mismatched WAN protocols on a serial link between two routers indicate a problem at which OSI layer?**

(a) physical

(b) data link

(c) network

(d) transport

**14. What combination of IP address and wildcard mask should be used to specify only the last 8 addresses in the subnet 192.168.3.32/28?**

(a) 192.168.3.32 0.0.0.7

(b) 192.168.3.32 0.0.0.15

(c) 192.168.3.40 0.0.0.7

(d) 192.168.3.40 0.0.0.15

**15. You want to filter inbound routes from an OSPF neighbor. Which command do you use?**

(a) Distribute-list  
(b) Route-list  
(c) Prefix-list  
(d) Filter-list

**16. What is the format of the IPv6?**

(a) Numeric format

(b) Hexadecimal format

(c) Octet format

(d) All of the above

**17. How many bits are in IPv6?**

(a) 256 bits

(b) 128 bytes

(c) 64 bits

(d) 128 bits

**18. Which command will show all current information on routing?**

(a) #show running-config

(b) #show run

(c) #sh run

(d) All of the above

**19. Which three parameters can ACLs use to filter traffic? (Choose three.)**

(a) Packet size

(b) Protocol suite

(c) Source address

(d) Destination address

(e) Destination router interface

**20. What is the function of ARP?**

(a) Find the hardware address of destination

(b) Find the IP address of destination

(c) Find the hardware address of source

(d) Find the IP address of source

**21. DHCP is used when a client sends a release message to terminate a lease early describes what aspect of DHCP?**

(a) Lease expiration

(b) Reboot

(c) Address Release

(d) DHCP Discover

**22. Which protocol will allow auto configuration across the network of IP address?**

(a) HDLC

(b) PPP

(c) SLIP

(d) ARP

**Assessment Outcome**

|  |  |
| --- | --- |
| **Question** | **Correct (✓)** |
| 1 |  |
| 2 |  |
| 3 |  |
| 4 |  |
| 5 |  |
| 6 |  |
| 7 |  |
| 8 |  |
| 9 |  |
| 10 |  |
| 11 |  |
| 12 |  |
| 13 |  |
| 14 |  |
| 15 |  |
| 16 |  |
| 17 |  |
| 18 |  |
| 19 |  |
| 20 |  |
| 21 |  |
| 22 |  |

**Assessed by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Assessor Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

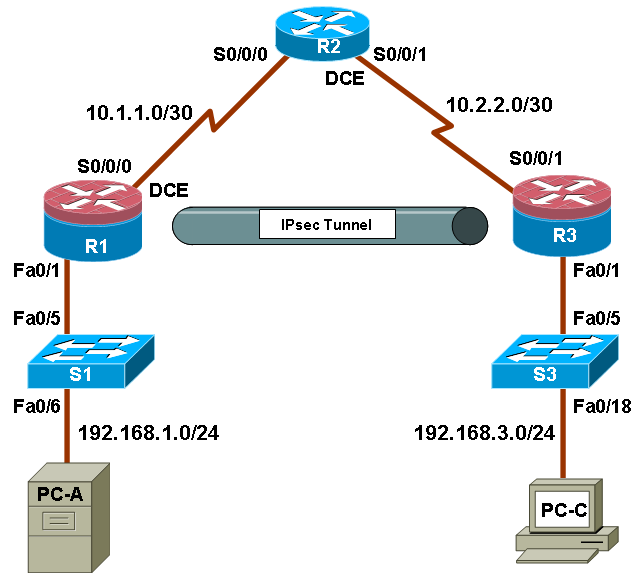
**Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Skills Assessment (Practical Tasks)**

|  |
| --- |
| **ASSESSOR NOTE**  **These instructions must be followed when assessing the student in this unit. The checklist on the following page is to be completed for each student. Please refer to separate mapping document for specific details relating to alignment of this task to the unit requirements**.  This competency is to be assessed using standard and authorised work practices, safety requirements and environmental constraints.  Assessment of essential underpinning knowledge will usually be conducted in an off-site context.  Assessment is to comply with relevant regulatory or Australian standards' requirements.  Resource implications for assessment include:  • an induction procedure and requirement  • realistic tasks or simulated tasks covering the mandatory task requirements  • relevant specifications and work instructions  • tools and equipment appropriate to applying safe work practices  • support materials appropriate to activity  • workplace instructions relating to safe work practices and addressing hazards and emergencies  • material safety data sheets  • research resources, including industry related systems information.  Reasonable adjustments for people with disabilities must be made to assessment processes where required. This could include access to modified equipment and other physical resources, and the provision of appropriate assessment support. |

**Task 1 – Configuring a Site-to-Site VPN Using Cisco IOS or SDM**

Topology



IP Addressing Table

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** | **Switch Port** |
| R1 | FA0/1 | 192.168.1.1 | 255.255.255.0 | N/A | S1 FA0/5 |
|  | S0/0/0 (DCE) | 10.1.1.1 | 255.255.255.252 | N/A | N/A |
| R2 | S0/0/0 | 10.1.1.2 | 255.255.255.252 | N/A | N/A |
|  | S0/0/1 (DCE) | 10.2.2.2 | 255.255.255.252 | N/A | N/A |
| R3 | FA0/1 | 192.168.3.1 | 255.255.255.0 | N/A | S3 FA0/5 |
|  | S0/0/1 | 10.2.2.1 | 255.255.255.252 | N/A | N/A |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 | S1 FA0/6 |
| PC-C | NIC | 192.168.3.3 | 255.255.255.0 | 192.168.3.1 | S3 FA0/18 |

Objectives

Part 1: Basic Router Configuration

* Configure host names, interface IP addresses, and access passwords.
* Configure the EIGRP dynamic routing protocol.

Part 2: Configure a Site-to-Site VPN Using Cisco IOS

* Configure IPsec VPN settings on R1 and R3
* Verify site-to-site IPsec VPN configuration
* Test IPsec VPN operation

Part 3: Configure a Site-to-Site VPN Using SDM

* Configure IPsec VPN settings on R1
* Create a mirror configuration for R3
* Apply the mirror configuration to R3
* Verify the configuration
* Test the VPN configuration using SDM

Background

VPNs can provide a secure method of transmitting data over a public network, such as the Internet. VPN connections can help reduce the costs associated with leased lines. Site-to-Site VPNs typically provide a secure (IPsec or other) tunnel between a branch office and a central office. Another common implementation that uses VPN technology is remote access to a corporate office from a telecommuter location such as a small office or home office.

In this lab, you build a multi-router network and configure the routers and hosts. You use Cisco IOS and SDM to configure a site-to-site IPsec VPN and test it. The IPsec VPN tunnel is from router R1 to router R3 via R2. R2 acts as a pass-through and has no knowledge of the VPN. IPsec provides secure transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (peers), such as Cisco routers.

**Note:** The router commands and output in this lab are from a Cisco 1841 with Cisco IOS Release 12.4(20)T (Advanced IP image). Other routers and Cisco IOS versions can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the router model and Cisco IOS version, the commands available and output produced might vary from what is shown in this lab.

**Note:** Make sure that the routers and the switches have been erased and have no startup configurations.

Required Resources

* 3 routers with SDM 2.5 installed (Cisco 1841 with Cisco IOS Release 12.4(20)T1 or comparable)
* 2 switches (Cisco 2960 or comparable)
* PC-A (Windows XP or Vista)
* PC-C (Windows XP or Vista)
* Serial and Ethernet cables as shown in the topology
* Rollover cables to configure the routers via the console

#### Part 1: Basic Router Configuration

In Part 1 of this lab, you set up the network topology and configure basic settings, such as the interface IP addresses, dynamic routing, device access, and passwords.

**Note:** All tasks should be performed on routers R1, R2, and R3. The procedure for R1 is shown here as an example.

Step 1: Cable the network as shown in the topology.

Attach the devices shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each router.

1. Configure host names as shown in the topology.
2. Configure the interface IP addresses as shown in the IP addressing table.
3. Configure a clock rate for the serial router interfaces with a DCE serial cable attached.

R1(config)#interface S0/0/0

R1(config-if)#clock rate 64000

Step 3. Disable DNS lookup.

To prevent the router from attempting to translate incorrectly entered commands, disable DNS lookup.

R1(config)#no ip domain-lookup

Step 4: Configure the EIGRP routing protocol on R1, R2, and R3.

1. On R1, use the following commands.

R1(config)#router eigrp 101

R1(config-router)#network 192.168.1.0 0.0.0.255

R1(config-router)#network 10.1.1.0 0.0.0.3

R1(config-router)#no auto-summary

1. On R2, use the following commands.

R2(config)#router eigrp 101

R2(config-router)#network 10.1.1.0 0.0.0.3

R2(config-router)#network 10.2.2.0 0.0.0.3

R2(config-router)#no auto-summary

1. On R3, use the following commands.

R3(config)#router eigrp 101

R3(config-router)#network 192.168.3.0 0.0.0.255

R3(config-router)#network 10.2.2.0 0.0.0.3

R3(config-router)#no auto-summary

Step 5: Configure PC host IP settings.

1. Configure a static IP address, subnet mask, and default gateway for PC-A, as shown in the IP addressing table.
2. Configure a static IP address, subnet mask, and default gateway for PC-C, as shown in the IP addressing table.

Step 6: Verify basic network connectivity.

1. Ping from R1 to the R3 Fa0/1 interface at IP address 192.168.3.1.

Were the results successful?

|  |
| --- |
|  |
|  |
|  |
|  |

If the pings are not successful, troubleshoot the basic device configurations before continuing.

1. Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.

Were the results successful?

|  |
| --- |
|  |
|  |
|  |
|  |

If the pings are not successful, troubleshoot the basic device configurations before continuing.

**Note:** If you can ping from PC-A to PC-C, you have demonstrated that the EIGRP routing protocol is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the show run and show ip route commands to help identify routing protocol-related problems.

Step 7: Configure a minimum password length.

**Note:** Passwords in this lab are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

Use the **security passwords** command to set a minimum password length of 10 characters.

R1(config)#security passwords min-length 10

Step 8: Configure the basic console and vty lines.

1. Configure a console password and enable login for router R1. For additional security, the exec-timeout command causes the line to log out after 5 minutes of inactivity. The logging synchronous command prevents console messages from interrupting command entry.

**Note:** To avoid repetitive logins during this lab, the exec-timeout can be set to 0 0, which prevents it from expiring. However, this is not considered a good security practice.

R1(config)#line console 0

R1(config-line)#password ciscoconpass

R1(config-line)#**exec-timeout 5 0**

R1(config-line)#login

R1(config-line)#logging synchronous

1. Configure the password on the vty lines for router R1.

R1(config)#line vty 0 4

R1(config-line)#password ciscovtypass

R1(config-line)#**exec-timeout 5 0**

R1(config-line)#login

1. Repeat these configurations on both R2 and R3.

Step 9: Encrypt clear text passwords.

1. Use the **service password-encryption** command to encrypt the console, aux, and vty passwords.

R1(config)#service password-encryption

1. Issue the show run command. Can you read the console, aux, and vty passwords? Why or why not?

|  |
| --- |
|  |
|  |
|  |
|  |

1. Repeat this configuration on both R2 and R3.

Step 10: Save the basic running configuration for all three routers.

1. Save the running configuration to the startup configuration from the privileged EXEC prompt.

R1#copy running-config startup-config

Step 11: Save the configuration on R1 and R3 for later restoration.

Use HyperTerminal or another means such as copy and paste to save the R1 and R3 running configurations from Part 1 of this lab and edit them so that they can be used to restore the routers in Part 3 of the lab to configure the VPN with SDM.

**Note:** When editing the captured running config text, remove all occurrences of “- - More - -.” Remove any commands that are not related to the items you configured in Part 1 of the lab, such as the Cisco IOS version number, no service pad, and so on. Many commands are entered automatically by the Cisco IOS software. Also replace the encrypted passwords with the correct ones specified previously and be sure to use the **no shutdown** command for interfaces that need to be enabled.

#### Part 2: Configure a Site-to-Site VPN with Cisco IOS

In Part 2 of this lab, you configure an IPsec VPN tunnel between R1 and R3 that passes through R2. You will configure R1 and R3 using the Cisco IOS CLI. You then review and test the resulting configuration.

### Task 1: Configure IPsec VPN Settings on R1 and R3

Step 1: Verify connectivity from the R1 LAN to the R3 LAN.

In this task, you verify that with no tunnel in place, the PC-A on the R1 LAN can ping the PC-C on R3 LAN.

1. From PC-A, ping the PC-C IP address of 192.168.3.3.

PC-A:\>ping 192.168.3.3

1. Were the results successful?

|  |
| --- |
|  |
|  |
|  |
|  |

1. If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 2: Enable IKE policies on R1 and R3.

IPsec is an open framework that allows the exchange of security protocols as new technologies, such as encryption algorithms, are developed.

There are two central configuration elements to the implementation of an IPsec VPN:

* Implement Internet Key Exchange (IKE) parameters
* Implement IPsec parameters

1. Verify that IKE is supported and enabled.

IKE Phase 1 defines the key exchange method used to pass and validate IKE policies between peers. In IKE Phase 2, the peers exchange and match IPsec policies for the authentication and encryption of data traffic.

IKE must be enabled for IPsec to function. IKE is enabled by default on IOS images with cryptographic feature sets. If it is disabled for some reason, you can enable it with the command **crypto isakmp enable**. Use this command to verify that the router IOS supports IKE and that it is enabled.

R1(config)#crypto isakmp enable

R3(config)#crypto isakmp enable

**Note:** If you cannot execute this command on the router, you need to upgrade the IOS image to one with a feature set that includes the Cisco cryptographic services.

1. Establish an Internet Security Association and Key Management Protocol (ISAKMP) policy and view the available options.

To allow IKE Phase 1 negotiation, you must create an ISAKMP policy and configure a peer association involving that ISAKMP policy. An ISAKMP policy defines the authentication and encryption algorithms and hash function used to send control traffic between the two VPN endpoints. When an ISAKMP security association has been accepted by the IKE peers, IKE Phase 1 has been completed. IKE Phase 2 parameters will be configured later.

Issue the **crypto isakmp policy** *number* configuration command on R1 for policy 10.

R1(config)#crypto isakmp policy 10

1. View the various IKE parameters available using Cisco IOS help by typing a question mark (?).

R1(config-isakmp)# ?

ISAKMP commands:

authentication Set authentication method for protection suite

default Set a command to its defaults

encryption Set encryption algorithm for protection suite

exit Exit from ISAKMP protection suite configuration mode

group Set the Diffie-Hellman group

hash Set hash algorithm for protection suite

lifetime Set lifetime for ISAKMP security association

no Negate a command or set its defaults

Step 3: Configure ISAKMP policy parameters on R1 and R3.

Your choice of an encryption algorithm determines how confidential the control channel between the endpoints is. The hash algorithm controls data integrity, ensuring that the data received from a peer has not been tampered with in transit. The authentication type ensures that the packet was indeed sent and signed by the remote peer. The Diffie-Hellman group is used to create a secret key shared by the peers that has not been sent across the network.

1. Configure an authentication type of pre-shared keys. Use AES 256 encryption, SHA as your hash algorithm, and Diffie-Hellman group 5 key exchange for this IKE policy.
2. Give the policy a life time of 3600 seconds (one hour). Configure the same policy on R3. Older versions of Cisco IOS do not support AES 256 encryption and SHA as a hash algorithm. Substitute whatever encryption and hashing algorithm your router supports. Be sure the same changes are made on the other VPN endpoint so that they are in sync.

**Note**: You should be at the R1(config-isakmp)# at this point. The crypto isakmp policy 10 command is repeated below for clarity.

R1(config)#crypto isakmp policy 10

R1(config-isakmp)#authentication pre-share

R1(config-isakmp)#encryption aes 256

R1(config-isakmp)#hash sha

R1(config-isakmp)#group 5

R1(config-isakmp)#lifetime 3600

R1(config-isakmp)#end

R3(config)#crypto isakmp policy 10

R3(config-isakmp)#authentication pre-share

R3(config-isakmp)#encryption aes 256

R3(config-isakmp)#hash sha

R3(config-isakmp)#group 5

R3(config-isakmp)#lifetime 3600

R3(config-isakmp)#end

1. Verify the IKE policy with the show crypto isakmp policy command.

R1#show crypto isakmp policy

Global IKE policy

Protection suite of priority 10

encryption algorithm: AES - Advanced Encryption Standard (256 bit keys).

hash algorithm: Secure Hash Standard

authentication method: Pre-Shared Key

Diffie-Hellman group: #5 (1536 bit)

lifetime: 3600 seconds, no volume limit

Step 4: Configure pre-shared keys.

1. Because pre-shared keys are used as the authentication method in the IKE policy, configure a key on each router that points to the other VPN endpoint. These keys must match for authentication to be successful. The global configuration command **crypto isakmp key** *key-string* **address** *address* is used to enter a pre-shared key. Use the IP address of the remote peer, the remote interface that the peer would use to route traffic to the local router.

Which IP addresses should you use to configure the IKE peers, given the topology diagram and IP addressing table?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

1. Each IP address that is used to configure the IKE peers is also referred to as the IP address of the remote VPN endpoint. Configure the pre-shared key of cisco123 on router R1 using the following command. Production networks should use a complex key. This command points to the remote peer R3 S0/0/1 IP address.

R1(config)#crypto isakmp key cisco123 address 10.2.2.1

1. The command for R3 points to the R1 S0/0/0 IP address. Configure the pre-shared key on router R1 using the following command.

R3(config)#crypto isakmp key cisco123 address 10.1.1.1

**Step 5: Configure the IPsec transform set and life times.**

1. The IPsec transform set is another crypto configuration parameter that routers negotiate to form a security association. To create an IPsec transform set, use the **crypto ipsec transform-set** *tag* parameters. Use **?** to see which parameters are available.

R1(config)#crypto ipsec transform-set 50 ?

ah-md5-hmac AH-HMAC-MD5 transform

ah-sha-hmac AH-HMAC-SHA transform

comp-lzs IP Compression using the LZS compression algorithm

esp-3des ESP transform using 3DES(EDE) cipher (168 bits)

esp-aes ESP transform using AES cipher

esp-des ESP transform using DES cipher (56 bits)

esp-md5-hmac ESP transform using HMAC-MD5 auth

esp-null ESP transform w/o cipher

esp-seal ESP transform using SEAL cipher (160 bits)

esp-sha-hmac ESP transform using HMAC-SHA auth

1. On R1 and R3, create a transform set with tag 50 and use an Encapsulating Security Protocol (ESP) transform with an AES 256 cipher with ESP and the SHA hash function. The transform sets must match.

R1(config)#crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac

R1(cfg-crypto-trans)#**exit**

R3(config)#crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac

R3(cfg-crypto-trans)#**exit**

1. What is the function of the IPsec transform set?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

1. You can also change the IPsec security association life times from the default of 3600 seconds or 4,608,000 kilobytes, whichever comes first. On R1 and R3, set the IPsec security association life time to 30 minutes, or 1800 seconds.

R1(config)#crypto ipsec security-association lifetime seconds 1800

R3(config)#crypto ipsec security-association lifetime seconds 1800

**Step 6: Define interesting traffic.**

1. To make use of the IPsec encryption with the VPN, it is necessary to define extended access lists to tell the router which traffic to encrypt. A packet that is permitted by an access list used for defining IPsec traffic is encrypted if the IPsec session is configured correctly. A packet that is denied by one of these access lists is not dropped, but sent unencrypted. Also, like any other access list, there is an implicit deny at the end, which, in this case, means the default action is to not encrypt traffic. If there is no IPsec security association correctly configured, no traffic is encrypted, and traffic is forwarded as unencrypted.
2. In this scenario, the traffic you want to encrypt is traffic going from R1’s Ethernet LAN to R3’s Ethernet LAN, or vice versa. These access lists are used outbound on the VPN endpoint interfaces and must mirror each other.
3. Configure the IPsec VPN interesting traffic ACL on R1.

R1(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

1. Configure the IPsec VPN interesting traffic ACL on R3.

R3(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

1. Does IPsec evaluate whether the access lists are mirrored as a requirement to negotiate its security association?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

**Step 7: Create and apply a crypto map.**

A crypto map associates traffic that matches an access list to a peer and various IKE and IPsec settings. After the crypto map is created, it can be applied to one or more interfaces. The interfaces that it is applied to should be the ones facing the IPsec peer.

1. To create a crypto map, use the global configuration command **crypto map** *name sequence-num type* to enter the crypto map configuration mode for that sequence number. Multiple crypto map statements can belong to the same crypto map and are evaluated in ascending numerical order. Enter the crypto map configuration mode on R1. Use a type of ipsec-isakmp, which means IKE is used to establish IPsec security associations.
2. Create the crypto map on R1, name it CMAP, and use 10 as the sequence number. A message will display after the command is issued.

R1(config)#crypto map CMAP 10 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

1. Use the **match address** *access-list* command to specify which access list defines which traffic to encrypt.

R1(config-crypto-map)#match address 101

1. To view the list of possible **set** commands that you can do in a crypto map, use the help function.

R1(config-crypto-map)#set ?

Identity Identity restriction.

Ip Interface Internet Protocol config commands

isakmp-profile Specify isakmp Profile

nat Set NAT translation

peer Allowed Encryption/Decryption peer.

pfs Specify pfs settings

security-association Security association parameters

transform-set Specify list of transform sets in priority order

1. Setting a peer IP or host name is required, so set it to R3’s remote VPN endpoint interface using the following command.

R1(config-crypto-map)#set peer 10.2.2.1

1. Hard code the transform set to be used with this peer, using the **set transform-set** *tag* command. Set the perfect forwarding secrecy type using the **set pfs** *type* command, and also modify the default IPsec security association life time with the **set security-association lifetime seconds** *seconds* command.

R1(config-crypto-map)#set pfs group5

R1(config-crypto-map)#set transform-set 50

R1(config-crypto-map)#set security-association lifetime seconds 900

R1(config-crypto-map)#**exit**

1. Create a mirrored matching crypto map on R3.

R3(config)#crypto map CMAP 10 ipsec-isakmp

R3(config-crypto-map)#match address 101

R3(config-crypto-map)#set peer 10.1.1.1

R3(config-crypto-map)#set pfs group5

R3(config-crypto-map)#set transform-set 50

R3(config-crypto-map)#set security-association lifetime seconds 900

R3(config-crypto-map)#**exit**

1. The last step is applying the maps to interfaces. Note that the security associations (SAs) will not be established until the crypto map has been activated by interesting traffic. The router will generate a notification that crypto is now on.
2. Apply the crypto maps to the appropriate interfaces on R1 and R3.

R1(config)#interface S0/0/0

R1(config-if)#crypto map CMAP

\*Jan 28 04:09:09.150: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON

R1(config)#end

R3(config)#interface S0/0/1

R3(config-if)#crypto map CMAP

\*Jan 28 04:10:54.138: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON

R3(config)#end

### Sub Task 2: Verify Site-to-Site IPsec VPN Configuration

Step 1: Verify the IPsec configuration on R1 and R3.

1. Previously, you used the **show crypto isakmp policy** command to show the configured ISAKMP policies on the router. Similarly, the **show crypto ipsec transform-set** command displays the configured IPsec policies in the form of the transform sets.

R1#show crypto ipsec transform-set

Transform set 50: { esp-256-aes esp-sha-hmac }

will negotiate = { Tunnel, },

Transform set #$!default\_transform\_set\_1: { esp-aes esp-sha-hmac }

will negotiate = { Transport, },

Transform set #$!default\_transform\_set\_0: { esp-3des esp-sha-hmac }

will negotiate = { Transport, },

R3#show crypto ipsec transform-set

Transform set 50: { esp-256-aes esp-sha-hmac }

will negotiate = { Tunnel, },

Transform set #$!default\_transform\_set\_1: { esp-aes esp-sha-hmac }

will negotiate = { Transport, },

Transform set #$!default\_transform\_set\_0: { esp-3des esp-sha-hmac }

will negotiate = { Transport, },

1. Use the **show crypto map** command to display the crypto maps that will be applied to the router.

R1#show crypto map

Crypto Map "CMAP" 10 ipsec-isakmp

Peer = 10.2.2.1

Extended IP access list 101

access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

Current peer: 10.2.2.1

Security association lifetime: 4608000 kilobytes/900 seconds

PFS (Y/N): Y

DH group: group5

Transform sets={

50: { esp-256-aes esp-sha-hmac } ,

}

Interfaces using crypto map MYMAP: Serial0/0/0

R3#show crypto map

Crypto Map "CMAP" 10 ipsec-isakmp

Peer = 10.1.1.1

Extended IP access list 101

access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

Current peer: 10.1.1.1

Security association lifetime: 4608000 kilobytes/900 seconds

PFS (Y/N): Y

DH group: group5

Transform sets={

50: { esp-256-aes esp-sha-hmac } ,

}

Interfaces using crypto map MYMAP: Serial0/0/1

**Note:** The output of these **show** commands does not change if interesting traffic goes across the connection. You test various types of traffic in the next task.

### Sub Task 3: Verify IPsec VPN Operation

Step 1: Display isakmp security associations.

The **show crypto isakmp sa** command reveals that no IKE SAs exist yet. When interesting traffic is sent, this command output will change.

R1#show crypto isakmp sa

dst src state conn-id slot status

Step 2: Display IPsec security associations.

1. The **show crypto ipsec sa** command shows the unused SA between R1 and R3. Note the number of packets sent across and the lack of any security associations listed toward the bottom of the output. The output for R1 is shown here.

R1#show crypto ipsec sa

interface: Serial0/0/0

Crypto map tag: CMAP, local addr 10.1.1.1

protected vrf: (none)

local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)

current\_peer 10.2.2.1 port 500

PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0

#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

#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.: 10.1.1.1, remote crypto endpt.: 10.2.2.1

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0

current outbound spi: 0x0(0)

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:

1. Why have no security associations (SAs) been negotiated?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

1. Step 3: Generate some uninteresting test traffic and observe the results.
2. Ping from R1 to the R3 S0/0/1 interface IP address 10.2.2.1. Were the pings successful?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

1. Issue the **show crypto isakmp sa** command. Was an SA created between R1 and R3?

|  |
| --- |
|  |
|  |
|  |
|  |

1. Ping from R1 to the R3 Fa01 interface IP address 192.168.3.1. Were the pings successful?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

1. Issue the **show crypto isakmp sa** command again. Was an SA created for these pings? Why or why not?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

1. Issue the command **debug eigrp packets**. You should see EIGRP hello packets passing between R1 and R3.

R1#debug eigrp packets

EIGRP Packets debugging is on

(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)

R1#

\*Jan 29 16:05:41.243: EIGRP: Received HELLO on Serial0/0/0 nbr 10.1.1.2

\*Jan 29 16:05:41.243: AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 pe

erQ un/rely 0/0

\*Jan 29 16:05:41.887: EIGRP: Sending HELLO on Serial0/0/0

\*Jan 29 16:05:41.887: AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0

R1#

\*Jan 29 16:05:43.143: EIGRP: Sending HELLO on FastEthernet0/1

\*Jan 29 16:05:43.143: AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0

R1#

1. Turn off debugging with the no **debug eigrp packets** or **undebug all** command.
2. Issue the **show crypto isakmp sa** command again. Was an SA created between R1 and R3? Why or why not?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

Step 4: Generate some interesting test traffic and observe the results.

1. Use an extended ping from R1 to the R3 Fa01 interface IP address 192.168.3.1. Extended ping allows you to control the source address of the packets. Respond as shown in the following example. Press enter to accept the defaults, except where a specific response is indicated.

R1#ping

Protocol [ip]:

Target IP address: 192.168.3.1

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface: 192.168.1.1

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:

Packet sent with a source address of 192.168.1.1

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 92/92/92 ms

1. Issue the **show crypto isakmp sa** command again.

R1#show crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst src state conn-id slot status

10.2.2.1 10.1.1.1 QM\_IDLE 1001 0 ACTIVE

1. Why was an SA created between R1 and R3 this time?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

1. What are the endpoints of the IPsec VPN tunnel?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

1. Ping from PC-A to PC-C. Were the pings successful?

|  |
| --- |
|  |
|  |
|  |
|  |

1. Issue the **show crypto ipsec sa** command. How many packets have been transformed between R1 and R3?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

R1#**show crypto ipsec sa**

interface: Serial0/0/0

Crypto map tag: CMAP, local addr 10.1.1.1

protected vrf: (none)

local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)

current\_peer 10.2.2.1 port 500

PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9

#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9

#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.: 10.1.1.1, remote crypto endpt.: 10.2.2.1

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0

current outbound spi: 0xC1DD058(203280472)

inbound esp sas:

spi: 0xDF57120F(3747025423)

transform: esp-256-aes esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2005, flow\_id: FPGA:5, crypto map: CMAP

sa timing: remaining key lifetime (k/sec): (4485195/877)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0xC1DD058(203280472)

transform: esp-256-aes esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2006, flow\_id: FPGA:6, crypto map: CMAP

sa timing: remaining key lifetime (k/sec): (4485195/877)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE

outbound ah sas:

outbound pcp sas:

1. The previous example used pings to generate interesting traffic. What other types of traffic would result in an SA forming and tunnel establishment?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

#### Part 3: Configure a Site-to-Site IPsec VPN with SDM

In Part 3 of this lab, you configure an IPsec VPN tunnel between R1 and R3 that passes through R2. In Task 2, you configure R1 using Cisco SDM. In Task 3, you mirror those settings to R3 using SDM utilities. You then review and test the resulting configuration.

### Sub Task 1: Restore Router R1 and R3 to the Basic Settings

To avoid confusion as to what was entered in Part 2 of the lab, start by restoring R1 and R3 to the basic configuration as described in Part 1 of this lab.

Step 1: Erase and reload the router.

1. Connect to the router console, and enter privileged EXEC mode.
2. Erase the startup config and then issue the **reload** command to restart the router.

Step 2: Restore the basic configuration.

1. When the router restarts, enter privileged EXEC mode with the enable command, and then enter global config mode. Use the HyperTerminal **Transfer > Send File** function, copy and paste or use another method to load the basic startup config for R1 and R3 that was created and saved in Part 1 of this lab.
2. Save the running config to the startup config for R1 and R3 using the copy run start command.
3. Test connectivity by pinging from host PC-A to PC-C. If the pings are not successful, troubleshoot the router and PC configurations before continuing.

### Task 2: Configure IPsec VPN Settings on R1 Using SDM

Step 1: Configure the enable secret password and HTTP router access prior to starting SDM.

1. From the CLI, configure the enable secret password for use with SDM on R1 and R3.

R1(config)#enable secret cisco12345

R3(config)#enable secret cisco12345

1. Enable the HTTP server on R1 and R3.

R1(config)#ip http server

R3(config)#ip http server

Step 2: Access SDM and set command delivery preferences.

1. Run the SDM application, or open a browser on PC-A and start SDM by entering the R1 IP address 192.168.1.1 in the address field.

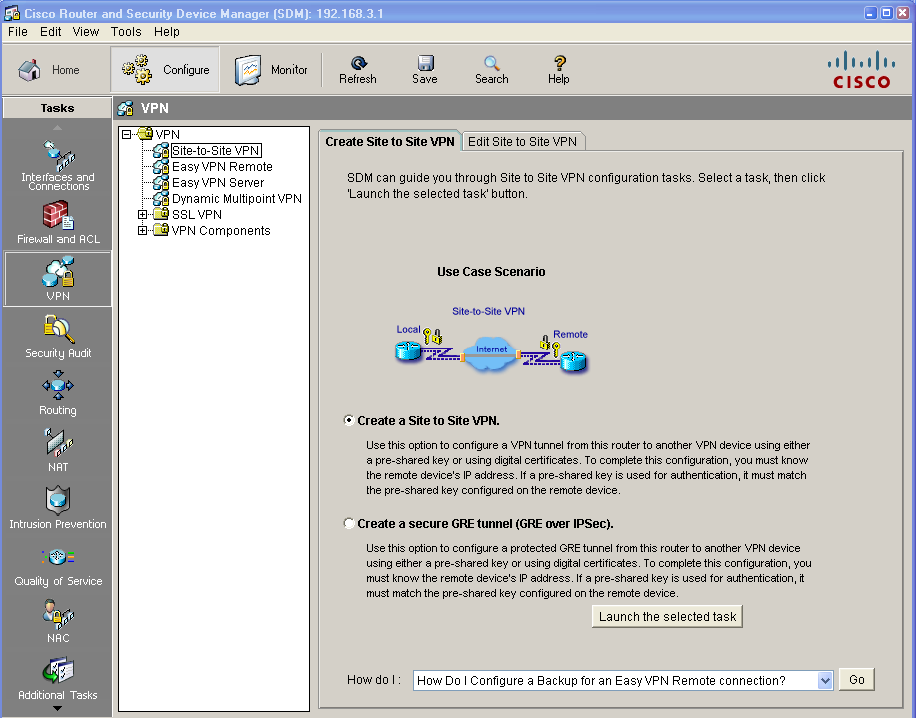
**Note:** You might be prompted by Internet Explorer to allow ActiveX during several of these steps. Click **Allow**.

1. Log in with no username and the enable secret password **cisco12345**.
2. In the Authentication Required dialog box, leave the Username field blank and enter **cisco12345** in the Password field. Click **Yes**.
3. If the IOS IPS login dialog displays, click the **Cancel** button to bypass this option.
4. Select **Edit** > **Preferences** to configure SDM to allow you to preview the commands before sending them to the router. In the User Preferences window, check the **Preview commands before delivering to router** check box and click **OK**.

Step 3: Start the SDM VPN wizard to configure R1.

1. Click the **Configure** button at the top of the SDM screen, and then click the **VPN** button. Select **Site-to-Site VPN** from the list of options. The default option is Create Site-to-Site VPN. Read through the description of this option.
2. What must you know to complete the configuration?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |



1. Click the **Launch the selected task** button to begin the SDM Site-to-Site VPN wizard.
2. On the initial Site-to-Site VPN wizard window, the **Quick Setup** option is selected by default. Click the **View Details** button to see what settings this option uses. What type of encryption does the default transform set use?

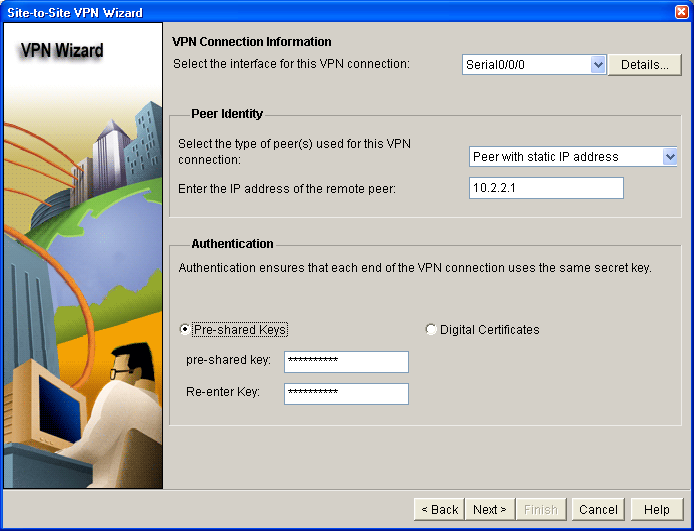
|  |
| --- |
|  |
|  |
|  |
|  |

1. From the initial Site-to-Site VPN wizard window, select the Step by Step wizard, and then click Next. Why would you use this option over the Quick setup option?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

Step 4: Configure basic VPN connection information settings.

1. From the VPN Connection Information window, select the interface for the connection, which should be R1 Serial0/0/0.
2. In the Peer Identity section, select **Peer with static address** and enter the IP address of remote peer R3 S0/0/1 (10.2.2.1).
3. In the Authentication section, click **Pre-shared keys**, and enter the pre-shared VPN key **cisco12345**. Re-enter the key for confirmation. This key is what protects the VPN and keeps it secure. When finished, your screen should look similar to the following. Once you have entered these settings correctly, click **Next**.



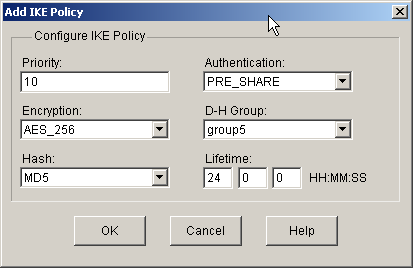
Step 5: Configure IKE policy parameters.

IKE policies are used while setting up the control channel between the two VPN endpoints for key exchange. This is also referred to as the IKE secure association (SA). In contrast, the IPsec policy is used during IKE Phase II to negotiate an IPsec security association to pass target data traffic.

1. In the IKE Proposals window, a default policy proposal is displayed. You can use this one or create a new one. What function does this IKE proposal serve?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

1. Click the **Add** button to create a new IKE policy.
2. Set up the security policy as shown in the Add IKE Policy dialog box below. These settings are matched later on R3. When finished, click **OK** to add the policy. Then click **Next.**



1. Click the **Help** button to assist you with answering the following questions. What is the function of the encryption algorithm in the IKE policy?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

1. What is the purpose of the hash function?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

1. What function does the authentication method serve?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

1. How is the Diffie-Hellman group in the IKE policy used?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

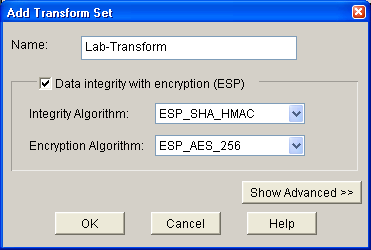
1. What event happens at the end of the IKE policy’s lifetime?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

Step 6: Configure a transform set.

The transform set is the IPsec policy used to encrypt, hash, and authenticate packets that pass through the tunnel. The transform set is the IKE Phase 2 policy.

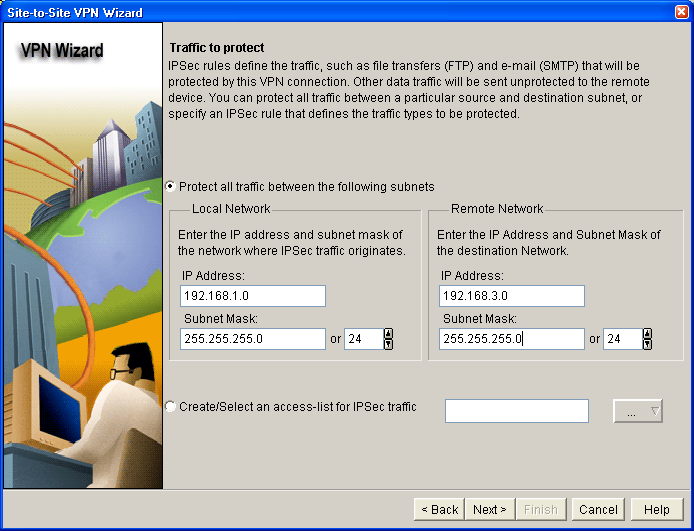
1. An SDM default transform set is displayed. Click the **Add** button to create a new transform set.
2. Set up the transform set as shown in the Transform Set dialog box below. These settings are matched later on R3. When finished, click **OK** to add the transform set. Then click **Next.**



Step 7: Define interesting traffic.

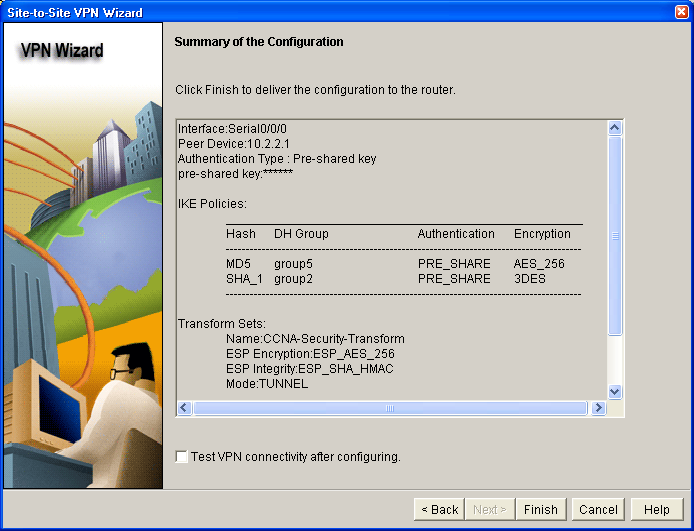
You must define interesting traffic to be protected through the VPN tunnel. Interesting traffic will be defined through an access list when applied to the router. If you enter source and destination subnets, SDM generates the appropriate simple access list for you.

In the Traffic to protect window, enter the information as shown below. These are the opposite of the settings configured on R3 later in the lab. When finished, click **Next.**



Step 8: Review the summary configuration and deliver commands to the router.

1. Review the summary of the Configuration window. It should look similar to the one below. Do not select the checkbox for Test VPN connectivity after configuring. This is done after configuring R3.



1. In the Deliver Configuration to router window, select **Save running config to router’s startup config** and click the **Deliver** button. After the commands have been delivered, click **OK**. How many commands were delivered?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

### Sub Task 3: Create a Mirror Configuration for R3

Step 1: Use SDM on R1 to generate a mirror configuration for R3.

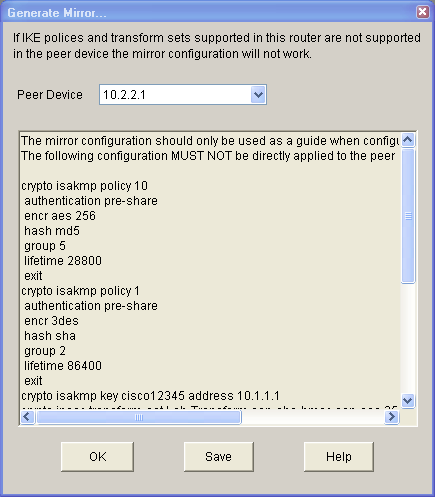
1. On R1, select **VPN > Site-to-Site VPN** and click the **Edit Site-to-Site VPN** tab. You should see the VPN configuration you just created on R1 listed. What is the description of the VPN?

|  |
| --- |
|  |
|  |
|  |
|  |

1. What is the status of the VPN and why?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

1. Select the VPN policy you just configured on R1 and click the **Generate Mirror** button in the lower right of the window. The Generate Mirror window displays the commands necessary to configure R3 as a VPN peer. Scroll through the window to see all the commands generated.



1. The text at the top of the window states that the configuration generated should only be used as a guide for setting up a site-to-site VPN. What commands are missing to allow this crypto policy to function on R3?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

**Hint:** Look at the description entry following the **crypto map SDM\_CMAP\_1** command.

Step 2: Save the configuration commands for R3.

1. Click the **Save** button to create a text file for use in the next task.
2. Save the commands to the desktop or other location and name it VPN-Mirror-Cfg-for-R3.txt.

**Note:** You can also copy the commands directly from the **Generate Mirror** window.

1. (Optional) Edit the file to remove the explanation text at the beginning and the description entry following the **crypto map SDM\_CMAP\_1** command.

### Sub Task 4: Apply the Mirror Configuration to R3 and Verify the Configuration

Step 1: Access the R3 CLI and copy the mirror commands.

**Note:** You can also use SDM on R3 to create the appropriate VPN configuration, but copying and pasting the mirror commands generated from R1 is easier.

1. On R3, enter privileged EXEC mode and then global config mode.
2. Copy the commands from the text file into the R3 CLI.

Step 2: Apply the crypto map to the R3 S0/0/1 interface.

R3(config)#interface s0/0/1

R3(config-if)#crypto map SDM\_CMAP\_1

\*Jan 30 13:00:38.184: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON

Step 3: Verify the VPN configuration on R3 using Cisco IOS.

1. Display the running config beginning with the first line that contains the string “0/0/1” to verify that the crypto map is applied to S0/0/1.

R3#sh run | beg 0/0/1

interface Serial0/0/1

ip address 10.2.2.1 255.255.255.252

crypto map SDM\_CMAP\_1

1. On R3, use the **show crypto isakmp policy** command to show the configured ISAKMP policies on the router. Note that the default SDM policy is also present.

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

Protection suite of priority 10

encryption algorithm: AES - Advanced Encryption Standard (256 bit keys

).

hash algorithm: Message Digest 5

authentication method: Pre-Shared Key

Diffie-Hellman group: #5 (1536 bit)

lifetime: 28800 seconds, no volume limit

1. In the above output, how many ISAKMP policies are there?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

1. Issue the **show crypto ipsec transform-set** command to display the configured IPsec policies in the form of the transform sets.

R3#show crypto ipsec transform-set

Transform set Lab-Transform: { esp-256-aes esp-sha-hmac }

will negotiate = { Tunnel, },

Transform set #$!default\_transform\_set\_1: { esp-aes esp-sha-hmac }

will negotiate = { Transport, },

Transform set #$!default\_transform\_set\_0: { esp-3des esp-sha-hmac }

will negotiate = { Transport, },

1. Use the **show crypto map** command to display the crypto maps that will be applied to the router.

R3#show crypto map

Crypto Map "SDM\_CMAP\_1" 1 ipsec-isakmp

Description: Apply the crypto map on the peer router's interface having

IP address 10.2.2.1 that connects to this router.

Peer = 10.1.1.1

Extended IP access list SDM\_1

access-list SDM\_1 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

Current peer: 10.1.1.1

Security association lifetime: 4608000 kilobytes/3600 seconds

PFS (Y/N): N

Transform sets={

Lab-Transform: { esp-256-aes esp-sha-hmac } ,

}

Interfaces using crypto map SDM\_CMAP\_1:

Serial0/0/1

1. In the above output, the ISAKMP policy being used by the crypto map is the SDM default policy with sequence number priority 1, indicated by the number 1 in the first output line: Crypto Map “SDM\_CMAP\_1” 1 ipsec-isakmp. Why is it not using the one you created in the SDM session — the one shown with priority 10 in Step 3b above?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

1. (Optional) You can force the routers to use the more stringent policy that you created by changing the crypto map references in the R1 and R3 router configs as shown below. If this is done, the default ISAKMP policy 1 can be removed from both routers.

R1(config)#interface s0/0/0

R1(config-if)#no crypto map SDM\_CMAP\_1

R1(config-if)#exit

\*Jan 30 17:01:46.099: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is OFF

R1(config)#no crypto map SDM\_CMAP\_1 1

R1(config)#crypto map SDM\_CMAP\_1 10 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

R1(config-crypto-map)#description Tunnel to 10.2.2.1

R1(config-crypto-map)#set peer 10.2.2.1

R1(config-crypto-map)#set transform-set Lab-Transform

R1(config-crypto-map)#match address 100

R1(config-crypto-map)#exit

R1(config)#int s0/0/0

R1(config-if)#crypto map SDM\_CMAP\_1

R1(config-if)#e

\*Jan 30 17:03:16.603: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON

R3(config)#interface s0/0/1

R3(config-if)#no crypto map SDM\_CMAP\_1

R3(config-if)#exit

R3(config)#no crypto map SDM\_CMAP\_1 1

R3(config)#crypto map SDM\_CMAP\_1 10 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

R3(config-crypto-map)#description Tunnel to 10.1.1.1

R3(config-crypto-map)#set peer 10.1.1.1

R3(config-crypto-map)#set transform-set Lab-Transform

R3(config-crypto-map)#match address 100

R3(config-crypto-map)#exit

R3(config)#int s0/0/1

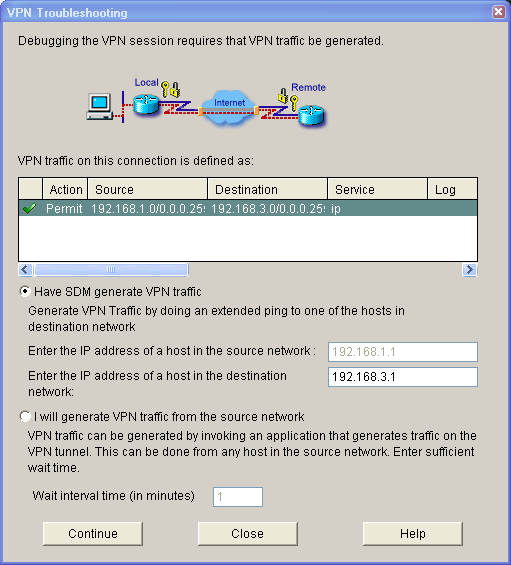
R3(config-if)#crypto map SDM\_CMAP\_1

R3(config-if)#

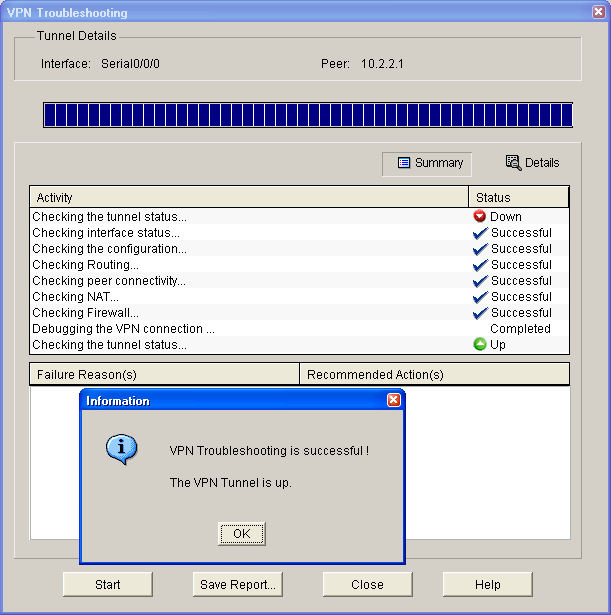
\*Jan 30 22:18:28.487: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON

**Sub Task 5: Test the VPN Configuration Using SDM on R1.**

1. On R1, use SDM to test the IPsec VPN tunnel between the two routers. Select **VPN > Site-to-Site VPN** and click the **Edit Site-to-Site VPN** tab.
2. From the Edit Site to Site VPN tab, select the VPN and click **Test Tunnel**.
3. When the VPN Troubleshooting window displays, click the **Start** buttonto have SDM start troubleshooting the tunnel.
4. When the SDM Warning window displays indicating that SDM will enable router debugs and generate some tunnel traffic, click **Yes** to continue.
5. In the next VPN Troubleshooting window, the IP address of the R1 Fa0/1 interface in the source network is displayed by default (192.168.1.1). Enter the IP address of the R3 Fa0/1 interface in the destination network field (192.168.3.1) and click **Continue** to begin the debugging process.



1. If the debug is successful and the tunnel is up, you should see the screen below. If the testing fails, SDM displays failure reasons and recommended actions. Click **OK** to remove the window.



1. You can save the report if desired; otherwise, click **Close**.

**Note:** If you want to reset the tunnel and test again, you can click the **Clear Connection** button from the Edit Suite-to-Site VPN window. This can also be accomplished at the CLI using the **clear crypto session** command.

1. Display the running config for R3 beginning with the first line that contains the string 0/0/1 to verify that the crypto map is applied to S0/0/1.

R3#sh run | beg 0/0/1

interface Serial0/0/1

ip address 10.2.2.1 255.255.255.252

crypto map SDM\_CMAP\_1

<output omitted>

1. Issue the **show crypto isakmp sa** command on R3 to view the security association created.

R3#show crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst src state conn-id slot status

10.2.2.1 10.1.1.1 QM\_IDLE 1001 0 ACTIVE

1. Issue the **show crypto ipsec sa** command. How many packets have been transformed between R1 and R3?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

R3#show crypto ipsec sa

interface: Serial0/0/1

Crypto map tag: SDM\_CMAP\_1, local addr 10.2.2.1

protected vrf: (none)

local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)

current\_peer 10.1.1.1 port 500

PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 116, #pkts encrypt: 116, #pkts digest: 116

#pkts decaps: 116, #pkts decrypt: 116, #pkts verify: 116

#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.: 10.2.2.1, remote crypto endpt.: 10.1.1.1

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/1

current outbound spi: 0x207AAD8A(544910730)

inbound esp sas:

spi: 0xAF102CAE(2937072814)

transform: esp-256-aes esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2007, flow\_id: FPGA:7, crypto map: SDM\_CMAP\_1

sa timing: remaining key lifetime (k/sec): (4558294/3037)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x207AAD8A(544910730)

transform: esp-256-aes esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2008, flow\_id: FPGA:8, crypto map: SDM\_CMAP\_1

sa timing: remaining key lifetime (k/sec): (4558294/3037)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE

outbound ah sas:

outbound pcp sas:

### Sub Task 6: Reflection

1. Would traffic on the Fast Ethernet link between PC-A and the R1 Fa0/0 interface be encrypted by the site-to-site IPsec VPN tunnel? Why or why not?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

1. What are some factors to consider when configuring site-to-site IPsec VPNs using the manual CLI compared to using the SDM VPN wizard GUI?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

Router Interface Summary Table

| Router Interface Summary | | | | |
| --- | --- | --- | --- | --- |
| Router Model | Ethernet Interface #1 | Ethernet Interface #2 | Serial Interface #1 | Serial Interface #2 |
| 1700 | Fast Ethernet 0 (FA0) | Fast Ethernet 1 (FA1) | Serial 0 (S0) | Serial 1 (S1) |
| 1800 | Fast Ethernet 0/0 (FA0/0) | Fast Ethernet 0/1 (FA0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2600 | Fast Ethernet 0/0 (FA0/0) | Fast Ethernet 0/1 (FA0/1) | Serial 0/0 (S0/0) | Serial 0/1 (S0/1) |
| 2800 | Fast Ethernet 0/0 (FA0/0) | Fast Ethernet 0/1 (FA0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| **Note:** To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface. | | | | |

**Task 2 – WAN Link Installation and Network Element Configuration**

This assessment task requires the installation of, as required:

* adaptors
* communications cables and connectors
* hubs
* routers
* servers
* switches

For the purposes of creation WAN Links and configuring IP Services. This includes:

* planning and preparing for the wide area network (WAN) link installation task
* installing and configuring WAN links
* configure and troubleshooting the following internet protocol (IP) services:
* network address translation (NAT)
* dynamic host configuration protocol (DHCP)
* access control lists (ACLs)
* configure and troubleshoot ADSL links
* configure and troubleshoot VPNs
* document solutions.

The installation may be for a client whuch can include:

* external organisations
* individuals
* internal departments
* internal employees

Which may be an actual workplace environment or simulated within your practice environment. Where a simulated environment is used, your Assessor will take the role of the client.

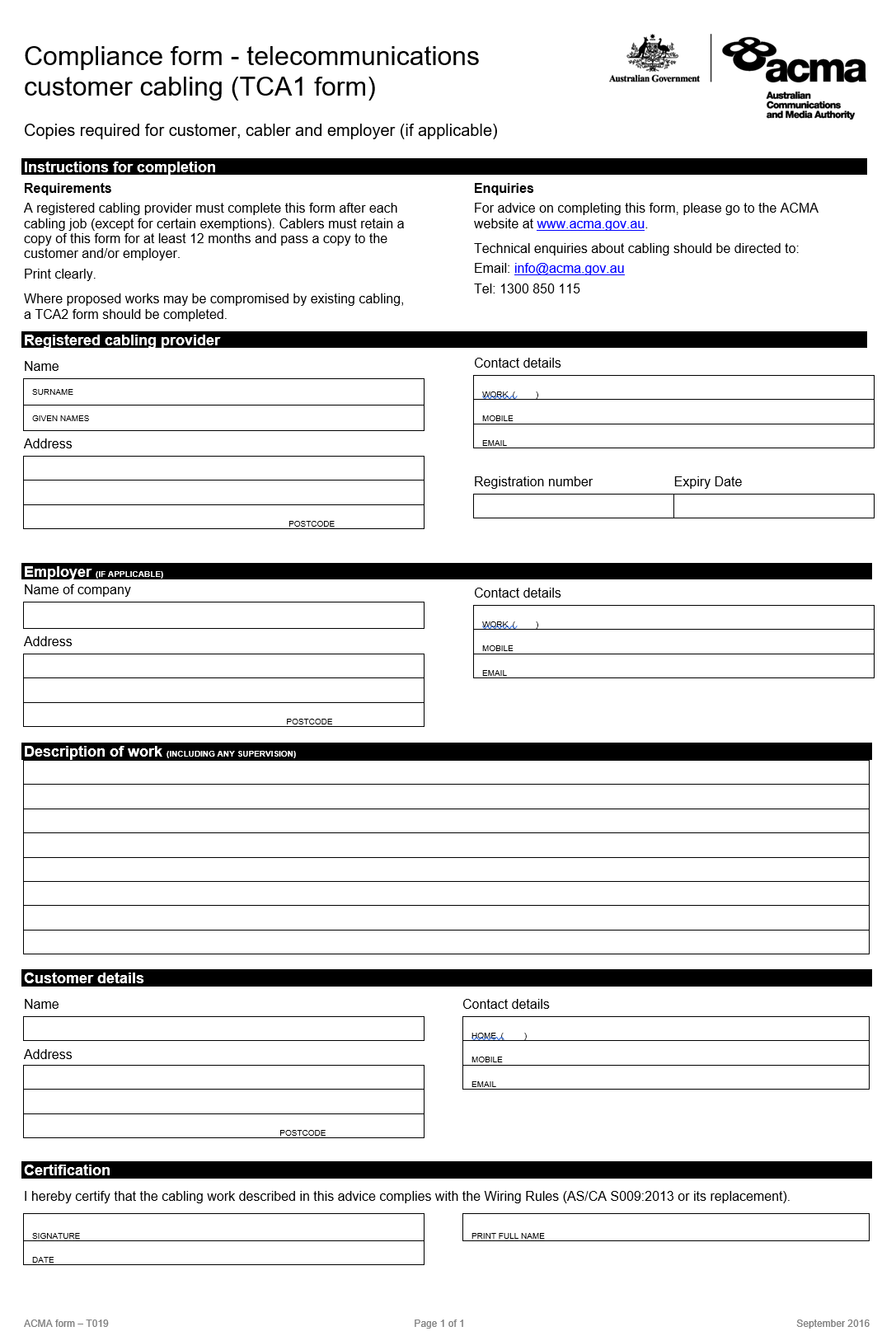
Create documentation to include:

* equipment inventory
* International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and Australian Standards (AS) standards
* naming standards
* project management templates and report writing
* satisfaction reports
* version control.

and complete the attached cabling compliance form for any cabling installed.

The following must be installed, tested and verified and Assessment includes demonstration of the satisfactory function of the network services:

* DHCP
* NAT
* ACL
* VPN
* ADSL

****



**ICTNWK506 Configure, verify and troubleshoot WAN links and IP services in a medium enterprise network**

**Assessment Outcome Record**

In order to be deemed competent in this unit, the candidate must answer all written questions correctly and satisfactorily complete all practical tasks. In order to complete all practical tasks, all Observation Criteria need to be satisfied, i.e. demonstrated and marked as an 'S'. The task summary outcome must be noted as satisfactory to note the demonstration of a satisfactory outcome for each practical task requirement.

|  |  |
| --- | --- |
| Student Name |  |
| 🞎 Not Yet Competent | 🞎 Competent |
| Comments | |
|  | |
|  | |
|  | |
|  | |
|  | |

|  |  |
| --- | --- |
| Assessor (Name) |  |
| Assessor Signature |  |
| Date |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Student Feedback Form** | | | | | | | | |
| **Unit** | **ICTNWK506 Configure, verify and troubleshoot WAN links and IP services in a medium enterprise network** | | | | | | | |
| **Student Name:** |  | | Date | | |  | | |
| **Assessor Name:** |  | | | | | | | |
| Please provide us some feedback on your assessment process. Information provided on this form is used for evaluation of our assessment systems and processes.  This information is confidential and is not released to any external parties without your written consent. There is no need to sign your name as your feedback is confidential. | | | | | | | | |
|  | | **Strongly**  **Disagree** | |  | **Agree** | |  | **Strongly**  **Agree** |
| I received information about the assessment requirements prior to undertaking the tasks | | 1 | | 2 | 3 | | 4 | 5 |
| The assessment instructions were clear and easy to understand | | 1 | | 2 | 3 | | 4 | 5 |
| I understood the purpose of the assessment | | 1 | | 2 | 3 | | 4 | 5 |
| The assessment meet your expectation | | 1 | | 2 | 3 | | 4 | 5 |
| My Assessor was organised and well prepared | | 1 | | 2 | 3 | | 4 | 5 |
| The assessment was Fair, Valid, Flexible and Reliable | | 1 | | 2 | 3 | | 4 | 5 |
| My Assessor's conduct was professional | | 1 | | 2 | 3 | | 4 | 5 |
| The assessment was an accurate reflection of the unit requirements | | 1 | | 2 | 3 | | 4 | 5 |
| I was comfortable with the outcome of the assessment | | 1 | | 2 | 3 | | 4 | 5 |
| I received feedback about assessments I completed | | 1 | | 2 | 3 | | 4 | 5 |
| The pace of this unit was: | | Too Slow | |  | Great  Pace | |  | Too Fast |
| **Comments:** | | | | | | | | |
|  | | | | | | | | |
|  | | | | | | | | |
|  | | | | | | | | |

**Please return this completed form to Reception once you have completed this unit of competency.**