

---

---

## Chapter 2 Configuration

### Configuring the Perimeter Firewall

If the satellite MTL is behind a perimeter firewall, it needs to be configured to allow the VPN traffic both to the 2640 VPN Router and to the 5001 VPN server.

Since we use IPSec protocol for VPN connections, the following ports need to be opened on the firewall:

IP port	Source	Destination
UDP 500	Any	Cisco2640 & CVPN 5001 routers
IP protocol 50	Any	Cisco2640 & CVPN 5001 routers
IP protocol 51	Any	Cisco2640 & CVPN 5001 routers

**NOTE:** Additional IP ports may need to be opened if FTCs in MTL need Internet access.

### Configuring the 2640 VPN Router

The VPN Router 2640 is used primarily to set up and manage the VPN with the master MTL as a lan-to-lan VPN router, but it can also be used for accessing/providing internet access to MTL and management system and for providing routing between VLANs.

1. Once you connect your console cable to the router and power it on, you will see a message similar to the following:

---

```
--- System Configuration Dialog ---  
Would you like to enter the initial configuration dialog? [yes/no]:
```

---

2. Answer “no” and continue. You may need to hit “enter” a few times to get past system messages, until you get to the system prompt:

---

```
Router>
```

---

- 
3. Type “enable” and then “config t” to get into **enable** mode and begin to configure the router. The enable or privileged mode access is required to make changes to the router, and the actual changes are made from the configuration mode.

---

```
Router> enable
Router# config t
Router(config)#
```

---

4. Set the Hostname for the router (this is done for descriptive purposes only).

---

```
Router(config)# hostname 2640
2640(config)#
```

---

5. Set the “enable secret” to “cisco”. The “enable secret” is an encrypted password that protects privileged mode access.

---

```
2640(config)# enable secret <password>
```

---

6. Now, set up and enforce protection of the telnet line so that only the Configuration server at 10.10.1.4 can access the 2640 via telnet. First create an access list that defines who will be allowed to telnet to the 2640.

---

```
2640(config)# access-list 10 permit host 10.10.60.3
```

---

7. Next, apply it to the telnet “lines”.

---

```
2640(config)# line vty 0 15
2640(config-line)# access-class 10 in
```

---

8. You also need to apply the telnet password of “cisco”.

---

```
2640(config-line)# password <password>
```

---

9. Configure the router so that it does not try to resolve typos to DNS. This is not required, but it is a good precaution for a bad typist since any typing mistakes will disable the router that may be trying to resolve those typos.

---

```
2640(config)# no ip domain-lookup
```

---

10. Now, you are ready to configure the physical interfaces on Cisco 2640. For each interface, configure the IP address, set the interface to full duplex and 100mbps. Take it out of administrative shutdown.

We will use FastEthernet 0/0 as the external address that faces the PIX, and FastEthernet0/1 as the internal interface that faces “e-utilica”.

---

```
2640(config)# interface FastEthernet0/0
2640(config-if)# ip address <Public IP & Netmask>
2640(config-if)# duplex full
2640(config-if)# speed 100
2640(config-if)# no shutdown
```

---

- 
11. Once you have configured the interface, exit the interface configuration mode.
- 

```
2640(config-if)# exit
2640(config)#
```

---

12. The interface FastEthernet0/1 also provides routing between VLANs. Therefore, you need to create sub interfaces for each VLAN and assign an IP address for each sub interface:
- 

```
2640(config)# interface FastEthernet0/1
2640(config-if)# ip address 10.10.60.2 255.255.255.0
2640(config-if)# duplex full
2640(config-if)# speed 100
2640(config-if)# no shutdown
2640(config-if)# exit
```

```
2640(config)# interface FastEthernet0/1.1
2640(config-if)# encapsulation dot1Q 5
2640(config-if)# ip address 10.10.50.1 255.255.255.0
2640(config-if)# no shutdown
2640(config-if)# exit
```

```
2640(config)# interface FastEthernet0/1.2
2640(config-if)# encapsulation dot1Q 6
2640(config-if)# ip address 10.10.51.1 255.255.255.0
2640(config-if)# no shutdown
2640(config-if)# exit
```

```
2640(config)# interface FastEthernet0/1.3
2640(config-if)# encapsulation dot1Q 7
2640(config-if)# ip address 10.10.53.1 255.255.255.0
2640(config-if)# no shutdown
2640(config-if)# exit
```

```
2640(config)# interface FastEthernet0/1.4
2640(config-if)# encapsulation dot1Q 8
2640(config-if)# ip address 10.10.54.1 255.255.255.0
2640(config-if)# no shutdown
2640(config-if)# exit
```

---

13. Define the default route for Cisco 2640 (this should be the ISP router).
- 

```
2640(config)# ip route 0.0.0.0 0.0.0.0 <ISP Router>
2640(config)# exit
2640# write memory
```

---

14. Later, we will configure the IPSEC parameters for this router.
- 

```
2640(config)# crypto isakmp policy 10
2640(config-isakmp)#encryption des
2640(config-isakmp)#hash md5
2640(config-isakmp)#authentication pre-share
2640(config-isakmp)#lifetime 3600
2640(config-isakmp)#exit
2640(config)#
```

---

- 
15. To set up a VPN with the Master MTL, we need to define the pre-shared key, which must match exactly on both routers.

However, each router points to the other IP address, which is the peer that you expect to exchange this key with (custkey100 is assumed for this example).

---

```
2640(config)# crypto isakmp key custkey100 address 208.47.192.66
```

---

16. Again, you need to define a transform set that defines the IPSEC parameters.

---

```
2640(config)#crypto ipsec transform-set des esp-des esp-md5-hmac
2640(cfg-crypto-trans)#exit
2640(config)#
```

---

17. Create the crypto map with the name “eutilica” and the sequence “100” and specify “ipsec-isakmp”.

---

```
2640(config)#crypto map eutilica 100 ipsec-isakmp
2640(config-crypto-map)#set peer 208.47.192.66
2640(config-crypto-map)#match address 100
2640(config-crypto-map)#set transform-set des
2640(config-crypto-map)#exit
2640(config)#
```

---

18. Create the access list that was specified in the crypto map.

---

```
2640(config)#ip access-list extended 100
2640(config-ext-nacl)# access-list 100 permit ip 10.10.51.0 0.0.0.255 10.10.10.0 0.0.0.255
2640(config-ext-nacl)#exit
```

---

Note: The above access list is only partial. For the complete access list please look at the sample router configuration given below.

19. The crypto map must be applied to the external interface in order to be effective. You also need to assign a public address to the external interface, set the media speed, etc.

---

```
2640(config)# interface FastEthernet0/0
2640(config-if)# crypto map eutilica
```

---

20. Cisco also recommends the execution of the following two commands on the external interface in order for IPSEC to function properly.

---

```
2640(config-if)# no ip route-cache
2640(config-if)# no ip mroute-cache
```

```
2640(config-if)# exit
2640(config)#
2640# write memory
```

---

---

## VTP Server Mode Configuration

When a switch is in the VTP server mode, we can change its VLAN configuration.

Using the privileged EXEC mode, follow these steps to configure the switch for the VTP server mode:

	Command	Purpose
Step 1	vlan database	Enter VLAN database mode.
Step 2	vtp domain <i>SingMTL</i>	Configure a VTP administrative-domain name. (The name can be from 1 to 32 characters.)
Step 3	vtp password <i>password-value</i>	(Optional) Set a password for the VTP domain. The password can be from 8 to 64 characters.
Step 4	vtp server	Configure the switch for VTP server mode (the default).
Step 5	exit	Return to privileged EXEC mode.
Step 6	show vtp status	Verify the VTP configuration. In the display, check the VTP Operating Mode and the VTP Domain Name fields.

---

## Add a VLAN

Each VLAN has a unique 4-digit ID that can be a number from 1 to 1001. To add a VLAN to the VLAN database, we need to assign a number and name to the VLAN. If the VLAN media type is NOT specified, the VLAN is an Ethernet VLAN.

Beginning in privileged EXEC mode, follow these steps to add an Ethernet VLAN:

	Command	Purpose
Step 1	vlan database	Enter VLAN database mode.
Step 2	Vlan 2 name <i>outside</i> Vlan 3 name <i>inside</i> Vlan 5 name <i>FTC1</i> Vlan 6 name <i>FTC2</i> Vlan 7 name <i>FTC3</i> Vlan 8 name <i>FTC4</i>	Add an Ethernet VLAN by assigning a number to it Add Vlans for outside, inside and FTCs
Step 3	exit	Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.
Step 4	show vlan name <i>vlan-name</i>	Verify the VLAN configuration.

---

## Assign Static-Access Ports to a VLAN and Set Speed

By default, all ports are in trunk-desirable mode and assigned to VLAN 1, which is the default management VLAN. If you are assigning a port on a switch to a VLAN, first log in to the switch.

Beginning in privileged EXEC mode, follow these steps to assign a port to a VLAN in the VTP database:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>fa/1</i>	Enter interface configuration mode, and define the interface to be added to the VLAN.
Step 3	switchport mode access	Define the VLAN membership mode for this port.
Step 4	switchport access vlan 2 Speed = 100 or 10 or auto Duplex= full or half or auto	Assign the port to the VLAN.
Step 5	exit	Return to privileged EXEC mode.
Step 6	show interface <i>interface-id</i> switchport	Verify the VLAN configuration. In the display, check the Operation Mode, Access Mode VLAN, and the Priority for Untagged Frames fields.
Step 7	Repeat the above instructions	Configure all the ports

---

## Set Speed and Duplex Parameters

Beginning in privileged EXEC mode, follow these steps to set the speed and duplex parameters on a port:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface</i>	Enter interface configuration mode, and enter the port to be configured.
Step 3	speed {10   100   1000   auto}	Enter the speed parameter for the port. The 10/100/1000 ports operate in 10 or 100 Mbps when they are set to half- or full-duplex mode, but only operate in full-duplex mode when set to 1000 Mbps. The GBIC module ports operate only at 1000 Mbps. 100BASE-FX ports operate only at 100 Mbps in full-duplex. Note The Catalyst 2950C-24 does not support the speed and duplex interface configuration commands in IOS Release 12.1(6)EA2.
Step 4	duplex {full   half   auto}	Enter the duplex parameter for the port. The 10/100/1000 ports operate in either half- or full-duplex mode when they are set to 10 or 100 Mbps, but when set to 1000 Mbps, they only operate in full-duplex mode. 100BASE-FX ports operate only at 100 Mbps in full-duplex. Note The Catalyst 2950C-24 does not support the speed and duplex interface configuration commands in IOS Release 12.1(6)EA2.
Step 5	end	Return to privileged EXEC mode.
Step 6	show running-config	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entry in the configuration file. This retains the configuration when the switch restarts.

---

## Set the Switch IP Address

Command	Purpose	Comment
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface vlan 1	Enter interface configuration mode, and enter the VLAN to which the IP information is assigned. VLAN 1 is the default management VLAN, but you can configure any VLAN from 1 to 1001.
Step 3	ip address <i>10.10.60.6</i> <i>255.255.255.0</i>	Enter the IP address and subnet mask.
Step 4	exit	Return to global configuration mode.
Step 5	ip default-gateway <i>10.10.60.6</i>	We don't want to set any default GW for this switch
Step 6	end	Return to privileged EXEC mode.
Step 7	show running-config	Verify that you entered the information was entered correctly by displaying the running configuration. If the information is incorrect, repeat the procedure.

### Misc. configurations:

Set the time and set ntp server as 10.10.60.2