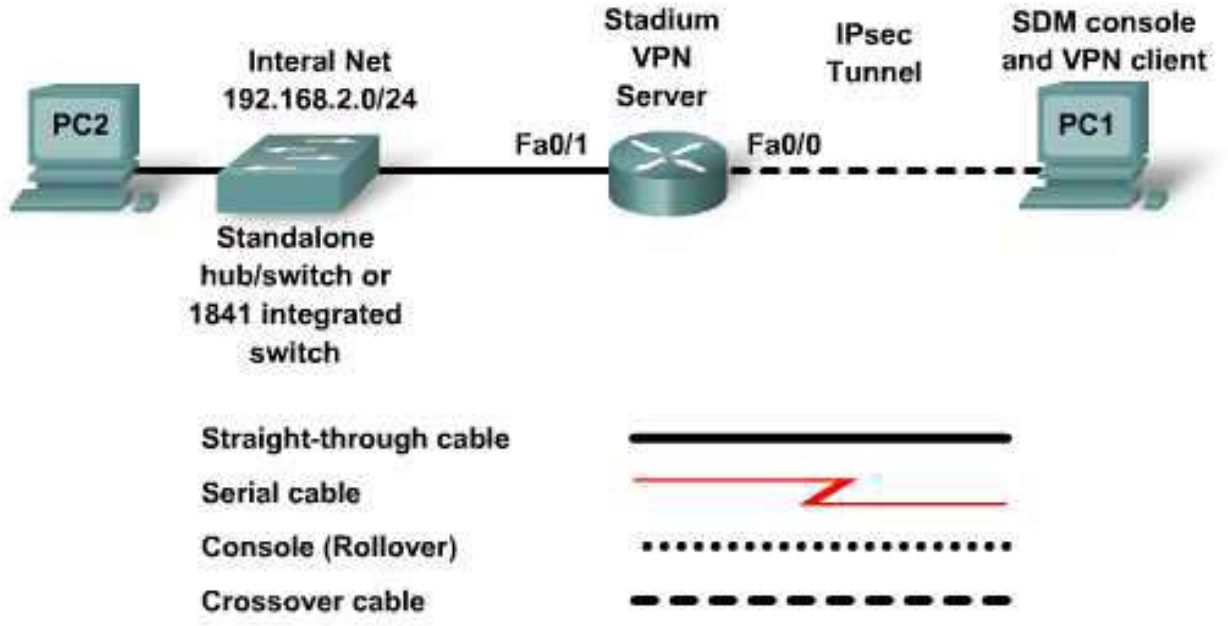
Lab 8.3.4.4 Configuring and Testing the VPN Client (Optional Lab)



Device	Host Name	FastEthernet 0/0 or NIC IP Address	FastEthernet 0/1 IP Address	Default Gateway	Enable Secret Password	Enable, vty, and Console Password
Router 1	VPN	10.10.10.1 /29	192.168.2.99 /24		class	cisco
Switch 1	S1					
Host 1	H1	10.10.10.2 /29		10.10.10.1		
Host 2	H2	192.168.2.6 /24		192.168.2.99		

Objectives

- Configure basic router settings using IOS.
- Configure a VPN client for remote access.
- Configure the internal network.
- Verify VPN tunnel establishment between client and server.
- Verify VPN client access to internal network resources.

640-802 CCNA Exam Objective

This lab contains skills that relate to the following CCNA exam objective:

- Describe VPN technology (including: importance, benefits, role, impact, components).

Expected Results and Success Criteria

Before starting this lab, read through the tasks that you are expected to perform. What do you expect the result of performing these tasks will be?

_____

_____

_____

How is the ability to implement VPN technology important in network design and prototyping?

_____

_____

_____

Background / Preparation

In this lab you will configure a VPN client to simulate remote access to the Stadium network internal LAN resources through a VPN server. Prior to starting this lab, you must complete Lab 8.3.4.3 to configure the 1841 VPN server using the SDM graphical user interface and the EasyVPN Server Wizard. You will test the remote VPN client access according to the test plan outlined previously in Lab 8.3.2.

NOTE: Even if the equipment is not available to actually perform this lab, you should read through it to get a better understanding of how VPNs function.

The following resources are required:

- Cisco 1841 router with 2 Fast Ethernet routed interfaces and the following:
    - IOS 12.4 Advanced IP Services IOS image
    - Virtual Private Network (VPN) Module
    - SDM version 2.4 installed
    - 4-port switch add-in module (an external hub or switch can be substituted)
- Windows XP computer for use with SDM EasyVPN configuration and to act as VPN client with the following:
    - Internet Explorer 5.5 or higher
    - SUN Java Runtime Environment (JRE) version 1.4.2_05 or later (or Java Virtual Machine (JVM) 5.0.0.3810)

- Cisco VPN Client installed

- Windows XP computer or other computer to act as internal host (Use of Discovery CD Server is an option but addressing for internal network will need to match the 172.16.1.1/16 address of the server)
- Console cable with DB-9 to RJ-45 adapter
- Access to PC network TCP/IP configuration and command prompt
- Cabling as shown in the topology and described in test plan Lab 8.3.2

Task 1: Build the Network and Configure the Devices for SDM Access

Step 1: Connect the PCs and devices as shown in the topology diagram

a. The internal VPN router interface Fa0/1 may be connected to the integrated 1841 Ethernet switch, if one is installed, or may be attached to a standalone hub or switch.

b. It is not necessary to configure the switch. If an external standalone switch is used, erase the startup configuration file and delete the vlan.dat file. Issue the **reload** command or power-cycle the switch to clear any previous configurations.

c. Connect host H2 to the same switch (1841 integrated or standalone hub/switch) as the router Fa0/1 interface. Configure the IP address as shown in the topology diagram table.

Step 2: Configure the router as a VPN server

a. Host H1 connects to the router console port for basic IOS configuration and connects via the router Fa0/0 port for SDM EasyVPN configuration. Refer to Lab 8.3.4.3 for PC setup to access the router SDM GUI. After configuring the router as a VPN server, host H1 acts as the VPN client.

b. Refer to Lab 8.3.4.3 for instructions on configuring the 1841 as a VPN server using IOS commands and SDM. Be sure to erase the startup configuration file and issue the **reload** command to clear any previous configurations.

c. Assign an IP internal LAN address to the VPN server Fa0/1 interface to act as the gateway for internal hosts.

```
VPN(config)#interface FastEthernet0/1
VPN(config-if)#ip address 192.168.2.99 255.255.255.0
VPN(config-if)#no shutdown
```

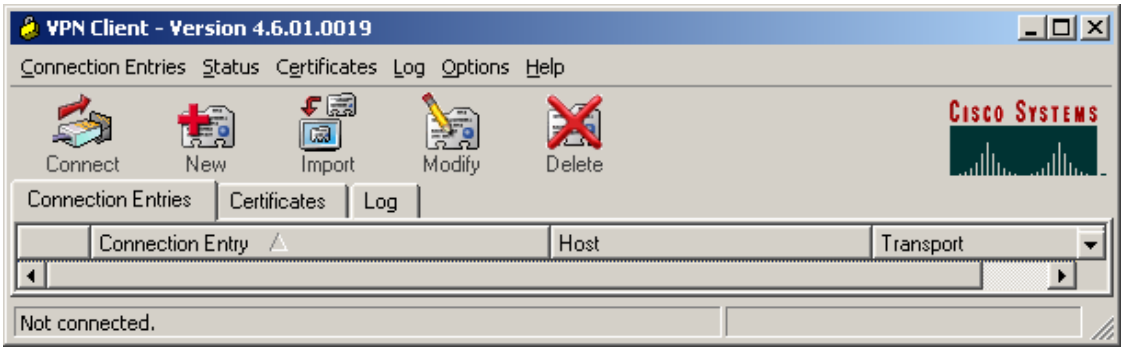
Task 2: Configure the VPN Client

Step 1: Install the Cisco VPN client

If not already installed, install Cisco VPN Client software on host H1. If you do not have the Cisco VPN Client software or are unsure of the process, contact your instructor.

Step 2: Configure the PC as a VPN client to access the VPN server

a. Start the **Cisco VPN Client** and select **Connection Entries > New**.



b. Enter the following information to define the new connection entry. Click **Save** when you are finished.

Connection Entry: **VPN**

Description: **Connection to Stadium network**

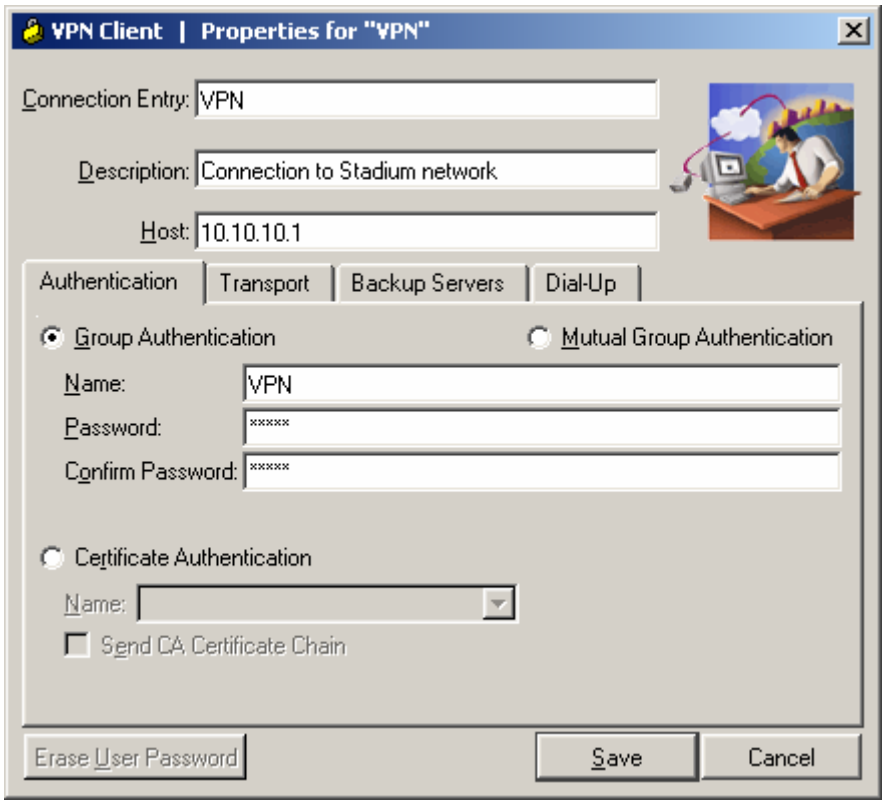
Host: **10.10.10.1**

Group Authentication Name: **VPN** (Configured in Lab 8.3.4.3)

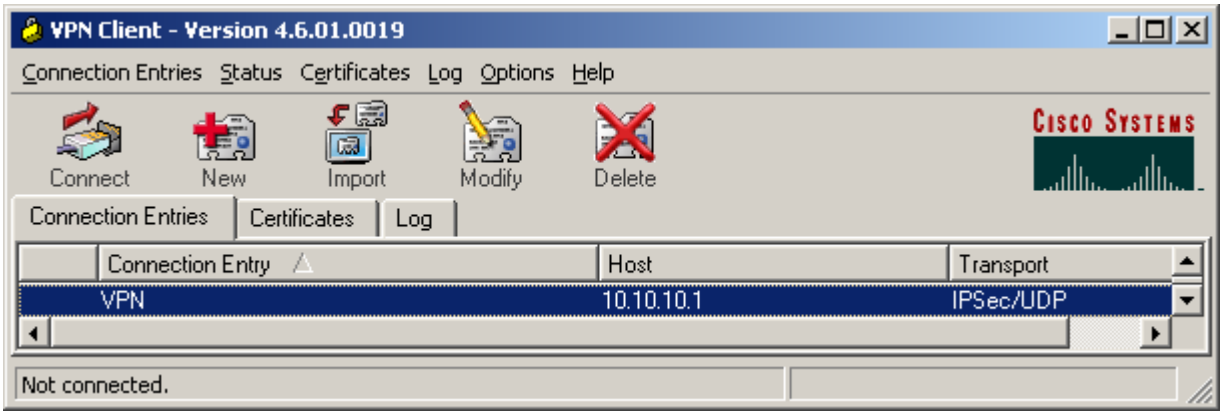
Password: **cisco** (Configured in Lab 8.3.4.3)

Confirm Password: **cisco**

NOTE: Name and password are case-sensitive and must match the ones created on the VPN server.



c. Select the newly created connection and click **Connect**.



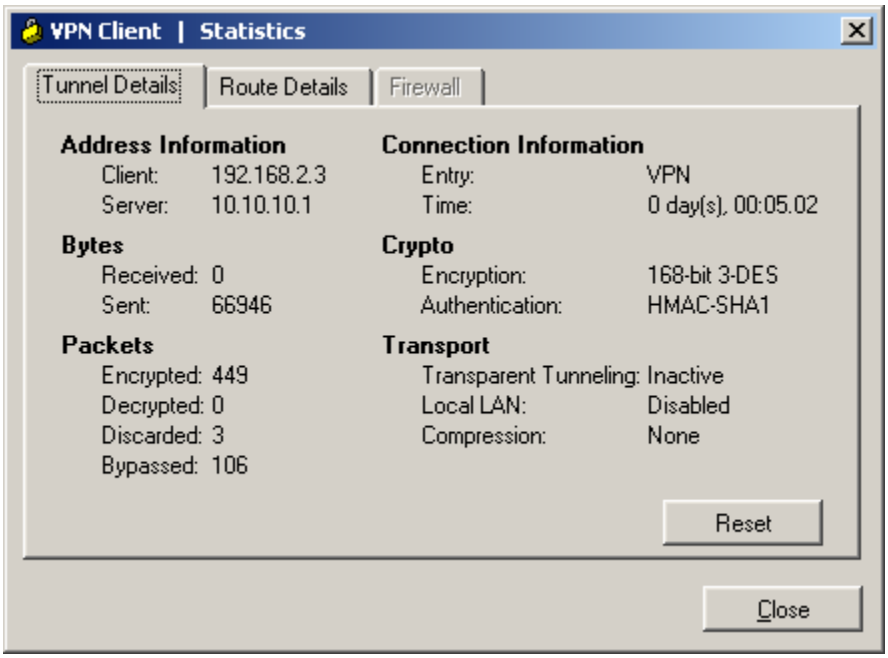
d. Enter the user name **admin** created previously on the VPN router and enter the password of **cisco123**. Click **OK** to continue. The VPN Client window will minimize to an icon in the tools tray of the taskbar.

Task 3: Verify the VPN Tunnel between Client, Server, and the Internal Network

Perform testing as outlined in Lab 8.3.2 Test 2 of the VPN Connectivity Test Plan and as described here.

Step 1: Check the tunnel statistics

Open the VPN Client icon and click the **Status** menu and then the **Statistics** option to display the Tunnel Details tab.



What is the Client IP address obtained from the VPN server?

_____

What is the VPN server address? _____

How many packets have been encrypted? _____

What is the encryption method being used? _____

What is the authentication being used? _____

Step 2: Open a command prompt window and verify the VPN connection

Click **Start > Run,** enter **cmd** and press **Enter**. Use the **`ipconfig /all`** command to see the network connections currently in use.

```
C:\>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : H1
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection 1:
```

```
        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel(R) PRO/100 VE Network
Connection
        Physical Address. . . . . . . . . : 00-07-E9-63-CE-53
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 10.10.10.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.248
        Default Gateway . . . . . . . . . : 10.10.10.1

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Cisco Systems VPN Adapter
        Physical Address. . . . . . . . . : 00-05-9A-3C-78-00
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.2.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.2.4
```

What is the IP configuration for the first Local Area Connection?

IP Address: _____

Subnet Mask: _____

Default Gateway: _____

Description: _____

What is the IP configuration for the second Local Area Connection?

IP Address: _____

Subnet Mask: _____

Default Gateway: _____

Description: _____

Step 3: Test connectivity between the remote VPN client and the internal stadium network

Ping from the external (remote) host H1 to host H2 (IP address 192.168.2.6) on the internal stadium network to simulate access to internal resources.

Were the pings successful? _____ If they are not, troubleshoot until they are.

```
C:\>ping 192.168.2.6

Pinging 192.168.2.6 with 32 bytes of data:

Reply from 192.168.2.6: bytes=32 time=1ms TTL=64
Reply from 192.168.2.6: bytes=32 time<1ms TTL=64
Reply from 192.168.2.6: bytes=32 time<1ms TTL=64
Reply from 192.168.2.6: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.2.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Task 4: Reflection

Why is VPN a good option for remote users?

_____

_____

_____

_____

What would happen if the VPN client tunneling protocol or encryption did not match that of the VPN server?

_____

_____