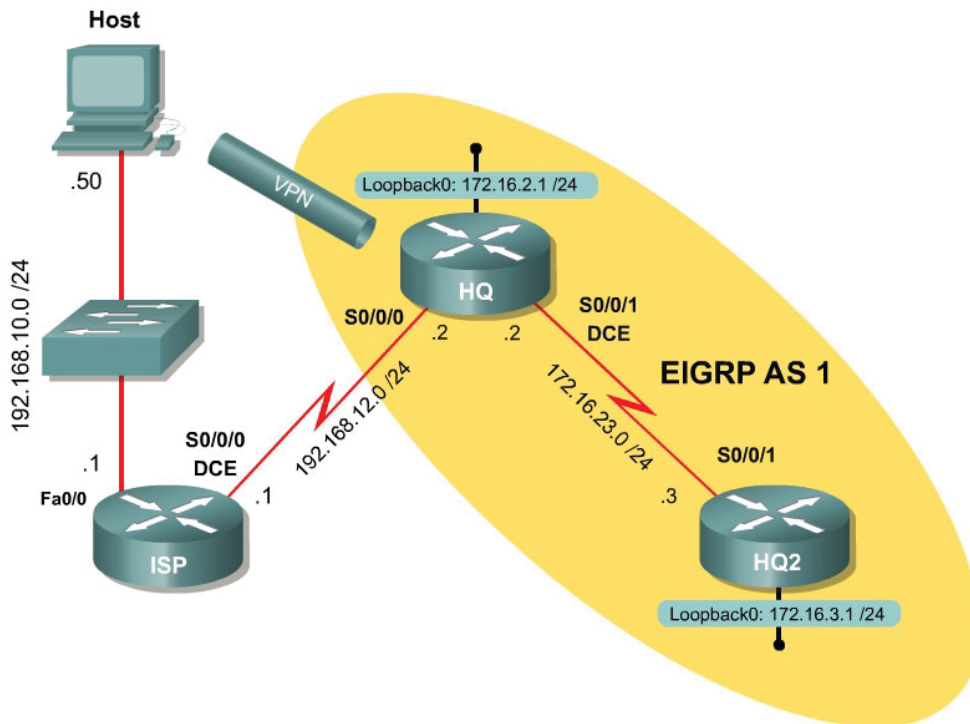


## Configuring Remote Access VPN with the IOS CLI

### Learning Objectives

- Configure EIGRP on a router
- Configure Easy VPN Server
- Install the Cisco VPN Client to a host
- Connect to the VPN using Cisco VPN client
- Verify VPN operation

### Topology Diagram



### Scenario

In this lab, you will set up Easy VPN for the International Travel Agency and connect to Headquarters (HQ) using the IOS Command Line Interface (CLI). The host will simulate an employee connecting from home over the Internet. ISP will simulate an internet router representing the Internet connection for both the home user and the company headquarters.

## Step 1: Configure Addressing

Configure the loopback interfaces with the addresses shown in the diagram. Also configure the serial interfaces shown in the diagram. Set the clockrate on the appropriate interfaces and issue the **no shutdown** command on all serial connections. Verify that you have connectivity across the local subnet using the **ping** command. Do not set up the tunnel interface.

```
ISP# configure terminal
ISP(config)# interface fastethernet 0/0
ISP(config-if)# ip address 192.168.10.1 255.255.255.0
ISP(config-if)# no shutdown
ISP(config-if)# interface serial 0/0/0
ISP(config-if)# ip address 192.168.12.1 255.255.255.0
ISP(config-if)# clockrate 64000
ISP(config-if)# no shutdown
```

```
HQ# configure terminal
HQ(config)# interface loopback 0
HQ(config-if)# ip address 172.16.2.1 255.255.255.0
HQ(config-if)# interface serial0/0/0
HQ(config-if)# ip address 192.168.12.2 255.255.255.0
HQ(config-if)# no shutdown
HQ(config-if)# interface serial 0/0/1
HQ(config-if)# ip address 172.16.23.2 255.255.255.0
HQ(config-if)# clockrate 64000
HQ(config-if)# no shutdown
```

```
HQ2# configure terminal
HQ2(config)# interface loopback 0
HQ2(config-if)# ip address 172.16.3.1 255.255.255.0
HQ2(config-if)# interface serial 0/0/1
HQ2(config-if)# ip address 172.16.23.3 255.255.255.0
HQ2(config-if)# no shutdown
```

## Step 2: Configure EIGRP AS 1

Configure EIGRP for AS1 on HQ and HQ2. Add the entire 172.16.0.0/16 major network and disable automatic summarization. ISP will not participate in this routing process.

```
HQ(config)# router eigrp 1
HQ(config-router)# no auto-summary
HQ(config-router)# network 172.16.0.0

HQ2(config)# router eigrp 1
HQ2(config-router)# no auto-summary
HQ2(config-router)# network 172.16.0.0
```

An EIGRP neighbor adjacency should form between HQ and HQ2. If not, troubleshoot by checking your interface configuration, EIGRP configuration, and physical connectivity.

### Step 3: Configure a Static Default Route

Since ISP represents a connection to the Internet, send all traffic whose destination network does not exist in the routing tables at company headquarters out this connection via a default route. This route can be statically created on HQ, but will need to be redistributed into EIGRP so HQ2 will learn the route too.

```
HQ(config)# ip route 0.0.0.0 0.0.0.0 192.168.12.1
HQ(config)# router eigrp 1
HQ(config-router)# redistribute static
```

For which types of routes is it unnecessary to assign a default/seed metric when redistributing into EIGRP?

When redistributing connected, static, and IGRP routes into EIGRP, it is unnecessary to configure a default or seed metric. EIGRP will naturally assign a connected, static or IGRP route a metric.

How else could you configure HQ to advertise the default route?

You could also use the **ip default-network** command to advertise a network as a candidate default route.

### Step 4: Enable AAA on HQ

To run Easy VPN server, AAA must be enabled on the router. To prevent getting locked out of the router, create a local username and make sure that authentication is performed through the local database. HQ will be the Easy VPN Server, so this is where it must be configured.

```
HQ(config)# username cisco password cisco
HQ(config)# aaa new-model
HQ(config)# aaa authentication login default local none
```

### Step 5: Create the IP Pool

Create a pool that VPN clients will draw their IP addresses from using the command **ip local pool name low-address high-address**. Use addresses from 172.16.2.100 to 172.16.2.200.

```
HQ(config)# ip local pool VPNCLIENTS 172.16.2.100 172.16.2.200
```

### Step 6: Configure the Group Authorization

Use the AAA authorization command **aaa authorization network name types** to configure the VPN group authentication list. This list will authenticate remote

users connecting to the VPN using the group set up in their client. Use the local group list, which will be configured in the next step.

```
HQ(config)# aaa authorization network VPNAUTH local
```

## Step 7: Create an IKE Policy and Group

Just like previous crypto configurations, you must set up ISAKMP policies to be used during IKE Phase I negotiation. Use the following settings. If your version of the IOS does not support the same settings that appear here, try to make them as similar as possible.

```
HQ(config)# crypto isakmp policy 10
HQ(config-isakmp)# authentication pre-share
HQ(config-isakmp)# encryption aes 256
HQ(config-isakmp)# group 2
```

Since you don't know specific peers, you cannot statically associate ISAKMP keys with IP addresses or hosts. Rather, VPN clients could connect from anywhere on the internet. So, we configure an ISAKMP client group, instead. The group will exist locally on the router, as specified by the AAA network authorization command in the last step.

To enter the ISAKMP group configuration mode, use the global configuration command **crypto isakmp client configuration group** *name*. Use the name "ciscogroup". Use ? once in this mode to find out what options you have available.

```
HQ(config)# crypto isakmp client configuration group ciscogroup
HQ(config-isakmp-group)# ?
ISAKMP group policy config commands:
  access-restrict  Restrict clients in this group to an interface
  acl              Specify split tunneling inclusion access-list number
  backup-gateway  Specify backup gateway
  dns             Specify DNS Addresses
  domain          Set default domain name to send to client
  exit            Exit from ISAKMP client group policy configuration mode
  firewall        Enforce group firewall feature
  group-lock      Enforce group lock feature
  include-local-lan Enable Local LAN Access with no split tunnel
  key             pre-shared key/IKE password
  max-logins      Set maximum simultaneous logins for users in this group
  max-users       Set maximum number of users for this group
  netmask         netmask used by the client for local connectivity
  no              Negate a command or set its defaults
  pfs            The client should propose PFS
  pool            Set name of address pool
  save-password   Allows remote client to save XAUTH password
  split-dns       DNS name to append for resolution
  wins            Specify WINS Addresses
```

Configure a pre-shared key to be the same as the group name. Also, associate the address pool created earlier with this group. In addition, specify an access list to be used as the split tunneling list, to enable split tunneling in this

configuration. This access list doesn't exist yet, but you will create it shortly. Finally, set the network mask, since the IP pool does not specify one.

```
HQ(config-isakmp-group)# key ciscogroup
HQ(config-isakmp-group)# pool VPNCLIENTS
HQ(config-isakmp-group)# acl 100
HQ(config-isakmp-group)# netmask 255.255.255.0
```

Now that you have referenced the split tunneling access-list, create it. Source networks permitted by the access-list will be sent to the VPN clients and injected into their IP table. Create an access list allowing traffic sourced from the entire 172.16.0.0/16 network.

```
HQ(config)# access-list 100 permit ip 172.16.0.0 0.0.255.255 any
```

### Step 8: Configure the IPsec Transform Set

Configure an IPsec transform set for use with the VPN. Use the 3DES algorithm for encryption and the SHA-HMAC hash function for data integrity.

```
HQ(config)# crypto ipsec transform-set mytrans esp-3des esp-sha-hmac
HQ(cfg-crypto-trans)# exit
```

### Step 9: Create a Dynamic Crypto Map

As in previous IPsec configurations, you must set up a crypto map. However, this type of crypto map will be different than earlier configurations. Previously you configured static crypto maps, which configure certain traffic to establish VPNs with certain peers. However, since you don't know what the peers will be, as well as what the triggering traffic will be, create and apply a dynamic crypto map.

Use the global configuration command **crypto dynamic-map** *name sequence*, similar to a regular crypto map. Use the name "mymap" and the sequence number 10. Once you have entered crypto map configuration mode, set the transform set you configured in the previous step. Use the command **reverse-route**, which ensures that a route is installed on the local router for the remote VPN peer.

```
HQ(config)# crypto dynamic-map mymap 10
HQ(config-crypto-map)# set transform-set mytrans
HQ(config-crypto-map)# reverse-route
```

After creating the map, there are more commands that modify it. The first of these will make the map respond to VPN requests, which is the **crypto map** *name client configuration address respond* command. The next command is **crypto map** *name isakmp authorization list name*, which associates an AAA group authorization list with the map. The final command creates a regular crypto map using the dynamic one created earlier.

```
HQ(config)# crypto map mymap client configuration address respond
HQ(config)# crypto map mymap isakmp authorization list VPNAUTH
```

```
HQ(config)# crypto map mymap 10 ipsec-isakmp dynamic mymap
```

Finally, apply the crypto map to the interface that is facing ISP.

```
HQ(config)#int serial0/0/0
HQ(config-if)#crypto map mymap
```

## Step 10: Enable IKE DPD and User Authentication

IKE Dead Peer Detection (DPD) is a keepalive mechanism for checking VPN connections. This is beneficial when a VPN server has to manage many connections that are potentially on unstable connections. To configure IKE DPD, use the global configuration command **crypto isakmp keepalive seconds retry-time**, where seconds is how often to send a keepalive packet and retry-time is how soon to retry if one is missed. Use a keepalive timer of 30 seconds and a retry-time of 5 seconds.

```
HQ(config)# crypto isakmp keepalive 30 5
```

Xauth, or extended authentication, is the method used to authenticate VPN clients on a per-user basis, in addition to the group authentication. To configure this, use the AAA login authentication command **aaa authentication login group types**. We will reuse the name VPNAUTH (the last time we used it, it was for network authentication, not login authentication), and keep the authentication type as local. Also, add a user for VPN access with the username/password of ciscouser/ciscouser.

```
HQ(config)# aaa authentication login VPNAUTH local
HQ(config)# username ciscouser password ciscouser
```

Globally configure the Xauth timeout to be 60 seconds using the **crypto isakmp xauth timeout seconds** command. This controls the amount of time that the VPN server will wait before terminating the IKE session with a client if user authentication is not performed.

```
HQ(config)# crypto isakmp xauth timeout 60
```

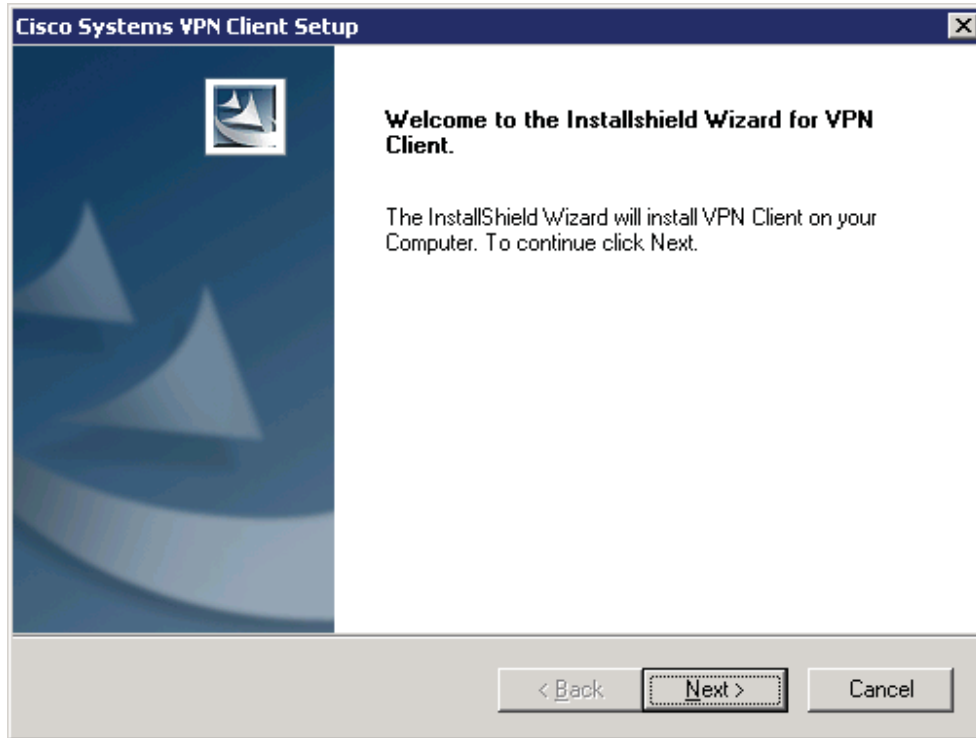
Finally, associate the AAA login list with the crypto map configured earlier.

```
HQ(config)# crypto map mymap client authentication list VPNAUTH
```

## Step 11: Install the Cisco VPN Client

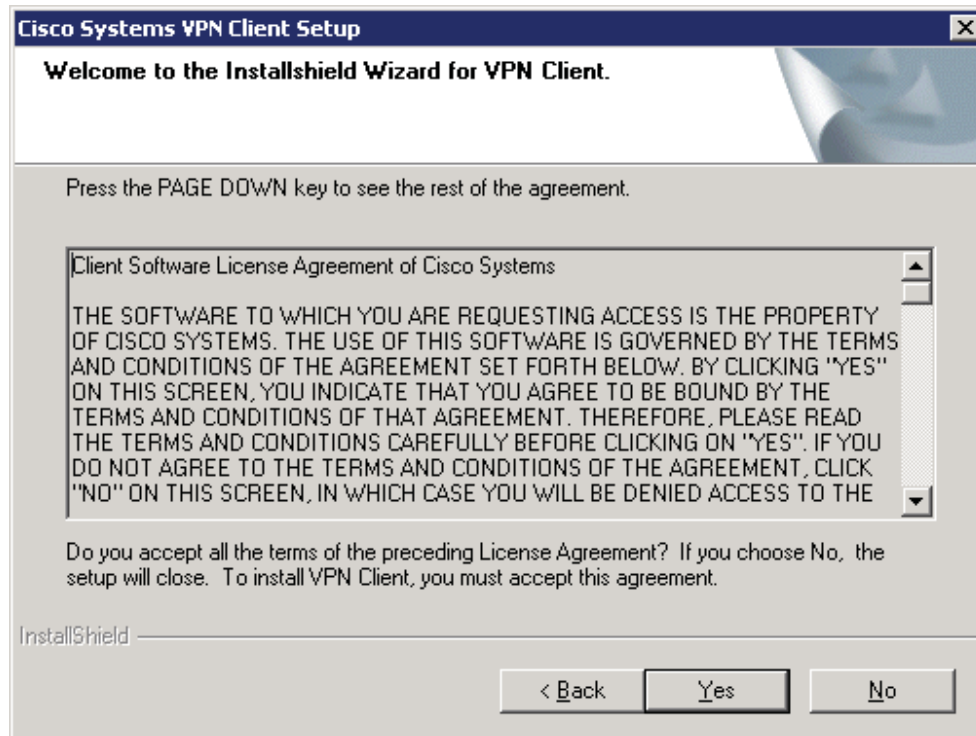
Now that HQ has been set up as an Easy VPN Server, the host will change its role from management host to a VPN client connecting across the Internet to HQ. Before you can connect, you must install the Cisco VPN Client if you haven't already. If you have already installed the VPN client, skip this step and move on to Step 12.

To begin the installation, download the VPN Client from Cisco, and extract it to a temporary directory. Run the setup.exe file in the temporary directory to start installation. Click **Next** when the installer welcomes you.



**Figure 11-1: VPN Client Installation Wizard**

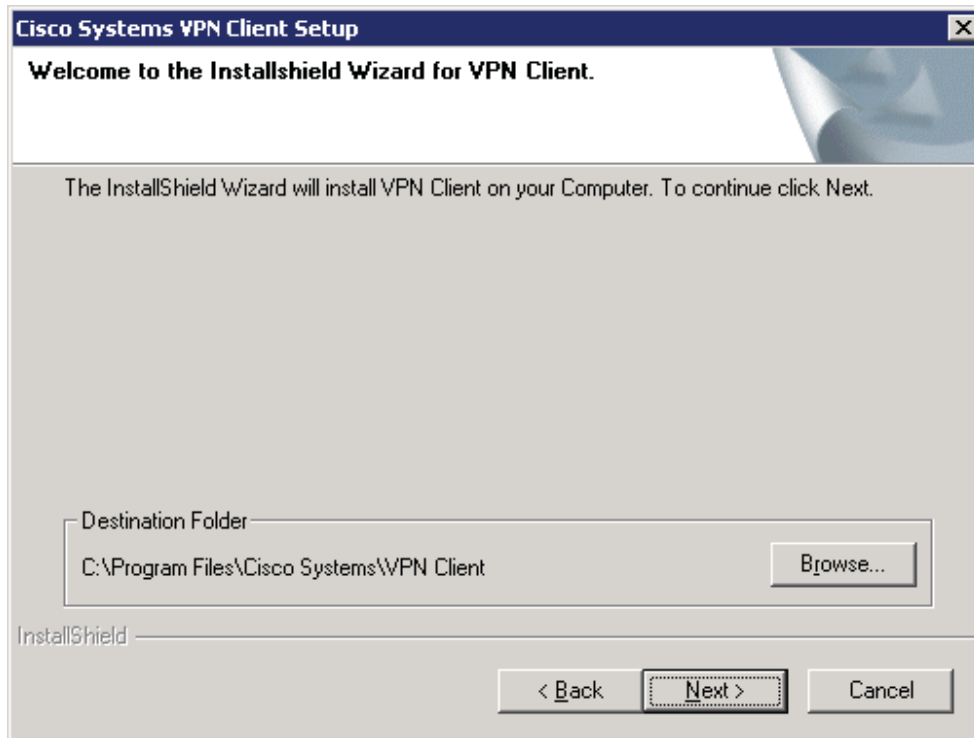
Click **Yes** after reading the software license agreement.



**Figure 11-2: Cisco VPN Client License Agreement**

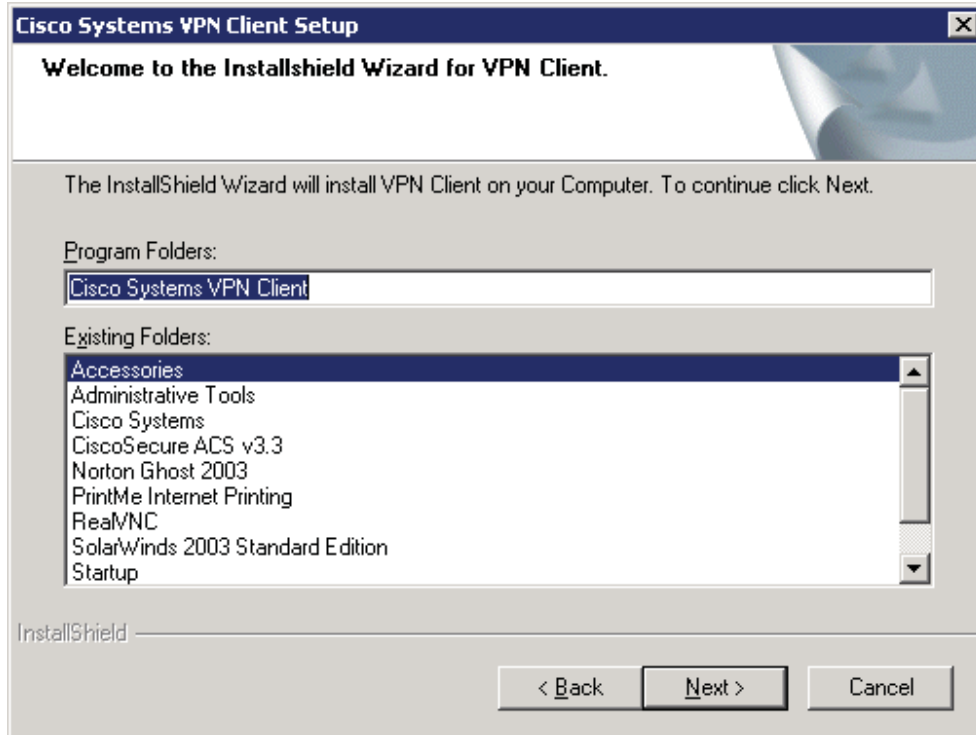
Click **Next** to use the default installation.





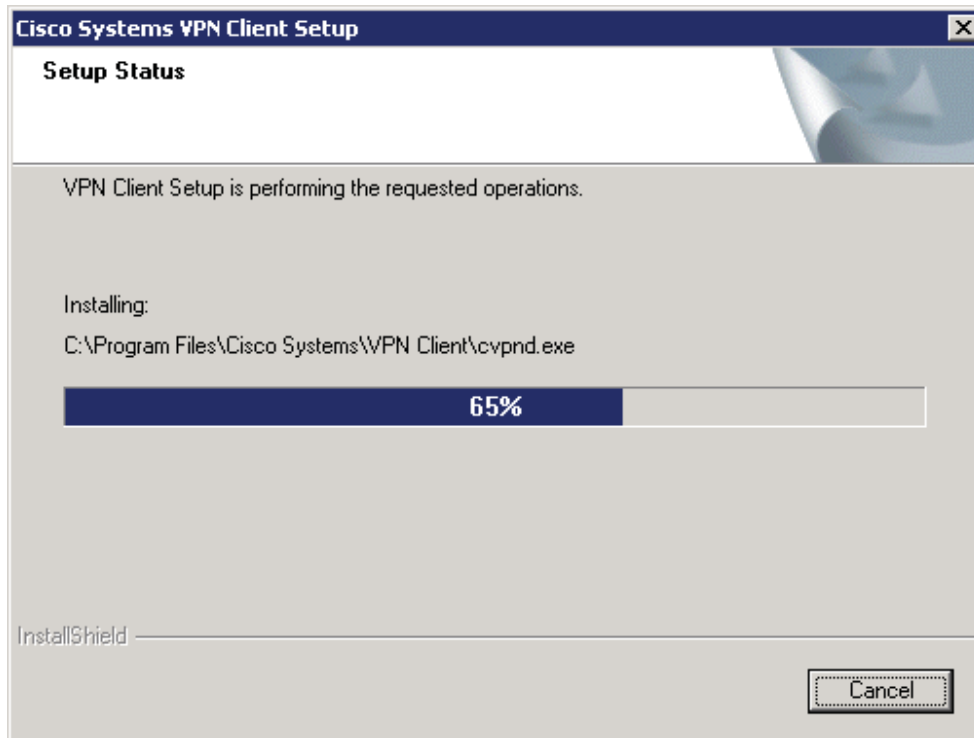
**Figure 11-3: VPN Client Installation Location**

Choose the default program group and click **Next**.



**Figure 11-4: Start Menu Program Folder Selection**

Allow the wizard to install all the necessary files. Toward the end of the process, the wizard will try to add the virtual network interfaces required for VPN use. This may take some time.



**Figure 11-5: VPN Client Installation Progress Indicator**

At the end of the installer, you will be required to restart. Click **Finish** to let your computer restart.

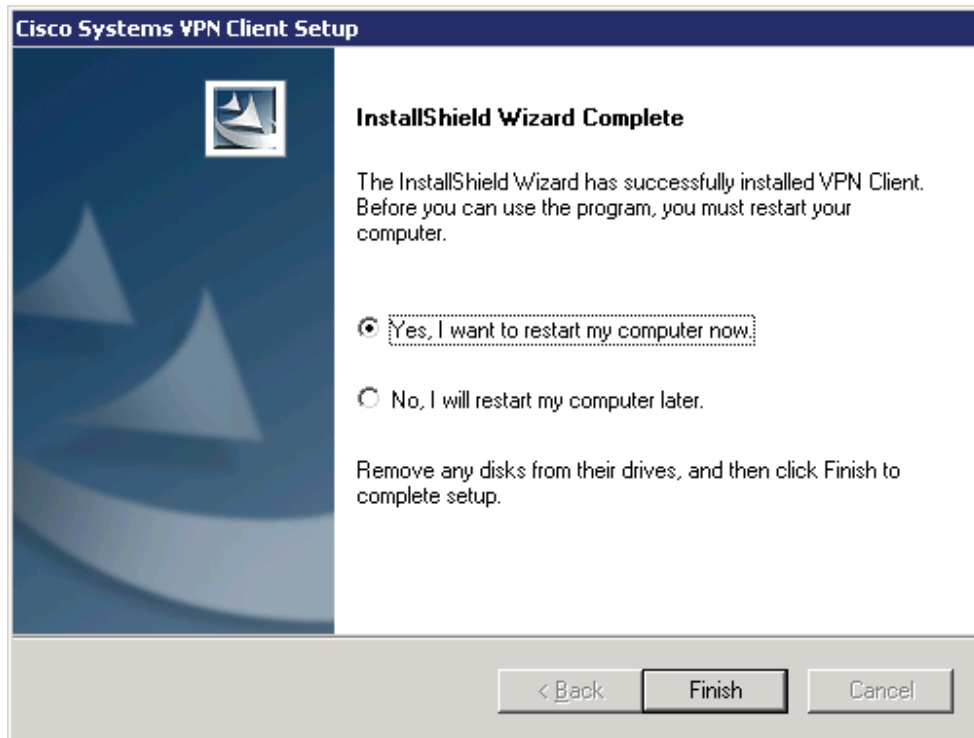
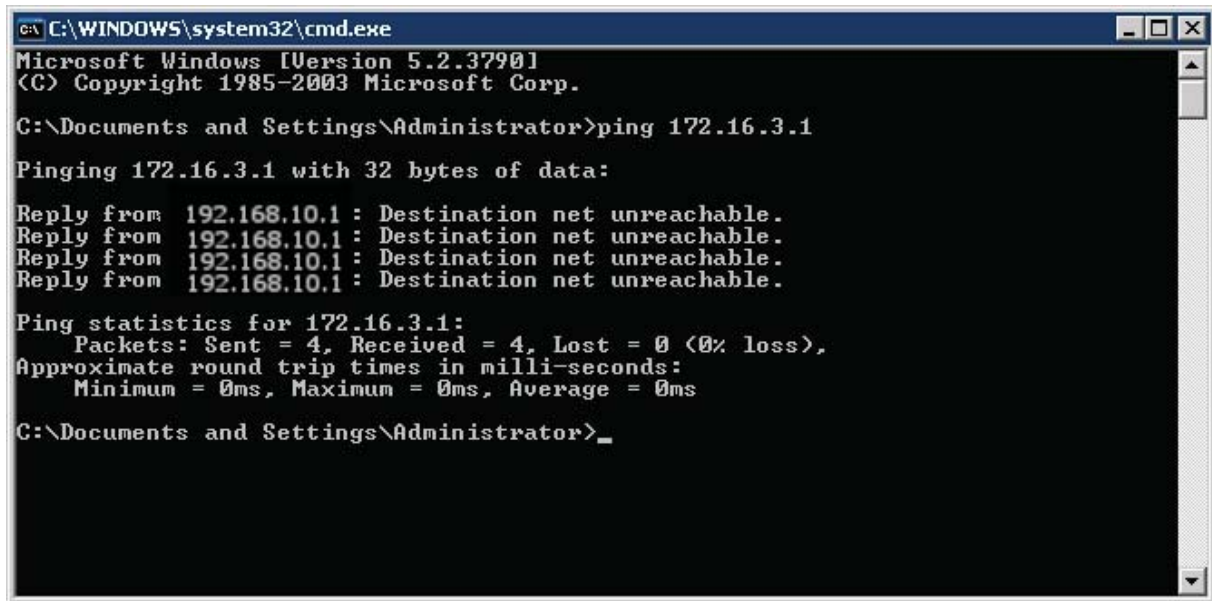


Figure 11-6: Final Installation Wizard Window

### Step 12: Test Access from Client without VPN Connection

After restarting the host with the VPN client installed, open up a command prompt. Click on the **Start** button, choose **Run...** and type **cmd**, and click **OK**. Try pinging HQ2's loopback address. The pings should fail.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 172.16.3.1

Pinging 172.16.3.1 with 32 bytes of data:

Reply from 192.168.10.1 : Destination net unreachable.
Reply from 192.168.10.1 : Destination net unreachable.
Reply from 192.168.10.1 : Destination net unreachable.
Reply from 192.168.10.1 : Destination net unreachable.

Ping statistics for 172.16.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

Figure 12-1: Unsuccessful Pings Without VPN

### Step 13: Connect to the VPN

To start the Cisco VPN Client, click the **Start** button and choose **Programs > Cisco Systems VPN Client > VPN Client**.

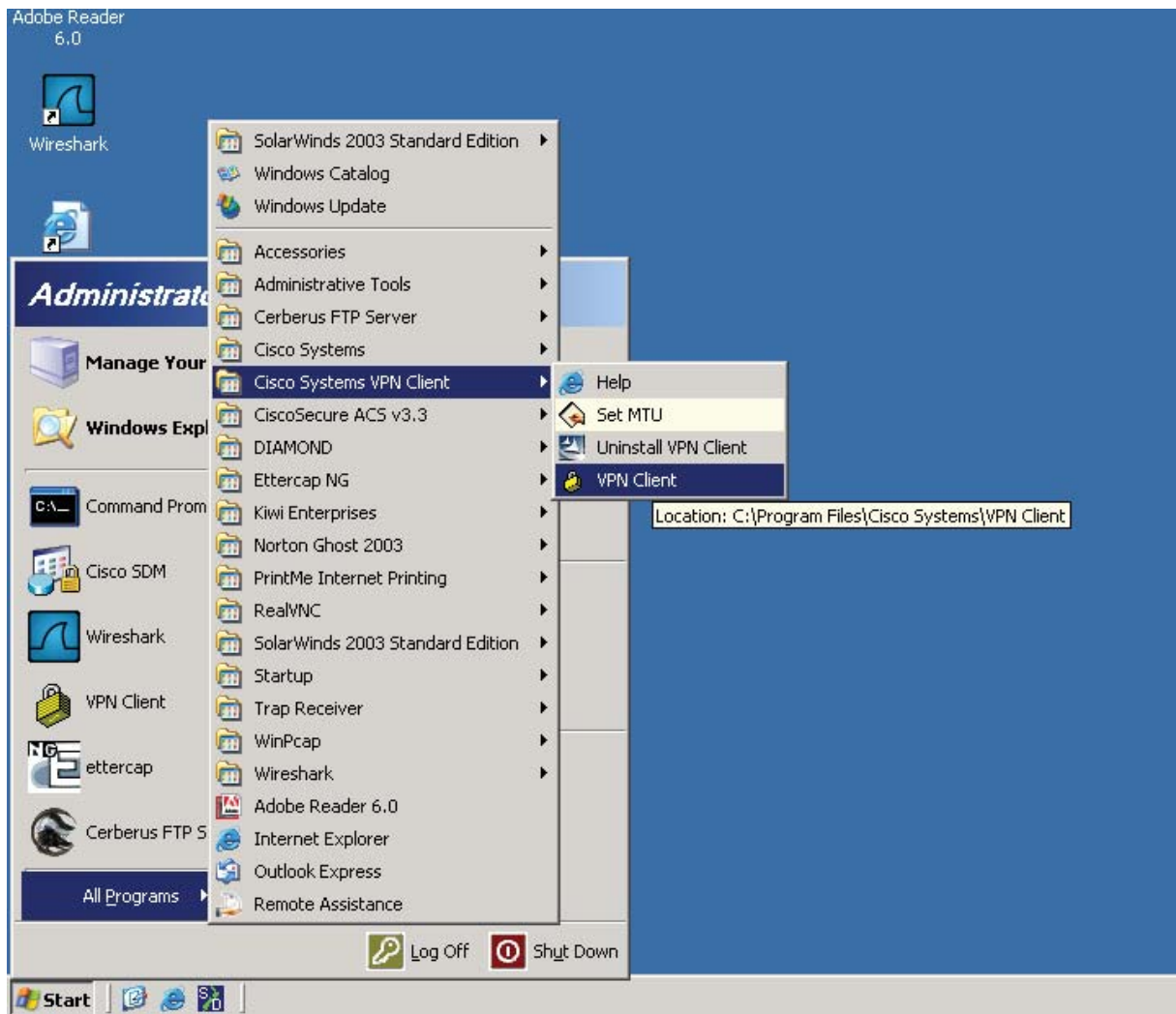
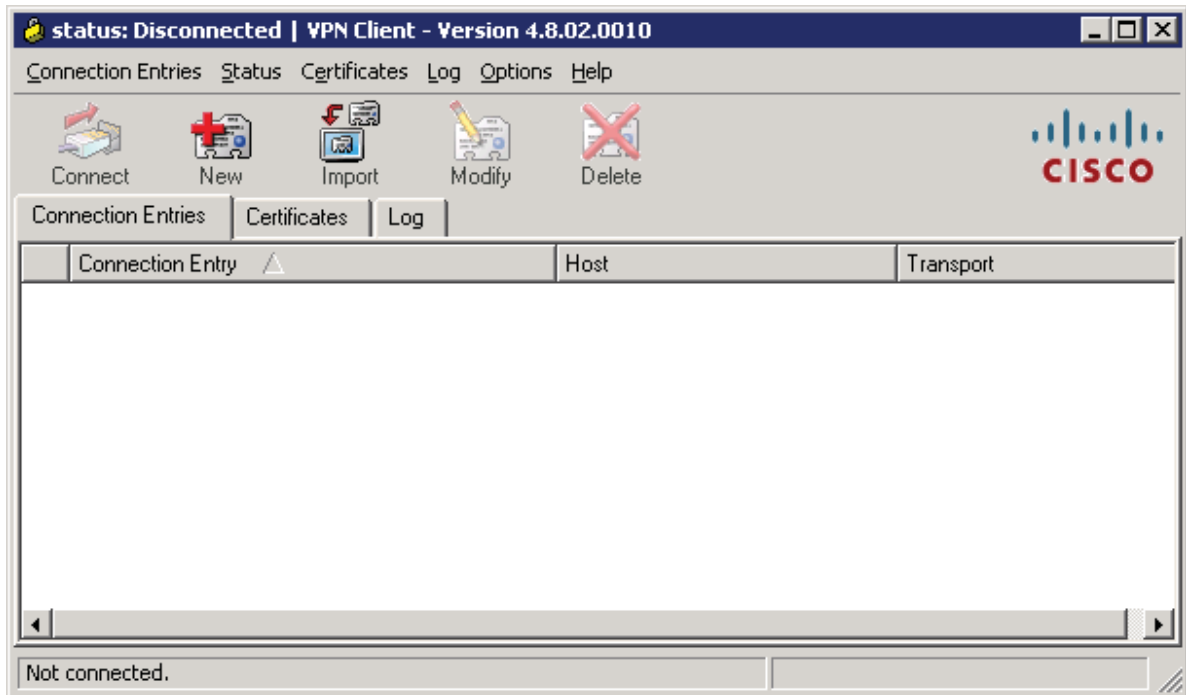
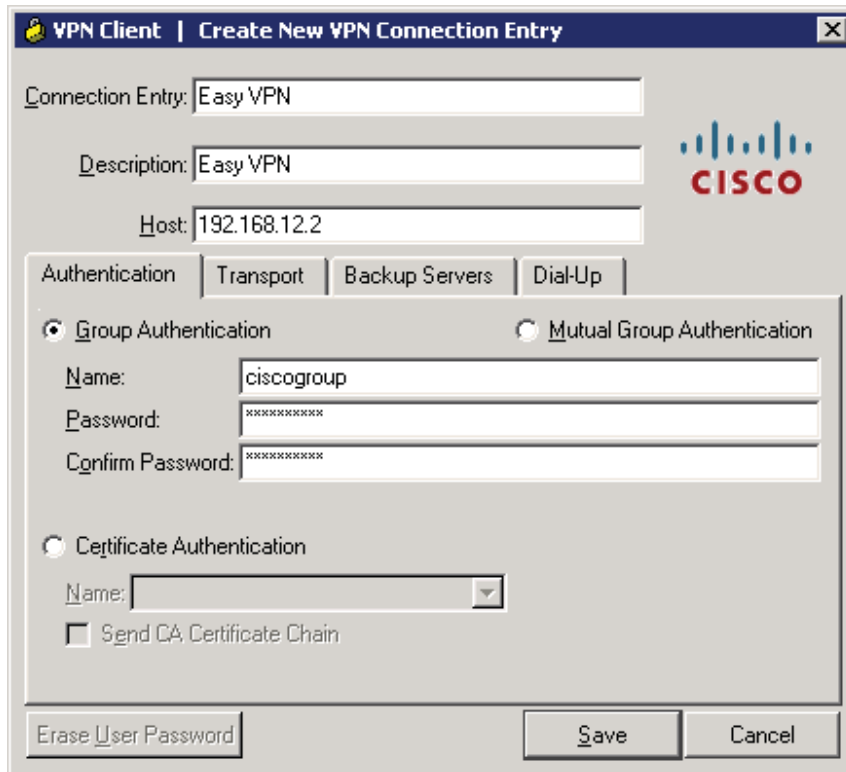


Figure 13-1: Launching the VPN Client



**Figure 13-2: VPN Client Application**

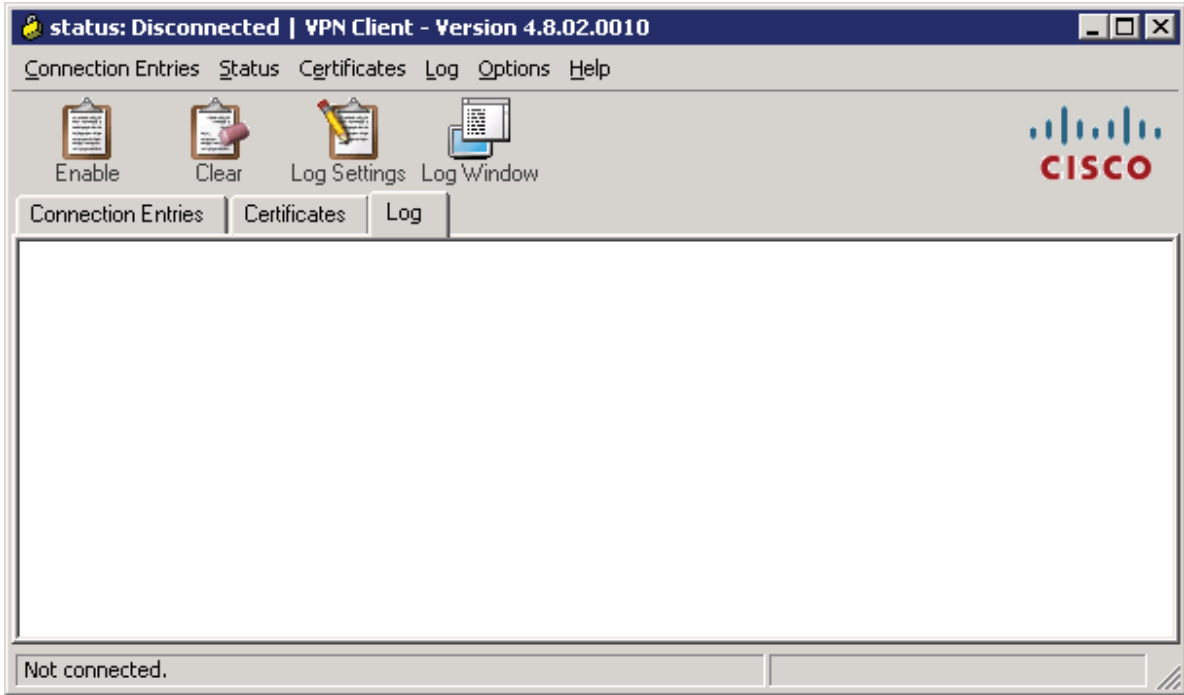
Once the VPN Client is open, you will need to create a new connection profile to connect to HQ. Click the **New** button. Create the new connection with any name and description you want. For host, enter the IP of HQ's Serial0/0/0 interface, 192.168.12.2. The host IP address represents the IP address of the VPN server or concentrator to which you wish to connect. In this case, HQ is running the Easy VPN Server and will function as such. Use the group name and password previously configured in the Easy VPN wizard. Click **Save** when you are done configuring.



**Figure 13-3: Create New VPN Connection Dialog**

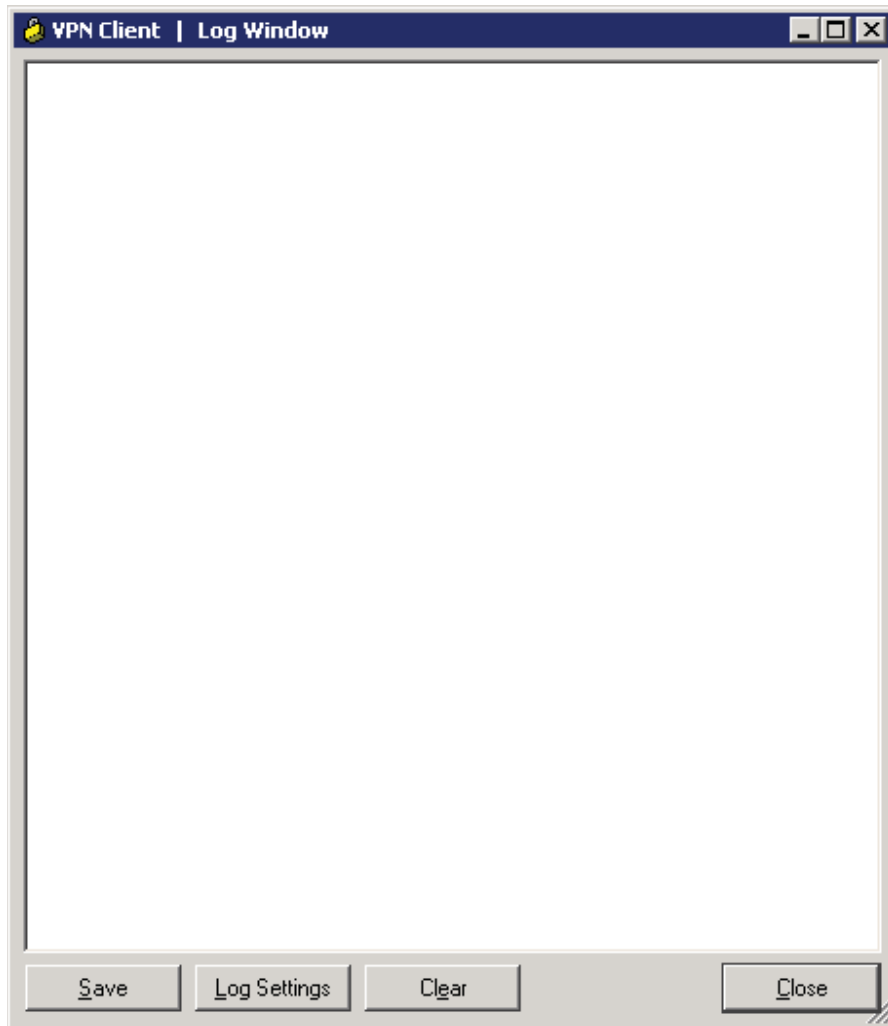
You should see your new profile appear in the profiles list. Before connecting, click the **Log** tab so you can enable logging before attempting to connect. Logging is not normally required but it is helpful in this lab to watch the VPN client connect.





**Figure 13-4: VPN Client Log Tab**

Click **Log Window** to open up logging in a separate window.



**Figure 13-5: Log Window**

While you have the log window open, go back to the main VPN client window and click **Log Settings**. Change the logging settings for IKE and IPsec to **3 – High**. Click **OK** to apply these settings.

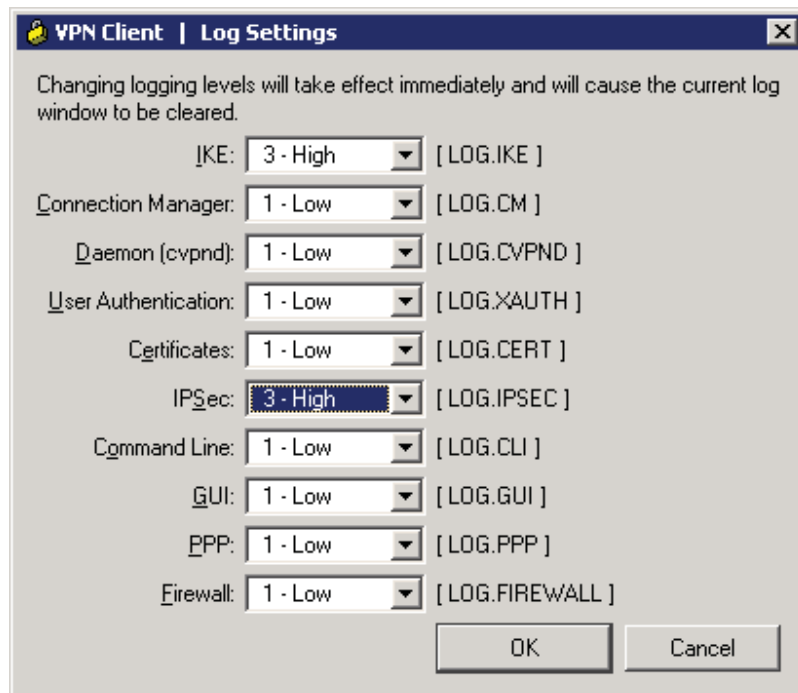


Figure 13-6: Logging Settings

Click **Enable** to enable logging. The **Enable** button should change to a **Disable** button.

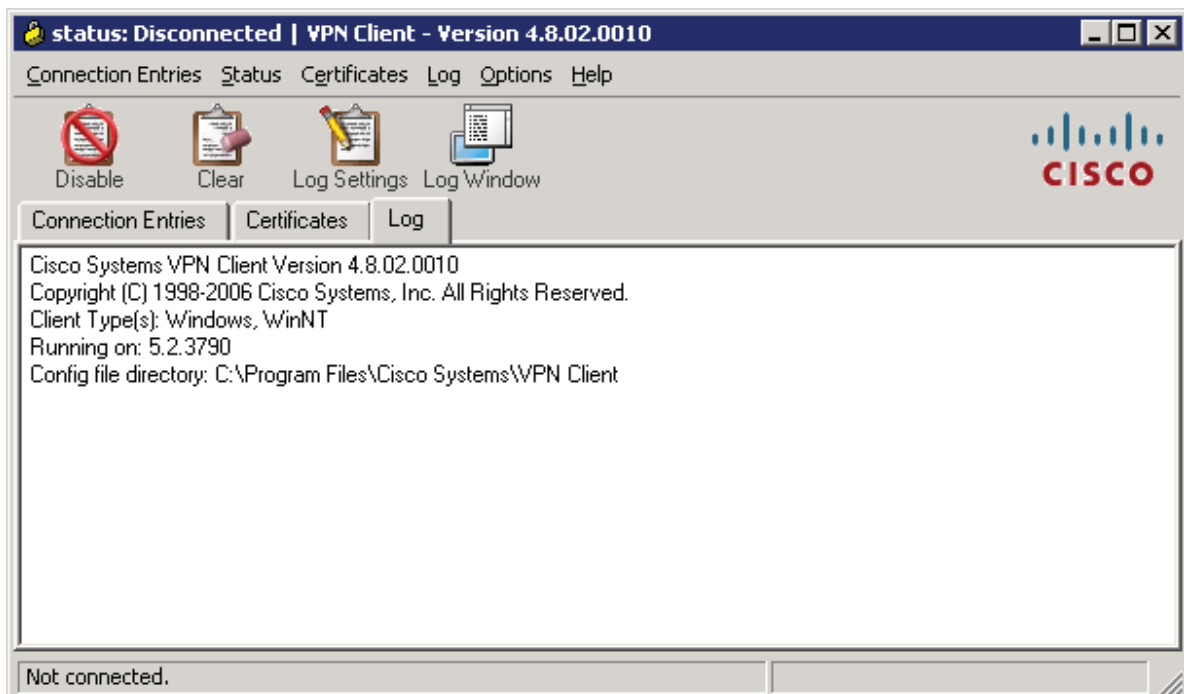
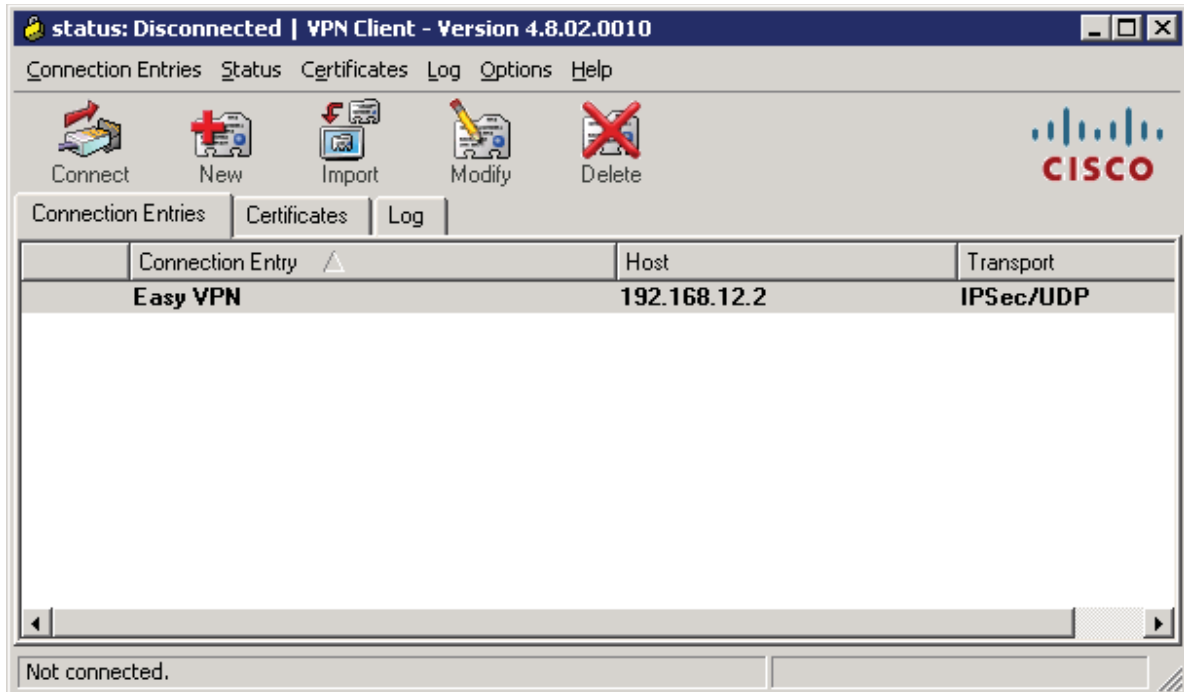


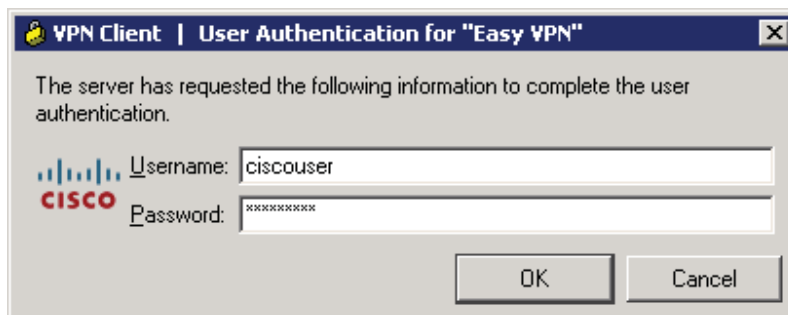
Figure 13-7: Log Tab with Logging Enabled

Click the **Connection Entries** tab, and double-click the entry or click **Connect** to connect to this profile.



**Figure 13-8: VPN Client Connections Tab**

While the VPN client tries to connect to the VPN, it will prompt you for a username and password. Enter the user credentials you specified earlier during the VPN client wizard.



**Figure 13-9: User Authentication Prompt**

When the VPN has successfully connected, you should see a locked padlock icon in the system tray.

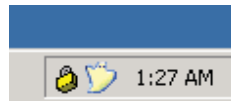


Figure 13-10: VPN Client System Tray Icon, Status: Connected

You can also see that your connection has populated the log window with information. After reviewing the information here, click **Close** to close this window. This logging functionality can be very useful when troubleshooting VPN client problems.

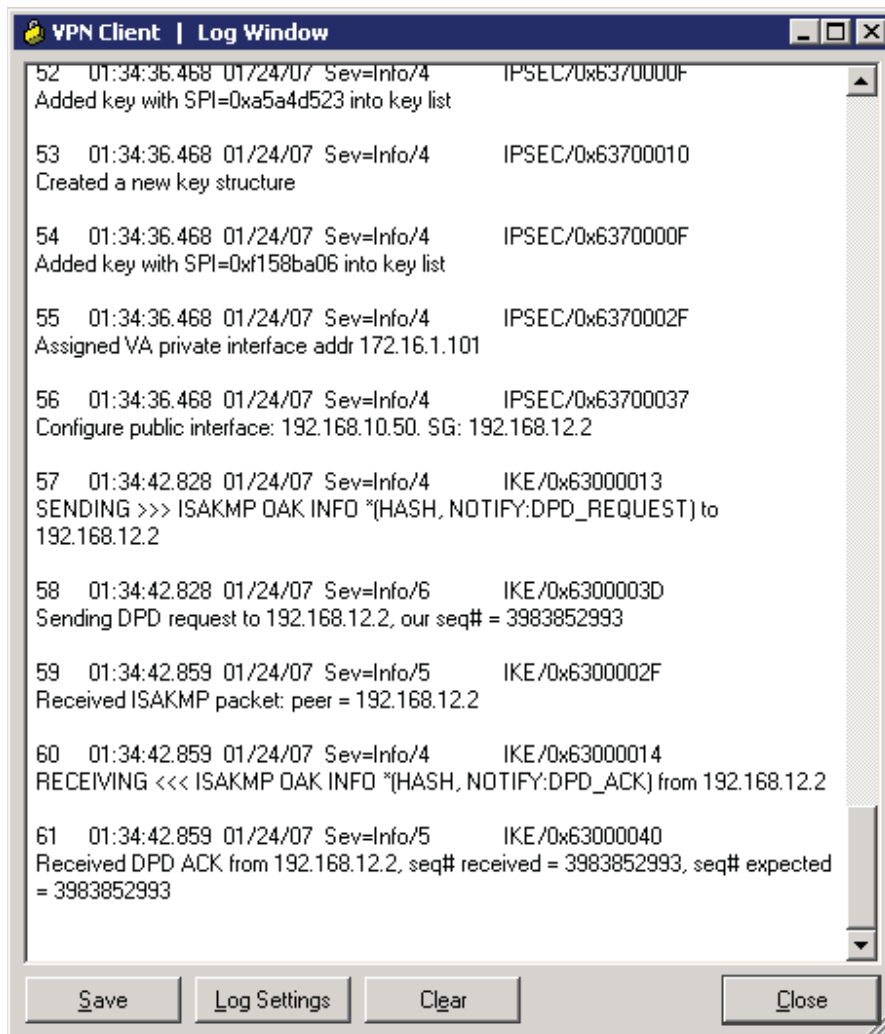


Figure 13-11: Log Window, Populated with Connection Messages

To view VPN connection statistics, right-click the padlock icon in the system tray and click **Statistics....**

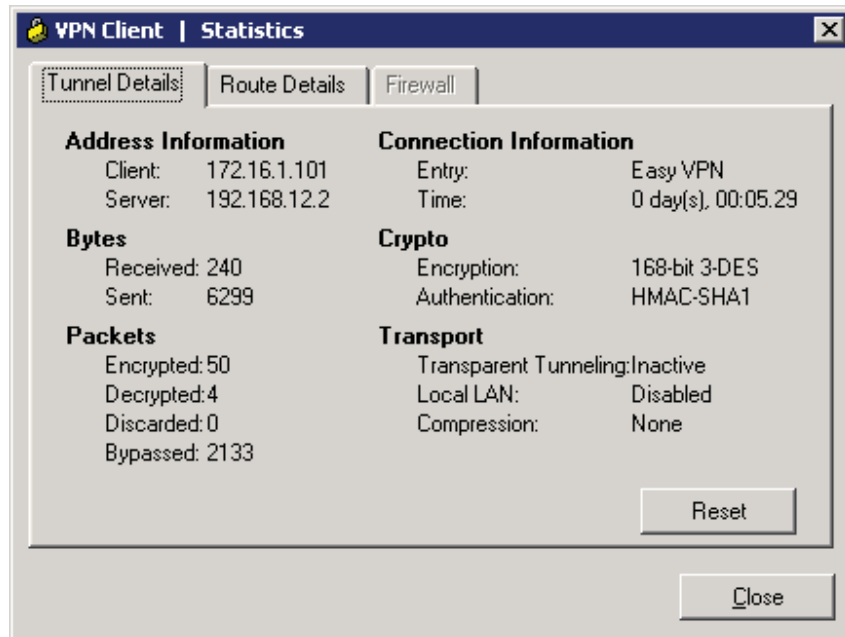


Figure 13-12: VPN Client Statistics

Click the **Route Details** tab to view routes sent out through split tunneling.

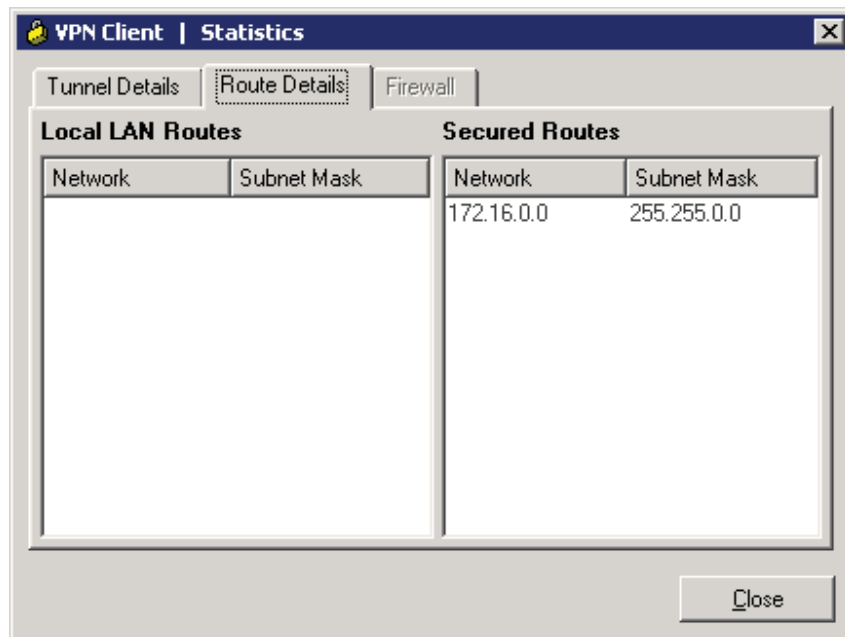
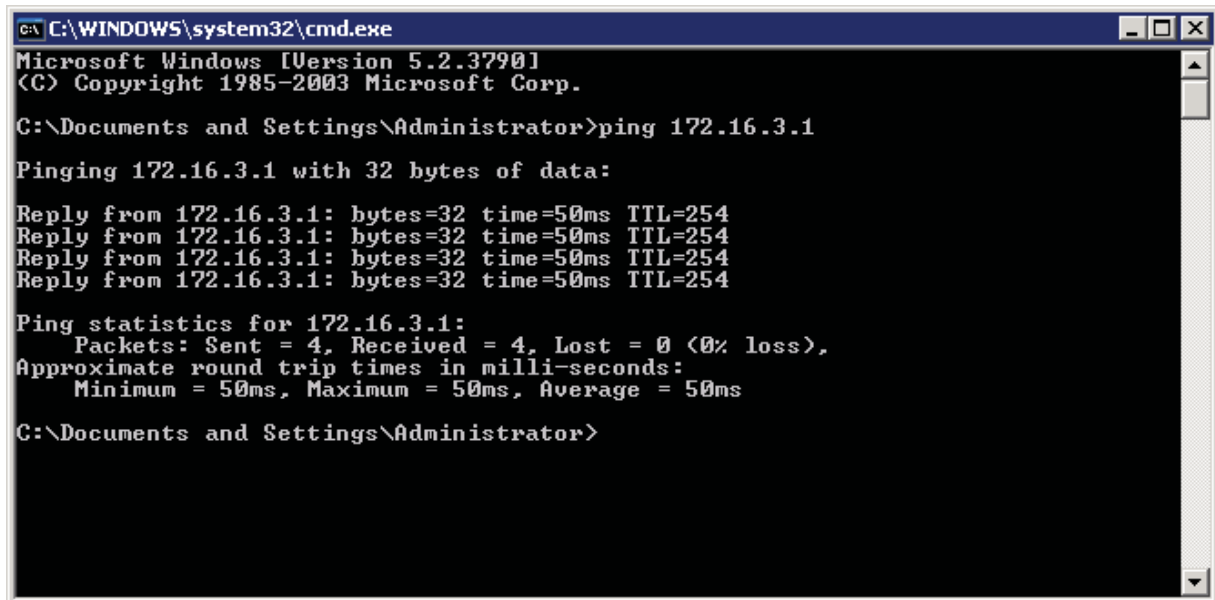


Figure 13-13: Route Details Tab

Close the Statistics window when done.

## Step 14: Test Inside VPN Connectivity

Now that the host has connected to the VPN, open up the command prompt again (see earlier steps if you don't remember how) and ping HQ2's loopback. This time, it should be successful.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 172.16.3.1

Pinging 172.16.3.1 with 32 bytes of data:

Reply from 172.16.3.1: bytes=32 time=50ms TTL=254
Reply from 172.16.3.1: bytes=32 time=50ms TTL=254
Reply from 172.16.3.1: bytes=32 time=50ms TTL=254
Reply from 172.16.3.1: bytes=32 time=50ms TTL=254

Ping statistics for 172.16.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 50ms, Maximum = 50ms, Average = 50ms

C:\Documents and Settings\Administrator>
```

Figure 14-1: Successful Pings With VPN

## Step 15: Verify VPN Operation using the CLI

There are many command line **show** commands that you can use to verify VPN configuration. You can use the **show crypto isakmp sa** and **show crypto ipsec sa** commands to verify crypto security associations.

```
HQ# show crypto isakmp sa
dst          src          state          conn-id slot status
192.168.12.2 192.168.10.50 QM_IDLE          1      0 ACTIVE

HQ# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: mymap, local addr 192.168.12.2

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): (172.16.2.100/255.255.255.255/0/0)
current_peer 192.168.10.50 port 1471
    PERMIT, flags={}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 44, #pkts decrypt: 44, #pkts verify: 44
    #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.: 192.168.12.2, remote crypto endpt.: 192.168.10.50
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0xECC953E1(3972617185)
```

```
inbound esp sas:
spi: 0xB18FB7F1(2978985969)
  transform: esp-3des esp-sha-hmac ,
  in use settings = {Tunnel, }
  conn id: 3001, flow_id: NETGX:1, crypto map: mymap
  sa timing: remaining key lifetime (k/sec): (4600939/3552)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

inbound ah sas:

inbound pcp sas:

```
outbound esp sas:
spi: 0xECC953E1(3972617185)
  transform: esp-3des esp-sha-hmac ,
  in use settings = {Tunnel, }
  conn id: 3002, flow_id: NETGX:2, crypto map: mymap
  sa timing: remaining key lifetime (k/sec): (4600946/3551)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

Use the command **show ip local pool** to view IP pool information.

```
HQ# show ip local pool
```

Pool	Begin	End	Free	In use
VPNCLIENTS	172.16.2.100	172.16.2.200	100	1

## Step 16: Disconnecting the VPN Client

Right-click the padlock icon in the system tray and click **Disconnect**. The VPN client will disconnect.

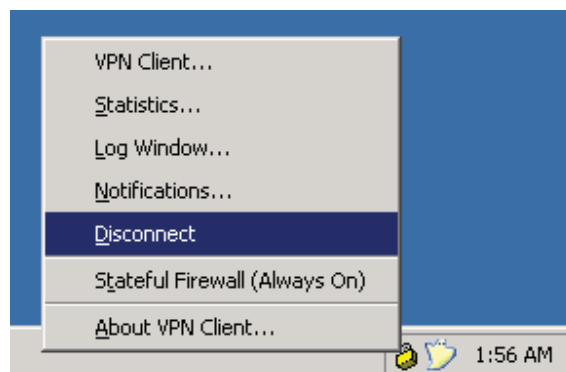


Figure 16-1: Disconnecting from the VPN via the System Tray Icon



The padlock should first change to a padlock with an 'X' through it, indicating that it is disconnecting. It will change to an unlocked icon, indicating no VPN connection. Finally, right-click the padlock and click **Exit** to quit the VPN client.

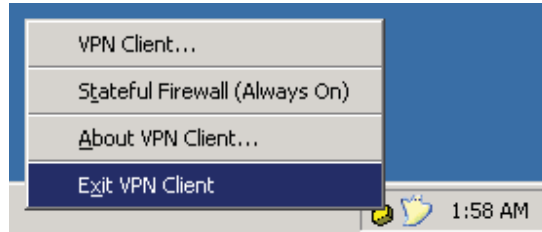


Figure 16-2: Exiting the VPN Client via the System Tray Icon

## Final Configurations

```
ISP# show run
hostname ISP
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 192.168.12.1 255.255.255.0
 clock rate 64000
 no shutdown
end

HQ# show run
hostname HQ
!
aaa new-model
!
aaa authentication login default local none
aaa authentication login VPNAUTH local
aaa authorization network VPNAUTH local
!
username cisco password 0 cisco
username ciscouser password 0 ciscouser
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp keepalive 30 5
crypto isakmp xauth timeout 60
!
crypto isakmp client configuration group ciscogroup
 key ciscogroup
 pool VPNCLIENTS
 acl 100
 netmask 255.255.255.0
!
crypto ipsec transform-set mytrans esp-3des esp-sha-hmac
!
crypto dynamic-map mymap 10
 set transform-set mytrans
 reverse-route
!
```

```

crypto map mymap client authentication list VPNAUTH
crypto map mymap isakmp authorization list VPNAUTH
crypto map mymap client configuration address respond
crypto map mymap 10 ipsec-isakmp dynamic mymap
!
interface Loopback0
 ip address 172.16.2.1 255.255.255.0
!
interface Serial0/0/0
 ip address 192.168.12.2 255.255.255.0
 crypto map mymap
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.23.2 255.255.255.0
 clock rate 64000
 no shutdown
!
router eigrp 1
 redistribute static
 network 172.16.0.0
 no auto-summary
!
ip local pool VPNCLIENTS 172.16.2.100 172.16.2.200
ip route 0.0.0.0 0.0.0.0 192.168.12.1
!
access-list 100 permit ip 172.16.0.0 0.0.255.255 any
end

```

```

HQ2# show run
hostname HQ2
!
interface Loopback0
 ip address 172.16.3.1 255.255.255.0
!
interface Serial0/0/1
 ip address 172.16.23.3 255.255.255.0
 no shutdown
!
router eigrp 1
 network 172.16.0.0
 no auto-summary
end

```