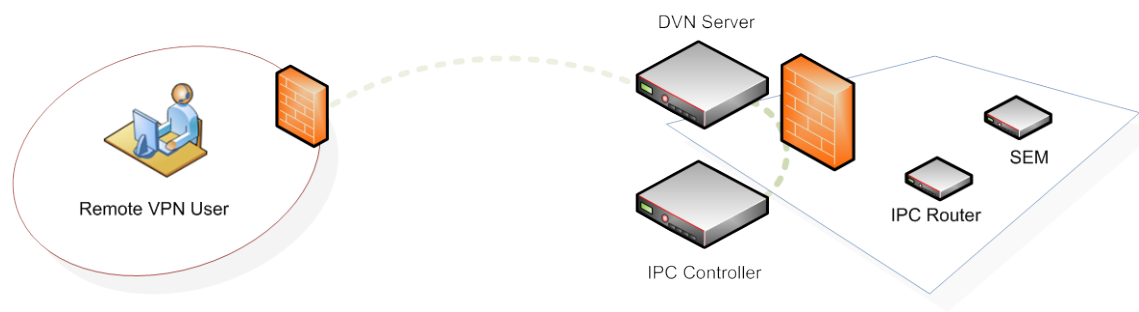




Implementing DVN

directPacket Product Guide



1 DVN and the IPC Community

The Secure Dedicated Versatile Network (DVN) Server is a hardened internet facing device with its own integrated firewall technology designed to defend itself in hostile environments. Its primary functions are to perform signaling and media validation and to provide the secure transmission of IP video, audio (SIP/H3.23), and provisioning packets without modifying or impeding the integrity of such packets.

The Secure Dedicated Versatile Network (DVN) Server is positioned in the Internet Cloud and listens for Secure connection requests from Industry Standard VPN clients.

The communication between the IPC Controller and the Dedicated Versatile Network (DVN) Server is established via one single TCP (only)* TLS/SSLv3 AES 256 bit encrypted stream. The communication between the Dedicated Versatile Network (DVN) server and a VPN client is established via industry standard VPN protocols. Once the link between the DVN server and the VPN client has been established the solution then directs all video, audio, and provisioning packet transmissions to the secure IP controller which then disseminates those packets to their corresponding destination within the Secure IPC Community.

2 Setting up the DVN Server

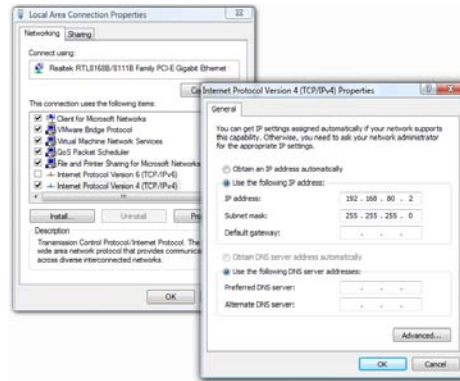
Summary: This section will walk you through configuring IP settings and connecting your DVN Server to your IPC Controller.

Checklist:

You need the following directPacket devices:
DVN Server
IPC Controller

2.1

Configure your notebook IP address to 192.168.81.2 with a subnet of 255.255.255.0.



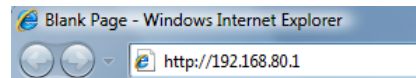
2.2

Connect a notebook via the service port on the IPC Controller using a crossover cable.



2.3

Open the URL: **http://192.168.81.1**
This URL is only accessible from this port.



2.4

Once the following page is displayed, login using:

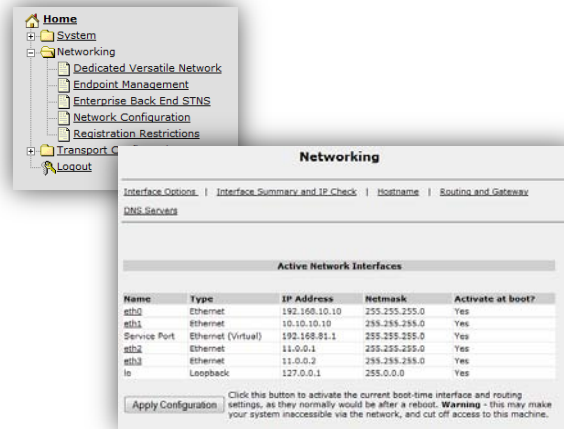
Username: admin
Password: 12pilot34



2.5

Once successfully logged in, you will see the page displayed above.

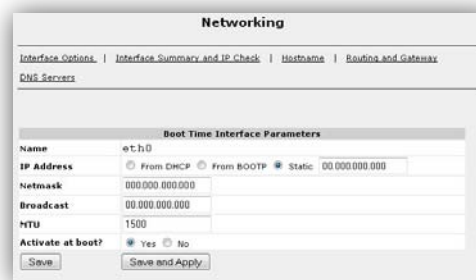
First, we will configure the network ports. Select **Networking** and then select **Network Configuration**.



2.6

Select eth0.

Set the **IP address**, **Netmask**, **Broadcast** and **MTU** settings of your choice. If there isn't a preferred MTU setting, use 1500. Once completed, click **Save**.

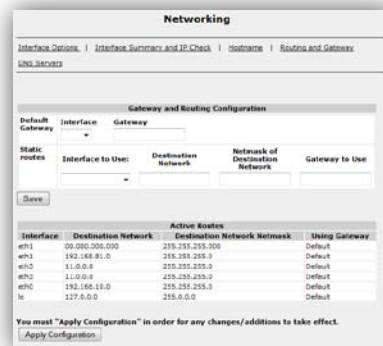


2.7

Select the **Routing and Gateway** link.

Click the Interface drop down and choose eth0 and specify the Gateway settings.

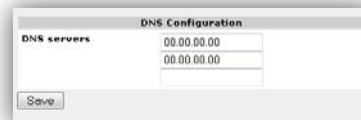
Click **Save**.



2.8

Select **DNS Servers** and enter in the appropriate DNS servers you have received from your network administrator.

Select the Interface Options link and click **Save** and then click on **Apply Configuration**.



2.9

Under Interface Summary and IP Check, verify the Speed and Duplex are set to 100 or 1000 Mbits Full for eth0 and that there is no IP conflicts detected. If there is an IP conflict, please revisit the IP configuration and verify your network settings.



eth0 Summary		eth1 Summary	
MAC Address:	00:10:F3:0F:2B:1C	MAC Address:	00:10:F3:0F:2B:1D
IP Address:	00.000.000.000	IP Address:	Unknown (15536)
Current link speed:	1000Mbps	Current link speed:	Unknown (15536)
Current Duplex:	Full	Current Duplex:	Unknown (15536)
IP Conflict Detected?	No	IP Conflict Detected?	No

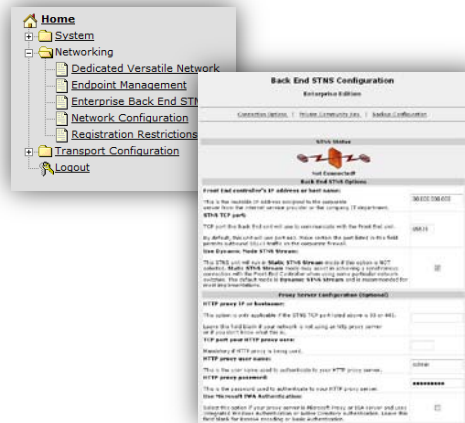
eth2 Summary		eth3 Summary	
MAC Address:	00:10:F3:0F:2B:1E	MAC Address:	00:10:F3:0F:2B:1F
IP Address:	11.0.0.1	IP Address:	11.0.0.2
Current link speed:	Unknown (15536)	Current link speed:	Unknown (15536)
Current Duplex:	Unknown (15536)	Current Duplex:	Unknown (15536)
IP Conflict Detected?	No	IP Conflict Detected?	No

2.10

Navigate to **Networking** and **Enterprise Back End STNS**. Enter the IP Address or host name of the IPC Controller.

If you are using a proxy server, enter the address and TCP port of the HTTP proxy server and authentication information if necessary. Otherwise, leave them blank.

Scroll to the bottom of the page and click Connect. Watch your browser, and do not navigate away from this page. This process can take up to 120 seconds.



3 Configuring DVN's H.323 Settings

Summary: Configuration of H.323 and hierarchy settings within DVN.

Checklist:

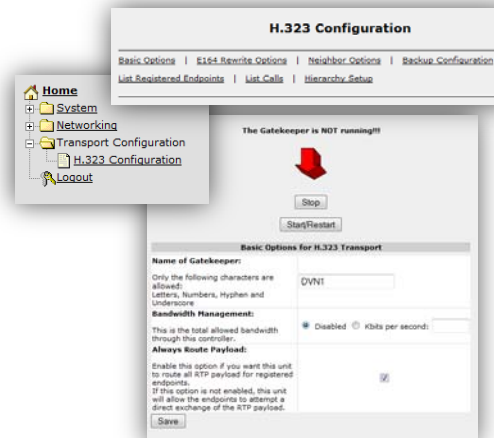
DVN Server Setup waiting for connections.

3.1

In the left hand navigation pane, choose: **Transport Configuration** and then **H.323 Configuration**.

Change the Gatekeeper to a unique name. For example: DVN1, DPDVN1, DVN01.

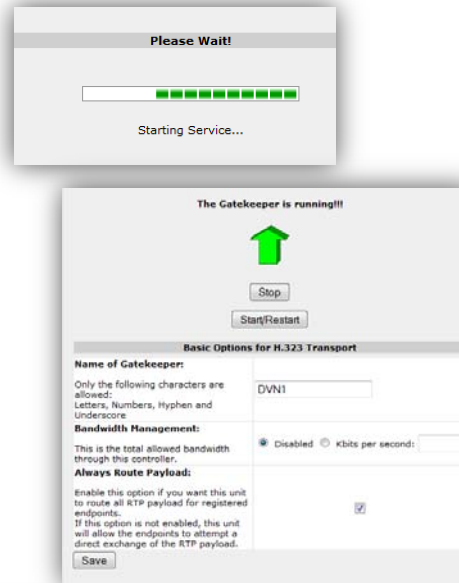
Click **Save** and then **Start/Restart Gatekeeper**.



3.2

Press the **Start/Restart** button. The process can take up to two minutes to complete. Watch the browser's progress indicator and do not navigate away from this page.

Once the process is complete, the user will be redirected to the status page shown below.

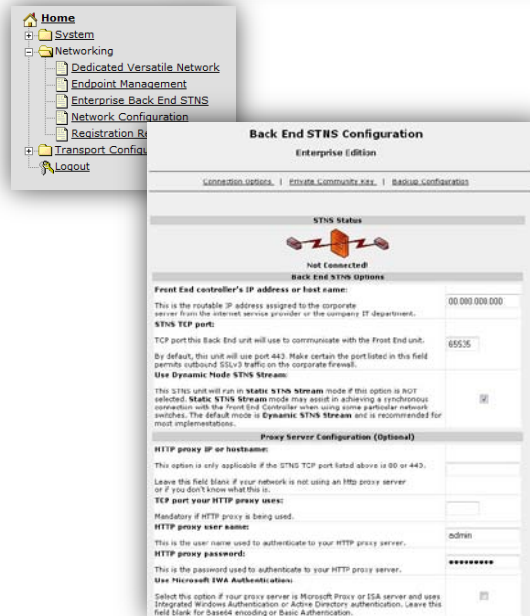


3.3

Navigate to **Networking** and **Enterprise Back End STNS**. Enter the IP Address or host name of the IPC Controller.

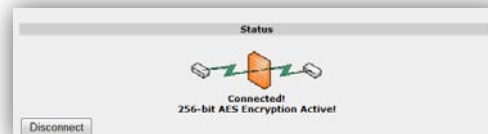
If you are using a proxy server, enter the address and TCP port of the HTTP proxy server and authentication information if necessary. Otherwise, leave them blank.

Scroll to the bottom of the page and click Connect. Watch your browser, and do not navigate away from this page. This process can take up to 120 seconds.



3.4

The DVN Server is now connected to the IPC Controller and integrated into the IPC Network.



4 Configuring Endpoint Management

Summary: Configuration of Endpoint Management for use with the SEM server and provisioning data where needed.

Checklist: DVN Server awaiting connections. Established IPC Community. SEM Server with endpoint management modules on IPC Controller.

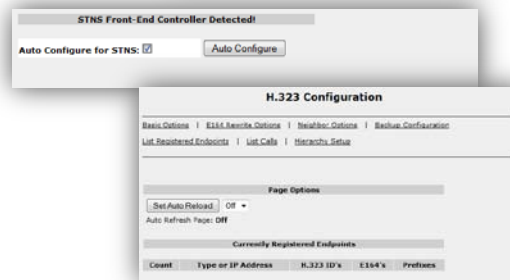
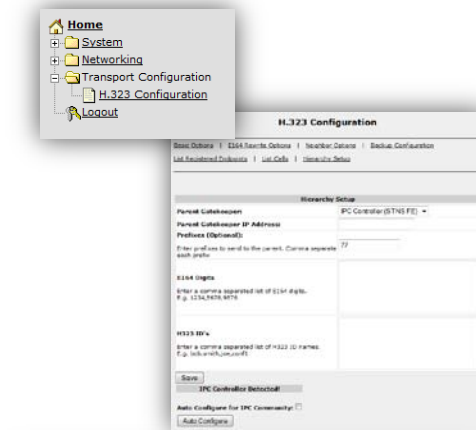
4.1

Next, we need to list which endpoints will be traversing the firewall.

Navigate to **Transport Configuration, H.323 Configuration, and Hierarchy Setup.**

Place a checkmark in the **Auto Configure for STNS** and click **Auto Configure**. The E164's for all registered endpoints will show up in the E164 digits field. Remove any E164 which you do NOT wish to traverse the firewall. Prefixes can be added at this time if desired. Click **Save** and then **Start/Restart Gatekeeper**.

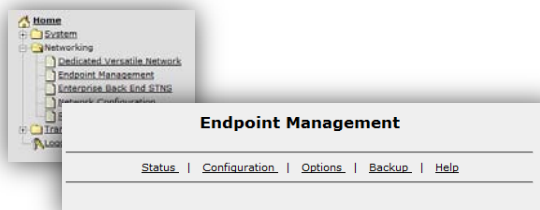
Once a user has connected to DVN, their H.323 connection can be listed under **Transport Configuration, H.323 Configuration, and List Registered Endpoints.**



4.2

To allow provisioning and endpoint management, the Endpoint Management service must be configured. In the following steps, the endpoints will be configured through the DVN server.

Navigate to **Networking – Endpoint Management – Configuration.**



4.3

Methods to add endpoints to the SEM management scope:

- Scan Address Pool.
The following formats are allowed:
CIDR – 192.168.1.0/24
Range – 192.168.1.1-254
Wild – 192.168.1.*
Combo – 192.168.1-6*

Previous scans will be saved in the IP range field.

- The DVN server can also search the H.323 registration table. There will be a checkbox under Scan Address Pool section. Simply check the box and click Scan.
- Manually Add endpoints. These addresses will not be saved in the fields.

Once scanned, you will be prompted with Save Only or Restart Service. Click **Restart Service**.

The screenshot shows the 'Endpoint Management' configuration page. It has a navigation bar with 'Status', 'Configuration', 'Options', 'Backup', and 'Help'. The main content is divided into two sections: 'Scan Address Pool' and 'Manually Add'. Both sections have fields for 'Address Pool', 'SNMP Community Name', 'User Name', and 'Password'. The 'Scan Address Pool' section has a 'Scan' button, and the 'Manually Add' section has an 'Add' button. A 'Configuration Saved' dialog box is overlaid on top, with the message 'You must restart the service before the changes will take effect.' and two buttons: 'Save Only' and 'Restart Service'.

4.4

Once the service is restarted, the IPC Controller must inventory the IPC-Routers and DVN server to manage endpoints.

Log into the IPC-Controller. Navigate to **Networking – Endpoint Management – Configuration**.

Click **Inventory Community**.

The screenshot shows the 'Endpoint Management' configuration page with a sidebar on the left containing a tree view of the system's configuration. The main content area is titled 'Endpoint Management' and has a navigation bar with 'Status', 'Configuration', 'Backup', and 'Help'. The main content is divided into two sections: 'Perform Community Inventory' and 'Update Community'. The 'Perform Community Inventory' section has an 'Inventory Community' button. The 'Update Community' section has an 'Update Community' button and a warning message: '*WARNING* This will disrupt communication'.

4.5

The IPC Controller will take an inventory of the IPC Routers and DVN server. Once complete, click Restart Service. This will not interrupt any existing calls and will only restart the Endpoint Management service.



4.6

Endpoint Management configuration is complete.

5 Configure DVN Settings

Summary: Configure master SEM unit and Endpoint Management modules.

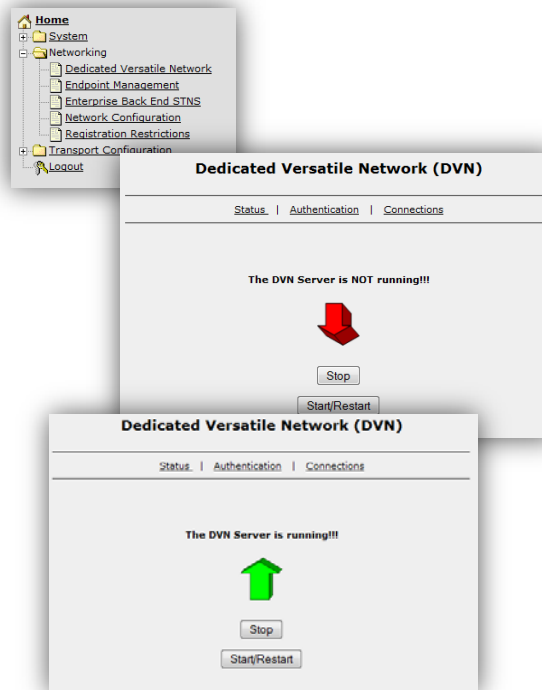
Checklist:

DVN Server Setup waiting for connections

5.1

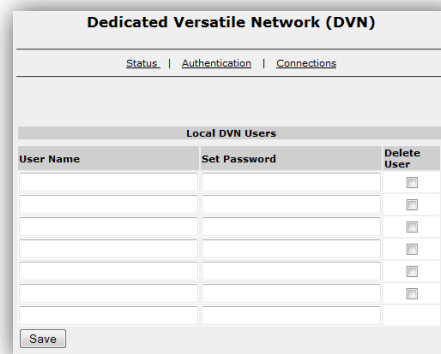
Select Networking – Dedicated Versatile Network on the left hand menu.

Select Start/Restart to start the DVN service.



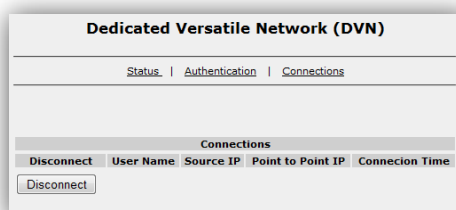
5.2

Users are setup under Authentication. There are no limits to the number of users in the system. Multiple users may use the same login. Licensing is based on concurrent connections.



5.3

Under Connections, if there are any active calls they will be listed and can be disconnected if necessary.



6 Configure Windows VPN Client

Summary: Configure master SEM unit and Endpoint Management modules.

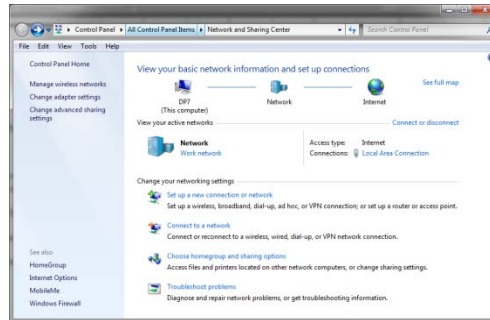
Checklist:

- DVN Server Setup waiting for connections
- Windows Client with a network connection.

Although Windows Vista, Windows XP and Windows 2000 are able to connect using PPTP connections, this manual will only cover Windows 7.

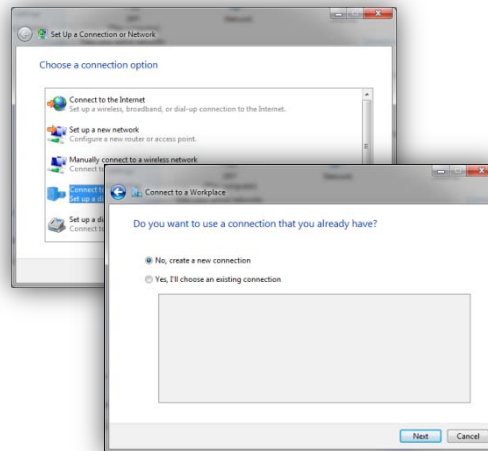
6.1

In the Control Panel and Network and Sharing Center, choose **Set up a new connection or network**.



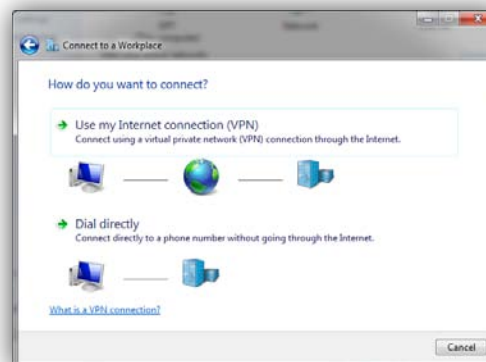
6.2

On the Set Up a Connection or Network dialog, choose **No, create new connection**. Then choose **Connect to a workplace**.



6.3

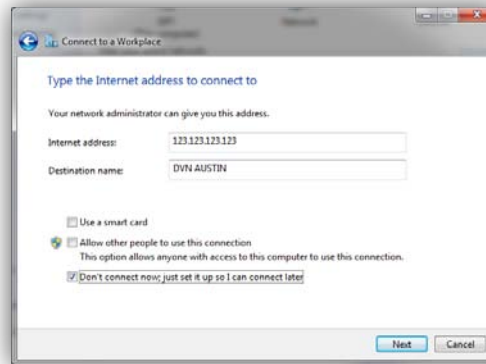
Next, choose **Use my Internet Connection (VPN)**.



6.4

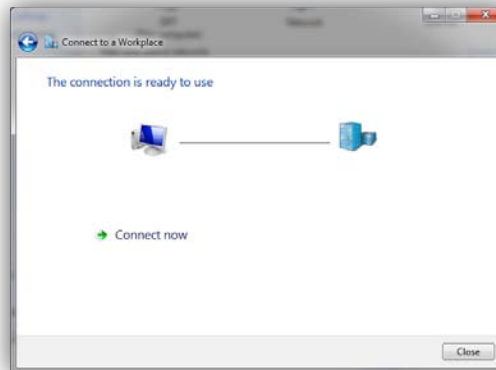
Enter the Internet Address of the DVN Server and enter a destination name.

Check **Don't connect now, just set it up so I can connect later.**



6.5

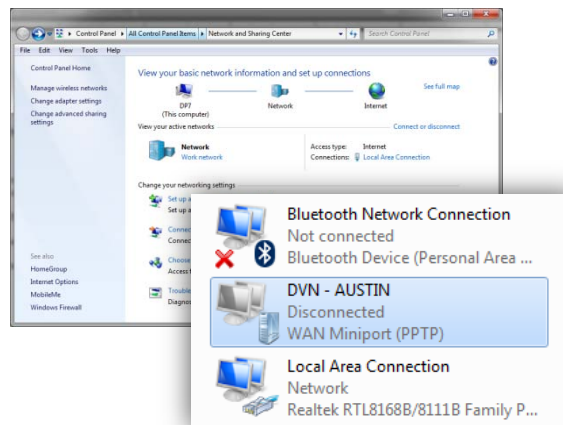
Click **Close.**



6.6

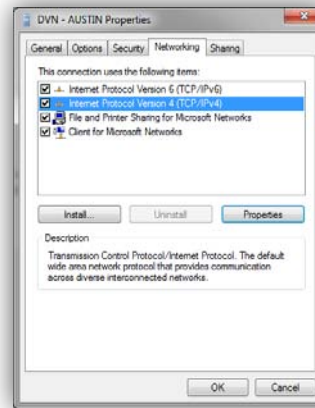
We need to modify the properties of the VPN connection. In the Networking and Sharing Center, choose **Change Adapter Settings.**

Right Click on the DVN connection you just created. Choose Properties.



6.7

In the properties, select the Networking Tab. Then select, **Internet Protocol Version 4(TCP/IPv4)** and click on **Properties**.

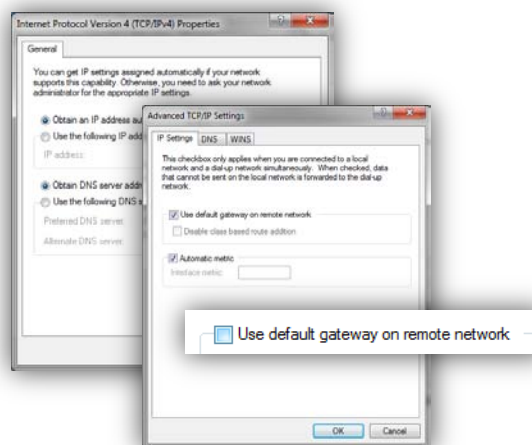


6.8

Click Advanced.

Next, Uncheck Use default gateway on remote network. If this is left checked, all of the traffic will be routed through the DVN server. As a result, web pages, email, and any other services will not be work properly.

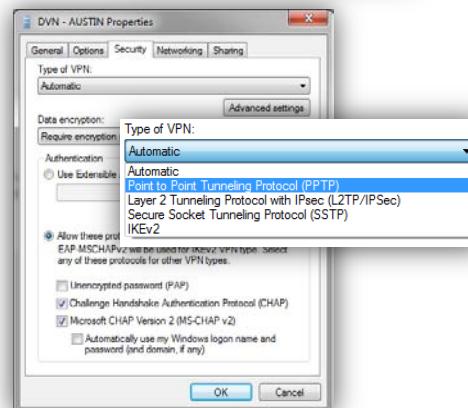
Click OK and OK.



6.9

Next, under the Security tab, select **Point to Point tunneling Protocol (PPTP)** under Type of VPN.

Click OK.



6.10

The VPN connection is setup and complete. The system can log into the DVN network and place audio or video calls with a username and password provided by the administrator of the DVN server.

Where provisioning data is necessary, such as PVX, the IP of 172.20.1.1 is the IP for the H.323 Gatekeeper.

7 Mac Client Configuration

Checklist:

DVN Server Setup waiting for connections
Apple Client with a network connection.

7.1

To set up a VPN connection, open up the settings panel in OSX. Click on **Network**.

Click on the + sign on the bottom left corner to add another network connection.



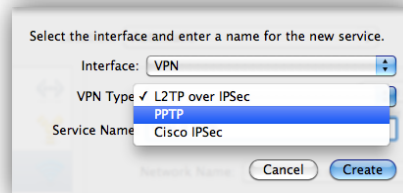
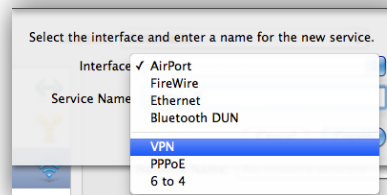
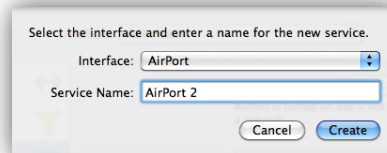
7.2

In the next dialog box, change the Interface to VPN.

Choose PPTP as the VPN type.

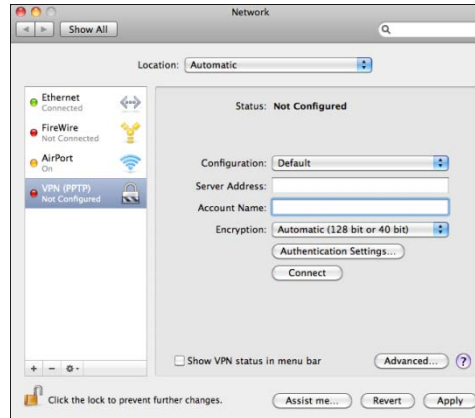
Change the Service name to DVN or a name that corresponds to your DVN server.

Click **Create**.



7.3

The VPN connection is now created. To configure the connection, select it in the left pane under Network.



7.4

Enter your name and password. Click OK and save changes. Close out of Network settings.

You will be able to connect to the DVN server through the VPN connection at anytime by selecting it in the drop down panel on the top of the screen.



7.5

The VPN connection is setup and complete. The system can log into the DVN network and place audio or video calls with a username and password provided by the administrator of the DVN server.

Where provisioning data is necessary, the IP of 172.20.1.1 is the IP for the H.323 Gatekeeper.