

Virtual Private Network and Remote Access

Introduction

A virtual private network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link.

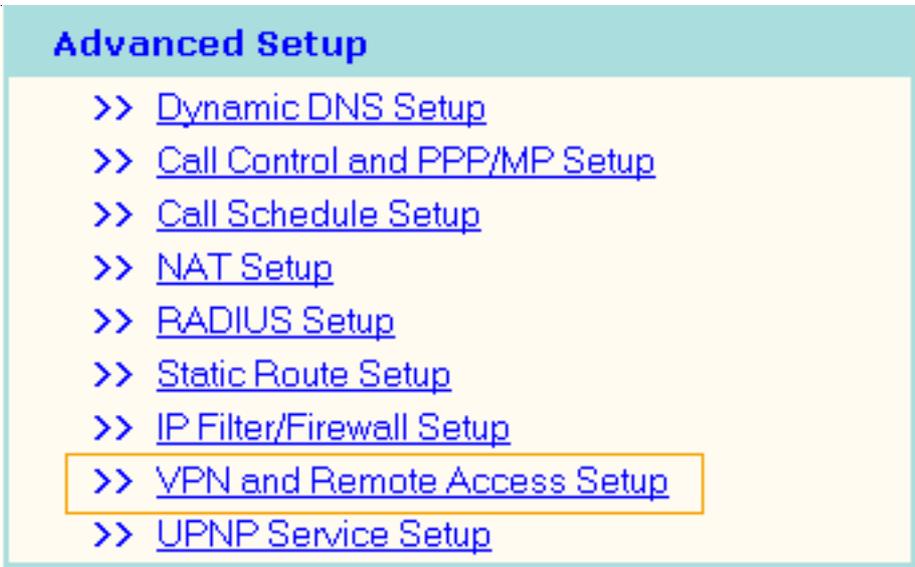
There are two types of VPN connections: the remote dial-in access VPN connection and the LAN-to-LAN VPN connection. The first, Remote Dial-In Access means the router allows a remote access node, a NAT router or a single user computer, to dial into a VPN router through the Internet to access the network resources of the remote network. The second, LAN-to-LAN Access provides a solution to connect two independent LANs for mutual sharing of network resources. For example, the head office network can access the branch office network, and vice versa.

Virtual private networking (VPN) supports Internet-industry standards technology to provide customers with open interoperable VPN solutions such as Internet Protocol Security (IPSec) and Layer 2 Tunneling Protocol (L2TP) as well as Point-to-Point Tunneling Protocol (PPTP).

This chapter explains the capabilities of VPNs and remote access on the router. Use the following setup links on the Setup Main Menu to setup VPN and remote access functions.

Advanced Setup

> VPN and Remote Access Setup



The screenshot shows a menu titled "Advanced Setup" with a light blue header. Below the header is a list of menu items, each preceded by two right-pointing chevrons (">>>"). The item "VPN and Remote Access Setup" is highlighted with a yellow rectangular box. The other items are: "Dynamic DNS Setup", "Call Control and PPP/MP Setup", "Call Schedule Setup", "NAT Setup", "RADIUS Setup", "Static Route Setup", "IP Filter/Firewall Setup", and "UPNP Service Setup".

- >> [Dynamic DNS Setup](#)
- >> [Call Control and PPP/MP Setup](#)
- >> [Call Schedule Setup](#)
- >> [NAT Setup](#)
- >> [RADIUS Setup](#)
- >> [Static Route Setup](#)
- >> [IP Filter/Firewall Setup](#)
- >> [VPN and Remote Access Setup](#)
- >> [UPNP Service Setup](#)

The VPN and Remote Access Setup main menu has five main sub menus.

- >> [Remote Access Control Setup](#)
- >> [PPP General Setup](#)
- >> [VPN IKE / IPSec General Setup](#)
- >> [Remote Dial-In User Setup](#)
- >> [LAN-to-LAN Profile Setup](#)

The **Remote Access Control Setup** allows you to enable each type of VPN service or disable it for VPN pass-through purpose. For example, you can enable IPSec and L2TP VPN service on your router and disable PPTP VPN service if you intend running a PPTP server inside your LAN. Further, you also can enable or disable the ISDN remote access including remote dial-in and LAN-to-LAN access.

Use the **PPP General Setup** to configure PPP authentication method as well as IP assignment range for remote dial-in user. This sub menu only apply to PPP related VPN type such as PPTP, L2TP and L2TP over IPSec, and ISDN-based remote access.

The **VPN IKE / IPSec General Setup** let you configure a common Pre-shared key and security method for remote dial-in user or node(LAN-to-LAN) which uses dynamic ip.

Use **The Remote Dial-In User Setup** to create dial-in user accounts. Vigor router supports three types of dial-in methods, PPTP, L2TP, L2TP over IPSec and ISDN. The PPTP VPN is compatible with all Windows platforms which have PPTP protocol built-in. The L2TP and L2TP over IPSec are compatible with Window 2000 and XP.

Use **The LAN-to-LAN Profile Setup** to create profiles for LAN to LAN VPNs. Vigor router supports four types of LAN-to-LAN VPN, IPSec Tunnel, PPTP, L2TP, L2TP over IPSec and ISDN. Simultaneously you can establish up to 8 VPN tunnels including remote dial-in users.

1. Remote Access Control Setup

Check the box to enable the VPN service type you want to provide. If you intend running a VPN server inside your LAN, you should uncheck the appropriate protocol below to allow pass-through, as well as the appropriate NAT settings. For example, DMZ or open port. You also can allow the ISDN dial-in by checking **Enable ISDN Dial-In**.

> **Advanced Setup** > **Remote Access Control Setup** << [Main Menu](#)

Remote Access Control Setup << [Back](#)

<input checked="" type="checkbox"/>	Enable PPTP VPN Service
<input checked="" type="checkbox"/>	Enable IPsec VPN Service
<input checked="" type="checkbox"/>	Enable L2TP VPN Service
<input checked="" type="checkbox"/>	Enable ISDN Dial-In

Note : If you intend running a VPN server inside your LAN, you should uncheck the appropriate protocol above to allow pass-through, as well as the appropriate NAT settings.

2. PPP General Setup

PPP/MP Protocol

Dial-In PPP Authentication:

PAP: Selecting this option will force the router to authenticate dial-in users with the PAP protocol.

PAP or CHAP: Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.

Mutual Authentication (PAP): Enable this only if the connecting router requires mutual authentication. By default, the option is set to **No**.

PPP General Setup

PPP/MP Protocol

Dial-In PPP Authentication:

Mutual Authentication (PAP): Yes No

Username:

Password:

<< [Back](#)

IP Address Assignment for Dial-In Users

Start IP Address

IP Address Assignment for Dial-In Users

Start IP Address: Enter a start IP address to be assigned to the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 to be the Start IP Address.

3. VPN IPSec / IKE General Setup

Set up a common Pre-shared key and security method for remote dial-in user or non-specified node(LAN to LAN) which do not have fixed ip address. This setup only apply to IPSec related type of VPN. For example, L2TP over IPSec and IPSec tunnel.

> [Advanced Setup](#) > [VPN IKE / IPSec General Setup](#) << [Main Menu](#)

VPN IKE/IPSec General Setup << [Back](#)

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method

Pre-Shared Key

Re-type Pre-Shared Key

IPSec Security Method

Medium (AH)
Data will be authentic, but will not be encrypted.

High (ESP)

Data will be encrypted and authentic.

IKE Authentication Method: Currently only support Pre-Shared Key authentication.

Pre-Shared Key: Specify a key for IKE authentication.

Re-type Pre-Shared-Key: Confirm pre-shared-key.

IPSec Security Method: Select allowed IPSec security methods.

Medium (AH): Data will be authentic, but not be encrypted.

High (ESP): Data will be encrypted and authentic.

For VPN dial out, you also should set up a common Pre-shared key and security method which assigned by each LAN-to-LAN profile. This setup only apply to IPSec related type of VPN. For example, L2TP over IPSec and IPSec tunnel.

4. Creating an Access Account for a Dial-in User

After completing the general setup, you must create an access account for each dial-in user. The router provides 20 access accounts for dial-in users. Besides, you can extend the user accounts to the RADIUS server through the built-in RADIUS client function.

Index	Dial-in Username	Status	Index	Dial-in Username	Status
1.	???	x	11.	???	x
2.	???	x	12.	???	x
3.	???	x	13.	???	x
4.	???	x	14.	???	x
5.	???	x	15.	???	x
6.	???	x	16.	???	x
7.	???	x	17.	???	x
8.	???	x	18.	???	x
9.	???	x	19.	???	x
10.	???	x	20.	???	x

Status: v --- Active, x --- Inactive

Set to Factory Default: Clicking here will clear all dial-in user accounts.

Index: Click the index number to open an individual setup page for a dial-in user account.

> **Advanced Setup > Remote Dial-In User Setup** << **Main Menu**

Index No. 1 << **Back** | **Clear** |

User account and Authentication	Callback Function
<input type="checkbox"/> Check to enable the user account Username <input style="width: 100%;" type="text" value="???"/> Password <input style="width: 100%;" type="password"/> Idle Timeout <input style="width: 50%;" type="text" value="300"/> second(s) <input type="checkbox"/> Specify Remote Node Peer ISDN Number or Peer VPN Server IP <input style="width: 100%;" type="text"/> Allowed Dial-In Type <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP with IPsec Policy <input style="width: 50%;" type="text" value="None"/>	<input type="checkbox"/> Check to enable Callback function <input type="checkbox"/> Specify the callback number Callback Number <input style="width: 100%;" type="text"/> <input checked="" type="checkbox"/> Check to enable Callback Budget Control Callback Budget <input style="width: 50%;" type="text" value="30"/> minute(s)

User Account and Authentication

Check to enable the user account: Check this item to activate the individual user account.

Username: Specify a username for the specific dial-in user.

Password: Specify a password for the specific dial-in user.

Idle Timeout: By default, set to 300 seconds. If the dial-in user is idle over the limit set by the timer, the router will drop this connection.

Check to enable CLID authentication: For extra security, enable the option to allow the dial-in user to connect only from a specific IP address or ISDN number.

Allowed Dial-In Type : Select allowed dial-in types.

ISDN: Allowed the remote user to make an ISDN dial-in access.

PPTP: Allowed remote dial-in user to make a PPTP VPN connection through the Internet.

L2TP: Allowed remote dial-in user to make a L2TP VPN connection through the Internet Specifies the IPsec policy to “None”, “Nice to Have”, or “Must”.

Callback Function

The callback function provides a callback service only for the ISDN dial-in user. The router owner will be charged the connection fee by the telecom.

Check to enable the Callback function: Enables the callback function.

Specify the callback number: The option is for extra security. Once enabled, the router will only call back to the specified ISDN number defined in the next parameter, Callback Number.

Callback Number: If the previous option has been enabled, enter the dial-in ISDN line number of the user here.

Check to enable Callback Budget Control: By default, the callback function has a time restriction. Once the callback budget has been exhausted, the callback mechanism will be disabled automatically.

Callback Budget (Unit: minutes): Specifies the time budget for the dial-in user. The budget will be decreased automatically per callback connection.

5. Creating a LAN-to-LAN Profile

You can create up to 16 LAN-to-LAN profiles.

LAN-to-LAN Profiles: [<< Back](#) | [Set to Factory Default](#)

Index	Name	Status	Index	Name	Status
1.	???	x	9.	???	x
2.	???	x	10.	???	x
3.	???	x	11.	???	x
4.	???	x	12.	???	x
5.	???	x	13.	???	x
6.	???	x	14.	???	x
7.	???	x	15.	???	x
8.	???	x	16.	???	x

Status: v --- Active, x --- Inactive

Set to Factory Default: Click here will clear all the LAN-to-LAN profiles.

Index: Click a number in the Index to open a detailed setting page for each profile.

Name: Indicates the name of the LAN-to-LAN profile. The symbol ??? means the profile is available.

Status: Indicates the status of the individual profiles. The symbol v means the profile is active, x means inactive.

Each LAN-to-LAN profile includes 4 subgroups: **Common Settings**, **Dial-Out Settings**, **Dial-In Settings**, and **TCP/IP Network Settings**. The following will explain each subgroup in detail.

1. Common Settings

Profile Name <input type="text" value="???"/> <input type="checkbox"/> Enable this profile	Call Direction <input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-In <input type="checkbox"/> Always on Idle Timeout <input type="text" value="300"/> second(s) <input type="checkbox"/> Enable PING to keep alive PING to the IP <input type="text"/>
---	---

Common Settings

Profile Name: Specify a name for the remote network.

Enable this profile: Check here to activate this profile.

Call Direction: Specify the call direction for this profile. **Both** means it can be used for outgoing and incoming access. **Dial-Out** means it can only be used for outgoing access. **Dial-In** allows only incoming access.

Idle Timeout: By default, set to 300 seconds. If the profiles connection is idle for over the limit set by the timer, the router will drop the connection.

2. Dial-Out Settings

<p>Type of Server I am calling</p> <input checked="" type="radio"/> ISDN <input type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/>	Link Type <input type="text" value="64k bps"/> Username <input type="text" value="???"/> Password <input type="text"/> PPP Authentication <input type="text" value="PAP/CHAP"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) <input type="text"/>	<p>IKE Pre-Shared Key</p> <input type="text"/>
	<p>IPsec Security Method</p> <input checked="" type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) <input type="text" value="DES with Authentication"/>
	<p>Scheduler (1-15)</p> <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
	<p>Callback Function (CBCP)</p> <input type="checkbox"/> Require Remote to Callback <input type="checkbox"/> Provide ISDN Number to Remote

Dial Out Settings

Username: Specify a username for authentication by the remote router.

Password: Specify a password for authentication by the remote router.

Dial Number for ISDN or Server IP/Host Name for VPN: Specify the ISDN dial number or the destination VPN server IP address or Host Name for dialup.

Type of Server I am calling: Indicates the dial-out VPN type.

ISDN: Specify the dial-out LAN-to-LAN connection is ISDN.

PPTP: Specify the dial-out VPN connection is PPTP.

IPSec Tunnel: Specify the dial-out VPN connection is IPSec Tunnel.

L2TP: Specify the dial-out VPN connection is L2TP.

L2TP with IPSec Policy: Specify IPSec policy for L2TP.

None: Does not apply IPSec.

Nice to Have: Apply IPSec first. If fails, tries without IPSec again.

Must: Specify L2TP over IPSec.

If IPSec Tunnel or L2TP with IPSec Policy set to **Nice to Have** or **Must**, please fill a Pre-shared Key and select security methods as described in followings.

Medium(AH): Specify the IPSec protocol is the Authentication Header protocol. The data will be authentic, but will not be encrypted.

High(ESP): Specify the IPSec protocol is the Encapsulating Security Payload protocol. The data will be encrypted.

DES without Authentication: Use DES encryption algorithm and not apply any authentication.

DES with Authentication: Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

3DES without Authentication: Use triple DES encryption algorithm and not apply any authentication.

3DES with Authentication: Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

Link Type: Indicates the ISDN dial-out link type.

Disable: Deactivates the dial-out action.

64k bps: Specifies the outgoing connection speed is restricted to 64kbps (one B-channel).

128k bps: Specifies the outgoing connection speed is 128kbps (two B-channels).

BOD: Specifies the link type to be dynamic bandwidth control (Bandwidth-on-Demand).

PPP Authentication: Specify the PPP authentication method for ISDN, PPTP, L2TP or L2TP over IPSec. Normally set to **PAP/CHAP** for the widest compatibility.

VJ Compression: VJ Compression means TCP/IP protocol header compression. Normally set to Yes to improve bandwidth utilization.

Scheduler (1-15): Specify the index of the call schedule.

Callback Function (CBCP)

The callback function is implemented by the CBCP protocol which is part of the PPP protocol suite. It only works for ISDN LAN-to-LAN connection.

Require Remote to Callback: Inactive by default. When active, the router exchanges connection information with the remote router and requires the remote router to call back to make a connection.

Provide ISDN Number to Remote: In some cases, the remote router requires the ISDN number for calling back. Check here to allow the local router to send the ISDN number to the remote router.

3. Dial-In Settings

<p>Allowed Dial-In Type</p> <p><input type="checkbox"/> ISDN</p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> IPsec Tunnel</p> <p><input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/></p> <p><input type="checkbox"/> Specify ISDN CLID or Remote VPN Gateway</p> <p>Peer ISDN Number or Peer VPN Server IP <input type="text"/></p>	<p>Username <input data-bbox="1214 748 1458 786" type="text" value="???"/></p> <p>Password <input data-bbox="1214 792 1458 831" type="password"/></p> <p>PPP Authentication <input type="text" value="PAP/CHAP"/></p> <p>VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off</p> <hr/> <p>IKE Pre-Shared Key <input data-bbox="1214 943 1458 981" type="text"/></p> <p>IPsec Security Method</p> <p><input type="checkbox"/> Medium (AH)</p> <p><input checked="" type="checkbox"/> High (ESP) <input type="text" value="DES"/></p>
--	---

Dial-In Settings

Username: Specify a username for authentication by the remote router.

Password: Specify a password for authentication by the remote router.

Enable CLID Authentication: Check to enable the CLID authentication function. For ISDN, if checked, you should put ISDN number into the following input block **Peer ISDN Number**. For IPsec Tunnel or L2TP with IPsec Policy set to **Nice to Have** or **Must**, if checked, you should put the IP address of the dial-in router into the following input block **Peer VPN Server IP**.

Allowed Dial-In Type: Indicate the allowed dial-in connection type.

ISDN: Check to allow ISDN dial-in connection.

PPTP: Check to allow PPTP dial-in connection.

IPsec Tunnel: Check to allow IPsec tunnel dial-in connection.

L2TP: Check to allow L2TP dial-in connection.

L2TP with IPsec Policy: Specify IPsec policy for L2TP.

None: Do not apply IPsec.

Nice to Have: Apply IPsec first. If fails, tries without IPsec again.

Must: Specify L2TP over IPsec.

Link Type: Indicates the ISDN dial-out link type.

Disable: Deactivates the dial-out action.

64k bps: Specifies the outgoing connection speed is restricted to 64kbps (one B-channel).

128k bps: Specifies the outgoing connection speed is 128kbps (two B-channels).

BOD: Specifies the link type to be dynamic bandwidth control (Bandwidth-on-Demand).

PPP Authentication: Specify the PPP authentication method for PPTP, L2TP or L2TP over IPsec. Normally set to PAP/CHAP for the widest compatibility.

VJ Compression: VJ Compression means TCP/IP protocol header compression. Normally set to Yes to improve bandwidth utilization.

Callback Function (CBCP)

Enable Callback Function: Check to allow this router to accept requests from a remote router for call back.

Use Following Number to Callback & Callback Number: Check here and enter a callback number for the router to call.

Callback Budget: Specifies a time budget for the callback function. By default the value is zero, which means there is no time limitation on call backs.

4. TCP/IP Network Settings	
My WAN IP	<input type="text" value="0.0.0.0"/>
Remote Gateway IP	<input type="text" value="0.0.0.0"/>
Remote Network IP	<input type="text" value="0.0.0.0"/>
Remote Network Mask	<input type="text" value="255.255.255.0"/>
	<input type="button" value="More"/>
RIP Direction	<input type="text" value="TX/RX Both"/>
RIP Version	<input type="text" value="Ver. 2"/>
For NAT operation, treat remote sub-net as	
	<input type="text" value="Private IP"/>
<input type="checkbox"/> Change default route to this VPN tunnel	

TCP/IP Network Settings

The following settings are required for proper LAN-to-LAN operation.

My WAN IP: In most cases you may accept the default value 0.0.0.0 in this field. The router will then get a WAN IP address from the remote router during the IPCP negotiation phase. If the WAN IP address is fixed by remote, specify the fixed IP address here.

Remote Gateway IP: In most cases you may accept the default value 0.0.0.0 in this field. The router will then get a Remote Gateway IP address from the remote router during the IPCP negotiation phase. If the Remote Gateway IP address is fixed by remote, specify the fixed IP address here.

Note: If you are not familiar with IPCP protocol, please set these two fields to 0.0.0.0.

Remote Network IP: Specify the network identification of the remote network. For example, 192.168.1.0 is a network identification of a class-C subnet with netmask 255.255.255.0 (/24).

Remote Network Mask: Specify the netmask of the remote network.

More: Let you add a static route when this connection is up.

RIP Direction: The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here.

RIP Version: Select the RIP protocol version. Specify Ver. 2 for greatest compatibility.

For NAT operation, treat remote sub-net as: The router has two local IP networks: the 1st subnet and 2nd subnet. Here you set which subnet will be used as local network for VPN connection and exchange RIP packets with the remote network. Usually set to **Private IP** for routing between the 1st subnet and the remote network

6. An example of LAN-to-LAN VPN connection

This example is based on the network configuration as the following table to describe how to set up a LAN-to-LAN profile to connect two private networks through Internet. As shown in the table, the private network 192.168.1.0/24 is located at head office, the network of off-site branch office is 192.168.2.0/24.

	Head Office	Branch Office
Network ID	192.168.1.0/24	192.168.2.0/24
Router IP address/netmask	192.168.1.1/24	192.168.2.1/24
Access Account	UN: head PW: head	UN: branch PW: branch
VPN Server IP Address	87.65.43.21	123.45.67.89
Type of VPN connection	L2TP over IPSec	L2TP over IPSec
IKE Pre-shared Key	ABC123	ABC123
IPSec Security Method	AH	AH

Before configuring the LAN-to-LAN profile for each site, you should click **VPN and Remote Access Setup > VPN IKE / IPSec Setup** to configure the pre-shared key **ABC123** in advance.

Creating a LAN-to-LAN profile at Head Office

> Advanced Setup > LAN-to-LAN Profile Setup		<< Main Menu
Profile Index : 1		<< Back Clear
1. Common Settings		
Profile Name <input type="text" value="head"/> <input checked="" type="checkbox"/> Enable this profile	Call Direction <input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-In <input type="checkbox"/> Always on Idle Timeout <input type="text" value="300"/> second(s) <input type="checkbox"/> Enable PING to keep alive PING to the IP <input type="text"/>	
2. Dial-Out Settings		
Type of Server I am calling <input type="radio"/> ISDN <input type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input checked="" type="radio"/> L2TP with IPsec Policy <input type="text" value="Must"/>	Link Type <input type="text" value="64k bps"/> Username <input type="text" value="branch"/> Password <input type="text" value="****"/> PPP Authentication <input type="text" value="PAP/CHAP"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off <hr/> IKE Pre-Shared Key <input type="text"/>	
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) <input type="text" value="123.45.67.89"/>	IPsec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) <input type="text" value="DES with Authentication"/>	
Scheduler (1-15) <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>		
Callback Function (CBCP) <input type="checkbox"/> Require Remote to Callback <input type="checkbox"/> Provide ISDN Number to Remote		
3. Dial-In Settings		
Allowed Dial-In Type <input type="checkbox"/> ISDN <input type="checkbox"/> PPTP <input type="checkbox"/> IPsec Tunnel <input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="Must"/>	Username <input type="text" value="head"/> Password <input type="text" value="****"/> PPP Authentication <input type="text" value="PAP/CHAP"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off <hr/> IKE Pre-Shared Key <input type="text"/>	
<input checked="" type="checkbox"/> Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP <input type="text" value="87.65.43.21"/>	IPsec Security Method <input type="checkbox"/> Medium (AH) <input type="checkbox"/> High (ESP) <input type="text" value="DES"/>	
4. TCP/IP Network Settings		
My WAN IP <input type="text" value="0.0.0.0"/> Remote Gateway IP <input type="text" value="0.0.0.0"/> Remote Network IP <input type="text" value="192.168.2.0"/> Remote Network Mask <input type="text" value="255.255.255.0"/> <input type="button" value="More"/>	RIP Direction <input type="text" value="TX/RX Both"/> RIP Version <input type="text" value="Ver. 2"/> For NAT operation, treat remote sub-net as <input type="text" value="Private IP"/> <hr/> <input type="checkbox"/> Change default route to this VPN tunnel	
<input type="button" value="OK"/>		

Creating a LAN-to-LAN profile at Branch Office

> **Advanced Setup > LAN-to-LAN Profile Setup** << [Main Menu](#)

Profile Index : 1 << [Back](#) | [Clear](#)

1. Common Settings

Profile Name <input type="text" value="branch"/> <input checked="" type="checkbox"/> Enable this profile	Call Direction <input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-In <input type="checkbox"/> Always on Idle Timeout <input type="text" value="300"/> second(s) <input type="checkbox"/> Enable PING to keep alive PING to the IP <input type="text"/>
---	---

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> ISDN <input type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input checked="" type="radio"/> L2TP with IPsec Policy <input type="text" value="Must"/>	Link Type <input type="text" value="64k bps"/> Username <input type="text" value="head"/> Password <input type="text" value="****"/> PPP Authentication <input type="text" value="PAP/CHAP"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off <hr/> IKE Pre-Shared Key <input type="text"/> IPsec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) <input type="text" value="DES with Authentication"/> <hr/> Scheduler (1-15) <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/> <hr/> Callback Function (CBCP) <input type="checkbox"/> Require Remote to Callback <input type="checkbox"/> Provide ISDN Number to Remote
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) <input type="text" value="87.65.43.21"/>	

3. Dial-In Settings

Allowed Dial-In Type <input type="checkbox"/> ISDN <input type="checkbox"/> PPTP <input type="checkbox"/> IPsec Tunnel <input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="Must"/>	Username <input type="text" value="branch"/> Password <input type="text" value="****"/> PPP Authentication <input type="text" value="PAP/CHAP"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off <hr/> IKE Pre-Shared Key <input type="text"/> IPsec Security Method <input type="checkbox"/> Medium (AH) <input type="checkbox"/> High (ESP) <input type="text" value="DES"/>
<input checked="" type="checkbox"/> Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP <input type="text" value="123.45.67.89"/>	

4. TCP/IP Network Settings

My WAN IP <input type="text" value="0.0.0.0"/> Remote Gateway IP <input type="text" value="0.0.0.0"/> Remote Network IP <input type="text" value="192.168.1.0"/> Remote Network Mask <input type="text" value="255.255.255.0"/> <input type="button" value="More"/>	RIP Direction <input type="text" value="TX/RX Both"/> RIP Version <input type="text" value="Ver. 2"/> For NAT operation, treat remote sub-net as <input type="text" value="Private IP"/> <hr/> <input type="checkbox"/> Change default route to this VPN tunnel
---	---

Validation and Troubleshooting

Initial a VPN connection

Once the VPN configurations are completed, any traffic from local LAN to remote LAN will trigger the VPN connection. Or you can use VPN Connection Management in System Management to direct "Dial" or connect a VPN from dial-out router. Once the link is up the VPN connection status/information will also show in VPN Connection Management page. A "Drop" button will let you to disconnect the link.

System Management

- >> [Online Status](#)
- >> [VPN Connection Management](#)
- >> [Configuration Backup / Restoration](#)
- >> [SysLog Setup](#)
- >> [Time Setup](#)
- >> [Management Setup](#)
- >> [Diagnostic Tools](#)
- >> [Reboot System](#)
- >> [Firmware Upgrade \(TFTP Server\)](#)

> System Management > VPN Connection Management
<< [Main Menu](#)

Dial-out Tool Refresh Seconds :

VPN Connection Status

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime	
1 (Vigor 1)	IPSec Tunnel DES-MD5	172.16.2.199	192.168.8.0/24	2180	66	2258	70	0 : 24 : 25	<input type="button" value="Drop"/>
2 (to Cisco)	IPSec Tunnel DES-MD5	172.16.4.2	172.17.1.0/24	17984	1165	34035	70914	0 : 5 : 59	<input type="button" value="Drop"/>
3 (for win2k)	L2TP 3DES-MD5	172.19.4.10	192.168.2.0/24	2028	66	2062	70	0 : 35 : 46	<input type="button" value="Drop"/>
4 (VPN18)	L2TP 3DES-MD5	172.16.2.141	172.18.4.0/24	1871	66	1871	68	0 : 35 : 29	<input type="button" value="Drop"/>
5 (to win2k 2)	PPTP	172.16.2.142	172.18.5.0/24	2000	63	2006	63	0 : 34 : 45	<input type="button" value="Drop"/>

xxxxxxxx : Data is encrypted.
 xxxxxxxx : Data isn't encrypted.