
Virtual Private Network and Remote Access Setup

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 network 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 “Remote Dial-In Access” facility 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.

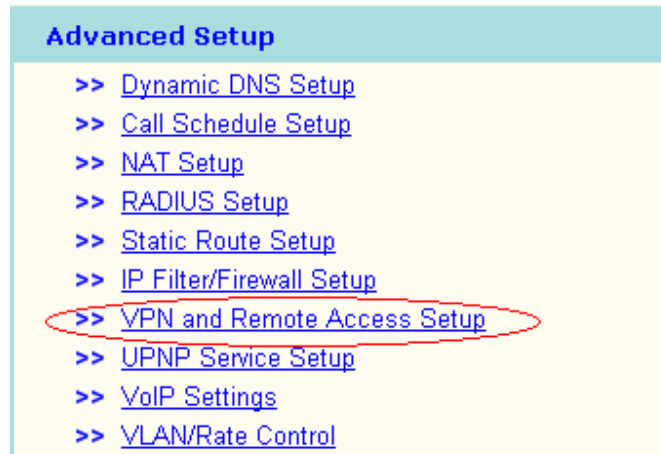
The “LAN-to-LAN Access” facility provides a solution to connect two independent LANs for mutual sharing of network resources. For example, the head office network can access the branch office network, and vice versa.

The VPN technology employed in the Vigor 2600V series of ADSL VoIP routers supports Internet-industry standard to provide customers with interoperable VPN solutions, such as Internet Protocol Security (IPSec), Layer 2 Tunneling Protocol (L2TP), and Point-to-Point Tunneling Protocol (PPTP).

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

VPN and Remote Access Setup

Advanced Setup > VPN and Remote Access Setup



The VPN and Remote Access Setup has five main functions, as shown below. You may set up Remote Access Control, PPP, VPN IKE/IPSec, Remote Dial-in, and LAN-to-LAN Profile on demand.



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.

Use the PPP General Setup to configure your router's PPP authentication method as well as IP assignment range for remote dial-in user. This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP and L2TP over IPSec.

VPN and Remote Access Setup

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 address.

Use Remote User Profile Setup (Teleworker) to create dial-in user accounts. Vigor router supports three types of dial-in methods, PPTP, L2TP, and L2TP over IPSec. The PPTP VPN connection is compatible with all Windows platforms which have built-in PPTP protocol. 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. The Vigor router supports four types of LAN-to-LAN VPN, IPSec Tunnel, PPTP, L2TP, and L2TP over IPSec. You can establish simultaneously up to 16 VPN tunnels including remote dial-in users.

Remote Access Control Setup

As depicted in the following picture, click the appropriate check box to enable the VPN service type that you want to provide. If you intend to run a VPN server inside your LAN, you should disable the appropriate protocol to allow pass-through, as well as the appropriate NAT settings. For example, DMZ or open port.

The screenshot shows a web-based configuration interface for a Vigor router. At the top, a teal header bar contains the text "> Advanced Setup> Remote Access Control Setup" in red and a blue link "<<Main Menu". Below this, the main content area has a yellow background. It features a title "Remote Access Control Setup" in blue, followed by a list of four services with checkboxes: "Enable PPTP VPN Service" (checked), "Enable IPSec VPN Service" (checked), "Enable L2TP VPN Service" (checked), and "Enable ISDN Dial-In" (unchecked). A blue link "<< Back" is positioned to the right of the list. Below the list, a note in orange text states: "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." At the bottom, there are three buttons: "Cancel", "Clear", and "OK".

> Advanced Setup> Remote Access Control Setup <<Main Menu

Remote Access Control Setup << Back

- ☒ Enable PPTP VPN Service
- ☒ Enable IPSec VPN Service
- ☒ Enable L2TP VPN Service
- ☐ 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.

Cancel Clear OK

PPP General Setup

PPP/MP Protocol

Dial-In PPP Authentication:

PAP Only: Select this option to 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.

The screenshot shows a web-based configuration interface for a router. At the top, there is a navigation bar with "> Advanced Setup> PPP General Setup" on the left and "<<Main Menu" on the right. Below this is a title bar for the "PPP General Setup" window, with "<< Back" on the right. The main content area is divided into two columns. The left column is titled "PPP/MP Protocol" and contains the following settings: "Dial-In PPP Authentication" set to a dropdown menu showing "PAP or CHAP", "Dial-In PPP Encryption(MPPE)" set to a dropdown menu showing "Optional MPPE", "Mutual Authentication (PAP)" with radio buttons for "Yes" and "No" (where "No" is selected), and input fields for "Username" and "Password". The right column is titled "IP Address Assignment for Dial-In Users" and contains a "Start IP Address" field with the value "192.168.1.200". At the bottom center of the window is an "OK" button.

Dial-In PPP Encryption (MPPE):

Optional MPPE: This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data.

Require MPPE (40/128bits): Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 40-bit MPPE

VPN and Remote Access Setup

encryption method is not available, then 128-bit encryption scheme will be applied to encrypt the data.

Maximum MPPE: This option indicates that the router will use the MPPE encryption scheme with maximum bits (128 bits) to encrypt the data.

Mutual Authentication (PAP): The **Mutual Authentication** function is mainly used to communicate with other routers or clients which need bidirectional authentication in order to provide stronger security. For example, Cisco routers. That is, enable it only if the connecting router requires mutual authentication. By default, the option is set to *No*. Notice that if you enable the **Mutual Authentication** function, you should further specify the *Username* and **Password for communication purpose**.

Username: Specify the username for the purpose of the Mutual Authentication.

Password: Specify the password for the purpose of the Mutual Authentication.

IP Address Assignment for Dial-In Users

Start IP Address: Enter a start IP address for 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.

VPN IPSec / IKE General Setup

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

VPN and Remote Access Setup

The screenshot shows a web-based configuration interface for VPN IKE/IPSec General Setup. At the top, there is a breadcrumb trail: > Advanced Setup > VPN IKE / IPSec General Setup, and a link << Main Menu. The main title is VPN IKE/IPSec General Setup, with a << Back link. Below the title, a description reads: Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN). The configuration is divided into two sections: IKE Authentication Method and IPSec Security Method. Under IKE Authentication Method, there are two text input fields: Pre-Shared Key (containing a series of dots) and Re-type Pre-Shared Key. Under IPSec Security Method, there are three options: Medium (AH) with a checked checkbox and a description 'Data will be authentic, but will not be encrypted.'; High (ESP) with a checked checkbox and a description 'Data will be encrypted and authentic.'; and two sub-options for High (ESP): DES with a checked checkbox, 3DES with a checked checkbox, and AES with a checked checkbox. At the bottom, there are two buttons: Cancel and OK.

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 the pre-shared-key.

IPSec Security Method: Select allowed IPSec security methods.

Medium (AH): Data will be authenticated, but not be encrypted. By default, this option is active.

High (ESP): Data will be encrypted and authenticated. Herein, we support DES, 3DES, and AES encryption methods. By default, these methods are available to support.

Creating an Access Account for a Remote Dial-in User

After completing the general setup, you must create an access account for each remote 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. The following figure shows the Remote User Profile Setup for up to 20 access accounts.

VPN and Remote Access Setup

Remote Access User Accounts: << [Back](#) | [Set to Factory Default](#)

Index	User	Status	Index	User	Status
1.	calvin	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): Click here to clear all dial-in user accounts.

User: Display the username for the specific dial-in user. of the LAN-to-LAN profile.

The symbol ??? represents that the profile is empty.

Status: Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.

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

> **Advanced Setup** > **Remote User Profile Setup (Teleworker)** << [Main Menu](#)

Index No. 1 << [Back](#) | [Clear](#) |

<p>User account and Authentication</p> <p><input checked="" type="checkbox"/> Enable this account</p> <p>Idle Timeout <input type="text" value="300"/> second(s)</p> <p>Allowed Dial-In Type</p> <p><input checked="" 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 Remote Node</p> <p>Remote Client IP or Peer ISDN Number <input type="text"/></p> <p>or Peer ID <input type="text"/></p>	<p>Username <input type="text" value="calvin"/></p> <p>Password <input type="password" value="•••••"/></p> <p>IKE Pre-Shared Key <input type="text"/></p> <p>IPsec Security Method</p> <p><input checked="" type="checkbox"/> Medium (AH)</p> <p>High (ESP)</p> <p><input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>Local ID <input type="text"/> (optional)</p> <p>Callback Function</p> <p><input type="checkbox"/> Check to enable Callback function</p> <p><input type="checkbox"/> Specify the callback number</p> <p>Callback Number <input type="text"/></p> <p><input checked="" type="checkbox"/> Check to enable Callback Budget Control</p> <p>Callback Budget <input type="text" value="30"/> minute(s)</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

User Account and Authentication

Enable this account: Check this item to activate the individual dial-in user account.

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

Allowed Dial-In Type : Select the allowed dial-in type. Herein, the Vigor 2600V series of ADSL VoIP routers provides three types: **PPTP**, **IPSec Tunnel**, and **L2TP with IPSec Policy**. For the **L2TP with IPSec Policy**, you have other three choices (None, Nice to Have, and Must) to set up the dial-in VPN type.

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

IPSec Tunnel: Allow the remote dial-in user to trigger a IPSec VPN connection through Internet.

L2TP: Allow the remote dial-in user to make a L2TP VPN connection through the Internet. Specify the IPSec policy to be “None”, “Nice to Have”, or “Must”.

None: Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec Policy can be viewed as one pure L2TP connection.

Nice to Have: Apply the IPSec policy first, if it is available. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.

Must: Specify the IPSec policy to be definitely applied on the L2TP connection.

Notice that when you choose either the PPTP or the L2TP with IPSec Policy for the dial-in VPN type, you should specify the Username and Password. Other functions including **IKE Pre-Shared Key**, IPSec Security Method, Remote Client IP or Peer ID and optional Local ID are reserved for the option of the IPSec Tunnel and will be disabled for the PPTP or the L2TP with IPSec Policy option. One exception for the L2TP with IPSec Policy option is that policy sets to Nice to Have or **Must**. In this exception, you should

VPN and Remote Access Setup

move on the setting of **IKE Pre-Shared Key**, IPSec Security Method, Remote Client IP or Peer ID, and optional Local ID.

Hence, if you enable the **PPTP** or **L2TP without IPSec Policy** option for the remote dial-in VPN type, you should move on the following setting

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

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

Once you enable the **IPSec Tunnel** or **L2TP with IPSec Policy** with selection of **Nice to Have** or **Must** for the remote dial-in setting, you should move on the following setting.

Specify Remote Node: For extra security, you should enable the option to allow the remote client to connect only from a specific IP address.

Remote Client IP or Peer ID: Specify the IP address of the remote client or the peer ID in the field. Afterward, you should fill a Pre-Shared Key for this specific node.

IKE Pre-shared Key: Click it and a window will be automatically popped up for you, as depicted below. Please fill a Pre-shared Key and confirm it for this specific node.



The screenshot shows a web browser window titled "Router Web Configurator - Microsoft Internet Explorer". Inside the browser, there is a dialog box titled "IKE Authentication Method". The dialog box contains two text input fields: "Pre-Shared Key" and "Re-type Pre-Shared Key". Below these fields is a "Confirm" button.

IPSec Security Method: Specify the IPSec security method, either authentication or encryption algorithm, to determine the security level. You can only select one.

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

High (ESP): Specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted. Supported algorithms are DES, 3DES, and AES. By default, these three algorithms are available.

VPN and Remote Access Setup

Local ID: Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional.

Notice that if you do not activate the “Specify Remote Node” and leave the field of “Remote Client IP or Peer ID” to be empty, the settings of *IKE Pre-Shared Key*, IPSec Security Method, Remote Client IP or Peer ID, and optional Local ID will be disabled and, therefore, no IPSec-related VPN connection can be triggered successfully.

Creating a LAN-to-LAN Profile

In this section, we will explain how to set up the LAN-to-LAN Profile in more detail. The path to configure it in the Web configurator is Advanced Setup > VPN and Remote Access Setup > LAN-to-LAN Profile Setup. The web page is shown below. Herein, you can create up to 16 LAN-to-LAN profiles.

> Advanced Setup > LAN-to-LAN Profile Setup << Main Menu

LAN-to-LAN Profiles: << Back | Set to Factory Default

Index	Name	Status	Index	Name	Status
1.	Office	v	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 to open a detailed setting page for each profile.

Name: Indicate the name of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.

Status: Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.

Each LAN-to-LAN profile includes 4 subgroups: Common Settings, Dial-Out Settings, Dial-In Settings, and TCP/IP Network Settings. In the following, we

explain each subgroup in detail.

Common Settings

> Advanced Setup > LAN-to-LAN Profile Setup		<< Main Menu	
Profile Index : 1		<< Back Clear	
1. Common Settings			
<div>Profile Name <input type="text" value="office"/></div> <div><input checked="" type="checkbox"/> Enable this profile</div>		<div>Call Direction <input type="radio"/> Both <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-In</div> <div><input type="checkbox"/> Always on</div> <div>Idle Timeout <input type="text" value="0"/> second(s)</div> <div><input type="checkbox"/> Enable PING to keep alive</div> <div>PING to the IP <input type="text"/></div>	

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.

Always on: Click it to always activate this profile. The field of **Idle Timeout** will be grayed to disallow any input.

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

Enable PING to keep alive: Click this item to enable the transmission of PING packets to an IP address defined in the field of “**PING to the IP**”.

PING to the IP: Specify the IP address of the remote host that located at the other-end of the VPN tunnel.

Notice that this function is useful to determine the state of a specific VPN connection. Normally, when the remote host wants to disconnect the VPN connection, this host should send some necessary packets to inform the Vigor router. Accordingly, the Vigor router will drop the designated VPN connection and clear its associated parameters, for example, key for encryption. However, once the remote host abnormally disconnects a VPN connection, say VPN k, the Vigor router has no ideal about VPN k at this moment

due to its abnormal behaviour. Hence, the Vigor router will regard this VPN k to be alive, which results in no more packets to send within the VPN k and no more chance to trigger the VPN k again. To resolve this dilemma, this function (***Enable PING to keep alive***) is designed to determine of the status of the VPN k. By continuously sending PING packets to the remote host, the Vigor router can know the existence of this VPN k. If there is no response for PING packets, the Vigor router will consider the state of the VPN k as disconnection. In this way, the Vigor router will clear all related parameters of the VPN k so that the VPN k can be triggered again.

Dial Out Settings

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> ISDN <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy None	Link Type 64k bps Username ??? Password PPP Authentication PAP/CHAP VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Pre-Shared Key IPsec Security Method <input type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) DES without Authentication Advance Scheduler (1-15) , , , Callback Function (CBCP) <input type="checkbox"/> Require Remote to Callback <input type="checkbox"/> Provide ISDN Number to Remote
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) 203.67.188.62	

Type of Server I am calling: Indicate the dial-out VPN type. Herein, three options are available and only one option can be activated. These options are **PPTP**, **IPsec Tunnel**, and **L2TP with IPsec Policy**. For the **L2TP with IPsec Policy**, you have other three choices (None, Nice to Have, and Must) to set up the dial-out VPN type.

PPTP: Specify the dial-out VPN connection to be the PPTP connection.

IPsec Tunnel: Specify the dial-out VPN connection to be the IPsec Tunnel

connection.

L2TP with IPsec Policy: Specify the IPsec policy for the L2TP connection.

None: Do not apply IPsec. Accordingly, the VPN connection employed the L2TP without IPsec Policy can be viewed as one pure L2TP connection.

Nice to Have: Apply the IPsec policy first, if it is available. Otherwise, the dial-out VPN connection becomes one pure L2TP connection.

Must: Specify the IPsec policy to be definitely applied on the L2TP connection.

Notice that when you choose either the PPTP or the L2TP with IPsec Policy for the dial-out VPN type, you should specify the Username, Password, **PPP Authentication**, and **VJ Compression**. Other functions including **IKE Pre-Shared Key**, IPsec Security Method, Server IP/Host Name for VPN, Scheduler, and Advance Setting are reserved for the option of the IPsec Tunnel and will be disabled for the PPTP or the L2TP with IPsec Policy option. One exception for the L2TP with IPsec Policy option is that policy sets to Nice to Have or *Must*. In this exception, you should move on the setting of **IKE Pre-Shared Key**, IPsec Security Method, and **Server IP/Host Name for VPN**.

Hence, if you enable the **PPTP** or **L2TP without IPsec Policy** option for the dialout VPN type, you should move on the following setting.

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

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

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

VJ Compression: VJ Compression is used for TCP/IP protocol header compression. Normally set to **Yes** to improve bandwidth utilization.

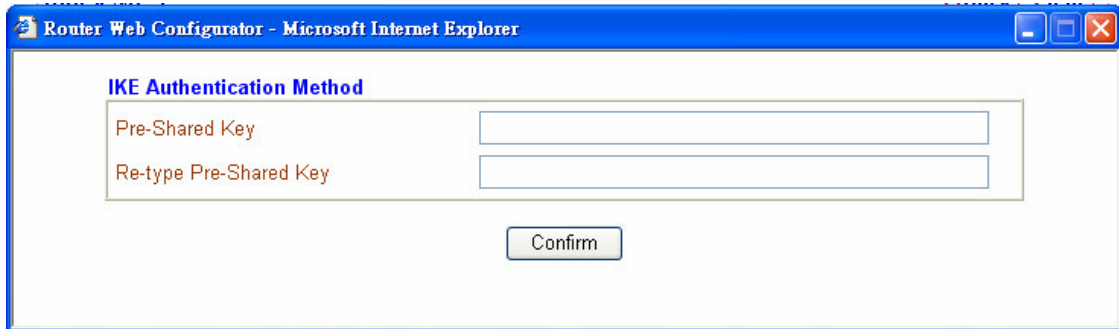
Once you enable the **IPsec Tunnel** or the **L2TP with IPsec Policy (applying Nice to Have or Must option)** for the dial-out VPN type, you should move on the following setting.

Server IP/Host Name for VPN: Specify the IP address of the destination VPN server or the Host Name for dialup.

IKE Pre-shared Key: Click it and a window will be automatically popped up for you,

VPN and Remote Access Setup

as depicted below. Please fill a Pre-shared Key and confirm it for this specific node.



The screenshot shows a web browser window titled "Router Web Configurator - Microsoft Internet Explorer". The main content area is titled "IKE Authentication Method". It contains two text input fields: "Pre-Shared Key" and "Re-type Pre-Shared Key". A "Confirm" button is located below the input fields.

IPSec Security Method: Specify the IPSec security method, either authentication or encryption algorithm, to determine the security level. You can only select one.

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

High (ESP): Specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted. Supported algorithms are listed below.

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

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 scheme.

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

Advanced Setting: Click it and a window will be automatically popped up for advanced setting, as shown below. In this window, you need to decide which mode (Main mode or Aggressive Mode) to be used for Phase 1 IKE negotiation process, specify the authentication and encryption algorithms, fill the lifetime for the IKE phase 1 and phase 2, enable or disable the “Perfect Forward Secret”,

and provide the Local ID for remote VPN gateway.

IKE advance settings

IKE phase 1 mode: ☒ Main mode ☐ Aggressive mode

IKE phase 1 proposal: DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_MD5_G2

IKE phase 1 key lifetime: 28800 (900 ~ 86400)

IKE phase 2 key lifetime: 3600 (600 ~ 86400)

Perfect Forward Secret: ☒ Disable ☐ Enable

Local ID:

Cancel OK

IKE phase 1 mode: *Main mode* and *Aggressive mode* are provided in the Vigor 2600V series of ADSL VoIP routers. Basically, both modes are two kinds of Phase 1 IKE negotiation process. Most VPN servers support Main mode and so does the Vigor 2600V series of routers. Aggressive mode is a more recent implementation to speed up the negotiation process, but may incur less security. The Vigor 2600V series of routers also support this Aggressive mode. By default, Main mode is active for consideration of greatest compatibility.

IKE phase 1 proposal: As stated above, you should specify authentication scheme, encryption algorithm, or their combinations. Then the router will deliver the specified algorithm to the remote VPN server and ask whether it supports such an algorithm. Two options are available for selection in Aggressive mode and nine choices are provided for Main mode. For Main mode, you have better to choose the latest term, i.e. “DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_MD5_G2”. This is because that more selections are available, more likelihood of consistent algorithm is.

IKE phase 1 key lifetime: In order to increase the security level, the router should limit the key lifetime. By default, the key lifetime is set to the standard value, i.e. 28800 seconds. You are able to specify a value in between 900 and 86400

seconds on demand.

IKE phase 2 key lifetime: By default, the phase 2 key lifetime is set to the standard value, i.e. 3600 seconds. You also are able to specify a value in between 600 and 86400 seconds according to your demand.

Perfect Forward Secret: If you enable this term, then the Phase 1 key will be reused to reduce the computation complexity in phase 2. Otherwise, a new key will be generated for phase 2 key. By default, this option is inactive.

Local ID: This term is mainly used in Aggressive mode and is on behalf of the IP address to perform identity authentication with remote VPN server. It is not necessary for Main mode.

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

Dial-In Settings

3. Dial-In Settings

Allowed Dial-In Type <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input checked="" type="checkbox"/> L2TP with IPsec Policy None ▼ <input type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text"/> or Peer ID <input type="text"/>	Username <input type="text" value="???"/> Password <input type="text"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Pre-Shared Key <input type="text"/> IPsec Security Method <input checked="" type="checkbox"/> Medium (AH) High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Allowed Dial-In Type: Indicate the allowed dial-in connection type. In the Vigor 2600V series of ADSL VoIP routers, we provide three options: **PPTP**, **IPsec Tunnel**, and **L2TP with IPsec Policy**. By default, these three options are active.

PPTP: Check to allow the PPTP dial-in connection.

IPsec Tunnel: Click it to allow the IPsec tunnel dial-in connection.

L2TP with IPsec Policy: Specify the IPsec policy for the L2TP connection.

None: Do not apply the IPsec policy.

VPN and Remote Access Setup

Nice to Have: Apply the IPSec policy first. If it fails, the dial-in VPN connection will be the L2TP connection without employing the IPSec policy.

Must: Specify the IPSec policy to be definitely applied on the L2TP connection.

Notice that, similar to the setting for dial-out users, when you choose either the PPTP or the L2TP with IPSec Policy for dial-in setting, you should specify the Username, Password, PPP Authentication, and VJ Compression. Other functions including IKE Pre-Shared Key, IPSec Security Method, and Peer VPN Server IP or Peer ID are reserved for the option of IPSec Tunnel and will be disabled for the PPTP or L2TP with IPSec Policy option. One exception for the L2TP with IPSec Policy option is that policy sets to Nice to Have or **Must**. In this exception, you should move on the setting of IKE Pre-Shared Key, IPSec Security Method, and Peer VPN Server IP or Peer ID.

Hence, if you enable the PPTP, L2TP, or L2TP with IPSec Policy option for dial-in setting, you should move on the setting of the following fields.

Username: Specify a username to authenticate the dial-in router.

Password: Specify a password to authenticate the dial-in router.

PPP Authentication: Specify the PPP authentication method for PPTP, L2TP, and L2TP over IPSec. Normally set to PAP/CHAP for the widest compatibility. VJ Compression: VJ Compression is used for TCP/IP protocol header compression. Normally set to Yes to improve bandwidth utilization.

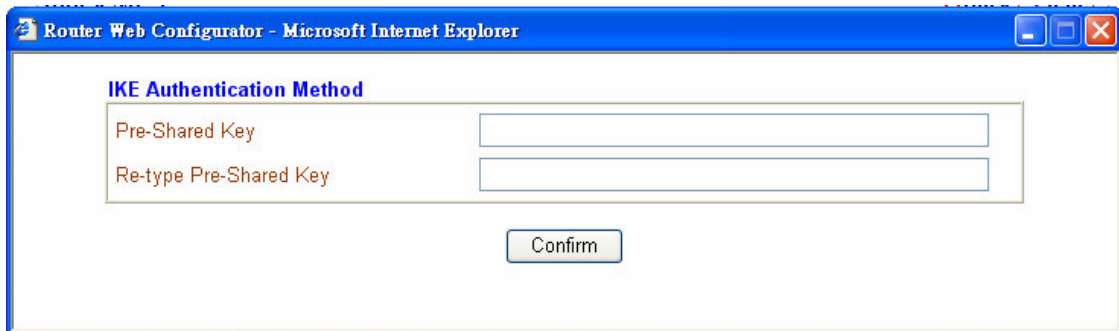
Once you enable the **IPSec Tunnel** or **L2TP with IPSec Policy** with selection of **Nice to Have** or **Must** for dial-in setting, you should move on the following setting.

Specify Remote VPN Gateway: For extra security, you should enable the option to allow the remote client to connect only from a specific IP address.

Peer VPN Server IP or Peer ID: Specify the IP address of the remote VPN server or the peer ID in the field. Afterward, you should fill a Pre-Shared Key for this specific node.

IKE Pre-shared Key: Click it and a window will be automatically popped up for you, as depicted below. Please fill a Pre-shared Key for this specific node.

VPN and Remote Access Setup



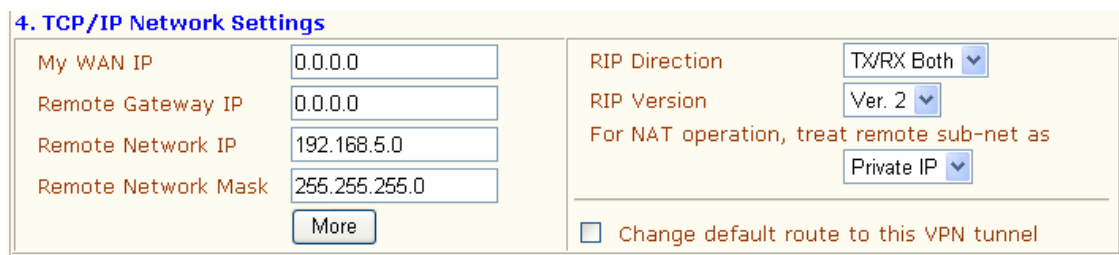
IPSec Security Method: Specify the IPSec security method, either authentication or encryption algorithm, to determine the security level. You can only select one.

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

High (ESP): Specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted. Supported algorithms are DES, 3DES, and AES. By default, these three algorithms are available.

Notice that if you do not activate the “Specify Remote VPN Gateway” and leave the field of “Peer VPN Server IP or Peer ID” to be empty, the settings of **IKE Pre-Shared Key**, and IPSec Security Method will be disabled and, therefore, no IPSec-related VPN connection can be triggered successfully.

TCP/IP Network Settings



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

MyWAN IP: In most cases, you may accept the default value of 0.0.0.0 in this field.

The router will then get a WAN IP address from the remote router during the

VPN and Remote Access Setup

IPCP negotiation phase. If the WAN IP address is fixed by remote side, specify the fixed IP address here.

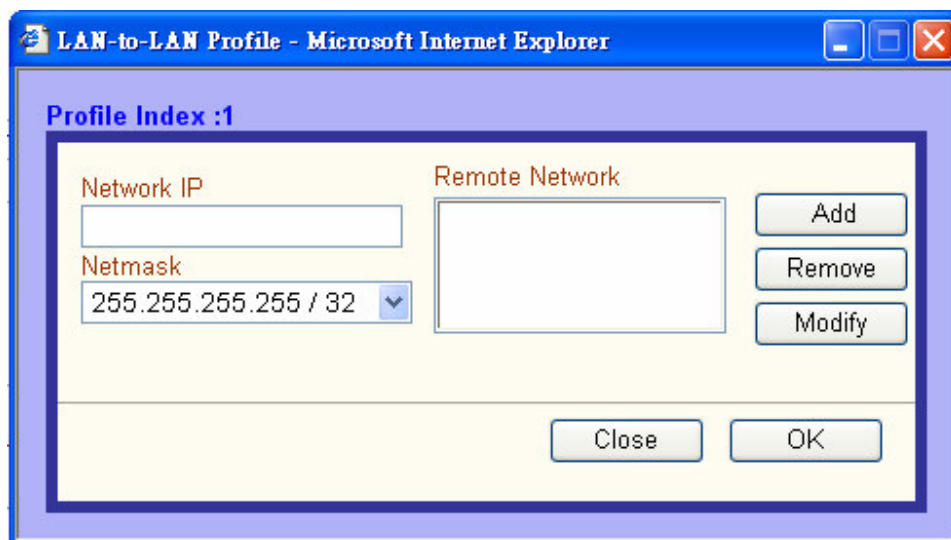
Remote Gateway IP: In most cases, you may accept the default value of 0.0.0.0 in this field. The router will then get a Remote Gateway IP address from the remote router during the IPCP negotiation phase. If the Remote Gateway IP address is fixed, specify the fixed IP address here.

Notice that if you are not familiar with IPCP protocol, please set these two fields as 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 subnet mask of 255.255.255.0 (/24).

Remote Network Mask: Specify the subnet mask of the remote network.

More: This button let you add a static route when this connection is up. Clicking it will pop up a window for more setting, as depicted below.



RIP Direction: The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.

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

VPN and Remote Access Setup

For NAT operation, treat remote sub-net as: The Vigor router supports two local IP networks: the 1st subnet and 2nd subnet. Thus, you can set which subnet will be used as the 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 there mote network.

An example of LAN-to-LAN VPN connection

This example is based on the network configuration shown in 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

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="password" value="....."/> PPP Authentication <input type="text" value="PAP/CHAP"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Pre-Shared Key <input type="password" value="....."/> IPSec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) <input type="text" value="DES without Authentication"/> <input type="button" value="Advance"/> 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
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input type="text" value="123.45.67.89"/>	

3. Dial-In Settings	
Allowed Dial-In Type <input checked="" 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"/> <input checked="" type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text" value="123.45.67.89"/> or Peer ID <input type="text"/>	Username <input type="text" value="head"/> Password <input type="password" value="....."/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Pre-Shared Key <input type="password" value="....."/> IPSec Security Method <input checked="" type="checkbox"/> Medium (AH) High (ESP) <input type="checkbox"/> DES <input type="checkbox"/> 3DES <input type="checkbox"/> AES

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"/> <input type="checkbox"/> Change default route to this VPN tunnel

Creating a LAN-to-LAN profile at Branch Office

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="???"/> Password <input type="text"/> PPP Authentication <input type="text" value="PAP/CHAP"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Pre-Shared Key <input type="text" value="....."/> IPsec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) <input type="text" value="DES without Authentication"/> <input type="button" value="Advance"/> 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 checked="" 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"/> <input checked="" type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text" value="87.65.43.21"/> or Peer ID <input type="text"/>	Username <input type="text" value="branch"/> Password <input type="text" value="...."/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Pre-Shared Key <input type="text"/> IPsec Security Method <input checked="" type="checkbox"/> Medium (AH) High (ESP) <input type="checkbox"/> DES <input type="checkbox"/> 3DES <input type="checkbox"/> AES
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"/> <input type="checkbox"/> Change default route to this VPN tunnel