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.

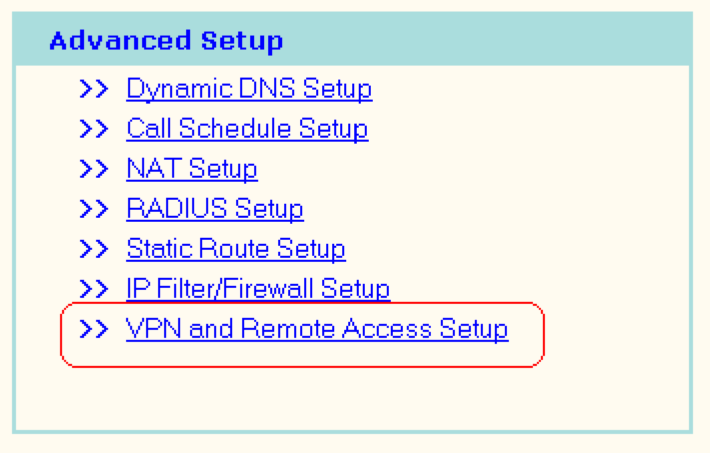
There are two types of VPN connections: the remote dial-in access VPN connection and the LAN-to-LAN VPN connection. The first, “Remote Dial-In Access” means the router allows a remote access node, a NAT router or a single user computer, to dial into a VPN router through the Internet to access the network 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.

Draytek Vigor router’s 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).

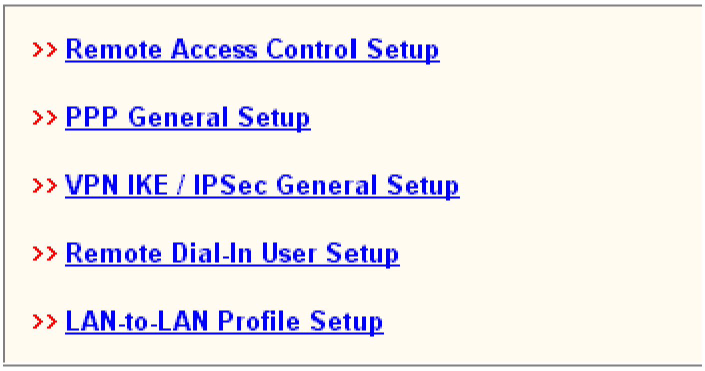
This chapter explains the capabilities of VPNs and remote access on the router. Use the following setup links on the Setup Main Menu to setup VPN and remote access functions.

Advanced Setup

> VPN and Remote Access Setup



The VPN and Remote Access Setup main menu has five main submenus.


>> 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.

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 apply to PPP related VPN type such as PPTP, L2TP and L2TP over IPSec.

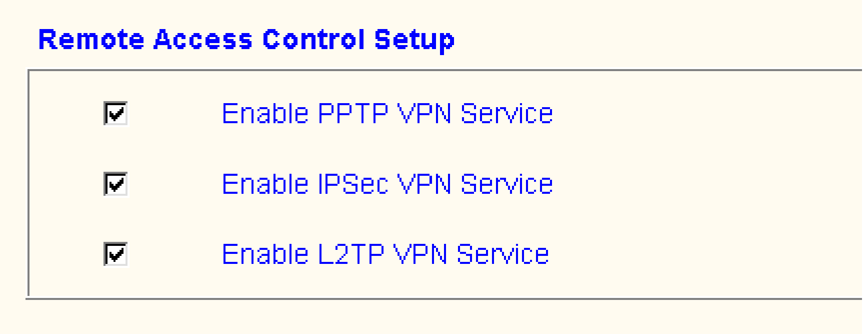
The **VPN IKE/IPSec General Setup** let you configure a common Pre-shared key and security method for remote dial-in user or node(LAN-to-LAN) which uses dynamic ip.

Use **The Remote Dial-In User Setup** to create dial-in user accounts. Vigor router supports three types of dial-in methods, PPTP, L2TP, and L2TP over IPSec. The PPTP VPN is compatable with all Windows plateforms 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 suppots four types of LAN-to-LAN VPN, IPSec Tunnel, PPTP, L2TP, and L2TP over IPSec. Simultaneously you can establish up to 16 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.



Remote Access Control Setup

☑ Enable PPTP VPN Service

☑ Enable IPSec VPN Service

☑ Enable L2TP VPN Service

2. PPP General Setup

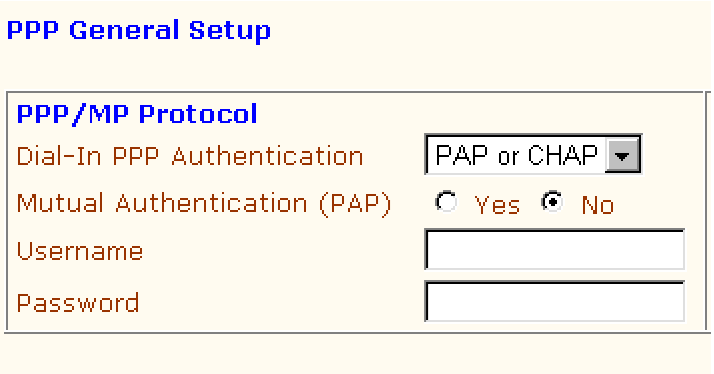
PPP/MP Setup

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

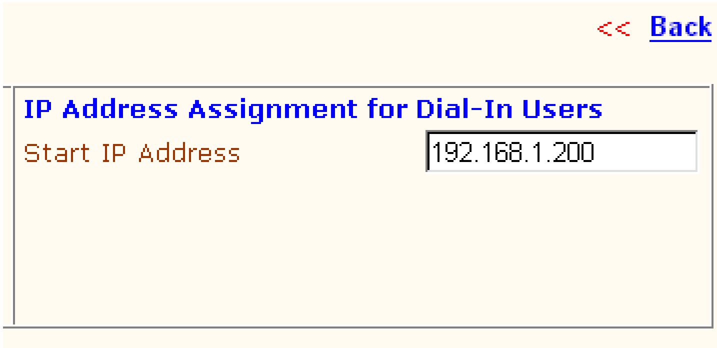
PPP/MP Protocol

Dial-In PPP Authentication: PAP or CHAP

Mutual Authentication (PAP): ○ Yes ● No

Username:

Password:



IP Address Assignment for Dial-In Users

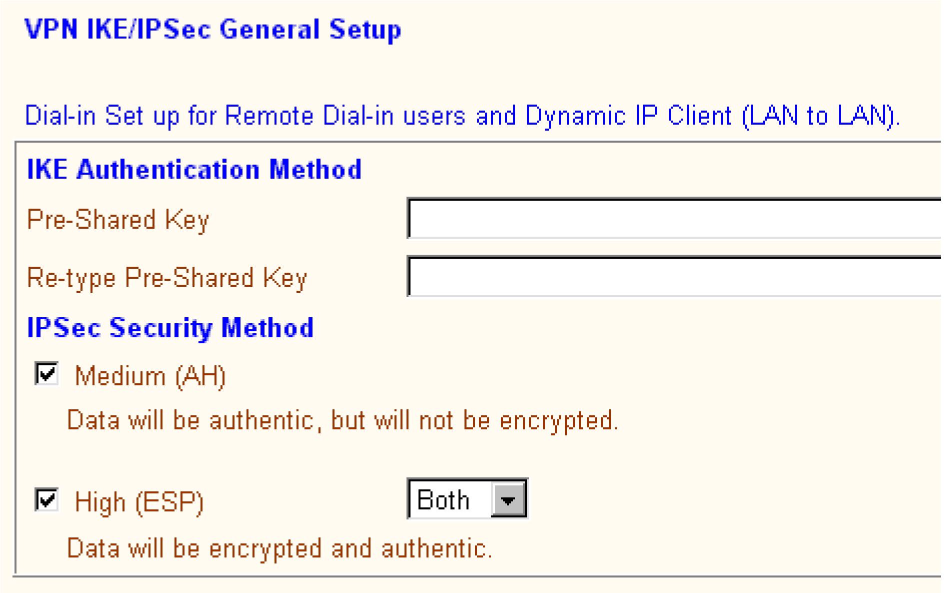
Start IP Address: 192.168.1.200

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.



VPN IKE/IPSec General Setup

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) Both

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.

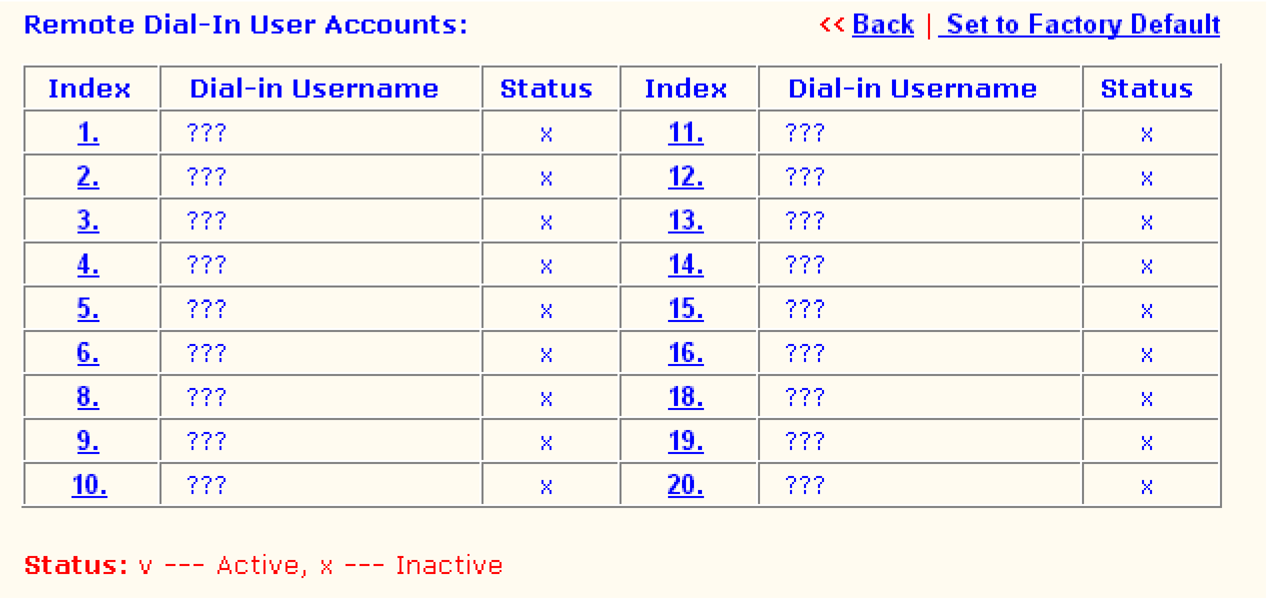
IPSec Security Method: Select allowed IPSec security methods.

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

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

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.



Remote Dial-In User Accounts:

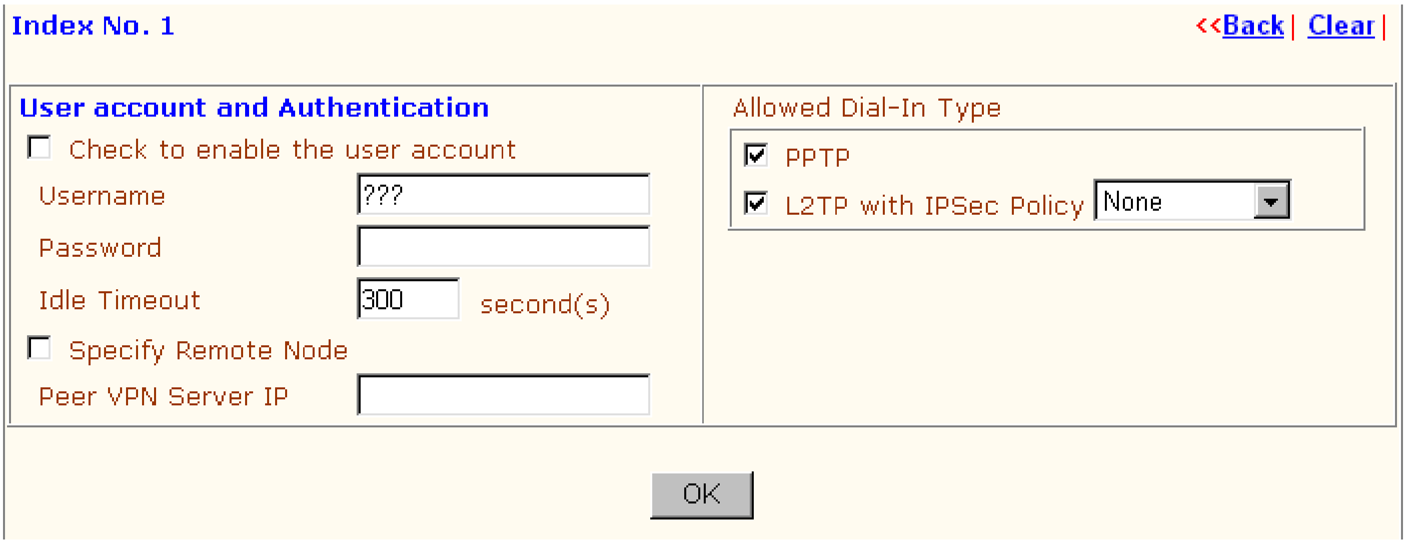
<< Back | Set to Factory Default

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
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.



Index No. 1

<<Back | Clear |

User account and Authentication

☐ Check to enable the user account

Username: ???

Password:

Idle Timeout: 300 second(s)

☐ Specify Remote Node

Peer VPN Server IP:

Allowed Dial-In Type

☑ PPTP

☑ L2TP with IPSec Policy: None

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 Specify Remote Node: For extra security, enable the option to allow the dial-in user to connect only from a specific IP address.

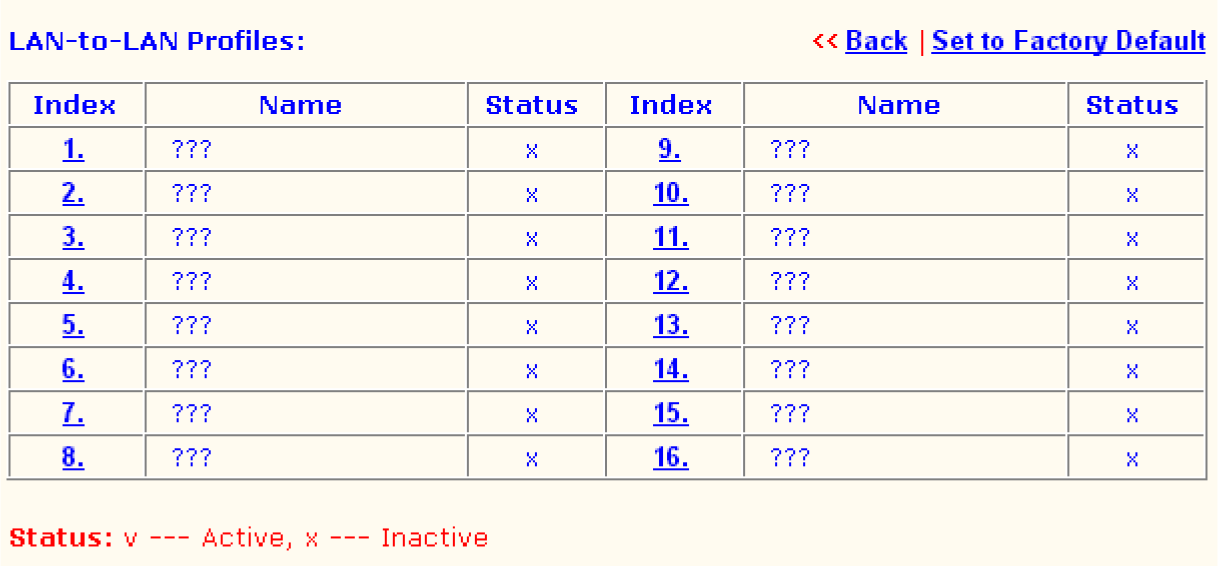
Allowed Dial-In Type : Select allowed dial-in types.

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”.

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

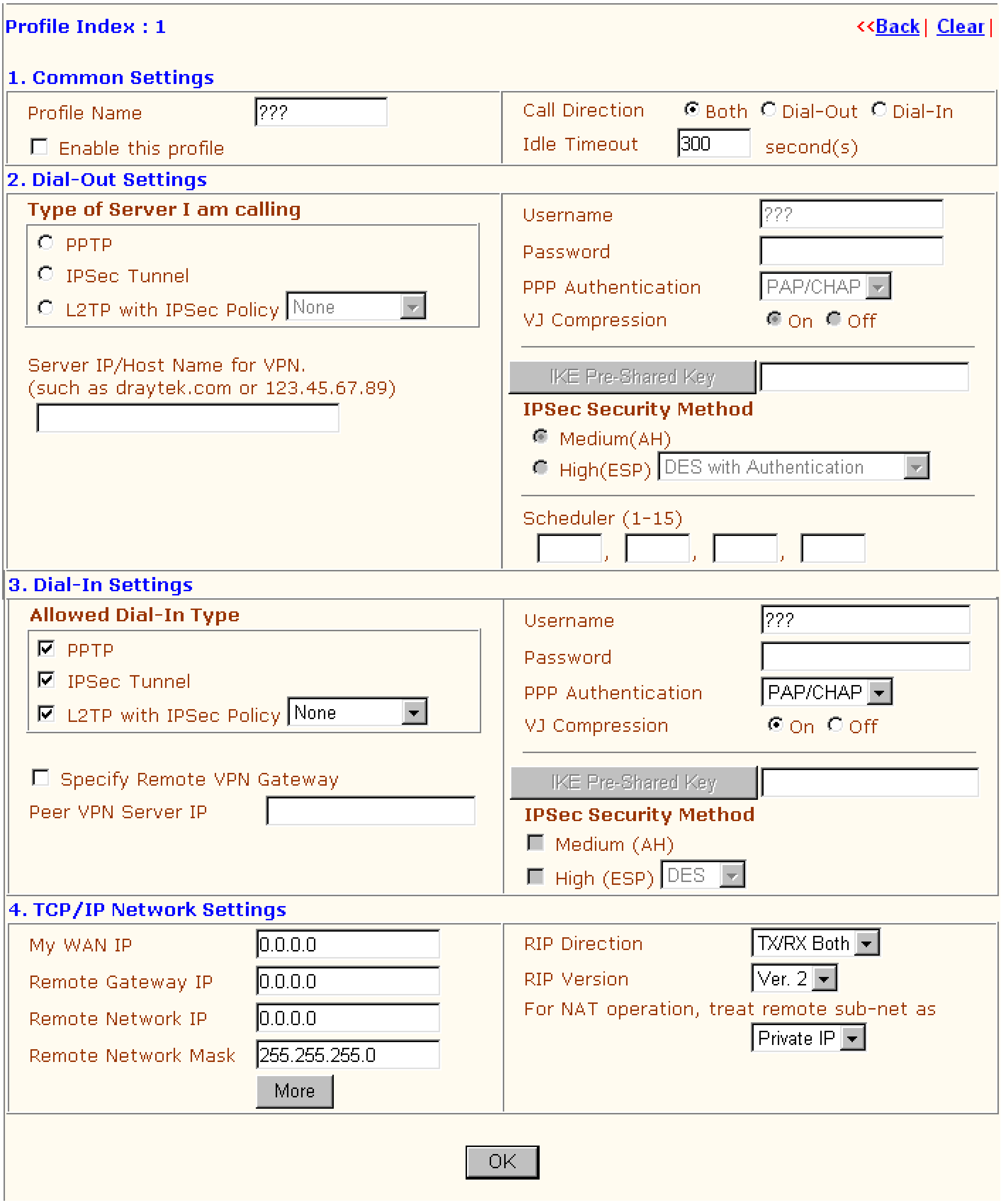
Set to Factory Default: Click here will clear all the LAN-to-LAN profiles.

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: ???
☐ Enable this profile
Call Direction: ● Both ○ Dial-Out ○ Dial-In
Idle Timeout: 300 second(s)

2. Dial-Out Settings

Type of Server I am calling
○ PPTP
○ IPSec Tunnel
○ L2TP with IPSec Policy: None

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)

Username: ???
Password:
PPP Authentication: PAP/CHAP
VJ Compression: ● On ○ Off

IKE Pre-Shared Key:

IPSec Security Method
● Medium(AH)
○ High(ESP): DES with Authentication

Scheduler (1-15): , , ,

3. Dial-In Settings

Allowed Dial-In Type
☑ PPTP
☑ IPSec Tunnel
☑ L2TP with IPSec Policy: None

☐ Specify Remote VPN Gateway
Peer VPN Server IP:

Username: ???
Password:
PPP Authentication: PAP/CHAP
VJ Compression: ● On ○ Off

IKE Pre-Shared Key:

IPSec Security Method
☐ Medium (AH)
☐ High (ESP): DES

4. TCP/IP Network Settings

My WAN IP: 0.0.0.0
Remote Gateway IP: 0.0.0.0
Remote Network IP: 0.0.0.0
Remote Network Mask: 255.255.255.0

RIP Direction: TX/RX Both
RIP Version: Ver. 2
For NAT operation, treat remote sub-net as: Private IP

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.

Dial-Out Settings

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

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.

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

If the dial-out VPN type is PPP related such as PPTP, L2TP or L2TP over IPSec. Please set up the following fields.

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, 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.

Dial-In Settings

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

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.

If IPSec Tunnel or L2TP with IPSec Policy set to **Nice to Have** or **Must**, select security methods as described in followings.

Check to Specify Remote VPN Gateway: For extra security, enables the option to allow the remote client to connect only from a specific IP address. If IPSec tunnel or L2TP over IPSec tunnel are selected, please fill a Pre-shared Key for this specific node.

Peer VPN Server IP: If **Specify Remote VPN Gateway** is enabled, enter the remote VPN server IP address in this field.

If any PPP related VPN types such as PPTP, L2TP or L2TP over IPSec are selected, please set up 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 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.

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.

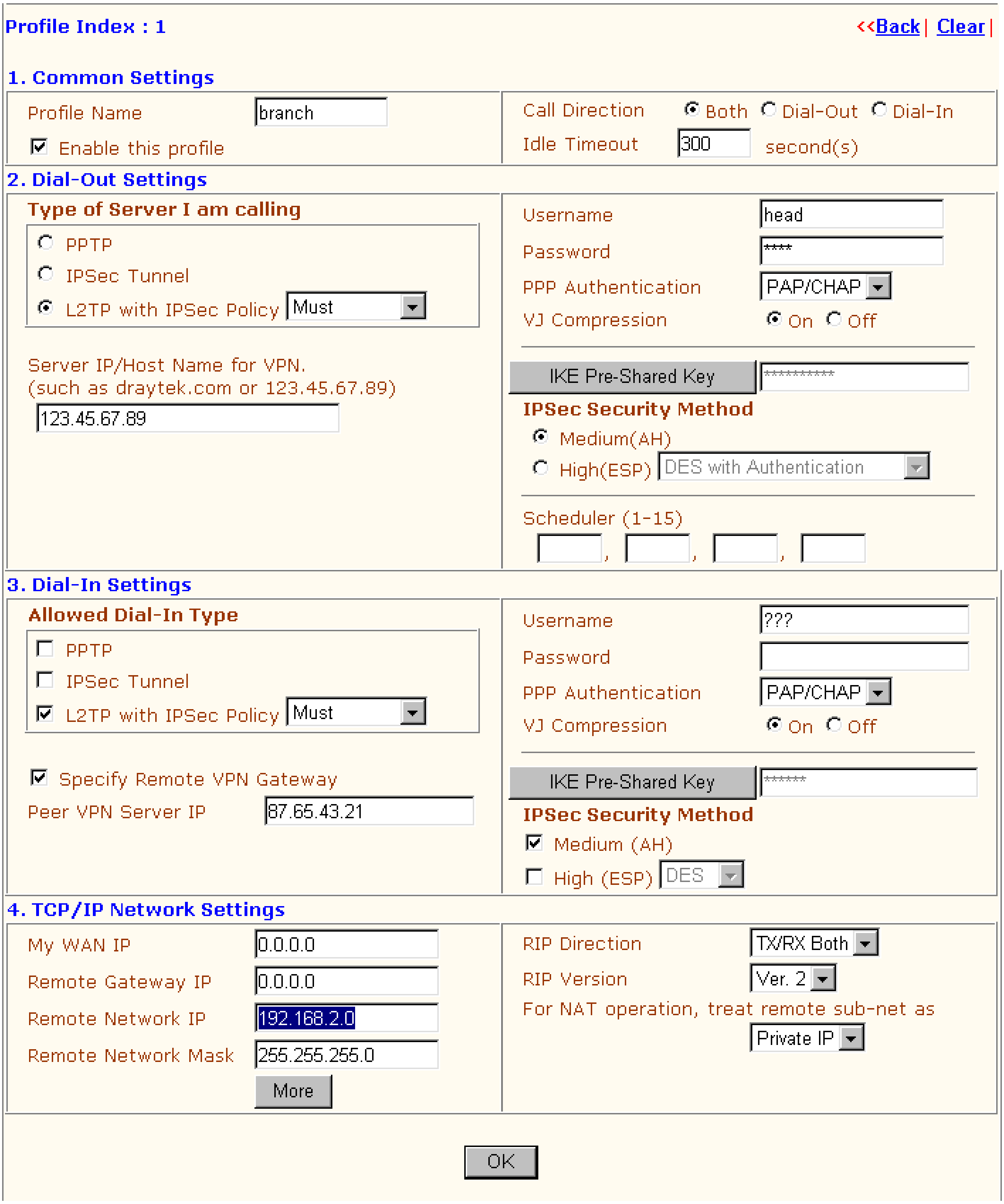
For NAT operation, treat remote sub-net as: The router has two local IP networks: the1st subnet and 2nd subnet. Here you set which subnet will be used as local network for VPN connection and exchange RIP packets with the remote network. Usually set to **Private IP** for routing between the 1st subnet 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

Head Office



Profile Index : 1

1. Common Settings

Profile Name: branch

☑ Enable this profile

Call Direction: ● Both ○ Dial-Out ○ Dial-In

Idle Timeout: 300 second(s)

2. Dial-Out Settings

Type of Server I am calling

○ PPTP

○ IPSec Tunnel

● L2TP with IPSec Policy: Must

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)

123.45.67.89

Username: head

Password: ****

PPP Authentication: PAP/CHAP

VJ Compression: ● On ○ Off

IKE Pre-Shared Key: ***********

IPSec Security Method

● Medium(AH)

○ High(ESP): DES with Authentication

Scheduler (1-15): ☐, ☐, ☐, ☐

3. Dial-In Settings

Allowed Dial-In Type

☐ PPTP

☐ IPSec Tunnel

☑ L2TP with IPSec Policy: Must

☑ Specify Remote VPN Gateway

Peer VPN Server IP: 87.65.43.21

Username: ???

Password:

PPP Authentication: PAP/CHAP

VJ Compression: ● On ○ Off

IKE Pre-Shared Key: *******

IPSec Security Method

☑ Medium (AH)

☐ High (ESP): DES

4. TCP/IP Network Settings

My WAN IP: 0.0.0.0

Remote Gateway IP: 0.0.0.0

Remote Network IP: 192.168.2.0

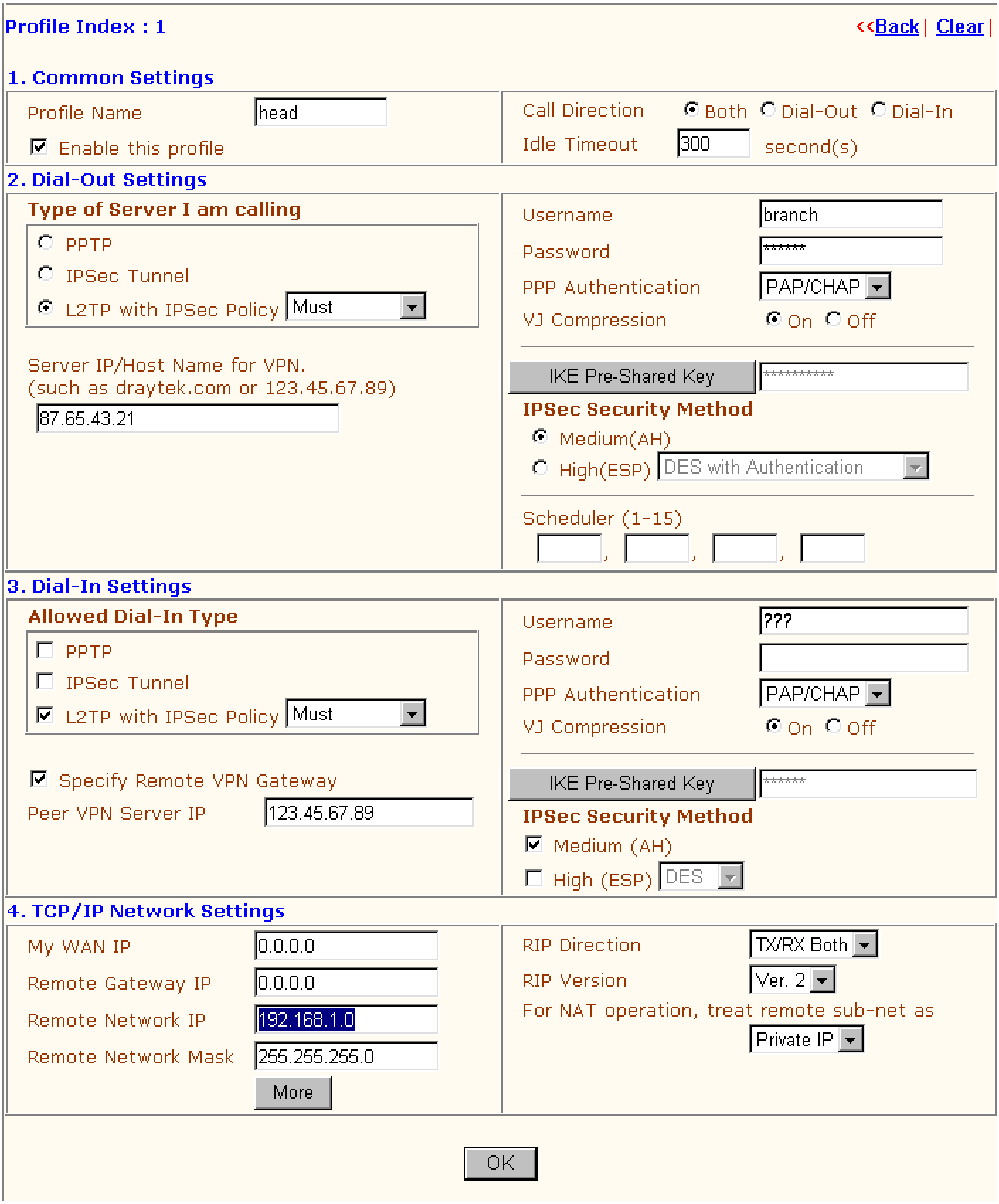
Remote Network Mask: 255.255.255.0

RIP Direction: TX/RX Both

RIP Version: Ver. 2

For NAT operation, treat remote sub-net as: Private IP

Branch Office



Profile Index : 1

<<Back | Clear |

1. Common Settings

Profile Name: head

☑ Enable this profile

Call Direction: ● Both ○ Dial-Out ○ Dial-In

Idle Timeout: 300 second(s)

2. Dial-Out Settings

Type of Server I am calling

○ PPTP

○ IPSec Tunnel

● L2TP with IPSec Policy: Must

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)
87.65.43.21

Username: branch

Password: ******

PPP Authentication: PAP/CHAP

VJ Compression: ● On ○ Off

IKE Pre-Shared Key: ***********

IPSec Security Method

● Medium(AH)

○ High(ESP): DES with Authentication

Scheduler (1-15): , , ,

3. Dial-In Settings

Allowed Dial-In Type

☐ PPTP

☐ IPSec Tunnel

☑ L2TP with IPSec Policy: Must

☑ Specify Remote VPN Gateway

Peer VPN Server IP: 123.45.67.89

Username: ???

Password:

PPP Authentication: PAP/CHAP

VJ Compression: ● On ○ Off

IKE Pre-Shared Key: ******

IPSec Security Method

☑ Medium (AH)

☐ High (ESP): DES

4. TCP/IP Network Settings

My WAN IP: 0.0.0.0

Remote Gateway IP: 0.0.0.0

Remote Network IP: 192.168.1.0

Remote Network Mask: 255.255.255.0

More

RIP Direction: TX/RX Both

RIP Version: Ver. 2

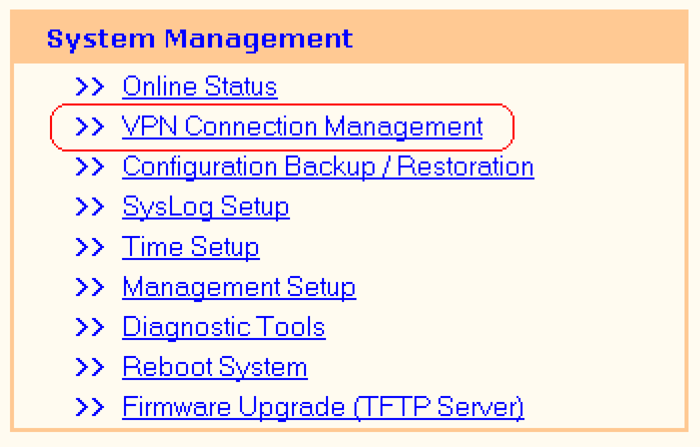
For NAT operation, treat remote sub-net as: Private IP

OK

Validation and Troubleshooting

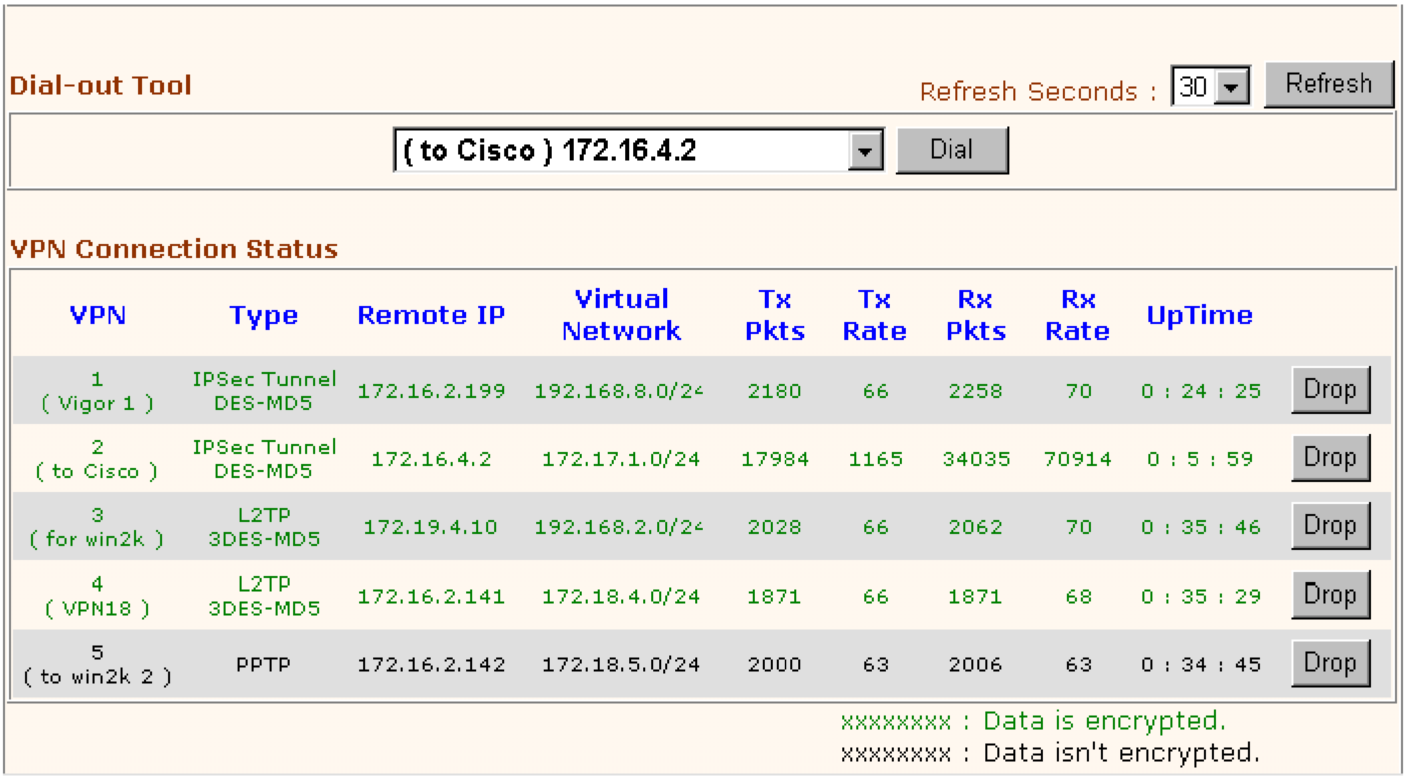
Initial a VPN connection

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" buttom 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)



Dial-out Tool

Refresh Seconds : 30

(to Cisco) 172.16.4.2

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	192.168.8.0/2	2180	66	2258	70	0 : 24 : 25	Drop
2 (to Cisco)	IPSec Tunnel DES-MD5	172.16.4.2	172.17.1.0/24	17984	1165	34035	70914	0 : 5 : 59	Drop
3 (for win2k)	L2TP 3DES-MD5	172.19.4.10	192.168.2.0/2	2028	66	2062	70	0 : 35 : 46	Drop
4 (VPN18)	L2TP 3DES-MD5	172.16.2.141	172.18.4.0/24	1871	66	1871	68	0 : 35 : 29	Drop
5 (to win2k 2)	PPTP	172.16.2.142	172.18.5.0/24	2000	63	2006	63	0 : 34 : 45	Drop

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