CHAPTER 10

Virtual Private Network and Remote Access Setup

10.1 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.

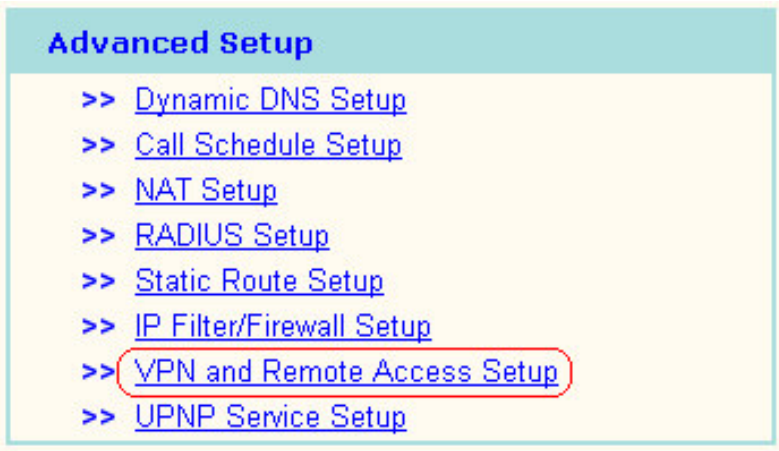
There are two types of VPN connections: the remote dial-in access VPN connection and the LAN-to-LAN VPN connection. The “Remote Dial-In Access” facility allows a remote access node, a NAT router or a single user computer, to dial into a VPN router through the Internet to access the network resources 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. However, Vigor 2600Ge only provides “LAN-to-LAN Access” of VPN connection. If the “Remote Dial-In Access” of VPN connection is necessary for using, you can refer to other Vigor series of routers.

The VPN technology employed in the Vigor routers support 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

Advanced Setup > VPN and Remote Access Setup



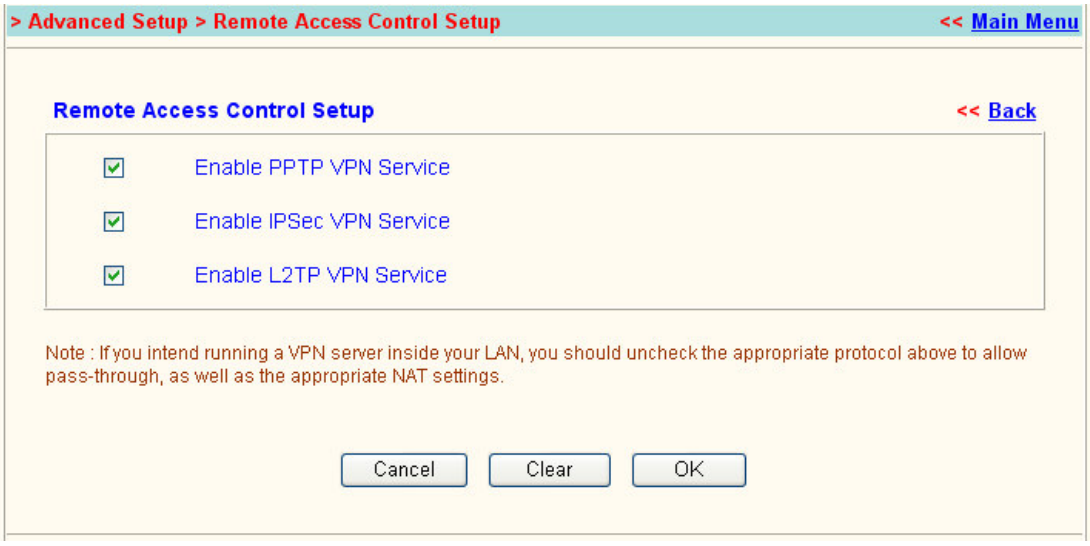
The **VPN and Remote Access Setup** has five main functions, as shown below. You may set up **Remote Access Control**, and **LAN-to-LAN Profile** on demand.

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 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 2 VPN tunnels.

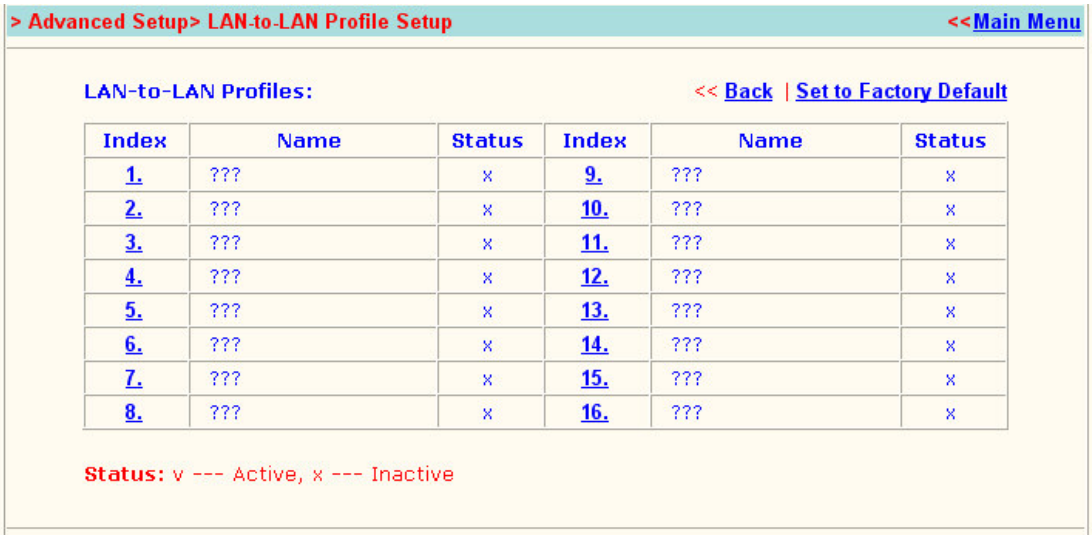
10.2 Remote Access Control Setup

As depicted in the following picture, click the appropriate checkbox 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.



10.3 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.



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

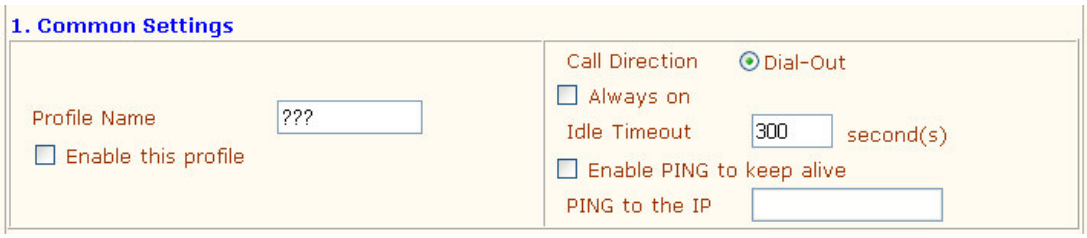
Index: Click a number to open a detailed setting page for each profile.

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 3 subgroups: **Common Settings**, **Dial-Out Settings**, and **TCP/IP Network Settings**. In the following, we explain each subgroup in detail.

10.3.1 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. ***Dial-Out*** means it can only be used for outgoing 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, it set to 300 seconds. If the profiles connection is idle over the limitation of the timer, the router will drop the connection.

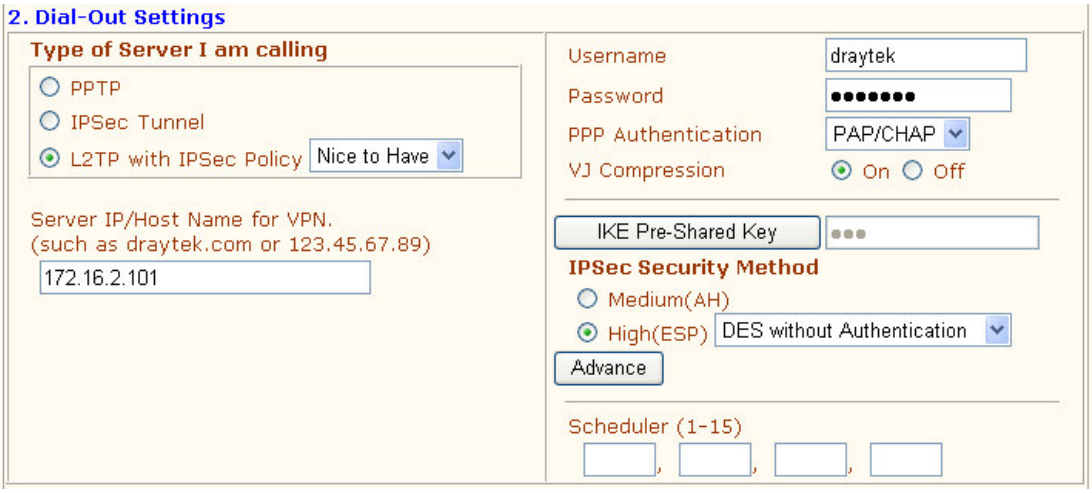
Enable PING to keep alive: Click this item to enable the transmission of PING packets to an IP address defined in the field of "***PING to the IP***".

***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.

10.3.2 Dial Out Settings



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

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.

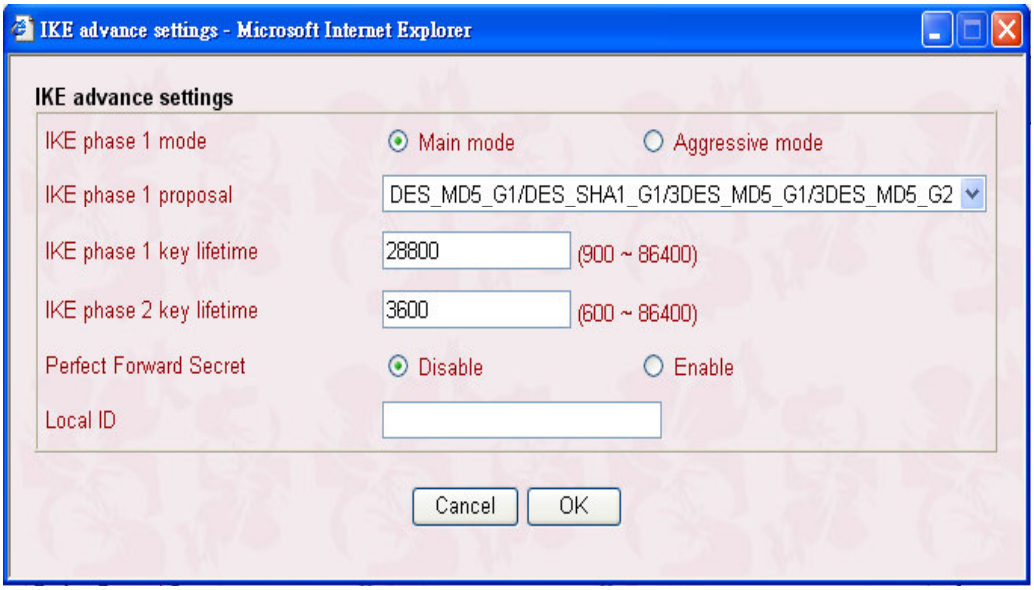
***DES with Authentication*:** Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

***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 phase 1 mode: ***Main mode*** and ***Aggressive mode*** are provided in the Vigor routers. Basically, both modes are two kinds of Phase 1 IKE negotiation process. Most VPN servers support Main mode and so does the Vigor 2900 series of routers. Aggressive mode is a more recent implementation to speed up the negotiation process, but may incur less security. The Vigor router also supports 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 lastest term, i.e. "DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_MD5_G2".
This is because that more selections are available, more likehood 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.

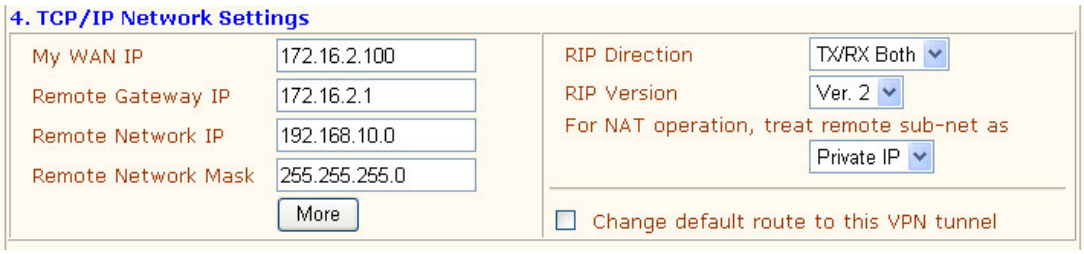
IKE phase 2 key lifetime: By default, the phase 2 key lifetime is set to the standard value, i.e. 3600 seconds. You also are able to specify a value in between 600 and 86400 seconds according to your demand.

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.

10.3.3 TCP/IP Network Settings



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

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

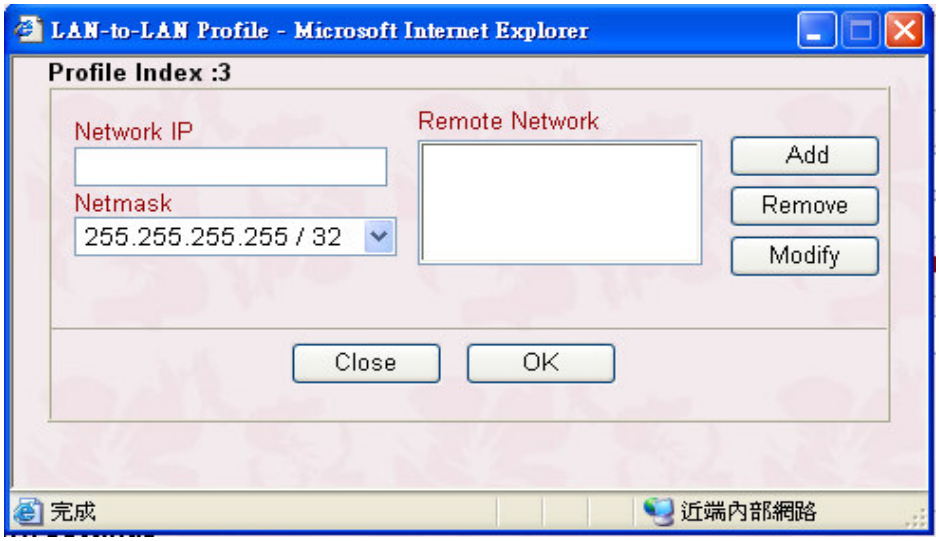
Remote Gateway IP: In most cases, you may accept the default value of 0.0.0.0 in this field. The router will then get a Remote Gateway IP address from the remote router during the IPCP negotiation phase. If the Remote Gateway IP address is fixed, specify the fixed IP address here.

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.

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 the remote network.

10.4 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