



# Vigor 3300 Series Application Notes

Version : 2.0  
Date : 2006/6/12

# Table of Contents

<b>Chapter 1 . High Availability Function .....</b>	<b>1</b>
1.1 Introduction.....	1
1.2 Examples and Web Configurations.....	2
<b>Chapter 2 . VPN Function.....</b>	<b>4</b>
2.1 VPN Dial-in Function.....	4
2.1.1 Introduction .....	4
2.1.2 Examples and Web Configurations.....	5
2.2 VPN Dial-out Function.....	14
2.2.1 Introduction .....	14
2.2.2 Examples and Web Configurations.....	15
2.3. VPN Three Parts Communication .....	23
2.3.1 Introduction .....	23
2.3.2 Examples and Web Configurations.....	25
2.4 IPSec Host-to-LAN (Smart VPN Client) --- DHCP over IPSec.....	42
2.4.1 Introduce .....	42
2.4.2 Configuration on Server.....	42
2.4.3 Configuration on Smart VPN Client .....	44
2.5 VPN PPTP Host-to-LAN by Smart VPN Client .....	48
2.5.1 Introduction .....	48
2.5.2 Configuration.....	48
<b>Chapter 3. VoIP Function .....</b>	<b>54</b>
3.1 VoIP Example 1 - Basic Configuration and Registration.....	54
3.1.1 Vigor 3300V Configuration Example.....	55
3.1.2 Vigor 2900V Configuration Example.....	59
3.2 VoIP Example 2 - Basic Calling Method.....	61
3.2.1 Direct IP Call (Call with each other without registration).....	61
3.2.2 Intercommunication with one SIP Proxy Server (registration) .....	64
3.2.3 Intercommunication with different SIP Proxy Servers.....	66
3.3 VoIP Example 3 - VoIP over VPN .....	67
3.3.1 Vigor 3300V Configuration Example.....	69
3.3.2 Vigor 2900V Configuration Example.....	70
3.3.3 Vigor 2200V Configuration Example.....	71
3.4 VoIP Example 4 - Practical Application of FXS .....	73
3.5 VoIP Example 5 - Practical Application of FXO.....	76
3.6 VoIP Example 6 - Register with Private IP Address.....	79
3.6.1 Vigor 2600V Configuration Example.....	80
3.6.2 Vigor 3300V Configuration Example.....	82
3.7 Asterisk Application .....	84
3.7.1 Introduce .....	84
3.7.2 Configuring Asterisk.....	85
3.7.3 Configuring Vigor 3300V.....	95

<b>Chapter 4. Load Balance Policy .....</b>	<b>98</b>
4.1 Introduction.....	98
4.2 Examples and Web Configurations.....	98
<b>Chapter 5. 802.1Q VLAN.....</b>	<b>102</b>
5.1 VLAN Overview .....	102
5.2 VLAN Trunk.....	103
5.3 Why Use VLANs?.....	103
5.4 LAN to LAN Communication .....	104
5.5 Management Port.....	105

# Chapter 1 . High Availability Function

This chapter shows how to setup high availability function.

This chapter is divided into the following sections,

Section 1.1: Introduction

Section 1.2: Examples and Web Configurations

## 1.1 Introduction

The basic application graph is shown in Figure 1-1. There are two Vigor 3300V routers connected to the Internet. One is as Master and the other one is as Slave. Both are connected to a subnet – 192.168.1.x from the LAN port. For the further more settings, please refer to the next section.

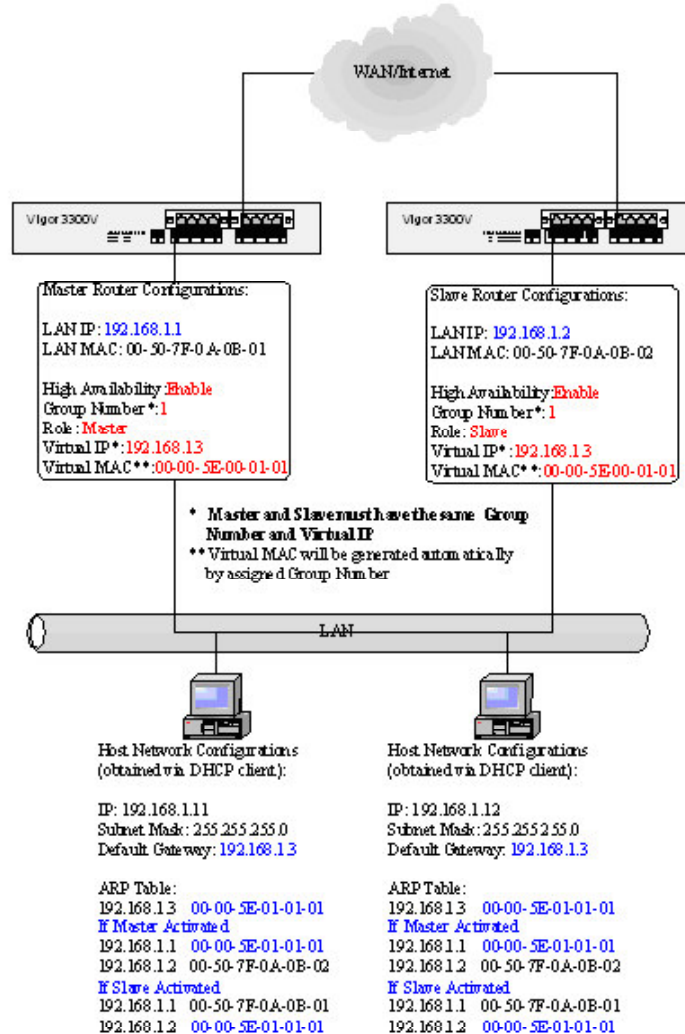


Figure 1-1. A Scenario of High Availability

## 1.2 Examples and Web Configurations

At first, we need to configure High Availability in the Master device. Please refer to the Figure 1-2.

The screenshot shows the 'Network - LAN - High Availability' configuration page for a Vigor3300 series device. The page has a navigation bar with 'Quick Setup', 'System', 'Network', 'Advanced', 'Firewall', 'QoS', 'VPN', and 'VoIP'. The 'Network' menu is selected. The main content area contains the following settings:

- High Availability:  Disable  Enable
- Group Number:  (Range: 1-255)
- Role:
- Virtual IP:

Buttons for 'Apply' and 'Cancel' are at the bottom right. A footer note reads: 'DrayTek Corp. © 1997 - 2009 All rights reserved. DrayTek provides enterprise network solutions.'

Figure 1-2. Web settings of the Master

Then, we have to configure High Availability in the Slave device. Please refer to the Figure 1-3.

The screenshot shows the 'Network - LAN - High Availability' configuration page for a Vigor3300 series device. The page has a navigation bar with 'Quick Setup', 'System', 'Network', 'Advanced', 'Firewall', 'QoS', 'VPN', and 'VoIP'. The 'Network' menu is selected. The main content area contains the following settings:

- High Availability:  Disable  Enable
- Group Number:  (Range: 1-255)
- Role:
- Virtual IP:

Buttons for 'Apply' and 'Cancel' are at the bottom right. A footer note reads: 'DrayTek Corp. © 1997 - 2009 All rights reserved. DrayTek provides enterprise network solutions.'

Figure 1-3. Web settings of the Slave

The most important points are as below –

Both the Master and Slave must share the same Group number value.

The “Role” value of the Master device is different from that of the Slave device.

Both the Master and Slave must share the same Virtual IP value.

### ***Master Failure / Shutdown***

Once the Master unit is shut down or fails, Slave would be switched from idle state to active state after 3 to 4 seconds and then take over Master.

### ***Master Restart***

Once Master is back to normal, and then Slave will be restored to be idleness.

### ***Multiple Slaves***

There should be only one Master, but multiple Slaves are allowed. Generally speaking, the Slave with the greater LAN IP address will have higher priority to play the role of Master if the original Master is shut down or fails. For example, the IP address 192.168.1.4 will have higher priority over 192.168.1.3.

### ***Reference***

The HA function was developed based on VRRP (Virtual Router Redundancy Protocol). For further detailed information about VRRP, please refer to RFC 2338.

## Chapter 2 . VPN Function

This chapter is divided into the following sections,

Section 2.1: VPN Dial-in Function

Section 2.2: VPN Dial-out Function

Section 2.3: VPN Three Parts Communication

Section 2.4: IPSec Host to LAN ( Smart VPN Client ) – DHCP over IPSec

Section 2.5: VPN PPTP Host-to LAN by Smart VPN Client

### 2.1 VPN Dial-in Function

#### 2.1.1 Introduction

The first example is to establish a LAN to LAN VPN Tunnel. The basic form of LAN to LAN VPN is to let both routers' internal networks can connect with to each other. In this example since only one site has a fixed IP address, the VPN tunnel must be established in one direction .(from dynamic-IP site to fixed-IP site). If you do want both sites can always to initiate the connection automatically, the router with the dynamic IP must be always online. Otherwise, only one direction can work normally. In this example, only Vigor 3300V has a fixed IP address, so when the VPN Tunnel is dropped, Vigor 3300V cannot initiate a connection to Vigor 2900V.

Suppose the Headquarters in Taipei uses a Vigor 3300V, while the branch office in Shanghai uses a Vigor2900V. The network administrator requires the employees in branch office to access the database in the headquarters through the encrypted VPN tunnels. The purpose is to avoid leakage of relevant confidential information which is important. Please refer to Figure 2-1.

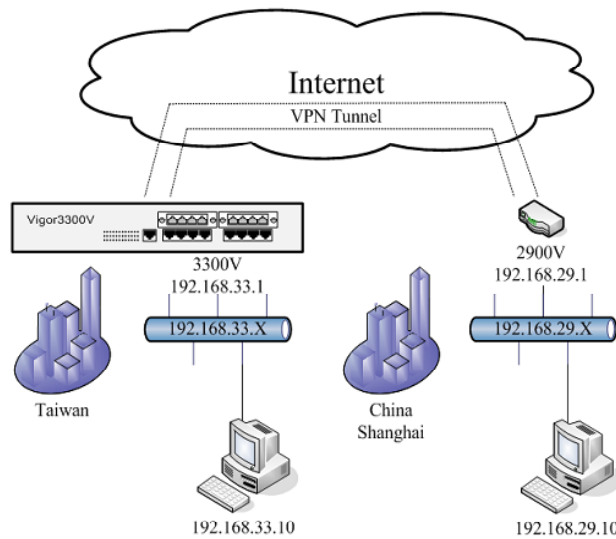


Figure 2-1. A scenario of VPN in dial-in from Vigor 2900V

There Below is a configuration table as below between Vigor 3300V and Vigor 2900V.

	Vigor 3300V Headquarters	Vigor 2900V Branch Office
WAN IP	220.135.240.207 PPPoE, fixed IP	61.31.167.135 PPPoE, dynamic IP
LAN IP	192.168.33.1	192.168.29.1
Internal Network	192.168.33.X	192.168.29.X
Encryption Method	DES-SHA1	
Preshared Key	3300	

## 2.1.2 Examples and Web Configurations

### 2.1.2.1 Configurations in Vigor 3300V

#### Step 1

Suppose the subnet of Vigor 3300V internal network is 192.168.33.X, for detailed setup instructions please refer to the LAN Setup chapter. Enter VPN\IPSec\Policy Table, click 1, and then press Edit. Please refer to Figure 2-2.

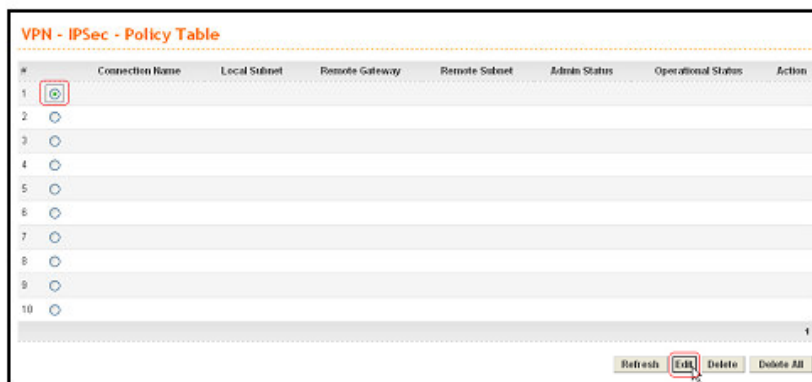


Figure 2-2. Edit of policy table1

#### Step 2

First you should enter the **Default** page. There are three fields on this page.

#### **Basic**

It deals with basic settings, including profile name, authentication type, preshared key, etc.

#### **Name**

You can specify a name to this profile. To facilitate easy management and differentiation, please type “**2900V**”.

#### **Preshared Key**

Type “**3300**” (It must be identical with 2900V's).



### *Admin Status*

Use the default settings (**Enable**).

### **Local Gateway**

It deals with relevant settings of the local router, including selection of the WAN and internal network, etc.

### *WAN Interface*

Vigor 3300V has 4 WAN ports. In this example, we choose **WAN1** to establish the VPN tunnel.

### *Network IP / Subnet Mask*

It is the internal network of Vigor 3300V. Please enter **192.168.33.0 /24** (/24 = Mask 255.255.255.0).

### **Remote Gateway**

It deals with relevant settings of the remote router, including WAN IP and internal network, etc.

### *Security Gateway*

It is about the WAN IP of Vigor2900V. In this example it is not fixed, so please enter **0.0.0.0**.

### *Network IP / Subnet Mask*

It is the internal network of Vigor2900V. Please enter **192.168.29.0 /24** (/24 = Mask 255.255.255.0).

Please refer to Figure 2-3.

The screenshot shows the 'VPN - IPSec Tunnel' configuration interface. It has two tabs: 'Default' (selected) and 'Advanced'. The 'Basic' section contains: Name: 2900V; Authentication: Pre-shared Key; Pre-shared Key: \*\*\*\*; Security Protocol: ESP; Admin Status: Enable. The 'Local Gateway' section contains: WAN Interface: WAN1; Local Certificate: (empty); Security Gateway: default; Network IP / Subnet Mask: 192.168.33.0 /24; Next hop: default. The 'Remote Gateway' section contains: Remote ID: (empty); DHCP-over-IPSec: OFF; Security Gateway: 0.0.0.0; Network IP / Subnet Mask: 192.168.29.0 /24. Red boxes highlight the values 2900V, WAN1, 192.168.33.0 /24, 0.0.0.0, and 192.168.29.0 /24. 'Apply' and 'Cancel' buttons are at the bottom right.

Figure 2-3. Web settings of Vigor 3300V

### Step 3

#### Advanced page

In this example since the connection is initiated by Vigor 2900V, the encryption method is determined by Vigor 2900V. By default Vigor 3300V allows des-md5, des-sha1, 3des-md5 and 3des-sha1, so no change is required. Just press the Apply button to finish the configuration. Please refer to Figure 2-4.

VPN - IPsec Tunnel

Default **Advanced**

IKE Phase1 (main mode)

Key lifetime: 480 minutes

Proposal: des-md5-aodp768 des-sha-aodp768 3des-md5-aodp768 3des-sha-aodp1024

IKE Phase2 (quick mode)

Key lifetime: 60 minutes

Proposal: des-md5 des-sha1 3des-md5 3des-sha1

PFS (Perfect Forward Secrecy)

Dead Peer Detection

Status:  Disable  Enable

Delay: 30 seconds

Timeout: 120 seconds

Apply Cancel

Figure 2-4. Advanced settings of Vigor 3300V

### Step 4

After configuration, the router will jump switch to the VPN - IPsec - Policy Table page. Confirm if the settings are correct. Now the setup for 3300V configuration is completed. Please refer to Figure 2-5.

VPN - IPsec - Policy Table

#	Connection Name	Local Subnet	Remote Gateway	Remote Subnet	Admin Status	Operational Status	Action
1	2900V	192.168.33.0/24	0.0.0.0	192.168.29.0/24	enable	down	edit
2							
3							
4							
5							
6							
7							
8							
9							
10							

1

Refresh Edit Delete Delete All

Figure 2-5. Policy table of Vigor 3300V

### 2.1.2.2 Configurations in Vigor2900V

There are some setup procedures as below.

#### Step 1

Enter the web page of Vigor2900V, and click the **VPN and Remote Access Setup** link. Please refer to Figure 2-6.



Figure 2-6. VPN web of Vigor2900V

#### Step 2

Click the **LAN-to-LAN Profile Setup** link. Please refer to 11-7.



Figure 2-7. LAN to LAN settings of Vigor2900V

### Step 3

Click **Index 1**, and enter relevant settings of the VPN tunnel connected to Vigor 3300V. Please refer to Figure 2-8.

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

<< **1-16** | **17-32** >>

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

Figure 2-8. LAN to LAN profiles of Vigor2900V

### Step 4

#### Common Setting

It deals with basic settings, including profile name, enable or disable the profile, call direction, etc.

#### Profile Name

Specify a name to this profile. To facilitate easy management and differentiation, please type “3300V”.

#### Call Direction

Specify the call direction to this profile. In this example the connection is initiated from Vigor 2900V to Vigor 3300V, so please select Dial-Out. In this example V3300V is not allowed to dial in.

#### Idle Timeout

By default, it is 300 seconds. If the profile connection is idle over the threshold of the timer, the router will drop the connection.

Please refer to Figure 2-9.

**1. Common Settings**

Profile Name:

Enable this profile

Call Direction:  Both  Dial-Out  Dial-In

Always on

Idle Timeout:  second(s)

Enable PING to keep alive

PING to the IP:

Figure 2-9. Common settings of Vigor2900V

## Dial-Out Setting

It deals with relevant settings of Dial-Out connection, including encryption method, preshared key and remote site's WAN IP.

Select **IPSec Tunnel** and enter the WAN IP **220.135.240.207** of Vigor 3300V. Press the **IKE Pre-Shared Key** button, and then a window will pop up. Just type **3300** (It must be identical to 3300V's). Press finish the configuration of IKE Pre-Shared Key. Then click **High (ESP)** and select **DES with Authentication** (default is DES without Authentication).

Figure 2-10. Dial-out settings of Vigor 2900V

## Dial-in Setting

It deals with relevant settings of Dial-In connection. In this example you do not need to configure this part.

Figure 2-11. Dial-in settings of Vigor 2900V

## TCP/IP Network Settings

It deals with the internal network of the remote site, etc.

In the **Network IP** and **Mask** field, enter **192.168.33.0** and **255.255.255.0** respectively, and then press “OK” to finish the configuration. Please refer to Figure 2-12.

4. TCP/IP Network Settings

My WAN IP: 0.0.0.0

Remote Gateway IP: 0.0.0.0

Remote Network IP: 192.168.33.0

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

Change default route to this VPN tunnel

More

OK

Figure 2-12. TCP/IP network settings of Vigor2900V

## Step 5

After configuration, the router will automatically switch to the **LAN-to-LAN Profiles Setup** page. Confirm if the settings are correct. Now the setup configuration for of Vigor2900V is completed. Please refer to Figure 2-13.

LAN-to-LAN Profiles:

Index	Name	Status	Index	Name	Status
1.	3300V	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

<< 1-16 | 17-32 >>

Figure 2-13. Created profiles of Vigor2900V

## Step 6

Enter the main page of Vigor2900V and click the **VPN Connection Management** link. From the pull-down menu, select **(3300V) 220.135.240.207**, and then press “Dial”. Vigor 2900V will initiate the VPN connection to Vigor 3300V. Please refer to Figure 2-14.

System Management > VPN Connection Management

Dial-out Tool

Refresh Seconds: 10 Refresh

(3300V) 220.135.240.207 Dial

VPN Connection Status

Current Page: 1 Next

VPN Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime
----------	-----------	-----------------	---------	---------	---------	---------	--------

Figure 2-14. Connection settings of Vigor2900V

### Step 7

Please wait about 5~10 seconds, you will find the VPN tunnel has been established. Please refer to Figure 2-15.

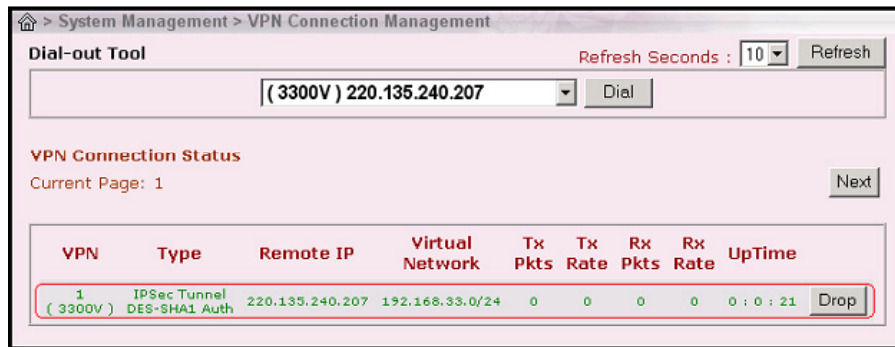


Figure 2-15. Connection status of Vigor2900V

### Step 8

Please enter the CLI and try to **ping 192.168.33.1** (Vigor 3300V) to see if there is any response. Please refer to Figure 2-16.

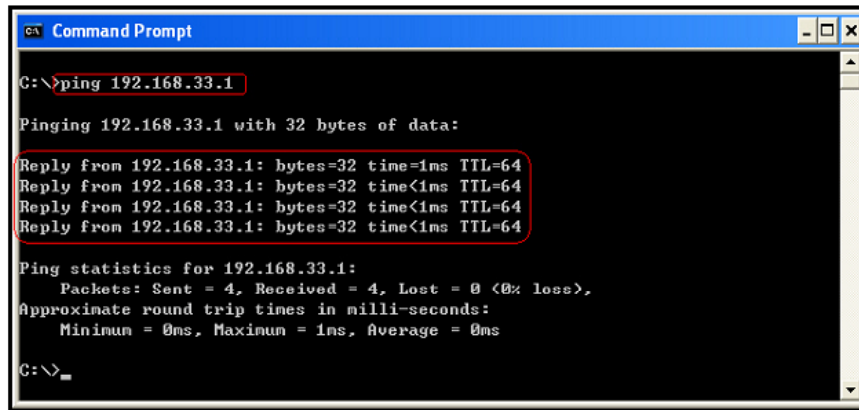


Figure 2-16. Ping status

### Step 9

If the numbers of Tx Pkts & Rx Pkts increase, it means there is traffic through the VPN tunnel. Please refer to Figure 2-17.

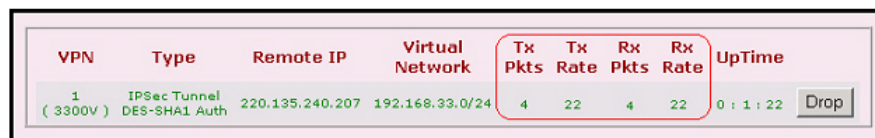
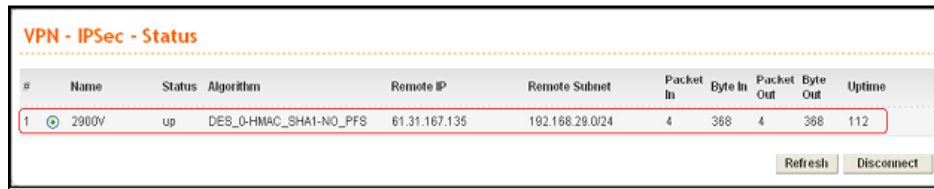


Figure 2-17. Statistics status

### Step 10

Enter the page of Vigor 3300V Web and enter **VPN\IPSec\Status**, and then you will find the VPN tunnel has been established. Please refer to Figure 2-18.

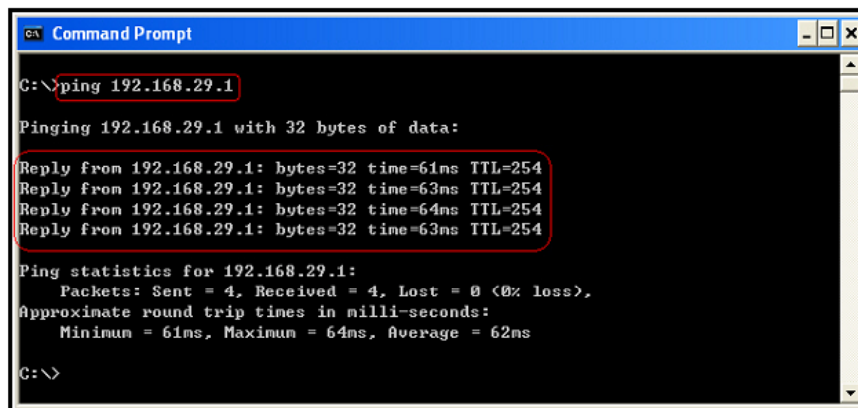


#	Name	Status	Algorithm	Remote IP	Remote Subnet	Packet In	Byte In	Packet Out	Byte Out	Uptime
1	2900V	up	DES_0-HMAC_SHA1-NO_PFS	61.31.167.135	192.168.29.0/24	4	368	4	368	112

Figure 2-18. IPSec status

### Step 11

Enter the CLI and attempt to **ping 192.168.29.1** (Vigor 2900V) to see if there is any response. Please refer to Figure 2-19.



```
Command Prompt
C:\>ping 192.168.29.1
Pinging 192.168.29.1 with 32 bytes of data:
Reply from 192.168.29.1: bytes=32 time=61ms TTL=254
Reply from 192.168.29.1: bytes=32 time=63ms TTL=254
Reply from 192.168.29.1: bytes=32 time=64ms TTL=254
Reply from 192.168.29.1: bytes=32 time=63ms TTL=254

Ping statistics for 192.168.29.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 61ms, Maximum = 64ms, Average = 62ms

C:\>
```

Figure 2-19. Ping status

### Step 12

If the numbers of Packet In & Packet Out increase, it means there are packets passing is traffic through the VPN tunnel.

Now the VPN tunnel has been successfully established.



## 2.2 VPN Dial-out Function

### 2.2.1 Introduction

This case is based on example 1. The difference is that both sites have a fixed IP address and the connection is initiated from Vigor 3300V (Dial-Out) to Vigor 2900V (Dial-In).

Suppose the Headquarters in Taipei use a Vigor 3300V, while the branch office in Shanghai uses a Vigor 2900V. The network administrator requires the employees in branch office to access the database in the headquarters through the encrypted VPN tunnel. The purpose is to avoid leakage of confidential information.

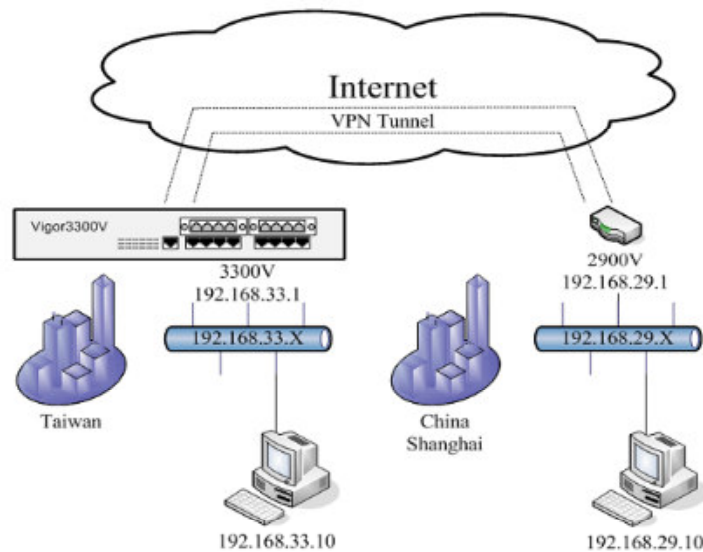


Figure 2-20. A scenario architecture graph

Below is a configuration table between Vigor 3300V and Vigor 2900V.

	<b>3300V</b> Headquarters	<b>2900V</b> Branch Office
WAN IP	220.135.240.207	61.31.167.135
	PPPoE, fixed IP	PPPoE, fixed IP
LAN IP	192.168.33.1	192.168.29.1
Internal Network	192.168.33.X	192.168.29.X
Encryption Method	DES-SHA1	
Preshared Key	<b>3300</b>	

## 2.2.2 Examples and Web Configurations

### 2.2.2.1 Configurations in Vigor 2900V

There are some procedures as below.

#### Step 1

Enter Vigor 2900V's web page of Vigor 2900V, click the **VPN and Remote Access Setup** link.



Figure 2-21. Vigor 2900V web configuration

#### Step 2

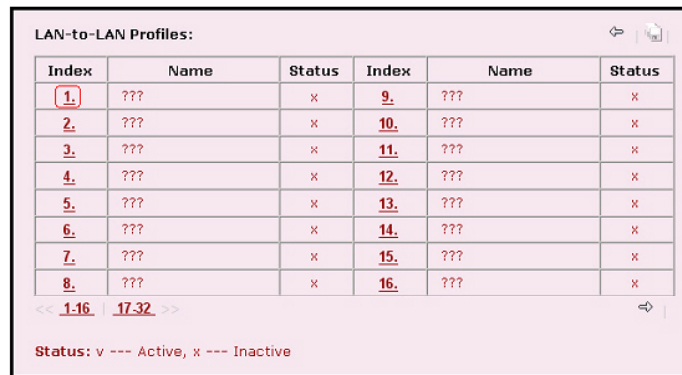
Click the **LAN-to-LAN Profile Setup** link.



Figure 2-22. LAN-to-LAN profile setup

### Step 3

Click **Index 1** and enter relevant settings for the VPN tunnel to Vigor 3300V. Please refer to Figure 12-4.



LAN-to-LAN Profiles:

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

<< 1-16 17-32 >>

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

Figure 2-23. Enter relevant VPN setup

### Step 4

On this page there are four sections for relevant VPN setup as below.

#### Common Settings

These are basic settings, including profile name, enable or disable the profile, call direction, etc.

#### Profile Name

Specify a name to this profile. To facilitate easy management and differentiation, please type **3300V**.

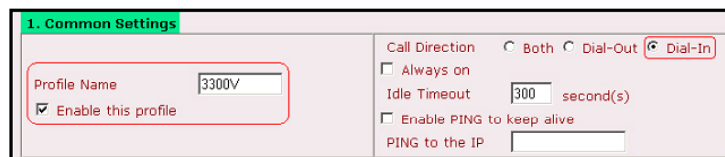
#### Call Direction

Specify the call direction to this profile. In this example the connection is initiated from V3300V to Vigor 2900V, so please select **Dial-In**.

#### Idle Timeout

By default, it is 300 seconds. If the profile connection is idle over the threshold of the timer, the router will drop the connection.

Please refer to Figure 12-5.



1. Common Settings

Profile Name: 3300V

Enable this profile

Call Direction:  Both  Dial-Out  Dial-In

Always on

Idle Timeout: 300 second(s)

Enable PING to keep alive

PING to the IP: \_\_\_\_\_

Figure 2-24. Common settings in Vigor 2900V

## Dial-Out Settings

It deals with relevant settings of Dial-Out connection. In this example, we do not need to configure this part.

**2. Dial-Out Settings**

**Type of Server I am calling**

ISDN  
 PPTP  
 IPSec Tunnel  
 L2TP with IPsec Policy None

Dial Number for ISDN or Server IP/Host Name for VPN.  
(such as 5551234, draytek.com or 123.45.67.89)

Link Type 64k bps

Username ???

Password

PPP Authentication PAP/CHAP

VJ Compression  On  Off

IKE Pre-Shared Key

**IPsec Security Method**

Medium(AH)  
 High(ESP) DES without Authentication

Advance

Scheduler (1-15)

**Callback Function (CBCP)**

Require Remote to Callback  
 Provide ISDN Number to Remote

Figure 2-25. Dial-Out settings in Vigor 2900V

## Dial-In Settings

It deals with relevant settings of Dial-In connection, including encryption method, preshared key and the WAN IP of remote site.

Select **IPSec Tunnel** and enter the WAN IP **220.135.240.207** of Vigor 2900V. Press the IKE Pre-Shared Key button, and then a window will pop up. Type **3300** (It must be identical with 3300V's). Press the “Confirm” button to finish the configuration of IKE Pre-Shared Key. Please refer to Figure 12-7.

**3. Dial-In Settings**

**Allowed Dial-In Type**

ISDN  
 PPTP  
 IPSec Tunnel  
 L2TP with IPsec Policy None

Specify ISDN CLID or Remote VPN Gateway

Peer ISDN Number or Peer VPN Server IP  
220.135.240.207  
or Peer ID

Username ???

Password

VJ Compression  On  Off

IKE Pre-Shared Key

**IPsec Security Method**

Medium (AH)  
 High (ESP)  
 DES  3DES  AES

**Callback Function (CBCP)**

Enable Callback Function  
 Use the Following Number to Callback  
Callback Number   
Callback Budget 0 minute(s)

Figure 2-26. Dial-In settings in Vigor 2900V

## TCP/IP Network Settings

It deals with the internal network of the remote site, etc.

In the **Network IP** and **Mask** fields, enter **192.168.33.0** and **255.255.255.0** respectively, and then press “OK” to finish the configuration. Please refer to Figure 2-27.

4. TCP/IP Network Settings

My WAN IP: 0.0.0.0

Remote Gateway IP: 0.0.0.0

Remote Network IP: 192.168.33.0

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

Change default route to this VPN tunnel:

More

OK

Figure 2-27. VPN setup- TCP/IP network settings

## Step 5

After configuration, the router will automatically switch to the LAN-to-LAN Profiles Setup page. Confirm if the settings are correct. Now the configuration of Vigor 2900V is completed. Please refer to Figure 2-28.

LAN-to-LAN Profiles:

Index	Name	Status	Index	Name	Status
1.	3300V	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

<< 1-16 | 17-32 >>

Figure 2-28. Table of LAN-to-LAN settings in Vigor 2900V

### 2.2.2.2 Configurations in Vigor 3300V

There are some procedures as below.

#### Step1

Suppose the internal network inside Vigor 3300V is 192.168.33.X, for detailed setup instructions please refer to the **LAN Setup** chapter. Enter **VPN IPSec Policy Table**, and click 1. Then press “Edit”. Please refer to Figure 2-29.

#	Connection Name	Local Subnet	Remote Gateway	Remote Subnet	Admin Status	Operational Status	Action
1							<input checked="" type="radio"/> Edit
2							<input type="radio"/>
3							<input type="radio"/>
4							<input type="radio"/>
5							<input type="radio"/>
6							<input type="radio"/>
7							<input type="radio"/>
8							<input type="radio"/>
9							<input type="radio"/>
10							<input type="radio"/>

Refresh Edit Delete Delete All

Figure 2-29. IPSec policy table

#### Step 2

First you should configure the **Default** page. In Basic settings, there are three parts users need to configure.

#### Basic

It deals with basic settings, including profile name, authentication type, preshared key, etc.

#### *Name*

You can specify a name to this profile. To facilitate easy management and differentiation, please type **2900V**.

#### *Preshared Key*

Type **3300** (It must be identical with 2900V's).

#### *Admin Status*

Use the default settings (**Enable**).

#### **Local Gateway**

It deals with relevant settings of the local router, including selection of the WAN and internal network, etc.

### ***WAN Interface***

Vigor 3300V has 4 WAN ports. In this example, we choose **WAN1** to establish the VPN tunnel.

### ***Network IP / Subnet Mask***

It is the internal network of Vigor 3300V. Please enter **192.168.33.0 /24** (/24 = Mask 255.255.255.0)

### **Remote Gateway**

It deals with relevant settings of the remote router, including WAN IP and internal network, etc.

### ***Security Gateway***

The WAN IP of Vigor 2900V. Please enter **61.31.167.135**.

### ***Network IP / Subnet Mask***

The internal network of Vigor 2900V. Please enter **192.168.29.0 /24** (/24 = Mask 255.255.255.0).

The screenshot shows the 'VPN - IPsec Tunnel' configuration interface. It has two tabs: 'Default' (selected) and 'Advanced'. The configuration is organized into three main sections:

- Basic:** Name: 2900V; Authentication: Pre-shared Key; Pre-shared Key: \*\*\*\*; Security Protocol: ESP; Admin Status: Enable.
- Local Gateway:** WAN Interface: WAN1; Local Certificate: (empty); Security Gateway: default; Network IP / Subnet Mask: 192.168.33.0 /24; Next Hop: default.
- Remote Gateway:** Remote ID: (empty); DHCP-over-IPsec: OFF; Security Gateway: 61.31.167.135 (with a note '(0.0.0.0 for dynamic client)'); Network IP / Subnet Mask: 192.168.29.0 /24 (with a note '(0.0.0.0 for dynamic client)').

Buttons for 'Apply' and 'Cancel' are located at the bottom right of the form.

Figure 2-29. Default page setup

### Step 3

#### Advanced page

By default, Vigor 3300V allows des-md5, des-sha1, 3des-md5 and 3des-sha1. Change the sequence of des-md5 and des-sha1 so that des-sha1 is in first place. Press “Apply” to finish the configuration.

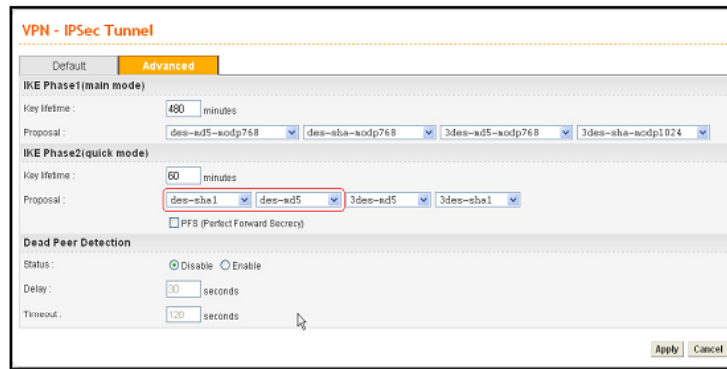


Figure 2-30. Advanced page setup

### Step 4

After configuration, the router will switch to the **VPN - IPsec - Policy Table** page. Click “Initiate”.

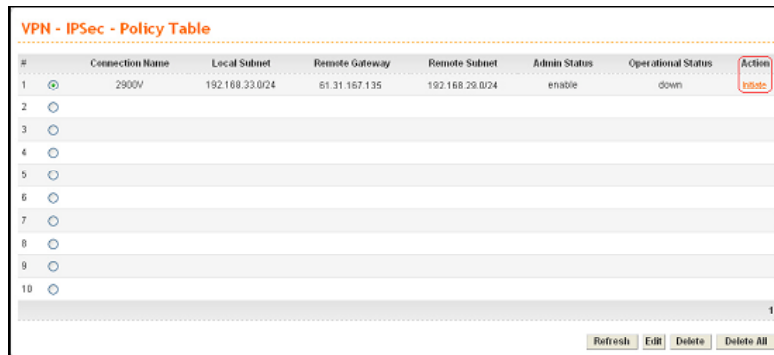


Figure 12-31. IPsec policy table

### Step 5

A window for this Dial-Out connection will pop up. Press “OK” to initiate this tunnel.

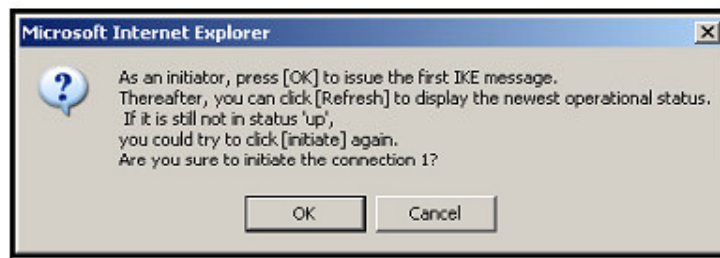
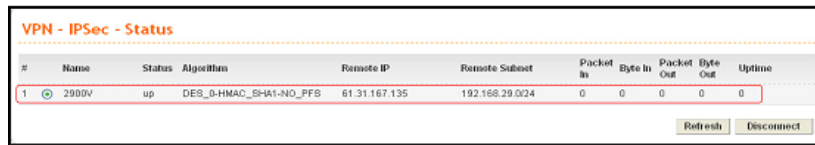


Figure 2-32. The confirmation window



### Step 6

Please wait for 30~60 seconds, and then enter the **VPN - IPSec – Status** page of Vigor 3300V. You will find that this VPN tunnel has been established.

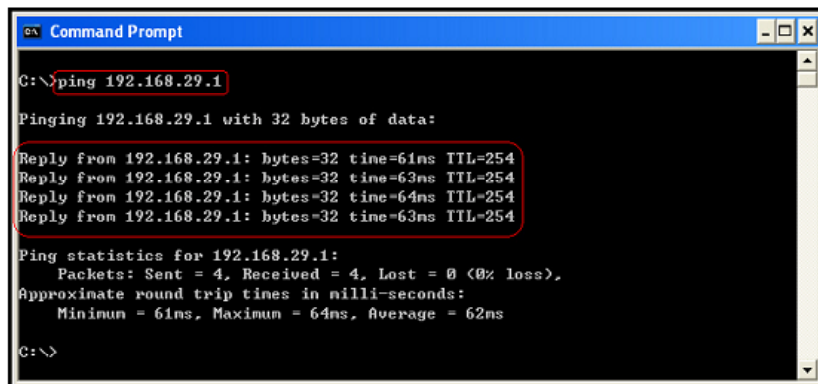


#	Name	Status	Algorithm	Remote IP	Remote Subnet	Packet In	Byte In	Packet Out	Byte Out	Uptime
1	2900V	up	DES_0-HMAC_SHA1-NO_PFS	61.31.167.135	192.168.29.0/24	0	0	0	0	0

Figure 2-33. VPN - IPSec - Status page

### Step 7

Please enter the CLI and **ping 192.168.29.1(2900V)** to see if there is any response.



```
C:\>ping 192.168.29.1

Pinging 192.168.29.1 with 32 bytes of data:
Reply from 192.168.29.1: bytes=32 time=61ms TTL=254
Reply from 192.168.29.1: bytes=32 time=63ms TTL=254
Reply from 192.168.29.1: bytes=32 time=64ms TTL=254
Reply from 192.168.29.1: bytes=32 time=63ms TTL=254

Ping statistics for 192.168.29.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 61ms, Maximum = 64ms, Average = 62ms

C:\>
```

Figure 2-34. Command prompt

### Step 8

If the numbers of Packet In & Packet Out increase, it means there is traffic through the VPN tunnel.

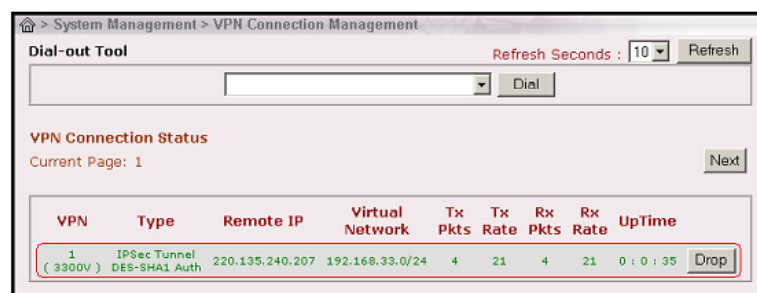


#	Name	Status	Algorithm	Remote IP	Remote Subnet	Packet In	Byte In	Packet Out	Byte Out	Uptime
1	2900V	up	DES_0-HMAC_SHA1-NO_PFS	61.31.167.135	192.168.29.0/24	3	240	3	240	25

Figure 2-35. The numbers of packet in & packet out

### Step 9

Please enter the main page of Vigor 2900V and click “**VPN Connection Management**”. And then you will find this VPN tunnel has been established.

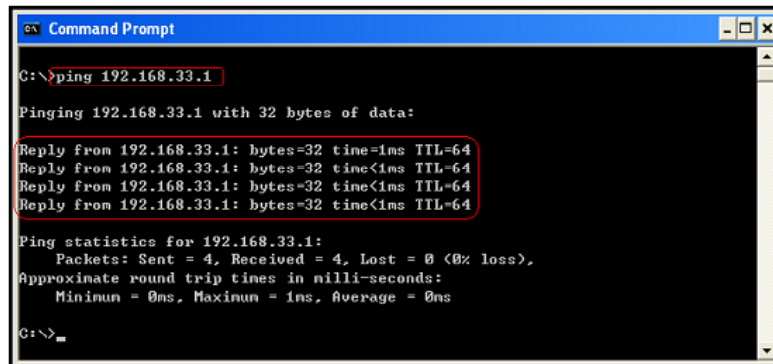


VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime
1 (3300V)	IPSec Tunnel DES-SHA1 Auth	220.135.240.207	192.168.33.0/24	4	21	4	21	0 : 0 : 35

Figure 2-36. VPN connection management

## Step 10

Enter the CLI and ping 192.168.33.1(3300V) to see if there is any response.



```
Command Prompt
C:\>ping 192.168.33.1
Pinging 192.168.33.1 with 32 bytes of data:
Reply from 192.168.33.1: bytes=32 time=1ms TTL=64
Reply from 192.168.33.1: bytes=32 time<1ms TTL=64
Reply from 192.168.33.1: bytes=32 time<1ms TTL=64
Reply from 192.168.33.1: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.33.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
```

Figure 2-37. Command prompt

## Step 11

If the numbers of Tx Pkts & Rx Pkts increase, it means there is traffic through the VPN tunnel.



VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime
1	IPSec Tunnel (3300V)	220.135.240.207	192.168.33.0/24	8	15	8	15	0 : 2 : 25

Figure 2-38. The numbers of Tx Pkts & Rx Pkts

Now the VPN tunnel has been successfully established.

If you want to keep a permanent connection, please refer to the step 2 the configuration of Vigor 3300V and change “Admin Status” from Enable to **Always-On**. Before the connection is established Vigor 3300V will continuously attempt to initiate VPN tunnel every 20 seconds.



**Basic**

Name : 2900V

Authentication : Preshared Key

Preshared Key : ●●●●

Security Protocol : ESP

Admin Status : **Always-On**

Figure 2-39. The admin status

## 2.3. VPN Three Parts Communication

### 2.3.1 Introduction

The second example is to configure 2 LAN to LAN VPN Tunnels. So that all three routers' internal networks can connect to each other through one of the router. In this example, since only one site (Vigor 3300V) has a fixed IP address, to maintain stable connections the other two routers (Vigor 2900V and Vigor 2200V) using dynamic IP addresses must enable "Always On". Vigor 3300V is set as the central site accepting incoming VPN connections from the other two routers. The VPN traffic between Vigor 2900V and Vigor 2200V are all passed through the Vigor 3300V. These 3 sites' internal networks must be within the same subnet (192.168.X.X). The subnet of the VPN's configuration of Vigor 3300V must fall into 192.168.0.0/16.

Suppose the headquarters in Taipei uses Vigor 3300V, while the branch office in Shanghai uses a Vigor 2900V. The teleworkers in Beijing use a Vigor 2200V. The network administrator requires 3 sites to communicate with each other through the encrypted VPN tunnel. The purpose is to avoid leakage of confidential information.

Since only the headquarters have confidential fixed IP address, teleworkers have to access the resources in the branch office through the headquarters. All the VPN traffic from Vigor 2900V and Vigor 2200V is firstly directed to the headquarters. To avoid overload of the lines, Vigor 3300V uses WAN1 to establish the VPN tunnel with the branch offices and uses WAN2 to establish the VPN tunnel with teleworkers.

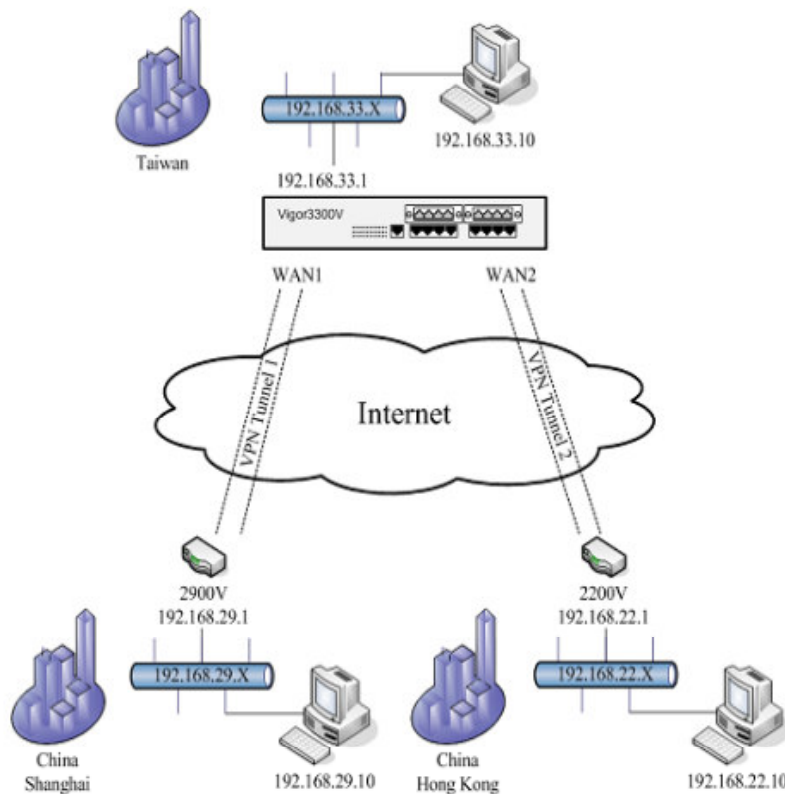


Figure 2-40. Setup 2 LAN to LAN VPN tunnels

	<b>3300V</b> Headquarters	<b>2900V</b> Branch Offices	<b>2200V</b> Teleworker
WAN IP	220.135.240.207 PPPoE, fixed IP	61.31.167.135 PPPoE, dynamic IP	
LAN IP	219.81.160.206 PPPoE, fixed IP 192.168.33.1	192.168.29.1	61.230.207.146 PPPoE, dynamic IP 192.168.22.1
Internal Network	192.168.33.X	192.168.29.X	192.168.22.X
Encryption Method	DES-SHA1		
Preshared Key	<b>3300</b>	<b>3300</b>	
	<b>1234</b>		<b>1234</b>

In this example since only Vigor 3300V has fixed IP address, to maintain a stable connection between Vigor 2900V and Vigor 2200V, you must enable “Always ON” in the VPN profiles of Vigor 2900V and Vigor 2200V.

## 2.3.2 Examples and Web Configurations

### 2.3.2.1 Configurations in Vigor 3300V

#### Step 1

Suppose the internal network of Vigor 3300V is 192.168.33.X, for detailed instructions please refer to the LAN Setup chapter. Enter VPN \IPSec\Policy Table, and click 1. Then press “Edit”.

#	Connection Name	Local Subnet	Remote Gateway	Remote Subnet	Admin Status	Operational Status	Action
1							<input checked="" type="radio"/>
2							<input type="radio"/>
3							<input type="radio"/>
4							<input type="radio"/>
5							<input type="radio"/>
6							<input type="radio"/>
7							<input type="radio"/>
8							<input type="radio"/>
9							<input type="radio"/>
10							<input type="radio"/>

Refresh Edit Delete Delete All

Figure 2-41. IPSec policy table

#### Step 2

First you should enter the **Default** page. There are three fields on this page.

## **Basic**

It deals with basic settings, including profile name, authentication type, preshared key, etc.

### *Name*

You can specify a name to this profile. To facilitate easy management and differentiation please type **2900V**.

### *Preshared Key*

Type **3300** (It must be identical with 2900V's).

### *Admin Status*

Use the default settings (**Enable**).

## **Local Gateway**

It deals with relevant settings of the local router, including selection of the WAN and internal network, etc.

### *WAN Interface*

Vigor 3300V has 4 WAN ports. In this example, we choose **WAN1** to establish the VPN tunnel.

### *Network IP / Subnet Mask*

The internal network of Vigor 2900V. Please enter **192.168.0.0 /16** (/16 = Mask 255.255.0.0).

## **Remote Gateway**

It deals with relevant settings of the remote router, including WAN IP and internal network, etc.

### *Security Gateway*

The WAN IP of Vigor 2900V. In this example it isn't fixed, so please enter 0.0.0.0.

### *Network IP / Subnet Mask*

The internal network of Vigor 2900V. Please enter **192.168.29.0 /24** (/24 = Mask 255.255.255.0).

Figure 2-42. VPN – IPsec tunnel - Default page setup

### Step 3

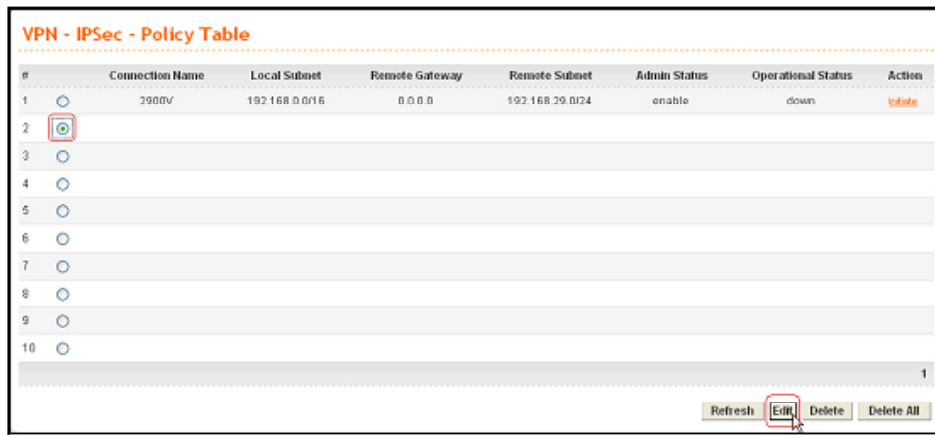
#### Advanced page

In this example since the connection is initiated by Vigor 2900V, the encryption method is determined by Vigor 2900V. By default Vigor 3300V allows des-md5, des-sha1, 3des-md5 and 3des-sha1, so no change is required. Just press the Apply button to finish the configuration.

Figure 2-43. VPN - IPsec tunnel - Advanced page setup

#### Step 4

After configuration, the router will automatically switch to the **VPN - IPSec - Policy Table** page. Click 2, and then press Edit.



#	Connection Name	Local Subnet	Remote Gateway	Remote Subnet	Admin Status	Operational Status	Action
1	2900V	192.168.0.0/16	0.0.0.0	192.168.29.0/24	enable	down	delete
2							
3							
4							
5							
6							
7							
8							
9							
10							

Refresh Edit Delete Delete All

Figure 2-44. VPN - IPSec - Policy table (edit 2)

#### Step 5

Firstly you should enter the **Default** page. There are three fields on this page.

##### Basic

It deals with basic settings, including profile name, authentication type, preshared key, etc.

##### Name

You can specify a name to this profile. To facilitate easy management and differentiation please type **2200V**.

##### Preshared Key

Type **1234** (It must be identical with 2200V's).

##### Admin Status

Use the default settings (**Enable**).

##### Local Gateway

It deals with relevant settings of the local router, including selection of the WAN and internal network, etc.

##### WAN Interface

Vigor 3300V has 4 WAN ports. In this example, we choose **WAN2** to establish the VPN tunnel.

### ***Network IP / Subnet Mask***

The internal network of Vigor 3300V. Please enter **192.168.0.0 /16** (/16 = Mask 255.255.0.0).

### **Remote Gateway**

It deals with relevant settings of the remote router, including WAN IP and internal network, etc.

### ***Security Gateway***

The WAN IP of Vigor 2900V. In this example it is not fixed, so please enter **0.0.0.0**.

### ***Network IP / Subnet Mask***

It is the internal network of Vigor 2900V. Please enter **192.168.22.0 /24** (/24 = Mask 255.255.255.0).

**VPN - IPSec Tunnel**

Default | Advanced

**Basic**

Name: 2200V

Authentication: Pre-shared Key

Pre-shared Key: \*\*\*\*

Security Protocol: ESP

Admin Status: Enable

**Local Gateway**

WAN Interface: WAN2

Local Certificate: [dropdown]

Security Gateway: default

Network IP / Subnet Mask: 192.168.0.0 /16

Next hop: default

**Remote Gateway**

Remote ID: [empty]

DHCP-over-IPSec: OFF

Security Gateway: 0.0.0.0 (0.0.0.0 for dynamic client)

Network IP / Subnet Mask: 192.168.22.0 /24 (0.0.0.0/32 for dynamic client)

Apply Cancel

Figure 2-45. VPN - IPSec tunnel - Default page setup



## Step 6

### Advanced page

In this example since the connection is initiated by Vigor 2200V, the encryption method is determined by Vigor 2200V. By default Vigor 3300V allows des-md5, des-sha1, 3des-md5 and 3des-sha1, so no change is required. Just press the Apply button to finish the configuration.

**VPN - IPsec Tunnel**

Default **Advanced**

**IKE Phase1(main mode)**

Key lifetime: 480 minutes

Proposal: des-md5-acdp768, des-sha-acdp768, 3des-md5-acdp768, 3des-sha-acdp1024

**IKE Phase2(quick mode)**

Key lifetime: 60 minutes

Proposal: des-md5, des-sha1, 3des-md5, 3des-sha1

PFS (Perfect Forward Secrecy)

**Dead Peer Detection**

Status:  Disable  Enable

Delay: 30 seconds

Timeout: 120 seconds

Apply Cancel

Figure 2-46. VPN - IPsec tunnel - Advanced page setup

## Step 7

After configuration, the router will switch to the **VPN - IPsec - Policy Table** page. Confirm if the settings are correct. Now the configuration of Vigor 3300V is completed.

**VPN - IPsec - Policy Table**

#	Connection Name	Local Subnet	Remote Gateway	Remote Subnet	Admin Status	Operational Status	Action
1	2900V	192.168.0.0/16	0.0.0.0	192.168.29.0/24	enable	down	Delete
2	2200V	192.168.0.0/16	0.0.0.0	192.168.22.0/24	enable	down	Delete
3							
4							
5							
6							
7							
8							
9							
10							

Refresh Edit Delete Delete All

Figure 2-47. The setup for 3300V is completed

## 2.3.2.2 Configurations in Vigor 2900V

### Step 1

Enter the web page of Vigor 2900V, and click the VPN and Remote Access Setup link.



Figure 2-48. 2900V web configuration

### Step 2

Click the LAN-to-LAN Profile Setup link. Please refer to Figure 13-10.

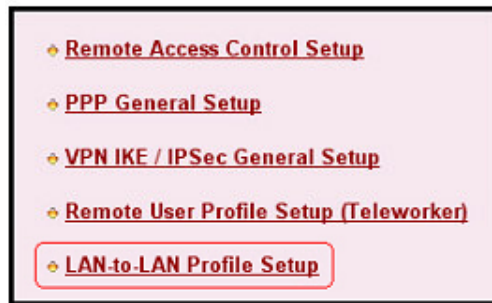


Figure 2-49. LAN-to-LAN profile setup

### Step 3

Click **Index 1**, and enter relevant settings of the VPN tunnel connected to Vigor 3300V.

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

<< **1.16** | **17.32** >>

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

Figure 2-50. Enter relevant VPN setup

### Step 4

On this page there are four sections regarding VPN configuration.

#### **Common Setting**

It deals with basic settings, including profile name, enable or disable the profile, call direction, etc.

#### **Profile Name**

You can specify a name to this profile. To facilitate easy management and differentiation, please type **3300V**.

#### **Call Direction**

You can specify the call direction to this profile. In this example the connection is initiated from Vigor 2900V to Vigor 3300V, so please select **Dial-Out**. In this example Vigor 3300V is not allowed to dial in.

#### **Idle Timeout**

By default, it is 300 seconds. If the profile connection is idle over the threshold of the timer, the router will drop the connection.

#### **Always On**

If the VPN connection is terminated, the router will continuously attempt to establish the VPN.

### ***PING to Keep Alive***

To avoid the situation in which the connection goes down unexpectedly, Vigor uses "Ping to keep alive" method to detect if the peer router is reachable. Enable this feature and enter "192.168.33.1" in the "PING to the IP" field.

1. Common Settings

Profile Name: 3300V

Enable this profile

Call Direction:  Both  Dial-Out  Dial-In

Always on

Idle Timeout: -1 second(s)

Enable PING to keep alive

PING to the IP: 192.168.33.1

Figure 2-51. VPN setup - Common settings

### **Dial-Out Setting**

It deals with relevant settings of Dial-Out connection, including encryption method, preshared key and WAN IP of the remote site.

Select **IPSec Tunnel** and enter the WAN IP **220.135.240.207** of Vigor 2900V. Press the IKE Pre-Shared Key button, and then a window will popup Type **3300** (It must be identical with 3300V's). Press the "Confirm" button to finish the configuration of IKE Pre-Shared Key. Then click **High (ESP)** and select **DES with Authentication** (default is DES without Authentication).

2. Dial-Out Settings

Type of Server I am calling

ISDN

PPTP

IPSec Tunnel

L2TP with IPsec Policy: None

Dial Number for ISDN or Server IP/Host Name for VPN.  
(such as 5551234, draytek.com or 123.45.67.89)

220.135.240.207

Link Type: 64k bps

Username: ???

Password:

PPP Authentication: PAP/CHAP

VJ Compression:  On  Off

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

IPsec Security Method

Medium(AH)

High(ESP) DES with Authentication

Advance

Scheduler (1-15)

Callback Function (CBCP)

Require Remote to Callback

Provide ISDN Number to Remote

Figure 2-52. VPN setup - Dial-out settings

## Dial-in Setting

It deals with relevant settings of Dial-In connection. In this example, there is no need to configure this part.

Figure 2-53. VPN setup - Dial-in settings

## TCP/IP Network Settings

The internal network of the remote site, etc.

In the **Network IP** and **Mask** fields, enter **192.168.0.0** and **255.255.0.0** respectively, and then press “OK” to finish the configuration.

Figure 2-54. VPN setup - TCP/IP network settings

## Step 5

After configuration, the router will automatically switch to the **LAN-to-LAN Profiles Setup** page. Confirm if the settings are correct. Now the configuration of Vigor 2900V is completed.

LAN-to-LAN Profiles:

Index	Name	Status	Index	Name	Status
1.	3300V	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

<< 1-16 | 17-32 >>

Figure 2-55. The setting status for Vigor 2900V is completed

### Step 6

Enter the main page of Vigor 2900V, click **VPN Connection Management**. Since “Always On” is enabled, the VPN connection has been established.

System Management > VPN Connection Management

Dial-out Tool Refresh Seconds : 10 Refresh

( 3300V ) 220.135.240.207 Dial

VPN Connection Status

Current Page: 1 Next

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime
1 ( 3300V )	IPSec Tunnel DES-SHA1 Auth	220.135.240.207	192.168.33.0/24	0	0	9	16	0 : 0 : 20

Drop

Figure 2-56. VPN connection management

### Step 7

Enter the CLI and try to **ping 192.168.33.1(3300V)** to see if there is any response.

```

C:\>ping 192.168.33.1
Pinging 192.168.33.1 with 32 bytes of data:
Reply from 192.168.33.1: bytes=32 time=1ms TTL=64
Reply from 192.168.33.1: bytes=32 time<1ms TTL=64
Reply from 192.168.33.1: bytes=32 time<1ms TTL=64
Reply from 192.168.33.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.33.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>_

```

Figure 2-57. Command prompt

## Step 8

If the numbers of Tx Pkts & Rx Pkts increase, it means there is traffic through the VPN tunnel.

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime
1 (3300V)	IPSec Tunnel DES-SHA1 Auth	220.135.240.207	192.168.33.0/24	4	3	44	19	0 : 1 : 20

Figure 2-58. The numbers of Tx Pkts & Rx Pkts

### 2.3.2.3 Configurations in Vigor 2200V

#### Step 1

Enter the web page of Vigor 2200V. Click the VPN and Remote Access link.

The screenshot shows the 'System Status' page of the Vigor 2200V/VG VPN VoIP Router. The page includes a navigation menu on the left and a main content area with the following information:

- System Status:**
  - Model Name: Vigor2200V series
  - Firmware Version: v2.5.5.4
  - Build Date/Time: Mon May 9 17:54:8.85 2005
- LAN:**
  - MAC Address: 00:60:7F:27:6C:47
  - IP Address: 192.168.22.1
  - Subnet Mask: 255.255.255.0
  - DHCP Server: Yes
- WAN:**
  - MAC Address: 00:60:7F:27:6C:48
  - Connection: PPPoE
  - IP Address: 61.230.207.146
  - Default Gateway: 61.230.192.254
  - DNS: 168.95.1.1
- VoIP:**
  - Channel: 1
  - SIP Registrar: lgitel.org
  - Account ID: 388822
  - Registrar: Yes
  - C Codec:
  - In Calls: 0
  - Out Calls: 0

Figure 2-59. Vigor 2200V web configuration

#### Step 2

Click the **LAN-to-LAN Profiles** link. Click **Index 1** and enter relevant settings of the VPN tunnel of Vigor 3300V.

The screenshot shows the 'LAN-to-LAN Profile Setup' page in the Vigor 2200V/VG web configuration. It displays a table of LAN-to-LAN Profiles with the following data:

Index	Name	Status	Index	Name	Status
1	???	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

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

Figure 2-60. LAN-to-LAN profiles setup

### Step 3

On this page there are four sections regarding VPN configuration.

#### Common Setting

It deals with basic settings, including profile name, enable or disable the profile, call direction, etc.

#### Profile Name

You can specify a name to this profile. To facilitate easy management and differentiation, please type **3300V**.

#### Call Direction

Specify the call direction to this profile. In this example the connection is initiated from Vigor 2200V to Vigor 3300V, so please select **Dial-Out**. In this example Vigor 3300V is not allowed to dial in.

#### Always On

If the VPN connection is terminated, the router will continuously attempt to establish the VPN.

#### PING to Keep Alive

To avoid the situation in which the connection goes down unexpectedly, Vigor uses "Ping to keep alive" method to detect if the peer router is reachable. Enable this feature and enter "192.168.33.1" in the "PING to the IP" field.

1. Common Settings

Profile Name: 3300V

Enable this profile

Call Direction:  Both  Dial-Out  Dial-In

Always on

Idle Timeout: -1 second(s)

Enable PING to keep alive

PING to the IP: 192.168.33.1

Figure 2-61. VPN setup - Common settings



## Dial-Out Setting

It deals with relevant settings of Dial-Out connection, including encryption method, preshared key and the WAN IP of remote site.

Select **IPSec Tunnel** and enter the WAN IP **219.81.160.206** of Vigor 2900V. Press IKE Pre-Shared Key button and a window will pop-up, type **1234** (It must be identical with 3300V's). Press Confirm to finish the configuration of IKE Pre-Shared Key. Then click **High (ESP)** and select **DES with Authentication** (default is DES without Authentication ).

**2. Dial-Out Settings**

**Type of Server I am calling**

- ISDN
- PPTP
- IPSec Tunnel**
- L2TP with IPsec Policy **None**

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

Link Type

Username  Password

PPP Authentication  VJ Compression  On  Off

**IKE Pre-Shared Key**

**IPSec Security Method**

- Medium(AH)
- High(ESP)**

**Advance**

Scheduler (1-15)

,  ,  ,

**Callback Function (CBCP)**

- Require Remote to Callback
- Provide ISDN Number to Remote

Figure 2-62. VPN setup - Dial-out settings

## Dial-in Setting

It deals with relevant settings of Dial-In connection. In this example, there is no need to configure this part.

**3. Dial-In Settings**

**Allowed Dial-In Type**

- ISDN
- PPTP
- IPSec Tunnel**
- L2TP with IPsec Policy **None**
- Specify Remote VPN Gateway

Peer VPN Server IP

or Peer ID

Username  Password

VJ Compression  On  Off

**IKE Pre-Shared Key**

**IPSec Security Method**

- Medium (AH)**
- High (ESP)
  - DES  3DES  AES

**Callback Function (CBCP)**

- Enable Callback Function
- Use the Following Number to Callback
  - Callback Number
  - Callback Budget  minute(s)

Figure 2-63. VPN setup - Dial-In settings

## TCP/IP Network Settings

The internal network of the remote site, etc.

In the **Network IP** and **Mask** fields, enter **192.168.0.0** and **255.255.0.0** respectively, and then press “OK” to finish the configuration.

4. TCP/IP Network Settings

My WAN IP	0.0.0.0	RIP Direction	TX/FX Both
Remote Gateway IP	0.0.0.0	RIP Version	Ver. 2
Remote Network IP	192.168.0.0	For NAT operation, treat remote sub-net as	Private IP
Remote Network Mask	255.255.0.0		

More

Change default route to this VPN tunnel

OK Clear Cancel

Figure 2-64. VPN setup - TCP/IP network settings

## Step 4

After configuration, the router will automatically switch to the **LAN-to-LAN Profiles Setup** page. Confirm if the settings are correct. Now the configuration of Vigor 2200V is completed.

Vigor2200V/VG  
VPN VoIP Router

VPN and Remote Access >> LAN-to-LAN Profile Setup

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

Index	Name	Status	Index	Name	Status
1.	3300V	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

Status: Ready

Figure 2-65. The setting status for Vigor 2200V is completed

## Step 5

Enter the main page of Vigor 2200V, click **VPN Connection Management**. Since “Always On” is enabled, the VPN connection has been established.



Figure 2-66. VPN connection management

## Step 6

You may attempt to **ping 192.168.33.1**( Vigor 3300V) and **ping 192.168.29.1**( Vigor 2900V) to see if there is any response.

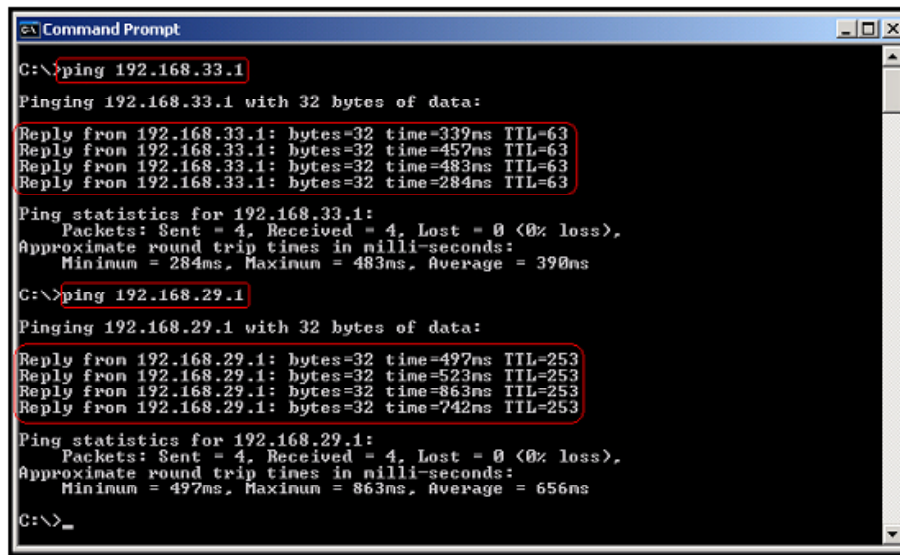
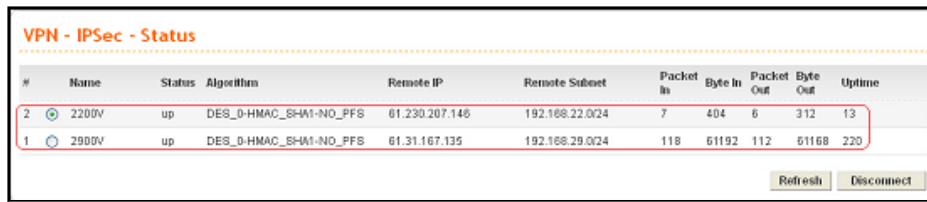


Figure 2-67. Command prompt

### Step 7

Enter the web page of Vigor 3300V and enter **VPN\IPSec\Status**, you will see two VPN tunnels have been established.



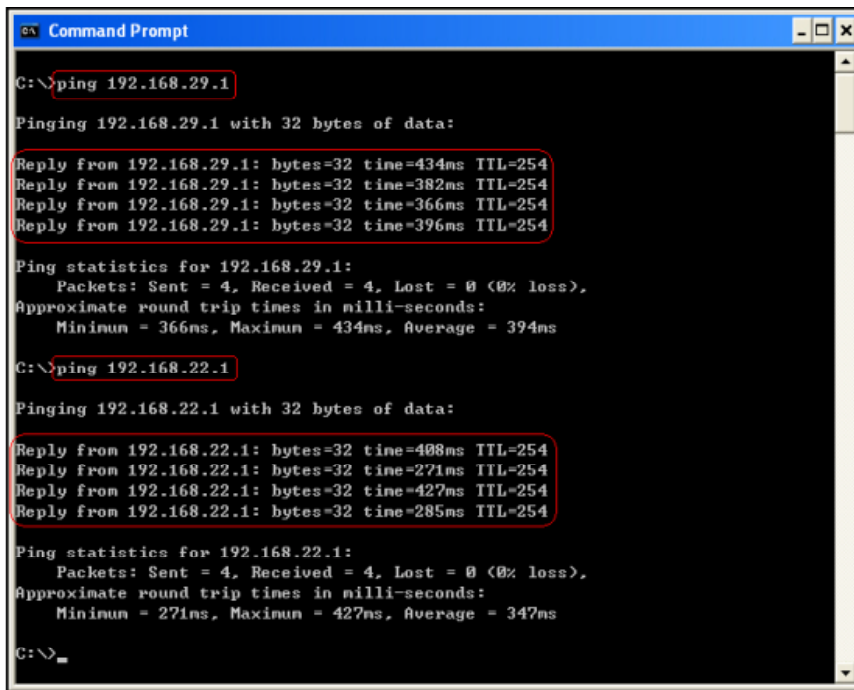
#	Name	Status	Algorithm	Remote IP	Remote Subnet	Packet In	Byte In	Packet Out	Byte Out	Uptime
2	2200V	up	DES_D-HMAC_SHA1-NO_PFS	61.230.207.146	192.168.22.0/24	7	404	6	312	13
1	2900V	up	DES_D-HMAC_SHA1-NO_PFS	61.31.167.135	192.168.29.0/24	118	61192	112	61168	220

Refresh Disconnect

Figure 2-68. VPN - IPSec – Status

### Step 8

Enter the CLI and attempt to **ping 192.168.29.1** ( Vigor 2900V) and **ping 192.168.22.1**( Vigor 2200V) to see there is any response.



```
Command Prompt
C:\>ping 192.168.29.1
Pinging 192.168.29.1 with 32 bytes of data:
Reply from 192.168.29.1: bytes=32 time=434ms TTL=254
Reply from 192.168.29.1: bytes=32 time=382ms TTL=254
Reply from 192.168.29.1: bytes=32 time=366ms TTL=254
Reply from 192.168.29.1: bytes=32 time=396ms TTL=254
Ping statistics for 192.168.29.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 366ms, Maximum = 434ms, Average = 394ms
C:\>ping 192.168.22.1
Pinging 192.168.22.1 with 32 bytes of data:
Reply from 192.168.22.1: bytes=32 time=408ms TTL=254
Reply from 192.168.22.1: bytes=32 time=271ms TTL=254
Reply from 192.168.22.1: bytes=32 time=427ms TTL=254
Reply from 192.168.22.1: bytes=32 time=285ms TTL=254
Ping statistics for 192.168.22.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 271ms, Maximum = 427ms, Average = 347ms
C:\>
```

Figure 2-69. Command prompt

Now all these 3 sites can connect to each other.

### Note

*Please note all the VPN traffic will be passed through the 3300V. If there is much data flow between Vigor 2200V and Vigor 2900V, the bandwidth of Vigor 3300V, especially the upstream one will be heavily consumed accordingly.*

## 2.4 IPSec Host-to-LAN (Smart VPN Client) --- DHCP over IPSec

### 2.4.1 Introduce

Vigor 3300 series router supports two kinds of VPN type – PPTP & IPSec.

It supports only Host-to-LAN and a maximum of 16 tunnels in all for PPTP connection; while it supports both Host-to-LAN & LAN-to-LAN VPN, and a maximum of 200 tunnels for IPSec.

Hence, when deploying a large-scale network, the IPSec tunnel is recommended.

However, there is a limitation for IPSec tunnel:

For traditional IPSec VPN, the dial-in side cannot obtain a private IP address from the peer side, which is different from PPTP VPN (for PPTP, there will be a PPP virtual interface for the remote dial-in side.). So there is only a one-way access for the tunnel – “dial-in side→central server side”, while the backward is not available.

Nevertheless, we DrayTek have built a unique technique – “DHCP over IPSec” to overcome such limitation.

To implement this feature, we’ll add a virtual NIC on the PC, thus, while connecting to the server via IPSec tunnel, PC will obtain an IP address from the remote side through DHCP protocol, which is quite similar with PPTP.

The following document describes the detailed configuration steps for this application.

### 2.4.2 Configuration on Server

Which is different to the Vigor2x00 series router, Vigor 3300 does not distinguish the Remote Teleworker and LAN-to-LAN Setup. That is, the settings in policy table operates on both Host-to-LAN & LAN-to-LAN tunnel.

*Note:*

- Vigor 3300 does not require the remote dial-in user should own a fixed IP, a dynamic IP address can also be OK.
- The remote dial-in user can be directly on the Internet (public IP), but also can be behind the NAT.
- However, if the user is behind the NAT, that NAT router should support IPSec VPN pass-through.
- If the remote user is behind the NAT, then other hosts within the same subnet cannot connect to the VPN server. That is, only one host can dial IPSec to the VPN server at the same time if behind the NAT.

1. In **VPN - IPSec - Policy Table** page, select certain index and press **Edit**

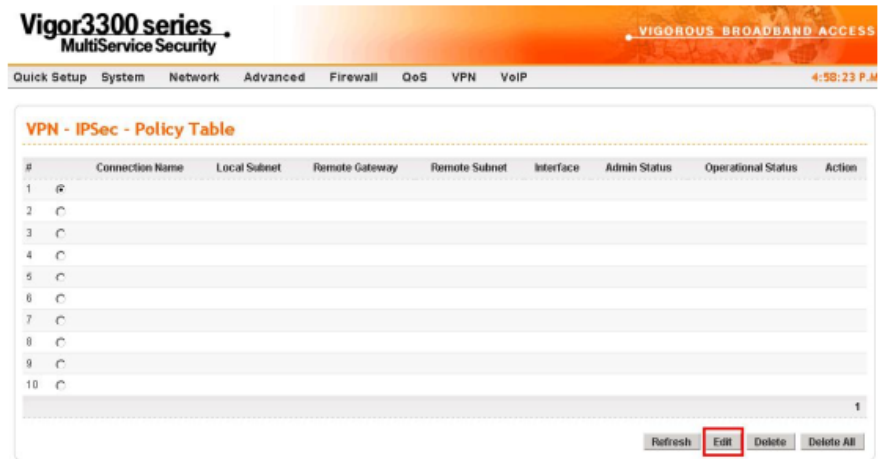


Figure 2-70

2. In the following page, configure as the picture below:

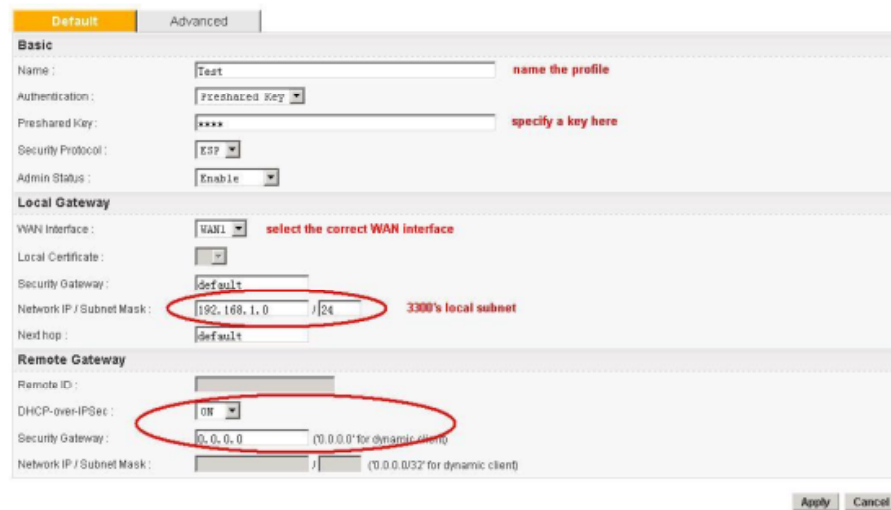


Figure 2-71

Please enable the **DHCP over IPSec**, you'll see **Network IP / Subnet Mask** field is grayed.

Besides, if the dial-in user has a fixed IP, then enter the IP in the **Security Gateway** field. But if the remote user just owns a dynamic IP, then type 0.0.0.0 there.

- In the Advance page, you may make some detailed settings for the two IKE phases.

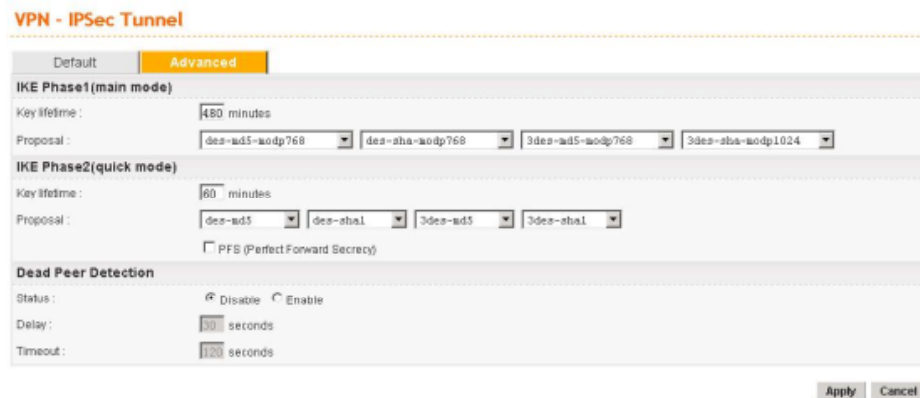


Figure 2-72

**Note:**

- Since 3300 series router has multiple WAN interface, if the security gateway was set as 0.0.0.0, then each WAN interface can only owns one Pre-Shared Key. In other words, suppose you've set 3 policies which all uses WAN1 as WAN interface, and 0.0.0.0 as security gateway, then only the Pre-Shared Key of the last policy will be regarded as valid and can be used for WAN1's IPsec tunnel.
- In above scenario, if the security gateway of 3 policies was configured as certain fixed IP addresses, then you may set a different Pre-Shared Key for each policy, while there will be no conflict among them.

### 2.4.3 Configuration on Smart VPN Client

- Download the Smart VPN Client from our website <http://www.draytek.com/support/download.php> and install it. During the installation, a virtual NIC can be installed on your PC. If you want to use DHCP over IPsec feature, you MUST install it.

**LAN or High-Speed Internet**

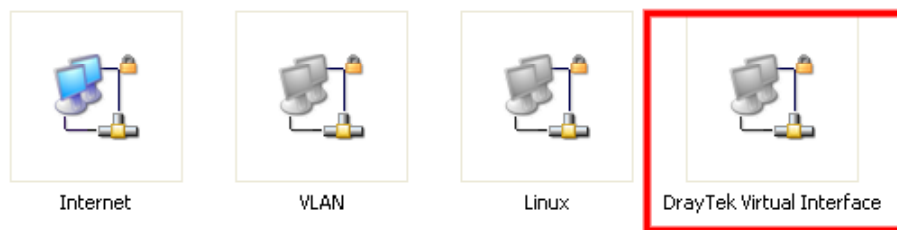


Figure 2-73

2. Run the **Start → All Programs → Draytek Smart VPN Client → Smart VPN Client**, and press **Insert** button.

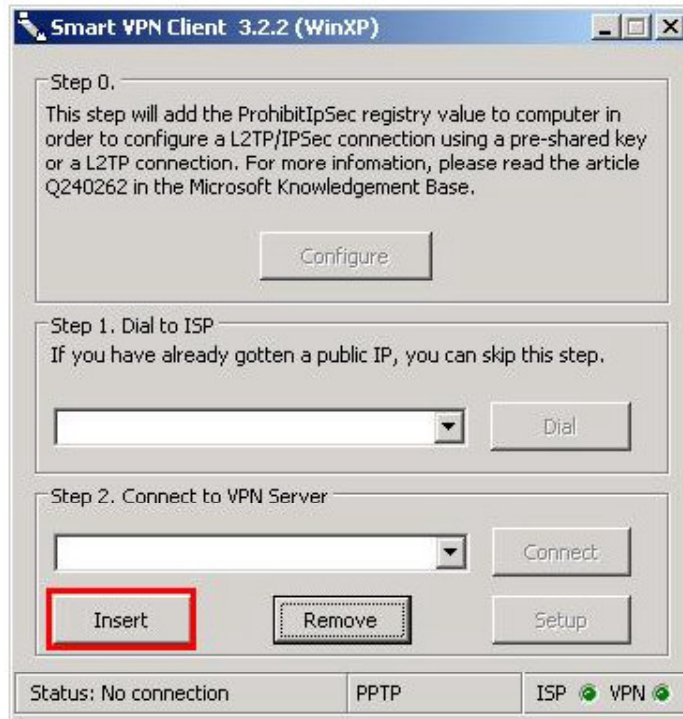


Figure 2-74

3. Then a new VPN profile will be created. Please enter the 3300's WAN IP (be sure to select the correct WAN interface), and tick the **IPSec Tunnel** box, then press **OK**.



Figure 2-75



- In the coming up configuration page, tick the **Virtual IP** box. You may **Obtain an IP address automatically** or **Specify an IP address** as your wish. As for the security settings (including Security Method and Pre-Shared Key etc.), you **MUST** make sure they are exactly the same with the server sides.

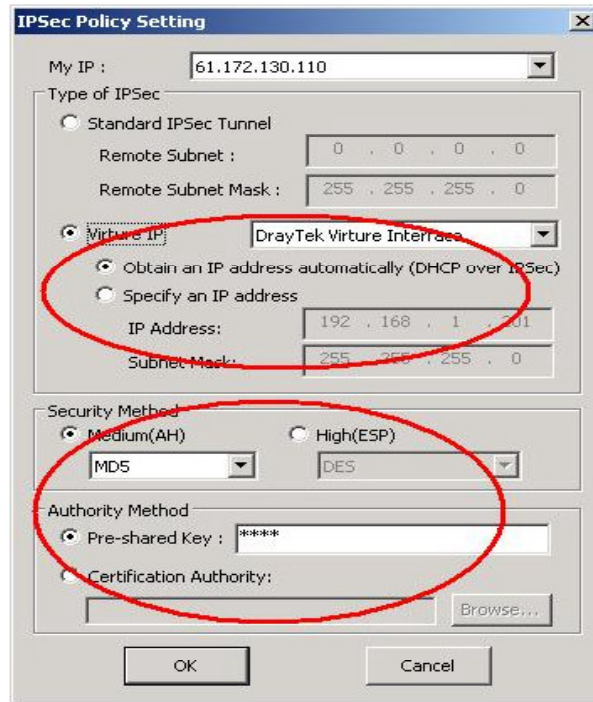


Figure 2-76

*Note: If you're running multiple NICs on the PC, please be sure to select the correct one for **My IP** field.*

- Press OK, after you finish the configuration. And then activate the IPsec tunnel.



Figure 2-77

6.

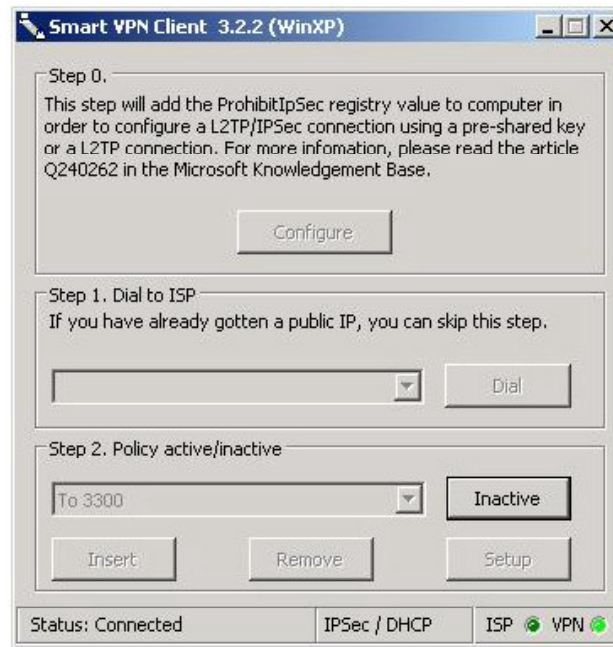


Figure 2-78

7. You may try pinging the remote private IP so as to check if the connection is up.

```
C:\Documents and Settings\Caesar>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Documents and Settings\Caesar>_
```

Figure 2-79

## 2.5 VPN PPTP Host-to-LAN by Smart VPN Client

### 2.5.1 Introduction

This document describes how to establish a PPTP tunnel from the Smart VPN Client to Vigor 3300 series router.

Suppose the network environment is as below:

	Vigor 3300V Headquarters	Smart VPN Client
WAN IP	218.242.130.19 (Static IP)	58.33.150.31 (Dynamic IP)
LAN IP	192.168.1.1	/
Local Network	192.168.1.*/28	/

### 2.5.2 Configuration

#### 2.5.2.1 Server Side

##### Step 1

Enter **VPN - PPTP - General Setup**, activate the setup, and select corresponding Authentication and Encryption settings for PPTP. The **User Authentication** should use the default value “Local”.

The screenshot displays the web management interface for a Vigor3300 series router. The page title is "Vigor3300 series MultiService Security". The navigation menu includes "Quick Setup", "System", "Network", "Advanced", "Firewall", "QoS", "VPN", and "VoIP". The current page is "VPN - PPTP - General Setup".

The configuration options are as follows:

- Status:  Active  Inactive
- PPTP Authentication: MS-CHAP
- PPTP Encryption: MPPE 40 bits
- User Authentication:  Local  RADIUS Server
- Mutual Authentication:  Enable  Disable
- User Name: [Text Input Field]
- Password: [Text Input Field]

Buttons for "Apply" and "Cancel" are located at the bottom right of the configuration area.

Figure 2-80. PPTP general setup

## Step 2

Enter **VPN - PPTP - Group Table**. And you can specify the IP range that be allocated to the remote hosts (**Star IP**), and the local IP range which is accessible to the remote hosts (**Accessed IP**).

There're 4 groups of IP range in the Group Table as following Figure 2-81.

Group	Start IP	Subnet Mask	Accessed IP	Subnet Mask
A	192.168.1.224	/28	192.168.1.16	/28
B		/24		/24
C		/24		/24
D		/24		/24

Figure 2-81. PPTP group table

### Note:

*If you leave the Accessed IP field empty, then the whole local subnet is fully accessible to the remote dial-in user.*

*And the Start IP field MUST be configured; Otherwise, the tunnel will not be established.*

## Step 3

Go to **VPN - PPTP – Authentication**, and select a related entry, then click **Edit** to modify the entry.

#	User Name	Group
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Figure 2-82. PPTP authentication

#### Step 4

In the following page, please type in the **User Name & User Password**, and select a group.

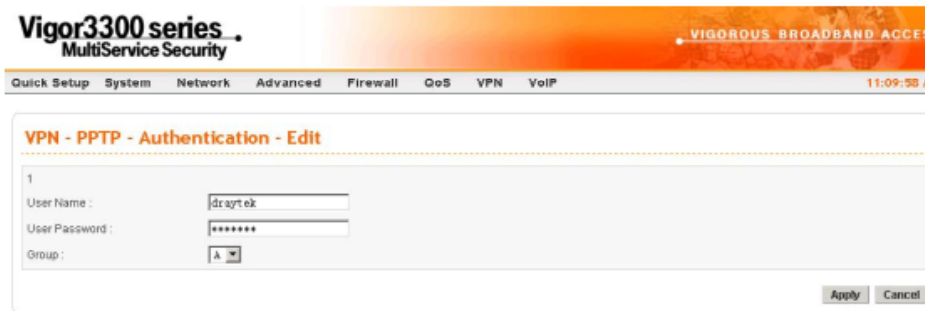


Figure 2-83. PPTP authentication – Edit

#### Step 5

After the tunnel is created, you can check the tunnel status on **VPN - PPTP – Status** as below Figure 2-84.



Figure 2-84. PPTP status

### 2.5.2.2 Client Side

#### Step 1

Download the latest Smart VPN Client from our web site - <http://www.draytek.com/support/download.php>, and install it.

#### Step 2

Go to Start \ All Programs \ DrayTek Smart VPN, and click the **Smart VPN Client**.

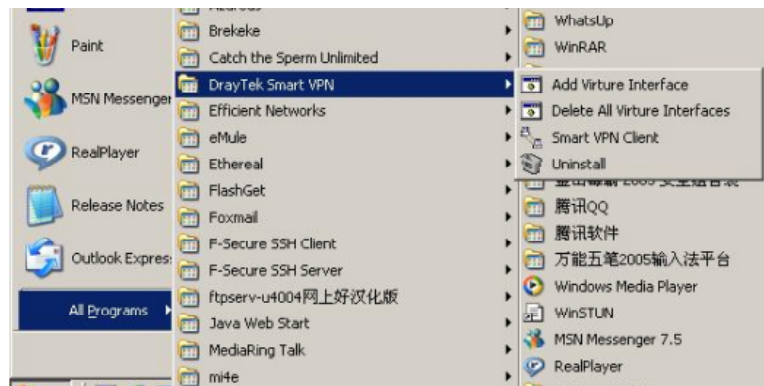


Figure 2-85. The location of Smart VPN Client

### Step 3

Press click **Insert** to create a new VPN profile.

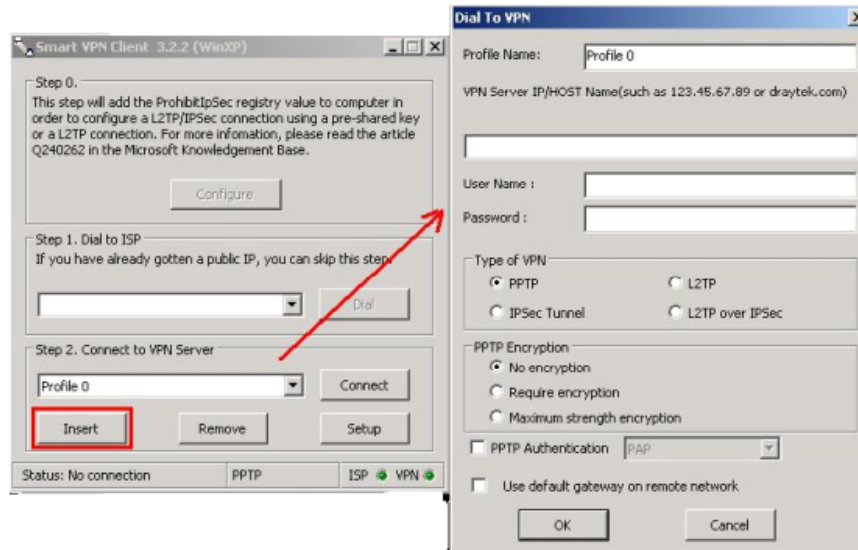


Figure 2-85. Create a new VPN profile

### Step 4

Specify a name for this profile (surely you may leave this option as default), type 218.242.130.19 (WAN interface IP address in 3300) in the VPN server IP field, enter the username/password, and select PPTP in the Type of VPN. Please be sure to enter the identical Authentication and Encryption settings that you set in Vigor 3300. And you do not have to click “**Use default gateway on remote network**”, unless you want all the traffic to be routed via the remote network.



Figure 2-86. Dial to VPN

## Step 5

Click **OK** then click **Connect** to the Vigor 3300.

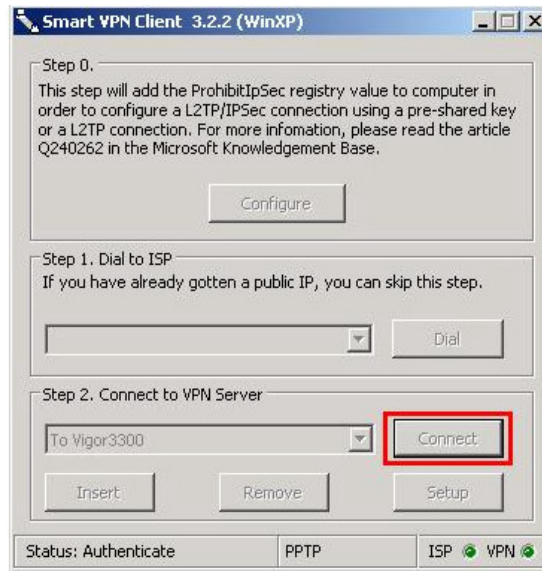


Figure 2-87. Connect to VPN server

## Step 6

After the tunnel is established, you may see the status is “**Connected**”.

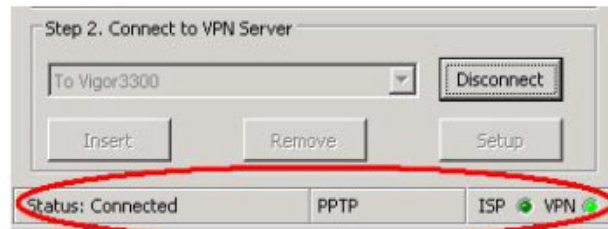


Figure 2-88. Check the tunnel status

Also you may try to ping the remote private network, to check whether the VPN PPTP tunnel is created or not.

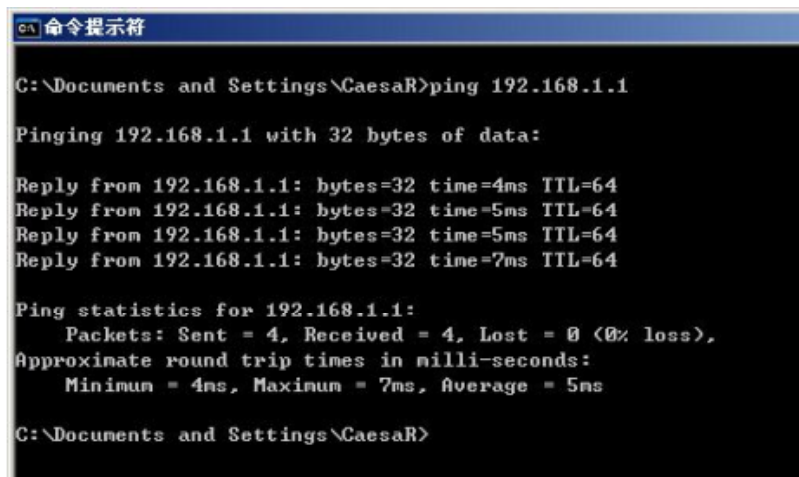


Figure 2-89. Ping status

## 29. VoIP Example 1 (Basic Configuration and Registration)

This chapter shows how to set up a practical example to use VoIP function.

This chapter is divided into the following sections.

Section 29.1: Basic Configuration and Registration

Section 29.2: 3300V Configuration Example

Section 29.3: 2900V Configuration Example

There are many different kinds of applications about VoIP function, most of VoIP callings must be via a VoIP Server by registering, except we can dial VoIP number by the IP address directly. We will set up a basic configuration and registration as an example 1. The other examples might be revised based on this example.

The VoIP function mainly depends on the requirement and application. All the examples are based on example 1 to revise configuration in accordance with the usage requirement and application.

### **Example 1**

Basic Configuration and Registration

### **Example 2**

Basic Dialing Mode

### **Example 3**

VoIP over VPN

### **Example 4**

Practical Application of FXS

### **Example 5**

Practical Application of FXO

### **Example 6**

Register with Private IP Address



## Chapter 3. VoIP Function

This chapter is divided into the following sections,

Section 3.1: VoIP Example 1 - Basic Configuration and Registration

Section 3.2: VoIP Example 2 - Basic Calling Method

Section 3.3: VoIP Example 3 - VoIP over VPN

Section 3.4: VoIP Example 4 - Practical Application of FXS

Section 3.5: VoIP Example 5 - Practical Application of FXO

Section 3.6: VoIP Example 6 - Register with Private IP Address

Section 3.7: Asterisk Application

### 3.1 VoIP Example 1 - Basic Configuration and Registration

In this case, Vigor 3300V uses a FXS card and a FXO card with four groups of “iptel” numbers and “fwd” numbers respectively. The codec is G.729A. WAN IP address is 220.135.240.207.

Vigor 2900V has two VoIP Ports with an iptel number and the fwd number respectively. The Codec is G.729A/B. WAN IP is 61.1.1.1.

Table 3-1. Example1-basic settings in Vigor 3300V and Vigor 2900V

	WAN IP	Port Number	Phone Number	Proxy	Codec
<b>3300V</b>	220.135.240.207	Port1(FXS)	888833	iptel	G.729A
		Port2(FXS)	888834	iptel	G.729A
		Port3(FXS)	660533	fwd	G.729A
		Port4(FXS)	660534	fwd	G.729A
		Port5(FXO)	888835	iptel	G.729A
		Port6(FXO)	888836	iptel	G.729A
		Port7(FXO)	660525	fwd	G.729A
		Port8(FXO)	660526	fwd	G.729A
<b>2900V</b>	61.31.167.135	Port1(FXS)	888829	iptel	G.729A
		Port2(FXS)	660529	fwd	G.729A

Table 3-2. Example1-basic settings in Vigor 3300V and Vigor 2900V

	Proxy	Domain	Port
iptel	iptel.org	iptel.org	5060
fwd	fwd.pulver.com	fwd.pulver.com	5060

### 3.1.1 Vigor 3300V Configuration Example

#### Step 1

Enter **VoIP - Protocol** page and configure related settings on SIP Configuration.

Figure 3-1. SIP configuration of protocol in Vigor 3300V

#### Step 2

Enter **VoIP - Port Settings** page, click the **Edit** icon of port1.

Figure 3-2. Edit of port1

#### Step 3

Enter the **Port1** page. This page falls into six sections.

- **Port1 (FXS)**

Display the port type, **enable** or **disable** the port, setup the account, etc.

#### Disable or Enable

By default is **Enable**.

#### Username & Password

Type the registrar's account **888833** and password.

#### Display Name

Display incoming call's information. To facilitate ease differentiation please type **3300V\_Port1\_ipstel**.

### Proxy Server

Select the SIP Server used for registration from the pull-down menu. There are **None** and three SIP Servers available, which are set in the **VoIP- Protocol** page. Please select **ipstel**.

- **FXO**

Dedicated settings for FXO card.

Incoming Pre-Set Number: The transfer number auto dialed after the FXO receives a call from the Internet.



The screenshot shows a web interface titled "VoIP - Port Settings - Port1 - Edit". Under the heading "Port 1 (FXS)", there are several configuration options: "Disable" and "Enable" radio buttons, with "Enable" selected; a "Username:" text box containing "888833"; a "Password:" text box with masked characters "\*\*\*\*"; a "Display Name:" text box containing "3300V\_Port1\_ipstel"; a "Proxy Server:" dropdown menu with "ipstel" selected; and a "VoIP IP Address:" dropdown menu with "VAN" selected.

Figure 3-3. Port1 setting page

- **Codec**

Setup the voice compression mode and transfer rate, etc.

#### Preferred Codec

Preferred voice compression mode. It will affect voice quality and transferred data size. By default is G.729A – 8kbps.

#### Codec Rate

Transfer rate of the voice packets. By default is **20ms**.

#### Codec VAD

This feature can reduce the number of transmitted bits and packets during silence periods. But it may slightly affect the voice quality. By default is **Disable**.

- **CAS**

Adjust the volume of the conversation.

#### RX Gain

The default value is **0**.

#### TX Gain

The default value is **0**.

- **FAX**

Relevant settings used for FAX over VoIP.

### FAX Mode

Compression mode used for transferring FAX. By default is **T.38 Relay**.

### FAX Bypass Codec

Select the compression mode when FAX Mode selects Bypass.

### FAX Bypass Codec Rate

Select the transfer rate of voice packets when FAX Mode selects Bypass.

- **DTMF**

DTMF are the audible sounds you hear when you press keys on your phone.

### DTMF Relay

By default is **RFC2833**.

After configuration, click Apply to save the settings. Router will auto jump to the **VoIP - Port Settings** page.

VoIP - Port Settings page.

The screenshot shows the 'VoIP - Port Settings' configuration page. It includes sections for Codec (Preferred Codec: G.729A -8kbps, Codec Rate: 20 (ms), Codec VAD: Disable), CAS (RX Gain: 0, TX Gain: 0), FAX (FAX Mode: T.38 Relay, FAX Bypass Codec: G.711U (PCMU) -6.4kbps, FAX Bypass Codec Rate: 20 (ms)), DTMF (DTMF Relay: RFC2833), and Call Forwarding (Disable selected). There are also fields for SIP URL and buttons for Apply and Cancel.

Figure 3-4. Page of port settings

## Step 4

Set Port2~Port8 one by one in turn.

## Type

Port1~Port4 are **FXS**, Port5~Port8 are **FXO**.

## Active

Port1~Port8 are all **active** (√=Enable).

## Group

Port1~Port8 are **Group1~Group8** independently.

**Username**

**Phone Number** of Port1~Port8.

**Proxy**

Port1, 2, 5, and 6 are registered to **iptel** Proxy, and Port3, 4, 7, 8 are registered to **fwd** Proxy.

**Codec**

Port1~Port8 all prior use **G.729A - 8kbps**.

#	Phone Number	Type	Active	Group	Username	Proxy	Codec
1	888833	FXS	V	1	888833	iptel	G.729A-8kbps
2	888834	FXS	V	2	888834	iptel	G.729A-8kbps
3	660533	FXS	V	3	660533	fwd	G.729A-8kbps
4	660534	FXS	V	4	660534	fwd	G.729A-8kbps
5	888835	FXO	V	5	888835	iptel	G.729A-8kbps
6	888836	FXO	V	6	888836	iptel	G.729A-8kbps
7	660525	FXO	V	7	660525	fwd	G.729A-8kbps
8	660526	FXO	V	8	660526	fwd	G.729A-8kbps

Figure 3-5. Port2~Port8 Settings

**Step 5**

Enter the **VoIP - Status** page, wait one or two minutes (The time depends on SIP Server's response speed and the network condition).

**Register Status**

Display the register information from Port1~Port8. **OK** means this port is registered successfully.

**Call Status**

Display calling information from Port1~Port8. **Idle** means there is no conversations on Port1~Port8.

#	Register Status	Call Status	Call Type	Caller Number	Callee Number	Start Time	Remote RTP Address	Remote RTP Port	RTP Statistic	Codec Type	Packet Period	VAD	DTMF Relay
1	OK	Idle											
2	OK	Idle											
3	OK	Idle											
4	OK	Idle											
5	OK	Idle											
6	OK	Idle											
7	OK	Idle											
8	OK	Idle											

Figure 3-6. Status of Vigor 3300V

**Note**

*This page will automatically refresh every 6 second, so as to display the latest status. You may click Refresh button to renew immediately.*

### 3.1.2 Vigor 2900V Configuration Example

#### Step 1

Open the Web of 2900V and click **VoIP Setup**.



Figure 3-7. VoIP web page of Vigor 2900V

#### Step 2

Click **SIP Related Functions Setup**.

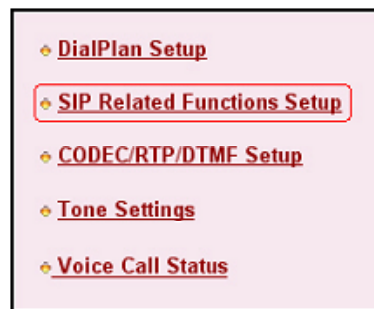


Figure 3-8. SIP related function setting of Vigor 2900V

#### Step 3

Setup Port1 and Port2. This page falls into two sections,

- SIP: Setup relevant SIP Servers used for registration respectively.
- Ports: Type account and password.

After configuration please click OK to save the settings. 2900V will go to VoIP – Setup page automatically.

SIP	
<b>Port 1</b>	<b>Port 2</b>
SIP Port: 5060	SIP Port: 5060
Domain: iptel.org	Domain: fwd.pulver.com
Proxy: iptel.org	Proxy: fwd.pulver.com
Outbound Proxy:	Outbound Proxy:

Ports Setting	
<b>Port 1</b>	<b>Port 2</b>
Register via: WAN	Register via: WAN
Display Name: 2900V_Port1_jc	Display Name: 2900V_Port2_fw
Account Name: 000029	Account Name: 660529
Authentication ID: 888829	Authentication ID: 660529
Password: ****	Password: ****
Expiry Time: 1 hour, 3600 sec	Expiry Time: 1 hour, 3600 sec

Stun Server

OK Cancel

Figure 3-9. Setup port1 and port2 of Vigor 2900V

#### Step 4

Click **Voice Call Status**.

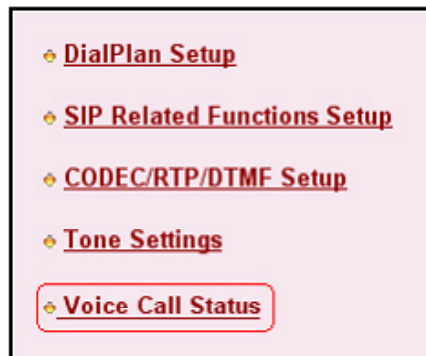


Figure 3-10. Voice call status of Vigor 2900V

#### Step 5

Wait one or two minutes (The time depends on SIP Server's response speed and the network condition)

#### Channel

**R** means Port1 and Port2 register successfully.

#### Status

**IDLE** means there is no conversations on Port1~Port8.

Channel	Status	Codec	PeerID	Connect Time	Tx Pkts	Rx Pkts	Rx Losses	Rx Jitter (ms)	In Calls	Out Calls	Volume Gain
1 (R)	IDLE			0	0	0	0	0	0	0	5
2 (R)	IDLE			0	0	0	0	0	0	0	5

(R) : Means you have registered your SIP server

Figure 3-11. VoIP connection status of Vigor 2900V

Now the configuration is completed.

## 3.2 VoIP Example 2 - Basic Calling Method

We will introduce three basic VoIP calling methods, involving Direct IP Call, Intercommunication with one SIP Proxy Server and Intercommunication with different SIP Proxy Servers. All the settings are based on the VoIP Example 1(Basic Configuration and Registration).

### 3.2.1 Direct IP Call (Call with each other without registration)

Connect a telephone into Vigor 3300V's Port1 and Vigor 2900V's Port1 respectively. They can call with each other directly with IP addresses if only Vigor 3300V and Vigor 2900V both have public IP addresses and have set up the Phone Numbers.

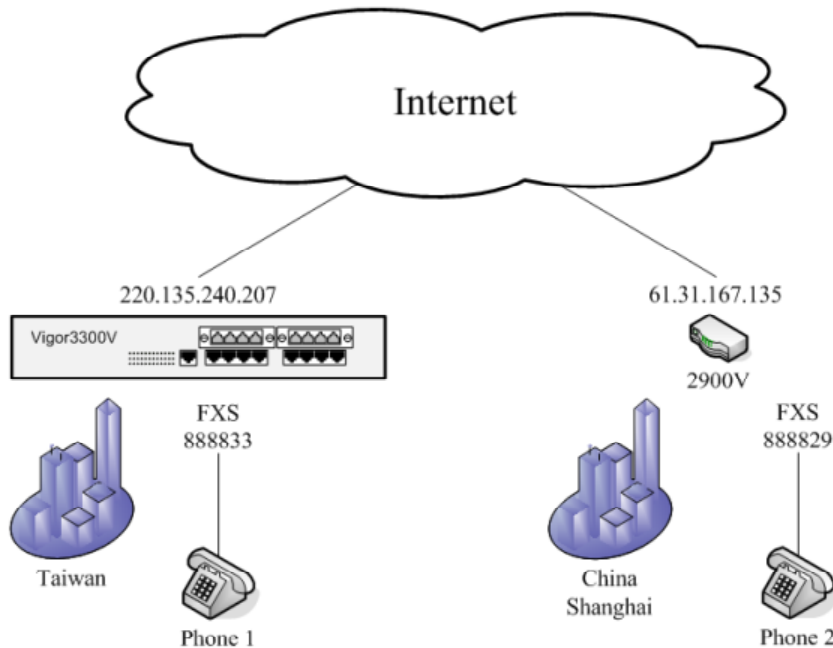


Figure 3-12. A scenario architecture graph



Table 3-3. Configuration table

	WAN IP	Port Number	Phone Number	Proxy	Codec
3300V	220.135.240.207	Port1(FXS)	888833	iptel	G.729A
2900V	61.31.167.135	Port1(FXS)	888829	iptel	G.729A

Furthermore, do **NOT** enable the **Outbound Proxy** feature when you set up 3300V and 2900V to use Direct IP Call. (It isn't **active** in the Example 1; please see Figure 3-2 shown below) Otherwise even if you dial the IP address, the call is still sent to the SIP Proxy Server always. And if the SIP Proxy Server doesn't forward the call to remote VoIP user's WAN IP, you can't do this action

The screenshot shows the 'VoIP - Protocol' configuration page. It has two main sections: 'SIP Configuration' and 'Ports Setting'.  
**SIP Configuration:** 'Select Protocol' has 'SIP' selected. 'SIP Local Port' is set to 5060. Below is a table for proxy settings:  

#	Active	Outbound Proxy	Proxy Name	Proxy Address
1.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	iptel	iptel.org
2.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	fwd	fwd.pulver.com
3.	<input type="checkbox"/>	<input type="checkbox"/>		

  
**Ports Setting:** 'Port 1' settings include 'SIP Port' (5060), 'Domain' (iptel.org), 'Proxy' (iptel.org), and 'Outbound Proxy' (empty). 'Port 2' settings are also visible but partially obscured. 'Register via' is set to 'WAN'. 'Display Name' is '2900V\_Port1\_IP', 'Account Name' is '888829', and 'Authentication ID' is '888829'.

Figure 3-13. Outbound proxy feature

### 3.2.1.1 Vigor 3300V Configuration Example

#### Step 1

Enter **VoIP - Speed Dial** page, configure relevant settings for Vigor 2900V's Port1.

Speed Dial Phone Number: type **2901**.

Speed Dial Destination: Cal lee's **Number@IP**, type **888829@61.31.167.135**.

Memo: To facilitate ease differentiation please type **2900V\_Port1\_IP**.

Click **Apply** to save the settings and finish the configuration.

The screenshot shows the 'VoIP - Speed Dial' configuration page with a table for speed dial entries:  

#	Speed Dial Phone Number	Speed Dial Destination	Memo
1	2901	888829@61.31.167.135	2900V_Port1_IP
2			
3			
4			
5			

  
 Below the table, an 'Example' row shows '101' and '101@iptel.org'. At the bottom right, there are 'Apply', 'Cancel', and 'Clear This Page' buttons.

Figure 3-14. Speed dial port1 setting

### 3.2.1.2 2900V Configuration Example

#### Step 1

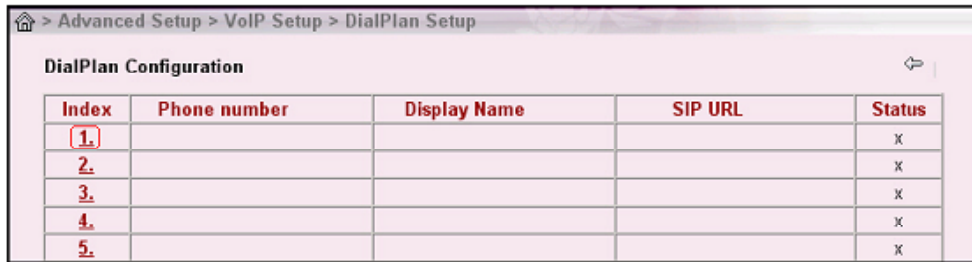
Click **DialPlan Setup** in the **VoIP Setup** page.



Figure 3-15. DialPlan setting of Vigor 2900V

#### Step 2

Click **Index1**.



Index	Phone number	Display Name	SIP URL	Status
1.				X
2.				X
3.				X
4.				X
5.				X

Figure 3-16. DialPlan configuration of Vigor 2900V

#### Step 3

Enter relevant settings for Vigor 3300V's Port1. Click **OK** to save the settings.

Enable: click (√) to activate the entry.

Phone Number : type **3301**.

Display Name : To facilitate ease differentiation please type **3300V\_Port1\_IP**.

SIP URL : Cal lee's **Number@IP**, please type **888833@220.135.240.207**.

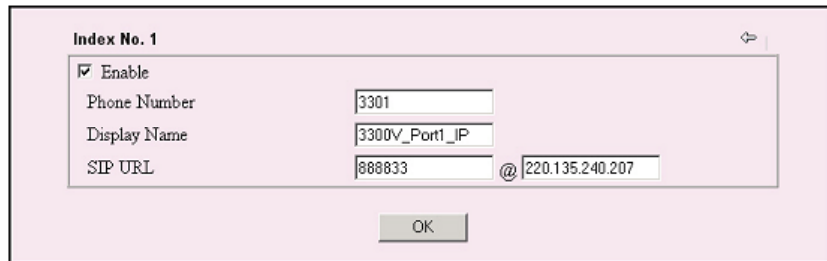
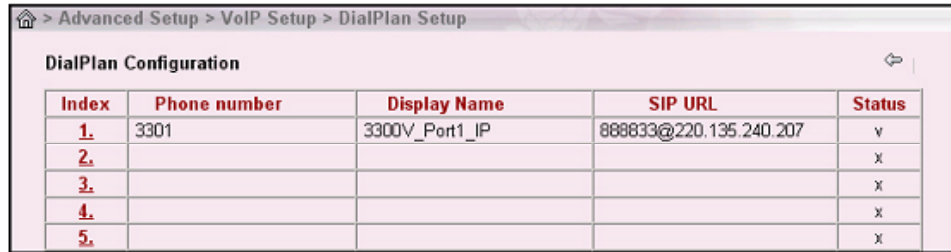


Figure 3-17. Enter relevant settings of index1

## Step 4

Confirm the settings are correct, and then finish the configuration.



Index	Phone number	Display Name	SIP URL	Status
1.	3301	3300V_Port1_IP	888833@220.135.240.207	v
2.				x
3.				x
4.				x
5.				x

Figure 3-18. Finish DialPlan configuration

## Start to dial by using telephones

### Phone1 calls Phone2

Press **2901#** or **888829\*61\*31\*167\*135#**.

### Phone2 calls Phone1

Press **3301#**.

### Note

*# indicates termination of the phone number. After pressing #, VoIP is immediately called out. Or you may wait 3 seconds if you do not press #.*

With 2900V you can't only dial alphanumeric addresses or @ symbols. To dial an IP address, start and end it with a # (hash) replace the dots with \* (star). In this example you have to press #220\*135\*240\*207#. But 3300V can only receive the format of Number@IP. So it is required to setup 3300V's number (888833@220.135.240.207) in the DialPlan entry.

## 3.2.2 Intercommunication with one SIP Proxy Server (registration)

Connect telephones into Vigor 3300V's Port1 & Port3 and Vigor 2900V's Port1 & Port2 respectively. Each port needs to register in the SIP Server.

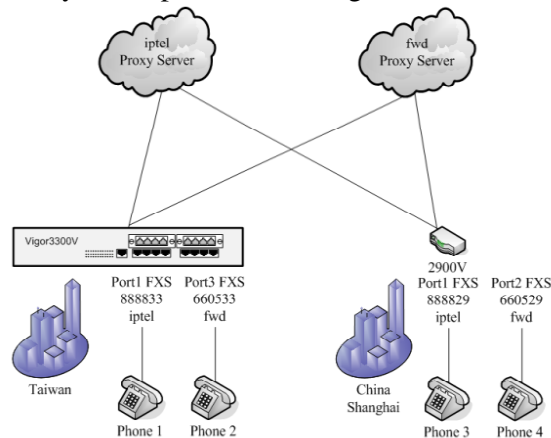


Figure 3-19. A scenario architecture graph

Table 3-4. Configurations between Vigor 3300V and Vigor 2900V

	WAN IP	Port Number	Phone Number	Proxy	Codec
3300V	220.135.240.207	Port1(FXS)	888833	iptel	G.729A
		Port3(FXS)	660533	fwd	G.729A
2900V	61.31.167.135	Port1(FXS)	888829	iptel	G.729A
		Port2(FXS)	660529	fwd	G.729A

You can also add Speed Dial numbers in **Speed Dial** to speed up the dialing, or to accommodate the setup of company's extension numbers.

### 3.2.2.1 Vigor 3300V Configuration Example

#### Step 1

Enter the **VoIP - Speed Dial** page and add the second and third group of Speed Dial number. Then click **Apply** to save the settings and finish the configuration.

#	Speed Dial Phone Number	Speed Dial Destination	Memo
1	2501	888829@61.31.167.135	2500V_Port1_IP
2	291	888829	2900V_Port1
3	292	660529	2900V_Port2
4			
5			

Example 101      101@iptel.org

1 2 3 4 5 6

Apply   Cancel   Clear This Page

Figure 3-20. Speed dial port2 and port3 settings

#### Start to dial by using telephones

##### Phone1 call Phone3

Press **888829#** or **291#**.

##### Phone2 call Phone4

Press **660529#** or **292#**.

##### Phone3 call Phone1

Press **888833#**.

##### Phone4 call Phone2

Press **660533#**.

**Note**

# indicates termination of the phone number. After pressing #, VoIP is immediately called out. Or you may wait 3 seconds if you do not press #.

### 3.2.3 Intercommunication with different SIP Proxy Servers

Connect telephones into 3300V's Port1 & Port3 and 2900V's Port1 & Port2 respectively. Each phone registers to the SIP Server. The settings and scenario are the same as the above example. But they must be set up in conjunction with the Speed Dial.

#### 3.2.3.1 Vigor 3300V Configuration Example

**Step 1**

Enter the **VoIP - Speed Dial** page and add the 4th and 5th group of Speed Dial number. Then press Apply to save the settings and finish the configuration.

#	Speed Dial Phone Number	Speed Dial Destination	Memo
1	2901	888829@61.31.167.135	2900V_Port1_IP
2	291	888829	2900V_Port1
3	292	660529	2900V_Port2
4	2911	888829@iptel.org	2900V_Port1_iptel
5	2912	660529@fwd.pulver.com	2900V_Port2_fwd
Example	101	101@iptel.org	

Apply Cancel Clear This Page

Figure 3-21. Speed dial port4 and port5 settings

#### 3.2.3.2 Vigor 2900V Configuration Example

**Step 1**

Click **DialPlan Setup** in the **VoIP Setup** page. Then add the second and third group of Speed Dial number.

Index	Phone number	Display Name	SIP URL	Status
1.	3301	3300V_Port1_IP	888833@220.135.240.207	v
2.	3311	3300V_Port1_iptel	888833@iptel.org	v
3.	3312	3300V_Port2_fwd	660533@fwd.pulver.com	v
4.				x
5.				x

Figure 3-22. DialPlan configuration of index2 and index3

**Start to dial by using telephone**

**Phone1 call Phone4**

Press **2912#**.

**Phone2 call Phone3**

Press **2911#**.

**Phone3 call Phone1**

Press **3312#**.

**Phone4 call Phone2**

Press **3311#**.

*Note*

*# indicates termination of the phone number. After pressing #, VoIP is immediately called out. Or you may wait 3 seconds if you do not press #.*

### **3.3 VoIP Example 3 - VoIP over VPN**

Based on the **VoIP Example 1 ( Basic Configuration and Registration )**, we will introduce how to dial the VoIP call through an encrypted VPN tunnel.

In this example Vigor 3300V acts as a bridge accepting incoming VPN connections from the other two routers ( Vigor 2900V and Vigor 2200V). The VPN traffic between Vigor 2900V and Vigor 2200V are all passed through Vigor 3300V. These three sites internal networks must be within the same subnet ( 192.168.X.X ). Either site can ping the other two routers. Then you can make a VoIP call through the encrypted VPN tunnel by directly dialing remote router's LAN IP.

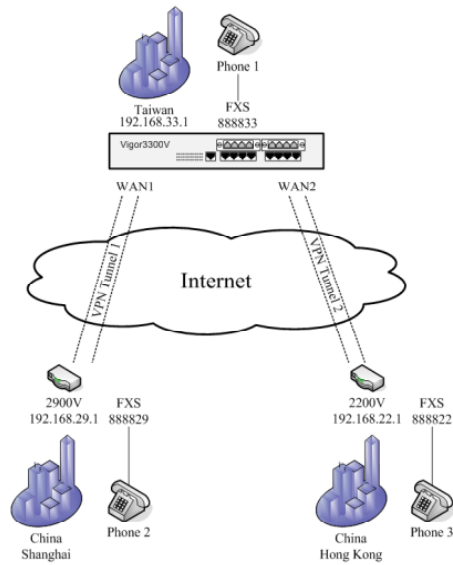


Figure 3-23. A scenario architecture graph

Table 3-5. Configuration table

	3300V Headquarters	2900V Branch Offices	2200V Teleworker
WAN IP	220.135.240.207 PPPoE, fixed IP	61.31.167.135 PPPoE, dynamic IP	
	219.81.160.206 PPPoE, fixed IP		61.230.207.146 PPPoE, dynamic IP
LAN IP	192.168.33.1	192.168.29.1	192.168.22.1
Internal network	192.168.33.X	192.168.29.X	192.168.22.X
Encryption method	DES-SHA1		
Preshared Key	3300		
	1234		1234

Table 3-6. Configuration table

	WAN IP	Port Number	Phone Number	Proxy	Codec
3300V	220.135.240.207	Port1(FXS)	888833		G.729A
2900V	61.31.167.135	Port1(FXS)	888829		G.729A
2200V	61.230.207.146	Port1(FXS)	888822		G.729A

About the VPN configurations please refer to **VPN Example 3(three part communication)**. About VoIP basic configuration please refer to **VoIP Example 1(Basic Configuration and Registration)**.

The following examples are modified based on these two examples.

### 3.3.1 Vigor 3300V Configuration Example

#### Step 1

Enter the **VoIP - Protocol** page; Disable all the **Active** entries by removing the (✓) box. After configuration please click **Apply** to save the settings.

#	Active	Outbound Proxy	Proxy Name	Proxy Address	Proxy Port	Registrar Addr	Registrar Port	Expires (sec)	Domain
1.	<input type="checkbox"/>	<input type="checkbox"/>	iptel	iptel.org	5060	iptel.org	5060	300	iptel.org
2.	<input type="checkbox"/>	<input type="checkbox"/>	fwd	fwd.pulver.com	5060	fwd.pulver.com	5060	300	fwd.pulver.com
3.	<input type="checkbox"/>	<input type="checkbox"/>			5060		5060	300	
Example			iptel	iptel.org		iptel.org			iptel.org

Figure 3-24. Protocol settings of 3300V

Port 1 (FXS)  
 Disable  Enable  
Username: 888833  
Password: \*\*\*\*  
Display Name: 3300V\_Port1\_iptel  
Proxy Server: iptel  
VoIP IP Address: LAN/VPN

Figure 3-25. Edit of port1 settings

#### Note

***In Vigor 3300V firmware v2.5.5 you can only choose WAN or LAN/VPN. And the call can be received or dialed just in one direction (WAN or LAN/VPN).***

Or select **none** as Proxy Server for each Port.

Port 1 (FXS)  
 Disable  Enable  
Username: 888833  
Password: \*\*\*\*  
Display Name: 3300V\_Port1\_iptel  
Proxy Server: none  
VoIP IP Address: LAN/VPN  
Hotline: none, iptel, fwd, undefined proxy 3

Figure 3-26. Edit of port1 settings

#### Step 2



Enter the **VoIP - Port Settings** page, now the Proxy entries all display Disable. (If you select **none** as Proxy Server for each Port, the Proxy entries are blank.)

#	Edit	Type	Active	Group	Username	Proxy	Codec
1		FXS	V	1	888833	iptel (Disable)	G.729A-8kpbs
2		FXS	V	2	888834	iptel (Disable)	G.729A-8kpbs
3		FXS	V	3	660533	fwd (Disable)	G.729A-8kpbs
4		FXS	V	4	660534	fwd (Disable)	G.729A-8kpbs
5		FXO	V	5	888835	iptel (Disable)	G.729A-8kpbs
6		FXO	V	6	888836	iptel (Disable)	G.729A-8kpbs
7		FXO	V	7	660525	fwd (Disable)	G.729A-8kpbs
8		FXO	V	8	660526	fwd (Disable)	G.729A-8kpbs

Figure 3-27. Display of proxy

### Step 3

Enter the **VoIP - Speed Dial** page and input the first and second group of Speed Dial Phone Number. Click **Apply** to save the settings.

#	Speed Dial Phone Number	Speed Dial Destination	Memo
1	2901	888829@192.168.29.1	2900V_Port1_VPN
2	2201	888822@192.168.22.1	2200V_Port1_VPN
3			
4			
5			

Example 101      101@ictel.org

1 2 3 4 5 6

Apply   Cancel   Clear This Page

Figure 3-28. Speed dial phone number settings

## 3.3.2 Vigor 2900V Configuration Example

### Step 1

Enter **VoIP Setup - SIP Related Functions Setup** page and change **Register via** from WAN to **LAN/VPN** for Port1 and Port2. Press OK to save the settings.

Figure 3-29. SIP related functions settings of Vigor 2900V

**Note**

*Do not set up the Outbound Proxy and Stun Server when calling through VPN.*

**Step 2**

Click **DialPlan Setup** in the **VoIP Setup** page and add the first and second group of Speed Dial Phone Number.

Index	Phone number	Display Name	SIP URL	Status
1.	3301		888833@192.168.33.1	v
2.	2201		888822@192.168.22.1	v
3.				x
4.				x
5.				x

Figure 3-30. Add index1 and index2 speed dial phone number

**Note**

*Do not set up the Display Name when calling through the VPN with 2900V firmware v2.5.6. Otherwise you can't get ring back and communicate with remote user after getting through.*

**3.3.3 Vigor 2200V Configuration Example**

**Step 1**

Enter Vigor 2200V's Web and click **VoIP - SIP Related Function** page.

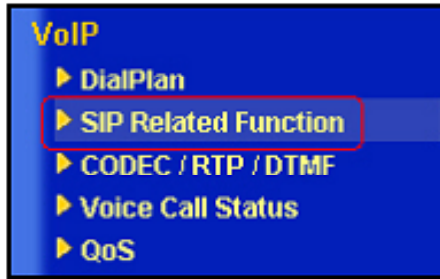


Figure 3-31. SIP related function of Vigor 2200V

## Step 2

Setup Port 1. This page falls into two sections,

- SIP: Set up the SIP Server used for registration.
- Ports: Set up the account details.

After configuration please click **OK** to save the settings.



Figure 3-32. Port1 setting

## Note

**Do not set up the Proxy and Stun Server when calling through VPN. While in 2200V firmware v2.5.5.4, the Proxy will be active if Use Registrar is enabled. So make sure not click Use Registrar.**

## Step 3

Enter **VoIP - DialPlan** page and the first and second group of Speed Dial Phone Number.

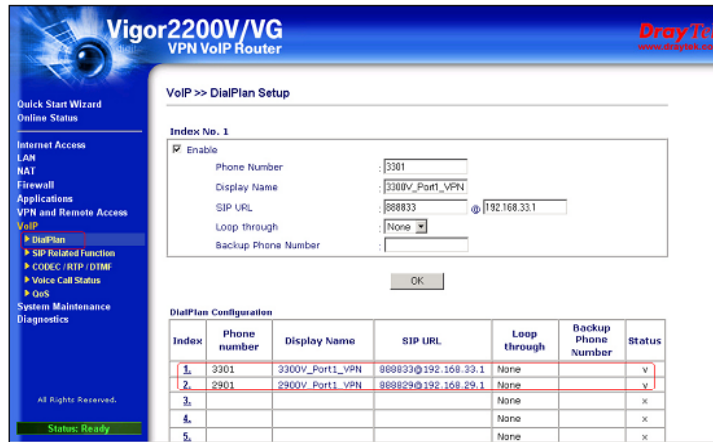


Figure 3-33. Add index1 and index2 speed dial phone number

After configuration, please confirm that the VPNs are established and they can communicate with each other. (Please refer to VPN - IPSec - LAN to LAN Usage Example 2).

### Start to dial by using telephones

#### Phone1 call Phone2

Press **2901#** or **888829\*192\*168\*29\*1#**.

#### Phone1 call Phone3

Press **2201#** or **888822\*192\*168\*22\*1#**.

#### Phone2 call Phone1

Press **3301#**.

#### Phone2 call Phone3

Press **2201#** or **#192\*168\*22\*1#**.

#### Phone3 call Phone1

Press **3301#**.

#### Phone3 call Phone2

Press **2901#** or **#192\*168\*29\*1#**.

### Note

*# indicates termination of the phone number. After pressing #, VoIP is immediately called out. Or you may wait 3 seconds if you do not press #.*

## 3.4 VoIP Example 4 - Practical Application of FXS

Based on the **VoIP Example 1(Basic Configuration and Registration)**, we will introduce the practical application of FXS.

Generally the practical application of FXS falls into the following two sections.

Connect the telephones (Please refer to VoIP Example 1). Two VoIP equipments call with each other.

Connect PBX's Outside Lines. The usage is the same as that of PSTN line. Different PBX has its own settings and required configuration by you.

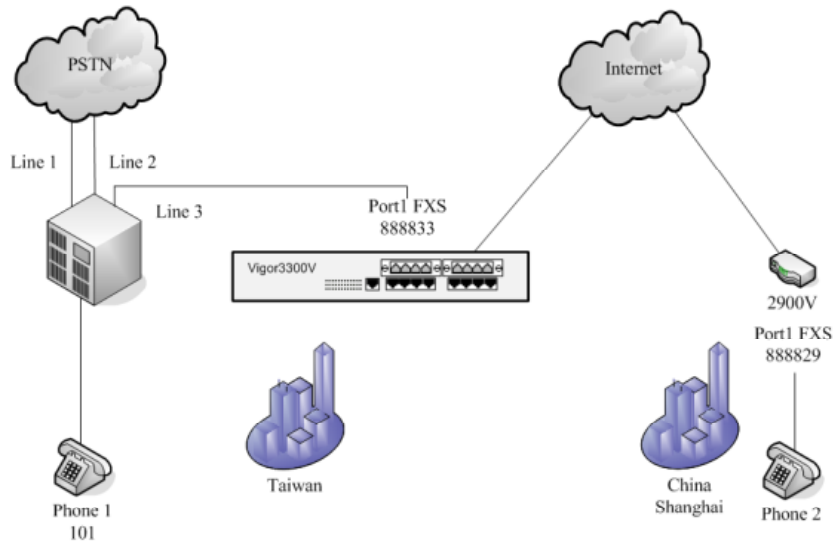


Figure 3-34. A scenario architecture graph

Table 3-7. Configuration table between Vigor 3300V and Vigor 2900V

	WAN IP	Port Number	Phone Number	Proxy	Codec
<b>3300V</b>	220.135.240.207	Port1(FXS)	888833	iptel	G.729A
<b>2900V</b>	61.31.167.135	Port1(FXS)	888829	iptel	G.729A

Suppose there are two PSTN lines connected to PBX's Outside Lines. The third Outside Line is connected to 3300V's FXS Port1. The Inside Line is connected to a telephone with the extension 101. If the extension wants to dial VoIP using Line3, you must firstly press 3, and then dial the phone number.

Table 3-8. Example of lines connections

	PBX	Phone Number
Line3(3)	Outside Lines	888833
Phone1	Inside Lines	101

### Start to dial by using telephones

#### Phone1 calls Phone2

Press **3**, after hearing the dial tone press VoIP number **888829#**.

#### Phone2 calls Phone1

Press **888833#**, after getting through you will hear the auto reply from the PBX. Then press the extension **101**.

#### Note

*# indicates termination of the phone number. After pressing #, VoIP is immediately called out. Or you may wait 3 seconds if you do not press #.*

This example is the intercommunication with one SIP Proxy Server. For the applications of Direct IP Call and Intercommunication with different SIP Proxy Servers please refer to **VoIP Example 2(Basic Calling Method)**. The VoIP call can also work with VPN, please refer to **VoIP Example 3(VoIP over VPN)**.

Also you can set up the Speed Dial entry. To accommodate the extension please set up 888829 to **291**, 888833 to **331**. You may refer to the figures shown below and **VoIP Example 2(Basic Calling Method)**.

**VoIP - Speed Dial**

#	Speed Dial Phone Number	Speed Dial Destination	Memo
1	291	666629	2900V_Port1
2			
3			
4			
5			

Example 101      101@iptel.org

1 2 3 4 5

Apply   Cancel   Clear This Page

Figure 3-35. Speed dial phone number settings

**Index No. 1**

Enable

Phone Number      331

Display Name      3300V\_Port1

SIP URL      888833 @ iptel.org

OK

Figure 3-36. Edit of index1

### 3.5 VoIP Example 5 - Practical Application of FXO

Based on the **VoIP Example 1(Basic Configuration and Registration)**, we will introduce the practical application of FXO.

Generally the practical application of FXO falls into the following two sections,

Connect to PSTN line

By connecting 3300V's FXO Port5 to a PSTN line VoIP is seamlessly integrated to PSTN line, allow you to call not only the remote VoIP user, but also the remote PSTN user. Also the PSTN user can call the VoIP user.

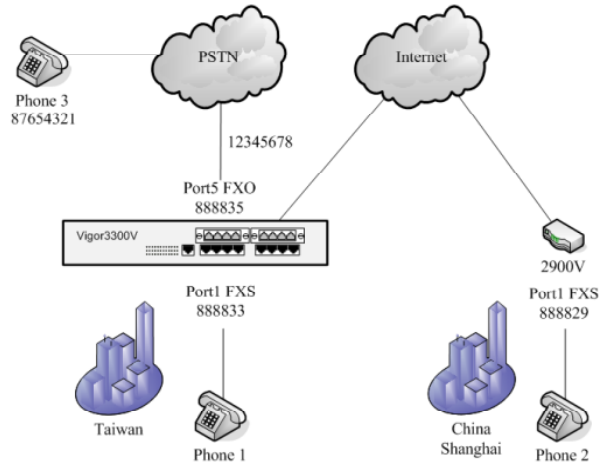


Figure 3-37. A scenario architecture graph

Table 3-9. Configuration table between 3300V and 2900V

	WAN IP	Port Number	Phone Number	Proxy	Codec
3300V	220.135.240.207	Port1(FXS)	888833	iptel	G.729A
		Port5(FXO)	888835	iptel	G.729A
2900V	61.31.167.135	Port1(FXS)	888829	iptel	G.729A

The number of the PSTN line connected into the FXO Port5 on the 3300V is 12345678. The number of another PSTN line is 87654321.

About VoIP basic settings please refer to **VoIP Example 1(Basic configuration and registration)**

**Start to dial by using telephones**

**Phone1 calls Phone3**

Press **888835#**. After getting through you will hear the dial tone, then press the PSTN number **87654321#**.

**Phone2 calls Phone3**

Press **888835#**. After getting through you will hear the Dial tone, then press the PSTN number **87654321#**.

**Phone3 calls Phone2**

Press **12345678**. After getting through you will hear the Dial tone, then press the VoIP number **888829#**.

**Phone3 calls Phone1**

Press **12345678**. After getting through you will hear the Dial tone, then press the VoIP number **888833#**.

*Note*

*# indicates termination of the phone number. After pressing #, VoIP is immediately called out. Or you may wait 3 seconds if you do not press #.*

- Connect PBX's Inside Lines. The usage is the same as that of common extension. Different PBX has its own settings and required configuration by you.

By connecting 3300V's FXO Port5 to PBX's Inside Line VoIP is seamlessly integrated to PBX's inside lines, allow you to call not only the VoIP, but also the PSTN line and PBX's extension. Also the remote user can call you from the PSTN line and PBX's extension.



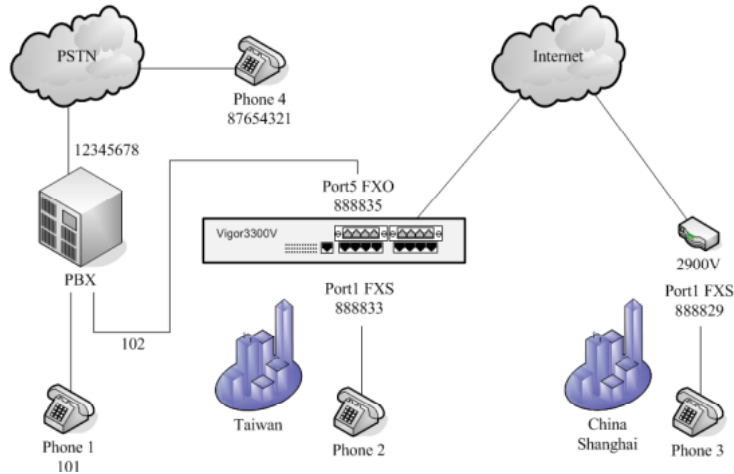


Figure 3-38. A scenario architecture graph

Table 3-10. Configuration table between Vigor 3300V and Vigor 2900V

	WAN IP	Port Number	Phone Number	Proxy	Codec
<b>3300V</b>	220.135.240.207	Port1(FXS)	888833	iptel	G.729A
		Port5(FXO)	888835	iptel	G.729A
<b>2900V</b>	61.31.167.135	Port1(FXS)	888829	iptel	G.729A

Suppose the number of PBX's Outside Line is 12345678. One Inside Line is connected to a telephone with the extension 101. If you want to use PSTN from the extension, you must firstly press 0, and then dial the phone number.

The FXO Port5 on the 3300V is connected to PBX's Inside Line with the number 102. The number of another PSTN line is 87654321.

About VoIP basic settings please refer to **VoIP Example 1. (Basic configuration and registration)**

#### **Start to dial by using telephones**

##### **Phone1calls Phone2**

Press extension **102**. After getting through you will hear the dial tone, then press the VoIP number **888833#**.

##### **Phone1calls Phone3**

Press extension **102**. After getting through you will hear the Dial tone, then press the VoIP number **888829#**.

##### **Phone2 calls Phone1**

Press **888835#**. After getting through you will hear the Dial tone, then press the extension **101**.

**Phone2 calls Phone4**

Press **888835#**. After getting through you will hear the Dial tone. Press outside line **0**, then press **87654321**.

**Phone3 calls Phone1**

Press **888835#**. After getting through you will hear the Dial tone, then press the extension **101**.

**Phone3 call Phone4**

Press **888835#**. After getting through you will hear the Dial tone. Press outside line **0**, then press **87654321**.

**Phone4 calls Phone2**

Press **12345678**. After getting through you will hear the auto reply from the PBX, then press the extension **102**. After getting through you will hear the Dial tone, then press the VoIP number **888833#**.

**Phone4 calls Phone3**

Press **12345678**. After getting through you will hear the auto reply from the PBX, then press the extension **102**. After getting through you will hear the Dial tone, then press the VoIP number **888829#**.

*Note*

*# indicates termination of the phone number. After pressing #, VoIP is immediately called out. Or you may wait 3 seconds if you do not press #.*

This example is intercommunication with one SIP Proxy Server. For the applications of Direct IP Call and Intercommunication with different SIP Proxy Servers please refer to **VoIP Example 2(Basic Calling Method)**. The VoIP call can also work with VPN, please refer to **VoIP Example 3(VoIP over VPN)**.

### **3.6 VoIP Example 6 - Register with Private IP Address**

Based on the **VoIP Example 1(Basic Configuration and Registration)**, we will introduce how to register with the SIP Server when Vigor 3300V has no Public IP address but a Private IP address.

When Vigor 3300V's WAN uses a Private IP, the VoIP traffic must pass through the upper-layer NATs. Now STUN feature should be enabled so that VoIP can work normally.

In this example Vigor 3300V is connected in the LAN of Vigor 2600V. It obtains a private IP address from the Vigor 2600V and accesses the Internet through the Vigor 2600V. Vigor 3300V uses this private IP to register with the SIP Server because it doesn't

know Vigor 2600V's WAN IP, which results in that SIP Server can't find Vigor 3300V. But if Vigor 3300V uses STUN, it can discover Vigor 2600V's WAN IP and will use this IP as SIP content to identify its location. When SIP Server contacts with Vigor 3300V, the packets are firstly sent to Vigor 2600V, and then forwarded by Vigor 2600V to Vigor 3300V.

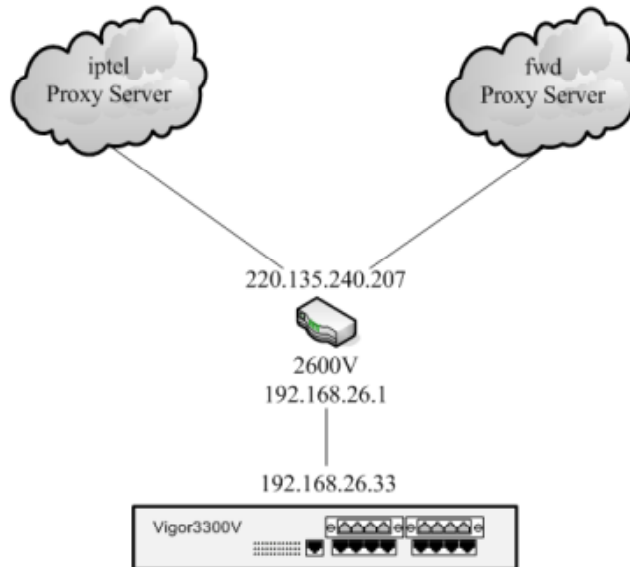


Figure 3-39. A scenario architecture graph

Table 3-12. Configuration table between Vigor 3300V and Vigor 2600V

	WAN IP	Port Number	Phone Number	Proxy	Codec
3300V	192.168.26.33	Port1(FXS)	888833	iptel	G.729A
		Port3(FXS)	660533	fwd	G.729A
2600V	220.135.240.207	Port1(FXS)	888829	iptel	G.729A

Vigor 2600V's internal network is 192.168.26.X, Vigor 3300V uses Static IP 192.168.26.33. For VoIP basic settings please refer to **VoIP Example 1(Basic Configuration and Registration)**.

### 3.6.1 Vigor 2600V Configuration Example

#### Step 1

Enter 2600V via Web and click **NAT Setup** page.



Figure 3-40. NAT setup of Vigor 2600V

**Step 2**

click **Open Ports Setup**.



Figure 3-41. Open ports settings of Vigor 2600V

**Step 3**

Click **Index1**.

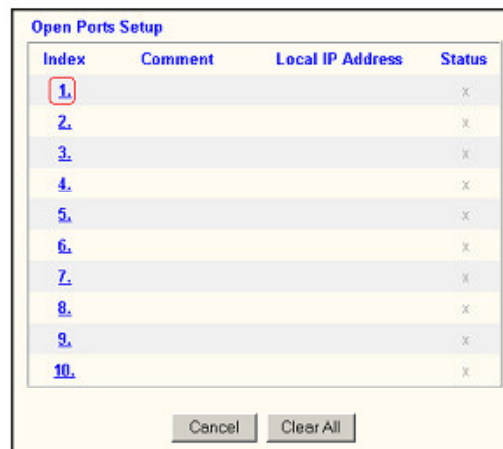


Figure 3-42. Open ports profile Index 1

#### Step 4

Forward the packets sent to **UDP 5060, 13456~13470** and **49170~49184** to Vigor 3300V's WAN IP **192.168.26.33**. Press OK to save the settings.

Index	Protocol	Start Port	End Port	Index	Protocol	Start Port	End Port
1.	UDP	5060	5060	6.	--	0	0
2.	UDP	13456	13470	7.	--	0	0
3.	UDP	49170	49184	8.	--	0	0
4.	--	0	0	9.	--	0	0
5.	--	0	0	10.	--	0	0

Figure 3-43. Settings of Index 1

#### Step 5

After configuration it will automatically jump to **Open Ports Setup** page. Confirm the settings to be correct. The setup is completed.

Index	Comment	Local IP Address	Status
1.	3300V_VoIP	192.168.26.33	v
2.			x
3.			x
4.			x
5.			x
6.			x
7.			x
8.			x
9.			x
10.			x

Figure 3-44. Index1 configuration

### 3.6.2 Vigor 3300V Configuration Example

#### Step 1

Enter the **VoIP - NAT Traversal** page and enable the STUN function. Then click **Apply** to save the setting.

Figure 3-35. NAT Traversal of Vigor 3300V

## Step 2

Enter **VoIP - Status** page, wait one or two minutes (The time depends on SIP Server's response speed and the network condition). When you see the Register Status is OK, the registration is successful.

#	Register Status	Call Status	Call Type	Caller Number	Callee Number	Start Time	Remote RTP Address	Remote RTP Port	RTP Statistic	Codec Type	Packet Period	VAD	DTMF Policy
1	OK	Idle											
2	OK	Idle											
3	OK	Idle											
4	OK	Idle											
5	OK	Idle											
6	OK	Idle											
7	OK	Idle											
8	OK	Idle											

Figure 3-36. Status of Vigor 3300V

## Note

*Iptel SIP Server itself supports STUN function, so 3300V can register without STUN enabled.*

At present the above configuration has a precondition that Vigor 2600's VoIP isn't active. If VoIP function is enabled, the packets on UDP 5060 will be received by Vigor 2600V and not forwarded to Vigor 3300V. So you have to change Vigor 3300V's Local Port from 5060 to **5061**.

#	Active	Outbound Proxy	Proxy Name	Proxy Address	Proxy Port	Registrar Addr	Registrar Port	Expires (sec)	Domain
1.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	iptel	iptel.org	5060	iptel.org	5060	300	iptel.org
2.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	fwd	fwd.pulver.com	5060	fwd.pulver.com	5060	300	fwd.pulver.com
3.	<input type="checkbox"/>	<input type="checkbox"/>			5060		5060	300	
Example			iptel	iptel.org		iptel.org			iptel.org

Figure 3-37. Protocol of Vigor 3300V

The Open Ports setup in Vigor 2600V also must be changed to **5061**.

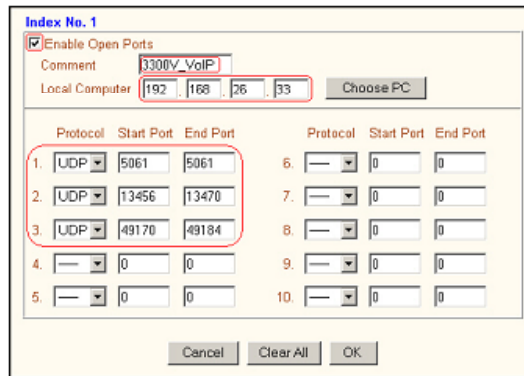


Figure 3-38. Open port setup

## 3.7 Asterisk Application

### 3.7.1 Introduce

In this chapter, we offer the application shows that it is convenient and cost saving to implement the free IP-PBX using Asterisk and Vigor 3300V when users want to use the Soft Phone or IP Phone instead of traditional telephone in the company.

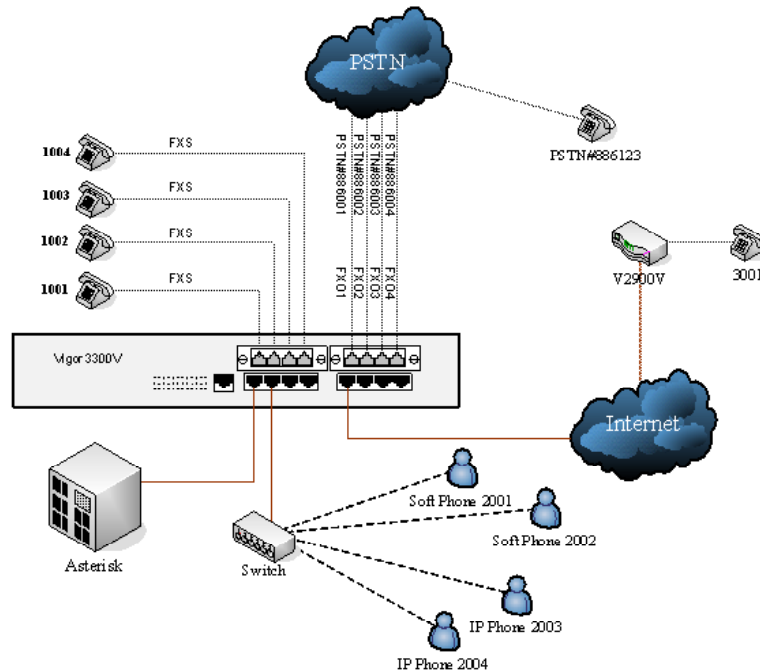


Figure 3-40. The scenario

In the figure using FXO port of Vigor 3300V to connect to PSTN. So, users do not need the other equipment to as the IP-PBX. The way that we work normally with the FXO of Vigor 3300V is that we could make a call from extension of IP-PBX which is the telephones connected with FXS of Vigor 3300V, Soft Phone or IP Phone to PSTN Network. We also could make a call from PSTN to the IP-PBX, there are four PSTN line (the maximum is 8), then forwarding the call to any extension of IP-PBX, or make a call from extensions to remote peer user through VPN in the Internet, or reverse direction call.

Another application is workable that putting the Asterisk to the Internet for branch office communication.

### 3.7.1.1 Configuration

IP Address List:

Asterisk – 172.16.2.234

Vigor 3300V – 172.16.2.237

SoftPhone 2001 – 172.16.2.201

SoftPhone 2002 – 172.16.2.202

SoftPhone 2003 – 172.16.2.203

SoftPhone 2004 – 172.16.2.204

Vigor 2900V (VPN) – 172.16.2.205

### 3.7.1.2 Installing Asterisk

1. Download Asterisk from the Asterisk website page <http://www.asterisk.org/>.
2. Install the Asterisk and refer to the installation guide from the Asterisk website.

### 3.7.2 Configuring Asterisk

#### sip.conf

Modify the sip.conf, the file is usually placed on the location /etc/asterisk.

[general] Setting in sip.conf

Modify the realm value to 172.16.2.234 for digest authentication.

```
realm=172.16.2.234 ; Realm for digest authentication
```

Modify the tos value, users could choose one kind of type. There are “lowdelay”, “throughput”, “reliability”, “mincost” and “none”. It is depend on the network status.

```
Tos=lowdelay
```

Modify the defaultexpiry value for registration.

```
Defaultexpiry=300 ; Default length of incoming/outgoing registration
```

Modify the codec settings.

```
disallow=all ; First disallow all codecs  
allow=ulaw ; Allow codecs in order of preference
```



```
allow = alaw
allow=g729
allow=g726
```

Modify the language value for all users.

```
language=en ; Default language setting for all users/peers
```

Modify the rtptimeout value for RTP activity.

```
rtptimeout=60 ; Terminate call if 60 seconds of no RTP activity
```

Modify the dtmfmode value.

```
dtmfmode = rfc2833; Set default dtmfmode for sending DTMF. Default:
rfc2833
; Other options:
; info : SIP INFO messages
; inband : Inband audio (requires 64 kbit codec -alaw, ulaw)
; auto : Use rfc2833 if offered, inband otherwise
```

### Add Phone Number

Add phone setting for each phone number.

```
[1001]
type=friend
nat=no
canreinvite=yes
host=dynamic
defaultip=172.16.2.237
username=1001
secret=0000
dtmfmode=info ; Choices are inband, rfc2833, or info
call-limit=1
mailbox=1000 ; Mailbox for message waiting indicator
context=sip
callerid="1001" <1001>
disallow=all
```

```
allow=ulaw
allow=g729
allow=g723.1
```

```
[1002]
```

```
type=friend
nat=no
canreinvite=yes
host=dynamic
defaultip=172.16.2.237
username=1002
secret=0000
dtmfmode=info ; Choices are inband, rfc2833, or info
call-limit=1
mailbox=1000 ; Mailbox for message waiting indicator
context=sip
callerid="1002" <1002>
disallow=all
allow=ulaw
allow=g729
allow=g723.1
```

```
[1003]
```

```
type=friend
nat=no
canreinvite=yes
host=dynamic
defaultip=172.16.2.237
username=1003
secret=0000
dtmfmode=info ; Choices are inband, rfc2833, or info
call-limit=1
mailbox=1000 ; Mailbox for message waiting indicator
context=sip
```

callerid="1003" <1003>

disallow=all

allow=ulaw

allow=g729

allow=g723.1

[1004]

type=friend

nat=no

canreinvite=yes

host=dynamic

defaultip=172.16.2.237

username=1004

secret=0000

dtmfmode=info ; Choices are inband, rfc2833, or info

call-limit=1

mailbox=1000 ; Mailbox for message waiting indicator

context=sip

callerid="1004" <1004>

disallow=all

allow=ulaw

allow=g729

allow=g723.1

[2001]

type=friend

nat=no

canreinvite=yes

host=dynamic

defaultip=172.16.2.201

username=2001

secret=2001

dtmfmode=info ; Choices are inband, rfc2833, or info

call-limit=1

mailbox=1000 ; Mailbox for message waiting indicator

```
context=sip
callerid="2001" <2001>
disallow=all
allow=ulaw
allow=g729
allow=g723.1

[2002]
type=friend
nat=no
canreinvite=yes
host=dynamic
defaultip=172.16.2.202
username=2002
secret=2002
dtmfmode=info ; Choices are inband, rfc2833, or info
call-limit=1
mailbox=1000 ; Mailbox for message waiting indicator
context=sip
callerid="2002" <2002>
disallow=all
allow=ulaw
allow=g729
allow=g723.1

[2003]
type=friend
nat=no
canreinvite=yes
host=dynamic
defaultip=172.16.2.203
username=2003
secret=2003
dtmfmode=info ; Choices are inband, rfc2833, or info
call-limit=1
```

mailbox=1000 ; Mailbox for message waiting indicator  
context=sip  
callerid="2003" <2003>  
disallow=all  
allow=ulaw  
allow=g729  
allow=g723.1

[2004]

type=friend  
nat=no  
canreinvite=yes  
host=dynamic  
defaultip=172.16.2.204  
username=2004  
secret=2004  
dtmfmode=info ; Choices are inband, rfc2833, or info  
call-limit=1  
mailbox=1000 ; Mailbox for message waiting indicator  
context=sip  
callerid="2004" <2004>  
disallow=all  
allow=ulaw  
allow=g729  
allow=g723.1

[3001]

type=friend  
nat=no  
canreinvite=yes  
host=dynamic  
defaultip=172.16.2.205  
username=3001  
secret=3001  
dtmfmode=info ; Choices are inband, rfc2833, or info

```
call-limit=1
mailbox=1000 ; Mailbox for message waiting indicator
context=sip
callerid="3001" <3001>
disallow=all
allow=ulaw
allow=g729
allow=g723.1
```

```
[fxo1]
type=friend
secret=1234
context=sip
disallow=all
allow=ulaw
allow=g729
allow=g723.1
dtmfmode=info
canreinvite=no
host=dynamic
defaultip=172.16.2.237
```

```
[fxo2]
type=friend
secret=1234
context=sip
disallow=all
allow=ulaw
allow=g729
allow=g723.1
dtmfmode=info
canreinvite=no
host=dynamic
defaultip=172.16.2.237
```

```
[fxo3]
type=friend
secret=1234
context=sip
disallow=all
allow=ulaw
allow=g729
allow=g723.1
dtmfmode=info
canreinvite=no
host=dynamic
defaultip=172.16.2.237
```

```
[fxo4]
type=friend
secret=1234
context=sip
disallow=all
allow=ulaw
allow=g729
allow=g723.1
dtmfmode=info
canreinvite=no
host=dynamic
defaultip=172.16.2.237
```

mgcp.conf

Modify the mgcp.conf, the file is usually placed on the location /etc/asterisk.

*[general] Setting in mgcp.conf*

Modify the Call Agent port value to 2727 for Vigor 3300V.

```
port = 2727
```

## *Add Endpoint for MGCP*

Modify the port value to 2727 for Call Agent.

```
[172.16.2.237]
host = 172.16.2.237
context = mgcp
line => aaln/1
line => aaln/2
line => aaln/3
line => aaln/4
line => aaln/5
line => aaln/6
line => aaln/7
line => aaln/8
```

```
[172.16.2.201]
host = 172.16.2.201
context = mgcp
line => aaln/1
```

```
[172.16.2.202]
host = 172.16.2.202
context = mgcp
line => aaln/1
```

```
[172.16.2.203]
host = 172.16.2.203
context = mgcp
line => aaln/1
```

```
[172.16.2.204]
host = 172.16.2.204
context = mgcp
line => aaln/1
```



```
[172.16.2.205]
host = 172.16.2.205
context = mgcp
line => aaln/1
```

extensions.conf

Add extensions for SIP.

```
[sip]
exten => 1001,1,Dial(SIP/1001,20,tr)
exten => 1002,1,Dial(SIP/1002,20,tr)
exten => 1003,1,Dial(SIP/1003,20,tr)
exten => 1004,1,Dial(SIP/1004,20,tr)
exten => 2001,1,Dial(SIP/2001,20,tr)
exten => 2002,1,Dial(SIP/2002,20,tr)
exten => 2003,1,Dial(SIP/2003,20,tr)
exten => 2004,1,Dial(SIP/2004,20,tr)
exten => 3001,1,Dial(SIP/3001,20,tr)
exten => 1,1,Dial(SIP/fxo1,20,tr)
exten => 2,1,Dial(SIP/fxo2,20,tr)
exten => 3,1,Dial(SIP/fxo3,20,tr)
exten => 4,1,Dial(SIP/fxo4,20,tr)
```

Add extensions for MGCP.

```
[mgcp]
exten => 1001,1,Dial(MGCP/aa1n/1@172.16.2.237)
exten => 1002,1,Dial(MGCP/aa1n/2@172.16.2.237)
exten => 1003,1,Dial(MGCP/aa1n/3@172.16.2.237)
exten => 1004,1,Dial(MGCP/aa1n/4@172.16.2.237)
exten => 1,1,Dial(MGCP/aa1n/5@172.16.2.237)
exten => 2,1,Dial(MGCP/aa1n/6@172.16.2.237)
exten => 3,1,Dial(MGCP/aa1n/7@172.16.2.237)
exten => 4,1,Dial(MGCP/aa1n/8@172.16.2.237)
exten => 2001,1,Dial(MGCP/aa1n/1@172.16.2.201)
exten => 2002,1,Dial(MGCP/aa1n/1@172.16.2.202)
exten => 2003,1,Dial(MGCP/aa1n/1@172.16.2.203)
```

```

exten => 2004,1,Dial(MGCP/aaln/1@172.16.2.204)
exten => 3001,1,Dial(MGCP/aaln/1@172.16.2.205)

```

### 3.7.3 Configuring Vigor 3300V

#### 3.7.3.1 SIP Configuration

##### 1. SIP Proxy

**VoIP - Protocol**

Select Protocol:  SIP  MGCP

**SIP Configuration** | MGCP Configuration

SIP Local Port:

#	Active	Outbound Proxy	Proxy Name	Proxy Address	Proxy Port	Registrar Addr	Registrar Port	Expires (sec)	Domain
1.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Asterisk	172.16.2.234	5060	172.16.2.234	5060	300	172.16.2.234
2.	<input type="checkbox"/>	<input type="checkbox"/>		0	5060	0	5060	300	0
3.	<input type="checkbox"/>	<input type="checkbox"/>		0	5060	0	5060	300	0
Example			iptel	iptel.org		iptel.org			iptel.org

Figure 3-41. SIP configuration

##### 2. Port Setting

Configure each port in Vigor 3300V. For example, the setting for port 1 shows as below. Input the correct data to Username, Password, Display Name, Authentication ID and Proxy Server. The VoIP IP Address should be selected to LAN1/VPN in the scenario, because the Asterisk server is placed on LAN.

**VoIP - Port Settings - Port1 - Edit**

**Port 1 (FXS)**

Disable  Enable

Username:

Password:

Display Name:

Authentication ID:

Proxy Server:

VoIP IP Address:

Figure 3-42. Port setting-edit

Choose the “SIP INFO” for DTMF Mode to meet the Asterisk setting.

**DTMF**

DTMF Mode:  InBand  OutBand(RFC2833)  SIP INFO Cisco

DTMF Volume:  (Range: 0 - 31)

**Call Forwarding**

Disable

Call forwarding all calls

Call forwarding busy

Call forwarding no answer after  rings (Range:1-10)

SIP URL:  (Example: 8001@iptel.org)

Figure 3-43. DTMF mode

**VoIP - Port Settings**

Phone Number		Group					
#	Edit	Type	Active	Group	Username	Proxy	Codec
1		FXS	V	1	1001	Asterisk	G.729A-8kbps
2		FXS	V	2	1002	Asterisk	G.729A-8kbps
3		FXS	V	3	1003	Asterisk	G.729A-8kbps
4		FXS	V	4	1004	Asterisk	G.729A-8kbps
5		FXO	V	5	fxo1	Asterisk	G.729A-8kbps
6		FXO	V	6	fxo2	Asterisk	G.729A-8kbps
7		FXO	V	7	fxo3	Asterisk	G.729A-8kbps
8		FXO	V	8	fxo4	Asterisk	G.729A-8kbps

Figure 3-44. Port setting configuration

### 3.7.3.2 MGCP Configuration

1. Configure VoIP IP Address to LAN1/VPN for each port in the scenario, because the Asterisk server is placed on LAN.

**VoIP - Port Settings - Port1 - Edit**

**Port 1 (FXS)**

Disable  Enable

Username:

Password:

Display Name:

Authentication ID:

Proxy Server: Asterisk

VoIP IP Address: LAN1/VPN

Figure 3-45. VoIP IP address

## 2. Configuring the Call Agent IP address.

**VoIP - Protocol**

Select Protocol:  SIP  MGCP

SIP Configuration **MGCP Configuration**

MGCP Local Port:

**MGCP Call Agent Address:**

MGCP Call Agent Port:

EndPoint Name Style:  aaln#@[ip\_addr]  mac\_addr#@[ip\_addr]  aaln#@[mac\_addr]

aaln#@

Wild-carded RSIP:  Each endpoint sends its own RSIP  Send only one wild RSIP

Figure 3-46. MGCP call agent address

# Chapter 4. Load Balance Policy

This chapter is divided into the following sections,

Section 4.1: Introduction

Section 4.2: Examples and Web Configurations

## 4.1 Introduction

This feature allows specific outgoing traffic (defined by IP, port or protocol) to be always sent to through fixed WAN interface which is available.

## 4.2 Examples and Web Configurations

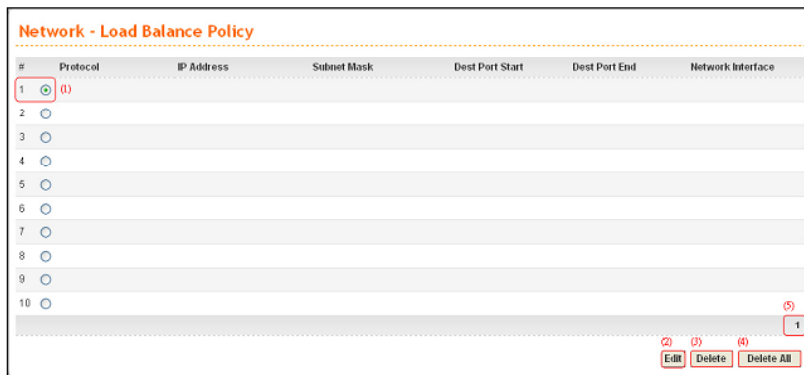


Figure 4-1. Load balance policy of network

(1) After clicking the appropriate index number, you can edit or delete the corresponding entry.

(2) The Network - Load Balance Policy – Edit page appears after you click the Edit button. Click the Apply button to save the current settings.

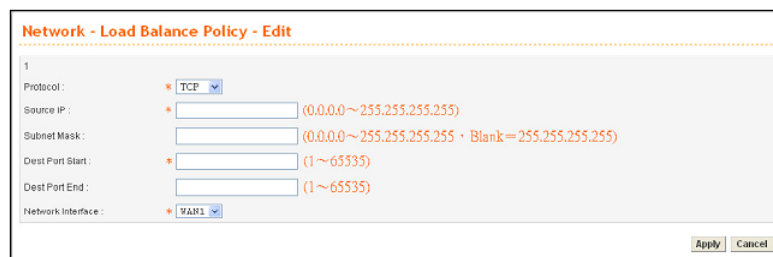


Figure 4-2. Edit item

### Note

*Fields with \* are required to be filled in. The letters in ( ) indicate the range and style of the value you can type.*

If the select **TCP** or **UDP** protocol, you need to enter the port numbers in the **Dest Port Start** field. When you select other protocols from Protocol's pull-down menu, the **Dest**

**Port Range** will be gray marked. It is because these protocols have been pre-defined as follows. Please refer to Table 4-1.

Table 4-1. Selected protocol

	<b>Protocol</b>	<b>Port</b>
FTP	TCP	21
TFTP	UDP	69
HTTP	TCP	80
SMTP	TCP	25
POP3	TCP	110

Load Balance Policy will compare the packets by the rules from the first item. When one entry coincides with another entry, the one which has the smallest index number takes precedence over all other identical entries.

(3) Click the **Delete** button to remove the specified entry. You will see the following window as Figure 4-3.

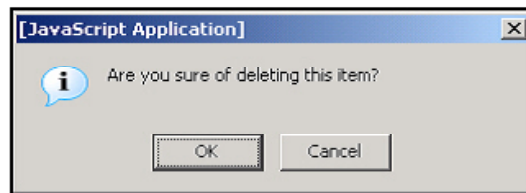


Figure 4-3. Delete item

(4) Click the **Delete All** button to delete all entries. You will see the following window as Figure 4-4.

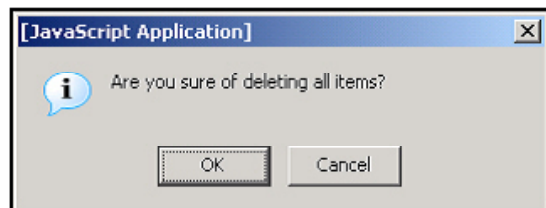


Figure 4-4. Delete all item

(5) It shows the current page number. There are ten entries in one page. The 2 appears after the 10th entry is set up.



Figure 4-5. Second page

Click on 2 to jump to the second page, and so on. We recommend setting up to 50 entries at most to ensure a good performance in Vigor 3300 router.

Network - Load Balance Policy						
#	Protocol	IP Address	Subnet Mask	Dest Port Start	Dest Port End	Network Interface
11	<input type="radio"/>					
12	<input type="radio"/>					
13	<input type="radio"/>					
14	<input type="radio"/>					
15	<input type="radio"/>					
16	<input type="radio"/>					
17	<input type="radio"/>					
18	<input type="radio"/>					
19	<input type="radio"/>					
20	<input type="radio"/>					

Figure 4-6. Second page

### Load Balance Policy – Configuration Example

Suppose the subnets of the company are listed in the Table 4-2 below (Please refer to **Multiple WAN** for detailed configuration). MIS has the following requests. Web sites (HTTP Protocol) or Servers are applied to WAN1, Directors or MIS are applied to WAN2, other departments or DHCP clients are applied to WAN3. FTP sites (FTP Protocol) are applied to WAN3. The Mail Server is always applied to WAN1.

Table 4-2. Subnets of the company

IP Address	Subnet Mask	User	IP Number
192.168.33.0	255.255.255.0	This Network	255
192.168.33.11	255.255.255.255	Mail Server	1
192.168.33.16~31	255.255.255.240	Administrator	16
192.168.33.32~63	255.255.255.224	MIS	32
192.168.33.64~95	255.255.255.224	Accounting Department	32
192.168.33.96~127	255.255.255.224	Business Department	32
192.168.33.128~191	255.255.255.192	RD Department	64
192.168.33.192~254	255.255.255.192	DHCP	63

Network - Load Balance Policy						
#	Protocol	IP Address	Subnet Mask	Dest Port Start	Dest Port End	Network Interface
1	<input checked="" type="radio"/> HTTP	192.188.33.1	255.255.255.240			WAN1
2	<input type="radio"/> HTTP	192.188.33.16	255.255.255.240			WAN2
3	<input type="radio"/> HTTP	192.188.33.32	255.255.255.224			WAN2
4	<input type="radio"/> HTTP	192.188.33.0	255.255.255.0			WAN3
5	<input type="radio"/> FTP	192.188.33.0	255.255.255.0			WAN3
6	<input type="radio"/> TCP	192.188.33.11		1	65535	WAN1
7	<input type="radio"/> UDP	192.188.33.11	255.255.255.255	1	65535	WAN1
8	<input type="radio"/>					
9	<input type="radio"/>					
10	<input type="radio"/>					

Figure 4-7. The settings of Load Balance Policy

**Policy 1**

For computers (Server) with IP range from 192.168.33.1 to 192.168.33.15, with HTTP protocol traffics are applied to WAN1 interface.

**Policy 2**

For computers (Directors) with IP range from 192.168.33.16 to 192.168.33.31, with HTTP protocol traffics are applied to WAN2 interface.

**Policy 3**

For computers (MIS) with IP range from 192.168.33.32 to 192.168.33.63, with HTTP protocol traffics are applied to WAN2 interface.

**Policy 4**

For other computers with IP range from 192.168.33.0 to 192.168.33.255, with HTTP traffics are applied to WAN3 interface. (The network set in this policy covers the network set in Policy1~ Policy3). And the protocol is also the HTTP protocol. However the Load Balance Policy will compare the traffics with the policy rules item by item from the smallest index number rule. So although the settings are overlapped, actually these policies can work normally. For an easy management you may set separate IP range for each policy.

**Policy 5**

For all the computers with IP range from 192.168.33.0 to 192.168.33.255, with FTP protocol traffics are applied to WAN3 interface.

**Policy 6**

For a computer (Mail Server) with IP address 192.168.33.11, with TCP Port 1~65535 are applied to WAN1 interface (The Subnet Mask is empty to be equal to 255.255.255.255).

**Policy 7**

For a computer (Mail Server) with IP range 192.168.33.11, with UDP Port 1~65535 are applied to WAN1 interface.



# Chapter 5. 802.1Q VLAN

## 5.1 VLAN Overview

Virtual LANs (VLANs) are logical, independent workgroups within a network. These workgroups communicate as if they had a physical connection to the network. However, VLANs are not limited by the hardware constraints that physically connect traditional LAN segments to a network. As a result, VLANs allow the network manager to segment the network with a logical, hierarchical structure. VLANs can define a network by application or department. For instance, in the enterprise, a company might create one VLAN for multimedia users and another for e-mail users; or a company might have one VLAN for its Engineering Department, another for its Marketing Department, and another for its guest who can only use Internet not Intranet. VLANs can also be set up according to the organization structure within a company. For example, the company president might have his own VLAN, his executive staff might have a different VLAN, and the remaining employees might have yet a different VLAN. VLANs can also set up according to different company in the same building to save the money and reduce the device establishment.

The Figure 5-1 shows the IEEE 802.1Q tag frame and its insertion point within the Ethernet and 802.3 frames. The 802.1Q tag contains 3 priority bits and 12 VLAN ID bits. The 3 priority bits are for 802.1P. Ethernet switches and endpoints must be capable of interpreting the 802.1Q tag to make use of the tag. If an Ethernet switch or an endpoint cannot interpret the 802.1Q tag, the presence of the tag may cause problems.

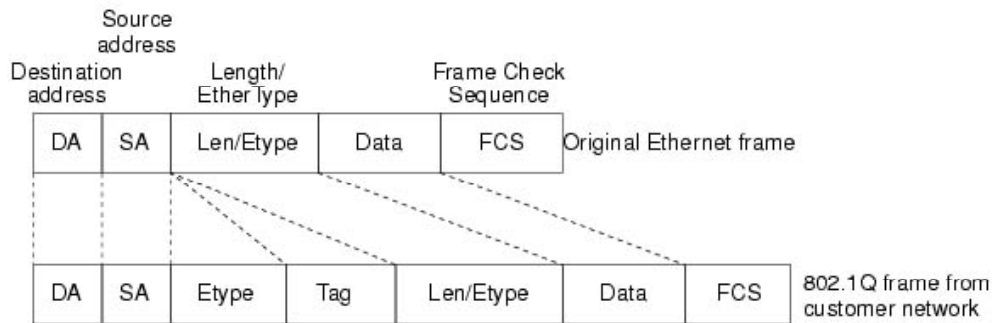


Figure 5-1. Untagged and 802.1Q-Tagged Ethernet frames

## 5.2 VLAN Trunk

A more efficient approach to combine multiple VLAN in a port to allow connect more switches spreading the network. A VLAN trunk consolidates the traffic of multiple VLANs across a single physical port, as shown in Figure 5-2.

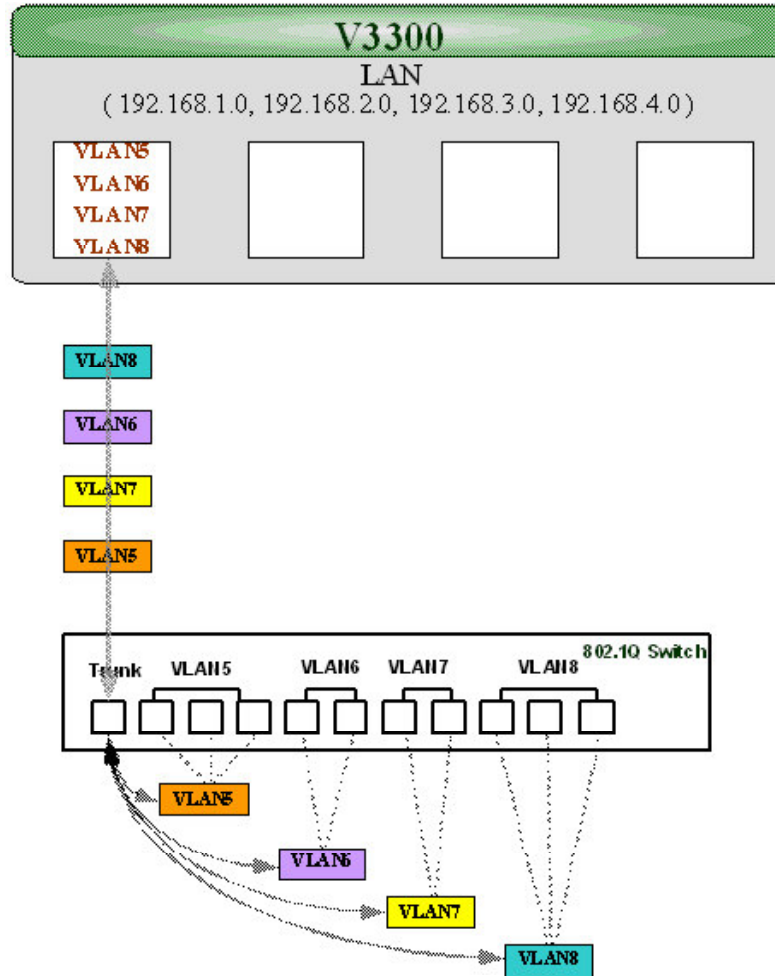


Figure 5-2. VLAN trunk

## 5.3 Why Use VLANs?

- **Security**

VLANs is a communication control. Once a user is assigned to a VLAN, the user only can communicate with the same VLAN group members.

- **Administrative Control for Flexibility and scalability**

Typically, subnets are defined by their physical location. Users have the same subnet in the same area. But VLANs allow each port on a router defines a different subnet. This results that users in the same departments but in different physical locations get the same subnet IP address.

- **Broadcast control for Performance Improvement**

TCP/IP network protocols and most other protocols broadcast frames periodically to advertise or discover network resources. This can have a significant impact on the network performance with a large number of end users. VLANs can prevent traffic from flooding the entire network. Nowadays, many virus attacks influence the network traffic. Using VLANs to avoid extending the virus.

## 5.4 LAN to LAN Communication

The Vigor 3300 allow users to setup the LAN to LAN communication. For instance, a company might create multiple subnet for employees and wish they can communicate with each other. The administrator should allow the LAN to LAN communication. On the other hand, a company does not allow communicate with different department. The administrator should block the LAN to LAN communication.

Configure firewall to allow or deny LAN to LAN communication. Add following setting to block different VLAN communication.

**Firewall - IP Filter Table**

Group Name :   
 Next Group Name :   
 Comment :

IP Filter Table											
Index	Source IP	Subnet Mask	Port	Destination IP	Subnet Mask	Port	Protocol	Direction	Block	Active	
1	any			any			any protocol	LAN to LAN	Block immediately	<input checked="" type="checkbox"/>	

Figure 5-3. IP Filter table

**Firewall - IP Filter - Edit Filter Rule**

Active

Source :  
 IP :   
 Subnet Mask :   
 Port :   -

Destination :  
 IP :   
 Subnet Mask :   
 Port :   -

Group Name :   
 Protocol :   
 Direction :   
 Fragment :

**Action**  
 Block or Pass :   
 Next Group Name :

Figure 5-4. IP Filter setting

## 5.5 Management Port

The management port can help user to always communicate with router even though configuring the wrong setting in the 802.1Q VLAN. The management port is fixed on the P4 of LAN. We recommend that users enable the management port, unless users want to use the fourth VLAN and ensure the setting is correct.

**Advanced - LAN VLAN Setting**

Disable  Port Base VLAN  802.1Q VLAN

Port Base VLAN: **802.1Q VLAN**

Index	Active	Name	VLAN ID	Member				Frame Tag Operation			
				P1	P2	P3	P4	P1	P2	P3	P4
1	<input type="checkbox"/>	VLAN5	5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Untagged	Tagged	Tagged	Tagged
2	<input type="checkbox"/>	VLAN6	6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tagged	Untagged	Tagged	Tagged
3	<input type="checkbox"/>	VLAN7	7	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Untagged	Tagged
4	<input checked="" type="checkbox"/>	VLAN8	8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Tagged	Tagged	Tagged	Untagged

Management Port:

Port Setting

Port VLAN ID	P1: 5	P2: 6	P3: 7	P4: 8
--------------	-------	-------	-------	-------

Apply Reset Cancel

Figure 5-5. LAN VLAN setting

### **Application 1:**

A company wants to separate the Engineer Department, Sales Department, Marketing Department and Other Department to limit their communication with each other to ensure the security. So, we defined four VLANs that are VLAN5, VLAN6, VLAN7 and VLAN8. The subnet of VLAN5 is 192.168.1.0, the subnet of VLAN6 is 192.168.2.0, the subnet of VLAN7 is 192.168.3.0, and the subnet of VLAN8 is 192.168.4.0. However, each PC in the company does not support 802.1Q.

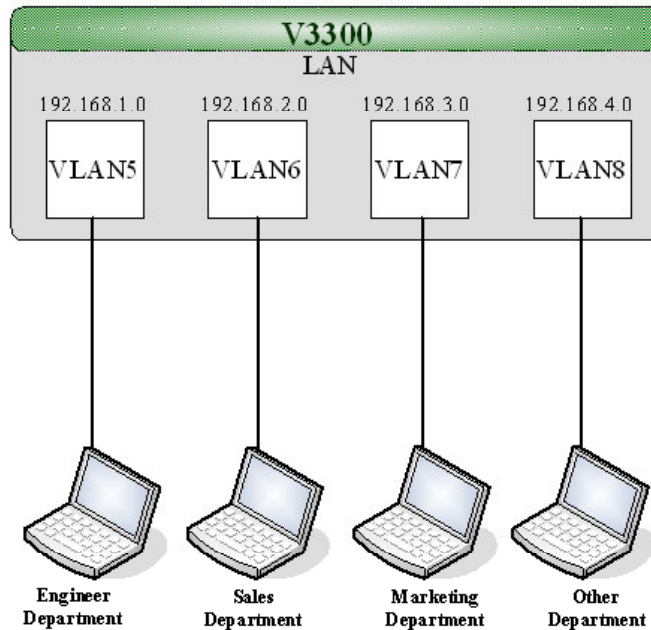


Figure 5-6. Application 1

### Configuration:

1. Block LAN-to-LAN communication.
2. Create VLAN5, VLAN6, VLAN7 and VLAN8 Groups.
3. In the VLAN5, input “5” to VLAN ID. In the Member field, choose p1. Then choose the “Untagged” for Frame Tag Operation in p1. We should configure the PVID to “5”, because the device does not support 802.1Q VLAN.
4. In the VLAN6, input “6” to VLAN ID. In the Member field, choose p2. Then choose the “Untagged” for Frame Tag Operation in p2. We should configure the PVID to “6”, because the device does not support 802.1Q VLAN.
5. In the VLAN7, input “7” to VLAN ID. In the Member field, choose p3. Then choose the “Untagged” for Frame Tag Operation in p3. We should configure the PVID to “7”, because the device does not support 802.1Q VLAN.
6. In the VLAN8, input “8” to VLAN ID. In the Member field, choose p4. Then choose the “Untagged” for Frame Tag Operation in p4. We should configure the PVID to “8”, because the device does not support 802.1Q VLAN.
7. After applying the settings, the web page will be redirected to “reboot” web page. User can ignore it and continue to configure the Network setting. After Network setting, then you can do the reboot procedure.

### Note

After rebooting, the tagged ports will only communicate with 802.1Q tagged devices.

Advanced - LAN VLAN Setting

Disable  Port Base VLAN  802.1Q VLAN

Port Base VLAN: 802.1Q VLAN

Index	Active	Name	VLAN ID	Member				Frame Tag Operation			
				P1	P2	P3	P4	P1	P2	P3	P4
1	<input checked="" type="checkbox"/>	VLAN5	5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Untagged	Tagged	Tagged	Tagged
2	<input checked="" type="checkbox"/>	VLAN6	6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tagged	Untagged	Tagged	Tagged
3	<input checked="" type="checkbox"/>	VLAN7	7	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Untagged	Tagged
4	<input checked="" type="checkbox"/>	VLAN8	8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Tagged	Tagged	Tagged	Untagged

Management Port:

Port Setting

Port VLAN ID	P1	P2	P3	P4
	5	6	7	8

Apply Reset Cancel

Figure 5-7. LAN VLAN configuration

8. In the Network setting, input the subnet 192.168.1.0 to LAN. For example, the VLAN5 LAN IP is 192.168.1.1 and Subnet Mask is 255.255.255.0. Then, users in the Engineer Department can set IP address from 192.168.1.2 to 192.168.1.254.

**Network - LAN**

LAN IP/DHCP | LAN2 IP/DHCP | LAN3 IP/DHCP | LAN4 IP/DHCP | DHCP Relay Agent | IP Routing

**IP Configuration**

IP Address :

Subnet Mask :

**DHCP Server**

Status :  Enable  Disable  Relay Agent

Start IP :

End IP :

Primary DNS :

Secondary DNS :

Lease Time (Min) :

Gateway IP(Optional) :

Figure 5-8. LAN IP configuration

- In the Network setting, input the subnet 192.168.2.0 to LAN2. For example, the VLAN6 LAN IP is 192.168.2.1 and Subnet Mask is 255.255.255.0. Then, users in the Engineer Department can set IP address from 192.168.2.2 to 192.168.2.254.

**Network - LAN**

LAN IP/DHCP | LAN2 IP/DHCP | LAN3 IP/DHCP | LAN4 IP/DHCP | DHCP Relay Agent | IP Routing

**IP Configuration**

IP Address :

Subnet Mask :

**DHCP Server**

Status :  Enable  Disable  Relay Agent

Start IP :

End IP :

Primary DNS :

Secondary DNS :

Lease Time (Min) :

Gateway IP(Optional) :

Figure 5-9. LAN2 IP configuration

- In the Network setting, input the subnet 192.168.3.0 to LAN3. For example, the VLAN7 LAN IP is 192.168.3.1 and Subnet Mask is 255.255.255.0. Then, users in the Engineer Department can set IP address from 192.168.3.2 to 192.168.3.254.

**Network - LAN**

LAN IP/DHCP | LAN2 IP/DHCP | **LAN3 IP/DHCP** | LAN4 IP/DHCP | DHCP Relay Agent | IP Routing

**IP Configuration**

IP Address : 192.168.3.1

Subnet Mask : 255.255.255.0

**DHCP Server**

Status :  Enable  Disable  Relay Agent

Start IP : 192.168.3.10

End IP : 192.168.3.200

Primary DNS :

Secondary DNS :

Lease Time (Min) : 1440

Gateway IP(Optional) :

Figure 5-10. LAN3 IP configuration

11. In the Network setting, input the subnet 192.168.4.0 to LAN4. For example, the VLAN8 LAN IP is 192.168.4.1 and Subnet Mask is 255.255.255.0. Then, users in the Engineer Department can set IP address from 192.168.4.2 to 192.168.4.254.

**Network - LAN**

LAN IP/DHCP | LAN2 IP/DHCP | LAN3 IP/DHCP | **LAN4 IP/DHCP** | DHCP Relay Agent | IP Routing

**IP Configuration**

IP Address : 192.168.4.1

Subnet Mask : 255.255.255.0

**DHCP Server**

Status :  Enable  Disable  Relay Agent

Start IP : 192.168.4.10

End IP : 192.168.4.200

Primary DNS :

Secondary DNS :

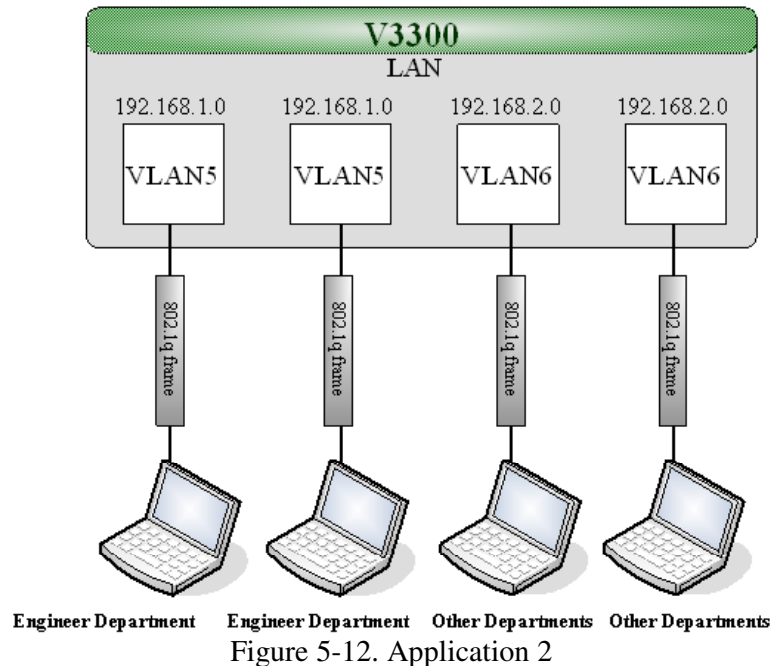
Lease Time (Min) : 1440

Gateway IP(Optional) :

Figure 5-11. LAN4 IP configuration

**Application 2:**

A company wants to separate the Engineer Department and Other Departments to limit their communication to ensure the engineering data. So, we defined two VLANs that are VLAN5 and VLAN6, the subnet of VLAN5 is 192.168.1.0, and the subnet of VLAN6 is 192.168.2.0.



### **Configuration:**

1. Block LAN-to-LAN communication.
2. Create VLAN5 and VLAN6 Groups.
3. In the VLAN5, input “5” to VLAN ID. In the Member field, choose p1 and p2. Then choose the “Tagged” for Frame Tag Operation in p1 and p2. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from the PC of Engineer Department.
4. In the VLAN6, input “6” to VLAN ID. In the Member field, choose p3 and p4. Then choose the “Tagged” for Frame Tag Operation in p3 and p4. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from other departments.
5. After applying the settings, the web page will be redirected to “reboot” web page. User can ignore it and continue to configure the Network setting. After Network setting, then you can do the reboot procedure.

**Note** After rebooting, the tagged ports will only communicate with 802.1Q tagged devices.



**Advanced - LAN VLAN Setting**

Disable  Port Base VLAN  802.1Q VLAN

Port Base VLAN **802.1Q VLAN**

Group

Index	Active	Name	VLAN ID	Member				Frame Tag Operation			
				P1	P2	P3	P4	P1	P2	P3	P4
1	<input checked="" type="checkbox"/>	VLAN5	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Tagged	Tagged
2	<input checked="" type="checkbox"/>	VLAN6	6	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Tagged	Tagged	Tagged	Tagged
3	<input type="checkbox"/>	VLAN7	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Untagged	Tagged
4	<input type="checkbox"/>	VLAN8	8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Tagged	Untagged

Management Port:

Port Setting

Port VLAN ID P1: 5 P2: 6 P3: 7 P4: 8

Apply Reset Cancel

Figure 5-13. LAN VLAN configuration

- In the Network setting, input the subnet 192.168.1.0 to LAN. For example, the VLAN5 LAN IP is 192.168.1.1 and Subnet Mask is 255.255.255.0. Then, users in the Engineer Department can set IP address from 192.168.1.2 to 192.168.1.254.

**Network - LAN**

LAN IP/DHCP LAN2 IP/DHCP LAN3 IP/DHCP LAN4 IP/DHCP DHCP Relay Agent IP Routing

IP Configuration

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

DHCP Server

Status:  Enable  Disable  Relay Agent

Start IP: 192.168.1.10

End IP: 192.168.1.200

Primary DNS:

Secondary DNS:

Lease Time (Min): 1440

Gateway IP(Optional):

Figure 5-14. LAN IP configuration

- In the Network setting, input the subnet 192.168.2.0 to LAN2. For example, the VLAN6 LAN IP is 192.168.2.1 and Subnet Mask is 255.255.255.0. Then, users in the other departments can set IP address from 192.168.2.2 to 192.168.2.254.

**Network - LAN**

LAN IP/DHCP LAN2 IP/DHCP LAN3 IP/DHCP LAN4 IP/DHCP DHCP Relay Agent IP Routing

IP Configuration

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

DHCP Server

Status:  Enable  Disable  Relay Agent

Start IP: 192.168.2.10

End IP: 192.168.2.200

Primary DNS:

Secondary DNS:

Lease Time (Min): 1440

Gateway IP(Optional):

Figure 5-15. LAN2 IP configuration

### **Application 3:**

There are four companies in the same building. They share the broadband network and use the Vigor 3300V router to achieve the load balance, security, and VoIP features. So, we defined four VLANs that are VLAN5, VLAN6, VLAN7 and VLAN8, the subnet of VLAN5 is 192.168.1.0, the subnet of VLAN6 is 192.168.2.0, the subnet of VLAN7 is 192.168.3.0, and the subnet of VLAN8 is 192.168.4.0.

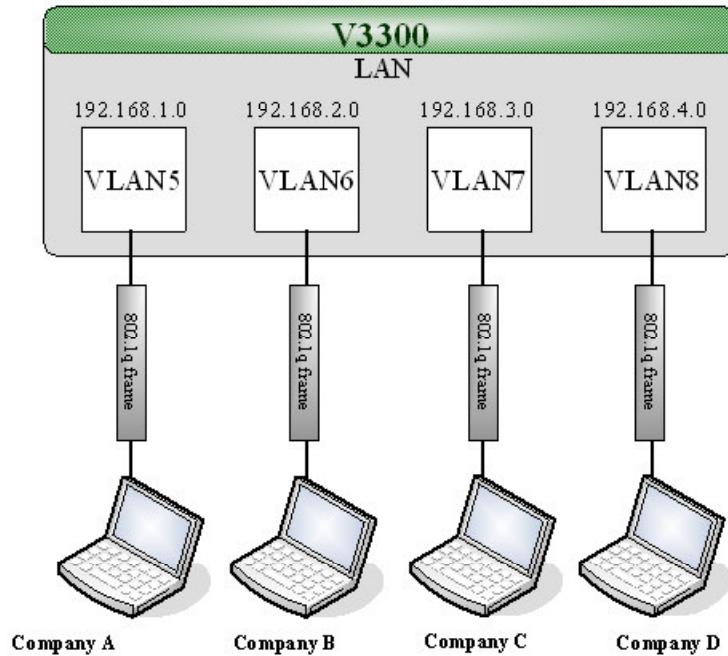


Figure 5-16. Application 3

### **Configuration:**

1. Block LAN-to-LAN communication.
2. Create VLAN5, VLAN6, VLAN7 and VLAN8 Groups.
3. In the VLAN5, input “5” to VLAN ID. In the Member field, choose p1. Then choose the “Tagged” for Frame Tag Operation in p1. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from the PC of company A.
4. In the VLAN6, input “6” to VLAN ID. In the Member field, choose p2. Then choose the “Tagged” for Frame Tag Operation in p2. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from company B.
5. In the VLAN7, input “7” to VLAN ID. In the Member field, choose p3. Then choose the “Tagged” for Frame Tag Operation in p3. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from the PC of company C.
6. In the VLAN8, input “8” to VLAN ID. In the Member field, choose p4. Then choose the “Tagged” for Frame Tag Operation in p4. We can ignore the PVID

(Port VLAN ID), because 802.1q tag will be inserted to the frame from company D.

- After applying the settings, the web page will be redirect to “reboot” web page. User can ignore it and continue to configure the Network setting. After Network setting, then you can do the reboot procedure.

**Note** After rebooting, the tagged ports will only communicate with 802.1Q tagged devices.

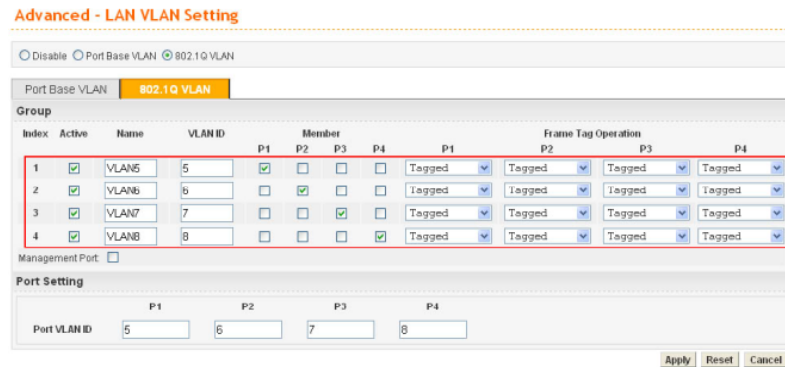


Figure 5-17. LAN VLAN setting

The network configuration is the same with application 1. Please refer to application 1 part.

#### **Application 4:**

A company wants to separate the Engineer Department, Sales Department, Marketing Department and guest to limit their communication with any department to ensure the security. So, we defined four VLANs that are VLAN5, VLAN6, VLAN7 and VLAN8, the subnet of VLAN5 is 192.168.1.0, the subnet of VLAN6 is 192.168.2.0, the subnet of VLAN7 is 192.168.3.0, and the subnet of VLAN8 is 192.168.4.0. However, the notebook of guest does not support 802.1Q.

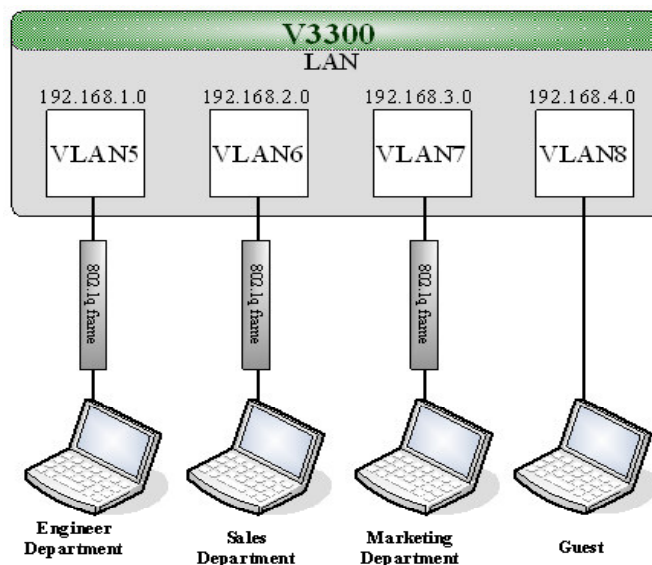


Figure 5-18. Application 4

## **Configuration:**

1. Block LAN-to-LAN communication.
2. Create VLAN5, VLAN6, VLAN7 and VLAN8 Groups.
3. In the VLAN5, input “5” to VLAN ID. In the Member field, choose p1. Then choose the “Tagged” for Frame Tag Operation in p1. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from the PC of Engineer Department.
4. In the VLAN6, input “6” to VLAN ID. In the Member field, choose p2. Then choose the “Tagged” for Frame Tag Operation in p2. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from Engineer Department.
5. In the VLAN7, input “7” to VLAN ID. In the Member field, choose p3. Then choose the “Tagged” for Frame Tag Operation in p3. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from the PC of Engineer Department.
6. In the VLAN8, input “8” to VLAN ID. In the Member field, choose p4. Then choose the “Untagged” for Frame Tag Operation in p4. We should configure the PVID to “8”, because the device does not support 802.1Q VLAN.
7. After applying the settings, the web page will be redirected to “reboot” web page. User can ignore it and continue to configure the Network setting. After Network setting, then you can do the reboot procedure.

**Note** After rebooting, the tagged ports will only communicate with 802.1Q tagged devices.

**Advanced - LAN VLAN Setting**

Disable  Port Base VLAN  802.1Q VLAN

Port Base VLAN **802.1Q VLAN**

Index	Active	Name	VLAN ID	Member				Frame Tag Operation			
				P1	P2	P3	P4	P1	P2	P3	P4
1	<input checked="" type="checkbox"/>	VLAN5	5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Tagged	Tagged
2	<input checked="" type="checkbox"/>	VLAN6	6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Tagged	Tagged
3	<input checked="" type="checkbox"/>	VLAN7	7	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Tagged	Tagged
4	<input checked="" type="checkbox"/>	VLAN8	8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Tagged	Tagged	Tagged	Untagged

Management Port:

**Port Setting**

P1	P2	P3	P4
Port VLAN ID: 5	6	7	8

Apply Reset Cancel

Figure 5-19. LAN VLAN setting

The network configuration is the same with application 1. Please refer to application 1 part.

## **Application 5:**

A company wants to separate the Engineer Department, Sales Department, Marketing Department and other departments to limit their communication with each other to ensure the security. Many employees of the company use some switches supported 802.1Q

VLAN to expand the network. So, we defined four VLANs that are VLAN5, VLAN6, VLAN7 and VLAN8, each LAN port is Trunk port which supports multiple VLAN, the subnet of VLAN5 is 192.168.1.0, the subnet of VLAN6 is 192.168.2.0, the subnet of VLAN7 is 192.168.3.0, and the subnet of VLAN8 is 192.168.4.0.

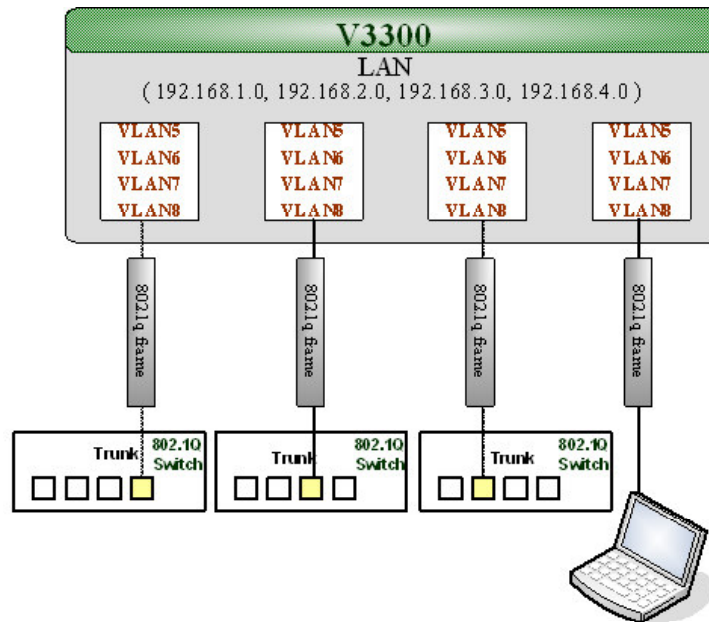


Figure 5-20. Application 5

**Configuration:**

1. Block LAN-to-LAN communication.
2. Create VLAN5, VLAN6, VLAN7 and VLAN8 Groups.
3. In the VLAN5, input “5” to VLAN ID. In the Member field, choose p1, p2, p3 and p4. Then choose the “Tagged” for Frame Tag Operation in p1, p2, p3 and p4. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from the switch.
4. In the VLAN6, input “6” to VLAN ID. In the Member field, choose p1, p2, p3 and p4. Then choose the “Tagged” for Frame Tag Operation in p1, p2, p3 and p4. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from switch.
5. In the VLAN7, input “7” to VLAN ID. In the Member field, choose p1, p2, p3 and p4. Then choose the “Tagged” for Frame Tag Operation in p1, p2, p3 and p4. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from the switch.
6. In the VLAN8, input “8” to VLAN ID. In the Member field, choose p1, p2, p3 and p4. Then choose the “Tagged” for Frame Tag Operation in p1, p2, p3 and p4. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from some users.
7. After applying the settings, the web page will be redirected to “reboot” web page. User can ignore it and continue to configure the Network setting. After Network setting, then you can do the reboot procedure.

**Note** After rebooting, the tagged ports will only communicate with 802.1Q tagged devices.

### Advanced - LAN VLAN Setting

Disable
  Port Base VLAN
  802.1Q VLAN

Port Base VLAN: 802.1Q VLAN

**Group**

Index	Active	Name	VLAN ID	Member				Frame Tag Operation			
				P1	P2	P3	P4	P1	P2	P3	P4
1	<input checked="" type="checkbox"/>	VLAN5	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Tagged	Tagged	Tagged	Tagged
2	<input checked="" type="checkbox"/>	VLAN6	6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Tagged	Tagged	Tagged	Tagged
3	<input checked="" type="checkbox"/>	VLAN7	7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Tagged	Tagged	Tagged	Tagged
4	<input checked="" type="checkbox"/>	VLAN8	8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Tagged	Tagged	Tagged	Tagged

Management Port:

**Port Setting**

Port VLAN ID:
 P1: 
 P2: 
 P3: 
 P4:

Figure 5-21. LAN VLAN setting

The network configuration is the same with application 1. Please refer to application 1 part.