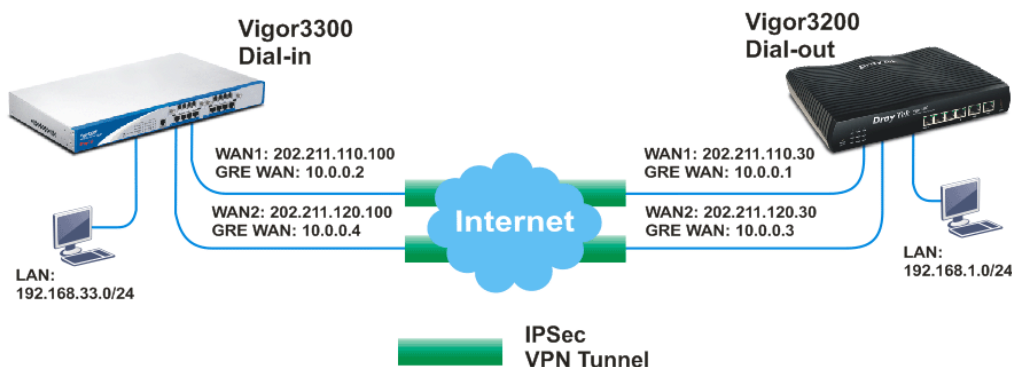


VPN Trunk Load-Balance between Vigor3200 and Other Vigor Router

This section will discuss how to build VPN Trunk with load-balance between Vigor3200 and other router (e.g., Vigor3300).

Scenario 1: One-pair VPN Trunk

The purpose is to setup a VPN trunk between Vigor3200 (192.168.1.0/24) and Vigor3300 (192.168.33.0/24).



At present, Vigor3200 just supports one VPN trunk group with two members for the same VPN network pair. In this case, the VPN trunk is built for 192.168.1.0/24 <-> 192.168.33.0/24. In other word, although Vigor3200 supports 4 WAN connections, it just allows you to use 2 VPN connections over two WAN ports for one VPN trunk group between the networks 192.168.1.0/24 and 192.168.33.0/24.

Note:

- You can still setup two VPN trunk groups over 4 WAN connections between the networks 192.168.1.0/24 and 192.168.33.0/24. But the VPN traffic can just pass through one VPN trunk group.
- You can create arbitrary number of VPN trunk groups between Vigor3200 and Vigor3300 for different VPN network pairs. For example, suppose there is another network (192.168.10.0/24) behind Vigor3300. You may create a VPN trunk group over WAN1 and WAN2 connections for 192.168.1.0/24 <-> 192.168.33.0/24, and the other VPN trunk group over WAN3 and WAN4 for 192.168.1.0/24 <-> 192.168.10.0/24. Please refer to the Scenario 2 described in this document later.

Vigor3200 as a VPN client (dial out site),

LAN: 192.168.1.0/24

WAN 1 IP: 202.211.110.30 (My GRE IP, 10.0.0.1, Peer GRE IP, 10.0.0.2)

WAN 2 IP: 202.211.120.30 (My GRE IP, 10.0.0.3, Peer GRE IP, 10.0.0.4)

Vigor3300 as a VPN server (dial in site),

LAN: 192.168.33.0/24

WAN 1 IP: 202.211.110.100 (Local GRE IP, 10.0.0.2, Remote GRE IP, 10.0.0.1)

WAN 2 IP: 202.211.120.100 (Local GRE IP, 10.0.0.4, Remote GRE IP, 10.0.0.3)

Settings for Vigor 3200:

1. Open **VPN and Remote Access>>>LAN to LAN**. Choose Index number **1** for configuring a VPN LAN to LAN profile.

VPN and Remote Access >> LAN to LAN

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

Index	Name	Status	Index	Name	Status
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X

2. In the following page, please configure the settings as the following figure.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name: wan1_only

Enable this profile

VPN Dial-Out Through: WAN1 Only

Netbios Naming Packet: Pass Block

Multicast via VPN: Pass Block
(for some IGMP, IP-Camera, DHCP Relay..etc.)

Call Direction: Both Dial-Out Dial-in

Always on

Idle Timeout: -1 second(s)

Enable PING to keep alive

PING to the IP: _____

2. Dial-Out Settings

Type of Server I am calling

PPTP

IPsec Tunnel

L2TP with IPsec Policy: None

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

202.211.110.100

Username: ???

Password: _____

PPP Authentication: PAP/CHAP

VJ Compression: On Off

IKE Authentication Method

Pre-Shared Key

IKE Pre-Shared Key: ●●●●●●●●

Digital Signature(X.509)

Peer ID: None

Local ID: _____

Alternative Subject Name First

Subject Name First

Local Certificate: None

IPsec Security Method

Medium(AH)

High(ESP) DES without Authentication

Advanced

Index(1-15) in **Schedule** Setup:

3. Dial-In Settings

Allowed Dial-In Type

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 Authentication Method

Pre-Shared Key

IKE Pre-Shared Key: _____

Digital Signature(X.509)

None

Local ID: _____

Alternative Subject Name First

Subject Name First

IPsec Security Method

Medium(AH)

High(ESP) DES 3DES AES

4. GRE over IPsec Settings

Enable IPsec Dial-Out function GRE over IPsec

Logical Traffic

My GRE IP: 10.0.0.1

Peer GRE IP: 10.0.0.2

5. 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

Local Network IP: 192.168.1.1

Local Network Mask: 255.255.255.0

RIP Direction: Disable

From first subnet to remote network, you have to do: _____

Route

Change default route to this VPN tunnel (Only single WAN supports this)

- Click **OK** to save the configuration and return to previous page. Choose Index number **2** for configuring another VPN LAN to LAN profile.

VPN and Remote Access >> LAN to LAN

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

Index	Name	Status	Index	Name	Status
<u>1.</u>	wan1 only	X	<u>17.</u>	???	X
<u>2.</u>	???	X	<u>18.</u>	???	X
<u>3.</u>	???	X	<u>19.</u>	???	X

- In this page, please configure the settings as the following figure.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name: wan2 only

Enable this profile

VPN Dial-Out Through: WAN2 Only

Netbios Naming Packet: Pass Block

Multicast via VPN: Pass Block
(for some IGMP, IP-Camera, DHCP Relay..etc.)

Call Direction: Both Dial-Out Dial-in

Always on:

Idle Timeout: -1 second(s)

Enable PING to keep alive:

PING to the IP: _____

2. Dial-Out Settings

Type of Server I am calling:

PPTP

IPsec Tunnel

L2TP with IPsec Policy: None

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

202.211.120.100

Username: ???

Password: _____

PPP Authentication: PAP/CHAP

VJ Compression: On Off

IKE Authentication Method:

Pre-Shared Key

IKE Pre-Shared Key: ●●●●●●●●

Digital Signature(X.509)

Peer ID: None

Local ID:

Alternative Subject Name First

Subject Name First

Local Certificate: None

IPsec Security Method:

Medium(AH)

High(ESP) DES without Authentication

Advanced

Index(1-15) in Schedule Setup:

3. Dial-In Settings

Allowed Dial-In Type:

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 Authentication Method:

Pre-Shared Key

IKE Pre-Shared Key: _____

Digital Signature(X.509)

None

Local ID:

Alternative Subject Name First

Subject Name First

IPsec Security Method:

Medium(AH)

High(ESP) DES 3DES AES

4. Gre over IPsec Settings

Enable IPsec Dial-Out function GRE over IPsec

Logical Traffic

My GRE IP: 10.0.0.3

Peer GRE IP: 10.0.0.4

5. 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

Local Network IP: 192.168.1.1

Local Network Mask: 255.255.255.0

RIP Direction: Disable

From first subnet to remote network, you have to do:

Route

Change default route to this VPN tunnel (Only single WAN supports this)

- Click **OK** to save the configuration.
- Open **VPN and Remote Access>>VPN TRUNK Management**. Add these VPN profiles to the VPN Trunk and set **Load Balance** as the **Attribute Mode**.

Load Balance Profile List | [Set to Factory Default](#)

Note: [Active:NO] The LAN-to-LAN Profile is disabled or under Dial-In(Call Direction) at present.

No.	Status	Name	Member1 (Active) Type	Member2 (Active) Type
1	v	wan1wan2	1 (YES) IPSec	2 (YES) IPSec

Advanced | wan1wan2

General Setup

Status: **Enable** Disable

Profile Name: wan1wan2

Member1: Please select a LAN-to-LAN Dial-Out profile.

Member2: Please select a LAN-to-LAN Dial-Out profile.

Active Mode: Backup **Load Balance**

Add Edit Delete

- Click **Advanced** for specifying **Load Balance Algorithm**.

VPN Load Balance Advance Settings

Profile Name: Trunk1

Load Balance Algorithm:

Round Robin
 Weighted Round Robin
 Auto Weighted
 According to Speed Ratio (Member1:Member2): 50:50
 Fastest

VPN Load Balance - Binding Tunnel Policy

Create After insert

Tunnel Bind Table Index: (1~400)

Active: In-active/Delete

Binding Dial Out Index: 1

Binding Src IP Start: 0.0.0.0 End: 0.0.0.0

Binding Dest IP Start: 0.0.0.0 End: 0.0.0.0

Binding Dest Port Start: 1 End: 65535

Binding Fragmented: NO Binding Protocol: ANY 0

OK Close

Detail Information

[VPN Load Balance Profile name: Trunk1]
 [Algorithm: Round Robin]

- When the VPN trunk is successfully connected, you may check the connection status by viewing the page of **VPN and Remote Access>>Connection Management**. Transferred packets (Tx Pkts) will keep increasing through both tunnels when outgoing packets sent to the remote VPN network.

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds : Refresh

General Mode:	<input type="text"/>	Dial
Backup Mode:	<input type="text"/>	Dial
Load Balance Mode:	(wan1wan2) 202.211.110.100	Dial

VPN Connection Status

Current Page: 1 Page No. Go >>

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime	
1 (wan1 only)	IPSec Tunnel DES-No Auth	202.211.110.100 via WAN1	192.168.33.0/24	1983	42	3971	60	1:6:10	Drop
2 (wan2 only)	IPSec Tunnel DES-No Auth	202.211.120.100 via WAN2	192.168.33.0/24	2334	18	137	3	1:15:22	Drop

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

Settings for Vigor3300:

- Open **VPN>>IPSec>>VPN Trunk>>Policy Table**. Choose Index **1** and click **Edit**.

VPN - IPSec - VPN Trunk - Policy Table

#	Connection Name	Local GRE IP	Remote Gateway	Remote GRE IP	Interface	Profile Status	Operational Status
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

Refresh Edit Delete Delete All

2. In this page, please configure the settings as the following figure.

VPN - IPSec - VPN Trunk - Policy Table - Edit

Default | Advanced

Basic

Profile Status :

Name :

Authentication :

Preshared Key :

Security Protocol :

NAT Traversal :

Local Gateway

WAN Interface :

Local Certificate :

Security Gateway :

Local GRE IP :

Next hop :

Remote Gateway

Remote ID :

Security Gateway : ('0.0.0.0' for dynamic client)

Remote GRE IP :

3. Click **Apply** to save the configuration and return to previous page. Choose Index 2 for configuring another VPN Trunk policy.
4. In this page, please configure the settings as the following figure.

VPN - IPSec - VPN Trunk - Policy Table - Edit

Default | Advanced

Basic

Profile Status :

Name :

Authentication :

Preshared Key :

Security Protocol :

NAT Traversal :

Local Gateway

WAN Interface :

Local Certificate :

Security Gateway :

Local GRE IP :

Next hop :

Remote Gateway

Remote ID :

Security Gateway : ('0.0.0.0' for dynamic client)

Remote GRE IP :

- Click **Apply** to save the configuration.
- Open **VPN>>VPN Trunk>>Group Table** to group these two VPN policies.

VPN - VPN Trunk - Group Table

#	Profile Status	Name	Local Subnet	Remote Subnet
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"/>			

1

- Choose Index 1 and click **Edit**. Add these two VPN profiles (wan1 and wan2) to a VPN Trunk.

VPN - VPN Trunk - Group Table - Edit

1

Profile Status : Disable Enable

Name :

Local Subnet : /

Remote Subnet : /

Tunnel 1 : Weight :

Tunnel 2 : Weight :

Tunnel 3 : Weight :

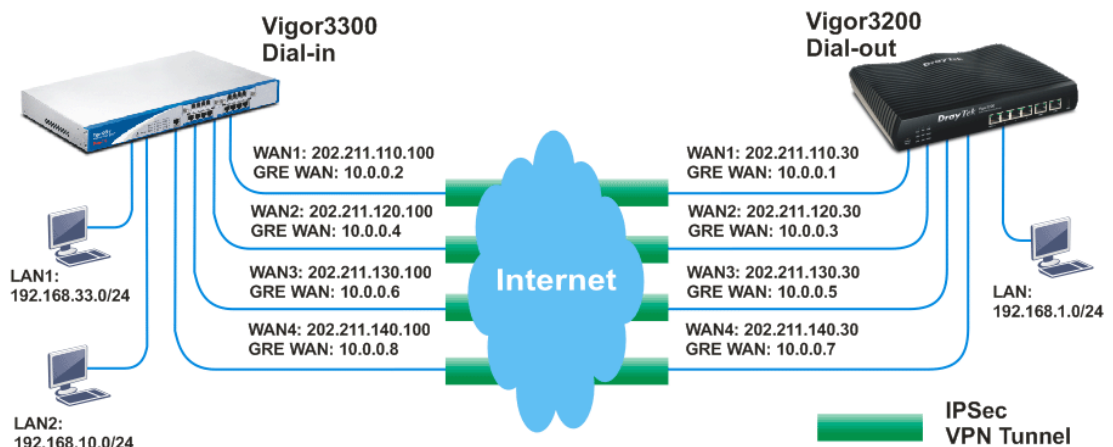
Tunnel 4 : Weight :

Backup

Active	Master	Slave
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

Now, one-pair VPN trunk between Vigor3200 (192.168.1.0/24) and Vigor3300 (192.168.33.0/24) has be established.

Scenario 2: Two-pair VPN Trunk



Vigor3200 as VPN client (dial out site)

LAN: 192.168.1.0/24

WAN 1 IP: 202.211.110.30 (My GRE IP, 10.0.0.1, Peer GRE IP, 10.0.0.2)

WAN 2 IP: 202.211.120.30 (My GRE IP, 10.0.0.3, Peer GRE IP, 10.0.0.4)

WAN 3 IP: 202.211.130.30 (My GRE IP, 10.0.0.5, Peer GRE IP, 10.0.0.6)

WAN 4 IP: 202.211.140.30 (My GRE IP, 10.0.0.7, Peer GRE IP, 10.0.0.8)

Vigor3300 as VPN server (dial in site),

LAN1: 192.168.33.0/24

LAN2: 192.168.10.0/24

WAN 1 IP: 202.211.110.100 (Local GRE IP, 10.0.0.2, Remote GRE IP, 10.0.0.1)

WAN 2 IP: 202.211.120.100 (Local GRE IP, 10.0.0.4, Remote GRE IP, 10.0.0.3)

WAN 3 IP: 202.211.130.100 (Local GRE IP, 10.0.0.6, Remote GRE IP, 10.0.0.5)

WAN 4 IP: 202.211.140.100 (Local GRE IP, 10.0.0.8, Remote GRE IP, 10.0.0.7)

Settings for Vigor 3200:

1. Open **VPN and Remote Access>>>LAN to LAN**.
2. Create LAN to LAN profile 1-4. Setting configuration is the same as Scenario 1. The differences are, Remote Network IP of Profile 1 and Profile 2 must be 192.168.33.0/24 and Remote Network IP of Profile 3 and Profile 4 must be 192.168.10.0/24.

LAN-to-LAN Profiles:

| [Set to Factory Default](#) |

Index	Name	Status	Index	Name	Status
1.	wan1 only	√	17.	???	×
2.	wan2 only	√	18.	???	×
3.	wan3 only	√	19.	???	×
4.	wan4 only	√	20.	???	×
5.	???	×	21.	???	×
6.	???	×	22.	???	×
7.	???	×	23.	???	×
8.	???	×	24.	???	×
9.	???	×	25.	???	×
10.	???	×	26.	???	×
11.	???	×	27.	???	×
12.	???	×	28.	???	×
13.	???	×	29.	???	×

- Open **VPN and Remote Access>>VPN TRUNK Management**. Add these VPN profiles to the VPN Trunk and set **Load Balance** as the **Attribute Mode**. Setting configuration is the same as Scenario 1. Profile 1 and Profile 2 are one pair; Profile 3 and Profile 4 are the other pair.

Load Balance Profile List | [Set to Factory Default](#) |

Note: [Active:NO] The LAN-to-LAN Profile is disabled or under Dial-In(Call Direction) at present.

No.	Status	Name	Member1 (Active) Type	Member2 (Active) Type
1	v	wan1wan2	1 (YES) IPSec	2 (YES) IPSec
2	v	wan3wan4	3 (YES) IPSec	4 (YES) IPSec

Advanced wan1wan2 ▾

General Setup

Status **Enable** **Disable**

Profile Name

Member1

Member2

Active Mode **Backup** **Load Balance**

- When the VPN trunk is successfully connected, you may check the connection status by viewing the page of **VPN and Remote Access>>Connection Management**. Transferred packets (Tx Pkts) will keep increasing through both tunnels when outgoing packets sent to the remote VPN network.

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds :

General Mode:

Backup Mode:

Load Balance Mode:

VPN Connection Status

Current Page: 1

Page No.

VPN	Type	Remote IP	Network	Pkts	Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime	
1 (wan1 only)	IPSec Tunnel DES-No Auth	202.211.110.100 via WAN1	192.168.33.0/24	3393	24	6800	60	1:53:18	<input type="button" value="Drop"/>
2 (wan2 only)	IPSec Tunnel DES-No Auth	202.211.120.100 via WAN2	192.168.33.0/24	3753	39	137	3	2:2:30	<input type="button" value="Drop"/>
3 (wan3 only)	IPSec Tunnel DES-No Auth	202.211.130.100 via WAN3	192.168.10.0/24	3630	39	7213	60	2:2:28	<input type="button" value="Drop"/>
4 (wan4 only)	IPSec Tunnel DES-No Auth	202.211.140.100 via WAN4	192.168.10.0/24	3583	24	0	0	2:2:19	<input type="button" value="Drop"/>

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

Settings for Vigor3300:

1. Open **Advanced>>LAN VLAN**. Choose the tab of **802.1Q VLAN**. Configure the settings as the following figure.

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	20	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Untagged	Tagged	Tagged	Tagged
2	<input checked="" type="checkbox"/>	VLAN6	21	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tagged	Untagged	Tagged	Tagged
3	<input checked="" type="checkbox"/>	VLAN7	22	<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

Enable management port for P4
 Enable packet forwarding between VLANs

Port Setting

Port VLAN ID	P1	P2	P3	P4
	20	21	22	8

Apply Reset Cancel

2. Next, open **Network>>LAN**. Set two LAN subnet: LAN1 192.168.33.0/24 and LAN2 192.168.10.0/24.

Network - LAN

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

IP Configuration

IP Address : 192.168.33.1

Subnet Mask : 255.255.255.0

DHCP Server

Status : Enable Disable Relay Agent

Start IP : 192.168.33.10

End IP : 192.168.33.254

Primary DNS :

Secondary DNS :

Lease Time (Min) : 1440

Gateway IP(Optional) :

Apply Cancel

Network - LAN

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

IP Configuration

IP Address : 192.168.10.1

Subnet Mask : 255.255.255.0

DHCP Server

Status : Enable Disable Relay Agent

Start IP : 192.168.10.10

End IP : 192.168.10.254

Primary DNS :

Secondary DNS :

Lease Time (Min) : 1440

Gateway IP(Optional) :

Apply Cancel

3. Click **Apply**.
4. Open **VPN>>IPSec>>VPN Trunk>>Policy Table** to create VPN Trunk policy.

The way to configure the setting is the same as Scenario 1.

VPN - IPSec - VPN Trunk - Policy Table

#	Connection Name	Local GRE IP	Remote Gateway	Remote GRE IP	Interface	Profile Status	Operational Status
1	<input checked="" type="radio"/> wan1	10.0.0.2	0.0.0.0	10.0.0.1	WAN1	enable	up
2	<input type="radio"/> wan2	10.0.0.4	0.0.0.0	10.0.0.3	WAN2	enable	up
3	<input type="radio"/> wan3	10.0.0.6	0.0.0.0	10.0.0.5	WAN3	enable	up
4	<input type="radio"/> wan4	10.0.0.8	0.0.0.0	10.0.0.7	WAN4	enable	up
5	<input type="radio"/>						
6	<input type="radio"/>						
7	<input type="radio"/>						
8	<input type="radio"/>						
9	<input type="radio"/>						
10	<input type="radio"/>						

1

DrayTek Corp. © 1997 - 2009 All rights reserved. DrayTek Enterprise Network Solutions.

- Open **VPN>>VPN Trunk>>Group Table** to group these VPN policies. Group two VPN policies as the following figure and then click **Apply**. The way to configure the setting is the same as Scenario 1.

VPN - VPN Trunk - Group Table

#	Profile Status	Name	Local Subnet	Remote Subnet
1	<input checked="" type="radio"/> Enable	192.168.33.0	192.168.33.0/24	192.168.1.0/24
2	<input type="radio"/> Enable	192.168.10.1	192.168.10.0/24	192.168.1.0/24
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"/>			

1

DrayTek Corp. © 1997 - 2009 All rights reserved. DrayTek Enterprise Network Solutions.

Now, two-pair VPN trunk between Vigor3200 (192.168.1.0/24) and Vigor3300 (192.168.33.0/24) has be established.