

# ***Vigor3300 Series Application Notes***

**(Part 1)**

**V1.0**

## History Table

[illegible]

# Table of Contents

<b>CHAPTER 1 ADVANCED SPEED DIAL FUNCTION.....</b>	<b>- 4 -</b>
<b>CHAPTER 2 HIGH AVAILABILITY FUNCTION .....</b>	<b>- 6 -</b>
2.1 Introduction.....	- 6 -
2.1 Examples and Web Configurations .....	- 8 -
<b>CHAPTER 3 MULTI-DMZ FUNCTION.....</b>	<b>- 10 -</b>
3.1 Introduction.....	- 10 -
3.2 Web Configurations.....	- 11 -
<b>CHAPTER 4 SIP CALL, PROXY, OUTBOUND PROXY AND DOMAIN ..</b>	<b>- 13 -</b>
4.1 Introduction.....	- 13 -
4.2 Examples and Web Configurations .....	- 14 -
<b>CHAPTER 5 VOIP NAT TRAVERSAL FUNCTION .....</b>	<b>- 22 -</b>
5.1 Introduction.....	- 22 -
5.2 Example and Web configurations .....	- 23 -
<b>CHAPTER 6 MULTI NAT FUNCTION.....</b>	<b>- 30 -</b>
6.1 Introduction.....	- 30 -
6.2 Examples and Web Configurations .....	- 31 -
<b>CHAPTER 7 VOIP INCOMING CALL BARRING FUNCTION .....</b>	<b>- 33 -</b>
7.1 Introduction.....	- 33 -
7.2 Examples and Web configurations .....	- 34 -
<b>CHAPTER 8 PORT MIRRORING FUNCTION .....</b>	<b>- 46 -</b>
8.1 Introduction.....	- 46 -
8.2 Examples and Web Configurations .....	- 47 -
<b>CHAPTER 9 FXO HOT LINE FUNCTION .....</b>	<b>- 48 -</b>
9.1 Introduction.....	- 48 -
9.2 Examples and Web Configurations .....	- 50 -

## CHAPTER 1

# Advanced Speed Dial Function

The feature allows users to create a proprietary dial plan. A dial plan essentially describes the number and pattern of digits that a user dials to reach a particular telephone number. For instance, when user calls a telephone number, the dial plan can help you to append the area codes or strip digits that are in the head of the telephone number.

### *The “Advanced Speed Dial” settings*

- “Prefix” is the prefix pattern that is used to check whether the telephone number needs to be modified. Once the pattern is matched, this number will be revised by following settings – “Strip”, “Append” and “Destination”.
- “Strip” is the strip length that is used to remove the pre-digits from the telephone number.
- “Append” is the number that is used to append the digits after the telephone number.
- “Destination” is the destination address that is used to forward the call to the peer address.
- “Memo” is used to describe the meaning of the entry in the dial plan.

The page is shown in Figure 1-1 and Figure 1-2.

#	Prefix	Strip	Append	Destination	Memo
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

**Figure 1-1. Advanced speed dial setting page**

**VoIP - Advanced Speed Dial - Edit**

---

1

Prefix :

Strip :

Append :

Destination :

Memo :

**Figure 1-2. Advanced speed dial edit page**

We list some examples as followings,

Telephone Number	Prefix	Strip	Append	Destination	SIP URL
012345	0	1		10.1.1.1	<b>12345@10.1.1.1</b>
00212345	0	3		10.1.1.1	<b>12345@10.1.1.1</b>
025	0	2	1234	10.1.1.1	<b>12345@10.1.1.1</b>
0	0	1	8001	iptel.org	<b>8001@iptel.org</b>
5972727	597	0	0028863	draytek.com	<b>00288635972727@draytek.com</b>

For example, at the last number group, the prefix value is “597”, the number is “5972727”; The first three digits “597” of telephone number is matched with the value of Prefix, it will access this number by other settings as “Strip”, “Append” and “Destination”. In this case, the strip value is “0”, so it will not remove any pre digits; The append value is “0028863”, so it will add these digits after the telephone number; Finally, it will add “draytek.com” sting after “@” in this telephone number because the destination value is not empty.

## **CHAPTER 2**

# **High Availability Function**

---

This chapter shows how to setup high availability function.

This chapter is divided into the following sections,

- Section 2.1: Introduction
- Section 2.2: Examples and Web Configurations

## **2.1 Introduction**

The basic application graph is shown in Figure 2-1. There are two Vigor3300V routers connect 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 LAN port. For the further more settings, please refer to the next section.

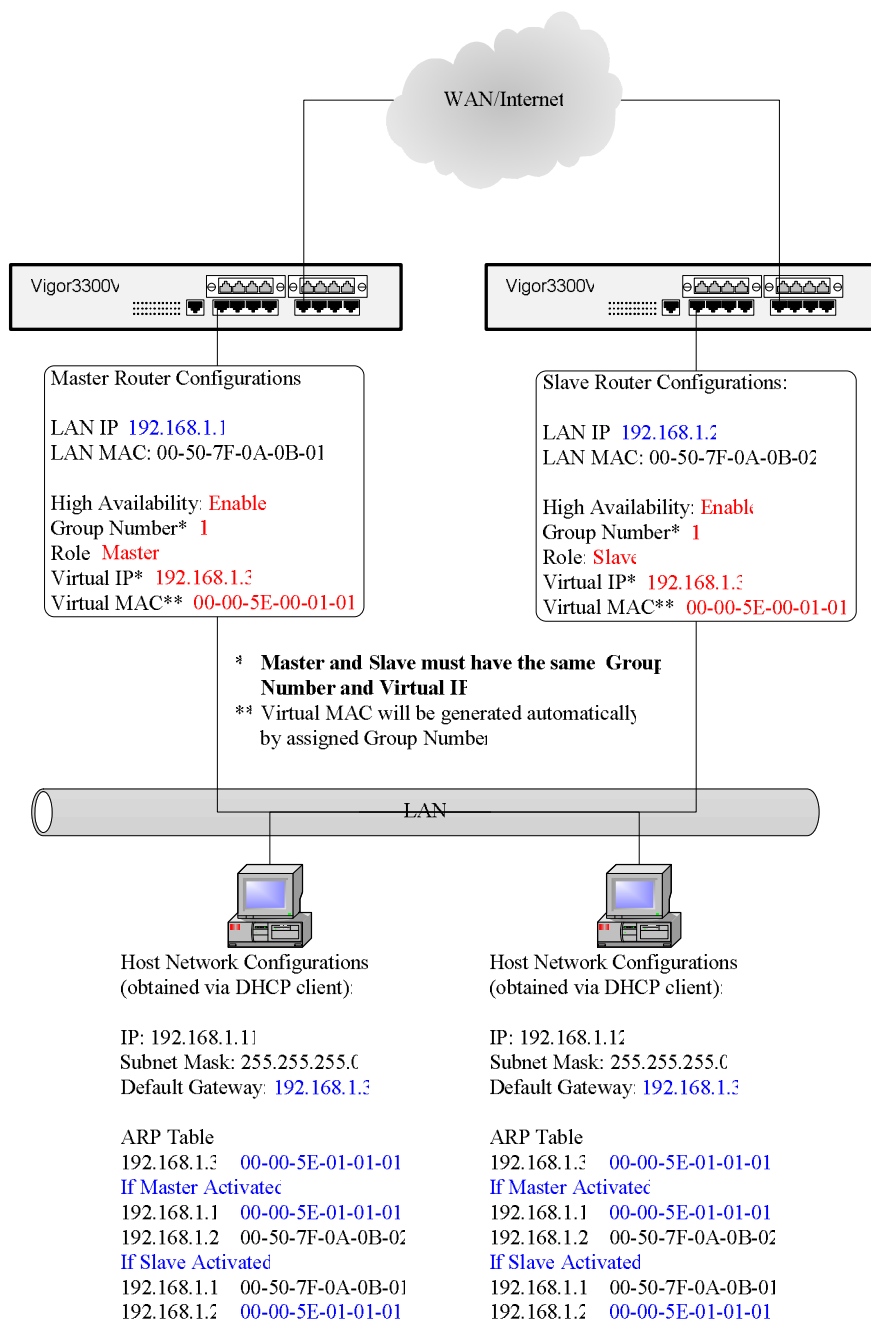


Figure 2-1. A Scenario of High Availability

## 2.1 Examples and Web Configurations

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

The screenshot shows the Vigor3300 series MultiService Security web interface. The top navigation bar includes 'Quick Setup', 'System', 'Network', 'Advanced', 'Firewall', 'QoS', 'VPN', and 'VoIP'. The 'Network' tab is selected. The page title is 'Network - LAN - High Availability'. The configuration fields are as follows:

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

Buttons: Apply, Cancel

Footer: DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

**Figure 2-2. Web settings of the Master**

Then, we have to configure High Availability in the Slave device. Please refer to the Figure 2-3.

The screenshot shows the Vigor3300 series MultiService Security web interface. The top navigation bar includes 'Quick Setup', 'System', 'Network', 'Advanced', 'Firewall', 'QoS', 'VPN', and 'VoIP'. The 'Network' tab is selected. The page title is 'Network - LAN - High Availability'. The configuration fields are as follows:

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

Buttons: Apply, Cancel

Footer: DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

**Figure 2-3. Web settings of the Slave**

The most important points are as below –

- The Group Number value must be same between the Master and Slave.
- The value of Role is different in the Master and Slave.
- The value of Virtual IP must be same between the Master and Slave.



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

Once Master unit is shut down or suffered a failure, Slave would be transferred from idle state to active state after 3 to 4 seconds then handover over Master.

### ***Master Restart***

Once the problem in Master is recovered, and then Slave will be transferred to be idle state.

### ***Multiple Slaves***

There should be only one Master, but multiple Slaves are allowed. Generally speaking, the Slave with greater LAN IP address will have higher priority to play Master's role if the original Master is shut down or failed. For example, the IP address 192.168.1.4 will have higher priority than 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 3

# Multi-DMZ Function

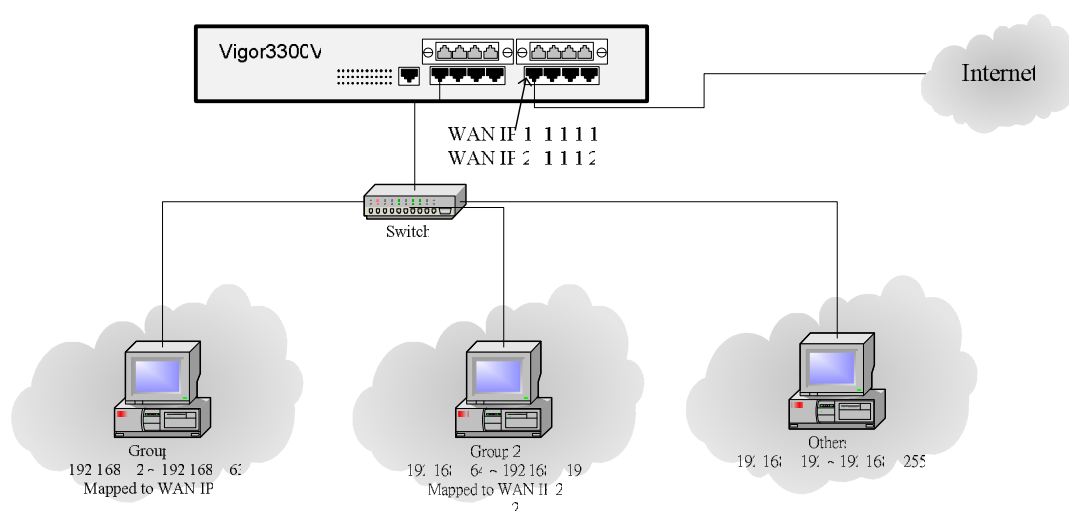
This chapter shows how to setup Multi-DMZ function.

This chapter is divided into the following sections,

- Section 3.1: Introduction
- Section 3.2: Examples and Web Configurations

### 3.1 Introduction

The following simple example shows how to set up Multi-DMZ function. There are two hosts to be connected to the LAN side. On the WAN side, we configure one WAN interface with IP alias. For the more details, please refer to Figure 3-1.



**Figure 3-1. Example of the Multi-DMZ function**

## 3.2 Examples and Web Configurations

At first, users must configure WAN interfaces. In this application, we set WAN1 as static mode in Figure 3-2.

**Network - WAN - WAN1 - Fast Ethernet**

Mac Address :

☒ Router Default ☐ User Definition

Downstream Rate :

(kbps)

Upstream Rate :

(kbps)

Type :

Physical Mode :

IP Mode :

☒ Static ☐ DHCP ☐ PPPoE ☐ PPTP

**Static/DHCP Configuration**

PPPoE/PPTP Configuration

IP Address :

WAN IP 1

Subnet Mask :

Default Gateway :

Primary DNS :

Secondary DNS :

**IP Alias List**

1.

WAN IP 2

3.

5.

Figure 3-2. WAN configuration

Please refer to Figure 3-3, it shows the configuration of DMZ host1 (192.168.1.11).

The screenshot shows the 'Advanced - NAT - DMZ Host - Edit' configuration page for host 1. The WAN Interface is set to WAN1. The Private IP is 192.168.1.11. The Use IP Alias option is set to Disable. The IP Alias is 1.1.1.2. The page includes 'Apply' and 'Cancel' buttons. The top navigation bar includes 'Quick Setup', 'System', 'Network', 'Advanced', 'Firewall', 'QoS', 'VPN', and 'VoIP'. The top status bar shows 'VIGOROUS BROADBAND ACCESS' and the time '4:17:26 P.M.'.

Figure 3-3. DMZ settings (host1)

**Note:**

*Any packets sent to IP (1.1.1.1) will be transferred to LAN IP (192.168.1.11).*

Please refer to Figure 3-4, it shows the configuration of DMA host2 (192.168.1.77) with applying IP Alias settings.

The screenshot shows the 'Advanced - NAT - DMZ Host - Edit' configuration page for host 2. The WAN Interface is set to WAN1. The Private IP is 192.168.1.77. The Use IP Alias option is set to Enable. The IP Alias is 1.1.1.2. The page includes 'Apply' and 'Cancel' buttons. The top navigation bar includes 'Quick Setup', 'System', 'Network', 'Advanced', 'Firewall', 'QoS', 'VPN', and 'VoIP'. The top status bar shows 'VIGOROUS BROADBAND ACCESS' and the time '1:46:58 P.M.'.

Figure 3-4. DMZ settings (host2)

**Note:**

*Any packets sent to IP (1.1.1.2) will be transferred to LAN IP (192.168.1.77).*

## CHAPTER 4

# SIP Call, Proxy, Outbound Proxy and Domain

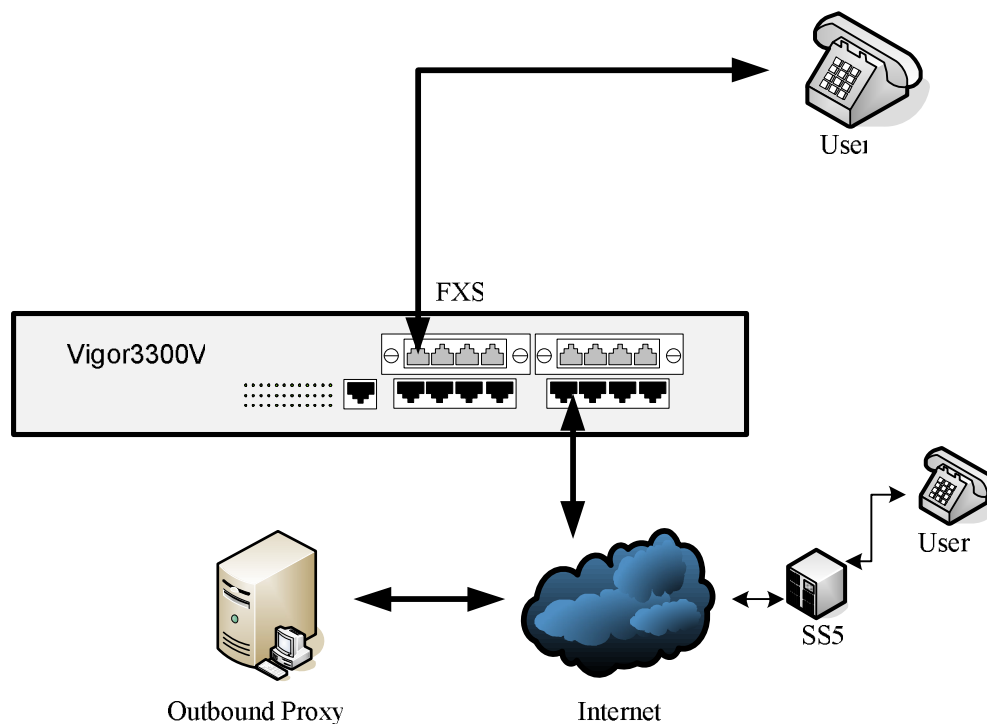
This chapter shows how SIP Proxy, Outbound Proxy and Domain work in a SIP outgoing call.

This chapter is divided into the following sections,

- Section 4.1: Introduction
- Section 4.2: Examples and Web Configurations

### 4.1 Introduction

There is a scenario graph in Figure 4-1.



**Figure 4-1. A Scenario of SIP outgoing calls in Vigor 3300V**

## 4.2 Examples and Web Configurations

Assume the following two entries already exist in Speed Dial table; please refer to the Figure 4-2.

Phone Number	Destination
111	luke@draytel.com
222	steven

**Vigor3300 series**  
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 7:49:04 P.M.

### VoIP - Speed Dial

#	Speed Dial Phone Number	Speed Dial Destination	Memo
1	111	luke@draytel.com	
2	222	steven	
3			
4			
5			

Example 101 101@iptel.org

1 2 3 4 5 6 7 8 9 10 >

Apply Cancel Clear This Page

DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Figure 4-2. Speed dial settings

## 4.2.1 SIP Protocol Configurations (Case 1)

Proxy/Registrar: 1.1.1.1

Outbound Proxy: yes

Domain: domain.net

**Vigor3300 series**  
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 9:24:53 P.M.

**VoIP - Protocol**

Select Protocol: ☒ SIP ☐ MGCP

VoIP IP Address: WAN

**SIP Configuration** MGCP Configuration

SIP Local Port: 5060

#	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"/>	proxy	1.1.1.1	5060	1.1.1.1	5060	600	domain.net
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

Apply Cancel

Figure 4-3. Case 1 SIP protocol configurations

Dialed Number	Destination URI and Action	Where the call will be sent
111	-> send "INVITE sip:luke@draytel.com"	to 1.1.1.1(Proxy)
222	-> send "INVITE sip:steven@domain.net"	to 1.1.1.1(Proxy)
333	-> send "INVITE sip:333@domain.net"	to 1.1.1.1(Proxy)
1*2*2*2*2	-> send "INVITE sip:1@2.2.2.2"	to 1.1.1.1(Proxy)

In this case, no matter what number we dialed, the SIP message will always send to SIP Proxy directly because we have enabled Outbound Proxy function.

“111” could be found in Speed Dial table and the corresponding destination is “luke@draytel.com”, so the call will be sent to SIP Proxy (1.1.1.1) then SIP Proxy will relay the call to draytel.com

“222” could be also found in Speed Dial table and the corresponding alias (no address in the destination) is “steven”, so the destination will become

**“steven@domain.net”** (composed of alias and SIP Domain), and this call will send to SIP Proxy (1.1.1.1), then SIP Proxy will dispatch the call to “steven”. (“steven” should have already registered to SIP Proxy, so that SIP Proxy could know where “steven” is. If “steven” has not registered to SIP Proxy, SIP Proxy could not find “steven”, then SIP Proxy will return a “404 Not Found” message to the caller, then the caller will hear Busy Tone)

**“333”** could **not** be found in Speed Dial table, so the callee should belong to SIP Proxy’s Domain, the destination will become **“333@domain.net”** (composed of number and SIP Domain), and this call will send to SIP Proxy (1.1.1.1), then SIP Proxy will dispatch the call to “333”. (“333” should have already registered to SIP Proxy, so that SIP Proxy could know where “333” is. If “333” have not registered to SIP Proxy, SIP Proxy could not find “333”, then SIP Proxy will return a “404 Not Found” message to the caller, then the caller will hear Busy Tone)

**1\*2\*2\*2\*2** is a special dialing method (named **“direct IP call”**) which means the destination is 1@2.2.2.2. The call will be sent to SIP Proxy (1.1.1.1) then SIP Proxy will relay the call to 2.2.2.2.



## 4.2.2 SIP Protocol Configurations (Case 2)

Proxy/Registrar: 1.1.1.1

Outbound Proxy: no

Domain: domain.net

**Vigor3300 series**  
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 9:47:29 P.M.

**VoIP - Protocol**

Select Protocol: ☒ SIP ☐ MGCP

VoIP IP Address: WAN

**SIP Configuration** MGCP Configuration

SIP Local Port: 5060

#	Active	Outbound Proxy	Proxy Name	Proxy Address	Proxy Port	Registrar Addr	Registrar Port	Expires (sec)	Domain
1.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	proxy	1.1.1.1	5060	1.1.1.1	5060	600	domain.net
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

Apply Cancel

Figure 4-4. Case 2 SIP protocol configurations

Dialed Number	Destination URI and Action	Where the call will be sent
111	-> send "INVITE sip:luke@draytel.com"	to draytel.com
222	-> send "INVITE sip:steven@domain.net"	to 1.1.1.1(Proxy)
333	-> send "INVITE sip:333@domain.net"	to 1.1.1.1(Proxy)
1*2*2*2*2	-> send "INVITE sip:1@2.2.2.2"	to 2.2.2.2

In this case, because Outbound Proxy function has been disabled, if the destination contains callee's address (not Domain), then the SIP messages will send to this address directly (such like "111" and "1\*2\*2\*2\*2"). If callee's address is not specified in the destination, then the SIP message will still send to SIP Proxy (such like "222" and "333").

### 4.2.3 SIP Protocol Configurations (Case 3)

Proxy/Registrar: 1.1.1.1

Outbound Proxy: yes

Domain: 0 (none)

The screenshot shows the 'Vigor3300 series MultiService Security' web interface. The top navigation bar includes 'Quick Setup', 'System', 'Network', 'Advanced', 'Firewall', 'QoS', 'VPN', and 'VoIP'. The 'VoIP' tab is selected, and the 'VoIP - Protocol' sub-tab is active. Under 'Select Protocol', 'SIP' is selected. The 'VoIP IP Address' is set to 'WAN'. The 'SIP Configuration' sub-tab is active, showing 'SIP Local Port' as 5060. Below this is a table for SIP configurations:

#	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"/>	proxy	1.1.1.1	5060	1.1.1.1	5060	600	0
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: proxy: iptel, Proxy Address: iptel.org, Registrar Addr: iptel.org, Domain: iptel.org									

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

Figure 4-5. Case 3 SIP protocol configurations

Dialed Number	Destination URI and Action	Where the call will be sent
111	-> send "INVITE sip:luke@draytel.com"	to 1.1.1.1(Proxy)
222	-> send "INVITE sip:steven@1.1.1.1"	to 1.1.1.1(Proxy)
333	-> send "INVITE sip:333@1.1.1.1"	to 1.1.1.1(Proxy)
1*2*2*2*2	-> send "INVITE sip:1@2.2.2.2"	to 1.1.1.1(Proxy)

This case, like case 1, the SIP message will always send to SIP Proxy directly because Outbound Proxy function has been enabled. However, because SIP Domain is not specified, so it will be replaced by SIP Proxy address.

## 4.2.4 SIP Protocol Configurations (Case 4)

Proxy/Registrar: 1.1.1.1

Outbound Proxy: no

Domain: 0 (none)

**Vigor3300 series**  
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 10:03:29 P.M.

**VoIP - Protocol**

Select Protocol: ☒ SIP ☐ MGCP

VoIP IP Address: WAN

**SIP Configuration** MGCP Configuration

SIP Local Port: 5060

#	Active	Outbound Proxy	Proxy Name	Proxy Address	Proxy Port	Registrar Addr	Registrar Port	Expires (sec)	Domain
1.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	proxy	1.1.1.1	5060	1.1.1.1	5060	600	0
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									

Apply Cancel

Figure 4-6. Case 4 SIP protocol configurations

Dialed Number	Destination URI and Action	Where the call will be sent
111	-> send "INVITE sip:luke@draytel.com"	to draytel.com
222	-> send "INVITE sip:steven@1.1.1.1"	to 1.1.1.1(Proxy)
333	-> send "INVITE sip:333@1.1.1.1"	to 1.1.1.1(Proxy)
1*2*2*2*2	-> send "INVITE sip:1@2.2.2.2"	to 2.2.2.2

This case, like case 2, because Outbound Proxy function has been disabled, if the destination contains callee's address, then the SIP messages will send to this address directly (such like "111" and "1\*2\*2\*2\*2"). If callee's address is not specified in the destination, then the SIP message will still send to SIP Proxy (such like "222" and "333"). And in this case, because SIP Domain is not specified, so it will be replaced by SIP Proxy address.

## 4.2.5 SIP Protocol Configurations (Case 5)

**Proxy/Registrar:** 0 (none)

**Outbound Proxy:** don't care (no use if Proxy is none)

**Domain:** 0 (none)

**Vigor3300 series**  
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 1:43:18 P.M.

**VoIP - Protocol**

Select Protocol: ☒ SIP ☐ MGCP

VoIP IP Address: WAN

**SIP Configuration** MGCP Configuration

SIP Local Port: 5060

#	Active	Outbound Proxy	Proxy Name	Proxy Address	Proxy Port	Registrar Addr	Registrar Port	Expires (sec)	Domain
1.	<input type="checkbox"/>	<input type="checkbox"/>		0	5060	0	5060	300	0
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

Apply Cancel

**Figure 4-7. Case 5 SIP protocol configurations**

Dialed Number	Destination URI and Action	Where the call will be sent
111	-> send "INVITE sip:luke@draytel.com"	to draytel.com
222	-> caller hears Busy Tone	
333	-> caller hears Busy Tone	
1*2*2*2*2	-> send "INVITE sip:1@2.2.2.2"	to 2.2.2.2

In this case, because both SIP Proxy and SIP Domain are not specified, if the destination does not contain callee's address, the SIP messages will not send out, and then the caller will hear Busy Tone (such like "222" and "333"). If callee's address is already specified in the destination, then the SIP message will still send to the address (such like "111" and "1\*2\*2\*2\*2").

## 4.2.6 SIP Protocol Configurations (Case 6)

**Proxy/Registrar:** 0 (none)

**Outbound Proxy:** don't care (no use if Proxy is none)

**Domain:** domain.net

**Vigor3300 series**  
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 2:15:42 P.M.

### VoIP - Protocol

Select Protocol : ☒ SIP ☐ MGCP

VoIP IP Address : WAN

**SIP Configuration** MGCP Configuration

SIP Local Port : 5060

#	Active	Outbound Proxy	Proxy Name	Proxy Address	Proxy Port	Registrar Addr	Registrar Port	Expires (sec)	Domain
1.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	proxy	0	5060	0	5060	300	domain.net
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									

Apply Cancel

**Figure 4-8. Case 6 SIP protocol configurations**

Dialed Number	Destination URI and Action	Where the call will be sent
111	-> send "INVITE sip:luke@draytel.com"	to draytel.com
222	-> send "INVITE sip:steven@domain.net"	to domain.net
333	-> send "INVITE sip:333@domain.net"	to domain.net
1*2*2*2*2	-> send "INVITE sip:1@2.2.2.2"	to 2.2.2.2

This case, like case 5, but SIP Domain is already specified, if the destination does not contain callee's address, the SIP messages will send to the SIP Domain (such like "222" and "333"). If callee's address is already specified in the destination, then the SIP message will still send to the address (such like "111" and "1\*2\*2\*2\*2").

## CHAPTER 5

# VoIP NAT Traversal Function

This chapter shows how to setup VoIP NAT Traversal function.

This chapter is divided into the following sections,

- Section 5.1: Introduction
- Section 5.2: Example and Web Configurations

## 5.1 Introduction

The following flow chart shows how to setup VoIP NAT Traversal function.

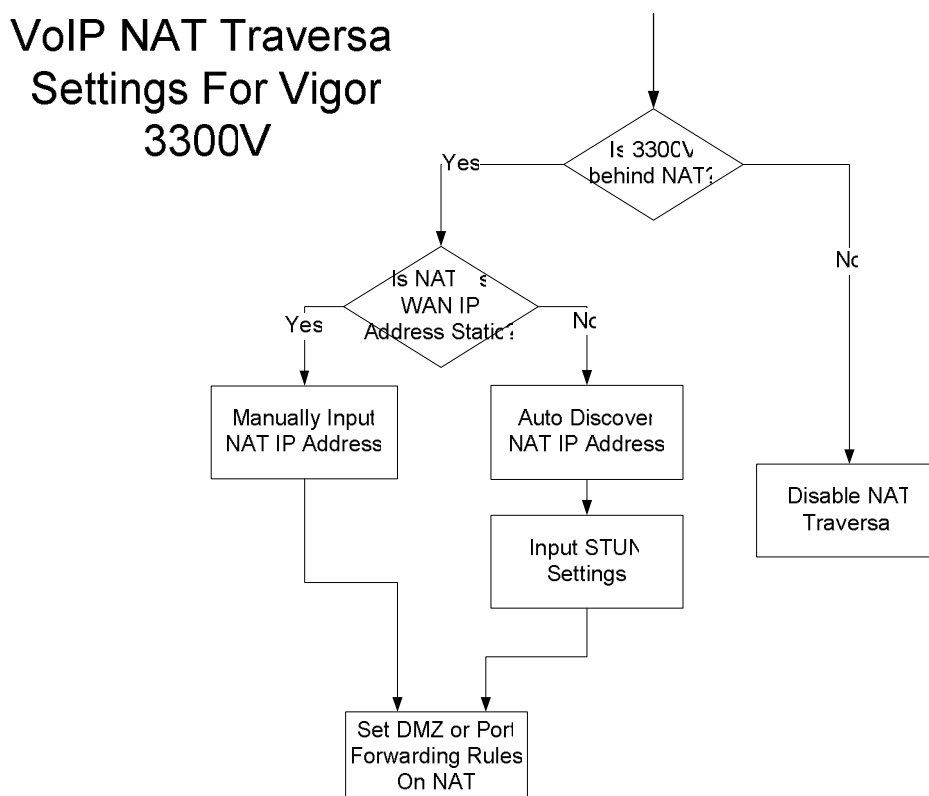


Figure 5-1. Flowchart of setting VoIP NAT Traversal function

## 5.2 Example and Web configurations

There are three cases listed as below.

### 5.2.1 Vigor 3300V with Static WAN IP

Vigor3300V has a public IP address in WAN1, it is not behind any NAT router. Figure 5-2 shows the scenario.

In this case, the users don't need to enable NAT Traversal function, so we left it "Disable", please refer to Figure 5-3.

#### Case 1 Vigor3300V Has Public WAN IP Address (Not Behind NAT)

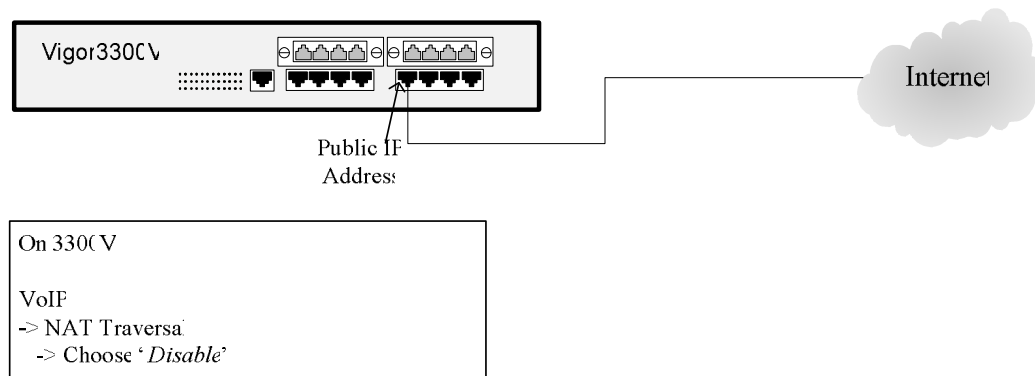


Figure 5-2. Case 1 Scenario

**Vigor3300 series**  
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 1:47:44 P.M.

**VoIP - NAT Traversal**

☒ Disable

☐ Manually Input NAT IP Address

NAT IP Address : 127.0.0.1

☐ Auto Discover NAT IP Address

STUN Local Port : 3478

STUN Server Address : stun.fwdnet.net

STUN Server Port : 3478

NAT Status

NAT Type: N/A, Local IP Address: 4.4.4.4, WAN IP Address: 4.4.4.4

Apply Cancel

DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Figure 5-3. Case 1 settings

Vigor3300V is behind a NAT router, the NAT router has a static Public WAN IP Address; please refer to Figure 5-4.

In this case, the user should choose “Manually Input NAT IP Address” then input 1.1.1.1 (NAT router’s WAN IP).

**Then, the user should configure DMZ or Port forwarding Rules on the NAT router.**

Set DMZ -> *192.168.1.10*

or

Set the following Port Forwarding Rules,

<i>UDP Port 5060 (SIP)</i>	<i>Forward to</i>	<i>192.168.1.10</i>
<i>UDP Port 13456~13470 (RTP)</i>	<i>Forward to</i>	<i>192.168.1.10</i>
<i>UDP Port 49170~49184 (T.38)</i>	<i>Forward to</i>	<i>192.168.1.10</i>



## 5.2.2 Vigor 3300V Behind NAT, Static WAN IP

### Case 2: Vigor3300V Behind NAT, NAT Uses Static WAN IP Address:

NAT's Static WAN IP Address: 1.1.1.1  
 3300V's WAN IP address: 192.168.1.10  
 3300V's SIP Local Port: 5060  
 3300V's RTP Port: 13456 (Beginning)  
 3300V's T.38 Port: 49170 (Beginning)

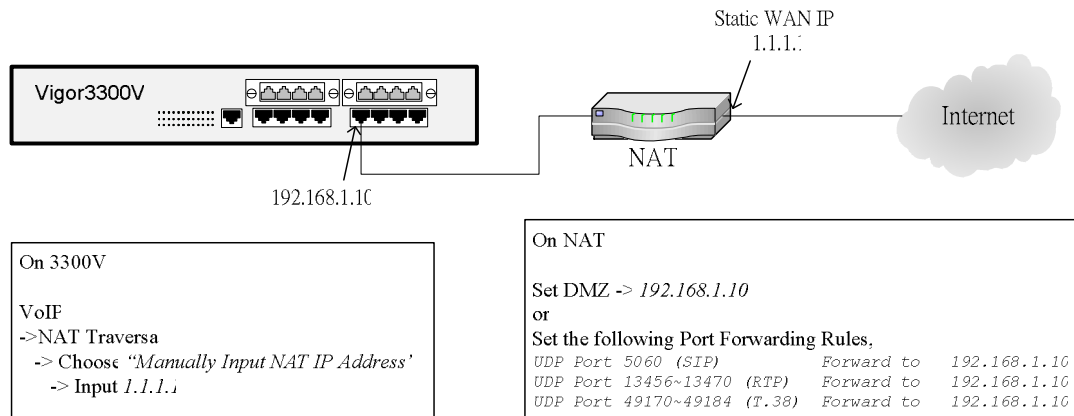


Figure 5-4. Case 2 Scenario

Figure 5-5 shows the Web settings on Vigor3300V.

### (NAT Traversal)

**Vigor3300 series**  
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 2:36:01 P.M.

#### VoIP - NAT Traversal

☐ Disable

☒ Manually Input NAT IP Address

NAT IP Address : 1.1.1.1

☐ Auto Discover NAT IP Address

STUN Local Port : 3478

STUN Server Address : stun.fwdnet.net

STUN Server Port : 3478

NAT Status

NAT Type: N/A, Local IP Address: 4.4.4.4, WAN IP Address: 1.1.1.1

Apply Cancel

DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

### (WAN)

**Vigor3300 series**  
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 2:32:55 P.M.

#### Network - WAN - WAN1 - Fast Ethernet

MAC Address : ☒ Default MAC ☐ User Defined MAC

00:50:7f:64:3a:9a

Downstream Rate : 102400 (kbps)

Upstream Rate : 102400 (kbps)

Type : Fast Ethernet

Physical Mode : Auto Negotiation

IP Mode : ☒ Static ☐ DHCP ☐ PPPoE ☐ PPTP

**Static/DHCP Configuration** **PPPoE/PPTP Configuration**

IP Address : 192.168.1.10

Subnet Mask : 255.255.255.0

Default Gateway : 192.168.1.100

Host Name :

Domain Name :

(Host Name and Domain Name are required for some ISPs.)

## (SIP Local Port)

**Vigor3300 series**  
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 2:37:22 P.M.

**VoIP - Protocol**

Select Protocol : ☒ SIP ☐ MGCP

VoIP IP Address : WAN

**SIP Configuration** MGCP Configuration

SIP Local Port : 5060

## (RTP and T.38 Ports)

**Vigor3300 series**  
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 4:03:13 P.M.

**VoIP - Miscellaneous**

RTP Starting Port: 13456

T.38 Starting Port: 49170

T.38 Redundancy number: 1 (Range: 0~4)

VoIP TOS : 0x20

FXO auto disconnection if no packet is received in 3 minutes.(Range:1~60, 0:no auto disconnection)

Apply Cancel

DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Figure 5-5. Case 2 settings

### 5.2.3 Vigor3300V Behind NAT, NAT Uses Dynamic Public WAN IP Address (Via DHCP or PPPoE Client)

Like case 2, Vigor3300V is behind a NAT router. However the NAT router uses a Dynamic Public WAN IP address (via DHCP or PPPoE client). Because the user may have no idea what Public IP is being used, “Manually Input NAT IP Address” will not work in this case, so the user should specify a STUN Server for Vigor3300V to detect the NAT router’s WAN IP automatically. Figure 5-6 shows the scenario.

**After the user has set up the STUN server on Vigor3300V, the user should then configure DMZ or Port forwarding Rules on the NAT router.**

Set DMZ -> 192.168.1.10

or

Set the following Port Forwarding Rules,

UDP Port 5060 (SIP)	Forward to	192.168.1.10
UDP Port 13456~13470 (RTP)	Forward to	192.168.1.10
UDP Port 49170~49184 (T.38)	Forward to	192.168.1.10

**Case 3: Vigor3300V Behind NAT, NAT Uses Dynamic WAN IP Address (Via DHCP or PPPoE Client)**

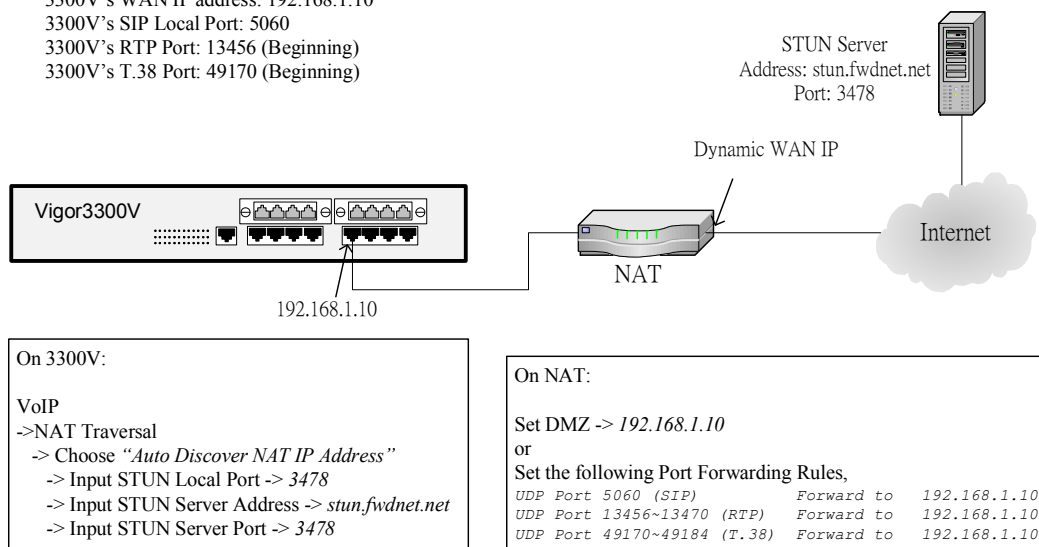
NAT's WAN IP Address: Dynamic (Via DHCP or PPPoE Client)

3300V's WAN IP address: 192.168.1.10

3300V's SIP Local Port: 5060

3300V's RTP Port: 13456 (Beginning)

3300V's T.38 Port: 49170 (Beginning)



**Figure 5-6. Case 3 scenario of NAT Traversal**

Figure 5-7 shows the Web configurations on Vigor3300V for NAT Traversal. For the SIP Local Port, RTP and T.38 Ports Settings please refer Figure 5-5.

(NAT Traversal)

**Vigor3300 series**  
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 2:49:00 P.M.

### VoIP - NAT Traversal

☐ Disable  
☐ Manually Input NAT IP Address  
☒ Auto Discover NAT IP Address

NAT IP Address : 1.1.1.1

STUN Local Port : 3478

STUN Server Address : stun.fwdnet.net

STUN Server Port : 3478

NAT Status

NAT Type: N/A, Local IP Address: 4.4.4.4, WAN IP Address: 4.4.4.4

Apply Cancel

DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

**Figure 5-7. Case 3 settings of NAT Traversal**

--- stun.fwd.net is a free, well-know STUN server

## CHAPTER 6

# Multi NAT Function

This chapter shows how to setup Multi NAT function.

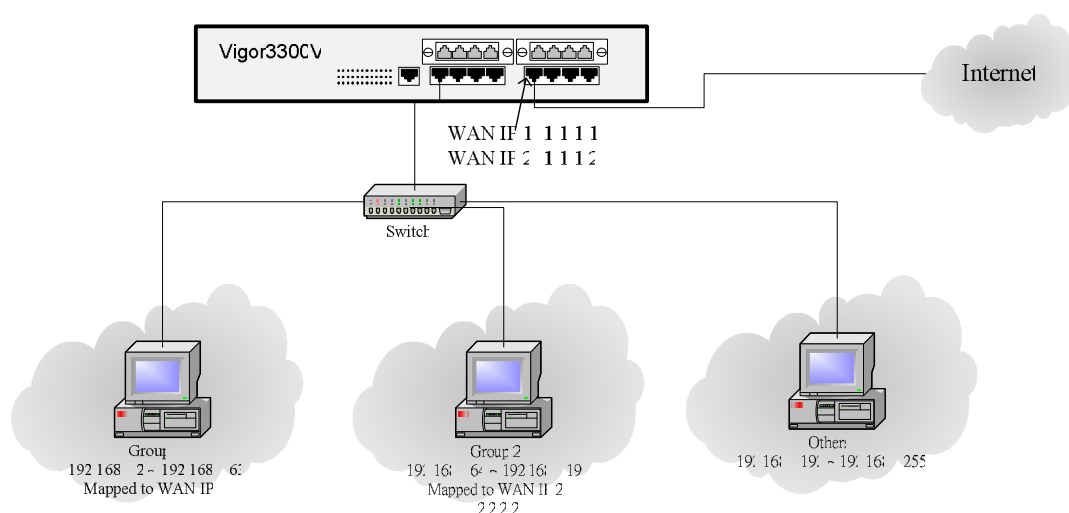
This chapter is divided into the following sections,

- Section 6.1: Introduction
- Section 6.2: Example and Web Configurations

## 6.1 Introduction

There are three groups connected to Vigor3300V by a switch proprietarily. Then we setup a WAN interface connected to the Internet. The scenario graph is in Figure 6-1.

### Vigor3300 Multi-NAT Example



**Figure 6-1. A Scenario of Multi NAT**

## 6.2 Examples and Web Configurations

There are some steps as followings.

### Step 1:

**Network - WAN - WAN1 - Fast Ethernet**

Mac Address : ☒ Router Default ☐ User Definition

Downstream Rate :  (kbps)

Upstream Rate :  (kbps)

Type :

Physical Mode :

IP Mode : ☒ Static ☐ DHCP ☐ PPPoE ☐ PPTP

**Static/DHCP Configuration** | PPPoE/PPTP Configuration

IP Address :  **WAN IP 1**

Subnet Mask :

Default Gateway :

Primary DNS :

Secondary DNS :

**IP Alias List**

1.	<input type="text" value="1.1.1.2"/> <b>WAN IP 2</b>
3.	<input type="text"/>
5.	<input type="text"/>

Figure 6-2. Step1 in WAN settings

## Step 2

**Advance - NAT - Address Mapping - Edit**

---

1

Protocol :  select All

Public IP :  WAN IP 1

Private IP :  Group 1 Starting IP

Subnet Mask :  Group 1 Subnet Mask

## Step 3

**Advance - NAT - Address Mapping - Edit**

---

2

Protocol :  Select All

Public IP :  WAN 2 IP

Private IP :  Group2 Starting IP

Subnet Mask :  Group2 Subnet Mask

Note Other IPs will by default use WAN IP

**Figure 6-3. Step2 & 3 in NAT settings**



## CHAPTER 7

# VoIP Incoming Call Barring Function

---

This chapter describes how to setup VoIP Incoming Call Barring settings.

This chapter is divided into the following sections,

- Section 7.1: Introduction
- Section 7.2: Examples and Web Configurations

## 7.1 Introduction

Incoming Call Barring is used to bar incoming calls from internet. User can specify barring class to allow or deny incoming calls. There are five barring classes on the device and default setting is “Allow all incoming calls”. When user wish to bar specify calls, they could select the other classes and these classes is flexible.

### Barring Classes

- Allow all incoming calls  
It will always allow each incoming callings without any limitation.
- Allow only calls from allow list  
It only allows incoming callings existed in user defined allow list.
- Allow only calls from speed dial entries  
It only allows incoming callings existed in user defined speed dial table.
- Deny only calls from deny list  
It only denies incoming callings existed in user defined deny list.
- Deny all incoming calls  
It will always deny each incoming callings without any limitation.

Please refer to Figure 7-1 in Web page of Vigor3300V.

Figure 7-1. Barring Classes in Vigor3300V

## 7.2 Examples and Web configurations

The example is shown in Figure 7-2. There are three users in Internet want to make a call to a user behind of Vigor3300V. The user information is as below.

Name	IP/Domain
David	61.1.1.100
Jack	iptel.org
Linda	ms10.hinet.net

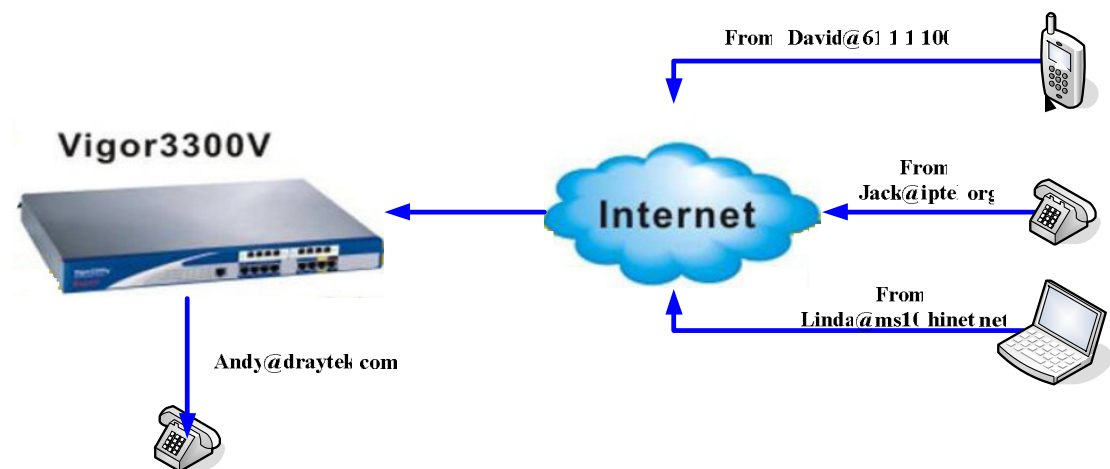


Figure 7-2. A Scenario on incoming call

There are two methods to be checked incoming calls for ensuring the calling which you want to check. These are “Name” (username) or “IP/Domain” (hostname) and both in the header of SIP invite message. Please refer to the Figure 7-3. Each method can be disabled or enabled independently or simultaneously.

**Vigor3300 series**  
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 7:55:25 P.M.

### VoIP - Incoming Call Barring - Set

**Barring Class**  
Allow only calls from allow list

**Match Method**

Name : ☒ Disable ☐ Enable  
Remind:

IP/Domain : ☒ Disable ☐ Enable  
Remind:

**Speed Dial Entries**  
From: 1 To: 30

Apply Cancel

DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

**Figure 7-3. Comparing methods for incoming call barring**

Assume there are three users David, Jack and Linda will call from Internet. Please refer to the scenario in Figure 7-2.

## 7.2.1 Allow All Incoming Calls

The barring class of V3300V is “Allow all incoming calls”. All of people could call to Andy. The Web settings are shown in Figure 7-4.

**Vigor3300 series**  
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 8:05:07 P.M.

### VoIP - Incoming Call Barring - Set

**Barring Class**  
 Allow all incoming calls

**Match Method**

Name: ☐ Disable ☐ Enable  
 Remind:

IP/Domain: ☐ Disable ☐ Enable  
 Remind:

**Speed Dial Entries**  
 From: 1 To: 30

Apply Cancel

DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Figure 7-4. Web settings

## 7.2.2 Allow Only Calls From Allow List

The barring class of V3300V is “Allow only calls from allow list”. There are two entries in allow list as shown in Figure 7-5.

**Vigor3300 series**  
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 8:08:09 P.M.

### VoIP - Incoming Call Barring - Allow List

#	Name	IP/Domain
1	David	ms10.hinet.net
2	Jack	iptel.org
3		
4		
5		

Example John 192.168.1.1 or iptel.org

1 2 3 4 5 6

Apply Cancel

DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Figure 7-5. Allow List settings

### 7.2.2.1 Name and IP/Domain Are Both Enabled (Case 1)

Please refer to the Web settings in Figure 7-6.

The screenshot shows the 'Vigor3300 series MultiService Security' web interface. The top navigation bar includes 'Quick Setup', 'System', 'Network', 'Advanced', 'Firewall', 'QoS', 'VPN', and 'VoIP'. The 'VoIP' tab is selected, and the page title is 'VoIP - Incoming Call Barring - Set'. The 'Barring Class' dropdown is set to 'Allow only calls from allow list'. Under the 'Match Method' section, there are two rows: 'Name' and 'IP/Domain'. Each row has 'Disable' and 'Enable' radio buttons. In both rows, the 'Enable' radio button is selected. Below this is the 'Speed Dial Entries' section with 'From' and 'To' dropdowns set to '1' and '30' respectively. At the bottom right are 'Apply' and 'Cancel' buttons. A footer note reads: 'DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.'

**Figure 7-6. Match Method – Case 1 settings**

The result is only Jack could call Andy and the others will be blocked. The reason is the Name and Domain of Jack are both matched in the allow list.

### 7.2.2.2 Only Name Option is Enabled (Case 2)

Please refer to the Web settings in Figure 7-7.

The screenshot shows the same 'Vigor3300 series MultiService Security' web interface. The 'VoIP' tab is selected, and the page title is 'VoIP - Incoming Call Barring - Set'. The 'Barring Class' dropdown is set to 'Allow only calls from allow list'. Under the 'Match Method' section, there are two rows: 'Name' and 'IP/Domain'. In the 'Name' row, the 'Enable' radio button is selected. In the 'IP/Domain' row, the 'Disable' radio button is selected. Below this is the 'Speed Dial Entries' section with 'From' and 'To' dropdowns set to '1' and '30' respectively. At the bottom right are 'Apply' and 'Cancel' buttons. A footer note reads: 'DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.'

**Figure 7-7. Match Method – Case 2 settings**

The result is both David and Jack could call Andy, and Linda will be blocked because Linda is not in the allow list.

### 7.2.2.3 Only IP/Domain Option is Enabled (Case 3)

Please refer to the Web settings in Figure 7-8.

The screenshot shows the Vigor3300 series MultiService Security web interface. The top navigation bar includes links for Quick Setup, System, Network, Advanced, Firewall, QoS, VPN, and VoIP. The current page is titled "VoIP - Incoming Call Barring - Set". Under the "Barring Class" section, the "Allow only calls from allow list" option is selected. The "Match Method" section is highlighted with a red box and contains two rows of settings: "Name" and "IP/Domain". For "Name", the "Disable" radio button is selected, and the "Remind" field is empty. For "IP/Domain", the "Enable" radio button is selected, and the "Remind" field is empty. The "Speed Dial Entries" section at the bottom shows "From: 1" and "To: 30". The "Apply" and "Cancel" buttons are located at the bottom right of the configuration area.

**Figure 7-8. Match Method – Case 3 settings**

Both Jack and Linda could call to Andy, and David will be blocked. The reason is that the IP/Domain option of Jack and Linda are matched in the allow list, however David's IP/Domain option is not existed in the allow list.

## 7.2.3 Allow Only Calls from Speed Dial Entries

The barring class of V3300V is “Allow only calls from speed dial entries”. There are three entries in speed dial table and the groups are from 1 to 3 shown in Figure 7-9.

#	Speed Dial Phone Number	Speed Dial Destination	Memo
1	2001	David@draytek.com	
2	3001	Jack@iptel.org	
3	4001	Linda@61.2.2.2	
4			
5			

Example 101 101@iptel.org

1 2 3 4 5 6 7 8 9 10 >

Apply Cancel Clear This Page

Figure 7-9. Speed Dial Table settings

### 7.2.3.1 Name and IP/Domain Options Are Both Enabled (Case 1)

Please refer to the Web settings in Figure 7-10.

Barring Class

Allow only calls from speed dial entries

Match Method

Name: ☐ Disable ☒ Enable  
Remind: match username in speeddial destination

IP/Domain: ☐ Disable ☒ Enable  
Remind: match hostname in speeddial destination

Speed Dial Entries

From: 1 To: 30

Apply Cancel

Figure 7-10. Match Method – Case 1 settings



The result is only Jack could call Andy and the others will be blocked because the Name and IP/Domain options of Linda and David are not matched in Speed Dial Table.

### 7.2.3.2 Only Name Option is Enabled (Case 2)

Please refer to the Web settings in Figure 7-11.

The screenshot shows the web interface of a Vigor3300 series device. The top navigation bar includes links for Quick Setup, System, Network, Advanced, Firewall, QoS, VPN, and VoIP. The main content area is titled "VoIP - Incoming Call Barring - Set". Under the "Barring Class" section, a dropdown menu is set to "Allow only calls from speed dial entries". The "Match Method" section contains two rows: "Name" and "IP/Domain". For "Name", the "Enable" radio button is selected, with a reminder "Remind: match username in speeddial destination". For "IP/Domain", the "Disable" radio button is selected, with a reminder "Remind: match hostname in speeddial destination". A red box highlights these two rows. Below this is the "Speed Dial Entries" section with "From" set to 1 and "To" set to 30. At the bottom right are "Apply" and "Cancel" buttons. The footer contains the text: "DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution."

**Figure 7-11. Match Method – Case 2 settings**

The result is that David, Jack and Linda could call Andy because the Name option of these three persons is matched in Speed Dial Table.



### 7.2.3.3 Only IP/Domain Option is Enabled (Case 3)

Please refer to the Web settings in Figure 7-12.

The screenshot shows the Vigor3300 series MultiService Security web interface. The top navigation bar includes links for Quick Setup, System, Network, Advanced, Firewall, QoS, VPN, and VoIP. The current page is titled "VoIP - Incoming Call Barring - Set".

The configuration is divided into three main sections:

- Barring Class:** A dropdown menu set to "Allow only calls from speed dial entries".
- Match Method:** This section is highlighted with a red box. It contains two rows of settings:
  - Name:** Radio buttons for "Disable" (selected) and "Enable". Below it, a reminder text: "Remind: match username in speeddial destination".
  - IP/Domain:** Radio buttons for "Disable" and "Enable" (selected). Below it, a reminder text: "Remind: match hostname in speeddial destination".
- Speed Dial Entries:** A section with "From:" and "To:" dropdown menus, currently set to "1" and "30" respectively.

At the bottom right of the configuration area are "Apply" and "Cancel" buttons. The footer of the interface reads: "DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution."

**Figure 7-12. Match Method – Case 3 settings**

The result is only Jack could call Andy and the others will be blocked because the IP/Domain option of Linda and David is not matched in Speed Dial Table.

## 7.2.4 Deny Only Calls from Deny List

The barring class of V3300V is “Deny only calls from deny list”. There are two entries in deny list shown in Figure 7-13.

#	Name	IP/Domain
1	David	draytek.com
2	Jack	iptel.org
3		
4		
5		
Example	John	192.168.1.1 or iptel.org

Figure 7-13. Deny List settings

### 7.2.4.1 Name and IP/Domain Options Are Both Enabled (Case 1)

Please refer to the Web settings in Figure 7-14.

The screenshot shows the 'Vigor3300 series MultiService Security' web interface. The top navigation bar includes 'Quick Setup', 'System', 'Network', 'Advanced', 'Firewall', 'QoS', 'VPN', and 'VoIP'. The 'VoIP' tab is selected, and the page title is 'VoIP - Incoming Call Barring - Set'. The 'Barring Class' dropdown is set to 'Deny only calls from deny list'. Under the 'Match Method' section, there are two rows: 'Name' and 'IP/Domain'. Each row has 'Disable' and 'Enable' radio buttons. In both rows, the 'Enable' radio button is selected. Below this is the 'Speed Dial Entries' section with 'From' set to 1 and 'To' set to 30. At the bottom right are 'Apply' and 'Cancel' buttons. The footer text reads: 'DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.'

**Figure 7-14. Match Method – Case 1 settings**

The result is only Jack will be blocked because Jack's Name and IP/Domain options are matched in Deny list. For the others, Linda and David, they can call Andy without any limitation.

### 7.2.4.2 Only Name Option is Enabled (Case 2)

Please refer to the Web settings in Figure 7-15.

**Vigor3300 series**  
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 3:37:45 P.M.

#### VoIP - Incoming Call Barring - Set

**Barring Class**  
Deny only calls from deny list

**Match Method**

Name : ☐ Disable ☒ Enable  
Remind: \_\_\_\_\_

IP/Domain : ☒ Disable ☐ Enable  
Remind: \_\_\_\_\_

**Speed Dial Entries**  
From: 1 To: 30

Apply Cancel

DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

**Figure 7-15. Match Method – Case 2 settings**

The result is both David and Jack will be blocked because their Name option are matched in Deny List. Linda can call Andy without any limitation.

### 7.2.4.3 Only IP/Domain Option is Enabled (Case 3)

Please refer to the Web settings in Figure 7-16.

**Vigor3300 series**  
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 3:40:33 P.M.

#### VoIP - Incoming Call Barring - Set

**Barring Class**  
Deny only calls from deny list

**Match Method**

Name : ☒ Disable ☐ Enable  
Remind: \_\_\_\_\_

IP/Domain : ☐ Disable ☒ Enable  
Remind: \_\_\_\_\_

**Speed Dial Entries**  
From: 1 To: 30

Apply Cancel

DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

**Figure 7-16. Match Method – Case 3 settings**

The result is only Jack will be blocked because Jack's IP/Domain option is matched in Deny List. The others, Linda and David, can call Andy without limitation.

## 7.2.5 Deny All Incoming Calls

The barring class of V3300V is "Deny all incoming calls". The Web settings are shown in Figure 7-17.

The screenshot displays the web management interface for a Vigor3300 series device. The top navigation bar includes links for Quick Setup, System, Network, Advanced, Firewall, QoS, VPN, and VoIP. The main content area is titled "VoIP - Incoming Call Barring - Set". Under the "Barring Class" section, a dropdown menu is set to "Deny all incoming calls". The "Match Method" section contains two rows, each with "Name:" and "IP/Domain:" labels, and radio buttons for "Disable" (selected) and "Enable". Below these are "Remind:" input fields. The "Speed Dial Entries" section at the bottom shows "From:" set to 1 and "To:" set to 30. "Apply" and "Cancel" buttons are located at the bottom right of the settings area. A footer at the very bottom reads: "DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution."

**Figure 7-17. Web settings**

In this case, all calls from internet will be blocked.

## **CHAPTER 8**

# **Port Mirroring Function**

---

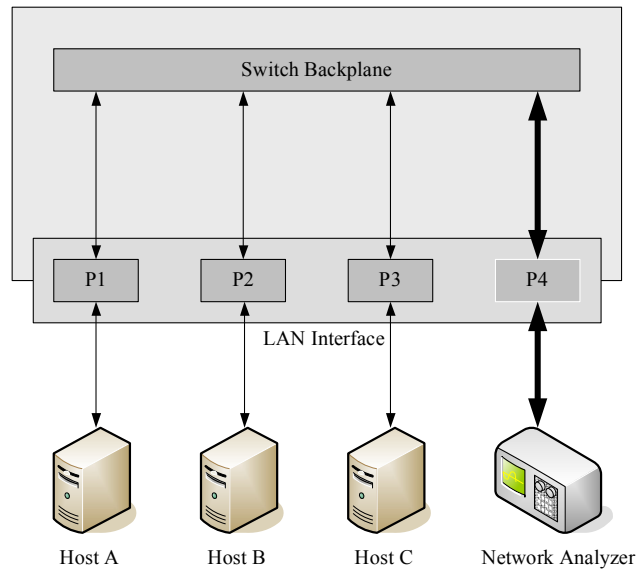
This chapter describes how to setup Port Mirroring function.

This chapter is divided into the following sections,

- Section 8.1: Introduction
- Section 8.2: Examples and Web Configurations

## **8.1 Introduction**

Port Mirroring is a network debugging and administration feature. The feature can help the network manager to determine the location of a problem and monitor the traffic on network efficiently. Port Mirroring, is configured by assigning these ports which aggregate all traffic on these ports to the mirror port. Finally, when the process is started, all frames bound for or sourced from the selected source (mirrored) port will be sent to the selected destination (mirroring) port. In Figure 11-1, traffic from one or more network ports is switched through the backplane to its normal destination port and a copy to the mirroring port. The LAN port mirroring page can be used to configure the selection of ports to be mirrored as in Figure 8-2.



**Figure 8-1. LAN Port mirroring**

There are three hosts – A, B and C which are connected to P1, P2 and P3 in LAN ports. In the P4, we setup a monitoring tool like as Network Analyzer. The purpose is to get and monitor all packets accessing in P1, P2 and P3.

## 8.2 Examples and Web Configurations

In this case, we need to select Port 4 as a Mirroring Port, and choose the other ports as Mirrored ports. Please refer to the settings in Figure 8-2.

**Advanced - LAN Port Mirroring**

☐ Disable ☒ Enable

Mirroring Port: Port 4

Mirrored Port(s):

- ☒ Port 1
- ☒ Port 2
- ☒ Port 3
- ☒ Port 4

**Figure 8-2. LAN Port Mirroring setting**

## **CHAPTER 9**

# **FXO Hot Line Function**

---

This chapter shows how to setup Hot Line function by FXO port.

This chapter is divided into the following sections,

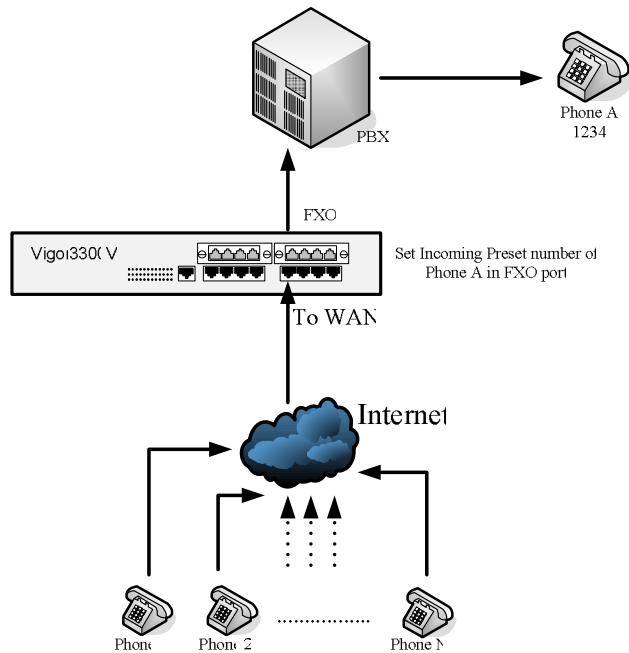
- Section 9.1: Introduction
- Section 9.2: Examples and Web Configurations

### **9.1 Introduction**

Hot line application is so very convenient for users in VoIP phone. It can shorten the dialing time for users to make a call to the destination. There are two scenario graphs in the Figure 9-1. One is incoming, the other one is for outgoing side.

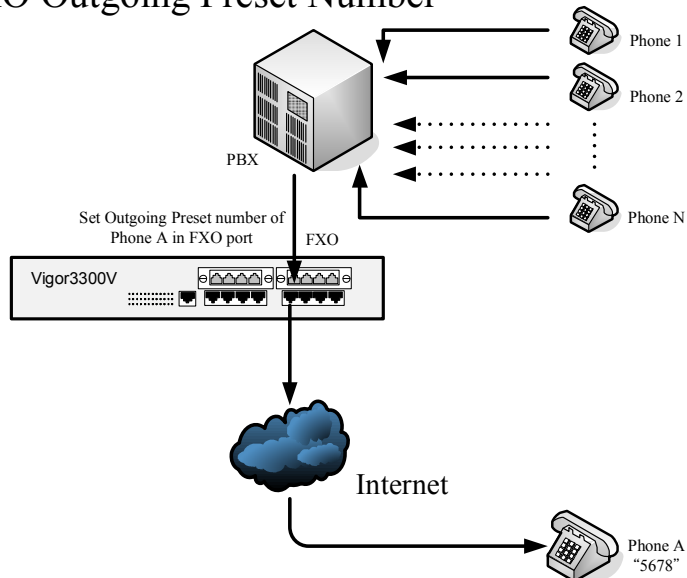


## Hot line in FXO Incoming Preset Number



When any phone of Phone 1 to Phone N calls to the FXO port in 3300v via Internet this FXO port will dial defined incoming preset number "1234" of Phone A automatically via PBX

## Hot line in FXO Outgoing Preset Number



When any phone of Phone 1 to Phone N calls to the FXO port of 3300V via PBX, this FXO port will dial defined outgoing preset number "5678" of Phone A automatically via the Internet.

**Figure 9-1. Two Scenarios of Hot Line**

## 9.2 Examples and Web Configurations

At first, we need to setup the preset number for a VoIP port. The preset number is independently for each VoIP port.

### 9.2.1 Incoming Preset Number

First of all, we need to setup an incoming preset number in the FXO port which is connected to the Phone A by a PBX. About the settings of incoming preset number, please refer to the Figure 9-2. The incoming preset number is normally a number of Phone A on the PBX system.

The screenshot shows the web configuration interface for a Vigor3300 series device. The top navigation bar includes links for Quick Setup, System, Network, Advanced, Firewall, QoS, VPN, and VoIP. The main content area is titled 'VoIP - Port Settings - Port5 - Edit'. Under the 'Port 5 (FXO)' section, the 'Enable' radio button is selected. Below this, there are fields for Username (1005), Password (masked with dots), Display Name (1005), and Proxy Server (none). At the bottom, under the 'FXO' section, the 'Incoming Pre-Set Number' is set to 1234. Red boxes highlight the 'Enable' button and the 'Incoming Pre-Set Number' field.

**Figure 9-2. The Web settings of incoming preset number**

In this case, when any phone of Phone 1 to Phone N in the Internet makes a call to the FXO port of Vigor3300V, the FXO port will dial “1234” (the Incoming Preset Number) automatically to PBX. The PBX will transfer the call to Phone A (ext.1234)

## 9.2.2 Outgoing Preset Number

First of all, we need to setup an outgoing preset number in the FXO port which is connected to the Phone A via the Internet. About the settings of outgoing preset number, please refer to the Figure 9-3. The outgoing preset number is normally a number of remote Phone A.

The screenshot shows the web interface of a Vigor3300 series device. The top navigation bar includes links for Quick Setup, System, Network, Advanced, Firewall, QoS, VPN, and VoIP. The main content area is titled 'VoIP - Port Settings - Port5 - Edit'. Under the 'Port 5 (FXO)' section, the 'Enable' radio button is selected. The 'Username' field contains '1005', the 'Password' field contains four dots, the 'Display Name' field contains '1005', and the 'Proxy Server' dropdown is set to 'none'. In the 'FXO' section, the 'Incoming Pre-Set Number' field contains '1234', the 'Outgoing Pre-Set Number' field contains '5678' (highlighted with a red box), and the 'Manual Disconnection' button is labeled 'Disconnect'.

**Figure 9-3. The Web settings of Outgoing preset number**

In this case, when any phone of Phone 1 to Phone N on PBX makes a call to the FXO port of Vigor3300V via PBX, the FXO port will dial “5678” (the Outgoing Preset Number) automatically to Phone A (ext. 5678) via the Internet.