Vigor3300 Series Application Notes

(Part 1)

V1.0

DrayTek

History Table

Date	Descriptions	Version	By
2005/8/17	Initial	V1.0	Jenny, Luke, Jimmy, Amy

Table of Contents

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.

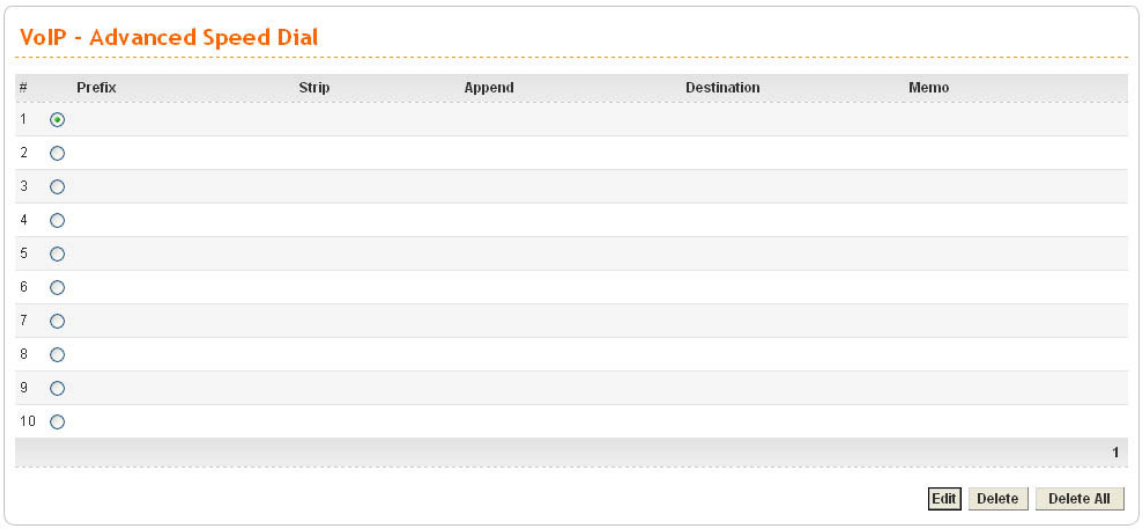


Figure 1-1. Advanced speed dial setting page

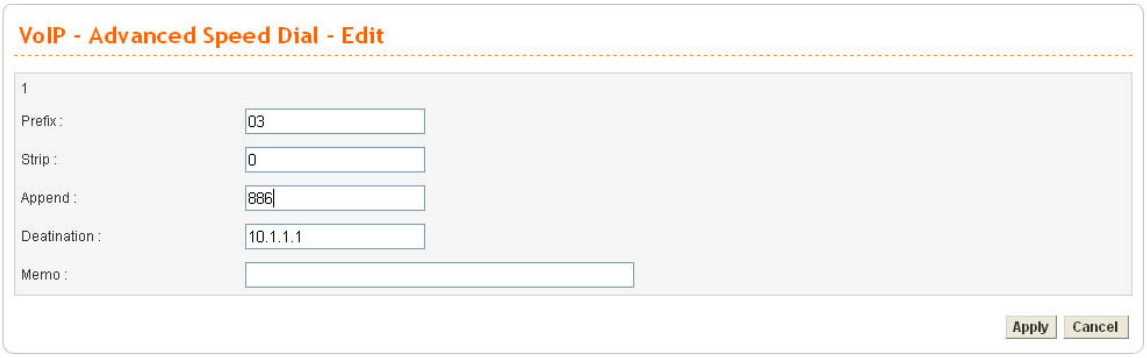


Figure 1-2. Advanced speed dial edit page

We list some examples as followings,

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

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.

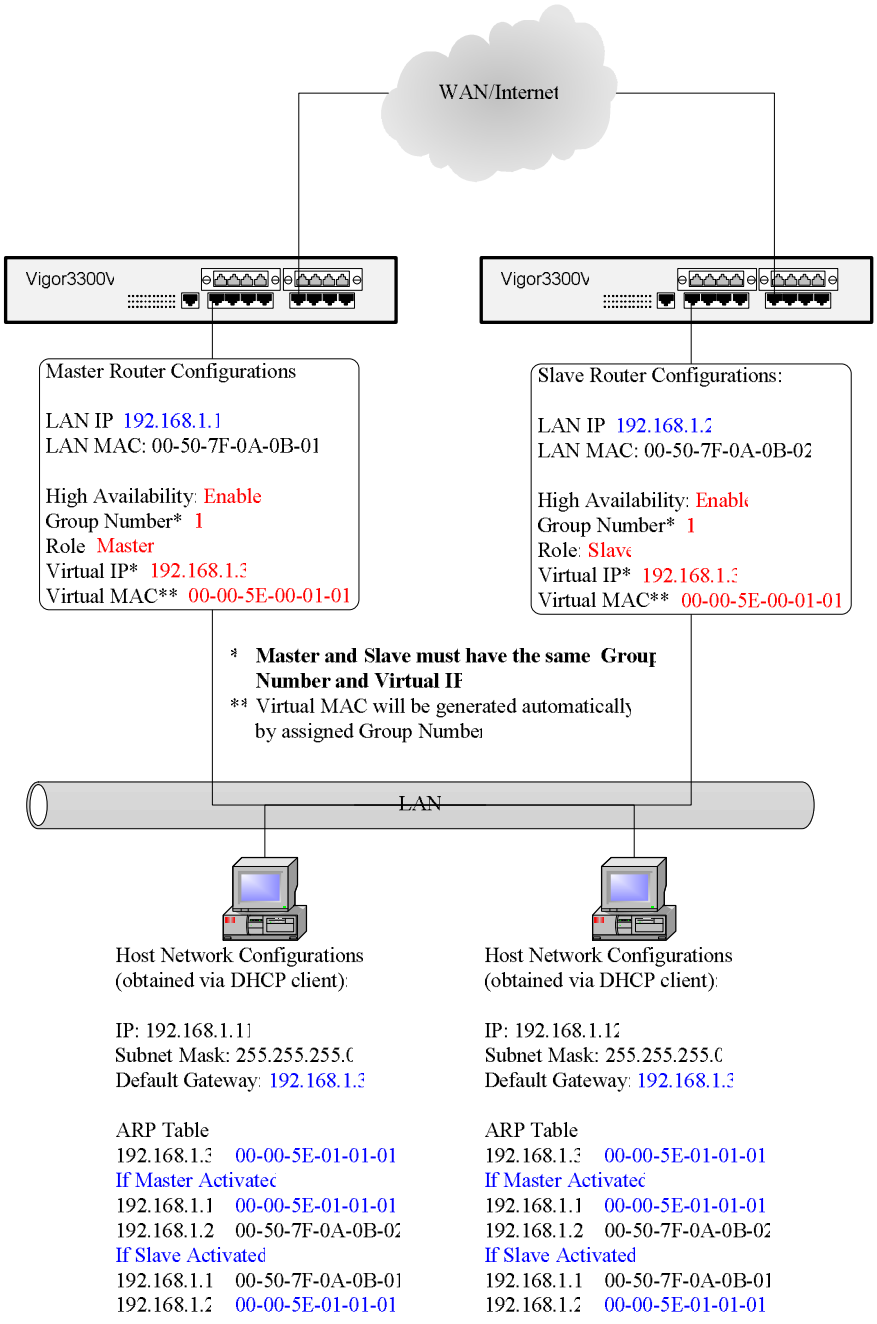


Figure 2-1. A Scenario of High Availability

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.

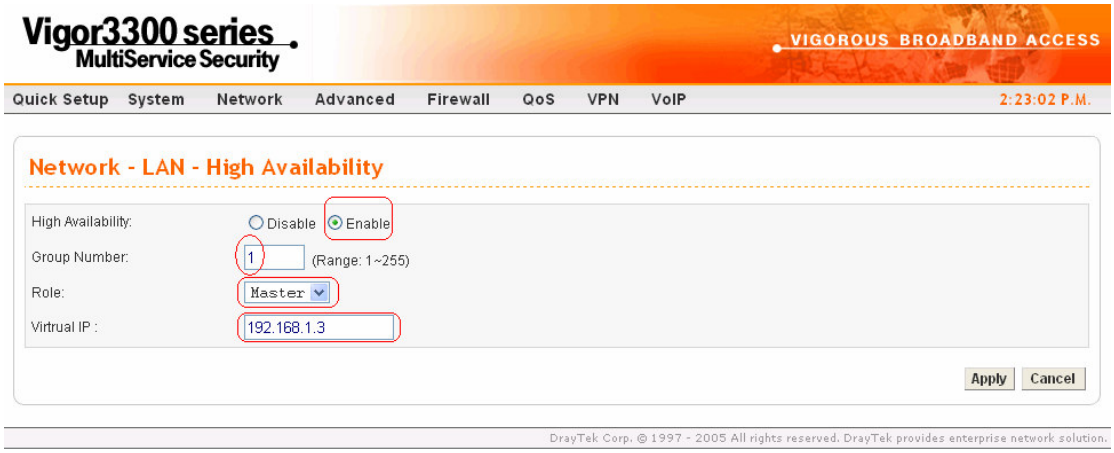


Figure 2-2. Web settings of the Master

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

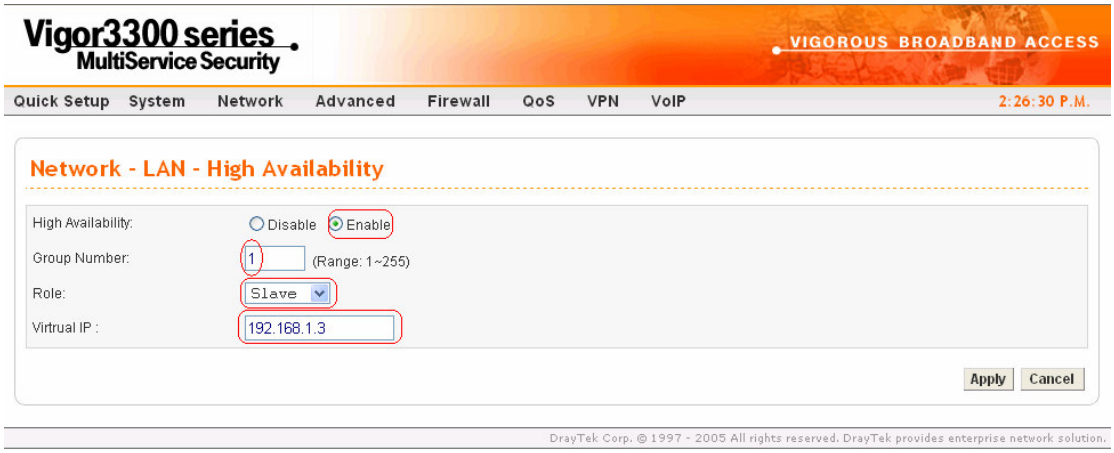


Figure 2-3. Web settings of the Slave

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.

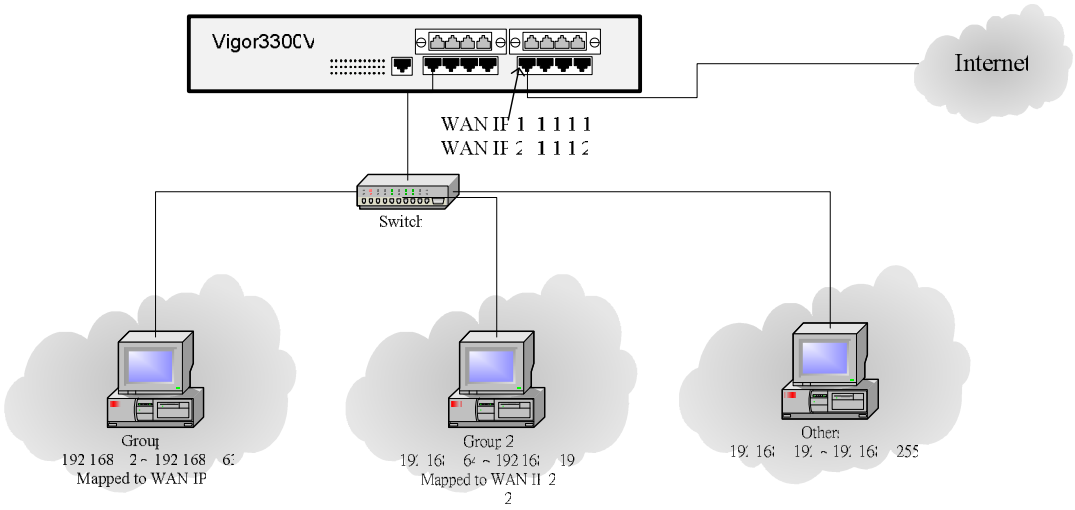


Figure 3-1. Example of the Multi-DMZ function

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.

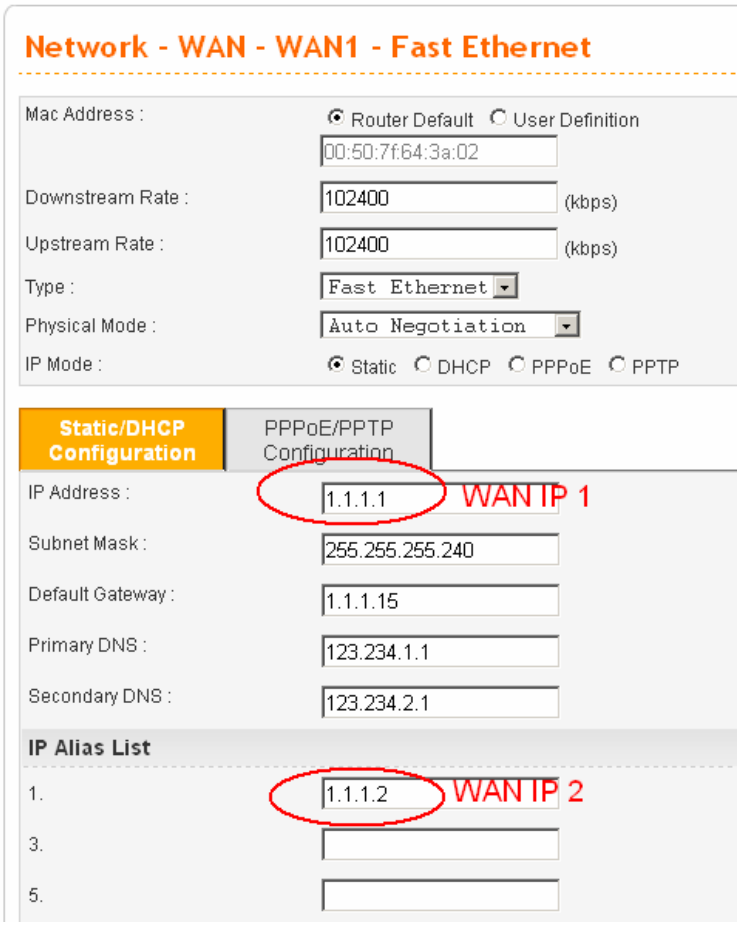


Figure 3-2. WAN configuration

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

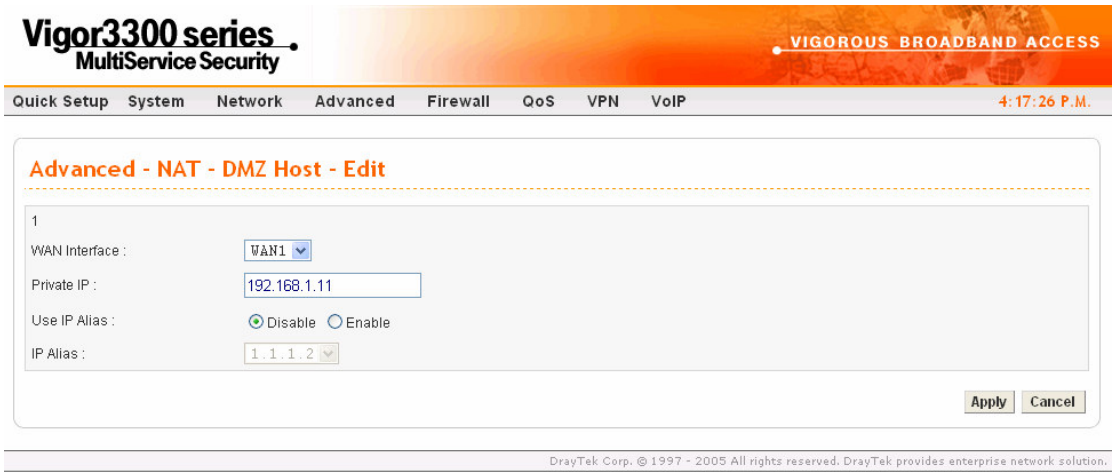


Figure 3-3. DMZ settings (host1)

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.

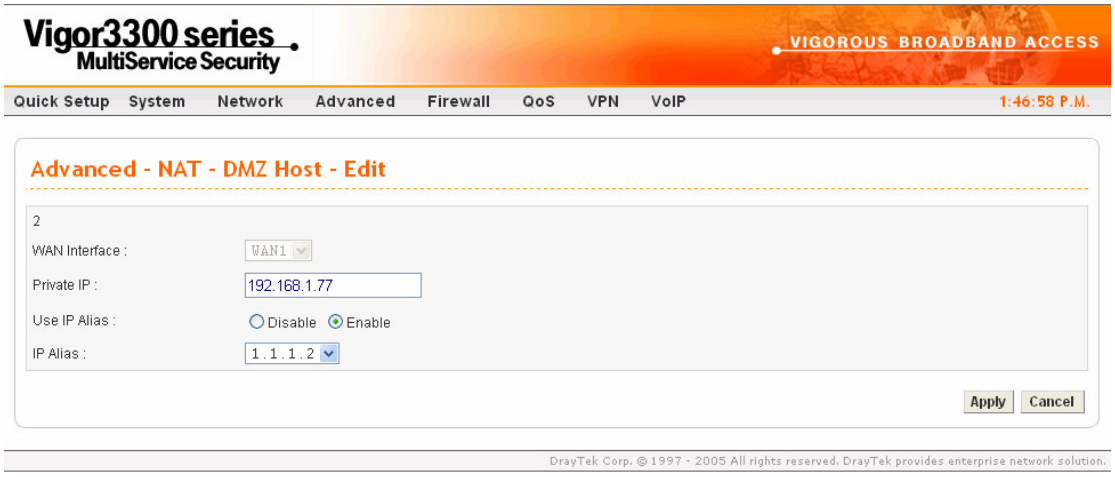


Figure 3-4. DMZ settings (host2)

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.

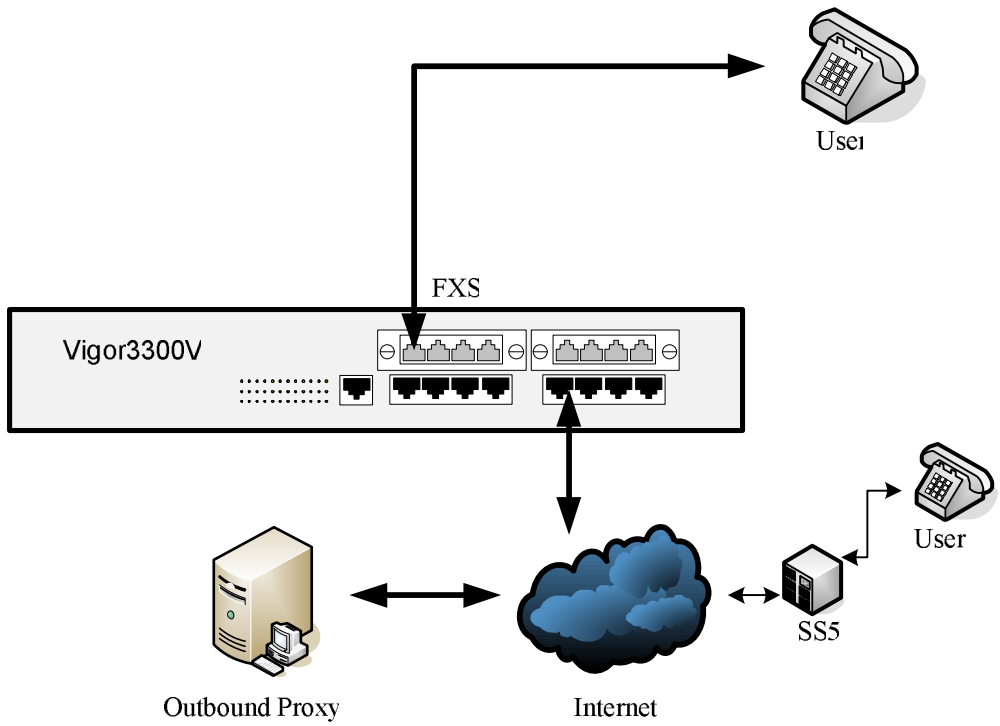


Figure 4-1. A Scenario of SIP outgoing calls in Vigor 3300V

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

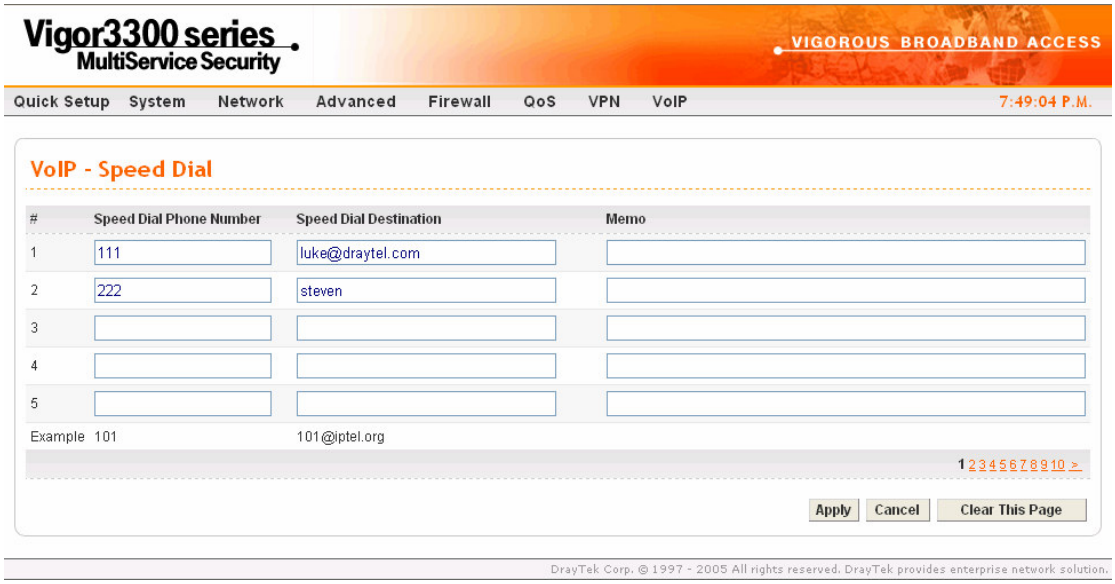


Figure 4-2. Speed dial settings

4.2.1 SIP Protocol Configurations (Case 1)

Proxy/Registrar: 1.1.1.1
Outbound Proxy: yes
Domain: domain.net

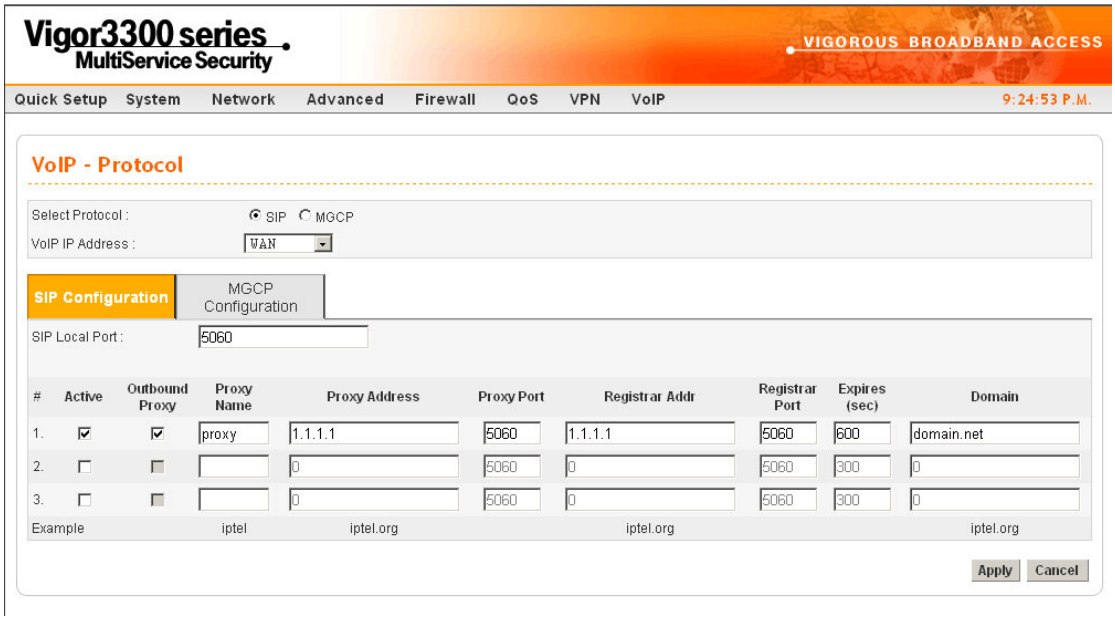


Figure 4-3. Case 1 SIP protocol configurations

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**

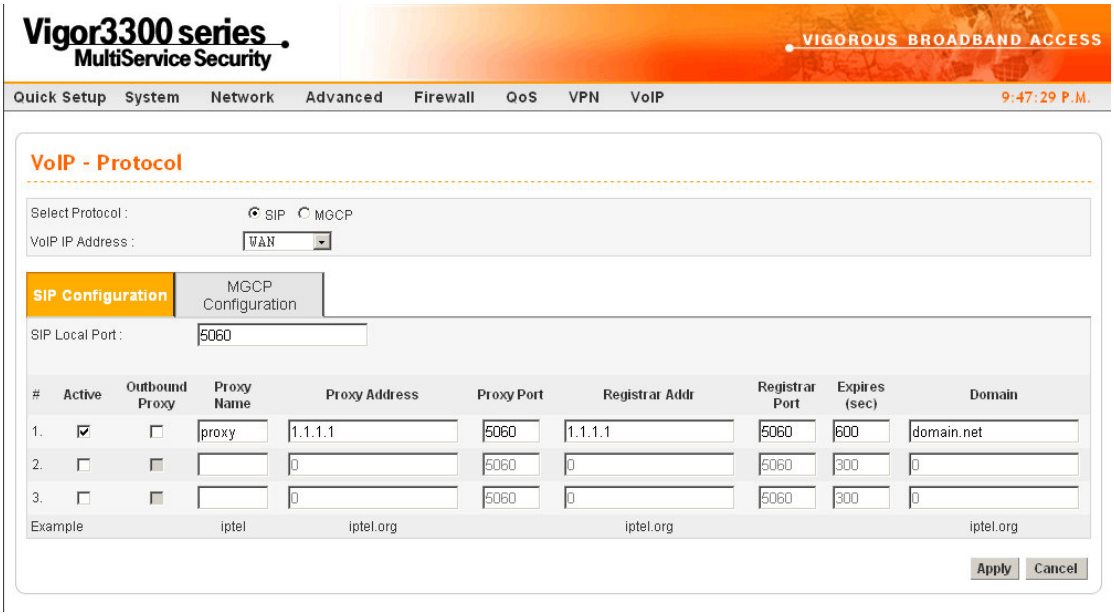


Figure 4-4. Case 2 SIP protocol configurations

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)**

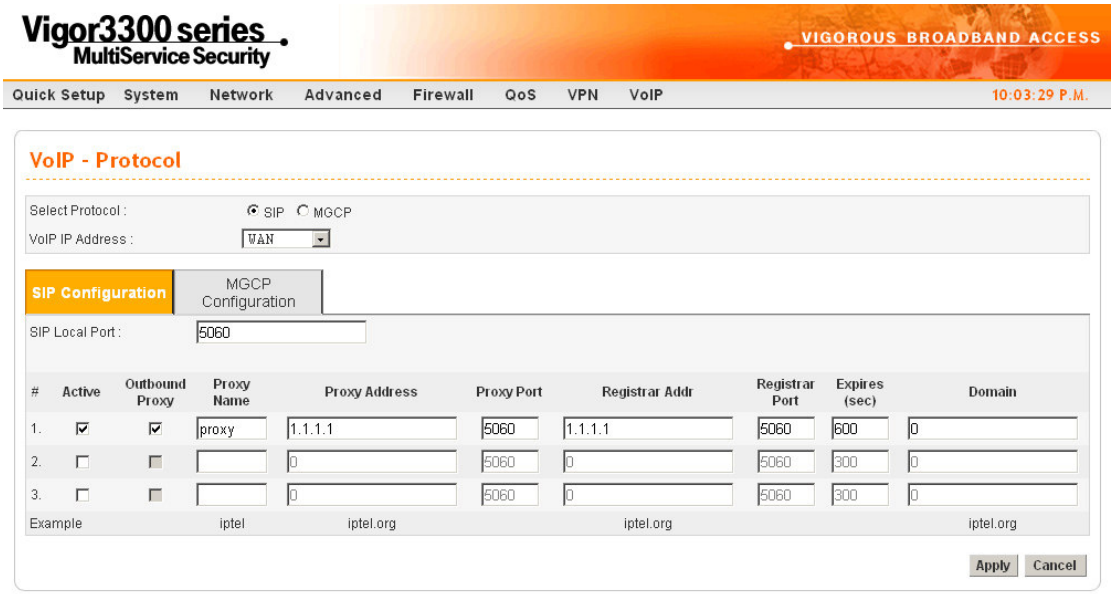


Figure 4-5. Case 3 SIP protocol configurations

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)

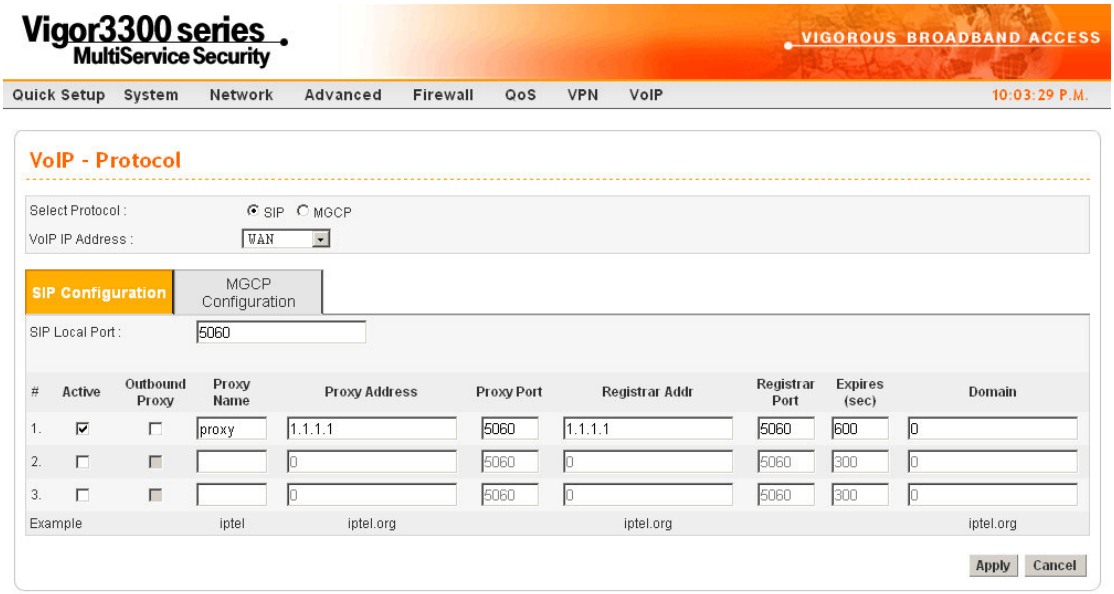


Figure 4-6. Case 4 SIP protocol configurations

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)**

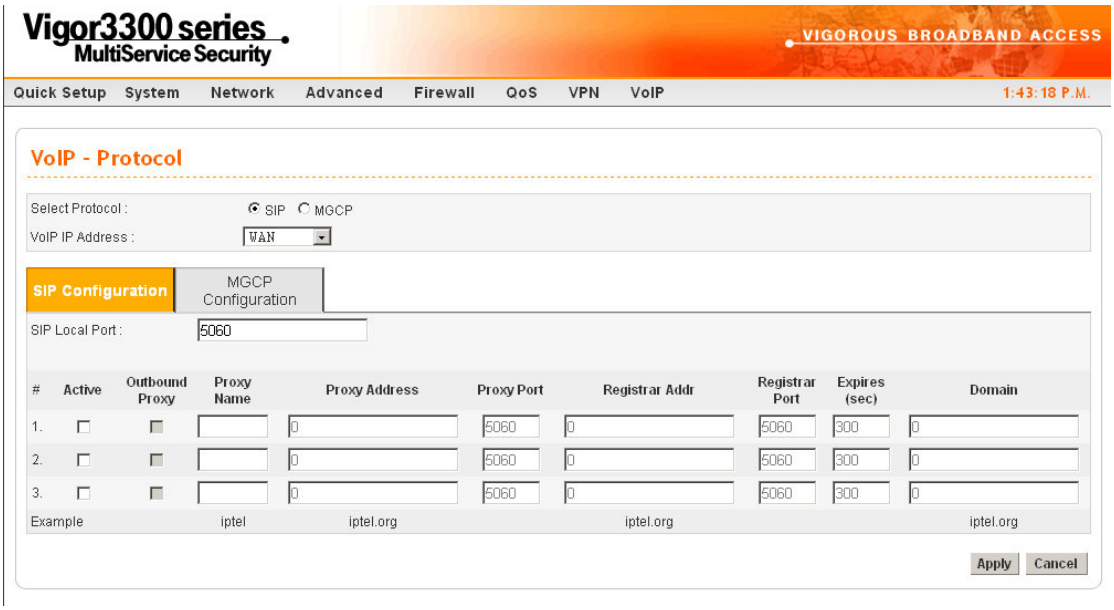


Figure 4-7. Case 5 SIP protocol configurations

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**

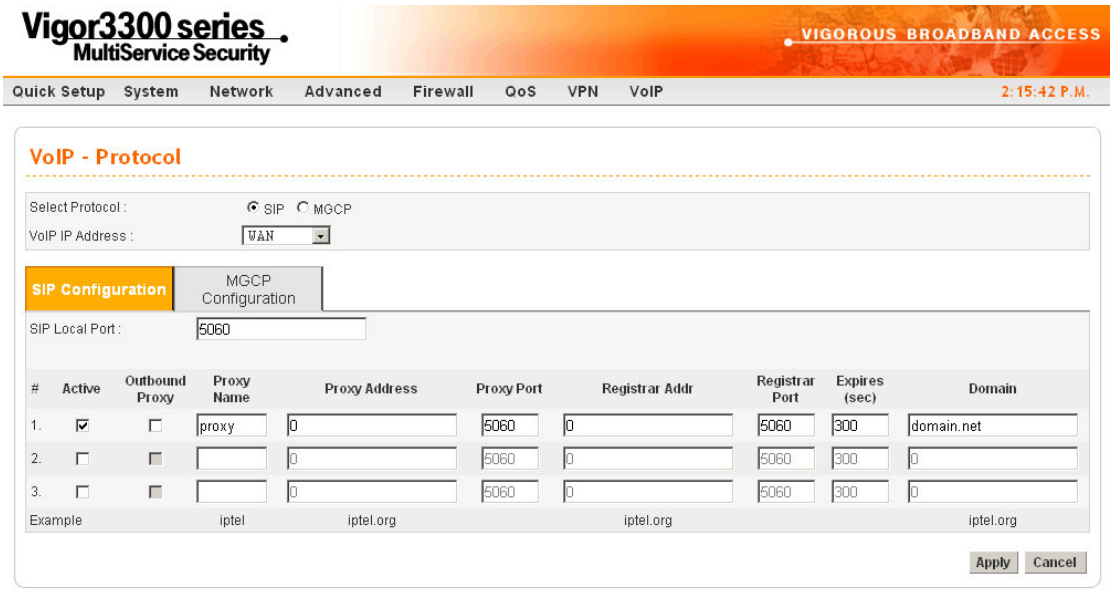


Figure 4-8. Case 6 SIP protocol configurations

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.

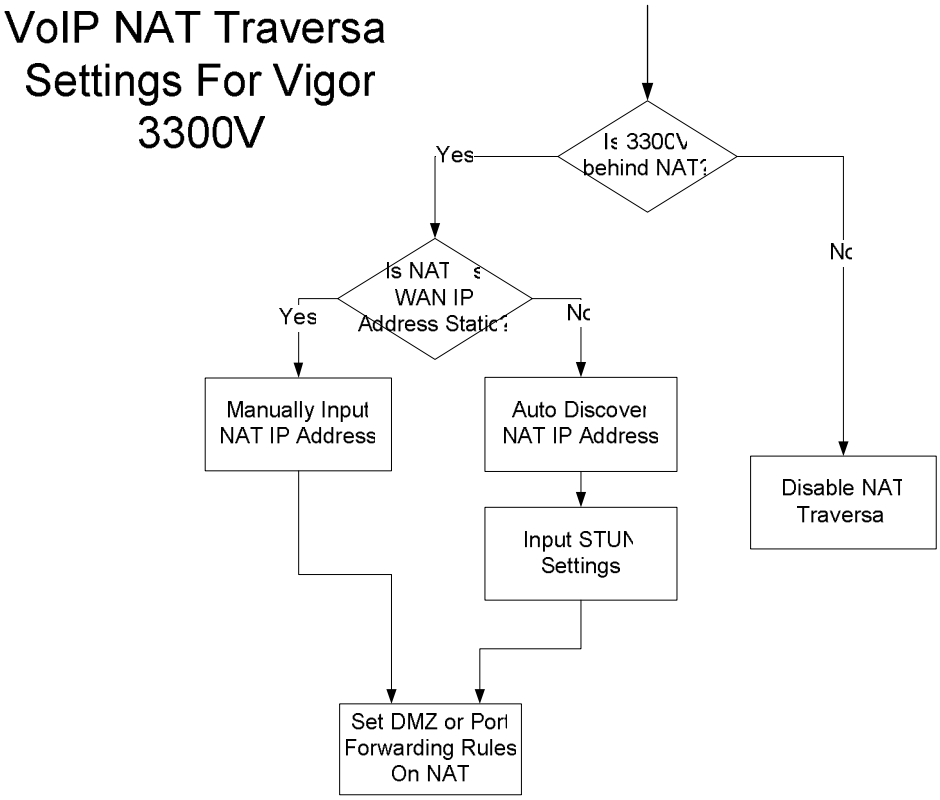


Figure 5-1. Flowchart of setting VoIP NAT Traversal function

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.

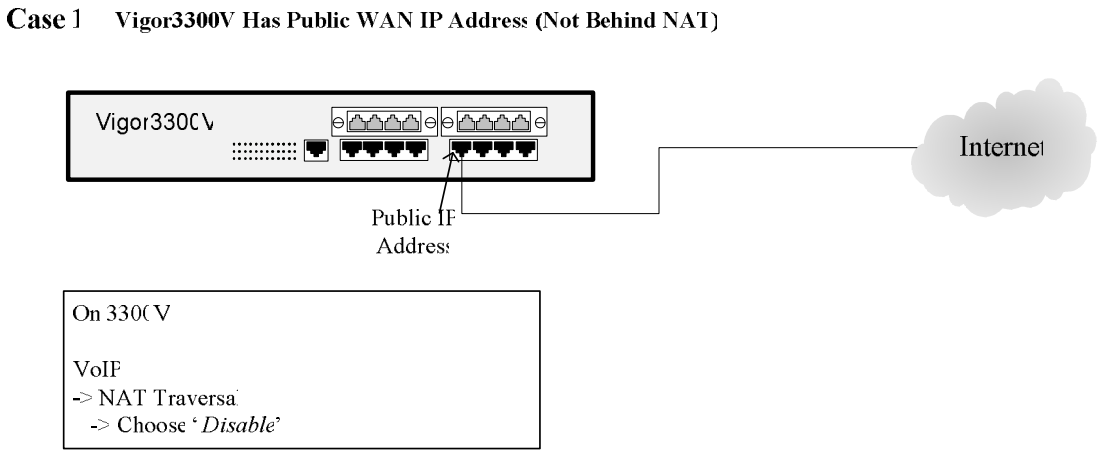


Figure 5-2. Case 1 Scenario

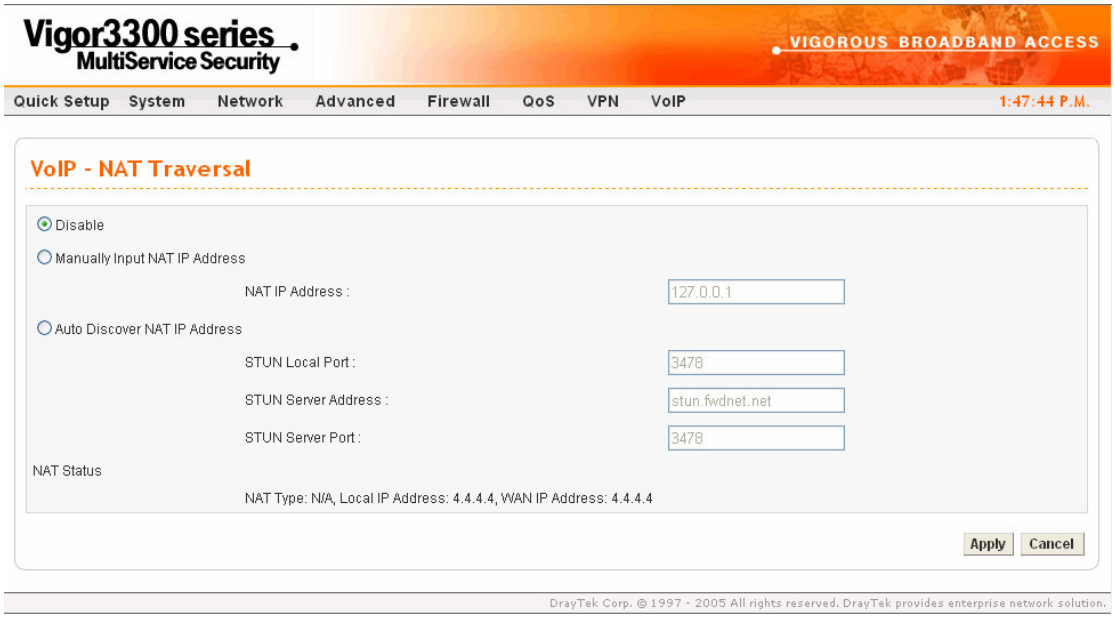


Figure 5-3. Case 1 settings

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.

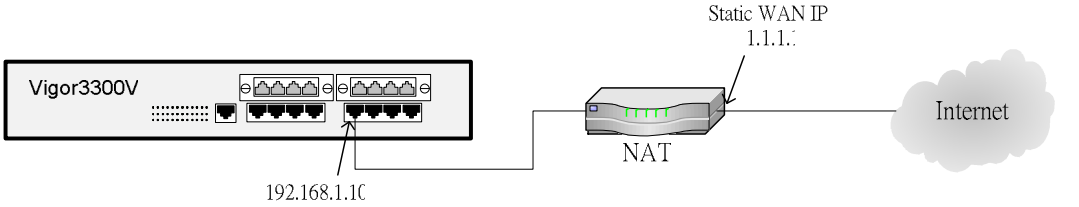
Set DMZ -> *192.168.1.10*
or
Set the following Port Forwarding Rules,

```
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
```

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)



On 3300V

VoIP
->NAT Traversa
-> Choose *"Manually Input NAT IP Address"*
-> Input *1.1.1.1*

On NAT

Set DMZ -> *192.168.1.10*
or
Set the following Port Forwarding Rules,

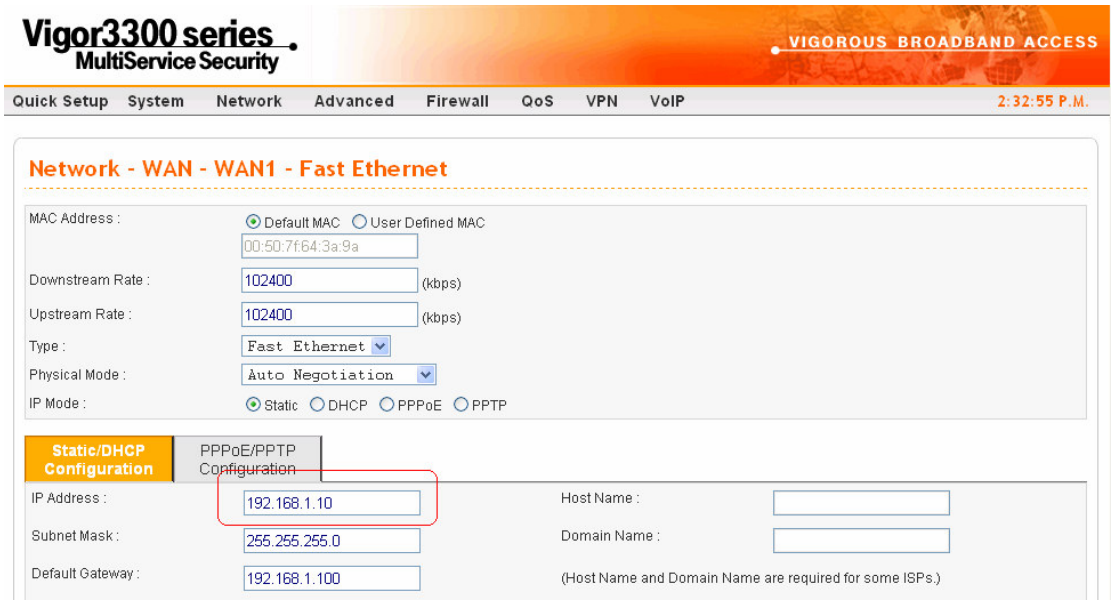
```
UDP Port 5060 (SIP)           Forward to   192.168.1.10
UDP Port 13456~13470 (RTP)    Forward to   192.168.1.10
UDP Port 49170~49184 (T.38)   Forward to   192.168.1.10
```

Figure 5-4. Case 2 Scenario

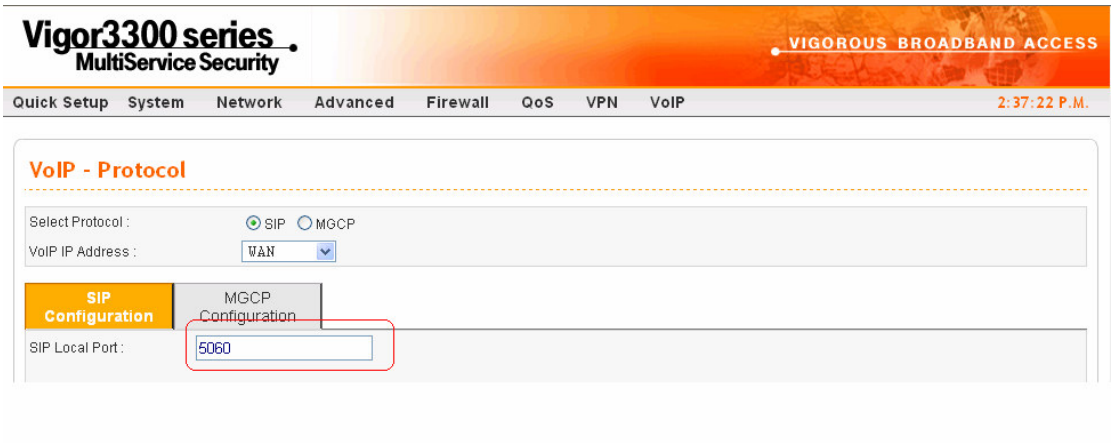
Figure 5-5 shows the Web settings on Vigor3300V.

(NAT Traversal)

(WAN)



(SIP Local Port)



(RTP and T.38 Ports)

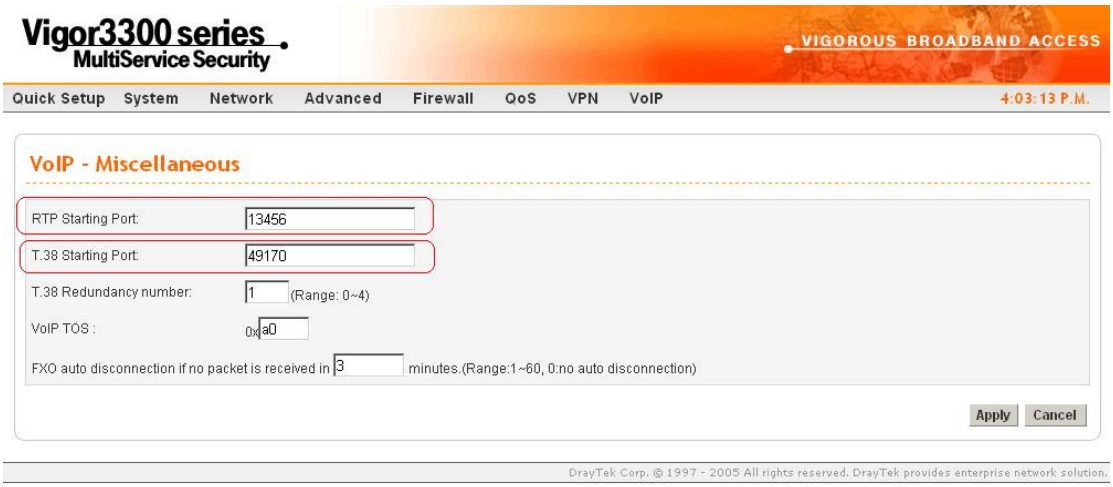


Figure 5-5. Case 2 settings

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)

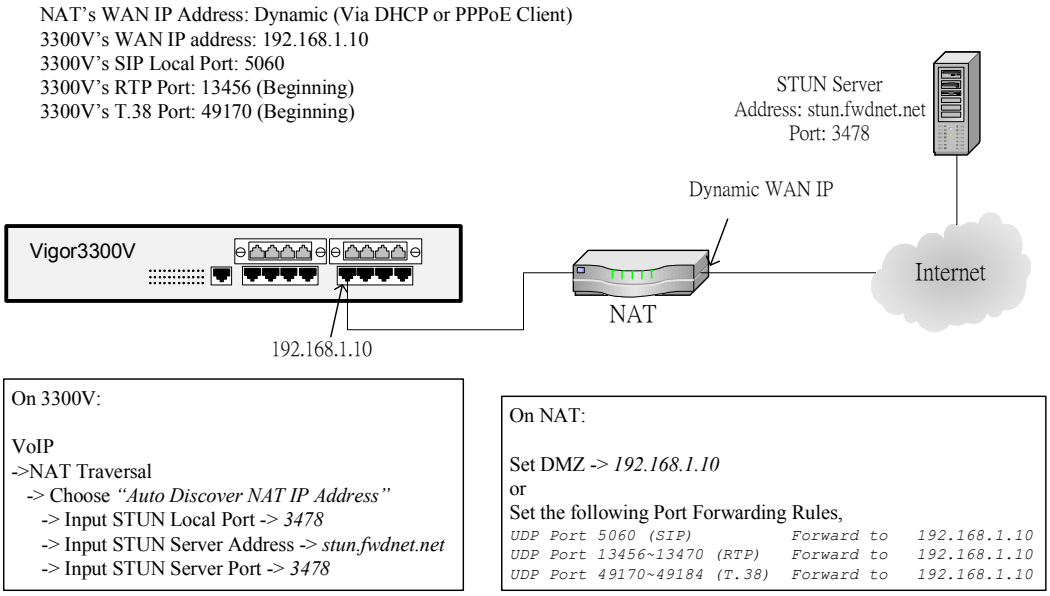


Figure 5-6. Case 3 scenario of NAT Traversal

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)

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.

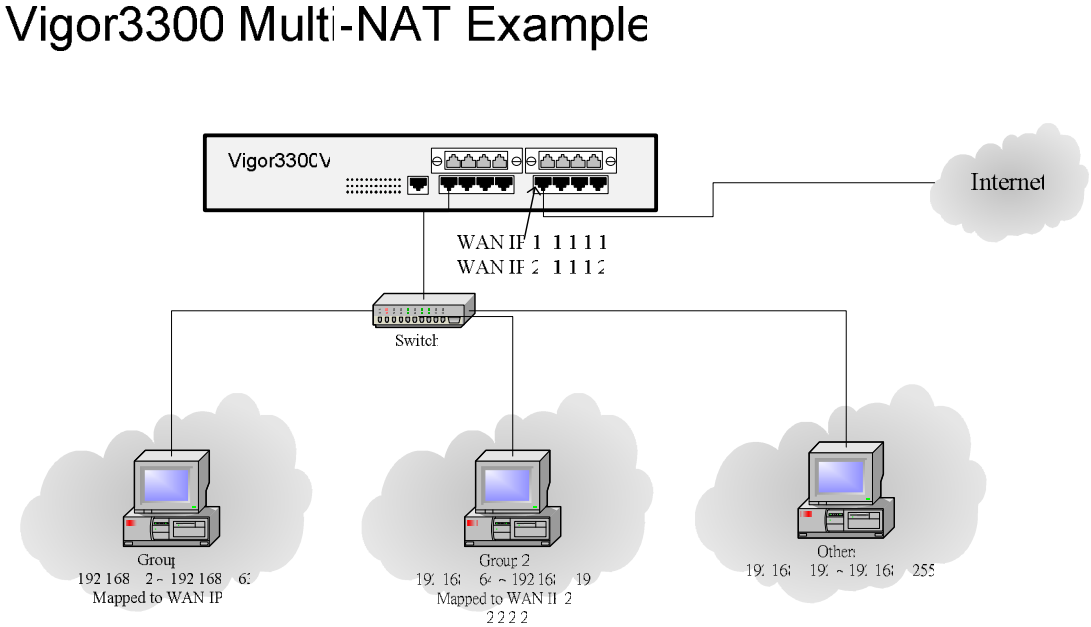


Figure 6-1. A Scenario of Multi NAT

6.2 Examples and Web Configurations

There are some steps as followings.

Step 1:

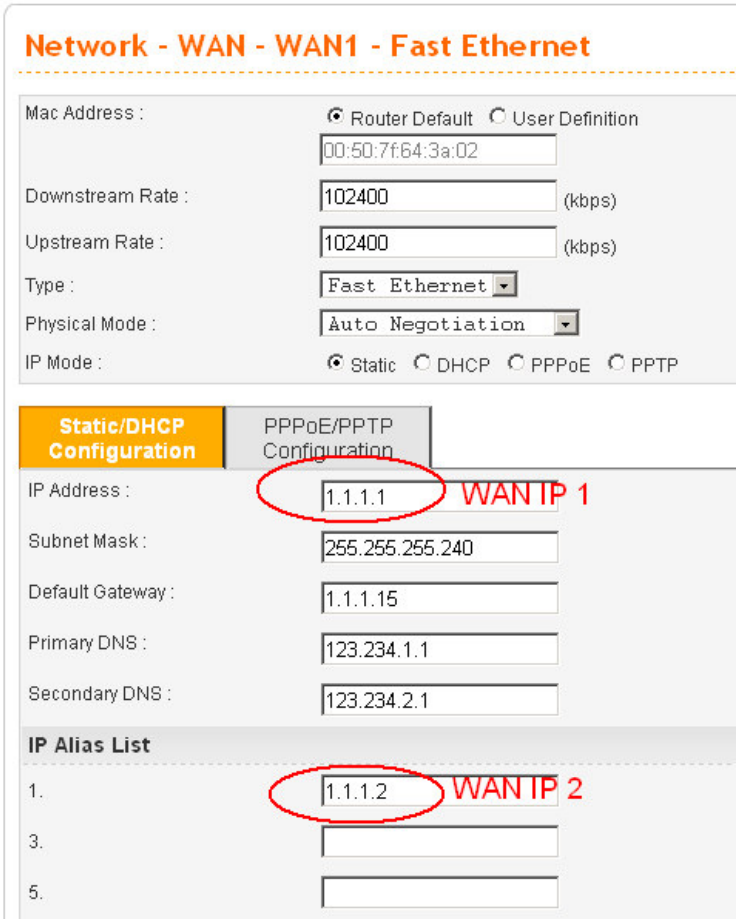
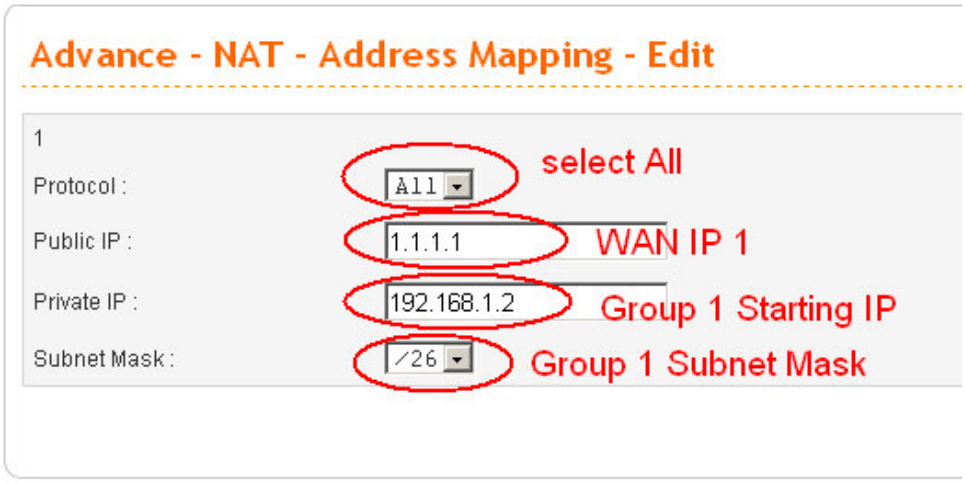
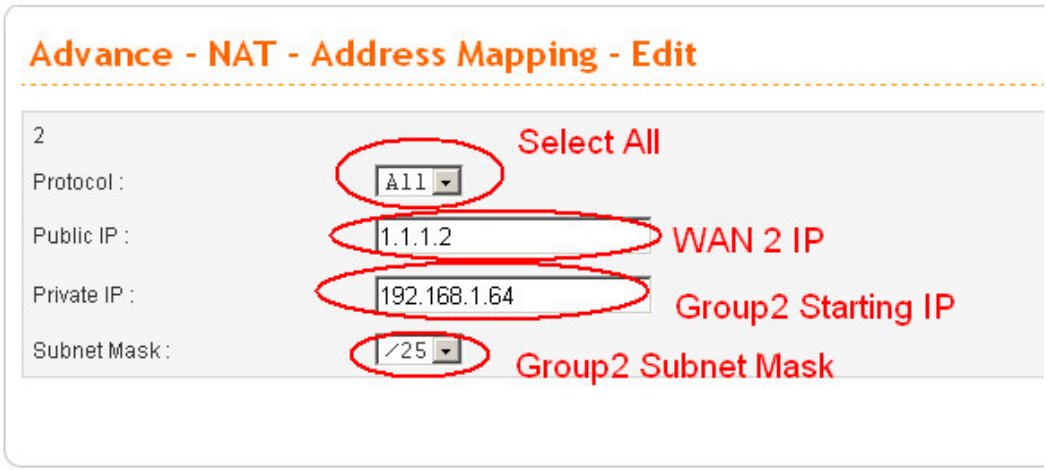


Figure 6-2. Step1 in WAN settings

Step 2



Step 3



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.

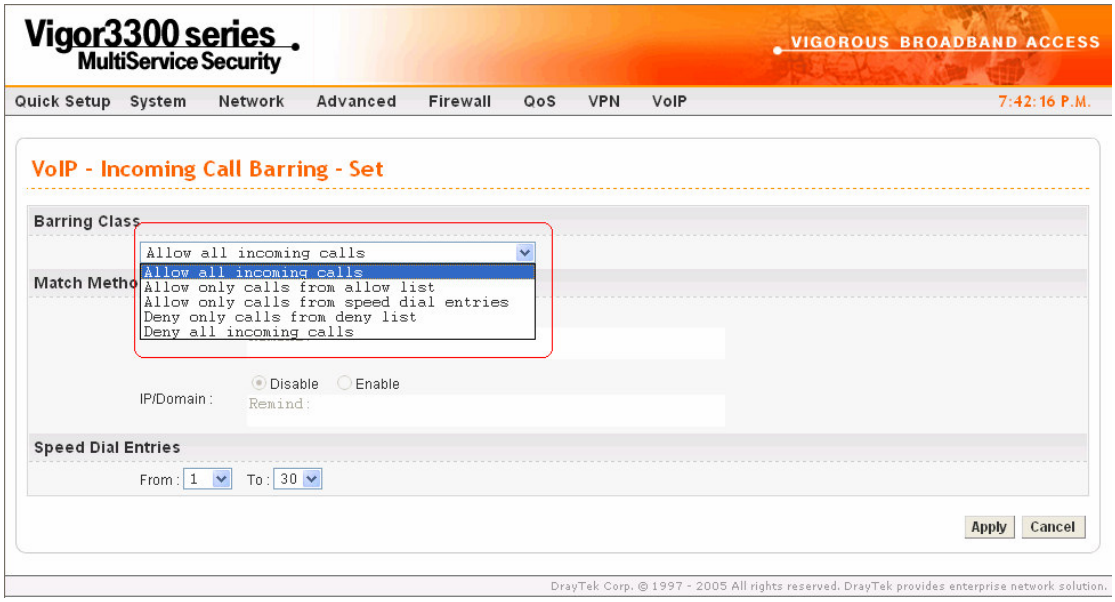


Figure 7-1. Barring Classes in Vigor3300V

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

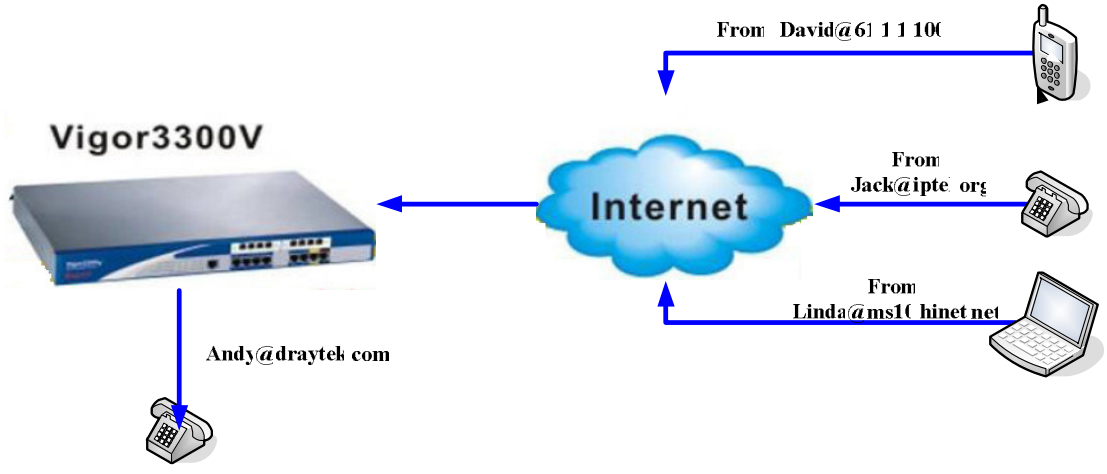


Figure 7-2. A Scenario on incoming call

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.

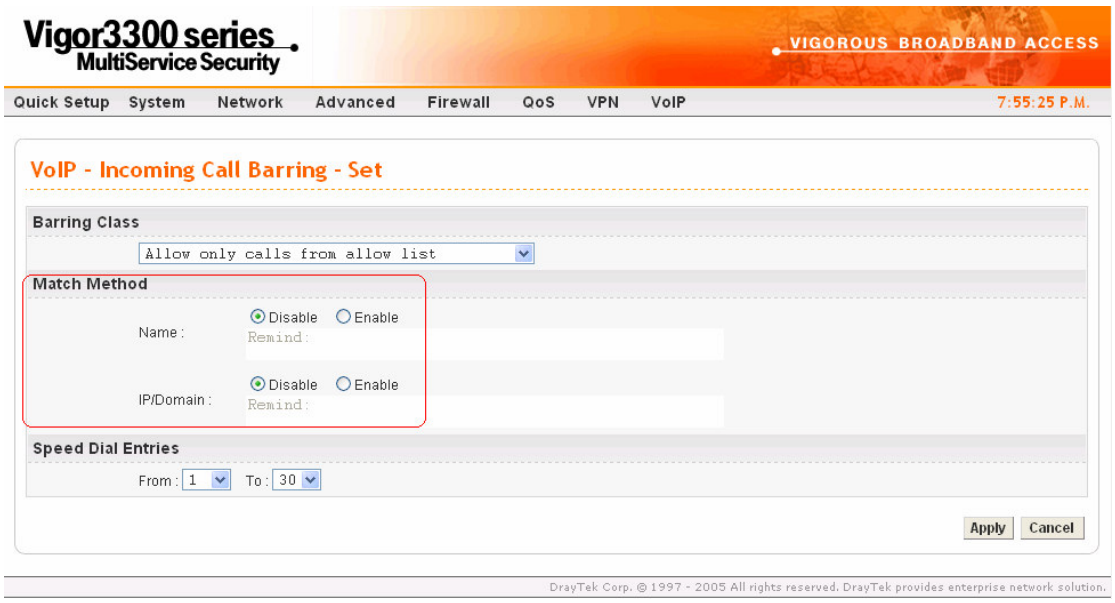


Figure 7-3. Comparing methods for incoming call barring

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.

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.

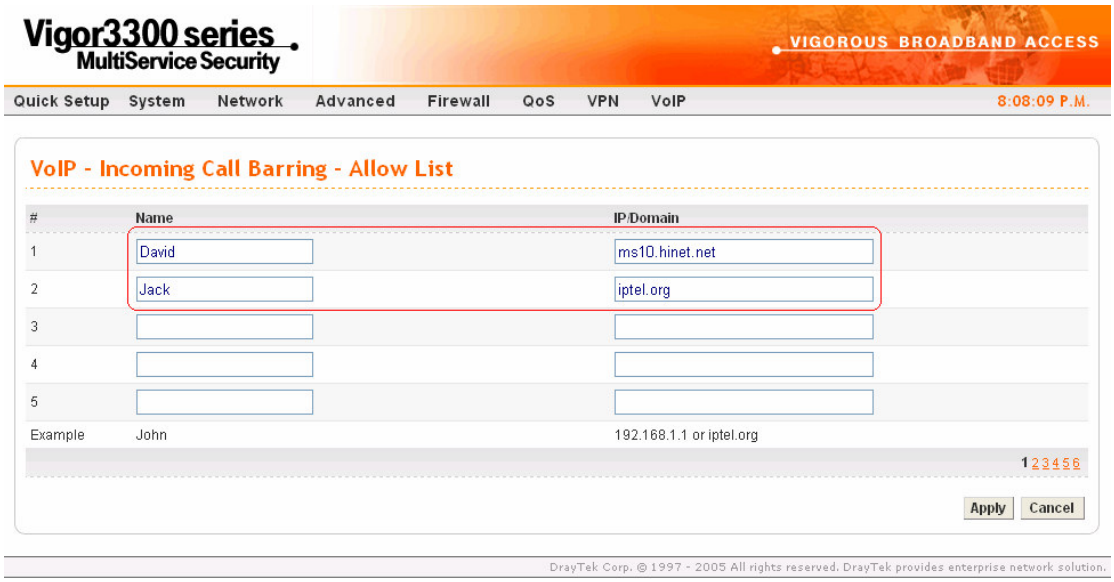


Figure 7-5. Allow List settings

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

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

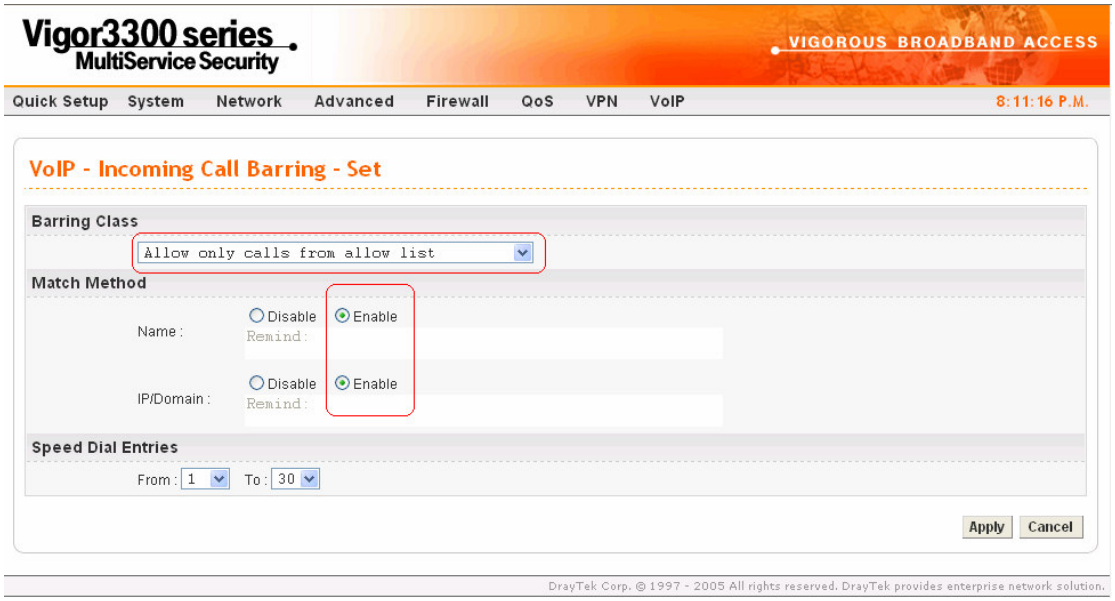


Figure 7-6. Match Method – Case 1 settings

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.

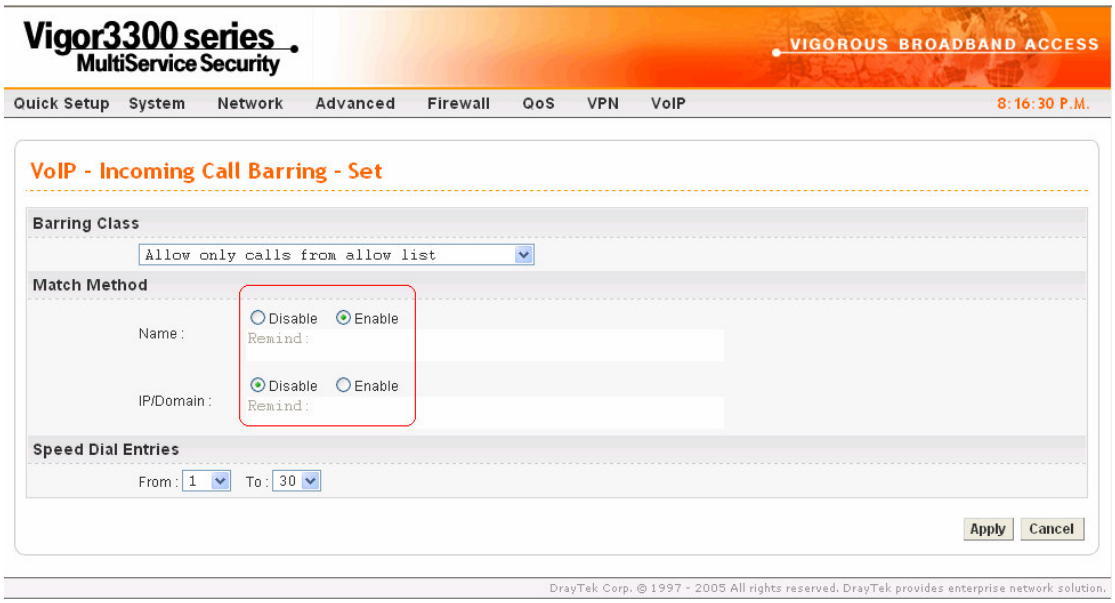


Figure 7-7. Match Method – Case 2 settings

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.

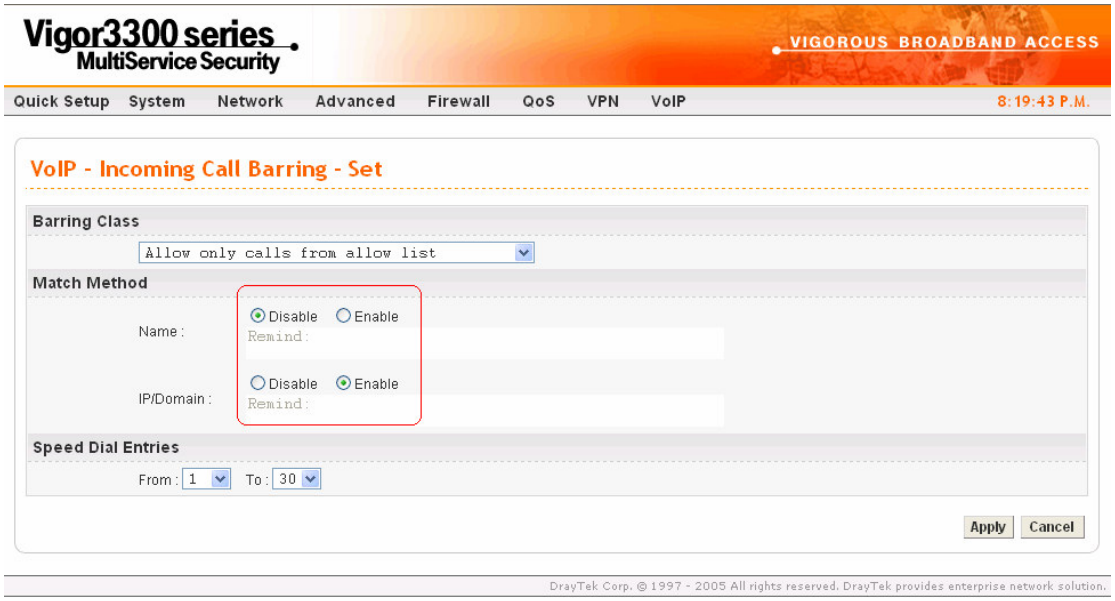


Figure 7-8. Match Method – Case 3 settings

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.

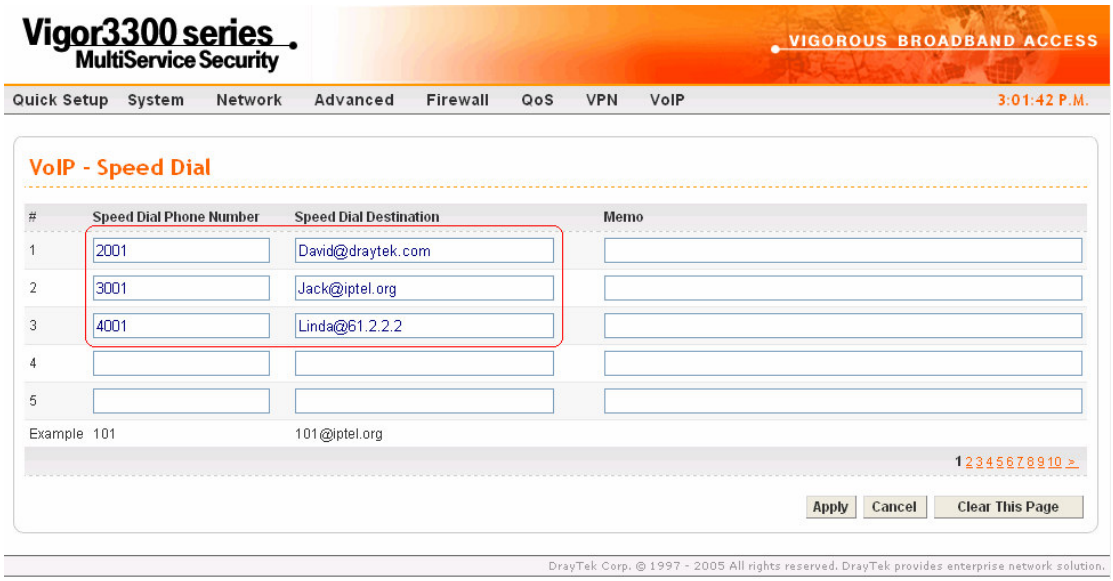


Figure 7-9. Speed Dial Table settings

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

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

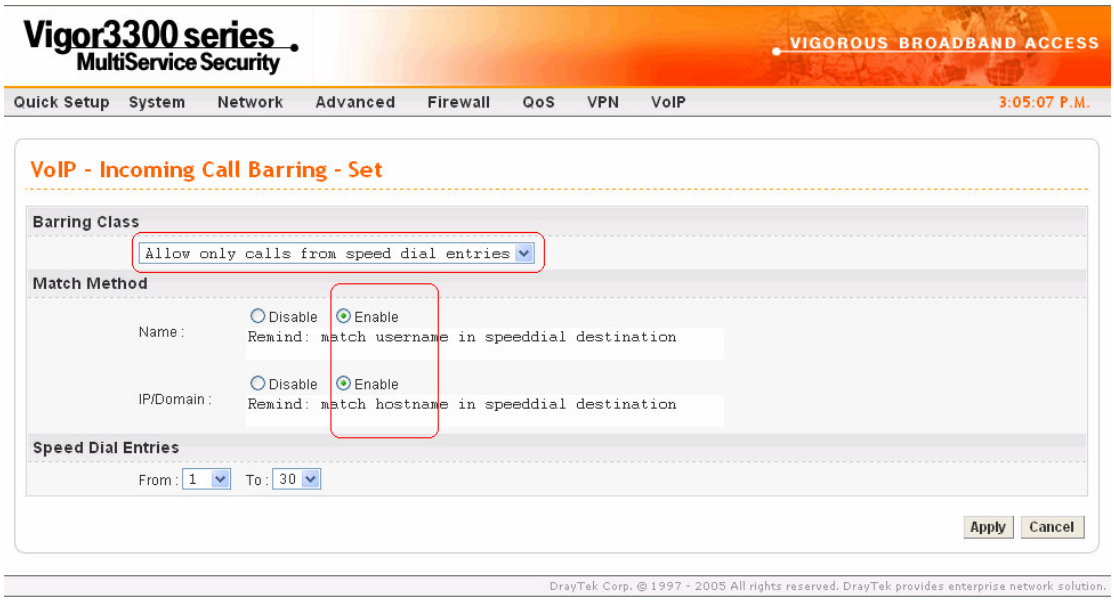


Figure 7-10. Match Method – Case 1 settings

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.

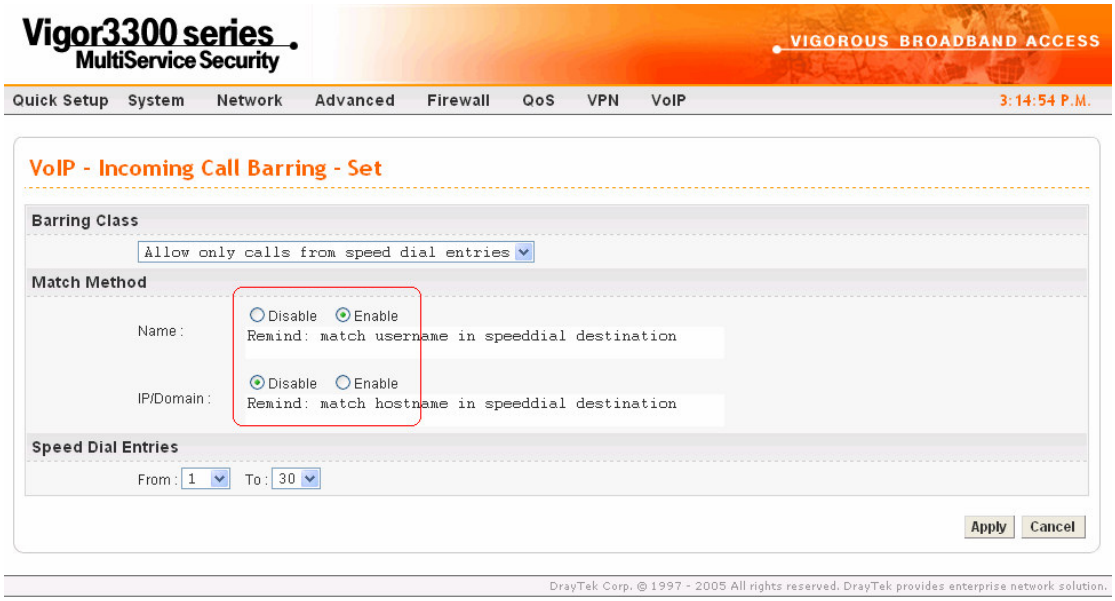


Figure 7-11. Match Method – Case 2 settings

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.

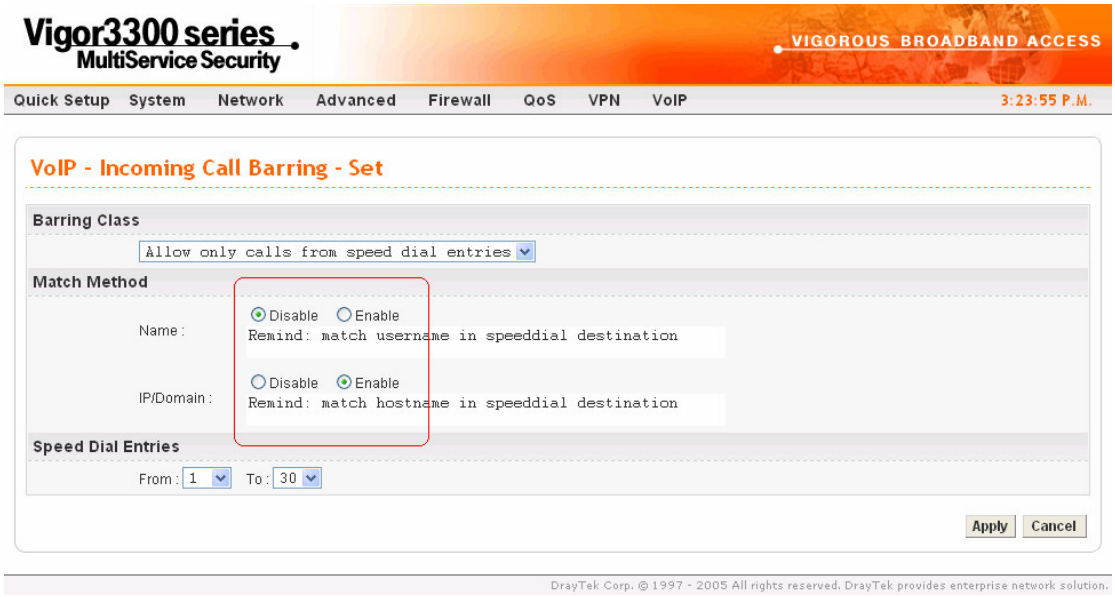


Figure 7-12. Match Method – Case 3 settings

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.

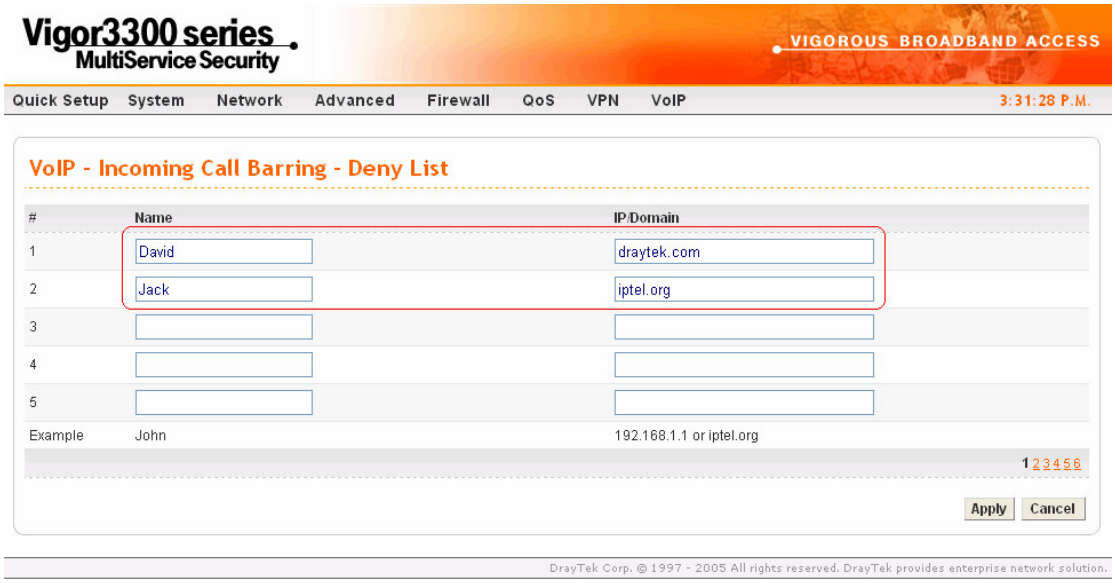


Figure 7-13. Deny List settings

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

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

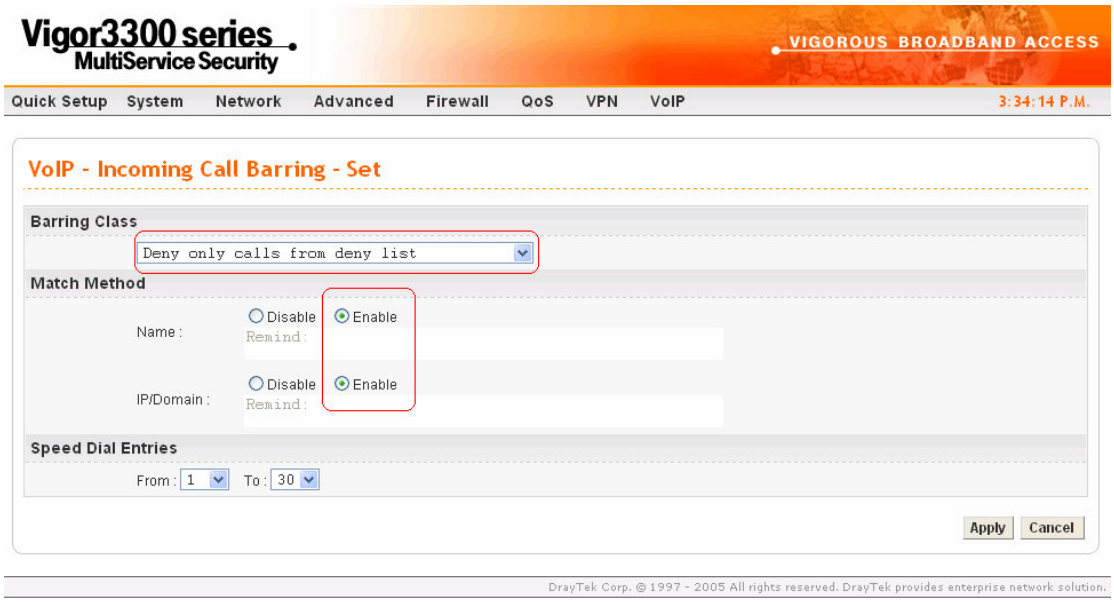


Figure 7-14. Match Method – Case 1 settings

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.

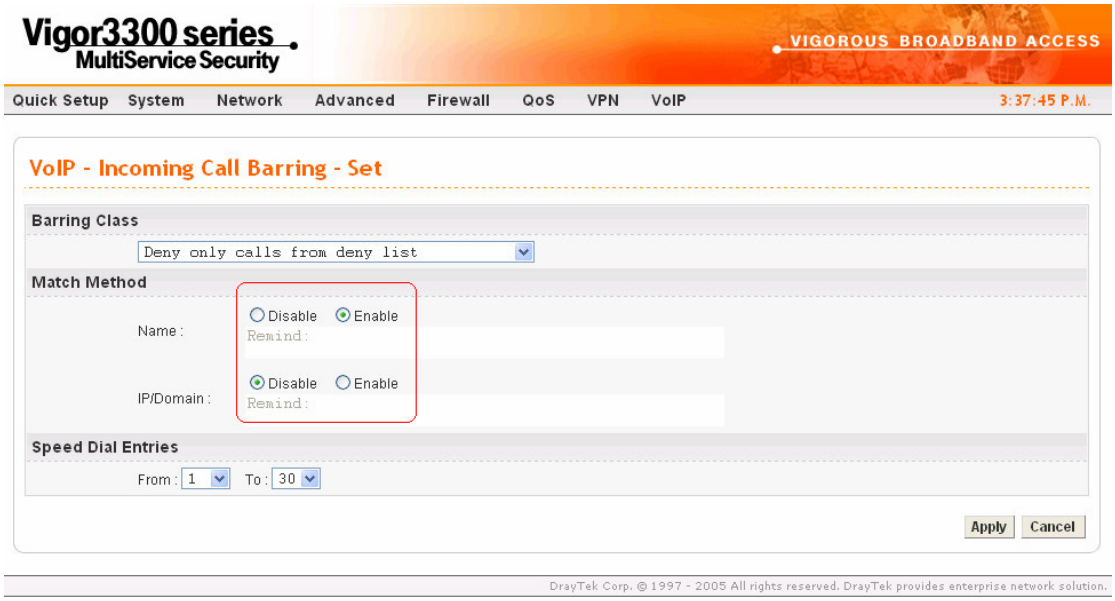


Figure 7-15. Match Method – Case 2 settings

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.

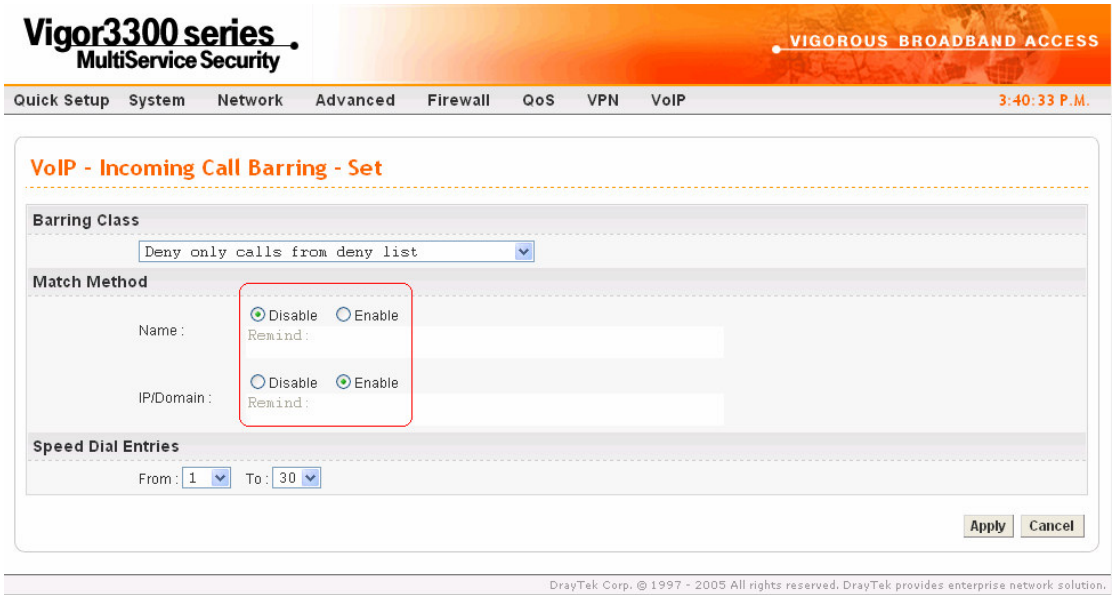


Figure 7-16. Match Method – Case 3 settings

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.

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.

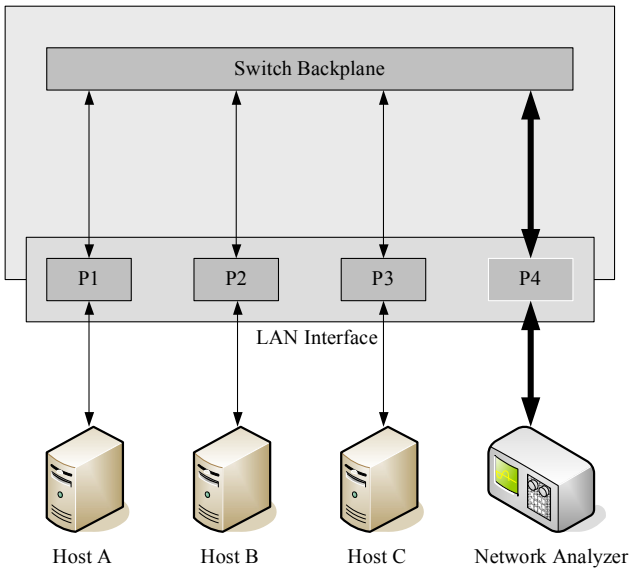


Figure 8-1. LAN Port mirroring

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.

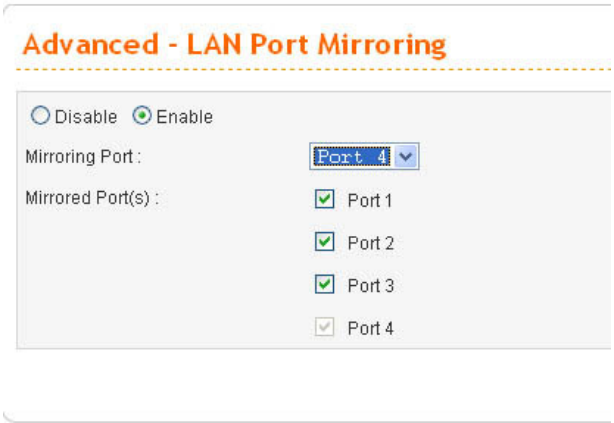


Figure 8-2. LAN Port Mirroring setting

CHAPTER 9
FXO Hot Line Function

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

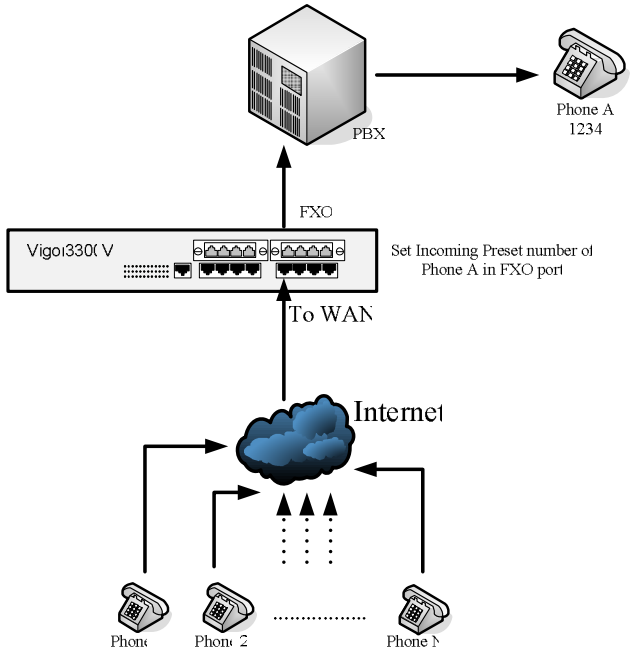
This chapter is divided into the following sections,

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

9.1 Introduction

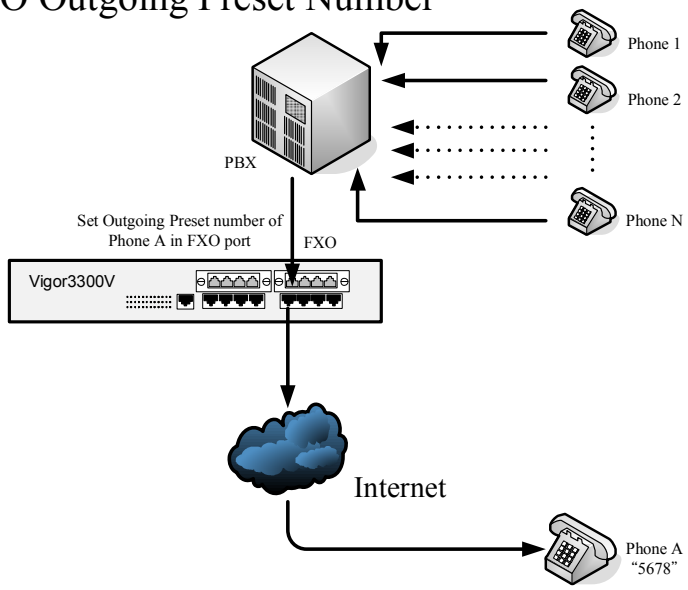
Hot line application is so very convenient for users in VoIP phone. It can shorten the dialing time for users to make a call to the destination. There are two scenario graphs in the Figure 9-1. One is incoming, the other one is for outgoing side.

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.

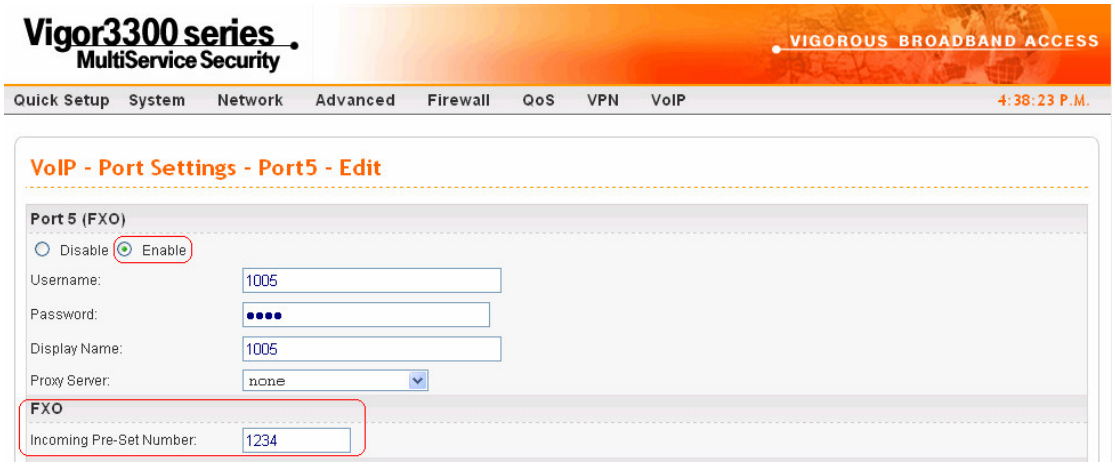


Figure 9-2. The Web settings of incoming preset number

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.

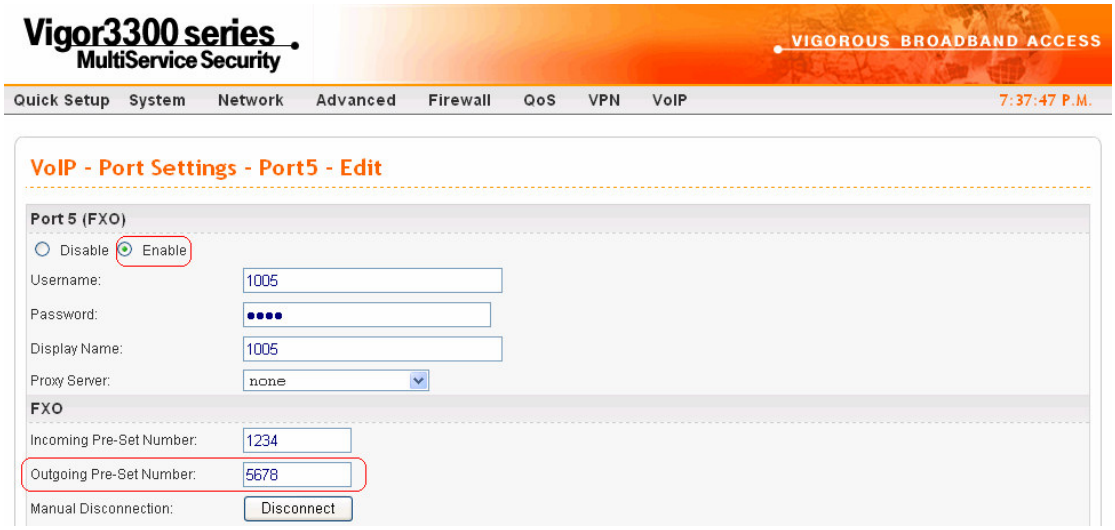


Figure 9-3. The Web settings of Outgoing preset number

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.