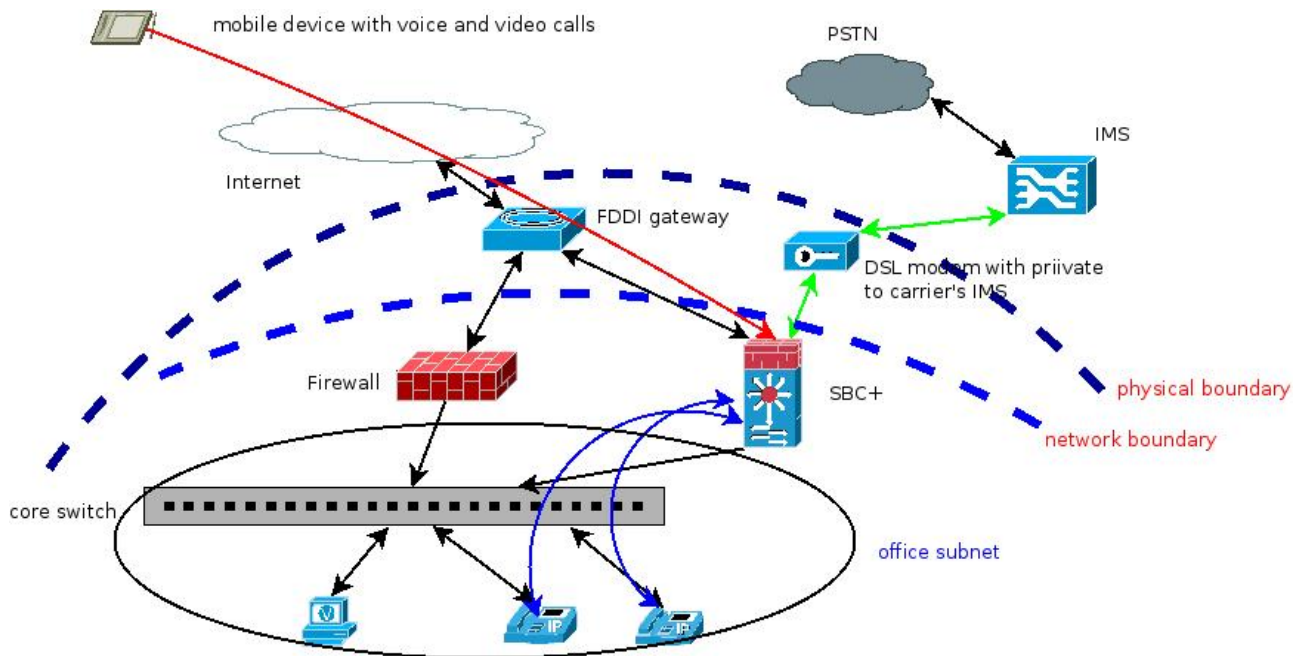


Deployment Guide with Chunghwa IMS

Abstract: This document is to summarize the deployment procedure for dealing with Chunghwa IMS in the field.

Introduction

Chunghwa telecom is with two systems for IMS – one is NGN IMS and the other is Mobile IMS. But at the moment of writing this document (Jan, 2017) only NGN IMS is allowed to be connected directly from customers. In this document, we simply describe the environment in the field. The connection to IMS from CPE (Customer Premises End) is provided by using Chunghwa's MOD (Multimedia on Demand) infrastructure with dedicated circuit (ATM PVC or MPLS over DSL); it is not exposed to the Internet.

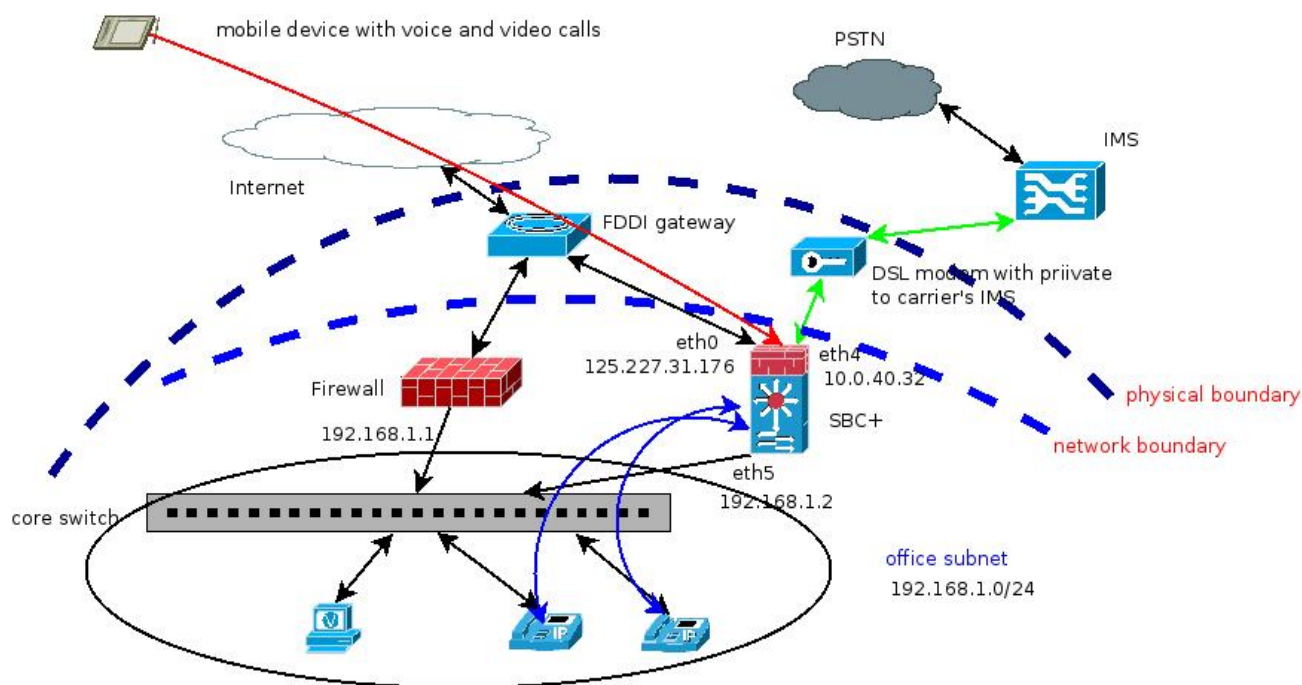


However, that link should still be considered as “insecure” due to the fact that there are other Chunghwa's customers on that network. In our system's factory setup, only “eth0” is used as “WAN” port to connect to the Internet. In this case, another Ethernet port will be used as another WAN port to connect to IMS.

In the setup for the connection to the Internet, an IP address with netmask and default gateway will be provided by the ISP; similarly, on the connection to IMS, another set of IP address, netmask, and default gateway will be provided. Usually on normal condition at one host, there is only one “default” gateway.

The function of the “default” gateway is: if you do not know which gateway to send the packets to the destination, then send to the “default” gateway. If we can spell all the subnets on the connection to IMS one by one, we probably can enter routing entries one by one by using that gateway. However, sometimes it is not possible to do that even if we know that network is not as large as the Internet; it is still quite large. To be flexible to adapt to the condition, we just create another routing table in addition to the main routing table and force specific traffic to look into this routing table only. Thus, on each routing table, it can have its own “default” gateway.

The following is an example with IP addresses specified: the port “eth0” is connected to the Internet, “eth4” is connected to the network with IMS, and “eth5” is connected to the office local network:



In the following sections, we list the associated steps with the screen snapshots. For more details, please refer to the manual.

Changing IP addresses and Port Configuration

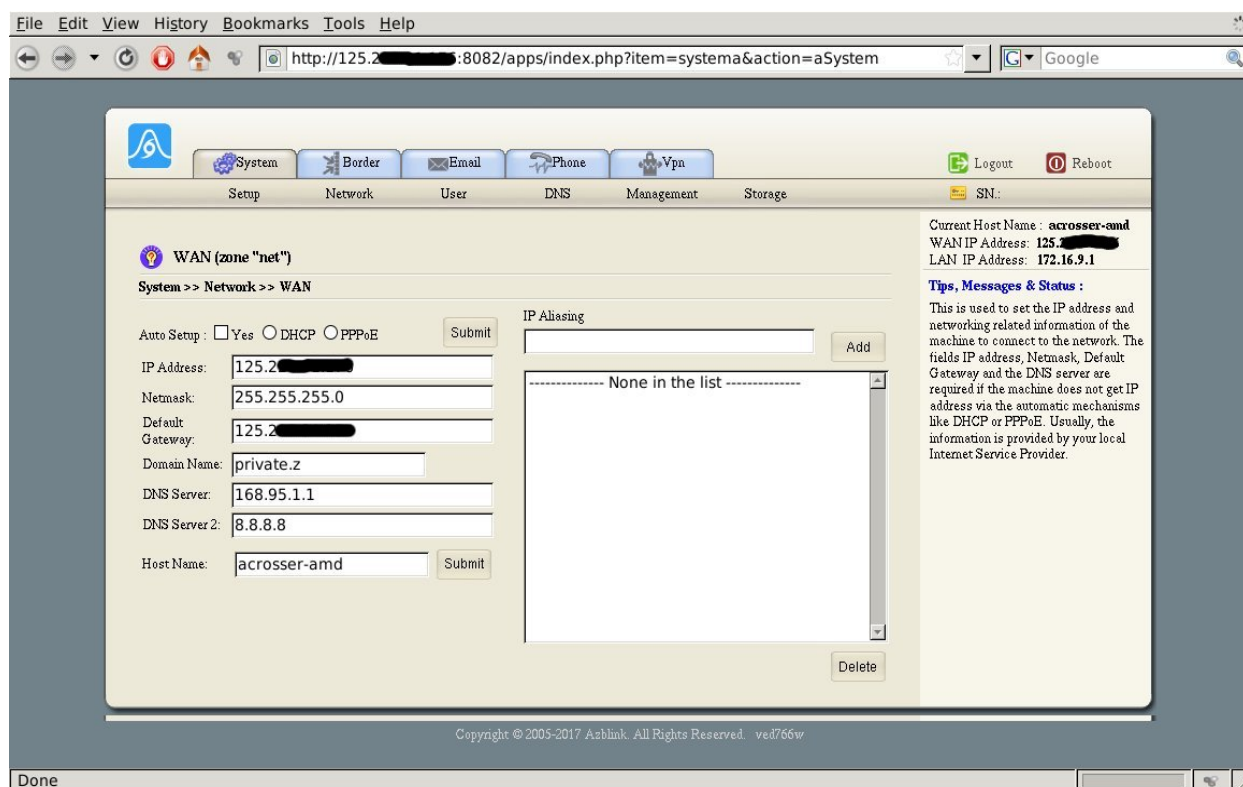
The WAN IP address can be changed at “**System >> Network >> WAN**”:

The screenshot shows a web-based network management interface. The top navigation bar includes tabs for System, Border, Email, Phone, Vhost, and Vpn. The main content area is titled "WAN (zone 'net')". It contains several input fields for configuration: IP Address (192.168.11.201), Netmask (255.255.255.0), Default Gateway (192.168.11.49), Domain Name (private.z), DNS Server (206.13.28.12), DNS Server 2 (172.16.9.1), and Host Name (iCenter-Server1). There are "Submit" buttons for the Auto Setup section and the Host Name field. An "IP Aliasing" section is also present with an "Add" button and a list showing "None in the list". A "Delete" button is at the bottom right. On the right side, there is a status box showing "Current Host Name : iCenter-Server1", "WAN IP Address: 192.168.11.201", and "LAN IP Address: 172.16.9.1". Below this, a "Tips, Messages & Status" section provides information about setting IP addresses and DNS servers. The bottom status bar indicates "Transferring data from 192.168.11.201..."

If we are given with the following information from ISP:

IP address: 125.23.2.12
Netmask: 255.255.255.0
gateway: 125.23.2.254

then we can change the setting accordingly. The screen will look as follows:



And this is the setting for “eth0” – the port we intend for the use of the Internet.

The next step is: we want to use “eth4” to connect to IMS network and “eth5” for the office local network. The Ethernet ports “eth4” and “eth5” belong to the region “loc” (Local network) and we would like to change “eth4” from “loc” (Local Network) to “net” (Internet/WAN). On “eth4” (to IMS network), we have

IP address: 10.0.40.132
Netmask: 255.255.248.0
Gateway: 10.0.47.254

And the IP address of “eth5” is given as

IP address: 192.168.1.2
Netmask: 255.255.255.0

The setting of IP address and Netmask for each port can be done via **“System >> Network >> Ethernet / DHCP”**:

File Edit View History Bookmarks Tools Help

Login Admin

System Border Email Phone Vhost Vpn Logout Reboot

Setup Network User DNS Management Storage SN:

Ethernet / DHCP

System >> Network >> Ethernet / DHCP

Ethernet Bridge (br0)

IP Address: 172.16.35.253 Netmask: 255.255.255.0

Start IP: 172.16.35.100 End IP: 172.16.35.200

☐ Turn on DHCP Server

☐ Enable Bridge br0

Ethernet Ports in Bridge br0: tap0 eth1 eth2 eth3 eth4

Ethernet Bridge (br1)

IP Address: 172.16.36.253 Netmask: 255.255.255.0

Start IP: 172.16.36.100 End IP: 172.16.36.200

☐ Turn on DHCP Server

☐ Enable Bridge br1

Ethernet Ports in Bridge br1: tap1 eth5

Current Host Name: iCenter-Server1
WAN IP Address: 192.168.11.201
LAN IP Address: 172.16.9.1

Tips, Messages & Status :

This is to set the IP address and DHCP server for each of the Ethernet ports except eth0. The system is implemented with DHCP server running on the 2nd and 3rd Ethernet ports if there are two or three Ethernet ports on the machine. The DHCP server can be turned on/off. If turned on, the administrator can set the IP range so that the DHCP server will only assign those IP addresses within the defined range for IP devices with DHCP clients in the subnet.

They are changed as follows by turning off DHCP server on each port:

File Edit View History Bookmarks Tools Help

http://125.203.21.135:8082/apps/index.php?item=systema&action=aSystem Google

eth1 ☒ Turn on DHCP Server

IP Address: 172.16.9.1 Netmask: 255.255.255.0

Start IP: 172.16.9.100 End IP: 172.16.9.200

eth2 ☒ Turn on DHCP Server

IP Address: 172.16.1.1 Netmask: 255.255.255.0

Start IP: 172.16.11.100 End IP: 172.16.11.200

Extra Ethernet Interface Setting

eth3 ☒ Turn on DHCP Server

IP Address: 172.16.12.1 Netmask: 255.255.255.0

Start IP: 172.16.12.100 End IP: 172.16.12.200

eth4 ☐ Turn on DHCP Server

IP Address: 10.0.40.132 Netmask: 255.255.248.0

Start IP: 172.16.13.100 End IP: 172.16.13.200

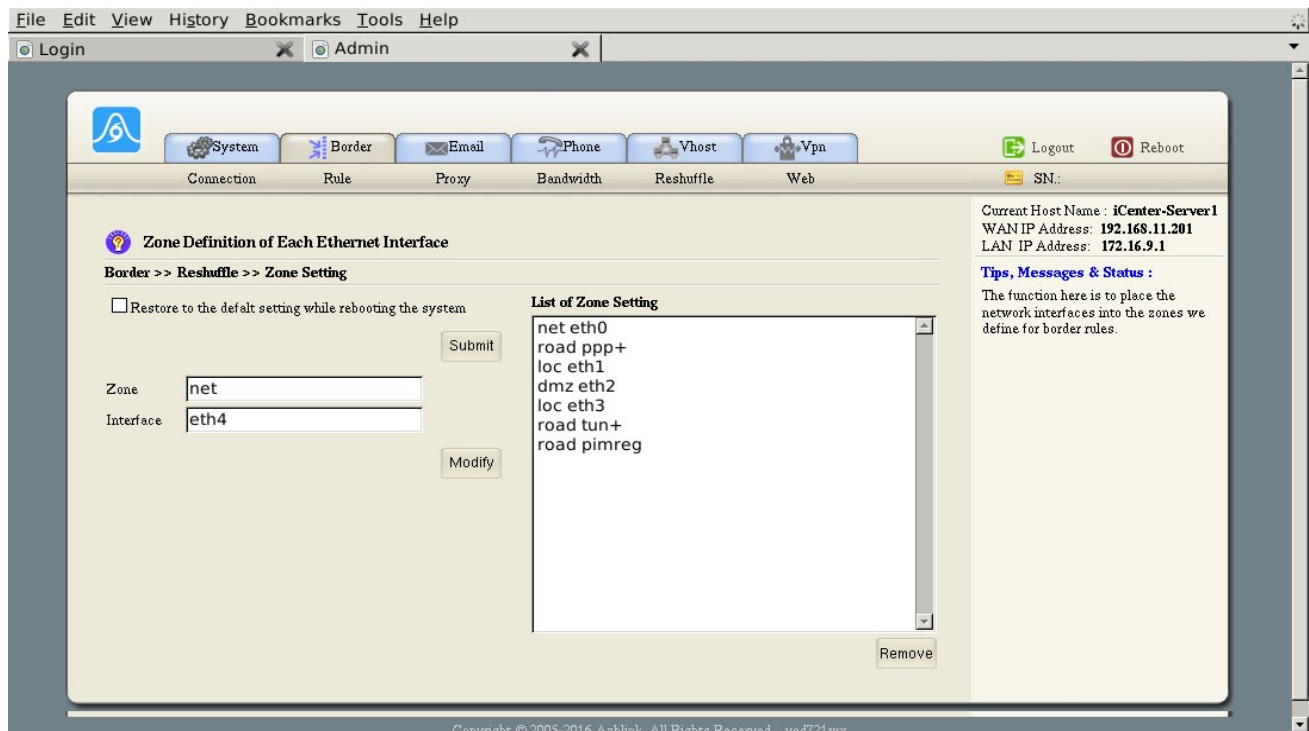
eth5 ☐ Turn on DHCP Server

IP Address: 192.168.1.2 Netmask: 255.255.255.0

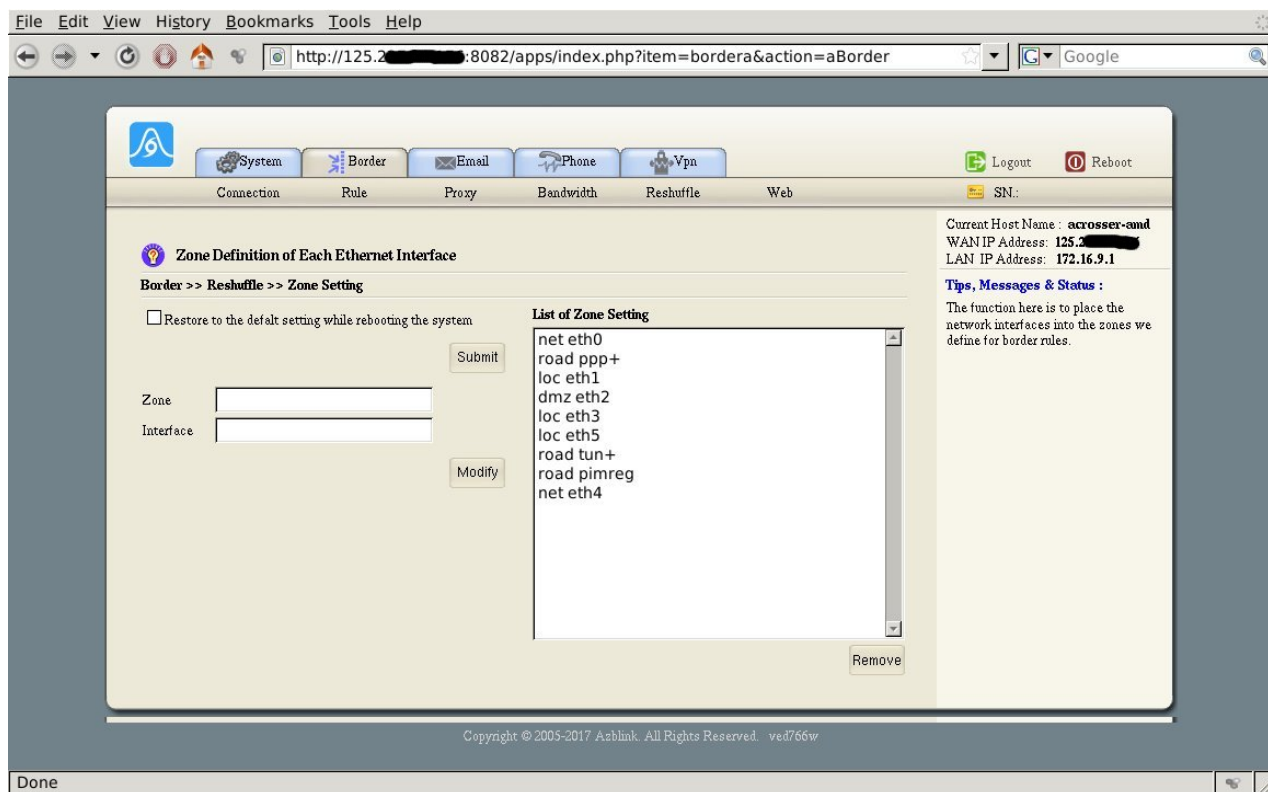
Start IP: 192.168.1.100 End IP: 192.168.1.200

Done

And remember that we want to change “eth4” from “loc” to “net”. We start from “**Border >> Reshuffle >> Zone Setting**” by removing the original zone of “eth4”, and uncheck the box to avoid the system coming back to the default setting after reboot, and put “eth4” into “net” zone:



Press “**Modify**” to submit the change, and the setting will take into effect after reboot.



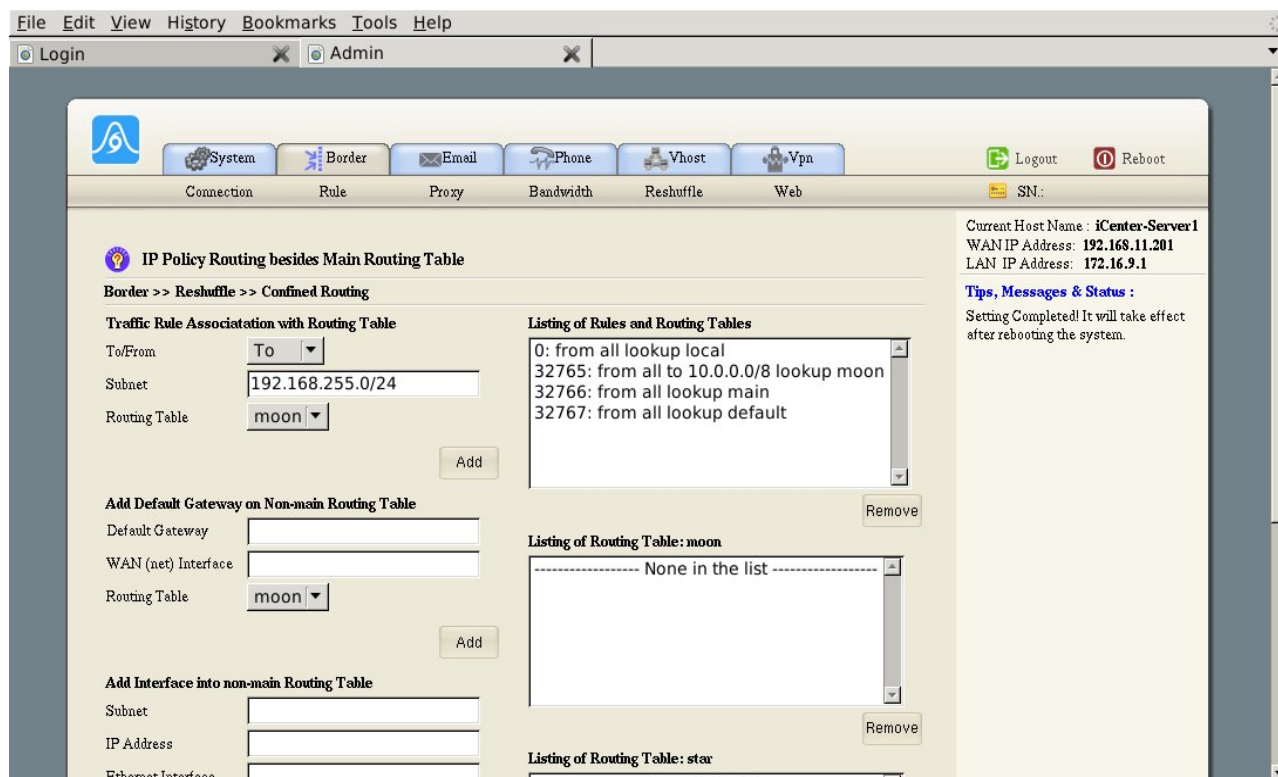
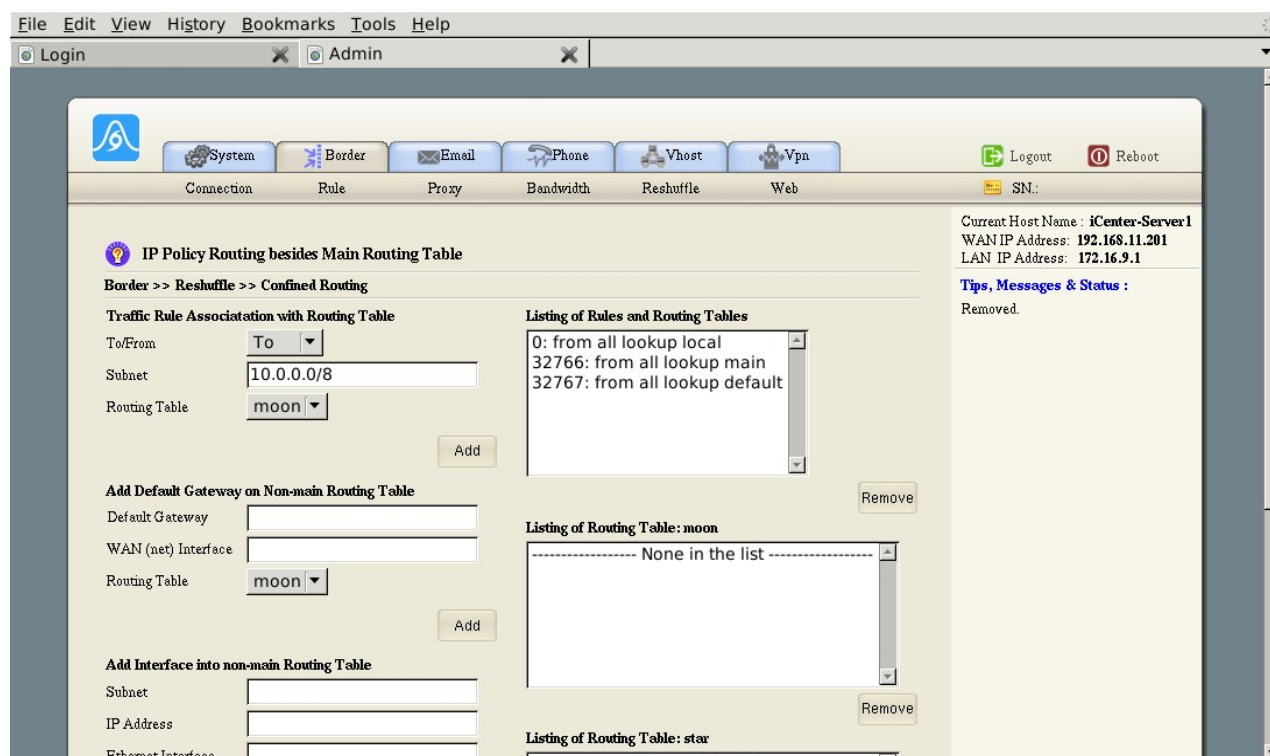
The following steps make “eth4” look into another routing table instead of main routing table. Recall that we have the following for “eth4”

IP address: 10.0.40.132
Netmask: 255.255.248.0
Gateway: 10.0.47.254

And if the proxy IP address to IMS is

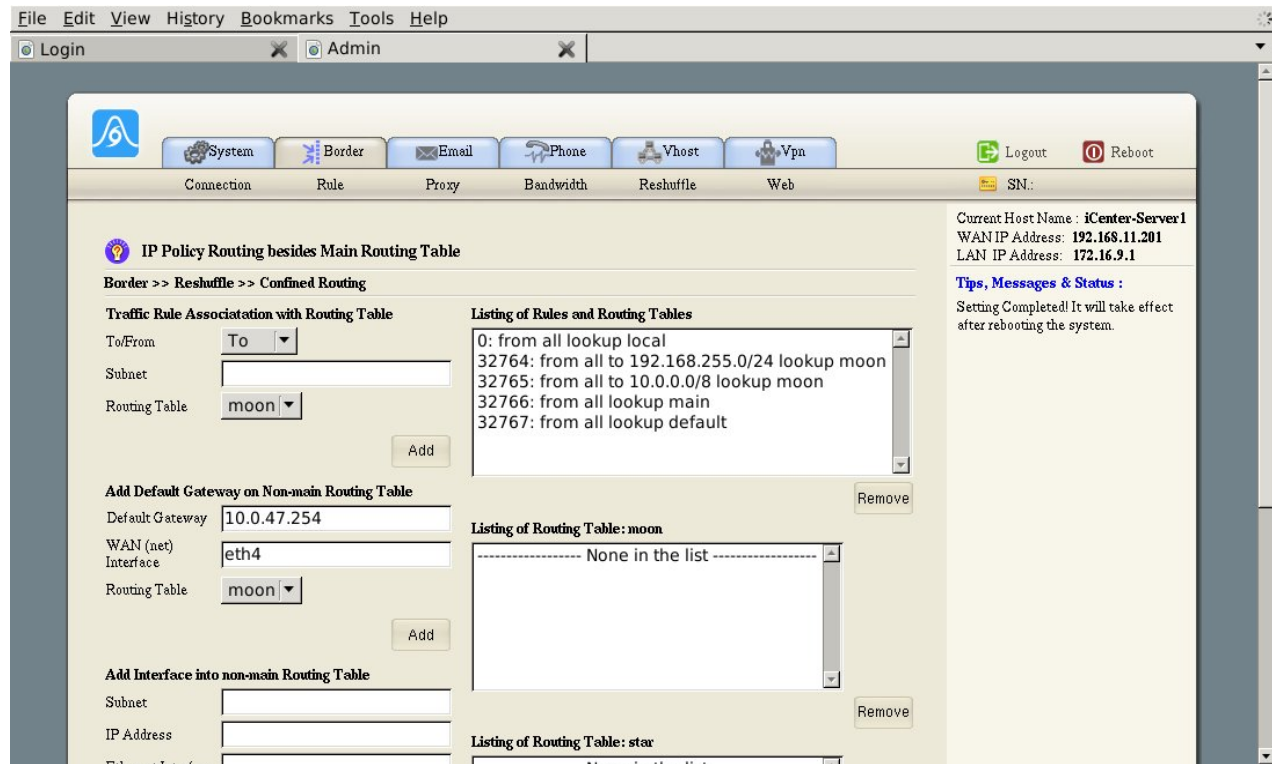
192.168.255.4

It implies the traffic To/From the two subnets 10.0.0.0/8 and 192.168.255.0/24 will look into another routing table (in our system, we name this routing table as “moon”). We start with “**Border >> Reshuffle >> Confined Routing**”:

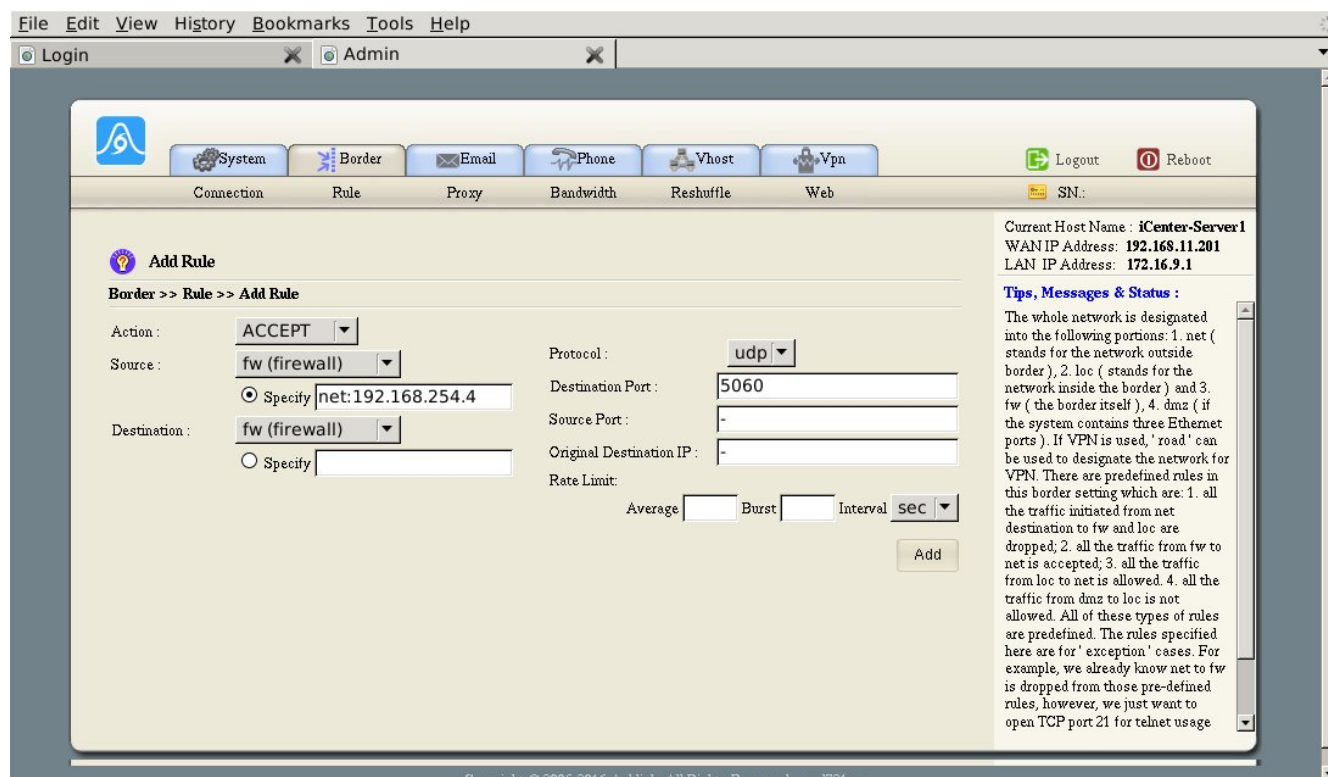
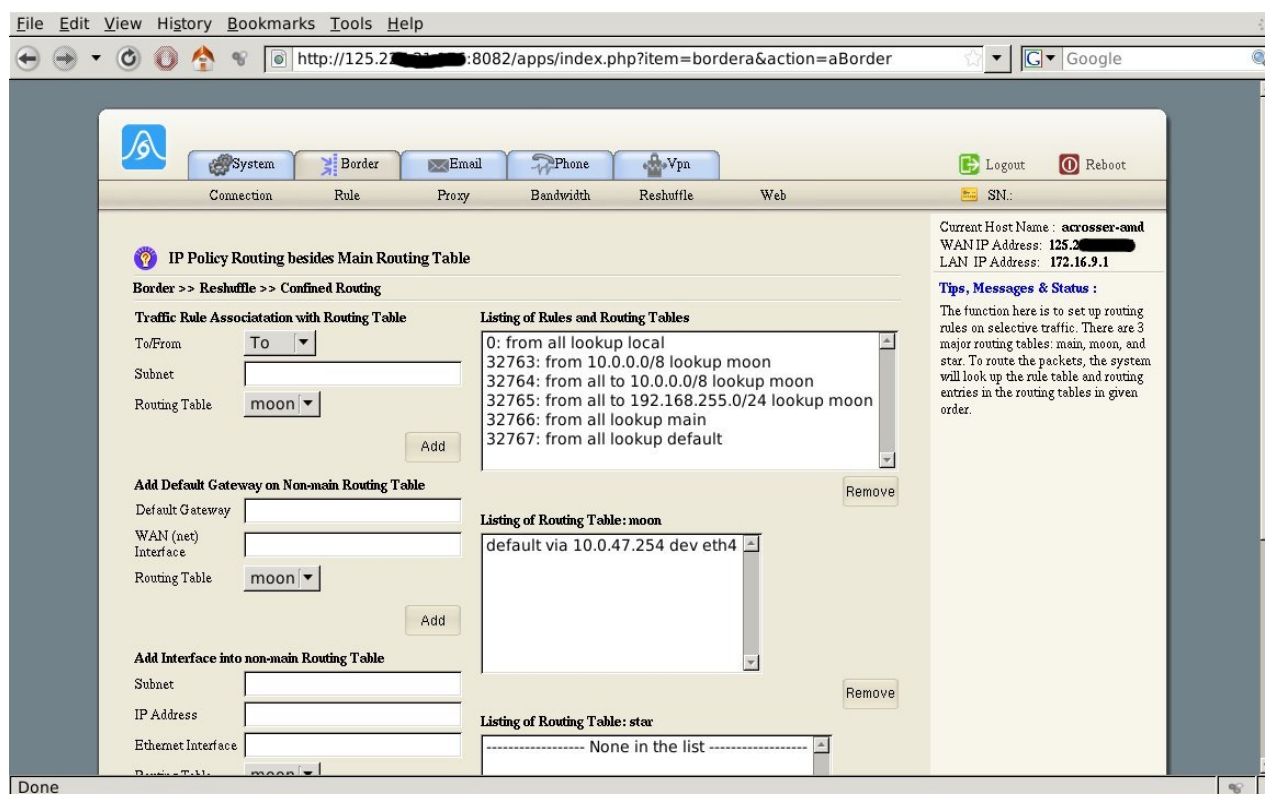


Similarly, you might set “From” 10.0.0.0/8 and “192.168.255.0/24 to look into this “moon” routing table.

And we set default gateway of “eth4” on this “moon” routing table as follow:



Then we will have the configuration shown as the diagram below:



Up to this point, we have "eth4" in the zone "net". Since the default rule for "net to loc" is "REJECT", we need to change the firewall setting to accept the traffic from IMS via "**Border >> Rule >> Add Rule**":

File Edit View History Bookmarks Tools Help

Login Admin

System Border Email Phone Vhost Vpn

Connection Rule Proxy Bandwidth Reshuffle Web

Logout Reboot

SN:

Add Rule

Border >> Rule >> Add Rule

Action: **ACCEPT**

Source: **fw (firewall)**

☒ Specify **net:192.168.254.0/24**

Destination: **fw (firewall)**

☐ Specify

Protocol: **udp**

Destination Port: -

Source Port: -

Original Destination IP: -

Rate Limit: Average Burst Interval **sec**

Add

Current Host Name : **iCenter-Server1**
WAN IP Address: **192.168.11.201**
LAN IP Address: **172.16.9.1**

Tips, Messages & Status :

The whole network is designated into the following portions: 1. net (stands for the network outside border), 2. loc (stands for the network inside the border) and 3. fw (the border itself), 4. dmz (if the system contains three Ethernet ports). If VPN is used, ' road ' can be used to designate the network for VPN. There are predefined rules in this border setting which are: 1. all the traffic initiated from net destination to fw and loc are dropped; 2. all the traffic from fw to net is accepted; 3. all the traffic from loc to net is allowed. 4. all the traffic from dmz to loc is not allowed. All of these types of rules are predefined. The rules specified here are for ' exception ' cases. For example, we already know net to fw is dropped from those pre-defined rules, however, we just want to open TCP port 21 for telnet usage

Copyright © 2005-2016 Azblink. All Rights Reserved. ved721xy

File Edit View History Bookmarks Tools Help

http://125.2[REDACTED]:8082/apps/index.php?item=bordera&action=aBorder Google

System Border Email Phone Vpn

Connection Rule Proxy Bandwidth Reshuffle Web

Logout Reboot

SN:

Add Rule

Border >> Rule >> Add Rule

Action: **ACCEPT**

Source: **fw (firewall)**

☐ Specify

Destination: **fw (firewall)**

☐ Specify

Protocol: **tcp**

Destination Port: -

Source Port: -

Original Destination IP: -

Rate Limit: Average Burst Interval **sec**

Add

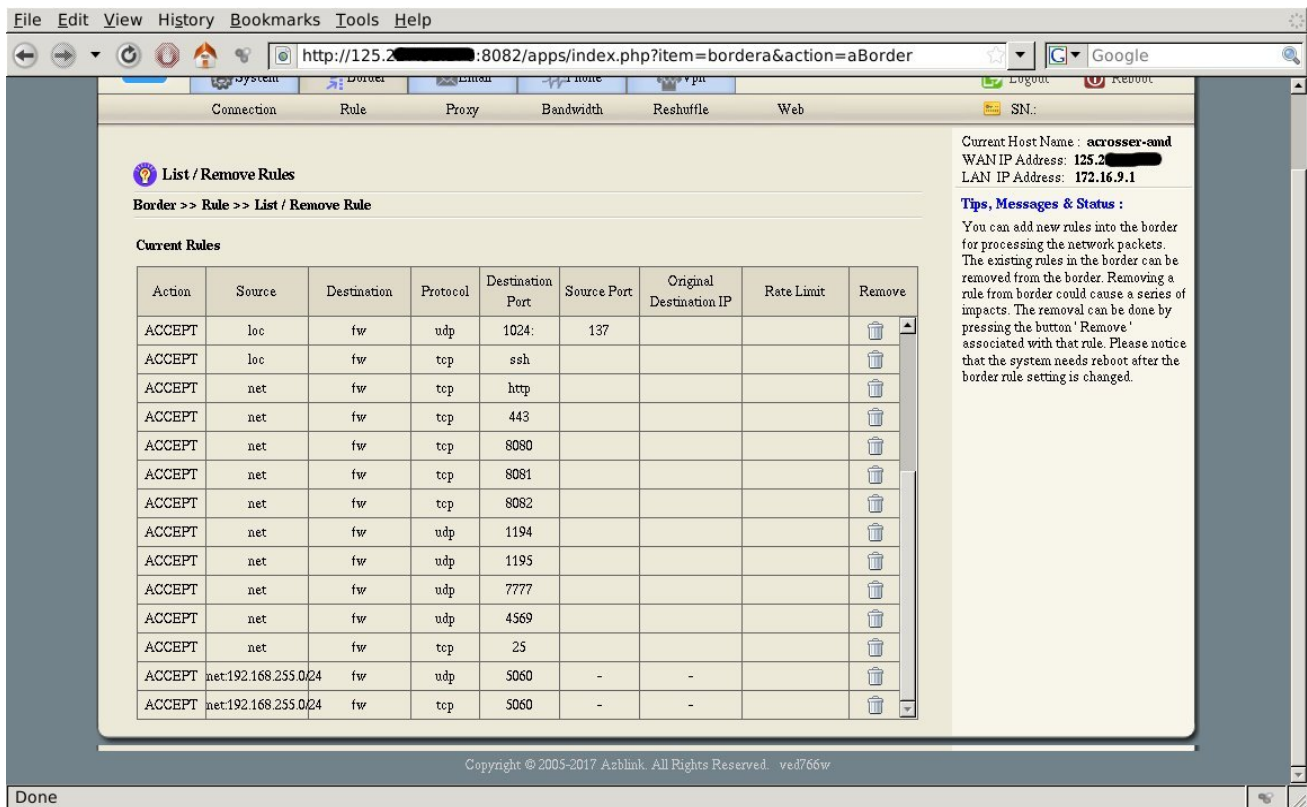
Current Host Name : **acrosser-and**
WAN IP Address: **125.2[REDACTED]**
LAN IP Address: **172.16.9.1**

Tips, Messages & Status :

The whole network is designated into the following portions: 1. net (stands for the network outside border), 2. loc (stands for the network inside the border) and 3. fw (the border itself), 4. dmz (if the system contains three Ethernet ports). If VPN is used, ' road ' can be used to designate the network for VPN. There are predefined rules in this border setting which are: 1. all the traffic initiated from net destination to fw and loc are dropped; 2. all the traffic from fw to net is accepted; 3. all the traffic from loc to net is allowed. 4. all the traffic from dmz to loc is not allowed. All of these types of rules are predefined. The rules specified here are for ' exception ' cases. For example, we already know net to fw is dropped from those pre-defined rules, however, we just want to open TCP port 21 for telnet usage

Copyright © 2005-2017 Azblink. All Rights Reserved. ved766w

Done



In the following section, we introduce how to set up SIP trunk to Chunghwa IMS.

Setting Up SIP Trunk

The connection parameters for the connection to IMS will be given as follows:

Proxy IP: 192.168.255.4
Domain: ims1.cht.com.tw
CallerID: +886233153545

Please note that the CallerID is combined as : +(Taiwan National Code)(Area Code)(Local Phone Number). And the domain name can not be resolved from Internet DNS; it is only known to the proxy. However, in our recent build the domain name has to resolved locally. Otherwise, the system will refuse to connect to the remote IMS network. But the service provide will not release the true IP address of the server. The simple work-around is that we create a local host map by pointing the name "ims1.cht.com.tw" to the proxy IP. It can be done

via **"System >> Setup >> Control Panel"** :

The screenshot shows a web browser window with the Azbink Control Panel. The browser tabs are "Horde :: Log in" and "Admin". The page has a navigation bar with icons for System, Border, Email, Phone, Vhost, and Vpn, and a sub-bar with links for Setup, Network, User, DNS, Management, and Storage. The main content area is titled "Control Panel" and "System >> Setup >> Control Panel".

On the left, under "Hide Application", there are checkboxes for Border, Email, Phone, Vhost, Vpn, and Azbox. A "Save" button is located below these checkboxes.

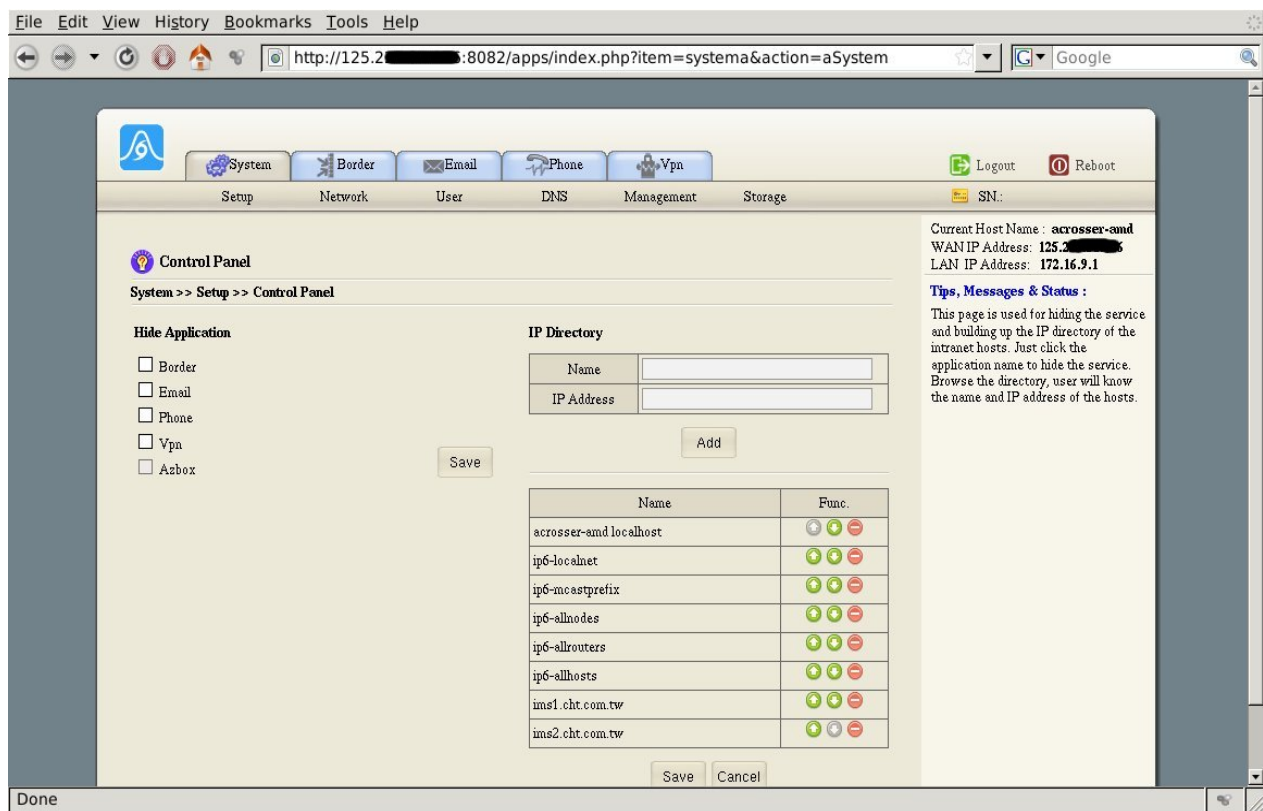
On the right, under "IP Directory", there is a form with two input fields: "Name" (containing "ims1.cht.com.tw") and "IP Address" (containing "192.168.254.4"). Below these fields is an "Add" button.

Below the "Add" button is a table with the following data:

| Name | Func. |
|---------------------------|-------|
| iCenter-Server1 localhost | |
| ip6-localnet | |
| ip6-mcastprefix | |
| ip6-allnodes | |
| ip6-allrouters | |
| ip6-allhosts | |

At the bottom of the table area are "Save" and "Cancel" buttons.

The footer of the page contains the text: "Copyright © 2005-2016 Azbink. All Rights Reserved. ved721wx".



After this, we can start to set up SIP trunk. Navigate via **“Phone >> Cascade >> SIP Trunk”**:

File Edit View History Bookmarks Tools Help

Horde :: Log in Admin

System Border Email Phone Vpn

Basic Cascade Queue Audit

Connect to other hosts via SIP

Phone >> Cascade >> SIP Trunk

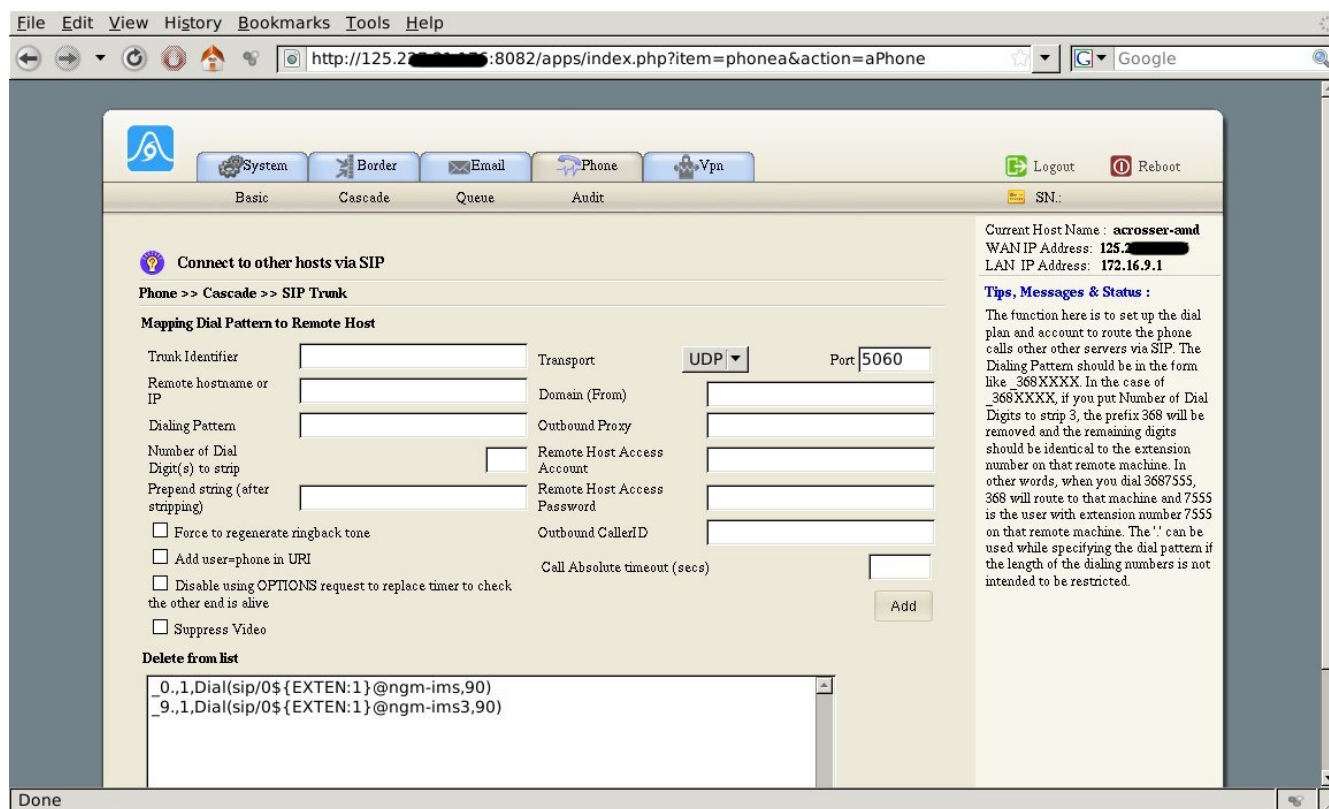
Mapping Dial Pattern to Remote Host

| | | | | | |
|---|--|------------------------------|---|------|-----------------------------------|
| Trunk Identifier | <input type="text" value="ngm-ims"/> | Transport | UDP | Port | <input type="text" value="5060"/> |
| Remote hostname or IP | <input type="text" value="ims1.cht.com.tw"/> | Domain (From) | <input type="text" value="ims.cht.com.tw"/> | | |
| Dialing Pattern | <input type="text" value="_0."/> | Outbound Proxy | <input type="text" value="192.168.255.4"/> | | |
| Number of Dial Digit(s) to strip | <input type="text" value="1"/> | Remote Host Access Account | <input type="text"/> | | |
| Prepend string (after stripping) | <input type="text" value="0"/> | Remote Host Access Password | <input type="text"/> | | |
| <input type="checkbox"/> Force to regenerate ringback tone | | Outbound CallerID | <input type="text" value="+886233153545"/> | | |
| <input type="checkbox"/> Add user=phone in URI | | Call Absolute timeout (secs) | <input type="text"/> | | |
| <input type="checkbox"/> Disable using OPTIONS request to replace timer to check the other end is alive | | | | | |
| <input checked="" type="checkbox"/> Suppress Video | | | | | |

Delete from list

Copyright © 2005-2017 Azblink. All Rights Reserved. ved766c


Please note: the IMS need "0" to prepend – compared to the normal dialing habit we have on PSTN; and "Video" has to be suppress. Furthermore, the inbound calls might be also from the other proxy (for example, "192.168.255.248"). Thus, we need to set up another dummy trunk to allow the inbound calls from that IP address.



The setting of the Inbound calls is via **“Phone >> Cascade >> DID Number Mapping”**. Usually, we just map that number to auto attendant:

File Edit View History Bookmarks Tools Help

Horde :: Log in Admin

 System Border Email Phone Vpn

Basic Cascade Queue Audit

Map DID Number to Extension

Phone >> Cascade >> DID Number Mapping

☒ Activate DID Number Mapping

Mapping Incoming Number to Extension

Incoming Number

☐ Extension to send

☒ To automatic attendant

☐ Extract from TO field of SIP Header

☐ Strip the incoming digits

Delete from list

-----none-----

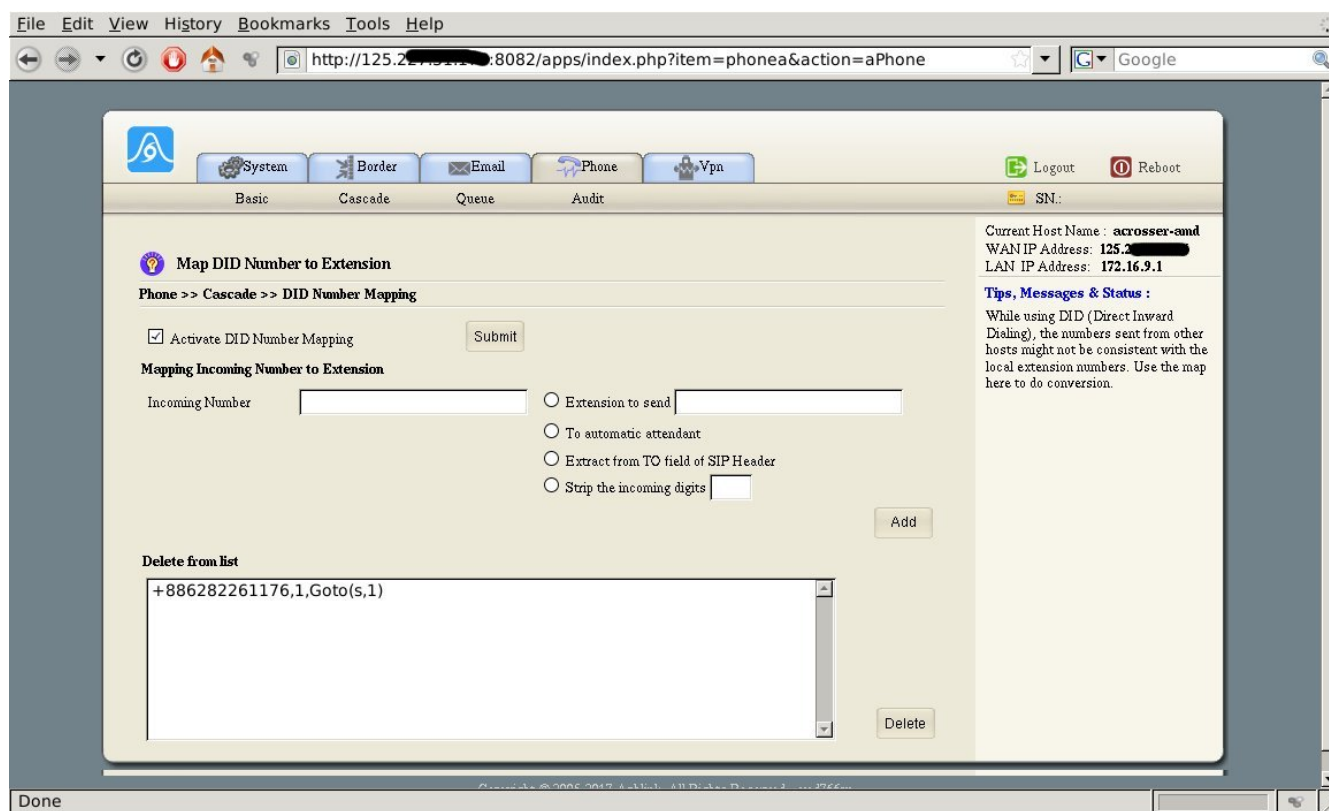
Current Host IP

Tips, M

While us
Dialing)
hosts mi
local ext
here to c

Copyright © 2005-2017 Azblink. All Rights Reserved. ved766c

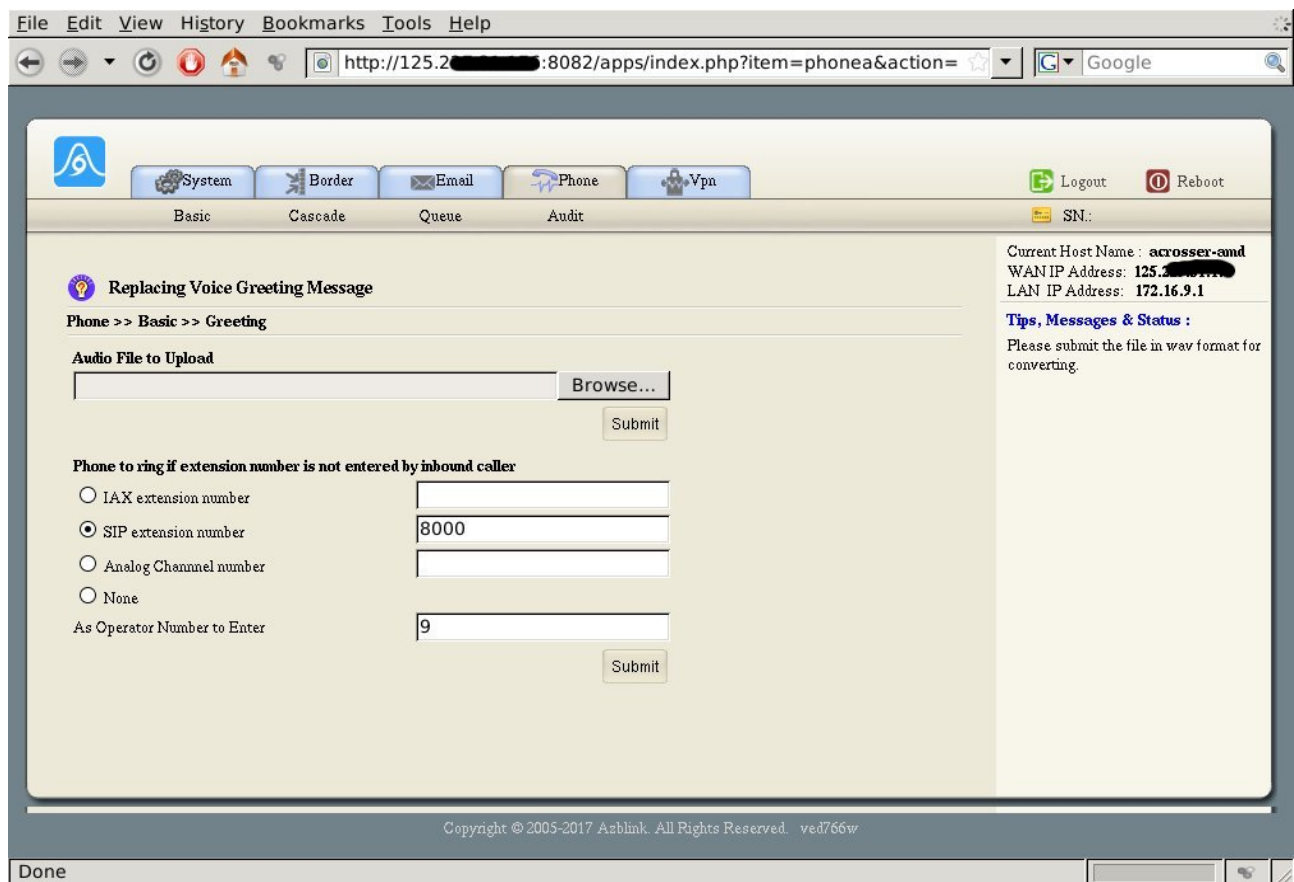
If we want to do DID to sending the coming calls directly to an extension for a specific incoming number, please remember that that extension has to disable "video". Otherwise, Chunghwa's IMS will interrupt the call once the call is picked up.



Before you settle with the inbound calls here, please make sure the auto attendant greeting message and operator number are uploaded and set via **“Phone >> Basic >> Greeting”** (shown in the following diagram). In the auto attendant greeting message, you can prepare a voice file in WAV format by indicating how to reach the operator. For example, the message might go like “This is XXXX. Please dial your party extension or 9 for the operator. “

The following example shows the SIP extension number “8000” is chosen to be operator, and it allows pressing “9” to reach the operator.

Please note that any changes made here will reset the dial rules in “default” context (SIP trunk rules might disappear if they are in the context “default” or DID activation box will be unchecked). SIP trunk rules usually are placed in the context “all” so that they should not be affected unless you move them into the context “default”. Thus, it suffices to go to **“Phone >> Cascade >> DID Number Mapping”** to check if any change is made at **“Phone >> Basic >> Greeting”**.



Create User Accounts for Mobile Devices

The rest of the work is to create user accounts for mobile device. We have APP (known as Azfone) on mobile devices (Android and iOS) to place voice/video calls. And the APP AzFone has to bind with VPN client (OpenVPN) to use. Once an account is created, the user can just the AzFone program to scan the QR code for that user to read configuration file and start to use.

To reach to that goal, it is necessary to check the following items. At first, we need to check if CA (certificate authority) and server key/certificate for VPN are generated successfully (**Vpn >> Connection >> Key Generation**):

File Edit View History Bookmarks Tools Help

http://125.2[REDACTED]:8082/apps/index.php?item=vpn&action=aVpn

System Border Email Phone Vpn Logout Reboot

Connection Site-to-Site Bridge PPTP SN:

Certificate and Key Generation

Setup Wizard: Previous - Steps 3/4 - Next

Vpn >> Connection >> Key Generation

Country Code: NB State Code: NA
 Locality: here3 Org. Name: thisPlace
 Org. Unit: IT Email: me@myhost.mydomi

Submit

CA Generation:
 Common Name: thunder
 CA Certificate Expiration: Jan 18 05:16:30 2027 GMT

Cert. & Key for Server:
 Common Name: arrow
 Generate

Cert. & Key for Client(s):
 Common Name:
 Valid days:
 Generate

Client Configuration Set List

| | |
|-----------------------|--------------------------|
| client1:azblinktest | Jan 18 05:18:10 2027 GMT |
| client2:khc | Jan 23 00:39:17 2027 GMT |
| client3:aztest-mobile | Jan 23 04:41:19 2027 GMT |
| client4:test08-mobile | Feb 1 04:24:20 2027 GMT |

Remove Purge

Tips, Messages & Status:
 CA and Server certificate should be generated at the very first beginning. All the Common Names for CA, Server, and Client(s) shall be unique. Each of them can not be the same as other Common Names. Pressing Remove button to remove a client can revoke that client. If Common Names was not shown in Client Configuration Set List box, it means it was not generated successfully; it could be using the same Common Name as others. Purge button will remove everything so that you need to regenerate keys and certificates for CA, Server, and client(s) all over again. Please note that you need to fill in data in sequence order from top to bottom and left to right.

Copyright © 2005-2017 Azblink. All Rights Reserved. ved766w

Done

And check if VPN server is started (**Vpn >> Connection >> Address Pool**):

File Edit View History Bookmarks Tools Help

http://125.2[REDACTED]:8082/apps/index.php?item=vpn&action=aVpn

System Border Email Phone Vpn Logout Reboot

Connection Site-to-Site Bridge PPTP SN:

Subnet Allocated for VPN

Setup Wizard: Steps 1/4 - Next

Vpn >> Connection >> Address Pool

Network Address: 172.16.38.0
 Netmask: 255.255.255.0
 Maximum Number Of Concurrent Clients: 91

☐ Turn Off VPN Server Process

☐ Allow Client to Client
☐ Force to use TLS1.2
 Data Cipher: AES-128-CBC
 AES-128-CBC

Submit

The IP address of VPN server will be the first one in the range you specify on above. Changing Data Cipher requires all the clients fetching new configuration.

Tips, Messages & Status:
 VPN IP address pool is the space of IP addresses allocated for VPN. It can not use the same IP address space on the network where your VPN server or VPN client resides.

Copyright © 2005-2017 Azblink. All Rights Reserved. ved766w

Done

And create extension numbers (**Phone >> Basic >> Extension Account**):

The screenshot shows the Asterisk Manager GUI. The browser address bar indicates the URL: `http://125.255.8082/apps/index.php?item=phonea&action=aPhone`. The page title is "Extension Account Setting". The breadcrumb trail is "Phone >> Basic >> Extension Account".

On the left, there is a table of existing SIP extensions:

| <input type="checkbox"/> | VoIP | Extension Number | Password | Caller ID | Dial Rule Context |
|--------------------------|------|------------------|----------|------------------|-------------------|
| <input type="checkbox"/> | SIP | 8001 | | "Frank"<8001> | All |
| <input type="checkbox"/> | SIP | 8002 | | "Barbet"<8002> | All |
| <input type="checkbox"/> | SIP | 8101 | | "Kenchen"<8101> | All |
| <input type="checkbox"/> | SIP | 8102 | | "Henry"<8102> | All |
| <input type="checkbox"/> | SIP | 8201 | | "Ray"<8201> | All |
| <input type="checkbox"/> | SIP | 8202 | | "Well"<8202> | All |
| <input type="checkbox"/> | SIP | 8203 | | "Steven"<8203> | All |
| <input type="checkbox"/> | SIP | 8301 | | "Loren"<8301> | All |
| <input type="checkbox"/> | SIP | 8302 | | "Sarara"<8302> | All |
| <input type="checkbox"/> | SIP | 8303 | | "Cckjhott"<8303> | All |
| <input type="checkbox"/> | SIP | 8800 | | "test00"<8800> | All |
| <input type="checkbox"/> | SIP | 8801 | | "test01"<8801> | All |
| <input type="checkbox"/> | SIP | 8808 | | "test08"<8808> | All |

On the right, there is a form to add a new extension:

VoIP: ☒ IAX ☐ SIP

* Extension Number:

* Password:

Dial Rule Context:

Caller ID:

Name:

Number:

☐ Suppress Video (only for SIP)

Network allowed (e.g. 172.16.9.0/24):

Buttons: Add, Cancel

On the far right, system status information is displayed:

Current Host Name: **acrosser-and**
 WAN IP Address: **125.255.8082**
 LAN IP Address: **172.16.9.1**

Logout, Reboot buttons are also present.

After creating SIP extension number, please navigate via "**System >> Users >> Add User**" to create account for XMPP; and fill that SIP extension number in the field "**VoIP**".

File Edit View History Bookmarks Tools Help

http://125.2.2.8082/apps/index.php?item=systema&action=aSystem

Google

System Border Email Phone Vpn

Setup Network User DNS Management Storage

Logout Reboot

SN:

New user information

System >> Users >> Add User

| | | | |
|--------------|----------|----------------------|----------|
| Account | | Title | |
| Password | rtdty9jn | User Enter or System | Generate |
| First Name | | Last Name | |
| Email | | | |
| Home Address | | | |
| Work Address | | | |
| Home Phone | | Work Phone | |
| Mobile | | VoIP | |
| Free/Busy | | | |

Options

☒ The frequency to update password : 30 days

Save Clear Cancel

Current Host Name : acrosser-and
WAN IP Address: 125.2.2.8082
LAN IP Address: 172.16.9.1

Tips, Messages & Status :

This page is to add a new user to this system. NOTICE: The password is randomly generated; User can choose to change the password by modifying the generated text of the entry directly or from the User Side Interface. On this page, among the data entries, the Account and Password are required. Others are optional.

Copyright © 2005-2017 Azblink. All Rights Reserved. ved766w


Done

If those are set, just navigate via **“System >> User >> User QR”** to scan QR code for that account:

FileEditViewHistoryBookmarksToolsHelp

http://125.227.31.176:8082/apps/index.php?item=systema&action=aSystem

Google




SystemBorderEmailPhoneVpn

SetupNetworkUserDNSManagementStorage

LogoutReboot

SN:


View User Information via QR code

System >> User >> User QR

☒ Hide the accounts used by the system processes

| User Account List |
|-------------------|
| aztest |
| barbet |
| callmgr |
| cockhott |
| dudu |
| frank |
| henry |
| kenchen |
| loren |
| ray |
| sarana |
| steven |
| test08 |
| well |

User Information in QR Code: test08



Download

☐ Hide XMPP GPS button☐ Hide XMPP File Upload button

Regenerate

Current Host Name : **acrosser-and**

WAN IP Address: **125.227.31.176**

LAN IP Address: **172.16.9.1**

Tips, Messages & Status :

Done