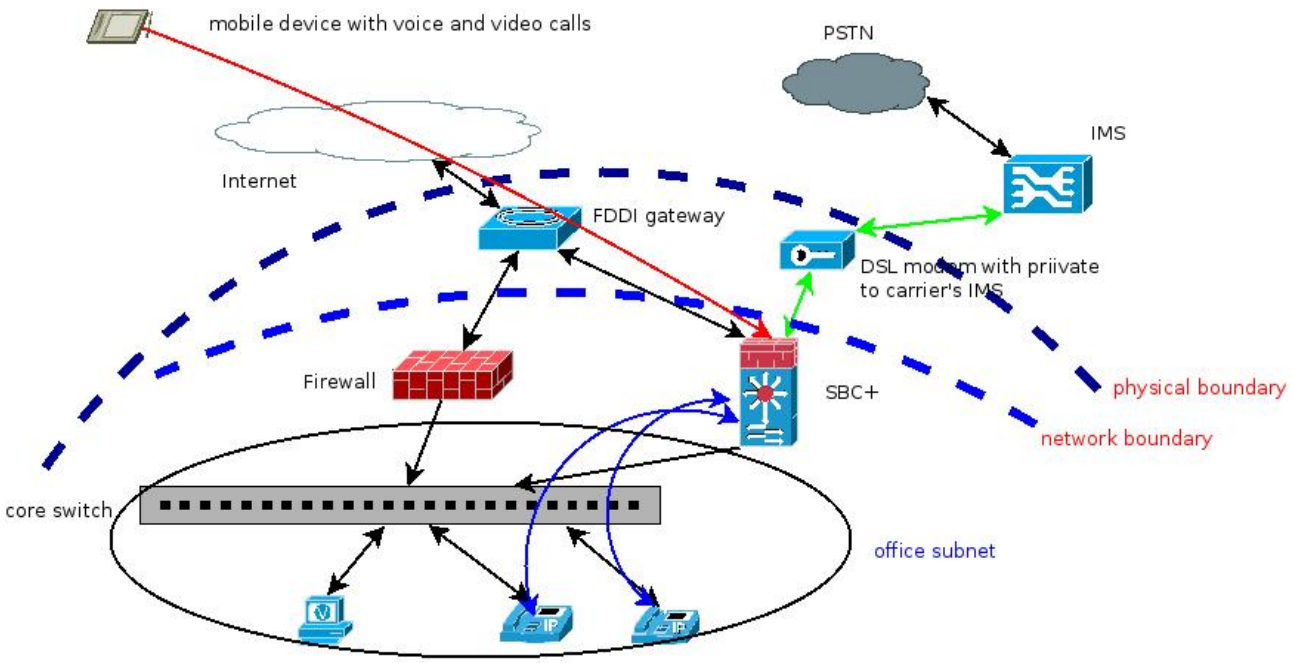
Deployment Guide with Chunghwa IMS

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.

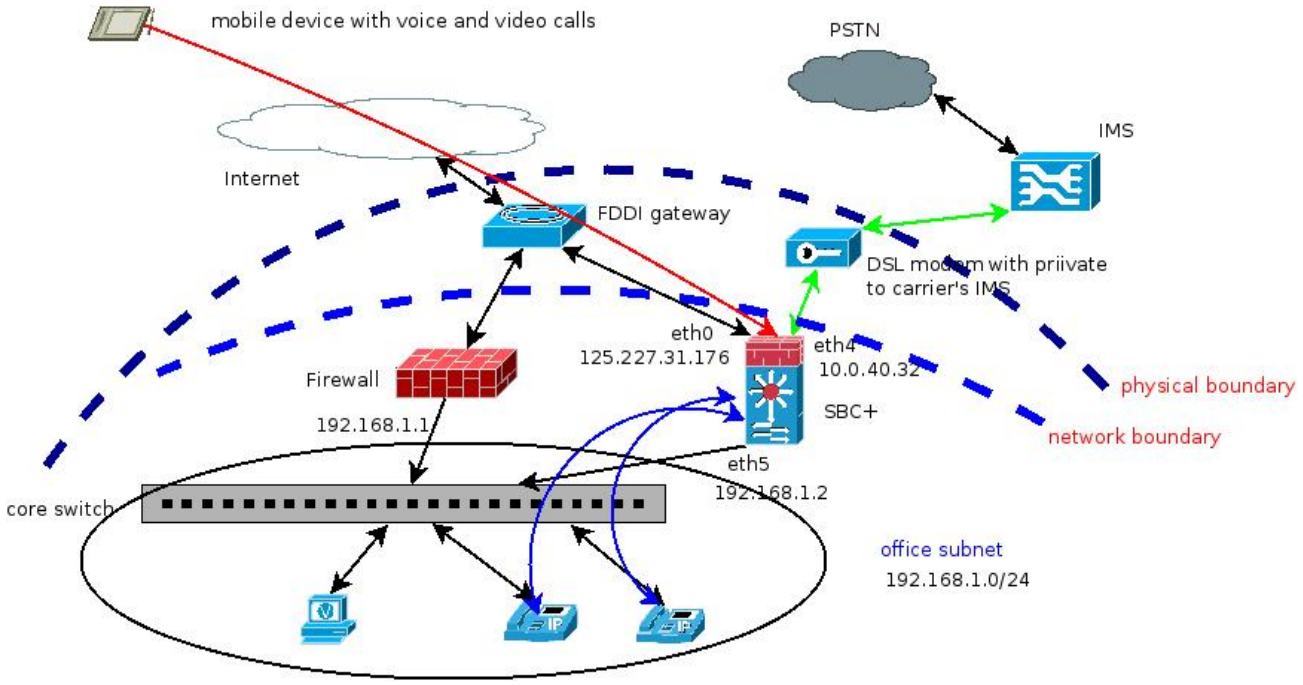


However, that link should still be considered as “insecure” due to the fact that there are other Chunghwa's customers on that network. In our system's factory setup, only “eth0” is used as “WAN” port to connect to the Internet. In this case, another Ethernet port will be used as another WAN port to connect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

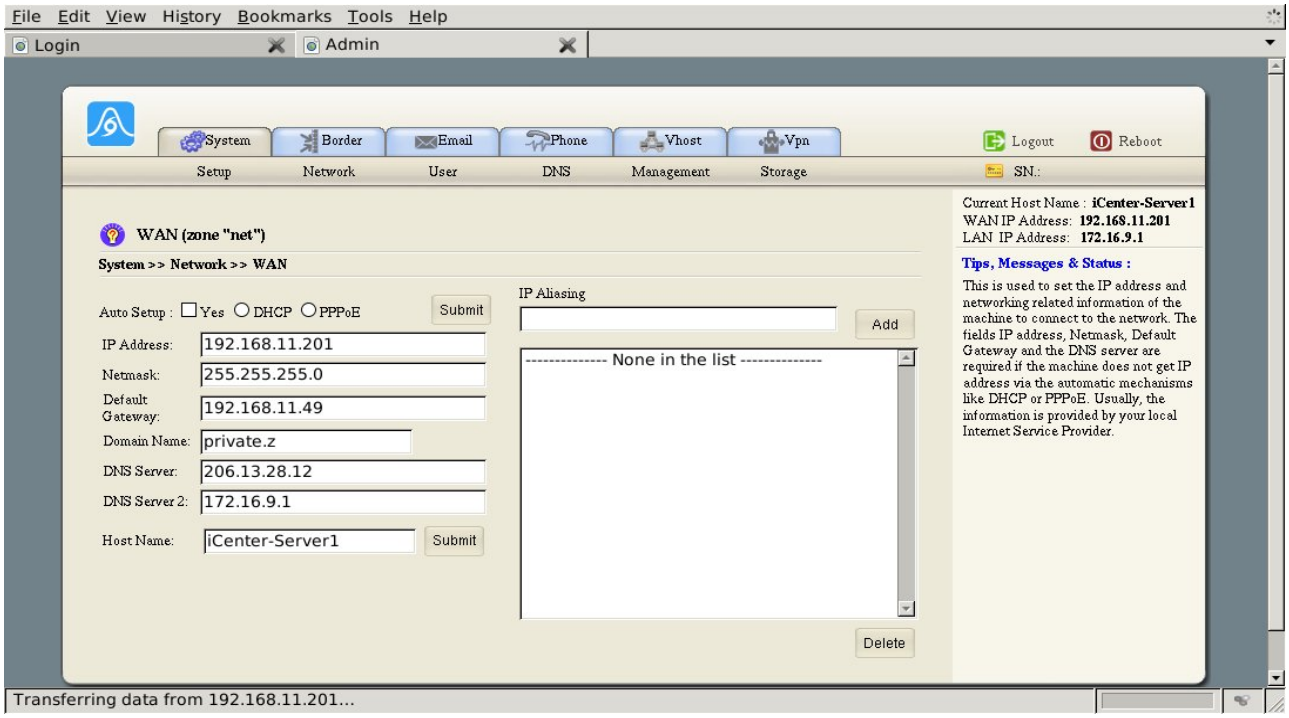
The following is an example with IP addresses specified: the port “eth0” is connected to the Internet, “eth4” is connected to the network with IMS, and “eth5” is connected to the office local network:



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

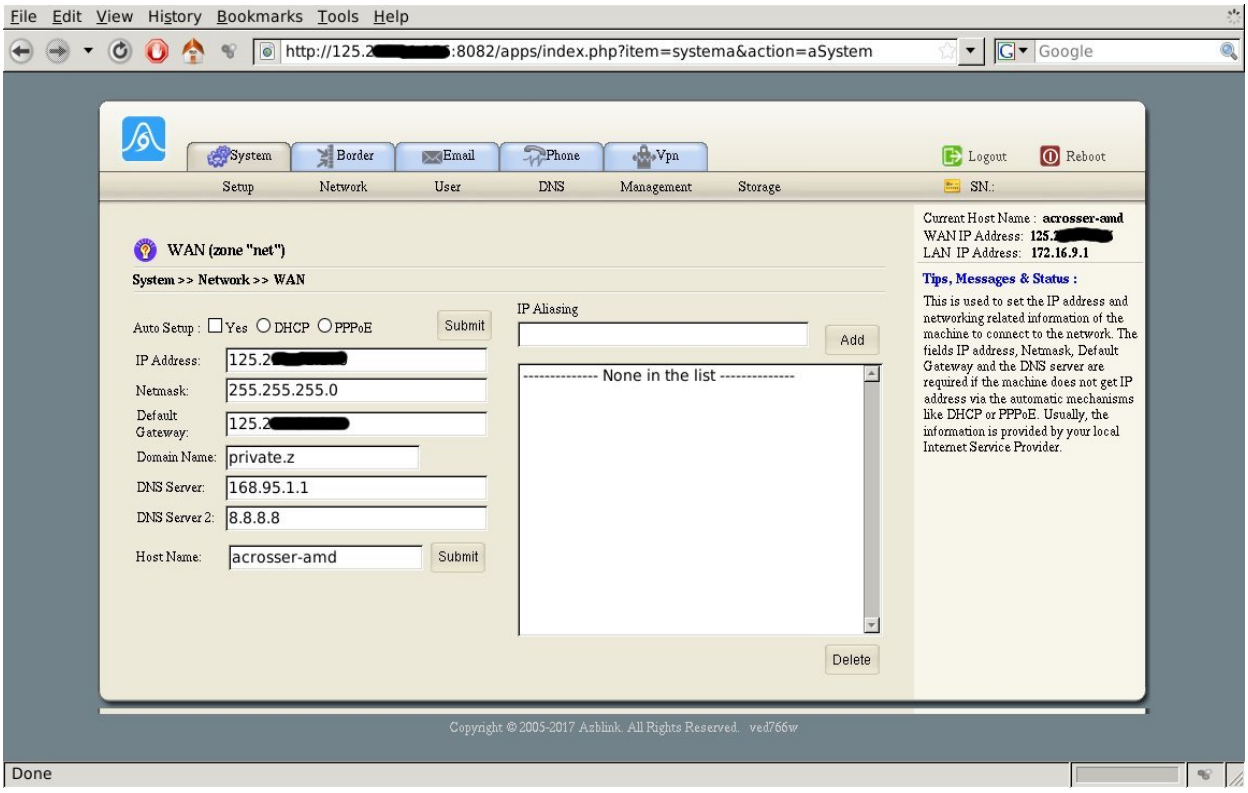
The WAN IP address can be changed at "**System >> Network >> WAN**":



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.

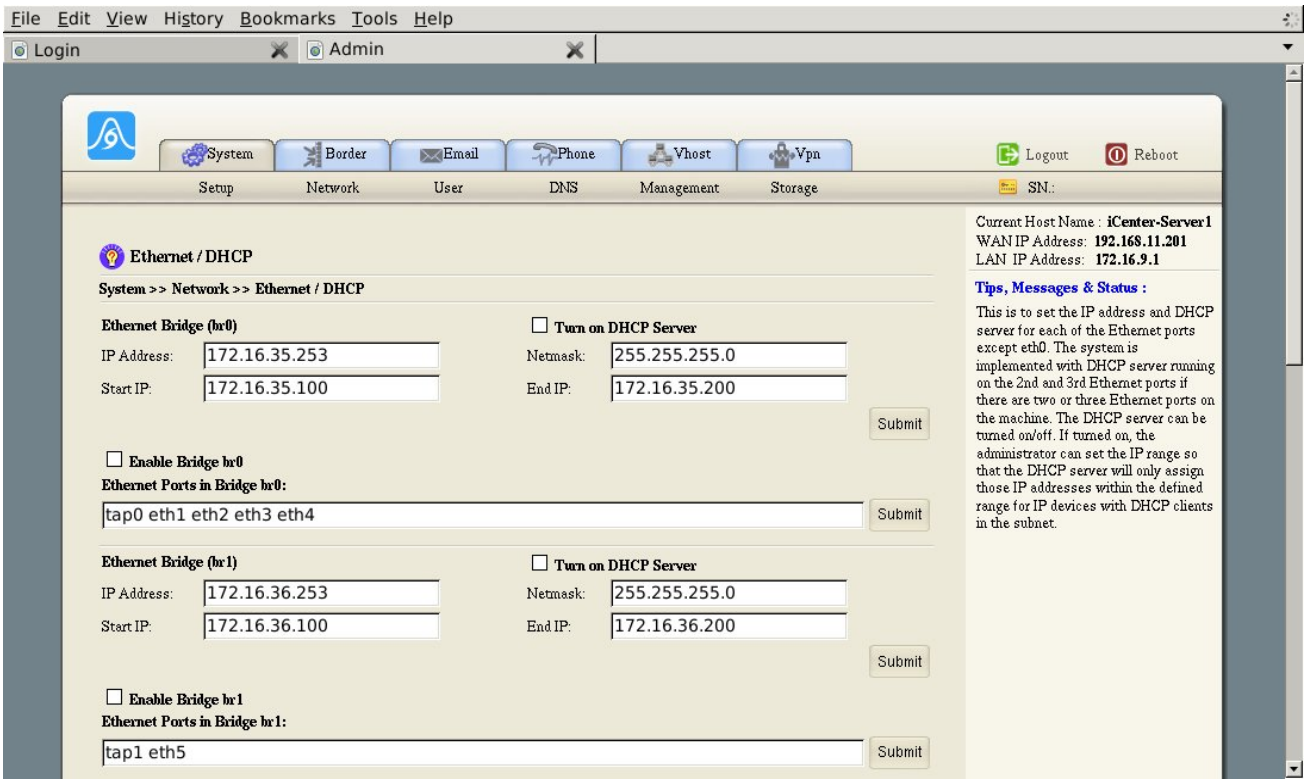
The next step is: we want to use “eth4” to connect to IMS network and “eth5” for the office local network. The Ethernet ports “eth4” and “eth5” belong to the region “loc” (Local network) and we would like to change “eth4” from “loc” (Local Network) to “net” (Internet/WAN). On “eth4” (to IMS network),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

IP address: 10.0.40.132
Netmask: 255.255.248.0
Gateway: 10.0.47.254

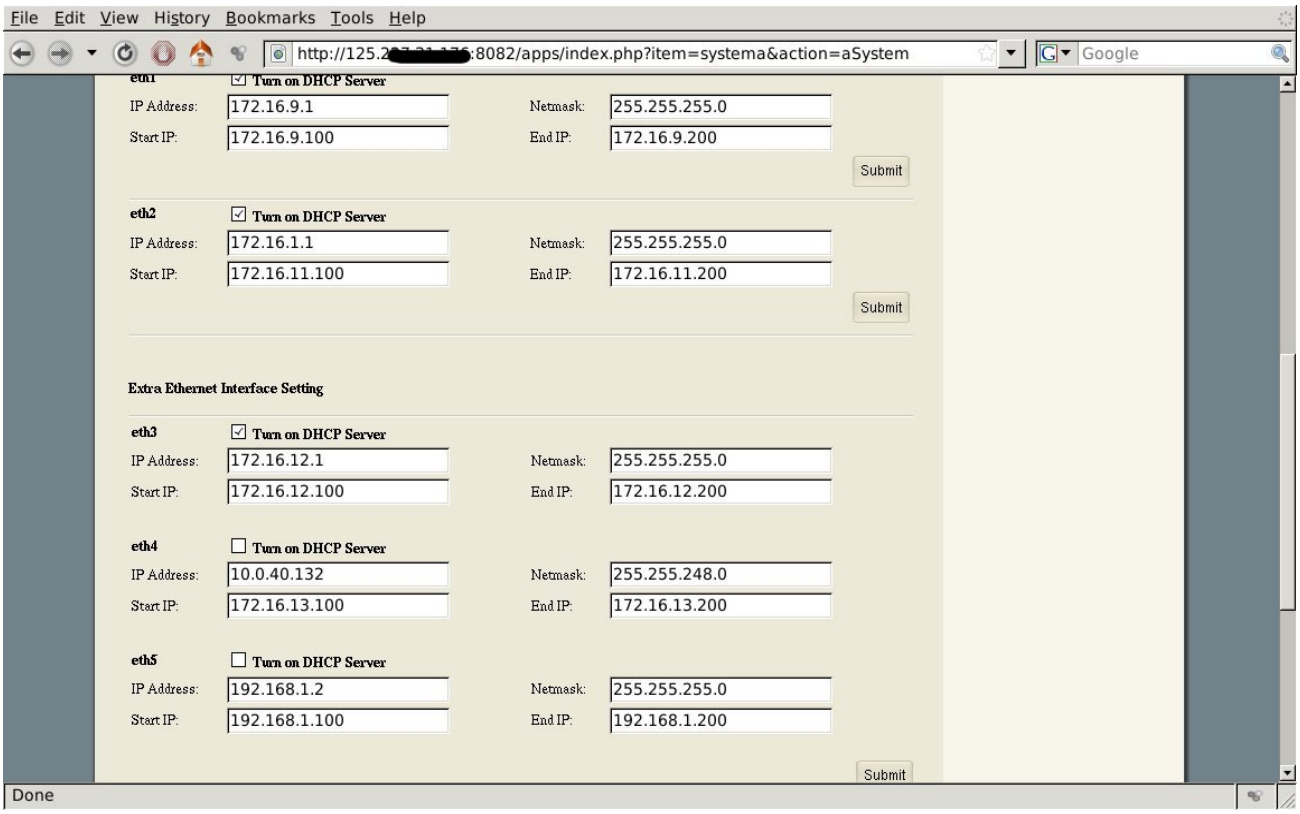
And the IP address of “eth5” is given as

IP address: 192.168.1.2
Netmask: 255.255.255.0

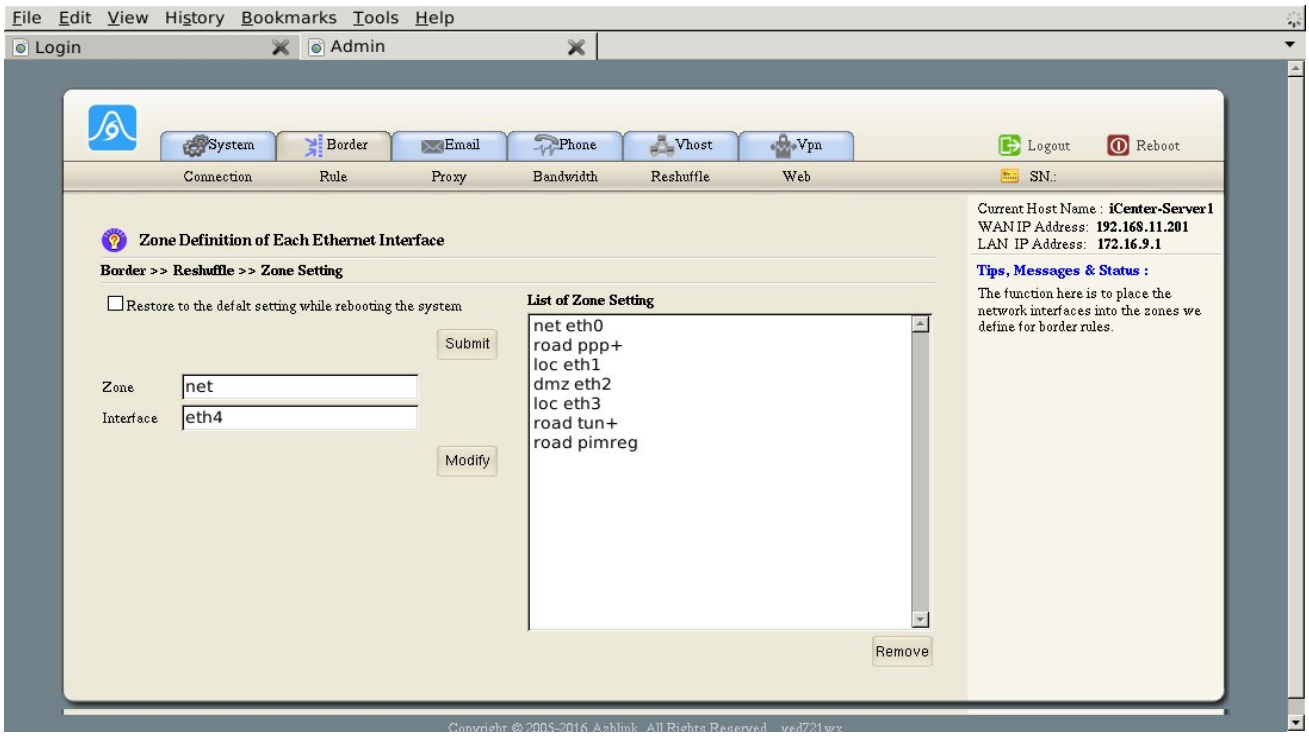
The setting of IP address and Netmask for each port can be done via “**System >> Network >> Ethernet / DHCP**”:



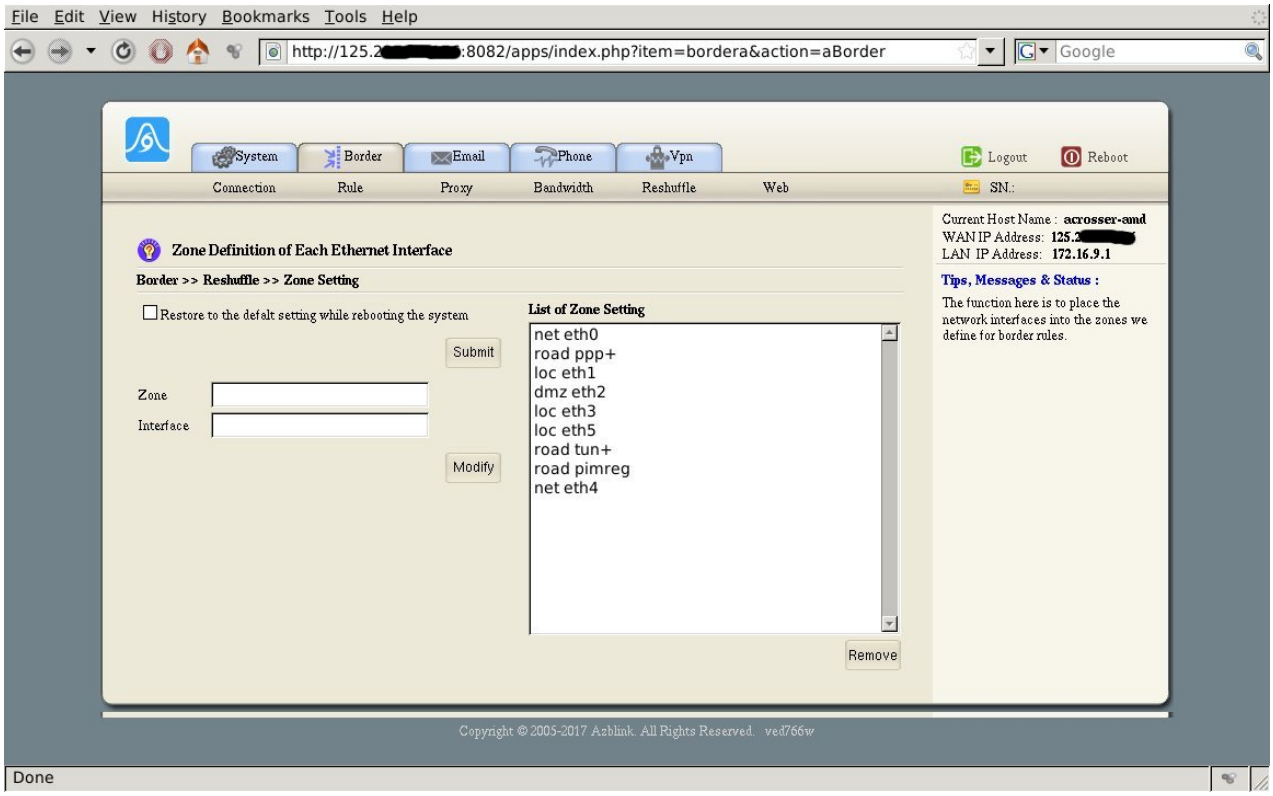
They are changed as follows by turning off DHCP server on each port:



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.



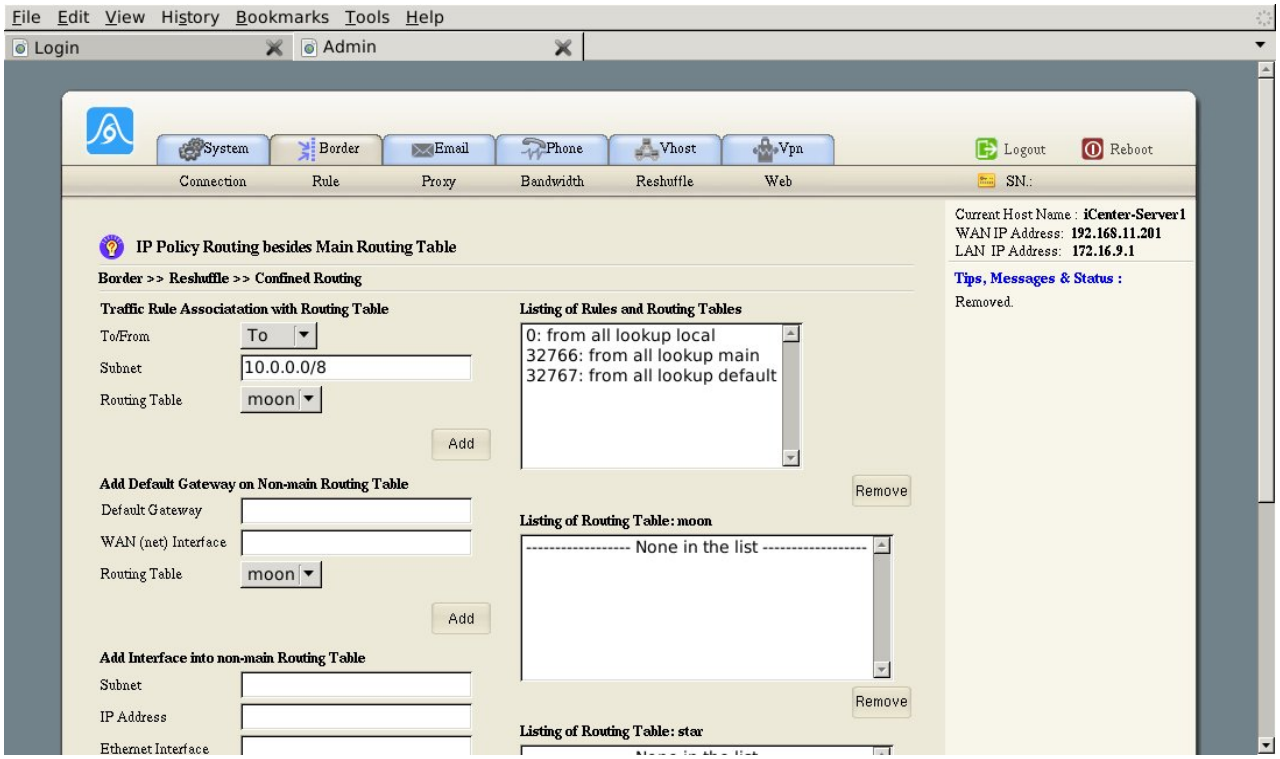
The following steps make “eth4” look into another routing table instead of main routing table. Recall that we have the following for “eth4”

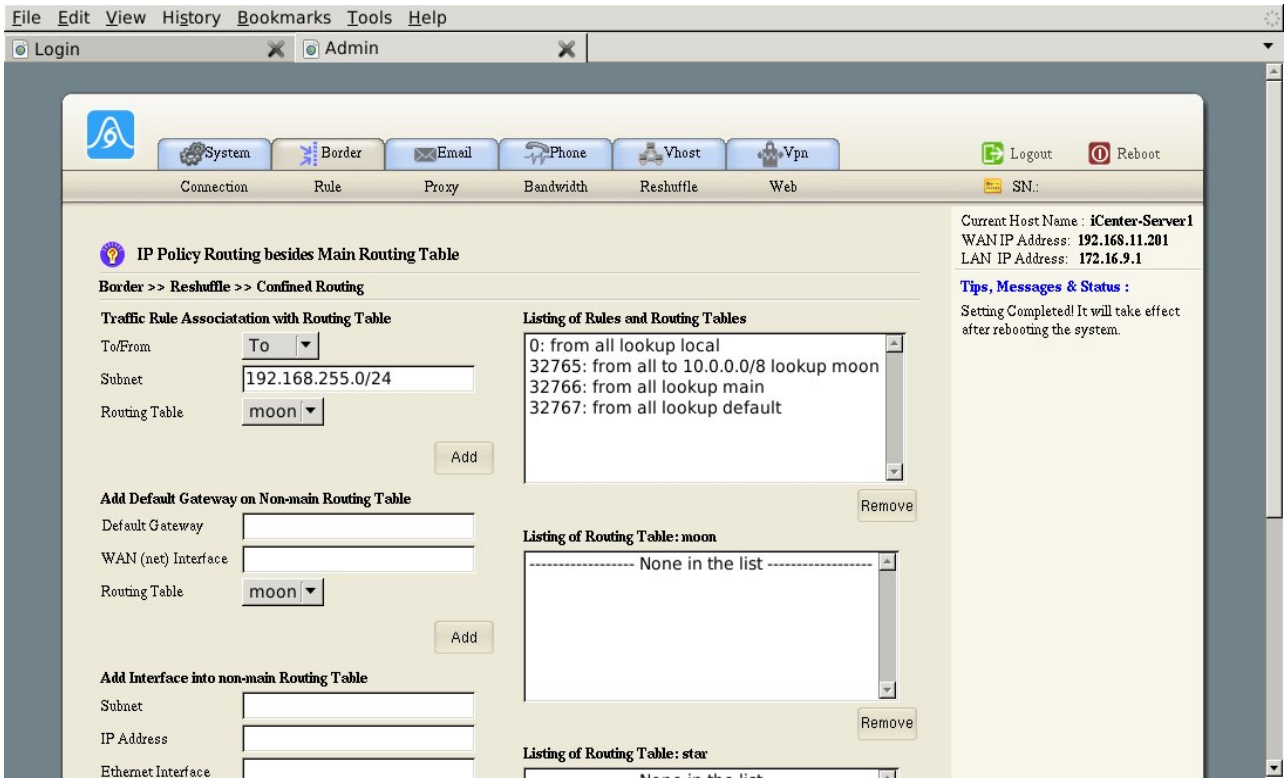
IP address: 10.0.40.132
Netmask: 255.255.248.0
Gateway: 10.0.47.254

And if the proxy IP address to IMS is

192.168.255.4

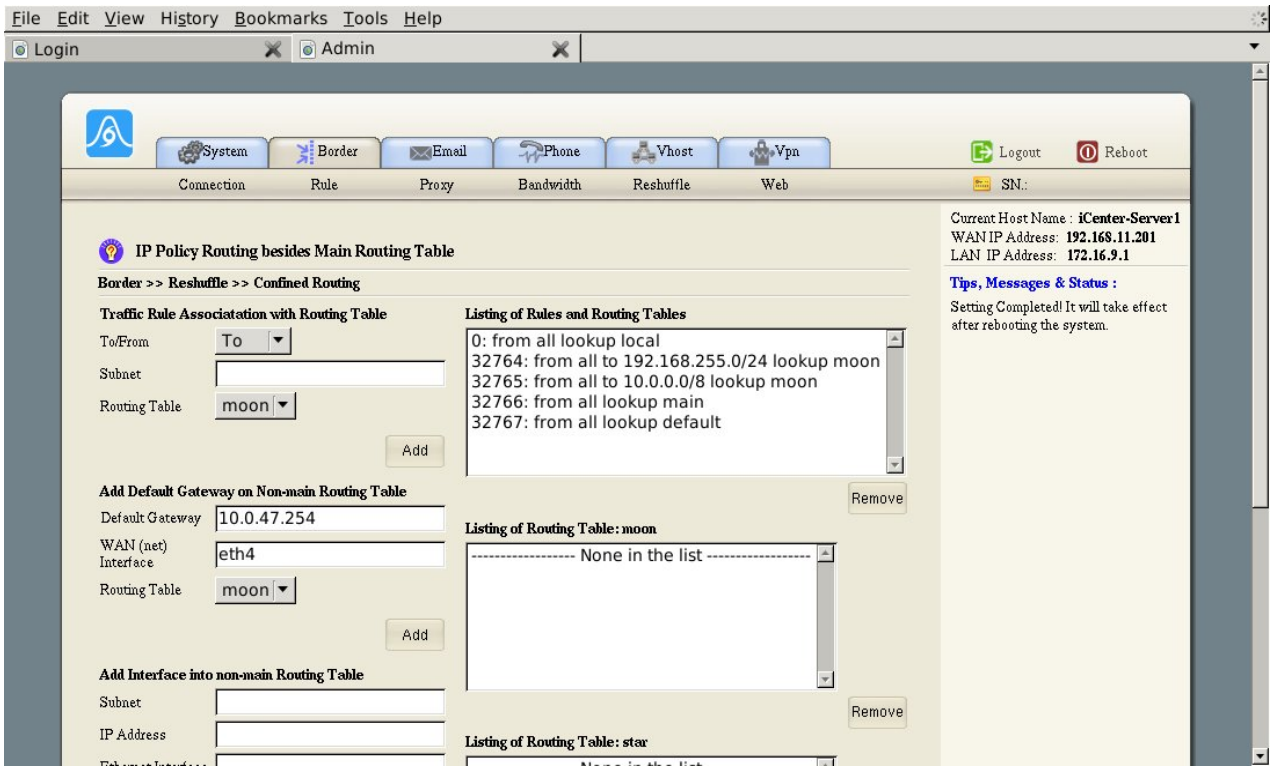
It implies the traffic To/From the two subnets 10.0.0.0/8 and 192.168.255.0/24 will look into another routing table (in our system, we name this routing table as “moon”). We start with “**Border >> Reshuffle >> Confined Routing**”:



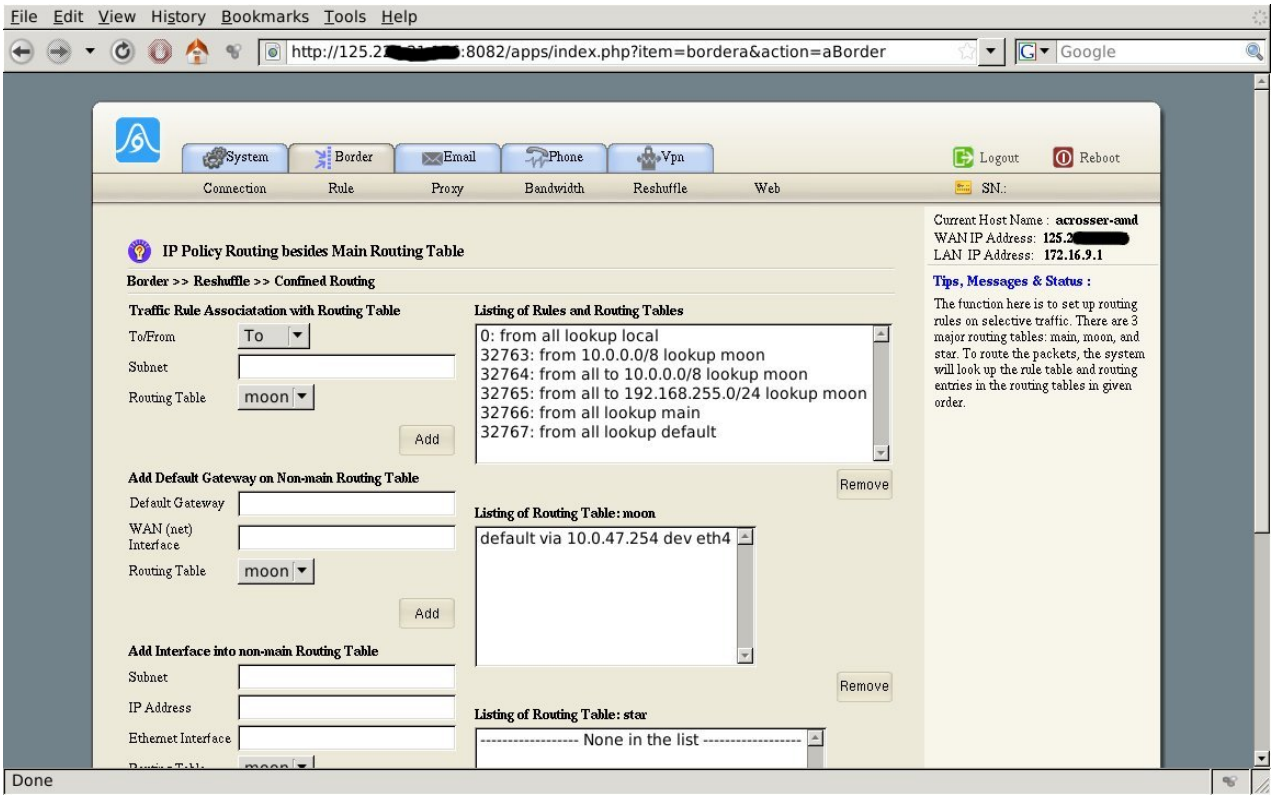


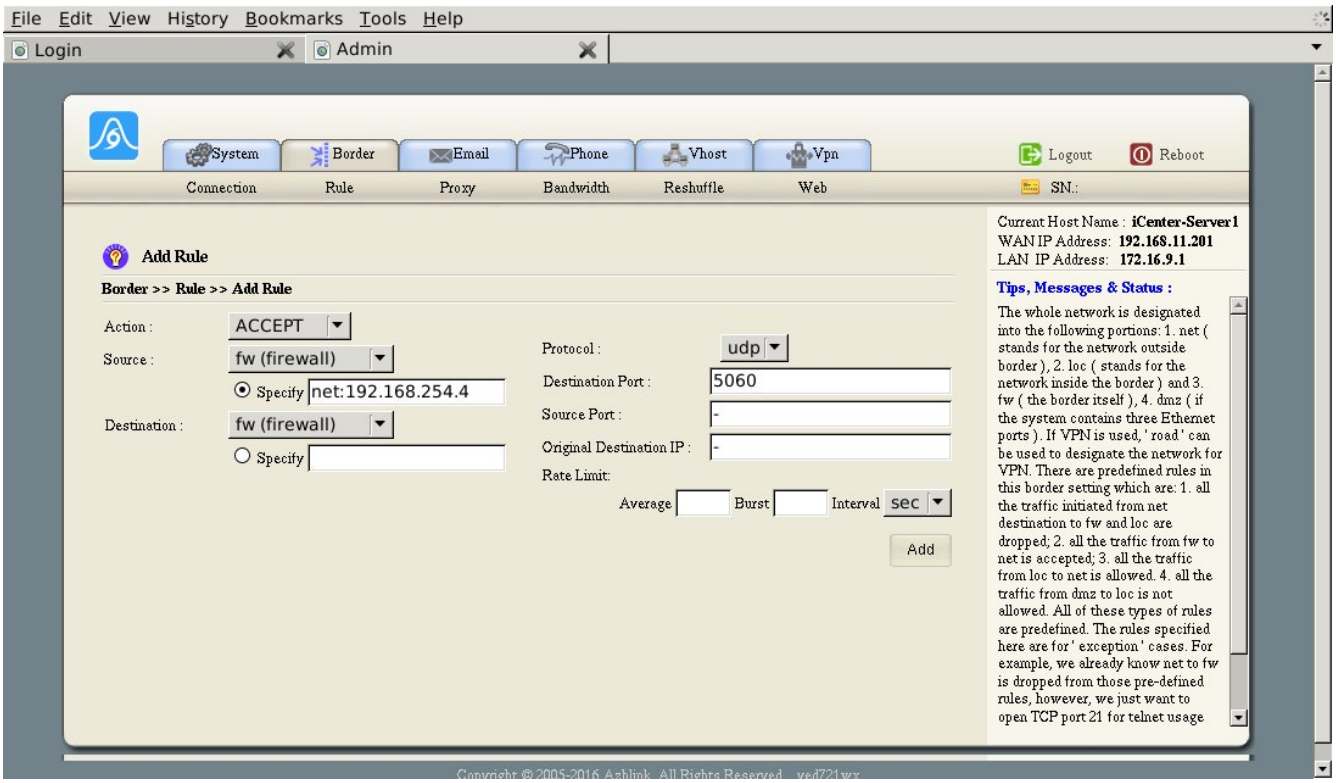
Similarly, you might set “From” 10.0.0.0/8 and “192.168.255.0/24 to look into this “moon” routing table.

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 | Logout | Reboot

Connection | Rule | Proxy | Bandwidth | Reshuffle | Web | SN.:

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

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

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

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 | Logout | Reboot

Connection | Rule | Proxy | Bandwidth | Reshuffle | Web | SN.:

Current Host Name : **acrosser-amd**
WAN IP Address: **125.2[redacted]**
LAN IP Address: **172.16.9.1**

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:

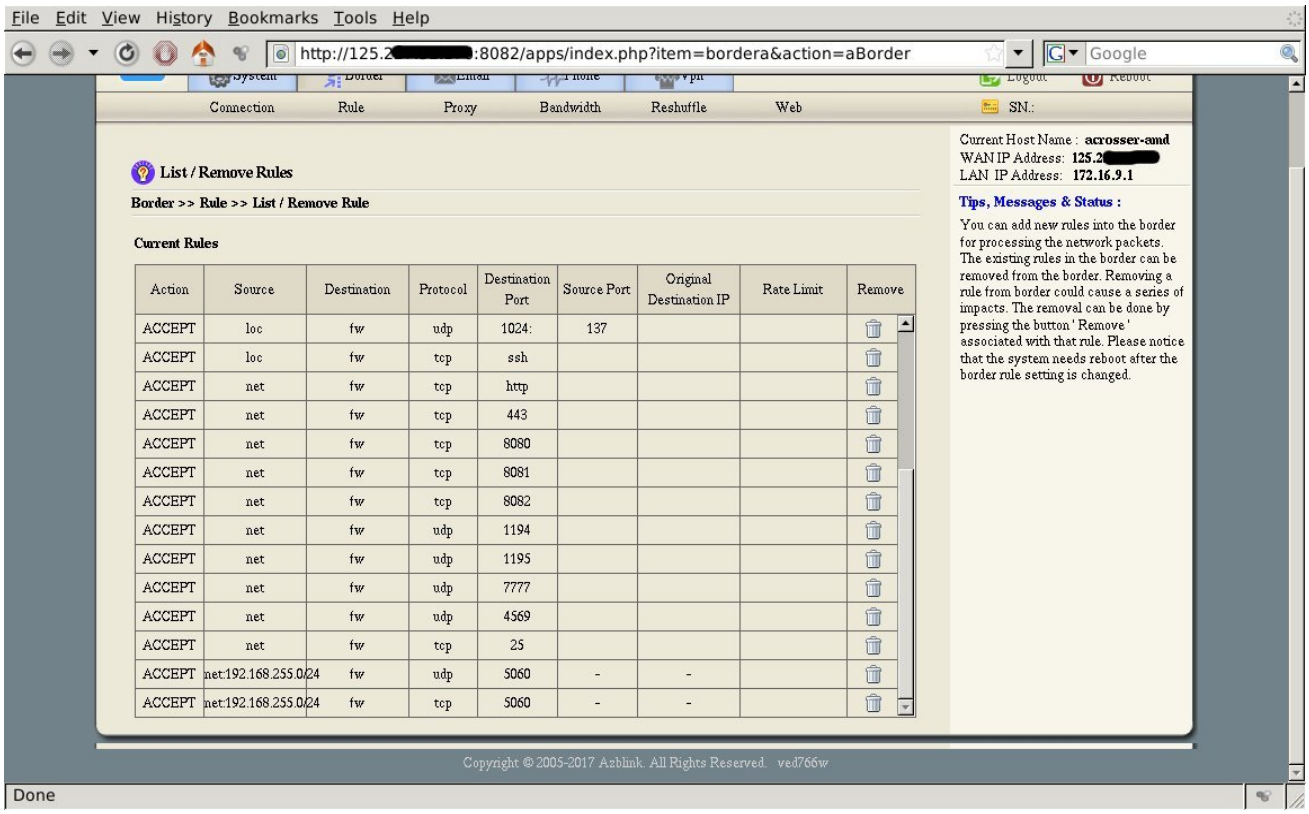
Average Burst Interval sec

Add

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

Done



Action	Source	Destination	Protocol	Destination Port	Source Port	Original Destination IP	Rate Limit	Remove
ACCEPT	loc	fw	udp	1024:	137			
ACCEPT	loc	fw	tcp	ssh				
ACCEPT	net	fw	tcp	http				
ACCEPT	net	fw	tcp	443				
ACCEPT	net	fw	tcp	8080				
ACCEPT	net	fw	tcp	8081				
ACCEPT	net	fw	tcp	8082				
ACCEPT	net	fw	udp	1194				
ACCEPT	net	fw	udp	1195				
ACCEPT	net	fw	udp	7777				
ACCEPT	net	fw	udp	4569				
ACCEPT	net	fw	tcp	25				
ACCEPT	net:192.168.255.0/24	fw	udp	5060	-	-		
ACCEPT	net:192.168.255.0/24	fw	tcp	5060	-	-		

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

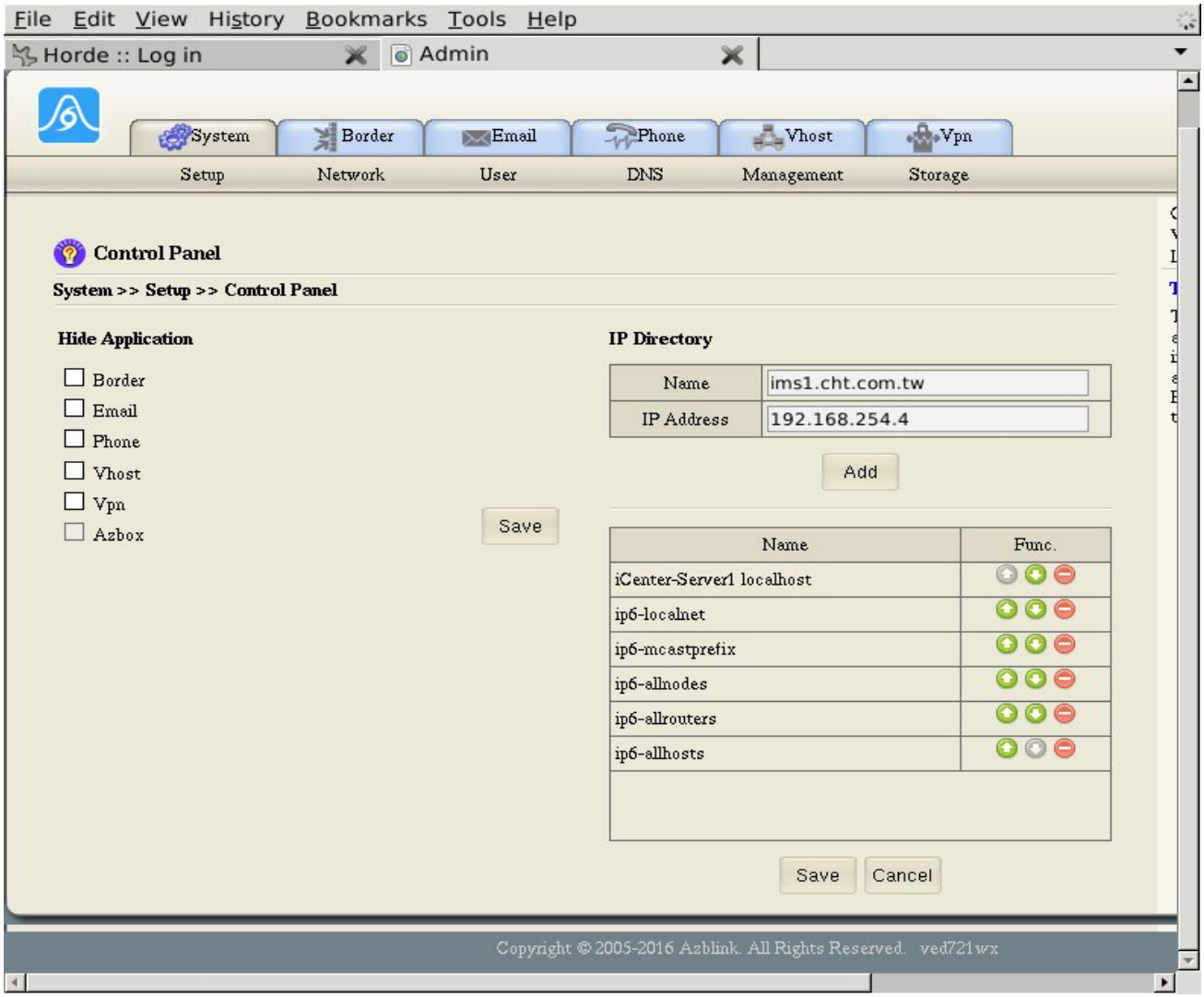
Setting Up SIP Trunk

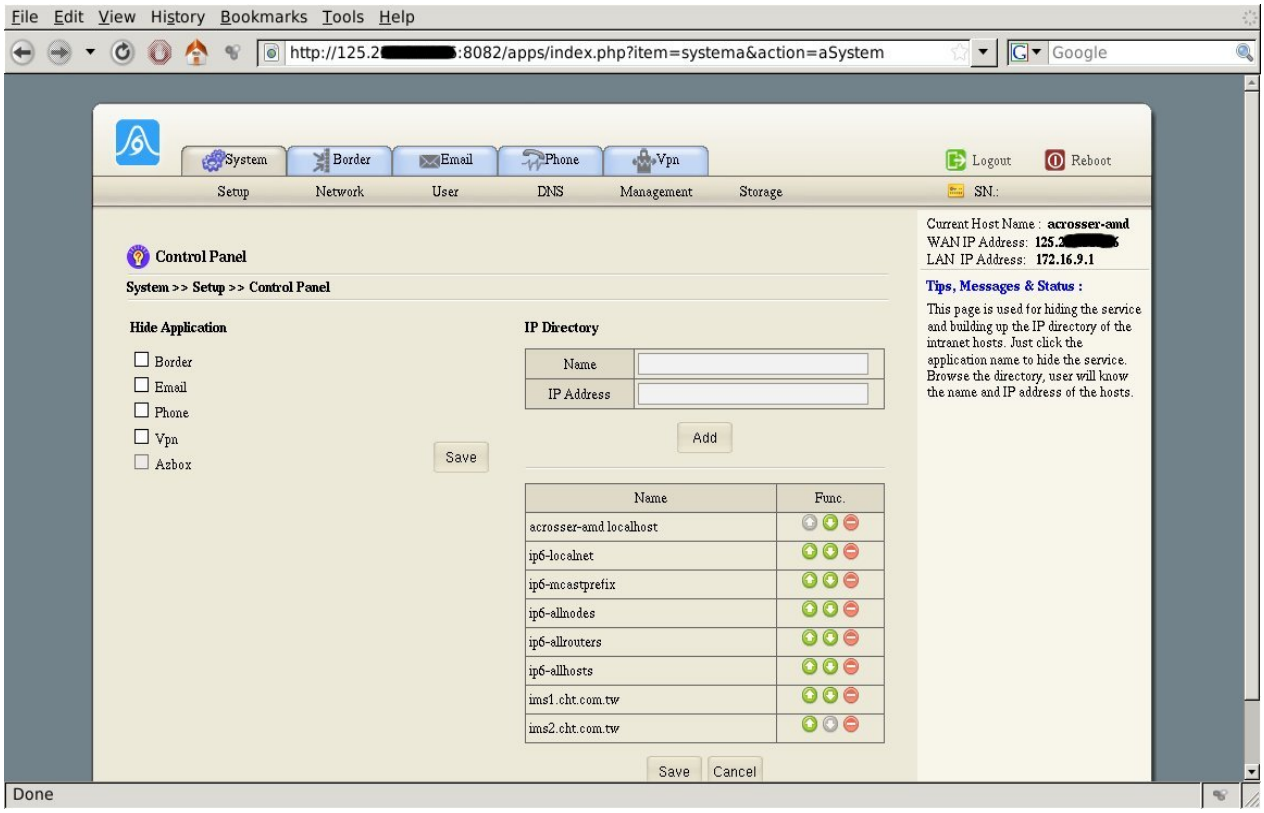
The connection parameters for the connection to IMS will be given as follows:

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

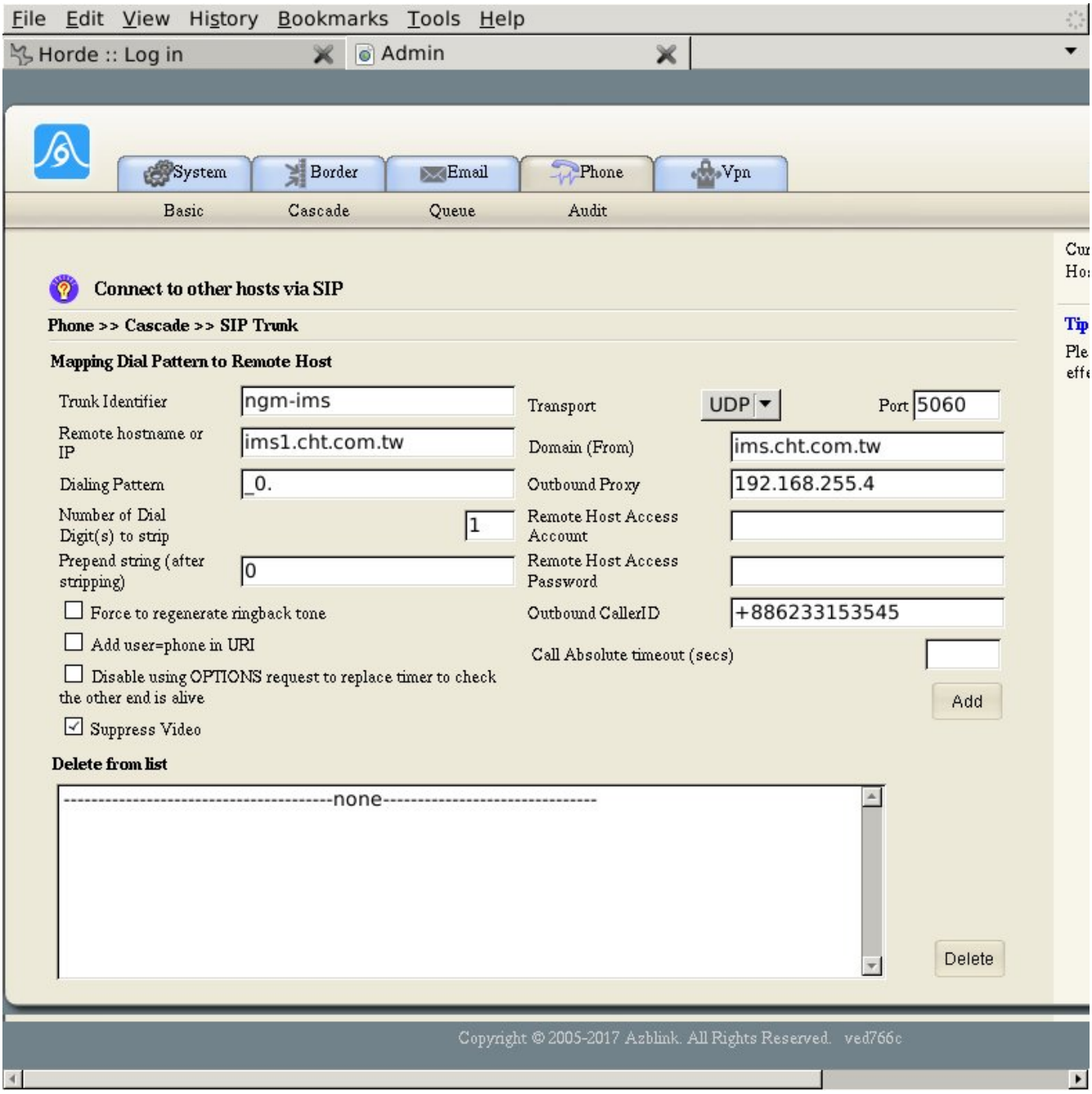
Please note that the CallerID is combined as : +(Taiwan National Code)(Area Code)(Local Phone Number). And the domain name can not be resolved from Internet DNS; it is only known to the proxy. However, in our recent build the domain name has to resolved locally. Otherwise, the system will refuse to connect 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**” :

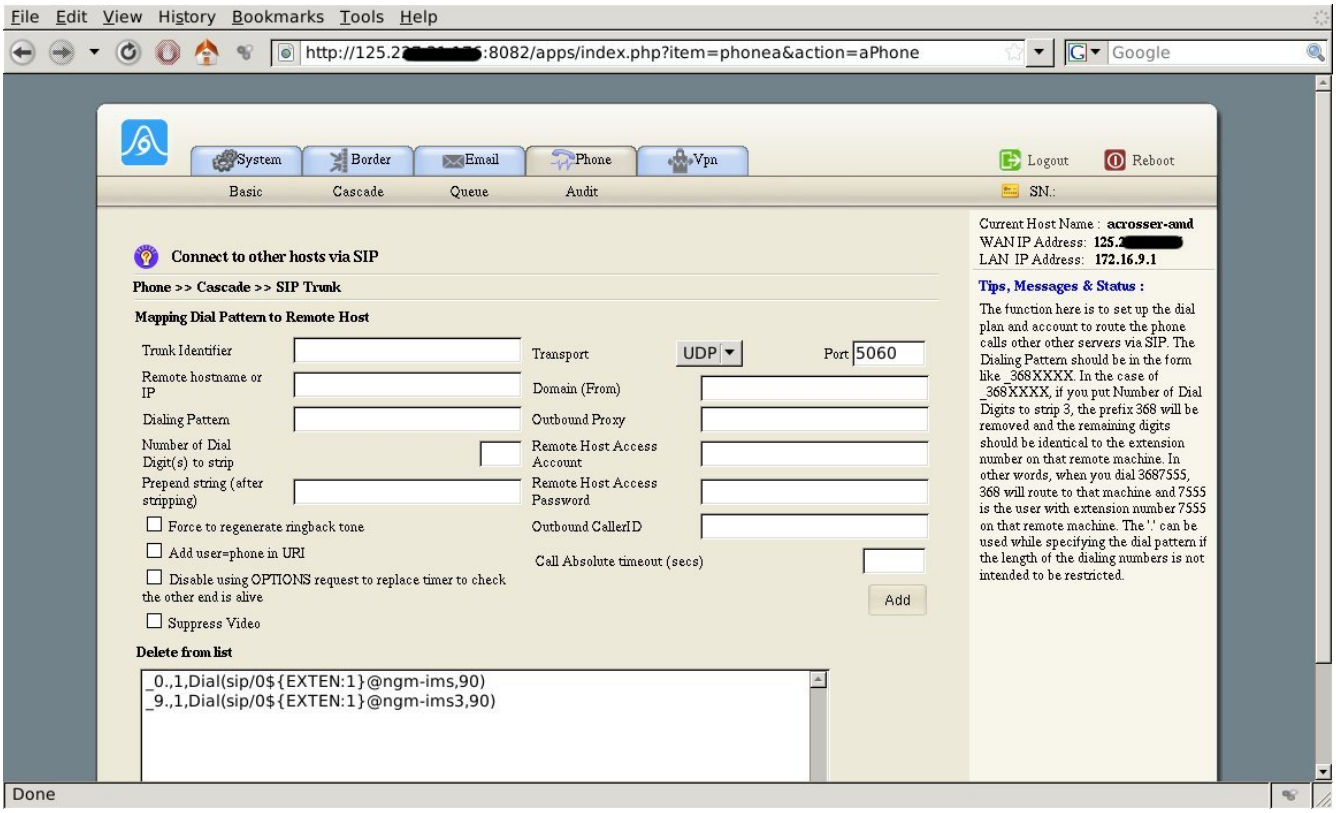




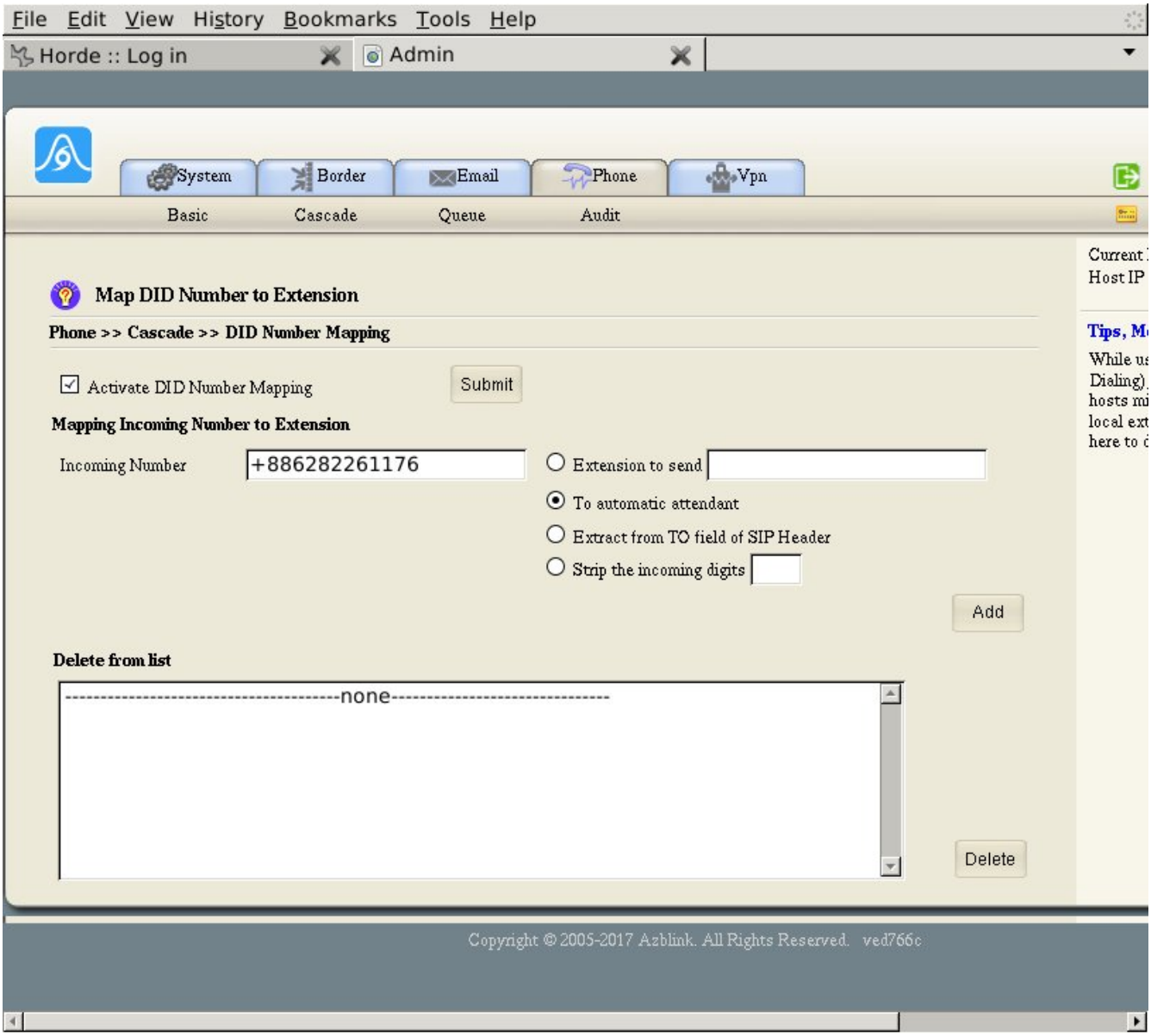
After this, we can start to set up SIP trunk. Navigate via "**Phone >> Cascade >> SIP Trunk**":



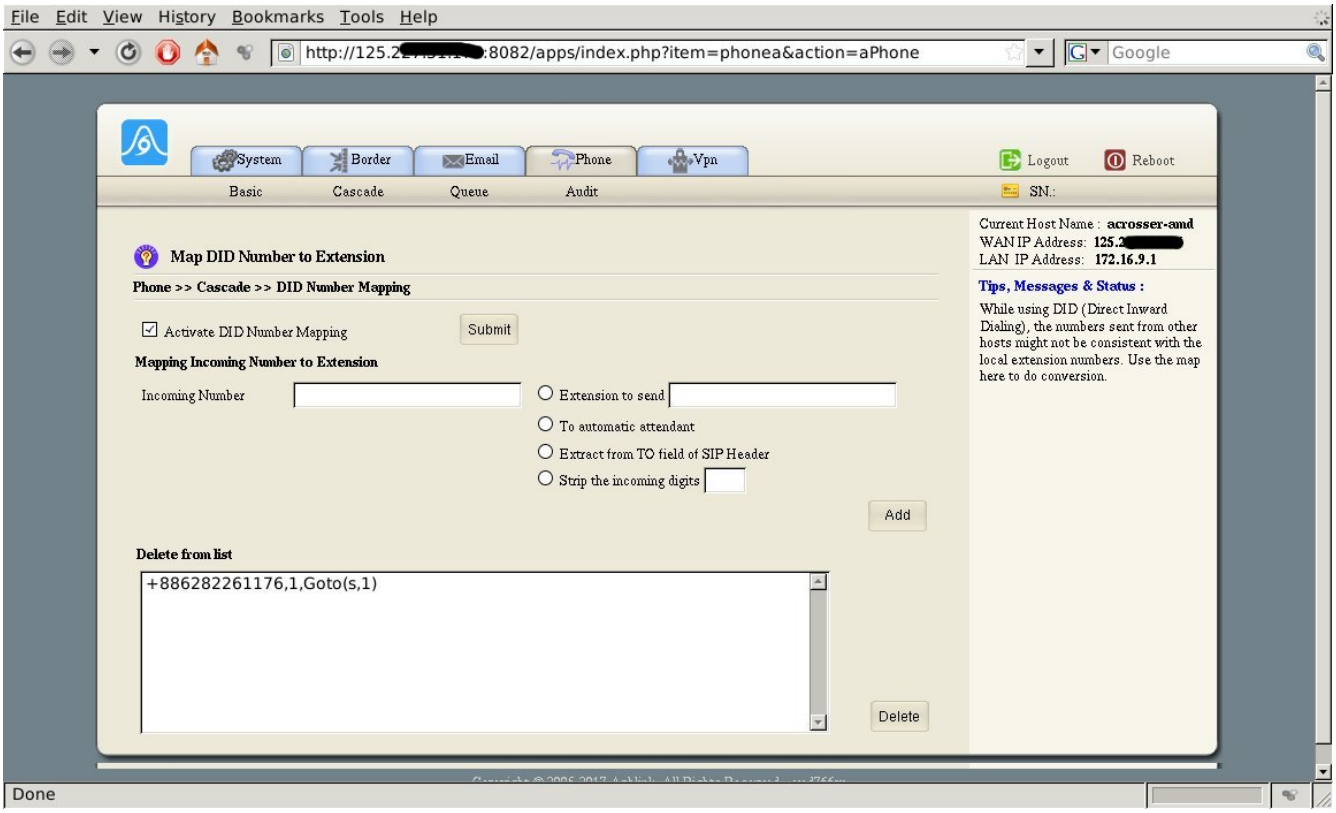
Please note: the IMS need “0” to prepend – compared to the normal dialing habit we have on PSTN; and “Video” has to be suppress. Furthermore, the inbound calls might be also from the other proxy (for example, “192.168.255.248”). Thus, we need to set up another dummy trunk to allow the inbound calls from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



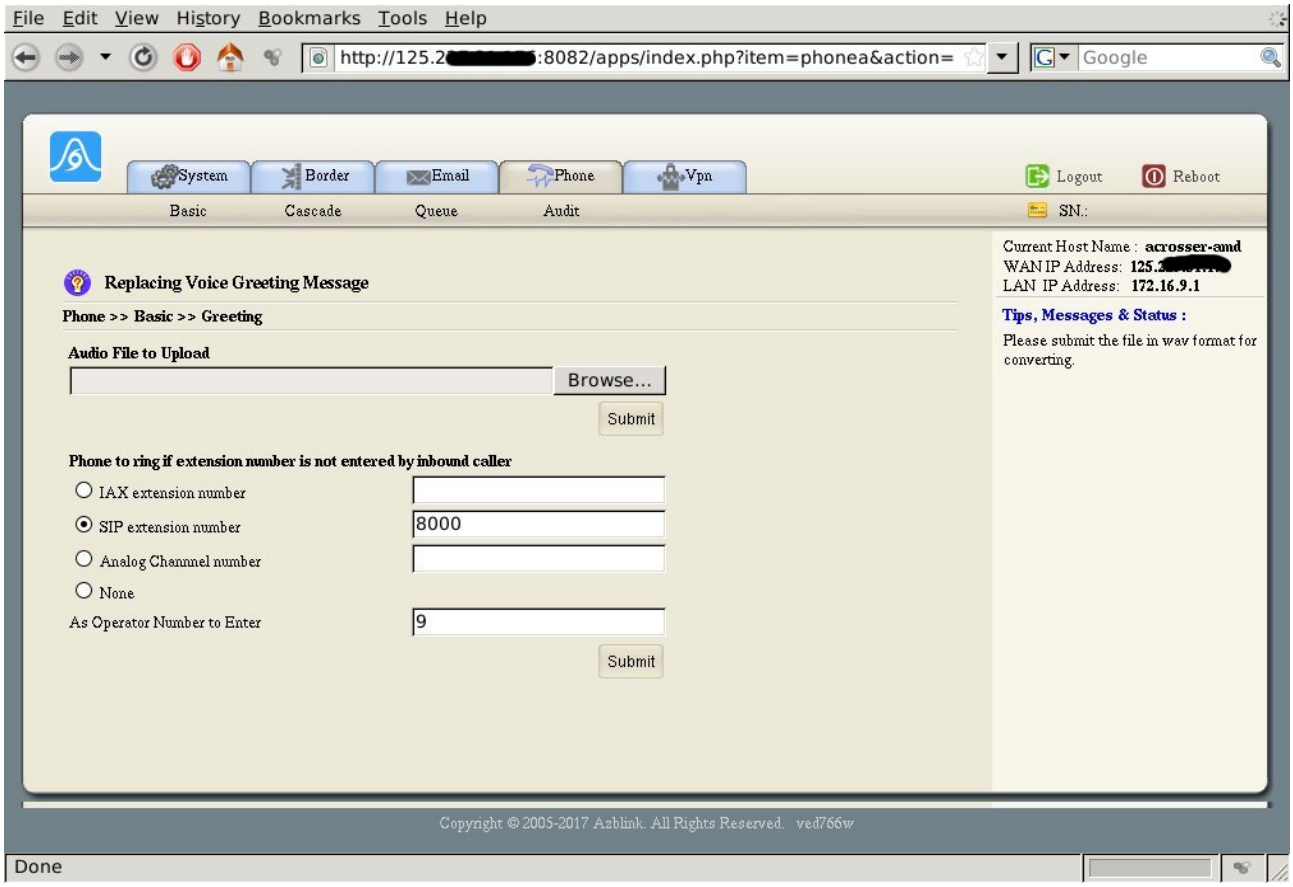
If we want to do DID to sending the coming calls directly to an extension for a specific incoming number, please remember that that extension has to disable “video”. Otherwise, Chunghwa's IMS will interrupt the call once the call is picked up.



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.

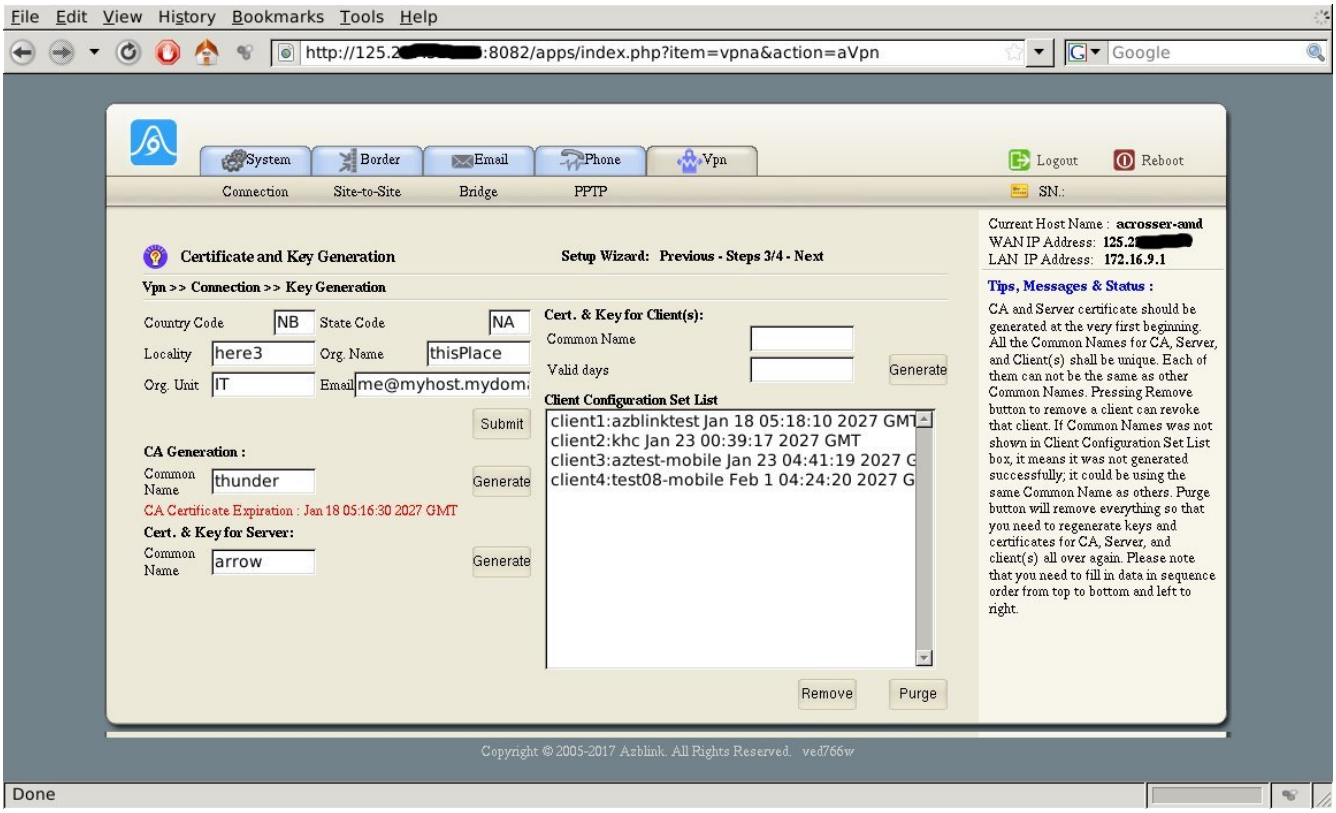
Please note that any changes made here will reset the dial rules in "default" context (SIP trunk rules might disappear if they are in the context "default" or DID activation box will be unchecked). SIP trunk rules usually are placed in the context "all" so that they should not be affected unless you 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**".



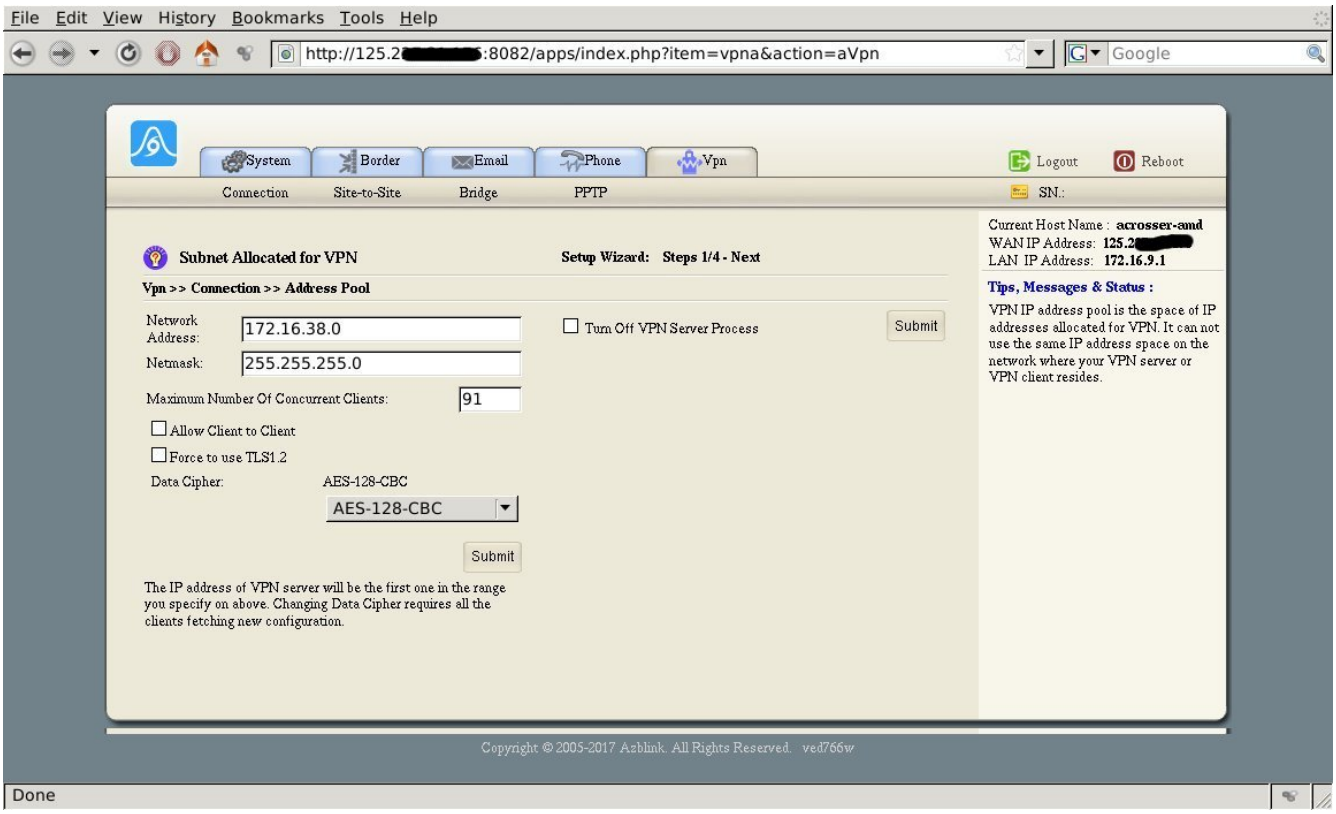
Create User Accounts for Mobile Devices

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.

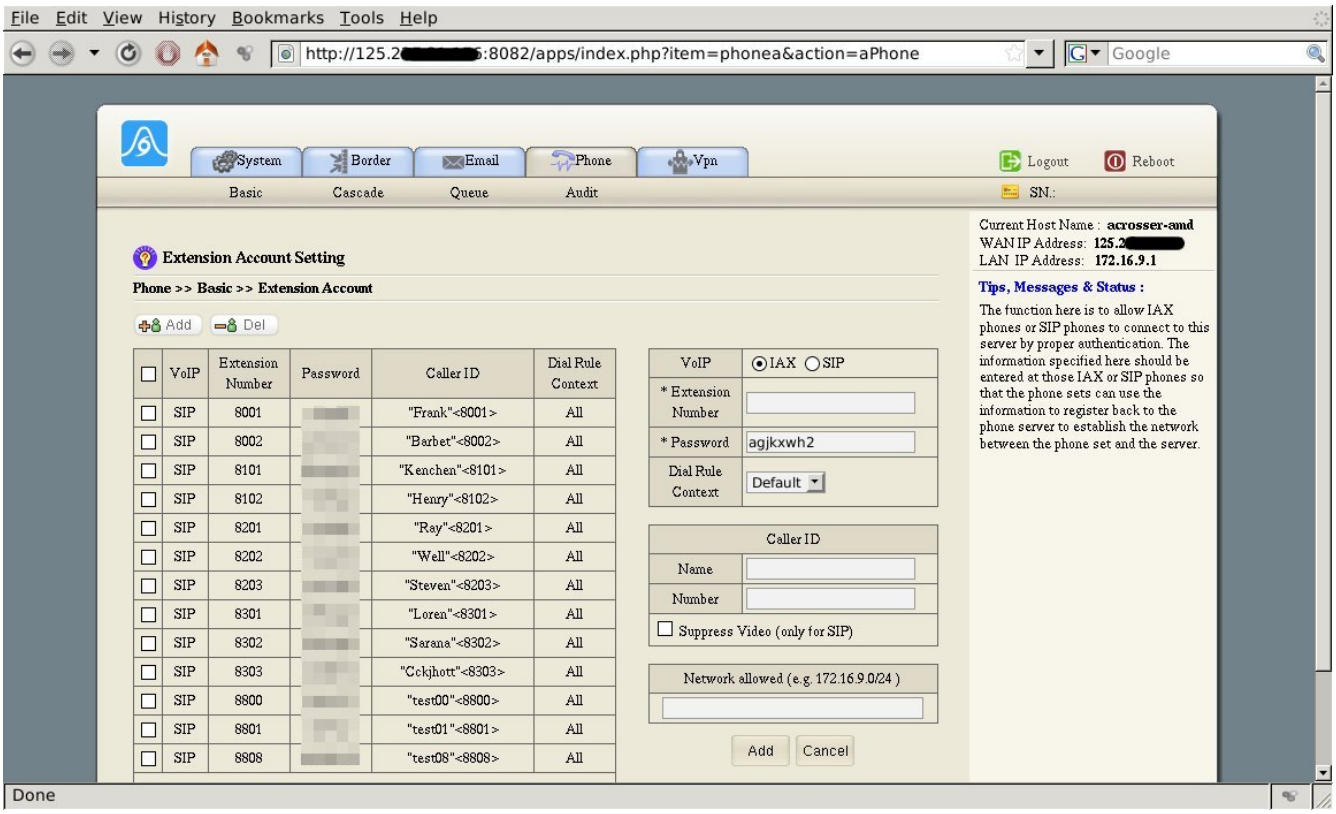
To reach to that goal, it is necessary to check the following items. At first, we need to check if CA (certificate authority) and server key/certificate for VPN are generated successfully (**Vpn >> Connection >> Key Generation**):



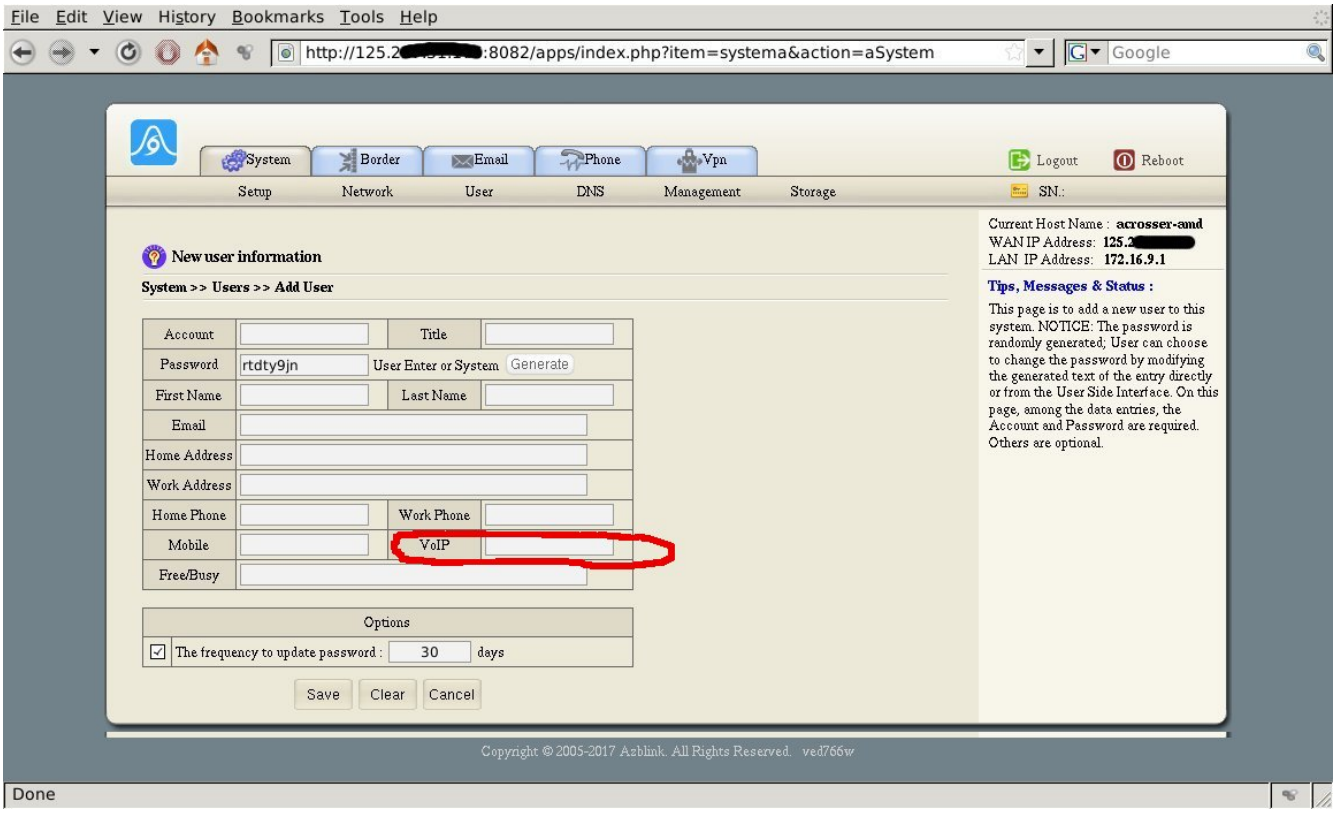
And check if VPN server is started (**Vpn >> Connection >> Address Pool**):



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



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**".



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

File Edit View History Bookmarks Tools Help

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

System | Border | Email | Phone | Vpn | Logout | Reboot

Setup | Network | User | DNS | Management | Storage | SN.:

Current Host Name : **acrosser-amd**
WAN IP Address: **125.2[redacted]**
LAN IP Address: **172.16.9.1**

Tips, Messages & Status :

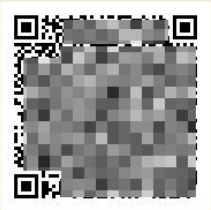
View User Information via QR code

System >> User >> User QR

☑ Hide the accounts used by the system processes

User Account List
aztest
barbet
callmgr
cckjhott
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

Done