Administration Manual

Publication Information

Toshiba America Information Systems, Inc.
Telecommunication Systems Division

Publication Information

Toshiba America Information Systems, Inc., Telecommunication Systems Division, reserves the right, without prior notice, to revise this information publication for any reason, including, but not limited to, utilization of new advances in the state of technical arts or to simply change the design of this document.

Further, Toshiba America Information Systems, Inc., Telecommunication Systems Division, also reserves the right, without prior notice, to make such changes in equipment design or components as engineering or manufacturing methods may warrant.

Version 14, April 2014

VIPedge R1.4.5 and later

Our mission to publish accurate, complete and user accessible documentation. At the time of printing the information in this document was as accurate and current as was reasonably possible. However, in the time required to print and distribute this manual additions, corrections or other changes may have been made. To view the latest version of this or other documents please refer to the Toshiba FYI web site.

Toshiba America Information Systems shall not be liable for any commercial losses, loss of revenues or profits, loss of goodwill, inconvenience, or exemplary, special, incidental, indirect or consequential damages whatsoever, or claims of third parties, regardless of the form of any claim that may result from the use of this document.

THE SPECIFICATIONS AND INFORMATION PROVIDED HEREIN ARE FOR INFORMATIONAL PURPOSES ONLY AND ARE NOT A WARRANTY OF ACTUAL PERFORMANCE, WHETHER EXPRESSED OR IMPLIED. THE SPECIFICATIONS AND INFORMATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. ACTUAL PERFORMANCE MAY VARY BASED ON INDIVIDUAL CONFIGURATIONS, USE OF COLLATERAL EQUIPMENT, OR OTHER FACTORS.

Trademarks

Toshiba, IPedge, VIPedge, CIX, eManager, and Net Phone are trademarks of Toshiba Corporation or Toshiba America Information Systems, Inc.
Visualware and MyConnection Server are trademarks of Visualware, Inc.
Adtran is a registered trademark of Adtran, Inc.
iTunes is a trademark of Apple, Inc.
Google and Google Play are registered trademarks of Google Inc.
Audacity is a trademark of Dominic M Mazzoni.
Cisco is a registered trademark of Cisco Technology, Inc.
Mozilla and Firefox are registered trademarks of Mozilla Foundation Corp.
Windows, Outlook, and Microsoft are registered trademarks of Microsoft.
Trademarks, registered trademarks, and service marks are the property of their respective owners.

General End User Information

FCC Requirements

Means of Connection: The VIPedge does not connect directly to the telephone network. All direct connections are made to a gateway. Please refer to the gateway manufacturer's documentation

Radio Frequency Interference

Warning: This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the manufacturer's instruction manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case, the user, at his/her own expense, will be required to take whatever measures may be required to correct the interference.

Underwriters Laboratory

This system is listed with Underwriters Laboratory (UL). Secondary protection is required, on any wiring from any telephone that exits the building or is subject to lightning or other electrical surges, and on DID, OPS, and Tie lines. (Additional information is provided in this manual.)

c UL us
LISTED
301756
I.T.E

CP01, Issue 8, Part I Section 14.1

Notice: The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the Equipment will operate to the user's satisfaction.

Repairs to Certified Equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

CAUTION! **Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.**

Important Notice — Music-On-Hold

In accordance with U.S. Copyright Law, a license may be required from the American Society of Composers, Authors and Publishers, or other similar organization, if radio or TV broadcasts are transmitted through the music-on-hold feature of this telecommunication system. Toshiba America Information Systems, Inc., strongly recommends not using radio or television broadcasts and hereby disclaims any liability arising out of the failure to obtain such a license.

Hearing Aid Compatibility Notice: The FCC has established rules that require all installed business telephones be hearing aid compatible. This rule applies to all telephones regardless of the date of manufacture or installation. There are severe financial penalties which may be levied on the end-user for non-compliance.

Patent Marking for G.729a: Products may be covered by one or more of the following US patents and their counterparts in other countries:
US5,787,391, US5,717,825, US5,708,757, US5,754,976, US5,701,392, US5,699,482, US5,444,816

Toshiba America Information Systems, Inc.
Toshiba VIPedge Services Terms and Conditions
Refer to http://www.telecom.toshiba.com/Telephone_Systems_Support/VIPedge-Terms/terms-andconditions.pdf

Toshiba America Information Systems, Inc.
Telecommunication Systems Division, VIPedge Acceptable Use Policy
Refer to http://www.telecom.toshiba.com/Telephone_Systems_Support/VIPedge-Terms/acceptableuse.pdf

Toshiba America Information Systems, Inc.
Telecommunication Systems Division, End User License Agreement
Refer to http://www.telecom.toshiba.com/Telephone_Systems_Support/warranty.cfm

Toshiba America Information Systems, Inc.
Telecommunication Systems Division, End User Standard User Limited Warranty
Refer to http://www.telecom.toshiba.com/Telephone_Systems_Support/warranty.cfm

Toshiba America Information Systems, Inc.
Telecommunication Systems Division, Redistribution of OpenSource GPL Attribution
Refer to Toshiba Internet FYI > VIPedge > Documentation.

Emergency Service (911) Warning

The VIPedge system must have a constant source of electricity and network connection availability to function. In the event of a power failure or network availability outage the VIPedge system's SIP service will be disabled. The user understands that in the event of a power or network outage the VIPedge system will not support 911 emergency services and further, that such services will only be available via user's regular telephone line not connected to the VIPedge system or gateway. User further acknowledges that any interruption in the supply or delivery of electricity or network availability is beyond Toshiba's control and that Toshiba shall have no responsibility for losses arising from such interruption.

Security Warning

All equipment shipped to support the VIPedge system ship with the same default user names and passwords. To help protect your VIPedge system from unauthorized administrator access change the user names and passwords. Any equipment that is not properly protected may expose the system to toll fraud, denial of service or other attacks.

Contents

Chapter 1 – Administration Portal

Chapter 2 – Network Requirements

Chapter 3 – System Installation

Chapter 4 – Station Install

Chapter 5 – SIP Trunk Configuration

Chapter 6 – Enterprise Manager

Chapter 7 – VIPedge Webmin

Chapter 8 – VIPedge System Backup

Chapter 9 – Net Server

Chapter 10 – Messaging

Chapter 11 – VALCOM ACCESSORIES

Chapter 12 – Adtran NetVanta 3120 Setup

Chapter 13 – Adtran NetVanta 3448 Setup

Chapter 14 – Customer Admin Portal

This page is intentionally left blank.

Chapter 1 – Administration Portal

DEALER ADMINISTRATION

This document is a guide to the VIPedge Dealer Portal setup and new customer administration.

Outline

The Dealer Portal is the administration entry point for VIPedge dealers.

New Dealer

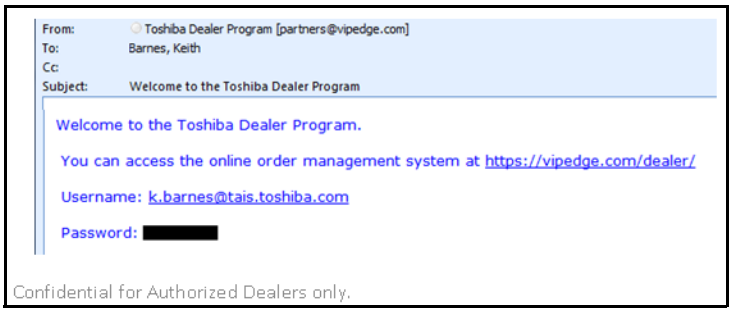
- New dealers must login to their account to setup a password and, as needed, edit the Account Details.

All Dealers

- Add a New Customer to the list
- Create then, submit a Quote to a customer
- Process the order when the customer accepts the quote.
- Make programming changes to a customer's system
- Assign Reps and Technicians

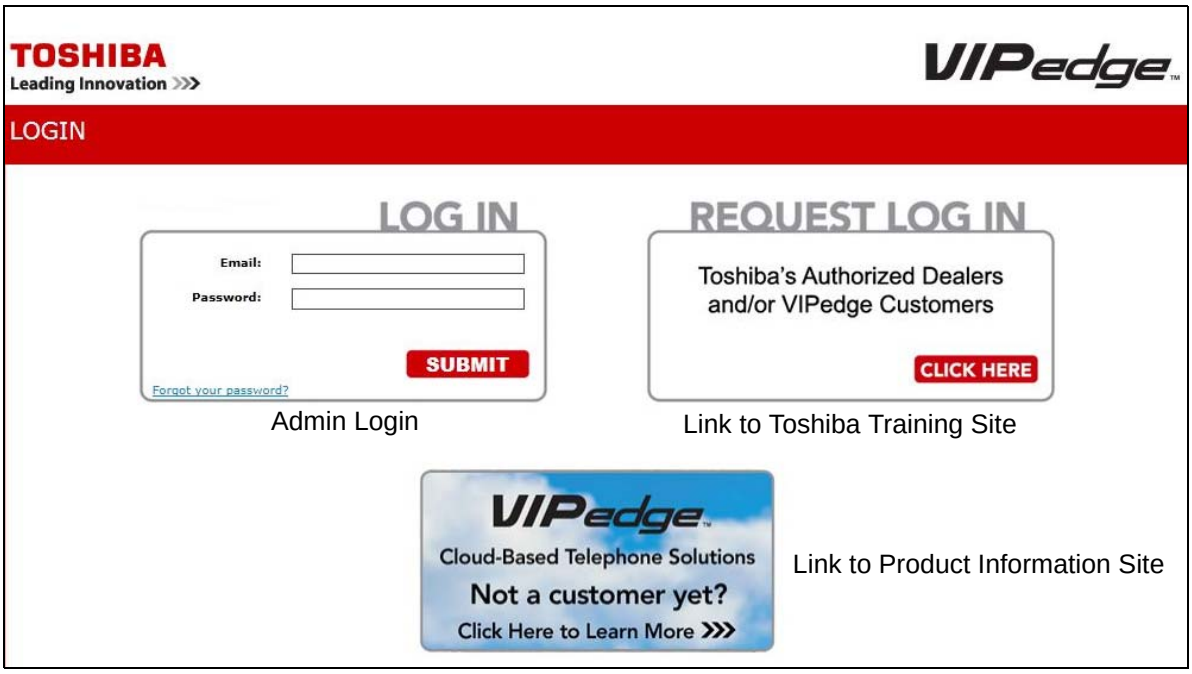
Dealer Login

1. When your Dealer account is created by Toshiba you will receive a welcome email from partners@vipedge.com. To ensure that you receive this, and other, email be sure your email spam filter is set to allow **@vipedge.com** into your mailbox.
2. The email will contain your user name (your email address) and a temporary password. The user name is case sensitive.



3. Use one of these browsers to access the VIPedge portal.
   - Internet Explorer 8 or Internet Explorer 9

4. Login to the VIPedge portal at www.vipedge.com



Admin Login

Link to Toshiba Training Site

Link to Product Information Site

5. The first time you login the system will require a new password. The new password must be a 'strong' password with the following:
   - At least six characters, not more than 16 characters
   - At least one character must be a capital letter
   - At least one character must be a number
   - At least one character must be a special character: ! @ # $ % ^ & *) (

6. On the right side of the screen Enterprise Manager should be running. If not click on Provision AC.
7. Click on Account Details to review your account details.

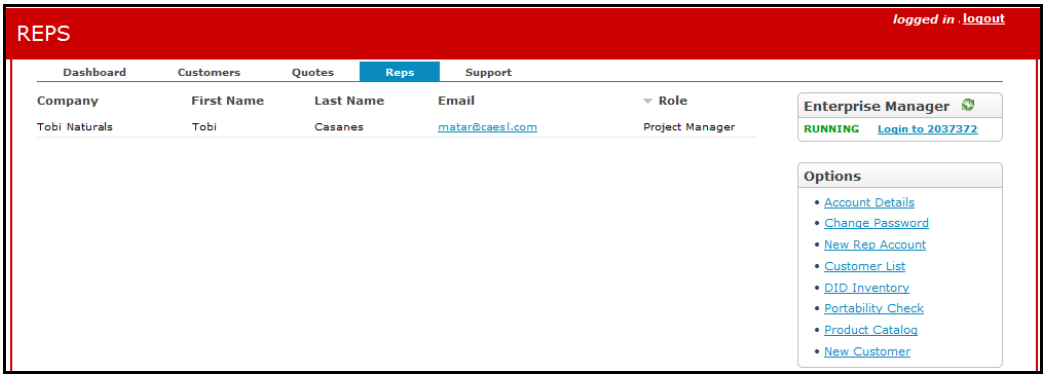
Note: When entering or editing your address remember that there must not be a - (dash) or period (.) in the address.

Each time you login the Dashboard will be displayed. The dashboard will be empty unless there are unpaid invoices or other notices.

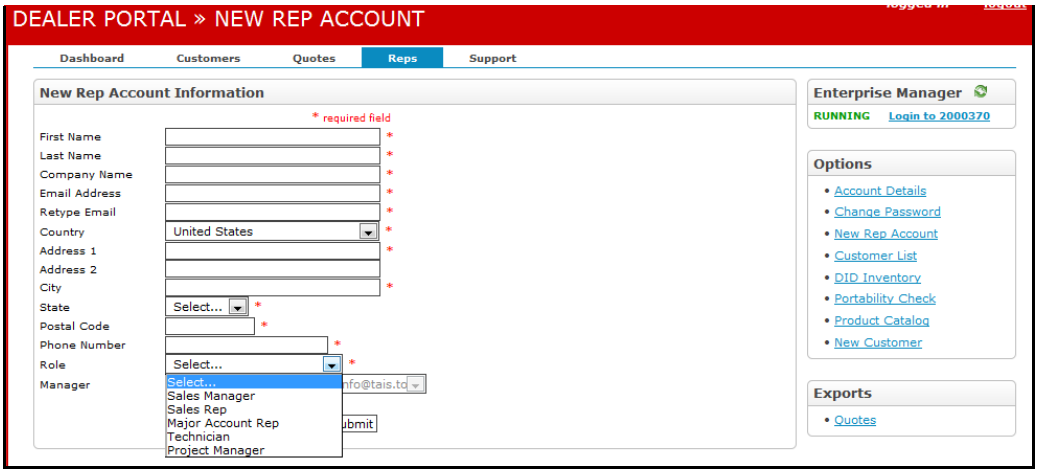
NEW DEALER ROLES Sales Reps, Managers and Technicians can added to your container.

Add New Reps

1. To add a new Rep, from the Dealer Portal, click on the New Rep Account link in the Reps tab.



2. Enter the infoprmation in the fields then select the Role. Refer to the table below for an explanation of the roles.



Permissions / Roles	Sales Manager	Sales Rep	Major Account Rep	Technician	Project Manager
Add Customers - Create a new customer.	x	x		x	
Add IPT - Add IPT serial numbers associated with the customer.				x	x
Change Customer Rep - Assign a different role to a user.	x				
Edit Customer - Edit the Customer profile.	x	x			x
View All Customers - View all customers for the dealer.	x		x	x	x
View Billing - View a customer's billing.	x	x			x
View Customers -View their own customers.	x	x	x	x	x

Permissions / Roles	Sales Manager	Sales Rep	Major Account Rep	Technician	Project Manager
View IPT - View IPT serial numbers entered for customers in the IPT tab.	x	x	x	x	x
View LNP - View LNP for customers.	x	x	x	x	x
Add Reps - Assign new Reps to this dealer.	x				
View All Reps - View all of the Reps assigned to this dealer.	x				x
View Reps - View the portal, no view of other Reps.	x		x		x
Create Port Request - Create new Port Requests.	x	x			x
Edit Port Request - Edit existing Port Requests.	x	x			x
Create Quote - Create new quotes or change orders.	x	x			x
Delete Quote - Delete quotes.	x	x			x
Process Quote - Process quotes accepted by the customer.	x				x
View All Quotes - View all quotes created by the dealer.	x			x	x
View Quotes - View their own quotes.	x	x	x	x	x
Manage Product Catalog - Create and manage the Dealer Product Catalog.					
Manage Servers - Create and manage change orders and see PBXs.	x	x		x	x
View AC - Access Enterprise Manager.			x	x	x
View DID Inventory - Create a list of available DIDs.	x	x	x	x	x

(Sheet 2 of 2)

NEW CUSTOMER SETUP

Customers are added to your container in a series of steps.

Add to the List

1. To add a new customer click on the New Customer link in the Options box on the right side of the screen.
2. Enter the customer's information. Remember; no dash (-) or period (.) in the address.

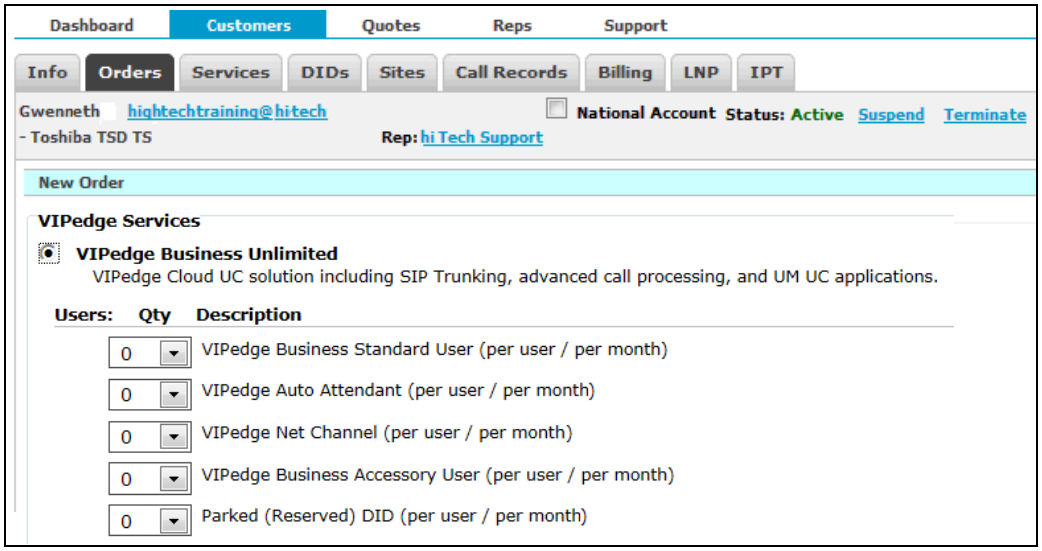
Note: The Customer Name must be 50 characters or less.

Important! Each customer must have a unique email address.

QUOTES

The customer must be added as shown above before you can create a quote. Click on Create new order to start a quote. The items that can be selected on the New Order page and the quote process page, are shown below.

VIPedge Services Click to select **VIPedge System**. This is the license that creates the system container for the customer's VIPedge system.



Users There are five types of users.

The **Business Standard User** licenses allow one IP Telephone (IPT, or IP4100) for each license. These stations can make and receive calls on the Unlimited and Call Center channels defined later.

The **Auto Attendant** licenses allow a directory number but no physical telephone. These directory numbers can receive calls from the Unlimited and Call Center channels.

The **VIPedge Net Channel** license allows a network connection to a Strata CIX or IPedge system. Each channel provides one conversation. Determine the number of simultaneous network connections for your network configurations up to the maximum of 64. VIPedge Net can connect to a single IPedge system or Strata CIX system at each location. When a multi-node system is in the network the VIPedge Net connects to a single node.

Note that each Strata CIX system will require Strata Net licenses and each IPedge system will require IPedge Net licenses.

The **Business Accessory** licenses allow an accessory only for use on the VIPedge Business platform. This can be used for lobby phones, warehouse phones, door phones or other internal SIP devices such as external paging systems. DID, mailbox, Call Manager w/VoIP Plug-in, or Unified Messaging licenses are not included.

The **Parked (Reserved) DID** allows a directory number to be parked and then used later. These DID numbers can be; numbers ported over to the VIPedge or purchased but not yet placed in service. There is a fee for DID parking, and porting charges still apply. Calls to parked numbers will be answered with a "not in service" message.

Package

There are two types of packages:

- Unlimited (up to 1200 minutes average per channel)
- Call Center (Over 1200 minutes per channel)

The channels for a system will be one or the other, not a mix.

Unlimited Channels

VIPedge Channel - Unlimited - These both way channels include up to 1200 minutes (average) Local and Long Distance minutes. International Calling is charged on Per Minute basis. There must be at least one standard user when these are ordered.

Unlimited Local / Long Distance service is subject to Toshiba's Acceptable Use Policy. The policy can be viewed on Toshiba's web site: http://www.telecom.toshiba.com/Telephone_Systems_Support/VIPedge-Terms/acceptable-use.pdf. If a business fits the Call Center classification for one or more months, the business will be re-configured with "V-BIZ-CHCC - VIPedge Channel - Call Center" channels and will be charged based on the standard Call Center per minute rate plan.

Call Center

VIPedge Channel - Call Center - These both way channels are charged Per Minute for Local, Long Distance and International calling. The first 1200 Minutes of Local and Long Distance is included, then charged Per Minute for overage. International Calling is always charged on a Per Minute basis. There must be at least one standard user when these are ordered.

Trunk Channels

Concurrent Calls is the number of simultaneous trunk calls the system can support.

Build A Quote

Quotes, once started are automatically saved. If you exit the quote before sending all of data is saved and will be displayed in the Quotes tab when you return.

1. In the admin screen select **Customer List**.
2. Click on a customer in the list.
3. Click on **Create New Order**.
4. Select the amounts of each item. **VIPedge Services** and **Account Options** are automatically added to the column on the right. **Phones and Equipment** are not added until the **Add Selected** Items button is clicked.
5. The **Installation and Peripherals** section is used to add labor and installation costs. These are added when you click the **Update Totals** button.
6. Select the **Freight and Handling** method. This charge will be added to the One Time total.
7. Select:

   Email Quote - Sends an email of the work sheet. This is only the information about the quote. You must submit the quote for the customer to accept it.

   Create PDF - Creates a PDF document of the worksheet

Submit Quote - Sends the quote to the customer with a link in the email. This link allows the customer to accept the quote.

8. After the quote has been accepted and the payment details are processed you will be able to start programming that customer's service. Logon to the Dealer Portal, display the customer list. Select the customer then, click on login to server. Login to Enterprise Manager.

Process a Quote

When the quote was submitted an email was sent to the customer. The email includes a PDF of the quote. Also, in the email is a secure link to the VIPedge system and a temporary password. The customer can accept or refuse the quote. When the customer accepts the quote he/she will go to the account setup section. This is where the credit card or bank account information is entered. This information is not available to the dealer.

When the customer completes this process the dealer will receive an email that the order has been accepted. This email includes a link to the VIPedge system.

1. Login, the order information will be displayed. Scroll to the bottom of the page.
2. Click on the Process Order button.
3. The customer server will initialize.
4. After the server has initialized you will be able to login to Enterprise Manager for this customer.

Note: Do not make any programming changes until the server has been licensed.

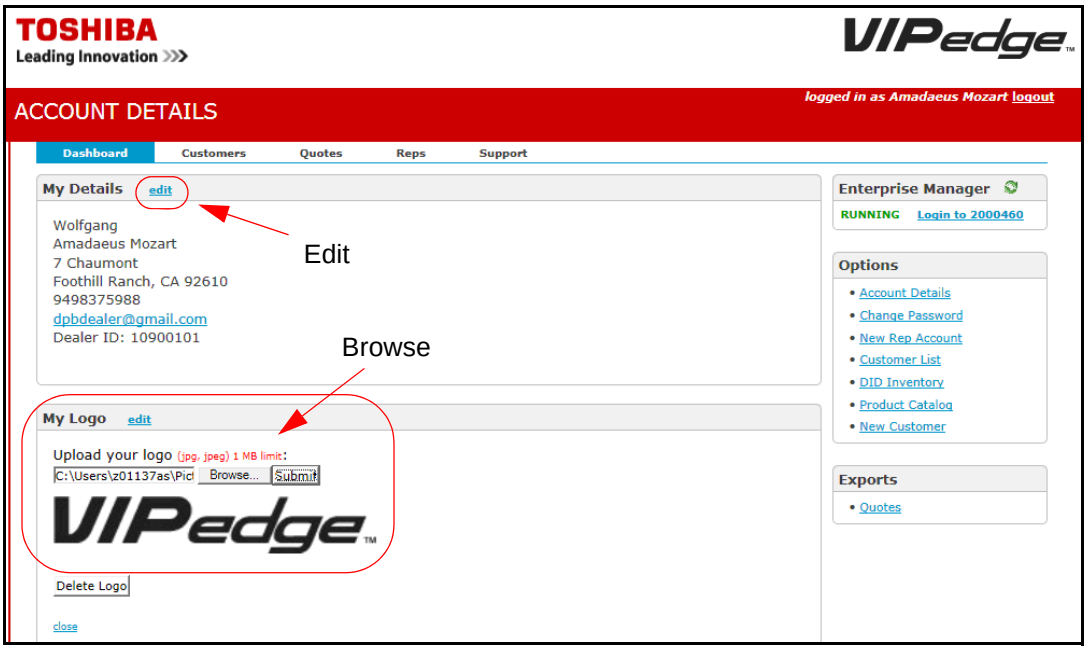
5. When the licenses have been applied you can begin the customer database programming.

DID AVAILABILITY

In the Dealer Portal click on the DID Preview link to find available DID numbers in your customer's area.

DEALER LOGO

Your dealer logo can be uploaded to your container and will be included on Quotes and Invoices sent to your customers.



1. In the Account Details, in the Dashboard tab, click **Edit**. Then **Browse** to navigate to the logo file.
2. Click on **Submit**.

DEALER CATALOG

To allow dealers to provide customer support services to VIPedge customers, a Product Catalog has been created. This feature allows dealers to create services that are added to the monthly service section of the quote.

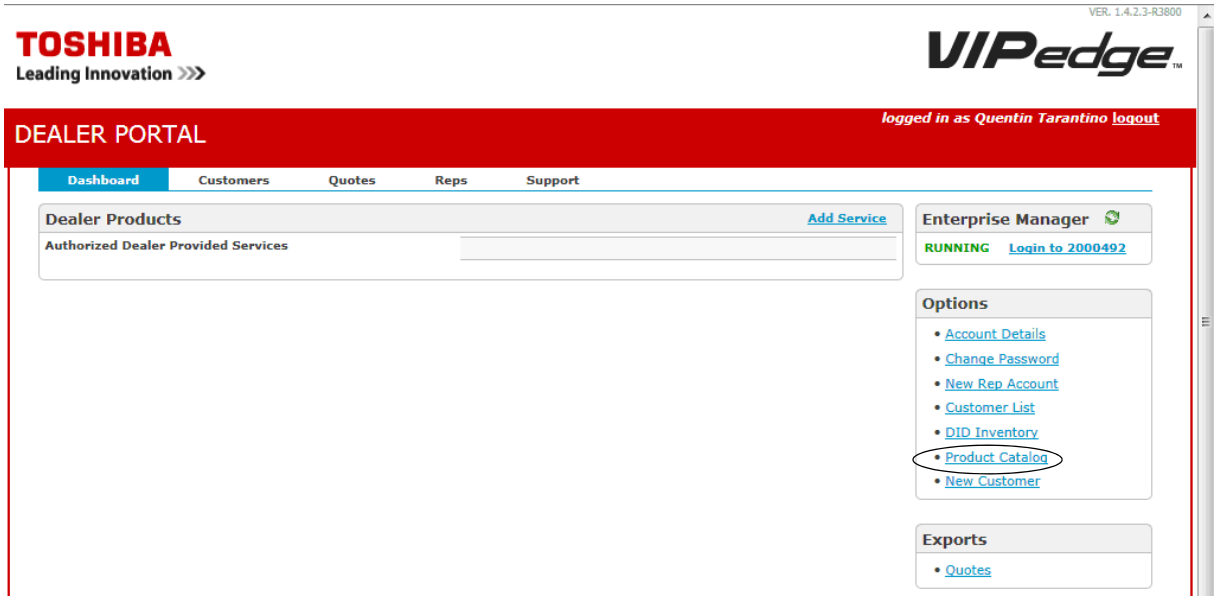
Only products in the catalog can be added to a Quote. Catalog items can only be sold when a new quote for a customer is created. A quote only for catalog items cannot be created. Catalog items cannot be added to a Change Order.

Create a Catalog Item

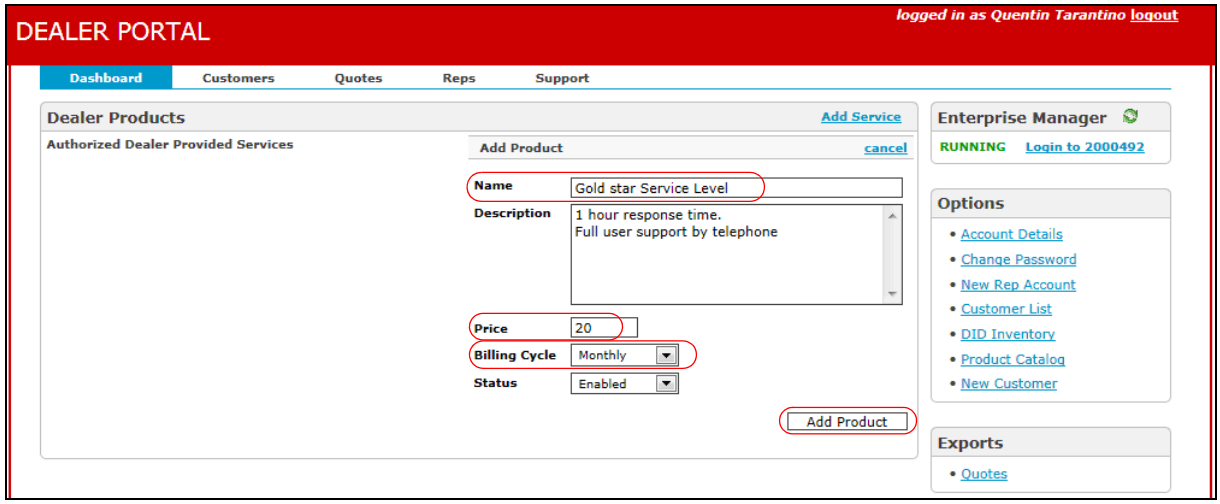
Items must be in the catalog before you can add them to a quote.

1. Login to as dealer.

2. Click on the **Product Catalog** link.

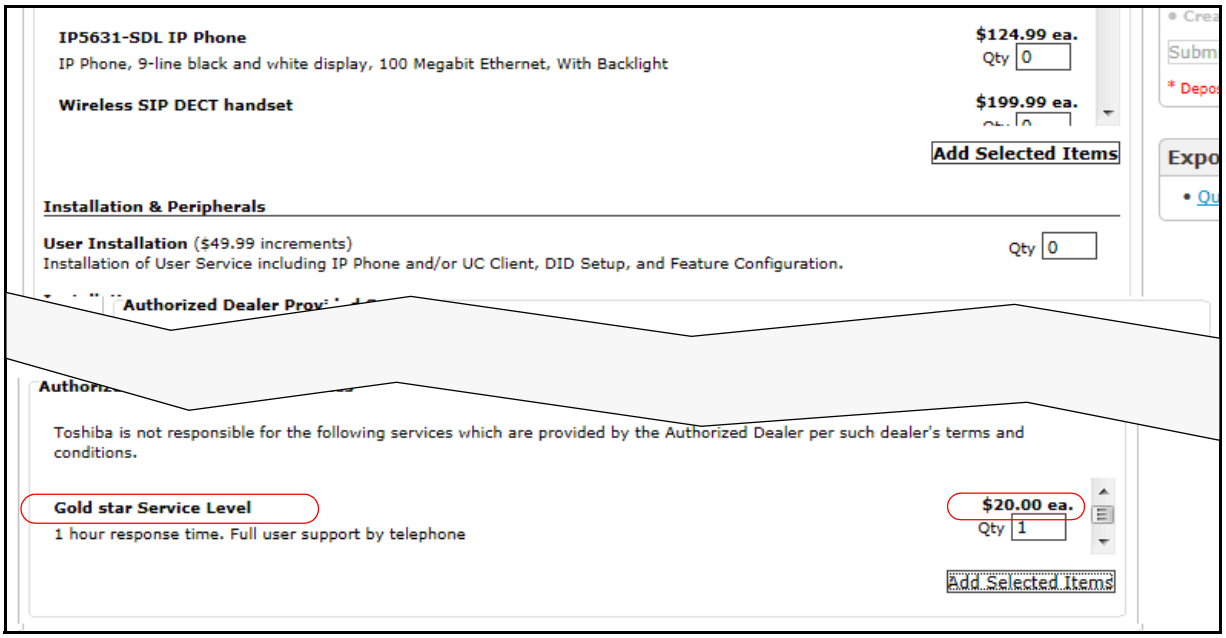


3. Click on **add services**.
4. Fill in the form and click **add product**.
   The billing cycle is always **Monthly**.
   The Status is **enabled**. Selecting Disabled will remove the product from the catalog.



5. You can edit the item or add additional items.

6. The product will appear as an item that can be selected in a quote.



ACCESS the CUSTOMER SYSTEM

The procedure shown below can be used to access a customer's server through the Dealer Portal. This is used to login to Enterprise Manager for programming that customer's database.

1. Login to the Dealer Portal.
2. Select **Customers**.
3. Click on customer name in the list.
4. Click on the **Servers** tab.
5. Click on the **Login to Server** link.
6. In the Enterprise Manager login screen enter your dealer login.

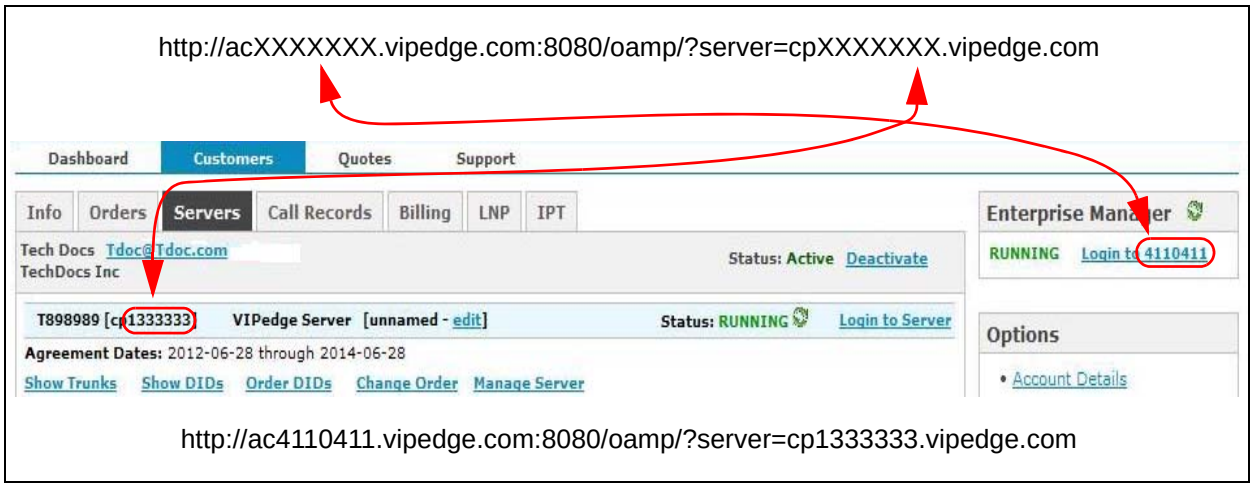
Note: If this is the first time you have entered this server be sure that the server has licenses before starting any programming.

7. You can edit the server name. A descriptive name can make administration easier.

Customer User Access

This procedure is used to create the link for the Users to login to the EMPA on the Customer's server.

1. Login to the Dealer Portal.
2. Select **Customers**.
3. Click on customer name in the list.
4. Click on the **Servers** tab.

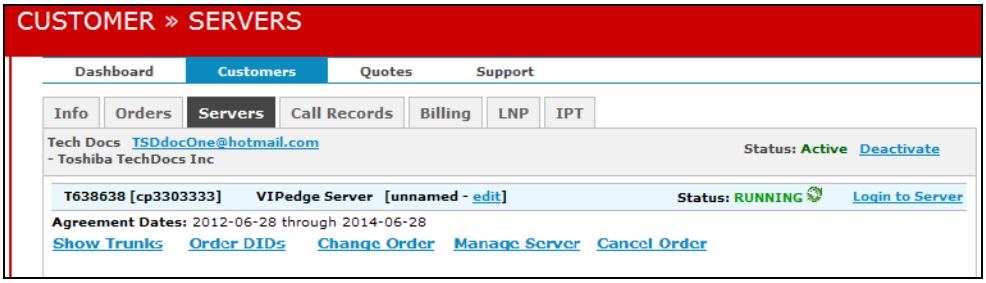


5. At the top of the example above is the format of the EMPA address (URL). Insert the AC (login) and CP numbers as shown.
6. The URL shown at the top of the example above is the address that will be given to the station users and/or the system administrator for the customer.

CUSTOMER SERVERS

1. Login to the Dealer Portal.

2. Select **Customers**.
3. Click on customer name in the list.
4. Click on the **Servers** tab.



5. Click on:

   Show Trunks - Displays the number of each type trunk and the international calling level allowed.

   Show DIDs - Display a complete list of DID (used and unused). Click Check DID Order to display the status of each DID number.

   Change Order - Add or delete users, channels; Order IPTs

   Manage Server - Used only as directed by Toshiba Technical Support

   Cancel Order - Intended to delete an order made in error. When Cancel Order is selected a cancel request is send to Toshiba's administration center. When Toshiba gets the cancel order customer order is canceled. If an active account is selected the order and the telephone system is canceled and deleted.

CAUTION! Do not Start Server, Stop Server, or Reboot Server unless instructed by Toshiba Technical Support.

Chapter 2 – Network Requirements

Important! Toshiba requires a through network assessment before deploying a VIPege system. Toshiba recommends the assement take place pre-sale. During and after installation setup network monitoring with a tool such as MyConnection Server™ by Visualware®.

NETWORK REQUIREMENTS

Listed below are the requirements for a successful VIPedge implementation.

LAN Requirements

- Network Assessment (Pathview and/or AppCritical or Similar)
- Network topology diagram
- POE for IP telephones is recommended
- Layer 3 voice prioritization
  - Layer 3: DiffServ:Enabled
  - Type:DSCP / DSCP for Voice: 46
- 88kbps (G.711 audio) in each direction per simultaneous call
- 32kbps (G.729 audio) in each direction per simultaneous call
- Jitter: 10mS or less (+/- 5mSec)
- Packet Loss: <0.1%.
- Full Duplex Ethernet on all ports
- Target MOS (Mean Opinion Score) is 4.0
- Recommend LG / Ericson 8/24/48 port switches

VoIP Requirements for Remote Users

- Network Reliability – on the link in the customer's control 99.99%
- Layer 3 voice prioritization recommended
  - Layer 3: DiffServ:Enabled / ToS Type:DSCP / DSCP for Voice: 46
- 88kbps (G.711 audio) in each direction per simultaneous call

  Note: Media traffic may be Peer-to-Peer, depending on endpoint type and where the calling party and called party are located.
- Less than 80 ms latency recommended
- Jitter: 20mS or less (+/- 10mSec)
- Packet Loss: < 1%

VoIP Requirements for WiFi Users

- VoIP Products and Applications

  - PCs with Call Manager
- QoS
  - 802.11e/WMM recommended
  - Layer 3 DiffServ/DSCP/ToS 46
- Network Reliability: 99.99%
- 88kbps (G.711 audio) in each direction per simultaneous call
- 32kbps (G.729 audio) in each direction per simultaneous call

  Note: Media traffic is Peer-to-Peer, depending on endpoint type and where the calling party and called party are located.
- Less than 80 ms latency recommended
- Jitter: 20ms or less (+/- 10mSec)
- Packet Loss: < 1%
- Support for 802.11b,g,a & n

Router/Firewall

- Adtran Netvanta® router/firewall
- Cisco® ASA firewall

The router/firewall setup is critical to the successful deployment of voice services with QoS. To ensure successful deployment, Toshiba will support the above mentioned routers only.

WAN

The wide area network (WAN) data service is critical to the successful deployment of VIPedge service. Business quality services must be used.

- Business-class Cable service
- T1/E1 data service
- Metro Ethernet data service

Note: DSL services are not supported.

Chapter 3 – System Installation

Important! The customer server must be licensed before you make any program changes.

VIPedge SERVER SETUP

VIPedge server setup is done through the Dealer Portal. Some of the basic data base programming, such as Station and Voice Mail DNs, are already done.

1. Login to Enterprise Manager on the VIPedge server using your dealer User ID (email address) and Password.

System Summary Information

2. The System Summary information must be entered. The first screen shown after login is the System Summary. Click on the **Edit** icon. Enter the Enterprise Name and Address for this server. Enter the phone number and an email address. Click on the **OK** button.

LICENSE

Licenses are available through the VIPedge Dealer Portal. After the licenses have been purchased Toshiba will load and apply the licenses.

Display License Information

To display the items and quantities licensed on the server.

1. Login to the Enterprise Manager on the VIPedge server you want to check.
2. Select **Maintenance > Licensing > License Information**.
3. Select the server to display.

Note: The License Information may not be available to all Enterprise Manager Users.

E911 CUSTOMER SITE SETUP

When the DID numbers are assigned in the Dealer Administration portal it is critical that the physical address, the Emergency Response Location (ERL) of each telephone is also entered. When the system is brought online the first time the address of each station will be entered into the national E911 emergency dispatch database. The warning labels shipped with the telephones must be applied to each telephone. The text of the label is shown below.

WARNING! You may NOT be able to contact emergency personnel by dialing 9-1-1 from a telephone or from Call Manager. Use an alternate service, e.g., a mobile phone, to dial 9-1-1 if there is no dial tone; emergency personnel do not answer when you dial 9-1-1; or you reach the wrong emergency call center unless instructed otherwise.

E911 Customer Site Address Setup

Each VIPedge telephone set is identified by it's DID number. The physical address (ERL) of that DID number must have the address entered into the national E911 emergency dispatch database.

When a telephone, defined by the DID number, is moved to a new location, the new address must be entered into the national E911 emergency dispatch database as a new ERL.

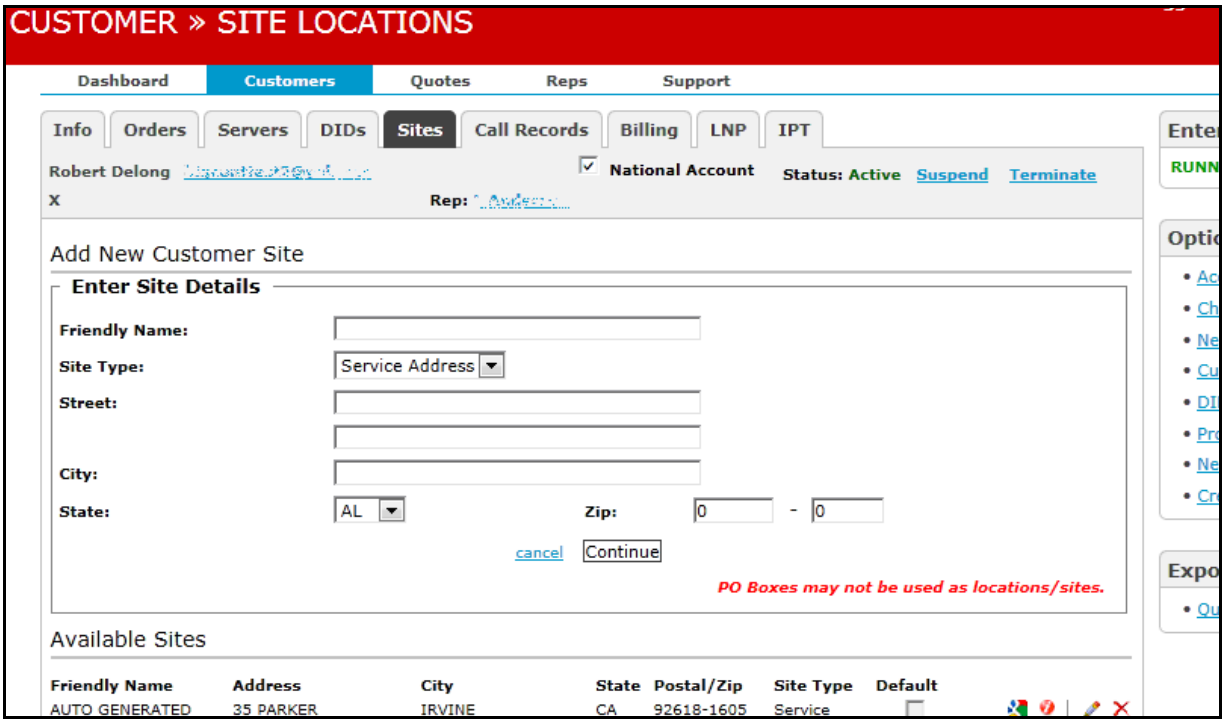
Important! Although their IP phones should be appropriately labeled to indicate that they are not to be used for 911 calls, dealers are still responsible for ensuring that address change notifications are handled promptly and accurately.

Site (Telephone Location) Assignment

The address of every telephone location must be programmed into the system. Select the customer then click on the **Sites** tab.

1. In the Sites tab click on **ADD NEW CUSTOMER SITE**.
2. Enter a name for the location, the street address, City, State, and zip code.

3. Select **Service Address** from the Site Type pull-down.
4. Click on **Continue**.
5. The system will attempt to verify that the address you entered could be vaild. If the address does not seem to be valid the system will prompt for corrections.
6. If the address seems valid you will be presented with one or more addresses. Click to select the correct address then click on **Submit**.

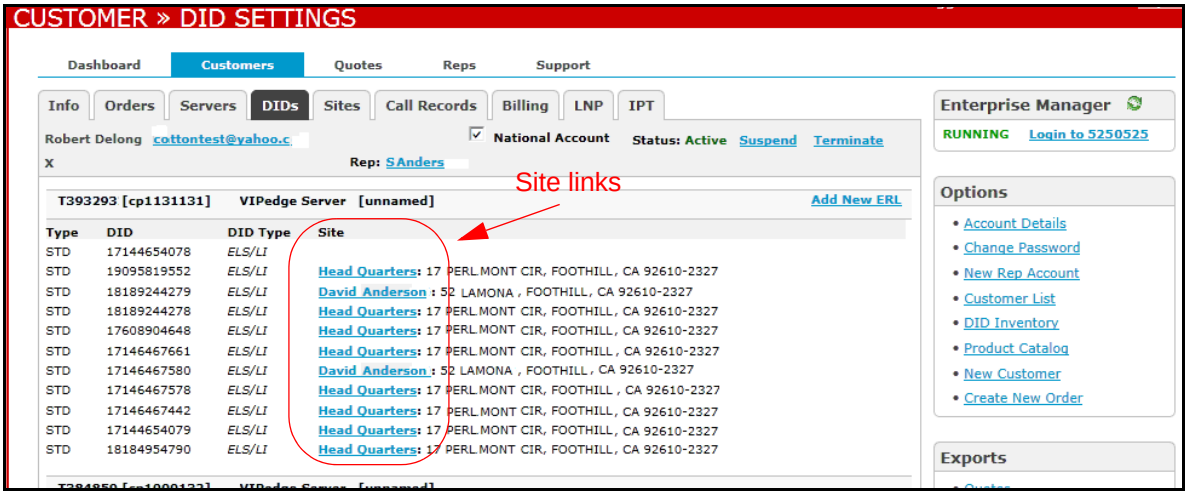


The Site setup can also be entered from the DID tab. Click on **Add New ERL**.

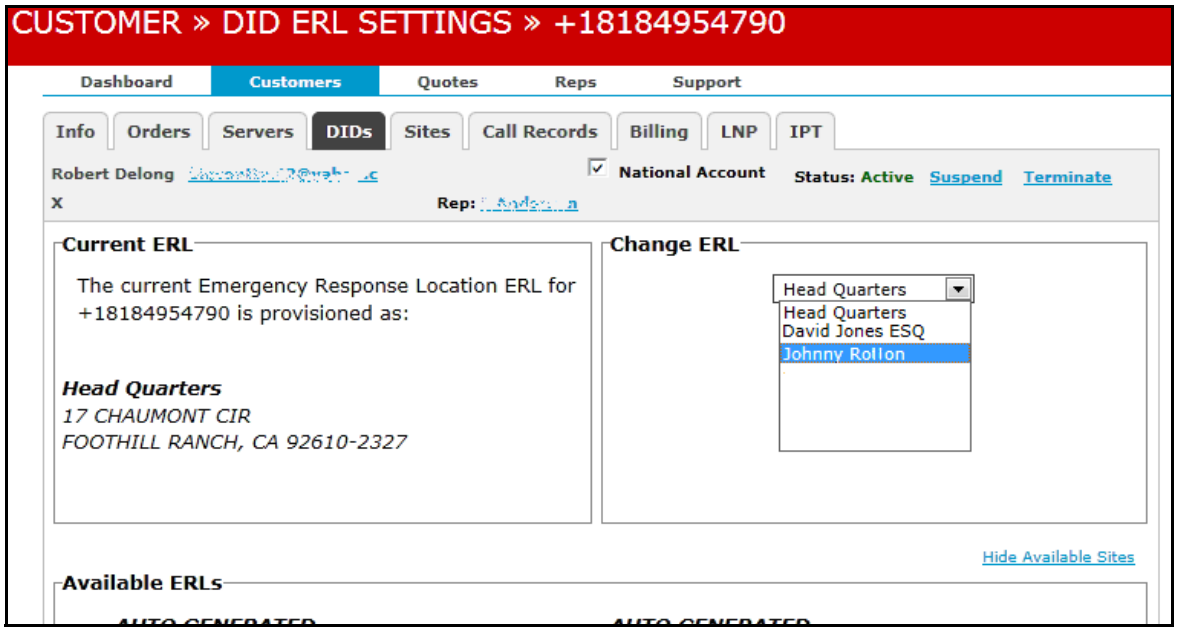
E911 Address Setup

When the DID numbers ordered (Servers > Order DIDs) the system requires an address to process the order. That address is the default ERL address for all of the DIDs ordered. To change the ERL of a DID number go to the Customers DIDs tab (refer to the figure below). Click on the link next to the DID number.

1. To assign an ERL address to a DID number select the **DID** tab. Then click on the 'site' link for the DID number.



2. The display will change to show the current ERL assignment.



3. To change the address select the new address form the pull-down menu in the **Change ERL** section.
4. Click on **Update**.
5. Wait several seconds while the system changes the ERL address in the system database and sends the notice to the national dispatch database.

Chapter 4 – Station Install

VIPedge STATION INSTALL

This chapter covers the IP Telephone installation steps. Additional detailed information is available in the IPedge/VIPedge IP Telephone Installation manual.

1. The client's VIPedge container must be setup. Refer to the previous chapters of this manual.
2. The dealer then enters the Serial Numbers of the IP5000 series telephone into the container.
3. Program the IPT stations into the customers database.
4. Install the stations at the customer site.

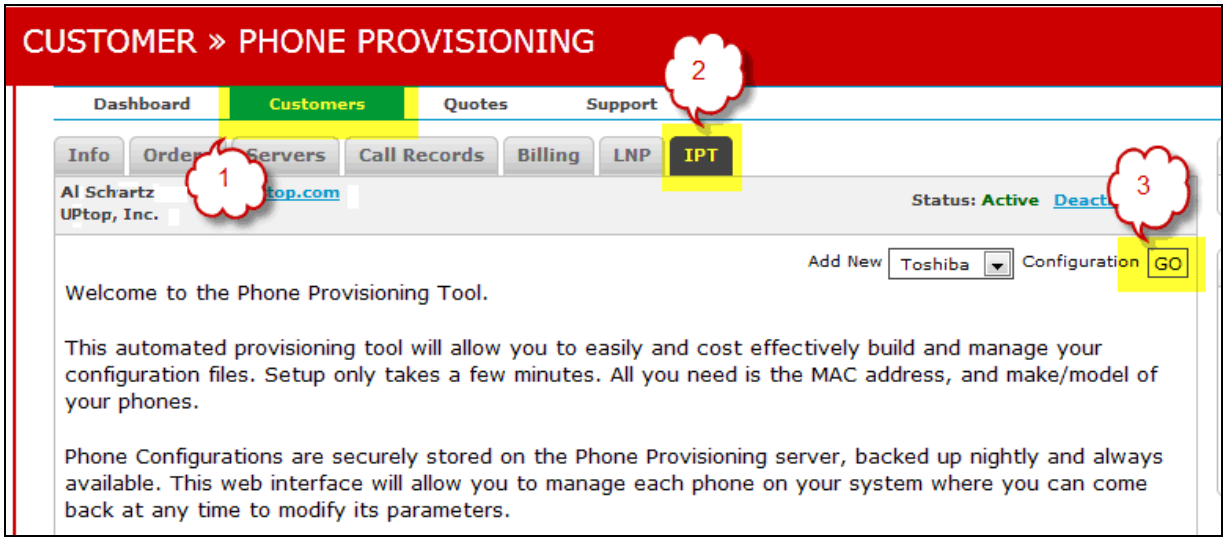
ADD / REMOVE IPT SERIAL NUMBERS

The portal is built to accommodate the addition or deletion of IPT's. This function is the process that used in the warranty replacement of a phone.

Add IPT Serial Number

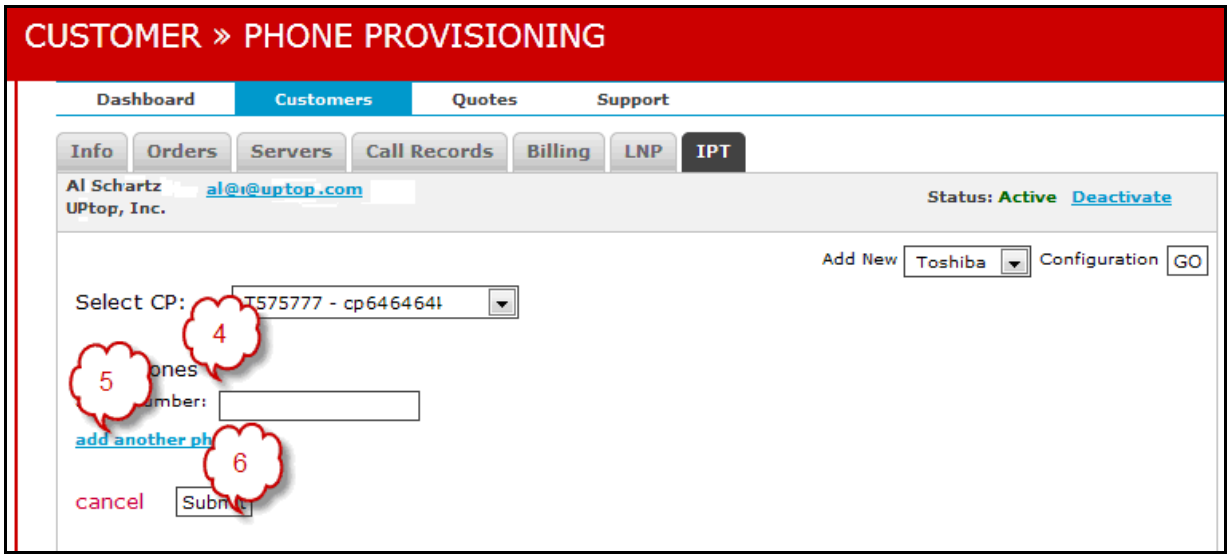
Use these steps to add and delete IPT serial numbers to/from the portal.

1. Login and select your customer.
2. Select the IPT Tab.
3. Click on **GO**.



4. Enter the IPT serial number.
5. Click **add another phone** and add the next serial number, repeat for all that you want to add.

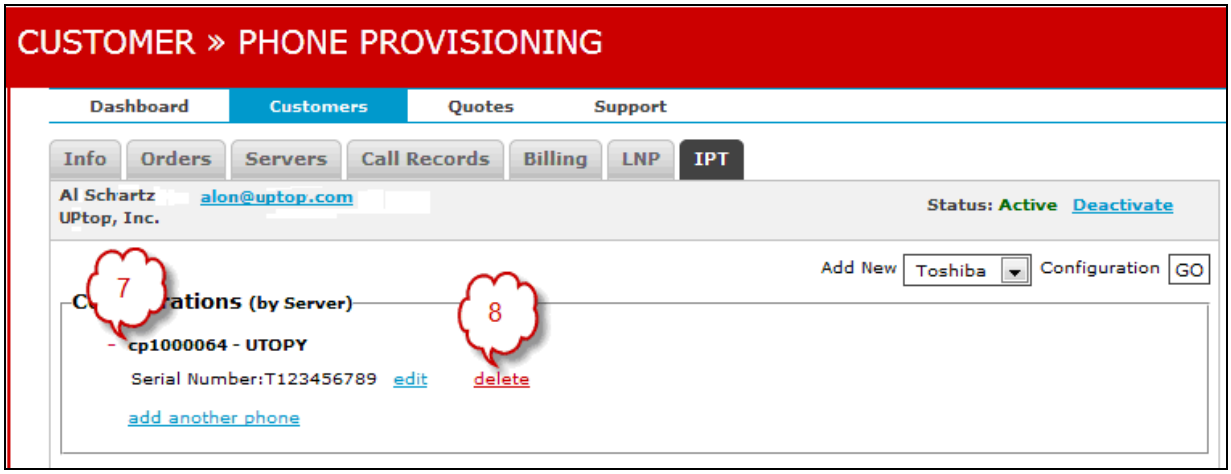
6. Click Submit.



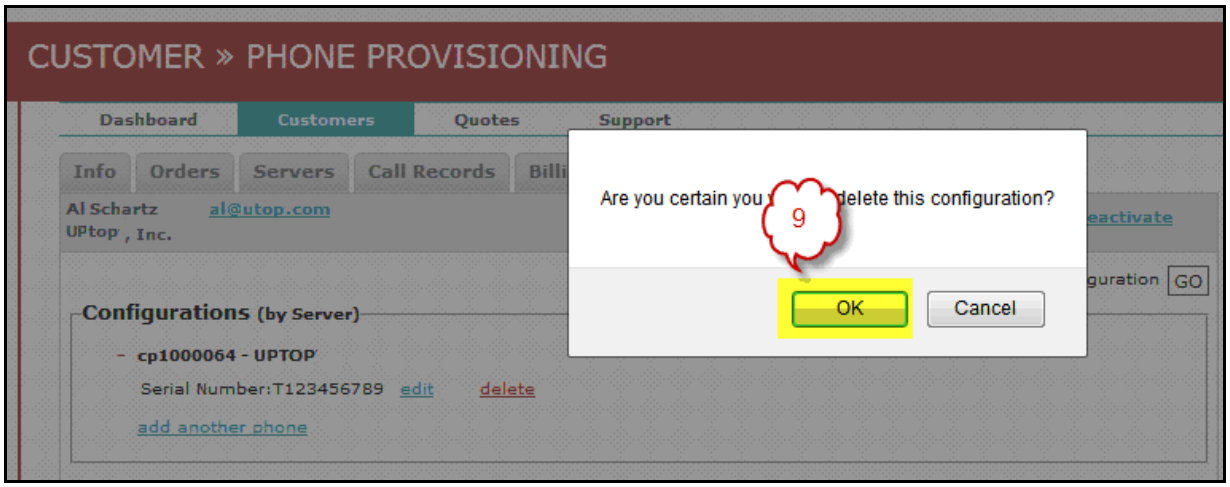
Delete IPT Serial Number

When you need to delete a serial number:

1. Click on the customer's number
   (in this example: + cp6464064 – UPTOPY).
2. Find the serial number to be deleted and click on **delete**.



9. Click on **OK** to delete the serial number.



STATION PREPARATION

The IP Telephones (IPT) must have software level M2P2 or later. If the telephone is already software level M2P2 or later go to Client Site Install. If the telephone is not software level M2P2 or later go to Station Software Update.

Client Site Install

The LAN must have POE or a local power supply is required for each IPT. Do not use both.

Note: A DHCP server must be deployed in the customer network in order for IPT phones to obtain their IP address and public DNS server address.

Plug the IPT into the client's LAN. The IPT will boot up.

1. After the IPT connects to the VIPedge service a prompt to enter the Directory Number will appear.
2. Enter the DN then, press the **Enter** soft key.
3. If prompted enter the Password then, press the **Enter** soft key.

The telephone is ready for use.

Station Software Update

The IPTs must have software level M2P2 or later. If the telephone is running earlier software refer to the IPedge Install manual for the IPT software update procedure.

Client Site

When the telephone has been updated, plug the IPT into the client's LAN. The LAN must have POE or a local power supply is required for each IPT. Note: Do not use both. The IPT will reboot.

After the reboot a message will appear on the screen about entering the URL. Use the following procedure to configure the telephone.

1. Simultaneously press 3 + 6+ 9 + Hold keys.
2. Press the **Initialize** soft key.
3. Press the **All Data** soft key.
4. Press the **Exec** soft key.
5. Press the **Exec** soft key again.
6. After the IPT connects to the VIPedge service a prompt to enter the Directory Number will appear.
7. Enter the DN then, press the **Enter** soft key.

The telephone is ready for use.

IPT POWER REQUIREMENTS

The table below shows the power consumption of the IPTs. This table can be used to estimate PoE power requirements and UPS backup time.

Table 4-1 IP Telephone and Add-On Module Power Consumption

Telephone Model	Option		Power Rating (Watts)	Current (A) [1]	Typical (Watts) [2]	Typical Current (A) [3]	IEEE802.3af PD Class
	Model	Qty					
IP5131-SDL	none	--	7.4	0.15	6.2	0.13	0
IP5531-SDL	none	--	3.6	0.08	3.0	0.06	2
IP5631-SDL	none	--	4.1	0.08	3.3	0.07	2
IP5131-SDL	LM5110	2	10.3	0.21	8.6	0.18	0
IP5131-SDL	LM5110	1	9.4	0.20	7.8	0.16	0
IP5631-SDL	LM5110	2	6.4	0.13	5.3	0.11	2
IP5631-SDL	LM5110	1	5.6	0.12	4.7	0.10	2

1. Power ratings are only telephone and option modules consumption. The values do not include LAN cable power loss, and apply to PoE, not local power supplies.
2. Typical means that it is only an example and there is no guarantee implied. The "typical" value might be used for a calculation of actual UPS backup time in an average installation
3. Typical Current (A) = Typical Watts / 48 v

STATION PROGRAMMING

For detailed station installation and programming procedures Refer to the IPedge / VIPedge IP Telephone Installation manual available on Toshiba's FYI web site.

Chapter 5 – SIP Trunk Configuration

VIPedge SIP TRUNK OVERVIEW

The client's VIPedge container must be setup.

1. Login to your dealer portal. Select the customers tab.
2. Order new DID numbers, complete request to port existing DID number or, both.

The total number of DID numbers cannot be greater than the number of users.

TRUNKS

1. Login to the Dealer Portal.
2. Select **Customers**.
3. Click on customer name in the lis1t.
4. Click on the **Servers** tab.

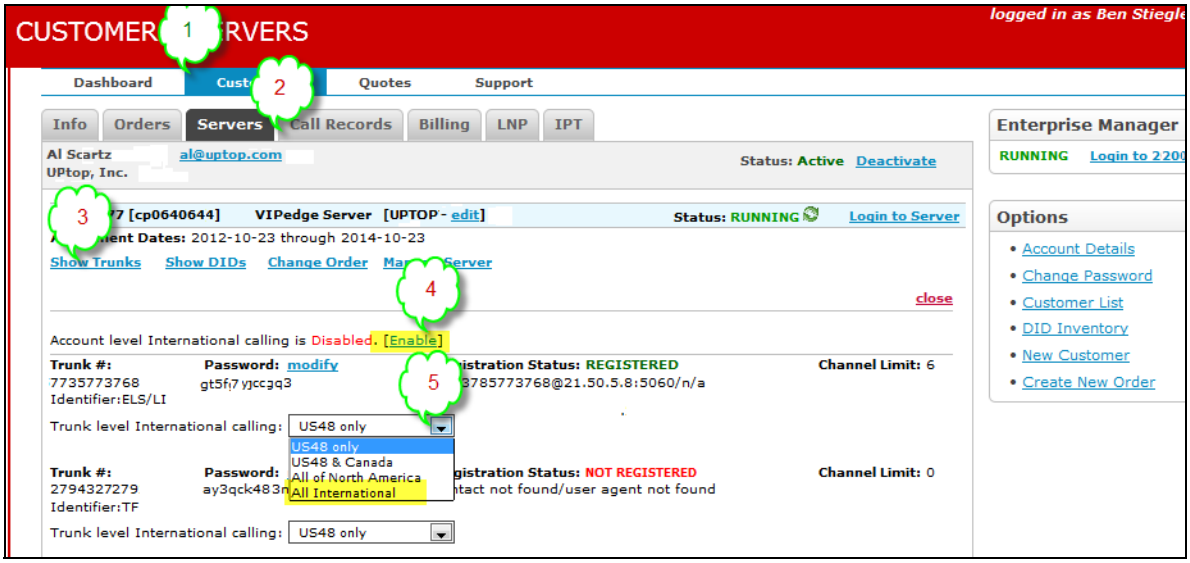
5. Click on:
   Show Trunks - Displays the number of each type trunk and the international calling level allowed.
   Show DIDs - Display a complete list of DID numbers (used and unused).

INTERNATIONAL DIALING

All VIPedge systems have international calling disabled by default. Use the following procedure to enable international dialing.

1. Login to the container administration and select your customer.
2. Select the **Servers** tab.
3. Click on the **Show Trunks** link.

4. The **Account Level International calling** will be set to Disable. Click on **Enable**.



5. Use the pull-down menu in the **Trunk level International Calling** line. Set the appropriate level for your customer.

Trunk Level	48 Contiguous States	Alaska & Hawaii	Canada	Mexico	All Other Countries
US 48 Only	Yes	Yes	No	No	No
US48 & Canada	Yes	Yes	Yes	No	No
All of North America	Yes	Yes	Yes	Yes	No
All International	Yes	Yes	Yes	Yes	Yes

Use the VIPedge Destination Restriction feature to limit calling areas if needed. The changes will take effect immediately.

ORDER NEW DID NUMBERS

This procedure is for ordering new DID numbers. For porting existing DID numbers to this system refer to “E911 Customer Site Address Setup” on page Chapter 2 –-2.

1. Login to your dealer account and select the customer server.
2. Click on the **Servers** tab.
3. Click on the **Order DIDs** link.
4. Verify that the address shown is the physical location of the stations that will use the DID numbers you are about to order. This address is the ERL that will be will be sent to the Public Safety Answering Point (PSAP) when one of these stations dials 911.

Note: To change the address for a DID number refer to “E911 CUSTOMER SITE SETUP” on Page 2

5. Select the Area Code.

6. Click on **Select Numbers**.
7. The available DID numbers will be displayed. Check mark the DID number you want to order.

Note: The quantity of DID numbers cannot exceed the number of trunk user licenses on this system.

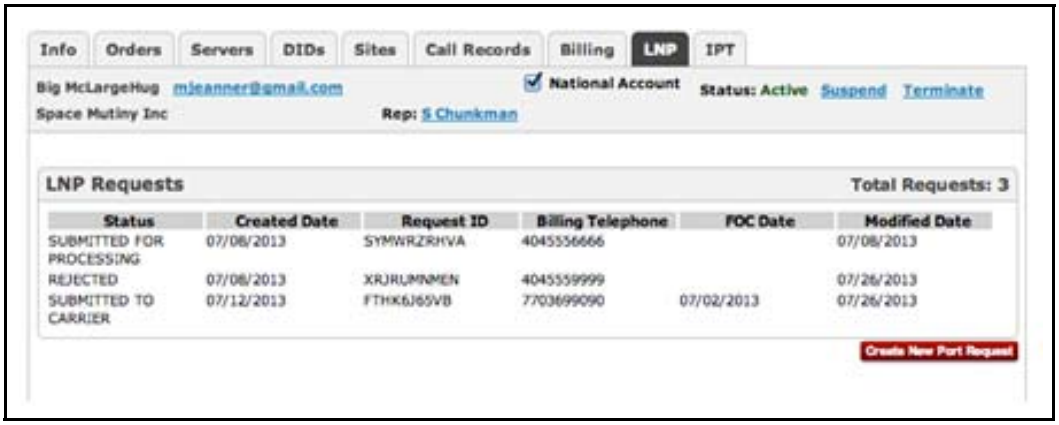
8. Click on **Order Selected DIDs**.

PORTING EXISTING DID NUMBERS

VIPedge R1.4.3 and later systems have three enhancements to Local Number Porting (LNP); a Summary, a Detailed View, and a Dashboard.

Summary

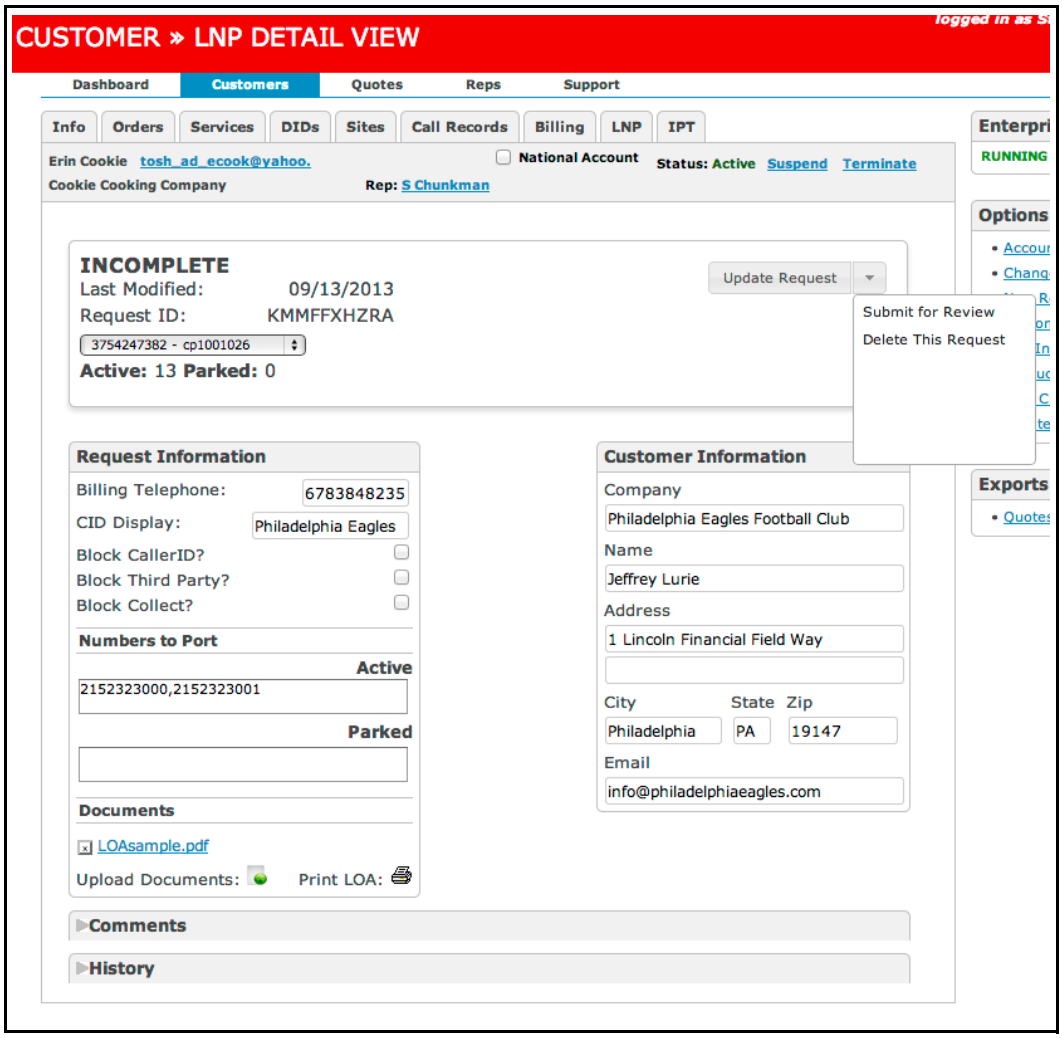
Dealers will be able to view the a summary of their port requests.



Detailed view and Upload LOA for LNP

The new Detailed View includes Comments, History, and the ability to upload the Letter of Authorization (LOA) agreement directly. Also,

improve the reliability of the Firm Order Commit (FOC) date, the it can be set after the LOA has been uploaded.



Local Number Porting Procedure

This procedure is for porting existing DID numbers to this system.

Important! Local Number Portability will take up to three calendar weeks (7 to 21 days).

1. Login to the customer account.
2. Click on the **Servers** tab.
3. Click on the **LNP** link.
4. Click on **Update Request** to save this information.
5. Click on **Print LOA** to display the LOA document.
6. Print then sign the LOA.
7. Scan the document.
8. Click on the **Upload Documents** link.

9. Click on the pull-down arrow next to the **Update Request** and select **Submit** to order the number porting.

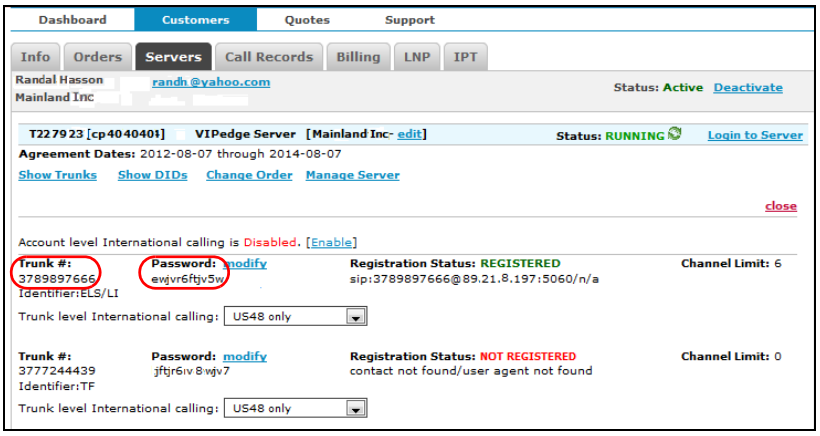
Note: If you are porting only a 'Main published' number or Toll-free number program the VIPedge database to send those calls to an Auto Attendant.

Important! Make a list of the DID numbers ordered for this customer.

Display Trunks

Use this procedure to display the trunks and DID information programmed on a system.

1. Login to the customer account.
2. Click on the **Servers** tab.
3. Click on the **Show Trunks** link.

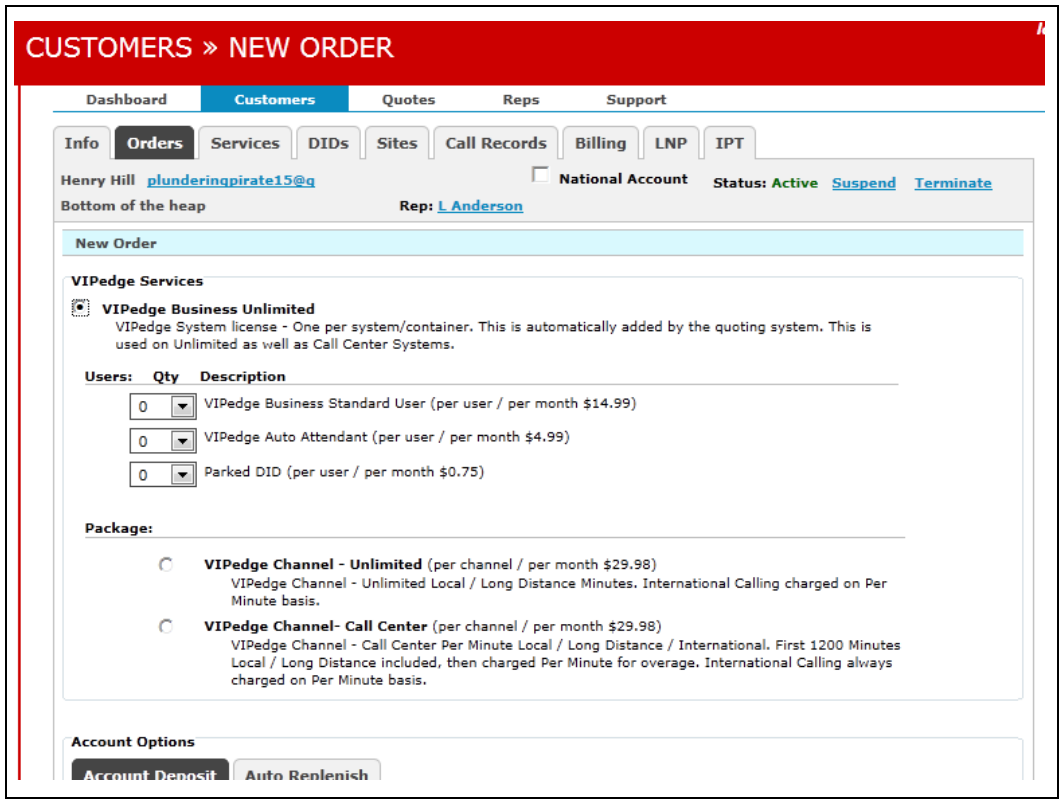


4. Make note of the 10-digit Trunk number and the Password for use while programming the SIP Trunks. The trunk number is not a telephone number is a circuit identification number.

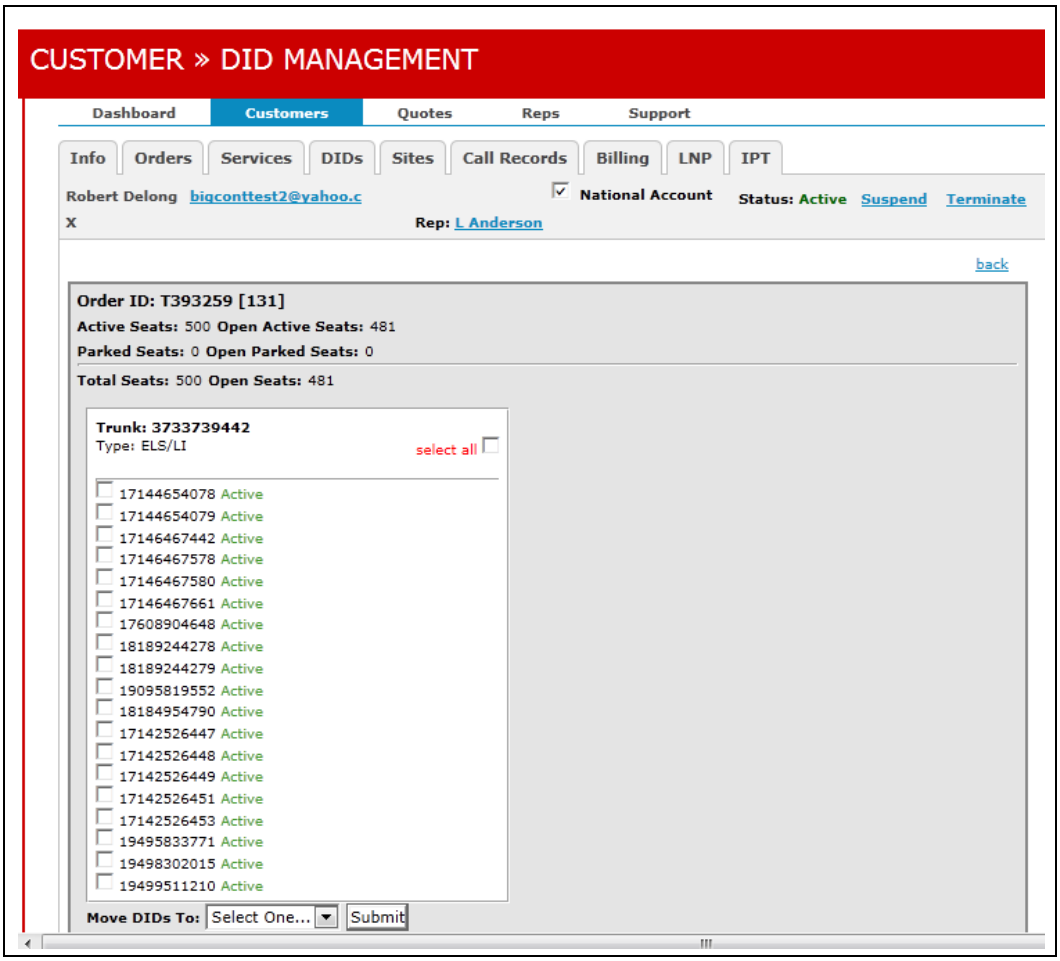
DID PARKING

Customers may have blocks of numbers that they want to move over to the VIPedge system but, not put all of the numbers in service. Customers may want to purchase DID numbers for future use. The DID parking line item on the ordering portal is for the numbers that will not be used immediately. This allows a number of DID numbers to be parked and then used later. There is a minimal fee for DID parking (VIPedge DID Parking fee, P/N V-BIZ-DIDPK, ais a monthly recurring charge.). Porting charges still apply. Calls to parked numbers will be answered with a "not in

service" message. Parked Numbers can be Quoted and Ordered in the ordering portal as shown below.



Numbers can be parked after they are ported in the DID management tab.

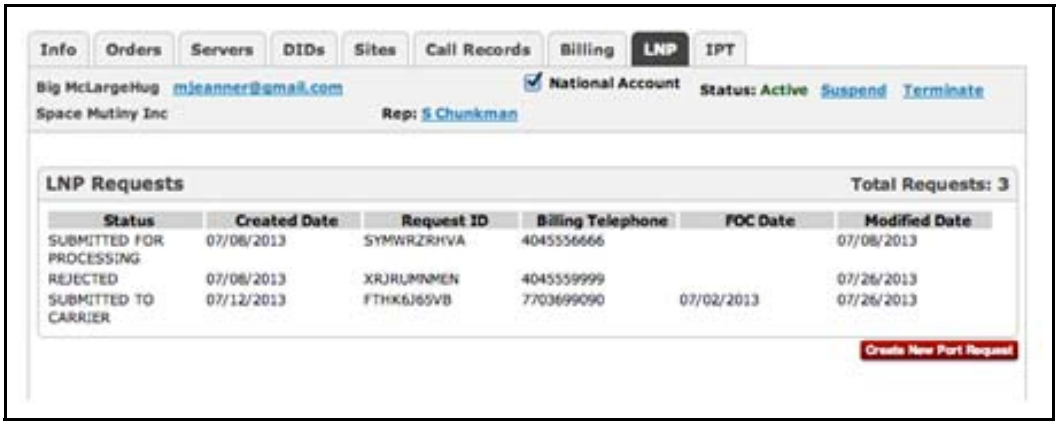


LOCAL NUMBER PORTING

There are three enhancements to Local Number Porting (LNP) in release 1.4.3 and later systems; a Summary, a Detailed View, and an Expedite Capability. There are also several behind the scenes improvements to workflows, alerting, and comments.

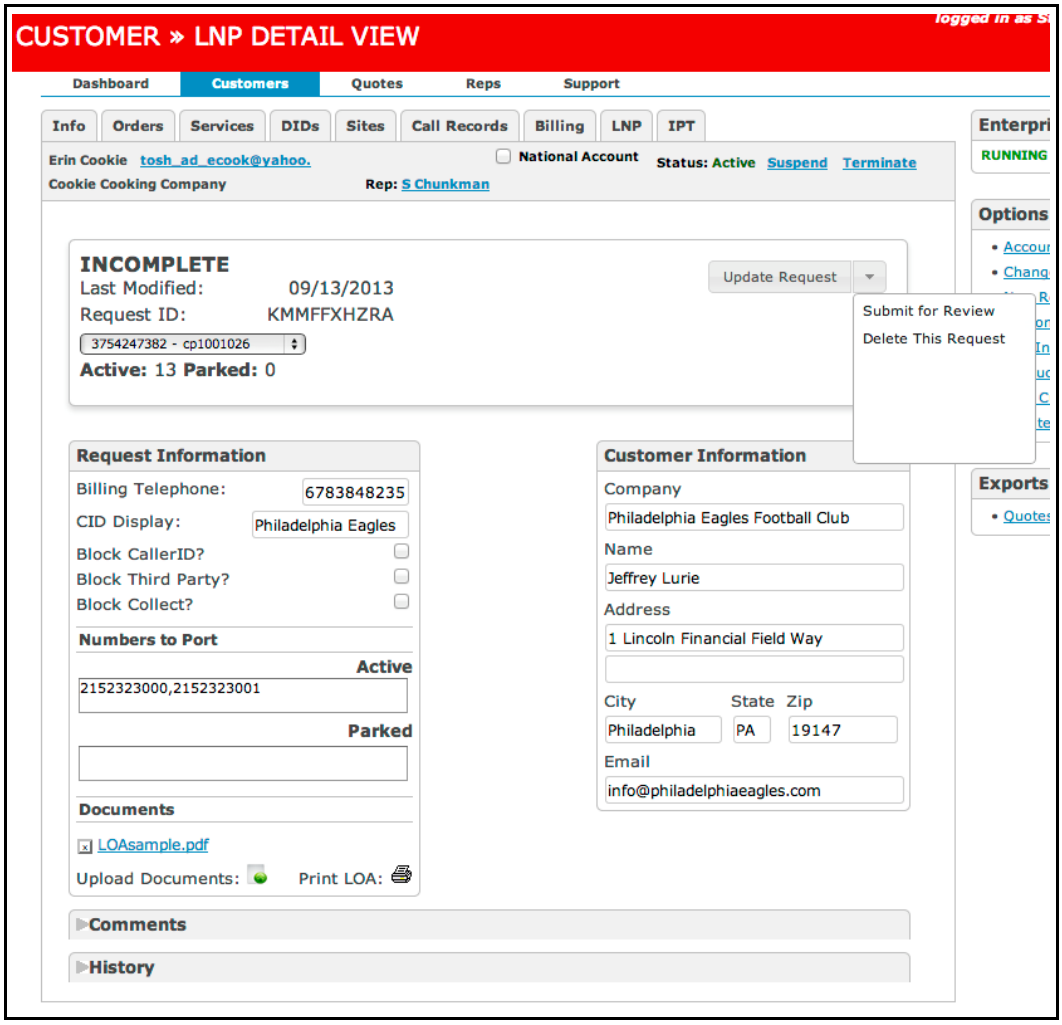
Summary

Dealers will be able to view the a summary of their port requests.



Detailed View and Upload LOA for LNP

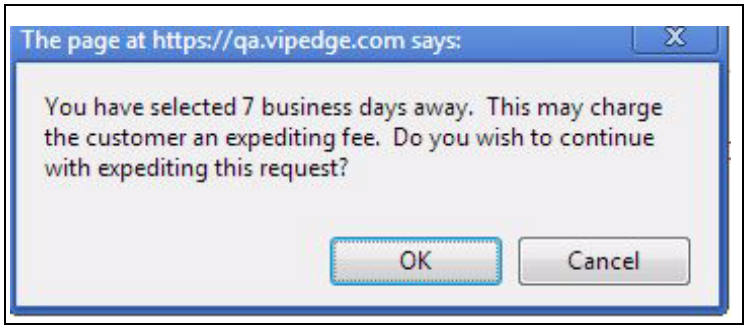
The new Detailed View includes Comments, History, and the ability to upload the Letter of Authorization (LOA) agreement directly. Also, to improve the reliability of the Firm Order Commit (FOC) date, it can be set after the LOA has been uploaded.



Expedite

After the LOA document has been uploaded, you will be able to set the FOC (Firm Order Commit) date. The general requirement is that this date must be at least 11 business days in the future, in order to allow time for processing by the losing carrier. We have created an expedite process where earlier FOC dates can be requested. If an earlier date is requested,

and after investigation it is possible to meet that date, there will be a $100 fee per DID number.

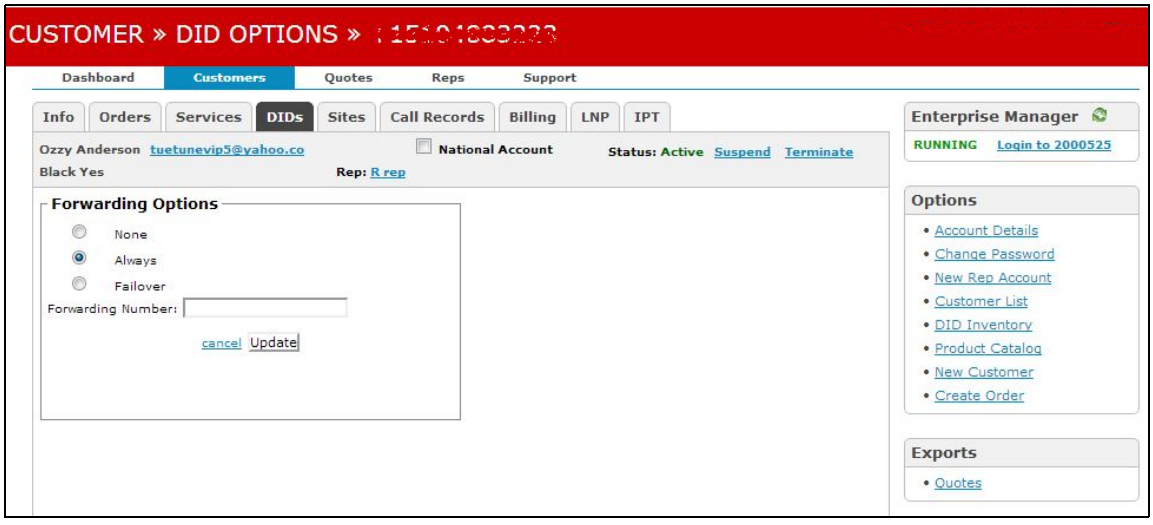


DID FORWARDING

DID Forwarding is a feature that allows incoming DID calls on a VIPedge trunk to be forwarded to another number. This feature can be used, for example, to forward a person's calls to his cell phone. DID forwarding is available on R1.4.3 and later VIPedge trunks.

If the 'Always Forward' box is checked, all calls will be forwarded to the Forwarding Number.

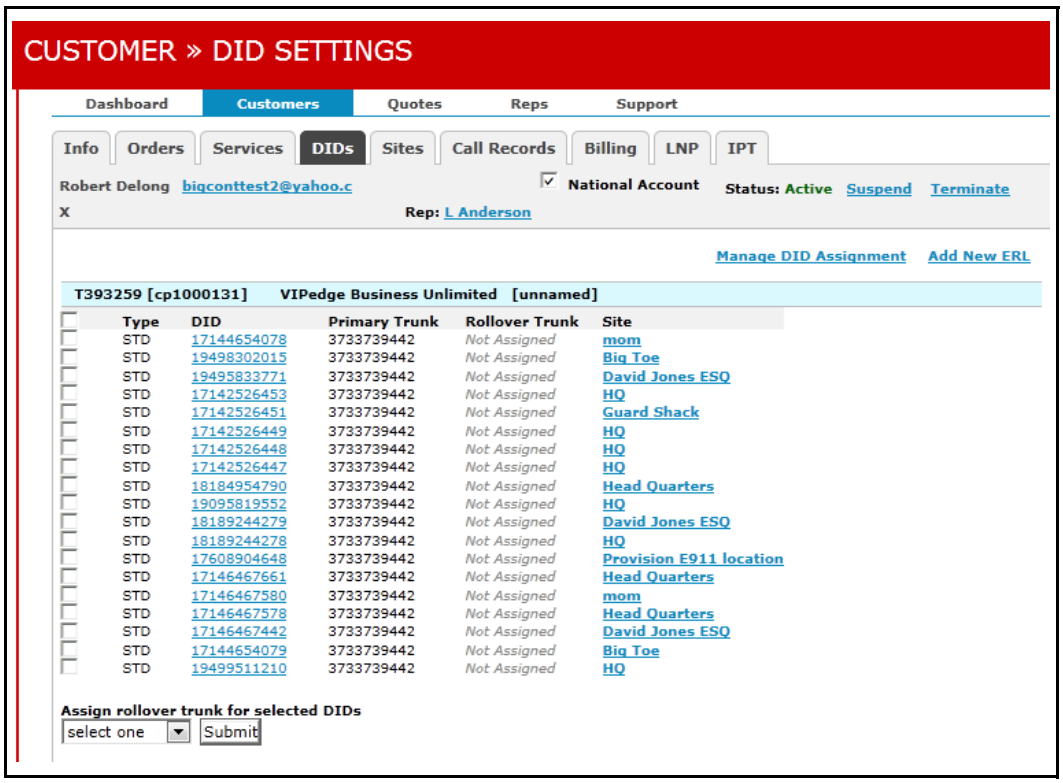
If the 'Failover' box is checked calls will be forwarded to the forwarding number when there is a failure. Examples are; the SIP trunk is not registered or, when there is a WAN failure.



ROLL OVER TRUNKS

DID calls can be configured to roll over to a second trunk on R1.4.3 and later systems. In the DID screen, select the desired DIDs then, select the

trunk the call will roll over to from the drop-down list. The rollover trunk can be any other trunk belonging to that customer.



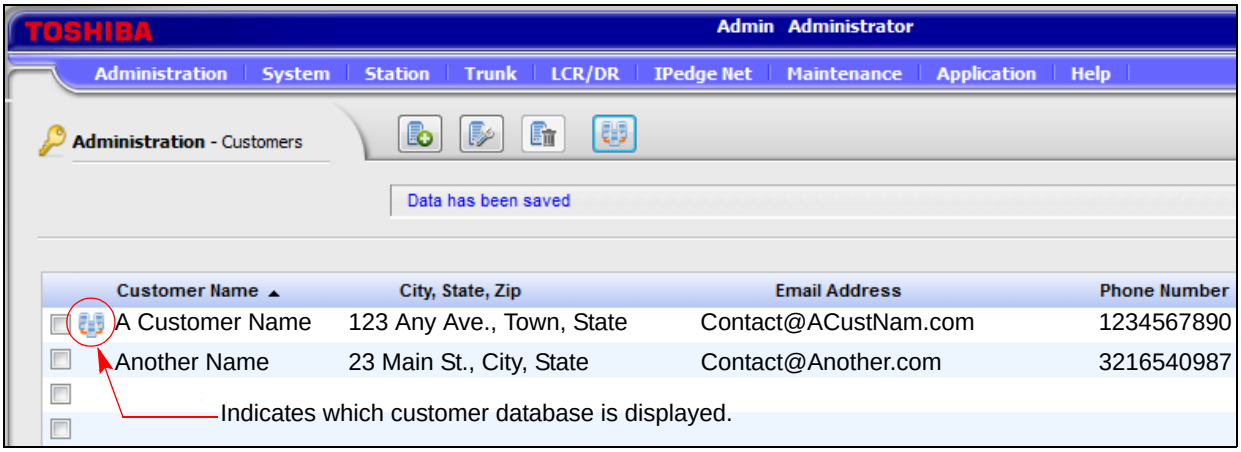
VIPedge DID TRUNK CONFIGURATION

The process of configuring DID numbers and DID trunks is more efficient if done in the following order.

- The Trunk Group ILG and OLG are pre configured
- Configure the DIDs. (Trunk > DIDs)
- Use the Create URI Range function in Trunks > SIP Trunking, the Service URI tab to create URIs for all of the DID station numbers.

Enterprise Manager Login

Login to your VIPedge Administration portal. Select the customer database to configure.



SIP Trunking

In Enterprise Manager select **Trunk > SIP Trunking**.

When the VIPedge container for a new customer is configured the ILG and OLG is created in the database.

In the database, the Service Definition for each trunk is SD1 (Standard).

DID Dialing Destination

Define where the DID numbers will ring.

1. In Enterprise Manager select **Trunk > DID**.
2. Click on the **New** icon.
3. Enter a DID number.
4. In the DID Audio; Audio Day 1, Audio Day 2, Audio Night fields define the Station Number it will ring to.
5. Repeat for every DID number.

SIP URI SETUP

SIP URI Number for each trunk type is configured as follows:

- The Attribution of SIP URI Number 1 is always **MAIN**.
- The SIP URI and the SIP User Name is the same as the Trunk number shown in the VIPedge container (refer to Display Trunks on page 5-5).
- The Password is the same as the password show in the Display Trunks admin screen.

All of the other SIP URI Numbers for that trunk type are configured as follows:

- The SIP URI is **1 + the 10-digit** DID number.

- The SIP User Name and SIP URI Password are the same as SIP URI Number 1.
- The SIP URI Attribution for all SIP URI Numbers (except 1) is **SUB**. Refer to and 5-1

Important! The User Name and Password must be assigned to every SIP URI Number.

SIP URI Tab

Enter the DID numbers as SIP URIs.

1. In Enterprise Manager select **Trunk > SIP Trunking**.
2. Select the URI Tab.
3. Select the Service Definition Index for the trunk your are configuring.
4. Click on the **New** icon.

   – OR –

   Click on the **Create URI range** icon to use the wizard to create URIs from the DID numbers.
5. Repeat for all SDIs.

Note: In the **Add At Front of DID Numbers** field enter the 1+ AC + OC.

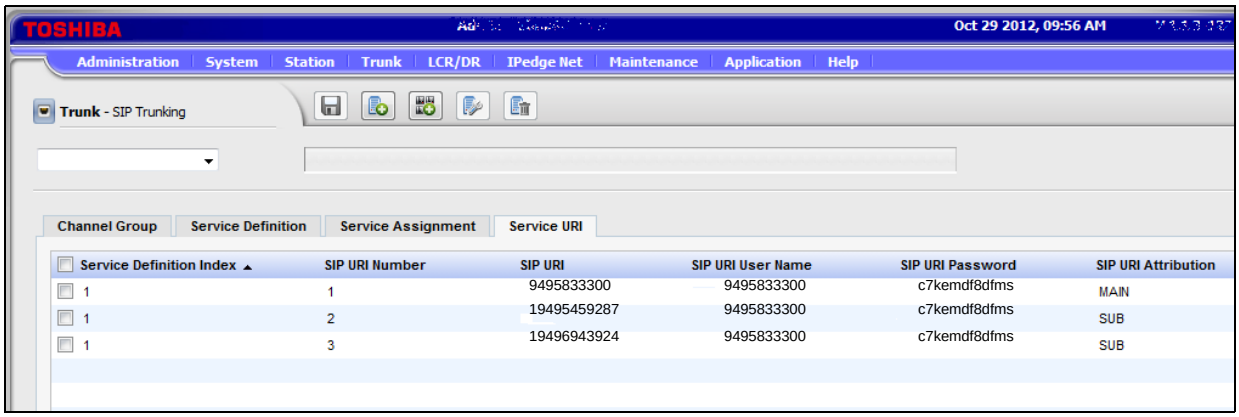


Figure 5-1 SIP Trunk Service URI Assignments

Adding Channels

When adding channels to an existing system add the capacity using the Container Admin then, change the VIPedge database using Enterprise Manager.

In Enterprise Manager select **Trunk > SIP Trunking**. Select the Channel Group tab. Change the number of SIP Trunk Channels. This step must done before any more trunk configuration is tried.

Chapter 6 – Enterprise Manager

Enterprise Manager is a web browser based application that resides on the VIPedge server.

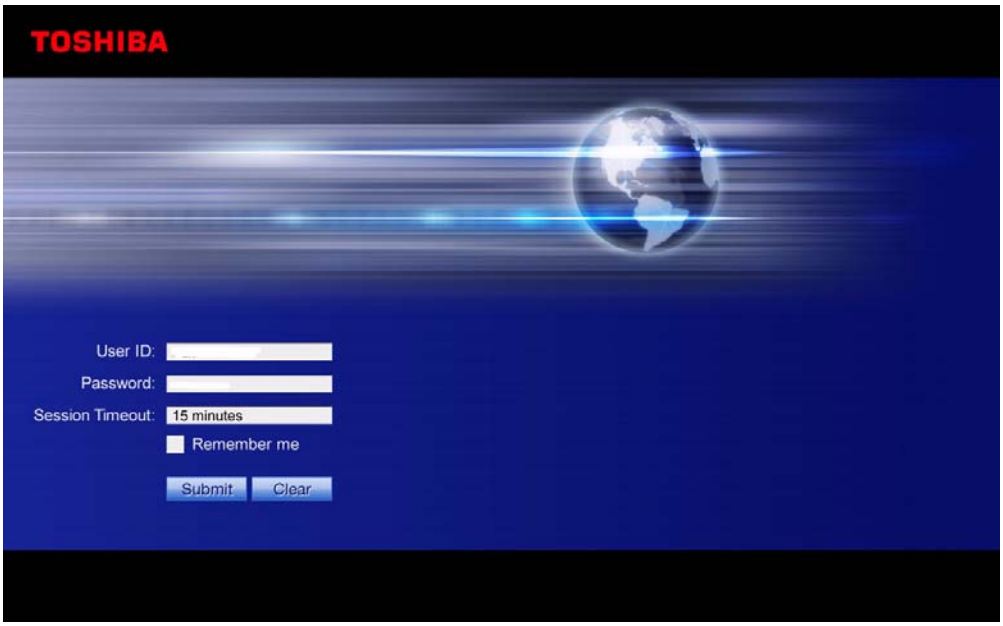
The Administration Terminal is a PC connected to the network, no special software is required.

SUPPORTED BROWSERS

The Enterprise Manager can be accessed using Microsoft™ Internet Explorer version 7 or later.

LOGIN

Login to your Dealer Portal to access your customer container or enter your customer's admin address (EMPA address) in the address bar of your browser. For Admin access use your dealer email address and password. The dealer email address is the address on record when the VIPedge account was set up.



ROLES

The VIPedge system has System Administrator (technician) roles and two Enterprise Manager Personal Administrators (EMPA) telephone user roles.

EMPA

System Administrators have access to the system configuration database. EMPA users can access only selected items of their telephone configuration.

The EMPA roles for your customers are;

- EMPA Normal Users have access only to their own telephone configuration.
- EMPA Super Users can administer their own telephone and the telephones of users assigned to them.

System Administrator

Dealers can create Customer Group Administrator (Limited CP Access) users for technicians with a list of specific CPs assigned to each admin user. When one of these Users is logged in they are only able to display and access the CPs in the list assigned to this admin user.

This supports existing dealer technician assignments where the responsibilities of some technicians are divided to cover specific geographical areas. Each technician can be limited to the CPs that are within their covered area and are denied access and visibility to CPs outside of their area.

Dealers can also create System Administrator users for technicians with access to all of the dealer's CPs. When one of these Users is logged in they are only able to display and access the CPs in the list assigned to this admin user.

Each role is defined as a list of permission items (access rights) that determine the user's access level in Enterprise Manager.

USERS

As each **Station** is configured it is assigned, among other things, a DN and a Telephone User role.

Administration User

To add an administration user:

1. Login to Enterprise Manager.
2. Select **Administration > Users** a list of users will display.
3. Click on the **New** user icon and select the **Personal Administration Role Group** then click on OK.
4. Enter the following parameters. Unless otherwise noted the entries are required.

   Login Name - The screen name of the user.

   First Name - The user's first name

   Middle Name - Optional, this field does not require an entry.

   Last Name - The user's last name

   Role Name - Select the name of the role that defines the permissions for this user.

VIPedge CUSTOMER GROUP ADMINISTRATION (Limited CP Access)

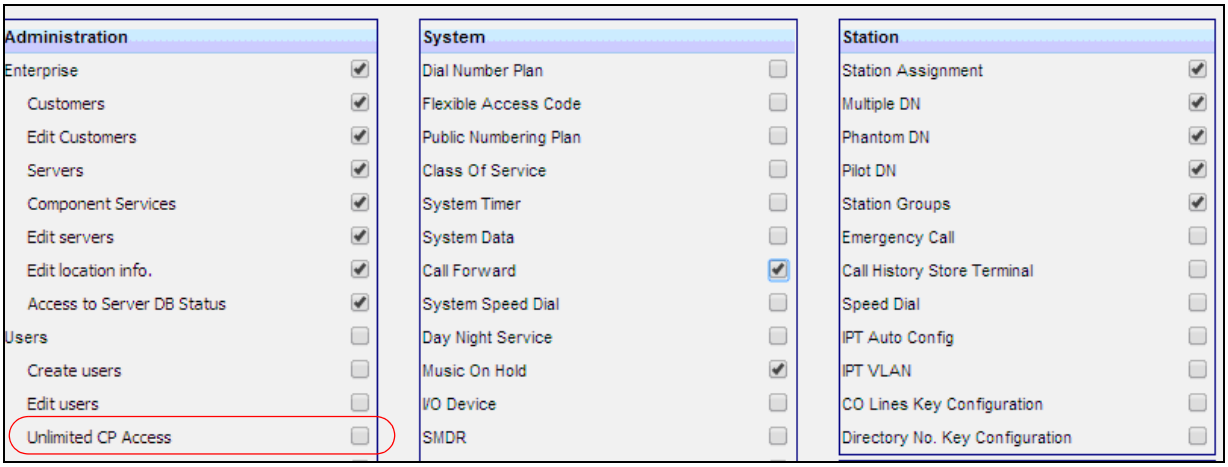
Dealers can create Enterprise Manager for users (technicians) with a list of specific CPs list assigned to each user. When one of these Users is logged in they are only able to display and access the CPs in the list assigned to this admin user.

This supports existing dealer technician assignments where the responsibilities of some technicians are divided to cover specific geographical areas. Each technician can be limited to the CPs that are within their covered area and are denied access and visibility to CPs outside of their area.

Limited CP Access Permission

In Release 1.4.5 a permission item in the Roles Permission table, the Limited CP Access was added. Enterprise Manager shows the “Limited CP Access” permission in the Enterprise section on the Edit Role page.

Select **Administration > Roles**. To create a Role with a defined group ensure that the Unlimited CP Access box is NOT checked. The figure below is from the default Limited CP Role already in the system.

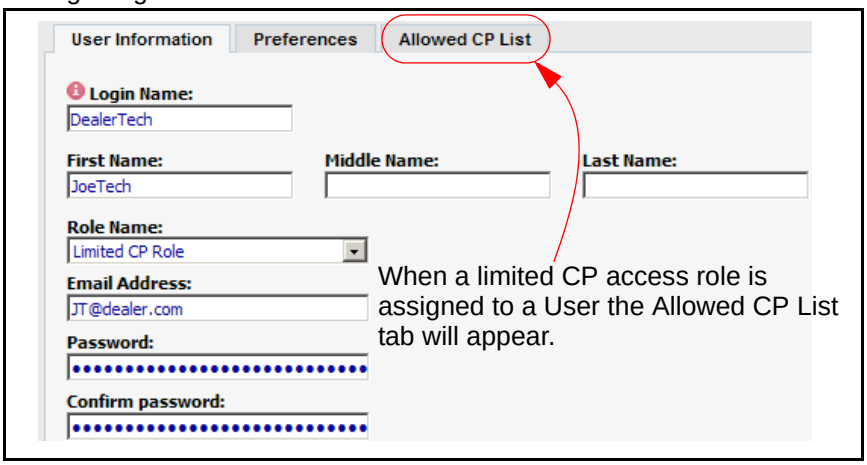


If the “Unlimited CP Access” permission is ON (checked) in a role, there is no limitation, users assigned that role have access to all CP containers as in earlier versions. Unlimited CP Access permission set to ON is the default. To limit CP access, a role must be created with the “Unlimited CP Access” permission OFF (not check marked). And a “Permitted CP List” for this user is then created.

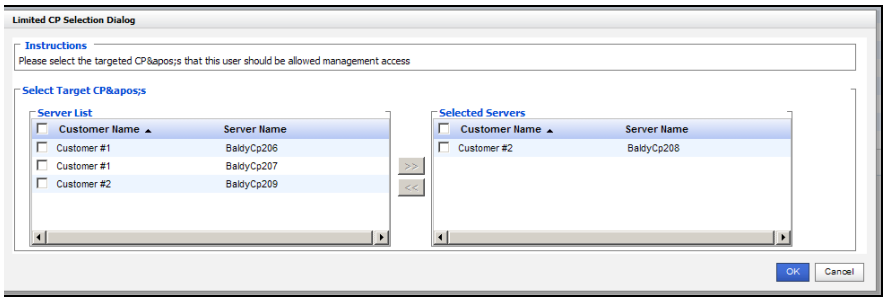
Limited CP User

When a role has the “Limited CP Access” permission is set to ON the role and user management permissions for that role are automatically turned OFF. This prevents a user with a limited CP access role from managing

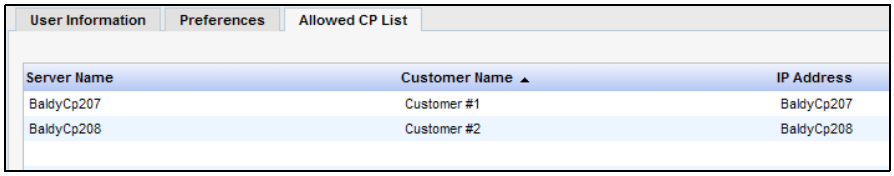
roles and other users which would allow this user to create a Enterprise Manager login with less or no limitation.



Each admin user has its own Permitted CP List or no Permitted CP list at all depending on their assigned role. If the user has a Limited CP Access but the Permitted CP List is empty the user will not be able to login.



When all of the allowed CPs are moved to the right hand side click on **OK**



Users with Limited CP Access will not see all of the CPs.

When Webmin is launched by a Limited CP user only the user's Permitted CP List can be accessed.

Limited CP User Login

Limited CP Access Admin users can login to GeM in two ways:

- With a URL that does not include a targeted CP FQDN argument
- With a URL that includes a targeted CP FQDN

When a URL does not include a CP FQDN, such as http://VIPedge.com, the user will have to select a customer from the list of customers to which that user has access.

When the URL has the targeted CP FQDN the user will go directly to that customer, so the logged in user can immediately proceed to configuration pages. If the CP FQDN from the login URL cannot be found in the system, the login be the same as no CP FQDN.

When using any URL, if the “Limited CP Access” admin user has a Permitted CP List is empty, Enterprise Manager will deny the login.

When a change is made to a Role, the change takes effect the next time a user logs in.

Note: If the admin user has permission to access only a subset of CPs within a Customer, the IPedge Net setup for the customer will also be limited to include only the permitted CPs. To be able to configure a full IPedge Net setup for a specific Customer, the admin user should have access to all CPs of that Customer.

This page is intentionally left blank.

Chapter 7 – VIPedge Webmin

VIPedge Webmin is a graphical user interface used to simplify Linux operating system management. VIPedge Webmin lets you perform these tasks through a web interface, and automatically updates all of the required configuration files.

VIPedge Webmin is accessed through Enterprise Manager, select **Application > VIPedge Webmin**. The VIPedge Webmin application on all of the customer servers are accessed through Enterprise Manager.

Although VIPedge Webmin is accessed through Enterprise Manager it is not part of Enterprise Manager.

VIPedge Webmin is used to:

- Monitor System and Server Status
- Upload and download custom MOH Files or reset MOH to factory defaults
- Access the Backup and Restore functions in Bacula

MUSIC ON HOLD

The system has a total of fifteen music sources and Quiet Tone on the Media server for Music On Hold (MOH). The administrator selects from these 15 internal WAV files, and quiet tone. Administrators can upload their own WAV files to the system.

This feature provides music or tone to a station or line that is held by a station with Line Hold or Consultation Hold and the speech path is released.

The music sources will ‘loop’ continuously. Whenever the music is requested to start, it always plays from the beginning of the file.

You can assign the MOH source of your choice to the functions in your system (trunk groups, Uniform Call Groups, ect.).

The following table shows the MOH choices.

Music Number	Source
1 through 15	Music (.WAV) file on Media Server
Quiet Tone	Media Server

Programming

To upload a custom MOH file.

1. Login to Enterprise Manager Personal Administrator.
2. Select **Application > Custom MOH**.
3. Click on the **Browse** button next to the MOH source number you want to customise.
4. Navigate the audio file you want to upload. Refer to the Music On Hold File Formats shown below.
5. Click on the **Upload** button.

Music On Hold File Formats

The audio files can be named anything (as long as they end with .wav). Supported audio wav files are shown in the table below.

Digitizing Method	Sampling Rate (kHz)	Resolution (Bits)	Bit Rate (Kbps)
OKI ADPCM	6	4	24
OKI ADPCM	8	4	32
G.711 PCM A-law and mu-law	6	8	48
G.711 PCM A-law and mu-law	8	8	64
Linear PCM	8	16	128
Linear PCM	11	8	88
GSM 6.10 full rate (Microsoft format)	8	value ignored	13
G.726 bit exact	8	2	16
G.726 bit exact	8	4	32

MOH COMPATIBLE WAV

The Media Server (MS) is specified to handle up to 15 MOH audio .wav files. The audio files can be named anything as long as they end with .wav

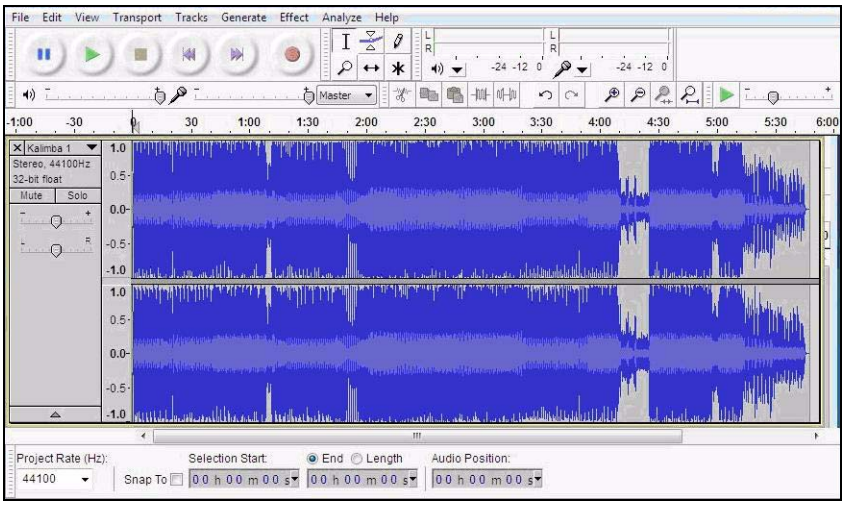
CONVERT MP3 TO WAV

An MP3 file can be converted to a compatible WAV file for use as a MOH source. One method is by using a freely downloadable program called Audacity® (http://code.google.com/p/audacity/). Audacity is a trademark of Dominic M Mazzoni.

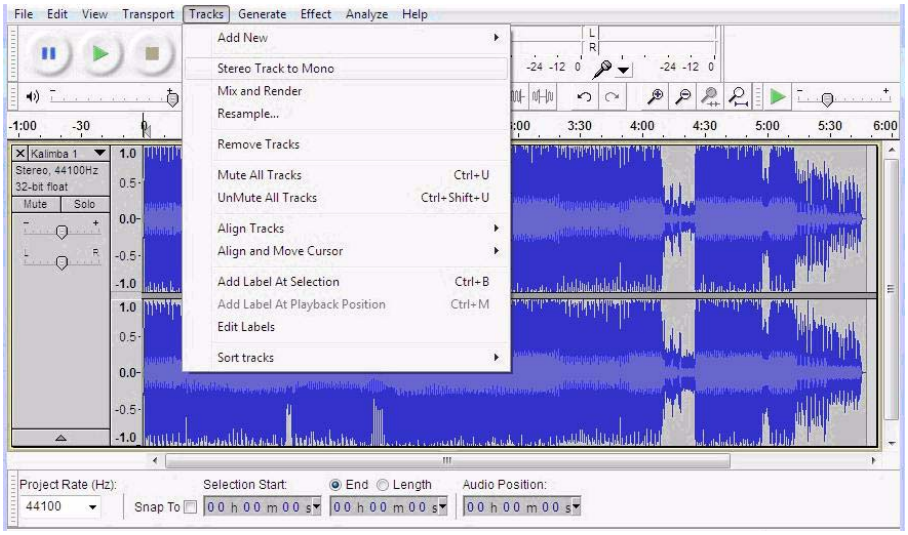
Note: Run the MP3 to WAV conversions on an administration PC, not the VIPedge server.

The following procedure shows the MP3 to WAV conversion using Audacity.

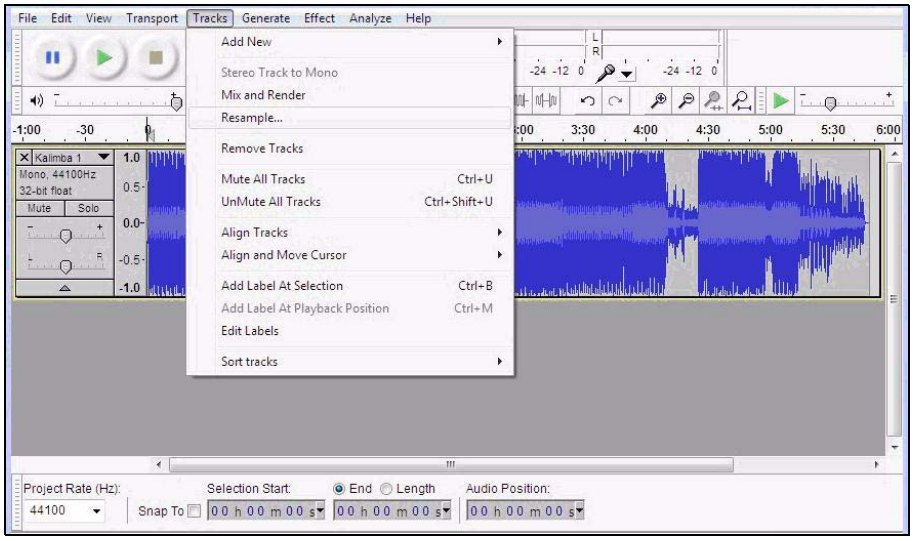
1. After installation, open the MP3 file you need to convert in Audacity:



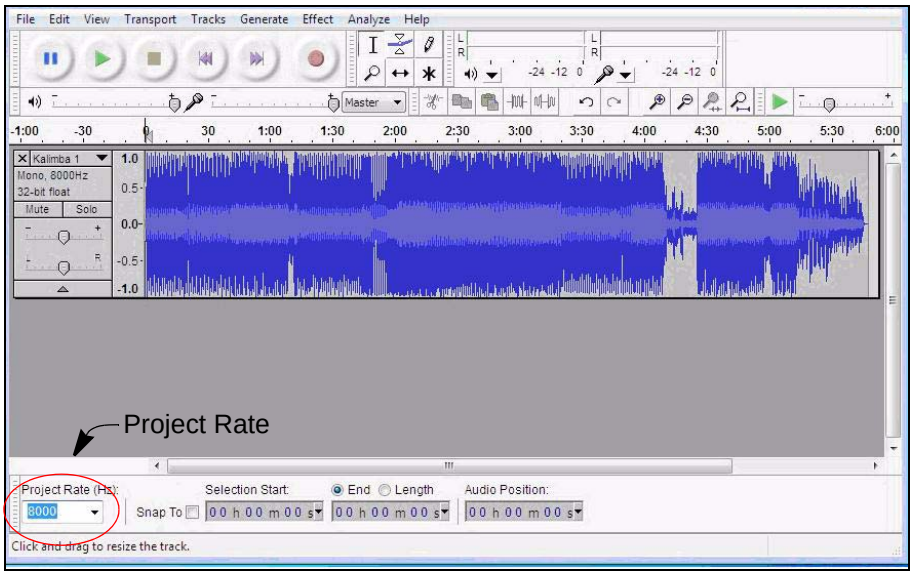
2. If in stereo, as shown above, convert the file from stereo to mono. Select **Tracks > Stereo Track to Mono**.



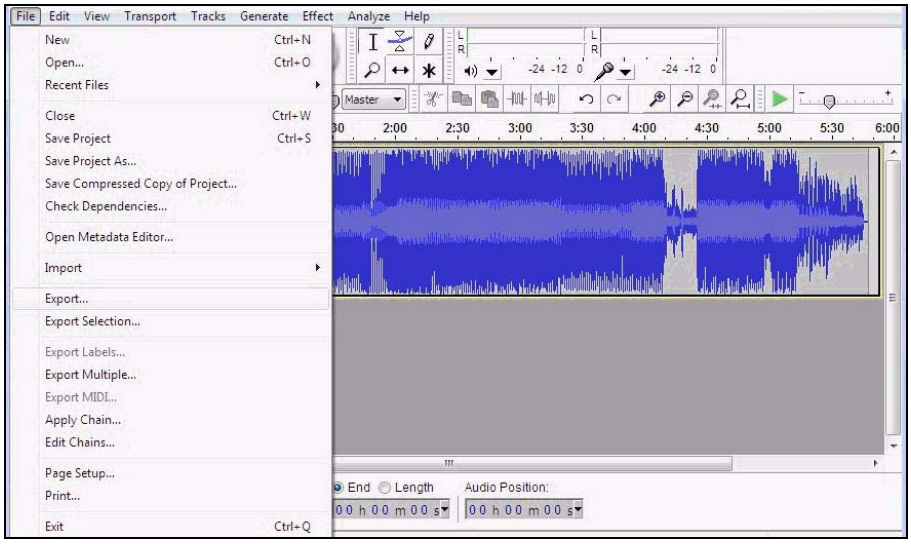
3. Then, resample the file. Select **Tracks > Resample**. Set new sample rate to **8000 Hz**:



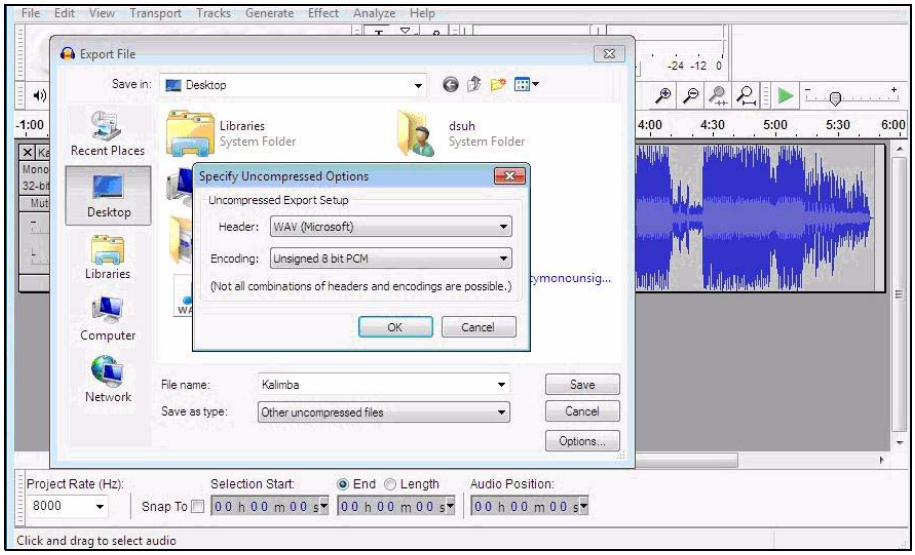
4. Change the Project Rate to 8000 Hz:



5. Select **Export** to save the file.

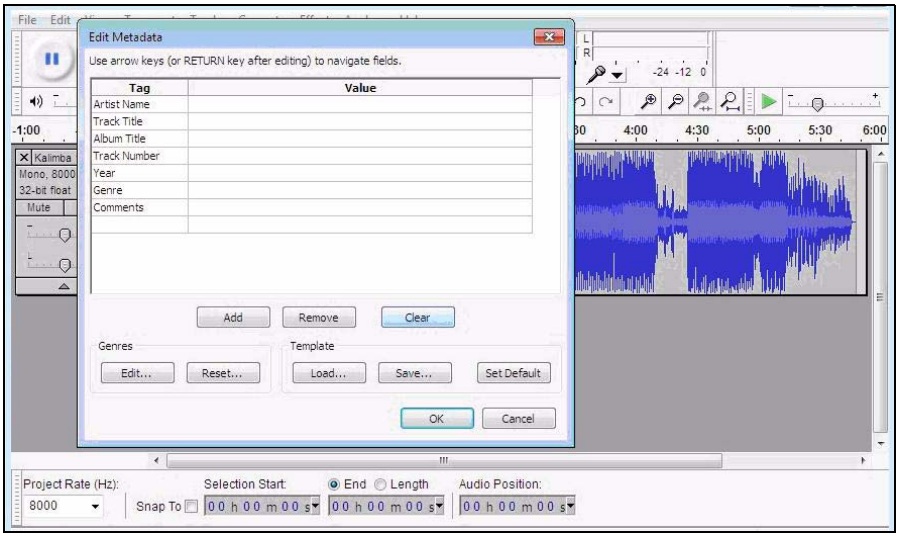


6. In the Export dialog enter the name for the file in the File name field. In the Save as type field select **Other uncompressed files**.
7. Click on the **Options…** button. For R1.2 and later systems select **WAV (Microsoft)** in the Header field and **Signed 16 bit PCM** in the Encoding field. For R1.1.2 (and earlier) systems select **WAV (Microsoft)** in the Header field and **Unsigned 8 bit PCM** in the Encoding field.



8. Click on **Save**.

9. In the last dialog box, click on **Clear** and then **OK**.



Adjusting MOH Volume

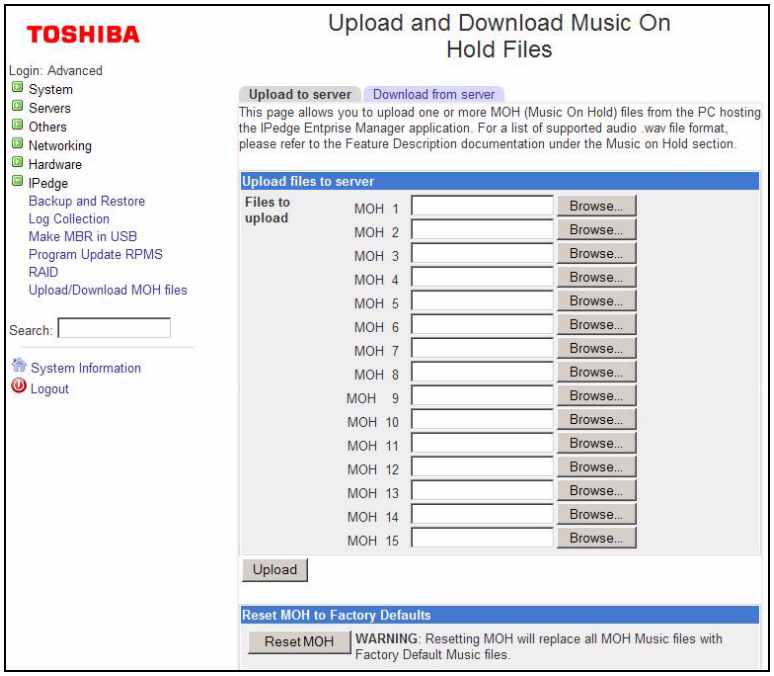
Use Audacity to adjust the volume using the **Effect > Amplify** function after the MOH file is loaded into the Audacity application.

UPLOAD WAV TO VIPedge SERVER

Upload the WAV file to the VIPedge server using VIPedge Webmin.

1. Login to Enterprise Manager. Select **Application > VIPedge Webmin**.
2. Select the server or customer.

3. In VIPedge Webmin select **IPedge > Upload/Download MOH Files**.



4. Click on the **Browse** button next to the MOH number for this file.
5. Browse to the WAV file you just converted.
6. Click on the **Upload** button.

BACKUP

The custom Music On Hold files are not part of the System Backup. Toshiba recommends that you maintain a backup of the MOH files that were uploaded to the VIPedge server in a secure location.

This page is intentionally left blank.

Chapter 8 – VIPedge System Backup

BACULA

The VIPedge system manual backup process is controlled by Bacula. Bacula is a set of programs that manage the backup, recovery, and verification of the VIPedge configuration database. Bacula runs entirely upon the VIPedge server.

Bacula is accessed through Enterprise Manager, select **Application > Webmin**. On the Webmin screen select **IPedge > Backup and Restore**. The Bacula Backup System home screen will open.

Figure 8-1 Bacula Main Page

VIPedge, Messaging backup is integrated with the backup of the VIPedge system configuration and call processing database. You don't need to backup the Messaging data separately.

The Music On Hold files are not part of the System Backup. Toshiba recommends that you maintain a backup of the MOH files that were uploaded to the VIPedge server.

BACKUP SCHEDULE

When a system is installed the backup volume, which is the location of the backup files are defined in the default configuration. The backup schedule for each VIPedge server is set to sometime between 3:00AM and 4:20AM local time during the VIPedge server provisioning. You can verify when the backup is run for each customer through the Director Status page. A full backup is performed every Tuesday. An incremental backup is run Wednesday through Monday.

Verify Backup Job Status

1. Navigate the Bacula main screen.
2. Click on the Director Status icon.

RESTORE FROM BACKUP

The system restore from the backup files is done only by Toshiba Technical Support.

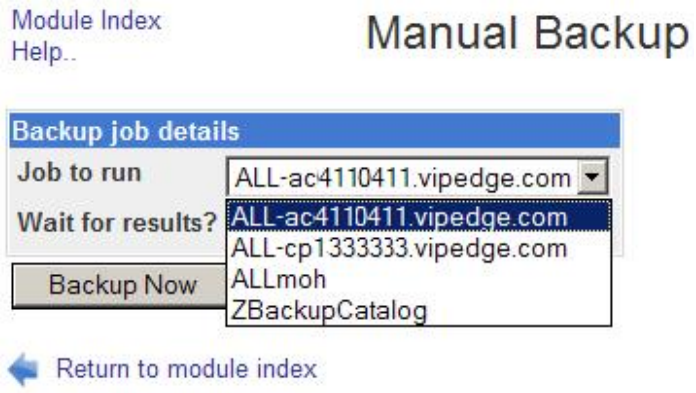
MANUAL BACKUP

A backup can be run manually any time. Running a manual backup does not effect the automatic backup schedule. Toshiba recommends that you run a backup before making a critical change.

Manual Backup Procedure

This creates a backup as a file in the backup section on the VIPedge server.

1. Login to Enterprise Manager. Select **Application > Webmin**.
2. In the Webmin screen select **IPedge > Backup and Restore**. Click on the **Manual Backup** icon.
3. In the Job to run pull-down select; All-Server Name. Where ServerName is the server you wish to backup.



4. Ensure that **Wait for results** is set to **Yes**. Click on **Backup Now**.
5. Wait for the backup to finish. When finished the system will display "… backup complete."

MANUAL RESTORE

The system restore from the backup files is done only by Toshiba Technical Support.

Chapter 9 – Net Server

Net Server allows applications to integrate with VIPedge to provide advanced services. Toshiba Call Manager is a typical example of a client application which works with the VIPedge In order to support those applications, Net Server manages Call Manager users, other application logins, and user groups.

Net Server is pre-installed on the VIPedge system and can be activated using VIPedge Enterprise Manager. After the license is applied, Net Server is ready to be used. If further configuration of Net Sever is necessary for server based Call Manager configuration, please refer to the Net Server administration section for details.

NET SERVER ADMINISTRATION

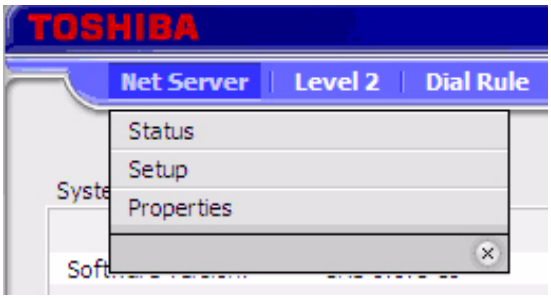
Net Server administration allows the administrator to configure the Net Server to control the behavior of Call Manager client application. It is designed to provide the basic operations of Call Manager without any configuration. If the administrator requires the advanced operations such as pushing settings to the clients, Net Server administration needs to be used.

To access Net Server

Using Enterprise Manger, go to Application > Net Server.

NET SERVER MENU

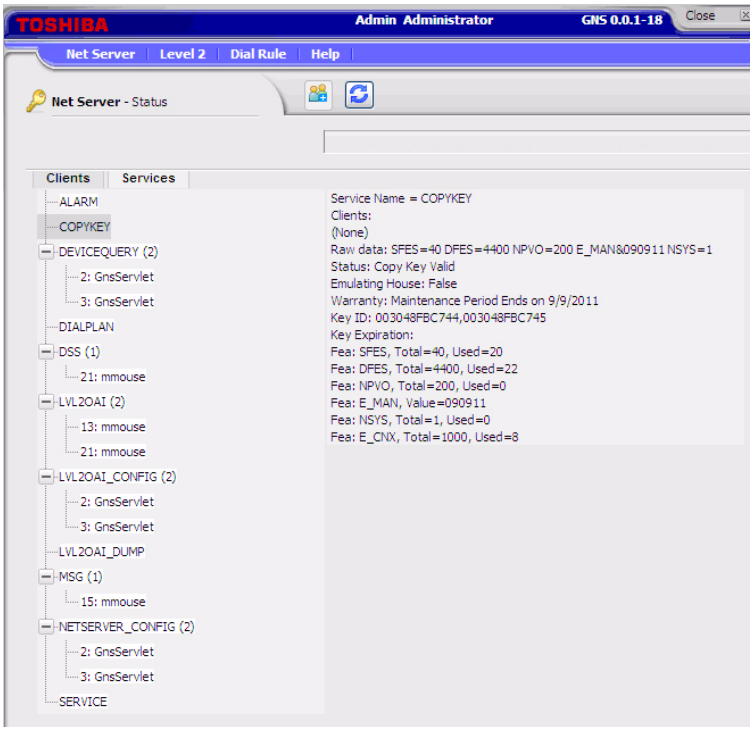
Net Server menu provides access to the basic setup for Net Server application on VIPedge server.



Status The Status sub menu provides real time information on the Net Server.

Clients Tab Clients tab shows the status of all the client applications that are connected to the Net Server. It includes all the component applications that are parts of Net Server and all the client Call Manager applications that are connected to the Net Server.

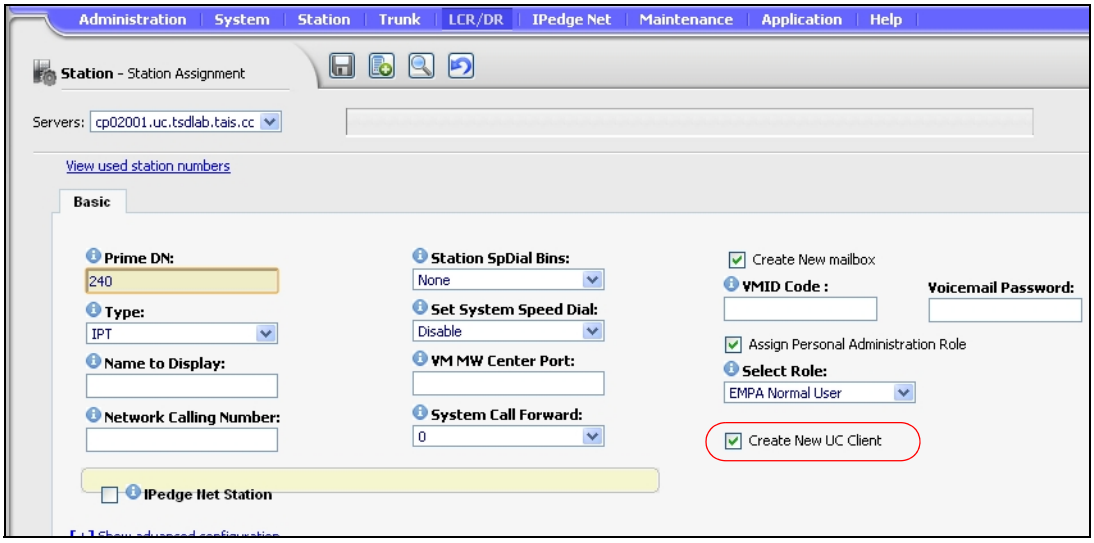
Services Tab Services tab shows the real time status of system component services running.



Setup Setup sub menu allows the administrator to manage client users, service components, applications, and groups.

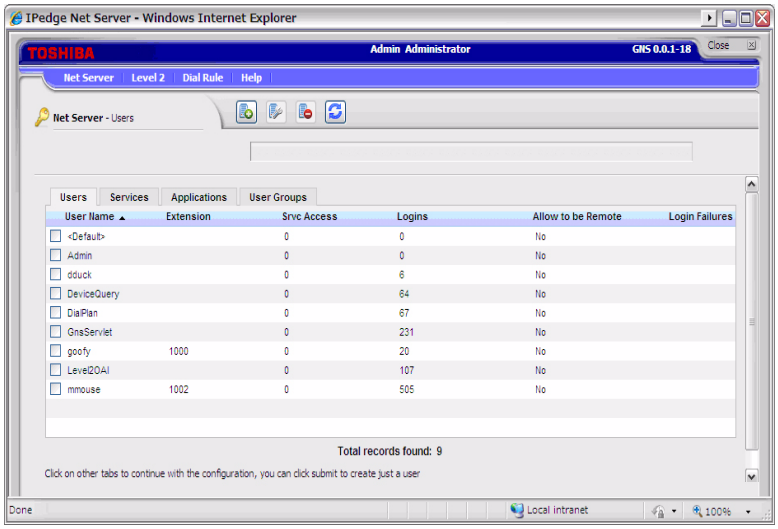
VIPedge Station Setup

1. Login to IPedge Enterprise Manager (http://<IPedge IP address>:8080/oamp/).
1. Go to Administration > **Enterprise** > **Customers**.
2. Select customer and click on “Manage the selected customer” button.
2. Create a station. Select **Station** > **Station Assignment**.
3. Click on the New icon.
4. Enter a Prime DN. The other parameters can be left as defaults.
5. Click on the Save icon to save the Station assignment.
6. Change the station Preference to Tone First in the Preference, Tone Ring/Voice Announce field.



Net Server Setup

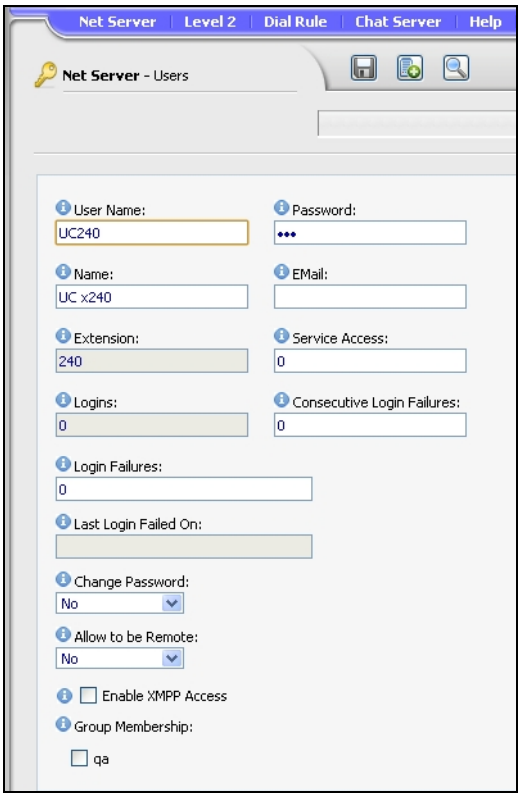
Users tab is used to manage the login information of the client applications. Clients can be added/modified from this tab. For security reasons automatic user addition is not allowed in the VIPedge system. All Call Manager users must be created before the user starts Call Manager on the client PC.

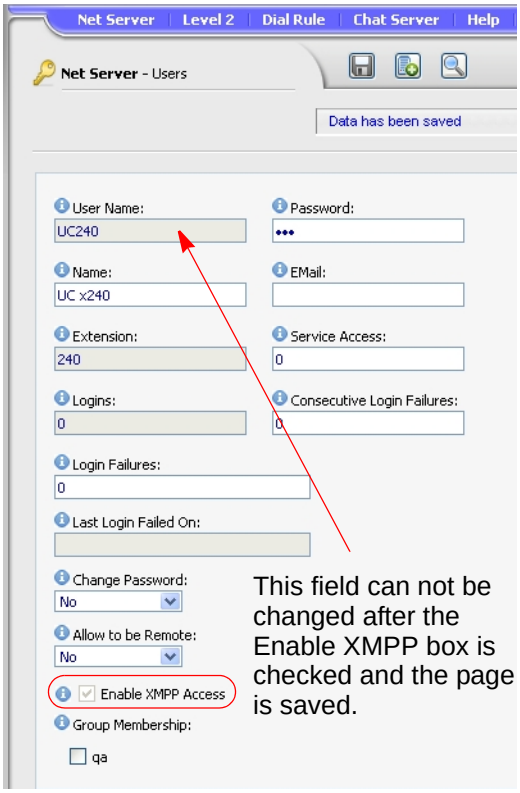


1. Create a Net Server User (Use the same DN created in VIPedge database. In Enterprise Manager select **Application** > **Net Server**.
2. In the Net Server administration window select **Net Server** > **Setup**.
3. Click on the New icon.
4. **User Name** is UC + DN. This is the default value, users can change this value when the UC client user is automatically created through station assignment. However, it is strongly recommend to use the real name as it will be displayed to other users. User Name can contain: alphanumeric characters, period (.), dash (-), and underscore (_).
5. **Password** The default password created by station assignment is DN, and Toshiba recommends a stronger password. Any printable character can be used for the password. The password cannot be blank. The administrator will need to supply the User Name and Password to each Net Server user so that they can login.
6. **Name** = DN (This is the default value, users can change this value.)
7. **Extension** = DN (as created above in station).
8. The other parameters can be left as defaults. The administrator must supply the User Name and Password information to each UC client user for them to login.
9. Click on the **Save** icon.

When you Add or Edit a checked entry, data can be entered from the following screen.

Note: After the XMPP box has been check-marked and the page has been saved the User Name cannot be changed. If it is necessary to change one of these you must delete the station then install it as a new station.



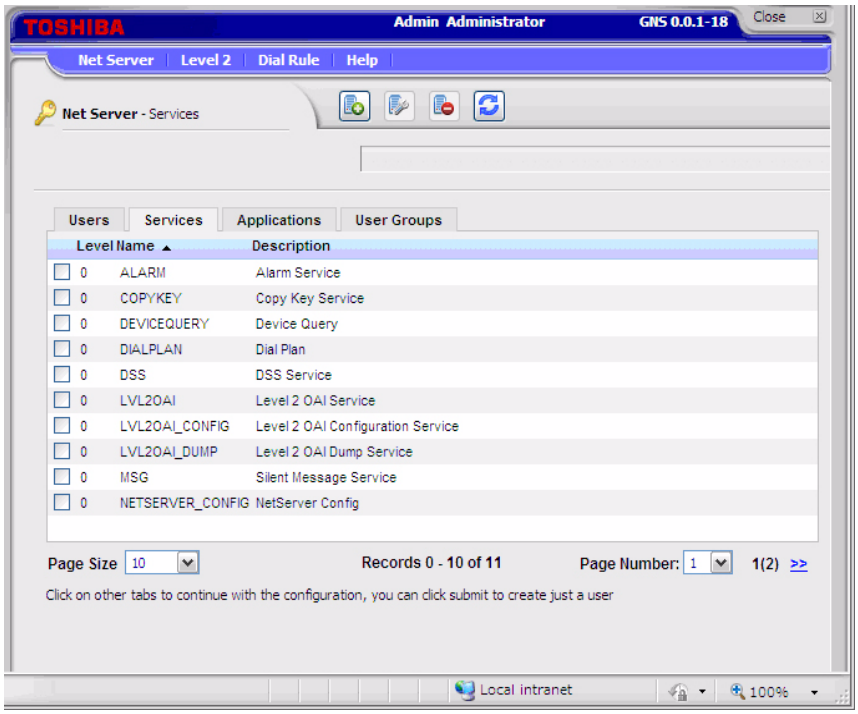


Name	Description
User Name	Name of the user to use for Net Server login (Required)
Password	Password used for Net Server login (Required)
Extension	Directory Number (DN) of extension that the user controls
Service Access	This is a number that determines which services the client has access to. Each service has a Service Level number, and a client will have access to all services whose Service Level is less than or equal to the client's service level access number.
Logins	Count of logins
Consecutive Login Failures	Count of consecutive login failures. Can be edited to reset the count.
Login Failures	Count of login failures. Can be edited to reset the count.
Last Login Failed on	Date and time of the last login failure
Change Password	Yes to allow the user to change the password
Allow to Remote	Yes to allow the user to connect remotely using the remote port (TCP port:8768)
Group Membership	A list of defined Groups is listed, Placing a check mark in the appropriate Group Name assigns that user to that Group. New Group can be created from User Group tab.
Enable XMPP Access	This check-box creates to link for this station in Net Server to the XMPP server. This is required for Call Manager operation. Once checked the User Name cannot be changed for this user.

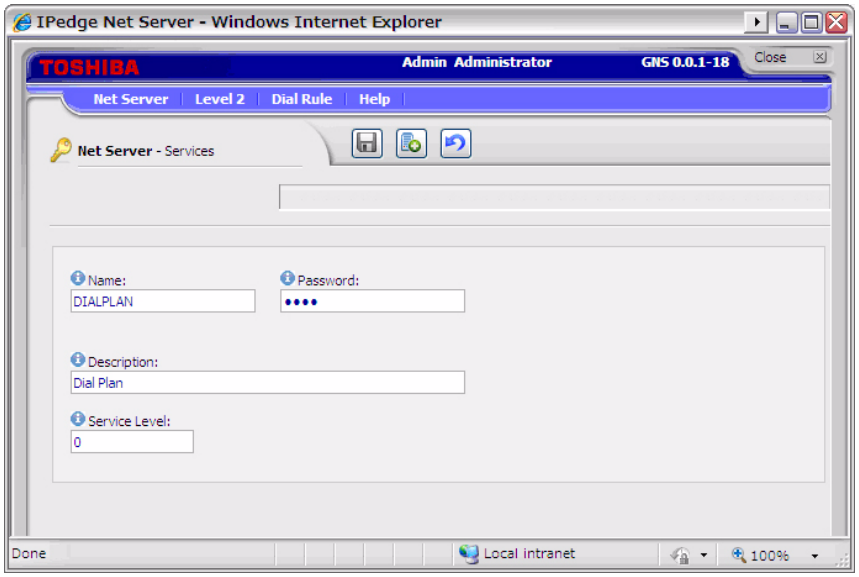
Services Tab

Use the Services tab to manage the component services running under Net Server.

It defines which services are on the server and what clients can use them. Services are automatically defined when they are installed, and do not need to be modified.



When you Add or Edit a checked entry, data can be entered from the following screen.

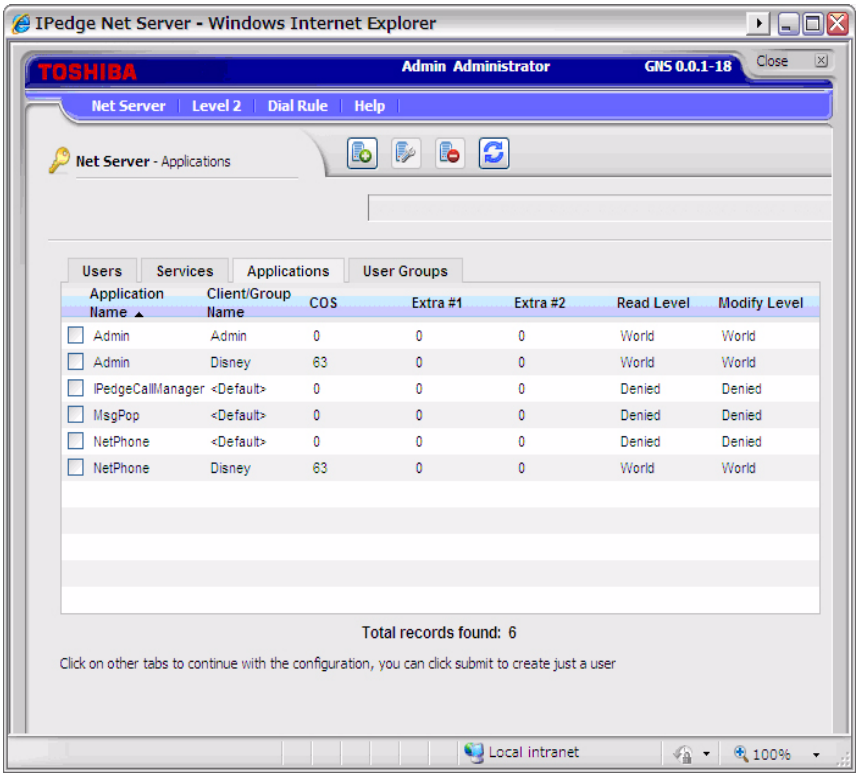


Field	Description
Name	Service name which must be unique in the system
Password	Password for the service to login to Net Server. Typically, it should not be changed.
Description	Description of the service
Service Level	Service Level determines which clients can access this service. Each client has a service level access number, and a client will have access to all services whose Service Level is less than or equal to the client's service level access number.

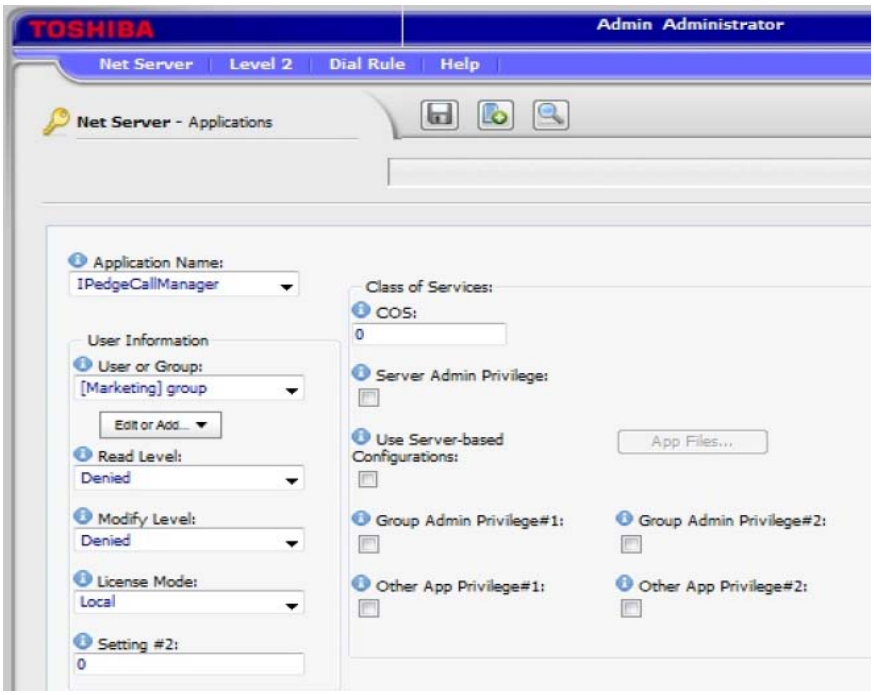
Application Tab

The Application tab defines the users for each application and allows you to assign a policy based on the user or the group. Please see the Group tab section for the specific information on the group policies.

See the SERVER BASED CALL MANAGER CONFIGURATION on page 9-18 for setting up the server based configuration for Call Manager.



When you Add or Edit a checked entry, data can be entered from the following screen.



Field	Description
Application Name	Name of the application
User or Group	Usually, the client name of the user is shown (see Clients). When it is set to <Default> (or leaving it blank) the settings for the Default User can be defined. It can be used to define the settings of typical users while any additional clients that need settings other than those of the Default User can be defined separately. Each user can be assigned to a group by setting this number (application may use this to standardize settings/ features for each group).
Read Level	This defines the access privileges for being able to read information about the application. The settings are Denied, Self, Group, or World.
Modify Level	This defines the access privileges for being able to modify the information about the application. The settings are Denied, Self, Group, or World.
License Mode	Specify the license that users in the group should use: Local – Use Advanced or Standard license specified during the installation. Advanced – Use Advanced license. Standard – Use Standard license. Auto – Try Advanced license first, and if not available, try standard license.
Setting #2	Reserved for future use.
COS	Define a COS number. These options are used to control the user access privileges. COS ranges from 0 to 63 is the sum of values assigned to each privilege shown below.

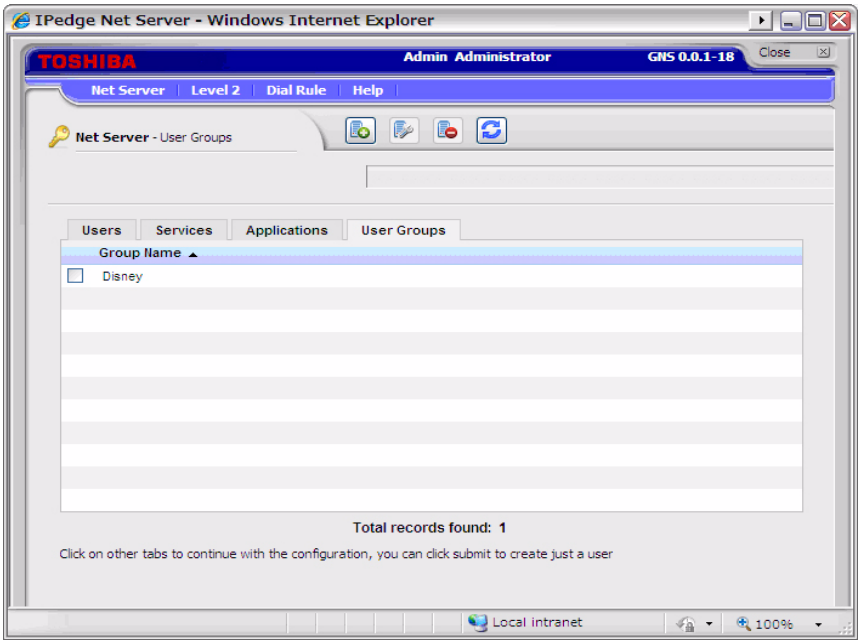
(Sheet 1 of 2)

Field	Description (continued)
Server Admin Privilege	Enables the user to do administration of server configuration files. (value: 1)
Use Server-based Configuration	When enabled, user will get the program configuration settings from the server specified by application files. If this is disabled, the user will get configuration settings from the local PC. (value: 2)
Group Admin Privilege#1/2	Determines if this user can perform functions for the group (unique to each application). (value: 4/8)
Other App Privilege#1/2	Determines if this user can perform other functions (unique to each application). (value: 16/32)

(Sheet 2 of 2)

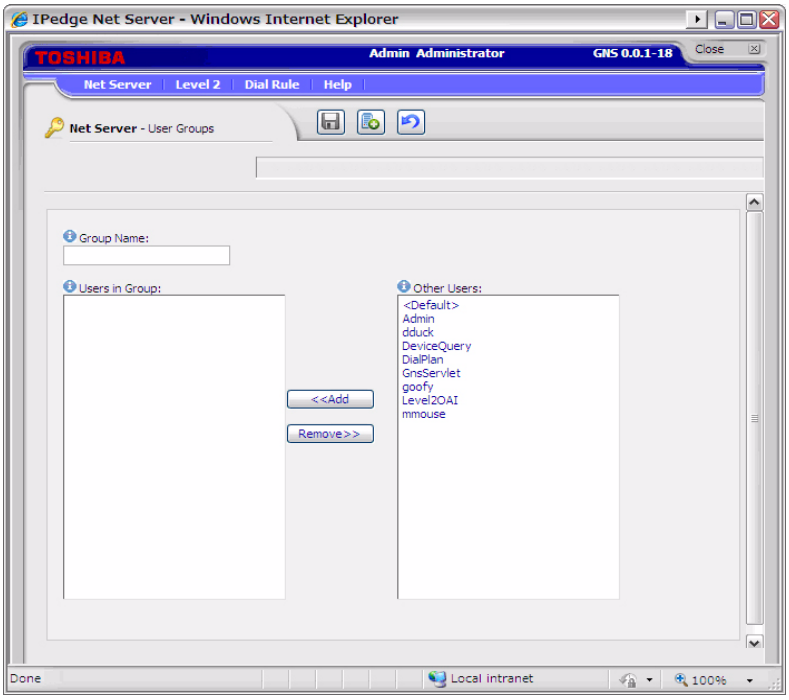
User Groups Tab

User Groups tab defines the group of users to apply the common settings to multiple users.



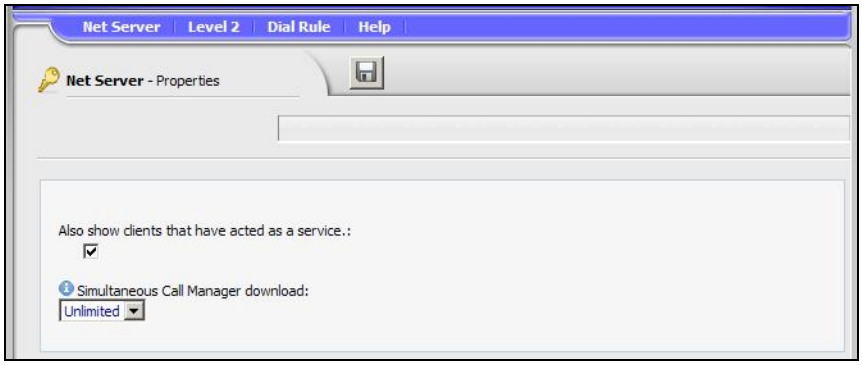
When you Add or Edit a checked entry, data can be entered from the following screen.

For an example refer to Create User Groups on page 9-18.



Field	Description
Group Name	Name of the group
Users in Group	List of users that are currently included in the group. A user can be removed from the group by selecting the user and clicking Remove.
Other users	List of users that are not currently in the group. A user can be added by electing the user and clicking Add.

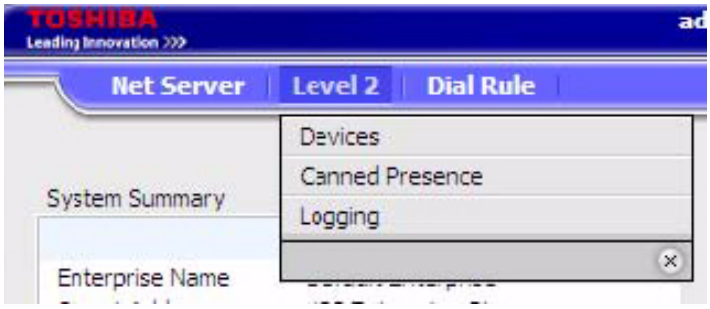
Properties Tab Properties tab is used to configure the Net Server.



Item	Description
Also show clients that have acted as a service	Control whether to show a component that is acting as a server in the client list. When checked, the Net Server Administrator / Users tab will show the main services running like Dial Plan, Level2OAI. When un-checked, it only shows the Call Manager Users, and Admin Accounts.
Simultaneous Call Manager download	Do not change.

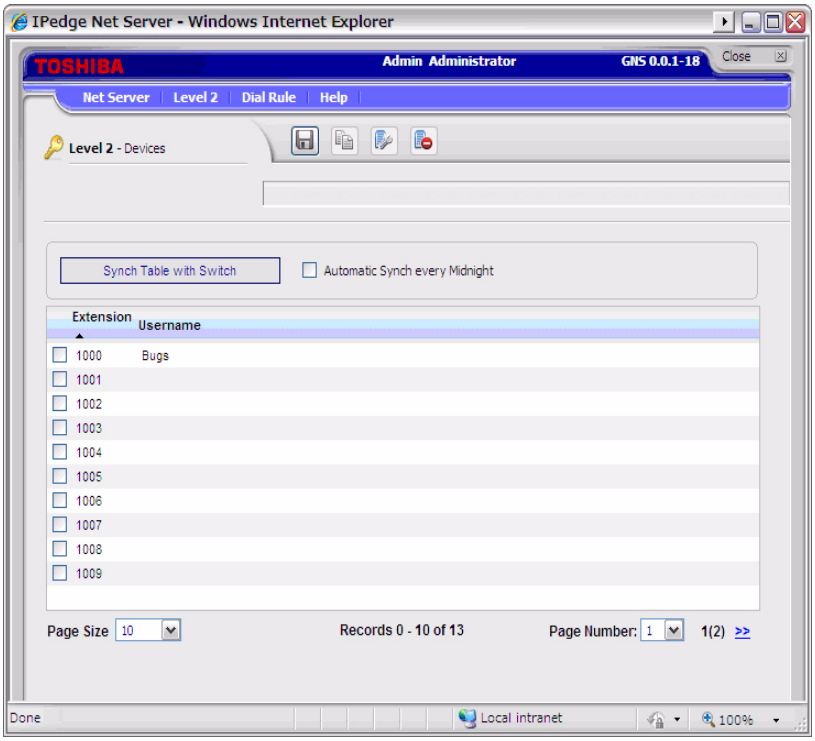
LEVEL 2 MENU

Level 2 menu allows the administrator to configure various items managed by Level 2 which processes the Computer Telephony Integration with the VIPedge system.



Devices Menu

Device menu manages the device table which provides an Extension Directory for Call Manager.



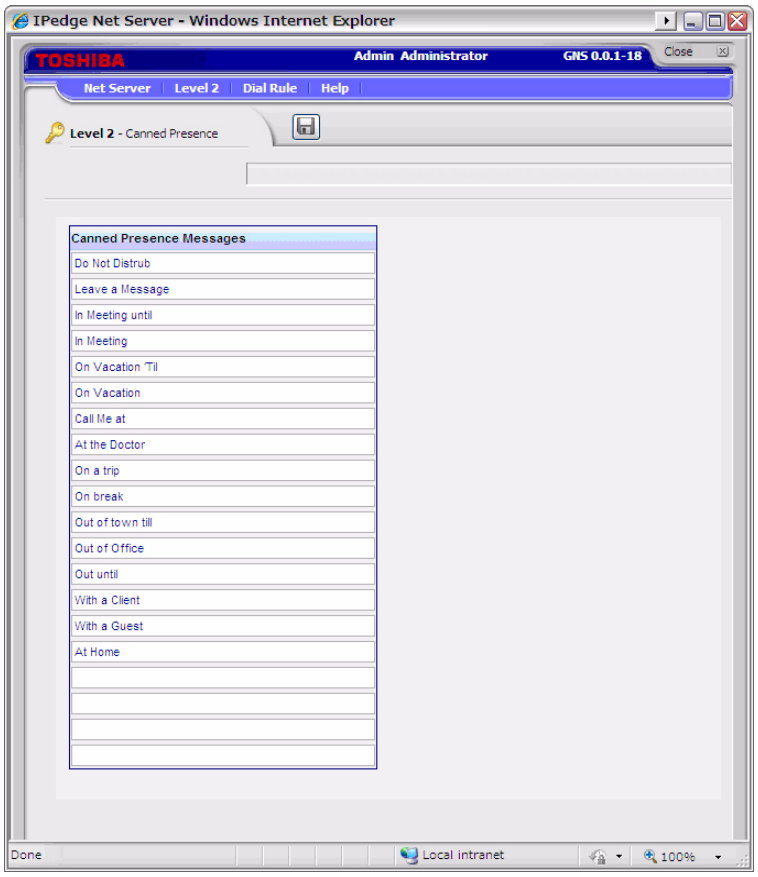
Device Table

Device table can be created manually by creating or copying an entry, or it can be automatically populated by using Synch Table with Switch.

It is also possible to automatically update every midnight by checking Automatic Synch Every Midnight check box.

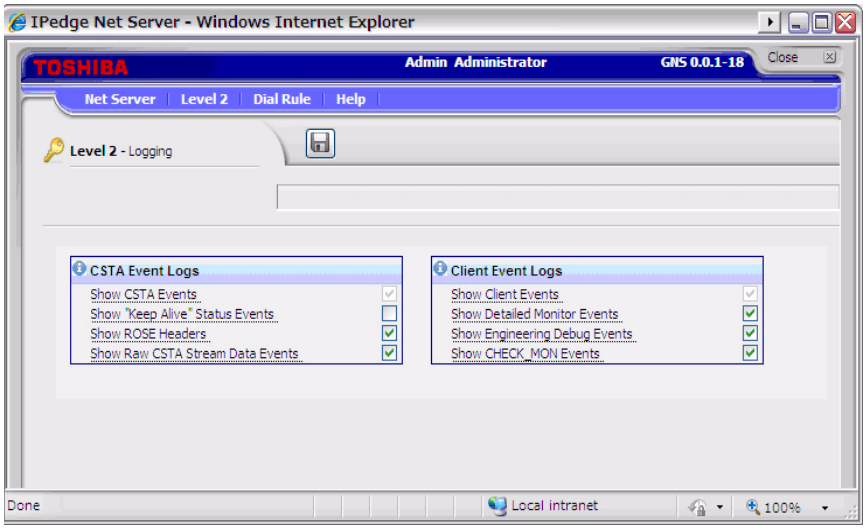
Canned Presence (Message)

Canned Presence (Message) menu enables the administrator to define messages used by Call manager for the additional information on the presence status. System standard default messages are defined, and the administrator can change them. Twenty different messages are possible.



Logging

Logging menu can control the level of trace information for problem investigation. All items are checked by default and do not have to be changed unless instructed to so by Toshiba Technical Support.

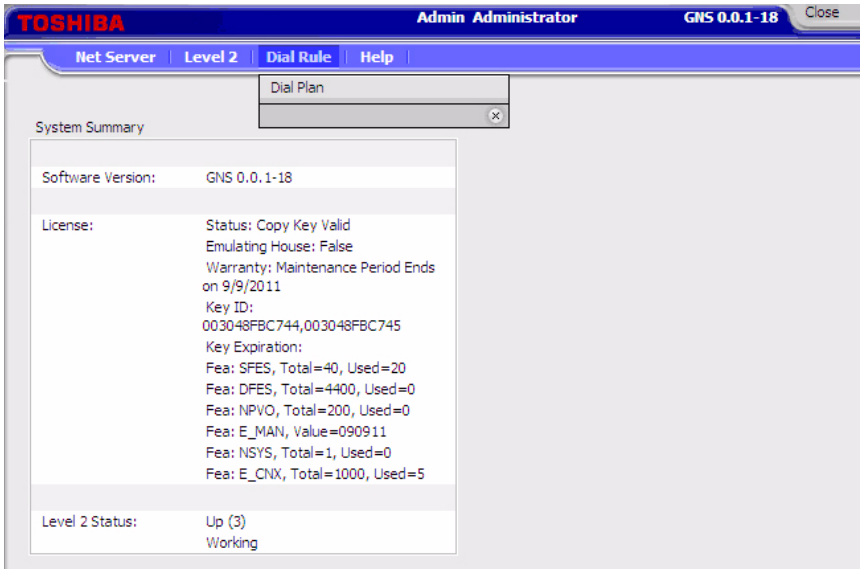


DIAL RULE MENU

Dial Rule Menu allows the administrator to define the dialing rule to be applied automatically when an application such as Call Manager makes a call.

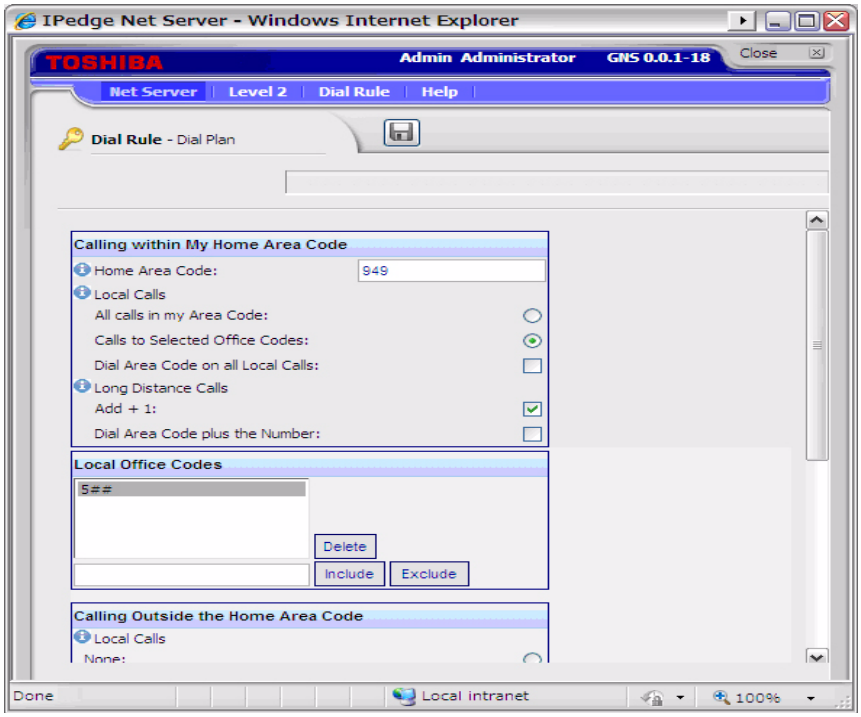
Dial Plan

Dial Plan sub menu defines how the system interprets the dialing string. When the Use SERVER Dial Plan is checked in the Preference in Call Manager, dialing digits from Call Manager are interpreted based on the rule defined in the Dial Plan.



Calls dialed on the VIPedge system go out on SIP trunks. The trunks require 1+10 digit dialing for all calls. These pages generally define how to setup tthe Call Manager dial plan..

1. Login and select the Call Manager administration.
2. Select Dial Rule > Dial Plan.
3. In the Calling within My Home Area Code section enter an unused area code (i.e., 999) in the Home Area Code field. Do not enter your real home area code.
4. Check-mark the Add +1 box.
5. In the Calling Outside the Home Area Code section check-mark the Add +1 box.
6. Click on the Save icon.



Test a Phone Number

Test a Phone Number – Dialing plans can become complex. Use these boxes to enter different telephone numbers and check to see the number that will be dialed. The dialed number should be identical to what you need to dial when using your phone to manually dial.

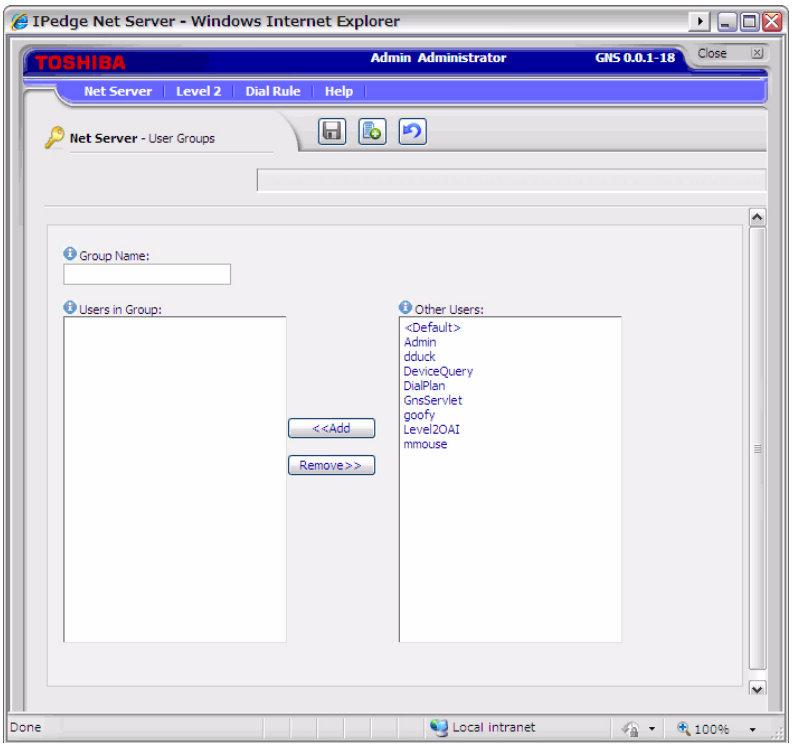
SERVER BASED CALL MANAGER CONFIGURATION

Creating a Server-based Class of Service for Call Manager begins in the group creation of Net Server administration, followed by creating your configuration on the Call Manager Admin, then publishing the configuration files to the Net Server.

The steps below show an example of creating two user groups, users and administrators, and assigning a class of service to each. Multiple groups can be assigned, each with its own configuration created by the Administrator common to that group.

Create User Groups

1. Use Net Server > Setup and click User Groups tab.
2. Click on the **Add** button
3. Type in a group name to represent the Call Manager administrator (CallManager Admin in this example) and click Save.

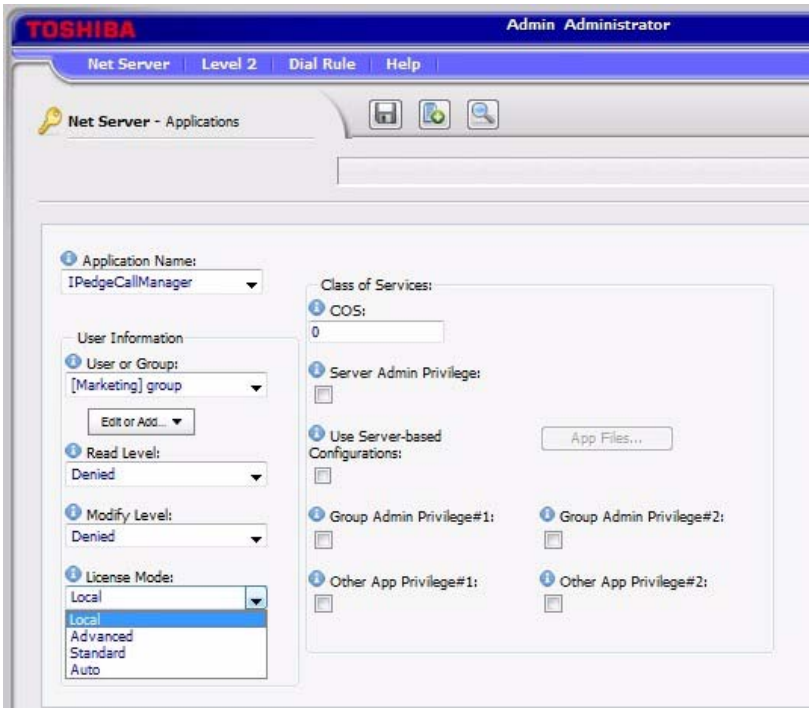


4. Click Add button again, and this time, type in a name to represent the Call Manager Users' group (Call Manager User in this example).
5. Repeat above steps for other groups if necessary.

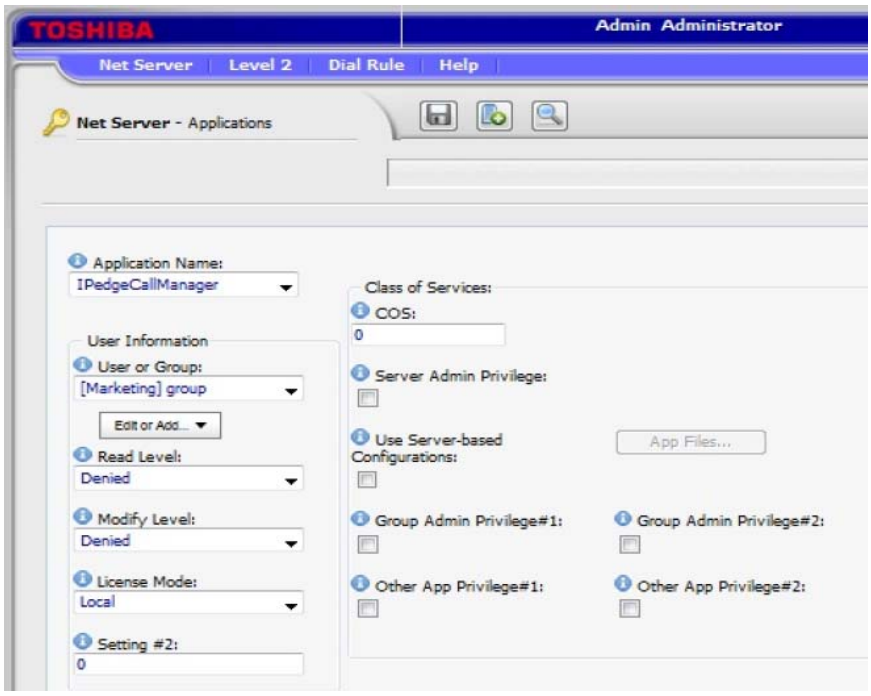
Assign Users to Call Manager Application

By assigning Groups to the Call manager application enables you to assign a common “Class of Service” and “Configurations” for all users in a group. Individuals that are not part of a group can also be assigned as a Call Manager application user.

1. Select the Applications tab, and click on the **Add** icon.
2. Select the Call Manager in Application Name drop down.
3. Select the administrator group (ex. Call Manager Admin) from the drop down menu for User or Group.
4. Select World for both Read Level and Modify Level from their respective drop-down boxes.
5. Place a checkmark in the Server Admin Privilege checkbox.
6. Select the License Mode.
7. Click on the **Save** icon.



8. Click Add icon.
9. Select the Call Manager in Application Name drop down.
10. Select the Call Manager User Group created previously from the User or Group drop-down box.
11. Select Denied for both the Read Level and Modify Level from their respective drop-down boxes.
12. Uncheck the Server Admin Privilege checkbox.
13. Select the License Mode.
14. Place a checkmark in the Use Server-based Configurations checkbox.
15. Click Save icon.

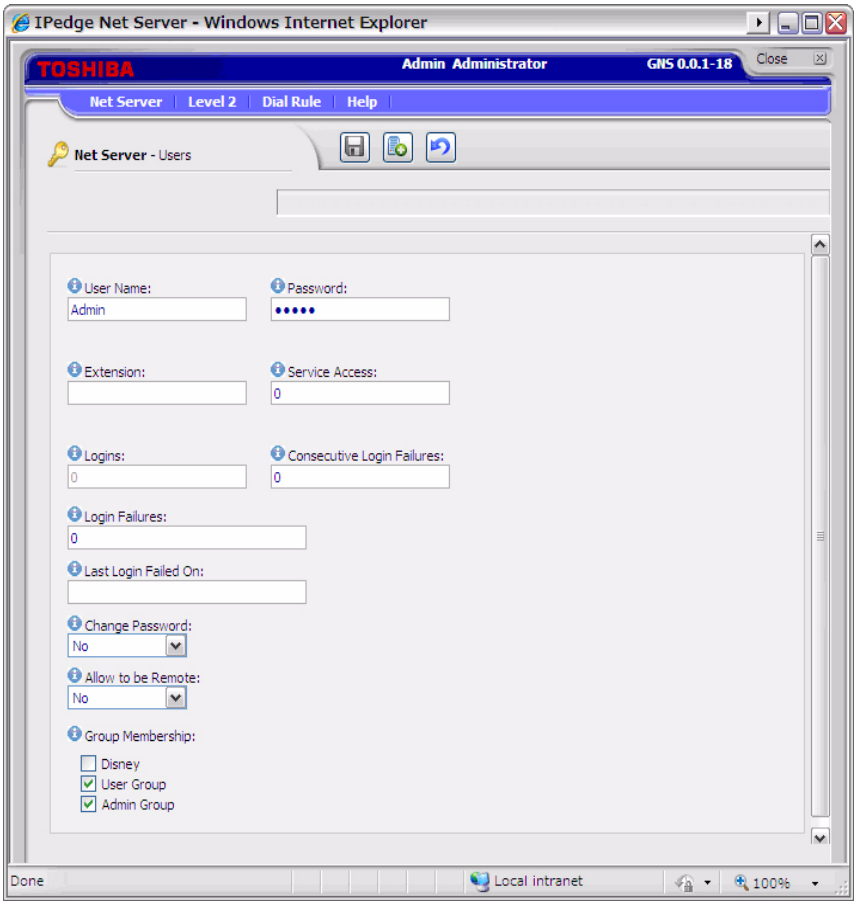


16. Repeat the preceding steps to add any remaining Call Manager user groups.
17. Default in User or Group can be used to setup the default settings for all users that are not included in any group or individual.
18. To exclude certain users from the Default, choose an individual user.

Assign Users to User Groups

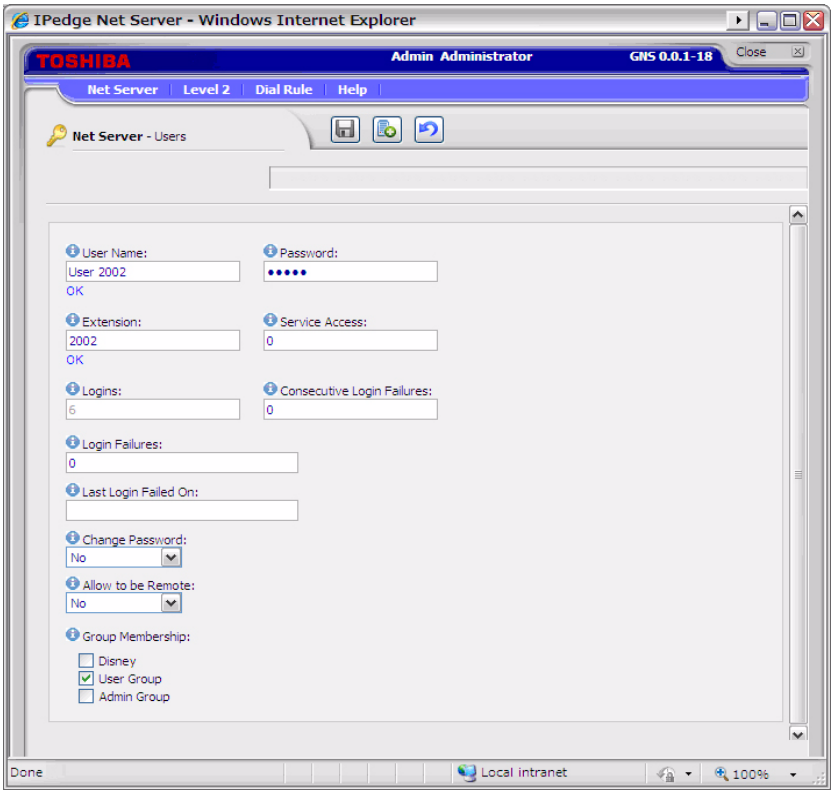
To Assign Users as Call Manager Administrators

1. Use Net Server menu > Setup, then Users tab.
2. Check the user who needs to be a Call manager administrator and click Edit icon.
3. Place a checkmark in both the Admin and Users groups as is shown in the screen below.
4. Click Save icon.
5. Repeat for other Call Manager users to be assigned as Administrators.



To assign a Call Manager User to the User Group

1. Check the user who is a Call Manager user and click Edit icon.
2. Place a checkmark in the User group only as is shown in the following screen:
3. Click Save icon.
4. Repeat for other Call Manager users to be assigned to a User Group.

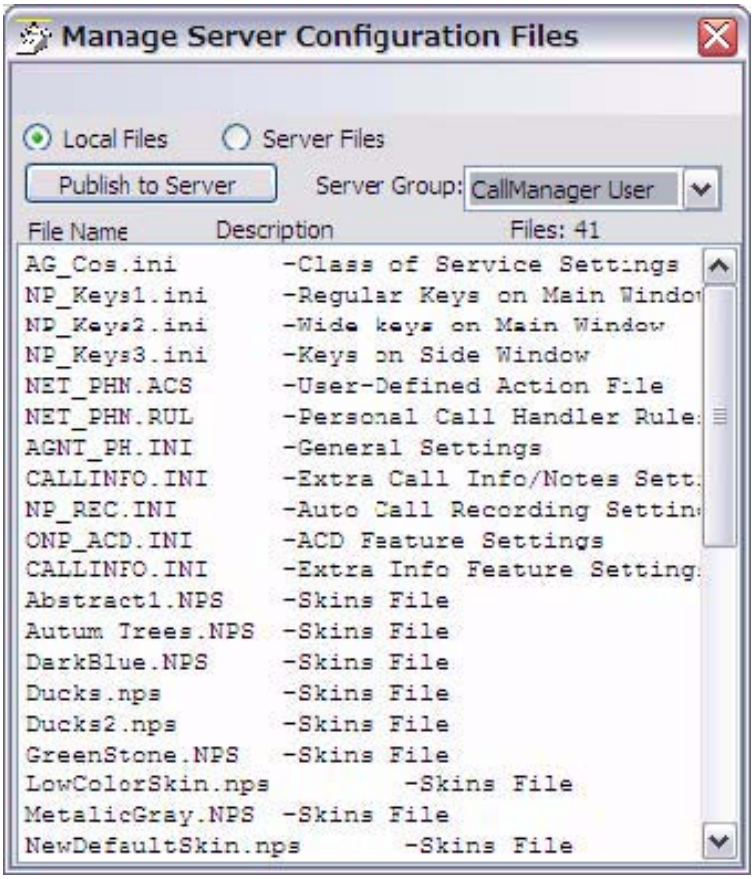


Create Configuration Files using Admin Call Manager

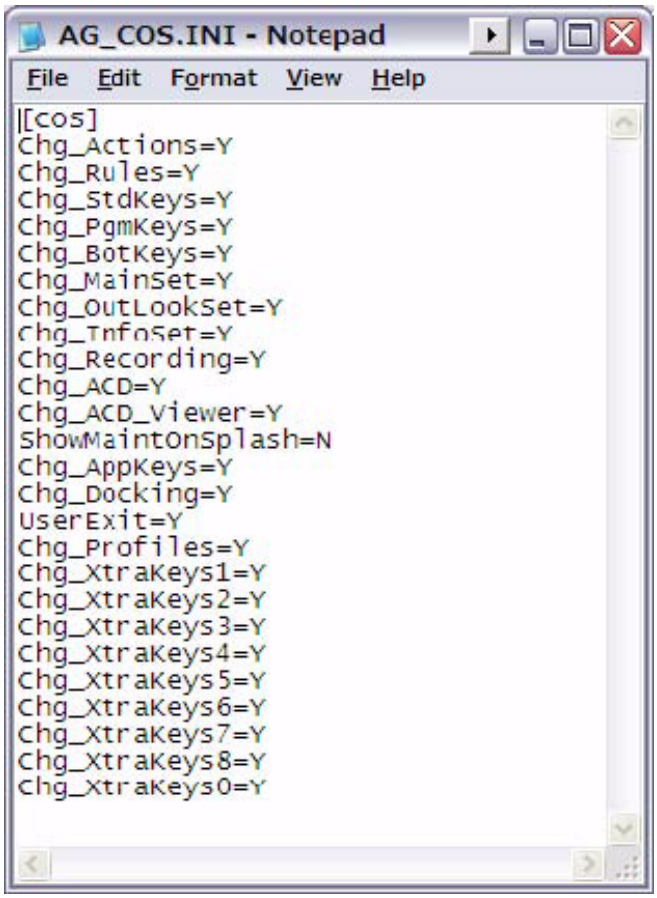
1. Restart the Administrator's Call manager if it is running
2. Set up the buttons, Call Handler rules, skins, etc. as you would like the users' Call Manager to be configured. Use the Call Manager User's Guide as needed for how to configure Call Manager. To access the user guide click on the SCM button in the Call Manager banner and select **Help**.

To Change the COS Configuration

1. Once the configuration is done, using Call Manager, select Tools > Publish.
2. Select the Server Group: Call manager User (the group created in Net Server).



3. Left-click on the file name "AG_COS.INI" to highlight it.
4. Right-click on the highlighted file and choose Edit. The following window is shown. Change each value from =Y to =N that should be set and controlled from the Server. Any items left using the =Y setting will allow the user to change and keep those settings on that local PC. The file from the server will not be downloaded.
5. Click File > Save to save the changes. Close the "AG_COS.INI" file.



CALL MANAGER MOBILE

If you are implementing Call Manager Mobile on this system the following items will need to be sent to each client.

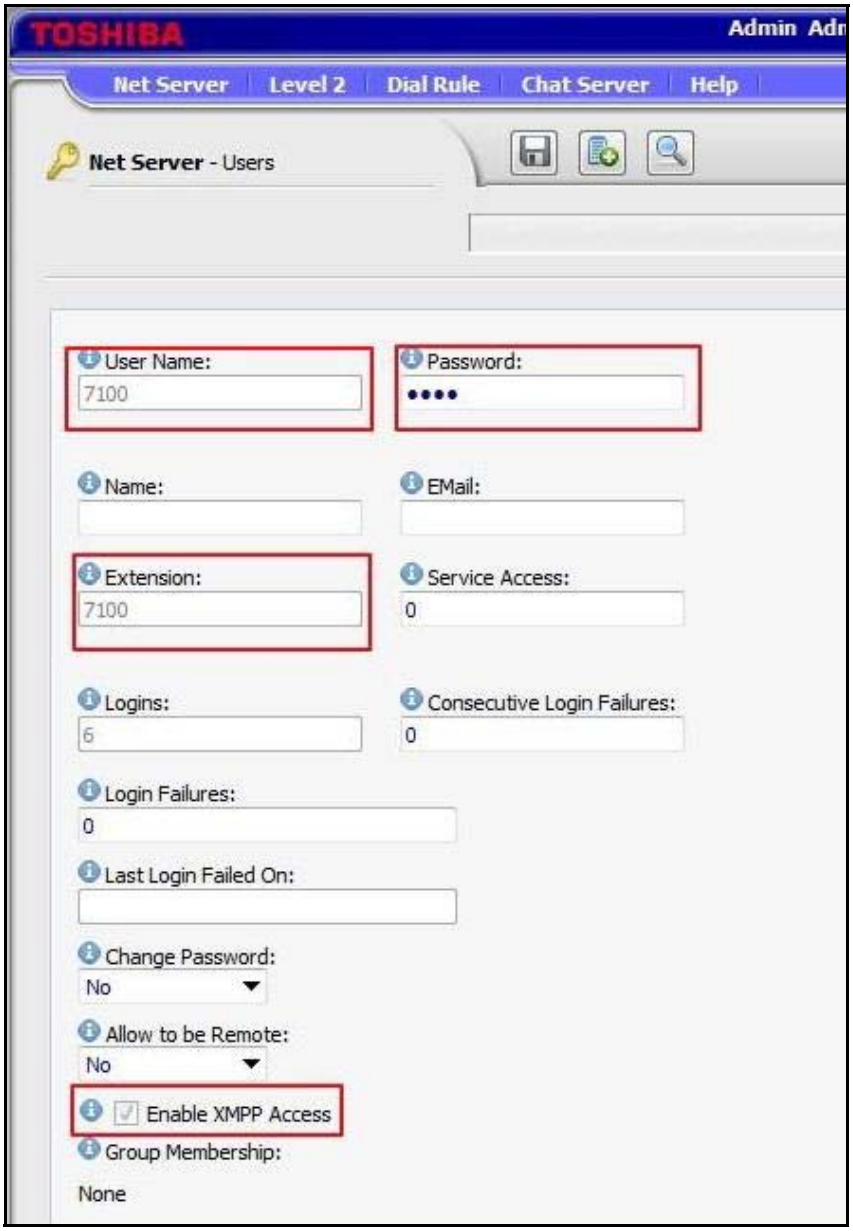
1. The client's Net Server User Name. The default is UC + DN.
2. The client's Net Server Password. The password is set during Net Server setup. Advise the user to change it to a strong password.
3. The VIPedge domain Name (example: cp2005907.vipedge.com)
4. The IP address of the VIPedge server.

CALL MANAGER MOBILE SETUP

This is the Call Manager Mobile implementation procedure.

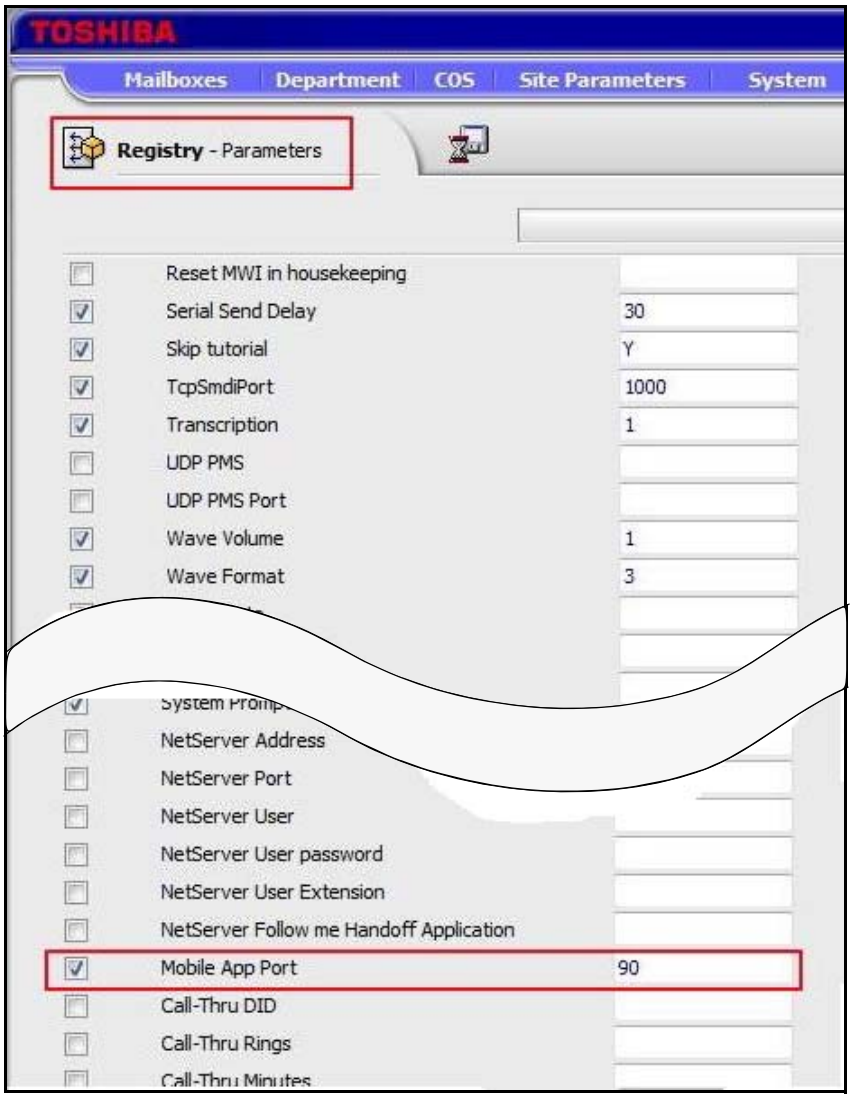
1. Login to Enterprise Manager for the customer's VIPedge container.
2. Select **Application > NetServer**.
3. In the NetServer screen select **NetServer > Setup**. Select the **Users** tab. Click on the **Add** icon.

4. Setup one Net Server user for each CAll Manager Mobile user. To add a NetServer User; enter the **Username**, **Password**, **Extension**, click to check-mark the **Enable XMPP Access** box. Click on **Save**.



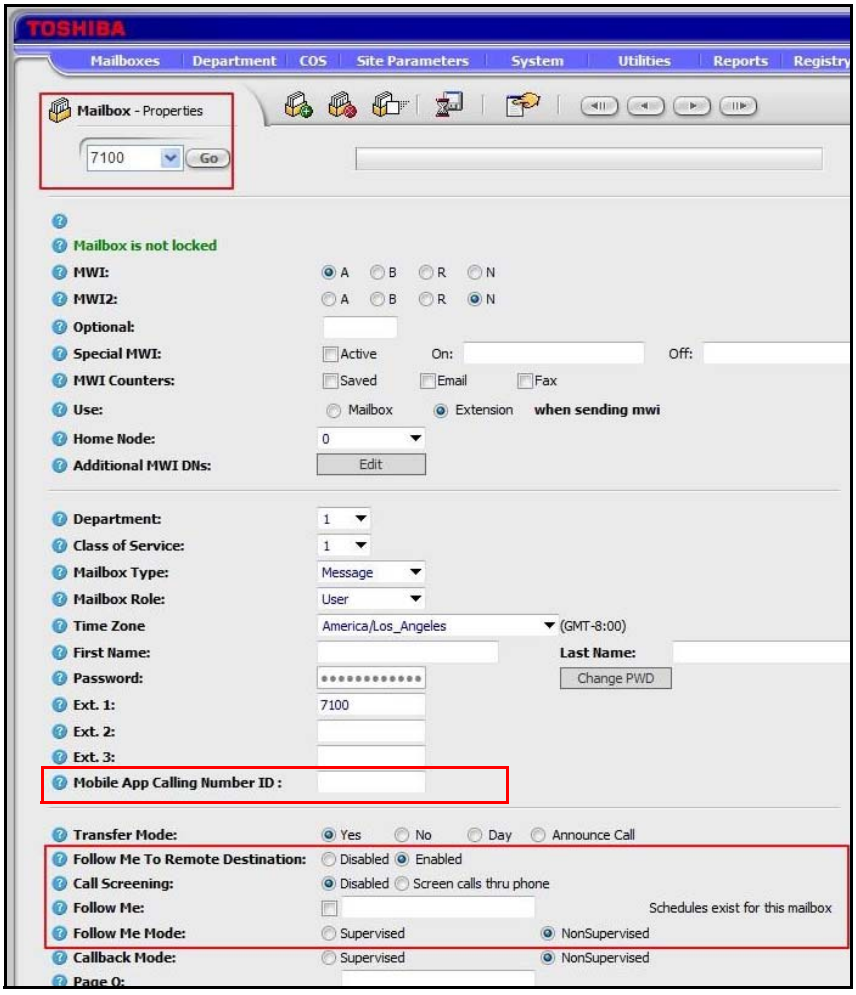
5. Close the NetServer Admin screen. In **Enterprise Manager** select **Application > Messaging**.

6. In the Messaging administration select **Registry > Parameters**, check-mark the Mobile App Port. Enter **90** as the value. Click on **Save**.



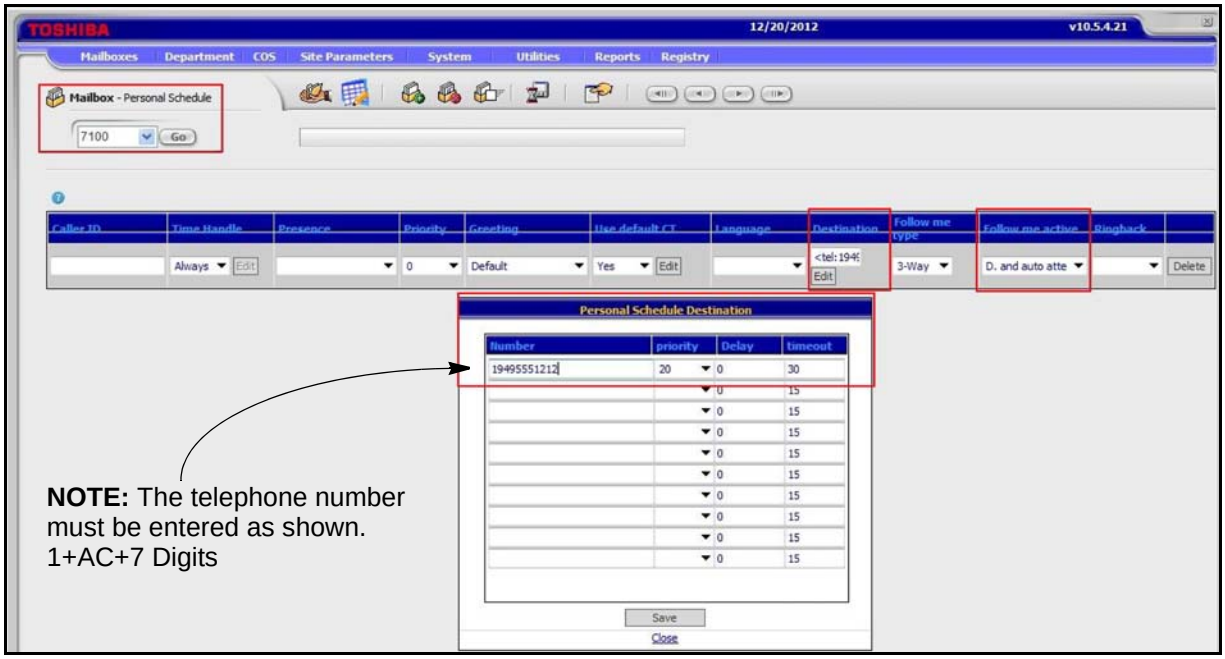
7. Select **Registry > Security**. Click on the **Generate Self Signed SSL Certificate** button.
8. Enter all the information in the **Certificate Details** window then, click on the **Generate** button.
9. Close the Messaging admin screen.
10. In Enterprise Manager select **Maintenance > System Maintenance > Core System Processes**.
11. Check-mark the **Messaging VM** box then, click on the **Restart** icon to restart the Messaging VM service.
12. Wait until Messaging restarts. The Messaging status will change from restarting to Running. Login to Enterprise Manager. Select **Application > Messaging**.
13. In the Messaging administration screen select **Mailbox > Properties**.

14. In the pull-down list select a User mailbox number that matches the NetServer User setup in step 4.
15. In the **Mobile App Calling Number ID** field enter the number that will be output when the mobile app makes a call. If left blank the calling number will display zeros on the called party's telephone.
16. Set the **Follow Me to Remote Destination** to Enabled. Leave the **Follow Me** field **blank**. Set the **Follow Me Mode** to **Non-Supervised**.



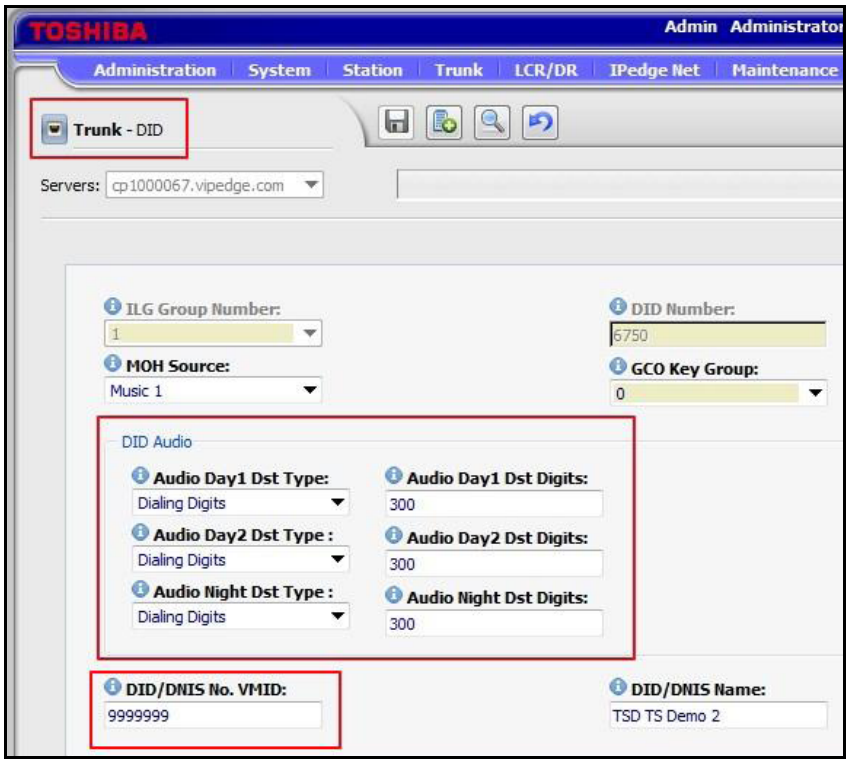
17. Click on **Save**.
18. From this screen select **Mailboxes > E-mail Settings**. Under Permissions, check-mark the box next to **Email Client**. Click on **Save**.
19. Select **Mailbox > Schedule > Personal Schedule**, click on the New Schedule icon. Select the Mailbox number of the user Mailbox for the user setup in step 14 from the pull-down list.
20. Click on **Destination**. In the Personal Schedule Destination dialog box enter the User's cell phone number in the number field. set the **Priority** value to **20** and enter **30** in the **Timeout** field.
21. Click on **Save** in the dialog box.

22. In the **Follow Me Active** field to **D. and Auto Attendant**, click on **Save**.



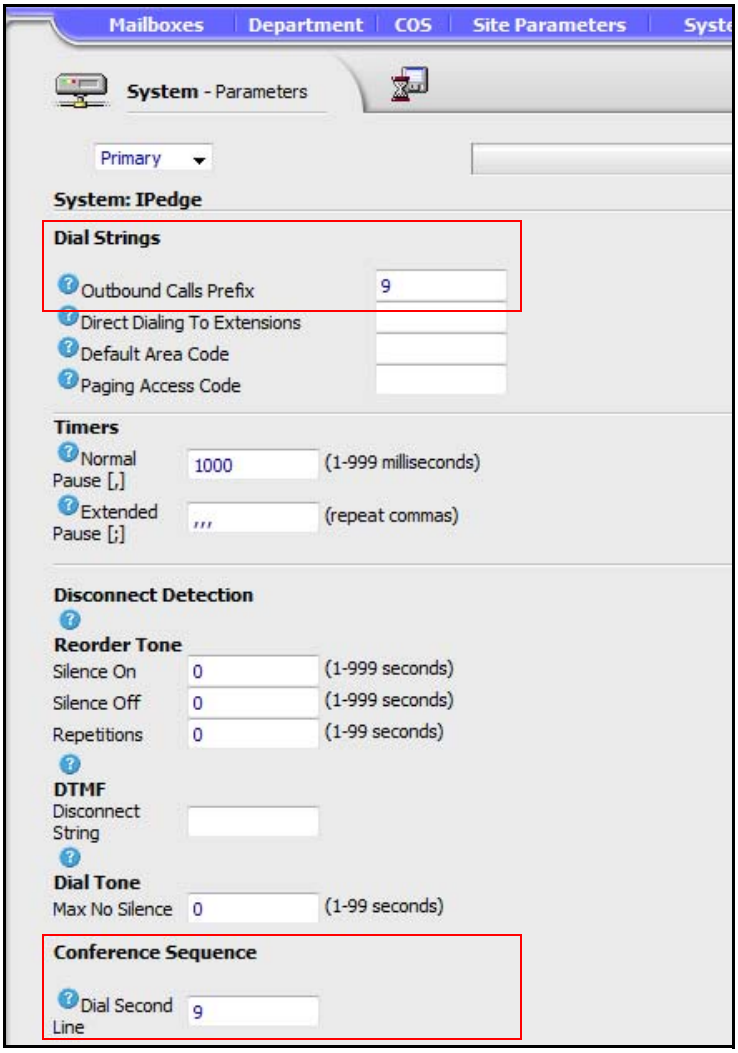
23. In Enterprise Manager select **Trunk > DID**, select the Call MAnager Mobile user's DID number.

24. Enter **9999999** (the number "9" entered 7 times) into the **DID/DNIS No. VMID** field.



25. Click on the **Save** icon.

26. Select **System > Parameters**. Set the **Outbound Calls Prefix** to **9** and the **Dial Second Line** to **9**.



27. Save then close the administration screen.

IPMobility APP INSTALLATION

Gather the following information to send to the Users. They will need this information to configure the Call Manager Mobility application.

- Domain name of the VIPedge container
- IP address of the IPedge server
- Mailbox number - usually thier extension
- Voicemail Password
- Direct Inward Dialing (DID) Number. This is the number for the IPedge system

Download IPMobility Application

Important! The IPMobility setup must be complete before the mobile devices can be setup.

The Call Manager Mobility app requires internet access to the host VIPedge.

Note: Mobile devices require a data plan with an option to enable Wi-Fi access for locations with poor cell network service. The IPMobility App must be installed on the mobile device.

The IPMobility application may be downloaded from Google Play™ or the iTunes™ App Store, search Call Manager Mobile.

For Android: https://play.google.com/store/apps

For iPhone: http://www.apple.com/itunes/

Call Manager Mobile App

After the download and installation the application needs to be configured.

1. Tap on the Call Manager Mobile application icon. The main login screen displays.

2. Tap the Configuration icon on the right corner of the screen.

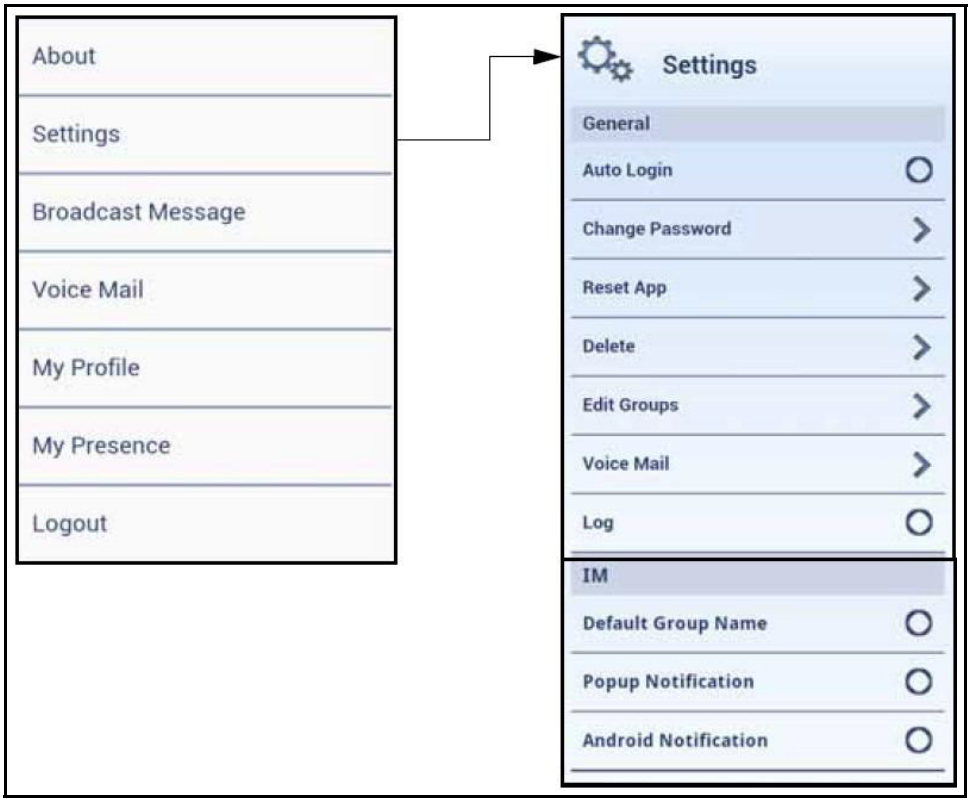
3. Click on **First Time Setup**.
4. Enter the **Domain Name** supplied by your dealer (example: cp23030308.vipedge.com) and the VIPedge Server IP address in the **Server IP** field. This information will be provided by your System Administrator.
5. Tap the **back button** on the upper left corner. The login screen will display.
6. Enter the **Username** and **Password** for this client. The User Name is the UC+VIpedge telephone extension number. For example UC2378. The password is the extension number. In this example the password is 2378.

   Note: The UC must be capitalized, as shown.

7. Check mark the **Automatic Presence** box. This enables others to see your presence status.
8. Click on the **Sign In** button.

Client Telephone Configuration

Once logged in the Configuration menu has several other menus. Click on the Configuration icon to access the Configuration menu (shown below).



Important! Voicemail must be configured properly as shown in the procedures below. Outgoing calls cannot be made if these settings are not configured. (see below)

VOICEMAIL CONFIGURATION FOR CALL MANAGER MOBILE

Voicemail must be configured for Twinning to work with Call Manager Mobile. The twinning function of the VIPedge Voicemail system performs outgoing calls from within the Call Manager Mobile application. Incoming calls use the Follow Me function of the IPedge system voicemail.

This procedure will configure Twinning on your Call Manager Mobile device.

1. Login to Call Manager Mobile, from the main screen, click on the Configuration icon on the top right corner of the screen. The Configuration page will display.
2. Select **Settings > Voice Mail**. The voicemail menu displays.

3. In the Voicemail Details menu, enter the necessary information as shown below.

Parameter	Description
Number	The user's VIPedge mailbox number (eg: 2378)
Password	The user's VIPedge voice mailbox password.
Cell Phone No	The telephone number of the cell phone the Call Manager Mobile application is running on.
DID No	The DID number the cell phone will use to make outgoing calls through the VIPedge system.
Dial Using Call Thru / Callback	Call Thru is the preferred setting.

This page is intentionally left blank.

Chapter 10 – Messaging

Messaging is pre-installed on the VIPedge system and can be activated using VIPedge Enterprise Manager. Once the Messaging license is activated, add the Messaging application to Enterprise Manager and then Messaging, then configure the application using the Application menu in Enterprise Manager.

ASSIGN THE VOICEMAIL SIP STATIONS

The VIPedge system has stations 3001 ~ 30xx (301 ~ 312 before R1.4) pre-configured as the SIP VoiceMail stations. Use the steps below to change the station DN assignments.

Change VM Station DN

1. From the **Station** menu, select **Station Assignment**.
2. Click to check-mark the station you want to change the DN.
3. Click on **Change station Primary DN** icon.
4. Click on **OK**.
5. Repeat for each station you want to change.

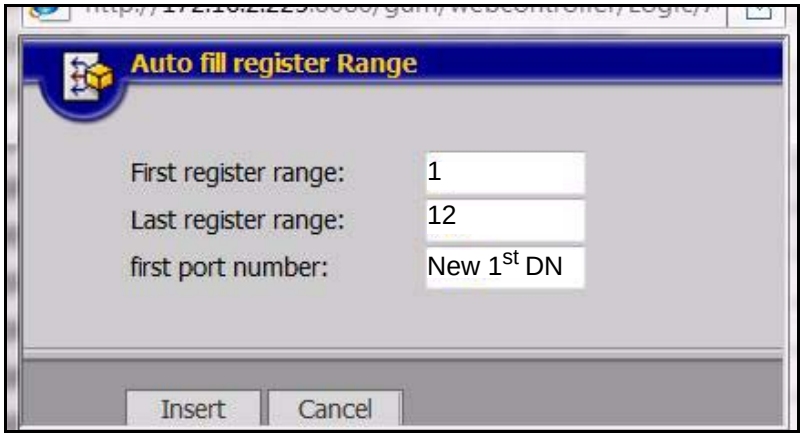
Change VM Pilot

1. Select **Station > Station Groups**. Group Type should be Hunt Group.
2. Select the group then click on the **Edit** icon.
3. Change the Pilot Number DN and Number to Display, then click on the **Save** icon.
4. Under **System > Voice Mail Data** change Transfer Direct to VM DN to the new Pilot Number.
5. In Station Assignments change the VM MW Center Port to the new VM Pilot Number.
6. Change the VM station numbers in **Applications > Messaging > Registry > VoIP**.
7. Restart Messaging, refer to RESTART MESSAGING on page 10-2.

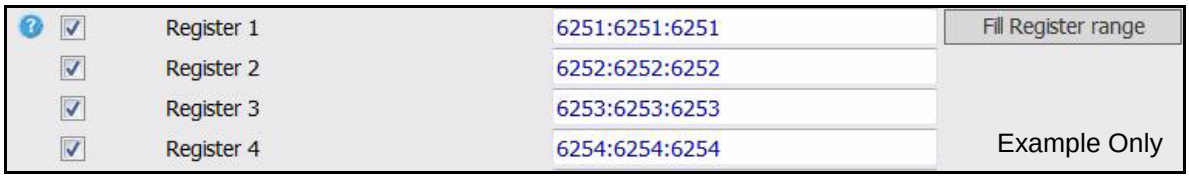
PROGRAM MESSAGING

1. Using Enterprise Manager, select **Application > Messaging**.
2. Select the customer container then, click on **OK**.
3. From the main menu, click **Registry > Parameters**.
4. Check **Default VIPedge**.
5. Click the **Save** icon.

6. Click **Registry > VOIP**.
7. Scroll down to the Registry assignments, click on the **Fill Register range** button.
8. In the Auto fill register Range dialog box enter the register range, based on the number of licenses. First Register Range is always 1. The Last is the number of licenses. Enter the first DN of the SIP station DNs assigned for messaging.



9. Click on the **Insert** button.



10. Assign SIP PBX Address with <cpXXXXXXXX.vipedge.com>.
11. Assign VM SIP Port as 5070 (default setting). Click Save.
12. Restart Messaging.
    See RESTART MESSAGING.

Relay Server UM Authentication

The VIPedge Relay Server must have email authentication credentials to send UM messages to email servers.

1. Select **Applications > Messaging > Registry > SMTP**.
2. Check-mark the box next to **Mail Server**.
3. In the adjoining Value field enter: **mail1.vipedge.com**.

RESTART MESSAGING

1. Go to Enterprise Manager **Maintenance > System Maintenance - Core System Processes**.
2. Click to select **Messaging vm**.
3. Click on the **Send stop action** icon.
4. Click to select **Messaging vm**.

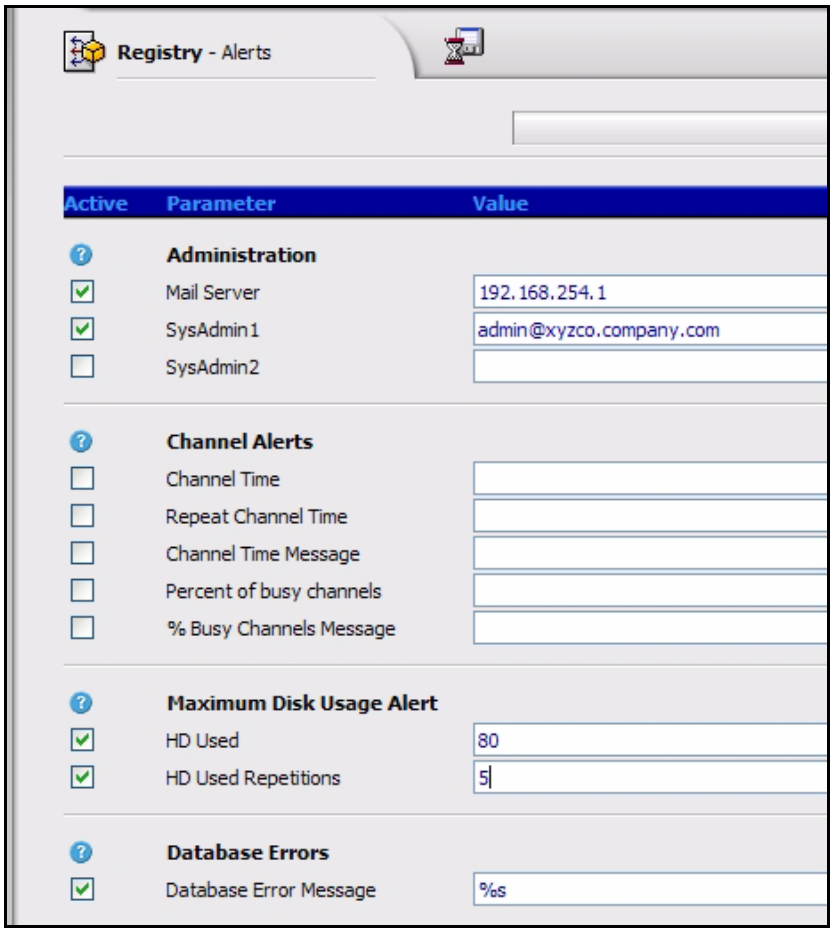
5. Click on the **Send restart action** icon.

Note: If you encounter a problem stopping or stating Messaging contact Toshiba Technical Support.

DISK FULL NOTIFICATION

Under some conditions the server disk can become full. Use the following procedure to setup an email alert to the system administrator when the disk is 80% full.

1. Using Enterprise Manager, select **Applications > Messaging**. In the Messaging administration screen select **Registry > Alerts**.



2. Under Administration, enter the name of the Mail Server.
3. Enter the email address for the administrator where the alerts should be sent.
4. Under Maximum Disk Usage Alert, ensure that HD Used is checked and set at 80 for the Administrator to receive an email notification when the hard disk is 80% full (default setting).
5. HD Used Repetitions – Enter the number of times for the Administrator is to be notified via email.
6. Check Database Error Message. Enter the value %s (default setting).

FOLLOW-ME SETUP

This procedure is used to setup the Follow-Me feature in Messaging.

Registry Parameters

Assign the Follow-Me parameters in Messaging.

1. Log into Enterprise Manager.
2. Select **Application > Messaging**. Select the server.
3. In the Messaging administration select **Registry > Parameters**.
4. Scroll down to the Netserver parameters. Enter the following:

   Netserver Address – The IP address of the Net Server if Follow Me control/hand-off from the phone button is required. Use 127.0.0.1 when the built-in Net Server is used or the actual IP address of the Net Server when the external ACD/Net Server is used.

   Netserver Port – The TCP port number (typically 8767) of the Net Server if Follow Me control/hand-off from the phone button is required.

   Netserver User – The user name to connect to the Net Server if Follow Me control/hand-off from the phone button is required. Use the pilot DN unless there is a specific need for the login name.

   Netserver User password – The password to connect to the Net Server if Follow Me control/hand-off from the phone button is required. Use the pilot DN unless there are specific needs for the password. If the password needs to be reset once it is set, it can be only erased from Net Server administration menu.

   Netserver User Extersion – The extension number (unique in the system) to connect to the Net Server if Follow Me control/hand-off from the phone button is required. Use the pilot DN unless there are specific needs for the Extension number.

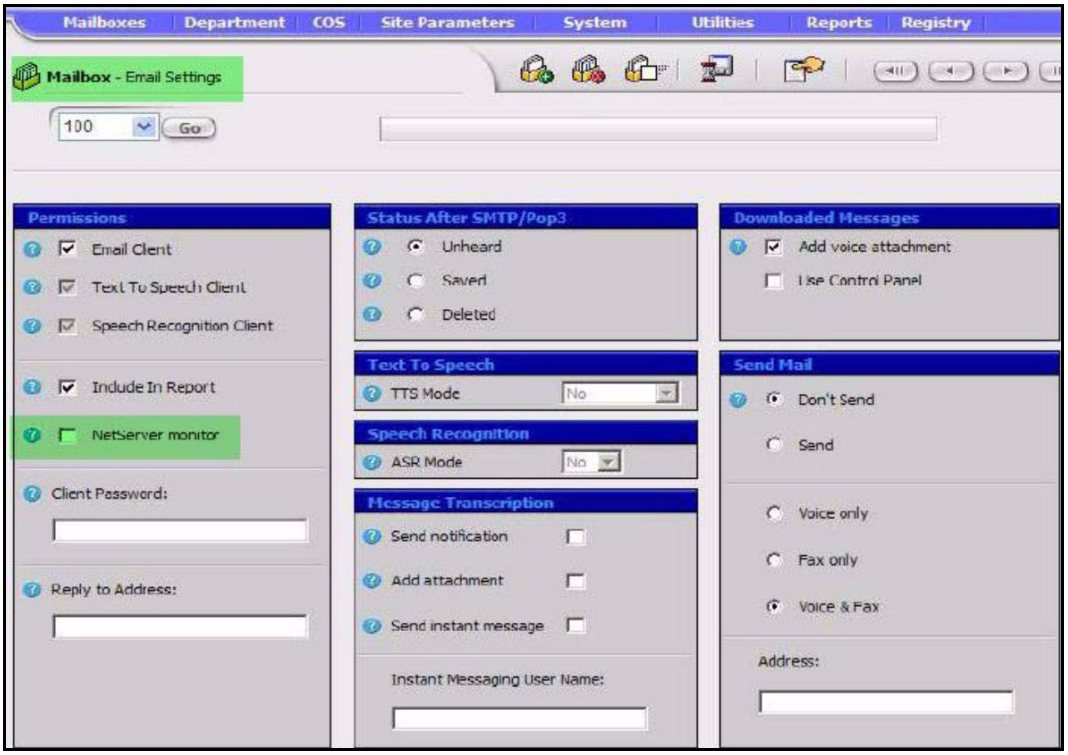
   Netserver Follow me Handoff Application – The Application ID to connect to the Net Server if Follow Me control/hand-off from the phone button is required. The Application ID must match with the one assigned to each phone. Use 80 if “Follow Me” is assigned to a button from the Enterprise Manager.

Mailbox – Email Settings

Assign the Net Server Monitor parameter to the mailbox in Messaging. Log into Enterprise Manager.

1. Log into Enterprise Manager.
2. Select **Application > Messaging**. Select the server.
3. In the Messaging administration screen select **Mailboxes > Email Settings**.

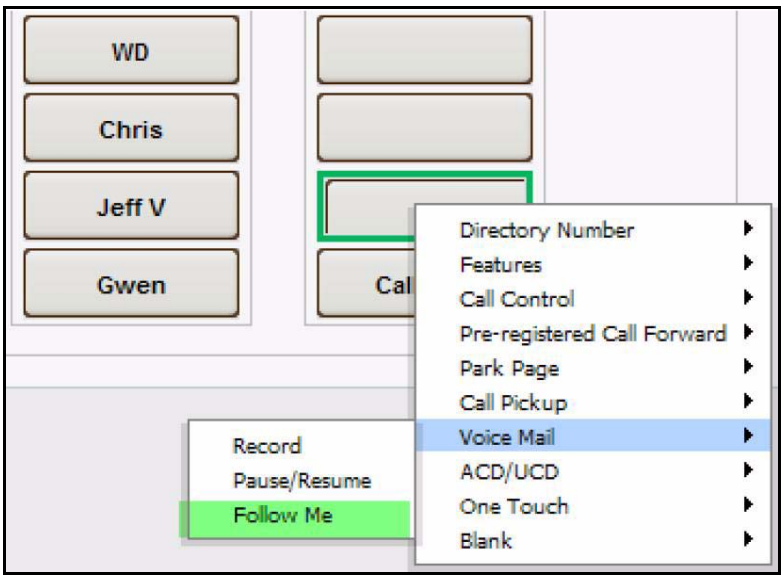
4. **Net Server Monitor** – Check-mark this box if Follow Me control/ hand-off from the phone button is required. In order to use this feature, Net Server on VIPedge or Windows server is required.



Station - Key Assignment

Assign the Follow Me key in either Enterprise Manager Key assignments or through Enterprise Manager Personal Admin.

Select the key, right click, and select Voice Mail, Follow Me, once selected click Save.



Refer to the IPedge Messaging manual for detailed instructions on recording Department prompts, Class Of Service definition, Auto Attendant setup and other features.

Chapter 11 – VALCOM ACCESSORIES

Valcom IP Solutions products can be used to create Internet Protocol (IP) paging systems and a SIP Door Phone. All of the Valcom devices described in this section require the Valcom IP Solution Setup Tool running on a PC that is on the same network as the devices. Download the latest version of the free IP Solutions Setup Tool and the Reference Manual from the Valcom web site: www.valcom.com/vipsetuptool

VALCOM DEVICE SETUP

Device management is accomplished over the data network via Valcom's Windows based programming tool. Network programming is used to adjust individual speaker volume, change system audio groups and other device configuration changes from a centralized location.

Valcom IP Setup Tool

The VIP-102B IP Solutions Tool provides a mechanism to set the IP address via broadcast and/or multicast. After each device has been assigned an IP address, the IP Solutions Tool will be able to retrieve device-specific information and the remaining configuration tasks can be completed.

The general procedure for programming Valcom IP devices involves the following steps:

1. Install the devices on the network.
2. Scan the network using the VIP-102B IP Solutions Tool to create an inventory of the available devices.
3. Program the devices with IP addresses and other network information appropriate to the physical network on which the devices are installed.
4. Re-scan the network to allow the IP Solutions Tool to retrieve complete device configuration information.
5. Configure the individual device settings within the IP Solutions Tool for each device on the network with the specific settings necessary for the paging system being installed.
6. Upload the new configuration to each device from the IP Solutions Tool.
7. Restart the device to enable the new configuration settings.

After the endpoint devices are connected to an appropriately configured network, programming is accomplished through the use of the VIP-102B IP Solutions Setup Tool. This software tool should be installed on a Microsoft Windows® based computer connected to the same network as the Valcom IP devices.

NETWORK REQUIREMENTS

Before attempting to configure the Valcom devices, please ensure the network is configured to support IP paging.

The network should support broadcast and multicast traffic within local subnets and multicast traffic among all subnets where Valcom IP devices are connected. If the network cannot be configured to support these protocols, some features of the IP paging solution may not be available. Please contact Valcom Technical Support for details.

The Valcom IP devices have a factory-default IP address of 192.168.6.200. Because the default IP address is the same for all devices, the devices will conflict with each other when first installed.

Important! These Valcom units will not function behind NAT. They can be used with a Toshiba qualified SIP ALG router such as the Adtran 3120 or 3448.

Network Hardware Requirements	10/100 Mbps Ethernet network
Bandwidth Requirements	86 kbps per active One Way Page
	172 kbps per active Two Way Call
TCP Requirements	Port 21 for FTP access
	Port 23 for Telnet access
	Port 80 for Web based access
UDP Requirements	3 Bi-directional Ports (Factory default 4097, 4098, 4099)
Multicast Requirements	IGMPv3 enabled network
	3 Multicast addresses (Factory defaults: 239.1.1.2, 239.1.1.3 and, 239.1.1.4)
Power requirements for IP speakers	802.3af Power over Ethernet (PoE) compatible network switches or power injectors
Other Suggested settings	Separate VLAN for optimal performance

VIPedge SPECIFIC INFORMATION

In the setup tool use the following:

- Realm = The Fully Qualified Domain Name of the VIPedge server (for example: cp01234567.vipedge.com)
- SIP Server = Leave blank
- Port = 5060
- RTP Port = 20000
- Station = The DN of the SIP station assigned in the VIPedge data base. The VIP-801 will have one DN. The VIP-201 can support up to eight zones of IP paging, each zone will require a DN assignment.

VIPedge systems require a standard user seat for each SIP station or endpoint. Valcom devices require SIP stations.

DOOR PHONE

The VIP-172L - SIP Door Phone is a SIP endpoint. The door phone is an IP Hands-free Talkback intercom with a dial code operated relay. This device requires a single SIP station programmed in the VIPedge system. The door phone can make and receive calls.

Each Valcom VIP-172L - SIP Door Phone requires a standard user seat.

The door phone consists of two physical parts.

- VIP-172L Door plate - The speaker/microphone which mounts near the door. The door-plate is suitable for indoor or outdoor installation.
- Network Interface - Can be wall or table mounted. Power must be supplied by a PoE (802.3af, class 3) switch (or a 802.3af power injector).

The door plate has:

- Single push-button switch to make a call
- LED status indicator
- Relay contact for door lock control

Door Phone Operation

A person pressing the “Call” button on the doorplate receives a confirmation tone or recorded message and the unit initiates a call to the telephone number programmed into the door phone, and the LED on the door plate begins to flash. Note that the telephone number called is programmed into the door phone using the Valcom IP Setup Tool. When the call is answered, a hands-free communications path is established to the door plate, and the LED on the door plate remains lit. The form C relay included with the VIP-172L may be activated by pressing the # key on the answering telephone, with the relay typically being used to activate door entry equipment. When the door phone extension is dialed it will auto-answer.

Note: The Door Phone is a SIP telephone. The telephone number dialed when the Call button is pressed is programmed into the door phone. That number should call a hunt group, multiple calling group, or a paging group in order to help ensure that there is somebody to answer the call from the door phone. If the SIP Door phone is configured to call just one extension, that call may be missed or get routed to voicemail when the phone is unattended, busy, or in Do Not Disturb.

Door Phone Configuration

Information specific to your application will need to be programmed into the VIP-172L using a computer running Valcom’s IP Solution Setup Tool and connected to the same subnet as the VIP-172L. Setup will be done using Valcom’s IP Solution Setup Tool. Download the latest version of the

free IP Solutions Setup Tool from the Valcom web site: www.valcom.com/vipsetuptool

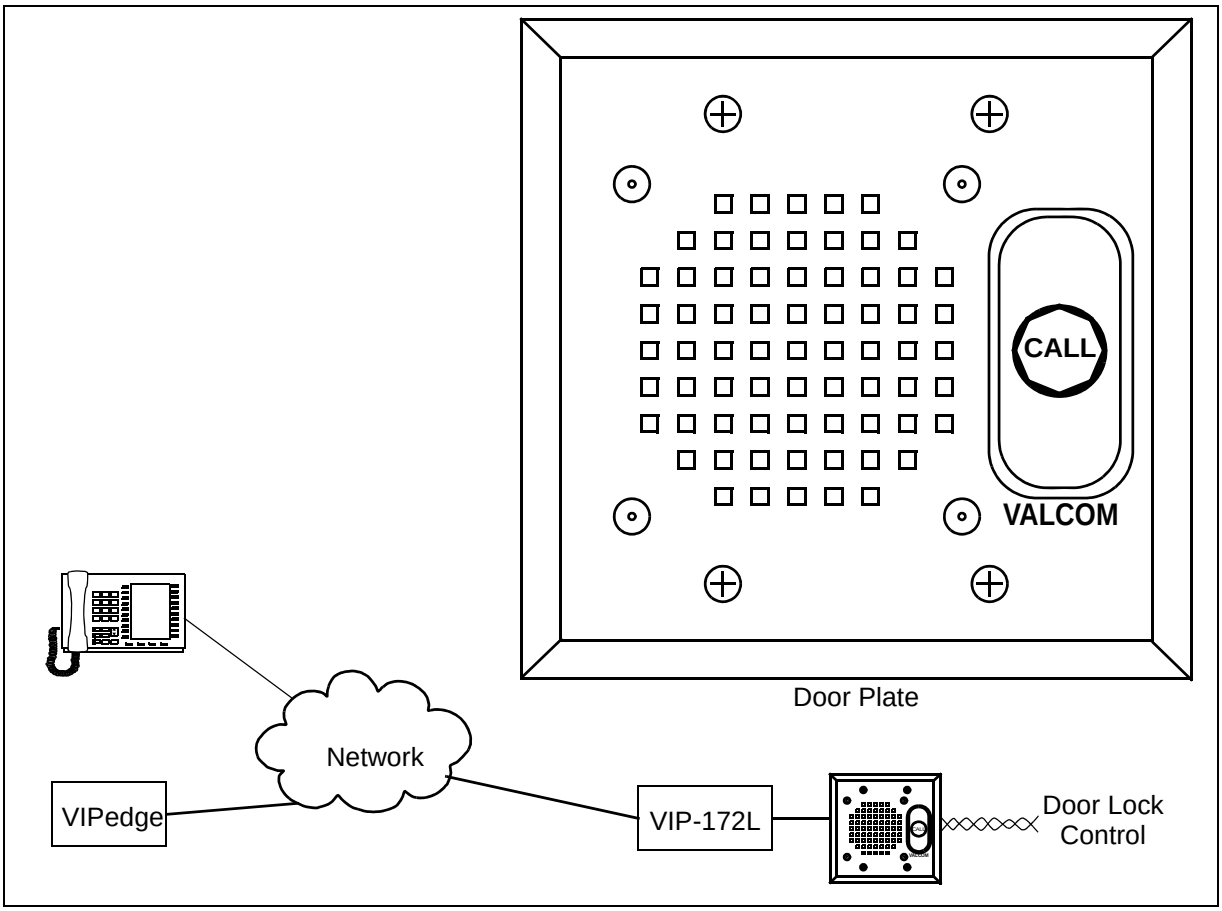


Figure 11-1 Door Phone Plate and Network Diagram

PAGING

The **VIP 801** is a single SIP end point, programmed in the VIPedge as a SIP station and requires a standard user seat. When a call is made to this device the VIP 801 will answer and connect the call to a pair of terminals on the chassis. This provides one zone of one-way paging. The output on the terminals is an analog voice signal for connection to voice paging equipment. The paging equipment can be an amplified speaker, or a paging amplifier.

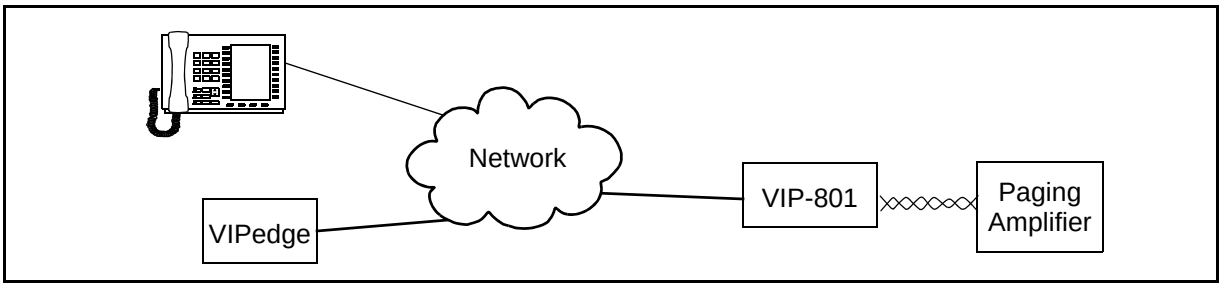


Figure 11-2 VIP 801 Single Paging Port Diagram

The **VIP 201 SIP Paging Gateway** is a rack mount, 1U (1.75 in.) multicast paging server. The VIP 201 can support; one zone of analog paging and eight IP paging groups.

A SIP station in the VIPedge system is required for each paging group used. One standard user seat is required for each station assigned for the VIP 201 gateway. Each channel in the server can be programmed for different functions.

The VIP 201 device has analog paging signaling on output terminals for analog paging equipment. Each server channel can also be programmed to broadcast to one or more IP endpoints.

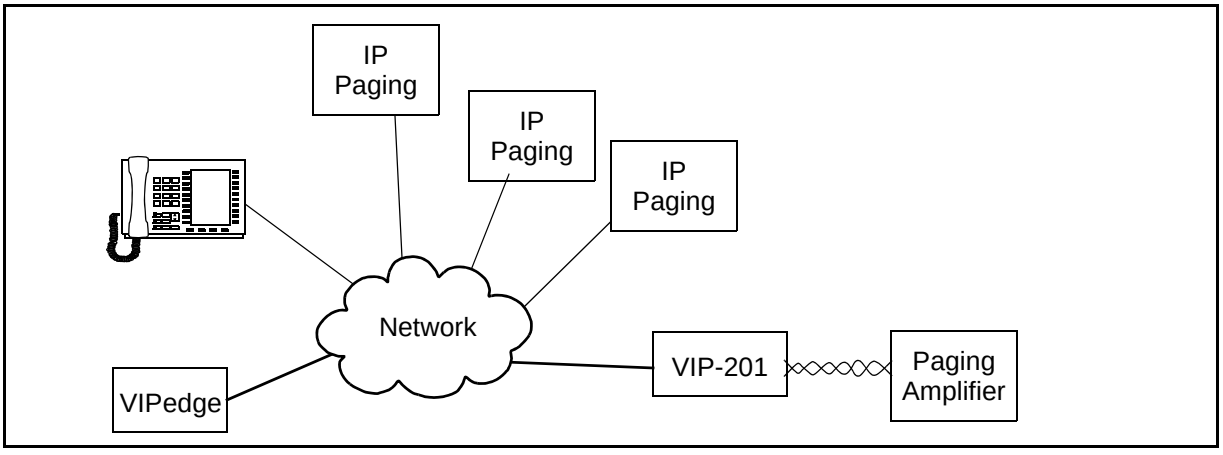


Figure 11-3 VIP 201 Paging Gateway Diagram

VIP 201 Hardware

The preferred method of powering a VIP-201 is via a power over Ethernet switch meeting the 802.3af specification.

If the rear panel barrel connector is used for power, the preferred power supply is a Valcom VIP-324D.

Note: Make all required signal connections before applying power to the unit.

Chapter 12 – Adtran NetVanta 3120 Setup

ADTRAN NETVANTA 3120 SETUP

This procedure is for a router that is already set to the factory default settings, a new router or a router reset to factory default settings. This procedure can also be used for an Adtran NetVanta 3120 router that is already on the network functioning as a firewall. For installed routers already functioning as a firewall go to ADTRAN QoS CONFIGURATION on page 12-11.

New Router Setup

1. Plug in the following:
   WAN cable to the eth0/1 connector
   LAN cable to the Port 1 connector
2. Power up the Router.

Note: The ETH0/1 connector indicators may not light.

3. Set your PC to:
   IP address 10.10.10.10
   Subnet mask 255.255.255.0
4. Launch an internet browser and browse to router at:
   http://10.10.10.1.
   User ID = admin
   Password = password

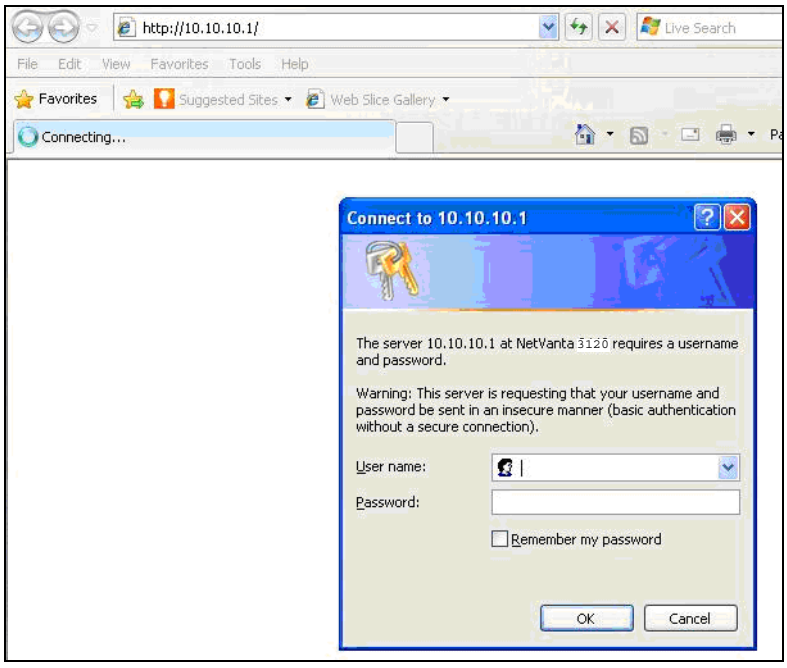
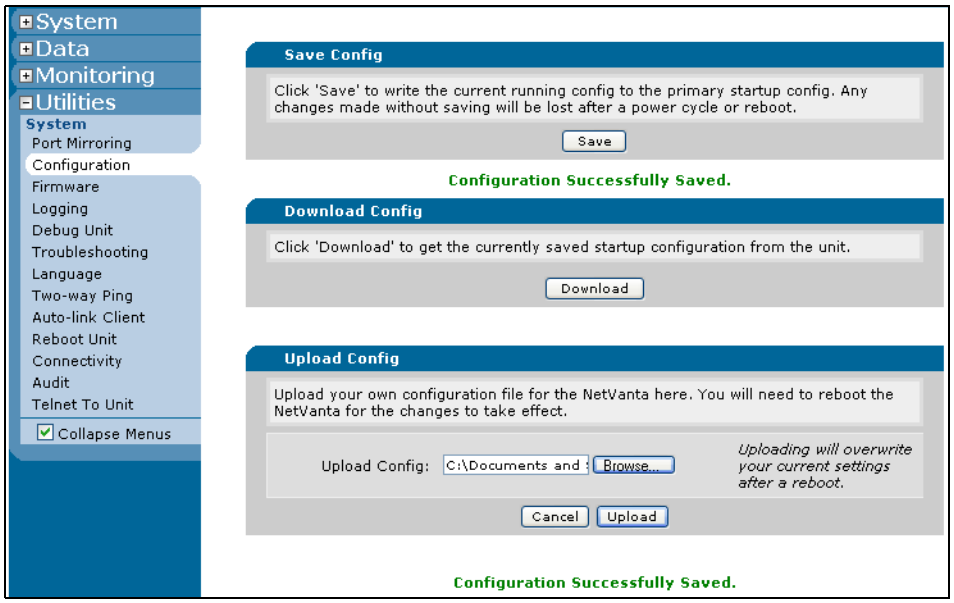


Figure 12-1 Browse to Router http Server

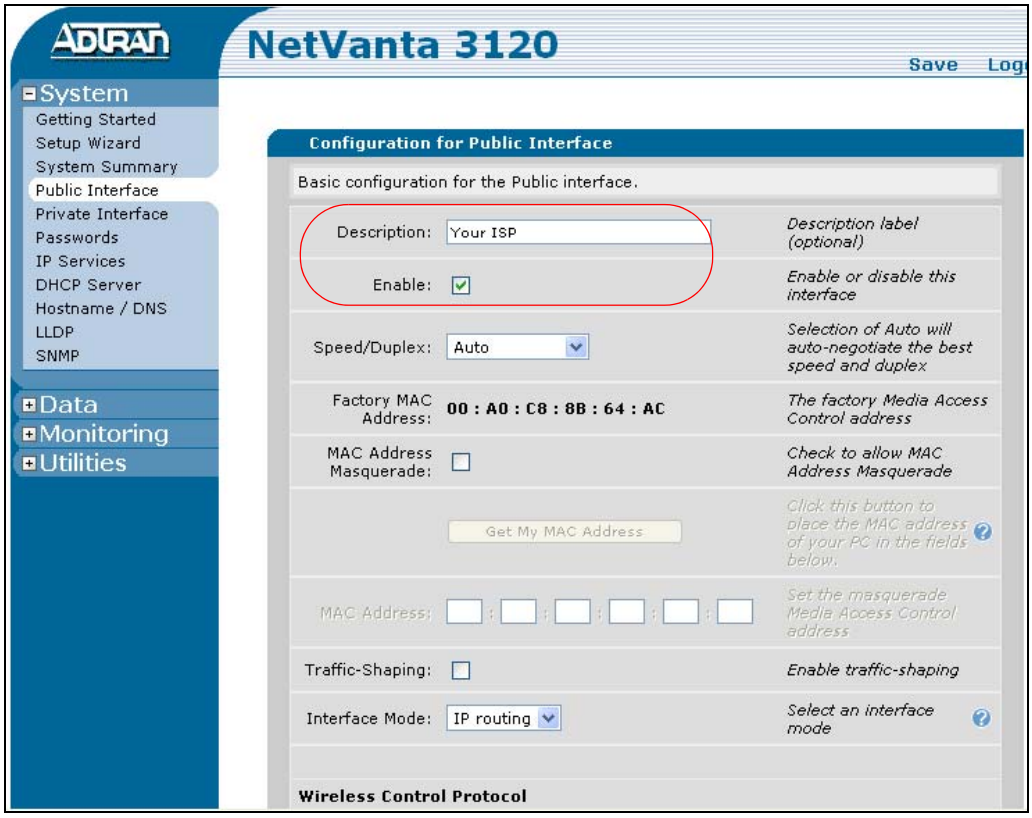
5. In the NetVanta administration menu select **System >Configuration**, click on **Download** to copy the configuration file from the Netvanta unit to your PC.
6. Edit the configuration file on your PC for this installation.
7. In the NetVanta administration menu select **System >Configuration > Upload Configuration**.
8. In the Upload Config area **Browse** to the configuration file on your PC. Click on **Upload**.



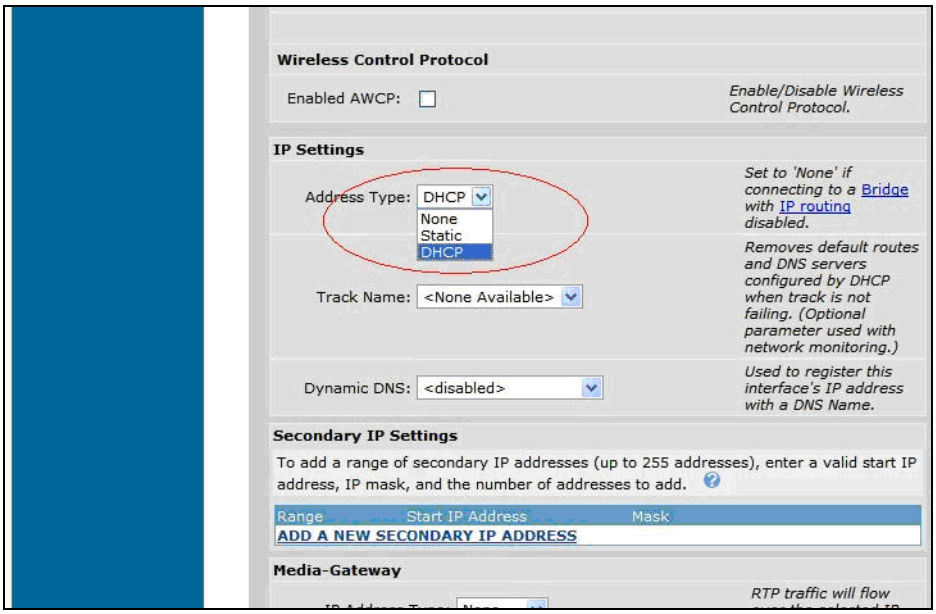
9. When the upload is complete click on **Reboot Now**.
10. Login to the router.

Router Interface Setup

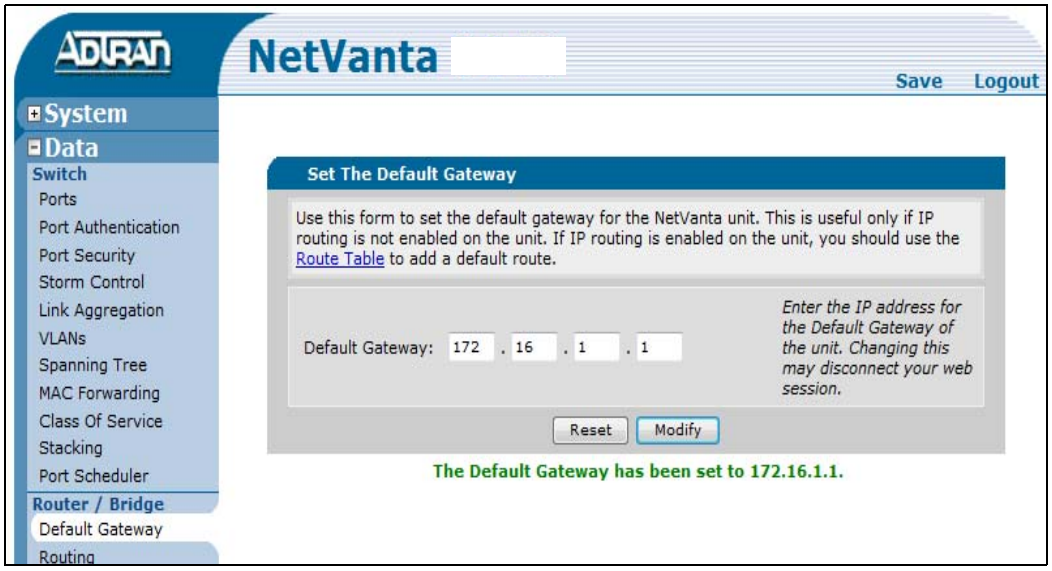
1. Set up the WAN physical Interface. Select **System > Public Interface**. The router will default to DHCP operation.
2. Name the WAN connection. Use a descriptive name.
   Check-mark the **Enable** box
   Ensure that the Wireless Control Protocol, the Enabled AWCP box, is not checked.


NetVanta 3120
Save
System
Getting Started
Setup Wizard
System Summary
Public Interface
Private Interface
Passwords
IP Services
DHCP Server
Hostname / DNS
LLDP
SNMP
Data
Monitoring
Utilities
Configuration for Public Interface
Basic configuration for the Public interface.
Description: Your ISP
Description label (optional)
Enable:
Enable or disable this interface
Speed/Duplex: Auto
Selection of Auto will auto-negotiate the best speed and duplex
Factory MAC Address: 00 : A0 : C8 : 8B : 64 : AC
The factory Media Access Control address
MAC Address Masquerade:
Check to allow MAC Address Masquerade
Get My MAC Address
Click this button to place the MAC address of your PC in the fields below.
MAC Address:
Set the masquerade Media Access Control address
Traffic-Shaping:
Enable traffic-shaping
Interface Mode: IP routing
Select an interface mode
Wireless Control Protocol

3. In the IP Settings, Address Type field select DHCP or Static, check with your service provider.
   If STATIC enter the IP address, Subnet Mask and Default gateway address provided by your ISP then, click on **Apply**.
   If DHCP click on **Apply.**



4. If you selected **DHCP**, scroll down to the IP Status section. Make a note of the Default Gateway Address for use in the next step.
   If you selected **Static** go to the next step.
5. Select **Data > Default Gateway**. Enter the address then, click on **Modify**. Note that the eth 0/1 connector activity indicator should be lit.



6. Select **Data > Route Table**.
   Enter 0.0.0.0 in the Destination Address
   Enter 0.0.0.0 in the Destination Mask

7. Under Gateway click on the **Address** button then, enter the IP address from the Setup section Step 3 (static) or Step 4 (DHCP) then, click on **Add**.

Note: Some of these values may already be set by default.

8. Select **System > DHCP Server**. In the DHCP Pools tab enter a Pool Name then, click on **ADD**. The DHCP Server Pool screen will open. You can enter a name or use Private.
9. In the **Required Configuration** tab Click the **Assign IP address to all DHCP clients on a subnet** radio button.
   Enter Subnet Address: 10.10.10.0
   Enter Subnet Mask: 255.255.255.0
   Under DHCP Options enter Default Gateway: 10.10.10.1

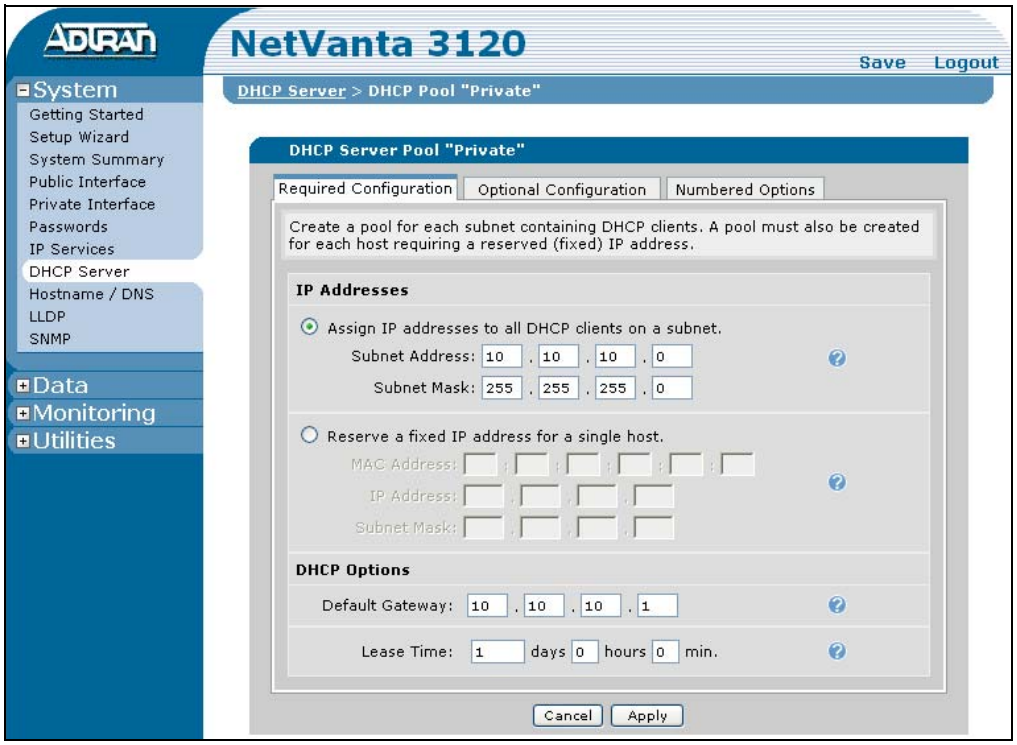
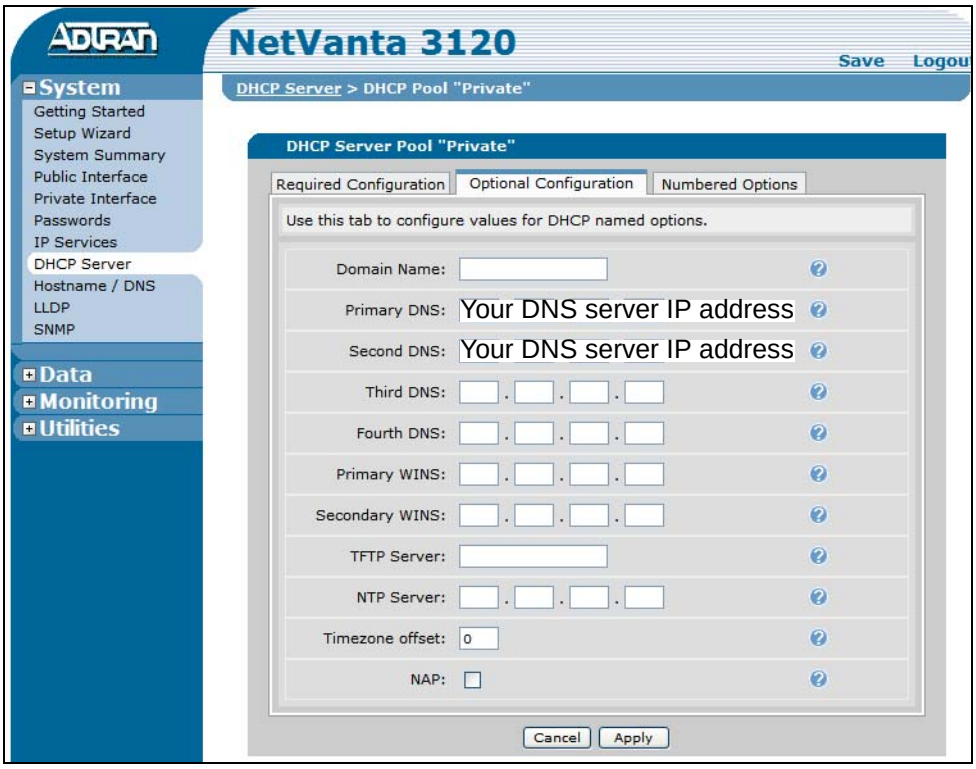


Figure 12-2 DHCP Server Address

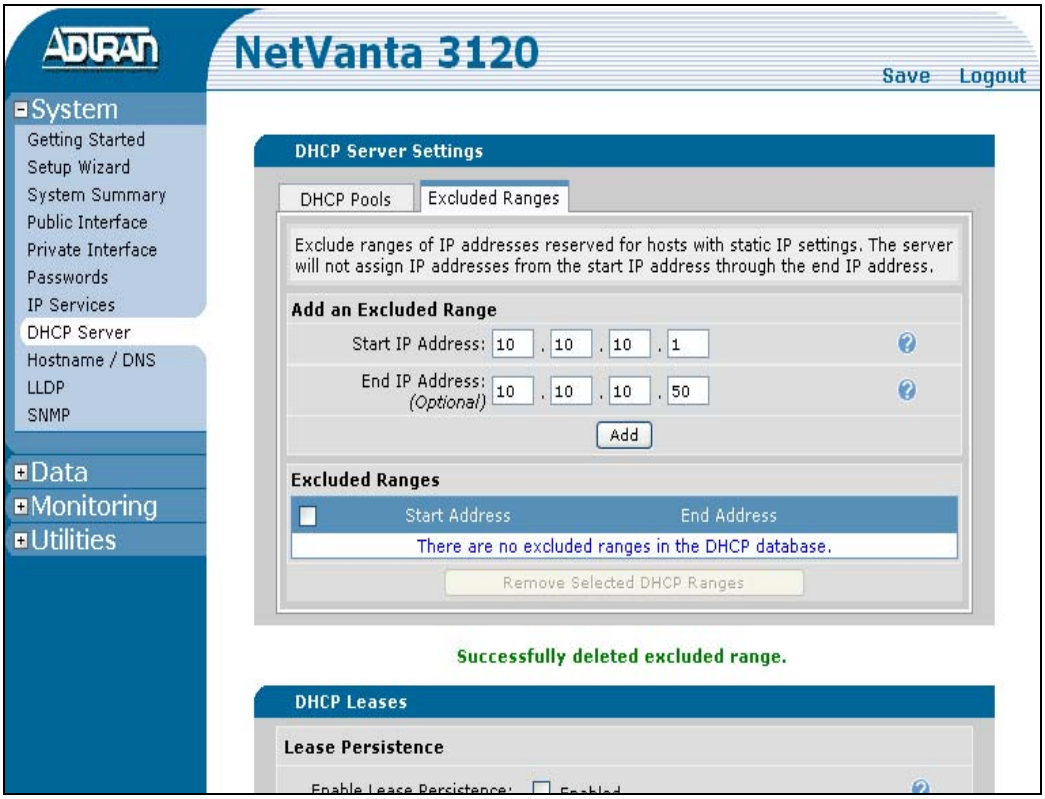
10. Click on the **Apply** button.

Note: If a “Invalid NTP IP address” message appears go to Step 11.

11. In the **Optional Configuration** tab enter the DNS address(es) provided by your Internet Service Provider. Be sure the NTP Sever data fields are empty then, click on **Apply**.



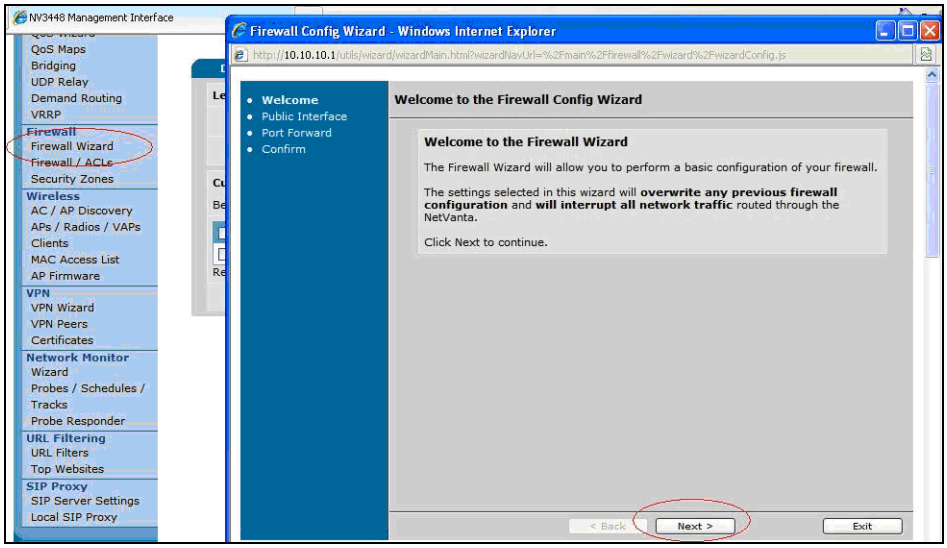
12. Select **System > DHCP** then, select the **Excluded Range** tab. Enter the range of IP addresses that should not given out to DHCP clients. These are IP addresses (typically 50 addresses) you are holding in reserve so that they can be assigned as static address for servers and other devices. Click on **Add**.


NetVanta 3120
Save
Logout
System
Getting Started
Setup Wizard
System Summary
Public Interface
Private Interface
Passwords
IP Services
DHCP Server
Hostname / DNS
LLDP
SNMP
Data
Monitoring
Utilities
DHCP Server Settings
DHCP Pools
Excluded Ranges
Exclude ranges of IP addresses reserved for hosts with static IP settings. The server will not assign IP addresses from the start IP address through the end IP address.
Add an Excluded Range
Start IP Address: 10 . 10 . 10 . 1
End IP Address: (Optional) 10 . 10 . 10 . 50
Add
Excluded Ranges
Start Address
End Address
There are no excluded ranges in the DHCP database.
Remove Selected DHCP Ranges
Successfully deleted excluded range.
DHCP Leases
Lease Persistence

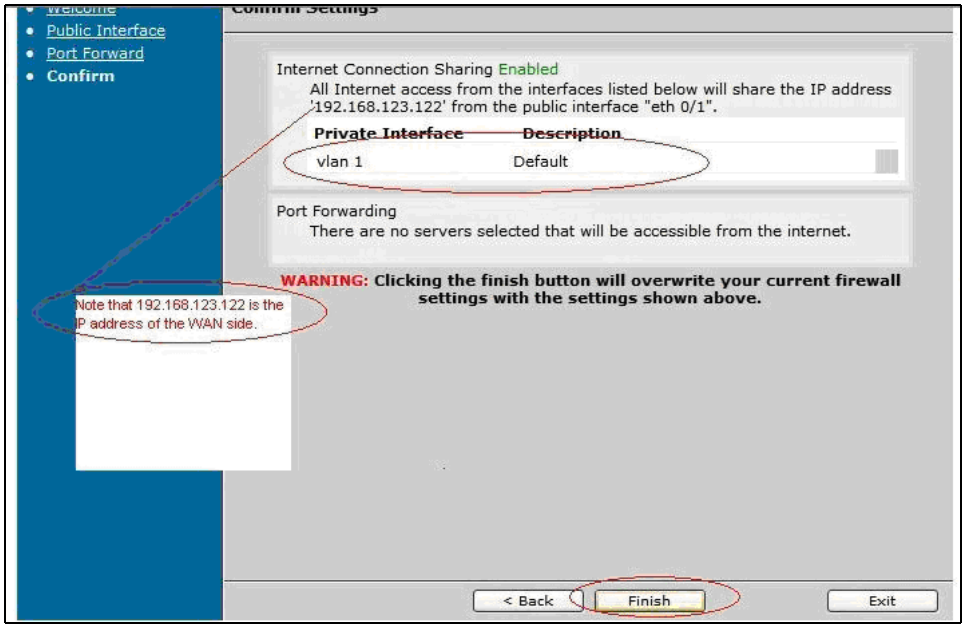
SETUP THE FIREWALL

Use the Adtran Wizard to the setup the firewall.

1. Select **Data > Firewall Wizard** from the Adtran menu. Then click on **Next**.

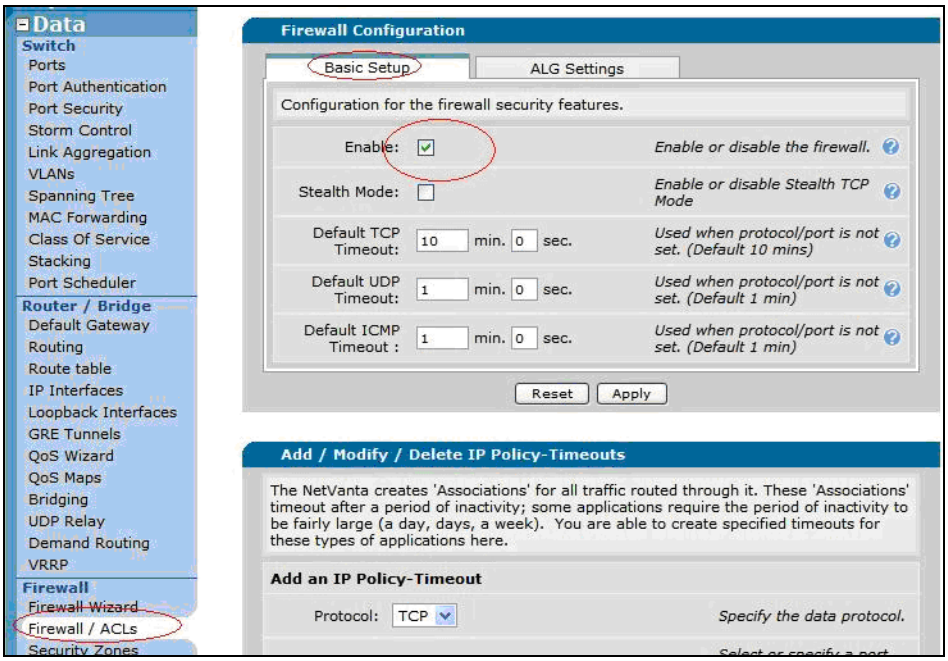


2. Select the **eth0/1** interface from the pull-down list in the Interface field then, click on **Next**.
3. Click on the radio button for: **No**, I don't have any servers that need to be accessed from the internet. Then click on **Next**.
4. Click on **Finish**.

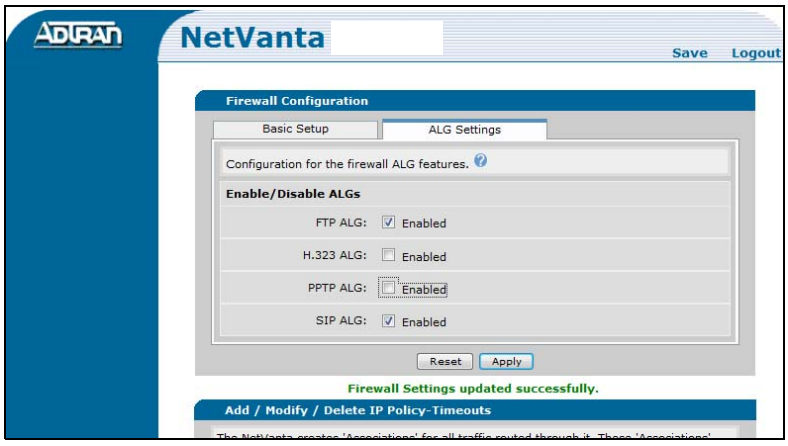


5. The router LAN IP address is set as the Default Gateway for the LAN subnet automatically.
6. When the wizard is complete click on **Exit**.

7. Select **Data > Firewall/ACLs**. In the Basic Setup tab check-mark the firewall security **Enabled** box.

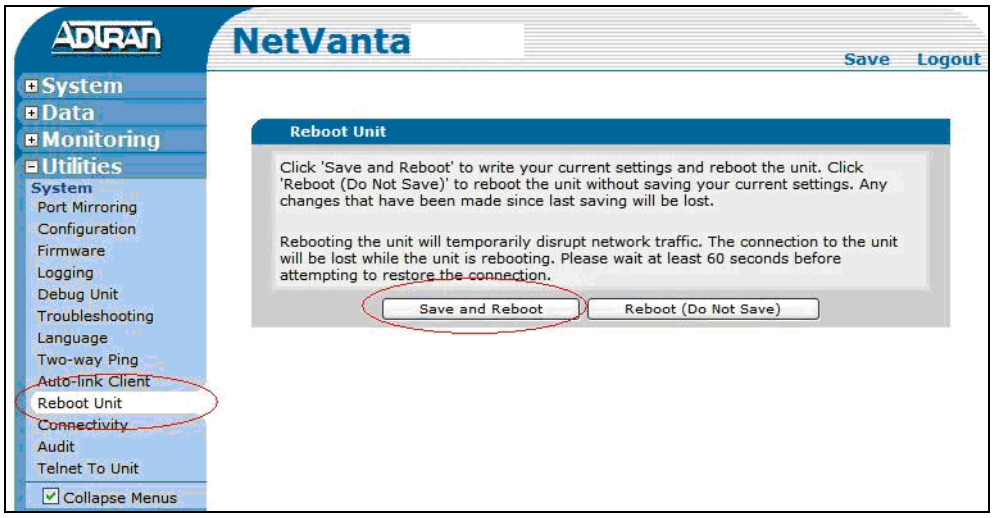


8. In the ALG Settings check-mark the **FTP ALG** and **SIP ALG** boxes. Ensure that all others are off.



9. Click on the **Apply** button.

10. Select Utilities > Reboot unit. Click on **Save and Reboot**.



11. Set your PC to use DHCP.
12. Verify that you can access the internet.

ADTRAN QoS CONFIGURATION

1. Login to the Adtran NetVanta Router.
2. Define WAN bandwidth subscribed from Internet Service Provider (ISP). Select **Data > IP Interfaces**.

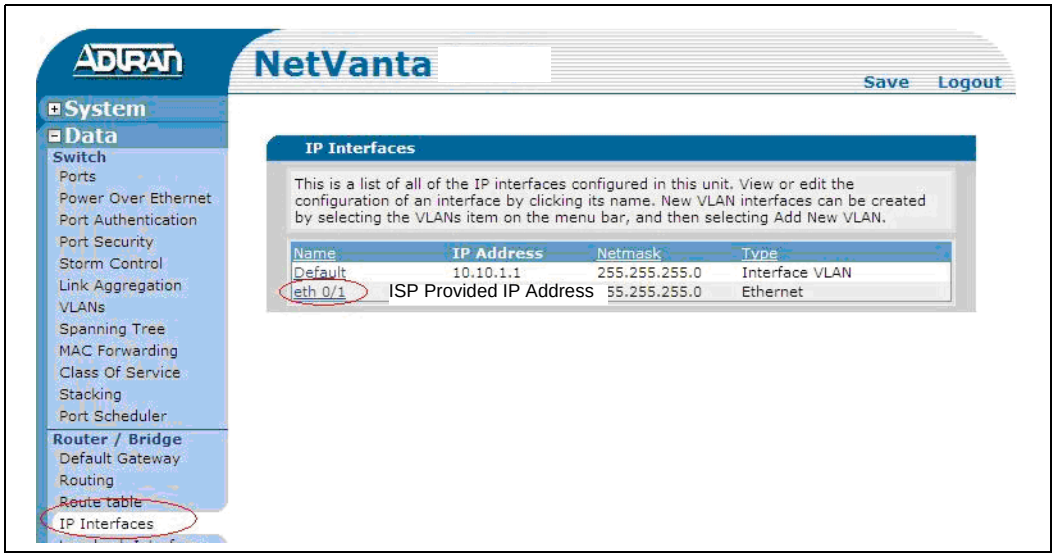


Figure 12-3 Select WAN Interface

3. Click on **eth 0/1**.
4. Specify the bandwidth that was subscribed from the ISP. In the example shown in Figure 12-4 the data rate is 1.5Mbps. This is the **uplink** rate. Check mark the **Traffic-Shaping** box then, enter the data rate in the **Traffic-shaping** rate field.

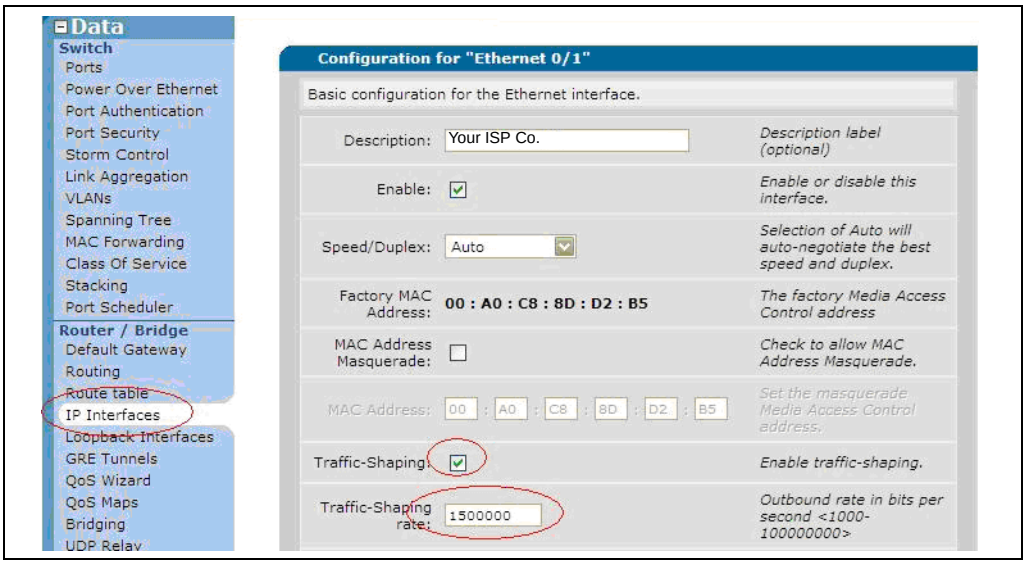


Figure 12-4 Enter the ISP Data Rate (1.5Mbps shown in this example)

5. Scroll down to click on the **Apply** button.

6. Create matched Access Control Lists (ACL) for Inbound and Outbound QoS Maps. At the bottom of the screen, select **Data > Firewall / ACLs**. Click on the **Configure ACL** button.

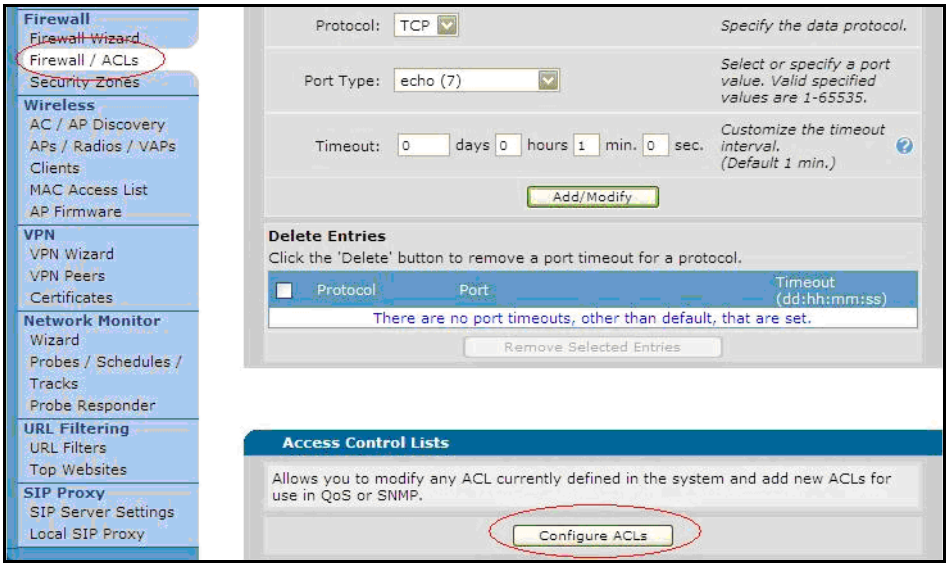


Figure 12-5 Define Matched Rules For QoS Map

7. If you have uploaded the Configuration File you can go to Traffic Class Queuing on page 12-16.

8. Create an ACL for VoIP ports and another ACL for data ports. Enter a name that describes the application for the new ACL (VoIP-Out) into the ACL Name field. Then click on the **Add New ACL** button.

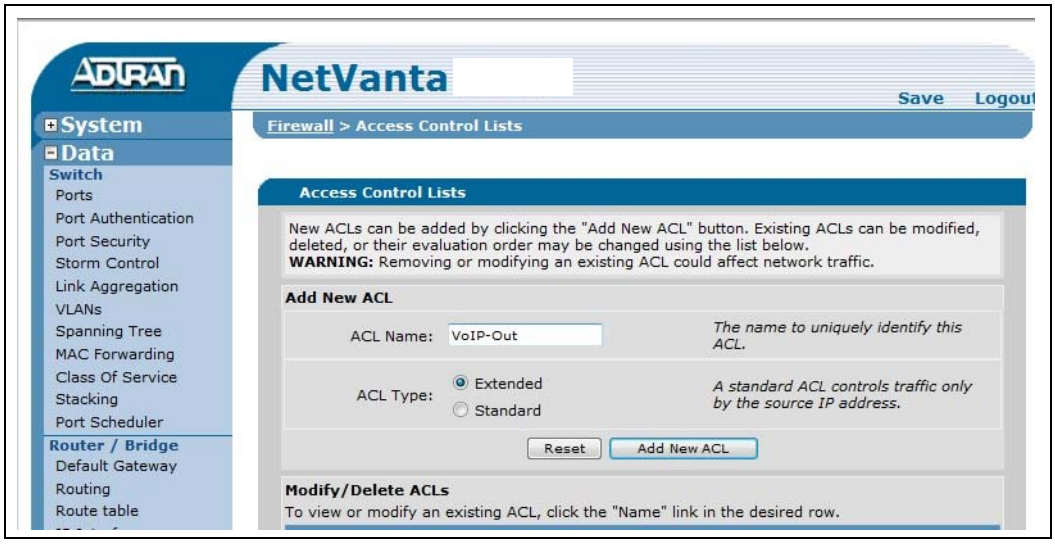


Figure 12-6 Enter a Descriptive ACL name (this example is the VoIP ACL)

9. In the dialog box click on the **Add New Traffic Selector ...** button.

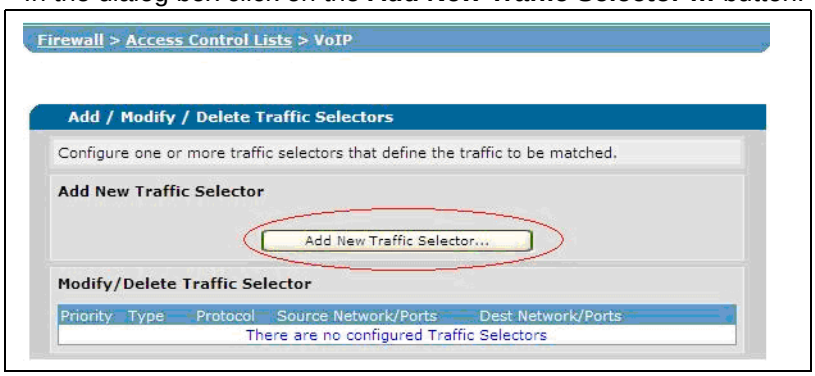


Figure 12-7 Add Traffic Rules to VoIP ACL

10. Set the ports and the protocol to allow the ports shown below in the table. Set:
Filter Type to Permit
Protocol to (value from the table)
Destination Data in the Destination Ports area, select **Specified**, select Equal to for a single port or Range for a range of ports. Enter the port(s). Then, click on **Apply**.

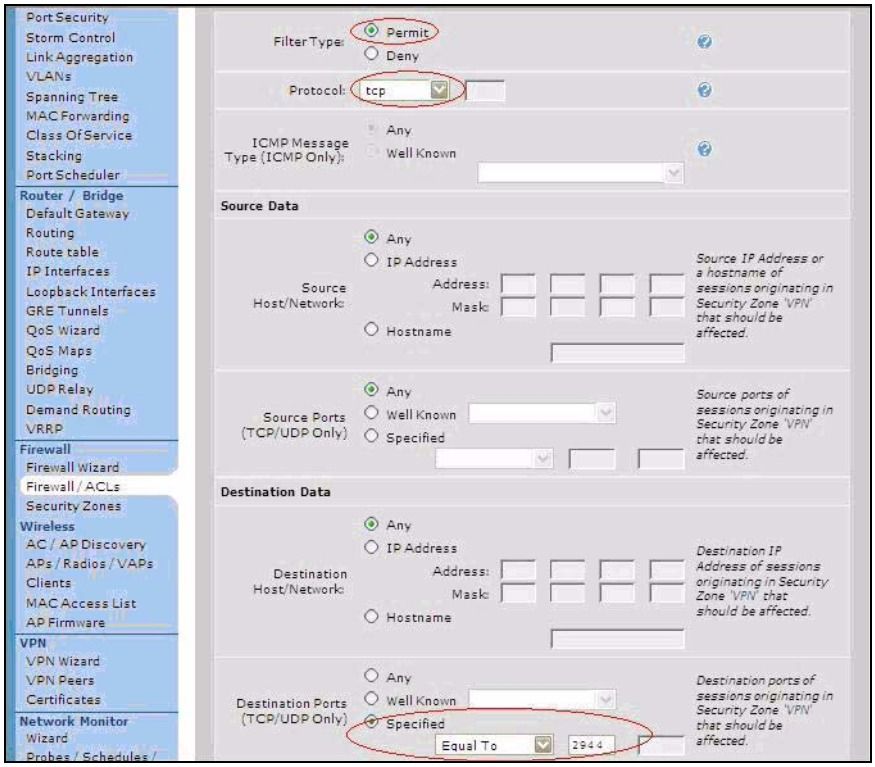


Figure 12-8 Permit Traffic to VoIP ACL (Example: TCP traffic on port 2944 is allowed)

Allow the following ports:

Protocol	Source Data	Destination Data	Use
UDP	Any	5060	Only for SIP telephones
Messaging	1007	TCP	Use by the System monitor Applet
	1008	TCP	Fax printer driver and Email Callback app
UDP	Any	1718~1719	IPTs
TCP	Any	2944	IPTs
TCP	Any	8446	IPTs
UDP	Any	27000~27399 (up to 60 users) 27000~28903 (more than 60 users)	RTP
UDP	49152~49154	Any	RTP

11. Repeat Step 9 and Step 10 to setup all of the ports shown in the table above.

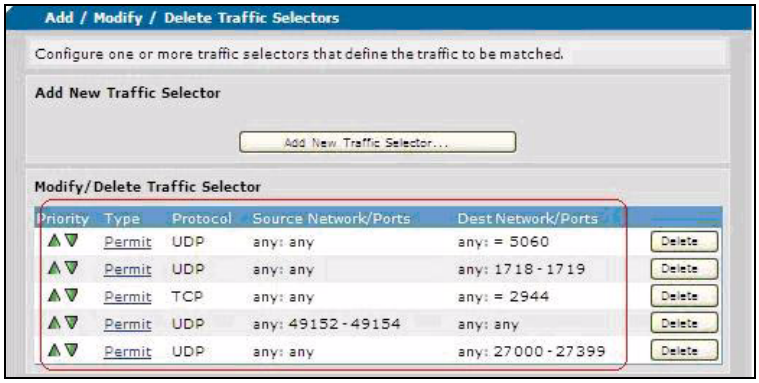


Figure 12-9 Permitted Ports for Outbound VoIP (example)

Create LAN to WAN QoS Maps

12. Select **Data > QoS Maps** enter 'VIPedgeQoS' as the Map Name. Enter Sequence Number 10.

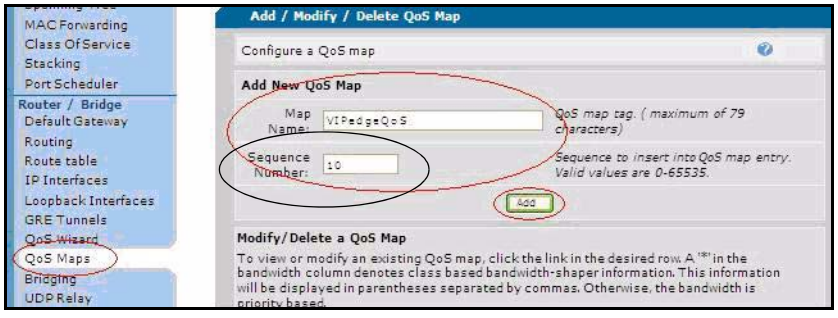
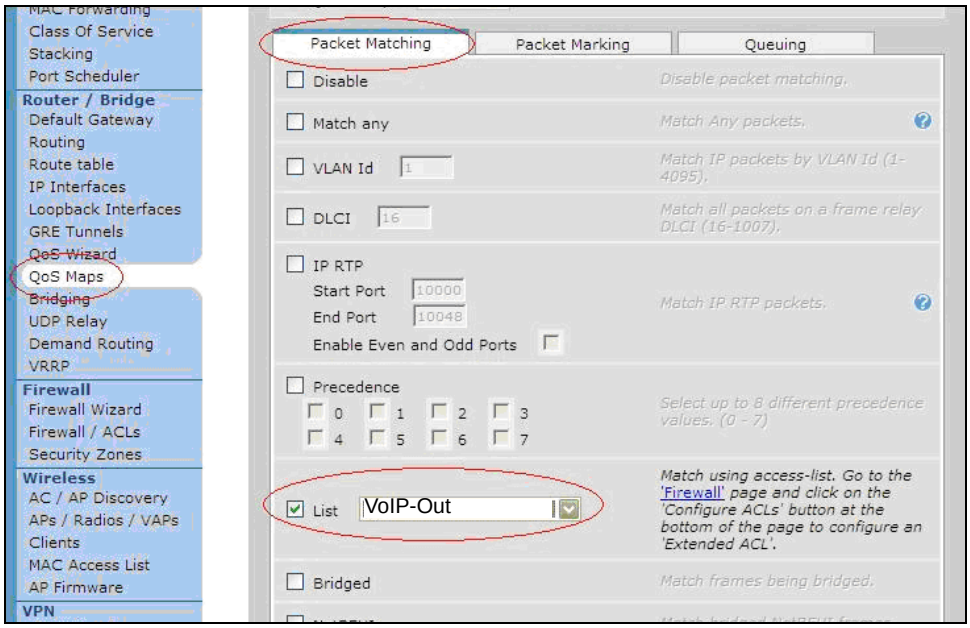


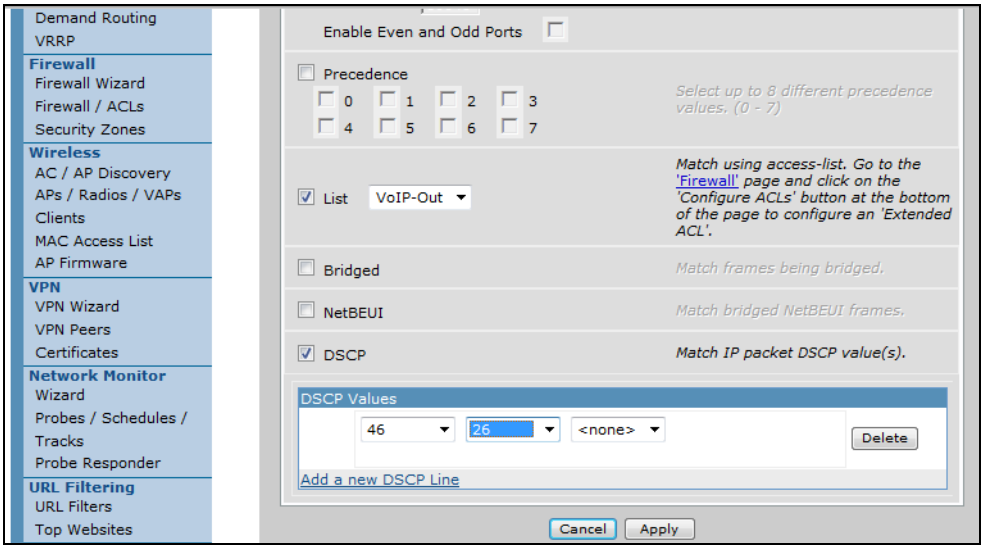
Figure 12-10 Create Outbound "VIPedgeQoS" for VoIP

13. Click on **Add**.

14. In the Packet Matching tab check-mark the box **List** and select **VoIP-Out**.



15. Scroll down to check-mark the **DSCP** box. Click on **Add a new DSCP line**.



16. In the DSCP Values field enter **46, 26** then, click on **Apply**.

Traffic Class Queuing

17. Click on the QoS map you just created in Step 12. Click to select **Traffic Class Queuing**. Under Shaping click to check-mark the **Average** box.

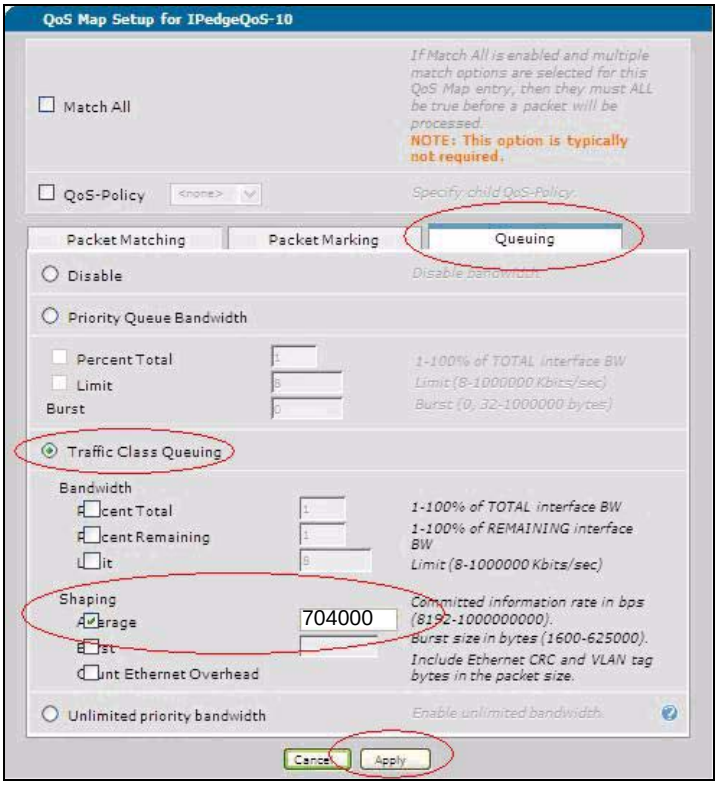


Figure 12-11 Create outbound QoS "VIPedgeQoS"

Queuing

18. The Adtran NetVanta router will reserve 25 percent of the bandwidth for system critical functions.

    In this example the ISP provided a 1.5 Mbps connection. The router will reserve 25 percent of the 1500000 bps = 375000. That leaves 1250000 bps.

19. Multiply the number of VoIP channels by 88000 bps. Enter this value in the Committed information rate field. For example, if the system has 8 channels the calculation would be: 8 x 88000 = 704000.

    Note: If this number is greater than the number calculated in Step 18 you will need an ISP connection with a higher data rate.

20. Click on **Apply**.

21. Select **Data > QoS Maps**. Scroll down to the QoS-policy assignment and statistics area. On the eth 0/1 line in the Outbound QoS-policy column select VIPEDGQoS (the name assigned in Step 12.

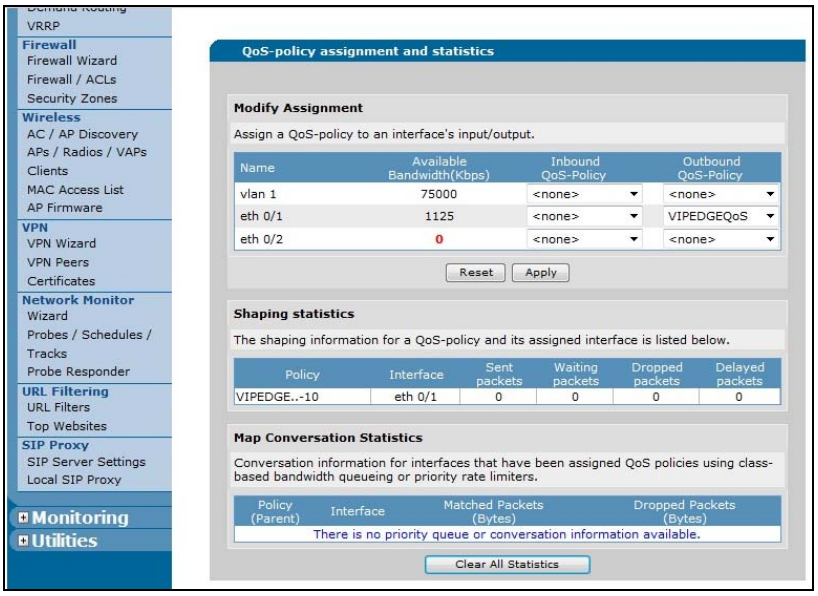


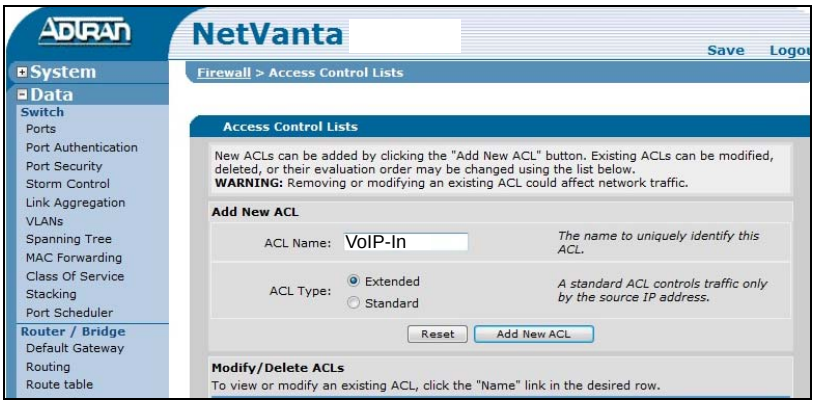
Figure 12-12 Configure Outbound QoS Map "VIPEDGEQoS"

22. If you uploaded a Configuration File you can go to VIPedge CONFIGURATION on page 12-19.

WAN to LAN Configuration

These steps configure the VoIP-In parameters.

1. Select **Data > Firewall/ACLs**. Click on **Configure ACLs**.
2. Enter VoIP-In as the **ACL Name**. Set **ACL Type** to Extended. Enter VoIP-In in the ACL Name field.



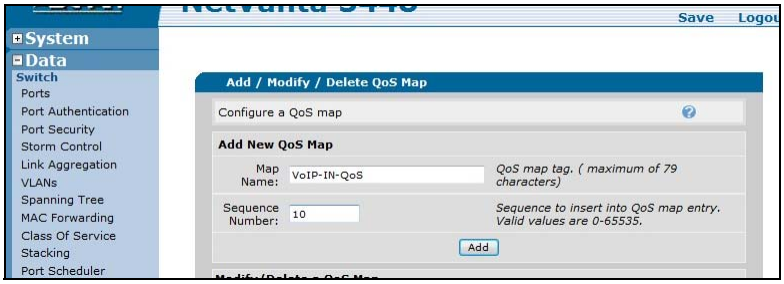
3. Click on **Add New ACL**.
4. In the dialog box click on the **Add New Traffic Selector…** button.

5. In the Firewall/ACL screen select Filter Type as **Permit**.
   In the Protocol field select **udp**.
   In the Source Data section select **Any**.
   For Source Ports select **Specified** then, select **Range.**

   Enter the range of **27000** to **27399** (up to 60 users) or
   Enter the range of **27000** to **28903** (over 60 users).

   Click on **Apply**.

6. Select **Data > QoS Maps**. Enter the map name: **VoIP-In-QoS**
   Set the Sequence Number to **10**.



7. Click on **Add**.
8. In the Packet Matching tab:
   Check-mark the **List** box and select **VoIP-In**.
9. Check-mark the **DSCP** box. In the DSCP values click on **Add a new DSCP Line**, select **46** and **26**.
10. In the Packet Marking tab select **DSCP** then enter **46**.
11. Click on **Apply**.
12. Select **Data > QoS Maps**. Scroll down to click on **eth 0/1 Inbound Policy**. Select **VIPEDGEQoS**, vlan VoIP-In-QoS.
13. Click on **Apply**.

VIPedge CONFIGURATION

1. Login to the VIPedge call processor Enterprise Manager.
2. Select **System > System IP Data**.
3. Set the following parameters. Refer to Figure 12-13.
   Diffserv: Enable
   TOS Field Type: DSCP
   DSCP: 46

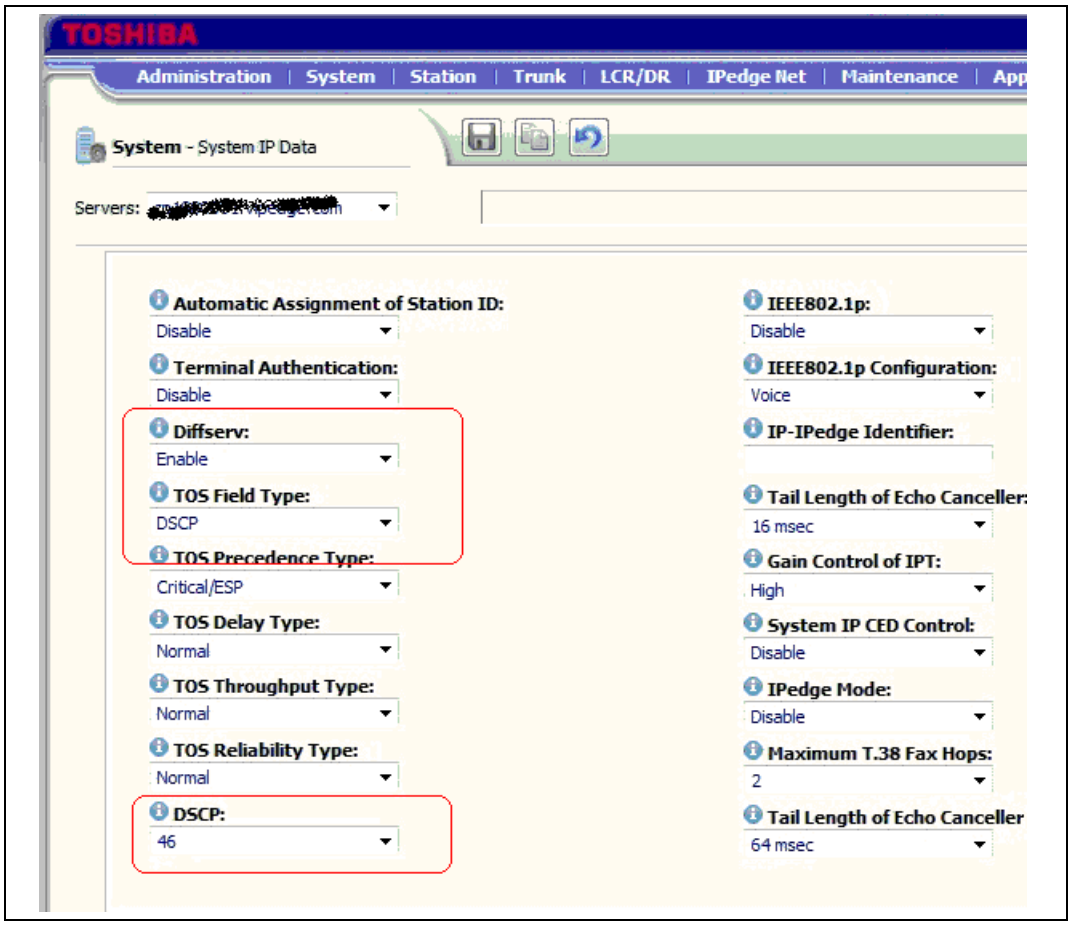


Figure 12-13 Setup IPT Traffic for Diffserv and DSCP 46

NETWORK SECURITY

Change the User Name and Password of your NetVanta router. Record the new login information in a secure location.

NETWORK CONFIGURATIONS

The following diagrams show three different network topologies. The recommended configuration is shown in Figure 12-14.

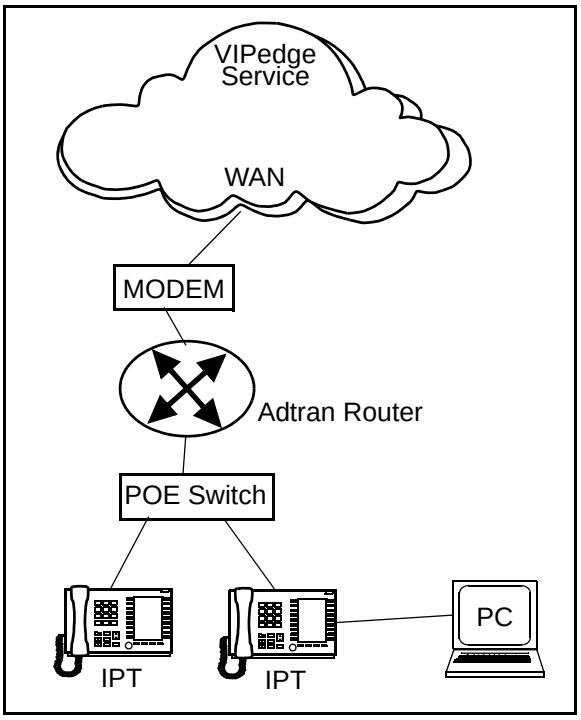


Figure 12-14 Recommended Network Topology

The network configuration shown on the left side of Figure 12-15 is functional but not optimum. The network configuration shown on the right side of the figure is not acceptable.

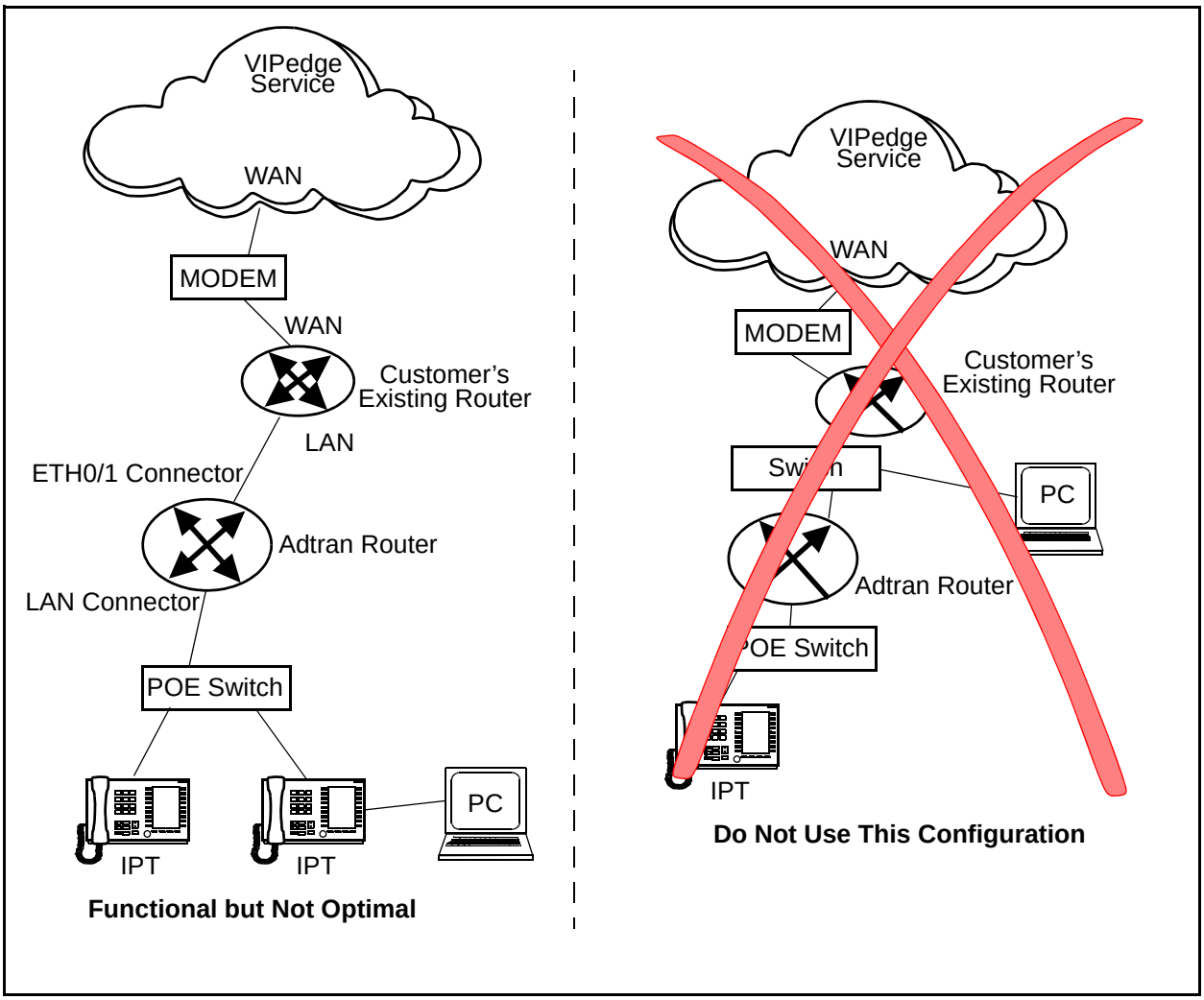


Figure 12-15 Other Network Topologies

This page is intentionally left blank.

Chapter 13 – Adtran NetVanta 3448 Setup

ADTRAN NETVANTA 3448 SETUP

This procedure is for a router set to the factory default settings, a new router or a router reset to factory default settings. This procedure can also be used for an Adtran NetVanta 3448 router that is already on the network functioning as a firewall. For installed routers already functioning as a firewall go to ADTRAN QoS CONFIGURATION on page 13-11.

New Router Setup

1. Plug in the following:
   WAN cable to the eth0/1 connector
   LAN cable to the Port 1 connector
2. Power up the Router.

Note: The ETH0/1 connector indicators may not light.

3. Set your PC to:
   IP address 10.10.10.10
   Subnet mask 255.255.255.0
4. Launch an internet browser and browse to router at:
   http://10.10.10.1.
   User ID = admin
   Password = password

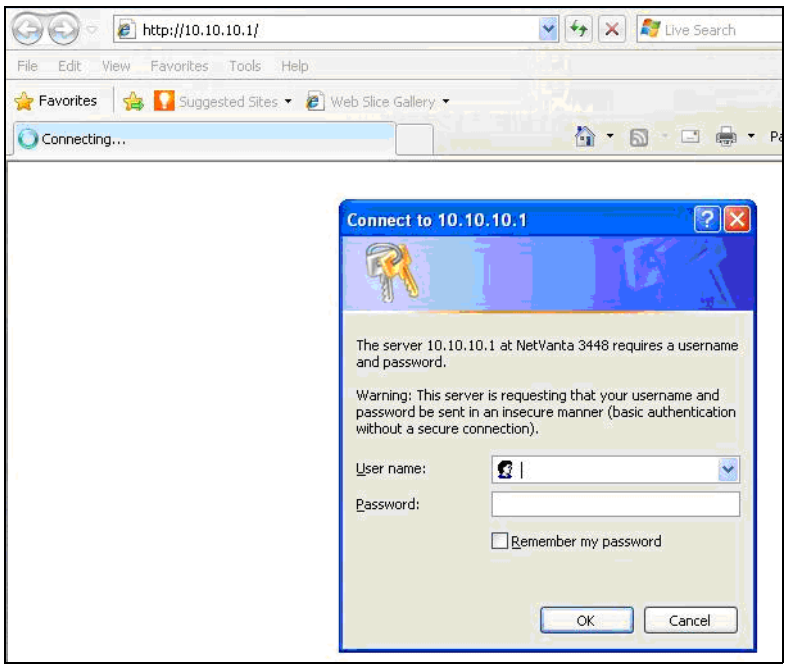
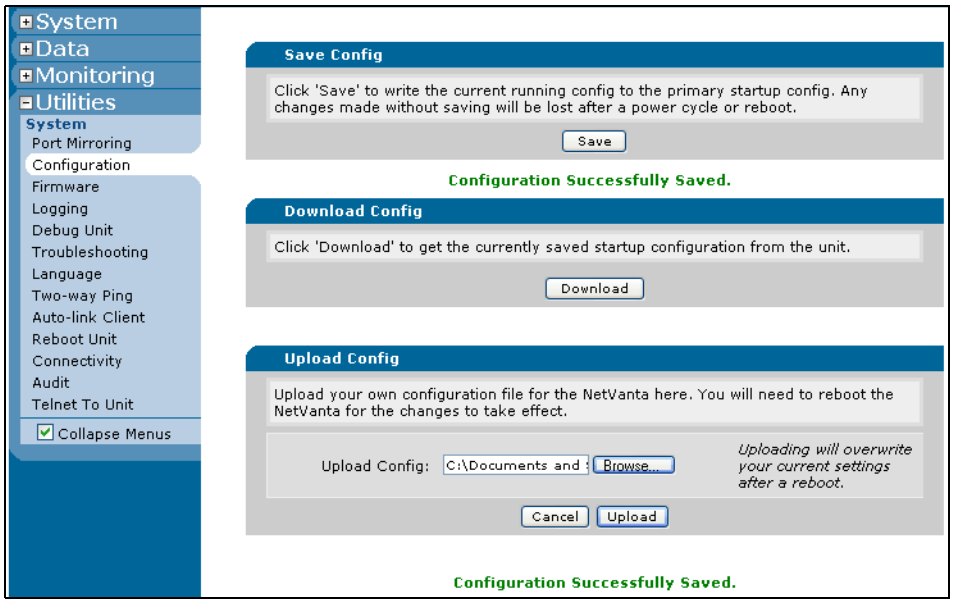


Figure 13-1 Browse to Router http Server

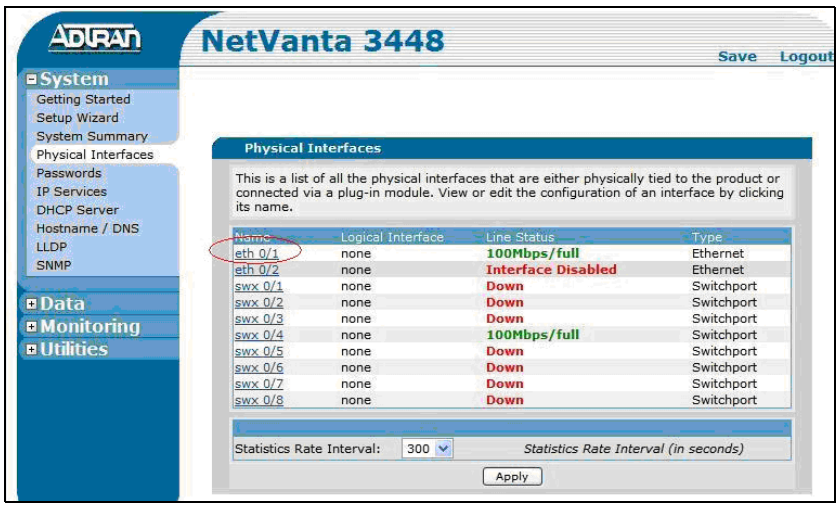
5. In the NetVanta administration menu select **System >Configuration**, click on **Download** to copy the configuration file from the Netvanta unit to your PC.
6. Edit the configuration file on your PC for this installation.
7. In the NetVanta administration menu select **System >Configuration > Upload Configuration**.
8. In the Upload Config area **Browse** to the configuration file on your PC. Click on **Upload**.



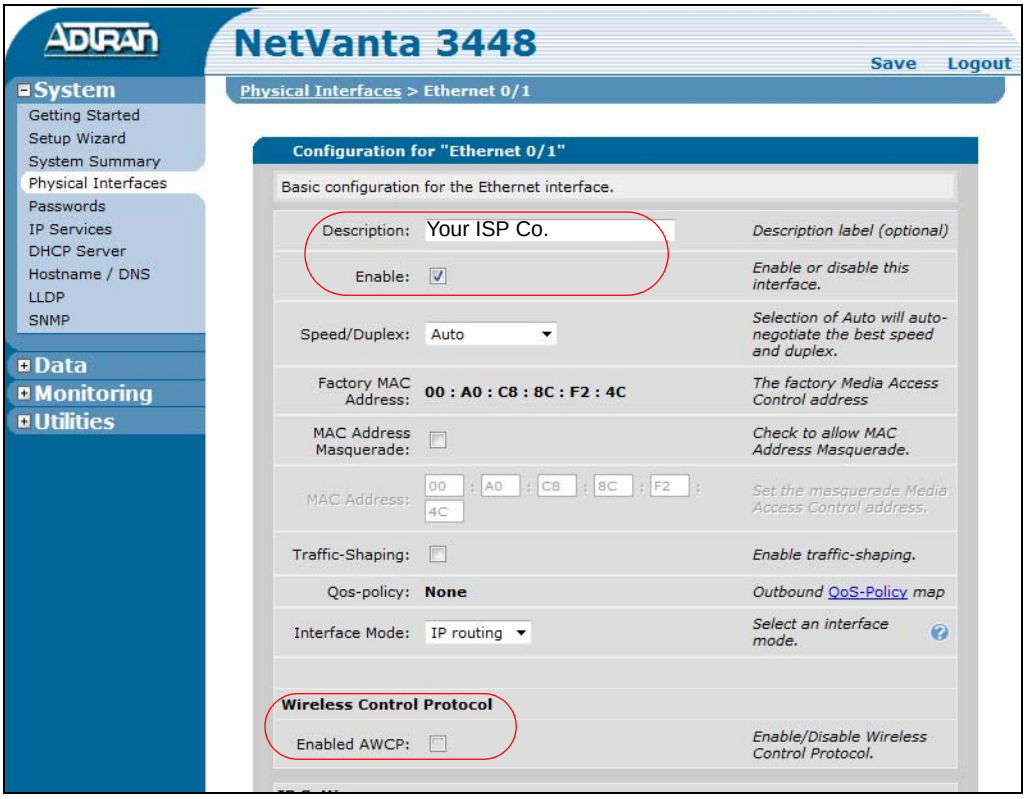
9. When the upload is complete click on **Reboot Now**.
10. Login to the router.

Router Interface Setup

1. Set up the WAN physical Interface. Select **System > Physical Interfaces**. Click on eth 0/1.

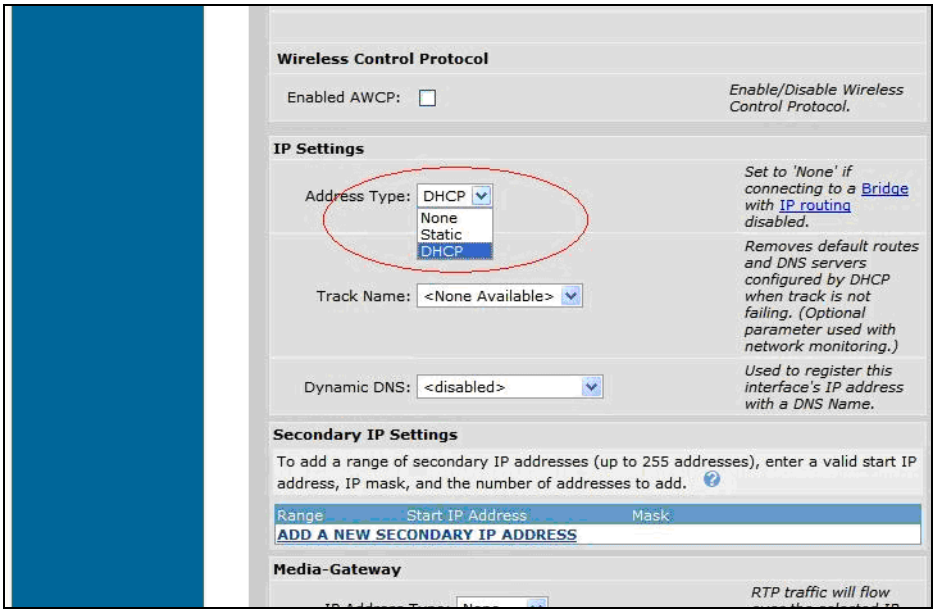


2. Name the WAN connection. Use a descriptive name.
   Check-mark the **Enable** box
   Ensure that the Wireless Control Protocol, the Enabled AWCP box, is not checked.

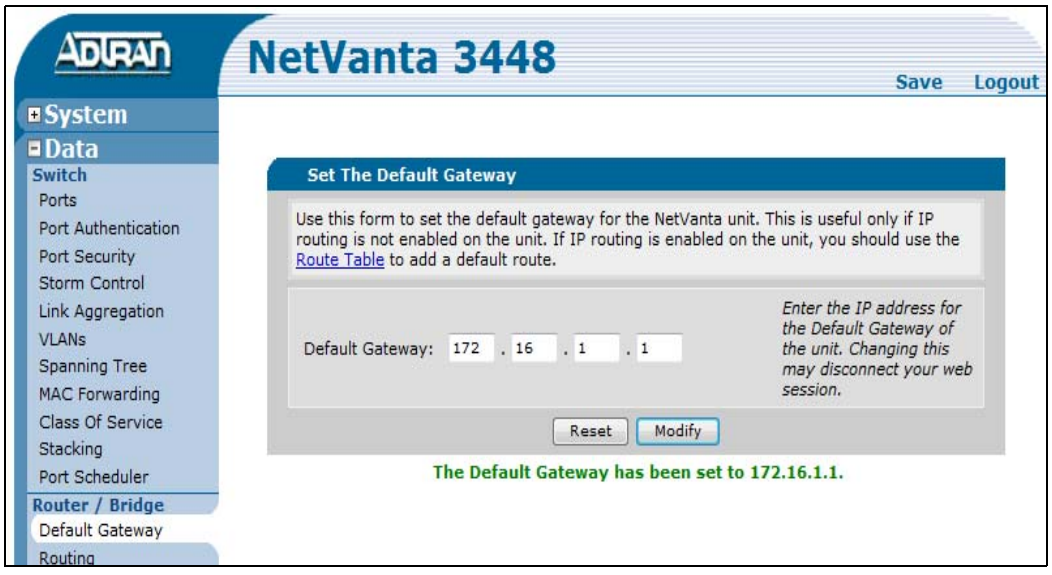


3. In the IP Settings, Address Type field select DHCP or Static, check with your service provider.
   If STATIC enter the IP address and Subnet Mask provided by your

ISP then, click on **Apply**.
If DHCP click on **Apply.**



4. If you selected **DHCP**, scroll down to the IP Status section. Make a note of the Default Gateway Address for use in the next step.
   If you selected **Static** go to the next step.
5. Select **Data > Default Gateway**. Enter the address then, click on **Modify**. Note that the eth 0/1 connector activity indicator should be lit.



6. Select **Data > Route Table**.
   Enter 0.0.0.0 in the Destination Address
   Enter 0.0.0.0 in the Destination Mask
7. Under Gateway click on the **Address** button then, enter the IP address from the Setup section Step 3 (static) or Step 4 (DHCP) then, click on **Add**.

8. Select **System > DHCP Server**. In the DHCP Pools tab enter a Pool Name (for example; Private) then, click on **ADD**. The DHCP Server Pool screen will open.
9. In the **Required Configuration** tab Click the **Assign IP address to all DHCP clients on a subnet** radio button.
   Enter Subnet Address: 10.10.10.0
   Enter Subnet Mask: 255.255.255.0
   Under DHCP Options enter Default Gateway: 10.10.10.1

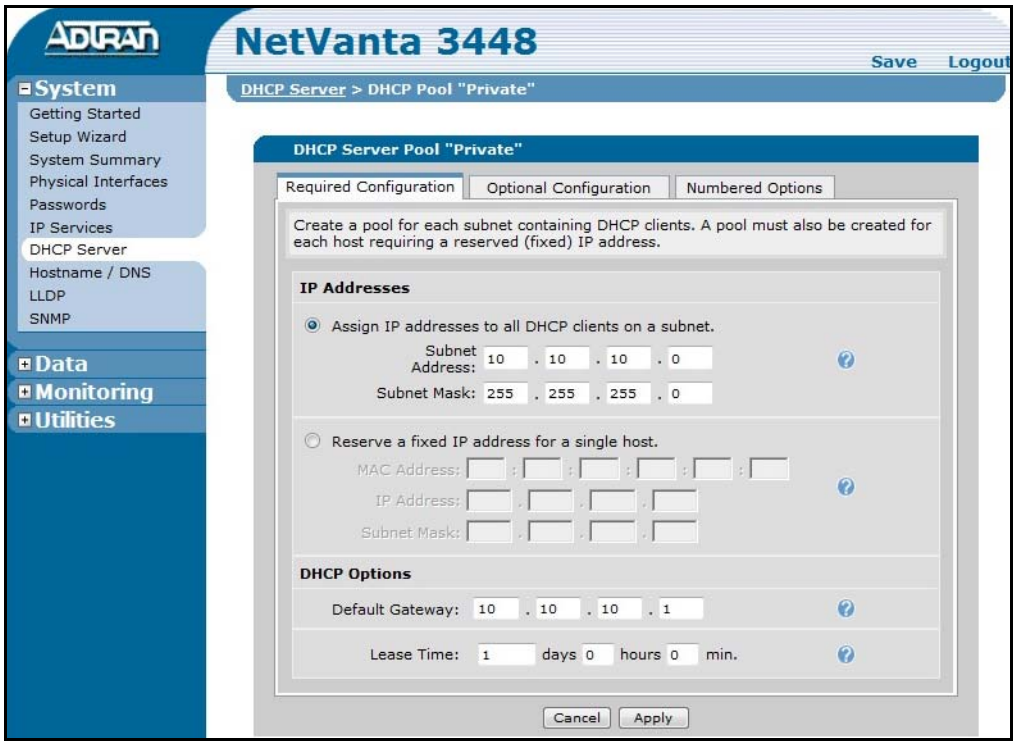
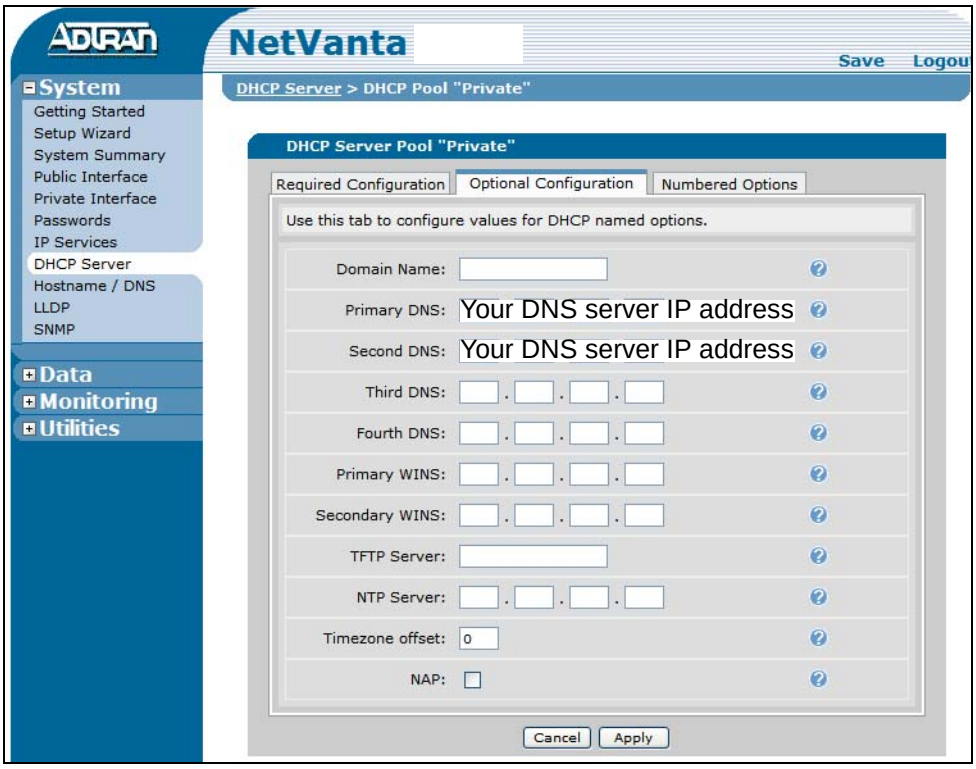


Figure 13-2 DHCP Server Address

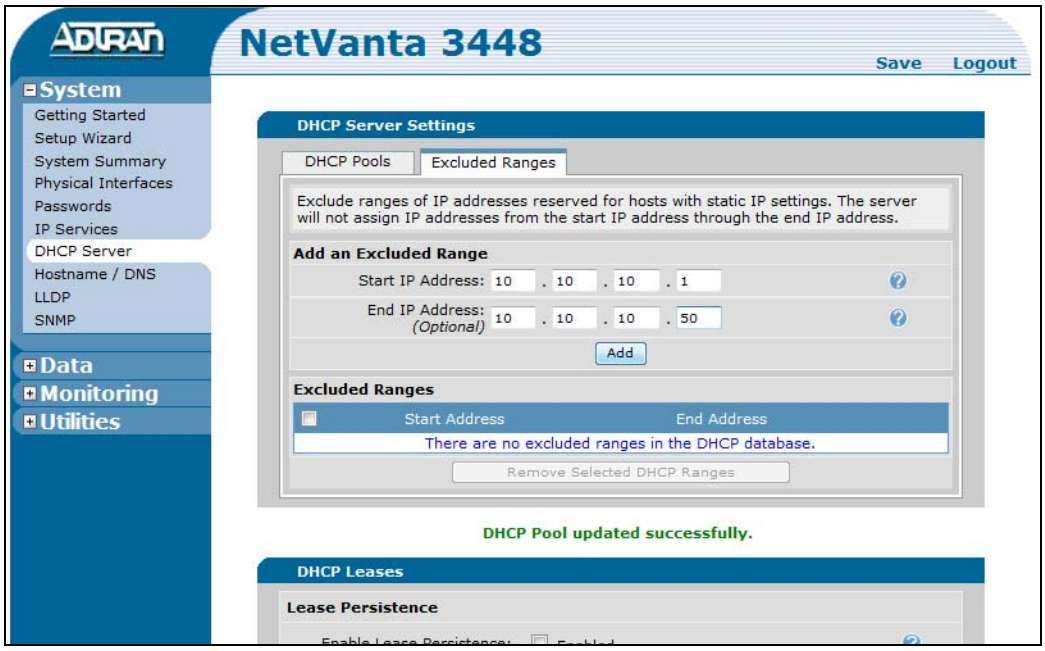
10. Click on the **Apply** button.

Note: If a “Invalid NTP IP address” message appears go to Step 11.

11. In the **Optional Configuration** tab enter the DNS address(es) provided by your Internet Service Provider. Be sure the NTP Sever data fields are empty then, click on **Apply**.



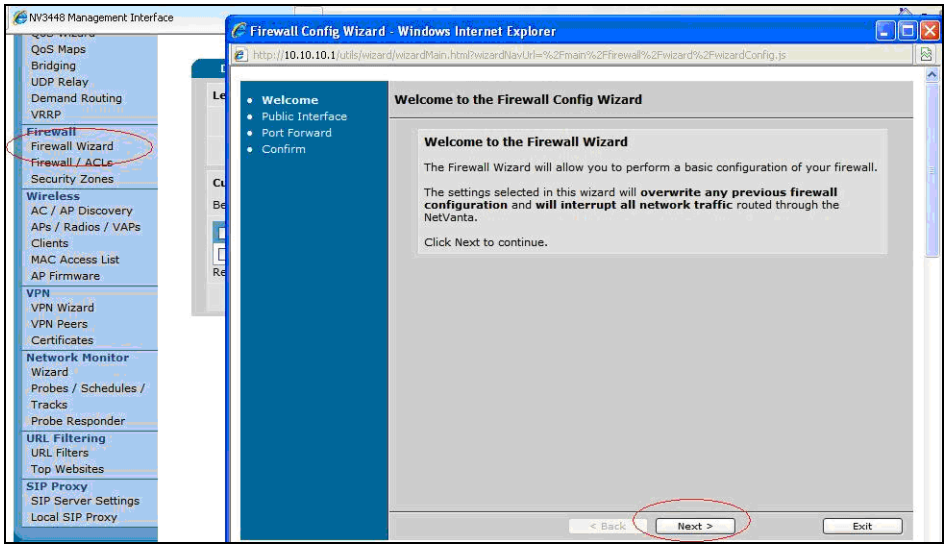
12. Select **System > DHCP** then, select the **Excluded Range** tab. Enter the range of IP addresses that should not given out to DHCP clients. These are IP addresses (typically 50 addresses) you are holding in reserve so that they can be assigned as static address for servers and other devices. Click on **Add**.


NetVanta 3448
Save
Logout
System
Getting Started
Setup Wizard
System Summary
Physical Interfaces
Passwords
IP Services
DHCP Server
Hostname / DNS
LLDP
SNMP
Data
Monitoring
Utilities
DHCP Server Settings
DHCP Pools
Excluded Ranges
Exclude ranges of IP addresses reserved for hosts with static IP settings. The server will not assign IP addresses from the start IP address through the end IP address.
Add an Excluded Range
Start IP Address: 10 . 10 . 10 . 1
End IP Address: (Optional) 10 . 10 . 10 . 50
Add
Excluded Ranges
Start Address
End Address
There are no excluded ranges in the DHCP database.
Remove Selected DHCP Ranges
DHCP Pool updated successfully.
DHCP Leases
Lease Persistence

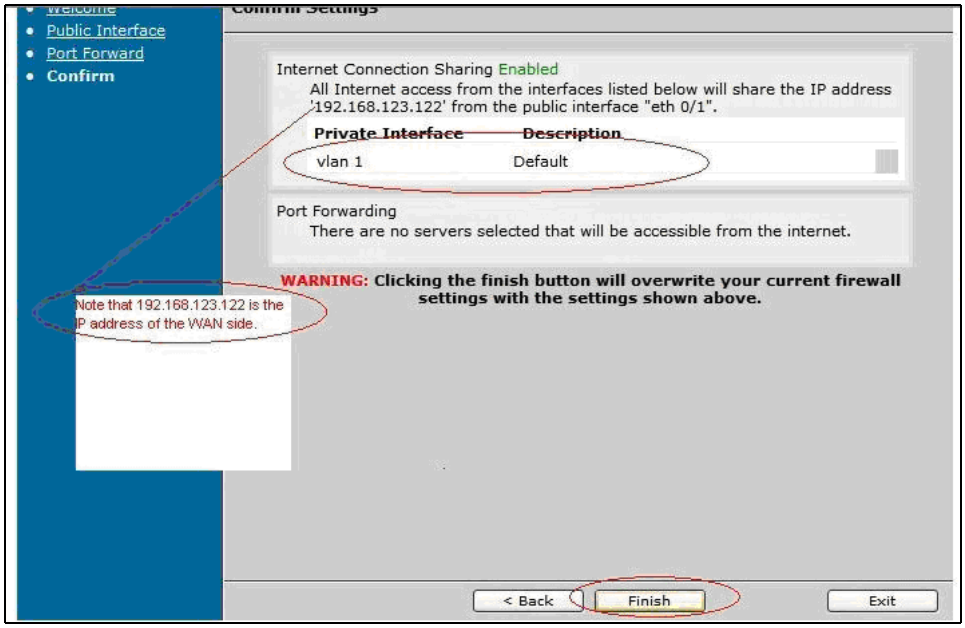
SETUP THE FIREWALL

Use the Adtran Wizard to the setup the firewall.

1. Select **Data > Firewall Wizard** from the Adtran menu. Then click on **Next**.

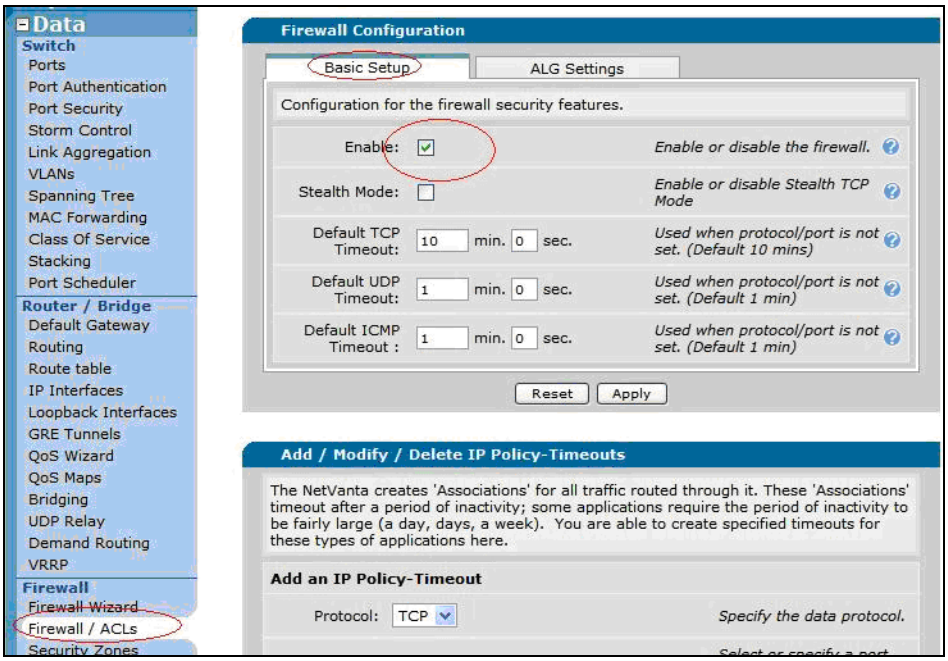


2. Select the **eth0/1** interface from the pull-down list in the Interface field then, click on **Next**.
3. Click on the radio button for: **No**, I don't have any servers that need to be accessed from the internet. Then click on **Next**.
4. Click on **Finish**.

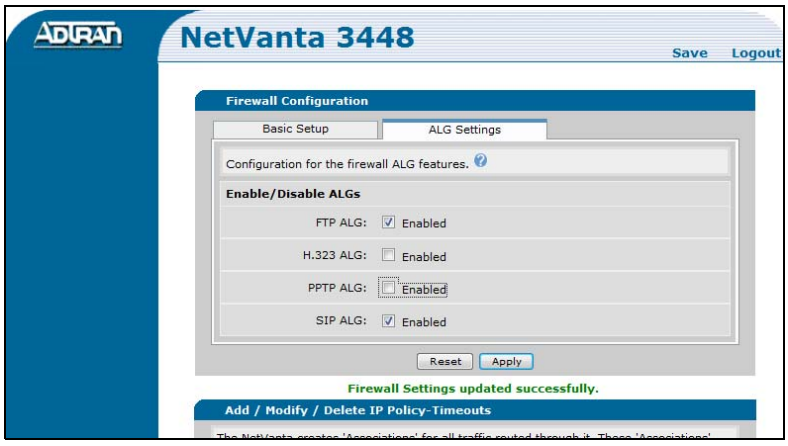


5. The router LAN IP address is set as the Default Gateway for the LAN subnet automatically.
6. When the wizard is complete click on **Exit**.

7. Select **Data > Firewall/ACLs**. In the Basic Setup tab check-mark the firewall security **Enabled** box.

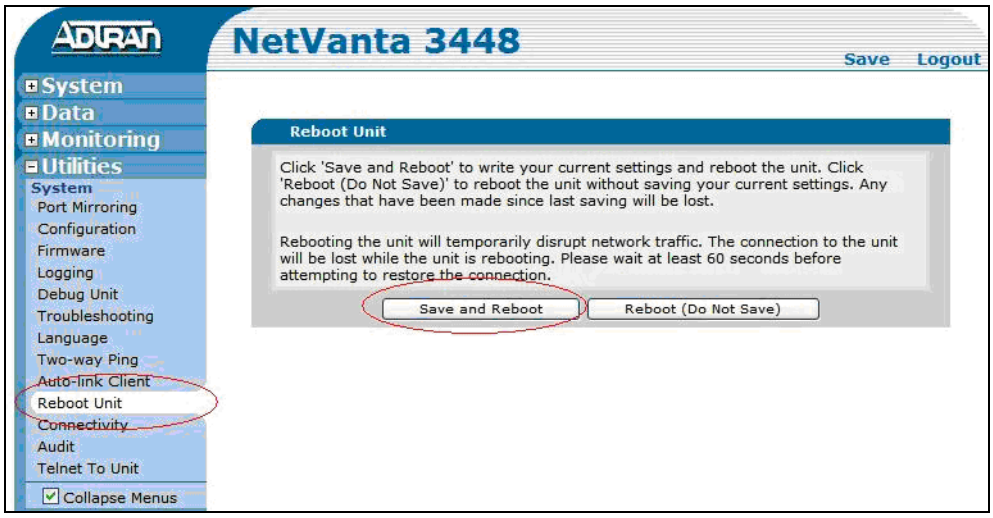


8. In the ALG Settings check-mark the **FTP ALG** and **SIP ALG** boxes. Ensure that all others are off.



9. Click on the **Apply** button.

10. Select Utilities > Reboot unit. Click on **Save and Reboot**.



11. Set your PC to use DHCP.
12. Verify that you can access the internet.

ADTRAN QoS CONFIGURATION

1. Login to the Adtran NetVanta Router.
2. Define WAN bandwidth subscribed from Internet Service Provider (ISP). Select **Data > IP Interfaces**.

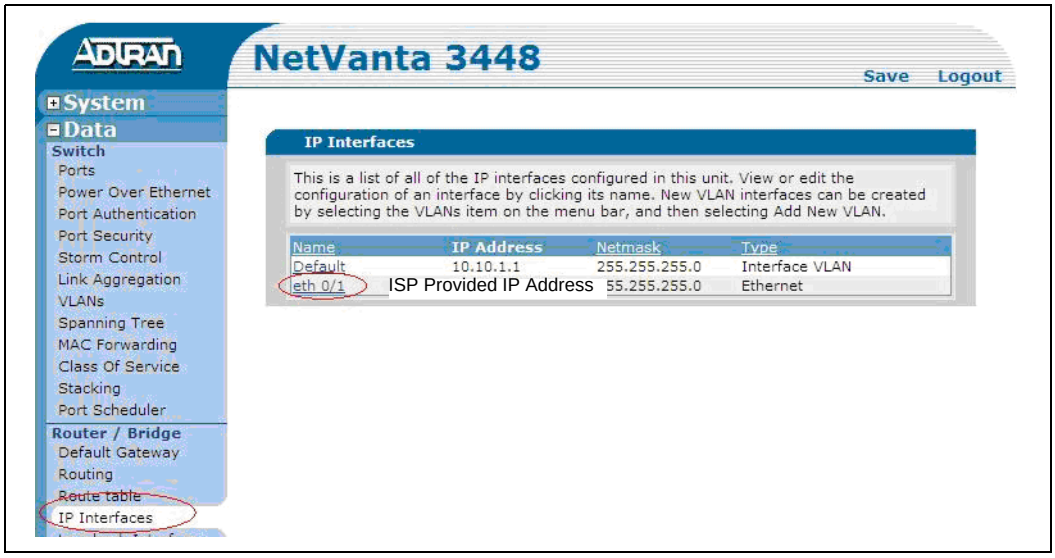


Figure 13-3 Select WAN Interface

3. Click on **eth 0/1**.
4. Specify the bandwidth that was subscribed from the ISP. In the example shown in Figure 13-4 the data rate is 1.5Mbps. This is the **uplink** rate. Check mark the **Traffic-Shaping** box then, enter the data rate in the **Traffic-shaping** rate field.

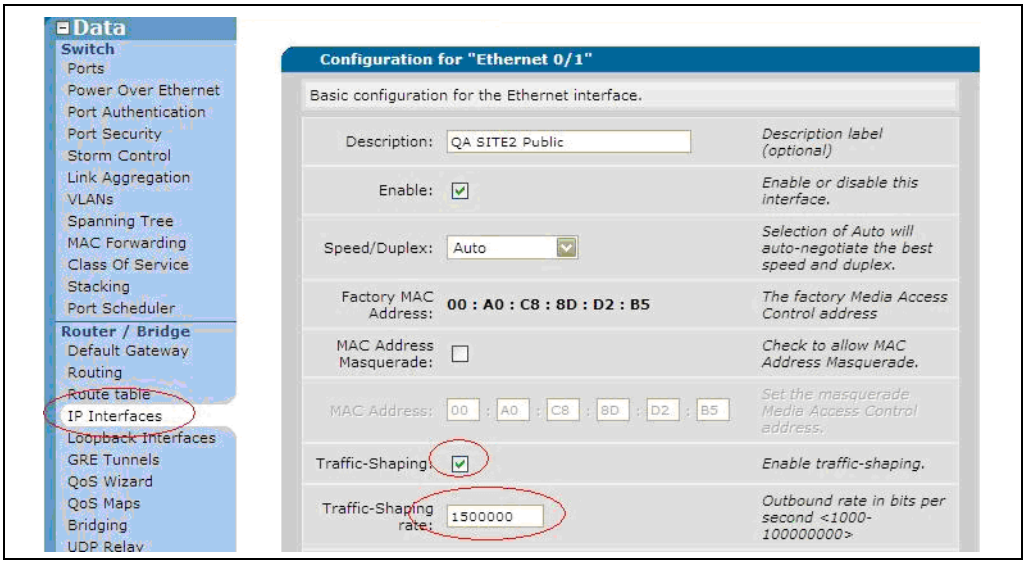


Figure 13-4 Enter the ISP Data Rate (1.5Mbps shown in this example)

5. Scroll down to click on the **Apply** button.

Access Control List

6. Create matched Access Control Lists (ACL) for Inbound and Outbound QoS Maps. At the bottom of the screen, select **Data > Firewall / ACLs**. Click on the **Configure ACL** button.

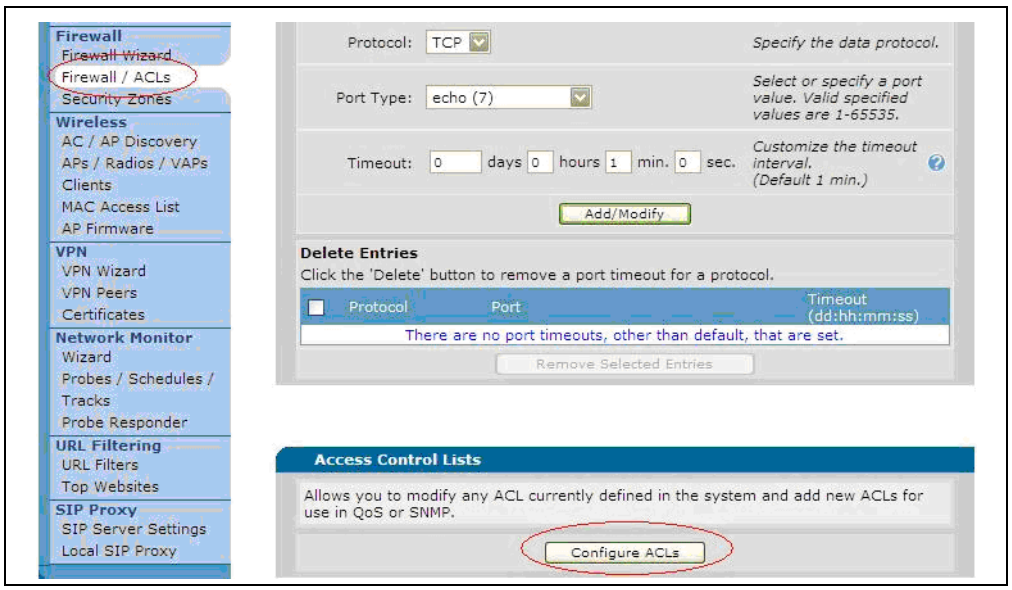


Figure 13-5 Define Matched Rules For QoS Map

7. If you have uploaded the Configuration File you can go to Traffic Class Queuing on page 13-16.

8. Create an ACL for VoIP ports and another ACL for data ports. Enter a name that describes the application for the new ACL (VoIP-Out) into the ACL Name field. Then click on the **Add New ACL** button.

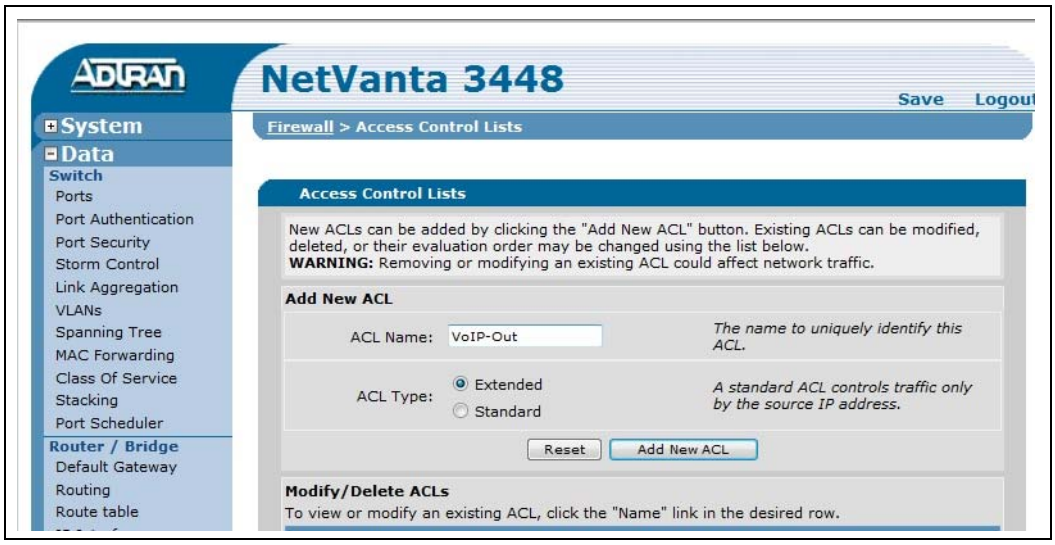


Figure 13-6 Enter a Descriptive ACL name (this example is the VoIP ACL)

9. In the dialog box click on the **Add New Traffic Selector …** button.

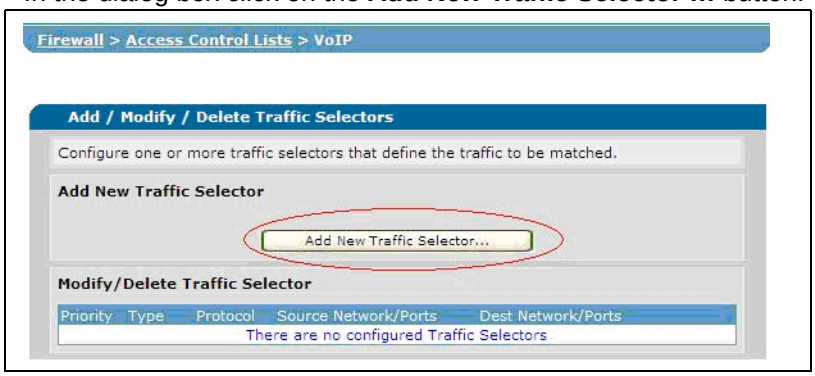


Figure 13-7 Add Traffic Rules to VoIP ACL

10. Set the ports and the protocol to allow the ports shown below in the table. Set:
Filter Type to Permit
Protocol to (value from the table)
Destination Data in the Destination Ports area, select **Specified**, select Equal to for a single port or Range for a range of ports. Enter the port(s). Then, click on **Apply**.

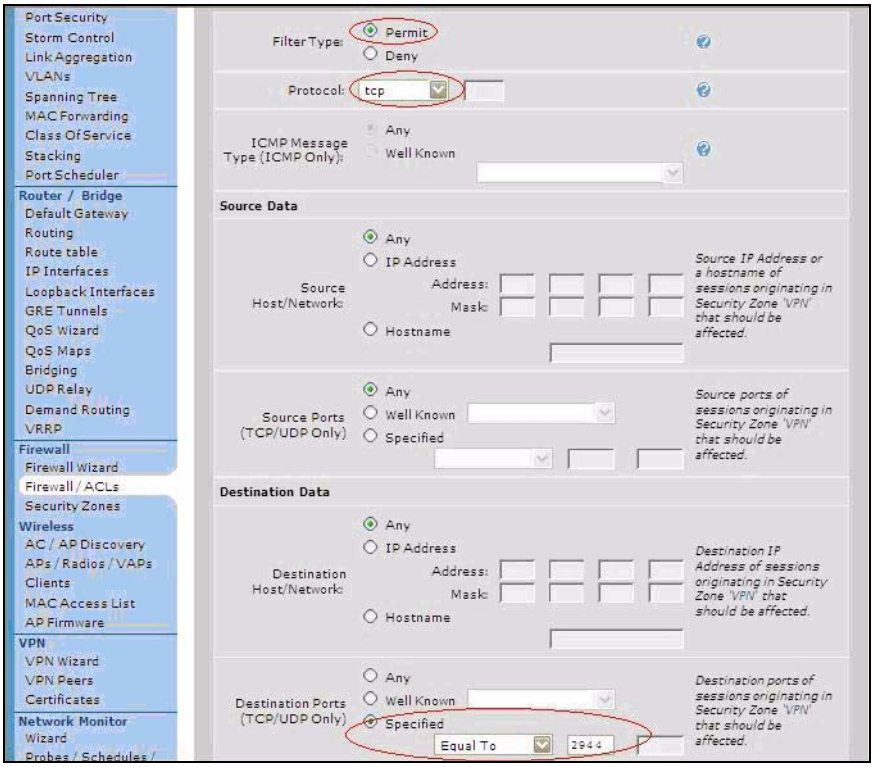


Figure 13-8 Permit Traffic to VoIP ACL (Example: TCP traffic on port 2944 is allowed)

Allow the following ports:

Protocol	Source Data	Destination Data	Use
UDP	Any	5060	Only for SIP telephones
Messaging	1007	TCP	Use by the System monitor Applet
	1008	TCP	Fax printer driver and Email Callback app
UDP	Any	1718~1719	IPTs
TCP	Any	2944	IPTs
TCP	Any	8446	IPTs
UDP	Any	27000~27399 (up to 60 users) 27000~28903 (more than 60 users)	RTP
UDP	49152~49154	Any	RTP

11. Repeat Step 9 and Step 10 to setup all of the ports shown in the table above.

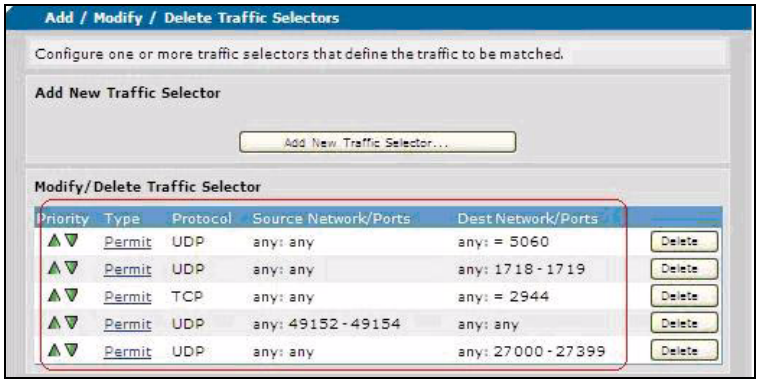


Figure 13-9 Permitted Ports for Outbound VoIP (example)

Create LAN to WAN QoS Maps

12. Select **Data > QoS Maps** enter 'VIPedgeQoS' as the Map Name. Enter Sequence Number 10.

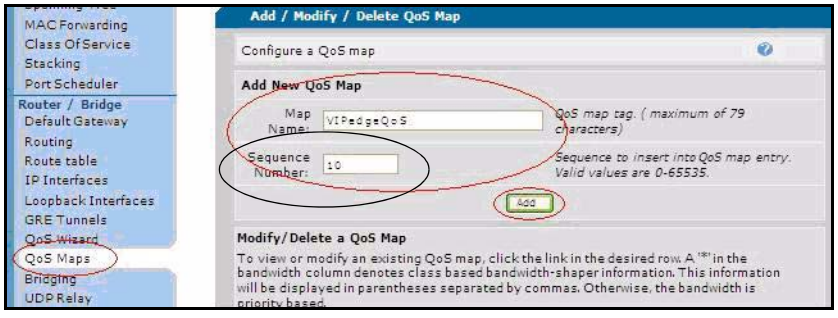
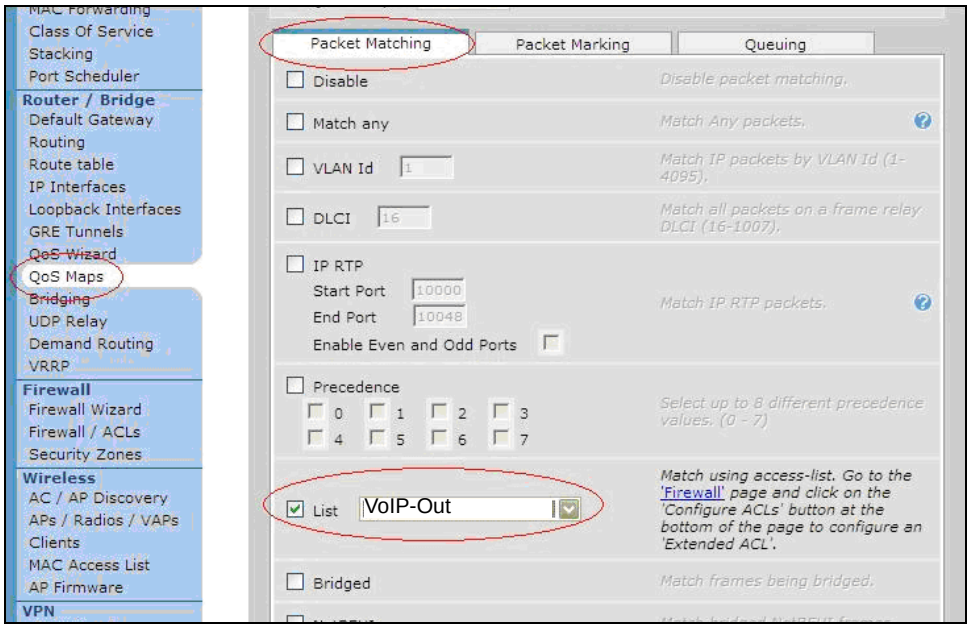


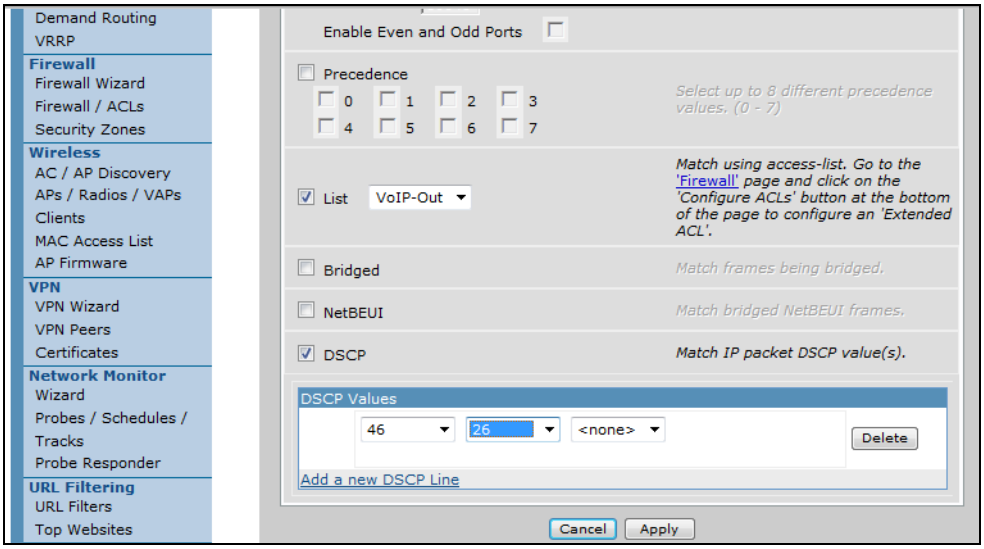
Figure 13-10 Create Outbound "VIPedgeQoS" for VoIP

13. Click on **Add**.

14. In the Packet Matching tab check-mark the box **List** and select **VoIP-Out**.



15. Scroll down to check-mark the **DSCP** box. Click on **Add a new DSCP line**.



16. In the DSCP Values field enter **46, 26** then, click on **Apply**.

Traffic Class Queuing

17. Click on the QoS map you just created in Step 12. Click to select **Traffic Class Queuing**. Under Shaping click to check-mark the **Average** box.

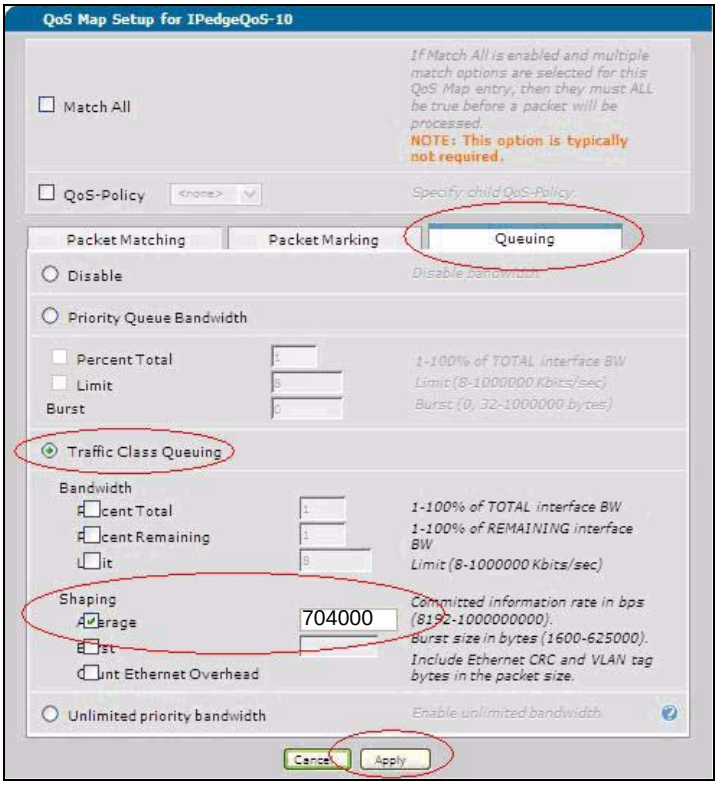


Figure 13-11 Create outbound QoS "VIPedgeQoS"

Queuing

18. The Adtran NetVanta router will reserve 25 percent of the bandwidth for system critical functions.

    In this example the ISP provided a 1.5 Mbps connection. The router will reserve 25 percent of the 1500000 bps = 375000. That leaves 1250000 bps.

19. Multiply the number of VoIP channels by 88000 bps. Enter this value in the Committed information rate field. For example, if the system has 8 channels the calculation would be: 8 x 88000 = 704000.

Note: If this number is greater than the number calculated in Step 18 you will need an ISP connection with a higher data rate.

20. Click on **Apply**.

21. Select **Data > QoS Maps**. Scroll down to the QoS-policy assignment and statistics area. On the eth 0/1 line in the Outbound QoS-policy column select VIPEDGQoS (the name assigned in Step 12.

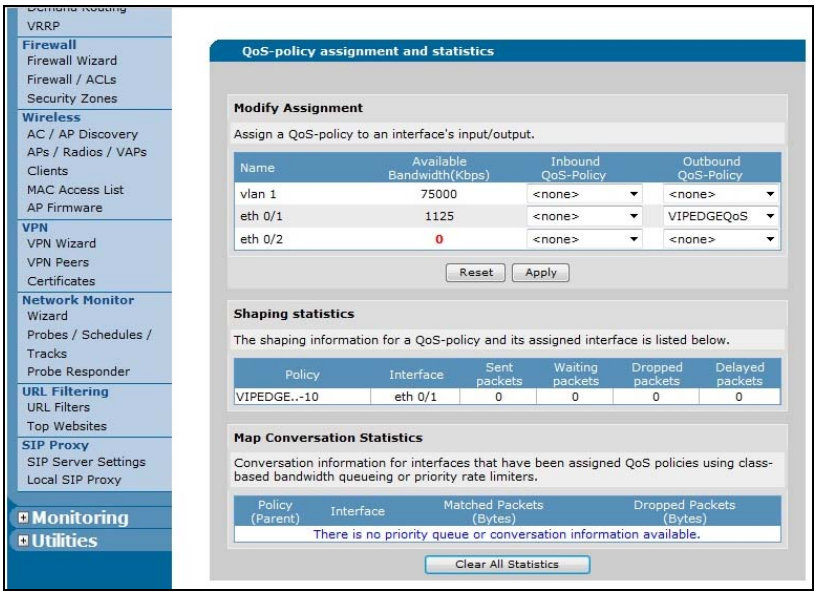


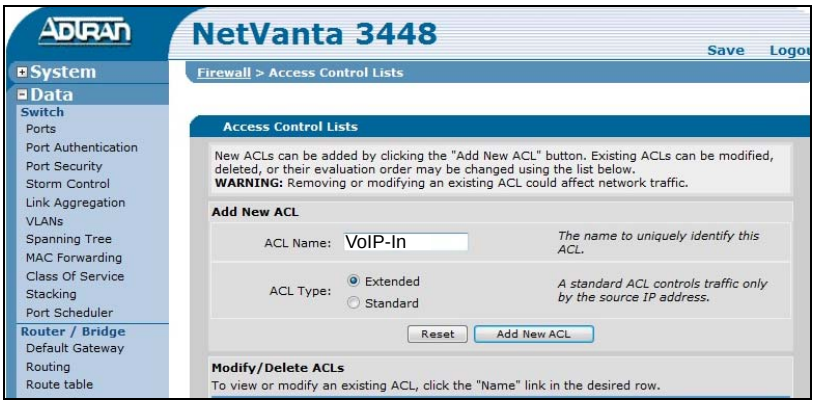
Figure 13-12 Configure Outbound QoS Map "VIPEDGEQoS"

22. If you uploaded a Configuration File you can go to VIPedge CONFIGURATION on page 13-19.

WAN to LAN Configuration

These steps configure the VoIP-In parameters.

1. Select **Data > Firewall/ACLs**. Click on **Configure ACLs**.
2. Enter VoIP-In as the **ACL Name**. Set **ACL Type** to Extended. Enter VoIP-In in the ACL Name field.



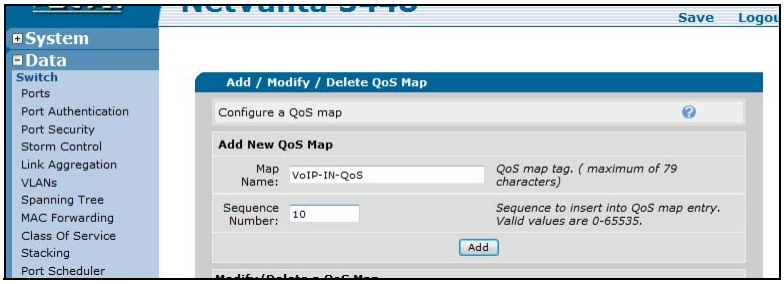
3. Click on **Add New ACL**.
4. In the dialog box click on the **Add New Traffic Selector…** button.

5. In the Firewall/ACL screen select Filter Type as **Permit**.
   In the Protocol field select **udp**.
   In the Source Data section select **Any**.
   For Source Ports select **Specified** then, select **Range.**

   Enter the range of **27000** to **27399** (up to 60 users) or
   Enter the range of **27000** to **28903** (over 60 users).

   Click on **Apply**.

6. Select **Data > QoS Maps**. Enter the map name: **VoIP-In-QoS**
   Set the Sequence Number to **10**.



7. Click on **Add**.
8. In the Packet Matching tab:
   Check-mark the **List** box and select **VoIP-In**
9. Check-mark the **DSCP** box. In the DSCP values click on **Add a new DSCP Line**, select **46** and **26**.
10. In the Packet Marking tab select **DSCP** then enter **46**.
11. Click on **Apply**.
12. Select **Data > QoS Maps**. Scroll down to click on **eth 0/1 Inbound Policy**. Select **VIPEDGEQoS**, vlan VoIP-In-QoS.
13. Click on **Apply**.

VIPedge CONFIGURATION

1. Login to the VIPedge call processor Enterprise Manager.
2. Select **System > System IP Data**.
3. Set the following parameters. Refer to Figure 13-13.
   Diffserv: Enable
   TOS Field Type: DSCP
   DSCP: 46

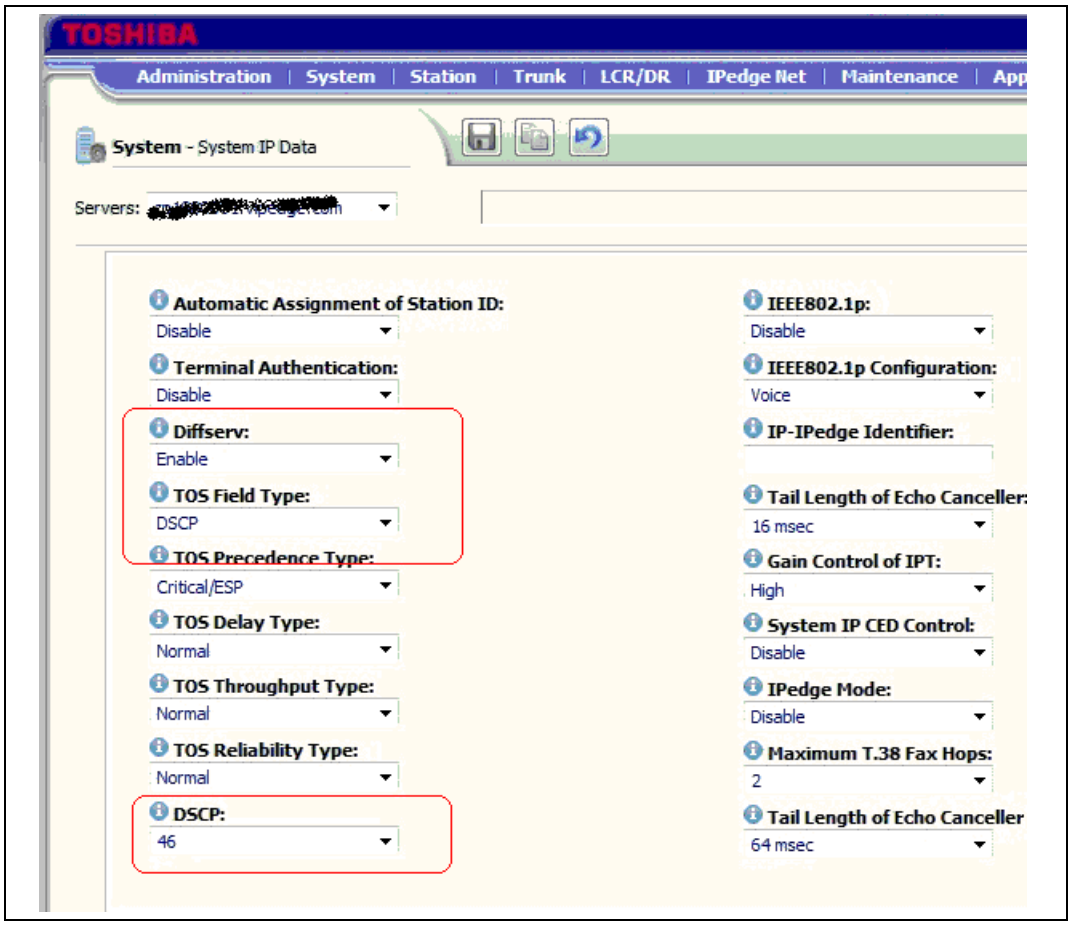


Figure 13-13 Setup IPT Traffic for Diffserv and DSCP 46

NETWORK SECURITY

Change the User Name and Password of your NetVanta router. Record the new login information in a secure location.

NETWORK CONFIGURATIONS

The following diagrams show three different network topologies. The recommended configuration is shown in Figure 13-14.

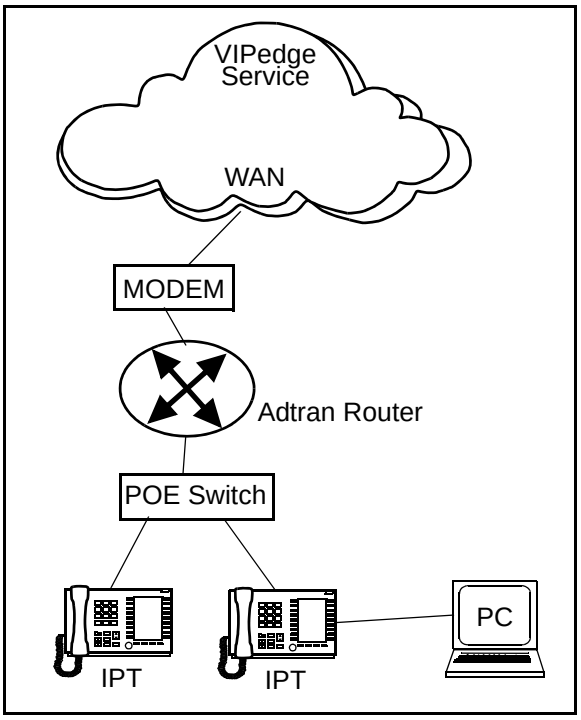


Figure 13-14 Recommended Network Topology

The network configuration shown on the left side of Figure 13-15 is functional but not optimum. The network configuration shown on the right side of the figure is not acceptable.

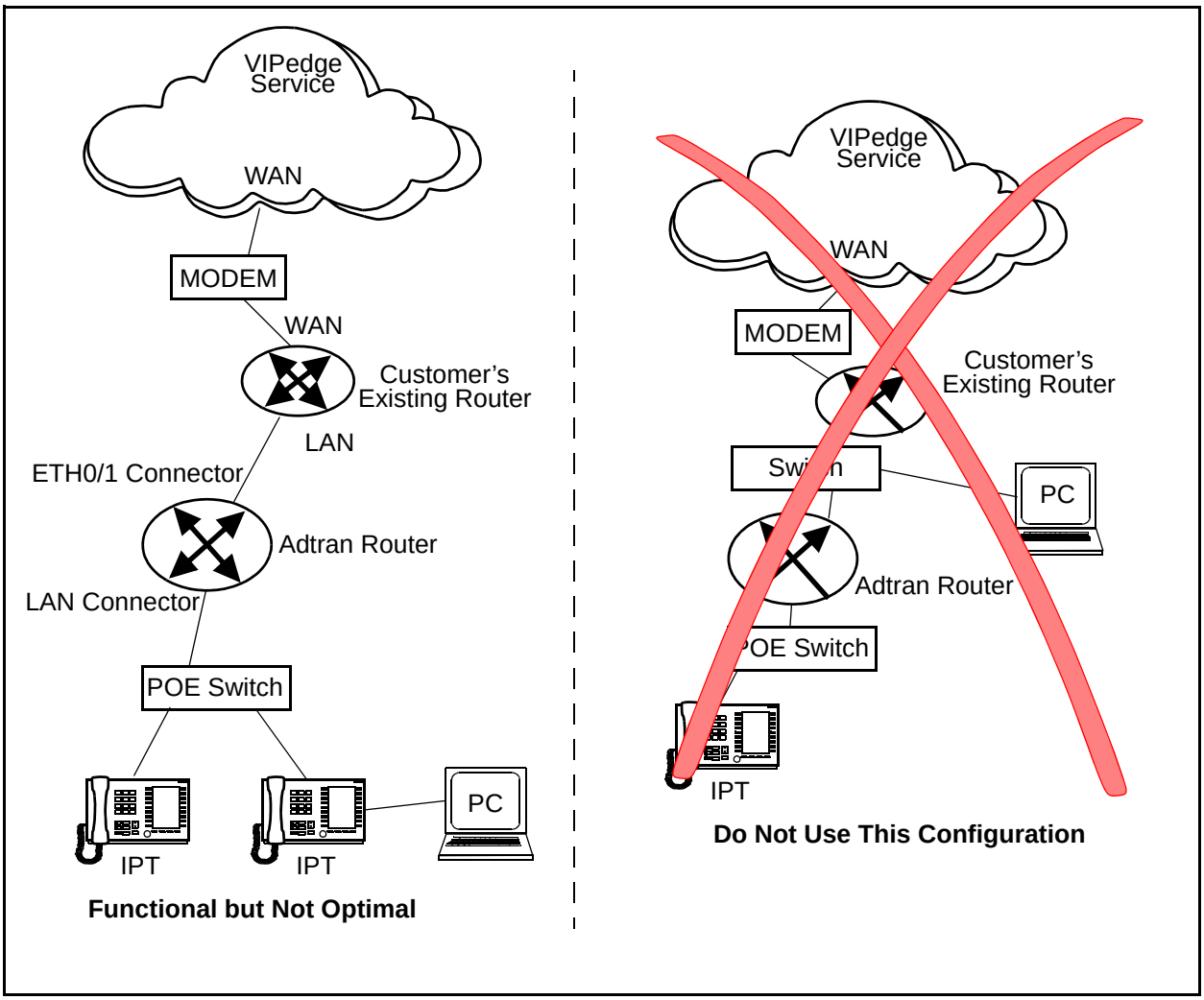


Figure 13-15 Other Network Topologies

This page is intentionally left blank.

Chapter 14 – Customer Admin Portal

This chapter is the same information that is available in the VIPedge Customer Administration manual.

CUSTOMER ADMINISTRATION

This document is a guide to the VIPedge Customer Administration Portal.

Outline

The Customer Portal is the administration entry point for VIPedge system Users.

New Customer

- You must login to your account to setup a password and, as needed, edit the Account Details.

All Customers

- Change credit card/bank information
- View the billing history
- View call detail records which include the cost of calls
- Modify the auto replenish setup
- Change password

Customer Login

1. When your quote was processed by the dealer you received an email.
2. The email contained your user name (your email address) and a temporary password.
3. Use one of these browsers to access the VIPedge portal.
    - Internet Explorer 7 or 8
4. Login to the VIPedge portal at www.vipedge.comfi

5. The first time you login the system will require a new password. The new password must be a ‘strong’ password with the following:
    - At least six characters, not more than 16 characters
    - At least one character must be a capital letter
    - At least one character must be a number
    - At least one character must be a special character ! @ # $ % ^ & *) (

6. Click on Account Details to review your account details.

Note: When entering or editing your address remember that there must not be a - (dash) or period (.) in the address.

ACCESS EMPA

Your Dealer will send you a URL (IP address) to access the Enterprise Manager Personal Administrator. This is the URL that station users will use to access the EMPA for their stations without access to the Customer Information such as billing and banking.

1. Launch an internet browser.
2. Copy the URL provided by your dealer into the address field of your browser.
3. The Enterprise Manager login page will open.
4. Use your directory number as the login ID and password.

MUSIC ON HOLD

The system has a total of fifteen music sources plus Quiet Tone on the Media server for Music On Hold (MOH). The administrator selects from these 15 internal WAV files, and quiet tone. Administrators can upload their own WAV files to the system.

This feature provides music or tone to a station or line that is held by a station with Line Hold or Consultation Hold and the speech path is released.

The music sources will ‘loop’ continuously. Whenever the music is requested to start, it always plays from the beginning of the file.

Your dealer can assign the MOH source of your choice to the functions in your system (trunk groups, Uniform Call Groups, etc.) in your system.

The following table shows the MOH choices.

Music Number	Source
1 through 15	Music (.WAV) file on Media Server
Quiet Tone	Media Server

Programming

To upload a custom MOH file.

1. Login to Enterprise Manager Personal Administrator.
2. Select **Application > Custom MOH**.
3. Click on the **Browse** button next to the MOH source number you want to customise.
4. Navigate the audio file you want to upload. Refer to the Music On Hold File Formats shown below.
5. Click on the **Upload** button.

Music On Hold File Formats

The audio files can be named anything (as long as they end with .wav). Supported audio wav files are shown in the table below.

Digitizing Method	Sampling Rate (kHz)	Resolution (Bits)	Bit Rate (Kbps)
OKI ADPCM	6	4	24
OKI ADPCM	8	4	32
G.711 PCM A-law and mu-law	6	8	48
G.711 PCM A-law and mu-law	8	8	64
Linear PCM	8	16	128
Linear PCM	11	8	88
GSM 6.10 full rate (Microsoft format)	8	value ignored	13
G.726 bit exact	8	2	16
G.726 bit exact	8	4	32

MOH COMPATIBLE WAV

The Media Server (MS) is specified to handle up to 15 MOH audio .wav files. The audio files can be named anything as long as they end with .wav

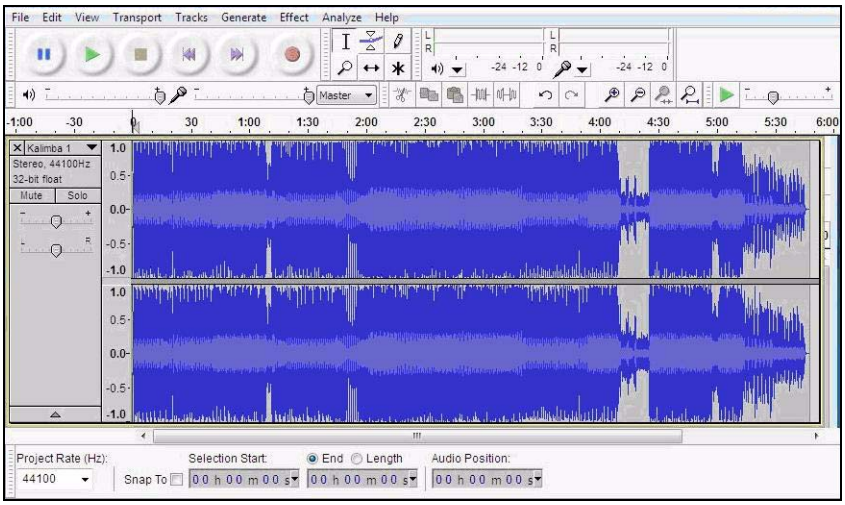
CONVERT MP3 TO WAV

An MP3 file can be converted to a compatible WAV file for use as a MOH source. One method is by using a freely downloadable program called Audacity® (http://code.google.com/p/audacity/). Audacity is a trademark of Dominic M Mazzoni.

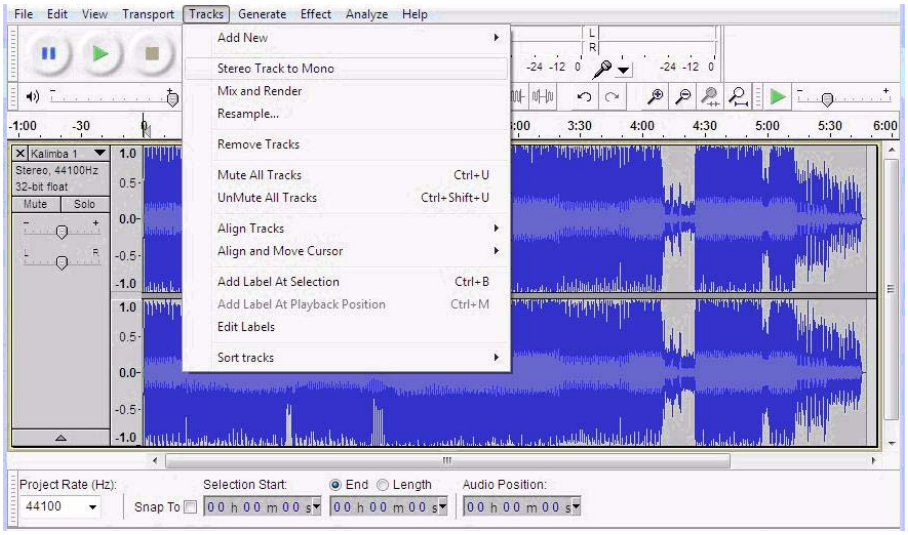
Note: Run the MP3 to WAV conversions on an administration PC, not the VIPedge server.

The following procedure shows the MP3 to WAV conversion using Audacity.

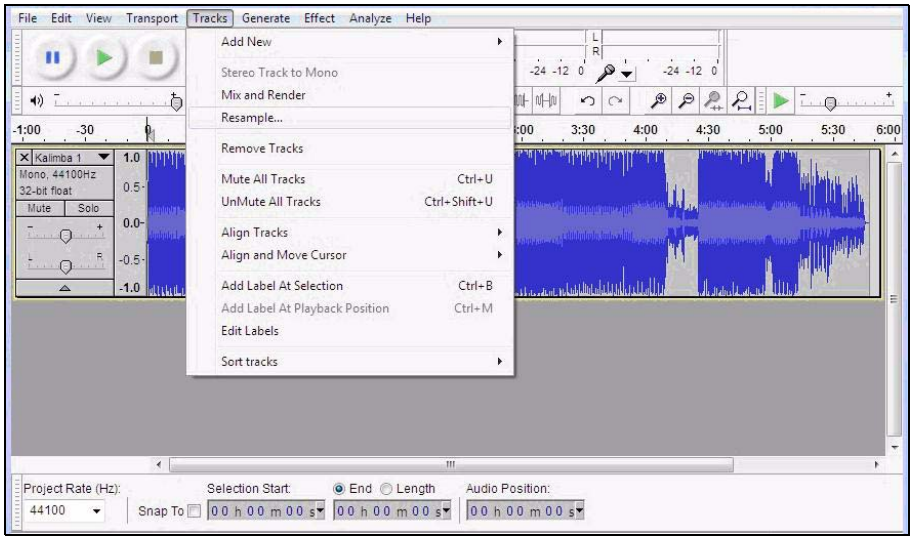
1. After installation, open the MP3 file you need to convert in Audacity:



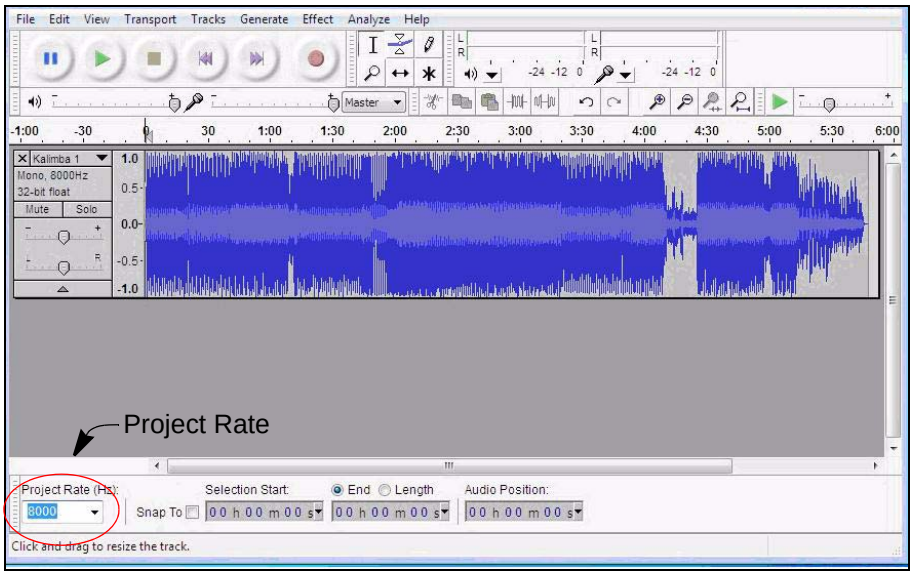
2. If in stereo, as shown above, convert the file from stereo to mono. Select **Tracks > Stereo Track to Mono**.



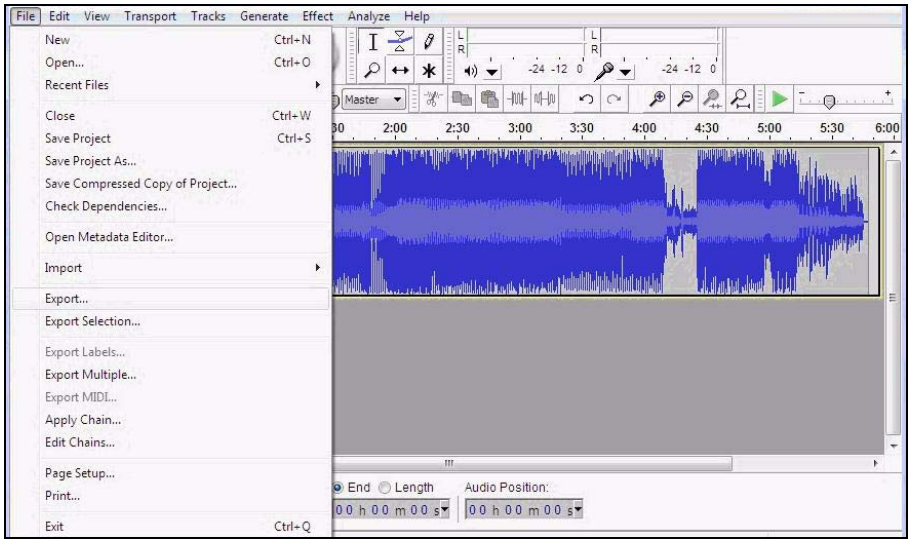
3. Then, resample the file. Select **Tracks > Resample**. Set new sample rate to **8000 Hz**:



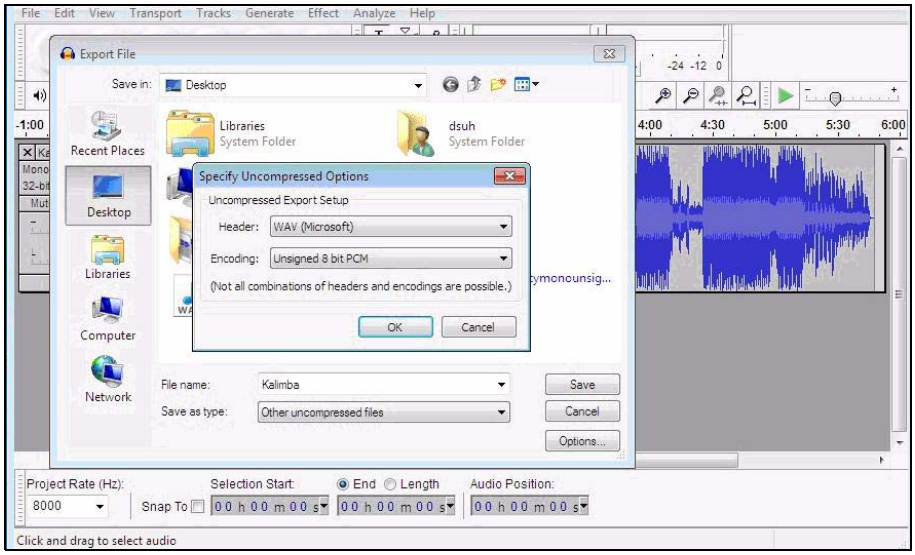
4. Change the Project Rate to 8000 Hz:



5. Select **Export** to save the file.

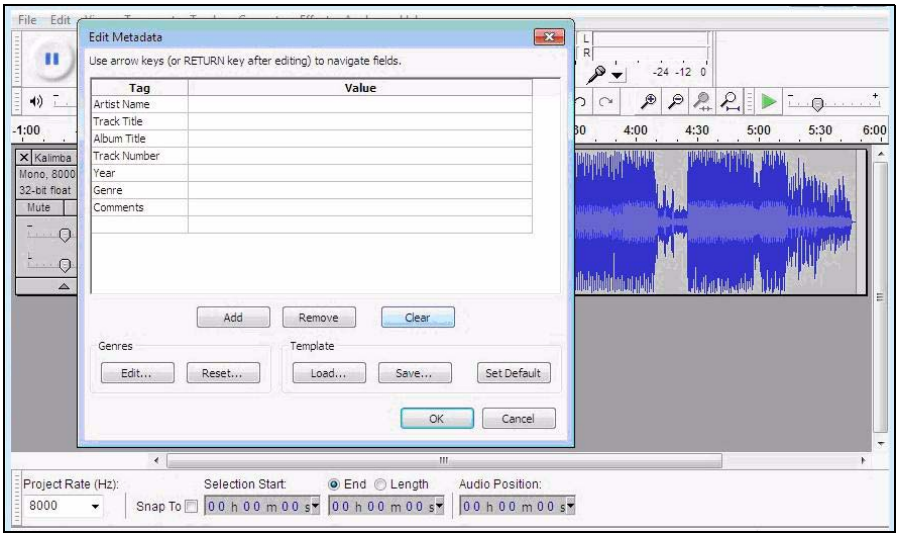


6. In the Export dialog enter the name for the file in the File name field. In the Save as type field select **Other uncompressed files**.
7. Click on the **Options…** button. For R1.2 and later systems select **WAV (Microsoft)** in the Header field and **Signed 16 bit PCM** in the Encoding field. For R1.1.2 (and earlier) systems select **WAV (Microsoft)** in the Header field and **Unsigned 8 bit PCM** in the Encoding field.



8. Click on **Save**.

9. In the last dialog box, click on **Clear** and then **OK**.



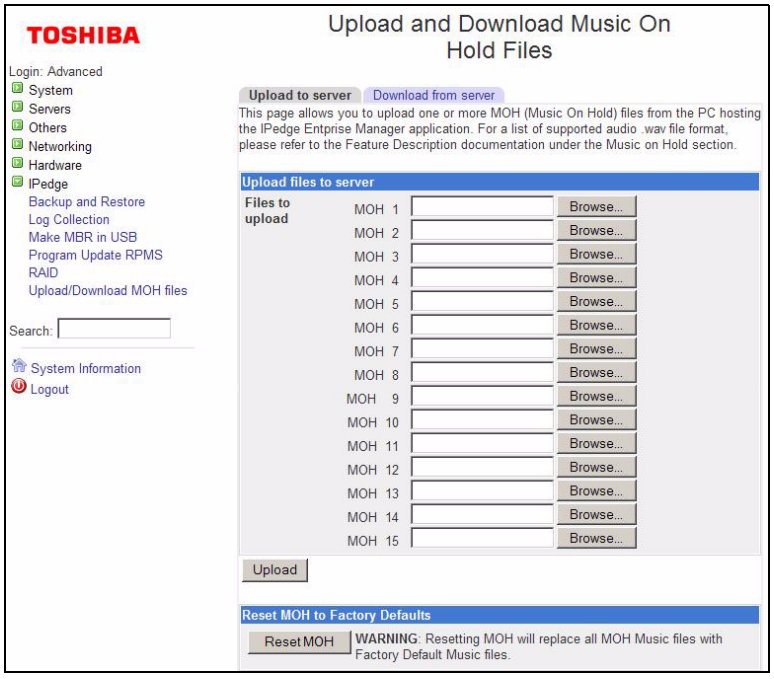
Adjusting MOH Volume

Use Audacity to adjust the volume using the **Effect > Amplify** function after the MOH file is loaded into the Audacity application.

UPLOAD WAV TO VIPedge

Upload the WAV file to the VIPedge server using Webmin.

1. Login to Enterprise Manager. Select **Application > Webmin**.
2. Select the server or customer.
3. In Webmin select **IPedge > Upload/Download MOH Files**.



4. Click on the **Browse** button next to the MOH number for this file.
5. Browse to the WAV file you just converted.
6. Click on the **Upload** button.

BACKUP

The Music On Hold files are not part of the System Backup. Toshiba recommends that you maintain a backup of the MOH files that were uploaded to the VIPedge server in a secure location.

THIS IS THE END OF THE DOCUMENT.