



AdTran Configuration Guide v3.1

ADTRAN 3120 / 3130 Configuration Guide



5600 Avenida Encinas, Suite 170
Phone & Fax: (800) 477-1477

Introduction

Thank you for choosing FreedomVoice for your industry-leading hosted VoIP phone system. We are glad to have you on board as part of our team and this document should help answer any questions you may have on setting up the AdTran router.

There are two main parts to this document. The first is the **Internet Configuration Guide** that covers setting up basic Internet access and getting the router online. The second section is the **AdTran QoS Configuration Guide** which provides the procedure for configuring QoS (Quality of Service) on the device.

Part 1; The **Internet Configuration Guide** will step you through the procedure for configuring Internet access on the AdTran 3120/3130 router in its new or reset state. Setting up the router is a four step process:

1. Change the default password.
2. Configuration of the Public Interface (Internet access).
3. Disabling the SIP ALG (application level gateway).
4. Configuring SNTP (simple network time protocol).
5. Enabling Remote Access.

ADTRAN 3120 / 3130

Product Information: ADTRAN 3120

The ADTRAN 3120 series is a Fixed-port Access Router that is ideal for enterprise-level Internet access and/or IP Telephony using broadband access such as DSL or cable. The 3120 includes one Ethernet WAN port, an integrated four-port Ethernet Switch, a built-in firewall for network security, QoS to priority delay sensitive traffic like VoIP, and a host of other features such as DHCP, Network Address Translation (NAT), and IPsec VPN.

Features:

- Fixed-port Access Router for broadband access such as DSL or cable
- Ethernet WAN Interface and Integral four-port, non-blocking, Ethernet switch
- Stateful inspection firewall for network security
- Quality of Service (QoS) for delay-sensitive traffic like Voice over IP (VoIP)
- Inherent URL filtering for easy content filtering
- IPsec Virtual Private Network (VPN) for secure corporate connectivity across the Internet

Product Information: ADTRAN 3130

The ADTRAN 3130 series is a Fixed-port Access Router that is ideal for enterprise-level Internet access and/or IP Telephony ADSL, ADSL2, or ADSL2+ broadband access. The 3130 includes one ADSL WAN port, integrated four port switch, built in firewall, QoS, DHCP, NAT, and an IPsec VPN.

Features:

- Fixed-port Access Router for ADSL, ADSL2, or ADSL2+
- ADSL WAN Interface and Integral four-port, non-blocking, Ethernet switch
- Stateful inspection firewall for network security
- Quality of Service (QoS) for delay-sensitive traffic like Voice over IP (VoIP)
- Inherent URL filtering for easy content filtering
- IPsec Virtual Private Network (VPN) for secure corporate connectivity across the Internet

Change Default Username/Password

It is important that you change the default username and password to something secure. This new login information ensures that no one within the LAN can make unauthorized changes, but can also be used as the default remote login information for remote access to the router in the event changes need to be made remotely by a partner or a FreedomVoice representative.

Default login information:

- Gateway: "10.10.10.1"
- Username: "admin"
- Password: "password"

Follow these steps to update the admin login information:

1. From the "System" section in the left column, select "Passwords".
2. Scroll to the bottom of the page and select the "Enable" tab.
3. Check "Use password" and enter your new password twice.
4. Click the "Apply" button toward the bottom of the page.
5. Click the "Save" button at the top of the page.

Configuring Internet Access

Follow these steps closely to set up the AdTran 3120/3130 via the built in GUI. **Your ISP should have provided you with general instructions** related to your internet connection. If you are unsure what these settings are, contact your ISP with regard to the settings you will need for your router. In 99% of all cases your service provider will either have you to set your router to DHCP mode or they will provide you with IP address, Gateway, Subnet and DNS server settings. **You will need this information to continue the set up.**

Follow these steps to configure internet access:

1. From the "System" section in the left column, select "Public Interface".
2. Go to "IP Settings" halfway down the page. Your ISP settings will determine whether you need to choose "Static" or "DHCP" from the drop down. If your ISP has provided you with a specific IP, select "Static". If you select "DHCP" skip to step 10. ([Screenshot Internet](#))
3. Enter your IP address in the related field.
4. Enter your subnet mask in the related field.
5. Enter your default gateway in the related field.
6. Click the "Apply" button toward the bottom of the page.
7. Click the "Save" button at the top of the page.
8. From the "System" section in the left column, select "Hostname/DNS".
9. Enter the primary and secondary DNS addresses provided by ISP. ([Screenshot DNS](#))
10. Click the "Apply" button toward the bottom of the page.
11. Click the "Save" button at the top of the page.
12. Cycle power on the router and give the device 3-5 minutes to boot.
13. Cycle power on any connected devices such as computers, phones etc.

NOTE: See next page for configuration screenshot.

Configuration Screen 1 of 2

System → Public Interface

[\(Back to instructions\)](#)

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:	<input type="text"/>	Description label (optional)
Enable:	<input checked="" type="checkbox"/>	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 : 49 : A0 : 49	The factory Media Access Control address
MAC Address Masquerade:	<input type="checkbox"/>	Check to allow MAC Address Masquerade
	<input type="button" value="Get My MAC Address"/>	Click this button to place the MAC address of your PC in the fields below.
MAC Address:	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Set the masquerade Media Access Control address
Traffic-Shaping:	<input type="checkbox"/>	Enable traffic-shaping
Interface Mode:	IP routing	Select an interface mode

Wireless Control Protocol

Enabled AWCP:	<input checked="" type="checkbox"/>	Enable/Disable Wireless Control Protocol.
---------------	-------------------------------------	---

IP Settings

Address Type:	Static	Set to 'None' if connecting to a Bridge with IP routing disabled.
IP Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	IP address for this numbered interface
Subnet Mask:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	Subnet Mask for this numbered interface
Default Gateway:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	Enter the IP address for the Default Gateway.
Dynamic DNS:	<disabled>	Used to register this interface's IP address with a DNS Name.

Secondary IP Settings

To add a range of secondary IP addresses (up to 255 addresses), enter a valid start IP address, IP mask, and the number of addresses to add.

Range	Start IP Address	Mask
<input type="button" value="ADD A NEW SECONDARY IP ADDRESS"/>		

Media-Gateway

IP Address Type:	None	RTP traffic will flow over the selected IP address.
------------------	------	---

Monitoring

RTP Monitoring:	<input checked="" type="checkbox"/>	Enables RTP monitoring on this interface.
-----------------	-------------------------------------	---

NOTE: On Adtran 3130 DSL routers, the default gateway option is listed under "Data" → "Router/Bridge" → "Default Gateway".

Configuration Screen 2 of 2

System → Hostname / DNS

[\(Back to instructions\)](#)

ADTRAN 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

DNS Setup

Configure the hostname and domain name for the NetVanta. The domain name is used when hosts on the private network of the NetVanta use DNS queries to resolve domain names.

Host Name:	<input type="text" value="NetVanta3120"/>	Alphanumeric string to be used as a unique description for the unit.
Domain:	<input type="text"/>	Default IP domain name to be used by the unit to resolve host names. ?
Primary DNS IP Address:	<input type="text" value="68"/> . <input type="text" value="105"/> . <input type="text" value="28"/> . <input type="text" value="16"/>	Primary name server to use for name-to-address resolution (optional).
Secondary DNS IP Address:	<input type="text" value="68"/> . <input type="text" value="105"/> . <input type="text" value="29"/> . <input type="text" value="16"/>	Secondary name server to use for name-to-address resolution (optional).
Enable DNS Lookup:	<input checked="" type="checkbox"/>	Enable/Disable the IP DNS (domain naming system), allowing DNS-based host translation (name-to-address).
Enable DNS Proxy:	<input checked="" type="checkbox"/>	Enable/Disable DNS proxy for the unit. DNS Proxy enables this unit to act as a proxy for other units on the network.

Disable SIP ALG

The AdTran 3120/3130 needs to have SIP ALG disabled to function properly with the FreedomVoice service. FreedomVoice phones will not work with the AdTran router if SIP ALG is enabled. This is an option typically used for premise based VoIP systems. Disabling this option is a simple check box within the router configuration. If you purchased this router from FreedomVoice the SIP ALG setting will already be disabled by default.

To access the SIP ALG option, follow these steps:

1. In left column under "Data" then "Firewall", select "Firewall/ACLs".
2. In left column under firewall select "Firewall / ACLs".
3. In the main screen click on the "ALG Settings" tab.
4. In the main screen uncheck the "SIP ALG" option.
5. In the main screen click the "Apply" button.
6. At the top of the screen click the "Save" button.

SIP ALG Settings

Data → Firewall / ACLs → ALG Settings

The screenshot displays the NetVanta configuration interface. On the left is a navigation menu with categories: System, Data, Router / Bridge, and Firewall. The 'Firewall' section is expanded, showing 'Firewall Wizard', 'Firewall / ACLs', and 'Security Zones'. The main content area is titled 'Firewall Configuration' and has two tabs: 'Basic Setup' and 'ALG Settings'. The 'ALG Settings' tab is active, showing a configuration box for firewall ALG features. Below this box are 'Reset' and 'Apply' buttons. A second section, 'Add / Modify / Delete IP Policy-Timeouts', contains explanatory text about associations and a form to 'Add an IP Policy-Timeout'. The form has a 'Protocol' dropdown set to 'TCP' and a label 'Specify the data protocol.'. Below the form is a label 'Select or specify a port'.

Configuring SNTP (Simple Network Time Protocol)

The ADTRAN 3120/3130 should have the SNTP configured so that logs and voice quality monitoring reflect the proper time in the event that traffic logs need to be viewed for a specific time. If you purchased this router from FreedomVoice, the SNTP server will already be set up for Pacific Time. In this case you will just need to choose the correct time zone for your area.

To set up SNTP follow these steps:

1. In left column under “System” select “System Summary”.
2. In the main screen click on the “Time Server” link.
3. In the time server drop down, select “SNTP”. ([Screenshot SNTP](#))
4. In the field SNTP Server Hostname type in your SNTP server (such as: time.apple.com).
5. At the bottom of the screen click the “Apply” button.
6. At the top of the screen click the “Save” button.

SNTP Settings 1 of 2

ADIRAN

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

System Information

Hostname	NetVanta3120
Firmware Version	17.08.01.00.E
Part Number	1700601G2
Serial Number	LBADTN0931AE064
System Uptime	4 days, 23 hours, 31 minutes, 21 seconds
System Time	01:35:22 AM UTC
System Date	August 01, 2010
Memory	Total Heap: 31,353,840 Bytes Free Heap: 20,589,552 Bytes
CPU Utilization	System Load: 4.42% 1 Min Avg Load: 9.9% 5 Min Avg Load: 9.84% Min Load: 0% Max Load: 100% Context Switch Load: 0.6%
File System	Total: 30,093,672 Bytes Used: 10,199,728 Bytes Free: 19,893,944 Bytes
Time Server	(Not Configured)

Refresh in 4 seconds...

SNTP Settings 2 of 2

[\(Back to instructions\)](#)

ADIRAN

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

System > Time Server Configuration

Time Server Configuration

Warning: Configuring the unit to use SNTP will cause any previous configuration for NTP to be invalid.

Use this form to configure the time server.

Time Server:	<input type="text" value="SNTP"/>	?
Time:	<input type="text" value="01"/> : <input type="text" value="40"/> <input type="text" value="AM"/>	?
Date:	<input type="text" value="August"/> <input type="text" value="01"/> <input type="text" value="2010"/>	?
Auto-Correct DST:	<input checked="" type="checkbox"/>	?
Time Zone:	<input type="text" value="(GMT-05:00) Eastern Time (US & Canada)"/>	?
SNTP Server Hostname:	<input type="text" value="time.apple.com"/>	?
SNTP Server Version:	<input type="text" value="1"/>	?
SNTP Wait Time:	<input type="text" value="86400"/>	?
SNTP Retry Timeout:	<input type="text" value="5"/>	?

ENABLE REMOTE ACCESS

The ADTRAN 3120/3130 allows you to configure remote access to the GUI or command line interface.

Follow these steps to configure remote access:

1. In the left column under “Data” and “Firewall”, select “Security Zones”.
2. In the edit security zones section, click on “Public”. ([Screenshot Security Zones](#))
3. In the main screen click “Add Policy to Zone Public”. ([Screenshot Public](#))
4. In the main screen under “Policy Type:” select “Admin access” from the drop down. ([Screenshot Policy Type](#))
5. You can set the description to something like “Remote Access”. The only other thing you’ll need to do is check “HTTPS” and if you want remote command line access check “SSH”. ([Screenshot Remote Access](#))
6. At the bottom of the screen click the “Apply” button.
7. At the top of the screen click the “Save” button.

Remote Access 1 of 4

Data → Firewall → Security Zones

[\(Back to instructions\)](#)

System

- Data**
 - Switch
 - Ports
 - Port Authentication
 - Port Security
 - Storm Control
 - Link Aggregation
 - VLANs
 - Spanning Tree
 - MAC Forwarding
 - Class Of Service
 - Port Scheduler
 - Router / Bridge**
 - Default Gateway
 - Routing
 - Route table
 - IP Interfaces
 - Loopback Interfaces
 - GRE Tunnels
 - QoS Wizard
 - QoS Maps
 - Bridging
 - UDP Relay
 - Demand Routing
 - VRRP
 - Firewall**
 - Firewall Wizard
 - Firewall / ACLs
 - Security Zones

Assign Interfaces to Security Zones

Each interface must be associated with a Security Zone. A Security Zone is configured with a set of policies that define what action the firewall will perform on data sessions originating from that zone.

Interface Name	Current Security Zone	New Security Zone
Public	Public	Public ▼
Default	Private	Private ▼

Edit Security Zones

A security zone contains one or more policies. The security zone can be applied to interfaces to allow, discard or NAT traffic as it enters the NetVanta. A security zone that has no configured policies will allow all traffic to enter the interface. Click on the 'Active Sessions' number to view the running version of your policy-class association table.

Modify Security Zones

Click on the link on the security zone name in order to modify that security zone.

Security Zone	Active Sessions	
Public	0	<input type="button" value="Rename"/>
Private	8	<input type="button" value="Rename"/>
<Click to add a Security Zone>	N/A	<input type="button" value="Rename"/>

Remote Access 2 of 4

Data → Firewall → Security Zones → Public

[\(Back to instructions\)](#)

- Data**
- Switch
 - Ports
 - Port Authentication
 - Port Security
 - Storm Control
 - Link Aggregation
 - VLANs
 - Spanning Tree
 - MAC Forwarding
 - Class Of Service
 - Port Scheduler
- Router / Bridge**
 - Default Gateway
 - Routing
 - Route table
 - IP Interfaces
 - Loopback Interfaces
 - GRE Tunnels
 - QoS Wizard
 - QoS Maps
 - Bridging
 - UDP Relay
 - Demand Routing
 - VRRP

Configure Policies for Security Zone 'Public'

New policies can be added to Security Zone 'Public' by clicking the "Add Policy" button. Existing policies can be modified or deleted or their evaluation order may be changed using the list below.

Add New Policy to Security Zone 'Public'

[Add Policy to Zone 'Public'](#)

Modify/Delete Policies in Security Zone 'Public'

To view or modify an existing policy, click the "Description" link in the desired row. [?](#)

Priority	Description	Action
	There are no configured policies; all traffic from Security Zone 'Public' will be blocked.	

Remote Access 3 of 4

Data → Firewall → Security Zones → Public → Add Policy to Zone Public

[\(Back to instructions\)](#)

- Switch**
 - Ports
 - Port Authentication
 - Port Security
 - Storm Control
 - Link Aggregation
 - VLANs
 - Spanning Tree
 - MAC Forwarding
 - Class Of Service
 - Port Scheduler
- Router / Bridge**
 - Default Gateway
 - Routing
 - Route table
 - IP Interfaces
 - Loopback Interfaces
 - GRE Tunnels
 - QoS Wizard
 - QoS Maps
 - Bridging
 - UDP Relay
 - Demand Routing
 - VRRP
- Firewall**
 - Firewall Wizard
 - Firewall / ACLs
 - Security Zones
- Wireless**
 - AC / AP Discovery
 - APs / Radios / VAPs
 - Clients
 - MAC Access List
 - AP Firmware
- VPN**

Add New Policy -- Select Policy Type

Select which type of policy to create. Explanations of each policy type are listed below.

Policy Type: [Select which policy type to create, then click Continue.](#)

Policy Types Explained

The following policy types may be configured:

- Port Forward:** Allows hosts from the 'Public' Security Zone to access all or selected ports on a private server in another Security Zone. Depending on the configuration, a Port Forward will NAT a public IP Address to a private IP Address for all protocols and ports or just a subset, like TCP/FTP and TCP/WWW. Typically used when Security Zone 'Public' is applied to interfaces connected to the Internet.
- Many:1 NAT:** Allows hosts from the 'Public' Security Zone to share a single public IP address for Internet access. Also known as Internet connection sharing. Typically used when Security Zone 'Public' is applied to interfaces connected to a private (local) network.
- Admin Access:** Used to allow administrative access to the NetVanta from hosts in the 'Public' Security Zone.
- Filter:** Blocks specified traffic from the 'Public' Security Zone from entering any other Security Zone.
- Allow:** Allows specified traffic from the 'Public' Security Zone to continue toward all other Security Zones unaffected.
- Static 1:1 Outbound NAT Pool:** Allows each local host in a given range from the 'Public' Security Zone to have a unique public IP address for Internet access. Typically used when Security Zone 'Public' is applied to interfaces connected to a private (local) network.
- Static 1:1 Inbound NAT Pool:** Allows each local host in a given range from the 'Public' Security Zone to access hosts in a given range on a private (local) network in another Security Zone. This policy type will NAT a public IP address to a private IP address. Typically used when Security Zone 'Public' is applied to interfaces connected to the Internet.
- Advanced:** Allows low-level configuration of all policy parameters.

Remote Access 4 of 4

Data → Firewall → Security Zones → Public → Add Policy to Zone Public → Admin Access

[\(Back to instructions\)](#)

- Data
 - Switch
 - Ports
 - Port Authentication
 - Port Security
 - Storm Control
 - Link Aggregation
 - VLANs
 - Spanning Tree
 - MAC Forwarding
 - Class Of Service
 - Port Scheduler
 - Router / Bridge**
 - Default Gateway
 - Routing
 - Route table
 - IP Interfaces
 - Loopback Interfaces
 - GRE Tunnels
 - QoS Wizard
 - QoS Maps
 - Bridging
 - UDP Relay
 - Demand Routing
 - VRRP
 - Firewall**
 - Firewall Wizard
 - Firewall / ACLs
 - Security Zones

Add New Policy to Security Zone 'Public'

Policy Type:	Admin Access	<i>Used to restrict administrative access to the NetVanta.</i>
Policy Description:	Remote	<i>Optional description for this policy</i>
Admin Access Data		
	<input checked="" type="radio"/> Any	
	<input type="radio"/> Specified	<i>The NetVanta will only allow admin access from the specified address.</i>
Public Address:	Address: <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
	Mask: <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
Admin Access Type:	<input type="checkbox"/> HTTP <input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP	<i>These are the methods used to access the NetVanta remotely.</i>
	<input checked="" type="checkbox"/> HTTPS <input type="checkbox"/> Telnet	
	<input type="checkbox"/> FTP <input type="checkbox"/> Ping	

Configuring QoS

The AdTran 3120/3130 comes partially preconfigured for QoS when ordered directly from FreedomVoice. If the router is reset or the router has been purchased from a different source, you can follow these instructions to set up QoS. There are two ways to edit router settings: through the GUI (Graphical User Interface) or CLI (Command Line Interface).

First, enable traffic shaping on the public (WAN) interface and set your measured upload rate.

1. From "System" in the left column, click on "Public Interface".
2. Check the "Traffic-Shaping" box.
3. Enter a traffic-shaping rate equal to that of your measured upload speed.
4. At the bottom of the screen click the "Apply" button.
5. At the top of the screen click the "Save" button.

The screenshot shows the 'Configuration for Public Interface' page. The left sidebar has 'System' expanded, with 'Public Interface' selected. The main content area shows the following configuration:

Basic configuration for the Public interface.	
Description:	Description label (optional)
Enable: <input checked="" type="checkbox"/>	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 : 5F : 63 : 60	The factory Media Access Control address
MAC Address Masquerade: <input type="checkbox"/>	Check to allow MAC Address Masquerade
MAC Address: : : : : :	Set the masquerade Media Access Control address
Traffic-Shaping: <input checked="" type="checkbox"/>	Enable traffic-shaping
Traffic-Shaping rate: 10000000	Outbound rate in bits per second <1000-100000000>
Interface Mode: IP routing	Select an interface mode
Wireless Control Protocol	
Enabled AWCP: <input checked="" type="checkbox"/>	Enable/Disable Wireless Control Protocol.
IP Settings	

Configuring QoS with the GUI, Step 1: Create Access Control Lists

Data → Firewall / ACLs → Configure ACLs

The screenshot shows the 'Access Control Lists' configuration page. The left sidebar has 'Data' expanded, with 'Firewall / ACLs' selected. The main content area shows the following configuration:

New ACLs can be added by clicking the "Add New ACL" button. Existing ACLs can be modified, deleted, or their evaluation order may be changed using the list below.
WARNING: Removing or modifying an existing ACL could affect network traffic.

Add New ACL

ACL Name: *The name to uniquely identify this ACL.*

ACL Type: Extended *A standard ACL controls traffic only by the source IP address.*
 Standard

Modify/Delete ACLs

To view or modify an existing ACL, click the "Name" link in the desired row.

<input type="checkbox"/>	ACL Name	ACL Type	Security Zone(s)
<input type="checkbox"/>	Audio_ACL	Extended	---
<input type="checkbox"/>	Signal_ACL	Extended	---
<input type="checkbox"/>	web-acl-3	Extended	Public
<input type="checkbox"/>	wizard-ics	Standard	Private

Start by creating an ACL which will be used to identify the SIP signaling traffic so that later on we can mark the packets with CS3.

1. From "Data" in the left column, select "Firewall / ACLs".
2. Scroll to the bottom of the page and click "Configure ACLs".
3. Enter an ACL name ("Signal"), select "Extended" and then click "Add New ACL".
4. Click on the new "ACL" name and click "Add New Traffic Selector".
5. Set the Filter Type to "Permit".
6. Select "UDP" from the Protocol drop down.
7. Under Destination Data/Destination ports check "Specified".
8. Select "Range" from the drop down.
9. In the first box, enter 5060 and in the second box enter 5061.
10. At the bottom of the screen click the "Apply" button.
11. At the top of the screen click the "Save" button.

Next, create another ACL that will be used for traffic shaping by identifying inbound non-phone traffic. Note, FreedomVoice Ships the router with this ACL set to look for all inbound TCP traffic. This rule is very generic. You should first have your phones segregated on their own separate logical network. Then, modify this ACL with the instructions below to traffic shape the other devices so they will not interfere with phones when downloading.

1. **If you already have this ACL in your router, skip to step 5. If not, start at step 2.**
2. From "Data" in the left column, select "Firewall / ACLs".
3. Scroll to the bottom of the page and click "Configure ACLs".
4. Enter an ACL name ("Shaping"), select "Extended" and then click "Add New ACL".
5. Click on the "ACL" name and click "Add New Traffic Selector".
6. Set the Filter Type to "Permit".
7. Select "ANY" from the Protocol drop down.
8. Under Destination Data/Destination Host/Network, check "IP Address".
9. In the 4 "Address" boxes, enter your computer (non-phone) network.
10. In the 4 "Mask" fields, enter the network mask for the computer (non-phone) network.
11. At the bottom of the screen click the "Apply" button.
12. At the top of the screen click the "Save" button.

NOTE: If you cannot segregate the phones onto their own network, the best you can do here is identify TCP traffic. Follow the screenshot below titled "TCP shaping only" for the proper settings.

TCP shaping only (use this if you don't have a separate logical network for phones)

Modify Custom ACL Entry

Enter the information on this form to specify which packets will trigger the specified action.

Filter Type: Permit Deny [?](#)

Protocol: tcp [?](#)

ICMP Message Type (ICMP Only): Any Well Known [?](#)

Source Data

Source Host/Network: Any IP Address Hostname

Address: . . . *Source IP Address or a hostname of sessions originating in Security Zone 'VPN' that should be affected.*

Mask: . . .

Source Ports (TCP/UDP Only): Any Well Known to

to *Source ports of sessions originating in Security Zone 'VPN' that should be affected.*

Destination Data

Destination Host/Network: Any IP Address Hostname

Address: . . . *Destination IP Address of sessions originating in Security Zone 'VPN' that should be affected.*

Mask: . . .

Destination Ports (TCP/UDP Only): Any Well Known to

to *Destination ports of sessions originating in Security Zone 'VPN' that should be affected.*

Data → Firewall/ACLs → Configure ACLs → Add New ACL → (ACL) → Add New Traffic Selector

Modify Custom ACL Entry

Enter the information on this form to specify which packets will trigger the specified action.

Filter Type: Permit Deny ?

Protocol: any [] ?

ICMP Message Type (ICMP Only): Any Well Known [] ?

Source Data

Source Host/Network: Any IP Address Hostname

Address: [] . [] . [] . []
Mask: [] . [] . [] . []

Source IP Address or a hostname of sessions originating in Security Zone 'VPN' that should be affected.

Source Ports (TCP/UDP Only): Any Well Known [] Specified [] to []

Source ports of sessions originating in Security Zone 'VPN' that should be affected.

Destination Data

Destination Host/Network: Any IP Address Hostname

Address: 192 . 168 . 2 . 0
Mask: 255 . 255 . 255 . 0

Destination IP Address of sessions originating in Security Zone 'VPN' that should be affected.

Destination Ports (TCP/UDP Only): Any Well Known [] Specified [] to []

Destination ports of sessions originating in Security Zone 'VPN' that should be affected.

Cancel Apply

Configuring QoS with the GUI, Step 2: Create QoS Maps

Three QoS maps will be created.

- One for marking SIP packets with CS3
- One for identifying VoIP packets via EF and CS3 markings and then prioritizing them over other traffic
- One for enforcing inbound QoS by traffic shaping (rate limiting) non-phone traffic.

First, create a Traffic Marking QoS Map:

1. From "Data" in the left column, select "QoS Maps".
2. Under "Add New QoS Map", in the "Map Name" field type a description ("marking").
3. In the "Sequence Number" field enter a high priority number such as 10. The available range is 0-65535 and click "Add". (*lower numbers = higher priority*)
4. You'll be taken to the configuration page for your new QoS map.
5. Select the "Packet Matching" tab. Check "List" and select the signal ACL you created in the previous step.
6. Select the "Packet Marking" tab and check "DCSP alias", then choose "CS3 (011000)".
7. At the bottom of the screen click the "Apply" button.
8. At the top of the screen click the "Save" button.

Data → QoS Maps

Add / Modify / Delete QoS Map

Configure a QoS map ?

Add New QoS Map

Map Name: QoS map tag. (maximum of 79 characters)

Sequence Number: Sequence to insert into QoS map entry. Valid values are 0-65535.

Modify/Delete a QoS Map

To view or modify an existing QoS map, click the link in the desired row. A '*' in the bandwidth column denotes class based bandwidth-shaper information. This information will be displayed in parentheses separated by commas. Otherwise, the bandwidth is priority based.

<input type="checkbox"/>	QoS Map	QoS-Policy	Matching	Marking	Bandwidth
<input type="checkbox"/>	Marking-10	<none>	ACL	DSCP(cs3)	disabled
<input type="checkbox"/>	Queuing-10	<none>	DSCP(ef cs3)	disabled	unlimited
<input type="checkbox"/>	Shaping-10	<none>	disabled	disabled	disabled

QoS-policy assignment and statistics

Modify Assignment

Assign a QoS-policy to an interface's input/output.

Name	Available Bandwidth(Kbps)	Inbound QoS-Policy	Outbound QoS-Policy
vlan 1	75000	Marking ▼	Shaping ▼
eth 0/1	75000	<none> ▼	Queuing ▼

Data → QoS Maps → Packet Matching

QoS Map Setup for Marking-10

Match All *If Match All is enabled and multiple match options are selected for this QoS Map entry, then they must ALL be true before a packet will be processed.
NOTE: This option is typically not required.*

QoS-Policy <none> *Specify child QoS-Policy.*

Packet Matching | Packet Marking | Queuing

Disable *Disable packet matching.*

Match any *Match Any packets.* ?

VLAN Id *Match IP packets by VLAN Id (1-4095).*

DLCI *Match all packets on a frame relay DLCI (16-1007).*

IP RTP
 Start Port
 End Port *Match IP RTP packets.* ?
 Enable Even and Odd Ports

Precedence
 0 1 2 3
 4 5 6 7 *Select up to 8 different precedence values. (0 - 7)*

List Signal *Match using access-list. Go to the 'Firewall' page and click on the 'Configure ACLs' button at the bottom of the page to configure an 'Extended ACL'.*

Bridged *Match frames being bridged.*

NetBEUI *Match bridged NetBEUI frames.*

DSCP *Match IP packet DSCP value(s).*

Data → QoS Maps → Packet Marking

QoS Map Setup for Marking-10

Match All *If Match All is enabled and multiple match options are selected for this QoS Map entry, then they must ALL be true before a packet will be processed.
NOTE: This option is typically not required.*

QoS-Policy <none> *Specify child QoS-Policy.*

Packet Matching | **Packet Marking** | Queuing

Disable *Disable all marking.*

DSCP *DSCP field value (0-63)*

DSCP alias CS3 (011000) *DSCP alias* ?

Precedence *Precedence field value (0-7)*

CoS *Mark packet Ethernet VLAN Priority field with value (0-7).*

Next, create a traffic queuing QoS Map:

1. From “Data” in the left column, select “QoS Maps”.
2. Under “Add New QoS Map”, in the “Map Name” field, use a name such as “queuing”.
3. In the “Sequence Number” field enter a high priority number such as 10.
4. You’ll be taken to the configuration page for your new QoS map.
5. Select the “Packet Matching” tab.
6. Check “DSCP” and click “Add a new DSCP Line”.
7. Select “EF” from the first dropdown.
8. Select “CS3” from the second dropdown.
9. Select the “Queuing” tab and select the radio button “Unlimited Priority Bandwidth”.
10. At the bottom of the screen click the “Apply” button.
11. At the top of the screen click the “Save” button.

Lastly, create a traffic shaping QoS Map:

1. From “Data” in the left column, select “QoS Maps”.
2. Under “Add New QoS Map”, in the “Map Name” field, use a name such as “Shaping”.
3. In the “Sequence Number” field enter a high priority number such as 10.
4. You’ll be taken to the configuration page for your new QoS map.
5. Select the “Packet Matching” tab.
6. Check “List” and select the “Shaping” ACL created earlier.
7. Select the “Queuing” tab and select the radio button “Traffic Class Queuing”.
8. Under “Bandwidth”, check the box next to “Percent Remaining”.
9. Enter “100” in the “Percent Remaining” field.
10. At the top of the screen click the “Save” button.

Configuring QoS with the GUI, Step 3: Apply QoS

Finally, attach the QoS policies to the Vlan 1 and Eth0/1 interfaces:

1. From “Data” in the left column, select “QoS Maps”.
2. Under QoS-policy assignment and statistics, locate “vlan 1”.
3. For vlan 1 “Inbound QoS-Policy”, select your “Marking” QoS policy.
4. For eth 0/1 “Outbound QoS-Policy”, select your “Queuing” QoS policy.
5. For vlan 1 “Outbound QoS-Policy”, select your “Shaping” QoS policy.
6. At the bottom of the screen click the “Apply” button.
7. At the top of the screen click the “Save” button.

- QoS is now complete
-

Technical Support

Technical support for FreedomVoice is available from 3:00 AM PST to 6:00 PM PST, Monday through Friday, Saturday from 6:30am PST to 3:30pm PST and can be reached either by phone or by email. Emergency support is available 24/7.

Phone: 888-955-3520 ext. 2

Use this number to reach a trained FreedomVoice technical support representative during normal support hours. If calling outside of normal hours, you will be provided the option to either leave a voicemail message or connect to the emergency support service (see below).

Numerous documents and support materials are available through the FreedomVoice Weblink. Please log into Weblink and select the support tab and review the documentation that is available online there.

Support Email: customercare@freedomvoice.com

Emails are automatically forwarded to our ticketing system. An auto-reply will be sent within a few minutes indicating the case number generated. Emails are generally returned within two hours during normal support hours, but may take longer depending on the current volume of tickets received. All emails should, however, be returned same day. For an issue that requires a faster turn-around time, please use the phone numbers listed above.