

nextiva

**Nextiva Clarity**  
User Guide

[nextiva.com/support](https://nextiva.com/support)

# Contents

---

Hardware Configuration .....	3
Establishing a physical connection .....	3
Testing your internet connection .....	4
Hardware lights.....	4
User Dashboard (GUI) .....	5
Authentication .....	5
Site Overview .....	6
Diagnostics .....	8
Change Log.....	8
MOS History.....	9
Network Health .....	10
Security and Compliance.....	17
General Settings.....	19
DHCP Server.....	20
Interfaces .....	22
VLAN.....	26
Firewall.....	27
Static Routes .....	30
Traffic Shaping .....	31
VPN.....	32

## Hardware Configuration

### Establishing a Physical Connection

When you receive your Nextiva Clarity package, you should have several items in the box:

- A Nextiva Clarity device (NA250B, NA250BW)
- An Ethernet cable
- Power supply
- A Getting Started guide

The Nextiva Clarity device (based on the 12 character MAC address) is listed in the Nextiva Clarity online dashboard.

To get started, take a single computer or laptop and move to where the router will be activated. Turn off the laptop/PC, (Personal Computer) so you can generate a clean ARP (Address Resolution Protocol) record. Connect the provided Ethernet cord to the WAN Port on the Nextiva Clarity device. Next, connect the other end of the Ethernet cord to your modem and power on the Nextiva Clarity device. It will take 2-10 minutes to fully boot depending on your Internet speed. Once the device has booted up, plug your laptop/PC into the LAN port and turn it on (*Figure 1-1*).



*Figure 1-1: Nextiva Hardware*

**Important Note:** For this product to work properly, please verify with your ISP (Internet Service Provider) that your modem is in “Transparent Bridge Mode”. This is a common requirement for any network using a modem/router combination device or gateway.

You should now be able to connect the device to the Internet. Once you have confirmed an Internet connection, plug in all applicable switches to the Nextiva Clarity device followed by connecting any phones or computers into the switch. Once you have established these connections, you will need to reboot/restart all computers and phones to ensure they obtain a new IP (Internet Protocol) address.

## Testing your Internet connection

On your laptop or PC that is directly connected to your Nextiva Clarity device, open an Internet browser and type [www.nextiva.com](http://www.nextiva.com). One of two screens will appear, either a 'calibration' screen or a 'failed to detect screen' (Figure 1-2). If the 'calibration' screen is displayed, wait 1-2 minutes, and then you will be connected to [www.nextiva.com](http://www.nextiva.com).

If the 'failed to detect' screen is displayed, you may need some basic information from your ISP (below).

- Public, Static IP Address, Subnet Mask, Default Gateway
- PPPOE/PPTP Username and Password

Enter this information into the defined text boxes on the screen and select **Save**.

**Important Note:** Once you input the information on the screen and it successfully connects, the information will be saved to the dashboard for completion. You should not have to re-enter this information again. After you have saved, open your Internet browser and type in [www.nextiva.com](http://www.nextiva.com). The 'calibration' page will display; wait 2-3 minutes for the page to complete the process and you should successfully be online.



Figure 1-2: Calibration Screen (left) Failed to Detect Screen (right)

## Hardware lights

- 1 Solid light – Unit Has Power
- 2 Solid lights – Internet connection has been detected
- 1 Solid light, 1 Flashing light – Calibrating, Internet connection is in progress
- 3 Solid lights – System is ready and operational

## User Dashboard (GUI)

---

**Note:** All screenshots are displayed using the 'Advanced View' in the User Dashboard.

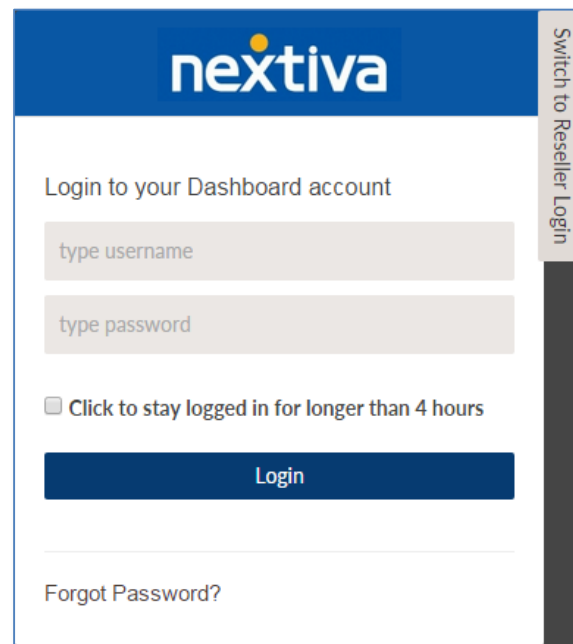
### Authentication

Users have the option to log in to their Nextiva Clarity device to review settings, statistics and make changes. Permission to log in to the GUI (Graphical User Interface) must be granted by Nextiva in order to view or modify these settings. For dedicated network administrators, please contact Nextiva to request an administration login for your Nextiva Clarity device if you have not already been provided one. You must be an 'Authorized User' for the account and have access to your four-digit security PIN to complete the transaction.

To ensure ongoing network security, Nextiva may also lease a temporary login (designed to expire at midnight) for singular transactions, GUI changes and updates. To request a temporary login, please contact Nextiva.

Once you have been given these credentials, log in to the Nextiva Clarity device by navigating to <http://nextiva.mycloudconnection.com> and selecting the + icon located in the upper right-hand corner (*Figure 1-3*).

Next, select the option labelled, **Nextiva Login to your Dashboard account also known as a 'User Login'**. You will be prompted to enter your Username and Password.



*Figure 1-3: Nextiva Dashboard Login*

## Site Overview

The Nextiva user dashboard has a lot of information immediately available to you upon logging in. This will be your top-level, or birds-eye view, of the Nextiva Clarity device. You will be able to view the following network data (*Figure 1-4*):

- Daily Bandwidth Monitoring – Daily throughput in megabits
- Location Information – Physical device location and IP information
- Geo-Coded Google Map of location
- MOS Rating – Quality of VoIP calls
- Latency – Connection response time
- Jitter – Response time
- SLA (Service Level Agreement) - The amount of time your site is online
- Packet Loss – Packets that have been lost or dropped
- CPU (Central Processing Unit) – Usage amounts
- Memory – Usage amounts
- ARP Table – Devices that are connected to the appliance
- Alerts
- Blocked Attacks

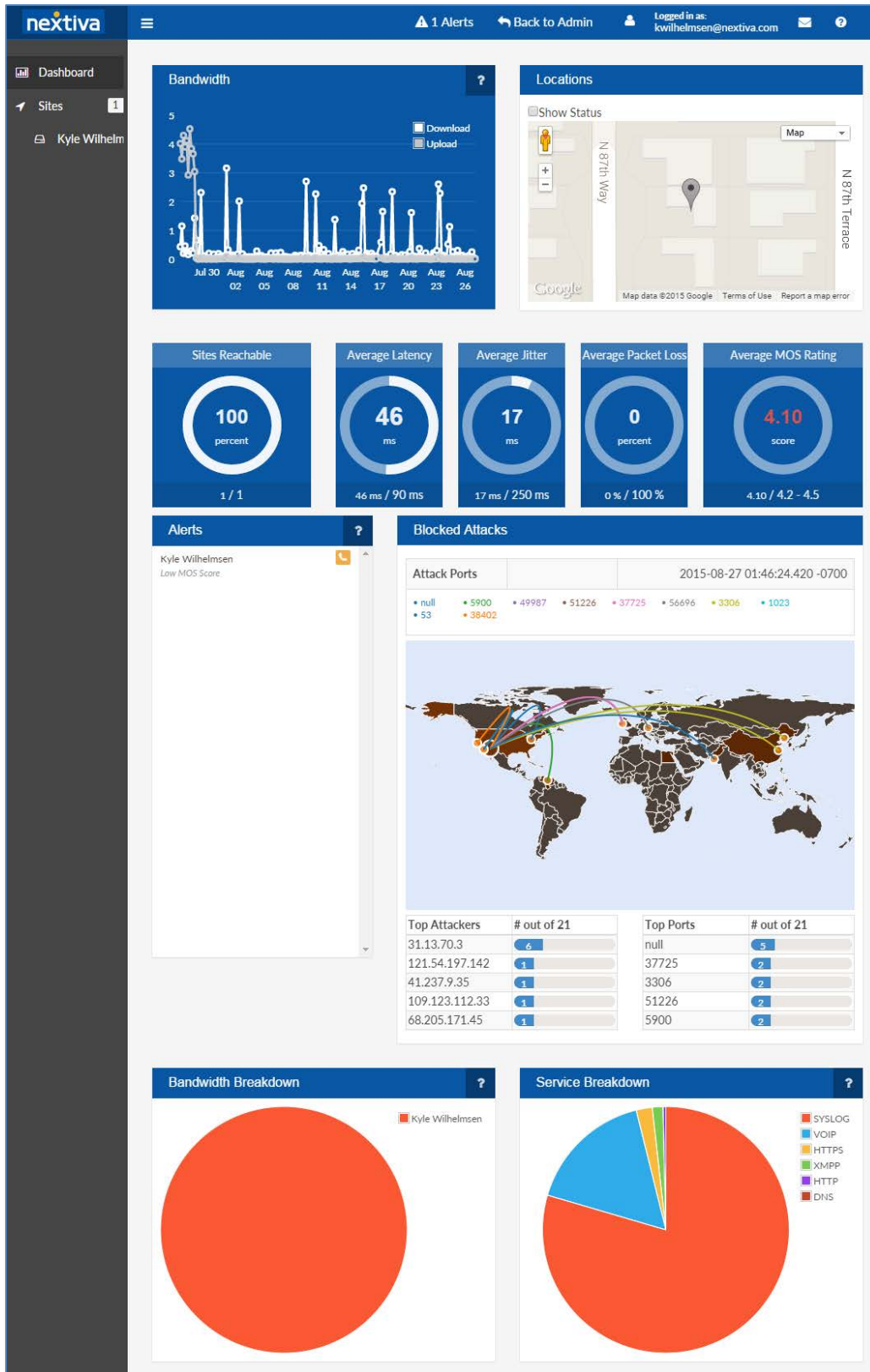


Figure 1-4: Site Overview

## Diagnostics

Diagnostics will provide several options to evaluate the status of your network along with any changes, updates or degradations occurring with your hardware. You will have the option to view the following settings within the diagnostics view:

- Change Log
- MOS History
- Network Health
- Packet Capture
- Speed Tests
- Sync Logs

## Change Log

The Change Log allows the network administrator to view and monitor any changes made to the configuration of the Nextiva Clarity device or firewall updates. This information is stored indefinitely and logs can be searched through the Nextiva GUI. Each log will display the following categories:

- Date of Change
- Username
- Action
- Item
- Changes

By typing in key-word text into the **Search** box you can locate specific information, such as changes made by username or automatic updates completed by the 'system'. You may also search by action, such as 'update,' to itemize all similar updates through the change log (*Figure 1-5*).

Change Log for Site 2225

There are some limitations to this log.

- Item relationships are not logged. For example, changing the Interface of a Firewall Rule will not currently be shown.
- Some numerical or true/false values are logged even when they haven't changed. For example, log entries may show Status = 1 or Port = 80 even when there was really no change.

Current Time:  
2015-08-27 15:53:05 MST

10 records per page

Search: System

Date	Username	Action	Item	Changes
2015-08-26 12:36:13 MST	system	update	Site Status 2225 (on Site 2225)	Alive = true
2015-08-17 20:06:57 MST	system	update	Site Status 2225 (on Site 2225)	Alive = true
2015-08-01 00:42:33 MST	system	update	Site 2225	Firstbilledat = Sat, 01 Aug 2015 00:00:00 +0000

Figure 1-5: Change Log



## MOS History

MOS (Mean Opinion Score) information is stored for your network for 30 days. This allows you to evaluate VoIP phone calls completed on the network and display a MOS rating for all calls. In multimedia (audio, voice telephony, or video), especially when codecs are used to compress the bandwidth requirement, the MOS provides a numerical indication of the perceived quality from the users' perspective of received media after compression and/or transmission. The MOS is expressed as a single number in the range 1 to 5, where 1 is lowest perceived audio quality and 5 is the highest perceived audio quality measurement (*Figure 1-6*). Expected MOS ratings should range between 4.0 - 4.5 indicating a high quality phone call.

5	Excellent
4	Good
3	Fair
2	Poor
1	Bad

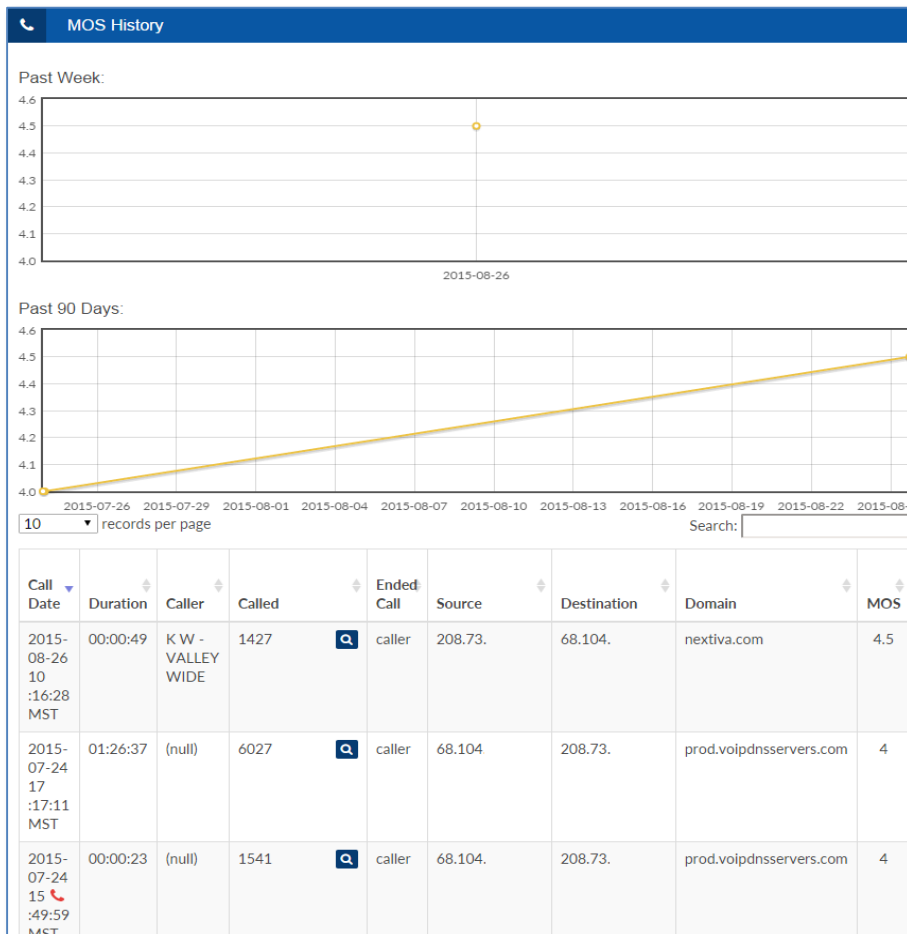


Figure 1-6: MOS History

## Network Health

The Network Health selection is located within the Diagnostics section and can help a network administrator quickly review the overall performance of a network. Located in this section you will be able to perform a traceroute, view bandwidth and latency performance, as well as SLA (Service Level Agreement) information related to the network. Also located within Network Health is the option to perform an “Intensive 48-Hour Latency Test”. This is a useful tool to help network administrators identify consistent packet loss or high-latency issues.

### Traceroute (Figure 1-7)

A traceroute is a computer network diagnostic tool for displaying the route and measuring transit delays of packets across the Internet. A traceroute records the round-trip times of the packets received from each successive host in the route; the sum of the mean times in each hop indicate the total time spent to establish the connection.

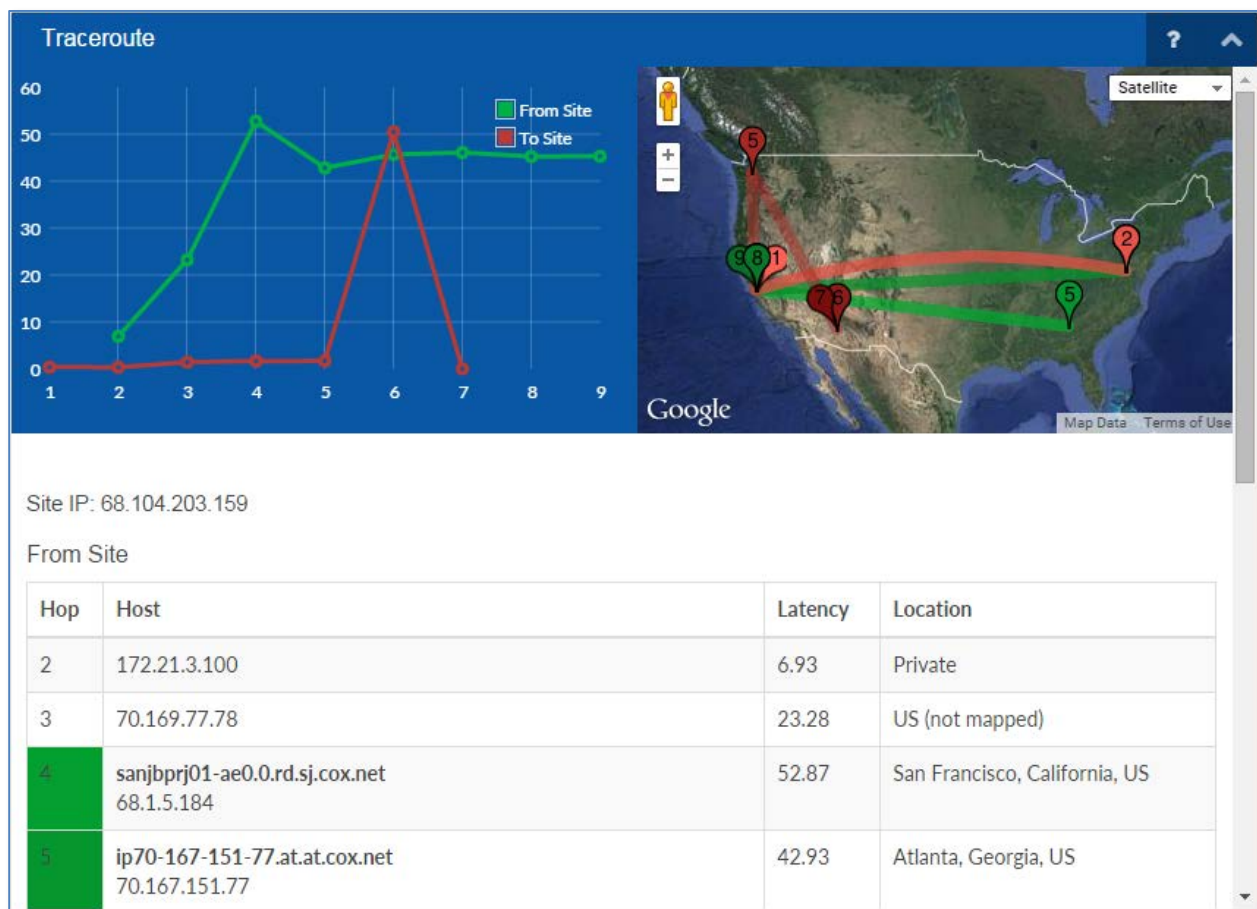


Figure 1-7: Traceroute

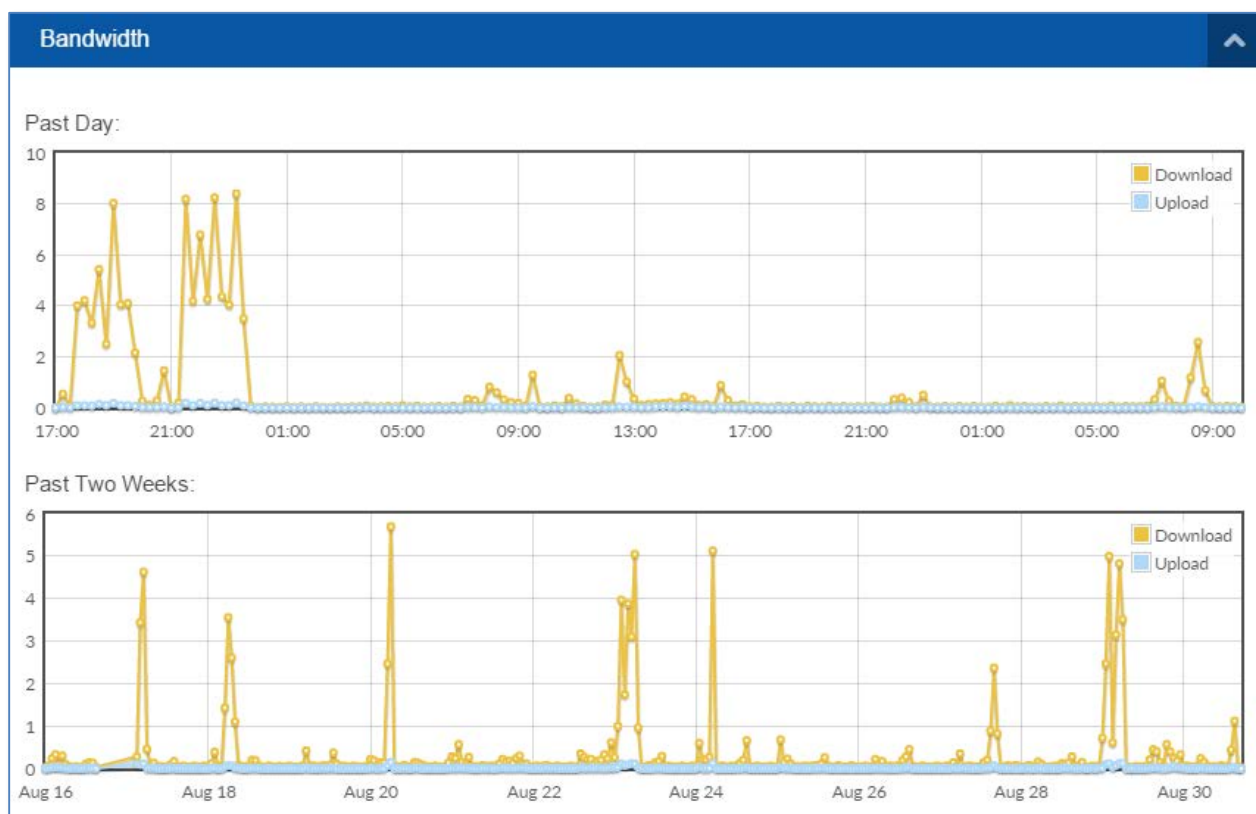
## Bandwidth (Figure 1-8)

### Network bandwidth capacity

The term Bandwidth sometimes defines the net bit rate, channel capacity, or the maximum throughput of a logical or physical communication path in a digital communications system. For example, bandwidth tests measure the maximum throughput of a computer network.

### Network bandwidth consumption

Bandwidth in bit(s) may also refer to consumed bandwidth, corresponding to achieve throughput, i.e., the average rate of successful data transfer through a communication path. This sense applies to concepts and technologies such as bandwidth shaping, bandwidth management, bandwidth throttling, bandwidth cap, and bandwidth allocation. A bit stream's bandwidth is proportional to the average consumed signal bandwidth in Hertz (the average spectral bandwidth of the analog signal representing the bit stream) during a studied time interval.



### Latency (Figure 1-9)

Latency refers to a short period of delay (usually measured in milliseconds) between when an audio signal enters and when it emerges from a system. Potential contributors to latency in an audio system include analog-to-digital conversion, buffering, digital signal processing, transmission time, digital-to-analog conversion, and the speed of sound in air.

On a stable connection with sufficient bandwidth and minimal latency, VoIP systems typically have a minimum of 20 ms inherent latency and target 150 ms as a maximum latency for general consumer use. With end-to-end QoS managed and assured rate connections, latency can be reduced to analogue PSTN/POTS levels. Latency is a larger consideration in these systems when an echo is present.

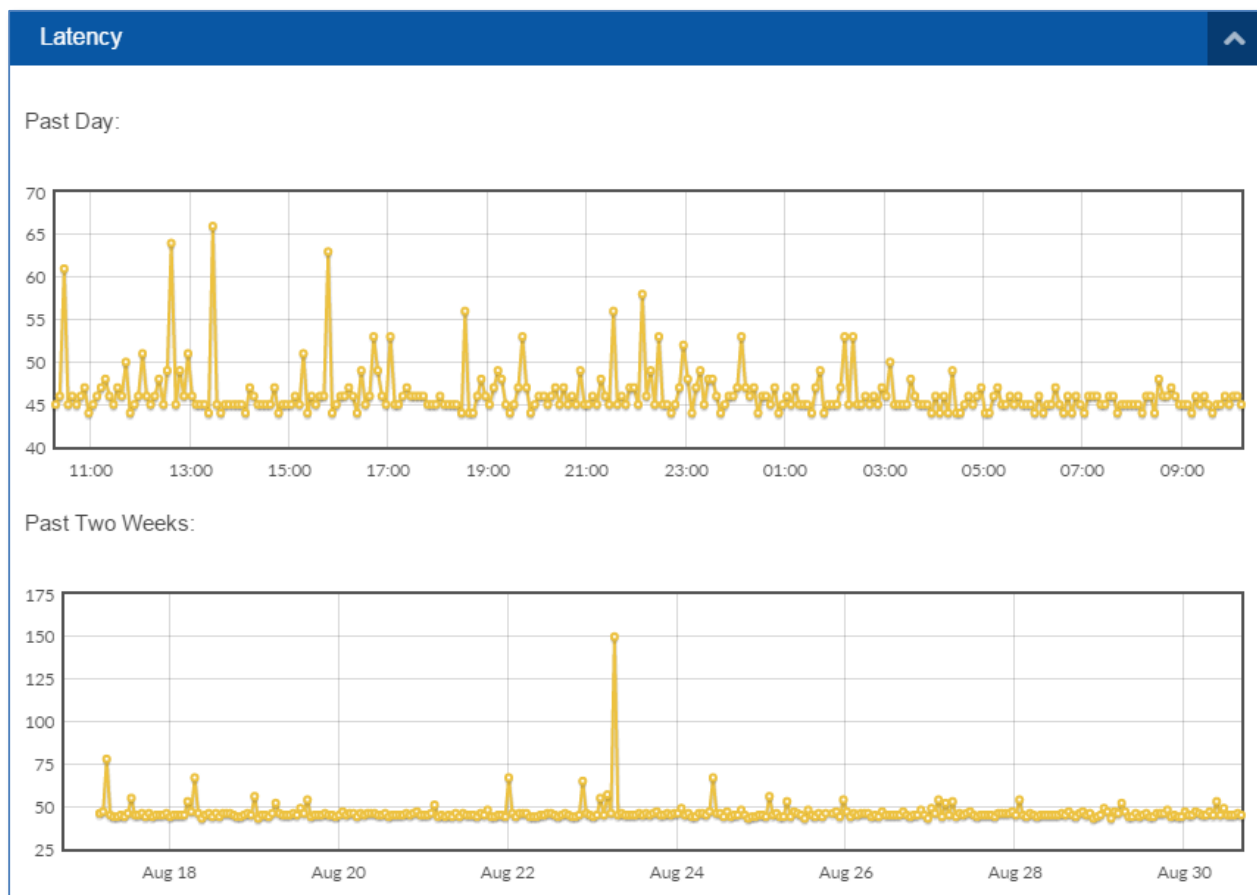


Figure 1-9: Latency

### SLA (Service Level Agreement) (Figure 1-10)

The SLA is a percentage value shown on the **Site** page, and is based on the number of ping responses received over the past 30 days. Gaps in the graph below represent a likely ISP outage or other communication issue between the Site and the Site's Server POP (Post Office Protocol).

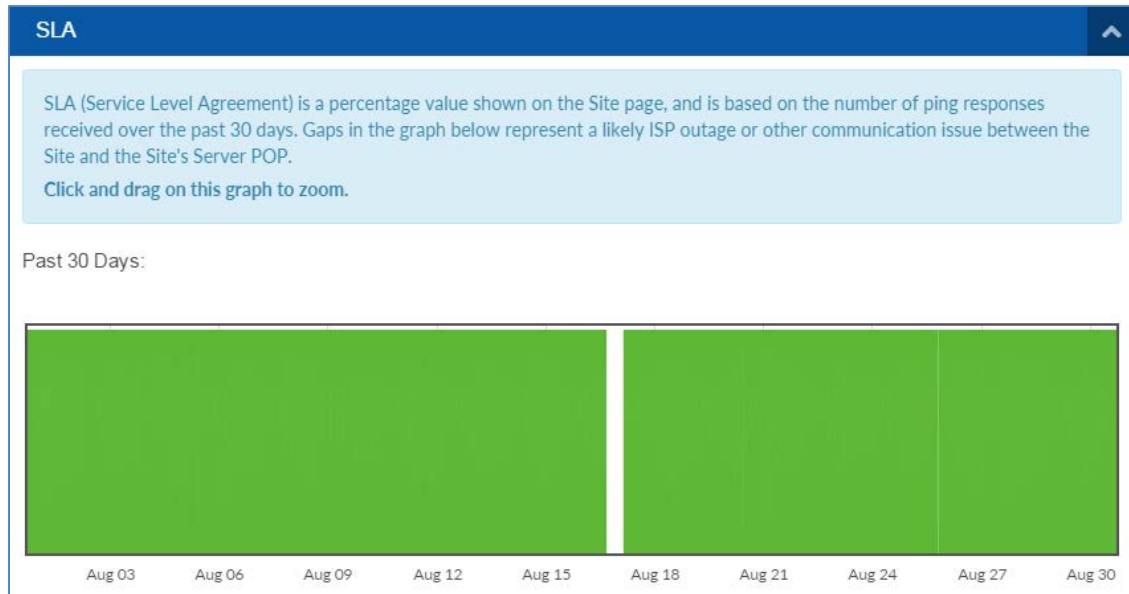


Figure 1-10: SLA

### Intensive 48-Hour Latency Test (Figure 1-11)

This tests latency at a very intense level for 48 hours to help diagnose connection issues that may not appear on normal 5-minute interval tests. Data will disappear after 72 hours. It is recommended that this test be performed during peak business hours and it will not cause any disruption or degradation in service.

Figure 1-11 Intensive 48-Hour Latency Test

### Packet Capture (Figure 1-12)

Packet Capture is a computer networking term for intercepting a data packet that is crossing or moving over a specific computer network. Once a packet is captured, it is stored temporarily so that it can be analyzed. The packet is inspected to help diagnose and solve network problems and determine whether network security policies are being followed. Network managers analyze and manage overall network traffic and performance. To examine and capture real-time running packets over a network, different packet capturing techniques are used. You may also be required to have software available for viewing the packet captures, such as Wireshark™ for example. Once the recording has been stopped by the administrator or timed out after five minutes, your Internet browser will attempt to download the file.

Select from the following:

- Start Packet Capture (WAN)
- Start Packet Capture (LAN)

**Note:** Once the recording begins, the results will time out in approximately 5 minutes.



Figure 1-12: Packet Capture

## Speed Tests (Figure 1-13)

These speed tests are based on 100-megabyte downloads to public servers, which will provide a conservative result compared to other speed test websites. However, conservative values are preferred for VoIP traffic shaping in order to provide a smooth, consistent experience. Traffic shaping can be disabled via the Advanced View in the Traffic Shaping menu, however it is not recommended if this site has VoIP phones. Speed tests are generated when the firewall reboots. It is recommended to generate speed tests during normal business hours in order to accurately measure typical business speeds.



Figure 1-13: Speed Tests

### Sync Logs (Figure 1-14)

Sync Logs show how often the Nextiva Clarity device and firewall are syncing up with the Nextiva cloud dashboard. Like many VoIP devices, the Nextiva Clarity device is provisioned and configured via the “cloud”. To ensure on-going security, it is necessary for the Nextiva Clarity device to continually sync with the server. Within this section you can verify how often this process occurs, as well as use this information for network troubleshooting purposes.

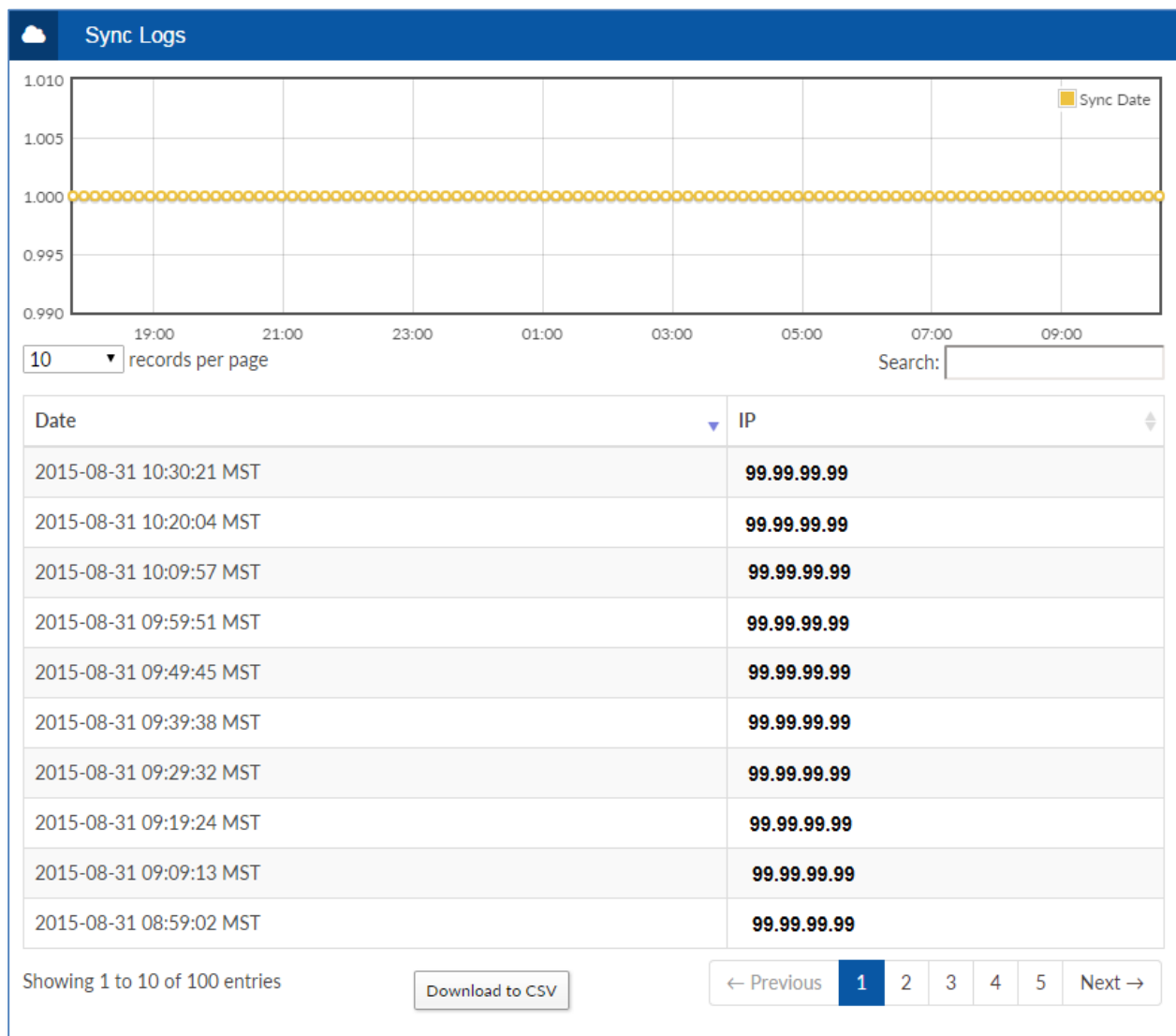


Figure 1-14: Sync Logs



## Security and Compliance

### PCI Compliance (Figure 1-15)

The Payment Card Industry (PCI) officially launched the PCI Security Standards Council in 2006 and develops, maintains and manages the PCI Security Standards, which include Data Security Standards (DSS), Payment Application Data Security Standards (PA-DSS) and PIN Transaction Security (PTS). These standards cover everything from the point of entry of card data into a system to how the data is processed through secure payment applications. Their goal is to protect and educate industry players such as merchants, processors, financial institutions, and any other organizations that store, process and transmit cardholder data around the world. This council was founded by American Express, Discover Financial, JCB International, Mastercard, Visa Inc., and Visa Europe.

Nextiva has developed network PCI compliance options for consumers. This service will provide users with real-time alerts regarding their network PCI compliance. This option will help network administrators monitor and calculate risks associated with DSS requirements. PCI summary information is available for view at all times; however, for more detailed information and risk assessment an add-on feature will be required.

**Note:** This service is an add-on feature and will require an additional recurring monthly fee.

Section	Grade
PCI Compliance - Network	<span style="color: red;">Fail</span> (1 Fail, 3 Warning, 13 Total)
PCI Compliance - User Security	<span style="color: red;">Fail</span> (1 Fail, 5 Warning, 12 Total)
PCI Compliance - Network Risks	<span style="color: green;">Pass</span> (0 Fail, 0 Warning, 0 Total)
Traffic Security (Past 30 Days)	<span style="color: orange;">Warning</span> (0 Fail, 1 Warning, 3 Total)
Current Firmware	<span style="color: green;">Pass</span> (0 Fail, 0 Warning, 1 Total)

Figure 1-15: PCI Compliance Summary

### HIPAA Compliance (Figure 1-16)

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was enacted to protect health insurance coverage for workers and their families when they change or lose their job. To date, there have been many updates and changes to this Act, which directly impacts medical providers, with requirements to keep medical records secure and confidential. As of 2015, HIPAA compliance awareness has reached a pinnacle and the U.S. government is strictly enforcing these security measures. Medical providers may receive hefty fines as a result of not being HIPAA compliant. As medical records are often provided through digital transmissions, medical providers must have a heightened sense of network security.

Nextiva has developed network HIPAA compliance options for consumers. This service will provide users with real-time alerts regarding their network HIPAA compliance. This option will help network administrators monitor and calculate risks associated with DSS requirements. HIPAA summary information is available for view at all times; however, for more detailed information and risk assessment an add-on feature will be required.

**Note:** This service is an add-on feature and will require an additional recurring monthly fee.

Section	Grade
HIPAA Compliance - Network	Pass (0 Fail, 0 Warning, 8 Total)
HIPAA Compliance - User Security	Fail (1 Fail, 5 Warning, 12 Total)
HIPAA Compliance - Network Risks	Pass (0 Fail, 0 Warning, 0 Total)
Traffic Security (Past 30 Days)	Warning (0 Fail, 1 Warning, 3 Total)

Figure 1-17: HIPAA Compliance Summary

## General Settings

The **General Settings** section of the Nextiva Clarity device allows for standard functionality commonly found in all gateways (*Figure 1-18*). On this page you will find options that allow you to specify:

- Hostname
- Domain
- DNS Servers
- ICMP (Internet Control Message Protocol)
- SIP ALG (Session Initiation Protocol Application Layer Gateway)
- DNS (Domain Name System) Forwarding
- DNS Server override by DHCP/PPP (Point to Point Protocol) on WAN (Wide Area Network)

## Hostname and Domain

Specifying a hostname and domain is commonly a valuable feature to Network Administrators utilizing Microsoft™ networks. This service may apply to administrators utilizing WINS (Windows Internet Name Service), which will simplify active directory naming conventions for local devices over the network. This feature may also help administrators complete DHCP via the 'hostname', as well as improving overall communication by using a private FQDN (Fully Qualified Domain Name). For public FQDNs, Nextiva uses its version called vMPLS (Multiprotocol Label Switching).

## ICMP

This feature determines whether your Nextiva Clarity device will respond to Ping from other network devices. It's more secure to block ICMP traffic from the Internet; however, that will prevent troubleshooting tools such as Ping and Traceroute from working properly.

## SIP ALG

SIP ALG (sometimes called SIP Transformations) is an application layer gateway designed to help manage SIP-based traffic on a network, and is common in many commercial routers. It intends to prevent some of the problems caused by router firewalls by inspecting VoIP traffic packets and modifying them if necessary. Many routers have SIP ALG turned on by default.

**Nextiva Recommendation:** SIP ALG modifies SIP packets in unexpected ways, corrupting them and making them unreadable. This can give you unexpected behavior, such as:

- One-Way Audio: When you call someone and you can hear them, but they cannot hear you or vice versa.
- Incoming Call Failure: Incoming calls do not ring and do not seem to reach your device at all.
- Call Dropping: When the call suddenly drops after any length of time without being terminated by either member of the call.

To avoid registration issues with SIP ALG, we utilize port 5062 for SIP traffic. Beyond that, SIP ALG must be disabled when utilizing service with Nextiva.

## DNS Forwarding

This feature can be disabled if you are experiencing DNS trouble or want DHCP (Dynamic Host Configuration Protocol) clients to use the specified DNS servers directly.

The screenshot shows the configuration interface for DNS settings. It is divided into two main sections: 'Basic Configuration' and 'DNS Servers'.

**Basic Configuration:**

- Hostname:** A text input field.
- Domain:** A text input field.
- Custom VoIP Port for MOS scoring (Blank = default 5060 SIP port):** A text input field.
- ICMP (Ping) on WAN:** A dropdown menu set to 'Do Not Allow'.
- SIP ALG / Proxy:** A dropdown menu set to 'Disabled'.
- Allow DNS server override by DHCP/PPP on WAN:** A dropdown menu set to 'Enabled'.
- DNS Forwarding:** A dropdown menu set to 'Disabled'.
- Save:** A blue button at the bottom left.

**DNS Servers:**

Address	Actions
8.8.8.8	[Edit] [Delete]
208.67.222.222	[Edit] [Delete]

Figure 1-18: General Settings

## DHCP Server

The DHCP menu allows you to configure the Nextiva LAN-side (Local Area Network) options. Here you will find the following settings:

- DHCP Servers
- DHCP Options
- DHCP Reservation List
- DHCP Lease

### DHCP Servers *(Figure 1-19)*


This section will display your current DHCP range available for assignment, as well as the LAN IP address of the Nextiva Clarity device. This example shows the LAN IP as 192.168.1.1 (Default). By selecting the



**Edit** icon, you will be provided additional options such as:

- Turning on/off DHCP
- MAC (Media Access Control) Filtering
- Adjust the DHCP Range
- Adjust the Default Lease Time
- Adjust the Maximum Lease Time

### DHCP Options

When adding additional options to the DHCP menu, you may select the  **Add** icon. In this menu you will be given the ability to complete PXE (Preboot eXecution Environment) such as:

Option 66 – “Next Server” is “tftp-server-name”.

Option 67 – “Boot File” is “bootfile-name”.

Simply specify the option name and value. Values listed on this page may contain a number, IP address, IP address pair, MAC address, or quoted string depending on the option.

### DHCP Reservation

The DHCP server allocates an IP address based on a preconfigured mapping to each client's MAC address when they are connected to the network. This is not the same thing as a static IP address, as static IP addresses are assigned manually and have to be provisioned carefully so that each device has its own address with no overlap.

If your client is configured for WINS and your WINS database becomes corrupt at any time, a simple "ipconfig /release", "ipconfig /renew" from an MS-DOS prompt will force the client to re-register with the primary WINS server.

## DHCP Leases

This section will show you a client table of all devices currently receiving an IP address from the Nextiva Clarity device. This section will also display when the device will renew its IP address.

DHCP Servers				
Interface	Range	Gateway	Status	
LAN	192.168.1.30 - 192.168.1.99	192.168.1.1	Enabled	

DHCP Options		
DHCP Server	Option	Value

DHCP Reservation List			
DHCP Server	MAC Address	IP Address	Description

DHCP Leases				
MAC Address	IP Address	Hostname	Start	End
c4:85:08:0e:8d:14	192.168.1.93	GuestLoaner-LT	2015-08-30 12:29:19 MST	2015-08-31 12:29:19 MST

Figure 1-19: General Settings

## Interfaces

Within this section you are able to modify settings specific to the WAN (Wide Area Network) and LAN (Local Area Network) sides of the Nextiva Clarity device. Nextiva Clarity devices are hardcoded with a failover protocol that helps ensure network connectivity. For example, setting a Nextiva Clarity device up with a static IP address (WAN) at times may impact the device's ability to obtain an Internet connection if moved to another location or a change of ISP occurs. Your Nextiva Clarity device will automatically failover to a DHCP protocol in an attempt to obtain an Internet connection. This process requires the device to restart and the failover threshold timer to occur. It is highly recommended that the settings be actively managed and adjusted when appropriate.

## LAN

Within the LAN configuration page, you will be able to perform the following tasks:

- Modify the router's LAN IP address (*Figure 1-20*)
- Modify the router's Subnet Mask
- Setup Proxy ARP / CIDR (Classless Inter-Domain Routing) Blocks

*Figure 1-20: Edit the LAN IP and Subnet Mask*

Subnet Mask Table (*Figure 1-21*)

<b>/24 (255.255.255.0 - 254 addresses)</b>
-----
/30 (255.255.255.252 - 2 addresses)
/29 (255.255.255.248 - 6 addresses)
/28 (255.255.255.240 - 14 addresses)
/27 (255.255.255.224 - 30 addresses)
/26 (255.255.255.192 - 62 addresses)
/25 (255.255.255.128 - 126 addresses)
/23 (255.255.254.0 - 510 addresses)
/22 (255.255.252.0 - 1,022 addresses)
/21 (255.255.248.0 - 2,046 addresses)
/20 (255.255.240.0 - 4,094 addresses)
/19 (255.255.224.0 - 8,190 addresses)
/18 (255.255.192.0 - 16,382 addresses)
/17 (255.255.128.0 - 32,766 addresses)
/16 (255.255.0.0 - 65,534 addresses)

*Figure 1-21: Subnet Mask Table*

### Proxy ARP / CIDR Blocks (Figure 1-22)

Proxy ARP is commonly used to allow the Nextiva interface to respond to additional IP addresses or networks besides what is assigned in the above LAN section. A Network (CIDR Block) will require the network to proxy under this rule; for example, in CIDR notation like 1.2.3.4/24. You may also leave a description outlining any changes made to this rule.

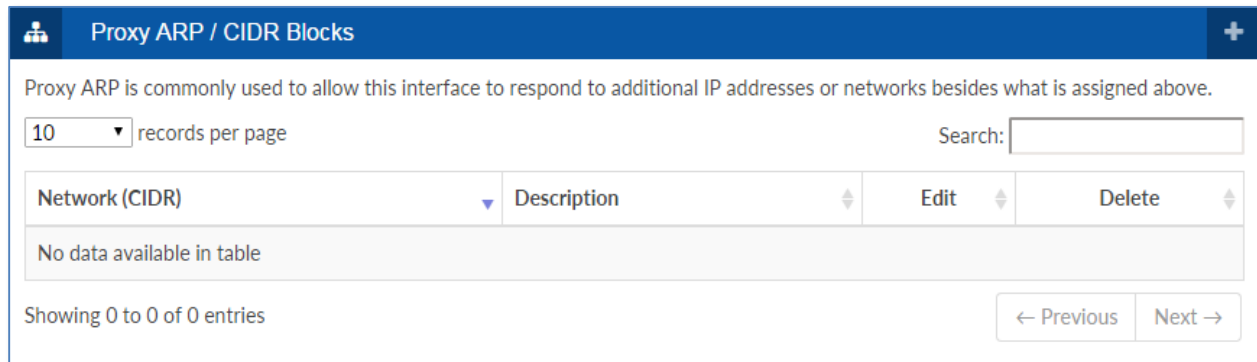


Figure 1-22: Proxy ARP / CIDR Blocks

### WAN (Figure 1-23)

The WAN side of your Nextiva Clarity device is the Internet-facing side. Within this section, you are able to update critical changes that will directly impact your devices ability to receive an Internet connection.

#### WAN Type:

- DHCP
- Static PPPOE (Point to Point Protocol Over Ethernet); requires username and password from ISP.

#### MAC Address

- Override the MAC address of the WAN interface (required for some cable connections)

#### Hostname

- This performs DHCP client identification when requesting a lease.

#### Proxy ARP

- Proxy ARP is commonly used to allow the WAN interface to respond to additional IP addresses or networks besides its assigned IP/network. For example, if your ISP has assigned you one IP



address in one subnet and a CIDR block of addresses in another subnet, you can set the WAN interface IP to that single IP and add the CIDR block as a Proxy ARP entry below.

The screenshot displays the WAN configuration interface, divided into two main sections: 'Edit WAN' and 'Proxy ARP'.

**Edit WAN Section:**

- WAN Type\*:** A dropdown menu with 'DHCP' selected. Below it is the instruction: 'Select the WAN interface protocol'.
- MAC Address:** A text input field with the instruction: 'Override the MAC address of the WAN interface (for some cable connections)'.
- Hostname:** A text input field with the instruction: 'DHCP client identification when requesting a lease'.
- A 'Save' button is located below the input fields.

**Proxy ARP Section:**

- A header bar with a plus sign on the right.
- Text explaining Proxy ARP: 'Proxy ARP is commonly used to allow the WAN interface to respond to additional IP addresses or networks besides its assigned IP/network. For example, if your ISP has assigned you one IP address in one subnet, and a CIDR block of addresses in another subnet, you can set the WAN Interface IP to that single IP and add the CIDR block as a Proxy ARP entry below.'
- A dropdown menu set to '10' records per page and a search input field.
- A table with columns: 'Network (CIDR)', 'Description', 'Edit', and 'Delete'. The table is currently empty, showing 'No data available in table'.
- Footer text: 'Showing 0 to 0 of 0 entries' and navigation buttons '← Previous' and 'Next →'.

Figure 1-23: WAN Configuration

## vLAN

Within this section you can set up vLANs (Virtual Local Area Network) within your specified network. Here you will need to specify the name of the vLAN, parent interface (LAN/WAN), vLAN tags, virtual WAN settings, IP Address, and Subnet Mask (*Figure 1-24*).

Virtual WAN link this vLAN to the WAN interface and subnet. This allows WAN IPs on the LAN, while remaining behind the firewall. Appropriate firewall rules must also be created.

**Please Note:** All switches on the network will need to support vLANs.

vLANs are useful for fragmenting access to your network, which makes your network organized and clean and also makes hacking more difficult. If your Phone vLAN becomes compromised, the server and PC vLAN are not affected.

**New VLAN**

Name\* [?](#)

Parent Interface\* [?](#)

VLAN Tag\* [?](#)

Virtual WAN [?](#)

IP Address\* [?](#)

Subnet Mask\* [?](#)

Enabled [?](#)

Save

**Proxy ARP / CIDR Blocks**

Proxy ARP is commonly used to allow this interface to respond to additional IP addresses or networks besides what is assigned above.

Network (CIDR)	Description	Edit	Delete
----------------	-------------	------	--------

Figure 1-24: VLAN configuration

## Firewall

A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on applied security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, which is assumed to not be secure or trusted.

### Firewall Rules (Figure 1-25)

This section requires that you list the following requirements for a Firewall rule:

- Action (Block, Reject, Allow)
- Interface (WAN/LAN)
- Protocol
- Source (IP Address)
- Destination (Port)
- Description

**Firewall Rules**

Note: Lower-numbered priorities are "higher priority"; the first rule that matches the traffic will be applied.

10 records per page Search:

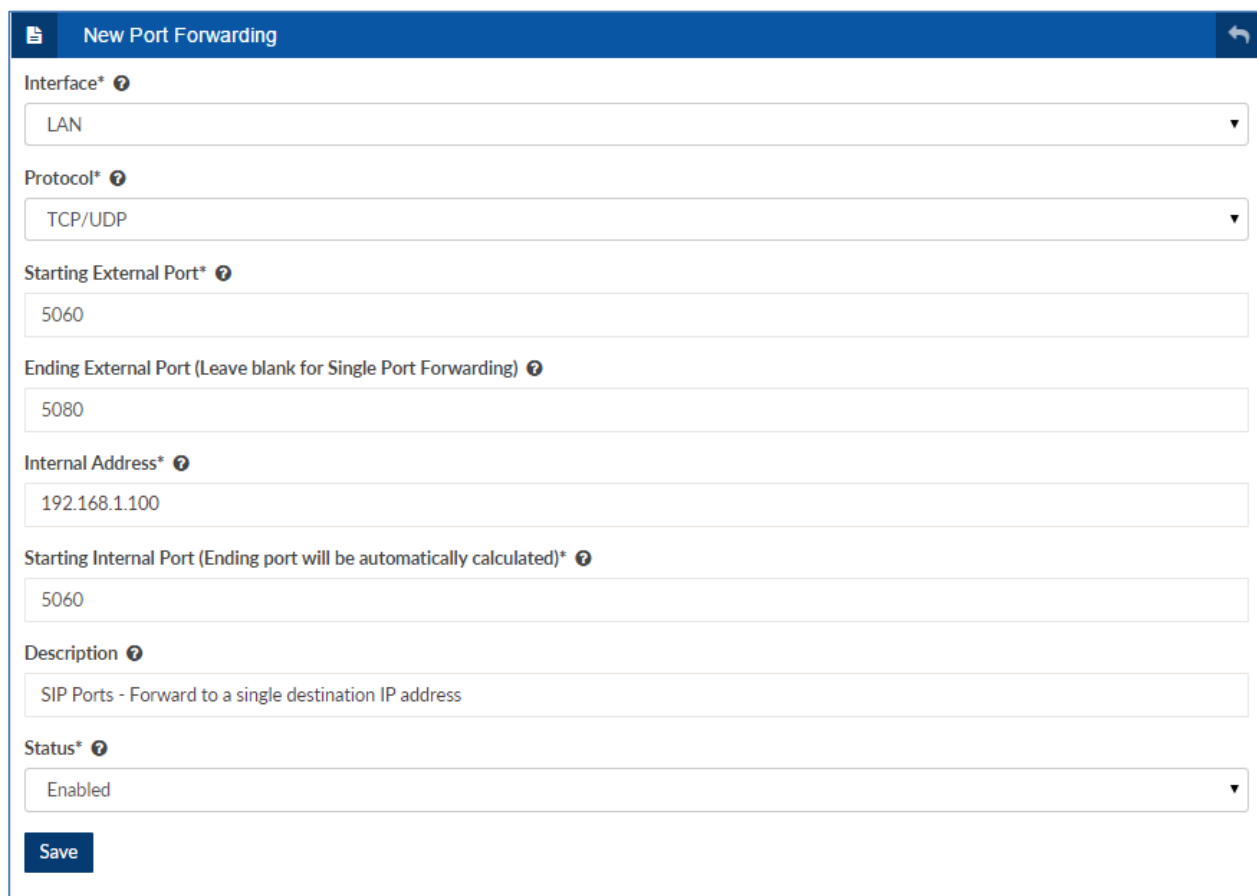
Priority	Action	Interface	Protocol	Source	Destination	Description	Status	
0	Block	WAN	TCP/UDP	*:*	*:23		Enabled	↑ ↓ ✎ 🗑️
1	Block	WAN	TCP/UDP	*:*	*:21105		Enabled	↑ ↓ ✎ 🗑️
2	Block	WAN	TCP/UDP	*:*	*:22		Enabled	↑ ↓ ✎ 🗑️

Figure 1-25: Firewall Access Rules

## Port Forwarding (Figure 1-26)

Port Forwarding is an application of NAT that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall. This feature is commonly used to make services on a host residing on an external network available to hosts on the internal network by remapping the destination IP address and port number of the communication to an internal host.

**Note:** It is highly recommended to use a static IP address or DHCP reservations on any listed, port-forwarded, IP addresses.



The screenshot shows a 'New Port Forwarding' configuration window with the following fields and values:

- Interface\*:** LAN
- Protocol\*:** TCP/UDP
- Starting External Port\*:** 5060
- Ending External Port (Leave blank for Single Port Forwarding):** 5080
- Internal Address\*:** 192.168.1.100
- Starting Internal Port (Ending port will be automatically calculated)\*:** 5060
- Description:** SIP Ports - Forward to a single destination IP address
- Status\*:** Enabled

A 'Save' button is located at the bottom left of the form.

Figure 1-26: New Port Forwarding Rule

### DMZ (Figure 1-27)

The purpose of a DMZ is to add an additional layer of security to an organization's LAN. An external network node only has direct access to equipment in the DMZ, rather than any other part of the network. The name is derived from the term 'demilitarized zone', an area between nations in which military operation is not permitted.

**Note:** When a DMZ Host is specified, the WAN interface will port-forward all traffic to the DMZ Host.

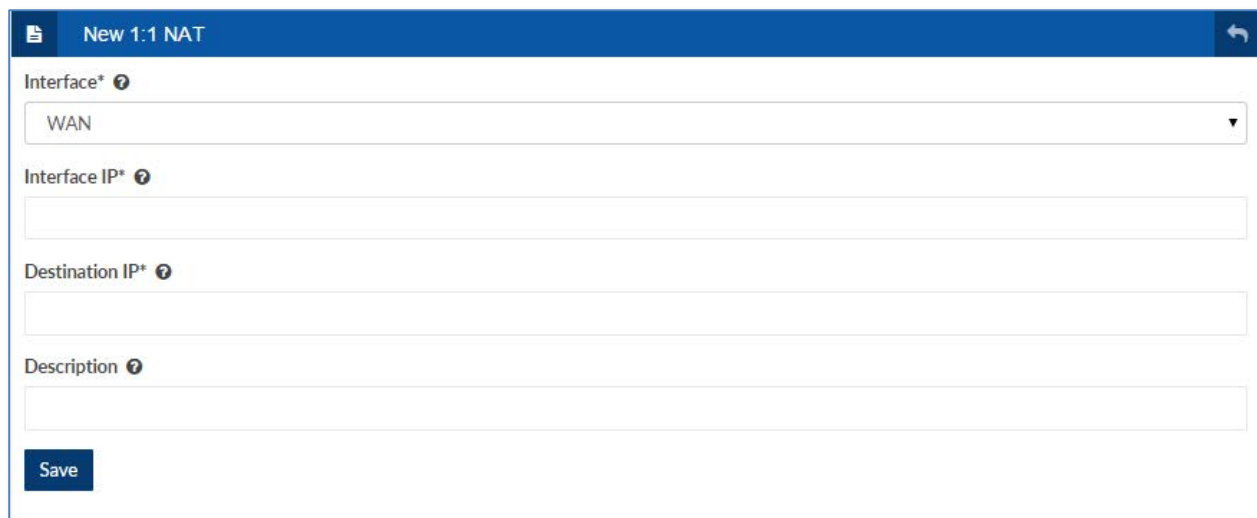


The screenshot shows a configuration window titled "DMZ". It features a label "DMZ Host (Leave blank for none)" with a help icon. Below this is a text input field containing the IP address "192.168.2.1". At the bottom left of the window is a "Save" button.

Figure 1-27: Setting a DMZ Host

### NAT (Figure 1-28)

Use this option to map an IP address on the WAN side of the Nextiva Clarity device to a local IP address on your network. Here you will need to determine whether you are mapping your traffic from WAN to LAN or LAN to WAN. Next, specify the "Interface IP" and "Destination IP". The Interface IP is the IP address on the router that will typically receive the traffic. This is commonly set up as a Proxy ARP address. The Destination IP is the IP address of the computer that the traffic will be forwarded to.



The screenshot shows a configuration window titled "New 1:1 NAT". It contains four fields: "Interface\*" with a dropdown menu showing "WAN"; "Interface IP\*"; "Destination IP\*"; and "Description\*". A "Save" button is located at the bottom left.

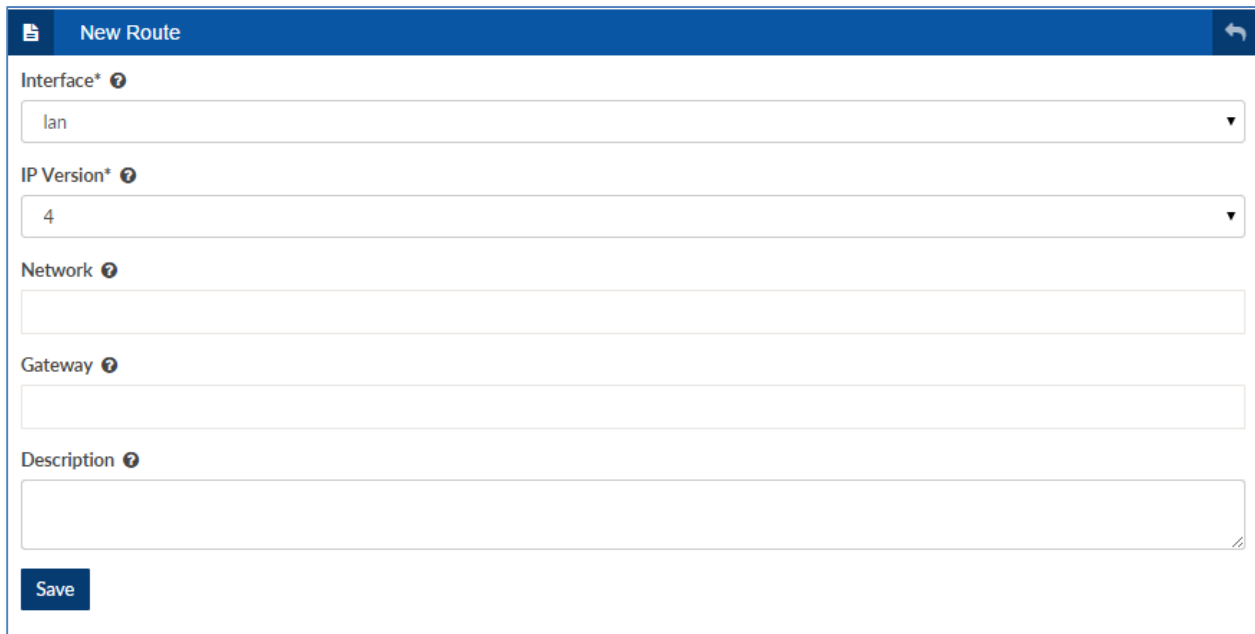
Figure 1-28: Setting a new 1:1 NAT

## Static Routes

Static routing is a form of routing that occurs when a router uses a manually configured routing entry rather than information from a dynamic routing path. In this case, static routes are manually configured by a network administrator by adding entries to a routing table. Unlike dynamic routing, static routes are fixed and do not change even if the network is changed or reconfigured. Static routing and dynamic routing are not mutually exclusive. Both dynamic routing and static routing are usually used on a router to maximize routing efficiency and to provide backups in the event that dynamic routing information fails to be exchanged.

In this section you will need to specify the following text fields (*Figure 1-29*):

- **Interface** - The interface that is able to contact the specified gateway
- **IP Version** - Specify IPv4 or IPv6
- **Network** - The network (in CIDR notation, like 1.2.3.0/24) that can be reached via the specified gateway
- **Gateway** - The gateway (must be contactable via this interface) that will know how to deliver traffic to the specified network



*Figure 1-29: Setting up Static Routes*

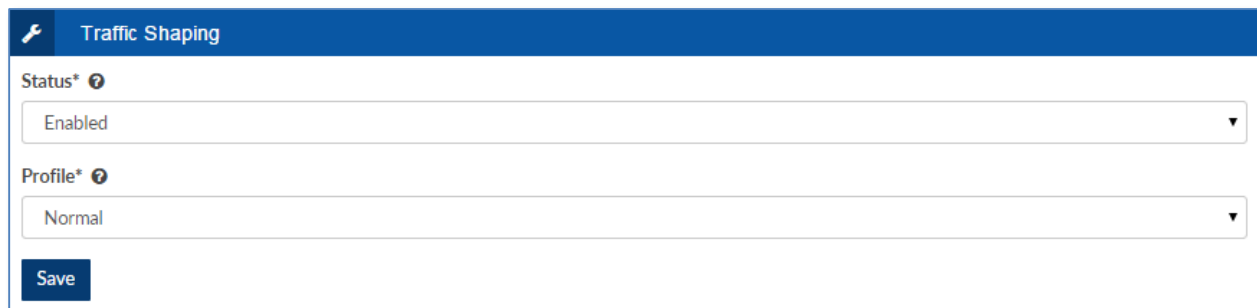
## Traffic Shaping

Also known as packet shaping, this feature is a technique used to manage network traffic which delays some or all datagrams to bring them into compliance with a desired traffic profile. Traffic shaping is used to optimize or guarantee performance, improve latency, and/or increase usable bandwidth for some kinds of packets by delaying other kinds. If a link becomes saturated to the point where there is a significant level of contention (either upstream or downstream) latency can rise substantially. Traffic shaping can be used to prevent this from occurring and keep latency in check. Traffic shaping provides a means to control the volume of traffic being sent into a network in a specified period, or the maximum rate at which the traffic is sent.

Within this section, you will need to specify the following settings (*Figure 1-30*):

**Status:** Disable to turn off traffic shaping, which may cause unexpected behavior on high-bandwidth clients. Recommended: leave on when not troubleshooting.

**Profile:** The level of aggressiveness for traffic shaping. Choose normal unless you are experiencing poor VoIP quality. Normal = interface is limited to 100% of the last speed test; Moderate = 80%; Aggressive = 60%.



The screenshot shows a configuration panel for Traffic Shaping. It features a blue header with a wrench icon and the text "Traffic Shaping". Below the header, there are two dropdown menus. The first is labeled "Status\*" and has a help icon; the selected value is "Enabled". The second is labeled "Profile\*" and has a help icon; the selected value is "Normal". At the bottom left of the form is a blue "Save" button.

*Figure 1-30: Traffic Shaping*

## VPN

A Virtual Private Network (VPN) extends a private network across a public network, such as the Internet. It enables a computer or network-enabled device to send and receive data across shared or public networks as if it was directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols or traffic encryption. Nextiva Clarity devices allow you to implement an IPsec VPN.

Within this section you will need to configure the following settings (*Figures 1-31, 1-32*):

- **Interface** - Select the interface that handles traffic for the Local Network.
- **NAT-t** – Enabling this will help the tunnel communicate from behind another router.
- **DPD Interval (seconds)** – Dead Peer Detection (DPD) determines how often to check that the other router is still online (and re-initiate the tunnel if it's offline).
- **Local Network** – The network or IP on this router, which will be able to use this tunnel. Specify an IP for Single Host, or a CIDR block for Network, like 1.2.3.0/24.
- **Remote Network** – The network on the other router, which will be accessible via this tunnel. Specify a CIDR block, like 192.168.1.0/24. Do not specify a subnet mask in IP notation, like 255.255.255.0/24. Look up CIDR Addressing if you need assistance.
- **Remote Gateway** – The remote router to connect to (usually the WAN IP).
- **Negotiation Mode** – Main is more secure, Aggressive starts the connection faster.
- **My Identifier** – Some other routers require identifiers such as the router's WAN IP, or a certificate. This should be unique to this router.
- **Phase 1 Encryption Algorithm** – This should match the remote router. 3DES or Blowfish is recommended, but not DES.
- **Phase 1 Hash Algorithm** – This should match the remote router. SHA1 is recommended.
- **DH Key Group** – How strong of an authentication key to use. This should match the Phase 1/ Authentication DH Group of the remote router.
- **Authentication Lifetime (seconds)** – This should match the Phase 1 / Authentication lifetime of the remote router, and be greater than the SA Lifetime.
- **Authentication Method** – This should match the authentication method of the remote router.
- **Pre-Shared Key** – A very long password that is used to secure the connection. Must match the remote router.
- **Certificate** – Paste this router's certificate in X509 PEM format here.
- **Private Key** – Paste this router's RSA private key in X509 PEM format here.
- **Peer Certificate** – Paste the remote router's certificate in X509 PEM format here. Leave blank to validate the remote router's identity with a Certificate Authority.
- **IPSec Protocol** – This should match the remote router. Using encryption is recommended.
- **Phase 2 Encryption Algorithms** – This should match the remote router. 3DES or Blowfish is recommended, but not DES.
- **Phase 2 Hash Algorithms** – This should match the remote router. SHA1 is recommended.



- **Perfect Forward Secrecy** – This should match the remote router. At least 2 (1024 bit) is recommended.
- **SA Lifetime (seconds)** – This should match the Phase 2 / IPsec SA lifetime of the remote router, and be lower than the Authentication Lifetime.

**New IPSEC Tunnel**

Enabled\* ⓘ

Interface\* ⓘ  
WAN

Nat-t ⓘ

DPD Interval (seconds) ⓘ  
(leave blank to disable)

Local Network\* ⓘ  
LAN Subnet  
(automatically detected)

Remote Network\* ⓘ  
Example: 4.5.6.0/24

Remote Gateway\* ⓘ  
Example: 1.2.3.4

Negotiation Mode\* ⓘ  
Main

My Identifier\* ⓘ  
My IP Address  
(automatically detected)

Phase 1 Encryption Algorithm\* ⓘ  
3DES

Phase 1 Hash Algorithm\* ⓘ  
SHA1

DH Key Group\* ⓘ  
2 (1024 bit)

Authentication Lifetime (seconds)\* ⓘ  
86400

Authentication Method\* ⓘ  
Pre-Shared Key

Pre-Shared Key\* ⓘ  
(64 characters recommended, max 255 characters) Show

Figure 1-31: VPN, IPsec configuration

Certificate ⓘ

Private Key ⓘ

Peer Certificate ⓘ

IPSec Protocol\* ⓘ

ESP (Encryption) ▼

Phase 2 Encryption Algorithms\* ⓘ  
(ctrl-click or command-click for multiple)

DES  
3DES  
Blowfish  
CAST128  
GCM (AES-128)

Phase 2 Hash Algorithms\* ⓘ  
(ctrl-click or command-click for multiple)

SHA1  
MD5

Perfect Forward Secrecy\* ⓘ

2 (1024 bit) ▼

SA Lifetime (seconds)\* ⓘ

3600

Description ⓘ

Save

Figure 1-32: VPN, IPSec configuration continued.