Calix 844G/854G GigaCenter User's Guide

August, 2015

#220-00771, Rev 11

Contents

About This Guide

This *Calix 844G/854G GigaCenter User Manual* defines the gateway's Embedded Web Interface (EWI) and provides instructions for managing a GigaCenter via the EWI. This guide explains how to set up and maintain Ethernet network settings, 800G GigaCenter devices, and any subtended subscriber devices attached to GigaCenter. In addition, information on the set-up and maintenance of the dual 2.4 GHz/5 GHz Wi-Fi radios is also provided.

Note: This guide is intended to educate users in setup and configuration of the 800G GigaCenter gateway for use in the home network. This guide does not address the provisioning of network access services on the GigaCenters themselves. For information on services provisioning, refer to the appropriate platform documentation.

Intended Audience

This guide is intended for use by consumers. Cursory knowledge of Internet Protocol (IP) and GPON based systems as well as a general understanding of IP addressing, routing principles, and internet security are also highly desired. This document assumes that the subscriber's laptop or PC is equipped with a supported web browser (Internet Explorer or Firefox) and that the user is familiar with its use. Familiarity with datacom, telecom, and standards-based Ethernet technologies and conventions is also recommended.

Note: For the purposes of this guide, it is assumed your service provider has already activated your GigaCenter on the GPON network and is being managed remotely.

Related Documentation

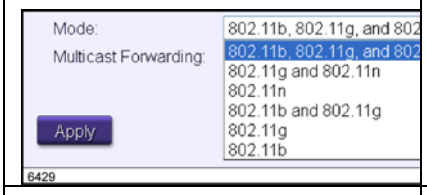
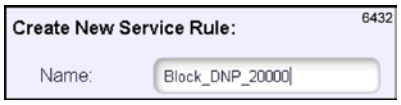
You can access all Calix product documentation from the Calix Resource Center online at *support.calix.com*.

The related Calix GigaCenter documentation includes:

- *Calix 844/854G GigaCenter Installation Guide*
- *Calix Residential Service Gateway Wi-Fi Best Practices Guide*

Site Conventions

The following elements and controls are used consistently throughout the 800G GigaCenter EWI:

Website Display Elements		
Example Icon	**Element Name**	**Description**
	Action Button	May include Edit, Add, Remove
	Radio Button	Typically offers a choice between two options
	Check Box	Typically used to enable or disable a feature
	Drop-down List	Provides a pre-existing list from which to choose
	Alpha-text Box	Alpha-numeric input box typically used for naming a function, port, service, or device. Note: Values exceeding field length maximums are truncated at the max field length.
	Numeric-text Box	Numeric input box typically used for naming a function, port, service, or device Note: Invalid entries return a "value out of range" error message.

System Defaults

Fields that carry a pre-defined default values are marked with an "‡" symbol in the last column of each table.

Username and Passwords

Within the GUI, there are several screens that require the entry of a user name and password. The following table details the allowable syntax for each username/password combination.

Username and Password Handling						
	Username Field			Password Field		
Page Location	Min. Char.	Max. Char.	Validity	Min. Char.	Max. Char.	Validity
Advanced > IP Addressing > Dynamic DNS	1	64	Allowed: A-Z, a-z, 0-9	1	32	Not allowed: ^<>()"%&'+;
Advanced > IP Addressing > WAN Settings	0	256	Not allowed: ~`!#$%^&*()-_+={}[]|\:;"?/	0	32	No restrictions
Advanced > Remote Management > Remote GUI	1	15	Allowed: A-Z, a-z, 0-9, !*()-_.	1	15	Allowed: A-Z, a-z, 0-9, !*()-_.
Advanced > Remote Management > Remote Telnet	1	15	Allowed: A-Z, a-z, 0-9, !*()-_.	1	15	Allowed: A-Z, a-z, 0-9, !*()-_.
Advanced > Security > Administrator Credentials	1	64	Allowed: A-Z, a-z, 0-9, !*()-_.	0	32	Allowed: A-Z, a-z, 0-9, !*()-_.
Quick Start > Connect to Internet	0	256	Not allowed: ~`!#$%^&*()-_+={}[]|\:;"?/	0	32	No restrictions
Support > TR-069	1	any	Not allowed: spaces	1	32	Not allowed: spaces

Chapter 1

844G/854G GigaCenter Overview

The Calix 844G and 854G GigaCenter are in a family of Premises delivery platforms optimized to extend the network demarcation to inside the subscribers home. They are the first Calix products to support carrier class Wi-Fi using 802.11ac technology allowing all services to be delivered over wireless. Carrier class Wi-Fi as defined incorporates 4x4 Multiple-Input-Multiple-Output (MIMO) at 5GHz, support of the entire 5GHz band including Dynamic Frequency Selection (DFS) channels, implicit and explicit beamforming, use of 80MHz combined channels at 5GHz, as well as software management tools and quality of service capabilities.

Calix GigaCenters are currently available in the following models:

- 844G-1 GigaCenter, 2 POTS, 4 Gig-Ethernet, Dual Wi-Fi, 1 USB, UPS Power Interface
- 844G-2 GigaCenter, 2 POTS, 4 GE, Dual Wi-Fi, 1 USB, Power Adapter Interface
- 854G-1 GigaCenter, 2 POTS, 4 Gig-Ethernet, Dual Wi-Fi, 1 USB, 1 RF, UPS Power Interface
- 854G-2 GigaCenter, 2 POTS, 4 Gig-Ethernet, Dual Wi-Fi, 1 USB, 1 RF, Power Adapter Interface

The 844G and 854G GigaCenters also includes a Home Gateway functionality first introduced in Calix' 836GE Residential Service Gateway (RSG). The 836GE supports the 802.11n standard at either 2.4GHz or 5GHz. GigaCenters support concurrent dual-band networking, allowing continued usage of the 2.4GHz band for data and legacy consumer devices while supporting IPTV and high-speed data at 5GHz. The GigaCenters are designed to meet service providers' and end-users' requirements for broadband access throughout the residence driven by the growth of smart mobile devices and media rich content. These Wi-Fi devices range from low bandwidth IP cameras, security sensors, smart phones, tablets, printers, and support for bandwidth intensive Quality Of Service (QoS) sensitive Wi-Fi capable Set Top Boxes (STBs) and TVs. To meet these user requirements, some of GigaCenter highlights include:

- Supports the latest 802.11ac standard for the 5GHz radio. Some basic 802.11ac enhancements include:
  - Dynamic beamforming for high performance and longer reaches.
  - 80Mhz channels for greater speeds,
  - QoS support allowing prioritization of Video SSID over lower priority best effort HSI data SSIDs.
- Dual band concurrent radios allows the use of legacy 2.4 GHz clients while accessing seven times the spectrum of 2.4 GHz using the 5 GHz band.
- GigaCenters support the E7-2 and E7-20 Ethernet Service Access Platforms (ESAP) GPON. The 844G and 854G are GPON only devices.
- In conjunction with the Calix Compass software, a rich set of tools is supported for provisioning, maintaining, and troubleshooting the Wi-Fi home network. Compass's ability to store vast amounts of performance management data allows service providers the ability to troubleshoot issues that are time of day based along with the ability to generate trend analysis to predict congestion issues
- GigaCenters are designed to help service providers generate new revenue streams such as smart home applications through the continued release of software features. To support these features GigaCenters supports a high performance CPU and larger memory than other products on the market

About the Home Gateway

The 844G and 854G utilize a common residential gateway service model as the 836GE RSG and 700GE support of Home Gateway. The embedded web interface (EWI) and relevant gateway features such as NAT, DHCP, DNS and firewall handle network traffic at speeds up to 1 Gbps.

Home Gateway Functionality

- Layer 2 and 3 switching and routing
- DHCP server options
- DHCP (IPoE) and PPPoE network connections
- Network Access Translation (NAT), public to private IP addressing
- Configurable IP address schemes, subnets, static-IP addresses
- DNS server
- Bridge port assignment and data traffic mappings
- Port forwarding
- Firewall and security
- Application and website filtering
- Selectable forwarding and blocking policies
- DMZ hosting
- Parental controls, time of day usage
- Denial of service
- MAC filtering
- Time/Zone support
- Universal Plug-and-Play (UPnP)

Wireless Functionality

- 2.4GHz and 5GHz, simultaneous dual-band
- 5GHz 802.11ac certified, 802.11a/g/n compatible
- 2.4GHz 802.11n certified, 802.11b/g compatible
- WPA/WPA2
- WPS push-button
- WEP 64/128 bit encryption
- Airtime Fairness on 2.4 GHz and 5 GHz radios
- Eight SSID per band with factory default SSIDs
- Two SSID assigned to Primary/Guest and six operator defined SSIDs

- 5 GHz radio support of 64 clients (assigned to Primary/Guest with maximum 102 clients per radio
- 64 Clients supported per band with 38 reserved for operator defined SSIDs
- MAC filtering

Four Gigabit Ethernet (GE) interfaces

- Symmetrical 1 Gbps bandwidth for IPTV and data services
- Multi-rate 10/100/1000 BaseT Ethernet, auto-negotiating

USB port

- USB 2.0 - Type A configured as a host controller device

System Features

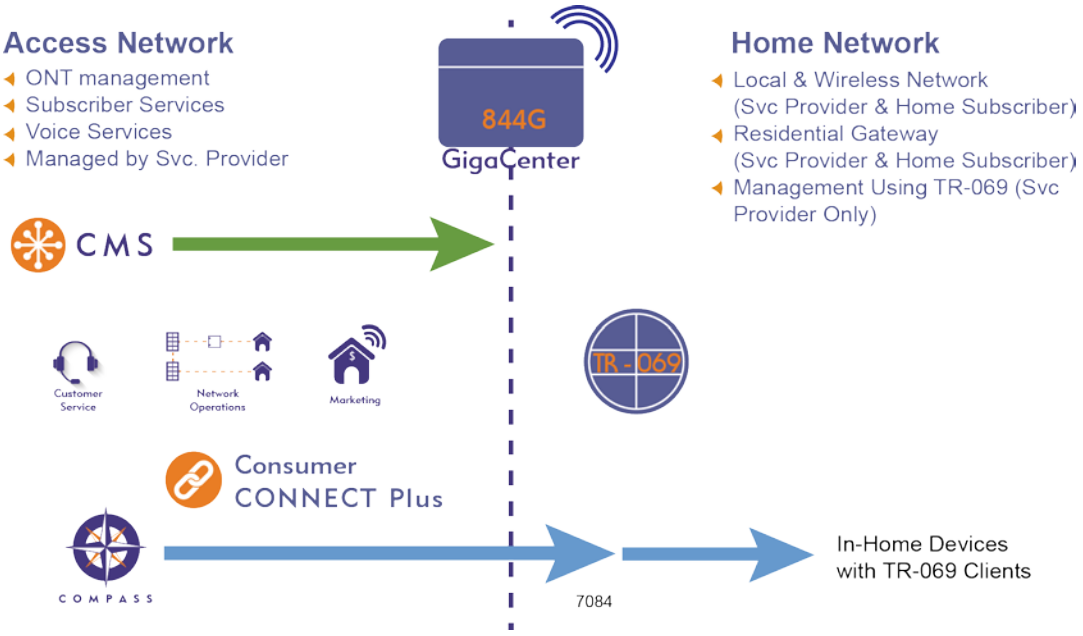
- Supports multiple data service profiles
- Traffic management and Quality of Service (QoS):
  - 802.1Q VLANs
  - 802.1p service prioritization
  - Q-in-Q tagging
  - Multiple VLANs
  - Rate limiting
  - DiffServ
  - Pre-defined QoS on service type
- IPTV, IGMPv2, IGMPv3
- IGMP Snooping and Proxy
- IGMP Fast Leaves
- OAM&P support via Calix Management System (CMS)
- Gateway Management:
  - TR-069
  - TR-98
  - TR-104
  - Local Home Gateway GUI, access provisionable
  - Remote WAN side GUI access
  - Default username/password
  - Set-up persistence, factory reboot option

GigaCenter Management Architecture

GigaCenters combine GPON access technology with gateway functionality and divides these tasks into two separate partitions:

- The GPON partition that provides the WAN access as well as voice services and GigaCenter management.
- The Home Gateway partition that offers LAN and wireless network support as well as Home Gateway services such as LAN routing, and TR-069 client management.

An overview of the system architecture is shown below for reference.



Home Gateway IPv6 Support

With E-Series platform Release 2.4, the Calix GigaCenter Home Gateway has been enhanced to include direct support of IPv6 connectivity. IPv6 is the next Internet Protocol version to meet the expanding requirements for IP addressing. It is currently being used to supplement IPv4 but is expected to eventually replace IPv4.

IPv4 addresses are 32 bits, written in dot-decimal notation. IPv6 addresses are 128 bits long, written in colons-hexadecimal notation with eight groups of four digits. Direct connectivity of IPv6 negates the need for Network Address Translation (NAT) with each device having a unique IP address, and includes special addressing features and a significantly larger subnet space.

To help in the transition and implementation of IPv6 from IPv4 there are a number of different strategies to help operators depending on the network infrastructure and environment:

- Single or Dual-stack IPv4/IPv6
- DS-Lite
- 6rd

All GigaCenters supporting Home Gateway Layer 3 services support Single or Dual-stack IPv4/IPv6. GigaCenters also support DS-Lite for IPv6 carriage (tunneling of IPv4) or 6rd for IPv4 carriage (tunneling of IPv6).

The Home Gateway support of IPv6 only supports IPv6 for High Speed Internet (HSI) data services. The release does not support IPv6 for IPTV multicast video, voice services and TR-069 management.

Note: Only one variant of IPv6 support can be applied to a gateway, and only one service WAN interface can support the IPv6 variant which will be constrained to HSI only.

Note: The IPv6 interface can support IPoE Dynamicv6, IPoE Staticv6 and PPPoEv6.

To implement IPv6 support on a GigaCenter requires moving to the External configuration mode with RG configuration file download, either via OMCI download or Consumer CONNECT Plus.

Note: Support and provisioning of IPv6 is not supported using Native mode.

IPv6 Notation Syntax

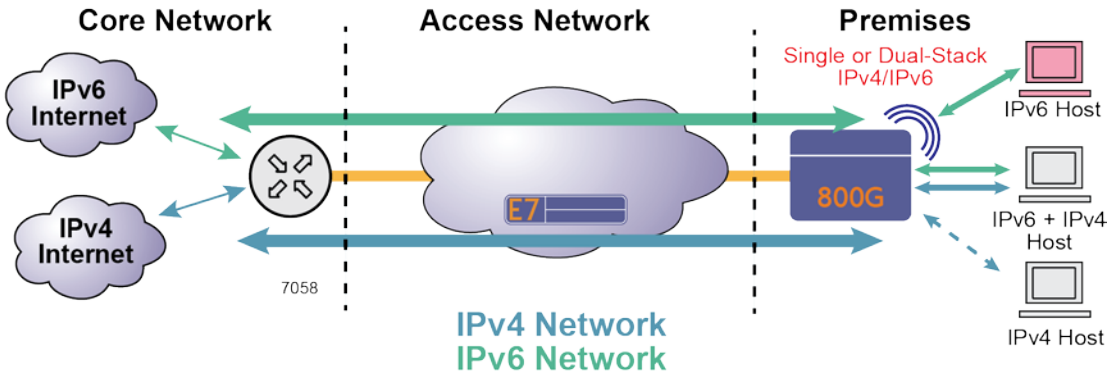
Keep the following information in mind when deciphering IPv6 IP addresses:

- Leading zeros in any 16-bit field are suppressed. For example, 2001:0db8::0001 is rendered as 2001:db8::1, though any all-zero field that is explicitly presented is rendered as 0.
- "::" is not used to shorten just a single 0 field. For example, 2001:db8:0:0:0:0:2:1 is shortened to 2001:db8::2:1, but 2001:db8:0000:1:1:1:1:1 is rendered as 2001:db8:0:1:1:1:1:1.
- Representations are shortened as much as possible. The longest sequence of consecutive all-zero fields is replaced by double-colon. If there are multiple longest runs of all-zero fields, then it is the leftmost that is compressed. E.g., 2001:db8:0:0:1:0:0:1 is rendered as 2001:db8::1:0:0:1 rather than as 2001:db8:0:0:1::1.
- Hexadecimal digits are expressed as lower-case letters. For example, 2001:db8::1 is preferred over 2001:DB8::1.

Dual Stack IPv4/IPv6

Single stack IPv6 assumes a WAN interface will only connect using an IPv6 address. Dual Stack IPv4/IPv6 implements both connection types on an interface at the same time, subscriber devices can connect to either the IPv4 or IPv6 address protocol. The process is driven by DNS where a dual stack device will query the name of the destination, and if the response is a IPv6 address the device will send IPv6 packets. It allows the gateway to support simultaneous support of IPv4 and IPv6 content.

The dual stack IPv4/IPv6 implementation is shown in the below figure:



Dual stack IPv4/IPv6 is the most desirable variant of IPv6 support since it facilitates direct connections of both IPv4 and IPv6 devices and avoids complexities of tunneling, security, and timing delays that are introduced when translating between protocols required when using Carrier Grade NAT.

When supporting IPv6, the Home Gateway EWI has separate display of IPv6 statistics and packet performance. It does include support of firewall for IPv6 in same way it supports firewall for IPv4 with a general option of off/low/medium/high and ability to change traffic in/traffic out settings for protocols and ports. The firewall settings for IPv6 are managed separately from IPv4.

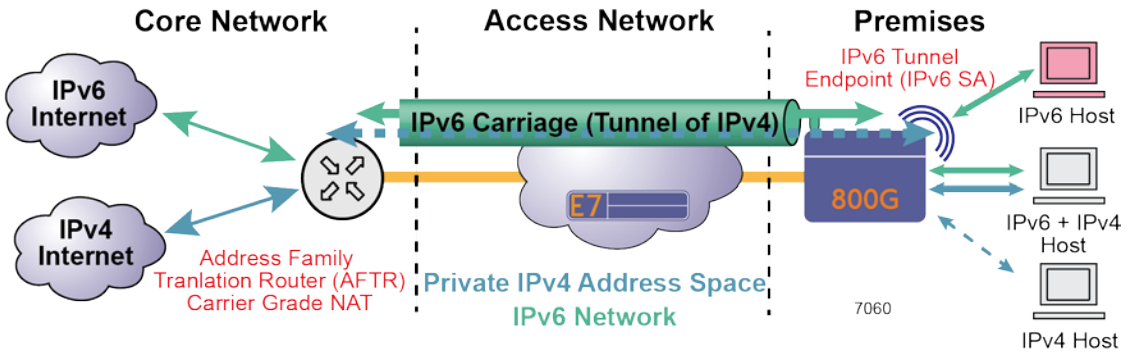
For additional information on configuring IPv6 services, refer to *IPv6 Parameters and Options* later on in this guide.

DS-Lite

With the depletion of IPv4 public addresses some operators have had to discontinue support of IPv4 in their networks and solely deploy IPv6 network infrastructure. Because not all subscriber devices support IPv6 it requires tunneling and translation of IPv4 addresses to the gateway.

The GigaCenter supporting Home Gateway continues to distribute private IPv4 addresses on the LAN and wireless interfaces. DS-Lite encapsulates IPv4 packet inside a IPv6 packet with network termination to an Address Family Translation Router (AFTR) supporting Carrier Grade NAT with global IPv6 connection. At the AFTR the IPv6 packet is decapsulated, restored to IPv4, and routed to the public IPv4 Internet.

The DS-Lite implementation is shown in the below figure:



To facilitate the tunneling of IPv4 packets the AFTR uniquely marks each traffic flow using the Gateway IPv6 address, the private IPv4 address and port number. The gateway obtains the URL of the AFTR via DHCPv6 (RFC 6334) or it can be provisioned manually with the AFTR URL via EWI, TR-069 or RG configuration file.

On its WAN side, Network Area and Port Translation (NAPT) is disabled and the IPv4 tunnel becomes the default IPv4 route. Via DHCPv4, the gateway can either advertise itself as the DNSv4 server or advertise DNSv4 servers provisioned via EWI or TR-069 or RG configuration file. In the former case the gateway proxies "A" record queries from IPv4 to a WAN-side DHCPv6 server.

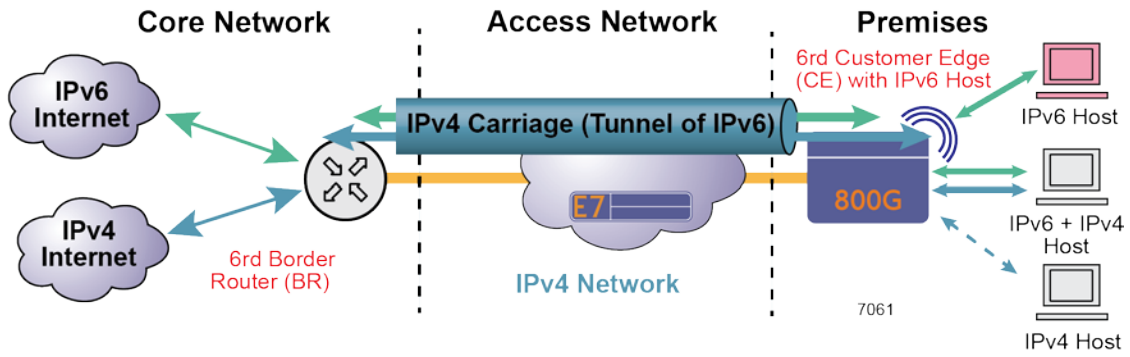
The GigaCenter supporting Home Gateway only supports a single instance of DS-Lite on a routed WAN interface. The WAN interface is assumed to be supporting HSI services. Support of DS-Lite for HSI is independent of IPTV services and is not supported for TR-069 management.

6rd

For service providers with networks that do not have IPv6 infrastructure the GigaCenter supporting Home Gateway will support dual stack 6rd. The variant of 6rd allows IPv6 service to be deployed over a pure IPv4 access network. The core network is not aware of IPv6, it does not require IPv6 infrastructure such as core routers, DHCP or DNS servers

The 6rd mechanism encapsulates IPv6 inside IPv4 between the Border Router (BR) and Customer Edge (CE). It follows all of the same IPv4 routing functions. On the GigaCenter supporting Home Gateway the LAN interfaces appear as Dual-Stack IPv4/IPv6 to the LAN interfaces and subscriber.

The dual stack 6rd implementation is shown in the below figure:



At the subscriber location the gateway operates in a 'hub-and-spoke' mode with IPv6 tunneled traffic flows between the BR and gateway. The gateway can be provisioned to support 6rd by obtaining network data via DHCPv4 Option 212 or via EWI, TR69 or RG configuration file. The specific 6rd provisioning data consists of:

- IPv4 Mask Length
- 6rd Prefix
- 6rd Prefix Length
- BR IPv4 address

Provisioning of 6rd includes configuring the necessary parameters via EWI, TR-069 and DHCPv4, creation of the prefix, using the created prefix as a "delegated prefix" for purpose of including one of its /64s in RA messages, and modifying the IP header for traffic that goes between the WAN and LAN devices. Once configured for dual stack 6rd, the gateway advertises DNSv6 servers provisioned via EWI, TR-069 or RG configuration file.

As noted previously, the GigaCenter and supporting Home Gateway only support a single instance of 6rd on a routed WAN interface. The WAN interface is assumed to be supporting HSI services. Dual stack 6rd is not supported for IPTV multicast over routed interface and TR-069.

For additional information on configuring 6rd services, refer to *6rd Parameters and Options* later on in this guide.

About GigaCenter Voice Services

From a home subscriber's perspective, the configuration of voice services delivered from the GigaCenter must be performed by your local service provider. Many customizable features are available and your service provider will configure your phone system based on the network environment and subscriber wishes.

Chapter 2

Wireless Networking

About the 5 GHz Wi-Fi Radio

The new 5 GHz radio incorporated into GigaCenter products includes the following features and attributes:

- For the 844G-1 and 854G-1 models, both 2.4 GHz and 5 GHz Wi-Fi radios operate at the maximum conductive emissions allowed by the FCC. GigaCenters have significantly higher power than the 836GE RSG at 2.4 GHz and with 5 GHz, the radio is both higher power and has beamforming gain from the 4x4 antennas.
- The 5 GHz radio was designed for critical IPTV services and supports channel hoping during operation, thereby avoiding service disruption due to interference.
- The 5 GHz radio is FCC certified to use the Dynamic Frequency Selection (DFS) channels which comprise 60% of the 5 GHz channel spectrum. These are largely unused frequencies as commercial routers sold over retail counters generally are not certified to operate with these channels.

Note: Not all Wi-Fi capable clients and devices support the DFS channels. Service providers must enable DFS support to ensure DFS interoperability issues do not occur.

- The 5 GHz radio has a Wi-Fi QoS feature that can be assigned to multiple SSIDs. In this release, IPTV services are assigned to a pre-defined video SSID called "5 GHz_IPTV_SSID" with usage and QOS set. This allows this pre-defined IPTV SSID to be prioritized over best effort data services assigned to other 5 GHz SSIDs.
- The 5 GHz radio supports up to 8 STB clients using 4x4 Quantenna radios. In other words the use case is defined as supporting 8 simultaneous HD video channels to 8 STBs located throughout a home with additional bandwidth reserved for HSI data applications using the 5 GHz band. This level of capability qualifies the 5 GHz radio as a Carrier Class Wi-Fi network.

Wireless Network Performance

Residential wireless networks have become quite common for several reasons:

- They are easy to install
- Wi-Fi networks support mobile devices
- Wireless appliances are now plug-and-play
- Elimination of CAT5 cabling throughout the home

Wireless network performance and reliability are characteristically different than a direct LAN connection to a GigaCenter. A number of factors and variables can affect Wi-Fi coverage and data throughput. The expected performance of a wireless LAN network requires insight into the variables that impact performance.

The operative data rate for Wireless LANs is based on the IEEE 802.11 standards. Proponents of the 5 GHz spectrum claim data rates up to 1733 Mbps when associated with an 802.11ac access point using 80 MHz channels and 4x4 MIMO (supported by GigaCenters). These reflect the standard physical layer rate (PHY rate) of a link. Proponents of the 2.4 GHz spectrum using 2x2 MIMO claim rates up to 300Mbps using 40 MHz channels. These claims do not reflect the actual data throughput expected when communicating over a wireless interface. Some of the main differences between PHY rate and actual payload data throughput are:

1. Higher overhead and packet headers required for wireless connections
2. Data re-transmission necessary because of temporary changes in a wireless links
3. Varying number of clients being supported over a common radio channel

Whereas overhead and re-transmission are inherent features that reduce the data throughput of all wireless networks, there are wireless propagation factors that significantly affect Wi-Fi coverage and throughput. These range from the design and placement of the Access Point (AP) and its antennas, orientation of the antennas, and constant changes in the level of radio signal interference. Variables that affect wireless network performance generally fall into the following categories:

- Design and performance characteristics of the wireless Access Point
  - Operating mode of 802.11 design standard: a/b/g/n/ac
  - Support of spatial multiplexing
    - Single Input, Single Output (SISO) vs Multiple Input, Multiple Output (MIMO)
  - 2.4 GHz vs. 5 GHz frequency band selection
  - 20 MHz, 40 MHz and 80 MHz bandwidth selection
  - Transmit power
  - Receive sensitivity

    - Antenna pattern, gain, polarization and orthogonally
- Number and types of wireless clients being supported
    - Support of a high number of wireless clients
        - Multiple wireless devices in the home including tablets, computers, smart phones, video media players, audio players, gaming consoles and appliances
    - Requirements to mix clients supporting new and legacy wireless technologies
        - 802.11g clients on a 802.11n network can severely affect total network performance for all devices
    - Software versions and backward compatibility
- Installed environment
    - Over the air distance, building materials, physical obstructions
    - Placement of the AP relative to the client
    - Orientation of the client if device only supports single polarity
- Level of radio frequency interference

The following chart provides a snapshot of the Wi-Fi 802.11 protocols and some of their characteristics including PHY data rates per link:

802.11 Protocol	Released	Frequency Band	Bandwidth (MHz)	Link Data Rates per Stream (Mbps)	MIMO Streams
a	9/1999	5 GHz	20	6, 9, 12, 18, 24, 36, 48, 54	1
b	9/1999	2.4 GHz	20	1, 2, 5.5, 11	1
g	6/2003	2.4 GHz	20	6, 9, 12, 18, 24, 36, 48, 54	1
n	10/2009	2.4 GHz	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	2
		5 GHz	20/40	15, 30, 45, 60, 90, 120, 135, 150	2
ac	12/2013	5 GHz	20/40/80	32, 65, 98, 130, 195, 260, 293, 325, 390, 433	4

The standard transmission rates vary for each of the Wi-Fi protocols. Within each protocol there are a number of "standard" transmission rates beginning with a rate that is approximately 1/10th of the maximum link bit rate per stream. The support of MIMO technology represents Multiple Input, Multiple Output. The column titled "Allowable MIMO Streams" indicates if multiple data streams can be used to provide MIMO spatial multiplexing. With 2x2 MIMO on a 5 GHz 802.11n system that would equate to a speed of 300MHz (2*150).

As noted there are a number of factors that influence the expected GigaCenter coverage and throughput data rate as wireless signals propagate over an open air interface. Moving a connected Wi-Fi client away from the AP causes a progressive degradation of the data stream until it can no longer receive or transfer data due to low or poor signal quality.

With ONT Release 11.1, the concept of Air-Time Fairness was introduced for both the 2.4 GHz and 5 GHz radios. With this technology, devices capable of transmitting at peak wireless modes or data rates are never limited by other older wireless devices connected to the same radio. In other words, air-time is allocated evenly to all clients on the network, regardless of the wireless technology being used.

About Multiple Input, Multiple Output (MIMO)

Systems with multiple antennas at the transmitter and receiver are referred to as MIMO systems. Some of the technologies employed with MIMO are beam forming which focuses the Wi-Fi power to each client which improves signal strength. Spatial Multiplexing allows the transmitter to send independent streams. A 2 x 2 system can double the effective bandwidth, a 3 x 3 system offers triple the performance and the 4 x 4 design of GigaCenter allows for a 4x increase. GigaCenter supports a 2 x 2 antenna design for the 2.4 GHz radio and a 4 x 4 design for its 5 GHz radio.

Note: Support for the new Wave 2 802.11ac standard is not supported in this release. Calix plans to support this standard in a future release and will allow the GigaCenter to send separate and simultaneous streams to multiple mobile clients at a time.

About the 2.4 GHz and 5 GHz Spectrums

GigaCenters support dual simultaneous 2.4 GHz and 5 GHz transmission frequency radios. The characteristics of each determine which is best to use for a specific wireless deployment. The lower frequency 2.4GHz band has better wireless propagation characteristics and is generally used to cover a larger area. One downside of the 2.4 GHz band is that it is more susceptible to radio interference from other 2.4 GHz access points (neighbor or municipality based wireless networks) as well as household appliances such as microwave ovens. The 5 GHz band is less susceptible to interference but many early 802.11 clients such as printers and consumer appliances currently only support the 2.4 GHz frequency band.

The 2.4 GHz spectrum supports 11 overlapping 20 MHz channels with center frequencies separated by 5 MHz. In reality, this creates only 3 non-overlapping 20 MHz channels. Conversely, the 5 GHz spectrum supports 23 non-overlapping 20 MHz channels that, when combined, support (11) 40 MHz and (5) 80 MHz non overlapping channels. One of the main benefits of 802.11ac (which only supports the 5 GHz spectrum) is to get subscribers off the slower and crowded 2.4 GHz spectrum and onto the quicker, less utilized 5 GHz spectrum.

In addition, some of the 5 GHz radio channels have special requirements placed on their usage. These channels can be used by radar systems and there are FCC standards for the Wi-Fi equipment to sense if radar is present and if so, to hop to a different channel. This ability to sense radar and jump to a different channel is called Dynamic Frequency Selection (DFS) and requires equipment vendors to certify their equipment as being DFS compliant. Some vendors have chosen to not support DFS which reduces the amount of capacity in 5 GHz systems.

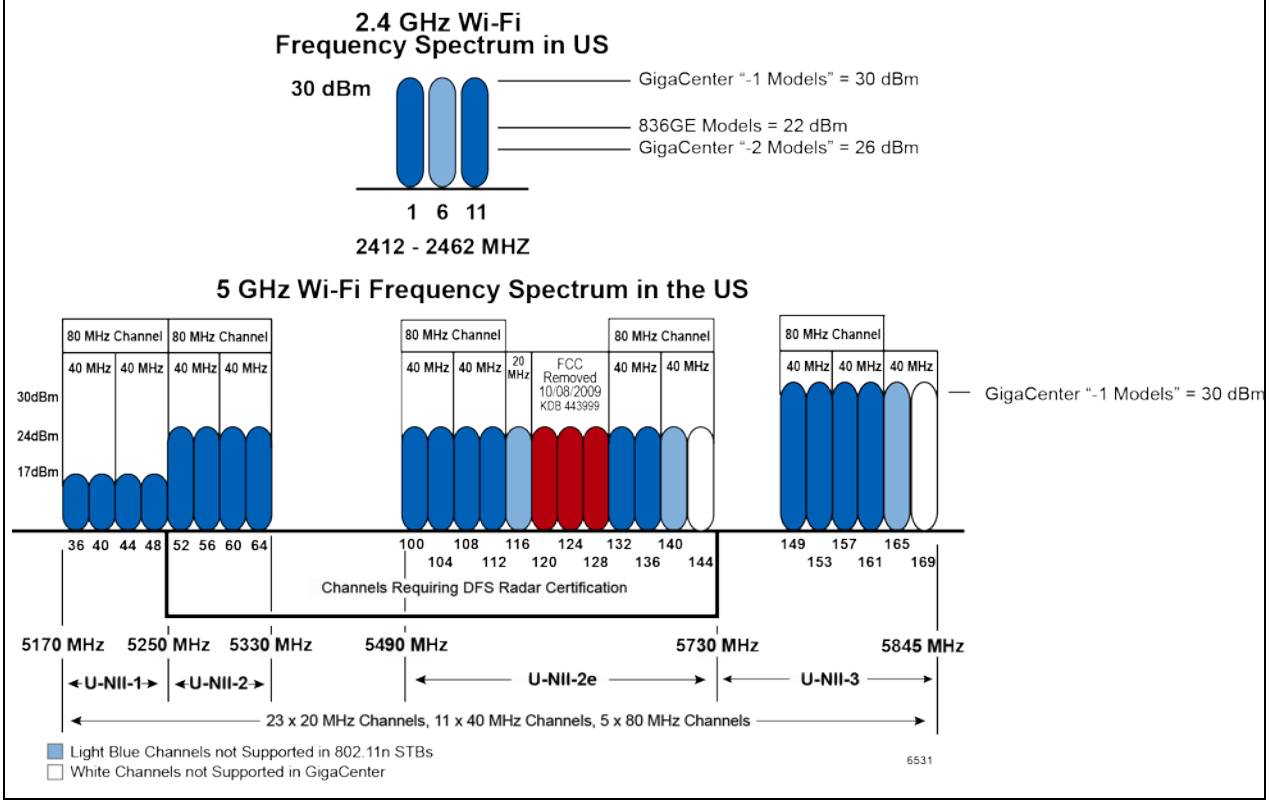
Note: GigaCenters are fully compliant with DFS certification.

The DFS channels comprise 60% of the 5 GHz channels. These may be considered the "beach front property" for in home Wi-Fi networks. Many commercial routers sold by retailers are not certified so this frequency band is mostly empty. If there is no radar in the vicinity of the home, the DFS channels will generally have minimal traffic. This allows operators who deploy GigaCenter products to leverage DFS channels to ensure high performance Wi-Fi for their end users and/or for the delivery of IPTV Video to their Wi-Fi capable set top boxes.

Not all current generations of Video Access Point (VAP) or Wi-Fi enabled Set top boxes support DFS. Also, not all data clients support DFS and therefore they cannot take advantage of the GigaCenters DFS capabilities. To support the needs of the service provider, GigaCenters allows the service provider to enable or disable the usage of the DFS specific channels. Below is a picture of how the 2.4 GHz and 5 GHz radio spectrum is broken down.

2.4 GHz and 5 GHz Wi-Fi Radio Spectrum

- 2.4 GHz includes 3 channels = 5 GHz includes 20 channels
- 2.4 GHz has somewhat better wall penetration
- 5 GHz has many channels to hop to, upon interference
- Over 1/2 the channels are DFS (Dynamic Frequency Selection)
  - Devices must be FCC certified to be able to hop away from a channel if radar is detected
  - Currently there is very little usage of DFS



Operational Notes

To increase data throughput, the 802.11n standard allows for bonding wireless channels to increase usable spectrum. With the 2.4 GHz model, band bonding channels to 40 MHz bandwidths is not practical because of channel overlap and interference. The 5 GHz band allows you to configure 20 MHz or 40 MHz of channel bandwidth enabling support of greater throughput by utilizing a larger portion of spectrum.

About Air Time Fairness

With the proliferation of newer and faster Wi-Fi clients, networks with older, outdated Wi-Fi devices may experience an over-all degradation in speed. In every day terms, a network may provide more time for these older clients to connect and pass their traffic. Air Time Fairness levels the playing field by allocating equal time to each device on the network, regardless of their data transfer speeds. This fairness quotient may encourage subscribers to update older Wi-Fi clients since they will tend to receive insufficient air time when compared to newer, faster models.

Note: Air Time Fairness is enabled on both the 2.4 GHz and the 5 GHz radio by default.

Carrier Class Wi-Fi Quality of Service (Qos)

To remain competitive, service providers have expanded their service offerings and offer complete triple play services (Voice, Data, and Video) packages. To ensure a high quality user experience for their video offering, a hardware connection was required to each set top and/or DVR. To make the installation easier and to give end users even more flexibility to the placement of additional video screens, GigaCenters support delivery of IPTV with the 5 GHz radio.

GigaCenters are designed to support both IPTV and HSI applications over 802.11ac at 5 GHz, as well as HSI over 2.4 GHz with the pre-ac standards. GigaCenter supports QoS prioritization by SSID provisioning. The initial release dedicates an SSID in the 5 GHz band specific for video IPTV applications with higher quality of service. This ensures that the service providers IPTV content will always be prioritized higher than the consumers HSI Data or the Guest SSID.

Getting Additional Information

To more thoroughly understand the capabilities of Wi-Fi in your particular environment, refer to the *Calix Application Note: Calix Residential Gateway Wi-Fi Best Practices Guide.*

Chapter 3

Turning up a GigaCenter

GigaCenter Activation and Configuration Options

The GigaCenter can be activated and managed using a variety of web-based or network-based tools.

Note: It is assumed your service provider has already activated your GigaCenter on the GPON network and is able to manage all functions of the device remotely.

GIGACENTER TOOLS			
Home Gateway Configuration and Management			
Software Tool	**Functionality**	**How Access**	**Intended User**
Subscriber EWI • Local Access • Administrator account	Manage Home Gateway	Web Browser via IP 192.168.0.2	Subscriber

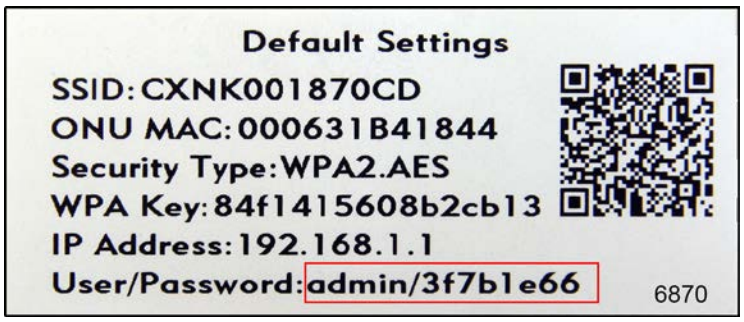
For most GigaCenter deployments that involve data-only use cases, or access modes that require a single VLAN service, the default RG profile that is created when the GigaCenter becomes operational is adequate.

For more advanced access models that require multiple VLANs associated with the routed WAN interface, set-up of PPPoE or Static IPoE connections, or enabling IPTV and other services on separate VLANs, an RG configuration must be applied to set up the gateway partition. In these use cases, RG configuration may include setting up multiple routed WAN interfaces, static routes and other network defined attributes.

Connecting to the GigaCenter Home Gateway

To connect to the GigaCenter's Embedded Web Interface for the first time

1. Attach an Ethernet cable to any of the Ethernet ports on the back of the GigaCenter to an Ethernet port on your PC.
2. From your browser, enter the IP address 192.168.1.1.
3. At the login prompt, enter the credentials found on the adhesive back label shipped inside the carton of the GigaCenter. credentials as follows:
   a. Login: **admin**
   b. password: **Enter character string on label**



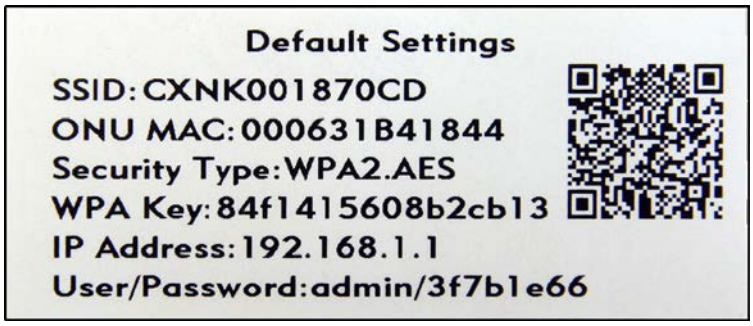
4. You now have access to Internet and Wi-Fi services on your GigaCenter.

GigaCenter Inventory

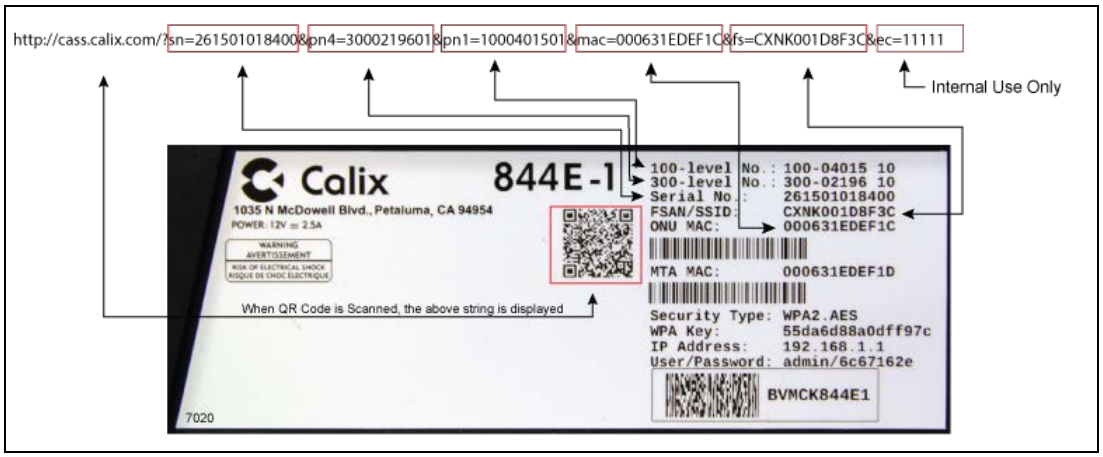
Inserted inside the shipping carton of each GigaCenter, the inventory label provides necessary product information for use in your inventory management system:

- Serial Number of the GigaCenter
- FSAN/SSID used for identifying the RSG on the Wi-Fi network.
- MAC Address of the unit needed by the Management VLAN.
- Default Wi-Fi security type and encryption scheme used by the Home Gateway
- A Default Wi-Fi WPA key such that other devices can "associate" with the Wi-Fi circuit on the GigaCenter.
- IP Address of the Unit (LAN side).
- User Name/Password credentials needed to login to the Web Interface on the LAN side of the unit

- QR Code providing links to support documentation for all Calix products. This same QR code is also printed on the product label affixed to the GigaCenter.



The QR code printed on the inventory label above and the product label below provides useful information about the GigaCenter as follows:



QR Code Output Definitions	
Scan Segment	**Description**
sn	Serial Number of the 844E Electronics
pn4	A Manufacturing level part number for tracking sub-assemblies
pn1	The orderable complete assembly part number of the unit
mac	The Optical Network Units assigned MAC address
fs	The FSAN serial number of the GigaCenter (Assigned SSID out of the box)
ec	Internal manufacturing code

About GigaCenter Resets

The 844E GigaCenter offers several different facilities for resetting and/or restoring factory default settings.

844G/854G Factory Reset Behavior			
Location of Reset	**Screen Name or Physical Location**	**Expected Behavior**	**Notes**
Utilities Menu	Restore Default	• GigaCenter Reboots. • Residential Gateway values are reset to factory default.*	Since control is available to home subscriber, restoring defaults are limited to controls that the subscriber can modify.
Rear of GigaCenter	Labeled RESET	• GigaCenter Reboots. • Residential Gateway values are reset to factory default.*	**IMPORTANT:** The RESET button must be pressed and held until the GigaCenter LEDs flash (about 5 seconds). Pressing the RESET button momentarily (less than 5 seconds executes a simple reboot of the GigaCenter (Home Gateway values persisted). **Note:** Pressing Utilities > Restore Defaults above and clicking the manual reset on the back of the GigaCenter yields identical results.
* - Examples include security credentials, SSID Names, Wi-Fi radio behaviors, and the like.			

Chapter 4

Embedded Web Interface

The Embedded Web Interface (EWI) is available for viewing and managing GigaCenters through your personal computers browser. The EWI allows you to login into any Home Gateway connected GigaCenter using its IP Address and the appropriate login credentials. Once connected, management of the device can be executed from your desktop.

In the following pages, a high level overview of the EWI is presented. Links are also provided that will allow you to drill more deeply into each item with specific field definitions for all displayed options.

The Home Gateway partition of the GigaCenter is managed through the GigaCenter Embedded Web Interface (EWI) and includes the following deployment options presented as menu items in the top navigation bar:

Embedded Web Interface Field Definitions

The Home Gateway partition of the GigaCenter is managed through the GigaCenter Embedded Web Interface (EWI) and includes the following deployment options presented as menu items in the top navigation bar:

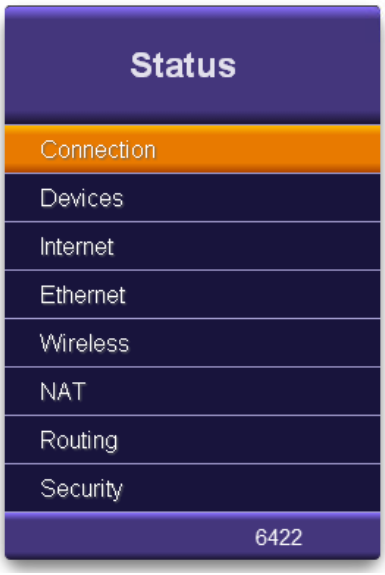
GigaCenter Embedded Web Interface	
Status Menu	
Sub-Menu Item	**Description**
Connections (on page 35)	The Connections page provides network status/details for the GigaCenter network. The table below reflects the current state of the WAN, Local Internet, and the IP Gateway connections.
Devices (on page **Error! Bookmark not defined.**)	The devices table displays a list of devices currently connected to the Local Area Network. Devices can be edited from the Edit Device table.
Internet (on page **Error! Bookmark not defined.**)	Current Internet status of the Internet Service Provider is viewable. Basic connection status, ISP statistics, and IPv4/IPv6 Addressing parameters are available.
Ethernet (on page **Error! Bookmark not defined.**)	The table reflects the Ethernet port connection status including connection speeds and current packet statistics.
Wireless (on page **Error! Bookmark not defined.**)	The table displays a summary of the settings for each wireless network (by device).
NAT (on page **Error! Bookmark not defined.**)	This dynamic table reflects the current state of the Network Address Translation (NAT). As IP addresses are resolved against the NAT table, contents of this screen are updated in real time.
Routing (on page **Error! Bookmark not defined.**)	The table displays the current routing assignments for Internet traffic on the network.
Security (on page **Error! Bookmark not defined.**)	The table displays all modified security settings from the factory default values.
Quick Start Menu	
Sub-Menu Item	**Description**
Connect to Internet (on page 48)	Gateway device connection settings are provisioned here.
Configure Wireless Network (on page 50)	Configure Wireless Network is used to enable or disable connections between this gateway device and other wireless devices. Use this screen to configured your SSID and password for the wireless network.
Set Time Zone (on page 51)	Set Time Zone is used to display this gateway device's time settings.

Wireless Menu	
Sub-Menu Item	**Description**
2.4G Network (on page 53)	Provides settings for enabling the radio, SSID set-up, wireless security, MAC Authentication, and WMM.
5G Network (on page 53)	Provides settings for enabling the radio, SSID set-up, wireless security, and MAC Authentication.
Advanced Radio Set-up (on page **Error! Bookmark not defined.**)	Various countries will allow or block certain Wi-Fi channels and as such, you can specify what country the radio is being deployed in. In addition, these countries may have varying Wi-Fi signal power levels which are also selectable by country.
WPS (on page **Error! Bookmark not defined.**)	WPS provides a secure way to establish a wireless network by sharing the wireless key between the device and wireless client.
Utilities Menu	
Sub-Menu Item	**Description**
Configuration Save (on page 62)	Configuration Backup is used to save the gateway device configuration information to a file on your PC. Configuration Restore reloads the file from your PC to restore your gateway device back to the same settings as when the backup file was last saved.
Restore Defaults (on page **Error! Bookmark not defined.**)	Select the restore button to restore the gateway device to the default settings
Reboot (on page **Error! Bookmark not defined.**)	Select the Reboot button to reboot the gateway device.
Web Activity Log (on page **Error! Bookmark not defined.**)	Web Activity Log displays a list of the most recently accessed websites. This table displays URL's accessed by the CPE on the LAN side of the RSG.
Ping Test (on page **Error! Bookmark not defined.**)	Test your internet connectivity to a specific host using the ping test below. Results of completed ping tests are displayed with detailed statistics.
Traceroute (on page **Error! Bookmark not defined.**)	Traceroute is used to determine the route taken by packets across a network. Each test reports the round trip times for 3 ICMP packets. Each response shows the maximum number of hops displayed in the first column. The test repeats until the host is reached or the maximum hop count of 30 is reached. The times for each ICMP packet are displayed in the table. An asterisk (*) in a field means that no-response was received for the ICMP packet request.
System Log (on page **Error! Bookmark not defined.**)	The system log provides an accounting of significant gateway device events.
Firewall Log (on page **Error! Bookmark not defined.**)	The Firewall Log page provides a table of the most recently dropped packets by the firewall.
Advanced Menu	
Sub-Menu Item	**Description**
Scheduling and Blocking (on page 74)	Scheduling and Blocking allows for the configuration of network access, service blocking, and website blocking.

IP Addressing (on page 82)	IP Addressing settings allow for the configuration of WAN, DHCP, and DNS settings across the network.
Static Routing (on page **Error! Bookmark not defined.**)	Routing settings allow for the configuration of dynamic (RIP) or static routing across the network.
Quality of Service (on page 90)	Quality of Service settings allow for the configuration of QoS prioritization rules across the network.
Security (on page 92)	The Calix GigaCenter incorporates various features that ensure overall network security.
Remote Management (on page 104)	Remote Management settings allow for the configuration of a secure connection to the GigaCenter network from a remote location.

Status Menu

The Status Menu provides information on the status of GigaCenter network settings.



Status Menu Overview

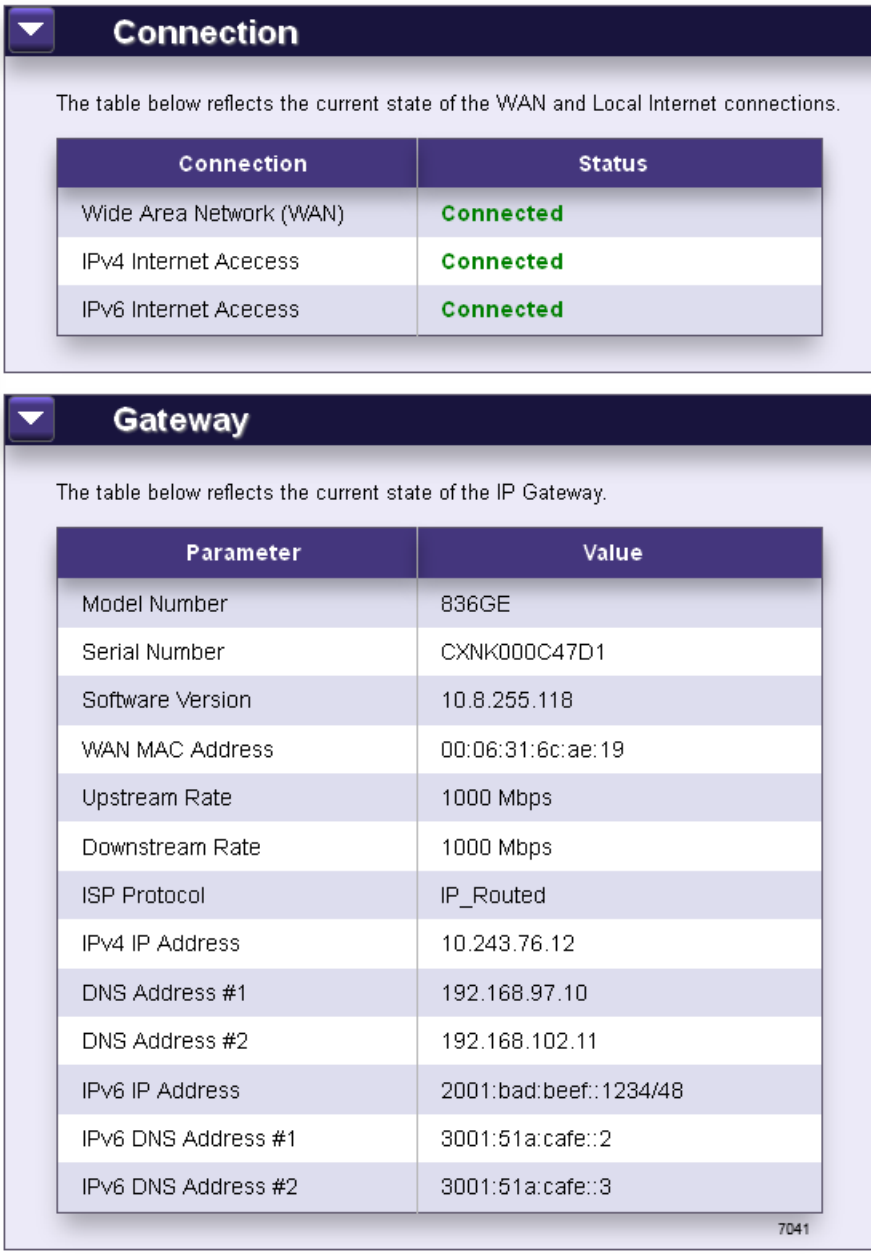
The Status menu provides real time information on all network elements.

- **Connections** - Provides information on network connectivity status as well as IP Gateway state and status.
- **Devices** - Provides a list of active or inactive devices residing on the network. Also provides the option of editing specific device names and changing the icon representing the device.
- **Internet** - Provides information on the ISP connection, protocols used, traffic statistics, and IP Addressing information for devices and DNS service locations.

- **Ethernet** - Displays the GigaCenters Ethernet ports and provides connection status with packet statistics.
- **Wireless** - Provides state and status of any of four possible Wi-Fi networks (selectable) provisioned on the GigaCenter.
- **NAT** - Provides a dynamic display of the Network Address Translation table including Source/Destination IP info, protocol used, and source/destination port.
- **Routing** - Provides a table of IPv4 routing assignments including Destination IP, Network Mask, and Gateway IP address information.
- **Security** - Provides a table of security features that have customized "rules" applied that deviate from the default behavior

Connections

The Connections page provides network status/details for the GigaCenter network. The table below reflects the current state of the WAN, Local Internet, and the IPv4/IPv6 Gateway connections.



Connection

The table below reflects the current state of the WAN and Local Internet connections.

Connection	Status
Wide Area Network (WAN)	Connected
IPv4 Internet Acecess	Connected
IPv6 Internet Acecess	Connected

Gateway

The table below reflects the current state of the IP Gateway.

Parameter	Value
Model Number	836GE
Serial Number	CXNK000C47D1
Software Version	10.8.255.118
WAN MAC Address	00:06:31:6c:ae:19
Upstream Rate	1000 Mbps
Downstream Rate	1000 Mbps
ISP Protocol	IP_Routed
IPv4 IP Address	10.243.76.12
DNS Address #1	192.168.97.10
DNS Address #2	192.168.102.11
IPv6 IP Address	2001:bad:beef::1234/48
IPv6 DNS Address #1	3001:51a:cafe::2
IPv6 DNS Address #2	3001:51a:cafe::3

7041

Status - Connection - Connection Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
Wide Area Network (WAN)	Connection status of the GigaCenter to the WAN	Info Only	N	Connected‡, Not Connected
IPv4 Internet Access	Displays the current connection state of the GigaCenter	Info Only	N	Unconfigured, Connecting, Connected, Disconnecting, Disconnected, Blank‡
IPv6 Internet Access	Displays the current connection state of the GigaCenter	Info Only	N	Unconfigured, Connecting, Connected, Disconnecting, Disconnected, Blank‡
To edit the above settings, go to Advanced > IP Addressing > WAN Settings				
Status - Connection - Gateway Field Definitions				
Software Version	Version of operating system software currently loaded on the GigaCenter	Info Only	N	Firmware Release Number
Model Number	Calix GigaCenter Model Number	Info Only	N	Model Number
Serial Number	Unique FSAN Serial Number	Info Only	N	FSAN Serial Number. Begins with CXNK followed by 8 alphanumeric digits
WAN MAC Address	WAN's Medial Access Code (MAC) Address	Info Only	N	MAC Address (xx:xx:xx:xx:xx:xx)
Downstream Rate	Current rate the GigaCenter is receiving data from the WAN	Info Only	N	Numeric Value in bits/second
Upstream Rate	Current rate the GigaCenter is sending data to the WAN	Info Only	N	Numeric Value in bits/second
PPP User Name	Point-to-Point Protocol User Name	Info Only	N	URL of the PPPoE User Name. Value set at *Quick Start > Connect to Internet > PPPoE Set-up.*
ISP Protocol	Protocol used to connect with the ISP	Info Only	N	DHCP, PPPoE, or Static. Value established at *Quick Start > Connect to Internet.*
Device IP Address	IP address assigned to the GigaCenter	Info Only	N	dot delimited, xx.xx.xx.xx. value established at *Quick Start > Connect to Internet.*
IPv4 DNS Address # 1 and IPv4 DNS Address # 2	The Domain Name Server (DNS) Addresses #1 and #2 are the IPv4 IP addresses of the primary and secondary servers that provide the URL to IP address translation for a specific site on the Internet. When a URL is entered into the address bar of a browser, the designated DNS translates the domain to an IP address to find the site on the Internet.	Info Only	N	dot delimited, xx.xx.xx.xx. Can be automatic or static value. Value established at *Quick Start > Connect to Internet*.
IPv6 IP Address	IP address assigned to the GigaCenter	Info Only	N	dot delimited, xx.xx.xx.xx. Value established at Quick Start > Connect to Internet.
IPv6 DNS Address # 1 and IPv6 DNS Address # 2	The Domain Name Server (DNS) Addresses #1 and #2 are the IPv6 IP addresses of the primary and secondary servers that provide the URL to IP address translation for a specific site on the Internet. When a URL is entered into the address bar of a browser, the designated DNS translates the domain to an IP address to find the site on the Internet.	Info Only	N	colons-hexadecimal notation. Can be automatic or static value. Value established at *Quick Start > Connect to Internet*.
To edit the above settings, go to Advanced > IP Addressing > WAN Settings ‡ = Default Value				

Devices

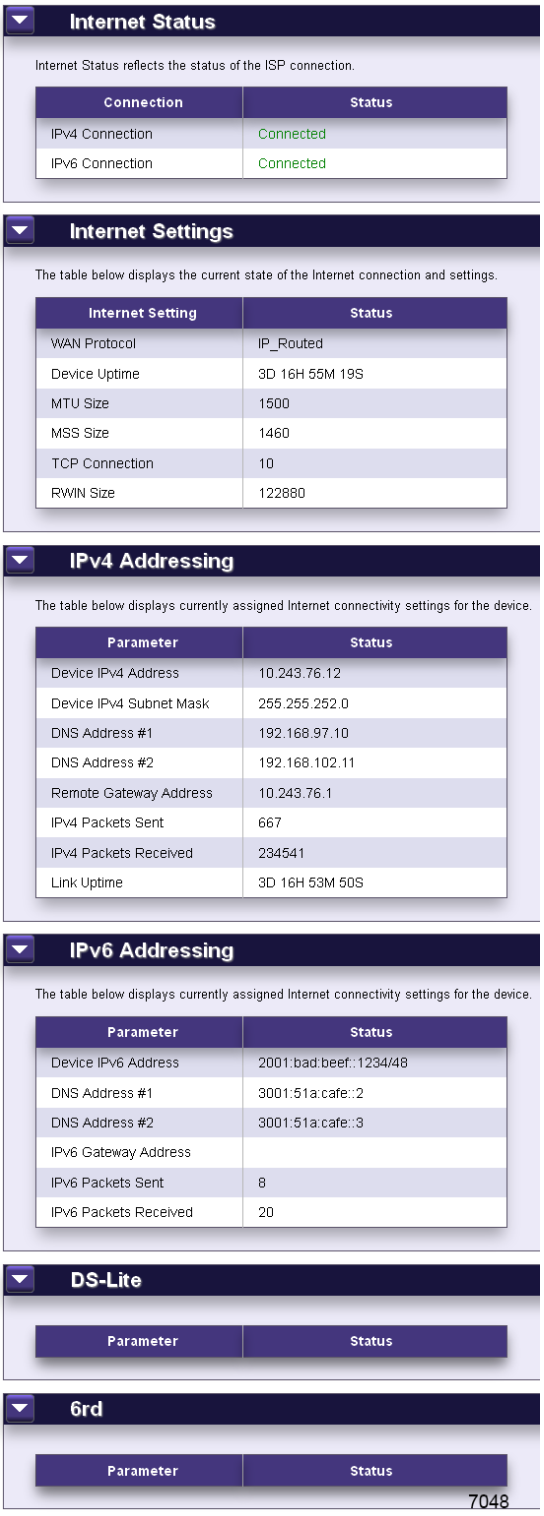
The table below displays a list of devices currently connected to the Local Area Network. Devices can be edited from the Edit Device table.

Status - Devices Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
Show inactive devices	Selecting this box displays or hides the list of inactive devices connected to the GigaCenter	Check Box	Yes	N/A - For Inactive devices, text is displayed as "grayed out" if check box is selected.
Icon	Graphical depiction of the device connected to the GigaCenter	Info Only	To edit an icon, see section below.	Available icons include: Camera, Cell Phone, Computer, Gaming Console, iPhone, IPTV STB, Phone, Printer, PS-3, Router, Satellite Receiver, Server, Video Camera, Wii, X-Box 360.
Device	Name assigned to device connected to the GigaCenter	Info Only	To edit a device name, see section below.	Alphanumeric String - 16 characters maximum
IP Address	IP address of the device connected to the GigaCenter	Info Only	No	Auto-populate. When device connects and is recognized, IP address is displayed in this field.
MAC Address	MAC address of the device connected to the GigaCenter	Info Only	No	Auto-populate. When device connects and is recognized, MAC address is displayed in this field.
Connection Type	Type of connection between GigaCenter and this device	Info Only	No	Auto-populate. Wi-Fi or Ethernet.

Status - Edit Device Field Definitions				
Select the LAN device	Choose the LAN device connected to the GigaCenter from the pull down menu	Drop-down List	No, list reflects connected device's name (name can be changed in "Enter the new device name" field below)	The device's IP Address is the default device name.
Enter the new device name	Change the selected LAN device's name	Alpha-text Box	Yes	Alpha-numeric string **Note:** Spaces are not allowed in this string.
Select a device icon	Choose the graphical element to be displayed that represents this device	Drop-down List	Yes	Available icons include: Camera, Cell Phone, Computer, Gaming Console, iPhone, IPTV STB, Phone, Printer, PS-3, Router, Satellite Receiver, Server, Video Camera, Wii, X-Box 360.
NOTE: Static Devices are not displayed in this table.				

Internet

Current Internet status of the Internet Service Provider is viewable. Basic connection status, ISP statistics, and IPv4/IPv6 Addressing parameters are available.

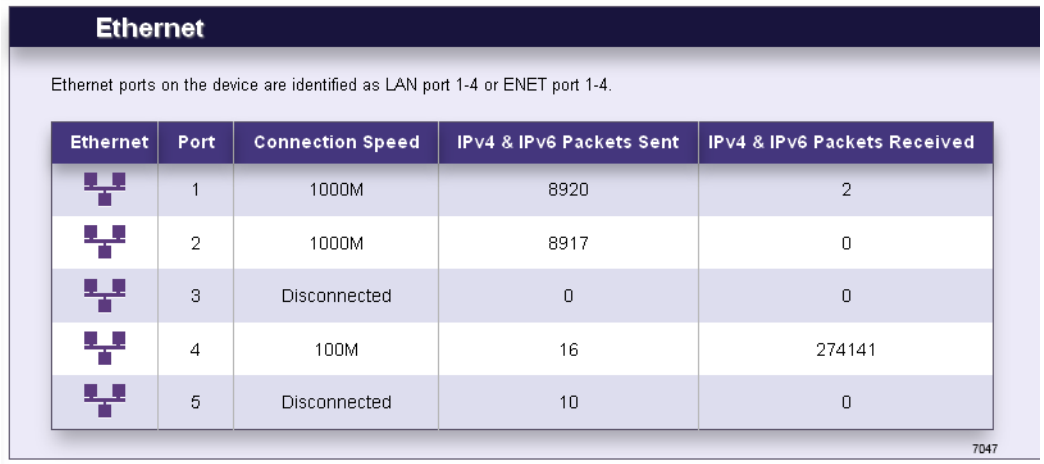


Status - Internet - Internet Status Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
IPv4 Connection	Status of the IPv4 Internet Connection	Info Only	No	Unconfigured, Connecting, Connected, Disconnecting, Disconnected, Blank‡
IPv6 Connection	Status of the IPv6 Internet Connection	Info Only	No	Unconfigured, Connecting, Connected, Disconnecting, Disconnected, Blank‡
Status - Internet - Internet Settings Field Definitions				
WAN Protocol	WAN protocol type	Info Only	No	IP Routed
Device Uptime	Elapsed time since last loss of connection of the GigaCenter	Info Only	No	Days/Hours/Minutes/Seconds format Example: *6D 17H 26M 15S*
MTU Size	The Maximum Transmission Unit size reflects the largest number of bytes able to be carried in a protocol's data transmission packet including header information	Info Only	No	Maximum number of bytes in a packet *including* header info. Default: 1500 bytes
MSS Size	The Maximum Segment Size reflects the largest number of bytes able to be carried in a protocol's data transmission packet not including header information	Info Only	No	Maximum number of bytes in a packet *not including* header info. Default: 1460 bytes
TCP Connection	Transmission Control Protocol connection manages a data stream across the Internet ensuring reliable delivery	Info Only	No	Numeric Default: 22
RWIN Size	RWIN (TCP Receive Window) size is the amount of data that a computer can accept without acknowledging the sender	Info Only	No	Numeric Default: 122880 bytes
Status - Internet - IPv4 Addressing Field Definitions				
Device IPv4 Address	IPv4 address for the GigaCenter	Info Only	No	Dot delimited, xx.xx.xx.xx
Device IPv4 Subnet Mask	Internet Protocol v4 Subnet Mask is used to split and confine traffic to one network. A subnet mask keeps all local network traffic local and only routes Internet traffic to the Internet preserving network resources	Info Only	No	Dot delimited, xx.xx.xx.xx Default: 255.255.255.0
DNS Address #1	The Domain Name Server (DNS) Addresses #1 and #2 are the IP addresses of the primary and secondary servers that provide the URL to IP address translation for a specific site on the Internet. When a URL is entered into the address bar of a browser, the designated DNS translates the domain to an IP address to find the site on the Internet	Info Only	No	Dot delimited, xx.xx.xx.xx
DNS Address #2		Info Only	No	Dot delimited, xx.xx.xx.xx
Remote Gateway Address	Remote Gateway IP Address for the device	Info Only	No	Dot delimited, xx.xx.xx.xx
IPv4 Packets Sent	Number of IPv4 packets sent by the GigaCenter	Info Only	No	Numeric
IPv4 Packets Received	Number of IPv4 packets received by the GigaCenter	Info Only	No	Numeric
Link Uptime	Elapsed time since last loss of connection to the gateway of the GigaCenter	Info Only	No	Days/Hours/Minutes/Seconds format Example: *6D 17H 26M 15S*

Status - Internet - IPv6 Addressing Field Definitions				
Device IPv6 Address	IPv6 address for the GigaCenter	Info Only	No	colon-hexadecimal notation
DNS Address # 1	The Domain Name Server (DNS) Addresses #1 and #2 are the IP addresses of the primary and secondary servers that provide the URL to IP address translation for a specific site on the Internet. When a URL is entered into the address bar of a browser, the designated DNS translates the domain to an IP address to find the site on the Internet	Info Only	No	colon-hexadecimal notation
DNS Address # 2		Info Only	No	colon-hexadecimal notation
IPv6 Gateway Address	IPv6 Gateway Address for this device	Info Only	No	Numeric
IPv6 Packets Sent	Number of IPv6 packets sent by the GigaCenter	Info Only	No	Numeric
IPv6 Packets Received	Number of IPv6 packets received by the GigaCenter	Info Only	No	Numeric

Ethernet

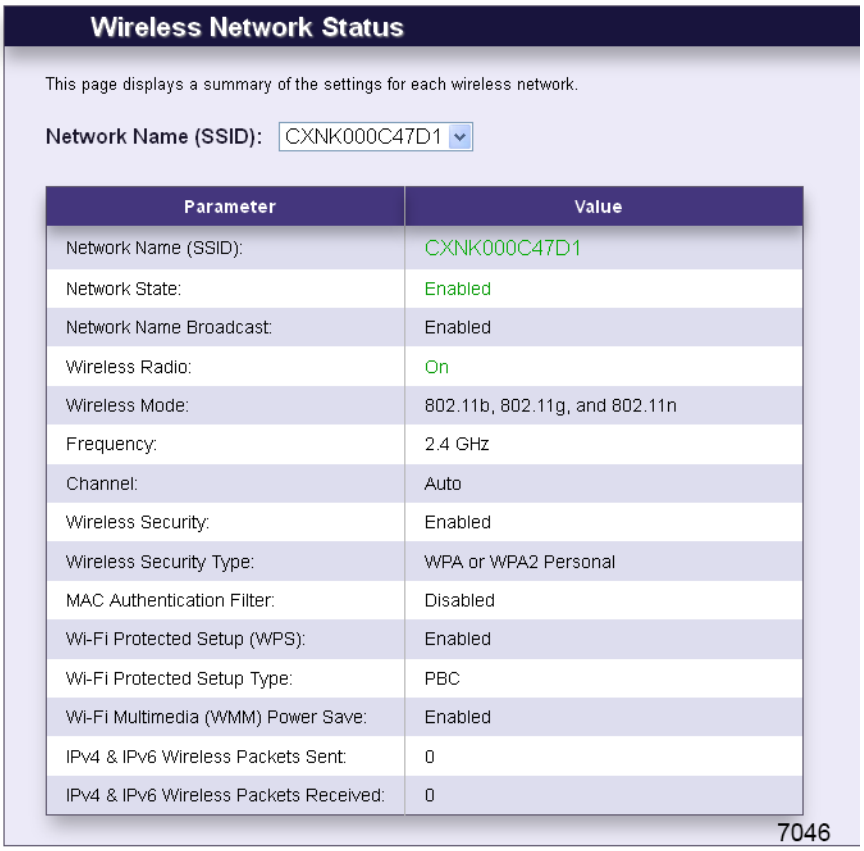
The table below reflects the Ethernet port connection status including connection speeds and current packet statistics.



Status - Ethernet Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
Port	Ethernet ports 1 through 4 as labeled on the GigaCenter	Info Only	No	1 through 4
Connection Speed	10/100/1000 BaseT Ethernet connection speed	Info Only	No	Auto-sensing and Auto-negotiating speed values: 10M, 100M, 1000M, Disconnected‡
IPv4 & IPv6 Packets Sent	Packets sent to each device connected to an GigaCenter Ethernet Port	Info Only	No	Number of packets sent - Numeric
IPv4 & IPv6 Packets Received	Packets received from each device connected to an GigaCenter Ethernet Port	Info Only	No	Number of packets received - Numeric

Wireless

The table below displays a summary of the settings for each wireless network (by device).



Status - Wireless Network Status Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
Network Name (SSID)	Pull down list of wireless network names (SSID)	Drop-down List	Yes	List of Network Names created in the system. Up to 4 networks are allowed.
Network State	State of the selected wireless network	Info Only	No	Enabled‡/Disabled
Network Name Broadcast	Wireless broadcast of wireless network name	Info Only	No	Enabled‡/Disabled
Wireless Radio	Wireless Radio State	Info Only	No	On‡/Off
Wireless Mode	List of wireless modes supported	Info Only	No	802.11b, 802.11g, and 802.11n
Frequency	Wireless radio broadcast frequency	Info Only	No	x.x GHz Default: 2.4 GHz
Operating Channel	Number of active wireless radio broadcast channels	Info Only	No	Number of active channels
Channel Mode	Defines whether the current channel displayed was dynamically assigned (Auto Select) or manually selected (Manual)	Info Only	No	Auto‡ or Manual

Status - Wireless Network Status Field Definitions				
Wireless Security	State of wireless network security	Info Only	No	Enabled‡/Disabled See *Wireless* > *WPS* (on page 59)
Wireless Security Type	Type of wireless network security being used	Info Only	No	WPA - WPA2-Personal, WPA-Personal, WPA2-Personal, WEP See *Wireless* > *Security* (on page 59)
MAC Authentication Filter	State of the MAC authentication filter	Info Only	No	Enabled/Disabled‡
Wi-Fi Protected Setup (WPS)	State of the WPS feature	Info Only	No	Enabled/Disabled‡
Wi-Fi Protected Setup Type	How is Wi-Fi Protected Setup mode launched (method employed)?	Info Only	No	Push Button Control (PBC)‡
Wi-Fi Multimedia (WMM) Power Save	State of the WMM Power Save mode	Info Only	No	Enabled‡/Disabled See *Wireless* > *Security* > *WMM* (on page 57)
IPv4 & IPv6 Wireless Packets Sent	Number of wireless packets sent from the GigaCenter	Info Only	No	Numeric - Number of packets sent
IPv4 & IPv6 Wireless Packets Received	Number of wireless packets received from the GigaCenter	Info Only	No	Numeric - Number of packets received
Connected Devices				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
Icon	Graphic depiction of the connected device	Info Only	No	N/A
Device	Device Type	Info Only	No	N/A
IP Address	IP Address of the connected device	Info Only	No	IPv4 dot delimited or IPv6 colon-hexadecimal delimited IP Address
Mac Address	MAC Address of the connected device	Info Only	No	NA
Type	Network protocol being used	Info Only	No	b, g, n, ac

NAT (Network Address Translation)

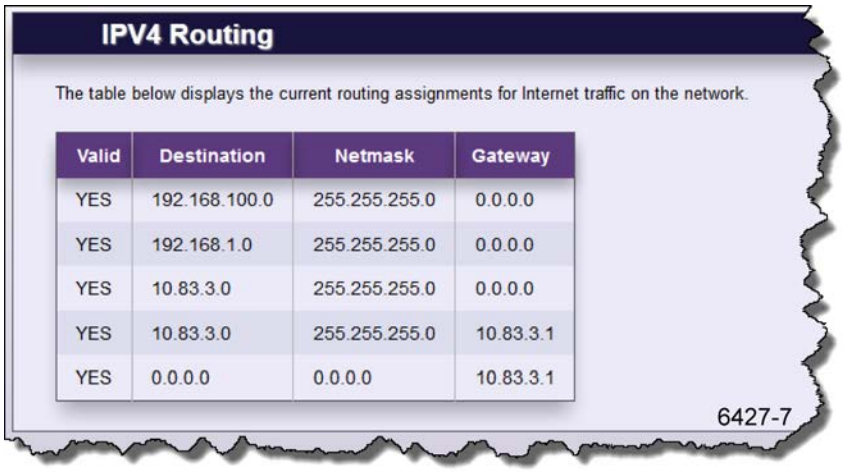
This dynamic table reflects the current state of the Network Address Translation (NAT). As IP addresses are resolved against the NAT table, contents of this screen are updated in real time.

Protocol	Timeout	Source IP	Source Port	Destination IP	Destination Port
tcp	61	192.168.12.14	51143	10.83.3.58	8080
tcp	38	192.168.12.14	51140	10.83.3.58	8080
tcp	116	192.168.12.14	51149	10.83.3.58	8080
tcp	48	192.168.12.14	51141	10.83.3.58	8080
tcp	116	192.168.12.14	51148	10.83.3.58	8080
tcp	18	192.168.12.14	51134	10.83.3.58	8080
tcp	18	192.168.12.14	51133	10.83.3.58	8080
tcp	13	192.168.12.14	51129	10.83.3.58	8080
tcp	3	192.168.12.14	51127	10.83.3.58	8080
tcp	61	192.168.12.14	51146	10.83.3.58	8080
tcp	18	192.168.12.14	51135	10.83.3.58	8080
tcp	16	192.168.12.14	51132	10.83.3.58	8080
udp	17	192.168.1.1	1900	239.255.255.250	1900
tcp	0	192.168.12.14	51128	10.83.3.58	8080
tcp	116	192.168.12.14	51147	10.83.3.58	8080
tcp	18	192.168.12.14	51138	10.83.3.58	8080
tcp	61	192.168.12.14	51144	10.83.3.58	8080
tcp	6	192.168.12.14	51130	10.83.3.58	8080
tcp	431999	192.168.12.14	51151	10.83.3.58	8080
tcp	59	192.168.12.14	51142	10.83.3.58	8080

Status - NAT - Network Address Translation (NAT) Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
Protocol	Type of protocol used to manage Internet data streams on this device	Info Only	No	Alphanumeric protocol name. TCP, UDP
Timeout	Number of seconds remaining for this table entry.	Info Only	No	1-120 seconds Note: Entry of 431999 indicates an entry that has just expired.
Source IP	Data stream source device IP address	Info Only	No	Dot delimited, xx.xx.xx.xx
Source Port	Data stream source device port number	Info Only	No	Numeric (1-65535)
Destination IP	IP Address of the GigaCenter	Info Only	No	Dot delimited, xx.xx.xx.xx
Destination Port	Destination Port for the GigaCenter	Info Only	No	Numeric port Number, 5 digit maximum

Routing

The table below displays the current routing assignments for Internet traffic on the network.

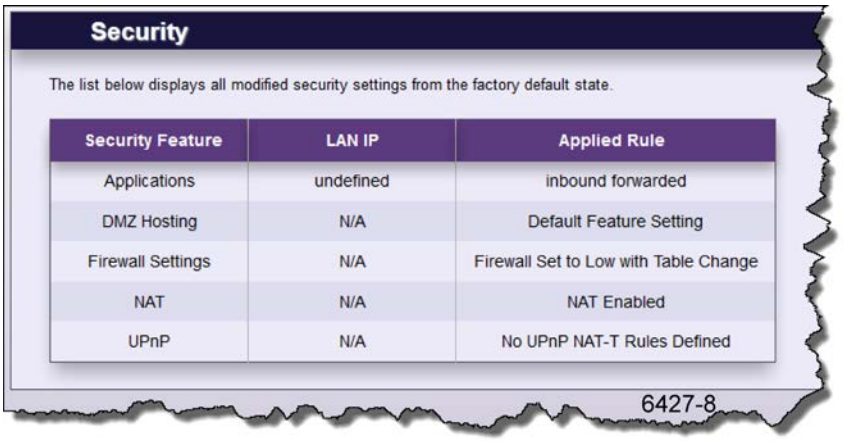


Status - Routing - IPv4 Routing Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
Valid	Valid IPv4 routing assignments	Info Only	No	YES/NO
Destination	Data streams WAN Destination IP Address	Info Only	No	Dot delimited, xx.xx.xx.xx
Netmask	GigaCenter Lan IP network mask	Info Only	No	Dot delimited, xx.xx.xx.xx
Gateway	GigaCenter Gateway IP Address	Info Only	No	Dot delimited, xx.xx.xx.xx

Note: GigaCenters do not currently support IPv6 routing.

Security

The table below displays all modified security settings from the factory default values.



Status - Security - Security Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
Security Feature	WAN and Lan security feature descriptions	Info Only	No	Applications, DMZ Hosting, Firewall Settings, NAT, UpNp
LAN IP	The IP address of the LAN interface	Info Only	No	Dot delimited, xx.xx.xx.xx. If no LAN is configured, undefined is displayed.
Applied Rule	Description of applied rule when deviating from default security settings	Info Only	No	Displays currently assigned rule for security features shown above

Quick Start Menu

Residential Service Gateway turn-up settings and parameters are contained in this menu category.

Quick Start Menu Overview

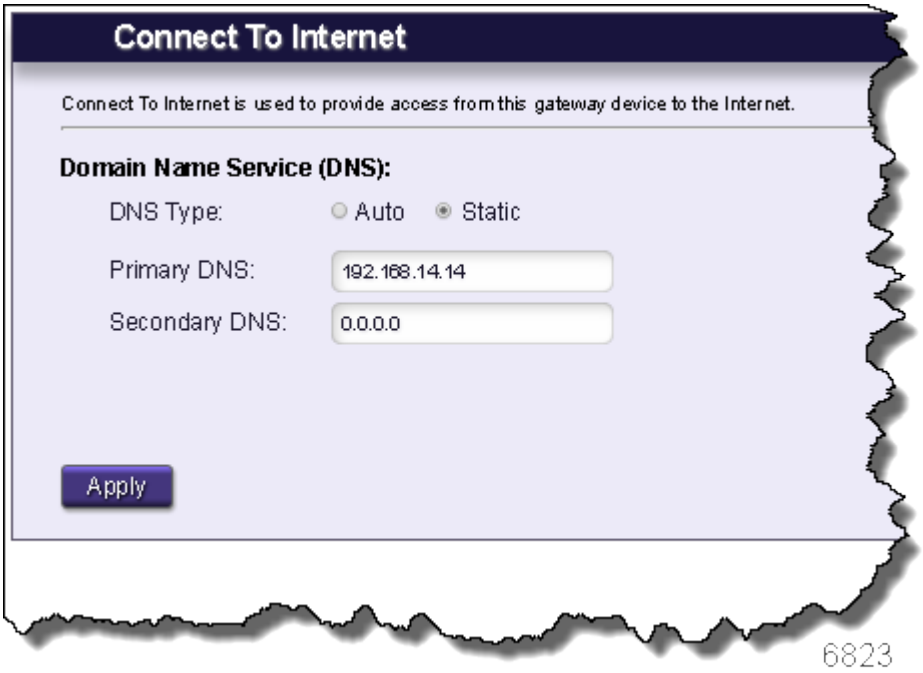
The Quick Start menu provides initial internet and wireless network connection options as well as set-up for the network clock.

- **Connect to Internet** - Provides provisioning options for connecting to the Internet including connection type, configuration of DHCP or Static IP addressing versus Point to Point over Ethernet connections, and identification of the Domain Name Server service.
- **Configure Wireless Network** - Provides facilities for configuring any 1 of 4 possible Wi-Fi networks provided by the GigaCenter. Wi-Fi can be enabled or disabled, given a network name and password for access. This Wi-Fi network is initialized via Wireless Protected Set-up (WPS/WPA, and the like). Both 2.4 GHz and 5.0 GHz radios can be enabled simultaneously.
- **Set Time Zone** - To ensure network elements remain in synchronization, the time zone must be set. A facility for adjusting to Daylight Savings time is also provided.

Connect to Internet

Gateway device connection settings are provisioned here.

Note: Since the DHCP server handles IP address functionality, no additional information is needed.



Quick Start - Connect to Internet Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
Domain Name Service (DNS)	Type of DNS	Radio Button	Yes	Auto, Static. Regardless of the connection type, defining the DNS type and Primary/Secondary DNS server addresses are needed.
Primary DNS	IP address of the Primary Domain Name Service	Numeric text box	Yes	dot delimited IP address x.x.x.x
Secondary DNS	IP address of the Secondary Domain Name Service	Numeric text box	Yes	dot delimited IP address x.x.x.x

Configure Wireless Network

Configure Wireless Network is used to enable or disable connections between this gateway device and other wireless devices. Use this screen to configure your SSID and password for the wireless network.

Quick Start - Configure Wireless Network Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
Wireless	Enables or disables the wireless network from the GigaCenter to all other wireless devices	Radio Button	Yes	On‡ or Off
Network Name	Wireless network name. This is typically the GigaCenter FSAN Serial Number.	Alpha-text Box	Yes	Alphanumeric - 32 characters maximum
WPA/WPA2 Password	Wireless network security key	Alpha-text Box	No	Alphanumeric - 63 characters maximum* Default: Field is auto-populated with password configured at factory. This password also appears on the GigaCenter label. Note: To change to a Custom Security Key, navigate to Wireless > SSID Setup > Security > Security Key/Passphrase and then enter a Custom Security Key. * Only the first 27 characters of the string are displayed in this window. To avoid confusion, keep security keys shorter than 27 characters.
Apply	Button for applying changes to Wireless Network Settings	Action Button	No	Apply changes to above settings

Wireless Protected Setup				
Connect	Wireless Protected Setup (WPS) is an easy and secure way to establish a wireless network connection between the GigaCenter and another wireless device by sharing the wireless password between the devices. Press the Connect button in the menu and then press the WPS button on the other wireless device. Conversely, pressing the WPS button on the GigaCenter achieves the same result.	Action Button	No	Ready the GigaCenter for connection to other wireless devices (Ready state).

Set Time Zone

Set Time Zone is used to display this gateway device's time settings.

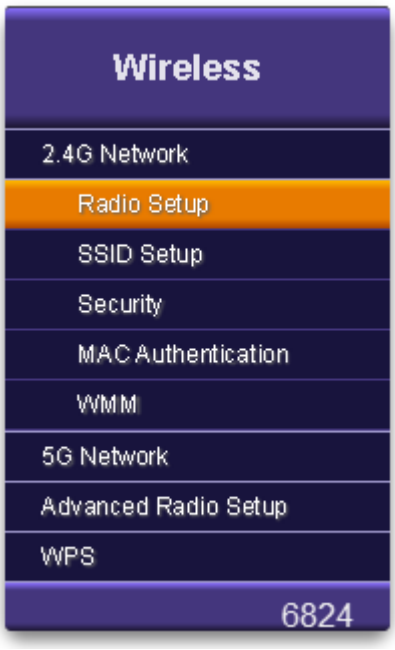
The displayed timezone setting for the GigaCenter is controlled by the NTP server setting that is pre-provisioned in the GigaCenter configuration file.

Quick Start - Set Time Zone Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
Current Time Zone	Displays time zone based on location of GigaCenter Important: Time displayed is in UTC Time. **Note:** In a GPON environment, Timing is derived from the OLT's timing source and will over-ride any settings made here.	Drop-down List	View Only	Default: Pacific Time (US and Canada)
Automatically adjust clock for Daylight Saving Time	Determine whether the NTP Server time makes adjustment for Daylight Saving Time.	Check box	View Only	Default: Unchecked (No adjustment for daylight savings time)

Wireless Menu

Under the Wireless menu, Wi-Fi, security, WPS, and MAC authentication parameters are provisioned.

Note: For purposes of this guide, definitions for both 2.4 GHz and 5.0 GHz wireless radios are combined and shown as one screen. Differences between the two protocols are noted.



Wireless Menu Overview

The Wireless menu provides set-up for the wireless radio, SSID, security, authentication, and Wi-Fi Multimedia prioritization. Set-up is available for the 2.4 GHz and 5.0 GHz frequency bands independently.

- **Radio Setup** - Includes option for enabling or disabling the Wi-Fi "radio". Options are available for setting frequency, channel, channel bandwidth, power level, and 802.11 wireless mode.
- **SSID Setup** - Allows for enabling additional SSID's for the wireless network. Configure the SSID for unique subnets or defined start URL's. The device supports one default SSID (printed on the GigaCenters label that is shipped with the product), and three optional SSID settings. The default SSID is broadcast when the gateway is powered on for the first time.
- **Security** - Wireless Security allows for configuration of a unique Wireless Equivalent Privacy (WEP) key or Wi-Fi Protected Access (WPA and WAP2) security key/pass phrase. Wireless security can also be disabled.

- **MAC Authentication** - Wireless MAC Authentication limits wireless network access to devices based on their MAC addresses. For a gateway to access a network with wireless MAC authentication, the MAC address of the gateway must be known by the wireless router.
- **WMM** - Wireless Multimedia (WMM) provides Quality of Service (QoS) on the wireless network by prioritizing traffic depending on the traffic type. Applies to the 2.4 GHz frequency only
- **Advanced Radio Set-up** - Wireless services based on country specific requirements can be selected.
- **WPS** - Wi-Fi Protected Setup (WPS) provides secure connections to wireless networks. When enabled on the router and end device, network security settings are shared. Once set-up is complete, only authenticated devices are available on the network.

Radio Setup

Radio Setup provides the ability to customize the wireless radio settings. Both 2.4 GHz and 5.0 GHz radios can be configured separately.

2.4 and 5.0 GHz Wireless - Radio Setup Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
Wireless Radio	Enable or Disable the internal wireless radio of the RSG	Radio Button	Yes	ON‡ or OFF
Wireless Mode	Used to select the wireless protocol standard	Drop-down List	Yes	802.11b* 802.11n* 802.11g* 802.11ac (applies to 5 GHz radio only) * - Applies to 2.4 GHz radio only‡. Can be configured to support a single protocol and any combination of the three.
Wireless Bandwidth	Used to set the wireless network bandwidth in the 5 GHz frequency range. Note: For the 2.4 GHz frequency, only 20 MHz service is available.	Drop-down List	Yes	20 ‡ or 40 MHz
Wireless Channel	Used to select the wireless network channel. In Auto mode, system selects best available channel.	Drop-down List	Yes	Channels 1 through 13 or Auto ‡
Wireless Power Level	Used to select the power level of the wireless radio. Calix recommends keeping the power level set to 100% under most circumstances.	Drop-down List	Yes	Percentage from 100% ‡ to 10% in 10% increments

2.4 and 5.0 GHz Wireless - Radio Setup Field Definitions				
Wireless Multicast Forwarding	Used to distribute multicast IP signals to multiple wireless devices.	Check Box	Yes	Checked (allow forwarding) ‡ When checked, multicast traffic received at the gateway is forwarded to all associated wireless clients Not Checked (block forwarding)
DFS Enable	On the 5 GHz band only, dynamic selection of frequencies in the 5.25-5.35 and 5.47-5.725 GHz ranges is supported. Enable or disable Dynamic Frequency Selection (DFS) here.	Check Box	Yes	Enable‡ or Disable
Apply	Button used to apply all settings above	Action Button	No	Apply and save changes

SSID Setup

Service Set Identifier (SSID) is used to identify this gateway device for connection to other wireless devices. The SSID may be broadcast to publish its value to aid in connecting this device to other wireless devices or it may be hidden to prevent unauthorized access. The factory-defined SSID values may be redefined to a user-specified name.

Wireless - Service Set Identifier (SSID) Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
SSID (Network Name)	The name of the GigaCenter (needed for identifying the GigaCenter when connecting to other wireless devices)	Drop-down List	Yes	Alphanumeric Default: SSID on GigaCenter product label
Broadcast SSID	Allows or restricts the wireless broadcast of the SSID (GigaCenter network name) so networked and non-networked wireless devices are aware of the wireless network	Radio Button	Yes	Enabled ‡ or Disabled
Rename SSID	Rename the selected SSID (Network Name)	Alpha-text Box	Yes	Alphanumeric - 32 characters Default: Initially populated with SSID Network Name

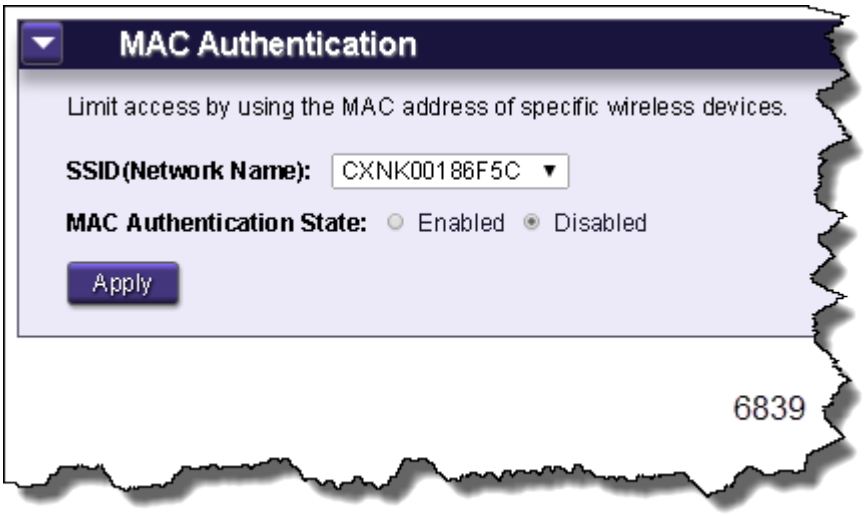
Wireless Security

Secure your wireless traffic from security threats since wireless traffic transmits unprotected.

Wireless - Security Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
SSID (Network Name)	A list of the SSID names for the GigaCenter wireless network	Drop-down List	Yes	Listed names Default: SSID from GigaCenter product label
Security Type	A list of security types and options. WPA-WPA2-Personal and WEP types require different types of "Encryption" and "Authentication"	Drop-down List	Yes	Listed security types: WPA-WPA2-Personal ‡, WEP, Security Off
Encryption Type	A list of encryption types and options	Drop-down List	Yes	AES ‡, TKIP, or Both
Security Key/Passphrase	Security key/passphrase used for *WPA-WPA2* secured network type (from above)	Radio Button	Yes	Alphanumerical string, 63 characters max. Default: Security Key/Passphrase listed on GigaCenter product label
	Security key/passphrase used for *WEP* secured network type (from above)	Radio Button for each SSID with Alpha-text Box for changing security key	Yes	Numeric hexadecimal or decimal string (12 characters maximum for 128 bit security, 10 characters maximum for 64 bit security) Default: 123456789012
Apply	Button used to apply above settings	Action Button	Yes	Apply and save changes

MAC Authentication

Limit access to your GigaCenter by using the MAC address of specific wireless devices. A device list is also provided.

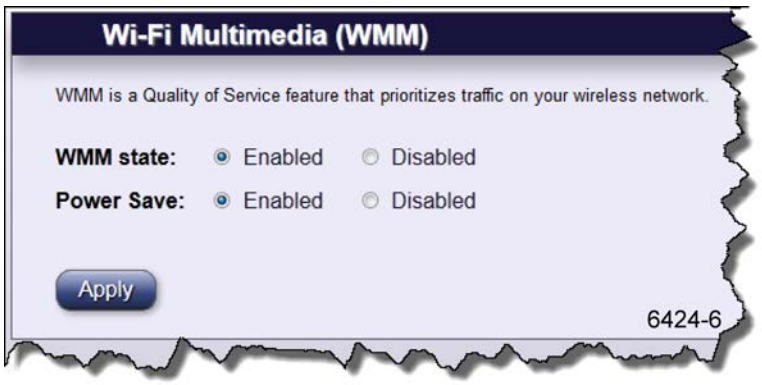


Wireless - MAC Authentication Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
SSID (Network Name)	A list of up to four SSIDs (Network Names)	Drop-down List	Yes	Up to 4 network names are displayed Default: SSID name from GigaCenter product label
MAC Authentication State	MAC Authentication limits network access by using the MAC address of specific wireless device as a key for network access	Radio Button	Yes	Enable or Disable Default: Enabled
Apply	Applies changes to MAC Authentication	Action Button	Yes	Click to Apply

WMM (Wi-Fi Multimedia)

WMM is a Quality of Service feature that prioritizes traffic on your wireless network.

Note: Applies to 2.4 GHz radio only.



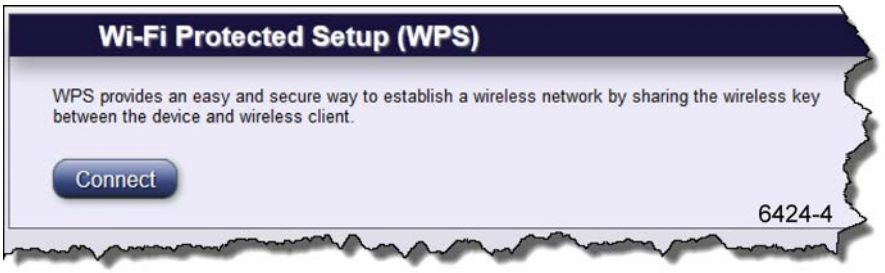
Wireless - WWM Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
WMM state	Enables or disables Wi-Fi Multimedia functionality	Radio button	Yes	Enabled ‡ or Disabled
Power Save	Enables or disables Power Save functionality	Radio button	Yes	Enabled ‡ or Disabled
Apply	Button used to apply above settings	Action Button	No	Apply and save above changes

Advanced Radio Set-up

Various countries will allow or block certain Wi-Fi channels and as such, you can specify what country the radio is being deployed in. In addition, these countries may have varying Wi-Fi signal power levels which are also selectable by country.

WPS (Wi-Fi Protected Setup)

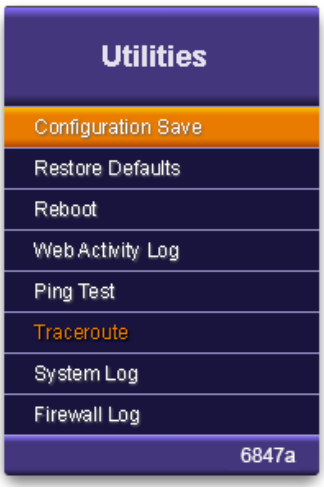
WPS provides a secure way to establish a wireless network by sharing the wireless key between the device and wireless client.



Wireless - WPS Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
Connect	Connect button activates WPS for two minutes. During that time the GigaCenter shares the wireless network key with other WPS activated devices. WPS mode can also be triggered after depressing the WPS button on the GigaCenter unit itself.	Radio Button	No	N/A

Utilities Menu

The Utilities menu provides controls for executing routine network tasks as well as providing links to various system troubleshooting routines.



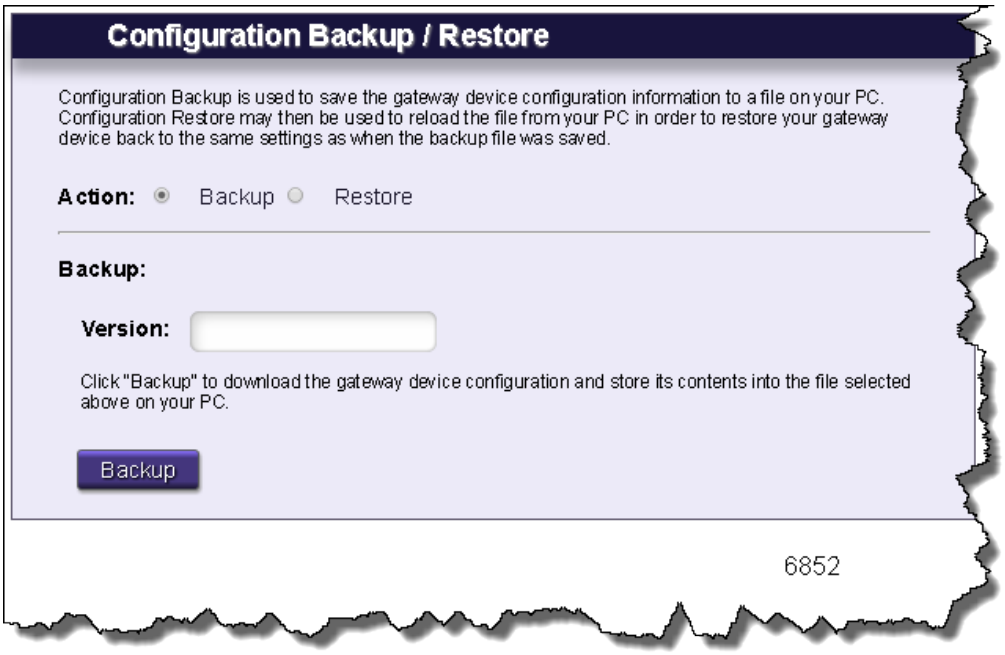
Utilities Menu Overview

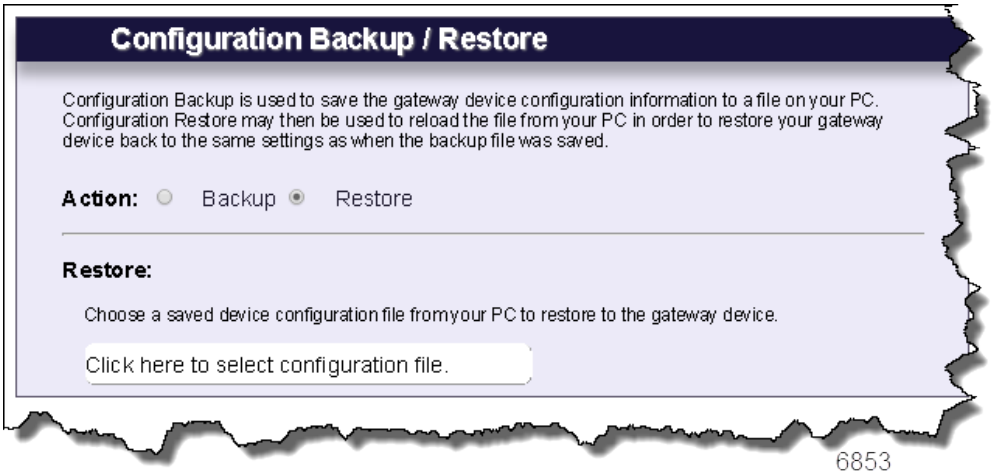
The Utilities menu provides set-up for the wireless radio, SSID, security, authentication, and Wi-Fi Multimedia prioritization.

- **Configuration Save -** Downloads the Home Gateway configuration on your PC. The file can be used to program the gateway at a later date, restoring all custom settings.
- **Restore Defaults -** Restores four different default factory settings for the device:
  - PPP Username and Password
  - Wireless Settings
  - Firewall Settings
  - Home Gateway to the Factory Default State
- **Reboot -** Rebooting the modem restarts all modem systems refreshing all connections and memory usage.
- **Web Activity Log -** Displays a list of websites visited from the gateway. The list provides the IP address of the LAN device that visited the website.
- **Ping Test -** Executes a ping test for Ethernet packets formatted for IPv4/IPv6 using the entered URL and packet size.
- **Traceroute -** Displays the Traceroute (route taken for Ethernet packets across the network) for IPv4/IPv6 formatted traffic.
- **System Log -** Records the Home Gateway setup and statistics into a text log file. This can be executed manually or automatically based on a set time interval. The gateway also captures the log file prior to a device reboot.
- **Firewall Log** - Records a history of the most recently dropped packets by the firewall.

Configuration Save

Configuration Backup is used to save the gateway device configuration information to a file on your PC. Configuration Restore reloads the file from your PC to restore your gateway device back to the same settings as when the backup file was last saved.





Utilities - Configuration Backup/Restore Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
Action	Choice of Backup or Restore to save the gateway configuration to a PC or reload the gateway configuration from the PC to the GigaCenter Note: If Restore is chosen, the Restore dialog is displayed. Note: If Backup is chosen, the Backup dialog is displayed.	Radio Button	No	Backup or Restore
Backup/Restore	Click "Backup" to download the gateway device configuration and store its contents into the file selected on your PC. Click "Restore" to retrieve a previously saved back-up. Clicking in the file name box launches Window Explorer to allow file name selection. Once a valid Restore file is selected , click "Restore" to load the contents of the saved configuration file into the GigaCenter. The GigaCenter will automatically reboot when the configuration file is loaded on the GigaCenter. The GigaCenter will then be restored back to the state of the saved configuration file settings Note: Choosing a non-valid restore file results in an error message being displayed. Click OK to choose another restore file.	Action Button	No	Begin backup/Retrieve backup

Restore Defaults

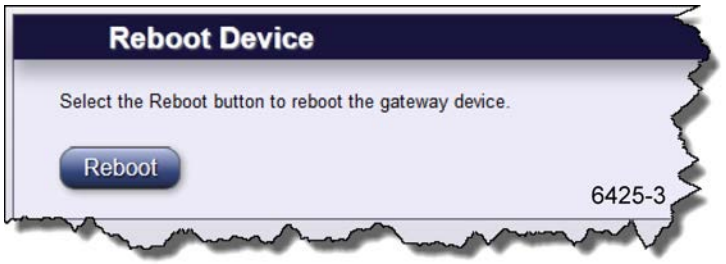
Select the restore button to restore the gateway device to the default settings Upon selecting this option, the GigaCenter will be restored to factory default settings.

Important: Any changes to the configuration since the last time this command was executed will be lost.

Utilities - Restore Defaults Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
Restore	Restores the GigaCenter to factory default settings. **Note:** While the GigaCenter is resetting, the screen may show an error condition which is considered normal. Once the reset has completed, the Restore Defaults screen will reappear. **Note:** Pressing and holding the Reset button on the back of the GigaCenter for over 15 seconds provides the same results as the Restore Defaults page.	Action Button	No	Restore

Reboot

Select the Reboot button to reboot the gateway device.



Utilities - Reboot Defaults Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
Reboot	Press the Reboot button to reboot the GigaCenter	Action Button	No	Reboot the GigaCenter

Web Activity Log

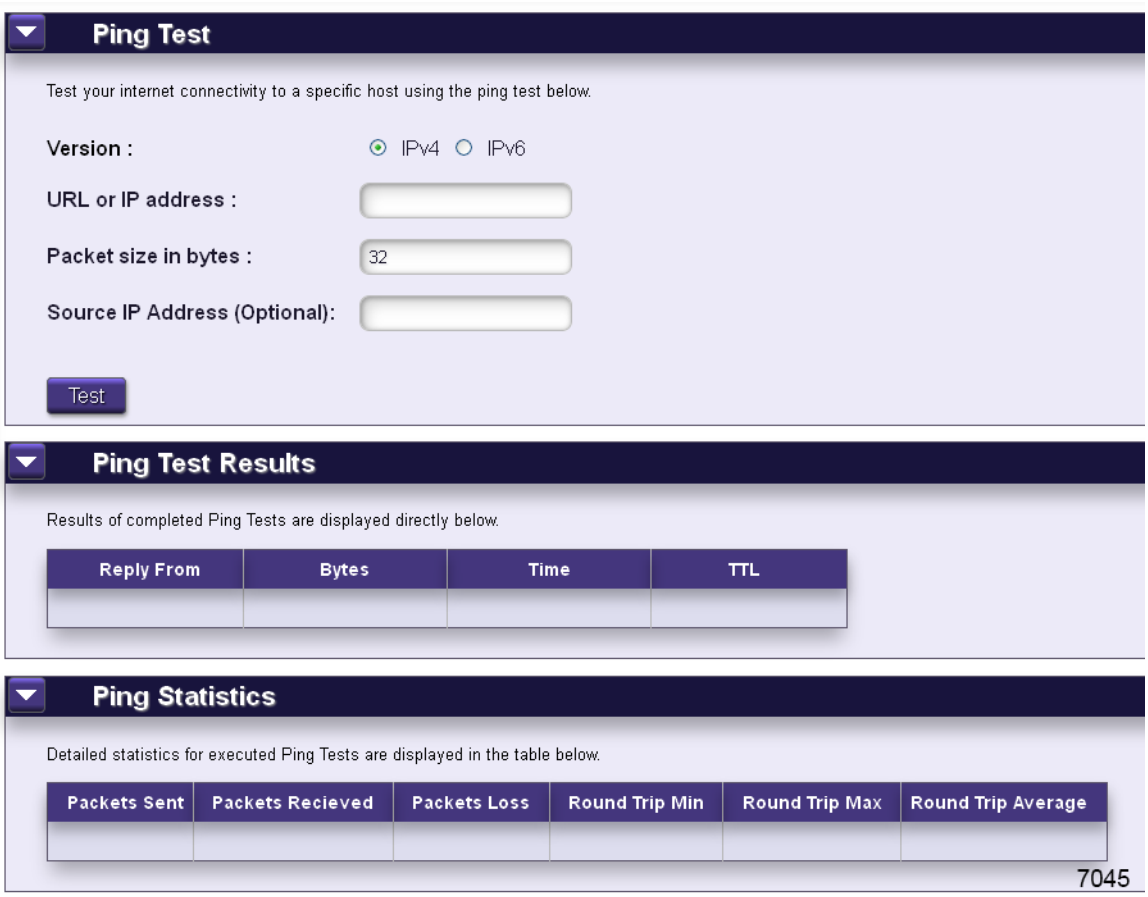
Web Activity Log displays a list of the most recently accessed websites. This table displays URL's accessed by the CPE on the LAN side of the RSG.

Utilities - Web Activity Log Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
Logging	"Enabled" and "Disabled" buttons used to activate and deactivate the logging of Web activity. When logging is disabled, the Refresh option and table are not displayed.	Radio Button	Yes	Enabled ‡ or Disabled
Refresh	Allows the Web Activity Log, displayed on the Web Activity Log page, to be refreshed manually or automatically as well as setting the auto-refresh intervals	"Manual" and "Auto" Radio Button	Yes	Manual ‡ or Auto with Refresh Rate setting. Auto refresh intervals: Realtime, 10, 20, 30, or 60 seconds If Auto is chosen, a drop-down list of auto refresh intervals is displayed. If Manual is chosen, a "Refresh" action button is displayed
Web Activity Log Output				
Date	Date of activity/event	Info Only	No	Date format: M/DD/YYYY
Time	Time of activity/event	Info Only	No	Time format: H:MM:SS
IP Address	IP address of website visited	Info Only	No	Dot delimited: xx.xx.xx.xx
Website	URL of website visited	Info Only	No	Alpha-numeric: URL format

Ping Test

Test your internet connectivity to a specific host using the ping test below. Results of completed ping tests are displayed with detailed statistics.

Note: When executing the ping test, 4 packets (32 bytes) are sent consecutively for statistical purposes.

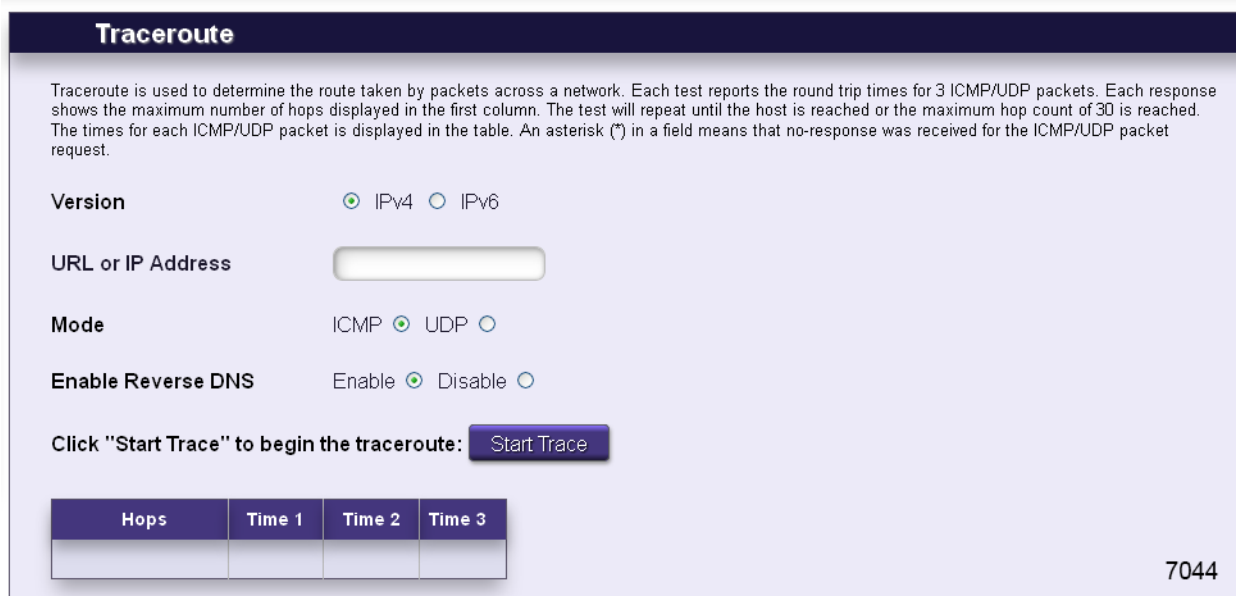


Utilities - Ping Test Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
Version	Define whether IPv4 or IPv6 IP Addresses are pinged.	Radio Button	Yes	IPv4‡, IPv6
URL or IP Address	IPv4 or IPv6 address of specific Web host to be tested or url for specific IP address.	Alpha-text Box	Yes	URL or IP Address syntax
Packet size in bytes	Specific packet size to be sent	Numeric-text Box	Yes	In bytes
Source IP Address (Optional)	IP Address of GigaCenter initiating ping	Numeric-text Box	Yes	Dot delimited: xx.xx.xx.xx or colon-hexadecimal delimited
Test	Click "Test" to commence ping test	Action Button	Yes	Performs ping test

Ping Test Results				
Reply From	URL or IP address of host being tested	Info Only	No	Recognizable URL or IP Address
Bytes	Bytes received from the pinged host	Info Only	No	Number of bytes
Time	Time ping reply was received from host	Info Only	No	Date and time
TTL	Total router "hops" before packet times out.	Info Only	No	Numeric
Ping Statistics				
Packets Sent	Number of packets sent to the host	Info Only	No	Total number of packets sent per ping request.
Packets Received	Number of packets received back from the host	Info Only	No	Total number of packets received per ping request.
Packets Loss	Number of test packets sent by the GigaCenter minus the number of packets received back by the GigaCenter	Info Only	No	Percentage of total packets versus packets lost.
Round Trip Min	Minimum elapsed time for a ping-test packet to be sent by the GigaCenter and received back from the host by the GigaCenter	Info Only	No	Round trip minimum time in milli-seconds.
Round Trip Max	Maximum elapsed time for a ping-test packet to be sent by the GigaCenter and received back from the host by the GigaCenter	Info Only	No	Round trip maximum time in milli-seconds.
Round Trip Average	Average amount of elapsed time for a ping-test packet to be sent by the GigaCenter and received back from the host by the GigaCenter	Info Only	No	Average round trip time for all 4 packets sent.

Traceroute

Traceroute is used to determine the route taken by packets across a network. Each test reports the round trip times for 3 ICMP packets. Each response shows the maximum number of hops displayed in the first column. The test repeats until the host is reached or the maximum hop count of 30 is reached. The times for each ICMP packet are displayed in the table. An asterisk (*) in a field means that no-response was received for the ICMP packet request.



Utilities - Traceroute Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
Version	Specify whether the traceroute command is applied to an IPv4 or IPv6 IP address.	Radio Button	Yes	IPv4‡, IPv6
Enter a URL or IP Address	Enter the URL or IP address of the destination host	Alpha-text Box	Yes	Recognizable URL or IP Address
Mode	Select the Traceroute protocol	Radio Button	Yes	ICMP, UDP
Enable Reverse DNS	Enable or Disable reverse DNS execution. With reverse DNS enabled, an IP address search provides domain name registry and registry table information. You may be able to identify spammers or malicious attacks on your firewall by using reverse DNS lookup. Also useful in determining the ISP name for a particular IP address.	Radio Button	Yes	Enable/Disable
Start Trace	Initiate the traceroute request	Action Button	Yes	Initiate traceroute

Traceroute Results				
Hops	Maximum number of hops (up to 30)	Info Only	No	Numeric up to 30
Time 1, 2, 3	Time of round trip for each ICMP packet from hop to hop	Info Only	No	Time value in milli-seconds
Host/IP Address	Displays URL or IP address of traceroute host	Info only	No	Recognizable URL or IP Address

This site performs a reverse DNS lookup of an IP address by searching domain name registry and registrar tables. IP addresses are four numbers in the range of 0 to 255 separated by periods.

You may be able to identify the domain name of a spammer sending you spam email or the domain name of a computer trying to break into your firewall or someone trying to hack your system.

You may also be able to use this information to determine the name of the internet service provider assigned to a particular IP address.

System Log

The system log provides an accounting of significant gateway device events.

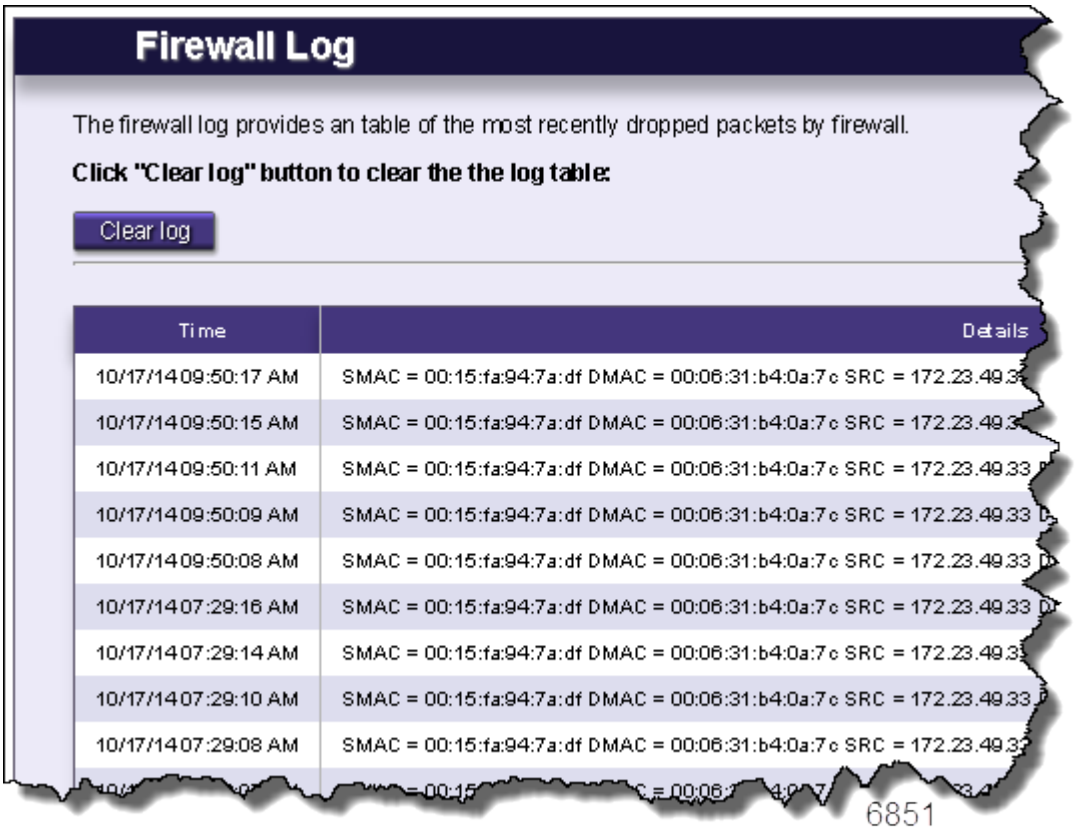
Utilities - System Log Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
Refresh Interval - Manual Refresh	Allows the System Log to be refreshed manually or automatically as well as setting the auto-refresh intervals	Radio Button with Action Button	Yes	See options directly below
Manual Refresh	Allows for on-demand refresh of the System Log	"Manual Refresh" button and a "Refresh" radio button for manual refresh	Yes	Manual Refresh ‡ Action Radio Button with Refresh Action Button
Auto Refresh	Allows and schedules auto-refresh of the System Log	"Auto Refresh" button along with a pull-down list of auto refresh intervals	Yes	Auto Refresh Radio Button with Refresh Action Button Auto refresh intervals list: Real time, 10, 20, 30 seconds, or 1 minute ‡ Manual "Refresh" Radio Button
Reboot Behavior	Controls System Log reboot behavior for clearing or saving the System Log information	N/A	N/A	N/A
Clear on Reboot	When chosen, clears the System Log on reboot	Clear on Reboot action button	Yes	Clear on Reboot
Save on Reboot	When chosen, saves the System Log on reboot	Save on Reboot action button	Yes	Save on Reboot
Save Log	Click button to save SystemLog to your PC	Action Button	No	Save Log action button

System Log Table Field Definitions				
Date	Date of significant GigaCenter event	Info Only	No	Date format: mm/dd/yy
Time	Time of significant RSG event	Info Only	No	Time format: hh:mm:ss AM/PM
System	GigaCenter system that experienced the event	Info Only	No	System event Name
Action	GigaCenter response to the event	Info Only	No	System Response

Firewall Log

The Firewall Log page provides a table of the most recently dropped packets by the firewall. The output includes information on:

- Source MAC Address
- Destination MAC Address
- Source IP Address
- Destination IP Address
- Packet protocol
- Source Port Assignment
- Destination Port Assignment

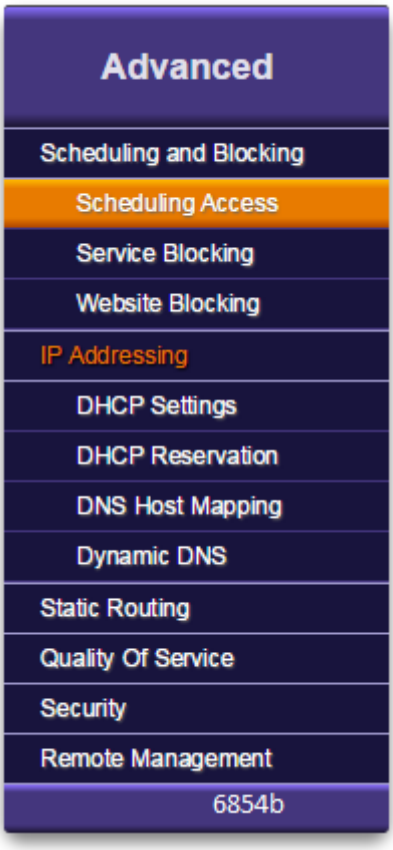


Utilities - Firewall Log Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
Time	Displays the date and time the log was captured	Display Only	No	date format: mm/dd/yy time format: hh:mm:ss AM/PM
Details	Displays MAC Address, IP Address, Packet Protocol, and Port Assignment information.	Display Only	No	N/A

Advanced Menu

The Advanced Menu provides controls for:

- Scheduling/blocking access to specific sites or services
- Customization of all IP Addressing protocols
- Dynamic vs. Static Routing controls
- QoS settings
- Additional Security settings
- Remote EWI settings



Scheduling and Blocking Overview

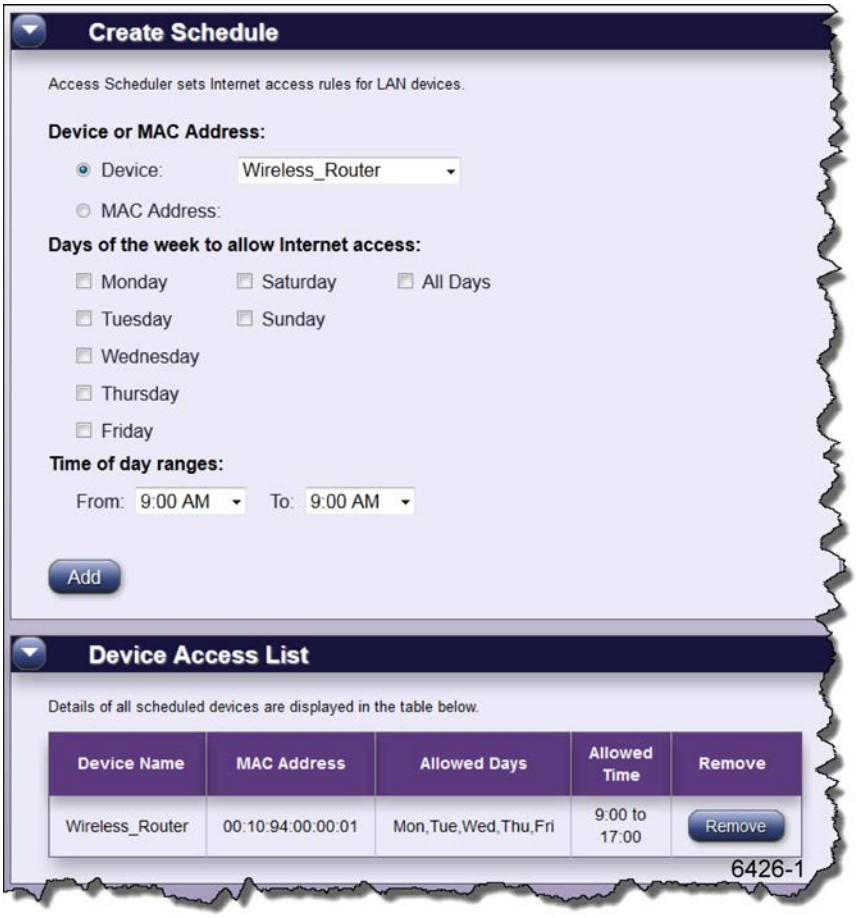
Scheduling and Blocking allows for the configuration of network access, service blocking, and website blocking.

Note: Features listed below can be customized under the Advanced > Scheduling and Blocking tab of the EWI.

- **Scheduling Access** - Limits can be applied to LAN devices as to the time and day these devices can access the Internet. Configurable by device name or MAC address.
- **Service Blocking** - Service blocking prevents specific devices from accessing internet applications. Blocking is accomplished by creating an association between a service and device name or IP address.
- **Website Blocking** - Website blocking prevents specific internet sites from being accessible. Blocking is accomplished by associating a specific URL with a device name or IP address.

Scheduling Access

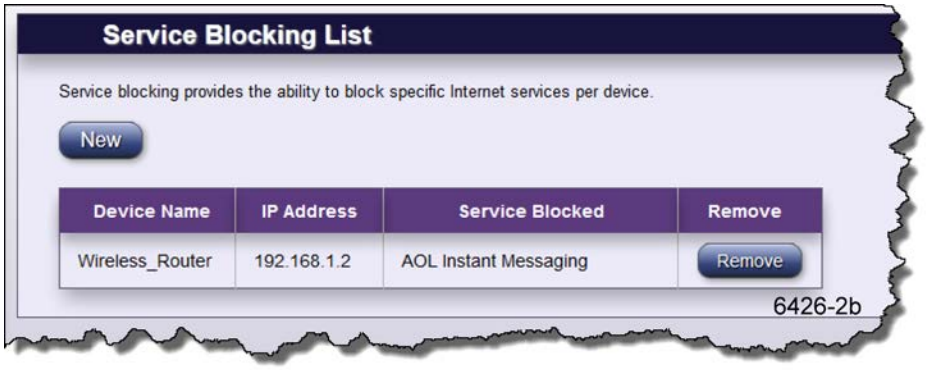
Access Scheduler sets Internet access rules for LAN devices. Scheduled devices are displayed in the Device Access List.



Advanced- Scheduling and Blocking - Scheduling Access Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
Device	If Device Radio Button is chosen, Drop-down List of device names is displayed	Radio Button and Drop-down List	Yes	Alphanumeric Names Default: Connected LAN devices
MAC Address	If MAC Address is chosen, Alpha-text box is displayed	Radio Button and Alpha-text Box	Yes	Colon delimited (xx:xx:xx:xx:xx:xx)
Days of the week to allow Internet Access	Check days of week to allow LAN devices Internet access	Check Box	Yes	Selectable by day of week
Time of day ranges	Set the hours of the day devices are allowed Internet access	Drop-down List	Yes	Select pre-defined start and stop times for schedule range
Add	Add the chosen device's Internet access schedule	Action Button	Yes	Click to apply and save changes
Device Access List				
Device Name	List of LAN devices that are controlled by Internet access list "Create Schedule"	Info Only	Yes - see above	List of days allowed (Mon, Tue, Wed, Thur, Fri, Sat, Sun)
MAC Address	MAC address of LAN devices that are controlled by Internet access list "Create Schedule"	Info Only	Yes - see above	Alpha-numeric colon delimited MAC address
Allowed Days	Days Internet access is allowed for each device	Info Only	Yes - see above	Drop-down List
Allowed Time	Starting and Stopping times to allow Internet access to the device or service	Info Only	Yes - see above	Drop-down List
Remove	Remove device from "Create Schedule". Note - removed devices have no restrictions unless specified otherwise in Service Blocking or Website Blocking	Action Button	Yes	Remove scheduling restrictions on chosen device

Service Blocking

Service blocking provides the ability to block specific Internet services per device. From the Service Blocking tab, a new association can be created between a service and a device. Newly created association details are displayed in the Service Blocking List.



Advanced - Scheduling and Blocking - Service Blocking List Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
New	Select the "New" button to set up blocking of an Internet service per device.	Action Button	Yes	Select the New button to open the "Create New Association Dialog shown above"
Service Blocking List				
Device Name	List of "Device Names" set up with service blocking	Info Only	No	Alphanumeric name of the device where service blocking is desired.
IP Address	"IP Address" list of devices set up with service blocking	Info Only	No	Dot delimited IP address of the device. (xx.xx.xx.xx)
Service Blocked	Name of "Service Blocked"	Info Only	No	Alphanumeric name of the type of service to be blocked.
Remove	Button to "Remove" the LAN device from service blocking	Action Button	Yes	Remove Service Blocking between this device and the listed service.

By clicking the New action button on the Service Blocking List screen, an association can be created between a specific service and a specific device.

Advanced - Scheduling and Blocking - Create New Association				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
Service	A list of service rules previously configured for service blocking	Drop-down List	Yes - see below	Previously configured service blocking rules appear in this drop-down list.
View	Button to "View" an info only chart listing: "Service Rule", "Protocol" type, "Port Start", "Port End", and "Port Map" for the chosen "Service" pull down menu	Action Button	Yes	View only
New	Reveals the "Create New Service Rule" page used to create a new service to be added to the "Service" pull down list. "Create a New Service Rule" consists of "Name" field, "Protocol" pull down list, "Clear Fields" radio button, "Port Start" field, "Port End" field, "Port Map" field and "Apply" and "Cancel" radio buttons - See Create New Service Rule below	Action Button	Yes	See next section below.
Associate Service with Device	"Device" button used to associate selected name on pull down with the above listed "Service"	Action Button	Yes	Device button with alphanumeric list of devices - Device or IP Address
Associate Service with IP Address	"IP Address" button used to reveal a field for entering the IP Address of a device to be associated with the above listed "Service"	Action Button	Yes	Device button with alphanumeric list of devices - Device or IP Address
Apply/Cancel Button	"Apply" radio button applies and saves the "Create New Rule" settings into the Service Rule Chart and pull down "Services " list "Cancel" radio button cancels application of the service rule setting on the "Create New Service Rule" page and exits the page	Action Button	Yes	Apply and Save changes or Cancel

By clicking the New Service action button in the Create New Association screen, rules can be configured for specific services.

Advanced - Scheduling and Blocking - Create New Service Rule				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
Name	Name of the new service blocking rule to create	Drop-down List	Yes	Alpha-numeric name
Protocol	Packet protocol to be used for the service rule	Drop-down List	No	TCP, UDP, or Both Default: TCP
Clear Fields	Use the "Clear Fields" radio button to clear the "Name", "Port Start", "Port End" and "Port Map" fields in the "Create New Service Rule" section	Action Button	Yes	Clear fields radio button.
Port Start	Starting TCP or UDP port number to that is affected by the blocking rule.	Alpha-numeric Text	Yes	Port 1 through 65535
Port End	Ending TCP or UDP port number to that is affected by the blocking rule.	Alpha-numeric Text	Yes	Port 1 through 65535
Port Map		Alpha-numeric Text	Yes	Port 1 through 65535
Apply/Cancel	Apply and Save or Cancel the changes to the service rule	Action Button	Yes	Apply or Cancel radio button

Website Blocking

Website blocking provides the ability to block specific websites per device or IP address.

Advanced - Scheduling and Blocking - New Website Blocking Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
New	Select the "New" button to set up blocking of a specific website per device or IP address	Action Button	Yes	Create Blocking for a website.
List of Blocked Websites				
Device Name	Specific Device or List of all devices tagged for blocking	Info Only	No	Static Table Default: All Devices
IP Address	Specific IP Address or all IP addresses associated with a particular device	Info Only	No	Static Table Default: Device Button Selected
Website Blocked	Specific website to be blocked	Info Only	No	URL of website to be blocked (dot delimited format)
Remove	Button to Remove the network device from website blocking	Action Button	Yes	Remove radio button

Choosing New from the screen above opens the "Create New Association" window where specific websites, devices, or IP addresses may be blocked.

Advanced - Scheduling and Blocking - Create New Association Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
New	Select the "New" button to set up blocking of a specific website per device or IP address	Action Button	Yes	Create Blocking for a website.
Create New Association				
Website Address	Input a website address that is to be blocked	Alpha-numeric Text	Yes	Alpha-numeric text in URL format
Associate Website with Device	Choose a currently connected network device to block the URL input above	Radio Button with Drop-down List	Yes	Default: Device Button Selected Default: Drop-down List "All Devices"
Associate Website with IP Address	Choose a currently connected network device by inputting its IP address	Radio Button with Numeric Text	Yes	Dot-delimited IP address Default: Radio Button Not Selected Default: All IP addresses
Apply/Cancel	Apply creates an association as provisioned above and saves the association. Cancel discards all changes	Action Button	Yes	Apply and Save changes.

IP Address Overview

IP Addressing settings allow for the configuration of WAN, DHCP, and DNS settings across the network.

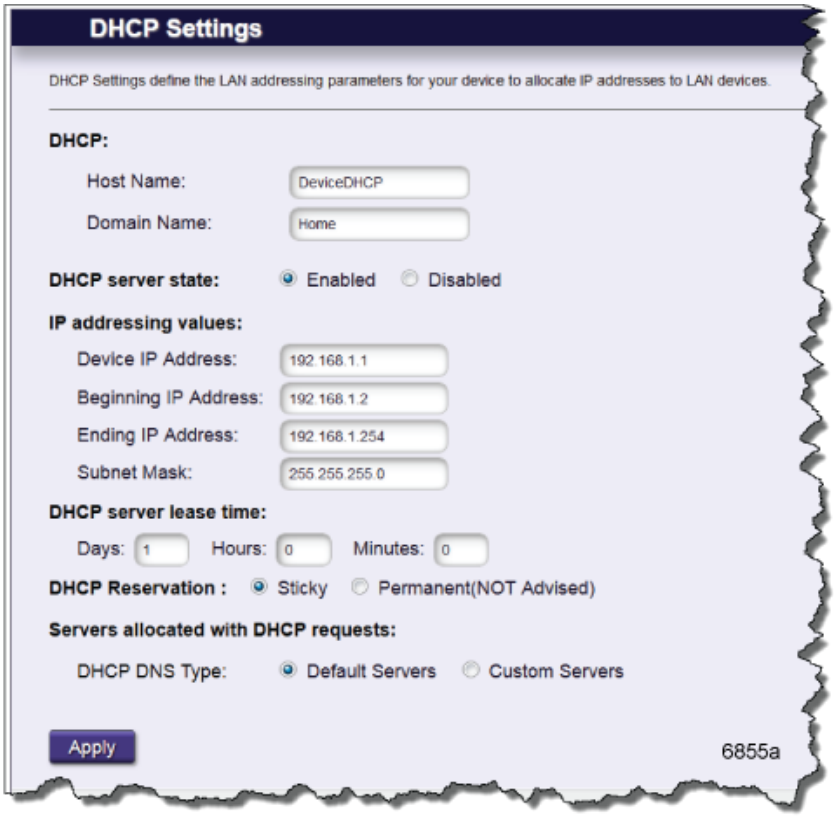
Note: Features listed below can be customized under the Advanced > IP Addressing tab of the GUI.

- **WAN Settings -** Sets ISP requirements and parameters for internet access.
- **IPv6 LAN Settings** - Sets up parameters for IPv6 addressing.
- **DHCP Settings** - DHCP server configuration, IP addressing reservations, server lease times, as well as DNS server parameters are configured here.
- **DHCP Reservation** - DHCP reservations allow for the permanent allocation of a DHCP address to a client, even after a reboot.
- **DNS Host Mapping** - DNS Host Mapping creates a static host name for a specific IP address at the router. Both WAN and LAN IP addresses can be mapped here.
- **Dynamic DNS** - Dynamic DNS associates a WAN IP address with a specific host name and updates the DNS server when the WAN IP address changes.

Note: The Dynamic DNS service is hosted through *www.dyndns.com* (*http://www.dyndns.com*)

DHCP Settings

DHCP Settings define the LAN addressing parameters for your device to allocate IP addresses to LAN devices.



Advanced - IP Addressing - DHCP Settings Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
DHCP Host Name	Defined host name for the DHCP service.	Alpha text box	Yes	Alpha-numeric string.
Domain Name	Assigned Domain Name for the IP Address associated with this GigaCenter	Alpha text box	Yes	Alpha-numeric string.
DHCP server state	Set the "Enabled" or "Disabled" state of the GigaCenter to allocate IP addresses to attached LAN devices	Radio Button	Yes	Enable or Disable the DHCP Server
Device IP Address	The IP Address of the GigaCenter device	Numeric	Yes	Dot delimited, xx.xx.xx.xx
Beginning IP Address	The first assignable IP address for LAN devices	Numeric	Yes	Dot delimited, xx.xx.xx.xx
Ending IP Address	The last assignable IP address for LAN devices	Numeric	Yes	Dot delimited, xx.xx.xx.xx
Subnet Mask	The assigned "Subnet Mask" is used to split and confine traffic to one network. A subnet mask keeps all local network traffic local and only routes Internet traffic to the Internet preserving network resources	Numeric	Yes	Dot delimited, xxx.xxx.xxx.xxx Default: 255.255.255.0
DHCP Server Lease Time	The length of time the DHCP server lease remains active without renewing	Alpha-numeric Text	Yes	Enter lease time in Days, Hours, and Minutes

Advanced - IP Addressing - DHCP Settings Field Definitions				
DHCP Reservation	Sticky: Once the router initially assigns a particular IP address to a client (laptop, tablet, smart phone, etc.) the client keeps that same address until the router is rebooted. Upon reboot, the router attempts to restore the existing DHCP address. This is the default behavior. In this mode, leases expire and are re-issued using the same IP address if possible. Permanent: Once the router assigns a particular address to a client, the client always gets that address until the router is rebooted. Upon reboot, a different address is assigned to the client however the previous lease/IP address are retained. **Note:** Usage of "permanent" may result in exhaustion of the IP address pool and should be used only in rare circumstances. Please contact your operator before using permanent. **Note:** Performing a factory reset restores the default behavior (Sticky).	Radio Button	Yes	Sticky‡ or Permanent
Servers allocated with DHCP requests - DHCP DNS Type	If Default Servers are selected, assigned DNS server (192.168.1.1) is passed to LAN-side DHCP clients during Offer/ACK messaging . If Custom Servers is selected, the primary and secondary DNS servers provide the URL to IP translation for a specific site (the ISP assigns DNS server addresses). Note: This behavior is dependent on NAT settings as well. With NAT enabled, whether custom or default servers are chosen, the GigaCenter always acts as the DNS proxy agent to LAN side clients, behaving as the default server (192.168.1.1). If NAT is disabled, Custom server information from the ISPs DHCP offers will be sent (when this field is set to Custom Servers).	Radio Button	Yes	Default Servers ‡ or Custom Servers Note: If you enable Dynamic Routing (RIP) without disabling NAT, an error message appears reminding you to disable NAT before proceeding.
Apply	Apply and Save changes to DHCP settings	Action Button	Yes	Apply and save changes

This field defines the DNS-Server IP addresses that will be passed to LAN-side DHCP-clients in the Offer/Ack messages.

- If "Default" is selected, the GigaCenter local LAN host (192.168.1.1) will be sent.
- If "Custom" is selected, there is a complication with this that Randy will need to explain. Something to do with NAT….

IPv6 LAN Settings

IPv6 LAN settings determine whether IPv6 addressing will be supported on this GigaCenter and now it functions.

Advanced - IP Addressing - IPv6 LAN Settings				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
Select LAN	Select the LAN type. In this release, only Primary Bridge is available.	Drop-down List	Yes	Primary Bridge
IPv6 Status	Enable or Disable IPv6 address support	Radio Button	Yes	Enabled, Disabled
DHCPv6 Server	Enable or Disable a DHCPv6 capable server. Enabled (Stateful) specifies a standard DHCPv6 server while Enable (Stateless) uses the Stateless Address Auto-Configuration (SLAAC) method to obtain IPv6 addresses.	Radio Button	Yes	Enabled (Stateful), Enable (Stateless), Disabled
Name Server Mode	Select whether the default Name Server mode is used (DNS servers used by the WAN) or a custom DNS server is available. For custom mode, you must enter a Primary and Secondary DNS server IP address.	Radio Button	Yes	Default, custom

DHCP Reservations

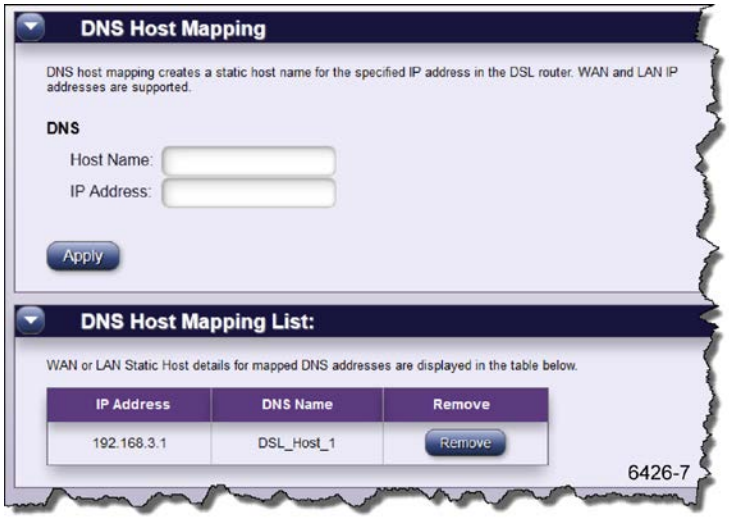
DHCP reservation leases a permanent DHCP allocated address to a client and displays a list of these reservations.

Advanced - IP Addressing - DHCP Reservations Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
Select Device or manually enter a MAC address	Select the type of LAN device identifier, "Device" or a "MAC Address", to associate with an IP Address Choosing the "Device" button reveals a pull down list used to select the LAN device to be associated with an "IP Address" Choosing the "MAC Address" button reveals a field used to identify the LAN device to be associated with an "IP Address"	Radio Button	Yes	Choose Device ‡ or MAC Address. If Device is chosen, select a device from the drop-down list. If MAC address is chosen, default is Null.
Select an IP address to associate with a MAC address	Select the "IP Address" from the pull down range of IP Addresses to be associated with the "Devices" and "MAC Addresses" connected to the GigaCenter	Drop-down List	Yes	IP Addresses from the drop-down list. Range: 192.168.1.2 through 192.168.1.254 Default: 192.168.1.2
Apply	"Apply" radio button applies and saves the "DHCP Reservation" settings	Action Button	Yes	Applies and saves changes

DHCP Reservation List				
Device Name	Device Name selected from above	Info Only	No	Alpha-numeric
MAC Address	MAC Address input above	Info Only	No	Numeric - MAC address format: xx:xx:xx:xx:xx:xx
IP Address	IP Address selected from the drop-down list above	Info Only	No	Dot delimited IP Address xx.xx.xx.xx
Remove	Remove the LAN device specified from the DHCP Reservation List	Action Button	Yes	Remove the device

DNS Host Mapping

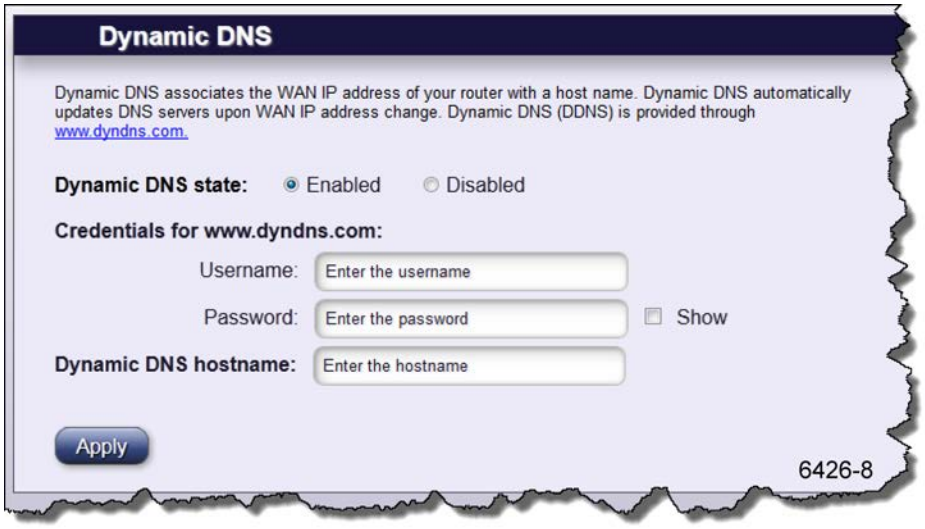
DNS host mapping creates a static host name for the specified IP address in the DSL router. WAN and LAN IP addresses are supported. A list of DNS Host mappings is also displayed.



Advanced - IP Addressing - DNS Host Mapping Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
DNS Host Name	DNS Host Name to be associated with the DNS IP Address	Alpha-numeric Text	Yes	Alphanumeric Default: Null
DNS IP Address	DNS IP Address to be associated with the above DNS Host Name	Alpha-numeric Text	Yes	Dot delimited IP Address (xx.xx.xx.xx) Default: Null
Apply	"Apply" radio button applies and saves the "DNS Host Mapping List"	Action Button	Yes	Click to apply and save DNS Host Mapping
DNS Host Mapping List				
IP Address	IP Address for the WAN or LAN Static Host	Info Only	No	Dot delimited IP Address (xx.xx.xx.xx)
DNS Name	DNS Name of the Static Host	Info Only	No	Alpha-numeric text
Remove	Click to remove the DNS Host IP Address from the Host Mapping table	Action Button	Yes	Click to remove mapping

Dynamic DNS

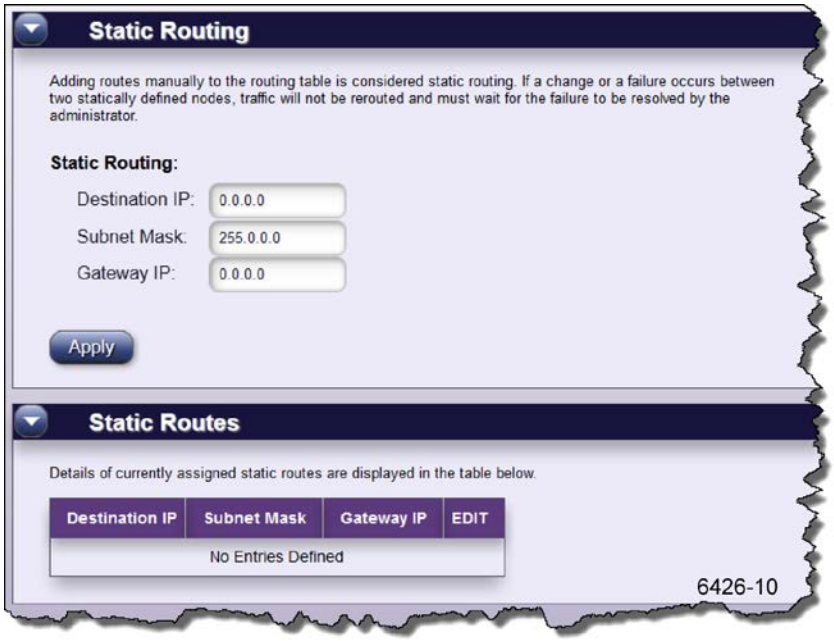
Dynamic DNS associates the WAN IP address of your router with a host name. Dynamic DNS automatically updates DNS servers upon WAN IP address change. Dynamic DNS (DDNS) is provided through www.dyndns.com.



Advanced - IP Addressing - Dynamic DNS Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
Dynamic DNS state	Select "Enabled" or "Disabled" Dynamic DNS state If DDNS is set to Disabled, the credential options are not displayed.	Radio Button	Yes	Enabled or Disabled ‡
Credentials for www.dyndns.com				
Username	Enter "Username" in field to access data base that associates WAN IP address of RSG with a host name	Alpha-numeric Text	Yes	AlphaNumeric Default: Null
Password	Enter "Password" in field to access data base that associates WAN IP address of RSG with a host name	Alpha-numeric Text	Yes	AlphaNumeric Default: Null
Show	Show the password	Radio Button	Yes	If selected, actual password is displayed. If not checked, password is masked (all "bullets") Default: Values are masked
Dynamic DNS hostname	Enter the DNS host name. The dynamic DNS service will automatically update DNS servers with any WAN IP address change to the RSG	Alpha-numeric Text	Yes	AlphaNumeric Default: Null
Apply	"Apply" radio button applies and saves the "Dynamic DNS host name"	Action Button	Yes	Apply and Save Dynamic DNS security information

Static Routing

Adding routes manually to the routing table is considered static routing. If a change or a failure occurs between two statically defined nodes, traffic will not be rerouted and must wait for the failure to be resolved by the administrator. A list of assigned static routes is also provided.



Advanced - Routing - Static Routing Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
Destination IP	Manually add the IP address of a connected device to the gateway routing table	Numeric	Yes	Dot delimited xx.xx.xx.xx Default: 0.0.0.0
Subnet Mask	Manually add the Subnet Mask of the connected device to the gateway routing table	Numeric	Yes	Dot delimited xx.xx.xx.xx Default: 255.0.0.0
Gateway IP	Manually add the Gateway IP address to the gateway routing table	Numeric	Yes	Dot delimited xx.xx.xx.xx Default: 0.0.0.0
Apply	"Apply" radio button applies and saves the "Static Routing" settings	Action Button	Yes	Click to apply and save changes.
Static Routes				
Destination IP	IP address of connected device	Info Only	No	Dot delimited xx.xx.xx.xx Default: 0.0.0.0
Subnet Mask	Subnet Mask of connected device	Info Only	No	Dot delimited xx.xx.xx.xx
Gateway IP	Gateway IP address	Info Only	No	Dot delimited xx.xx.xx.xx Default: 0.0.0.0
Edit (Remove)	Remove selected static route from routing table	Action Button	No	Click Remove to discard static route

Quality of Service Overview

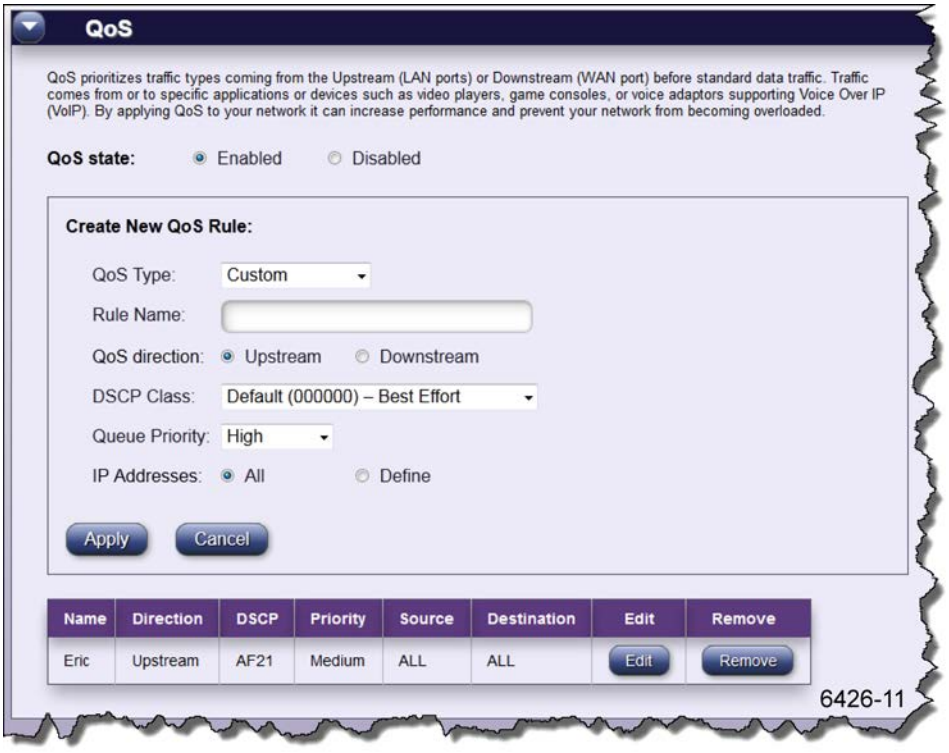
Quality of Service settings allow for the configuration of QoS prioritization rules across the network.

Note: Features listed below can be customized under the Advanced > Quality of Service tab of the EWI.

QoS - Quality of Service helps prioritize LAN to WAN packet movement in and out of a router. Options exist for classifying traffic type (video, voip, custom), traffic direction (upstream or down), and DSCP class. Can be applied to all traffic of a given type or only traffic from a given IPv4 or IPv6 address.

QoS (IPv4)

QoS prioritizes traffic types coming from the Upstream (LAN ports) or Downstream (WAN port) before standard data traffic. Traffic comes from or to specific applications or devices such as video players, game consoles, or voice adaptors supporting Voice over IP (VoIP). By applying QoS to your network it can increase performance and prevent your network from becoming overloaded.



Advanced- Quality of Service - QoS Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
QoS State	Sets the "Enabled" or "Disabled" state for prioritizing the Quality of Service	Radio Button	Yes	"Enabled" ‡ or "Disabled"
New	"New" radio button for creating a QoS rule	Radio Button	Yes	Create a new rule
Create New QoS Rule				
QoS Type	Select or create a QoS type from the pull down list: Video, VOIP, VOIP Signaling, Custom	Drop-down List	Yes	Choose Video, VOIP, VOIP Signaling, Custom‡ to create rule.
Rule Name (Custom only)	If QoS Type = Custom, then enter a name for the rule. Select or create a QoS type from the pull down list: Video, VOIP, VOIP Signaling, Custom	Alpha-numeric Text	Yes	Alpha-numeric Text Default: Null
QoS Direction	Choose whether QoS is enforced on the upstream or downstream traffic	Radio Button	Yes	Upstream ‡ or Downstream
DSCP Class (Custom only)	If QoS Type = Custom, Differentiated Services Code Point (DSCP) for coding QoS rule in IP packet to define "Class" of service	Drop-down List	Yes	Selectable options from pull down list of 7 classes of service as well as "Best Effort" ‡ and "Expedited Forwarding"
Queue Priority (Custom only)	Queue Priority of "Custom" QoS Type: High, Medium, Low, Best Effort	Drop-down List	Yes	Selectable options from pull down list of: High ‡, Medium, Low, Best Effort
IP Addresses (Custom only)	IP Addresses affected by the "QoS Rule": All or Defined	Radio Button	Yes	Choose either All IP Addresses ‡ or specific IP Addresses that need to abide by QoS Rules.
Source IP (Define Only)	Apply QoS rule to the source IP address	Info only	No	N/A
IP	Apply QoS rule to this source IP address	Numeric	Yes	Dot delimited xx.xx.xx.xx
Network Mask	Apply QoS rule to this source Netmask	Numeric	Yes	Dot delimited xx.xx.xx.xx Default: 255.255.255.0
Port Range to	Apply QoS rule to this source Port Range	(2) Numeric Fields (to-from)	Yes	Alphanumeric range, xxxx.... to xxx....
Destination IP	Apply QoS rule to the destination IP Address	Info Only	No	N/A
IP	Apply QoS rule to this destination IP Address	Numeric	Yes	Dot delimited xx.xx.xx.xx
Network Mask	Apply QoS rule to this destination Netmask	Numeric	Yes	Dot delimited xx.xx.xx.xx Default: 255.255.255.0
Port Range to	Apply QoS rule to this destination Port Range	(2) Numeric Fields (to-from)	Yes	Alphanumeric range, xxx. . . to xxx. . . Default: Null
Apply	"Apply" radio button applies and saves the "QoS Rule" settings	Radio Button	Yes	Click to apply and save changes
Cancel	"Cancel" radio button cancels the "QoS Rule" settings	Radio Button	Yes	Click to cancel QoS Rule settings

New QoS Definitions List				
Name	Name of QoS rule	Info Only	"Edit" mode only	Info Only
Direction	Data flow direction to which QoS rule is applied	Info Only	"Edit" mode only	Info Only
DSCP	Differentiated Services Code Point (DSCP) QoS class of service applied	Info Only	"Edit" mode only	Info Only
Priority	Priority of service applied	Info Only	"Edit" mode only	Info Only
Source	Source of data to which QoS rule is applied	Info Only	"Edit" mode only	Info Only
Destination	Destination of data to which QoS rule is applied	Info Only	"Edit" mode only	Info Only
Edit	Edit this QoS rule	Radio Button	Yes	Click Edit to change QoS Rule settings
Remove	Remove this QoS rule	Radio Button	Yes	Click Remove to discard this QoS Rule

Security Overview

The Calix GigaCenter incorporates various features that ensure overall network security.

Note: Features listed below can be customized under the Advanced > Security tab of the EWI.

- **Administrator Credentials** - Administrator credentials prevent outsiders from accessing the gateway device's firmware settings.
- **Application Forwarding** - The Application Forwarding feature allows a LAN device to receive incoming WAN traffic on a "per-application" basis. All traffic into the device associated with a given application is forwarded to the defined device. Associations are made between an application and a device name (or IP Address).
- **Port Forwarding** - Similar to Application Forwarding, Port Forwarding allows a LAN device to received traffic on a port range basis. Traffic from a specific local port (or range of ports) and a specific remote port (or range) are specified.
- **Firewall** - The Firewall blocks incoming IPv4 or IPv6 traffic based on the level of security desired. Pre-programmed services can be manipulated to allow or ban incoming or outgoing traffic based on the security level chosen.
- **DMZ Hosting** - Digital Media Zone Hosting allows for the placement of any LAN device outside the firewall. Since this device, by definition, is now being hosted elsewhere, it can now be accessed using the WAN IP address (Connection Status page).
- **UPnP** - UPnP (Universal Plug and Play) capable devices simplify the connection and implementation of devices into your network.

Administrator Credentials

Administrator credentials prevent outsiders from accessing the gateway device's firmware settings. After creating a username and password, you will need to enter them before you can access the gateway device's configuration settings.

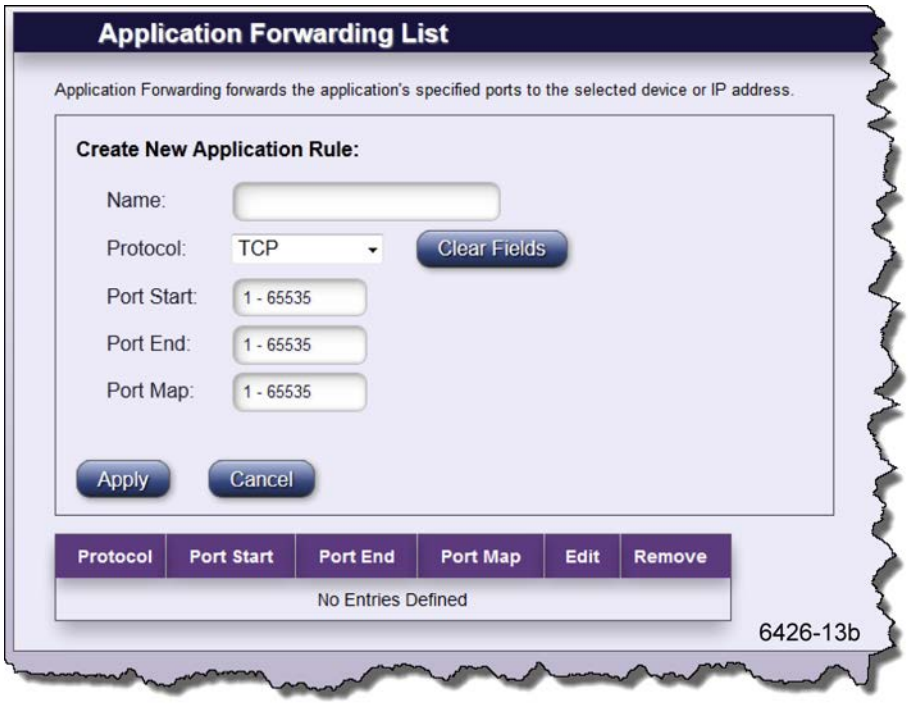
Advanced- Security - Administrator Credentials Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
Credentials	Determines whether credentials are required to gain access to the gateway device's configuration settings	Radio Button	Yes	Required ‡ or Not Required Note: If Not Required is chosen, Login and Password fields are not displayed
Administrator - Login	If credentials are required, the login name is entered here.	Alpha-numeric Text	Yes	See the topic entitled Passwords for a list of allowable characters Default: *admin*
Administrator - Password	If credentials are required, the password is entered here.	Alpha-numeric Text	Yes	See the topic entitled Passwords for a list of allowable characters. Default: See label shipped with GigaCenter
Show	When checkbox is checked, displays the un-masked password	Checkbox	Yes	When unchecked, the password is not displayed (masked with a string of bullets)
Apply	Click to apply and save login and password	Action Button	Yes	Click to apply and save changes

Application Forwarding

Application Forwarding forwards the application's specified ports to the selected device or IP address. The subscriber can forward traffic from the WAN source to a local LAN device on a per-port basis.

Advanced- Security - Applications Forwarding List Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
Create New Association - Application	Create a new association between an application's specified port and a device or IP address. Applications are defined using the New Association radio button to the right.	Drop-down List	Yes	Choose from a previously defined application from the drop-down list. If none exists, create one using the *New* radio button. To view previously created associations, click the *View* radio button. Default: Null
View	This button allows the application rules for the selected application to be viewed	Radio Button	Yes	View Radio Button (see description above)
New	This button allows a new application rule to be created	Radio Button	Yes	New Radio Button (see description above)
Application Forwarding List				
Device Name	Name of device to be associated with an application	Info Only	No	Listing device name
IP Address	Name of IP address to be associated with an application	Info Only	No	IP Address of device to be forwarded
Application Forwarded	Name of application being forwarded to device or IP address	Info Only	No	Application name being forwarded
Remove	Eliminate the application forwarding association	Action Button	Yes	Click Remove to discard application forwarding rule

Upon clicking the New radio button described above, the Create New application Rule screen is displayed:



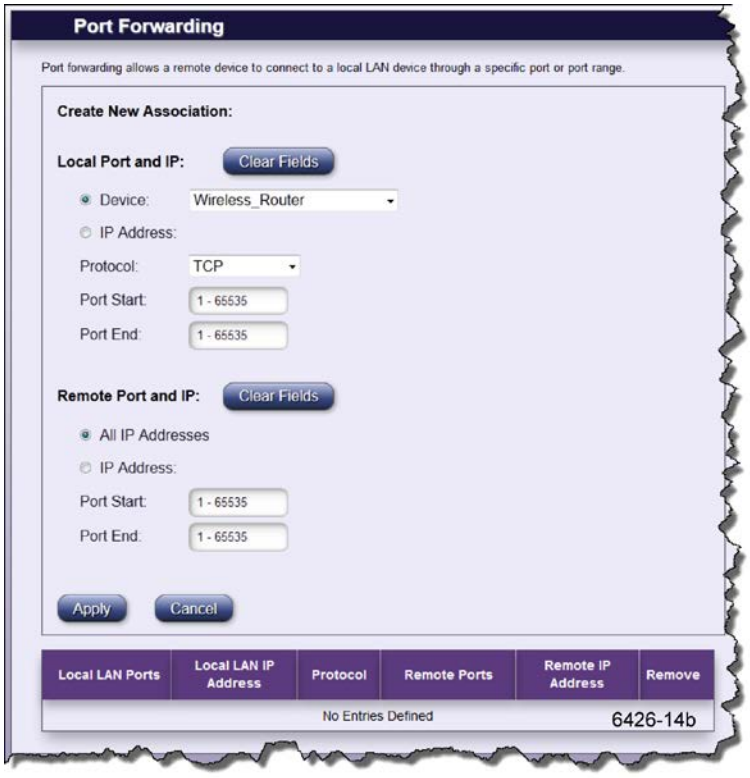
Advanced- Security - Create New Application Rule Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
Name	Assign a name to the new application rule	Alpha-numeric Text	Yes	Alpha-numeric text Default: Null
Protocol	Protocol used for application forwarding	Drop-down List	Yes	TCP ‡ , UDP, TCP/UDP
Clear Fields	This button clears the fields to allow a new rule to be created	Radio Button	Yes	Clear all fields to allow entry of new rule
Port Start	Enter the number of the application's specified start port	Numeric	Yes	Numerals from 1 to 65535 Default: Null
Port End	Enter the number of the application's specified end port	Numeric	Yes	Numerals from 1 to 65535 Default: Null
Port Map	Enter the number of the application's specified port map	Radio Button	Yes	Numerals from 1 to 65535 Default: Null
Apply/Cancel	"Apply" radio button applies and saves the "Create New Application Rule" settings or "Cancel" radio button cancels the "Create New Application Rule" settings	Action Button	Yes	Choose Apply to apply and save changes. Click Cancel to discard changes

Advanced - Security - Application Rule List				
Protocol	Protocol used for application forwarding	Info Only	No unless in edit mode	Info Only
Port Start	The number of the application's specified start port	Info Only	No unless in edit mode	Info Only
Port End	The number of the application's specified end port	Info Only	No unless in edit mode	Info Only
Port Map	The number of the application's specified port map	Info Only	No unless in edit mode	Info Only
Edit	Edit the application rule	Radio Button	Yes	Click radio button to edit the rule
Remove	Eliminate the application rule	Radio Button	Yes	Click radio button to remove rule
Associate Application With	Associate an application with a device or IP address	Info Only	N/A	N/A
Device	Select "Device" button to reveal a pull down list of defined devices for association with an application	"Device" button for selecting category and pull down list for selecting device	Selectable button and selectable pull down list	"Device" button and alphanumeric selectable pull down list Default: "Device" button Default: Wireless_Router
IP Address	Select "IP Address" to reveal a field to enter an IP address for association with an application	"IP Address" button for selecting category and numeric field for entering IP address	Selectable button and editable numeric field	"IP Address" button and a dot delimited numeric entry field Default: 0.0.0.0
Apply	"Apply" radio button applies and saves the "Create New Association" settings	Radio Button	Yes	Apply and Save the Application Rule
Cancel	"Cancel" radio button cancels the "Create New Association" settings	Radio Button	Yes	Cancel changes to the Application Rule

Port Forwarding

Port forwarding allows a remote device to connect to a local LAN device through a specific port or port range. Subscribers can forward traffic from the WAN source to a local LAN device based on a port or range of port addresses.

Advanced- Security - Port Forwarding Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
New	Create a new association between a remote device and a local LAN device through a specified port or port range	Radio Button	Yes	Click to create a new port association
Port Forwarding Rules List				
Local LAN Ports	Number or range of numbers for the local LAN port	Info Only	No	N/A
Local LAN IP Address	IP address of the local device	Info Only	No	N/A
Protocol	Protocol used to connect between local and remote devices	Info Only	No	N/A
Remote Ports	Number or range of numbers for remote port	Info Only	No	N/A
Remote IP Address	Remote IP address or all IP addresses associated with the remote port	Info only	No	N/A
Remove	Remove the port forwarding association	Radio Button	Yes	Click Remove to discard the association



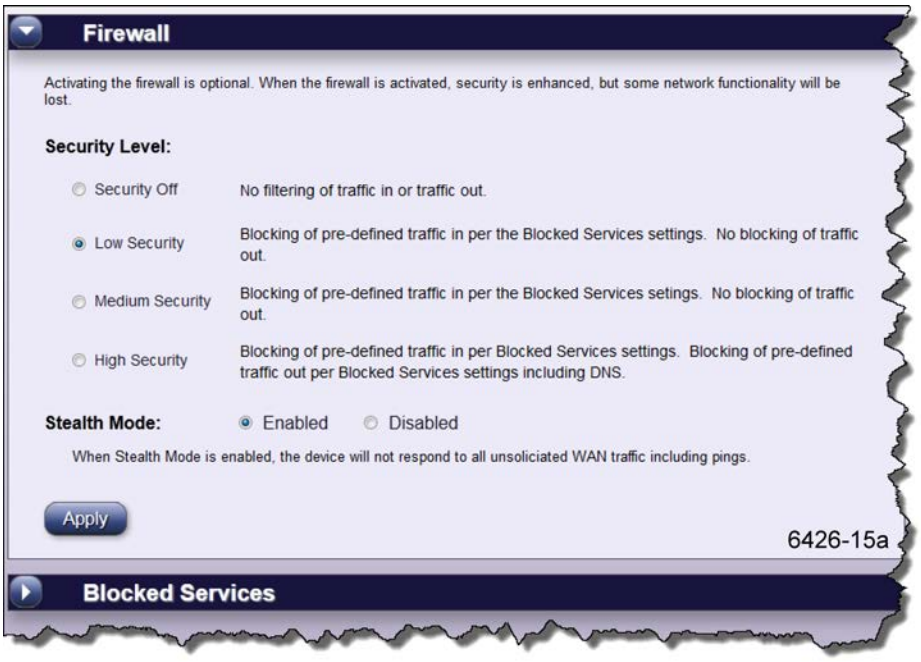
Advanced- Security - Create New Association Port Forwarding Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
Local Port and IP				
Clear Fields	Clears the Local Port and IP fields to allow a new association to be created	Action Button	Yes	Click to clear previously entered data
Device	Select the local LAN device to be connected to the remote device.	"Device" button with a drop-down list of devices	Yes	Radio button with drop-down list of currently connected local devices. Default: Device is selected but drop-down list is blank until devices are added.
IP Address	Select "IP Address" to display a field to enter an IP address for association with the local device	Radio Button with numeric IP Address field	Yes	Click to enter IP Address (dot delimited xx.xx.xx.xx) Default: Not selected
Protocol	Protocol used to connect between local and remote devices	Drop-down list	Yes	TCP, UDP, TCP/UDP Default: TCP
Port Start	Enter the number of the local port association's specified start port	Numeric	Yes	1-65535 Default: Null
Port End	Enter the number of the local port association's specified end port	Numeric	Yes	1-65535 Default: Null

Remote Port and IP				
Clear Fields	Clears the Remote Port and IP fields to allow a new association to be created	Action Button	Yes	Click to clear previously entered data
All IP Addresses	Select "All IP Addresses" to associate all remote IP addresses with a specified port or range of ports	Radio Button	Yes	Choose between associating all IP addresses or a specific IP address for creating a port forwarding rule (association) Default: Selected
IP Address	Select "IP Address" to display a field to enter an IP address for association with the local device	Radio Button with numeric IP Address field	Yes	Click radio button to enter an IP address (dot delimited xx.xx.xx.xx) Default: Not Selected
Port Start	Enter the number of the remote port association's specified start port	Numeric	Yes	1-65535 Default: Null
Port End	Enter the number of the remote port association's specified end port	Numeric	Yes	1-65535 Default: Null
Apply/Cancel	"Apply" radio button applies and saves the "Create New Association" settings or "Cancel" radio button cancels the "Create New Association" settings	Action Buttons	Yes	Click Apply to apply and save changes. Click Cancel to remove port association.

Firewall

Activating the firewall is optional. When the firewall is activated, security is enhanced, but some network functionality will be lost.

Note: For additional information on system security settings, refer to the topic entitled *System Security* (on page **Error! Bookmark not defined.**) presented earlier in this guide.

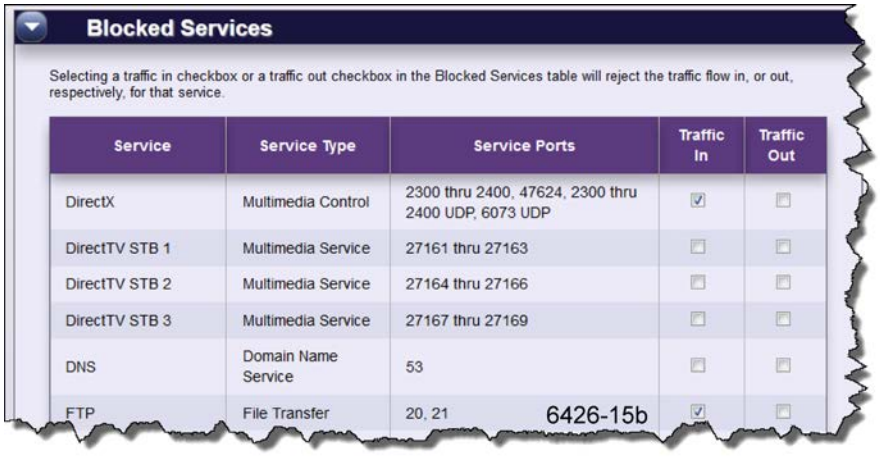


Advanced- Security - Firewall Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
Security Level				
Security Off	No filtering of incoming or outgoing traffic	Radio Button	Yes	Turn security off Default: Selected (Security Off)
Low Security	Block pre-defined traffic in per the "Blocked Services" settings. No blocking of outgoing traffic	Radio Button	Yes	Apply Low Security Settings Default: Not Selected
Medium Security	Block pre-defined traffic in per the "Blocked Services" settings. No blocking of outgoing traffic	Radio Button	Yes	Apply Medium Security Settings Default: Not Selected
High Security	Block pre-defined traffic in per the "Blocked Services" settings. Block pre-defined traffic out per the "Blocked Services" settings including DNS	Radio Button	Yes	Apply High Security Settings Default: Not Selected
Stealth Mode				
Stealth Mode	With "Stealth Mode" enabled, the GigaCenter device will not respond to all unsolicited WAN traffic including pings	Radio Button	Yes	Enable or Disable Stealth Mode Default: Disabled
Apply	"Apply" radio button applies and saves the "Firewall" settings	Action Button	Yes	Click Apply to apply and save security settings.

If the security level above is set to Low, Medium, or High, the following table is displayed.

Note: Depending on the security level chosen, blocked services will change as it pertains to traffic in, traffic out, and ports affected.

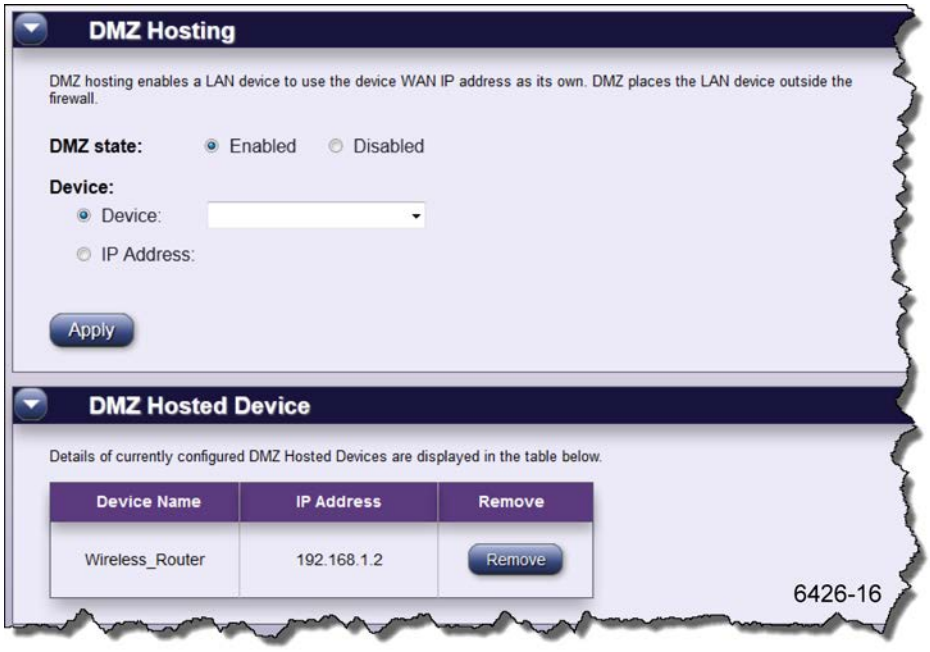
Note: Blocked Services are disabled and are not displayed when the firewall security level is set to off.



Advanced- Security - Firewall Blocked Services Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
Service	Name of service that is set up for blocking	Info Only	No	N/A
Service Type	Service Type Name that is set up for blocking	Info Only	No	N/A
Service Ports	Defined service ports that are set up for blocking	Info Only	No	N/A
Traffic In	Select whether you want downstream traffic to be blocked	Checkbox	Yes	Click the checkbox to enforce incoming traffic blocking Default: Not blocked
Traffic Out	Select whether you want upstream traffic to be blocked	Checkbox	Yes	Click the checkbox to enforce outgoing traffic blocking Default: Not blocked

DMZ Hosting

DMZ hosting enables a LAN device to use the device WAN IP address as its own. DMZ places the LAN device outside the firewall.

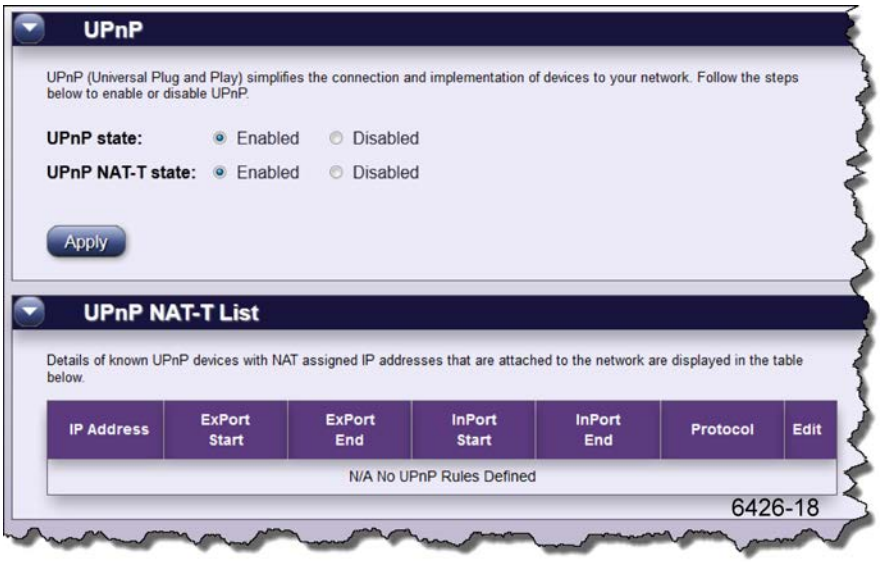


Advanced- Security - DMZ Hosting Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
DMZ State	Enable or Disable DMZ hosting	Radio Button	Yes	Select Enable or Disable Default: Disabled
Device (If DMZ = Enabled)	Select the LAN device to be hosted outside the firewall	Radio Button with Drop-down list of Device names	Yes	Device Default: Not Selected Drop-down list is alpha-numeric Default: Null field
IP Addressed (If DMZ = Enabled)	Select an IP address of a device to be hosted outside the firewall	Radio button with numeric field for IP address	Yes	Default: IP Address radio button is selected IP address numeric field (dot delimited xx.xx.xx.xx) Default: Null field
Apply	Apply button applies and saves the DMZ Host settings	Action Button	Yes	Apply to apply and save changes
DMZ Hosted Device Listing				
Device Name	Name of currently configured DMZ Hosted device	Info only	No	N/A
IP Address	IP address of the device	Info only	No	N/A
Remove	Remove the associated device name and IP address from the DMZ Hosted list	Action Button	Yes	Removes the device from the DMZ list - the listed device will return to being hosted inside the DMZ.

UPnP

Universal Plug n Play is a network protocol whose general purpose is to enable zero-configuration, automatic discovery, and simple configuration of network services on a LAN. It was developed in 1998 by a consortium led by Microsoft. It allows devices to join a network, obtain an IP address, announce itself and its services, and learn about the presence and availability of other UPnP devices and services. UPnP devices are divided into 2 categories: Control Points (CP's) and Controlled Devices (CD's).

The most common use cases at present time are for printer discovery and installation, media server/player discovery and control, and Internet router control. UPnP can allow PC's to discover and automatically identify and install drivers for network accessible printers. It allows network media players such as DLNA clients to automatically locate DLNA servers on the LAN. Internet routers can be discovered and various elements of control can be exerted upon them. Each of these functionalities is governed by a particular schema that fits within the UPnP protocol and those schemas are defined by individual UPnP Working Groups.



Advanced- Security - UPnP Field Definitions				
Label	**Definition**	**Field Type**	**Editable ?**	**Allowable Values/Defaults**
UPnP state	Universal Plug and Play (UPnP) can be enabled or disabled by selecting the appropriate buttons	Radio Button	Yes	Enabled ‡ or Disabled
UPnP NAT-T state	When "Enabled" the UPnP Network Address Translator (NAT-T) masks the IP addresses of devices on the LAN behind the Home Gateway	Radio Button	Yes	Enabled ‡ or Disabled
Apply	Applies and saves the UPnP settings	Action Button	Yes	Apply and save changes

UPnP NAT-T List				
IP Address	The NAT assigned IP addresses of UPnP devices masked behind the Home Gateway	Info Only	No	N/A
ExPort Start	Displays the starting port number for the external device that you want to allow access	Info Only	No	N/A
ExPort End	Displays the ending port number for the external device that you want to allow access	Info Only	No	N/A
InPort Start	Displays the starting port number for the internal device that you want to allow access	Info Only	No	N/A
InPort End	Displays the ending port number for the internal device that you want to allow access	Info Only	No	N/A
Protocol	Protocol being used to connect the external and internal devices via UPnP	Info Only	No	N/A
Edit	Edit the UPnP NAT-T list	Action Button	Yes	Select the Edit Button

Remote Management Overview

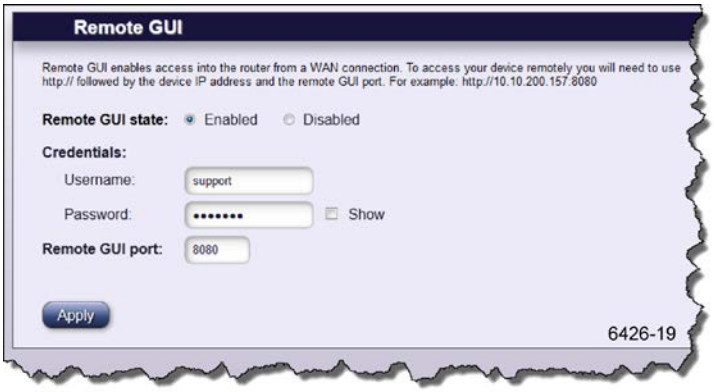
Remote Management settings allow for the configuration of a secure connection to the GigaCenter network from a remote location.

Note: Features listed below can be customized under the Advanced > Remote Management tab of the EWI.

Remote EWI - Provides added security when accessing the GigaCenter EWI from a remote location.

Remote EWI

Remote EWI enables access into the router from a WAN connection. To access your device remotely you will need to use http:// followed by the device IP address and the remote EWI port. For example: http://10.10.200.157:8080



Advanced - Remote Management - Remote EWI Field Definitions				
Label	**Definition**	**Field Type**	**Editable?**	**Allowable Values/Defaults**
Remote EWI state	When "Enabled" the feature provides remote EWI access to the router from a WAN connection	Radio Button	Yes	Select Enable or Disable Default: Disabled
Credentials				
Username	User name used to remotely access the Home Gateway's EWI	Alpha-numeric text	Yes	Alphanumeric string Default: Null field
Password	Password used to remotely access the EWI	Alpha-numeric text	Yes	Alpha-numeric string Default: Null field
Show	Selecting this option displays the password (not masked)	Checkbox	Yes	Check box Default: Not checked
Remote EWI port	Port on the Home Gateway for remote EWI access	Numeric	Yes	Numeric string Default: 8080
Apply	Applies and saves the Remote EWI security settings	Action Button	Yes	Click to apply and save changes

Appendix A

Appendix

Wi-Fi Protected Set-up LED Behavior

Depending on the services being configured, the WPS button and associated WPS LED will react differently.

For data services, WPS is enabled upon pressing the WPS a single time. The WPS LED begins to flash (green) and continues to do so for up to 180 seconds. During this time, other Wi-Fi capable devices can be paired to the GigaCenters Wi-Fi radios (either the 2.4 GHz or the 5.0 GHz band) by initializing a similar WPS function on the remote device, thereby creating an association with the primary SSID of the GigaCenter and the other device. WPS LED behavior for pairing to the primary SSID (either 2.4 GHz or 5.0 GHz) is as follows:

- Press WPS button a single time.
- WPS LED illuminates green and flashes for up to 120 seconds.
- Wi-Fi 5.0 GHz LED begins flashing after approximately 10 seconds indicating the pairing process has begun.
- If another device is found, the GigaCenter pairs with the device, the Wi-Fi 5.0 GHz LED remains on continuously, and the WPS LED goes out.
- If no device is found, the WPS LED turns red after the initial 120 second time-out and remains red for another 120 seconds.

For IPTV services, WPS is enabled upon pressing the WPS three times in approximately 1 second intervals. After a short delay, the WPS LED begins to flash (amber) and continues to do so for up to 180 seconds. During this time, other Wi-Fi capable devices can be paired to the GigaCenters 5 GHz Wi-Fi radio by initializing a similar WPS function on the remote device, thereby creating an association with the reserved IPTV SSID (5GHz_IPTV_SSID) of the GigaCenter and the other device. WPS LED behavior for pairing to the IPTV SSID (5.0 GHz) is as follows:

- Press WPS button exactly three times, at one second intervals. WPS LED turns green and begins flashing after the 3rd press.
- WPS LED illuminates amber after approximately 10 seconds and flashes for up to 120 seconds. The GigaCenter has entered IPTV SSID pairing mode.
- If another device is found, the GigaCenter pairs with the device and the WPS LED turns green and remains on for approximately 120 seconds.
- If no device is found, the LED turns red after the 120 second time-out and remains red for 120 seconds.

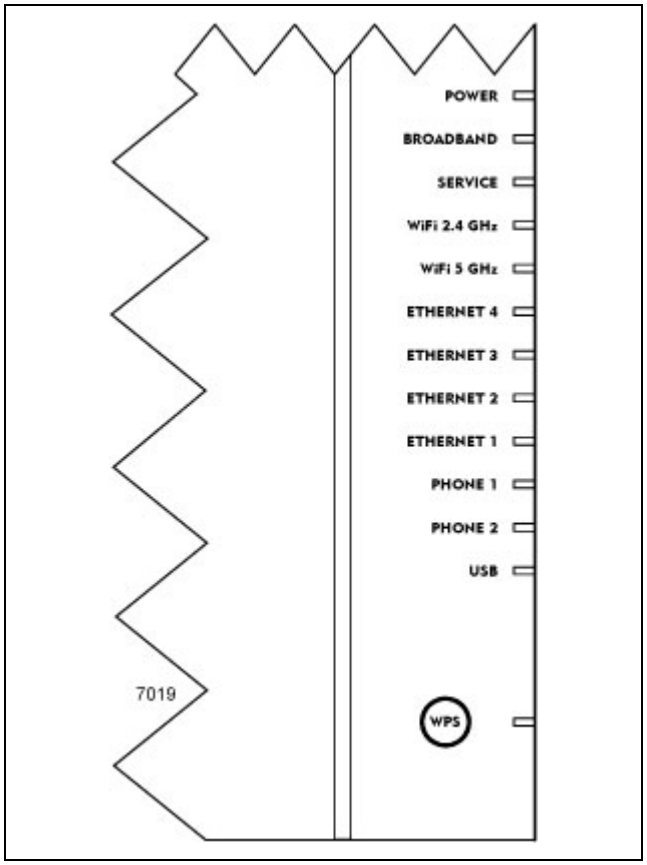
GigaCenter LED Behavior

Before leaving the site, verify that the GigaCenter is communicating with the GPON network. Viewing the LEDs helps the installer determine the exact state of the device.

A properly installed and functional GigaCenter exhibits the following LED behavior:

- When power is initially applied, the power LED behaves differently based on the state/status of the UPS:
  - If no UPS is present or if a UPS is present and is not currently providing primary power, the power LED illuminates and remains lit.
  - If a UPS is present and a battery alarm condition exists, the power LED blinks to indicate an alarm status.
  - If LED does not light, power is off or the UPS power supply is not functional.
- During initial power-up, all remaining LED's come on momentarily (lamp test).
- If the SC-APC pigtail is not connected, the Phone 1 LED will begin to blink when Voice Smart Activate is activated.
- If the SC-APC pigtail is connected, the Broadband LED begins flashing once downstream synchronization has been completed. The LED switches to solid green if the GigaCenter has been provisioned.
- As Ethernet ports are initialized, the corresponding LED illuminates provided an Ethernet device is connected to the port.

Note: Phone service is not available until the Broadband LED lights and remains on.



Note: The integrated WPS feature allows for the sync'ing of remote WIFI capable products with the GigaCenter. When in WPS mode (pressing the WPS button), the WIFI LED blinks rapidly for 120 seconds, indicating the remote device is attempting to pair with the GigaCenter.

Note: By default, the Wi-Fi radio is disabled upon start-up. Once initialized (via graphical user interface), the Wi-Fi LED assumes normal functionality).

LED States and Status

The LED's located on the face of the GigaCenter provide information on the status and current state of the device.

LED States and Status			
LED NAME	**ON**	**OFF**	**BLINK**
POWER	Main AC power (either power adapter or UPS) is present at the ONT/RSG.	No power present (AC power or battery back-up).	ONT/RSG is on battery and the battery remains in a fully functional state.
BROADBAND	Broadband physical connection has been established. GigaCenter has ranged with GPON network.	Broadband interface is not powered - no signal detected.	When WAN is active, broadband interface has detected a carrier signal. LED blinks at 50% duty cycle when optical light is detected and the GigaCenter is in ranging mode.
SERVICE	**See table below for specific behaviors**		
WiFi 2.4 GHZ **WiFi 5 GHz**	Wi-Fi is enabled.	Wi-Fi is disabled.	N/A
ETHERNET 4 through ETHERNET 1	A powered device is connected to the port.	The GigaCenter is not powered, cable is not attached, or no powered device is connected to the port.	Activity is present on associated device - downstream traffic present. Rate of blink loosely translates to the amount of packets being transported.
PHONE 1 **PHONE 2**	At least one POTS port is off hook.	Zero POTS ports are in service (off hook)	Smart Activate or Voice Activate is in process.
USB	A device is connected, and associated with the USB port however the port is currently idle.	The device is not powered, no cable connected, or no powered devices connected to the port.	Activity is present on the USB port. Rate of blink loosely translates to the amount of packets being transported.
RF **Model 854-1 AND 854-2 only**	RF video optical level is within prescribed AGC range.	RF Video optical level is outside prescribed range (too low) or no signal is present.	N/A
WPS	GREEN: On for three minutes or until WPS button is pressed again. RED: On for two minutes. An error has occurred unrelated to security such as no partner found, protocol aborted. Press WPS button again to restart. WPS function.	The device is not currently in WPS mode and is waiting for the next authentication attempt.	GREEN: The Wi-Fi protected setup PBC procedure is in progress. RED: Session overlap detected (security risk). Wait for 2 minutes, then press WPS button again to restart. If error persists, refer to PIN-based configuration method.

Service LED States and Status			
LED Appearance	**Bridged Mode**	**RG Mode**	**Mixed Mode**
OFF*	No Ethernet port has been provisioned	No IP address has been received or PPPoE session authentication has not occurred.	N/A
Solid GREEN (Indicates internet service)	At least one Ethernet port has been provisioned.	The GigaCenter has received an IP addressed or a PPPoE session authentication (with credentials) has been completed.	Same as RG Mode
Solid RED	N/A	GigaCenter attempted to connect via IP and failed (DHCP/PPPoE response or authentication failed)	Same as RG Mode
* For all modes, the Service Gateway is not powered and a physical broadband connection has not been detected.			

Acronyms

Acronyms			
ACS	Auto Configuration Server	AE	Active Ethernet
AGC	Automatic Gain Control	ALG	Application Level Gateway
AP	Access Point	CC	Closed Caption
CLI	Command Line Interface	CoS	Class of Service
CMS	Calix Management System	DDNS	Dynamic Domain Name Service (System)
DFS	Dynamic Frequency Selection	DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service (System)	DSCP	Differentiated Services Code Point
ESAP	Ethernet Service Access Platform	EWI	Embedded Web Interface
FB	Full Bridge	FTP	File Transfer Protocol
FXS	Foreign Exchange Service	GE	Gigabit Ethernet
HB	Half Bridge	HSI	High Speed Internet
IGMP	Internet Group Management Protocol	IP	Internet Protocol
IP SRV	IP Source Verify	IPoE	Internet Protocol over Ethernet
IPTV	Internet Protocol Television	ISP	Internet Service Provider
LAN	Local Area Network	MACFF	Media Access Controller Forced Forwarding
MDU	Multiple Dwelling Unit	MEF	Metro Ethernet Forum
MVR	Multicast VLAN Registration	MIMO	Multiple-Input_Multiple_Output
MMR	Microsoft Media Room	NAT	Network Address Translation
NFV	Network Functions Virtualization	NTP	Network Time Protocol

Acronyms			
OMCI	ONT Management Control Interface	ONT	Optical Network Terminal
ONU	Optical Network Unit	OOB	Out-of-Band
PBC	Push Button Control	PHY	Physical Layer Protocol
PPPoE	Point-to-Point over Ethernet	PWE 3	Pseudo-wire End-to-End Emulation
QoS	Quality of Service	RG	Residential Gateway
RIP	Routing Information Protocol	RONTA	Remote ONT Activation
RSG	Residential Service Gateway	SFU	Single Family Unit
SIP	Session Initiation Protocol	SISO	Single-Input-Single-Output
SSID	Service Set Identifier	STB	Set-top Box
TCP	Transport Control Protocol	TDM	Time Division Multi-plexed
TFTP	Trivial File Transfer Protocol	UNI	User Network Interface
UPnP	Universal Plug 'n Play	USB	Universal Serial Bus
VAP	Video Access Point	VM	Virtual Machine
VoIP	Voice over Internet Protocol	WAN	Wide Area Network
WEP	Wireless Encryption Protocol	WMM	Wireless Multimedia
WPA	Wireless Protected Access	WPS	Wi-Fi Protected Set-up
XML	Extensible Markup Language		