Software Defined WAN (SD-WAN)

Deployment Guide

U.S. Headquarters:

Edgewater Networks, Inc.
5225 Hellyer Ave., Suite 100
San Jose, California 95138

Phone: 408.351.7200
Fax: 408.727.6430

edgewaternetworks.com

Trademarks

Copyright

Software Export Controls

Purchaser acknowledges that these products are subject to the U.S. Export Administration Regulations (“EAR”) and that Purchaser will comply with the EAR. Purchaser expressly acknowledges that it is not located in Cuba, Iran, North Korea, Sudan or Syria. Purchaser will not export or re-export Edgewater Networks’ Product, directly or indirectly to: (i) any countries that are subject to the EAR, (ii) any known end-user who will use the Product in the design, development or production of nuclear, chemical or biological weapons, or rocket systems, space launch vehicles, and sounding rockets, or unmanned air vehicle systems, or (iii) any end-user who has been prohibited from participating in U.S. export transactions by any federal agency of the U.S. government. In addition, Purchaser is responsible for complying with any local laws in Purchaser’s jurisdiction which may impact Purchaser’s right to import, export or use Edgewater Networks’ Products.

Licensing

Use this product in accordance with the instructions in this document.

Typographical Errors

This publication could include technical inaccuracies or typographical errors, for which Edgewater Networks never can or shall be held liable. Changes are made periodically to the information herein; these changes will be incorporated in new releases of this publication. Edgewater Networks may make improvements or changes in the product or products described in this publication at any time, without prior notice.

Document Release Date:

01/18/2019

Document Revision:

Rev 1.3

Contents

About This Guide

1 SD-WAN Overview

2 Deploying SD-WAN

3 SD-WAN Configuration Settings

About This Guide

This guide provides an overview of the SD-WAN capabilities offered by Edgewater Networks and introduces its various components. It provides information about deployment of the SD-WAN feature, how to set it up in your network for the first time and configuration steps to access its functionalities. It also includes compliance and certification notices and hardware and software warranty information.

Audience

This deployment guide is intended for network administrators and network engineers whose primary function is to deploy and configure SD-WAN. An understanding of Ethernet and experience in network deployment, architecture and management is necessary to deploy SD-WAN.

Typographic Conventions

User input is displayed in **boldface** type and can represent keyboard input, mouse selections in a browser window, and buttons on the GUI, depending on the context. For example, the notation **File** > **Open...** means that you first click the **File** menu and then select **Open...** from the sub-menu in the GUI.

Command Line Interface (CLI) text is shown in `courier font`.

Note

Notes highlight information that is important or that has special interest.

Tip

Tips provide additional information that is helpful in performing a particular task but is not mandatory to perform the task.

Caution

Cautions alert you of actions or events that may cause system damage or loss of data.

Warning

Warnings alert you of actions or events that may cause bodily harm.

Document Organization

Item	Description
Chapter 1, *SD-WAN Overview*	Describes SD-WAN, its features and components.
Chapter 2, *Deploying SD-WAN*	Describes how deploy SD-WAN in your network for the first time and how to configure basic network settings for the first time.
Chapter 3, *SD-WAN Configuration Settings*	Describes the various configuration settings in the SD-WAN GUI.

Contact and Support Information

Headquarters
5225 Hellyer Ave., Suite 100
San Jose, CA 95138
(408) 351-7200
Fax: 408.727.6430

General: info@edgewaternetworks.com
Sales: sales@edgewaternetworks.com

Edgewater Networks, Inc. - Technical Assistance Center
Phone - 408.351.7200 ext. 2
support@edgewaternetworks.com

1

SD-WAN Overview

Deploying and managing traditional WAN is complex, time-consuming and expensive. In addition to being data-center dependent, the performance statistics is unsteady. SD-WAN comes as a simpler, more cost-effective alternative to traditional WAN architecture.

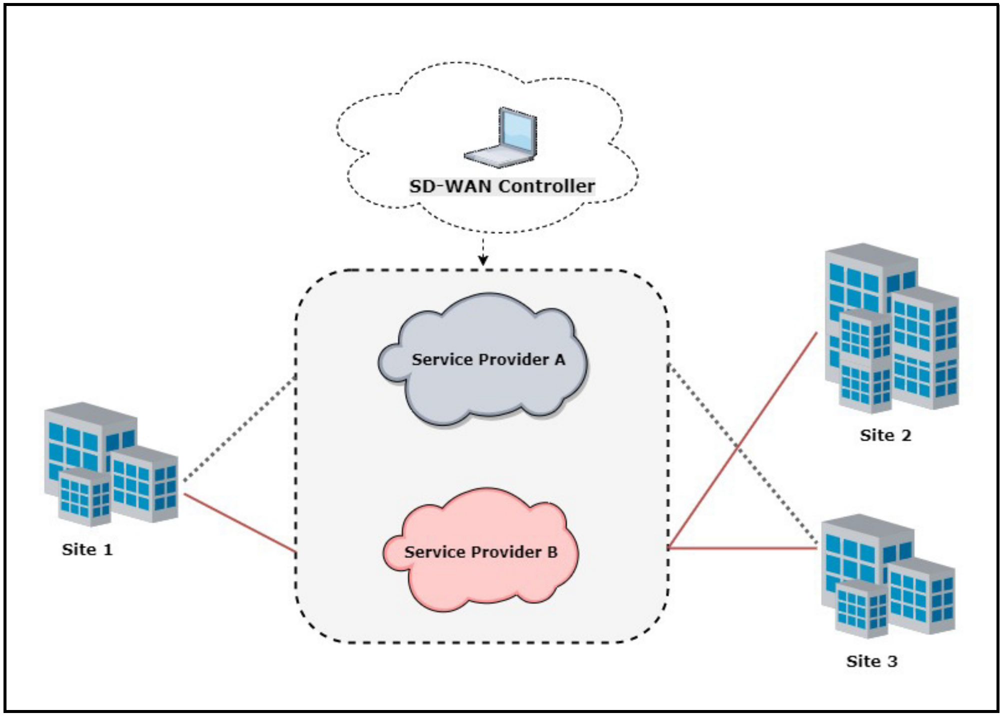
Software Defined WAN (SD-WAN) is a new networking technology that optimizes bandwidth usage, enables more efficient traffic management, and lowers operational time and cost, without compromising on security. SD-WAN simplifies WAN management by virtualizing WAN connections. The SD-WAN approach centralizes network control and moves it to the cloud, making it easier for administrators to monitor the network and to configure routers.

SD-WAN Architecture

SD-WAN enables remote configuration and centralized management of WAN networks and routers. This feature ensures real-time and prioritized traffic flow. The SD-WAN functionality offers an excellent alternative to the financially and operationally taxing traditional WAN connectivity, enabling enterprises to maximize cost-efficiency, bandwidth usage and performance. The operation of critical applications are given high priority, ensuring that they suffer no disruptions.

A simple deployment procedure will help integrate Edgewater Networks SD-WAN into enterprise networks.

Figure 1-1 Typical SD-WAN Topology



SD-WAN Licensing

The Edgewater Network SD-WAN feature requires a separate license. The SD-WAN license will only be available on a subscription basis as part of Cloud2Edge Complete. It will not be available as a perpetual license or as a subscription for perpetual licensed hardware.

For more details contact your system administrator or contact support at support@edgewaternetworks.com

2

Deploying SD-WAN

This chapter explains how to connect to the EdgeMarc and access the graphical user interface (GUI) to configure SD-WAN network settings for the first time. Refer to the *EdgeMarc User Guide* for complete details on how to configure your EdgeMarc device for your network deployment.

- Connecting to the EdgeMarc for the First Time
- Deploying and Configuring SD-WAN

This chapter also takes a look at the prerequisites to be fulfilled on the EdgeMarc to enable EdgeView control of SD-WAN.

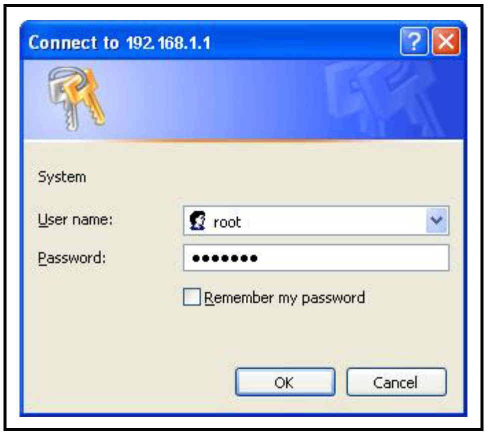
- Enabling EdgeView control of SD-WAN

Connecting to the EdgeMarc for the First Time

The LAN interface ports are pre-configured with the IP address 192.168.1.1.

1. Connect a computer to the LAN interface port (LAN Port 1) using an Ethernet cable or connect to an Ethernet switch (using the IP address 192.168.1.2 and subnet mask 255.255.255.0).
2. Launch a web browser on your computer and enter the following URL: http://192.168.1.1.
3. Press **Return**. The EdgeMarc login screen is displayed.

Figure 2-2 EdgeMarc login screen



Connect to 192.168.1.1

System

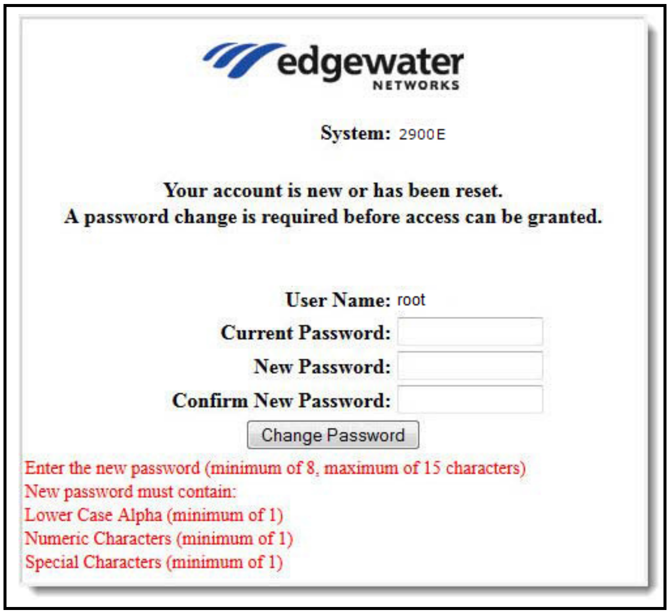
User name: root

Password: •••••••

□ Remember my password

4. Enter your initial username in the field provided: **root**
5. Enter your initial password in the field provided: **default**
6. Click **OK**.
7. After you have logged in to the system for the first time with the default credentials, you are directed to the Change Password page.

Figure 2-3 Change Password Page



System: 2900E

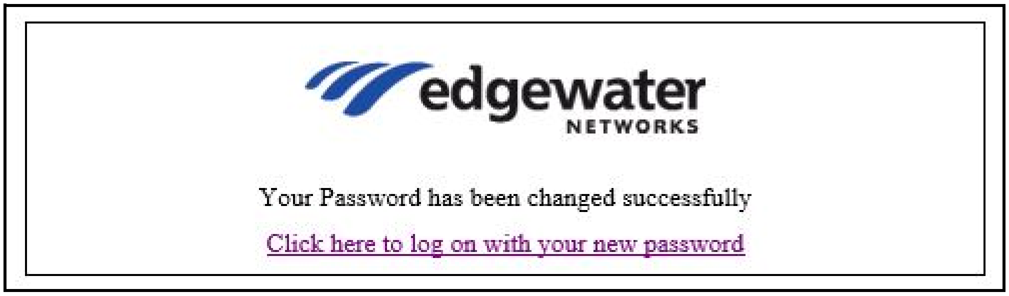
Your account is new or has been reset.
A password change is required before access can be granted.

User Name: root
Current Password:
New Password:
Confirm New Password:

Enter the new password (minimum of 8, maximum of 15 characters)
New password must contain:
Lower Case Alpha (minimum of 1)
Numeric Characters (minimum of 1)
Special Characters (minimum of 1)

8. Enter your Current and New Passwords in the Change Password Page according to the new password instructions given in the page and then click **Change Password**. The Password Change Confirmation Page will be displayed (Figure 2-4).

Figure 2-4 Password Change Confirmation Page

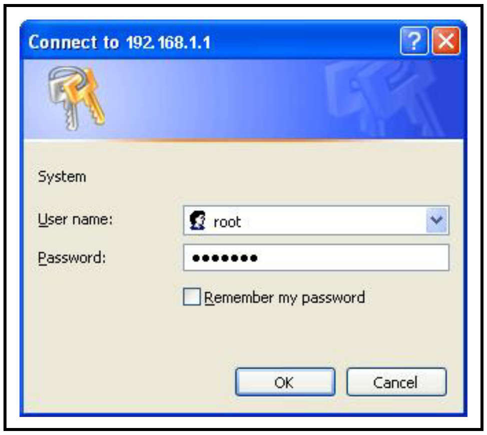


Your Password has been changed successfully

Click here to log on with your new password

9. Select **Click here to log on with your new password** from the Password Change Confirmation Page (Figure 2-4).
10. You will be navigated again to the EdgeMarc login screen (Figure 2-5). Log in to the EdgeMarc Admin landing page (Figure 2-6) with your User Name and New Password from the EdgeMarc login screen.

Figure 2-5 EdgeMarc login screen



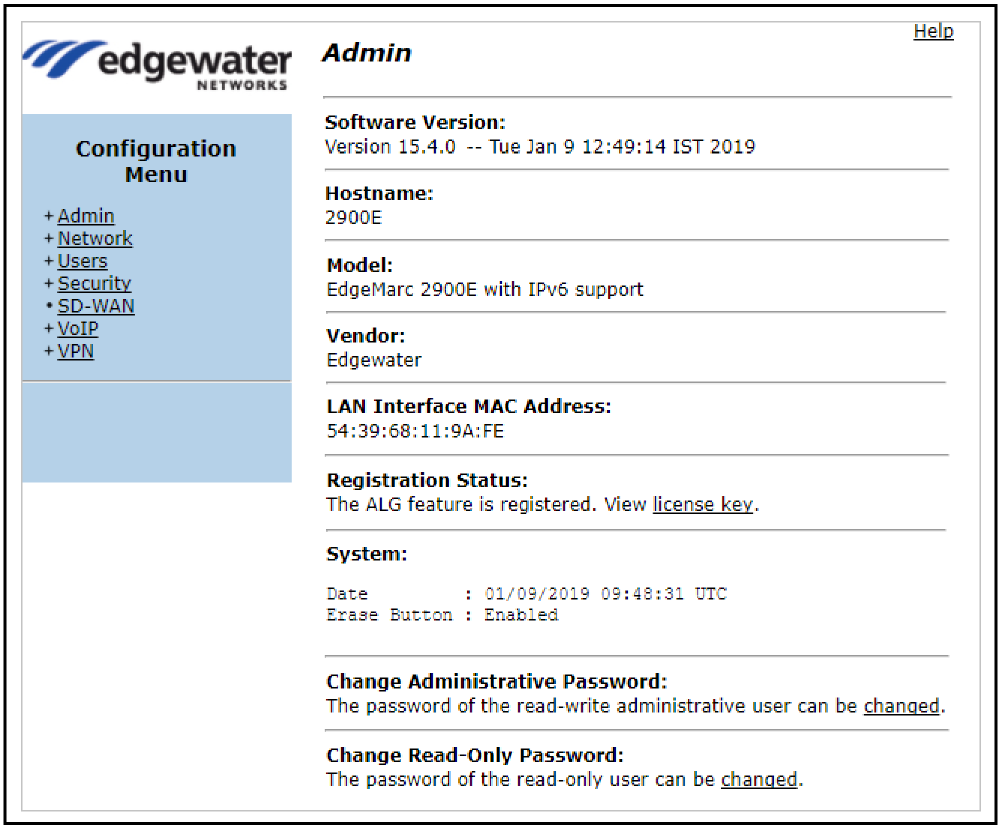
System

User name: root

Password: •••••••

☐ Remember my password

Figure 2-6 EdgeMarc Admin Landing Page



Admin

Software Version:
Version 15.4.0 -- Tue Jan 9 12:49:14 IST 2019

Hostname:
2900E

Model:
EdgeMarc 2900E with IPv6 support

Vendor:
Edgewater

LAN Interface MAC Address:
54:39:68:11:9A:FE

Registration Status:
The ALG feature is registered. View license key.

System:

```
Date         : 01/09/2019 09:48:31 UTC
Erase Button : Enabled
```

Change Administrative Password:
The password of the read-write administrative user can be changed.

Change Read-Only Password:
The password of the read-only user can be changed.

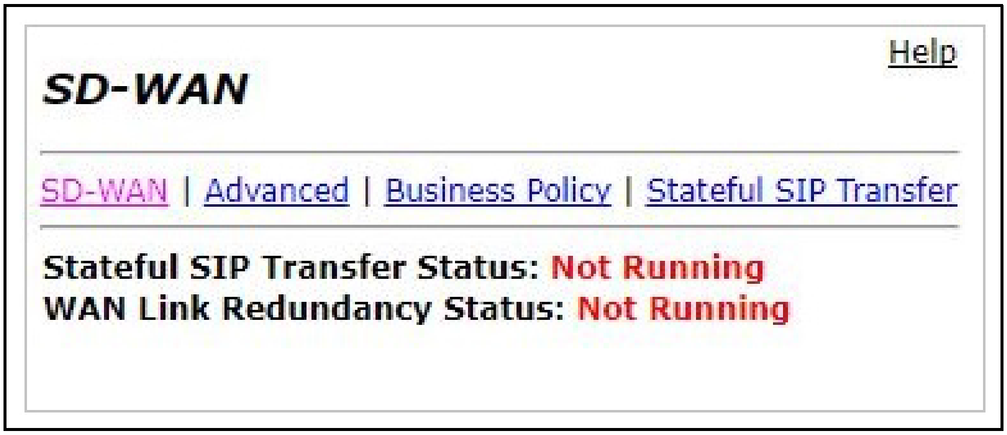
For details about how to configure and deploy the EdgeMarc device in your network, refer to the EdgeMarc online help and the *EdgeMarc VOS User Guide* available in the Edgewater Networks Knowledgebase at www.edgewaternetworks.com/kb.

Deploying and Configuring SD-WAN

To configure and deploy SD-WAN in your network for the very first time, start by selecting the **SD-WAN** option under **Configuration Menu** in the EdgeMarc GUI.

The **SD-WAN** page will be displayed. The status tab (Figure 2-7) will appear by default.

Figure 2-7 SD-WAN Status Tab



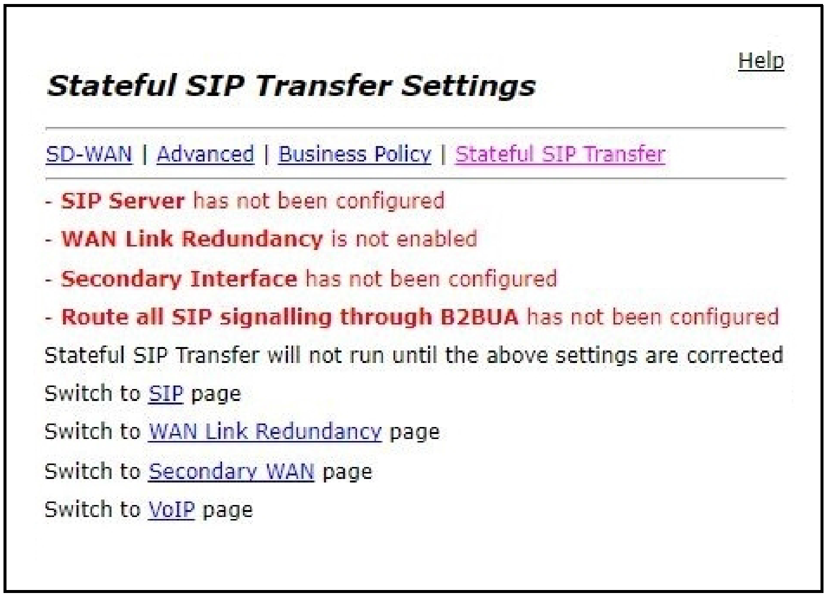
Stateful SIP Transfer Status: Not Running
WAN Link Redundancy Status: Not Running

Stateful SIP Transfer

The Stateful SIP Transfer is a feature for voice calls. This enhancement enables WAN link failover during an ongoing voice call, ensuring that the call is not disrupted during the WAN link switch. There is a seamless movement of the SIP session from one WAN link to another when primary link quality has degraded.

1. Go to the **Stateful SIP Transfer** tab (Figure 2-8) and successively configure the changes mentioned on the page, as mentioned below.

Figure 2-8 Stateful SIP Transfer Tab



Stateful SIP Transfer Settings

Help

SD-WAN | Advanced | Business Policy | Stateful SIP Transfer

- **SIP Server** has not been configured
- **WAN Link Redundancy** is not enabled
- **Secondary Interface** has not been configured
- **Route all SIP signalling through B2BUA** has not been configured

Stateful SIP Transfer will not run until the above settings are corrected

Switch to SIP page

Switch to WAN Link Redundancy page

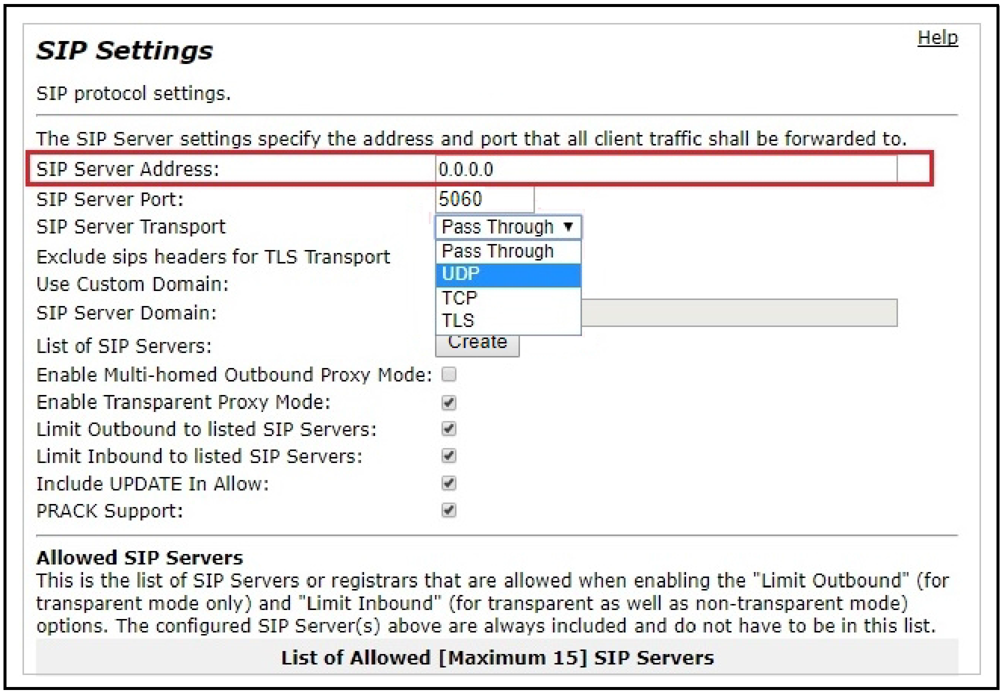
Switch to Secondary WAN page

Switch to VoIP page

- ### SIP Server Configuration

  Click the **SIP** page link on the **Stateful SIP Transfer** tab (Figure 2-8). You are navigated to the **SIP Settings** page. Here, configure the **SIP Server Address** (Figure 2-9).

Figure 2-9 SIP Settings Page



SIP Settings

Help

SIP protocol settings.

The SIP Server settings specify the address and port that all client traffic shall be forwarded to.

SIP Server Address: 0.0.0.0

SIP Server Port: 5060

SIP Server Transport: Pass Through ▾

Exclude sips headers for TLS Transport

Use Custom Domain:

SIP Server Domain:

List of SIP Servers: Create

Enable Multi-homed Outbound Proxy Mode: ☐

Enable Transparent Proxy Mode: ☑

Limit Outbound to listed SIP Servers: ☑

Limit Inbound to listed SIP Servers: ☑

Include UPDATE In Allow: ☑

PRACK Support: ☑

Allowed SIP Servers

This is the list of SIP Servers or registrars that are allowed when enabling the "Limit Outbound" (for transparent mode only) and "Limit Inbound" (for transparent as well as non-transparent mode) options. The configured SIP Server(s) above are always included and do not have to be in this list.

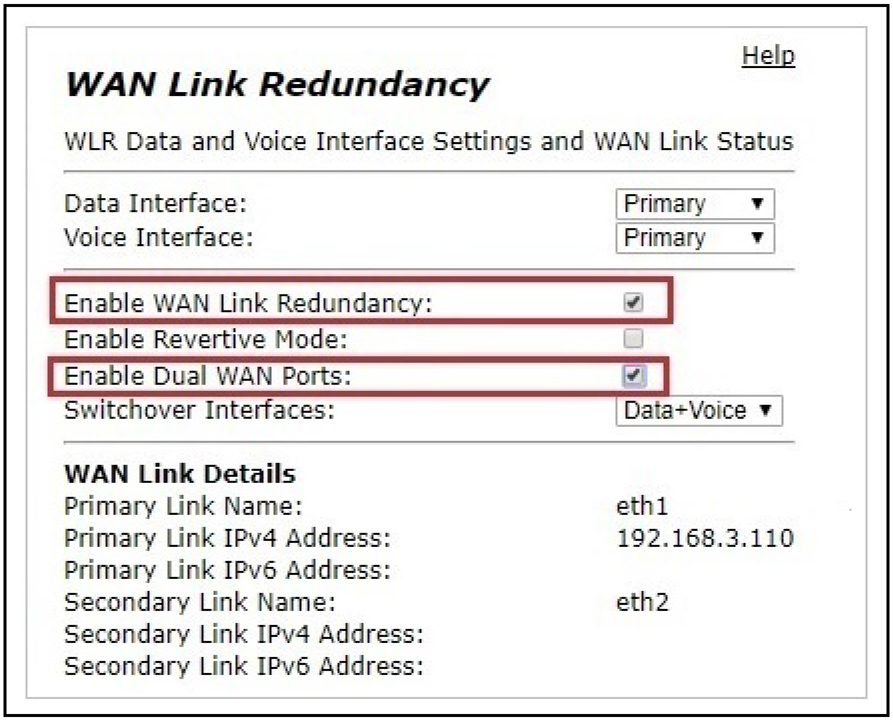
List of Allowed [Maximum 15] SIP Servers

- ### Enable WAN Link Redundancy

  Select the **WAN Link Redundancy** link on the **Stateful SIP Transfer** tab (Figure 2-8). You are directed to the **WAN Link**

Redundancy page. Enable both WAN Link Redundancy and Dual WAN Ports (Figure 2-10).

Figure 2-10 WAN Link Redundancy Page



WAN Link Redundancy

WLR Data and Voice Interface Settings and WAN Link Status

Data Interface: Primary ▼
Voice Interface: Primary ▼

Enable WAN Link Redundancy: ☑
Enable Revertive Mode: □
Enable Dual WAN Ports: ☑
Switchover Interfaces: Data+Voice ▼

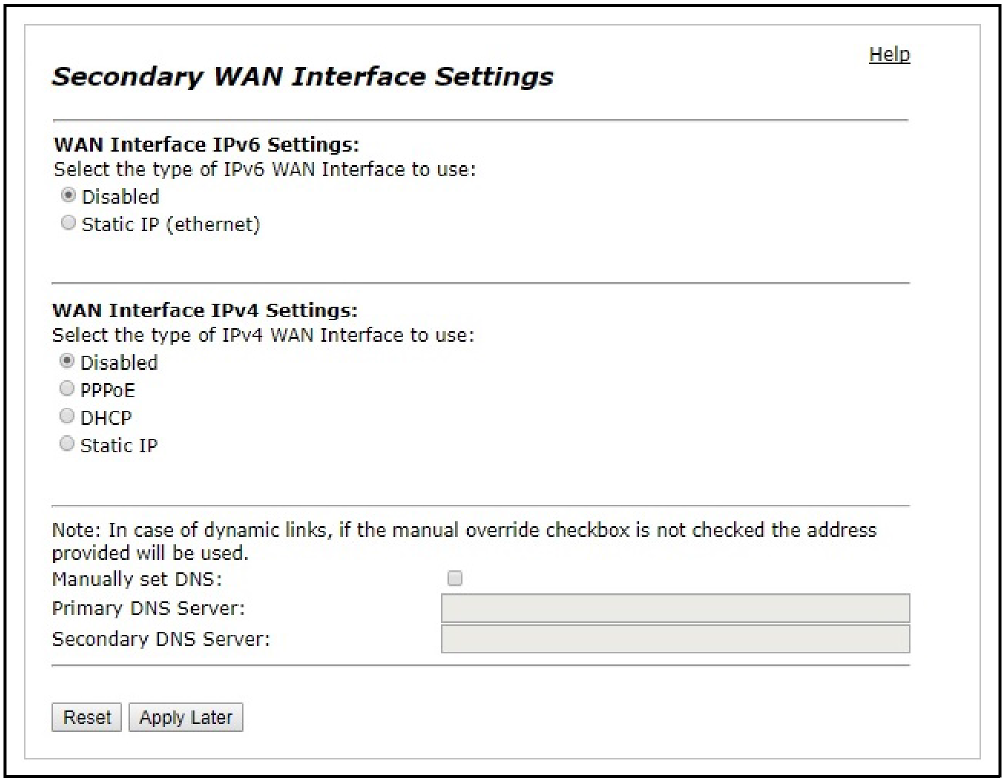
WAN Link Details

Primary Link Name: eth1
Primary Link IPv4 Address: 192.168.3.110
Primary Link IPv6 Address:
Secondary Link Name: eth2
Secondary Link IPv4 Address:
Secondary Link IPv6 Address:

- **Configure Secondary Interface**

  To configure the Secondary Interface, go to the **Secondary WAN Interface Settings** page (Figure 2-11) by clicking the **Secondary WAN** link on the **Stateful SIP Transfer** tab (Figure 2-8). Configure the Secondary WAN Interface according to your network setup.

Figure 2-11 Secondary WAN Interface Settings Page



Secondary WAN Interface Settings

WAN Interface IPv6 Settings:

Select the type of IPv6 WAN Interface to use:

● Disabled
○ Static IP (ethernet)

WAN Interface IPv4 Settings:

Select the type of IPv4 WAN Interface to use:

● Disabled
○ PPPoE
○ DHCP
○ Static IP

Note: In case of dynamic links, if the manual override checkbox is not checked the address provided will be used.

Manually set DNS: □

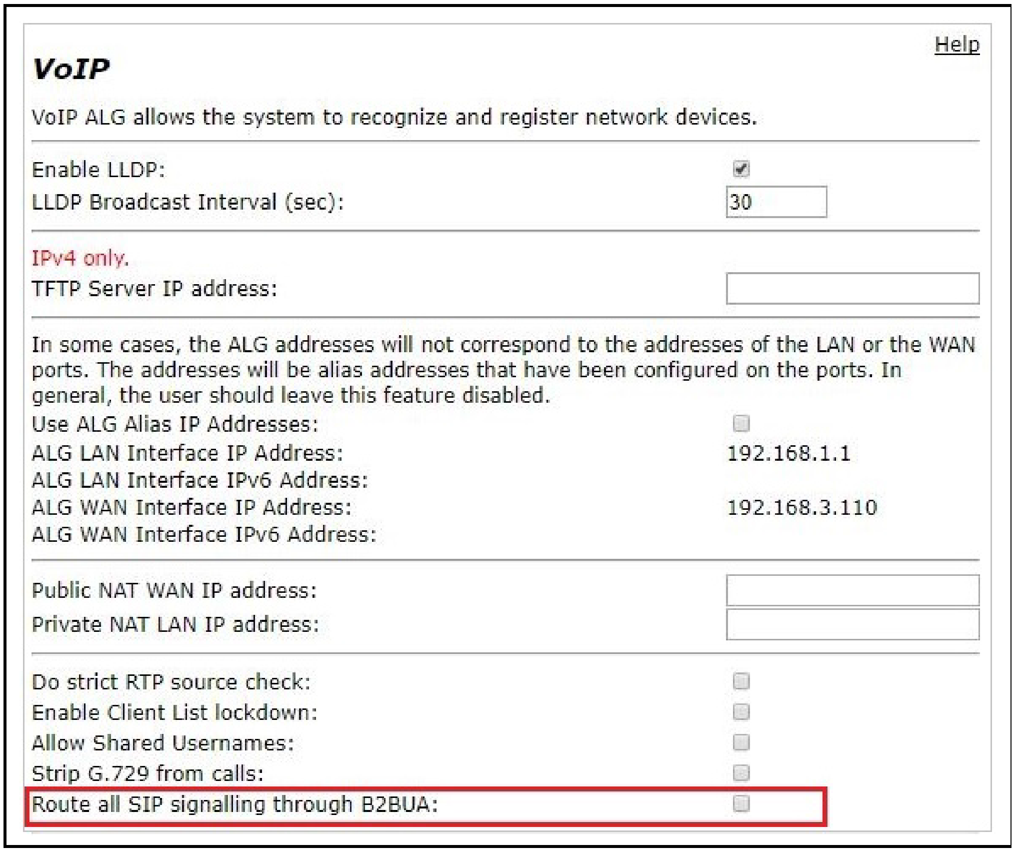
Primary DNS Server:

Secondary DNS Server:

- **Configure VoIP Settings**

  On the **VoIP** page, enable **Route all SIP signalling through B2BUA** (Figure 2-12).

Figure 2-12 VoIP Settings Page



Help

VoIP

VoIP ALG allows the system to recognize and register network devices.

Enable LLDP: ☑
LLDP Broadcast Interval (sec): 30

IPv4 only.
TFTP Server IP address:

In some cases, the ALG addresses will not correspond to the addresses of the LAN or the WAN ports. The addresses will be alias addresses that have been configured on the ports. In general, the user should leave this feature disabled.

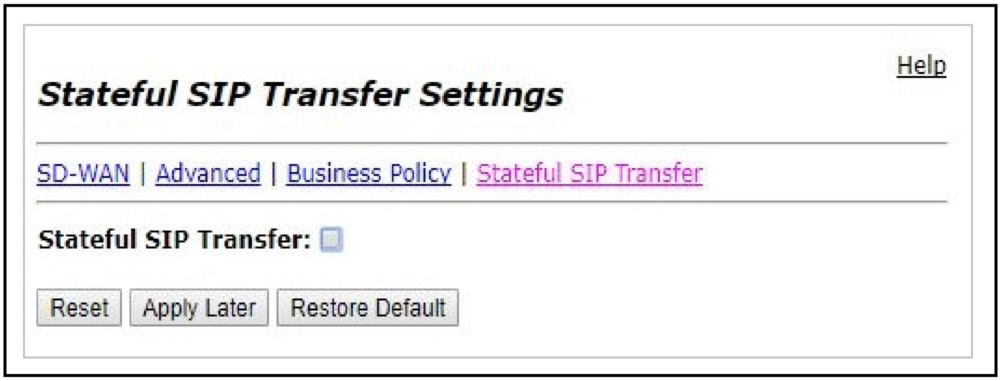
Use ALG Alias IP Addresses: □
ALG LAN Interface IP Address: 192.168.1.1
ALG LAN Interface IPv6 Address:
ALG WAN Interface IP Address: 192.168.3.110
ALG WAN Interface IPv6 Address:

Public NAT WAN IP address:
Private NAT LAN IP address:

Do strict RTP source check: □
Enable Client List lockdown: □
Allow Shared Usernames: □
Strip G.729 from calls: □
Route all SIP signalling through B2BUA: □

2. Once the configuration changes are made, an option to enable **Stateful SIP Transfer** will appear on the **Stateful SIP Transfer** tab (Figure 2-13).

Figure 2-13 Enable Stateful SIP Transfer



Help

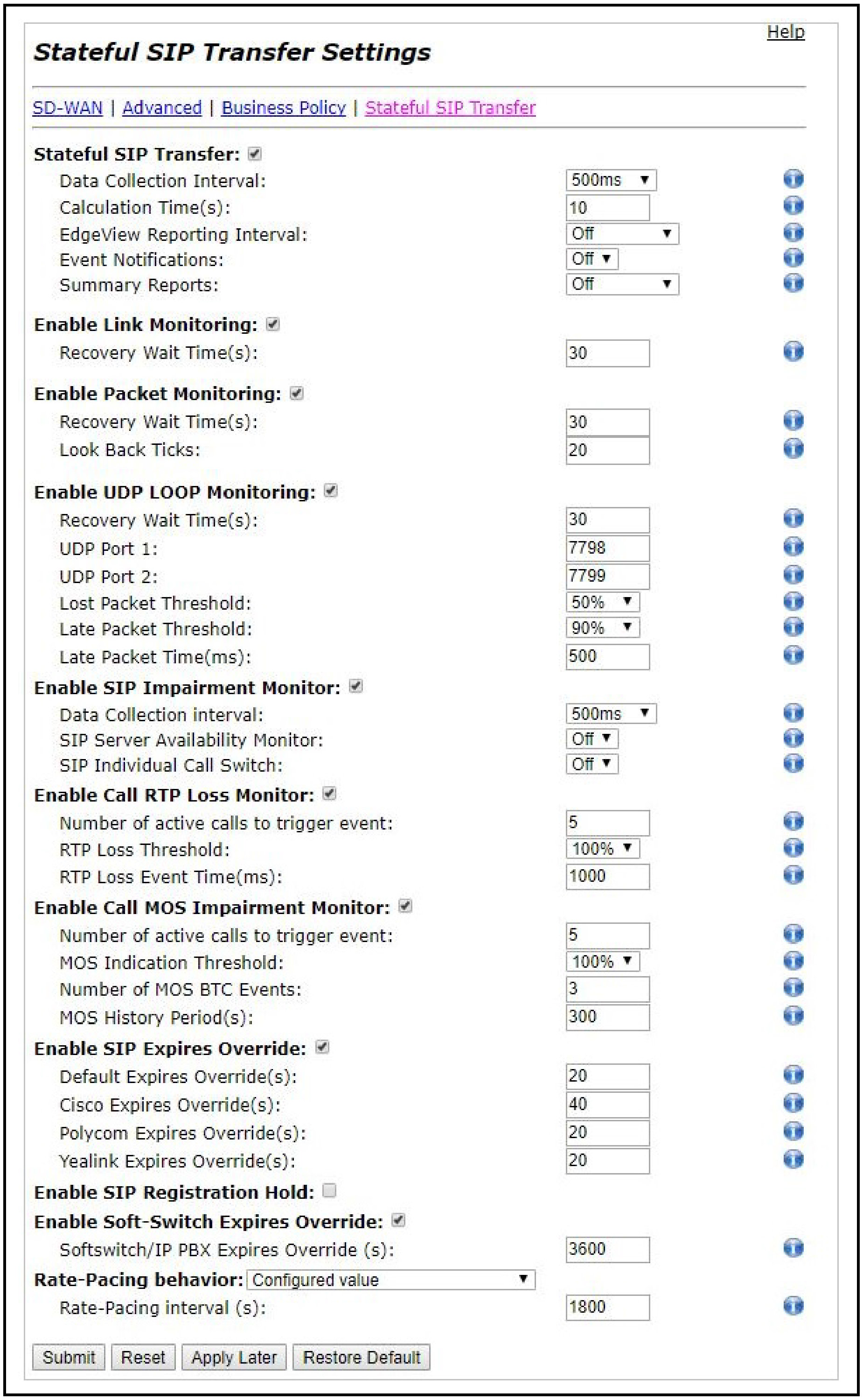
Stateful SIP Transfer Settings

SD-WAN | Advanced | Business Policy | Stateful SIP Transfer

Stateful SIP Transfer: □

3. Enable **Stateful SIP Transfer** upon which a detailed configuration menu will appear (Figure 2-14). The tool tip adjacent to each parameter will provide a quick help for configuring each parameter.

Figure 2-14 Stateful SIP Transfer Configuration Menu



Stateful SIP Transfer Settings

Help

SD-WAN | Advanced | Business Policy | Stateful SIP Transfer

Stateful SIP Transfer: ☑	
Data Collection Interval:	500ms ▾
Calculation Time(s):	10
EdgeView Reporting Interval:	Off ▾
Event Notifications:	Off ▾
Summary Reports:	Off ▾
Enable Link Monitoring: ☑	
Recovery Wait Time(s):	30
Enable Packet Monitoring: ☑	
Recovery Wait Time(s):	30
Look Back Ticks:	20
Enable UDP LOOP Monitoring: ☑	
Recovery Wait Time(s):	30
UDP Port 1:	7798
UDP Port 2:	7799
Lost Packet Threshold:	50% ▾
Late Packet Threshold:	90% ▾
Late Packet Time(ms):	500
Enable SIP Impairment Monitor: ☑	
Data Collection interval:	500ms ▾
SIP Server Availability Monitor:	Off ▾
SIP Individual Call Switch:	Off ▾
Enable Call RTP Loss Monitor: ☑	
Number of active calls to trigger event:	5
RTP Loss Threshold:	100% ▾
RTP Loss Event Time(ms):	1000
Enable Call MOS Impairment Monitor: ☑	
Number of active calls to trigger event:	5
MOS Indication Threshold:	100% ▾
Number of MOS BTC Events:	3
MOS History Period(s):	300
Enable SIP Expires Override: ☑	
Default Expires Override(s):	20
Cisco Expires Override(s):	40
Polycom Expires Override(s):	20
Yealink Expires Override(s):	20
Enable SIP Registration Hold: ☐	
Enable Soft-Switch Expires Override: ☑	
Softswitch/IP PBX Expires Override (s):	3600
Rate-Pacing behavior: Configured value ▾	
Rate-Pacing interval (s):	1800

For more details on Stateful SIP Transfer configuration, refer Stateful SIP Transfer Settings.

Note

It should be noted that **SST** and **Survivability** are not used in tandem. When **SST** is enabled, **Survivability** should be disabled.

Similarly, **HA** will not work when **SST** is enabled.

Business Policy

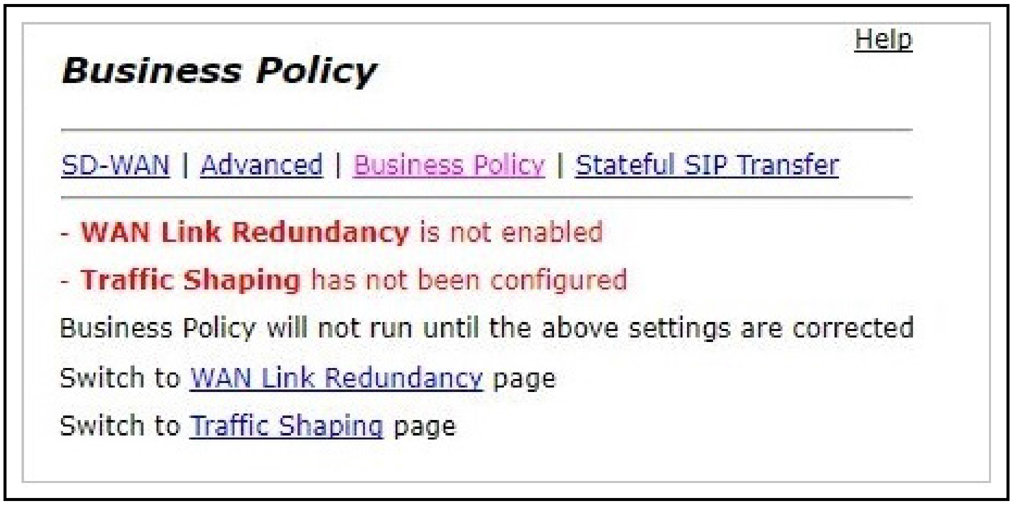
Business Policy enables traffic prioritization. Business Policy rules allow data flow to be classified based on URL, IP Address or destination port.

1. On the **Business Policy** tab (Figure 2-15), successively configure the changes mentioned on the page, as mentioned below.
   - Click on the **WAN Link Redundancy** page link on the **Business Policy** tab (Figure 2-15) and select the **Enable WAN Link Redundancy** check-box (Figure 2-10).

Note

If you have already enabled Stateful SIP Transfer, this message will not be displayed. This is because the WAN Link Redundancy parameter has to be enabled prior to enabling Stateful SIP Transfer.

Figure 2-15 Business Policy Tab



- **WAN Link Redundancy** is not enabled
- **Traffic Shaping** has not been configured

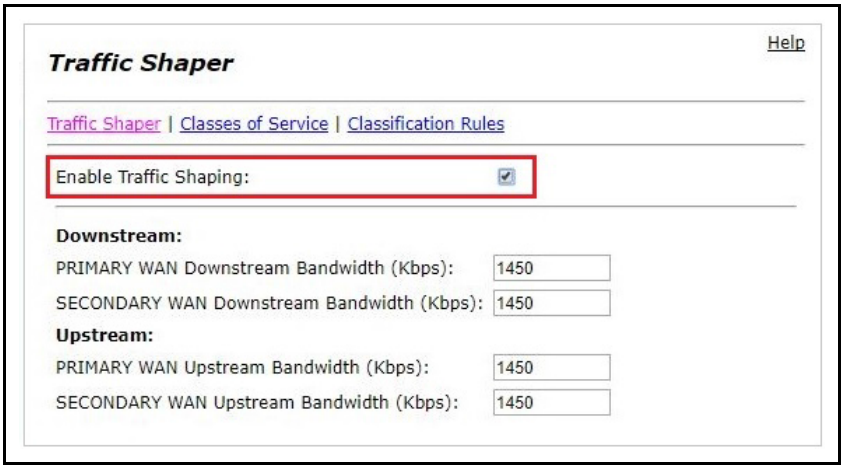
Business Policy will not run until the above settings are corrected

Switch to WAN Link Redundancy page

Switch to Traffic Shaping page

   - After submitting the change, go back to **Business Policy** and click the **Traffic Shaping** page link. You will be navigated to the **Traffic Shaper** page. Enable Traffic Shaping (Figure 2-16) and **Submit** change.

Figure 2-16 Traffic Shaper Page



Traffic Shaper

Enable Traffic Shaping: ☑

Downstream:

PRIMARY WAN Downstream Bandwidth (Kbps): 1450

SECONDARY WAN Downstream Bandwidth (Kbps): 1450

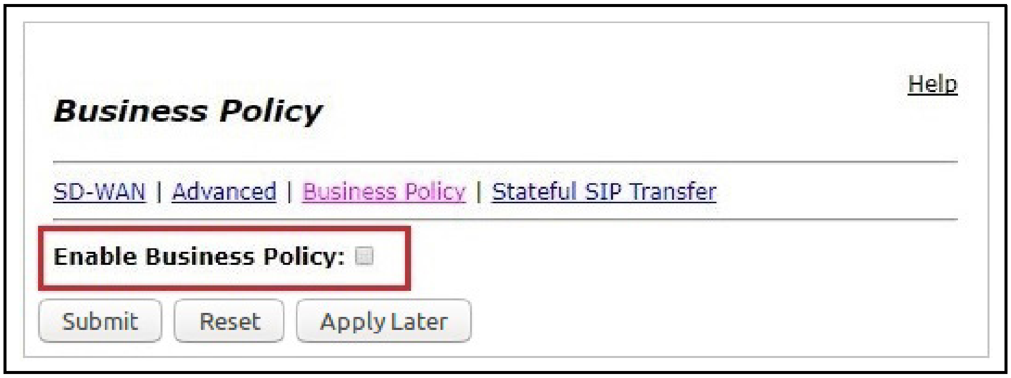
Upstream:

PRIMARY WAN Upstream Bandwidth (Kbps): 1450

SECONDARY WAN Upstream Bandwidth (Kbps): 1450

2. On the **Business Policy** tab, an option to enable Business Policy will appear (Figure 2-17).

Figure 2-17 Enable Business Policy

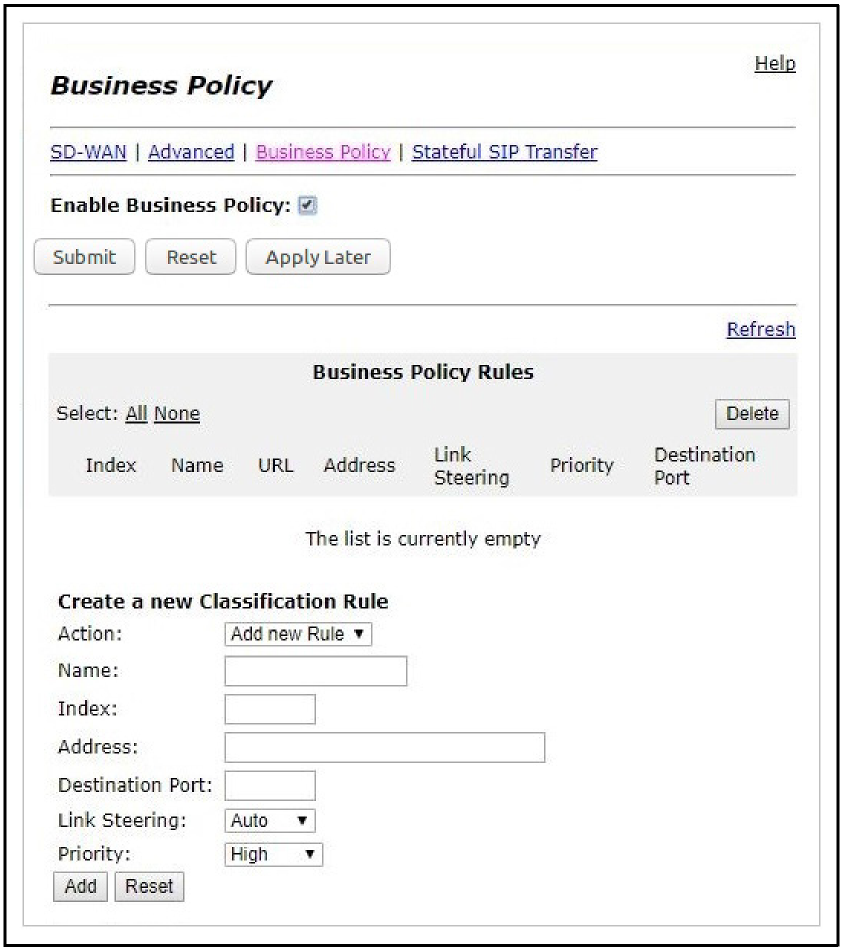


Business Policy

Enable Business Policy: □

3. Select the **Enable Business Policy** check-box and click the Submit button to enable business policy. Once the business policy is enabled successfully, a detailed configuration menu will appear (Figure 2-18).

Figure 2-18 Business Policy Configuration Menu



Business Policy

Enable Business Policy: ☑

Business Policy Rules

Index	Name	URL	Address	Link Steering	Priority	Destination Port

The list is currently empty

Create a new Classification Rule

Action:	Add new Rule ▼
Name:	
Index:	
Address:	
Destination Port:	
Link Steering:	Auto ▼
Priority:	High ▼

For more details on **Business Policy** configuration, refer Business Policy.

Note

It should be noted that **Business Policy** and **Fastpath Hardware Acceleration** cannot be enabled in tandem. **Fastpath Hardware Acceleration** is available only on E4800 platform devices.

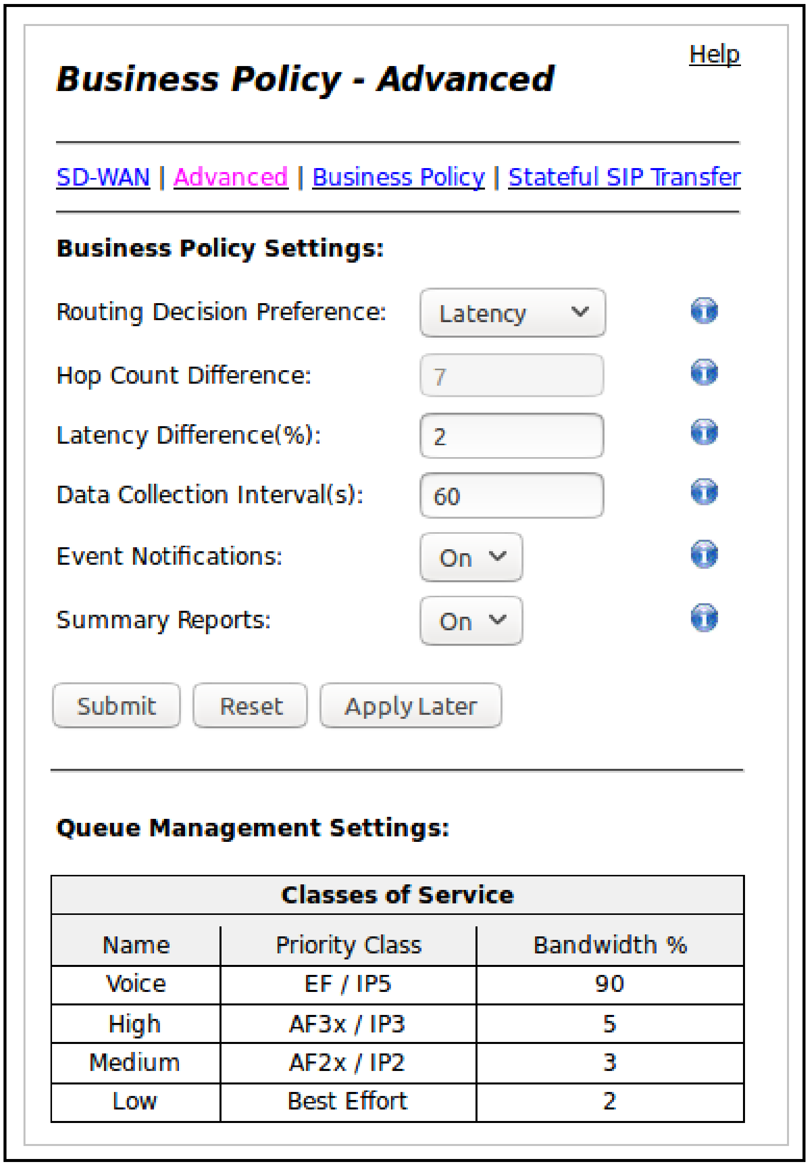
Advanced

1. On the **Business Policy - Advanced** page, configure the changes as mentioned on the page. **Business Policy - Advanced** page will prompt you to enable the Traffic Shaper. Enable Traffic Shaping by clicking on the **Traffic Shaping** page link. Once it is enabled, the **Business Policy - Advanced** is displayed (Figure 2-19).

Note

If you have already enabled **Traffic Shaping**, this message will not be displayed. This is because traffic shaping has to be enabled prior to enabling **Business Policy**.

Figure 2-19 Advanced Business Policy Page



Business Policy - Advanced

Business Policy Settings:

Routing Decision Preference: Latency

Hop Count Difference: 7

Latency Difference(%): 2

Data Collection Interval(s): 60

Event Notifications: On

Summary Reports: On

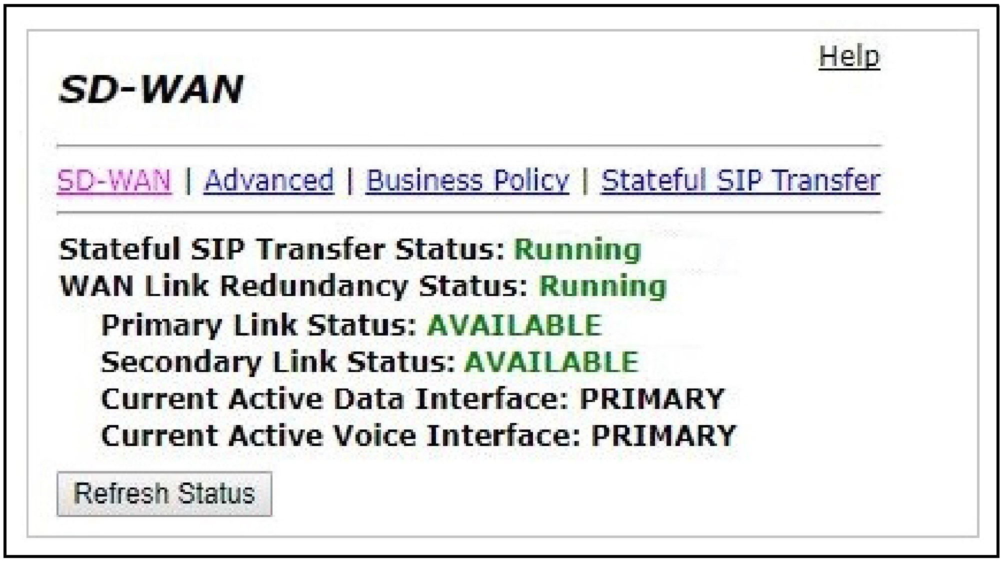
Queue Management Settings:

Classes of Service		
Name	Priority Class	Bandwidth %
Voice	EF / IP5	90
High	AF3x / IP3	5
Medium	AF2x / IP2	3
Low	Best Effort	2

To know more about configuring the Advanced Business Policy page, refer Business Policy - Advanced.

Once the Stateful SIP Transfer, Business Policy and Advanced Business Policy settings are configured, go back to the **SD-WAN** status tab. The Stateful SIP Transfer and WAN Link Redundancy status will be **Running**, and the Primary Link and Secondary Link status will be displayed as **Available** (Figure 2-20).

Figure 2-20 Updated SD-WAN Status Tab



SD-WAN

Stateful SIP Transfer Status: Running
WAN Link Redundancy Status: Running
Primary Link Status: AVAILABLE
Secondary Link Status: AVAILABLE
Current Active Data Interface: PRIMARY
Current Active Voice Interface: PRIMARY

Enabling EdgeView control of SD-WAN

To enable control of SD-WAN via EdgeView, there are a few configuration prerequisites on EdgeMarc. Configure these changes as mentioned below.

SD-WAN License

The Edgewater Networks SD-WAN requires a license that should be purchased separately. This license is available only as a subscription license, and not as a perpetual license. Ensure that your SD-WAN licensed, to be able to control it via EdgeView.

Enable WAN Link Redundancy

From the **Configuration Menu**, select **Network** > **WAN Failover**. Select **Enable WAN Link Redundancy** (Figure 2-10) and **Submit** change.

Enable Traffic Shaping

From the **Configuration Menu**, select **Network** > **Traffic Shaper**. Select **Enable Traffic Shaping** (Figure 2-16) and **Submit** change.

Note

To view EdgeMarc devices on the EdgeView **Devices List** page, configure the following parameters in the **evagent.conf** file.

EVAGENT_ENABLE=on

EDGEVIEW_HOST="IP address**"**

That is, set **EVAGENT_ENABLE** to **on** and enter the EdgeView IP address next to **EDGEVIEW_HOST**.

3

SD-WAN Configuration Settings

This chapter explains basic configuration settings of the SD-WAN functionality. Although the SD-WAN parameters are pre-configured with a set of default values, the following section details the function and use of each parameter.

- Stateful SIP Transfer Settings
- Business Policy
- Business Policy - Advanced

Stateful SIP Transfer Settings

This page allows the system administrator to enable and configure the Stateful SIP Transfer system.

Stateful SIP Transfer

Stateful SIP Transfer (SST) is a WAN failover enhancement for SIP voice services.

- **Data Collection Interval**
  The SST process does not run continuously. It runs in intervals. This setting tells the process how often data should be collected and analyzed. In between runs, the process listens for events from the WAN interfaces. This pause when the process listens for events is known as the 'tick' time.
- **Calculation Time(s)**
  Calculation time is the total time period for which the SST process will hold calculation data. This data is for Packet Monitoring and UDP Loop Monitoring.
- **EdgeView Reporting Interval**
  EdgeView Reporting Interval is the time interval after which Operational Measurements (OM) reports are sent to the database. The provided intervals are 1 minute, 15 minutes, 1 hour, and 1 day. Once a time interval is selected, all OM reports of greater time intervals are also sent on the shorter time interval.

- **Event Notifications**

  Enable to generate and send link switching event notifications to EdgeView.

- **Summary Reports**

  Enable to generate and send report data to the EdgeView. Report summaries is a report based upon the data used to determine when a link switching event should occur. The summary report is useful for historical references when troubleshooting issues or visualizing the metrics for quality or WAN health information. There are three settings for this option, **Off**, **On-Normal** and **On-Debug**.

  Off: Turns reporting off

  On-Normal: This setting will generate reports during link switch events with details of the switch.

  On-Debug: This setting reports internal state information. The option will generate large amounts of reports, and should only be activated when directed by customer support.

Enable Link Monitoring

This lets the SST process react to changes in link status of the physical Ethernet interface, i.e., if one WAN link is physically down, the SST process detects this. Although the process constantly listens for such events, it will trigger a WAN link switch only if this option is enabled.

- **Recovery Wait Time(s)**

  Recovery Wait Time specifies the time gap to be maintained before a switch to the primary WAN link is made, following a physical fail. Although the switchover is made only after the failed link returns to service, this setting is necessary to protect the device from multiple rapid switches if a link is rapidly going into and out of service.

Enable Packet Monitoring

Enable Packet Monitoring enables the SST process to detect possible packet losses. When this is enabled, the process will look at the total packet counts of each link on each tick. If the received packet count is not incrementing in line with the transmitted packet count, the process detects a possible problem. It will then look at the ping data coming from the WAN failover process. If the WAN failover process has ping issues, the process will initiate a link switch.

- **Recovery Wait Time(s)**

  Recovery Wait Time specifies the time gap to be maintained before a switch to the primary WAN link is made, following a WAN failover. It is also the time period for which the SST process remains in contact with the WAN failover process for ping statistics, on problem detection.

- **Look Back Tick**

The number of time slices (ticks) in the data history that is compared to the current received packet count.

Note

This field will automatically change with the **Data Collection Interval** or **Calculation Time(s)**.

Enable UDP LOOP Monitoring

Enabling this setting will start a 2-way UDP loop between the primary and secondary WAN links. 19 byte UDP packets are sent out to each link. The frequency of packet deployment is one packet per tick. If a late or lost packet is detected, the process will then look at the ping data coming from the WAN failover process. If the WAN failover process is observed to have ping issues, a link switch is initiated.

- **Recovery Wait Time(s)**

  Recovery Wait Time specifies the time gap to be maintained before a switch to the primary WAN link is made, following a WAN failover. It is also the time period for which the SST process remains in contact with the WAN failover process for ping statistics, on problem detection.

- **UDP Port 1**

  This is the port to be used for the primary WAN link. The default port is set to 7798, but any available port between 1025-65535 can be used. This port cannot be the same as UDP Port 2.

- **UDP Port 2**

  This is the port to be used for the secondary WAN link. The default port is set to 7799, but any available port between 1025-65535 can be used. This port cannot be the same as UDP Port 1.

- **Lost Packet Threshold**

  The percentage number of lost packets in the **Calculation Time** period that will cause an alarm.

- **Late Packet Threshold**

  The percentage number of late packets in the **Calculation Time** period that will cause an alarm.

- **Late Packet Time (ms)**

  The time period (in milliseconds) after which an expected UDP test loop packet is considered late. This time period will be different for each installation depending on the path length between the two WAN networks.

Enable SIP Impairment Monitor

Enables SIP to monitor several impairments that could indicate possible WAN link problems.

- **Data Collection interval**

  This setting selects how often the SIP process examines impairments on the system.

- **SIP Server Availability Monitor**

  SIP Server Availability Monitor enables SIP to request a WAN link switch if no SIP server is available on the active WAN link. SIP will try this only once and will not switch back and forth between links repeatedly.

- **SIP Individual Call Switch**

  This setting enables SIP to switch individual calls between the primary and secondary WAN interface if there is any issue in the call media. This issue is detected either by **Call RTP Loss Monitor** or **Call MOS Impairment Monitor**. Individual call switch is initiated only if the secondary WAN interface is found available by the system.

Enable Call RTP Loss Monitor

This parameter enables SIP to check for RTP Loss Events on each call.

- **Number of active calls to trigger event**

  This is the minimum number of calls that should be active in order to trigger a switch. This prevents a small number of calls with RTP problems from triggering a link switch.

- **RTP Loss Threshold**

  RTP Loss Threshold specifies the minimum percentage of calls with RTP loss events that will trigger a WAN link switch.

- **RTP Loss Event Time (ms)**

  This is the minimum amount of time that has to pass since a call receives an RTP packet to be considered an RTP loss.

Enable Call MOS Impairment Monitor

This setting enables SIP to check for MOS Score events. These events are generated every 10 seconds for a call, if the call encounters a MOS score of 2.5 or less.

- **Number of active calls to trigger event**

  This is the minimum number of calls that should be active on the system to initiate this check. If the number of calls is below this number, MOS Impairment will not trigger a WAN link switch. This setting prevents a small number of calls with MOS problems from triggering a link switch.

- **MOS Indication Threshold**

MOS Indication Threshold specifies the minimum percentage of calls with MOS score events that will trigger a WAN link switch

- **Number of MOS BTC Events**

  This is the number of MOS BTC reports in the MOS History Period that will flag a call as having MOS problem.

- **MOS History Period(s)**

  This is the time period for which MOS BTC events are collected.

Enable SIP Expires Override

This setting modifies the Expires value in the SIP 200OK REGISTER response message.

- **Default Expires Override(s)**

  Default expires override sets the Expires value in the SIP 200OK REGISTER response message for non-vendor specific SIP devices.

- **Cisco Expires Override(s)**

  Cisco expires override sets the Expires value in the SIP 200OK REGISTER response message for Cisco specific SIP devices.

Warning

Some Cisco SIP devices loaded with older versions of the IOS firmware may not function correctly with Expires values less than 40s.

- **Polycom Expires Override(s)**

  Polycom expires override sets the Expires value in the SIP 200OK REGISTER response message for Polycom specific SIP devices.

- **Yealink Expires Override(s)**

  Yealink expires override sets the Expires value in the SIP 200OK REGISTER response message for Yealink specific SIP devices.

Enable SIP Registration Hold

SIP Registration Hold provides a feature to increase the availability of LAN side devices registering to a host voice SIP provider.

Note

By default the **Expires Override** and **SIP Registration Hold** values are the same. Changing these to non-matching values should be done with caution. If the SIP device does not receive a 200OK response in a timely manner it may become unregistered. The default matching values provided for all vendors are acceptable timings for a 200OK response. These values allow the device to remain registered and capable of placing calls.

- **Default SIP Registration Hold(s)**

  The time delay (in seconds) before sending the SIP 200OK register response message for non-vendor specific SIP devices.

- **Cisco SIP Registration Hold(s)**

  The time delay (in seconds) before sending the SIP 200OK register response message for Cisco specific SIP devices.

- **Polycom SIP Registration Hold(s)**

  The time delay (in seconds) before sending the SIP 200OK register response message for Polycom specific SIP devices.

- **Yealink SIP Registration Hold(s)**

  The time delay (in seconds) before sending the SIP 200OK register response message for Yealink specific SIP devices.

Enable Soft-Switch Expires Override

When enabled, this value will replace the Expires value given by the phone in the SIP REGISTER message. This value should be higher than the rate-pacing value, otherwise, the SIP server may consider the phones' registration to have expired.

- **Softswitch/IP PBX Expires Override(s)**

  The number of seconds for which the SIP server should consider the registration valid.

Rate-Pacing behavior

This field controls the rate-pacing mode being used. This setting impacts the throttling rate at which SIP registrations will be forwarded through the system to the configured SIP server. SIP client registrations during this interval will be responded to by the system with a 200OK response. After the interval has expired the SIP client's next REGISTER message will be forwarded to the SIP server.

The drop-down menu offers three options to choose from.

None: Choosing this will disable rate pacing. SIP REGISTER messages will now be forwarded to the SIP server at the client frequency.

Soft-Switch/IP PBX provided value: The rate is calculated from the expires value provided by the SIP server. This value is calculated by subtracting 2 times the configured Phone Expires Override value from the SIP Server Expires value.

Configured value: This is the configured rate at which the SIP registrations are forwarded through the system to the configured SIP Server.

- **Rate-Pacing interval(s)**

  This is the configured rate of which SIP registrations will be forwarded through the system to the configured SIP server.

Warning

Before setting this value confirm the SIP servers 200OK response Expires value and verify that this setting holds a lower value. If the setting holds a higher value than the SIP servers Expires value, the SIP server will remove the client's registration binding and calls will fail.

Business Policy

Business policy rules allow the system to classify traffic flow into classes of service based on their URL, IP Address, or destination port.

When a rule is configured and saved, the system will modify each packet in the flow with the configured data priority.

The packet then enters the traffic shaper and based on data priority, the shaper applies the prioritization and bandwidth guarantees for the class-of-service the packet belongs to.

Warning

Traffic Shaping must be enabled and configured for the both the **Upstream** and **Downstream** bandwidths in case of Dual WAN support. The WAN connection provides priority through the system for the configured classification rules. When the system is installed and configured for Dual WAN support, be sure to configure both WANs’ Upstream and Downstream bandwidth settings.

Note

When Business Policy rules are added, edited, or deleted, network services are not restarted. Saved changes are reflected immediately on the system.

- **Refresh**

  Select to refresh the table. When a new URL rule is added, the system will resolve the URL to a DNS A address (i.e., IPv4 address). This field will display **Resolving Host**. The system will also test to verify which WAN interface provides the best path for traffic when **Link Steering** is configured for **Auto** and will display **Determining Interface**.

Note

When configuring a URL rule type for priority, the system will initiate a DNS A query to resolve the URL to IPv4 addresses and will then apply the configured priority to these IPs. The DNS A response will contain a TTL (time-to-live) value that indicates the time for which this specific DNS record is valid. After this TTL time has expired, the system will automatically re-query the DNS and update the IPv4 address and provide priority to the new IPv4 destination. Clicking Refresh will fetch the current set of IPv4 addresses of URLs specified in the Classification Rules.

- **Deleting an existing entry**

  To delete an existing rule, select the check-box for the rule to be deleted. One or more rules can be deleted at the same time. After the rules to be deleted are selected, click the Delete button.

- **Index**

  Determines the placement of the rule in the table. Rules are processed by the system from top to bottom. Edit the rule and enter the new index number as desired.

Note

When the index is configured for 0 the rule will be added to the top of the list. When no index is specified the rule will be added to the bottom of the list.

- **Name**

  Displays the configured name for the rule.

- **URL**

  Displays the configured DNS A record name for the rule.

- **Address**

  Displays the configured IPv4, IPv6 or the resolved address associated with the configured URL.

- **Link Steering**

  Displays the interface preference for the configured rule.

- **Priority**

  Displays the configured priority assigned to the traffic for the configured URL.

- **Destination Port**

  Displays the configured port assigned to the traffic for the configured rule.

- **Interface**

  Displays the current interface the rule is using. When the rules' **Link Steering** is configured to Auto, the system will analyze traffic and apply the **Routing Decision Preference** and settings on the **Advanced** page. This will determine which WAN the rules traffic should be routed through.

Create a new Classification Rule

- **Action**

  Select desired action from drop-down menu.

  Add New Rule: Select this to define a new classification rule. The Maximum number of rules that can added is 75.

  Edit Rule: Select the rule you wish to edit, then make the desired changes and click the **Edit** button to save the changes.

- **Name**

  This field specifies a unique name for the classification rule. Only alphanumeric, underscore(_), hyphen(-) and dot(.) characters are allowed.

- **Index**

  Index specifies the rule placement in the table.

- **Address**

  The address field can contain a URL, a single IPv4 address or a single IPv6 address.

  When configuring a URL, the URL must be a DNS A record name. DNS SRV record resolution is not supported.

- **Destination Port**

  The destination port can be configured as a single port.

  When configuring a port, you must select a specific transport protocol, the protocol cannot be configured when configuring port based priority.

Note

If **Address** is entered, the **Destination Port** cannot be entered. If the **Destination Port** is entered, **Address** cannot be entered. Only one of the two can be entered.

- **Link Steering**

  Specifies the preferred link for data routing. Options are WAN 1, WAN 2 and Auto.

  WAN 1 and WAN2 forces the rules' traffic flow to the WAN1 and WAN2 interface respectively.

  Auto option allows the system to determine the desired link depending on the **Routing Decision Preference** and settings on the **Advanced page**.

Note

Preference to WLR data interface for Auto rules is only considered at startup and not for subsequent link failures.

- **Priority**

  This value determines which Class of Service the flow belongs to. The system will display the class of service name that is created on the **Advanced** page. The system will not permit data flows to be assigned to the **Voice** class queue. The traffic priority can be set as either **High**, **Medium** or **Low**.

Note

It is not recommended to set the traffic priority to **Low** even though the setting is available.

Note

Business Policy does not execute a **config_network** to make the changes happen. The changes come into effect immediately.

Business Policy - Advanced

Business Policy - Advanced provides advanced business policy settings.

Business Policy Settings

- **Routing Decision Preference**

  Business Policy routing decision preference determines which WAN interface is preferable for a configured Business Policy rule. The system performs active analysis on the configured Business Policy rule to allow the network traffic associated with that rule to be directed to the best possible WAN interface available to the system at that time.

  When **Latency** is selected, the system will perform a test on each of the destination IPv4 addresses on both WAN interfaces to determine which WAN network path is of the lowest latency. The test is performed by the value configured in **Data Collection Interval** and using the value configured in **Latency Difference** as the metric difference.

  Latency: When Latency is selected, the system will determine which WAN interface has the lower latency to the configured rule.

  Hop Count: When Hop Count is selected, the system will determine which WAN interface has the lowest hop count to the configured rule.

Note

By default, **Routing Decision Preference** is set to **Latency**.

- **Hop Count Difference (Range 2 to 15)**

  This specifies the difference between the hop counts of traceroute output of both links after which a switch should occur. Default value is 7.

- **Latency Difference(%) (Range 10 to 100)**

  This setting specifies the difference in percentage between the latency of traceroute output of both links after which a switch should occur. Default value is 100 (percentage).

- **Data Collection Interval(s) (Range 60 to 300 sec)**

  Specifies the interval after which traceroute should be executed. Default value is 180 seconds.

- **Event Notifications**

  Enable to generate and send link switching event notifications to EdgeView. By default it is disabled.

- **Summary Reports**

  Enables to generate and send monitoring reports to EdgeView. Report summaries is a report based upon the data used in determining when a link switching event should occur. The summary report is useful for historical references when troubleshooting issues, visualizing the metrics for quality or for WAN health information. Reports will be available in the DB for a maximum period of 15 minutes to be consumed by EdgeView. By default it is disabled.

Queue Management Settings

- **Classes of Service**

  In order to prioritize and guarantee bandwidth for different types or class of traffic, network traffic must be grouped into classes of service. This page allows creation and modification of classes of service on the system and to allocate a percentage of bandwidth to each class.

  The percentage of bandwidth should equal 100%. By default the system has 4 classes - **Voice**, **High**, **Medium**, and **Low**. These four default classes have default bandwidth percentages assigned that total 100%. This 100% is based upon the configured Upstream and Downstream values from the Traffic Shaping configuration.

  Classes of service on the system create queues to guarantee service priority based upon the priority class assigned. For example, **Voice** is assigned a value of **EF** and allocated 90% of the WAN bandwidth. Classing **Voice** as EF means this traffic will be given higher priority and processed before classes below it, i.e., **AF3x**, **AF2x**, and **Best Effort**.

Classing data flows with **High**, **Medium** and **Low** allow control of the priority and percentage of WAN bandwidth allocated to that service.

Note

The configured percentage is the guaranteed allocation of WAN bandwidth. However, any class can borrow up to 100% when there is no traffic using any other classes. For example, if a **Business Policy** is configured for **Medium** priority which is currently allocated 3% of the total WAN upstream and downstream bandwidth and there are no current voice calls and no other traffic on the system then this class can use 100% of the total bandwidth on the system.

When voice calls or other traffic classes are present, then the system will balance the total bandwidth dynamically until a class like **Voice** starts to require 90% of the bandwidth. Then the other classes will only have access to their configured bandwidth percentages.

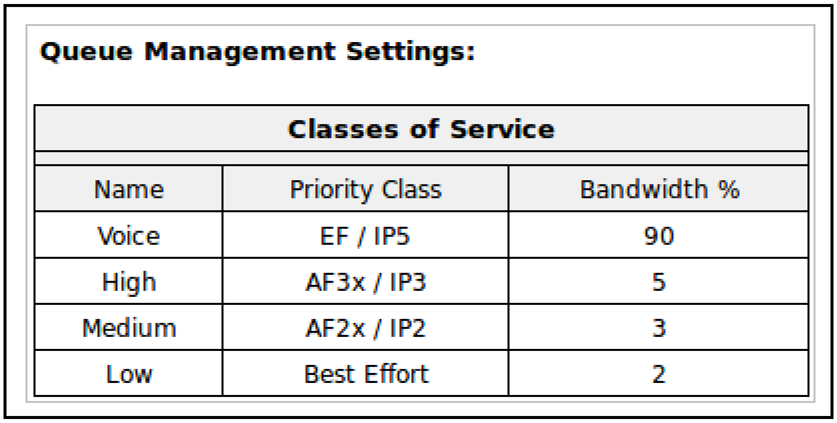
Below is the mapping of Priority Classes with the name:

Voice - EF

High - AF3x

Medium - AF2x

Figure 3-21 Classes of Service Bandwidth percentage



Queue Management Settings:

Classes of Service

Name	Priority Class	Bandwidth %
Voice	EF / IP5	90
High	AF3x / IP3	5
Medium	AF2x / IP2	3
Low	Best Effort	2

- **Name**

  Name specifies a name for the Class of Service.

- **Priority Class**

  The system supports 4 classes of service. They are listed below (from low to high priority).

  Best Effort: This is the default class. All unmarked traffic is assigned to this class. This traffic is also the first to be dropped during times of congestion. Examples of best effort traffic include web, email, SNMP, etc.

Assured Forwarding / IP Precedence (2 and 3): Assured Forwarding is suggested for applications that require a better reliability than the best-effort service. There are two Assured Forwarding classes of service. These classes also map to IP Precedece classes 2 and 3.

Expedited Forwarding / IP Precedence 5: Provides low-loss, low-latency, low-jitter and guaranteed bandwidth. This class is recommended for real-time voice traffic. This class also maps to IP Precedence class 5.

- **Bandwidth Percentage (%)**

  In general, higher priority classes should be configured to receive a greater percentage of the total bandwidth. The sum of bandwidth percentages across all configured classes cannot exceed 100%. When some of the classes are not in use, extra bandwidth % will be distributed across the other classes.