EdgeMarc Troubleshooting Guide

Debugging CPE VoIP Issues Using the EdgeMarc

Version 1.0

Edgewater Networks, Inc.
2730 San Tomas Expressway
Suite 200
Santa Clara, Ca. 95051
Phone: 408.351.7200
info@edgewaternetworks.com

1. Table of Contents

2. Problem Classification

This debugging guide breaks down problems into a few high-level areas. Find the appropriate starting point from the table below.

Problem	Description	Go To
PC connectivity	Basic problem with PC data connectivity	**3. PC Connectivity**, page 5
Call audio quality	Calls work but have audio issues	**4. Call Audio Quality**, page 11
Call connectivity	Calls not working, either always failing or intermittently	**5. Call Connectivity**, page 17
General debug	Using the EdgeMarc to debug many CPE issues	**6. General CPE Problem Source Identification**, page 21

3. PC Connectivity

Issues with PC data application access to the Internet or wide area network. Includes access issues to an EdgeMarc-controlled DMZ or additional LAN-side subnets.

3.1 High-level debug steps available

3.2 PC unable to acquire an IP address

Description: EdgeMarc is expected to deliver an IP address to a PC via DHCP. However, when connecting a PC to the LAN interface of an EdgeMarc no IP address is assigned.

3.2.1 EdgeMarc VLANs are not in use

Debug steps:

Step	Task	Next Step, based on Task	
1)	7.2 **Verify PC is configured to request an IP address via DHCP**, page 22	yes	go to next step
		no	Fix PC
2)	7.3 **Verify EdgeMarc is configured for** DHCP, page 22	yes	go to next step
		no	Enable DHCP Server
3)	7.28 **Verify only one DHCP Server is on LAN,** page 40	yes	go to next step
		no	Disable one of the DHCP servers
4)	7.4 **Verify DHCP addresses are still available**, page 24	yes	7.29 **Problem open at end of debug steps**, page 40
		no	3.7 **DHCP Server incorrectly out of addresses**, page 9

3.2.2 EdgeMarc VLANs are in use

Debug steps:

Step	Task	Next Step, based on Task	
1)	7.2 **Verify PC is configured to request an IP address via DHCP**, page 22	yes	go to next step
		no	Fix PC
2)	7.30 **Verify VLANs are configured properly**, page 40	yes	go to next step
		no	Correct VLAN configuration and/or connected devices
3)	7.3 **Verify EdgeMarc is configured for** DHCP, page 22	yes	go to next step
		no	Enable DHCP Server
4)	7.31 **Verify packets are reaching intended VLAN**, page 41	yes	go to next step
		no	Determine why network infrastructure is not delivering packet to

			EdgeMarc
5)	7.28 **Verify only one DHCP Server is on LAN,** page 40	yes	go to next step
		no	Disable one of the DHCP servers
6)	7.4 **Verify DHCP addresses are still available**, page 24	yes	7.29 **Problem open at end of debug steps**, page 40
		no	3.7 **DHCP Server incorrectly out of addresses**, page 9

3.3 PC unable to reach Internet

Description: Clients behind the EdgeMarc are not able to connect to the Internet

Debug Steps:

Step	Task	Next Step, based on Task	
1)	7.6 **Verify EdgeMarc is PC's default router**, page 25	yes	go to next step
		no	Correct client to point to EdgeMarc as default router
2)	Verify PC can ping its own loopback address: 127.0.0.1	yes	go to next step
		no	Fix PC configuration
3)	7.7 **Verify PC can ping EdgeMarc**, page 25	yes	go to next step
		no	3.4 **PC unable to ping EdgeMarc LAN**, page 7
4)	7.8 **Verify PC can ping a WAN-side address**, page 25	yes	go to next step
		no	3.6 **PC unable to ping beyond EdgeMarc**, page 8
5)	7.9 **Verify PC can resolve a DNS name**, page 25	yes	go to next step
		no	3.8 **PC unable to ping via DNS name**, page 9
6)	7.11 **Verify EdgeMarc can ping upstream default router**, page 26	yes	7.29 **Problem open at end of debug steps**, page 40
		no	Correct problem with upstream router

3.4 PC unable to ping EdgeMarc LAN

Description: A PC is unable to ping the LAN side of the EdgeMarc

Debug Steps:

Step	Task	Next Step, based on Task	
1)	Double check that EM's LAN IP is correct and is the address you are trying to ping	yes	go to next step
		no	Use correct address
2)	If PC is in a different subnet from EdgeMarc LAN interface, verify EdgeMarc has an IP route back to the PC's subnet	yes	go to next step
		no	Add Route via GUI **System->Route**
3)	7.10 **Verify LAN-device pings reach EdgeMarc and return**, page 26	yes	Fix blocking of EdgeMarc's reply, or, 7.29 **Problem open at end of debug steps**, page 40
		no	7.29 **Problem open at end of debug steps**, page 40

3.5 PC unable to ping EdgeMarc WAN

Description: A PC is unable to ping the EdgeMarc's WAN IP

Debug Steps:

Step	Task	Next Step, based on Task	
1)	If not already done, first complete: 3.4 **PC unable to ping EdgeMarc LAN**, above	go to next step	
2)	7.6 **Verify EdgeMarc is PC's default router**, page 25	yes	go to next step
		no	Set EdgeMarc as PC's default router
3)	If PC is in a different subnet from EdgeMarc LAN interface, verify EdgeMarc has an IP route back to the PC's subnet	yes	7.29 **Problem open at end of debug steps**, page 40
		no	Add Route via GUI **System->Route**

3.6 PC unable to ping beyond EdgeMarc

Description: A PC is unable to ping beyond the EdgeMarc

Debug Steps:

Step	Task	Next Step, based on Task	
1)	If not already done, first complete: 3.5 **PC unable to ping EdgeMarc WAN**, above	go to next step	
2)	7.11 **Verify EdgeMarc can ping upstream**	yes	go to next step

	default router, page 26	no	Determine failure with or to upstream router. If necessary, 7.29 **Problem open at end of debug steps**, page 40
3)	7.12 **Verify EdgeMarc can ping an Internet address**, page 27	yes	7.29 **Problem open at end of debug steps**, page 40
		no	Problem with upstream router

3.7 DHCP Server incorrectly out of addresses

Description: The EdgeMarc DHCP server is not delivering addresses because it is out of unused addresses. However, there are fewer attached devices than available addresses, so they appear not to be properly freed up.

Debug steps:
The most frequent cause of this failure is that the time on the EdgeMarc is not now, or at some point in the past was not, set to the correct time. If the start/stop times stored in the EdgeMarc's DHCP leases are not correct, then addresses may not be properly freed over time.

Step	Task	Next Step, based on Task	
1)	7.5 **Verify DHCP leases have proper timestamps**, page 24	yes	Need to examine leases further. Optionally, go to next step.
		no	go to next step
2)	Using EdgeMarc GUI, ensure proper time is set on EdgeMarc.	go to next step	
3)	7.1 **Clear DHCP Server addresses**, page 22	Problem should now be resolved. If not, 7.29 **Problem open at end of debug steps**, page 40	

3.8 PC unable to ping via DNS name

Description: A PC can ping an Internet device by IP address but not by DNS name.

Debug Steps:

Step	Task	Next Step, based on Task	
1)	Determine DNS server IP address being used by PC	go to next step	
2)	Verify PC can ping DNS server's IP address	yes	Verify DNS address

			is a functioning DNS server
		no	3.6 **PC unable to ping beyond EdgeMarc**, page 8

–- End of Section –-

4. Call Audio Quality

Issues with call audio quality. Calls connect but the quality is either consistently or intermittently unsatisfactory.

4.1 High-level debug steps available

4.2 Determine if EdgeMarc can help diagnose cause

Description: Determine if the poor audio quality might be due to the data path taken by the voice packets. Only some audio quality issues are affected by the data path; for other issues, such as gateway-induced echo, the EdgeMarc can neither cause nor diagnose the source of the problem.

Debug Steps:

Step	Task	Next Step, based on Task	
1)	Audio quality issue is echo	yes	4.3 **Poor audio quality due to echo**, page 12
		no	go to next step
2)	Audio quality issue is broken words, dropped syllables	yes	4.4 **Look for basic call-quality causes**, page 13
		no	go to next step
3)	Audio quality issue is periods of silence followed by return of audio	yes	4.4 **Look for basic call-quality causes**, page 13
		no	go to next step
4)	Audio quality issue is loss of audio mid-call, without return	yes	4.4 **Look for basic call-quality causes**, page 13
		no	7.29 **Problem open at end of debug steps**, page 40

4.3 Poor audio quality due to echo

Description: Echo is classified as one of two types:

- Acoustic echo: caused by sound bleeding from the earpiece of a headset back into the mouthpiece.
- Electrical echo: caused by the conversion of a digital audio signal to/from an analog segment of the phone network.

Note: The EdgeMarc is unable to cause, measure, influence or prevent either of these echo types. It is unable to introduce echo of either type and it is unable to reduce echo of either type.

While not caused by the EdgeMarc, the steps below might help pinpoint where the echo is being created.

Debug steps:

Step	Task	Next Step, based on Task	
1)	VoIP-to-PSTN call (initiated either way). Echo heard by VoIP end.	yes	Most likely VoIP Gateway requires impedance adjustment to match analog telephone network.
		no	go to next step
2)	VoIP-to-PSTN call (initiated either way). Echo heard by PSTN end.	yes	Possibly VoIP handset volume causing voice to bleed over from earpiece to microphone.
		no	go to next step
3)	VoIP-to-VoIP call, between "A" and "B". Echo heard at "A".	yes	Possibly VoIP handset volume too high at "B", causing A's voice to bleed over from B's earpiece to microphone.
		no	7.29 **Problem open at end of debug steps**, page 40

4.4 Look for basic call-quality causes

Description: Look for some of the more common causes of call-quality issues.

Debug Steps:

Step	Task	Next Step, based on Task	
1)	7.18 **Verify Ethernet interface is Full-Duplex, 100Mbps, Fixed**, page 32	yes	go to next step
		no	Change, if possible.
2)	Verify that the matching interface (on the other router or switch) is likewise configured: auto-to-auto or fixed-to-fixed, and, half-to-half or full-to-full.	matching	go to next step
		mismatch	Change to match.
3)	7.27 **Verify interfaces have no layer-2 frame errors**, page 39	no errors	No basic call-quality cause found, see text below
		errors	Examine further the cause of packet errors.

Once basic call quality failures are eliminated the advanced tools of the EdgeMarc and EdgeView working together are necessary to dig into where errors are being introduced. The process consists of the following high-level steps:

1. Using the EdgeMarc's MOS calculations and RTP statistics, along with EdgeView's display and analysis, look for patterns in the poor-quality calls. Based on analysis of the patterns the source of the failure may become apparent. This process is begun in section 4.5 **Examine MOS statistics for an EdgeMarc**, page 14

2. While the above step will point towards (if not identify) the source of the audio problem, it does not provide an actual capture example of the problem. A 30-second capture during a poor-quality event will present clear evidence of what is happening on the network. Having the EdgeMarc automatically perform such a capture is described in section 4.6 **Analyzing 30-second Below Threshold Event captures**, page 15

4.5 Examine MOS statistics for an EdgeMarc

Description: Perform the following steps to begin the process of looking for patterns in the MOS statistics captured by an EdgeMarc.

Debug Steps:

<table>
<tr><th>Step</th><th>Task</th><th colspan="2">Next Step, based on Task</th></tr>
<tr><td>1)</td><td>7.32 Ensure MOS capture is being performed, page 43. Capture at least four hours of call statistics.</td><td colspan="2">go to next step</td></tr>
<tr><td>2)</td><td>7.14 Obtain MOS statistics for an EdgeMarc, page 27</td><td colspan="2">go to next step</td></tr>
<tr><td colspan="4">Look for patterns in the low-quality calls.

The goal should be to address the most significant call quality issues. It is most effective to focus on a group of calls that have significant and similar low-quality characteristics. It is less effective to attempt to examine all imperfect calls at once; this will result in missing appropriate patterns and failing to address the customer's most serious issues first and quickly.

Below are important patterns to look for.</td></tr>
<tr><td rowspan="3">3)</td><td rowspan="3">7.15 Determine primary direction of poor-quality calls, page 30</td><td>wan</td><td>Potentially WAN-side call-quality issue. Go to next step.</td></tr>
<tr><td>lan</td><td>Potentially LAN-side call-quality issue. Go to next step.</td></tr>
<tr><td>both for <u>same</u> call</td><td>Potentially EM issue, possibly due to LAN problem such as broadcast storm. Go to next step.</td></tr>
<tr><td>4)</td><td>7.16 Determine if quality issue affects all active calls, page 30</td><td>all calls</td><td>Potential source of problem is a common link, such as the last-hop</td></tr>
</table>

Step	Task		Next Step, based on Task
			WAN link or common LAN link. Go to next step.
		subset of calls	Potential source of problem is an individual endpoint or gateway or isolated WAN or LAN link. Go to next step.
5)	7.17 **Capture traffic snapshots during BTC events**, page 31	4.6 **Analyzing 30-second Below Threshold Event captures**, page 15	

4.6 Analyzing 30-second Below Threshold Event captures

Description: Below Threshold events have been occurring and a set of 30-second captures have been retrieved for these events (as described in 7.17 **Capture traffic snapshots during BTC events**, page 31).

Examine these captures for patterns that might explain what is occurring. Contact Edgewater Technical Support for additional help on performing this analysis. (See 7.29 **Problem open at end of debug steps**, page 40.)

Debug Steps:

Step	Task	Next Step, based on Task	
1)	Using Ethereal, determine maximum jitter and lost packets for audio stream(s) within capture	go to next step	
2)	Look for a period of high latency or a large number of lost packets	found	go to next step
		not found	Find another 30-second capture to analyze
3)	Go to the next RTP packet immediately after a period of high jitter or lost packets	go to next step	
4)	Look at the incoming traffic just prior to this RTP packet	No incoming packets at all	Something may be stopping data from being delivered to EdgeMarc at all (or to an upstream router)
		Data only packets (no RTP)	go to next step
5)	Look at the period just as RTP starts to arrive again	Many RTP packets arriving rapidly, arrival rate between packets is well below 20msec.	Data traffic is starving out voice. The EdgeMarc's traffic shaping usually prevents this, so does the WAN have its own QoS

Step	Task	Next Step, based on Task	
			algorithm active?

–- End of Section –-

5. Call Connectivity Failures

Conditions where one or all phones are consistently or periodically unable to make calls or unable to perform a call-control action, such as transfer or hold.

5.1 High-level debug steps available

5.2 SIP phone is unable to Register

Description: A SIP phone behind an EdgeMarc is unable to Register with the softswitch.

5.2.1 SIP phone configured for "Registrar" FSR mode

The **Registrar** Flexible SIP Routing mode is where a VoIP phone is configured with a SIP Proxy value of the EdgeMarc's LAN interface (ex. 192.168.1.1) and no Outbound Proxy has been configured (or it is also set to the EM LAN interface).

Debug Steps:

Step	Task	Next Step, based on Task	
1)	7.19 **Verify phone is sending Register messages to EdgeMarc**, page 33	yes	go to next step
		no	Correct phone config.
2)	7.21 **Verify EdgeMarc is forwarding Register to softswitch**, page 34	yes	go to next step
		no	Verify EM can reach softswitch.
3)	7.22 **Verify softswitch is sending Register response to EM**, page 35	yes	go to next step
		no	Continue debug at softswitch.
4)	7.20 **Verify EdgeMarc is forwarding Register response to phone**, page 34	yes	7.29 **Problem open at end of debug steps**, page 40
		no	5.3 **EdgeMarc not forwarding SIP message to phone**, page 18

5.3 EdgeMarc not forwarding SIP message to phone

Description: The EdgeMarc is receiving a SIP message from the softswitch but is not forwarding it to a LAN-side phone

Debug Steps:

Step	Task	Next Step, based on Task	
1)	Verify SIP client, based on DID, is listed in Clients List, with correct IP address.	yes	go to next step
		no	Verify client (DID) is on LAN and is set to Register with the softswitch.
2)	Verify EdgeMarc can ping phone's IP	yes	Further debugging steps require Edgewater tracing. See 7.29 **Problem open at end of debug steps**, page 40

		no	Determine why ping is failing

5.4 General phone operation failure, easily recreated

Description: A failure in a phone operation is occurring and can be easily recreated. Desire is to capture SIP signaling to a PC in order to analyze further.

Debug Steps:

Step	Task	Next Step, based on Task
1)	Perform both a LAN and WAN capture to a file. These captures must be simultaneous (ie capturing the LAN and WAN trace for the same call). See 7.23.2 **Capture to a pcap file**, page 36	go to next step
2)	Create failing scenario	go to next step
3)	7.26 **Upload a file from EdgeMarc to PC**, page 37	See below

It is beyond the current scope of this document to describe how to analyze SIP signaling. Using the captured data you can work with a SIP-knowledgeable individual responsible for the softswitch and/or contact Edgewater Networks to examine the protocol flow and determine what is occurring.

5.5 General phone operation failure, intermittent

Description: A failure in a phone operation is occurring, but only periodically. Examples of this would include a transfer operation that only fails periodically.

The method to address such a failure is to perform continuous signaling capture using an EdgeView and the EdgeMarc. In cooperation with the end-user, determine the time of a failure and then use the captured signaling traces to determine exactly what occurred.

Debug Steps:

Step	Task	Next Step, based on Task
1)	7.24 **Activate continuous signaling capture to EdgeView**, page 36	go to next step
2)	Wait for a failure event to occur. Work with customer to understand that failures need to be reported at this time. A failure report from the customer needs to include:	go to next step

	• VoIP extension that experienced failure • Time of failure (best provided as time displayed on phone) • Far-end phone number, if known • Short description of what happened	
3)	7.25 **Find and download specific signaling capture from EdgeView**, page 37	See below

It is beyond the current scope of this document to describe how to analyze SIP signaling. Using the captured data you can work with a SIP-knowledgeable individual responsible for the softswitch and/or contact Edgewater Networks to examine the protocol flow and determine what is occurring. See 7.29 **Problem open at end of debug steps**, page 40.

–- End of Section –-

6. General CPE Problem Source Identification

The EdgeMarc is the most powerful tool in a service provider's toolkit for debugging VoIP – as well as general data – CPE issues. Using the EdgeMarc's general Linux O/S capabilities and the ability to create a RAM-based disk drive, it is possible to look for and capture many subtle networking errors.

6.1 General protocol capture

Description: Use the EdgeMarc to capture a specific protocol flow to a specific LAN-side device.

This capture technique is limited by the size of the ramdrive created on the EdgeMarc. The maximum size recommended is an 8MB (8000K) ramdrive. A smaller drive size should be specified when possible (commonly 4MB [4000K]).

Debug Steps:

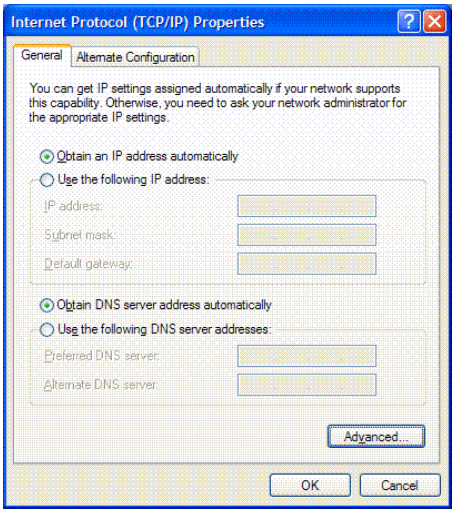
Step	Task	Next Step, based on Task
1)	Follow the steps in 7.23 **Capture an EdgeMarc protocol trace**, page 35, to capture a protocol flow to a pcap file. Due to the limited ramdisk space available, it is recommended that the **port** filter and/or **host** filter be used to limit the data captured.	go to next step
2)	7.26 **Upload a file from EdgeMarc to PC**, page 37	Perform analysis as desired for captured file. If necessary, 7.29 **Problem open at end of debug steps**, page 40

7. Tasks

7.1 Clear DHCP Server addresses

3. SSH into EdgeMarc CLI
4. Type: `cd /etc/config`
5. Type: `rm dhcpd.leases`
6. Type: `/etc/conf/bin/config_network`

7.2 Verify PC is configured to request an IP address via DHCP

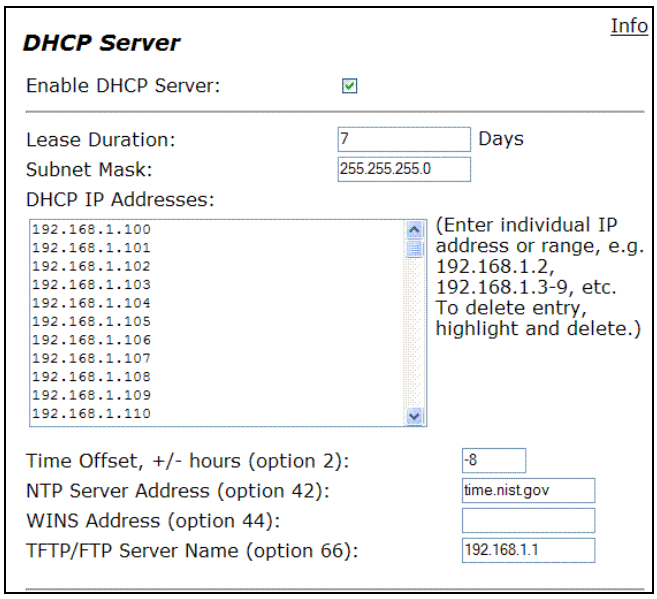


Verify **Obtain an IP address automatically** is checked.

7.3 Verify EdgeMarc is configured for DHCP

7.3.1 VLANs are NOT in use

7. From EdgeMarc GUI, click on **DHCP Server**.

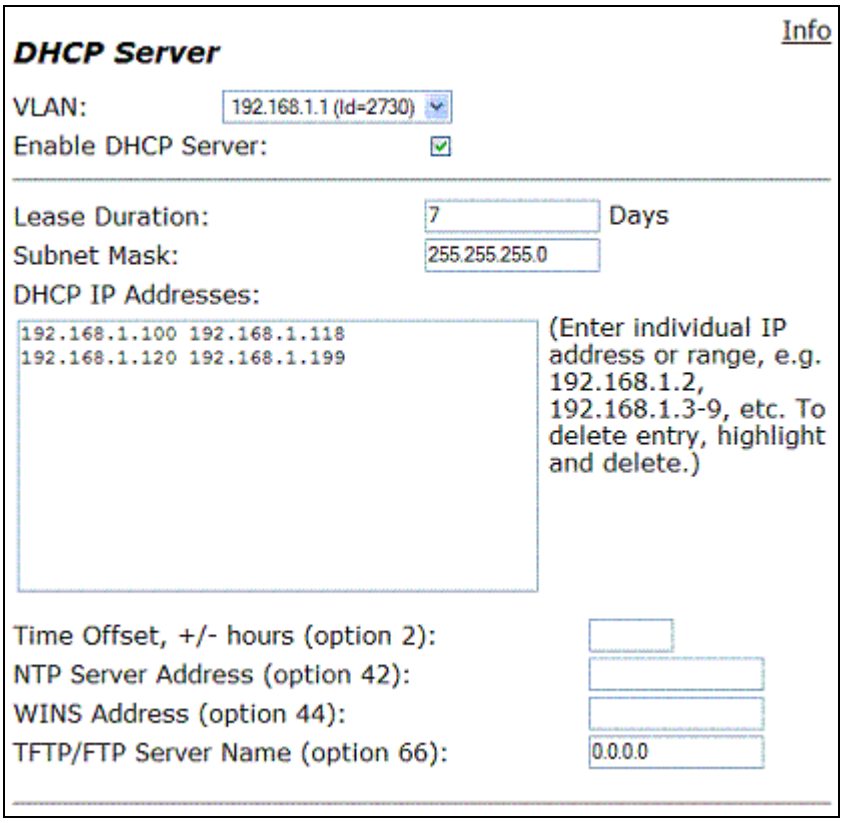


Verify:

- **Enable DHCP Server** is checked
- One or more IP addresses are listed in the box under **DHCP IP Addresses**.

7.3.2 VLANs are in use

1. From EdgeMarc GUI, click on **DHCP Server**.



2. From the **VLAN** drop-down box select the VLAN for which the EdgeMarc should be delivering DHCP addresses.

Verify:

- **Enable DHCP Server** is checked
- One or more IP addresses are listed in the box under **DHCP IP Addresses**

7.4 Verify DHCP addresses are still available

1. Log in to EdgeMarc CLI
2. Type: `cat dhcpd.leases | grep lease | sort`
3. You'll see a list of output similar to:

```
lease 10.10.11.150 {
lease 10.10.11.151 {
lease 10.10.11.152 {
lease 10.10.11.153 {
```

4. If all addresses specified on DHCP Server page are taken, then range is fully used.

7.5 Verify DHCP leases have proper timestamps

1. Type: `cat /etc/config/dhcpd.leases`
2. You'll see output similar to the following:

```
lease 10.10.11.158 {
```

```
        starts 1 2005/10/10 11:46:27;
        ends 1 2005/10/17 11:46:27;
        hardware ethernet 00:04:f2:00:38:38;
}
```

3. Look at each of the leases provided. If the **starts** and **ends** times are not correct (usually years in the past or future), then the leases have improper timestamps.
4. If the timestamps are improper then they must be erased and recreated, **after** the EdgeMarc's system clock is set to the right time.

7.6 Verify EdgeMarc is PC's default router

1. Open a DOS window on the PC, via **Start->Run->cmd**
2. Type: `ipconfig`
3. Verify that the **Default Gateway** shown is the EdgeMarc's LAN IP address

7.7 Verify PC can ping EdgeMarc

1. Open a DOS window on the PC, via **Start->Run->cmd**
2. Type: `ping` *`EM_LAN_IP_Address`*
3. Verify that the pings are responded to:

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
```

7.8 Verify PC can ping a WAN-side address

1. Open a DOS window on the PC, via **Start->Run->cmd**
2. Type: `ping 4.2.2.2`
3. Verify that the pings are responded to:

```
C:\>ping 4.2.2.2

Pinging 4.2.2.2 with 32 bytes of data:

Reply from 4.2.2.2: bytes=32 time=5ms TTL=247
Reply from 4.2.2.2: bytes=32 time=5ms TTL=247
Reply from 4.2.2.2: bytes=32 time=5ms TTL=247
Reply from 4.2.2.2: bytes=32 time=5ms TTL=247
```

7.9 Verify PC can resolve a DNS name

1. Open a DOS window on the PC, via **Start->Run->cmd**

2. Type: `ping edgewaternetworks.com`
3. Verify that DNS name is properly translated to an IP:

```
C:\>ping edgewaternetworks.com

                                    expected response
Pinging edgewaternetworks.com [204.202.2.188] with 32 bytes of data:

Reply from 204.202.2.188: bytes=32 time=6ms TTL=53
Reply from 204.202.2.188: bytes=32 time=5ms TTL=53
```

Failure example:

```
C:\>ping aabbccdd.com
Ping request could not find host aabbccdd.com. Please check the name and
try again.
```

7.10 Verify LAN-device pings reach EdgeMarc and return

Verify that when a LAN-side device pings the EdgeMarc its pings are actually reaching the EdgeMarc.

1. SSH into EdgeMarc CLI
2. Type: `tcpdump -ei eth0 icmp or arp`
3. From the LAN device issue pings to the EdgeMarc
4. The tcpdump should show **icmp echo requests** and **icmp echo responses**

```
# tcpdump -ei eth0 icmp or arp

tcpdump: listening on eth0
           source MAC    dest MAC
23:43:38.07 0:e0:98:ac:63:66 0:c0:2:b8:c9:6e ip 74: 192.168.1.51 > 192.168.1.1: icmp: echo
request

           source MAC    dest MAC
23:43:38.07 0:c0:2:b8:c9:6e 0:e0:98:ac:63:66 ip 74: 192.168.1.1 > 192.168.1.51: icmp: echo
reply
```

5. Verify that the MAC address in the icmp messages is actually the EdgeMarc's LAN interface MAC address
   a. Type: ifconfig eth0

```
eth0      Link encap:Ethernet  HWaddr 00:C0:02:B8:C9:6E
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
```

   b. Verify that the **HWaddr** shown is the same as:
      . The destination MAC in the **echo request**.
      . The source MAC in the **echo reply**.
6. Also, verify that the MAC address in the icmp response is actually the PC's MAC address

7.11 Verify EdgeMarc can ping upstream default router

1. SSH into EdgeMarc CLI
2. Type: `route`

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
```

```
64.186.171.0    *               255.255.255.0   U     0      0        0 eth1
192.168.1.0     *               255.255.255.0   U     0      0        0 eth0
127.0.0.0       *               255.0.0.0       U     0      0        0 lo
default         64.186.171.1    0.0.0.0         UG    0      0        0 eth1
```

3. Look for **"default"** entry. Note **Gateway** IP address, this is the upstream gateway (**64.186.171.1** in the above example).
4. Type: `ping` *`gateway_ip_address`*
5. Verify pings are successful

7.12 Verify EdgeMarc can ping an Internet address

1. SSH into EdgeMarc CLI
2. Type: `ping 204.202.2.188` OR `ping 4.2.2.2` OR another IP address (not domain name) of your choosing
3. Verify pings are successful

7.13 Gather audio quality measurements for analysis

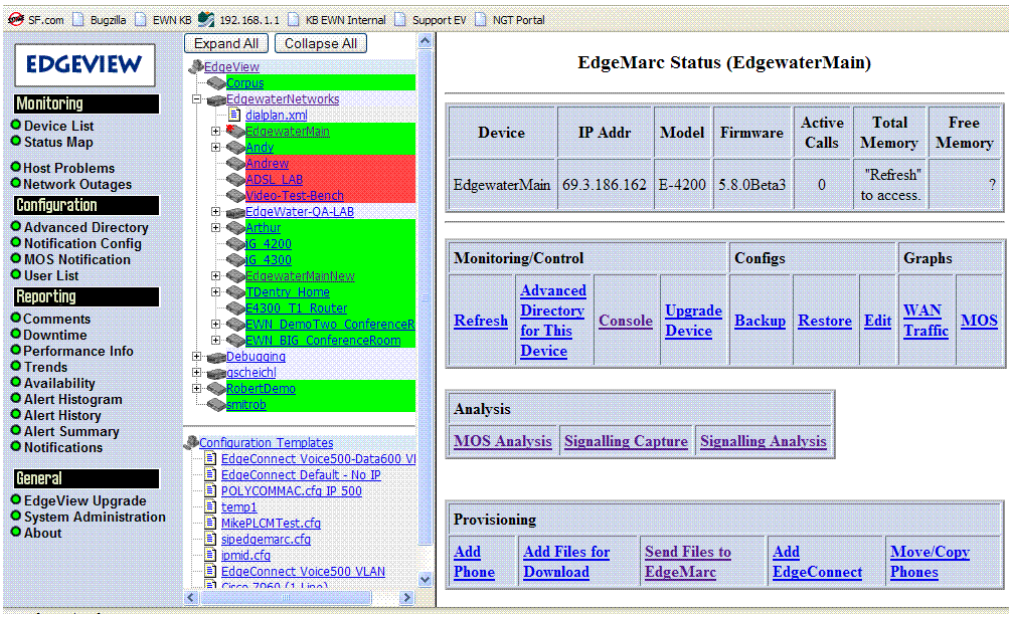
The following steps are intended to gather audio statistics (MOS scores and associated stats) in order to further analyze the cause of poor call quality.

1. From EdgeMarc with which to perform analysis:
   a. From GUI go to **System->Services Configuration**
   b. Enable **Remote System Logging**
   c. Point EdgeMarc to an EdgeView for syslog capture
2. Request customer to continue making calls. Capture data for at least a 4 hour period. A good volume of data is necessary to determine call-quality patterns. Short data collection times can result in misleading patterns detected or actual patterns being missed.
3. After data has been collected, continue with debug steps in section 4.1 **High-level debug steps available**, page 11

7.14 Obtain MOS statistics for an EdgeMarc

Perform the following steps to begin the process of looking for patterns in the MOS statistics captured for a particular EdgeMarc.

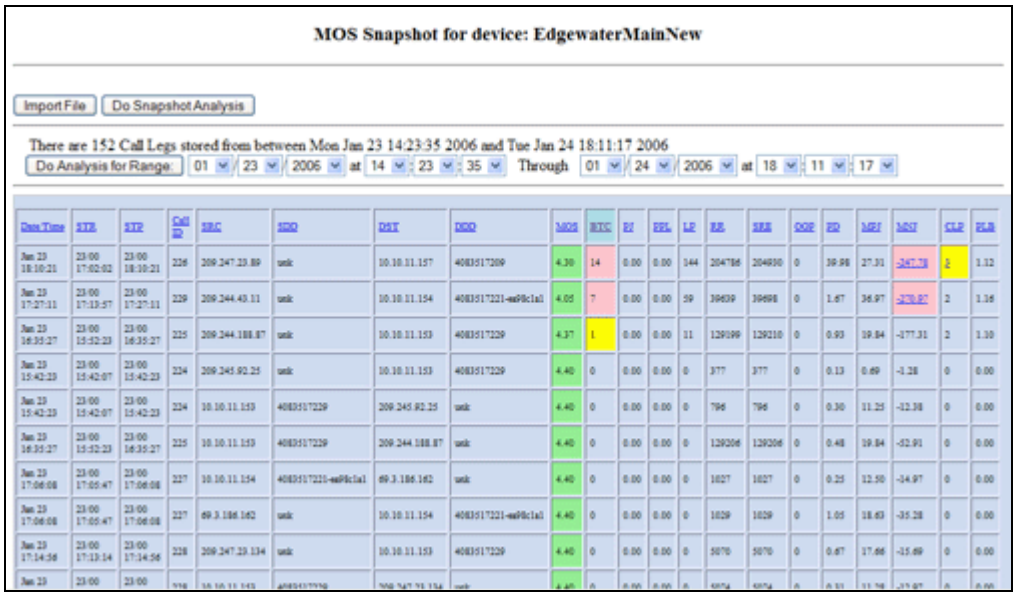
1. Click on the EdgeMarc within the EdgeView device list (middle pane). This brings up the EdgeMarc status page (right pane).


SF.com
Bugzilla
EWN KB
192.168.1.1
KB EWN Internal
Support EV
NGT Portal
EDGEVIEW
Monitoring
Device List
Status Map
Host Problems
Network Outages
Configuration
Advanced Directory
Notification Config
MOS Notification
User List
Reporting
Comments
Downtime
Performance Info
Trends
Availability
Alert Histogram
Alert History
Alert Summary
Notifications
General
EdgeView Upgrade
System Administration
About
Expand All
Collapse All
EdgeView
Corpus
EdgewaterNetworks
dialplan.xml
EdgewaterMain
Andy
Andrew
ADSL_LAB
Video-Test-Bench
EdgeWater-QA-LAB
Arthur
IG_4200
IG_4300
EdgewaterMainNew
TDentry_Home
E4300_T1_Router
EWN_DemoTwo_ConferenceR
EWN_BIG_ConferenceRoom
Debugging
gscheichl
RobertDemo
smirok
Configuration Templates
EdgeConnect Voice500-Data600 VI
EdgeConnect Default - No IP
POLYCOMMAC.cfg IP 500
temp1
MikePLCMTest.cfg
sipedgemarc.cfg
ipmid.cfg
EdgeConnect Voice500 VLAN
EdgeMarc Status (EdgewaterMain)
Device
IP Addr
Model
Firmware
Active Calls
Total Memory
Free Memory
EdgewaterMain
69.3.186.162
E-4200
5.8.0Beta3
0
"Refresh" to access.
?
Monitoring/Control
Configs
Graphs
Refresh
Advanced Directory for This Device
Console
Upgrade Device
Backup
Restore
Edit
WAN Traffic
MOS
Analysis
MOS Analysis
Signalling Capture
Signalling Analysis
Provisioning
Add Phone
Add Files for Download
Send Files to EdgeMarc
Add EdgeConnect
Move/Copy Phones

2. Click on MOS Analysis. This brings up the MOS snapshot page.
3. Click on **Do Analysis for Range**. The range can be restricted if you are looking for the behavior after a specific network change was made. In general, however, it is best to bring up as large a range as is available.

   Note: If the **Do Analysis for Range** button is missing then EdgeView is not properly configured to capture and store MOS scores in its database. (The scores are still captured in the EdgeView's syslog, but they are not being analyzed and placed within EdgeView's SQL database.) This must be corrected by following the instructions in the EdgeView manual and/or contacting the Edgewater Networks TAC.

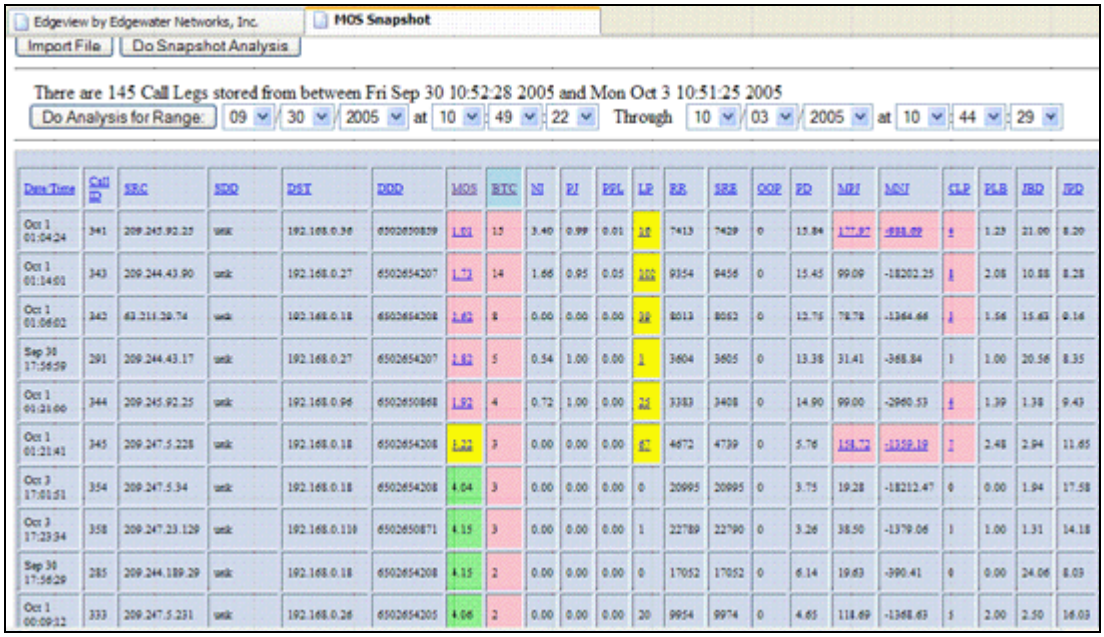
   A properly analysis response will look similar to the following:



4. Click on the **BTC** column to sort by Below Threshold Count value, least-to-most
5. Click on the **BTC** column to re-sort from most-to-least (as pictured above)
6. Note that even calls with overall good quality may have experienced multiple 10-second intervals of below-threshold MOS events. (By default these are periods with MOS below 2.5.)

7.15 Determine primary direction of poor-quality calls

1. Sort MOS statistics by **BTC** column, as described in 7.14 **Obtain MOS statistics for an EdgeMarc.**



2. Examine the **SRC** and **DST** addresses.
   a. If the SRC is a public WAN address and the DST is a private LAN address, then the poor call quality is incoming from the WAN side. The RTP stream is bad by the time it hits the EdgeMarc's WAN interface.
   b. If the SRC is a private LAN address and the DST is a public WAN address, then the poor call quality is incoming from the LAN side. The RTP stream is bad by the time it hits the EdgeMarc's LAN interface.

7.16 Determine if quality issue affects all active calls

Make a determination if the source of poor audio quality is such that it affects all active calls or if it only affects a subset of the calls that are active at a given moment.

1. We will start by finding a subset of the EdgeView syslog that overlaps with the poor-quality calls seen in the MOS statistics table (as gathered in **7.14 Obtain MOS statistics for an EdgeMarc**, on page 27).
2. SSH into the EdgeView CLI
3. Use one of the following grep commands to extract a portion of the syslog for this particular EdgeMarc and the specific call of interest or a time range of interest.
   a. Type:
   `egrep -i '`*`MMM`*`( |  )(`*`Day`*`).*`*`hostname`*`.*mos' /var/log/messages >`*`hostname-MM-DD`*`.txt`
      . *MMM* = 3-letter month
      . *Day* = Day of month (no leading zeros)

. *hostname* = The hostname for the EM in question. The EdgeMarc will use its hostname in each syslog message. You can use the EM's IP address here, too.

b. If you are able to use a Linux editor, then keep the file on the EdgeView. If you are more comfortable using a PC editor, then transfer the `hostname-MM-DD.txt` file to a PC.

4. Open the file of extracted syslog messages in a text editor. You can use the VI or emacs editors on Linux or an editor of your choice on a PC. If emacs is to be used, type: `emacs -nw hostname-MM-DD.txt`
("-nw" will bring up emacs in the text-based SSH window.)
5. Scan through the syslog messages searching for Below Threshold events:
   a. Search for "`below threshold`", and/or
   b. Search for "`call id XXX`" looking for "`below threshold`" messages
6. You are looking to determine if Below Threshold messages are issued for all active calls at any one point in time or only a subset of active calls. The way to tell is by comparing the "**Current Calls=**" value against the Call IDs specified in Below Threshold messages.

   a. Here is an example where only one call out of 3 is resulting in Below Threshold events at a given moment. One Call Id is generating messages while 3 calls are active.

```
Sep 29 20:31:21 69.3.186.162 2005(1) EWN-Office-4200 mand: Call ID 1079 10.10.10.204-
>209.244.188.87 MOS=2.44 below threshold 2.50 (Long Term=1.93, Current Calls=3)
Sep 29 20:31:31 69.3.186.162 2005(1) EWN-Office-4200 mand: Call ID 1079 10.10.10.204-
>209.244.188.87 MOS=2.39 below threshold 2.50 (Long Term=1.97, Current Calls=3)
Sep 29 20:31:41 69.3.186.162 2005(1) EWN-Office-4200 mand: Call ID 1079 10.10.10.204-
>209.244.188.87 MOS=1.84 below threshold 2.50 (Long Term=1.98, Current Calls=3)
```

   b. Here is an example where all active calls are resulting in a Below Threshold event at a given moment. Two Call Ids are generating messages and exactly 2 calls are active:

```
Jan 24 00:56:45 69.3.186.162 2006(1) EWN-Office-4200 mand: Call ID 452 209.244.42.253-
>10.10.10.204 MOS=1.69 below threshold\
 2.50 (Long Term=4.36, Current Calls=2)
Jan 24 00:56:46 69.3.186.162 2006(1) EWN-Office-4200 mand: Call ID 448 209.244.42.250-
>10.10.10.188 MOS=1.00 below threshold\
 2.50 (Long Term=4.37, Current Calls=2)
Jan 24 00:56:55 69.3.186.162 2006(1) EWN-Office-4200 mand: Call ID 452 209.244.42.253-
>10.10.10.204 MOS=1.00 below threshold\
 2.50 (Long Term=4.31, Current Calls=2)
Jan 24 00:56:56 69.3.186.162 2006(1) EWN-Office-4200 mand: Call ID 448 209.244.42.250-
>10.10.10.188 MOS=1.00 below threshold\
 2.50 (Long Term=4.34, Current Calls=2)
```

7.17 Capture traffic snapshots during BTC events

It may be valuable to capture a snapshot of LAN or WAN traffic at the moment a Below Threshold event occurs. If it is known that the call-quality issue is always on one side (from the LAN or from the WAN), than traffic from that interface should be captured when a Below Threshold event is detected by the EdgeMarc.

These captures are limited by the fact that they begin <u>after</u> a below threshold event is detected. So they are only able to capture events that continue beyond that first event – that is, continue for more than 10 seconds.

This is an advanced capability of the EdgeMarc, previously only available to Edgewater engineers. The linux script to perform this capture should be copy-and-pasted from the Knowledgebase article mentioned below. If this is the first time you are using this capture technique it is recommended you contact the Edgewater TAC for assistance.

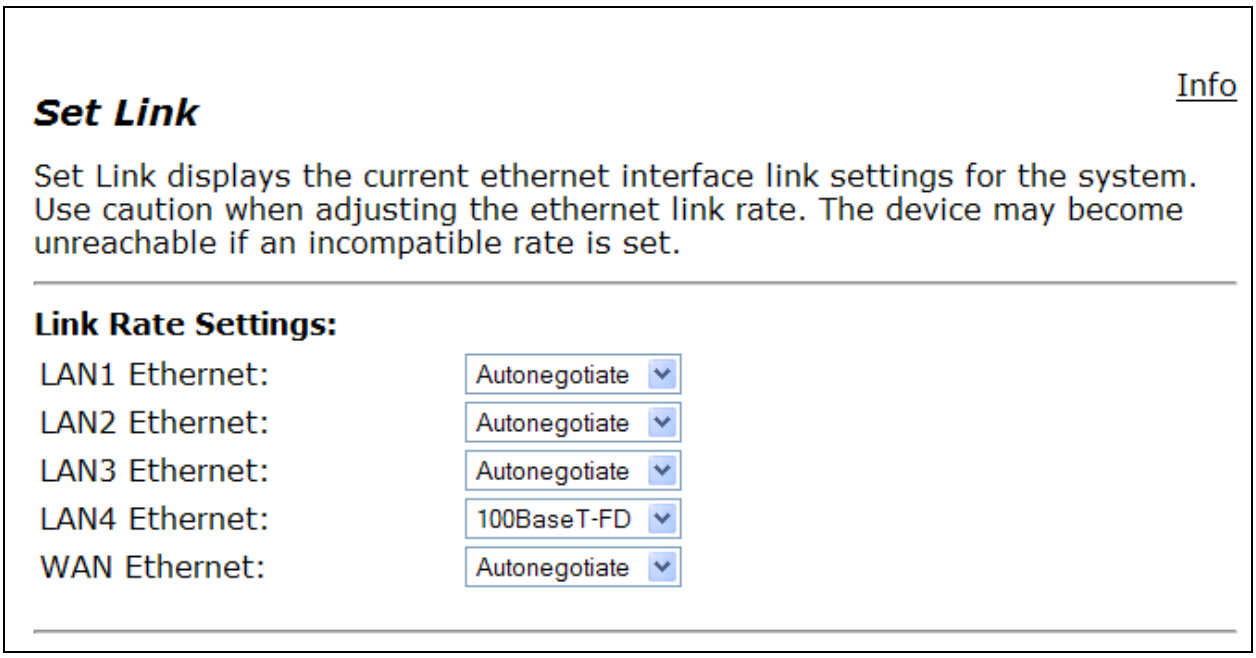
1. SSH into the EdgeMarc CLI
2. Follow the instructions in Knowledgebase article **Capture WAN/LAN RTP audio problems (#151065)**. This will begin capture of 30 seconds of WAN or LAN & WAN traffic whenever a Below Threshold event occurs.
3. Let the capture run until a few captures have occurred.
   - Use an FTP client to examine the FTP server and watch for a few capture files from this EdgeMarc hostname
4. Use the following grep command to extract the recent Below Threshold messages from the EdgeView syslog for this particular EdgeMarc.
   c. Type: `egrep -i 'MMM( |  )(Day).*hostname.*below' /var/log/messages >hostname-MM-DD.txt`
      . *MMM* = 3-letter month
      . *Day* = Day of month (no leading zeros)
      . *hostname* = The hostname for the EM in question. The EdgeMarc will use its hostname in each syslog message. You can use the EM's IP address here, too.
   d. If you are able to use a Linux editor, then keep the file on the EdgeView. If you are more comfortable using a PC editor, then transfer the `hostname-MM-DD.txt` file to a PC.
5. Open the file of extracted syslog messages in a text editor. You can use the VI or emacs editors on Linux or an editor of your choice on a PC. If emacs is to be used, type: `emacs -nw hostname-MM-DD.txt`
   ("-nw" will bring up emacs in the text-based SSH window.)
6. Note the timestamps on the 30-second capture files on the FTP server.
7. Look through the syslog messages. You should generally be able to find a one-to-one mapping between BTC messages and 30-second captures. (Note, however, that only one 30-second capture is performed at any one time.)
8. The ideal 30-second snapshots to examine are those that occur during a burst of Below Threshold events. These are the most likely periods where a quality-affecting event lasted more than 10 seconds, and therefore is likely to appear in the capture file.
9. Download a potentially interesting 30-second capture to your PC and open it with Ethereal (or other .pcap capable tool).

7.18 Verify Ethernet interface is Full-Duplex, 100Mbps, Fixed

Generally the EdgeMarc's Ethernet interfaces should be configured as Full-Duplex, 100Mbps, Fixed (non-autonegotiate). This is very important when connecting to Cisco routers and switches.

The default interface configuration is auto-negotiate. It is only possible to turn off auto negotiation if the other end of the link is a managed device that likewise supports setting its Ethernet interface to FD 100Mbps Fixed. If the device does not offer this, then the EdgeMarc must be left at auto-negotiate.

1. From EdgeMarc GUI click on **System->Set Link**



2. From the bottom part of the page determine if the various EdgeMarc interfaces are auto-negotiating or are fixed, and if they are running as full-duplex or half-duplex.

```
eth0(2): negotiated 100baseTx-FD, link ok
  product info: vendor 00:08:85, model 5 rev 0
  basic mode:   autonegotiation enabled
  basic status: autonegotiation complete, link ok
  capabilities: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
  advertising:  100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD flow-control
  link partner: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
eth0(3): no link
  product info: vendor 00:08:85, model 5 rev 0
  basic mode:   autonegotiation enabled
  basic status: no link
  capabilities: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
  advertising:  100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD flow-control
eth0(4): 100 Mbit, full duplex, link ok
  product info: vendor 00:08:85, model 5 rev 0
  basic mode:   100 Mbit, full duplex
  basic status: link ok
  capabilities: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
  advertising:  100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD flow-control
```

7.19 Verify phone is sending Register messages to EdgeMarc

1. SSH into the EdgeMarc CLI
2. Determine the IP address of the (or a) phone to be examined.
   – This step can be skipped if little other phone activity is occurring on the LAN
3. Capture LAN-side SIP traffic, per **7.23 Capture an EdgeMarc protocol trace**, page **35**.
4. Look for a SIP message from phone to EdgeMarc:
   `<<<<<<<<<<<<<<<sip header stop<<<<<<<<<<<<<<<<<<<<`

```
 [tos 0xb8]
21:52:43.513061 192.168.1.100.5060 > 192.168.1.1.5060:
                from phone IP        to EdgeMarc LAN IP

>>>>>>>>>>>>>>>sip header start>>>>>>>>>>>>>>>>>>
REGISTER sip:192.168.1.1 SIP/2.0
             EdgeMarc IP

Via: SIP/2.0/UDP 192.168.1.100:5060;branch=z9hG4bK015ce041
From: sip:7202664646@192.168.1.1
To: sip:7202664646@192.168.1.1
Call-ID: 00036b54-c4440002-237eb191-79b72c37@192.168.1.100
```

7.20 Verify EdgeMarc is forwarding Register response to phone

1. SSH into the EdgeMarc CLI
2. Perform steps in **7.19 Verify phone is sending Register messages to EdgeMarc**.
3. Capture LAN-side SIP traffic, per **7.23 Capture an EdgeMarc protocol trace**, page 35.
4. Look for a SIP message from EdgeMarc back to phone:

```
<<<<<<<<<<<<<<<sip header stop<<<<<<<<<<<<<<<<<<
 [tos 0x60]
21:52:43.705579 192.168.1.1.5060 > 192.168.1.100.5060:
                from EM LAN IP     to phone IP
>>>>>>>>>>>>>>>sip header start>>>>>>>>>>>>>>>>>>
SIP/2.0 200 OK
expect 200 OK
Via: SIP/2.0/UDP 192.168.1.100:5060;branch=z9hG4bK015ce041
Record-Route: <sip:7202664646@192.168.1.1;lr>
expected line, added by EdgeMarc
From: <sip:7202664646@192.168.1.1>
To: <sip:7202664646@192.168.1.1>
Call-ID: 00036b54-c4440002-237eb191-79b72c37@192.168.1.100
```

7.21 Verify EdgeMarc is forwarding Register to softswitch

1. Perform steps in **7.19 Verify phone is sending Register messages to EdgeMarc**.
2. Capture WAN-side SIP traffic, per **7.23 Capture an EdgeMarc protocol trace**, page **35**.

3. Look for a SIP message from EdgeMarc to softswitch:

```
<<<<<<<<<<<<<<<sip header stop<<<<<<<<<<<<<<<<<<<
 (DF)
22:36:57.935750 64.186.171.70.5060 > 63.123.133.23.5060:
                from EM WAN IP       to S/S IP

>>>>>>>>>>>>>>>sip header start>>>>>>>>>>>>>>>>>>
REGISTER sip:cps.onvoip.net:5060 SIP/2.0
             value on VoIP ALG->SIP page

Via: SIP/2.0/UDP 64.186.171.70:5060;branch=z9hG4bK5a7a5035
Record-Route: <sip:7202664646@64.186.171.70;lr>
expected line, added by EdgeMarc

From: <sip:7202664646@cps.onvoip.net:5060>
To: <sip:7202664646@cps.onvoip.net:5060>
Call-ID: 00036b54-c4440002-237eb191-79b72c37@192.168.1.100
         will match value originally sent by phone
```

7.22 Verify softswitch is sending Register response to EM

1. Perform steps in **7.21 Verify EdgeMarc is forwarding Register to softswitch**
2. Capture WAN-side SIP traffic, per **7.23 Capture an EdgeMarc protocol trace**, page **35**.
3. Look for a SIP message from EdgeMarc to softswitch:

```
<<<<<<<<<<<<<<<sip header stop<<<<<<<<<<<<<<<<<<<
 [tos 0xb8]
22:36:57.984575 63.123.133.23.64558 > 64.186.171.70.5060:
>>>>>>>>>>>>>>>sip header start>>>>>>>>>>>>>>>>>>
SIP/2.0 200 OK
Expect 200 OK

Via:SIP/2.0/UDP 64.186.171.70:5060;branch=z9hG4bK5a7a5035
From:<sip:7202664646@cps.onvoip.net:5060>
To:<sip:7202664646@cps.onvoip.net:5060>
Call-ID:00036b54-c4440002-237eb191-79b72c37@192.168.1.100
        will match value originally sent by phone
```

7.23 Capture an EdgeMarc protocol trace

7.23.1 Capture to the CLI console

Capture a protocol trace and display it directly within the SSH session to an EdgeMarc CLI.

1. SSH into the EdgeMarc CLI
2. Type: `tcpdump -ni iface -s 0 [port port_number]`
   - Ex: `tcpdump -ni eth0 -s 0 port 5060`
     Decode SIP traffic from the LAN interface (VLANs not in use)
   - Ex: `tcpdump -ni eth0.500`
     Decode all traffic from VLAN ID 500
   - Ex: `tcpdump -ni hdlc0 -s 0 port 5060`
     Decode SIP traffic from an HDLC WAN interface

More details can be found in the following Knowledgebase article:

Using the tcpdump command (#90642)
This article includes the valid values for *iface*.

Note: It is not recommended to decode all traffic on a busy production box in this manner. It could impact call (audio) performance.

7.23.2 Capture to a pcap file

Capture a protocol trace to a pcap file and then transfer it to a PC for Ethereal analysis.

1. SSH into the EdgeMarc CLI
2. Type: `mkdir /var/ramdisk`
3. Type: `mount -t tmpfs tmpfs /var/ramdisk -o size=4000k`
4. Type: `cd /var/ramdisk`
5. Type: `tcpdump -ni iface -s 0 [port port_number] –w myfile.pcap`

To perform tcpdumps on two interfaces at the same time, either:

- Background the tcpdump:
  - Append an "&" to the end of the command line.
    Ex: `tcpdump -ni eth1 -s 0 port 5060 -w myfile.pcap &`
  - Start a second tcpdump similarly
  - Stop the tcpdump(s) later by typing: `killall tcpdump`
- Open two SSH sessions and execute a tcpdump separately in each
  - Both tcpdumps should write a file to /var/ramdisk. Use unique filenames for each, of course.

More details can be found in the following Knowledgebase articles:

Create a RAM Drive to capture large tcpdumps (#151062)
Capture tcpdump to a file (#96589)
Using the tcpdump command (#90642)

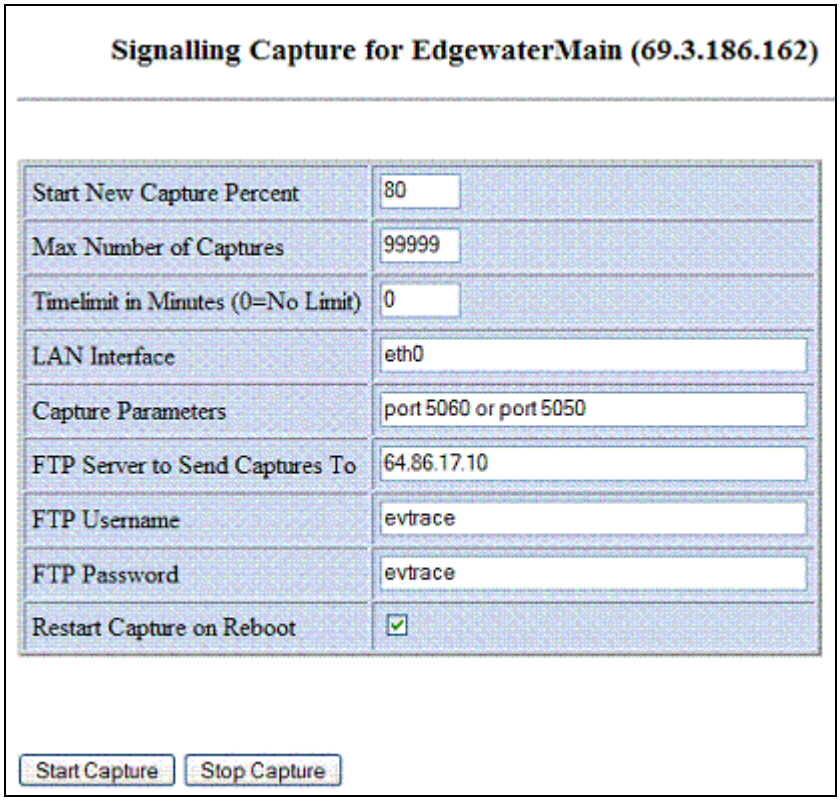
7.24 Activate continuous signaling capture to EdgeView

Use EdgeView to direct an EdgeMarc to capture and send signaling traces to EdgeView. Those traces are matched with an EdgeMarc's MOS scores to produce a by-call signaling capture.

The following steps assume that the EdgeMarc in question is already configured within the EdgeView network management system.

1. From EdgeView, click on the EdgeMarc for which signaling traces are to be captured.
2. Click on **Signaling Capture**.
3. Start signaling capture using default parameter values with the following exceptions:
   - Max number of captures: 9999
   - LAN Interface: Usually **eth0**. Add vlan number if VLANs are in use, ex. **eth0.500**

– Restart Capture on Reboot: Checked



4. Click **Start Capture**

7.25 Find and download specific signaling capture from EdgeView

1. From EdgeView, click on the EdgeMarc for which signaling traces are being captured.
2. Click on **Signaling Analysis**.
3. Click on the drop-down and determine if a signaling trace has been uploaded for the time specified by the customer.
   a. Do not forget to convert the customer's reported time into GMT when looking for capture files.
   b. If the trace is not yet available, then:
      i. From the EdgeMarc status page click on **Signaling Capture**
      ii. Stop the signaling capture.
      iii. Allow 30-60 seconds for the capture files to be uploaded to the EdgeMarc
      iv. Restart the signaling capture.
4. Select the capture file that overlaps with the time of the failure event.
5. Download that pcap capture file.

7.26 Upload a file from EdgeMarc to PC

There are multiple ways of getting a file from the EdgeMarc to a PC.

7.26.1 Text-based file

For text-based files it is often easiest to use cut-and-paste, as follows:

1. SSH into the EdgeMarc CLI
2. Ensure your SSH terminal as a sufficiently large scrollback buffer to capture the file you're intending to transfer.
3. Type: `cat /path/filename`
4. Using your SSH software select and copy the text displayed.
   - "**PuTTY**" version SSH software offers a "copy all to clipboard" function from its upper-left menu pulldown.

7.26.2 Binary file

Two techniques are available: FTP and in-band via zModem protocol.

7.26.2.1 Using FTP

7.26.2.1.1 Customer-provided FTP server

Using a customer-provided public FTP server:

1. Type: `cd /path_to_file`
2. Type: `ftp your_ftp_server`
3. Put the file onto your server

7.26.2.1.2 Using EdgeView's built-in FTP server

EdgeView has a built-in FTP server that is used for capturing signaling traces. You may reuse this FTP server to upload a file.

1. Type: `cd /path_to_file`
2. Type: `ftp your_edgeview_server`
3. Login:
   a. Username (default): **evtrace**
   b. Password (default): **evtrace**
4. Put the file onto the server
5. Log into the server from your PC using a standard FTP client
6. Download the file to your PC

7.26.2.2 Using in-band Zmodem protocol

VOS supports the Zmodem protocol for the in-band transfer of binary data between a CLI session and a PC running a Zmodem-capable program. One such program is Windows' HyperTerminal.

Using, for example, HyperTerminal, it is possible to Telnet to an EdgeMarc and then within the Telnet session itself transfer a file, such as a pcap tcpdump capture directly to your PC. This avoids the steps of FTPing the capture to a public server and then downloading the capture to your PC.

1. Log in to the EdgeMarc appliance using a Zmodem-capable client, such as HyperTerminal. This can be another login in addition to your SSH session, if your SSH client does not support Zmodem (as is the case with PuTTY, for example).
2. Type: `cd /path_to_file`
3. Type: `lsz filename1 [filename2…]`.
   – Example: `lsz eth0.pcap eth1.pcap`
4. Perform the steps necessary to cause your Zmodem-capable client to begin a file upload. In the case of HyperTerminal, the client will automatically recognize and upload the named files.

Note 1: You may see some characters remaining on the screen. This is normal and does not impact the transfer or the CLI.

Note 2: The HyperTerminal program will not erase an already-existing file in the PC destination directory.

7.27 Verify interfaces have no layer-2 frame errors

1. From the EdgeMarc GUI click on **System -> Network Information**.
2. Look in the section labeled **Interface Information**

```
eth0      Link encap:Ethernet  HWaddr 00:C0:02:B8:C9:6E
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10728 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10192 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:256

eth1      Link encap:Ethernet  HWaddr 00:C0:02:B8:C9:6F
          inet addr:64.186.171.70  Bcast:64.255.255.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:755774 errors:0 dropped:0 overruns:0 frame:0
          TX packets:282058 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:256

hdlc0     Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:65.113.32.38  P-t-P:65.113.32.37  Mask:255.255.255.252
          UP POINTOPOINT RUNNING NOARP  MTU:1500  Metric:1
          RX packets:12512220 errors:2 dropped:0 overruns:2 frame:6
          TX packets:12041846 errors:0 dropped:2174 overruns:0 carrier:0
          collisions:0 txqueuelen:50
          Interrupt:28
```

3. Examine the rows beginning **RX packets** and **TX packets**. Look specifically at the **errors, dropped, overruns and frame/carrier** fields.

   Note: You do not need to examine VLAN interfaces, such as **eth0.500**. Only examine the primary LAN Ethernet interface, **eth0**.

4. A non-zero value is not a problem in itself; errors can register when an interface is initially connected and the statistics will not reset. You must refresh the screen and determine if the error values are growing. If they are, then there are layer-2 interface errors that must be addressed.

   Note: The lack of a growing error counter does not guarantee there are no errors. In certain misconfiguration scenarios, such as when one side of the interface is configured for half-duplex and the other side is configured for full-duplex, neither device may register errors even though there is significant packet loss.

7.28 Verify only one DHCP Server is on LAN

1. From EdgeMarc GUI click on **DHCP Server**
2. Temporarily uncheck **Enable DHCP Server**. Click Submit at bottom of page.
3. Click on (the new) **Test for Other DHCP Servers** button at the bottom of the page.
4. The EdgeMarc will respond with whether or not there is another DHCP Server operating on the LAN.
5. Re-enable the EdgeMarc DHCP Server. Click Submit.

7.29 Problem open at end of debug steps

There will be times when the specified debug steps do not resolve your issue. When this occurs you may continue debugging yourself and/or contact Edgewater Network's TAC.

The Edgewater TAC is available to authorized Edgewater resellers. The TAC contact info is:

Email: support@edgewaternetworks.com
Phone: 408.351.7255

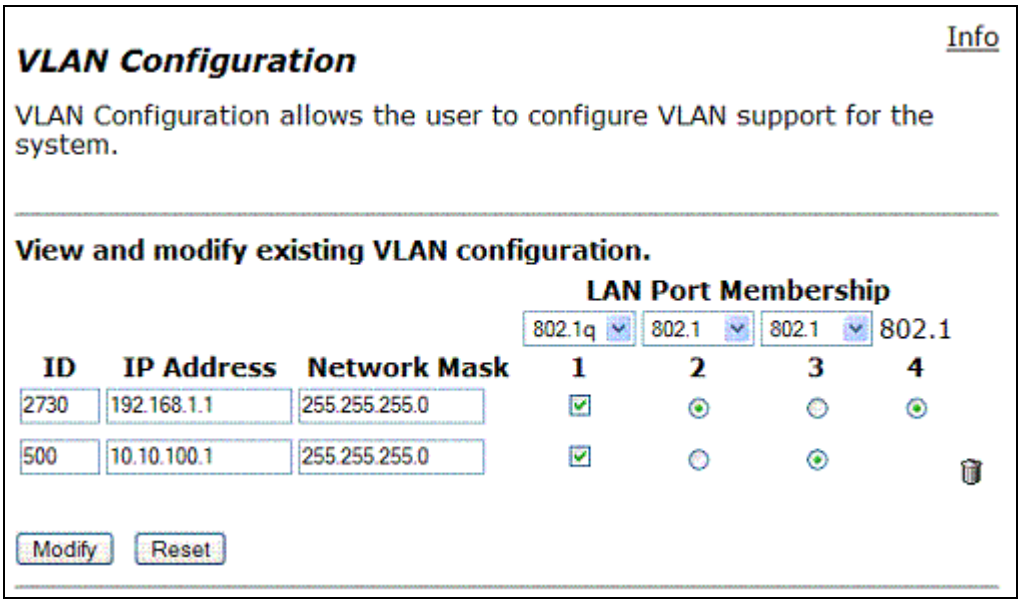
When contacting the TAC be prepared to supply:

- Your company name (must be an Edgewater reseller)
- For an EdgeMarc, the MAC address of the EdgeMarc as shown on the **System** page of the GUI (or eth0 from the CLI)
- The MAC will be used to determine Support eligibility
- Description and Severity of problem
- Debug steps completed

7.30 Verify VLANs are configured properly

1. From the EdgeMarc GUI click on **Network**
2. Under "**LAN Interface Settings:**" verify "**Enable VLAN support**" is checked

3. Click on the "VLAN Settings" hyperlink. (The VLAN page is also reachable from **System->VLAN Configuration**.) The following is displayed:



4. Ensure that tagging (802.1q or 802.1) matches that of the attached devices
5. Ensure that the subnets specified match that of the attached devices

Note: Be aware that an EM-4300's LAN ports do **not** support both 802.1 and 802.1q packets simultaneously. Either one framing type or the other must be used for any given port. Packets not using the tagging mode specified will be dropped by the 4300's internal LAN switch.

7.31 Verify packets are reaching intended VLAN

Verify that IP packets (usually BOOTP, ARP, or ICMP Requests) are reaching the EdgeMarc on the expected VLAN.

1. Follow the steps in **7.30 Verify VLANs are configured properly**, page 40
2. SSH into the EdgeMarc CLI
3. Type: `ifconfig`
   You will see the main Ethernet LAN interface and as well as all the VLAN interfaces, similar to the following:

```
eth0      Link encap:Ethernet  HWaddr 00:C0:02:B8:C9:6E
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1775 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1450 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:256

eth0.500  Link encap:Ethernet  HWaddr 00:C0:02:B8:C9:6E
          inet addr:10.10.100.1  Bcast:10.255.255.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1496  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
```

```
          collisions:0 txqueuelen:0

eth0.2730 Link encap:Ethernet  HWaddr 00:C0:02:B8:C9:6E
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1496  Metric:1
          RX packets:113 errors:0 dropped:0 overruns:0 frame:0
          TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

4. For the VLAN on which the PC or phone is expected to send its traffic, type:
   `tcpdump -nei eth0.nnn arp or icmp or broadcast`
5. From the endpoint in question attempt communication
6. You should see requests to/from the endpoint in question. Use the MAC address displayed to ensure the right endpoint's traffic is being received.

```
# tcpdump -nei eth0.2730 arp or icmp or broadcast
tcpdump: listening on eth0.2730
                 source mac      destination mac
20:00:20.784889 0:3:6b:54:c4:44 ff:ff:ff:ff:ff:ff 0800 367: 0.0.0.0.68 >
255.255.255.255.67: udp 325
20:00:20.789782 0:3:6b:54:c4:44 ff:ff:ff:ff:ff:ff 0806 60: arp who-has
192.168.1.100 tell 192.168.1.100
20:00:20.790297 0:3:6b:54:c4:44 ff:ff:ff:ff:ff:ff 0806 60: arp who-has
192.168.1.1 tell 192.168.1.100
20:00:20.790338 0:c0:2:b8:c9:6e 0:3:6b:54:c4:44 0806 42: arp reply
192.168.1.1 is-at 0:c0:2:b8:c9:6e
```

7. If traffic is not being received from the expected endpoint the likely causes are:
   - A connectivity failure between endpoint, LAN fabric, and EdgeMarc
   - The endpoint's traffic is being delivered on a different VLAN ID
   - The endpoint's traffic is being delivered to the EdgeMarc's LAN port with frame tagging that does not match that configured for the port (802.1 or 802.1q)
8. It is possible to view all traffic being delivered to the LAN interface by using tcpdump and not specifying a VLAN ID.

   Notes:
   - tcpdump filters are not available in this mode.
   - Untagged (802.1) packets sent to tagged (802.1q) port will NOT be shown.

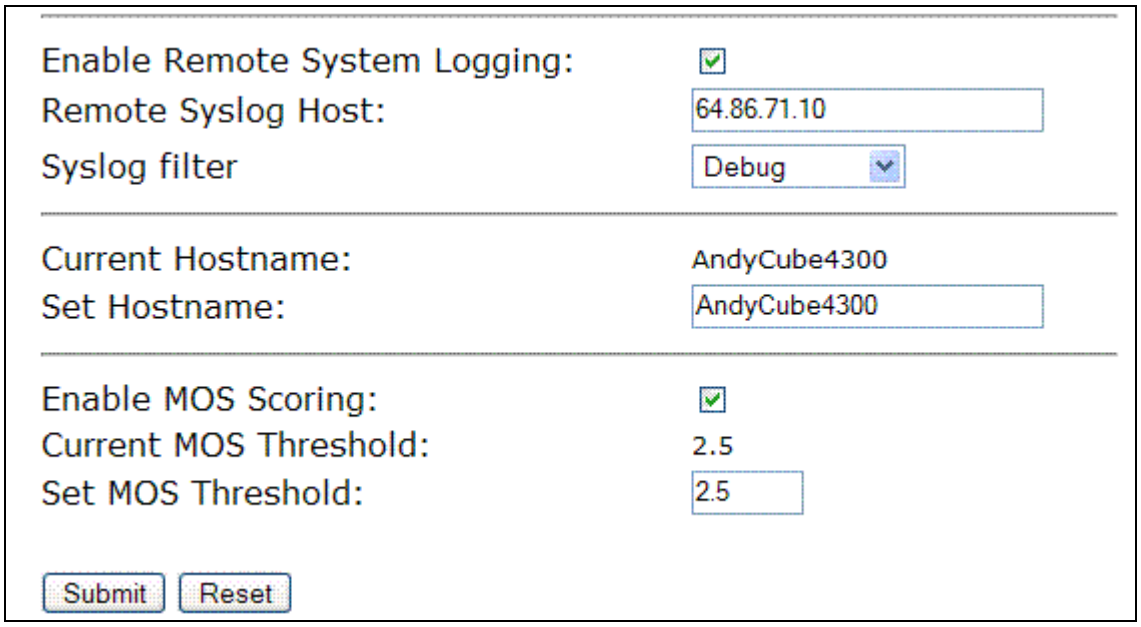
```
# tcpdump -i eth0
                        expected message
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: listening on eth0

                       VLAN tag
22:21:03.343493 802.1Q vlan#2730 P0 1:0:c:cc:cc:cc > 0:3:6b:54:c4:44 snap
I (s=0,r=6,C) len=137
22:21:04.343254 802.1Q vlan#2730 P0 1:0:c:cc:cc:cc > 0:3:6b:54:c4:44 snap
I (s=0,r=6,C) len=137
22:21:05.343255 802.1Q vlan#2730 P0 1:0:c:cc:cc:cc > 0:3:6b:54:c4:44 snap
I (s=0,r=6,C) len=137
22:21:13.751694 802.1Q vlan#2730 P0 0.0.0.0.68 > 255.255.255.255.67: udp
325
22:21:13.754430 802.1Q vlan#2730 P0 192.168.1.1.67 > 255.255.255.255.68:
udp 300 [tos 0x10]
```

```
22:21:13.755713 802.1Q vlan#2730 P0 arp who-has 192.168.1.100 tell
192.168.1.100
22:21:13.756227 802.1Q vlan#2730 P0 arp who-has 192.168.1.1 tell
192.168.1.100
22:21:13.756390 802.1Q vlan#2730 P0 arp reply 192.168.1.1 is-at
0:c0:2:b8:c9:6e
22:21:13.904188 802.1Q vlan#2730 P0 192.168.1.100.50225 >
192.168.1.1.tftp:  [tos 0x10]
22:21:13.914747 802.1Q vlan#2730 P0 192.168.1.1.1030 >
192.168.1.100.50225: udp 19 (DF)
```

7.32 Ensure MOS capture is being performed

Ensure that the EdgeMarc and EdgeView are properly configured to capture and store MOS statistics.

1. Go to the **System->Services Configuration** GUI page:



   - Ensure the syslog is pointing to the EdgeView
   - Ensure a hostname is configured (to aid viewing of the syslog, if necessary)
   - Ensure MOS scoring is enabled and (generally) set the threshold for MOS Below Threshold alerts to 2.5.
2. If any changes needed to be made above, then allow at least one off-site call to be made (either inbound or outbound call)
3. Follow the first 3 steps in 7.14 **Obtain MOS statistics for an EdgeMarc**, page 27, to ensure that MOS scores are being collected by EdgeView.
4. Allow scores to be collected for at least 4 hours of calling before attempting to perform any call-quality analysis based on MOS scores.