EAN-Network Configuration

2021-06-17

Exports: Export Summary Sheet

EULA: End User License Agreement

Web: sightlineapplications.com

Sales: sales@sightlineapplications.com

Support: support@sightlineapplications.com

Phone: +1 (541) 716-5137

⚠ **CAUTION:** Alerts to a potential hazard that may result in personal injury, or an unsafe practice that causes damage to the equipment if not avoided

ⓘ **IMPORTANT:** Identifies crucial information that is important to setup and configuration procedures.

Used to emphasize points or reminds the user of something. Supplementary information that aids in the use or understanding of the equipment or subject that is not critical to system use.

1 Overview

This document describes network management and configuring such as static IP address for the 1500-OEM, 3000-OEM, and 4000-OEM. It additionally covers sending telemetry to multiple IP address destinations. General knowledge of IP addressing is recommended.

1.1 Additional Support Documentation

Additional Engineering Application Notes (EANs) can be found on the Documentation page of the SightLine Applications website.

The Panel Plus User Guide provides a complete overview of settings and dialog windows located in the Help menu of the Panel Plus application.

The Interface Command and Control (IDD) describes the native communications protocol used by the SightLine Applications product line. The IDD is also available as a PDF download on the Documentation page under Software Support Documentation.

1.2 SightLine Software Requirements

ⓘ **IMPORTANT:** The Panel Plus software version should match the firmware version running on the board. Firmware and Panel Plus software versions are available on the Software Download page.

2 Default IP Addressing

Dynamic Host Configuration Protocol (DHCP) is supported on all SightLine OEM systems. This support allows SightLine systems to automatically obtain an Internet Protocol (IP) address. This assignment includes the subnet mask and default gateway.

If a DHCP server is not available on the connected network, each system will then default to a predefined IP address in the Link Local address space.

Table 1: Sightline OEM Default IP Addressing

SightLine Hardware	Predefined IP Address	Subnet Mask	Default Gateway
1500-OEM	169.254.1.180	255.255.0.0	No gateway defined
3000-OEM	169.254.1.181	255.255.0.0	No gateway defined
4000-OEM	169.254.1.182	255.255.0.0	No gateway defined

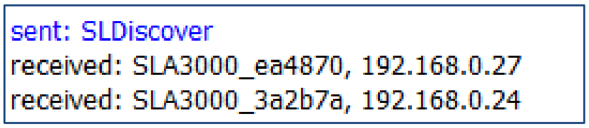
This predefined assignment supports the implemented address block of 169.254.0.0/16.

If a Windows PC starts without a static or DHCP assigned IP address, it will default within this same address block (and subnet).

These addresses are only valid on the link, i.e., as a local network segment or point-to-point connection that a host PC is connected to. These addresses are not routable and cannot be the source or destination of packets crossing the internet.

3 Discover Systems on the Network

When opening the Panel Plus software, it will broadcast an *SLDiscover* packet on the connected network to look for any SightLine OEM systems (see the IDD). All OEM systems that respond will be displayed to the *SightLine Boards* drop-down menu on the *Connect* tab. An example is shown in Figure 1.



```
sent: SLDiscover
received: SLA3000_ea4870, 192.168.0.27
received: SLA3000_3a2b7a, 192.168.0.24
```

Figure 1: SLDiscover Command Sequence

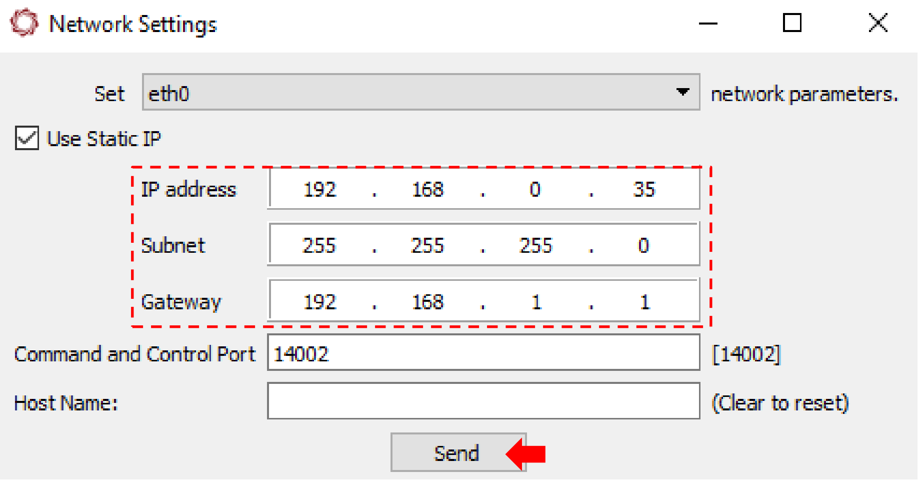
It is important to know the address of the system that you want to connect with and to ensure the host PC is on the same network/subnet:

- The default IP address of the 1500-OEM (when no DHCP server is available) is the local-link address of 169.254.1.180.
- The default IP address of the 3000-OEM (when no DHCP server is available) is the local-link address of 169.254.1.181.
- The default IP address of the 4000-OEM (when no DHCP server is available) is the local-link address of 169.254.1.182.

If the OEM board is not shown see Connection Issues for more information.

4 Define Static IP Address

1. Connect to the board using the Panel Plus application. See the appropriate OEM startup guide for connection instructions.
2. Once connected to the board, from the main menu go to *Configure* » *Network Settings*.
3. Select the checkbox for *Use Static IP*. Enter the IP Address, Subnet, and Gateway address.
4. Click *Send* to update the parameter file.



Network Settings

Set eth0 network parameters.

☑ Use Static IP

IP address 192 . 168 . 0 . 35

Subnet 255 . 255 . 255 . 0

Gateway 192 . 168 . 1 . 1

Command and Control Port 14002 [14002]

Host Name: (Clear to reset)

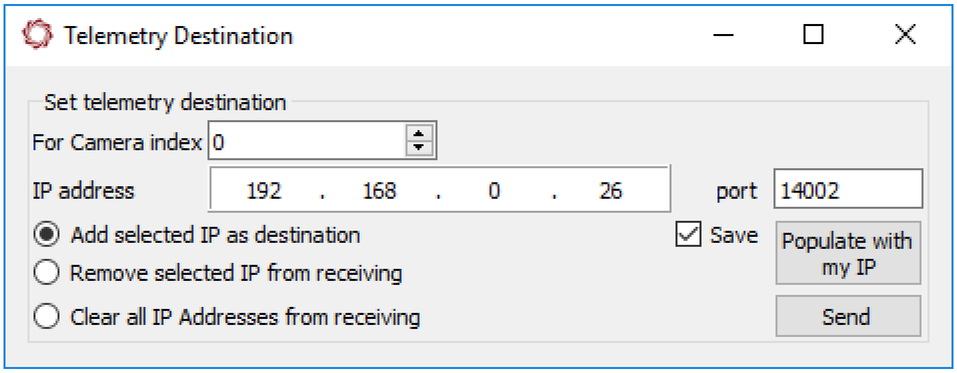
5. Save and activate the settings:
    a. Main menu » *Parameters* » *Save to Board*.
    b. Main menu » *Reset* » *Board*.
    c. After the system reboots reconnect to the board. Make sure the board connects.
6. After rebooting the board will now have the newly assigned IP address.

Make sure to change the IP address on the host PC to an address on the same logical subnet.

5 Telemetry Destination IP Addresses

The destination IP address for telemetry will typically be the IP address of the gimbal control system, the autopilot program, or Ground Control Station.

1. From the main menu in Panel Plus go to *Configure* » *Telemetry Destination*
2. In the Telemetry Destination dialog window, select the camera index number. This will be the source camera for the pixel telemetry.
3. Set the destination IP address and port. Telemetry is sent as a UDP packet, and the port will be a listening UDP port on the remote system.
4. Select the *Add selected IP as destination*, and then click *Send*. Up to five telemetry destinations may be added.


Telemetry Destination

Set telemetry destination

For Camera index: 0

IP address: 192 . 168 . 0 . 26

port: 14002

● Add selected IP as destination

○ Remove selected IP from receiving

○ Clear all IP Addresses from receiving

☑ Save

To enter additional telemetry destination after the maximum (5) has been reached, a destination IP address will need to be removed. Use the Remove selected IP from receiving and then click Send.

To clear all the telemetry destination IP addresses, select Clear all IP Addresses from receiving and then click Send.

5. From the main menu, go to *Parameters* » *Save to board*.
6. From the main menu, go to *Reset* » *Board* or power cycle the board.
7. Wait for the system to boot, and then reconnect to the board.

6 Connection Issues

Panel Plus uses a broadcast message (255.255.255.255) to query the network for SightLine units. This allows for discovery and response across separate networks. Panel Plus will still discover the hardware and will display a warning about the hardware not being on the same network. If the problem persists, try connecting the PC to the SightLine hardware directly using a network cable to remove any problems that may be caused by network switches or routers blocking certain types of network traffic.

6.1 Network Switch

A powered network switch between the PC and SightLine video processing boards are recommended for bench testing. Without a powered switch, when the 1500-OEM / 3000-OEM / 4000-OEM is power cycled, the PC may lose its network. It can take up to three minutes for windows to reestablish its network connection, which can cause a DHCP timeout. This is not an issue if the PC is assigned a static IP address.

6.2 Netmask

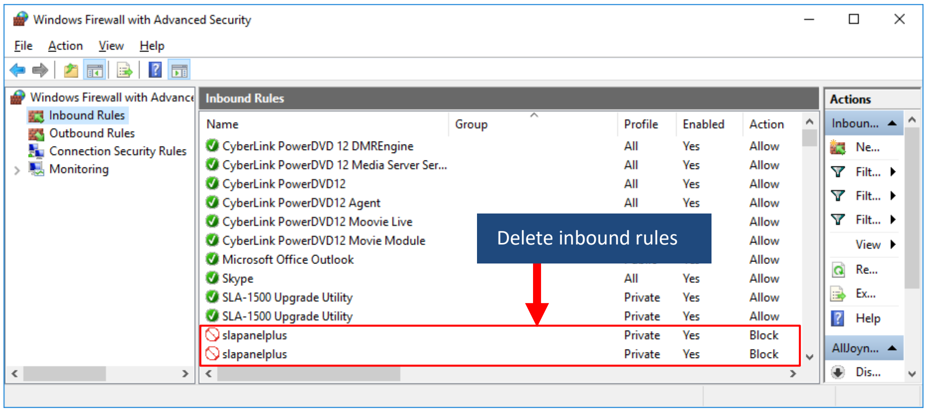
If there is a network mask mismatch between the host PC and the 1500-OEM / 3000-OEM / 4000-OEM, Panel Plus will report this problem when connecting to the SightLine hardware.

For most networks, 255.255.255.0 is the correct netmask. For link-local networks in the 169.254.0.0/16 range, 255.255.0.0 is the correct netmask.

6.3 Windows Firewall

Failure to allow access in the Windows Security Alert prompt upon initial startup of the Panel Plus application can cause connection issues.

1. Close the Panel Plus software application and open the Window Firewall Security Manager on the host PC.
2. Go to *Inbound Rules* and delete the two *slapanelplus* rules (TCP and UDP).
3. Re-start the Panel Plus application and allow access in the Windows Security Alert prompt window.



Inbound Rules

Name	Group	Profile	Enabled	Action
CyberLink PowerDVD 12 DMREngine		All	Yes	Allow
CyberLink PowerDVD 12 Media Server Ser...		All	Yes	Allow
CyberLink PowerDVD12		All	Yes	Allow
CyberLink PowerDVD12 Agent		All	Yes	Allow
CyberLink PowerDVD12 Moovie Live				Allow
CyberLink PowerDVD12 Movie Module				Allow
Microsoft Office Outlook				Allow
Skype		All	Yes	Allow
SLA-1500 Upgrade Utility		Private	Yes	Allow
SLA-1500 Upgrade Utility		Private	Yes	Allow
slapanelplus		Private	Yes	Block
slapanelplus		Private	Yes	Block

Delete inbound rules

6.4 Serial Connection

Many network connection issues are related to either cabling, IP addresses conflicts, or subnets not matching properly.

A serial port can be used for troubleshooting if a network connection cannot be established.

The Panel Plus software will automatically recognize serial ports and list them in the drop-down menu for available connections.

See the Serial Communications section in the appropriate OEM startup guide for setting up a serial connection in Panel Plus.

ⓘ **IMPORTANT:** If connecting to the serial port on the 1500-OEM or 3000-OEM from a host PC, the connection may require a null modem serial cable or adapter for proper communications. The pinout for this cable can be found in the ICD-1500-OEM, the ICD-3000-OEM, or ICD-4000-OEM.

For additional issues and support, please contact Support.

6.5 Change Panel Plus Network Interface Metric

Panel Plus connection issues occur when multiple network interface controllers (NICs) exist on a PC. Network interface metrics can be changed to allow the use of a wireless adapter for general internet access (web browsing, etc.) and allow Panel Plus to use a local LAN (hard wired interface) connection to the SightLine system.

The Network Sharing user interface will vary based on the Windows version.

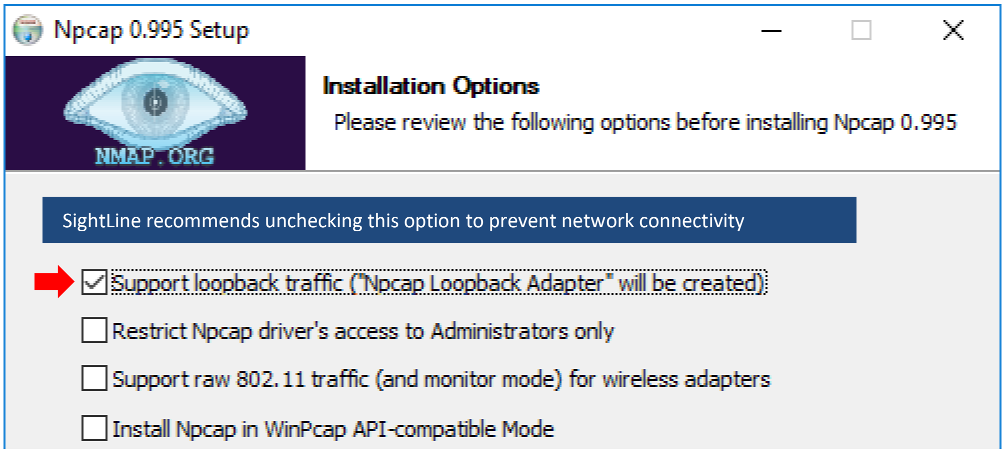
To change the network interface metric:

1. Go to the *Network Sharing Center* in Windows. It is in the Control Panel in all versions of Windows.
2. Click on *Change Adapter Settings*.
3. Right click on the local area network adapter and select properties.
4. Click on Internet *Protocol Version 4 (TCP/IPv4)*, and then click on *Properties*.
5. Click on *Advanced*.
6. Uncheck the *Automatic metric* check box. Set the interface metric to 1. A low number designates this adapter. Click *OK* in the dialog windows and close.
7. Select a new wireless adapter and repeat the process above. Set the interface metric higher than 999.
8. Disable and re-enable the adapters (or reboot PC) for the settings to take effect.

6.6 Npcap/WinPcap Virtual Loopback Adapter

Npcap and WinPcap are both Windows implementations of the libpcap packet capture library. Install either one to capture network traffic with Wireshark. The installer for Wireshark 3.0 and later versions includes Npcap, and older releases include WinPcap.

Both Npcap and WinPcap create a virtual loopback network adapter as a default install option. The loopback adapter is used for capturing packets between services on the host PC. It is not needed to capture other traffic.



Npcap 0.995 Setup

Installation Options

Please review the following options before installing Npcap 0.995

SightLine recommends unchecking this option to prevent network connectivity

☑ Support loopback traffic ("Npcap Loopback Adapter" will be created)

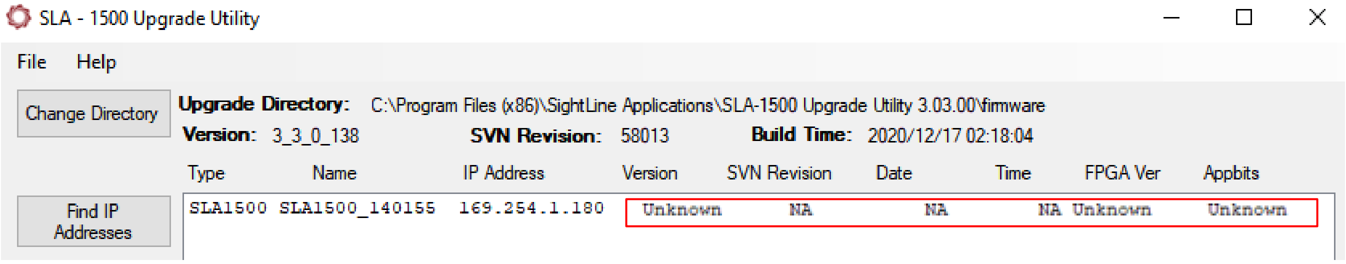
□ Restrict Npcap driver's access to Administrators only

□ Support raw 802.11 traffic (and monitor mode) for wireless adapters

□ Install Npcap in WinPcap API-compatible Mode

Figure 2: Npcap Virtual Loopback Adapter Install Option

Typically, Panel Plus and the firmware upgrade utility applications do not recognize virtual adapters. However, virtual loopback adapters created by Npcap and WinPcap are recognized because they are incorrectly identified to the host operating system as physical adapters. This can cause connectivity issues and unexpected behavior when applications attempt to communicate through the loopback adapter (Figure 3).



SLA - 1500 Upgrade Utility

Upgrade Directory: C:\Program Files (x86)\SightLine Applications\SLA-1500 Upgrade Utility 3.03.00\firmware

Version: 3_3_0_138 **SVN Revision:** 58013 **Build Time:** 2020/12/17 02:18:04

Type	Name	IP Address	Version	SVN Revision	Date	Time	FPGA Ver	Appbits
SLA1500	SLA1500_140155	169.254.1.180	Unknown	NA	NA	NA	Unknown	Unknown

Figure 3: Virtual Loopback Adapter Connectivity Issue

If loopback traffic capture is required for a particular use case, SightLine recommends disabling the Npcap/Winpcap virtual adapter when using Panel Plus, the firmware upgrade utility, VLC and other applications connecting to the board. The loopback adapter can be disabled from the host PC under:

- *Settings* » *Network and Internet* » *Ethernet* » *Change adapter options*
- *Control Panel* » *All Control Panel Items* » *Network Connections* (ncpa.cpl), or
- Winkey (⊞) + R » *devmgmt.msc* » Device Manager.

6.6.1 Uninstall Virtual Loopback Adapter

The virtual loopback adapter can be removed without uninstalling Npcap/WinPcap.

1. Press Winkey (⊞) + R to open a Run prompt.
2. Enter *devmgmt.msc* to open the Device Manager.
3. Expand *Network adapters* in the device tree.
4. Right click *Npcap Loopback Adapter* and select *Uninstall*. Click the *Uninstall* button when prompted.

7 Advanced Networking Tip and Techniques

SightLine OEM products run a version of embedded Linux on the ARM processor. Many network services and capabilities can be accessed. Additional functionality (such as Ethernet to serial passthrough) can be accomplished with the Panel Plus software interface.

7.1 Terminology

SightLine hardware	General purpose term to describe any OEM product sold by SightLine
Target	Refers to the Linux Kernel running on SightLine hardware
Host	Refers to the host PC used to interface with SightLine hardware
root@slaNNNN#	Linux command prompt on target, where NNNN is either 1500 or 3000
$	Linux command prompt on host

Prior to firmware release 2.25.xx the 1500-OEM command prompt was DM-37x# shown in some screen captures in the subsequent sections.

When making changes to the 3000-OEM filesystem (Example: passwd) remount the filesystem with write access. From the root@sla3000:~# prompt, type:

```
mount -w -o remount /
```

7.2 Tool Summary

Table 2: Tool Summary

Utility	Description
SSH (Secure Shell)	Allows users to logon to target and execute commands
FTP	Allows users to move files from host to target
SCP (Secure Copy)	Used to transfer files from host to target
TC (Traffic Control)	Used to modify the flow of Ethernet packets
VCONFIG	Create and remove virtual Ethernet devices (VLAN)
NETSTAT	Used to display networking information such as open ports
ROUTE	Used to create route tables
IFCONFIG	Used to configure network interfaces
IP	Used to configure network interfaces (4000-OEM)
ETHTOOL	Used to modify Ethernet interface parameters
IPERF	Industry standard network performance measurement tool
PING	Used to test reachability of systems on the network.

7.3 Third Party Utilities

Use of third-party support tools and utilities are integral to the integration and support of SightLine products. SightLine Applications offers the links shown below as a convenience. Users that download third party tools do so at their own risk and are bound to the usage agreements contained for each product.

There are many tools and utilities that are available on the web that provide identical functionality. Developers should use the tools that works best for their application.

FTP - FileZilla	FTP client utility
Tera Term	Recommend SSH client to connect SightLine OEM systems.
Wireshark	Network protocol analyzer

7.4 Usernames and Passwords

SightLine uses the following conventions for usernames and passwords shown in Table 3.

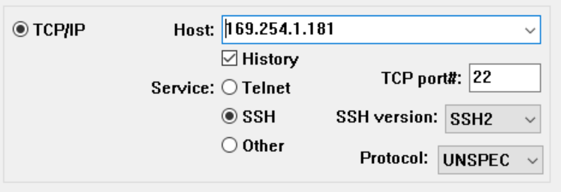
Table 3: Username and Passwords

System	Username	Password
Target Hardware	*root*	*root*
Host (PC)	*slroot*	*slroot*

7.5 Change Target Default Password

ⓘ **IMPORTANT:** Use discretion when performing this operation. Some SightLine documentation and software such as Panel Plus assumes *root* is used as the default username and password. Changing this default behavior may render some operations unavailable.

1. Open a terminal emulator and establish an SSH session to the target.

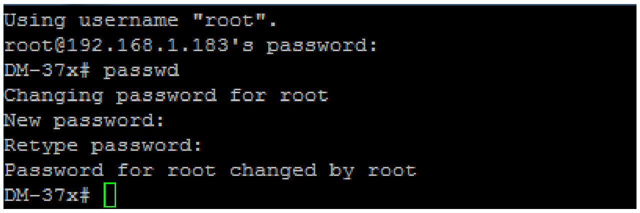


● TCP/IP Host: 169.254.1.181
☑ History
Service: ○ Telnet TCP port#: 22
● SSH SSH version: SSH2
○ Other Protocol: UNSPEC

2. Login using the default username and password:
   - 1500-OEM and 3000-OEM: *root*
   - 4000-OEM: *slroot*
3. At the command prompt, type:

```
passwd
```

4. Enter a new password and follow the prompts. Use characters and numbers to create a strong password.

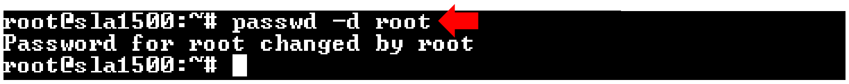


```
Using username "root".
root@192.168.1.183's password:
DM-37x# passwd
Changing password for root
New password:
Retype password:
Password for root changed by root
DM-37x#
```

7.6 Remove Passwords

The utility *passwd* can also be used to remove a password. Type:

```
# passwd -d root
```



```
root@sla1500:~# passwd -d root
Password for root changed by root
root@sla1500:~# 
```

7.7 Default Inbound SSH Port

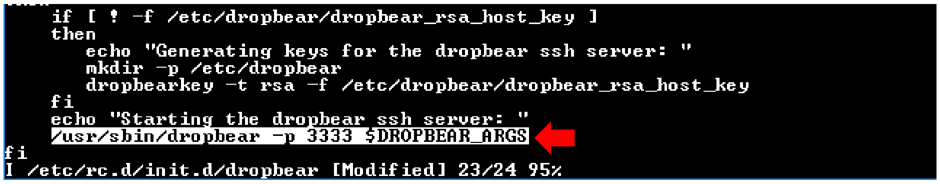
SightLine systems listen for incoming SSH connections on port 22 by default. The inbound SSH port may be changed by editing the *dropbear* SSH server configuration file.

7.7.1 1500-OEM - Changing the Inbound SSH Port

1. Open a terminal emulator and establish an SSH session to the target.
2. From the *DM-37x#* prompt, type:

   ```
   vi /etc/rc.d/init.d/dropbear
   ```

3. Press the (I) key to enter insert mode.
4. Insert `-p port` between `/usr/sbin/dropbear` and `$DROPBEAR_ARGS` in the second to last line. Port 3333 is used in the example below:

   ```
       if [ ! -f /etc/dropbear/dropbear_rsa_host_key ]
       then
          echo "Generating keys for the dropbear ssh server: "
          mkdir -p /etc/dropbear
          dropbearkey -t rsa -f /etc/dropbear/dropbear_rsa_host_key
       fi
       echo "Starting the dropbear ssh server: "
       /usr/sbin/dropbear -p 3333 $DROPBEAR_ARGS
   fi
   I /etc/rc.d/init.d/dropbear [Modified] 23/24 95%
   ```

5. Press the *Escape* key, and then type:

   ```
   :wq
   ```

6. Press the *Enter* key to save the file and exit the vi editor.
7. From the *DM-37x#* prompt, type:

   ```
   reboot
   ```

8. Once the board has rebooted establish an SSH session via the specified port to verify the change.
9. Optional: from the *DM-37x#* prompt enter `netstat -l` to view active connections. `(null):port` should appear in the under the local address column with the state `LISTEN`.

7.7.2 3000-OEM - Changing the Inbound SSH Port

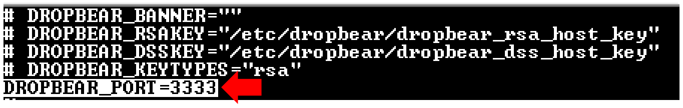
1. Open a terminal emulator and establish an SSH session to the target.
2. Remount the filesystem with write access. From the *root@sla3000:~#* prompt, type:

   ```
   mount -w -o remount /
   ```

3. From the *root@sla3000~#* prompt, type:

   ```
   vi /etc/default/dropbear
   ```

4. Press the (I) key to enter insert mode.
5. Add a new line containing `DROPBEAR_PORT=port` to the end of the file. Port 3333 is used in this example:



```
# DROPBEAR_BANNER=""
# DROPBEAR_RSAKEY="/etc/dropbear/dropbear_rsa_host_key"
# DROPBEAR_DSSKEY="/etc/dropbear/dropbear_dss_host_key"
# DROPBEAR_KEYTYPES="rsa"
DROPBEAR_PORT=3333
```

6. Press the *Escape* key, and then type:

```
:wq
```

7. Press the *Enter* key to save the file and exit the vi editor.
8. From the *root@sla3000~#* prompt, type:

```
reboot
```

9. Once the board has rebooted, establish an SSH session via the specified port to verify the change.
10. Optional: To view active connections from the *root@sla3000~#* prompt, type:

```
netstat -l
```

`null):port` should appear in the under the local address column with the state `LISTEN`.

7.7.3 4000-OEM - Changing the Inbound SSH Port

SSH port configuration on the 4000-OEM is not supported.

7.8 Assign Multiple IP Addresses to Single NIC

It is possible to route specific traffic to different networks. This process is referred to as multihome. In this example, the target has the existing IP address of *192.168.1.183*. The other network segment has an IP address of *192.168.0.42*.

1. Open a terminal emulator and establish an SSH session to the target.
2. To view the current settings, type:

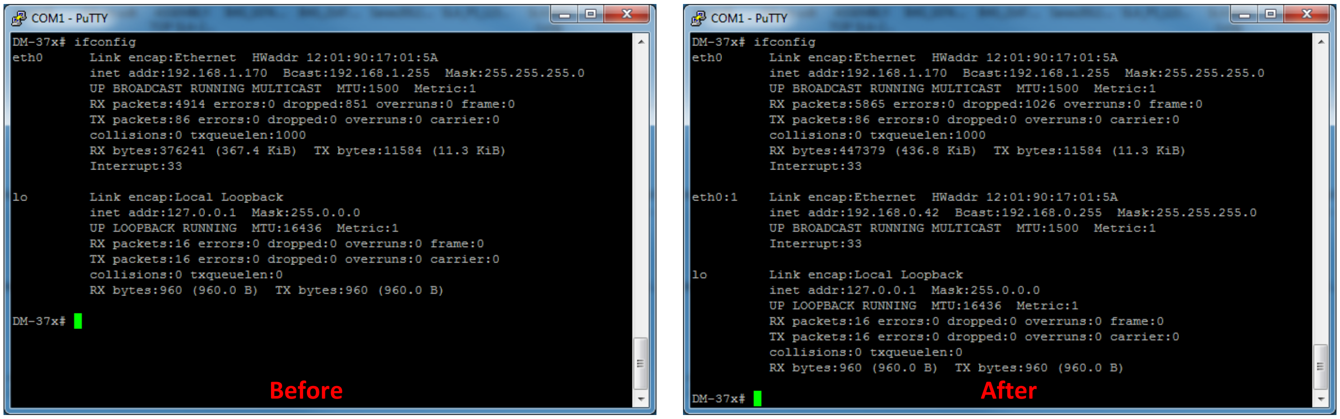
```
ifconfig
```

3. To add another IP, type:

```
ifconfig eth0:1 192.168.0.42 netmask 255.255.255.0 multicast up
```

Both IP addresses (192.168.1.183 and 192.168.0.42) are now accessible on the LAN.

eth0:1 can be changed as needed to match your system. For example, eth0:1 is already in use on the 3000-OEM, therefore eth0:2 or similar can be used. On 4000-OEM the adapter name is enP2p1s0.



```
DM-37x# ifconfig
eth0      Link encap:Ethernet  HWaddr 12:01:90:17:01:5A
          inet addr:192.168.1.170  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4914 errors:0 dropped:851 overruns:0 frame:0
          TX packets:86 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:376241 (367.4 KiB)  TX bytes:11584 (11.3 KiB)
          Interrupt:33

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:960 (960.0 B)  TX bytes:960 (960.0 B)

DM-37x#
```

Before

```
DM-37x# ifconfig
eth0      Link encap:Ethernet  HWaddr 12:01:90:17:01:5A
          inet addr:192.168.1.170  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5865 errors:0 dropped:1026 overruns:0 frame:0
          TX packets:86 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:447379 (436.8 KiB)  TX bytes:11584 (11.3 KiB)
          Interrupt:33

eth0:1    Link encap:Ethernet  HWaddr 12:01:90:17:01:5A
          inet addr:192.168.0.42  Bcast:192.168.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:33

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:960 (960.0 B)  TX bytes:960 (960.0 B)
DM-37x#
```

After

Figure 4: Routing Specific Traffic to Different Networks

7.9 Add and Configure VLAN

1500-OEM:

This example can be found in *…/scripts/sla_vlan.sh*. It can be added to the */etc/rc.d/rc.local* for the 1500-OEM.

Alternate option: Modify */etc/network/interfaces* so that this configuration is created on startup.

1. Establish an SSH session to the target.
2. Type:

	Reason:
`vconfig add eth0 5`	Add VLAN ID 5
`ifconfig eth0.5`	To see the VLAN
`ifconfig eth0.5 192.168.42.100 netmask 255.255.255.0 broadcast 192.168.42.255 up`	To add an IP address for the VLAN
`cat /proc/net/vlan/eth0.5`	To check the status

4000-OEM:

This example can be found in *…/scripts/sla_vlan.sh***.** It can be added to the *sla_init.sh* or *vt_start.sh* scripts.

1. Establish an SSH session to the target.
2. Type:

	Reason:
`sudo modprobe 8021q`	Load the 802.1q module
`sudo ip link add link enP2p1s0 name enP2p1s0.5 type vlan id 5`	Add VLAN ID 5
`ip -d link show enP2p1s0.5`	To see the VLAN
`sudo ip addr add 192.168.42.100/24 brd 192.168.1.255 dev enP2p1s0.5`	To add an IP address for the VLAN
`sudo ip link set dev enP2p1s0.5 up`	Enable the interface
`cat /proc/net/vlan/eth0.5`	To check the status

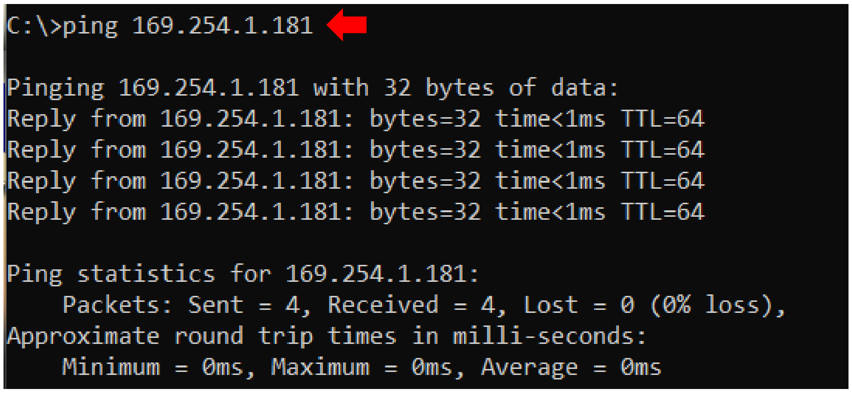
7.9.1 Remove VLAN

1. Establish an SSH session to the target.
2. Type:

```
ifconfig eth0.5 down
vconfig rem eth0.5
```

7.10 Ping Utility (ICMP)

The Ping utility can be used to test the reachability of the target hardware on the network from the PC command line. The example in Figure 5 shows a Ping test from the PC to the 3000-OEM.



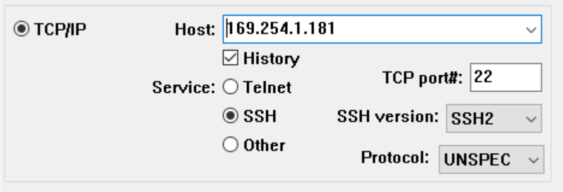
```
C:\>ping 169.254.1.181

Pinging 169.254.1.181 with 32 bytes of data:
Reply from 169.254.1.181: bytes=32 time<1ms TTL=64
Reply from 169.254.1.181: bytes=32 time<1ms TTL=64
Reply from 169.254.1.181: bytes=32 time<1ms TTL=64
Reply from 169.254.1.181: bytes=32 time<1ms TTL=64

Ping statistics for 169.254.1.181:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 5: Ping 3000-OEM Test Example From PC

The Ping command can also be used from the SightLine hardware to test the reachability of other devices, e.g., a PC, using a terminal emulator program.

The following example shows how to perform a Ping test to the PC from the 3000-OEM.

1. Open a terminal emulator and establish an SSH session to the target.



● TCP/IP Host: 169.254.1.181

☑ History

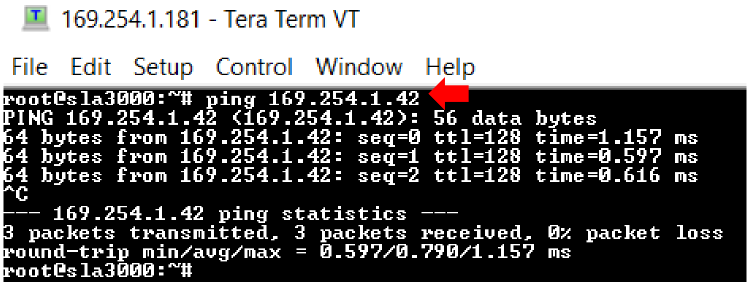
Service: ○ Telnet TCP port#: 22

● SSH SSH version: SSH2

○ Other Protocol: UNSPEC

2. At the command prompt, type in the Ping command and IP address of the PC.

```
root@sla3000:~# ping 169.254.1.42
```


169.254.1.181 - Tera Term VT
File Edit Setup Control Window Help

```
root@sla3000:~# ping 169.254.1.42
PING 169.254.1.42 (169.254.1.42): 56 data bytes
64 bytes from 169.254.1.42: seq=0 ttl=128 time=1.157 ms
64 bytes from 169.254.1.42: seq=1 ttl=128 time=0.597 ms
64 bytes from 169.254.1.42: seq=2 ttl=128 time=0.616 ms
^C
--- 169.254.1.42 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.597/0.790/1.157 ms
root@sla3000:~#
```

Figure 6: Ping PC Test Example From 3000-OEM

7.11 Traffic Control (tc)

This example can be found in *…/scripts/sla_runtc.sh*. It can be added to the */etc/rc.d/rc.local* for the 1500-OEM or *…/sla3000_init.sh* for the 3000-OEM. For the 4000-OEM it can be added to the *sla_init.sh* or *vt_start.sh scripts*.

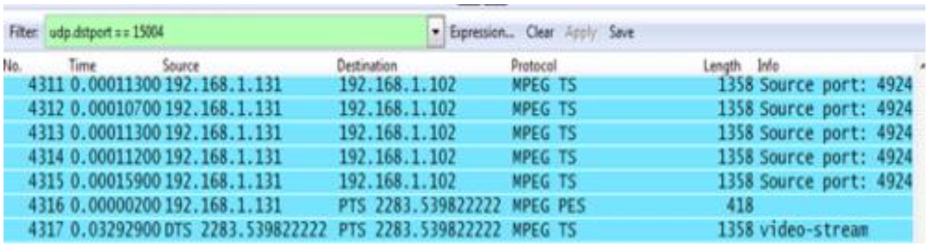
Traffic control (tc) can be used to normalize the rate that packets are transmitted preventing massive peaks when using IP radios or similar.

ⓘ **IMPORTANT:** Not all traffic shaping/policing methods are supported on all OEM platforms. Please contact Support for additional assistance.

In this example, the target will be configured to transmit video, and then the packet formation will be adjusted.

The following steps reference the Panel Plus software.

1. Connect to target using Panel Plus.
2. Set up for Network Output.
3. Configure MPEG2-TS + H.264 video streaming.
4. Click *Send*. The target should now be streaming video.
5. Start Wireshark.
6. From the main menu go to *Capture* » *Interfaces.*
7. Filter the H.264 packets that are going to port 15004.



Filter: udp.dstport == 15004

No.	Time	Source	Destination	Protocol	Length	Info
4311	0.00011300	192.168.1.131	192.168.1.102	MPEG TS	1358	Source port: 4924
4312	0.00010700	192.168.1.131	192.168.1.102	MPEG TS	1358	Source port: 4924
4313	0.00011300	192.168.1.131	192.168.1.102	MPEG TS	1358	Source port: 4924
4314	0.00011200	192.168.1.131	192.168.1.102	MPEG TS	1358	Source port: 4924
4315	0.00015900	192.168.1.131	192.168.1.102	MPEG TS	1358	Source port: 4924
4316	0.00000200	192.168.1.131	PTS 2283.539822222	MPEG PES	418	
4317	0.03292900	DTS 2283.539822222	PTS 2283.539822222	MPEG TS	1358	video-stream

8. Configure the scale to view the base line data and periodic large data peaks.
   a. *Menu » Statistics » IO Graph*
   b. *X Axis » Tick Interval = 0.1 sec*
   c. *Y Axis » Unit: Bytes/Tick*
9. Establish an SSH session to the target.
10. To configure and run the traffic control (tc) binary, type:

```
tc qdisc replace dev eth0 handle 1:0 root tbf burst 3000 limit 300k rate 2000000
peakrate 3000000 mtu 3000
```

Edit parameters such as rate, burst, etc. as necessary.

Other traffic shaping/policing techniques such as HTB are also available (see below).

In Wireshark there should be less peaks and more consistent output packet rate.

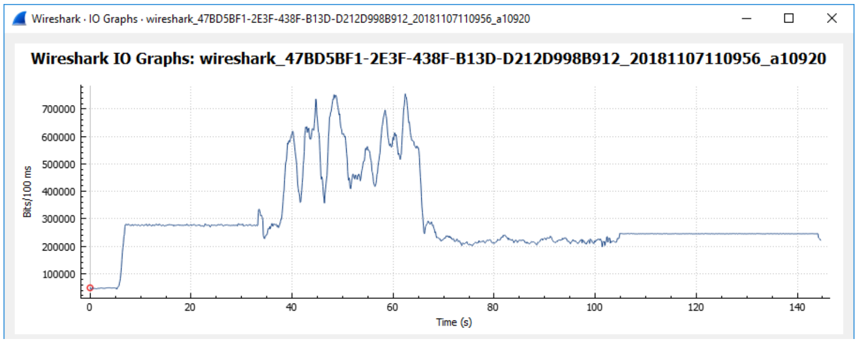


Figure 7: Wireshark IO Graphs

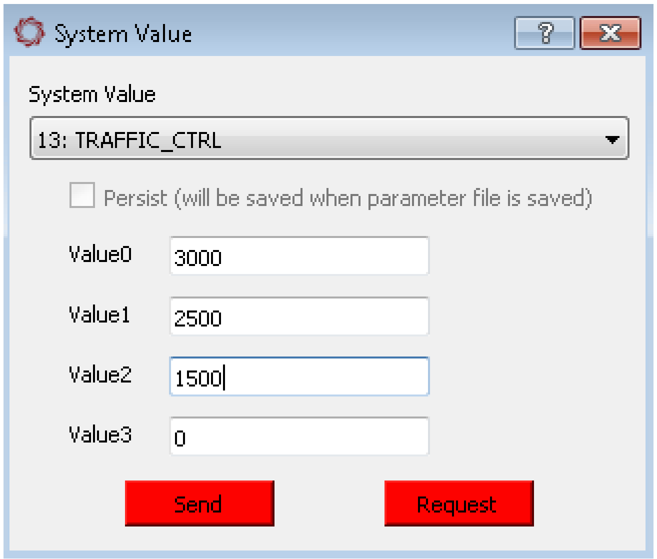
7.11.1 Alternate TC Methods

Other traffic shaping and policing options are available as well, for example:

```
tc qdisc del dev eth0 root &> /dev/null
tc qdisc add dev eth0 root handle 1: htb default 1
tc class add dev eth0 parent 1: classid 1:1 htb rate 3000kbit burst 2500 mtu 1500
```

7.11.2 Test Using Set System Value

Set System Value (0x92) command can also be used to experiment with setting traffic control parameters.



System Value

13: TRAFFIC_CTRL

□ Persist (will be saved when parameter file is saved)

Value0 3000

Value1 2500

Value2 1500

Value3 0

Figure 8: Set System Value - Set Traffic Control

7.12 FTP

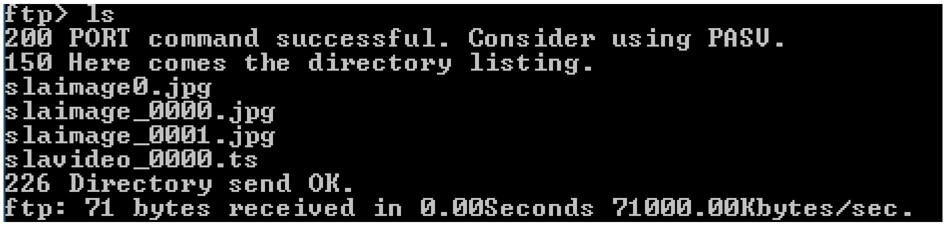
There are many FTP client applications available for this process. In this example the Windows command line is used. The default username and password are *root*.

When connecting to SightLine hardware, it will access the */mnt/mmcblk0p1* directory. This is the directory of the microSD card (if installed).

Use the following commands to manage the files:

List files:

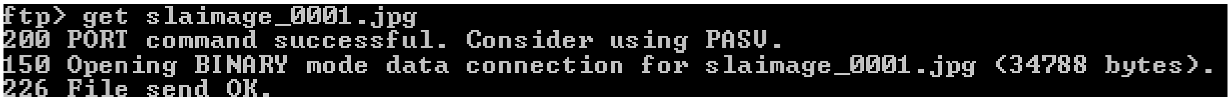
```
ls
```



```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
slaimage0.jpg
slaimage_0000.jpg
slaimage_0001.jpg
slavideo_0000.ts
226 Directory send OK.
ftp: 71 bytes received in 0.00Seconds 71000.00Kbytes/sec.
```

Get a file:

```
get sla_image_0001.jpg
```

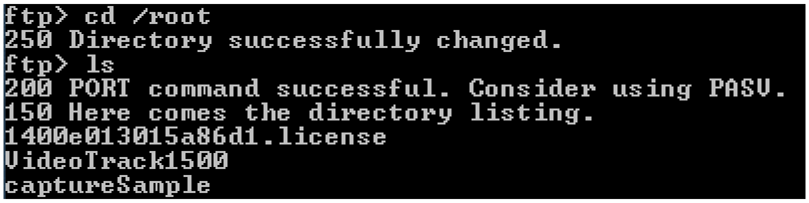


```
ftp> get slaimage_0001.jpg
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for slaimage_0001.jpg (34788 bytes).
226 File send OK.
```

Change directory:

```
cd /root
```

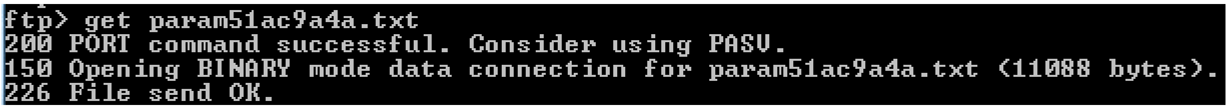
For the 4000-OEM: `cd /home/slroot/sl/bin`



```
ftp> cd /root
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
1400e013015a86d1.license
VideoTrack1500
captureSample
```

Get param file:

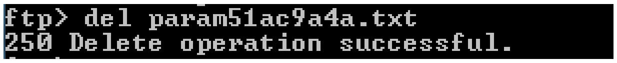
```
get param51ac9a4a.txt
```



```
ftp> get param51ac9a4a.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for param51ac9a4a.txt (11088 bytes).
226 File send OK.
```

Remove param file:

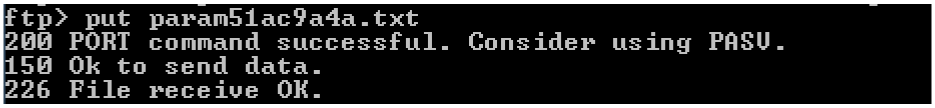
```
del param51aca4a.txt
```



```
ftp> del param51ac9a4a.txt
250 Delete operation successful.
```

Upload a new param file:

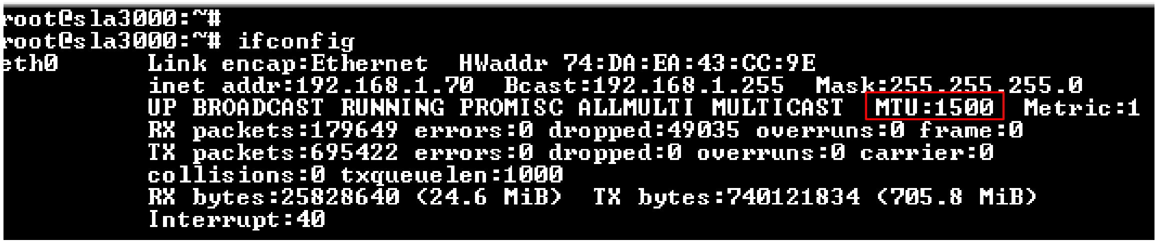
```
put param51ac9a4a.txt
```



```
ftp> put param51ac9a4a.txt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 File receive OK.
```

7.13 Maximum Transmission Unit (MTU)

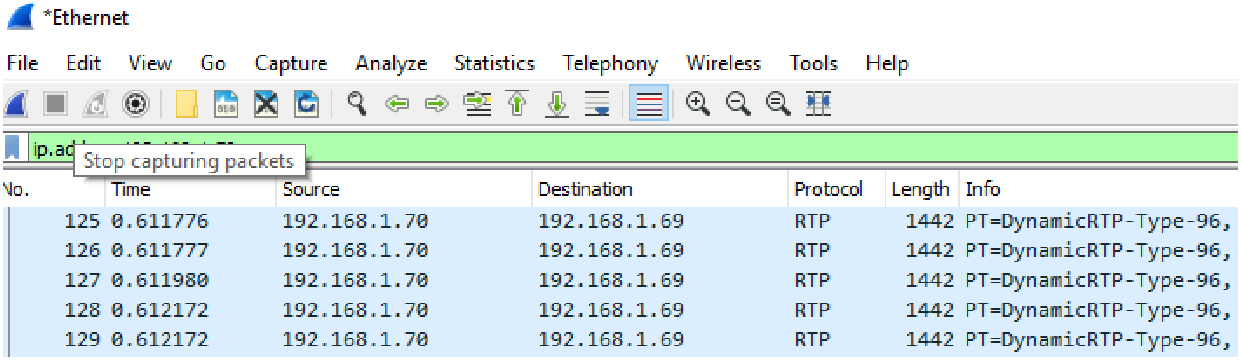
Based on radio capability or other network issues, it may be necessary to reduce the Maximum Transmission Unit (MTU) or packet size. The default MTU is 1500 as shown in Figure 7.



```
root@sla3000:~#
root@sla3000:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 74:DA:EA:43:CC:9E
          inet addr:192.168.1.70  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING PROMISC ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:179649 errors:0 dropped:49035 overruns:0 frame:0
          TX packets:695422 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:25828640 (24.6 MiB)  TX bytes:740121834 (705.8 MiB)
          Interrupt:40
```

Figure 9: Default MTU

Use Wireshark to view packets. Note that most packets in this example are 1442 bytes.

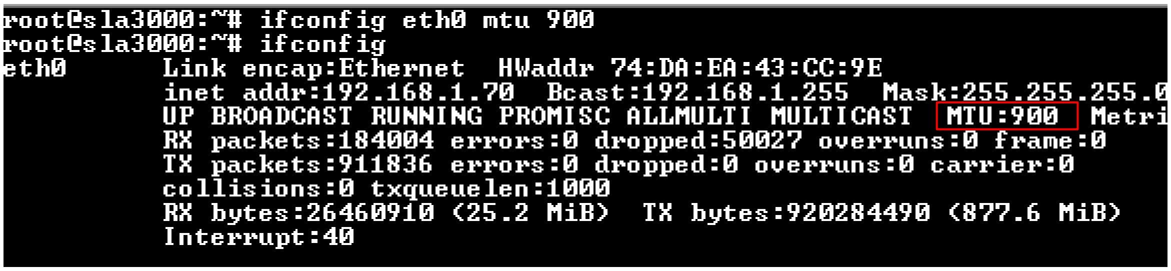


No.	Time	Source	Destination	Protocol	Length	Info
125	0.611776	192.168.1.70	192.168.1.69	RTP	1442	PT=DynamicRTP-Type-96,
126	0.611777	192.168.1.70	192.168.1.69	RTP	1442	PT=DynamicRTP-Type-96,
127	0.611980	192.168.1.70	192.168.1.69	RTP	1442	PT=DynamicRTP-Type-96,
128	0.612172	192.168.1.70	192.168.1.69	RTP	1442	PT=DynamicRTP-Type-96,
129	0.612172	192.168.1.70	192.168.1.69	RTP	1442	PT=DynamicRTP-Type-96,

Figure 10: Packet Sizes in Wireshark

It is possible to manually change the MTU. In this example the MTU has been changed to 900 [bytes] by using the following command:

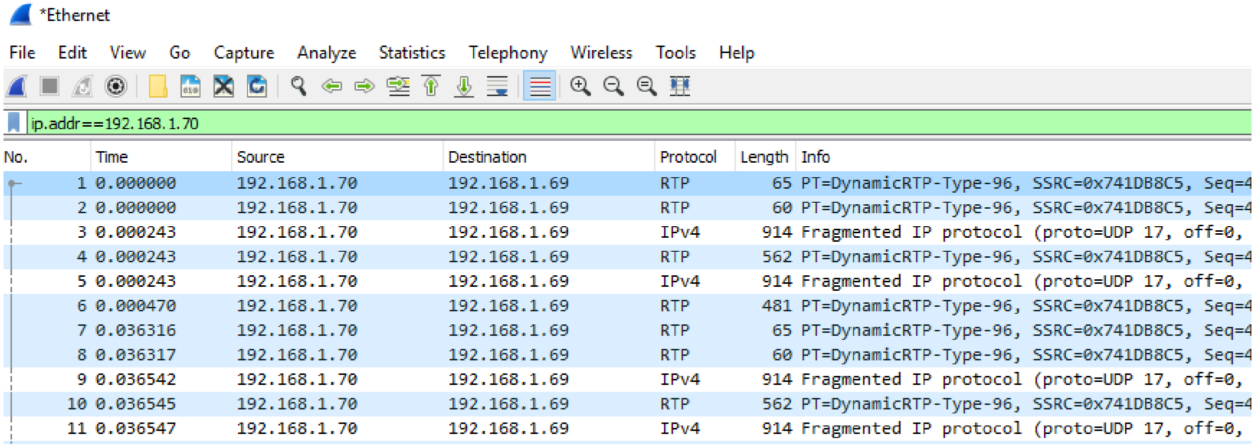
```
ifconfig eth0 mtu 900
```



```
root@sla3000:~# ifconfig eth0 mtu 900
root@sla3000:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 74:DA:EA:43:CC:9E
          inet addr:192.168.1.70  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING PROMISC ALLMULTI MULTICAST  MTU:900  Metri
          RX packets:184004 errors:0 dropped:50027 overruns:0 frame:0
          TX packets:911836 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:26460910 (25.2 MiB)  TX bytes:920284490 (877.6 MiB)
          Interrupt:40
```

Figure 11: MTU Reduced from 1500 to 900 Bytes

In Wireshark note the smaller packets and fragmentation after the MTU change.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.1.70

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.70	192.168.1.69	RTP	65	PT=DynamicRTP-Type-96, SSRC=0x741DB8C5, Seq=4
2	0.000000	192.168.1.70	192.168.1.69	RTP	60	PT=DynamicRTP-Type-96, SSRC=0x741DB8C5, Seq=4
3	0.000243	192.168.1.70	192.168.1.69	IPv4	914	Fragmented IP protocol (proto=UDP 17, off=0,
4	0.000243	192.168.1.70	192.168.1.69	RTP	562	PT=DynamicRTP-Type-96, SSRC=0x741DB8C5, Seq=4
5	0.000243	192.168.1.70	192.168.1.69	IPv4	914	Fragmented IP protocol (proto=UDP 17, off=0,
6	0.000470	192.168.1.70	192.168.1.69	RTP	481	PT=DynamicRTP-Type-96, SSRC=0x741DB8C5, Seq=4
7	0.036316	192.168.1.70	192.168.1.69	RTP	65	PT=DynamicRTP-Type-96, SSRC=0x741DB8C5, Seq=4
8	0.036317	192.168.1.70	192.168.1.69	RTP	60	PT=DynamicRTP-Type-96, SSRC=0x741DB8C5, Seq=4
9	0.036542	192.168.1.70	192.168.1.69	IPv4	914	Fragmented IP protocol (proto=UDP 17, off=0,
10	0.036545	192.168.1.70	192.168.1.69	RTP	562	PT=DynamicRTP-Type-96, SSRC=0x741DB8C5, Seq=4
11	0.036547	192.168.1.70	192.168.1.69	IPv4	914	Fragmented IP protocol (proto=UDP 17, off=0,

Figure 12: Smaller Packet Sizes in Wireshark

In 3.0.8 software, in SetSystemValue (0x92) a new system value type (13 - Linux Traffic Control) was added to allow setting the MTU at runtime in addition to setting the peak bitrate.

7.13.1 Setting MTU Example

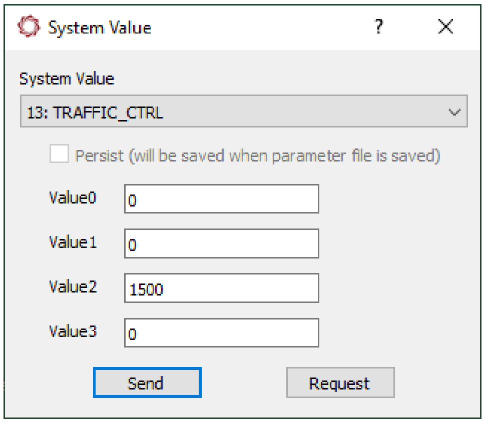
The following steps show an example of how to set MTU using **SetSystemValue (0x92)**.

> ⚠ **CAUTION:** Setting the MTU can cause network instability and communication issues if set incorrectly.

1. Connect to the OEM using the Panel Plus application. See the appropriate OEM startup guide for connection instructions.
2. From the main menu go to » *Configure* » *System Value* to open the *System Value* dialog window.

If Value0 or Value1 are set to zero (0), then the traffic control and MTU are reset to default values.

Before:

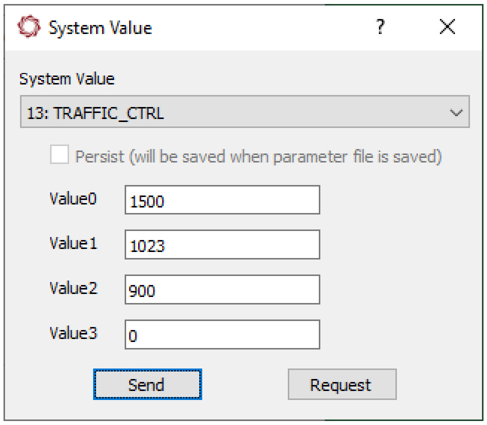


System Value: 13: TRAFFIC_CTRL

□ Persist (will be saved when parameter file is saved)

Value0: 0
Value1: 0
Value2: 1500
Value3: 0

After:



System Value: 13: TRAFFIC_CTRL

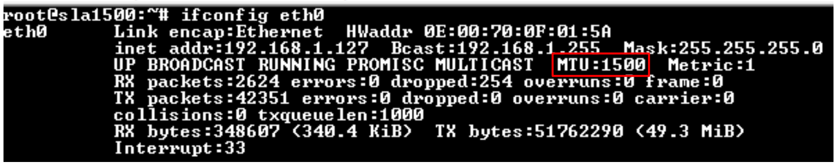
□ Persist (will be saved when parameter file is saved)

Value0: 1500
Value1: 1023
Value2: 900
Value3: 0

3. Click *Send* when complete.

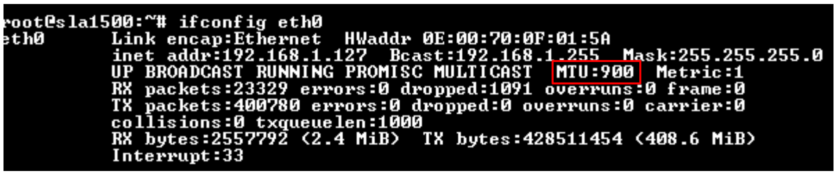
4. To verify, use SSH to connect to the system and use ifconfig (or ip -addr on the 4000-OEM).

   MTU = 1500 before:



```
root@sla1500:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 0E:00:70:0F:01:5A
          inet addr:192.168.1.127  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:2624 errors:0 dropped:254 overruns:0 frame:0
          TX packets:42351 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:348607 (340.4 KiB)  TX bytes:51762290 (49.3 MiB)
          Interrupt:33
```

   MTU = 900 after:



```
root@sla1500:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 0E:00:70:0F:01:5A
          inet addr:192.168.1.127  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:900  Metric:1
          RX packets:23329 errors:0 dropped:1091 overruns:0 frame:0
          TX packets:400780 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2557792 (2.4 MiB)  TX bytes:428511454 (408.6 MiB)
          Interrupt:33
```

7.14 Iperf (3000-OEM and 4000-OEM only)

Iperf is an industry standard cross-platform tool for measuring network performance that is available on the 3000-OEM. Iperf uses a client-server model and creates data streams to measure throughput.

The following example demonstrates configuring an iperf server on a Windows PC using UDP port 11000, connecting an iperf client on a 3000-OEM, and measuring throughout over a switched Ethernet network.

Windows PC uses a precompiled iperf 2.05 32-bit Windows binary from iperf.fr. This version is compatible with Windows XP-10 x86/x64 and is interoperable with the 3000-OEM version. The PC IP address for this example is `<<pc_ip_address>`.

1. Open a command prompt (cmd.exe) on the PC and type `cd` to the path of the iperf binary.
2. To start the iperf server (-s):

```
iperf -s -u -i 1 -p 11000
```

3. Open a terminal emulator and establish an SSH session to the 3000-OEM.
4. Start the iperf client (-c). From the *root@sla3000~#* prompt, type:

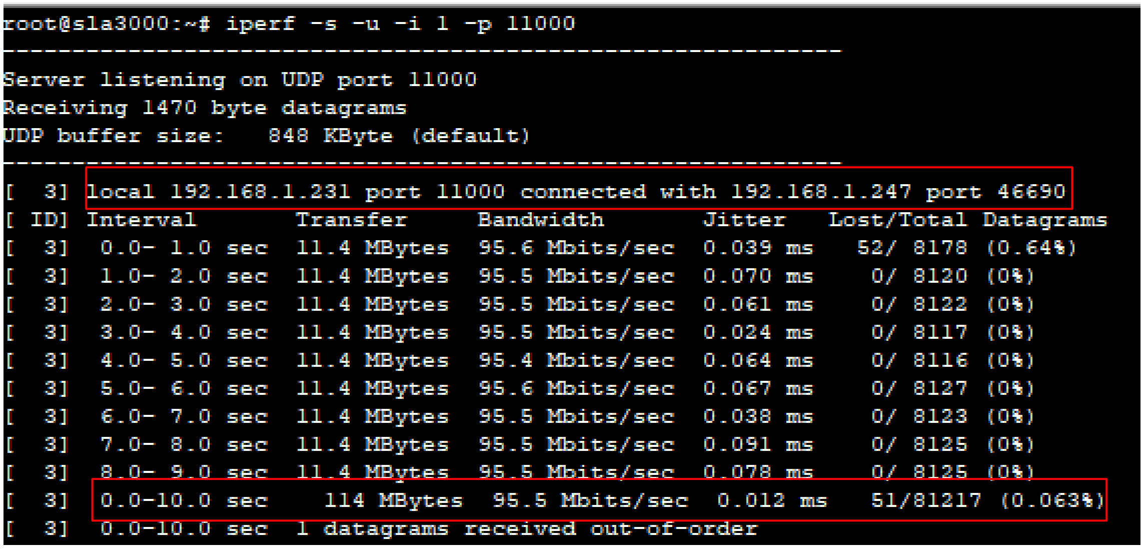
```
iperf -c <<pc_ip_address>> -u -i 1 -b 95m -p 11000
```

The -b parameter specifies target bandwidth in Mb/s. During testing, values above 95 dramatically reduced performance with the 3000-OEM configured as the client. The maximum real-world throughput of the 3000-OEM 10/100 Ethernet adapter is ≈95 Mb/s under ideal conditions. The -b parameter should not exceed 95m when the 3000-OEM is configured as the client.

If successful, the client and server will note the connection established on port 11000. The client reports the data transferred and measured bandwidth in one second intervals.

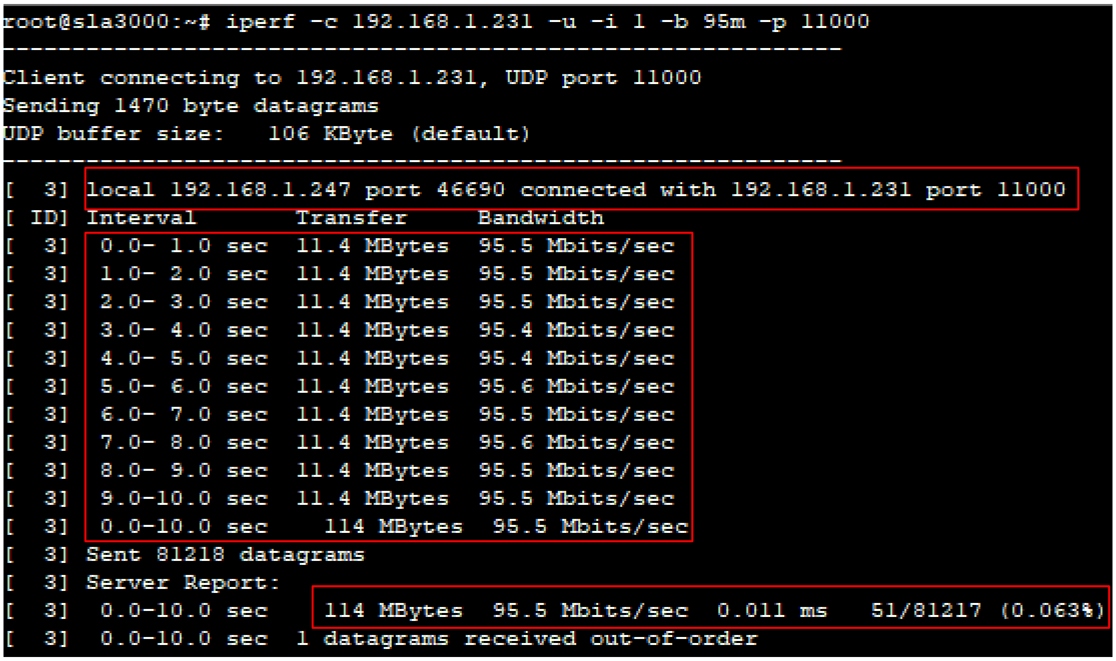
Once the test is the complete, the client and server display the average bandwidth, lost/total packets, jitter, and amount of data transferred during the test period (Figure 11 and Figure 12).

To configure the 3000-OEM as the server and the PC as the client, swap the example commands.



```
root@sla3000:~# iperf -s -u -i 1 -p 11000
------------------------------------------------------------
Server listening on UDP port 11000
Receiving 1470 byte datagrams
UDP buffer size:   848 KByte (default)
------------------------------------------------------------
[  3] local 192.168.1.231 port 11000 connected with 192.168.1.247 port 46690
[ ID] Interval       Transfer     Bandwidth        Jitter   Lost/Total Datagrams
[  3]  0.0- 1.0 sec  11.4 MBytes  95.6 Mbits/sec  0.039 ms   52/ 8178 (0.64%)
[  3]  1.0- 2.0 sec  11.4 MBytes  95.5 Mbits/sec  0.070 ms    0/ 8120 (0%)
[  3]  2.0- 3.0 sec  11.4 MBytes  95.5 Mbits/sec  0.061 ms    0/ 8122 (0%)
[  3]  3.0- 4.0 sec  11.4 MBytes  95.5 Mbits/sec  0.024 ms    0/ 8117 (0%)
[  3]  4.0- 5.0 sec  11.4 MBytes  95.4 Mbits/sec  0.064 ms    0/ 8116 (0%)
[  3]  5.0- 6.0 sec  11.4 MBytes  95.6 Mbits/sec  0.067 ms    0/ 8127 (0%)
[  3]  6.0- 7.0 sec  11.4 MBytes  95.5 Mbits/sec  0.038 ms    0/ 8123 (0%)
[  3]  7.0- 8.0 sec  11.4 MBytes  95.5 Mbits/sec  0.091 ms    0/ 8125 (0%)
[  3]  8.0- 9.0 sec  11.4 MBytes  95.5 Mbits/sec  0.078 ms    0/ 8125 (0%)
[  3]  0.0-10.0 sec    114 MBytes  95.5 Mbits/sec  0.012 ms   51/81217 (0.063%)
[  3]  0.0-10.0 sec  1 datagrams received out-of-order
```

Figure 13: Inbound Connection and Average Bandwidth During Test Period



```
root@sla3000:~# iperf -c 192.168.1.231 -u -i 1 -b 95m -p 11000
------------------------------------------------------------
Client connecting to 192.168.1.231, UDP port 11000
Sending 1470 byte datagrams
UDP buffer size:   106 KByte (default)
------------------------------------------------------------
[  3] local 192.168.1.247 port 46690 connected with 192.168.1.231 port 11000
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 1.0 sec  11.4 MBytes  95.5 Mbits/sec
[  3]  1.0- 2.0 sec  11.4 MBytes  95.5 Mbits/sec
[  3]  2.0- 3.0 sec  11.4 MBytes  95.5 Mbits/sec
[  3]  3.0- 4.0 sec  11.4 MBytes  95.4 Mbits/sec
[  3]  4.0- 5.0 sec  11.4 MBytes  95.4 Mbits/sec
[  3]  5.0- 6.0 sec  11.4 MBytes  95.6 Mbits/sec
[  3]  6.0- 7.0 sec  11.4 MBytes  95.5 Mbits/sec
[  3]  7.0- 8.0 sec  11.4 MBytes  95.6 Mbits/sec
[  3]  8.0- 9.0 sec  11.4 MBytes  95.5 Mbits/sec
[  3]  9.0-10.0 sec  11.4 MBytes  95.5 Mbits/sec
[  3]  0.0-10.0 sec    114 MBytes  95.5 Mbits/sec
[  3] Sent 81218 datagrams
[  3] Server Report:
[  3]  0.0-10.0 sec    114 MBytes  95.5 Mbits/sec  0.011 ms   51/81217 (0.063%)
[  3]  0.0-10.0 sec  1 datagrams received out-of-order
```

Figure 14: Outbound Connection and Bandwidth in 1s Intervals

7.15 Change Interface Speed / Duplex / Auto-Negotiation Configuration

When disabling auto-negotiation, confirm that the other side of the network cable has disabled auto-negotiation and is using the same network speed and duplex.

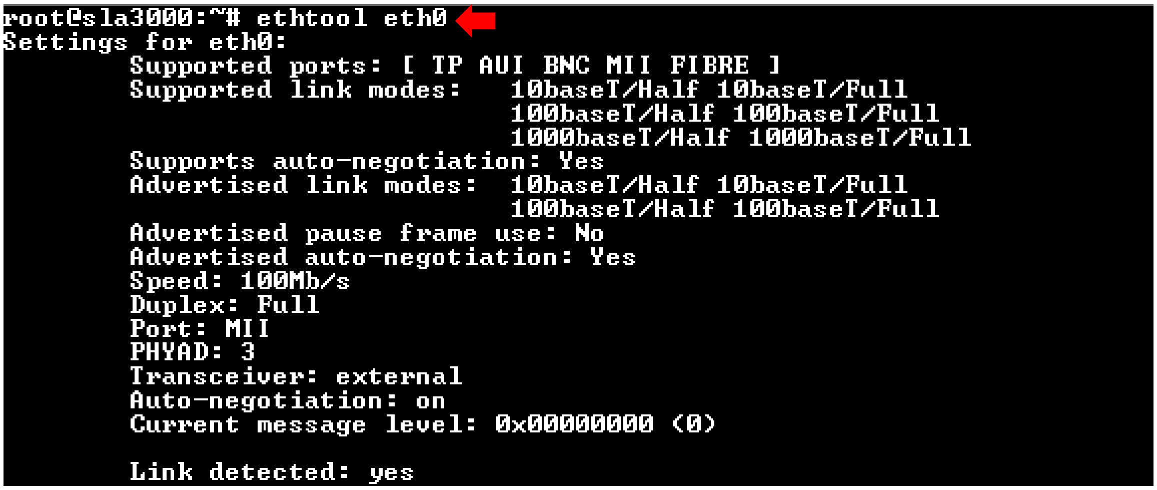
The speed, duplex, and auto-negotiation configuration of the SightLine hardware Ethernet interface can be adjusted using the *ethtool* binary on the embedded Linux system. This may be useful when integrating older devices or specialized network hardware such as satellite radios.

Open a terminal emulator and establish an SSH session to the target. To check the current Ethernet interface configuration:

```
ethtool eth0
```

For the 4000-OEM:

```
ethtool enP2p1s0
```

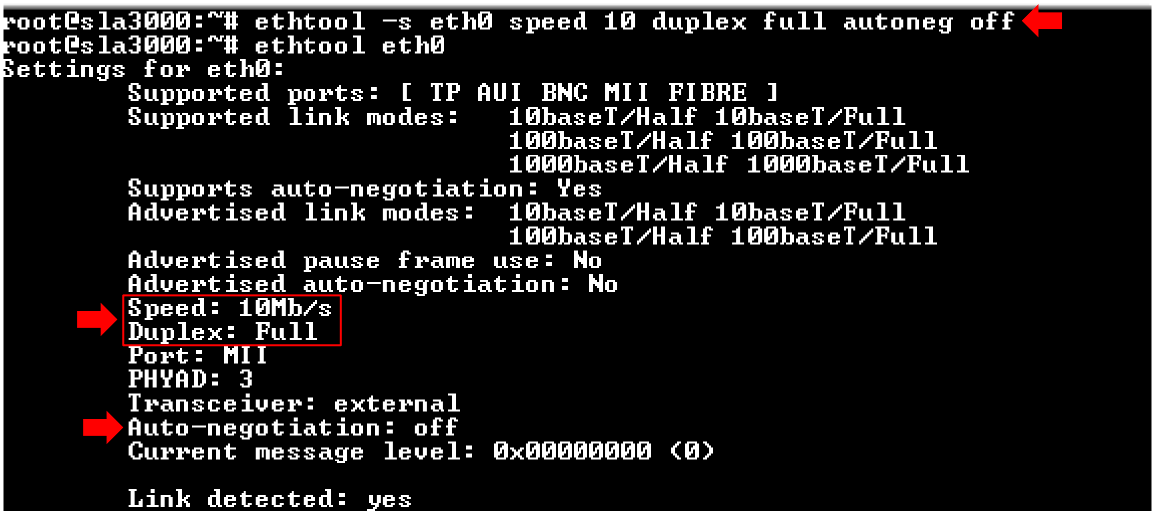


```
root@sla3000:~# ethtool eth0
Settings for eth0:
        Supported ports: [ TP AUI BNC MII FIBRE ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Half 1000baseT/Full
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
        Advertised pause frame use: No
        Advertised auto-negotiation: Yes
        Speed: 100Mb/s
        Duplex: Full
        Port: MII
        PHYAD: 3
        Transceiver: external
        Auto-negotiation: on
        Current message level: 0x00000000 (0)

        Link detected: yes
```

Figure 15: Check Ethernet Interface Configuration

In Figure 14 the interface configuration has been changed to 10 Mbps full duplex with auto-negotiation disabled by using the command:

```
ethtool -s eth0 speed 10 duplex full autoneg off
```



```
root@sla3000:~# ethtool -s eth0 speed 10 duplex full autoneg off
root@sla3000:~# ethtool eth0
Settings for eth0:
        Supported ports: [ TP AUI BNC MII FIBRE ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Half 1000baseT/Full
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
        Advertised pause frame use: No
        Advertised auto-negotiation: No
        Speed: 10Mb/s
        Duplex: Full
        Port: MII
        PHYAD: 3
        Transceiver: external
        Auto-negotiation: off
        Current message level: 0x00000000 (0)

        Link detected: yes
```

Figure 16: Interface Speed / Duplex / Auto-Negotiation Configuration Changed

7.15.1 1500-OEM Ethernet Interface Configuration Startup

To set the interface configuration at startup, add an *ethtool* command to the *rc.local* script.

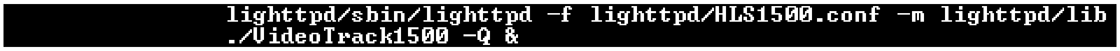
1. Open a terminal emulator and establish an SSH session to the target.
2. Open *rc.local* in the vi editor. From the command line, type:

```
vi /etc/rc.d/rc.local
```

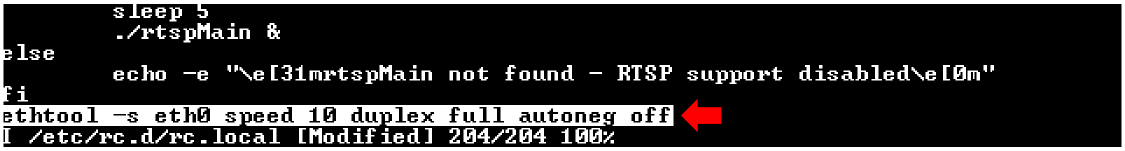
3. Navigate to the end of the file using *Page Down* or the down ↓ arrow key.
4. Press the (I) key to enter insert mode.
5. If an empty line is not present at the end of the file, press the *Enter* key to insert a new line.

ⓘ **IMPORTANT:** Add the *ethtool* command to the end of the file. The intended interface configuration may be overridden if *ethtool* is called prior to *x_Discover_Release* and/or *VideoTrack1500*.

6. Enter the *ethtool* command.



```
                lighttpd/sbin/lighttpd -f lighttpd/HLS1500.conf -m lighttpd/lib
                ./VideoTrack1500 -Q &
```



```
        sleep 5
        ./rtspMain &
else
        echo -e "\e[31mrtspMain not found - RTSP support disabled\e[0m"
fi
ethtool -s eth0 speed 10 duplex full autoneg off
I /etc/rc.d/rc.local [Modified] 204/204 100%
```

7. Press the *Escape* key, and then type:

```
:wq
```

8. Press the *Enter* key to save the file and exit the vi editor.
9. At the command line, type:

```
reboot
```

Auto-negotiation will be enabled during the initial boot process, and the interface will briefly initialize with auto-negotiated parameters once the Linux kernel has loaded. Modifying the interface parameters with ethtool may add up to 10 seconds to the startup process.

7.15.2 3000-OEM and 4000-OEM Ethernet Interface Configuration Startup

To set the interface configuration at startup, add an *ethtool* command to the initialization script. On 3000 the initialization script is sla3000_init.sh. On 4000 the initialization script sla_init.sh is in /home/slroot/sl/scripts

1. Open a terminal emulator and establish an SSH session to the target.
2. Open *initialization script* in the vi editor. From the command line, type:

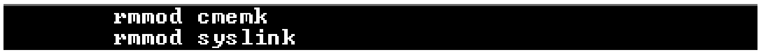
```
vi sla3000_init.sh (or vi /home/slroot/sl/scripts/sla_init.sh on 4000)
```

3. Navigate to the end of the file using *Page Down* or the down arrow ↓ key.
4. Press the (I) key to enter insert mode.

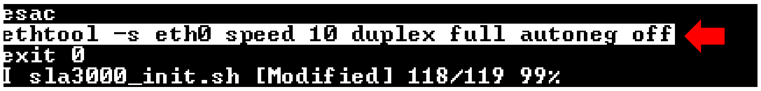
5. Position the cursor in the empty line between `esac` and `exit 0`.

ⓘ **IMPORTANT:** Add the *ethtool* command to the end of the file. The intend interface configuration may be overridden if *ethtool* is called prior to *x_Discover_Release* and/or *VideoTrack3000*.

6. Enter the *ethtool* command.



```
        rmmod cmemk
        rmmod syslink
```



```
esac
ethtool -s eth0 speed 10 duplex full autoneg off
exit 0
I sla3000_init.sh [Modified] 118/119 99%
```

7. Press the *Escape* key, and then type:

```
:wq
```

8. Press the *Enter* key to save the file and exit the vi editor.

9. At the command line, type:

```
reboot
```

Auto-negotiation will be enabled during the initial boot process. The interface will briefly initialize with auto-negotiated parameters once the Linux kernel has loaded. Modifying the interface parameters with ethtool can add up to 10 seconds to the startup process.

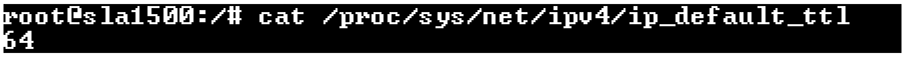
7.16 Change Time-To-Live (TTL)

1. Open a terminal emulator and establish an SSH session to the target.

2. Type:

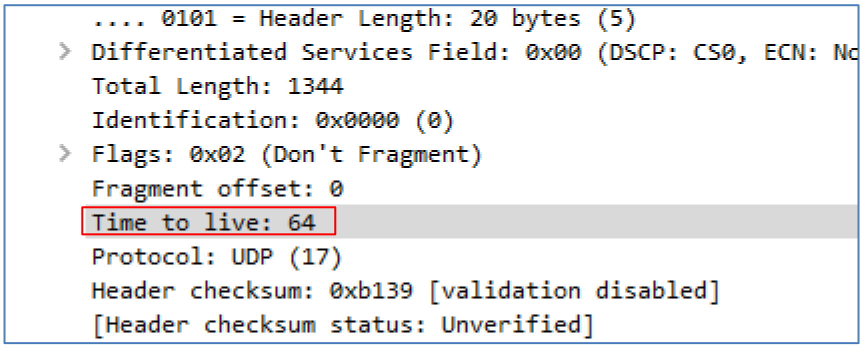
```
cat /proc/sys/net/ipv4/ip_default_ttl
```

3. Confirm value is *64*.



```
root@sla1500:/# cat /proc/sys/net/ipv4/ip_default_ttl
64
```

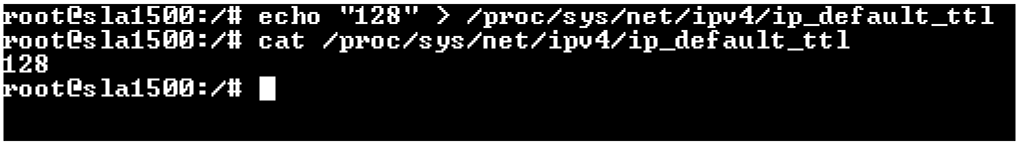
Wireshark can also be used to confirm the value.



```
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: No
     Total Length: 1344
     Identification: 0x0000 (0)
   > Flags: 0x02 (Don't Fragment)
     Fragment offset: 0
     Time to live: 64
     Protocol: UDP (17)
     Header checksum: 0xb139 [validation disabled]
     [Header checksum status: Unverified]
```

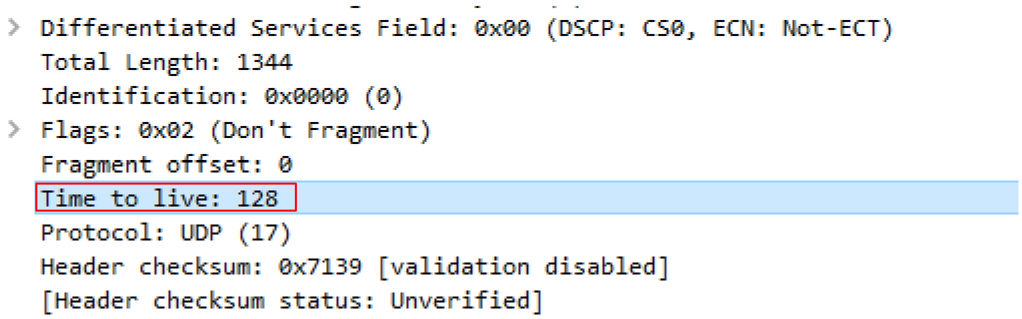
4. Set TTL to new value, type:

```
echo “128” > /proc/sys/net/ipv4/ip_default_ttl
```



```
root@sla1500:/# echo "128" > /proc/sys/net/ipv4/ip_default_ttl
root@sla1500:/# cat /proc/sys/net/ipv4/ip_default_ttl
128
root@sla1500:/#
```

5. Confirm new TTL with Wire Shark.



```
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 1344
  Identification: 0x0000 (0)
> Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: UDP (17)
  Header checksum: 0x7139 [validation disabled]
  [Header checksum status: Unverified]
```

6. The rc.local (1500-OEM), sla3000_init.sh (3000-OEM), or sl/bin/sla_init.sh (4000-OEM) can be modified. This allows the TTL to be set every time the system reboots.

7.17 Improve UDP Performance

One of the most common causes of lost UDP datagrams is an undersized receive buffer on the socket. Use these commands to query the current UDP/IP receive buffer default and max value:

```
$ sysctl net.core.rmem_max
net.core.rmem_max = 212992
$ sysctl net.core.rmem_default
net.core.rmem_default = 212992
```

Video hesitation and packet drops are common if the UPD receive buffer size is too small. More so if the video is streamed through RTSP.

The RTSP server recommended UDP receive buffer size should be at least 868352 bytes.

Use the following commands to change the UPP receive buffer size (both commands are required):

```
$ sysctl -w net.core.rmem_max=868352
net.core.rmem_max = 868352
$ sysctl -w net.core.rmem_default=868352
net.core.rmem_default = 868352
```

Adding the two lines of commands to the beginning of init scripts (/etc/rc.d/rc.local for the 1500-OEM and /home/root/sla3000_init.sh for the 3000-OEM) will make the changes effective at bootup.

7.18 Improve TCP Performance

TCP interleaved RTSP can saturate the send buffer in slower or high latency network environments. Increasing the buffer may help smooth out issues. This change can also be added to the startup scripts mentioned above.

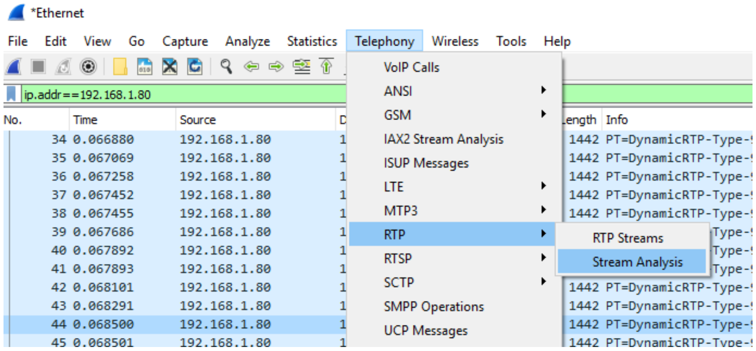
```
$ sysctl -w net.ipv4.tcp_wmem="4096 868352 868352"
```

7.19 Analyze RTP with Wireshark

Wireshark can analyze the integrity of an RTP stream by detecting missed RTP packets and packets received out of order. This can be useful when there are any quality issues when streaming with RTP or RTSP.

To analyze a stream:

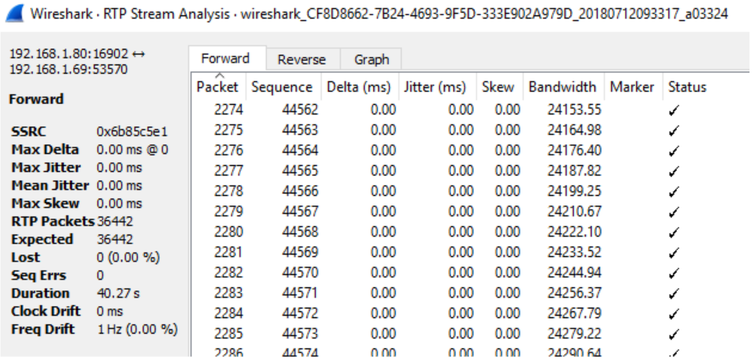
1. Capture an RTP stream and select an RTP packet.
2. From the main menu » *Telephony* » *RTP* » *Stream Analysis*.



ip.addr==192.168.1.80

```
No.        Time       Source         D   Length  Info
      34 0.066880   192.168.1.80    1    1442 PT=DynamicRTP-Type-
      35 0.067069   192.168.1.80    1    1442 PT=DynamicRTP-Type-
      36 0.067258   192.168.1.80    1    1442 PT=DynamicRTP-Type-
      37 0.067452   192.168.1.80    1    1442 PT=DynamicRTP-Type-
      38 0.067455   192.168.1.80    1    1442 PT=DynamicRTP-Type-
      39 0.067686   192.168.1.80    1                        Type-
      40 0.067892   192.168.1.80    1                        Type-
      41 0.067893   192.168.1.80    1                        Type-
      42 0.068101   192.168.1.80    1    1442 PT=DynamicRTP-Type-
      43 0.068291   192.168.1.80    1    1442 PT=DynamicRTP-Type-
      44 0.068500   192.168.1.80    1    1442 PT=DynamicRTP-Type-
      45 0.068501   192.168.1.80    1    1442 PT=DynamicRTP-Type-
```

3. Review the summary window. It will show details of each RTP packet captured including any lost packets.



Wireshark · RTP Stream Analysis · wireshark_CF8D8662-7B24-4693-9F5D-333E902A979D_20180712093317_a03324

192.168.1.80:16902 ↔
192.168.1.69:53570

Forward

SSRC	0x6b85c5e1
Max Delta	0.00 ms @ 0
Max Jitter	0.00 ms
Mean Jitter	0.00 ms
Max Skew	0.00 ms
RTP Packets	36442
Expected	36442
Lost	0 (0.00 %)
Seq Errs	0
Duration	40.27 s
Clock Drift	0 ms
Freq Drift	1 Hz (0.00 %)

Packet	Sequence	Delta (ms)	Jitter (ms)	Skew	Bandwidth	Marker	Status
2274	44562	0.00	0.00	0.00	24153.55		✓
2275	44563	0.00	0.00	0.00	24164.98		✓
2276	44564	0.00	0.00	0.00	24176.40		✓
2277	44565	0.00	0.00	0.00	24187.82		✓
2278	44566	0.00	0.00	0.00	24199.25		✓
2279	44567	0.00	0.00	0.00	24210.67		✓
2280	44568	0.00	0.00	0.00	24222.10		✓
2281	44569	0.00	0.00	0.00	24233.52		✓
2282	44570	0.00	0.00	0.00	24244.94		✓
2283	44571	0.00	0.00	0.00	24256.37		✓
2284	44572	0.00	0.00	0.00	24267.79		✓
2285	44573	0.00	0.00	0.00	24279.22		✓
2286	44574	0.00	0.00	0.00	24290.64		✓

7.20 Disable Network Services

Use Table 4 to disable the following network features in the SightLine Hardware. Reboot the target for the settings to take effect.

Starting with 2.23, these files can be edited in the Upgrade Utility subfolder on the host PC. The modified files will be copied to the target during the firmware upgrade process.

Table 4: Disable Network Services

Network Feature	Hardware	File to be edited (use vi):	Changes to file:
SSH	1500-OEM	/etc/rc.d/init.d/dropbear	As the second line add: `exit 0`
	3000-OEM	/etc/init.d/dropbear	`Change NO_START=0 to NO_START=1`

	4000-OEM		To disable:
			`sudo systemctl disable ssh.socket`
			To enable:
			`sudo systemctl enable ssh.socket`

FTP	1500-OEM	/etc/inetd.conf	Insert # in front of: `ftp stream tcp nowait root /usr/sbin/vsftpd`
	3000-OEM	/etc/rc5.d/S80slaVsFtpd.sh	As the second line add: `exit 0`

	4000-OEM		To disable:
			`sudo systemctl disable vsftpd`
			To enable:
			`sudo systemctl enable vsftpd`

HLS (HTTP Live Streaming)	1500-OEM	/etc/rc.d/rc.local	Comment out (#) the following line: `lighttpd/sbin/lighttpd -f lighttpd/HLS1500.conf -m lighttpd/lib`

	3000-OEM	/home/root/sla3000_init.sh	Comment out (#) the following lines:
			`mkdir /var/cache/lighttpd`
			`lighttpd/sbin/lighttpd -D -f lighttpd/HLS.conf -m lighttpd/lib &`

	4000-OEM	/home/slroot/sl/scripts/sla_init.sh:	Comment out (#) the following line: `lighttpd -D -f /home/slroot/sl/lighttpd/HLS.conf &`

RTSP	1500-OEM	/etc/rc.d/rc.local	Comment out (#) the following lines:
			`if [ -f rtspMain ]; then`
			`sleep 5`
			`./rtspMain &`
			`else`
			`echo -e "\e[31mrtspMain not found - RTSP support disabled\e[0m"`
			`fi`

	3000-OEM	/home/root/sla3000_init.sh	Comment out (#) the following lines:
			`if [ -f rtspMain ]; then`
			`sleep 5`
			`./rtspMain &`
			`else`
			`echo -e "\e[31mrtspMain not found - RTSP support disabled\e[0m"`
			`fi`

	4000-OEM	/home/slroot/sl/scripts/sla_init.sh	Comment out (#) the following line: `./1_rtspMain_ARM64_Release.out &`

8 Questions and Additional Support

For questions and additional support, please contact Support. Additional support documentation and Engineering Application Notes (EANs) can be found on the Documentation page of the SightLine Applications website.

Appendix - SightLine Ports Commonly Used

Table A1: SightLine Ports Commonly Used

Port	Description
14001	Inbound commands on SightLine hardware
14002	Input reply port on PC
51000	SLDISCOVER listen port
5004	Default port for RTP-MJPEG
15004	Default port for MPEG2-TS H.264
52000	Watchdog timer port for diagnostics information
21	FTP port
23	SSH port
14003	Inbound commands on SightLine hardware from internal ARM programs
45001	TCP port number for upgrade