Taking a Wireshark Capture Remotely on a Polycom® RealPresence® Group Series System

Introduction

Polycom® RealPresence® Group Series Software Release 4.1.1 introduced the ability to take a Wireshark capture remotely on the RealPresence Group Series system without having to mirror a port on a switch or using a hub. This feature allows Ethernet frames which are flowing in and out of the LAN interface on a RealPresence Group Series system to be captured on a remote PC. This is done based on a client-server model. The Wireshark capture is started on the RealPresence Group Series system. Wireshark client is then configured to connect remotely to the RealPresence Group Series system to capture Ethernet frames remotely.

This document describes the steps to enable this feature and how to use the feature to capture Ethernet frames on a remote PC.

Prerequisites

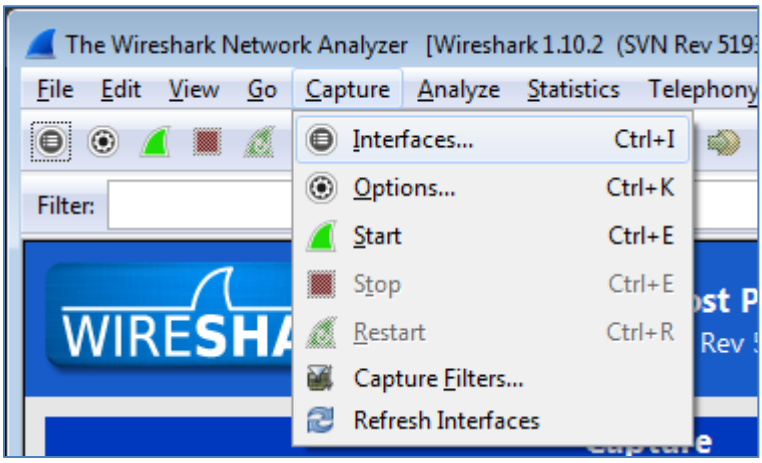
- A Windows-based PC with Wireshark 1.8.0 or later installed.
- A RealPresence Group Series system with Software Release 4.1.1 or later. The Admin password must be enabled on the system.

Enabling Remote Capture on a RealPresence Group Series System

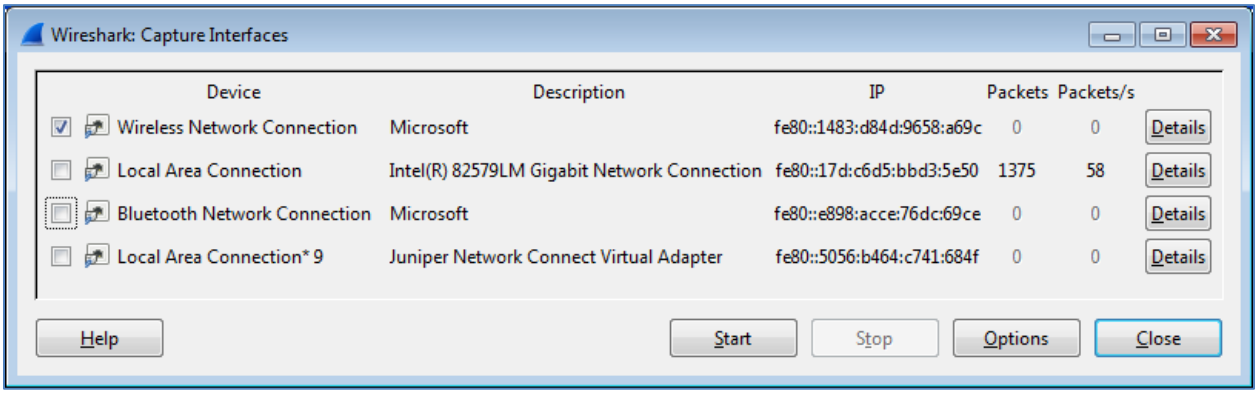
1. Telnet into the RealPresence Group Series system on port 23/tcp.
2. If prompted to enter a password, enter the admin password configured on the RealPresence Group Series system.
3. Type in the following command to enable the remote capture feature:
   `capture Remote Start`
4. If prompted to enter a password, enter the admin password configured on the RealPresence Group Series system.
5. Verify that the RealPresence Group Series system returns the following into the telnet session:
   `Starting Remote Capture`

Configuring Remote Interface in Wireshark

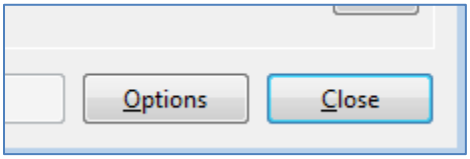
6. Launch Wireshark application on the PC.
7. From the menu, execute **Capture > Interfaces…**.



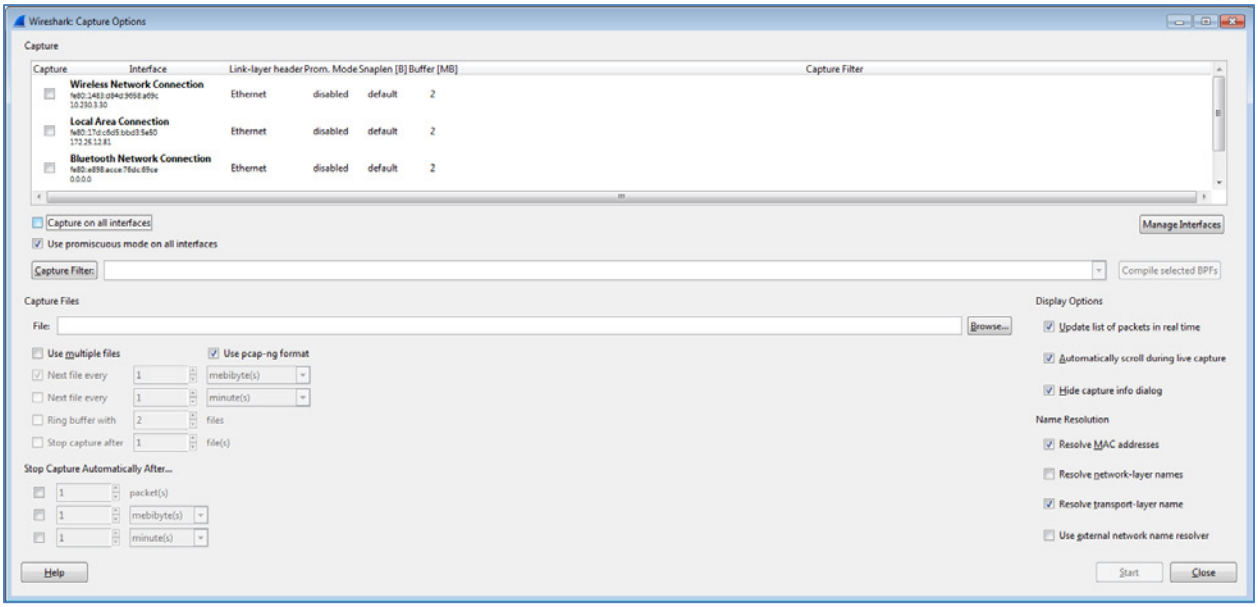
Wireshark: Capture Interfaces dialog box will open.



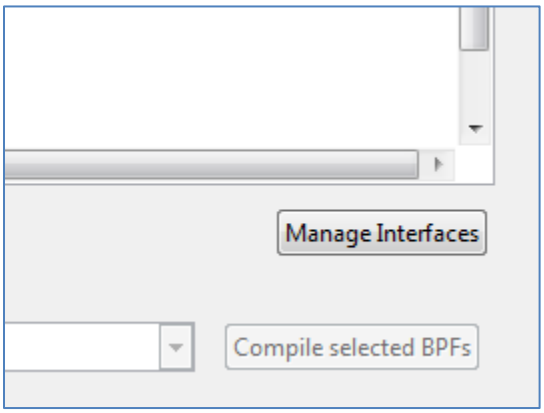
8. In **Wireshark: Capture Interfaces** dialog box, click **Options**.



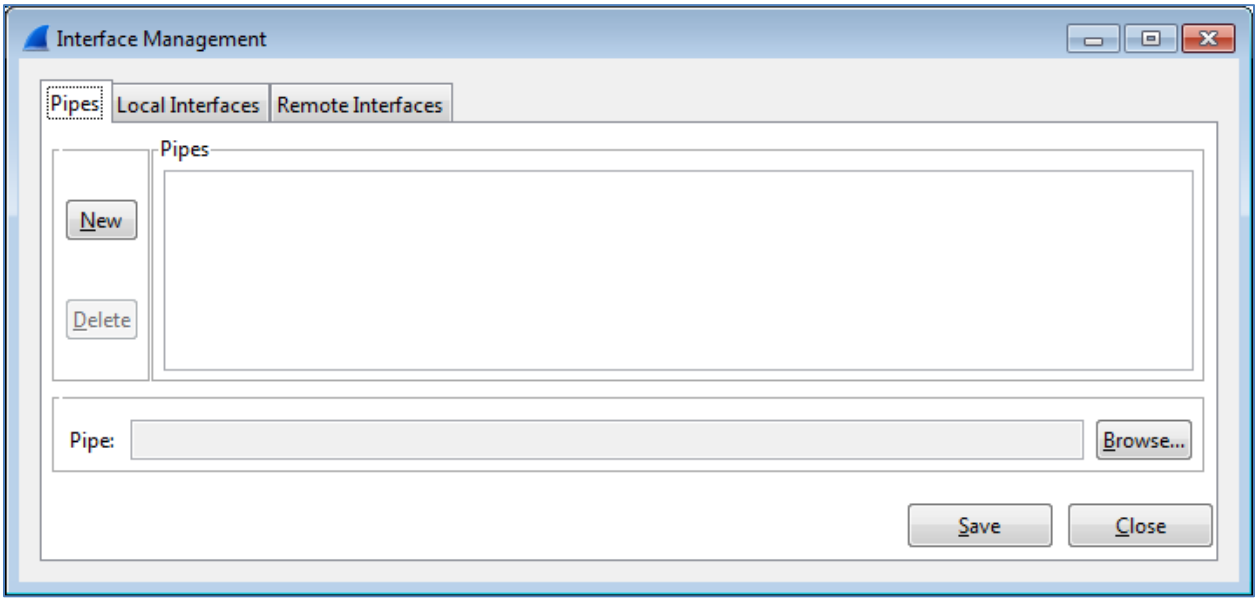
Wireshark: Capture Options dialog box will open.



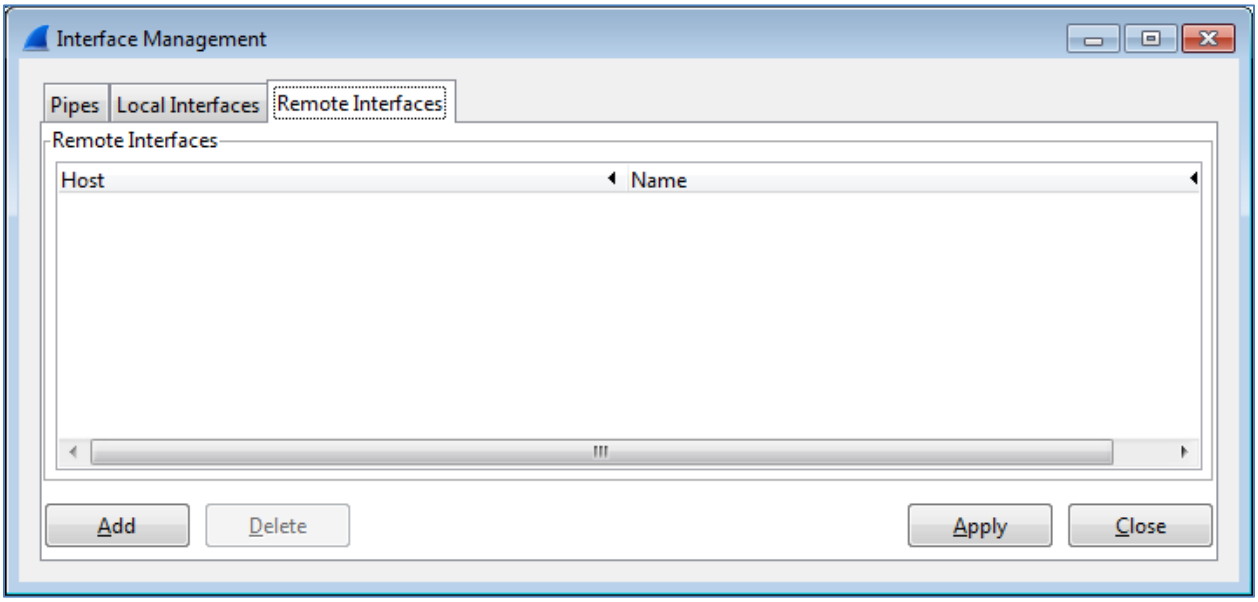
9. In **Wireshark: Capture Options** dialog box, Click **Manage Interfaces**.



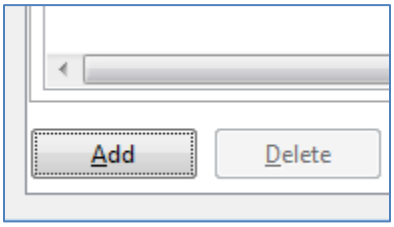
Interface Management dialog box will open.



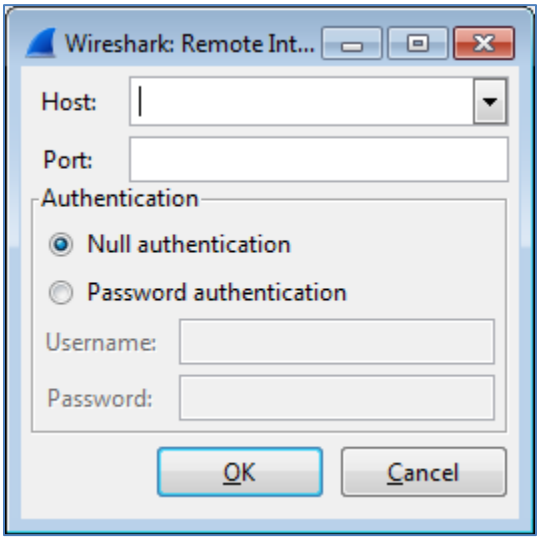
10. In **Interface Management** dialog box, click on **Remote Interfaces** tab.



11. Click on **Add** to add a new remote interface.

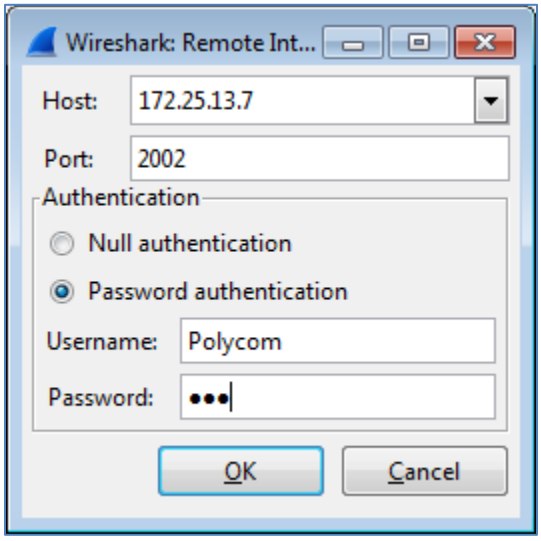


Wireshark: Remote Interface dialog box will open.



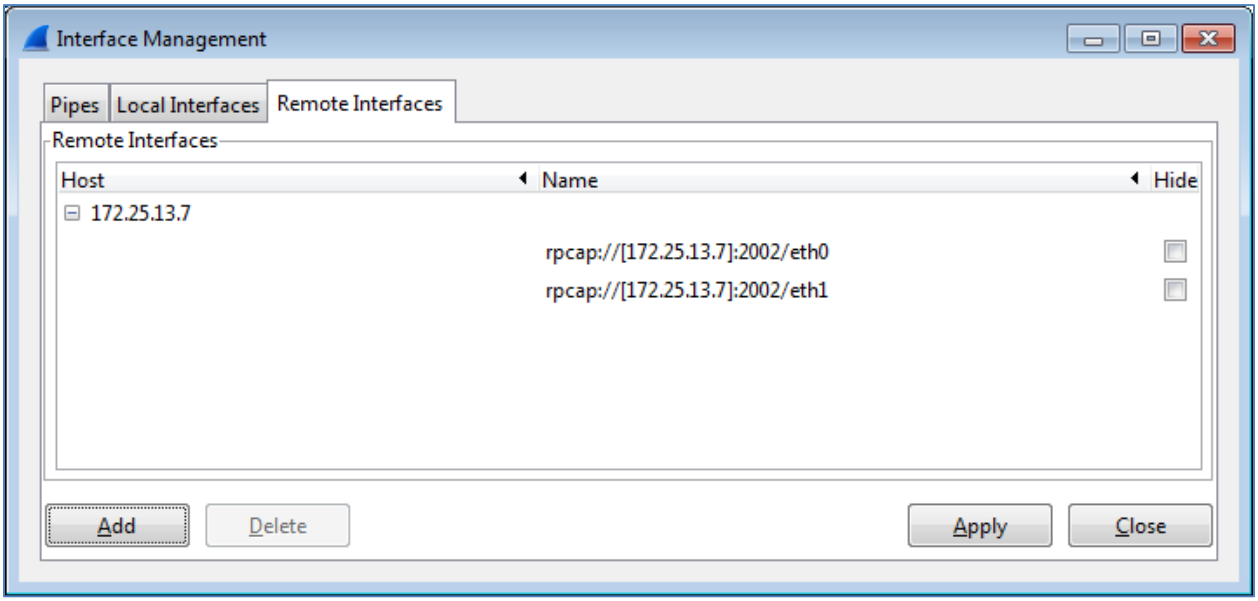
12. In **Wireshark: Remote Interface** dialog box, specify the following:

- **Host**: IP address of the RealPresence Group Series system
- **Port**: **`2002`**
- Select **Password authentication**
- **Username**: **`Polycom`**
- **Password**: the admin password configured on the RealPresence Group Series system



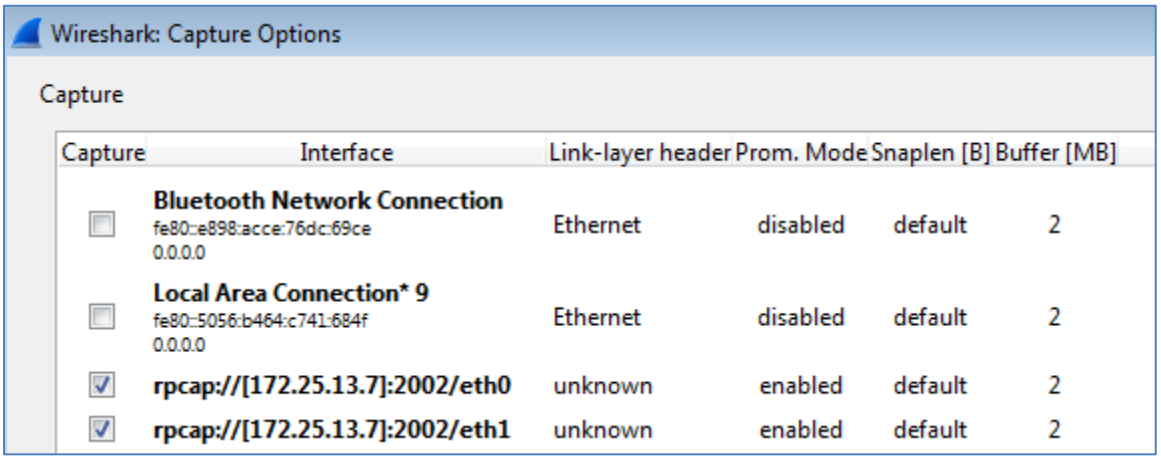
13. Click **OK** to close the **Wireshark: Remote Interface** dialog box.

    The Ethernet port of the RealPresence Group Series system should now appear as a remote interface in **Interface Management** dialog box. For RealPresence Group 700 system, two interfaces should appear.



14. Click **Close** to close the **Interface Management** dialog box.

15. In **Wireshark: Capture Options** dialog box, verify that the newly-added remote capture interface appears as a choice of interfaces available.

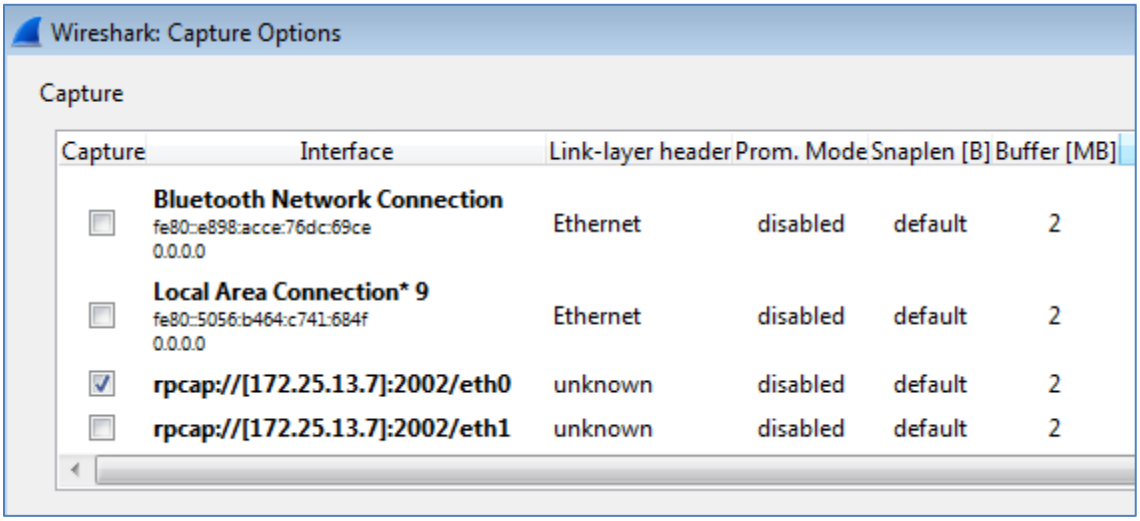


Starting the Capture

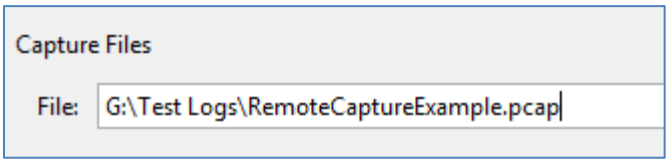
[NOTE] Below is just one of many methods which can be used to perform remote capturing using Wireshark. The steps provided below reduce compute required on the PC when taking the capture. Overstressing the CPU on the PC can cause some Ethernet frames to get dropped during the capture. Polycom recommends that the steps below are followed in order to capture the data as accurate as possible.

16. In **Wireshark: Capture Options** dialog box, select the remote capture interface of the RealPresence Group Series.

    On RealPresence Group 700, **`eth0`** is the LAN interface; **`eth1`** is the PC port.

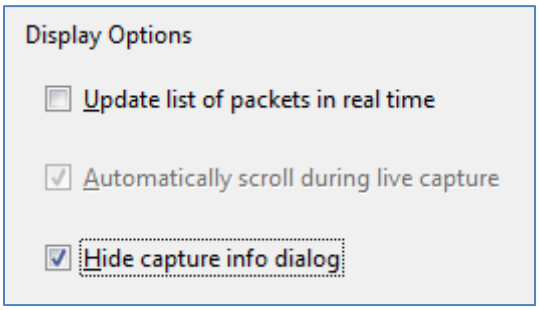


17. Under **Capture Files**, click on **Browse…** and specify location and filename to which the captured data will be stored. For the filename, use **`.cap`** or **`.pcap`** file extension so that it can easily be identified that it's a Wireshark capture file.

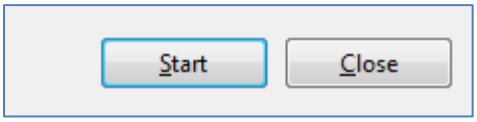


18. Disable **Update list of packets in real time** checkbox.

19. Enable **Hide capture info** dialog checkbox.

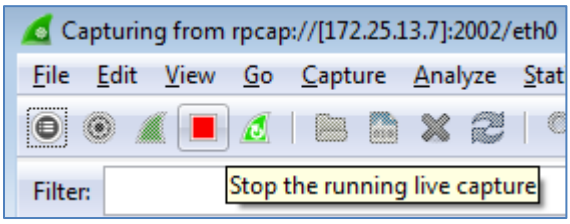


20. Click on **Start** to start remote capturing.



Stopping the Capture

21. To stop the capture, click on **Stop the running live capture** button  on the main Wireshark console.



Disabling Remote Capture on a RealPresence Group Series System

[NOTE] Once Remote Capture is enabled on a RealPresence Group Series system, it is enabled until it is manually disabled. The setting will persist across system restarts.

22. Telnet into the RealPresence Group Series system on port 23/tcp.
23. If prompted to enter a password, enter the admin password configured on the RealPresence Group Series system.
24. Type in the following command to disable the remote capture feature:
    `capture Remote Stop`
25. Verify that RealPresence Group Series system returns the following into the telnet session:
    `Stopping Remote Capture`

Troubleshooting

Issue	Try the Following Steps
Can't get list of interfaces error appears when attempting to connect Wireshark to the eth0 interface of the RealPresence Group Series system	1. Verify that the admin password is configured on the RealPresence Group Series system. 2. Verify that the correct IP address and port are specified. 3. Verity that **Password authentication** is selected, and Username **`Polycom`** and the correct admin password are specified.