Contents

Introduction

This document describes the procedure to collect the packets that are sent to and from the network interface on a Cisco Video Surveillance Media Server 6.x/7.x.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco Video Surveillance Media Server 6.x/7.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Cisco Video Surveillance Media Server Packet Capture

When you troubleshoot issues with Cisco Video Surveillance Media Server 6.x/7.x, it is sometimes necessary to collect the packets that are sent to and from the network interface on the server. Follow these steps:

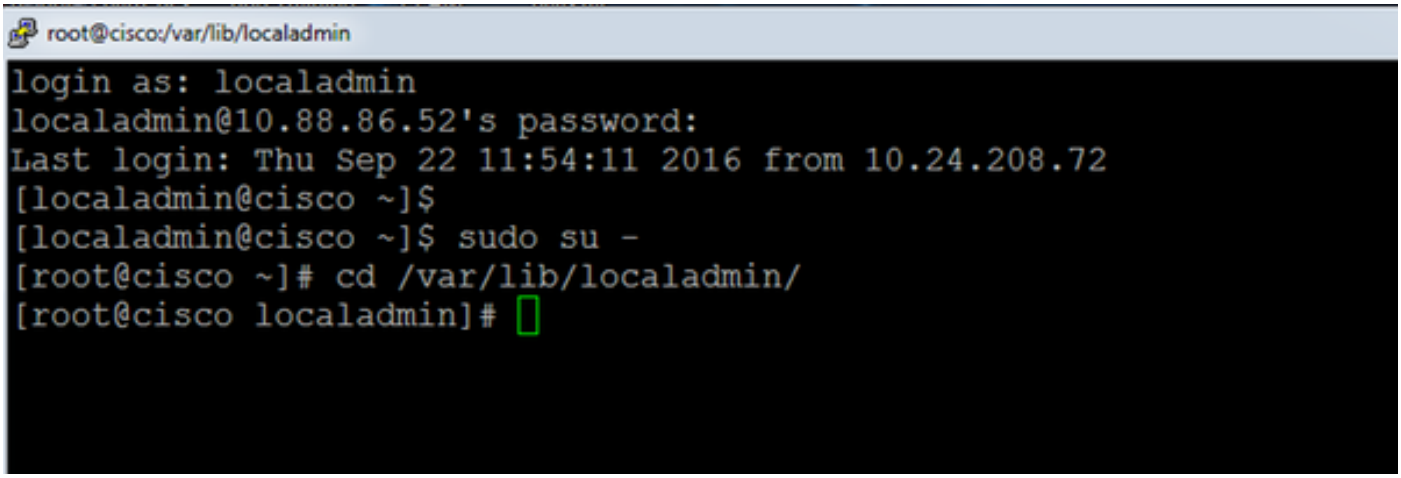
1. Start the Capture
2. Reproduce the Problem Symptom or Condition
3. Stop the Capture
4. Collect the Capture from the Server

Step 1. Start the Capture

In order to start the capture, establish a secure shell (SSH) session to the Cisco Video

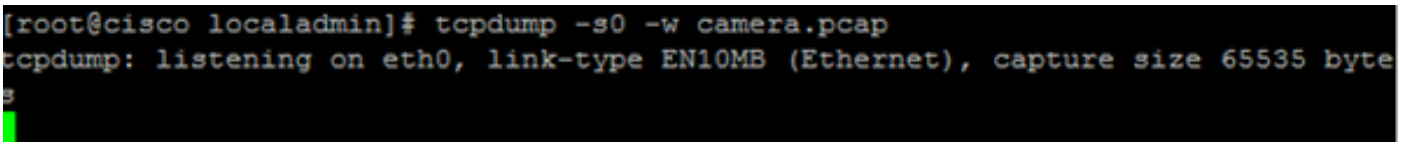
Surveillance Media server, and authenticate with the localadmin account, as shown.

Navigate to the **/var/lib/localadmin** folder with the command **cd /var/lib/localadmin/**



For a typical capture, to collect all packets of all sizes from and to all addresses and save the output to a capture file called **camera.pcap** use the following command :

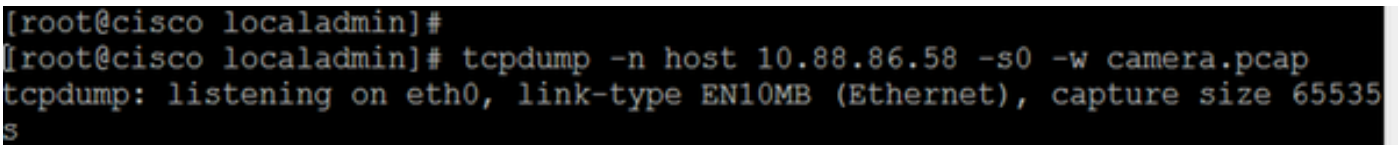
tcpdump -s0 -w camera.pcap



When you troubleshoot an issue with Cisco Video Surveillance Media Server and a particular host, you can use the **host** option in order to filter for traffic to and from a particular host, as shown:

tcpdump -n host 10.88.86.58 -s0 -w camera.pcap

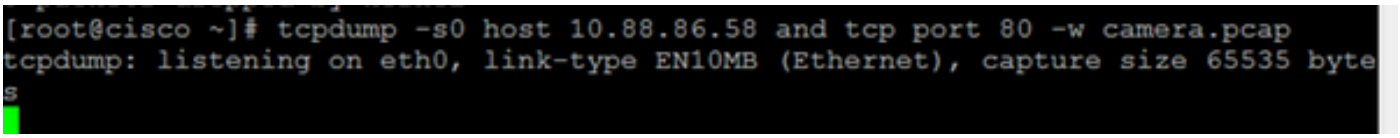
Here 10.88.86.58 is the IP of the problematic host



When you troubleshoot a Pan tilt zoom(PTZ) camera related issue on a Cisco or 3rd party ONVIF camera, which uses TCP port 80 for PTZ communication, use this command:

tcmpdump -s0 host 10.88.86.58 and tcp port 80 -w camera.pcap

Here 10.88.86.58 is the IP of the problematic host



Step 2. Reproduce the Problem Symptom or Condition

While the capture runs, reproduce the problem symptom or condition so that the necessary packets are included in the capture. If the problem is intermittent, run the capture for an extended period. If the capture ends, it is because the buffer is filled. Restart the capture in such cases. If a capture is needed for an extended period of time, it can be worthwhile to capture at the network level through other means, such as through the use of a monitor session on a switch.

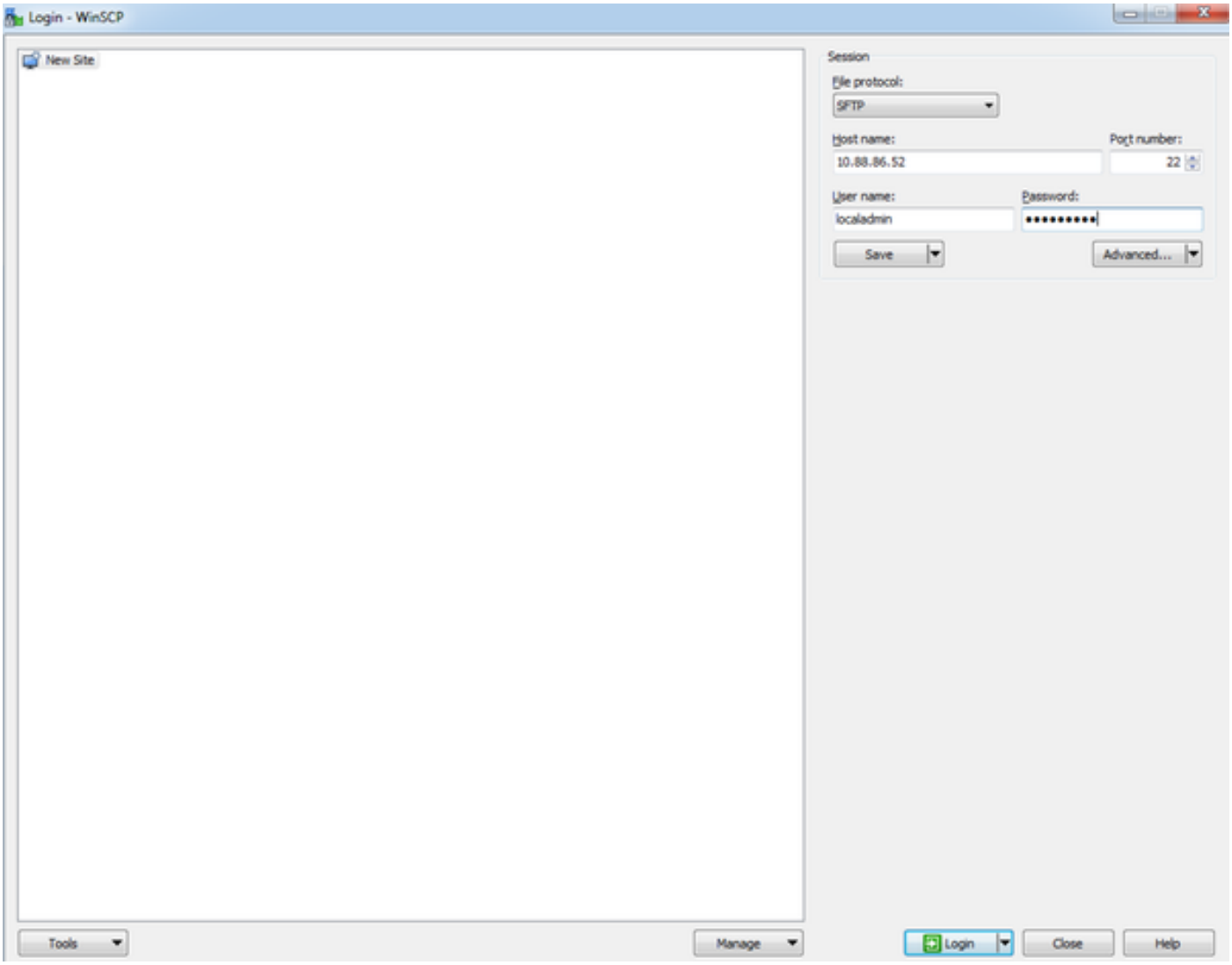
Step 3. Stop the Capture

In order to stop the capture, hold the **Control** key and press **C** on the keyboard. This causes the capture process to end and no new packets are added to the capture dump.

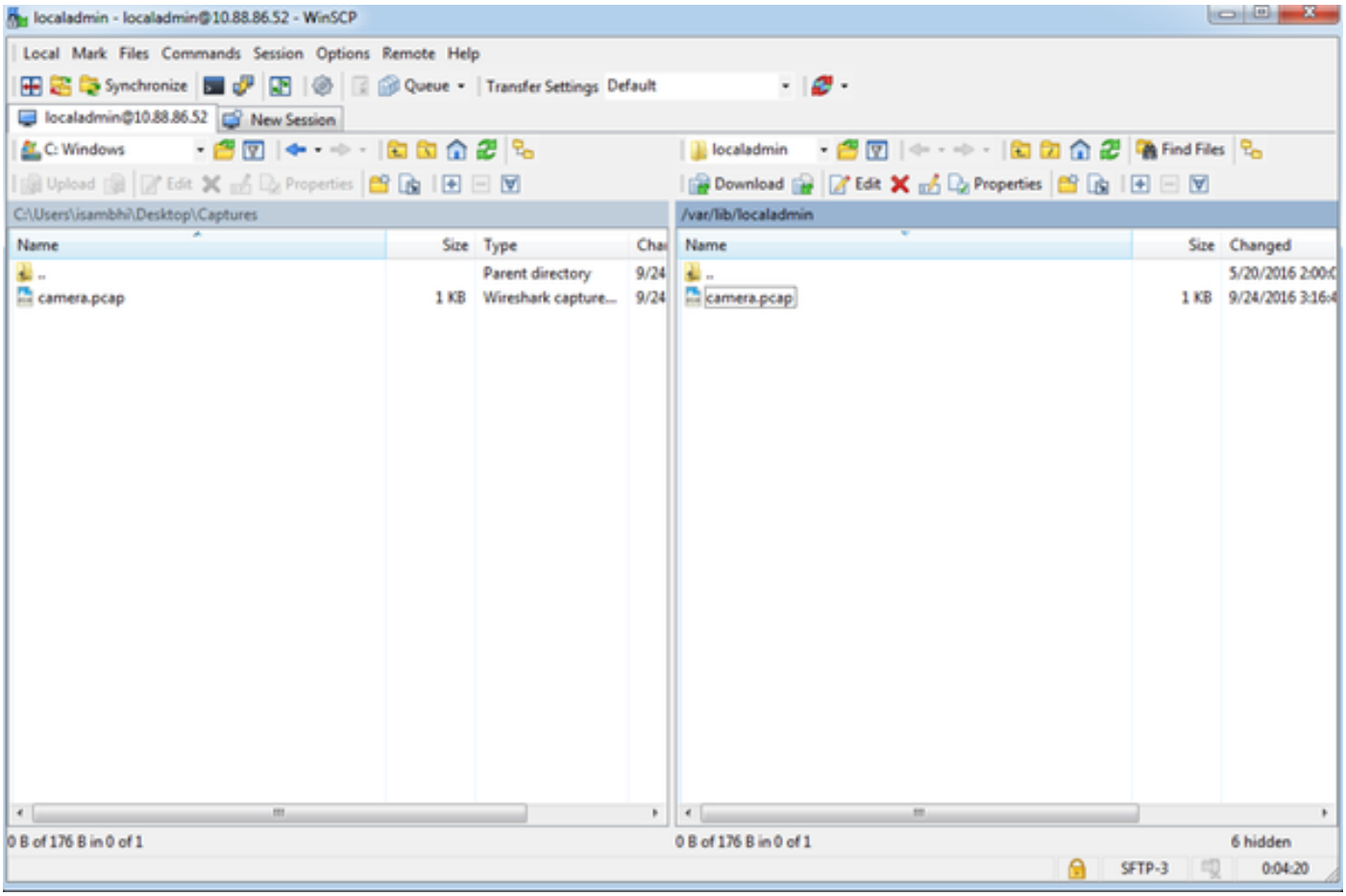
```
[root@cisco localadmin]# tcpdump -s0 -w camera.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byte
s
158 packets captured
158 packets received by filter
0 packets dropped by kernel
[root@cisco localadmin]#
```

Step 4. Collect the Capture from the Server

Use the WinSCP application to SFTP into the server to download the file.



Drag and drop the file from the server onto the desired location on your computer.



Related Information

- If the logs were requested by a Cisco TAC Engineer, they can be uploaded to the TAC case with one of the methods outlined in this document: **http://www.cisco.com/c/en/us/about/security-center/tac-customer-file-uploads.html**
- **Technical Support & Documentation - Cisco Systems**