Contents

Introduction

Prerequisites

Requirements

Component Used

Problem

Troubleshoot

Solution

Related Cisco Support Community Discussions

Introduction

This document describes how to isolate the IP address that sends packets to the Telepresence Management Server (TMS) on behalf of the endpoint, causing the issue. When any managed device is added to TMS, its status shows Reachable on LAN by default for sometime however after sometime the status might change to Behind the Firewall. This generally happens when packets received from device have source IP address different from the system IP address that is received from device's xstatus by the TMS.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Telepresence Endpoint running TC (Telepresence Codec) software or MXP
- TMS

Component Used

This document is not restricted to specific software and hardware versions.

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.

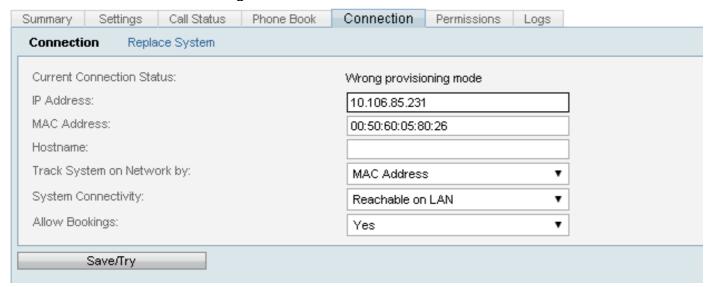
Problem

Endpoints managed by the TMS change from Reachable on LAN status to Behind the firewall status automatically, causing the TMS to stop the management of the device. It is considered that in order to troubleshoot, you must have HTTP communication that is allowed in the network between the managed device and the TMS.

Troubleshoot

In order to verify a packet capture from the TMS is required:

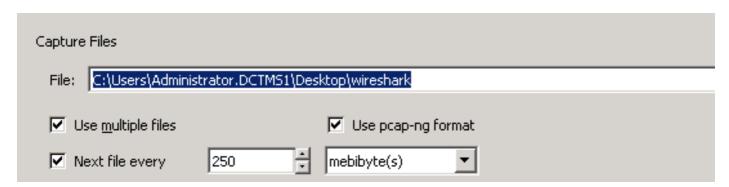
- 1. Connect to TMS server via Remote Desktop Protocol (RDP).
- 2. Ensure that TMS and endpoint have HTTP communication enabled and that HTTPS is disabled.
- 3. Install/Run Wireshark and Select default network interface.
- 4. Do not apply any filter and start the capture.
- 5. Navigate to Connection tab of the endpoint with which you are facing issue, Click **Save/Try** button as shown in this image.



6. When endpoint falls back to behind firewall, stop wireshark capture.

Note: Sometimes the issue might take longer than is expected. To re-create hence while starting the Wireshark capture ensure to save in multiple file.

7. Go to **Capture File** option and select the **Use multiple files** check box.



Open Wireshark

- Apply filter such as xml.cdata ==IP_ADDRESS_OF_DEVICE
- After applying this filter you might see that response will change from actual device ip address to some different ip address.

As shown in this image, the actual IP address of device is x.x.x.174; however later this IP changes to x.x.x.145



Due to change of this IP address, the TMS verifies that the device IP address sent in xstatus is not the same as the IP address in IP header and hence it changes the device to Behind the firewall status.

Solution

To solve this issue you need to ensure that there is no device in the network between the Endpoint and TMS that is changing source IP address in IP header, hence causing the Source IP in the IP header to be different from the actual IP of the endpoint.