

# TMS に追加された TelePresence エンドポイントが自動的にステータスを「Behind the Firewall」に変更する問題のトラブルシューティング

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題](#)

[トラブルシューティング](#)

[解決策](#)

[Cisco サポート コミュニティ - 特集対話](#)

## 概要

この資料に問題を引き起こす IP アドレスを TelePresence 管理 サーバ ( TMS ) にエンドポイントに代わってパケットを送信する隔離する方法を記述されています。どの管理対象装置でも TMS に追加されるとき、ステータスはしかしデフォルトでしばらくの間ファイアウォールの後ろでに変更するかもしれませんことをいつかステータスの後で LAN で到達可能ことを示します。これは一般に TMS によってデバイスの xstatus から届くデバイスから受信されるパケットにシステム IP アドレスと別のソース IP アドレスがあると起こります。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- TC ( TelePresence コーデック ) ソフトウェアが MXP を実行する Cisco TelePresence エンドポイント
- TMS

### 使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## 問題

TMS によって管理されるエンドポイントはファイアウォール ステータスの後ろの LAN ステータスの到達可能から自動的に変更し、デバイスの管理を停止するために TMS を引き起こします。解決するために、管理対象装置と TMS 間のネットワークで許可される HTTP 通信を持たなければならないことが考慮されます。

## トラブルシューティング

TMS からのパケットキャプチャを確認することが必要となります:

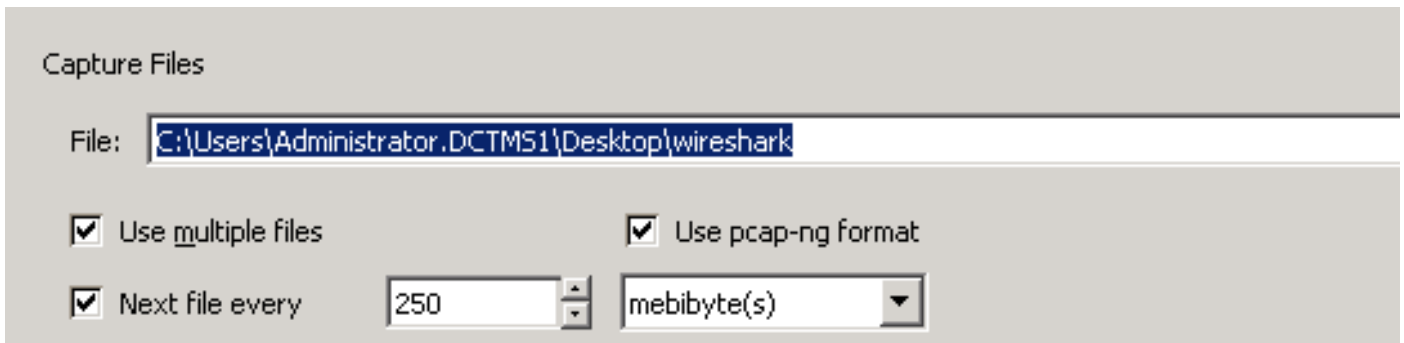
1. リモート デスクトッププロトコル ( RDP ) によって TMS サーバに接続して下さい。
2. TMS におよびエンドポイントに有効になる HTTP 通信があること、そして HTTPS が無効であることを確認して下さい。
3. Wireshark インストールして下さいおよび Select default 実行されたネットワーク インターフェイス。
4. フィルタを適用しないし、キャプチャを開始して下さい。
5. このイメージに示すように『SAVE』をクリックしましたり/試みボタンは問題に直面しているエンドポイントの Connection タブにナビゲートします。

Summary	Settings	Call Status	Phone Book	Connection	Permissions	Logs
<b>Connection</b> <a href="#">Replace System</a>						
Current Connection Status:		Wrong provisioning mode				
IP Address:	<input type="text" value="10.106.85.231"/>					
MAC Address:	<input type="text" value="00:50:60:05:80:26"/>					
Hostname:	<input type="text"/>					
Track System on Network by:	MAC Address ▼					
System Connectivity:	Reachable on LAN ▼					
Allow Bookings:	Yes ▼					
<input type="button" value="Save/Try"/>						

6. エンドポイントが後ろファイアウォールに戻って下るとき、wireshark キャプチャを停止して下さい。

**注:** 時々問題は期待されるより時間がかかるかもしれません。複数のファイルで保存するために Wireshark キャプチャを開始している間それ故に作り直すために確認して下さい。

7. キャプチャ ファイル オプションに行き、使用 **複数のファイル** チェックボックスを選択して下さい。



Wireshark を開いて下さい

- xml.cdata ==IP\_ADDRESS\_OF\_DEVICE のようなフィルタを適用して下さい
- このフィルタを適用した後応答が実機器 IP アドレスから別の IP アドレスに変更することがわかるかもしれません。

このイメージに示すように、デバイスの実際の IP アドレスは x.x.x.174 です; ただしこの IP が x.x.x.145 に変更する以降

No.	Time	Source	Destination	Protocol	Length	Info
5001	45.112269	174	10.61.71.4	HTTP/1.1	1042	POST /tms/public/external/management/systemmanagementservice.asr
5302	45.759734	174	10.61.71.4	HTTP/1.1	104	POST /tms/public/feedback/postdocument.aspx HTTP/1.1
5410	45.938035	174	10.61.71.4	HTTP/1.1	446	POST /tms/public/feedback/postdocument.aspx HTTP/1.1
8025	50.725647	174	10.61.71.4	HTTP/1.1	1038	POST /tms/public/external/management/systemmanagementservice.asr
8419	51.353143	174	10.61.71.4	HTTP/1.1	148	POST /tms/public/feedback/postdocument.aspx HTTP/1.1
9205	52.664311	174	10.61.71.4	HTTP/1.1	914	POST /tms/public/feedback/postdocument.aspx HTTP/1.1
12154	75.116110	145	10.61.71.4	HTTP/1.1	1364	HTTP/1.1 200 OK
12221	75.754949	145	10.61.71.4	HTTP/1.1	155	HTTP/1.1 200 OK
12334	76.496791	145	10.61.71.4	HTTP/1.1	1364	HTTP/1.1 200 OK

この IP アドレスの変更すること当然 TMS は xstatus で送信される デバイス IP アドレスが IP ヘッダーの IP アドレスがそれ故にそれファイアウォール ステータスの後ろのにデバイスを変更する同じではないことを確認し。

## 解決策

IP ヘッダーのソース IP アドレスを変更しているエンドポイントの実際の IP と異ならせませすそれ故に IP ヘッダーで出典 IP を、エンドポイントと TMS 間のネットワークにデバイスがないことを確認する必要があるこの問題を解決するため。