

# Pesquisa defeitos o valor-limite do TelePresence adicionado a TMS que muda atrás do estado do Firewall automaticamente

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componente usado](#)

[Problema](#)

[Troubleshooting](#)

[Solução](#)

[Cisco relacionado apoia discussões da comunidade](#)

## Introdução

Este documento descreve como isolar o endereço IP de Um ou Mais Servidores Cisco ICM NT que envia pacotes ao servidor de gerenciamento do TelePresence (TMS) em nome do valor-limite, causando a edição. Quando todo o dispositivo gerenciado é adicionado a TMS, suas mostras do estado alcançáveis no LAN à revelia para algum dia contudo após algum dia o estado puderam mudar atrás do Firewall. Isto acontece geralmente quando os pacotes recebidos do dispositivo têm o endereço IP de origem diferente do endereço IP do sistema que está recebido do xstatus do dispositivo pelo TMS.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Valor-limite do Cisco TelePresence que executa o software TC (codec do TelePresence) ou o MXP
- TMS

### Componente usado

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

# Problema

Os valores-limite controlados pelo TMS mudam de alcançável no status de LAN atrás do estado do Firewall automaticamente, fazendo com que o TMS pare o Gerenciamento do dispositivo. Considera-se que a fim pesquisar defeitos, você deve ter uma comunicação HTTP que seja permitida na rede entre o dispositivo gerenciado e o TMS.

## Troubleshooting

A fim verificar uma captura de pacote de informação do TMS é exigida:

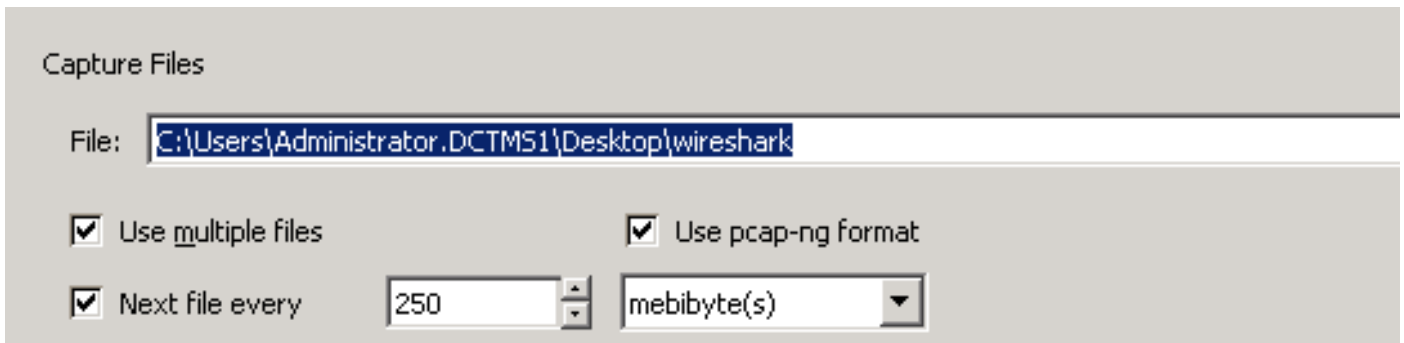
1. Conecte ao server TMS através do protocolo do Desktop remoto (RDP).
2. Assegure-se de que TMS e o valor-limite tenham uma comunicação HTTP permitida e que o HTTPS está desabilitado.
3. Instale/relação de rede padrão executado de Wireshark e Select.
4. Não aplique nenhum filtro e comece a captação.
5. Navegue à aba da conexão do valor-limite com que você está enfrentando a edição, botão da **salvaguarda do clique/tentativa** segundo as indicações desta imagem.

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:	<input type="text" value="MAC Address"/>					
System Connectivity:	<input type="text" value="Reachable on LAN"/>					
Allow Bookings:	<input type="text" value="Yes"/>					
<input type="button" value="Save/Try"/>						

6. Quando o valor-limite cai de volta ao Firewall de trás, pare a captação do wireshark.

Nota: Às vezes a edição pôde tomar mais por muito tempo do que é esperado. Para recriar daqui ao começar a captação de Wireshark assegure para salvar no arquivo múltiplo.

7. Vá à opção do **arquivo de captura** e selecione a caixa de verificação dos **arquivos múltiplos do uso**.



## Abra Wireshark

- Aplique o filtro tal como `xml.cdata == IP_ADDRESS_OF_DEVICE`
- Após ter aplicado este filtro você pôde ver que a resposta mudará do endereço IP de Um ou Mais Servidores Cisco ICM NT do dispositivo real a algum endereço IP de Um ou Mais Servidores Cisco ICM NT diferente.

Segundo as indicações desta imagem, o endereço IP de Um ou Mais Servidores Cisco ICM NT real do dispositivo é x.x.x.174; de qualquer modo mais tarde este IP muda a x.x.x.145

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

Devido mudar deste endereço IP de Um ou Mais Servidores Cisco ICM NT, o TMS verifica que o endereço IP de Um ou Mais Servidores Cisco ICM NT do dispositivo enviado no xstatus não é o mesmo como o endereço IP de Um ou Mais Servidores Cisco ICM NT no cabeçalho IP e daqui ele muda o dispositivo atrás do estado do Firewall.

## Solução

Para resolver esta edição que você precisa de se assegurar de que não haja nenhum dispositivo na rede entre o valor-limite e o TMS que está mudando o endereço IP de origem no cabeçalho IP, daqui fazendo com que o IP da fonte no cabeçalho IP esteja diferente do IP real do valor-limite.