

# Migração de SNMP para telemetria no IOS XR

## Contents

[Introduction](#)

[SNMP](#)

[Componentes do SNMP](#)

[Gerenciador SNMP](#)

[Agente SNMP](#)

[MIB do SNMP](#)

[Operações SNMP](#)

[MIBs e RFCs](#)

[Versões do SNMP](#)

[Modelos Yang](#)

[Modelos OpenConfig](#)

[Modelos nativos](#)

[Telemetria](#)

[Telemetria orientada por modelo](#)

[Telemetria acionada por eventos](#)

[Transporte](#)

[TCP](#)

[gRPC](#)

[gNMI/gNOI](#)

[Codificação](#)

[JSON](#)

[GPB-KV](#)

[GPB](#)

[Configuração de MDT no IOS XR](#)

[Modo de discagem externa](#)

[Modo de discagem](#)

[Migração de SNMP para MDT](#)

[Migração de MIB para XPATH](#)

[BGP4-MIB](#)

[CISCO-BGP4-MIB](#)

[CISCO-CLASS-BASED-QOS-MIB](#)

[CISCO-ENHANCED-MEMPOOL-MIB](#)

[CISCO-ENTITY-FRU-CONTROL-MIB](#)

[CISCO-ENTITY-SENSOR-MIB](#)

[CISCO-FLASH-MIB](#)

[CISCO-PROCESS-MIB](#)

[ENTITY-MIB](#)

[IF-MIB](#)

[IP-MIB](#)

[IPMIB-COMMMON](#)

[LLDP-MIB](#)

[MPLS-TE-STD-MIB](#)

[RFC2465-MIB](#)

[SNMP-MIB](#)

[TCP-MIB](#)

[UDP-MIB](#)

[Migração de interceptações SNMP](#)

[Considerações sobre segurança](#)

## Introduction

Este artigo apresenta os componentes do Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol) e fornece uma correlação entre as implementações atuais com base no monitoramento SNMP na abordagem de Telemetria Orientada a Modelo (MDT - Model Driven Telemetry).

## SNMP

O SNMP é um protocolo da camada de aplicação que fornece um formato de mensagem para comunicação entre gerentes e agentes SNMP. O SNMP fornece uma estrutura padronizada e uma linguagem comum que é usada para monitorar e gerenciar dispositivos em uma rede

## Componentes do SNMP

A estrutura SNMP tem os seguintes componentes, que são descritos nas seguintes seções:

- [Gerenciador SNMP](#)
- [Agente SNMP](#)
- [MIB do SNMP](#)

### Gerenciador SNMP

O gerenciador SNMP é um sistema que controla e monitora as atividades dos hosts de rede usando SNMP. O sistema de gerenciamento mais comum é um sistema de gerenciamento de rede (NMS). O termo NMS pode ser aplicado a um dispositivo dedicado usado para gerenciamento de rede ou aos aplicativos usados nesse dispositivo.

### Agente SNMP

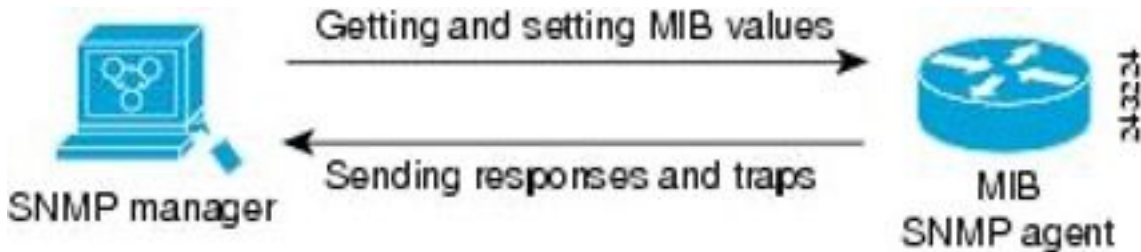
O agente SNMP é o componente de software em um dispositivo gerenciado que mantém os dados do dispositivo e relata esses dados, conforme necessário, para gerenciar sistemas. O agente reside no dispositivo de roteamento (roteador, servidor de acesso ou switch).

### MIB do SNMP

Um agente SNMP contém variáveis MIB, cujos valores podem ser solicitados ou alterados pelo gerenciador SNMP por meio de operações 'Get' ou 'Set'. Um gerente pode obter um valor de um

agente ou armazenar um valor nesse agente. O agente coleta dados do SNMP MIB, o repositório para informações sobre parâmetros de dispositivos e dados de rede. O agente também pode responder às solicitações do gerente para obter ou definir dados.

A figura abaixo ilustra as comunicações entre o gerenciador SNMP e o agente. Um gerente envia solicitações de agente para obter e definir os valores SNMP MIB. O agente responde a essas solicitações. Independentemente dessa interação, o agente pode enviar ao gerente notificações não solicitadas (armadilhas ou informações) para notificar o gerente sobre as condições da rede.



## Operações SNMP

Os aplicativos SNMP executam as seguintes operações para recuperar dados, modificar variáveis de objeto SNMP e enviar notificações:

- [SNMP Get](#)
- [SNMP SET](#)
- [Notificações SNMP](#)

### SNMP Get

A operação SNMP GET é executada por um NMS para recuperar variáveis de objeto SNMP. Há três tipos de operações GET:

- GET—Recupera a instância exata do objeto do agente SNMP.
- GETNEXT—Recupera a próxima variável de objeto, que é um sucessor lexicográfico para a variável especificada.
- GETBULK—Recupera uma grande quantidade de dados de variáveis de objeto, sem a necessidade de operações GETNEXT repetidas.

### SNMP SET

A operação SNMP SET é executada por um NMS para modificar o valor de uma variável de objeto.

### Notificações SNMP

Um recurso importante do SNMP é sua capacidade de gerar notificações não solicitadas de um agente SNMP.

Notificações não solicitadas (assíncronas) podem ser geradas como interceptações ou solicitações de informações (informa). Armadilhas são mensagens que alertam o gerenciador do Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol) sobre uma condição na rede. Informações são armadilhas que incluem uma solicitação de

confirmação de recebimento do gerenciador SNMP. As notificações podem indicar autenticação de usuário inadequada, reinicializações, fechamento de uma conexão, perda de conexão com um dispositivo vizinho ou outros eventos significativos.

As armadilhas são menos confiáveis do que as informações porque o receptor não envia uma confirmação quando recebe uma armadilha. O remetente não sabe se a armadilha foi recebida. Um gerenciador SNMP que recebe uma informação confirma a mensagem com uma PDU (Unidade de Dados de Protocolo) de resposta SNMP. Se o remetente nunca receber uma resposta, a informação poderá ser enviada novamente. Assim, as informações têm mais probabilidade de chegar ao destino desejado.

As armadilhas são geralmente preferidas mesmo que sejam menos confiáveis porque as informações consomem mais recursos no dispositivo e na rede. Ao contrário de uma armadilha, que é descartada assim que é enviada, uma informação deve ser mantida na memória até que uma resposta seja recebida ou a solicitação expire. Além disso, as armadilhas são enviadas apenas uma vez, enquanto que uma informação pode ser enviada várias vezes. As novas tentativas aumentam o tráfego e contribuem para uma sobrecarga mais alta na rede. O uso de armadilhas e informações exige uma compensação entre confiabilidade e recursos.

## MIBs e RFCs

Os módulos da Base de Informações de Gerenciamento (MIB - Management Information Base) geralmente são definidos em documentos de RFC (Request for Comments, Solicitação de Comentários) enviados à Internet Engineering Task Force (IETF), um organismo internacional de padrões. Os RFCs são escritos por indivíduos ou grupos para consideração pela Internet Society e pela comunidade da Internet como um todo, normalmente com a intenção de estabelecer um padrão recomendado para a Internet. Antes de receber o status de RFC, as recomendações são publicadas como documentos de I-D (Internet Draft, rascunho da Internet). Os RFCs que se tornaram padrões recomendados também são rotulados como documentos de padrões (STDs). Você pode saber mais sobre o processo de padrões e as atividades da IETF no site Internet Society em <http://www.isoc.org>. Você pode ler o texto completo de todos os RFCs, I-Ds e STDs mencionados na documentação da Cisco no site da IETF em <http://www.ietf.org>.

A implementação Cisco de SNMP usa as definições de variáveis MIB II descritas em RFC 1213 e definições de armadilhas SNMP descritas em RFC 1215.

A Cisco fornece suas próprias extensões MIB privadas com cada sistema. Os MIBs corporativos da Cisco cumprem as diretrizes descritas nos RFCs relevantes, a menos que indicado de outra forma na documentação. Você pode encontrar os arquivos de definição do módulo MIB e a lista de MIBs suportados em cada plataforma Cisco no site Cisco MIB no Cisco.com.

## Versões do SNMP

Atualmente, os dispositivos Cisco suportam as seguintes versões de SNMP:

- SNMPv1—Simple Network Management Protocol: um padrão completo de Internet, definido no RFC 1157. (O RFC 1157 substitui as versões anteriores publicadas como RFC 1067 e RFC 1098.) A segurança é baseada em community strings.
- SNMPv2c—A estrutura administrativa baseada em string de comunidade para SNMPv2. SNMPv2c (o "c" é para "comunidade") é um protocolo de Internet experimental definido em RFC 1901, RFC 1905 e RFC 1906. O SNMPv2c é uma atualização das operações de

protocolo e dos tipos de dados do SNMPv2p (SNMPv2 Classic) e usa o modelo de segurança baseado em comunidade do SNMPv1.

- **SNMPv3**—Versão 3 do SNMP. O SNMPv3 é um protocolo baseado em padrões interoperáveis definido em RFCs 3413 a 3415. O SNMPv3 fornece acesso seguro a dispositivos autenticando e criptografando pacotes pela rede.

Os recursos de segurança fornecidos em SNMPv3 são os seguintes:

- **Integridade da mensagem**—Garantindo que um pacote não tenha sido adulterado em trânsito.
- **Autenticação**—Determinando se a mensagem é de uma origem válida.
- **Criptografia**—embaralhando o conteúdo de um pacote para evitar que ele seja apreendido por uma origem não autorizada.

O SNMPv1 e o SNMPv2c usam uma forma de segurança baseada na comunidade. A comunidade de gerenciadores SNMP pode acessar o agente MIB é definida por uma string de comunidade.

O suporte a SNMPv2c inclui um mecanismo de recuperação em massa e relatórios detalhados de mensagens de erro para as estações de gerenciamento. O mecanismo de recuperação em massa suporta a recuperação de tabelas e grandes quantidades de informações, minimizando o número de viagens de ida e volta necessárias. O suporte aprimorado de tratamento de erros do SNMPv2c inclui códigos de erro expandidos que distinguem diferentes tipos de erros; essas condições são relatadas por meio de um único código de erro em SNMPv1. Os três tipos de exceções a seguir também são relatados: nenhum objeto, nenhuma instância e fim da exibição MIB.

O SNMPv3 é um modelo de segurança no qual uma estratégia de autenticação é configurada para um usuário e o grupo no qual o usuário reside. Um nível de segurança é o nível de segurança permitido em um modelo de segurança. Uma combinação de um modelo de segurança e um nível de segurança determina qual mecanismo de segurança é usado ao tratar um pacote SNMP.

Três modelos de segurança estão disponíveis: SNMPv1, SNMPv2c e SNMPv3. A tabela abaixo lista as combinações de modelos e níveis de segurança e seus significados.

| Modelo | Nível        | Autenticação  | Criptografia                          | O que acontece  |
|--------|--------------|---|---------------------------------------|---|
| v1     | noAuthNoPriv | String da comunidade                                  | No                                    | Usa uma comparação de série de comunidade para autenticação.  |
| v2c    | noAuthNoPriv | String da comunidade                                  | No                                    | Usa uma comparação de série de comunidade para autenticação.  |
| v3     | noAuthNoPriv | Nome de usuário                                       | No                                    | Usa uma correspondência de nome de usuário para autenticação.   |
| v3     | authNoPriv   | Message Digest 5 (MD5) ou Secure Hash Algorithm (SHA) | No                                    | Fornece autenticação com base nos algoritmos HMAC-MD5 ou HMAC-SHA.  |
| v3     | authPriv     | MD5 ou SHA  | Padrão de criptografia de dados (DES) | Fornece autenticação com base nos algoritmos HMAC-MD5 ou HMAC-SHA. Fornece criptografia DES de 56 bits além da autenticação baseada no padrão CBC-DES (DES-56). |

Um agente SNMP deve ser implementado para usar a versão do SNMP suportada pela estação de gerenciamento. Um agente pode se comunicar com vários gerentes.

O SNMPv3 suporta RFCs 1901 a 1908, 2104, 2206, 2213, 2214 e 2271 a 2275. Para obter informações adicionais sobre o SNMPv3, consulte RFC 2570, Introdução à versão 3 da Estrutura de Gerenciamento de Rede padrão da Internet (este não é um documento de padrões).

## Modelos Yang

Os modelos Yang representam uma abstração estruturada em árvore de um recurso específico ou das características de hardware de um sistema. Em elementos de rede, um modelo Yang pode representar um protocolo de roteamento, arrays internos de sensores físicos. O idioma e a terminologia YANG são descritos no [RFC 6020](#) e atualizados em seguida no [RFC 7950](#). Em nível superior, um modelo Yang organiza os dados que representam a estrutura principal em submódulos e contêineres que são uma lista de subnós relacionados. Vários tipos de nó são explicados a seguir.

Um nó de folha contém dados simples como um inteiro ou uma string. Tem exatamente um valor de um tipo específico e nenhum nó filho.

```
leaf host-name {
    tipo string;
    descrição "Nome de host para este sistema";
}
```

Uma lista de folhas é uma sequência de nós de folha com exatamente um valor de um tipo específico por folha.

```
leaf-list domain-search {
    tipo string;
    descrição "Lista de nomes de domínio a pesquisar";
}
```

Um nó de contêiner é usado para agrupar nós relacionados em uma subárvore. Um contêiner tem apenas nós filho e nenhum valor. Um contêiner pode conter qualquer número de nós filho de qualquer tipo (incluindo folhas, listas, contêineres e listas de folhas).

```
sistema contêiner {
    login do contêiner {
        mensagem de folha {
            tipo string;
            descrição
                "Mensagem fornecida no início da sessão de início de sessão";
        }
    }
}
```

Uma lista define uma sequência de entradas da lista. Cada entrada é como uma estrutura ou uma instância de registro e é identificada exclusivamente pelos valores de seus folhetos principais. Uma lista pode definir vários folhetos principais e pode conter qualquer número de nós filho de qualquer tipo (incluindo folhetos, listas, contêineres, etc.).

Finalmente, um modelo de exemplo que une todos esses tipos de notas se parece com o seguinte exemplo:

```
## Contents of "example-system.yang" module example-system { yang-version 1.1; namespace
"urn:example:system"; prefix "sys"; organization "Example Inc."; contact "joe@example.com";
description "The module for entities implementing the Example system."; revision 2007-06-09 {
description "Initial revision."; } container system { leaf host-name { type string; description
"Hostname for this system."; } leaf-list domain-search { type string; description "List of
domain names to search."; } container login { leaf message { type string; description "Message
given at start of login session."; } list user { key "name"; leaf name { type string; } leaf
full-name { type string; } leaf class { type string; } } } } }
```

No entanto, o idioma Yang usado nos modelos Yang não indica a organização dos dados em contêineres/listas/folhetos. É por isso que um determinado recurso em um elemento de rede pode ser representado por diversos modelos Yang. Este desafio foi abordado com os seguintes tipos de modelos Yang:

- [Modelos OpenConfig](#)
- [Modelos nativos](#)

## Modelos OpenConfig

Os modelos OpenConfig foram desenvolvidos usando uma organização de fornecedores independente para o modelo que representa um recurso específico, o benefício dessa abordagem é que um NMS pode usar esses modelos para interagir com elementos de rede em ambientes de vários fornecedores ou até mesmo de várias plataformas.

Como o nome diz, esses modelos estão abertos e estão disponíveis publicamente para inspeção em repositórios como github neste link:

<https://github.com/openconfig/public/tree/master/release/models>

Como exemplo, você pode encontrar um modelo openconfig para o BGP (Border Gateway Protocol), outro para o LACP (Link Aggregation Control Protocol) e outro para o ISIS, com modelo específico diferente. No caso do BGP, você pode encontrar um modelo para erros de BGP, outro para política de BGP e assim por diante. Os modelos podem ser relacionados, e alguns modelos podem chamar outro pacote yang. Por exemplo, openconfig-bgp-neighbor.yang pertence a openconfig-bgp.yang:

```
module openconfig-bgp { yang-version "1"; ## namespace namespace
"http://openconfig.net/yang/bgp"; prefix "oc-bgp"; ## import some basic inet types import
openconfig-extensions { prefix oc-ext; } import openconfig-rib-bgp { prefix oc-bgprib; } ##
Include the OpenConfig BGP submodules ## Common: defines the groupings that are common across
more than ## one context (where contexts are neighbor, group, global) include openconfig-bgp-
common; ## Multiprotocol: defines the groupings that are common across more ## than one context,
and relate to Multiprotocol include openconfig-bgp-common-multiprotocol; ## Structure: defines
groupings that are shared but are solely used for ## structural reasons. include openconfig-bgp-
common-structure; ## Include peer-group/neighbor/global - these define the groupings ## that are
specific to one context include openconfig-bgp-peer-group; include openconfig-bgp-neighbor;
include openconfig-bgp-global;
```

Resumindo, os modelos OpenConfig são orientados para protocolos comuns a todas as plataformas, como recursos padronizados de IETF ou RFC.

## Modelos nativos

Em contrapartida, os modelos nativos são modelos orientados a fornecedores que abrangem estruturas detalhadas específicas a uma plataforma específica. Por exemplo, modelos que

agrupam sensores de valores físicos dentro de um elemento de rede, como voltagens, temperaturas, contadores ASIC, contadores Fabric e assim por diante. Como eles dependem da plataforma, é comum encontrar modelos específicos para NCS6K, ASR9K ou Cisco 8000.

Como os modelos OpenConfig, os modelos nativos também estão disponíveis no repositório Github:

<https://github.com/YangModels/yang/tree/master/vendor/cisco/xr>

Como esses modelos tendem a ser muito mais específicos e completos do que os modelos OpenConfig, eles estão vinculados a versões de software específicas e sujeitos a alterações entre versões de software.

Há duas categorias principais para modelos nativos:

- Modelos "superiores", usados para recuperar informações de um elemento.

Por exemplo, [Cisco-IOS-XR-eigrp-oper.yang](#)

- Modelos "Cfg", usados para configurar um elemento de rede

Por exemplo, [Cisco-IOS-XR-eigrp-cfg.yang](#)

Em termos gerais, a Telemetria Orientada por Modelo usa modelos "oper" para transmitir dados da infraestrutura e o NMS como o NSO usa modelos "cfg" para fazer alterações na configuração em elementos de rede.

Os modelos Yang nativos e OpenConfig estão presentes no software XR na pasta /pkg/yang e podem ser listados para descobrir se há algum modelo Yang disponível em uma plataforma. Este exemplo é para XRv9k executando cXR 6.4.2:

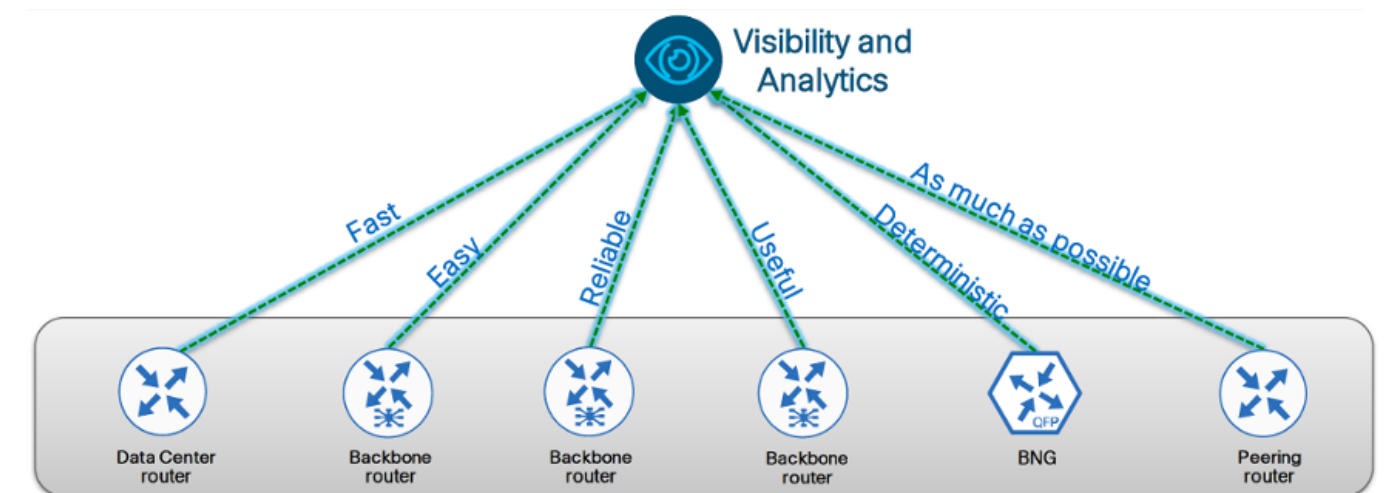
```
RP/0/RP0/CPU0:xrv9k1#run ls /pkg/yang | grep isis
setembro 22 14:21:27.471 CLST
Cisco-IOS-XR-clns-isis-cfg.yang
Cisco-IOS-XR-clns-isis-datatypes.yang
Cisco-IOS-XR-clns-isis-oper-sub1.yang
Cisco-IOS-XR-clns-isis-oper-sub2.yang
Cisco-IOS-XR-clns-isis-oper-sub3.yang
Cisco-IOS-XR-clns-isis-oper.yang
Cisco-IOS-XR-isis-act.yang
openconfig-isis-lsdb-types.yang
openconfig-isis-lsp.yang
openconfig-isis-policy.yang
openconfig-isis-routing.yang
openconfig-isis-types.yang
openconfig-isis.yang
RP/0/RP0/CPU0:xrv9k1#
```



# Telemetria

A telemetria é um processo que permite coletar informações de diferentes elementos remotos em um local central que agrega a visibilidade e a camada de análise.

Em ambientes de rede, os dados podem ser produzidos por todos os elementos da rede, roteadores, switches entre outros e as informações podem estar relacionados a um conjunto muito grande de protocolos específicos, contadores de desempenho ou medidas de sensores físicos.



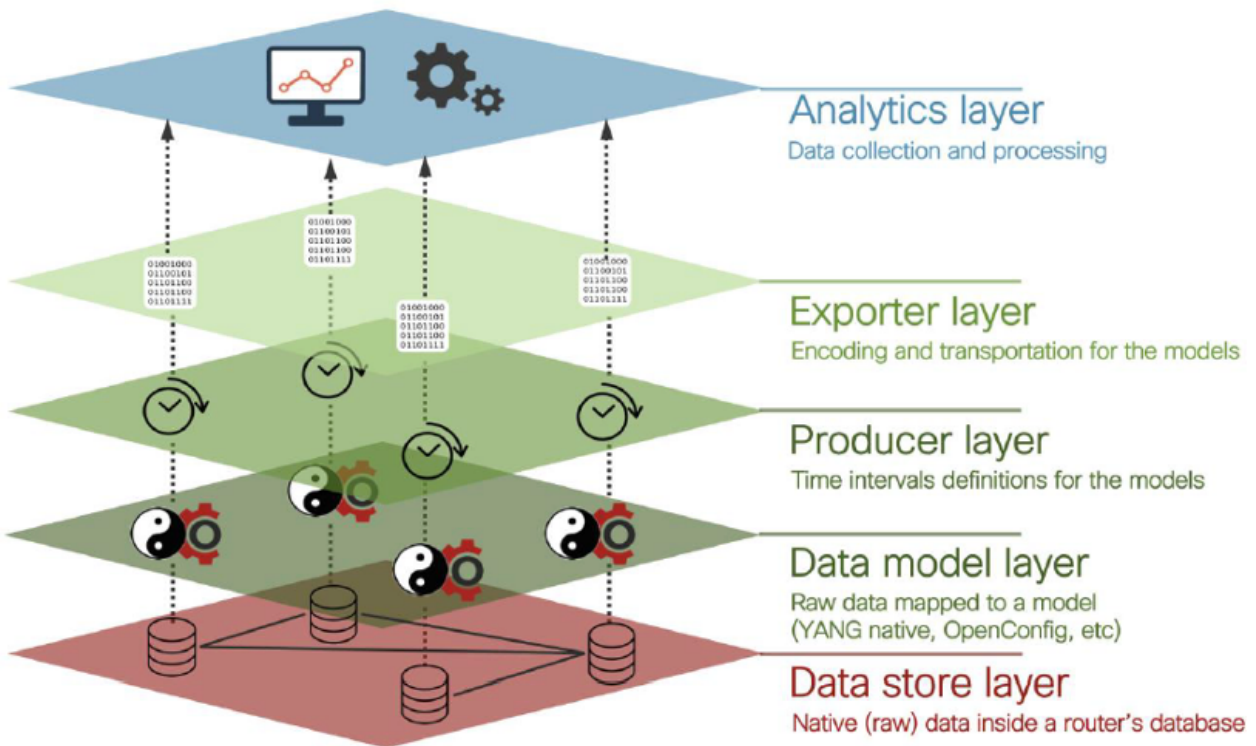
Em geral, as funções de Visibilidade e Análise estão localizadas em pontos centrais nas redes, a transmissão de informações de telemetria é feita usando mecanismos de transporte de rede, de modo que as informações de telemetria devem ser o mais rápido possível, permitindo a expansão.

Ao contrário dos mecanismos legados de SNMP, a telemetria usa um paradigma Push, no qual a rede deve ser provisionada para transmitir seus próprios dados sem ser pesquisada em intervalos regulares, que é a principal característica do monitoramento baseado em SNMP. Essa provisão é frequentemente chamada de assinatura e é baseada em um conjunto de variáveis a serem monitoradas, o intervalo regular para o intervalo de amostragem para coleta de dados e o sistema remoto para enviar esses dados pela rede.

## Telemetria orientada por modelo

MDT afirma Telemetria Orientada por Modelo e, como o nome diz, é baseada em Modelos Yang. Cada aspecto do equipamento de rede pode ser representado por Modelos Yang, por exemplo, tabela de vizinhos OSPF, Sensores RIB ou de temperatura para cada componente em sistemas modulares.

Em relação à arquitetura MDT, ela pode ser dividida nas seguintes camadas:



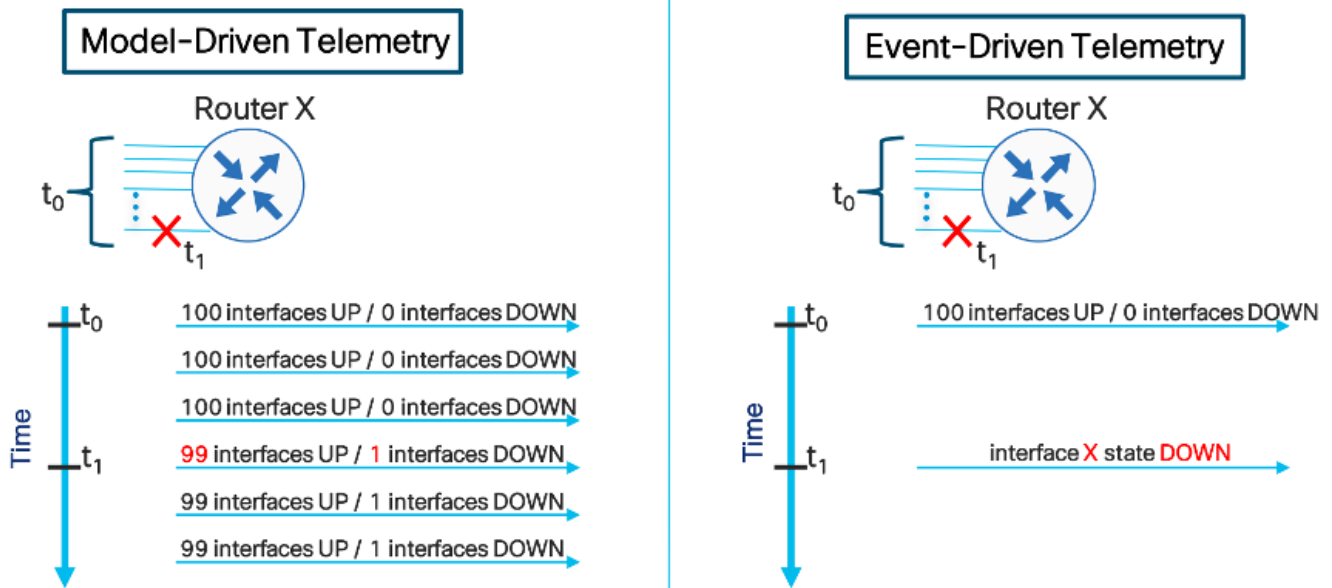
**Note:** Em relação à camada de produtor, na telemetria orientada por modelo, há uma definição de intervalo de amostragem que controla com que frequência o dispositivo consulta o banco de dados interno para dados brutos e organiza esses dados na camada do modelo de dados.

A assinatura de telemetria também define quais modelos e com contêineres/caminho produziram dados a serem transmitidos para a camada de análise. Esta definição teria impacto nas informações relevantes para fins comerciais. A definição de MDT desse caminho do sensor seria analógica para definir OID para recuperação via SNMP, já que ambas as tecnologias produzem dados estruturados em taxa de amostragem definida.

## Telemetria acionada por eventos

EDT significa Telemetria Orientada a Eventos e também se baseia em modelos Yang para a estrutura. A principal diferença é que o disparador para a coleta e o fluxo de dados não é o intervalo regular, mas é um evento específico, como cruzamento de limiares, eventos de enlace, falha de hardware e assim por diante.

A comparação de um evento com Telemetria Orientada por Modelo e Telemetria Orientada por Eventos é apresentada a seguir:



Tip: Esta figura mostra mensagens redundantes usando MDT, mas somente mensagens representando alterações usando EDT.

## Transporte

A telemetria deve ser o mais confiável possível, portanto, faz sentido usar o transporte baseado no Protocolo de Controle de Transmissão (TCP - Transmission Control Protocol) para usar soquetes orientados a sessão entre a infraestrutura e a camada de Análise, que deve implementar coletores para fazer a sessão.

Há duas abordagens principais ao usar a telemetria e elas diferem entre si no fluxo inicial do handshake triplo.

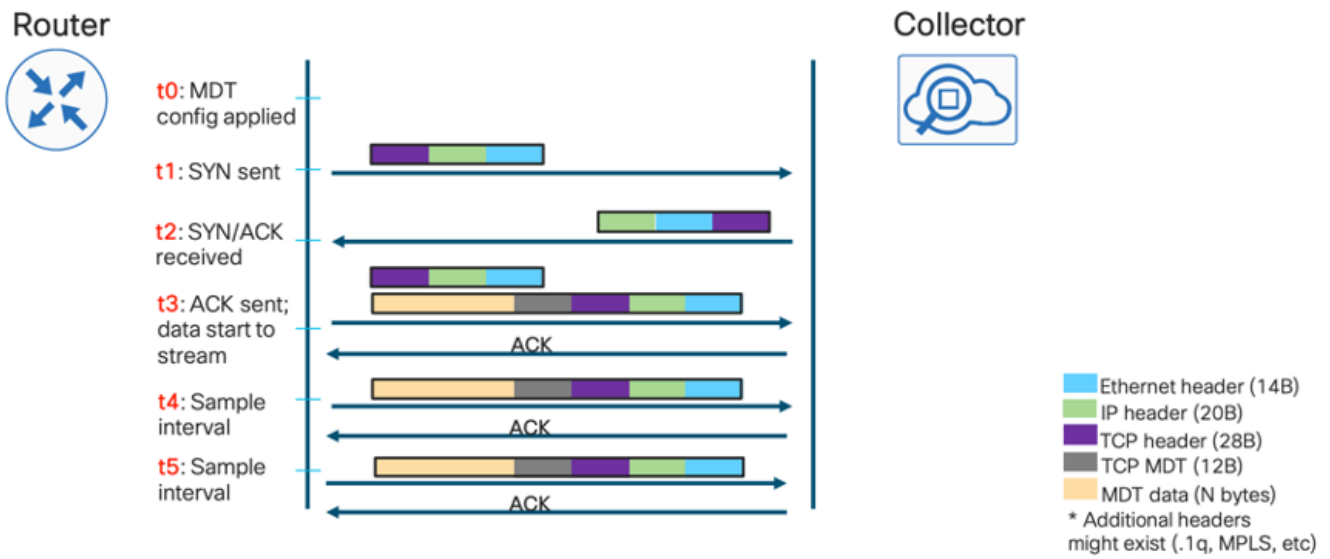


Note: No modo de discagem externa, a configuração da sessão é iniciada no lado da infraestrutura, o que implica que os sensores de interesse devem ser configurados nos elementos da rede. Na restrição, a abordagem de discagem permite uma configuração mais leve em elementos de rede, já que o coletor deve pedir caminhos de sensores específicos na fase de configuração.

## TCP

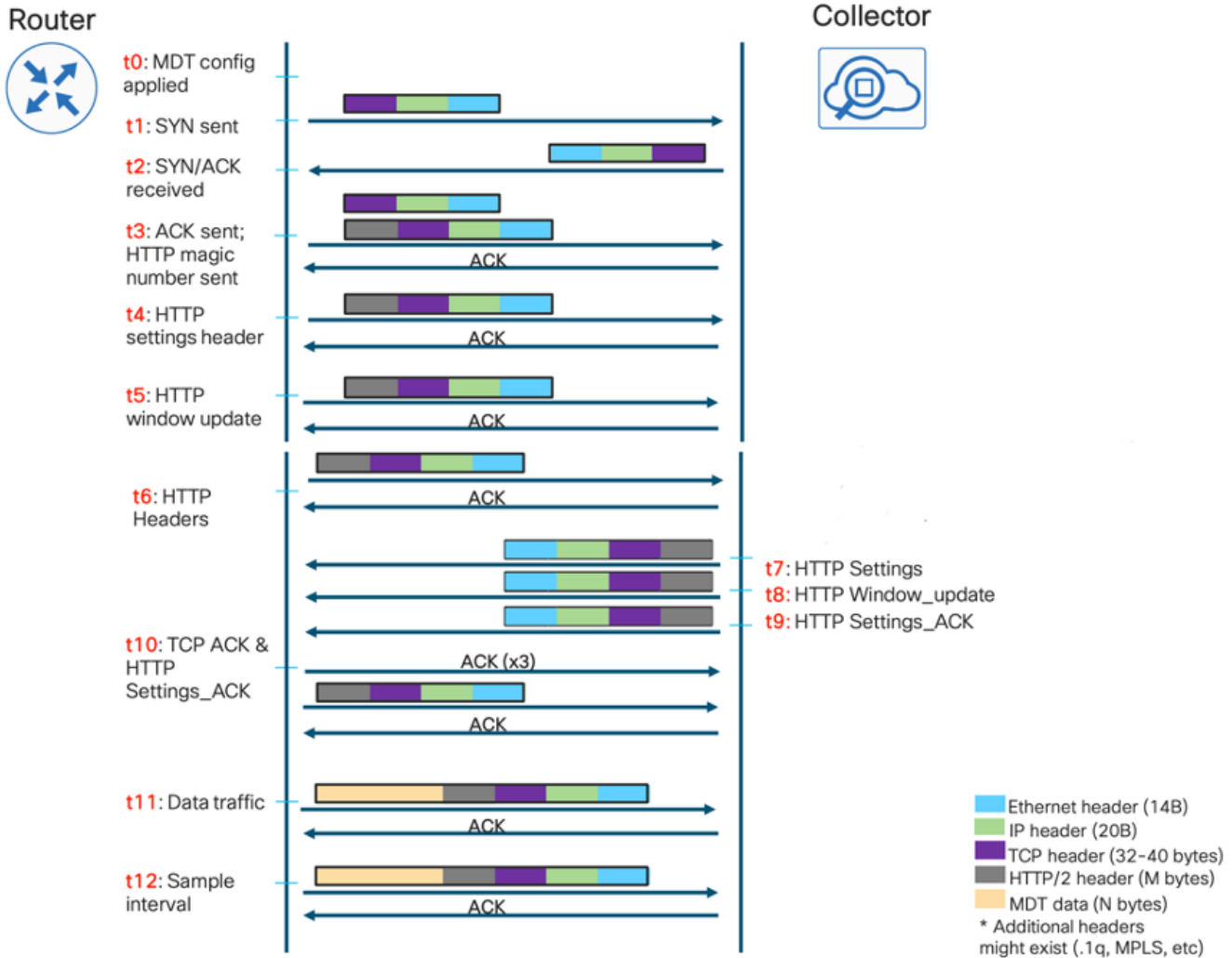
O TCP é a maneira mais simples de fazer uma sessão orientada a conexão entre um elemento de

rede e um coletor de telemetria, e o fluxo de dados começa do Roteador para o Coletor, que enviou o ACK de volta ao roteador para fins de confiabilidade:



## gRPC

Como o Google Protocol RPC (gRPC) funciona no Hypertext Transfer Protocol/2 (HTTP/2), a sessão em si deve se formar na configuração e permite o controle de velocidade do lado do coletor nativamente:



## gNMI/gNOI

gRPC Network Management Interface (gNMI) é o protocolo de gerenciamento de rede gRPC desenvolvido pelo Google. O gNMI fornece o mecanismo para instalar, manipular e excluir a configuração de dispositivos de rede e também para exibir dados operacionais. O conteúdo fornecido através do gNMI pode ser modelado usando o YANG.

O gNMI usa o gRPC-HTTP/2 para configurar uma conexão e fornece um canal bidirecional entre elementos de rede e um NMS que também pode ser um coletor de telemetria, mas também fornece e faz interface para gerenciar os dispositivos.

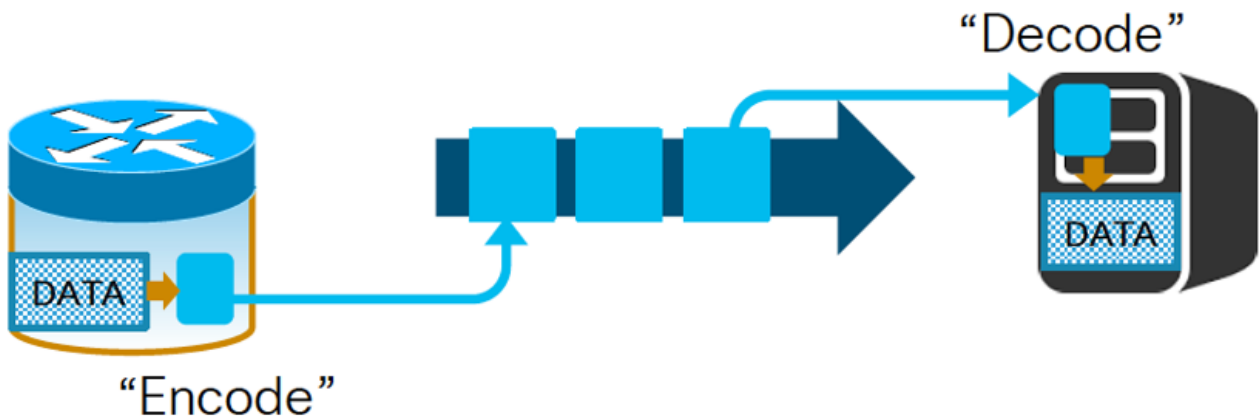
Entre as operações suportadas por este protocolo, podemos encontrar gNMI Get, gNMI Set que retornam as informações solicitadas, mensagens de erro ou de sucesso.

gRPC Network Operations Interface (gNOI) é uma coleção de microsserviços que usa o mesmo canal de comunicação que o gNMI, mas permite operações genéricas não relacionadas à configuração propriamente dita, como ping, reinicialização, alteração de certificados SSL, limpeza, etc.

## Codificação

Os modelos de Yang definem a estrutura dos dados, sua hierarquia e o tipo de cada nó de folha. No entanto, a modelagem não indica como esses dados devem ser serializados. Esse processo

rege a conversão de dados estruturados em um fluxo de bytes a serem enviados pela conexão TCP (TCP bruto, gRPC, gNMI, etc.).



**Note:** Esse processo deve ser implementado com um mecanismo equivalente no elemento de rede que deve codificar os dados, e o coletor deve decodificá-los.

## JSON

O primeiro mecanismo de codificação é o formato JavaScript Object Notation (JSON) nativo, que é bem conhecido, mas orientado para humanos, pois tem cada chave representada como uma string que é ineficiente em termos de tamanho da mensagem. O principal benefício do uso do JSON é que é fácil de analisar e ler como é baseado em texto como o próximo exemplo:

```
{ "node_id_str": "test-IOSXR ", "subscription_id_str": " if_rate", "encoding_path": "Cisco-IOS-XR-
infra-statsdoper:infra-statistics/interfaces/interface/latest/datarate", "collection_id": 49,
"collection_start_time": 1510716302467, "msg_timestamp": 1510716302479, "data_json": [ {
"timestamp": 1510716282334, "keys": { "interface-name": "Null0" }, "content": { "input-data-rate": 0,
"input-packet-rate": 0, "output-data-rate": 0, "output-packet-rate": 0, <> { "timestamp":
1510716282344, "keys": { "interface-name": "GigabitEthernet0/0/0/0" }, "content": { "input-data-
rate": 8, "input-packet-rate": 1, "output-data-rate": 2, "output-packet-rate": 0, <>
"collection_end_time": 1510716302372 } }
```

## GPB-KV

O formato de codificação GPB-KV (Buffers-Key Value) do Google também é chamado de GPB autodescritivo porque usa buffers de protocolo para fazer uso de mensagens que apontam para elementos específicos em modelos Yang. Isso implica que somente um arquivo .proto é necessário para codificar/decodificar finalidades, e as próprias chaves dos dados estão em strings autodescritas.

```
node_id_str: "test-IOSXR" subscription_id_str: "if_rate" encoding_path: "Cisco-IOS-XR-infra-
statsd-oper:infrastatistics/interfaces/interface/latest/data-rate" collection_id: 3
collection_start_time: 1485793813366 msg_timestamp: 1485793813366 data_gpbkv { timestamp:
1485793813374 fields { name: "keys" fields { name: "interface-name" string_value: "Null0" } }
fields { name: "content" fields { name: "input-data-rate" 8: 0 } fields { name: "input-packet-
rate" 8: 0 } fields { name: "output-data-rate" 8: 0 } fields { name: "output-packet-rate" 8: 0 }
<> data_gpbkv { timestamp: 1485793813389 fields { name: "keys" fields { name: "interface-name"
string_value: "GigabitEthernet0/0/0/0" } } fields { name: "content" fields { name: "input-data-
```

```
rate" 8: 8 } fields { name: "input-packet-rate" 8: 1 } fields { name: "output-data-rate" 8: 2 }
fields { name: "output-packet-rate" 8: 0 } <> } ... collection_end_time: 1485793813405
```

## GPB

Finalmente, o Google Protocol Buffers (GPB), também chamado de compact GPB, leva essa abordagem um passo adiante e exige que os arquivos .proto mapeiem cada chave da estrutura, tornando-a muito mais eficiente em termos de tamanho de mensagem, já que tudo é enviado como valores binários. No entanto, a desvantagem é a necessidade de compilar cada arquivo .proto associado a cada modelo Yang suportado pela infraestrutura/coletor.

```
node_id_str: "test-IOSXR" subscription_id_str: "if_rate" encoding_path: "Cisco-IOS-XR-infra-
statsdoper:infrastatistics/interfaces/interface/latest/data-rate" collection_id: 5
collection_start_time: 1485794640452 msg_timestamp: 1485794640452 data_gpb { row { timestamp:
1485794640459 keys: "\n\005Null10" content: "\220\003\000\230\003\000\240\003\000\250\0
03\000\260\003\000\270\003\000\300\003\000\ 310\003\000\320\003\000\330\003\t\340\003\00
0\350\003\000\360\003\377\001" } row { timestamp: 1485794640469 keys:
"\n\026GigabitEthernet0/0/0/0" content: "\220\003\010\230\003\001\240\003\002\250\0
03\000\260\003\000\270\003\000\300\003\000\ 310\003\000\320\003\300\204=\330\003\000\34
0\003\000\350\003\000\360\003\377\001" } collection_end_time: 1485794640480
```

## Configuração de MDT no IOS XR

Os principais componentes usados em dados de telemetria orientados por modelo de fluxo contínuo são:

- Sessão
- Caminho do sensor
- Assinatura
  
- Transporte e codificação

As opções de sessão podem ser Discar ou Discar, conforme discutido anteriormente. Para criar a configuração no IOS XR.

### Modo de discagem externa

para o modo de discagem externa, o roteador inicia uma sessão para os destinos com base na assinatura e o processo deve incluir as seguintes etapas:

- Criar um grupo de destinos
- Criar um grupo de sensores
- Criar uma assinatura
- Validar configuração de discagem externa

Para criar um grupo de destinos, você precisa saber o endereço IP versão 4 (IPv4) / IPv6 (Internet Protocol versão 6) do coletor e a porta que atenderia a esse aplicativo. Além disso, você precisa especificar o protocolo e a codificação que devem ser acordados no dispositivo de rede e no coletor.

Finalmente, talvez seja necessário especificar o Virtual Routing and Forwarding (VRF) usado para se comunicar com o endereço de rede do coletor.

Em seguida, um exemplo de configuração de discagem externa é apresentado:

```
orientado por modelo de telemetria
destination-group DG1
vrf MGMT
address-family ipv4 192.168.122.20 port 5432
codificação autodescritiva-gpb
protocolo tcp
!
```

As opções de codificação são apresentadas em seguida:

```
RP/0/RP0/CPU0:C8000-1(config-model-drive-dest-addr)#encoding ?
codificação GPB
codificação JSON
autodescritivo-gpb Codificação GPB autodescritiva ← também conhecida como GPB-KV
RP/0/RP0/CPU0:C8000-1(config-model-drive-dest-addr)#encoding
```

As opções de protocolos:

```
RP/0/RP0/CPU0:C8000-1(config-model-drive-dest-addr)#protocol ?
grpc gRPC
TCP TCP TCP TCP
UDP udp
RP/0/RP0/CPU0:C8000-1(config-model-drive-dest-addr)#protocol grpc ?
compactação de mensagem gzip gRPC
no-tls No TLS
tls-hostname nome de host TLS
<cr>
RP/0/RP0/CPU0:C8000-1(config-model-drive-dest-addr)#protocol tcp ?
<cr>
RP/0/RP0/CPU0:C8000-1(config-model-drive-dest-addr)#protocol udp ?
tamanho do pacote UDP
<cr>
RP/0/RP0/CPU0:C8000-1(config-model-drive-dest-addr)#protocol udp
```

O protocolo TCP é direto e só precisa das configurações de porta conectadas ao endereço IPv4/IPv6. O User Datagram Protocol (UDP), em contraste, é sem conexão, portanto o status do grupo de destino sempre estará ativo.

A compactação em gRPC pode ser obtida com o uso da palavra-chave opcional **gzip**. O gRPC usa TLS por padrão, portanto, um certificado deve ser instalado localmente no roteador para esse uso. Esse comportamento pode ser substituído pela configuração da palavra-chave **no-tls**. Finalmente, você pode especificar um nome de host diferente para fins de certificado usando a palavra-chave **tls-hostname**.

Em seguida, a seção **sensor-group** deve ser adicionada listando os caminhos do sensor do nosso interesse. Esta seção é direta, mas é importante saber que o próprio **sensor-path** permite que a filtragem otimize vários recursos, como a CPU (Central Processing Unit) e a largura de banda.

```
orientado por modelo de telemetria
sensor-group SG1
sensor-path Cisco-IOS-XR-wdsysmon-fd-oper:system-monitoring/cpu-usage
sensor-path Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface[interface-name='Mgmt*']/data-rate
!
```

**Note:** O formato necessário para um caminho do sensor é <nome do modelo>:<caminho do contêiner>

Este documento apresenta o mapeamento do monitoramento baseado em SNMP usando OID que representa "folhas" nesta abordagem antiga em modelos YANG, representados por XPATHs que correspondem às mesmas "folhas".

O estágio final de configuração deve ser configurar uma assinatura, que vincula o grupo de sensores a uma cadência para a transmissão de telemetria para um grupo de destino.



```
orientado por modelo de telemetria
assinatura SU1
sensor-group-id SG1 sample-interval 5000
destination-id DG1
!
```

Este exemplo usa um intervalo de amostragem de 5000 milissegundos (5 segundos) que é relativo ao fim da coleção anterior. Para alterar esse comportamento, você pode alterar a palavra-chave *sample-interval* com a opção *strict-timer*.

Para verificação, você pode usar o seguinte comando que aborda o status da assinatura. Esse método também permite cobrir informações de sensor-group e destination-group.

```
RP/0/RP0/CPU0:C8000-1#sh assinatura orientada por modelo de telemetria SU1
Qua Nov 18 15:38:01.397 UTC
Assinatura: SU1
—
Estado: ACTIVE
Grupos de sensores:
ID: SG1
Exemplo de intervalo: 5000 ms
Intervalo de pulsação: NA
Caminho do sensor: Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface[interface-name='Mgmt*']/data-rate
Estado do caminho do sensor: resolvido
Caminho do sensor: Cisco-IOS-XR-wdsysmon-fd-oper:monitoramento do sistema/utilização da cpu
Estado do caminho do sensor: resolvido
Grupos de destinos:
ID do grupo: DG1
IP de destino: 192.168.122.10
Porta de destino: 5432
Vrf De Destino: MGMT(0x60000001)
Codificação: gpb autodescritivo
Transporte: tcp
Estado: Ativo
TLS: Falso
Total de bytes enviados: 636284346
Total de pacotes enviados: 4189
Última mensagem enviada: 2020-11-18 15:37:58.1700077650 +0000
Grupos de coleção:
—
ID: 9
Exemplo de intervalo: 5000 ms
Intervalo de pulsação: NA
Pulsação sempre: Falso
Codificação: gpb autodescritivo
Número da coleção: 1407
Tempo de coleta: mínimo: 4 ms máximo: 13 ms
Tempo total: Mín.: 8 ms Média: 10 ms Máx.: 20 ms
Total diferido: 0
Total de erros de envio: 0
Total de quedas de envio: 0
Total de outros erros: 0
Nenhuma instância de dados: 1407
Último Início da Coleta:2020-11-18 15:37:57.1699545994 +0000
Final da última coleta: 2020-11-18 15:37:57.169955589 +0000
Caminho do sensor: Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/data-rate
ID: 10
Exemplo de intervalo: 5000 ms
Intervalo de pulsação: NA
Pulsação sempre: Falso
Codificação: gpb autodescritivo
Número da coleção: 1391
Tempo de coleta: mínimo: 178 ms máximo: 473 ms
Tempo total: Mín.: 247 ms Média: 283 ms Máx.: 559 ms
Total diferido: 0
Total de erros de envio: 0
Total de quedas de envio: 0
Total de outros erros: 0
Nenhuma instância de dados: 0
Último Início da Coleta:2020-11-18 15:37:58.1699805906 +0000
Final da última coleta: 2020-11-18 15:37:58.1700078415 +0000
Caminho do sensor: Cisco-IOS-XR-wdsysmon-fd-oper:monitoramento do sistema/utilização da cpu
RP/0/RP0/CPU0:C8000-1#
```

## Modo de discagem

No modo de discagem de entrada, o coletor inicia a conexão com os elementos de rede. Em seguida, o coletor deve indicar o interesse em criar uma assinatura.

A configuração tem as seguintes etapas:

- Ativar serviço gRPC
- Configurar grupos de sensores
- Verificação

Para habilitar o serviço gRPC, a configuração é exibida em seguida:

```
!  
grpc  
vrf MGMT  
porta 57400  
no-tls  
address-family dual  
!
```

As opções são simples, incluindo o VRF e a porta TCP. Por padrão, o gRPC usa TLS, mas pode ser desabilitado com palavra-chave *no-tls*. Finalmente, a opção *address-family dual* permite a conexão usando IPv4 e IPv6.

Em seguida, a discagem requer a definição de grupos de sensores localmente, que serão usados pelo coletor posteriormente para definir uma assinatura.

```
orientado por modelo de telemetria  
sensor-group SG3  
sensor-path Cisco-IOS-XR-wdsysmon-fd-oper:system-monitoring/cpu-usage  
caminho do sensor Cisco-IOS-XR-fib-common-oper:fib-statistics/node/node/drops  
!  
!
```

Neste ponto, a configuração do modo de discagem de entrada está concluída e o próprio coletor pode fazer uma assinatura do roteador usando o gRPC. Para verificação, você pode fazer a mesma abordagem do modo de discagem externa:

```
RP/0/RP0/CPU0:C8000-1#sh telemetria modelo de assinatura anx-1605878175837  
sex nov 20 13:58:37.894 UTC  
Assinatura: anx-1605878175837
```

```
—  
Estado: ATIVO  
Grupos de sensores:  
ID: SG3  
Exemplo de intervalo: 15000 ms  
Intervalo de pulsação: NA  
Caminho do sensor: Cisco-IOS-XR-wdsysmon-fd-oper:monitoramento do sistema/utilização da cpu  
Estado do caminho do sensor: resolvido  
Caminho do sensor: Cisco-IOS-XR-fib-common-oper:fib-statistics/node/drops  
Estado do caminho do sensor: resolvido  
Grupos de destinos:  
ID do grupo: DialIn_1003  
IP de destino: 192.168.122.10  
Porta de destino: 46974  
Compressão: gzip  
Codificação: json  
Transporte: discagem  
Estado: Ativo  
TLS: Falso  
Total de bytes enviados: 71000035  
Total de pacotes enviados: 509  
Última hora de envio: 2020-11-20 13:58:32.1030932699 +0000  
Grupos de coleção:  
—  
ID: 5  
Exemplo de intervalo: 15000 ms  
Intervalo de pulsação: NA  
Batimento cardíaco sempre: Falso  
Codificação: json  
Número da coleção: 170  
Tempo de coleta: mínimo: 273 ms máx.: 640 ms
```

Tempo total: Mín.: 276 ms Média: 390 ms Máx.: 643 ms  
 Total diferido: 0  
 Total de erros de envio: 0  
 Total de quedas de envio: 0  
 Total de outros erros: 0  
 Nenhuma instância de dados: 0  
 Última Coleta Início:2020-11-20 13:58:32.1030283276 +0000  
 Último Fim da Coleta: 2020-11-20 13:58:32.1030910008 +0000  
 Caminho do sensor: Cisco-IOS-XR-wdsysmon-fd-oper:monitoramento do sistema/utilização da cpu  
 ID: 6  
 Exemplo de intervalo: 15000 ms  
 Intervalo de pulsação: NA  
 Pulsação sempre: Falso  
 Codificação: json  
 Número da coleção: 169  
 Tempo de coleta: mínimo: 15 ms máximo: 33 ms  
 Tempo total: Mín.: 17 ms Média: 22 ms Máx.: 33 ms  
 Total diferido: 0  
 Total de erros de envio: 0  
 Total de quedas de envio: 0  
 Total de outros erros: 0  
 Nenhuma instância de dados: 0  
 Último Início da Coleta:2020-11-20 13:58:32.1030910330 +0000  
 Último Fim da Coleta: 2020-11-20 13:58:32.1030932787 +0000  
 Caminho do sensor: Cisco-IOS-XR-fib-common-oper:fib-statistics/node/drops  
 RP/0/RP0/CPU0:C8000-1#

**Tip: Observe que nenhum cadência, codificação, IP do coletor ou transporte está codificado no roteador para o modo de discagem.**

## Migração de SNMP para MDT

Para realizar a migração do SNMP tradicional para o modelo de telemetria, os seguintes aspectos devem ser abordados:

- Migração de MIB para XPATH
- Migração de interceptações para telemetria
- Considerações sobre segurança

## Migração de MIB para XPATH

Para essa finalidade, poderíamos categorizar a MIB usando sua própria hierarquia, que poderia ser mapeada (pelo menos em alto nível) para uma funcionalidade específica.

### BGP4-MIB

A próxima tabela representa o nome e o número do OID e o XPATH correspondente a ser configurado em grupos de sensores de telemetria orientados por modelo relacionados às sessões de peering do BGP.

| Nome do OID      | Número OID            | Descrição do OID  | XPATH  |
|------------------|-----------------------|---|--|
| bgpPeerLastError | 1.3.6.1.2.1.15.3.1.14 | O último código de erro e subcódigo visto por este peer nesta conexão. Se nenhum erro tiver ocorrido, este campo será zero. Caso contrário, o primeiro byte dessa STRING de OCTET de dois bytes contém o código de erro e o | Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/neighbor-table/neighbor/last-notify-error-code |

|                          |                       |  |  |
|--------------------------|-----------------------|--|--|
|                          |                       | segundo byte contém o subcódigo.   |  |
| bgpPeerOutUpdates        | 1.3.6.1.2.1.15.3.1.11 | O número de mensagens BGP UPDATE transmitidas nesta conexão.   | Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neighbor-af-table/neighbor/update-messages-out          |
| bgpPeerInUpdates         | 1.3.6.1.2.1.15.3.1.10 | O número de mensagens BGP UPDATE recebidas nesta conexão.  | Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neighbor-af-table/neighbor/update-messages-in           |
| bgpPeerNegotiatedVersion | 1.3.6.1.2.1.15.3.1.4  | A versão negociada do BGP em execução entre os dois peers. Esta entrada DEVE ser zero (0), a menos que bgpPeerState esteja no estado openconfirm ou established. Observe que os valores legais para este objeto estão entre 0 e 255.                                   | Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neighbor-af-table/neighbor/negotiation-protocol-version |
| bgpPeerState             | 1.3.6.1.2.1.15.3.1.2  | O estado de conexão do peer BGP.   | Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neighbor-af-table/neighbor/connection-state             |
| bgpPeerRemoteAddr        | 1.3.6.1.2.1.15.3.1.7  | O endereço IP remoto do peer BGP desta entrada.  | Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neighbor-af-table/neighbor/connection-remote-address    |
| bgpPeerLocalAddr         | 1.3.6.1.2.1.15.3.1.5  | O endereço IP local da conexão BGP desta entrada.  | Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neighbor-af-table/neighbor/connection-local-address     |
| bgpPeerFsmSetTime        | 1.3.6.1.2.1.15.3.1.16 | Esse temporizador indica por quanto tempo (em segundos) esse peer está no estado estabelecido ou por quanto tempo se passou desde que esse peer foi o último no estado estabelecido. Ele é definido como zero quando um novo peer é configurado ou quando o roteador é | Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neighbor-af-table/neighbor/connection-established-time  |

inicializado.  
 O estado desejado da conexão BGP. Uma transição de 'stop' para 'start' fará com que o evento de início manual do BGP seja gerado. Uma transição de 'start' para 'stop' fará com que o evento de parada manual do BGP seja gerado. Esse parâmetro pode ser usado para reiniciar conexões de peer BGP. Deve-se ter cuidado ao fornecer acesso de gravação a este objeto sem autenticação adequada.

Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neighbor-af-table/neighbor/connection-admin-status

bgpPeerAdminStatus 1.3.6.1.2.1.15.3.1.3

## CISCO-BGP4-MIB

A próxima tabela representa o nome e o número do OID e o XPATH correspondente a serem configurados em grupos de sensores de telemetria orientados por modelo relacionados ao estado da sessão BGP e ao prefixo interalterado.

| Nome do OID                 | Número OID                     | Descrição do OID   | XPATH   |
|-----------------------------|--------------------------------|--|---|
| cbgpPeer2RemoteAs           | 1.3.6.1.4.1.9.9.187.1.2.5.1.11 | O número do sistema autônomo remoto recebido na mensagem BGP OPEN.         | Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/sessions/session/remote-as                                  |
| cbgpPeer2PrevState          | 1.3.6.1.4.1.9.9.187.1.2.5.1.29 | O estado anterior da conexão de peer BGP.                                  | Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neighbor-af-table/neighbor/previous-connection-state |
| cbgpPeer2State              | 1.3.6.1.4.1.9.9.187.1.2.5.1.3  | O estado de conexão do peer BGP.   | Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neighbor-af-table/neighbor/connection-state          |
| cbgpPeer2LocalAddr          | 1.3.6.1.4.1.9.9.187.1.2.5.1.6  | O endereço IP local da conexão BGP desta entrada.                          | Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neighbor-af-table/neighbor/connection-local-address  |
| cbgpPeer2PrefixosAnunciados | 1.3.6.1.4.1.9.9.187.1.2.8.1.6  | Este contador é incrementado quando um prefixo de rota, que pertence a uma | Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neighbor-af-   |

|                          |                               |   |   |
|--------------------------|-------------------------------|---|---|
|                          |                               | família de endereços, é anunciado nesta conexão. Ela é inicializada a zero quando a conexão é submetida a uma reinicialização forçada.  | table/neighbor/af-data/prefixes-advertise   |
| cbgpPeer2PrefixosAceitos | 1.3.6.1.4.1.9.9.187.1.2.8.1.1 | Número de prefixos de rota aceitos nesta conexão, que pertencem a uma família de endereços.   | Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neighbor-af-table/neighbor/af-data/prefixes-accept   |
| cbgpPeerPrefixLimit      | 1.3.6.1.4.1.9.9.187.1.2.1.1.3 | Número máximo de prefixos de rota aceitos nesta conexão   | Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neighbor-af-table/neighbor/af-data/neighbor-prefix-limit   |
| cbgpPeer2PrefixThreshold | 1.3.6.1.4.1.9.9.187.1.2.8.1.4 | O valor de limite de prefixo (%) para uma família de endereços nesta conexão na qual a mensagem de aviso indicando que a contagem de prefixos é ultrapassada ou a notificação SNMP correspondente é gerada. | Cisco-IOS-XR-ipv4-bgp-oper:bgp/config-instance/config-instance/config-default-vrf/entity-configuration/entity-configuration/af-dependency-config/max-prefix-warning-threshold |

## CISCO-CLASS-BASED-QOS-MIB

A próxima tabela representa o nome e o número do OID e o XPATH correspondente a serem configurados em grupos de sensores de telemetria orientados por modelo relacionados a estatísticas em classes/políticas de Qualidade de Serviço (QoS).

| Nome do OID        | Número OID                       | Descrição do OID   | XPATH   |
|--------------------|----------------------------------|--|---|
| cbQosCMDropBitRate | 1.3.6.1.4.1.9.9.166.1.15.1.1.1.8 | A taxa de bits das quedas por classe como resultado de todos os recursos que podem produzir quedas (por exemplo, polícia, detecção aleatória, etc.). | Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/input/service-policy-names/service-policy-instance/statistics/class-stats/general-stats/total-rate<br>Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/output/service-policy-names/service-policy-instance/statistics/class-stats/general-stats/total-rate |

|                         |                                  |   |  |
|-------------------------|----------------------------------|---|--|
| cbQosCMDropPkt64        | 1.3.6.1.4.1.9.9.166.1.15.1.1.1.4 | O contador de 64 bits de pacotes descartados por classe como resultado de todos os recursos que podem produzir quedas (por exemplo, polícia, detecção aleatória, etc.). | Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/input/service-policy-names/service-policy-instance/statistics/class-stats/general-stats/total-packets<br>Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/output/service-policy-names/service-policy-instance/statistics/class-stats/general-stats/total-packets<br>Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/input/service-policy-names/service-policy-instance/statistics/class-stats/general-stats/pre-policy-match-packets |
| cbQosCMPrePolicyPkt64   | 1.3.6.1.4.1.9.9.166.1.15.1.1.1.3 | A contagem de 64 bits de pacotes de entrada antes de executar qualquer política de QoS.   | Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/output/service-policy-names/service-policy-instance/statistics/class-stats/general-stats/pre-policy-match-packets<br>Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/input/service-policy-names/service-policy-instance/statistics/class-stats/general-stats/pre-policy-match-packets  |
| cbQosCMName             | 1.3.6.1.4.1.9.9.166.1.7.1.1.1    | Nome do Classmap.   | Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/input/service-policy-names/service-policy-instance/statistics/class-stats/class-name<br>Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/input/service-policy-names/service-policy-instance/statistics/class-stats/child-policy/class-stats/general-stats/transmission-bytes  |
| cbQosCMPostPolicyByte64 | 1.3.6.1.4.1.9.9.166.1.15.1.1.1.4 | A contagem de 64 bits de octetos de saída após a execução de políticas de QoS.  | Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/output/service-policy-names/service-policy-instance/statistics/class-stats/child-policy/class-stats/general-stats/transmission-bytes  |
| cbQosIfIndex            | 1.3.6.1.4.1.9.9.166.1.1.1.1.4    | ifIndex para a interface à qual este  | Cisco-IOS-XR-infra-policymgr-oper:policy-  |

|                        |                                |   |  |
|------------------------|--------------------------------|---|--|
|                        |                                | serviço está conectado. Esse campo só faz sentido se a interface lógica tiver um snmp ifIndex. Por exemplo, o valor deste campo não tem significado quando cbQosIfType é controlPlane. Um índice de configuração arbitrário (atribuído pelo sistema) (independente da instância) para cada Objeto. Cada objeto com a mesma configuração compartilha o mesmo índice de configuração. | manager/global/policy-map/policy-map-types/policy-map-type/policy-maps   |
| cbQosConfigIndex       | 1.3.6.1.4.1.9.9.166.1.5.1.1.2  |   | Cisco-IOS-XR-infra-policymgr-oper:policy-manager/global/policy-map/policy-map-types/policy-map-type/policy-maps  |
|                        |                                |   | Cisco-IOS-XR-qos-man-oper:qos/interface-table/interface/input/service-policy-names/service-policy-instance/statistics/class-stats/child-policy/class-stats/general-stats/pre-policy-match-bytes  |
| cbQosCMPrePolicyByte64 | 1.3.6.1.4.1.9.9.166.1.15.1.1.6 | A contagem de 64 bits de octetos de entrada antes de executar qualquer política de QoS.   | Cisco-IOS-XR-qos-man-oper:qos/interface-table/interface/output/service-policy-names/service-policy-instance/statistics/class-stats/child-policy/class-stats/general-stats/pre-policy-match-bytes |

## CISCO-ENHANCED-MEMPOOL-MIB

A tabela a seguir representa o nome e o número do OID e o XPATH correspondente a serem configurados em grupos de sensores de telemetria orientados por modelo relacionados ao uso da memória.

| Nome do OID      | Número OID                    | Descrição do OID  | XPATH  |
|------------------|-------------------------------|---|--|
| cempMemPoolUsado | 1.3.6.1.4.1.9.9.221.1.1.1.1.7 | Indica o número de bytes do pool de memória que estão atualmente em uso por aplicativos na entidade física. | Cisco-IOS-XR-nto-misc-oper:memory-summary/nodes/node/sur-y |



|                   |                                |   |   |
|-------------------|--------------------------------|---|---|
| cempMemPoolHCUsed | 1.3.6.1.4.1.9.9.221.1.1.1.1.18 | Indica o número de bytes do pool de memória que estão atualmente em uso por aplicativos na entidade física. Este objeto é uma versão de 64 bits de cempMemPoolUsed. | Cisco-IOS-XR-nto-misc-oper:memory-summary/node/detail/total                 |
| cempMemPoolHCFree | 1.3.6.1.4.1.9.9.221.1.1.1.1.20 | Indica o número de bytes do pool de memória que estão atualmente não utilizados na entidade física. Este objeto é uma versão de 64 bits do cempMemPoolFree.         | Cisco-IOS-XR-nto-misc-oper:memory-summary/nodes/node/detail/physical-memory |

## CISCO-ENTITY-FRU-CONTROL-MIB

A tabela a seguir representa o nome e o número do OID e o XPATH correspondente a serem configurados em grupos de sensores de telemetria orientados por modelo relacionados às unidades substituíveis em campo no sistema monitorado.

| Nome do OID                    | Número OID                    | Descrição do OID  | XPATH   |
|--------------------------------|-------------------------------|---|---|
| cefcFRUPorostatus              | 1.3.6.1.4.1.9.9.117.1.1.2.1.2 | Estado de energia FRU operacional.  | Cisco-IOS-XR-invmgr-oper:inventário/entidades/atributos/fru-info/power-operational-state        |
| cefcFRUPowerAdminStatus        | 1.3.6.1.4.1.9.9.117.1.1.2.1.1 | Estado de energia FRU desejado administrativamente.   | Cisco-IOS-XR-invmgr-oper:inventário/entidades/atributos/fru-info/power-administrative-state     |
| cefcModuleStatusLastChangeTime | 1.3.6.1.4.1.9.9.117.1.2.1.1.4 | O valor de sysUpTime no momento em que cefcModuleOperStatus é alterado. Este objeto fornece o tempo de atividade do módulo desde que ele foi reinicializado pela última vez. Este objeto não é persistente; se um módulo for reiniciado, desligado, o tempo de ativação começará de zero. | Cisco-IOS-XR-invmgr-oper:inventário/entidades/atributos/fru-info/last-operational-status-change |
| cefcModuleUpTime               | 1.3.6.1.4.1.9.9.117.1.2.1.1.8 |   | Cisco-IOS-XR-invmgr-oper:inventário/entidades/atributos/fru-info/card-up-time                   |

|                       |                               |  |   |
|-----------------------|-------------------------------|--|---|
| cefcModuleResetReason | 1.3.6.1.4.1.9.9.117.1.2.1.1.3 | Este objeto identifica o motivo da última redefinição executada no módulo. | Cisco-IOS-XR-invmgr-oper:inventário/entidade/atributos/fru-info/card-reset-reason |
| cefcModuleOperStatus  | 1.3.6.1.4.1.9.9.117.1.2.1.1.2 | Este objeto mostra o estado operacional do módulo.                         | Cisco-IOS-XR-invmgr-oper:estoque/entidade/atributos/fru-info/operational-state    |
| cefcModuleAdminStatus | 1.3.6.1.4.1.9.9.117.1.2.1.1.1 | Este objeto fornece controle administrativo do módulo.                     | Cisco-IOS-XR-invmgr-oper:estoque/entidade/atributos/fru-info/administration-state |

## CISCO-ENTITY-SENSOR-MIB

A próxima tabela representa o nome e o número do OID e o XPATH correspondente a serem configurados em grupos de sensores de telemetria orientados por modelo relacionados a entidades de sensores no nó.

| Nome do OID                  | Número OID                   | Descrição do OID   | XPATH   |
|------------------------------|------------------------------|--|---|
| entSensorValue               | 1.3.6.1.4.1.9.9.91.1.1.1.1.4 | Esta variável relata a medição mais recente vista pelo sensor. Para exibir ou interpretar corretamente o valor desta variável, você também deve conhecer entSensorType, entSensorScale e entSensorPrecision. Entretanto, você pode comparar entSensorValue com os valores de limite fornecidos em entSensorThresholdTable sem nenhum conhecimento semântico. Esta variável indica o resultado da avaliação mais recente do limite. Se a condição de limite for verdadeira, | Cisco-IOS-XR-invmgr-oper:inventário/entidade/atributos/fru-info/sensor-info/value |
| entSensorThresholdEvaluation | 1.3.6.1.4.1.9.9.91.1.2.1.1.5 | entSensorThresholdEvaluation é verdadeiro(1). Se a condição de limite for falsa, entSensorThresholdEvaluation é falso(2). Os limites são avaliados à taxa indicada por entSensorValueUpdateRate.   | Cisco-IOS-XR-invmgr-oper:inventário/entidade/atributos/lin                        |

## CISCO-FLASH-MIB

A tabela a seguir representa o nome e o número do OID e o XPATH correspondente a serem configurados em grupos de sensores de telemetria orientados por modelo relacionados ao armazenamento em flash no sistema.

| Nome do OID                          | Número OID                      | Descrição do OID  | XPATH  |
|--------------------------------------|---------------------------------|---|--|
| ciscoFlashPartitionName              | 1.3.6.1.4.1.9.9.10.1.1.4.1.1.10 | <p>Nome da partição Flash usado para se referir a uma partição pelo sistema. Pode ser qualquer sequência de caracteres alfanuméricos da forma AAAAAAAAnn, em que A representa um caractere alfa opcional e um caractere numérico. Qualquer caractere numérico deve sempre formar a parte final da string. O sistema removerá os caracteres alfabéticos e usará a parte numérica para mapear para um índice de partição. As operações em Flash são direcionadas para uma partição de dispositivo com base nesse nome. O sistema tem um conceito de partição padrão. Essa seria a primeira partição no dispositivo. O sistema direciona uma operação para a partição padrão sempre que um nome de partição não é especificado. O nome da partição é, portanto, obrigatório, exceto quando a operação está sendo feita na partição padrão, ou o dispositivo tem apenas uma partição (não está particionado). Tamanho da partição Flash. Deve ser um múltiplo integral de</p> | Cisco-IOS-XR-shellutil-filesystem/oper:file-system/node/file-system/type       |
| CiscoFlashPartitionSizeExtended      | 1.3.6.1.4.1.9.9.10.1.1.4.1.1.13 | <p>ciscoFlashDeviceMinPartitionSize. Se houver uma única partição, esse tamanho será igual a ciscoFlashDeviceSize. Este objeto é uma versão de 64 bits de</p>   | Cisco-IOS-XR-shellutil-filesystem/oper:file-system/node/file-system/size       |
| ciscoFlashPartitionFreeSpaceExtended | 1.3.6.1.4.1.9.9.10.1.1.4.1.1.14 | <p>Espaço livre em uma partição Flash. Observe que</p>  | Cisco-IOS-XR-shellutil-filesystem/oper:file-system/node/file-system/free-space |

o tamanho real de um arquivo em Flash inclui uma pequena sobrecarga que representa o cabeçalho do arquivo do sistema de arquivos. Alguns sistemas de arquivos também podem ter uma sobrecarga de cabeçalho de partição ou dispositivo a ser considerada ao calcular o espaço livre. O espaço livre será calculado como o tamanho total da partição menos o tamanho de todos os arquivos existentes (arquivos válidos/inválidos/excluídos e incluindo o cabeçalho do arquivo de cada arquivo), menor tamanho de qualquer cabeçalho da partição, menor tamanho do cabeçalho do próximo arquivo a ser copiado. Resumindo, este objeto fornecerá o tamanho do maior arquivo no qual pode ser copiado. Não se espera que a entidade de gerenciamento conheça ou use quaisquer despesas gerais, como tamanho de cabeçalho de arquivo e partição, já que essas despesas gerais podem variar de sistema de arquivos a sistema de arquivos. Os arquivos excluídos na Flash não liberam espaço. Uma partição pode ter que ser apagada para recuperar o espaço ocupado pelos arquivos. Este objeto é uma versão de 64 bits do `ciscoFlashPartitionFreeSpace` e

`oper:file-system/node/file-system/free`

## CISCO-PROCESS-MIB

A próxima tabela representa o nome e o número do OID e o XPATH correspondente a ser

configurado em grupos de sensores de telemetria orientados por modelo relacionados ao uso da CPU e alocação de recursos para processos.

| Nome do OID                 | Número OID                     | Descrição do OID  | XPATH   |
|-----------------------------|--------------------------------|---|---|
| cpmCPUTotal1minRev          | 1.3.6.1.4.1.9.9.109.1.1.1.1.7  | O percentual geral de ocupação da CPU no último período de 1 minuto. Este objeto pretere o objeto cpmCPUTotal1min e aumenta o intervalo de valores para (0.100).  | Cisco-IOS-XR-wdsysmon-fd-oper:system-monitoring/cpu-usage/total-cpu-one-minute              |
| cpmCPUTotal5minRev          | 1.3.6.1.4.1.9.9.109.1.1.1.1.8  | O percentual geral de ocupação da CPU no último período de 5 minutos. Este objeto pretere o objeto cpmCPUTotal5min e aumenta o intervalo de valores para (0.100).   | Cisco-IOS-XR-wdsysmon-fd-oper:system-monitoring/cpu-usage/total-cpu-five-minutes            |
| cpmCPUTotal15minRev         | 1.3.6.1.4.1.9.9.109.1.1.1.1.31 | O percentual geral de ocupação da CPU no último período de 15 minutos. Este objeto pretere o objeto cpmCPUTotal15min e aumenta o intervalo de valores para (0.100).   | Cisco-IOS-XR-wdsysmon-fd-oper:sistema-monitoramento/cpu-utilização/total-cpu-quinze minutos |
| cpmProcessName              | 1.3.6.1.4.1.9.9.109.1.2.1.1.2  | O nome associado a este processo. Se o nome tiver mais de 32 caracteres, ele será truncado para os primeiros 31 caracteres e um `*` será anexado como o último caractere a indicar que este é um nome de processo truncado. | Cisco-IOS-XR-wdsysmon-fd-oper:system-monitoring/cpu-usage/process-cpu/process-name          |
| cpmProcessTextSegmentSize   | 1.3.6.1.4.1.9.9.109.1.2.3.1.15 | Indica a memória de texto de um processo e de todos os seus objetos compartilhados.   | Cisco-IOS-XR-processes-memory/nodes/node-ids/process-ids/seg-size                           |
| cpmProcessDynamicMemorySize | 1.3.6.1.4.1.9.9.109.1.2.3.1.18 | Isso indica a quantidade de memória dinâmica que está sendo usada pelo processo.  | Cisco-IOS-XR-processes-memory/nodes/node-ids/process-ids/limit                              |
| cpmProcessDataSegmentSize   | 1.3.6.1.4.1.9.9.109.1.2.3.1.16 | Isso indica o segmento de dados de um processo e todos os seus objetos compartilhados.  | Cisco-IOS-XR-processes-memory/nodes/node-ids/process-ids/seg-size                           |
| cpmProcExtMemAllocations    | 1.3.6.1.4.1.9.9.109.1.2.3.1.1  | A soma de toda a memória alocada dinamicamente  | Cisco-IOS-XR-processes-   |

|                       |                               |  |  |
|-----------------------|-------------------------------|--|--|
| cpmProcExtMemFreedRev | 1.3.6.1.4.1.9.9.109.1.2.3.1.2 | que esse processo recebeu do sistema. Isso inclui a memória que pode ter sido retornada. A soma da memória livre é fornecida por cpmProcExtMemFreedRev. Este objeto substitui cpmProcExtMemAllocado. A soma de toda a memória que este processo retornou ao sistema. Este objeto substitui cpmProcExtMemFreed. | memory/nodes/nod<br>cess-ids/process-id<br><br>Cisco-IOS-XR-proc<br>oper:processes-<br>memory/nodes/nod<br>cess-ids/process-id |
|-----------------------|-------------------------------|--|--|

## ENTITY-MIB

A tabela a seguir representa o nome e o número do OID e o XPATH correspondente a ser configurado em entidades físicas relacionadas a grupos de sensores de telemetria orientados por modelo no sistema.

| Nome do OID     | Número OID               | Descrição do OID   | XPATH  |
|-----------------|--------------------------|--|--|
| entPhysicalName | 1.3.6.1.2.1.47.1.1.1.1.7 | O nome textual da entidade física. O valor desse objeto deve ser o nome do componente conforme atribuído pelo dispositivo local e deve ser adequado para uso em comandos inseridos no `console` do dispositivo. Pode ser um nome de texto, como `console` ou um número de componente simples (por exemplo, número de porta ou de módulo), como `1`, dependendo da sintaxe de nome do componente físico do dispositivo. Se não houver um nome local ou se este objeto não for aplicável, então este objeto contém uma string de comprimento zero. Observe que o valor de entPhysicalName para duas entidades físicas será o mesmo caso a interface do console não faça distinção entre elas, por exemplo, slot-1 e placa no slot-1. | Cisco-IOS-XR-snm<br>entitymib-oper:entity-<br>physical-index |
| entLogicalDescr | 1.3.6.1.2.1.47.1.2.1.1.2 | Uma descrição textual da entidade lógica. Este objeto deve conter uma cadeia de  | Cisco-IOS-XR-snm<br>agent-<br>oper:snmp/informatio           |

|                        |                          |   |   |
|------------------------|--------------------------|---|---|
|                        |                          | caracteres que identifique o nome do fabricante para a entidade lógica e deve ser definido para um valor distinto para cada versão da entidade lógica.  | em-name/  |
| entPhysicalDescr       | 1.3.6.1.2.1.47.1.1.1.1.2 | Uma descrição textual da entidade física. Este objeto deve conter uma cadeia de caracteres que identifique o nome do fabricante para a entidade física e deve ser definido para um valor distinto para cada versão ou modelo da entidade física. O valor de entPhysicalIndex para a entidade física que 'contém' esta entidade física. Um valor zero indica que essa entidade física não está contida em nenhuma outra entidade física. Observe que o conjunto de relações de "contenção" define uma hierarquia estrita; isto é, recursão não é permitida. No caso de uma entidade física ser contida por mais de uma entidade física (por exemplo, módulos double-wide), este objeto deve identificar a entidade que contém o menor valor de entPhysicalIndex. | Cisco-IOS-XR-snmp-agent-oper:snmp/Cisco-IOS-XR-snmp-entity-mib/oper:entity-mib/entity-physical-indexes/ |
| entPhysicalContidosEm  | 1.3.6.1.2.1.47.1.1.1.1.4 | Uma indicação do tipo de hardware geral da entidade física. Um agente deve definir esse objeto com o valor de enumeração padrão que indica com mais precisão a classe geral da entidade física ou a classe primária se houver mais de uma. Se não existir um identificador de registro padrão apropriado para esta entidade física, o valor 'other(1)' será retornado. Se o valor for desconhecido por esse agente, o valor 'desconhecido(2)' será retornado.   | Cisco-IOS-XR-invmgr-oper:inventário/entidade/atributos/inv-bag/unique-id                                |
| entPhysicalClass       | 1.3.6.1.2.1.47.1.1.1.1.5 | A string de revisão de hardware específica do   | Cisco-IOS-XR-invmgr-oper:inventário/entidade  |
| entPhysicalHardwareRev | 1.3.6.1.2.1.47.1.1.1.1.8 |   | Cisco-IOS-XR-invmgr-oper:inventário/entidade  |

fornecedor para a entidade física. O valor preferencial é o identificador de revisão de hardware realmente impresso no próprio componente (se presente). Observe que se as informações de revisão forem armazenadas internamente em um formato não imprimível (por exemplo, binário), o agente deverá converter essas informações em um formato imprimível, de maneira específica da implementação. Se nenhuma string de revisão de hardware específica estiver associada ao componente físico, ou se essa informação for desconhecida do agente, esse objeto conterá uma string de comprimento zero.

A string de revisão de firmware específica do fornecedor para a entidade física. Observe que se as informações de revisão forem armazenadas internamente em um formato não imprimível (por exemplo, binário), o agente deverá converter essas informações em um formato imprimível, de maneira específica da implementação. Se nenhum programa de firmware específico estiver associado ao componente físico, ou se essas informações forem desconhecidas do agente, esse objeto conterá uma string de comprimento zero.

A string de revisão de software específica do fornecedor para a entidade física. Observe que se as informações de revisão forem armazenadas internamente em um formato não imprimível (por exemplo, binário), o agente deverá converter essas informações em um formato imprimível, de

ntidade/atributos/inv-b  
bag/revisão de hardw

Cisco-IOS-XR-invmgr  
oper:inventário/entida  
ntidade/atributos/inv-b  
bag/firmware-revisão

Cisco-IOS-XR-invmgr  
oper:inventário/entida  
ntidade/atributos/inv-b  
bag/revisão de softwa

entPhysicalFirmwareRev 1.3.6.1.2.1.47.1.1.1.1.9

entPhysicalSoftwareRev 1.3.6.1.2.1.47.1.1.1.1.10



maneira específica da implementação. Se nenhum programa de software específico estiver associado ao componente físico, ou se essas informações forem desconhecidas do agente, esse objeto conterá uma string de comprimento zero. A cadeia de caracteres do número de série específica do fornecedor para a entidade física. O valor preferido é a sequência de caracteres do número de série realmente impressa no próprio componente (se presente). Na primeira instância de uma entidade física, o valor de entPhysicalSerialNum associado a essa entidade é definido como o número de série atribuído pelo fornecedor correto, se essas informações estiverem disponíveis para o agente. Se um número de série for desconhecido ou inexistente, entPhysicalSerialNum será definido como uma string de comprimento zero. Observe que as implementações que podem identificar corretamente os números de série de todas as entidades físicas instaladas não precisam fornecer acesso de gravação ao objeto entPhysicalSerialNum. Os agentes que não podem fornecer armazenamento não volátil para as strings entPhysicalSerialNum não são necessários para implementar acesso de gravação para este objeto. Nem todos os componentes físicos terão um número de série, ou mesmo precisarão de um. As entidades físicas para as quais o valor associado do objeto

entPhysicalSerialNum

1.3.6.1.2.1.47.1.1.1.1.11

Cisco-IOS-XR-invmgr  
oper:inventário/entida  
ntidade/atributos/inv-t  
bag/número de série

entPhysicalIsFRU é igual a 'false(2)' (por exemplo, as portas do repetidor dentro de um módulo do repetidor) não precisam de seu próprio número de série exclusivo. Um agente não precisa fornecer acesso de gravação para tais entidades e pode retornar uma string de comprimento zero. Se o acesso de gravação for implementado para uma instância de entPhysicalSerialNum, e um valor for gravado na instância, o agente deverá reter o valor fornecido na instância entPhysicalSerialNum associada à mesma entidade física enquanto essa entidade permanecer instanciada. Isso inclui instanciações em todas as reinicializações/reinicializações do sistema de gerenciamento de rede, incluindo aquelas que resultam em uma alteração do valor entPhysicalIndex da entidade física. O nome do fabricante deste componente físico. O valor preferido é a string do nome do fabricante realmente impressa no próprio componente (se presente). Observe que as comparações entre instâncias dos objetos entPhysicalModelName, entPhysicalFirmwareRev, entPhysicalSoftwareRev e entPhysicalSerialNum são significativas apenas entre entPhysicalEntries com o mesmo valor de entPhysicalMfgName. Se a cadeia de caracteres do nome do fabricante associada ao componente físico for desconhecida do agente, esse objeto conterá uma

entPhysicalMfgName

1.3.6.1.2.1.47.1.1.1.1.12

Cisco-IOS-XR-invmgr-oper:inventário/entidade/atributos/inv-bag/nome do fabricante

|                      |                           |   |   |
|----------------------|---------------------------|---|---|
| entPhysicalModelName | 1.3.6.1.2.1.47.1.1.1.1.13 | cadeia de caracteres de comprimento zero.<br>A cadeia de identificação do nome do modelo específico do fornecedor associada a este componente físico. O valor preferencial é o número de peça visível ao cliente, que pode ser impresso no próprio componente. Se a string do nome do modelo associada ao componente físico for desconhecida para o agente, esse objeto conterá uma string de comprimento zero. | Cisco-IOS-XR-invmgr-oper:inventário/entidade/atributos/inv-bag/model-name |
|----------------------|---------------------------|---|---|

## IF-MIB

A tabela a seguir representa o nome e o número do OID e o XPATH correspondente a serem configurados em grupos de sensores de telemetria orientados por modelo relacionados às características da interface e aos contadores.

| Nome do OID   | Número OID          | Descrição do OID   | XPATH  |
|---------------|---------------------|--|--|
| ifMtu         | 1.3.6.1.2.1.2.2.1.4 | O tamanho do maior pacote que pode ser enviado/recebido na interface, especificado em octetos. Para interfaces usadas para transmitir datagramas de rede, esse é o tamanho do maior datagrama de rede que pode ser enviado na interface.   | Cisco-IOS-XR-pfi-im-oper:interfaces/interface-xr/interface/mtu   |
| ifPhysAddress | 1.3.6.1.2.1.2.2.1.6 | O endereço da interface em sua sub-camada de protocolo. Por exemplo, para uma interface 802.x, esse objeto normalmente contém um endereço MAC. A MIB específica de mídia da interface deve definir a ordem de bits e bytes e o formato do valor desse objeto. Para interfaces que não têm esse endereço (por exemplo, uma linha serial), este objeto deve conter uma string de octeto de comprimento zero. | Cisco-IOS-XR-pfi-im-oper:interfaces/interface-xr/interface/interface-type-information/bundle-information/member/maddress |
| ifType        | 1.3.6.1.2.1.2.2.1.3 | O tipo de interface. Valores adicionais para ifType são atribuídos pela Internet Assigned Numbers Authority (IANA), por meio da  | Cisco-IOS-XR-pfi-im-oper:interfaces/interface-xr/interface/interface-type  |

|                  |                         |   |   |
|------------------|-------------------------|---|---|
| ifOutUcastPkts   | 1.3.6.1.2.1.2.2.1.17    | <p>atualização da sintaxe da convenção textual IANAifType. O número total de pacotes que os protocolos de nível mais alto pediram para serem transmitidos e que não foram endereçados a um endereço multicast ou de broadcast nessa subcamada, incluindo os que foram descartados ou não enviados. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime. O número total de pacotes que os protocolos de nível mais alto pediram para serem transmitidos e que não foram endereçados a um endereço multicast ou de broadcast nessa subcamada, incluindo os que foram descartados ou não enviados. Este objeto é uma versão de 64 bits de ifOutUcastPkts. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime.</p> | Cisco-IOS-XR-pfi-im-c<br>oper:interfaces/interfac<br>xr/interface/interface-<br>statistics/full-interface-<br>stats/packets-sent    |
| ifHCOutUcastPkts | 1.3.6.1.2.1.31.1.1.1.11 | <p>O número total de pacotes que os protocolos de nível mais alto pediram para serem transmitidos e que não foram endereçados a um endereço multicast ou de broadcast nessa subcamada, incluindo os que foram descartados ou não enviados. Este objeto é uma versão de 64 bits de ifOutUcastPkts. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime.</p>   | Cisco-IOS-XR-pfi-im-c<br>oper:interfaces/interfac<br>xr/interface/interface-<br>statistics/full-interface-<br>stats/packets-sent    |
| ifInUcastPkts    | 1.3.6.1.2.1.2.2.1.11    | <p>O número de pacotes, entregues por essa sub-camada a uma (sub)camada superior, que não foram endereçados a um endereço multicast ou de broadcast nessa sub-camada. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime.</p>   | Cisco-IOS-XR-pfi-im-c<br>oper:interfaces/interfac<br>xr/interface/interface-<br>statistics/full-interface-<br>stats/packets-receive |
| ifHCInUcastPkts  | 1.3.6.1.2.1.31.1.1.1.7  | <p>O número de pacotes, entregues por essa sub-camada a uma (sub)camada</p>   | Cisco-IOS-XR-pfi-im-c<br>oper:interfaces/interfac<br>xr/interface/interface-  |

|                    |                        |  |  |
|--------------------|------------------------|--|--|
|                    |                        | <p>superior, que não foram endereçados a um endereço multicast ou de broadcast nessa sub-camada. Este objeto é uma versão de 64 bits de ifInUcastPkts. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime. Para interfaces orientadas a pacotes, o número de pacotes de saída que não puderam ser transmitidos devido a erros. Para interfaces orientadas a caracteres ou de comprimento fixo, o número de unidades de transmissão de saída que não puderam ser transmitidas devido a erros. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime.</p> | <p>statistics/full-interface-stats/packets-receive</p>   |
| ifOutErrors        | 1.3.6.1.2.1.2.2.1.20   | <p>Para interfaces orientadas a pacotes, o número de pacotes de saída que não puderam ser transmitidos devido a erros. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime. O número de pacotes de saída que foram escolhidos para serem descartados mesmo que nenhum erro tenha sido detectado para impedir a transmissão. Uma possível causa do descarte desse pacote poderia ser para a liberação de espaço em buffer. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime.</p>   | <p>Cisco-IOS-XR-pfi-im-coper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/output-errors</p>     |
| ifOutDiscards      | 1.3.6.1.2.1.2.2.1.19   | <p>O número total de pacotes que os protocolos de nível superior solicitaram ser transmitidos e que foram endereçados a um endereço multicast nesta subcamada, incluindo os que foram descartados ou não</p>   | <p>Cisco-IOS-XR-pfi-im-coper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/output-drops</p>      |
| ifOutMulticastPkts | 1.3.6.1.2.1.31.1.1.1.4 |  | <p>Cisco-IOS-XR-pfi-im-coper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/multicast-packets</p> |

|                      |                         |   |  |
|----------------------|-------------------------|---|--|
| ifHCOutMulticastPkts | 1.3.6.1.2.1.31.1.1.1.12 | <p>enviados. Para um protocolo de camada MAC, isso inclui endereços de grupo e funcionais. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime. O número total de pacotes que os protocolos de nível superior solicitaram ser transmitidos e que foram endereçados a um endereço multicast nesta subcamada, incluindo os que foram descartados ou não enviados. Para um protocolo de camada MAC, isso inclui endereços de grupo e funcionais. Este objeto é uma versão de 64 bits de ifOutMulticastPkts. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime. O número de pacotes, entregues por essa subcamada a uma (sub)camada superior, que foram endereçados a um endereço multicast nesta sub-camada.</p> | Cisco-IOS-XR-pfi-im-c<br>oper:interfaces/interfac<br>xr/interface/interface-<br>statistics/full-interface-<br>stats/multicast-packets            |
| ifInMulticastPkts    | 1.3.6.1.2.1.31.1.1.1.2  | <p>Para um protocolo de camada MAC, isso inclui endereços de grupo e funcionais. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime. O número de pacotes, entregues por essa subcamada a uma (sub)camada superior, que foram endereçados a um endereço multicast nesta sub-camada.</p>  | Cisco-IOS-XR-pfi-im-c<br>oper:interfaces/interfac<br>xr/interface/interface-<br>statistics/full-interface-<br>stats/multicast-packets<br>receive |
| ifHCInMulticastPkts  | 1.3.6.1.2.1.31.1.1.1.8  | <p>O número de pacotes, entregues por essa subcamada a uma (sub)camada superior, que foram endereçados a um endereço multicast nesta sub-camada.</p>  | Cisco-IOS-XR-pfi-im-c<br>oper:interfaces/interfac<br>xr/interface/interface-<br>statistics/full-interface-<br>stats/multicast-packets<br>receive |

|              |                      |  |  |
|--------------|----------------------|--|--|
| ifInErrors   | 1.3.6.1.2.1.2.2.1.14 | <p>Para um protocolo de camada MAC, isso inclui endereços de grupo e funcionais. Este objeto é uma versão de 64 bits de ifInMulticastPkts. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime. Para interfaces orientadas a pacotes, o número de pacotes de entrada que continha erros que os impediam de serem entregues a um protocolo de camada superior. Para interfaces orientadas a caracteres ou de comprimento fixo, o número de unidades de transmissão de entrada que continha erros que os impediam de serem entregues a um protocolo de camada superior. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime.</p> | Cisco-IOS-XR-pfi-im-c<br>oper:interfaces/interfac<br>xr/interface/interface-<br>statistics/full-interface-<br>stats/input-errors |
| ifInDiscards | 1.3.6.1.2.1.2.2.1.13 | <p>O número de pacotes de entrada que foram escolhidos para serem descartados mesmo que nenhum erro tenha sido detectado para impedir que eles sejam entregues a um protocolo de camada superior. Uma possível causa do descarte desse pacote poderia ser para a liberação de espaço em buffer. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime.</p>  | Cisco-IOS-XR-pfi-im-c<br>oper:interfaces/interfac<br>xr/interface/interface-<br>statistics/full-interface-<br>stats/input-drops  |
| ifOutOctets  | 1.3.6.1.2.1.2.2.1.16 | <p>O número total de octetos transmitidos para fora da</p>   | Cisco-IOS-XR-pfi-im-c<br>oper:interfaces/interfac  |

|                    |                         |  |  |
|--------------------|-------------------------|--|--|
|                    |                         | interface, incluindo caracteres de enquadramento. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime. O número total de octetos transmitidos para fora da interface, incluindo caracteres de enquadramento. Este objeto é uma versão de 64 bits de ifOutOctets. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime. O número total de octetos recebidos na interface, incluindo caracteres de enquadramento. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime. O número total de octetos recebidos na interface, incluindo caracteres de enquadramento. Este objeto é uma versão de 64 bits do ifInOctets. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime. O número total de pacotes que os protocolos de nível superior solicitaram ser transmitidos e que foram endereçados a um endereço de broadcast nesta sub-camada, incluindo os que foram descartados ou não | xr/interface/interface-statistics/full-interface-stats/bytes-sent  |
| ifHCOctets         | 1.3.6.1.2.1.31.1.1.1.10 |  | Cisco-IOS-XR-pfi-im-coper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/bytes-sent             |
| ifInOctets         | 1.3.6.1.2.1.2.2.1.10    |  | Cisco-IOS-XR-pfi-im-coper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/bytes-recebidos        |
| ifHCInOctets       | 1.3.6.1.2.1.31.1.1.1.6  |  | Cisco-IOS-XR-pfi-im-coper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/bytes-recebidos        |
| ifOutBroadcastPkts | 1.3.6.1.2.1.31.1.1.1.5  |  | Cisco-IOS-XR-pfi-im-coper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/broadcast-packets-sent |



|                      |                         |   |  |
|----------------------|-------------------------|---|--|
| ifHCOutPktsBroadcast | 1.3.6.1.2.1.31.1.1.1.13 | <p>enviados. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime. O número total de pacotes que os protocolos de nível superior solicitaram ser transmitidos e que foram endereçados a um endereço de broadcast nesta sub-camada, incluindo os que foram descartados ou não enviados. Este objeto é uma versão de 64 bits de ifOutBroadcastPkts. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime.</p> | Cisco-IOS-XR-pfi-im-coper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/broadcast-packetsent     |
| ifInBroadcastPkts    | 1.3.6.1.2.1.31.1.1.1.3  | <p>O número de pacotes, entregues por essa sub-camada a uma (sub)camada superior, que foram endereçados a um endereço de broadcast nesta sub-camada. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo valor de ifCounterDiscontinuityTime.</p>  | Cisco-IOS-XR-pfi-im-coper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/broadcast-packetsreceive |
| ifHCInBroadcastPkts  | 1.3.6.1.2.1.31.1.1.1.9  | <p>O número de pacotes, entregues por essa sub-camada a uma (sub)camada superior, que foram endereçados a um endereço de broadcast nesta sub-camada. Este objeto é uma versão de 64 bits de ifInBroadcastPkts. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e, outras vezes, como indicado pelo</p>   | Cisco-IOS-XR-pfi-im-coper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/broadcast-packetsreceive |

|              |                     |  |  |
|--------------|---------------------|--|--|
| ifIndex      | 1.3.6.1.2.1.2.2.1.1 | <p>valor de ifCounterDiscontinuityTime. Um valor exclusivo, maior que zero, para cada interface. Recomenda-se que os valores sejam atribuídos continuamente a partir de 1. O valor para cada subcamada de interface deve permanecer constante pelo menos de uma reinicialização do sistema de gerenciamento de rede da entidade para a próxima reinicialização.</p>  | Cisco-IOS-XR-pfi-im-c<br>oper:interfaces/interfac<br>xr/interface/if-index                       |
| ifDescr      | 1.3.6.1.2.1.2.2.1.2 | <p>Uma string textual contendo informações sobre a interface. Essa string deve incluir o nome do fabricante, o nome do produto e a versão do hardware/software da interface.</p>   | Cisco-IOS-XR-pfi-im-c<br>oper:interfaces/interfac<br>xr/interface/description                    |
| ifSpeed      | 1.3.6.1.2.1.2.2.1.5 | <p>Uma estimativa da largura de banda atual da interface em bits por segundo. Para interfaces que não variam na largura de banda ou para aquelas em que não é possível fazer uma estimativa precisa, este objeto deve conter a largura de banda nominal. Se a largura de banda da interface for maior do que o valor máximo reportável por este objeto, este objeto deve relatar seu valor máximo (4.294.967.295) e ifHighSpeed deve ser usado para relatar a velocidade da interface. Para uma subcamada que não tem conceito de largura de banda, esse objeto deve ser zero.</p> | Cisco-IOS-XR-pfi-im-c<br>oper:interfaces/interfac<br>xr/interface/bandwidth                      |
| ifOperStatus | 1.3.6.1.2.1.2.2.1.8 | <p>O estado operacional atual da interface. O estado de teste(3) indica que nenhum pacote operacional pode ser passado. Se ifAdminStatus estiver inoperante(2) então ifOperStatus deve estar inoperante(2). Se ifAdminStatus for alterado para up(1) então ifOperStatus deve ser alterado para up(1) se a</p>  | Cisco-IOS-XR-pfi-im-c<br>oper:interfaces/interfac<br>non-dynamic/interface<br>dynamic/oper-state |

|               |                        |   |   |
|---------------|------------------------|---|---|
| ifAdminStatus | 1.3.6.1.2.1.2.2.1.7    | <p>interface estiver pronta para transmitir e receber tráfego de rede; deve ser alterada para inativa(5) se a interface estiver aguardando ações externas (como uma linha serial aguardando uma conexão de entrada); deve permanecer no estado inativo(2) se e somente se houver uma falha que impeça que ele vá para o estado ativo(1); deve permanecer no estado notPresent(6) se a interface tiver componentes ausentes (geralmente, hardware). O estado desejado da interface. O estado de teste(3) indica que nenhum pacote operacional pode ser passado. Quando um sistema gerenciado é inicializado, todas as interfaces começam com ifAdminStatus no estado inativo(2). Como resultado de uma ação de gerenciamento explícita ou de informações de configuração mantidas pelo sistema gerenciado, ifAdminStatus é alterado para os estados up(1) ou test(3) (ou permanece no estado down(2)).</p> | Cisco-IOS-XR-pfi-im-c<br>oper:interfaces/interfac<br>non-dynamic/interface<br>dynamic/admin-state |
| ifName        | 1.3.6.1.2.1.31.1.1.1.1 | <p>O nome textual da interface. O valor desse objeto deve ser o nome da interface como atribuído pelo dispositivo local e deve ser adequado para uso em comandos inseridos no `console' do dispositivo. Pode ser um nome de texto, como `le0' ou um número de porta simples, como `1', dependendo da sintaxe de nome da interface do dispositivo. Se várias entradas na tabela ifTable representarem uma única interface nomeada pelo dispositivo, cada uma terá o mesmo valor de ifName. Observe que para um agente que responde a consultas</p>   | Cisco-IOS-XR-pfi-im-c<br>oper:interfaces/interfac<br>brief/interface-<br>brief/interface-name     |

SNMP relativas a uma interface em algum outro dispositivo (proxied), o valor de ifName para tal interface é o nome local do dispositivo proxy. Se não houver um nome local, ou se este objeto não for aplicável, então este objeto contém uma string de comprimento zero.

Uma estimativa da largura de banda atual da interface em unidades de 1.000.000 bits por segundo. Se esse objeto relata um valor de `n' então a velocidade da interface está em algum lugar na faixa de `n-500 mil' a `n+499.999'. Para interfaces que não variam na largura de banda ou para aquelas em que não é possível fazer uma estimativa precisa, este objeto deve conter a largura de banda nominal. Para uma subcamada que não tem conceito de largura de banda, esse objeto deve ser zero.

Cisco-IOS-XR-pfi-im-c  
oper:interfaces/interfac  
brief/interface-  
brief/bandwidth64 bits

ifAlta velocidade 1.3.6.1.2.1.31.1.1.1.15

## IP-MIB

A tabela a seguir representa o nome e o número do OID e o XPATH correspondente a serem configurados em grupos de sensores de telemetria orientados por modelo relacionados às estatísticas e aos valores operacionais do Internet Protocol (IP).

| Nome do OID        | Número OID      | Descrição do OID  | XPATH  |
|--------------------|-----------------|---|--|
| icmplnDestUnreachs | 1.3.6.1.2.1.5.3 | O número de mensagens ICMP Destination Unreachable recebidas. | Cisco-IOS-XR-ipv4-io-<br>oper:ipv4-<br>network/nodes/node/st<br>s/traffic/icmp-stats |
| icmplnParmProbs    | 1.3.6.1.2.1.5.5 | O número de mensagens ICMP Parameter Problem recebidas.       | Cisco-IOS-XR-ipv4-io-<br>oper:ipv4-<br>network/nodes/node/st<br>s/traffic/icmp-stats |
| icmplnSrcQuenchs   | 1.3.6.1.2.1.5.6 | O número de mensagens ICMP Source Quench recebidas.           | Cisco-IOS-XR-ipv4-io-<br>oper:ipv4-<br>network/nodes/node/st<br>s/traffic/icmp-stats |
| icmplnEchos        | 1.3.6.1.2.1.5.8 | O número de mensagens ICMP Echo (request) recebidas.          | Cisco-IOS-XR-ipv4-io-<br>oper:ipv4-<br>network/nodes/node/st<br>s/traffic/icmp-stats |
| icmplnEchoReps     | 1.3.6.1.2.1.5.9 | O número de mensagens   | Cisco-IOS-XR-ipv4-io-  |

|                     |                  |  |  |
|---------------------|------------------|--|--|
|                     |                  | ICMP Echo Reply recebidas.   | oper:ipv4-network/nodes/node/stats/traffic/icmp-stats<br>Cisco-IOS-XR-ipv4-io- |
| icmpInTimestamps    | 1.3.6.1.2.1.5.10 | O número de mensagens ICMP Timestamp (request) recebidas.  | oper:ipv4-network/nodes/node/stats/traffic/icmp-stats<br>Cisco-IOS-XR-ipv4-io- |
| icmpInAddrMask      | 1.3.6.1.2.1.5.12 | O número de mensagens ICMP Address Mask Request recebidas.   | oper:ipv4-network/nodes/node/stats/traffic/icmp-stats<br>Cisco-IOS-XR-ipv4-io- |
| icmpInAddrMaskReps  | 1.3.6.1.2.1.5.13 | O número de mensagens ICMP Address Mask Reply (Resposta de máscara de endereço ICMP) recebidas.  | oper:ipv4-network/nodes/node/stats/traffic/icmp-stats<br>Cisco-IOS-XR-ipv4-io- |
| icmpOutMsgs         | 1.3.6.1.2.1.5.14 | O número total de mensagens ICMP que esta entidade tentou enviar. Observe que esse contador inclui todos aqueles contados por icmpOutErrors. | oper:ipv4-network/nodes/node/stats/traffic/icmp-stats<br>Cisco-IOS-XR-ipv4-io- |
| icmpOutDestUnreachs | 1.3.6.1.2.1.5.16 | O número de mensagens ICMP Destination Unreachable enviadas.   | oper:ipv4-network/nodes/node/stats/traffic/icmp-stats<br>Cisco-IOS-XR-ipv4-io- |
| icmpOutTimeExcds    | 1.3.6.1.2.1.5.17 | O número de mensagens ICMP Tempo Excedido enviadas.  | oper:ipv4-network/nodes/node/stats/traffic/icmp-stats<br>Cisco-IOS-XR-ipv4-io- |
| icmpOutParmProbs    | 1.3.6.1.2.1.5.18 | O número de mensagens ICMP Parameter Problem enviadas.   | oper:ipv4-network/nodes/node/stats/traffic/icmp-stats<br>Cisco-IOS-XR-ipv4-io- |
| icmpOutSrcQuenchs   | 1.3.6.1.2.1.5.19 | O número de mensagens ICMP Source Quench enviadas.   | oper:ipv4-network/nodes/node/stats/traffic/icmp-stats<br>Cisco-IOS-XR-ipv4-io- |
| icmpOutRedirects    | 1.3.6.1.2.1.5.20 | O número de mensagens ICMP Redirect enviadas. Para um host, esse objeto sempre será zero, pois os hosts não enviam redirecionamentos.        | oper:ipv4-network/nodes/node/stats/traffic/icmp-stats<br>Cisco-IOS-XR-ipv4-io- |
| icmpOutEchos        | 1.3.6.1.2.1.5.21 | O número de mensagens ICMP Echo (request) enviadas.  | oper:ipv4-network/nodes/node/stats/traffic/icmp-stats<br>Cisco-IOS-XR-ipv4-io- |
| icmpOutEchoReps     | 1.3.6.1.2.1.5.22 | O número de mensagens ICMP Echo Reply enviadas.  | oper:ipv4-network/nodes/node/stats/traffic/icmp-stats<br>Cisco-IOS-XR-ipv4-io- |
| icmpOutTimestamps   | 1.3.6.1.2.1.5.23 | O número de mensagens ICMP Timestamp (request) enviadas.   | oper:ipv4-network/nodes/node/stats/traffic/icmp-stats<br>Cisco-IOS-XR-ipv4-io- |

|                         |                      |  |  |
|-------------------------|----------------------|--|--|
| icmpOutAddrMask         | 1.3.6.1.2.1.5.25     | O número de mensagens ICMP Address Mask Request (Solicitação de máscara de endereço) enviadas.   | Cisco-IOS-XR-ipv4-io-<br>oper:ipv4-<br>network/nodes/node/st<br>s/traffic/icmp-stats                   |
| icmpOutAddrMaskReps     | 1.3.6.1.2.1.5.26     | O número de mensagens ICMP Address Mask Reply (Resposta de máscara de endereço ICMP) enviadas.   | Cisco-IOS-XR-ipv4-io-<br>oper:ipv4-<br>network/nodes/node/st<br>s/traffic/icmp-stats                   |
| ipAdEntIfIndex          | 1.3.6.1.2.1.4.20.1.2 | O valor de índice que identifica exclusivamente a interface à qual essa entrada é aplicável. A interface identificada por um valor específico desse índice é a mesma interface identificada pelo mesmo valor do ifIndex da RFC 1573.   | Cisco-IOS-XR-ipv4-io-<br>oper:ipv4-<br>network/nodes/node/   |
| ipAdEntAddr             | 1.3.6.1.2.1.4.20.1.1 | O endereço IP ao qual as informações de endereçamento desta entrada pertencem.   | Cisco-IOS-XR-ipv4-io-<br>oper:ipv4-<br>network/interfaces/inte<br>vrfs/vrf/detail/primary-<br>address  |
| ipAdEntNetMask          | 1.3.6.1.2.1.4.20.1.3 | A máscara de sub-rede associada ao endereço IP dessa entrada. O valor da máscara é um endereço IP com todos os bits de rede definidos como 1 e todos os bits de host definidos como 0. O valor do bit menos significativo no endereço de broadcast IP usado para enviar datagramas na interface (lógica) associada ao endereço IP dessa entrada. Por exemplo, quando o endereço de broadcast padrão da Internet all-ones é usado, o valor será 1. Esse valor se aplica aos endereços de broadcast da sub-rede e da rede usados pela entidade nessa interface (lógica). | Cisco-IOS-XR-ipv4-io-<br>oper:ipv4-<br>network/interfaces/inte<br>vrfs/vrf/detail/prefix-len           |
| ipAdEntBcastAddr        | 1.3.6.1.2.1.4.20.1.4 | O endereço de broadcast padrão da Internet all-ones é usado, o valor será 1. Esse valor se aplica aos endereços de broadcast da sub-rede e da rede usados pela entidade nessa interface (lógica).  | Cisco-IOS-XR-ipv4-io-<br>oper:ipv4-<br>network/interfaces/inte<br>vrfs/vrf/detail/direct-<br>broadcast |
| ipNetToMediaPhysAddress | 1.3.6.1.2.1.4.22.1.2 | O endereço 'físico' dependente da mídia.   | Cisco-IOS-XR-ipv4-arp<br>oper:arp/node/entries/e<br>hardware-address                                   |

## IPMIB-COMMMON

A tabela a seguir representa o nome e o número do OID e o XPATH correspondente a serem configurados em grupos de sensores de telemetria orientados por modelo relacionados às estatísticas IP.

| Nome do OID | Número OID | Descrição do OID | XPATH |
|-------------|------------|------------------|-------|
|-------------|------------|------------------|-------|

|                         |                         |   |   |
|-------------------------|-------------------------|---|---|
| ipLfStatsHCOutTransmits | 1.3.6.1.2.1.4.31.3.1.31 | O número total de datagramas IP que esta entidade forneceu às camadas inferiores para transmissão. Este objeto conta os mesmos datagramas de ipLfStatsOutTransmits, mas permite valores maiores. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e em outras ocasiões, conforme indicado pelo valor de ipLfStatsDiscontinuityTime. | Cisco-IOS-XR-ipv4-io-<br>oper:ipv4-<br>network/nodes/node/s<br>cs/traffic/ipv4-stats/pa<br>forwarding |
| ipLfStatsInReceives     | 1.3.6.1.2.1.4.31.3.1.3  | O número total de datagramas IP de entrada recebidos, incluindo os recebidos por erro. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e em outras ocasiões, conforme indicado pelo valor de ipLfStatsDiscontinuityTime.   | Cisco-IOS-XR-ipv4-io-<br>oper:ipv4-<br>network/nodes/node/s<br>cs/traffic/ipv4-stats/inp<br>packets   |
| ipLfStatsHCInReceives   | 1.3.6.1.2.1.4.31.3.1.4  | O número total de datagramas IP de entrada recebidos, incluindo os recebidos por erro. Este objeto conta os mesmos datagramas de ipLfStatsInReceives, mas permite valores maiores. As descontinuidades no valor desse contador podem ocorrer na reinicialização do sistema de gerenciamento e em outras ocasiões, conforme indicado pelo valor de ipLfStatsDiscontinuityTime.               | Cisco-IOS-XR-ipv4-io-<br>oper:ipv4-<br>network/nodes/node/s<br>cs/traffic/ipv4-stats/inp<br>packets   |

## LLDP-MIB

A próxima tabela representa o nome e o número do OID e o XPATH correspondente a serem configurados em grupos de sensores de telemetria orientados por modelo relacionados aos dados operacionais do Protocolo de Identificação de Camada de Enlace (LLDP - Link Layer Discovery Protocol) no nó monitorado.

| Nome do OID          | Número OID               | Descrição do OID   | XPATH   |
|----------------------|--------------------------|--|---|
| IldpLockPortId       | 1.0.8802.1.1.2.1.3.7.1.3 | O valor de string usado para identificar o componente de porta associado a uma determinada porta no sistema local. | Cisco-IOS-XR-ethernet-<br>lldp-<br>oper:lldp/nodes/node/<br>bors/devices/lldp-<br>neighbor/port-id-detail |
| IldplocPortIdSubtype | 1.0.8802.1.1.2.1.3.7.1.2 | O tipo de codificação do   | Cisco-IOS-XR-ethernet-  |

|                              |                          |   |   |
|------------------------------|--------------------------|---|---|
|                              |                          | identificador de porta usado no objeto 'IldpLocationPortId' associado.  | Ildp-<br>oper:Ildp/node/neighbor/<br>evices/device/Ildp-<br>neighbor/mib/port-id-s<br>type<br>Cisco-IOS-XR-etherne    |
| IldpLockChassisIdSubtip<br>o | 1.0.8802.1.1.2.1.3.1     | O tipo de codificação usado para identificar o chassi associado ao sistema local.   | Ildp-<br>oper:Ildp/node/neighbor/<br>evices/device/Ildp-<br>neighbor/mib/chassis-<br>sub-type<br>Cisco-IOS-XR-etherne |
| IldplocSysName               | 1.0.8802.1.1.2.1.3.3     | O valor de string usado para identificar o nome do sistema do sistema local. Se o agente local suportar IETF RFC 3418, o objeto IldpLockSysName deve ter o mesmo valor do objeto sysName. | Cisco-IOS-XR-etherne<br>Ildp-<br>oper:Ildp/nodes/node/<br>bors/devices/Ildp-<br>neighbor/detail/system<br>name        |
| IldpRemSysName               | 1.0.8802.1.1.2.1.4.1.1.9 | O valor de string usado para identificar o nome do sistema do sistema remoto.   | Cisco-IOS-XR-etherne<br>Ildp-<br>oper:Ildp/nodes/node/<br>bors/devices/Ildp-<br>neighbor/detail/system<br>name        |
| IldpRemChassisId             | 1.0.8802.1.1.2.1.4.1.1.5 | O valor de string usado para identificar o componente do chassi associado ao sistema remoto.  | Cisco-IOS-XR-etherne<br>Ildp-<br>oper:Ildp/nodes/node/<br>bors/devices/Ildp-<br>neighbor/chassis-id                   |
| IldpRemChassisIdSubtip<br>o  | 1.0.8802.1.1.2.1.4.1.1.4 | O tipo de codificação usado para identificar o chassi associado ao sistema remoto.  | Cisco-IOS-XR-etherne<br>Ildp-<br>oper:Ildp/node/neighbor/<br>evices/device/Ildp-neig                                  |
| IldpRemPortIdSubtype         | 1.0.8802.1.1.2.1.4.1.1.6 | O tipo de codificação do identificador de porta usado no objeto 'IldpRemPortId' associado.  | Cisco-IOS-XR-etherne<br>Ildp-<br>oper:Ildp/node/neighbor/<br>evices/device/Ildp-neig                                  |
| IldpRemPortId                | 1.0.8802.1.1.2.1.4.1.1.7 | O valor de string usado para identificar o componente de porta associado ao sistema remoto.   | Cisco-IOS-XR-etherne<br>Ildp-<br>oper:Ildp/node/neighbor/<br>evices/device/Ildp-neig                                  |
| IldpLockIdDoChassi           | 1.0.8802.1.1.2.1.3.2     | O valor de string usado para identificar o componente do chassi associado ao sistema local.   | Cisco-IOS-XR-ethern<br>Ildp-<br>oper:Ildp/nodes/node/<br>bors/details/Ildp-<br>neighbor/chassis-id                    |

## MPLS-TE-STD-MIB

A próxima tabela representa o nome e o número do OID e o XPATH correspondente a serem configurados em grupos de sensores de telemetria orientados por modelo relacionados aos valores operacionais de Engenharia de Tráfego de Multiprotocol Label Switching (MPLS) no dispositivo gerenciado.



| Nome do OID             | Número OID                   | Descrição do OID  | XPATH  |
|-------------------------|------------------------------|---|--|
| mplsTunnelName          | 1.3.6.1.2.1.10.166.3.2.2.1.5 | O nome canônico atribuído ao túnel. Esse nome pode ser usado para se referir ao túnel na porta de console do LSR. Se mplsTunnelsIf estiver definido como true, o ifName da interface correspondente a este túnel deve ter um valor igual a mplsTunnelName. Veja também a descrição de ifName no RFC 2863.         | Cisco-IOS-XR-mpls-te-oper:mpls-te/p2p-p2r-tunnel/tunnel-heads/tunnel-head/tunnel-name                        |
| mplsTunnelDescr         | 1.3.6.1.2.1.10.166.3.2.2.1.6 | Uma string textual contendo informações sobre o túnel. Se não houver descrição, este objeto contém uma string de comprimento zero. Este objeto não pode ser sinalizado por protocolos de sinalização MPLS, portanto, o valor deste objeto em LSRs de trânsito e saída PODE ser gerado automaticamente ou ausente. | openconfig-network-instance/network-instance/network-instance/mpls/lsp/conned-path/tunnel/state/description  |
| mplsTunnelPerfHCpackets | 1.3.6.1.2.1.10.166.3.2.9.1.2 | Contador de alta capacidade para o número de pacotes encaminhados pelo túnel.   | openconfig-network-instance/network-instance/network-instance/mpls/lsp/conned-path/tunnel/state/countpackets |
| mplsTunnelPerfHCBytes   | 1.3.6.1.2.1.10.166.3.2.9.1.5 | Contador de alta capacidade para o número de bytes encaminhados pelo túnel.   | openconfig-network-instance/network-instance/network-instance/mpls/lsp/conned-path/tunnel/state/countbytes   |
| mplsTunnelHopIpAddr     | 1.3.6.1.2.1.10.166.3.2.4.1.5 | O endereço de salto de túnel para este salto de túnel. O tipo desse endereço é determinado pelo valor do mplsTunnelHopAddrType correspondente. O valor deste objeto não pode ser alterado se o valor do objeto mplsTunnelHopRowStatus correspondente for 'ative'.   | Cisco-IOS-XR-mpls-te-oper:mpls-te/p2p-p2r-tunnel/tunnel-heads/tunnel-head/destination/description-address    |

## RFC2465-MIB

A próxima tabela representa o nome e o número do OID e o XPATH correspondente a serem

configurados em grupos de sensores de telemetria orientados por modelo relacionados aos valores globais do IPv6.

| Nome do OID         | Número OID             | Descrição do OID  | XPATH  |
|---------------------|------------------------|---|--|
| ipv6AddrPfxLength   | 1.3.6.1.2.1.55.1.8.1.2 | O comprimento do prefixo (em bits) associado ao endereço IPv6 dessa entrada.                                      | Cisco-IOS-XR-ipv6-management/oper:ipv6-network/nodes/node/interface-<br>-data/vrfs/vrf/brief/address-length  |
| ipv6AddrAnycastFlag | 1.3.6.1.2.1.55.1.8.1.4 | Este objeto tem o valor 'true(1)', se este endereço for um endereço anycast e o valor 'false(2)', caso contrário. | Cisco-IOS-XR-ipv6-management/oper:ipv6-network/nodes/node/interface-<br>-data/vrfs/vrf/brief/address-anycast |

## SNMP-MIB

A próxima tabela representa o nome e o número do OID e o XPATH correspondente a serem configurados em grupos de sensores de telemetria orientados por modelo relacionados ao próprio agente SNMP, se disponível.

| Nome do OID | Número OID        | Descrição do OID                                      | XPATH   |
|-------------|-------------------|---|---|
| sysUpTime   | 1.3.6.1.2.1.1.3   | String que representa o tempo de atividade do sistema | Cisco-IOS-XR-snmp-agent/oper:snmp/information/system-up-time/ |
| sysObjectID | 1.3.6.1.2.1.1.2.0 | String representando o OID do sistema                 | Cisco-IOS-XR-snmp-agent/oper:snmp/information/system-oid/     |
| sysDescr    | 1.3.6.1.2.1.1.1   | String que representa a descrição do sistema          | Cisco-IOS-XR-snmp-agent/oper:snmp/information/system-down     |

## TCP-MIB

A próxima tabela representa o nome e o número do OID e o XPATH correspondente a serem configurados em grupos de sensores de telemetria orientados por modelo relacionados a contadores específicos do TCP.

| Nome do OID | Número OID       | Descrição do OID   | XPATH  |
|-------------|------------------|--|--|
| tcpInErrs   | 1.3.6.1.2.1.6.14 | O número total de segmentos recebidos por erro (por exemplo, somas de verificação TCP incorretas).   | Cisco-IOS-XR-ip-tcp-<br>oper:tcp/nodes/node/stack/<br>/ipv4-traffic/tcp-checksum-error-packets |
| tcpInSegs   | 1.3.6.1.2.1.6.10 | O número total de segmentos recebidos, incluindo os recebidos por erro. Essa contagem inclui segmentos recebidos em conexões estabelecidas atualmente. | Cisco-IOS-XR-ip-tcp-<br>oper:tcp/nodes/node/stack/<br>/ipv4-traffic/tcp-input-packets          |
| tcpOutSegs  | 1.3.6.1.2.1.6.11 | O número total de segmentos enviados, incluindo os das   | Cisco-IOS-XR-ip-tcp-<br>oper:tcp/nodes/node/stack/   |

conexões atuais, mas excluindo os que contêm apenas octetos retransmitidos.

/ipv4-traffic/tcp-output-pa

## UDP-MIB

A tabela a seguir representa o nome e o número do OID e o XPATH correspondente a serem configurados em grupos de sensores de telemetria orientados por modelo relacionados a contadores específicos do UDP.

| Nome do OID        | Número OID      | Descrição do OID  | XPATH  |
|--------------------|-----------------|---|--|
| udpOutDatagramas   | 1.3.6.1.2.1.7.4 | O número total de datagramas UDP enviados desta entidade.   | Cisco-IOS-XR-ip-udp-oper:/udp/nodes/node/sts/ipv4-traffic/udp-output-packets<br>Cisco-IOS-XR-ip-udp-oper:/udp/nodes/node/sts/ipv6-traffic/udp-output-packets             |
| udpNoPorts         | 1.3.6.1.2.1.7.2 | O número total de datagramas UDP recebidos para os quais não havia aplicação na porta de destino.   | Cisco-IOS-XR-ip-udp-oper:/udp/nodes/node/sts/ipv4-traffic/udp-no-port-packets<br>Cisco-IOS-XR-ip-udp-oper:/udp/nodes/node/sts/ipv6-traffic/udp-no-port-packets           |
| Erros deEntradaudp | 1.3.6.1.2.1.7.3 | O número de datagramas UDP recebidos que não puderam ser entregues por outros motivos além da falta de um aplicativo na porta de destino. | Cisco-IOS-XR-ip-udp-oper:/udp/nodes/node/sts/ipv4-traffic/udp-checks-error-packets<br>Cisco-IOS-XR-ip-udp-oper:/udp/nodes/node/sts/ipv6-traffic/udp-checks-error-packets |
| udpInDatagramas    | 1.3.6.1.2.1.7.1 | O número total de datagramas UDP entregues a usuários UDP.  | Cisco-IOS-XR-ip-udp-oper:/udp/nodes/node/sts/ipv4-traffic/udp-input-packets<br>Cisco-IOS-XR-ip-udp-oper:/udp/nodes/node/sts/ipv6-traffic/udp-input-packets               |

## Migração de interceptações SNMP

Traps SNMP são mensagens disparadas por eventos dinâmicos no dispositivo gerenciado. Portanto, essas mensagens se comportam de forma análoga ao conceito de EDT que abordamos antes.

No lado da configuração, o MDT permite a mesma estrutura para EDT, que depende da implementação no coletor de telemetria em termos de opções ou recursos de discagem de

entrada ou discagem de saída.

## **Considerações sobre segurança**

O SNMPv2 usa apenas a comunidade como um mecanismo de autenticação/autorização. No entanto, SNMPv3 como abordado anteriormente na seção SNMP, pode usar credenciais para autenticação e modelo de criptografia AES para proteger as informações.

Na abordagem de telemetria, o IOS XR permite o uso de técnicas gRPC/TLS com base em certificados para executar a autenticação. Esses certificados podem ser usados com um ponto central de confiança (um servidor CA, por exemplo). Após o processo de criação de uma relação de confiança, todas as mensagens de telemetria são enviadas dentro de uma sessão gRPC que é criptografada com TLS realizando os mesmos benefícios do SNMPv3.