Migración SNMP a Telemetría en IOS XR

Contenido

Introducción

En este artículo se presentan los componentes del protocolo simple de administración de red (SNMP) y se proporciona una correlación entre las implementaciones actuales basadas en la supervisión SNMP en el enfoque de telemetría basada en modelos (MDT).

SNMP (Protocolo de administración de red simple)

El SNMP es un protocolo de la capa de aplicación que proporciona un formato de mensaje para la comunicación entre los administradores y agentes de SNMP. SNMP proporciona un marco de trabajo estandarizado y un lenguaje común que se utiliza para monitorear y administrar los dispositivos de una red

Componentes de SNMP

El marco SNMP tiene los siguientes componentes, que se describen en las secciones siguientes:

- Administrador SNMP
- Agente SNMP
- SNMP MIB

Administrador SNMP

El administrador SNMP es un sistema que controla y monitorea las actividades de los hosts de red mediante SNMP. El sistema de administración más común es un sistema de administración de redes (NMS). El término NMS se puede aplicar a un dispositivo dedicado usado para la administración de red o a las aplicaciones usadas en tal dispositivo.

Agente SNMP

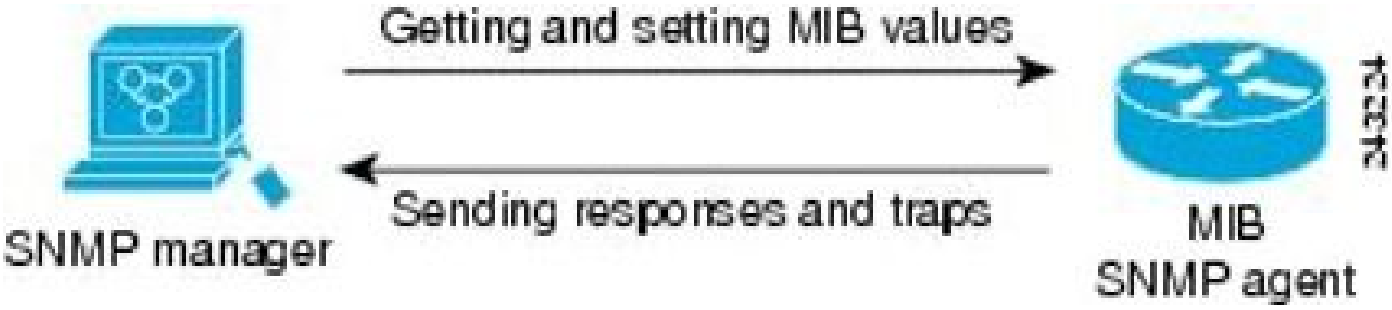
El agente SNMP es el componente de software de un dispositivo administrado que mantiene los datos del dispositivo y genera informes de esos datos, según las necesidades, para los sistemas administradores. El agente reside en el dispositivo de ruteo (router, servidor de acceso o switch).

SNMP MIB

Un agente SNMP contiene variables MIB, cuyos valores pueden ser solicitados o cambiados por el administrador SNMP a través de las operaciones 'Get' o 'Set'. Un administrador puede obtener un valor de un agente o almacenar un valor en ese agente. El agente recopila datos de SNMP MIB, el repositorio para obtener información sobre los parámetros del dispositivo y los datos de

red. El agente también puede responder a las solicitudes del administrador para obtener o establecer datos.

La siguiente figura ilustra las comunicaciones entre el administrador SNMP y el agente. Un administrador envía solicitudes a un agente para obtener y establecer los valores MIB de SNMP. El agente responde a estas solicitudes. Independientemente de esta interacción, el agente puede enviar al administrador notificaciones no solicitadas (trampas o informaciones) para notificarle el estado de la red.



Operaciones del SNMP

Las aplicaciones SNMP realizan las siguientes operaciones para recuperar datos, modificar variables de objeto SNMP y enviar notificaciones:

- Get de SNMP
- SET DE SNMP
- Notificaciones SNMP

Get de SNMP

La operación get de SNMP se lleva a cabo en un NMS para recuperar variables de objeto de SNMP. Hay tres tipos de operaciones get:

- get: recupera la instancia exacta del objeto del agente SNMP.
- getNext: recupera la siguiente variable de objeto, que es sucesora lexicográfica de la variable especificada.
- getBulk: Recupera una gran cantidad de datos variables del objeto, sin necesidad de operaciones getNext repetidas.

SET DE SNMP

La operación SNMP SET la realiza un NMS para modificar el valor de una variable de objeto.

Notificaciones SNMP

Una función clave de SNMP es su capacidad para generar notificaciones no solicitadas desde un agente SNMP.

Las notificaciones (asíncronas) no solicitadas se pueden generar como trampas o solicitudes de

informes (informes). Las trampas son mensajes que alertan al administrador del Protocolo simple de administración de red (SNMP) de una condición en la red. Los informes son trampas que incluyen una solicitud de confirmación de la recepción por parte del administrador SNMP. Las notificaciones pueden indicar una autenticación de usuario incorrecta, reinicios, el cierre de una conexión, la pérdida de conexión con un dispositivo vecino u otros eventos significativos.

Las trampas son menos fiables que los informes porque el receptor no envía un acuse de recibo cuando recibe una trampa. El remitente no sabe si se recibió la trampa. Un administrador SNMP que recibe un informe reconoce el mensaje con una PDU (unidad de datos de protocolo de respuesta) SNMP. Si el remitente nunca recibe una respuesta, la información se puede enviar otra vez. De esta manera, las notificaciones de información tienen más posibilidades de llegar al destino deseado.

A menudo, se prefieren las trampas aunque sean menos fiables porque los informes consumen más recursos en el dispositivo y la red. A diferencia de una trampa, la cual se descarta tan pronto como se envía, un informe se debe mantener en la memoria hasta que se reciba una respuesta o se agote el tiempo de espera de la solicitud. Además, las trampas se envía una sola vez, mientras que un informe puede reenviarse varias veces. Los reintentos incrementan el tráfico y contribuyen a una sobrecarga mayor en la red. El uso de trampas e informes requiere un equilibrio entre la fiabilidad y los recursos.

MIBs y RFCs

Los módulos de Base de información de administración (MIB) se definen normalmente en los documentos de solicitud de comentarios (RFC) enviados al Grupo de trabajo de ingeniería de Internet (IETF), un organismo de estándares internacionales. Los RFC son escritos por individuos o grupos para su análisis por parte de la Internet Society y de la comunidad de Internet en general, normalmente con la intención de establecer un estándar de Internet recomendado. Antes de que se les asigne el estatus de RFC, las recomendaciones se publican como documentos Internet Draft (I-D). Las RFC que se han convertido en estándares recomendados también se etiquetan como documentos de estándares (STD). Puede obtener más información sobre el proceso de estándares y las actividades del IETF en el sitio web de Internet Society en http:// www.isoc.org. Puede leer el texto completo de todos los RFC, I-Ds y STD a los que se hace referencia en la documentación de Cisco en el sitio web de IETF en http:// www.ietf.org.

La implementación de Cisco de SNMP utiliza las definiciones de las variables MIB II descritas en RFC 1213 y las definiciones de trampas SNMP descritas en RFC 1215.

Cisco proporciona sus propias extensiones MIB privadas con cada sistema. Los MIBs de Cisco Enterprise cumplen con las pautas descritas en los RFCs pertinentes a menos que se indique de otra forma en la documentación. Puede encontrar los archivos de definición del módulo MIB y la lista de MIBs soportados en cada plataforma de Cisco en el sitio web de MIB de Cisco en Cisco.com.

Versiones de SNMP

Actualmente, los dispositivos de Cisco admiten las siguientes versiones de SNMP:

- SNMPv1: protocolo simple de administración de red: estándar de Internet completo, definido en RFC 1157. (RFC 1157 sustituye a las versiones anteriores publicadas como RFC 1067 y RFC 1098.) La seguridad se basa en cadenas de comunidad.
- SNMPv2c — El marco de trabajo administrativo basado en cadena de comunidad para SNMPv2. SNMPv2c (la "c" significa "comunidad") es un protocolo de Internet experimental definido en RFC 1901, RFC 1905 y RFC 1906. SNMPv2c es una actualización de las operaciones de protocolo y de los tipos de datos de SNMPv2p (SNMPv2 Classic) y utiliza el modelo de seguridad basado en la comunidad de SNMPv1.
- SNMPv3 - Versión 3 de SNMP. SNMPv3 es un protocolo basado en estándares interoperable definido en los RFCs 3413 a 3415. SNMPv3 proporciona acceso seguro a los dispositivos mediante paquetes de autenticación y encripción a través de la red.

Las funciones de seguridad proporcionadas en SNMPv3 son las siguientes:

- Integridad del mensaje: garantía de que un paquete no se ha manipulado durante el tránsito.
- Autenticación: determinar que el mensaje procede de un origen válido.
- Cifrado: codificación del contenido de un paquete para evitar que lo detecte una fuente no autorizada.

Tanto SNMPv1 como SNMPv2c utilizan una forma de seguridad basada en la comunidad. La comunidad de administradores SNMP que pueden acceder a la MIB del agente está definida por una cadena de comunidad.

El soporte de SNMPv2c incluye un mecanismo de recuperación masiva y un informe de mensajes de error detallado para las estaciones de administración. El mecanismo de recuperación masiva soporta la recuperación de tablas y grandes cantidades de información, minimizando el número de viajes de ida y vuelta requeridos. La compatibilidad con el control de errores mejorado de SNMPv2c incluye códigos de error expandidos que distinguen diferentes tipos de errores; estas condiciones se notifican a través de un único código de error en SNMPv1. También se informa de los siguientes tres tipos de excepciones: no existe tal objeto, no existe tal instancia y fin de la vista MIB.

SNMPv3 es un modelo de seguridad en el cual se configura una estrategia de autenticación para un usuario y para el grupo en el que reside el usuario. Un nivel de seguridad es el nivel de seguridad permitido dentro de un modelo de seguridad. Una combinación de un modelo de seguridad y un nivel de seguridad determina qué mecanismo de seguridad se emplea al gestionar un paquete SNMP.

Hay tres modelos de seguridad disponibles: SNMPv1, SNMPv2c y SNMPv3. En la tabla siguiente se enumeran las combinaciones de niveles y modelos de seguridad y sus significados.

Modelo	‘Nivel’	Autenticación	Cifrado	Qué Sucede
v1	noAuthNoPriv	Cadena de comunidad	No	Usa una correspondencia de identificaciones de comunidad para autenticación.

v2c	noAuthNoPriv	Cadena de comunidad	No	Usa una correspondencia de identificaciones de comunidad para autenticación.
v3	noAuthNoPriv	Nombre de usuario	No	Utiliza las coincidencias de nombre de usuario para autenticar.
v3	authNoPriv	Algoritmo de resumen de mensajes 5 (MD5) o Algoritmo de hash seguro (SHA)	No	Proporciona autenticación sobre la base de algoritmos HMAC-MD5 o HMAC-SHA.
v3	authPriv	MD5 o SHA	Estándar de Encripción de Datos (DES)	Proporciona autenticación sobre la base de algoritmos HMAC-MD5 o HMAC-SHA. Proporciona cifrado DES de 56 bits además de autenticación basada en el estándar CBC-DES (DES-56).

Se debe implementar un agente SNMP para utilizar la versión de SNMP admitida por la estación de administración. Un agente puede comunicarse con varios jefes.

SNMPv3 soporta los RFCs 1901 a 1908, 2104, 2206, 2213, 2214 y 2271 a 2275. Para obtener más información sobre SNMPv3, vea el RFC 2570, Introducción a la Versión 3 de Internet-standard Network Management Framework (no se trata de un documento de estándares).

Modelos Yang

Los modelos Yang representan una abstracción estructurada en árbol de una característica específica o características de hardware de un sistema. En los elementos de red, un modelo Yang podría representar un protocolo de routing, matrices de sensores físicos internos. El lenguaje y la terminología YANG se describen en RFC 6020 y se actualizan a continuación en RFC 7950. En el nivel superior, un modelo Yang organiza los datos que representan la estructura principal en submódulos y contenedores que son una lista de subnodos relacionados. A continuación se explican varios tipos de nodos.

Un nodo de hoja contiene datos simples como un entero o una cadena. Tiene exactamente un valor de un tipo determinado y no tiene nodos secundarios.

```
leaf host-name {

            type string;

            description "Hostname for this system";
```

```
       }
```

Una lista de hojas es una secuencia de nodos de hojas con exactamente un valor de un tipo determinado por hoja.

```
leaf-list domain-search {

         type string;

         description "List of domain names to search";

      }
```

Un nodo contenedor se utiliza para agrupar nodos relacionados en un subárbol. Un contenedor sólo tiene nodos secundarios y ningún valor. Un contenedor puede contener cualquier número de nodos secundarios de cualquier tipo (incluidas hojas, listas, contenedores y listas de hojas).

```
container system {

         container login {

             leaf message {

                 type string;

                 description

                     "Message given at start of login session";

             }

         }

     }
```

Una lista define una secuencia de entradas de la lista. Cada entrada es como una estructura o una instancia de registro y se identifica de forma única por los valores de sus hojas clave. Una lista puede definir múltiples hojas clave y puede contener cualquier número de nodos secundarios de cualquier tipo (incluyendo hojas, listas, contenedores, etc.).

Por último, un modelo de ejemplo que enlaza todos estos tipos de notas se parece al ejemplo siguiente:

```
## 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;
        }
      }
    }
  }
}
```

Sin embargo, el lenguaje Yang utilizado en los modelos Yang no indica la organización de los datos en contenedores/lista/hojas. Esta es la razón por la que una cierta característica en un elemento de red podría representarse con diversos modelos Yang. Este desafío se ha abordado con los siguientes tipos de modelos Yang:

- Modelos OpenConfig
- Modelos nativos

Modelos OpenConfig

Los modelos OpenConfig se desarrollaron utilizando una organización de proveedor independiente para el modelo que representa una función específica. La ventaja de este enfoque es que un NMS podría utilizar estos modelos para interactuar con los elementos de red en un entorno de varios proveedores o incluso de varias plataformas.

Como su nombre indica, estos modelos están abiertos y disponibles públicamente para inspeccionar repositorios como github en este enlace:

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

Como ejemplo, puede encontrar un modelo openconfig para el Protocolo de gateway fronterizo (BGP), otro para el Protocolo de control de agregación de enlaces (LACP) y otro diferente para ISIS, con un modelo específico diferente. En el caso de BGP, puede encontrar un modelo para los errores BGP, otro para la política BGP y así sucesivamente. Los modelos podrían estar relacionados, y algunos modelos pueden llamar a otro paquete Yang. Por ejemplo, openconfig-bgp-neighbor.yang pertenece 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;
```

En resumen, los modelos OpenConfig están orientados a protocolos comunes a todas las plataformas, como las funciones estandarizadas de IETF o RFC.

Modelos nativos

Por el contrario, los modelos nativos son modelos orientados al proveedor que cubren en profundidad estructuras específicas de una plataforma determinada. Por ejemplo, modelos que agrupan sensores de valores físicos dentro de un elemento de red como voltajes, temperaturas, contadores ASIC, contadores de fabric, etc. Dado que dependen de la plataforma, es habitual encontrar modelos específicos para NCS6K, ASR9K o Cisco 8000.

Como modelos OpenConfig, los modelos nativos también están disponibles en el repositorio de Github:

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

Dado que estos modelos suelen ser mucho más específicos y completos que los modelos de OpenConfig, están vinculados a una versión de software específica y sujetos a cambios entre versiones de software.

Existen dos categorías principales para los modelos nativos:

- Modelos "Oper", utilizados para recuperar información de un elemento.

Por ejemplo, Cisco-IOS-XR-eigrp-oper.yang

- Modelos "Cfg", utilizados para configurar un elemento de red

Por ejemplo, Cisco-IOS-XR-eigrp-cfg.yang

En términos generales, Model Driven Telemetry utiliza modelos "oper" para transmitir datos desde la infraestructura y NMS como NSO utiliza modelos "cfg" para realizar cambios en la configuración de los elementos de red.

Los modelos Yang nativos y OpenConfig están presentes en el software XR en la carpeta /pkg/yang y se pueden enumerar para averiguar si algún modelo Yang está disponible en una plataforma. Este ejemplo es para el XRrv9k que ejecuta cXR 6.4.2:

```
RP/0/RP0/CPU0:xrv9k1#run ls  /pkg/yang | grep isis
Tue Sep 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
```

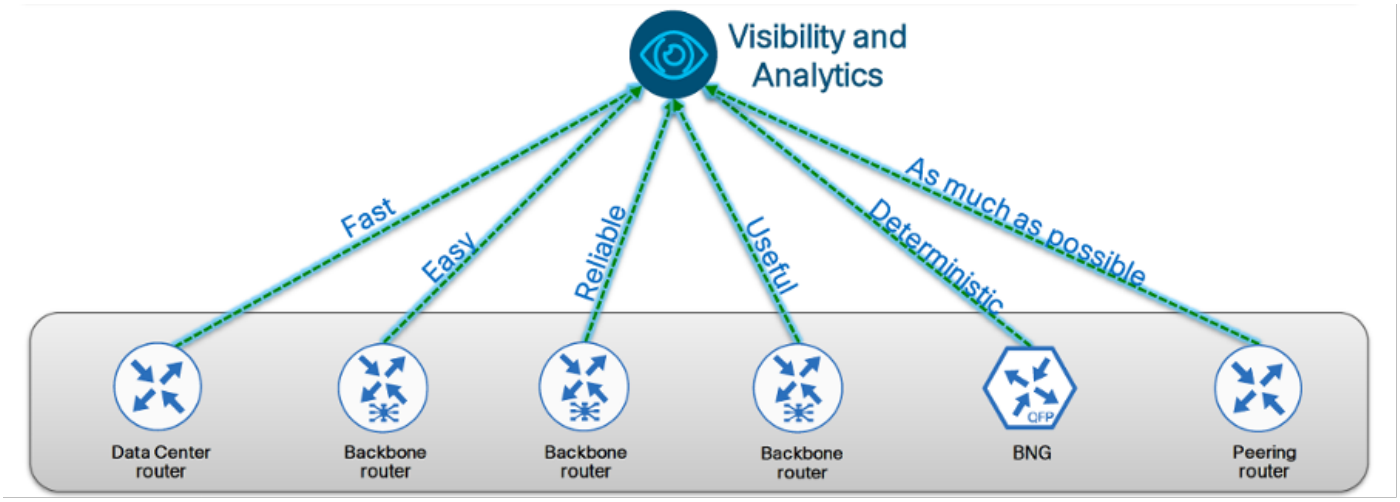
```
openconfig-isis-lsdb-types.yang
openconfig-isis-lsp.yang
openconfig-isis-policy.yang
openconfig-isis-routing.yang
openconfig-isis-types.yang
openconfig-isis.yang


RP/0/RP0/CPU0:xrv9k1#
```

Telemetría

La telemetría es un proceso que permite recopilar información de diferentes elementos remotos en una ubicación central que agrega visibilidad y capa de análisis.

En los entornos de red, los datos se pueden generar a partir de cada elemento de la red, routers, switches entre otros y la información puede estar relacionada con un conjunto muy amplio de protocolos específicos, contadores de rendimiento o medidas de sensores físicos.



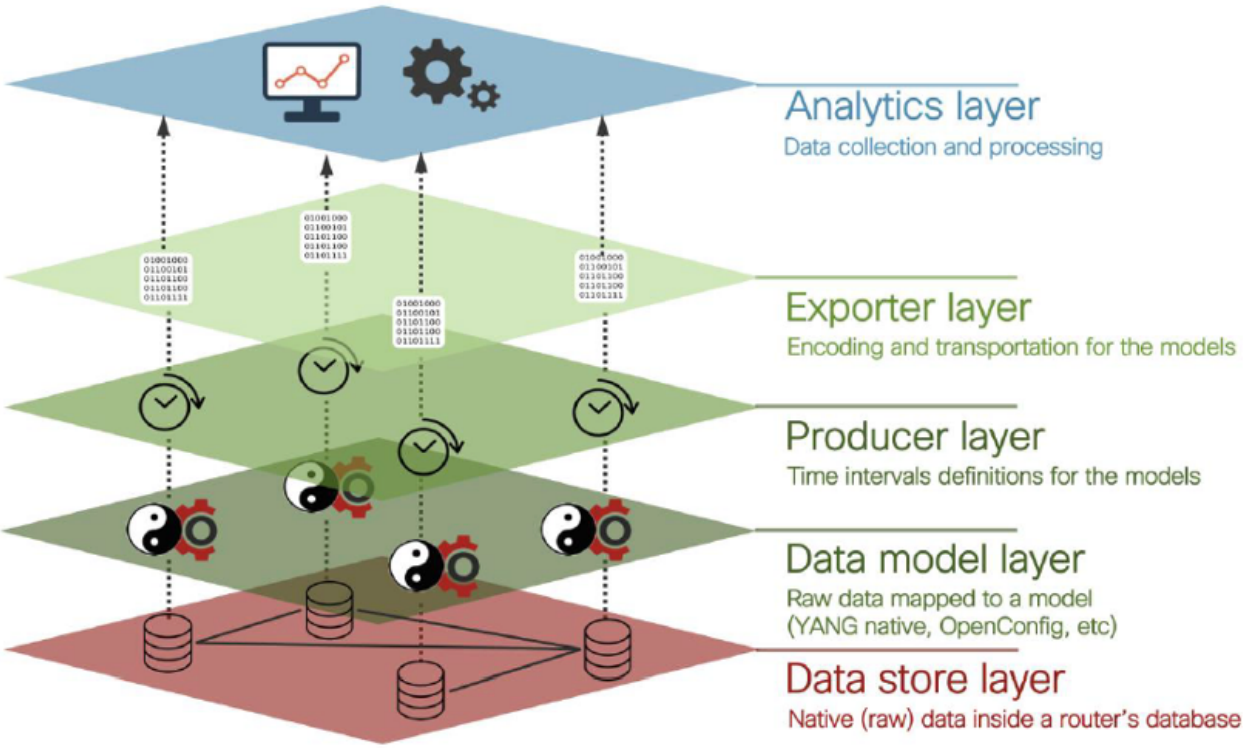
En general, las funciones de visibilidad y análisis se encuentran en puntos centrales de las redes, la transmisión de la información de telemetría se realiza mediante mecanismos de transporte de red, por lo que la información de telemetría debe ser lo más rápida posible para poder ampliarse.

A diferencia de los mecanismos SNMP heredados, la telemetría utiliza un paradigma de inserción, donde la red debe aprovisionarse para transmitir sus propios datos sin sondear a intervalos regulares, que es la característica principal de la supervisión basada en SNMP. Esta provisión se denomina a menudo suscripción, y se basa en un conjunto de variables que se deben monitorear, el intervalo regular para el intervalo de muestreo para la recolección de datos y el sistema remoto para enviar estos datos a través de la red.

Telemetría basada en modelos

Los estados MDT para la telemetría basada en modelos, y como su nombre lo indica, se basa en modelos Yang. Todos los aspectos de los equipos de red podrían representarse con los modelos Yang, por ejemplo la tabla OSPF Neighbors, RIB o sensores de temperatura para cada componente de los sistemas modulares.

En cuanto a la arquitectura MDT, se puede dividir en las siguientes capas:



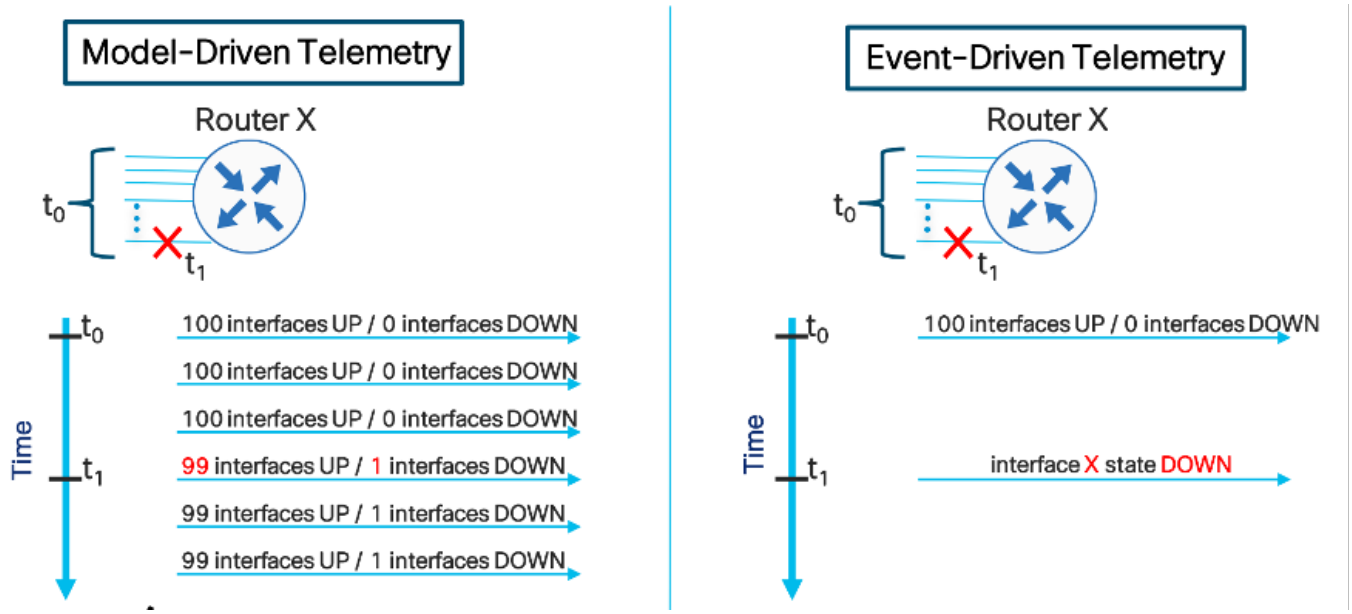
> Nota: Con respecto a la capa del productor, en la telemetría basada en modelos hay una definición de intervalo de muestreo que controla la frecuencia con la que el dispositivo consulta la base de datos interna para obtener datos sin procesar y organiza estos datos en la capa del modelo de datos.

La suscripción de telemetría también define qué modelos y con contenedores/ruta producirían datos para transmitirlos a la capa de análisis. Esta definición repercutiría en la información pertinente para fines empresariales. La definición MDT de esta trayectoria de sensor sería analógica para definir OID para recuperar a través de SNMP, ya que ambas técnicas producen datos estructurados a una velocidad de muestreo definida.

Telemetría basada en eventos

EDT significa telemetría dirigida por eventos y también se basa en modelos Yang para la estructura. La diferencia principal es que el desencadenador de la recopilación y el flujo de datos no es un intervalo regular, sino un evento específico, como una cruz de umbral, eventos de vínculo, errores de hardware, etc.

A continuación se presenta una comparación de un evento con la telemetría basada en modelos y la telemetría basada en eventos:



Sugerencia: en esta figura se muestran mensajes redundantes que utilizan MDT, pero sólo mensajes que representan cambios mediante EDT.

Transporte

La telemetría debe ser lo más fiable posible, por lo que tiene sentido utilizar transporte basado en el protocolo de control de transmisión (TCP) para utilizar sockets orientados a sesión entre la infraestructura y la capa de análisis, que debe implementar recopiladores para realizar la sesión.

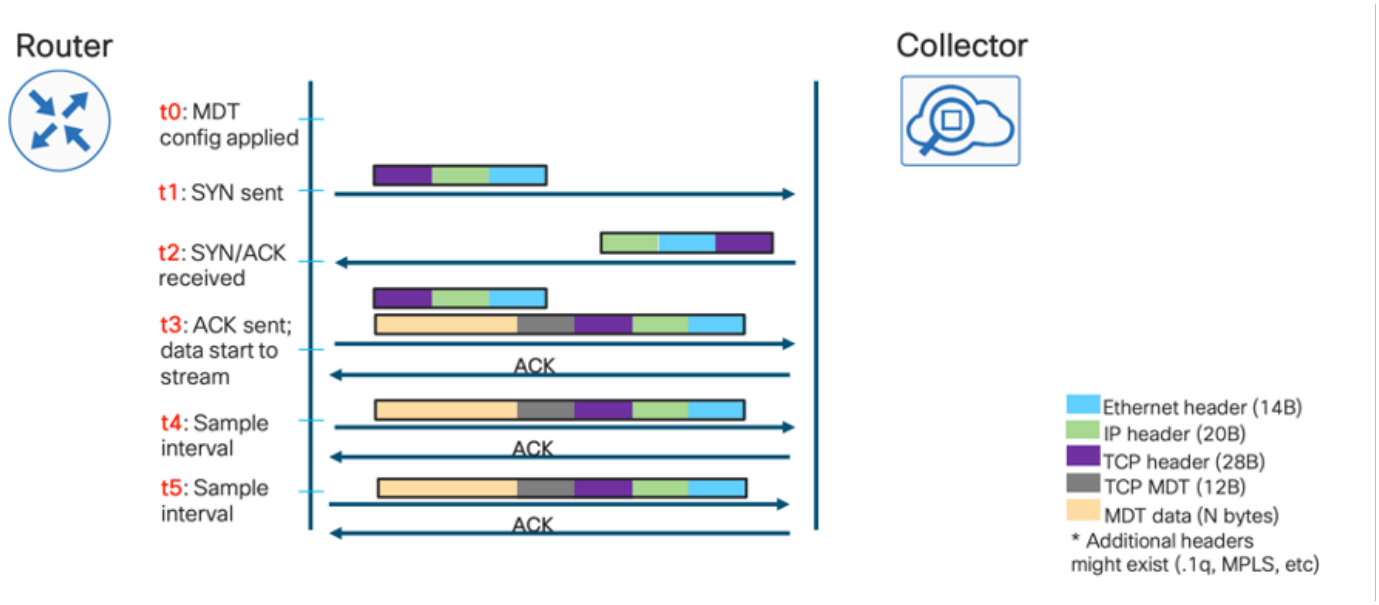
Existen dos enfoques principales al utilizar la telemetría, y difieren entre sí en el flujo inicial de entrada en contacto de 3 vías.

Nota: En el modo de marcado de salida, la configuración de la sesión se inicia en el lado de la infraestructura, lo que implica que los sensores de interés deben configurarse en los elementos de la red. En resumen, el enfoque de marcado de entrada permite una configuración más ligera de los elementos de red, ya que el recopilador debe solicitar rutas de

sensor específicas en la fase de configuración.

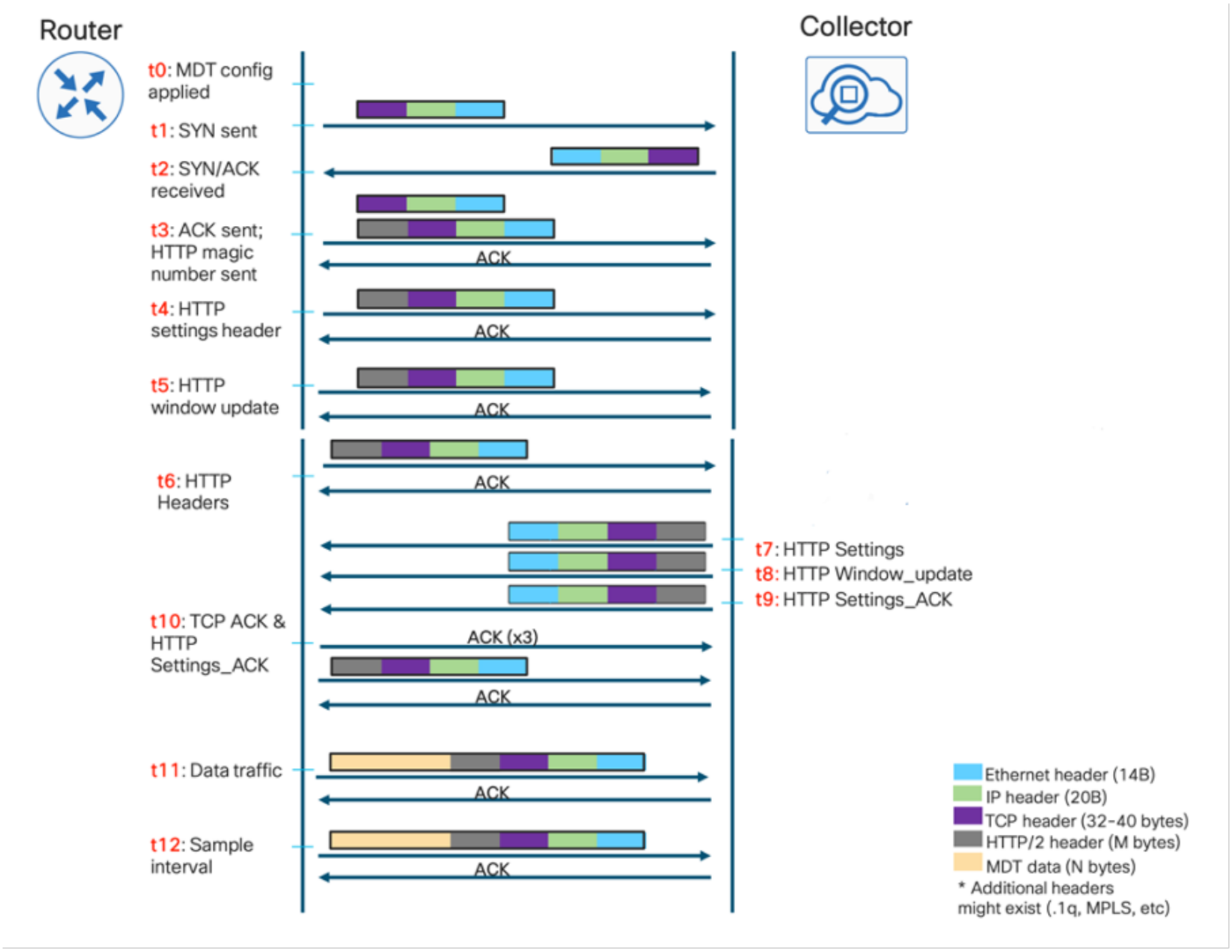
TCP

TCP es la forma más sencilla de realizar una sesión orientada a la conexión entre un elemento de red y un recopilador de telemetría, y el flujo de datos comienza del router al recopilador que envió ACK de vuelta al router con fines de fiabilidad:



gRPC

Dado que Google Protocol RPC (gRPC) funciona sobre Hypertext Transfer Protocol/2 (HTTP/2), la sesión en sí debería formarse en la configuración, y permite el control de velocidad desde el lado del colector de forma nativa:



gNMI/gNOI

gNMI es un protocolo de administración de redes desarrollado por Google. gNMI proporciona el mecanismo para instalar, manipular y eliminar la configuración de los dispositivos de red, así como para ver los datos operativos. El contenido proporcionado a través de gNMI se puede modelar utilizando YANG.

gNMI utiliza gRPC-HTTP/2 para configurar una conexión y proporciona un canal bidireccional entre los elementos de red y un NMS que también podría ser un colector de telemetría, pero también proporciona una interfaz para administrar los dispositivos.

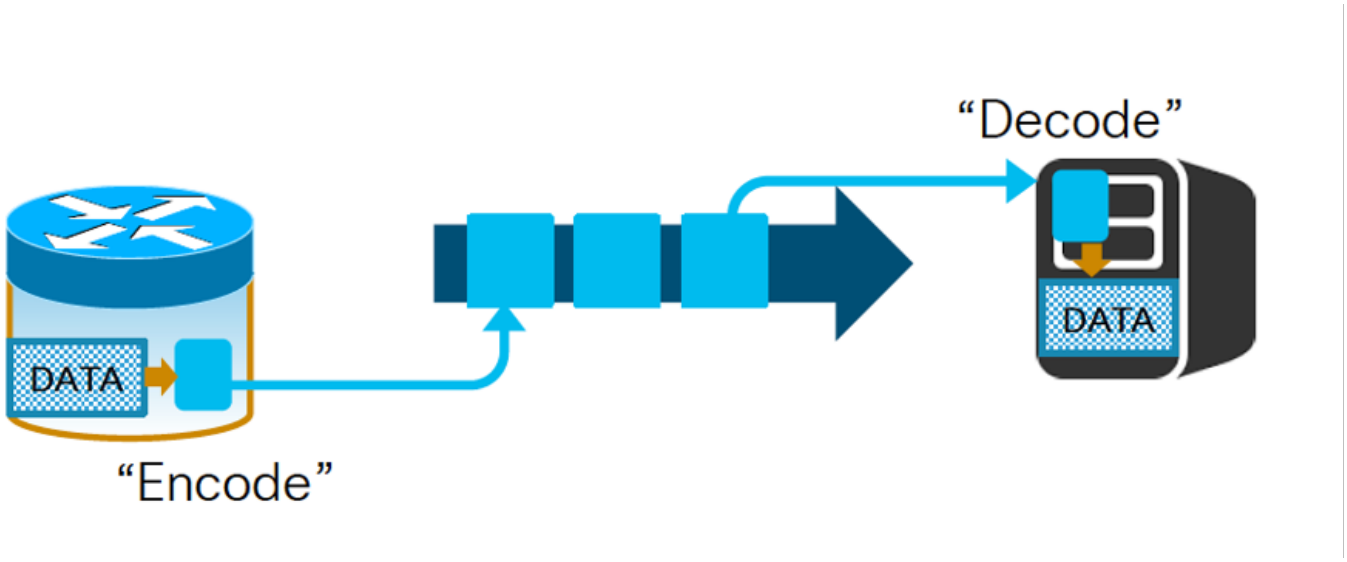
Entre las operaciones soportadas por este protocolo, podemos encontrar gNMI Get, gNMI Set que devuelven la información solicitada, mensajes de éxito o error.

gRPC Network Operations Interface (gNOI) es una colección de microservicios que utiliza el mismo canal de comunicación que gNMI pero permite operaciones genéricas no relacionadas con la configuración en sí como ping, reboot, cambio de certificados SSL, borrado, etc.

Codificación

Los modelos Yang definen la estructura de los datos, su jerarquía y el tipo de cada nodo de hoja

que contiene. Sin embargo, el modelado no indica cómo se deben serializar estos datos. Este proceso rige la conversión de datos estructurados en una secuencia de bytes que se enviará a través de la conexión TCP (TCP sin formato, gRPC, gNMI, etc.).



Nota: Este proceso debe implementarse con un mecanismo equivalente en el elemento de red que debe codificar los datos, y el recopilador debe descodificar estos datos.

JSON

El primer mecanismo de codificación es el formato nativo de JavaScript Object Notation (JSON), que es bien conocido pero está orientado a las personas, ya que todas las claves se representan como cadenas, lo que es ineficaz en términos de tamaño del mensaje. La principal ventaja de utilizar JSON es que es fácil de analizar, y se puede leer en base a texto como el siguiente ejemplo:

```
{
“node_id_str”:"test-IOSXR ",
"subscription_id_str":" if_rate",
"encoding_path":"Cisco-IOS-XR-infra-statsdoper:infra-statistics/interfaces/interface/latest/datarate",
"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

El formato de codificación de valor de clave de búferes de protocolo de Google (GPB-KV) también se denomina GPB autodescriptivo porque hace uso de búferes de protocolo para hacer uso de mensajes que apuntan a elementos particulares en modelos Yang. Esto implica que sólo se necesita un archivo .proto para codificar/descodificar propósitos, y las claves mismas de los datos están en cadenas 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, Google Protocol Buffers (GPB), también llamado compact GPB, lleva este enfoque un paso más allá y requiere archivos .proto para mapear cada clave de la estructura, lo que hace que sea mucho más eficiente en términos de tamaño del mensaje, ya que todo se envía como valores binarios. Sin embargo, el inconveniente es la necesidad de compilar cada archivo .proto asociado a cada modelo Yang soportado por la infraestructura/colector.

```
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\005Null0"
   content: "\220\003\000\230\003\000\240\003\000\250\0 03\000\260\003\000\270\003\000\300\003\000\ 310
   }
  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
   }
collection_end_time: 1485794640480
```

Configuración de MDT en IOS XR

Los componentes principales utilizados en la transmisión de datos de telemetría basados en modelos son:

- Sesión
- Ruta del sensor
- Suscripción
- Transporte y codificación

Las opciones de sesión pueden ser Marcado de entrada o Marcado de salida, como hemos comentado anteriormente. Para construir la configuración en IOS XR.

Modo de marcado de salida

para el modo de marcado de salida, el router inicia una sesión en los destinos según la suscripción, y el proceso debe incluir los siguientes pasos:

- Crear un grupo de destino
- Crear un grupo de sensores
- Crear una suscripción
- Validar configuración de acceso telefónico de salida

Para crear un grupo de destino, debe conocer la dirección del colector del protocolo de Internet versión 4 (IPv4) / protocolo de Internet versión 6 (IPv6) y el puerto que abastecería a esta aplicación. Además, debe especificar el protocolo y la codificación que deben acordarse en el dispositivo de red y el recopilador.

Por último, puede que necesite especificar el reenvío y routing virtual (VRF) utilizado para comunicarse con la dirección de red del recopilador.

A continuación, se presenta un ejemplo de configuración de marcado de salida:

```
telemetry model-driven
 destination-group DG1
  vrf MGMT
  address-family ipv4 192.168.122.20 port 5432
   encoding self-describing-gpb
   protocol tcp
  !
 !
```

A continuación se presentan las opciones de codificación:

<#root>

```
RP/0/RP0/CPU0:C8000-1(config-model-driven-dest-addr)#encoding ?
  gpb                   GPB encoding
  json                  JSON encoding
  self-describing-gpb  Self describing GPB encoding
← Also known as GPB-KV
```

```
RP/0/RP0/CPU0:C8000-1(config-model-driven-dest-addr)#encoding
```

Las opciones de los protocolos:

```
RP/0/RP0/CPU0:C8000-1(config-model-driven-dest-addr)#protocol ?
  grpc  gRPC
  tcp   TCP
  udp   UDP
RP/0/RP0/CPU0:C8000-1(config-model-driven-dest-addr)#protocol grpc ?
  gzip          gRPC gzip message compression
  no-tls        No TLS
  tls-hostname  TLS hostname
```

```
RP/0/RP0/CPU0:C8000-1(config-model-driven-dest-addr)#protocol tcp ?
```

```
RP/0/RP0/CPU0:C8000-1(config-model-driven-dest-addr)#protocol udp ?
  packetsize  UDP packet size
```

```
RP/0/RP0/CPU0:C8000-1(config-model-driven-dest-addr)#protocol udp
```

El protocolo TCP es sencillo y sólo necesita los parámetros de puerto asociados a la dirección IPv4/IPv6. El protocolo de datagramas de usuario (UDP), por el contrario, no tiene conexión, por lo que el estado del grupo de destino siempre sería activo.

La compresión en gRPC se puede lograr mediante el uso de la palabra clave opcional gzip. gRPC usa TLS de forma predeterminada, por lo que se debe instalar un certificado localmente en el

router para este uso. Este comportamiento puede ser invalidado por la configuración de la palabra clave no-tls. Finalmente, puede especificar un nombre de host diferente para propósitos de certificado usando la palabra clave tls-hostname.

A continuación, se debe añadir una sección de grupos de sensores en la que se enumeren las rutas de sensores de nuestro interés. Esta sección es sencilla, pero es importante saber que la trayectoria del sensor en sí permite que el filtrado optimice varios recursos como la unidad de procesamiento central (CPU) y el ancho de banda.

```
telemetry model-driven
 sensor-group SG1
  sensor-path Cisco-IOS-XR-wdsysmon-fd-oper:system-monitoring/cpu-utilization
  sensor-path Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface[interface-na
 !
!
```

> Nota: El formato necesario para una trayectoria de sensor es <model-name>:<container-path>

Este documento presenta el mapeo de monitoreo basado en SNMP usando OID representando "hojas" en este enfoque heredado en modelos YANG, representados con XPATH que coinciden con las mismas "hojas".

La etapa de configuración final debe ser la configuración de una suscripción, que vincula el grupo de sensores con una cadencia para la transmisión de telemetría a un grupo de destino.

```
telemetry model-driven
 subscription SU1
  sensor-group-id SG1 sample-interval 5000
  destination-id DG1
 !
!
```

Este ejemplo utiliza un intervalo de muestreo de 5000 milisegundos (5 segundos) que es relativo al final de la recopilación anterior. Para cambiar este comportamiento, puede cambiar la palabra clave sample-interval con la opción strict-timer.

Para la verificación, puede utilizar el siguiente comando que cubre el estado de la suscripción. Este método también permite cubrir la información del grupo de sensores y del grupo de destino.

```
RP/0/RP0/CPU0:C8000-1#sh telemetry model-driven subscription SU1

Wed Nov 18 15:38:01.397 UTC

Subscription:  SU1

-------------

  State:       ACTIVE

  Sensor groups:

  Id: SG1

    Sample Interval:      5000 ms

    Heartbeat Interval:   NA

    Sensor Path:          Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface[

    Sensor Path State:    Resolved

    Sensor Path:          Cisco-IOS-XR-wdsysmon-fd-oper:system-monitoring/cpu-utilization

    Sensor Path State:    Resolved


  Destination Groups:

  Group Id: DG1

    Destination IP:       192.168.122.10

    Destination Port:     5432

    Destination Vrf:      MGMT(0x60000001)

    Encoding:             self-describing-gpb

    Transport:            tcp

    State:                Active

    TLS :                 False

    Total bytes sent:     636284346

    Total packets sent:   4189

    Last Sent time:       2020-11-18 15:37:58.1700077650 +0000
```

```
Collection Groups:
------------------
  Id: 9
  Sample Interval:      5000 ms
  Heartbeat Interval:   NA
  Heartbeat always:     False
  Encoding:             self-describing-gpb
  Num of collection:    1407
  Collection time:      Min:     4 ms Max:    13 ms
  Total time:           Min:     8 ms Avg:    10 ms Max:    20 ms
  Total Deferred:       0
  Total Send Errors:    0
  Total Send Drops:     0
  Total Other Errors:   0
  No data Instances:    1407
  Last Collection Start:2020-11-18 15:37:57.1699545994 +0000
  Last Collection End:  2020-11-18 15:37:57.1699555589 +0000
  Sensor Path:          Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/

  Id: 10
  Sample Interval:      5000 ms
  Heartbeat Interval:   NA
  Heartbeat always:     False
  Encoding:             self-describing-gpb
  Num of collection:    1391
  Collection time:      Min:   178 ms Max:   473 ms
  Total time:           Min:   247 ms Avg:   283 ms Max:   559 ms
  Total Deferred:       0
  Total Send Errors:    0
  Total Send Drops:     0
```

```
    Total Other Errors:   0
    No data Instances:    0
    Last Collection Start:2020-11-18 15:37:58.1699805906 +0000
    Last Collection End:  2020-11-18 15:37:58.1700078415 +0000
    Sensor Path:          Cisco-IOS-XR-wdsysmon-fd-oper:system-monitoring/cpu-utilization


RP/0/RP0/CPU0:C8000-1#
```

Modo de marcado

En el modo Marcar en, el recopilador inicia la conexión a los elementos de red. Entonces, el colector debe indicar el interés para construir una suscripción.

La configuración consta de los siguientes pasos:

- Habilitar servicio gRPC
- Configurar grupos de sensores
- Verificación

Para habilitar el servicio gRPC, la configuración se muestra a continuación:

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

Las opciones son sencillas, incluido el VRF, y el puerto TCP. De forma predeterminada, gRPC utiliza TLS, pero se puede inhabilitar con la palabra clave no-tls. Por último, la opción dual address-family permite la conexión mediante IPv4 e IPv6.

A continuación, el acceso telefónico requiere la definición de grupos de sensores a nivel local, que el recopilador utilizará posteriormente para definir una suscripción.

```
telemetry model-driven
 sensor-group SG3
  sensor-path Cisco-IOS-XR-wdsysmon-fd-oper:system-monitoring/cpu-utilization
  sensor-path Cisco-IOS-XR-fib-common-oper:fib-statistics/nodes/node/drops
 !
!
```

En este punto, la configuración para el modo de Marcado de entrada está completa, y el colector mismo puede realizar una suscripción al router usando gRPC. Para la verificación, puede seguir el mismo procedimiento que en el modo de acceso telefónico:

```
RP/0/RP0/CPU0:C8000-1#sh telemetry model-driven subscription anx-1605878175837
Fri Nov 20 13:58:37.894 UTC
Subscription:  anx-1605878175837
-------------
  State:       ACTIVE
  Sensor groups:
  Id: SG3
    Sample Interval:      15000 ms
    Heartbeat Interval:   NA
    Sensor Path:          Cisco-IOS-XR-wdsysmon-fd-oper:system-monitoring/cpu-utilization
    Sensor Path State:    Resolved
    Sensor Path:          Cisco-IOS-XR-fib-common-oper:fib-statistics/nodes/node/drops
    Sensor Path State:    Resolved

  Destination Groups:
  Group Id: DialIn_1003
    Destination IP:       192.168.122.10
    Destination Port:     46974
    Compression:          gzip
    Encoding:             json
```

```
  Transport:            dialin
  State:                Active
  TLS :                 False
  Total bytes sent:     71000035
  Total packets sent:   509
  Last Sent time:       2020-11-20 13:58:32.1030932699 +0000


Collection Groups:
------------------
  Id: 5
  Sample Interval:      15000 ms
  Heartbeat Interval:   NA
  Heartbeat always:     False
  Encoding:             json
  Num of collection:    170
  Collection time:      Min:   273 ms Max:   640 ms
  Total time:           Min:   276 ms Avg:   390 ms Max:   643 ms
  Total Deferred:       0
  Total Send Errors:    0
  Total Send Drops:     0
  Total Other Errors:   0
  No data Instances:    0
  Last Collection Start:2020-11-20 13:58:32.1030283276 +0000
  Last Collection End:  2020-11-20 13:58:32.1030910008 +0000
  Sensor Path:          Cisco-IOS-XR-wdsysmon-fd-oper:system-monitoring/cpu-utilization


  Id: 6
  Sample Interval:      15000 ms
  Heartbeat Interval:   NA
  Heartbeat always:     False
```

```
    Encoding:             json

    Num of collection:    169

    Collection time:      Min:    15 ms Max:    33 ms

    Total time:           Min:    17 ms Avg:    22 ms Max:    33 ms

    Total Deferred:       0

    Total Send Errors:    0

    Total Send Drops:     0

    Total Other Errors:   0

    No data Instances:    0

    Last Collection Start:2020-11-20 13:58:32.1030910330 +0000

    Last Collection End:  2020-11-20 13:58:32.1030932787 +0000

    Sensor Path:          Cisco-IOS-XR-fib-common-oper:fib-statistics/nodes/node/drops


RP/0/RP0/CPU0:C8000-1#
```

> Sugerencia: Tenga en cuenta que no se ha codificado en el router ninguna cadencia, codificación, IP de recopilador o transporte para el modo de marcado.

Migración de SNMP a MDT

Para realizar la migración del SNMP tradicional al modelo de telemetría, se deben tratar los siguientes aspectos:

- Migración de MIB a XPATH
- Migración de trampas a telemetría
- Observaciones de seguridad

Migración de MIB a XPATH

Para este propósito, podríamos categorizar MIB usando su propia jerarquía que se podría asignar (al menos en el nivel superior) a una funcionalidad particular.

BGP4-MIB

La siguiente tabla representa el nombre y número de OID y la XPATH correspondiente que se configurará en los grupos de sensores de telemetría basados en modelos relacionados con las sesiones de peering BGP.

Nombre de OID	Número de OID	Descripción de OID	XPATH
bgpPeerLastError	1.3.6.1.2.1.15.3.1.14	Último código de error y subcódigo que vio este par en esta conexión. Si no se ha producido ningún error, este campo es cero. De lo contrario, el primer byte de esta CADENA DE OCTETOS de dos bytes contiene el código de error y el segundo byte contiene el código auxiliar.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/instance active/default-vrf/neighbor-missing-eor-table/neighbor/last-notify-error-code
bgpPeerOutUpdates	1.3.6.1.2.1.15.3.1.11	El número de mensajes BGP UPDATE transmitidos en esta conexión.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/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	La cantidad de mensajes de ACTUALIZACIÓN BGP recibidos en esta conexión.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/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	La versión negociada de BGP que se ejecuta entre los dos peers. Esta entrada DEBE ser cero (0) a menos que bgpPeerState	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/instance active/default-vrf/afs/af/neighbor-af-table/neighbor/negotiated-protocol-version

		esté en el estado openconfirm o establecido. Tenga en cuenta que los valores válidos para este objeto están entre 0 y 255.	
bgpPeerState	1.3.6.1.2.1.15.3.1.2	El estado de conexión de peer BGP.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/instance active/default-vrf/afs/af/neighbor-af-table/neighbor/connection-state
bgpPeerRemoteAddr	1.3.6.1.2.1.15.3.1.7	La dirección IP remota del par BGP de esta entrada.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/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	La dirección IP local de la conexión BGP de esta entrada.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/instance active/default-vrf/afs/af/neighbor-af-table/neighbor/connection-local-address
bgpPeerFsmEstablishedTime	1.3.6.1.2.1.15.3.1.16	Este temporizador indica cuánto tiempo (en segundos) este par ha estado en el estado establecido o cuánto tiempo desde que este par estuvo por última vez en el estado establecido. Se establece en cero cuando se configura un	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/instance active/default-vrf/afs/af/neighbor-af-table/neighbor/connection-set-time

		nuevo par o cuando se inicia el router.	
bgpPeerAdminStatus	1.3.6.1.2.1.15.3.1.3	El estado deseado de la conexión BGP. Una transición de 'stop' a 'start' hará que se genere el evento de inicio manual de BGP. Una transición de 'start' a 'stop' hará que se genere el evento de detención manual de BGP. Este parámetro se puede utilizar para reiniciar las conexiones de peer BGP. Se debe tener cuidado al proporcionar acceso de escritura a este objeto sin la autenticación adecuada.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/instance active/default-vrf/afs/af/neighbor-af-table/neighbor/connection-admin-status

CISCO-BGP4-MIB

La siguiente tabla representa el nombre y número de OID y la XPATH correspondiente que se configurará en los grupos de sensores de telemetría basados en modelos relacionados con el estado de sesión BGP y el prefijo intercambiado.

Nombre de OID	Número de OID	Descripción de OID	XPATH
cbgpPeer2RemoteAs	1.3.6.1.4.1.9.9.187.1.2.5.1.11	El número del sistema	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/

		autónomo remoto recibido en el mensaje BGP OPEN.	active/default-vrf/sessions/session/remote
cbgpPeer2PrevState	1.3.6.1.4.1.9.9.187.1.2.5.1.29	El estado anterior de la conexión de peer BGP.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neig table/neighbor/previous-con state
cbgpPeer2State	1.3.6.1.4.1.9.9.187.1.2.5.1.3	El estado de conexión de peer BGP.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neig table/neighbor/connection-s
cbgpPeer2LocalAddr	1.3.6.1.4.1.9.9.187.1.2.5.1.6	La dirección IP local de la conexión BGP de esta entrada.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neig table/neighbor/connection-lo address
cbgpPeer2AdvertisedPrefixes	1.3.6.1.4.1.9.9.187.1.2.8.1.6	Este contador se incrementa cuando un prefijo de ruta, que pertenece a una familia de direcciones, se anuncia en esta conexión. Se inicializa a cero cuando la conexión se somete a un reinicio completo.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neig table/neighbor/af-data/prefix advertised
cbgpPeer2AcceptedPrefixes	1.3.6.1.4.1.9.9.187.1.2.8.1.1	Número de prefijos de ruta aceptados en esta conexión, que pertenecen	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neig table/neighbor/af-data/prefix accept

		a una familia de direcciones.	
cbgpPeerPrefixLimit	1.3.6.1.4.1.9.9.187.1.2.1.1.3	Número máximo de prefijos de ruta aceptados en esta conexión	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance/active/default-vrf/afs/af/neig table/neighbor/af-data/max-limit
cbgpPeer2PrefixThreshold	1.3.6.1.4.1.9.9.187.1.2.8.1.4	Valor de umbral de prefijo (%) para una familia de direcciones en esta conexión en la que se cruza el umbral un mensaje de advertencia que indica el recuento de prefijo o se genera la notificación SNMP correspondiente.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/config-instance/co instance/config-instance-de vrf/entity-settings/entity-configuration/af-dependent-config/max-prefix-warn-thre

CISCO-CLASS-BASED-QOS-MIB

La siguiente tabla representa el nombre y número de OID y la XPATH correspondiente que se configurará en los grupos de sensores de telemetría basados en modelos relacionados con las estadísticas de las clases/políticas de calidad de servicio (QoS).

Nombre de OID	Número de OID	Descripción de OID	XPATH
cbQosCMDropBitRate	1.3.6.1.4.1.9.9.166.1.15.1.1.18	La tasa de bits de las caídas por clase como resultado de todas las	Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/input/service-policy-names/service-policy-instance/statistics/class-stats/general-stats/total-drop-

		funciones que pueden producir caídas (por ejemplo, policía, detección aleatoria, etc.).	rate Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/output/service-policy-names/service-policy-instance/statistics/class-stats/general-stats/total-drop-rate
cbQosCMDropPkt64	1.3.6.1.4.1.9.9.166.1.15.1.1.14	El contador de 64 bits de paquetes descartados por clase como resultado de todas las funciones que pueden producir caídas (por ejemplo, policía, detección aleatoria, etc.).	Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/input/service-policy-names/service-policy-instance/statistics/class-stats/general-stats/total-drop-packets Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/output/service-policy-names/service-policy-instance/statistics/class-stats/general-stats/total-drop-packets
cbQosCMPrePolicyPkt64	1.3.6.1.4.1.9.9.166.1.15.1.1.3	El conteo de 64 bits de los paquetes entrantes antes de ejecutar cualquier política de QoS.	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 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
cbQosCMName	1.3.6.1.4.1.9.9.166.1.7.1.1.1	Nombre del mapa de clase.	Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/input/service-

			policy-names/service-policy-instance/statistics/class-stats/class-name
cbQosCMPostPolicyByte64	1.3.6.1.4.1.9.9.166.1.15.1.1.10	El recuento de 64 bits de octetos salientes después de ejecutar las políticas de QoS.	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/transmit-bytes 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/transmit-bytes
cbQosIfIndex	1.3.6.1.4.1.9.9.166.1.1.1.1.4	ifIndex para la interfaz a la que está conectado este servicio. Este campo sólo tiene sentido si la interfaz lógica tiene un ifIndex snmp. Por ejemplo, el valor de este campo no tiene sentido cuando cbQosIfType es controlPlane.	Cisco-IOS-XR-infra-policymgr-oper:policy-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	Un índice de configuración	Cisco-IOS-XR-infra-policymgr-oper:policy-

		(independiente de la instancia) arbitrario (asignado por el sistema) para cada objeto. Cada objeto con la misma configuración comparte el mismo índice de configuración.	manager/global/policy-map/policy-map-types/policy-map-type/policy-maps
cbQosCMPrePolicyByte64	1.3.6.1.4.1.9.9.166.1.15.1.1.6	El recuento de 64 bits de octetos entrantes antes de ejecutar cualquier política de QoS.	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/pre-policy-match-bytes 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/pre-policy-match-bytes

CISCO-ENHANCED-MEMPOOL-MIB

La siguiente tabla representa el nombre y número de OID y la XPATH correspondiente que se configurará en los grupos de sensores de telemetría basados en modelos relacionados con el uso de memoria.

Nombre de OID	Número de OID	Descripción de OID	XPATH
cempMemPoolUsed	1.3.6.1.4.1.9.9.221.1.1.1.1.7	Indica el número de	Cisco-IOS-XR-nto-misc-

		bytes del grupo de memoria que están utilizando actualmente las aplicaciones en la entidad física.	oper:memory-summary/nodes/node/summa
cempMemPoolHCUsed	1.3.6.1.4.1.9.9.221.1.1.1.1.18	Indica el número de bytes del grupo de memoria que están utilizando actualmente las aplicaciones en la entidad física. Este objeto es una versión de 64 bits de cempMemPoolUsed.	Cisco-IOS-XR-nto-misc-oper:memory-summary/nodes/node/detail/to used
cempMemPoolHCFree	1.3.6.1.4.1.9.9.221.1.1.1.1.20	Indica el número de bytes del grupo de memoria que no se utilizan actualmente en la entidad física. Este objeto es una versión de 64 bits de cempMemPoolFree.	Cisco-IOS-XR-nto-misc-oper:memory-summary/nodes/node/detail/fr physical-memory

CISCO-ENTITY-FRU-CONTROL-MIB

La siguiente tabla representa el nombre y número de OID y la XPATH correspondiente que se configurará en los grupos de sensores de telemetría basados en modelos relacionados con las unidades reemplazables en campo del sistema monitoreado.

Nombre de OID	Número de OID	Descripción de OID	XPATH
cefcFRUPowerOperStatus	1.3.6.1.4.1.9.9.117.1.1.2.1.2	Estado de alimentación de FRU operativa.	Cisco-IOS-XR-in oper:inventario/e info/power-opera
cefcFRUPowerAdminStatus	1.3.6.1.4.1.9.9.117.1.1.2.1.1	Estado de alimentación de FRU deseado administrativamente.	Cisco-IOS-XR-in oper:inventario/e info/power-admir

cefcModuleStatusLastChangeTime	1.3.6.1.4.1.9.9.117.1.2.1.1.4	El valor de sysUpTime en el momento en que se cambia cefcModuleOperStatus.	Cisco-IOS-XR-in oper:inventario/e info/last-operatio
cefcModuleUpTime	1.3.6.1.4.1.9.9.117.1.2.1.1.8	Este objeto proporciona el tiempo de actividad del módulo desde la última vez que se reinicializó. Este objeto no es persistente; si un módulo se reinicia, reinicia o apaga, el tiempo de actividad comienza desde cero.	Cisco-IOS-XR-in oper:inventario/e info/card-up-time
cefcModuleResetReason	1.3.6.1.4.1.9.9.117.1.2.1.1.3	Este objeto identifica el motivo del último restablecimiento realizado en el módulo.	Cisco-IOS-XR-in oper:inventario/e info/card-reset-re
cefcModuleOperStatus	1.3.6.1.4.1.9.9.117.1.2.1.1.2	Este objeto muestra el estado operativo del módulo.	Cisco-IOS-XR-in oper:inventario/e info/card-operati
cefcModuleAdminStatus	1.3.6.1.4.1.9.9.117.1.2.1.1.1	Este objeto proporciona control administrativo del módulo.	Cisco-IOS-XR-in oper:inventario/e info/card-adminis

CISCO-ENTITY-SENSOR-MIB

La siguiente tabla representa el nombre y número de OID y la XPATH correspondiente que se configurará en los grupos de sensores de telemetría basados en modelo relacionados con las entidades de sensor en el nodo.

Nombre de OID	Número de OID	Descripción de OID	XPATH
entSensorValue	1.3.6.1.4.1.9.9.91.1.1.1.1.4	Esta variable informa de la medición más reciente que ha	Cisco-IOS-XR- oper:inventario

		visto el sensor. Para mostrar o interpretar correctamente el valor de esta variable, también debe conocer entSensorType, entSensorScale y entSensorPrecision. Sin embargo, puede comparar entSensorValue con los valores de umbral dados en entSensorThresholdTable sin ningún conocimiento semántico.	sensor-info/val
entSensorThresholdEvaluation	1.3.6.1.4.1.9.9.91.1.2.1.1.5	Esta variable indica el resultado de la evaluación más reciente del umbral. Si la condición de umbral es true, entSensorThresholdEvaluation es true(1). Si la condición de umbral es false, entSensorThresholdEvaluation es false(2). Los umbrales se evalúan a la velocidad indicada por entSensorValueUpdateRate.	Cisco-IOS-XR-oper:inventario

CISCO-FLASH-MIB

La siguiente tabla representa el nombre y número de OID y la XPATH correspondiente que se configurará en los grupos de sensores de telemetría basados en modelos relacionados con el almacenamiento flash en el sistema.

Nombre de OID	Número de OID	Descripción de OID
ciscoFlashPartitionName	1.3.6.1.4.1.9.9.10.1.1.4.1.1.10	Nombre de la partición Flash que el sistema utiliza para referirse a una partición. Puede ser cualquier cadena de caracteres alfanuméricos con el formato AAAAAAAAnn, donde A representa un carácter alfa opcional y n un carácter numérico. Los caracteres

		numéricos deben formar siempre la parte final de la cadena. El sistema quitará los caracteres alfabéticos y utilizará la parte numérica para asignar un índice de partición. Las operaciones de Flash se dirigen a una partición de dispositivo basada en este nombre. El sistema tiene un concepto de partición predeterminada. Esta sería la primera partición del dispositivo. El sistema dirige una operación a la partición predeterminada siempre que no se especifica un nombre de partición. Por lo tanto, el nombre de la partición es obligatorio, excepto cuando la operación se realiza en la partición predeterminada o cuando el dispositivo sólo tiene una partición (no está particionado).
ciscoFlashPartitionSizeExtended	1.3.6.1.4.1.9.9.10.1.1.4.1.1.13	Tamaño de la partición Flash. Debe ser un múltiplo integral de ciscoFlashDeviceMinPartitionSize. Si hay una sola partición, este tamaño será igual a ciscoFlashDeviceSize. Este objeto es una versión de 64 bits de ciscoFlashPartitionSize
ciscoFlashPartitionFreeSpaceExtended	1.3.6.1.4.1.9.9.10.1.1.4.1.1.14	Espacio libre dentro de una partición Flash. Tenga en cuenta que el tamaño real de un archivo en Flash incluye una pequeña sobrecarga que representa el encabezado del sistema de archivos. Algunos sistemas de archivos también pueden tener una sobrecarga de encabezado de dispositivo o partición que se debe tener en cuenta al calcular el espacio libre. El espacio libre

		se calculará como el tamaño total de la partición menos el tamaño de todos los archivos existentes (archivos válidos/no válidos/eliminados e incluyendo el encabezado de archivo de cada archivo), menos el tamaño de cualquier encabezado de partición, menos el tamaño del encabezado del siguiente archivo que se copiará. En resumen, este objeto dará el tamaño del archivo más grande que se puede copiar. No se espera que la entidad de administración conozca o utilice sobrecargas, como la longitud de los encabezados de los archivos y las particiones, ya que dichas sobrecargas pueden variar de un sistema de archivos a otro. Los archivos eliminados en Flash no liberan espacio. Es posible que haya que borrar una partición para recuperar el espacio ocupado por los archivos. Este objeto es una versión de 64 bits de ciscoFlashPartitionFreeSpace

CISCO-PROCESS-MIB

La siguiente tabla representa el nombre y número de OID y la XPATH correspondiente que se configurará en los grupos de sensores de telemetría basados en modelos relacionados con el uso de la CPU y la asignación de recursos para los procesos.

Nombre de OID	Número de OID	Descripción de OID	XPATH
cpmCPUTotal1minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.7	El porcentaje de ocupación total de la CPU en el último período de 1 minutos. Este objeto desaprueba el objeto cpmCPUTotal1min y aumenta el intervalo de valores a (0.100).	Cisco-IOS-X oper:supervis sistema/utiliz CPU/total-cp

cpmCPUTotal5minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.8	El porcentaje de ocupación total de la CPU en el último período de 5 minutos. Este objeto deprecia el objeto cpmCPUTotal5min y aumenta el intervalo de valores a (0..100).	Cisco-IOS-X oper:supervis sistema/utiliz CPU/total-cp
cpmCPUTotal15minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.31	El porcentaje de ocupación total de la CPU en el último período de 15 minutos. Este objeto desaprueba el objeto cpmCPUTotal15min y aumenta el intervalo de valores a (0..100).	Cisco-IOS-X oper:supervis sistema/utiliz CPU/total-cp
cpmProcessName	1.3.6.1.4.1.9.9.109.1.2.1.1.2	El nombre asociado a este proceso. Si el nombre tiene más de 32 caracteres, se truncará a los primeros 31 caracteres y se añadirá un `*' como último carácter para insinuar que se trata de un nombre de proceso truncado.	Cisco-IOS-X oper:system- utilization/pro cpu/process-
cpmProcessTextSegmentSize	1.3.6.1.4.1.9.9.109.1.2.3.1.15	Indica la memoria de texto de un proceso y todos sus objetos compartidos.	Cisco-IOS-X oper:process memory/nod ids/process-i
cpmProcessDynamicMemorySize	1.3.6.1.4.1.9.9.109.1.2.3.1.18	Indica la cantidad de memoria dinámica que está utilizando el proceso.	Cisco-IOS-X oper:process memory/nod ids/process-i
cpmProcessDataSegmentSize	1.3.6.1.4.1.9.9.109.1.2.3.1.16	Indica el segmento de datos de un proceso y todos sus objetos compartidos.	Cisco-IOS-X oper:process memory/nod ids/process-i
cpmProcExtMemAllocatedRev	1.3.6.1.4.1.9.9.109.1.2.3.1.1	Suma de toda la memoria	Cisco-IOS-X

		asignada dinámicamente que este proceso ha recibido del sistema. Esto incluye la memoria que puede haber devuelto. La suma de la memoria liberada la proporciona cpmProcExtMemFreedRev. Este objeto deja de ser cpmProcExtMemAllocated.	oper:process memory/nod ids/process-i
cpmProcExtMemFreedRev	1.3.6.1.4.1.9.9.109.1.2.3.1.2	Suma de toda la memoria que este proceso ha devuelto al sistema. Este objeto deja de ser cpmProcExtMemFreed.	Cisco-IOS-X oper:process memory/nod ids/process-i

ENTITY-MIB

La siguiente tabla representa el nombre y número de OID y la XPATH correspondiente que se configurará en las entidades físicas relacionadas con los grupos de sensores de telemetría basados en modelos en el sistema.

Nombre de OID	Número de OID	Descripción de OID	XPATH
entPhysicalName	1.3.6.1.2.1.47.1.1.1.1.7	El nombre textual de la entidad física. El valor de este objeto debe ser el nombre del componente asignado por el dispositivo local y debe ser adecuado para su uso en comandos ingresados en la `consola' del dispositivo. Puede ser un nombre de texto, como `console' o un número de componente simple (por ejemplo, número de puerto o de módulo), como `1', dependiendo de la sintaxis de	Cisco-IOS-XR-snmp-entity-r physical-index

		nomenclatura del componente físico del dispositivo. Si no hay un nombre local o este objeto no es aplicable, este objeto contiene una cadena de longitud cero. Observe que el valor de entPhysicalName para dos entidades físicas será el mismo en el caso de que la interfaz de la consola no distinga entre ellas, por ejemplo, slot-1 y la tarjeta en slot-1.	
entLogicalDescr	1.3.6.1.2.1.47.1.2.1.1.2	Una descripción textual de la entidad lógica. Este objeto debe contener una cadena que identifique el nombre del fabricante de la entidad lógica y debe establecerse en un valor distinto para cada versión de la entidad lógica.	Cisco-IOS-XR-snmp-agent- oper:snmp/information/syste
entPhysicalDescr	1.3.6.1.2.1.47.1.1.1.1.2	Una descripción textual de la entidad física. Este objeto debe contener una cadena que identifique el nombre del fabricante de la entidad física y debe establecerse en un valor distinto para cada versión o modelo de la entidad física.	Cisco-IOS-XR-snmp-agent- IOS-XR-snmp-entity-mib-op mib/entity-physical-indexes/
entPhysicalContainin	1.3.6.1.2.1.47.1.1.1.1.4	El valor de entPhysicalIndex para la entidad física que 'contiene' esta entidad física. Un valor de cero indica que esta entidad física no está contenida	Cisco-IOS-XR-invmgr- oper:inventario/entidades/en basic-bag/unique-id

		en ninguna otra entidad física. Observe que el conjunto de relaciones de 'contención' define una jerarquía estricta; es decir, no se permite la recursividad. En el caso de que una entidad física esté contenida por más de una entidad física (por ejemplo, módulos de ancho doble), este objeto debe identificar la entidad contenedora con el valor más bajo de entPhysicalIndex.	
entPhysicalClass	1.3.6.1.2.1.47.1.1.1.1.5	Indicación del tipo de hardware general de la entidad física. Un agente debe establecer este objeto en el valor de enumeración estándar que indique con mayor precisión la clase general de la entidad física o la clase principal si hay más de una. Si no existe un identificador de registro estándar adecuado para esta entidad física, se devuelve el valor 'other(1)'. Si este agente desconoce el valor, se devuelve el valor 'unknown(2)'.	Cisco-IOS-XR-invmgr-oper:inventario/entidades
entPhysicalHardwareRev	1.3.6.1.2.1.47.1.1.1.1.8	La cadena de revisión de hardware específica del proveedor para la entidad física. El valor preferido es el identificador de revisión de hardware realmente impreso en el propio componente (si	Cisco-IOS-XR-invmgr-oper:inventario/entidades/en basic-bag/hardware-revisior

		está presente). Tenga en cuenta que si la información de revisión se almacena internamente en un formato no imprimible (p. ej., binario), el agente debe convertir dicha información a un formato imprimible, de una manera específica de la implementación. Si no hay ninguna cadena de revisión de hardware específica asociada al componente físico, o si el agente desconoce esta información, este objeto contendrá una cadena de longitud cero.	
entPhysicalFirmwareRev	1.3.6.1.2.1.47.1.1.1.1.9	La cadena de revisión de firmware específica del proveedor para la entidad física. Tenga en cuenta que si la información de revisión se almacena internamente en un formato no imprimible (p. ej., binario), el agente debe convertir dicha información a un formato imprimible, de una manera específica de la implementación. Si no hay programas de firmware específicos asociados al componente físico, o si el agente desconoce esta información, este objeto contendrá una cadena de longitud cero.	Cisco-IOS-XR-invmgr-oper:inventario/entidades/en basic-bag/firmware-revision
entPhysicalSoftwareRev	1.3.6.1.2.1.47.1.1.1.1.10	La cadena de revisión de	Cisco-IOS-XR-invmgr-

		software específica del proveedor para la entidad física. Tenga en cuenta que si la información de revisión se almacena internamente en un formato no imprimible (p. ej., binario), el agente debe convertir dicha información a un formato imprimible, de una manera específica de la implementación. Si no hay programas de software específicos asociados al componente físico, o si el agente desconoce esta información, este objeto contendrá una cadena de longitud cero.	oper:inventario/entidades/en basic-bag/software-revision
entPhysicalSerialNum	1.3.6.1.2.1.47.1.1.1.1.11	La cadena de número de serie específica del proveedor para la entidad física. El valor preferido es la cadena de número de serie que se imprime realmente en el propio componente (si existe). En la primera instanciación de una entidad física, el valor de entPhysicalSerialNum asociado a esa entidad se establece en el número de serie asignado por el proveedor correcto, si el agente dispone de esta información. Si un número de serie es desconocido o inexistente, entPhysicalSerialNum se	Cisco-IOS-XR-invmgr-oper:inventario/entidades/en basic-bag/serial-number

		establecerá en una cadena de longitud cero. Tenga en cuenta que las implementaciones que pueden identificar correctamente los números de serie de todas las entidades físicas instaladas no necesitan proporcionar acceso de escritura al objeto entPhysicalSerialNum. Los agentes que no pueden proporcionar almacenamiento no volátil para las cadenas entPhysicalSerialNum no necesitan implementar el acceso de escritura para este objeto. No todos los componentes físicos tendrán un número de serie, o incluso necesitarán uno. Las entidades físicas para las que el valor asociado del objeto entPhysicalIsFRU es igual a 'false(2)' (por ejemplo, los puertos del repetidor dentro de un módulo del repetidor), no necesitan su propio número de serie único. Un agente no tiene que proporcionar acceso de escritura para dichas entidades y puede devolver una cadena de longitud cero. Si se implementa el acceso de escritura para una instancia de entPhysicalSerialNum y se escribe un valor en la instancia, el agente debe	

		conservar el valor proporcionado en la instancia de entPhysicalSerialNum asociada a la misma entidad física durante el tiempo que dicha entidad permanezca instanciada. Esto incluye las instanciaciones a través de todas las reinicializaciones/reinicios del sistema de administración de redes, incluidas aquellas que resultan en un cambio del valor entPhysicalIndex de la entidad física.	
entPhysicalMfgName	1.3.6.1.2.1.47.1.1.1.1.12	El nombre del fabricante de este componente físico. El valor preferido es la cadena de nombre del fabricante que se imprime realmente en el propio componente (si existe). Tenga en cuenta que las comparaciones entre instancias de los objetos entPhysicalModelName, entPhysicalFirmwareRev, entPhysicalSoftwareRev y entPhysicalSerialNum sólo tienen sentido entre entPhysicalEntries con el mismo valor de entPhysicalMfgName. Si el agente desconoce la cadena de nombre de fabricante asociada al componente físico, este objeto contendrá una cadena de longitud cero.	Cisco-IOS-XR-invmgr-oper:inventario/entidades/en basic-bag/nombre-fabricante

entPhysicalModelName	1.3.6.1.2.1.47.1.1.1.1.13	Cadena de identificador de nombre de modelo específico del proveedor asociada a este componente físico. El valor preferido es el número de pieza visible para el cliente, que se puede imprimir en el propio componente. Si el agente desconoce la cadena de nombre de modelo asociada al componente físico, este objeto contendrá una cadena de longitud cero.	Cisco-IOS-XR-invmgr-oper:inventario/entidades/en basic-bag/model-name

IF-MIB

La siguiente tabla representa el nombre y número de OID y la XPATH correspondiente que se configurará en los grupos de sensores de telemetría basados en modelos relacionados con las características y los contadores de la interfaz.

Nombre de OID	Número de OID	Descripción de OID	XPATH
ifMtu	1.3.6.1.2.1.2.2.1.4	El tamaño del paquete más grande que se puede enviar/recibir en la interfaz, especificado en octetos. Para las interfaces que se utilizan para transmitir datagramas de red, este es el tamaño del datagrama de red más grande que se puede enviar en la interfaz.	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/mtu
ifPhysAddress	1.3.6.1.2.1.2.2.1.6	La dirección de la interfaz en su subcapa de protocolo. Por ejemplo, para una interfaz 802.x, este objeto normalmente contiene una dirección MAC. La MIB específica de medios de la	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/tipo-información-de-interfaz/información-de-conjunto/miembro/dirección-mac

		interfaz debe definir el orden de bits y bytes y el formato del valor de este objeto. Para las interfaces que no tienen tal dirección (por ejemplo, una línea serial), este objeto debe contener una cadena de octetos de longitud cero.	
ifType	1.3.6.1.2.1.2.2.1.3	El tipo de interface. La Autoridad de números asignados de Internet (IANA, Internet Assigned Numbers Authority) asigna valores adicionales para ifType mediante la actualización de la sintaxis de la convención textual IANAifType.	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-type
ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17	El número total de paquetes que los protocolos de nivel superior solicitaron que se transmitieran y que no se dirigieron a una dirección de multidifusión o difusión en esta subcapa, incluidos los que se descartaron o no se enviaron. Las discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de ifCounterDiscontinuidadTime.	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/packets-sent
ifHCOutUcastPkts	1.3.6.1.2.1.31.1.1.1.11	El número total de paquetes que los protocolos de nivel superior solicitaron que se transmitieran y que no se dirigieron a una dirección de multidifusión o difusión en esta subcapa, incluidos los	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/packets-sent

		que se descartaron o no se enviaron. Este objeto es una versión de 64 bits de ifOutUcastPkts. Las discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de ifCounterDiscontinuidadTime.	
ifInUcastPkts	1.3.6.1.2.1.2.2.1.11	El número de paquetes, entregados por esta subcapa a una (sub)capa superior, que no se dirigieron a una dirección de multidifusión o difusión en esta subcapa. Las discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de ifCounterDiscontinuidadTime.	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/packets-received
ifHCInUncastPkts	1.3.6.1.2.1.31.1.1.1.7	El número de paquetes, entregados por esta subcapa a una (sub)capa superior, que no se dirigieron a una dirección de multidifusión o difusión en esta subcapa. Este objeto es una versión de 64 bits de ifInUcastPkts. Las discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de ifCounterDiscontinuidadTime.	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/packets-received

ifOutErrors	1.3.6.1.2.1.2.2.1.20	Para interfaces orientadas a paquetes, el número de paquetes salientes que no se pudieron transmitir debido a errores. Para interfaces orientadas a caracteres o de longitud fija, el número de unidades de transmisión saliente que no se pudieron transmitir debido a errores. Las discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de ifCounterDiscontinuidadTime.	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/output-errors
ifOutDiscards	1.3.6.1.2.1.2.2.1.19	El número de paquetes salientes que se eligieron para descartarse aunque no se detectaron errores para evitar que se transmitieran. Una razón posible para descartar este paquete podría ser la necesidad de liberar espacio en la memoria intermedia. Las discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de ifCounterDiscontinuidadTime.	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/output-drops
ifOutMulticastPkts	1.3.6.1.2.1.31.1.1.1.4	El número total de paquetes que los protocolos de nivel superior solicitaron que se transmitieran y que se dirigieron a una dirección de multidifusión en esta subcapa, incluidos los que se	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/multicast-packets-sent

		descartaron o no se enviaron. Para un protocolo de capa MAC, esto incluye las direcciones de grupo y funcionales. Las discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de ifCounterDiscontinuidadTime.	
ifHCOutMulticastPkts	1.3.6.1.2.1.31.1.1.1.12	El número total de paquetes que los protocolos de nivel superior solicitaron que se transmitieran y que se dirigieron a una dirección de multidifusión en esta subcapa, incluidos los que se descartaron o no se enviaron. Para un protocolo de capa MAC, esto incluye las direcciones de grupo y funcionales. Este objeto es una versión de 64 bits de ifOutMulticastPkts. Las discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de ifCounterDiscontinuidadTime.	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/multicast-packets-sent
ifInMulticastPkts	1.3.6.1.2.1.31.1.1.1.2	La cantidad de paquetes, entregados por esta subcapa a una (sub)capa más alta, que fueron dirigidos a una dirección multicast en esta subcapa. Para un protocolo de capa MAC, esto incluye las direcciones de grupo y	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/multicast-packets-received

		funcionales. Las discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de ifCounterDiscontinuidadTime.	
ifHCInMulticastPkts	1.3.6.1.2.1.31.1.1.1.8	La cantidad de paquetes, entregados por esta subcapa a una (sub)capa más alta, que fueron dirigidos a una dirección multicast en esta subcapa. Para un protocolo de capa MAC, esto incluye las direcciones de grupo y funcionales. Este objeto es una versión de 64 bits de ifInMulticastPkts. Las discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de ifCounterDiscontinuidadTime.	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/multicast-packets-received
ifInErrors	1.3.6.1.2.1.2.2.1.14	Para las interfaces orientadas a paquetes, el número de paquetes entrantes que contenían errores que impedían que se entregaran a un protocolo de capa superior. Para interfaces orientadas a caracteres o de longitud fija, el número de unidades de transmisión entrante que contenían errores que impedían que se entregaran a un protocolo de capa superior. Las	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/input-errors

		discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de ifCounterDiscontinuidadTime.	
ifInDiscards	1.3.6.1.2.1.2.2.1.13	El número de paquetes entrantes que se eligieron para descartarse aunque no se detectaron errores para evitar que se entregaran a un protocolo de capa superior. Una razón posible para descartar este paquete podría ser la necesidad de liberar espacio en la memoria intermedia. Las discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de ifCounterDiscontinuidadTime.	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/input-drops
ifOutOctets	1.3.6.1.2.1.2.2.1.16	Número total de octetos transmitidos fuera de la interfaz, incluidos los caracteres de entramado. Las discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de ifCounterDiscontinuidadTime.	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/bytes-sent
ifHCOutOctets	1.3.6.1.2.1.31.1.1.1.10	Número total de octetos transmitidos fuera de la	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-

		interfaz, incluidos los caracteres de entramado. Este objeto es una versión de 64 bits de ifOutOctets. Las discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de ifCounterDiscontinuidadTime.	xr/interface/interface-statistics/full-interface-stats/bytes-sent
ifInOctets	1.3.6.1.2.1.2.2.1.10	Número total de octetos recibidos en la interfaz, incluidos los caracteres de trama. Las discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de ifCounterDiscontinuidadTime.	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/bytes-received
ifHCInOctets	1.3.6.1.2.1.31.1.1.1.6	Número total de octetos recibidos en la interfaz, incluidos los caracteres de trama. Este objeto es una versión de 64 bits de ifInOctets. Las discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de ifCounterDiscontinuidadTime.	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/bytes-received
ifOutBroadcastPkts	1.3.6.1.2.1.31.1.1.1.5	El número total de paquetes que los protocolos de nivel superior solicitaron que se transmitieran y que se	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-statistics/full-interface-

		dirigieron a una dirección de difusión en esta subcapa, incluidos los descartados o no enviados. Las discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de ifCounterDiscontinuidadTime.	stats/broadcast-packets-sent
ifHCOutBroadcastPkts	1.3.6.1.2.1.31.1.1.1.13	El número total de paquetes que los protocolos de nivel superior solicitaron que se transmitieran y que se dirigieron a una dirección de difusión en esta subcapa, incluidos los descartados o no enviados. Este objeto es una versión de 64 bits de ifOutBroadcastPkts. Las discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de ifCounterDiscontinuidadTime.	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/broadcast-packets-sent
ifInBroadcastPkts	1.3.6.1.2.1.31.1.1.1.3	La cantidad de paquetes, entregados por esta subcapa a una (sub)capa más alta, que se dirigieron a una dirección de difusión en esta subcapa. Las discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/broadcast-packets-received

		ifCounterDiscontinuidadTime.	
ifHCInBroadcastPkts	1.3.6.1.2.1.31.1.1.1.9	La cantidad de paquetes, entregados por esta subcapa a una (sub)capa más alta, que se dirigieron a una dirección de difusión en esta subcapa. Este objeto es una versión de 64 bits de ifInBroadcastPkts. Las discontinuidades en el valor de este contador pueden ocurrir en la reinicialización del sistema de administración, y en otros momentos según lo indicado por el valor de ifCounterDiscontinuidadTime.	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/interface-statistics/full-interface-stats/broadcast-packets-received
ifIndex	1.3.6.1.2.1.2.2.1.1	Un valor único mayor que cero para cada interfaz. Se recomienda que los valores se asignen de forma contigua a partir de 1. El valor de cada subcapa de interfaz debe permanecer constante al menos desde una reinicialización del sistema de administración de redes de la entidad hasta la siguiente reinicialización.	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/if-index
ifDescr	1.3.6.1.2.1.2.2.1.2	Una cadena de texto que contiene información sobre la interfaz. Esta cadena debe incluir el nombre del fabricante, el nombre del producto y la versión del hardware/software de la interfaz.	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-xr/interface/description
ifSpeed	1.3.6.1.2.1.2.2.1.5	Una estimación del ancho de banda actual de la interfaz	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interfaz-

		en bits por segundo. Para interfaces que no varían en ancho de banda o para aquellas en las que no se puede hacer una estimación precisa, este objeto debe contener el ancho de banda nominal. Si el ancho de banda de la interfaz es mayor que el valor máximo del que puede informar este objeto, este objeto debe informar de su valor máximo (4.294.967.295) y ifHighSpeed debe utilizarse para informar de la velocidad de la interfaz. Para una subcapa que no tiene concepto de ancho de banda, este objeto debe ser cero.	xr/interfaz/ancho de banda
ifOperStatus	1.3.6.1.2.1.2.2.1.8	El estado operativo actual de la interfaz. El estado testing(3) indica que no se pueden pasar paquetes operativos. Si ifAdminStatus está desactivado(2), ifOperStatus debería estar desactivado(2). Si ifAdminStatus se cambia a up(1), ifOperStatus debería cambiar a up(1) si la interfaz está lista para transmitir y recibir tráfico de red; debería cambiar a dormant(5) si la interfaz está esperando acciones externas (como una línea serial esperando una conexión entrante); debería permanecer en el estado down(2) si y solo si hay un fallo que impide que pase al estado up(1); debería permanecer en el estado	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interfaz-no-dinámica/interfaz-no-dinámica/estado de oper

		notPresent(6) si la interfaz ha perdido componentes (normalmente, hardware).	
ifAdminStatus	1.3.6.1.2.1.2.2.1.7	El estado deseado de la interfaz. El estado testing(3) indica que no se pueden pasar paquetes operativos. Cuando se inicializa un sistema gestionado, todas las interfaces comienzan con ifAdminStatus en el estado down(2). Como resultado de una acción de administración explícita o de la información de configuración conservada por el sistema administrado, ifAdminStatus se cambia a los estados up(1) o testing(3) (o permanece en el estado down(2)).	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interfaz-no-dinámica/interfaz-no-dinámica/estado de administración
ifName	1.3.6.1.2.1.31.1.1.1.1	El nombre textual de la interfaz. El valor de este objeto debe ser el nombre de la interfaz según lo asignado por el dispositivo local y debe ser adecuado para su uso en comandos ingresados en la `consola' del dispositivo. Puede ser un nombre de texto, como `le0' o un número de puerto simple, como `1', dependiendo de la sintaxis de nomenclatura de la interfaz del dispositivo. Si varias entradas de ifTable juntas representan una sola interfaz nombrada por el dispositivo, cada una tendrá el mismo valor de ifName. Tenga en cuenta que para un agente que responde a consultas SNMP relativas a una interfaz en algún otro	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interface-brief/interface-name

		dispositivo (con proxy), el valor de ifName para dicha interfaz es el nombre local del dispositivo con proxy para él. Si no hay un nombre local o este objeto no es aplicable, este objeto contiene una cadena de longitud cero.	
ifHighSpeed	1.3.6.1.2.1.31.1.1.1.15	Una estimación del ancho de banda actual de la interfaz en unidades de 1.000.000 bits por segundo. Si este objeto informa de un valor de `n', la velocidad de la interfaz se encuentra en algún punto del intervalo de `n-500.000' a `n+499.999'. Para interfaces que no varían en ancho de banda o para aquellas en las que no se puede hacer una estimación precisa, este objeto debe contener el ancho de banda nominal. Para una subcapa que no tiene concepto de ancho de banda, este objeto debe ser cero.	Cisco-IOS-XR-pfi-im-cmd-oper:interfaces/interfaces-brief/interfaz-brief/ancho de banda64 bits

IP-MIB

La siguiente tabla representa el nombre y el número de OID y la XPATH correspondiente que se configurará en los grupos de sensores de telemetría basados en modelos relacionados con las estadísticas del protocolo de Internet (IP) y los valores operativos.

Nombre de OID	Número de OID	Descripción de OID	XPATH
icmpInDestUnreachs	1.3.6.1.2.1.5.3	El número de mensajes ICMP de destino inalcanzable	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/statistics/traffic/icm

		recibidos.	
icmpInParmProbs	1.3.6.1.2.1.5.5	Número de mensajes de problema de parámetro ICMP recibidos.	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/statistics/traffic/icm
icmpInSrcQuenchs	1.3.6.1.2.1.5.6	El número de mensajes de ICMP Source Quench recibidos.	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/statistics/traffic/icm
icmpInEchos	1.3.6.1.2.1.5.8	El número de mensajes de eco ICMP (solicitud) recibidos.	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/statistics/traffic/icm
icmpInEchoReps	1.3.6.1.2.1.5.9	Número de mensajes de respuesta de eco ICMP recibidos.	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/statistics/traffic/icm
icmpInTimestamps	1.3.6.1.2.1.5.10	El número de mensajes ICMP Timestamp (request) recibidos.	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/statistics/traffic/icm
icmpInAddrMasks	1.3.6.1.2.1.5.12	Número de mensajes de solicitud de máscara de dirección ICMP recibidos.	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/statistics/traffic/icm
icmpInAddrMaskReps	1.3.6.1.2.1.5.13	Número de mensajes de respuesta de	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/statistics/traffic/icm

		máscara de dirección ICMP recibidos.	
icmpOutMsgs	1.3.6.1.2.1.5.14	El número total de mensajes ICMP que esta entidad intentó enviar. Tenga en cuenta que este contador incluye todos los contados por icmpOutErrors.	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/statistics/traffic/icm
icmpOutDestUnreachs	1.3.6.1.2.1.5.16	El número de mensajes ICMP de destino inalcanzable enviados.	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/statistics/traffic/icm
icmpOutTimeExcds	1.3.6.1.2.1.5.17	El número de mensajes ICMP Time Exceeded enviados.	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/statistics/traffic/icm
icmpOutParmProbs	1.3.6.1.2.1.5.18	Número de mensajes de problema de parámetro ICMP enviados.	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/statistics/traffic/icm
icmpOutSrcQuenchs	1.3.6.1.2.1.5.19	El número de mensajes de ICMP Source Quench enviados.	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/statistics/traffic/icm
icmpOutRedirects	1.3.6.1.2.1.5.20	El número de mensajes de redirección ICMP enviados.	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/statistics/traffic/icm

		Para un host, este objeto siempre será cero, ya que los hosts no envían redirecciones.	
icmpOutEchos	1.3.6.1.2.1.5.21	El número de mensajes de eco ICMP (solicitud) enviados.	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/statistics/traffic/icm
icmpOutEchoReps	1.3.6.1.2.1.5.22	Número de mensajes de respuesta de eco ICMP enviados.	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/statistics/traffic/icm
icmpOutTimestamps	1.3.6.1.2.1.5.23	El número de mensajes ICMP Timestamp (request) enviados.	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/statistics/traffic/icm
icmpOutAddrMasks	1.3.6.1.2.1.5.25	Número de mensajes de solicitud de máscara de dirección ICMP enviados.	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/statistics/traffic/icm
icmpOutAddrMaskReps	1.3.6.1.2.1.5.26	Número de mensajes de respuesta de máscara de dirección ICMP enviados.	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/statistics/traffic/icm
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2	El valor de índice que identifica de forma única la	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/nodes/node/

		interfaz a la que se aplica esta entrada. La interfaz identificada por un valor particular de este índice es la misma interfaz identificada por el mismo valor de ifIndex de RFC 1573.	
ipAdEntAddr	1.3.6.1.2.1.4.20.1.1	La dirección IP a la que pertenece la información de direccionamiento de esta entrada.	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/interfaces/interface/vrfs/vrf/deta address
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3	Máscara de subred asociada a la dirección IP de esta entrada. El valor de la máscara es una dirección IP con todos los bits de red establecidos en 1 y todos los bits de hosts establecidos en 0.	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/interfaces/interface/vrfs/vrf/deta length
ipAdEntBcastAddr	1.3.6.1.2.1.4.20.1.4	Valor del bit menos significativo en la dirección de difusión IP utilizada para enviar datagramas en la interfaz	Cisco-IOS-XR-ipv4-io-oper:ipv4-network/interfaces/interface/vrfs/vrf/deta broadcast

		(lógica) asociada con la dirección IP de esta entrada. Por ejemplo, cuando se utiliza la dirección de difusión de todo unos estándar de Internet, el valor será 1. Este valor se aplica tanto a la subred como a las direcciones de difusiones de red utilizadas por la entidad en esta interfaz (lógica).	
ipNetToMediaPhysAddress	1.3.6.1.2.1.4.22.1.2	La dirección "física" dependiente de los medios.	Cisco-IOS-XR-ipv4-arp-oper:arp/nodes/node/entries/entry/hardv address

IPMIB-COMMON

La siguiente tabla representa el nombre y número de OID y la XPATH correspondiente que se configurará en los grupos de sensores de telemetría basados en modelos relacionados con las estadísticas IP.

Nombre de OID	Número de OID	Descripción de OID	XPATH
ipIfStatsHCOutTransmits	1.3.6.1.2.1.4.31.3.1.31	El número total de datagramas IP que esta entidad suministró a las capas inferiores para la transmisión. Este objeto cuenta los mismos datagramas que ipIfStatsOutTransmits pero permite valores mayores.	Cisco-IOS-XR-ipv4-io-oper: network/nodes/node/statisti stats/packets-forwarding

		Las discontinuidades en el valor de este contador pueden ocurrir al reiniciar el sistema de administración, y en otros momentos como lo indica el valor de ipIfStatsDiscontinuidadTime.	
ipIfStatsInReceives	1.3.6.1.2.1.4.31.3.1.3	Número total de datagramas IP de entrada recibidos, incluidos los recibidos por error. Las discontinuidades en el valor de este contador pueden ocurrir al reiniciar el sistema de administración, y en otros momentos como lo indica el valor de ipIfStatsDiscontinuidadTime.	Cisco-IOS-XR-ipv4-io-oper: network/nodes/node/statisti stats/input-packets
ipIfStatsHCInReceives	1.3.6.1.2.1.4.31.3.1.4	Número total de datagramas IP de entrada recibidos, incluidos los recibidos por error. Este objeto cuenta los mismos datagramas que ipIfStatsInReceives pero permite valores mayores. Las discontinuidades en el valor de este contador pueden ocurrir al reiniciar el sistema de administración, y en otros momentos como lo indica el valor de ipIfStatsDiscontinuidadTime.	Cisco-IOS-XR-ipv4-io-oper: network/nodes/node/statisti stats/input-packets

LLDP-MIB

La siguiente tabla representa el nombre y el número de OID y la XPATH correspondiente que se configurará en los grupos de sensores de telemetría basados en modelos relacionados con los datos operativos del Protocolo de descubrimiento de la capa de enlace (LLDP) en el nodo supervisado.

Nombre de OID	Número de OID	Descripción de OID	XPATH
lldpLocPortId	1.0.8802.1.1.2.1.3.7.1.3	Valor de cadena utilizado para identificar el componente de puerto asociado a un puerto determinado en el sistema local.	Cisco-IOS-XR-ethernet-lldp-oper:lldp/nodes/node/neighbors/devi neighbor/port-id-detail
lldpLocPortIdSubtype	1.0.8802.1.1.2.1.3.7.1.2	El tipo de codificación del identificador de puerto utilizado en el objeto 'lldpLocPortId' asociado.	Cisco-IOS-XR-ethernet-lldp-oper:lldp/nodes/node/neighbors/devi neighbor/mib/port-id-sub-type
lldpLocChassisIdSubtype	1.0.8802.1.1.2.1.3.1	El tipo de codificación utilizado para identificar el chasis asociado con el sistema local.	Cisco-IOS-XR-ethernet-lldp-oper:lldp/nodes/node/neighbors/devi neighbor/mib/chassis-id-sub-type
lldpLocSysName	1.0.8802.1.1.2.1.3.3	Valor de cadena utilizado para identificar el nombre del sistema local. Si el agente local admite IETF RFC 3418, el objeto lldpLocSysName debe tener el mismo valor del objeto sysName.	Cisco-IOS-XR-ethernet-lldp-oper:lldp/nodes/node/neighbors/devi neighbor/detail/system-name
lldpRemSysName	1.0.8802.1.1.2.1.4.1.1.9	Valor de cadena	Cisco-IOS-XR-ethernet-lldp-

		utilizado para identificar el nombre del sistema del sistema remoto.	oper:lldp/nodes/node/neighbors/devi neighbor/detail/system-name
lldpRemChassisId	1.0.8802.1.1.2.1.4.1.1.5	Valor de cadena utilizado para identificar el componente de chasis asociado con el sistema remoto.	Cisco-IOS-XR-ethernet-lldp-oper:lldp/nodes/node/neighbors/devi neighbor/chassis-id
lldpRemChassisIdSubtype	1.0.8802.1.1.2.1.4.1.1.4	El tipo de codificación utilizada para identificar el chasis asociado con el sistema remoto.	Cisco-IOS-XR-ethernet-lldp-oper:lldp/nodes/node/neighbors/devi neighbor
lldpRemPortIdSubtype	1.0.8802.1.1.2.1.4.1.1.6	El tipo de codificación del identificador de puerto utilizado en el objeto 'lldpRemPortId' asociado.	Cisco-IOS-XR-ethernet-lldp-oper:lldp/nodes/node/neighbors/devi neighbor
lldpRemPortId	1.0.8802.1.1.2.1.4.1.1.7	Valor de cadena utilizado para identificar el componente de puerto asociado con el sistema remoto.	Cisco-IOS-XR-ethernet-lldp-oper:lldp/nodes/node/neighbors/devi neighbor
lldpLocChassisId	1.0.8802.1.1.2.1.3.2	Valor de cadena utilizado para identificar el componente de chasis asociado	Cisco-IOS-XR-ethernet-lldp-oper:lldp/nodes/node/neighbors/deta neighbor/chassis-id

		al sistema local.	

MPLS-TE-STD-MIB

La siguiente tabla representa el nombre y número de OID y la XPATH correspondiente que se configurará en los grupos de sensores de telemetría basados en modelos relacionados con los valores operativos de ingeniería de tráfico de conmutación de etiquetas multiprotocolo (MPLS) en el dispositivo administrado.

Nombre de OID	Número de OID	Descripción de OID	XPATH
mplsTunnelName	1.3.6.1.2.1.10.166.3.2.2.1.5	El nombre canónico asignado al túnel. Este nombre se puede utilizar para hacer referencia al túnel en el puerto de la consola del LSR. Si mplsTunnelIsIf se establece en true, el ifName de la interfaz correspondiente a este túnel debe tener un valor igual a mplsTunnelName. Vea también la descripción de ifName en RFC 2863.	Cisco-IOS-XR-mpls-te- p2mp-tunnel/tunnel-hea head/tunnel-name
mplsTunnelDescr	1.3.6.1.2.1.10.166.3.2.2.1.6	Una cadena de texto que contiene información sobre el túnel. Si no hay descripción, este objeto contiene una cadena de longitud cero. Es posible que los protocolos de señalización MPLS no señalen este objeto, por lo que el valor de este objeto en los LSR de tránsito y egreso PUEDE generarse automáticamente o estar ausente.	openconfig-network-ins instance/network- instance/mpls/lsps/restr path/tunnels/tunnel/stat

mplsTunnelPerfHCPacket	1.3.6.1.2.1.10.166.3.2.9.1.2	Contador de alta capacidad para el número de paquetes reenviados por el túnel.	openconfig-network-ins instance/network-instance/mpls/lsps/restr path/tunnels/tunnel/stat
mplsTunnelPerfHCBytes	1.3.6.1.2.1.10.166.3.2.9.1.5	Contador de alta capacidad para el número de bytes reenviados por el túnel.	openconfig-network-ins instance/network-instance/mpls/lsps/restr path/tunnels/tunnel/stat
mplsTunnelHopIpAddress	1.3.6.1.2.1.10.166.3.2.4.1.5	La dirección de salto de túnel para este salto de túnel. El tipo de esta dirección viene determinado por el valor del mplsTunnelHopAddrType correspondiente. El valor de este objeto no se puede cambiar si el valor del objeto mplsTunnelHopRowStatus correspondiente es 'active'.	Cisco-IOS-XR-mpls-te- p2mp-tunnel/tunnel-hea head/destination/destin address

RFC2465-MIB

La siguiente tabla representa el nombre y número de OID y la XPATH correspondiente que se configurará en los grupos de sensores de telemetría basados en modelos relacionados con los valores globales de IPv6.

Nombre de OID	Número de OID	Descripción de OID	XPATH
ipv6AddrPfxLength	1.3.6.1.2.1.55.1.8.1.2	Longitud del prefijo (en bits) asociado a la dirección IPv6 de esta entrada.	Cisco-IOS-XR-ipv6-ma-oper:ipv6-network/nodes/node/interface-data/vrfs/vrf/brief/brief/address/prefix-length
ipv6AddrAnycastFlag	1.3.6.1.2.1.55.1.8.1.4	Este objeto tiene el valor	Cisco-IOS-XR-ipv6-ma-oper:ipv6-network/nodes/node/interface-

		'true(1)', si esta dirección es una dirección de difusión por proximidad y el valor 'false(2)' en caso contrario.	data/vrfs/vrf/brief/brief/address/is-anycast

MIB DE SNMP

La siguiente tabla representa el nombre y número de OID y la XPATH correspondiente que se configurará en los grupos de sensores de telemetría basados en modelos relacionados con el propio agente SNMP, si está disponible.

Nombre de OID	Número de OID	Descripción de OID	XPATH
sysUpTime	1.3.6.1.2.1.1.3	Cadena que representa el tiempo de actividad del sistema	Cisco-IOS-XR-snmp-agent-oper:snmp/information/system-up-time/
sysObjectID	.1.3.6.1.2.1.1.2.0	Cadena que representa el OID del sistema	Cisco-IOS-XR-snmp-agent-oper:snmp/information/system-oid/
sysDescr	1.3.6.1.2.1.1.1	Cadena que representa la descripción del sistema	Cisco-IOS-XR-snmp-agent-oper:snmp/information/system-descr

TCP-MIB

La siguiente tabla representa el nombre y número de OID y la XPATH correspondiente que se configurará en los grupos de sensores de telemetría basados en modelos relacionados con los contadores específicos de TCP.

Nombre de OID	Número de OID	Descripción de OID	XPATH
tcpInErrs	1.3.6.1.2.1.6.14	El número total de segmentos recibidos por error (por ejemplo,	Cisco-IOS-XR-ip-tcp-oper:tcp/nodes/node/statistics/ipv4-traffic/tcp-checksum-error-packets

		sumas de comprobación TCP incorrectas).	
tcpInSegs	1.3.6.1.2.1.6.10	El número total de segmentos recibidos, incluidos los recibidos por error. Este recuento incluye los segmentos recibidos en las conexiones establecidas actualmente.	Cisco-IOS-XR-ip-tcp-oper:tcp/nodes/node/statistics/ipv4-traffic/tcp-input-packets
tcpOutSegs	1.3.6.1.2.1.6.11	El número total de segmentos enviados, incluidos los de las conexiones actuales pero excluyendo los que contienen solo octetos retransmitidos.	Cisco-IOS-XR-ip-tcp-oper:tcp/nodes/node/statistics/ipv4-traffic/tcp-output-packets

MIB DE UDP

La siguiente tabla representa el nombre y número de OID y la XPATH correspondiente que se configurará en los grupos de sensores de telemetría basados en modelos relacionados con los contadores específicos de UDP.

Nombre de OID	Número de OID	Descripción de OID	XPATH
udpOutDatagrams	1.3.6.1.2.1.7.4	El número total de datagramas UDP enviados desde esta entidad.	Cisco-IOS-XR-ip-udp-oper:/udp/nodes/node/statistics/ipv4-traffic/udp-output-packets Cisco-IOS-XR-ip-udp-oper:/udp/nodes/node/statistics/ipv6-traffic/udp-output-packets
udpNoPorts	1.3.6.1.2.1.7.2	Número total de datagramas UDP recibidos para los que no había ninguna aplicación en el puerto de destino.	Cisco-IOS-XR-ip-udp-oper:/udp/nodes/node/statistics/ipv4-traffic/udp-no-ports-packets Cisco-IOS-XR-ip-udp-oper:/udp/nodes/node/statistics/ipv6-traffic/udp-no-ports-packets

udpInErrors	1.3.6.1.2.1.7.3	El número de datagramas UDP recibidos que no se pudieron entregar por razones distintas a la falta de una aplicación en el puerto de destino.	Cisco-IOS-XR-ip-udp-oper:/udp/nodes/node/statistics/ipv4-traffic/udp-checksum-error-packets Cisco-IOS-XR-ip-udp-oper:/udp/nodes/node/statistics/ipv6-traffic/udp-checksum-error-packets
udpInDatagrams	1.3.6.1.2.1.7.1	El número total de datagramas UDP entregados a usuarios UDP.	Cisco-IOS-XR-ip-udp-oper:/udp/nodes/node/statistics/ipv4-traffic/udp-input-packets Cisco-IOS-XR-ip-udp-oper:/udp/nodes/node/statistics/ipv6-traffic/udp-input-packets

Migración de trampas SNMP

Las trampas SNMP son mensajes activados por eventos dinámicos en el dispositivo administrado. Por lo tanto, estos mensajes se comportan de manera análoga al concepto de EDT que hemos tratado anteriormente.

En cuanto a la configuración, MDT permite la misma estructura para EDT, que depende de la implementación en el recopilador de telemetría en términos de opciones o capacidades de marcado de entrada o de marcado de salida.

Observaciones de seguridad

SNMPv2 utiliza solamente la comunidad como mecanismo de autenticación/autorización. Sin embargo, SNMPv3 como hemos descrito anteriormente en la sección SNMP, podría utilizar credenciales para la autenticación y el modelo de cifrado AES para proteger la información.

En el enfoque de telemetría, IOS XR permite el uso de técnicas gRPC/TLS basadas en certificados para realizar la autenticación. Estos certificados se podrían utilizar con un punto de confianza central (por ejemplo, un servidor de CA). Después del proceso de construir una relación de confianza, todos los mensajes de telemetría se envían dentro de una sesión gRPC que se cifra con TLS logrando las mismas ventajas de SNMPv3.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).