Monitoring Policies Reference

The following topics describe the monitoring policies used by Cisco EPN Manager. For information on the supported MIBs and MIB objects, see Cisco EPN Manager.

- Device Health Monitoring Policy, on page 1
- Interface Health Monitoring Policy, on page 2
- Custom MIB Polling Monitoring Policy, on page 2
- IP SLA Y.1731 Monitoring Policy, on page 3
- Pseudowire Emulation Edge to Edge Monitoring Policy, on page 4
- PTP/SyncE Monitoring Policy, on page 4
- Quality of Service Monitoring Policy, on page 4
- IP SLA Monitoring Policy, on page 5
- ME1200 EVC QoS Monitoring Policy, on page 5
- MPLS Link Performance Monitoring Policy, on page 6
- BNG Sessions and IP Pools Monitoring Policy, on page 7
- TDM/SONET Ports Monitoring Policy, on page 7
- Optical SFP Monitoring Policy, on page 8
- Optical 1 day, Optical 15 mins, and Optical 30 secs Monitoring Policies, on page 8
- CEM Monitoring Policy, on page 9
- Device Sensor Monitoring Policy, on page 10
- Performance Counters for Optical Monitoring Policies, on page 10
- GNSS Monitoring Policy, on page 20

Device Health Monitoring Policy

The Device Health Monitoring Policy monitors device CPU utilization, memory pool utilization, environmental temperature, and device availability for all devices in the network. By default, the policy polls devices for this information every 5 minutes, and an alarm is generated if CPU utilization, memory pool utilization, or environmental temperature thresholds are surpassed.

This monitoring policy is activated by default after installation.

Note This policy does not monitor the device CPU utilization and memory pool utilization for supported Cisco ONS or Cisco NCS 2000 devices, but it does monitor memory utilization and device availability.

For information on how to manage this policy, see Set Up Basic Device Health Monitoring.

Note A Device Health Monitoring Policy should not have more than 100 devices under it. For example, if you want to add more than 100 cBR-8 devices in Cisco Evolved Programmable Network Manager, best approach is to create multiple policies and split the devices amongst them.

Interface Health Monitoring Policy

An Interface Health Monitoring Policy monitors over 30 attributes to check interface operational status and performance. It polls device interfaces every 5 minutes and generates an alarm when interface discard, error, utilization, or byte rate thresholds are exceeded.

To protect the performance of large deployments, this policy is not activated by default.

Note This policy does not monitor optical interfaces. Use an optical policy to monitor that information. See Optical 1 day, Optical 15 mins, and Optical 30 secs Monitoring Policies, on page 8.

See these topics for information on how to manage this policy:

- To check whether an Interface Health policy is actively monitoring interfaces, see Check What Cisco Evolved Programmable Network Manager Is Monitoring.
- To set up interface monitoring, see Set Up Basic Interface Monitoring.
- To adjust an interface monitoring policy, see Adjust What Is Being Monitored.

Custom MIB Polling Monitoring Policy

The Custom MIB Polling monitoring policy is a customizable policy that you can use to monitor unsupported parameters—that is, parameters that are not polled by any of the existing monitoring policy types. While creating a custom MIB polling policy, you can choose from an extensive list of Cisco and other MIBs, or import new MIBs into the policy. For more information on managing Custom MIB Polling monitoring policies, see the following topics:

- To check if a custom MIB polling policy is being used to monitor information, see Check What Cisco Evolved Programmable Network Manager Is Monitoring.
- To create a new custom MIB polling policy, see Create a Monitoring Policy for Unsupported Parameters and Third-Party Devices.
- To adjust an existing custom MIB polling policy, see Adjust What Is Being Monitored.

- To schedule and generate custom MIB reports, see Schedule Custom MIB reports

IP SLA Y.1731 Monitoring Policy

An IP SLA Y.1731 monitoring policy uses the Y.1731 ITU-T recommendation to monitor over 70 fault and performance attributes in Metro Ethernet networks.

When you create an IP SLA Y.1731 monitoring policy, by default, it polls the parameters every 15 minutes (by default) and generates an alarm when delay, jitter, frame loss, ccm frame loss, and other thresholds are exceeded.

Cisco EPN Manager stores data at the same interval at which data is stored in the history bucket of the device. For example, if the history buckets on the device are updated every 5 mins and the monitoring policy is configured to poll the device every 15 minutes, Cisco EPN Manager stores 3 buckets of data every 15 minutes.

To collect all polled data without any bucket:

1. Ensure that time interval of the aggregated history buckets is longer than the polling interval of the monitoring policy.
2. Configure at least two history buckets on the device.

This enhancement is available in:

- Cisco IOS-XR devices that run 6.1.1 OS version and higher. Data collection for all probe types (loss and delay) must be triggered at the same time for all devices. All devices must be configured with the same history bucket duration.
- Cisco IOS-XE devices - NCS 42xx and NCS 520 devices that run 17.3.1 OS version and higher.

Note For devices where this enhancement is not applicable (devices running an older software version or with the collection conditions mentioned above not met), Cisco EPN Manager collects and aggregates data from relevant buckets according to the policy collection interval.

For each measurement, the forward, backward and two way data is collected. Bins statistics data is not polled by default. To enable the collection of this data, choose a polling frequency, for details see Change the Polling for a Monitoring Policy.

Note This policy collects Bins statistics data on ME 1200, NCS 42xx and ASR 9xx devices.

For ME 1200 devices, if the MEG ID is longer than 18 characters, Bin statistics data will not be collected and presented in the Y1731 dashboard tab.

For more information on how to configure and manage an IP SLA Y.1731 monitoring policy, see these topics:

- To check if IP SLA Y.1731 parameters are being monitored , see Check What Cisco Evolved Programmable Network Manager Is Monitoring.
- To create a new IP SLA Y.1731 monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types.

- To adjust an existing IP SLA Y.1731 monitoring policy, see Adjust What Is Being Monitored.

Pseudowire Emulation Edge to Edge Monitoring Policy

A Pseudowire Emulation Edge to Edge (PWE3) monitoring policy polls approximately 20 attributes that emulate edge-to-edge services over a Packet Switched Network (PSN). When you create and enable a monitoring policy that uses this policy type, attributes are polled every 15 minutes by default. In addition, Cisco Evolved Programmable Network Manager generates a minor alarm when the thresholds for the following attributes are surpassed on pseudowire virtual circuits (PW VCs):

- HC packets and bytes—Total in and total out rates
- Operational status up, inbound and outbound operational status up

For more information on how to configure and manage a PWE3 monitoring policy, see these topics:

- To check if PWE3 parameters are being monitored , see Check What Cisco Evolved Programmable Network Manager Is Monitoring.
- To create a new PWE3 monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types.
- To adjust an existing PWE3 monitoring policy, see Adjust What Is Being Monitored.

PTP/SyncE Monitoring Policy

The PTP/SyncE monitoring policy measures PTP and SyncE performance. When you create a PTP/SyncE Monitoring policy, it polls the parameters every 30 minutes by default. The polling frequency can also be set to 5 , 15 or 60 minutes.

For more information on how to configure and manage a PTP/SyncE monitoring policy, see these topics:

- To check what the PTP/SyncE monitoring policy is monitoring , see Check What Cisco Evolved Programmable Network Manager Is Monitoring.
- To create a new PTP/SyncE monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types.
- To adjust an existing PTP/SyncE monitoring policy, see Adjust What Is Being Monitored.

Quality of Service Monitoring Policy

A Quality of Service monitoring policy polls over 60 service parameters to validate the quality of services running on network devices. When you create a Quality of Service monitoring policy, it polls the parameters every 15 minutes and generates an alarm when certain thresholds are exceeded. The following is a partial list of parameters that can cause an alarm:

- Dropped/discarded bytes and packets rates

- Pre-policy bytes and packets rates, utilization, percent of Committed Information Rate (CIR), Peak Information Rate (PIR)
- Post-policy bytes rates, utilization, percent of Committed Information Rate (CIR), Peak Information Rate (PIR)

To view all Quality of Service parameters that can cause TCAs, see Check Which Parameters and Counters Are Polled By a Monitoring Policy.

For more information on how to configure and manage a Quality of Service monitoring policy, see these topics:

- To check if Quality of Service parameters are being monitored , see Check What Cisco Evolved Programmable Network Manager Is Monitoring.
- To create a new Quality of Service monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types.
- To adjust an existing Quality of Service monitoring policy, see Adjust What Is Being Monitored.

IP SLA Monitoring Policy

An IP SLA monitoring policy monitors approximately 20 parameters to provide real-time performance information. When you create an IP SLA monitoring policy, it polls the parameters every 15 minutes. This monitoring policy does not generate any alarms; if you want to generate IP SLA-based alarms, use the IP SLA Y.1731 monitoring policy.

For more information on how to configure and manage an IP SLA monitoring policy, see these topics:

- To check if IP SLA parameters are being monitored , see Check What Cisco Evolved Programmable Network Manager Is Monitoring.
- To create a new IP SLA monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types.
- To adjust an existing IP SLA monitoring policy, see Adjust What Is Being Monitored.

ME1200 EVC QoS Monitoring Policy

A ME1200 QoS monitoring policy polls 28 service parameters to validate the quality of selected services running on ME1200 devices. When you create a ME1200 Quality of Service monitoring policy, it polls the parameters every 15 minutes by default but does not generate an alarm when certain thresholds are exceeded. The polling frequency can be changed by selecting the preferred value from the drop down list.

The following is a partial list of parameters that are polled by ME1200 QoS monitoring policy:

- Transmitted and discarded bytes and packets rates.
- Average bit and frame rates for green (conforming), yellow (exceeding), red (violating), and discard traffic (both inbound and outbound)

Note To ensure that you are viewing accurate ME1200 QoS data, when you enable the ME1200 EVC Quality of Service monitoring policy, first disable the EVC performance monitoring session on the ME1200 devices.

To view all ME1200 QoS parameters that are polled, see Check Which Parameters and Counters Are Polled By a Monitoring Policy.

For more information on how to configure and manage a ME1200 QoS monitoring policy, see these topics:

- To check if ME1200 QoS parameters are being monitored , see Check What Cisco Evolved Programmable Network Manager Is Monitoring.
- To create a new ME1200 QoS monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types.
- To adjust an existing ME1200 QoS monitoring policy, see Adjust What Is Being Monitored.

MPLS Link Performance Monitoring Policy

The MPLS Link Performance monitoring policy measures link delay in MPLS. When you create a MPLS link performance Monitoring policy, it polls the parameters every 15 minutes by default. The polling interval can also be set to 1, 5 or 60 minutes.

Note This policy collects data on the following devices:

- For Link delay:
  - ASR 9000 devices, version 7.0.1 and above.
  - NCS 5500 devices , version 7.1.1 and above .
- For TWAMP Light responder metrics:
  - ASR 9000 devices, version 7.0.1 and above.
  - NCS 540 devices, version 7.2.1 and above.

This policy polls the following parameters:

- Average Delay
- Min Delay
- Max Delay
- RX packets
- TX packets

For more information on how to configure and manage a MPLS Link Performance monitoring policy, see these topics:

- To check what the MPLS Link Performance monitoring policy is monitoring , see Check What Cisco Evolved Programmable Network Manager Is Monitoring.
- To create a new MPLS Link Performance monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types.
- To adjust an existing MPLS Link Performance monitoring policy, see Adjust What Is Being Monitored.

BNG Sessions and IP Pools Monitoring Policy

This monitoring policy polls over 5 parameters to monitor the BNG sessions as well as the IP addresses leased from the IP pools. When you create a BNG Sessions and IP Pools monitoring policy, it polls the parameters every 15 minutes and generates an alarm when certain thresholds are exceeded. The following is a partial list of parameters that can cause an alarm:

- Number of used or free IP addresses in the IP pools.
- Number of sessions for authenticated and up subscribers.

To view all BNG Sessions and IP Pools parameters that can cause TCAs, see Check Which Parameters and Counters Are Polled By a Monitoring Policy.

For more information on how to configure and manage a BNG Sessions and IP Pools monitoring policy, see these topics:

- To check if BNG Sessions and IP Pools parameters are being monitored , see Check What Cisco Evolved Programmable Network Manager Is Monitoring.
- To create a new BNG Sessions and IP Pools monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types.
- To adjust an existing BNG Sessions and IP Pools monitoring policy, see Adjust What Is Being Monitored.

TDM/SONET Ports Monitoring Policy

When you create a TDM/SONET Ports monitoring policy, it polls the parameters based on the polling frequency selected. You can define alarms that will be generated if any thresholds parameters are exceeded.

For more information on how to configure and manage a TDM/SONET Ports monitoring policy, see these topics:

- To check if TDM/SONET Ports parameters are being monitored , see Check What Cisco Evolved Programmable Network Manager Is Monitoring.
- To create a new TDM/SONET Ports monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types.
- To adjust an existing TDM/SONET Ports monitoring policy, see Adjust What Is Being Monitored.

Optical SFP Monitoring Policy

An Optical SFP monitoring policy polls health and performance information for optical Small Form-Factor Pluggable (SFP) interfaces. This policy polls temperature, voltage, current, and optical TX/RX power. When you create an Optical SFP monitoring policy, it polls the parameters every 1 minute.

For more information on how to configure and manage an Optical SFP monitoring policy, see these topics:

- To check if Optical SFP parameters are being monitored , see Check What Cisco Evolved Programmable Network Manager Is Monitoring.
- To create a new Optical SFP monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types.
- To adjust an existing Optical SFP monitoring policy, see Adjust What Is Being Monitored.

Optical 1 day, Optical 15 mins, and Optical 30 secs Monitoring Policies

Monitoring policies play a crucial role in collecting valuable network performance and status data for analysis and optimization. The Optical 1 day, Optical 15 minutes, and Optical 30 seconds monitoring policies are configurations used for data collection and monitoring purposes.

Optical 1 day monitoring policy: The Optical 1 day monitoring policy must be enabled to poll the device data for a time period of more than 2 weeks. The Optical 1 day monitoring policy polls the following optical interfaces:

Optical 15 minutes monitoring policy: The Optical 15 mins monitoring policy must be enabled to collect the device data from 1 hour to 1 week. The Optical 15 mins monitoring policy polls the following optical interfaces:

- Physical, OTN, OTU FEnd, OTU NEnd, ODU FEnd, ODU NEnd, OTN GFP, OTN FEC, Ethernet, and SONET/SDH interfaces on Cisco NCS 4000 series, Cisco ASR 9000 series routers, Cisco NCS 5500 series, Cisco NCS 5700 series routers, Cisco 8000 series routers, and Cisco NCS 1000 series devices.
- DWDM interfaces on Cisco NCS 2000 series and Cisco ONS devices.

Optical 30 seconds monitoring policy: The Optical 30 sec monitoring policy is specifically enabled to collect 1 hour device data for the following optical interfaces:

- Physical, OTN, and Ethernet parameters on the Cisco NCS 1010 and NCS 1004 devices.

Note For the above-mentioned devices, to collect data for longer durations, ranging from 6 hours to 1 week, Optical 15 minutes monitoring policy must be enabled.

By following the recommended monitoring policies, you can optimize data collection, make informed decisions, and maintain a high-performing and reliable network infrastructure across your NCS devices. For detailed

steps on configuring these monitoring policies or any other specific settings, please refer to the device-specific documentation.

See Performance Counters for Optical Monitoring Policies, on page 10 for a list of the parameters that these policies poll.

For more information on how to configure and manage the Optical 1 day, Optical 15 mins, and Optical 30 secs monitoring policy, see the following topics:

- To check if Optical 1 day, Optical 15 mins, and Optical 30 secs parameters are being monitored, see Check What Cisco Evolved Programmable Network Manager Is Monitoring.
- To create a new Optical 1 day, Optical 15 mins, and Optical 30 secs monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types.
- To adjust an existing Optical 1 day, Optical 15 mins, and Optical 30 secs monitoring policy, see Adjust What Is Being Monitored.

Note For IOS-XR devices, you can generate a collected OTN 15 mins report or choose a specific OTN 15 mins parameter to generate separate configuration reports. The different options are:

- OTU FEnd
- OTU NEnd
- ODU FEnd
- ODU NEnd
- OTN GFP
- OTN FEC

CEM Monitoring Policy

Use the CEM Monitoring Policy to poll the following CEM parameters:

- Jitter Buffer Overruns
- Generated Lbits
- Received Lbits
- Generated Rbits
- Received Rbits
- Generated Nbits
- Received Nbits
- Generated Pbits
- Received Pbits

The polling happens through the CLI and the delta of the current and last collection is taken as the current entry.

Note This polling data is not displayed in the dashboard.

Device Sensor Monitoring Policy

Use the Device Sensor monitoring policy to poll the sensor information through SNMP to the devices that are added to this policy. The sensor details such as voltage, power, and current temperature are polled to the device.

Note There are no calculations involved in the device sensor data.

Performance Counters for Optical Monitoring Policies

The following topics list the performance counters used by the optical monitoring policies. This information is provided here because it is not available from the web GUI.

- Reference—Performance Counters for Physical Interfaces, on page 10
- Reference—Performance Counters for OTN-FEC Interfaces, on page 13
- Reference—Performance Counters for OTN-ODU Interfaces, on page 13
- Reference—Performance Counters for OTN-OTU Interfaces, on page 14
- Reference—Performance Counters for Ethernet Interfaces, on page 15
- Reference—Performance Counters for SONET Interfaces, on page 16
- Reference—Performance Counters for SDH Interfaces, on page 17
- Reference—Performance counters for DS1/DS3, on page 19

Reference—Performance Counters for Physical Interfaces

The following table lists the performance counters used by the optical policy types to monitor physical interfaces.

Performance counters marked with an asterisk (*) are applicable for all Cisco Optical Networking Services (ONS) and Cisco Network Convergence System (NCS) 2000 series devices. Performance counters marked with a double asterisk (**) are applicable for Cisco Network Convergence System (NCS) 4000 series devices.

Physical Interface Performance Counter	Description
OPR-MIN	Minimum output power received by the optical circuit.

OPR-AVG	Average output power received by the optical circuit.
OPR-MAX	Maximum output power received by the optical circuit.
OPT-MIN	Minimum output power transmitted from the optical circuit.
OPT-AVG	Average output power transmitted from the optical circuit.
OPT-MAX	Maximum output power transmitted from the optical circuit.
OSC_PWR	Power received by the optical circuit.
LBC-MIN* LBCL-MIN	Minimum laser bias current for the optical circuit.
LBC-AVG* LBCL-AVG	Average laser bias current for the optical circuit.
LBC-MAX* LBCL-MAX	Maximum laser bias current for the optical circuit.
DGD-MIN**	Minimum differential group delay for the optical circuit.
DGD-AVG**	Average differential group delay for the optical circuit.
DGD-MAX**	Maximum differential group delay for the optical circuit.
SOPMD-MIN**	Minimum second order polarization mode dispersion for the optical circuit.
SOPMD-AVG**	Average second order polarization mode dispersion for the optical circuit.
SOPMD_MAX**	Maximum second order polarization mode dispersion for the optical circuit.
OSNR-MIN**	Minimum optical signal to noise ratio for the optical circuit.
OSNR-AVG**	Average optical signal to noise ratio for the optical circuit.
OSNR-MAX**	Maximum optical signal to noise ratio for the optical circuit.
eSNR-MIN**	Minimum electrical signal to noise ratio for the optical circuit.
eSNR-AVG**	Average electrical signal to noise ratio for the optical circuit.
eSNR-MAX**	Maximum electrical signal to noise ratio for the optical circuit.
PDL-MIN**	Minimum polarization-dependent loss for the optical circuit.
PDL-AVG**	Average polarization-dependent loss for the optical circuit.
PDL-MAX**	Maximum polarization-dependent loss for the optical circuit.
PCR-MIN**	Minimum polarization change rate for the optical circuit.

Monitoring Policies Reference

PCR-AVG**	Average polarization change rate for the optical circuit.
PCR-MAX**	Maximum polarization change rate for the optical circuit.
PMD-AVG*,**	Average polarization mode dispersion for the optical circuit.
PMD-MIN*,**	Minimum polarization mode dispersion for the optical circuit.
PN-MIN**	Minimum phase noise for the optical circuit.
PN-AVG**	Average phase noise for the optical circuit.
PN-MAX**	Maximum phase noise for the optical circuit.
PREFEC-BER*	Preforward error correction bit error rate for the optical circuit.
CD-MIN**	Minimum chromatic dispersion for the optical circuit.
CD-AVG**	Average chromatic dispersion for the optical circuit.
CD-MAX**	Maximum chromatic dispersion for the optical circuit.

Note PMD-MIN and PMD-AVG are not applicable for SVO devices.

The following table lists the performance counters used by the optical policy types to monitor physical interfaces and collect data in real time from NCS1004, NCS560, NCS5500, CISCO8XXX, NCS540 and ASR9K devices.

Physical Interface Performance Counter	**Description**
CD	Chromatic dispersion
DGD	Differential group delay
SOPMD	Second order polarization mode dispersion
PCR	Polarization change rate
PDL	Polarization-dependent loss
OSNR	Optical signal to noise ratio
TX-POWER	Optical power transmitted
RX-POWER	Optical power received
LBC	Laser Bias Current
RX-SIG	Received signal power
FREQ-OFF	Frequency Difference

Qfactor	Quality Factor
Qmargin	Quality Factor Margin
BAUDRATE	Rate of information transfer (bits per second)
Pre-FEC-Val	Pre Forward Error Correction Value
Pre-FEC-BER	Pre Forward Error Correction Value Bit Error Rate
Post-FEC-BER	Post Forward Error Correction Value Bit Error Rate

Reference—Performance Counters for OTN-FEC Interfaces

The following table lists the performance counters used by the optical policy types to monitor OTN-FEC interfaces.

Performance counters marked with an asterisk (*) are applicable for all Cisco Optical Networking Services (ONS) and Cisco Network Convergence System (NCS) 2000 series devices.

OTN-FEC Interface Performance Counter	**Description**
BIT-EC* BIEC	Number of bit errors corrected.
UNC-WORDS* UCW	Number of uncorrectable words.

Reference—Performance Counters for OTN-ODU Interfaces

The following table lists the performance counters used by the optical policy types to monitor OTN-ODU interfaces.

OTN-ODU Interface Performance Counter	**Description**
BBE-PM	Number of background block errors in path monitoring.
BBER-PM	Background block errors ratio in path monitoring.
ES-PM	Number of errored seconds in path monitoring.
ESR-PM	Errored seconds ratio in path monitoring.
SES-PM	Number of severely errored seconds in path monitoring.
SESR-PM	Severely errored seconds ratio in path monitoring.
UAS-PM	Number of unavailable seconds in path monitoring.
FC-PM	Number of failure counts (AIS/RFI detected) in path monitoring.

gfpStatsRxFrames	Number of generic framing procedure (GFP) frames received.
gfpStatsTxFrames	Number of GFP frames transmitted.
gfpStatsRxOctets	Number of GFP bytes received.
gfpStatsTxOctets	Number of GFP bytes transmitted.
gfpStatsRxCRCErrors	Number of packets received with a payload frame check sequence (FCS) error.
gfpStatsRxMBitErrors	Number of multiple bit errors. In the GFP core header at the GFP-transparent (GFP-T) receiver, these are uncorrectable.
gfpStatsRxSBitErrors	Number of single bit errors. In the GFP core header at the GFP-T receiver, these are correctable.
gfpStatsRxTypeInvalid	Number of packets received with invalid GFP type. This includes unexpected user payload identifier (UPI) type and errors in core header error check (CHEC).
gfpStatsRxCIDInvalid	Number of packets received with invalid CID.
gfpStatsRoundTripLatencyUSec	Round trip delay for the end-to-end Fibre Channel transport in milliseconds.
gfpStatsTxDistanceExtBuffers	Number of buffer credit transmitted for GFP-T transmitter (valid only if distance extension is enabled).
gfpStatsRxSblkCRCErrors	Number of super block cyclic redundancy check (CRC) errors.
gfpStatsCSFRaised	Number of GFP client signal fail (CSF) frames detected at the GFP-T receiver.
gfpStatsLFDRaised	Number of GFP loss of frame delineation (LFD) detected.
gfpRxCmfFrame	Number of client management frames (CMF) received.
gfpTxCmfFrame	Number of client management frames (CMF) transmitted.
gfpStatsCHecRxMBitErrors	Number of core header error control (cHEC) CRC multiple bit errors.
gfpStatsTHecRxMBitErrors	Number of type header error control (tHEC) CRC multiple bit errors.

Reference—Performance Counters for OTN-OTU Interfaces

The following table lists the performance counters used by the optical policy types to monitor OTN-OTU interfaces.

OTN-OTU Interface Performance Counter	**Description**
BBE-SM	Number of background block errors in section monitoring.

BBER-SM	Background block error ratio in section monitoring.
ES-SM	Number of errored seconds in section monitoring.
ESR-SM	Errored seconds ratio in section monitoring.
SES-SM	Number of severely errored seconds in section monitoring.
SESR-SM	Severely errored seconds ratio in section monitoring.
UAS-SM	Number of unavailable seconds in section monitoring.
FC-SM	Number of failure counts (AIS/RFI detected) in section monitoring.

Reference—Performance Counters for Ethernet Interfaces

The following table lists the performance counters used by the optical policy types to monitor Ethernet interfaces.

Ethernet Interface Performance Counter	Description
ifInOctets	The total number of octets received on the interface, including framing octets.
ifInErrors	The total number of received packets that were discarded because of errors.
ifOutOctets	The total number of transmitted octets, including framing packets.
ifInUcastPkts	The total number of unicast packets received since the last counter reset.
ifOutUcastPkts	The total number of packets requested by the higher-level protocols to be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
ifInMulticastPkts	The total number of multicast packets received since the last counter reset.
ifOutMulticastPkts	The total number of multicast frames transmitted error free.
ifInBroadcastPkts	The total number of broadcast packets received since the last counter reset.
ifOutBroadcastPkts	The total number of packets requested by higher-level protocols and addressed to a broadcast address at this sublayer, including those that were not transmitted.
txTotalPkts	The total number of packets transmitted.
rxTotalPkts	The total number of packets received.
etherStatsOctets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
etherStatsOversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed. Note that for tagged interfaces, this number becomes 1522 bytes.

dot3StatsFCSErrors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check.
dot3StatsFrameTooLongs	A count of frames received on a particular interface that exceed the maximum permitted frame size.
etherStatsJabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherStatsPkts64Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts65to127 Octets	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts128to255 Octets	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts256to511 Octets	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts512to1023Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts1024to1518Octets	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsMulticastPkts	The total number of good packets received that were directed to a multicast address.
etherStatsBroadcastPkts	The total number of good packets received that were directed to the broadcast address.
etherStatsUndersizePkts	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.

Reference—Performance Counters for SONET Interfaces

The following table lists the performance counters used by the optical policy types to monitor SONET interfaces.

Performance counters marked with an asterisk (*) are applicable for all Cisco Optical Networking Services (ONS) and Cisco Network Convergence System (NCS) 2000 series devices.

SONET Interface Performance Counter	Description	Available over
Errored Seconds (ES)*	Number of errored seconds for near end and far end devices.	Line* Path VT-Path Section* (applicable only for near end devices)
Severely Errored Seconds (SES)*	Number of severely errored seconds for near end and far end devices.	Line* Path VT-Path Section* (applicable only for near end devices)
Severely Errored Framing Seconds (SEFS)*	Number of severely errored framing seconds for near end devices.	Section* (applicable only for near end devices)
Coding Violations (CV)*	Number of coding violations for near end and far end devices. .	Line* Path VT-Path Section* (applicable only for near end devices)
Unavailable Seconds (UAS)*	Number of unavailable seconds for near end and far end devices.	Line* Path VT-Path

Reference—Performance Counters for SDH Interfaces

The following table lists the performance counters used by the optical policy types to monitor SDH interfaces.

SDH Interface Performance Counter	Description
MS-ES	Number of errored seconds per multiplex section for near end and far end devices.
MS-ESR	Error seconds ratio per multiplex section for near end and far end devices.
MS-SES	Number of severely errored seconds per multiplex section for near end and far end devices.
MS-SESR	Severely errored seconds ratio per multiplex section for near end and far end devices.

MS-BBE	Number of background block errors per multiplex section for near end and far end devices.
MS-BBER	Background block error ratio per multiplex section for near end and far end devices.
MS-UAS	Number of unavailable seconds per multiplex section for near end and far end devices.
MS-EB	Number of errored block per multiplex section for near end and far end devices.
MS-FC	Number of failure counts per multiplex section for near end and far end devices.
MS-PSC	Protection switching count per multiplex section. PSC is the number of times the service switches from a working card to a protection card and back.
MS-PSC-R	Protection switching count ring per multiplex section. This count is incremented only if ring switching is used.
MS-PSC-S	Protection switching count span per multiplex section. This count is incremented only if span switching is used.
MS-PSC-W	Protection switching count working per multiplex section. It is the count of the number of times traffic switches away from the working capacity in the failed line and back to the working capacity after the failure is cleared. PSC-W increments on the failed working line.
MS-PSD	Protection switching duration applies to the length of time, in seconds, that service is carried on another line.
MS-PSD-R	Protection switching duration ring is a count of the seconds that the protection line was used to carry service. This count is incremented only if ring switching is used.
MS-PSD-S	Protection switching duration span is a count of the seconds that the protection line was used to carry service. This count is incremented only if span switching is used.
MS-PSD-W	Protection switching duration working per multiplex section.
RS-ES	Number of errored seconds per regenerator section.
RS-ESR	Errored seconds ratio per regenerator section.
RS-SES	Number of severely errored seconds per regenerator section.
RS-SESR	Severely errored seconds ratio per regenerator section.
RS-BBE	Number of background block errors per regenerator section.
RS-BBER	Background block errors ratio per regenerator section.
RS-UAS	Number of unavailable seconds per regenerator section.
RS-EB	Number of errored block per regenerator section.
RS-OFS	Number of out-of-frame seconds per regenerator section.

Reference—Performance counters for DS1/DS3

Performance counters for DS1

DS1 Performance Counter	Description
Unavailable Seconds (UAS)	Number of unavailable seconds for near end and far end devices.
Code Violations (CV)	Number of code violations for near end and far end devices.
Controlled Slip Seconds (CSS)	Number of controlled slip seconds for near end and far end devices.
Errored Seconds (ES)	Number of errored seconds for near end and far end devices.
Severely Errored Seconds (SES)	Number of severely errored seconds for near end and far end devices.
Severely Errored Framing Seconds (SEFS)	Number of severely errored framing seconds for near end and far end devices.
Bursty Error Seconds (BES)	Number of bursty error seconds for near end and far end devices.
Degraded Minutes (DM)	Number of degraded minutes for near end and far end devices.

Performance Counters for DS3

DS3 Performance Counter	Description
Errored Seconds (ES)	Number of errored seconds for near end and far end devices.
Severely Errored Seconds (SES)	Number of severely errored seconds for near end devices.
Code Violations (CV)	Number of code violations for near end and far end devices.
P-bit Code Violations (CVP)	Number of P-bit code violations for near end devices.
P-bit Errored Seconds (ESP)	Number of P-bit errored seconds for near end devices.
Severely Errored Seconds P-bit (SESP)	Number of P-bit severely errored seconds for near end and far end devices.
Severely Errored Framing Seconds (SEFS)	Number of severely errored framing seconds for near end devices.
Unavailable Seconds (UAS)	Number of unavailable seconds for near end and far end devices.
C-bit Coding Violations (CVC)	Number of C-bit coding violations for near end and far end devices.

DS3 Performance Counter	Description
C-bit Errored Seconds (ESC)	Number of C-bit errored seconds for near end and far end devices.
Severely Errored Seconds CP-bit (SESCP)	Number of CP-bit severely errored seconds for near end and far end devices.

GNSS Monitoring Policy

When you create a Global Navigation Satellite System (GNSS) monitoring policy, Cisco EPN Manager collects data from a network device by polling the following parameters:

- GNSS Module Presence Status
- GNSS Module Slot State
- GNSS Satellite Visibility Status
- GNSS Module Satellite Count
- GNSS Module SvId SNR
- GNSS Antenna Short Alarm Status
- GNSS Antenna Open Alarm Status

The policy polls every 30 minutes by default. You can change the default interval by changing the polling frequency. Note that GNSS monitoring policy does not have a threshold crossing alarm.

For more information on how to configure and manage GNSS monitoring policy, see these topics:

- To check what the GNSS monitoring policy is monitoring, see Check What Cisco Evolved Programmable Network Manager Is Monitoring.
- To create a new GNSS monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types.
- To adjust an existing GNSS monitoring policy, see Adjust What Is Being Monitored.