

Supported Collectors and Tools

This section contains the following topics:

- Collector Descriptions, on page 1
- Collect Basic Topology Information, on page 3
- Collect LSP Information, on page 9
- Collect PCEP LSP Information Using SR-PCE, on page 10
- Collect Multicast Flow Data from a Network, on page 12
- Discover BGP Topology, on page 14
- Discover VPN Topology, on page 17
- Collect Hardware Inventory Information, on page 18
- Collect Port, LSP, SRLG, and VPN Information Using Configuration Parsing, on page 24
- Improve Network Model Visualization, on page 27
- Collect Traffic Statistics, on page 29
- Collect Traffic Demands Information, on page 33
- NetFlow Data Collection, on page 34
- Run External Scripts Against a Network Model, on page 37
- Merge AS Plan Files, on page 38

Collector Descriptions

Each collector in Cisco Crosswork Planning has capabilities that determine what it collects or deploys.

Table 1: Collector Descriptions

Collector	Description	Prerequisite/Notes	Configuration Steps
Basic Topology Collection			
IGP database	Discovers IGP topology using login and SNMP.	This is a basic topology collection. The resulting network model is used as the source network for other collectors.	See Collect Topology Information Using the IGP Database Collector, on page 4

Collector	Description	Prerequisite/Notes	Configuration Steps
SR-PCE	Discovers Layer 3 topology using SR-PCE. It uses raw SR-PCE data as the source for the topology. Node and interface/port properties are discovered using SNMP.	• The SR-PCE agents must be configured before running this collection. For details, see Configure Agents. • This is a basic topology collection for networks using SR-PCE. The resulting network model is used as the source network for other collectors.	See Collect Topology Information Using the SR-PCE Collector, on page 5
Advanced Modeling Collection			
LSP	Discovers LSP information using SNMP.	• A network model with basic topology collection must exist. • If using SR-PCE, the Collect Topology Information Using the SR-PCE Collector, on page 5 must be completed before running this collection.	See Collect LSP Information, on page 9
PCEP LSP	(Accessible only when SR-PCE collector is selected as the basic topology collector) Discovers PCEP LSPs using SR-PCE.	The Collect Topology Information Using the SR-PCE Collector, on page 5 must be completed before running this collection.	See Collect PCEP LSP Information Using SR-PCE, on page 10
BGP	Discovers BGP peering using login and SNMP.	A network model with basic topology collection must exist.	See Discover BGP Topology, on page 14
VPN	Discovers Layer 2 and Layer 3 VPN topology.	A network model with basic topology collection must exist.	See Discover VPN Topology, on page 17
Config parsing	Discovers and parses information from router configurations in the network.	A network model with basic topology collection must exist.	See Collect Port, LSP, SRLG, and VPN Information Using Configuration Parsing, on page 24
Traffic and Demands Collection			
Inventory	Collects hardware inventory information.	A network model with basic topology collection must exist.	See Collect Hardware Inventory Information, on page 18
Multicast	Collects multicast flow data from a given network.	A network model with basic topology collection must exist.	See Collect Multicast Flow Data from a Network, on page 12

Collector	Description	Prerequisite/Notes	Configuration Steps
Layout	Adds layout properties to a source model to improve visualization.	• An aggregated network model. • After the Layout collector is configured, a plan file containing layout properties must be imported back into the Layout model.	See Improve Network Model Visualization, on page 27
Traffic collection	Collects traffic statistics (interface traffic, LSP traffic, MAC traffic, and VPN traffic) using SNMP polling.	• A network model with basic topology collection must exist. • If collecting LSP traffic, a network model with LSP collection must exist. See Collect LSP Information, on page 9. • If collecting VPN traffic, a network model with VPN collection must exist. See Discover VPN Topology, on page 17.	See Collect Traffic Statistics, on page 29
Demand deduction	Collects information regarding traffic demands from the network.	Source DARE network containing traffic data must exist.	See Collect Traffic Demands Information, on page 33
NetFlow	Collects and aggregates exported NetFlow and related flow measurements.	A network model with basic topology collection must exist.	See Configure the NetFlow Collection, on page 35
Custom Scripts			
External script	Runs customized scripts to append additional data to a source network model.	A source network model and a custom script must exist.	See Run External Scripts Against a Network Model, on page 37

Collect Basic Topology Information

The network model resulting from basic topology collectors is used as the source network for additional data collections. There are two collectors in Cisco Crosswork Planning which are used for this purpose, **IGP database** and **SR-PCE**. For detailed information on how to configure these collectors to collect the topology information, see Collect Topology Information Using the IGP Database Collector, on page 4 and Collect Topology Information Using the SR-PCE Collector, on page 5.

Collect Topology Information Using the IGP Database Collector

In Cisco Crosswork Planning, there are two topology collectors: IGP database and SR-PCE. In a single collection, you can choose any one of these collectors for collecting information related to topology. Selecting both collectors is not permitted.

To use the SR-PCE collector for topology collection, see Collect Topology Information Using the SR-PCE Collector, on page 5.

The **IGP database** collector discovers network topology using IGP database with the collection of node properties and interface and port discovery using SNMP. This is typically the first collector that is configured before other collectors, because it provides the basic data collection needed. This collector provides full topology discovery. Collection of multi instances of OSPF and IS-IS is also supported. All links collected from routers will have an associated IGP process ID.

The network model resulting from topology discovery is used as the source network for additional collections, because it provides the core node, circuit, and interface information used by other collectors.

Before you begin

- Complete the steps mentioned in Workflow: Preconfiguration Steps.

Follow these steps to configure the IGP database collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections or Edit Collections.

Step 2 Select **IGP database** from the **Basic topology** section and click **Next**.

Step 3 On the Configure page, under the **Seed router** section, enter the following configuration parameters:

- **Index**—Index number for the seed router.
- **Router IP**—Management IP address of the seed router.
- **Protocol type**—Select the IGP protocol that is running on the network. The options are: ospf, ospfv3, isis, and isisv6.

  If you choose either **ospf** or **ospfv3** as the Protocol type, enter the value for **OSPF area** in the Advanced page (click ⚙). The OSPF area option specifies the area ID or all. The default is area 0.

  If you choose either **isis** or **isisv6** as the Protocol type, enter the value for **ISIS level** (1, 2, or BOTH) in the Advanced page (click ⚙).

- **Collect interfaces**—Check this check box to discover full network topology. By default, this option is enabled.

Step 4 (Optional) To add more seed routers, click **+ Add router** and repeat Step 3 for each seed router. Ensure that the index number is unique for each seed router.

Step 5 (Optional) To exclude or include individual QoS information from the nodes, under **Advanced settings** > **QoS Node Filter** section, click **+ Add node filter** and enter the values as required.

Step 6 (Optional) Expand the **Advanced settings** panel and enter the details in the relevant fields. For descriptions of these advanced options, see IGP and SR-PCE Collection Advanced Options, on page 7.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

What to do next

- Configure schedules for the collection job. You can schedule the collection job to run immediately or schedule it to run at specific intervals. For details, see Schedule Collections.
- Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit Collections.

Collect Topology Information Using the SR-PCE Collector

Note In Cisco Crosswork Planning, there are two topology collectors: IGP database and SR-PCE. In a single collection, you can choose any one of these collectors for collecting information related to topology. Selecting both collectors is not permitted.

To use the IGP database collector for topology collection, see Collect Topology Information Using the IGP Database Collector, on page 4.

The **SR-PCE** collector discovers Layer 3 topology using SR-PCE. An SR-PCE agent is a Cisco Crosswork Planning component which will connect to SR-PCE server and process the telemetry data sent by server. SR-PCE agent uses two different REST connections with SR-PCE, one for LSP and the other for Topology data collection. After topology and LSP data collection, SR-PCE agent will (optionally) subscribe to SR-PCE and listen to further network change events.

Node and interface/port properties are discovered using SNMP. For testing purposes, you can also use the SR-PCE topology discovery using SR-PCE only (the Extended discovery field disabled) when no SNMP access is available. The network model resulting from topology discovery is used as the source network for additional collections, because it provides the core node, circuit, and interface information used by other collectors.

The SR-PCE collector also captures network updates for any changes in IGP Metric, Delay, and Node Overload.

It populates the FlexAlgoAffinities, FlexAlgorithms, SRv6NodeSIDs, SRv6InterfaceSIDs, NodePrefixLoopbacks, and NodeSIDPrefixLoopbacks tables. It does not populate the SRv6NodeSIDPrefixLoopbacks table as the loopback address associated with SRv6 is not obtained using SR-PCE. To populate the SRv6NodeSIDPrefixLoopbacks details, you must add an external script while configuring the collector. Otherwise, the cross-table filter from SRv6NodeSIDs to NodePrefixLoopbacks will not display any results in the Cisco Crosswork Planning Design application. For details on running the external scripts, see Run External Scripts Against a Network Model, on page 37.

Note

- The default ISIS level is set to level2 for NodePrefixLoopbacks. The same is also populated for an OSPF network.
- Cisco Crosswork Planning does not reflect the update of non-null to null value in the FlexAlgo columns. The values will start reflecting after a DARE re-sync.

The SR-PCE collector reads the LocalDomainIdentifier column of NetIntXtcLinks and populates the IGP Process ID in the Interfaces table.

Note

- Dual stack support (capability to handle both IPv4 and IPv6 simultaneously), and the configuration of OSPF or ISIS on an interface are populated correctly as part of data collection. However, during SR-PCE collection, when the dual protocol (OSPF and ISIS) is enabled on a single interface for data collection, dual stack and its interface resolution are not supported.
- The IPv4 metric value is populated in IGP metric table and the Ipv6 value is populated in IPv6-IGP metric table. The TE metric values will also be updated similarly.

Before you begin

- Complete the steps mentioned in Workflow: Preconfiguration Steps.
- An SR-PCE agent must be configured and running. For more information, see Configure Agents.

Follow these steps to configure the SR-PCE collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections or Edit Collections.

Step 2 Select **SR-PCE** from the **Basic topology** section and click **Next**.

Step 3 On the Configure page, enter the following configuration parameters:

- **SR-PCE host**—Choose an SR-PCE agent.
- **Backup SR-PCE host**—Choose a backup SR-PCE agent. You can enter the same SR-PCE agent if you do not have a backup.
- **ASN**—Enter 0 to collect information from all autonomous systems in the network, or enter the autonomous system number (ASN) to collect information only from a particular ASN. For example, if the SR-PCE agent has visibility to ASN 64010 and ASN 64020, enter 64020 to collect information only from ASN 64020.
- **IGP protocol**—Choose the IGP protocol that is running on the network.
- **Extend discovery**—Check the **Enabled** check box to discover the full network topology (nodes and interfaces).
- **Reactive network**—Check the **Enabled** check box to subscribe to notifications from SR-PCE to update the addition or deletion of nodes or links.
- **Trigger collection**—Check the **Enabled** check box to collect topology collection on new topology additions (nodes or links).

Step 4 (Optional) Expand the **Advanced settings** panel and enter the details in the relevant fields. For descriptions of these advanced options, see IGP and SR-PCE Collection Advanced Options, on page 7.

Step 5 Click **Next**.

Step 6 Preview the configuration and then click **Create** to create the collection.

What to do next

- Configure schedules for the collection job. You can schedule the collection job to run immediately or schedule it to run at specific intervals. For details, see Schedule Collections.
- Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit Collections.

IGP and SR-PCE Collection Advanced Options

You can configure several advanced options when using the IGP database and SR-PCE collectors.

Option	Description
Options applicable for both IGP and SR-PCE collection:	
Nodes	
Node performance collection	Collects node performance data, if enabled.
Remove node suffix	Removes node suffixes from node names if the node contains the specified suffix. For example, 'company.net' removes the domain name for the network.
QoS queues	Allows interfaces (configured with QoS in the router) to display QoS information.
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.
QoS node filter	Indicates the filter for determining the nodes for which the QoS data is obtained.
Interfaces	
Find parallel links	Finds parallel links that are not in the IGP database (when IS-IS TE extensions are not enabled).
IP guessing	Indicates the level of IP address guessing to perform for interfaces that are not present in the topology database. This is used when IS-IS TE extensions are not enabled.) • OFF—Performs no guessing. • Safe—Chooses guesses that have no ambiguity. • FULL—Makes best-guess decisions when there is ambiguity.
Port LAG discovery	Enables LAG discovery of port members.

Option	Description
LAG port match	Determines how to match local and remote ports in port circuits. • Guess—Creates port circuits to match as many ports as possible. • Exact—Matches based on LACP. • Complete—Matches based on LACP first, and then tries to match as many as possible. • None—Does not create port circuits.
Cleanup circuits	Removes circuits that do not have IP addresses associated to interfaces. Circuit removal is sometimes required with IS-IS databases to fix IS-IS advertising inconsistencies.
Copy description	Copies physical interface descriptions to logical interfaces if there is only one logical interface and its description is blank.
Physical ports	Collects L3 physical ports for Cisco.
Minimum IP guessing	Indicates the minimum IP guessing prefix length. All interfaces with equal or larger prefix lengths are considered.
Minimum prefix length	Indicates the minimum prefix length to allow when finding parallel links. All interfaces with equal or larger prefix lengths (but less than 32) are considered.
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.
Debug	
Verbosity	Indicates the log verbosity level. It refers to the degree of detail and information provided in log messages. The default is 30, and the valid range is 1 to 60.
Net recorder	Records SNMP messages. The options are: Off, Record, and Playback. The default is Off. • Record—The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback—The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off—No recording or playback is performed.
Option applicable only for SR-PCE collection:	
Single-ended eBGP discovery	Discovers eBGP links that only have a single link end (not common).

Collect LSP Information

The **LSP** collector collects the RSVP LSP information in the network using SNMP.

Before you begin

Complete the steps mentioned in Workflow: Preconfiguration Steps.

Follow these steps to configure the LSP collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections or Edit Collections.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **LSP** from the **Advanced modeling** section and click **Next**.

Step 4 On the Configure page, click **LSP** in the **Selected collectors** pane on the left.

Note
Ensure that the Basic topology parameters are updated as per your needs. Update the parameters, if required.

Step 5 Enter the following configuration parameters:

- **Source**—Choose the source collector whose output serves as the input for this collector.
- **Get FRR LSPs**—Check the **Enabled** check box to discover Multiprotocol Label Switching (MPLS) Fast Reroute (FRR) LSP (backup and bypass) information.

Step 6 (Optional) Expand the **Advanced settings** panel and enter the details in the relevant fields. For descriptions of these advanced options, see LSP Collection Advanced Options, on page 9.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

What to do next

- Configure schedules for the collection job. You can schedule the collection job to run immediately or schedule it to run at specific intervals. For details, see Schedule Collections.
- Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit Collections.

LSP Collection Advanced Options

You can configure several advanced options when using the LSP collector.

Option	Description
Use calculated hops	Uses the calculated path hops table instead of the actual path hops table when discovering path hops.
Find actual path	Discovers actual paths for the LSPs.
Get extras	Collects additional LSP properties.
Use signaled name	Uses the LSP tunnel signaled name instead of LSP tunnel name (IOS-XR).
Auto bandwidth	Discovers auto bandwidth.
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.
Debug	
Verbosity	Indicates the log verbosity level. It refers to the degree of detail and information provided in log messages. The default is 30, and the valid range is 1 to 60.
Net recorder	Records SNMP messages. The options are: Off, Record, and Playback. The default is Off. • Record—The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback—The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off—No recording or playback is performed.

Collect PCEP LSP Information Using SR-PCE

The **PCEP LSP** collector uses the data collected from the SR-PCE collector and appends LSP information, thus creating a new network model.

Before you begin

- Complete the steps mentioned in Workflow: Preconfiguration Steps.
- Confirm that BGP-LS topology collection using SR-PCE (SR-PCE collector) has been completed for a network. You will need to use this model as the source network for collecting LSPs. For more information, see Collect Topology Information Using the SR-PCE Collector, on page 5.

Follow these steps to configure the PCEP LSP collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections or Edit Collections.

Step 2 Select **SR-PCE** from the **Basic topology** section.

Step 3 Select **PCEP LSP** from the **Advanced modeling** section and click **Next**.

Step 4 On the Configure page, click **PCEP LSP** in the **Selected collectors** pane on the left.

Note
Ensure that the Basic topology parameters are updated as per your needs. Update the parameters, if required.

Step 5 Enter the following configuration parameters:

- **Source**—Choose the source collector whose output serves as the input for this collector.
- **Agents**—Choose the relevant SR-PCE agents from the drop-down list. For information on creating agents, see Configure Agents.
- **Reactive network**—Check the **Enabled** check box to subscribe to notifications from SR-PCE to update LSPs based on addition or deletion. This option is enabled by default.

Step 6 (Optional) Expand the **Advanced settings** panel and enter the following information:

- **RSVP use signaled name**—Check the **Enabled** check box to use the RSVP LSP tunnel signaled-name instead of LSP tunnel name (IOS-XR).
- **SR use signaled name**—Check the **Enabled** check box to use the SR LSP tunnel signaled-name instead of LSP tunnel name (IOS-XR).
- **SR add index**—Check the **Enabled** check box to add indexes to SR LSP tunnels from associated interfaces (IOS-XR).
- **Data collection timeout**—Enter the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

What to do next

- Configure schedules for the collection job. You can schedule the collection job to run immediately or schedule it to run at specific intervals. For details, see Schedule Collections.
- Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit Collections.

Collect Multicast Flow Data from a Network

The **Multicast** collector collects multicast flow data from a given network. It is a collection of the following collectors:

- **Login find multicast**—Log in to the router to fetch or parse multicast flow data.
- **Login poll multicast**—Log in to the router to get multicast traffic rate
- **SNMP find multicast**—Collect multicast data for multicast flows using SNMP.
- **SNMP poll multicast**—Collect traffic data rate for multicast flows using SNMP.

Before you begin

Complete the steps mentioned in Workflow: Preconfiguration Steps.

Follow these steps to configure the Multicast collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections or Edit Collections.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **Multicast** from the **Traffic and Demands** section and click **Next**.

Step 4 On the Configure page, click **Multicast** in the **Selected collectors** pane on the left.

Note
Ensure that the Basic topology parameters are updated as per your needs. Update the parameters, if required.

Step 5 Enter the following configuration parameters:

- **Source**—Choose the source collector whose output serves as the input for this collector.
- **Data collection source**—Choose the collector using which you want to collect the multicast data. The options are: Login find multicast, Login poll multicast, SNMP find multicast, and SNMP poll multicast.

Step 6 (Optional) Expand the ***Collector* settings** panel and enter the details in the relevant fields. Based on the collectors that you selected in the previous step, the options differ. For descriptions of these advanced options, see Multicast Collection Advanced Options, on page 13.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

What to do next

- Configure schedules for the collection job. You can schedule the collection job to run immediately or schedule it to run at specific intervals. For details, see Schedule Collections.

- Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit Collections.

Multicast Collection Advanced Options

You can configure several advanced options when using the Multicast collectors.

Option	Description
Login find multicast settings	
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 30 minutes.
Use existing config	Uses existing collected multicast configurations from cache.
Force config update	Updates multicast configuration files even if they exist in the data directory.
Save configs	Specifies whether the multicast configurations are to be saved in the cache or discarded.
Overwrite files	Specifies if the existing files are to be overwritten.
Login poll multicast settings	
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 30 minutes.
No of samples	Indicates the number of samples that will be taken.
Polling interval	Indicates the time delay between the login rate readings (in seconds).
Traffic level name	Indicates the name of traffic level.
Traffic filtering	Specifies how to filter multicast traffic from multiple sources for each S|G group.
Use existing config	Uses existing collected multicast configurations from cache.
Force config update	Updates multicast configuration files even if they exist in the data directory.
Save configs	Specifies whether the multicast configurations are to be saved in the cache or discarded.
Overwrite files	Specifies if the existing files are to be overwritten.
SNMP find multicast settings	
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 30 minutes.

Option	Description
SNMP poll multicast settings	
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 30 minutes.
No of samples	Indicates the number of samples that will be taken.
Polling interval	Indicates the time delay between the login rate readings (in seconds).
Traffic level name	Indicates the name of traffic level.
Traffic filtering	Specifies how to filter multicast traffic from multiple sources for each S|G group.
Debug	
Verbosity	Indicates the log verbosity level. It refers to the degree of detail and information provided in log messages. The default is 30, and the valid range is 1 to 60.
Net recorder	Records SNMP messages. The options are: Off, Record, and Playback. The default is Off. • Record—The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback—The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off—No recording or playback is performed.

Discover BGP Topology

The **BGP** collector discovers BGP topology via SNMP and login. It uses a topology network (typically an IGP topology collector output) as its source network and adds BGP links to external ASN nodes.

Before you begin

Complete the steps mentioned in Workflow: Preconfiguration Steps.

Follow these steps to configure the BGP collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections or Edit Collections.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **BGP** from the **Advanced modeling** section and click **Next**.

Step 4 On the Configure page, click **BGP** in the Selected Collectors pane on the left.

Note
Ensure that the Basic topology parameters are updated as per your needs. Update the parameters, if required.

Step 5 From the **Source** drop-down list, choose the source collector whose output serves as the input for this collector.

Step 6 (Optional) Expand the **Advanced settings** panel and enter the details in the relevant fields. For descriptions of these advanced options, see BGP Topology Advanced Options, on page 15.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

What to do next

- Configure schedules for the collection job. You can schedule the collection job to run immediately or schedule it to run at specific intervals. For details, see Schedule Collections.
- Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit Collections.

BGP Topology Advanced Options

You can configure several advanced options when using the BGP collector.

Option	Description
ASN include	Allows you to enter the ASNs to include. By default, all ASNs are included.
Internal ASNs	Allows you to enter the internal ASNs.
Protocol	Specifies the Internet Protocol (IP) versions. The options are: IPv4 and IPv6.
Min IPv4 prefix length	Indicates the minimum prefix length to control how restrictive IPv4 subnet matching is in discovering interfaces as BGP links.
Min IPv6 prefix length	Indicates the minimum IPv6 prefix length to control how restrictive IPv6 subnet matching is in discovering interfaces as BGP links.
Login multi hop	Indicates whether to log in to routers that potentially contain multi-hop peers.
Force login platform	Overrides platform detection and uses the specified platform. Valid values: cisco, juniper, alu, huawei.
Fallback login platform	Indicates the fallback vendor in case platform detection fails. Valid values: cisco, juniper, alu, huawei.
Try send enable	Sends an enable password if the platform type is not detected when logging in to a router.
Telnet username prompt	Indicates the alternative custom username prompt.

Option	Description
Telnet password prompt	Indicates the alternative custom password prompt.
Find internal ASN links	Finds links between two or more internal ASNs. Normally this action is not required because IGP discovers these links.
Find non IP exit interface	Searches for exit interfaces that are not represented as next-hop IP addresses, but rather as interfaces (which are rare). **Note** This action increases the amount of SNMP requests for BGP discovery, which affects performance.
Internal exit interface	Discovers BGP links to internal ASNs.
Get MAC address	Collects source MAC addresses of BGP peers connected to an Internet Exchange public peering switch. This action is required only for MAC accounting.
Use DNS	Indicates whether to use DNS to resolve BGP IP addresses.
Force check all	Indicates whether to check all routers even if there is no indication of potential multi-hop peers. This action could be slow.
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.
Debug	
Verbosity	Indicates the log verbosity level. It refers to the degree of detail and information provided in log messages. The default is 30, and the valid range is 1 to 60.
Net recorder	Records SNMP messages. The options are: Off, Record, and Playback. The default is Off. • Record—The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback—The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off—No recording or playback is performed.

Option	Description
Login record mode	Records the discovery process. The options are: Off, Record, and Playback. The default is Off. • Record—The messages to and from the live network are recorded internally as the tool runs. It is used for debugging. • Playback—The recorded messages are played back through the tool as if they came from the live network, thus providing offline debugging of network collection. • Off—No recording or playback is performed.

Discover VPN Topology

The **VPN** collector discovers Layer 2 and Layer 3 VPN topology.



Note Currently, only P2P-VPWS xconnect discovery is supported for Layer 2 VPN.

Before you begin

Complete the steps mentioned in Workflow: Preconfiguration Steps.

Follow these steps to configure the VPN collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections or Edit Collections.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **VPN** from the **Advanced modeling** section and click **Next**.

Step 4 On the Configure page, click **VPN** in the **Selected collectors** pane on the left.

Note
Ensure that the Basic topology parameters are updated as per your needs. Update the parameters, if required.

Step 5 Enter the following configuration parameters:

- **Source**—Choose the source collector whose output serves as the input for this collector.
- **VPN type**—Choose at least one VPN type:
  - **VPWS**—Choose this type when Virtual Private Wire Service (VPWS) is being used in the network.
  - **L3VPN**—Choose this type when Layer 3 VPN is being used in the network.

Step 6 (Optional) Expand the **Advanced settings** panel and enter the following information:

- **Data collection timeout**—Maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.
- **Verbosity**—Log verbosity level. It refers to the degree of detail and information provided in log messages. The default is 30, and the valid range is 1 to 60.
- **Net recorder**—Records SNMP messages. The options are: Off, Record, and Playback. The default is Off. If set to 'Record', SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. If set to 'Playback', the recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

What to do next

- Configure schedules for the collection job. You can schedule the collection job to run immediately or schedule it to run at specific intervals. For details, see Schedule Collections.
- Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit Collections.

Collect Hardware Inventory Information

The Inventory collector collects hardware inventory information.

Collected Hardware

The **Inventory** collector creates a series of NetIntHardware* tables that store the collected hardware information based on hardware type. Each of the following objects are defined by node IP address and SNMP ID.

- NetIntHardwareChassis—Router chassis objects identified by node IP address and SNMP ID.
- NetIntHardwareContainer—Each entry represents a slot in a router (anything that can have a field replaceable unit (FRU) type device installed into it). Examples include chassis slots, module slots, and port slots.
- NetIntHardwareModule—Hardware devices that can be installed into other hardware devices. Generally, these devices directly support traffic such as line cards, modules, and route processors, and do not fall into one of the other function-specific hardware tables.
- NetIntHardwarePort—Physical ports on the router.

Hardware Hierarchy

The hardware has a parent-child relationship based on where the object resides within the router. The chassis has no parent and is considered as the *root object*. Other than the chassis, each object has one parent and can have one or more child objects. Objects with no children are called *leaf objects*, such as ports and empty

containers. This hierarchy generally reflects how hardware objects are installed within other objects. For example, a module representing a line card might have a parent object that is a container representing a slot.

The parent is identifiable in the NetIntHardware* tables by the ParentTable and ParentId columns. Using these two columns along with the Node (node IP address) column, you can find the parent object for any hardware object.

Example: This NetIntHardwareContainer entry identifies that container 172.23.123.456 has a chassis as a parent. In the NetIntHardwareChassis, there is an SnmpID entry that matches the container's ParentId of 2512347.

NetIntHardwareContainer							
Node	SnmpID	ParentID	Model	Name	NumChildren	ParentTable	SlotNumber
172.23.123.456	2503733	2512347		slot mau 0/0/0/5	0	NetIntHardwareChassis	0

Tracing the hierarchy from each leaf object to its corresponding root object based on the parent-child relationships results in a series of object types that form its hardware hierarchy. It is this trace that the Inventory collector uses to determine how to process the hardware devices. This is also the process you must use if adding an entry to the HWInventoryTemplates table.

Example: Chassis-Container-Module-Module-Container-Port

Tables for Processing Inventory

The Inventory collector constructs the NetIntNodeInventory table by processing the NetIntHardware* tables. The collector requires two configuration files and can additionally use an optional one.

- Template file (required)—This file contains these tables.
  - HWInventoryTemplates—Contains entries that categorize the devices in the final NetIntNodeInventory table, as well as prune from inclusion.
  - HWNameFormatRules—Contains entries that format the hardware object names to make them more usable, as well as correct unexpected SNMP results.
- Exclude file (required)—Contains the ExcludeHWList table that prevents (blocked lists) hardware objects from being included in the final NetIntNodeInventory table. This can be useful when for excluding hardware that does not forward or carry traffic.
- Hardware spec file (optional)—Contains the HardwareSpec table that can be used to adjust collected data in terms of the number of slots in a specified device when the slots returned by SNMP is inaccurate.

If you modify the template or choose to exclude files, ensure these changes persist across software upgrades.

Configure Hardware Templates

The **Template file** option under the **Build inventory options** section calls a file containing both the HWInventoryTemplates and the HWNameFormatRules tables.

HWInventoryTemplates Table

The HWInventoryTemplates table tells the Inventory collector how to interpret hardware referenced by the NetIntHardware* tables. It enables the Inventory collector to categorize objects into common, vendor-neutral hardware types, such as chassis, linecards, and slots, as well as to remove hardware types that are not of interest.

Inventory hardware is categorized as a chassis, slot, line card, module slot, module, port slot, port, or transceiver. A container is categorized as either a slot, module slot, or port slot. A module is categorized as either a module or a line card. All other hardware objects are categorized by their same name. For instance, a chassis is categorized as a chassis.

The Inventory collector looks at the following columns of the HWInventoryTemplates table for matches in the NetIntHardware* tables in this order.

- DiscoveredHWHierarchy, Vendor, Model
- DiscoveredHWHierarchy, Vendor, * (where * means all entries in the Model column)

You can further enhance the search using the **Guess template** option. In this instance, if no matches are found using the first two criteria, Cisco Crosswork Planning collector then looks for matches only for DiscoveredHWHierarchy and Vendor, and does not consider Model.

If a match is found, the subsequent columns after DiscoveredHWHierarchy tell the Inventory collector how to categorize the hardware. These latter columns identify hardware object types: chassis, slot, line card, module slot, module, port slot, port, or transceiver. Each column entry has the *Type,Identifier,Name* format.

- Type is the discovered hardware type, such as “container.”
- Identifier specifies which object (of one or more of the same type) in the hierarchy is referenced (0, 1, ...).
- Name specifies a column heading in the NetIntHardware* table. This is the name that appears in for that object in the NetIntNodeInventory table.

Example: Module,0,Model. "Model" is a column heading in the NetIntHardwareModule table)

Multiple name source columns can be specified with a colon.

Example: Container,0,Model:Name

If a hardware category does not exist or is empty, the Inventory collector does not include it in the final NetIntNodeInventory table.

Example:

Using the first row of the default Template file, the Cisco Crosswork Planning collector searches the NetIntHardware* tables for ones that have entries that match the Vendor, Model, and DiscoveredHWHierarchy columns as Cisco ASR9K Chassis-Container-Module-Port-Container-Module.

Thereafter, it categorizes each entry in the hardware hierarchy (DiscoveredHWHierarchy column), and defines its location in the hardware types columns.

The first Module entry is defined as a line card, it is identified as #0, and the name that appears in the NetIntNodeInventory table is the one appearing in the Model column of the NetIntHardwareModule table. The second module is defined as a transceiver object and is identified as #1. It uses the same name format.

Notice that there are two containers in the hierarchy, but there is only one defined as a Type. This means that the second container would not appear in the NetIntNodeInventory table.

Add HWInventoryTemplates Entries

If the Cisco Crosswork Planning collector encounters an inventory device that is not in the HWInventoryTemplates table, it generates a warning that specifies pieces of the hardware hierarchy, including the SNMP ID of the leaf object and the IP address of the router. You can use this information to manually

trace the objects from the leaf to the root and derive an appropriate entry in the HWInventoryTemplates table. For information on tracing hardware hierarchies, see Hardware Hierarchy.

1. Copy the warning message for reference, and use it for Step 2.
2. Using the router's IP address, as well as the SNMP ID, name, and model of the leaf object, find the leaf object referenced in the warning in either the NetIntHardwarePort or the NetIntHardwareContainer table.
3. Use the leaf object's ParentTable and ParentId columns to trace the leaf back to its parent. For each successive parent, use its ParentTable and ParentId columns until you reach the root object (chassis) in the NetIntHardwareChassis table.
4. Once each object in the hardware hierarchy is found, add it to the DiscoveredHWHierarchy column of the HWInventoryTemplates table. Complete the Vendor and Model columns.
5. For each object in the hardware hierarchy (DiscoveredHWHierarchy column), classify it into one of the standard hardware types, which are the columns listed after the DiscoveredHWHierarchy column.

HWNameFormatRules Table

The HWNameFormatRules table specifies how to format the names in the NetIntNodeInventory table. This is useful for converting long or meaningless names to ones that are easier to read and clearer for users to understand.

For each entry in the HWInventoryTemplates table, the HWNameFormatRules table is searched for a matching vendor, hardware type (HWType), name (PatternMatchExpression). Then, rather than using the name specified in the HWInventoryTemplates table, the NetIntNodeInventory table is updated with the name identified in the ReplacementExpression column.

If multiple matches apply, the first match found is used. Both the PatternMatchExpression and the ReplacementExpression can be defined as a literal string in single quotes or as a regular expression.

Example:

HWNameFormatRules			
Vendor	HWType	PatternMatchExpression	ReplacementExpression
Cisco	Chassis	\A4\Z	'7507'
Cisco	Linecard	800-20017-.*	'1X10GE-LR-SC'
Juniper	Chassis	Juniper (MX960) Internet Backbone Router	$1

The entries in the table work as follows:

- Replaces all Cisco chassis name with 7507 if the name has four characters where A is the beginning of the string and Z is the end of the string.
- Replaces all Cisco linecard names that match 800-20017-.* with 1X10GE-LR-SC.
- Replaces all Juniper chassis named "Juniper (MX960) Internet Backbone Router" with MX960.

Note SNMP returns many slot names as text, rather than integers. It is a best practice to remove all text from slot numbers for optimal use.

Exclude Hardware by Model or Name

The **Exclude file** option under the **Build inventory options** section option calls a file containing the ExcludeHWList table. This table enables you to identify hardware objects to exclude from the NetIntNodeInventory table based on model, name, or both. This is useful, for instance, when excluding management ports and route processors. The model and names can be specified using regular expressions or they can be literals.

Example:

ExcludeHWList			
HWTable	Vendor	Model	Name
NetIntHardwarePort	Cisco		\/CPU0\/129$
NetIntHardwareModule	Cisco	800-12308-02	
NetIntHardwarePort	Cisco		Mgmt

The entries in the table work as follows:

- Exclude all objects in the NetIntHardwarePort table where the vendor is Cisco and the name ends with CPU0/129.
- Exclude all objects in the NetIntHardwareModule table where the vendor is Cisco and the model is 800-12308-02.
- Exclude all objects in the NetIntHardwarePort table where the vendor is Cisco and the name is Mgmt.

HardwareSpec

The **Hardware spec file** option under the **Build inventory options** section calls a file containing the HardwareSpec table. This table enables you to adjust data returned from SNMP. You can adjust both the total number of slots (TotSlot) and the slot numbering range (SlotNum). For instance, SNMP might return 7 slots for a chassis when there are actually 9, including route processors.

This table looks only for hardware that contains slots, module slots, or port slots, and thus, the hardware type (HWType column) must be chassis, line card, or module. SlotNum indicates the slot number range. For instance, some routers start with slot 0, whereas others start with slot 1.

Example:

HardwareSpec				
Vendor	HWType	Model	TotSlot	SlotNum
Cisco	Chassis	7609	9	1-9

This table entry sets the Cisco 7609 chassis to have a total of 9 slots and to start the slot numbering with 9.

Configure Inventory Collection

Before you begin

Complete the steps mentioned in Workflow: Preconfiguration Steps.

Follow these steps to configure the Inventory collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections or Edit Collections.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **Inventory** from the **Traffic and Demands** section and click **Next**.

Step 4 On the Configure page, click **Inventory** in the **Selected collectors** pane on the left.

Note
Ensure that the Basic topology parameters are updated as per your needs. Update the parameters, if required.

Step 5 From the **Source** drop-down list, choose the source collector whose output serves as the input for this collector.

Step 6 (Optional) Expand the **Advanced settings** panel and enter the details in the relevant fields. For descriptions of these advanced options, see Inventory Collection Advanced Options, on page 23.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

What to do next

- Configure schedules for the collection job. You can schedule the collection job to run immediately or schedule it to run at specific intervals. For details, see Schedule Collections.
- Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit Collections.

Inventory Collection Advanced Options

You can configure several advanced options when using the Inventory collector.

Option	Description
Get inventory options	
Login allowed	Allows logging in to the router to collect inventory data.
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 30 minutes.
Build inventory options	
Exclude file	Indicates the file containing ExcludeHWList table that defines hardware characteristics to match against for exclusion in the output. Click the **Download sample file** link to download a sample file containing ExcludeHWList table.

Option	Description
Guess template	Indicates whether to broaden the search when processing raw inventory data.
Template file	Indicates the hardware template file containing HWInventory Templates and HWNameFormatRules tables. Click the **Download sample file** link to download a sample template file.
Hardware spec file	Indicates the file containing HardwareSpec table that defines slot counts for specific types of hardware to verify SNMP data returned from routers. Click the **Download sample file** link to download a sample file containing HardwareSpec table.
Debug	
Verbosity	Indicates the log verbosity level. It refers to the degree of detail and information provided in log messages. The default is 30, and the valid range is 1 to 60.
Net recorder	Records SNMP messages. The options are: Off, Record, and Playback. The default is Off. • Record—The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback—The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off—No recording or playback is performed.

Collect Port, LSP, SRLG, and VPN Information Using Configuration Parsing

Note The **Config parsing** collector is not a base topology collector. It must only be used to augment details missing from other methods of collection like SNMP and SR-PCE.

Before you begin

Complete the steps mentioned in Workflow: Preconfiguration Steps.

Follow these steps to configure the Config parsing collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections or Edit Collections.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **Config parsing** from the **Advanced modeling** section and click **Next**.

Step 4 On the Configure page, click **Config parsing** in the **Selected collectors** pane on the left.

Note
Ensure that the Basic topology parameters are updated as per your needs. Update the parameters, if required.

Step 5 From the **Source** drop-down list, choose the source collector whose output serves as the input for this collector.

Step 6 Expand the **Get config** and **Parse config** panels, and enter the details in the relevant fields. For field descriptions, see Configuration Parsing Advanced Options, on page 25.

Note

- L2VPN config parse is not supported.
- When L3VPN information is collected by Config Parsing collector, it is assumed that all VPNs are connected to each other.
- If the Config Parsing collector is collecting VPN information and VPN collector is also being run, make sure that VPN collector is before Config Parsing collector in the collector chain.
- Single ended SRLGs with other end missing will be collected via SR-PCE. SRLGSCircuits table is not updated for the same though.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

What to do next

- Configure schedules for the collection job. You can schedule the collection job to run immediately or schedule it to run at specific intervals. For details, see Schedule Collections.
- Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit Collections.

Configuration Parsing Advanced Options

You can configure several advanced options when using the Config parsing collector.

Option	Description
Get config options	

Option	Description
Collect configuration	Collects configuration from devices or routers.
Force login platform	Overrides platform detection and uses the specified platform. Valid values: cisco, juniper, alu, huawei.
Fallback login platform	Indicates the fallback vendor in case platform detection fails. Valid values: cisco, juniper, alu, huawei.
Try send enable	Sends an enable password if the platform type is not detected when logging in to a router.
Telnet username prompt	Indicates the alternative custom username prompt.
Telnet password prompt	Indicates the alternative custom password prompt.
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.
Parse config options	
Protocol type	Allows you to choose the IGP protocol running in the network. The options are: isis, ospf, and None. The default is **isis**.
ISIS level	Indicates the ISIS level to use. The agent can read IS-IS Level 1, Level 2, or both Level 1 and Level 2 metrics. If both are selected, the agent combines both levels into a single network. Level 2 metrics take precedence.
OSPF area	Indicates whether to collect a single OSPF area or all areas. This option specifies the area ID or all. The default is area 0.
ASN	Indicates the Autonomous System Number (ASN) to collect. ASN is ignored by default. However, for networks that span multiple BGP ASNs, use this option to read information from more than one IGP process ID or instance ID in an ASN.
Include objects	Allows you to select the configuration objects that you want to parse. The available options are: LAG, SRLG, RSVP, VPN, FRR, SR LSPS, LMP, and SR Policies.
Circuit match	Indicates the criteria to use to form circuits.
LAG port match	Determines how to match local and remote ports in port circuits. • Guess—Creates port circuits to match as many ports as possible. • None—Does not create port circuits.
OSPF process ID	Indicates the OSPF process ID to use when there are multiple OSPF processes.

Option	Description
IS-IS instance ID	Indicates the IS-IS instance ID to use when there are multiple IS-IS instances.
Loopback interface	Indicates the loopback interface number to use for the router IP.
Resolve references	Resolves IP address references, if enabled.
Multithreading	Indicates whether to use multithreading.
Filter showcommands	Filters multiple show commands.
Build topology	Builds network topology after parsing the configuration.
Shared media	Creates pseudonodes for shared media.
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.
Debug	
Verbosity	Indicates the log verbosity level. It refers to the degree of detail and information provided in log messages. The default is 30, and the valid range is 1 to 60.
Net recorder	Records SNMP messages. The options are: Off, Record, and Playback. The default is Off. • Record—The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback—The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off—No recording or playback is performed.

Improve Network Model Visualization

The **Layout** collector adds layout properties to a source network model to improve visualization when importing the plan file into Cisco Crosswork Planning. The collector automatically records changes to the layout properties. When the source network model changes, the layout of the destination model is updated.

The layout in the destination network serves as a template that is applied to the source network. The resulting network is saved as the new destination network. If the source layout contains no layout information, the layout from the destination network is simply added to the source network. If the source network contains layout information, that layout is maintained unless there is a conflict with the layout in the destination network. If a conflict exists, the layout information in the destination network takes precedence over the information in the source network.

Note The Layout collector saves only the node and site mappings. It does not save the node's coordinates.

Before you begin

Complete the steps mentioned in Workflow: Preconfiguration Steps.

Follow these steps to configure the Layout collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections or Edit Collections.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **Layout** from the **Traffic and Demands** section and click **Next**.

Step 4 On the Configure page, click **Layout** in the **Selected collectors** pane on the left.

Note
Ensure that the Basic topology parameters are updated as per your needs. Update the parameters, if required.

Step 5 Enter the following configuration parameters:

- **Source**—Choose the source collector whose output serves as the input for this collector.
- **Template file**—Enter the template plan file path from where the layout details are copied.

  Note
  If you are migrating the collector configuration either from Cisco WAE or from another Cisco Crosswork Planning instance, ensure that the **Template file** field is updated with the correct file after importing the collector configuration. This is necessary because, after importing the configuration, the server restores only the file name and not the actual file. If the field is not updated with the correct file, then the collection fails.

Step 6 (Optional) Expand the **Advanced settings** panel and enter the following information:

- **Timeout**—Maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

What to do next

- Configure schedules for the collection job. You can schedule the collection job to run immediately or schedule it to run at specific intervals. For details, see Schedule Collections.
- Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit Collections.

Collect Traffic Statistics

The **Traffic collection** collector collects traffic statistics (interface traffic, LSP traffic, MAC traffic, and VPN traffic) using SNMP polling. After configuring the **Traffic collection** collector, you can view the traffic poller agent details in the **Collector** > **Agents** page. The agent's name is the same as that of the collection.

Note During the initial traffic collection run, the traffic data is not populated in the plan file due to insufficient data to compute traffic details. Starting from the second or third run, depending on the schedule duration and the configuration of the minimum and maximum window lengths, traffic data begins to populate in the plan file.

Before you begin

- Complete the steps mentioned in Workflow: Preconfiguration Steps.
- If collecting VPN traffic, a VPN network model must exist. See Discover VPN Topology, on page 17.
- If collecting LSP traffic, an LSP network model must exist. See Collect LSP Information, on page 9.

Follow these steps to configure the Traffic collection collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections or Edit Collections.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **Traffic collection** from the **Traffic and Demands** section and click **Next**.

Step 4 On the Configure page, click **Traffic collection** in the **Selected collectors** pane on the left.

Note
Ensure that the Basic topology parameters are updated as per your needs. Update the parameters, if required.

Step 5 Check the **Traffic collection** check box to enable the traffic poller.

Step 6 From the **Source** drop-down list, choose the source collector whose output serves as the input for this collector.

Step 7 To run continuous traffic collection for interfaces, enable **Interface traffic poll** and then enter the following:

- **Polling period**—Enter the polling period, in seconds. We recommend starting with 60 seconds.
- **QoS**—Check the **Enable** check box if you want to enable queues traffic collection.
- **VPN**—Check the **Enable** check box if you want to enable VPN traffic collection. If enabled, confirm that the source network model has VPNs enabled.

Step 8 To run continuous traffic collection for LSPs, enable **LSP traffic poll** and then enter the following:

- **Polling period**—Enter the polling period, in seconds. We recommend starting with 60 seconds.

Note
If **LSP traffic poll** is enabled, make sure that the source network model has all the LSP details.

Step 9 To run continuous traffic collection for MAC accounting, enable **MAC traffic poll** and then enter the following:

- **Polling period**—Enter the polling period, in seconds. We recommend starting with 60 seconds.

Note
If **MAC traffic poll** is enabled, make sure that the source network model has MAC addresses.

Step 10 (Optional) Expand the **SNMP traffic computation** panel and enter the details in the relevant fields. For field descriptions, see Traffic Collection Advanced Options, on page 30.

Step 11 Click **Next**.

Step 12 Preview the configuration and then click **Create** to create the collection.

You need to configure a schedule to populate the collected traffic data in the plan files. The traffic details are updated in the plan files only on running the scheduled jobs. If a job is not executed, the traffic data is not updated in the plan files.

What to do next

- Configure schedules for the collection job. You can schedule the collection job to run immediately or schedule it to run at specific intervals. For details, see Schedule Collections.
- Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit Collections.

Traffic Collection Advanced Options

You can configure several advanced options when using Traffic collection.

Option	Description
Minimum window length	Indicates the minimum window length for traffic calculation, in seconds. The default is 300 seconds.
Maximum window length	Indicates the maximum window length for traffic calculation, in seconds. The default is 450 seconds.
Raw counter TTL	Indicates how long to keep raw counters (in minutes). The default is 15 minutes.
Discard over capacity	Discards traffic rates that are higher than capacity.
Net recorder file max size	Indicates the maximum size for the net record file.
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.
Debug	

Option	Description
Verbosity	Indicates the log verbosity level. It refers to the degree of detail and information provided in log messages. The default is 30, and the valid range is 1 to 60.
Net recorder	Records SNMP messages. The options are: Off, Record, and Playback. The default is Off. • Record—The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback—The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off—No recording or playback is performed.

Tuning traffic polling

Traffic poller collects raw traffic counters from the network. Collection time depends on network size, network latency, and response time from individual nodes.

To run traffic polling efficiently, do the following:

1. Set the traffic poller verbosity to 40 in the **Traffic collection** configuration page.
2. Start with the default options and run continuous collection for several hours. The default values are:

   ```
   Interface traffic poll > Polling period = 60
   LSP traffic poll > Polling period = 60
   Minimum window length = 300
   Maximum window length = 450
   Raw counter TTL = 15
   ```

3. Configure the Traffic collection scheduler to run every 300 seconds.
4. Download the `continuous_poller_out.log` file using the showtech option.
   a. From the main menu, choose **Administration** > **Crosswork Manager** > **Crosswork Health** > **Collector**.
   b. Click the **Microservices** tab.
   c. Click ••• for the **collection-service** and choose **Request logs**.
   d. Download the resulting tar file to view the log file.
5. Search for actual collection times. For example:

   ```
   Info [40]: LSP Traffic Poller: Collection complete. Duration: 43.3 sec
   Info [40]: Interface Traffic Poller: Collection complete. Duration: 42.7 sec
   ```

   The fastest pace at which the poller can poll network in the example above is around 40-50 secs. This is the minimum value for `Interface traffic poll > Polling period` and `LSP traffic poll > Polling period`. Since traffic poller populates traffic for both interfaces and LSPs at the same time, it is recommended to set both values to the same value.

Traffic Poller calculates traffic by collecting raw traffic counters c1, c2, ..., cn. It requires at least two counters to calculate traffic.

```
(c2.counter - c1.counter)/(c2.timestamp - c1.timestamp)
```

Note the following:

- A sliding window namely `Minimum window length` is used to sample two counters. It looks for two counters which are farthest apart, that is, latest and earliest for a specified period. The average traffic is calculated for this period. Since the poller requires at least two counters, the smallest value for `Minimum window length` is 2 * `polling period`. To accommodate for variations, add 25% or more.

  In case `Minimum window length` fails to find counters for the specified period due to increased network latency or node response time, it will report traffic as `N/A`. To avoid empty traffic, there is an insurance window, namely `Maximum window length` which has a minimum value equal to 2 * `polling period`. To accommodate for longer polling period, add 50% or more. For unresponsive nodes, add 100% or more.

- Traffic poller stores raw counters in memory for traffic calculation. This takes up RAM space. Once in a while traffic poller cleans up old counters stored in memory. Anything older than `Raw counter TTL` (mins) is cleaned up. Therefore, given above constraints, minimum value for `Raw counter TTL` is `Maximum window length` or more.

- Traffic population in traffic poller is the process of calculating traffic in the network and populating the plan file. The duration it takes depends on network size. The actual time it takes to populate traffic can be found in the `snmp-traffic-poller-service.log` file.

  For example:

  ```
  TrafficCalculatorRfs Did-52-Worker-46: - Traffic calculation took (ms) 379976
  TrafficCalculatorRfs Did-52-Worker-46: - Traffic calculation took (ms) 391953
  TrafficCalculatorRfs Did-52-Worker-46: - Traffic calculation took (ms) 388853
  ```

  In the above example, the fastest rate at which traffic can be populated (and consumed by other tools) is about 400 secs.

- Sometimes in the `snmp-traffic-poller-service.log` file, you can also see `Invalid counter` warnings to indicate that counter values do not make sense, for example, `c1.counter` is greater than `c2.counter` (which would result in negative traffic). This happens when counters reset or overflow. It is common for 32-bit counters. If there are a lot of them seen, increase the sliding window sizes to process more counters and reduce chances of failure.

- However, it is not recommended to poll network at a faster rate than populating traffic. In the example above, the most aggressive setting for traffic polling is 50 secs, but population takes around 400 secs. This amounts to 8 network polls which are wasted. Therefore, traffic polling period can be increased (along with sliding window sizes and `Raw counter TTL`).

  Here is the configuration recommended for the above network:

  1. Set the following values:

     ```
     Interface traffic poll > Polling period 180
     LSP traffic poll enabled
     LSP traffic poll > Polling period 180
     Minimum window length 400
     Maximum window length 800
     Raw counter TTL 15
     Data collection timeout 60
     ```

  2. Configure Traffic collection scheduler to run every 400 seconds.

Note Data collection timeout is adjusted to 60 mins for traffic population. This timeout is not used generally and should be just high enough.

Sample configuration above is the most aggressive in terms of traffic polling and population. These numbers can be adjusted to be less aggressive to save CPU resources and network bandwidth. For example:

1. Set the following values:

```
Interface traffic poll > Polling period 240
LSP traffic poll enabled
LSP traffic poll > Polling period 240
Minimum window length 600
Maximum window length 1200
Raw counter TTL 20
Data collection timeout 60
```

2. Configure Traffic collection scheduler to run every 600 seconds.

Collect Traffic Demands Information

The **Demand deduction** collector collects information regarding traffic demands from the network.

Before you begin

Complete the steps mentioned in Workflow: Preconfiguration Steps.

Follow these steps to configure the Demand deduction collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections or Edit Collections.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **Demand deduction** from the **Traffic and Demands** section and click **Next**.

Step 4 On the Configure page, click **Demand deduction** in the **Selected collectors** pane on the left.

Note
Ensure that the Basic topology parameters are updated as per your needs. Update the parameters, if required.

Step 5 From the **Source** drop-down list, choose the source collector whose output model serves as the input for this collector.

Step 6 Under **Demand mesh steps**, click **+ Add step** to add a step. In the **Add Mesh Step** window, enter the following details:

a) In the **Name** field, enter the name for the step.
b) In the **Step number** field, enter the order in which this step must be performed.
c) From the **Tool** drop-down list, choose the required tool. The available tools are: Demands for P2MP LSPs, Demand deduction, External executable script, Copy demands, Demands for LSPs, and Demand mesh creator.
d) Check the **Enable** check box to run the selected tools.

e) Update or enter the details in the **Tool configuration** section. Based on the tool you selected, the options differ in this section.
f) (Optional) Expand the **Advanced** panel and enter the details.
g) Click **Continue**.

Repeat this step to add more steps to the configuration.

To remove any of the steps added, select the step and click the **Delete** button in the Mesh Step window.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

What to do next

- Configure schedules for the collection job. You can schedule the collection job to run immediately or schedule it to run at specific intervals. For details, see Schedule Collections.
- Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit Collections.

NetFlow Data Collection

Cisco Crosswork Planning can collect and aggregate exported NetFlow and related flow measurements. These measurements can be used to construct accurate demand traffic data for Cisco Crosswork Planning Design. Flow collection provides an alternative to the estimation of demand traffic from interfaces, LSPs, and other statistics using Demand deduction. NetFlow gathers information about the traffic flow and helps to build traffic and demand matrix. Importing flow measurements is particularly useful when there is full or nearly full flow coverage of a network's edge routers. Additionally, it is beneficial when accuracy of individual demands between external autonomous systems (ASes) is of interest.

Network data collected separately by collectors, including topology, BGP neighbors, and interface statistics, is combined with the flow measurements to scale flows and provide a complete demand mesh between both external autonomous systems and internal nodes.



Note If the NetFlow collector is part of multiple collections, you cannot execute those collections at the same time. Each collection must be run individually, as the NetFlow collector does not support simultaneous execution of collections.

Cisco Crosswork Planning gathers the following types of data to build a network model with flows and their traffic measurements aggregated over time:

- Flow traffic using NetFlow, JFlow, CFlowd, IPFIX, and Netstream flows
- Interface traffic and BGP peers over SNMP
- BGP path attributes over peering sessions

NetFlow Collection Configuration

The flow collection process supports IPv4 and IPv6 flows captured and exported by routers in the ingress direction. It also supports IPv4 and IPv6 iBGP peering.

Routers must be configured to export flows to and establish BGP peering with the flow collection server. Note the following recommendations:

- NetFlow v5, v9, and IPFIX datagram export to the UDP port number of the flow collection server, which has a default setting of 2100. Export of IPv6 flows requires NetFlow v9 or IPFIX.
- Define a BGP session on the routers configured as iBGP Route Reflector Client for the flow collector server. If configuring this in the router itself is not feasible, then a BGP Route Reflector Server with a complete view of all relevant routing tables can be used instead.
- Configure the source IPv4 address of flow export datagrams to be the same as the source IPv4 address of iBGP messages if they are in the same network address space.
- Explicitly configure the BGP router ID.
- If receiving BGP routes, the maximum length of the BGP `AS path` attribute is limited to three hops. The reason is to prevent excessive server memory consumption, considering that the total length of BGP attributes, including `AS path`, attached to a single IP prefix can be very large (up to 64 KB).

Configure the NetFlow Collection

Before you begin

- Complete the steps mentioned in Workflow: Preconfiguration Steps.
- Configure NetFlow agents to operate in single mode.

Follow these steps to configure the NetFlow collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections or Edit Collections.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **NetFlow** from the **Traffic and Demands** section and click **Next**.

Step 4 On the Configure page, click **NetFlow** in the **Selected collectors** pane on the left.

Note
Ensure that the Basic topology parameters are updated as per your needs. Update the parameters, if required.

Step 5 Enter the following configuration parameters:

- **Source**—Choose the source collector whose output serves as the input for this collector.
- **Agents**—Select the applicable agents from the drop-down list.

Step 6 Under the **Common config** section, from the **Split AS flows on ingress** drop-down list, select the traffic aggregation strategy for external ASNs.

(Optional) Enter the information in the other fields. For field descriptions, see NetFlow Collection Advanced Options, on page 36.

Step 7 (Optional) Expand the **IAS flows** and **Demands** panels, and enter the details in the relevant fields. For descriptions of these options, see NetFlow Collection Advanced Options, on page 36.

Step 8 Click **Next**.

Step 9 Preview the configuration and then click **Create** to create the collection.

What to do next

- Configure schedules for the collection job. You can schedule the collection job to run immediately or schedule it to run at specific intervals. For details, see Schedule Collections.
- Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit Collections.

NetFlow Collection Advanced Options

You can configure several advanced options when using the NetFlow collector.

Option	Description
Common config settings	
Split AS flows on ingress	Indicates the traffic aggregation strategy for external ASNs.
ASN	Indicates the ASN of the internal AS in the network.
Address family	Indicates the protocol version to include in IAS flows and demands computation.
Ext node tags	Allows you to enter one or more node tags. Click + to enter a list of one or more node tags.
Split AS flows on egress	Splits Inter AS flows on egress through all the interfaces connecting to the egress AS.
Extra aggregation	Allows you to select the list of aggregation keys from the drop-down list.
Log level	Indicates the log level of the tool. The options are: Off, Fatal, Error, Warn, Notice, Info, Debug, and Trace.
Number of threads	Indicates the maximum number of threads to be used in parallel computation.
IAS flows settings	
Trim inter AS flows	Indicates the value in MBits/sec below which the Inter AS flows for traffic is strictly discarded.

Option	Description
Match BGP external info	Indicates whether to match egress IP addresses in the BGP peer relation.
Ingress interface filter	Indicates a filter of node and interface in the form Node:InterfaceName that will be applied while reading the flow matrix to filter in only those ingress interfaces.
Egress interface filter	Indicates a filter of node and interface in the form Node:InterfaceName that will be applied while reading the flow matrix to filter in only those egress interfaces.
Back track micro flows	Indicates whether to generate files showing a relationship between micro flows from the input file and those demands or inter-as-flows that aggregate them.
Flow import IDs	Allows you to enter comma separated flow IDs to import data from.
IAS computation timeout	Indicates the timeout for IAS flows computation (in minutes). The valid range is 1-1440. The default is 60 minutes.
Demands settings	
Demand name	Indicates the name for any new demands.
Demand tag	Indicates the tag for any new demands, or to append to the existing demands.
Trim demands	Indicates the value in MBits/sec below which the demands are strictly discarded.
Demand service class	Indicates the demand service class.
Demand traffic level	Indicates the demand traffic level.
Missing flows	Indicates the path where the file with interfaces that are missing flows is generated.

Run External Scripts Against a Network Model

The external scripts let you run a customized script against a selected network model. You might want to do this when you want specific data from your network that existing Cisco Crosswork Planning collectors do not provide. In this case, you take an existing collection model created in Cisco Crosswork Planning and append information from a custom script to create a final network model that contains the data you want.



Note If you are using a script from Cisco WAE and intend to use it within Cisco Crosswork Planning, it may not function as expected without modifications. This is due to architectural differences between Cisco WAE and Cisco Crosswork Planning, including variations in how the files are referenced. You must adjust the script appropriately for use in Cisco Crosswork Planning.

Before you begin

- Complete the steps mentioned in Workflow: Preconfiguration Steps.
- The custom script must be available.

Follow these steps to run external scripts against a network model.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections and Edit Collections.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 On the Configure page, click **+ Add external script** under the Advanced Modeling or Traffic and Demands section.

Step 4 Enter the following details:

- **Collector name**—Enter the name for this collection.
- **Is source a plan file?**—Check this check box if you want to run the script on a plan file. If you have selected this option, then enter the plan file details in the **Input plan file** field.
- **Source**—Select the collector on which you want to run the external script. For example, if you select BGP as the Source, then the custom script is executed on the BGP collector. The output model from the BGP collection is updated based on the specifications mentioned in the custom script.
- **Input file**—Upload any supporting file that is required for the custom script to execute successfully.
- **Executable script**—Enter the custom script details.
- **Script language**—Select the language of the custom script. The valid script languages are: PYTHON, SHELL, and PERL.
- **Aggregator properties**—If you want to specify any tables or columns to be aggregated, then specify them in a .properties file and upload the file using this field. By default, all columns and tables are aggregated.
- **Timeout**—Specify the action timeout. The default is 30 minutes.

Step 5 Click **Next**.

Step 6 Preview the configuration and then click **Create** to create the collection.

What to do next

Configure schedules for the collection job. You can schedule the collection job to run immediately or schedule it to run at specific intervals. For details, see Schedule Collections.

Merge AS Plan Files

The **Merge AS** tool helps to merge plan files from different Autonomous Systems (AS). The **Merge AS** tool resolves any conflicts across the plan files. Plan files in native format are also supported.

Each AS can be on a different Cisco Crosswork Planning server.

Note

- Only Autonomous Systems (AS), Circuits, Nodes, Interfaces, External Endpoints, External Endpoint Members with virtual nodes and unresolved interfaces are resolved.
- The following demands are resolved:
  - Source or Destination associated with virtual node that are resolved with real node.
  - Source or Destination associated with the interface in a specific format.
  - Source or Destination associated with the External Endpoints.
- The following demands are not resolved:
  - Source or Destination associated with ASN number only.
- For a given plan file, the internal AS number must match what other plan files see as an external AS number, and all the Autonomous Systems that are going to be merged need to be discovered in all the plan files.

Before you begin

- Collect topology and traffic information for different Autonomous Systems (AS).
- The plan files from different AS have to be present on the same Cisco Crosswork Planning server and the path to the plan files must be mentioned.
- Complete the steps mentioned in Workflow: Preconfiguration Steps.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections or Edit Collections.

Step 2 Click that the **Tools** radio button at the top.

Step 3 Select **Merge AS** from the **Tools** section and click **Next**.

Step 4 Enter the following configuration parameters:

- **Retain demands**—Check the **Enabled** check box to merge the demands.
- **Tag name**—Enter a tag name to help identify the updated rows in the .pln file. The tag column in the .pln file gets updated with the tag name for rows that are modified.

Step 5 Under the **Source collector** section, click **+ Add source collector**, and select the relevant Collection and Collector names.

Step 6 Under the **Source DB** section, click **+ Add source DB**, click **Browse**, and choose the source plan file located on your system.

Note
If you are migrating the configuration either from Cisco WAE or from another Cisco Crosswork Planning instance, ensure that the **DB file** field is updated with the correct file after importing the configuration. This is necessary because, after

importing the configuration, the server restores only the file name and not the actual file. If the field is not updated with the correct file, then the collection fails.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

What to do next

- Configure schedules for the collection job. You can schedule the collection job to run immediately or schedule it to run at specific intervals. For details, see Schedule Collections.
- Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit Collections.