Collecting Network Information

Collection Overview

The WAE collection process runs through a list of sequential tasks that discover network topology (including IGP, node, interface, LSP [SNMP], and PCEP information) and gather traffic statistics (or poll for traffic).

There are various methods in which to collect data (see Collection Methods). Regardless of the method used, the basic unit of data storage that is produced after the collection is called a plan file. Plan files contain network information at a specific time and are used by all WAE applications.

Since typical collection is done through a series of sequential tasks, you might want to have a few tasks performed asynchronously. You can configure WAE to enable continuous traffic polling and PCEP collection after the initial collection by using the WAE NI server. Configuring this feature is discussed in more detail in the following sections:

- Configure Continuous Polling and Collection in the WAE Collector UI
- Configure Continuous Polling and Collection Using Manual Collection

For more information on collection components (WAE Collector, WAE Network Interface, and the data topology workflow, see Data Flow After Collection.

Snapshot Files

Note

- Do not edit snapshot files if you are collecting network information using the WAE Collector UI.
- For snapshot file examples, see Appendix A, "Snapshot Examples."

The collection process uses configurations defined in snasphot files. The snapshot files consist of a .txt and an optional .inc file, and are located in the `$CARIDEN_HOME/etc` directory. Together, these files enable you to customize tasks that define how your network is discovered and modeled.

The `snapshot.txt` file contains *tasks* that are defined in the `snapshot.inc` file through a series of CLI tools. These tasks and their .inc definitions determine what network information is collected and how the network is modeled. The `snapshot.txt` file also defines environment variables called by the CLI tools in the in the `snapshot.inc` file, thus removing the need to manually update these variables more than one time if you reconfigure your network.

- Tasks in the `snapshot.txt` file are defined in the `snapshot.inc` file. These tasks are performed in the order in which they are sequentially listed in the `snapshot.txt` file.
- Variables `$(variable_name)` in the `snapshot.inc` files are defined in the <ENVIRONMENT> table of the `snapshot.txt` file.
- If there are multiple `snapshot.inc` files, they are executed in the order in which they are listed in the <ENVIRONMENT> table.
- If there are nested `snapshot.inc` files, they are executed in the order in which they are listed in the parent `snapshot.inc` file.

Typically, you need only to customize the `snapshot.txt` file, which contains all the steps needed to perform a typical network discovery. The default `snapshot.inc` file contains details of how each CLI tool is called to execute each task, and can often be left as is.

snapshot.txt

Note There are different types of snapshot.txt files; for example, snapshot_augment_collector.txt and snapshot_hardware_inventory.txt file. They all provide the same type of information and are generally referred to as snapshot.txt files throughout this document.

The `snapshot` tool reads the `snapshot.txt` configuration file to determine the following:

- The discovery environment, such as where to store the data, log files, and debug information (see Environment Variables).
- Which discovery tasks to perform.

Environment Variables

The <ENVIRONMENT> table defines numerous variables that are frequently called by tasks defined in the `snapshot.inc` file. By defining them here, you can avoid the repetition of entering them multiple times. The snapshot.txt file itself contains a description of each of these variables.

Snapshot environment variables apply to the snapshot process only, and are unrelated to host environment variables.

Example: Almost all the tasks call a `work_dir` variable to define the location in which to store the snapshot data.

- In the `snapshot.txt` <ENVIRONMENT> table, you could define the following:

```
home_dir /opt/cariden
work_dir /$(home_dir)/work
```

- In the `snapshot.inc` file, define that all tasks put their output in `$(work_dir)`.

Each parameter must be separated from its value by a TAB. At minimum, you must define the following variables in this table:

- `unique`
- `home_dir`
- `collector_url` (if getting a plan file from the Collector server or WAE Network Interface (NI) server)
- `seed_router` (manual collection only)
- `igp`

- Ensure `isis_level` or `ospf_area` is properly configured, depending on the `igp` setting

You can define your own environment variables for snapshot tasks that you create. However, if using the augmented method, you cannot create environment variables that use the same name as those that are applicable only to the manual collection method. To avoid this error, you could compare snapshot_augment_collector.txt to the `snapshot.txt` file to determine names you must avoid using.

snapshot.txt Tasks

The `snapshot` tool reads the `snapshot.txt` configuration file to determine which WAE Collector tasks to perform. The tasks are organized into four high-level tables, each of which contains a list of available tasks for the discovery process to perform.

snapshot.txt Task Type	Description
<DISCOVERY_TASKS>	Define what type of information to collect, such as IGP database, nodes, MPLS LSP paths, and more.
<POLLING_TASKS>	Define which traffic statistics polling functions to perform.
<FLOW_TASKS>	Define whether to collect NetFlow data and related flow measurements.
<ANALYSIS_TASKS>	• Simplify and arrange nodes and sites in the network plot. • Create and initialize a mesh of traffic demands.
<ARCHIVE_INSERT_TASKS>	Insert the completed plan into an existing archive repository.

Each default task is either enabled (no comment symbol [#]) or disabled (with a comment symbol). To enable a task, remove the comment. Conversely, to disable a task, add a comment to the beginning of its line.

Each task is customized and defined in the `snapshot.inc` file through a series of CLI tools. For information, see snapshot.inc. The `snapshot` tool executes the tasks in the order in which they are listed in the `snapshot.txt` file.

You can remove tasks, and you can add any task (with any name) provided you also reference and define it in the `snapshot.inc` file.

snapshot.inc

You can further customize the snapshot discovery process by adding one or more uniquely named `snapshot.inc` files to the <ENVIRONMENT> table in the `snapshot.txt` file. These `snapshot.inc` files define the behavior of each task that is called by the `snapshot.txt` file. Figure 2-1 shows an example.

- The order of the tasks defined in the `snapshot.txt` file is the order in which they are executed. The order of the task definitions in the `snapshot.inc` file does not matter.
- The `snapshot.inc` files are executed in the order in which they are listed in the <ENVIRONMENT> table.
- If there are nested `snapshot.inc` files, they are executed in the order in which they are listed in the parent `snapshot.inc` file.

The parameters used to call these tasks are listed in an individual task table (Table 2-1). The parameters used for the CLI tools within the tasks are listed in an associated options table (`<options-name>` in Table 2-2).

Within each table, references are made to variables defined in the `snapshot.txt` <ENVIRONMENT> table using the format `$(variable_name)`.

Some tasks can copy intermediate files to a debug folder by calling a `postcmd` after the main tool is called.

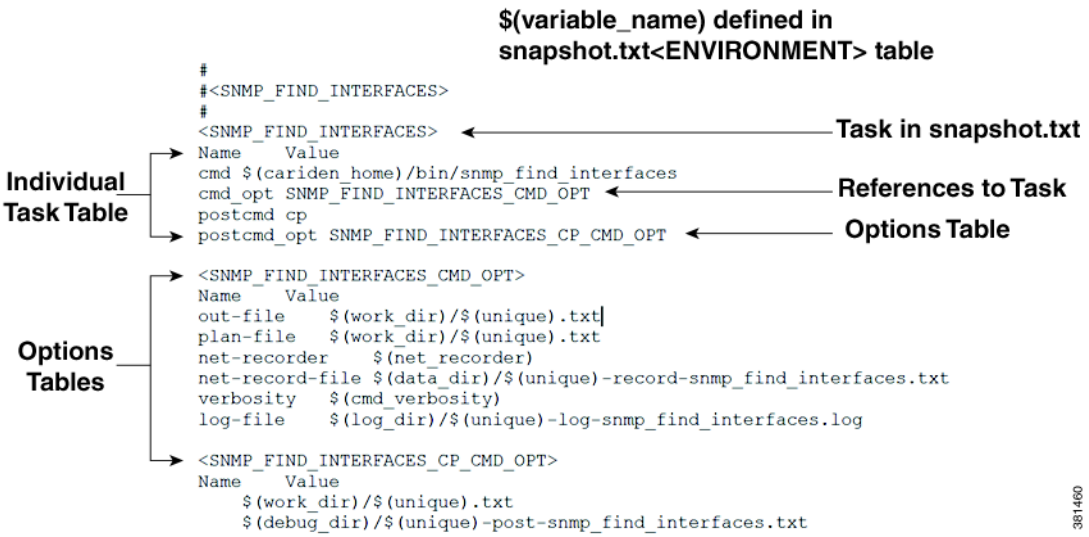
Table 2-1 Individual Task Table

Name	Value
cmd	Fully-qualified name and path of the CLI command to execute. You do not need to change this command during customization.
cmd_opt	Name of the table that defines the command options. You do not need to change the name of the table to change the command options. Instead, edit the contents of the options table by this name.
cmd_success	Determines what exit codes constitute a success for the command. The snapshot process terminates if the command is unsuccessful. 0 = successful, and 1 = unsuccessful
precmd	Fully-qualified name and path of a command to execute before the CLI command. For instance, it can be a task to prepare for the CLI command.
precmd_opt	Name of the table that defines the pre-command options. You can use any name, but its name must match the name of the table that defines the options.
postcmd	Fully-qualified name and path of a command to execute after the CLI command. The default is a Linux `cp` command that copies intermediate files to the debug directory (debug_dir).
postcmd_opt	Name of the table that defines the post-command options. You can use any name, but its name must match the name of the table that defines the options.

Table 2-2 Task Options Table

Name	Value
<option-name>	Value of the option. These are name-value pairs, and you can have as many entries as needed for the command. You can use environment variables to construct filenames. Example: $(work_dir)/$(unique).txt

Figure 2-1 Example Task Defined in snapshot.inc



Launch and Validate snapshot

The `snapshot` tool is located in the `$CARIDEN_HOME/bin` directory. To launch the snapshot tool, enter the following command:

```
snapshot -config-file $WAE_HOME/etc/snapshot.txt
```

You can launch `snapshot` manually or schedule it for periodic operation with a `cron` job. The usual process is to create a `$CARIDEN_ROOT/archives` directory and have the newly discovered plan files saved to it. If you run `snapshot` manually, the resulting plan is placed in the `$CARIDEN_ROOT/work` directory.

If you make changes to either of the snapshot files, we recommend that you initially run the snapshot with the `-dry-run` and `-verify-config` options.

A message of Success after running the tool means the snapshot process successfully executed the tasks identified in `snapshot.txt`. If this is your first time running snapshot, we recommend that you review files in the `$CARIDEN_ROOT/logs` directory for errors and warnings. If you find them, check the `$CARIDEN_ROOT/logs/debugs` directory to see if you can resolve them. You likely need to tweak the authentication, network access, or snapshot configuration file. Common errors include the following:

- Routers inaccessible due to authentication errors, such as incorrect communities.
- Routers not responding or returning incomplete data due to timeouts or other access errors.

When scheduling the `snapshot` tool to run repeatedly and storing plan files into an archive, it is useful to check periodically that the plan files are still valid. Following are a few ways to verify a plan file:

- Look for errors and warnings in the to the `$CARIDEN_ROOT/logs` directory; for example, using `grep`.
- Check the `$CARIDEN_ROOT/work` directory to verify the plan file was created.
- Open the plan file in the WAE Design GUI.

Interval Collections and Continuous Polling

Note For information on how to configure continuous collection and traffic polling, see:

- Configure Continuous Polling and Collection in the WAE Collector UI
- Configure Continuous Polling and Collection Using Manual Collection

Through the WAE Collector UI, you have the option to run collection based on intervals or to combine that with continuous polling.

- Interval collections—This method polls traffic twice during the collection window. The traffic statistics for those two time periods are averaged and added to the plan file as measured traffic. The amount of time for each polling interval is set using the Counter Polling Period field on the Continuous Poller page.
- Use continuous polling—This method polls the traffic continuously. The amount of time for each polling interval is set using the Counter Polling Period field on the What To Collect page. The time window over which the traffic rate is averaged is set in the Default Time Window field. The amount of traffic added is the average traffic for the specified time window at the moment when the plan file is generated.

  Example: Counter Polling Period is 60 seconds. Default Time Window is 15 minutes. Every 60 seconds traffic is polled and added to the plan file. The amount of traffic added is the average traffic for the last 15 minutes at the moment when the plan file is generated.

Collection Methods

There are three main collection methods:

- Basic Collection—Configure basic network collection using the WAE Collector UI. There is no need to edit the snapshot files. The snapshot files are automatically configured based on the entries you define in the WAE UI.

  Note If you edit the snapshot files manually and later decide to use the WAE Collector UI, any configurations made with the WAE Collector UI will overwrite the snapshot files.

- Augmented Collection—Configure basic network collection using the WAE Collector UI and then add more tasks and options using augmented snapshot files (snapshot_augment_collector.txt and snapshot_augment_collector.inc). This method retrieves a plan file for use in WAE Design and WAE Design Archive. Optionally, it enhances the plan file with additional collection, and enhances the plan file with modeling information, such as demands. Examples include parsing configurations for explicit LSP paths, collecting multicast traffic, and collecting flow traffic.

  Note If you only want to build a network model that includes the creation of demands after collection, copy a template plan file into a newly generated plan, and store the resulting plan file into an external plan file archive, then use the network Model Manager. For more information, see Chapter 3, “Viewing a Network Model.”

- Manual Collection—Configure collections using only the CLI. This method is used for advanced configurations that are not supported by the other collection methods. Examples include collection directly from configuration files, multi-networking collection, and collection from Alcatel-Lucent's 5620 Service Aware Manager (SAM) server.

See the following table to determine which collection method to use. Consider what it is you are trying to discover and what the application needs are.

Note The Augmented Collection column indicates features that are not supported if you run only Basic Collection using the WAE Collector UI. To enable these features, you must run Augmented Collection after Basic Collection is completed (see Collecting Information Using Augmented Collection).

Table 2-3 Collection by Configuration Method

	Basic Collection Using WAE UI[1]	Augmented Collection	Manual Collection
Uses SNMPv2c authentication	x		x
Uses SNMPv3 authentication	x		x
Directly discovers nodes using system IPv4 addresses	x		
Collects OSPF and IS-IS IPv4 topologies	x		x
Collects OSPF and IS-IS IPv6 topologies			x
Collects BGP LS topologies			x
Collects node properties	x		x
Collects interface properties, including TE extensions	x		x
Collects interface queues	x		x
Collects Segment Routing LSPs			x
Collects interface traffic based on egress shaping rate			x
Collects SRLGs		x	x
Discovers BGP peering	x		x
Continuously polls traffic statistics (requires the WAE NI server)	x		x
Continuously collects LSPs (requires the WAE NI server)	x		x
Collects basic RSVP LSP properties	x		x
Collects RSVP LSPs with multiple paths or named paths (EROs)		x	x
Collects LAG[2] ports	x		x
Collects RSVP LSP affinities			x
Collects Multicast		x	x
Collects VPNs	x (Layer 3 only)	x	x
Collects LDPs		x	x
Collects flow traffic		x	x
Collects topology from config files			x

Table 2-3 Collection by Configuration Method (continued)

	Basic Collection Using WAE UI[1]	Augmented Collection	Manual Collection
Collects Layer 1 and Layer 3 information			x
Can build network models after the collection process, including the creation of demands		x	x
Collects hardware inventory		x	x
Collects multiple networks			x
Collects from SAM server			x

1. This table does not include the advanced configuration options available in the Collector UI. Additionally, all collections are dependent on licenses and what you have configured for collection.
2. Vendors have different names for LAGs. For instance, Cisco IOS uses the term *EtherChannel* (port-channel interface), Cisco IOS XR uses the term *link bundling* (bundle-ether interface), and both Juniper and Alcatel-Lucent use the term *LAG*.

Plan Files

All WAE applications use plan files produced by WAE Collector. Plan files capture all relevant information about a network at a given time, and can include topology, traffic, routing, and related information. How and where plan files are created depends on the collection method and what is configured in the snapshot files.

- From the WAE Live UI, you specify where the application is to get its plan files: either from a server or from an external plan file archive that is used by the augmented and manual discovery methods.
- The WAE Design Archive UI uses the plan files that are stored in the external plan file archive.
- The WAE Design GUI can access plan files from either the plan file archive that is internal to WAE Live or from the external plan file archive simply by telling the GUI which remote server to access. The primary use for this application to access the plan file archives is to (1) create and update templates for use in WAE Live and WAE Design Archive, or (2) simulate traffic based on discovered data when designing and planning networks using WAE Design.

WAE Collector and Archives

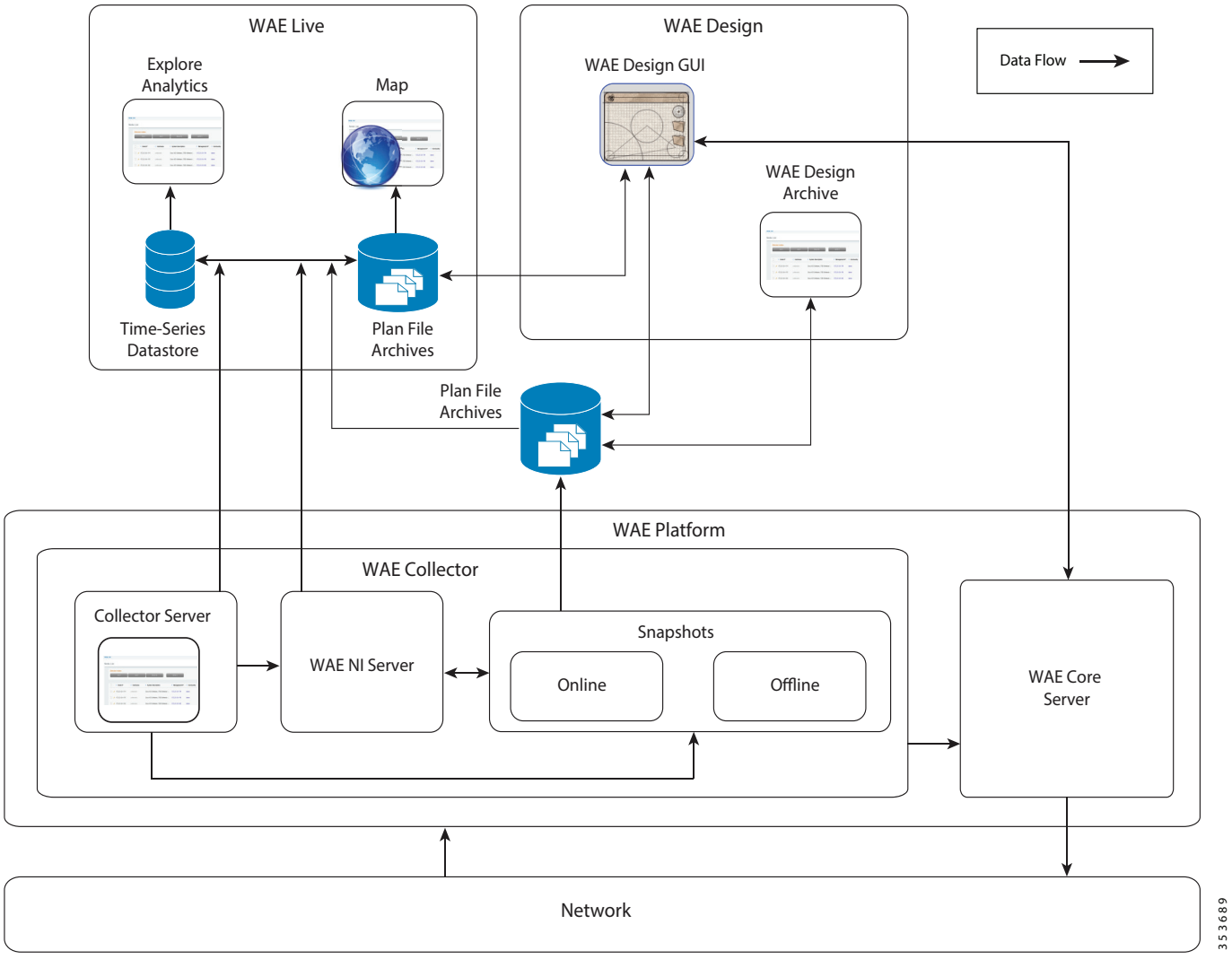
The first step is for WAE Collector to discover the network and create a plan file that represents your network.

- The Collector server, which is configured only through the WAE Collector UI, discovers the network at user-defined intervals to create and store the plan files on that server. The plan files reside on one of these servers until either WAE Live or a snapshot process requests them.
- If using the augmented method of discovery, the snapshot uses a plan file generated by the Collector server, and then adds other aspects of the network (such as Multicast). A common use case for augmented snapshots is to add modeling elements, such as demand meshes, and to perform demand deduction for use in applications. The resulting plan file is sent to an external plan file archive.
- If manually discovering the network, either through online or offline means, snapshots run at user-defined intervals and distribute the plan files to an external plan file archive repository. Optionally, you can configure the continuous polling of traffic statistics.
- WAE Collector sends updated plan files to the Network Modeler Module.

Note Optionally, you can configure the Collector server or a snapshot to push the plan file, as well as the access and authentication files, to the WAE NI server for the continuous polling of traffic statistics or for the continuous collection of LSPs. From a snapshot, you can also pull a plan file from the WAE NI server.

Table 2-3 shows how data flows between WAE Collector and the archives, and how data flows between the archives and the WAE applications. This diagram does not depict template flow, where *template* is a plan file containing the visual aspects that display the network in the application interfaces. For information on templates, see the *Cisco WAE Network Visualization Guide*.

Figure 2-2 Data Flow After Collection



Using Collections

You can use collections in the following ways:

- If using WAE Live, configure it to collect from the appropriate source and specify the Map archive location. For information, see the *Cisco WAE Live Administration Guide*.
- Use the WAE Design GUI to update a template for use by the applications. For information, refer to the *Cisco WAE Network Visualization Guide*.
- To verify the plan file collection has been set up correctly, open the plan file from the application you are using.

Collecting Basic Information Using the WAE Collector UI

Note Snapshot files are automatically configured using the WAE Collector UI. If you have previously performed a manual collection or edited the snapshot files, the configuration will not be applied. You will need to redo the configuration through the WAE Collector UI.

The WAE Collector UI enables you to configure the collection of basic network data for different networks. The Collector server handles router access and authentication, while enabling you to configure and schedule collection, and troubleshoot any issues. In many cases, the plan file produced can be used directly by WAE Live.

The WAE Collector UI predominantly uses the Collector server. You can also start the WAE NI server and thereafter connect to it through the WAE Collector UI. Then you can delegate traffic polling for objects and the continuous collection of LSPs to the WAE NI server.

Once the collection finishes, WAE Collector creates a plan file.

- If continuous polling is not running and if LSPs are not being continuously collected, the plan file is generated based on the completion of a collection as configured from the Schedule page. To retrieve the plan file, access it from the Collector server.
- If continuous polling is running or if LSPs are being continuously collected, the plan file is generated on demand, such as when the WAE Live application requests it. Additionally, the WAE NI server caches the plan file at regular intervals. To retrieve the plan file, access it from the WAE NI server.

New nodes are added when they are discovered. Nodes that are removed from the network (manually or through failure) are set to inactive. This inactive state is kept for a user-configurable time, after which the nodes are removed from the collection.

Workflow for Collecting Basic Information Using the WAE Collector UI

The initial workflow consists of the following steps. You can return to any of these steps at any time to change the configurations.

If you have not yet configured a node list used for collection or if you restarted WAE Collector, a setup wizard is available to lead you to the required Setup pages.

Note You are notified if another user is accessing the WAE Collector UI when you log in. Note that any changes you make will affect the other user's configuration, and vice versa.

Table 2-4 WAE Collector UI Collection Configuration Workflow

Step	Task	Description
1	Configure Node Discovery	Define how nodes are discovered and configure global default device SNMP community and login credentials.
2	Configure Node Access	Define the management IPs.
3	Configure Additional Node Access Profiles	(Optional) Configure and apply additional node access profiles. For example, apply a node access profile for nodes depending on vendor or model.
4	Configure Node Inclusion	(Optional) Set global rules for including and excluding nodes from being collected.
5	View and Manage the Node List	View and create override rules for specific nodes to which the global default credentials do not apply. You can also exclude nodes and apply profiles here.
6	Configure What to Collect	Configure which objects and traffic to collect, and set the counter polling period.
7	Configure Continuous Polling and Collection in the WAE Collector UI	Configure continuous traffic polling and collection using the WAE Network Interface server.
8	Schedule the Collection	Schedule how frequently you want to collect network data.
Other Tasks		
	Add Additional Networks for Collection	Add additional networks for collection.
	View Collection and WAE Collector Server Status Details	View local Collector server information.
	View Collector Server Logs	View collection events and messages.
	Save or Load Configurations	Save or load configurations that were made using the WAE Collector UI.

Configure Node Discovery

The initial step to configuring collection is to define how nodes are discovered by reading the IGP database of a seed router or by specifying a list of system IP addresses. You can combine these methods to populate the node list.

Note These rules can be overwritten on a per-node basis using the Node List.

For Node Discovery field descriptions, see Table 2-5.

Step 1 From the WAE UI, select **WAE Collector.**

Step 2 If you have multiple networks, select the applicable network that you want to configure collection for. The network icon is located next to the WAE Collector menu item.

Step 3 Choose **Setup > Node Discovery > Default Credentials** tab.

Step 4 Configure global default seed router credentials and click **Apply**.

Step 5 Select the IGP Discovery tab and configure IGP discovery settings and click **Apply**.

WAE Collector communicates with a seed router using its management IP address. The node list is populated with all nodes in the IGP database of the seed router. All WAE Collector interactions applied in the UI work from this node list.

Step 6 Select the Direct Node Discovery tab and configure direct node discovery using system IPv4 addresses and click **Apply**.

WAE Collector uses a list of user-specified system IPv4 IP addresses to discover nodes that may or may not be in the IGP database. SNMP is used to find and poll nodes and interfaces. Other objects, such as LSPs and VPNs, cannot be found using this method. One use case is for discovering L2 switches that reside within a router's domain, but are not listed in the IGP database.

Node Discovery Field Descriptions

Table 2-5 Node Discovery Field Descriptions

Node Discovery Tab	Description
Default Credentials	
SNMPv2c Default RO community	This field entry is required. Enter the community string that acts as a password. It is used to authenticate messages sent between the node and the seed router. You can specify SNMPv3 credentials for specific nodes by creating additional profiles and applying the profile to specific nodes on the node list. For more information, see Configure Additional Node Access Profiles and View and Manage the Node List.
Login	If you want to use a specific username and password to log into devices, select **Specify** and enter the appropriate credentials. If not, select **Disable**.
Security	This field entry is required. Enter a master password to enable you to de-encrypt the authentication file. The password must contain a lowercase and an uppercase character, a special character, and a number.
IGP Discovery	
Discover using IGP Database	Check the check box to use an IGP seed router to discover nodes.
Seed Router Management IP	Management IP address of the seed router used for all collections. The node list is populated with all nodes in the IGP database of the seed router.
Select IGP	**OSPFv2**—Select if collecting an OSPF database. **IS-IS**—Select if collecting an Intermediate System-to-Intermediate System (IS-IS) database. **Note** Node names are available if using IS-IS. You must log into the seed router to discover IS-IS.
IS-IS Level	This option is only available if IS-IS was selected as the database. Select whether to use Level 1, Level 2, or both. If a single Level is selected, the seed router must belong to that level. If selecting both, WAE Collector attempts to log into other routers as necessary, using the same credentials as the seed router, to assemble the nodes from both levels.

Table 2-5 Node Discovery Field Descriptions (continued)

Node Discovery Tab	Description
Select OSPF Area	**Specify**—Select if collecting from a single OSPF area and enter an area ID. The seed router must belong to the area specified. **All**—Select if collecting from all OSPF areas. In this case, WAE Collector attempts to log into all Area Border Routers (ABRs) using the same credentials as the seed router to assemble the nodes from each area. **Note** Unlike the IS-IS database, the OSPF database does not contain node names. Node names will only be available in the node list after SNMP access to each node is established using the Node Access page.
Initial Authentication	Select whether to log into the seed router or use SNMPv2 to access it. If discovering IS-IS, you must select Login.
Login Session Type	Select which login protocol to use: SSH or Telnet. The SSH protocol is more secure and is recommended, if available. The Telnet protocol does not encrypt the username and password.
Use Backup Seed Router	Check the check box to identify whether to use a backup router if the seed router becomes unreachable.
Backup Management IP	Management IP address of the backup router should the seed router not be reachable. This is required if "Use backup seed router" is enabled.
Direct Node Discovery	
Discovery using System IPv4 Addresses	Check the check box to use IP addresses to discover nodes. Enter one or more IPv4 addresses separated by commas. You cannot specify a subnet range.

Configure Node Access

The Node Access page enables you to define the management IPs, SNMP communities, and if necessary, login credentials used by WAE Collector to reach the nodes. The options on this page enable you to reach nodes that could not be reached using strictly the seed router defined on the Node Discovery page. Regardless of whether you are using login or SNMP to reach the seed router, you can use another mechanism to reach the other routers. For instance, you can configure SNMP to reach the seed router and use login to reach the other routers.

The nodes' management IP can be set to one of two rules: set the management IP address to be the same as the node ID (router ID) or replace the node IP address prefix with a user-defined IP prefix.

If discovering multi-hop BGP or if adding login tasks through the Advanced Configurations tab on the What to Collect page, you must enable login through the Login Access option. WAE Collector collects basic BGP information from SNMP, but may need to log into specific routers if multi-hop BGP is configured. You can optionally set these to be the same credentials as used by the seed router.

When the configuration is applied, whether a node is reachable is indicated in the SNMP and Login columns of the Node List table.

You can also configure additional credential profiles using the Additional Access Profile page.

Step 1 From the WAE UI, choose **WAE Collector > Setup > Node Access**.

Step 2 Select and enter the appropriate information. See Table 2-6 for field descriptions.

Step 3 Click **Apply**.

Step 4 (Optional) Configure additional node access profiles. For more information, see Configure Additional Node Access Profiles.

Note

- You can edit this page at any time. Doing so changes how nodes are reachable.
- The global node access rules can be overwritten on a per-node basis. If this is the first time you are setting up the node list, continue to Configure Node Inclusion.

Node Access Field Descriptions

Table 2-6 Fields in Node Access

Field	Description
Management IP	
Same as node IP	Select if the node management IP address is the same as the node IP address.
Replace node IP address prefix with	Select this option if the management IP address can be derived by changing the IP prefix. Enter the node IP address in the first field, and enter the substitution pattern in the second. **Example:** The node IP addresses are in the range 5.6.7.8/24, and the management IP addresses are in the range 5.6.77.8/24. Thus, 5.6.7.8.1 maps to 5.6.77.8.1. For example, to apply this rule, enter: 5.6.7.8/24 > 5.6.77.8/24

Configure Additional Node Access Profiles

You can configure and apply additional node access profiles to several nodes using the Additional Access Profile page. The creation of node access profiles, for example, allows you to easily apply specific credentials to a group of nodes that belong to a certain device model or vendor.

Step 1 From the WAE UI, choose **WAE Collector > Setup > Additional Access Profile**.

Step 2 Enter appropriate credential information (see Table 2-7).

Step 3 Click **Save**.

Step 4 To apply the new profile to specific nodes:

a. From the WAE UI, choose **WAE Collector > Node List**.

b. Check all nodes that you want to apply the new profile to.

Note To sort nodes, click the appropriate column heading.

c. Click **Edit**.

d. From the drop-down fields, select the new profile to apply to the nodes.

e. Click **OK**.

f. To verify that the profile has been applied correctly, click **Test**. View the node list to see if the credential status icons changed for the selected nodes.

Additional Access Profile Field Descriptions

Table 2-7 Fields in Additional Access Profile

Field	Description
Choose Profile	If one exists, choose a profile to edit.
Profile Name	Enter a name for the profile.
SNMP	
SNMP access options	Select either **SNMPv2c** or **SNMPv3**.
SNMPv2c Default RO community	Enter the community string that acts as a password. It is used to authenticate messages sent between the node and the seed router.
SNMPv3 Default Credentials	
Security Level	Select one of the following: • **noAuthNoPriv**—No authentication or privacy protocols are used. • **authNoPriv**—Authentication protocol is used. • **authPriv**—Both authentication and privacy protocols are used.
Username	Enter the username that is configured for the SNMP agent.
Authentication Protocol	Select **MD5** or **SHA** protocol used for authentication.
Authentication Password	Enter the password used for authentication. The password must be at least 8 characters long.
Encryption Protocol	Select **DES** or **AES-128** encryption.
Encryption Password	Enter the password used for encryption.The password must be at least 8 characters long.
Login	
Login access options	If you want to use a specific username and password to log into devices, select **Specify** and enter the appropriate credentials. If not, select **Disable**.

Configure Node Inclusion

The Node Inclusion page enables you to set global rules for including and excluding nodes from being collected. You can edit this page at any time. Doing so changes global rules for whether nodes are included or excluded from being collected. The exclusion rule always takes precedence.

All rules are set using regular expressions. Use the inclusion or exclusion options that make it easiest for you to define the necessary hostnames. For instance, inclusion rules can be useful when you are discovering more nodes than you have available licenses, or when you are only interested in collecting a subset of the nodes.

Example: These are the nodes.

- core1-atl2.acme.com
- core2-atl2.east7.com
- dist1-atl2.acme.com
- core2-atl1.acme.com
- core1-chg1.acme.com

Section	RegEx	Result
Include only nodes	.*	Include all five nodes
Exclude any nodes	^dist.*|.+east.*	Exclude all nodes with a prefix of "dist" or that contain the string "east." The excluded nodes are core2-atl2.east7.com and dist1-atl2.acme.com.

Step 1 From the WAE UI, choose **WAE Collector > Setup > Node Inclusion**.

Step 2 Enter regular expressions to filter what to nodes to include in the given area. To exclude nodes, click the **In addition, exclude any nodes with name matching regular expression** box and enter the regular expression in the given area.

Step 3 Click **Apply**. The updates are displayed in the Include column in the Nodes List table. For more information, see View and Manage the Node List.

The global node inclusion and exclusion rules can be overwritten on a per-node basis. Thereafter, if you continue to see a need to create per-node overrides, use the Node List page.

View and Manage the Node List

The Node List page allows you to create override rules for specific nodes to which the global default credentials do not apply.

The Node List table displays all nodes available to be used in the collection process. Use this table to determine whether nodes are included or excluded, whether nodes are accessible through SNMP or login, and the properties of each node.

The Node List page also provides a means of creating per-node rules that override the global ones. After configuring your global rules, use this editing feature to fine-tune the list of nodes collected.

Each row shows the node attributes, access status, and collection status. This is where you manually override the management IP, SNMP community, or login settings for nodes when the global rules do not succeed. You have the option of specifying explicit values, or you can scan a subnet trying different SNMP communities to find the correct IP address. This scan is useful when you enter an override rule for one or more nodes.

Note

- Nodes are based on two criteria on whether they are included in the collection or not. One is an exclusion based on global rules, and one is an exclusion based on per-node override rules.

- If the number of nodes discovered is more than the number of licenses available, licenses are allocated based on ascending order of system IP addresses, but all of them are included in the collection. Node license violations are listed at the top of Node List page and on the Status page.

Edit Node Credentials (Override Rules)

When new nodes appear, WAE tries the global community string in combination with the global management IP that were specified in the node discovery setup. If SNMP access fails, you can get information for these failures on the Status page. For more information, see View Collection and WAE Collector Server Status Details.

Once the problem is identified, use the Node List page to run a test to see which nodes are being collected, which ones are not, and which nodes were just installed. The nodes that are failing are the ones for which the global rules are likely not working.

For each failed node, if you know the management IP, the SNMP community string, and/or the login access information for that node, you can override the global credentials. If you do not know this information, you can use the scan feature that is available using the Discover option of the Edit field.

Step 1 From the WAE UI, choose **WAE Collector > Node List**.

Step 2 Check all nodes that you want to edit and apply the same credentials to.

Note If you want to only edit the management IP address of one or more nodes, click the management IP address and edit the cell directly from the table.

Step 3 Click **Edit**.

Step 4 Do the following:

a. Exclude from collection—Select to use existing inclusion rule configured from setup, or choose to exclude or include the node.

b. Edit—Select one of the following:

- **Specify**—Select whether to use global rules or override rules for the selected nodes. Then specify changes to management IP, SNMP community, and login access as needed. The SNMP status in the Node List is set to “unknown” until the next collection runs.
- **Discover**—Enter the subnet to search. Then enter multiple SNMP communities to try in succession. WAE Collector scans a range of management IPs combined with the different communities entered to find a node with an ID that matches the discovered node ID. WAE then scans the entire subnet using the entered communities strings in sequence. WAE then tries to find a combination of management IP and community string that allows SNMP access to a router. If such a combination is found, then SNMP access is used to verify whether the found router is in the node list.

  Example: A subnet contains 256 total addresses, and there are 2 SNMP communities to match. This yields a total of 512 attempts to find a node that matches the combination of the subnet and either of the SNMP community strings.

Step 5 Click **OK**.

Step 6 To verify that the credentials have been applied correctly, click **Test**. View the node list to see if the status icons changed for the selected nodes.

Delete, Test, and Apply Updates to the Node List

Step 1 From the WAE UI, choose **WAE Collector > Node List**.

Step 2 Check all nodes that you want to perform an action upon.

Step 3 Click one of the following:

- **Test**—Before applying the configuration, click **Test** to determine if the selected nodes are reachable and included. If a node is not reachable, change its per-node override rules as needed.
- **Delete**—Removes a node from the Node List.

Note WAE Collector never dynamically removes nodes from the Node List, even those that are no longer found during the discovery process. This avoids losing node-specific configurations of nodes that are removed and then later re-appear in the network. To remove a node from the Node List, you must manually delete it from the list.

- **Apply**—Applies the configuration, which updates the Node List.

Node List Table Columns

The Node List table identifies all nodes available for collection, their properties, and status.

If values are user-configured in the UI, they are color-coded based on how they are configured. If the field is blue, the associated node was derived using the global rules. If it is black, the node was derived from the override rules

Table 2-8 Status Columns

Icon	Include	SNMP	Login	Match
Green check	Include in the collection process	Successful SNMP query	Successful login using the management IP address	A match occurs if the node IP is one of the loopbacks configured on the node or if the node name is identical to the node name informed by SNMP.
Red cross	No license or invalid license, but the nodes are still included in the collection	Unsuccessful SNMP query using the management IP address	Unsuccessful login using the management IP address	There is no match. The node IP is not one of the loopbacks configured on the node and the node name is not identical to the node name informed by SNMP.
Blue cross	Excluded from collection by global exclusion rules	NA	NA	NA

Icon	Include	SNMP	Login	Match
Black cross	Excluded from collection by explicit per-node rule	NA	NA	NA
Gray circle	Not determined	SNMP not attempted	Login not attempted	NA

Table 2-9 Property Columns

Property	Description
Management IP	Node management IP address
Community	Encrypted SNMPv2c community string, which is a text string that acts as a password
Username	Name used by WAE Collector to reach the node
Password	Password used in conjunction with the username by WAE Collector to reach the node
Node IP	Router ID
Hostname	Node ID
Vendor	Router vendor
Model	Router model number
OS	Router operating system and version
Last IGP Update	Most recent timestamp of when the node was included in an IGP collection

Configure What to Collect

After you have verified the node list, the next step is to identify what to collect from these nodes. The What to Collect page enables you to optionally collect properties, traffic, BGP connectivity, and VPNs. The information collected for each object populates the plan file tables for use in WAE applications.

• Basic properties and traffic – Nodes – Interfaces – Interfaces queues – RSVP TE LSPs – LSPs	• BGP connectivity • Layer 3 VPNs and traffic

Node names collected from the network often have long suffixes that are the same for all nodes. This page enables you to remove these suffixes, acting on all nodes in the collection process, making for more readable plan files and WAE Live data. The page also provides a feature that enables you to set how long to keep inactive interfaces and circuits from the plan file, thus keeping plan files up to date.

Step 1 From the WAE UI, choose **WAE Collector > Collection > What To Collect**.

Step 2 Click the **Basic** or **BGP/VPN** tab and enter the applicable information. See Table 2-10 for field descriptions.

Note While all fields are optional, you must choose Interfaces, LSPs, BGP, or VPN to collect any data. After configuring these fields, click **Apply**.

Step 3 (Optional) To configure continuous LSP collection or traffic polling, follow the steps described in Configure Continuous Polling and Collection in the WAE Collector UI.

Step 4 (Optional) To add options to existing commands or add new commands, select the **Advanced** tab. This feature is only for advanced users. Modifying the configuration can break the collection process. New commands must be only for collection purposes. The validation process does not guarantee that the modified configuration will work. Consult your support representative for assistance.

Adding an option to a command that has an option with the same name overwrites the existing one. Therefore, always use unique option names.

If using continuous polling, options added to SNMP_POLL are ignored. If adding login commands, you must enable login through the Login Access option on the Node Access page (see View and Manage the Node List).

Step 5 Schedule the collection. For more information, see Schedule the Collection.

What To Collect Basic Field Descriptions

Table 2-10 Field Descriptions for What to Collect

What to Collect Tab	Description
Basic	
Interfaces	Check the check box to collectively identify each interface. For example, an interface's properties could include its interface name, capacity, IGP metric, and TE metric.
Interfaces: Include Queues	The list of interface queues configured on the router, together with per-queue traffic measurements.
Interfaces: Traffic	Incoming and outgoing traffic on an interface in Mbps.
Interfaces: Counter Polling Period	The intervals (in seconds) between successive traffic counter polls.
LSPs	Check the check box to collectively identify each LSP. For example, an LSP's properties could include its destination, setup bandwidth, and the actual path of the LSP.
LSPs: Non-PCEP LSPs	LSPs that are discovered using SNMP. **Note** To set up continuous collection for these LSPs, check this check box. For information, see Configure Continuous Polling and Collection in the WAE Collector UI.
LSPs: PCEP LSPs	LSPs that are managed by WAE or delegated to WAE. LSP delegation is when a node (router) grants WAE the right to update the LSP attributes on one or more LSPs. **Note** To set up continuous collection for these LSPs, check this check box and enable PCEP collection using the steps described in Configure Continuous Polling and Collection in the WAE Collector UI.

Table 2-10 Field Descriptions for What to Collect (continued)

What to Collect Tab	Description
LSPs: Traffic	Outgoing traffic on an LSP in Mbps. • **Counter polling period**— The intervals (in seconds) between successive WAE Collector traffic counter polls. This value must be lower than the LSP counter update period. **Note** Interval collection polls traffic twice during the collection window. The traffic statistics for those two time periods are averaged and added to the plan fils as the traffic. The amount of time for each polling interval is set here. • **Number of nodes with delayed counter update**—The number of nodes that have counters as specified in the Select Nodes field. Certain router vendors and models do not continuously update LSP polling counters. For accurate LSP polling, WAE Collector needs to know which nodes have delayed counters and what the update period is in order to correctly compute the LSP traffic. Use the LSP section to specify the subset of routers with delayed counter updates, and to specify the update delay. The nodes are defined with regular expressions written to find node IPs, node names, vendors, or OS's. If no value is set, the default is 0 and counters are ignored. • **Select Nodes**—Specify which nodes have delayed counter updates. This is specified using a regular expression match on an LSP property. • **Clear nodes**—Clears selection of nodes with delayed counters, and clears all selections made within the LSP section. • **Counter update period**—The amount of time (in seconds) between updates to the SNMP polling counter. Note this value must be higher than the LSP counter polling period.
Remove Node Name Suffixes	Comma separated list of suffixes to remove from node names. This can make the plan file much easier to read in the applications. **Example:** The suffixes acme.net and acme2.net from all nodes in the collection process. acme.net, acme2.net
Days to Expire Inactive Nodes and Circuits	The number of days an inactive node or circuit remains in the plan file before being removed.
BGP/VPN	
BGP	Check the check box to configure discovery of eBGP peers and neighboring external ASes. If discovering multi-hop BGP, you must enable login through the Login Access option on the Node Access page (see Configure Node Access). WAE Collector collects basic BGP information from SNMP, but may need to log into specific routers if multi-hop BGP is configured. You can optionally set these to be the same credentials as used by the seed router. If a default login is not possible, then configure the login access on a per-node basis from the Node List page (see View and Manage the Node List).
BGP: BGP Peer Protocol	Select to discover eBGP peers and neighboring external ASes. Options include searching for BGP peers based on IPv4 addresses, IPv6 addresses, or both.
BGP: Minimum IPv4 Prefix Length	Minimum prefix length to perform an IPv4 subnet match from 0 to 32.
BGP: Minimum IPv6 Prefix Length	Minimum prefix length to perform an IPv4 subnet match from 0 to 128.

Table 2-10 Field Descriptions for What to Collect (continued)

What to Collect Tab	Description
BGP: Multi-hop Discovery by Login	Log into the routers to discover the hops between them. This login must be specified on the Node List page (see View and Manage the Node List).
VPN	Check the check box to discover VPNs and their traffic.
VPN: VPN Type	Select to discover Layer 3 VPN nodes and their traffic. VPN traffic is polled at the same frequency set in the Counter Polling Period field in the Basic page.

Configure Continuous Polling and Collection in the WAE Collector UI

Note Continuous polling is available only on the Default network.

Continuous polling is available for interfaces, queues, VPNs, and LSPs. Queues and VPNs use the same polling period as interfaces.

The WAE Network Interface (NI) server (see Data Flow After Collection) uses SNMP to continuously poll traffic for discovered objects. The statistics gathered are used to calculate frequent, ongoing traffic averages. This can be useful for keeping traffic statistics up to date during the entire collection process, which generally takes a significantly longer time to run than a single polling period.

The WAE NI server also continuously collects LSPs that are can be deployed by WAE or delegated to WAE. (LSP delegation is when a node (router) grants WAE the right to update the LSP attributes on one or more LSPs.)

When configured through the WAE Collector UI, the WAE NI server generates a plan file every five minutes by default.

Continuous Polling and Collection Example:

Counter Polling Period = 120 seconds (this is configured in the Basic tab)

Default Time Window = 8 minutes

Max Expansion of the Window = 25%

Every 120 seconds traffic is polled. The amount of traffic added to the plan file is the average traffic for the last 8 minutes. If there are insufficient counters to calculate the average, the window is extended by 2 minutes (25% of 8 minutes is 2 minutes).

Prerequisites

- Node discovery has been configured.
- Node List is available.
- The WAE NI service must be running. If it is not running, enter the following command:

```
service wae-ni start
```

For Continuous Collection field descriptions, see Table 2-11.

Step 1 From the WAE UI, choose **WAE Collector > Collection > What To Collect > Continuous Collection** tab.

Step 2 To enable continuous traffic collection, check the **Continuous Polling** check box and enter or accept default options.

Step 3 To enable continuous LSP discovery, check the **LSP Collection** check box.

Note
- This option is available only if LSP (Non-PCEP and/or PCEP) collection is enabled from the Basic tab.
- When this option is enabled, continuous traffic collection is automatically enabled.

Step 4 Connect to the WAE NI server by entering Server Access and Server Configuration details or accept default entries.

Step 5 In the WAE Network Interface Server Access area, click **Apply**.

Step 6 Click the **Refresh** icon to verify the WAE NI server is running and reachable. If it is not, verify that you correctly configured its password, started the server , and correctly entered server information.

Note Status of the WAE NI server does not automatically refresh. You must click the Refresh icon to see the latest status.

Step 7 In the main Continuous Collection tab, click **Apply**.

Step 8 Schedule the collection. For more information, see Schedule the Collection.

Continuous Collection Field Descriptions

Table 2-11 Continuous Collection Field Descriptions

Field	Description
Continuous Polling	
Default Time Window	The amount of time, in minutes, over which to calculate (average) the polled traffic statistics. This window (calculation period) starts at the time the plan file is generated and goes backwards to get the statistics. For instance, if the plan file is generated at 8:00 AM and the Default Time Window is 10 minutes, the plan file generated uses statistics from 7:50 AM to 8:00 AM. **Example:** If set to 5 (300 seconds), to determine the incoming packet error rate, WAE Collector takes the average of these incoming packet errors over the last 5 minutes (difference in incoming packet errors over the 5-minute interval / difference in the timestamps of the collections of these readings).
Max Expansion of the Window	There are times in which average statistics cannot be calculated. For instance, router response time might be slow enough that the WAE NI server cannot get sufficient data. This field creates a safety net for such instances by giving the WAE NI server more time from which to collect data. The value is the percentage by which to expand (add to) the amount of time set in the Default Time Window field if no statistics are collected. The lapses in statistics collection do not have to be synchronous for this parameter to apply. **Example:** If the Default Time Window is 10 minutes and the Max Expansion is set to 50%, the window for calculating averages can be expanded up to 5 minutes (50% of 10 minutes) in the event no statistics are available at any time during the 10-minute window.
LSP Collection	
Collection Interval	The amount of time for each polling interval.

Table 2-11 Continuous Collection Field Descriptions (continued)

Field	Description
WAE Network Interface Server Access	
URL	Enter the hostname or IP address of the server that is running continuous polling. If the Collector server and WAE NI server are on the same device, you can use localhost.
Port	Enter the port number of the server that is running continuous polling. The default is 61617.
Username / Password	Enter the username and password that gives you access to the server that is running continuous polling. Both are case sensitive. The default username is "admin," and the default password is "cariden." If the password has changed and you do not know it, contact your administrator or support representative.

Schedule the Collection

Once you have the node list in place and have defined what you want to collect on these nodes, the final step in the configuration process is to schedule the collection and start it.

Note that a collection is also called a *snapshot*. Once a collection instance (snapshot) is stopped, a new collection automatically starts at the next scheduled collection interval unless you are running a single collection. If the Collector server is stopped, the collection process automatically resumes once the server is restarted. If continuously polling the traffic or if continuously collecting PCEP LSPs, that polling or collection is not affected by stopping the Collector server.

The first time you run a collection or if you have made significant changes to the Node List run the collection once and then check the Status page for warnings or errors to determine where you might need to further improve the collection.

Once the collection process is started, the Status and Logs pages are updated with warnings and errors as they occur. The current state is displayed in the top, right of the screen.

Step 1 From the WAE UI, choose **WAE Collector > Collection > Schedule**.

Step 2 Configure the scheduling options or leave the default values, and click **Apply**. See Table 2-12 for field descriptions.

Step 3 To start or end collection, click one of the following buttons:

- **Start**—Starts the collection process using the configured scheduling options.
- **Stop**—Terminates a scheduled collection.
- **Run Once**—Starts the collection, but it only runs one time.

Schedule Field Descriptions

Table 2-12 Field Descriptions for Schedule

Field	Description
Start new snapshot every	Specify how often you want the collection process to run (in minutes). The daily collection times are computed as 00:00 UTC on the hour. For example, if you set this to 16, collection would occur at 16 minutes after the top of the hour, 32, 48, and then again at the top of the next hour.
Collect snapshots	Specify when you want the collection process to run: throughout the day or up to three specified times periods. For example, if you know the network's peak traffic times and you want to run simulations on this traffic in WAE Design, you could collect only at those peak-traffic intervals. To specify a time period select a row, and then move either side of the sliding bar to set the start and end times. Overlapping time periods are not permitted.
Skipped snapshots before terminating	Collection instances might run longer than specified in the Start New Snapshot Every field. To ensure data collection continues, enter a number to specify how many new collection instances (snapshots) to skip before terminating the one that is running. This enables you to prevent multiple collection instan
Collect verbose diagnostics	Check the check box to specify whether to include SNMP recording files. These files are included when using the Downloading Diagnostics feature, which is available on the Status page.
Default log level	Determines the minimum level of severity in the messages that you collect in the log text file. • Fatal—Any error that is forcing a shutdown of the Collector server. • Error—An error that is fatal to the collection process, but not to the Collector server itself, such as the inability to collect an IGP database from the seed router or backup seed router. • Warn—Anything that could potentially cause oddities in the results, such as a switch over from the seed router to the backup router. • Info—Generally useful information such as when the collection process starts and stops. • Debug—Information that is diagnostically helpful. • Trace—Traces the code to find problems.

View Collection and WAE Collector Server Status Details

You can view local Collector server information using the Status page. This page does not report on the status of the WAE Network Interface (NI) server. For all event logs of all servers in an HA environment, go to the WAE Statistics > Events page. For diagnostic and process status information for all servers, go to the WAE Statistics > Diagnostics and WAE Statistics > Processes page, respectively.

Step 1 From the WAE UI, choose **WAE Collector > Collection > Status**.

Step 2 Select one of the following tabs to view collection and status details:

- **Last Snapshot Status**—This tab gives you a quick summary of what was collected in the last collection process (snapshot), as well as the snapshot's duration and whether there were any license violations. If you are running scheduled collections, it displays the next time a collection will run.

Clicking the Download Diagnostic button creates a .zip file containing information to help troubleshoot the last collection by the local Collector server. If calling Cisco for assistance, it is recommended that you e-mail this file to your support representative.

- **Collection Metrics**—This tab shows metrics for all collections for the last 30 days. Daily metrics are kept for the total number of hours data was collected, the number of collections, and whether there were any license violations. Metrics also include the minimum, maximum, and average collection duration, which could be useful for troubleshooting purposes or for adjusting future collection intervals.

  If using the Filter feature to find durations, the increments are h, m, and s for hours, minutes, and seconds, respectively. Do not enter a space between the number and the increment.

  Example: To find snapshots that lasted longer than 15 minutes, select and enter the following.

  Avg Duration Greater than 15m

- **Status Summary**—After each collection process finishes, the Status Summary tab shows the errors and warnings for the most recently completed collection.
  - Node Summary—This table shows errors and warnings that are attributable only to specific nodes, such as an SNMP access failure.

    To read an error or a warning, click the number in the Error count or Warning count cell.
  - Node Independent Issues—This table shows errors and warnings that are not tied to the discovery of nodes, but rather with the collection and post-collection processing steps.

  If you see there are problems, review the Node List to verify nodes are reachable and included. If they are not, try altering either the per-node override rules or the global rules. If you are still not able to troubleshoot and correct the problem, download the diagnostics and send them to your Cisco support representative.

View Collector Server Logs

You can view a list of all errors and warnings since the Collector server was last started. It is a superset of the information that is listed on the Status page, which is relevant only for the last collection.

The information on this page pertains only to the local Collector server. This page does not list logs for continuous polling or for continuous collection of PCEP LSPs. For all event logs of all servers in a local or distributed environment, go to the WAE Statistics > Events page. For diagnostic and process status information for all servers, go to the WAE Statistics > Diagnostics and WAE Statistics > Processes pages, respectively.

To refresh the list of logs without refreshing the browser page, click the **Refresh** button in the top right of the Logs table.

To view logs, go to the WAE UI and choose **WAE Collector > Collection > Logs**.

Save or Load Configurations

A configuration file contains the discovered objects and properties, as well as the configurations used to discover them.

Step 1 From the WAE UI, choose **WAE Collector > Settings > Configuration** tab.

Step 2 Choose one of the following options:

- **Load Configuration**—Overwrites the existing configuration file, and sets the UI settings to those used to configure the saved collection. If needed, you can use this option to load configuration files from the last major release.
- **Save Configuration**—Saves the current configuration file to `<install_directory>/etc/collector/server/configs`. The default installation directory is `/opt/cariden`.
- **Reset Configuration**—Resets all UI settings to their defaults, which includes emptying the node list.

These capabilities can be helpful when performing upgrades or when you need to recover previous configurations.

Configure Collection History

You can configure how many days to keep a collection or how many collections you want to save in the Collector Server. WAE will use the limit that is first reached.

Step 1 From the WAE UI, choose **WAE Collector > Settings > Collection History** tab.

Step 2 Enter the following:

- **Number of last collections**—Saves the specified number of past collections.
- **Max age in days**—The maximum days a collection is saved.

The current disk space storage is also displayed to help you estimate how much data you want to store.

Add Additional Networks for Collection

If you want to configure collection for additional networks, other than the Default network, do the following:

Note Continuous polling can only be performed on the Default network.

Step 1 From the WAE UI, choose **WAE Collector > Default** network icon.

Step 2 From the drop-down list, choose **Network Manager**. The Network Manager page appears.

Step 3 Click **Add**.

Step 4 Enter a network name and click **Save**. The new network should appear under the Networks list. Note:

- The network name cannot contain any spaces or special characters.
- To delete the network or change the network name, click the network under the Networks list.

- The Default network name cannot be changed.

Collecting Information Using Augmented Collection

The augmented collection method extends the plan file that a server creates to include additional collection and modeling for use in WAE Design and WAE Design Archive. If parsing configurations for explicit LSP paths or collecting multicast, LDP, or flow traffic, use the augmented method of collection. To determine the best collection method for your purposes, see Table 2-3 and Collection Methods.

The process begins by configuring and running basic collection (see Collecting Basic Information Using the WAE Collector UI) and then running an augmented snapshot. If you enable continuous collection, then both the Collector server and WAE NI server must continue to run. See Figure 2-3 for a graphical representation of the augmented collection process with continuous collection and polling enabled.

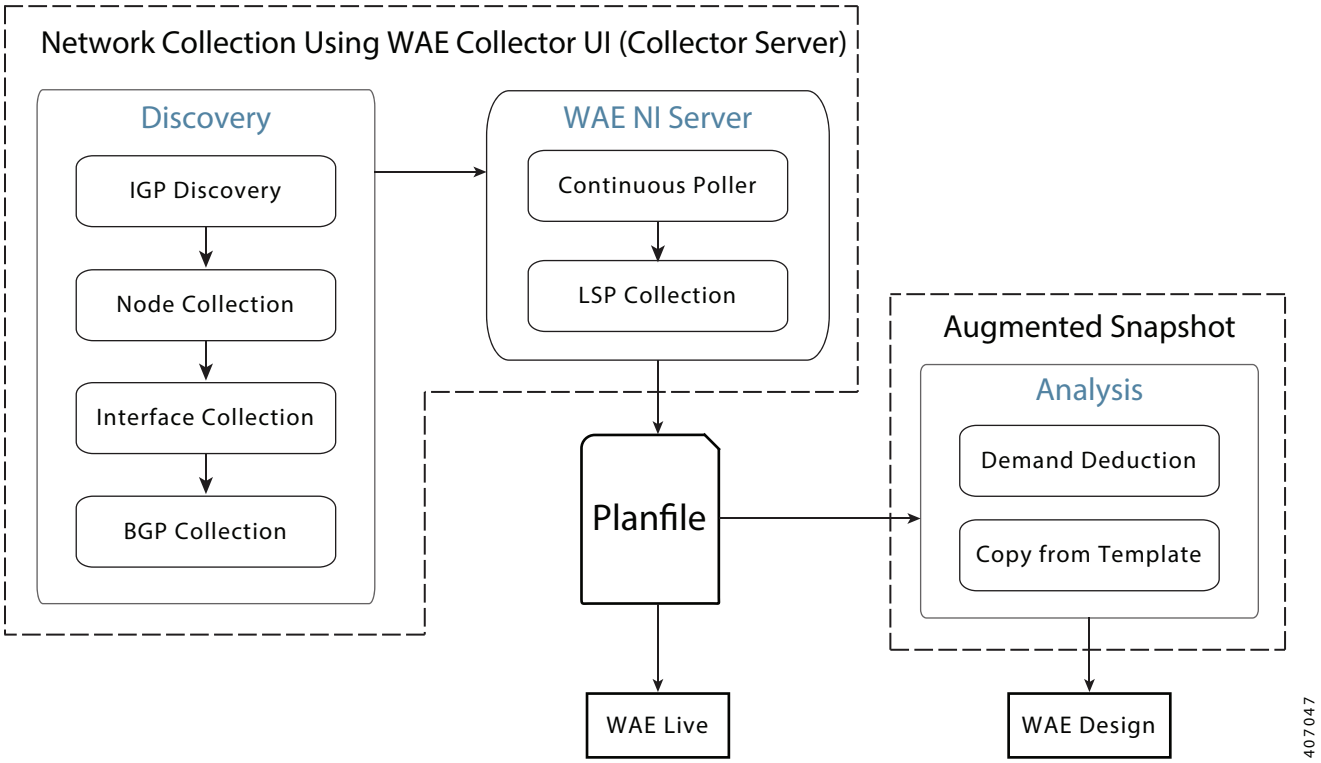
Thereafter, configure the snapshot files to get this plan file from one of these two servers, augment it with additional network data, model the result to visualize the network, and save it in an archive.

One instance of collection must first complete, and thereafter both the server and the augmented snapshot can run simultaneously.

Note If you only want to build a network model that includes the creation of demands after collection, copy a template plan file into a newly generated plan, and store the resulting plan file into an external plan file archive, then use network Model Manager. For more information, see Chapter 3, "Viewing a Network Model."

Note The instructions in this section use the `archive_insert` tool to insert plan files into an external archive. For information on manually inserting plan files into WAE Live, see Appendix A, "Snapshot Examples."

Figure 2-3 Network Collection Process Using Augmented Collection with Continuous Polling and Collection Enabled



Notes and Limitations

The augmented collection method has the following limitations and notable attributes:

- Using augmented snapshots, you cannot collect hardware inventory data, collect data from an Alcatel-Lucent SAM server, or use for multi-network collection. Use the manual method instead.
- This method uses SNMPv2c and SNMPv3 authentication. However, you must use the `mate_auth_init` tool to initiate the authentication file.
- Augmented snapshots can get the plan files from either the Collector server or the WAE NI server. Several of the configuration steps require that you configure one server or the other.
- In the augmented snapshot file, do **not** execute any collection tasks that are available through the WAE Collector UI, including the default ones or any that are configured through the Advanced Config option.
- Do **not** execute SNMP_POLL on interfaces, RSVP-TE LSPs, or VPNs if you are collecting traffic statistics for them through one of the servers.

Environment Variables

- `$CARIDEN_ROOT`—Location of the installation. By default, this is `/opt/cariden`. These terms are interchangeable.

- `$CARIDEN_HOME`—Directory in which the WAE Design, WAE Live, and WAE Collector executables and binaries are installed. The default is `/opt/cariden/software/mate/current`.

Workflow for Collecting Information Using Augmented Snapshots (Augmented Collection)

Before You Begin

We recommend that you back up all your configuration files.

Note If you are only using Augmented Collection to run demand deduction, copy from template, and save to archive tasks, you can use the Model Manager instead.

Table 2-13 Augmented Collection Configuration Workflow

Step	Task	Description / Notes
1	Configure and run network collection using the WAE Collector UI.	See Collecting Basic Information Using the WAE Collector UI. • Access the UI: `https://<Collector_server_IP>:8443/#collector` • If web service is not running, enter the following command: `service wae-web-server start` • Log in to the UI. default username: admin default password: cariden
2	Configure Credentials	Set credentials so that the `collector_getplan` tool can talk to the server from which the snapshot is getting the plan file.
3	Perform Pre-Snapshot Configuration Tasks	Create an authentication file using the `mate_auth_init` tool, optionally edit the network access file, and create two sets of snapshot files for later use.
4	Configure Augmented Snapshot Files	Edit the `snapshot_augment_collector.txt` and `snapshot_augment_collector.inc` files to customize collection.
5	Initialize Archive, Create Template, Run Collections	Post snapshot configuration.

Configure Credentials

You must set credentials so that the `collector_getplan` tool can talk to the server from which the snapshot is getting the plan file. By default, the snapshot authenticates the Collector server.

- You must authenticate the WAE Network Interface (NI) server if using it for continuous LSP collection or traffic polling.
- The credentials file used for the Collector server and WAE NI server must be different.

Before You Begin

Configure and run at least one network collection using the WAE Collector UI (see Collecting Basic Information Using the WAE Collector UI).

Step 1 Run the `collector_getplan` tool once to set the server's credentials for later use in the snapshot files. The only requirement is to use `-set-credentials true`.

```
collector_getplan -set-credentials true
```

The default credential file path, which is configurable, is `$WAE_ROOT/etc/credentials.enc`. To change it, use the `-credentials-file` option.

Example: Set the `-set-credentials` to `true` and change the name of the credentials.enc file.

```
collector_getplan -set-credentials true -credentials-file /opt/cariden/etc/creds.enc
```

Perform Pre-Snapshot Configuration Tasks

Before editing and running the augmented snapshots, you must do the following tasks:

Step 1 Run `mate_auth_init` to create an authentication file (`auth.enc`) used by SNMP and login tools.

```
mate_auth_init
```

This is an interactive tool that first prompts you to choose the SNMP version and the relevant parameters. For information, see Network Authentication.

Step 2 Optional: Customize network access. For information, see Network Access File.

Step 3 For new installations, copy the default snapshot_augment_collector.txt and snapshot_augment_collector.inc files to working configuration files.

```
cp /opt/cariden/software/mate/current/etc/snapshot_augment_collector.txt /opt/cariden/etc
cp /opt/cariden/software/mate/current/etc/snapshot_augment_collector.inc /opt/cariden/etc
```

If this is not a new installation, you can use existing augmented snapshot files in `/opt/cariden/etc` and make modifications noted in this chapter as needed.

Configure Augmented Snapshot Files

Note For information on configuring snapshot .txt and .inc files, see Snapshot Files.

Note A best practice is to add only a few tasks to the snapshot files, run the snapshot, and correct the errors. Then repeat this process until you have built the model of the network that you need.

Step 1 Edit the snapshot_augment_collector.txt file, which contains the collection, polling, modeling, and insertion tasks to perform. This file controls the sequence of execution and also contains environment variables of common values used in the snapshot_augment_collector.inc file.

a. Define the environment variables in the <ENVIRONMENT> section. Each parameter must be separated from its value by a TAB.

   – At minimum, you must define `unique`, `seed_router, home_dir`, and `collector_url`, and preferably the `backup_router`.

- The `collector_url` must be set to the location of the server URL. The default is `https://localhost:8443`, which is to the Collector server. If using the WAE NI server, the port on which it listens for incoming plans is 8086.

  Example: `collector_url https://localhost:8086`

b. If needed, edit the `include` environment variable to read the snapshot_augment_collector.inc file from `$(home_dir)/etc`.

```
include $(home_dir)/etc/snapshot_augment_collector.inc
```

c. Keep COLLECTOR_GETPLAN uncommented as the first task. Either remove or comment out all tasks used in discovering the topology. If you are getting the plan from the WAE NI server that is polling traffic, also remove or comment out all tasks that poll for traffic or collect flows.

Note Do **not** execute any collection tasks that are performed by the Collector server, including the default ones or any that are configured through the Advanced Config option available through the WAE Collector UI. Do **not** execute SNMP_POLL on interfaces, RSVP-TE LSPs, or VPNs if you are collecting traffic statistics for them through one of the servers.

Example:

```
<FLOW_TASKS>
#FLOW_GET
<DISCOVERY_TASKS>
COLLECTOR_GETPLAN
#GET_CONFIGS
#PARSE_CONFIGS
#SNMP_FIND_VPN
<POLLING_TASKS>
#SNMP_POLL
#POLL_LDP
```

d. Define whether to execute flow collection, define which tasks to execute to model the plan file, and define an insert task to specify where to insert the final plan files. Use the comments to enable or disable existing tasks, and add new tasks if needed. At minimum, uncomment the following tasks. For instructions specific to collecting flow data, see Offline Discovery.

- COPY_FROM_TEMPLATE—Copies selected values from the template plan file into the newly generated plan, while preserving network configuration information.
- ARCHIVE_INSERT—Stores the completed plan file in an external plan file archive. This archive can be accessed by all the applications.

Example:

```
<ANALYSIS_TASKS>
#BUILD_MODEL
MATE_CONVERT
COPY_FROM_TEMPLATE
DMD_MESH_CREATOR
DMD_DEDUCT
#MATE_SIM
<ARCHIVE_INSERT_TASKS>
ARCHIVE_INSERT
#ML_INSERT
```

Step 2 As needed, edit the snapshot_augment_collector.inc file to modify and add tools that are to be called from the snapshot_augment_collector.txt file. For information on any tool, refer to its `-help` output. For information on how to edit the snapshot_augment_collector.inc, see Snapshot Files.

For `collector_getplan`, keep `-set-credentials` to `false` so that the snapshot process does not stop to ask for credentials. You only need to set this to `true` once, which you have already done. The `-credentials-file` must match the name that you specified when you first set the credentials (as per Configure Credentials).

Initialize Archive, Create Template, Run Collections

Note Text in <angle brackets> refers to environment variables that you set in the snapshot.txt file.

Step 1 Run `archive_init` to initialize the archive repository into which the plan files will be inserted.

```
archive_init -archive $WAE_ROOT/archives/<unique>-archive
```

For example:
`archive_init -archive $WAE_ROOT/archives/default-archive` (for the default network)

Step 2 If collecting data for WAE Design Archive, use the `archive_config` tool to add the archive repository. At the same time, set up the template directory and template name.

```
archive_config -action add -name <unique> -path $WAE_ROOT/archives/<unique>-archive
-template-dir $WAE_ROOT/data -template-name <unique>-template.pln
```

Step 3 Create an empty template. You can ignore the warnings because the resulting file is an empty template file.

```
echo | mate_convert -plan-file - -out-file $WAE_ROOT/data/<unique>-template.pln
```

Note that WAE Live automatically creates the template.pln from the most recently collected plan file if no template exists. Therefore, for WAE Live, this step is not a requirement.

Step 4 Test the snapshot process by running it as a single tool to collect network data. Check the output for errors, fix them if needed, and rerun this test until it is successful before proceeding.

```
snapshot -config-file $WAE_ROOT/etc/snapshot_augment_collector.txt
```

Step 5 Create a cron job that repeats the process of creating snapshots and inserting them into the archive repository.

Note Both CARIDEN_ROOT and CARIDEN_HOME variables must be defined from within the crontab. You cannot use CARIDEN_HOME=$CARIDEN_ROOT/software/mate/current.

Open the file as follows.

```
crontab -e
```

At the end of the file, add the following lines.

```
CARIDEN_ROOT=/opt/cariden
CARIDEN_HOME=/opt/cariden/software/mate/current
0,15,30,45 * * * * $CARIDEN_HOME/bin/snapshot -config-file
$CARIDEN_ROOT/etc/snapshot_augment_collector.txt 2>&1
```

Collection Network Information Using Manual Collection

The manual collection method uses snapshot.txt and snapshot.inc files to discover the network, model the plan files, and insert the plan files into an archive repository. While this method can collect everything that can be collected through the Collector server or augmented method, unless one of the following conditions applies, it is recommended that you use either the Collector server or an augmented collection method for ease of maintainability.

- Multiple networks for use in the WAE Live application.
- SAM server (SAM_GETPLAN) integration.
- Other highly customized, advanced, or non-standard collection methods that require additional scripting or customized setups; this includes collection of different data at different frequencies.

To determine the best collection method for your purposes, see Collection by Configuration Method.

This chapter references the following terms.

- `$WAE_ROOT`—Location of the installation. By default, this is `/opt/cariden`.
- `$CARIDEN_HOME`—Directory in which the WAE Design, WAE Live, and WAE Collector executables and binaries are installed. The default is `/opt/cariden/software/mate/current`.

Note All instructions and examples assume you used `/opt/cariden` as the default installation directory. If you did not, then substitute your installation directory for `/opt/cariden`.

Workflow for Collecting Network Information Using Manual Collection

Before You Begin

We recommend that you back up all your configuration files.

Table 2-14 Manual Collection Configuration Workflow

Step	Task	Description/Notes
1	Perform Pre-Snapshot Configuration Tasks	Create an authentication file using the `mate_auth_init` tool, optionally edit the network access file, and create two sets of snapshot files for later use.
2	Modify Snapshot Files	Edit the snapshot files to customize collection, polling, modeling, etc. For examples of snapshot configurations, see Snapshot Examples.
3	Initialize Archive, Create Template, Run Collections	Post snapshot configuration.
4	Configure Continuous Polling and Collection Using Manual Collection	If using the data in applications, follow the steps described in this task.

Pre-Snapshot Configuration

Before editing and running the manual snapshots, you must do the following tasks:

Step 1 Run `mate_auth_init` to create an authentication file (`auth.enc`) used by SNMP and login tools.

```
mate_auth_init
```

This is an interactive tool that first prompts you to choose the SNMP version and the relevant parameters. For information, see Network Authentication.

Step 2 Optional: Customize network access. For information, see Network Access File.

Step 3 For new installations, copy the default snapshot.txt and snapshot.inc files to working configuration files.

```
cp /op. t/cariden/software/mate/current/etc/snapshot.txt /opt/cariden/etc
cp /opt/cariden/software/mate/current/etc/snapshot.inc /opt/cariden/etc
```

If this is not a new installation, you can use existing snapshot files in `/opt/cariden/etc`, and make modifications noted in this chapter as needed.

Modify Snapshot Files

For more information on how to modify snapshot files, see Snapshot Files.

Note A best practice is to add only a few tasks to the snapshot files, run the snapshot, and correct the errors. Then repeat this process until you have built the model of the network that you need.

Step 1 Edit the snapshot.txt file, which contains the collection, polling, modeling, and insertion tasks to perform. This file controls the sequence of execution and also contains environment variables of common values used in the snapshot.inc file.

- At minimum, you must define `unique`, `seed_router`, `igp`, and `home_dir`, `archive_dir`, and preferably the `backup_router`.

  By default, the `archive_insert` tool uses the `archive_dir` environment variables when inserting plan files into an external archive. Best practice is to use the default.

  Example: `archive_dir $(home_dir)/archives`

  To manually insert plan files into the WAE Live Map archive, create a new environment variable to specify the archive. Note that the location of the external archive and the Map archive must be different.

  Example: `map_archive_dir $(home_dir)/data/mldata`

- If needed, edit the `include` environment variable to read the snapshot.inc file from `$(home_dir)/etc`.

  ```
  include $(home_dir)/etc/snapshot.inc
  ```

Step 2 Define which tasks to execute to discover the network. Use the comments to enable or disable existing tasks, and add new tasks if needed. For examples, see Snapshot Examples.

For instructions specific to collecting flow data or SAM data, see Advanced Collection Configurations.

If you are discovering IS-IS, do the following:

- Uncomment the LOGIN_FIND_IGP_DB task, which discovers a basic IGP topology by logging into the seed router and parsing an IS-IS database. (To uncomment a task, remove the # sign.)
- Add a comment (#) to the beginning of the SNMP_FIND_OSPF_DB task.

  Example:

  ```
  <DISCOVERY_TASKS>
  #SAM_GETPLAN
  #SNMP_FIND_OSPF_DB
  ```

```
LOGIN_FIND_IGP_DB
SNMP_FIND_NODES
SNMP_FIND_INTERFACES
#GET_CONFIGS
#PARSE_CONFIGS
#FIND_BGP
SNMP_FIND_RSVP
SNMP_FIND_VPN
```

Step 3 Define which tasks to use for polling traffic.

Example:

```
<POLLING_TASKS>
SNMP_POLL
#POLL_LDP
```

Step 4 Define which tasks to execute to model the plan file. Use the comments to enable or disable existing tasks, and add new tasks if needed. If not using WAE Live, at minimum, uncomment COPY_FROM_TEMPLATE.

Example:

```
<ANALYSIS_TASKS>
#BUILD_MODEL
MATE_CONVERT
COPY_FROM_TEMPLATE
DMD_MESH_CREATOR
DMD_DEDUCT
#MATE_SIM
```

Step 5 Define which tasks to insert plan files. Use the comments to enable or disable existing tasks, and add new tasks if needed. For examples, see Snapshot Examples.

- ARCHIVE_INSERT—Insert the completed plan file into an external plan file archive that can be accessed by all the applications.
- ML_INSERT—Manually insert data into the WAE Live data store.
- MAP_ARCHIVE_INSERT—Manually insert plan files into the Map archive. Use only if using ML_INSERT and only if using the Map component. You must manually add this to the snapshot.inc file.

Example:

```
<ARCHIVE_INSERT_TASKS>
ARCHIVE_INSERT
ML_INSERT
MAP_ARCHIVE_INSERT
```

Step 6 Sometimes the IP management addresses that are discovered from the devices are different than the IP management addresses that are needed to communicate with the routers. If so, you need to create a <Nodes> table that lists the proper IP management addresses, and then use the `tab_merger` tool to insert the IP management addresses during the snapshot process. For information, contact your Cisco representative.

Step 7 As needed, edit the snapshot.inc file to modify and add tools that are to be called from the snapshot.txt file. You must add a definition for MAP_ARCHIVE_INSERT if you added that task.

Initialize Archive, Create Template, Run Collections

Note Text in <angle brackets> refers to environment variables that you set in the snapshot.txt file.

Step 1 Run `archive_init` to initialize the archive repository into which the plan files will be inserted. If you are using `archive_insert` to manually insert plan files into the WAE Live Map archive, this is not a required step.

```
archive_init -archive $WAE_ROOT/archives/<unique>-archive
```

Step 2 If collecting data for WAE Design Archive, use the `archive_config` tool to add the archive repository. At the same time, set up the template directory and template name.

```
archive_config -action add -name <unique> -path $WAE_ROOT/archives/<unique>-archive
-template-dir $WAE_ROOT/data -template-name <unique>-template.pln
```

Step 3 Create an empty template. You can ignore the warnings because the resulting file is an empty template file.

```
echo | mate_convert -plan-file - -out-file $WAE_ROOT/data/<unique>-template.pln
```

Note that WAE Live automatically creates the template.pln from the most recently collected plan file if no template exists. Therefore, for WAE Live, this step is not a requirement.

Step 4 Test the snapshot process by running it as a single tool to collect network data. Check the output for errors, fix them if needed, and rerun this test until it is successful before proceeding.

```
snapshot -config-file $WAE_ROOT/etc/snapshot.txt
```

Step 5 Create a cron job that repeats the process of creating snapshots and inserting them into the appropriate archive repository.

Note Both CARIDEN_ROOT and CARIDEN_HOME variables must be defined from within the crontab. You cannot use CARIDEN_HOME=$CARIDEN_ROOT/software/mate/current.

Open the file as follows.

```
crontab -e
```

At the end of the file, add the following lines.

```
CARIDEN_ROOT=/opt/cariden
CARIDEN_HOME=/opt/cariden/software/mate/current
0,15,30,45 * * * * $CARIDEN_HOME/bin/snapshot -config-file $CARIDEN_ROOT/etc/snapshot.txt
2>&1
```

Configure Continuous Polling and Collection Using Manual Collection

The manual collection method uses snapshot.txt and snapshot.inc files to discover the network, model the plan files, and insert the plan files into an archive repository. Optionally, it can push discovered topology to the WAE Network Interface (NI) server (using `collector_pushplan`), which can then

continuously poll traffic statistics and/or continuously discover PCEP LSPs; thereafter, an augmented snapshot can retrieve that plan file from the WAE NI server for further processing (using `collector_getplan`).

If configured, WAE Collector continuously collects LSPs managed by WAE. It also continuously polls LSP and interface statistics that are made available via SNMP.

This chapter references the following terms.

- `$CARIDEN_ROOT`—Location of the installation. By default, this is `/opt/cariden`.
- `$CARIDEN_HOME`—Directory in which the WAE Design, WAE Live, and WAE Collector executables and binaries are installed. The default is `/opt/cariden/software/mate/current`.

Note

- All instructions and examples assume you used `/opt/cariden` as the default installation directory. If you did not, then substitute your installation directory for `/opt/cariden`.
- You cannot use `sam_getplan` when using the WAE NI server.
- This chapter describes the full process of both pushing plan files to and retrieving them from the WAE NI server.

If you are using `collector_getplan` in an augmented snapshot after having configured the Collector server to push plan files to the WAE NI server, see Collecting Information Using Augmented Collection.

Workflow for Configuring Continuous Polling and Collection Using Manual Collection

Step 1 Best practice: Back up all configuration files before you begin.

Step 2 Set up the WAE NI server.

a. Configure Continuous Collection Parameters on the WAE NI Server.

b. Configure Authentication and Start Server.

Step 3 Execute Pre-Snapshot Configuration steps, which include creating an authentication file, optionally editing the network access file, and creating two sets of snapshot files for later use.

Step 4 Create Snapshot to Push Plan Files.

a. Configure Push Credentials.

b. Modify Push snapshot.txt to run only discovery tasks.

c. Modify Push snapshot.inc to include `collector_pushplan`.

Note If you do not need to run further tasks, such as creating demand meshes and running Demand Deduction, skip to Step 7.

Step 5 Create Snapshot to Get Plan Files.

a. Configure Get Credentials.

b. Configure Get Credentials to run post-discovery tasks.

c. Modify Get snapshot.inc to use `collector_getplan`.

d. Initialize Archive and Create Template.

Step 6 Run Collections.

Step 7 If using the data in applications, execute the Collecting Hardware Inventory steps.

Configure Continuous Collection Parameters on the WAE NI Server

Edit the `$WAE_HOME/wae-ni/etc/collection.cfg` file to tell the WAE NI server whether to continuously discover LSPs, as well as what to poll, how frequently to poll, and the amount of time to use when averaging the statistics.

Note Do not edit this file if you are collecting network information using the WAE Collector UI.

Parameter	Description
enablePcepLspCollection	True = Continuously collect PCEP LSPs. False = Do not continuously collect PCEP LSPs.

Continuously Poll Traffic Field Descriptions

Note Continuous polling applies to interfaces and LSP statistics that are made available via SNMP.

Parameter	Description
enableInterfaceStatsCollection	True = Continuously poll interface traffic. False = Do not poll interfaces.
interfaceStatsCollectionPeriodInSecs	The intervals (in seconds) between successive interface traffic counter polls. The minimum value is 60 seconds.
enableLspStatsCollection	True = Continuously poll LSP traffic. False = Do not poll LSPs.
lspStatsCollectionPeriodInSecs	The intervals (in seconds) between successive LSP traffic counter polls. The minimum value is 60 seconds.
enableQosStatsCollection	True = Continuously poll interface queue traffic. False = Do not poll interface queues.
enableVpnStatsCollection	True = Continuously poll VPN traffic. False = Do not poll VPNs.
statsComputingMinimumWindowLengthInSecs	This defines the minimum amount of time, in seconds, over which to generate averages of the polled traffic statistics. For example, if set to 300, to determine the rate of incoming packet errors, the WAE NI server takes the average of these incoming packet errors over the last 300 seconds. These traffic statistics are added to the plan file each time it is generated. The minimum value is 300 seconds.

statsComputingMaximumWindowLengthInSecs	There are times in which average statistics cannot be calculated. For instance, router response might be slow enough that the WAE NI server cannot get sufficient data. This parameter creates a safety net for such instances by giving the WAE NI server more time from which to collect data. The value is the percentage by which to expand (add to) the amount of time set in the statsComputingMinimumWindowLengthInSecs parameter if no statistics are collected. The lapses in statistics collection do not have to be synchronous for this parameter to apply. **Example:** If the statsComputingMinimumWindowLengthInSecs is 400 seconds and the statsComputingMaximumWindowLengthInSecs parameter is set to 25%, the window for calculating averages can be expanded up to 100 seconds (25% of 400 seconds) in the event no statistics are available at any time during the 10-minute window.
rawCounterTtlInMins	Defines the amount of time raw counters are kept in minutes. The minimum value is 5 minutes.
lspDiscoveryCollectionPeriodInSecs	Sets the LSP collection period in seconds (minimum is 60 seconds). This setting indicates how often the continuous poller will try to do LSP discovery.
lspDiscoveryUseCalculatedHops	Specifies whether to store calculated hops or actual hops in the plan file. The continuous poller collects both during discovery. True—Stores calculated hops, if available, in the plan file. False—Stores actual hops in the plan file.
lspDiscoveryUsePcepSignaledName	Specifies whether to use the PCEP signaled name while storing the LSP in the plan file. True—PCEP signaled name is used as the LSP name in plan file. False—The LSP name that is set on the router is used as the name in the plan file. **Note** If set to true, the Cisco router LSP name is stored as tunnel-te5.
lspDiscoveryUseAutobandwidth	Specifies whether or not to store the auto bandwidth in the plan file. True—If the auto bandwidth rate is discovered, then auto bandwidth is stored as the setup bandwidth in the plan file. False—The discovered setup bandwidth is stored in plan file.
l1DiscoveryEnabled	True—Enables Layer 1 discovery in WAE NI. False—Disables Layer 1 discovery in WAE NI.

Common Parameters

Parameter	Description
logVerbosity	Integer that defines the verbosity of the information returned by log files. Trace = 60 Debug = 50 Info = 40 Warn = 30 Error = 20
planFileGenerationIntervalInSecs	Defines how often a pre-calculated plan file is generated in seconds. The minimum value is 300 seconds. This value is used when the WAE NI server is configured through the WAE Collector UI. Note that both `collector_getplan` and WAE Live use on-demand plan files rather than pre-calculated plan files.

Configure Authentication and Start Server

Step 1 Configure the authentication for the WAE NI server.

default username: admin

default password: cariden

Step 2 If it is not running, start the WAE NI server.

Check the status: `service wae-ni status`

Start: `service wae-ni start`

Pre-Snapshot Configuration

Note For demonstration purposes, this chapter references two sets of files: snapshot-pushplan and snapshot-getplan .txt and .inc files. You can name these files whatever you choose. Therefore, where text states, for example, snapshot-pushplan.txt, this means the snapshot.txt file that is pushing the plan file to the WAE NI server. Additionally, all instructions and examples assume you used `/opt/cariden` as the default installation directory. If you did not, then substitute your installation directory for `/opt/cariden`.

Step 1 Run `mate_auth_init` to create an authentication file (`auth.enc`) used by SNMP and login tools.

```
mate_auth_init
```

This is an interactive tool that first prompts you to choose the SNMP version and the relevant parameters. For information, see Network Authentication.

Step 2 Optional: Customize network access. see Network Access File.

Step 3 Because you need to run two snapshots, create both sets of files now. Later you will edit both sets of files.

Copy the default snapshot.txt, snapshot.inc, snapshot_augment_collector.txt and snapshot_augment_collector.inc files to working configuration files in `$WAE_ROOT/etc` and **give them different names**.

Note that if you have existing snapshot files in `$WAE_ROOT/etc`, you can copy those files to snapshot-pushplan and snapshot-getplan files, and then make changes to those files aligned with the instructions in this chapter.

Examples:

```
cp /opt/cariden/software/mate/current/etc/snapshot.txt
/opt/cariden/etc/snapshot-pushplan.txt
cp /opt/cariden/software/mate/current/etc/snapshot.inc
/opt/cariden/etc/snapshot-pushplan.inc
cp /opt/cariden/software/mate/current/etc/snapshot_augment_collector.txt
/opt/cariden/etc/snapshot-getplan.txt
cp /opt/cariden/software/mate/current/etc/snapshot_augment_collector.inc
/opt/cariden/etc/snapshot-getplan.inc
```

Create Snapshot to Push Plan Files

Note For information on configuring snapshot.txt and snapshot.inc files, see Snapshot Files. This section assumes you know how to modify these files and how they work together.

Configure Push Credentials

Run the `collector_pushplan` tool once to set the WAE NI server's credentials for later use in the snapshot files. You must use `-set-credentials true`. When prompted, enter the username and password for the WAE NI server.

The default credential file is `$CARIDEN_ROOT/etc/collector/credentials.enc`. **The credentials file for the snapshot-pushplan and the snapshot-getplan files must be the same.** To change it, use the `-credentials-file` option.

Example: `collector_pushplan -set-credentials true -credentials-file /opt/cariden/etc/collector/credentials-CP.enc`

Note The credentials file used for the Collector server and WAE NI server must be different.

Modify Push snapshot.txt

Step 1 Define the environment variables in the <ENVIRONMENT> section. Each parameter must be separated from its value by a TAB.

- At minimum, define `unique`, `seed_router`, `igp`, and `home_dir`, and preferably the `backup_router`.
- If needed, edit the `include` environment variable to read the snapshot-pushplan.inc file from `$(home_dir)/etc`.

  Example: `include $(home_dir)/etc/snapshot-pushplan.inc`

Step 2 In the <DISCOVERY_TASKS> section, uncomment or add tasks that discover the topology. (See example in step 3.) Note that the order of these tasks determines the sequence of their execution.

Step 3 Immediately following the discovery tasks, add a COLLECTOR_PUSHPLAN task to push the plan file to the WAE NI server.

Example:

```
<DISCOVERY_TASKS>
#SAM_GETPLAN
SNMP_FIND_OSPF_DB
#LOGIN_FIND_IGP_DB
SNMP_FIND_NODES
SNMP_FIND_INTERFACES
#GET_CONFIGS
#PARSE_CONFIGS
#FIND_BGP
SNMP_FIND_RSVP
#SNMP_FIND_VPN
COLLECTOR_PUSHPLAN
```

Step 4 **Either remove or comment out all other tasks in the snapshot**.

Step 5 Sometimes the IP management addresses that are discovered from the devices are different than the IP management addresses that are needed to communicate with the routers. If so, you need to create a <Nodes> table that lists the proper IP management addresses, and then use the `tab_merger` tool to insert the IP management addresses during the snapshot process. For information, contact your Cisco representative.

Modify Push snapshot.inc

Step 1 As needed, edit and add collection tools that are to be called from the snapshot-pushplan.txt file.

Step 2 Add the `collector_pushplan` configuration. The required options are `-set-credentials`, `-credentials-file`, `-in-net-access-file`, and `-in-auth-file`.

Set the `-set-credentials` to `false` so that the snapshot process does not stop to ask for credentials. You only need to set this to `true` once, which you have already done (as per Configure Push Credentials).

The `-credentials-file` must match the name that you specified when you first set the credentials (as per Configure Push Credentials).

The `-in-plan-file` tells the WAE NI server the path and name of the plan file that is being sent to it.

By default, the net_access.txt file is in `$CARIDEN_HOME/etc`. If you modify this, then that same path and name must be configured for `collector_pushplan`, and it must reside in one of these locations.

- `~/.cariden/etc`
- `$CARIDEN_ROOT/etc`
- `$CARIDEN_HOME/etc`

The auth.enc file location must match the location in which the `mate_auth_init` put it.

JMS is the protocol that the Collector server uses to communicate with the WAE NI server. By default, the WAE NI server is using the same host (localhost) as the Collector server. By default, the WAE NI server listens on port 61617 to receive plan files pushed to it. You can change these using the `-jms-server-address` and `-jms-server-port` options.

Example COLLECTOR_PUSHPLAN

Name	Required Value
<COLLECTOR_PUSHPLAN>	
cmd	$(cariden_home)/bin/collector_pushplan
cmd_opt	COLLECTOR_PUSHPLAN_CMD_OPT
postcmd	cp
postcmd_opt	COLLECTOR_PUSHPLAN_CP_CMD_OPT
cmd_success	0
<COLLECTOR_PUSHPLAN_CMD_OPT>	
set-credentials	false
credentials-file	$(home_dir)/etc/collector/credentials-CP.enc
in-plan-file	$(work_dir)/$(unique).txt
in-net-access-file	$(cariden_home)/etc/net_access.txt
in-auth-file	$(home_dir)/etc/auth.enc
jms-server-address	localhost
jms-server-port	61617
<COLLECTOR_PUSHPLAN_CP_CMD_OPT>	
	$(work_dir)/$(unique).txt
	$(debug_dir)/$(unique).txt-post-collector_pushplan.txt

Create Snapshot to Get Plan Files

Note If you do not need to add further tasks to the snapshots, skip this section and go to Run Collections.

Configure Get Credentials

Run the `collector_getplan` tool once to set the WAE NI server's credentials for later use in the snapshot files. You must use `-set-credentials true`.

The default credential file is `$CARIDEN_ROOT/etc/collector/credentials.enc`. **The credentials file for the snapshot-pushplan and the snapshot-getplan files must be the same.** To change it, use the `-credentials-file` option.

Example: `collector_getplan -set-credentials true -credentials-file /opt/cariden/etc/collector/credentials-CP.enc`

Note The credentials file used for the Collector server and WAE NI server must be different.

Modify Get snapshot.txt

The instructions in this chapter use the `archive_insert` tool to insert plan files into an external archive. For information on manually inserting plan files into WAE Live, see Snapshot Examples.

Step 1 Define the environment variables in the <ENVIRONMENT> section. Each parameter must be separated from its value by a TAB.

- At minimum, define `unique`, `seed_router`, `igp`, and `home_dir`, and preferably the `backup_router`. **These must be the same as in the snapshot-pushplan.txt file.** The `archive_dir` must also be specified, and it is not relevant to the snapshot-pushplan.txt file.
- Add or edit the `collector_url` variable to set to the location of the WAE NI server. The default port on which it listens for incoming plans is 8086.

  Example: `collector_url https://localhost:8086`
- If needed, edit the `include` environment variable to read the snapshot-getplan.inc file from `$(home_dir)/etc`.

  Example: `include $(home_dir)/etc/snapshot-getplan.inc`

Step 2 Keep COLLECTOR_GETPLAN uncommented as the first task. Either remove or comment out all **tasks used in discovering the topology or polling for traffic.**

Example:

```
<DISCOVERY_TASKS>
COLLECTOR_GETPLAN
#GET_CONFIGS
#PARSE_CONFIGS
#SNMP_FIND_VPN
<POLLING_TASKS>
#SNMP_POLL
#POLL_LDP
```

Step 3 Define whether to execute flow collection, define which tasks to execute to model the plan file, and define an insert task to specify where to insert the final plan files. Use the comments to enable or disable existing tasks, and add new tasks if needed. Note that the order of these tasks determines the sequence of their execution. At minimum, uncomment the following tasks.

- COPY_FROM_TEMPLATE—Copies selected values from the template plan file into the newly generated plan, while preserving network configuration information.
- ARCHIVE_INSERT—Stores the completed plan file in an external plan file archive for use by applications.

Example:

```
<FLOW_TASKS>
FLOW_GET
<ANALYSIS_TASKS>
#BUILD_MODEL
MATE_CONVERT
COPY_FROM_TEMPLATE
DMD_MESH_CREATOR
DMD_DEDUCT
#MATE_SIM
<ARCHIVE_INSERT_TASKS>
ARCHIVE_INSERT
#ML_INSERT
```

Modify Get snapshot.inc

Step 1 As needed, add or edit flow, modeling, and insertion tools that are to be called from the snapshot-getplan.txt file.

Step 2 Keep the `collector_getplan` configuration `-url` option set to the `collector_url` environment variable.

Keep `-set-credentials` to `false` so that the snapshot process does not stop to ask for credentials. You only need to set this to `true` once, which you have already done (as per Configure Get Credentials).

The `-credentials-file` must match the name that you specified when you first set the credentials (as per Configure Get Credentials), and it must be the same as used in the snapshot-pushplan.inc file.

The `-out-file` tells the WAE NI server where (path and filename) to write the latest plan file.

The net_access_session_file.txt and auth_session_file.enc must reside in one of the following locations. Best practice is to put them wherever you put the net_access.txt and auth.enc file used in the snapshot-pushplan.inc file.

- `~/.cariden/etc`
- `$CARIDEN_ROOT/etc`
- `$CARIDEN_HOME/etc`

Example COLLECTOR_GETPLAN

Name	Required Value
<COLLECTOR_GETPLAN>	
cmd	$(cariden_home)/bin/collector_getplan
cmd_opt	COLLECTOR_GETPLAN_CMD_OPT
postcmd	cp
postcmd_opt	COLLECTOR_GETPLAN_CP_CMD_OPT
cmd_success	0
<COLLECTOR_GETPLAN_CMD_OPT>	
set-credentials	false
credentials-file	$(home_dir)/etc/collector/credentials-CP.enc
get	files
url	$(collector_url)
if-later-than-timestamp-file	$(timestamp_file)
out-file	$(work_dir)/$(unique).txt
out-net-access-file	$(net_access_session_file)
out-auth-file	$(auth_session_file)
<COLLECTOR_GETPLAN_CP_CMD_OPT>	
	$(work_dir)/$(unique).txt
	$(debug_dir)/$(unique).txt-post-collector_getplan.txt

Initialize Archive and Create Template

Note Text in <angle brackets> refers to environment variables that you set in the snapshot-getplan.txt file.

Step 1 Run `archive_init` to initialize the archive repository into which the plan files will be inserted.

```
archive_init -archive $WAE_ROOT/archives/<unique>-archive
```

Step 2 If collecting data for WAE Design Archive, use the `archive_config` tool to add the archive repository. At the same time, set up the template directory and template name.

```
archive_config -action add -name <unique> -path $WAE_ROOT/archives/<unique>-archive
-template-dir $WAE_ROOT/data -template-name <unique>-template.pln
```

Step 3 Create an empty template. You can ignore the warnings because the resulting file is an empty template file.

```
echo | mate_convert -plan-file - -out-file $WAE_ROOT/data/<unique>-template.pln
```

Note that WAE Live automatically creates the template.pln from the most recently collected plan file if no template exists. Therefore, for WAE Live, this step is not required.

Run Collections

Step 1 Test the snapshot process by running each one as a single tool to collect network data. Check the output for errors, fix them if needed, and rerun this test until it is successful before proceeding.

```
snapshot -config-file $WAE_ROOT/etc/snapshot-pushplan.txt
snapshot -config-file $WAE_ROOT/etc/snapshot-getplan.txt
```

Step 2 Create a cron job that repeats the process of creating snapshots and inserting them into the archive repository.

Note Both CARIDEN_ROOT and CARIDEN_HOME variables must be defined from within the crontab. You cannot use CARIDEN_HOME=$CARIDEN_ROOT/software/mate/current.

Open the file for editing as follows.

```
crontab -e
```

At the end of the file, add the following lines. If you used only the snapshot-pushplan configuration, do not add snapshot-getplan to the cron job.

```
CARIDEN_ROOT=/opt/cariden
CARIDEN_HOME=/opt/cariden/software/mate/current
SNAPSHOT="/opt/cariden/software/mate/current/bin/snapshot -log-to-screen false"
*/30 * * * * $SNAPSHOT -config-file $CARIDEN_ROOT/etc/snapshot-pushplan.txt
*/30 * * * * $SNAPSHOT -config-file $CARIDEN_ROOT/etc/snapshot-getplan.txt
```

Collecting Hardware Inventory

To easily collect and view hardware inventory information on your network, run the snapshot tool using the snapshot_hardware_inventory.txt file, and then view the information in WAE Live. For more information on WAE Live, see the *WAE LIVE User Guide*.

Prerequisite

- Run the following command:

  ```
  collector_getplan -set-credentials true
  ```

- A collection has been done using one of the collection methods and a plan file exists.
- `$CARIDEN_ROOT`—Location of the installation. By default, this is `/opt/cariden`. All instructions and examples assume `/opt/cariden` as the default installation directory. If you did not use the default, substitute your installation directory for /opt/cariden
- `$CARIDEN_HOME`—Directory in which the WAE Design, WAE Live, and WAE Collector executables and binaries are installed. The default is `/opt/cariden/software/mate/current`.

Step 1 Copy the snapshot_inventory_inc and snapshot_inventory.txt files from $CARIDEN_HOME/etc to $CARIDEN_ROOT/etc.

```
cp $CARIDEN_HOME/etc/snapshot_hardware_inventory* $CARIDEN_ROOT/etc
```

Step 2 To collect hardware inventory, enter the following command:

```
snapshot -config-file $CARIDEN_ROOT/etc/snapshot_hardware_inventory.txt
```

Note You might see errors because of third-party devices. You can ignore these errors.

Step 3 Check the output for errors, fix them if needed, and rerun this test until it is successful before proceeding.

Step 4 Create a cron job that repeats the process of creating snapshots to collect hardware inventory and inserting them into the WAE Live data store once a day.

Both `CARIDEN_ROOT` and `CARIDEN_HOME` variables must be defined from within the crontab. We recommend that you place these definitions at the top of the crontab because they are used globally within multiple crontab commands.

You cannot use `CARIDEN_HOME=$CARIDEN_ROOT/software/mate/current`. For example, you cannot use `$CARIDEN_HOME/bin/snapshot -config-file $CARIDEN_ROOT/etc/snapshot_hardware_inventory.txt` unless `$CARIDEN_HOME` and `$CARIDEN_ROOT` have been previously defined within crontab.

Open the file as follows.

```
crontab -e
```

At the end of the file, add the following lines:

```
CARIDEN_ROOT=/opt/cariden
CARIDEN_HOME=/opt/cariden/software/mate/current
0 0 * * * $CARIDEN_HOME/bin/snapshot -config-file $CARIDEN_ROOT/etc/snapshot_inventory.txt
2>&1
```

Customizing and Understanding Hardware Inventory Collection

Inventory collection collects and processes network hardware information to create the NetIntNodeInventory table used by WAE Live to produce inventory reports.

The following table lists the tasks that are performed in the snapshot_hardware_inventory.txt file and some of the options that can be edited in the snapshot_hardware_inventory.inc file.

Task	Description/Notes
COLLECTOR_GETPLAN	Calls the plan file.
GET_INVENTORY	Collects the network hardware and creates NetIntHardware tables that contain every device collected from MIB walks segregated by object type. The `get_inventory` tool also uses SSH and NETCONF to collect data that is not available in MIBs. To allow logging in to the router to collect inventory data, you can set the `get_inventory -login-allowed` option to `true`. By default, it is set to `true`.
BUILD_INVENTORY	Processes the raw hardware data information in the NetIntHardware* tables) to categorize and remove unwanted objects in the final NetIntNodeInventory table. To broaden the search when processing raw inventory data, you can set the `build_inventory -guess-template-if-nomatch` option to `true`.
MATE_CONVERT	Converts the plan .txt file to a .pln file
ML_INSERT_CTL	Inserts and schedules the insertion of inventory data into the WAE Inventory data store.

Collected Hardware

The `get_inventory` tool creates a series of NetIntHardware* tables that store the collected hardware information based on hardware type. While these tables are not directly usable by WAE Live, four of them are processed by `build_inventory` for use in WAE Live. 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 linecards, 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 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 instance, a module representing a linecard 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 `build_inventory` tool 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 `build_inventory` tool constructs the NetIntNodeInventory table by processing the NetIntHardware* tables. The tool requires two configuration files and can additionally use an optional one. If not specified, the files included in the `$CARIDEN_HOME/etc/inventory` are used.

- master_inventory_templates.txt (required)—This file contains these tables.
  - HWInventoryTemplates entries categorize the devices in the final NetIntNodeInventory table, as well as prune from inclusion.
  - HWNameFormatRules entries format hardware object names to make them more usable, as well as correct unexpected SNMP results.
- master_exclude_list.txt (required)—Contains the ExcludeHWList table that prevents (blacklists) 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.
- master_hw_spec.txt (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, you will want these changes to persist across software upgrades. To do so, you must move these files from $CARIDEN_HOME to $CARIDEN_ROOT and update the snapshot files accordingly.

1. Copy $CARIDEN_HOME/etc/inventory to $CARIDEN_ROOT/etc:

   ```
   cp -r $CARIDEN_HOME/etc/inventory $CARIDEN_ROOT/etc
   ```

2. Copy $CARIDEN_HOME/etc/snapshot_hardware_inventory.txt and .inc to $CARIDEN_ROOT/etc/inventory:

   ```
   cp $CARIDEN_HOME/etc/snapshot_hardware_inventory.*
   $CARIDEN_ROOT/etc/inventory/
   ```

3. Run the snapshot manually:

   ```
   $CARIDEN_HOME/bin/snapshot -config-file
   ```

```
$CARIDEN_ROOT/etc/inventory/snapshot_hardware_inventory.txt
```

4. Schedule the snapshot in crontab:

```
0 0 * * * $CARIDEN_HOME/bin/snapshot -config-file
$CARIDEN_ROOT/etc/inventory/snapshot_hardware_inventory.txt 2>$1t
```

Configure Hardware Templates

The `build_inventory -template-file` option calls a file containing both the HWInventoryTemplates and the HWNameFormatRules tables, which by default are in the `$CARIDEN_HOME/etc/inventory/master_inventory_templates.txt` file.

HWInventoryTemplates Table

The HWInventoryTemplates table tells the `build_inventory` tool how to interpret hardware referenced by the NetIntHardware* tables. It enables `build_inventory` 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, linecard, 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 linecard. All other hardware objects are categorized by their same name. For instance, a chassis is categorized as a chassis. These categorized hardware objects are available through the WAE Live application for use in inventory reports.

The build_inventory tool 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-if-nomatch true` option. In this instance, if no matches are found using the first two criteria, WAE 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 `build_inventory` how to categorize the hardware. These latter columns identify hardware object types: chassis, slot, linecard, module slot, module, port slot, port, or transceiver. Each column entry has the following format. For an example, see Figure 2-4.

Type,Identifier,Name

- 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 and thus, in WAE Live inventory reports.

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, `build_inventory` does not include it in the final NetIntNodeInventory table.

Example

Using the first row of the default master_inventory_templates.txt file, WAE Collector searches the NetIntHardware* tables for ones that have entries that match the Vendor, Model, and DiscoveredHWHierarchy columns, as follows.

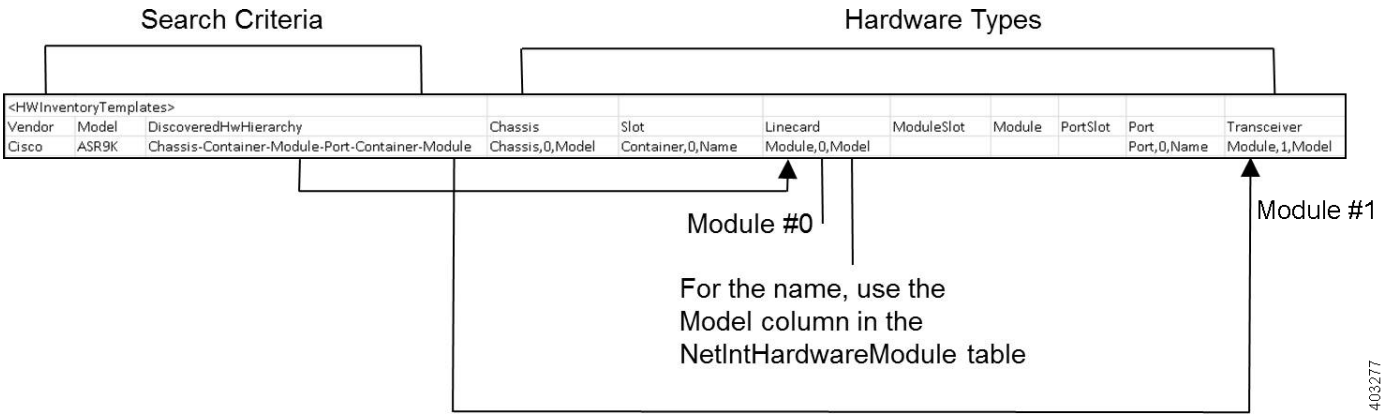
Cisco ASR9K Chassis-Container-Module-Port-Container-Module

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 linecard, 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.

Figure 2-4 Example HWInventoryTemplates Entry



Add HWInventoryTemplates Entries

If WAE 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.

Step 1 Copy the warning message for reference, and use it for Step 2.

Step 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.

Step 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.

Step 4 Once each object in the hardware hierarchy is found, add it to the DiscoveredHWHierarchy column of the HWInventoryTemplates table. Also complete the Vendor and Model columns.

Step 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: 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.

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

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 in WAE Live inventory reports.

Exclude Hardware by Model or Name

The `build_inventory -exclude-file` option calls a file containing the ExcludeHWList table, which by default is in the `$CARIDEN_HOME/etc/inventory/master_exclude_list.txt` file. 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: 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.

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

HardwareSpec

The `build_inventory -hardware-spec-file` option calls a file containing the HardwareSpec table, which by default is in the `$CARIDEN_HOME/etc/inventory/master_hw_spec.txt` file. 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, linecard, or module. SlotNum indicates the slot number range. For instance, some routers start with slot 0, whereas others start with slot 1.

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

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

Troubleshooting Collection

When collecting network information using the WAE Collector UI, you can use the WAE Collector UI to check for node access failures, nodes that are not responding, or other problems with collecting data. Using this information, you can correct the problems, often by setting override rules for problematic nodes or changing the global rules for collecting data. For example, if nodes with SNMP community strings differ from the majority of the discovered nodes, you can individually configure them to use specific SNMP community strings. Once such changes are applied, they take effect for the next instance of data collection.

WAE Collector Server Logging

On the Schedule page, you can configure the Collector server to generate detailed log files that are viewable on both the Status and Log pages.

If you need to contact Cisco support, we recommend that you first run Download Diagnostics or `mate_tech_support`, and send the resulting file to your representative.

- On the Status page, use the Download Diagnostics feature to create a .zip file containing the state of the local Collector server during the last collection.
- The `mate_tech_support` tool creates .tar file containing information for the Collector server, WAE NI server, WAE Core server, and WAE Live. Note this tool is applicable only if all three servers are on the same local device. For information on `mate_tech_support`, refer to its `-help` output.

For all event logs of all servers in an HA environment, go to the WAE Statistics > Events page. For diagnostic and process status information for all servers, go to the WAE Statistics > Diagnostics and WAE Statistics > Processes page, respectively.

WAE NI Logging

The WAE NI log file is located in `$WAE_ROOT/logs/wae-ni/collector-core.log`.

To change the log level at runtime, edit `$WAE_HOME/wae-ni/etc org.ops4j.pax.loggin.cfg`. Edit the `log4j.ogger.com.cisco=<log_level>` parameter where <log_level> is the minimum severity level you want displayed. For example, if `log4j.ogger.com.cisco=DEBUG`, then all severity levels set to DEBUG or higher will be captured during runtime. The log level severities are listed in the following order (from highest to lowest): FATAL, ERROR, WARN, INFO, and DEBUG.