# Troubleshoot Network Devices Using Network Reasoner

## About Network Reasoner

The Network Reasoner tool allows you to troubleshoot various issues on your network quickly. In the Cisco DNA Center GUI, click the **Menu** icon ( ≡ ) and choose **Tools** > **Network Reasoner** to launch the Network Reasoner Dashboard. The Network Reasoner dashboard hosts separate workflows using which you can proactively troubleshoot the network issues. The dashboard provides a brief description about the workflows, the number of affected devices in the last 24 hours, and impact of running a workflow on a network.

**Note** You must install the Machine Reasoning package to view the Network Reasoner feature under the Tools menu. For more information, see the Cisco DNA Center Administrator Guide.

## Validate Cisco SD-Access Migration Using the MRE Workflow

The following MRE workflows assist in planning your migration to Cisco SD-Access:

- SDA Hardware Readiness Check

- SDA Software Readiness Check

- Redundant Link Check

- L3 Access Check

- MTU Link Check

- SDA Health Check

- SDA Scale Limits Check

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon ( ☰ ) and choose **Tools** > **Network Reasoner**.

**Step 2** In the **Network Reasoner** dashboard, click the following workflows as required:

| Workflow | Description | Action |
|---|---|---|
| SDA Hardware Readiness Check | Checks whether the hardware is ready for Cisco SD-Access migration. | a. Click **SDA Hardware Readiness Check**.<br><br>b. Click **Run Machine Reasoning**. |
| SDA Software Readiness Check | Checks whether the software is ready for Cisco SD-Access migration. | a. Click **SDA Software Readiness Check**.<br><br>b. Click **Run Machine Reasoning**. |
| Redundant Link Check | Checks whether any redundant uplinks are present in your device and if there are ways to increase availability by configuring redundant uplinks on the access switches. | a. Click **Redundant Link Check**.<br><br>b. Select an appropriate device.<br><br>c. Click **Troubleshoot**. |
| L3 Access Check | Checks whether your network has access switches that are running Layer 3 routing protocols to move to Cisco SD-Access with minimal design changes. | a. Click **L3 Access Check**.<br><br>b. Select an appropriate device.<br><br>c. Click **Troubleshoot**. |
| MTU Link Check | Checks whether the links between the main network devices and the access, core, and other switches are configured with the correct MTU. | a. Click **MTU Link Check**.<br><br>b. Select an appropriate device.<br><br>c. Click **Troubleshoot**. |
| SDA Health Check: Fabric Count | Checks the health of the Cisco DNA Center cluster to determine whether it is reaching any scale limit thresholds due to managing fabrics. | a. Click **Fabric Count**.<br><br>b. Click **Run Machine Reasoning**. |
| SDA Health Check: SDA Scale Limits Check | Checks whether the number of client endpoints, network devices, and configured fabrics in Cisco DNA Center are within the published SDA limits. | a. Click **SDA Scale Limits Check**.<br><br>b. Click **Run Machine Reasoning**. |

| Workflow | Description | Action |
|---|---|---|
| SDA Health Check: Client Count | Checks the health of the Cisco DNA Center cluster to determine whether it is reaching any scale limit thresholds due to managing clients. | a. Click **Client Count**.<br>b. Click **Run Machine Reasoning**. |
| SDA Health Check: Device Count | Checks the health of the Cisco DNA Center cluster to determine whether it is reaching any scale limit thresholds due to managing network devices. | a. Click **Device Count**.<br>b. Click **Run Machine Reasoning**. |

# Troubleshoot High CPU Utilization

CPU utilization troubleshooting support is available only for the following network devices with software version 16.9.3 and later:

- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 3650 Series Switches

### Before you begin

- Install the Machine Reasoning package. See Download and Install Packages and Updates in the Cisco DNA Center Administrator Guide.
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the Cisco DNA Center Administrator Guide.

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon ( ≡ ) and choose **Tools** > **Network Reasoner**.

**Step 2** Click the **CPU Utilization** tab.

The **CPU Utilization** page displays the filtered list of devices with high CPU utilization in the past 24 hours.

Click **All** to see the list of all devices from the inventory, and you can choose any device to run the workflow.

**Step 3** Choose the device that you want to troubleshoot.

Click **Filter** and enter the devices by entering **Tag**, **Device Name**, **IP Address**, **Device Type**, **Site**, or **Reachability**.

**Step 4** Click **Troubleshoot**.

**Step 5** In the **Reasoner Input** window, enter the **CPU Utilization Threshold** percentage that you want to check against.

**Step 6** Click **Run Machine Reasoning**.

**Note** The following processes, if observed, are considered for detailed analysis:

- **MATM Process Group**: MATM RP Shim, NGWC Learning, and VMATM Callback

- **IOSXE Process Group**: IP Input, ARP Input, IOSXE-RP Punt Se, SISF Main Thread, DAI Packet, and ARP Snoop

The **CPU Utilization** window appears, where you can see the **Root Cause Analysis** of the high CPU utilization for the chosen device.

The **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process.

**Step 7** (Optional) Click **Stop** to stop the ongoing reasoning activity.

**Step 8** Click the **Conclusion** tab to see the processes that consume more CPU and the utilization percentage.

**Step 9** Click **View Relevant Activities** for each process to view the **Activity Details** in the right pane.

**Step 10** (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.

**Note** The Machine Reasoning Engine (MRE) implements a system-terminate algorithm that detects and terminates network reasoner workflows when thresholds exceed a specified level, or when no events are received from the timeout request for inactivity.

# Troubleshoot a Power Supply Failure

Power supply troubleshooting workflow support is available only for the following network devices with software version 16.6.1 and later:

- Cisco Catalyst 3650 Series Switches

- Cisco Catalyst 3850 Series Switches

- Cisco Catalyst 9300 Series Switches

- Cisco Catalyst 9400 Series Switches

- Cisco Catalyst 9500 Series Switches

**Before you begin**

- Install the Machine Reasoning package. See Download and Install Packages and Updates in the Cisco DNA Center Administrator Guide.

- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the Cisco DNA Center Administrator Guide.

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon ( ≡ ) and choose **Tools** > **Network Reasoner**.

**Step 2** Click the **Power Supply** tab.

The **Power Supply** page displays the filtered list of devices with power supply failures in the past 24 hours.

Click **All** to see the list of all devices in the inventory. You can choose any device to run the workflow.

**Step 3**    Choose the device that you want to troubleshoot.

Click **Filter** and filter the devices by entering **Tag**, **Device Name**, **IP Address**, **Device Type**, **Site**, or **Reachability**.

**Step 4**    Click **Troubleshoot**.

The **Power Supply** window appears, where you can see the **Root Cause Analysis** of the power supply failure for the chosen device.

The **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process.

**Step 5**    (Optional) Click **Stop** to stop the ongoing reasoning activity.

**Step 6**    Click the **Conclusion** tab to see the **Stack Identifier**, **Product ID**, **Serial Number**, and **Status** of the power supply for the chosen device and the suggested action.

**Step 7**    Click **View Relevant Activities** for each stack identifier to view the **Activity Details** in the right pane.

**Step 8**    (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.

**Note**         The MRE implements a system-terminate algorithm that detects and terminates network reasoner workflows when thresholds exceed a specified level, or when no events are received from the timeout request for inactivity.

# Troubleshoot a Downed Interface

Interface down troubleshooting workflow support is available only for the following network devices with software version 16.9.3, and later:

- Cisco Catalyst 3650 Series Switches

- Cisco Catalyst 3850 Series Switches

- Cisco Catalyst 9300 Series Switches

- Cisco Catalyst 9400 Series Switches

- Cisco Catalyst 9500 Series Switches

**Before you begin**

- Install the Machine Reasoning package. See Download and Install Packages and Updates in the Cisco DNA Center Administrator Guide.

- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the Cisco DNA Center Administrator Guide.

**Step 1**    In the Cisco DNA Center GUI, click the **Menu** icon ( ≡ ) and choose **Tools** > **Network Reasoner**.

**Step 2**    Click the **Interface Down** tab.

The **Interface Down** page displays the filtered list of devices with an interface that went down in the past 24 hours.

Click **All** to see the list of all devices from the inventory, and you can choose any device to run the workflow.

**Step 3**    Choose the device that you want to troubleshoot.

Click **Filter** and enter the devices by entering **Tag**, **Device Name**, **IP Address**, **Device Type**, **Site**, or **Reachability**.

**Step 4**    Click **Troubleshoot**.

**Step 5**    In the **Reasoner Input** window, enter the interface name that you suspect has issues.

**Step 6**    Click **Run Machine Reasoning**.

The **Interface Down** window appears, where you can see the **Root Cause Analysis** of the downed interface for the chosen device.

The **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process.

**Step 7**    (Optional) Click **Stop** to stop the ongoing reasoning activity.

**Step 8**    Click the **Conclusion** tab to see the potential root causes for the interface down issue and the suggested action.

**Step 9**    Click **View Relevant Activities** for each root cause analysis to view the **Activity Details** in the right pane.

**Step 10**    (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.

**Note**    The MRE implements a system-terminate algorithm that detects and terminates network reasoner workflows when thresholds exceed a specified level, or when no events are received from the timeout request for inactivity.

# Troubleshoot Network Connectivity

Only the following network devices running Cisco IOS-XE software version 16.9.3 or later support the network connectivity troubleshooting :

- Cisco Catalyst 9200 Series Switches

- Cisco Catalyst 9300 Series Switches

- Cisco Catalyst 9400 Series Switches

- Cisco Catalyst 9500 Series Switches

- Cisco Catalyst 9600 Series Switches

Use the following procedure to check the reachability of an end point from a device using IP address:

**Before you begin**

- Install the Machine Reasoning package. See Download and Install Packages and Updates in the Cisco DNA Center Administrator Guide.

- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the Cisco DNA Center Administrator Guide.

**Step 1**    In the Cisco DNA Center GUI, click the **Menu** icon ( ≡ ) and choose **Tools** > **Network Reasoner**.

**Step 2**   Click the **Network Connectivity** tab.

**Step 3**   You can view the device table with details, such as **Device Name**, **IP Address**, **Device Type**, **Site**, **Reachability**, **Role**, and **Platform**.

**Step 4**   Select a device and click **Troubleshoot**.
The **Reasoner Inputs** dialog box is displayed.

**Step 5**   In the **Destination IP address** field, enter a valid IP address and click **Run Machine Reasoning**.

> **Note**        Provide the Virtual Routing and Forwarding (VRF) name, if applicable.

**Step 6**   In the **Root Cause Analysis** window, under **Reasoning Activity**, you can view various workflows that are validated as a part of the troubleshooting process.

**Step 7**   In the **Conclusions** tab, you can view the status of the validation check and the suggested action.

# Troubleshoot IP Connectivity of a Device

As ping is a simple command, IP connectivity troubleshooting support is available for all the network devices.

**Before you begin**

- Install the Machine Reasoning package. See Download and Install Packages and Updates in the Cisco DNA Center Administrator Guide.

- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the Cisco DNA Center Administrator Guide.

**Step 1**   In the Cisco DNA Center GUI, click the **Menu** icon ( ☰ ) and choose **Tools** > **Network Reasoner**.

**Step 2**   In the **Network Reasoner** dashboard, click **Ping Device**.

**Step 3**   In the **Devices** window, choose a device and click **Troubleshoot**.

**Step 4**   In the **Reasoner Inputs** window, enter **Target IP Address** and click **Run Machine Reasoning**.

**Step 5**   Click **View Details** to view the ping status.

# Enable Network Bug Identifier

Cisco DNA Center network bug identifier tool allows you to scan the network for a selected set of defects or bugs that have been identified previously and are known to Cisco.

The Cisco DNA Center network bug identifier helps in identifying specific patterns in the device configuration or in the operational data of the device and matches them with known defects based on those patterns. This tool provides the following views:

- Bugs focused

- Device focused

The following procedure explains how to identify bugs using the network bug identifier tool:

### Before you begin

- Install the Cisco DNA Center core package. See Download and Install Packages and Updates in the *Cisco DNA Center Administrator Guide*.

- Install the Machine Reasoning package. See Download and Install Packages and Updates in the *Cisco DNA Center Administrator Guide*.

**Step 1**  In the Cisco DNA Center GUI, click the **Menu** icon ( ≡ ) and choose **Tools** > **Network Reasoner**.

**Step 2**  Select **Network Bug Identifier**.

**Step 3**  Click **Scan Network**.

**Step 4**  In the **Scan Network** window, do any one of the following:

- To scan your system for bugs immediately, click the **Now** radio button and click **Submit**.

- To schedule the scan for a later date and time, click the **Later** radio button and specify date and time.

The dashboard progress indicator shows the list of devices scanned in batches of 10.

**Step 5**  In the **Network Bug Identifier** page, click **Bugs on Devices** to view the following details:

- **Bug ID**

- **Affected Devices**

- **Severity**

- **Affected Versions**

- **Workaround**

**Step 6**  Click on the number of **Affected Devices** against a specific **Bug ID** to view the complete details of that devices affected by the bugs.

**Step 7**  In the **Network Bug Identifier** window, click **Affected Devices** to view the following details:

- **Device Name**

- **IP Address**

- **Device Type**

- **Site**

- **Reachability**

- **Bugs**

- **Image Version**

**Step 8**  Click the **Bugs** value against a specific **Device Name** to view the complete details about the bugs associated with the devices.

**Step 9** Click the Information icon against **BUG SUMMARY** and then click **View All** to view the full subset of bugs supported by Cisco Machine Reasoning Engine (MRE).

**Note** The current capability of this tool is limited to switches and routers running **IOS**- or **IOS-XE**-based images.

# Enable System Bug Identifier

The **System Bug Identifier** tool provides an option to identify bugs in the Cisco DNA Center. The following procedure explains how to enable the **System Bug Identifier** tool:

**Before you begin**

- Install the Cisco DNA Center core package. See Download and Install Packages and Updates in the *Cisco DNA Center Administrator Guide*.

- Install the Machine Reasoning package. See Download and Install Packages and Updates in the *Cisco DNA Center Administrator Guide*.

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon ( ≡ ) and choose **Tools** > **Network Reasoner**.

**Step 2** Select **System Bug Identifier**.

**Step 3** Click **Scan System**.

**Step 4** In the **Scan System** window, do any on the following:

 a. To scan your system for bugs immediately, click the **Now** radio button and click **Submit**

 b. To schedule the scan for a later date and time, click the **Later** radio button and specify date and time.

**Step 5** The **System Bug Identifier** page shows the **BUG SUMMARY** and the **Bugs Identified on Your System** table.

You can view the following details in the **Bugs Identified on Your System** table:

- **Bug ID**

- **Name**

- **Severity**

- **First identified**

- **Last identified**

- **Identified frequency**

- **Workaround**

- **Affected Versions**

**Step 6** Click the **Bug ID**.
The **Bug Details** dialog box appears and displays the details of the bug.

**Step 7** Click the arrow next to **Bug ID** and to go to the **Bug Search Tools** page, which shows more details about the bugs.