Navigating Assurance Network Health

Cisco DNA Center 1.2 Training
Contents

Basics
Why Is It Important?
Where Does It Happen?
What Skills Do I Need?
  Basic
  Proficient
What Terms Should I Know?
  Device Not Monitored / Unmonitored
  Device Role
  Fabric Domain
  MAP Server or MSMR Server on Control Plane Devices
  Network Hierarchy

Evaluating the Big Picture…
…on the Network Health Page.
What Will I See?
For SD-Access Deployments, Where Do I Find Fabric-Related Device Data?
What Will I See…
  …On the Geographical Map?
  …In the List View?
  …In the Topology View?
What Are the Common Page Features?
  Dashlet Chart Elements on the Network Health Page and Panels
  Detailed Information Panels
  Device Lists
How Can I Position Dashlets?
What Affects the Information That I Am Seeing?
  Time Stamps and Time Periods
  Changing the Time Period
  Persistent Filters on Page Navigation

How are Device Health Metrics Looking?
Get a Summary View of Device Health
What Will I See?
Where Do I Find…
  …The Health of Network Devices by Device Type?
    The Network Health by Device Role/Type Dashlet
    The Wireless WLC System Health Panel
    The System Health Panel for APs, Routers, and Switches
    The Wireless WLC Data Plane Connectivity Health Panel
    The AP Data Plane Connectivity Panel
Navigating Assurance Network Health

How is a Specific Network Device Doing?

Get a Holistic View on the Device 360

What Will I See?

How Do I Open a Device 360 Page…

...By Using the Global Search Function?
...By Using a Device Name Link?
...In the Topology View?

Where Do I Find…

...Issues That Are Affecting the Device?
...A List of Resolved Issues and Their Details?
...The Connections of the Device to Its Neighbors?
...The Tool for Evaluating the Path That Traffic Is Using?

Path Traces for Flow Mapping and Path Health
Unmanaged Devices in Traffic Paths
How Do I Prepare To Run a Path Trace?
How Do I Run a Path Trace?

...More Metrics and Detailed Information?

The Detail Information Section for Routers and Switches
The Detail Information for WLCs
The Detail Information for Access Points

What Was a Network Device Experiencing at a Certain Time?

Watch It Happen in DNA Center

Video

Evaluating a System User's Printer Connection (8:00)

Want More?

Find Product Information
Find Training
Contact Us About This Training
Basics

Why Is It Important?

Cisco DNA Center Assurance provides comprehensive functionality that helps you to ensure higher and more consistent service levels to meet growing business demands.

By correlating information from network devices and contextual sources, Cisco DNA Center delivers network monitoring results and proactive insights into:

- Network health, including
  - Routers.
  - Switches.
  - Wireless LAN controllers (WLCs).
  - Access points (APs).
- Potential or active network infrastructure issues or failures that can affect network or business operations.

Managing the network infrastructure that supports network traffic is key to:

- Ensuring that network devices meet performance, response, and operational requirements.
- Avoiding or mitigating network disruption.

Assurance presents detailed metrics, data, and history on network devices, including:

- Device health based on device types and their traffic management roles, referred to as device or network roles, on the network.
- Access Point (AP) analytics with network connectivity details and information about the APs most in use on the network.

Managing network devices effectively is critical to:

- Ensuring network service levels, network security, and end users’ network experiences.
- Managing enterprise operations.
- Proactively planning for network growth.
This training introduces you to:

- The types and levels of information that the Network Health page provides.
- The organization and layout of page features.
- General navigation and functions that you can use to access the information that you need.

**Important Note:** The functionality that you see and the tasks that you can perform depend on the system's licensing and configuration, and on your system user role.

To recognize the overarching features and navigation that are available in Assurance, review the Assurance Features and Navigation training.

It addresses such key concepts as:

- The automated Assurance data processing workflow.
- Health scoring.
- Time stamps and data aging.
- Geographical map and table view navigation.
- Steps to change data time periods and perform searches.
Where Does It Happen?

You can view device insights, health states, and performance metrics on the **Network Health** page for the NetFlow-enabled routers, switches, wireless LAN controllers, and access points that the system is managing.

**Note:** Assurance also provides the **Device 360** page for detailed health and metrics about a specific network device.
The **Assurance | Overall Health** page provides several methods by which you can open **Network Health**:

- **On the menu bar:**
  - On the **Health** menu, select **Network**.

- **In the Overall Health Summary dashlet:**
  - Below **Network**, click **View Network Health**.
When you use the menu or dashlet methods of navigation, the system opens the **Network Health** page and, by default, presents the health states and metrics for the previous 24-hour period for devices:

- In all of the locations **in the network hierarchy**.
- In SD-Access deployments, for all of the fabric domains.

You also can open **Network Health** so that it presents the data for a specific location in the network hierarchy automatically.

These methods are available on the geographical map and in the list view on the collapsed dashlet on the **Overall Health** page.

To open Network Health by using the dashlet toolbar:

- On the collapsed dashlet, click the list view or geographical map button.

To open Network Health by using the geographical map:

1. For the location of interest, zoom the map view to a single location level.
2. Click the location health indicator.
   - A pop-up window opens.
3. In the pop-up window, click **Network Devices**.
To open Network Health in the list view:

- Under **Network Health**, in the row of the location of interest, click the link.

When you use the map or list methods of navigation, the system opens the **Network Health** page and, by default, presents the health states and metrics for the previous 24-hour period for devices the specific location that you selected in the network hierarchy.
What Skills Do I Need?

To recognize, evaluate, and manage Assurance Network Health, you need the following experience.

Basic

- Practical network and LAN or WAN management experience
- Cisco Internetwork Operating System (IOS) concepts

Proficient

- Cisco DNA Center user interface and navigation
- OSI model
- Network hardware design and concepts
- Networking concepts

What Terms Should I Know?

Device Not Monitored / Unmonitored

Network health dashlets and lists include a Device Not Monitored status, which indicates the number or lists the network devices for which the system is managing, but is not collecting, telemetry data.

The terms are used interchangeably in the interface.

When you identify devices from which you need to see Assurance data that are in an unmonitored state, you can evaluate the device’s reachability and management statuses in Inventory, which can help provide insight into the unmonitored status.
Device Role

The location on the network where the device manages traffic.

For example, a router has the role of a border router when it manages traffic between the enterprise network and external networks or the role of a core router when it manages traffic within the enterprise network only.

Fabric Domain

A virtual network in a fabric topology, running over the physical infrastructure.

MAP Server or MSMR Server on Control Plane Devices

Fabric topologies use devices that are assigned control plane roles in the fabric to map and resolve the locations of devices on the network by using an internal MAP server function, sometimes referred to as an MSMR.

The interface interchanges the terms control plane and MSMR server. Other documentation can refer to the MAP server.

This document applies the term control plane.

Network Hierarchy

As an initial system configuration task, system users organize the network hierarchy, which arranges enterprise locations based on their geographical or organizational relationships. These relationships can include many sites, buildings at each site, and floors in each building in parent/child arrangements.

In the configuration and provisioning processes, system users assign devices to locations in the hierarchy.

Then Assurance organizes information based on the network hierarchy in various areas of Network Health to support the ability to identify locations or problem areas more easily.
Evaluating the Big Picture…

…on the Network Health Page.

What Will I See?

Filters and a timeline to control the information that Network Health displays

Collapsed dashlet with the geographical map, list view, and topology

A summary of device health states

Health states and metrics for each device type with links to details, possible issues, and tests

Access point statuses

A list of devices active with links to Device 360 pages
For SD-Access Deployments, Where Do I Find Fabric-Related Device Data?

To support SD-Access deployment, you also can review the health and metrics for network devices based on the fabric topology or topologies that they support.

**Note:** When Cisco DNA Center does not have fabric names, the drop-down list includes the **All Domains** selection only.

When you open **Network Health**, the page displays all network devices for all domains by default. You can use the domain drop-down list to filter the page to display the devices that support a specific domain and their associated data.

To review metrics and devices that support a specific fabric topology:

- In the domain drop-down list, select the fabric topology domain name.

The page updates all of the dashlets and the **Network Devices** list to display the associated data only.

**Important Note:** The fabric domains drop-down list is the only indicator on the page that the information is filtered. And, when you select a specific fabric domain on the **Network Health** page, it retains the change when you navigate away from it.

**Tip:** Always refer to the drop-down list to determine the fabric topology domain for which the page is displaying data.
What Will I See…

…On the Geographical Map?

The geographical map displays a visual representation of the device health states of the enterprise network, indicating each enterprise location, based on the network hierarchy, the zoom level of the map, and the other settings that can affect what you see.

Notes: The system collects sites’ network health metrics in approximately 5 minute intervals, varying based on back end data collection and database save intervals.

To ensure that you are seeing the latest data, refresh the page manually.

The location level health indicators are non-interactive.

The geographical map is available on the collapsed dashlet below the timeline.

To open the geographical map:

- On the collapsed dashlet, click the geographical map button.
...In the List View?

The list view applies a table layout to present device health states and selects the Hierarchical Site View by default, which organizes the list by the enterprise locations in the network hierarchy.

For each location, it organizes the health score indicators by device type and includes data based on the other settings that can affect what you see.

When you navigate to Network Health by using the menu or dashlet method, it indicates the health states combined for all sites.

![Data for all sites organized based on the network hierarchy](image1)

When you navigate to Network Health by using the geographical map or list method, the list selects and applies that location’s data.

![Data for a single site organized based on the network hierarchy](image2)

The list view is available on the collapsed dashlet below the timeline.

To open the list view:

- On the collapsed dashlet, click the list view button.
The list view indicates the percentage of the total number of devices that are in a healthy state in the **All** column. Parent locations’ percentages indicate the number of healthy network devices at the parent level, including all of its child locations.

It also breaks out the percentages of healthy devices at each location level by device type.

**Note:** The system collects sites’ network health metrics in approximately 5 minute intervals, varying based on back end data collection and database save intervals. To ensure that you are seeing the latest data, refresh the page manually.

You also can select the **Building View** layout, which organizes the list by building. When location groups have child sites or multiple buildings, each building is a separate line item in the list.

It also includes an entry for all of the buildings in the network hierarchy.
To review location level health metrics:

- Under **Apply to Page Location**, in the row of the location of interest, click **Apply**.

<table>
<thead>
<tr>
<th>Location</th>
<th>Network Health (%) Healthy Devices</th>
<th>Network Device Count</th>
<th>Apply</th>
<th>Apply</th>
<th>Applied</th>
<th>Apply</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netherlands</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All Sites</td>
<td>67% 100% -- -- -- 50% -- 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>USA</td>
<td>83% 50% 100% 100% 100% 80% -- 23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canada</td>
<td>100% 100% -- -- -- -- -- 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To review location level data for a child location:

- Expand the parent location, and then, in the applicable row, click **Apply**.

  The **Apply** link toggles to **Applied** and disables the link.

<table>
<thead>
<tr>
<th>Location</th>
<th>Network Health (%) Healthy Devices</th>
<th>Network Device Count</th>
<th>Apply</th>
<th>Apply</th>
<th>Applied</th>
<th>Apply</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Sites</td>
<td>63% 100% 100% 100% 0% -- 31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>USA</td>
<td>89% 60% 100% 100% 100% -- 18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SM</td>
<td>33% 0% -- 100% -- -- 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DC</td>
<td>100% -- 100% 100% 100% -- -- 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The page updates all of the dashlets and the **Network Devices** list to display the associated data only.

**Important Note:** When you change the location in the list view, the system applies the change to all of the dashlets. The **Network Health** page retains the change when you navigate away from it.
When you have a long list of locations, or are looking for specific data, you can use the search function to filter the list.

To filter the list:

- In the **Find** field, begin typing a character string that the data includes.

As you type, the list updates to display all of the items that match the criteria.
...In the Topology View?

The topology view presents and organizes the devices in the topology based on the device roles that the system assigns during device discovery or that a system user changed manually after discovery.

The topology view is available on the collapsed dashlet below the timeline.

To open the topology view:

- On the collapsed dashlet, click the topology view button.

When you open the topology view, the page displays the network topology in a horizontal layout.
When the topology is complex, you can use the search feature to find a specific device.

**To search the topology for a device:**

- In the **Search Topology** field, begin typing the device name or IP address.

As you type, a drop-down list opens with all of the devices matching the character string.

**Tip:** If you have searched for and do not see a device that you expect, open **Inventory** to see if the device is listed, reachable, and in a managed state.

Beside each device, the topology view displays its health score.
You can expand device groups vertically to see all of their associated devices at a sibling level in the hierarchy…

…to see devices and their health scores.

…or expand a group horizontally to see associated devices at a child level in the hierarchy.

You can click the **Toggle Layout** button to change the layout to a horizontal orientation…
…or a vertical orientation.

**Toggle Layout button**
To see a device’s name, role, IP address, and software version:

- Point to the device icon.

A pop-up window opens with the information. It also provides access to the associated Device 360 page.

**Note:** For more information on the Device 360 page, refer to the How is a Specific Network Device Doing? topic.
What Are the Common Page Features?

Dashlet Chart Elements on the Network Health Page and Panels

Chart elements include time interval tabs. Based on the time interval and the type of network device, the dashlet displays different chart types, such as circle or bar charts.

**Note:** In addition to health states, charts can include a No Data state, which indicates the number of devices for which the system has not collected telemetry data for the most recent data collection cycle.

When no telemetry data is available, the system indicates that the device is unmonitored, or not monitored.

**Tip:** In many cases, this state is transient and resolves on its own. If you want to investigate whether the system is capturing issues for a device, you can open the related Device 360 page.
For more information about a specific data element on the chart, you can point to it. This action opens a pop-up window with such details as affected numbers or percentages of devices, or of the metrics that the element represents.

**Detailed Information Panels**

Most Network Health dashlets provide access to detailed information on panels by using their View Details or device type-specific links.
When you click **View Details**, the system opens a panel that overlays the page.

On the **Network Health** dashlet, the **Wireless** tab has device type-specific links to open the associated device details in a panel.

On the **Wireless** tab, click the WLC or AP link for device-specific details.
Panels include charts displaying related information. Some charts provide tabs that display the chart data information based on time intervals.

Some charts display color-coding to help distinguish what the segments represent, for example, health states or metrics.

Some charts are interactive based on point or click actions.
Based on the panel that you open, data filters affect the information that is visible in Device Distribution and the device list.

For example, when you open the Network Health Summary panel, the filters apply to show all of the devices that the system is monitoring that are in a poor health state.

**Note:** When no devices match the filter criteria that the panel has applied automatically, Device Distribution and the device list do not display data.
You can click a chart segment or any data filters to populate the Device Distribution charts and the device list with the data related to the specific element that you clicked or selected.

For example, when you click a chart element representing a good health state for data plane connectivity:

- The Data Plane Connectivity data filter changes to indicate the health state.
- The Device Distribution charts and device list update to display the applicable devices.

![Diagram showing the device distribution and data plane connectivity](image-url)
Panels also can contain tabs below the panel name so that you can see details based on metrics or connectivity in charts and in the device list.

The panels that are available on the **Network Health Summary** and **Network Health by Device Role/Type** dashlets include **Device Distribution** charts.

When you open a panel, **Device Distribution** is collapsed by default below the data filters.
Device Distribution displays data based on the combination of data filters that the dashlet applies automatically.

The device filters update to apply the applicable information, and Device Distribution updates to display associated devices organized in the following categories, which can be helpful for identifying specific device attributes that might be contributing to an issue.

- Type
- Model number
- Operating system

You also can click a chart segment to populate Device Distribution.
Device Lists

The Network Health page and all of the detailed information panels include a network device list. It lists network devices based on the data filters that are available for the list and any other active settings that are affecting what you see on the page and in the list. The system provides data filters based on the type of information the list is presenting.

For example, in the screenshot below, the data filters include: Device, Type, and Overall Health... …while the device list in the Distribution detailed information panel below provides the Device data filter and Data Plane Connectivity health state data filter.
You can apply data or attribute filters to find the specific information that you need.

To apply a data filter:

- Beside the filter category, click the filter, and then click **Apply**.

The metric indicator turns blue to indicate it is active, and the system filters the list to display those devices that meet the criteria.

You also can apply filters in combinations to find the information that you need.

The attribute filter provides a drop-down list for each column heading.
You can click an attribute to open the drop-down list. You can select the specific attribute for which you need to see associated devices, or begin typing a character string to find a specific item.

**Important Note:** The character string search is case sensitive.

You can define a series of attributes for a more specific list.

**To apply attribute filters:**
- Click **Filter**, in each drop-down list, type or select each attribute parameter, and then click **Apply**
When you apply attribute filters, they appear below the Filter link.

To clear a filter:

- Under Filter, click the X on the filter that you want to remove. The list updates automatically.

To support detailed monitoring or troubleshooting, you can click a device name link to navigate to its associated Device 360 page. The page provides a holistic view of the device, issues it is experiencing, and other details.

Note: For detailed information on the layout and contents of the Network Devices list on the Network Health page, refer to the The Network Devices List topic.
**How Can I Position Dashlets?**

You can change the positions of dashlets for optimal visibility.

When you change dashlet positions, the system retains the changes when you navigate away from the page or log out of the system. Changes that you make do not affect other users’ layouts.

**To change dashlet positions:**

1. In the **Actions** drop-down list, select **Edit Dashboard**.

The system makes the page available for changes and opens the **Cancel** and **Save** buttons.

2. Drag each dashlet to the position that you want, and then click **Save**.
What Affects the Information That I Am Seeing?

Time Stamps and Time Periods

**Network Health** provides a page level time stamp to indicate the last time that the page data was refreshed, which occurs when you first open the page or when you refresh the page manually.

This way, you can determine the age of the information and whether you need to update it manually.

**Note:** For detailed information on time stamps and data aging, refer to the **Time Stamp and Data Aging Concepts** topic in the **Assurance Features and Navigation** training.

When you open the **Network Health** page, the system displays data for the previous 24 hours up to the current system time of the device that you are using by default.

The ending time of the time period applied to the page appears at the top of each dashlet and each dashlet includes metrics up to that ending time.

**Important Note:** The time period drop-down list and the timeline slider work together to affect the time period for which you are seeing data.

For example, you can select an earlier date or date range in the drop-down list, and then refine the time period further by using the slider.

Refer to the time stamps on the page, in dashlets, and in lists to ensure that you are seeing the data that you expect.

For additional information on time period settings, review the **Changing the Time Period** topic.
Changing the Time Period

The interval drop-down list provides time period ranges of 3 hours, 24 hours, or 7 days based on your local client time, which constrains the start and end dates and times that you can select.

For example, if the date is 15 June and you select 7 days, the **Start Date** fields change to indicate the date of 8 June and local client time; the **End Date** fields indicate the current date and local client time.

**Important Note:** If you open the time interval drop-down list and select a start date that is different from today’s date and then make other time period changes, those changes remain when you open the drop-down list subsequently and change the time interval or date selections.

For example, today’s date is 15 June and you change the start date to 12 June and apply it. The page updates to display the related data. Then, when you return to the calendar and change the date or time interval, the page refers to the 12 June date as its basis, not the current date.

To reset the automated calendar updates when you change a time interval:
- Refresh the page.

To select a specific time period by using the time interval drop-down list:

1. To indicate the time interval by which you want to constrain the data, under **Time Range**, click the applicable option button.
2. To indicate a custom time period based on the time constraint, in the **Start Date** and **End Date** fields, select the date and time periods.
3. Click **Apply**.

The geographical map displays the health states for the time period…
…as does the list view…

…and the topological view.

The dashlets and device list also display data based on the time period that you apply.

You also can customize the time interval by using the timeline sliders.

To customize the view by selecting a specific time period on the timeline:

- Drag each timeline slider to the interval that you want to view, and then click Apply.
When you change the time period by using the timeline slider, the geographical map, list view, and topological map display the related data.

The **Network Health Summary** and the **Network by Device Role/Type** dashlets provide a **Custom** tab, which display the metrics for the time period that you applied…
...and the **Network Devices** list displays the devices in the most critical health state for a 15 minute view based on the time stamp indicated beside the heading.

List data is for the 15 minute interval up to the time stamp.

<table>
<thead>
<tr>
<th>Device Type</th>
<th>IP Address</th>
<th>OS Version</th>
<th>Overall Health Score</th>
<th>System Health</th>
<th>Data Plane Connectivity</th>
<th>Control Plane Connectivity</th>
<th>Issue Count</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>LA2-3850-ACD-1.corp.local</td>
<td>10.30.255.103</td>
<td>16.3.3</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>999</td>
<td>USA/SM</td>
</tr>
<tr>
<td>LA2-3850-ACD-2.corp.local</td>
<td>10.30.255.104</td>
<td>16.6.2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>75</td>
<td>USA/SM</td>
</tr>
</tbody>
</table>
Persistent Filters on Page Navigation

When you apply specific settings to **Network Health**, those settings persist when you navigate away from the page. Persistent settings include changes to:

- For SD-Access deployments, the fabric domain.
- The time period in the drop-down list or on the timeline.
- The network location.

When you return to the **Network Health** page, any changes that you made previously still apply.

To determine the location for the data that you are seeing, you can refer to the **Location** field, which is always visible, or the list view.

When you change settings by using the fabric domains drop-down list, the name visible in the drop-down list is the only indicator on the page that the information is filtered.

**Tip:** Always refer to the Location field and fabric domains drop-down list to identify the data that you are seeing.
How are Device Health Metrics Looking?

Get a Summary View of Device Health

What Will I See?

The Network Health Summary provides an overview of network devices and their health states.

Under **Most Recent**, the system combines the health scores for all device types into a single percentage of monitored devices in a healthy state.

Under **15 Minutes**, it displays a chart of device health states by device type for the previous 15 minutes based on the time period applied to the page.

The second time period chart displays total devices in each health state for the time period applied to the page.

**Network Health Summary**

![Network Health Summary](image)

- **Most Recent**: 64% Healthy Devices
- **Total Devices**: 22
- **Devices Monitored**: 21
- **Devices Not Monitored**: 1

**15 Minutes chart with health by device type**

- **Core (1)**
- **Access (2)**
- **Distribution (2)**
- **Router (2)**
- **Wireless (10)**

**Total devices in each health state based on time period**

- **View Details**

**Combined percentage of healthy devices**
Under **15 Minutes**, to see the percentage of a device type that is experiencing the health state that the color-coding indicates, you can point to that segment of the chart.

In the total devices chart, you can point to the timeline to see the number of devices in a specific health state at a specific time.
You can filter the total devices chart to display the health states of a specific network device type.

**To filter the chart by device type:**

- In the device type drop-down list, select the device type of interest.

![Device type drop-down list](image)

The chart updates to display metrics for the device type.

![Access chart](image)

**Important Note:** When you apply a specific device type to the chart, it does not affect what you see when you open the chart details.
How are Device Health Metrics Looking?

Below the charts, you can open detailed information on device health states by clicking View Details.

You can click either link to open the same Network Health Summary detailed information panel. The chart and data are active for the time period associated with the link.

The Network Health Summary detailed information panel includes the related interactive chart, the Device Distribution charts, and the device list.
The data filters apply the monitored devices of all types in a poor health state settings automatically.

Select a chart segment to view results in Device Distribution and the device list.
Where Do I Find…

…The Health of Network Devices by Device Type?

The Network Health by Device Role/Type Dashlet

The **Network Health by Device Role/Type** dashlet displays metrics for WLCs, APs, switches, and routers on separate tabs **based on their network roles**.

Tabs organize devices by their network roles.

![Network Health by Device Role/Type Dashlet](image)

Each tab displays the percentage of devices in a healthy state out of the total number of devices with the same role, and provides charts illustrating the numbers of devices and their health states for:

- The devices, referred to as system health:
  - For WLCs: Memory utilization, free memory buffer, and free timer score
  - For APs, routers, and switches: CPU and memory usage
- Device data plane connectivity.
  - For WLCs: Packet pools, WQE pools, and link errors
  - For APs: Radio usage, noise, and interference
  - For switches: Interface availability and link errors
  - For routers: Link errors
- For all devices, control plane connectivity.
The **Wireless** tab provides links to WLC and AP detailed information panels separately for system health or data plane connectivity details. For control plane connectivity, you can open a WLC-related detailed information panel.

The router and switch tabs provide links to their associated detailed information panels.
The Wireless WLC System Health Panel

On the left, the panel displays the number of devices in the poorest health state overall and by attribute. It provides the number of devices in the poorest health state based on system-defined thresholds for the following attributes:

- Percentage of memory usage
- Percentage of available free memory buffer
- Percentage of free timer score

The chart indicates the total number of devices and illustrates the ratio of device health states. The chart also can indicate the number of devices for which the system is not collecting telemetry.
The System Health Panel for APs, Routers, and Switches

On the left, the panel displays the number of devices in the poorest health state overall and by attribute. It provides the number of devices in the poorest health state based on system-defined thresholds for CPU and memory usage.

The chart also can indicate the number of devices for which the system is not collecting telemetry.
The Wireless WLC Data Plane Connectivity Health Panel

On the left, the panel displays the number of devices in the poorest health state overall and by attribute.

It provides the number of devices in the poorest health state based on system-defined thresholds for the following attributes:

- Packet pool size
- WQE pools available for data packet storage during routing
- Link errors

The chart indicates the total number of devices and illustrates the ratio of device health states. It also can indicate the number of devices for which the system is not collecting telemetry.
The AP Data Plane Connectivity Panel

On the left, the panel displays the number of devices in the poorest health state overall and by attribute. It provides the number of devices in the poorest health state based on system-defined thresholds for the following attributes:

- Radio usage for all of the radios and their channels on the device
- Amount of noise
- Amount of interference
- Link errors

The chart indicates the total number of devices and illustrates the ratio of device health states. It also can indicate the number of devices for which the system is not collecting telemetry.
The Switch Data Plane Connectivity Panel

On the left, the panel displays the number of devices in the poorest health state overall and by attribute.

It provides the number of devices in the poorest health state based on system-defined thresholds for the following attributes:

- Interface availability
- Link errors

The chart indicates the total number of devices and illustrates the ratio of device health states. It also can indicate the number of devices for which the system is not collecting telemetry.
The Router Data Plane Connectivity Panel

On the left, the panel displays the number of devices in the poorest health state overall and by the link errors metric.

The chart indicates the total number of devices and illustrates the ratio of device health states. It also can indicate the number of devices for which the system is not collecting telemetry.
The Control Plane Connectivity Panel for WLCs, Routers, and Switches

Fabric topologies use devices that are assigned control plane roles in the fabric to map and resolve the locations of endpoints on the network by using an internal MAP server function.

The Control Plane Connectivity panel provides information based on whether a device has a role in the control plane or are connected to the control plane device.

For devices that have control plane roles, the panel indicates the health status for each device’s connectivity to the fabric’s control plane.

When devices do not have a control plane role, the panel indicates the health status of those devices’ connectivity to the control plane device itself.

**Note:** When WLCs, routers, or switches do not support a fabric topology, the panel indicates the status in blue and does not provide a connectivity health status. When you select a chart element or data filter, you can see the applicable devices and their overall health scores.
...Access Point Device States and Usage?

The AP Analytics Dashlet

The AP Analytics dashlet displays the status of access point connectivity and lists the APs with the greatest number of connected clients.

The Total APs Up/Down chart indicates the number of APs that are up or down, which helps emphasize access points that might need more immediate attention to avoid potential issues or mitigate ongoing ones.

It also provides access to the Total APs Up/Down detailed information panel.
The **Top APs by Client Count** lists the access points with the most connected clients on average during the time period applied to the page.

Point to a data element to see the number of clients that are connected to it.

Depending on the Cisco DNA Center release in which you are working, the number of APs in the list varies, as follows:

- In Cisco DNA Center 1.2.5 or older, the dashlet lists the access points with the most clients, up to 15.
- For Cisco DNA Center releases newer than 1.2.5, the dashlet lists all of the access points for which it has data during the time period.

You can click the AP name link below a data element to open the access point's **Device 360 page**. Detailed device information can help when determining device health or mitigating potential issues.
The Total APs Up/Down Panel

The Total APs Up/Down detailed information panel displays the same chart with access to a device list.
How are Device Health Metrics Looking?

...The Health States and Connectivity of Network Devices?

The Network Devices List

Network Devices lists each active network device based on the data filters. On page entry, the list displays all monitored devices in a poor health state.

**Important Note:** When there are no devices in a poor health state, the list will not display information.

You can use the data and attribute filters to see the specific devices that you need.

**Important Note:** When you navigate away from the page, or make a change to the time interval, the Network Devices list returns all of the filter settings to their default states.
You also can click a column heading to sort the list. When the list is sorted by a column, the sort indicator appears in the column and indicates in which direction the column is sorted.

The overall health score of each device indicates the most critical health score of the following metrics:

- System health
- Data plane connectivity
- Control plane connectivity

![Column sort indicator](image)
To see the specific health scores and associated metrics that are contributing to the overall health score:

- Point to the score.
  
  A pop-up window opens and lists all of the attributes and their health scores.

Other information includes:

- The device type, IP address, and OS version.
- The number of issues that the system has captured for the device for the time period applied to the page.
- Where the device is assigned in the network hierarchy.

You can click the Device name link to open the associated Device 360 page.
How is a Specific Network Device Doing?

Get a Holistic View on the Device 360

What Will I See?

The Device 360 provides insights into the performance of a specific network device.
The page includes the following types of information, organized in sections and on tabs:

- Issues that are occurring on the device.

  - Issues (1)  Jul 24, 2018 3:22 pm
    - Device
      - Device experiencing high memory utilization
      - Total occurrences: 1111
    - Jul 24, 2018 3:10 pm
    - Resolved Issues

- The connections of the device to its neighbors.

  - Physical Neighbor Topology  Last Updated: 07/24/18 03:22:27 pm  Refresh

- A detail information section with tabs the display device and connectivity metrics, and in SD-Access deployments in which the device is provisioned to a fabric topology, fabric metrics.
It also provides the path trace tool so that you can evaluate the health and performance of all of the devices between the device and a destination device.

**Path Trace**

To find the location of an issue, perform a path trace between two nodes in your network—a source device and a destination device.

Run New Path Trace

On page entry, all of the sections are expanded by default.

When the page sections are expanded, you can navigate to sections of or tabs on the **Device 360** page by using the links below the timeline.

**Important Note:** The links are not active when the associated section is collapsed on the page.
Below the device name, the page provides some details about the device. You also can open a panel that lists additional device attributes.

**To view additional device attributes:**
- Below the domain drop-down list, click **View Details**.

A panel opens, overlaying the page and lists device attributes.
How Do I Open a Device 360 Page…

…By Using the Global Search Function?

To open a Device 360 page by using the global search feature:

1. On the application toolbar, click the global search icon.

   The **Search** dialog box opens.

2. In the **Search** field, begin typing the device name, device type, the device’s IP address, or its software version.

   A list of results matching the characters that you type begins populating automatically.
3. To indicate the device that you want to see, in the **Network Devices** results list, click the device name.

![Network Devices results list]

The dialog box provides information about the device and links to related information to the right of the search results.

4. To open the **Device 360** page, click the **Device 360** link.

![Device 360 page]

Click to open the **Device 360** page.
...By Using a Device Name Link?

Device name links are available in:

- The AP Analytics dashlet.
- The Network Devices list and the device lists available in the detailed information panels.

To open a Device 360 by using a network device name link:

- In the list or dashlet, click the name link for the device of interest.
How is a Specific Network Device Doing?

...In the Topology View?

When you open the topology view, each device icon provides a pop-up window with access to its Device 360 page.

To open a Device 360 page:
- In the topology view, point to the device of interest, and then, in the pop-up window, click View Device 360.
**Where Do I Find…**

**…Issues That Are Affecting the Device?**

**Issues** lists the problems that are affecting the device. The system identifies issues by computing, analyzing, and correlating incoming data and correlating the data with system-defined metrics.

<table>
<thead>
<tr>
<th>Issues (3)</th>
<th>Jun 17, 2018 4:50 pm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td></td>
</tr>
<tr>
<td>High input/output error on interface &quot;GigabitEthernet1/1/1&quot;</td>
<td></td>
</tr>
<tr>
<td>Total occurrences: 2</td>
<td></td>
</tr>
<tr>
<td>Connected</td>
<td></td>
</tr>
<tr>
<td>High input/output error on interface &quot;Port-channel7&quot;</td>
<td></td>
</tr>
<tr>
<td>Total occurrences: 2</td>
<td></td>
</tr>
<tr>
<td>Connected</td>
<td></td>
</tr>
<tr>
<td>High input/output error on interface &quot;GigabitEthernet1/0/2&quot;</td>
<td></td>
</tr>
<tr>
<td>Total occurrences: 246</td>
<td></td>
</tr>
</tbody>
</table>

Providing this information with links to details helps to ensure that potential or ongoing problems receive more immediate attention or action, as needed.

**Tip:** For your reference, **Assurance** provides an issue catalog that categorizes and lists the issues that Cisco DNA Center presents. To open the list:

- Click **Issues**, and then, below the toolbar, click **View Issue Catalog**.

The catalog provides tabs for each issue category.
For each category, the issues in the list include descriptions and possible root causes for them. You can select an issue to see its related information.

Entries in the list are open and are occurring or have occurred during the time period that the page indicates in the time interval drop-down list or on the timeline.

The time stamp beside the issue indicates its most recent occurrence. The number of occurrences of the problem appear below the description link.

You can open detailed information about a specific issue.

To review issue details, under the issue heading:

- Click the issue description link.

A panel opens, overlaying the page.
The panel provides:

- The option to change the issue status from **Open** to **Resolve**.
- A description of the issue.
- Based on the type of issue and its complexity, related charts and metrics.
- Suggestions to correct the issue, and depending on issue, the ability to run commands that retrieve additional information from the device.

When issues are complex, the panel can provide various charts and information on the issue.

When you determine that an open issue is no longer a problem, you can resolve the issue.

**To indicate that the issue is resolved:**

- In the **Status** drop-down list, select **Resolve**.

**Important Note:** You cannot move or change the status of a resolved issue.
You can open the suggested actions to view more details.

When suggestions are collapsed, you can expand them to see a list of associated steps that you can take.

<table>
<thead>
<tr>
<th>Suggested Actions (3)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong> On Switch, verify which process is consuming high memory</td>
</tr>
<tr>
<td>show memory platform</td>
</tr>
<tr>
<td>show processes memory platform sorted</td>
</tr>
<tr>
<td>show platform software status control-processor brief</td>
</tr>
<tr>
<td><strong>2.</strong> Check the release notes for known bugs, if it is known issue, check if SMU is available and apply on the switch</td>
</tr>
<tr>
<td><strong>3.</strong> If you are unable to resolve the issue, contact Cisco TAC for support.</td>
</tr>
<tr>
<td>a. Cisco TAC worldwide contacts</td>
</tr>
<tr>
<td>b. Direct email: <a href="mailto:tac@cisco.com">tac@cisco.com</a></td>
</tr>
<tr>
<td>c. Open a support case using Support Case Manager</td>
</tr>
<tr>
<td>i. Provide your Serial Number or License Number for entitlement confirmation.</td>
</tr>
<tr>
<td>ii. Describe the problem using the Issue Details above and add any additional details.</td>
</tr>
</tbody>
</table>
Some suggested actions contain commands that you can run to obtain additional information.

To run commands.

- In the suggestion entry, click **Run**.

The task starts immediately. On completion of each step in the task, which the system indicates with a green check mark, the panel provides the results below each step.
...A List of Resolved Issues and Their Details?

The Issues section also includes a list of resolved issues. This information can be helpful when you are working to evaluate or resolve current issues.

To view a resolved issue:

- Below the Issues list, click Resolved Issues.

A panel opens the list of resolved issues.

When the system automatically or system users manually resolve issues, the Resolved Issues list retains the issue for 14 days, and then removes it from the list.

Important Note: You cannot move or change the status of a resolved issue.
...The Connections of the Device to Its Neighbors?

Under **Physical Neighbor Topology**, the page displays a graphical view of:

- The network device that is active on the **Device 360** and its physical or wireless connections to neighboring devices.
- The health state of each device and its health score, indicated in color-coding.
- The connectivity status, up or down, between each device in the topology, indicated in color-coding.

The layout is organized from the top down to illustrate the devices that are upstream or downstream from the selected device on the 360 page.

In the screenshot below, for the LA2 switch in the middle, the LA-3 switch is upstream and the APs and clients are downstream from it.
The topology layout and connectivity indicators vary based on the device type. The example below illustrates access point connectivity.

- **Upstream switch connectivity to WLC**
- **AP’s logical connectivity (CAPWAP tunnel) to the WLC indicator**
- **2.4 Ghz radio connectivity indicator**
- **5 Ghz radio connectivity indicator**
- **AP connectivity to upstream switch**

The device icons and connectivity status indicators provide pop-up windows with more information.

**To see connectivity status:**
- Point to the connectivity status indicator.

**To see key attributes for the active device on the Device 360:**
- Point to the device icon.

The pop-up window indicates the device’s role in the network topology, its IP address, and software version.

Today 11:16 AM

<table>
<thead>
<tr>
<th>LA2-3850-ACC-1.corp.local</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role: ACCESS</td>
</tr>
<tr>
<td>IP: 10.30.255.103</td>
</tr>
<tr>
<td>Software Version: 16.3.3</td>
</tr>
</tbody>
</table>

View detail information
For the active device, the system provides a link to the **Detail Information** section at the bottom of the **Device 360** page.

**Important Note:** The link works when the Detail Information section is expanded on the page. The link is disabled when the section is collapsed.

You can scroll to and expand the section to see the information.

To see key attributes for a neighboring device:

- Point to the neighboring device’s icon.
  
The pop-up window indicates the device’s role in the network topology, its IP address, and software version.

For a neighboring device, the system provides a link to the **Device 360** page for that device.
Physical Neighbor Topology also displays the total number of clients connected to the network device and provides access to more information about the clients.

To see more information about the clients:

- Point to the client group of interest, and then, in the pop-up window, click View Device List.

The system opens a panel containing the MAC address of each client, its health score, and the IP address to which it is connected.

Under Device, you can click a MAC address link to open the endpoint's Client 360 page.

Note: For more information on endpoint Client 360 pages, refer to the Navigating Assurance Client Health training.
How is a Specific Network Device Doing?

…The Tool for Evaluating the Path That Traffic Is Using?

Path Traces for Flow Mapping and Path Health

Path Trace provides the tool that you can use to map the complete path that traffic is taking from its source IP address to its destination.

Running a path trace supports monitoring and troubleshooting end-to-end connectivity.

When you initiate a path trace, Cisco DNA Center reviews and collects network topology and routing data from the devices supporting the traffic. Beyond a simple traceroute process of logging in to the devices, Cisco DNA Center analyzes the forwarding tables in layer 2 on each switch on the path to determine accurate and specific traffic routing.

Following is an example of a complete path trace.

A completed path trace displays:

- The path direction and its physical link.
- Each intermediate network device that traffic is using to traverse to its destination and their protocols, its health state, and the number of clients connected to it, when applicable.

Note: The Path Trace tool provides the flexibility to run a path trace from any source to any destination to support troubleshooting. For example, you can run a separate path trace to evaluate the reverse direction of the flow, when that is helpful.
Above the topology, a description of the path with a time stamp indicating the most recent time that you ran the path or the system refreshed it.

To the right of the trace topology, a legend defining the device icons and link types.

Based on items that you can select for the path trace to identify:

- At each ingress and egress interface, each access control list (ACL) on that interface that match the criteria that you indicate when you configure the path trace.
  - Permit ACLs appear in green color-coding.
  - Deny ACLs appear in red color-coding.
  - When there is lack of data, such as a missing source or destination interface or protocol, in the trace configuration, the trace returns an ACL result in black color-coding.

- Device level CPU and memory utilization statistics.
- Interface level ingress or egress drops.
You can point to a device to see device details and access a link to the **Device 360** page, which can provide insight when troubleshooting a problem.

You can point to a link to see the protocol running between two devices.

You can point to ingress and egress interface icons for a device to see the interface that the path is using, the VLAN that the interface is using and packet drop metrics.

When you include interface statistics in the trace, you can click **More Details** to open a panel with various metrics and information.

Tip: If a link in a pop-up window does not respond, rerun the path trace or refresh the page to enable it.
When you run a path trace with ACL results, you can point to an ACL icon to see the ACL name and its rule.

Unmanaged Devices in Traffic Paths

When a device that is not managed by Cisco DNA Center supports the traffic flow between source and destination devices, that device appears in the path trace results as **Unknown**.

Unmanaged devices cannot respond to queries from Cisco DNA Center, such as requests for forwarding table data. When Cisco DNA Center identifies a device's unmanaged state, it logs in to the previous device and performs a traceroute.

This action allows Cisco DNA Center to capture and display the device in the path trace results and to determine the device at the next hop on the path after the unmanaged device.

**Note:** The system cannot report statistics on unmanaged devices.

When Cisco DNA Center is not managing a device on a path, it can include it in results and run a traceroute on the predecessor device to determine the next hop device.
How Do I Prepare To Run a Path Trace?

Before you begin a path trace, you can review the system inventory to identify all of the devices, such as routers, switches, Cisco WLCs, and access points, between the source device and destination device, that it includes and that they are in a managed state.

**Note:** While the path trace results can include unmanaged devices, the system must be able to communicate with the source, destination, and some devices on the path.

To do so, you can review Inventory page, which you can access on the Cisco DNA Center home page.

![Inventory page](image)

When you need to run a path trace for a specific interface or port on either the source or destination device, obtain each interface and port number that you need.

**Source**
- IPv4
  - 10.30.255.103
- Interface (optional) -
  - 10.30.255.103
  - 10.30.253.3
  - 192.168.0.1

**Destination**
- IPv4
- Port (optional)
How Do I Run a Path Trace?

To run a path trace:

1. Under **Path Trace**, click **Run New Path Trace**.

The **Set up Path Trace** panel opens, and, under **Source**, the panel populates the IPv4 field with device's IP address.

![Set up Path Trace panel](image-url)
2. To identify the device at which you want the trace to start, under **Source**:
   a. In the **IPv4** field:
      - To use the IP address, validate and accept the default address that the panel populated.
      - To select another device or identifier, click the field, and then, in the drop-down list select the device.

      **Note:** For added flexibility during troubleshooting, you can select any source or destination device to run the trace. This way, you do not need to navigate to another 360 page to run the trace of interest.

      **Tip:** You can filter the list to find the device that you need by typing an IP address, a host name, a user name, or an application name. The list filters automatically as you type to display the results that match the string.
b. Optionally, to identify the interface on which you need to start the trace, in the Port field, type the interface number.

3. Under Destination, to indicate the point at which you want to end the trace.
   a. In the IPv4 field, click the field, and then, in the drop-down list, select the destination IP address.

   Tip: The Destination | IPv4 field accepts IP addresses only, but you can filter the drop-down list by using any criteria that is included in the description. Begin typing to filter the list, which populates automatically as you type with the results that match the string.

   Based on the type of device you select for the destination, the panel also opens the Interface field above the Port field.
b. Optionally, to indicate the interface on which you need to start the trace, in the **Interface** field, type the interface number.

c. Optionally, to indicate a specific port on the interface, in the **Port** field, type the port number.

4. Optionally, to indicate a specific protocol for Cisco DNA Center to use to establish the path trace connection, in the **Protocol** drop-down list, select tcp or udp.

![Options](image)

5. To indicate whether the system runs the trace at 30 second intervals:
   - To run the trace every 30 seconds, accept the default selection of On.
   - To run the trace once and evaluate the results, toggle the button to Off.

   ![Refresh Every 30 sec](image)

   **Note:** Rerunning a path trace at 30 second intervals can be helpful for ongoing troubleshooting, for example, when a network user is experiencing issues connecting to a specific device.

6. To indicate whether devices on the trace contain access control lists (ACLs) that match trace criteria:
   - To see the ACL indicators, accept the default selection of On.
   - To not see ACL indicators, toggle the button to Off.

   ![ACL Trace](image)

   **Important Note:** When you include source or destination interfaces or ports, or protocol options in the path trace, the ACL trace results will include only those ACLs that apply based on the combination of items that you defined or selected. That means that there can be one or more ACLs on the interface that do not appear in the path trace results.
7. To configure the path trace to collect additional metrics, under **Include Stats**:
   - To see device level CPU and memory statistics, select the **Device** check box.
   - To see ingress or egress interface drop statistics, select the **Interface** check box.

   **Tip:** The quality of service statistics are available for routers only and return a subset of complete QoS data.
   To ensure that you see the data that you want on any device, run the QoS command directly on that device.

8. To run the trace, click **Start**.

   The panel closes automatically, and the system indicates that the trace is in progress.

When the path trace is complete, the system displays the topology results based on the settings in the trace configuration.

To clear a path trace or run a subsequent one:
   - Manually refresh the page by using the browser button.
…More Metrics and Detailed Information?

The Detail Information Section for Routers and Switches

Under Detail Information, the Device 360 page includes the following tabs:

- **Device Info**
  Device level metrics over time

- **Connectivity**
  The number of bytes that the device transmits (Tx) and receives (Rx) and interface availability

- **Fabric**
  In SD-Access deployments, when the device supports a fabric topology, the device’s connectivity to fabric devices and services.

Some charts list components with check boxes so that you can select or clear to see the associated metric or remove it from the chart.

Select or clear a checkbox to toggle the metric on or off the chart.
Reviewing Device Level Metrics

The **Device Info** tab provides charts over the 24-hour time period for:

- CPU usage for each CPU on the device.
- Memory usage.
- Device up or down time.
- Temperature measurements for each temperature sensor on the device.
Reviewing Interface Level Metrics

The **Connectivity** tab provides charts over the 24-hour time period for:

- The percentage of use that each interface is experiencing when receiving (Rx) and transmitting traffic (Tx).
- The percentage of input and output errors that are occurring on each interface.
Interface up or down availability states.

Note: By default, the system shows the L3 interfaces in the chart. You can use the Show drop-down list to select L2 interface or both interface types.
In SD-Access Deployments, Reviewing Fabric Topologies

For routers and switches that support a fabric topology, the **Fabric** tab provides access to:

- Reachability.
- Uplink status.

At regular intervals, Cisco DNA Center validates the IP address level connectivity between the device and:

- Other fabric devices.
- The fabric control plane.
- Services, such as DHCP or DNS.

Under **Reachability**, you can review all of the device’s fabric IP-level connectivity statuses based on the validation results. To the right of the chart, you can select specific connectivity destinations.
Under **Uplink Status Graph**, you can review the device’s link connectivity statuses at the interface-level, based on the device’s role in the fabric.

For example, for an edge router, the chart displays the link statuses of the interfaces connecting the device to the fabric distribution layer. For a border router, the chart displays the link statuses of the interfaces connecting the device to intermediate fabric switches or connecting to fabric edge routers.

To the right of the chart, you can select specific device interfaces.
The Detail Information for WLCs

Reviewing Device Level Attributes, and Device, Access Point and Client Endpoint Metrics, and Licensing

The Device tab provides device level attributes and charts over the 24-hour time period for:

- Under **Availability**, the device’s uptime, reason for the last time that it was restarted, and the status of its power supplies.

<table>
<thead>
<tr>
<th>Availability</th>
<th>Uptime: 18 days 1:10:53</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Reset Reason</td>
<td>Planned Reset</td>
</tr>
<tr>
<td>Primary Power Supply Status</td>
<td>Present, OK</td>
</tr>
<tr>
<td>Secondary Power Supply Status</td>
<td>Absent/Failed</td>
</tr>
</tbody>
</table>

- In high availability deployments, under **HA Redundancy**, the WLC’s mode, placement in the cluster, and its local and peer-related states.

<table>
<thead>
<tr>
<th>HA Redundancy</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundancy Mode</td>
<td>Disabled</td>
</tr>
<tr>
<td>Redundancy Unit</td>
<td>Primary</td>
</tr>
<tr>
<td>Local State</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>Peer state</td>
<td>N/A</td>
</tr>
</tbody>
</table>

- The percentage of CPU and memory usage and comparison to the system-defined acceptable threshold.
- The number of access points that connected to the WLC and the baseline threshold that the system has calculated over the last 7 day period.

![AP Count](chart)

- The number of clients connected to every access point that is connected to the WLC, and the baseline threshold that the system has calculated over the last 7 day period.

![Client Count](chart)
- The history of the up or down status of the WLC.

- The total number of access point licenses that are installed on the WLC and the number in use.
The Detail Information for Access Points

Under Detail Information, the Device 360 page includes tabs, including:

- **Device**
  Device level attributes, metrics, and connectivity over time
- **Connectivity**
  Traffic bandwidth usage for each AP radio
- **RF**
  Each radio’s attributes, usage and performance metrics

Reviewing Device Level Attributes, Metrics, and Connectivity

The Device tab provides device and availability attributes with charts over the 24-hour time period for:

- CPU usage.
- Memory usage.
- Connectivity history.
Reviewing Radio Traffic Bandwidth Usage

The **Connectivity** tab provides a chart for each radio that illustrates the amount of bandwidth that traffic on the AP is consuming.

The chart indicates the transmitting and receiving bandwidth measurements separately.
Reviewing AP Radio Attributes, Channel Usage, and Performance Metrics

The **RF** tab provides for the following attributes and metrics:

- The attributes of each radio channel

<table>
<thead>
<tr>
<th>Device</th>
<th>Connectivity</th>
<th>RF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio 0 Channel and Width</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current Channel</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Current Channel Width</td>
<td>20 MHz</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>2.4 GHz</td>
<td></td>
</tr>
<tr>
<td>RF Profile</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>Radio 1 Channel and Width</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current Channel</td>
<td>153</td>
<td></td>
</tr>
<tr>
<td>Current Channel Width</td>
<td>20 MHz</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>5 GHz</td>
<td></td>
</tr>
<tr>
<td>RF Profile</td>
<td>NA</td>
<td></td>
</tr>
</tbody>
</table>

- The amount of 802.11 traffic that the AP can detect on its channel, from all sources, including from all of the APs and clients in its vicinity

In addition to usage, Cisco DNA Center calculates a predictive baseline threshold, indicated in red, based on what it captures as ongoing, regular usage. If usage peaks above the threshold, the radio channel is experiencing unusually high usage.

![Radio 0 Channel Utilization Chart](chart.png)
● The percentage of interference that each radio is experiencing

In addition to usage, Cisco DNA Center calculates a predictive baseline threshold, indicated in red, based on what it captures as ongoing, regular interference. If usage peaks above the threshold, the radio channel is experiencing unusually high interference.

![Radio 0 Interference Graph](image)

● The dB levels of each radio’s background noise

![Radio 0 Noise Graph](image)

● The amount of interference each radio is experiencing from non-radio sources

**Note:** Air quality above 40 indicates a good health score.
How is a Specific Network Device Doing?
What Was a Network Device Experiencing at a Certain Time?

A key feature of a Device 360 page is your ability to see historical information at a specific point in time by using the timeline. This information provides context when you are troubleshooting a past or recurring issue.

The timeline appears below device name and attributes.

When you point to a time on the timeline, a pop-up window indicates the device’s health score at that time, and lists all of the factors that contribute to the score.

It also lists those factors individually with their scores and metrics.

The information in the pop-up window varies based on the device type.
When you click a point on the timeline, an indicator emphasizes the time for which the page is displaying information and the specific time appears in the pop-up window…

…and the page refreshes to display issues and chart data that includes the beginning of the time period on the timeline up to the time that you clicked on the timeline. The **Issues** time stamp and the charts’ y-axes indicate the ending time of the time period.

**Notes:** When defining a time period, it does not apply to **Physical Neighbor Topology** or **Path Trace**.

When you click a point on the timeline, that time period persists until you click a different time or manually refresh the page.
Watch It Happen in Cisco DNA Center

Video

This step-by-step instructional video demonstrates all of the steps that you can take to complete the task.

And, it includes the context that you need for a deeper understanding of system processes, best practices, and considerations for optimal system usage and results.

Evaluating a System User’s Printer Connection (8:00)

Watch as we use the Assurance Path Trace tool to map the complete path that traffic is taking from its source IP address to its destination.

The results provide insight into ongoing or potential issues that might be affecting network traffic.

How To Watch a Video

To watch a video:

- Click the video’s title link, which opens an MP4 file.

Based on your system and configuration, you might need to start the video manually.

Note: Video download and streaming times can vary.
Want More?

Find Product Information

Visit the Cisco Web site to learn more about Cisco DNA Center.

Visit the Cisco Web site to review or download technical documentation.

Find Training

Visit the Cisco Web site to access other Cisco DNA Center learning opportunities.

Visit the Cisco Web site to access learning opportunities for other Cisco products.

Contact Us About This Training

Send us a message with questions or comments about this training.

Note: Please send messages that address training content only. Follow your regular business process to request technical support or address technical or application-related questions.