Cisco DNA Application Assurance

Solutions Adoption Prescriptive Reference—Design Guide

March, 2020

Table of Contents

Introduction

About the Solution

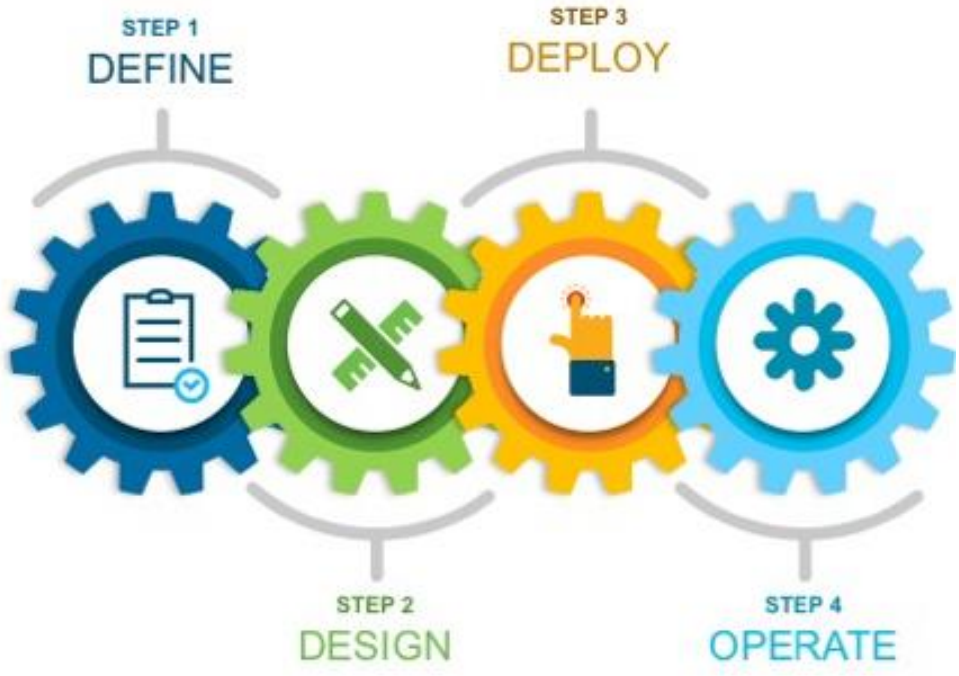
This solution focuses on how to deploy Cisco DNA Application Assurance within an enterprise network; and how to monitor and troubleshoot applications and their performance when the application traffic crosses observation points within the LAN & WAN, through Cisco DNA Application Assurance.

Cisco DNA Application Assurance is only one component of Cisco DNA Assurance which runs on Cisco DNA Center. Other components include Cisco DNA Network Assurance, Cisco DNA Client Assurance, Intelligent Capture, and Sensors & Sensor Tests. This design and deployment guide focuses primarily on Cisco DNA Application Assurance, although Cisco DNA Network Assurance will be touched upon within the discussion in the use cases at the end of the document.

About This Guide

This guide is intended to provide technical guidance to design, deploy, and operate Cisco DNA Application Assurance within Cisco DNA Center.

Figure 1 Implementation Flow



This document contains four major sections:

- The **Define the Network for Cisco DNA Application Assurance** section presents a high-level overview of the network in which Cisco DNA Application Assurance will be deployed through Cisco DNA Center.
- The **Design the Network for Cisco DNA Application Assurance** section will discuss the design decisions and implications regarding where to implement Cisco DNA Application Assurance within the network.
- The **Deploy the Network for Cisco DNA Application Assurance** section discusses how to enable the collection of Cisco DNA Application Assurance data within the network, through Cisco DNA Center.

- The **Operate the Network** section presents three use cases. The first two use cases discuss how Cisco DNA Application Assurance can be used to gain visibility into applications and their usage across the LAN and WLAN. The third use case discusses how a combination of Cisco DNA Application Assurance and Cisco DNA Network Assurance can be used to identify and troubleshoot an application performance issue across your network.

Define the Network for Cisco DNA Application Assurance

Audience

The audience for this document includes network design engineers and network operations personnel who wish to gain visibility into applications and the performance of those applications on their networks, through the use of Cisco DNA Application Assurance running within Cisco DNA Center.

Purpose of this Document

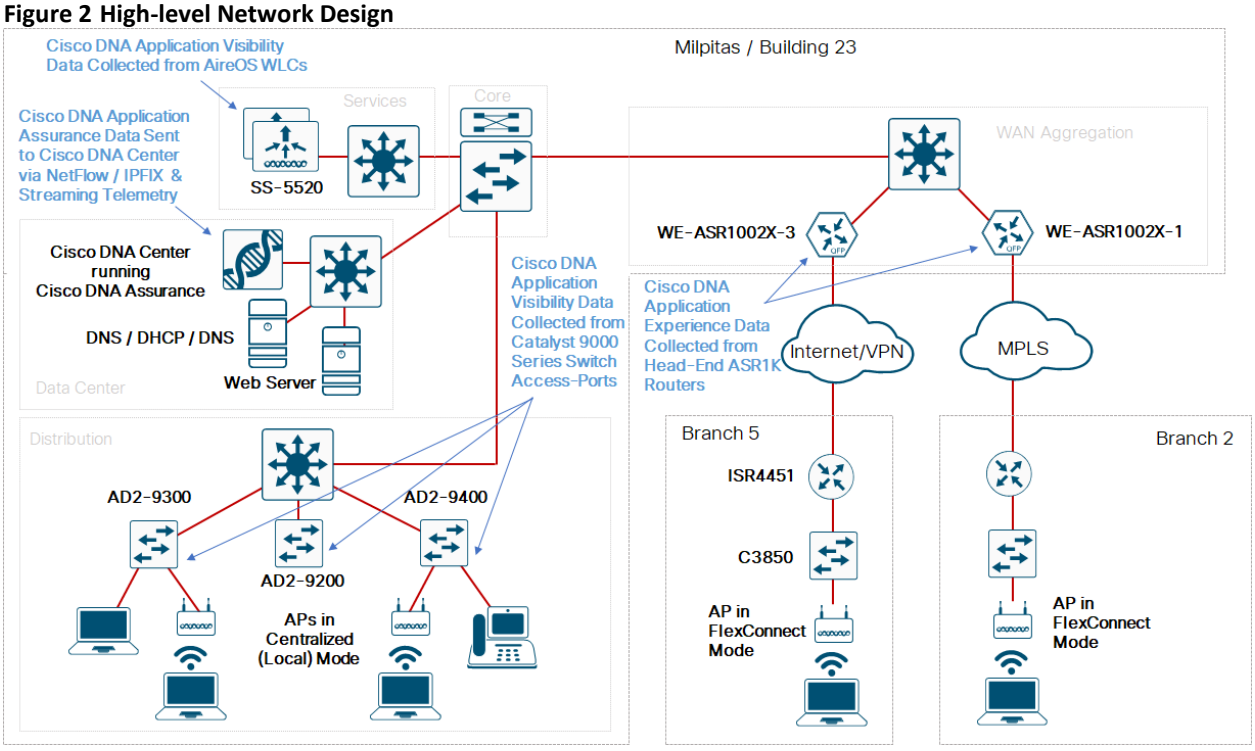
This guide focuses on the following:

- How to enable / deploy Cisco DNA Application Assurance within an enterprise network.
- How to monitor and troubleshoot applications and application performance as traffic crosses the LAN & WAN, through the use of Cisco DNA Application Assurance.

Solution Overview

The following figure shows the high-level network design for this deployment guide.

Figure 2 High-level Network Design



The Cisco DNA Center site hierarchy consists of a single campus and two branches. The WAN connectivity models were chosen to be consistent with common deployments seen within customer networks.

The WAN Aggregation block within the campus consists of two Cisco ASR 1K routers (**WE-ASR1002X-1** and **WE-ASR1002X-3**).

WE-ASR1002X-1 connects to a service provider (SP) managed services network that provides four classes of service (SP 4-class model). The DSCP markings of traffic leaving the enterprise network are re-marked to one of the four traffic-classes

supported by the SP network. Traffic entering the enterprise network from the SP is classified and re-marked to one of the 12 traffic-classes supported by the enterprise network through an NBAR-based ingress classification & marking QoS policy.

WE-ASR1002X-3 is connected to an Internet connection with the option of either DMVPN or IPsec protected GRE connectivity configuration. All traffic to-and-from **WE-ASR1002X-3** is sent through either the DMVPN or IPsec protected GRE connection. Although traffic sent to and from the Internet is remarked to a default value (DSCP 0), the original DSCP markings of the enterprise traffic are preserved within the DMVPN / IPsec protected GRE tunnel between **WE-ASR1002X-3** and **Branch 5**.

Branch 2 is connected through a service provider (SP) managed-services network which provides four classes of service (SP 4-Class model). The DSCP markings of traffic leaving **Branch 2** are re-marked to one of the four traffic-classes supported by the SP network. Traffic entering **Branch 2** from the SP network is classified and re-marked to one of the 12 traffic-classes supported by the enterprise network through an NBAR-based ingress classification & marking QoS policy.

Branch 5 is connected through an Internet connection with the option of either DMVPN or IPsec protected GRE connectivity configuration. All traffic between the campus and **Branch 5** is sent through either the DMVPN or IPsec protected GRE connection. Although traffic sent to and from the Internet is remarked to a default value (DSCP 0), the original DSCP markings of the enterprise traffic are preserved within the DMVPN / IPsec protected GRE tunnel between the campus and **Branch 5**.

The campus LAN distribution block consists of Catalyst 9000 Series switches configured as Layer 2 (L2) access switches, connected to a Layer 3 (L3) distribution switch. Wired traffic application visibility within the campus is accomplished through Flexible NetFlow flow monitors configured on the access-ports of the Catalyst 9000 access-layer switches.

The wireless design consists of a single pair of AireOS 5520 wireless LAN controllers (WLCs) supporting Access Points (APs) operating in FlexConnect mode within the branches; and APs operating in centralized (local) mode within the campus. Wireless clients are connected to the APs within the branches and the campus. Within the branches, FlexConnect mode is necessary to terminate branch wireless traffic onto the branch LAN switches, rather than backhauling it within a CAPWAP tunnel. This allows for visibility into the wireless traffic flows between the campus and the branch locations, at the head-end routers. Access Points (APs) operating in centralized (local) mode are deployed within the campus. APs operating in centralized mode encapsulate and backhaul all traffic within a CAPWAP tunnel from the AP to the wireless LAN controller (WLC). In centralized mode, all wireless traffic application visibility is lost at the access-layer switches because of the CAPWAP encapsulation. Wireless traffic application visibility within the campus is accomplished through streaming telemetry at the AireOS WLCs.

Technical Note: The implementation of the WAN, LAN, and WLAN deployment is not covered within this document.

Assumptions

This deployment guide makes the following assumptions:

- The network shown above is already designed and deployed.
- The site hierarchy within Cisco DNA Center has been created.
- The network devices have already been discovered and assigned to their respective sites within Cisco DNA Center.

The next section, **Design the Network for Cisco DNA Application Assurance**, will discuss the design decisions and implications regarding where to implement Cisco DNA Application Assurance within the network discussed above. Following that, the **Deploy Cisco DNA Application Assurance on the Network** section will discuss how to enable the collection of Cisco DNA Application Assurance data on the devices discussed within the design section. Finally, the **Operate the Network** section discusses multiple use cases regarding how Cisco DNA Application Assurance can be used to identify applications on the network and to assist in identifying and troubleshooting application performance issues.

Design the Network for Cisco DNA Application Assurance

As of Cisco DNA Center release 1.3.1, Cisco DNA Application Assurance has been expanded to collect application visibility data on Catalyst 9000 Series switches and AireOS WLCs. As a result of this, Cisco DNA Application Assurance now supports the following two different types of data collection, depending upon the platform deployed within the network.

- Application experience data
- Application visibility data

The following table summarizes the differences in the data collected and displayed within Cisco DNA Center depending upon whether the platform supports application experience data collection or application visibility data collection.

Table 1 Data Collected / Displayed by Application Experience & Application Visibility

Per-application data collected and/or displayed in Cisco DNA Center	Collected through application experience?	Collected through application visibility?
Application name	Yes	Yes
Usage and throughput statistics	Yes	Yes
Traffic-class	Yes	Yes
Performance metrics (latency, jitter, packet loss)	Yes, for certain flows (TCP, RTP, etc.)	No
Health scores (based on performance metrics)	Yes	No
QoS (DSCP) markings of traffic flows	Yes	No

Technical Note: The traffic-class for applications displayed within Cisco DNA Center is derived from the application name, and the mapping of the application name to the NBAR traffic-class attribute setting for that application within Cisco DNA Center. Likewise health scores are derived from the performance metrics for each application.

The following table summarizes the platforms which support the collection of the two types of Cisco Application Assurance data.

Table 2 Cisco Platform Support for Application Experience versus Application Visibility in Cisco DNA Center

Platform	Data Collection	Notes
Cisco IOS-XE routers	Application experience data collection	Requires IOS XE 16.x and higher with active NBAR2 license
Catalyst 9000 Series switches (Not including Catalyst 9600 or 9500 switches)	Application visibility data collection	Requires Cisco DNA Advantage license
Cisco AireOS WLCs	Application visibility data collection	AireOS version 8.8.114.130 and higher, except AireOS 8.9.x does not support Application Visibility

This section of the design and deployment guide presents a high-level discussion of the underlying technology behind how Cisco DNA Application Assurance data is collected on the various platforms listed in **Table 2**. This information is necessary to understand the design decisions which need to be made regarding where to enable Cisco DNA Application Assurance within the network – and the implications of those decisions. An understanding of how Cisco DNA Application Assurance data is collected is also beneficial in interpreting the application information displayed within Cisco DNA Center.

Cisco IOS-XE Router Platforms – Application Experience Data

Application experience data is collected through Cisco Performance Monitor (PerfMon). Specifically, a Cisco Easy Performance Monitor (Cisco ezPM) policy context that uses the Application Performance profile is deployed on Cisco IOS XE router platforms. A profile is a pre-defined set of traffic monitors that can be enabled or disabled for a given context. The context itself is then applied to one or more interfaces on the Cisco IOS XE router platforms. Cisco ezPM provides an "express" method of implementing Cisco PerfMon, requiring minimal configuration.

Technical Note: For more information regarding Cisco ezPM, as well as the available profiles and traffic monitors, please refer to the **Easy Performance Monitor (ezPM)** section of the **Cisco Application Visibility and Control User Guide**, located at the following URL:
https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/avc/guide/avc-user-guide/avc_config.html#55042

As of Cisco DNA Center release 1.3.1, Cisco Application Assurance deploys the Cisco ezPM Application Performance profile context only to Cisco router platforms running Cisco IOS XE 16.x software versions. Therefore, in a typical network, Cisco DNA Application Assurance is only capable of collecting application experience data for applications as the traffic crosses the WAN.

The following are additional restrictions for deployment of the Cisco ezPM Application Performance profile context, specific to Cisco DNA Center:

- The interface to which the Cisco ezPM Application Performance profile context is applied must be a routed (Layer 3) interface with an IP address configured. Cisco DNA Center will not apply the context to a main interface if the interface does not have an IP address configured. For example, if the main interface on the router supports sub-interfaces that have IP addresses configured, then the main interface will not have an IP address configured. In this configuration, Cisco DNA Center will not apply the Cisco ezPM Application Performance profile context to the main interface.

- The interface to which the Cisco ezPM Application Performance profile context is applied must not be a sub-interface. For example, if the main interface on the router supports sub-interfaces, and each sub-interface has an IP address configured, Cisco DNA Center will not apply the Cisco ezPM Application Performance profile context to the sub-interfaces.

- Cisco DNA Center will not apply the Cisco ezPM Application Performance profile context to logical interfaces on the router platform. Interfaces such as port-channel interfaces and tunnel interfaces are not supported by Cisco DNA Center. Only physical Ethernet interfaces are supported by Cisco DNA Center.

Cisco PerfMon uses the Cisco Network Based Application Recognition – Version 2 (NBAR2) engine within Cisco IOS XE to classify application traffic. Cisco NBAR2 releases are referred to as protocol packs. As of the current release (Protocol Pack 46.0.0), Cisco NBAR2 can classify over 1400 applications. The following is the link to the Cisco NBAR2 protocol library:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

Each of the 1400+ applications known to the Cisco NBAR2 taxonomy have multiple attributes. From a Cisco DNA Application Assurance perspective two of the more important attributes are traffic-class and business relevance. For each application, the Cisco NBAR2 taxonomy has a default setting for whether the application is considered **Business Relevant**, **Business Irrelevant**, or **Default**. The meanings of each of these three business relevance categories is as follows:

- **Business Relevant** –Applications which directly support the business objectives of your organization. These applications should be classified, marked, and treated according to industry-standard best practice recommendations. Examples may include network management applications, voice and video applications, etc., depending on your organization.

- **Business Irrelevant** – Applications which do not support the business objectives of your organization. Applications of this type should be treated with a less than best effort service. Examples of these applications could include gaming applications, etc. depending on your organization.

- **Default** - Traffic from applications which may or may not be relevant to the operations of your organization. For example, some generic web traffic (HTTP or HTTPS) – perhaps for internal web-based applications – may be relevant to the operations of your organization; while other web traffic – perhaps for browsing the Internet – may not be relevant to the operations of your organization. Such traffic may be treated with a default per hop behavior (DSCP marking) across your network.

Likewise, for each application, the Cisco NBAR2 taxonomy has a default setting for the traffic-class to which the application belongs. The traffic-class to which the application belongs determines its QoS treatment across the network – based upon the Cisco RFC 4594-based 12-class QoS model, shown in the following figure.

Figure 3 Cisco RFC 4594-based 12-class QoS model

	Application Class (Traffic-Class)	Per-Hop Behavior (DSCP)	Queuing & Dropping	Application Examples
Business Relevant	VoIP Telephony	EF	Priority Queue (PQ)	Cisco IP Phones (G.711, G.729)
	Broadcast Video	CS5	(Optional) PQ	Cisco IP Video Surveillance
	Real-Time Interactive	CS4	(Optional) PQ	Cisco TelePresence
	Multimedia Conferencing	AF4	BW Queue + DSCP WRED	Cisco Jabber, Cisco WebEx
	Multimedia Streaming	AF3	BW Queue + DSCP WRED	Cisco Digital Media System (VoDs)
	Network Control	CS6	BW Queue	EIGRP, OSPF, BGP, HSRP, IKE
	Signaling	CS3	BW Queue	SCCP, SIP, H.323
	Ops / Admin / Mgmt (OAM)	CS2	BW Queue	SNMP, SSH, Syslog
	Transactional Data	AF2	BW Queue + DSCP WRED	ERP Apps, CRM Apps, Database Apps
	Bulk Data	AF1	BW Queue + DSCP WRED	E-mail, FTP, Backup Apps, Content Distribution
Default →	Default Forwarding	DF	Default Queue + RED	Default Class
Business Irrelevant →	Scavenger	CS1	Min BW Queue (Deferential)	YouTube, Netflix, iTunes, BitTorrent, Xbox Live

Note that both the traffic-class and business relevance to which a particular application belongs can be modified through a QoS policy applied through Cisco DNA Center Application Policy. This is outside the scope of this document.

Where to Enable Cisco DNA Application Assurance on Cisco IOS-XE Router Platforms?

Cisco DNA Application Assurance can be used to view information regarding application traffic – only as the traffic crosses an observation point at which Cisco DNA Application Assurance data is being collected. For application experience data, observation points are the interfaces on the Cisco IOS XE routers to which the Cisco ezPM Application Performance profile context is applied.

When deciding to deploy Cisco DNA Assurance on Cisco router platforms, the first question that needs to be answered is what interface (or interfaces) on the Cisco IOS XE router platforms will serve as the application experience data observation points – based on the required use cases. The following sections discuss various options.

WAN Interfaces Connected to Managed-Services Networks

Traffic sent across a managed-services network, such as an MPLS network, may or may not be encapsulated and/or encrypted – depending upon the business requirements of the particular deployment.

If a tunneling protocol such as GRE is used to encapsulate all traffic (which may then be protected by IPsec), all application traffic entering / exiting the managed-services network will appear as GRE traffic. Visibility into the actual application traffic will be lost at the WAN-facing interface.

If application traffic is not encapsulated within GRE (which may then be protected by IPsec), then application traffic entering / exiting the managed-services network may be visible at the WAN-facing interface.

WAN Interfaces Connected to the Internet

If a tunneling protocol such as GRE is used to encapsulate all traffic (which may then be protected by IPsec), then all application traffic entering / exiting the Internet provider will appear as GRE traffic. Visibility into the actual application traffic will be lost at the WAN-facing interface.

From a Cisco DNA Center Application Assurance perspective, if the WAN-facing interface of a router were chosen as the application experience data observation point on either the head-end ASR1K routers or the branch routers, and if GRE encapsulation is used (which may then be protected by IPsec); all traffic appears as GRE, and visibility into the actual applications is lost. Hence, this design would not work for the use case of gaining visibility into the applications on the enterprise network.

LAN-Facing Interfaces

From a Cisco DNA Application Assurance perspective, when DMVPN or IPsec protected GRE tunnels are implemented on routers, application traffic is only encapsulated / decapsulated within GRE tunnels as the traffic is sent over the WAN. Therefore, enabling the observation points on the LAN-facing interfaces will work for the use case of gaining visibility into the applications on the enterprise network – at least for applications where traffic crosses the WAN between the campus and branch locations.

Head-end vs. Branch Routers

When deciding to deploy Cisco DNA Assurance, the next question that needs to be answered is what Cisco router platforms will serve as the application experience data observation points for Cisco DNA Application Assurance – based on the required use cases. The following are the choices:

- Branch routers
- Head-end routers
- Both the head-end and branch routers

Although the first impulse may be to simply enable application experience data observation points everywhere – with the thought that more visibility is better, some thought has to go into this decision – again based on the required use cases. The following sections discuss various options.

Branch Routers

Enabling application experience data observation points on the LAN-facing interfaces of each branch router will provide visibility into application traffic from the campus to each branch – but only if the traffic enters or exits one or more LAN-facing interfaces of the branch router. Traffic from data center management servers destined for interfaces such as Loopback0 on the branch router may not be visible, since the management traffic does not cross the observation point.

Application traffic between different subnets within the branch may be visible, but only if the subnets are terminated on separate interfaces on the branch router. The interface to which the Cisco ezPM Application Performance profile context is applied cannot not be a sub-interface. For example, if the main interface on the router supports sub-interfaces, and each sub-interface has an IP address configured, Cisco DNA Center will not apply the Cisco ezPM Application Performance profile context to the sub-interfaces.

Application flows between different branches will be visible. However, these flows will be double counted – once on each branch observation point.

Application flows within the campus are not visible.

If application experience data observation points are enabled within each branch router, the Cisco DNA Application Assurance data must be backhauled across the WAN via Flexible NetFlow / IPFIX. This will consume some of the available WAN bandwidth to each branch, depending upon the number of application flows seen, the amount of traffic per flow, etc. Likewise, the scale of the deployment may be limited by the number of Flexible NetFlow / IPFIX export flows which can be handled by Cisco DNA Center – since each branch will contribute at least one flow. Finally, enabling Cisco PerfMon (in the form of Cisco ezPM) and backhauling the traffic via Flexible NetFlow / IPFIX will result in some performance impact of each branch router. The specific impact depends on the router platform, Cisco IOS XE code revision, the number of application flows seen, the amount of traffic per flow, etc.

Head-end Routers

Enabling application experience data observation points on the LAN-facing interfaces of WAN head-end routers will again provide visibility into application traffic from the campus to each branch. Traffic from data center management servers destined for interfaces such as Loopback0 on the branch router will be visible, since the observation point is on the head-end router. Likewise, traffic from data center management servers destined for interfaces such as Loopback0 on the WAN head-end routers will also be visible – since the traffic has to enter/exit the LAN-facing interface to reach the Loopback0 interface.

Application traffic between subnets within the branch will not be visible. This is because the application traffic flows do not cross the application experience observation point at the WAN head-end router. Application traffic between branches connected to the same head-end router will not be visible – since the application traffic flows never cross the application experience data observation point at the LAN-facing interface of the WAN head-end router. Application traffic between branches connected to different WAN head-end routers may or may not be visible – depending upon whether the application traffic flows cross the application experience data observation points on the LAN-facing interfaces of the WAN head-end routers. Further, these flows may be double-counted – once on each WAN head-end router observation point. In other words, each WAN head-end router may display application statistics. However, the total amount of application traffic may not simply be the sum of the application statistics on the routers, since some flows may be duplicated.

Application flows within the campus are not visible.

If application experience data observation points are enabled within each WAN head-end router, the Cisco DNA Application Assurance data is only backhauled across the campus LAN via Flexible NetFlow / IPFIX. WAN bandwidth to each branch is not consumed. This is a significant advantage, since WAN bandwidth generally is a recurring expense, versus LAN bandwidth which can be increased relatively easily by increased interface speeds. Likewise, the scale of the deployment is not limited by the number of Flexible NetFlow / IPFIX export flows which can be handled by Cisco DNA Center – since there are relatively few WAN head-end routers, compared to branch routers.

However, since each WAN head-end router sees significantly more application flows – compared to individual branch routers, the performance impact of enabling Cisco PerfMon (in the form of Cisco ezPM) and backhauling the traffic via Flexible NetFlow / IPFIX to Cisco DNA Center, on the WAN head-end routers must be more carefully managed. Specifically, the CPU utilization and throughput of the current WAN head-end routers must be sufficient to account for the extra load when Cisco DNA Application Assurance is enabled.

Both Head-end and Branch Routers

The main advantage of enabling application experience data observation points on the LAN-facing interfaces of both branch and WAN head-end routers, is that it provides more visibility into application flows between subnets within a single branch, between branches, and between the campus and branches.

However, this benefit may be offset by duplication of flow data. For example, an application flow between two devices each within a different branch, with each branch connected to a different WAN head-end router – may be counted four times. This is because the flow may be seen at the application experience observation data point of the first branch, the application experience data observation point of the first WAN head-end router, the application experience data observation point of the second WAN head-end router, and the application experience data observation point of the second branch router. This may skew application usage statistics presented by Cisco DNA Application Assurance.

Application flows within the campus are not visible.

Finally, enabling application experience data observation points on both the head-end and branch routers is also limited by the scalability of having at least one Flexible NetFlow / IPFIX export flow per branch terminating on Cisco DNA Center, as well as the amount of bandwidth consumed on each branch due to the Flexible NetFlow / IPFIX flow data.

Cisco Catalyst 9000 Series Switch Platforms – Application Visibility Data

For Catalyst 9000 Series switches, application visibility data is collected through a wired AVC Flexible NetFlow (FNF) flow monitor applied bi-directionally (ingress and egress) to switch ports. The flow record corresponding to the flow monitor, includes the application name as a key value (a match statement as opposed to a collect statement). Inclusion of the application name as a field within the wired AVC FNF record automatically enables NBAR2 for the interfaces to which the flow monitor is applied.

Application visibility data collected by Cisco DNA Application Assurance on Catalyst 9000 Series switches complements the application experience data collected on Cisco IOS XE routers by providing visibility into applications without the application traffic having to cross a router interface – in other words without having to cross the WAN.

The following are additional restrictions for deployment of the wired AVC FNF flow monitor on Catalyst 9000 Series switches, specific to Cisco DNA Center:

- The switch port to which the wired AVC FNF flow monitor is applied must be configured as an access port. Specifically the command `switch-mode access` must be configured on the switch port. NBAR2 on Catalyst 9000 Series switches is scaled (in terms of performance) primarily for access ports on access-layer switches.
- Cisco DNA Center will not apply the wired AVC FNF flow monitor to trunk ports.
- Cisco DNA Center will not apply the wired AVC FNF flow monitor to switch ports configured as Layer 3 (L3) routed interfaces.
- Cisco DNA Center will not apply the wired AVC FNF flow monitor to logical interfaces such as port-channel interfaces, loopback interfaces, etc.

Where to Enable Cisco DNA Application Assurance on Cisco Catalyst 9000 Series Switch Platforms?

As with IOS XE router platforms, Cisco DNA Application Assurance can be used to view information regarding application traffic – but only as the traffic crosses an observation point at which Cisco DNA Application Assurance data is being collected. For application visibility data on Catalyst 9000 Series switch platforms, observation points are the switch ports to which the wired AVC FNF flow monitor is applied.

When deciding to deploy Cisco DNA Assurance on Catalyst 9000 Series switch platforms, a question that needs to be answered is what switch will serve as the application visibility data observation points – based on the required use cases. The following sections discuss various options.

Technical Note: SD-Access (fabric) deployments are not discussed within this deployment guide.

Uplink Ports on Access-layer Switches

For Catalyst 9000 Series switches deployed in the role of a traditional (non-fabric) Layer 2 (L2) access-switch, uplink ports are often configured as trunk ports, which support the various VLANs configured across the access-ports (i.e. ports connected to end-devices). As discussed in the additional restrictions above, Cisco DNA Center will not apply the wired AVC FNF Flow monitor for collecting application visibility data to trunk ports.

Also, Layer 2 (L2) switch uplink ports are frequently configured for high-availability via an EtherChannel configuration. In order to correctly classify certain applications, NBAR2 requires symmetric flows – meaning the application traffic must be

sent and received by the same interface (logical or physical). Port-channel interfaces are used to provide a single logical interface in such a configuration. However, Catalyst 9000 Series switches do not support the ability to configure wired AVC FNF flow monitors on Layer 2 (L2) port-channel interfaces. Therefore, Cisco DNA Center will not apply the wired AVC FNF flow monitor to logical interfaces, as discussed in the restrictions above.

For Catalyst 9000 Series switches deployed in the role of a traditional (non-fabric) Layer 3 (L3) access-switch or as a Cisco SD-Access Fabric-Edge (FE) switch, uplink ports are configured as routed interfaces. Cisco DNA Center will not apply the wired AVC FNF flow monitor for collecting application visibility data to routed interfaces.

Hence, the ability to collect application visibility data on uplink interfaces of access-layer switches is limited to the use case of a traditional (non-fabric) Layer 2 switch with no EtherChannel and no trunk configuration – in other words the uplink port configured as an access-port. Note however, that NBAR2 is scaled (in terms of performance) for access ports on access-layer switches.

Access-ports on Access-layer Switches

Regardless of whether a Catalyst 9000 Series switch is configured as a traditional (non-fabric) L2 or L3 access switch, ports connected to end-user devices are generally configured as access-ports. Cisco DNA Center will apply the wired AVC FNF flow monitor to these interfaces.

Technical Note: The network administrator must still express his/her business intent to collect application visibility data on each desired switch access-port by explicitly configuring the word `lan` within the interface description. Also, the switch port must explicitly be configured with the `switchport mode access` command in order for Cisco DNA Center to apply the wired AVC FNF flow monitor.

Therefore, application visibility deployed on access-ports of Catalyst 9000 Series access-layer switches will generally provide visibility into application traffic generated by wired devices connected to the switch ports.

However, for switch ports connected to wireless Access Points (APs), visibility into application traffic may be limited. If the wireless deployment is a centralized (local) mode deployment connected to a traditional (non-fabric) access-layer switch port – all application traffic to and from the APs is encapsulated in CAPWAP headers. If the AP is part of a FlexConnect mode wireless deployment connected to a traditional (non-fabric) access-layer switch port – the AP may be configured to support multiple VLANs. Hence the switch port may be configured as a trunk port, and Cisco DNA center will not apply the wired AVC FNF flow monitor to the switch port connected to the FlexConnect AP. Only when the FlexConnect AP is configured with a single VLAN, meaning the switch port is configured as an access-port, will application visibility data on the Catalyst 9000 Series switch provide visibility to applications on the switch port.

Distribution and Core Layer Switches

As mentioned in the restrictions above, Cisco DNA Center will only apply the wired AVC FNF flow monitor for application visibility data collection to Layer 2 (L2) access-ports on switches. Most distribution switches are generally configured for Layer 3 routed interfaces connecting to either Layer 3 core and access-switches. Alternatively, distribution switches may be configured with Layer 2 (L2) trunk interfaces connecting to Layer 2 access-switches – often in an EtherChannel configuration with port-channel interfaces. In other words, typically switch ports on distribution switches are not configured as access-ports, and therefore the wired AVC FNF flow monitor for application visibility may not be applied to such switch ports by Cisco DNA Center.

Likewise, typically switch ports on core switches are typically not configured as Layer 2 (L2) access-ports either. Therefore, the wired AVC FNF flow monitor for application visibility may not be applied to such switch ports by Cisco DNA center.

Again, note that NBAR2 is scaled (in terms of performance) for access ports on access-layer switches.

Technical Note: AVC / NBAR is not supported on Catalyst 9500 or Catalyst 9600 Series switches.

Cisco AireOS WLC Platforms – Application Visibility Data

For Cisco AireOS WLCs, application visibility data is collected at the WLC and streamed via telemetry from the WLC to Cisco DNA Center. Specifically, application visibility is collected through a subscription to the **Client-app-stat-events** network assurance telemetry channel within the AireOS WLC.

Technical Note: Unlike Catalyst 9000 Series switches, wired AVC Flexible NetFlow (FNF) flow monitors are not implemented for application visibility on Cisco AireOS WLCs.

Application visibility data collected by Cisco DNA Application Assurance on AireOS WLCs complements the application experience data collected on Cisco IOS XE routers and the application visibility data collected on Cisco Catalyst 9000 Series switches – by providing visibility into applications across the WLAN.

Technical Note: As of Cisco DNA Center release 1.3.1, application visibility data is only collected on Cisco AireOS WLCs. Collection and display of application visibility data on Cisco Catalyst 9800 WLCs is targeted for a future release.

The following are additional restrictions for application visibility on Cisco AireOS WLCs:

- Application visibility data on AireOS WLCs is not available for APs operating in FlexConnect mode.

Technical Note: SD-Access fabric-enabled wireless (FEW) deployments are not discussed within this deployment guide.

Where to Enable Cisco DNA Application Assurance on Cisco AireOS WLC Platforms?

As with IOS XE router platforms and Catalyst 9000 Series switches, Cisco DNA Application Assurance can be used to view information regarding application traffic – but only as the traffic crosses an observation point at which Cisco DNA Application Assurance data is being collected. For application visibility data on Cisco AireOS WLC platforms, observation points are essentially the APs to which the wireless clients are connected, although the application visibility data is sent from the AireOS WLC platforms that are subscribed to the **Client-app-stat-events** network assurance telemetry channel.

Deployment Guide Implementation

Ultimately, it is a design decision of the network administrator as to where to enable collection of Cisco DNA Application Assurance information to gain the desired visibility into application flows, while minimizing the collection of duplicate flows.

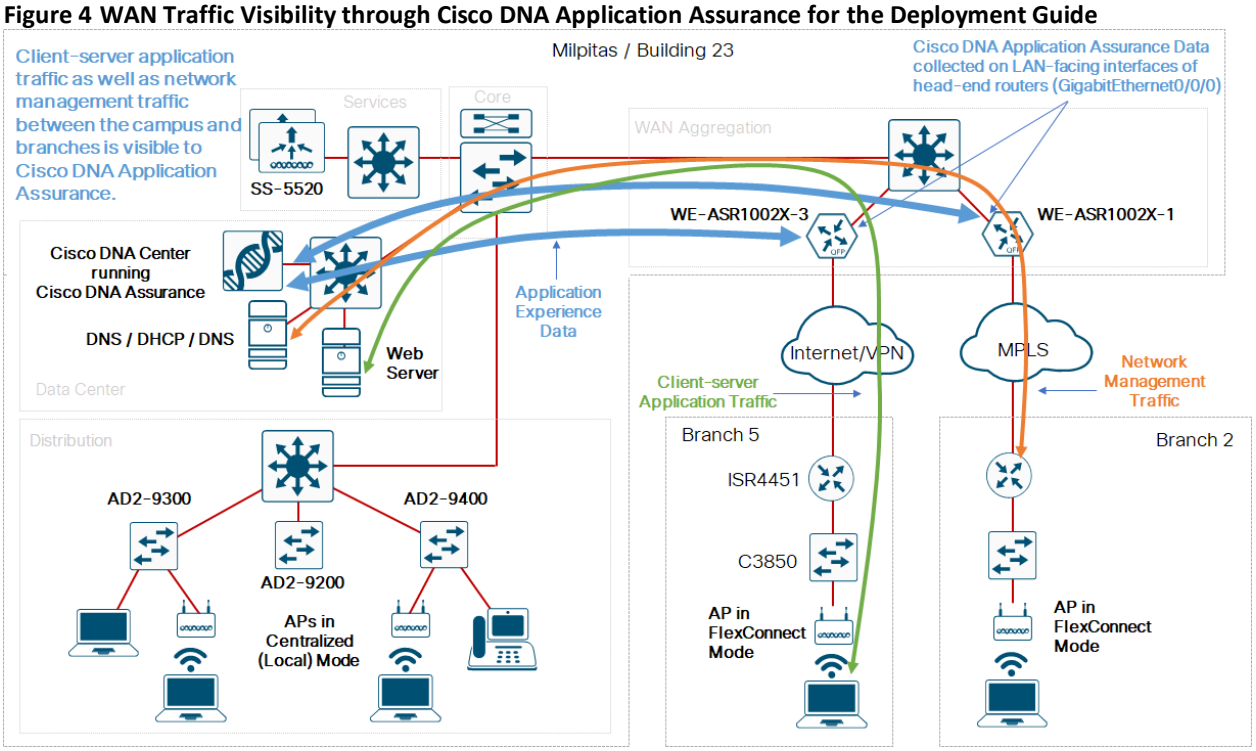
The following sections discuss the areas of the network where collection of Cisco DNA Application Assurance information was done for this deployment guide.

Wide Area Network (WAN)

The Cisco ezPM Application Performance profile context was applied to the LAN-facing interfaces (**GigabitEthernet0/0/0**) of the Cisco ASR 1K routers (**WE-ASR1002X-1** and **WE-ASR1002X-3**) serving as the WAN head-end routers within the campus. Application experience data is sent from the ASR 1K WAN head-end routers to Cisco DNA Center via Flexible NetFlow / IPFIX.

With this design, application flows between the campus and the branches are visible to Cisco DNA Center. This is highlighted in the figure below.

Figure 4 WAN Traffic Visibility through Cisco DNA Application Assurance for the Deployment Guide



The LAN-facing interfaces of the routers were chosen as observation points to ensure visibility of the application traffic across the enterprise network. The WAN head-end routers were chosen to minimize the number of Flexible NetFlow / IPFIX export flows which need to be handled by Cisco DNA Center and eliminate any bandwidth consumption due to exporting Flexible NetFlow / IPFIX data across the WAN.

However, not all application flows are visible with this design. Application flows within individual branches are not seen. Application flows between the two branches are seen, but only because each branch connects to a different head-end router. Flow information is also duplicated since branch-to-branch flows in this deployment guide cross the observation points of both head-end routers. Flows within the campus are not seen by the WAN head-end routers.

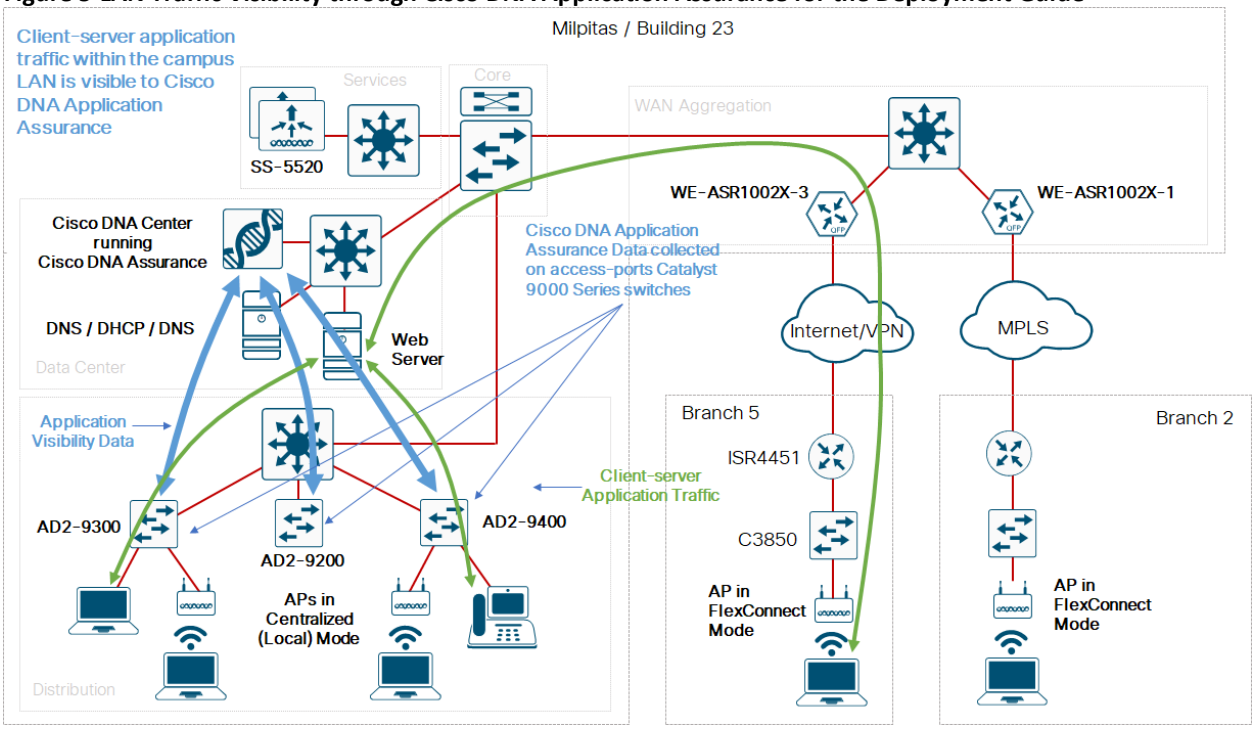
Finally, it should be noted that because Cisco DNA Center does not apply the Cisco ezPM Application Performance profile context to logical interfaces, a logical port-channel interface between the ASR 1K head-end routers and WAN aggregation switch was not implemented. Since NBAR2 requires symmetric routing – meaning return traffic must enter the same interface as outbound traffic – in order to identify certain applications; equal cost multi-path (ECMP) routes were also not used. A single routed uplink between each head-end ASR1K router ad the WAN aggregation switch was implemented for this deployment guide.

Local Area Network (LAN)

The wired AVC FNF flow monitor was applied to the access-ports (i.e. ports connected to end-user devices) of Catalyst 9000 Series switches access-layer switches within Cisco DNA Center.

With this design, application flows from wired end-user devices connected to the campus switches is visible to Cisco DNA Center. This is highlighted in the figure below.

Figure 5 LAN Traffic Visibility through Cisco DNA Application Assurance for the Deployment Guide



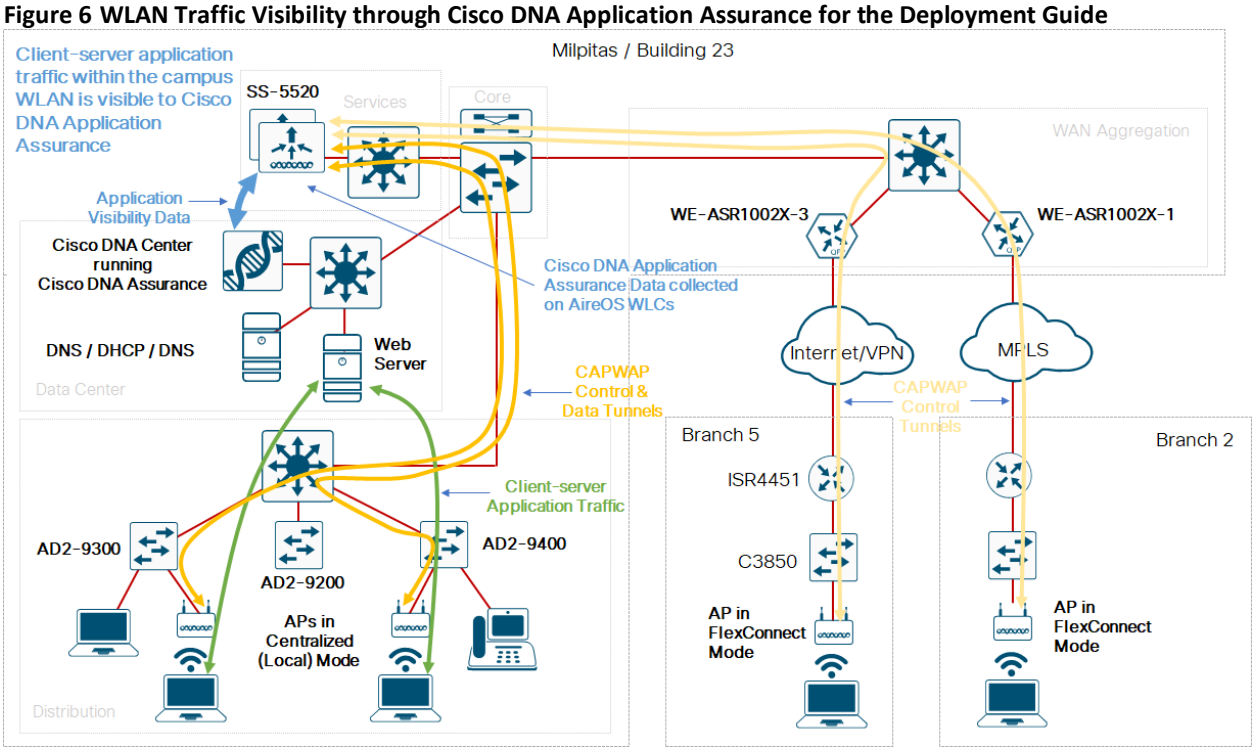
Since APs within the campus are operating in centralized (local) mode within this deployment guide, all traffic appears as either CAPWAP control or CAPWAP data traffic to the Catalyst 9000 Series switch ports. Therefore, although application visibility was enabled on the Catalyst 9000 Series switch ports connected to APs within the campus for this deployment guide, it provides limited value – other than displaying how much CAPWAP traffic is being generated by the APs connected to the switches. Visibility into the application traffic of campus wireless device is instead provided through the AireOS WLC itself.

Collection of application visibility data was not enabled for Catalyst 9000 Series distribution-layer or core switches within this deployment guide.

Wireless Local Area Network (WLAN)

Wireless telemetry was enabled at the campus AireOS WLC HA pair (SS-5520) for this deployment guide. With this design, application flows from wireless devices connected to APs within the campus are visible to Cisco DNA Center. This is highlighted in the figure below.

Figure 6 WLAN Traffic Visibility through Cisco DNA Application Assurance for the Deployment Guide



Since the APs within the branch are operating on FlexConnect mode, no application visibility data is provided through wireless telemetry for wireless devices within the branch. Visibility into the application traffic of branch wireless devices is instead provided through application experience data collected at the WAN head-end routers.

Deploy Cisco DNA Application Assurance on the Network

Enabling Cisco DNA Application Assurance on the network consists of the following procedures.

- Configure the IOS XE router interfaces for Cisco DNA Application Assurance
- Configure the Catalyst 9000 Series switch ports for Cisco DNA Application Assurance
- Configure the AireOS WLCs for Cisco DNA Application Assurance
- Configure routers, Catalyst 9000 Series switches, and AireOS WLCs for Maximal Telemetry within Cisco DNA Center

Procedure: Configure the IOS XE Router Interfaces for Cisco DNA Application Assurance

In order to specify the IOS XE router platform interfaces to which you wish to apply the Cisco ezPM Application Performance profile context, you must add the following tag to the interface description:

```
lan
```

For this design and deployment guide, Cisco DNA Application Assurance data is collected from the **GigabitEthernet0/0/0** interfaces of both WAN ASR1K head-end routers – **WE-ASR1002X-1** and **WE-ASR1002X-3**.

The following are the steps to configure an IOS XE router interface to collect Cisco DNA Application Assurance data.

1. SSH to the IOS XE router platform to which you wish to enable collection of Cisco DNA Application Assurance data.
2. Specify the necessary login credentials (userid/password or certificates).
3. Specify enable mode on the IOS XE router platform if necessary, by entering the exec-level command **enable** and pressing enter.

Technical Note: If the userid that you use to SSH into the platform has a privilege level of 15, you will automatically be taken into enable mode.

---

4. Enter configuration mode on the IOS XE router by entering the exec-level command **configuration terminal** and pressing enter.
5. Specify the interface which you wish receive Cisco DNA Application Assurance data. Press enter to go to the interface-level configuration.

For this deployment guide the command is **interface GigabitEthernet 0/0/0.**

6. Add the `lan` tag to the interface description.

For this deployment guide the command is **description lan Link to WA-6880-VSS**. Note that the tag only needs to appear within the description – it does not need to replace the description.

7. Exit interface-level configuration mode by typing the configuration-level command **exit** and pressing enter.
8. Exit configuration mode by typing the configuration-level command **exit** and pressing enter.
9. Save the running-configuration change to the startup-configuration by typing the exec-level command **copy running-config startup-config**.
10. Press enter to confirm the destination filename of **startup-config**.

11. Exit the router by typing the exec-level command **exit** and pressing enter.

The following example illustrates the steps above regarding how to specify that you want Cisco DNA Center to collect Cisco DNA Application Assurance data from the **GigabitEthernet0/0/0** interface of the **WE-ASR1002X-1** router platform with an IP address of **10.4.32.241**. Note that the userid has been modified within the example.

```
userid@host:~$ ssh userid@10.4.32.241
Password:


WE-ASR1002X-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
WE-ASR1002X-1(config)#interface GigabitEthernet 0/0/0
WE-ASR1002X-1(config-if)#description lan Link to WA-6880-VSS
WE-ASR1002X-1(config-if)#exit
WE-ASR1002X-1(config)#exit
WE-ASR1002X-1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
WE-ASR1002X-1#exit
Connection to 10.4.32.241 closed by remote host.
Connection to 10.4.32.241 closed.
userid@host:~$
```

12. Repeat **Steps 1- 11** for the second head-end router, **WE-ASR1002X-3**.

When you are complete both **GigabitEthenet0/0/0** interface descriptions should look as follows:

WE-ASR1002X-1

```
interface GigabitEthernet0/0/0
 description lan Link to WA-6880-VSS
 ip address 10.4.32.2 255.255.255.252
```

WE-ASR1002X-3

```
interface GigabitEthernet0/0/0
 description lan Link to WA-6880-VSS
 ip address 10.4.32.10 255.255.255.252
```

You should make sure Cisco DNA Center is synced with the configuration changes of the previous procedure before enabling **Maximal Visibility** within the **Network Telemetry** dashboard. You can wait until the inventory resync interval for the two ASR 1K WAN head-end routers (**WE-ASR1002X-1** and **WE-ASR1002X-3**) passes. Alternatively, you can manually resync the inventory for the two ASR 1K WAN head-end routers using the following steps.

13. Login to the Cisco DNA Center web console using the IP address or fully qualified domain name of your instance.

For example: https://<Cisco_DNA_Center_IPaddr_or_FQDN>. The credentials (userid and password) you enter must have SUPER-ADMIN-ROLE OR NETWORK-ADMIN-ROLE privileges.

14. From the main Cisco DNA Center dashboard, navigate to **Provision**.

This will take you to the main provisioning screen that displays the devices within the inventory. By default, the **Focus:** will be set for **Inventory**.

15. Locate and check the boxes next to **WE-ASR1002X-1** and **WE-ASR1002X-3**.

16. From the drop-down menu under **Actions**, select **Inventory > Resync Device**.

A pop-up warning will ask you to confirm the resync.

17. Select **OK** to confirm the resync and close the warning.

The **last sync status** of **WE-ASR1002X-1** and **WE-ASR1002X-3** will transition to **In Progress**. After a few moments the **last sync status** will transition back to **Managed**.

Once the two head-end routers are resynced, you can proceed to enable **Maximal Visibility** for the devices within the **Network Telemetry** dashboard.

Procedure: Configure the Catalyst 9000 Series switch ports for Cisco DNA Application Assurance

In order to specify the Catalyst 9000 Series switch ports to which you wish to apply the wired AVC FNF flow monitor, you must add the following tag to the switch port description:

```
lan
```

In addition to this, you must ensure that the switch port is explicitly configure as an access-port through the following interface-level command:

```
switchport mode access
```

For this design and deployment guide, Cisco DNA Application Assurance data is collected on the following Catalyst 9000 Series switch ports:

- **AD2-9200** - **GigabitEthernet1/0/1 – GigabitEthernet 1/0/24**
- **AD2-9300 – GigabitEthernet1/0/1 – GigabitEthernet 1/0/48** and **GigabitEthernet2/0/1 – GigabitEthernet 2/0/48**
- **AD2-9400 – GigabitEthernet1/0/1 – GigabitEthernet 1/0/48**, **GigabitEthernet2/0/1 – GigabitEthernet 2/0/48**, and **GigabitEthernet5/0/1 – GigabitEthernet 5/0/24**

The following are the steps to configure a range of Catalyst 9000 Series switch ports to collect Cisco DNA Application Assurance data.

1. SSH to the Catalyst 9000 Series switch platform to which you wish to enable collection of Cisco DNA Application Assurance data.

2. Specify the necessary login credentials (userid/password or certificates).

3. Specify enable mode on the router platform if necessary, by entering the exec-level command **enable** and pressing enter.

Technical Note: If the userid that you use to SSH into the platform has a privilege level of 15, you will automatically be taken into enable mode.

---

4. Enter configuration mode on the router by entering the exec-level command **configuration terminal** and pressing enter.

5. Specify the switch port range which you wish receive Cisco DNA Application Assurance data. Press enter to go to the interface-level configuration.

For the **AD2-9200** switch within this deployment guide the command is **interface range GigabitEthernet 0/0/0-24.**

6. Add the `lan` tag to the interface description.

For this deployment guide the command is **description lan**. Note that the tag only needs to appear within the description – it does not need to replace the description.

7. Exit interface-level configuration mode by typing the configuration-level command **exit** and pressing enter.

8. Exit configuration mode by typing the configuration-level command **exit** and pressing enter.

9. Save the running-configuration change to the startup-configuration by typing the exec-level command **copy running-config startup-config**.

10. Press enter to confirm the destination filename of **startup-config**.

11. Exit the Catalyst 9000 Series switch by typing the exec-level command **exit** and pressing enter.

The following example illustrates the steps above regarding how to specify that you want Cisco DNA Center to collect Cisco DNA Application Assurance data from the **GigabitEthernet0/0/0-24** interface range of the **AD2-9200** Catalyst 9000 Series switch platform with an IP address of **10.4.79.15**. Note that the userid has been modified within the example.

```
userid@host:~$ ssh userid@10.4.79.15
Password:


AD2-9200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AD2-9200(config)#interface range GigabitEthernet1/0/1-24
AD2-9200(config-if-range)#description lan
AD2-9200(config-if-range)#switchport mode access
AD2-9200(config-if-range)#exit
AD2-9200(config)#exit
AD2-9200#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
AD2-9200#exit
Connection to 10.4.79.15 closed by remote host.
Connection to 10.4.79.15 closed.
userid@host:~$
```

12. Repeat **Steps 1- 11** for the other two Catalyst 9000 Series switches, **AD2-9300** and **AD2-9400**.

When you are complete the GigabitEthernet switch ports of the three switches should include the following commands:

```
interface GigabitEthernet1/0/1
 description lan
 switchport mode access
```

As with the routers discussed above, you should make sure Cisco DNA Center is synced with the configuration changes of the previous procedure before enabling maximal visibility within the **Network Telemetry** dashboard. You can wait until the inventory resync interval for the three Catalyst 9000 Series access-switches (**AD2-9200**, **AD2-9300**, and **AD2-9400**) passes. Alternatively, you can manually resync the inventory for the three Catalyst 9000 Series switches using the following steps.

13. Login to the Cisco DNA Center web console using the IP address or fully qualified domain name of your instance.

For example: https://<Cisco_DNA_Center_IPaddr_or_FQDN>. The credentials (userid and password) you enter must have SUPER-ADMIN-ROLE OR NETWORK-ADMIN-ROLE privileges.

14. From the main Cisco DNA Center dashboard, navigate to **Provision**.

This will take you to the main provisioning screen that displays the devices within the inventory. By default, the **Focus:** will be set for **Inventory**.

15. Locate and check the boxes next to **AD2-9200**, **AD2-9300**, and **AD2-9400**.

16. From the drop-down menu under **Actions**, select **Inventory > Resync Device**.

A pop-up warning will ask you to confirm the resync.

17. Select **OK** to confirm the resync and close the warning.

The **last sync status** of **AD2-9200**, **AD2-9300**, and **AD2-9400** will transition to **In Progress**. After a few moments the **last sync status** will transition back to **Managed**.

Procedure: Configure the AireOS WLCs for Cisco DNA Application Assurance

Configuration of AireOS WLCs for Cisco DNA Application Assurance depends upon whether Cisco DNA Center is being used for automation of WLANs or not.

Cisco DNA Center Not Used for Automation of WLANs

Technical Note: For this deployment guide, the WLANs were deployed using Cisco DNA Center automation. The example shown in this section is for reference only.

When Cisco DNA Center is not used for automation of WLANs, you must add the following tag to the wireless profile names corresponding to SSIDs configured on the AireOS WLCs, in order to enable the collection of Cisco DNA Application Assurance data.

```
lan
```

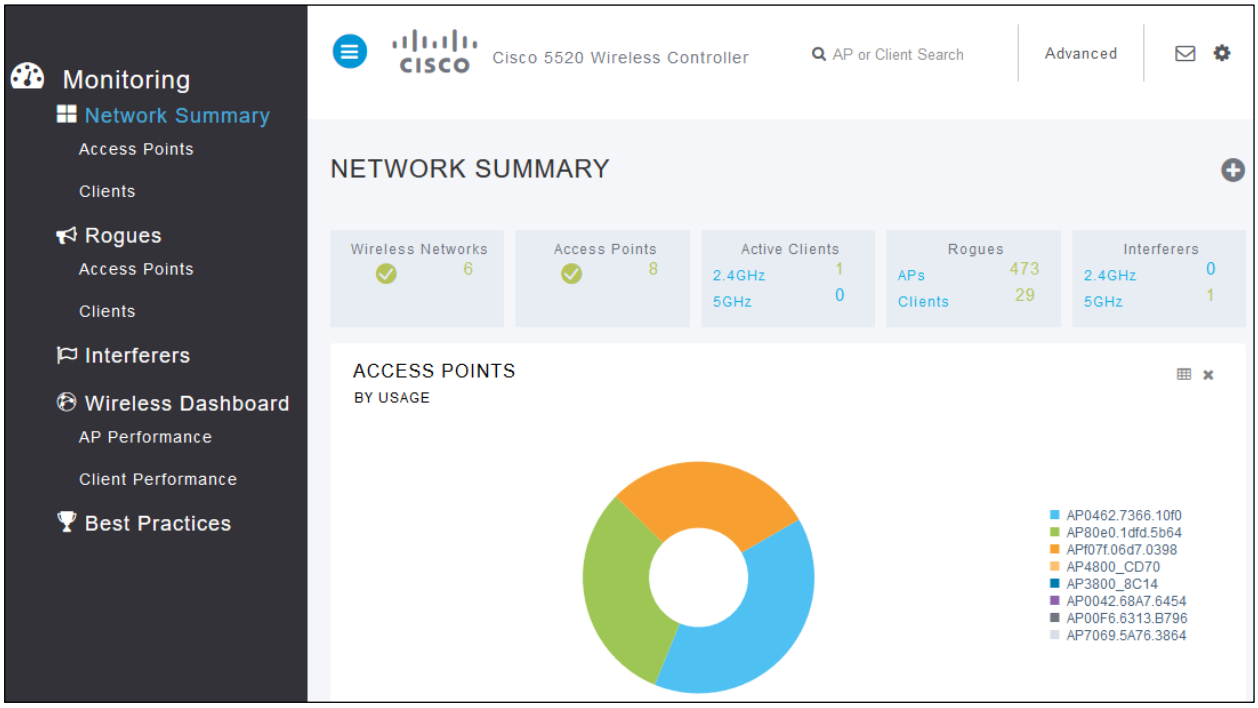
This can be done via the AireOS WLC GUI or via CLI. The following are the steps (using the web-based GUI) to configure an SSID on an AireOS WLC to collect Cisco DNA Application Assurance data.

18. Login to the AireOS WLC web console using the IP address or fully qualified domain name of your instance.

For example: https://<Cisco_AireOS_WLC_IPaddr_or_FQDN>. The credentials (userid and password) you enter must have ReadWrite access.

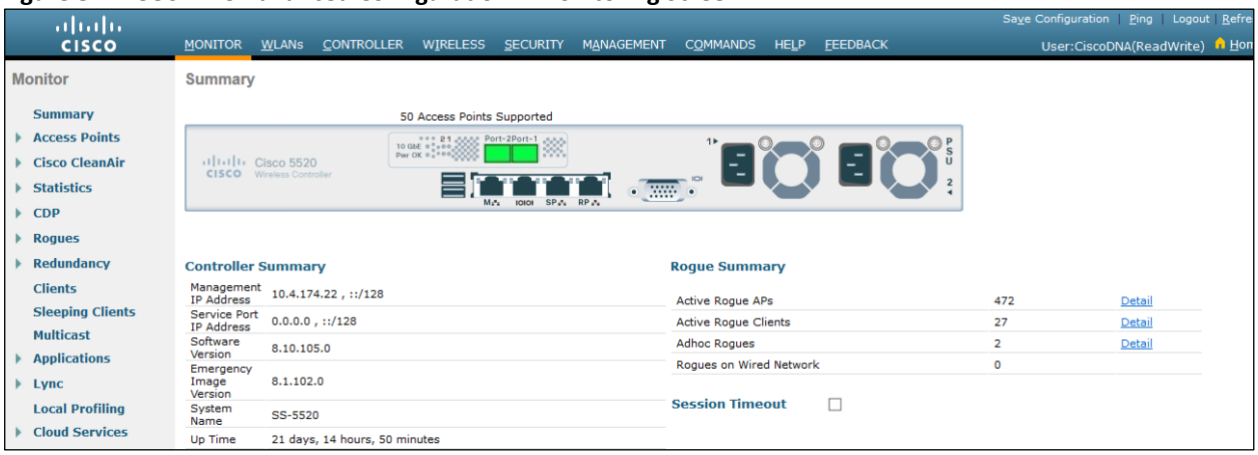
19. From the AireOS WLC **Monitoring → Network Summary** screen, click the **Advanced** button in the top right corner of the screen, as shown in the figure below.

Figure 7 AireOS WLC Monitoring → Network Summary screen



This will take you to a screen similar to that shown in the following figure.

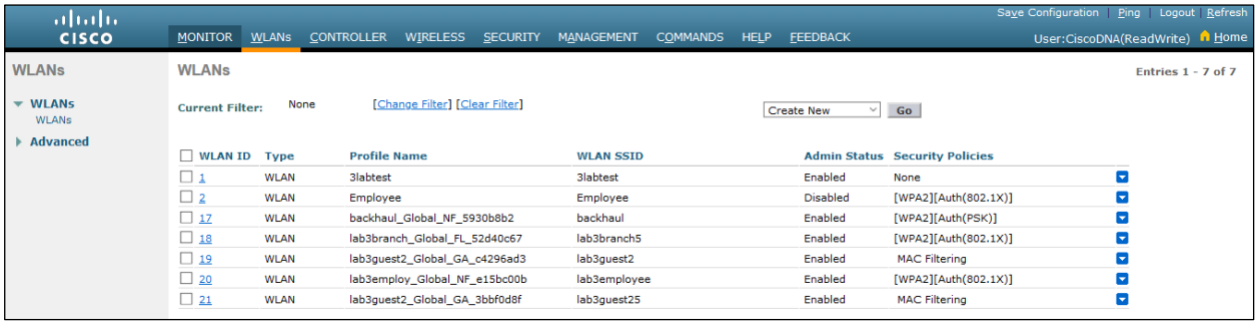
Figure 8 AireOS WLC Advanced Configuration – Monitoring Screen



20. Navigate to **WLANs**.

This will list the WLANs / SSIDs configured on the AireOS WLC. An example is shown in the following figure.

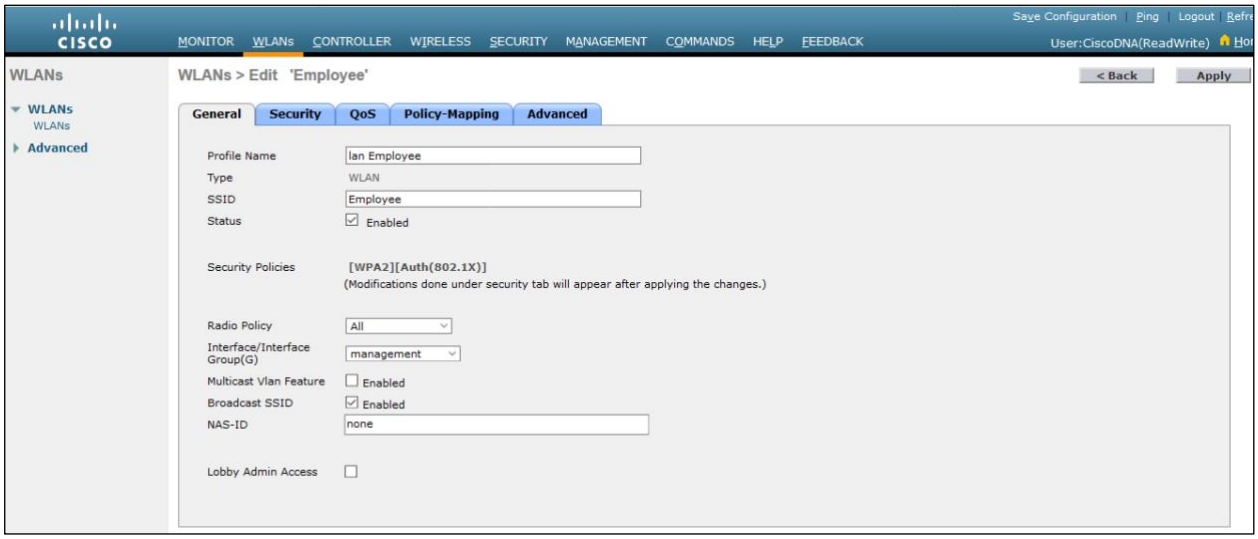
Figure 9 AireOS Controller WLANs



21. Click on the **WLAN ID** number (not the check box) to display details of the WLAN.

By default the **General** tab will be selected for the WLAN. An example of the **Employee** WLAN (**WLAN ID 2**) from the figure above, is shown in the figure below.

Figure 10 WLAN Details



22. Modify the Profile Name to include the word “lan” as shown in the figure above.

Note that the tag only needs to appear within the description – it does not need to replace the description.

23. Click the **Apply** button to apply the configuration changes to the WLAN.

24. Click the **Save Configuration** button in the upper right corner of the screen.

A pop-up box will appear asking you to confirm that you wish to save the configuration changes.

25. Click the **OK** button to save the changes to the WLAN.

26. Once the configuration changes are saved, click the **Logout** button in the upper right corner of the screen to log out of the WLC.

As with Catalyst 9000 Series switches and routers discussed above, you should make sure Cisco DNA Center is synced with the configuration changes of the previous procedure before enabling maximal visibility within the **Network Telemetry** dashboard. You can wait until the inventory resync interval for the AireOS WLC (**SS-5520**) passes. Alternatively, you can manually resync the inventory for the AireOS WLC using the following steps.

27. Login to the Cisco DNA Center web console using the IP address or fully qualified domain name of your instance.

For example: https://<Cisco_DNA_Center_IPaddr_or_FQDN>. The credentials (userid and password) you enter must have SUPER-ADMIN-ROLE OR NETWORK-ADMIN-ROLE privileges.

28. From the main Cisco DNA Center dashboard, navigate to **Provision**.

This will take you to the main provisioning screen that displays the devices within the inventory. By default, the **Focus:** will be set for **Inventory**.

29. Locate and check the boxes next to **SS-5520**.

30. From the drop-down menu under **Actions**, select **Inventory > Resync Device**.

A pop-up warning will ask you to confirm the resync.

31. Select **OK** to confirm the resync and close the warning.

The **last sync status** of **SS-5520** will transition to **In Progress**. After a few moments the **last sync status** will transition back to **Managed**.

Cisco DNA Center Used for Automation of WLANs

When Cisco DNA Center is used for automation of WLANs, Cisco DNA Application Assurance is automatically enabled when SSIDs are created through wireless network profiles and subsequently provisioned to the AireOS WLCs. No configuration changes need to be made to the wireless profile names corresponding to the SSIDs created, because application visibility is already part of wireless network profiles.

Technical Note: When using Cisco DNA Center for automation, **DO NOT** modify the wireless profile name on the AireOS WLCs corresponding to an SSID. The wireless profile name is dynamically generated by Cisco DNA Center during provisioning. If you change the wireless profile name and subsequently re-provision an AireOS WLC, Cisco DNA Center may attempt to remove / replace the modified WLAN / SSID. This may result in a wireless service outage (because the SSID will no longer be broadcast by the APs if it is removed by Cisco DNA Center) and may require manual intervention via the WLC GUI or CLI to correct.

Procedure: Configure IOS XE Routers, Catalyst 9000 Series Switches, and AireOS WLCs for Maximal Telemetry within Cisco DNA Center

The `lan` tag within the router or Catalyst 9000 Series switch interface description, or the AireOS WLAN profile name, only indicates to Cisco DNA Center the desire to collect Cisco DNA Application Assurance information on that interface. You must still configure the platforms for **Maximal Visibility** within the **Network Telemetry** dashboard within Cisco DNA Center.

Technical Note: You do not have to configure AireOS WLCs for **Maximal Visibility** if Cisco DNA Center has been used for automation of the WLANs, because application visibility is already part of wireless network profiles.

1. Login to the Cisco DNA Center web console using the IP address or fully qualified domain name of your instance.

For example: https://<Cisco_DNA_Center_IPaddr_or_FQDN>. The credentials (userid and password) you enter must have SUPER-ADMIN-ROLE OR NETWORK-ADMIN-ROLE privileges.

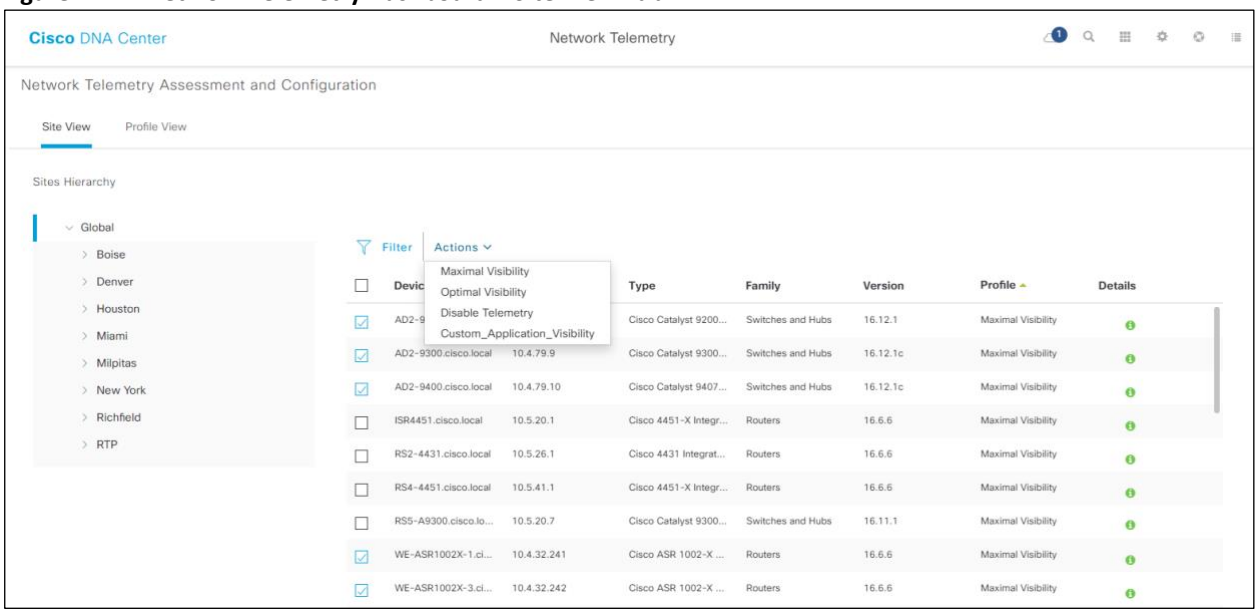
2. From the main Cisco DNA Center dashboard, click on the **Network Telemetry** widget in the **Tools** section at the bottom of the screen.

This will take you to the **Network Telemetry** dashboard.

3. Within the Network Telemetry dashboard click on the **Site View** tab.

An example is shown in the following figure.

Figure 11 Network Telemetry Dashboard – Site View Tab



4. Select the two ASR 1K WAN head-end routers (**WE-ASR1002X-1** and **WE-ASR1002X-3**), and the three Catalyst 9000 Series access-layer switches (**AD2-9200**, **AD2-9300**, and **AD2-9400**).

5. Optionally, if Cisco DNA Center has not been used to automate the deployment of the WLANs / SSIDs, select the AireOS WLC (**SS-5520**).

For this deployment guide the WLANs were deployed using Cisco DNA Center automation. Therefore, **Maximal Visibility** was not enabled for the AireOS WLC (**SS-5520**).

6. From the drop-down menu under **Actions**, select **Maximal Visibility**.

Under the **Profile** column, the entries for the network devices should change to **Maximal Visibility**.

Cisco DNA Center will immediately configure the devices to send Cisco DNA Application Assurance data to Cisco DNA Center. The following are the configuration changes provisioned by Cisco DNA Center onto each network device, based upon the network device type.

Cisco IOS XE Router Platforms

Cisco DNA Center will configure the Cisco ezPM Application Performance profile context on the Cisco IOS XE router platforms and apply the profile context to the interfaces with the `lan` tag in the description. These interfaces are known as the observation points within Cisco ezPM.

The following is an example of the configuration provisioned onto the Cisco IOS XE router platforms:

```
!
performance monitor context tesseract profile application-performance
 exporter destination 10.4.48.183 source Loopback0 transport udp port 6007
 traffic-monitor application-client-server-stats
 traffic-monitor application-response-time
 traffic-monitor media
!
```

```
~
!
interface GigabitEthernet0/0/0
 description lan Link to WA-6880-VSS
 ip address 10.4.32.2 255.255.255.252
 performance monitor context tesseract
!
```

Technical Note: Enabling telemetry – whether it is **Optimal Visibility** or **Maximal Visibility** on network devices configures more than the Cisco ezPM Application Performance profile discussed within this design and deployment guide. This design and deployment guide focuses only on Cisco DNA Application Assurance, and therefore focuses only on the specific additional functionality enabled on top of **Optimal Visibility**, when **Maximal Visibility** is configured for Cisco IOS XE routers. Additional design and deployment guides will discuss the functionality enabled and configuration configured when selecting **Optimal Visibility**.

As can be seen in the configuration example above, performance monitor data is exported to the IP address of the Cisco DNA Center cluster (which in this deployment guide is **10.4.83.183**) sourced from the **Loopback0** interface. The source interface of the performance monitor data must be able to reach the Cisco DNA Center cluster. Configuring a **Loopback0** interface on Cisco IOS XE routers, which is then specified to be used to manage the routers during the discovery of network devices, is a best practice for Cisco DNA Assurance, where possible.

Cisco Catalyst 9000 Series Switch Platforms

Cisco DNA Center will configure a wired AVC FNF flow record, flow monitor, and flow exporter on the Catalyst 9000 Series switch platforms; and then apply the flow monitor in both the ingress and egress directions to the switch ports with the `lan` tag in the description. These switch ports are known as the observation points for the wired AVC FNF flow monitor.

Wired AVC FNF on Catalyst 9000 Series switches supports two types of predefined flow records — Legacy Bidirectional flow records and Directional flow records (ingress and egress). A total of four different predefined flow records, two bidirectional flow records and two directional flow records, are supported. The legacy bidirectional records are client/server application statistics records, and the new directional records are application-stats for input/output. Please see the **System Management Configuration Guide, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9300 Switches)** for details regarding each of the predefined wired AVC FNF flow records supported by Catalyst 9000 Series switches:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-12/configuration_guide/sys_mgmt/b_1612_sys_mgmt_9300_cg/application_visibility_and_control_in_a_wired_network.html

Technical Note: User-defined FNF records which include AVC / NBAR are not supported on Catalyst 9000 Series switches. In other words, a user-defined FNF record cannot include 'match application name'. Only the four predefined wired AVC FNF flow records discussed above, support AVC / NBAR. However, FNF records which do not include AVC / NBAR – meaning they do not include 'match application name' and are therefore non-AVC FNF records – can be user-defined. Note that there may be differences in the restrictions for where non-AVC FNF flow monitors can be applied to switch ports.

Cisco DNA Center configures one of the predefined Legacy Bidirectional flow records, as shown in the example below, onto Catalyst 9000 Series switch platforms:

```
!
flow record dnacrecord
 match ipv4 version
 match ipv4 protocol
 match application name
 match connection client ipv4 address
 match connection server ipv4 address
 match connection server transport port
```

```
 match flow observation point
 collect timestamp absolute first
 collect timestamp absolute last
 collect flow direction
 collect connection initiator
 collect connection client counter packets long
 collect connection client counter bytes network long
 collect connection server counter packets long
 collect connection server counter bytes network long
 collect connection new-connections
!
```

The following is an example of the flow exporter and flow monitor configuration provisioned onto the Catalyst 9000 Series switch platforms:

```
!
flow exporter dnacexporter
 destination 10.4.48.183
 source Vlan179
 transport udp 6007
 export-protocol ipfix
 option interface-table timeout 10
 option vrf-table timeout 10
 option sampler-table
 option application-table timeout 10
 option application-attributes timeout 10
!
!
flow monitor dnacmonitor
 exporter dnacexporter
 cache timeout inactive 10
 cache timeout active 60
 record dnacrecord
!
~
!
interface GigabitEthernet1/0/1
 description lan
 switchport mode access
 ip flow monitor dnacmonitor input
 ip flow monitor dnacmonitor output
!
```

As can be seen in the configuration example above, wired AVC FNF flow exporter exports data to the IP address of the Cisco DNA Center cluster (which in this deployment guide is **10.4.83.183**) sourced from the **Vlan179** interface. Catalyst switches configured as Layer 2 (L2) access-switches often do not have loopback addresses. However, Layer 2 (L2) access-switches will require an IP address to be configured for management access by Cisco DNA Center. The source interface of the wired AVC FNF data must be able to reach the Cisco DNA Center cluster.

Cisco AireOS WLC Platforms

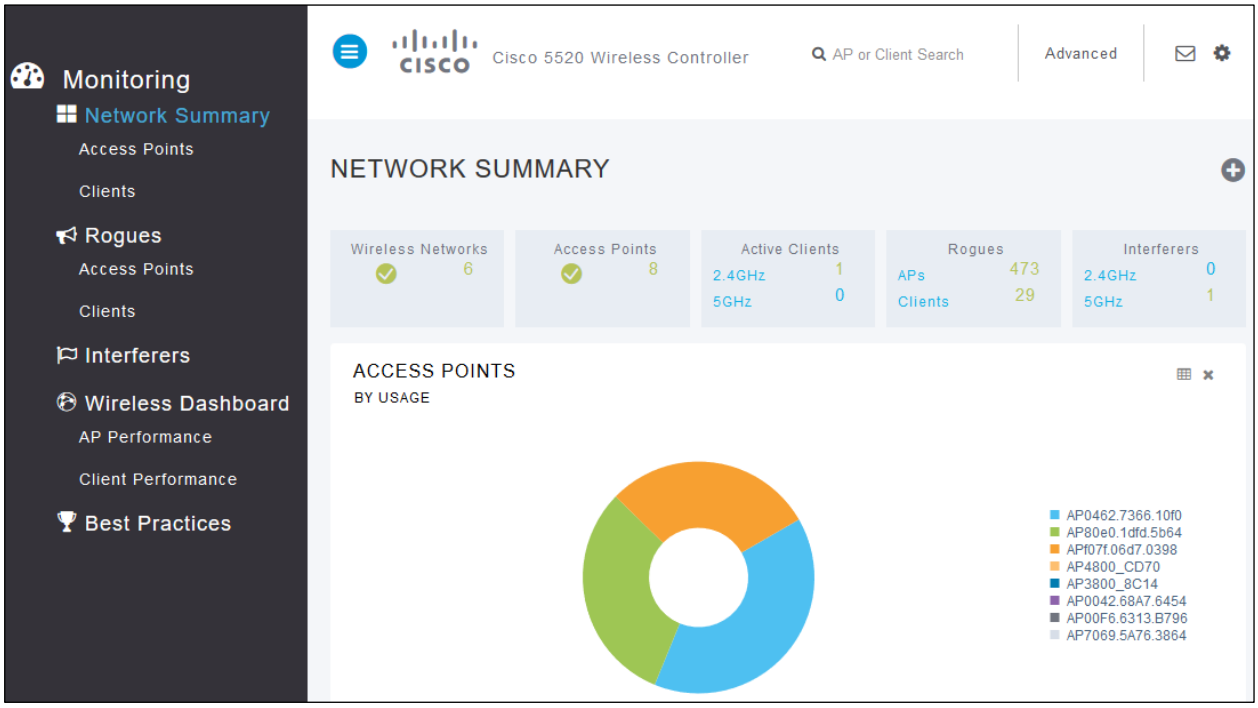
Cisco DNA Center will automatically enable wireless telemetry and subscribe to all available channels as part of Cisco DNA Assurance. You can view the configuration through the following steps.

1. Login to the AireOS WLC web console using the IP address or fully qualified domain name of your instance.

For example: https://<Cisco_AireOS_WLC_IPaddr_or_FQDN>. The credentials (userid and password) you enter must have ReadWrite access.

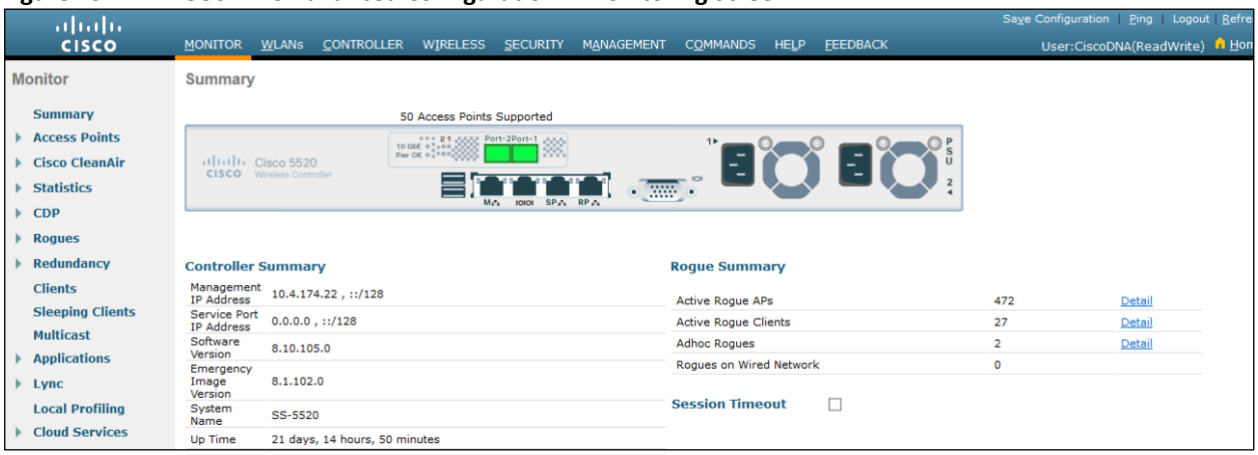
2. From the AireOS WLC **Monitoring → Network Summary** screen, click the **Advanced** button in the top right corner of the screen, as shown in the figure below.

Figure 12 AireOS WLC Monitoring → Network Summary screen



This will take you to a screen similar to that shown in the following figure.

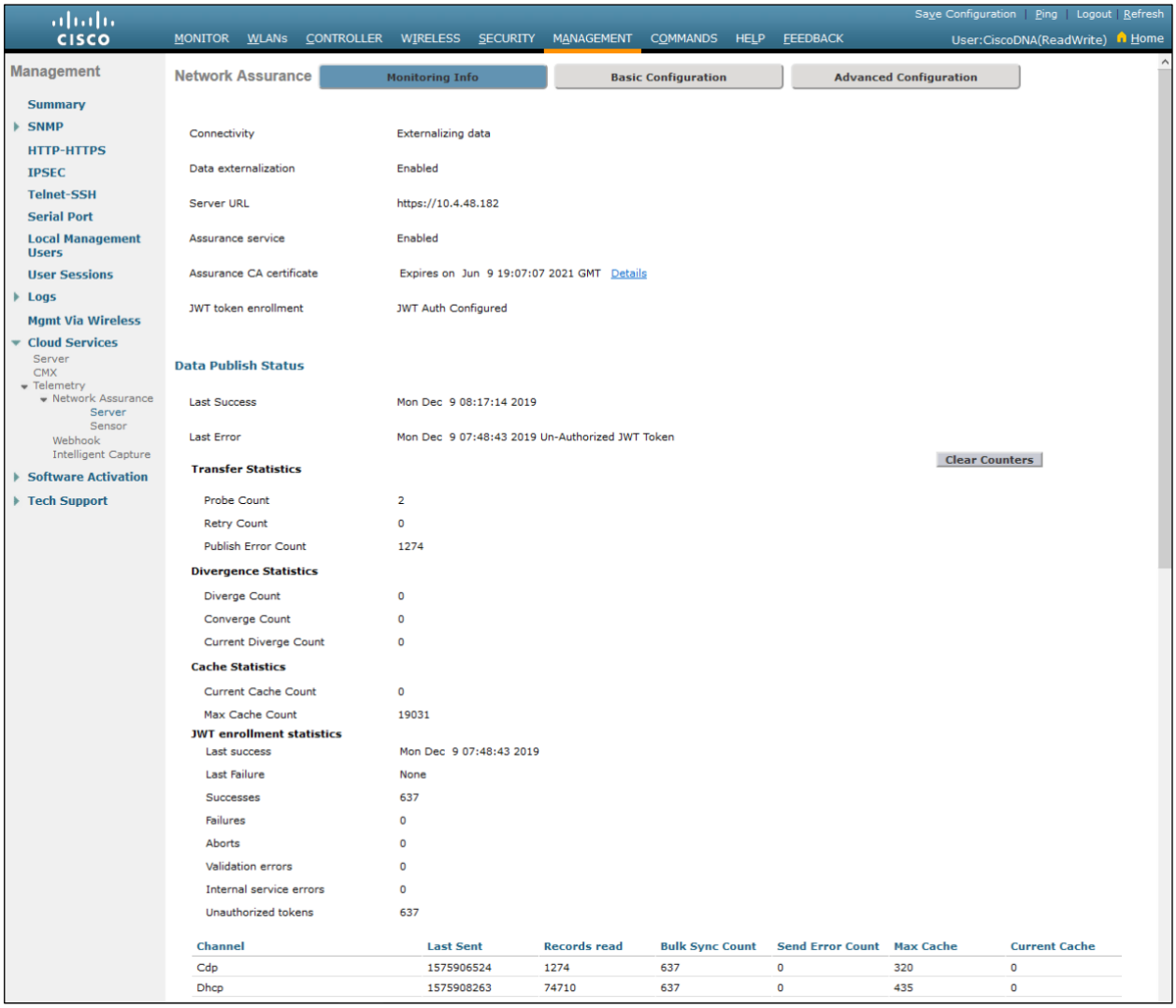
Figure 13 AireOS WLC Advanced Configuration – Monitoring Screen



3. Navigate to **Management → Cloud Services → Telemetry → Network Assurance → Server**.

This will take you to the monitoring tab of the Network Assurance screen. An example is shown in the following figure.

Figure 14 AireOS Controller Network Assurance – Monitoring Tab

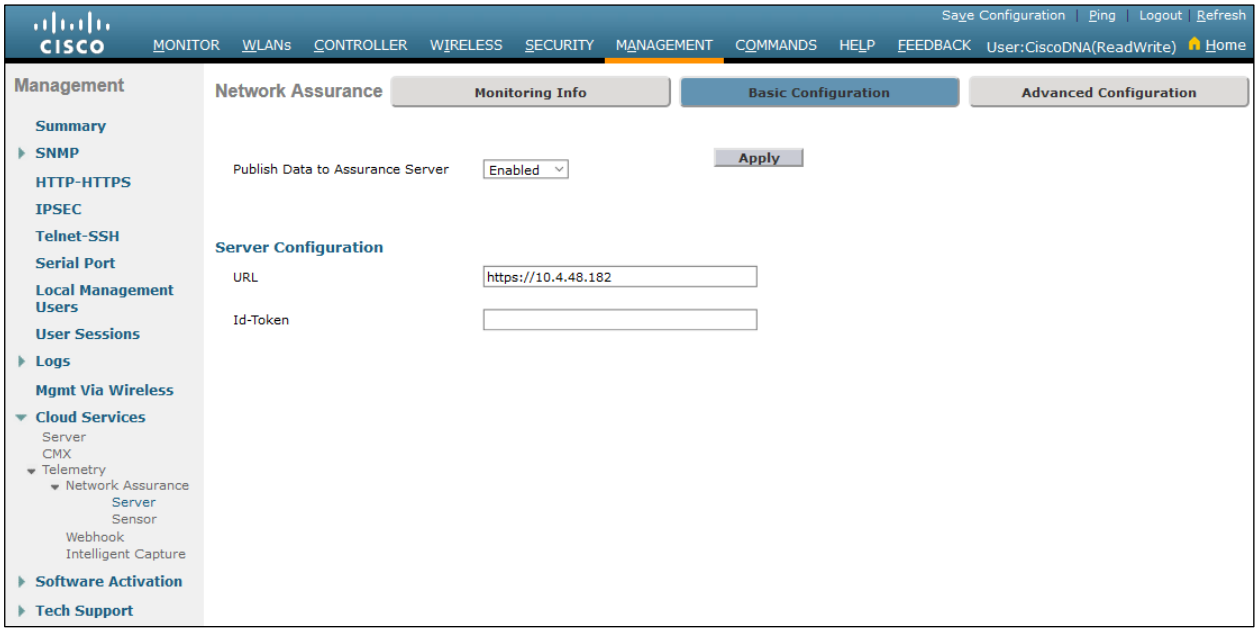


The **Monitoring** tab shows the current state of telemetry configured on the WLC, as well as the channels which are currently subscribed. Since telemetry is a publish / subscribe model, each subscribed channel will display the number of records sent as well as a timestamp of the last record sent.

4. Click on the **Basic Configuration** tab.

The **Basic Configuration** tab allows you to enable / disable the publishing of channel subscription data to the Cisco DNA Assurance server. Cisco DNA Center will automatically enable this as part of Cisco DNA Assurance. An example is shown in the figure below.

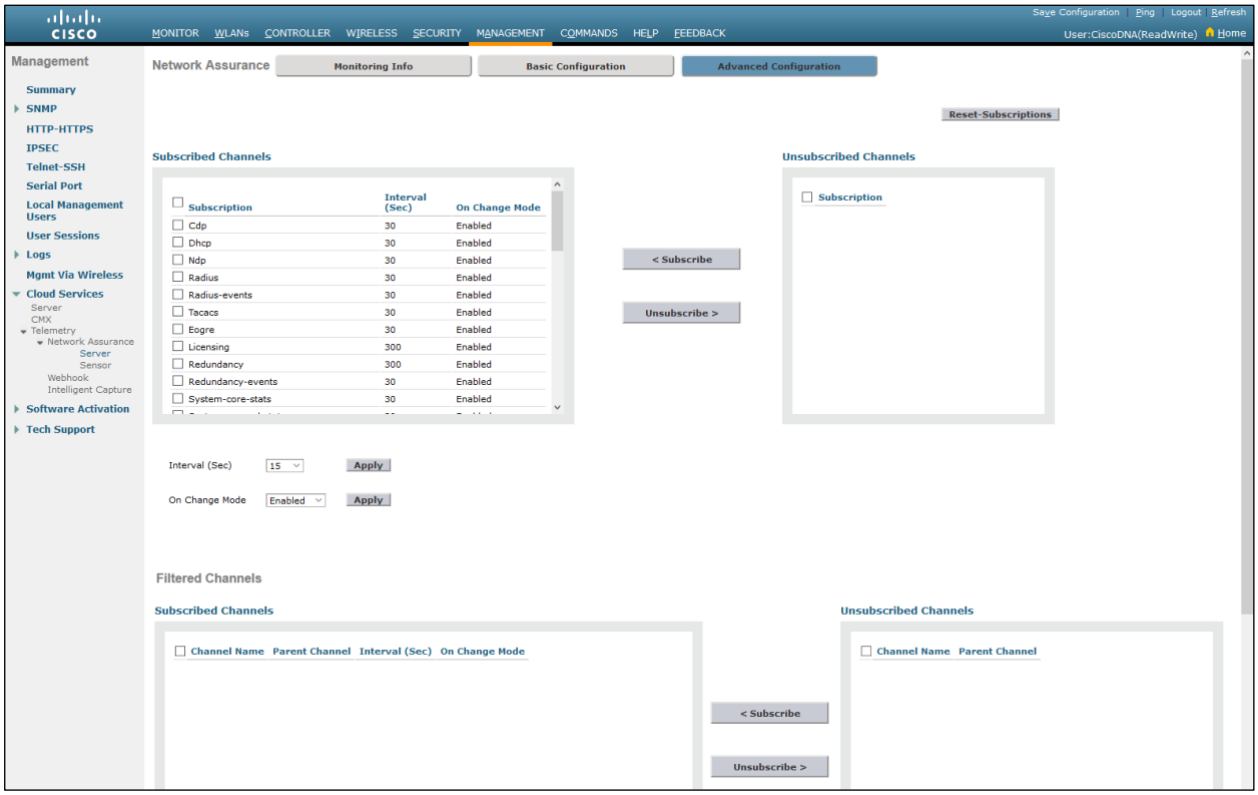
Figure 15 AireOS Controller Network Assurance – Basic Configuration Tab



5. Click on the **Advanced Configuration** tab.

The **Advanced Configuration** allows you to subscribe / unsubscribe to individual telemetry channels. Cisco DNA Center will automatically subscribe all channels as part of Cisco DNA Assurance. An example is shown in the figure below.

Figure 16 AireOS Controller Network Assurance – Advanced Configuration Tab



If you scroll down to the bottom of the subscribed channels, you will see the **Client-app-stats-events** channel is subscribed with an interval of **30 seconds**, and with **On Change Mode Enabled**. Based on this configuration, incremental application statistics for each interval will automatically be sent from the AireOS WLC to Cisco DNA Center every 30 seconds.

6. Once you have viewed the configuration, you can click the **Logout** button in the upper right corner of the screen to log out of the WLC.

Operate the Network

This section presents multiple use cases around how to monitor and troubleshoot applications and application performance through Cisco DNA Application Assurance. For a more comprehensive look at the application information which can be viewed through Cisco DNA Application Assurance, please see **Appendix C**.

Use Case #1: View Application Traffic across the LAN

Use Case Scenario

The following is the scenario for this use case. As a member of the network planning team, you wish to gain visibility into the applications and their usage across your LAN, through your Catalyst 9000 Series access-layer switches.

Procedure: Use Cisco DNA Application Assurance to View Application Traffic on Catalyst 9000 Series Switches

Cisco DNA Application Assurance can be used to gain visibility into applications and their throughput – as the application traffic crosses the observation points at which Cisco DNA Application Assurance data is being collected. For this use case, the Cisco DNA Application Assurance observation points are the access-ports (i.e. ports connected to end-user devices) of the Catalyst 9000 Series access-layer switches (**AD2-9200**, **AD2-9300**, and **AD2-9400**).

The following are the steps to view application visibility data on Catalyst 9000 Series switches from within Cisco DNA Center.

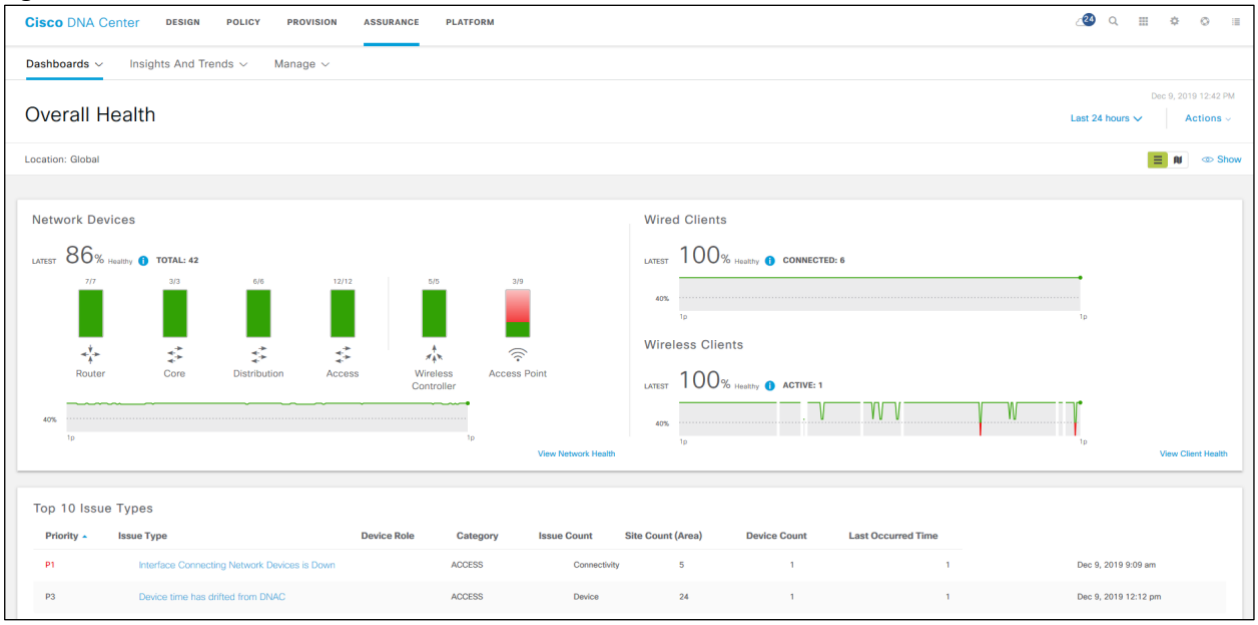
1. Login to the Cisco DNA Center web console using the IP address or fully qualified domain name of your instance.

For example: https://<Cisco_DNA_Center_IPaddr_or_FQDN>.

2. From the main Cisco DNA Center dashboard navigate to **Assurance**.

This will take you to the **Overall Health** dashboard within Cisco DNA Assurance. An example is shown in the following figure.

Figure 17 Cisco DNA Assurance Overall Health Dashboard



3. Navigate to **Dashboards → Health → Network Health**.

This will take you to the **Network Health** dashboard.

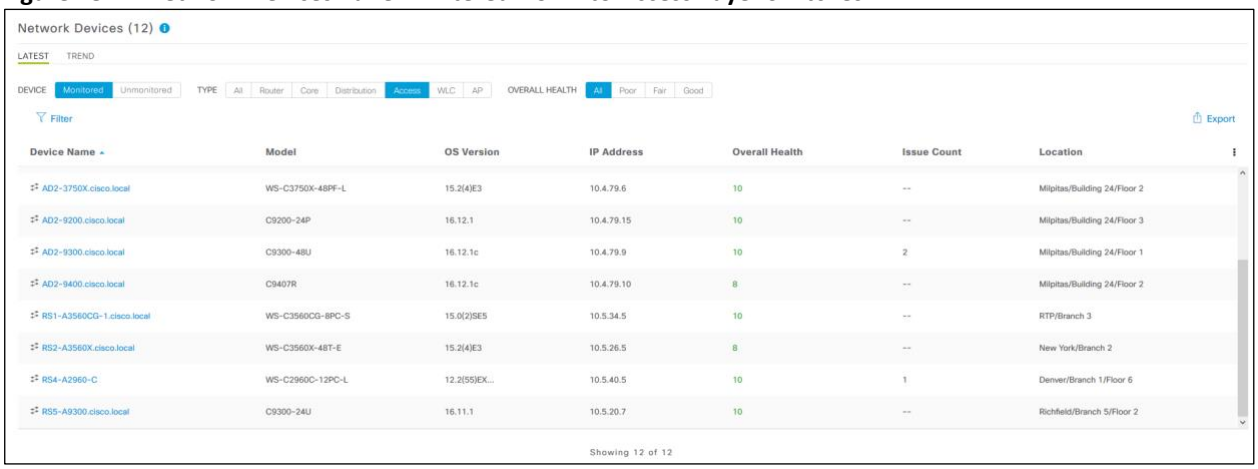
4. Scroll down to the **Network Devices** panel at the bottom of the **Network Health** dashboard.

Here you will see a list of network devices seen by Cisco DNA Application Assurance.

5. Select **DEVICE** – **Monitored**, **TYPE** – **Access**, **OVERALL HEALTH** - **All**

The network devices list will be filtered down to monitored access-layer switches. An example is shown in the figure below.

Figure 18 Network Devices Panel – Filtered Down to Access-Layer Switches



6. Locate one of the Catalyst 9000 Series access-layer switches in the list of network devices and click on it.

For this deployment guide, the Catalyst 9000 Series switch selected is **AD2-9300**. This will bring up the **Device 360** screen for the switch.

7. Scroll down and expand the **Application Experience** section of the **Device 360** screen for the switch.

This will display the applications seen by the switch ports of the Catalyst 9200 Series switch that are configured to be observation points. As previously mentioned, these are the access-ports to which the wired AVC FNF flow monitor is applied. An example of the **Application Experience** data is shown in the figure below.

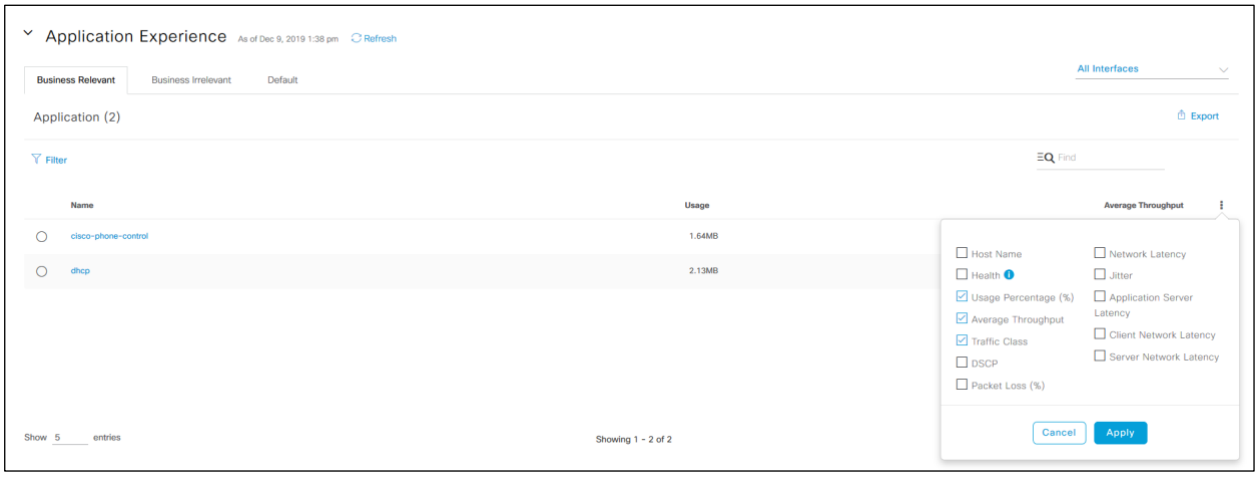
Figure 19 Device 360 – AD2-9300 Application Experience Section

For Catalyst 9000 Series switches, even though the **Device 360** section is titled **Application Experience**, the data collected is application visibility data and not application experience data – as summarized in **Table 1** earlier. Only three columns are displayed by default for Catalyst 9000 Series switches: application **Name**, **Usage**, and **Average Throughput**.

8. You can add additional columns, such as the **Traffic-class** to which the application belongs, and the **Usage Percentage (%)** for each application by clicking on the drop-down menu at the right of the screen and selecting these columns.

An example is shown in the figure below.

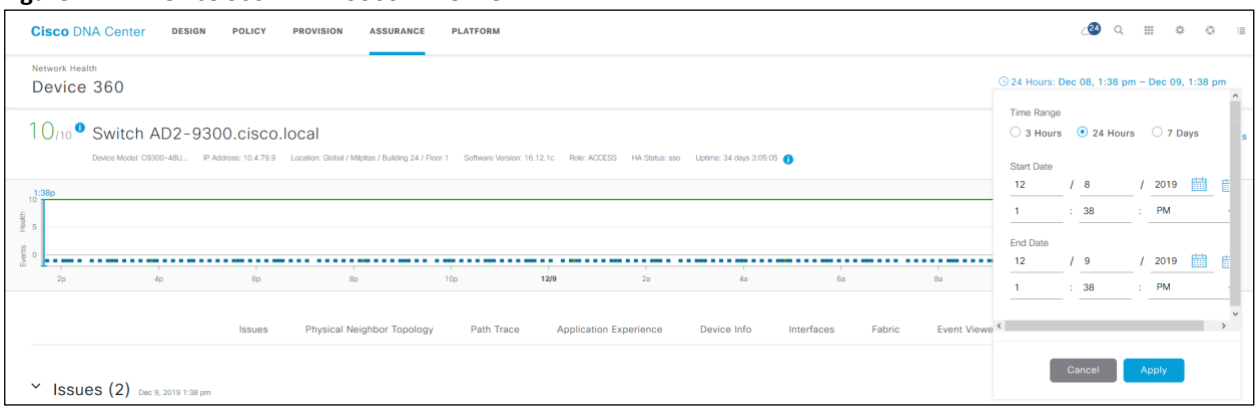
Figure 20 Device 360 – AD2-9300 Application Experience with Additional Columns



Since only application visibility data is collected on Catalyst 9000 Series switches, the remaining columns shown in the pop-up screen will not be populated if you select them. Statistics for these columns is only collected through application experience data, captured by a Cisco Easy Performance Monitor (Cisco ezPM) policy context that uses the Application Performance profile deployed on Cisco IOS XE router platforms.

The **Usage**, **Average Throughput, and Usage Percentage (%)** numbers are calculated across the overall length of the timeline displayed at the top of Device 360 screen for the Catalyst 9000 Series switch, as shown in the following figure.

Figure 21 Device 360 – AD2-9300 Timeline



By default, the timeline is set for 24 Hours.

9. You can modify the span of the timeline by clicking on it, which will bring up a pop-up window, as shown in the figure above.

Changing the timeline may change the **Usage**, **Average Throughput**, and **Usage Percentage (%)** numbers to reflect the statistics collected over the modified time span.

By default, the **Business Relevant** tab will be selected in the **Application Experience** section.

10. You can select the **Business Irrelevant** or **Default** tabs to display the applications seen by the Catalyst 9000 Series switch with those business-relevance attributes.

The information within the **Application Experience** section is not displayed per switch port. In other words, you cannot determine which applications were visible on which switch ports. However, you may be able to glean this information from additional information within the **Device 360** screen.

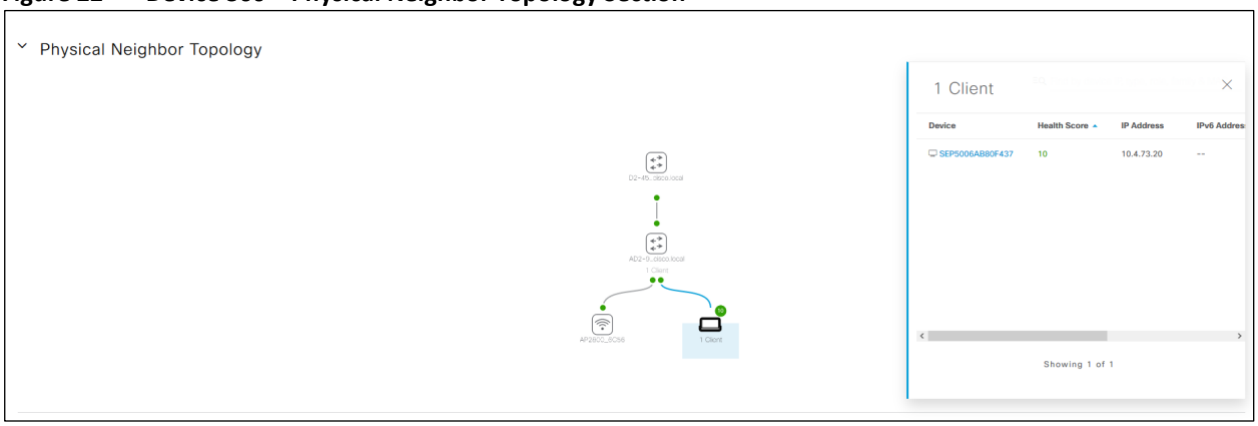
11. Scroll up and expand the **Physical Neighbor Topology** section.

This will display the devices connected to the Catalyst 9000 Series switch – both in the upstream direction (uplink ports) and the downstream direction (access-ports).

12. Click on one of the downstream clients bring up a side-panel with additional details regarding the client.

An example is shown in the figure below.

Figure 22 Device 360 – Physical Neighbor Topology Section



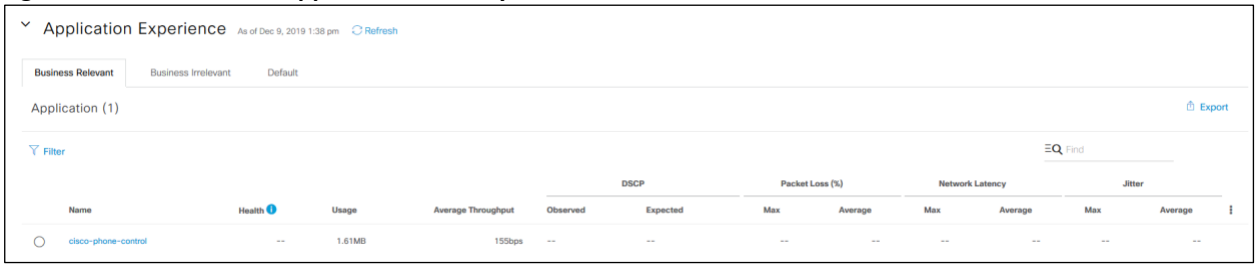
As can be seen in the figure above, the client **Device** (in this example Cisco IP Phone **SEP5006AB80F437**) is shown with an active link (highlighted in blue in the figure above). If you scroll to the end of the information listed, it will show the switch port to which the client is connected. In this example, the client is connected to **GigabitEthernet1/0/1** of the Catalyst 9000 Series switch (**AD2-9300**) – although this is not displayed in the figure above.

13. Click on the link corresponding to one of the clients within the side-panel to bring up the **Client 360** screen for that particular client.

14. Scroll down and expand the **Application Visibility** section for the client.

This will display the application statistics seen for that particular client, calculated across the overall length of the timeline displayed at the top of **Client 360** screen for that particular client. As with the **Device 360** screen, the time span of the timeline can be modified – which may change the statistics displayed in the **Application Visibility** section of the **Client 360** screen. An example of the **Application Visibility** section for the Cisco IP Phone client is shown in the figure below.

Figure 23 Client 360 – Application Visibility Section



As can be seen, the cisco-phone-control traffic, seen in the Application Experience section of the Device 360 screen in **Figure 20** above is entirely due to Cisco IP Phone **SEP5006AB80F437** connected to **GigabitEthernet1/0/1** of the Catalyst 9000 Series switch (**AD2-9300**).

Finally, note that the columns which display **DSCP** values, **Packet Loss(%)**, **Network Latency**, and **Jitter**, in the **Application Experience** section of the **Client 360** screen in the figure above are empty. Although this may seem slightly confusing at first, it is because the application statistics for this client were collected by a Catalyst 9000 Series switch, which only supports the collection of application visibility data, and not application experience data. If the traffic from this client had been seen at an observation point on a Cisco IOS XE router, then additional statistics such as **Packet Loss(%)**, **Network Latency**, and **Jitter** may be collected (depending upon whether the traffic flow was UDP, RTP, TCP, etc.), and additional information displayed.

Use Case Summary

Within this use case we have shown how Cisco DNA Application Assurance can be used to gain visibility into applications and their throughput on the LAN – as the application traffic crosses access-ports of Catalyst 9000 Series switches. This is done through the **Application Visibility** section of the **Device 360** screen for individual Catalyst 9000 Series switches. Additionally, we have demonstrated how application visibility can be extended down to individual clients connected to specific Catalyst 9000 Series switch ports, through the **Application Visibility** section of the **Client 360** screen.

Use Case #2: View Application Traffic across the WLAN

Use Case Scenario

This use case is similar in scope to **Use Case #1**. As a member of the network planning team, you wish to gain visibility into the applications and their usage across your wireless LAN (WLAN), through your AireOS wireless LAN controllers (WLCs).

Procedure: Use Cisco DNA Application Assurance to View Application Traffic on AireOS WLCs

Cisco DNA Application Assurance can be used to gain visibility into applications and their throughput – as the application traffic crosses the observation points at which Cisco DNA Application Assurance data is being collected. For this use case, the Cisco DNA Application Assurance observation points are the Access Points (APs) operating in local-mode connected to the AireOS WLC (**SS-5520**) within the campus.

The following are the steps to view application visibility data on AireOS WLCs from within Cisco DNA Center.

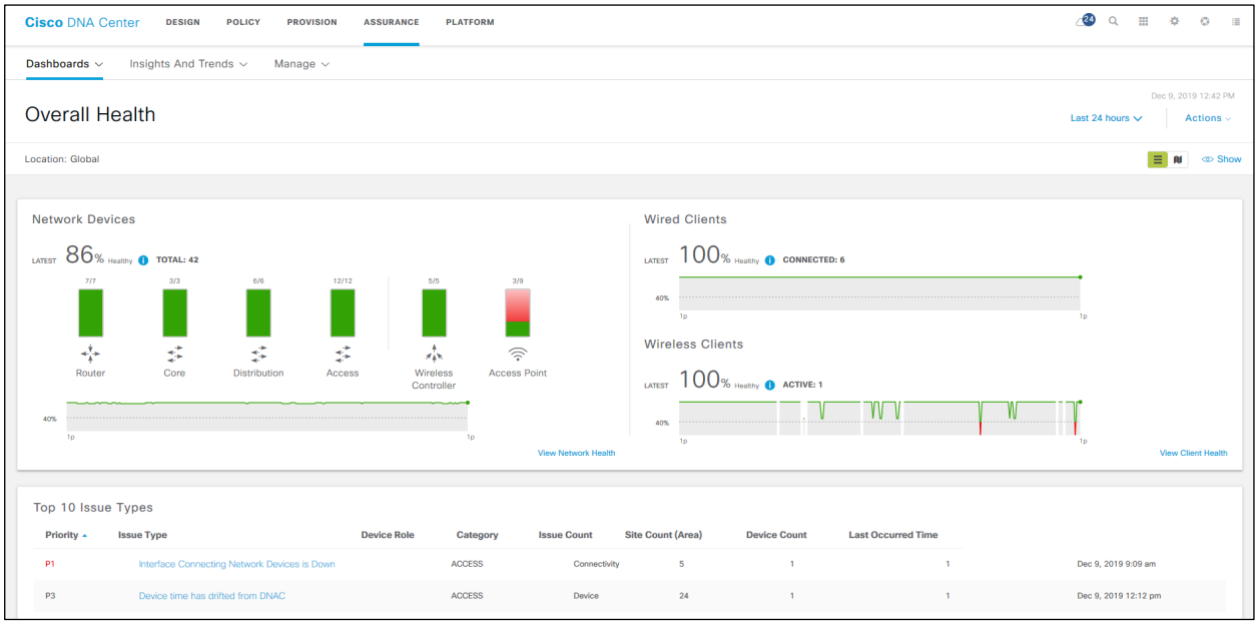
1. Login to the Cisco DNA Center web console using the IP address or fully qualified domain name of your instance.

For example: https://<Cisco_DNA_Center_IPaddr_or_FQDN>.

2. From the main Cisco DNA Center dashboard navigate to **Assurance**.

This will take you to the **Overall Health** dashboard within Cisco DNA Assurance. An example is shown in the following figure.

Figure 24 Cisco DNA Assurance Overall Health Dashboard



3. Navigate to **Dashboards → Health → Network Health**.

This will take you to the **Network Health** dashboard.

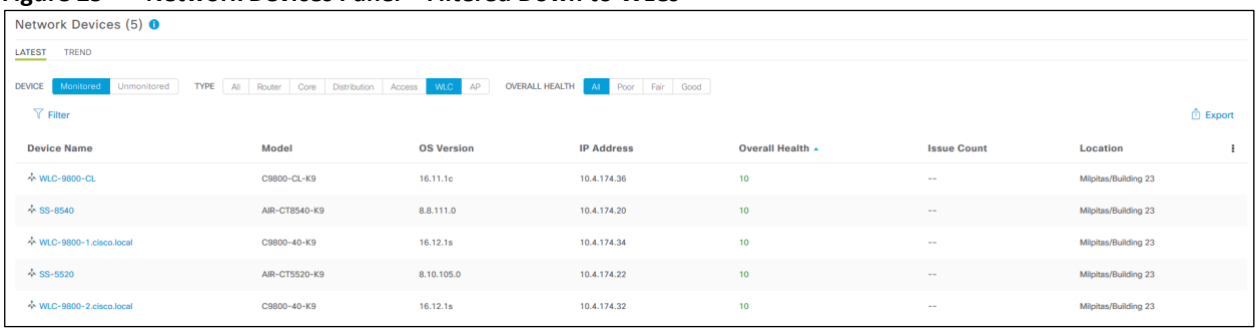
4. Scroll down to the **Network Devices** panel at the bottom of the **Network Health** dashboard.

Here you will see a list of network devices seen by Cisco DNA Application Assurance.

5. Select **DEVICE – Monitored**, **TYPE – WLC**, **OVERALL HEALTH - All**

The network devices list will be filtered down to monitored WLCs. An example is shown in the figure below.

Figure 25 Network Devices Panel – Filtered Down to WLCs



6. Locate one of the AireOS WLCs in the list of network devices and click on it.

For this deployment guide, the AireOS WLC selected is **SS-5520**. This will bring up the **Device 360** screen for the WLC.

7. Scroll down and expand the **Application Experience** section of the **Device 360** screen for the WLC.

This will display the applications seen by the APs operating in centralized (local) mode associated with the WLC. An example of the **Application Experience** data is shown in the figure below.

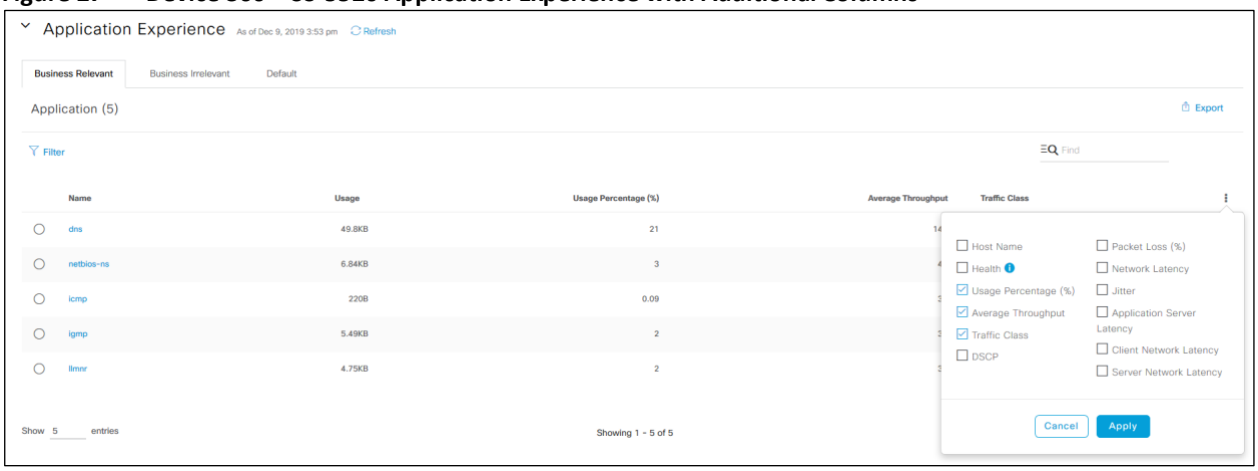
Figure 26 Device 360 – SS-5520 Application Experience Section

For AireOS WLCs, even though the **Device 360** section is titled **Application Experience**, the data collected is application visibility data and not application experience data – as summarized in **Table 1** earlier. Only three columns are displayed by default for AireOS WLCs: application **Name**, **Usage**, and **Average Throughput**.

8. You can add additional columns, such as the **Traffic-class** to which the application belongs, and the **Usage Percentage (%)** for each application by clicking on the drop-down menu at the right of the screen and selecting these columns.

An example is shown in the figure below.

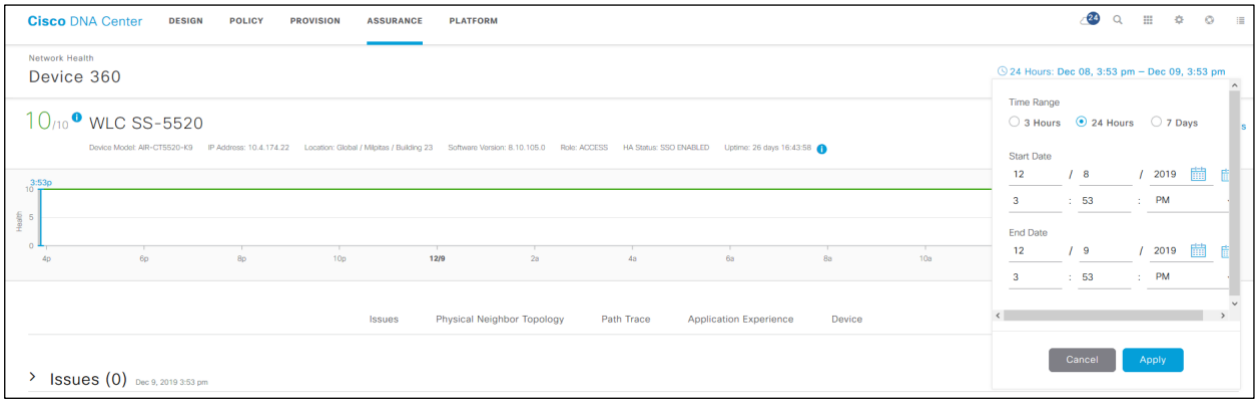
Figure 27 Device 360 – SS-5520 Application Experience with Additional Columns



Since only application visibility data is collected on AireOS WLCs, the remaining columns shown in the pop-up screen will not be populated if you select them. Statistics for these columns is only collected through application experience data, captured by a Cisco Easy Performance Monitor (Cisco ezPM) policy context that uses the Application Performance profile deployed on Cisco IOS XE router platforms.

The **Usage**, **Average Throughput, and Usage Percentage (%)** numbers are calculated across the overall length of the timeline displayed at the top of Device 360 screen for the AireOS WLC, as shown in the following figure.

Figure 28 Device 360 – SS-5520 Timeline



By default, the timeline is set for 24 Hours.

9. You can modify the span of the timeline by clicking on it, which will bring up a pop-up window, as shown in the figure above.

Changing the timeline may change the **Usage**, **Average Throughput**, and **Usage Percentage (%)** numbers to reflect the statistics collected over the modified time span.

By default, the **Business Relevant** tab will be selected in the **Application Experience** section.

10. You can select the **Business Irrelevant** or **Default** tabs to display the applications seen by the AireOS WLC with those business-relevance attributes.

The information within the **Application Experience** section is not displayed per Access Point (AP). In other words, you cannot determine which applications were seen by which AP or which SSID on which AP. However, you may be able to glean this information from additional information within the **Device 360** screen.

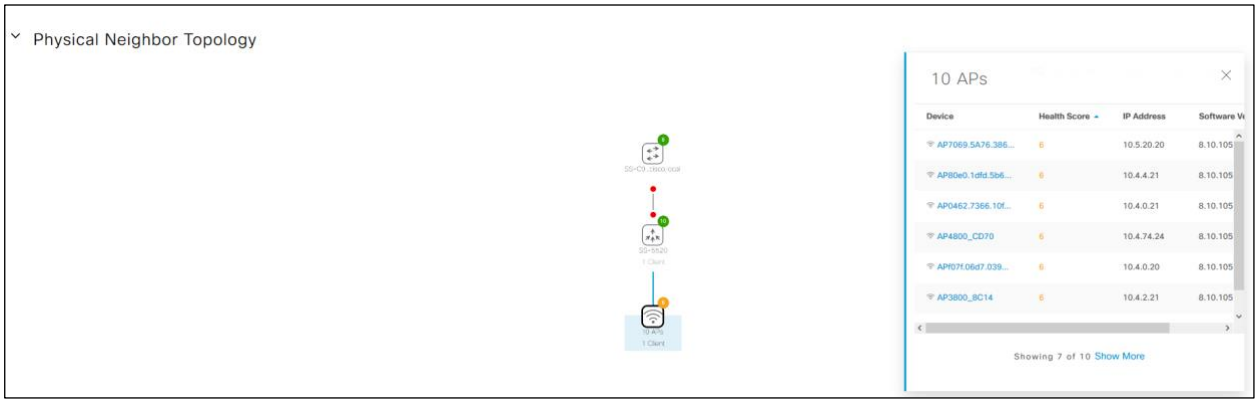
11. Scroll up and expand the **Physical Neighbor Topology** section.

This will display the devices connected to the AireOS WLC – both in the upstream direction (uplink ports) and the downstream direction (Access Points).

12. Click on the downstream APs to bring up a side-panel with additional details regarding the APs connected to the AireOS WLC.

An example is shown in the figure below.

Figure 29 Device 360 – SS-5520 Physical Neighbor Topology Section



As can be seen in the figure above, each of the APs is shown with an active link (highlighted in blue in the figure above).

13. Click on the link corresponding to one of the APs within the side-panel to bring up the **Device 360** screen for that particular AP.

For this deployment guide, the AP named **AP0462.7366.40f0** was selected.

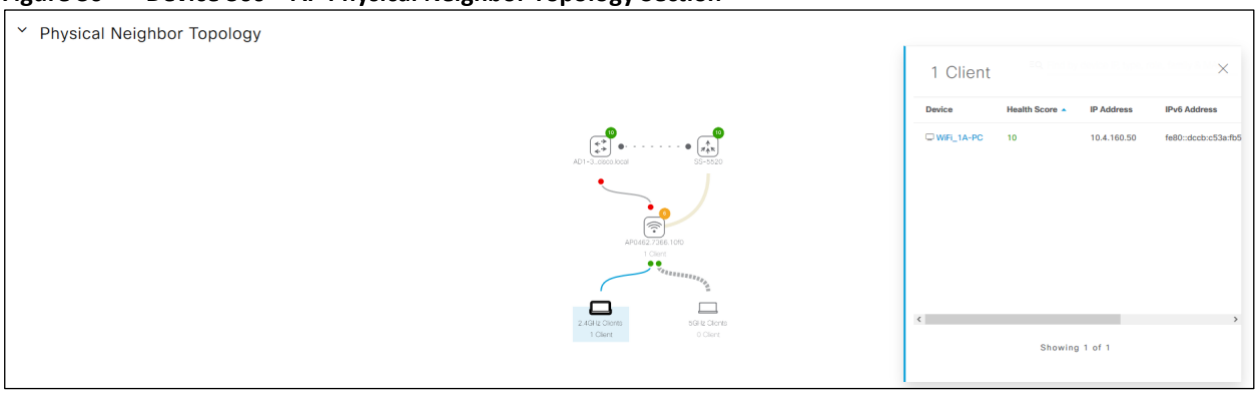
14. Scroll down and expand the **Physical Neighbor Topology** section for the AP.

This will display the devices connected to the AP – both in the upstream direction (WLC) and the downstream direction (clients). As can be seen in the figure above, there is a client connected to the 2.4 GHz radio.

15. Click on the **2.4 GHz Clients** to bring up a side-panel with additional details regarding the client.

An example is shown in the figure below.

Figure 30 Device 360 – AP Physical Neighbor Topology Section



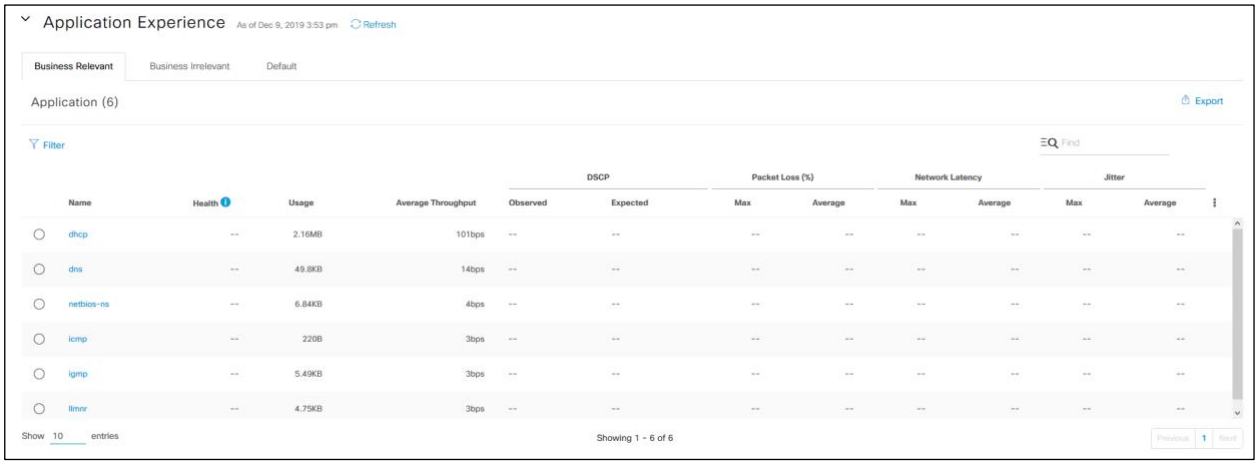
The client **Device** (in this example a PC named **WiFi_1A-PC**) is shown with an active link (highlighted in blue in the figure above). If you scroll to the end of the information listed, it will show the VLAN to which the client is connected. In this example, the client is connected to **VLAN ID 160** of the AireOS WLC (**WLC-5520**) – although this is not displayed in the figure above.

16. Click on the link corresponding to the client (**WiFi_1A-PC**) within the side-panel to bring up the **Client 360** screen for that particular client.

17. Scroll down and expand the **Application Visibility** section for the client.

This will display the application statistics seen for that particular client, calculated across the overall length of the timeline displayed at the top of **Client 360** screen for that particular client. As with the **Device 360** screen, the time span of the timeline can be modified – which may change the statistics displayed in the **Application Visibility** section of the **Client 360** screen. An example of the **Application Visibility** section for the **WiFi_1A-PC** client is shown in the figure below.

Figure 31 Client 360 – WiFi_1A-PC Application Visibility Section



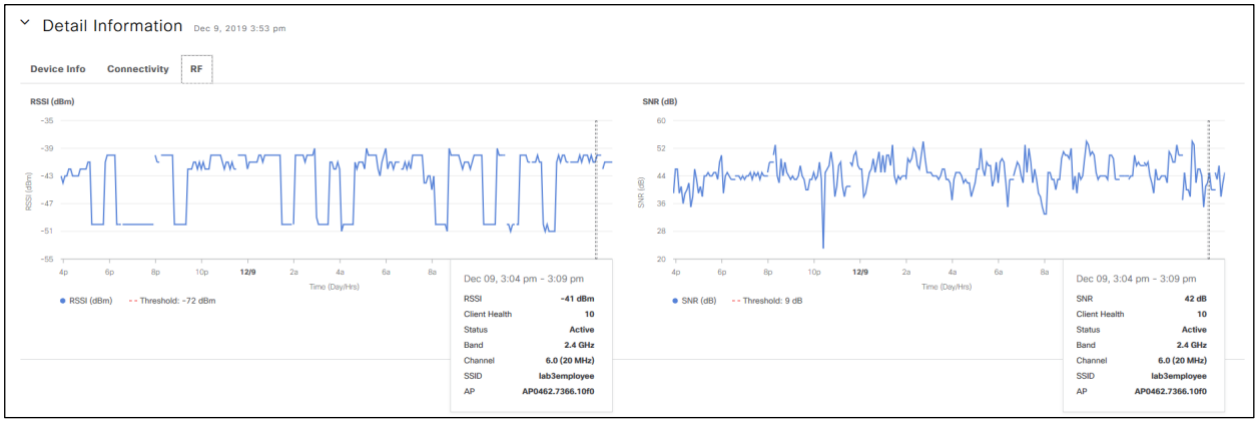
Here you can view the application traffic generated for this individual client, based upon business relevance attribute. By default the **Business Relevant** tab is selected.

Note that the columns which display **DSCP** values, **Packet Loss(%)**, **Network Latency**, and **Jitter**, in the **Application Experience** section of the **Client 360** screen in the figure above are empty. Although this may seem slightly confusing at first, it is because the application statistics for this client were collected by an AireOS WLC, which only supports the collection of application visibility data, and not application experience data. If the traffic from this client had been seen at an observation point on a Cisco IOS XE router, then additional statistics such as **Packet Loss(%)**, **Network Latency**, and **Jitter** may be collected (depending upon whether the traffic flow was UDP, RTP, TCP, etc.), and additional information displayed.

18. Scroll down and expand the **Detailed Information** section for the client, and select the **RF** tab.

This will display a historical graph of the RF connectivity of the client – across the overall length of the timeline displayed at the top of **Client 360** screen for that particular client.

Figure 32 Client 360 – Detailed Information – RF Tab



Hovering over any point in the RSSI or SNR graphs brings up additional detail regarding the client, including the AP to which the client was connected, and the WLAN / SSID to which the client was connected at that point. Provided the client has not roamed significantly between APs or changed SSIDs during the timeline displayed within the graph, this information may be used to provide a rough estimate of how much of the application usage data displayed within the **Application Experience** section of the **Client 360** screen was generated per WLAN/SSID and per AP by this client.

Use Case Summary

Within this use case we have shown how Cisco DNA Application Assurance can be used to gain visibility into applications and their throughput on the WLAN – as the application traffic crosses Access Points of AireOS WLCs operating in centralized (local) mode. This is done through the **Application Visibility** section of the **Device 360** screen for individual AireOS WLCs. Additionally, we have demonstrated how application visibility can be extended down to individual clients connected to specific APs associated with AireOS WLCs, through the **Application Visibility** section of the **Client 360** screen.

Use Case #3: Identifying and Troubleshooting an Application Performance Issue

Technical Note: This use case has been carried over as-is from the previous version of this deployment guide, which utilized Cisco DNA Center release 1.3.0. Although the use case is still valid, screen captures, and steps have not been updated to reflect any differences in Cisco DNA Center release 1.3.1.

Use Case Scenario

The following is the scenario for this use case. As a member of the application support team, you have received a trouble ticket indicating general slow response times and timeouts when regarding the SSH protocol. As is often typical of performance issues, the person who filed the trouble ticket doesn't remember the specific devices he/she was accessing. Also, since the trouble ticket was not considered high priority, the case has reached you – now three days after the issue occurred. Your goal is to troubleshoot the performance issue of the SSH protocol.

The following are the procedures which guide you through troubleshooting this issue:

- Determine if the application has degraded health.
- Determine where in the network the application health issues are occurring.
- Determine if the application health issues are network related.

Procedure: Determine if the Application has Degraded Health

Cisco DNA Application Assurance can be used to identify and troubleshoot performance issues of application traffic that crosses the observation points at which Cisco DNA Application Assurance data is being collected. For this design and deployment guide the Cisco DNA Application Assurance observation points are the GigabitEthernet0/0/0 interfaces of the Cisco ASR 1K WAN head-end routers (**WE-ASR1002X-1** and **WE-ASR1002X-2**). With this design, Cisco DNA Application Assurance can be used to identify and troubleshoot performance issues of application traffic that crosses the WAN between the campus and branch locations.

The following steps guide you determining if the application has degraded health, which could result in performance issues.

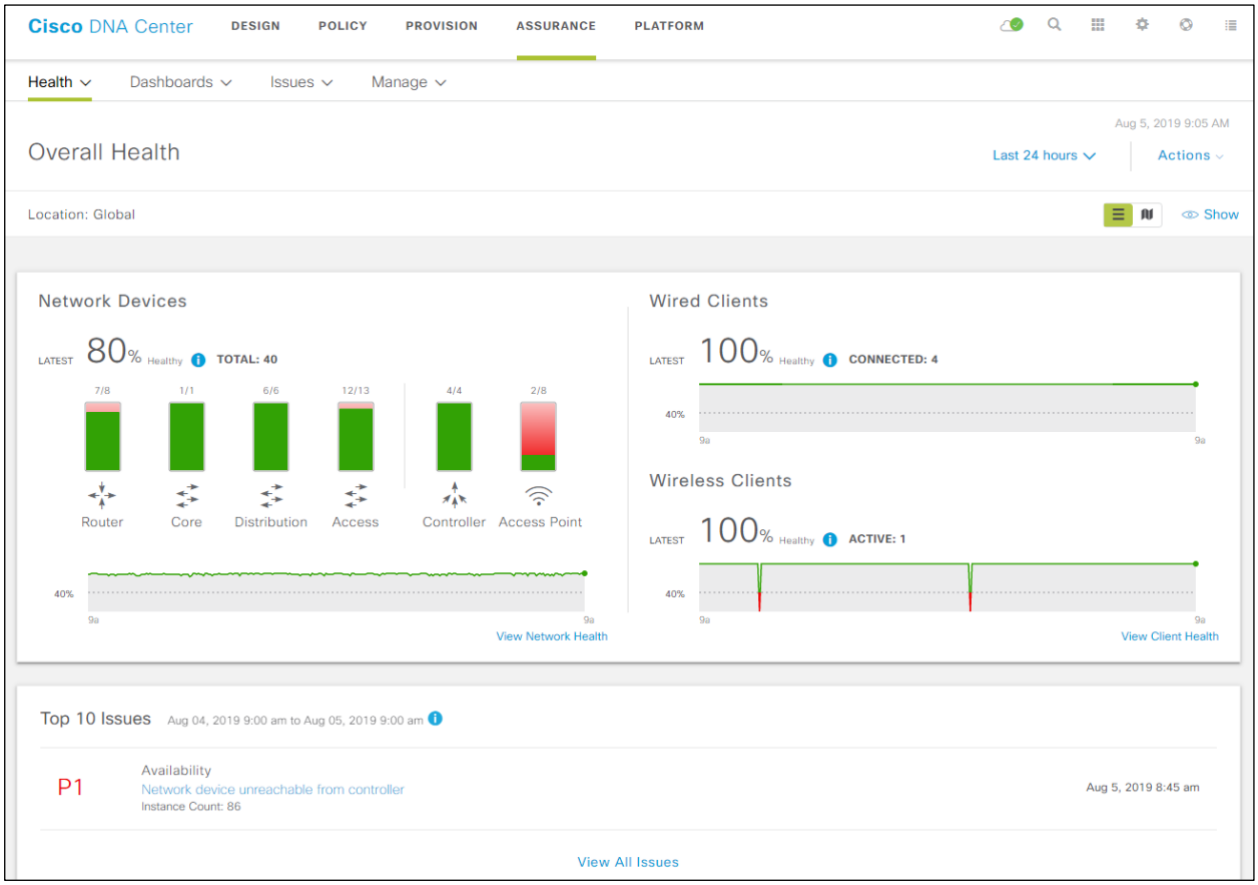
1. Login to the Cisco DNA Center web console using the IP address or fully qualified domain name of your instance.

For example: https://<Cisco_DNA_Center_IPaddr_or_FQDN>.

2. From the main Cisco DNA Center dashboard navigate to **Assurance**.

This will take you to the **Overall Health** dashboard within Cisco DNA Assurance. An example is shown in the following figure.

Figure 33 Cisco DNA Assurance Overall Health dashboard



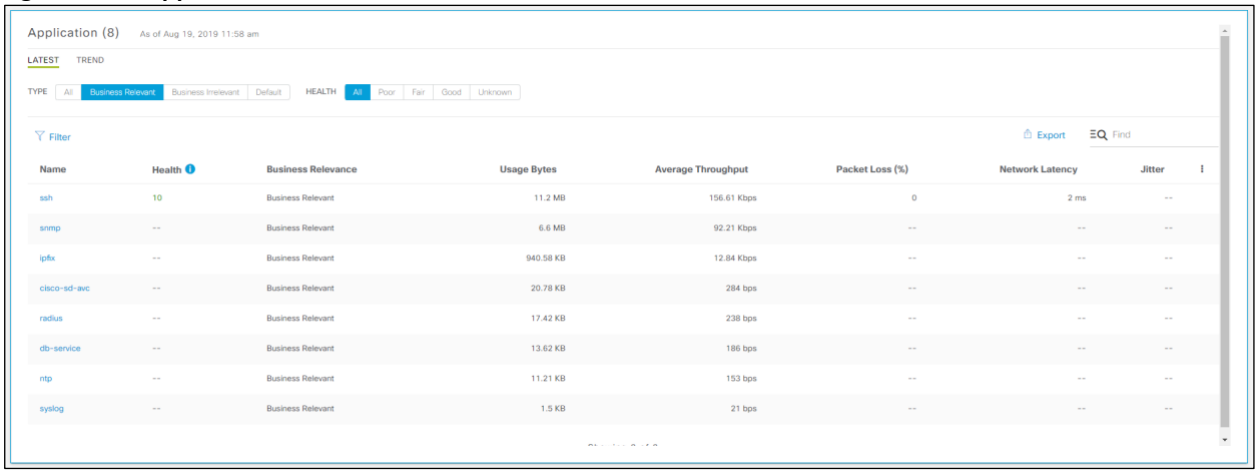
3. From the drop-down menu under **Health**, select **Application**.

This will take you to the **Application Health** dashboard.

4. Scroll down to the **Application** panel at the bottom of the **Application Health** dashboard.

Here you will see a list of applications seen by Cisco DNA Application Assurance.

Figure 34 Application Panel



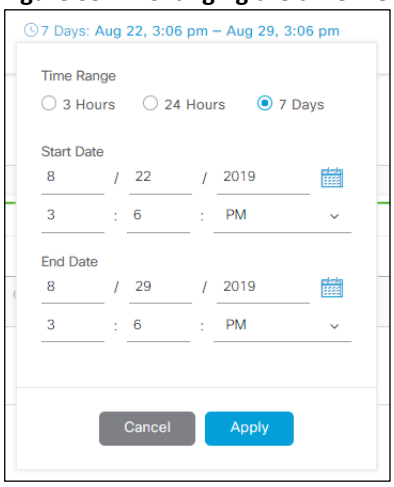
5. Locate and click on the SSH application.

This will take you to the **Application 360** dashboard for the SSH application.

6. At the top of the **Application 360** dashboard for SSH, change the timeline from 24 hours to 7 days, since the trouble ticket was filed 3 days ago.

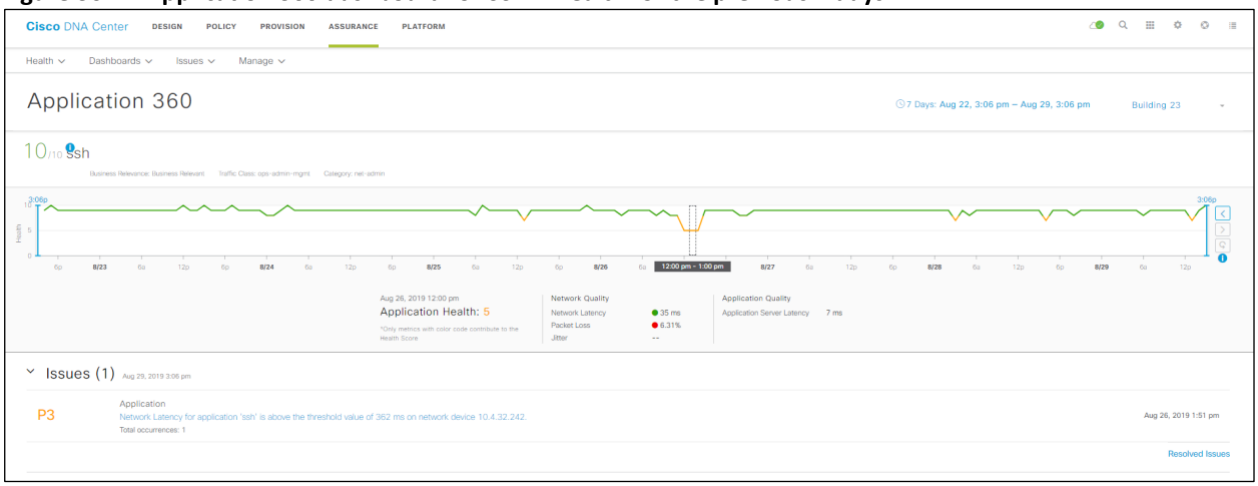
An example is shown in the figure below.

Figure 35 Changing the timeline of the top panel of the Application 360 dashboard



The timeline at the top of the **Application 360** dashboard for SSH will adjust to show the health of the application for the past 7 days. An example is shown in the following figure.

Figure 36 Application 360 dashboard for SSH – health for the previous 7 days



With an overall timeline set for 7 days, each collection interval within the timeline is 60 minutes. From this historical timeline, you can visually see that the SSH application has a noticeable period of degraded health 3 days ago (8/26), from roughly 11:00 am to 2:00 pm. This period of degraded application health appears in yellow in the graph above.

7. Hover over the area of degraded health (yellow area) in the timeline, as shown in the figure above.

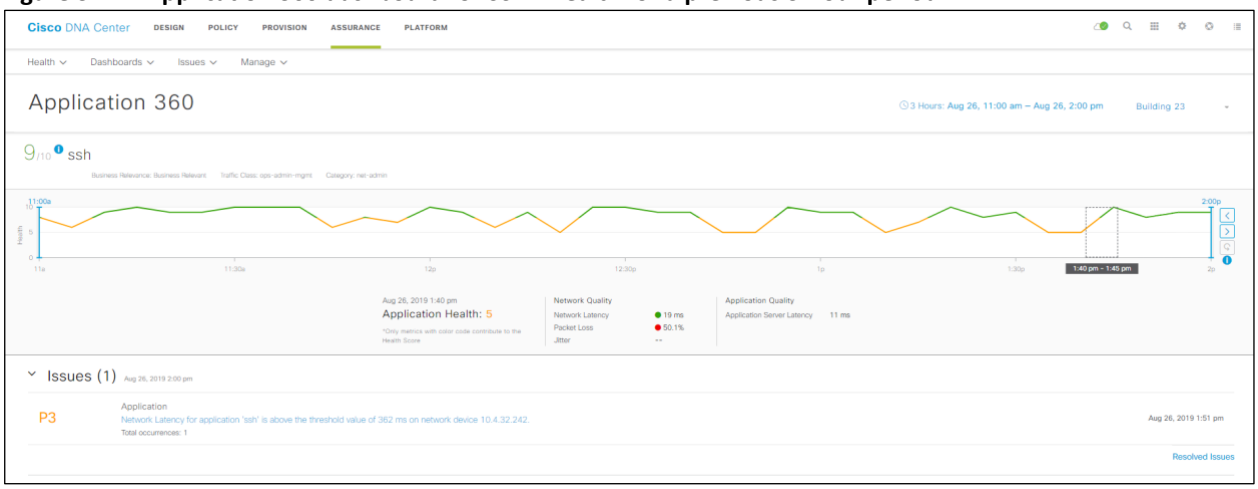
Under the timeline you will see details regarding the underlying cause of the degraded health score. As can be seen, SSH experienced 6.31% **Packet Loss** for the 60-minute collection interval shown, and a red dot – indicating a poor health score. Overall **Application Health** was given a score of 5 out of 10 – highlighted in yellow text – for that collection interval.

Now that you have identified an issue within the general time period of the trouble ticket, you can narrow the overall timeline show more granular details around the time period of the degraded health.

8. At the top of the **Application 360** dashboard for SSH, change the timeline from 7 days to 3 hours – from 11:00 am to 2:00 pm on 8/26.

The overall timeline at the top of the **Application 360** dashboard for SSH will adjust to show the health of the application for that specific 3-hour period. An example is shown in the following figure.

Figure 37 Application 360 dashboard for SSH - health for a previous 3-hour period



Since the overall timeline has been changed from 7 days to 3 hours, each collection interval has also decreased from 60 minutes to 5 minutes. Here we can see intermittent collection intervals of degraded health (areas in yellow), mixed in with collection intervals of good health (areas in green).

9. Hover over any area of degraded health (yellow area) in the timeline – as shown in the figure above.

As can be seen, SSH experienced an even higher percentage **Packet Loss** (50.1%) for the shorter 5-minute collection interval shown, and a red dot – indicating a poor health score. Overall **Application Health** was given a score of 5 out of 10 – highlighted in yellow text – for that 5-minute collection interval.

So, it appears clear that intermittent packet loss was occurring 3 days ago (8/26) for SSH traffic, from approximately slightly before 11:00 am until roughly 2:00 pm.

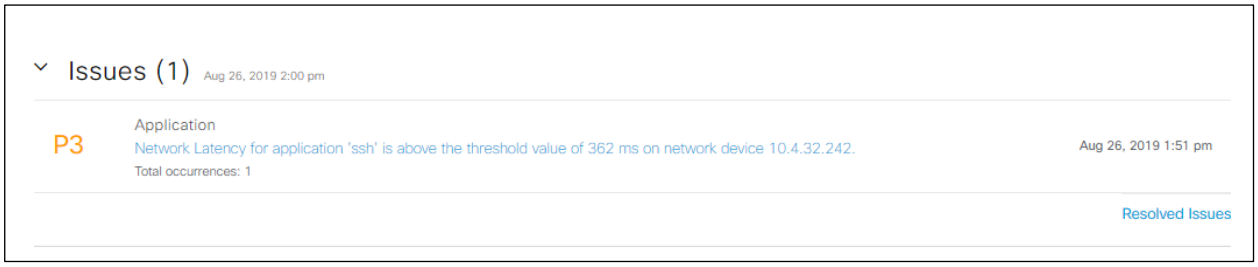
The next question you wish to answer is where was the SSH packet loss occurring?

Procedure: Determine Where in the Network the Application Health Issues are Occurring

10. Scroll down to the **Issues** panel in the **Application 360** dashboard for SSH.

An example is shown in the figure below.

Figure 38 Application 360 dashboard for SSH – Issues panel

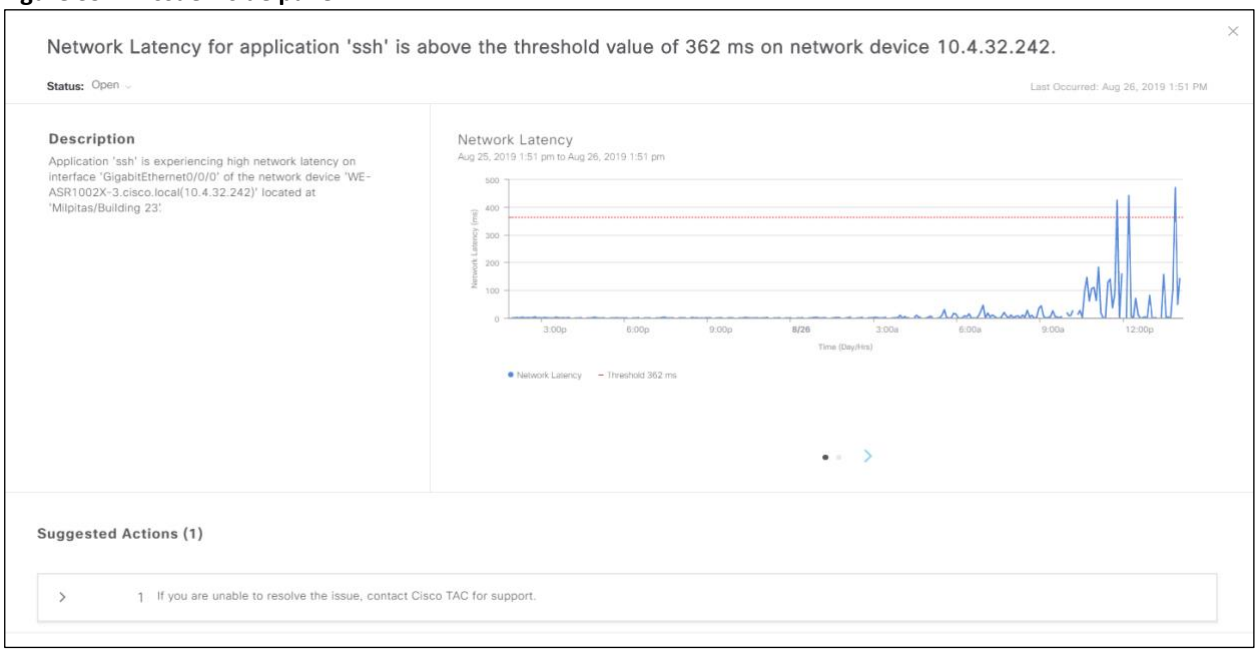


In the figure above, a single **P3** issue "**Network Latency for application 'ssh' is above the threshold value of 362 ms on network device 10.4.32.242**" is displayed.

11. Click on the description of the issue to bring up a side panel with further details of the issue.

An example is shown in the following figure.

Figure 39 Issue – side panel



The side panel provides a more detailed explanation as to why the issue was raised. Under **Description** we can see that the issue was high **Network Latency** seen on the **GigabitEthernet0/0/0** interface of WAN head-end router **WE-ASR1002X-3** at the **Milpitas/Building 23** location – which is the campus.

This narrows down the location of the health issues to the **WE-ASR1002X-3** head-end router, and/or the branches which are accessible through this router. High **Packet Loss** combined with high **Network Latency**, often point to a network issue, rather than an application issue. Therefore, the next question you may wish to answer is whether the low health scores are the result of network issues.

Procedure: Determine if the Application Health Issues are Network Related

The following steps walk you through viewing statistics provided through Cisco DNA Network Assurance, when trying to determine if an application performance issue is a result of network degradation or outages. Cisco DNA Network Assurance provides information regarding the health of network devices. The steps will walk you through viewing the health of the WAN head-end router (**WE-ASR1002X-3**), the branch router (**ISR4451**), and finally the branch switch (**C3850-1**). Cisco DNA

Network Assurance statistics are collected through a combination of SNMP queries, SNMP traps, and Syslog information. This procedure assumes telemetry with **Optimal Visibility** is enabled on the branch router (**ISR4451**) and branch switch (**C3850**).

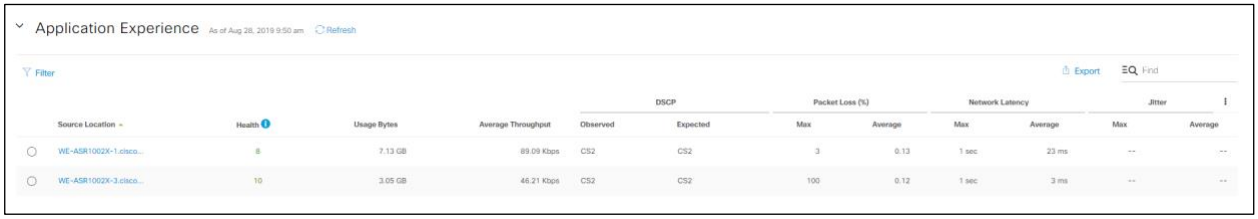
WAN head-end router (**WE-ASR1002X-3**)

1. When you are done viewing the side panel from the previous procedure, click on the **X** in the upper right corner to close the side panel and return to the **Application 360** dashboard for SSH.

2. Scroll down to the **Application Experience** panel in the **Application 360** dashboard for SSH.

An example is shown in the figure below.

Figure 40 Application 360 dashboard – Application Experience panel

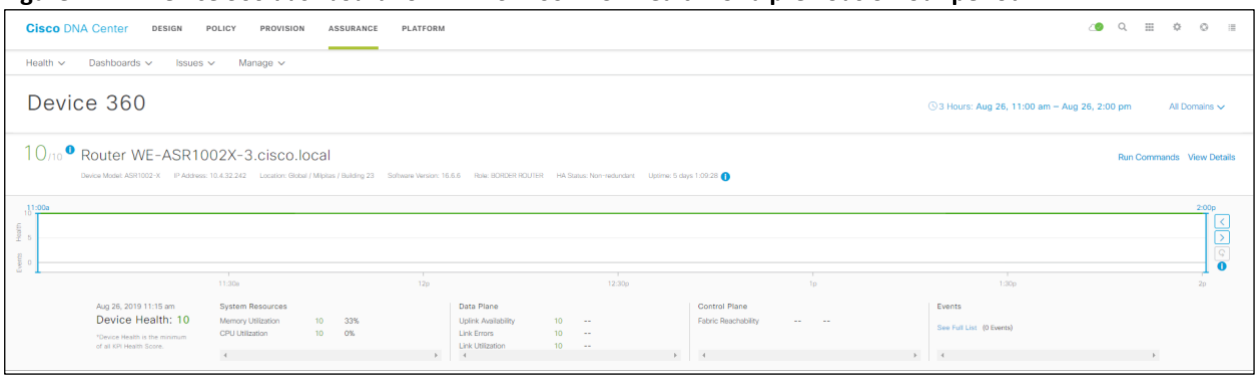


3. Click on **WE-ASR1002X-3** to go to the **Device 360** dashboard for the router.

4. At the top of the **Device 360** dashboard for **WE-ASR1002X-3**, change the timeline from 7 days to 3 hours – from 11:00 am to 2:00 pm on 8/26.

The overall timeline at the top of the **Device 360** dashboard for **WE-ASR1002X-3** will adjust to show the health of the router for that specific 3-hour period. An example is shown in the following figure.

Figure 41 Device 360 dashboard for WE-ASR1002X-3 - health for a previous 3-hour period

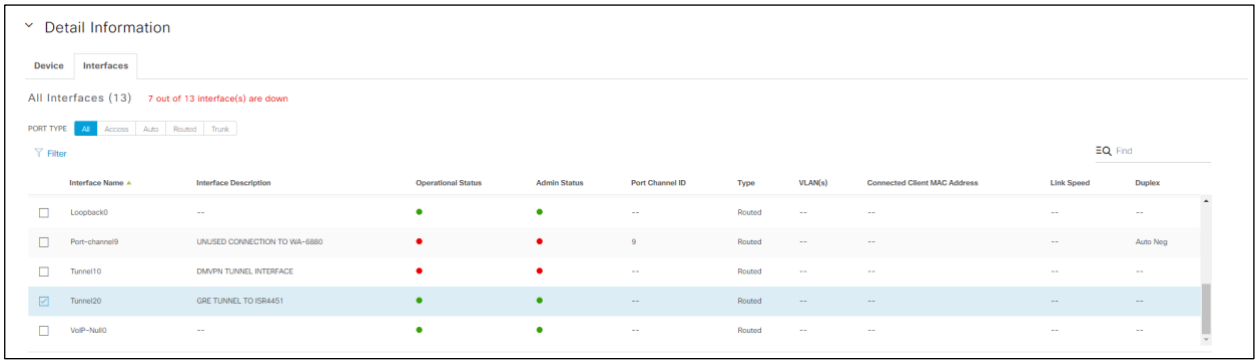


As can be seen, the health of **WE-ASR1002X-3,** appeared to have been 10/10 (good health) for the 3-hour period where SSH degradation was occurring.

5. Scroll down to the **Detail Information** panel and select the **Interfaces** tab.

Here we can see the interfaces on the router as shown in the following figure.

Figure 42 WE-ASR1002X-3 interfaces as seen from the Detail Information panel



Based on the interface description highlighted in the figure above, we can see that the router is connected to branch router **ISR4451** via an IPsec protected GRE tunnel (**Tunnel 20**).

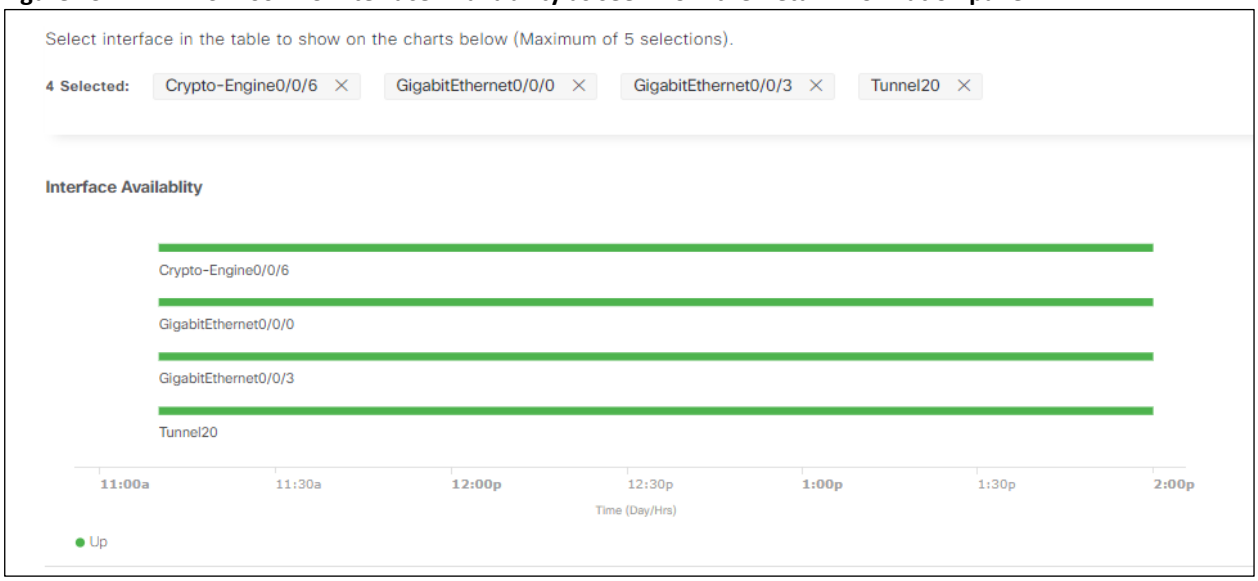
6. Select the following interfaces within the **Detail Information** panel – **Crypto-Engine0/06**, **Tunnel20**, **GigabitEthernet0/0/0**, and **GigabitEthernet0/0/3**.

These interfaces represent the crypto engine, GRE tunnel interface, the LAN-facing interface and the WAN-facing interfaces of **WE-ASR10002X-3**.

7. Scroll down to the **Interface Availability** section to view the status of these interfaces for the 3-hour period – from 11:00 am to 2:00 pm on 8/26, when the SSH degradation occurred.

An example of the **Interface Availability** section is shown below.

Figure 43 WE-ASR1002X-3 Interface Availability as seen from the Detail Information panel

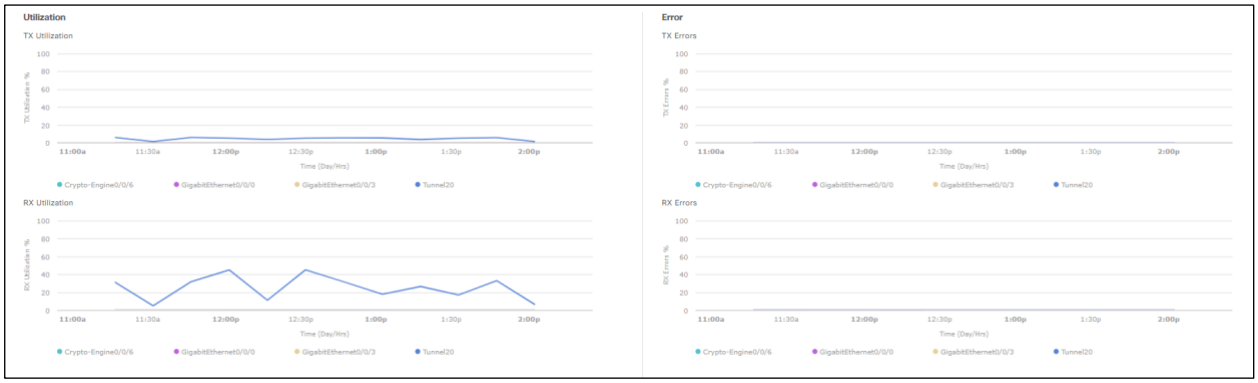


As can be seen, all four interfaces were up during the entire time.

8. Scroll down to the **Interface Utilization** and **Interface Errors** sections.

An example is shown in the following figure.

Figure 44 WE-ASR1002X-3 Interface Utilization and Interface Errors



As can be seen in the figure above, there are no interface errors reported. The receive (RX) utilization of the GRE tunnel interface (**Tunnel20**) does show utilization going up over 40% during part of the time period. This may increase latency slightly due to queuing delays during the higher utilization intervals. However, overall nothing on **WE-ASR1002X-3** appears to be the cause of the high SSH **Network Latency** and **Packet Loss**.

Since **WE-ASR1002X-3** is connected to branch router **ISR4451**, as shown in **Figure 18,** we should turn our attention to **ISR4451** next.

Branch router (**ISR4451**)

9. From the **Device 360** dashboard for **WE-ASR1002X-3** click on **Health > Network** to navigate back to the **Network Health** dashboard.

10. In the **Network Devices** panel at the bottom of the **Network Health** dashboard select the following and click the **Apply** button:

    DEVICE: **Monitored**

    TYPE: **Router**

    Overall Health: **ALL**

This will display only routers within the **Network Devices** panel. An example is shown in the figure below.

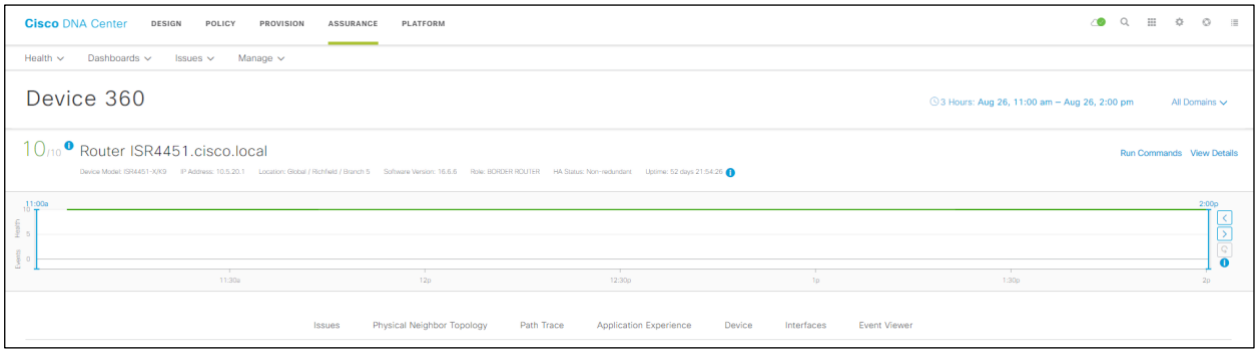
Figure 45 Network Devices panel displaying routers

11. Click on **ISR4451** to go to the **Device 360** dashboard for the router.

12. At the top of the **Device 360** dashboard for **ISR4451**, change the timeline from 7 days to 3 hours – from 11:00 am to 2:00 pm on 8/26.

The overall timeline at the top of the **Device 360** dashboard for **ISR4451** will adjust to show the health of the router for that specific 3-hour period. An example is shown in the following figure.

Figure 46 Device 360 dashboard for ISR4451 - health for a previous 3-hour period



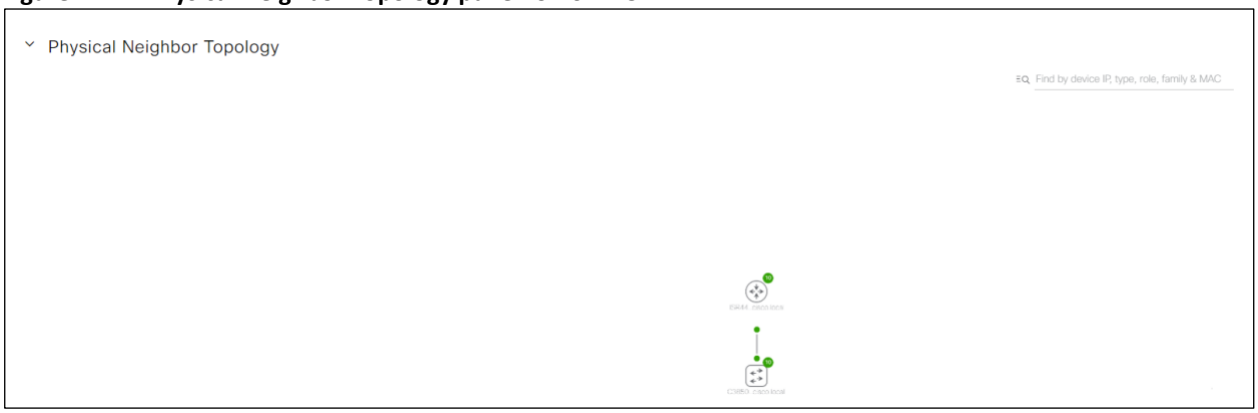
As can be seen, the health of **ISR4451,** appeared to have been a 10/10 (good health) for the 3-hour period where SSH degradation was occurring.

We can scroll through the same panels as we did for **WE-ASR1002X-3** to determine that **Interface Availability**, **Interface Utilization** and **Interface Errors** again, show no indication of anything which would cause degraded performance of SSH traffic as it passed through this router. The figures have not been included here simply for brevity.

13. Scroll to the **Physical Neighbor Topology** panel.

In the **Physical Neighbor Topology** panel, we can see that branch router **ISR4451** is connected to branch switch **C3850**, as shown in the following figure.

Figure 47 Physical Neighbor Topology panel for ISR4451



Therefore, we should turn our attention to **C3850** next.

Branch switch (**C3850**)

14. From the **Device 360** dashboard for **ISR4451** click on **Health > Network** to navigate back to the **Network Health** dashboard.

15. In the **Network Devices** panel at the bottom of the **Network Health** dashboard select the following and click the **Apply** button:

    DEVICE: **Monitored**

    TYPE: **Access**

    Overall Health: **ALL**

This will display only switches with the Cisco DNA Center role of **Access** within the **Network Devices** panel. An example is shown in the figure below.

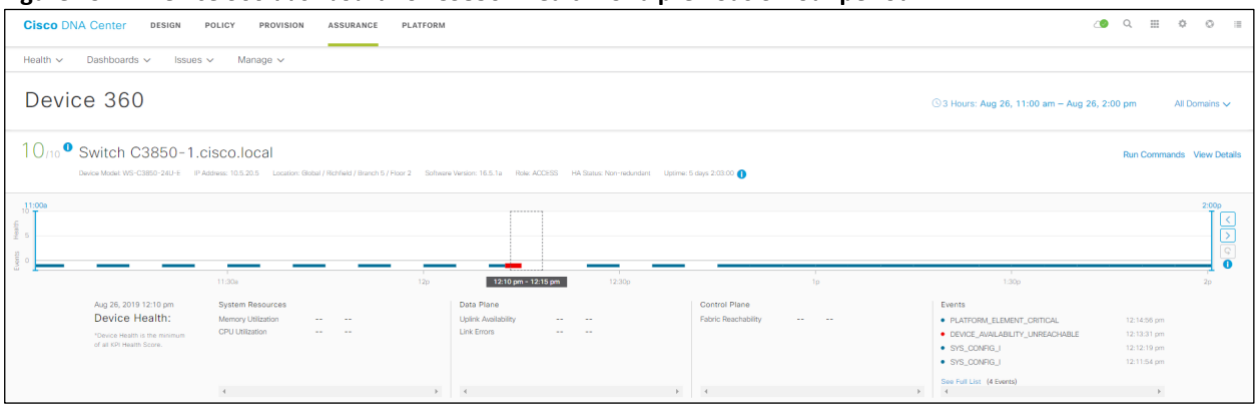
Figure 48 Network Devices panel displaying access switches

16. Click on **C3850** to go to the **Device 360** dashboard for the access switch.

17. At the top of the **Device 360** dashboard for **C3850**, change the timeline from 7 days to 3 hours – from 11:00 am to 2:00 pm on 8/26.

The overall timeline at the top of the **Device 360** dashboard for **C3850** will adjust to show the health of the access switch for that specific 3-hour period. An example is shown in the following figure.

Figure 49 Device 360 dashboard for C3850 - health for a previous 3-hour period



As can be seen, there were several issues with branch access switch **C3850** during this 3-hour time period, including one instance of the device being unreachable at approximately 12:13 PM.

Technical Note: **System Resources** statistics of **Memory Utilization** and **CPU Utilization** were not collected for collection interval highlighted in Figure 25. Any statistics that are not collected within a collection interval do not contribute to the health score of the device for that collection interval. Therefore, the health score appears as 10/10 (good health) in green text, although the device clearly has health issues.

---

18. Scroll down to the **Issues** panel in the **Device 360** dashboard for access switch **C3850**.

An example is shown in the figure below.

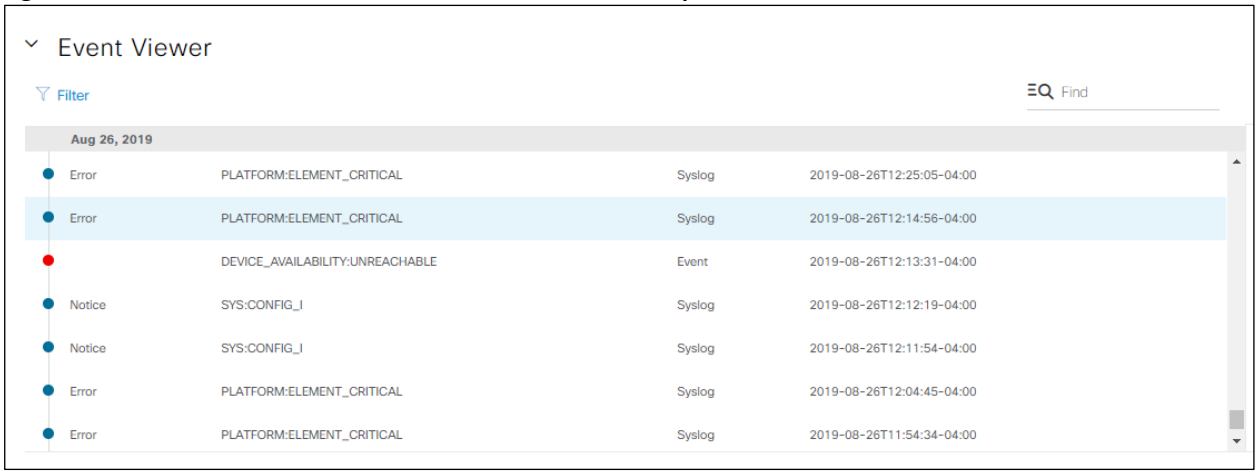
Figure 50 Device 360 dashboard for C3850 – Issues panel

In the figure above, a single **P1** issue "**Network Device 10.5.20.5 is Unreachable From Controller**" is displayed. Underneath the description, we can see that the issue has occurred 3 times during the 3-hour time period from 11:00 am to 2:00 pm on 8/26.

19. Scroll down to the **Event Viewer** panel in the **Device 360** dashboard for access switch **C3850**.

An example is shown in the figure below.

Figure 51 Device 360 dashboard for C3850 – Event Viewer panel

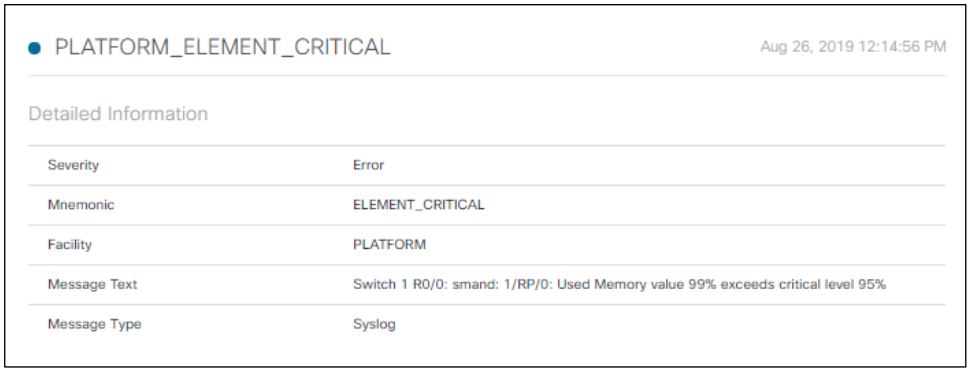


Within the **Event Viewer** panel, we can see multiple **Syslog** events with a severity level of 3 (**Error**) received from **C3850** by Cisco DNA Center, through Cisco DNA Network Assurance.

20. Click on one of the events titled **PLATFORM_ELEMENT_CRITICAL** to bring up a more detailed description of the Syslog message.

An example is shown in the figure below.

Figure 52 Device 360 dashboard for C3850 – detailed event description



In the panel to the right, within the **Message Text**, you can see that the syslog message was generated as a result of memory exceeding a threshold of 95% utilization. The actual memory utilization was 99%.

This helps explain why the **System Resources** statistics of **Memory Utilization** and **CPU Utilization** may not have been collected. These values are based on SNMP queries (SNMP GET commands) sent by Cisco DNA Center to the network device. If memory exceeded 99%, the switch may not have been able to respond to SNMP queries. This also highlights one of the benefits of the multiple telemetry sources implemented by Cisco DNA Network Assurance (SNMP GET commands, SNMP traps, Syslog, etc.). In this case, Syslog messages collected by Cisco DNA Center are still able to help us identify a problem with the network device.

Use Case Summary

Based upon the information provided by Cisco DNA Application Assurance, we can conclude that there were SSH application performance issues, consisting of high **Network Delay** and high **Packet Loss** between 11:00 AM and 2:00 PM on 8/26, visible on WAN head-end router **WE-ASR1002X-3**.

From the information provided by Cisco DNA Network Assurance, we can conclude that the WAN head-end router **WE-ASR1002X-3** and the branch router **ISR4451**, appeared healthy during this time period. However, branch access switch **C3850** appears to have been having issues with high memory utilization during this time.

Therefore, we can conclude that the SSH application performance issues were network related. We should further alert network operations to monitor branch access switch **C3850** to determine if the high memory utilization occurs again, and if so, determine what remediation actions need to be taken.

Appendix A—New in this guide

This guide has been updated to reflect new functionality added to Cisco DNA Center release 1.3.1. Specifically, application visibility has been added to Catalyst 9000 Series switches and Cisco AireOS WLCs. The overall network design of the deployment guide has been extended to include the collection of application statistics within the LAN (via Catalyst 9000 Series switches), within the WLAN (via Cisco AireOS WLCs), and across the WAN (via IOS XE routers). The prior use case of validating QoS markings as traffic crosses the WAN was removed. Two new use-cases reflecting the collection of application visibility data on Catalyst 9000 Series switches, and AireOS WLCs have been added. The final use case (**Use Case #3**) has not been modified from the prior version of this deployment guide, in order to reflect minor differences in screen captures and steps – although it still represents a valid use case for Cisco DNA Center release 1.3.1.

Appendix B—Hardware and software used for validation

This design & deployment guide was created using the following hardware and software.

Table 3 Hardware and software

Functional area	Product	Software version
Enterprise SDN Controller	Cisco DNA Center	1.3.1.3
WAN Head-End Routers	Cisco ASR1002-X Routers	IOS-XE 16.6.6
Branch Router	Cisco ISR 4451-X Router	IOS-XE 16.6.6
Branch Access Switch	Cisco Catalyst 3850 Series Switch	IOS-XE 16.5.1a
Campus Access-Layer Switch	Cisco Catalyst 9200 Series Switches	IOS-XE 16.12.1
Campus Access-Layer Switch	Cisco Catalyst 9300 Series Switches	IOS-XE 16.12.1c
Campus Access-Layer Switch	Cisco Catalyst 9400 Series Switches	IOS-XE 16.12.1c
Campus WLC	Cisco AireOS 5520 WLC HA Pair	AireOS 8.10.105

Appendix C – Viewing Cisco DNA Application Assurance Data

Cisco DNA Application Assurance data can be visualized in the following ways:

- Within the **Application Health** dashboard within Cisco DNA Center. The application information provided within the **Application Health** dashboard is not client-specific. It displays aggregate application statistics across specific sites.
- Within the **Application 360** dashboard for a specific application. The application information provided within the **Application 360** dashboard is again not client-specific. It displays application statistics for the selected application across specific sites, and across network devices.
- Within the **Device 360** dashboard for a specific network device. The application information provided within the **Device 360** dashboard is again not client-specific. It displays application statistics for the selected application across a specific network device.
- Within the **Client 360** dashboard for a specific wired or wireless client. The application information provided within the **Client 360** dashboard is client-specific – meaning the statistics are the result of traffic to or from the specific client.

This Appendix will walk you through viewing Cisco DNA Application Assurance data in all four areas.

Procedure: Viewing Application Information within the Application Health Dashboard

The following are steps to view Cisco DNA Application Assurance data collected by Cisco DNA Center through the **Application Health** dashboard.

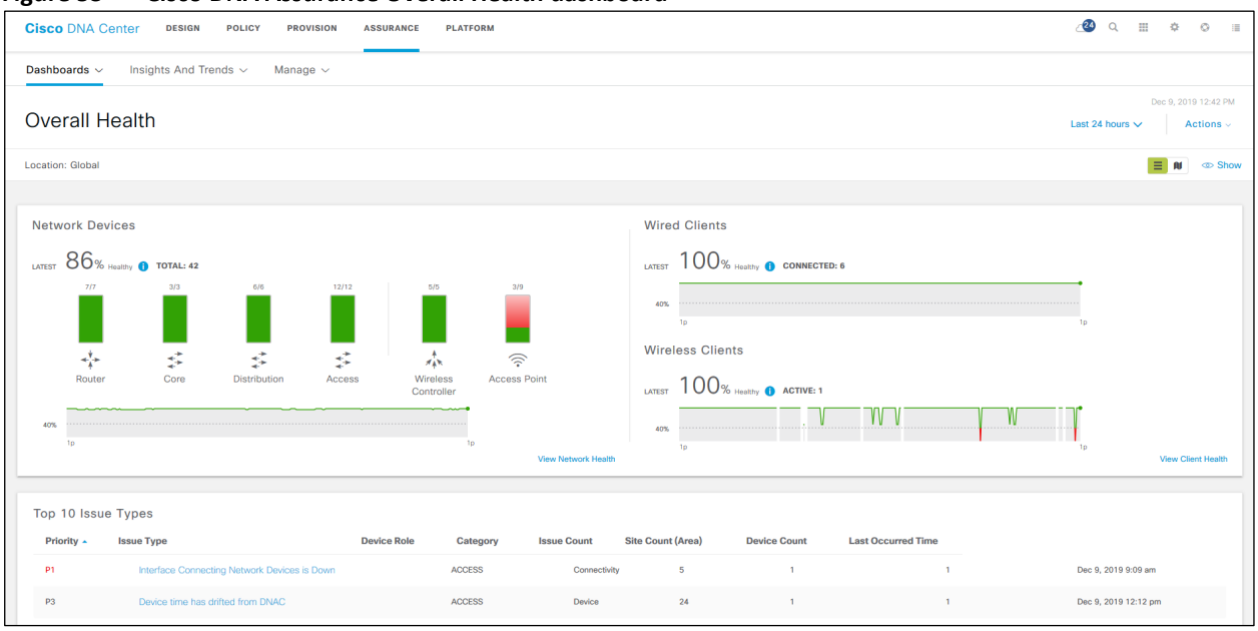
1. Login to the Cisco DNA Center web console using the IP address or fully qualified domain name of your instance.

For example: https://<Cisco_DNA_Center_IPaddr_or_FQDN>.

2. From the main Cisco DNA Center dashboard navigate to **Assurance**.

This will take you to the **Overall Health** dashboard within Cisco DNA Assurance. An example is shown in the following figure.

Figure 53 Cisco DNA Assurance Overall Health dashboard



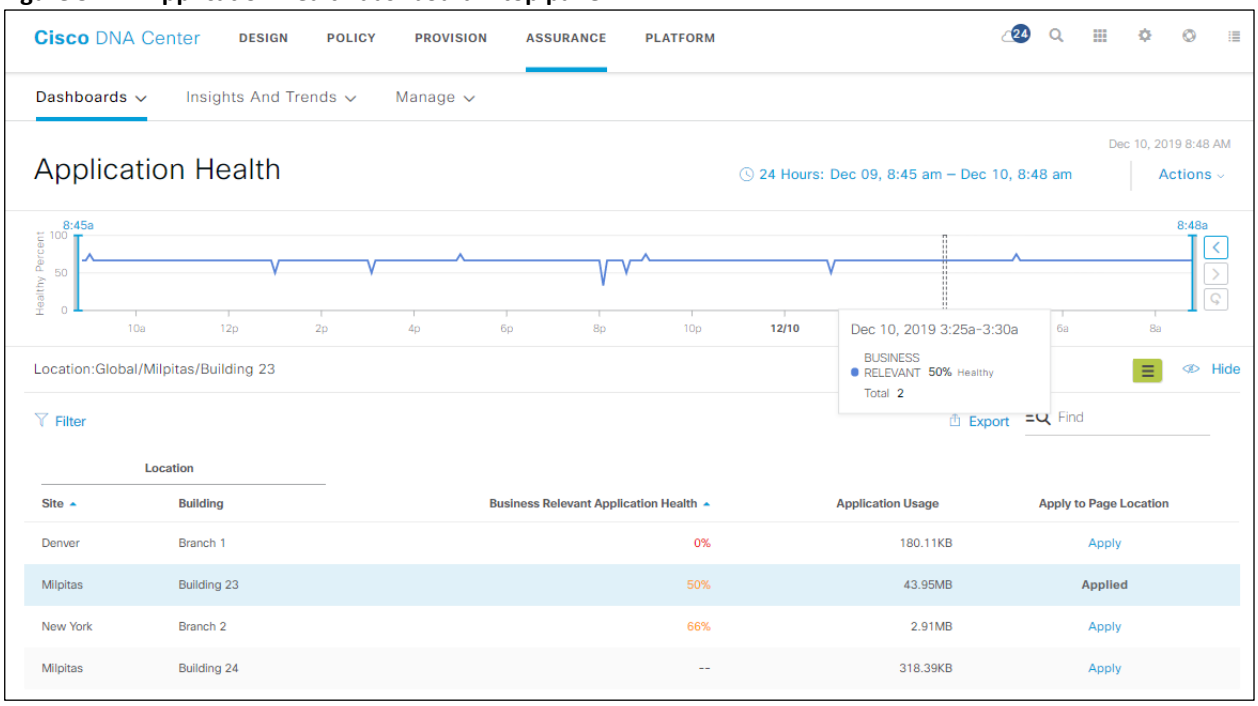
3. Navigate to **Dashboards → Health → Application Health**.

This will take you to the **Application Health** dashboard. The **Application Health** dashboard has several panels and side-panels, each presenting slightly different information regarding application health.

Application Health Dashboard – Top Panel

The top panel displays a historical timeline of the health of **Business Relevant** applications for the location specified, over the timeframe specified within the timeline. An example is shown in the figure below.

Figure 54 Application Health dashboard – top panel



4. Hover your cursor above any point on the timeline.

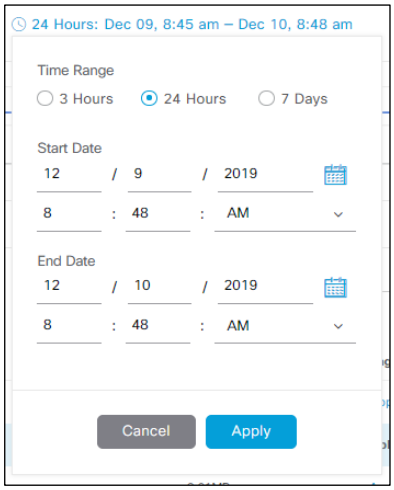
A pop-up window (see **Figure 54** above) will display the percentage of **Business Relevant** applications with a healthy score within each of the three categories discussed above. Healthy applications are those with a health score of 8 – 10 out of 10.

5. Click on the green icon with the three bars underneath the timeline.

This will allow you to choose the location within the DNA Center site hierarchy (site, and building) where the application data is collected and displayed.

The time period covered by the timeline can be changed by clicking on the link directly above the timeline. An example is shown in the figure below.

Figure 55 Changing the Timeline of the Top Panel of the Application Health Dashboard

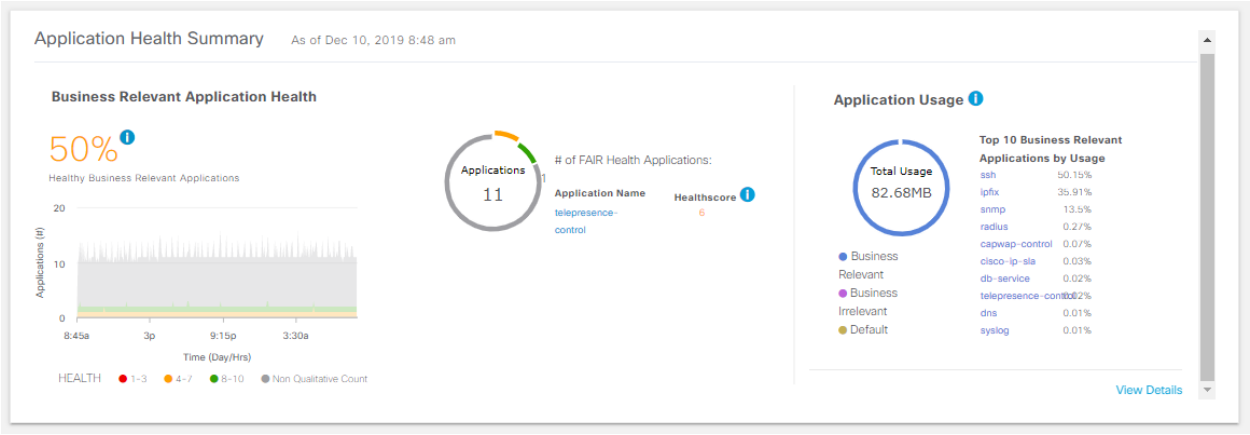


Changing the time period covered by the timeline will change the information displayed within the entire **Application Health** dashboard to reflect the new time period. For example, aggregate application usage statistics may change depending upon the timeframe over which the usage statistics are collected.

Application Health Summary Panel

The **Application Health Summary** panel is the second panel within the **Application Health** dashboard. An example is shown in the figure below.

Figure 56 Application Health Summary Panel



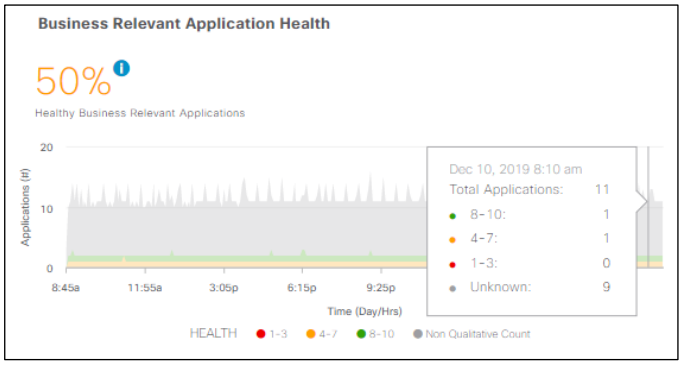
The **Application Health Summary** panel has two sections.

The section on the left displays a timeline of the aggregate health of all **Business Relevant** applications for the location specified in the panel above. The time period of the timeline is controlled through the setting within the top panel, as shown in **Figure 56** above.

6. Hover over any section of the timeline.

This will bring up a pop-up window showing details of the health scores of all **Business Relevant** applications seen for the location during that collection interval. An example is shown in the following figure.

Figure 57 Application Health Summary Timeline



As can be seen from the figure above, health scores are separated into one of four color-coded categories:

- A green dot indicates a good or healthy score with a value in the range of 8 – 10 out of a maximum score of 10.
- An orange dot indicates a fair health score with a value in the range of 4 – 7 out of a maximum score of 10.
- A red dot indicates a poor health score with a value in the range of 1 – 3 out of a maximum score of 10.
- A grey dot indicates an unknown health score – meaning that the heath score cannot be calculated for the application.

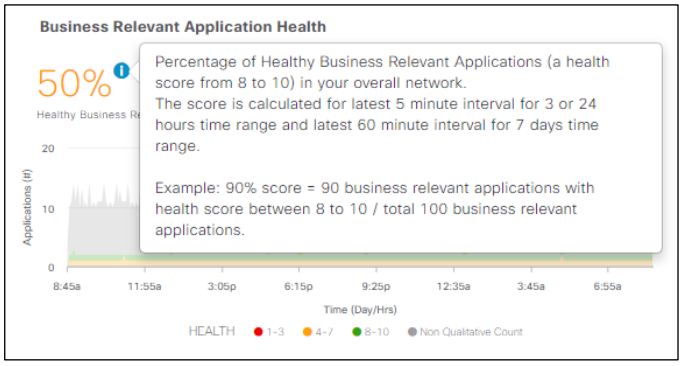
Application health scores are calculated for TCP and RTP-based applications as of Cisco DNA Center release 1.3.1. Health scores are not calculated for UDP-based applications. Further, health scores are only calculated if the application traffic is seen by an observation point which is collecting application experience statistics. Health scores are based on packet loss, latency, and jitter statistics which are captured by Cisco Performance Monitor (Cisco ezPM) running on Cisco IOS XE routers. Catalyst 9000 Series switches and Cisco AireOS WLCs only capture application visibility statistics which do not include packet loss, latency, and jitter. Therefore, application traffic seen only by an observation point which is collecting application visibility statistics will not have health scores.

In the figure above, two of the **Business Relevant** applications seen in the **Milpitas/Building 23** location for the collection interval shown in the pop-up window, have a health score calculated. The health score of one application is shown as being a green dot with a score of 8 – 10. The health score of the other application is shown as being an orange dot with a score of 4 – 7. There were 9 additional **Business Relevant** applications seen at the location during this collection interval. However, the health scores of these applications is marked as **Unknown**. This is because the other 9 applications are UDP-based applications.

7. Hover over the blue information **'i'** link next to the overall health score shown in the figure above.

This will display a pop-up information window, explaining how the aggregate health score is calculated. An example is shown in the following figure.

Figure 58 Application Health Summary – Aggregate Health Score Information



As can be seen from the figure above, the aggregate health score represents the percentage of all healthy **Business Relevant** applications seen over the latest collection interval. That time interval is 5 minutes when the timeline is set for either 3 hours or 24 hours. If the timeline is set for 7 days, the collection interval is the last 60 minutes. Again, this is an example of how the output changes, depending upon the overall timeline selected in the top panel of the **Application Health** dashboard.

In the figure above, only two **Business Relevant** applications have a health score. One of the two applications has a healthy score (green with a score from 8 – 10), while the other has a fair score (orange with a score from 4 – 7). Therefore the percentage of **Business Relevant** applications with a healthy score is one of two applications, or 50%.

The circular graph in the center of the **Application Health Summary** panel provides a color-coded visual percentage breakout of the health of **Business Relevant** applications for the location specified in the top panel.

8. Click on and hover over one of the color-coded sections of the circular graph (see **Figure 59**) in the center of the **Application Health Summary** panel.

A pop-up window will appear, showing the percentage of **Business Relevant** applications which have the health score based upon the health category chosen (green = good / healthy, orange = fair, red = poor, or grey = unknown). An example is shown in the following figure.

Figure 59 Application Health Summary – Percentage Breakout by Application Health

There are a total of 11 **Business Relevant** applications seen at the **Milpitas/Building 23** location within the current time interval. One application has a health core of **GOOD** representing 9.09% (1/11th) of all **Business Relevant** applications.

Adjacent to the circular graph, is a list of the application names which contributed to the percentage of applications seen within the chosen health category. In the figure above, since the green **GOOD** section was chosen, a single application, **SSH**, is listed with a health score of **10**, show in green text. This provides you with a quick visual display of what applications are healthy and which applications may be having performance issues at the specified location.

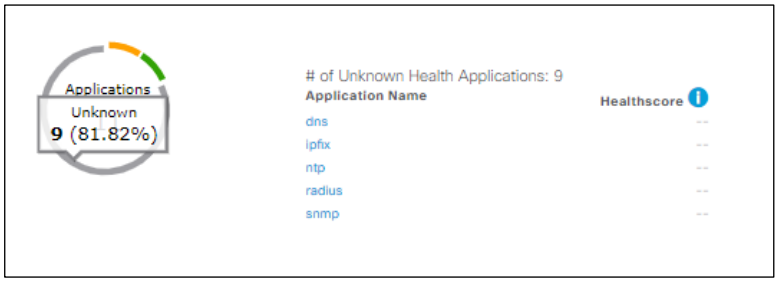
9. Hover over the blue information **'i'** link above the health score shown in the figure above.

This will display a pop-up information window, explaining which applications are listed in the table. Only the five applications with the lowest heath score for that health category are listed.

10. Click on and hover over the grey section of the circular graph – representing **Business Relevant** applications with unknown health scores.

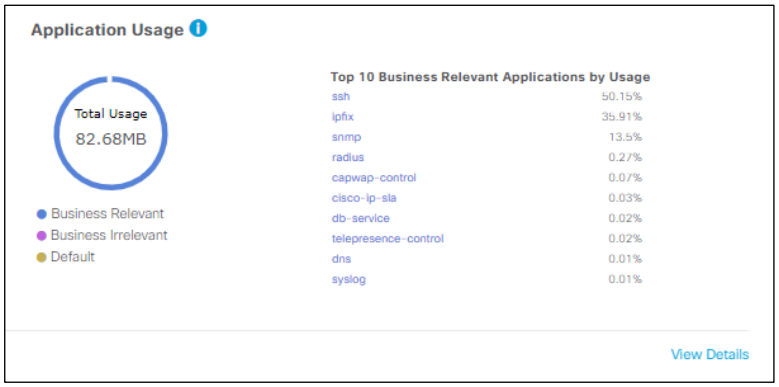
The remaining 9 business relevant applications are shown to have a health score of **Unknown** representing 81.82% (9/11th) of all **Business Relevant** applications. Only 5 applications will be listed in the table to the right of the circular graph. Note that no health scores will be listed for these applications. An example is shown in the following figure.

Figure 60 Application Health Summary – Applications with Unknown Health Scores



The section on the right-side of the **Application Health Summary** panel shows application usage – displayed as percentages – over the latest collection interval, again for the location specified in the top panel. An example is shown in the figure below.

Figure 61 Application Percentage



11. Hover over the blue information **'i'** link next to **Application Usage** in the figure above.

A pop-up window will appear indicating the time interval is again 5 minutes when the overall timeline is set for either 3 hours or 24 hours. If the overall timeline is set for 7 days, the collection interval is the last 60 minutes.

The center of the circular graph displays the overall amount of traffic seen across all observation points which Cisco DNA Application Assurance data is being collected, again for the location specified within the top panel. The circular graph under **Application Usage** in the figure above displays the percentage of overall traffic for the location, based upon the business relevance setting of the application traffic – **Business Relevant**, **Business Irrelevant**, or **Default**. The categories are color-coded in the circular graph.

If none of the business relevance categories is selected, the **Top 10 Applications by Usage** table displays the top ten applications across all business relevance categories – in terms of percentages.

12. Click on and hover over the **Business Relevant** section of the circular graph under **Application Usage**.

A pop-up window will appear showing the percentage of all traffic seen that is **Business Relevant**, and the total amount of **Business Relevant** traffic seen across all observation points for the location specified and the current collection time interval.

Figure 62 Business Relevant Application Percentage

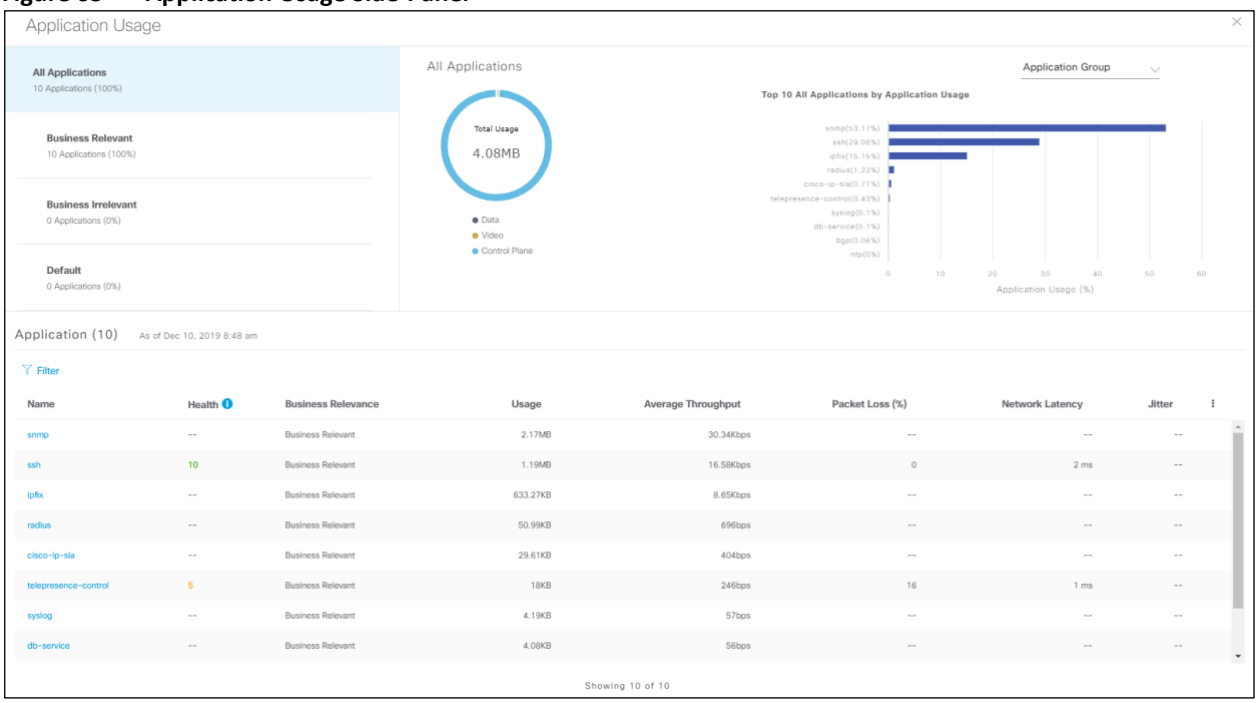
The table to the right of the circular graph will also change to list the **Top 10 Business Relevant Applications by Usage**.

Application Usage side-panel

13. Click on the **View Details** link at the bottom right-corner of the **Application Health Summary** panel.

This will bring up the **Application Usage** side-panel. An example is shown in the following figure.

Figure 63 Application Usage Side-Panel



The **Application Usage** side-panel provides much of the same information already seen in previous panels. For example, the number and percentage of applications in each of the three business relevance categories – **Business Relevant**, **Business Irrelevant**, and **Default** is displayed in the upper right corner of the **Application Usage** side-panel.

The bottom part of the panel lists all of the application which belong to the selected business relevance category. For example, if **All Applications** is selected – as shown in the figure above – then all applications seen at all observation points for the specified location by Cisco DNA Application Assurance will be listed.

The information listed in the table consists of the following, per application:

- A health score over the past 5 minute collection interval. Health scores are calculated if the application is TCP or RTP-based, and if Cisco DNA Application Assurance is able to calculate a health score for the application. Health scores are not calculated for UDP-based applications. Health scores are based on packet loss, jitter, and latency – which is only captured by observation points which collect application experience statistics (Cisco IOS XE routers). Application traffic which only crosses observation points that collect application visibility statistics (Catalyst 9000 Series switches and Cisco AireOS WLCs) will not have health scores.

- The business relevance of the application.

- The amount of traffic (usage) seen (in bytes) across all observation points where Cisco DNA Application Assurance statistics are collected, for the specified location, and over the time period specified within the top panel of the **Application Health** dashboard.

- The average throughput (in bits/second) of the traffic across all observation points where Cisco DNA Application Assurance statistics are collected, for the specified location, and over the time period specified within the top panel of the **Application Health** dashboard.

- The percentage packet loss of the traffic across all observation points where application experience statistics are collected, for the specified location, and over the time period specified within the top panel of the **Application Health** dashboard. For TCP-based applications, packet loss is estimated based on retransmissions seen by Cisco Performance Monitor (Cisco ezPM) running on IOS XE routers. For RTP-based applications, packet loss is estimated based upon gaps in subsequent RTP sequence numbers. Again, this is only seen by Cisco Performance Monitor (Cisco ezPM) running on IOS XE routers. Application visibility statistics collected by Catalyst 9000 Series switches and Cisco AireOS WLCs do not include packet loss.

- The network latency (in milliseconds) of the traffic across all observation points where application experience statistics are collected, for the specified location, and over the time period specified within the top panel of the **Application Health** dashboard. Network latency is based on timing of packet sequences between the source and destination, captured by Cisco Performance Monitor (Cisco ezPM). Hence, network latency is calculated for TCP and RTP-based application flows which cross observation points of Cisco IOS XE routers. Application visibility statistics collected by Catalyst 9000 Series switches and Cisco AireOS WLCs do not include network latency.

- The jitter (in milliseconds) of the traffic across all observation points where application experience statistics are collected, over the time period specified within the top panel of the **Application Health** dashboard. Jitter is based on timestamps within RTP flows captured by Cisco Performance Monitor (Cisco ezPM). Hence, jitter is only calculated for RTP-based application flows which cross observation points of Cisco IOS XE routers. Application visibility statistics collected by Catalyst 9000 Series switches and Cisco AireOS WLCs do not include jitter.

The circular graph at the top, center of the **Application Usage** side-panel displays application usage – separated into broad categories either based on **Application Group** or **Traffic Class**. This is controlled through the drop-down menu in the upper right corner of the side-panel.

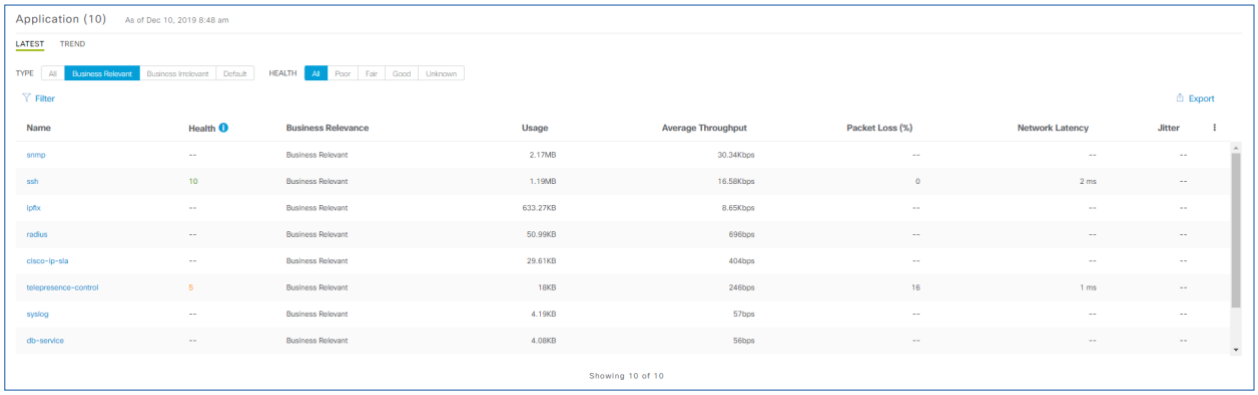
Information within the circular graph and the applications listed in the adjacent table will change, depending upon whether **All Applications**, **Business Relevant**, **Business Irrelevant**, or **Default** is selected.

14. When you are done viewing the **Application Usage** side-panel, close it by clicking on the **X** in the upper right corner of the side-panel to close it.

Application Panel

The bottom panel of the **Application Health** dashboard is the **Application** panel. The **Application** panel shows much of the same information displayed in the **Application Usage** side-panel discussed previously.

Figure 64 Application Panel



The applications displayed within the table can be filtered based upon the following criteria:

- **TYPE** – Displays only applications which have the selected business relevance – **All**, **Business Relevant**, **Business Irrelevant**, or **Default**.
- **HEALTH** – Displays only applications which have the selected health – **All**, **Poor**, **Fair**, **Good**, or **Unknown**.

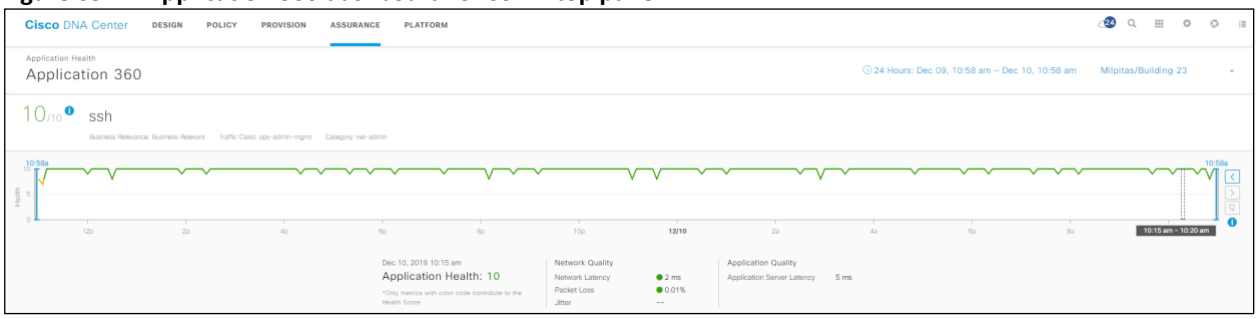
Procedure: Viewing Application Information within the Application 360 Dashboard

The **Application 360** dashboard for a given application is accessed by clicking on the application name from within the **Application** panel of the **Application Health** dashboard.

1. From the Application panel of the **Application Health** dashboard (see **Figure 64** above), click on the name of one of the applications.

This will bring up the **Application 360** dashboard for the selected application. The **Application 360** dashboard has multiple panels. An example of the top panel for the SSH application is shown in the following figure.

Figure 65 Application 360 dashboard for SSH – top panel

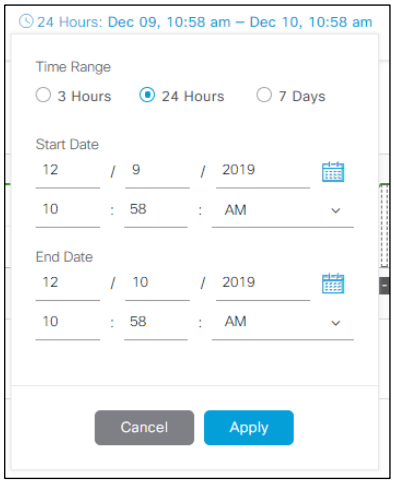


The top panel displays a historical timeline of the overall health of the application. By default, the time period covered by the timeline is the last 24 hours.

2. Click on the link directly above the timeline to change time period.

This will bring up a pop-up window allowing you to select a time period (3 hours, 24 hours, or 7 days) or specify a start and stop date and time. An example is shown in the figure below.

Figure 66 Application 360 Dashboard – Timeline Controls

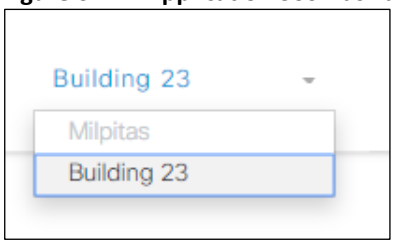


Changing the time period covered by the timeline will change the information displayed within the rest of the **Application 360** dashboard for the given application. For example, aggregate application usage statistics and average throughput may change depending upon the timeframe over which the statistics are displayed.

3. Click on the link adjacent to the time controls to change the location to which the health score applies.

This will bring up a pop-up window allowing you to select the location. An example is shown in the figure below.

Figure 67 Application 360 Dashboard – Site Controls



4. Hover your cursor above any point on the timeline (see **Figure 65** above).

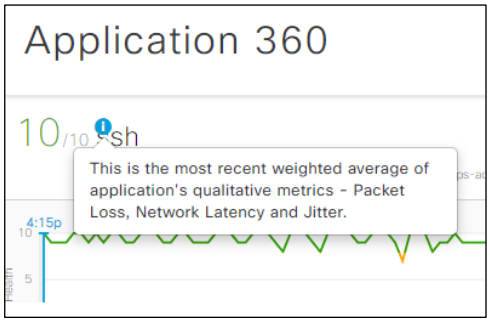
Under the timeline you will see details regarding how the overall health score is determined for that application for that particular time. For example, in **Figure 65** above it can be seen that the overall health score (10 out of a possible score of 10) for the SSH application is based on the score for **Network Quality**. The score for **Network Quality** is based on three factors – **Network Latency**, **Packet Loss** and **Jitter**. From **Figure 65** above, it can be seen that the health scores for **Network Latency** and **Packet Loss** show green dots, indicating a healthy score (8 – 10 out of a possible score of 10). Adjacent to the green dot are the latency (2 milliseconds) and packet loss (0.01%) values measured for that particular time.

Notice that **Jitter** shows no information. **Jitter** is only calculated for Real-time Transport Protocol (RTP) based applications through Cisco Performance Monitor (Cisco PerfMon), using the timestamps within the RTP header. In the case of protocols which do not support the calculation of **Jitter**, the Jitter information is simply not included within the overall **Network Quality** score.

5. Hover your cursor above the blue "i" indicating information directly above the name of the application.

This will display a pop-up window explaining how the overall **Application Health** score is calculated. An example is shown in the figure below.

Figure 68 Application 360 – Health Score information



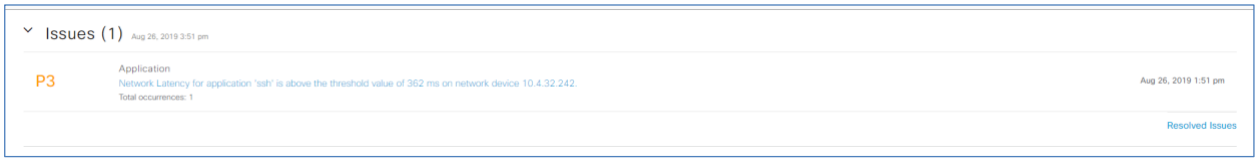
The **Application Health** score is the weighted average of the **Network Latency**, **Packet Loss**, and **Jitter** measured for the application over the particular time interval of the timeline. The weighting, as well as the values which constitute a good, fair, or poor score for each of the parameters (**Network Latency**, **Packet Loss**, and **Jitter**), is application dependent and determined based upon the application's tolerance to latency, jitter, and packet loss – based upon industry standard guidelines such as IETF RFC-4594 and ITU-T Y.1541.

The overall health score (10/10) displayed at the top of the **Application 360** dashboard for the SSH application (see **Figure 68**) is for the current collection time interval. That time interval is 5 minutes when the timeline is set for either three hours or 24 hours. If the timeline is set for 7 days, the collection interval is the last 60 minutes.

The information displayed when you hover over the timeline (see **Figure 65**) may also include **Application Quality**. Under **Application Quality** there is a single parameter, **Application Server Latency**. This is different from **Network Latency**. **Application Server Latency** is an estimate of the latency of the server itself – in other words, total latency minus network latency. This is calculated through Cisco Performance Monitor (Cisco PerfMon) as traffic flows across the router platform between client and server in a TCP-based application. Note that the client refers to the device which initiates the TCP session, while the server is the device which responds, when looking at **Application Server Latency**. The combination of **Network Latency** and **Application Server Latency** can be useful in determining if a performance issue is due the network (high **Network Latency**) or due to an overburdened server (high **Application Server Latency**).

The second panel in the **Application 360** dashboard is the **Issues** panel. An example is shown in the figure below.

Figure 69 Application 360 dashboard – Issues panel



The **Issues** panel displays any open (non-resolved) issues seen for the particular application over the time period displayed in the timeline at the top of the **Application 360** dashboard. The Issues panel displays the following information:

- The color-coded severity of each issue, from **P1** through **P4**.
- The category of the issue. Within Cisco DNA Center, issues are broadly identified as belonging to one of the following nine categories:
  - Onboarding
  - Connectivity
  - Connected
  - Device

- Availability
- Utilization
- Application
- Sensor Test
- AP Anomaly

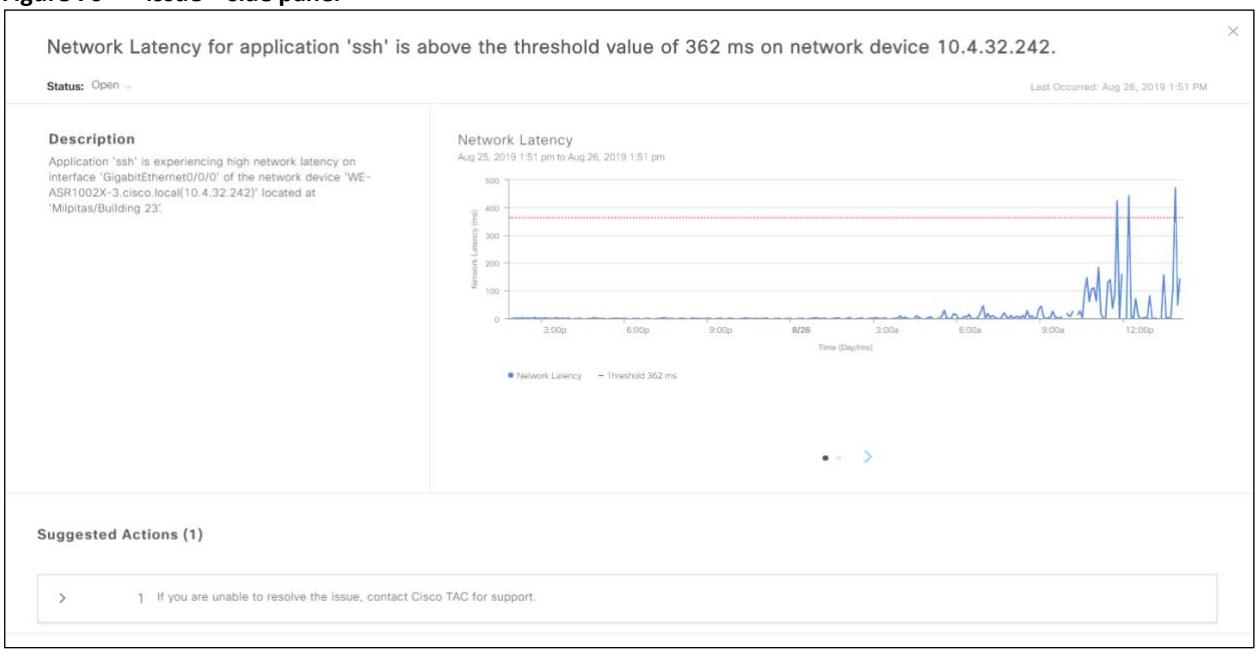
- A brief description of the issue.
- The number of occurrences of this issue seen over the time period covered by the timeline at the top of the **Application 360** dashboard.

In the figure above, a single **P3** issue "**Network Latency for application 'ssh' is above the threshold value of 362 ms on network device 10.4.32.242**" is displayed. Since the issue is being viewed from within the **Application 360** dashboard, the category of the issue is **Application**, as expected.

6. Click on the description of the issue to bring up a side panel with further details of the issue.

An example is shown in the following figure.

Figure 70 Issue – side panel



The side panel provides a more detailed explanation as to why the issue was raised. Under **Description** we can see that the issue was seen on the **GigabitEthernet0/0/0** interface of WAN head-end router **WE-ASR1002X-3** at the **Milpitas/Building 23** location. This corresponds to one of the observation points where Cisco DNA Application Assurance data is being collected for this design and deployment guide. In a large network with multiple Cisco DNA Network Assurance observation points, knowing where an application performance issue is occurring is important for assessing the impact of the issue as well as troubleshooting the issue.

The graph to the right of the **Description** provides a historical timeline of the parameter that was the cause of the issue. In this case it shows **Network Latency** over the time period set within the timeline in the **Application 360** dashboard. The red dashed line indicates a pre-set threshold of 362 milliseconds, which is specific to the SSH application. From this graph we can see that when **Network Latency** exceeds 362 milliseconds for the SSH application, a **P3** severity issue is generated.

From the graph we can also see that the high **Network Latency** does not appear to be periodic, and only began within the last three hours (from approximately 10 am onward) in the graph. This suggests a possible issue with the WAN uplink of the head-end router.

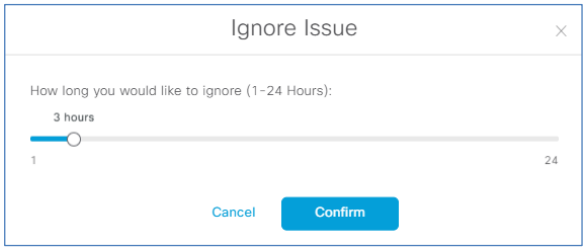
The **Suggested Actions** section may provide some possible actions to take to resolve the issue – depending upon the particular issue seen. For this particular issue, not enough information is available – based solely on infrequent high **Network Latency** – for any suggested actions.

7. Click on the drop-down menu next to **Status**, in the upper right corner of the side-panel, to change the status of the issue.

You can change the status of the issue from **Open** to **Resolve**, or you can **Ignore** the issue.

8. If you select **Ignore**, a pop-up screen will appear, asking you how long you wish to ignore the issue.

Figure 71 Ignore Issue pop-up window



9. Use the slider to determine how long you wish to ignore the issue – from 1 hour to 24 hours. The default is 3 hours.

10. Click **Confirm** to confirm temporarily ignoring the issue and close the pop-up window.

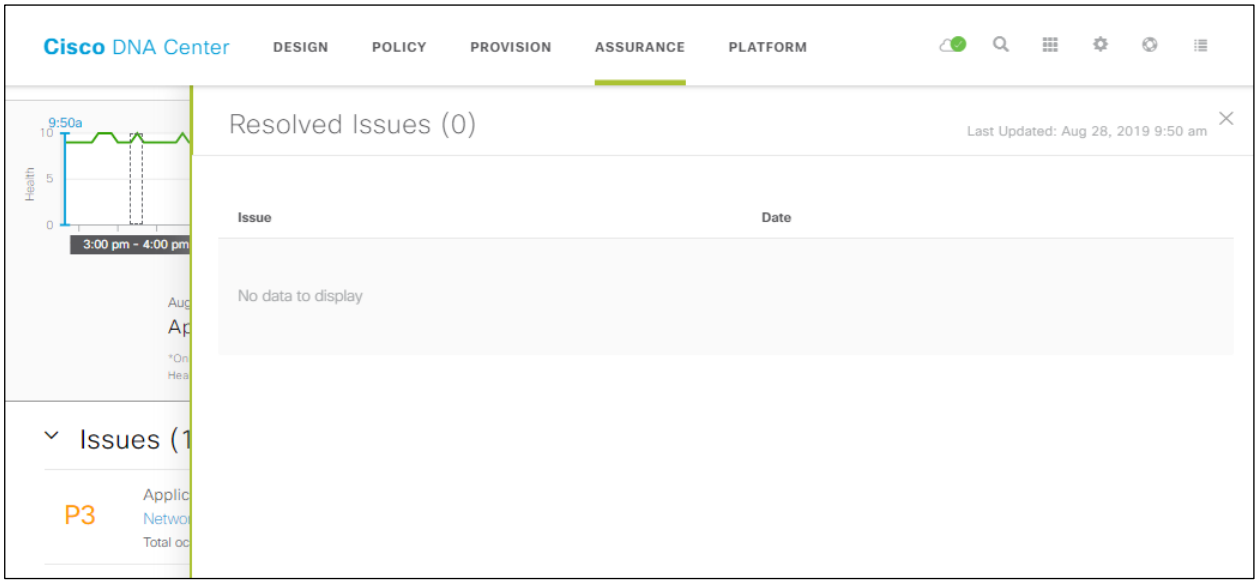
Temporarily ignoring an issue may be useful in the situation where resolution is ongoing, and you don't want to continue seeing the issue repeatedly come up.

11. When you are done with viewing the side panel, click on the **X** in the upper right corner to close the side panel and return to the **Application 360** dashboard.

12. If you wish to view resolved issues for the given application, click on the **Resolved Issues** link at the bottom right of the **Issues** panel within the **Application 360** dashboard.

This will bring up a side panel showing the resolved issues for the particular application. An example is shown in the following figure.

Figure 72 Resolved Issues Side-Panel



If no issues have been resolved for the particular application selected, the side panel will be empty.

13. Click on the **X** in the upper right corner of the **Resolved Issues** side panel to close it.

You can control the severity level (**P1** through **P4**) of the issues that are generated.

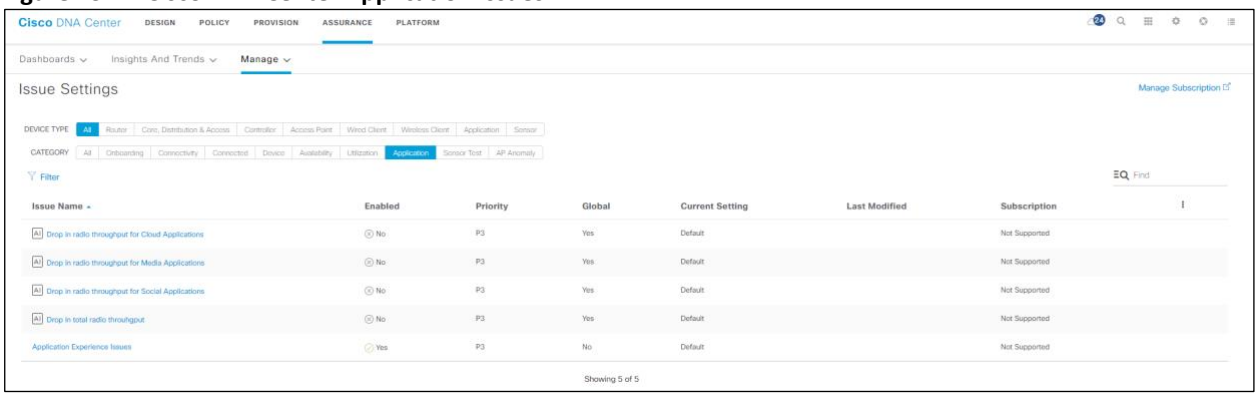
14. From the main **Application Health** dashboard navigate to **Manage > Issue Settings.**

This will take you to the **Issue Settings** dashboard.

15. Within the **Issue Settings** select the **Device Type** of **All** and the **Category** of **Application**.

This will display all **Application** issues which Cisco DNA Center can raise. An example is shown in the figure below.

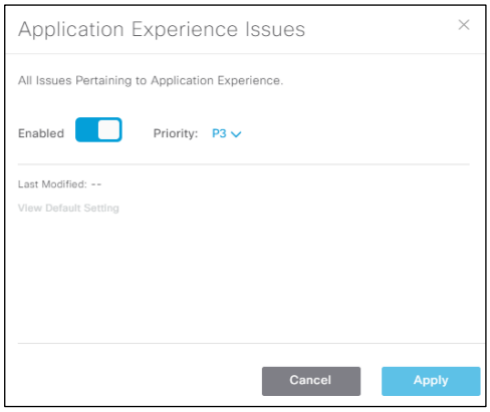
Figure 73 Cisco DNA Center Application Issues



16. Click on **Application Experience Issues**.

This will bring up a side-panel, allowing you to change the severity level of all application experience related issues – from **P1** through **P4**. The default is to report all application experience related issues with a severity level of **P3**. You can also enable / disable the reporting of application experience related issues if you choose. The default is enabled, meaning that application experience related issues are generated. An example is shown in the following figure.

Figure 74 Enabling / disabling and changing the severity level of Application Experience Issues



17. When you are done viewing the side panel, click on the **X** in the upper right corner to close the side panel if you have not made any changes, or click **Apply** if you have made changes, to return to the **Issues Settings** dashboard.

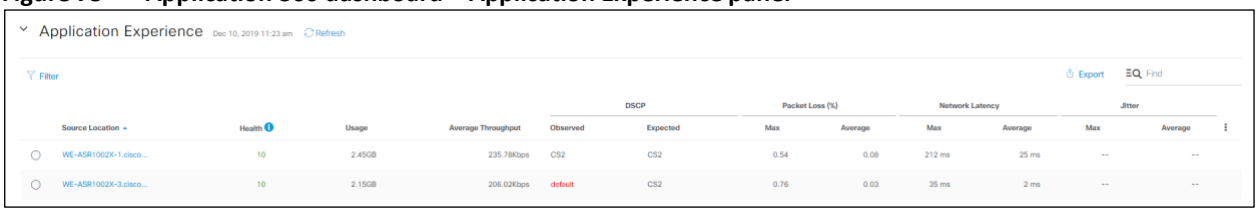
18. Navigate back to **Assurance → Dashboards → Health > Application Health.**

This will take you back to the **Application Health** dashboard.

19. In the **Application** (bottom) panel of the **Application Health** dashboard click on the application (SSH in this design guide) to return to the **Application 360** dashboard for the application.

The final panel in the **Application 360** dashboard is the **Application Experience** panel. An example is shown in the following figure.

Figure 75 Application 360 dashboard – Application Experience panel



The **Application Experience** panel provides a wealth of application information – from the perspective of the network device which serves as the observation point for the Cisco DNA Application Assurance data.

For this design and deployment guide, the WAN head-end ASR1K routers (**WE-ASR1002X-1** and **WE-ASR1002X-3**) are two observation points where application experience data collection has been enabled for the selected location (**Milpitas/Building 23**). Since the application selected within the **Application 360** dashboard is SSH, and since SSH traffic has crossed both WAN head-end routers, both network devices appear within the panel under the **Source Location** column.

The following information is displayed within the columns per network device:

Health – This column shows the health of the application (SSH in this case), as calculated at that network device. The health is calculated over the last 5 minute interval (you can display this by hovering over the blue "**i**" next to **Health**). In the figure above you can be seen that the health of the SSH application is a 10 out of 10 for both routers. Both are good / healthy scores, as indicated by the green coloring of the score. The color-coded health score provide a quick visual indication as to where possible issues are occurring within your network for the selected application.

Usage Bytes – This column shows the total amount of traffic (in bytes) seen for the selected application (SSH in this case) at that network device, for the time period covered within the timeline at the top of the **Application 360** dashboard. Changing the overall time period covered by the timeline at the top of the **Application 360** dashboard will change the usage displayed

within the **Application Experience** panel. The **Usage Bytes** column provides a quick visual indication of the amount of traffic for the selected application crossing a given network device.

Average Throughput – This column shows the amount of traffic seen for the selected application (SSH in this case) at that network device, averaged over the time period covered within the timeline at the top of the **Application 360** dashboard. Changing the overall time period covered by the timeline at the top of the **Application 360** dashboard will change the **Average Throughput** displayed within the **Application Experience** panel. The **Average Throughput** column provides a quick visual indication of the traffic rate for the selected application crossing a given network device.

DSCP Observed – This column show the actual DSCP markings of traffic flows from the selected application (SSH in this case) at that network device. The DSCP markings are provided through Flexible NetFlow records, which are part of the Cisco ezPM Application Performance profile context applied to the GigabitEthernet0/0/0 interfaces of the WAN head-end ASR1K routers.

DSCP Expected – This column shows the expected DSCP markings of the traffic flows based upon the traffic-class to which the selected application (SSH in this case) belongs. This is discussed within the design section of this document. Most network deployments have the same DSCP marking for a given application across the entire network. However, the **DSCP Expected** column displays the information per network device.

Packet Loss (%) Max – This column shows the maximum percentage packet loss seen over a collection interval within the overall time period, for the selected application (SSH in this case) at that network device. The collection interval varies based on the overall time period covered by the timeline at the top of the **Application 360** dashboard for the application.

Packet Loss (%) Average – This column shows the average percentage packet loss seen over all of the collection intervals within the overall time period, for the selected application (SSH in this case) at that network device. The collection interval varies based on the overall time period covered by the timeline at the top of the **Application 360** dashboard. The combination of the average and maximum packet loss can provide you with valuable information regarding where packet loss is occurring for the selected application – potentially degrading the end-user's experience and productivity; and whether the packet loss is a one-time event (high percentage packet loss during one collection interval) or an ongoing concern (low percentage packet loss occurring over multiple collection intervals). Packet loss statistics are only collected for TCP and RTP-based applications, and only by network devices which collect application experience statistics (Cisco IOS XE routers).

Network Latency Max – This column shows the maximum network latency seen over a collection interval within the overall time period, for the selected application (SSH in this case) at that network device. The collection interval varies based on the overall time period covered by the timeline at the top of the **Application 360** dashboard. Network latency statistics are only collected for TCP and RTP-based applications, and only by network devices which collect application experience statistics (Cisco IOS XE routers).

Network Latency Average – This column shows the average network latency seen over all of the collection intervals within the overall time period, for the selected application (SSH in this case) at that network device. The collection interval varies based on the overall time period covered by the timeline at the top of the **Application 360** dashboard. The combination of the average and maximum network latency can provide you with valuable information regarding where high network latency is occurring for the selected application – potentially degrading the end-user's experience and productivity; and whether the network latency is a one-time event (high network latency during one collection interval) or an ongoing concern (high network latency occurring over multiple collection intervals). Network latency statistics are only collected for TCP and RTP-based applications, and only by network devices which collect application experience statistics (Cisco IOS XE routers).

Jitter Max – This column shows the maximum jitter seen over a collection interval within the overall time period, for the selected application (SSH in this case) at that network device. The collection interval varies based on the overall time period covered by the timeline at the top of the **Application 360** dashboard.

Jitter Average – This column shows the average jitter seen over all of the collection intervals within the overall time period, for the selected application (SSH in this case) at that network device. The collection interval varies based on the overall time period covered by the timeline at the top of the **Application 360** dashboard. The combination of the average and maximum jitter can provide you with valuable information regarding where high jitter is occurring for the selected application –

potentially degrading the end-user's experience and productivity; and whether the jitter is a one-time event (high network jitter during one collection interval) or an ongoing concern (high jitter occurring over multiple collection intervals). Jitter statistics are only collected for RTP-based applications, and only by network devices which collect application experience statistics (Cisco IOS XE routers).

Procedure: Viewing Application Information within the Device 360 Dashboard

The following are steps to view Cisco DNA Application Assurance data collected by Cisco DNA Center through the **Device 360** dashboard for a given network device.

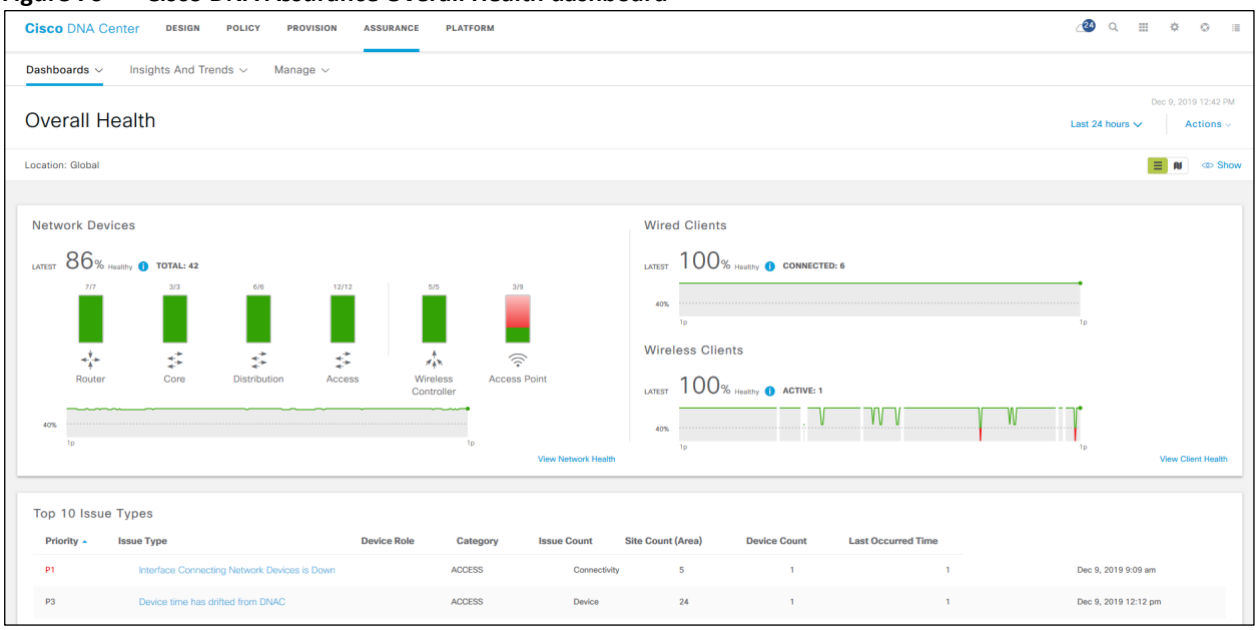
1. Login to the Cisco DNA Center web console using the IP address or fully qualified domain name of your instance.

For example: https://<Cisco_DNA_Center_IPaddr_or_FQDN>.

2. From the main Cisco DNA Center dashboard navigate to **Assurance**.

This will take you to the **Overall Health** dashboard within Cisco DNA Assurance. An example is shown in the following figure.

Figure 76 Cisco DNA Assurance Overall Health dashboard



3. Navigate to **Dashboards → Health → Network Health**.

This will take you to the **Network Health** dashboard.

4. Scroll to the **Network Devices** panel at the bottom of the **Network Health** dashboard.

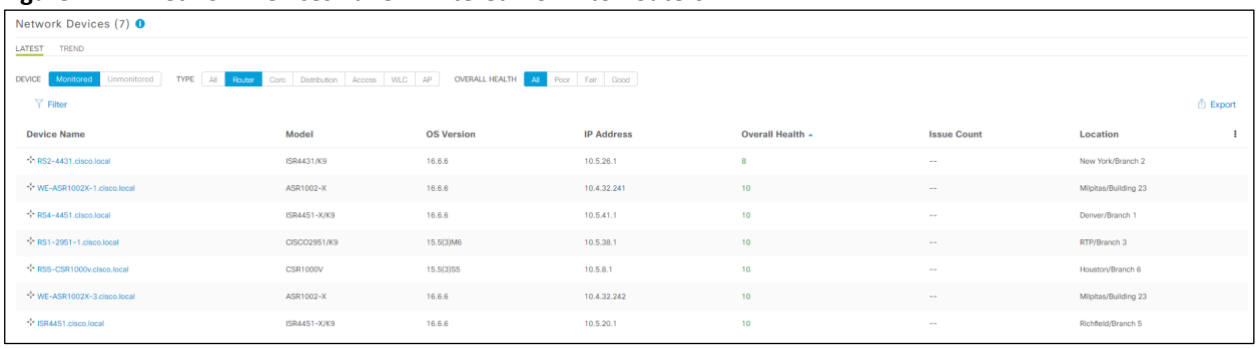
Here you will see a list of network devices seen by Cisco DNA Application Assurance. You can filter the network devices seen by Cisco DNA Center based upon the following:

- Whether the device is **Monitored** or **Unmonitored** by Cisco DNA Center
- The **Type** of Device – **All**, **Router**, **Core** switch, **Distribution** switch, Access switch, **WLC**, or Access Point (**AP**)
- The **Overall Health** of the device – **All** health scores, **Poor**, **Fair**, or **Good** health

5. Select **DEVICE** – **Monitored**, **TYPE** – **Router, OVERALL HEALTH** - **All**

The network devices list will be filtered down to monitored routers. An example is shown in the figure below.

Figure 77 Network Devices Panel – Filtered Down to Routers



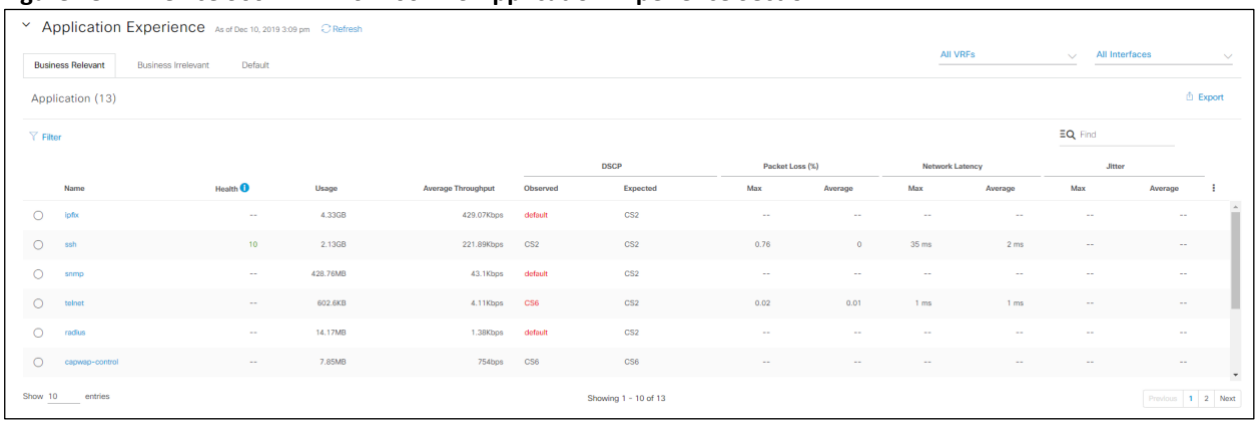
6. Locate one of the ASR1K head-end routers (**WE-ASR1002X-3**) and click on it.

This will bring up the **Device 360** screen for the ASR1K router.

7. Scroll down and expand the **Application Experience** section of the **Device 360** screen for the router.

This will display the applications seen by the **WE-ASR1002X-3**. An example of the **Application Experience** data is shown in the figure below.

Figure 78 Device 360 – WE-ASR1002X-3 Application Experience Section



The following information is displayed within the columns per network device:

- **Health** – This column shows the health of each application seen at that network device. The health is calculated over the last 5 minute interval (you can display this by hovering over the blue "**i**" next to **Health**). In the figure above you can be seen that the health of the SSH application is a 10 out of 10. This is a good / healthy score, as indicated by the green coloring of the score. The color-coded health score provide a quick visual indication as to which applications may be having issues across the observation point of the network device.

- **Usage** – This column shows the total amount of traffic (in Bytes) seen for each application at that network device, for the time period covered within the timeline at the top of the **Device 360** dashboard. Changing the overall time period covered by the timeline at the top of the **Device 360** dashboard will change the usage displayed within the **Application Experience** panel. The **Usage** column provides a quick visual indication of the amount of traffic for each application crossing the observation point of the network device.

- **Average Throughput** – This column shows the amount of traffic seen for each application at that network device, averaged over the time period covered within the timeline at the top of the **Device 360** dashboard. Changing the overall time period covered by the timeline at the top of the **Device 360** dashboard will change the **Average Throughput** displayed within the **Application Experience** panel. The **Average Throughput** column provides a quick visual indication of the traffic rate for each application crossing the observation point of the network device.

- **DSCP Observed –** This column show the actual DSCP markings of traffic flows from applications at the network device. The DSCP markings are provided through Flexible NetFlow records, which are part of the Cisco ezPM Application Performance profile context applied to IOS XE routers. **DSCP Observed** and **DSCP Expected** data is only collected and displayed by network devices which support the collection of application experience data (IOS XE Routers). Network devices which only support the collection of application visibility data (Catalyst 9000 Series switches and AireOS WLCs) will not display any DSCP markings for applications seen as traffic crosses the observation points of these platforms.

- **DSCP Expected –** This column shows the expected DSCP markings of traffic flows based upon the traffic-class to which the application belongs.

- **Packet Loss (%) Max** – This column shows the maximum percentage packet loss seen over a collection interval within the overall time period, for each application seen at the network device. The collection interval varies based on the overall time period covered by the timeline at the top of the **Device 360** dashboard for the network device.

- **Packet Loss (%) Average** – This column shows the average percentage packet loss seen over all of the collection intervals within the overall time period, for each application seen at the network device. The collection interval varies based on the overall time period covered by the timeline at the top of the **Device 360** dashboard. The combination of the average and maximum packet loss can provide you with valuable information regarding what applications are experiencing packet loss as the application traffic flows cross the observation point of the network device – potentially degrading the end-user's experience and productivity; and whether the packet loss is a one-time event (high percentage packet loss during one collection interval) or an ongoing concern (low percentage packet loss occurring over multiple collection intervals). Packet loss statistics are only collected and displayed for TCP and RTP-based applications, and only by network devices which collect application experience statistics (Cisco IOS XE routers).

- **Network Latency Max** – This column shows the maximum network latency seen over a collection interval within the overall time period, for each application seen at the network device. The collection interval varies based on the overall time period covered by the timeline at the top of the **Device 360** dashboard. Network latency statistics are only collected for TCP and RTP-based applications, and only by network devices which collect application experience statistics (Cisco IOS XE routers).

- **Network Latency Average** – This column shows the average network latency seen over all of the collection intervals within the overall time period, for each application seen at the network device. The collection interval varies based on the overall time period covered by the timeline at the top of the **Device 360** dashboard. The combination of the average and maximum network latency can provide you with valuable information regarding what applications may be experiencing high network latency as the application traffic flows cross the observation point of the network device – potentially degrading the end-user's experience and productivity; and whether the network latency is a one-time event (high network latency during one collection interval) or an ongoing concern (high network latency occurring over multiple collection intervals). Network latency statistics are only collected for TCP and RTP-based applications, and only by network devices which collect application experience statistics (Cisco IOS XE routers).

- **Jitter Max** – This column shows the maximum jitter seen over a collection interval within the overall time period, for each application seen at the network device. The collection interval varies based on the overall time period covered by the timeline at the top of the **Device 360** dashboard.

- **Jitter Average** – This column shows the average jitter seen over all of the collection intervals within the overall time period, for each application seen at the network device. The collection interval varies based on the overall time period covered by the timeline at the top of the **Device 360** dashboard. The combination of the average and maximum jitter can provide you with valuable information regarding what applications may be experiencing high jitter as the application traffic flows cross the observation point of the network device – potentially degrading the end-user's

experience and productivity; and whether the jitter is a one-time event (high network jitter during one collection interval) or an ongoing concern (high jitter occurring over multiple collection intervals). Jitter statistics are only collected for RTP-based applications, and only by network devices which collect application experience statistics (Cisco IOS XE routers).

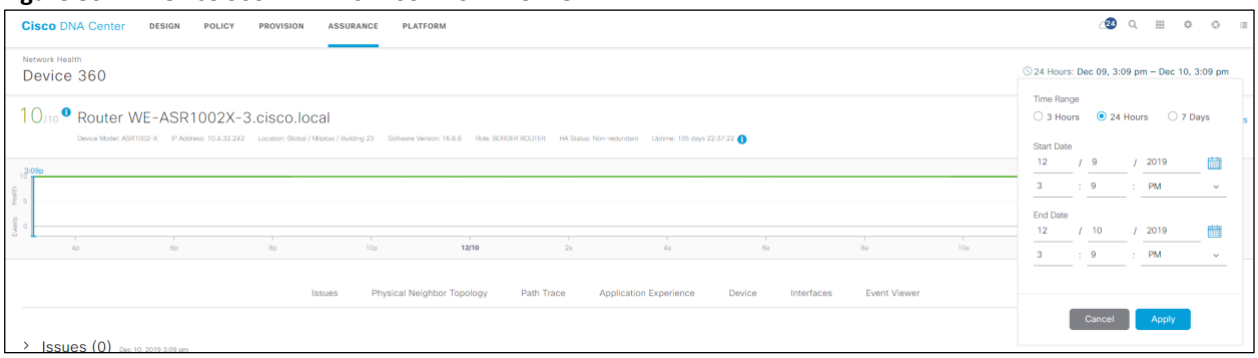
8. You can add additional columns, such as the **Traffic-class** to which the application belongs, the **Usage Percentage (%)** for each application, etc. by clicking on the drop-down menu at the right of the screen and selecting these columns.

An example is shown in the figure below.

Figure 79 Device 360 – WE-ASR1002X-3 Application Experience with Additional Columns

As discussed in the bullets above, many of the statistics are calculated across the overall length of the timeline displayed at the top of Device 360 screen for the network device, as shown in the following figure.

Figure 80 Device 360 – WE-ASR1002X-3 Timeline



By default, the timeline is set for 24 Hours.

9. You can modify the span of the timeline by clicking on it, which will bring up a pop-up window, as shown in the figure above.

Changing the timeline may result in a change to the displayed information, to reflect the statistics collected over the modified time span.

By default, the **Business Relevant** tab will be selected in the **Application Experience** section.

10. You can select the **Business Irrelevant** or **Default** tabs to display the applications seen by the network device with those business-relevance attributes.

Procedure: Viewing Information within the Device 360 Dashboard

The following are steps to view Cisco DNA Application Assurance data collected by Cisco DNA Center through the **Client 360** dashboard for a given network device.

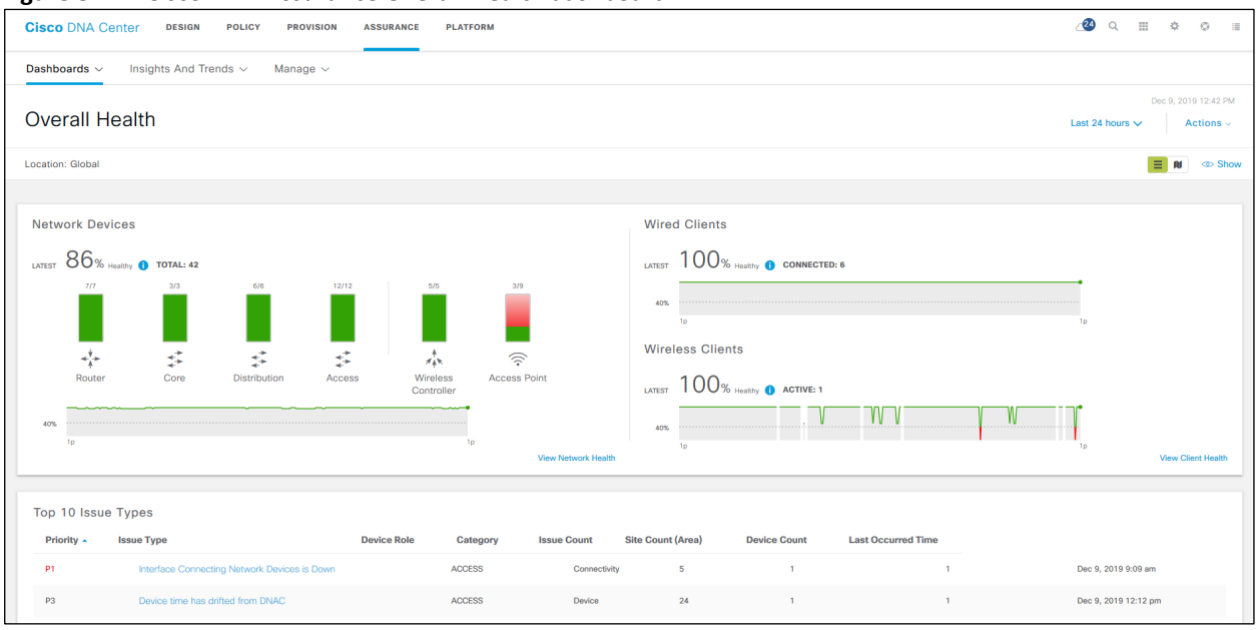
11. Login to the Cisco DNA Center web console using the IP address or fully qualified domain name of your instance.

For example: https://<Cisco_DNA_Center_IPaddr_or_FQDN>.

12. From the main Cisco DNA Center dashboard navigate to **Assurance**.

This will take you to the **Overall Health** dashboard within Cisco DNA Assurance. An example is shown in the following figure.

Figure 81 Cisco DNA Assurance Overall Health dashboard



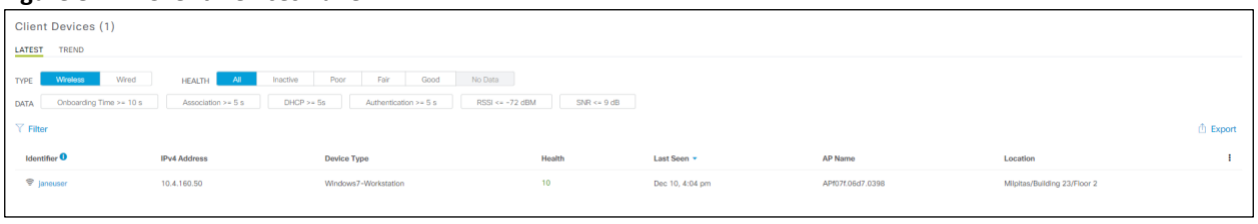
13. Navigate to **Dashboards → Health → Client Health**.

This will take you to the **Client Health** dashboard.

14. Scroll to the **Client Devices** panel at the bottom of the **Client Health** dashboard.

Here you will see a list of client devices seen by Cisco DNA Application Assurance. An example is shown in the figure below.

Figure 82 Client Devices Panel



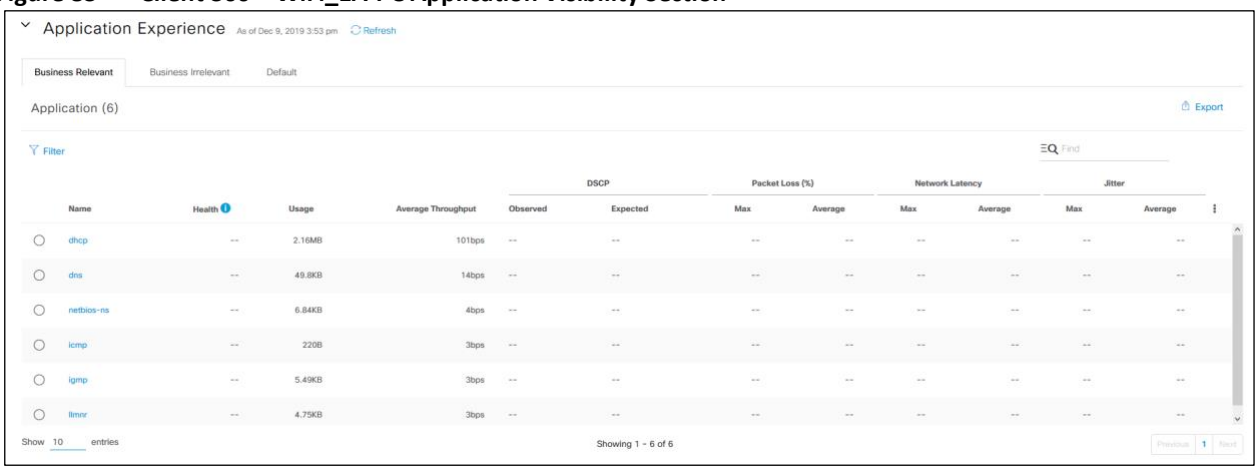
15. Locate one of the clients (**janeuser**) and click on it.

This will bring up the **Client 360** screen for the client.

16. Scroll down and expand the **Application Experience** section of the **Client 360** screen for the client.

This will display the application statistics seen for that particular client, calculated across the overall length of the timeline displayed at the top of **Client 360** screen for that particular client. As with the **Device 360** screen, the time span of the timeline can be modified – which may change the statistics displayed in the **Application Visibility** section of the **Client 360** screen. An example of the **Application Experience** section for the **WiFi_1A-PC** client is shown in the figure below.

Figure 83 Client 360 – WiFi_1A-PC Application Visibility Section



Here you can view the application traffic sent and received by this individual client, based upon business relevance attribute. By default the **Business Relevant** tab is selected. The meaning of the columns is the same as discussed in the previous procedure.

Note that the columns which display DSCP values, **Packet Loss(%)**, **Network Latency**, and **Jitter**, in the **Application Experience** section of the **Client 360** screen in the figure above are empty. Although this may seem slightly confusing at first, it is because the application statistics for this client were collected by an AireOS WLC, which only supports the collection of application visibility data, and not application experience data. If the traffic from this client had been seen at an observation point on a Cisco IOS XE router, then additional statistics such as **Packet Loss(%)**, **Network Latency**, and **Jitter** may be collected (depending upon whether the traffic flow was UDP, RTP, TCP, etc.), and additional information displayed.

Appendix D—Glossary

AP Access Point

Cisco ezPM Cisco Easy Performance Monitor

Cisco NBAR2 Cisco Network Based Application Recognition - Version 2

Cisco PerfMon Cisco Performance Monitor

CS2 Class Selector 2

DSCP Differentiated Services Code Point

ECMP Equal-Cost Multi-path

FEW Fabric Enabled Wireless

FNF Flexible NetFlow

L2 Layer 2

L3 Layer 3

LAN Local Area Network

OAM Operations, Administration, and Management

RTP Real-time Transport Protocol

SNMP Simple Network Management Protocol

SP Service Provider

SSH Secure Shell Protocol

TCP Transmission Control Protocol

UDP User Datagram Protocol

WAN Wide-Area Network

Wired AVC FNF Flexible NetFlow which includes the use of NBAR2, supported on wired access ports

WLAN Wireless Local-Area Network

WLC Wireless LAN Controller

About this guide

Feedback & Discussion

For comments and suggestions about our guides, please join the discussion on Cisco Community.