Smart Network Application

This chapter contains the following sections:

Smart Network Application (SNA)

Smart Network Application (SNA) is an embedded monitoring and management tool that simplifies the operation of your small business network. The SNA can discover network topology, display link status, monitor events, apply configurations and upgrade software images. You can view a short training video on the Smart Network Application here: https://video.cisco.com/video/5273189520001

To launch the SNA, complete the following steps:

Step 1 Open a Web browser.

Step 2 Enter the IP address of the device you are configuring in the address bar on the browser, and then press **Enter**.

Step 3 When the Login window is displayed, enter your username and password and select **Network Management**.

Step 4 When first entering SNA, the topology map is empty and blocked behind a modal. You are asked to enter your credentials (username of up to 20 characters and a password of up to 64 characters). If the credentials are rejected, you are informed of the rejection and of the rejection reason.

Step 5 After SNA loads, it creates a management sessions with all other SNA-capable devices in the network over a WebSocket using the same credentials used to login to SNA. As a result, only SNA-capable devices using the same credentials provide data and management capabilities. Other devices do not appear as SNA devices even if they have SNA capabilities.

An SNA session can have the following access permission levels:

- Full—A session begins in full access mode. All SNA operations are possible.
- Read Only—After a session is idle for 15 minutes, it changes into a Read-Only session.

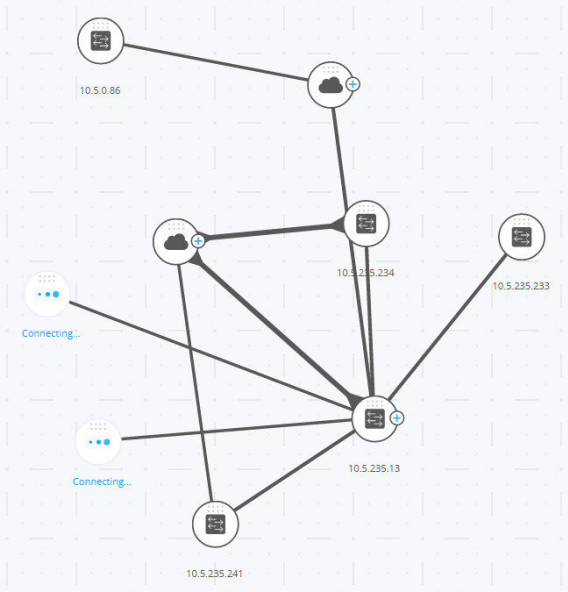
The SNA uses the same credentials as the web switch management application, and creates an HTTP management session over which it works. The SNA session counts against the number of possible concurrent web management sessions for the SNA manager along with active regular web management sessions.

Topology View

The topology view is the main view of the SNA.

Figure 1 is a graphical representation of a network that includes information on your network devices and their connections.

Figure 1 Topology View



Various overlays can be selected for the topology views that affect the graphic representation of elements. The topology discovery mechanism uses information gathered from LLDP and CDP TLVs to identify devices in the network.

To maximize information provided in the topology, all devices in the network, which support these protocols, must have them enabled.

Since the topology is created by creating management sessions with the participating SNA devices, when using the HTTPS protocol to launch the SNA, all SNA switches in the network must be authorized or added to the certificate exception list on the web client (browser) used for SNA.

Topology Overlays

Various overlays of the topology view are supported such as VLAN membership, Spanning Tree, PoE, and Link Utilization. If you select the VLAN Membership overlay, for example, VLAN information is added to the topological view.

Devices

Detected devices are represented as nodes in the topology view, as shown in the Figure 1.

Click on a device to display the following information in the right-hand information (if the information is available):

- Device type—The icon shape indicates the device type. Device types include: switch, access point, PC, or IP phone. If the device type is not pre-defined, or if the type is not detected properly for some reason, the device type is shown as Unknown.
- Switches discovered on the network are labeled as one of the following types:
  - SNA Switch— Switch (running version 2.2.5 or higher) with the full SNA feature set.
  - Unmanaged Switch— A switch that cannot be accessed through SNA.
- Device Name
- IP Address (A list if more than one is discovered)
- MAC Address (A list if more than one is discovered)
- Number of Notifications–The number of notifications is indicated by a number in orange on the device icon. The actual notifications are displayed in the right-hand information panel.
- SNA Support
- Manufacturer

Some devices (particularly SNA-capable devices) have additional information, such as individual port information. This information can be viewed by clicking on their icon and displaying a device explorer screen for the device.

Devices in the network are separated into the following categories:

- Backbone devices – Basic skeleton of the network. By default, all switches, routers and access points detected on the network are designated automatically as backbone devices. After a backbone device is detected, it remains on the topology map until it is manually removed. If the device is disconnected from the network, it still appears on the topology map as an offline device.
- Offline devices – Backbone devices that were previously added to the topology (either by the topology detection mechanisms or manually). These devices are no longer detected by SNA. Offline devices have the following characteristics:
  - Distinct visual appearance from online devices on the topology map.
  - Can be moved on the topology, and its placement can be saved. You can also add tags to the device.
  - Selectable and detectable by the search functionality. When an offline device is selected, the information panel displays the device’s basic identifying information and tags, but no services, notifications, or general information beyond the basic identifiers.

- Unable to launch the device explorer or the device management GUI of offline devices.
- Can be manually removed. After a device is removed, it no longer appears on the topology map until it is detected or added manually. All tags associated with this device are lost, and is not restored even if the device is detected again in the future.

SNA periodically attempts to connect to offline devices to verify if a managed or an SNA switch has come back online. During these attempts, an indication is displayed on the device.

- Client devices – End-point clients of the network (for example, PCs, IP phones) usually connected to a backbone device. In the topology map, these devices are displayed grouped with other devices of the same type that are connected to the same backbone device. If a device has one or more client devices attached to it, a + appears on it. Click on the + to display the clients.

Ports

To view the ports on a device, select the device and then double-click it. This opens a panel that displays all ports of the device, including all units if the device is in stack mode.

Connections Between Devices

Connections between devices are color-coded, depending on the current overlay. A connection may represent a single link between devices or an aggregation of links between two devices. The width of connections between the switches on the topology map is an indication of the aggregated bandwidth available on the connection as determined by the operational speed of the links in the connection.

The following connection widths are available (from narrowest to widest):

- Level 1—Less than 1GB
- Level 2—1GB to less than 10GB
- Level 3—More than 10 GB

Links whose capacity cannot be calculated or links between a backbone device and its clients are shown as level 1 links.

The connection between SNA-capable devices is detected from both sides. If there is a difference between the calculated capacities of the connection between the two sides, the width is drawn according to the lower of the two values.

Clouds

Clouds are sections of the network that SNA cannot map in detail. The SNA may determine that more than one device is connected to the network through a specific port, but is unable to map the relationship between those devices. This occurs because there are no SNA-capable devices among them. SNA draws a cloud on the topology map and displays the devices detected in this cloud as connected clients. Most SNA operations are not applicable to clouds.

Header Block

The following information is displayed in the header, according to the type of entity selected:

- Devices —Identifying information consisting of the type of device, and the strongest two forms of identification by which the device was recognized. Host name IP address MAC address.
- Interfaces — Identifying information is the name of the interface and the strongest form of identification of the device it belongs to: host name, IP address if the host name is not known, or MAC address if both the host name and the IP address are not known.
- Connections — Identifying information is the two strongest forms of identification of the devices on both sides of the connection (Host name IP address MAC address). A connection can contain one or more link.

Selecting a client group is a shortcut to selecting all members of the group. The header shows the number and type of device in the group. When selecting a client group together with other devices, the client groups counts as the number of devices that are contained in it. For example, when selecting a backbone device and a client group containing 5 clients the header shows six devices selected.

Right-Hand Information Panel Cogwheel

The following actions can be performed on selected devices or connections. To perform these actions, click on the cogwheel icon in the right-hand information panel.

- Manage Device—This option is only available for SNA and partial SNA switches, and only appears when a single device is selected. Selecting this action launches a web management session for the selected switch using the switch management application.
- Explore Device—This option is only available for SNA switches, and only appears when a single device is selected. Selecting this action opens the device explorer for the selected switch.
- Locate Device—This option is only available for SNA switches. Selecting this action will make the physical LEDs of the device start flashing for 5 minutes.
- Explore Connection—This option appears when a single connection is selected. Selecting this action opens the connection explorer for the selected connection.
- Explore Client Group—This option appears when a client group is selected. Selecting this action opens the client explorer, filtered by the type of device in the client group.
- Delete—This option only appears when all the selected devices are offline devices. Selecting this action deletes all the selected devices from the topology map.

Basic Information Block

The Basic Information block displays attributes of the selected single element (see tables below for a full description). The block is not displayed when more than one entity is selected.

Parameter Name	Notes	Example
Product name	From the device description MIB. This field only appears when the device is a switch with partial or full SNA capabilities.	SG500-52P - 52-Port Gigabit PoE Stackable Managed Switch
Host Name	String of maximum 58 characters	RND_1

Parameter Name	Notes	Example
IP Address	Displays the IP address used by SNA to connect to the device. Additional advertised existing addresses (IPv4 and IPv6) can be seen by pressing the icon next to the label.	192.168.1.55 923:a8bc::234
MAC Address	The base MAC address of the device.	00:00:b0:83:1f:ac
Description	Editable field of up to 80 characters. Saved on SNA storage.	
SNA Support	Possible values: • Full support for SNA devices • Partial Support for managed devices • No SNA support for unmanaged devices This parameter appears only for switches.	
The parameters below only appear when View all is clicked. This option is only available if the device is a switch with partial or full SNA capabilities.		
Existing VLANs	A list of the VLANs created on the device. Dashed lines are used to join consecutive VLANs.	1, 6, 13-19, 1054, 2012-2100, 4094
Active Firmware Version	The version number of the active firmware.	2.2.0.53
System Uptime	The time in days, hours, minutes and seconds since the device was booted up	
System Local Time	The local time on the device, in the format of the active language file.	English language file example: 2015-Nov-04 17:17:53
Number of Units	Only appears on stackable devices.	2
PoE Power on unit #/Available PoE Power	Displayed only on PoE-capable devices. Displays the available power used out of the maximum power supply. If the device is a stacked device, a field appears for each PoE-capable unit in the stack with the unit ID. If the device is standalone or a single unit, the label of the field does not mention the unit ID. This means that a maximum of eight fields may appear here.	15.22W/18.0W

The following information is displayed for offline backbone devices under Last Known Information:

Parameter Name	Notes	Example
Product Name	Taken from the device description MIB. This field only appears when the device is a switch with partial or full SNA capabilities.	SG500-52P - 52-Port Gigabit PoE Stackable Managed Switch
Host Name	String of up to 58 characters	RND_1
IP Address	Displays the last IP address used to connect to the device when last seen.	192.168.1.55
MAC Address	The base MAC address of the device	00:00:b0:83:1f:ac
Description	Editable field of a maximum of 80 characters.	
Last seen	The date and time the device was last seen by SNA in the format of the active language file.	English language file example: 2015-Nov-04 17:17:53

The following information is displayed for a client (end point device, such as a PC):

Parameter	Notes	Example
Host Name	String of a maximum of 58 characters	RND_1
IP Address	Shows the IP address used by SNA to connect to the device. Additional advertised addresses (IPv4 and IPv6) can be seen by clicking an icon next to the label	
MAC Address	The base MAC address of the device	00:00:b0:83:1f:ac
Device Type	The type of client device	Phone Host Unknown
Connected Interface	The interface through which the device is reached on the closest switch.	GE1/14
The following parameters only appear when View all is clicked:		
Connection Speed		100M 10G
VLAN Membership	Shows the active VLANs of which the connected interface is a member. Dashes are used to join consecutive VLANs.	1, 6, 13-19, 1054, 2012-2100, 4094
Port Utilization % (Tx/Rx)	Based on the information from the connected port.	80/42
PoE Consumption	Appears only if the client is connected to a PoE port.	8900 mW

The following information is displayed for a client group:

Parameter Name	Notes	Example
Host Name	This is the host name of the client group's parent device. This parameter and all other information on the parent device appears under a Connected to header. String of a maximum of 58 characters	RND_1
IP Address of parent device	Displays the IP address used by SNA to connect to the parent device. Additional advertised addresses (IPv4 and IPv6) can be seen by pressing an icon next to the label.	192.168.1.55 923:a8bc::234
MAC Address of parent device	The base MAC address of the parent device.	00:00:b0:83:1f:ac
Connected Through Cloud	This label appears if the client group is connected to the network through a cloud. The label replaces the host name, IP address and MAC address.	

The following information is displayed for Interfaces:

Parameter Name	Notes	Example
Interface Name		GE1/14 LAG12
Interface Type	Displayed only for ports	Copper-1G
Status	The operational status of the interface.	Up Down Down (ACL)
The parameters below only appear when View all is clicked.		
Interface Description	Uses the value of the interface's ifAlias MIB. String with a maximum of 64 characters.	"WS 28"
Operational Speed		100M 10G
LAG Membership	Displayed only for ports Can be None or the LAG name.	LAG15
Member Ports	Appears only for LAGs and displays a list of the interfaces that are active members in the LAG. Consecutive ranges of interfaces are joined by dashes.	GE1/4, GE1/6, XG2/4-8
VLAN Membership	Shows the active VLANs the interface is a member in. Dashed lines are used to join consecutive VLANs.	1, 6, 13-19,1054, 2012-2100, 4094
Port Utilization % (Tx/Rx)	Appears only for ports.	80/42

Parameter Name	Notes	Example
LAG Type	Appears only for LAGs. Possible values are Standard or LACP.	
Switchboard Mode	Possible values: • Access • Trunk • General • Customer • Private-Host • Private-Promiscuous	
PoE Power Consumption	Appears only for PoE-capable ports	8900 MW
Spanning Tree State	Displays the interface STP-state.	Blocking Forwarding Disabled

Note The Basic Information section is not displayed when selecting clients or layer 2 clouds.

Operations

The topology view displays the elements and their connections in the network. Operations can be performed on elements displayed in the topology view. When you select an element in the topology, it is possible to perform the following actions:

- View information regarding the element
- Configure an element
- Add a device or switch to the Topology View

Elements can be manually added to the topology view. If an SNA-capable device or a managed switch that exists in the network is not detected automatically and displayed in the topology, you can add it manually by performing the following:

Step 1 Click **+Add Switch** in the top right corner of the Topology view. An Enter IP Address text box is displayed.

Step 2 Enter the IP address of the switch to be added. If the device is not detected, feedback is displayed, and the device is added to the Topology view, as an offline unmanaged switch

Explorer

Explorers enable additional information to be displayed for SNA-capable switches, connections and client groups.

Device Explorer

The Device Explorer displays a table view of the ports and existing LAGs in the switch. Every entry in the table has several basic columns, and a small number of additional columns that appear only when the relevant overlay is active.

The following columns are displayed in the Device Explorer table:

- Port/LAG Name — Full interface name.
- Unit ID — Displays only in the port table and for stacked switches.
- Port Type — Displays only in the port table. Physical type of the port.
- Admin Status — The interface's administrative status.
- Operational Status — The interface's operational state. If the interface is suspended, the suspension reason appears in parenthesis.
- LAG Membership — Displays only in the port table. If the port is a member of a LAG, this column shows the LAG ID.
- Port Members — Displays only in the LAG table. Displays a list of the ports that are members in this LAG.
- Description — Description of the interface. Uses the MIB ifAlias.
- When the Link Utilization overlay is selected, the following columns are displayed:
  - Current Speed — Current speed of the interface (10M, 100M, 1G…).
  - Tx Utilization — Tx utilization of the interface as a percentage of the current speed. This column is not displayed for LAGs.
  - Rx Utilization — Rx utilization of the interface as a percentage of the current speed. This column is not displayed for LAGs
- When the PoE overlay is selected, the following columns are displayed:
  - Maximum Power Allocation — Displays only in the port table. Displays the maximum power allocation in MW. If a port does not support PoE, shows N/A.
  - Power Consumption — Appears only in the port table. Displays the actual power consumption in MW. If a port does not support PoE, displays N/A.
- When the VLAN overlay is selected, the following columns are displayed:
  - Switchport Mode — Active VLAN mode of the interface.
  - VLAN Membership — List of the VLANs of which the interface is a member. In trunk mode, displays a U next to the untagged VLAN.
- When the Spanning Tree overlay is selected, the following columns are displayed:

- STP Mode — Active STP mode of the interface.
- Port Role — STP role of the interface.
- Spanning Tree State — STP state of the interface.

Connection Explorer

The Connection Explorer displays additional details about the individual links collected in a single connection between backbone devices, or between an SNA-capable device and a cloud. The explorer displays the interfaces that anchor the connections on either side. Some information on interfaces may only be available if the interface belongs to an SNA-capable device. To display this information double-click on a connection until it becomes thick and then click a second time, to display the following information:

- The interface names of the interfaces on both sides of the link
- The LAG name (if any) on both sides of the link
- The speed of the link

This information about interface names and LAG membership is only available on the sides of the connection that belong to SNA-capable devices. If one of the sides of the connection is not a switch, its ports are not displayed.

Client Explorer

The Client Explorer enables viewing information on selected clients in a client group, such as a group of IP phones. The client explorer is not supported for client groups that are connected to the network through a cloud. The following information is displayed in the Client Explorer table:

- Device ID—Known information about the device: its host name, the IP address it uses to connect to its parent switch and the device's MAC address.
- Device Type—Type of client device.
- Connected port—The port on the parent switch to which this client is connected.
- Link Utilization Overlay Columns
  - Connection speed—Shows the speed of the connection to the parent switch (10M, 100M, 1G).
  - Tx Utilization—The Tx utilization of the device (Rx of the connected port) as a percentage of the current speed.
  - Rx Utilization—The Rx utilization of the device (Tx of the connected port) as a percentage of the current speed.
- PoE Overlay column
  - Power Consumption—Shows the power consumed by the device in MW. If the connected port does not support PoE, shows N/A.
- VLAN Overlay column—Connected VLAN. Shows the VLANs of which the connected port is a member.

The client explorer is not supported for client groups that are connected to the network through a cloud.

Overlays

Overlays are layers of information that can be activated on the topology view to add more information or affect the way the topology is displayed. This can be accomplished, for example, by coloring topology elements in different colors depending on various criteria or by changing the icons that are displayed on topology elements to show detailed data relevant to the selected overlay.

Select the overlay you want to use from a list of available overlays. Only one overlay can be active at a time, therefore selecting an overlay deactivates any other active overlay.

- Link Utilization
- PoE Information
- VLAN Membership
- STP Information

Link Utilization

This overlay adds information to the topology map and explorer screens regarding the current utilization level (for the last 15 seconds) of the connections in the network. The connections and links are color-coded, according to the volume of traffic that flows in them in both directions.

By default, the following are the thresholds and their colors:

- 0%-69% - Normal
- 70%-89% - Yellow
- 90%-100% - Red

Connections between devices in the topology view are colored according to the most heavily utilized individual link in the connection. When viewing the connection explorer, each link shows its own utilization in both directions. The utilization for each direction of a link is calculated by checking the information from both sides, if the link is between SNA-capable devices and using the higher value as the utilization value. When determining the most heavily-utilized link for the aggregated display on the topology map, each direction of a link is considered a separate link.

PoE Information

The PoE overlay displays the power supply and consumption status of the elements in the network. This overlay applies colors to links based on the amount of power provided by the link to power supplying devices based on their remaining power. The overlay also highlights devices requesting power that are not receiving the power requested. The user can select the thresholds where these colors change for each type of data, and the specific colors used for each threshold reached. An icon is added to power-supplying switches, and is colored according to the switches power budget consumption.

- Device supplying 0-80% of its power budget — Normal
- Device supplying 81-95% of its power budget — Yellow
- Device supplying 96-100% of its power budget — Red

Devices receiving power over Ethernet are surrounded by a halo. In the connection explorer, each link transferring power displays an indication of providing power, and the direction of the power flow.

VLAN Membership

The VLAN membership overlay enables viewing of the VLAN memberships of various ports and devices in the network. When activating this overlay, a list of existing VLANs in the network is displayed (listed by VLAN ID). When you select a VLAN, node, which are members in this VLAN, are highlighted.

Links between devices are displayed in one of the following states:

- A link between SNA devices, where neither of the connected interfaces on either device is a member of the VLAN, is unmarked.
- A link between an SNA device and a non-SNA device, whose interface on the SNA device is not in the VLAN, is unmarked.
- A link between SNA devices where the connected interfaces in both devices are members of the VLAN is highlighted as a member of the VLAN.
- A link between an SNA device and a non-SNA device whose interface on the SNA device is a member of the VLAN is highlighted.
- An asymmetric link between SNA devices where one of the connected interfaces is a member of the VLAN and the other one is not is marked in yellow.

The connection between an aggregation of links (LAGs) between devices in the topology map is marked according to the following rules:

- If at least one link is highlighted, the connection is highlighted.
- If at least one link has an asymmetric connection, the connection is yellow.

In the Connection Explorer, every link can be viewed individually. When a link is has an asymmetric configuration, in addition to being colored yellow, the connection explorer displays which side of the link is not a member of the VLAN.

STP Information

This overlay displays the active topology of the network. When this overlay is activated, an indication is added to the spanning tree root device and all connections. This indication highlights the links that are blocked by the common spanning tree.

Tags

Tags are used to identify devices in the Topology view by attributes or by user-defined names. Tags are used to quickly select multiple elements by searching for a specific tag. For example, you can search for all network nodes labelled with the IP Phone tag.

Tags can be built-in or user-defined.

- Built-in tags—Applied automatically to nodes based on information gathered by Discovery protocols.
- User-defined tags—Added manually and assigned to nodes in the topology map.

Built-in Tags

Built in tags are applied automatically to the nodes as they are added to the topology. These tags can be persistent or state-based. As long as the tag applies to the device, it cannot be removed from the device. The following is a list of built-in tags:

Tags	Method for Assigning Tag
SNA	According to SNA internal data
Partial SNA	According to SNA internal data
Offline	According to SNA internal data
Switch	According to advertised data on discovery protocols.
Router	According to advertised data on discovery protocols.
Access Point	According to advertised data on discovery protocols.
IP Phone	According to advertised data on discovery protocols.
PC	According to advertised data on discovery protocols.
Notifications	According to SNA internal data. State based, is displayed if unread notifications exist on the device.
PoE PSE	According to SNA internal data – displayed if a device is capable of supplying power via PoE (even if it doesn't actually supply any power).
PoE PD	According to SNA internal data. This is displayed if a device is capable of receiving power via PoE (even if it does not actually receive any power via PoE).

Operations

The topology view displays the elements and their connections in the network. Operations can be performed on elements displayed in the topology view. When you select an element in the topology, it is possible to perform the following actions:

- View information regarding the element
- Configure an element
- Add a device or switch to the Topology View

Elements can be manually added to the topology view. If an SNA-capable device or a managed switch that exists in the network is not detected automatically and displayed in the topology, you can add it manually by performing the following:

Step 1 Click **+Add Switch** in the top right corner of the Topology view. An Enter IP Address text box is displayed.

Step 2 Enter the IP address of the switch to be added. If the device is not detected, feedback is displayed, and the device is added to the Topology view, as an offline unmanaged switch

User-Defined Tags

You can create new tags and add them manually to selected elements in the topology. To create a new tag perform the following steps:

Step 1 In the Tags section, click **Add Tag Name** and enter a tag name.

Step 2 Click **ADD+**. The tag name is then displayed. The below shows that the tag first_floor has been created.

You may add tags that have the same names as built-in tags. These tags appear similar to user-defined tags and you can remove them at any time. Since these tags are distinct from the built-in tags, it is possible for tags with the same name to appear twice on a single element as long as one of them is user-defined and the other is built-in.

To add a tag to a device, complete the following steps:

Step 3 Select the device.

Step 4 In the Tag section, click **Add Tag Name**. A list of tags is displayed.

Step 5 Select the tag to be applied to the device.

SNA Dashboard

The network dashboard is a separate screen from the topology that displays general information about the status of the network.The dashboard contains the following sections.

Network Overview

This section displays general information about the network. All the information displayed here is provided by the SNA and partial SNA devices on the network.The following information is displayed:

- PoE power supplied by PoE devices on the network – Displayed in Watts
- Current power saved by green Ethernet – Displayed as a percentage and Watts value (for example: 20%; 5 Watts).
- Cumulative power saved by green Ethernet – Displayed as Watts * Hours.
- Projected annual power savings by green Ethernet – Displayed as Watts * Hours.
- Current power saved by power management policy – Displayed as Watts.
- Cumulative power saved by power management policy – Displayed as Watts * Hours.
- Projected annual power savings by power management policy – Displayed as Watts* Hours.

Alerts

This section displays the ten most recent alerts on the network. The alerts are notifications of severity rank 1. These alerts are displayed in a table with the following columns:

- Originating device - This appears only in the aggregated notifications display. The originating device is identified by the strongest available form of identification according to the following priority: Host name > IP address > MAC address.
- Timestamp
- Severity
- Syslog text.

The list can be sorted by device, time or severity and can be filtered by device or severity. By default, the list is sorted by timestamp, with the most recent notification appearing first.

Network Health

This section displays alerts if a health problem is detected on any SNA device in the network. Alerts display the device or connection that they happened in, provide a link to the appropriate device or connection explorer and the nature of the problem.They are displayed for the following events

- A fan fails
- A temperature sensor detects dangerously high temperature.
- PoE is overloaded (a request for PoE cannot be supplied because the budget is surpassed).
- A connection's traffic utilization reaches 70%/90% or higher.
- A device's CPU utilization reaches 96% or higher.

This section does not appear if there are no health problems in the network.

Suspended Interfaces

This section display information on all suspended ports in the network.The following information is displayed for each suspended interface:

- Device ID
- Interface Name
- Suspension Reason (string of up to 20 characters)
- Auto Recovery Status (Enabled/Disabled)
- A button to attempt to re-activate the interface (this button requires the SNA to be in full permission mode).

This section does not appear if there are no suspended interfaces in the network.

Notifications

Notifications are events that occur on the network that may require the system administrator's attention. The notification mechanism uses the SYSLOG feature of SNA switches in the network and displays the notifications on the topology map

Viewing Notifications

When a SYSLOG message is generated by an SNA device, an indication appears for that device on the Topology view.Notifications are derived from the RAM logs of SNA switches, so only SYSLOGs that pass the severity threshold configured for the RAM logs are detected by SNA.The notifications in SNA are separated according to the categories based on their SYSLOG severity level. The color of the notification indicates its severity, as described below:

- Rank 1 (Red): Critical, Alert or Emergency
- Rank 2 (Orange): Warning or Error
- Rank 3 (Blue): Informational or Notice

When an event generating a notification occurs, an indication appears on the relevant SNA device, which displays the number of new notifications on the device and the severity of the most severe notification. In addition, a general notification icon on the application masthead is displayed when there is a notification. These indications are cleared when logging out, and are updated again as events take place while SNA is operational.

Device Authorization Control

Use the Device Authorization Control (DAC) feature to configure a list of authorized client devices in the network. DAC activates 802.1x features on SNA devices in the network and an embedded RADIUS server (RADIUS host server) can be configured on one of the SNA devices. Device authorization is done via MAC authentication

To activate and then access DAC, complete the following steps:

Step 1 Activate DAC.
Step 2 Configure a RADIUS server device and client devices.
Step 3 Add the client devices to the white list.
Step 4 Next, to access DAC, click the options menu in the left-hand side of the masthead.
Step 5 Select **Edit DAC Mode**.

Specify a RADIUS Server and Clients

To specify a RADIUS server and client, complete the following steps:

Step 1 Click **Edit DAC Mode** in the Options menu. The application enters the DAC edit mode.

Step 2 Select one of the SNA devices and click on its menu.

Step 3 Designate it as the RADIUS server for the network by clicking **+ Set as DAC server**.

Step 4 If the device has more than a single IP address, select one of the IP addresses as the one to be used by DAC. The list of addresses indicates whether the IP interface is static or dynamic. You will be warned if selecting a dynamic interface that the address may not be stable. When editing an existing DAC server, the address currently used by its clients is pre-selected.

Step 5 Enter a key string that will be used by the DAC RADIUS server with all its clients on the network.

Step 6 Click **Done** The DAC RADIUS server is highlighted in the Topology view.

Step 7 Stand on the server and then click the menu of the device that you want to add as a client. Click **+Set as client**.

- If a switch is already a client of the DAC RADIUS server the switch is pre-selected.
- If a client is selected, which already has a RADIUS server configured for 802.1x, you will be notified that the proceedings will interrupt the existing RADIUS server operation.
- - If a client is selected, which has a RADIUS server configured for 802.1x in priority 0 an error message is displayed and DAC is not configured on this client.
- Select at least one client for the DAC RADIUS server. If no clients are selected, you will be unable to apply the settings.

Step 8 When a switch is selected as a client, a window with its ports is displayed. Select the ports from the client switch on which to apply 802.1 x authentications. The SNA recommends a list of all edge ports. You can select these recommended ports by clicking on **Select Recommended**.

Step 9 Click **Done**.

Step 10 Click **Apply** in the DAC Edit Mode found in the top menu.

After the DAC is configured, an alert is displayed whenever a new allowlisted device is rejected on the network through a DAC-enabled RADIUS server. You are asked whether to add this device to the allowlist of authorized devices, or send it into a blocklist so that you are not alerted again.

If a rejection event is received from a device that is not a DAC RADIUS server, the message is ignored, and all further messages from this device for the next 20 minutes are ignored. After 20 minutes, SNA checks again if the device is a DAC RADIUS server. If a user is added to the allowlist, the device is added to the DAC group of all DAC servers. When this configuration is saved, you can decide whether to save this setting immediately to the server's startup-configuration (this option is selected by default).

Until a device is added to the allowlist, it is not allowed access to the network.You can view and change the allowlist and blocklists at any time, as long as a DAC RADIUS server is defined and reachable.

When applying the DAC settings, you are presented with a report listing actions that will be applied to the participating devices. After you approve the changes, you can decide if the settings should additionally be copied to the startup configuration file of the configured devices (this option is selected by default). Finally, apply the configurations.

The report displays warnings if some steps of the DAC configuration process are missed, along with the status of the actions as handled by the devices.

The report displays the following fields:

Field	Value	Comments
Device	The device identifiers (Host name, IP address)	
Action	Possible actions for DAC server: • Enable RADIUS server • Disable RADIUS server • Update client list • Create RADIUS server group • Delete RADIUS server group Possible actions for DAC client: • Add RADIUS server connection • Update RADIUS server connection • Remove RADIUS server connection • Update 802.1x settings • Update interface authentication settings • Update interface host and session settings	It is possible (and likely) for multiple actions to appear for each device. Each action can have its own status.
Warnings	Possible warnings for DAC server include: • Selected IP interface is dynamic. Possible warnings for DAC clients include: • Device is already a client of a different RADIUS server. • No ports are selected.	Warnings also contain links to the sections of the DAC where they can be addressed. Changes can be applied when warnings are present.
Status	• Pending • Sucess • Failure	When the status is a failure, the error message is shown for the action.

DAC List Management

After you have added client devices and selected which of their ports are to be authenticated, all unauthenticated devices detected on those ports are added to the List of Unauthenticated Devices.

DAC supports the following lists of devices:

- Allowlist- List of all servers that can be authenticated.

- Blocklist - List of servers that must never be authenticated.

If you want devices and their ports to be authenticated, they must be added to the allowlists. If you do not want them to be authenticated, not action is required - they are added to the blocklist by default.

To add these devices to the allowlist or remove them from the blocklist:

Step 1 Click the Unauthenticated device icon.

Step 2 Select the devices you want to add to the allowlist and click **Add to Allowlist**.

Step 3 Select the devices you want to add to the blocklist and click **Add to Blocklist**.

Step 4 Click **Apply**. Packets entering on the ports on the device are authenticated on the RADIUS server.

Services

Services are configurations that can be activated on multiple SNA-capable devices or interfaces, simultaneously. These are only available for devices with full SNA support or for interfaces for those devices.

Services are selected from the right-hand panel. To apply a service, select one or more devices or interfaces from the Topology view, either manually from the map or by selecting them from the search results.

After a service is selected, a dedicated GUI for the service is displayed. The current settings for the relevant feature from all selected elements are displayed. The specific parameters displayed for each service are described below.

For most services, a GUI page is displayed where specific parameters can be defined for the service. After you enter the parameters in the GUI page, and all possible client side validations are performed on them, the settings are submitted to the selected devices or interfaces. A report then is displayed showing the results of the service as they are received.

If a configuration failed due to a communication error between SNA and the configured device, an option is displayed to retry the configuration. By default, all services copy the running configuration file to the startup configuration file automatically after the configuration is performed

Device-Level Services

The following services are available for switches:

- RADIUS Client Configuration
- DNS Client Configuration
- SYSLOG Server Configuration
- Time Settings Configuration
- File Management
- Power Management Policy (Device Level)
- VLAN Membership (Device Level)

For each of these device-level services, the tickets showing the current configurations of the selected devices show the following identifying information in addition to service specific parameters:

- Device host name
- IP address—If more than one IP address exists for the device, the one used by SNA to access the device is displayed.
- Device model—The alphanumeric string representing the device model. For example: SG350XG-2F10.

RADIUS Client Configuration

This service enables you to configure one or more devices as RADIUS clients by defining the RADIUS server they are using for login.

For every selected device, the current configuration displays the RADIUS server with usage type login or all of the lowest priority configured on it on the right-hand information.If more than one RADIUS server of the lowest priority exists, a single server is displayed, in the following order:

- The first RADIUS server (alphabetically) defined by host name.
- The RADIUS server with the lowest IPv4 address
- The RADIUS server with the lowest IPv6 address

The entry created by the service has a priority of 0 and usage type login. If an entry with the same IP address or host name as the new entry already exists, with priority 0 and usage type 802.1x, the existing entry is updated to usage type all.

Displayed/Editable Parameters

To configure selected devices as clients to a different RADIUS server than the currently-configured RADIUS server, enter the following fields:

- Server Address—IPv4 address or IPv6 address of the RADIUS server.
- Key string—Key string used for the RADIUS server (up to 128 characters).
- Authentication Port—Number of the authentication port.
- Authentication Methods—List of the authentication methods used for each device by the channel currently used on SNA (HTTP or HTTPS). The common values for this parameter are Local or RADIUS, Local. If the current value for a device is any other value, the copy option is not available for this device. When copying settings, the value RADIUS, Local is mapped to the RADIUS Primary Authentication Method radio button.
- Primary Authentication Method—Write-only parameter that appears in the configuration section. It is a selection between two values: Local Database, RADIUS. If RADIUS is selected, the actual value configured for all channels is RADIUS, Local.

DNS Client Configuration

The DNS Client Configuration service enables defining the DNS server that the selected devices use.

Displayed/Editable Parameters

To define a new DNS server, enter its IPv4 or IPv6 address.

SYSLOG Server Configuration

This service enables defining the SYSLOG server used by the selected devices.

For every selected device the SYSLOG server with the lowest index in the SYSLOG table is displayed.If a static entry existed and was displayed, the new entry created by the service replaces the pre-existing entry.

Displayed/Editable Parameters

To define a new SYSLOG server, enter the server's IPv4 or IPv6 address.

Time Settings Configuration

This service allows the time source and the system time of the selected devices to be defined.

Note It is highly recommended to run this service in order to synchronize the time settings between all devices in the network. It is especially advisable when viewing historical statistical information on multiple devices.

The current clock source, with the following options, is displayed:

- Default SNTP servers—Default servers displayed if the clock source is SNTP.
- User-defined SNTP server—Displayed if the clock source is SNTP and the current configuration has one or more non-default SNTP servers. In this case, the upper SNTP server is displayed according to the following priority:
  - First SNTP server (alphabetically) defined by host name.
  - Lowest SNTP server defined by IPv4
  - Lowest SNTP server defined by IPv6
- Local Clock—Displayed if the clock source is local.
- Current time—Display of the current time and time zone offset.

Editable Parameters

To change the clock source select one of the following options:

- Default SNTP Servers—Deletes all configured SNTP servers and re-creates three default servers.
- User Defined SNTP Server—Add the address of the SNTP server by entering either host name, IPv4 or IPv6. When applying the server, all current configured servers are deleted, and the server one is added. Time Zone must be configured with this option.
- Local Clock—Changes the device clock source to local clock. The date, time and time zone must be configured.
- Set Date and Time—Date and time if local clock is configured.
- Time Zone—Time zone offset if a user-defined SNTP server or local time is configured.

File Management

Unlike the services previously mentioned, the File Management service does not change the configuration of the selected devices directly. Instead, it performs an operation on all selected devices. Use this service to download new firmware versions or configuration files to the selected devices or reboot them.

Operations

The following operations are available from the service:

- Download firmware via HTTP - Used to download a new firmware file. In the local file system, browse to the new firmware file and select it. This file is then downloaded to all devices participating in the service. After downloading the new firmware, the device also automatically makes it the active firmware version.
- Download configuration via HTTP - Used to download a new configuration file. In the local file system, browse to the new configuration file and select it. This file is then downloaded to the startup-configuration of all devices participating in the service.
- Reboot - Click **Go** to reboot the devices without performing any other actions.

Power Management Policy (Device Level)

This service enables setting power policies for selected devices. The following parameters will be displayed.

- SNA Power Schedule (active/inactive)
- Power schedule details if active
- Whether time power is active each day, beginning on Monday and ending on Sunday
- Behavior of ports in off-schedule times. The options include:
    - PoE power inactive
    - Data inactive
    - Both PoE power and data inactive
    - Custom—Displayed if an SNA-created schedule is not applied uniformly to all Access ports. Access ports are ports whose VLAN mode is Access.
    - Configured ports—A list of all ports that are bound to the SNA-created schedule

Editable Parameters

You can create a power schedule and apply it to the devices. To perform this action, select the start time and end time of activity for every day of the week and then select one of the following behaviors for off times.

- PoE power inactive
- Data inactive
- PoE power and data inactive (default)

To properly activate the schedule on the devices, at least one port must be selected in each device. You can only select a behavior if at least one PoE device is selected. Otherwise, the schedule can only be created or deleted.

The schedule created by this service uses a reserved name (orch_power_sched). Time ranges with other names are ignored by SNA.When applying the settings, the applied behavior is bound to all selected ports. All ports that are not selected are unbound from the schedule if they were previously bound.

Non-PoE ports are only affected if one of the behaviors, which shut down data is selected. If a selected port is not affected by the selected behavior, a note is added to the success message. This note notifies the user that some ports were not bound because the selected behavior did not apply to them.

Setting up a Power Management Policy

To set up a power management policy, complete the following steps:

Step 1 Select a device in the Topology view.
Step 2 Select the Power Management service in the right-hand information.
Step 3 Click **Select Ports**.
Step 4 Select one or more ports and click **Done**.
Step 5 Click **+Add Schedule Time**.
Step 6 Complete the fields and click **Go**. A power management policy has been defined.

VLAN Membership (Device Level)

This service configures the VLAN membership of interfaces across multiple devices. For every device, the following parameters are displayed:

- Access ports—A list of the ports in access VLAN mode. This list is grouped by the access VLANs the ports belong to. Consecutive ranges of ports are shortened using dashes.
- Trunk ports—A list of the ports in trunk VLAN mode. This list is grouped by the native VLANs the ports belong to. Consecutive ranges of ports are shortened using dashes.

Editable Parameters

When editing the VLAN membership, first select a VLAN to operate on. This VLAN selection offers a selection of all existing VLANs in the network, and an option to create a new VLAN.

After a VLAN is selected, open a port selection panel that is connected to each device's card. In this panel, all ports that are members of the selected VLAN are marked according to their membership type:

- A—For access ports that are untagged members in the VLAN.
- U—For trunk ports that are untagged (native) members in the VLAN.
- "*"—For any other state, whether it's not a member of the VLAN or is a member under a different VLAN mode.

Clicking a port toggles between the A and U states (and the "*" state if the port was originally in that state). Ports that are LAG members display the marking based on their LAG, and when such a port is clicked, all the members of the same LAG toggle with it.

After editing the membership and applying, the VLAN will be created on all devices that will now have ports belonging to it (if that VLAN did not exist in them before).

Interface-Level Services

Some services are relevant to interfaces rather than devices. When activating these services, select one or more interfaces and then select a service from the list of services available.

The following services are available for interfaces:

- Power Management Settings (Port)—PoE priority and applying schedule behavior.
- VLAN Membership (port/LAG) — Switchport type (Access and Trunk), membership for Access and Trunk.

For each of these services, the tickets showing the current configurations for the selected interfaces display the following identifying information in addition to service specific parameters:

- Interface name
- Device host name (of the parent device of the interface)
- IP address (of the parent device of the interface)—If more than one IP address exists for the device, the IP address used by SNA to access the device is displayed.
- Device model (of the parent device of the interface)—The alphanumeric string representing the device model. For example: SG350XG-2F10.

Power Management Settings (Interface Level)

This service configures the Power settings on specific ports. This service can only be run when all selected ports belong to the same device (or stack).

Displayed Parameters

- PoE Administrative Status (Enabled/Disabled)—This parameter only appears for PoE ports.
- Port Power Priority (Low/High/Critical)—This parameter only appears for PoE ports.
- SNA Power Schedule (Applied/Not Applied)—This parameter appears only if the device has a power schedule created by SNA.
- Schedule behavior—This information appears only if the port has an applied SNA-defined power schedule. The possible values are:
    - PoE power inactive
    - Data inactive
    - PoE power and data inactive

If no PoE ports are selected, the schedule can only be applied or removed from the port, and no behavior can be selected. Applying the schedule to the ports has the same behavior as selecting the Data inactive option.

If a combination of PoE and non-PoE ports is selected, when applying the settings to the PoE ports, the option PoE power and data inactive is treated as if it were Data inactive, and the option PoE power inactive is treated as if the schedule was not activated on the non-PoE port.

VLAN Membership (Interface Level)

This service configures the VLAN membership of the selected interfaces.

Displayed/Editable Parameters

- Interface Name (Read-Only)
- Switchport Mode—For display, can be Access, Trunk, General, Customer, Private -Host, Private - Promiscious. When configuring, the user can choose Access or Trunk.
- Access VLAN—Appears only in Access mode. When displayed shows the Access VLAN ID, and when configuring allows selection of the access VLAN.
- Native VLAN (SNA version 2.3)—Appears only in Trunk mode. When displayed it shows the Native VLAN ID, and when configuring allows selection of the native VLAN.

The selection of VLANs is from a list where all present VLANs on the network can be selected. If the VLAN does not exist on a device to which a selected interface belongs, this VLAN will be created as part of the service operation.

The user can also select an option to add a VLAN (1-4094). This VLAN will be added to all switches that have interfaces that were selected for the service.

Interface Settings

This service configures basic interface settings for ports or LAGs.

Display Parameters

- Administrative Status—Up/Down.
- Current Status—Up/Down/Suspended. If the port is suspended, the suspension reason is shown in parenthesis. For example: "Suspended (ACL)".
- Auto Negotiation—Enabled/Disabled
- Administrative Speed—This parameter is only displayed if Auto Negotiation is disabled. The values can be 10M, 100M, 1000M, 2500M, 5G, or 10G.
- Current Speed—10M, 100M, 1000M, 2500M, 5G, or 10G.
- • Administrative Duplex Mode—This parameter is only displayed if Auto Negotiation is disabled. The values can be Half or Full.
- Current Duplex Mode—Half or Full

Editable Parameters

- Administrative Status—Up/Down.
- Auto Negotiation—Enabled/Disabled.
- Speed—This parameter is only available for editing if Auto Negotiation is disabled. The possible values for speed are: 10M, 100M, 1000M, 2500M, 5G, or 10G.
- Duplex Mode—This parameter is only available if Auto Negotiation is disabled and if the selected speed is 10M or 100M.

Saving SNA Settings

All changes made in the SNA system itself (not using services) can be saved. These settings are then available to the next SNA session launched on the network. This saved information is also available the next time you access the network from any SNA-device connected to the same network, and from any browser, as long as you use the same username for the next login.

When saving the settings, SNA attempts to save the changes in all detected online SNA devices (in a special SNA folder on the flash). If no copy of the settings can be saved, you are alerted of the failure

If the save operation failed on any or all of the devices, you can request a report showing the devices on which the settings were not saved. Each device in the report displays its ID and the error that was recorded on it

While operating SNA, if a newer version of the SNA settings is detected on any device in the network, you are alerted that a newer version was detected (including the time it was created and the device it was detected on), and prompted to select the version of settings that SNA should use.

The following settings can be saved:

- Positions of all backbone devices in the network.
- Any client device designated as a backbone device retains this status.
- Any tag manually added to elements in the network.
- Any device manually added to the network.
- A description string for backbone devices.
- The blocklist used by the DAC.

In addition to saving SNA settings to the network, you can also export and import settings to an external file for an additional backup. Importing a file or accepting a newer file that was detected on the network overrides the current SNA settings with the ones from the new file. After the file is imported and the topology is updated to the new parameters, you are prompted to keep the changes or revert back to the previous settings. If you choose to keep the changes, the new settings are saved to all devices in the network. If you choose to revert to the previous settings, the topology returns to the previous settings. If you manually save the settings after importing a new file, the option to revert is no longer available.