Access Network Workflow

Overview

The Access Network workflow in automates the access switch deployment in routed access networks in enterprise branch or campus networks. This includes building and managing access VLAN database, interface template management, and access ports configuration. The Access Network workflow provides complete automation for deploying access networks using Cisco catalyst 4500, 3850, 3650, 2960XR and 2960X series switches. In addition, it also automates the static or dynamic provisioning of access ports based on automatic device detection. The workflow reduces the deployment efforts and time by automatically deploying the applicable Cisco best practice configurations and provides a centralized view of the network for management purpose.

The Access Network workflow automates the following tasks:

- Simultaneous multiple access switch configuration—Allows the administrator to provision multiple access switches simultaneously, thus reducing the network provisioning efforts. Allows automatic access switch detection from a seed device, thus minimizing the efforts to detect all the access switches connected to a distribution switch.
- VLAN Management—Allows to create and maintain a database of access and voice VLANs used in the access layer. This database is used to configure access switches, ensuring uniformity in VLAN names and avoiding VLAN nomenclature/id mismatch errors.
- Provisioning Access Ports—Creates and applies templates and VLANs to automatically provision access ports for:
    - accepting Cisco devices that can be detected dynamically, such as Cisco IP phones, Cisco access points, Cisco video surveillance camera, Cisco TelePresence, and Cisco digital media player.
    - detecting non-Cisco devices that can be detected dynamically based on OUI or MAC address.
    - supporting devices such as laptops that cannot be detected dynamically.
- Deploys applicable Cisco Best Practice configurations, automatically.

Pre-requisites for Using Cisco Access Network Workflow

To successfully use the Cisco Access Network workflow, you must ensure that the following pre-requisites are met for the network devices and system:

- Routed Access network—Ensure that the access switches are connected to the distribution layer via layer 3 interfaces.
- Initial Device Setup—Devices are reachable from with SSH/Telnet and SNMP configured.
- Device On-boarding—Devices are added to Inventory.
- IOS Software—Devices have the recommended software version, see Supported Devices.
- Supported Platforms—Devices must belong the supported product families, see Supported Devices.

Supported Devices

The following table shows the supported switches for Access Network workflow.

Table 1: Supported Switches

Product	SKU Type	Mode	Modules	Minimum Software Version	Minimum Software License
WS-C2960X	Copper / POE	Standalone	-	IOS 15.2.2E	LANbase
WS-C2960X	Copper / POE	FlexStack	-	IOS 15.2.2E	LANbase
WS-C2960XR	Copper / POE	Standalone	-	IOS 15.2.2E	IP Lite
WS-C2960XR	Copper / POE	FlexStack	-	IOS 15.2.2E	IP Lite
WS-C3650	Copper / POE	Standalone	-	IOS-XE 3.7.3	IPBase
WS-C3650	Copper / POE	StackWise	-	IOS-XE 3.7.3	IPBase
WS-C3850	Copper / POE / mGig	Standalone	-	IOS-XE 3.7.3	IPBase
WS-C3850	Copper / POE / mGig	StackWise	-	IOS-XE 3.7.3	IPBase
WS-C45xx-E	Copper / POE / mGig	Standalone	Single and Dual Sup (SUP7E or SUP8E), with 47xx and 46xx series line cards	IOS-XE 3.6.4 and above	IPServices
WS-C45xx-R+E	Copper / POE / mGig	Standalone	Single and Dual Sup (SUP7E or SUP8E), with 47xx and 46xx series line cards	IOS-XE 3.6.4 and above	IPServices

Note Cisco Prime Infrastructure does not support IOS-XE SD-WAN image for any of the devices.

Using Access Network Workflow

To create to an Access Network deployment profile, do the following:

Step 1 Choose Services > Network Services > Access Network.

Step 2 Click New Deployment to create a new deployment profile.

Step 3 Ensure that the pre-requisites mentioned in the Before you Begin page are satisfied and then click Begin.

Step 4 Enter the Deployment Name, Description and click Save.

Step 5 Click Add Devices in the Action Panel and choose the devices you want to configure.

Step 6 Click Add.

The Cisco Best Practice configuration will be automatically added to the new devices.

Step 7 Alternately, you can add the devices by entering the seed device IP address to display the list of CDP neighbors of the seed device.

Step 8 Click Yes in the popup window, if you want to take back up of the device running configuration to the device local storage.

The Activity Log shows the Best Practice configuration job status and the back up job status of the newly added devices. You must wait until the jobs reach Completed status before moving to the Access Management page. If there are some errors in the Activity Log, the device may have some incompatible configurations that cause CLI deployment errors. Go to Administration > Dashboards > Job Dabshoard to see more information about the CLI errors. You can remove the failed devices, correct the errors, and add the device again.

Step 9 (Optional) If you want to remove any device from the Device Group pane, choose the device and click Remove Devices in the Action Panel.

Step 10 Click Next to move to the Access Management page to Add, Remove or Update the interface templates.

Step 11 Click the Add radio button in the Action Panel and do the following:

a) Choose the template type from the drop-down list containing workgroups, custom templates, and built-in templates (endpoints).
b) Enter the Name. The Template Name gets auto-populated based on the entered Name.
c) If you choose custom template, enter the device classification type and the classification value.
d) Choose a VLAN from the available VLANs or enter a new VLAN Name.

   If the VLAN does not exist, the workflow automatically creates a VLAN ID for the entered VLAN name. The VLAN name is expected to be common across switches, but may be associated with different VLAN IDs in different switches.

e) Click Apply.
f) (Optional) If you want to manually enter the VLAN ID when creating a new VLAN, click the VLANs tab in the Action Panel and set the Auto VLAN ID to OFF and enter the VLAN ID in the table.
g) Click Deploy.

Step 12 If you see templates with a red i icon indicating that these templates are missing in some devices or out-of-sync with other devices, choose Update to redeploy these templates to all devices to keep them in sync or choose Remove to remove the unwanted templates.

Step 13 Click Next to move to the Ports Management page to manage port groups, configure and administrate ports.

Step 14 Click the Add radio button and do the following in the Action Panel to create a new port group.

a) Enter the Group Name.
b) Choose the port group type from the drop-down list containing workgroups, custom groups, and built-in groups (endpoints).
c) Set the AutoConf and AutoQoS options to ON or OFF based on the chosen port group type.
d) Click Deploy.

Step 15 Click the Port Config tab in the Action Panel to bind the ports to port groups or configure individual ports.

a) Choose the device ports in the Ports Pane.
b) Click the Group Binding radio button in the Action Panel.
c) Choose the port group from the Group Name drop-down list to add the selected ports to the port group.
d) Click Apply.
e) Click Deploy.
f) Choose the device ports in the Ports Pane and click the Configure Ports radio button.
g) Choose the template type, template name, Data VLAN, AutoConf and Voice VLAN in the Action Panel.
h) Click Apply.
i) Click Deploy.
j) Choose the device ports in the Ports Pane and click the QoS Policy radio button and set the Automatic QoS to ON/OFF as required.

   QoS is not automatically enabled on the ports. If required, you can enable the Automatic QoS in the action panel. While enabling Automatic QoS, do not select the trunk ports, L3 ports or ports with existing QoS policies.

k) Click Apply.
l) Click Deploy.

Step 16 Click the Admin tab in the Action Panel and do the following:

a) Choose the ports in the Ports pane.
b) Click the Up, Down, or Reset radio buttons as required to change the port status.
c) Click Deploy.

Step 17 Click Next to view the configuration summary of the created deployment profile.

Related Topics

Pre-requisites for Using Cisco Access Network Workflow, on page 2
Supported Devices, on page 2