White Paper
Deploying Cisco Meraki Cloud-Managed Access Points Attached to Cisco Software-Defined Access

March 25, 2019
Preface

Obtaining documentation and submitting a service request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What’s New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the *What’s New in Cisco Product Documentation RSS feed*. The RSS feeds are a free service.

Organization

This guide includes the following sections:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>An introduction, overview, and use case for deploying cloud-managed wireless with SD-Access</td>
</tr>
<tr>
<td>Design</td>
<td>Overall network design explanation and scope</td>
</tr>
<tr>
<td>Deployment</td>
<td>Step-by-step deployment examples</td>
</tr>
<tr>
<td>Operation</td>
<td>An explanation of operational considerations</td>
</tr>
</tbody>
</table>

Cisco trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Cisco copyright

© 2019 Cisco Systems, Inc. All rights reserved.
Introduction

This white paper enables technical decision makers to understand the design and deployment of Cisco® Digital Network Architecture (Cisco DNA™) in an enterprise campus environment which includes Cisco Meraki® cloud-managed wireless access points connected to Cisco Software-Defined Access (SD-Access) fabric edge switches, and the interoperability provided.

Overview

Cisco DNA provides a roadmap to digitization and a path to realize immediate benefits of network automation, assurance, and security. Cisco Software-Defined Access (SD-Access) is the Cisco DNA evolution from traditional campus LAN designs to networks that directly implement the intent of an organization. SD-Access is enabled with an application package that runs as part of the Cisco DNA Center™ software for browser-based design, provisioning, policy application, and creation of an intelligent campus network.

Cisco Meraki® cloud-managed wireless access points are part of a portfolio of cloud-managed IT solutions built from the ground up for browser-based cloud management, providing feature rich, scalable, and intuitive centralized management. The Cisco Meraki cloud-managed platform also includes automation, orchestration, analytics, assurance, and embedded security.

Use case

Many organizations have deployed Cisco Meraki cloud-managed wireless on top of a traditional Cisco switching infrastructure for their campus networks (local area networks supporting devices used by the people within a location to connect to information). Those same organizations can gain additional advantages by migrating to SD-Access.

For example, an organization can use the integrated fabric technology to enable a physical network to host one or more logical networks as required to meet the design intent. Additionally, an organization can enhance control of communications, providing software-defined segmentation and policy enforcement based on user identity and group membership. Software-defined segmentation is seamlessly integrated using Cisco TrustSec® technology, providing micro-segmentation using scalable groups within a virtual network.

Using Cisco DNA Center for on-premise automation and provisioning for the traditional switching infrastructure reduces operational expenses, coupled with the advantage of reduced risk with integrated security and improved network performance provided by the assurance and analytics capabilities. Similarly, continuing to use Cisco Meraki cloud management for an existing wireless as a fabric-attached infrastructure continues to reap the benefits realized with cloud-managed wireless.

The following sections of the white paper describe the design, deployment, and operation of a Cisco Meraki cloud-managed wireless network attached to the fabric of a Cisco SD-Access network. Fabric-attached cloud-managed wireless interoperability differs from over-the-top technology, such as centralized Cisco Unified Wireless Networking, in that the data plane traffic terminates into fabric overlays for communication within the fabric instead of being tunneled outside of the fabric. Fabric-attached wireless also differs from fully integrated native SD-Access wireless in that fabric-attached wireless does not send VXLAN-encapsulated frames to the SD-Access fabric edge nodes—the fabric edge nodes encapsulate the fabric-attached wireless data traffic, just as if it were traffic from wired endpoints.
Design

The described design focuses on a subset of SD-Access and cloud-managed wireless options. Complete details for large-scale SD-Access design are found in the Software-Defined Access Design Guide and cloud-managed wireless options are available on the Cisco Meraki High-Density WiFi site.

Use this design as additional information for completing an SD-Access design requiring the attachment of Cisco Meraki APs to the SD-Access fabric. The design assumes that only cloud-managed wireless is used (the SD-Access fabric is not expected to be simultaneously using native SD-Access wireless or centralized Cisco Unified Wireless Network deployments). As required by SD-Access, the switching underlay network is designed as a routed access configuration, without the ability to onboard APs using a common L2 native VLAN across the fabric edge switches. Additionally, a Cisco Identity Services Engine (ISE) included as part of the SD-Access design is used for authentication purposes as part of the expanded wireless design.

The high-level design covers an SD-Access attached, cloud-managed wireless network. The design permits cloud management of the wireless infrastructure from the Cisco Meraki Dashboard, with initial AP onboarding via Cisco DNA Center. Wireless endpoints are transported through the network as if they were wired clients in overlay networks as part of subnets that stretch across Layer 3 boundaries in the underlay network.

Access point connectivity

To maintain separation of AP management communication from wireless endpoint data communication, Cisco Meraki APs use an Ethernet 802.1Q trunk. The APs send untagged frames on the Ethernet trunk to communicate with the cloud, authentication, and other management infrastructure. Wireless endpoint-to-AP communication is associated with a wireless SSID, which is assigned a unique VLAN tag on the Ethernet trunk, maintaining communication separation for the wireless domain connected to the wired domain. Likewise, the tagged wireless communication is separated from the untagged wired management communication.

The Ethernet 802.1Q trunk port from the AP is connected to an Ethernet switch port. The untagged management communication is mapped into a trunk VLAN for AP management. Each VLAN tag on the Ethernet trunk representing a wireless SSID maps to a unique VLAN on the switch for wireless endpoint communication.

SD-Access fabric edge switch connectivity

Organizations deploying cloud-managed wireless with SD-Access connect the APs to Ethernet switches deployed in the SD-Access fabric edge role. When connecting the APs to SD-Access, additional policies are available to be applied to AP communications. Consider applying a simple policy using micro-segmentation by means of scalable group tags (SGTs) to inhibit communication between the IP pool used for AP management and the IP pool used for wireless endpoint communications. Traffic from wireless endpoint SSIDs can be isolated from one another using SGTs applied to IP pools (SSID/VLANS). Additionally, macro-segmentation using VNs (similar to VRFs) can be applied for complete isolation of wireless management and even per-SSID for delivery to a policy enforcement point, such as a firewall.

This design describes mapping the tagged and untagged VLANS from the AP into SD-Access constructs at the fabric edge. Each tagged or untagged VLAN presented by the AP is associated with a VLAN/IP address pool grouping at the fabric edge switch, and all IP address pools are included as part of the same virtual network (VN) overlay. Multiple pools within a VN is an equivalent concept in traditional LANs to VLAN separation within the same VRF using a Layer-3 switch or basic VLAN separation using a Layer-2 switch. Additional macro and micro segmentation is available, though not shown in the design.

The design example creates an IP address pool mapped to the untagged VLAN from the AP, used for AP cloud management. An additional IP address pool is created for each wireless SSID supported on an AP, and the AP maps each SSID to an IP address pool in the fabric.
Design

The VLAN numbers associated with the VN overlays are created during fabric provisioning and cannot be explicitly defined. The arbitrary VLAN number assignment implies that the fabric edge switch native VLAN configuration and the Meraki Dashboard per-SSID VLAN assignment are unavailable and unknown for the design in advance of the deployment. Instead, the provisioned VLAN numbers must be inspected at deployment time and then used for provisioning a consistent end-to-end trunk. Configuration templates within Cisco DNA Center facilitate creation of the provisioning-dependent VLAN parameters.

(Optional)

The SD-Access INFRA_VN is a unique virtual network configuration available at the fabric edge switches. Network infrastructure devices such as native fabric APs use the INFRA_VN to access networks and provisioning resources that are part of the global routing table outside of the SD-Access fabric. It is possible to map the native VLAN for management of an AP to this VN and use it for AP onboarding and Cisco Meraki Dashboard management access. DHCP and DNS services are typically available using the SD-Access INFRA_VN, however, Internet communication services typically are not. This optional design choice using the INFRA_VN has additional configuration and policy design considerations that likely need to be investigated, dependent upon a specific deployment.

ISE for cloud-managed wireless authentication

This design includes Meraki wireless endpoints using ISE as a RADIUS authenticator for endpoints that associate with each SSID.
Deployment

Details of a complete SD-Access deployment are found in the Software-Defined Access Deployment Guide. The described deployment example uses Cisco Meraki MR52 indoor wireless access points deployed across arbitrary fabric edge devices in an SD-Access network, configured to allow Layer 2 roaming across at least three different fabric edge nodes in a single virtual network.

**Note:** The deployment describes one example verified to work in small-scale testing. It is not intended to imply equivalent performance is available in larger deployments using hundreds or thousands of endpoints during flash roaming events. **Additional deployment-specific scale and performance testing is required to understand expected behavior when considering the needs of an organization.**

Deployment prerequisites

The deployment assumes that the following tasks are complete before connecting the cloud-managed wireless devices.

- An SD-Access network is deployed and managed by Cisco DNA Center, as described in the Software-Defined Access Deployment Guide
- Internet connectivity is available to the fabric edge ports and pools assigned for wireless AP SSIDs and management connectivity and all required cloud management ports are available as documented in Firewall Rules for Cloud Connectivity
- DNS and DHCP services are available for all assigned address pools
- The Cisco Meraki MR devices are claimed to your organization within the Meraki Dashboard
- ISE is configured to accept RADIUS authentication connections from the Cisco Meraki MR devices
- ISE is configured to support user authentication for endpoints connecting to MR SSIDs

Product list

The following hardware and software versions were used during testing of this white paper, and many alternatives are available.

- Cisco DNA Center Appliance DN1-HW-APL; Cisco DNA Center 1.2.6; SD-Access package 2.1.24.60052
- Cisco Identity Services Engine VM Version 2.3 Patch 4
- Cisco Catalyst 9400 Series; WS-C9407; Supervisor Engine-1XL; C900-LC-24XS; IOS-XE 16.9.2 (fabric edge)
- Cisco Catalyst 3650 WS-C3650-24PS; IOS-XE 16.9.2 (fabric edge)
- Cisco Catalyst 6807-XL; SUP-6T-XL; C6800-32P10G; IOS 15.5(1)SY1 (fabric control plane)
- Cisco ASR 1002X; IOS-XE 16.9.2 (fabric border)
- Cisco Meraki MR52-HW; Firmware Version MR 25.13
Cisco SD-Access wireless overlay configuration

Validate initial Cisco SD-Access settings to prepare for the attachment of Cisco Meraki MR cloud-managed APs.

1. Using a web browser, login to Cisco DNA Center, navigate to DESIGN>Network Settings> IP Address Pools. Validate that an address pool with free addresses is available for assignment to wireless endpoints.

2. Navigate to DESIGN>Network Settings> IP Address Pools, on the left in the Network Hierarchy pane select the site for deploying the cloud-managed wireless (example: Site-3(HQ)), at the top right of the IP Address Pools pane for the site, click +Reserve IP Pool, fill in the pool information for IP Pool Name, Type, Global IP Pool, CIDR Notation, Gateway IP Address, DHCP Server(s), and DNS Server(s) (example: MR-B, LAN, ONE_SEVEN_TWO (172.16.0.12), 172.16.137.0, /24, 172.16.137.1, 198.51.100.30, 198.51.100.30), and then click Reserve.
3. Repeat the previous step to map each subnet for cloud-managed AP management and wireless SSIDs. In the deployment example for the design, the following are used:
   - MR-MANAGEMENT: 172.16.135.0/24 (used for cloud-managed traffic, VLAN untagged from AP)
   - MR-A: 172.16.136.0/24 (used for the first SSID, VLAN tagged)
   - MR-B: 172.16.137.0/24 (used for a second SSID, VLAN tagged)

4. Navigate to PROVISION>Fabric, under Fabric Domains and Transits, select the appropriate fabric domain (example: SJC), in the left hierarchy navigate to the site for deploying the cloud-managed wireless (example: Site-3(HQ)), click the Host Onboarding tab, under Virtual Networks click the virtual network used for the cloud-managed wireless (example: CAMPUS), leave any existing selections unchanged, select all additional IP pools created for cloud-managed wireless (examples: MR-A, MR-B), and then in the Choose Traffic drop-down, select Data. Do not click Update until the next step.

5. For each IP pool name created for cloud-managed wireless (examples: MR-MANAGEMENT, MR-A, MR-B), copy the text created under the Auth Policy column (examples: 172_16_135_0-CAMPUS, 172_16_136_0-CAMPUS, 172_16_137_0-CAMPUS), paste the text into a text document for use in a subsequent step, click Update, and then click Apply.
Wireless AP host onboarding

6. Within the Host Onboarding tab, under the Select Port Assignment section, select a switch for a cloud-managed AP connection (example: A_9407-01), select all ports used for cloud-managed APs, and then click Assign.

7. In the Port Assignments pop-up, for Connected Device Type choose Server, click Update, click Save, and then click Apply.

8. Repeat the previous two steps for each fabric edge switch where there are AP port assignments.

9. Using a text editing tool, update the previously captured text into a switch IOS-XE CLI command, by prepending the following text:

```
show vlan brief | section
```

Append the first block of captured text to the end of the same line. If there is more than one block of captured text then add logical or separators between the captured blocks so that the resulting command is formatted similarly to the following:

```
show vlan brief | section 172_16_135_0--CAMPUS | 172_16_136_0--CAMPUS | 172_16_137_0--CAMPUS
```
Note: If you choose the option to add Internet access to the INFRA_VN for AP management access, you can find the associated VLAN to use as the trunk native VLAN by executing the following command:

```
show vlan brief | section INFRA_VN
```

10. Within the Command Runner tool, under the Search by Device IP/ Search by Device Name toggle, select one of the switches previously configured for onboarding, copy the command text created in the previous step and paste the command, click Add, and then click Run Command(s).

![Command Runner](image)

The command is executed on the selected switch.

11. Select the submitted command to see the command results. Use a text editor to capture the first number on each resulting line (examples: 1046, 1047, 1057), representing the VLAN associated with each subnet created in the overlay VN for wireless.

![Command Runner Output](image)

Optionally, export the retrieved information.

The pool created for MR- MANAGEMENT (example: 172_16_135_0-CAMPUS) shows the associated VLAN (example: 1057), which is used as the trunk native VLAN. You use this VLAN identification for SD-Access fabric edge provisioning.

Additional VLANs (examples: 1046, 1047) are used on the trunk supporting each additional IP address pool in SD-Access for each wireless SSID, which is configured on the Cisco Meraki MR AP using Meraki cloud management.
Create a template for 802.1q trunk port native VLAN assignment

Use the VLAN identified in the previous step that is associated with the MR-MANAGEMENT to create a template enabling configuration of the native VLAN on the switch trunk port.

12. At the top-right of the Cisco DNA Center dashboard, navigate to Tools > Template Editor.

13. Within the Template Editor tool, click + (plus), Create Project, in the Add New Project slide out supply a Name (example: MR-TRUNK), supply any desired optional fields, and then click Add.

The template editor creates a new project.
14. Within the Template Editor tool, highlight the created project (example: MR-TRUNK), click the gear icon associated with the project, and then click Add Template.

![Template Editor](image1)

15. In the Add New Template slide out leave Regular Template selected, supply a Name (example: Trunk native VLAN), if desired supply optional fields, for Device Type select Switches and Hubs, for Software Type select IOS-XE, and then click Add.

![Add New Template](image2)

The template framework is created.

16. Select and copy the following text for the template:

```
interface $INTERFACE
  switchport trunk native vlan $NVLAN
  switchport mode trunk
end
```
17. **Within the Template Editor**, select the template just created (example: Trunk native VLAN). The editing pane appears. Click within the editing pane, and then right-click and select **Paste** to input the copied text.

![Template Editor](image)

18. In the template editor menu, select **Actions > Save**.

![Template Editor](image)

The template is validated and saved.

19. **At the top**, select **Actions > Commit**, and then in the slide out click **Commit**.

A success message is displayed.

**Use defined template to create a profile for applying 802.1q trunk port native VLAN assignment**

Assign the defined template to a network profile to use with the native VLAN information previously identified to update the cloud-managed wireless switch trunk ports.

20. **In Cisco DNA Center dashboard**, navigate to **DESIGN > Network Profiles**, click **Add Profile**, and then select **Switching**.
21. In the **Add a Network Profile** workflow that appears, click **Add**, in the top-left corner supply a **Profile Name** (example: TRUNK-PROFILE), for **Device Type** and **Template** select the template values previously created (examples: Switches and Hubs, Trunk native VLAN), and then click **Save**.

![Add a Network Profile](image)

The profile is saved.

**Provision fabric edge ports for cloud-managed wireless APs**

22. In Cisco DNA Center dashboard, navigate to **DESIGN > Network Profiles**, within the **Network Profiles** list, in the profile created (example: TRUNK-PROFILE), click **Assign Site**, in the **Add Sites** slide out, in **Choose a site** select applicable sites (example: San Jose/Site-3(HQ), and then click **Save**.

![Assign Site](image)

The saved profile is available at the assigned sites for device provisioning.

23. In Cisco DNA Center dashboard, navigate to **PROVISION > Devices > Inventory**, select relevant switches for provisioning, and then in the **Actions** menu select **Provision**.

![Inventory](image)
24. In the provisioning wizard, for **Assign Site** leave the defaults and click **Next**, at **Configuration** click **Next**, if any notification is displayed acknowledge the notification by clicking **OK**.

25. Under **Devices** select a switch, supply the trunk interface (examples: range gig1/0/5-6, gig1/0/5, gig2/0/5) and the native VLAN discovered previously (example: 1057), repeat for all selected switches, and then click **Next**.

26. At the summary screen click **Deploy**, and then click **Apply**. Provisioning of the devices with the advanced port templates begins. Status messages appear on the screen.

As provisioning completes, the **Provision Status** column for each device changes from **Configuring** to **Success**. Details of the provisioning are viewed by clicking **See Details**.
Verify 802.1q trunk port deployment

Use the Command Runner tool to verify deployed configurations.

27. At the top-right of the Cisco DNA Center dashboard, navigate to Tools > Command Runner.

28. Within the Command Runner tool, under Search by Device IP, select one of the switches previously configured for onboarding, paste a command to verify the configuration (example: show run int gig2/0/5 | in trunk), click Add, click Run Command(s), and then select the submitted command to see the command results.

Configure cloud-managed APs

Cloud-managed APs register with the Cisco Meraki cloud when booting while connected to an SD-Access fabric edge port assigned to an address pool with DHCP, DNS, and Internet services. When registered, cloud-managed APs are available to the assigned organization in the Meraki Dashboard, ready to configure.

29. Connect to the Meraki Dashboard, select the organization and network that the MR devices are assigned to, navigate to Wireless > Access Points. The APs that have connected via the management IP address pool in the SD-Access overlay (example: MR-MANAGEMENT) are displayed.
30. Navigate to **Wireless > SSIDs**. Change the names of the SSIDs used for wireless endpoint communication across the SD-Access overlay (examples: MR-A, MR-B), and then click **Save Changes**.

<table>
<thead>
<tr>
<th>SSIDs</th>
<th>MR-A</th>
<th>MR-B</th>
<th>Unconfigured SSID 3</th>
<th>Unconfigured SSID 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>enabled ▼</td>
<td>enabled ▼</td>
<td>disabled ▼</td>
<td>disabled ▼</td>
</tr>
<tr>
<td>Name</td>
<td>rename</td>
<td>rename</td>
<td>rename</td>
<td>rename</td>
</tr>
<tr>
<td>Access control</td>
<td>edit settings</td>
<td>edit settings</td>
<td>edit settings</td>
<td>edit settings</td>
</tr>
<tr>
<td>Encryption</td>
<td>Open</td>
<td>Open</td>
<td>Open</td>
<td>Open</td>
</tr>
<tr>
<td>Sign-on method</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Bandwidth limit</td>
<td>unlimited</td>
<td>unlimited</td>
<td>unlimited</td>
<td>unlimited</td>
</tr>
<tr>
<td>Client IP assignment</td>
<td>Meraki DHCP</td>
<td>Meraki DHCP</td>
<td>Meraki DHCP</td>
<td>Meraki DHCP</td>
</tr>
<tr>
<td>Clients blocked from using LAN</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Wired clients are part of Wi-Fi network</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>VLAN tag</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>VPN</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

31. Navigate to **Wireless > Access Control**, under **Network access > Association requirements**, select **WPA2-Enterprise**, in the drop-down select **my RADIUS server**.

32. Scroll down to **RADIUS servers**, select **Add a server**, in the boxes that appear add a **Host**, **Port**, and **Secret**, and then at the bottom of the screen click **Save**.

33. Repeat the previous step for any additional ISE servers.
34. In the **RADIUS servers** section next to a RADIUS server that has been defined, select **Test**, in the boxes that appear add a **Username** and **Password**, and then click **Begin test**.

![RADIUS server configuration](image)

All APs should be able to successfully reach ISE.

35. For each additional SSID, within **Wireless > Access Control**, at the top select the additional **SSID**, and repeat the previous RADIUS configuration steps.

![Access control configuration](image)
36. Navigate to **Wireless > Access Control**, select an SSID used for wireless endpoint communication across the SD-Access overlay (example: MR-A), scroll down to **Addressing and traffic**, under **Client IP assignment** select **Bridge mode: Make clients a part of the LAN**, under **VLAN tagging** select **Use VLAN tagging**, under the **VLAN ID** section that appears in the **VLAN ID** box add the VLAN ID associated with the SSID (example: 1046), and then click **Save Changes**.

37. Repeat the previous step for additional SSIDs used (example: MR-B) and VLAN ID (example:1047).

Wireless endpoints are now able to connect to each SSID associated with the Cisco SD-Access overlay.
**Operation**

Please use the feedback form to send comments and suggestions about this guide.