Cisco Platforms and Development Summary

8.8.1

What Did I Learn in this Module?

Understanding the Cisco API Platform

To help with sorting through all of the Cisco developer offerings, DevNet creates Dev Centers for each technology group, and those Dev Centers are a convenient way of grouping technologies together. Cisco Dev Centers include: Unified Communications Manager, Cloud, Collaboration, Data center, Internet of Things(IoT) and edge computing, Networking, Security, Wireless and mobile, and Application developers.

Cisco SDKs

SDK stands for Software Development Kit. Typically an SDK contains a set of software development tools integrated for developing applications for a specific device or system. An SDK can provide simpler authentication methods as well as enabling token refreshes as part of the package. SDKs often help with pagination or rate limiting constraints on responses for a particular API. Cisco provides a wide range of SDKs on different Cisco platforms.

Understanding Network Programmability and Device Models

Model-driven programmability inherits the power of models, matching devices' abilities and services to standardized models, making it easier to configure network devices. A data model is a structured method to describe any object. For example, the personal data on a passport or driver's license can describe a person in an individual way, so those are both "data models". YANG, an acronym for Yet Another Next Generation is "a data modeling language used to model configuration and state data manipulated by the Network Configuration Protocol (NETCONF), NETCONF remote procedure calls, and NETCONF notifications." There are two types of YANG models, open and native. Network Configuration (NETCONF) is a protocol designed to install, manipulate, and delete the configuration of network devices. It is the primary protocol used with YANG data models today. The NETCONF protocol provides a small set of operations to manage device configurations and retrieve device state information. The base protocol provides operations to retrieve, configure, copy, and delete configuration data stores. RESTCONF uses the datastore models and command verbs defined in the Network Configuration Protocol (NETCONF), encapsulated in HTTP messages. RESTCONF is not intended to replace NETCONF, but rather to provide an HTTP interface that follows the REST principles and is compatible with the NETCONF datastore model.

Cisco Network Management

Network automation is used for various common tasks in an organization: Device provisioning, Device software management, Compliance checks, Reporting, Troubleshooting, and Data collection and telemetry. IOS stands for "Internetwork Operating System." IOS was the original operating system for Cisco Systems routers and Cisco network switches. IOS XE is the next-generation programmable platform. In IOS XE the control plane and the data plane are separated. The control plane "controls" the network, meaning it stores the routes, mapping, generally all the "signals" that are needed to run the router or switch. The data plane contains the actual client, user, or application data that needs to go along the network from one device to another.

A Cisco DNA Center is a foundational controller and analytics platform for large and midsize organizations and is at the heart of a Cisco IBN. It provides a single dashboard for network management, network automation, network assurance, monitoring, analytics, and security. Cisco DNA Center provides both a web-based GUI dashboard and the RESTful Intent API used to programmatically access its services and functions. All Intent API methods respond with a JSON-structured content payload. Intent API PUT and POST methods require a JSON request payload. Both POST and PUT requests are handled within the Cisco DNA Center asynchronously.

The Cisco ACI platform is the Cisco solution for SDN. The centralized management system is the APIC, a cluster of controllers. The ACI/MSO modules permit the simple creation of playbook elements to perform inquiry, administration, and management tasks upon an ACI fabric. To simplify application development with ACI, Cisco has developed Cobra, a robust Python library for the APIC REST API. Objects in the Cobra library (SDK) map 1:1 to the objects within the Cisco ACI MIT. Cisco Meraki is a suite of cloud-managed network solutions that enables a single source of management for infrastructure, locations, and devices.

The Meraki cloud uses the physical location of access points to estimate the location of a client. NX-OS is a data center operating system for the Nexus switch. With the Nexus switches running the NX-OS, you can automatically provision Cisco switches in the data center and orchestrate changes much the same way you configure a Linux server.

NSO enables operators to adopt the service configuration solution dynamically, according to changes in the offered service portfolio. It delivers the SDN vision by providing a logically centralized interface to the multi-vendor network. NSO has three components: Model-driven programmable interface (YANG models), Configuration database, and Device and service abstraction layers. An NSO service is a function provided by network devices. Creating, modifying, or deleting the service manipulates the actual configuration of the end devices. Service transactions performed complete logical operations meeting ACID (Atomic, Consistent DB, Isolated, and Durable) transaction properties.

SD-WAN supports third-party API integration, allowing for simplicity, customization, and automation in day-to-day operations. Cisco SD-WAN includes the common routing protocols used for all enterprise SD-WAN deployments, such as BGP, OSPF, VRRP, and IPv6.

Cisco Compute Management

The Cisco Unified Computing System (UCS), along with its software and SaaS adjuncts, provides a complete physical and logical plant for compute, networking, and storage in the modern datacenter.

Cisco UCS Manager runs on the primary fabric interconnect and is assigned a virtual IP address (VIP), with failover capability to the subordinate fabric interconnect. The Cisco UCS Manager management requests from the GUI or CLI are encoded in XML. All XML requests to Cisco UCS are asynchronous and terminate on the active Cisco UCS Manager. Cisco UCS Manager mediates all communication within the system; no direct user access to the Cisco UCS components is required.

Cisco UCS Manager servers are either blades that reside in chassis (B-Series Servers) or rack-mounted (C-Series servers). Both are connected to a redundant pair of switches are called UCS Fabric Interconnects (FIs).

Cisco UCS Managed Objects are XML representations of a physical and logical entities in the UCS system. Cisco UCS API documentation is typically referred to as the UCS Object Model documentation. The Object Model documentation is available with the UCS Platform Emulator or online. Every UCS object class and method is listed in the documentation along with UCS types, events, faults, errors, and Syslog messages.

UCS PowerTool is a library of PowerShell Cmdlets that enable the management of UCS environments from Microsoft Operating Systems, via the UCS XML API.

Cisco UCS Director extends the unification of computing and networking layers through Cisco UCS to provide visibility and management of data center infrastructure components. You can use Cisco UCS Director to configure, administer, and monitor supported Cisco and non-Cisco components. When you enable the developer menu, Cisco UCS Director GUI provides a developer menu option for developers to access the report metadata and REST API Browser.

Cisco Intersight is a Software as a Service (SaaS) systems management platform capable of managing infrastructure at the edge and remote locations as well as in the data center. When using the service, you can scale infrastructure up or down as needs increase or decrease. Because it provides a REST API to access the MIM, you can manage the infrastructure as code. The Intersight API is consistently available with a cloud-based management model.

Cisco Collaboration Platforms

Cisco's suite of on-premise and cloud-based collaboration solutions includes Unified Communications Manager, Contact Center, Finesse, and Webex. Cisco Unified Communications Manager is also known as Unified CM, CUCM or CallManager. The primary function of Unified CM is to manage phone users, IP phones, directory numbers, and to connect and manage calls to the desired destinations.

AXL is an XML/SOAP-based interface that provides a mechanism for inserting, retrieving, updating, and removing data from the Unified Communication configuration database. The AXL API is for administration and configuration.

UDS is a REST-based API that provides a mechanism for inserting, retrieving, updating and removing data from the Unified Communication configuration database. The UDS API is designed for end users to configure settings.

Finesse is Cisco's browser-based contact center agent and supervisor desktop. Finesse has REST APIs and JavaScript APIs that can be used to build fully custom agent desktops, integrate contact center functionality into applications, and integrate applications into the Finesse agent and supervisor desktop. This integration can be accomplished in the form of OpenSocial gadgets.

Cisco Webex Teams is an online collaboration solution to connect people and teams through chat, voice, and video. With the Webex Teams app, you gain access to secure virtual work spaces. You also use messaging and file sharing with third-party app integrations. Webex Teams enables you to use a single app to contain content and information for team collaboration. Teams also integrates with Cisco Webex devices. Information remains safe and secure with advanced security and compliance built-in. Cisco Webex Devices provide access to all of Webex's features. Webex Boards, Room Devices, and Desk Devices enable collaboration through video, calling, and programmability.

Cisco Security Platforms

Cisco provides a large portfolio of security technologies and product families which are configurable and manageable via APIs:

- **Advanced Malware Protection (AMP) for Endpoints** - AMP for Endpoints provides API access to automate security workflows and includes advanced sandboxing capabilities to inspect any file that looks like malware in a safe and isolated way. AMP works with Windows, Mac, Linux, Android, and iOS devices through public or private cloud deployments.
- **Cisco Firepower Management Center (FMC)** - FMC is a central management console for the Firepower Threat Defense (FTD) Next-Generation Firewall. This console can configure all aspects of your FTD including key features like access control rules and policy object configuration, such as network objects. FMC provides a central configuration database enabling efficient sharing of objects and policies between devices. It provides a REST API to configure a subset of its functionality.
- **Cisco Firepower Threat Defense (FTD)** - FTD configuration with Firepower Device Manager also provides protective services including track, backup, and protect CA Certificates; manage, backup, encrypt, and protect private keys; IKE key management; and ACLs to select traffic for services.
- **Cisco Identity Services Engine (ISE)** - ISE provides a rule-based engine for enabling policy-based network access to users and devices. It enables you to enforce compliance and streamline user network access operations. With the ISE APIs, you can automate threat containment when a threat is detected. It integrates with existing identity deployments.
- **Cisco Threat Grid** - Threat Grid is a malware analysis platform that combines static and dynamic malware analysis with threat intelligence from global sources. You can add a Threat Grid appliance to your network, or use the Threat Grid service in the cloud. It can also be integrated into other security technologies such as AMP.
- **Cisco Umbrella** - Umbrella uses DNS to enforce security on the network. You configure your DNS to direct traffic to Umbrella, and Umbrella applies security settings on their global domain name list based on your organization's policies.

8.8.2

Packet Tracer - Compare using CLI and an SDN Controller to Manage a Network

In this Packet Tracer activity, you will compare the differences between managing a network from the command line interface (CLI) and using a software-defined networking (SDN) controller to manage the network.

You will complete these objectives:

- Part 1: Explore the Network Topology
- Part 2: Use the CLI to Gather Information
- Part 3: Configure an SDN Controller
- Part 4: Use an SDN Controller to Discover a Topology
- Part 5: Use an SDN Controller to Gather Information
- Part 6: Use an SDN Controller to Configure Network Settings

Compare using CLI and an SDN Controller to Mana...

Compare using CLI and an SDN Controller to Mana...

8.8.3

Packet Tracer – Implement REST APIs with an SDN Controller

In this Packet Tracer activity, you will use the Packet Tracer Network Controller and associated API documentation to send REST requests from Postman and from Visual Studio Code (VS Code). Packet Tracer also supports a Python coding environment. Therefore, in the final Part of this activity, you will send REST requests from within Packet Tracer

You will complete these objectives:

- Part 1: Launch the DEVASC VM
- Part 2: Verify External Connectivity to Packet Tracer
- Part 3: Request an Authentication Token with Postman
- Part 4: Send REST Requests with Postman
- Part 5: Send REST Requests with VS Code
- Part 6: Send REST Requests Inside Packet Tracer

Implement REST APIs with an SDN Controller

Implement REST APIs with an SDN Controller

8.8.4

Module 8: Cisco Platforms and Development Quiz

1. What is a characteristic of the Yet Another Next Generation (YANG) data model?

⚠ Topic 8.3.0 – YANG models use a tree structure. Within that structure, the models are similar in format to XML and are constructed in modules. These modules are hierarchical in nature and contain all the different data and types that make up a YANG device model.

- ◯ It uses a list structure.
- ◯ It uses the JSON data format.

- ◯ It uses a tree structure.
- ◯ It uses a MIBs structure.

2. Which two application-specific media types can be used for RESTCONF to identify a YANG construct? (Choose two.)

⚠ Topic 8.3.0 - According to RFC 8040 11.3. Media Types, there are two types, application/yang-data+xml and application/yang-data+json. “This document defines media types for XML and JSON serialization of YANG data. Other documents MAY define other media types for different serializations of YANG data.”

- ☐ application/yang+xml
- ☐ application/yang+json
- ☐ application/yang-data+xml
- ☐ application/yang-data+json
- ☐ application/yang+json+xml

3. What is the name of the Cisco SD-WAN dashboard?

⚠ Topic 8.4.0 - The vManage dashboard provides a visual window into the network to configure and manage SD-WAN network devices.

- ◯ vEdge
- ◯ vManage
- ◯ vBond
- ◯ vSmart

4. What is Cisco Finesse?

⚠ Topic 8.6.0 - Cisco Finesse is a contact center agent and supervisor desktop that is browser-based and comes with many APIs.

- ◯ a browser-based contact center agent and supervisor desktop
- ◯ an easy-to-use collaboration solution that keeps individuals and teams connected anytime and anywhere
- ◯ a network management and analytics platform for Cisco Digital Network Architecture
- ◯ an application to manage phone users, phones, directory numbers, and to connect and manage calls to the desired destinations

5. Which Software as a Service (SaaS) management platform offers API keys for remote or service access?

⚠ Topic 8.5.0 - Cisco Intersight is a Software as a Service (SaaS) systems management platform capable of managing infrastructure at the edge and remote locations as well as in the data center. There are a couple of ways to gain access to the Intersight API:
- Web browser as an Intersight API REST Client
- API keys for remote or service access

A developer can create API keys for the Intersight account for remote access through SDKs or other programming environments.

- ◯ Cisco Intersight
- ◯ APIC

6. Which Cisco SDK is primarily a call widget that is embedded in an iframe within another web page for Cisco UCS application?

⚠ Topic 8.2.0 - The Cisco Jabber Guest SDK for Web is primarily a call widget that is embedded in an iframe within another web page. The other piece, which is optional, is a small amount of JavaScript code in the hosting page to handle optional communication between the page and the widget.

- ◯ Jabber Guest SDK for Web
- ◯ Jabber Web SDK
- ◯ Jabber Guest SDK for iOS
- ◯ Jabber Guest SDK for Android

7. A developer is using a REST API to develop an application to communicate with a Webex Teams server. What is the default maximum number of items that can be returned by the Webex Teams API prior to using pagination?

⚠ Topic 8.6.0 - The Webex Teams API returns up to 100 items per page by default.

- ◯ 150
- ◯ 100
- ◯ 50
- ◯ 25

8.

```
x-ratelimit-limit: 3000
x-ratelimit-reset: 3588
x-ratelimit-remaining: 2980
```

Refer to the exhibit. A network administrator is developing an application that communicates with Cisco AMP using an AMP API. A response from an AMP service shows the API rate limits information. What is the unit of value indicated under the item x-ratelimit-limit?

⚠ Topic 8.7.0 - Three X- headers provide information about rate limiting with the AMP for Endpoints API:
- **X-Rate-Limit-Limit:** Number of total allowed requests in the current period
- **X-Rate-Limit-Remaining:** Number of requests left before reaching the limit
- **X-Rate-Limit-Reset:** Number of seconds before the limit is reset

- ◯ requests
- ◯ responses
- ◯ seconds
- ◯ bytes

9. What is the default TCP port assigned for NETCONF over SSH?

⚠ Topic 8.3.0 - NETCONF uses SSH as a transport. The default NETCONF SSH port is 830.

- ◯ 22
- ◯ 1080
- ◯ 443
- ◯ 830

10. Where can a corporate developer access the API Explorer with the Firepower Threat Defense API?

⚠ Topic 8.7.0 - A developer can access the Firepower Management Center REST API explorer on the device itself, at the URL **https://***<management_center_IP_or_name>*:*<https_port>***/api/api-explorer**. The Firepower Threat Defense REST API also has an API "Try it out" capability hosted on the FTD device.

- ◯ the domain name of the company
- ◯ the URL address of the device itself
- ◯ the local computer of the developer
- ◯ on the DevNet web site

Check Show Me

Reset

8.7
Cisco Security Platforms

8.9
Prepare for Your Exam and Launch Your C...