cisco The bridge to possible

Everyday Wireless Operational Headaches

Cured using Programmability!

Jeremy Cohoe, Technical Marketing Engineering
@jeremycohoe

cisco Live!

BRKEWN-2730

Cisco Webex App

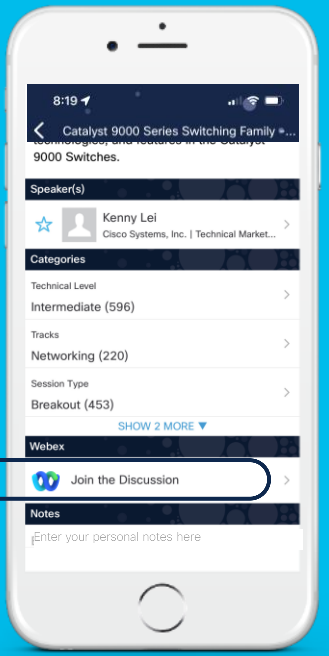
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated
until February 24, 2023.



8:19

Catalyst 9000 Series Switching Family •...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

This session provides an overview of the programmability and automation features that are supported on the Cisco IOS XE Catalyst 9800 platforms.

An overview of the YANG based API's and the associated YANG Suite tooling will be used extensively throughout this session, in addition to gRPC and gNMI.

The Model Driven Telemetry capabilities will also be discussed and the example Docker container for collection and visualization will be demonstrated as well as example dashboards from Grafana for Client and AP visibility.

Let's not forget Guest Shell, EEM, the Python and NETCONF API, and other innovations around Zero Touch Provisioning that enable WLCs to be deployed, managed, and configured with ease at scale.

Agenda

1. Introduction to WLC API P&A
2. YANG, YANG Suite, YANG Tooling
3. Model Driven Telemetry, TIG_MDT, Dashboards
4. On-Box Automation, ZTP, EEM, Python/NETCONF API
5. Conclusion and Resources

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

FYI

About Jeremy WxT/jcohoe@cisco.com

- From Vancouver, BC, Canada
- Amateur Radio Operator, VA7NSA
- Canadian Forces Army – Signals Operator – 4 yrs
- UBC – Wireless Infrastructure – 7 yrs
- Cisco – Enterprise Networks - 5 yrs

aws certified Cloud Practitioner

DEFCON

CISSP®

UBC

Cisco’s Next-gen Wireless Stack

Enabling next-generation mobility powered for Wi-Fi 6

Cisco Catalyst 9800
Wireless Controllers

Cisco Catalyst 9100
Access Points

Managed by

Cisco DNA Center

Translate business intent into network policy
and capture actionable insights

Digitized by

DNA SPACES

Cisco DNA Spaces

Digitize people, spaces and things

Resilient | Secure | Intelligent

Cisco New Wi-Fi 6E Portfolio

MR and C series APs are not convertible

One Product – Two personas

CW9162

- 2x2 + 2x2 + 2x2
- 2.5 Gbps mGig
- Power Options: PoE, DC Power
- Scanning Radio
- IoT ready + Bluetooth 5.x
- Standard Bracket

CW9164

- 2x2, 4x4, 4x4
- 2.5 Gbps mGig
- Power Options: PoE, DC Power
- Scanning Radio
- IoT Ready + Bluetooth 5.x
- Standard Bracket

CW9166

- 4x4 + 4x4, 4x4 (XOR 5/6)
- 5 Gbps mGig
- Power Options: PoE, DC Power
- IoT ready + Bluetooth 5.x
- Scanning Radio
- Environmental Sensor
- Common XOR Architecture
- Standard Bracket

MR57

- 4x4 + 4x4, 4x4 (XOR 5/6)
- Dual 5 Gbps mGig with failover
- Power Options: PoE, DC Power
- IoT ready + Bluetooth 5.x
- Scanning Radio
- XOR Architecture (High/Low band)
- Standard Bracket

C9136

- 4x4 + 8x8 + 4x4 or 4x4+4x4+4x4+4x4
- Dual 5 Gbps mGig with failover
- Power Options: PoE, DC Power
- IoT ready + Bluetooth 5.x
- Scanning Radio
- Environmental Sensor
- XOR Architecture (macro/meso)
- Standard Bracket

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

WLC API
IOS XE
Programmability
& Automation

Cisco IOS XE Programmability & Automation Lifecycle

Pre-boot Execution Environment (iPXE)

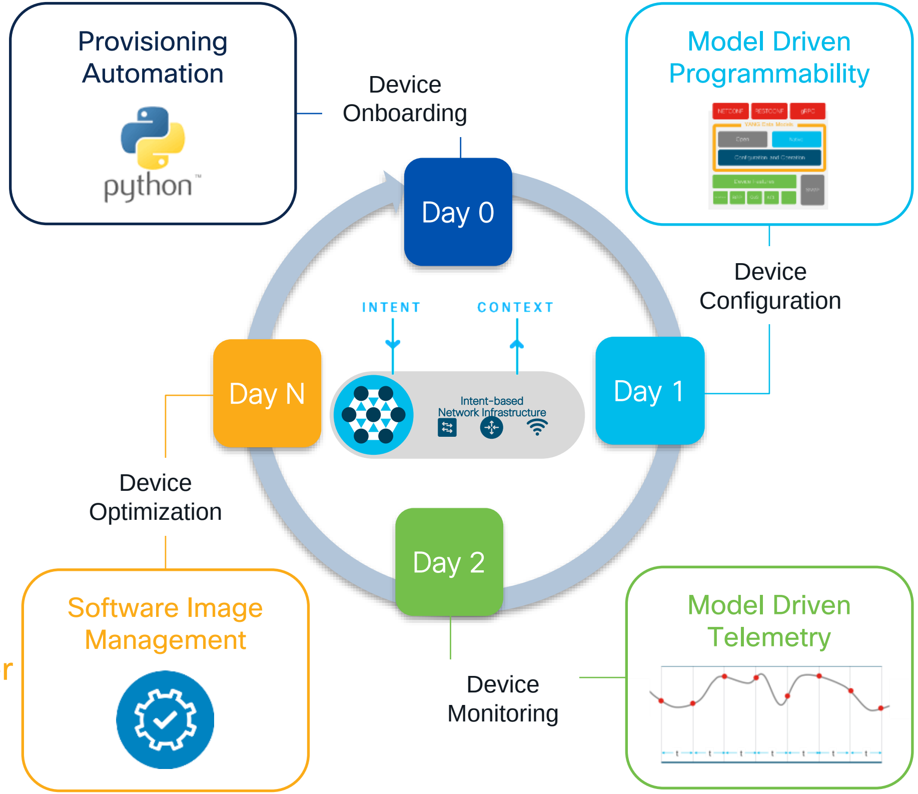
Zero Touch Provisioning

VM Automation

Network Configuration Protocol (NETCONF), RESTCONF, gNMI

YANG Data Models, OpenConfig, and YANG Suite tooling

Terraform, Ansible, pyATS



gNOI cert/os/reset proto

Guest Shell + NETCONF

CentOS 8 Python 3

Application Hosting with Docker

CLI to XML

TIG_MDT container + examples

YANG On-Change support

gRPC Dial-Out + DNS + TLS

gNMI/NETCONF Dial-In

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless feature support matrix

Platform x feature	EWC	C9800-CL	C9800-L	C9800-40/80
ZTP / Guest Shell	N/A	N/A	17.8 17.7* (data port only)	17.3.2a
NETCONF	16.12	16.10	16.12	16.10
RESTCONF	16.12	16.11	16.12	16.11
gNMI	N/A	17.8	Enabled	17.8
gNOI cert.proto	N/A	Enabled	Enabled	Enabled
gNOI factory reset	N/A	N/A	N/A	17.7.1
NETCONF Dial-In MDT	16.12 *	Enabled	Enabled	Enabled
gRPC Dial-Out MDT	N/A	Enabled	Enabled	17.1
gNMI Dial-In MDT	N/A	Enabled	Enabled	Enabled

N/A, Not Available	Enabled, not TAC or BU supported feature	Supported since release 17.11.1

* NETCONF EWC MDT @ https://www.cisco.com/c/en/us/td/docs/wireless/controller/ewc/16-12/config-guide/ewc_cg_16_12/network_monitoring.html
Confirmed accurate per https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/1710/b_1710_programmability_cg.html

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Programmable Interfaces

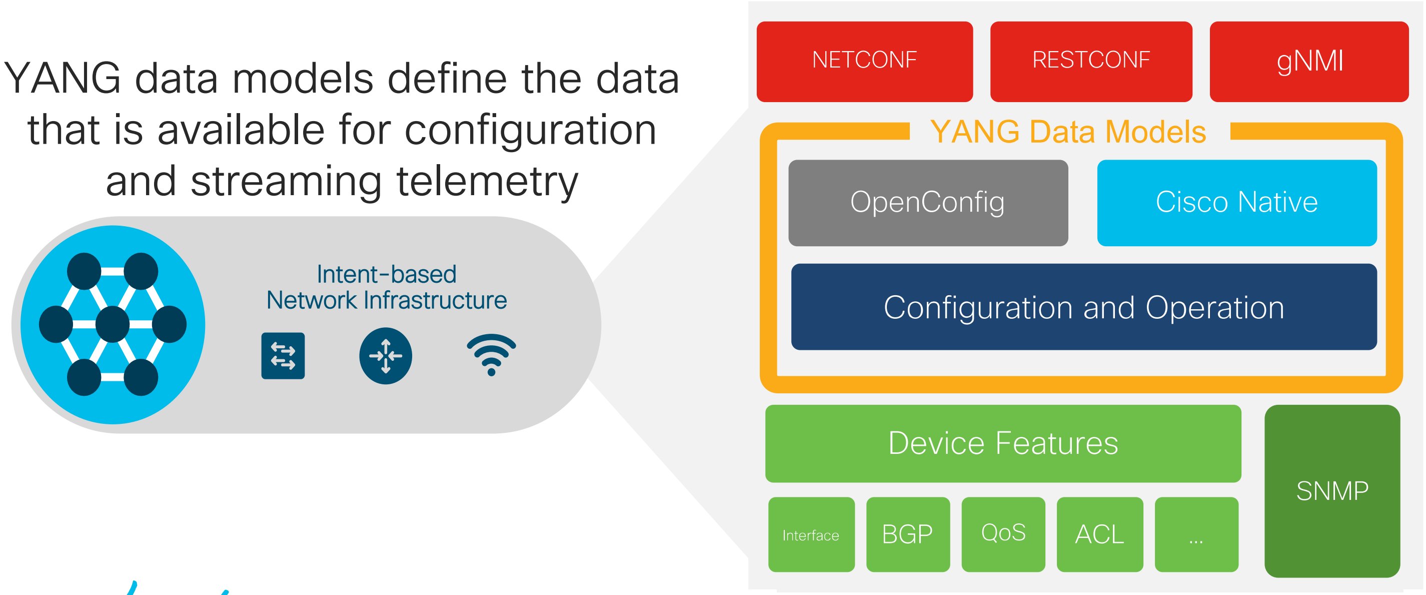
CLI

SNMP

WebUI

The NETCONF, RETCONF and gNMI are programmatic interfaces that provide additional methods for interfacing with the IOS XE device – Just like the CLI, SNMP, and WebUI is used for configuration changes and operational metrics so can the programmatic interfaces of NETCONF, RESTCONF and gNMI

YANG data models define the data that is available for configuration and streaming telemetry



IETF

OPENCONFIG

IEEE

CISCO

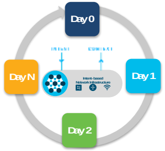
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Model Driven Programmability Interface Comparison

Network architecture, security posture and policy, YANG data modules, tools and language preferences are some considerations when leveraging the various MDP interfaces

	NETCONF	RESTCONF	gNMI
Minimum IOS XE Version	16.6	16.7	16.8
Recommended Version	17.6	17.6	17.7
Default Port	830	443	9339
Operations	<get>,<get-config>,<edit-config>,<establish-subscription>	GET, POST, PUT, PATCH, DELETE	GET, SET, SUBSCRIBE
Encoding	XML	XML or JSON	RFC7951 JSON_IETF
Security	SSH + PKI certificate or password	HTTPS user/pass	TLS certificate with user authentication
Transport Protocol	SSH	HTTPS	HTTP/2
Tooling	YANG Suite, ncclient, Netconf-console	YANG Suite*, Postman, python	YANG Suite*, gnmic, gnmi_cli
Content	YANG	YANG	YANG + Protobuf

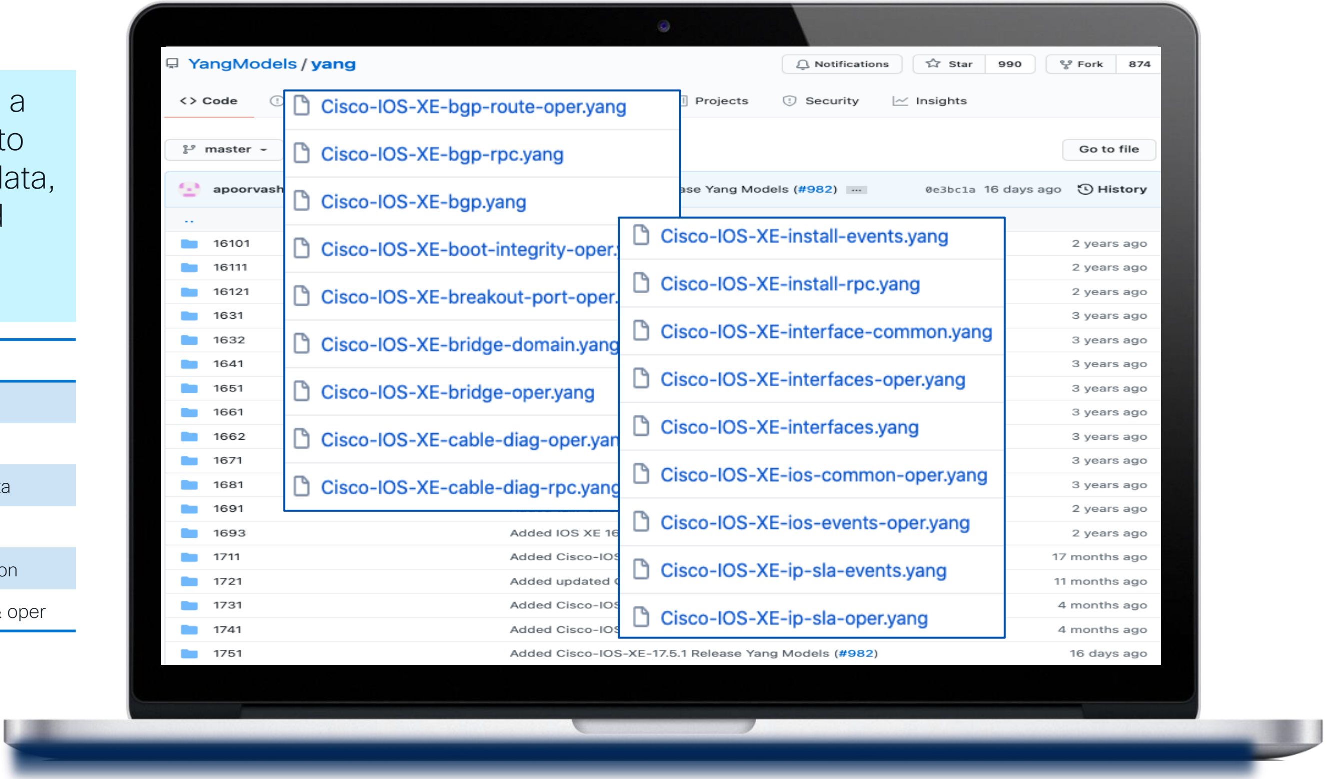
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public



IOS XE - YANG Model Coverage on GitHub

RFC7950 states that “YANG is a data modeling language used to model configuration data, state data, Remote Procedure Calls, and notifications for network management protocols”

YANG module name.yang	Description
Cisco-IOS-XE-native	running-config
Cisco-IOS-XE-{feature}-cfg	Feature configuration
Cisco-IOS-XE-{feature}-oper	Feature operational data
Cisco-IOS-XE-{feature}-rpc	Actions
Cisco-evpn-service	EVPN service abstraction
OpenConfig-{feature}	abstraction for config & oper



apoorvash … ase Yang Models (#982) … 0e3bc1a 16 days ago

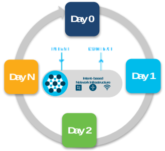
..		
16101		2 years ago
16111		2 years ago
16121		2 years ago
1631		3 years ago
1632		3 years ago
1641		3 years ago
1651		3 years ago
1661		3 years ago
1662		3 years ago
1671		3 years ago
1681		3 years ago
1691		2 years ago
1693	Added IOS XE 16	2 years ago
1711	Added Cisco-IOS	17 months ago
1721	Added updated	11 months ago
1731	Added Cisco-IOS	4 months ago
1741	Added Cisco-IOS	4 months ago
1751	Added Cisco-IOS-XE-17.5.1 Release Yang Models (#982)	16 days ago

- Cisco-IOS-XE-bgp-route-oper.yang
- Cisco-IOS-XE-bgp-rpc.yang
- Cisco-IOS-XE-bgp.yang
- Cisco-IOS-XE-boot-integrity-oper.
- Cisco-IOS-XE-breakout-port-oper.
- Cisco-IOS-XE-bridge-domain.yang
- Cisco-IOS-XE-bridge-oper.yang
- Cisco-IOS-XE-cable-diag-oper.yan
- Cisco-IOS-XE-cable-diag-rpc.yang

- Cisco-IOS-XE-install-events.yang
- Cisco-IOS-XE-install-rpc.yang
- Cisco-IOS-XE-interface-common.yang
- Cisco-IOS-XE-interfaces-oper.yang
- Cisco-IOS-XE-interfaces.yang
- Cisco-IOS-XE-ios-common-oper.yang
- Cisco-IOS-XE-ios-events-oper.yang
- Cisco-IOS-XE-ip-sla-events.yang
- Cisco-IOS-XE-ip-sla-oper.yang

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe

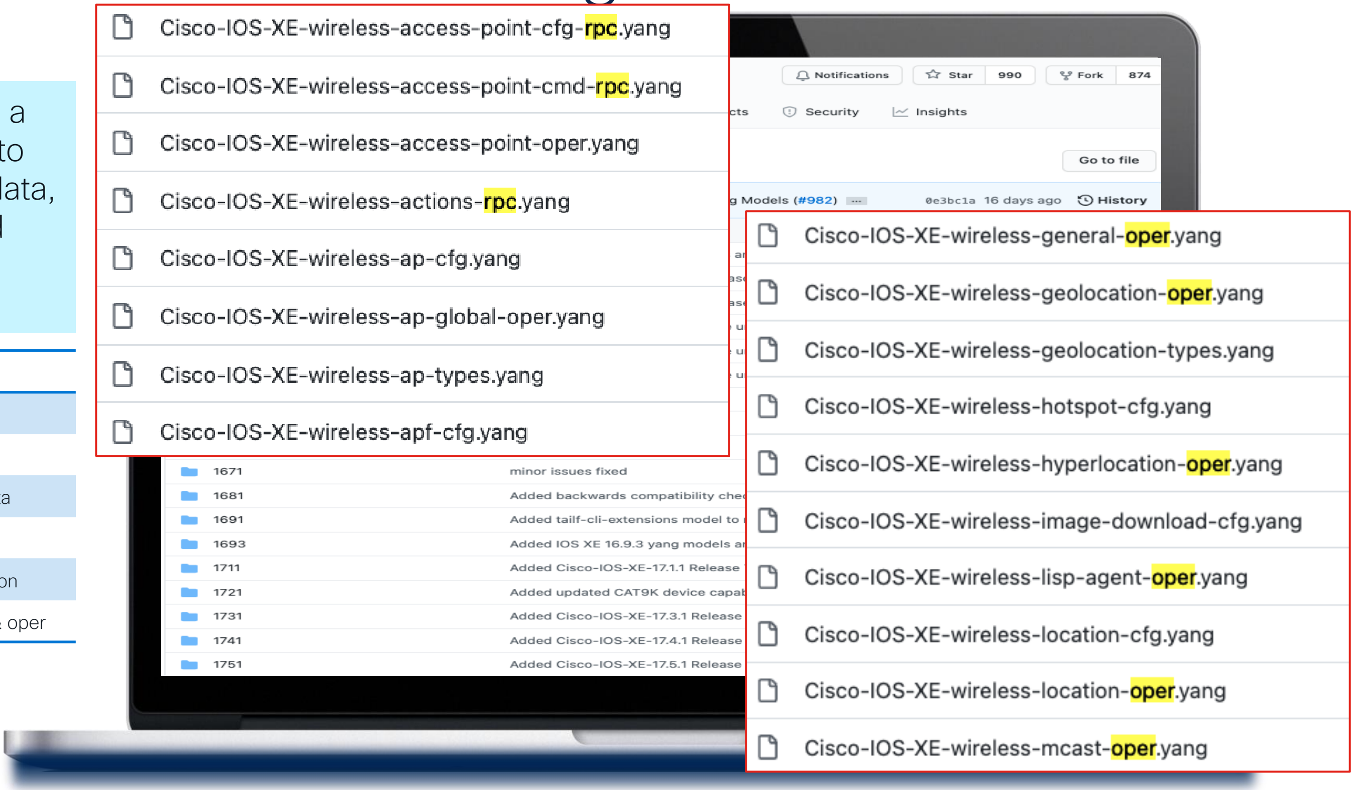
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public



IOS XE - YANG Model Coverage on GitHub

RFC7950 states that “YANG is a data modeling language used to model configuration data, state data, Remote Procedure Calls, and notifications for network management protocols”

YANG module name.yang	Description
Cisco-IOS-XE-native	running-config
Cisco-IOS-XE-{feature}-cfg	Feature configuration
Cisco-IOS-XE-{feature}-oper	Feature operational data
Cisco-IOS-XE-{feature}-rpc	Actions
Cisco-evpn-service	EVPN service abstraction
OpenConfig-{feature}	abstraction for config & oper



- Cisco-IOS-XE-wireless-access-point-cfg-rpc.yang
- Cisco-IOS-XE-wireless-access-point-cmd-rpc.yang
- Cisco-IOS-XE-wireless-access-point-oper.yang
- Cisco-IOS-XE-wireless-actions-rpc.yang
- Cisco-IOS-XE-wireless-ap-cfg.yang
- Cisco-IOS-XE-wireless-ap-global-oper.yang
- Cisco-IOS-XE-wireless-ap-types.yang
- Cisco-IOS-XE-wireless-apf-cfg.yang

1671	minor issues fixed
1681	Added backwards compatibility chec
1691	Added tailf-cli-extensions model to
1693	Added IOS XE 16.9.3 yang models ar
1711	Added Cisco-IOS-XE-17.1.1 Release
1721	Added updated CAT9K device capab
1731	Added Cisco-IOS-XE-17.3.1 Release
1741	Added Cisco-IOS-XE-17.4.1 Release
1751	Added Cisco-IOS-XE-17.5.1 Release

- Cisco-IOS-XE-wireless-general-oper.yang
- Cisco-IOS-XE-wireless-geolocation-oper.yang
- Cisco-IOS-XE-wireless-geolocation-types.yang
- Cisco-IOS-XE-wireless-hotspot-cfg.yang
- Cisco-IOS-XE-wireless-hyperlocation-oper.yang
- Cisco-IOS-XE-wireless-image-download-cfg.yang
- Cisco-IOS-XE-wireless-lisp-agent-oper.yang
- Cisco-IOS-XE-wireless-location-cfg.yang
- Cisco-IOS-XE-wireless-location-oper.yang
- Cisco-IOS-XE-wireless-mcast-oper.yang

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Provisioning Automation

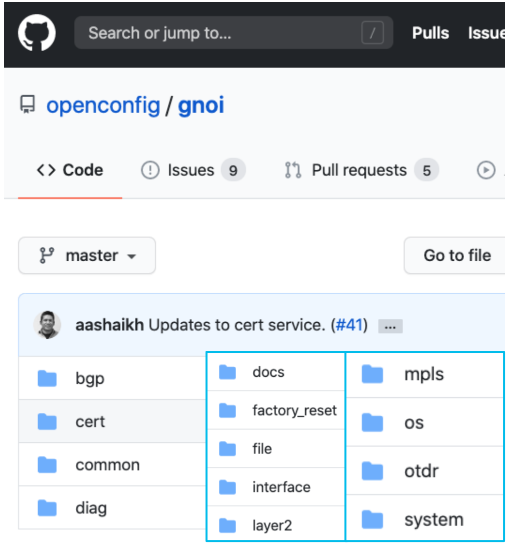
python

gNOI gRPC Network Operations Interface

1. gRPC Network Operations Interface, or gNOI, is a set of gRPC-based microservices, used for executing operational commands on network devices
2. gNOI operations are executed against the gNMI API interface
3. gNOI is defined and implemented on a per proto basis
4. There are many protos defined - some are more mature and evolve and different pace

Protobuf RPC	Use	Related CLI	Release
Cert.proto	TLS Certificate management	`crypto pki …`	17.3
Os.proto	Network Operating System management	`install add file …`	17.5
Reset.proto	Factory Reset and wipe	`factory-reset …`	17.7
File.proto	Not implemented	`copy, delete`	N/A
System.proto	Not implemented	`reload, set boot`	N/A

https://github.com/openconfig/gnoi



openconfig / gnoi

aashaikh Updates to cert service. (#41) …

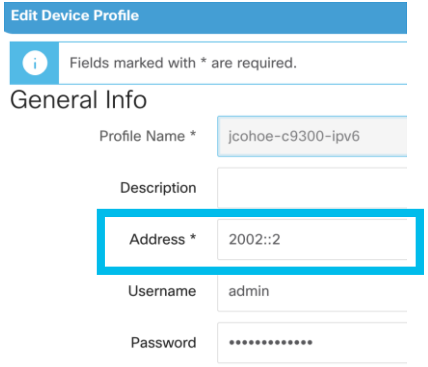
bgp
cert
common
diag
docs
factory_reset
file
interface
layer2
mpls
os
otdr
system

FYI – 17.10

IPv6 support for gNMI

Along with IPv4 support for gNMI, now Cisco IOS XE also supports IPv6 for gNMI.

YANG Suite



Edit Device Profile

Fields marked with * are required.

General Info

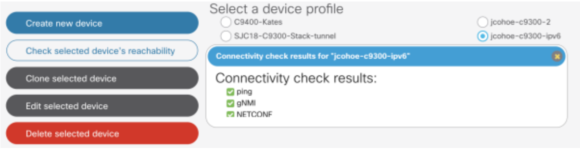
Profile Name * jcohoe-c9300-ipv6

Description

Address * 2002::2

Username admin

Password ••••••••••••••



Select a device profile

○ C9400-Kates
○ SJC18-C9300-Stack-tunnel
○ jcohoe-c9300-2
● jcohoe-c9300-ipv6

Connectivity check results for "jcohoe-c9300-ipv6"

Connectivity check results:

☑ ping
☑ gNMI
☑ NETCONF

NETCONF/RESTCONF also have IPv6 support

Subscriptions

```
{
  "subscribe": {
    "prefix": {}
    "subscription": {
       "path": {
            "origin": "openconfig"
              "elem": {
                "name": "system”
              }
              "elem": {
                "name": "system”
              }
            }
            "mode": "SAMPLE"
            }
    "subscription": {
            "path": {
            "origin": "openconfig"
              "elem": {
                "name": "system”
              }
              "elem": {
                "name": ”state”
              }
            }
            "mode": "SAMPLE"
            }
            "encoding": "JSON_IETF"
    }
}
```

Responses

```
update: {
  timestamp: 1661357167304760000
  update: {
    path: {
      origin: "openconfig"
      elem: {
        name: "system"
      }
      elem: {
        name: "state"
      )
    )
    val: {
      json_ietf_val: "{\"hostname\":\”jcohoe-c9300-ipv6\",\"domain-name\":\"cisco\",\"current-datetime\":\"2022-08-
24T21:36:07Z+00:00\",\"boot-time\":\"1659445935\",\"cisco-xe-openconfig-system-ext:license\":{\"eula\":\"\\nPLEASE
READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR\\nLICENSE KEY PROVIDED FOR ANY CISCO SOFTWARE
PRODUCT, PRODUCT FEATURE,\\nAND/OR SUBSEQUENTLY PROVIDED SOFTWARE FEATURES (COLLECTIVELY, THE\\n\\\"SOFTWARE\\\"),
AND/OR USING SUCH SOFTWARE CONSTITUT\"}}"
    )
  )
)


update: {
  timestamp: 1661357167307337000
  update: {
    path: {
      origin: "openconfig"
      elem: {
        name: "system"
      )
      elem: {
        name: "config"
      )
    )
    val: {
      json_ietf_val: "{\"hostname\":\"jcohoe-c9300-ipv6\",\"domain-name\":\"cisco\"}"
    }
  }
}
```

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

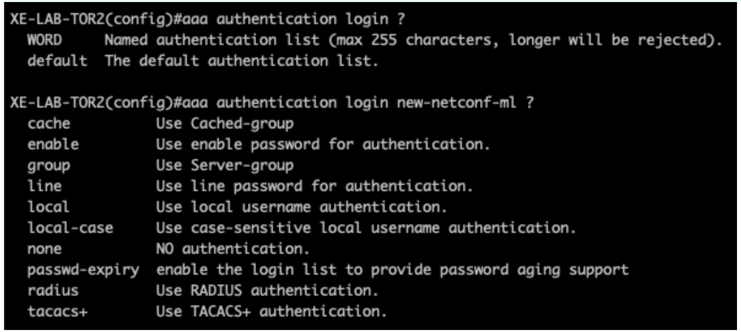
AAA Method List

FYI – 17.9

NETCONF
RESTCONF

The “default” AAA method list was required for programmatic operations
Now support for additional method lists is being introduced
In addition to default login, now we can specify additional AAA mechanisms

This makes programmatic access more resilient by enabling multiple authentication options



```
XE-LAB-TOR2(config)#aaa authentication login ?
  WORD     Named authentication list (max 255 characters, longer will be rejected).
  default  The default authentication list.

XE-LAB-TOR2(config)#aaa authentication login new-netconf-ml ?
  cache          Use Cached-group
  enable         Use enable password for authentication.
  group          Use Server-group
  line           Use line password for authentication.
  local          Use local username authentication.
  local-case     Use case-sensitive local username authentication.
  none           NO authentication.
  passwd-expiry  enable the login list to provide password aging support
  radius         Use RADIUS authentication.
  tacacs+        Use TACACS+ authentication.
```

```
netconf-yang
no aaa authentication login default local
no aaa authorization exec default local
tacacs server ISE-2
address ipv4 10.10.11.12
key Cisco123
aaa group server tacacs+ ise
server name ISE-2
ip vrf forwarding Mgmt-vrf
ip tacacs source-interface GigabitEthernet0/0
aaa authentication login netconf-authn group ise local
aaa authorization exec netconf-authz group ise local
aaa new-model
aaa session-id common
yang-interfaces aaa authentication method-list netconf-authn
yang-interfaces aaa authorization method-list netconf-authz
```

What are Method lists? Method lists for authorization define the ways that authorization is performed and the sequence in which these methods are performed. A method list is simply a named list describing the authorization methods to be queried (such as LDAP, RADIUS, or TACACS+), in sequence. Method lists enable one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted.

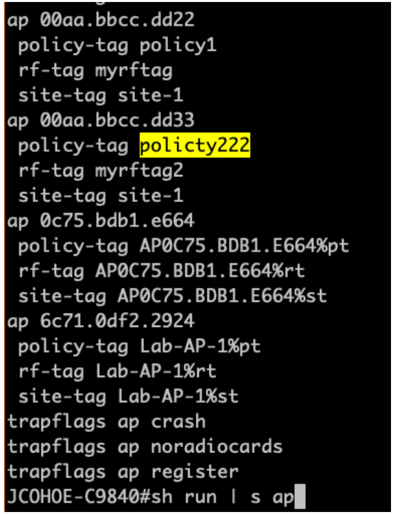
https://github.com/jeremycohoe/netconf-tacacs-aaa and https://github.com/jeremycohoe/netconf-tacacs-aaa/blob/main/custom-method-list.txt
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/178/b_178_programmability_cg/m_178_prog_model_based_aaa.html
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-mt/sec-usr-aaa-15-mt-book/configuring_authorization.html

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP provisioning example

CLI:

```
ap 188b.9dbe.6eac
 policy-tag policty222
 site-tag site-tag-name
 rf-tag rf-tag-name
```



```
ap 00aa.bbcc.dd22
 policy-tag policy1
 rf-tag myrftag
 site-tag site-1
ap 00aa.bbcc.dd33
 policy-tag policty222
 rf-tag myrftag2
 site-tag site-1
ap 0c75.bdb1.e664
 policy-tag AP0C75.BDB1.E664%pt
 rf-tag AP0C75.BDB1.E664%rt
 site-tag AP0C75.BDB1.E664%st
ap 6c71.0df2.2924
 policy-tag Lab-AP-1%pt
 rf-tag Lab-AP-1%rt
 site-tag Lab-AP-1%st
trapflags ap crash
trapflags ap noradiocards
trapflags ap register
JCOHOE-C9840#sh run | s ap
```

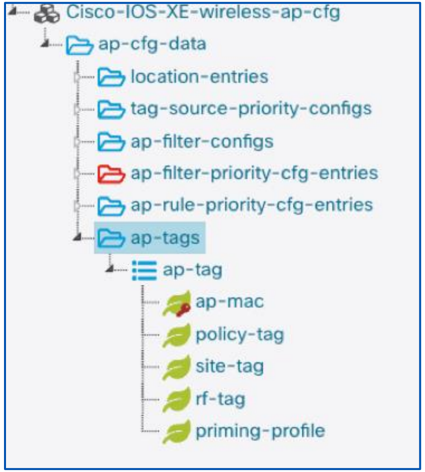
=

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <edit-config>
    <target>
      <running/>
    </target>
    <config>
      <ap-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-ap-cfg">
        <ap-tags>
          <ap-tag>
            <ap-mac>00:aa:bb:cc:dd:11</ap-mac>
            <policy-tag>policy1</policy-tag>
            <site-tag>site-1</site-tag>
            <rf-tag>myrftag</rf-tag>
          </ap-tag>
          <ap-tag>
            <ap-mac>00:aa:bb:cc:dd:22</ap-mac>
            <policy-tag>policy1</policy-tag>
            <site-tag>site-1</site-tag>
            <rf-tag>myrftag</rf-tag>
          </ap-tag>
          <ap-tag>
            <ap-mac>00:aa:bb:cc:dd:33</ap-mac>
            <policy-tag>policty222</policy-tag>
            <site-tag>site-1</site-tag>
            <rf-tag>myrftag2</rf-tag>
          </ap-tag>
        </ap-tags>
      </ap-cfg-data>
    </config>
  </edit-config>
</rpc>
```

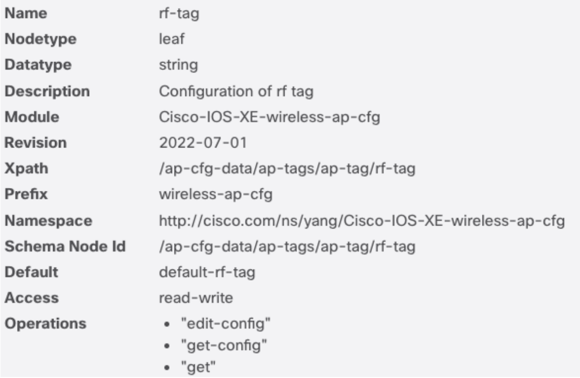
YANG model @ https://github.com/YangModels/yang/blob/main/vendor/cisco/xe/1791/Cisco-IOS-XE-wireless-ap-cfg.yang

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

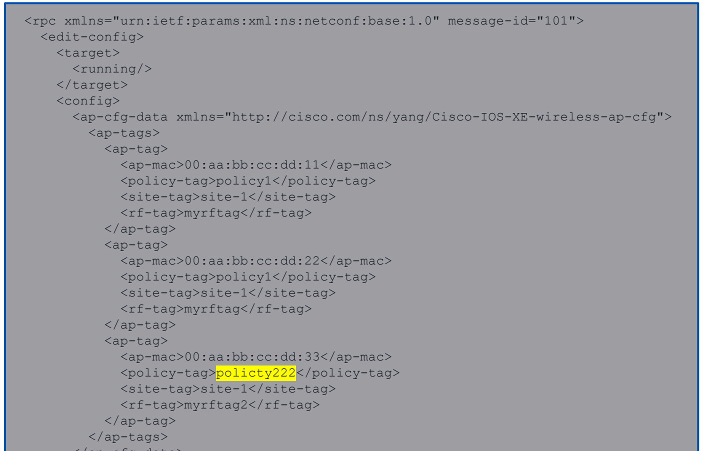
AP provisioning example



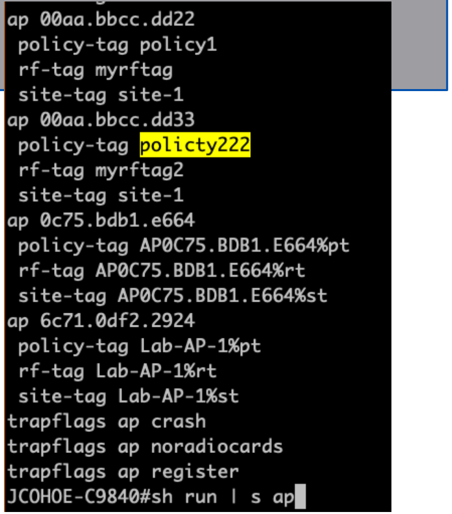
```
Cisco-IOS-XE-wireless-ap-cfg
  ap-cfg-data
    location-entries
    tag-source-priority-configs
    ap-filter-configs
    ap-filter-priority-cfg-entries
    ap-rule-priority-cfg-entries
    ap-tags
      ap-tag
        ap-mac
        policy-tag
        site-tag
        rf-tag
        priming-profile
```



Name	rf-tag
Nodetype	leaf
Datatype	string
Description	Configuration of rf tag
Module	Cisco-IOS-XE-wireless-ap-cfg
Revision	2022-07-01
Xpath	/ap-cfg-data/ap-tags/ap-tag/rf-tag
Prefix	wireless-ap-cfg
Namespace	http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-ap-cfg
Schema Node Id	/ap-cfg-data/ap-tags/ap-tag/rf-tag
Default	default-rf-tag
Access	read-write
Operations	• "edit-config" • "get-config" • "get"

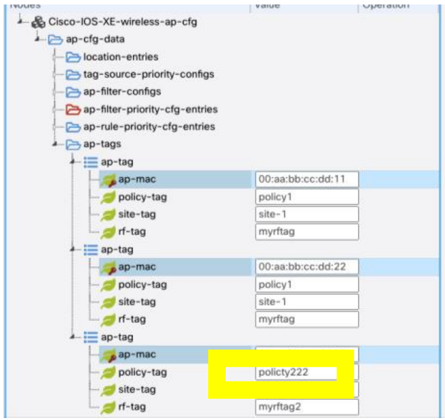


```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <edit-config>
    <target>
      <running/>
    </target>
    <config>
      <ap-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-ap-cfg">
        <ap-tags>
          <ap-tag>
            <ap-mac>00:aa:bb:cc:dd:11</ap-mac>
            <policy-tag>policy1</policy-tag>
            <site-tag>site-1</site-tag>
            <rf-tag>myrftag</rf-tag>
          </ap-tag>
          <ap-tag>
            <ap-mac>00:aa:bb:cc:dd:22</ap-mac>
            <policy-tag>policy1</policy-tag>
            <site-tag>site-1</site-tag>
            <rf-tag>myrftag</rf-tag>
          </ap-tag>
          <ap-tag>
            <ap-mac>00:aa:bb:cc:dd:33</ap-mac>
            <policy-tag>policty222</policy-tag>
            <site-tag>site-1</site-tag>
            <rf-tag>myrftag2</rf-tag>
          </ap-tag>
        </ap-tags>
      </ap-cfg-data>
    </config>
  </edit-config>
</rpc>
```

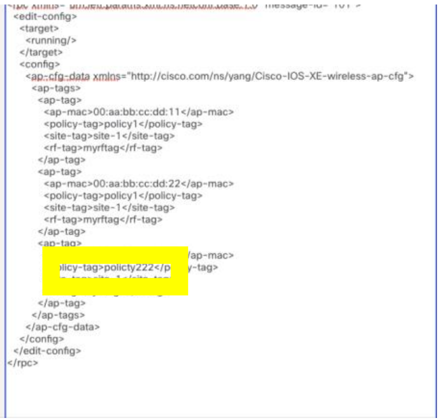


```
ap 00aa.bbcc.dd22
 policy-tag policy1
 rf-tag myrftag
 site-tag site-1
ap 00aa.bbcc.dd33
 policy-tag policty222
 rf-tag myrftag2
 site-tag site-1
ap 0c75.bdb1.e664
 policy-tag AP0C75.BDB1.E664%pt
 rf-tag AP0C75.BDB1.E664%rt
 site-tag AP0C75.BDB1.E664%st
ap 6c71.0df2.2924
 policy-tag Lab-AP-1%pt
 rf-tag Lab-AP-1%rt
 site-tag Lab-AP-1%st
trapflags ap crash
trapflags ap noradiocards
trapflags ap register
JCOHOE-C9840#sh run | s ap
```

CLI:
ap 188b.9dbe.6eac
 policy-tag policy222
 site-tag site-tag-name
 rf-tag rf-tag-name



```
Nodes                                   Value                Operation
Cisco-IOS-XE-wireless-ap-cfg
  ap-cfg-data
    location-entries
    tag-source-priority-configs
    ap-filter-configs
    ap-filter-priority-cfg-entries
    ap-rule-priority-cfg-entries
    ap-tags
      ap-tag
        ap-mac                          00:aa:bb:cc:dd:11
        policy-tag                      policy1
        site-tag                        site-1
        rf-tag                          myrftag
      ap-tag
        ap-mac                          00:aa:bb:cc:dd:22
        policy-tag                      policy1
        site-tag                        site-1
        rf-tag                          myrftag
      ap-tag
        ap-mac
        policy-tag                      policty222
        site-tag
        rf-tag                          myrftag2
```



```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
 <edit-config>
  <target>
   <running/>
  </target>
  <config>
   <ap-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-ap-cfg">
    <ap-tags>
     <ap-tag>
      <ap-mac>00:aa:bb:cc:dd:11</ap-mac>
      <policy-tag>policy1</policy-tag>
      <site-tag>site-1</site-tag>
      <rf-tag>myrftag</rf-tag>
     </ap-tag>
     <ap-tag>
      <ap-mac>00:aa:bb:cc:dd:22</ap-mac>
      <policy-tag>policy1</policy-tag>
      <site-tag>site-1</site-tag>
      <rf-tag>myrftag</rf-tag>
     </ap-tag>
     <ap-tag>
                 /ap-mac>
      olicy-tag>policty222</policy-tag>

     </ap-tag>
    </ap-tags>
   </ap-cfg-data>
  </config>
 </edit-config>
</rpc>
```

YANG model @ https://github.com/YangModels/yang/blob/main/vendor/cisco/xe/1791/Cisco-IOS-XE-wireless-ap-cfg.yang

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP rename example

Exec CLI:
ap name
<default_name>
name <new_name>

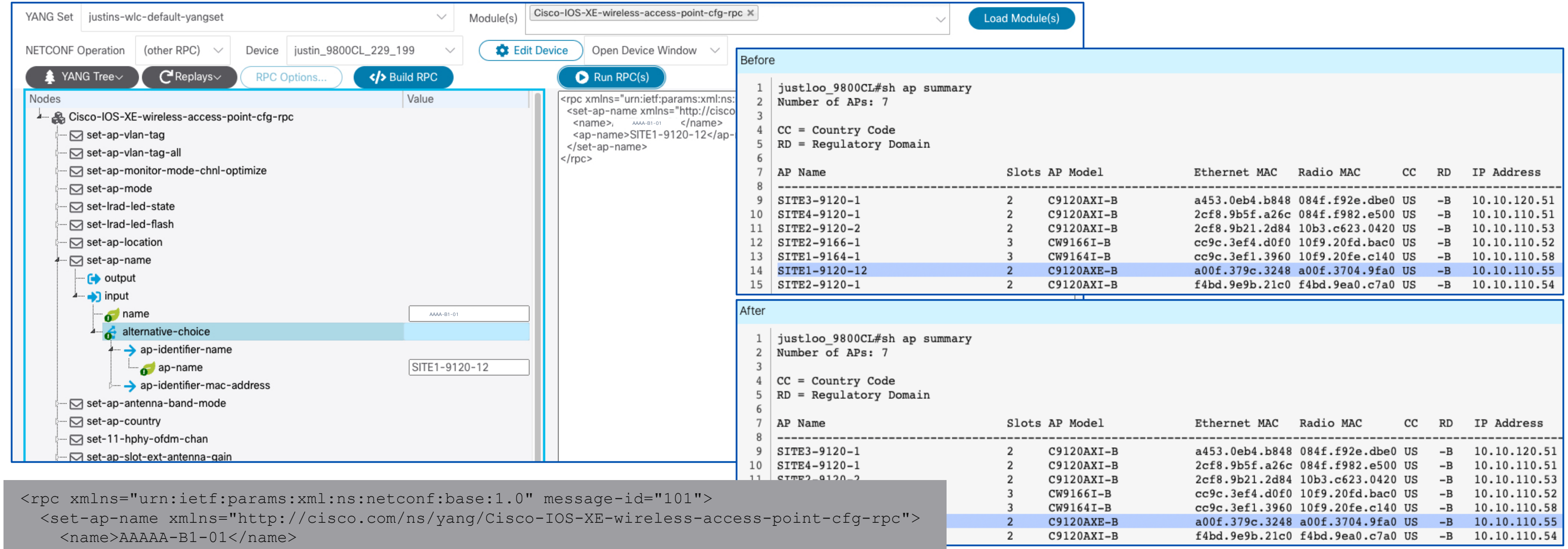
```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <set-ap-name xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-access-point-cfg-rpc">
    <name>AAAAA-B1-01</name>
    <ap-name>SITE1-9120-12</ap-name>
  </set-ap-name>
</rpc>
```

YANG: https://github.com/YangModels/yang/blob/main/vendor/cisco/xe/1791/Cisco-IOS-XE-wireless-access-point-cfg-rpc.yang

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP rename example

Exec CLI: ap name <default_name> name <new_name>



YANG Set: justins-wlc-default-yangset

Module(s): Cisco-IOS-XE-wireless-access-point-cfg-rpc

NETCONF Operation: (other RPC)

Device: justin_9800CL_229_199

name: AAAA-B1-01

ap-name: SITE1-9120-12

```
<rpc xmlns="urn:ietf:params:xml:ns:
  <set-ap-name xmlns="http://cisco
    <name>       AAAA-B1-01       </name>
    <ap-name>SITE1-9120-12</ap-
  </set-ap-name>
</rpc>
```

Before

```
justloo_9800CL#sh ap summary
Number of APs: 7

CC = Country Code
RD = Regulatory Domain

AP Name                          Slots AP Model             Ethernet MAC   Radio MAC      CC   RD   IP Address
-----------------------------------------------------------------------------------------------------------------
SITE3-9120-1                     2     C9120AXI-B           a453.0eb4.b848 084f.f92e.dbe0 US   -B   10.10.120.51
SITE4-9120-1                     2     C9120AXI-B           2cf8.9b5f.a26c 084f.f982.e500 US   -B   10.10.110.51
SITE2-9120-2                     2     C9120AXI-B           2cf8.9b21.2d84 10b3.c623.0420 US   -B   10.10.110.53
SITE2-9166-1                     3     CW9166I-B            cc9c.3ef4.d0f0 10f9.20fd.bac0 US   -B   10.10.110.52
SITE1-9164-1                     3     CW9164I-B            cc9c.3ef1.3960 10f9.20fe.c140 US   -B   10.10.110.58
SITE1-9120-12                    2     C9120AXE-B           a00f.379c.3248 a00f.3704.9fa0 US   -B   10.10.110.55
SITE2-9120-1                     2     C9120AXI-B           f4bd.9e9b.21c0 f4bd.9ea0.c7a0 US   -B   10.10.110.54
```

After

```
justloo_9800CL#sh ap summary
Number of APs: 7

CC = Country Code
RD = Regulatory Domain

AP Name                          Slots AP Model             Ethernet MAC   Radio MAC      CC   RD   IP Address
-----------------------------------------------------------------------------------------------------------------
SITE3-9120-1                     2     C9120AXI-B           a453.0eb4.b848 084f.f92e.dbe0 US   -B   10.10.120.51
SITE4-9120-1                     2     C9120AXI-B           2cf8.9b5f.a26c 084f.f982.e500 US   -B   10.10.110.51
                                 2     C9120AXI-B           2cf8.9b21.2d84 10b3.c623.0420 US   -B   10.10.110.53
                                 3     CW9166I-B            cc9c.3ef4.d0f0 10f9.20fd.bac0 US   -B   10.10.110.52
                                 3     CW9164I-B            cc9c.3ef1.3960 10f9.20fe.c140 US   -B   10.10.110.58
                                 2     C9120AXE-B           a00f.379c.3248 a00f.3704.9fa0 US   -B   10.10.110.55
                                 2     C9120AXI-B           f4bd.9e9b.21c0 f4bd.9ea0.c7a0 US   -B   10.10.110.54
```

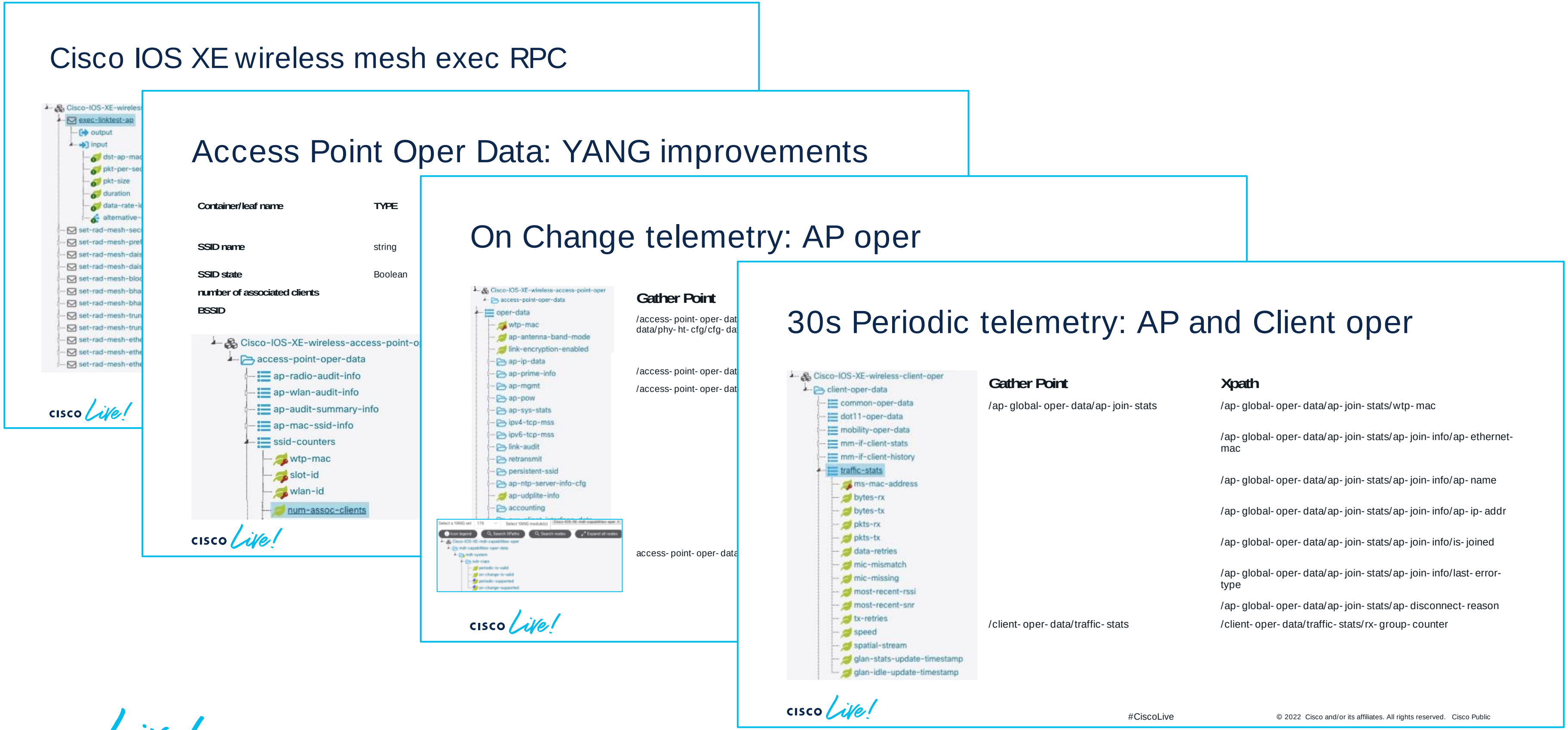
```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <set-ap-name xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-access-point-cfg-rpc">
    <name>AAAAA-B1-01</name>
    <ap-name>SITE1-9120-12</ap-name>
  </set-ap-name>
</rpc>
```

YANG: https://github.com/YangModels/yang/blob/main/vendor/cisco/xe/1791/Cisco-IOS-XE-wireless-access-point-cfg-rpc.yang

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

YANG
YANG Suite
YANG Tooling

Innovations in wireless YANG



Cisco IOS XE wireless mesh exec RPC

```
Cisco-IOS-XE-wireless
  exec-linktest-ap
    output
    input
      dst-ap-mac
      pkt-per-sec
      pkt-size
      duration
      data-rate-i
      alternative-
  set-rad-mesh-sec
  set-rad-mesh-pref
  set-rad-mesh-dais
  set-rad-mesh-dais
  set-rad-mesh-bloc
  set-rad-mesh-bha
  set-rad-mesh-bha
  set-rad-mesh-trun
  set-rad-mesh-trun
  set-rad-mesh-ethe
  set-rad-mesh-ethe
  set-rad-mesh-ethe
```

Access Point Oper Data: YANG improvements

Container/leaf name	TYPE
SSID name	string
SSID state	Boolean
number of associated clients	
BSSID	

```
Cisco-IOS-XE-wireless-access-point-o
  access-point-oper-data
    ap-radio-audit-info
    ap-wlan-audit-info
    ap-audit-summary-info
    ap-mac-ssid-info
    ssid-counters
      wtp-mac
      slot-id
      wlan-id
      num-assoc-clients
```

On Change telemetry: AP oper

```
Cisco-IOS-XE-wireless-access-point-oper
  access-point-oper-data
    oper-data
      wtp-mac
      ap-antenna-band-mode
      link-encryption-enabled
      ap-ip-data
      ap-prime-info
      ap-mgmt
      ap-pow
      ap-sys-stats
      ipv4-tcp-mss
      ipv6-tcp-mss
      link-audit
      retransmit
      persistent-ssid
      ap-ntp-server-info-cfg
      ap-udplite-info
      accounting
```

Select a YANG set 176 Select YANG module(s) Cisco-IOS-XE-mdt-capabilities-oper

```
Cisco-IOS-XE-mdt-capabilities-oper
  mdt-capabilities-oper-data
    mdt-system
      sub-caps
        periodic-is-valid
        on-change-is-valid
        periodic-supported
        on-change-supported
```

Gather Point

/access- point- oper- dat
data/phy- ht- cfg/cfg- da

/access- point- oper- dat

/access- point- oper- dat

access- point- oper- data

30s Periodic telemetry: AP and Client oper

```
Cisco-IOS-XE-wireless-client-oper
  client-oper-data
    common-oper-data
    dot11-oper-data
    mobility-oper-data
    mm-if-client-stats
    mm-if-client-history
    traffic-stats
      ms-mac-address
      bytes-rx
      bytes-tx
      pkts-rx
      pkts-tx
      data-retries
      mic-mismatch
      mic-missing
      most-recent-rssi
      most-recent-snr
      tx-retries
      speed
      spatial-stream
      glan-stats-update-timestamp
      glan-idle-update-timestamp
```

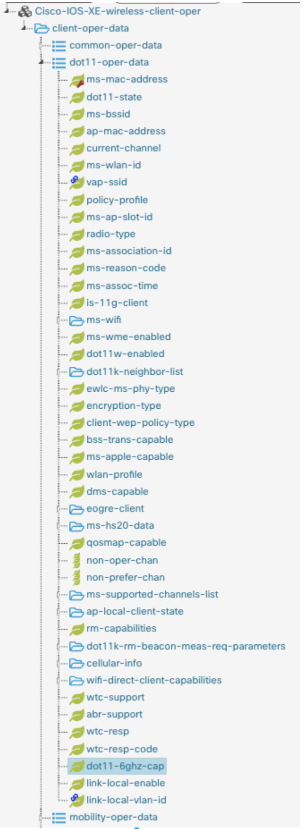
Gather Point	Xpath
/ap- global- oper- data/ap- join- stats	/ap- global- oper- data/ap- join- stats/wtp- mac
	/ap- global- oper- data/ap- join- stats/ap- join- info/ap- ethernet- mac
	/ap- global- oper- data/ap- join- stats/ap- join- info/ap- name
	/ap- global- oper- data/ap- join- stats/ap- join- info/ap- ip- addr
	/ap- global- oper- data/ap- join- stats/ap- join- info/is- joined
	/ap- global- oper- data/ap- join- stats/ap- join- info/last- error- type
	/ap- global- oper- data/ap- join- stats/ap- disconnect- reason
/client- oper- data/traffic- stats	/client- oper- data/traffic- stats/rx- group- counter

#CiscoLive

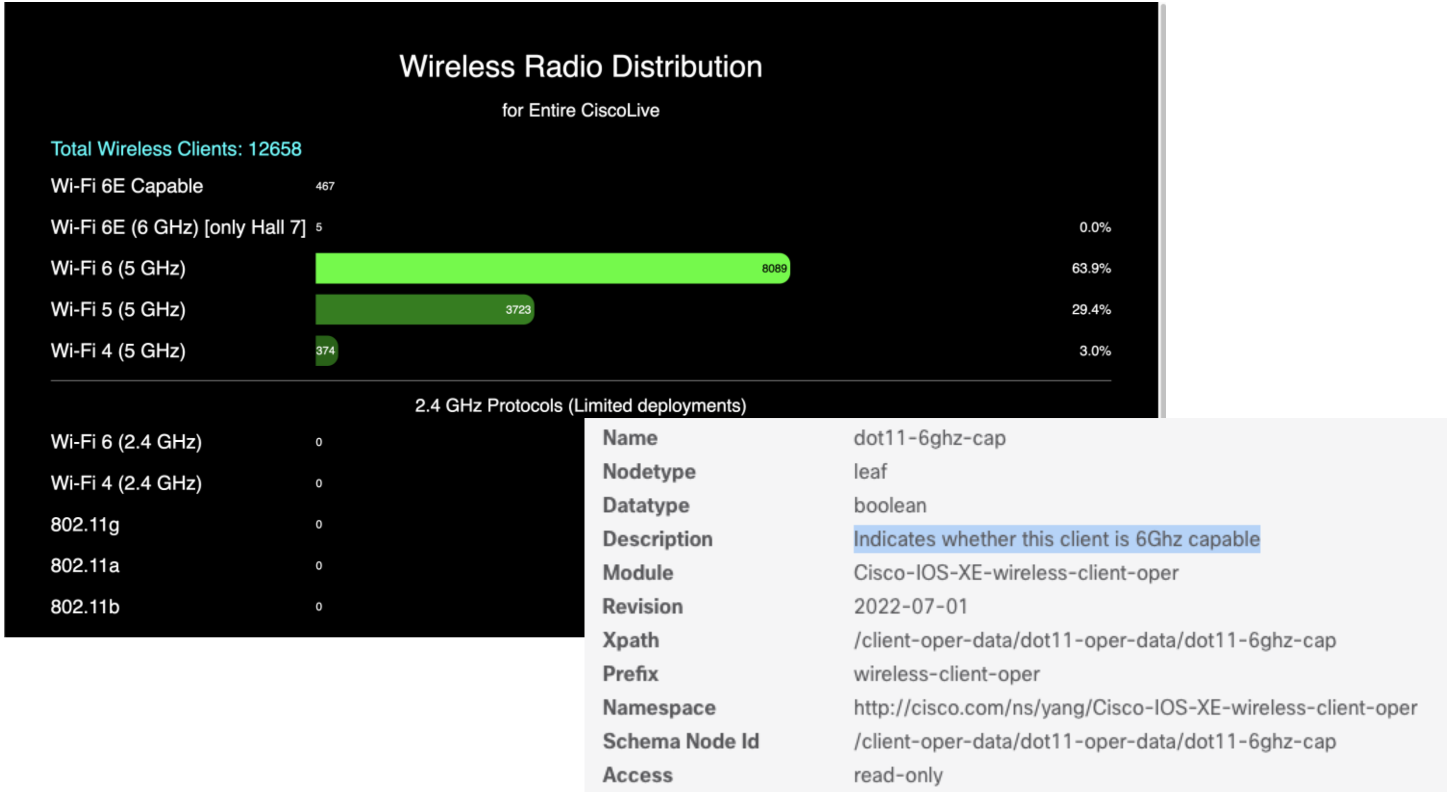
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wi-fi 6E Capable ?



```
Cisco-IOS-XE-wireless-client-oper
  client-oper-data
    common-oper-data
    dot11-oper-data
      ms-mac-address
      dot11-state
      ms-bssid
      ap-mac-address
      current-channel
      ms-wlan-id
      vap-ssid
      policy-profile
      ms-ap-slot-id
      radio-type
      ms-association-id
      ms-reason-code
      ms-assoc-time
      is-11g-client
      ms-wifi
      ms-wme-enabled
      dot11w-enabled
      dot11k-neighbor-list
      ewlc-ms-phy-type
      encryption-type
      client-wep-policy-type
      bss-trans-capable
      ms-apple-capable
      wlan-profile
      dms-capable
      eogre-client
      ms-hs20-data
      qosmap-capable
      non-oper-chan
      non-prefer-chan
      ms-supported-channels-list
      ap-local-client-state
      rm-capabilities
      dot11k-rm-beacon-meas-req-parameters
      cellular-info
      wifi-direct-client-capabilities
      wtc-support
      abr-support
      wtc-resp
      wtc-resp-code
      dot11-6ghz-cap
      link-local-enable
      link-local-vlan-id
    mobility-oper-data
```



Name	dot11-6ghz-cap
Nodetype	leaf
Datatype	boolean
Description	Indicates whether this client is 6Ghz capable
Module	Cisco-IOS-XE-wireless-client-oper
Revision	2022-07-01
Xpath	/client-oper-data/dot11-oper-data/dot11-6ghz-cap
Prefix	wireless-client-oper
Namespace	http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-client-oper
Schema Node Id	/client-oper-data/dot11-oper-data/dot11-6ghz-cap
Access	read-only

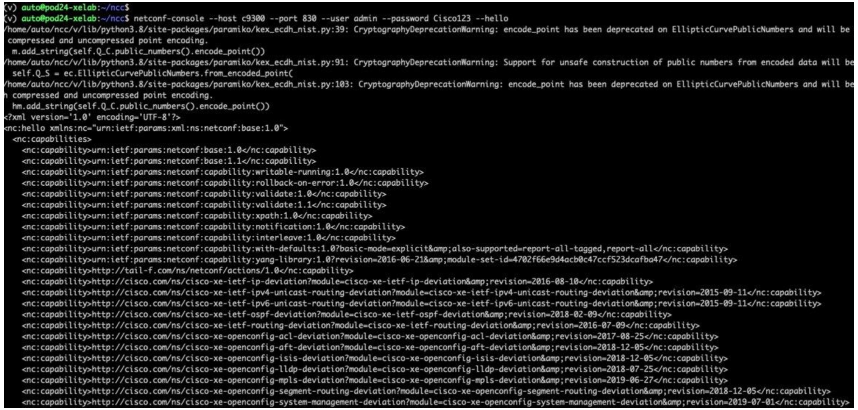
https://github.com/YangModels/yang/blob/main/vendor/cisco/xe/17101/Cisco-IOS-XE-wireless-client-oper.yang

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

17.10

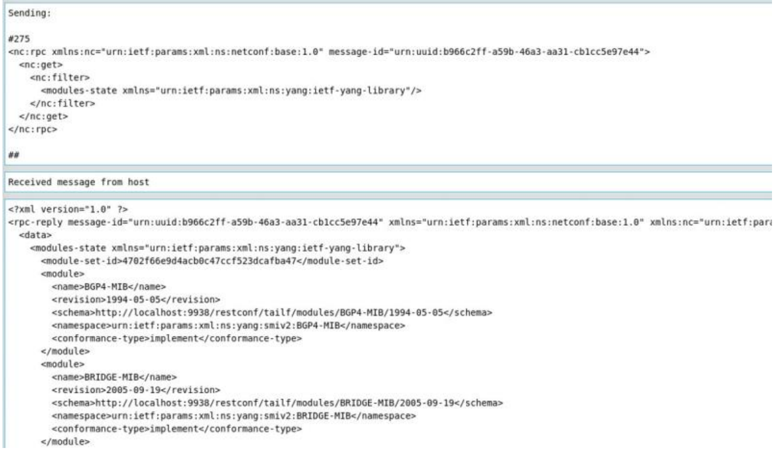
YANG 1.0 to 1.1 transition – YANG advertisement

Legacy YANG 1.0 capabilities exchange and NETCONF "hello" message will soon be unsupported



```
(v) auto@pod24-xelab:~/ncc$
(v) auto@pod24-xelab:~/ncc$ netconf-console --host c9300 --port 830 --user admin --password Cisco123 --hello
/home/auto/ncc/v/lib/python3.8/site-packages/paramiko/kex_ecdh_nist.py:39: CryptographyDeprecationWarning: encode_point has been deprecated on EllipticCurvePublicNumbers and will be
 compressed and uncompressed point encoding.
  m.add_string(self.Q_C.public_numbers().encode_point())
/home/auto/ncc/v/lib/python3.8/site-packages/paramiko/kex_ecdh_nist.py:91: CryptographyDeprecationWarning: Support for unsafe construction of public numbers from encoded data will be
  self.Q_S = ec.EllipticCurvePublicNumbers.from_encoded_point(
/home/auto/ncc/v/lib/python3.8/site-packages/paramiko/kex_ecdh_nist.py:103: CryptographyDeprecationWarning: encode_point has been deprecated on EllipticCurvePublicNumbers and will be
n compressed and uncompressed point encoding.
  hm.add_string(self.Q_C.public_numbers().encode_point())
<?xml version='1.0' encoding='UTF-8'?>
<nc:hello xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
  <nc:capabilities>
    <nc:capability>urn:ietf:params:netconf:base:1.0</nc:capability>
    <nc:capability>urn:ietf:params:netconf:base:1.1</nc:capability>
    <nc:capability>urn:ietf:params:netconf:capability:writable-running:1.0</nc:capability>
    <nc:capability>urn:ietf:params:netconf:capability:rollback-on-error:1.0</nc:capability>
    <nc:capability>urn:ietf:params:netconf:capability:validate:1.0</nc:capability>
    <nc:capability>urn:ietf:params:netconf:capability:validate:1.1</nc:capability>
    <nc:capability>urn:ietf:params:netconf:capability:xpath:1.0</nc:capability>
    <nc:capability>urn:ietf:params:netconf:capability:notification:1.0</nc:capability>
    <nc:capability>urn:ietf:params:netconf:capability:interleave:1.0</nc:capability>
    <nc:capability>urn:ietf:params:netconf:capability:with-defaults:1.0?basic-mode=explicit&amp;also-supported=report-all-tagged,report-all</nc:capability>
    <nc:capability>urn:ietf:params:netconf:capability:yang-library:1.0?revision=2016-06-21&amp;module-set-id=4702f66e9d4acb0c47ccf523dcafba47</nc:capability>
    <nc:capability>http://tail-f.com/ns/netconf/actions/1.0</nc:capability>
    <nc:capability>http://cisco.com/ns/cisco-xe-ietf-ip-deviation?module=cisco-xe-ietf-ip-deviation&amp;revision=2016-08-10</nc:capability>
    <nc:capability>http://cisco.com/ns/cisco-xe-ietf-ipv4-unicast-routing-deviation?module=cisco-xe-ietf-ipv4-unicast-routing-deviation&amp;revision=2015-09-11</nc:capability>
    <nc:capability>http://cisco.com/ns/cisco-xe-ietf-ipv6-unicast-routing-deviation?module=cisco-xe-ietf-ipv6-unicast-routing-deviation&amp;revision=2015-09-11</nc:capability>
    <nc:capability>http://cisco.com/ns/cisco-xe-ietf-ospf-deviation?module=cisco-xe-ietf-ospf-deviation&amp;revision=2018-02-09</nc:capability>
    <nc:capability>http://cisco.com/ns/cisco-xe-ietf-routing-deviation?module=cisco-xe-ietf-routing-deviation&amp;revision=2016-07-09</nc:capability>
    <nc:capability>http://cisco.com/ns/cisco-xe-openconfig-acl-deviation?module=cisco-xe-openconfig-acl-deviation&amp;revision=2017-08-25</nc:capability>
    <nc:capability>http://cisco.com/ns/cisco-xe-openconfig-aft-deviation?module=cisco-xe-openconfig-aft-deviation&amp;revision=2018-12-05</nc:capability>
    <nc:capability>http://cisco.com/ns/cisco-xe-openconfig-isis-deviation?module=cisco-xe-openconfig-isis-deviation&amp;revision=2018-12-05</nc:capability>
    <nc:capability>http://cisco.com/ns/cisco-xe-openconfig-lldp-deviation?module=cisco-xe-openconfig-lldp-deviation&amp;revision=2018-07-25</nc:capability>
    <nc:capability>http://cisco.com/ns/cisco-xe-openconfig-mpls-deviation?module=cisco-xe-openconfig-mpls-deviation&amp;revision=2019-06-27</nc:capability>
    <nc:capability>http://cisco.com/ns/cisco-xe-openconfig-segment-routing-deviation?module=cisco-xe-openconfig-segment-routing-deviation&amp;revision=2018-12-05</nc:capability>
    <nc:capability>http://cisco.com/ns/cisco-xe-openconfig-system-management-deviation?module=cisco-xe-openconfig-system-management-deviation&amp;revision=2019-07-01</nc:capability>
```

YANG 1.1 example: "ietf-yang-library” to retrieve supported YANG modules



```
Sending:

#275
<nc:rpc xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="urn:uuid:b966c2ff-a59b-46a3-aa31-cb1cc5e97e44">
  <nc:get>
    <nc:filter>
      <modules-state xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-library"/>
    </nc:filter>
  </nc:get>
</nc:rpc>

##
```

```
Received message from host
```

```
<?xml version="1.0" ?>
<rpc-reply message-id="urn:uuid:b966c2ff-a59b-46a3-aa31-cb1cc5e97e44" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns:nc="urn:ietf:para
  <data>
    <modules-state xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-library">
      <module-set-id>4702f66e9d4acb0c47ccf523dcafba47</module-set-id>
      <module>
        <name>BGP4-MIB</name>
        <revision>1994-05-05</revision>
        <schema>http://localhost:9938/restconf/tailf/modules/BGP4-MIB/1994-05-05</schema>
        <namespace>urn:ietf:params:xml:ns:yang:smiv2:BGP4-MIB</namespace>
        <conformance-type>implement</conformance-type>
      </module>
      <module>
        <name>BRIDGE-MIB</name>
        <revision>2005-09-19</revision>
        <schema>http://localhost:9938/restconf/tailf/modules/BRIDGE-MIB/2005-09-19</schema>
        <namespace>urn:ietf:params:xml:ns:yang:smiv2:BRIDGE-MIB</namespace>
        <conformance-type>implement</conformance-type>
      </module>
```

If the desired application previously parsed the NETCONF "hello" message to retrieve the supported YANG models, the parsing must be modified to reflect how version 1.1 advertises via "ietf-yang-library" instead of the NETCONF "hello" message.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

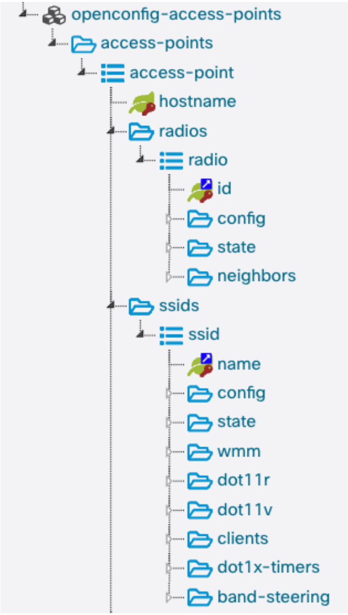
OC wireless: YANG model end of support

17.9

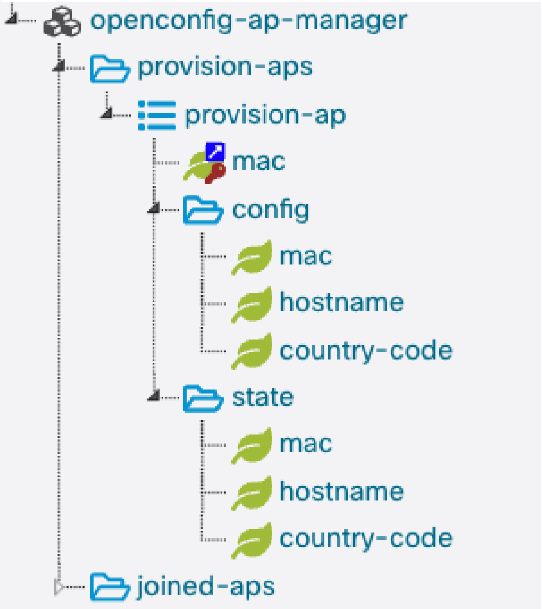
17.9 will be the last release supporting OC wifi YANG

https://github.com/openconfig/public/tree/master/release/models/wifi

- The YANG for OpenConfig Wireless including OpenConfig-access-points and OpenConfig-ap-manager YANG are no longer being supported after 17.9
- The constructs within OC Wireless support only flex deployments and direct AP management. There is no modelled concept of any CAPWAP tunnels or centralized controller infrastructure
- All or nothing: OC Wifi leverages a hostname centric view and does not use the MAC address. All config and operations must be via OC-wifi.YANG as the traditional YANG/CLI uses MAC centric view
- Most deployment are controller based/local mode, so the OC Wifi model is not applicable and not usable for most deployments
- OC Model version drift: the initial version implemented of 0.1.0 or 0.2.0 is not current with GitHub version of 1.0.0 so there are many mapping gaps making it even less usable



```
openconfig-access-points
  access-points
    access-point
      hostname
      radios
        radio
          id
          config
          state
          neighbors
      ssids
        ssid
          name
          config
          state
          wmm
          dot11r
          dot11v
          clients
          dot1x-timers
          band-steering
```



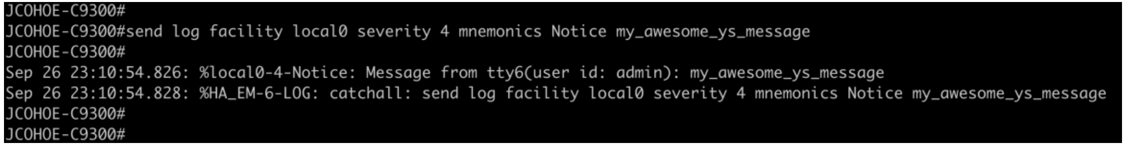
```
openconfig-ap-manager
  provision-aps
    provision-ap
      mac
      config
        mac
        hostname
        country-code
      state
        mac
        hostname
        country-code
  joined-aps
```

Image source: https://www.openconfig.net/img/oc-masthead.png

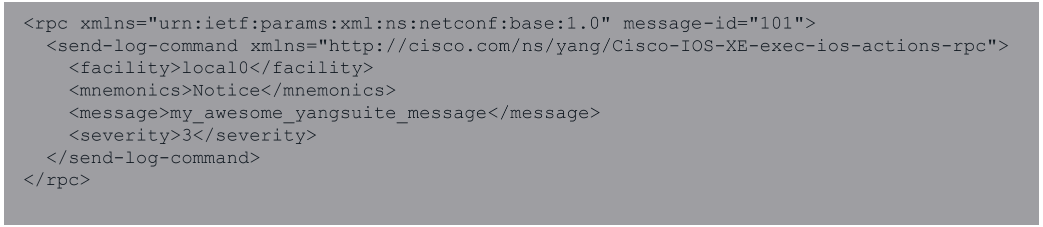
17.11

YANG model for Syslog generation

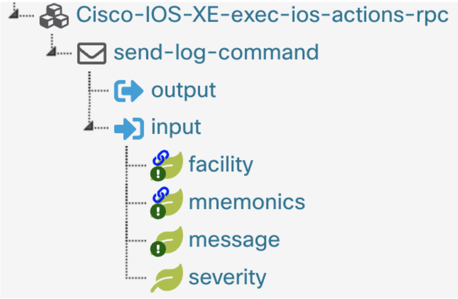
This YANG model can be used to programmatically generate syslog messages.
This ensures the network devices are securely connected to the remote syslog receiver.



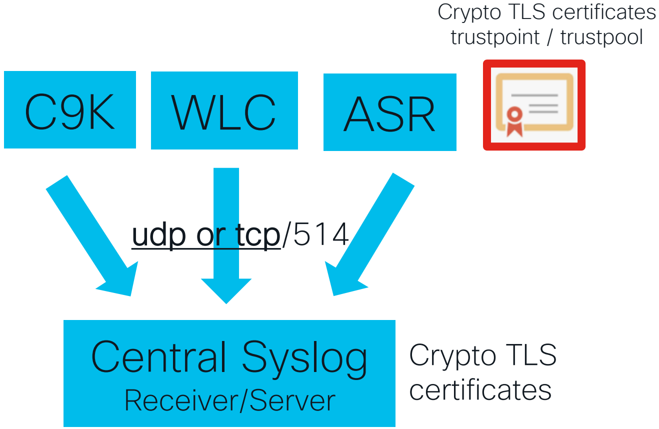
```
JCOHOE-C9300#
JCOHOE-C9300#send log facility local0 severity 4 mnemonics Notice my_awesome_ys_message
JCOHOE-C9300#
Sep 26 23:10:54.826: %local0-4-Notice: Message from tty6(user id: admin): my_awesome_ys_message
Sep 26 23:10:54.828: %HA_EM-6-LOG: catchall: send log facility local0 severity 4 mnemonics Notice my_awesome_ys_message
JCOHOE-C9300#
JCOHOE-C9300#
```



```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <send-log-command xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-exec-ios-actions-rpc">
    <facility>local0</facility>
    <mnemonics>Notice</mnemonics>
    <message>my_awesome_yangsuite_message</message>
    <severity>3</severity>
  </send-log-command>
</rpc>
```



```
Cisco-IOS-XE-exec-ios-actions-rpc
  send-log-command
    output
    input
      facility
      mnemonics
      message
      severity
```



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

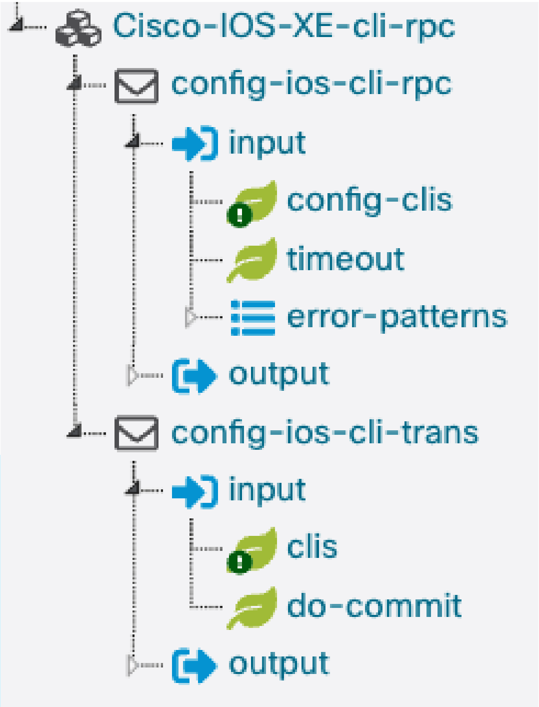
17.9

YANG model for CLI execution

Any configure CLI can now be sent within the YANG payload

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="101">
<config-ios-cli-rpc
xmlns=http://cisco.com/ns/yang/Cisco-IOS-XE-cli-rpc>
<config-clis>
interface Loopback111
description configured-via-CLI-YANG
no shutdown
</config-clis>
</config-ios-cli-rpc>
</rpc>]]>]]>
```

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="101">
<config-ios-cli-trans
xmlns=http://cisco.com/ns/yang/Cisco-IOS-XE-cli-rpc>
<clis>
interface Loopback111
description configured-via-CONFD-YANG
no shutdown
</clis>
</config-ios-cli-trans>
</rpc>]]>]]>
```



clis

config-clis

"cli rpc" sends CLI to the IOS parser

This is similar to configuring CLI on the VTY

Directly into running-config, then synchronized to ConfD

"transitional cli rpc" sends a list of CLI to ConfD

This is similar to sending edit-config RPCs corresponding to the CLI's.

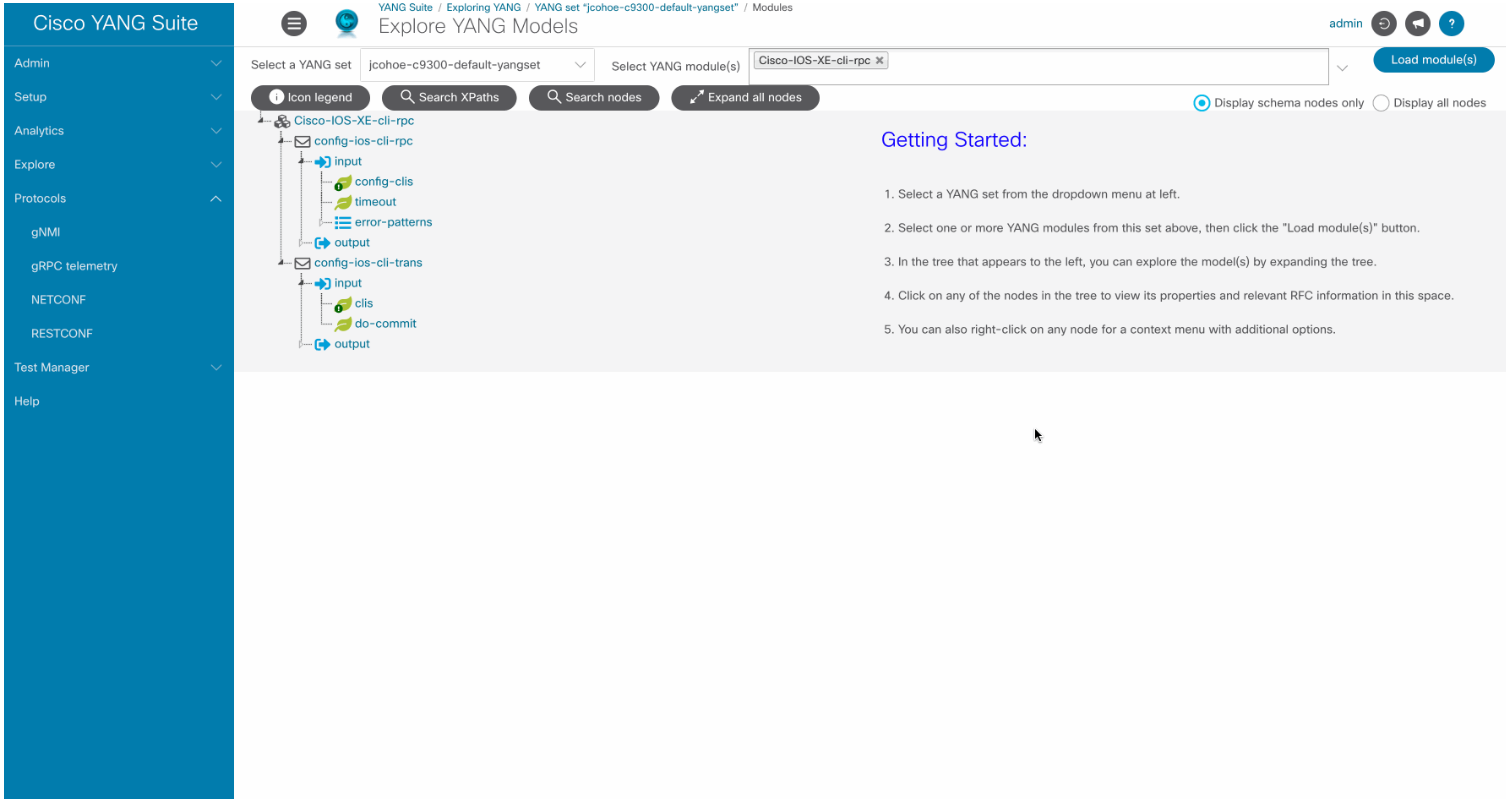
Synchronized from ConfD into the CLI running-config

cisco Live!

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

YANG model for CLI execution: Demo

Live Demo



Select a YANG set: jcohoe-c9300-default-yangset

Select YANG module(s): Cisco-IOS-XE-cli-rpc ✕

● Display schema nodes only ○ Display all nodes

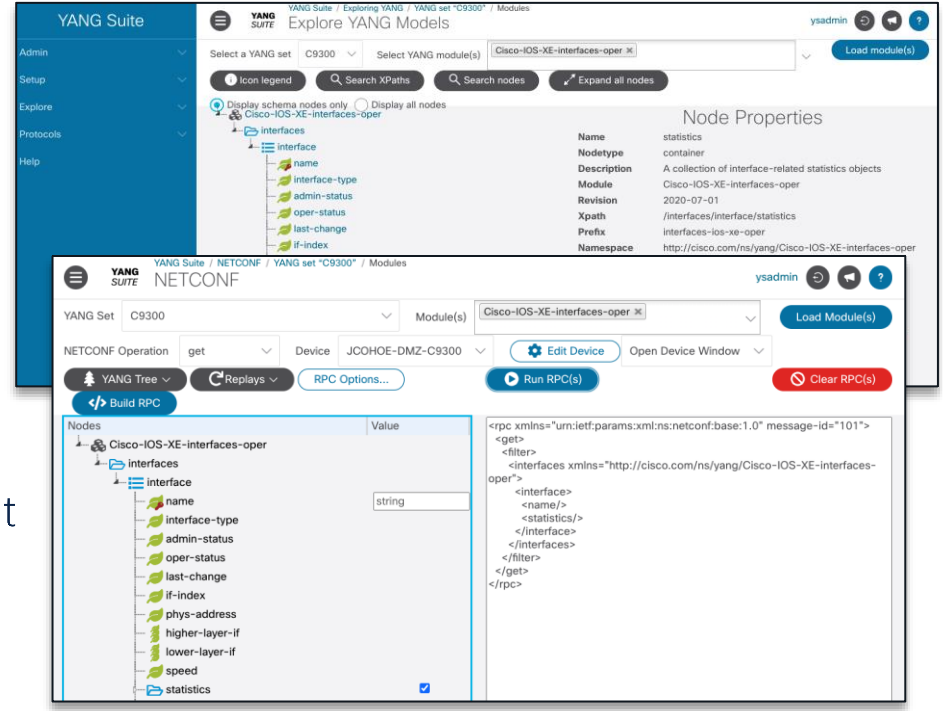
```
Cisco-IOS-XE-cli-rpc
  config-ios-cli-rpc
    input
      config-clis
      timeout
      error-patterns
    output
  config-ios-cli-trans
    input
      clis
      do-commit
    output
```

Getting Started:

1. Select a YANG set from the dropdown menu at left.
2. Select one or more YANG modules from this set above, then click the "Load module(s)" button.
3. In the tree that appears to the left, you can explore the model(s) by expanding the tree.
4. Click on any of the nodes in the tree to view its properties and relevant RFC information in this space.
5. You can also right-click on any node for a context menu with additional options.

Cisco YANG Suite

- YANG API Testing and Validation Environment
  - Construct and test YANG based APIs over NETCONF, RESTCONF, gRPC and gNMI
    - IOS XE / IOS XR / NX OS platforms



Select a YANG set: C9300
Select YANG module(s): Cisco-IOS-XE-interfaces-oper ×

● Display schema nodes only ○ Display all nodes

Node Properties

Name	statistics
Nodetype	container
Description	A collection of interface-related statistics objects
Module	Cisco-IOS-XE-interfaces-oper
Revision	2020-07-01
Xpath	/interfaces/interface/statistics
Prefix	interfaces-ios-xe-oper
Namespace	http://cisco.com/ns/yang/Cisco-IOS-XE-interfaces-oper

YANG Set: C9300
Module(s): Cisco-IOS-XE-interfaces-oper ×
NETCONF Operation: get
Device: JCOHOE-DMZ-C9300

name: string
statistics: ☑

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <get>
    <filter>
      <interfaces xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-interfaces-
oper">
        <interface>
          <name/>
          <statistics/>
        </interface>
      </interfaces>
    </filter>
  </get>
</rpc>
```

Now Generally Available !

developer.cisco.com/yangsuite

github.com/CiscoDevNet/yangsuite

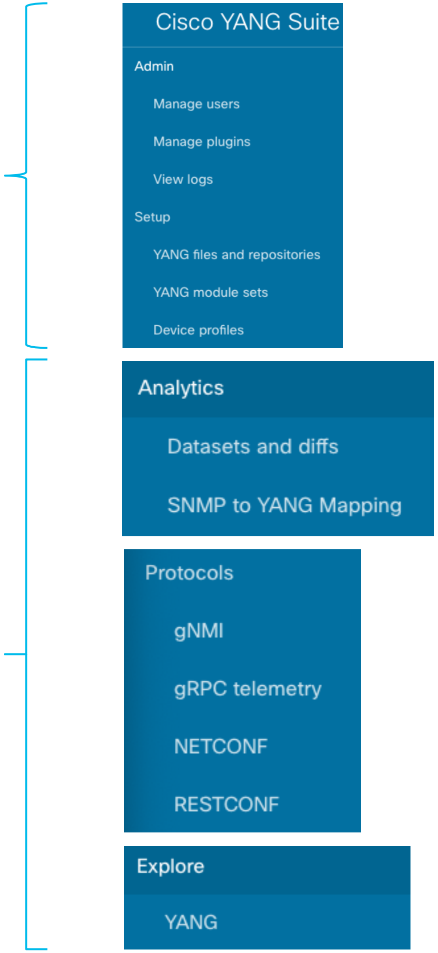
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

What’s Included

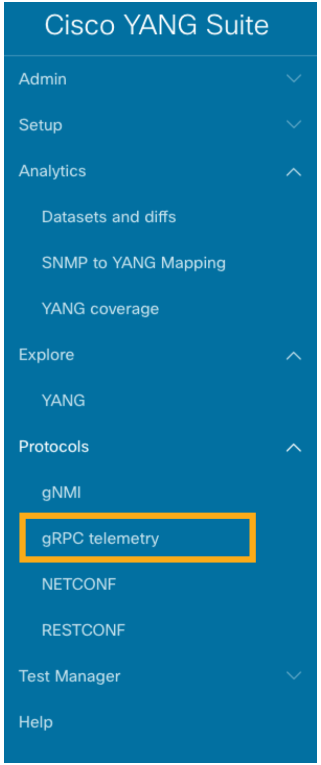
- Initial Release:
  - Plugin Manager
  - YANG File Manager
  - Device Manager
  - NETCONF (Python), gRPC Telemetry
  - Docker install support with HTTPS
- Second Release:
  - RESTCONF
  - gNMI
  - Python Integrations
- Third Release:
  - gRPC Telemetry with TLS Support
  - SNMP OID to YANG Xpath Mapping
  - Ansible Integrations
  - Pip install support

Core plugins

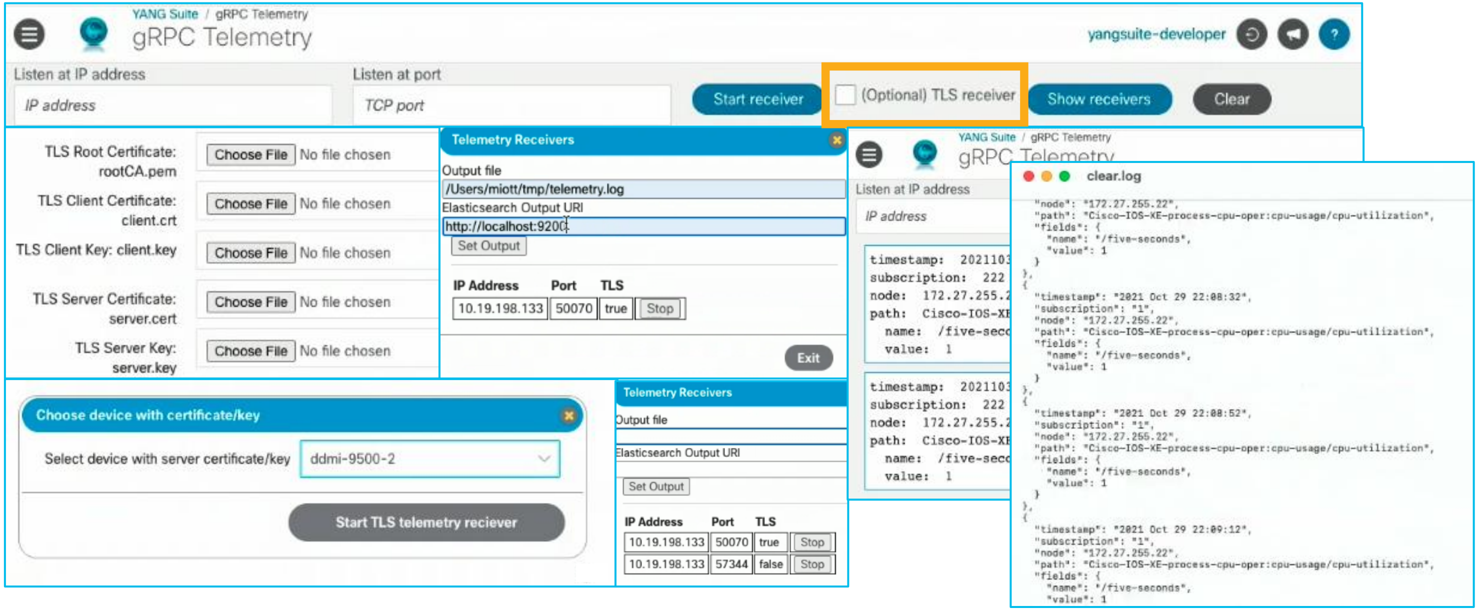
Additional plugins



gRPC Dial-Out with TLS Support



- Server Certificate and Key can now be provided within the Device Profile
  These certificates are used to secure the model driven telemetry data between YANG Suite and IOS XE
- Additional telemetry data outputs to file and Elasticsearch
- Multiple receivers are supported



Listen at IP address: IP address

Listen at port: TCP port

TLS Root Certificate: rootCA.pem — No file chosen

TLS Client Certificate: client.crt — No file chosen

TLS Client Key: client.key — No file chosen

TLS Server Certificate: server.cert — No file chosen

TLS Server Key: server.key — No file chosen

Telemetry Receivers

Output file: /Users/miott/tmp/telemetry.log

Elasticsearch Output URI: http://localhost:9200

IP Address	Port	TLS	
10.19.198.133	50070	true	Stop

Choose device with certificate/key

Select device with server certificate/key: ddmi-9500-2

Telemetry Receivers

Output file

Elasticsearch Output URI

IP Address	Port	TLS	
10.19.198.133	50070	true	Stop
10.19.198.133	57344	false	Stop

Listen at IP address: IP address

```
timestamp:  202110
subscription:  222
node:  172.27.255.2
path:  Cisco-IOS-XE
  name:  /five-seco
  value:  1
```

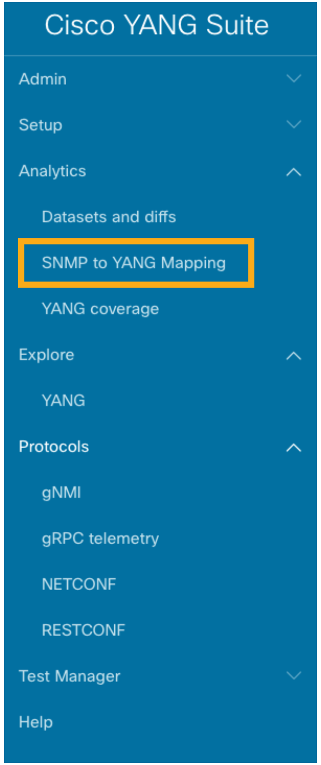
```
timestamp:  202110
subscription:  222
node:  172.27.255.2
path:  Cisco-IOS-XE
  name:  /five-seco
  value:  1
```

clear.log

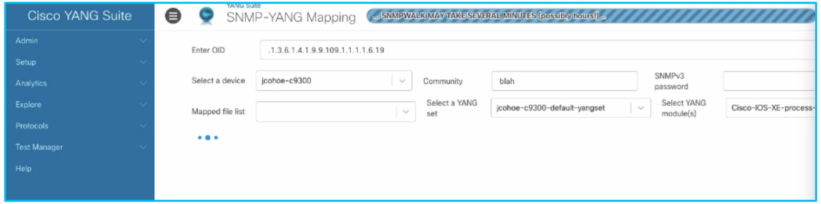
```
  "node": "172.27.255.22",
  "path": "Cisco-IOS-XE-process-cpu-oper:cpu-usage/cpu-utilization",
  "fields": {
    "name": "/five-seconds",
    "value": 1
  }
},
{
  "timestamp": "2021 Oct 29 22:08:32",
  "subscription": "1",
  "node": "172.27.255.22",
  "path": "Cisco-IOS-XE-process-cpu-oper:cpu-usage/cpu-utilization",
  "fields": {
    "name": "/five-seconds",
    "value": 1
  }
},
{
  "timestamp": "2021 Oct 29 22:08:52",
  "subscription": "1",
  "node": "172.27.255.22",
  "path": "Cisco-IOS-XE-process-cpu-oper:cpu-usage/cpu-utilization",
  "fields": {
    "name": "/five-seconds",
    "value": 1
  }
},
{
  "timestamp": "2021 Oct 29 22:09:12",
  "subscription": "1",
  "node": "172.27.255.22",
  "path": "Cisco-IOS-XE-process-cpu-oper:cpu-usage/cpu-utilization",
  "fields": {
    "name": "/five-seconds",
    "value": 1
```

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

SNMP to YANG migration mapping



Ease the transition from SNMP OID to YANG Xpath and easily verify the responses from both.



Enter OID .1.3.6.1.4.1.9.9.109.1.1.1.1.6.19

Select a device jcohoe-c9300

Community blah

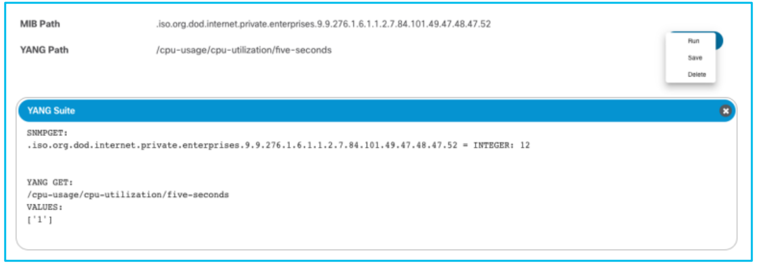
SNMPv3 password

Mapped file list

Select a YANG set jcohoe-c9300-default-yangset

Select YANG module(s) Cisco-IOS-XE-process-

OID: .1.3.6.1.4.1.9.9.109.1.1.1.1.6.19



MIB Path .iso.org.dod.internet.private.enterprises.9.9.276.1.6.1.1.2.7.84.101.49.47.48.47.52

YANG Path /cpu-usage/cpu-utilization/five-seconds

```
SNMPGET:
.iso.org.dod.internet.private.enterprises.9.9.276.1.6.1.1.2.7.84.101.49.47.48.47.52 = INTEGER: 12


YANG GET:
/cpu-usage/cpu-utilization/five-seconds
VALUES:
['1']
```

Right click > Run to retrieve from SNMP and NETCONF simultaneously.

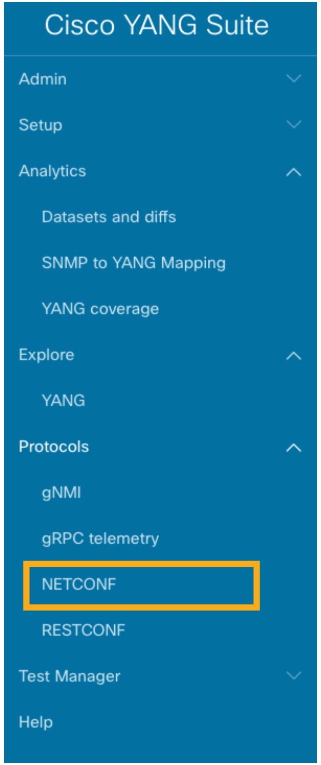
This solution utilizes the Python library for "fuzzy matching" of OID and XPATH values to identify most accurate match.

Please share any SNMP OID's to help validate the mapping and tooling
https://app.smartsheet.com/b/form/f45486e0a3da4cb5905d3a7d788388a0

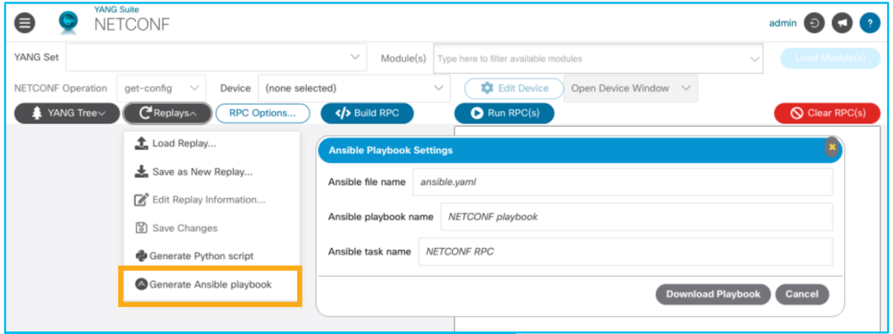
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

YANG Suite + Ansible integrations

using NETCONF, RESTCONF & gNMI OpenConfig



Quickly and easily generate Ansible playbook for deployments to be used with the inventory, similar to the "Generate Python script" button.

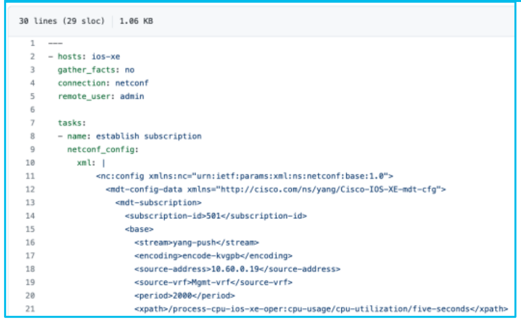


Ansible Playbook Settings

Ansible file name: ansible.yaml

Ansible playbook name: NETCONF playbook

Ansible task name: NETCONF RPC



30 lines (29 sloc) | 1.06 KB

```
---
- hosts: ios-xe
  gather_facts: no
  connection: netconf
  remote_user: admin

  tasks:
  - name: establish subscription
    netconf_config:
      xml: |
          <nc:config xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
            <mdt-config-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-mdt-cfg">
              <mdt-subscription>
                <subscription-id>501</subscription-id>
                <base>
                  <stream>yang-push</stream>
                  <encoding>encode-kvgpb</encoding>
                  <source-address>10.60.0.19</source-address>
                  <source-vrf>Mgmt-vrf</source-vrf>
                  <period>2000</period>
                  <xpath>/process-cpu-ios-xe-oper:cpu-usage/cpu-utilization/five-seconds</xpath>
```

Restrictions for gNMI

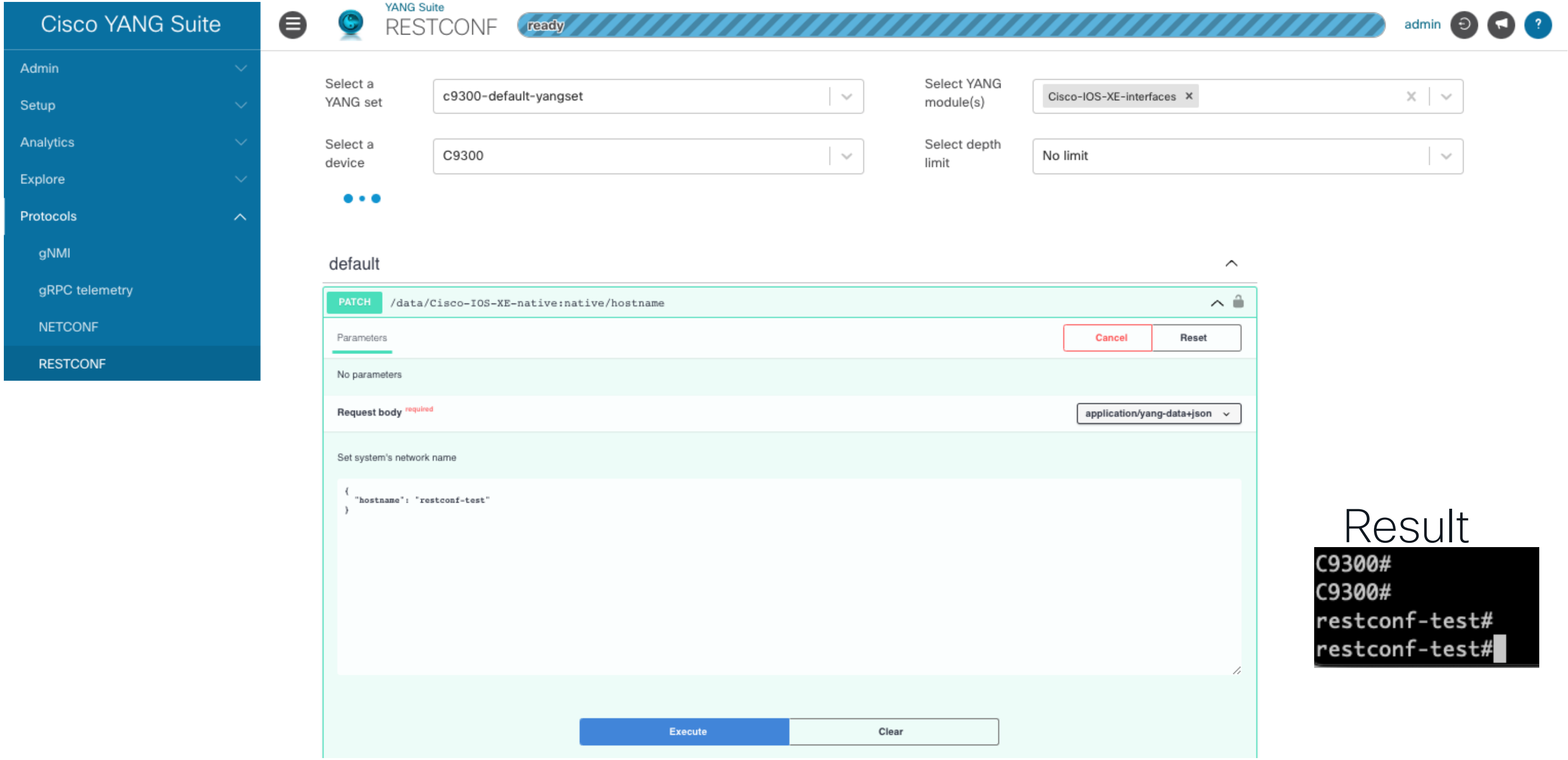
For OpenConfig YANG only

Using 3rd party plugin to Ansible from Nokia

```
$ ansible-galaxy collection install nokia.grpc
```

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

RESTCONF + Ansible



Select a YANG set: c9300-default-yangset

Select YANG module(s): Cisco-IOS-XE-interfaces

Select a device: C9300

Select depth limit: No limit

default

PATCH /data/Cisco-IOS-XE-native:native/hostname

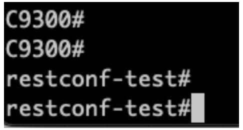
No parameters

Request body required application/yang-data+json

Set system's network name

```
{
  "hostname": "restconf-test"
}
```

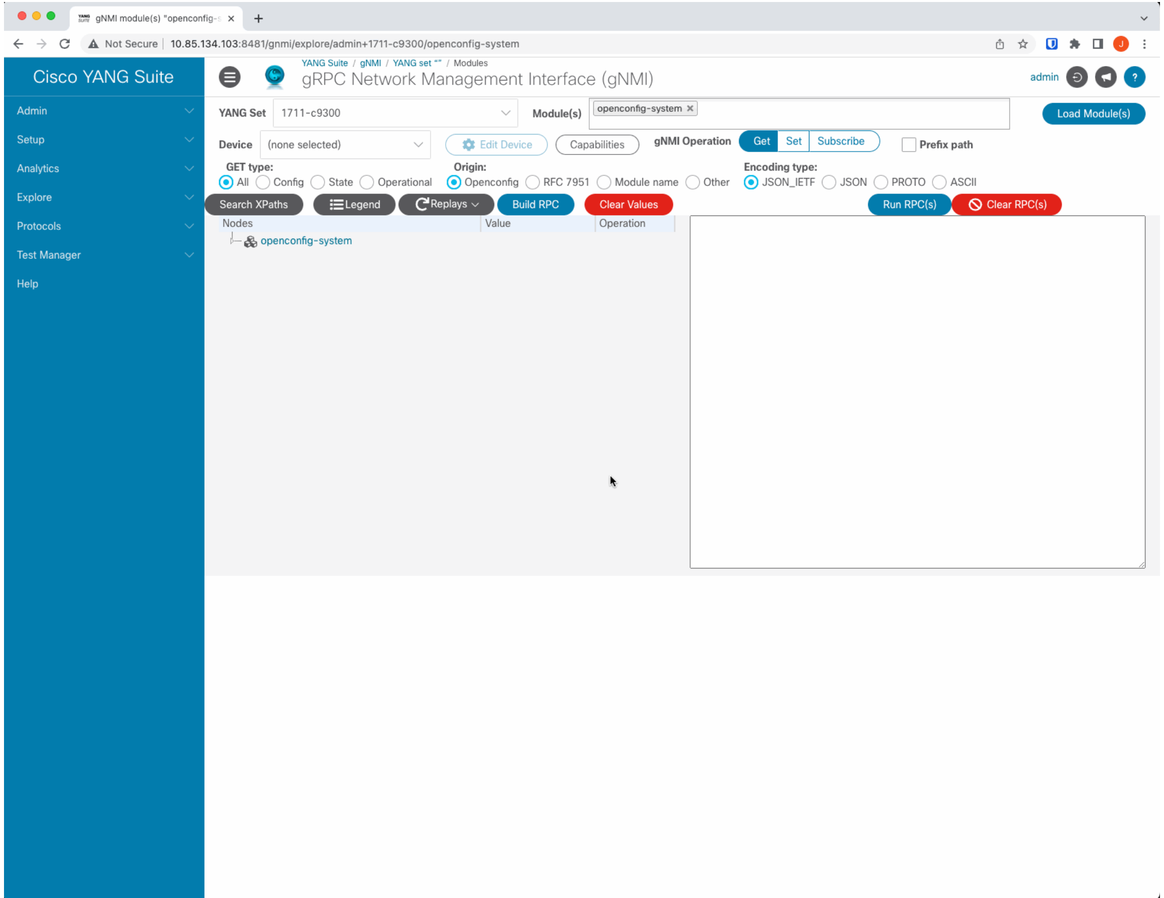
Result



```
C9300#
C9300#
restconf-test#
restconf-test#
```

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

gNMI + Ansible demo



YANG Set: 1711-c9300

Module(s): openconfig-system

Device: (none selected)

gNMI Operation: [✓ Get] Set Subscribe

□ Prefix path

GET type: ● All ○ Config ○ State ○ Operational

Origin: ● Openconfig ○ RFC 7951 ○ Module name ○ Other

Encoding type: ● JSON_IETF ○ JSON ○ PROTO ○ ASCII

Pip install support

Requirements:

- 64-bit Windows10, Mac, Ubuntu, CentOS, or FreeBSD support
- 8 GB Memory Requirement, Python 3
- Prerequisite: pip3 in Linux and Windows

```
pip3 install yangsuite
```

Ensure pre-requisites are installed

Ubuntu Linux example:

```
$ apt-get install git openssh-client iputils-ping python3.6 python3-pip sqlite3 snmp
```

Windows:

```
install python3 and python3-pip from python.org
```

Mac

```
Make sure python3 is installed
```

The Python Package Index (PyPI) is a repository of software for Python
https://pypi.org/project/yangsuite/

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

YANG Suite Resources

Blogs

March 8, 2021 3 Comments

Developer

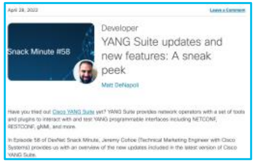
The Wait Is Over: Cisco YANG Suite Is Here!

Jeremy Cohoe

This blog is authored by Jeremy Cohoe and Kareem Iskander

As Cisco platforms (IOS XE, IOS XR, NX-OS) continue to support IETF, OpenConfig, and Cisco Native YANG models, we needed to develop a tool to help make the lives of network automation engineers easier!

https://blogs.cisco.com/developer/363-yangsuite-01



April 28, 2022 Leave a Comment

Snack Minute #58

Developer

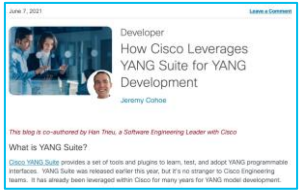
YANG Suite updates and new features: A sneak peek

Matt DeNapoli

Have you tried out Cisco YANG Suite yet? YANG Suite provides network operators with a set of tools and plugins to interact with and test YANG programmable interfaces including NETCONF, RESTCONF, gNMI, and more.

In Episode 58 of DevNet Snack Minute, Jeremy Cohoe (Technical Marketing Engineer with Cisco Systems) provides us with an overview of the new updates included in the latest version of Cisco YANG Suite.

https://blogs.cisco.com/developer/2022yangsuiteupdatesfeatures01



June 7, 2021 Leave a Comment

Developer

How Cisco Leverages YANG Suite for YANG Development

Jeremy Cohoe

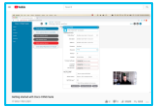
This blog is co-authored by Han Trieu, a Software Engineering Leader with Cisco

What is YANG Suite?

Cisco YANG Suite provides a set of tools and plugins to learn, test, and adopt YANG programmable interfaces. YANG Suite was released earlier this year, but it's no stranger to Cisco Engineering teams. It has already been leveraged within Cisco for many years for YANG model development.

https://blogs.cisco.com/developer/leverageyangsuite01?dtid=osscdc000283

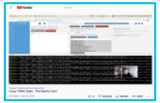
YouTube Videos



https://youtu.be/smrhjL5Ayz0

https://www.youtube.com/watch?v=dTun33611JA

https://www.youtube.com/watch?v=soyWPr0fJ0s



https://www.youtube.com/watch?v=PkbAOzZ1vNk

https://www.youtube.com/watch?v=3zmNDfn8b38

Additional Resources

https://github.com/CiscoDevNet/yangsuite/

https://developer.cisco.com/yangsuite/

https://eurl.io/#MaW78CeIS YANG Suite General (external)

Terraform

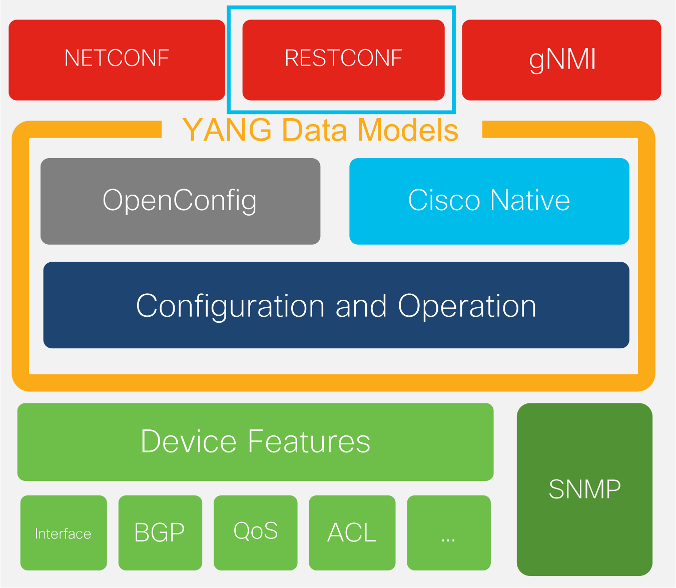
Terraform is…

Open-source Infrastructure as Code (IaC) Software Tool providing a consistent CLI workflow to manage hundreds of cloud services. Terraform codifies cloud APIs into declarative configuration files.

- Cloud Native Tooling circa 2014 from HashiCorp
- Agentless, single binary file
- Zero server-side dependencies

Resources:
Ask IOS XE Terraform Provider Webex space: https://eurl.io/#PtsT8eJFI
GitHub Provider Examples: https://github.com/CiscoDevNet/terraform-provider-iosxe/
Provider Binary: https://registry.terraform.io/search/providers?namespace=CiscoDevNet
Go Client: https://github.com/CiscoDevNet/iosxe-go-client
Blogs at https://blogs.cisco.com/tag/terraform

Terraform uses the RESTCONF API



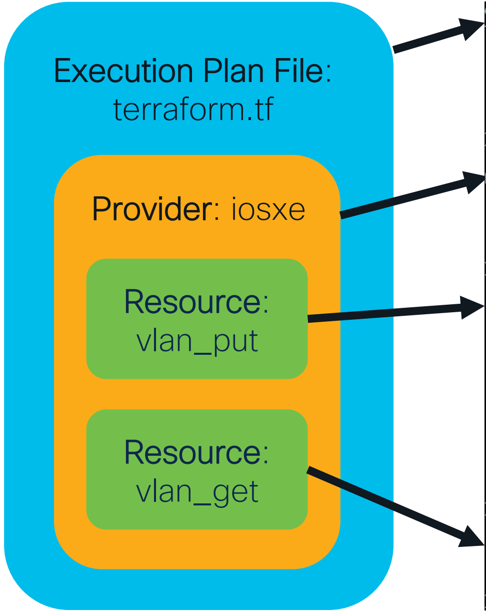
Terraform Terminology

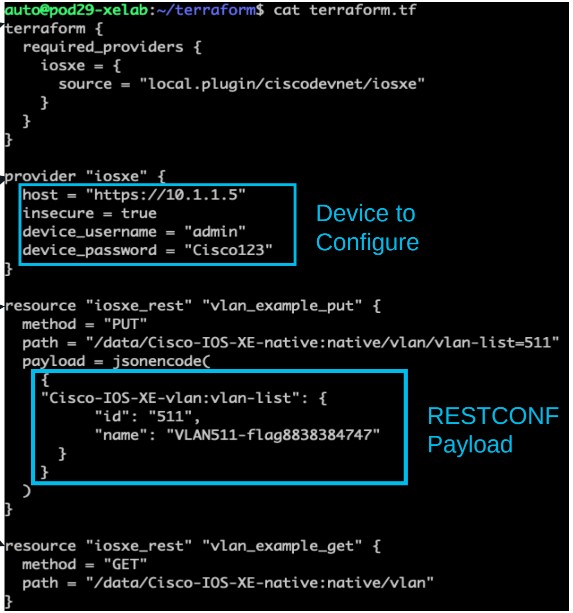
Terraform uses an execution plan file with a provider and resource definitions

An execution plan file defines the provider and resources. It is written in HashiCorp Configuration Language (HCL), similar to JSON, and stored with a .tf extension

A provider is a plugin to make a collection of resources accessible

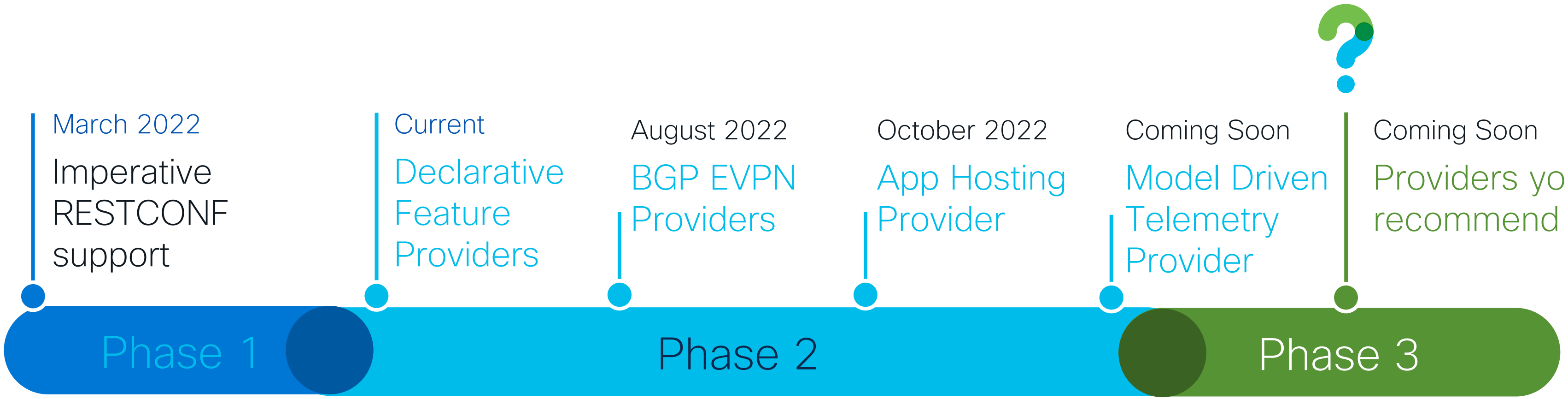
A resource (or infrastructure resource) describes one or more infrastructure objects managed by Terraform. With the IOS XE Terraform provider, resources can be considered the same as a configurable feature





```
auto@pod29-xelab:~/terraform$ cat terraform.tf
terraform {
  required_providers {
    iosxe = {
      source = "local.plugin/ciscodevnet/iosxe"
    }
  }
}

provider "iosxe" {
  host = "https://10.1.1.5"
  insecure = true
  device_username = "admin"
  device_password = "Cisco123"
}

resource "iosxe_rest" "vlan_example_put" {
  method = "PUT"
  path = "/data/Cisco-IOS-XE-native:native/vlan/vlan-list=511"
  payload = jsonencode(
    {
    "Cisco-IOS-XE-vlan:vlan-list": {
          "id": "511",
          "name": "VLAN511-flag8838384747"
      }
    }
  )
}

resource "iosxe_rest" "vlan_example_get" {
  method = "GET"
  path = "/data/Cisco-IOS-XE-native:native/vlan"
}
```

Evolution of Terraform Provider



March 2022

Imperative RESTCONF support

Current

Declarative Feature Providers

August 2022

BGP EVPN Providers

October 2022

App Hosting Provider

Coming Soon

Model Driven Telemetry Provider

Coming Soon

Providers you recommend

https://registry.terraform.io/providers/CiscoDevNet/iosxe/latest

https://registry.terraform.io/providers/robertcsapo/ciscoevpn/1.0.1

https://registry.terraform.io/providers/netascode/iosxe/latest/docs

https://github.com/netascode/terraform-iosxe-evpn-example

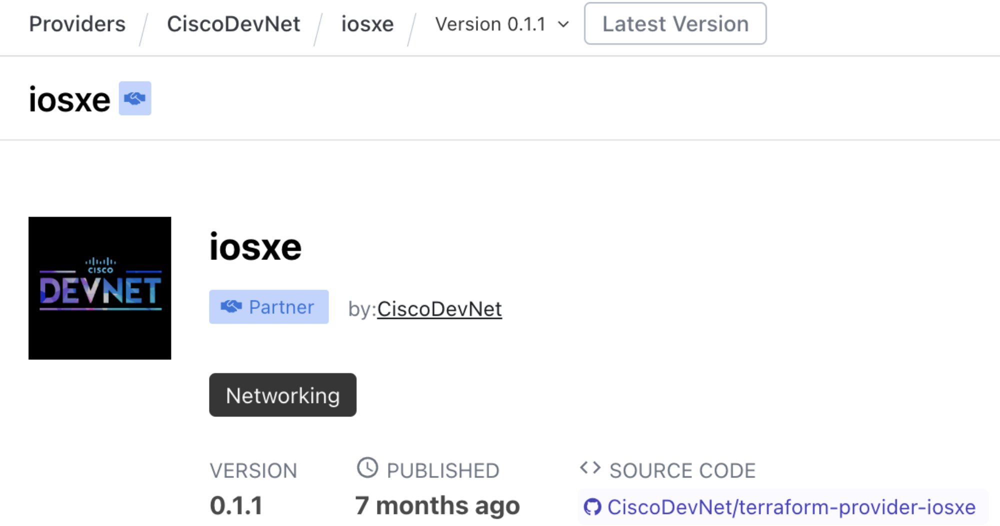
https://github.com/robertcsapo/terraform-provider-ciscoapphosting/tree/main/

Declarative providers leverage the SDK from the Phase 1 imperative provider

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Terraform use and adoption

We continue to see increased adoption of the IOS XE terraform resources



Providers / CiscoDevNet / iosxe / Version 0.1.1 ⌄ Latest Version

iosxe

iosxe

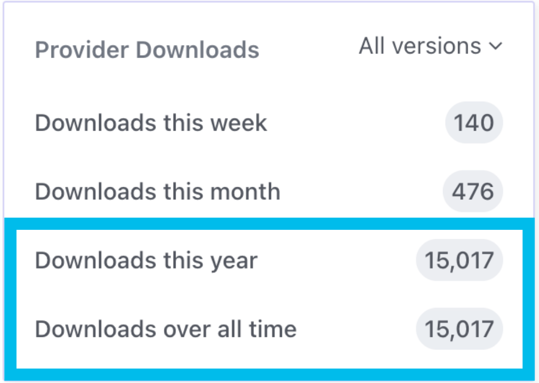
Partner by:CiscoDevNet

Networking

VERSION
0.1.1

PUBLISHED
7 months ago

SOURCE CODE
CiscoDevNet/terraform-provider-iosxe



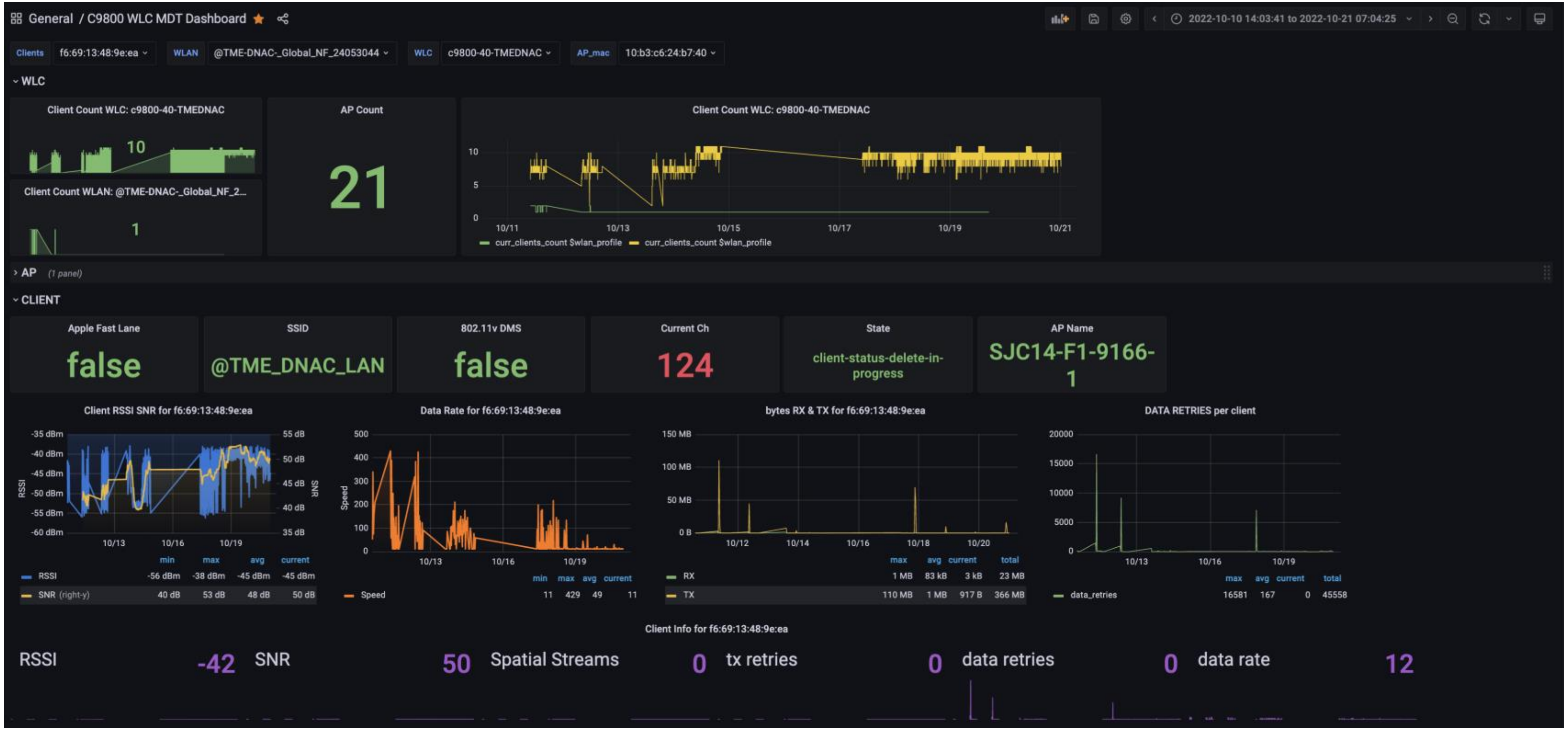
Provider Downloads	All versions ⌄
Downloads this week	140
Downloads this month	476
Downloads this year	15,017
Downloads over all time	15,017

https://registry.terraform.io/providers/CiscoDevNet/iosxe/0.1.1

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Model Driven Telemetry Telegraf, InfluxDB and Grafana (TIG) Docker

Grafana Demo Dashboard: C9800 Wireless



General / C9800 WLC MDT Dashboard

2022-10-10 14:03:41 to 2022-10-21 07:04:25

Clients: f6:69:13:48:9e:ea

WLAN: @TME-DNAC-_Global_NF_24053044

WLC: c9800-40-TMEDNAC

AP_mac: 10:b3:c6:24:b7:40

WLC

Client Count WLC: c9800-40-TMEDNAC: 10

Client Count WLAN: @TME-DNAC-_Global_NF_2...: 1

AP Count: 21

Client Count WLC: c9800-40-TMEDNAC

AP (1 panel)

CLIENT

Apple Fast Lane	SSID	802.11v DMS	Current Ch	State	AP Name
false	@TME_DNAC_LAN	false	124	client-status-delete-in-progress	SJC14-F1-9166-1

Client RSSI SNR for f6:69:13:48:9e:ea

	min	max	avg	current
RSSI	-56 dBm	-38 dBm	-45 dBm	-45 dBm
SNR (right-y)	40 dB	53 dB	48 dB	50 dB

Data Rate for f6:69:13:48:9e:ea

	min	max	avg	current
Speed	11	429	49	11

bytes RX & TX for f6:69:13:48:9e:ea

	max	avg	current	total
RX	1 MB	83 kB	3 kB	23 MB
TX	110 MB	1 MB	917 B	366 MB

DATA RETRIES per client

	max	avg	current	total
data_retries	16581	167	0	45558

Client Info for f6:69:13:48:9e:ea

RSSI	SNR	Spatial Streams	tx retries	data retries	data rate
-42	50	0	0	0	12

https://grafana.com/grafana/dashboards/12468-catalyst-9800-client-stats/

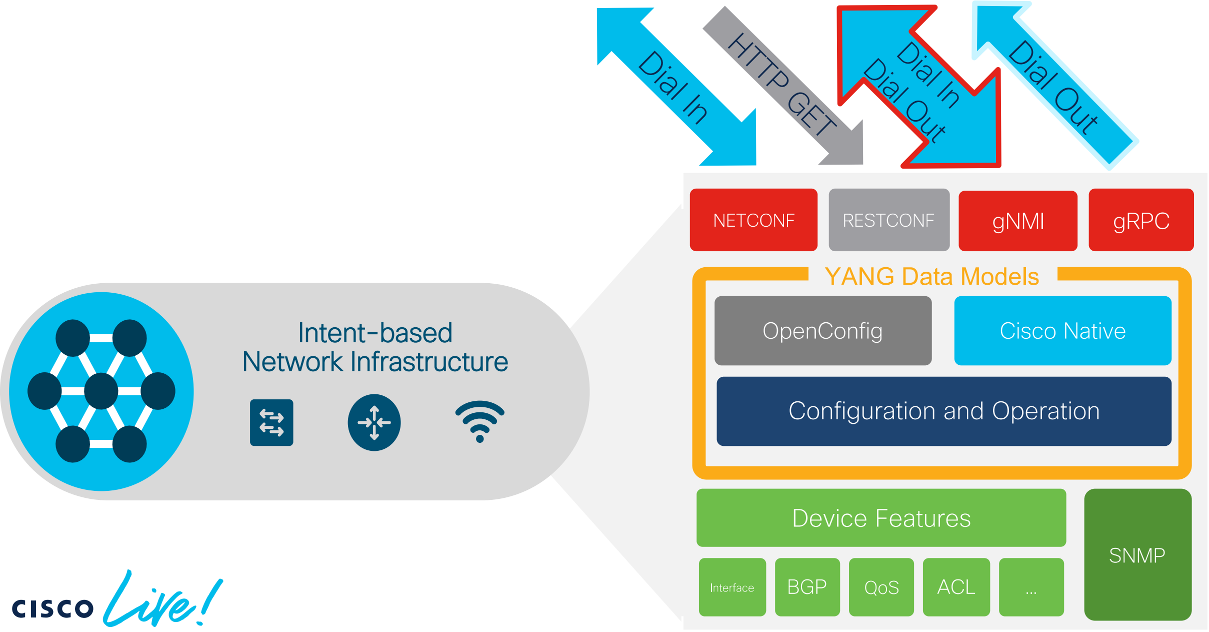
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Model Driven Telemetry Interfaces

⟷ Dial In: Collector establishes a connection to the device then subscribes to telemetry (pub/sub)

⟵ Dial Out: Telemetry is pushed from the device to the collector based off configuration (push)

Publication / Subscription



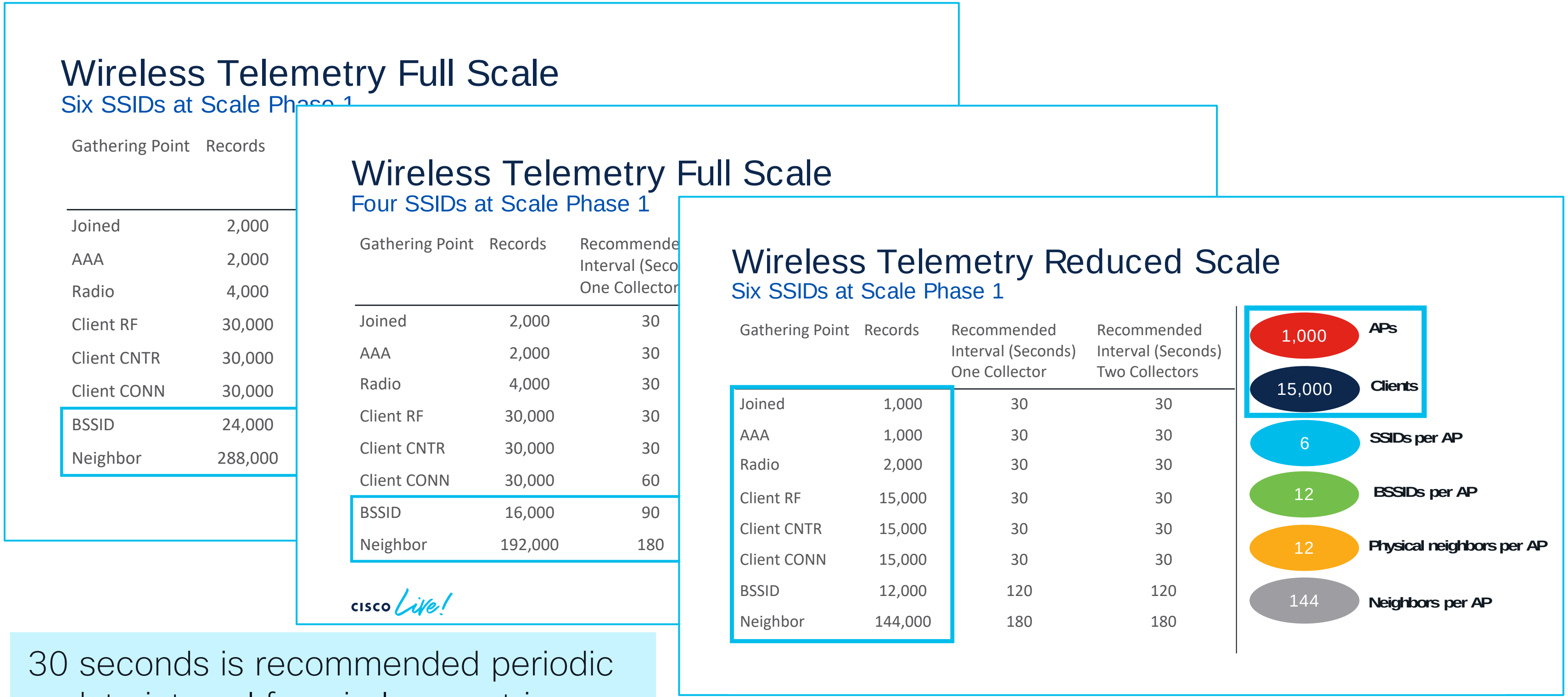
XML, JSON, proto and kvGPB encoding

Consistent YANG data models between interfaces

On-change event and time-based publication options

Innovations in wireless Telemetry

Source: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/178/b_178_programmability_cg/m_178_prog_ietf_telemetry.html



Wireless Telemetry Full Scale

Six SSIDs at Scale Phase 1

Gathering Point	Records
Joined	2,000
AAA	2,000
Radio	4,000
Client RF	30,000
Client CNTR	30,000
Client CONN	30,000
BSSID	24,000
Neighbor	288,000

Wireless Telemetry Full Scale

Four SSIDs at Scale Phase 1

Gathering Point	Records	Recommende Interval (Seco One Collector
Joined	2,000	30
AAA	2,000	30
Radio	4,000	30
Client RF	30,000	30
Client CNTR	30,000	30
Client CONN	30,000	60
BSSID	16,000	90
Neighbor	192,000	180

cisco Live!

Wireless Telemetry Reduced Scale

Six SSIDs at Scale Phase 1

Gathering Point	Records	Recommended Interval (Seconds) One Collector	Recommended Interval (Seconds) Two Collectors
Joined	1,000	30	30
AAA	1,000	30	30
Radio	2,000	30	30
Client RF	15,000	30	30
Client CNTR	15,000	30	30
Client CONN	15,000	30	30
BSSID	12,000	120	120
Neighbor	144,000	180	180

1,000	APs
15,000	Clients
6	SSIDs per AP
12	BSSIDs per AP
12	Physical neighbors per AP
144	Neighbors per AP

30 seconds is recommended periodic update interval for wireless metrics

cisco Live!

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Model Driven Telemetry

IOS XE Model Driven Telemetry

Cisco IOS XE

CLI

...or with...

YANG

pyATS

ANSIBLE

NSO

Terraform

gNMI Dial-In/Dynamic
NETCONF Dial-In

gRPC Dial-Out/Configured

Collector/Receiver
Decodes to text

telegraf

elastic

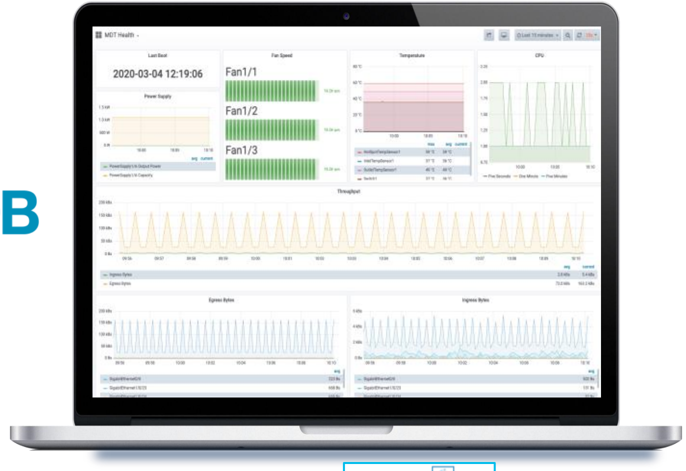
Storage
Time Series Database

splunk>

InfluxDB

Monitoring
and Visualizations

Grafana



https://hub.docker.com/r/jeremycohoe/tig_mdt https://github.com/jeremycohoe/cisco-ios-xe-mdt
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/179/b_179_programmability_cg/m_179_prog_ietf_telemetry.html

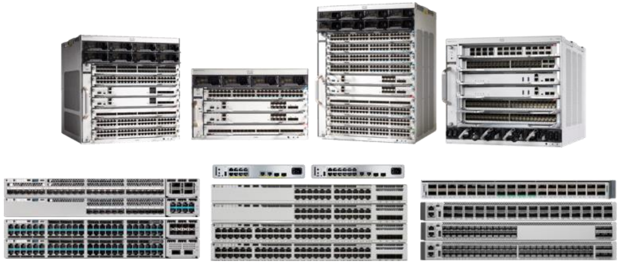
Model Driven Telemetry

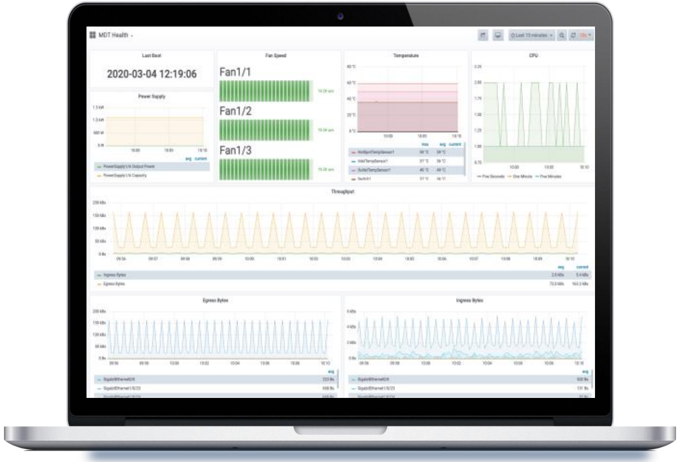
Updates to the TIG_MDT container

Upgrade coming to Telegraf, Influx, and Grafana Model Driven Telemetry (TIG_MDT) Docker container
Making it easier to consume telemetry in production

Upgraded Telegraf, InlfuxDB, and Grafana tools
Additional dashboards for
Device Health, Wireless Client, Wireless AP, RF etc
Examples for device CLI configuration for telemetry
Details of scale and data storage requirements

```
docker pull jeremycohoe/tig_mdt
docker run -ti -p 3000:3000 -p 57500:57500 jeremycohoe/tig_mdt
```





Collector/Receiver
Decodes to text

telegraf™

Storage
Time Series Database

InfluxDB

Monitoring and Visualizations

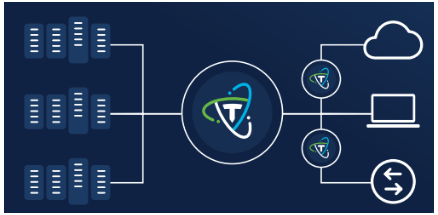
Grafana

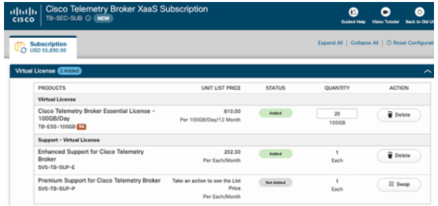
https://hub.docker.com/r/jeremycohoe/tig_mdt https://github.com/jeremycohoe/cisco-ios-xe-mdt
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/179/b_179_programmability_cg/m_179_prog_ietf_telemetry.html

Cisco Telemetry Data Broker (Telegraf)

Cisco Telemetry Broker provides many benefits include brokering, filtering, and transforming data. It provides the ability to replicate telemetry data.

- Cisco Secure Network Analytics (Stealthwatch) UDP Director (UDPD) replicates UDP traffic to multiple destinations.
- Cisco Telemetry Broker
  - Builds upon UDPD
  - Optimizes telemetry pipelines for the hybrid cloud
  - Simplifies the consumption of telemetry data for customers' business-critical tools by brokering hybrid cloud data, filtering unneeded data, and transforming data to a usable format





Cisco Telemetry Broker XaaS Subscription
TB-SEC-SUB NEW

Subscription
USD 55,890.00

Virtual License 2 Added

PRODUCTS	UNIT LIST PRICE	STATUS	QUANTITY	ACTION
Virtual License				
Cisco Telemetry Broker Essential License - 100GB/Day TB-ESS-100GB SA	810.00 Per 100GB/Day/12 Month	Added	20 100GB	Delete
Support - Virtual License				
Enhanced Support for Cisco Telemetry Broker SVS-TB-SUP-E	202.50 Per Each/Month	Added	1 Each	Delete
Premium Support for Cisco Telemetry Broker SVS-TB-SUP-P	Take an action to see the List Price Per Each/Month	Not Added	1 Each	Swap

▶ **Brokering Data:**
The ability to route and replicate telemetry data from a source location to multiple destination consumers.

Quickly onboard new telemetry-based tools!

▶ **Filtering Data:**
The ability to filter data that is being replicated to consumers for fine grain control over what consumers are able to see and analyze.

Save money sending data to expensive tools!

▶ **Transforming Data:**
The ability to transform data protocols from the exporter to the consumer's protocol of choice.

Enable tools to consume multiple data formats!

https://cs.co/telemetrybroker aka https://www.cisco.com/c/en/us/products/security/telemetry-broker/index.html
https://blogs.cisco.com/security/taking-full-control-of-your-telemetry-with-the-intelligent-telemetry-plane

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Model Driven Telemetry Interface Comparison

	NETCONF	gRPC Dial-Out	gNMI Dial-In	gNMI Dial-Out
Minimum IOS XE Version	16.6	16.10	16.12	17.11
Recommended Version	17.9	17.9	17.9	17.11
Telemetry Direction	Dial-In, IOS XE is server	Dial-Out IOS XE is client	Dial-In IOS XE is server	Dial-Out
Configuration	Dynamic per session	Static per configuration	Dynamic per session	Static
Telemetry Collector	Client	Server	Client	Server
Encoding	XML	KV GPB	JSON_IETF	PROTO + JSON_IETF
Security	SSH + PKI certificate or password	TLS or plain-text	TLS certificate with user authentication	Same
Transport Protocol	SSH	HTTP2	HTTP2	Same
Data Models	YANG	YANG	YANG	YANG

Network architecture, security posture and policy, YANG data modules, tools and language preferences are some considerations when leveraging the various MDT interfaces

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

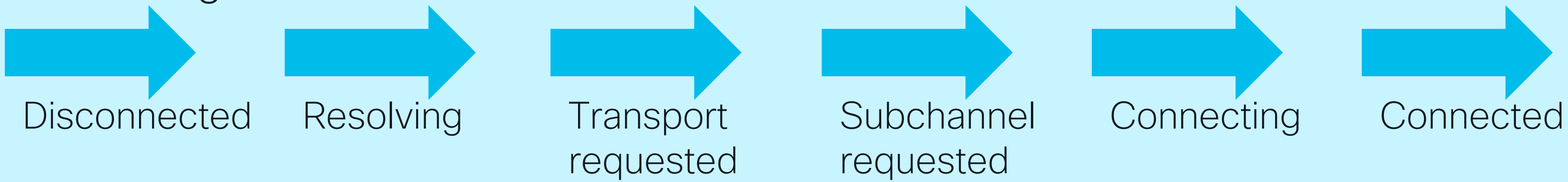
Scalable and Secure Model Driven Telemetry in production

- TIG_MDT update
- gRPC feature HA
- DNS resolver HA
- Cloud Collection HA

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

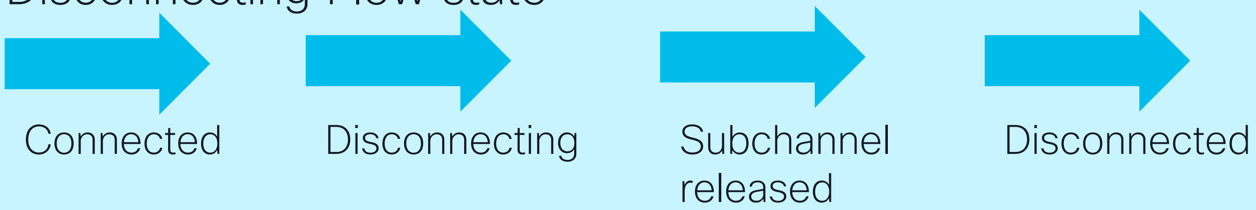
gRPC Dial-Out: High Availability

Connecting Flow state


Disconnected → Resolving → Transport requested → Subchannel requested → Connecting → Connected

- There is a 15 second delay between Disconnecting and Connecting flow states
- Flow states are per subscription: each individual subscription follows these workflows
- A single IP is resolved for each FQDN based DNS subscription
  - If FQDN resolves to multiple IP only 1 will be used for the connection
  - When multiple subscriptions/xpaths to the same FQDN with multiple IP there will be connections built to each IP provided by DNS

Disconnecting Flow state


Connected → Disconnecting → Subchannel released → Disconnected

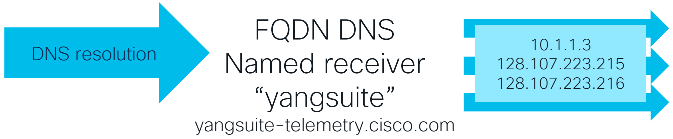
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

gRPC Dial-Out: FQDN DNS Resolver HA

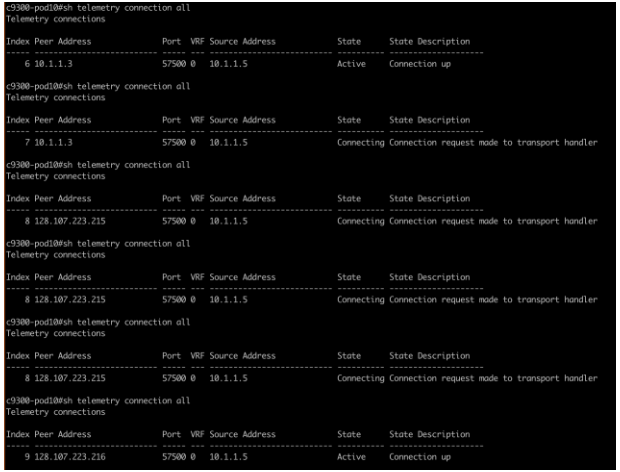
Resolving

Each telemetry subscription resolves the DNS name then connects to the server by IP
When DNS entry has multiple IP's the RFC will be followed and subscriptions will be established to any IP

Sub1 = xpath1
Sub2 = xpath2
Sub3 = xpath3
SubN = xpathN



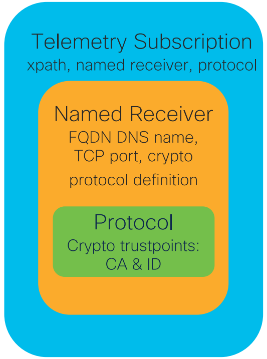
Sub1 resolves yangsuite and connects to 10.1.1.3
Sub2 resolves yangsuite and connects to 128.107.223.215
Sub3 resolves yangsuite and connects to 128.107.223.216
SubN = ip1, ip2, or ip3



```
c9300-pod10#sh telemetry connection all
Telemetry connections

Index Peer Address               Port  VRF Source Address              State      State Description
----- -------------------------- ----- --- -------------------------- ---------- --------------------
    6 10.1.1.3                   57500 0   10.1.1.5                   Active     Connection up

c9300-pod10#sh telemetry connection all
Telemetry connections

Index Peer Address               Port  VRF Source Address              State      State Description
----- -------------------------- ----- --- -------------------------- ---------- --------------------
    7 10.1.1.3                   57500 0   10.1.1.5                   Connecting Connection request made to transport handler

c9300-pod10#sh telemetry connection all
Telemetry connections

Index Peer Address               Port  VRF Source Address              State      State Description
----- -------------------------- ----- --- -------------------------- ---------- --------------------
    8 128.107.223.215            57500 0   10.1.1.5                   Connecting Connection request made to transport handler

c9300-pod10#sh telemetry connection all
Telemetry connections

Index Peer Address               Port  VRF Source Address              State      State Description
----- -------------------------- ----- --- -------------------------- ---------- --------------------
    8 128.107.223.215            57500 0   10.1.1.5                   Connecting Connection request made to transport handler

c9300-pod10#sh telemetry connection all
Telemetry connections

Index Peer Address               Port  VRF Source Address              State      State Description
----- -------------------------- ----- --- -------------------------- ---------- --------------------
    8 128.107.223.215            57500 0   10.1.1.5                   Connecting Connection request made to transport handler

c9300-pod10#sh telemetry connection all
Telemetry connections

Index Peer Address               Port  VRF Source Address              State      State Description
----- -------------------------- ----- --- -------------------------- ---------- --------------------
    9 128.107.223.216            57500 0   10.1.1.5                   Active     Connection up
```

In this example there is no receiver or collector listening at 128.107.223.215

Some subscriptions will resolve DNS to this IP and be unable to connect
These subscriptions will re-resolve the DNS name to find another IP and connect successfully



```
telemetry protocol grpc profile mtlsyangsuite
  ca-trustpoint myCA
  id-trustpoint myID

telemetry receiver protocol yangsuite
 host name yangsuite-telemetry.cisco.com 57500
 protocol grpc-tls profile mtlsyangsuite

telemetry ietf subscription 1010
 encoding encode-kvgpb
filter xpath /wireless-ble-ltx-oper:ble-ltx-oper-data/ble-ltx-ap-streami
 source-address 10.85.134.83
 stream yang-push
 update-policy periodic 6000
 receiver-type protocol
 receiver name yangsuite
```

There is no limit to the number of IP addresses that telemetry will connect to:
if the DNS entry has 100 IPs defined it will be treated the same as if it has 2 or 4

When using DNS to find the telemetry collector on the internetwork

© 2023 Cisco and/or its affiliates. All rights reserved.

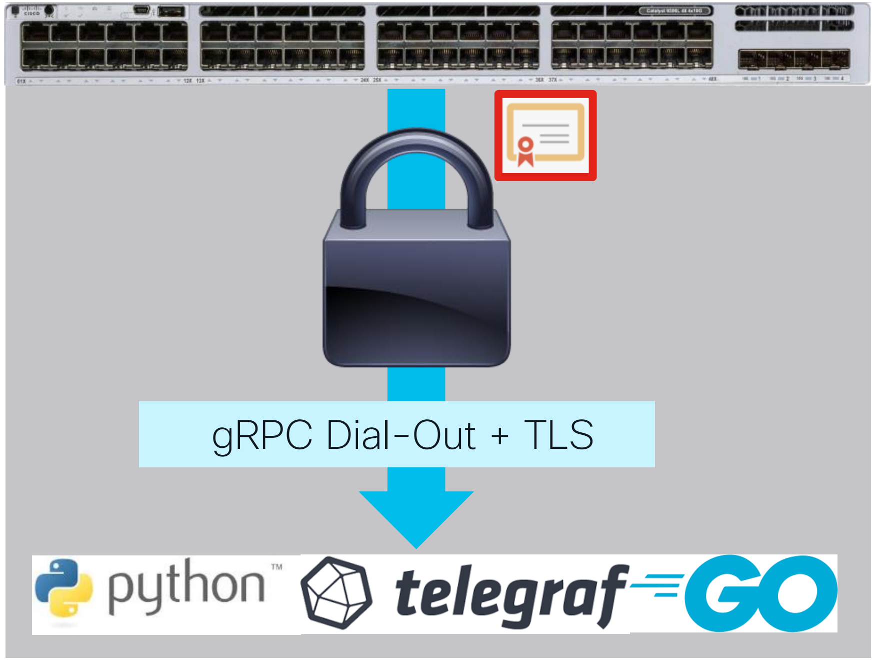
17.2

gRPC Dial-Out with TLS

- NETCONF and gNMI use PKI or TLS certificates for securing the telemetry session
- The Dial-Out gRPC telemetry interface can now be configured to use TLS certificates
- Tooling is available to receive the secured data
- Feature can be configured with up to 100 subscriptions with a mix of secure and plaintext

```
conf t
telemetry ietf subscription 1
 encoding encode-kvgpb
 filter xpath /process-cpu-ios-xe-oper:cpu-usage/cpu-utilization/five-seconds
 source-address 10.60.0.19
 source-vrf Mgmt-vrf
 stream yang-push
 update-policy periodic 2000
 receiver ip address 10.1.1.3 57501 protocol grpc-tls profile myca
```

Profile: create the certificate trustpoint profile ‘crypto pki trustpoint myca’ CLI or YANG or use gNOI cert.proto



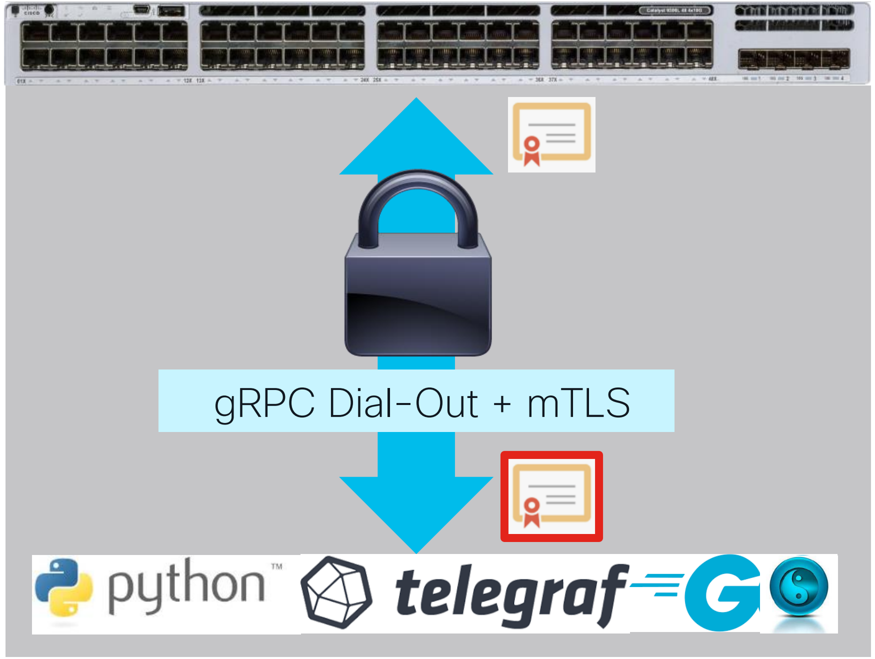
gRPC Dial-Out is a replacement for SNMP traps and can now be used securely

gRPC Dial-Out with mutual TLS (mTLS)

17.9

Ensuring gRPC Dial-Out + DNS + mTLS can be used in production, securely, and with infosec approval

- Enhancement to gRPC Dial-Out TLS secure telemetry to include mTLS
- Previously the client secured the telemetry connection to the server
- Now the server can also validate that the client has the correct certificates



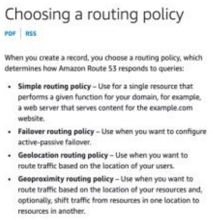
What is mutual TLS (mTLS)?
Mutual TLS, or mTLS for short, is a method for mutual authentication. mTLS ensures that the parties at each end of a network connection are who they claim to be by verifying that they both have the correct private key. The information within their respective TLS certificates provides additional verification.

mTLS is often used in a Zero Trust security framework to verify users, devices, and servers within an organization – it can also help keep APIs secure.

https://www.cloudflare.com/learning/access-management/what-is-mutual-tls/

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Case Study: Telemetry in production

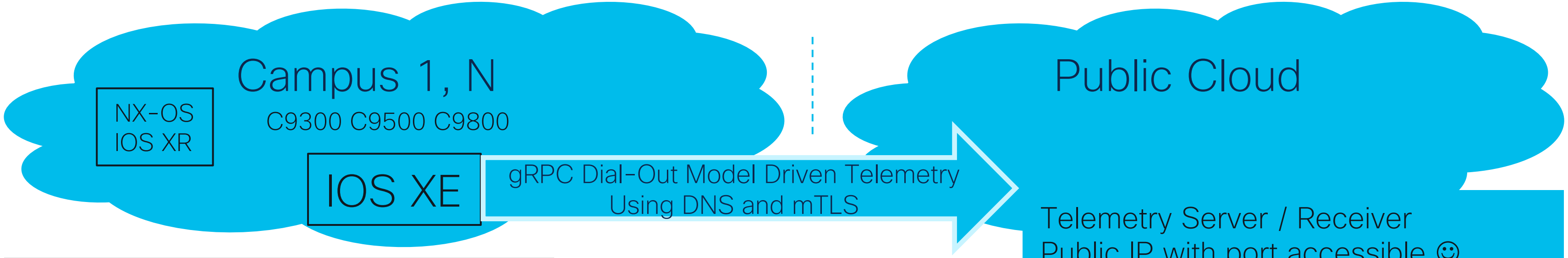


Choosing a routing policy

PDF | RSS

When you create a record, you choose a routing policy, which determines how Amazon Route 53 responds to queries:

- **Simple routing policy** – Use for a single resource that performs a given function for your domain, for example, a web server that serves content for the example.com website.
- **Failover routing policy** – Use when you want to configure active-passive failover.
- **Geolocation routing policy** – Use when you want to route traffic based on the location of your users.
- **Geoproximity routing policy** – Use when you want to route traffic based on the location of your resources and, optionally, shift traffic from resources in one location to resources in another.



Campus 1, N

NX-OS
IOS XR

C9300 C9500 C9800

IOS XE

gRPC Dial-Out Model Driven Telemetry
Using DNS and mTLS

Public Cloud

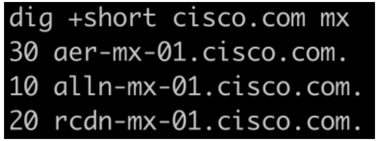
Telemetry Server / Receiver
Public IP with port accessible ☺
Mutual Authentication with mTLS

Cloud native backend data lake
S3, InfluxDB Cloud, etc

15+ Internal Business Customers:
Tooling, NOC/SOC, Dashboards, Charts, Alerts, Reports

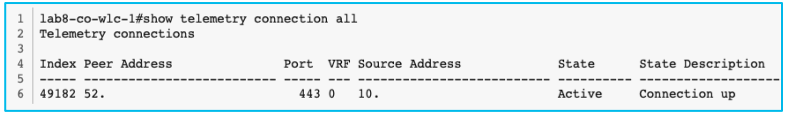
```
C9300#show run | i domain / i name-server
ip name-server 208.67.222.222
ip domain lookup

C9300#show run | sec telemetry
telemetry ietf subscription 101
 encoding encode-kvgpb
 filter xpath /access-point-oper-data/capwap-data
 receiver-type protocol
 source-address 10.4.20.188
 source-vrf Mgmt-intf
 stream yang-push
 update-policy periodic 6000
 receiver name yangsuite

telemetry receiver protocol yangsuite
 host name yangsuite-telemetry.cisco.com 443
 protocol grpc-tls profile yangsuite

telemetry protocol grpc profile yangsuite
 ca-trustpoint CAforMDTserver
 id-trustpoint CAforWLCclient
```

DNS Load Balancing is used to distribute the connections across a group of servers



```
dig +short cisco.com mx
30 aer-mx-01.cisco.com.
10 alln-mx-01.cisco.com.
20 rcdn-mx-01.cisco.com.
```

DNS Geo-location uses the geographic location of the client and the server resource

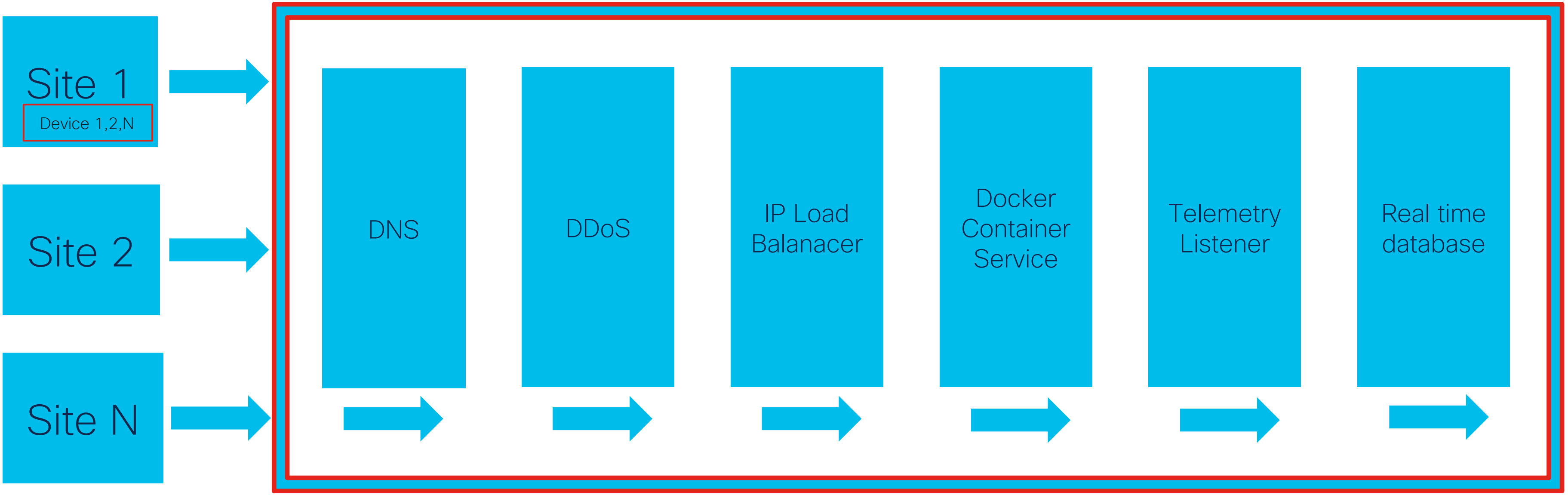


```
lab8-co-wlc-1#show telemetry connection all
Telemetry connections

Index Peer Address               Port  VRF Source Address            State      State Description
----- -------------------------- ----- --- -------------------------- ---------- -------------------
49182 52.                          443 0   10.                        Active     Connection up
```

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cloud-based HA Telemetry Architecture in AWS*



Site 1

Device 1,2,N

Site 2

Site N

DNS

DDoS

IP Load Balanacer

Docker Container Service

Telemetry Listener

Real time database

Cisco Catalyst:
C9300
C9500
C8500
C9800

1. Route 53 (+failover +geoLB) = DNS
2. Shield Standard = DDoS Protection
3. Network Load Balancer = Single Point of Contact
4. ECS = Docker Container Service
5. Fargate = Telemetry listener task
6. Kinesis Stream = Database for real time data

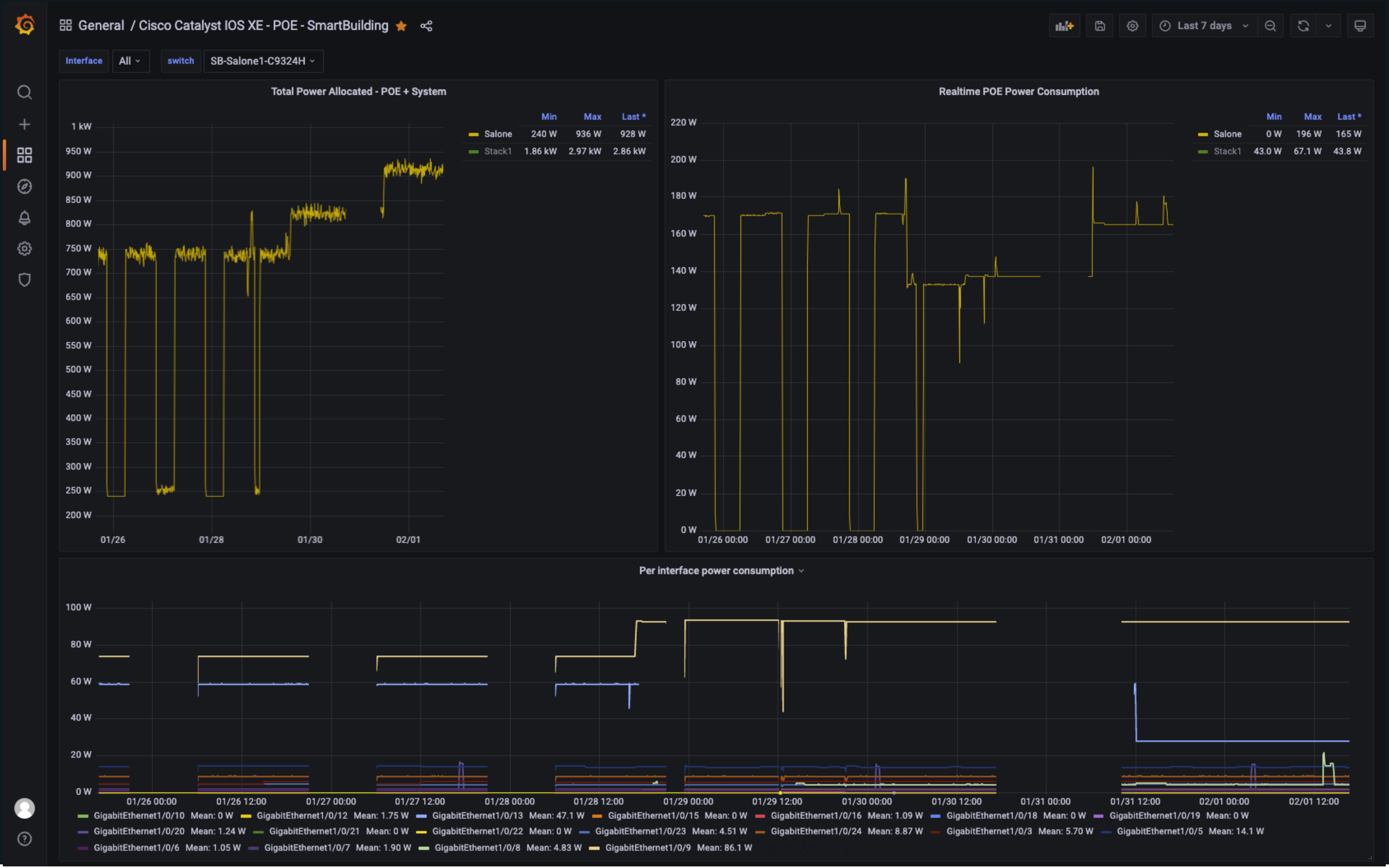
The UI into the Real Time Database provides value in charts & graphs to a variety of business users

* example is AWS components but applies to any cloud service provider, regions are not considered here

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Sustainability

powered by telemetry



General / Cisco Catalyst IOS XE - POE - SmartBuilding

Interface: All
switch: SB-Salone1-C9324H

Total Power Allocated - POE + System

	Min	Max	Last *
Salone	240 W	936 W	928 W
Stack1	1.86 kW	2.97 kW	2.86 kW

Realtime POE Power Consumption

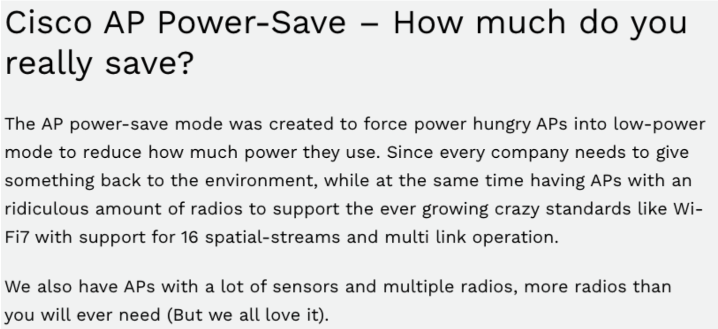
	Min	Max	Last *
Salone	0 W	196 W	165 W
Stack1	43.0 W	67.1 W	43.8 W

Per interface power consumption

GigabitEthernet1/0/10 Mean: 0 W — GigabitEthernet1/0/12 Mean: 1.75 W — GigabitEthernet1/0/13 Mean: 47.1 W — GigabitEthernet1/0/15 Mean: 0 W — GigabitEthernet1/0/16 Mean: 1.09 W — GigabitEthernet1/0/18 Mean: 0 W — GigabitEthernet1/0/19 Mean: 0 W
GigabitEthernet1/0/20 Mean: 1.24 W — GigabitEthernet1/0/21 Mean: 0 W — GigabitEthernet1/0/22 Mean: 0 W — GigabitEthernet1/0/23 Mean: 4.51 W — GigabitEthernet1/0/24 Mean: 8.87 W — GigabitEthernet1/0/3 Mean: 5.70 W — GigabitEthernet1/0/5 Mean: 14.1 W
GigabitEthernet1/0/6 Mean: 1.05 W — GigabitEthernet1/0/7 Mean: 1.90 W — GigabitEthernet1/0/8 Mean: 4.83 W — GigabitEthernet1/0/9 Mean: 86.1 W

AP Power Save

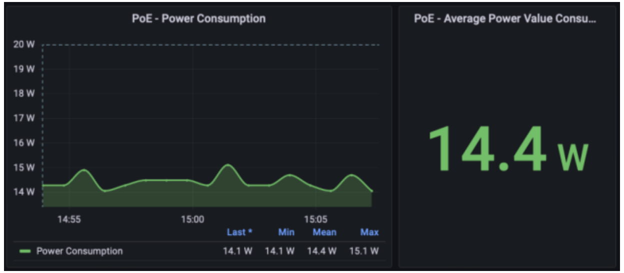
https://wirelessisfun.wordpress.com/2023/02/05/cisco-ap-power-save-how-much-do-you-really-save/



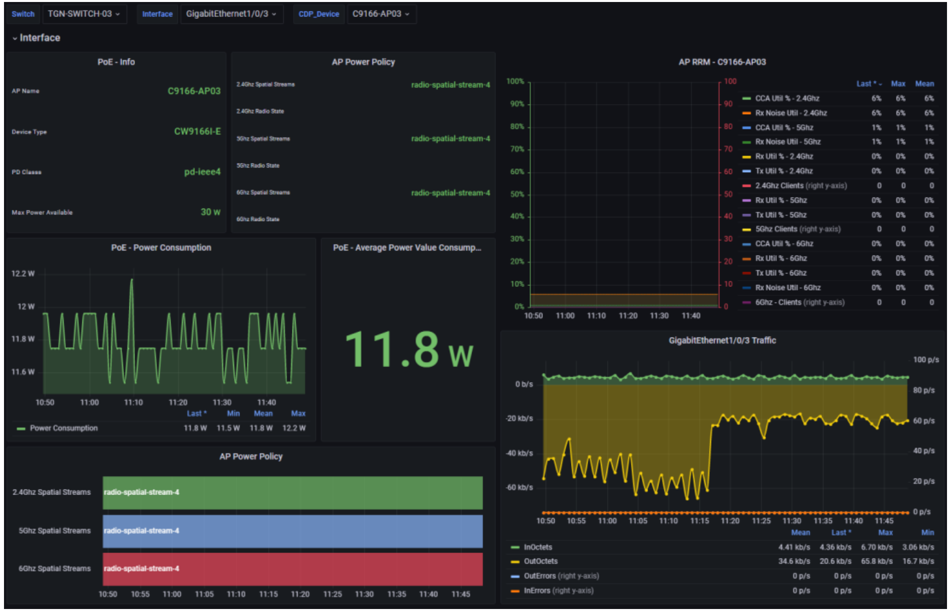
Cisco AP Power-Save – How much do you really save?

The AP power-save mode was created to force power hungry APs into low-power mode to reduce how much power they use. Since every company needs to give something back to the environment, while at the same time having APs with an ridiculous amount of radios to support the ever growing crazy standards like Wi-Fi7 with support for 16 spatial-streams and multi link operation.

We also have APs with a lot of sensors and multiple radios, more radios than you will ever need (But we all love it).



	Last *	Min	Mean	Max
Power Consumption	14.1 W	14.1 W	14.4 W	15.1 W



PoE - Info

AP Name: C9166-AP03
Device Type: CW9166I-E
PD Class: pd-ieee4
Max Power Available: 30 W

AP Power Policy

2.4Ghz Spatial Streams: radio-spatial-stream-4
2.4Ghz Radio State:
5Ghz Spatial Streams: radio-spatial-stream-4
5Ghz Radio State:
6Ghz Spatial Streams: radio-spatial-stream-4
6Ghz Radio State:

	Last *	Min	Mean	Max
Power Consumption	11.8 W	11.5 W	11.8 W	12.2 W

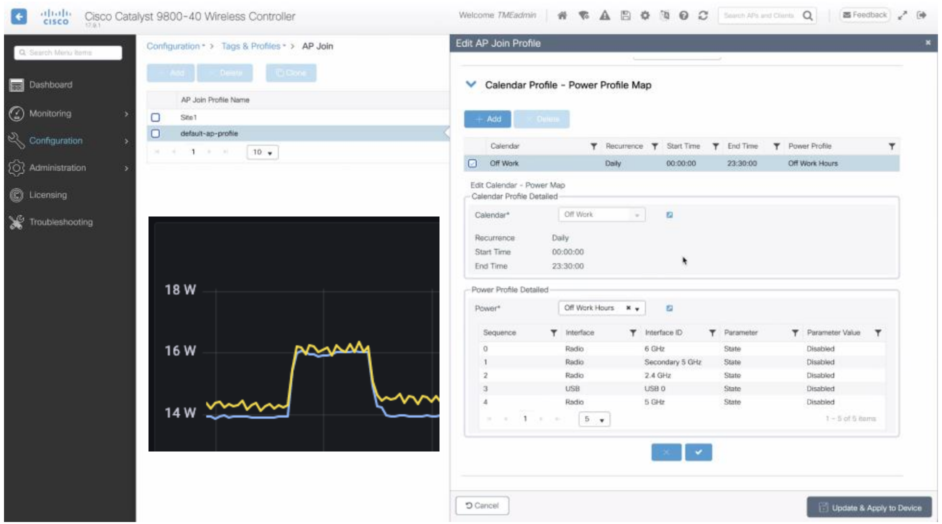
	Last *	Max	Mean
CCA Util % - 2.4Ghz	6%	6%	6%
Rx Noise Util - 2.4Ghz	6%	6%	6%
CCA Util % - 5Ghz	1%	1%	1%
Rx Noise Util - 5Ghz	1%	1%	1%
Rx Util % - 2.4Ghz	0%	0%	0%
Tx Util % - 2.4Ghz	0%	0%	0%
2.4Ghz Clients (right y-axis)	0	0	0
Rx Util % - 5Ghz	0%	0%	0%
Tx Util % - 5Ghz	0%	0%	0%
5Ghz Clients (right y-axis)	0	0	0
CCA Util % - 6Ghz	0%	0%	0%
Rx Util % - 6Ghz	0%	0%	0%
Tx Util % - 6Ghz	0%	0%	0%
Rx Noise Util - 6Ghz	0%	0%	0%
6Ghz - Clients (right y-axis)	0	0	0

	Mean	Last *	Max	Min
InOctets	4.41 kb/s	4.36 kb/s	6.70 kb/s	3.06 kb/s
OutOctets	34.6 kb/s	20.6 kb/s	65.8 kb/s	16.7 kb/s
OutErrors (right y-axis)	0 p/s	0 p/s	0 p/s	0 p/s
InErrors (right y-axis)	0 p/s	0 p/s	0 p/s	0 p/s

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Catalyst 9800 WLC Calendar Template scheduling

To enable power save mode on Cisco Catalyst Access Points



Calendar Profile - Power Profile Map

	Calendar	Recurrence	Start Time	End Time	Power Profile
☑	Off Work	Daily	00:00:00	23:30:00	Off Work Hours

Edit Calendar - Power Map

Calendar Profile Detailed

Calendar*: Off Work

Recurrence: Daily

Start Time: 00:00:00

End Time: 23:30:00

Power Profile Detailed

Power*: Off Work Hours

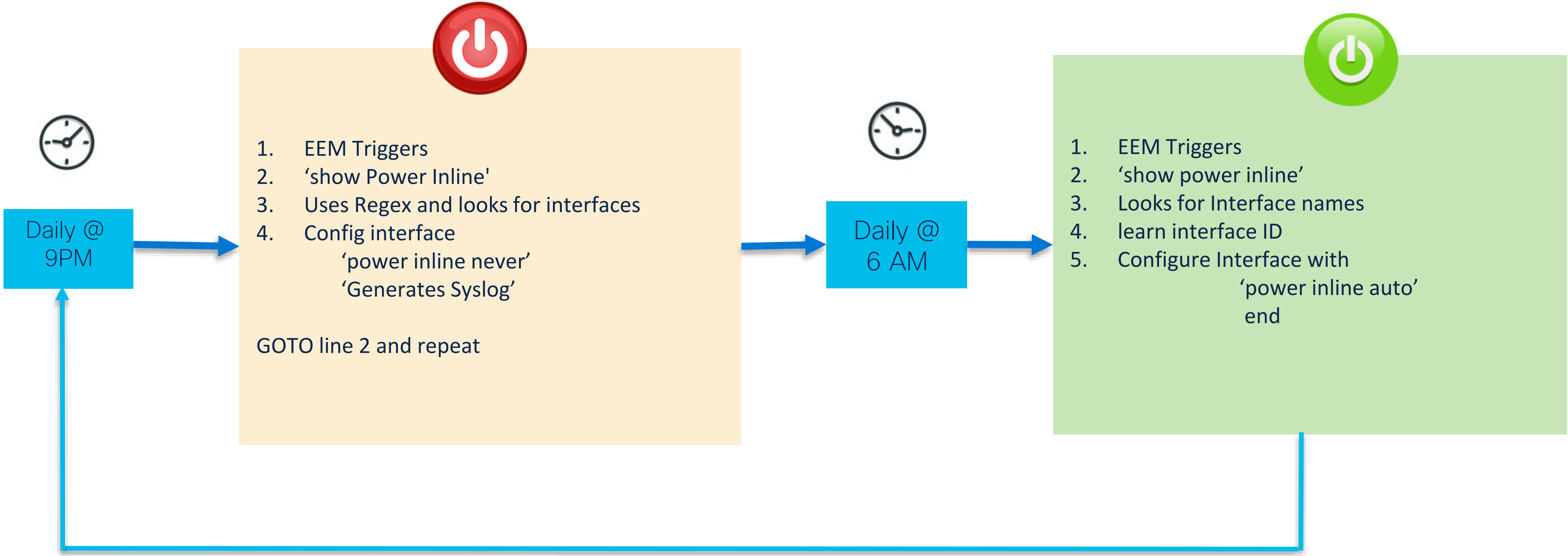
Sequence	Interface	Interface ID	Parameter	Parameter Value
0	Radio	6 GHz	State	Disabled
1	Radio	Secondary 5 GHz	State	Disabled
2	Radio	2.4 GHz	State	Disabled
3	USB	USB 0	State	Disabled
4	Radio	5 GHz	State	Disabled

1 - 5 of 5 items

```
wireless profile power "Off Work Hours"
 0 radio 6ghz state shutdown
 1 radio secondary-5ghz state shutdown
 2 usb 0 state disable
 3 radio 5ghz state shutdown

wireless profile calender-profile name "Off Work 5PM to Midnight"
 day monday
 day tuesday
 day wednesday
 day thursday
 day friday
 recurrance weekly
 start 17:00:00 end 23:59:59

wireless profile calender-profile name "Off Work Midnight to 8AM"
 day monday
 day tuesday
 day wednesday
 day thursday
 day friday
 recurrance weekly
 start 00:00:00 end 08:00:00

ap profile default-ap-profile
 calendar-profile "Workday 5pm to Midnight"
  action power-saving-mode power-profile "Off Work Hours"
 calendar-profile "Workday Midnight to 8am"
  action power-saving-mode power-profile "Off Work Hours"
```

Embedded Event Manager – Applet Flow

Cisco IOS XE Embedded Event Manager (EEM) is a powerful and flexible subsystem
It provides real-time network event detection and onboard automation.
It provides the ability to adapt the behavior of the network devices to better align with business needs.



Daily @ 9PM

1. EEM Triggers
2. ‘show Power Inline'
3. Uses Regex and looks for interfaces
4. Config interface
   ‘power inline never’
   ‘Generates Syslog’

GOTO line 2 and repeat

Daily @ 6 AM

1. EEM Triggers
2. ‘show power inline’
3. Looks for Interface names
4. learn interface ID
5. Configure Interface with
   ‘power inline auto’
   end

POE power management with EEM

EEM is used to toggle the power inline auto / never at 9 PM and 6 AM

Power on/off POE ports on a once daily time schedule

Trigger manually by setting event to none and sending CLI:
C9300-SB# event manager run SelectivePowerOn
C9300-SB# event manager run SelectivePowerOff

```
! EEM POE example SelectivePowerOff
no event manager applet SelectivePowerOff
event manager applet SelectivePowerOff
! Turn *OFF* POE power to the ports daily at 9PM: 0 21 * * *
event timer cron name SelectivePowerOff cron-entry "0 21 * * *"
! or
! event none
!
 action 0.0 cli command "enable"
 action 0.1 cli command "show power inline"
 action 0.2 foreach line "$_cli_result" "\n"
 action 1.1  regexp "^([^[:space:]]*)[[:space:]]*[^[:space:]]*[[:space:]]*on.*$" "$line" temp interface
 action 1.2  if $_regexp_result eq 1
 action 1.3   cli command "conf t"
 action 1.4   cli command "interface $interface"
 action 1.5   cli command "power inline never"
 action 1.6   syslog msg "Turned off PoE on $interface"
 action 1.7  end
 action 2.1 end
```

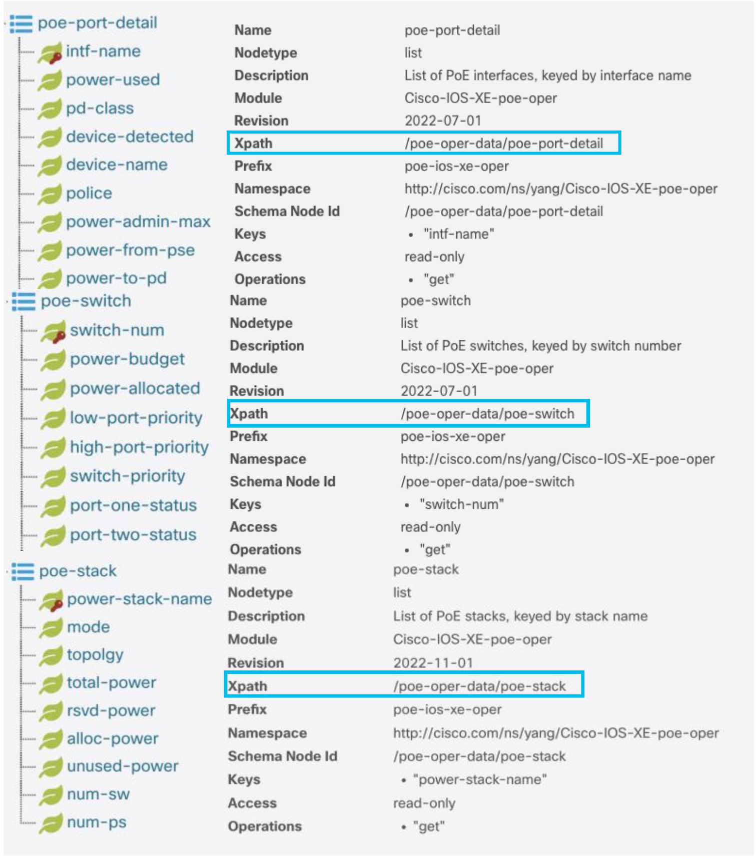
```
! EEM POE example SelectivePowerOn
no event manager applet SelectivePowerOn
event manager applet SelectivePowerOn
! Turn **ON** POE power to the ports daily at 6AM: 0 6 * * *
event timer cron name SelectivePowerOn cron-entry "0 6 * * *"
!
! or
! event none
!
 action 0.0 cli command "enable"
 action 0.1 cli command "show power inline"
 action 0.2 foreach line "$_cli_result" "\n"
 action 1.1  regexp "^([^[:space:]]*)[[:space:]]*off.*$" "$line" temp interface
 action 1.2  if $_regexp_result eq 1
 action 1.3   cli command "conf t"
 action 1.4   cli command "interface $interface"
 action 1.5   cli command "power inline auto"
 action 1.6   syslog msg "Turned on PoE on $interface"
 action 1.7  end
 action 2.1 end
```

Examples @ https://github.com/jeremycohoe/cisco-catalyst-eem-examples
Source: https://glennmatthys.wordpress.com/2014/08/24/intermediary-eem-scripting-more-fun-with-power-over-ethernet/
https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-16/216091-best-practices-and-useful-scripts-for-ee.html
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/command/eem-cr-book/eem-cr-e2.html

Telemetry for POE

This CLI telemetry configuration defines a 30 second periodic update interval

```
no telemetry ietf subscription 69001
telemetry ietf subscription 69001
 filter xpath /poe-oper-data/poe-port-detail
 receiver ip address 10.85.134.66 57508 protocol grpc-tcp
source-address 10.85.134.70
 source-vrf Mgmt-vrf
 stream yang-push
 update-policy periodic 3000
  encoding encode-kvgpb

no telemetry ietf subscription 69002
telemetry ietf subscription 69002
 filter xpath /poe-oper-data/poe-switch
 receiver ip address 10.85.134.66 57508 protocol grpc-tcp
source-address 10.85.134.70
 source-vrf Mgmt-vrf
 stream yang-push
 update-policy periodic 3000
  encoding encode-kvgpb

no telemetry ietf subscription 69003
telemetry ietf subscription 69003
 filter xpath /poe-oper-data/poe-stack
 receiver ip address 10.85.134.66 57508 protocol grpc-tcp
source-address 10.85.134.70
 source-vrf Mgmt-vrf
 stream yang-push
 update-policy periodic 3000
  encoding encode-kvgpb
```



- poe-port-detail
  - intf-name
  - power-used
  - pd-class
  - device-detected
  - device-name
  - police
  - power-admin-max
  - power-from-pse
  - power-to-pd

Name	poe-port-detail
Nodetype	list
Description	List of PoE interfaces, keyed by interface name
Module	Cisco-IOS-XE-poe-oper
Revision	2022-07-01
Xpath	/poe-oper-data/poe-port-detail
Prefix	poe-ios-xe-oper
Namespace	http://cisco.com/ns/yang/Cisco-IOS-XE-poe-oper
Schema Node Id	/poe-oper-data/poe-port-detail
Keys	• "intf-name"
Access	read-only
Operations	• "get"

- poe-switch
  - switch-num
  - power-budget
  - power-allocated
  - low-port-priority
  - high-port-priority
  - switch-priority
  - port-one-status
  - port-two-status

Name	poe-switch
Nodetype	list
Description	List of PoE switches, keyed by switch number
Module	Cisco-IOS-XE-poe-oper
Revision	2022-07-01
Xpath	/poe-oper-data/poe-switch
Prefix	poe-ios-xe-oper
Namespace	http://cisco.com/ns/yang/Cisco-IOS-XE-poe-oper
Schema Node Id	/poe-oper-data/poe-switch
Keys	• "switch-num"
Access	read-only
Operations	• "get"

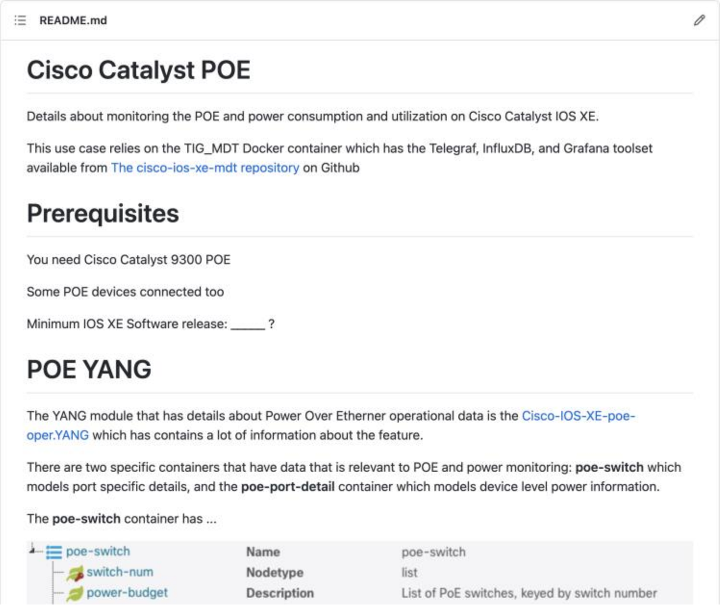
- poe-stack
  - power-stack-name
  - mode
  - topolgy
  - total-power
  - rsvd-power
  - alloc-power
  - unused-power
  - num-sw
  - num-ps

Name	poe-stack
Nodetype	list
Description	List of PoE stacks, keyed by stack name
Module	Cisco-IOS-XE-poe-oper
Revision	2022-11-01
Xpath	/poe-oper-data/poe-stack
Prefix	poe-ios-xe-oper
Namespace	http://cisco.com/ns/yang/Cisco-IOS-XE-poe-oper
Schema Node Id	/poe-oper-data/poe-stack
Keys	• "power-stack-name"
Access	read-only
Operations	• "get"

https://github.com/YangModels/yang/blob/main/vendor/cisco/xe/1791/Cisco-IOS-XE-poe-oper.yang

Github.com and Grafana.com documentation

https://github.com/jeremycohoe/cisco-mdt-poe/
https://grafana.com/grafana/dashboards/17238-catalyst-poe-dashboard/



README.md

Cisco Catalyst POE

Details about monitoring the POE and power consumption and utilization on Cisco Catalyst IOS XE.

This use case relies on the TIG_MDT Docker container which has the Telegraf, InfluxDB, and Grafana toolset available from The cisco-ios-xe-mdt repository on Github

Prerequisites

You need Cisco Catalyst 9300 POE

Some POE devices connected too

Minimum IOS XE Software release: _____ ?

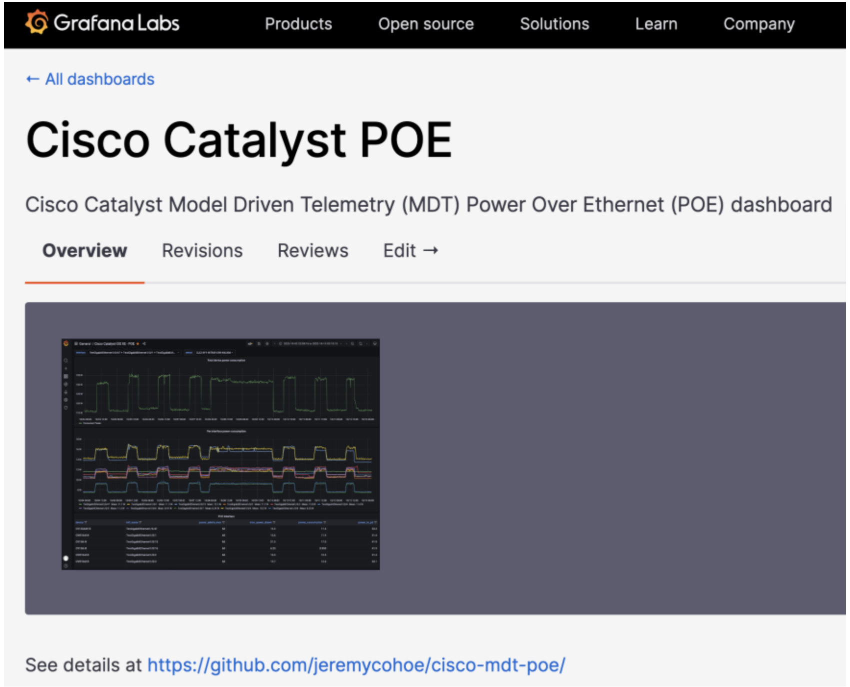
POE YANG

The YANG module that has details about Power Over Etherner operational data is the Cisco-IOS-XE-poe-oper.YANG which has contains a lot of information about the feature.

There are two specific containers that have data that is relevant to POE and power monitoring: **poe-switch** which models port specific details, and the **poe-port-detail** container which models device level power information.

The **poe-switch** container has ...

poe-switch	**Name**	poe-switch
switch-num	**Nodetype**	list
power-budget	**Description**	List of PoE switches, keyed by switch number



Cisco Catalyst POE

Cisco Catalyst Model Driven Telemetry (MDT) Power Over Ethernet (POE) dashboard

See details at https://github.com/jeremycohoe/cisco-mdt-poe/

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

On-Box Automation

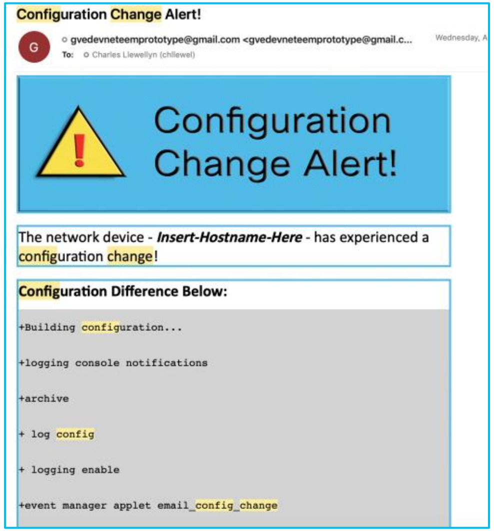
ZTP – Zero Touch Provisioning
EEM – Embedded Event Manager
Python & NETCONF API

Config Diff

Config diff on box with Guest Shell

Show run before + after change = run linux diff tools on-box

On-box EEM Automation can be used to create config deltas



Configuration Change Alert!

gvedevneteemprototype@gmail.com <gvedevneteemprototype@gmail.c... Wednesday, A

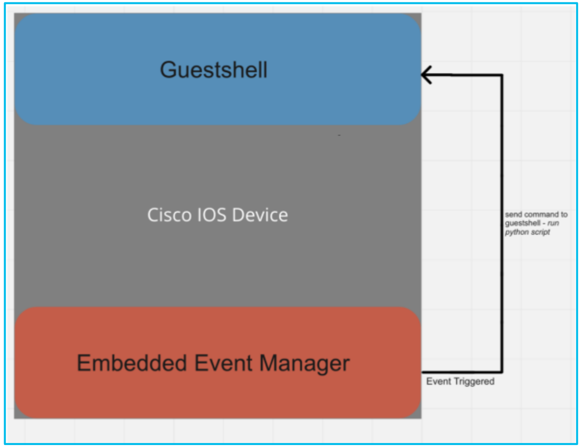
To: Charles Llewellyn (chllewel)

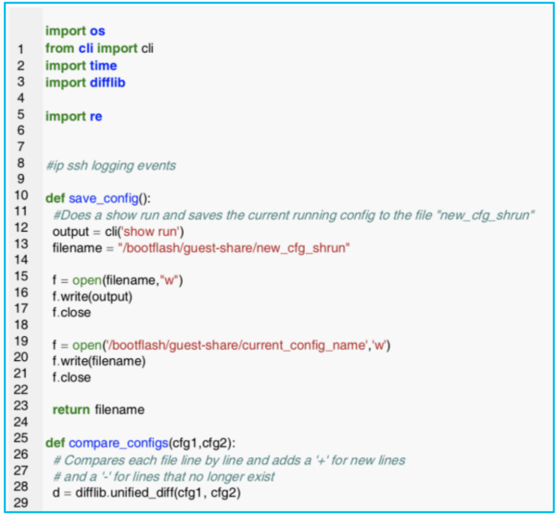
Configuration Change Alert!

The network device - ***Insert-Hostname-Here*** - has experienced a configuration change!

Configuration Difference Below:

```
+Building configuration...

+logging console notifications

+archive

+ log config

+ logging enable

+event manager applet email_config_change
```





```python
import os
from cli import cli
import time
import difflib

import re


#ip ssh logging events

def save_config():
  #Does a show run and saves the current running config to the file "new_cfg_shrun"
  output = cli('show run')
  filename = "/bootflash/guest-share/new_cfg_shrun"

  f = open(filename,"w")
  f.write(output)
  f.close

  f = open('/bootflash/guest-share/current_config_name','w')
  f.write(filename)
  f.close

  return filename

def compare_configs(cfg1,cfg2):
  # Compares each file line by line and adds a '+' for new lines
  # and a '-' for lines that no longer exist
  d = difflib.unified_diff(cfg1, cfg2)
```

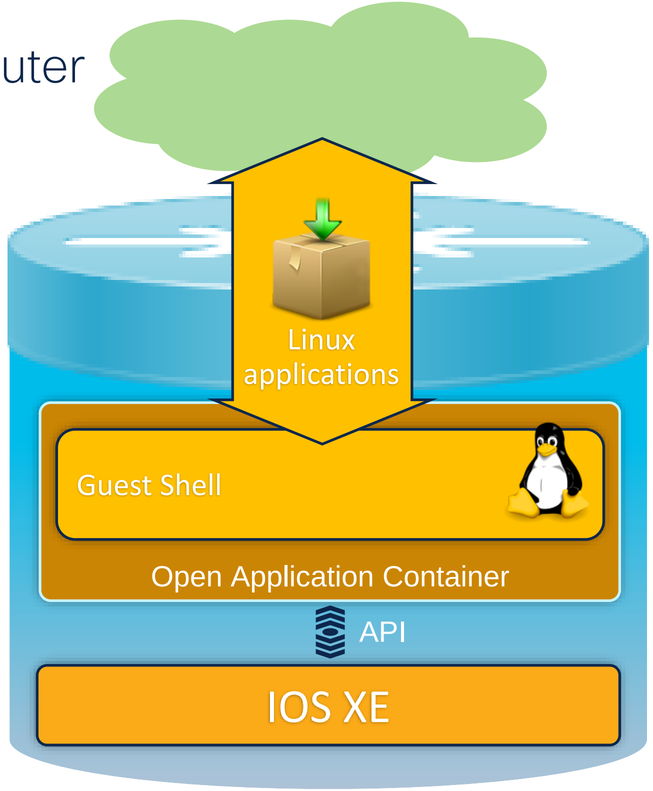
https://github.com/jeremycohoe/gve_devnet_eem_python_configuration_tracking

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Guest Shell Application

Linux Shell Environment On Your Switch or Router

- Maintain IOS-XE system integrity
  - Isolated User Space
  - Fault Isolation
  - Resource Isolation
- On-box rapid prototyping
  - Device-level API Integration
  - Scripting (Python)
  - Linux Commands
- Application Hosting
- Integrate into your Linux workflow
- Integrated with IOS-XE



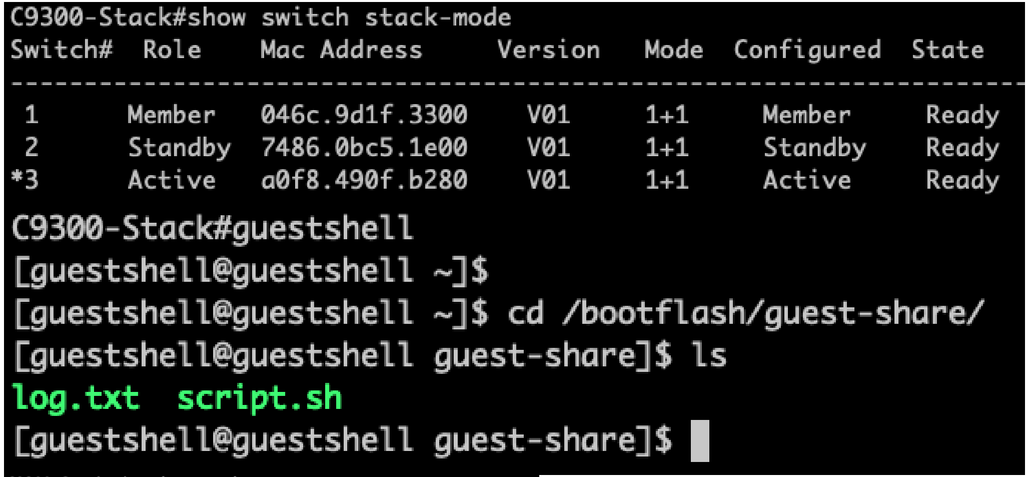
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Guest Shell High Availability: Folder Sync

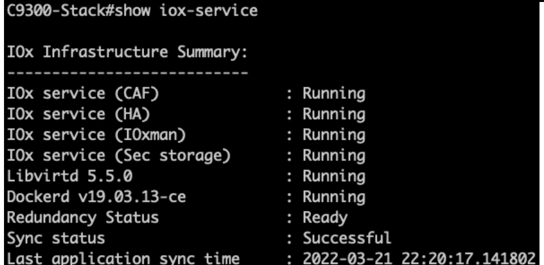
17.9
17.6.4

Files within the Guest-share folder are now maintained during HA switchover
Use case: Customer has a script running in Guest Shell to collect and parse custom statistics needed for security auditing requirements. After HA event the script and log files are maintained

- Improvements to Guest Shell storage and file handling means there is now a dedicated folder within the flash: that is shared with the Guest Shell
- All files from IOS XE flash are no longer shared with the Guest Shell and must be explicitly shared within the guest-share folder
- The Guest Shell state is maintained during a High Availability switchover
- 1+1 Stack Mode is not the default and must be set to specify the Standby switch to Linux inotify sync the files of up to 50 MB



```
C9300-Stack#show switch stack-mode
Switch#  Role     Mac Address     Version   Mode  Configured  State
----------------------------------------------------------------------
 1       Member   046c.9d1f.3300   V01      1+1    Member     Ready
 2       Standby  7486.0bc5.1e00   V01      1+1    Standby    Ready
*3       Active   a0f8.490f.b280   V01      1+1    Active     Ready
C9300-Stack#guestshell
[guestshell@guestshell ~]$
[guestshell@guestshell ~]$ cd /bootflash/guest-share/
[guestshell@guestshell guest-share]$ ls
log.txt  script.sh
[guestshell@guestshell guest-share]$
```



```
C9300-Stack#show iox-service

IOx Infrastructure Summary:
---------------------------
IOx service (CAF)              : Running
IOx service (HA)               : Running
IOx service (IOxman)           : Running
IOx service (Sec storage)      : Running
Libvirtd 5.5.0                 : Running
Dockerd v19.03.13-ce           : Running
Redundancy Status              : Ready
Sync status                    : Successful
Last application sync time     : 2022-03-21 22:20:17.141802
```

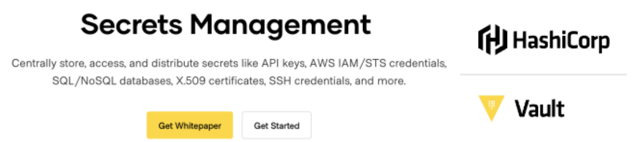
17.10

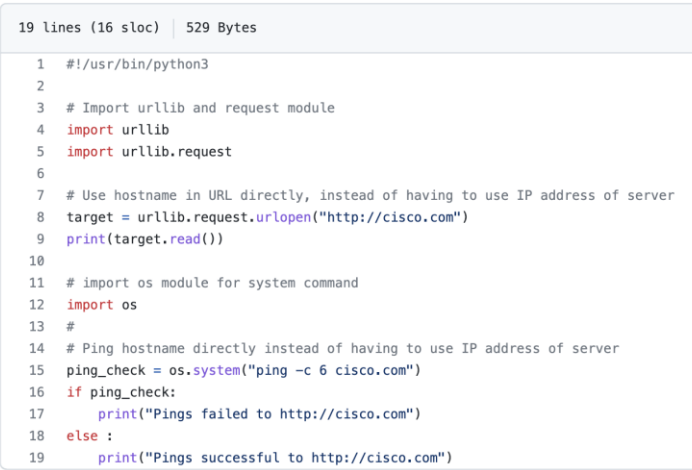
Day 0 Guest Shell DNS Enhancement Example

DNS has always been supported *to find* the Python file.
DNS from the DHCP service can now be used *within* the Python file.

This enhancement makes the DNS servers available for use within the Guest Shell – this makes using cloud-based services like Vault etc easier

This can be useful for credential management.
And to access other online resources via DNS name


Secrets Management
Centrally store, access, and distribute secrets like API keys, AWS IAM/STS credentials, SQL/NoSQL databases, X.509 certificates, SSH credentials, and more.
Get Whitepaper
Get Started
HashiCorp
Vault



19 lines (16 sloc) | 529 Bytes

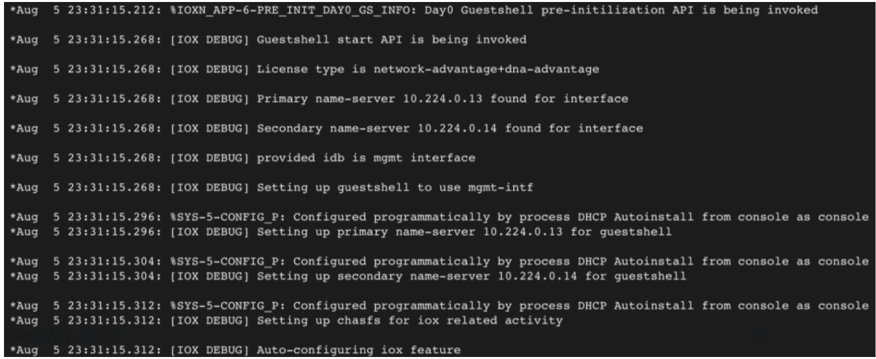
```python
#!/usr/bin/python3

# Import urllib and request module
import urllib
import urllib.request

# Use hostname in URL directly, instead of having to use IP address of server
target = urllib.request.urlopen("http://cisco.com")
print(target.read())

# import os module for system command
import os
#
# Ping hostname directly instead of having to use IP address of server
ping_check = os.system("ping -c 6 cisco.com")
if ping_check:
    print("Pings failed to http://cisco.com")
else :
    print("Pings successful to http://cisco.com")
```

https://github.com/jeremycohoe/IOSXE-Zero-Touch-Provisioning/blob/master/ztp-dns.py

Bootstrap script (ztp.py)

Device credentials (variables)

Cloud-based Secrets Management



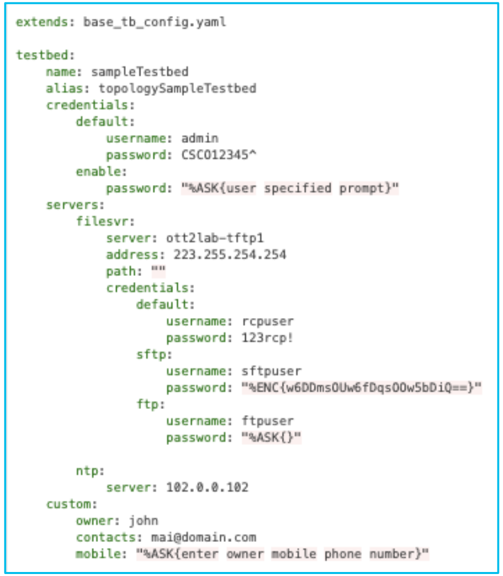
```
*Aug  5 23:31:15.212: %IOXN_APP-6-PRE_INIT_DAY0_GS_INFO: Day0 Guestshell pre-initilization API is being invoked

*Aug  5 23:31:15.268: [IOX DEBUG] Guestshell start API is being invoked

*Aug  5 23:31:15.268: [IOX DEBUG] License type is network-advantage+dna-advantage

*Aug  5 23:31:15.268: [IOX DEBUG] Primary name-server 10.224.0.13 found for interface

*Aug  5 23:31:15.268: [IOX DEBUG] Secondary name-server 10.224.0.14 found for interface

*Aug  5 23:31:15.268: [IOX DEBUG] provided idb is mgmt interface

*Aug  5 23:31:15.268: [IOX DEBUG] Setting up guestshell to use mgmt-intf

*Aug  5 23:31:15.296: %SYS-5-CONFIG_P: Configured programmatically by process DHCP Autoinstall from console as console
*Aug  5 23:31:15.296: [IOX DEBUG] Setting up primary name-server 10.224.0.13 for guestshell

*Aug  5 23:31:15.304: %SYS-5-CONFIG_P: Configured programmatically by process DHCP Autoinstall from console as console
*Aug  5 23:31:15.304: [IOX DEBUG] Setting up secondary name-server 10.224.0.14 for guestshell

*Aug  5 23:31:15.312: %SYS-5-CONFIG_P: Configured programmatically by process DHCP Autoinstall from console as console
*Aug  5 23:31:15.312: [IOX DEBUG] Setting up chasfs for iox related activity

*Aug  5 23:31:15.312: [IOX DEBUG] Auto-configuring iox feature
```

Python Automation Test System

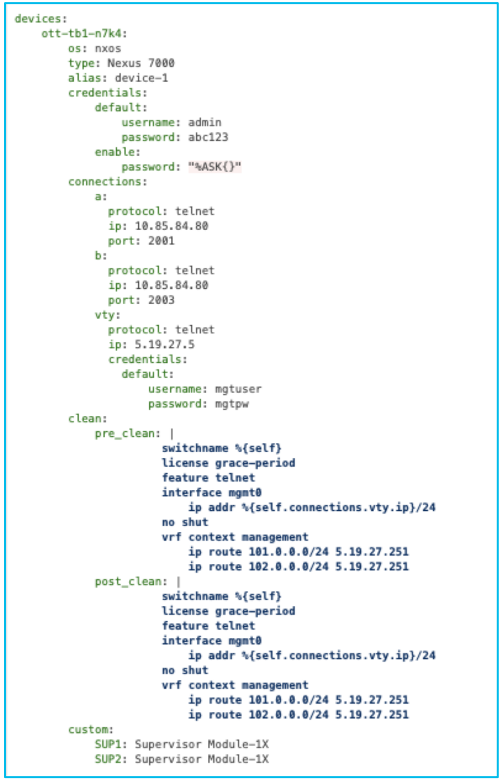
pyATS
print(network.profile)

pyATS provides sanity, feature, solution, system, and **scale test & verification** automation for products ranging from routers and switches, to access points, firewalls and cable CPEs.

It allows the device connections via **CLI**, **NETCONF**, or **RESTCONF**.



```yaml
extends: base_tb_config.yaml

testbed:
    name: sampleTestbed
    alias: topologySampleTestbed
    credentials:
        default:
            username: admin
            password: CSCO12345^
        enable:
            password: "%ASK{user specified prompt}"
    servers:
        filesvr:
            server: ott2lab-tftp1
            address: 223.255.254.254
            path: ""
            credentials:
                default:
                    username: rcpuser
                    password: 123rcp!
                sftp:
                    username: sftpuser
                    password: "%ENC{w6DDmsOUw6fDqsOOw5bDiQ==}"
                ftp:
                    username: ftpuser
                    password: "%ASK{}"

        ntp:
            server: 102.0.0.102
    custom:
        owner: john
        contacts: mai@domain.com
        mobile: "%ASK{enter owner mobile phone number}"
```



```yaml
devices:
    ott-tb1-n7k4:
        os: nxos
        type: Nexus 7000
        alias: device-1
        credentials:
            default:
                username: admin
                password: abc123
            enable:
                password: "%ASK{}"
        connections:
            a:
              protocol: telnet
              ip: 10.85.84.80
              port: 2001
            b:
              protocol: telnet
              ip: 10.85.84.80
              port: 2003
            vty:
              protocol: telnet
              ip: 5.19.27.5
              credentials:
                default:
                    username: mgtuser
                    password: mgtpw
        clean:
            pre_clean: |
                        switchname %{self}
                        license grace-period
                        feature telnet
                        interface mgmt0
                            ip addr %{self.connections.vty.ip}/24
                        no shut
                        vrf context management
                            ip route 101.0.0.0/24 5.19.27.251
                            ip route 102.0.0.0/24 5.19.27.251
            post_clean: |
                        switchname %{self}
                        license grace-period
                        feature telnet
                        interface mgmt0
                            ip addr %{self.connections.vty.ip}/24
                        no shut
                        vrf context management
                            ip route 101.0.0.0/24 5.19.27.251
                            ip route 102.0.0.0/24 5.19.27.251
        custom:
            SUP1: Supervisor Module-1X
            SUP2: Supervisor Module-1X
```

https://developer.cisco.com/pyats/
https://developer.cisco.com/docs/pyats/api/

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

RFC8572 (SZTP)

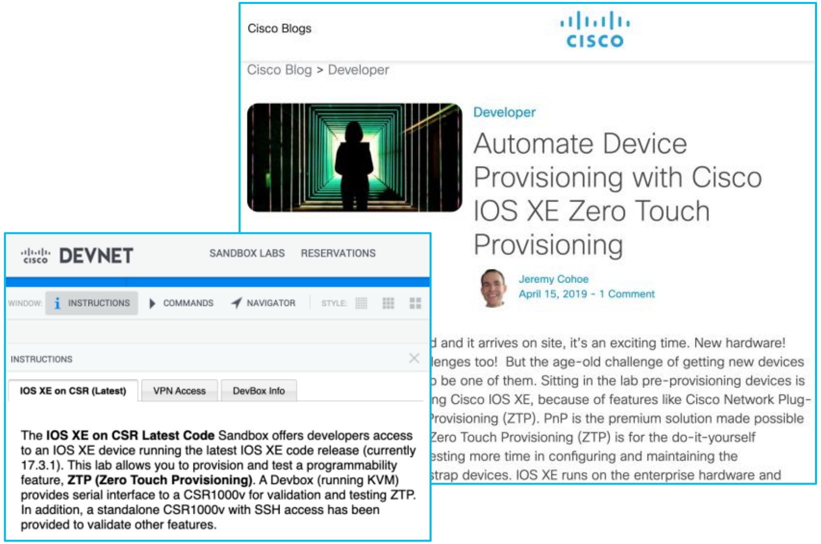
Secure Zero Touch Provisioning

Classic ZTP Overview

1. When an IOS XE device boots and no configuration is present, the device will issue a DHCP request on the management port and on the front panel port.

2. If the DHCP response contains option 67 then ZTP is initiated and the device will retrieve and execute the python script from within the Guest Shell

3. Guest Shell is started and networking is automatically configured



Cisco Blogs

Cisco Blog > Developer

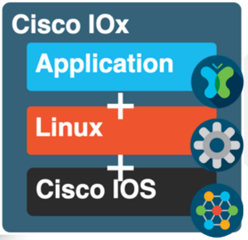
Developer

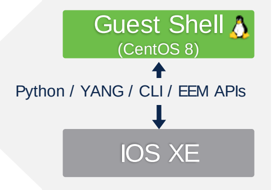
Automate Device Provisioning with Cisco IOS XE Zero Touch Provisioning

Jeremy Cohoe
April 15, 2019 - 1 Comment

d and it arrives on site, it's an exciting time. New hardware!
lenges too! But the age-old challenge of getting new devices
o be one of them. Sitting in the lab pre-provisioning devices is
ng Cisco IOS XE, because of features like Cisco Network Plug-
Provisioning (ZTP). PnP is the premium solution made possible
Zero Touch Provisioning (ZTP) is for the do-it-yourself
esting more time in configuring and maintaining the
strap devices. IOS XE runs on the enterprise hardware and

The **IOS XE on CSR Latest Code** Sandbox offers developers access to an IOS XE device running the latest IOS XE code release (currently 17.3.1). This lab allows you to provision and test a programmability feature, **ZTP (Zero Touch Provisioning)**. A Devbox (running KVM) provides serial interface to a CSR1000v for validation and testing ZTP. In addition, a standalone CSR1000v with SSH access has been provided to validate other features.





CentOS

https://www.youtube.com/watch?v=EAXnftG6odg
https://blogs.cisco.com/developer/device-provisioning-with-ios-xe-zero-touch-provisioning
https://devnetsandbox.cisco.com/RM/Diagram/Index/f2e2c0ad-844f-4a73-8085-00b5b28347a1?diagramType=Topology

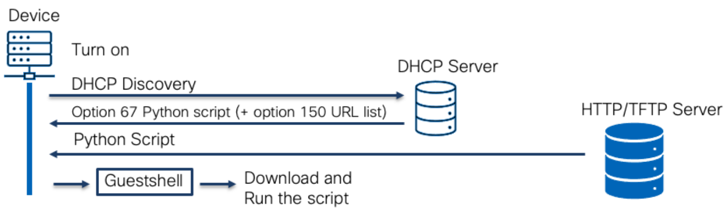
17.11

RFC8572 Secure ZTP

RFC details: https://www.rfc-editor.org/rfc/rfc8572.html

1. Conveyed Information: used to encode the redirect information and onboarding information (switch config)
2. Ownership Certificate: used by a device to verify the signature over the conveyed information
3. Ownership Voucher: used to verify a device owner as defined by the manufacturer (from the MASA)

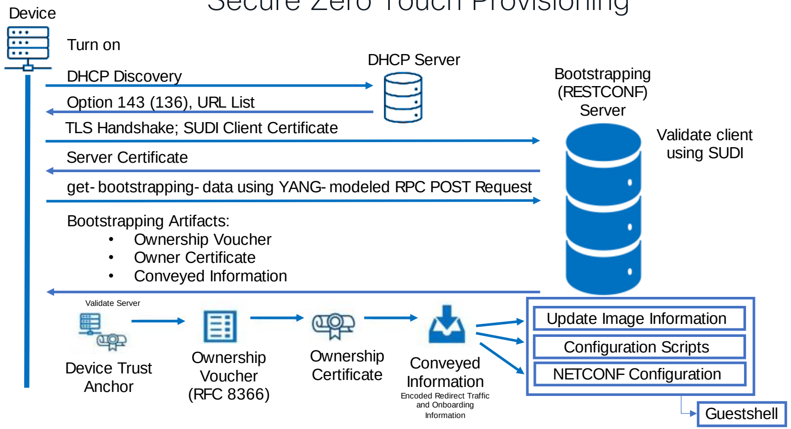
Classic Zero Touch Provisioning



Some security requirements for classic ZTP are resolved using Secure ZTP:

- Management system needs to validate the device
- Device needs to validate the server
- Device must validate the data is what server sent

Secure Zero Touch Provisioning



As part of the SZTP RFC, the device supports image upgrade as part of the conveyed information

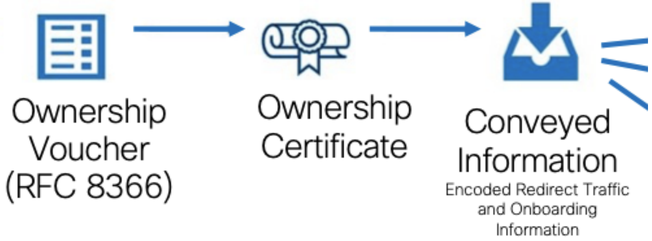
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

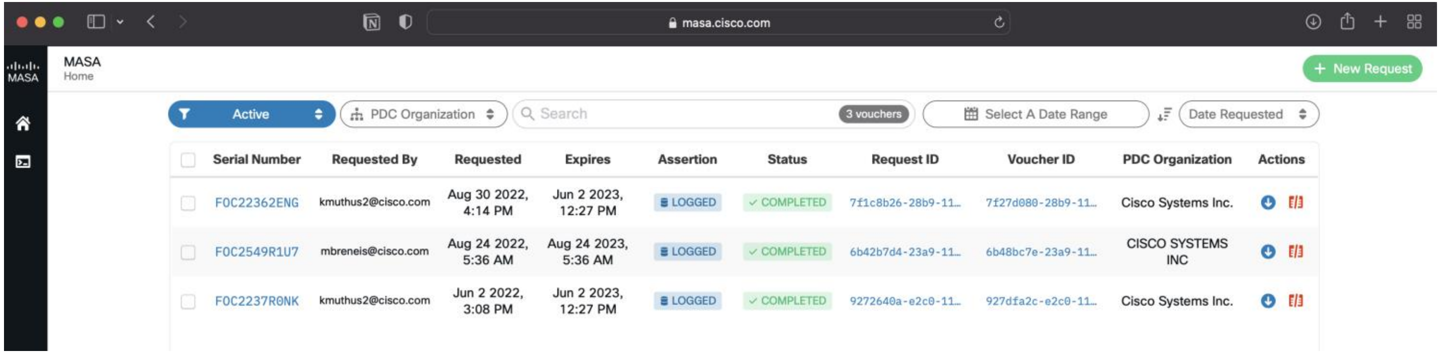
MASA and Certificate Signing for OV

(Manufacturer Authorized Signing Authority) = https://masa.cisco.com

The *Secure ZTP feature* on Cisco IOS XE is available in release 17.11

The upstream cloud-based *certificate verification* **(masa.cisco.com)** is being developed for IOS XE Ownership Voucher (OV) signing workflows


Ownership Voucher (RFC 8366)
Ownership Certificate
Conveyed Information
Encoded Redirect Traffic and Onboarding Information



Serial Number	Requested By	Requested	Expires	Assertion	Status	Request ID	Voucher ID	PDC Organization	Actions
FOC22362ENG	kmuthus2@cisco.com	Aug 30 2022, 4:14 PM	Jun 2 2023, 12:27 PM	LOGGED	✓ COMPLETED	7f1c8b26-28b9-11…	7f27d080-28b9-11…	Cisco Systems Inc.	
FOC2549R1U7	mbreneis@cisco.com	Aug 24 2022, 5:36 AM	Aug 24 2023, 5:36 AM	LOGGED	✓ COMPLETED	6b42b7d4-23a9-11…	6b48bc7e-23a9-11…	CISCO SYSTEMS INC	
FOC2237R0NK	kmuthus2@cisco.com	Jun 2 2022, 3:08 PM	Jun 2 2023, 12:27 PM	LOGGED	✓ COMPLETED	9272640a-e2c0-11…	927dfa2c-e2c0-11…	Cisco Systems Inc.	

Details @ https://xrdocs.io/automation/tutorials/setting-up-crosswork-for-sztp/

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Reference

Examples to set DHCP option 143

Once the device starts in the auto-install mode, the DHCP will be started automatically and if the DHCP server sends Option 143, SZTP will be executed. No device configuration is needed.

DHCPv4

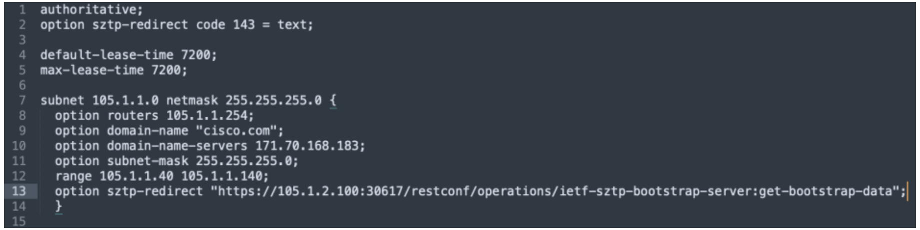
Configure the generic option under DHCP address pool.
Refer to RFC8572, Section 8 for DHCP Options to configure a valid option 143

```
ip dhcp pool SZTP-POOL
option 143 instance <instance-number> hex <option-data>
```

Cisco DHCP Guide:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book/config-dhcp-server.html#GUID-A7226CF3-66F5-46C3-B901-C94CAAB2FCDD

DHCPv4 or DHCPv6

Use open-source ISC-DHCP server and configure it to send option 143.



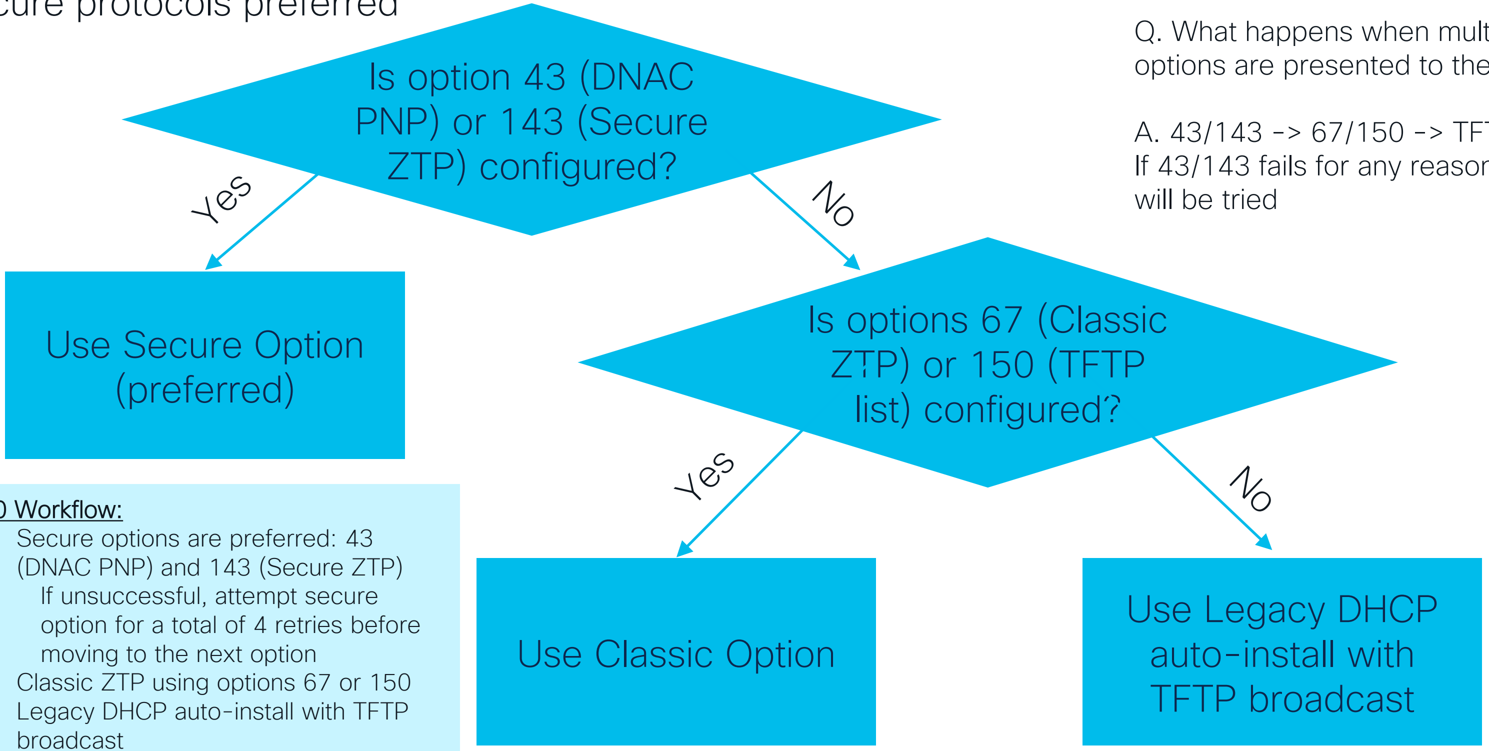
```
authoritative;
option sztp-redirect code 143 = text;

default-lease-time 7200;
max-lease-time 7200;

subnet 105.1.1.0 netmask 255.255.255.0 {
  option routers 105.1.1.254;
  option domain-name "cisco.com";
  option domain-name-servers 171.70.168.183;
  option subnet-mask 255.255.255.0;
  range 105.1.1.40 105.1.1.140;
  option sztp-redirect "https://105.1.2.100:30617/restconf/operations/ietf-sztp-bootstrap-server:get-bootstrap-data";
  }

```

Same DHCP infra workflow as classic ZTP: set the DHCP option to point to the server

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Day 0 device onboarding workflow

Secure protocols preferred


Is option 43 (DNAC PNP) or 143 (Secure ZTP) configured?
Yes
No
Use Secure Option (preferred)
Is options 67 (Classic ZTP) or 150 (TFTP list) configured?
Yes
No
Use Classic Option
Use Legacy DHCP auto-install with TFTP broadcast

Q. What happens when multiple Day 0 DHCP options are presented to the device?

A. 43/143 -> 67/150 -> TFTP Broadcast
If 43/143 fails for any reason, then 67/150 will be tried

Day 0 Workflow:

1. Secure options are preferred: 43 (DNAC PNP) and 143 (Secure ZTP)
   If unsuccessful, attempt secure option for a total of 4 retries before moving to the next option
2. Classic ZTP using options 67 or 150
3. Legacy DHCP auto-install with TFTP broadcast

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Conclusion & Resources

Cisco DEVNET

Start Now

Videos and Tutorials

Sandbox Learning Lab

Automation and Code Exchange

Learning and Certifications

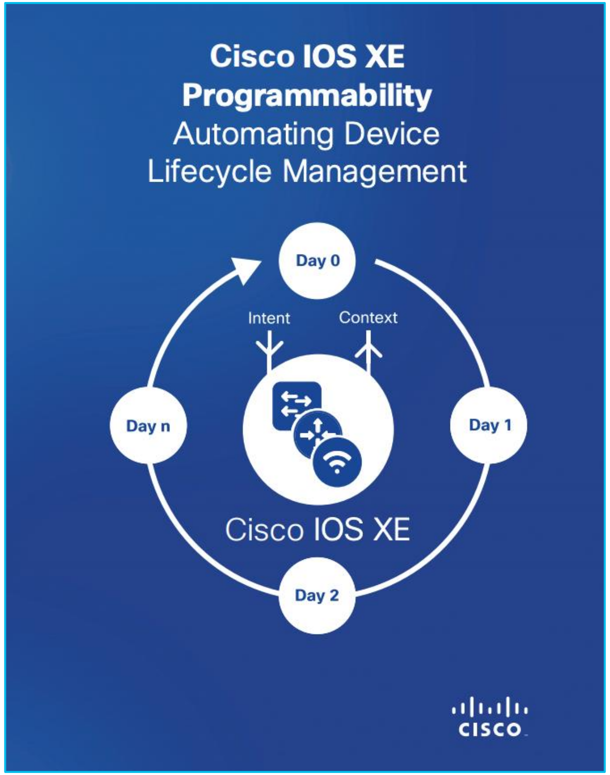
Community and Study Groups

developer.cisco.com

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco IOS XE Programmability – booksprint Book

http://cs.co/programmabilitybook OR https://www.cisco.com/c/dam/en/us/products/collateral/enterprise-networks/nb-06-ios-xe-prog-ebook-cte-en.pdf

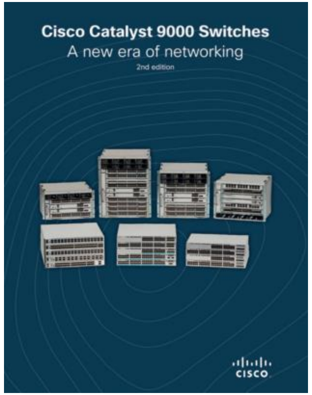


Cisco IOS XE Programmability
Automating Device Lifecycle Management

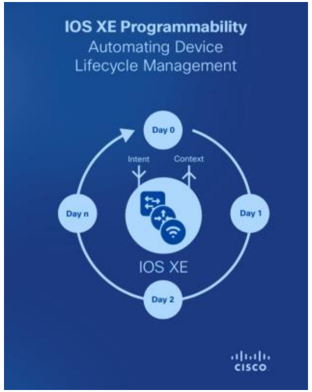
Table of Contents

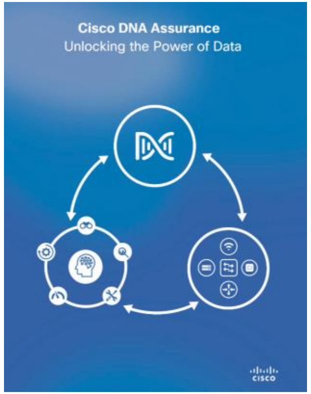
Enterprise Networks booksprints

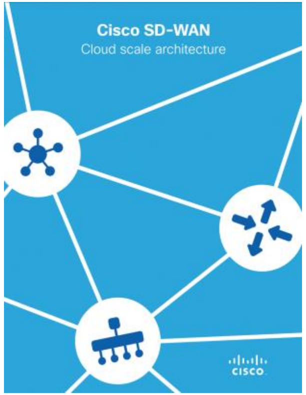
http://cs.co/cat9000book
http://cs.co/sdabook
http://cs.co/wirelessbook
http://cs.co/programmabilitybook
http://cs.co/assurancebook
http://cs.co/sdwanbook



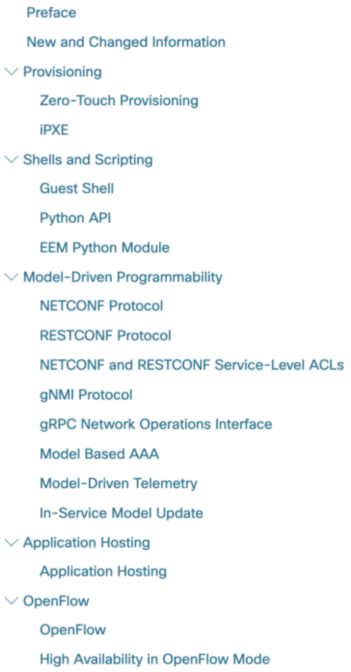
Cisco Software-Defined Access
Enabling intent-based networking
2nd edition
cisco







Programmability Configuration Guide



- Preface
- New and Changed Information
- Provisioning
  - Zero-Touch Provisioning
  - iPXE
- Shells and Scripting
  - Guest Shell
  - Python API
  - EEM Python Module
- Model-Driven Programmability
  - NETCONF Protocol
  - RESTCONF Protocol
  - NETCONF and RESTCONF Service-Level ACLs
  - gNMI Protocol
  - gRPC Network Operations Interface
  - Model Based AAA
  - Model-Driven Telemetry
  - In-Service Model Update
- Application Hosting
  - Application Hosting
- OpenFlow
  - OpenFlow
  - High Availability in OpenFlow Mode

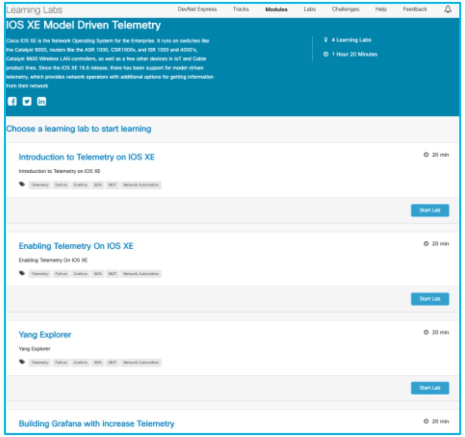
Programmability Configuration Guide, Cisco IOS XE Dublin 17.10.x

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/1710/b_1710_programmability_cg.html

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Learning Lab and Blog: IOS XE MDT

https://developer.cisco.com/learning/modules/iosxe_telemetry
https://blogs.cisco.com/developer/model-driven-telemetry-sandbox
https://blogs.cisco.com/developer/getting-started-with-model-driven-telemetry
https://youtu.be/QwwZakkWBng



IOS XE Model Driven Telemetry

Cisco IOS XE is the Network Operating System for the Enterprise. It runs on switches like the Catalyst 9000, routers like the ASR 1000, CSR1000v, and ISR 1000 and 4000's, Catalyst 9800 Wireless LAN controllers, as well as a few other devices in IoT and Cable product lines. Since the IOS XE 16.6 release, there has been support for model-driven telemetry, which provides network operators with additional options for getting information from their network

4 Learning Labs
1 Hour 20 Minutes

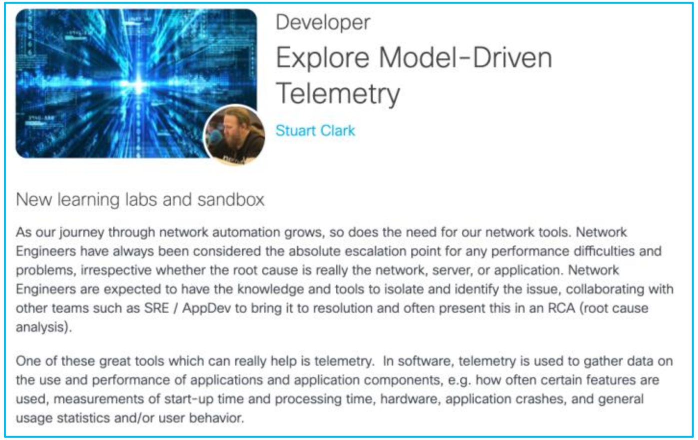
Choose a learning lab to start learning

Introduction to Telemetry on IOS XE — 20 min
Introduction to Telemetry on IOS XE
Telemetry · Python · Grafana · SDN · MDT · Network Automation

Enabling Telemetry On IOS XE — 20 min
Enabling Telemetry On IOS XE
Telemetry · Python · Grafana · SDN · MDT · Network Automation

Yang Explorer — 20 min
Yang Explorer
Telemetry · Python · Grafana · SDN · MDT · Network Automation

Building Grafana with increase Telemetry — 20 min



Developer

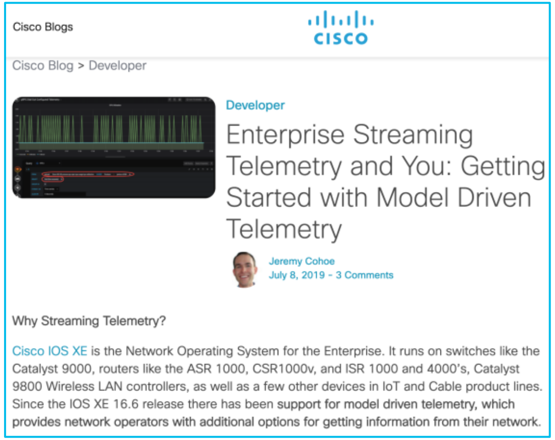
Explore Model-Driven Telemetry

Stuart Clark

New learning labs and sandbox

As our journey through network automation grows, so does the need for our network tools. Network Engineers have always been considered the absolute escalation point for any performance difficulties and problems, irrespective whether the root cause is really the network, server, or application. Network Engineers are expected to have the knowledge and tools to isolate and identify the issue, collaborating with other teams such as SRE / AppDev to bring it to resolution and often present this in an RCA (root cause analysis).

One of these great tools which can really help is telemetry. In software, telemetry is used to gather data on the use and performance of applications and application components, e.g. how often certain features are used, measurements of start-up time and processing time, hardware, application crashes, and general usage statistics and/or user behavior.



Cisco Blog > Developer

Developer

Enterprise Streaming Telemetry and You: Getting Started with Model Driven Telemetry

Jeremy Cohoe
July 8, 2019 - 3 Comments

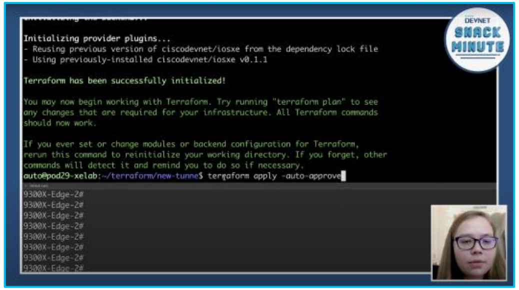
Why Streaming Telemetry?

Cisco IOS XE is the Network Operating System for the Enterprise. It runs on switches like the Catalyst 9000, routers like the ASR 1000, CSR1000v, and ISR 1000 and 4000's, Catalyst 9800 Wireless LAN controllers, as well as a few other devices in IoT and Cable product lines. Since the IOS XE 16.6 release there has been support for model driven telemetry, which provides network operators with additional options for getting information from their network.

Terraform blog and resources

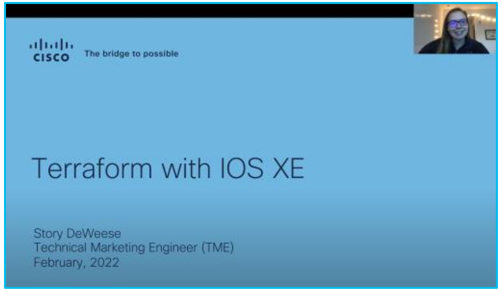
Questions? Join the Ask IOS XE Terraform Provider Webex space: https://eurl.io/#PtsT8eJFI

https://github.com/CiscoDevNet/terraform-provider-iosxe/
https://registry.terraform.io/search/providers?namespace=CiscoDevNet



```
Initializing provider plugins...
- Reusing previous version of ciscodevnet/iosxe from the dependency lock file
- Using previously-installed ciscodevnet/iosxe v0.1.1

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
auto@pod29-xelab:~/terraform/new-tunne$ terraform apply -auto-approve
9300X-Edge-2#
9300X-Edge-2#
9300X-Edge-2#
9300X-Edge-2#
9300X-Edge-2#
9300X-Edge-2#
9300X-Edge-2#
9300X-Edge-2#
```

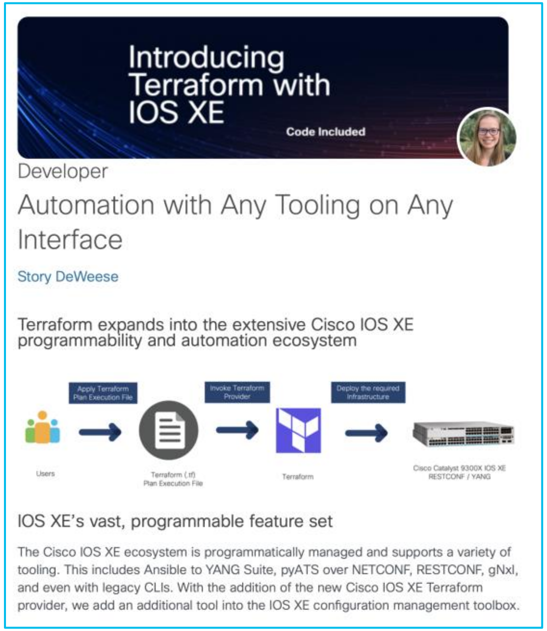
Demo Create a Crypto Tunnel Video:
https://www.youtube.com/watch?v=bPS0bhPacDw



Terraform with IOS XE

Story DeWeese
Technical Marketing Engineer (TME)
February, 2022

Intro to IOS XE Terraform Provider Video:
https://www.youtube.com/watch?v=GEY_hyXimbA


Introducing Terraform with IOS XE
Code Included

Developer

Automation with Any Tooling on Any Interface

Story DeWeese

Terraform expands into the extensive Cisco IOS XE programmability and automation ecosystem

Apply Terraform Plan Execution File
Invoke Terraform Provider
Deploy the required Infrastructure
Users
Terraform (.tf) Plan Execution File
Terraform
Cisco Catalyst 9300X IOS XE RESTCONF / YANG

IOS XE's vast, programmable feature set

The Cisco IOS XE ecosystem is programmatically managed and supports a variety of tooling. This includes Ansible to YANG Suite, pyATS over NETCONF, RESTCONF, gNxI, and even with legacy CLIs. With the addition of the new Cisco IOS XE Terraform provider, we add an additional tool into the IOS XE configuration management toolbox.

https://blogs.cisco.com/developer/terraformiosxe01

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.

- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard” at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue Your Education

- Visit the Cisco Showcase for related demos.
- Book your one-on-one Meet the Engineer meeting.
- Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

The bridge to possible

Thank you

cisco Live!

ALL IN