
cisco Live!
GO BEYOND
#CiscoLiveAPJC

Atomic Config Replace with Cisco Catalyst 9000

Story DeWeese & Ashil Parekh
Technical Marketing & Product Management
@StoryDeWeese

DEVNET-2385

Agenda

- Misconfiguration Consequences
- Atomic Config Replace
- Demo
- NETCONF CLI RPC
- Resources

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-2385

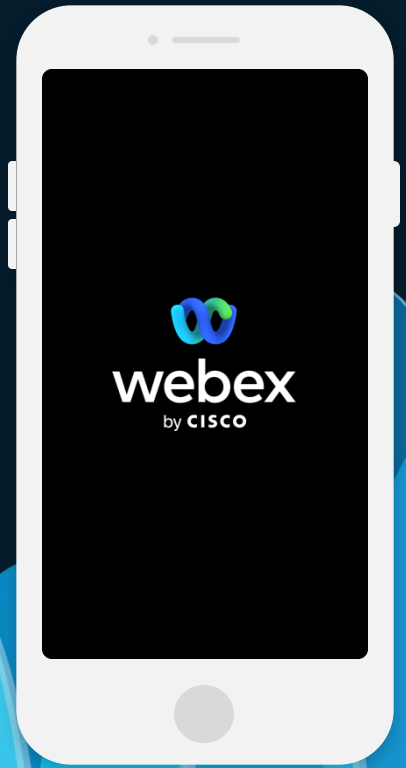
Questions?

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 by the speaker until November 15, 2024.



cisco Live!

NETWORK
OUTAGE

SECURITY
BREACH

State of Network Misconfigurations

45%

Network-related outages are caused by configuration failure[1]

22%

Data breaches are caused by human error[2]

$1 Million

25% respondents said their most recent outage cost more than $1 million [1]

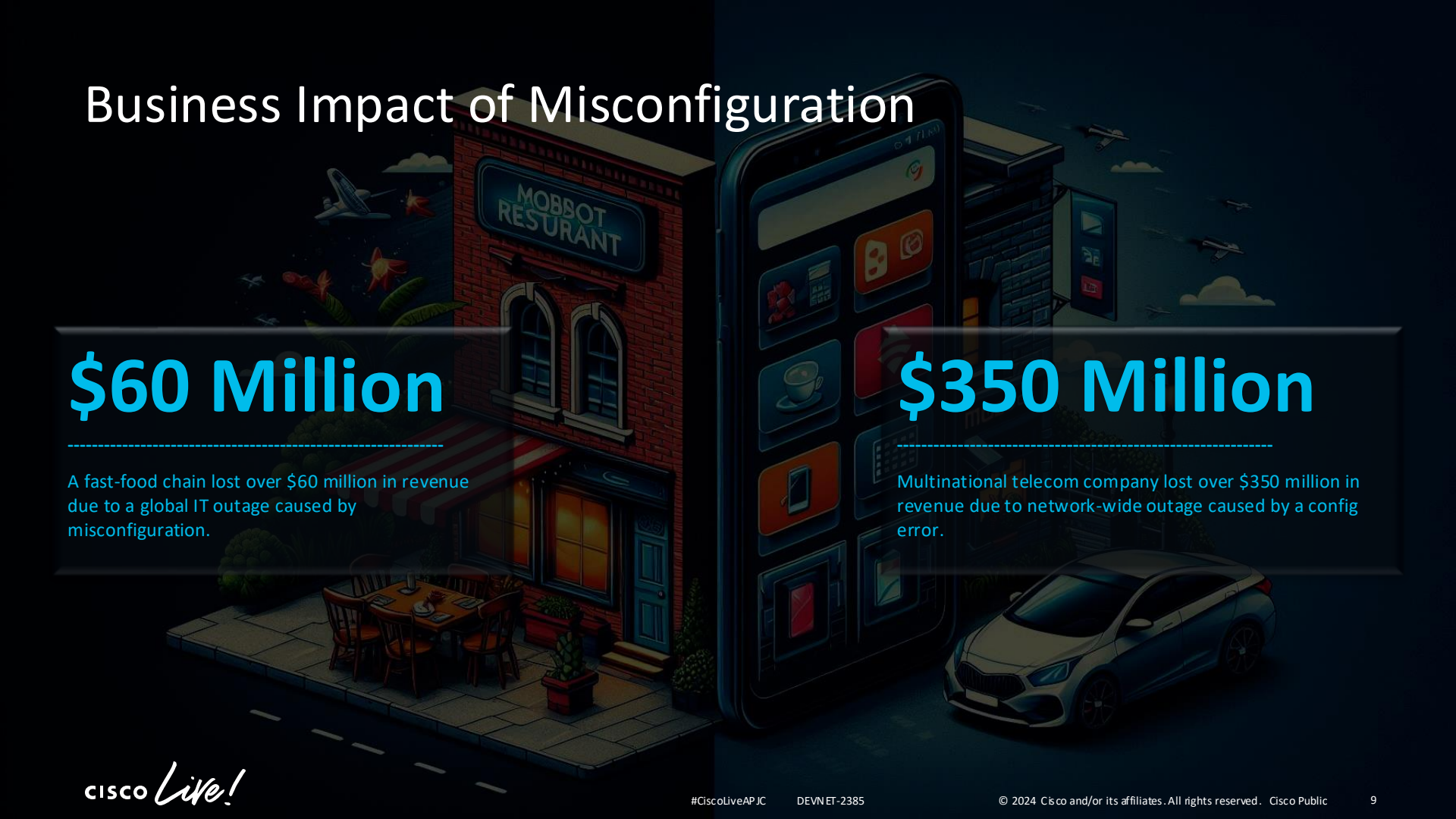
$4.8 Million

Is the global average cost of a data breach, increased by 10% compared to the previous year

[1] - Annual outages analysis 2023 – Uptime

[2] - Cost of a Data Breach Report 2024 - IBM

Business Impact of Misconfiguration



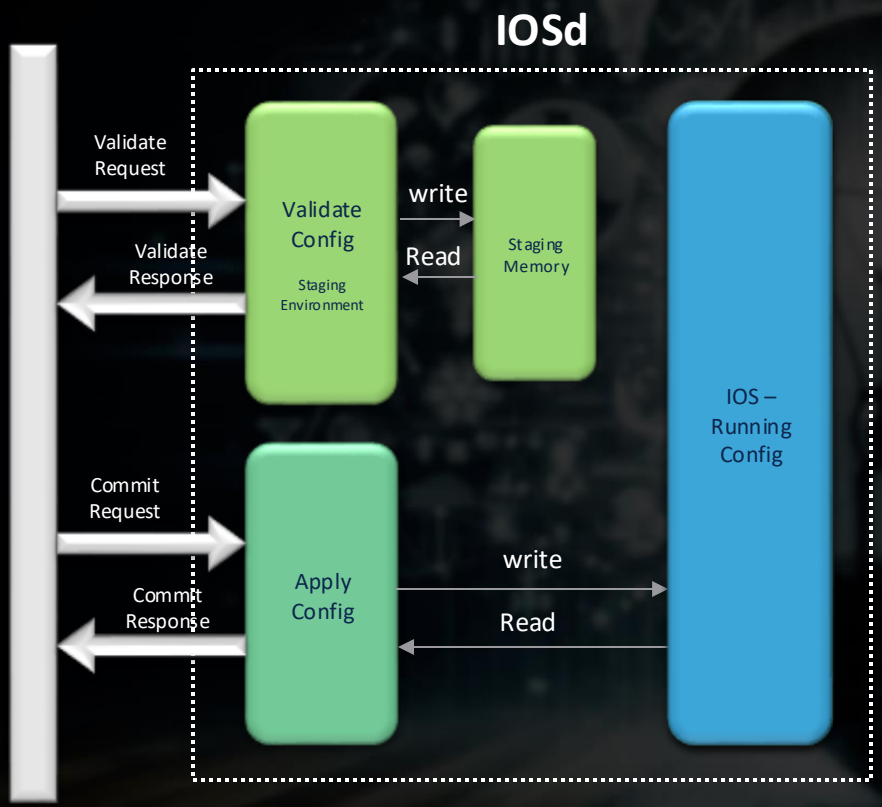
$60 Million

A fast-food chain lost over $60 million in revenue due to a global IT outage caused by misconfiguration.

$350 Million

Multinational telecom company lost over $350 million in revenue due to network-wide outage caused by a config error.

Introducing Atomic Configuration Replace



Validate Configuration

System verifies configuration integrity before applying. Catches potential errors early

Atomic Transaction

Apply configuration changes as a single transaction. All changes succeed, or none do

Config Rollback

If issues arise, revert to last known good configuration immediately

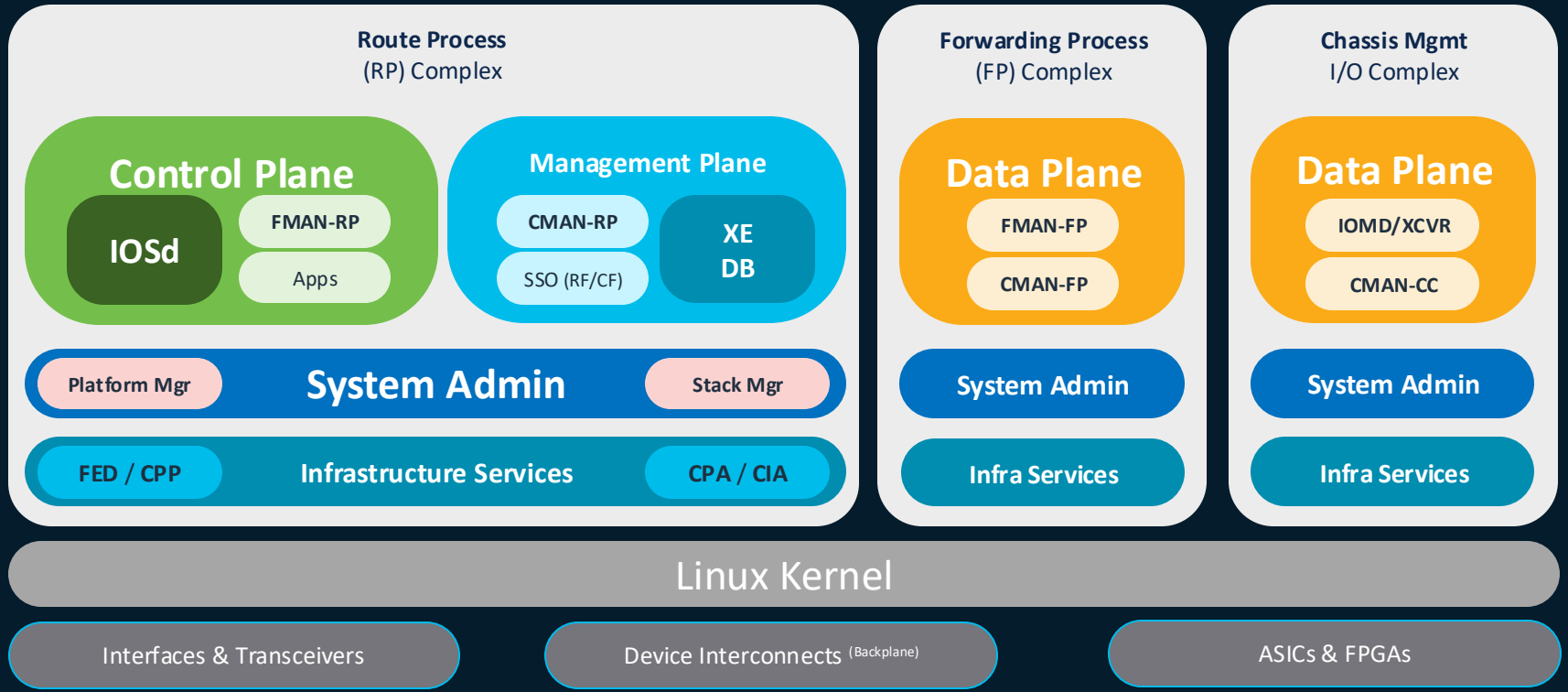
Evaluating ACR Benefits

Without Atomic Replace		With Atomic Replace
Manual Verification	Config Verification	Syntax, Semantic and Dependency Verification
Immediate Command Execution - Incremental Changes	Config Changes	Pre-Validated Configuration Deployment - Transactional Integrity
Costly configuration errors, Reactive troubleshooting with high risk of outage	Troubleshooting & Outage	Proactive error prevention and reduced risk of outage to enable seamless network management
Errors can leave the network exposed with higher risk of non-compliant configurations	Security & Compliance	Ensures adherence to security policies and compliance requirements

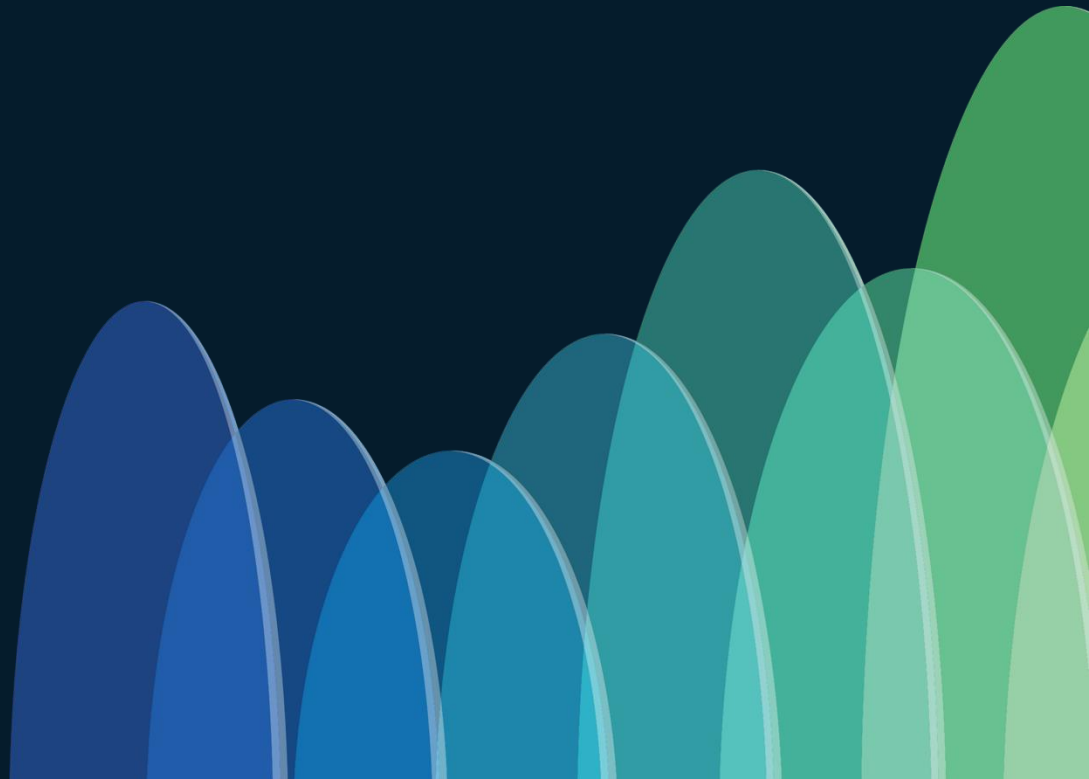
VS

Cisco IOS XE Architecture

Modularized Components for Software Abstraction

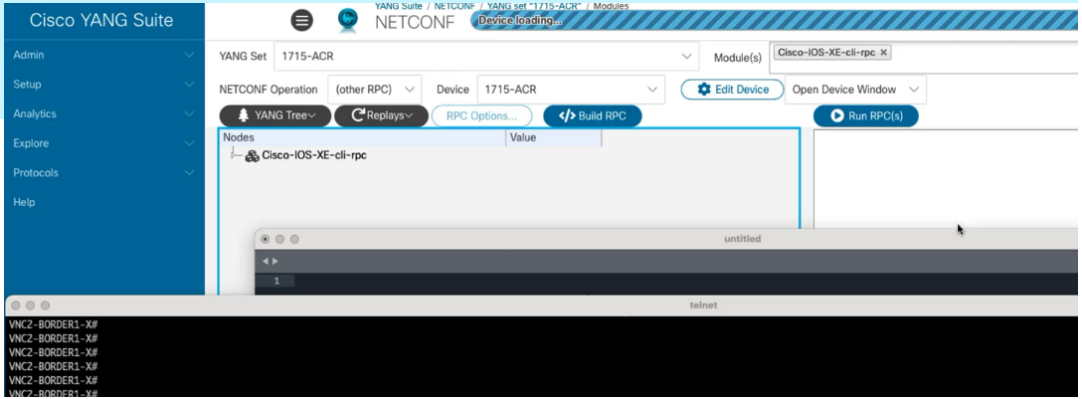


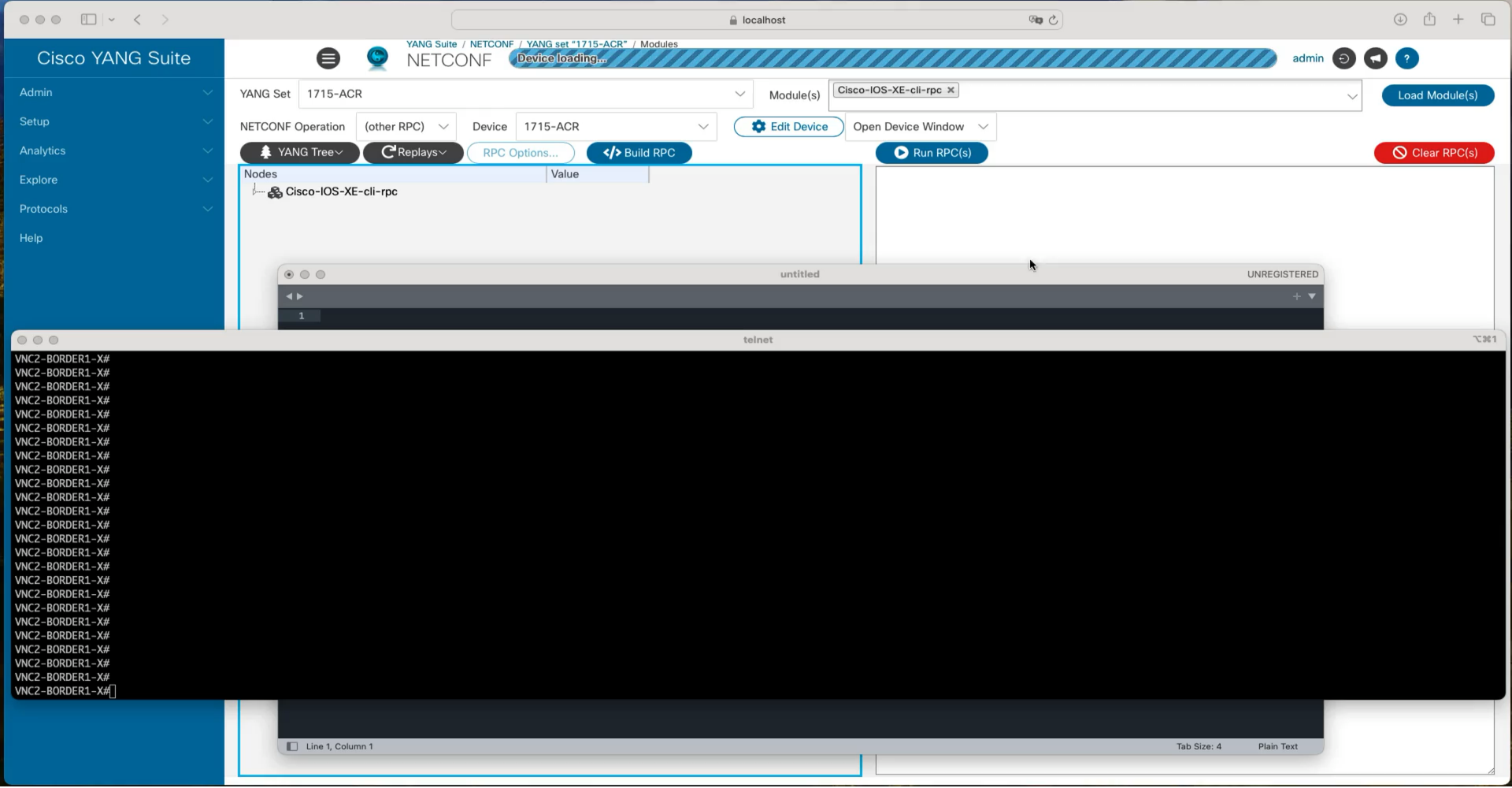
Demo



Detailed Demo Workflow

1. Load IOS XE release and CLI RPC YANG into YANG Suite
2. Run get-modelling-config-cli RPC to retrieve CLI config
3. Modify complete or partial config for supported features
4. Create new RPC using config-ios-cli-trans with operation “full” or “selective” replace
5. Send updated CLI payload into “clis” leaf
6. Verify change in YANG Suite payload
7. Verify change on C9300 console
8. Verify change in show run

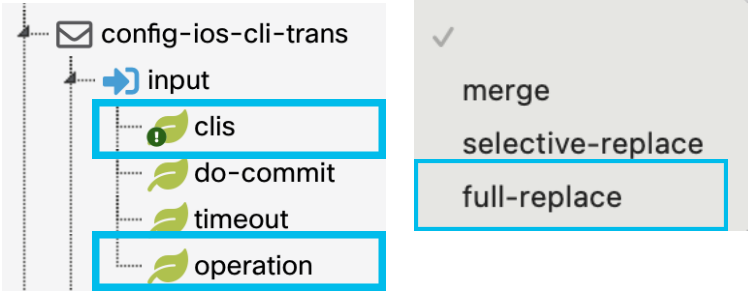




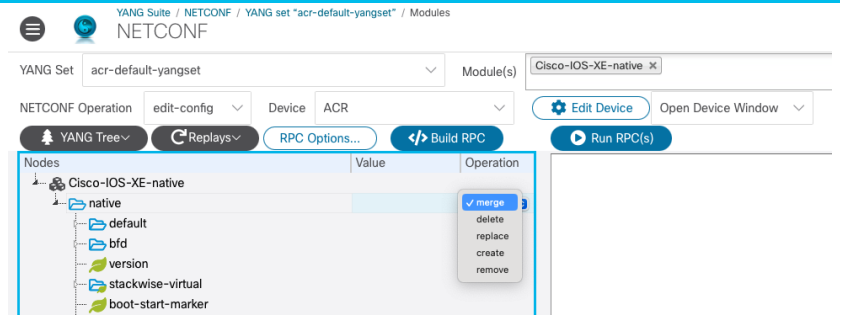
Atomic Config Replace - ACR

Atomic Config Replace enables full or partial config replace
Ability to send an entire configuration to the device in an XML/JSON payload
Support for traditionally documented CLI's over the CLI-RPC.YANG

Full and selective replace supported as part of CLI RPC over NETCONF/YANG



Merge, Replace operations supported as part of NETCONF/YANG

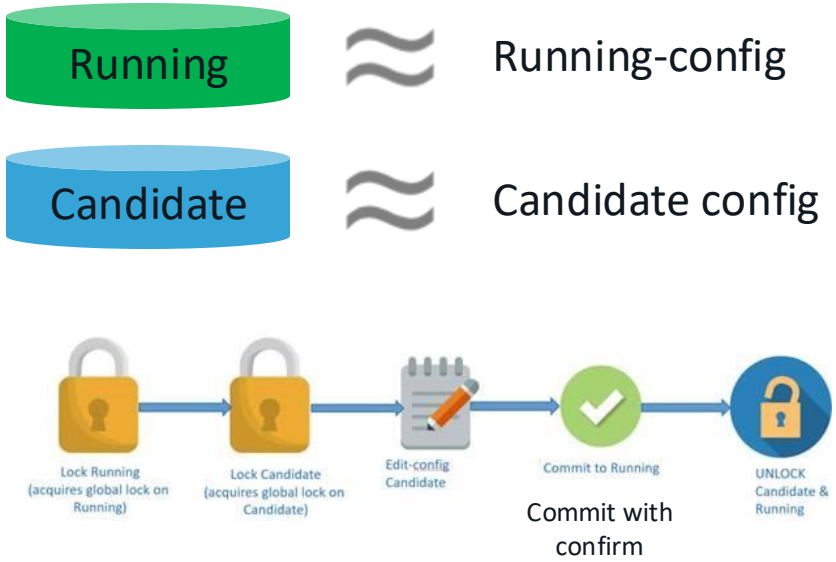


IOS XE NETCONF Datastores *

"A Datastore holds a copy of the configuration data that is required to get a device from its initial default state into a desired operational state"

Running is the default and only mandatory Datastore

The Candidate Configuration feature enables support for candidate capability by implementing RFC 6241 with a simple commit option.
The candidate datastore provides a temporary workspace in which a copy of the device's running configuration is stored.
The candidate configuration supports the confirmed commit capability



* Recommend to use running datastore only during this phase

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/1713/b_1713_programmability_cg/m_1713_prog_yang_netconf.html#id_78218

2-Stage Commit

- The 2-Stage commit process includes error and syntax checking
- It enabled a multi-stage commit process with verify before apply
- It is a non-disruptive application processes for the changes – no impact to packet processing
- 2-Stage Commit is only seen when config is rejected as there is no disruption to service

```
VNC2-BORDER1-X#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
VNC2-BORDER1-X(config)#yang-interfaces feature ios-two-stage
VNC2-BORDER1-X(config)#end
VNC2-BORDER1-X#sh run | i two-stage
yang-interfaces feature ios-two-stage
VNC2-BORDER1-X#
```

Enable 2-stage commit with	# yang-interfaces feature ios-two-stage
CLI will be simplified to	# yang-interfaces features atomic-config

Full-Replace vs Selective-Replace

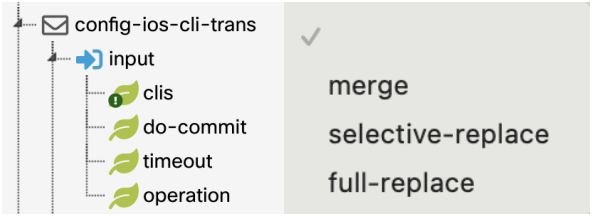
Full-replace

Full configuration replace – full config must be provided
This is the declarative approach where the config "delta" is computed and applied by IOS XE

Selective-replace

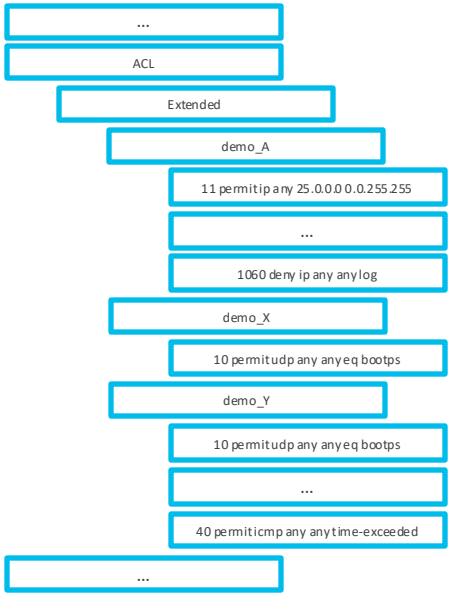
Partial Payload
Just the CLI/configs to update
Imperative Approach:

- DemoA updated
- DemoZ added
- Demo X Y unchanged
- Send "no" operation for Demo X Y to remove



Selective-replace

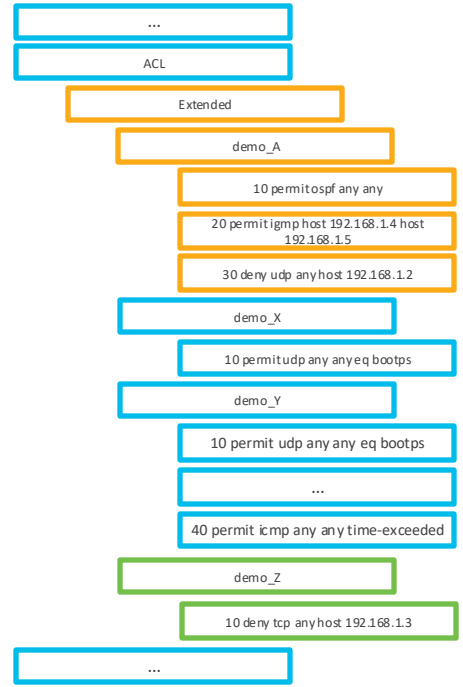
Original running-config



Selective-replace payload

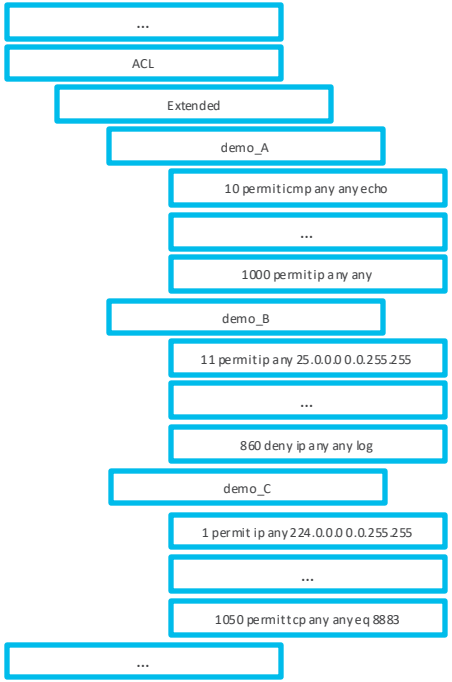
```
ip access-list extended demo_A
 10 permit ospf any any
 20 permit igmp host 192.168.1.4 host 192.168.1.5
 30 deny udp any host 192.168.1.2
ip access-list extended demo_Z
 10 deny tcp any host 192.168.1.3
```

Resulting running-config

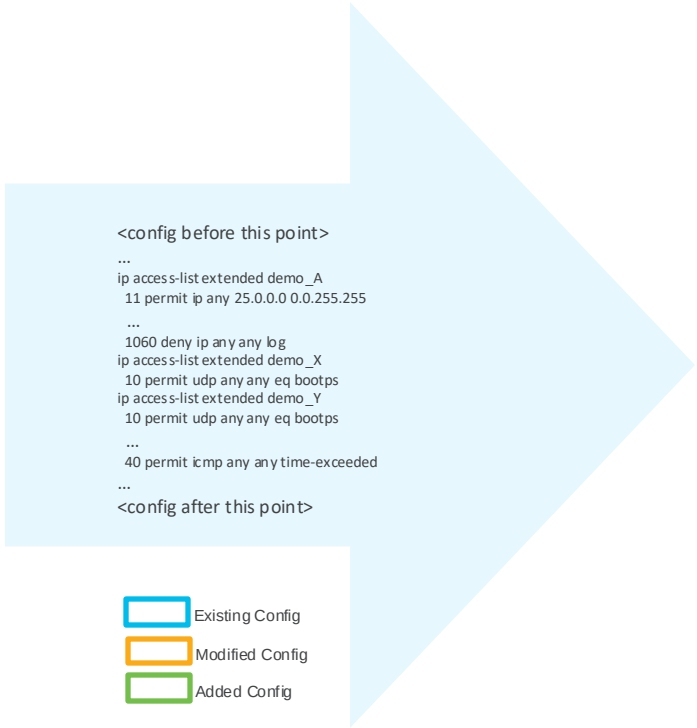


Full-replace

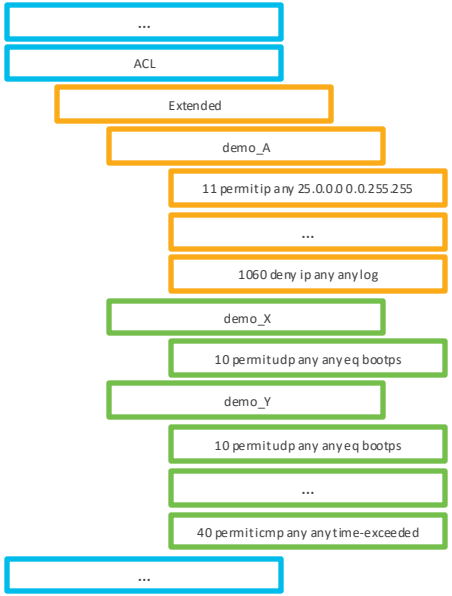
Original running-config



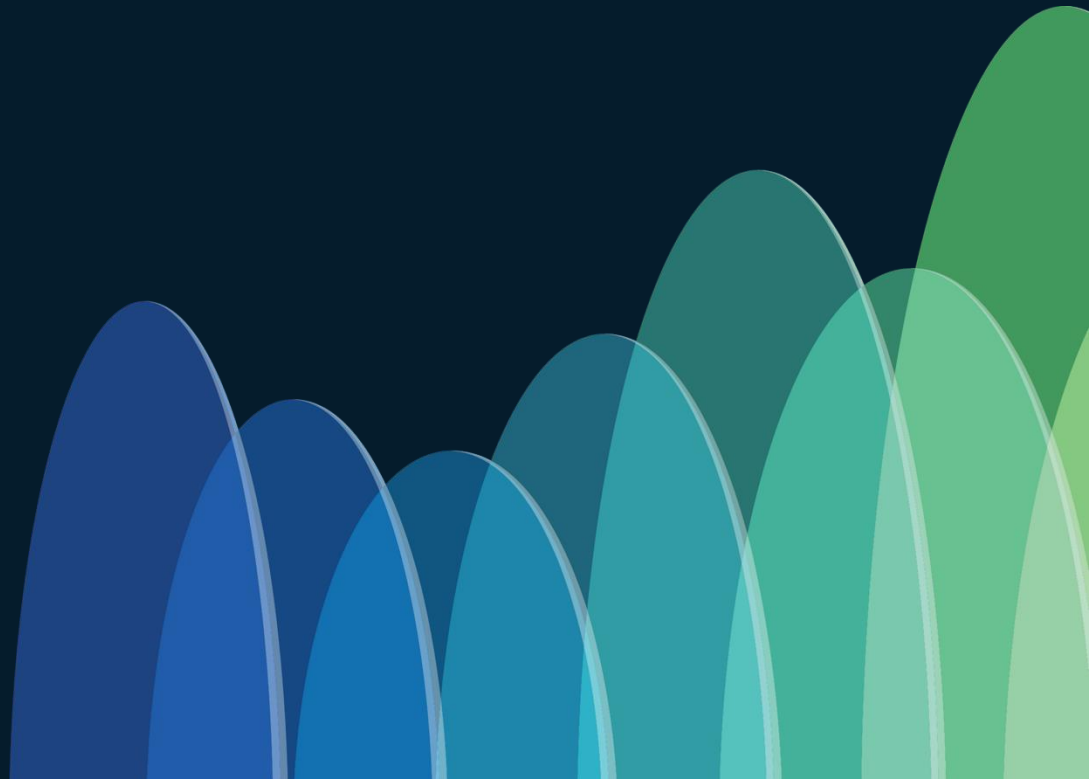
Full-replace payload



Resulting running-config



NETCONF CLI RPC



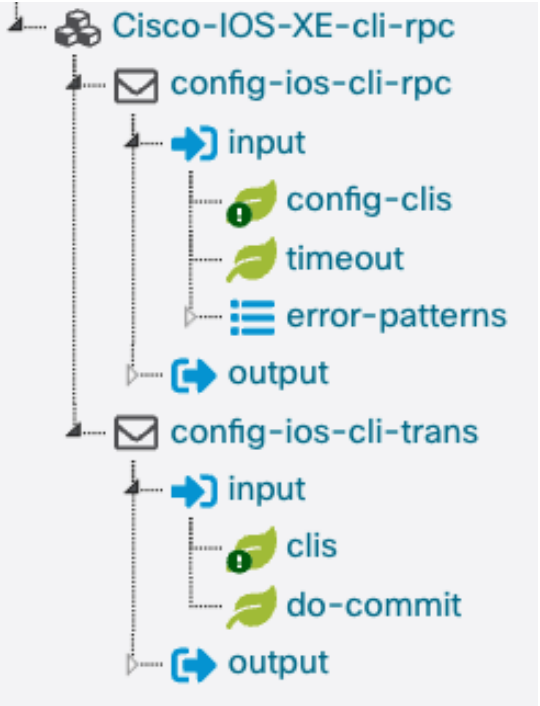
Original 17.9

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

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

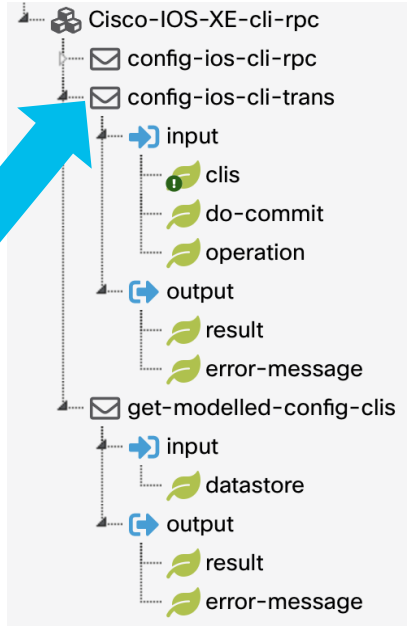
This is similar to sending edit-config RPCs corresponding to the CLI's.

Synchronized from ConfD into the CLI running-config

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

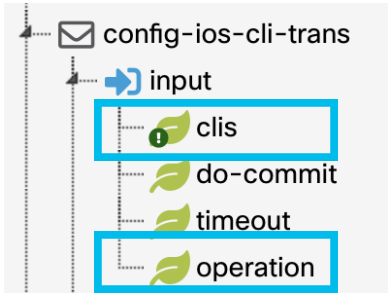
Cisco-IOS-XE-CLI-RPC.YANG

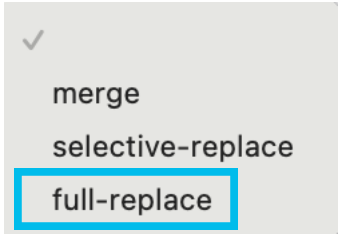
This YANG data model allows sending CLI through the YANG API interfaces
Previously only YANG modelled data was supported



Name	config-ios-cli-trans
Nodetype	rpc
Description	Configure using modelled config CLI. Wireless, app-hosting, telemetry features are not supported through this RPC.
Module	Cisco-IOS-XE-cli-rpc
Revision	2023-11-01
Xpath	/config-ios-cli-trans
Prefix	cli-ios-xe-rpc
Namespace	http://cisco.com/ns/yang/Cisco-IOS-XE-cli-rpc
Schema Node Id	/config-ios-cli-trans
Access	write
Operations	• "rpc"

Name	get-modelled-config-clis
Nodetype	rpc
Description	Retrieve configuration in CLI format from Running or Candidate datastore. Wireless, app-hosting, telemetry features are not supported through this RPC.
Module	Cisco-IOS-XE-cli-rpc
Revision	2023-11-01
Xpath	/get-modelled-config-clis
Prefix	cli-ios-xe-rpc
Namespace	http://cisco.com/ns/yang/Cisco-IOS-XE-cli-rpc
Schema Node Id	/get-modelled-config-clis
Access	write
Operations	• "rpc"

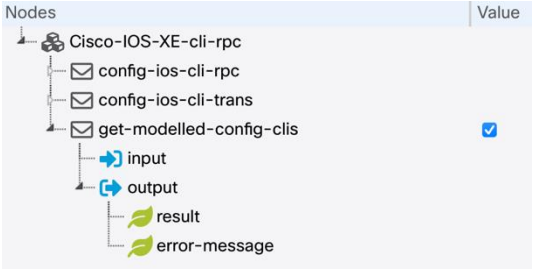




https://github.com/YangModels/yang/blob/main/vendor/cisco/xe/1791/Cisco-IOS-XE-cli-rpc.yang

Get Modelled Config CLI RPC

- Sending the “get-modelled-config-clis” RPC returns the modelled running-config in CLI format
- Anything not modelled will not be returned (AppH)
- Unsupported model config will be ignored (AppH)
- This is used as the template to update the device with after being modified as needed



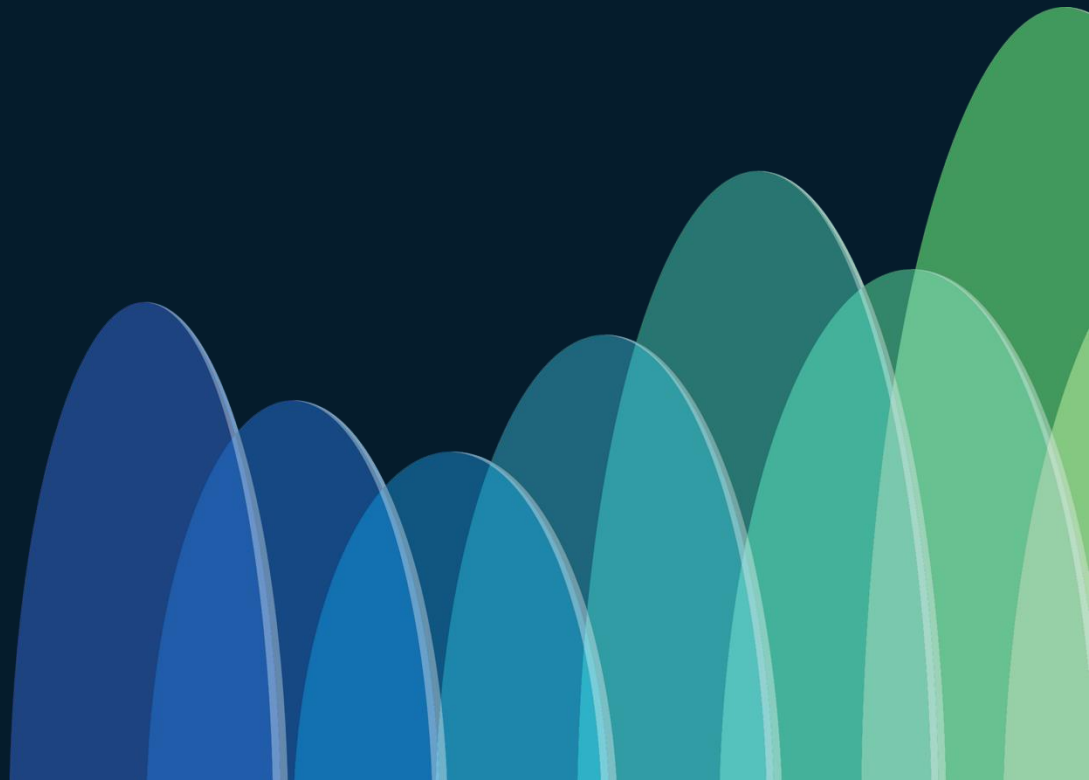

```
Sending:
#246
<nc:rpc xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="urn:uuid:afff
  <get-modelled-config-clis xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-cli-rpc"/>
</nc:rpc>


##
```

```
Received message from host
```

```
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns:nc="urn:ietf:params
<result xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-cli-rpc">version 17.14
memory free low-watermark processor 130582
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
no service tcp-small-servers
no service udp-small-servers
hostname JCOHOE-C9300-2
control-plane
 service-policy input system-cpp-policy
!
clock summer-time PDST recurring
clock timezone pacific -8 0
login on-success log
license boot level network-advantage addon dna-advantage
transceiver type all
 monitoring
!
iox
call-home
 contact-email-addr sch-smart-licensing@cisco.com
 profile CiscoTAC-1
  active
  destination transport-method http
```

```
RPC:
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <get-modelled-config-clis xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-cli-rpc"/>
</rpc>
```

Ready to get hands-on?

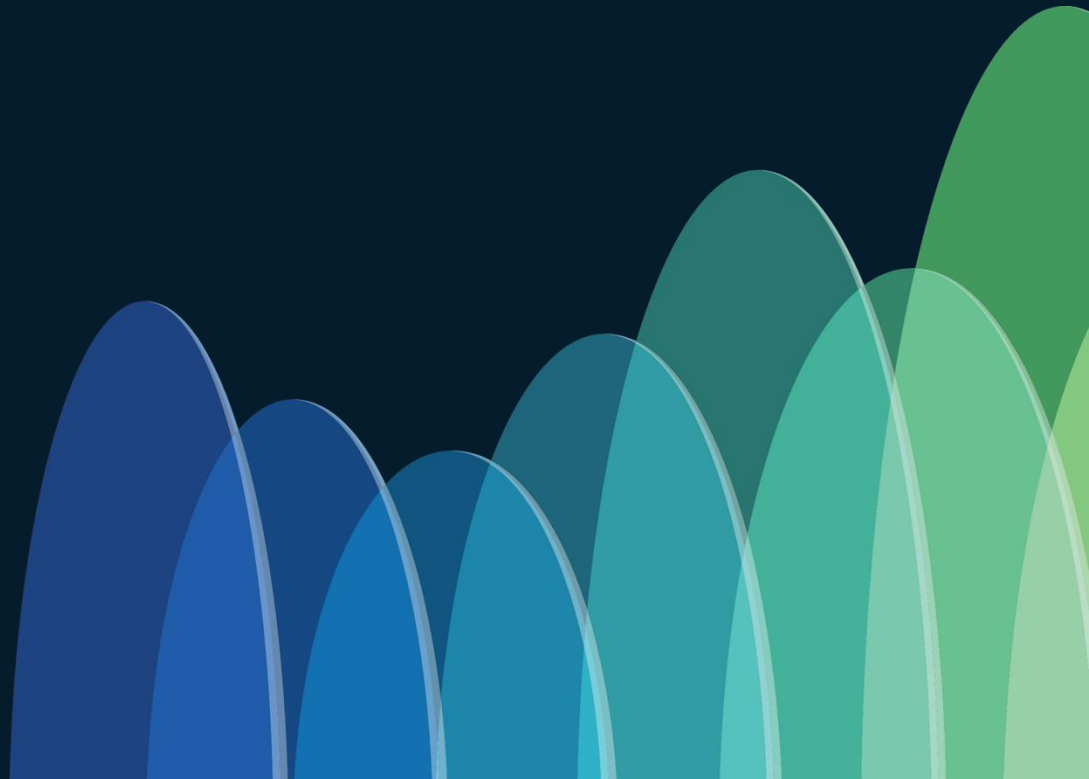


ACR : Scope and Limitations

- Validates only device-level configurations
  - Network-level configurations are not validated
- Pre-Release Feature : Available for Early Field Trials
- Supported only on Cat9300 & Cat9500
- Supported on programmable interfaces;
  - Exclusively with NETCONF & NETCONF CLI RPC
- Works with limited set of features

Category	Features
Basic L2	Ethernet interfaces, Port channel interfaces, Port channel, Spanning tree, LACP, Logging, Err-disable
L3 and SVL	VRF, VLAN interfaces, Loopback interfaces, IP, IP DHCP, IP Route, MPLS, ARP, Track
Policy (Security and Others)	Class-map, Policy-map, Route-map, AAA, Ssh, IP ACL, TACACS, Crypto, certs etc, Username
Management, Device configuration and access etc.	HTTP, SNMP, Banner, Line, NTP, Monitor, Call home, Hostname, Service, Archive, PnP, Event Manager

Resources



cisco Live!

Keynote Deep Dives

Wednesday
10:30am –11:30am

Experiences Amplified: How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106

Smart, Secure, Seamless: Transforming Experiences with Next-Generation Networking

Level 2
Room 204

Harness a Bold New Era: Transform Data Centre and Service Provider Connectivity

Level 2
Room 203

Securing User to Application and Everything in Between

Level 2
Melbourne Room 2

Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.

Complete your surveys in the **Cisco Live mobile app**.

Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand


cisco
Thank you
cisco Live!
#CiscoLiveAPJC


cisco Live!
GO BEYOND
#CiscoLiveAPJC