The bridge to possible

Managing and Accessing Remote IoT Equipment with Cloud Management

Emmanuel Tychon
@ManuNetworking

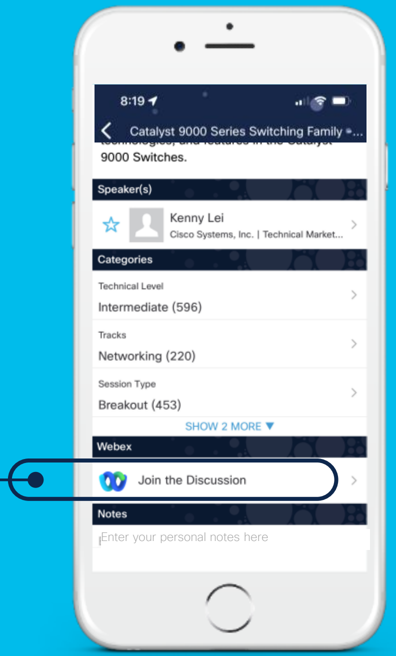
Cisco Webex App

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



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

Webex spaces will be moderated
until February 24, 2023.

Agenda

- Cisco IoT Remote and Mobile Routers
- Edge Device Manager (EDM)
- Application Management (IOx)
- Secure Equipment Access (SEA)
- Conclusion

Introduction

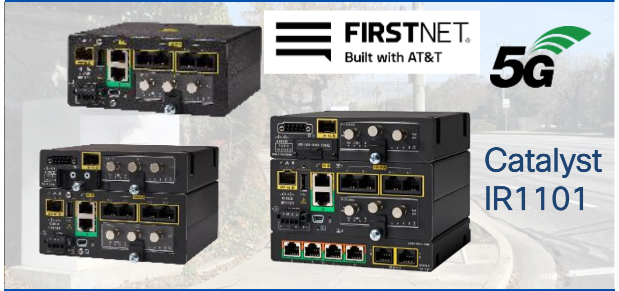
Cisco IoT Remote and Mobile Routers

A complete portfolio

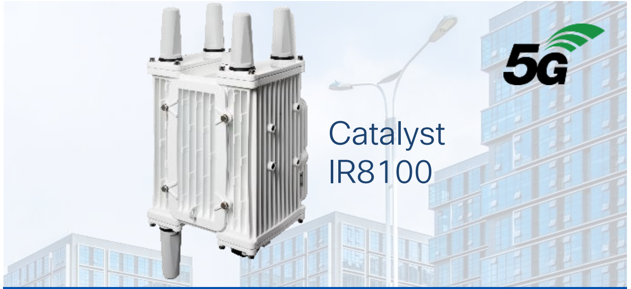
Secured and optimized for *every* use case

Demanding, mission critical deployments

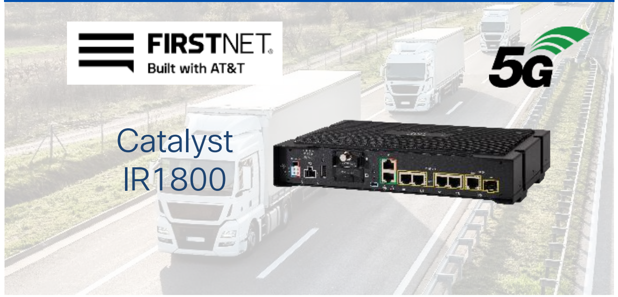
ATMs, low voltage substations, roadside traffic cabinets



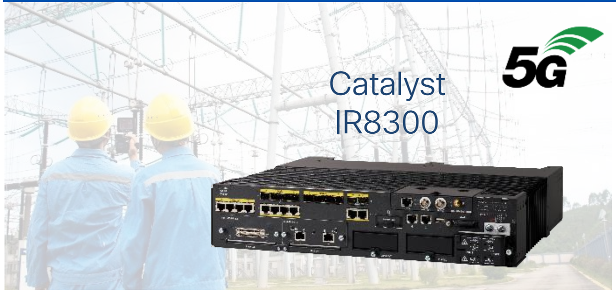
Remote monitoring, streetlights, intersections



Fleet, first-responders, pipelines



Mission-critical, Factory, high voltage substations



“What makes IoT routers unique compared to non-IoT routers?"

Cisco Industrial Routers Purpose Built for Harsh Environments

1 Size Weight Form-factor

2 Shock and Vibration Resistance

3 High MTBF Resilient Network Topologies

4 Din-Rail or Rack Mounts

5 Fanless -40 - +75°C Self-cooled

6 Industry Certifications

Catalyst IR1800 Industrial Router

Cisco Catalyst Industrial Router

Intent-based Networking

Built for harsh environments

Born for IP (v4 and v6)

Edge compute

Industry-leading security

Interoperable

SD-WAN enabled

5G Today

One Network

Industrial certifications

Enterprise and Operational Tools

Operations security

IR1800 Series Routers

Features	IR1821-K9	IR1831-K9	IR1833-K9	IR1835-K9
Processor (ARM 4 core)	600 MHz	600 MHz	600 MHz	1200MHz
Memory	4GB	4GB	4GB	8GB
LTE Slot	one	two	two	two
Wi-Fi6 Module	✓	✓	✓	✓
CAN Bus	✓	✓	✓	✓
PoE	✗	✗	✓	✓
mSATA Module	✗	✗	✓	✓
Automotive Dead Reckoning GNSS (Module)	✗	✗	✓	✓
GPIO	✗	✗	✗	✓
Serial Interface	RS232 (1)	RS232 (2)	RS232 (2)	RS232, RS232/485

Mobile Assets – IR1800

- Flat mounted for easy installation in vehicles, behind or under seats
- Ignition power management to prevent battery drain
- External antenna for WiFi, GPS, Cellular for external mounting
- Low power usage with CANBUS communication protocol

Example: mounted in an electricity maintenance van

Cisco Catalyst IR1101 Rugged Series Router

Expansion modules for more interfaces

SD-WAN IOS-XE unified image

First IoT Router with IOS XE
High-end security Programmability

Modular LTE (public/private) & 5G

Edge computing enabled*

Low average Power consumption of only 10W

IOS-XE unified image 17.2.1r
Classic IOS and SDWAN

Compact form factor for Din-rail installations

Investment protection

Lower TCO

Extended product lifetime

** edge compute on SDWAN is roadmap*

IR1101 Modularity

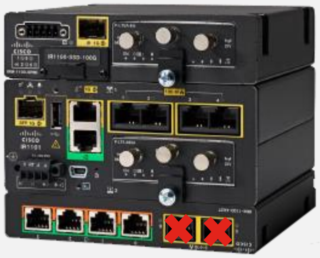
Deployment scenarios with expansion module

IR1101 + single Expansion Module

OR

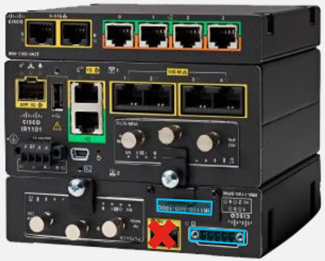
Majority of the use cases

IR1101 + LTE Expansion Module + Serial Expansion Module (Bottom)



Ethernet Ports on the expansion module will **not** work

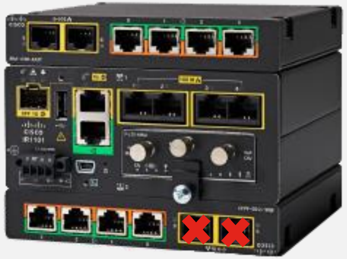
IR1101 + Serial Expansion Module + LTE Expansion Module (Bottom)



SFP on the expansion module will **not** work

MSATA and IO is on IOS-XE roadmap

IR1101 + 2x Serial Expansion



Ethernet ports on the expansion module in the bottom will **not** work

Ethernet Ports on Expansion Module total throughput limited to 1Gbps

Cellular Pluggable Interface Modules for Industrial Routers

Cellular Interface Modules

P-LTE-GB Cat4	P-LTE-US Cat4	P-LTE-VZ Cat4	P-LTE-MNA Cat4	P-LTE-IN Cat4	P-LTE-JN Cat4	P-LTEA-EA P-LTEA-LA Cat6	P-LTEAP18-GL Cat18	P-5GS6-GL 5G Sub-6GHz
↓ 150 Mbps	↓ 150 Mbps	↓ 150 Mbps	↓ 150 Mbps	↓ 150 Mbps	↓ 150 Mbps	↓ 300 Mbps	↓ 1.2 Gbps	↓ 3.5 Gbps
↑ 50 Mbps	↑ 50 Mbps	↑ 50 Mbps	↑ 50 Mbps	↑ 50 Mbps	↑ 50 Mbps	↑ 50 Mbps	↑ 150 Mbps	↑ 500 Mbps

FIRSTNET Built with AT&T

IR1101

FIRSTNET Built with AT&T

IR1821, IR1831, IR1833, IR1835

FIRSTNET Built with AT&T

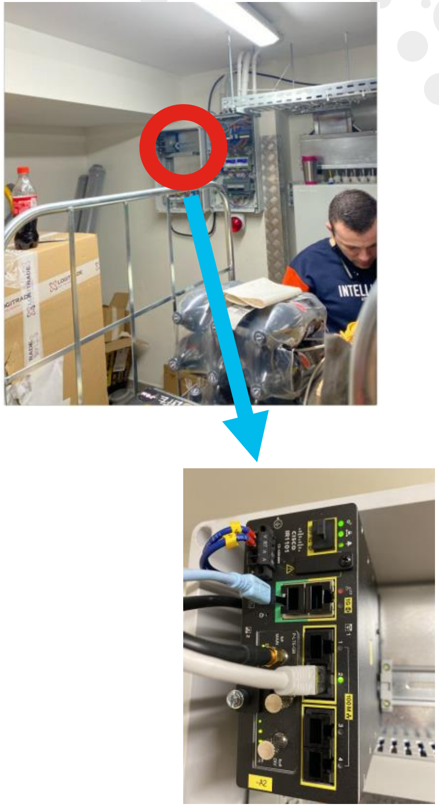
IR8100

IR8300

cisco Live!

Remote Location – IR1101

- IR1101 is perfectly suited for remote installations
- Small form factor to fit in DIN-rail cabinets
- Alarm input to detect when cabinet door open
- GigE / SPF / Cellular uplink with failover
- Modularity allows for changing reality after initial deployment



Example: mounted in a supermarket closet

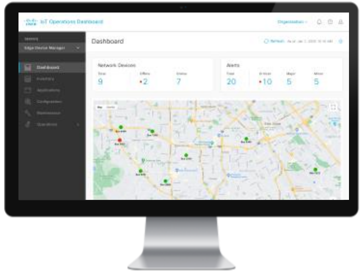
Cisco IoT Operations Dashboard

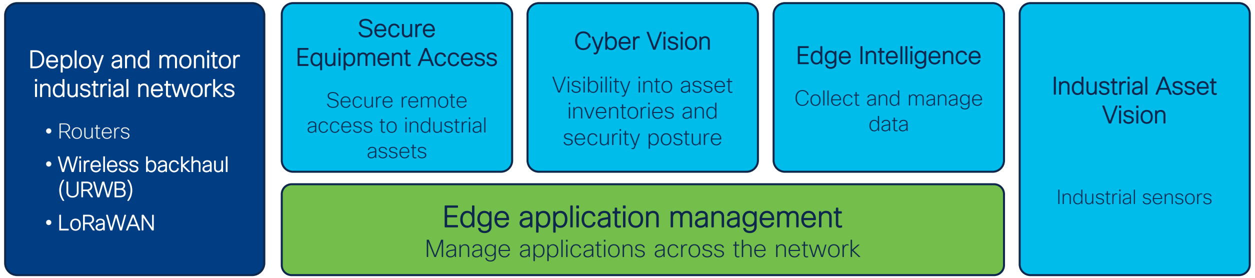
Edge Device Manager (EDM)

IoT Operations Dashboard

A cloud platform of OT services to connect, maintain and secure industrial assets and gain insights

IoT Operations Dashboard





Deploy and monitor industrial networks

- Routers
- Wireless backhaul (URWB)
- LoRaWAN

Secure Equipment Access

Secure remote access to industrial assets

Cyber Vision

Visibility into asset inventories and security posture

Edge Intelligence

Collect and manage data

Industrial Asset Vision

Industrial sensors

Edge application management

Manage applications across the network

Industrial networks

Industrial routing

Wireless backhaul

LoRaWAN

Roadway intersections | Transportation | Solar panels | EV chargers | Connected signage | Wind farms | Connected machines

What is Edge Device Manager (EDM)?

Core service in Cisco IoT OD to manage industrial network configurations at scale:

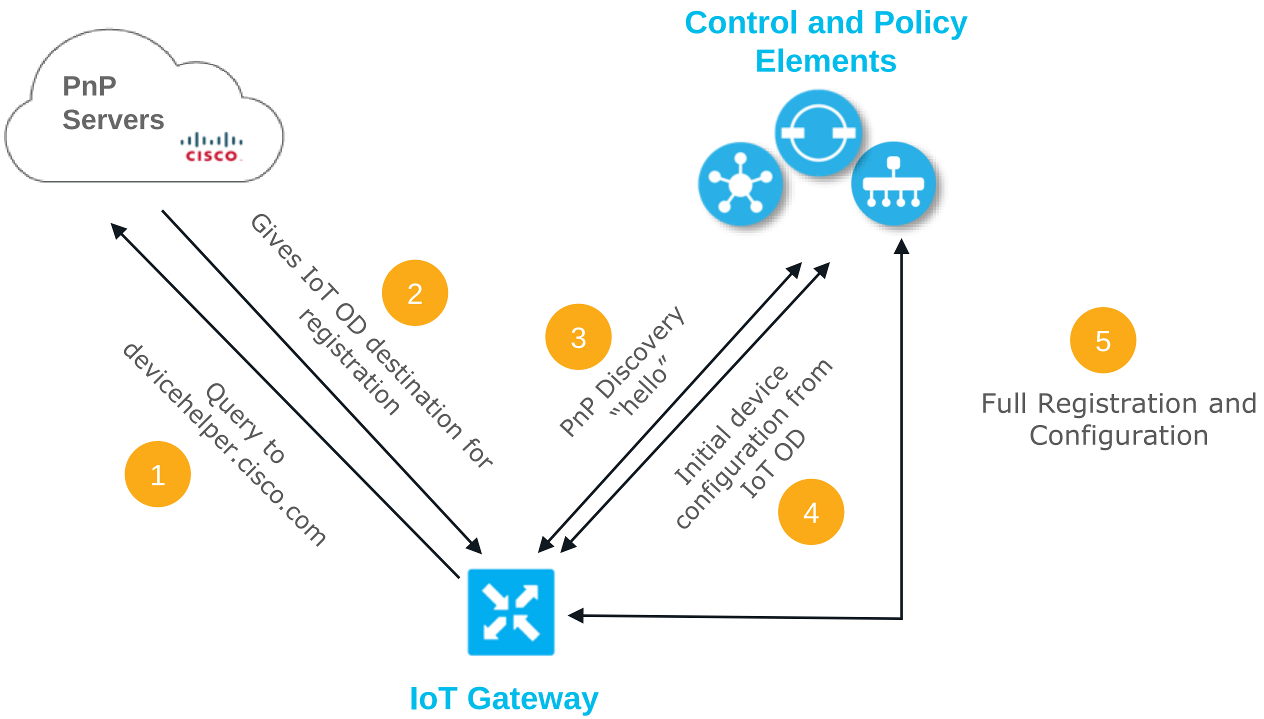
- Zero Touch Deployment (ZTD) using PnP Connect
- Configuration Management
- Visibility and Monitoring
- Troubleshooting Tools
- Software Upgrades (IOS, IOS-XE and embedded AP firmware)
- Cisco Validated Design Templates (eCVD)

Device Onboarding with PnP Connect

- Cisco cloud-based service to redirect devices to their management platform
- Leveraged by IoT OD, but also vManage and DNA-C
- Activates when the router boots without any configuration
- If pre-staging required, can be started by configuring:

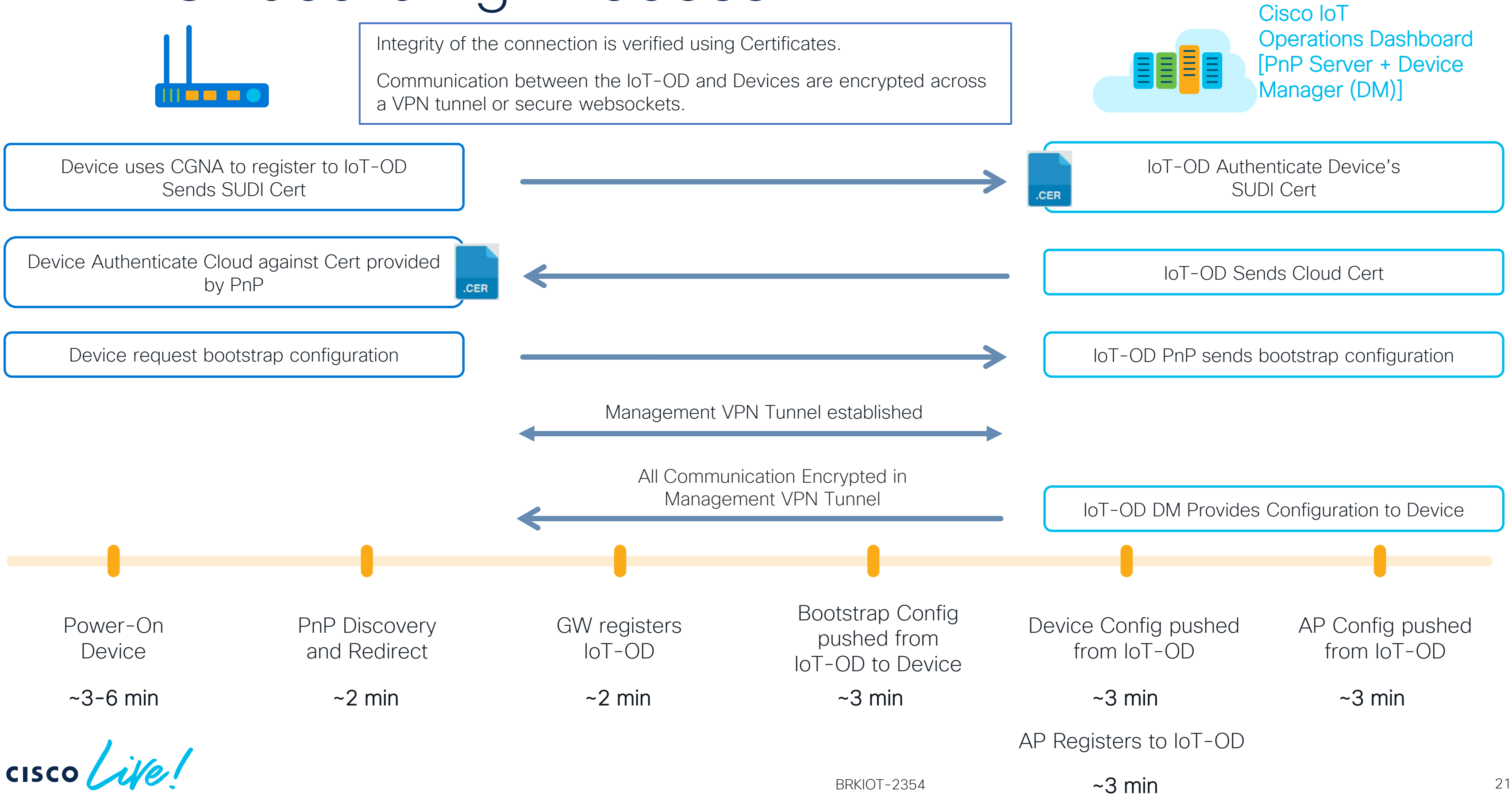
```
pnp profile pnp_cco_profile
  transport https host devicehelper.cisco.com port 443
```

On Boarding Gateway with PnP



PnP Servers
cisco
Control and Policy Elements
IoT Gateway
1
Query to devicehelper.cisco.com
2
Gives IoT OD destination for registration
3
PnP Discovery "hello"
4
Initial device configuration from IoT OD
5
Full Registration and Configuration

EDM Onboarding Process



Integrity of the connection is verified using Certificates.

Communication between the IoT-OD and Devices are encrypted across a VPN tunnel or secure websockets.

Cisco IoT Operations Dashboard [PnP Server + Device Manager (DM)]

Device uses CGNA to register to IoT-OD Sends SUDI Cert → IoT-OD Authenticate Device's SUDI Cert

Device Authenticate Cloud against Cert provided by PnP ← IoT-OD Sends Cloud Cert

Device request bootstrap configuration → IoT-OD PnP sends bootstrap configuration

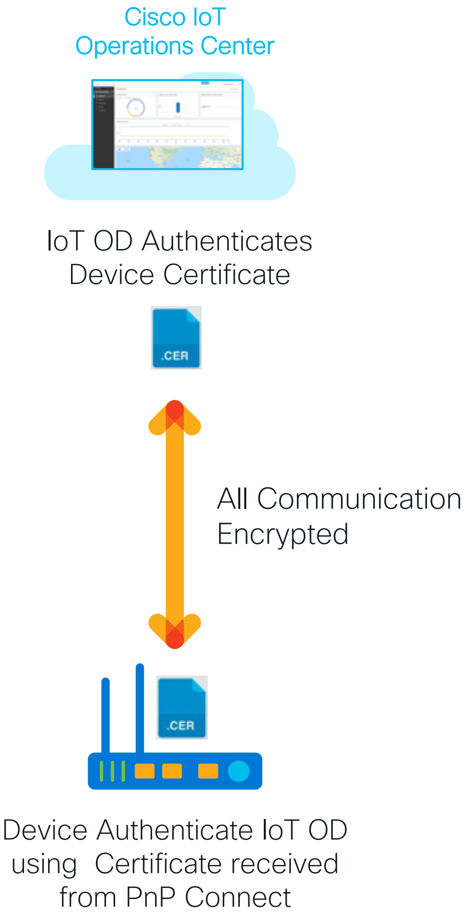
Management VPN Tunnel established

All Communication Encrypted in Management VPN Tunnel ← IoT-OD DM Provides Configuration to Device

Power-On Device	PnP Discovery and Redirect	GW registers IoT-OD	Bootstrap Config pushed from IoT-OD to Device	Device Config pushed from IoT-OD	AP Config pushed from IoT-OD
~3-6 min	~2 min	~2 min	~3 min	~3 min	~3 min
				AP Registers to IoT-OD	
				~3 min	

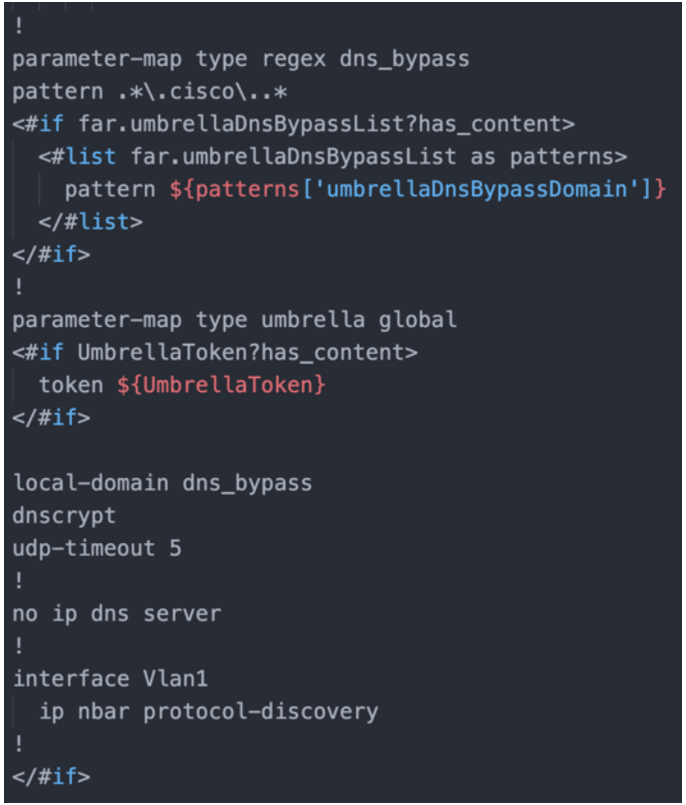
Onboarding Device Security

- Integrity of the connection is verified using Certificates.
- Gateway validates this is IoT OD by challenging a certificate received during PnP.
- IoT OD validates this is the right gateway by challenging the device SUDI crypto cert.
- Communication between IoT OD and Devices are encrypted across a VPN tunnel or secure WebSocket.



Template-based Configuration

- Leveraging template language Apache FreeMarker
- Write your own configuration from scratch
- Or use Cisco-provided eCVD templates
- Examples: https://github.com/etychon/eCVD-Templates

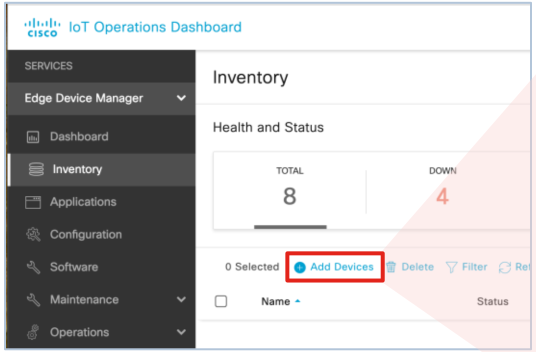


```
!
parameter-map type regex dns_bypass
pattern .*\.cisco\..*
<#if far.umbrellaDnsBypassList?has_content>
  <#list far.umbrellaDnsBypassList as patterns>
    pattern ${patterns['umbrellaDnsBypassDomain']}
  </#list>
</#if>
!
parameter-map type umbrella global
<#if UmbrellaToken?has_content>
  token ${UmbrellaToken}
</#if>

local-domain dns_bypass
dnscrypt
udp-timeout 5
!
no ip dns server
!
interface Vlan1
  ip nbar protocol-discovery
!
</#if>
```

Onboard and Power On Gateway

Onboard gateway to IoT OD

Add the gateway to the config group you've just made



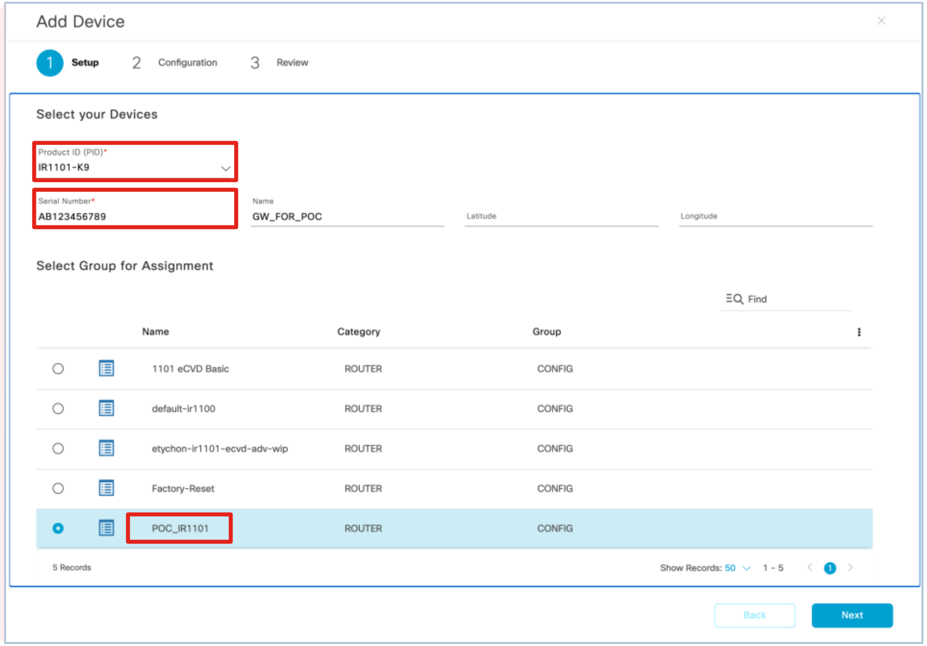
Inventory

Health and Status

TOTAL	DOWN
8	4

0 Selected Add Devices Delete Filter Re

□ Name Status



Select your Devices

Product ID (PID)*: IR1101-K9

Serial Number*: AB123456789

Name: GW_FOR_POC

Latitude

Longitude

Select Group for Assignment

Find

	Name	Category	Group
○	1101 eCVD Basic	ROUTER	CONFIG
○	default-ir1100	ROUTER	CONFIG
○	etychon-ir1101-ecvd-adv-wip	ROUTER	CONFIG
○	Factory-Reset	ROUTER	CONFIG
●	POC_IR1101	ROUTER	CONFIG

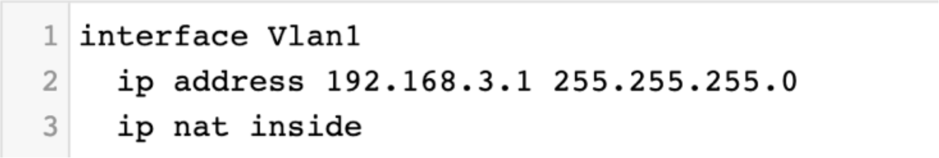
5 Records Show Records: 50 1 - 5 1

Leverage Templates for IT/OT separation

IT

- IT prepares a router configuration like usual
- Configuration contains all invariable parameters.

Base configuration:



```
interface Vlan1
  ip address 192.168.3.1 255.255.255.0
  ip nat inside
```

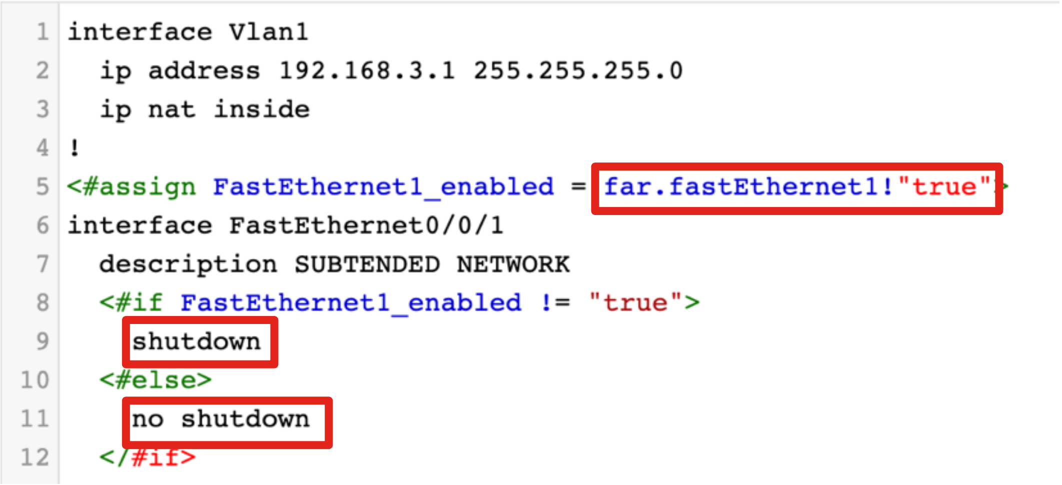
... but I also need to enable/disable FastEthernet1 on some gateways

Leverage Templates for IT/OT separation

IT

- **Variable** parameters are presented as options to the user
- IT uses Apache FreeMarker template language

Example:



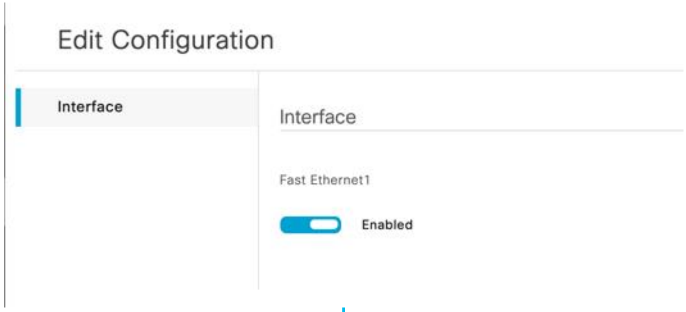
```
interface Vlan1
  ip address 192.168.3.1 255.255.255.0
  ip nat inside
!
<#assign FastEthernet1_enabled = far.fastEthernet1!"true">
interface FastEthernet0/0/1
  description SUBTENDED NETWORK
  <#if FastEthernet1_enabled != "true">
    shutdown
  <#else>
    no shutdown
  </#if>
```

Leverage Templates for IT/OT separation

OT

- OT users are only presented with parameters relevant to them
- In this case, there is only one parameter reducing the risk of error

Example:



Edit Configuration

Interface

Interface

Fast Ethernet1

Enabled

```
interface Vlan1
  ip address 192.168.3.1 255.255.255.0
  ip nat inside

interface FastEthernet0/0/1
  description SUBTENDED NETWORK
  no shutdown
```

Cisco IoT Operations Dashboard

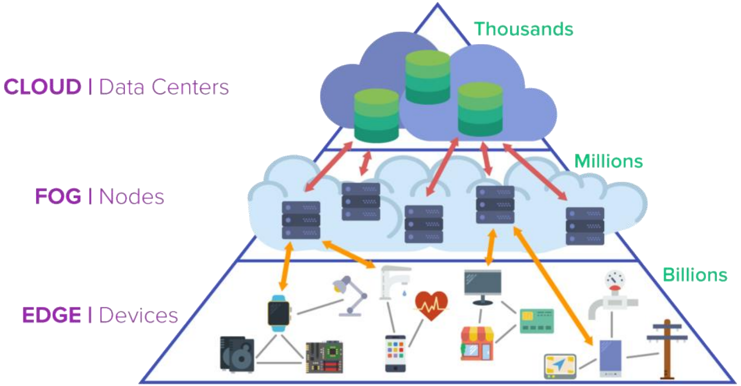
Application Management (IOx)

What is Cisco IOx?

- IOx is not IOS-XE, or IOS-XR, or NX-OS
- IOS and Linux = IOx
- Cisco IOx is an application hosting environment
- Hosts Virtual Machines as well as Containers
- Supports docker tooling for development
- Provisions services like GPS & Secure Storage, for applications
- Local Manager for application monitoring and resource usage
- APIs for Application Management (GMM, FND, FD, DNA-C,...)

Why Cisco IOx

- Run distributed compute at the edge
- Leverage secure connectivity of Cisco IOS software
- Manageable with on-premises or cloud-based interface
- Runs on wide variety of IoT platforms
- Builds on existing developer tools and trainings on DevNet



Cisco IoT Operations Dashboard

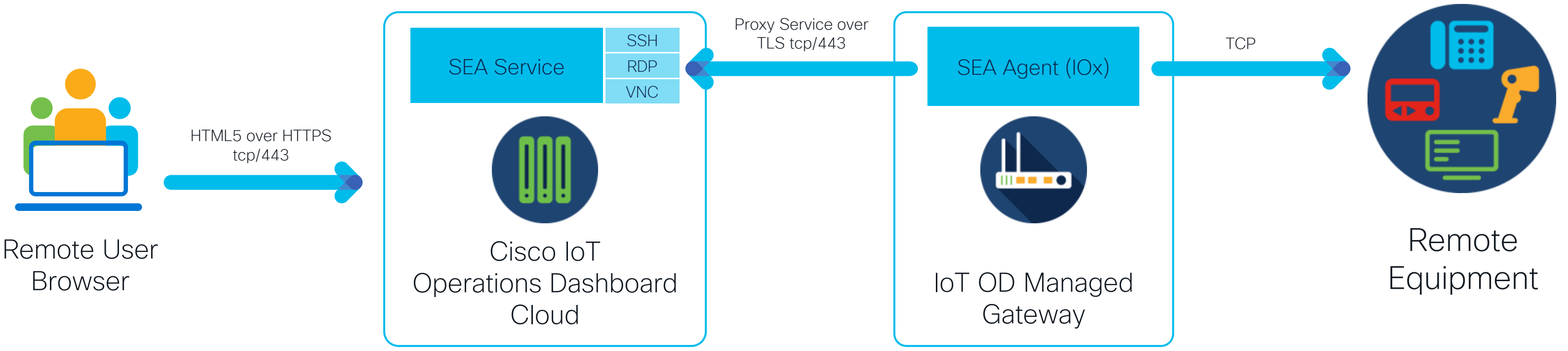
Secure Equipment Access (SEA)

How do you provide remote access today?

- TeamViewer or similar approach?
  - What is someone installs TeamViewer and PIN leaks out?
- VPN access?
  - How do you manage identities?
  - How to you restrict access to specific hosts?
  - How to filter out machine with malware from accessing network?
- Bastion Host?
  - How do you edit firewall rules?
  - How do you monitor who can access what and when?

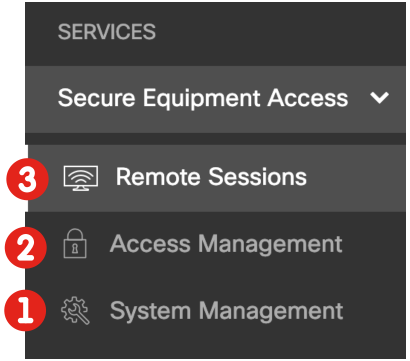
SEA Flow

- No installation required: equipment access through browser
- Proxy: SEA Agent on Gateway is a proxy over TLS/443
- Isolation: remote user is never directly connected to remote network



SEA Configuration Overview

Configured in
three main sections

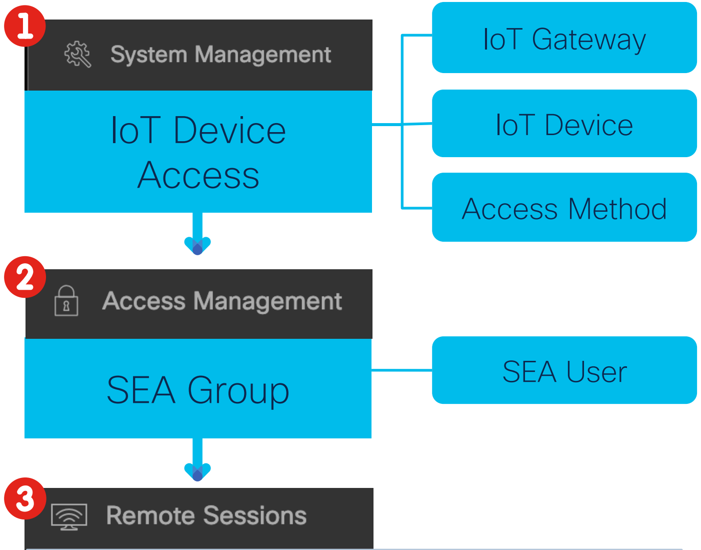

SERVICES

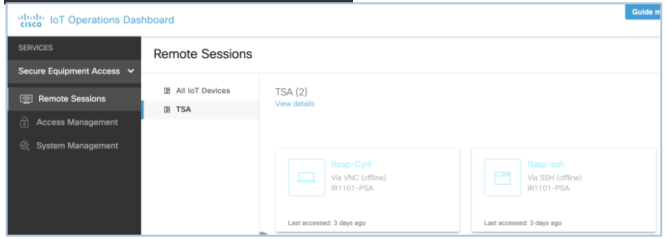
Secure Equipment Access

3 Remote Sessions

2 Access Management

1 System Management




IoT Operations Dashboard

Guide m

SERVICES

Secure Equipment Access

Remote Sessions

Access Management

System Management

Remote Sessions

All IoT Devices

TSA

TSA (2)
View details

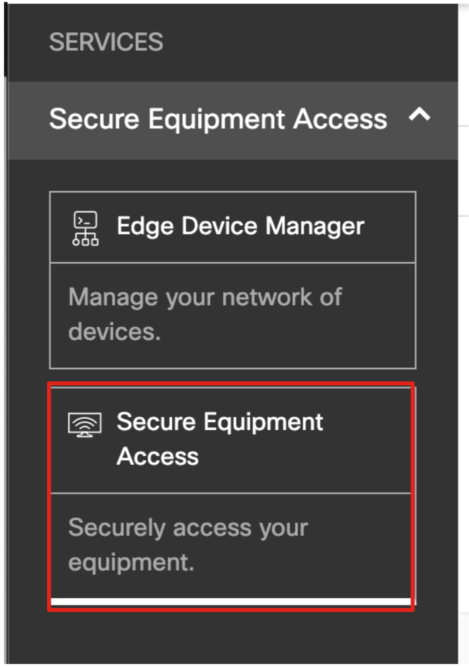
Rasp-Cyril
Via VNC (offline)
IR1101-PSA
Last accessed: 3 days ago

Rasp-ssh
Via SSH (offline)
IR1101-PSA
Last accessed: 3 days ago

SEA Configuration

Switch to SEA Service

- EDM manages gateways, config, software updates.
- SEA is a service that runs in IoT OD next to EDM
- In Services on the left switch to "Secure Equipment Access"



SERVICES

Secure Equipment Access

Edge Device Manager

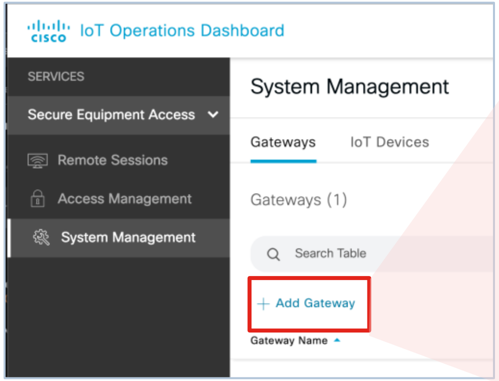
Manage your network of devices.

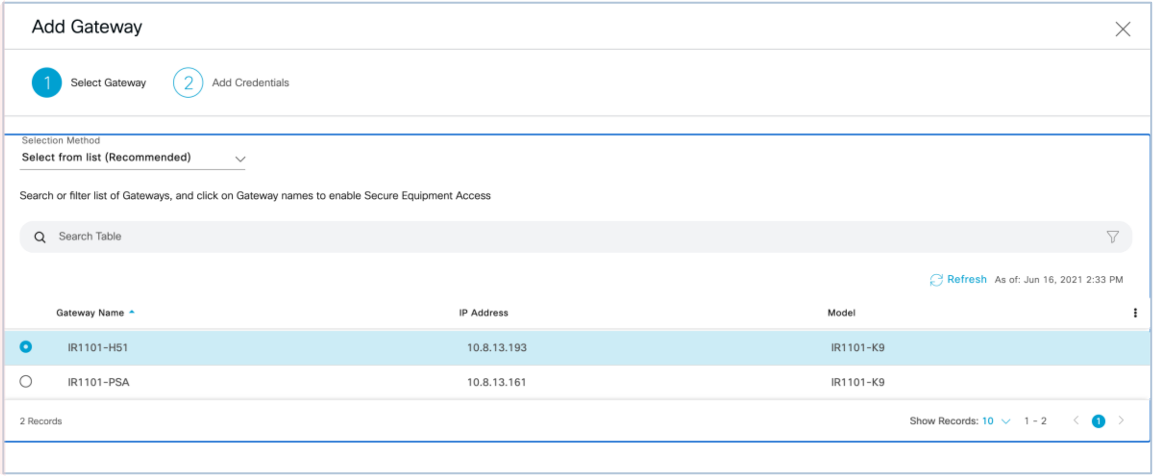
Secure Equipment Access

Securely access your equipment.

Add Gateway to SEA

- The SEA Agent will be automatically installed and configured on your gateway when added to SEA (do not install SEA agent in EDM Application Management!)
- In “System Management”, Click “+ Add Gateway”





Selection Method: Select from list (Recommended)

Search or filter list of Gateways, and click on Gateway names to enable Secure Equipment Access

As of: Jun 16, 2021 2:33 PM

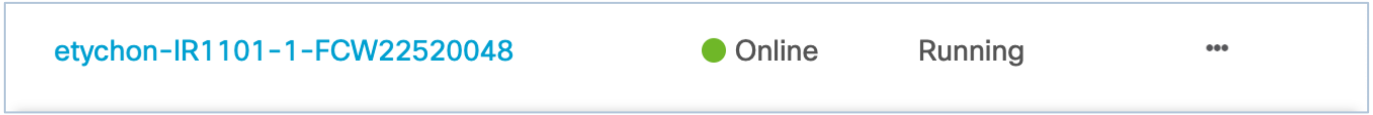
	Gateway Name	IP Address	Model
●	IR1101-H51	10.8.13.193	IR1101-K9
○	IR1101-PSA	10.8.13.161	IR1101-K9

2 Records

Show Records: 10 1 - 2

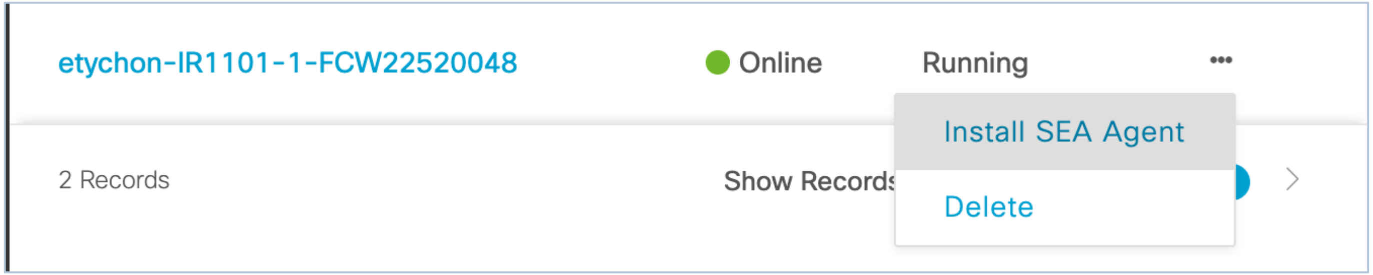
SEA IOx Agent auto-installation check (optional)

If SEA agent installs fine and connects to IoT OD cloud you will see status “online” and “running” in Systems Management



etychon-IR1101-1-FCW22520048 ● Online Running •••

If not, try to “Install SEA Agent” again:



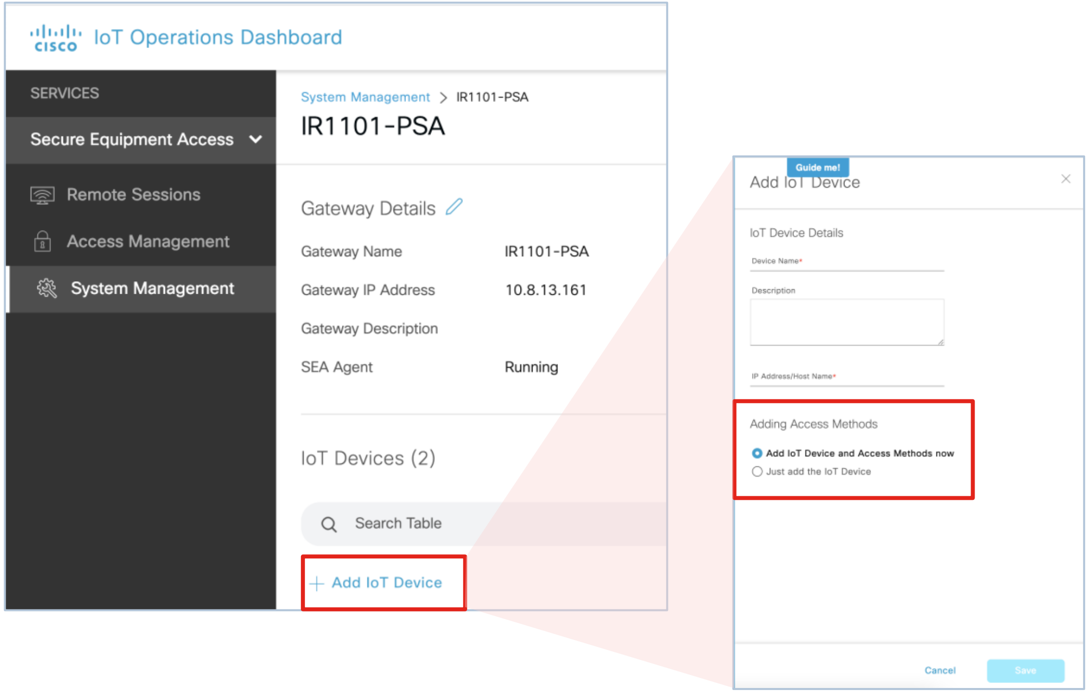
etychon-IR1101-1-FCW22520048 ● Online Running •••

2 Records

Show Records

Add IoT Devices

An IoT Device is connected behind an IoT Gateway



IR1101-PSA

Gateway Details

Gateway Name	IR1101-PSA
Gateway IP Address	10.8.13.161
Gateway Description	
SEA Agent	Running

IoT Devices (2)

Add IoT Device

IoT Device Details

Device Name*

Description

IP Address/Host Name*

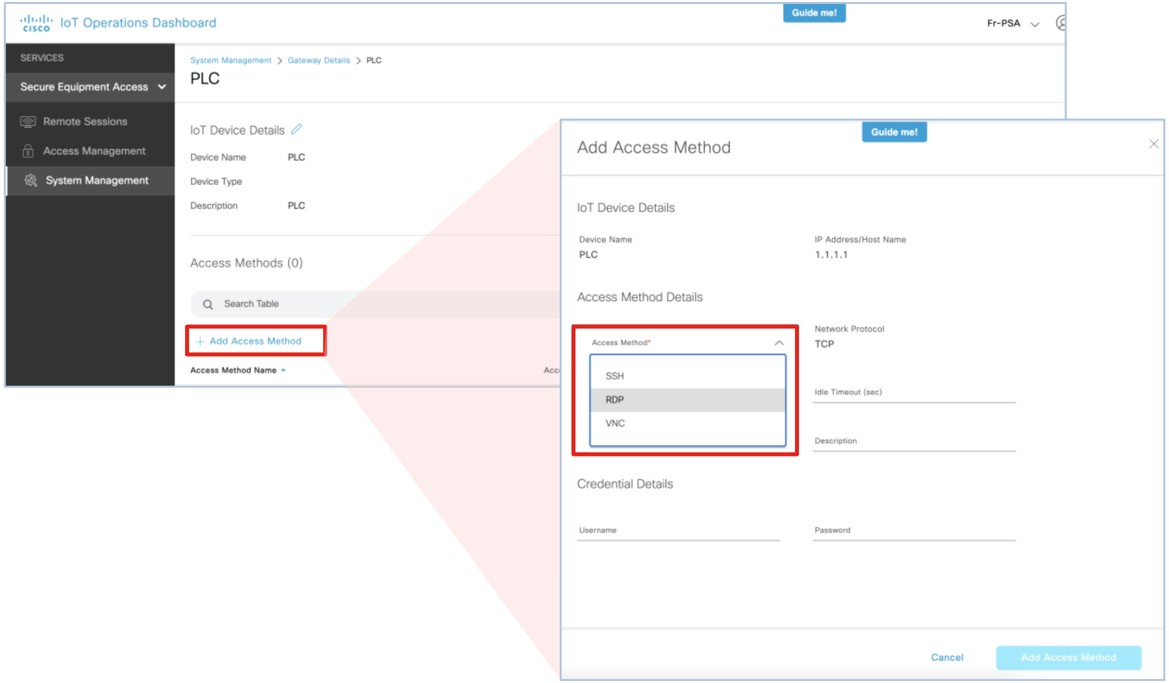
Adding Access Methods

● Add IoT Device and Access Methods now

○ Just add the IoT Device

Add Access Method

The access method defines *how* an IoT Device can be accessed



PLC

IoT Device Details

Device Name PLC

Device Type

Description PLC

Access Methods (0)

Add Access Method

IoT Device Details

Device Name: PLC

IP Address/Host Name: 1.1.1.1

Access Method Details

Access Method*: SSH / RDP / VNC

Network Protocol: TCP

Idle Timeout (sec)

Description

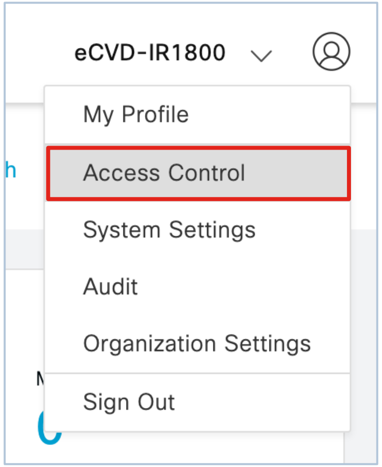
Credential Details

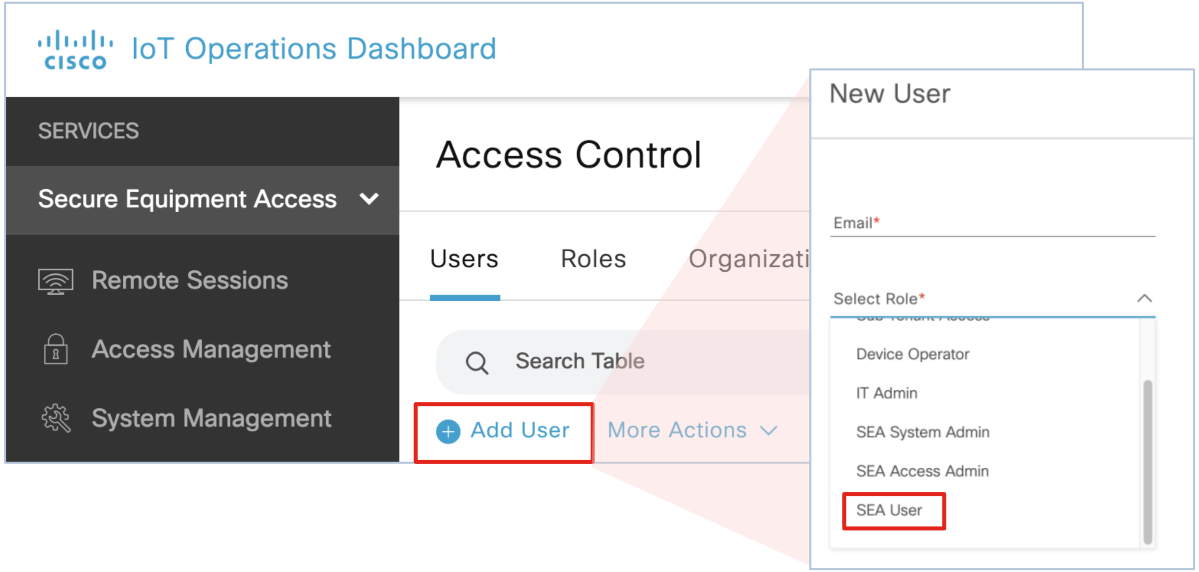
Username

Password

Users & Roles

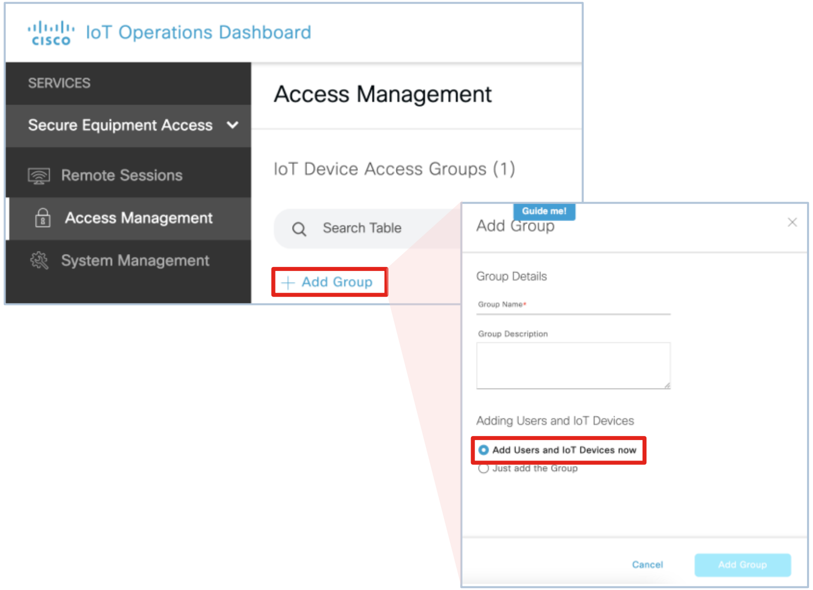
- To use SEA, remote users will need “SEA User” role.
- To add a new SEA remote user, use Dashboard “access control”

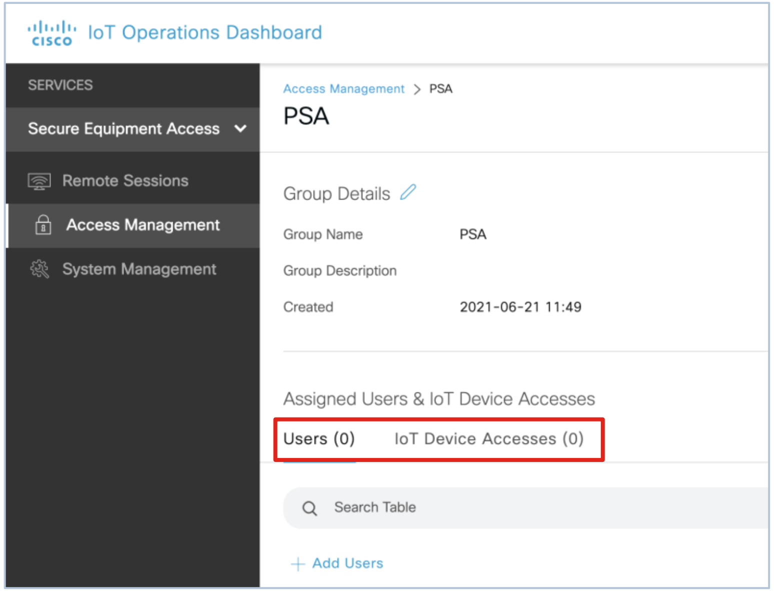




SEA Group Creation

Who (“Users”) has access to *what* (“IoT Device Access”) is defined in SEA “Group” under Access Management

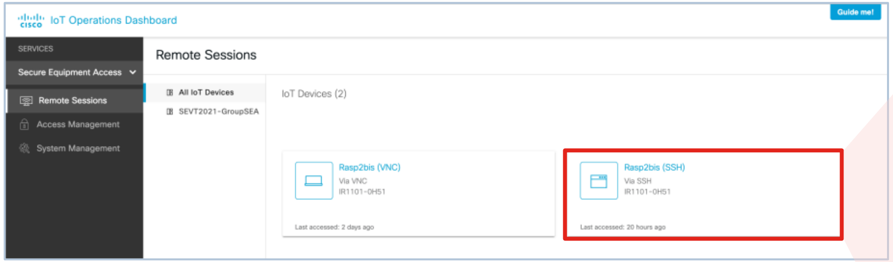


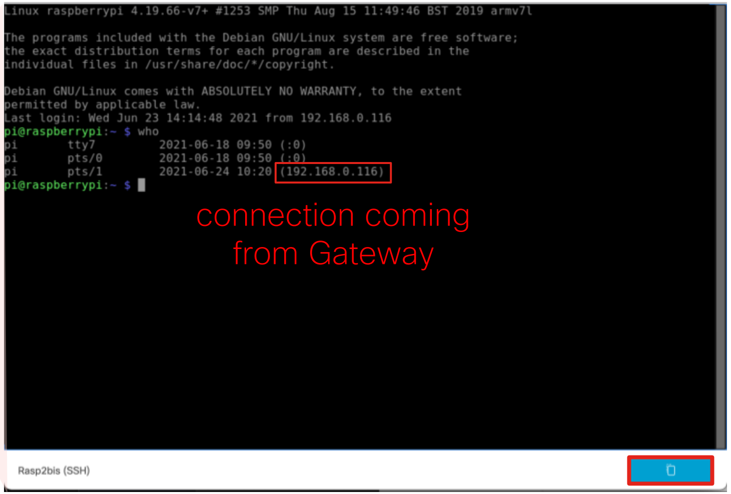


Group Name	PSA
Group Description	
Created	2021-06-21 11:49

SEA User Remote Session

One click equipment access for remote users.





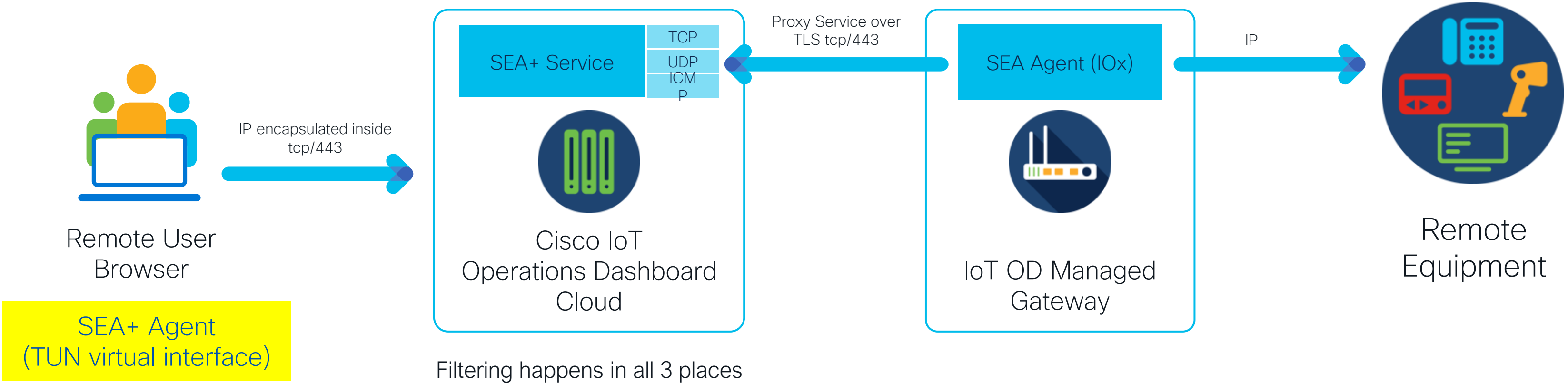
```
Linux raspberrypi 4.19.66-v7+ #1253 SMP Thu Aug 15 11:49:46 BST 2019 armv7l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun 23 14:14:48 2021 from 192.168.0.116
pi@raspberrypi:~ $ who
pi       tty7         2021-06-18 09:50 (:0)
pi       pts/0        2021-06-18 09:50 (:0)
pi       pts/1        2021-06-24 10:20 (192.168.0.116)
pi@raspberrypi:~ $ 
```

connection coming from Gateway

Cut and Paste button between local and remote

SEA+ Flow

- Agent installation **is required** – creates TUNTAP virtual network device
- TUN devices runs inside SEA TLS/443
- Remote user computer routes changed to use TUN device
- Remote user is **directly connected** to remote network

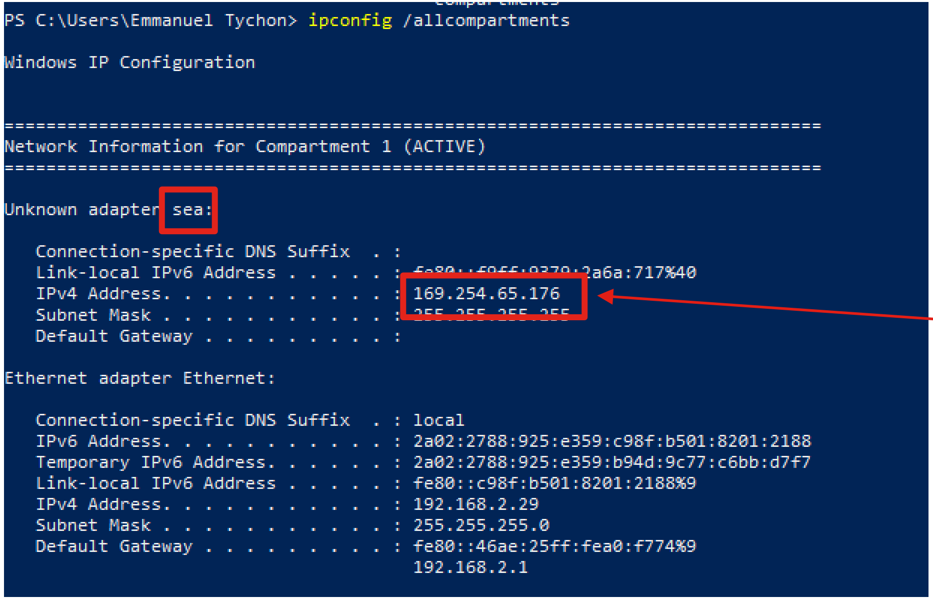


IP encapsulated inside tcp/443
Remote User Browser
SEA+ Agent (TUN virtual interface)
SEA+ Service
TCP
UDP
ICMP
Cisco IoT Operations Dashboard Cloud
Proxy Service over TLS tcp/443
SEA Agent (IOx)
IoT OD Managed Gateway
IP
Remote Equipment

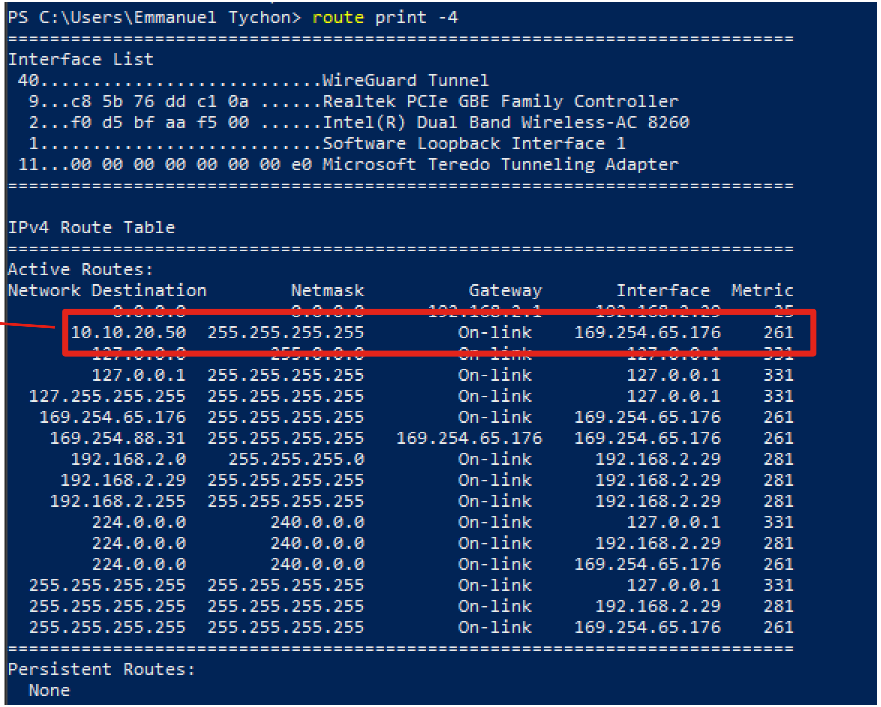
Filtering happens in all 3 places

1. in Windows SEA+ app,
2. in Cloud, and
3. in IOx SEA app.

SEA+ Creates on virtual TUN interface



```
PS C:\Users\Emmanuel Tychon> ipconfig /allcompartments

Windows IP Configuration


==============================================================================
Network Information for Compartment 1 (ACTIVE)
==============================================================================

Unknown adapter sea:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f9ff:9379:2a6a:717%40
   IPv4 Address. . . . . . . . . . . : 169.254.65.176
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : local
   IPv6 Address. . . . . . . . . . . : 2a02:2788:925:e359:c98f:b501:8201:2188
   Temporary IPv6 Address. . . . . . : 2a02:2788:925:e359:b94d:9c77:c6bb:d7f7
   Link-local IPv6 Address . . . . . : fe80::c98f:b501:8201:2188%9
   IPv4 Address. . . . . . . . . . . : 192.168.2.29
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::46ae:25ff:fea0:f774%9
                                       192.168.2.1
```



```
PS C:\Users\Emmanuel Tychon> route print -4
===========================================================================
Interface List
 40...........................WireGuard Tunnel
  9...c8 5b 76 dd c1 0a ......Realtek PCIe GBE Family Controller
  2...f0 d5 bf aa f5 00 ......Intel(R) Dual Band Wireless-AC 8260
  1...........................Software Loopback Interface 1
 11...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.2.1    192.168.2.29     25
      10.10.20.50  255.255.255.255         On-link   169.254.65.176    261
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link        127.0.0.1    331
    169.254.65.176  255.255.255.255         On-link   169.254.65.176    261
     169.254.88.31  255.255.255.255   169.254.65.176   169.254.65.176    261
      192.168.2.0    255.255.255.0         On-link     192.168.2.29    281
     192.168.2.29  255.255.255.255         On-link     192.168.2.29    281
    192.168.2.255  255.255.255.255         On-link     192.168.2.29    281
        224.0.0.0        240.0.0.0         On-link        127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link     192.168.2.29    281
        224.0.0.0        240.0.0.0         On-link   169.254.65.176    261
  255.255.255.255  255.255.255.255         On-link        127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link     192.168.2.29    281
  255.255.255.255  255.255.255.255         On-link   169.254.65.176    261
===========================================================================
Persistent Routes:
  None
```

SEA vs SEA+

- SEA is **easier** to use
- **More secure** with IP isolation
- To be used, when possible, for:
  - SSH
  - VNC
  - RDP
  - Telnet
  - Web

- SEA+ requires Windows, a client, and admin privilleges
- SEA+ is **more flexible**
- Can provide **direct IP connectivity** (ie. to a nativr client such as Profinet programmer)
- Allows file transfer (ie. with SFTP)

Use both SEA and SEA+ for different use cases

Conclusions

Conclusions

- Selection of IOS-XE hardware for remote and mobile applications
- Uplink over Ethernet or Cellular
- Routers can be Cloud-managed with IoT OD Operations Dashboard
- Easy procedure to provide remote access

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

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.

The bridge to possible

Thank you

cisco Live!
ALL IN