Architecting Private 5G

For Resiliency, Security, and Enterprise Network Convergence

Filipe Rodrigues

BRKSPM-2042

Agenda

- Cisco Private 5G Introduction
- Architecture Deep-Dive
- Enterprise Integration
- Summary

What's in it for me?

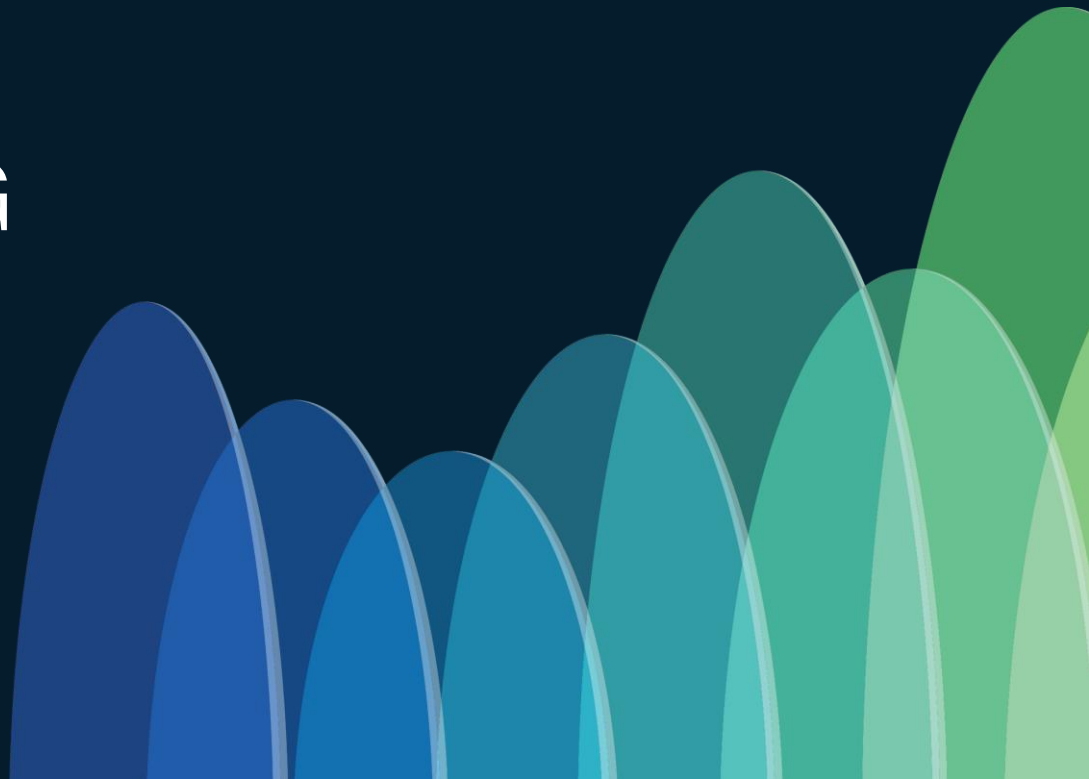
1. Understand what is private 5G and why it is important?
2. How to build resilient and secured P5G service?
3. Unified tools across Wi-Fi & P5G
   - P5G becomes access technology adjacent to Wi-Fi

Continue your education

This presentation assumes knowledge about:

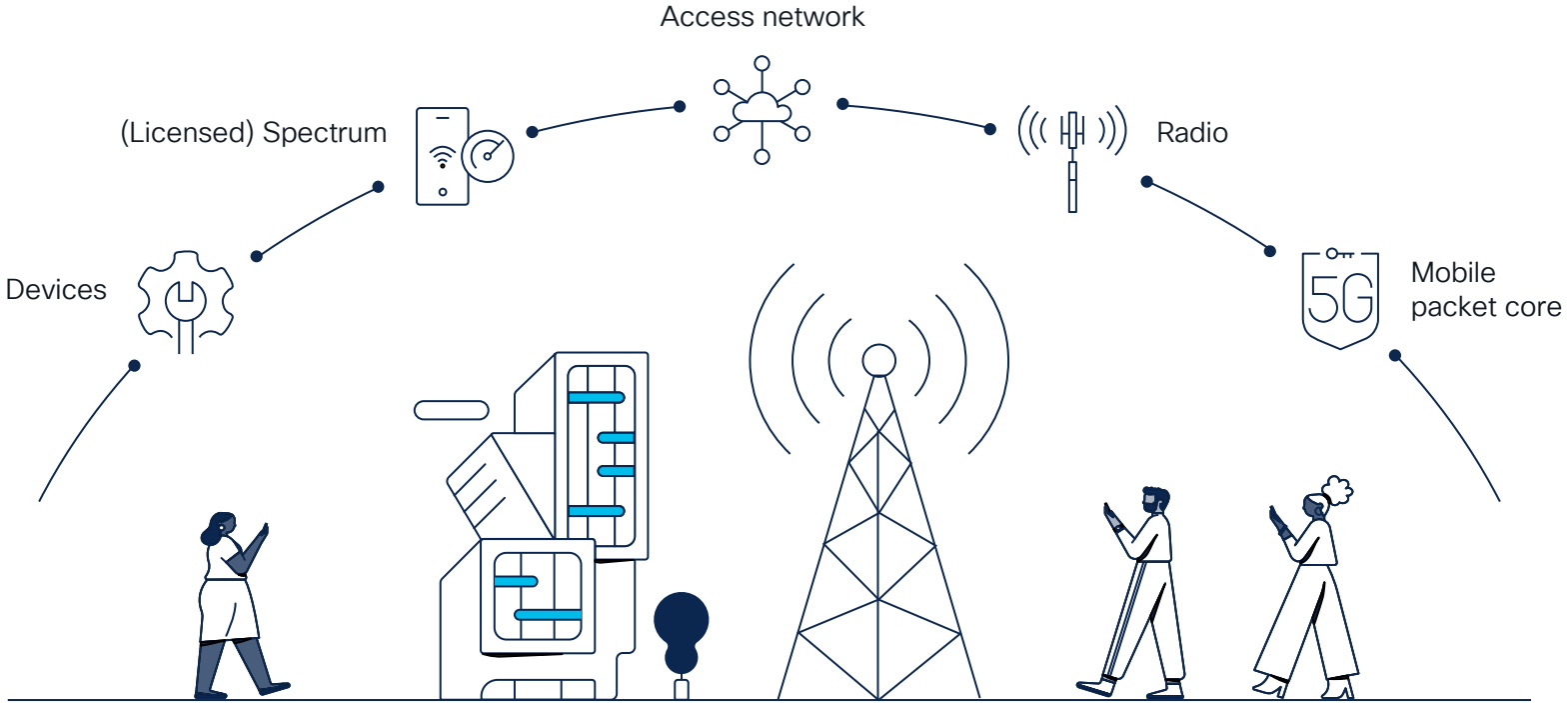
- Introductory knowledge of Private or Public 5G
- Introductory knowledge about Cisco Enterprise Portfolio primarily ISE, Umbrella, ThousandEyes, QoS.

Cisco Private 5G
Introduction



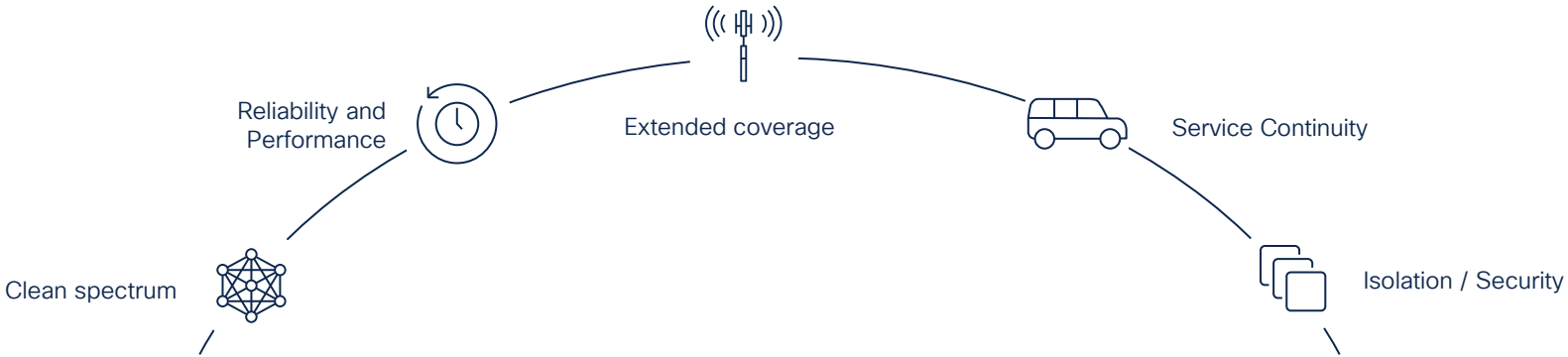
cisco Live!

What is Private 5G?



A private cellular network that is built using 3GPP 5G technology,
dedicated to carrying traffic from a specific entity (e.g., an enterprise) in licensed radio spectrum

Customer needs and use case sweet spots



Industrial and manufacturing

- Precision robotic control
- High speed SW downloads
- Smart tools
- Industrial Connectivity (Profinet)

Distribution and warehouses

- AGVs and driverless vehicles
- Automated conveyance
- Distribution line automation

Ports, hubs and energy

- Video surveillance
- Push-to-talk
- Unmanned autonomous vehicles
- Data offload
- Remote Expert

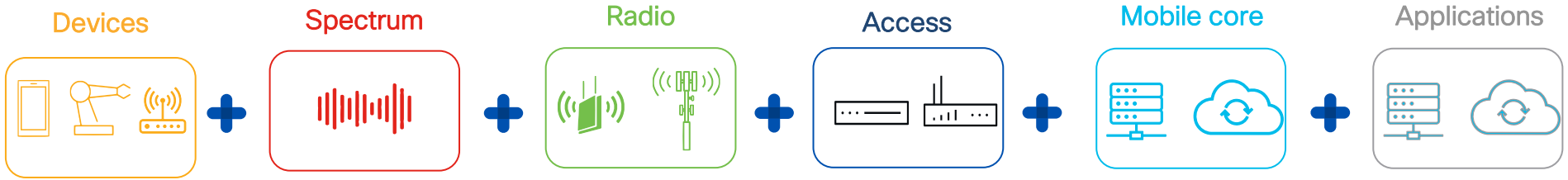
Venues

- Efficient and reliable backhaul for Wi-Fi-connected endpoints
- Clean spectrum for venue operators
- Mission-critical broadcasts
- Security & Video surveillance

Private 5G and Wi-Fi 7 are complementary

Wireless Technology	Private 5G	P5G + WIFI	Wi-Fi 6/6E/7 (802.11ax)
Optimized for	Clean spectrum for Mission-critical applications requiring ultra-reliability, ultra-low latency, or broad geographic coverage		Applications focused on Cost effective coverage, Broad device coverage, Client Density, “Guest” Access, local mobility.
Use Cases	xR interactive learning Mobile MRI Trucks Wide Area Coverage (ports, bases, refineries) Automated Guided Vehicles (AGVs) Enhanced Mobile Broadband Process Automation Robotics		

Wi-Fi and 5G Comparable Architectures



	User Equipment	Unlicensed Spectrum	Access Points (AP)	Enterprise	Wireless LAN Controller
Wi-Fi	Device with a Wi-Fi Radio Interface	2.4 GHz 5 GHz 6 GHz	Radio Antennas and Control Functions Wi-Fi6 = OFDMA	IBN / DNA SD-WAN SD-Access	User session Policy and Control Scale to Thousands of Devices
5G	Device with a 5G Radio Interface	Licensed Spectrum Shared or Private 20-50 GHz 1 – 7 GHz Sub 1 GHz	Radio Antennas and Control Functions 5G = OFDMA	Service Provider or Enterprise Optical Segment Routing MPLS L2/L3 VPN	Mobile Packet Core User session Policy and Control Scale to Millions of UEs

Enterprise

10s to 50 Thousand — 10s of Feet to 100s of Miles

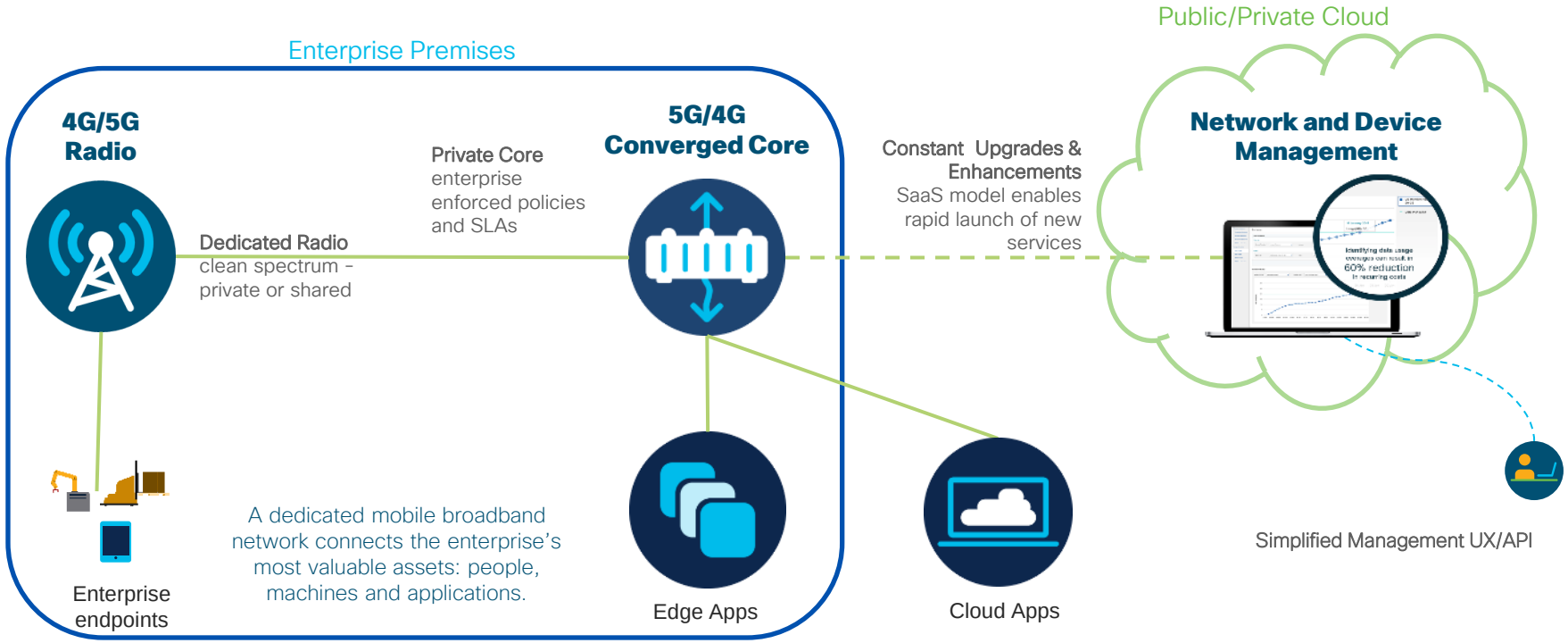
Internet / Enterprise

10s to > 1 Trillion — 10s of Feet to 10,000s of Miles

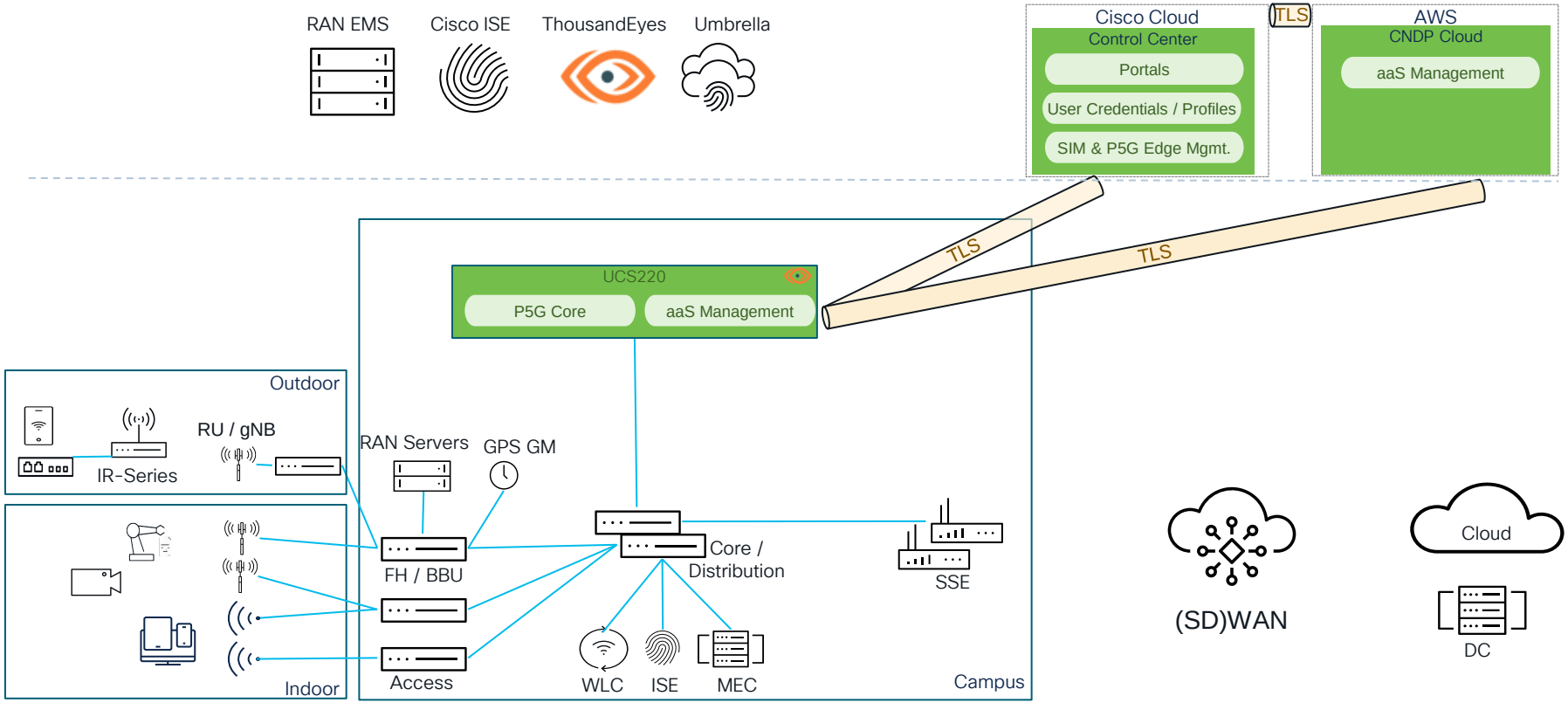
Open Architecture with Cloud Native Decentralized and Distributed Network Functions

Distributed Application Architectures

Cisco's Private 5G Architecture

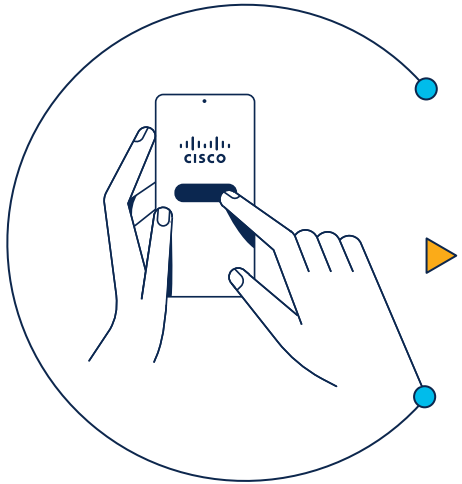


The Cisco P5G High-Level Architecture



Delivered by Cisco in an aaS model

Private 5G solution



Management
Cloud managed

Identity and policy
Intuitively integrated into existing enterprise systems

Mobility core
Industry-leading 4G/5G converged mobility core

Radios
Certified and validated Open RAN radio partners

Simple | Secured | Trusted

Cisco Private 5G

What's included

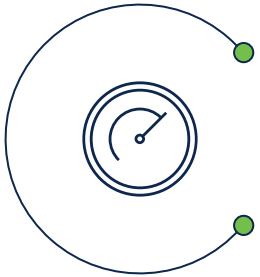
High-performance edge

- Compact mobile core
- Fully integrated with enterprise switches and routers
- Integrated identity and security
- 3GPP release support

Enterprise dashboard

- UX for customer onboarding and for management by customer or partner
- APIs for automation and enhanced services

Reliable operations



- 24x7 support
- SLA assurance
- Software and firmware for edge equipment
- New feature content

Cloud-managed service

- Packet core management
- Subscriber (SIM) management and authentication
- Monitoring and alerting of service/solution

Comprehensive 5G solution delivered with enterprise simplicity

P5G is part of one platform for Mobile services

current
future

powered by cloud and SaaS

Markets

Enterprise | SoHo/SMB | Self Service Digital Enablement

- Things/IoT (current) — (cars, assets, sensors)
- Places/Business (current) — (remote/mobile workplace)
- People/Workforce (future) — (business users on the go)

Technology

- Public Mobile Networks
  - Data Core: 2G-5G (current)
  - Remote edge (future)
  - Voice core (future)
- Private Mobile Networks
  - Private 5G edge (current)

On-prem mobile core Packet core (SMF, UPF, PCF; 4G, 5G)

Ecosystem, Architecture & Operation

- API and Ecosystem
  - developers (future)
  - partner (current)
- Distributed Architecture
- Digital Operation
  - AI/ML/Analytics (future)
  - Enterprise integrations

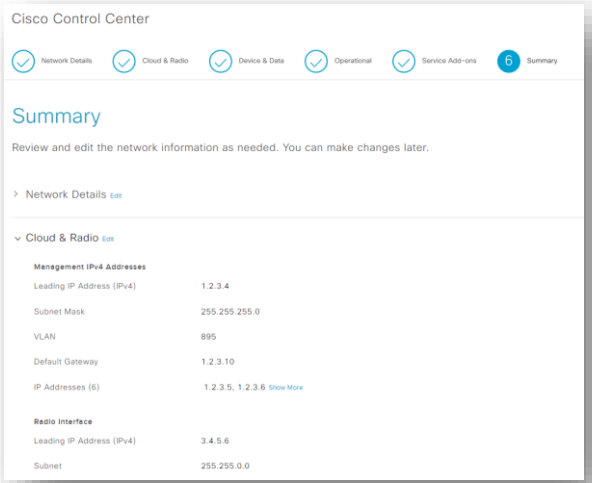
Easy to Deploy

Easy to Deploy

- Step-by-step Onboarding Wizard
  - Simplified configuration → Enterprise friendly
- Automated instantiation
  - Complete core network configuration → hours not days

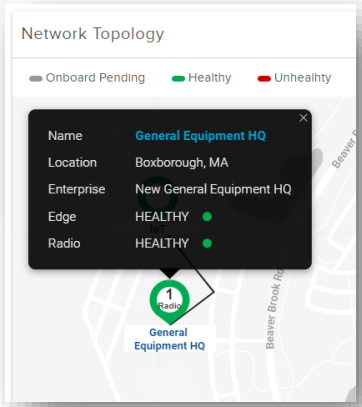
Log in.

Self-onboarding

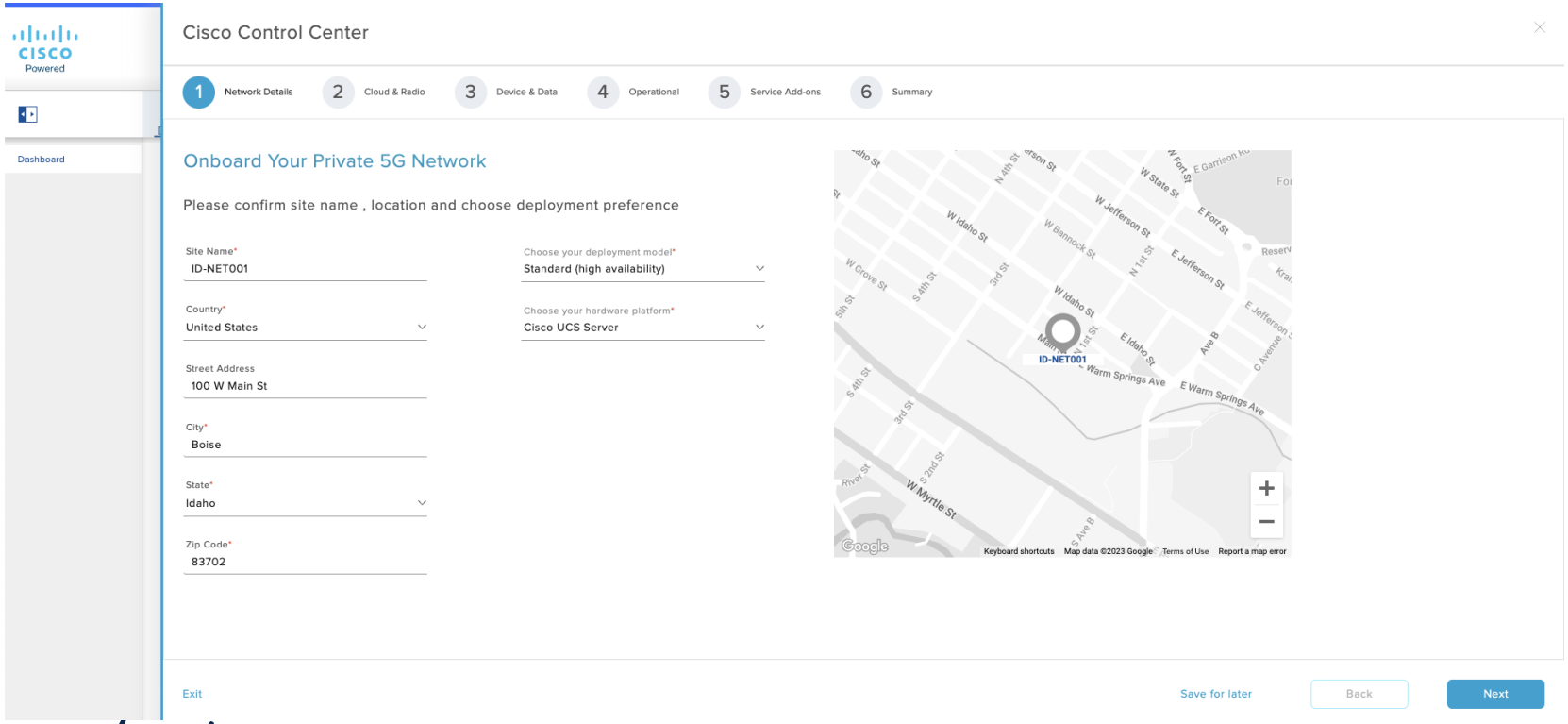


Install Hardware

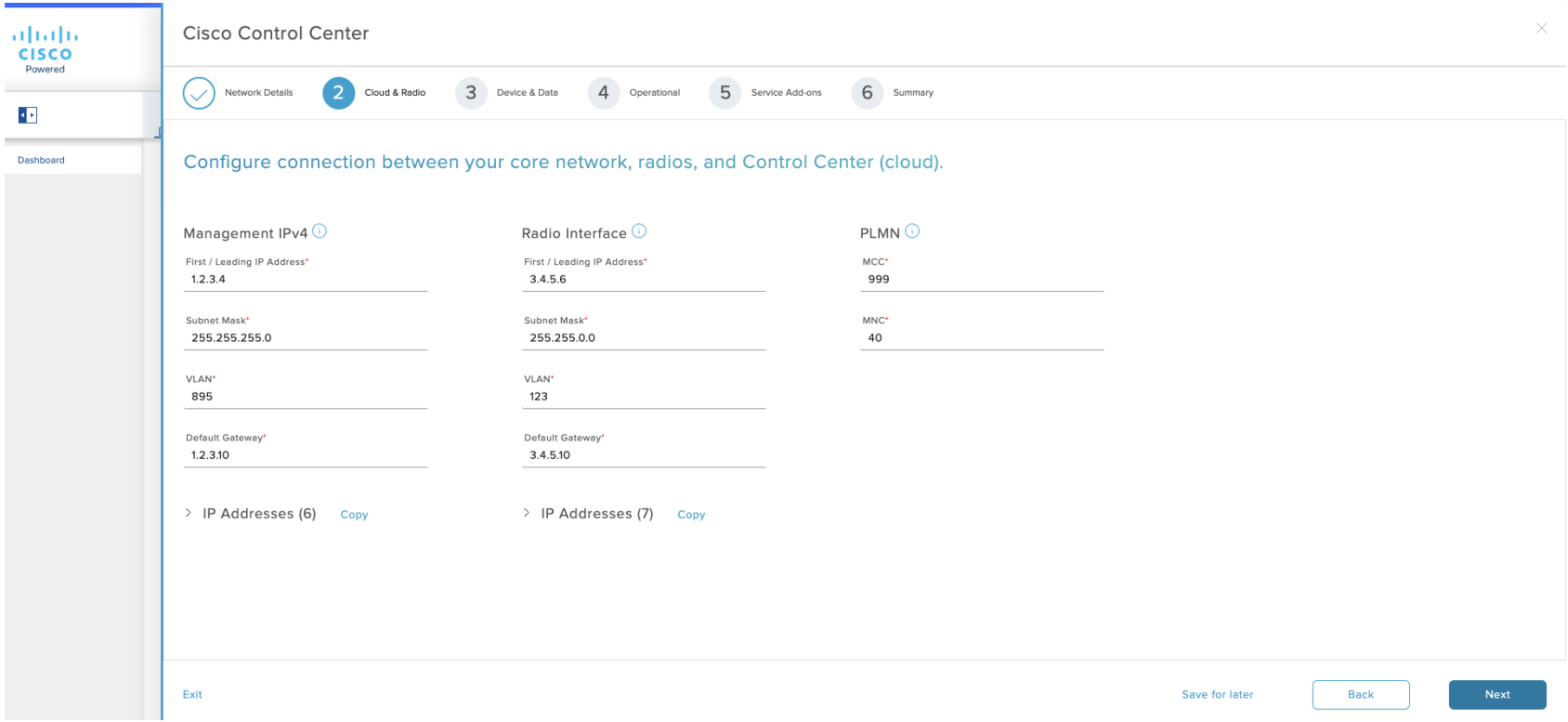
5G service is



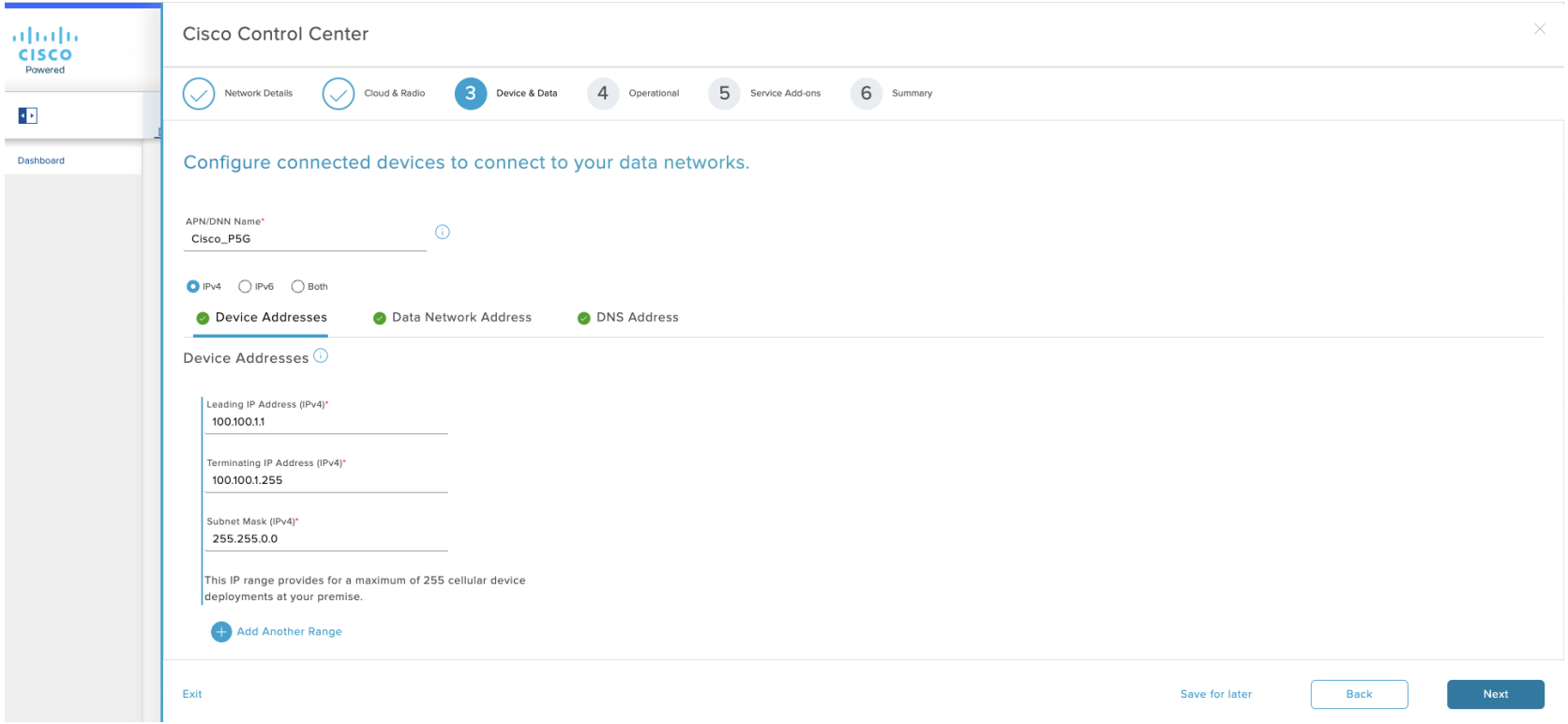
Cisco Control Center – Edge Appliance Installation 1/5



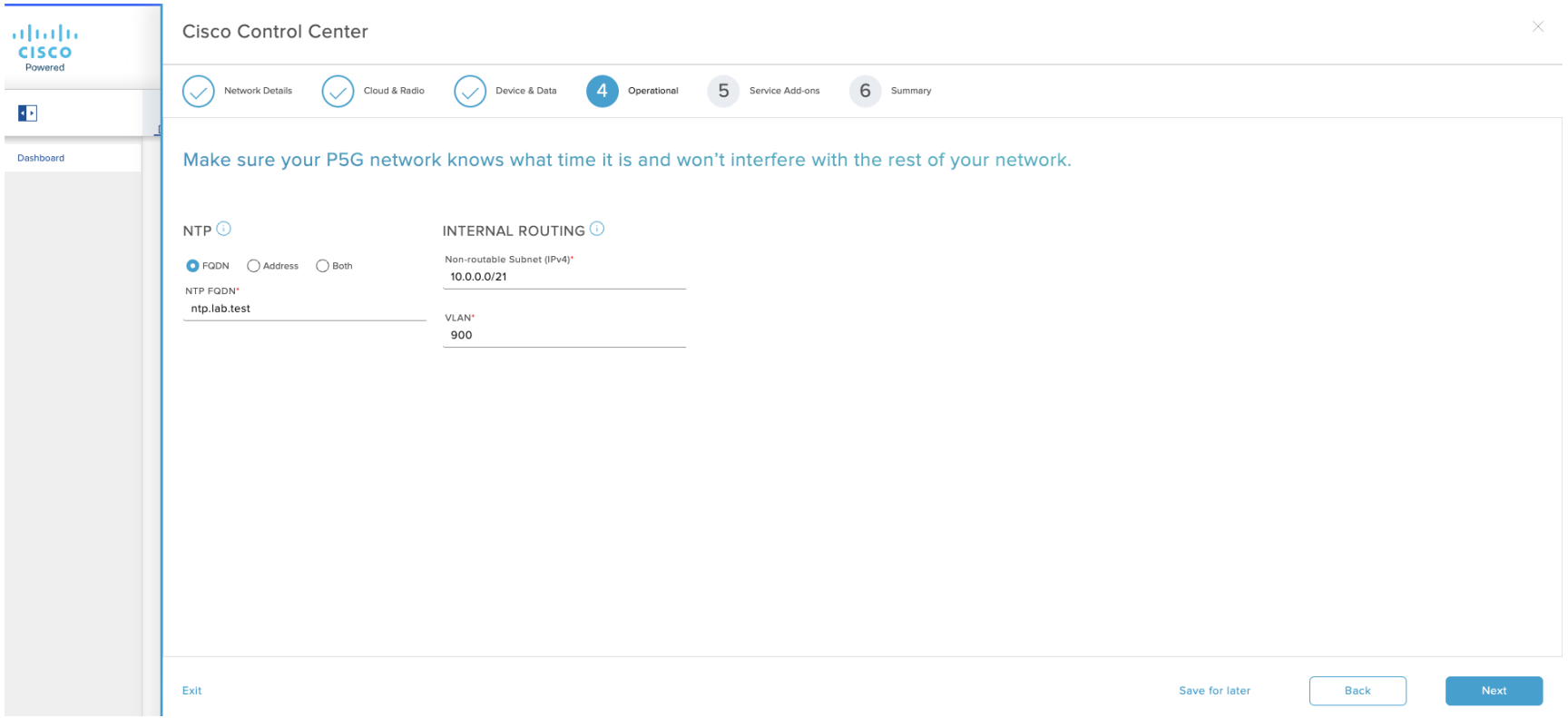
Cisco Control Center – Edge Appliance Installation 2/5



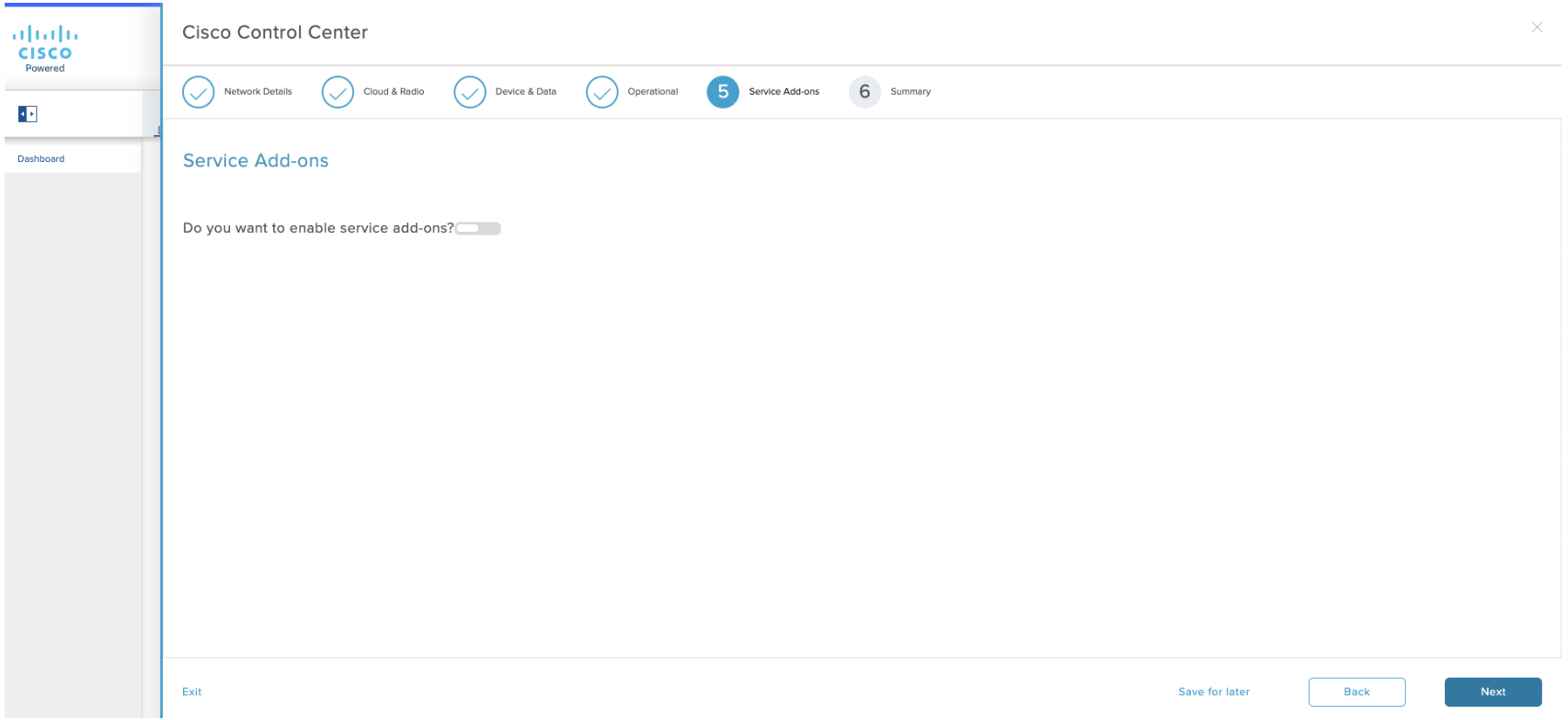
Cisco Control Center – Edge Appliance Installation 3/5



Cisco Control Center – Edge Appliance Installation 4/5



Cisco Control Center – Edge Appliance Installation 5/5

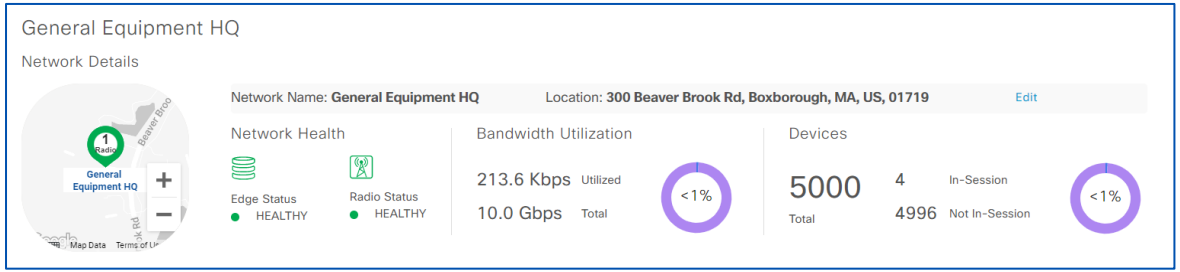


Easy to Operate

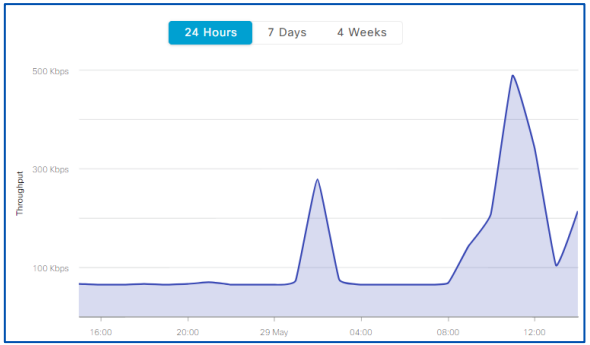
Easy to Operate

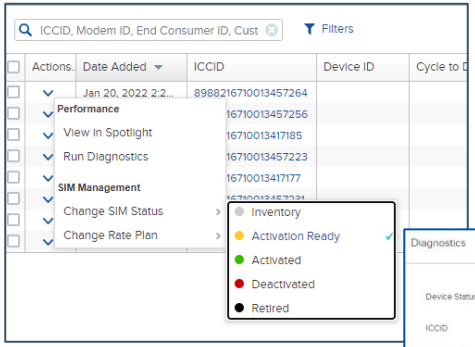
- Simple Device Management
  - Control SIM inventory
  - Create Device Groups
- Real Time Service Visibility
  - Core, Radio, Device views
  - Single and multi-tenant options

Holistic service visibility

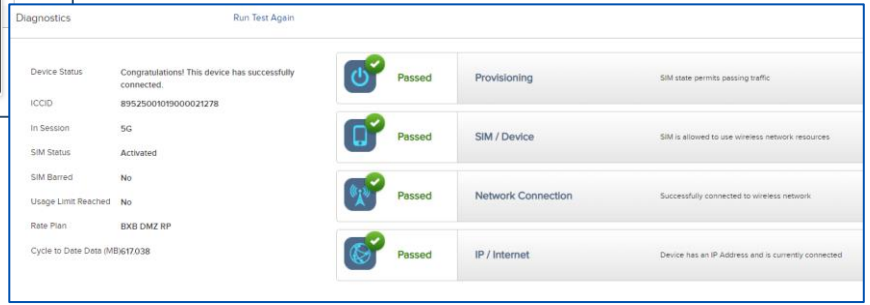


Time series views





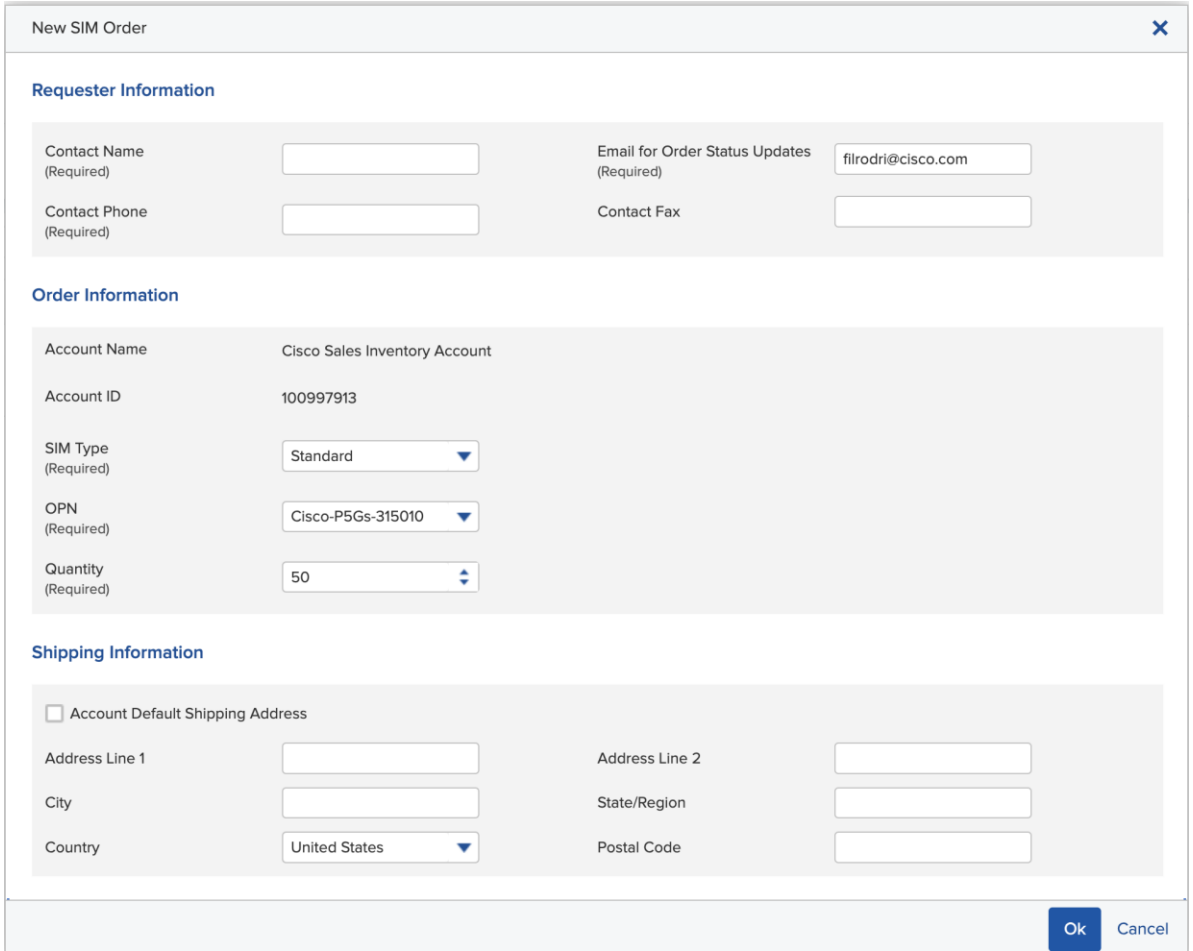
Service control and visibility at the SIM level



SIM

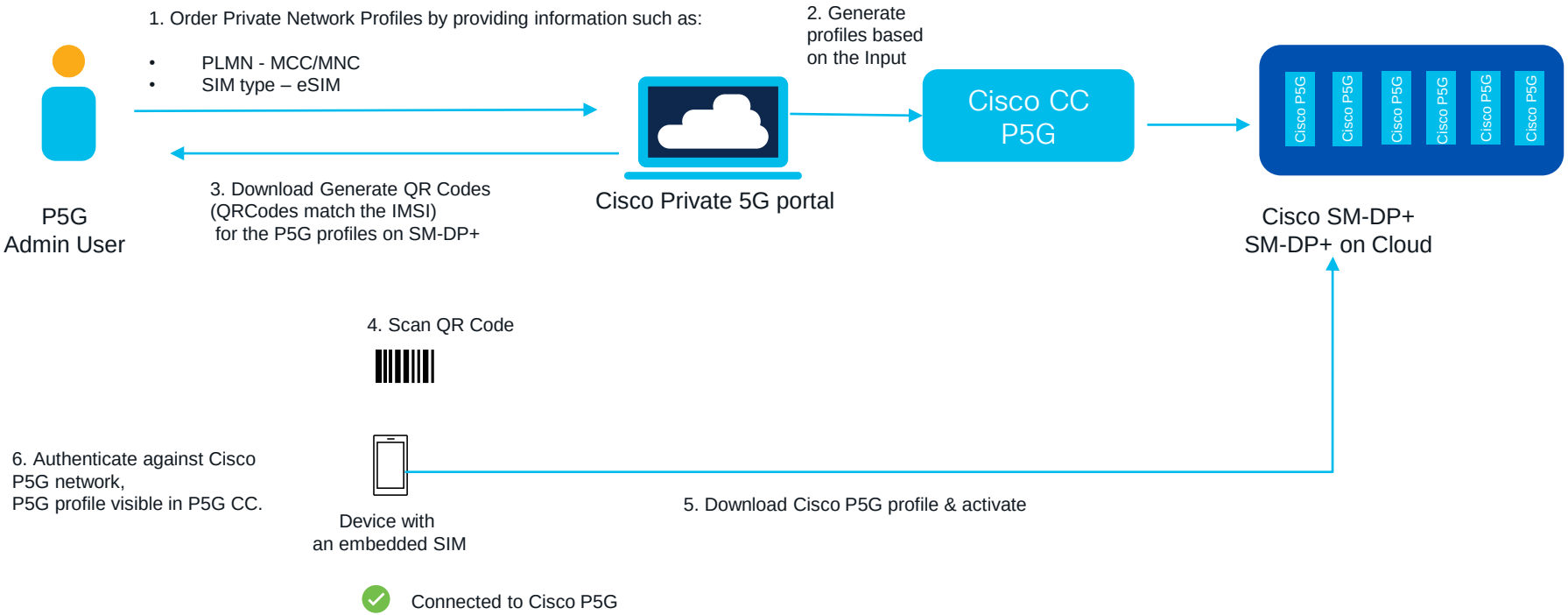
cisco Live!

Easy to order :

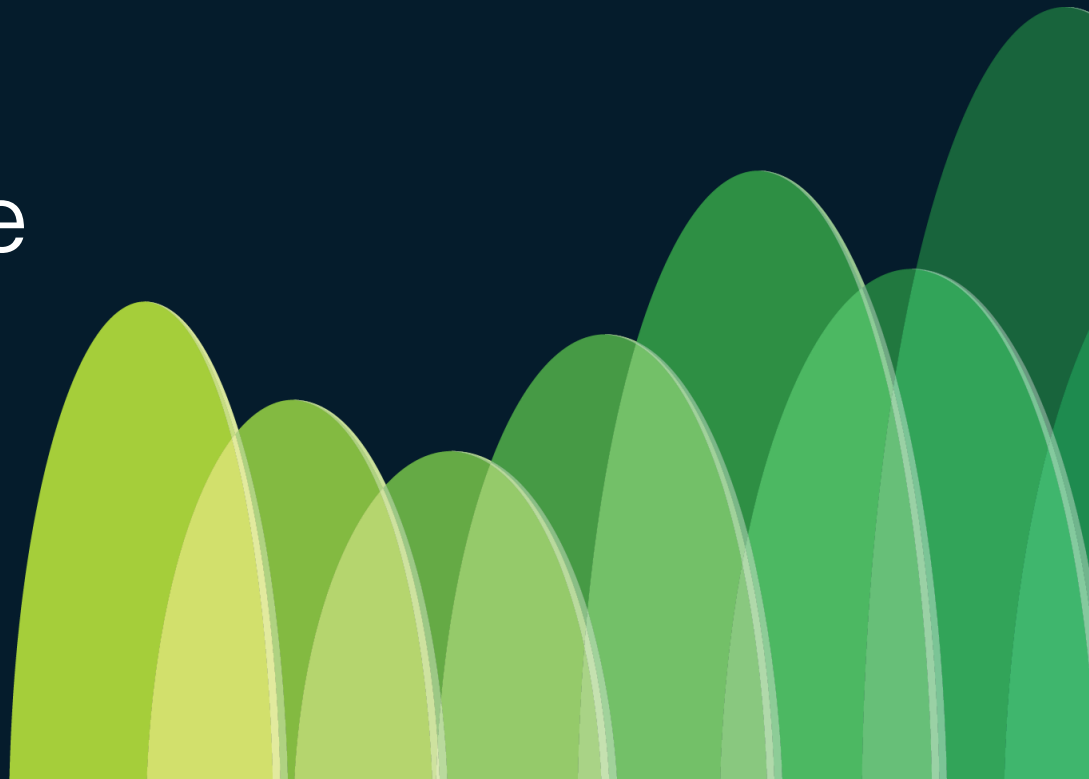


cisco Live!

Cisco P5G eSIM:

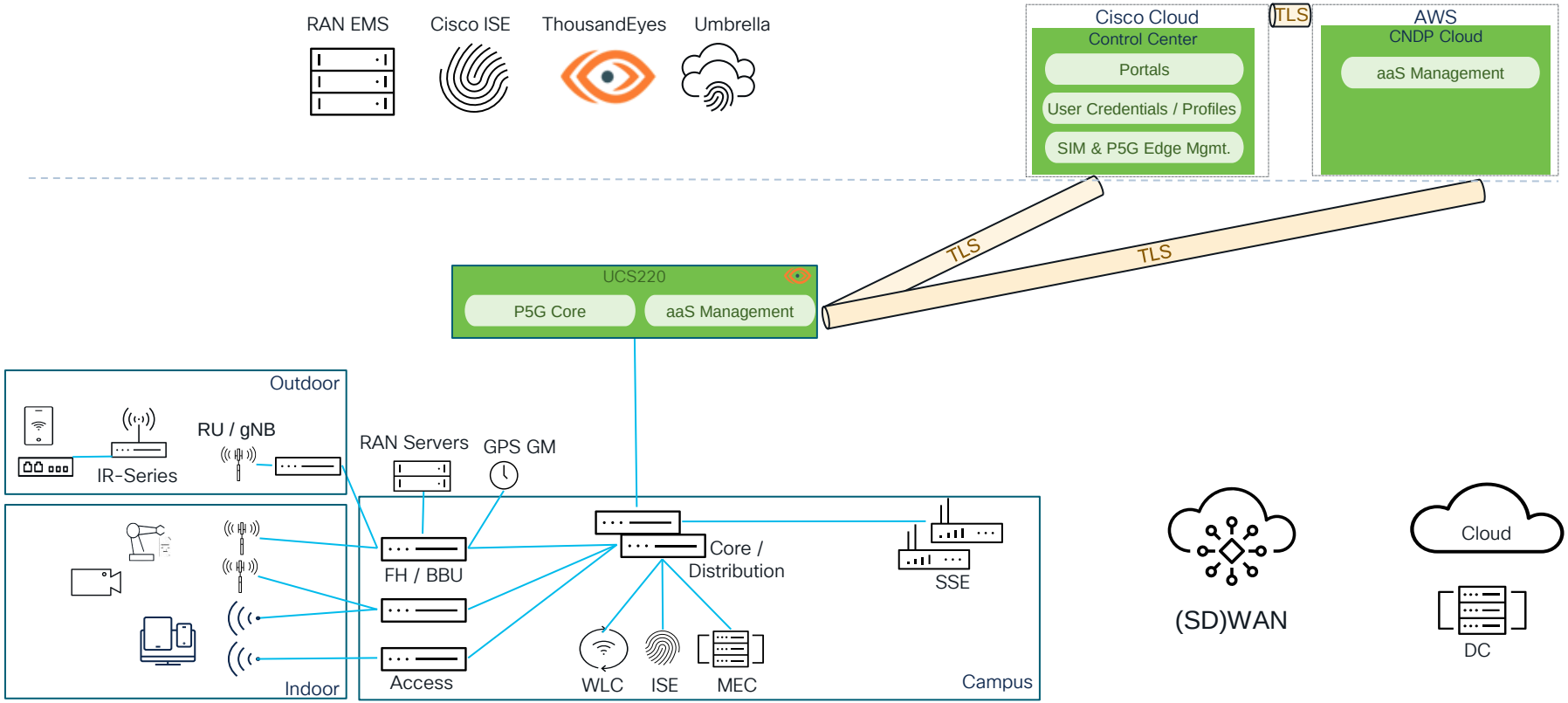


P5G Architecture Deep Dive



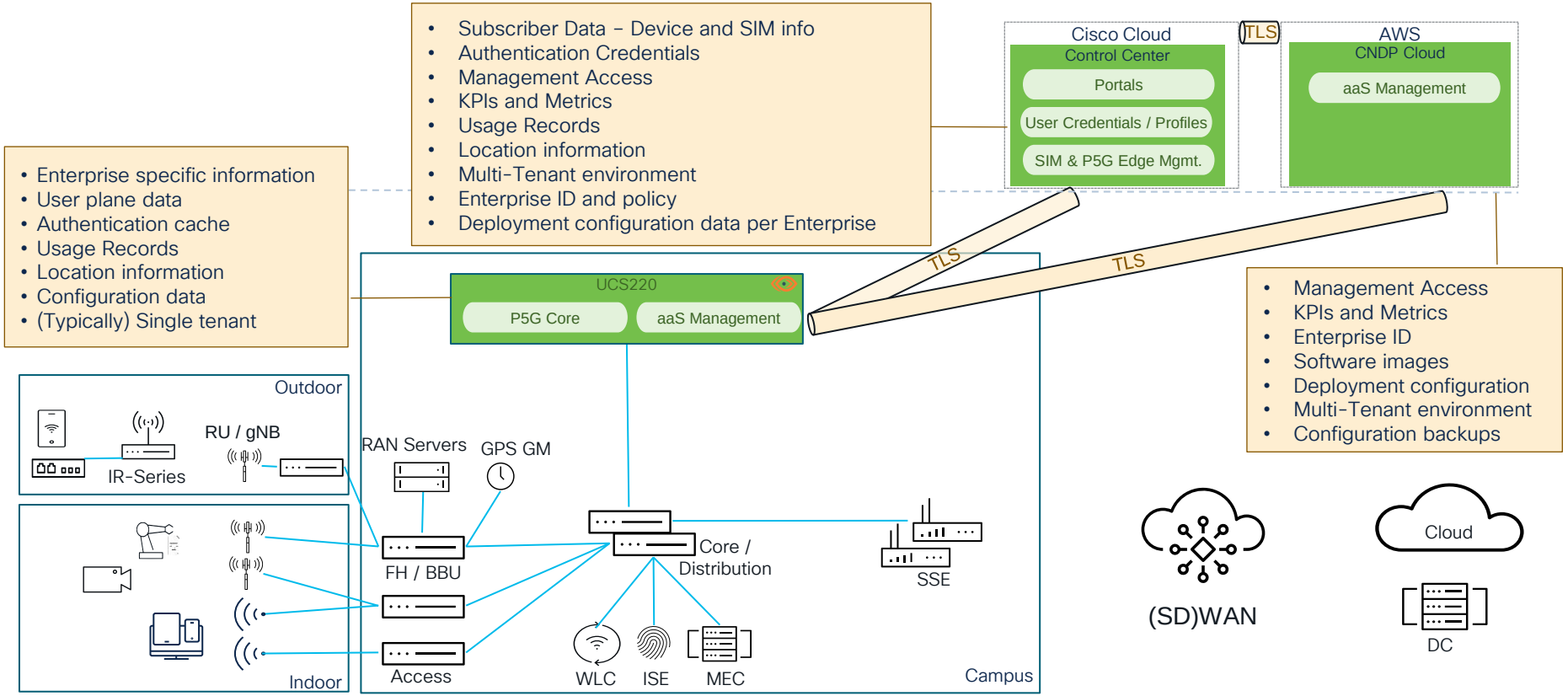
cisco Live!

The Cisco P5G High-Level Architecture



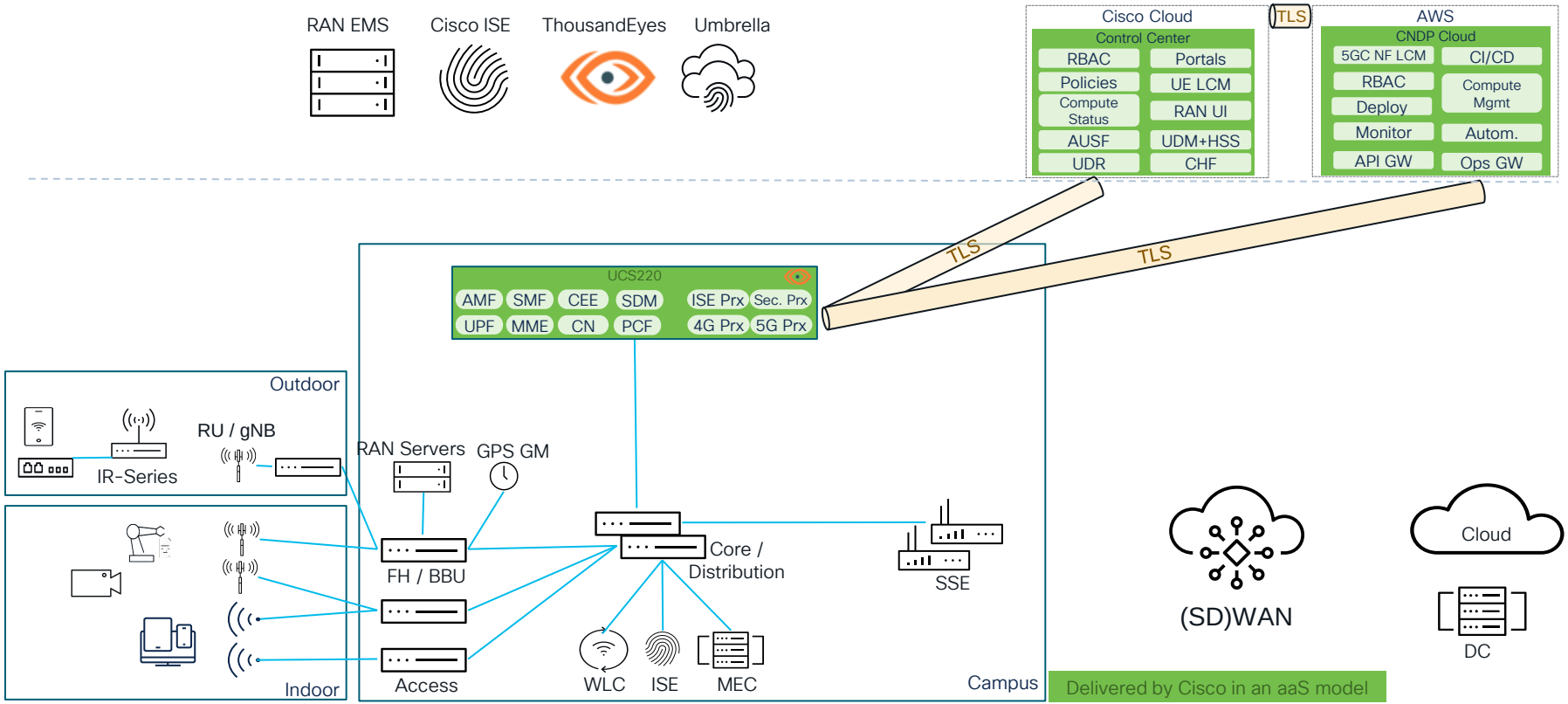
Delivered by Cisco in an aaS model

The Cisco P5G High-Level Architecture



Delivered by Cisco in an aaS model

Cisco Private 5G Core Network Function Hosting Local traffic Breakout & Cloud Managed



SDM -> AUSF / UDM / UDR / HSS

Key Cisco Solution Blocks

P5G Edge

Deployed per Enterprise site

Cisco Control Center

Geo-redundantly deployed across the continents

Cloud Native Deployment Platform

Deployed at CSP's availability zones

P5G edge

- Cloud managed single click automated edge deployment
- SP grade 4G and 5G network functions
- 20K sessions and 25Gbps throughput
- Scalable design
- 3GPP release support
- Fully integrated with enterprise switches and routers
- Seamless integration with Cisco ENT portfolio (ISE/Umbrella)

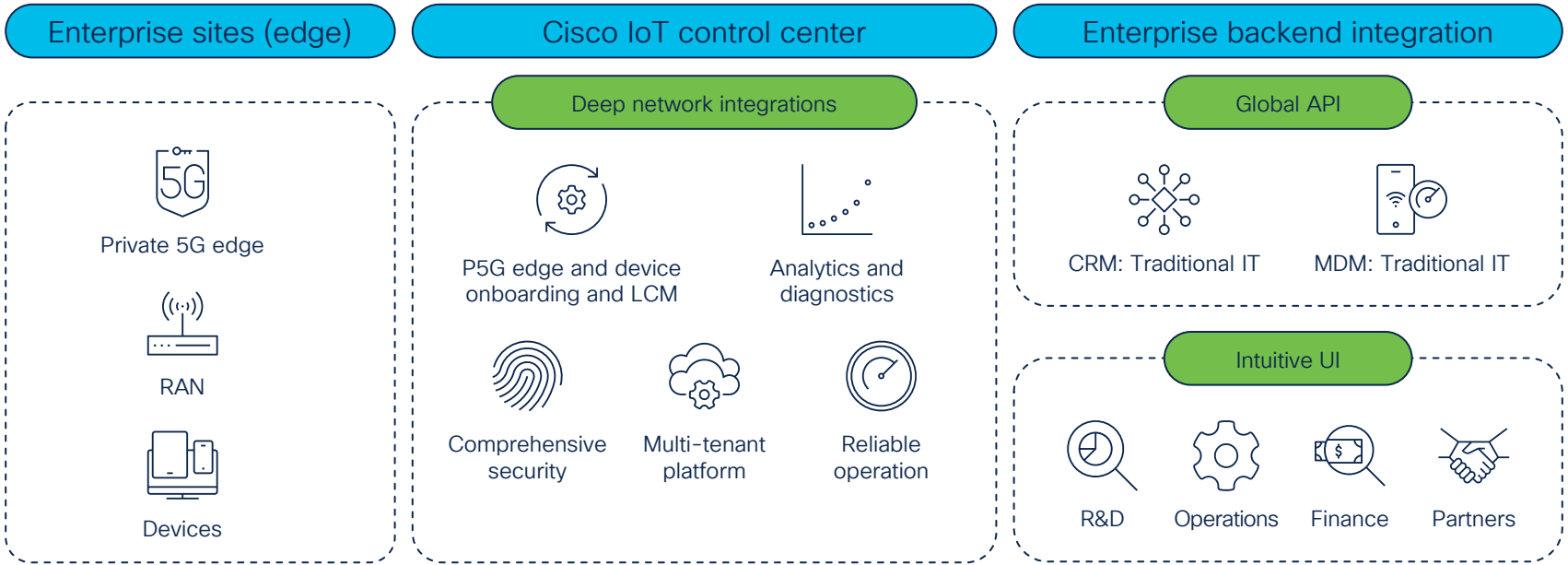
1.5B daily subscribers over Cisco packet core NFs

#1 mobile IoT share

First US-wide 5G IoT and consumer deployment

P5G Management Platform

Built on a strong foundation of mobile SaaS (IoT Control Center)

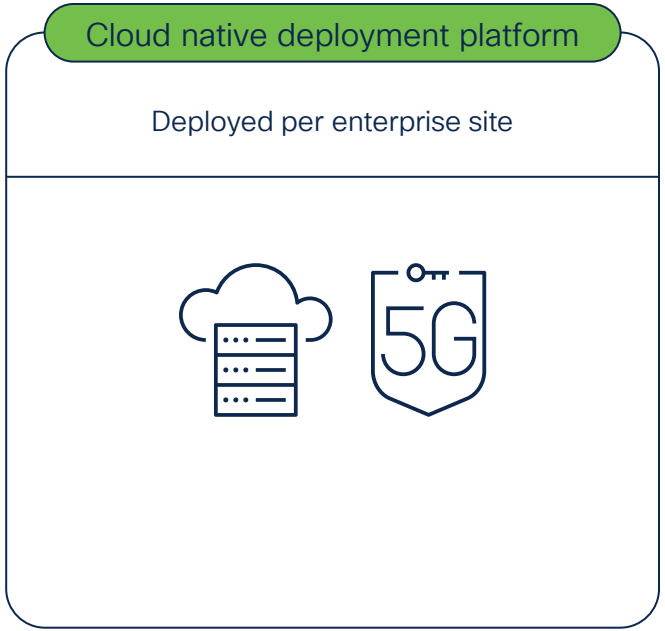


220M+ devices
82M+ connected card

60+ service providers
30K+ enterprises

120 countries
20+ industries

CNDP-Cloud



- P5G Edge management
- Leveraging industry best CSP practices
- North and south bound TLS end points
- Scalable design
- Closer to P5G edge to meet industry use cases
- Enables Cisco Cloud integration checkpoints
- Backend to have 24/7 support with SLA assurance

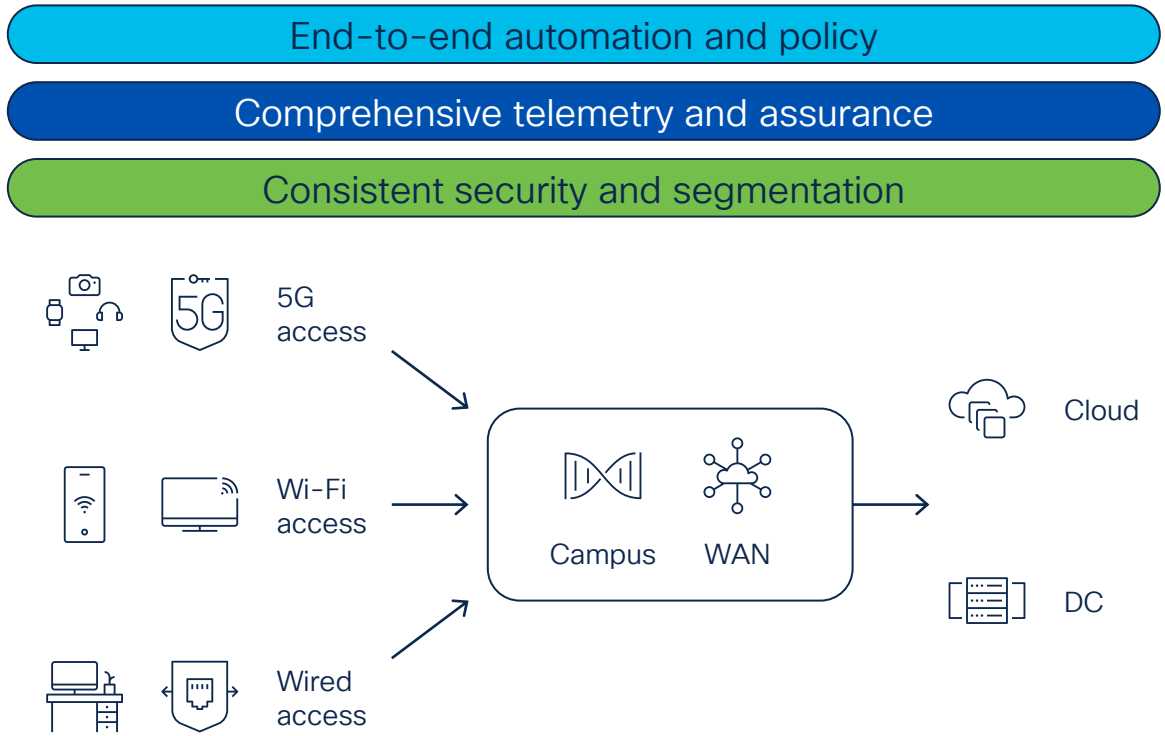
P5G edge LCM (CI/CD)

Tool suite for Cisco SRE team

APIs for automation and enhanced services

Cisco P5G integrated enterprise architecture vision

- Common transport
- Common enterprise policy
- Enterprise security integration
- Cisco endpoint/IoT GW integration
- Consolidated insights and analytics
- Unified identity framework
- Private and public mobility
- Unified EN operations

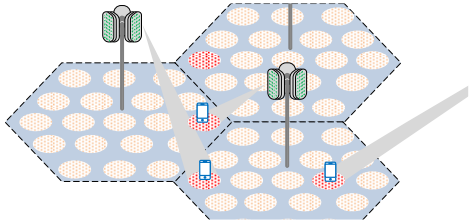


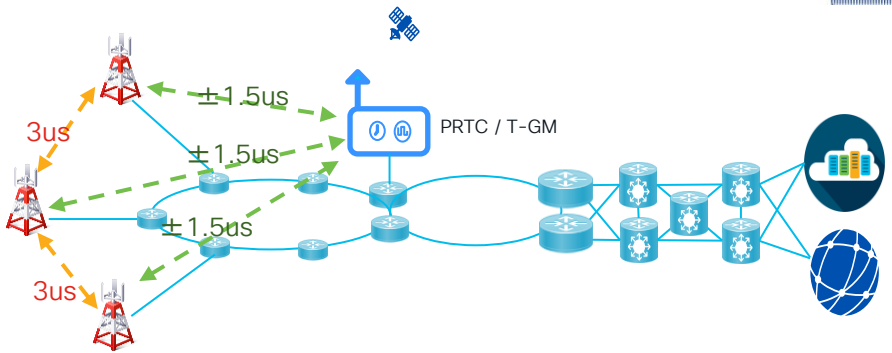
5G Frame sync

Frame sync is critical in particular in TDD

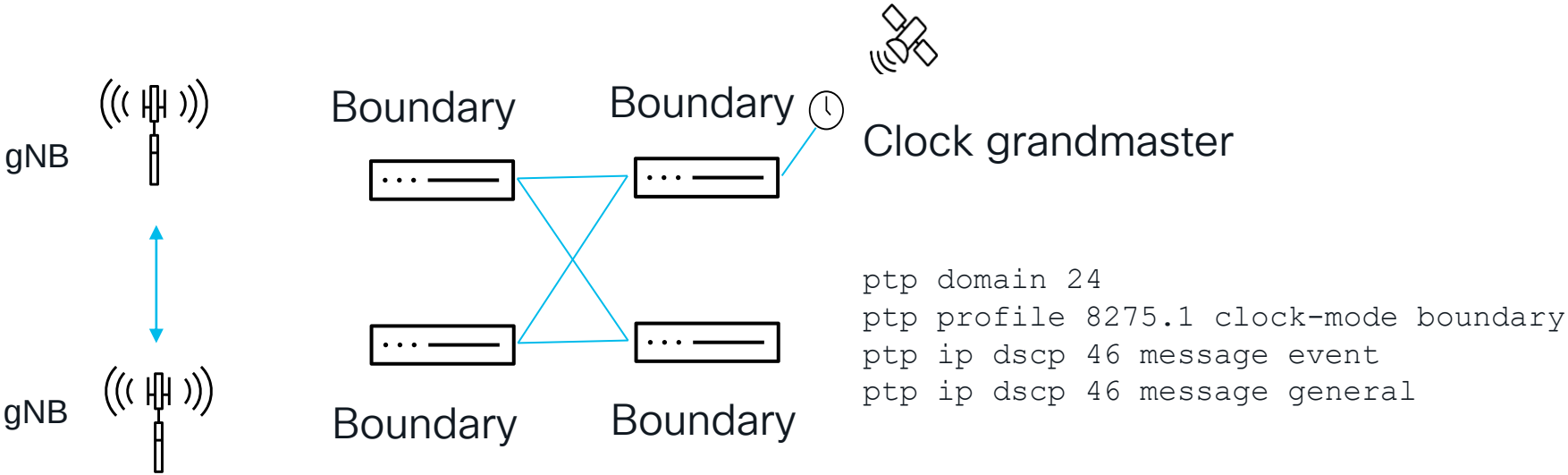
>3 µs are needed for avoiding inter symbol interferences (UL and DL)

This guarantee also complex operation like MIMO and Coordinated transmission





Integrating PTP in SDA design




```
ptp domain 24
ptp profile 8275.1 clock-mode boundary
ptp ip dscp 46 message event
ptp ip dscp 46 message general
```

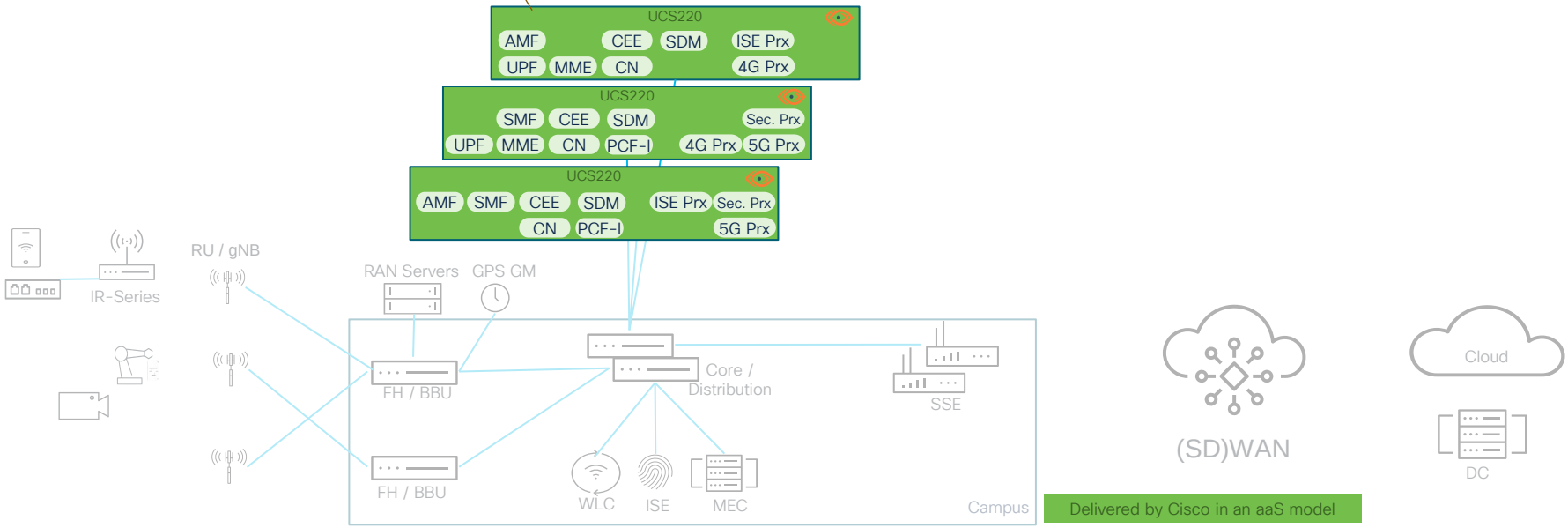
PTP configure in a L2 profile in the underlay

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-15/configuration_guide/lyr2/b_1715_lyr2_9500_cg/configuring_precision_time_protocol__ptp_.html

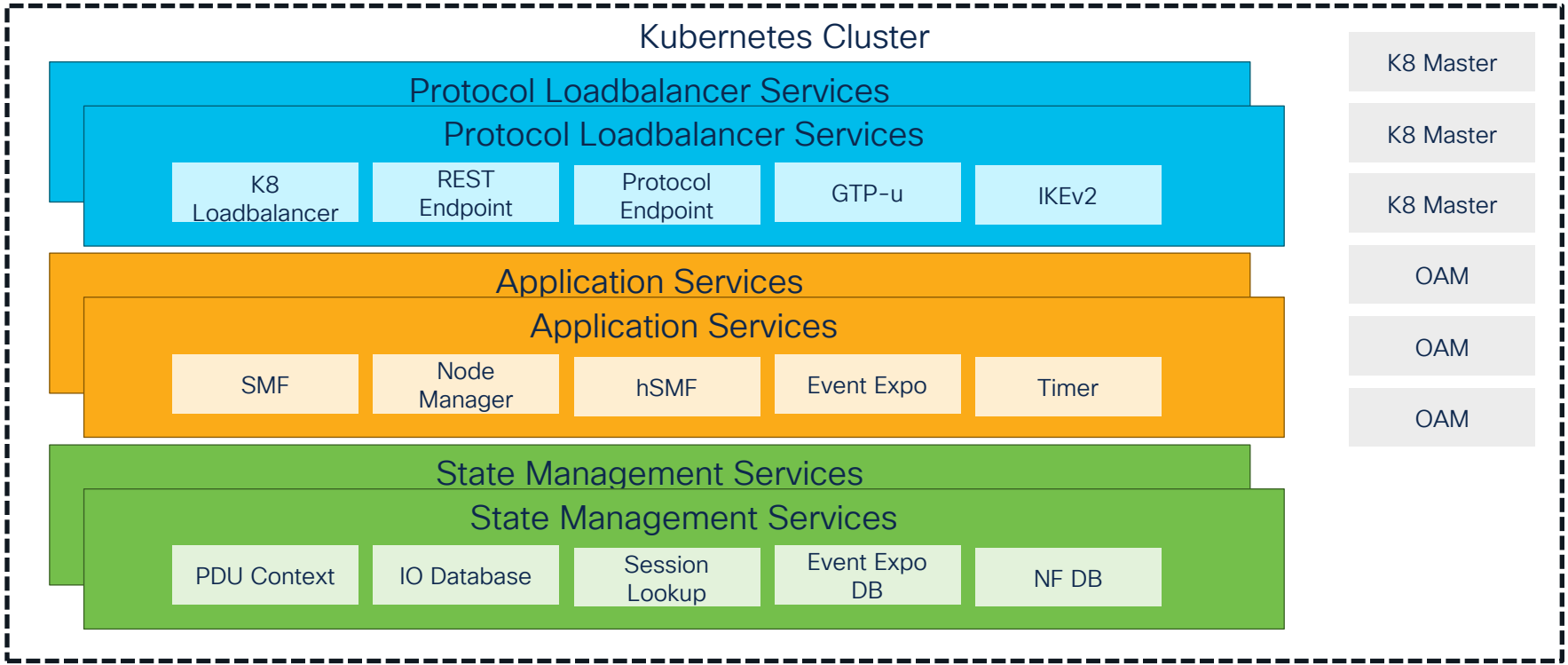
Resilient

Cisco Private 5G Resilience Architecture

- 3-node cluster Edge appliance
- Every NF runs twice – no single point of failure
- Redundant Transport
- Redundant Cloud



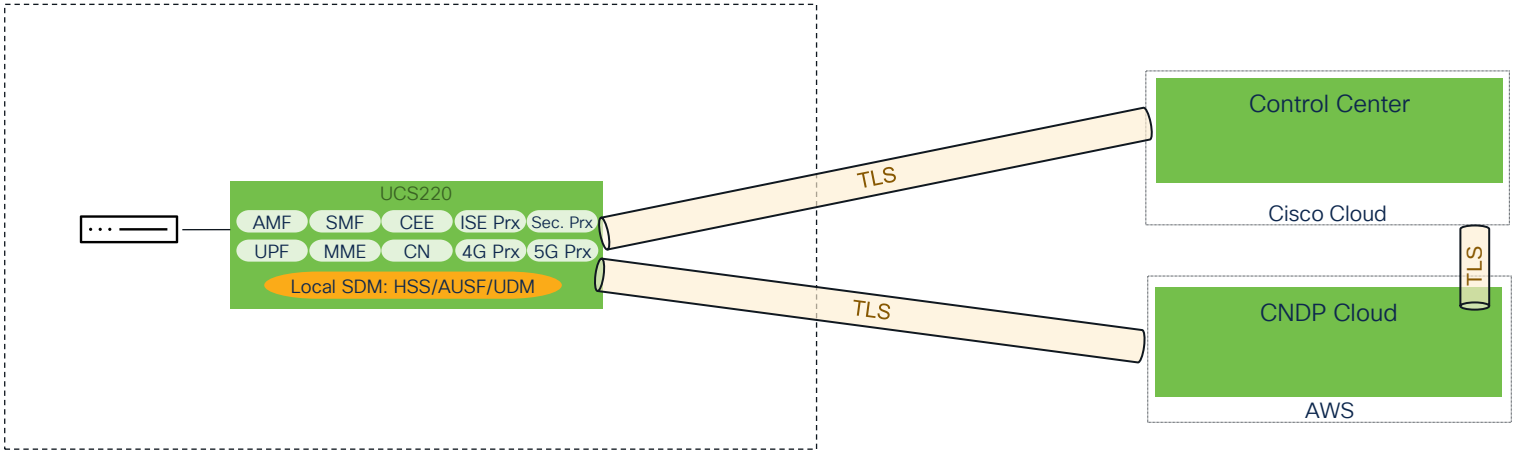
Cisco Private 5G Kubernetes Resilience



Cisco Edge Appliance Resilience Behavior

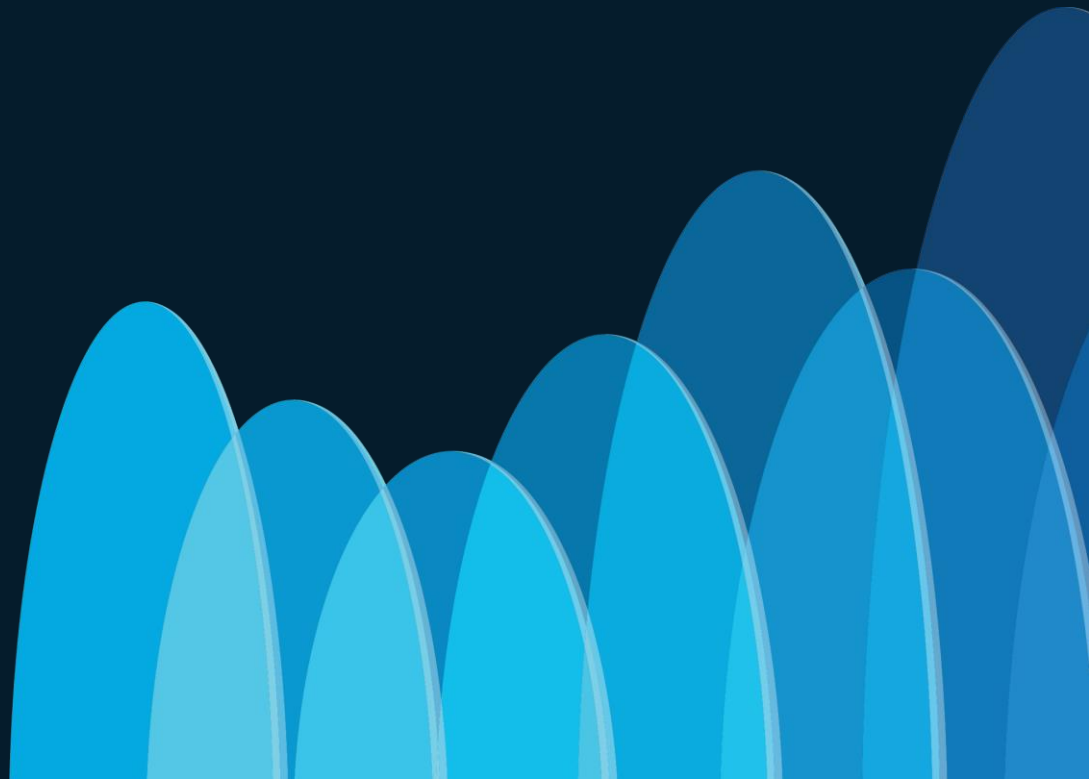
P5G Core Service	Mode	Comment
AMF	Active-Active	Two instances running the various AMF microservices (Figure 68) are instantiated on different hosts. Kubernetes manages the workload distribution.
SMF		
ISE Proxy		
4G Proxy		
5G Proxy		
Security Proxy		
CEE		
SCTP	Active-Standby	Two Stream Control Transmission Protocol (SCTP) microservices for each the AMF instantiated on different hosts. These provide protocol services for the AMF .
UPF	Active-Standby	Two UPF VNFs running in ICSR mode on two hosts, where only 1 instance is active at any point in time.
MME	Active-Active	Two MME VNFs running in an MME Pool instantiated on different hosts. Both MMEs are processing session traffic, but are not exchanging state information.

Cisco Private 5G Core: Local Caching of Subscriber Details



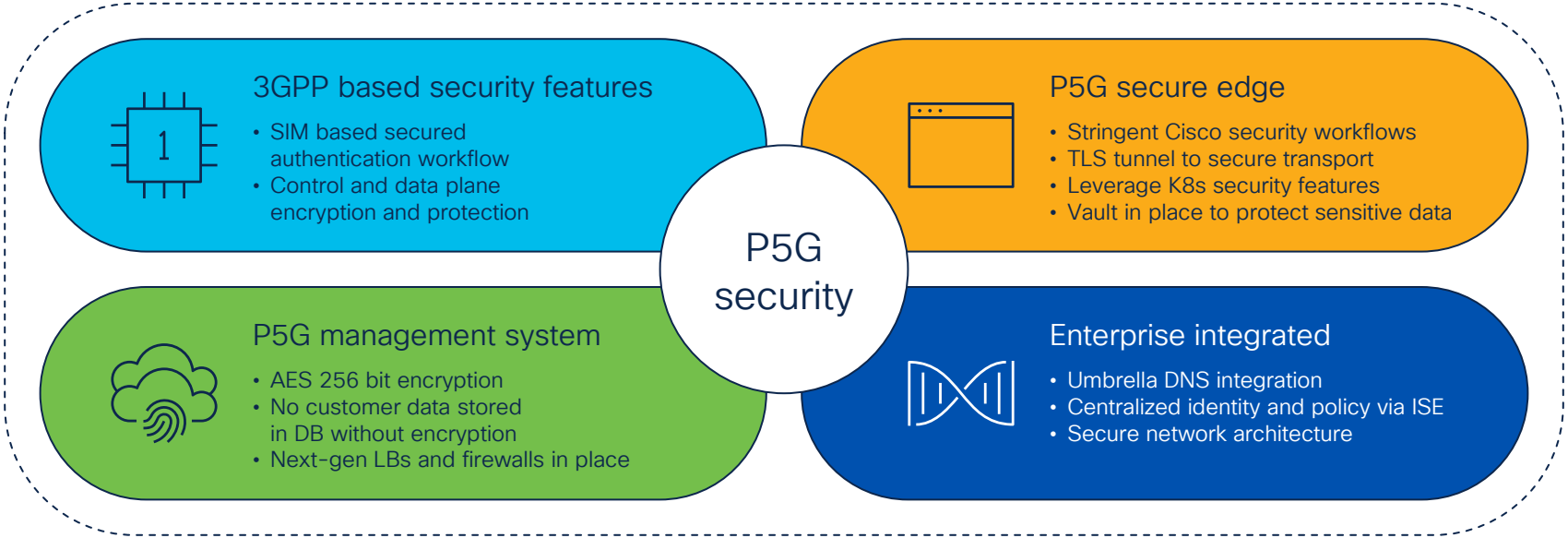
- Continue previously connected sessions on isolated edge (up to 4h)
- Allow net new connections on isolated edge based on locally loaded profile
- Local Subscriber Data Management
  - UE Authentication, registration, subscriber data (DB)
  - Profile syncing with the cloud
  - Initial portion of the traffic handled

Secured & Trusted



cisco Live!

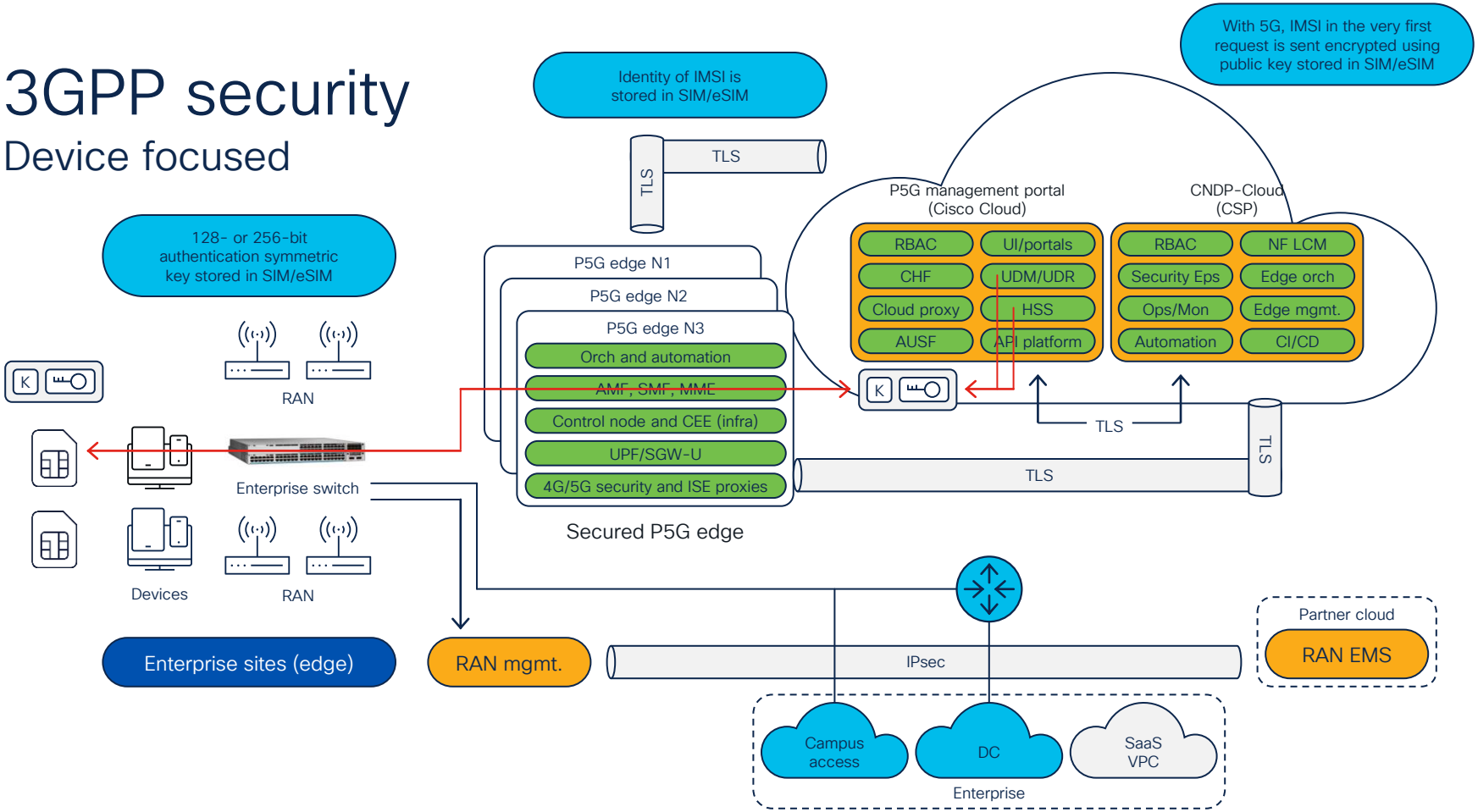
Security across the portfolio



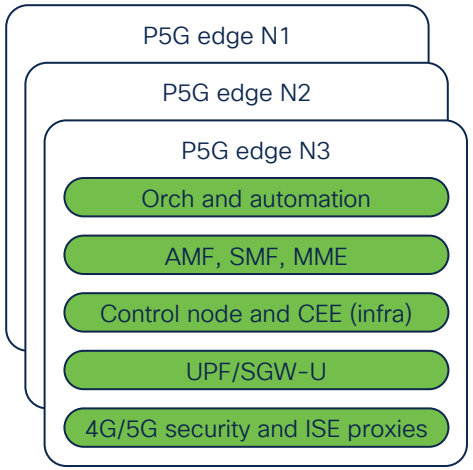
Enterprise grade security across the board

3GPP security

Device focused



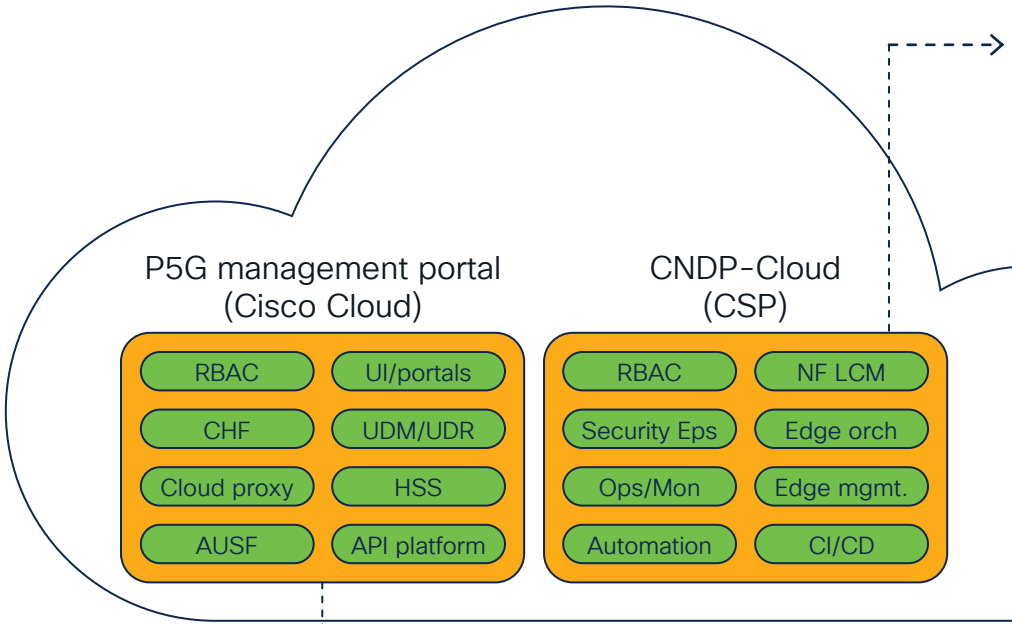
P5G edge security



Secured P5G edge

- Hardened microservices
- TLS connectivity between components
- No remote connection
- AES 256 volume encryption for data at Rest
- Enhanced app layer security over HTTPS via Secure proxy
- Frequent key rotation

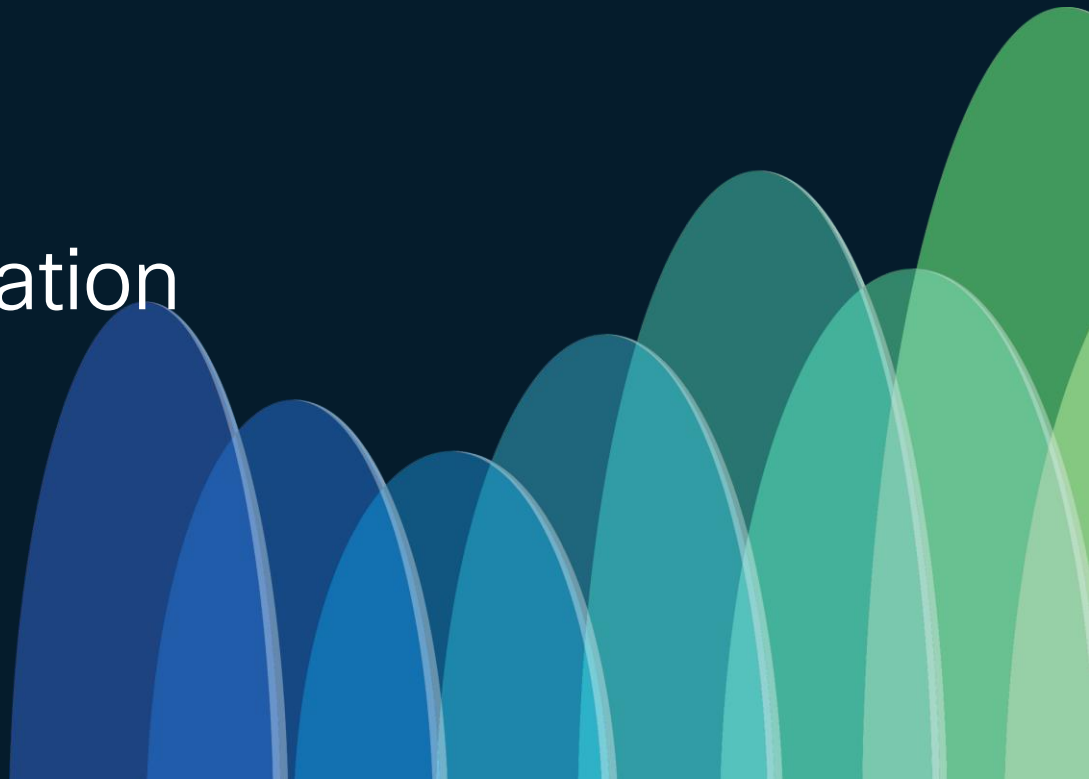
P5G cloud security



- AES 256 volume encryption for data at Rest
- Multi-tenant environment
- Frequent key rotation
- Encrypt/decrypt data before transmission using Vault; All customer data encrypted before storage

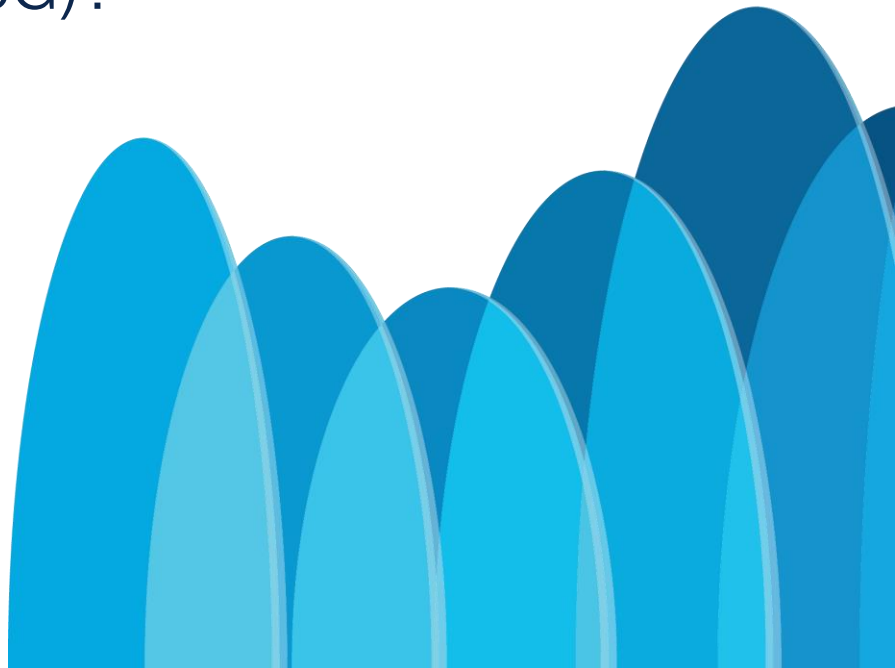
- Advanced load balancers and firewalls in place
- Hardened Microservices
- Geo-Redundant and Multi-tenant cloud environment
- Data remains isolated per enterprise tenant and secured to ensure separation of metrics

Trusted
Enterprise Integration



cisco Live!

““How can enterprise IT/OT admin have common policies and identity across various enterprise domains, such as Wi-Fi, wired, and cellular (4G and 5G)?”



Unified Identity and Policy across domains

P5G & ISE Integration

cisco Live!

Unified policy and identity are critical

Intent

Unified business goals across the enterprise domains driven by ISE

Use cases

Allow wired, wireless, or VPN access to network resources based upon the identity of the user and/or endpoint

Differentiate between corporate and guest users and devices

Classify the endpoints and authorize them appropriately with device profiling

Group-based policy allows for segmentation of the network using access control lists (ACLs)

Identity based policy allows the unified policy to users and devices

VLAN tagging on data plane traffic matching with rest of the campus logic

Security Group Tagging (SGT)

QoS profile

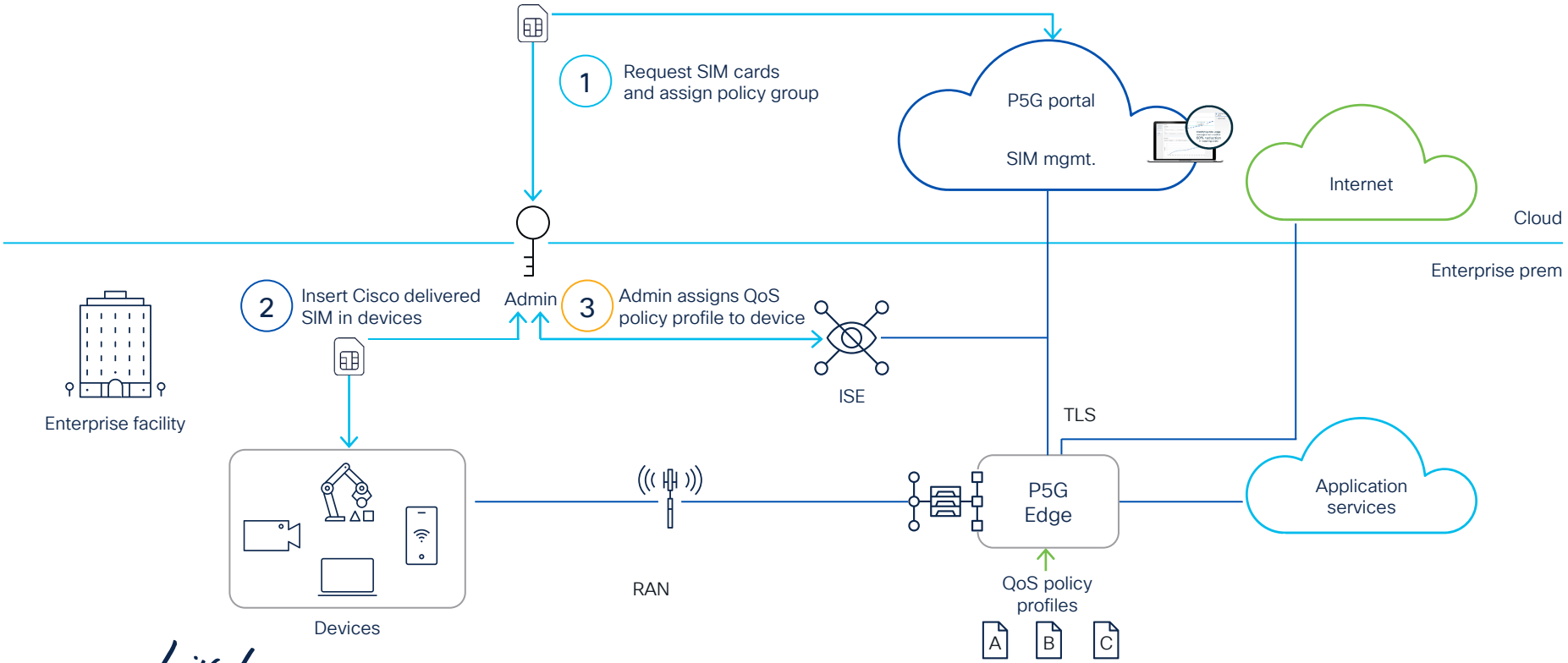
New in P5G

Uplink and downlink Aggregate Maximum Bit Rate (AMBR)

PDU type

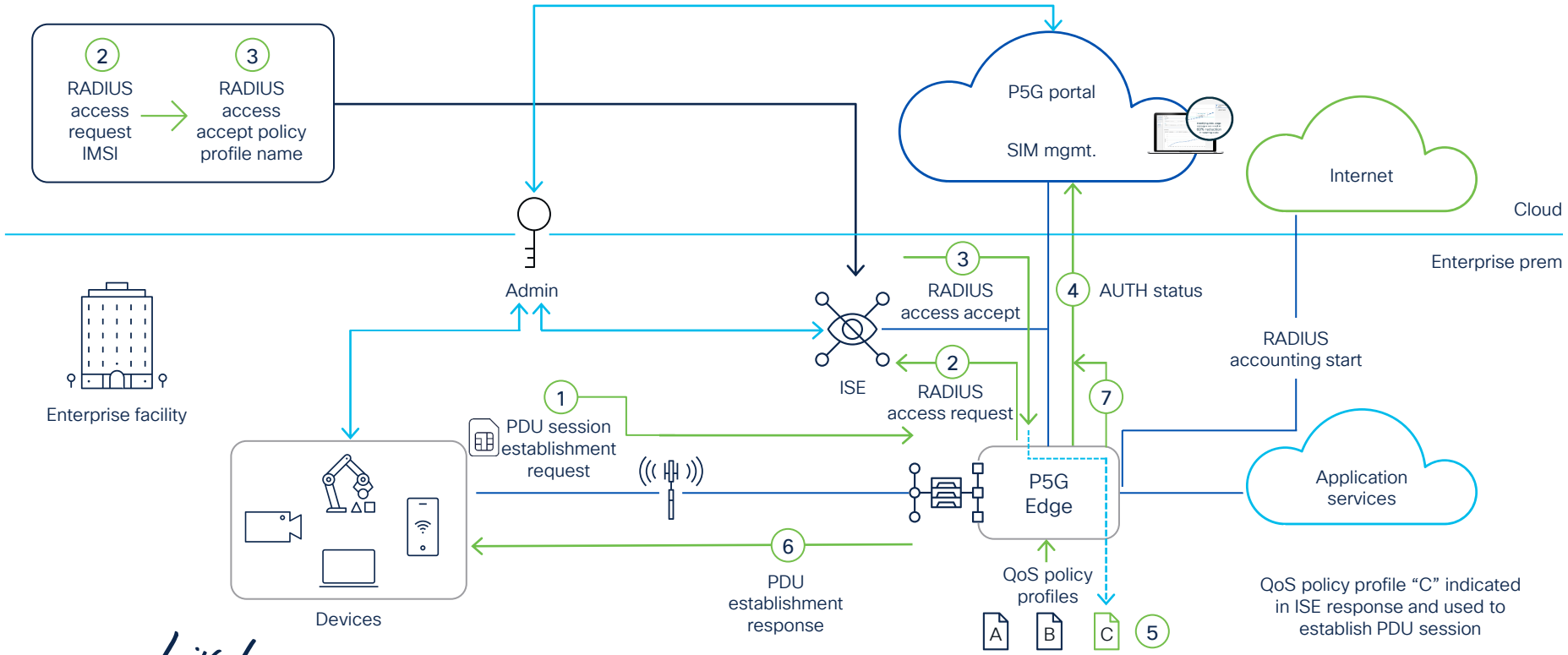
P5G and ISE integration

Overview



P5G and ISE integration

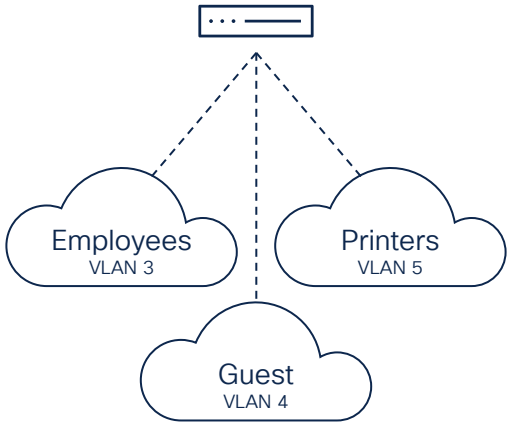
Secondary authorization workflow



Authorization enforcement options

VLANs

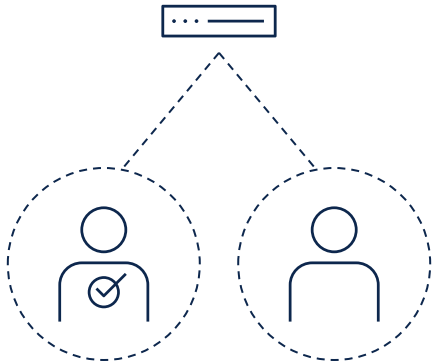
Dynamic VLAN assignments



Per port / per domain / per MAC

ACLs

Access Control Lists

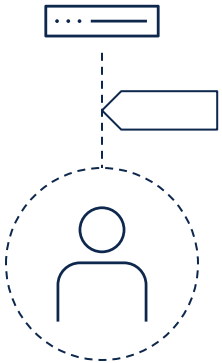


Employee
permit ip any any

Contractor
deny ip host <critical>
permit ip any any

SGTs*

Cisco group-based policy



16-bit SGT assignment and
SGT based access control

* Coming soon

ISE enables zero trust in P5G

Enterprise

Endpoints

- Users
- Devices
- Things

Network devices

- Switches
- WLCs / APs
- VPN
- P5G

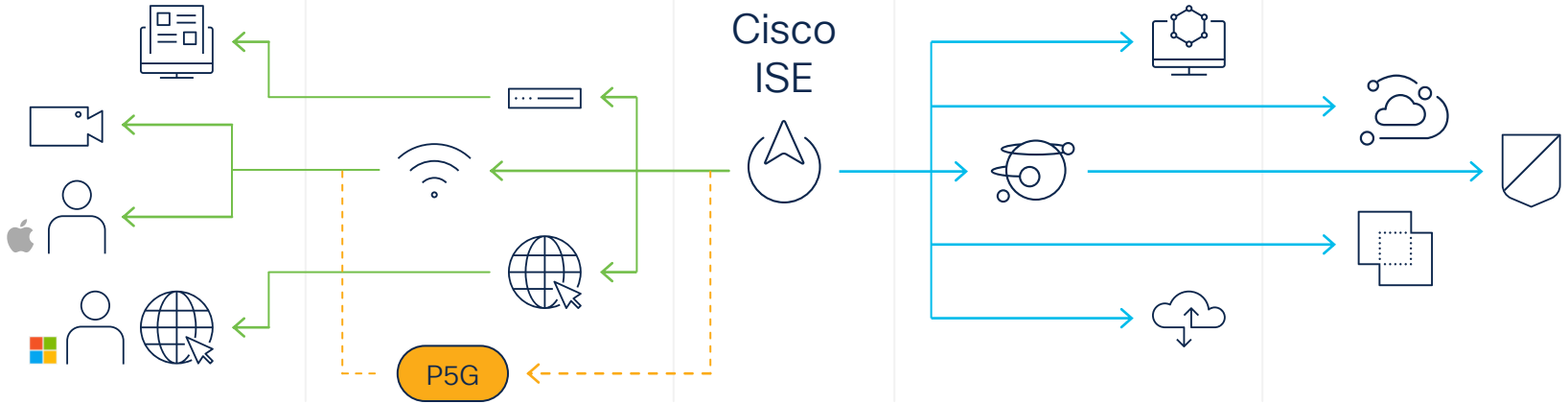
Security

Identity services

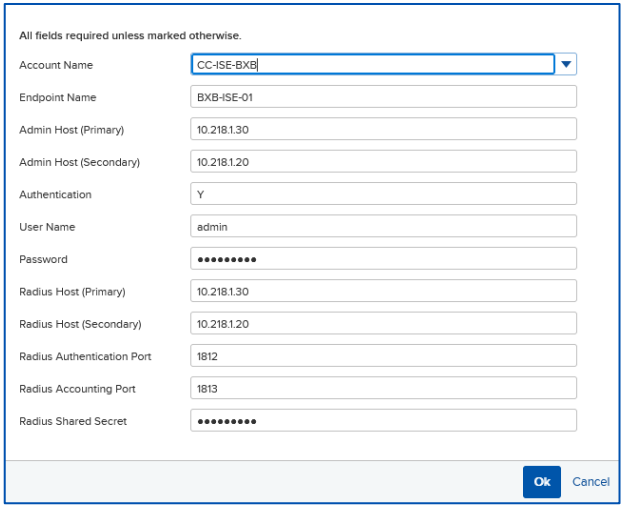
- Azure/AD/LDAP
- MDM
- SAML/MFA

Security services

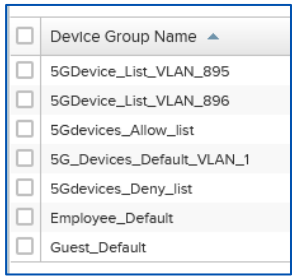
- Cloud analytics
- Secure firewall
- Partners



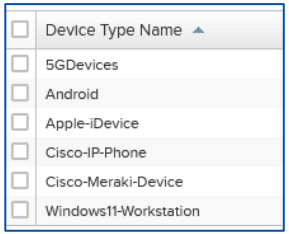
P5G & ISE Integration

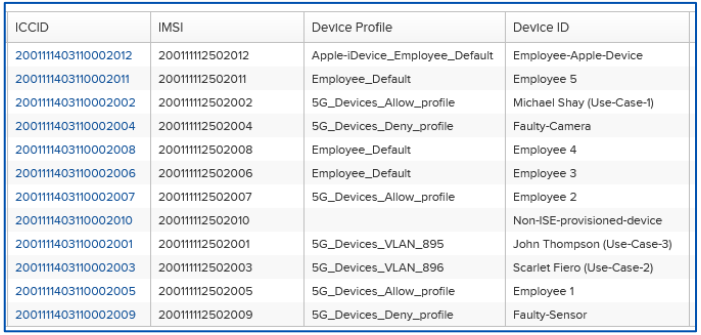


Connect P5G to an ISE Instance



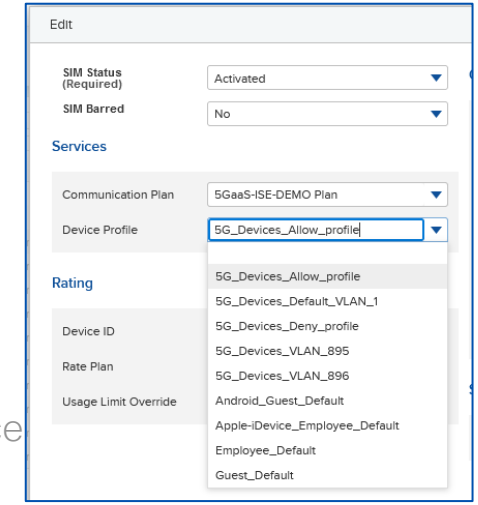
Import Device and User Groups from ISE





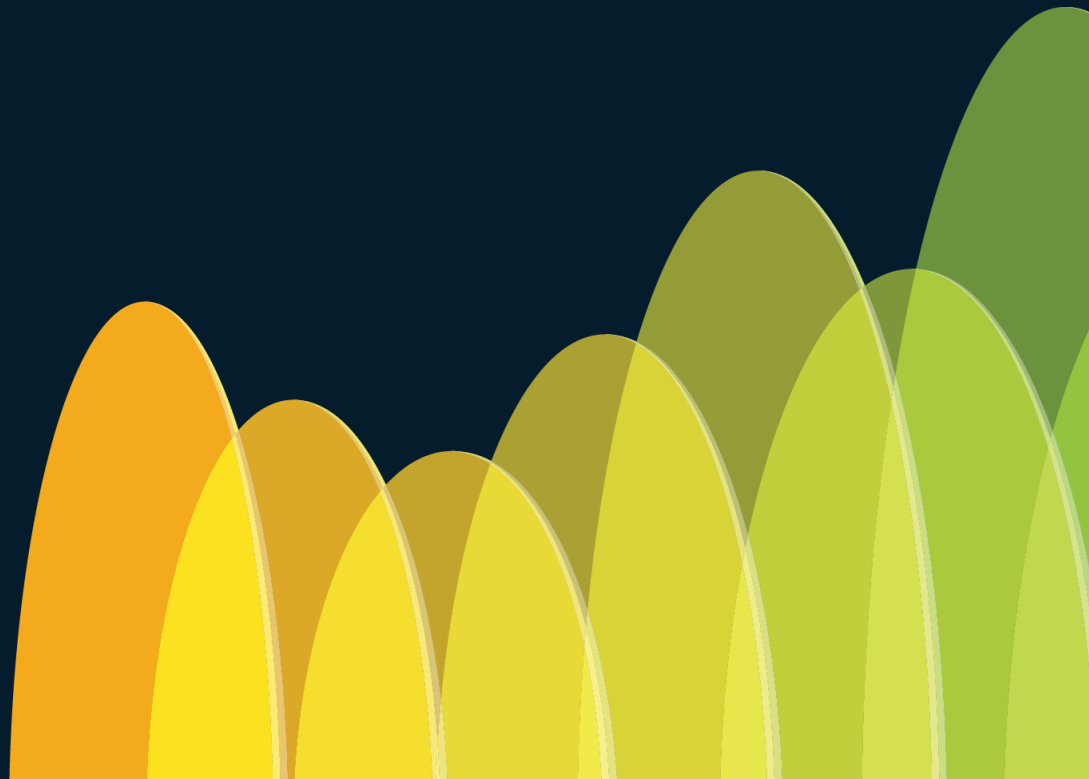
ICCID	IMSI	Device Profile	Device ID
2001111403110002012	200111112502012	Apple-iDevice_Employee_Default	Employee-Apple-Device
2001111403110002011	200111112502011	Employee_Default	Employee 5
2001111403110002002	200111112502002	5G_Devices_Allow_profile	Michael Shay (Use-Case-1)
2001111403110002004	200111112502004	5G_Devices_Deny_profile	Faulty-Camera
2001111403110002008	200111112502008	Employee_Default	Employee 4
2001111403110002006	200111112502006	Employee_Default	Employee 3
2001111403110002007	200111112502007	5G_Devices_Allow_profile	Employee 2
2001111403110002010	200111112502010		Non-ISE-provisioned-device
2001111403110002001	200111112502001	5G_Devices_VLAN_895	John Thompson (Use-Case-3)
2001111403110002003	200111112502003	5G_Devices_VLAN_896	Scarlet Fiero (Use-Case-2)
2001111403110002005	200111112502005	5G_Devices_Allow_profile	Employee 1
2001111403110002009	200111112502009	5G_Devices_Deny_profile	Faulty-Sensor

Create P5G Device Profiles



Assign Device Profiles

Umbrella DNS

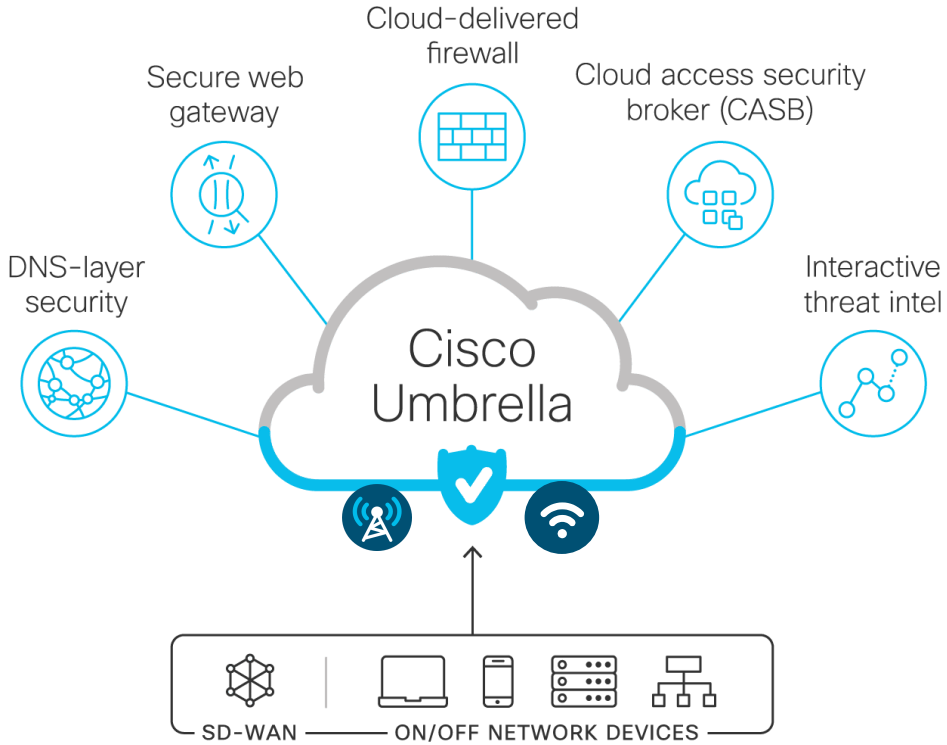


Enterprise Security

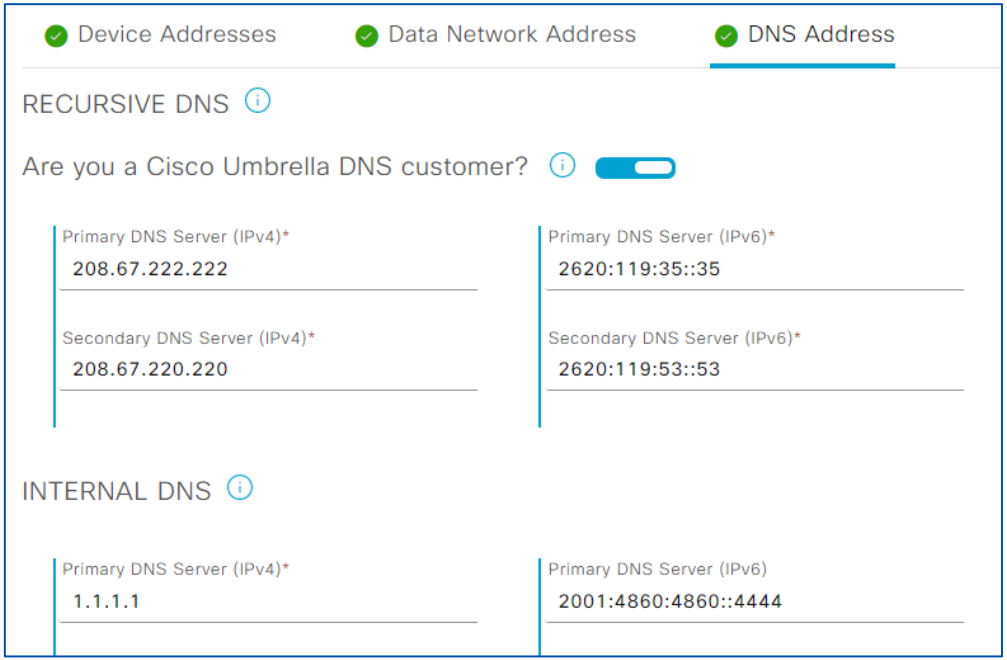
Bringing Enterprise Access, Edge and App Security to 5G

Offline Resource

- Proven Enterprise grade security from access edge to cloud
  - Extends 5G 3GPP SBA and SDA security
- Private 5G SIG and DNS security integration for on/off prem access
- Aligns with Cisco's enterprise security strategy



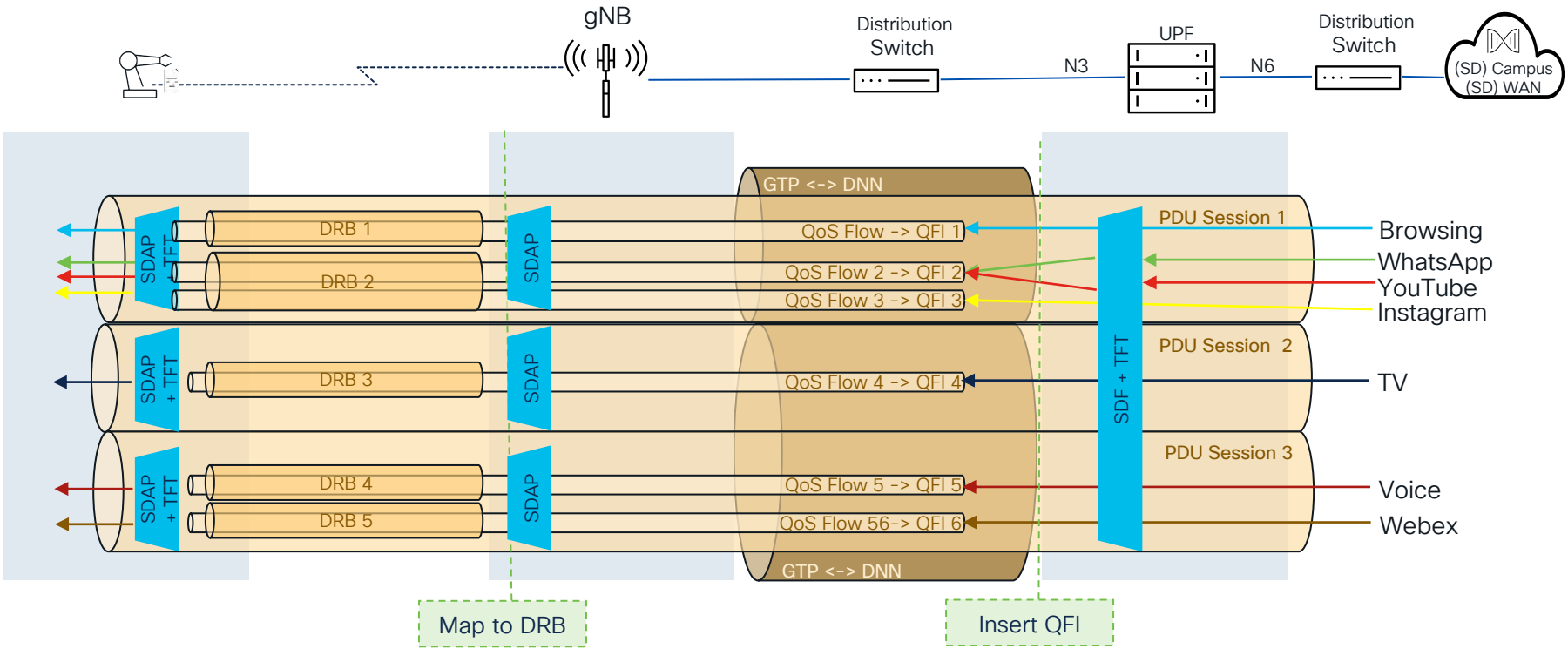
Umbrella DNS Integrates with Cisco Private 5G from Day 1



Configuring your recursive DNS to use Umbrella's DNS servers directs traffic from your network to the Cisco Umbrella global network.

QoS

Example: triple-play Service to a UE



5G QoS Flow Parameters

- Each QoS Flow is associated with a set of parameters in the RAN
- 5G QoS Identifier (5QI) provides a template for the main parameters
  - ARP: priority level, pre-emption capability, pre-emption vulnerability
  - Pre-emption capability: can the flow grab resources from other flows
  - Pre-emption vulnerability: can the flow release resources for other flows
- GBR Flows are associated with additional parameters
  - GFBR, MFBR, Max PLR, Notification Control
- In Addition, a PDU session AND an Endpoint (UE) can be associated with an Aggregate Maximum Bit Rate (AMBR)
  - Uplink and Downlink

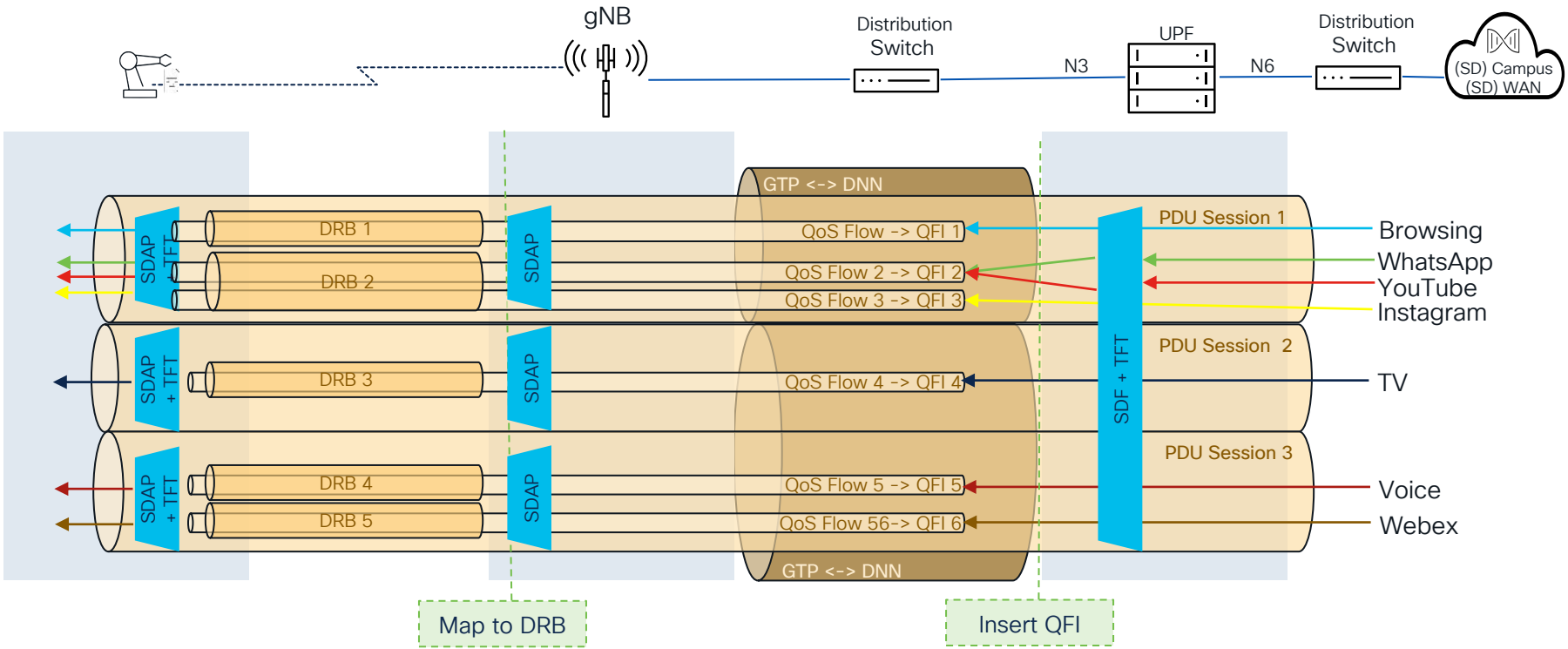
Non-GBR Flow

- 5QI
  - {GBR, non-GBR, delay-critical GBR}
  - Default Priority Level
  - Packet Delay Budget
  - Packet Error Rate
  - Default Maximum Data Burst Volume
  - Default Averaging Window
- Allocation & retention Policy
- Reflective QoS Attribute (seldom used)

- Guaranteed Frame Bit Rate
- Maximum Frame Bit Rate
- Notification Control
- Maximum Packet Loss Rate

GBR Flow

Example: triple-play Service to a UE



5G QoS Flow Parameters

- Each QoS Flow is associated with a set of parameters in the RAN
- 5G QoS Identifier (5QI) provides a template for the main parameters
  - ARP: priority level, pre-emption capability, pre-emption vulnerability
  - Pre-emption capability: can the flow grab resources from other flows
  - Pre-emption vulnerability: can the flow release resources for other flows
- GBR Flows are associated with additional parameters
  - GFBR, MFBR, Max PLR, Notification Control
- In Addition, a PDU session AND an Endpoint (UE) can be associated with an Aggregate Maximum Bit Rate (AMBR)
  - Uplink and Downlink

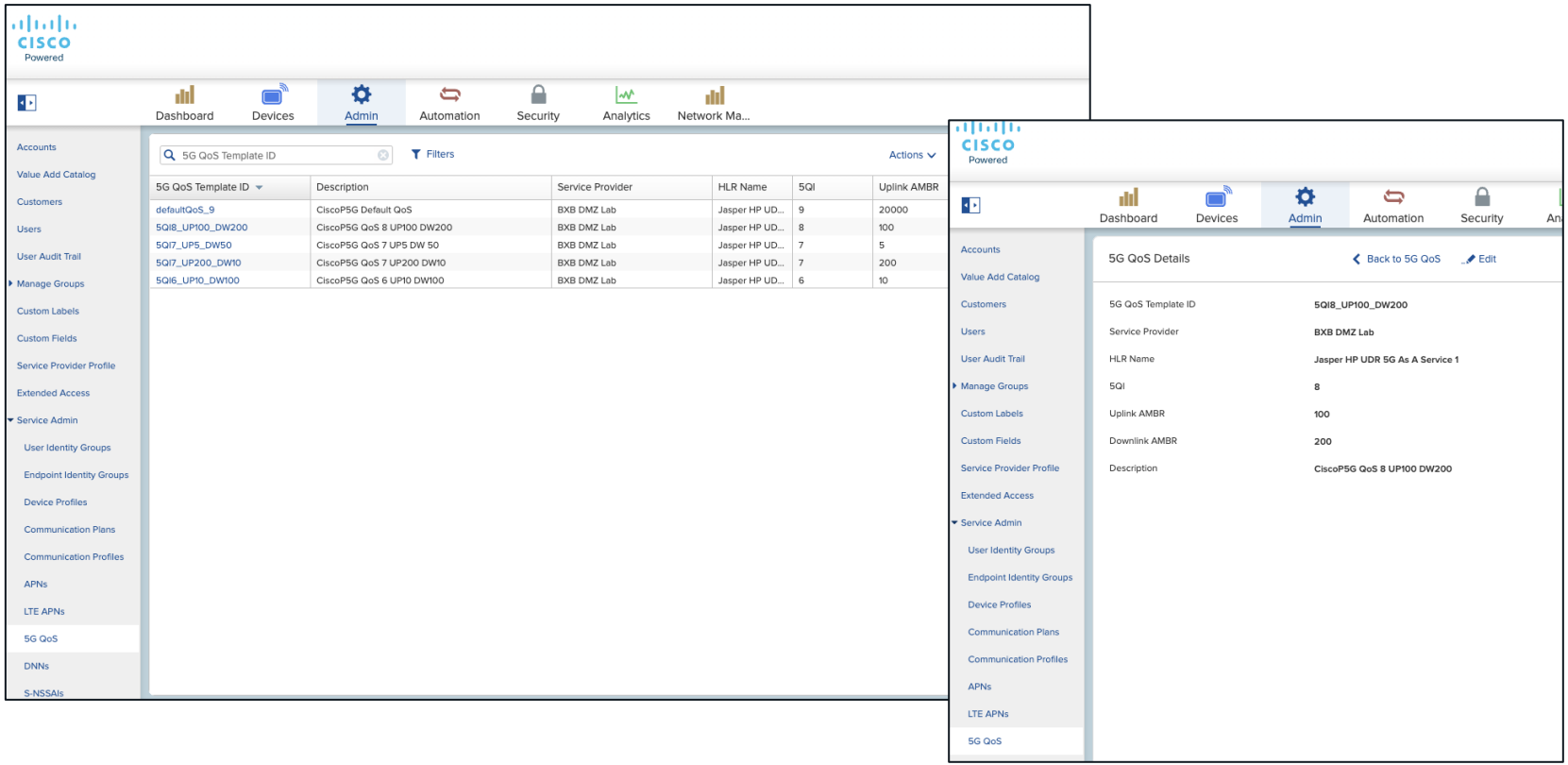
Non-GBR Flow

- 5QI
  - {GBR, non-GBR, delay-critical GBR}
  - Default Priority Level
  - Packet Delay Budget
  - Packet Error Rate
  - Default Maximum Data Burst Volume
  - Default Averaging Window
- Allocation & retention Policy
- Reflective QoS Attribute (seldom used)

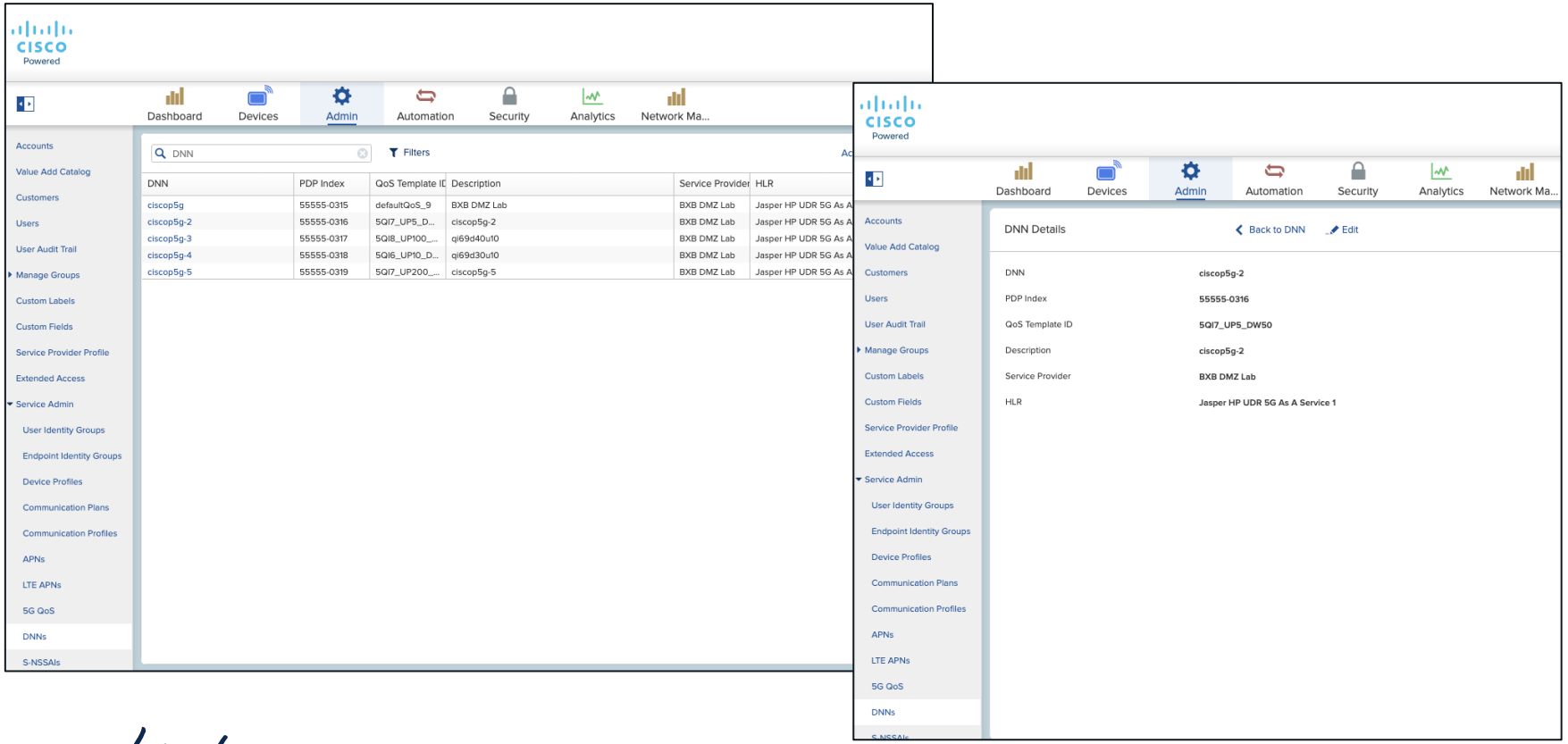
- Guaranteed Frame Bit Rate
- Maximum Frame Bit Rate
- Notification Control
- Maximum Packet Loss Rate

GBR Flow

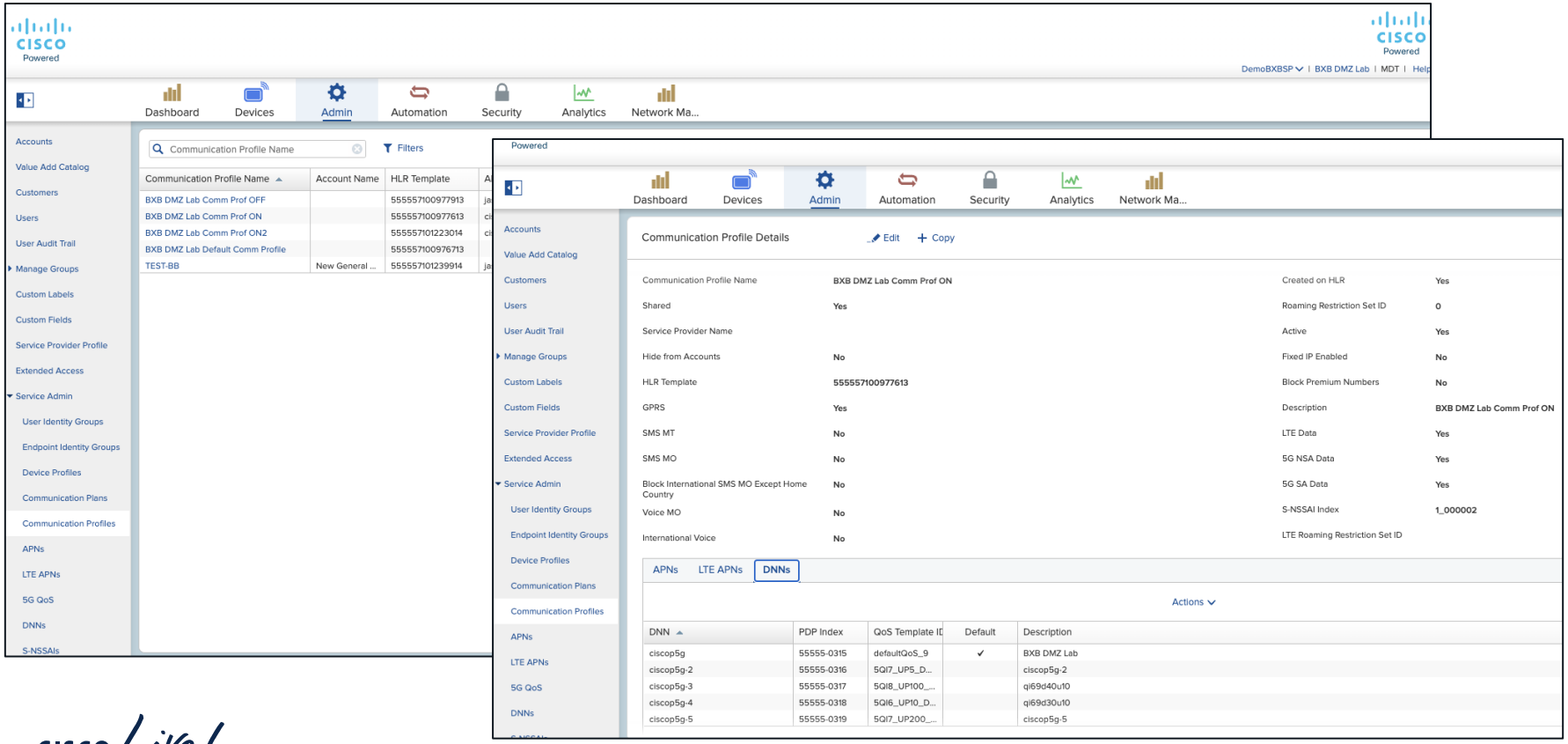
Cisco Control Center – QoS



Cisco Control Center – DNN



Cisco Control Center – Communication Profiles



Specific flows can be prioritized by dynamic GBR assignment

Cisco P5GaaS: Dynamic QoS

In the latest release, Cisco is introducing a Dynamic QoS (Quality of Service) feature, which allows certain types of devices or applications to request a guaranteed bit rate (GBR) from the Private 5G network.

A guaranteed minimum bandwidth significantly reduces the risk of packet loss or burst volumes for mission-critical use cases. Before a device or application connects to the network, Private 5G verifies that the requested minimum bandwidth is available end to end. If it is not, Private 5G denies the connection to ensure a quality user experience.

This feature is a service add-on that users can define in the onboarding wizard. To use the Dynamic QoS feature, the RAN vendor must offer GBR support.

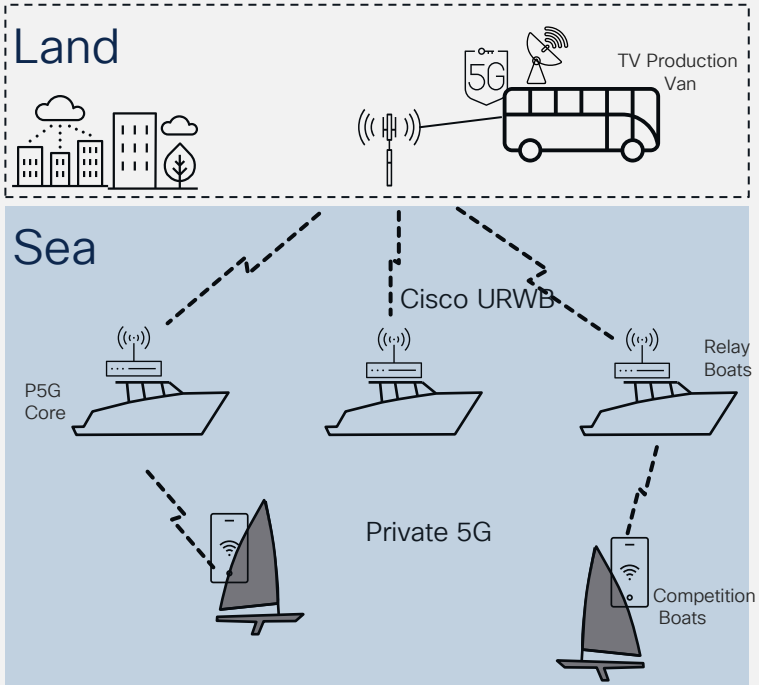
```
"addon_services":{
   "eps_support":true,
   "eps_support_config":{
      "eps_templates":[
         {
            "apn_dnn":"pvtqa.cisco.com",
            "default_session_rule":{
               "uplink":"1010",
               "downlink":"20",
               "5qi":9
            },
            "pcc_rules":[
               {
                  "rule_name":"camera",
                  "flow_infos":[
                     {
                        "flowDescription":"permit out 17 from any to any",
                        "flowDirection":"UPLINK"
                     },
                     {
                        "flowDescription":"permit out 17 from any to any",
                        "flowDirection":"DOWNLINK"
                     }
                  ],
                  "5qi":1,
                  "max_brUl":"70000",
                  "max_brDl":"10000",
                  "gbr_Ul":"60000",
                  "gbr_Dl":"5000"
               }
            ]
         }
      ]
   }
}
```

Sailing Competition Use-case

Description

- Sailing Competition: provide live video feeds from competitors
  - Sailboats equipped with mobile phones to provide video feeds
  - Kite / Wind surfers with Helmet cameras
- Wireless combination used to extend the coverage at sea
  - Using boats to relay signals
  - Relay boats host Private 5G Core and Cisco URWB tracking Horn Antenna
- Benefit:
  - P5G endpoint connectivity – dedicated spectrum!
  - Cisco URWB backhaul to extend field of play

Architecture



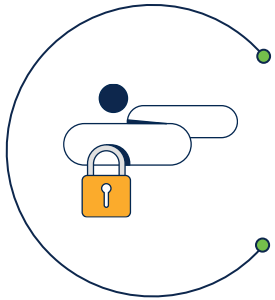
Summary

Summary

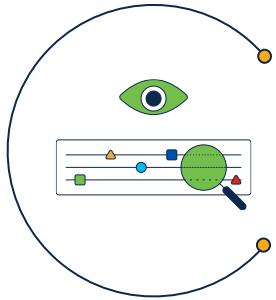
Cisco Private 5G

Enterprise-ready network

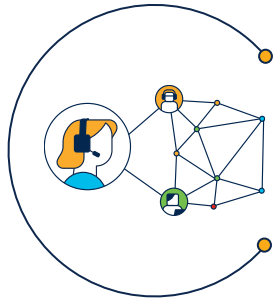
Highly available and resilient network (edge to cloud)



Enterprise-grade security across the board



Enabling partner and enterprise observability



Converged access network (no island)

Thank you

cisco Live!

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 February 28, 2025.

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

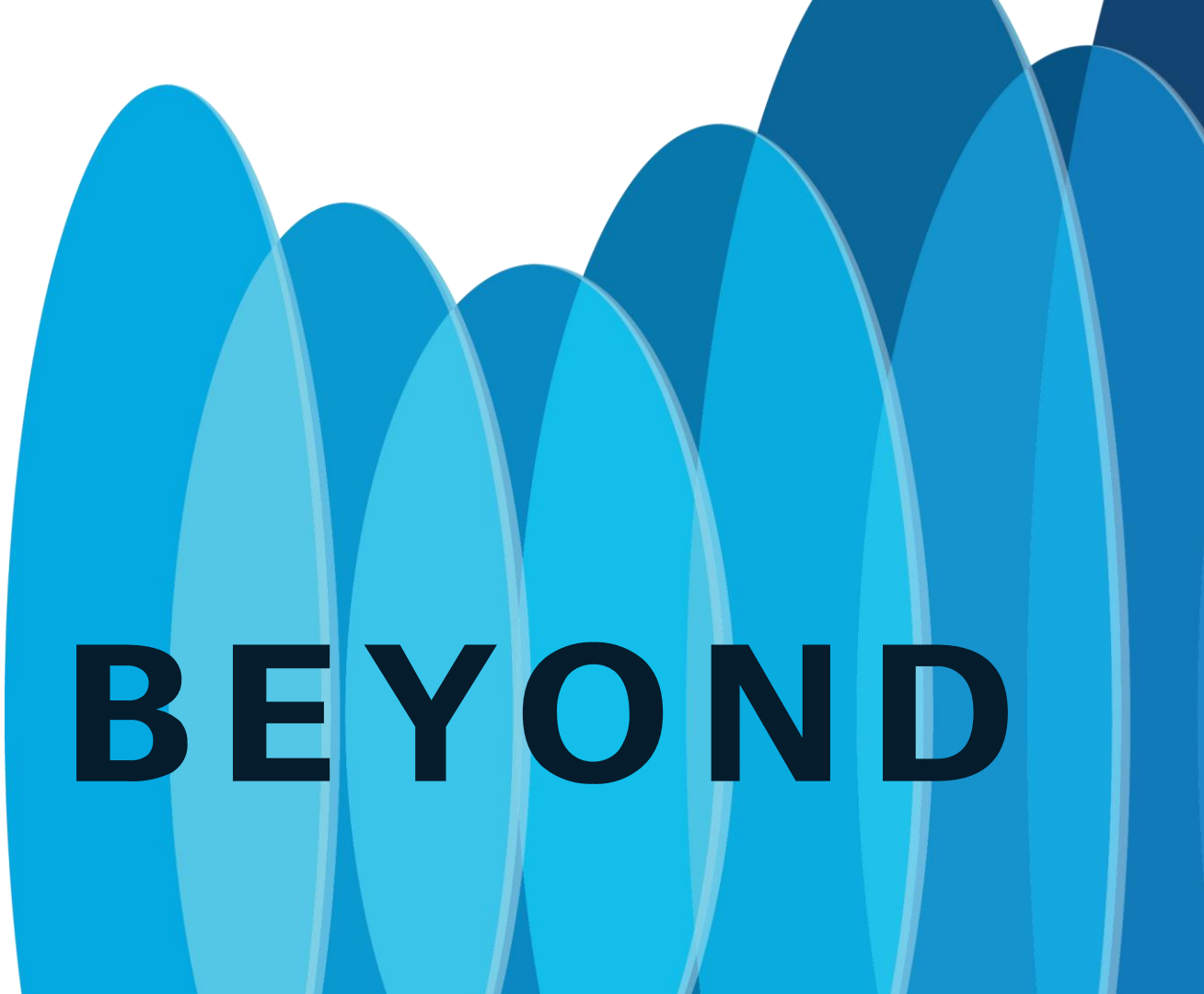
Content Catalog

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me at: filrodri@cisco.com

cisco Live!



GO BEYOND