

NBAR? CBAR? QoS? Confused Enough to Hit the Dive Bar?

CISCO Live !

Nathan Lee
Solutions Engineer

Webex App

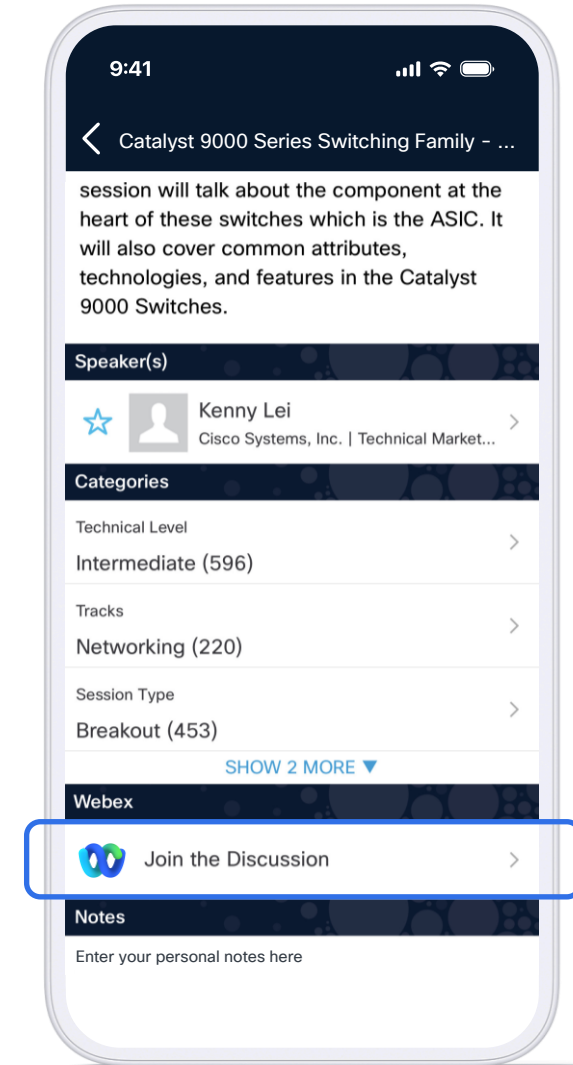
Questions?

Use Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Events 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 27, 2026.



Complete your session surveys



Complete your surveys in the Cisco Events App.



Complete a minimum of 4 session surveys and the overall event survey to receive a unique Cisco Live t-shirt.
(from 11:30 on Thursday, while supplies last)

Agenda

- 01 Introduction
- 02 Analyze Applications
- 03 Monitor Applications
- 04 Control Applications
- 05 Wrap Up

Introduction

Analyze, Monitor and Control Your Applications

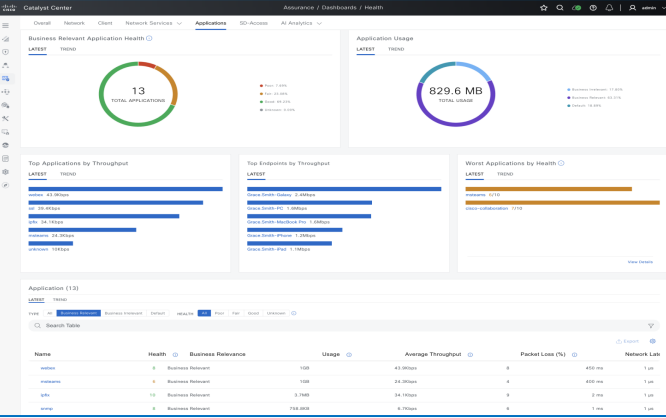
Analyze





Deep Packet Inspection
Encrypted Applications

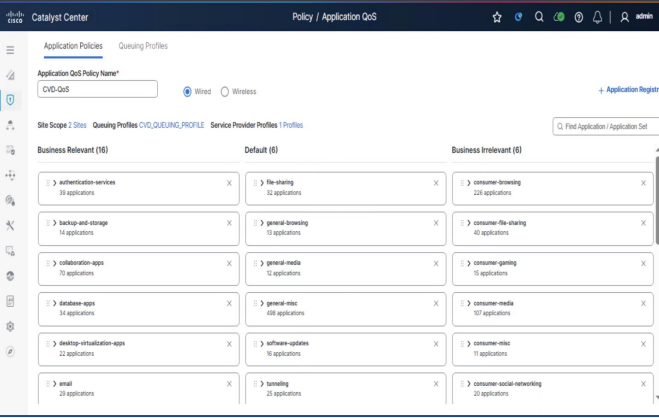
Monitor





Fault Isolation, Troubleshooting
Performance Assessment

Control





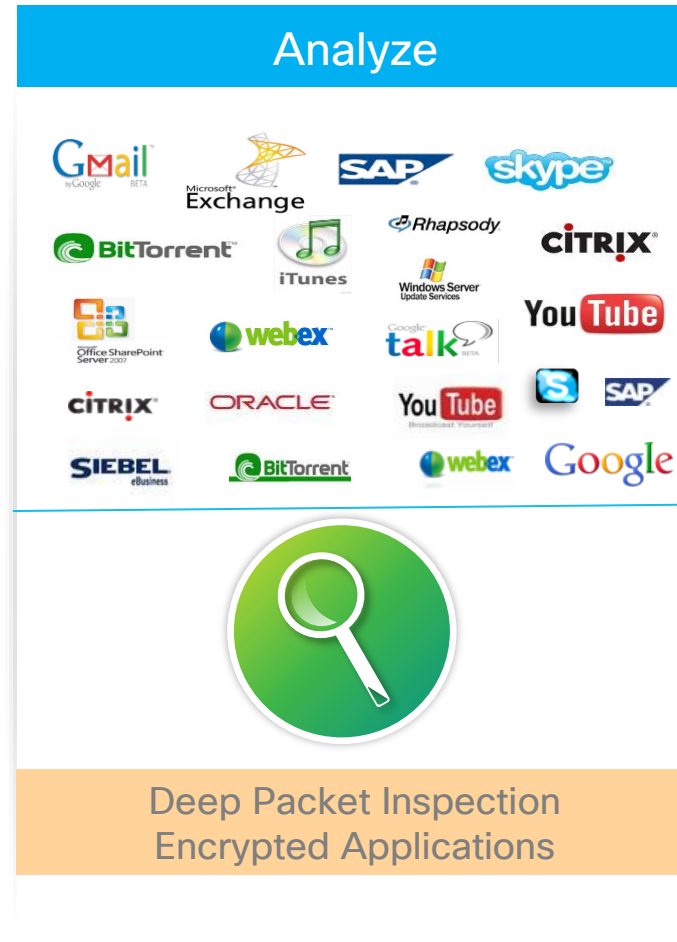
Prioritized Applications, Bandwidth
Management

Hardware and Software Versions

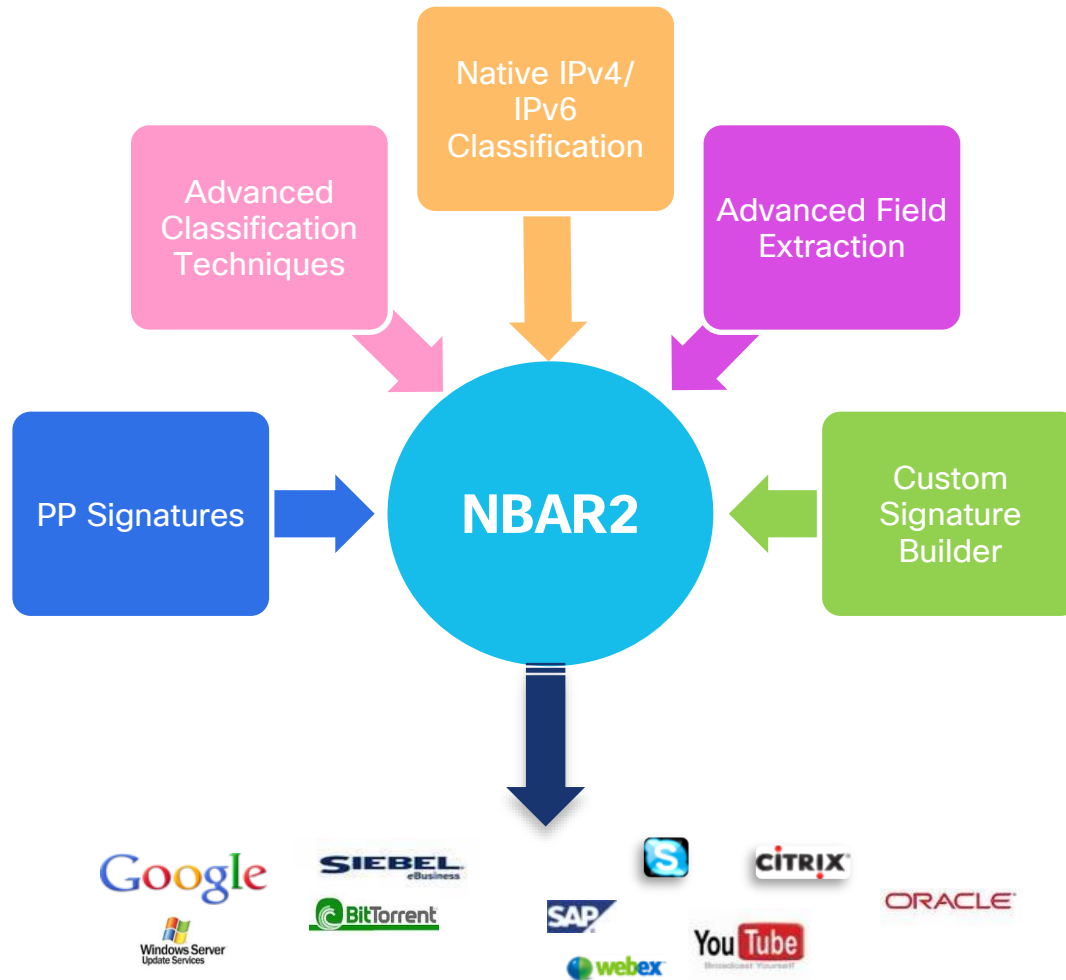
- Catalyst Center 3.2.1
- IOS-XE 17.18.2
- Advantage License

Analyze Applications

Know Your Applications



NBAR2: Advanced Deep Packet Inspection



- Network-Based Application Recognition to classify beyond simple port numbers
- Customized applications support
- Natively classify 1500+ apps, including encrypted ones
- Original data packets hardware switched while initial few packets copied for inspection to create cache
- Hitless protocol pack updates for new application recognition
- Other functions on device (e.g. NetFlow, App QoS) leverages NBAR
- Common app recognition engine across switches, wireless controllers, routers

Enabling NBAR Protocol Discovery

- Loaded NBAR engine with IOS-XE (Catalyst 9300 running IOS-XE 17.18.2)

```
Cat9300-2#show ip nbar protocol-pack active
```

Active Protocol Pack:

Name:	Advanced Protocol Pack
Version:	75.0
Publisher:	Cisco Systems Inc.
NBAR Engine Version:	55
State:	Active

IOS-XE native NBAR protocol pack

Minimum NBAR Engine version required to load protocol-pack

```
Cat9300-2#show ip nbar version
```

```
NBAR software version: 55
NBAR minimum backward compatible version: 55
NBAR change ID: BLD_NBAR_XE1718_20251113_165414
```

Current NBAR Engine version

Backward compatible with protocol-packs built for at least this version

Enabling NBAR Protocol Discovery

- Enable NBAR protocol discovery per interface to collect app usage and direction

```
Cat9300-2#conf t
Cat9300-2(config)#interface Gig1/0/10
Cat9300-2(config-if)#ip nbar protocol-discovery
```

```
Cat9300-2#show ip nbar control-plane | include NBAR state:
NBAR state: ACTIVATED
```

Enabling NBAR Protocol Discovery

- Verify Top-N applications seen by NBAR

```
Cat9300-2#show ip nbar protocol-discovery top-n
```

```
GigabitEthernet1/0/10
```

```
Last clearing of "show ip nbar protocol-discovery" counters 01:02:57
```

Protocol	Input	Output
	-----	-----
	Packet Count	Packet Count
	Byte Count	Byte Count
	5min Bit Rate (bps)	5min Bit Rate (bps)
	5min Max Bit Rate (bps)	5min Max Bit Rate (bps)

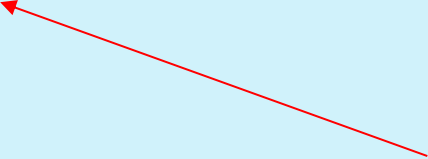
ssl	249485	1013482
	16136915	1455292271
	413000	36492000
	413000	36492000
binary-over-http	23127	94469
	1489700	135778311
	37000	3417000
	37000	3417000
ms-services	1716	2735
	496326	2824632
	0	20000
	16000	67000
instagram	437	1270
	32048	1778859
	0	2000

Enabling NBAR Protocol Discovery

- Update Protocol Pack to recognize new applications without device reboot

```
Cat9300-2#ip nbar protocol-pack flash:NewPack.pack [force]
```

“Force” to downgrade protocol pack



```
Cat9300-2#default ip nbar protocol-pack
```

Revert to protocol pack built into running IOS-XE



NBAR Protocol Pack Releases

- Release info and downloads: www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html





Products and ServicesSolutionsSupportLearnWhy Cisco

Support /

NBAR2 Protocol Pack Library

SavePrint

Updated: December 1, 2025

Bias-Free Language

Downloading NBAR2 Protocol Packs

Cisco NBAR2 Protocol Packs are available for download on the Cisco.com software download page, here:

<https://software.cisco.com/download/home>

On the download page, specify a platform model to display software available for download. One software option is NBAR2 Protocol Packs.

For example, to display protocol packs available for the Cisco ASR 1001-X platform, open the link provided above and navigate as follows:

Products > Routers > Service Provider Edge Routers > ASR 1000 Series Aggregation Services Routers > ASR 1001-X Router

Protocol Pack Support Model

- Protocol Pack upgrades are available for extended-support releases of Cisco IOS XE. See the Software Lifecycle Support Statement - IOS XE.
- Protocol Pack upgrade support continues for 18 months from the FCS date of an extended-support release.
- Cisco releases Protocol Packs with a cadence of 1 to 4 months.

Protocol Pack Details

See the [Cisco NBAR2 Protocol Reference](#) for the details of protocols used in Protocol Pack releases 61.0.0 and later.

NBAR2 Protocol Packs for Cisco IOS and IOS XE Releases

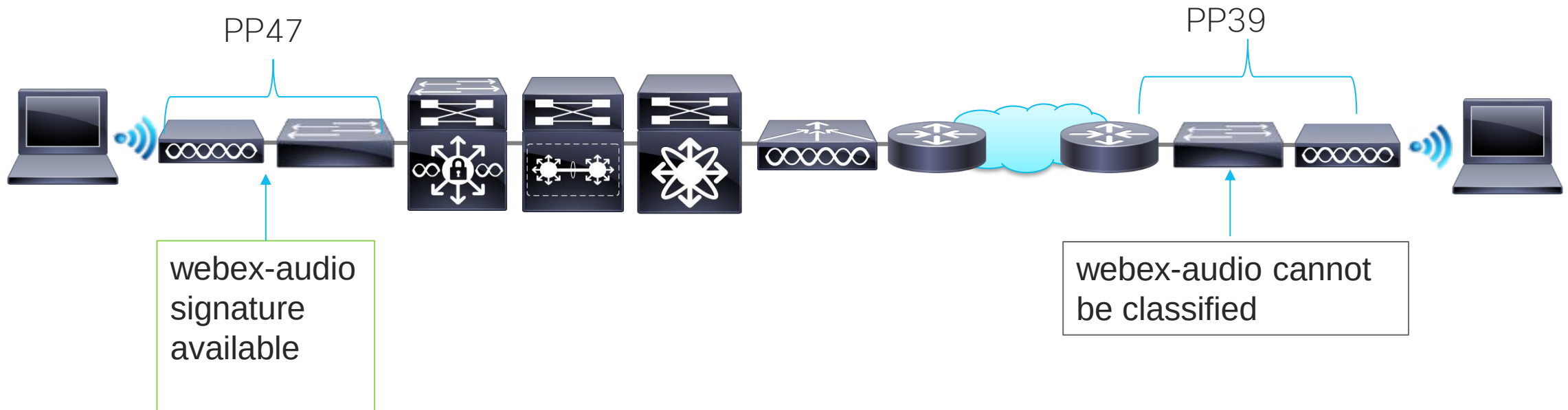
Protocol Pack	Supported Releases	Protocol Pack Release Date
Release Notes for Cisco Protocol Pack 77.0.0	Releases supported by Protocol Pack upgrade: IOS XE 17.15.1 IOS XE 17.15.1a IOS XE 17.18.1 IOS XE 17.18.1a	2025-11-27 2025-11-27 2025-11-27 2025-11-27
Release Notes for Cisco Protocol Pack 76.0.0	Releases supported by Protocol Pack upgrade: IOS XE 17.15.1 IOS XE 17.15.1a IOS XE 17.18.1 IOS XE 17.18.1a	2025-08-28 2025-08-28 2025-08-28 2025-08-28



NBAR Protocol Discovery Deployment at Scale

- NBAR engine runs locally on device
- Hundreds or thousands of network interfaces at access layer
- Updating and maintaining protocol pack consistency across hundreds/thousands of devices?
- Dynamic updates of new application signatures and rules?

Inconsistent App Recognition Without Central Management



Inconsistency in application classification results in poor application monitoring and QoS performance

Controller-Based Application Recognition

- CBAR runs exclusively on Catalyst Center, not on network devices
 - Enhances device-level NBAR through protocol pack management and rules update
- Collects application classification and rules (L3/L4 info mapped to App-ID) from network devices (“sensors”), as well as external sources (e.g. O365, InfoBlox, SAP, etc...)

id	IP	port	L4	vrf-id	vrf name	app-id	eng-id	sel-id	app-name	#hits	black	weight	rating
0	64.103.117.145	5902	TCP	0	global	100	13	100	vnc	1	no	69	1

- Creates Application Rules Pack with info from all sources and publishes to participating network devices (“consumers”)
- Pooling and sharing rules enhances encrypted app classification for the overall network by allowing devices to quickly bypass initial app classification
- Requires DNA-Advantage license on devices
- Supported for fabric or non-fabric network

Enabling CBAR Cloud for External Data Sources

- Use CCO ID to Register With Catalyst Cloud via [System -> Settings -> Cisco Catalyst Cloud](#)

The screenshot displays the Cisco Catalyst Center web interface. At the top, the 'System / Settings' breadcrumb is highlighted with a red box. On the left sidebar, the 'System' menu item is selected and highlighted. In the central pane, the 'Cisco Catalyst Cloud' option is highlighted with a red box. The right pane shows the 'Cisco Catalyst Cloud' settings page, which includes a 'Register' button also highlighted with a red box. The page text instructs users to register the Catalyst Center with Cisco Catalyst Cloud and login with their Cisco credentials.

System / Settings

System

Cisco Catalyst Cloud

Register

Settings > External Services

Cisco Catalyst Cloud

Use this page to register this Catalyst Center with Cisco Catalyst Cloud. You will be prompted to login with your Cisco credentials. Ensure pop-ups are allowed in your browser settings for seamless login.

Enabling CBAR Cloud for External Data Sources

- Successful registration using CCO ID

CiscoCatalyst Center

System / Settings

☆

admin

Design

Policy

Provision

Assurance

Workflows

Energy Management

Tools

Platform

Activities

Reports

System

Explore

Search

Stealthwatch

Talos IP Reputation

Destinations

Cisco Spaces/CMX Servers

Authentication and Policy Servers

Integrity Verification

SD-Access Compatibility Matrix

IP Address Manager

Global Manager Integration

Machine Reasoning Engine

Cisco Catalyst Cloud

Webex Integration

ThousandEyes Integration

System Configuration

System Health

Proxy

Debugging Logs

High Availability

Backup Configuration

Authentication API Encryption

Integration Settings

Visibility and Control of Configura...

Settings > External Services

Cisco Catalyst Cloud

Use this page to register this Catalyst Center with Cisco Catalyst Cloud.

Registered toCisco Catalyst Cloud Portal

Registered by

Account

Registered on5 February 2026

De-register

Click 'De-register' to unregister this Catalyst Center with Cisco Catalyst Cloud.

Applications (Total Count: 5)

Search

Name	Tenant Subscription Status	Category	Actions
Talos Threat Intelligence	Connected		...
Cisco User Defined Network	To Be Connected	UPN	...
Plug and Play as a Service	To Be Connected		...
Meraki Dashboard	To Be Connected	meraki, controller, net	...
AppX MS-Teams	To Be Connected	Data Analysis	...



Enabling CBAR Cloud for External Data Sources

- Verify CBAR Cloud connection via Provision -> Application Visibility -> CBAR Extensions

The screenshot displays the Cisco Catalyst Center interface for Application Visibility. The breadcrumb trail is Provision / Services / Service Catalog / Application Visibility. The left sidebar shows the Service Catalog > Application Visibility path. The main content area has tabs for Overview, Network Devices Enablement, Applications (1519), Application Sets (28), and CBAR Extensions (highlighted with a red box). Under CBAR Extensions, there is a CBAR Cloud button (highlighted with a red box) and an Enable toggle switch (highlighted with a red box). Below these, there is a checkbox for 'Improve network visibility by sharing telemetry' which is checked. The main section is titled 'CBAR Dynamic Application Feeds' and includes a sub-section 'Enable Application Feeds Update: ⓘ' with radio buttons for 'All' (selected) and 'Selected only'. A table lists various applications with their last update times and application counts, each with a checkmark in the top right corner.

Application	Last updated on	Applications
ServiceNow	Feb 8, 2026 02:30	1 applications
SAP	Feb 8, 2026 02:30	1 applications
HubSpot	Feb 8, 2026 02:30	1 applications
RingCentral	Feb 8, 2026 02:30	1 applications
GitHub	Feb 8, 2026 02:30	1 applications
Fastly	Feb 8, 2026 02:30	1 applications
Zscaler	Feb 8, 2026 02:30	1 applications
Microsoft Intune	Feb 8, 2026 02:30	1 applications
Code42	Feb 8, 2026 02:30	1 applications

Enabling CBAR to Manage Devices

- Verify NBAR/CBAR status of devices via Provision -> Application Visibility

Catalyst Center

Provision / Services / Service Catalog / Application Visibility

Service Catalog > Application Visibility

Q Search Hierarchy

Search Help

Global

Bay Area

Overview

Network Devices Enablement

Applications 1519

Application Sets 28

CBAR Extensions

Site Devices 4

Device Family

All

Routers

Switches

Wireless Controllers

Telemetry Appliance

Active Recognition Method

All

CBAR

NBAR

IP/Port

Not Supported

CBAR Readiness

All

Ready

Not ready

Enabled

Telemetry Readiness

All

Ready

Not ready

Enabled

Filter

CBAR

Application Telemetry

Update Protocol Pack

Device name	Management IP	Active recognition method	CBAR Deployment Status	Application Telemetry Deployment Status
☐ C9800-CL	100.64.0.103	Network-based (NBAR)	Not deployed	Not deployed
☐ Cat9300-1	100.124.0.11	Network-based (NBAR)	Not deployed	Not deployed
☐ Cat9300-2	100.124.0.12	Network-based (NBAR)	Not deployed	Not deployed
☐ Fusion.mango.local	100.127.0.2	Network-based (NBAR)	Not deployed	Not deployed

Enabling CBAR to Manage Devices

- Adjust visible columns for more info on CBAR readiness on devices

Filter

CBAR ⓘ

Application Telemetry ⓘ

Update Protocol Pack ⓘ

☐	Device name ⬆	Management IP	Active recognition method ⓘ	CBAR Deployment Status	Application Telemetry Deployment Status ⓘ
☐	C9800-CL	100.64.0.103	Network-based (NBAR)	Not deployed	
☐	Cat9300-1	100.124.0.11	Network-based (NBAR)	Not deployed	
☐	Cat9300-2	100.124.0.12	Network-based (NBAR)	Not deployed	
☐	Fusion.mango.local	100.127.0.2	Network-based (NBAR)	Not deployed	

☒ Active recognition method ⓘ
☐ OS version
☒ CBAR Readiness Status
☐ Protocol pack version ⓘ

☐ Service health status
☐ Application Telemetry Readiness Status
☒ Application Telemetry Deployment Status
☐ Application QoS Policy
☐ WAN Interfaces
☐ Trunk Interfaces

Cancel

Apply

Enabling CBAR to Manage Devices

- Adjust visible columns for more info on CBAR readiness on devices

☐	Device name ▴ ▾	Management IP	Active recognition method ⓘ	CBAR Readiness Status	CBAR Deployment Status	Application Telemetry Deployment ⓘ
☐	C9800-CL	100.64.0.103	Network-based (NBAR)	⚠ Not ready	Not deployed	Not deployed
☐	Cat9300-1	100.124.0.11	Network-based (NBAR)	ⓘ Ready	Not deployed	Not deployed
☐	Cat9300-2	100.124.0.12	Network-based (NBAR)	ⓘ Ready	Not deployed	Not deployed
☐	Fusion.mango.local	100.127.0.2	Network-based (NBAR)	⚠ Not ready WAN Interfaces	Not deployed	Not deployed

Enabling CBAR to Manage Devices

- Router requires at least one specified WAN interface for CBAR management

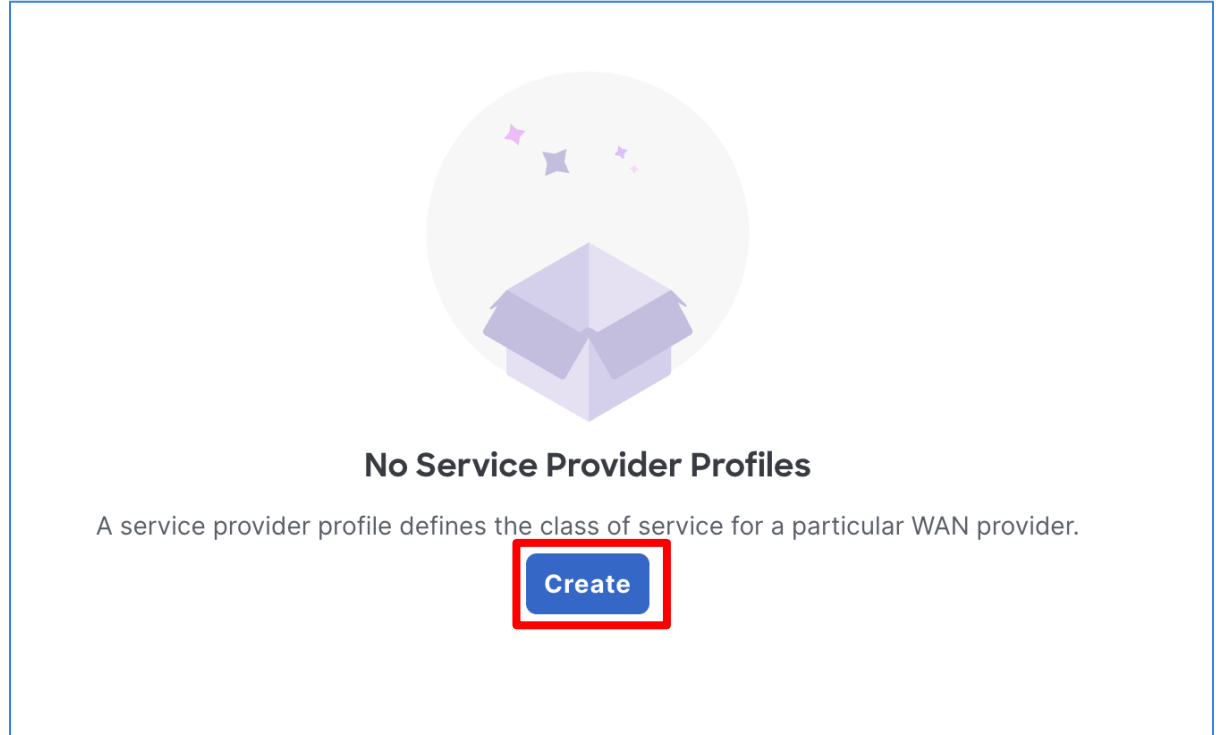
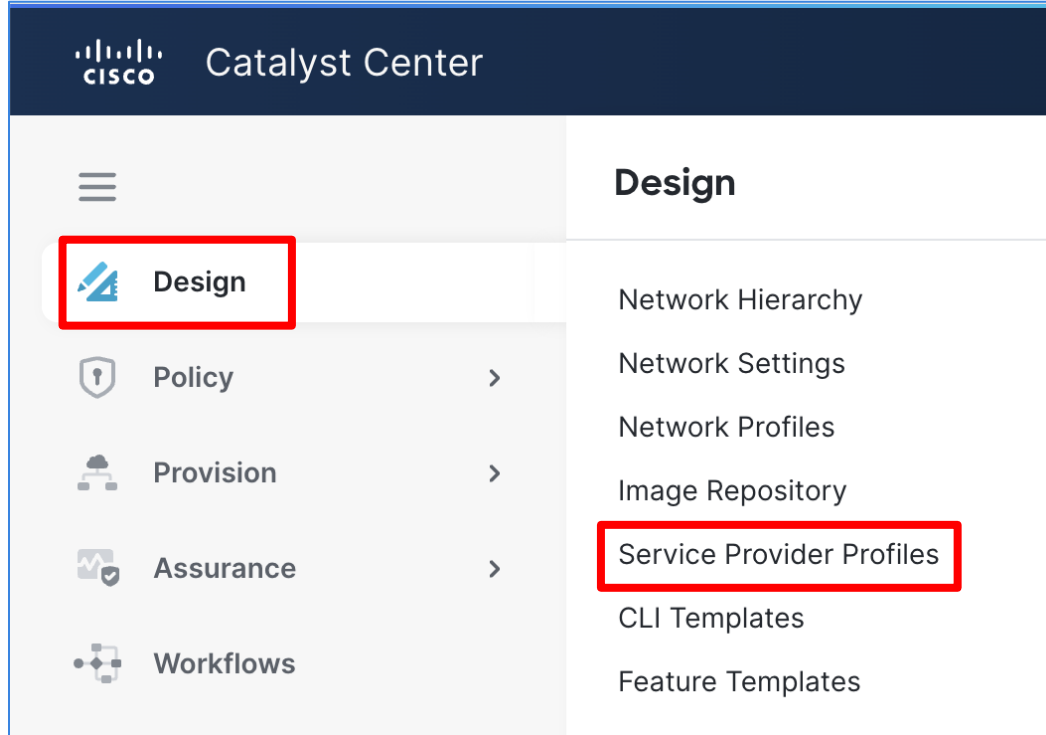
☐	Device name ▾	Management IP	Active recognition method ⓘ	CBAR Readiness Status	CBAR Deployment Status	Application Telemetry Deployment
☐	C9800-CL	100.64.0.103	Network-based (NBAR)	⚠ Not ready	Not deployed	Not deployed
☐	Cat9300-1	100.124.0.11	Network-based (NBAR)	⚠ Not ready	Not deployed	Not deployed
☐	Cat9300-2	100.124.0.12	Network-based (NBAR)	⚠ Not ready	Not deployed	Not deployed
☐	Fusion.mango.local	100.127.0.2	Network-based (NBAR)	⚠ Not ready	Not deployed	Not deployed

Application Visibility is not supported on this device.
To support it, define at least one WAN interface

[WAN Interfaces](#)

Enabling CBAR to Manage Devices

- Adding Service Provider Profile for CBAR and QoS queuing



Enabling CBAR to Manage Devices

- Profile specifies queuing service model (4, 5, 6 or 8 classes) for WAN provider

You can create a service provider (SP) profile that defines the class of service for a particular WAN provider. You can define 4-class, 5-class, 6-class, and 8-class service models.

Profile Name*

Internet-Provider

WAN Provider*

ISP

Model*

4 Class

+

Delete All

Reset

Save

Enabling CBAR to Manage Devices

- Correcting issue on router for CBAR management

☐	Device name 	Management IP	Active recognition method 	CBAR Readiness Status	CBAR Deployment Status	Application Telemetry Deployment 
☐	C9800-CL	100.64.0.103	Network-based (NBAR)	 Not ready	Not deployed	Not deployed
☐	Cat9300-1	100.124.0.11	Network-based (NBAR)	 Ready	Not deployed	Not deployed
☐	Cat9300-2	100.124.0.12	Network-based (NBAR)	 Ready	Not deployed	Not deployed
☐	Fusion.mango.local	100.127.0.2	Network-based (NBAR)	 Not ready WAN Interfaces	Not deployed	Not deployed

Enabling CBAR to Manage Devices

- Need to specify at least one WAN interface on router
- Recommended to attach Service Provider Profile for proper QoS marking and queuing

WAN Connectivity Settings for Device Fusion.mango.local

+ Add Row

Filter | Delete 0 Selected

☐	Interface	Role	Service Provider Profile	Sub-Line Rate (Mbps)
No data to display				

Enabling CBAR to Manage Devices

- Tie created SP Profile to WAN interface on router

WAN Connectivity Settings for Device Fusion.mango.local

×

+ Add Row

Filter | Delete 0 Selected

☐	Interface ▴ ▾	Role	Service Provider Profile	Sub-Line Rate (Mbps)
☐	Select Interface GigabitEtherne... ▾	Select Role WAN ▾	Select Profile Internet-Provid... ▾	100

CancelSave

Enabling CBAR to Manage Devices

- Router ready to be enabled for CBAR

Filter		CBAR		Application Telemetry		Update Protocol Pack	
Device		Device recognition method		CBAR Readiness Status		CBAR Deployment Status	
C9800		Network-based (NBAR)		⚠ Not ready		Not deployed	
Cat93		Network-based (NBAR)		ℹ Ready		Not deployed	
Cat9300-2		100.124.0.12 Network-based (NBAR)		ℹ Ready		Not deployed	
Fusion.mango.local		100.127.0.2 Network-based (NBAR)		👍 Ready		Not deployed	

Enabling CBAR to Manage Devices

- NBAR/CBAR configuration pushed to Router

```
platform wdvavc serviceability
```

```
avc sd-service
```

```
segment AppRecognition
```

```
controller
```

```
address <Catalyst Center IPv4/IPv6 address>
```

```
destination-ports sensor-exporter 21730
```

```
dscp 16
```

```
source-interface Loopback0
```

```
transport application-updates https url-prefix sdavc
```

```
interface GigabitEthernet0/0/0
```

```
ip nbar protocol-discovery
```

Catalyst Center address for CBAR functionalities

Transport to update protocol pack and application rule updates

NBAR protocol discovery command applies to specified WAN port

Enabling CBAR to Manage Devices

- WLC needs SSID created & provisioned
- AP(s) needs to be associated to WLC & provisioned

Filter

CBAR ⓘ Application Telemetry

☐	Device name	Management IP	Active		CBAR Deployment Status
☐	C9800-CL	100.64.0.103	Network-based (NBAR)	⚠ Not ready	Not deployed
☐	Cat9300-1	100.124.0.11	Network-based (NBAR)	ⓘ Ready	Not deployed
☐	Cat9300-2	100.124.0.12	Network-based (NBAR)	ⓘ Ready	Not deployed
☐	Fusion.mango.local	100.127.0.2	CBAR	✅ Enabled	Completed Re-Configure

Application Visibility is not supported on this device. To support it, provision at least one non-fabric/fabric/flex-connect enterprise ssid. Also ensure that APs are assigned to the site and provisioned.

Enabling CBAR to Manage Devices

- Enabling CBAR for WLC after creating/provisioning SSID and associating AP to WLC

Filter

CBAR ⓘ

Application Telemetry ⓘ

Update Protocol Pack ⓘ

Device

Enable CBAR on selected devices

Disable CBAR on selected devices

Enable CBAR on all ready devices

Disable CBAR on all devices

			Recognition method ⓘ	CBAR Readiness Status	CBAR Deployment Status
☒	C9800		Network-based (NBAR)	☒ Ready	Not deployed
☐	Cat93		Network-based (NBAR)	ⓘ Ready	Not deployed
☐	Cat9300-2	100.124.0.12	Network-based (NBAR)	ⓘ Ready	Not deployed
☐	Fusion.mango.local	100.127.0.2	CBAR	☒ Enabled	Completed Re-Configure

Enabling CBAR to Manage Devices

- All SSID types (Local, Flex, Fabric) supported for CBAR enablement
- Note that wireless policy profile on APs will momentarily shut down to apply configuration

Enable CBAR

You have chosen to enable CBAR on 1 wireless controllers.

For eCA devices with BORDER role, CBAR will be enabled only in wireless mode

AP provisioning is required for Enabling CBAR in wireless modes.
CBAR enable for flex/fabric on wireless controllers is not supported on OS version less than 17.7.1.

For each wireless controller, select the SSID types where you would like to enable CBAR.

C9800-CL

☒ Local ☐ Flex ☐ Fabric

Cancel Next



Warning

Enabling CBAR on the selected SSID types will cause APs connected to the device to reboot.

Are you sure?

No Yes

Enabling CBAR to Manage Devices



- NBAR/CBAR configuration pushed to WLC

avc sd-service

```
segment AppRecognition  
controller  
address <Catalyst Center IPv4/IPv6 address>  
destination-ports sensor-exporter 21730  
dscp 16  
source-interface Vlan64  
transport application-updates https url-prefix sdavc
```

```
wireless profile policy <WLAN-ProfileName>_profile  
ip nbar protocol-discovery
```

NBAR protocol discovery command applies to Policy Profile

Enabling CBAR to Manage Devices

- Enabling CBAR for switches

Filter

CBAR

Application Telemetry

Update Protocol Pack

Device

Enable CBAR on selected devices

Disable CBAR on selected devices

Enable CBAR on all ready devices

Disable CBAR on all devices

			Recognition method	CBAR Readiness Status	CBAR Deployment Status
☐	C9800			Enabled	Completed Re-Configure
☒	Cat9300-1	100.124.0.12	Network-based (NBAR)	Ready	Not deployed
☒	Cat9300-2	100.124.0.12	Network-based (NBAR)	Ready	Not deployed
☐	Fusion.mango.local	100.127.0.2	CBAR	Enabled	Completed Re-Configure

Enabling CBAR to Manage Devices

- Option to enable NBAR/CBAR on selected interfaces (default is all access ports)

Enable CBAR > Review Devices

×

Enable CBAR

Q Find Device

≡

Device Name ▾	Device Role	CBAR Exclusions
Cat9300-2	ACCESS	View Interfaces
Cat9300-1	ACCESS	View Interfaces

100.64.0.103

Cancel

Enable

Enable CBAR > Review Devices > Cat9300-2

×

Enable CBAR

Q Find Interface

Show

All

 Excluded Interfaces

Interfaces ▾	Status ⓘ
GigabitEthernet1/0/9	☒
GigabitEthernet1/0/8	☒
GigabitEthernet1/0/7	☒
GigabitEthernet1/0/6	☒
GigabitEthernet1/0/5	☒
GigabitEthernet1/0/4	☒
GigabitEthernet1/0/3	☒
GigabitEthernet1/0/2	☒
GigabitEthernet1/0/18	☒
GigabitEthernet1/0/17	☒

Cancel

Save

Enabling CBAR to Manage Devices

- NBAR (enhanced with CBAR) used for application recognition method on each device

☐ Device name 	Management IP	Active recognition method 	CBAR Readiness Status	CBAR Deployment Status
☐ C9800-CL	100.64.0.103	CBAR	 Enabled	Completed Re-Configure
☐ Cat9300-1	100.124.0.11	CBAR	 Enabled	Completed Re-Configure
☐ Cat9300-2	100.124.0.12	CBAR	 Enabled	Completed Re-Configure
☐ Fusion.mango.local	100.127.0.2	CBAR	 Enabled	Completed Re-Configure

Enabling CBAR to Manage Devices

- NBAR/CBAR configuration pushed to Switches

```
platform wdvavc serviceability
```

```
avc sd-service
```

```
segment AppRecognition
```

```
controller
```

```
address <Catalyst Center IPv4/IPv6 address>
```

```
destination-ports sensor-exporter 21730
```

```
dscp 16
```

```
source-interface Loopback0
```

```
transport application-updates https url-prefix sdavc
```

```
interface GigabitEthernet1/0/1
```

```
ip nbar protocol-discovery
```

```
interface GigabitEthernet1/0/2
```

```
ip nbar protocol-discovery
```

NBAR protocol discovery command applies to all ports by default; can selectively disable ports through “re-configure” link on Application Visibility dashboard

Enabling CBAR to Manage Devices



- Verifying CBAR Connection on Devices

```
Cat9300-2#show avc sd-service info summary
Status: CONNECTED
```

```
Device ID: Cat9300-2
Device segment name: AppRecognition
Device address: 100.124.0.12
Device OS version: 17.18.02
Device type: C9300-48U
```

Active controller:

```
Type      : Primary
Address   : 100.64.0.101
Status    : Connected
Version   : 4.8.0
```

```
Last connection: *19:48:12.000 UTC Sun Feb 5 2026
```

Active SDAVC import files:

```
Protocol pack:          Not loaded
Secondary protocol pack: Not loaded
Rules pack:             Not loaded
```

```
Cat9300-2#sh avc sd-service info summary
Status: CONNECTED
```

```
Device ID: Cat9300-2
Device segment name: AppRecognition
Device address: 100.124.0.12
Device OS version: 17.18.02
Device type: C9300-48U
```

Active controller:

```
Type      : Primary
Address   : 100.64.0.101
Status    : Connected
Version   : 4.8.0
```

```
Last connection: *19:51:14.000 UTC Sun Feb 5 2026
```

Active SDAVC import files:

```
Protocol pack:          Not loaded
Secondary protocol pack: PPKD_ALL-
SEGMENT_00af17b359b9f25a594e7ba3d18c42.pack
Rules pack:
pp_update_AppRecognition_a_v2_9e786e8b3cf3.pack
```

Moments later

Enabling CBAR to Manage Devices

- Updating Protocol Pack (Selective and Auto Update)

Filter

CBAR ⓘ

Application Telemetry ▾

Update Protocol Pack ▾ ⓘ

	Device name ▴ ▾	Management IP	Active re	Status	CBAR Deployment Status
☐	C9800-CL	100.64.0.103	CBAR		Completed Re-Configure
☒	Cat9300-1	100.124.0.11	CBAR		Completed Re-Configure
☒	Cat9300-2	100.124.0.12	CBAR		Completed Re-Configure
☐	Fusion.mango.local	100.127.0.2	CBAR	✔ Enabled	Completed Re-Configure

Update All Devices

Update Selected Devices

Update Selected Devices From File

☒ Auto Update

Include Selected Devices

Exclude Selected Devices

Enabling CBAR to Manage Devices

- Before Protocol Pack update

```
Cat9300-2#show ip nbar protocol-pack active
```

```
Active Protocol Pack:
```

```
  Name: Advanced Protocol Pack
```

```
  Version: 75.0
```

```
  Publisher: Cisco Systems Inc.
```

```
  NBAR Engine Version: 55
```

```
  State: Active
```

IOS-XE native NBAR protocol pack

```
  Name: Secondary Protocol Pack
```

```
  Version: 00a37dbdfccff7efa1d7df59278013
```

```
  Publisher: SD-AVC
```

```
  NBAR Engine Version: 1001
```

```
  Creation time: Thu Feb  5 19:34:22 UTC 2026
```

```
  NBAR PP level: 1
```

```
  File: flash:/sdavc/PPDK_ALL-SEGMENT_00af17b359b9f25a594e7ba3d18c42.pack
```

```
  State: Active
```

CBAR installed secondary protocol pack

Enabling CBAR to Manage Devices

- After Protocol Pack update through CBAR

```
Cat9300-2#show ip nbar protocol-pack active
```

```
Active Protocol Pack:
```

```
  Name:                Advanced Protocol Pack
```

```
  Version:             77.0
```

```
  Publisher:           Cisco Systems Inc.
```

```
  NBAR Engine Version: 55
```

```
  Creation time:       Tue Nov 25 13:56:59 UTC 2025
```

```
  File:                flash:/sdavc/pp-adv-cat9k-1718.1-55-77.0.0.pack
```

```
  State:               Active
```

IOS-XE protocol pack
updated through CBAR

```
  Name:                Secondary Protocol Pack
```

```
  Version:             00a37dbdfccff7efa1d7df59278013
```

```
  Publisher:           SD-AVC
```

```
  NBAR Engine Version: 1001
```

```
  Creation time:       Thu Feb  5 19:34:22 UTC 2026
```

```
  NBAR PP level:       1
```

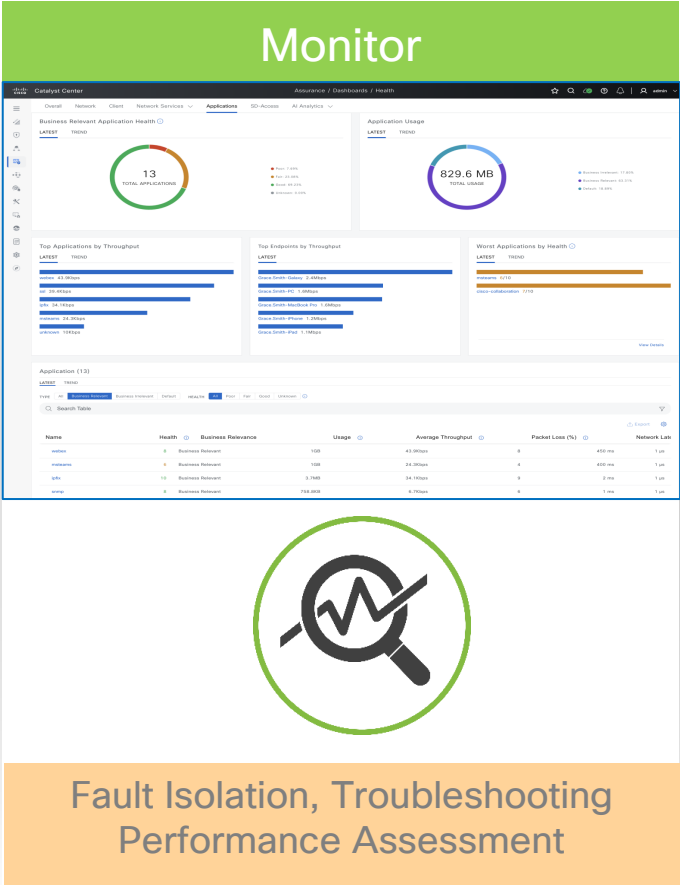
```
  File:                flash:/sdavc/PPDK_ALL-SEGMENT_00af17b359b9f25a594e7ba3d18c42.pack
```

```
  State:               Active
```

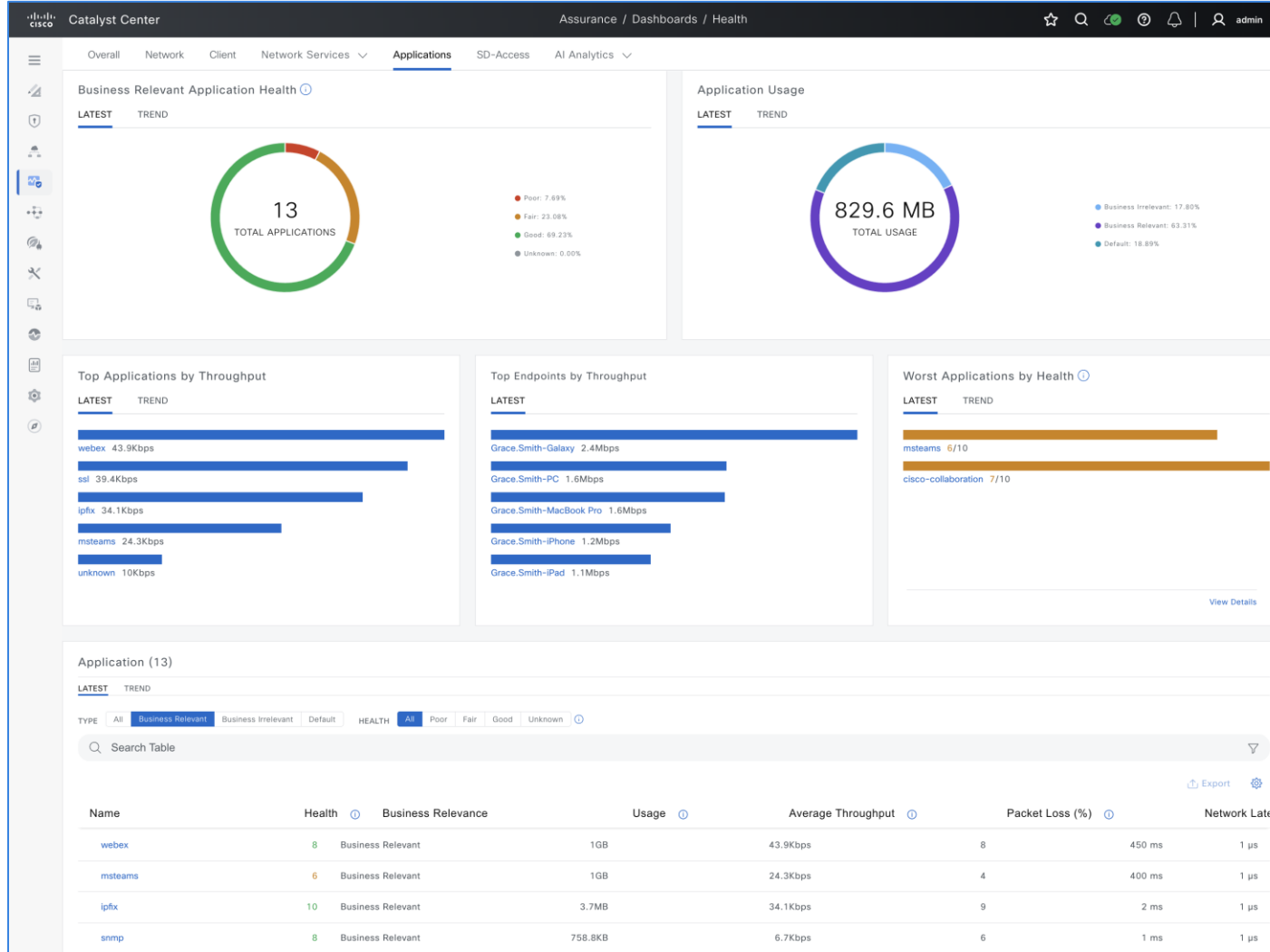
CBAR installed secondary protocol pack

Monitor Applications

Monitor Your Applications



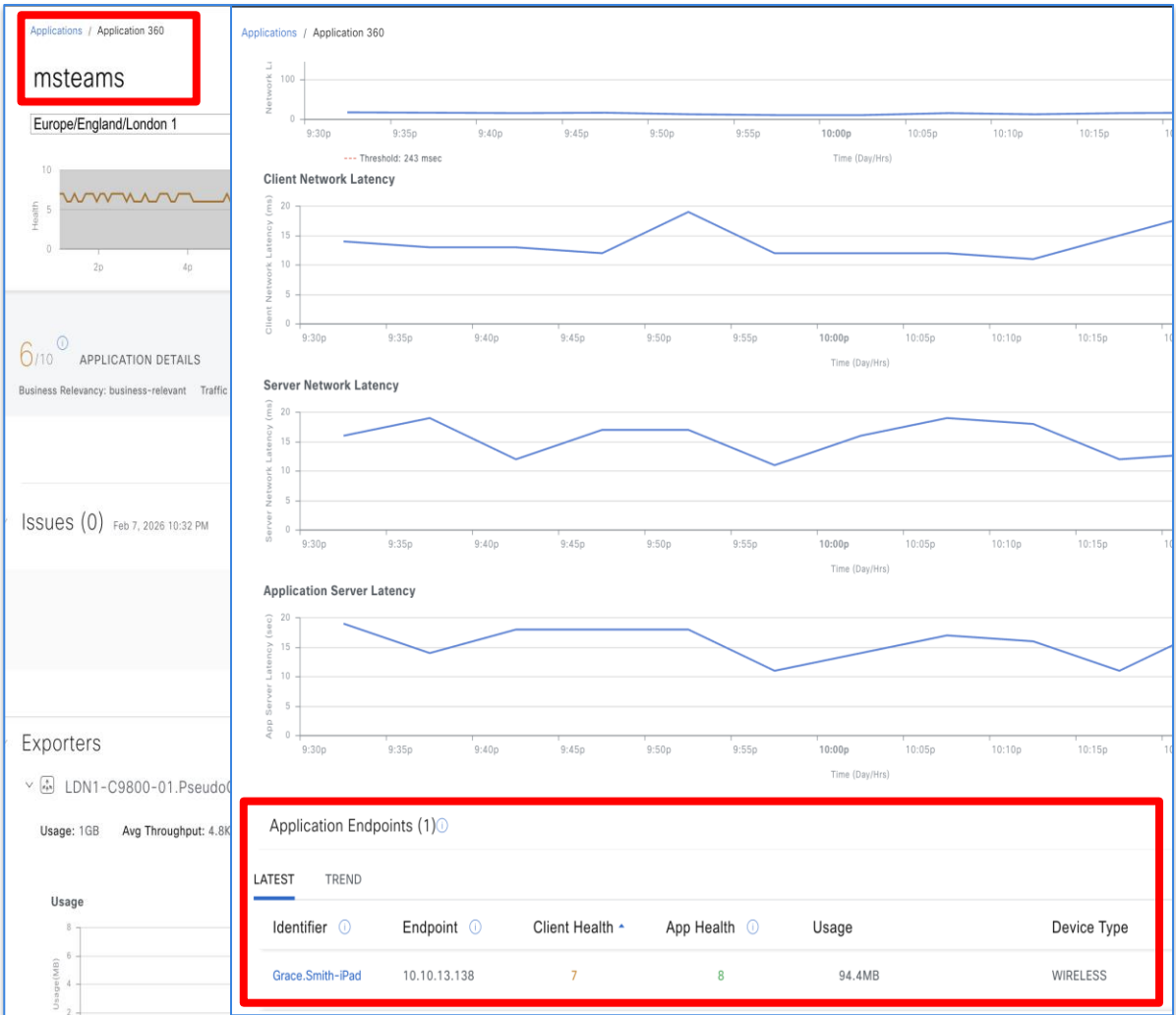
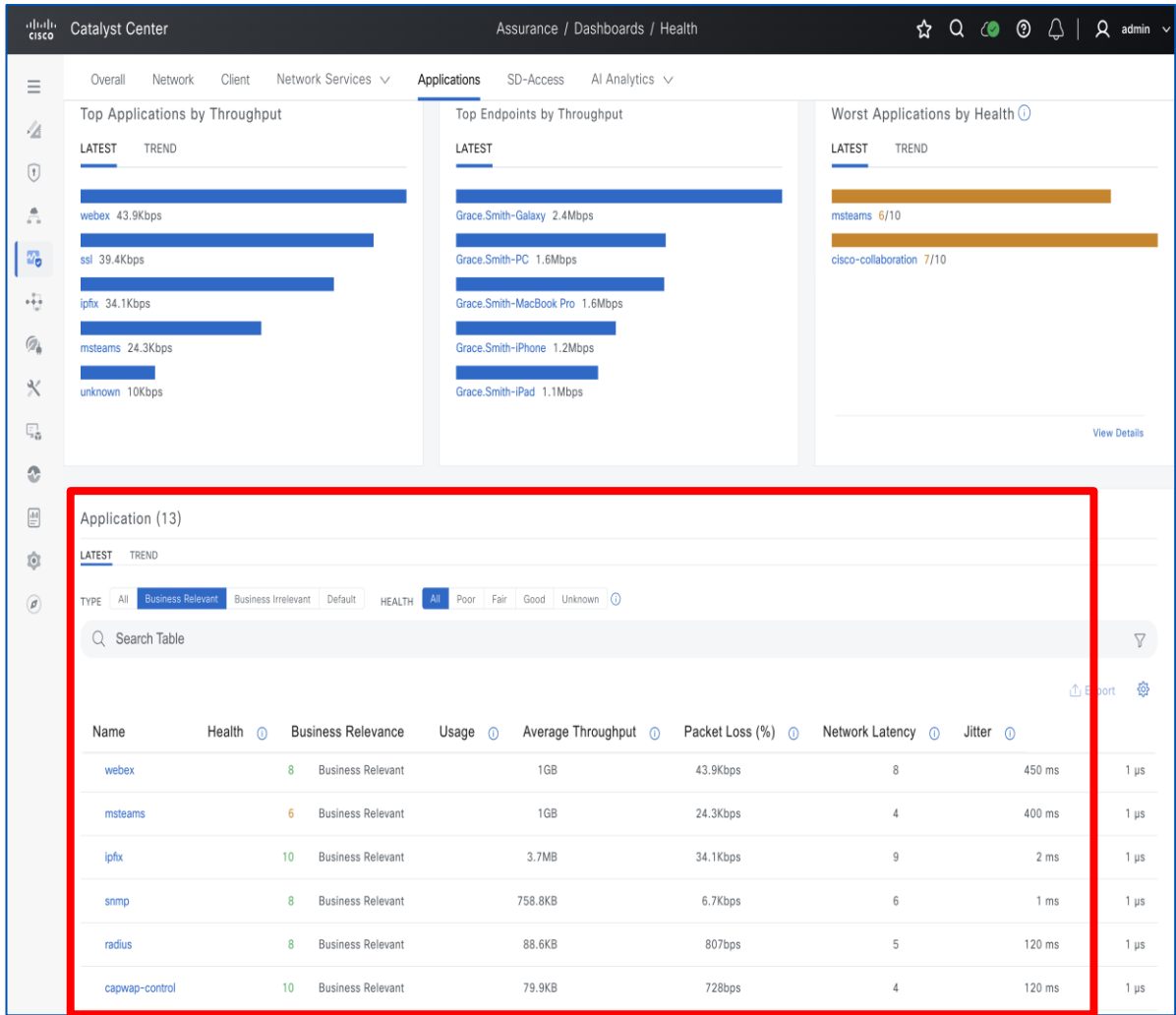
Catalyst Center Application Health



- Collects and tracks performance of key business applications
 - Granular to per application and per user/endpoint
- Integration with Webex and MS Teams for deep performance insights
- Correlate endpoint events with application health to reduce MTTR
- Integration with ThousandEyes to provide application health visibility beyond managed networks

Application Health on Catalyst Center

- Client level application health visibility



Application Telemetry Export to Catalyst Center

The screenshot shows the Cisco Catalyst Center web interface. The top navigation bar includes 'Design / Network Settings' and 'Telemetry'. The left sidebar shows a search bar and a navigation menu. The main content area is titled 'Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings when devices are assigned to a site or provisioned.' It includes a section for 'Application Visibility' with instructions on enabling NetFlow Application Telemetry and CBAR. A checkbox 'Enable by default on supported wired access devices' is highlighted in red. Below it, the radio button 'Use Catalyst Center as the Netflow Collector' is selected. The 'Wired Endpoint Data Collection' section is also visible.

- Application Telemetry provides visibility and health info via NetFlow export from network devices
- By default, App Telemetry not enabled on network devices
 - Telemetry export recommended at access layer (ports) to reduce data duplication
- Automatic App Telemetry can be set to enabled for Access switches when assigned to a Site under **Design -> Network Settings -> Telemetry**
 - Both NetFlow and NBAR/CBAR configs deployed automatically*

*Excludes switches onboarded through LAN Auto

Application Telemetry Export to Catalyst Center

- Switches only provide QUANTITATIVE (usage and throughput) insight for applications
- Routers and WLC provide QUANTITATIVE + QUALITATIVE (loss, jitter, delay) insight
- Application Telemetry configured on ACCESS mode ports (e.g. ports not configured for trunk or routed mode on switches) or Enterprise SSIDs only
 - Manually add keyword “lan” to interface description of desired interfaces or WLAN policy profiles to forcibly apply telemetry
 - If using “lan” keyword, ONLY ports or WLAN with keyword gets telemetry applied
- Support for fabric* and non-fabric networks
- Advantage License

*Some features not supported for fabric

Enabling Application Telemetry on Managed Devices

- App Telemetry enabled preferably via [Provision -> Application Visibility](#)

Overview

Network Devices Enablement

Applications 1519

Application Sets 28

CBAR Extensions

Site Devices 4 ⓘ

Device Family

AllRoutersSwitchesWireless ControllersTelemetry Appliance

Active Recognition Method

AllCBARNBARIP/PortNot Supported

CBAR Readiness

AllReadyNot readyEnabled

Telemetry Readiness

AllReadyNot readyEnabled

Filter

CBAR ⓘ

Application Telemetry ⓘ

Update Protocol Pack ⓘ

☒ Device name ⌵

Enable Application Telemetry

Disable Application Telemetry

Recognition method ⓘ

Application Telemetry Readiness Status

Application Telemetry Deployment Status

☒	C9800-CL	100.64.0.103	CBAR	👍 Ready	Not deployed
☒	Cat9300-1	100.124.0.11	CBAR	👍 Ready	Not deployed
☒	Cat9300-2	100.124.0.12	CBAR	👍 Ready	Not deployed
☒	Fusion.mango.local	100.127.0.2	CBAR	👍 Ready	Not deployed

Application Telemetry Orchestrated on Switches

- NetFlow configuration pushed to Access Switches (IPv4) – **Flow Record**

flow record dnacrecord

```
match ipv4 version
match ipv4 protocol
match application name
match connection client ipv4 address
match connection server ipv4 address
match connection server transport port
match flow observation point
collect timestamp absolute first
collect timestamp absolute last
collect flow direction
collect connection initiator
collect connection client counter packets long
collect connection client counter bytes network long
collect connection server counter packets long
collect connection server counter bytes network long
collect connection new-connections
collect datalink mac source address input
```

flow record dnacrecord_dns

```
match ipv4 version
match ipv4 protocol
match connection client ipv4 address
match connection server ipv4 address
match flow observation point
match application dns qtype
match application dns rcode
collect datalink mac source address input
collect timestamp absolute first
collect timestamp absolute last
collect connection client counter packets long
collect connection client counter bytes network long
collect connection server counter packets long
collect connection server counter bytes network long
collect application dns requests
collect application dns delay response sum
```

Application Telemetry Orchestrated on Switches



- NetFlow configuration pushed to Access Switches (IPv4) – **Flow Exporter and Monitor**

flow exporter dnacexporter

```
destination <Catalyst Center IPv4 address>
source <Mgmt-Interface-IP>
transport udp 6007
export-protocol ipfix
option interface-table timeout 300
option vrf-table timeout 300
option sampler-table
option application-table timeout 300
option application-attributes timeout 300
```

flow monitor dnacmonitor

```
exporter dnacexporter
cache timeout inactive 10
cache timeout active 60
record dnacrecord
```

flow monitor dnacmonitor_dns

```
exporter dnacexporter
cache timeout inactive 10
cache timeout active 60
record dnacrecord_dns
```

Application Telemetry Orchestrated on Switches

- NetFlow configuration pushed to Access Switches (IPv4) – **Interface Monitoring**

```
interface GigabitEthernet1/0/1
```

```
ip flow monitor dnacmonitor input
ip flow monitor dnacmonitor_dns input
ip flow monitor dnacmonitor output
ip flow monitor dnacmonitor_dns output
```

```
interface GigabitEthernet1/1/1
```

```
description LAN
ip flow monitor dnacmonitor input
ip flow monitor dnacmonitor_dns input
ip flow monitor dnacmonitor output
ip flow monitor dnacmonitor_dns output
```

keyword “lan” can be manually added to the interface description to forcefully apply NetFlow monitor to an interface not configured with “switchport mode access”

CAUTION: interfaces w/o “lan” keyword will NOT get NetFlow monitor applied, that otherwise would have automatically been configured

Application Telemetry Orchestrated on C9800 WLC



- NetFlow configuration pushed to standalone C9800 (IPv4) – **Flow Record and Monitor**
- **SDA or Flex Wireless**

```
flow monitor avc_ipv4_assurance_v9
```

```
exporter avc_exporter_v9  
cache timeout active 60  
record wireless avc ipv4 assurance
```

```
flow monitor avc_ipv4_assurance_rtp_v9
```

```
exporter avc_exporter_v9  
cache timeout active 60  
record wireless avc ipv4 assurance-rtp
```

```
wireless profile policy <POLICY-NAME>
```

```
ipv4 flow monitor avc_ipv4_assurance_v9 input  
ipv4 flow monitor avc_ipv4_assurance_rtp_v9 input  
ipv4 flow monitor avc_ipv4_assurance_v9 output  
ipv4 flow monitor avc_ipv4_assurance_rtp_v9 output
```

Application Telemetry Orchestrated on C9800 WLC



- NetFlow configuration pushed to standalone C9800 (IPv4) – **Flow Record and Monitor**
- **Central Switching (Non-Fabric) Wireless**

```
flow monitor avc_ipv4_assurance
```

```
exporter avc_exporter  
exporter avc_local_exporter  
cache timeout active 60  
record wireless avc ipv4 assurance
```

```
flow monitor avc_ipv4_assurance_rtp
```

```
exporter avc_exporter  
cache timeout active 60  
record wireless avc ipv4 assurance-rtp
```

```
flow monitor avc_ipv4_assurance_dns
```

```
exporter avc_exporter  
cache timeout active 60  
record wireless avc ipv4 assurance-dns
```

```
wireless profile policy <POLICY-NAME>
```

```
ipv4 flow monitor avc_ipv4_assurance input  
ipv4 flow monitor avc_ipv4_assurance_rtp input  
ipv4 flow monitor avc_ipv4_assurance_dns input  
ipv4 flow monitor avc_ipv4_assurance output  
ipv4 flow monitor avc_ipv4_assurance_rtp output  
ipv4 flow monitor avc_ipv4_assurance_dns output
```

Application Telemetry Orchestrated on C9800 WLC



- NetFlow configuration pushed to standalone C9800 (IPv4) – **Flow Exporter**

flow exporter avc_exporter

```
destination <Catalyst Center IPv4 Address>  
source <Mgmt-Interface-IP>  
transport udp 6007  
export-protocol ipfix  
option vrf-table timeout 300  
option ssid-table timeout 300  
option application-table timeout 300  
option application-attributes timeout 300
```

flow exporter avc_local_exporter

```
destination local wlc
```

Local SSID Telemetry selected

flow exporter avc_exporter_v9

```
destination <Catalyst Center IPv4 Address>  
source <Mgmt-Interface-IP>  
transport udp 6007  
option vrf-table timeout 300  
option ssid-table timeout 300  
option application-table timeout 300  
option application-attributes timeout 300
```

SDA/Flex SSID Telemetry selected

Application Telemetry Orchestrated Router

- Performance monitor configuration applies to both IPv4 and IPv6 traffic

```
performance monitor context tesseract profile application-assurance
```

```
exporter destination <Catalyst Center IPv4/IPv6 address> source <Mgmt-Interface-IP> transport udp port 6007  
traffic-monitor assurance-monitor  
traffic-monitor assurance-rtp-monitor  
traffic-monitor assurance-dns-monitor
```

```
interface GigabitEthernet0/0/1
```

```
description LAN Upstream to Enterprise  
ip address 100.124.126.1 255.255.255.252  
performance monitor context tesseract
```

```
interface GigabitEthernet0/0/2
```

```
description Downstream to Access Network lan  
ip address 100.124.126.5 255.255.255.252  
performance monitor context tesseract
```

Interface must be configured with IP address to have performance monitor applied

When keyword “LAN” is used, interfaces w/o keyword would NOT get App Telemetry configuration (that otherwise would have automatically been configured).

Control Applications

Control Your Applications

Control

Catalyst Center

Policy / Application QoS

Application Policies

Queueing Profiles

Application QoS Policy Name*

CVD-QoS

Wireless

Wireless

+ Application Registry

Site Scope: 2 Sites Queueing Profiles CVD,QUEUING_PROFILE Service Provider Profiles 1 Profiles

Find Application / Application Set

Business Relevant (16)

Default (6)

Business Irrelevant (6)

authentication-services

18 applications

X

file-sharing

12 applications

X

consumer-browsing

128 applications

X

backup-and-storage

14 applications

X

general-browsing

13 applications

X

consumer-file-sharing

40 applications

X

collaboration-apps

70 applications

X

general-media

12 applications

X

consumer-gaming

16 applications

X

database-apps

34 applications

X

general-misc

488 applications

X

consumer-media

107 applications

X

desktop-virtualization-apps

22 applications

X

software-updates

16 applications

X

consumer-misc

11 applications

X

email

29 applications

X

streaming

25 applications

X

consumer-social-networking

20 applications

X



Prioritized Applications, Bandwidth Management

IOS-XE Configuration for QoS – Partial Example

Traditional QoS Config

```
ip access-list extended qos-CALL-SIGNALING
permit udp 10.0.0.0 0.15.255.255 any range 5061 5063
permit tcp 10.0.0.0 0.15.255.255 any range 5061 5063
permit tcp 10.0.0.0 0.15.255.255 any eq 5269
permit tcp 10.0.0.0 0.15.255.255 any eq 53
permit udp 10.0.0.0 0.15.255.255 any eq 3478
```

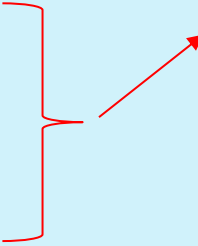
```
class-map match-any qos-CALL-SIGNALING
match access-group name qos-CALL-SIGNALING
```

```
policy-map qos-ACCESS
class qos-CALL-SIGNALING
set dscp ef
```

App Aware QoS Config

```
class-map match-any qos-CALL-SIGNALING
match protocol ms-lync

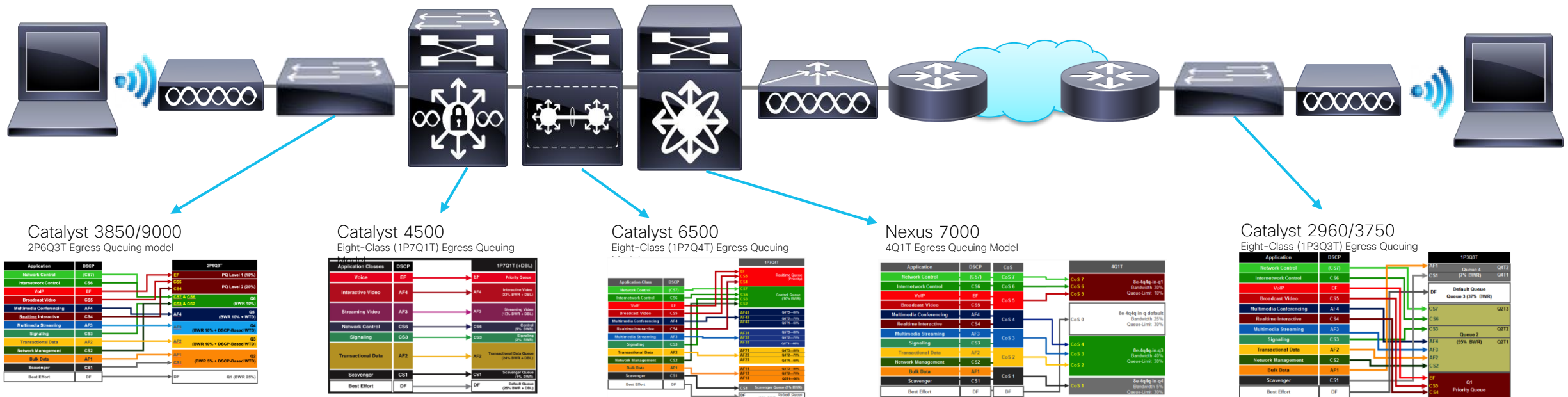
policy-map qos-ACCESS
class qos-CALL-SIGNALING
set dscp ef
```



QoS configuration can involve hundreds of lines of configuration on EACH device, even with App Aware QoS config

Different Platforms, Different Capabilities

- Configs need to account for different hardware capability on each box



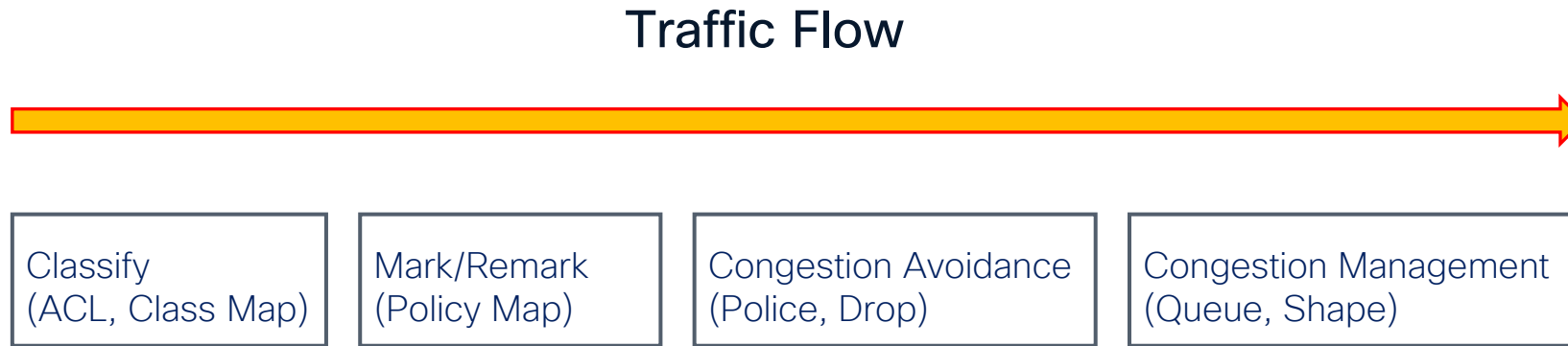
Managing Enterprise-wide QoS via Catalyst Center

The screenshot shows the Cisco Catalyst Center interface for configuring an Application QoS Policy. The page title is "Policy / Application QoS". The "Application Policies" tab is selected, and the "Queuing Profiles" sub-tab is active. The "Application QoS Policy Name" is set to "CVD-QoS". The "Wired" radio button is selected, and the "Wireless" radio button is unselected. The "Application Registry" link is visible. The "Site Scope" is set to "2 Sites". The "Queuing Profiles" are set to "CVD_QUEUING_PROFILE". The "Service Provider Profiles" are set to "1 Profiles". A search bar "Q Find Application / Application Set" is present. The main content area displays a table of applications categorized into three groups: Business Relevant (16), Default (6), and Business Irrelevant (6). Each application is shown with its name, the number of applications it covers, and a checkbox to select it.

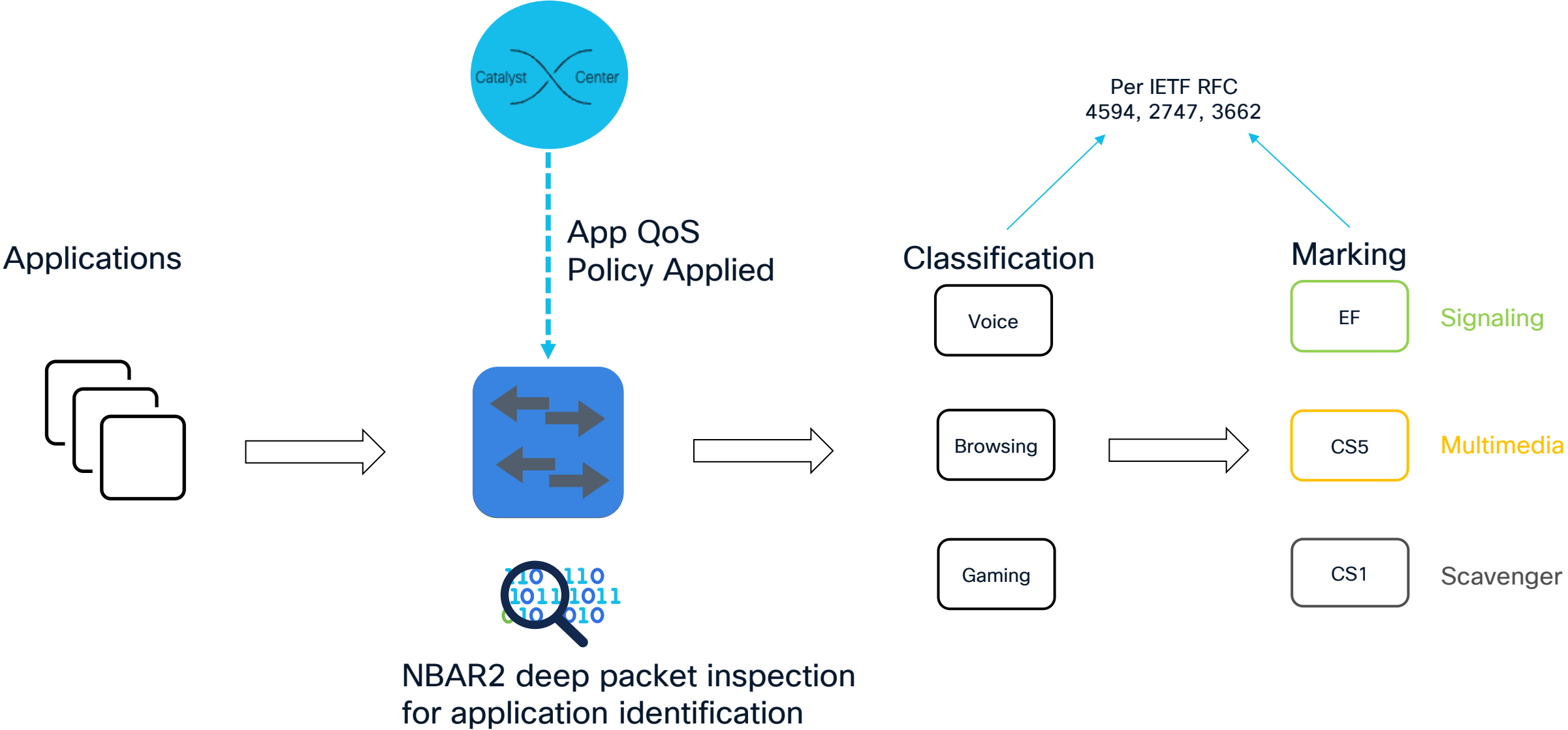
Business Relevant (16)	Default (6)	Business Irrelevant (6)
☒ authentication-services 39 applications	☒ file-sharing 32 applications	☒ consumer-browsing 226 applications
☒ backup-and-storage 14 applications	☒ general-browsing 13 applications	☒ consumer-file-sharing 40 applications
☒ collaboration-apps 70 applications	☒ general-media 12 applications	☒ consumer-gaming 15 applications
☒ database-apps 34 applications	☒ general-misc 498 applications	☒ consumer-media 107 applications
☒ desktop-virtualization-apps 22 applications	☒ software-updates 16 applications	☒ consumer-misc 11 applications
☒ email 29 applications	☒ tunneling 25 applications	☒ consumer-social-networking 20 applications

- Application QoS Policy has built-in QoS models tailored for all supported devices, e.g.
 - Cat9K: 2P6Q3T
 - Cat6500: 1P7Q4T
- Consistent end-to-end QoS policies across LAN, WAN, and WLAN to optimize treatment of business relevant applications
- Orchestration engine uses **VALIDATED** industry-standard best practices for QoS deployment
- Complex QoS configurations simplified through click-and-drag

General QoS Processing on Devices



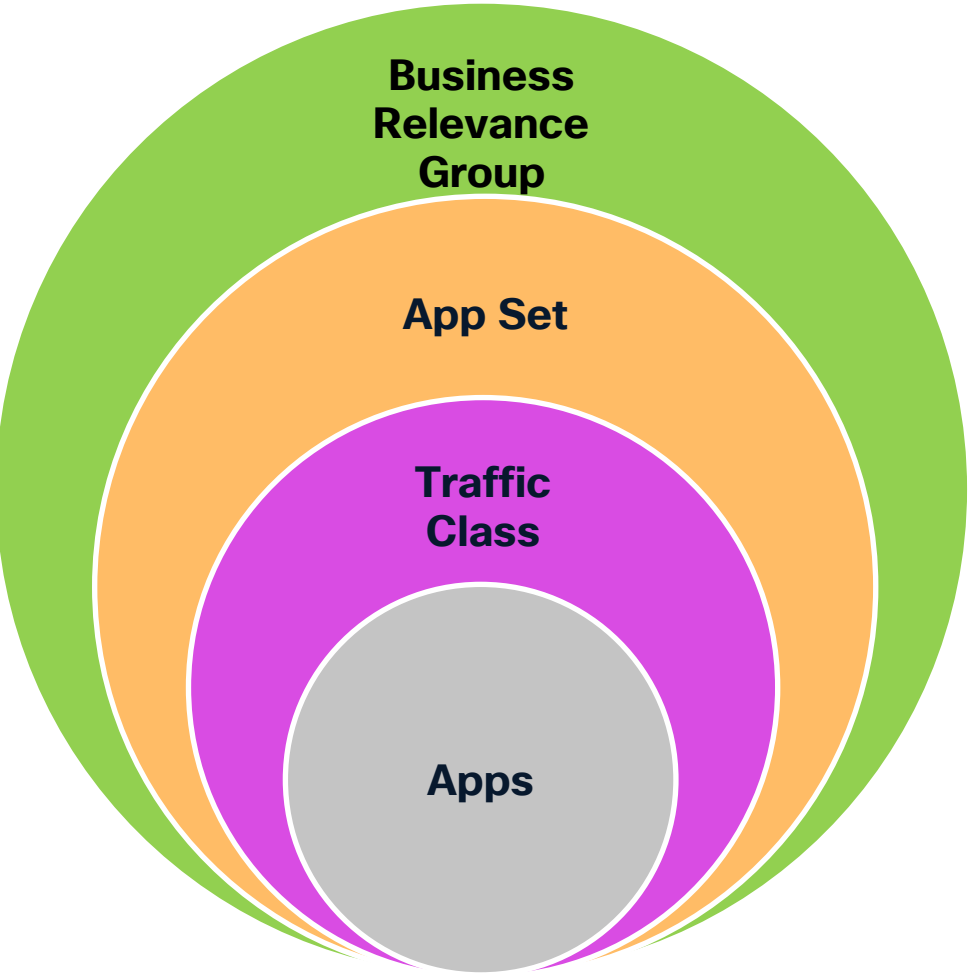
Classification and Marking Example



Application QoS Policy Components

NBAR/CBAR	Traffic Class
• Advanced NBAR2 engine inspects application type for incoming traffic at the application layer; CBAR enhances NBAR app recognition ability • Application QoS Policy uses protocol/attribute match statements per class-map to match on application traffic	• Every app categorized into one of 12 traffic classes, e.g. Cisco-IP-Camera assigned to Broadcast Video TC, MS-Stream assigned to Real Time Interactive; other classes include Network Control, Scavenger, Default • Bandwidth % and DSCP values apply to TC
Application Set	Business Relevance Groups
• Grouping of apps with similar network traffic needs (even if different TC), e.g. both Cisco-IP-Camera and MS-Stream grouped into Streaming-Media App Set • Catalyst Center has 28 App Sets by default; can add more with custom apps • Apps can be moved b/w different Sets	• 3 business-relevance groups (Relevant, Default, Irrelevant) • Each App Set categorized into one business-relevance group • Can move each App Set to different group based on business and operation needs

Application Association with Business Relevance



Cat9300-2#show ip nbar attribute business-relevance business-relevant application-set network-control	
aodv	AODV
at-rtmp	AppleTalk Routing Maintenance
aurp	AppleTalk Update-Based Routing Pro.
bgmp	BGMP
bgp	Border Gateway Protocol
capwap-control	Control And Provisioning of Wireless Access Points Control Protocol
cisco-controller	Cisco Network Controller
cisco-meraki	Cisco Meraki
cisco-sd-avc	Cisco software-defined AVC (SD-AVC)
cisco-tdp	Cisco TDP
dwr	dwr
egp	Exterior Gateway Protocol
eigrp	Enhanced Interior Gateway Routing Protocol
gacp	Gateway Access Control Protocol

Business Relevant – Network Control

Cat9300-2#show ip nbar attribute business-relevance default application-set file-sharing	
activesync	Microsoft Activesync protocol mobile data synchronization based on HTTP
bftp	Background File Transfer Program
binary-over-http	Binary traffic over HTTP
cifs	Common Internet File System
cvsup	Cvsup
fatserver	Fatmen Server
fix	Financial Information eXchange Protocol
ftp	File Transfer Protocol
ftp-agent	FTP Software Agent System
ftp-data	File Transfer Protocol, Data part only
ftps-data	Secure FTP (File Transfer Protocol) Data
gridftp	File Transfer Protocol over the Grid
gsiftp	GSI FTP
mftp	mftp

Default – File Sharing

Cat9300-2#show ip nbar attribute business-relevance business-irrelevance application-set consumer-browsing	
4chan	4chan - Website that hosts found images and discussions on them.
58-city	58 City - Classified information about 58 cities in China.
abc-news	ABC - Web Portal for television network.
accuweather	AccuWeather - Weather forecasting website.
adcash	Adcash - Advertising network.
addthis	AddThis - Social bookmarking service.
adweek	Adweek - Marketing, Media and advertising news.
airbnb	Airbnb - Online accommodation rental service.
akamai	Akamai Technologies
allrecipes	AllRecipes - Recipes and cooking guide.
amazon	A collection of services offered by Amazon.
ameba	Ameba - Japanese blogging and social networking website.
american-express	American Express - Financial services company.
ancestry-com	Ancestry.com - Online family history resource.

Business Irrelevant – Consumer Browsing

Business Relevance of Apps **Before** QoS Policy Deployed

- Devices with only CBAR enabled, no QoS policy deployed
- **Catalyst Center 3.1.6 and below**

Overview Network Devices Enablement Applications 1520 **Application Sets 29** CBAR Ex

Find Application / Application Set

Show All

All # A - F G - K L - P Q - T U - Z

> consumer-media 107 applications

> consumer-misc 11 applications

> consumer-social-netwo... 11 applications

> data 34 applications

> enter 20 applications

> gene 12 applications

☒ CustomApp-Set 1 applications

Find Application

☐ 0 Selected ⓘ

☐ ★ CustomApp-31

Default: Business Irrelevant

Custom Apps
default to Business
Relevant on device

```
Cat9300#show ip nbar protocol-attribute CustomApp-31
Protocol Name : CustomApp-31
  encrypted : encrypted-yes
  tunnel : tunnel-yes
  category : browsing
  sub-category : enterprise-transactional-apps
  application-group : other
  p2p-technology : p2p-tech-no
  traffic-class : real-time-interactive
  business-relevance : business-relevant
  application-set : general-browsing
  application-family : web
```

Business Relevance of Apps **Before** QoS Policy Deployed

- Devices with only CBAR enabled, no QoS policy deployed
- **Catalyst Center 3.2+**

The screenshot shows the 'Applications' page in Catalyst Center. The 'Application Sets' tab is selected and highlighted with a red box, showing 29 sets. Below the tabs, there is a search bar and a 'Show' dropdown set to 'All'. A list of application sets is displayed, including 'consumer-media' (107 applications), 'consumer-misc' (11 applications), and 'consumer-social-netwo...' (34 applications). A red box highlights the 'Default:Business Irrelevant' status for the 'consumer-media' set. Below this, a search bar for 'Find Application' is shown, and a list of applications is displayed. One application, 'CustomApp-32', is highlighted with a red box and a star icon.

Matches

```
Cat9300-2#show ip nbar protocol-attribute CustomApp-32
Protocol Name : CustomApp-31
encrypted : encrypted-yes
tunnel : tunnel-yes
category : browsing
sub-category : enterprise-transactional-apps
application-group : other
p2p-technology : p2p-tech-no
traffic-class : real-time-interactive
business-relevance : business-irrelevant
application-set : general-browsing
application-family : web
```

Application Treatment Per Business Relevance Group

Business Relevant

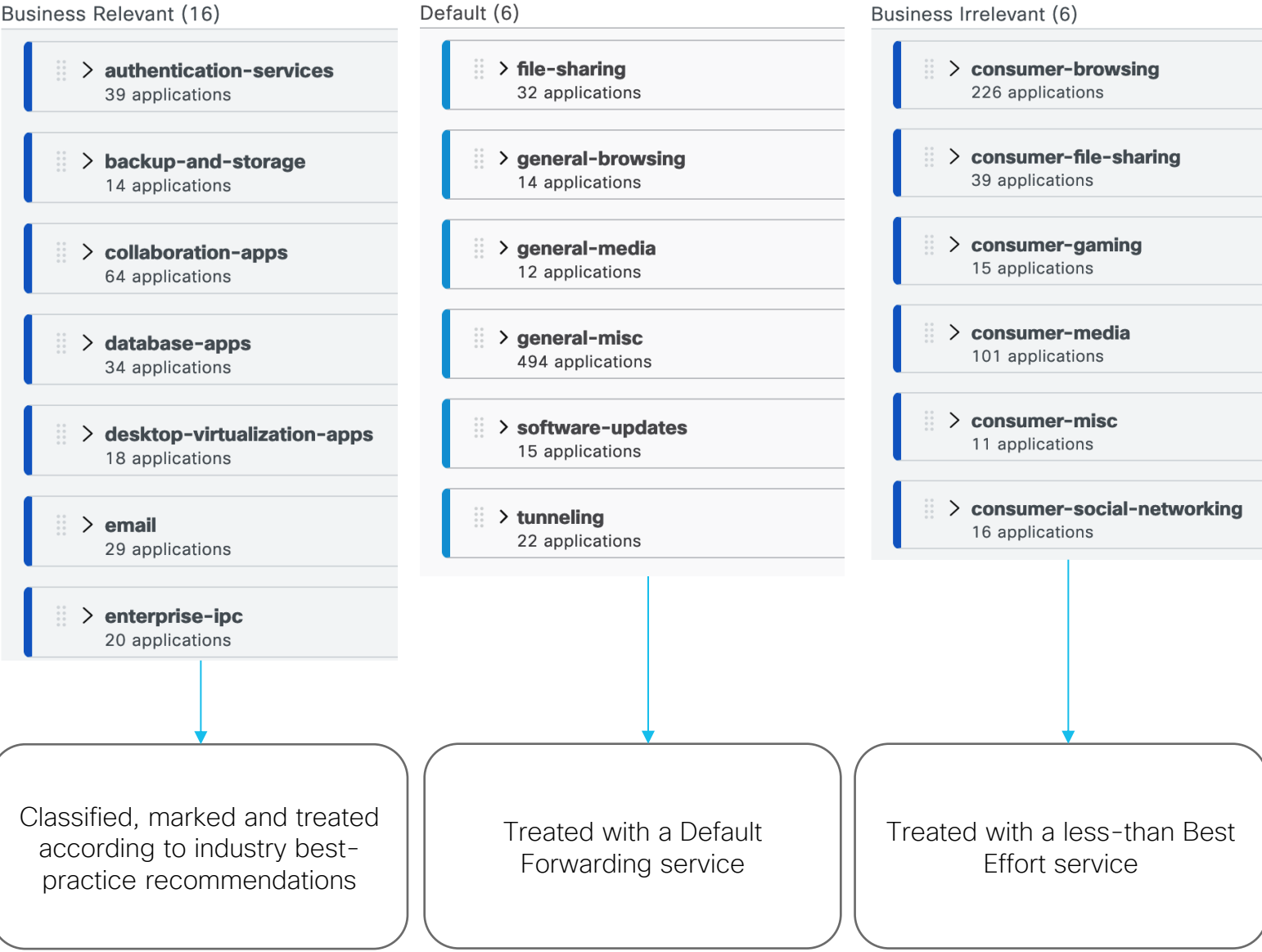
Application that directly support Business Objectives

Default

Applications that may support Business Objectives

Business Irrelevant

Applications that do not support Business Objectives



Application Treatment Per Business Relevance Group

Relevant

Default Irrelevant

Application Set	Traffic Class	DSCP Marking	Queuing and Dropping	Application Examples
Collaboration apps	VoIP Telephony	EF	Priority Queue (PQ)	Cisco IP Phones (G.711,G.729)
Streaming-media	Broadcast Video	CS5	(Optional) PQ	Cisco IP Video Surveillance / Cisco Enterprise TV
Collaboration apps	Real-Time Interactive	CS4	(Optional) PQ	Cisco Telepresence
General-media	Multimedia Conferencing	AF41	BW Queue + DSCP WRED	Cisco Jabber, Cisco WebEx
Consumer-media	Multimedia Streaming	AF31	BW Queue + DSCP WRED	Cisco Digital Media System (VoDs)
Network Control	Network Control	CS6	BW Queue	EIGRP, OSPF, BGP, HSRP, IKE
Signaling	Signaling	CS3	BW Queue	SCCP, SIP, H.323
Authentication-Services	Ops/ Admin/ Mgmt (OAM)	CS2	BW Queue	SNMP, SSH, Syslog
Consumer-browsing	Transactional Data	AF21	BW Queue + DSCP WRED	ERP Apps, CRM Apps, Database Apps
Backup and Storage	Bulk Data	AF11	BW Queue + DSCP WRED	E-mail, FTP, Backup Apps, Content Distribution
General-browsing	Default Forwarding	DF	Default Queue + RED	Default Class
General-misc	Scavenger	CS1	Min BW Queue (Deferential)	YouTube, Netflix, iTunes, BitTorrent, Xbox Live

Note: An Application Set may map to multiple Traffic Classes, e.g. Collaboration apps

CVD Queuing Profile - Marking

- Cisco Validated Design-based Profile is used by default for queuing policy
- DSCP marked traffic is associated to each queue as per the Traffic Class

DSCP per Class can be customized as needed

Business Relevant Voice 46 (EF) ▼	Business Relevant Signaling 24 (CS3) ▼
Business Relevant Broadcast Video 40 (CS5) ▼	Business Relevant OAM 16 (CS2) ▼
Business Relevant Real-Time Interactive 32 (CS4) ▼	Business Relevant Transactional Data 18 (AF21) ▼
Business Relevant Multimedia Conferencing 34 (AF41) ▼	Business Relevant Bulk Data 10 (AF11) ▼
Business Relevant Multimedia Streaming 26 (AF31) ▼	Business Irrelevant (Scavenger) 8 (CS1) ▼
Business Relevant Network Control 48 (CS6) ▼	Default (Best Effort) 0 (Best Effort) ▼

Class-map deployed on Device

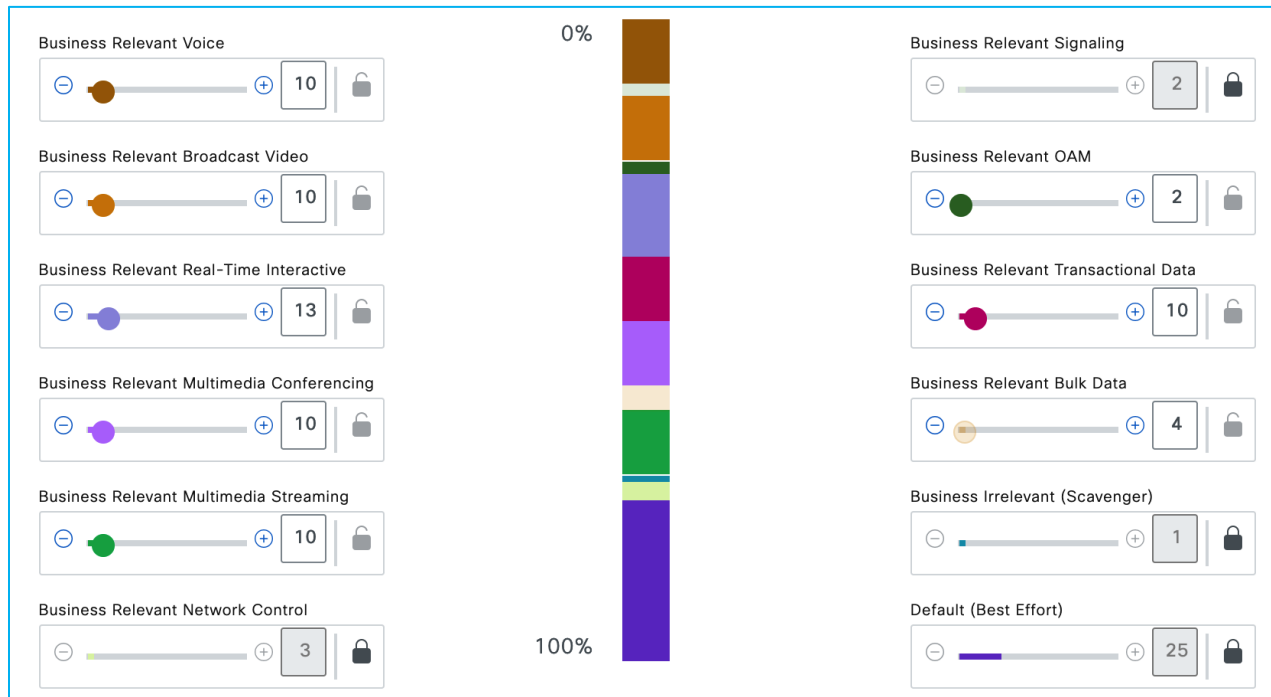
```
class-map match-any DNA-EZQ05_2P6Q3T_9K#BULK-DATA
match dscp cs1
match dscp af12
match dscp af13
match dscp af11
class-map match-any DNA-EZQ05_2P6Q3T_9K#CONTROL-PLANE
match dscp cs3
match dscp cs2
match dscp cs7
match dscp cs6
class-map match-any DNA-EZQ05_2P6Q3T_9K#MULTIMEDIA-CONFERENCING
match dscp af43
match dscp af41
match dscp af42
class-map match-any DNA-EZQ05_2P6Q3T_9K#VIDEO-PQ2
match dscp cs5
match dscp cs4
class-map match-any DNA-EZQ05_2P6Q3T_9K#VOICE-PQ1
match dscp ef
class-map match-any DNA-EZQ05_2P6Q3T_9K#TRANSACTIONAL-DATA
match dscp af23
match dscp af21
match dscp af22
class-map match-any DNA-EZQ05_2P6Q3T_9K#MULTIMEDIA-STREAMING
match dscp af32
match dscp af33
match dscp af31
```

QoS CVD: www.cisco.com/c/en/us/td/docs/solutions/CVD/Dec2017/APIC-EM-EasyQoS-DesignGuide-Dec2017.html

CVD Queuing Profile – Bandwidth Allocation

- Cisco Validated Design-based Profile is used by default for bandwidth allocation
- Traffic is policed on certain classes and DSCP based WRED is applied on data and default classes

Bandwidth per Class can be customized as needed



Policy Map deployed on Device

```
Policy Map DNA-dscp#APIC_Q05_Q_OUT
Class DNA-EZQ05_2P6Q3T_9K#VOICE-PQ1
  priority level 1
  police rate percent 10
  conform-action transmit
  exceed-action drop
  queue-buffers ratio 15
Class DNA-EZQ05_2P6Q3T_9K#VIDEO-PQ2
  priority level 2
  police rate percent 23
  conform-action transmit
  exceed-action drop
  queue-buffers ratio 10
Class DNA-EZQ05_2P6Q3T_9K#CONTROL-PLANE
  bandwidth remaining 10 (%)
  queue-buffers ratio 10
Class DNA-EZQ05_2P6Q3T_9K#MULTIMEDIA-CONFERENCING
  bandwidth remaining 15 (%)
  queue-buffers ratio 10
  queue-limit dscp af41 percent 100
  queue-limit dscp af42 percent 90
  queue-limit dscp af43 percent 80
Class DNA-EZQ05_2P6Q3T_9K#MULTIMEDIA-STREAMING
  bandwidth remaining 15 (%)
  queue-buffers ratio 10
  queue-limit dscp af32 percent 90
  queue-limit dscp af33 percent 80
Class DNA-EZQ05_2P6Q3T_9K#TRANSACTIONAL-DATA
  bandwidth remaining 15 (%)
  queue-buffers ratio 10
  percent-based wred
```

dscp	min-threshold	max-threshold
------	---------------	---------------

af21 (18)	80	100
af22 (20)	70	100
af23 (22)	60	100
default (0)	-	-

```
Class DNA-EZQ05_2P6Q3T_9K#BULK-DATA
  bandwidth remaining 7 (%)
  queue-buffers ratio 10
  percent-based wred
```

dscp	min-threshold	max-threshold
------	---------------	---------------

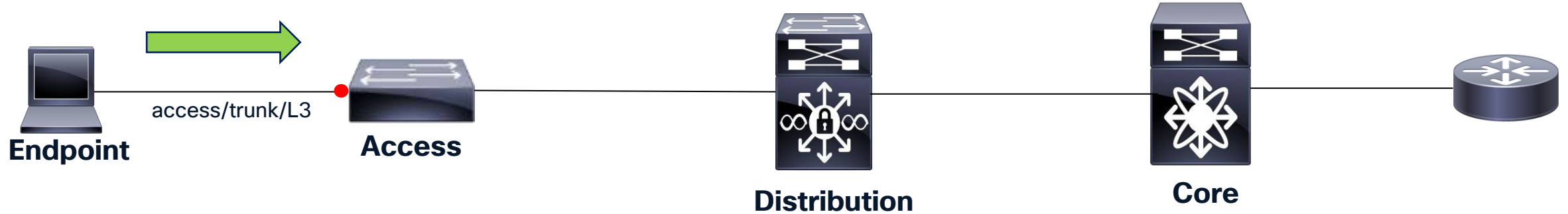
cs1 (8)	60	100
af11 (10)	80	100
af12 (12)	70	100
af13 (14)	60	100
default (0)	-	-

```
Class class-default
  bandwidth remaining 38 (%)
  queue-buffers ratio 25
  percent-based wred
```

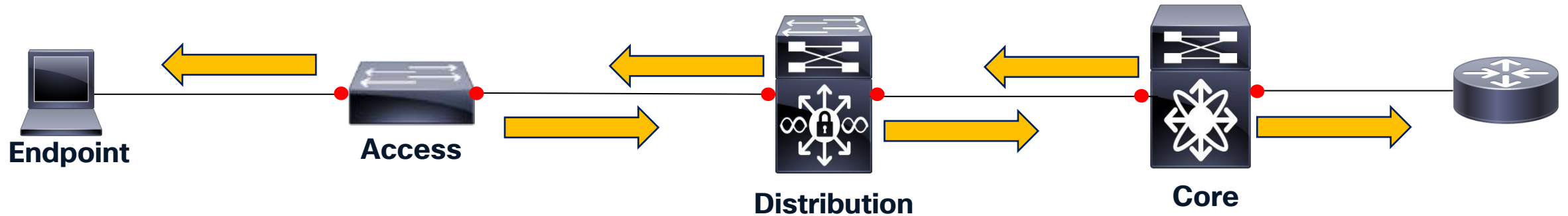
dscp	min-threshold	max-threshold
default (0)	80	100

WRED

Switch Device Role on Catalyst Center Matters

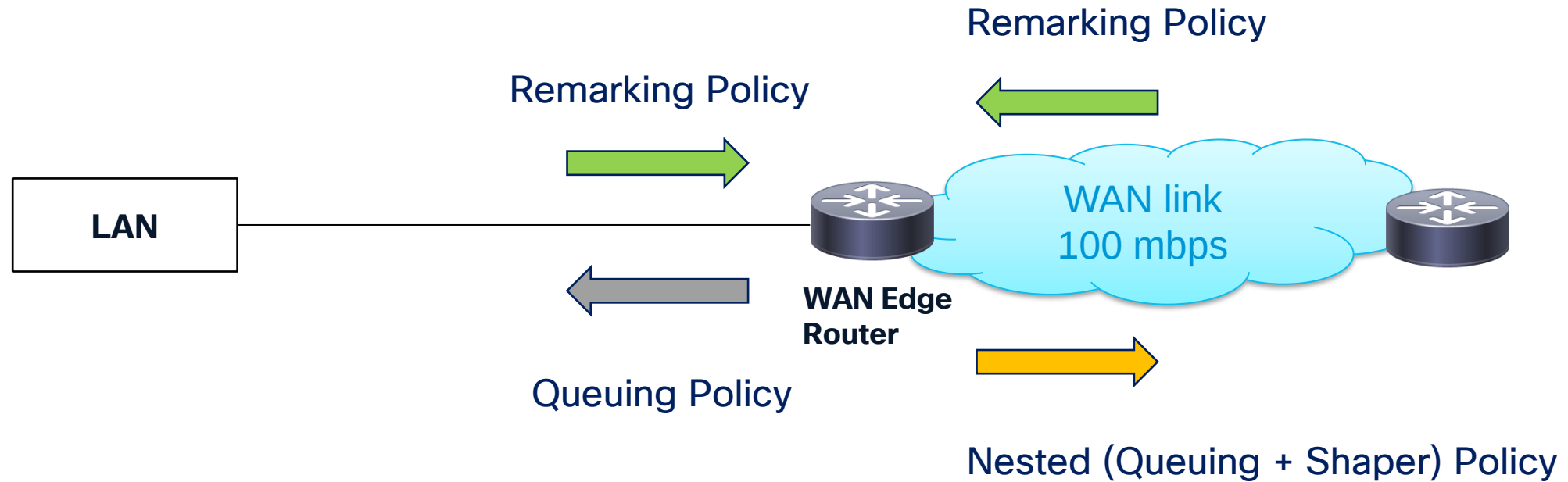


Marking is applied only on ingress on Access device



Queuing applied to egress on Access, Distribution, Core devices

QoS on WAN Routers



SP Profile

- Defines queuing model (4,5,6 or 8 Class) for WAN interface
- Profile maps each class into sets of DSCP values and Bandwidth percentage

Sub-line Rate

- Bandwidth provided by Service Provider
- Nested queuing policy with shaper configured per specified sub-line rate

Traffic Remarketing

- 12 Class Model return traffic from WAN remarked, mapped and queued into specified model in SP
- NBAR based re-marketing policy applied ingress

Mapping Traffic Classes to SP Service Model

- 12 Traffic Classes mapped into specified service model of Service Provider (SP) Profile

You can create a service provider (SP) profile that defines the class of service for a particular WAN provider. class, 6-class, and 8-class service models.

Profile Name*
Internet-Provider

WAN Provider*
ISP

Model*
4 Class

Find Profile

Internet-Provider

Class Name	DSCP	SP Bandwidth %	Queuing Bandwidth %	Admitted Traffic
Voice(Priority)	46 (EF)	10 %	10 %	voip_telephony
CLASS1 DATA	26 (AF31)	44 %	10 %	multimedia_streaming
			10 %	broadcast_video
			14 %	real_time_interactive
			10 %	multimedia_conferencing
CLASS2 DATA	18 (AF21)	25 %	5 %	bulk_data
			3 %	signaling
			3 %	ops_admin_mgmt
			14 %	transactional_data
Default	0 (Best Effo...	31 %	1 %	scavenger
			27 %	best_effort
			3 %	network_control ⓘ

Bandwidth % usage ⓘ

Priority(10%)+100%

Priority(10%)+100%

Specified Service Model

12 Traffic Classes

DSCP and Bandwidth of Service Model can be customized when adding new QoS Policy

Deploying Wired Application QoS Policy

- Add new wired policy under [Policy](#) -> [Application QoS](#) -> [Application Policies](#)

Cisco Catalyst Center

Policy / Application QoS

Application Policies

Queuing Profiles

☐ Deploy by default on wired devices ⓘ

As of: Feb 8, 2026 7:52 PM [+ Add](#)

Filter Actions

Policy Name	Version	Policy Status	Deployment Status	Scope	Queuing Profile
No data to display					

Deploying Wired Application QoS Policy

- Provide policy name; new policy should default to Wired QoS
- Select and edit site scope to deploy policy

The screenshot displays the Cisco configuration interface for deploying a Wired Application QoS Policy. The interface is divided into two main sections: **Application Policies** and **Site Scope**.

Application Policies Section:

- Application QoS Policy Name*:** A text field containing "CVD-QoS-Wired".
- Wired:** A radio button selected for the policy type.
- Site Scope 0 Sites:** A link indicating the current site scope, with a red arrow pointing to the **Site Scope** dialog box.
- Queueing Profiles:** A dropdown menu showing "CVD_QUEUING_PROFILE".
- Business Relevant (16):** A list of application categories with their respective application counts:
 - authentication-services (39 applications)
 - backup-and-storage (14 applications)
 - collaboration-apps (70 applications)
 - database-apps (34 applications)

Site Scope Dialog Box:

- Information:** A note stating: "Once you have selected sites, you must assign a Service Provider Profile to an interface of any WAN facing devices to ensure your policy is configured correctly."
- Search:** A search bar labeled "QSearch Hierarchy" with a "Search Help" link.
- Site Hierarchy:** A tree view showing the selection of sites:
 - Global (unchecked)
 - Bay Area (unchecked)
 - San_Francisco-1 (unchecked)
 - San_Jose-13 (checked)
- Configure devices:** A button next to the selected site "San_Jose-13".
- Buttons:** "Cancel" and "Save" buttons at the bottom right.

Deploying Wired Application QoS Policy

- Option to select devices and interfaces to exclude from QoS policy

Site Scope

Once you have selected sites, you must assign a Service Provider Profile to an interface of any WAN facing devices to ensure your policy is configured correctly.

QSearch Hierarchy

Search Help

- Global
- Bay Area
 - San_Francisco-1
 - San_Jose-13**

Configure devices

Cancel Save

Site > Devices

Devices in "San_Jose-13"

Find Device

Device Name	Device Role	Policy Exclusions	Service Provider Profile Settings
Cat9300-1	ACCESS	☐ Exclude Device Exclude Interfaces	N/A
Fusion.mango.local	BORDER ROUTER	☐ Exclude Device Exclude Interfaces	1 configured
Cat9300-2	ACCESS	☐ Exclude Device Exclude Interfaces	N/A

Showing 3 of 3 [Show more](#)

Cancel **Save**

Deploying Wired Application QoS Policy

- Option to select different queuing profile if CVD profile not desired
- Option to add additional Service Provider profile for WAN router (e.g. multiple WAN links)

The screenshot shows the 'Application Policies' configuration page for a 'Wired' application. The 'Application QoS Policy Name' is 'CVD-QoS-Wired'. The 'Site Scope' is '3 Sites'. The 'Queuing Profiles' section shows 'CVD_QUEUEING_PROFILE' selected. The 'Service Provider Profiles' section shows '1 Profiles'. A red arrow points to the 'file-sharing' application set in the 'Default (6)' column, with the text 'Each App Set can be dragged to different Business Relevance group as needed'. Yellow arrows point from the 'file-sharing' application set to the 'authentication-services' and 'general-browsing' application sets in the 'Business Relevant (16)' column.

Application Policies Queuing Profiles

Application QoS Policy Name*
CVD-QoS-Wired ☒ Wired ☐ Wireless [+ Application Registry](#)

Site Scope 3 Sites Queuing Profiles CVD_QUEUEING_PROFILE Service Provider Profiles 1 Profiles

Business Relevant (16)	Default (6)	Business Irrelevant (6)
authentication-services 39 applications	file-sharing 32 applications	consumer-browsing 226 applications
backup-and-storage 14 applications	general-browsing 13 applications	consumer-file-sharing 40 applications
collaboration-apps 70 applications	general-media 12 applications	consumer-gaming 15 applications
database-apps 34 applications	general-misc 498 applications	consumer-media 107 applications

Close Deploy

Deploying Wired Application QoS Policy

- Option to save intent as draft to be modified later
- Option to reset changes back to CVD defaults

Application Policies

Queuing Profiles

Application QoS Policy Name*

CVD-QoS-Wired

☒ Wired

☐ Wireless

+ Application Registry

Site Scope 3 Sites

Queuing Profiles CVD_QUEUING_PROFILE

Service Provider Profiles 1 Profiles

Find Application / Application Set

Business Relevant (16)	Default (6)	Business Irrelevant (6)
> authentication-services 39 applications ✕	> file-sharing 32 applications ✕	> consumer-browsing 226 applications ✕
> backup-and-storage 14 applications ✕	> general-browsing 13 applications ✕	> consumer-file-sharing 40 applications ✕
> collaboration-apps 70 applications ✕	> general-media 12 applications ✕	> consumer-gaming 15 applications ✕
> database-apps 34 applications ✕	> general-misc 498 applications ✕	> consumer-media 107 applications ✕

Save Draft

Reset to Cisco Validated Design

Close

Deploy

Deploying Wired Application QoS Policy

- Deploy with option to preview and schedule changes

Application Policies

Queuing Profiles

Application QoS Policy Name*

CVD-QoS-Wired

☒ Wired

☐ Wireless

+ Application Registry

Site Scope 3 Sites

Queuing Profiles CVD_QUEUING_PROFILE

Service Provider Profiles 1 Profiles

Find Application / Application Set

Business Relevant (16)

Default (6)

Business Irrelevant (6)

> authentication-services

39 applications

×

> backup-and-storage

14 applications

×

> collaboration-apps

70 applications

×

> database-apps

34 applications

×

> file-sharing

32 applications

×

> general-browsing

13 applications

×

> general-media

12 applications

×

> general-misc

498 applications

×

> consumer-browsing

226 applications

×

> consumer-file-sharing

40 applications

×

> consumer-gaming

15 applications

×

> consumer-media

107 applications

×

Close

Deploy

Deploying Wired Application QoS Policy

- Verify deployment status on devices

Application Policies

Queuing Profiles

☐ Deploy by default on wired devices ⓘ

As of: Feb 8, 2026 8:08 PM ↺ + Add

1 Selected Filter Actions ▾

Policy Name ↕	Version	Policy Status	Deployment Status	Scope	Queuing Profile
☒ CVD-QoS-Wired	1	Deployed	3/3 Devices Provisioned	3 Sites	CVD_QUEUING_PROFILE

Showing 1 of 1

CVD-QoS-Wired

3

Total devices

0

Failed devices

3

Successful devices

0

Terminated devices

0

New devices

0

Devices being configured

Filter

As of: Feb 8, 2026 8:08 PM ↺

Device Name	Site	Status	Status Details	Device Type	Network Role	Device IP Address
Cat9300-2	Global/Bay Area/San_Jose-13/SJC-13-2	✔ Success	N / A	Cisco Catalyst 9300 Switch	ACCESS	100.124.0.12
Cat9300-1	Global/Bay Area/San_Jose-13/SJC-13-1	✔ Success	N / A	Cisco Catalyst 9300 Switch	ACCESS	100.124.0.11
Fusion.mango.local	Global/Bay Area/San_Jose-13	✔ Success	N / A	Cisco 4431 Integrated Services Router	BORDER ROUTER	100.127.0.2

Application QoS Policy Deployed to Wired Devices



- Switch

<pre>ip access-list extended DNA-MARKING_IN#TUNNELED-NBAR__acl remark capwap-data PERMIT UDP any any eq 5246 PERMIT UDP any any eq 5247 remark vxlan PERMIT UDP any any eq 4789 ip access-list extended DNA-MARKING_IN#OAM_CUSTOM__acl remark dns PERMIT TCP any any eq 53 PERMIT TCP any any eq 5353 PERMIT UDP any any eq 53 PERMIT UDP any any eq 5353 class-map match-any DNA-MARKING_IN#TUNNELED-NBAR match access-group name DNA-MARKING_IN#TUNNELED-NBAR__acl class-map match-any DNA-MARKING_IN#VOICE_CUSTOM class-map match-any DNA-MARKING_IN#BROADCAST_CUSTOM class-map match-any DNA-MARKING_IN#REALTIME_CUSTOM class-map match-any DNA-MARKING_IN#MM_CONF_CUSTOM class-map match-any DNA-MARKING_IN#MM_STREAM_CUSTOM class-map match-any DNA-MARKING_IN#CONTROL_CUSTOM class-map match-any DNA-MARKING_IN#SIGNALING_CUSTOM class-map match-any DNA-MARKING_IN#OAM_CUSTOM match access-group name DNA-MARKING_IN#OAM_CUSTOM__acl class-map match-any DNA-MARKING_IN#TRANS_DATA_CUSTOM class-map match-any DNA-MARKING_IN#BULK_DATA_CUSTOM class-map match-any DNA-MARKING_IN#SCAVENGER_CUSTOM class-map match-all DNA-MARKING_IN#VOICE match protocol attribute traffic-class voip-telephony match protocol attribute business-relevance business-relevant class-map match-all DNA-MARKING_IN#BROADCAST match protocol attribute traffic-class broadcast-video match protocol attribute business-relevance business-relevant class-map match-all DNA-MARKING_IN#REALTIME match protocol attribute traffic-class real-time-interactive match protocol attribute business-relevance business-relevant class-map match-all DNA-MARKING_IN#MM_CONF match protocol attribute traffic-class multimedia-conferencing match protocol attribute business-relevance business-relevant class-map match-all DNA-MARKING_IN#MM_STREAM match protocol attribute traffic-class multimedia-streaming match protocol attribute business-relevance business-relevant class-map match-all DNA-MARKING_IN#CONTROL match protocol attribute traffic-class network-control match protocol attribute business-relevance business-relevant class-map match-all DNA-MARKING_IN#SIGNALING match protocol attribute traffic-class signaling match protocol attribute business-relevance business-relevant</pre>	<pre>class-map match-all DNA-MARKING_IN#OAM match protocol attribute traffic-class ops-admin-mgmt match protocol attribute business-relevance business-relevantclass-map match-all DNA-MARKING_IN#TRANS_DATA match protocol attribute traffic-class transactional-data match protocol attribute business-relevance business-relevant class-map match-all DNA-MARKING_IN#BULK_DATA match protocol attribute traffic-class bulk-data match protocol attribute business-relevance business-relevant class-map match-all DNA-MARKING_IN#SCAVENGER match protocol attribute business-relevance business-irrelevant class-map match-any DNA-EZQOS_2P6Q3T_9K#VOICE-PQ1 match dscp EF class-map match-any DNA-EZQOS_2P6Q3T_9K#VIDEO-PQ2 match dscp CS5 match dscp CS4 class-map match-any DNA-EZQOS_2P6Q3T_9K#CONTROL-PLANE match dscp CS3 match dscp CS2 match dscp CS7 match dscp CS6 class-map match-any DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-CONFERENCING match dscp AF43 match dscp AF41 match dscp AF42 class-map match-any DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-STREAMING match dscp AF32 match dscp AF33 match dscp AF31 class-map match-any DNA-EZQOS_2P6Q3T_9K#TRANSACTIONAL-DATA match dscp AF23 match dscp AF21 match dscp AF22 class-map match-any DNA-EZQOS_2P6Q3T_9K#BULK-DATA match dscp CS1 match dscp AF12 match dscp AF13 match dscp AF11</pre>	<pre>policy-map DNA-MARKING_IN class DNA-MARKING_IN#TUNNELED-NBAR class DNA-MARKING_IN#VOICE_CUSTOM set dscp ef class DNA-MARKING_IN#BROADCAST_CUSTOM set dscp cs5 class DNA-MARKING_IN#REALTIME_CUSTOM set dscp cs4 class DNA-MARKING_IN#MM_CONF_CUSTOM set dscp af41 class DNA-MARKING_IN#MM_STREAM_CUSTOM set dscp af31 class DNA-MARKING_IN#CONTROL_CUSTOM set dscp cs6 class DNA-MARKING_IN#SIGNALING_CUSTOM set dscp cs3 class DNA-MARKING_IN#OAM_CUSTOM set dscp cs2 class DNA-MARKING_IN#TRANS_DATA_CUSTOM set dscp af21 class DNA-MARKING_IN#BULK_DATA_CUSTOM set dscp af11 class DNA-MARKING_IN#SCAVENGER_CUSTOM set dscp cs1 class DNA-MARKING_IN#VOICE set dscp ef class DNA-MARKING_IN#BROADCAST set dscp cs5 class DNA-MARKING_IN#REALTIME set dscp cs4 class DNA-MARKING_IN#MM_CONF set dscp af41 class DNA-MARKING_IN#MM_STREAM set dscp af31 class DNA-MARKING_IN#CONTROL set dscp cs6 class DNA-MARKING_IN#SIGNALING set dscp cs3 class DNA-MARKING_IN#OAM set dscp cs2 class DNA-MARKING_IN#TRANS_DATA set dscp af21 class DNA-MARKING_IN#BULK_DATA set dscp af11 class DNA-MARKING_IN#SCAVENGER set dscp cs1 class class-default set dscp default</pre>	<pre>policy-map DNA-dscp#APIC_QOS_Q_OUT class DNA-EZQOS_2P6Q3T_9K#VOICE-PQ1 priority level 1 police rate percent 10 queue-buffers ratio 15 class DNA-EZQOS_2P6Q3T_9K#VIDEO-PQ2 priority level 2 police rate percent 23 queue-buffers ratio 10 class DNA-EZQOS_2P6Q3T_9K#CONTROL-PLANE bandwidth remaining percent 10 queue-buffers ratio 10 class DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-CONFERENCING bandwidth remaining percent 15 queue-buffers ratio 10 queue-limit dscp 34 percent 100 queue-limit dscp 36 percent 90 queue-limit dscp 38 percent 80 class DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-STREAMING bandwidth remaining percent 15 queue-buffers ratio 10 queue-limit dscp 28 percent 90 queue-limit dscp 30 percent 80 class DNA-EZQOS_2P6Q3T_9K#TRANSACTIONAL-DATA bandwidth remaining percent 15 queue-buffers ratio 10 random-detect dscp-based random-detect dscp af22 percent 70 100 random-detect dscp af23 percent 60 100 random-detect dscp af21 percent 80 100 class DNA-EZQOS_2P6Q3T_9K#BULK-DATA bandwidth remaining percent 7 queue-buffers ratio 10 random-detect dscp-based random-detect dscp af11 percent 80 100 random-detect dscp cs1 percent 60 100 random-detect dscp af12 percent 70 100 random-detect dscp af13 percent 60 100 class class-default bandwidth remaining percent 38 queue-buffers ratio 25 random-detect dscp-based random-detect dscp default percent 80 100 interface TenGigabitEthernet1/0/2 service-policy input DNA-MARKING_IN service-policy output DNA-dscp#APIC_QOS_Q_OUT</pre>
--	--	--	--



Application QoS Policy Deployed to Wired Devices

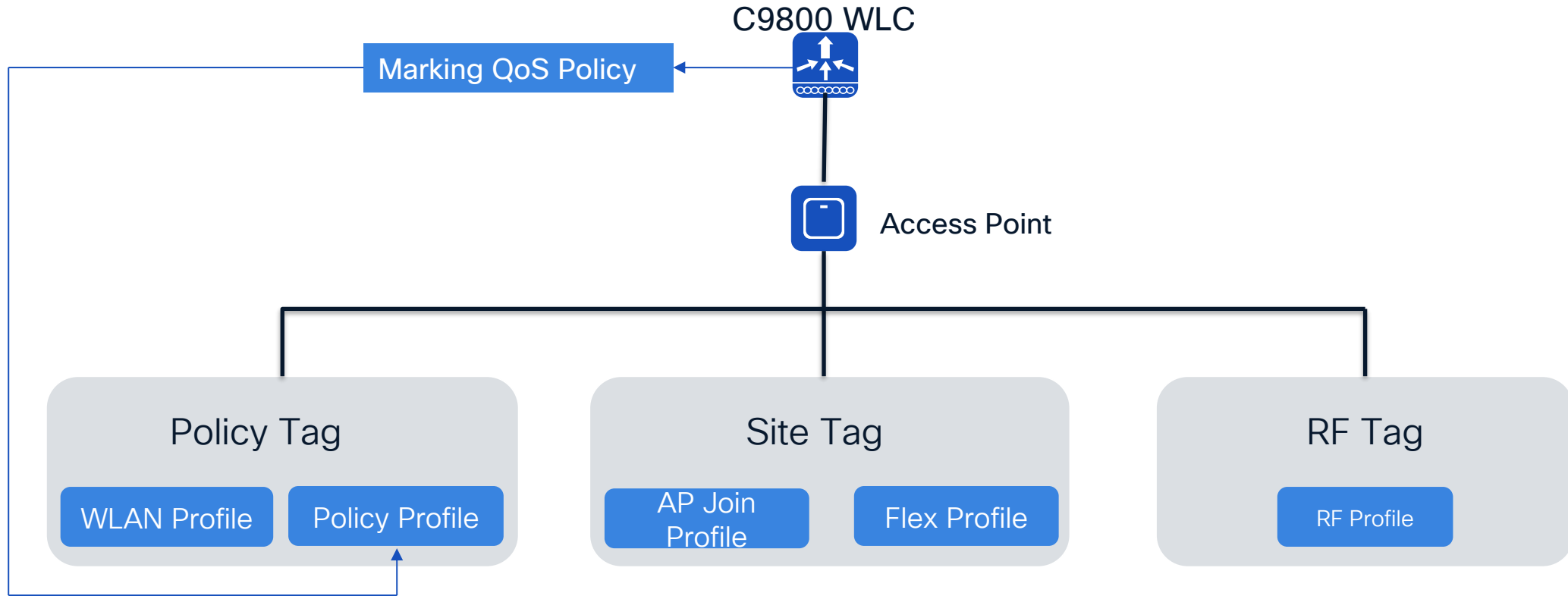


- Router

<pre>ip nbar attribute-map BRO attribute business-relevance business-relevant ip nbar attribute-set adobe-services BRO ip nbar attribute-set ms-live-accounts BRO ip nbar attribute-set github BRO class-map match-any DNA-MARKING_IN#TUNNELED-NBAR match protocol capwap-data match protocol vxlan class-map match-any DNA-MARKING_IN#VOICE_CUSTOM class-map match-any DNA-MARKING_IN#BROADCAST_CUSTOM class-map match-any DNA-MARKING_IN#REALTIME_CUSTOM class-map match-any DNA-MARKING_IN#MM_CONF_CUSTOM class-map match-any DNA-MARKING_IN#MM_STREAM_CUSTOM class-map match-any DNA-MARKING_IN#CONTROL_CUSTOM class-map match-any DNA-MARKING_IN#SIGNALING_CUSTOM class-map match-any DNA-MARKING_IN#OAM_CUSTOM class-map match-any DNA-MARKING_IN#TRANS_DATA_CUSTOM class-map match-any DNA-MARKING_IN#BULK_DATA_CUSTOM class-map match-any DNA-MARKING_IN#SCAVENGER_CUSTOM class-map match-all DNA-MARKING_IN#VOICE match protocol attribute traffic-class voip-telephony match protocol attribute business-relevance business-relevant class-map match-all DNA-MARKING_IN#BROADCAST match protocol attribute traffic-class broadcast-video match protocol attribute business-relevance business-relevant class-map match-all DNA-MARKING_IN#REALTIME match protocol attribute traffic-class real-time-interactive match protocol attribute business-relevance business-relevant class-map match-all DNA-MARKING_IN#MM_CONF match protocol attribute traffic-class multimedia-conferencing match protocol attribute business-relevance business-relevant class-map match-all DNA-MARKING_IN#MM_STREAM match protocol attribute traffic-class multimedia-streaming match protocol attribute business-relevance business-relevant class-map match-all DNA-MARKING_IN#CONTROL match protocol attribute traffic-class network-control match protocol attribute business-relevance business-relevant class-map match-all DNA-MARKING_IN#SIGNALING match protocol attribute traffic-class signaling match protocol attribute business-relevance business-relevant class-map match-all DNA-MARKING_IN#OAM match protocol attribute traffic-class ops-admin-mgmt match protocol attribute business-relevance business-relevant class-map match-all DNA-MARKING_IN#TRANS_DATA match protocol attribute traffic-class transactional-data match protocol attribute business-relevance business-relevant</pre>	<pre>class-map match-all DNA-MARKING_IN#BULK_DATA match protocol attribute traffic-class bulk-data match protocol attribute business-relevance business-relevant class-map match-all DNA-MARKING_IN#SCAVENGER match protocol attribute business-relevance business-irrelevant class-map match-any DNA-EZQOS_12C#VOICE match dscp EF class-map match-any DNA-EZQOS_12C#BROADCAST match dscp CS5 class-map match-any DNA-EZQOS_12C#REALTIME match dscp CS4 class-map match-any DNA-EZQOS_12C#MM_CONF match dscp AF43 match dscp AF41 match dscp AF42 class-map match-any DNA-EZQOS_12C#MM_STREAM match dscp AF32 match dscp AF33 match dscp AF31 class-map match-any DNA-EZQOS_12C#CONTROL match dscp CS6 class-map match-any DNA-EZQOS_12C#SIGNALING match dscp CS3 class-map match-any DNA-EZQOS_12C#OAM match dscp CS2 class-map match-any DNA-EZQOS_12C#TRANS_DATA match dscp AF23 match dscp AF21 match dscp AF22 class-map match-any DNA-EZQOS_12C#BULK_DATA match dscp AF12 match dscp AF13 match dscp AF11 class-map match-any DNA-EZQOS_12C#SCAVENGER match dscp CS1</pre>	<pre>policy-map DNA-dscp#EQ_Internet-Provider class DNA-EZQOS_12C#VOICE police rate percent 10 priority set dscp ef class DNA-EZQOS_12C#BROADCAST bandwidth remaining percent 10 set dscp af31 class DNA-EZQOS_12C#REALTIME bandwidth remaining percent 14 set dscp af31 class DNA-EZQOS_12C#MM_CONF bandwidth remaining percent 10 fair-queue set dscp af31 random-detect dscp-based class DNA-EZQOS_12C#MM_STREAM bandwidth remaining percent 10 fair-queue set dscp af31 random-detect dscp-based class DNA-EZQOS_12C#CONTROL bandwidth remaining percent 3 set dscp default class DNA-EZQOS_12C#SIGNALING bandwidth remaining percent 3 set dscp af21 class DNA-EZQOS_12C#OAM bandwidth remaining percent 3 set dscp af21 class DNA-EZQOS_12C#TRANS_DATA bandwidth remaining percent 14 fair-queue set dscp af21 random-detect dscp-based class DNA-EZQOS_12C#BULK_DATA bandwidth remaining percent 5 fair-queue set dscp af21 random-detect dscp-based class DNA-EZQOS_12C#SCAVENGER bandwidth remaining percent 1 set dscp default class class-default bandwidth remaining percent 27 fair-queue set dscp default random-detect dscp-based</pre>	<pre>policy-map DNA-dscp#EQ_Internet-Provider#shape#100.0 class class-default shape average 100000000 service-policy DNA-dscp#EQ_Internet-Provider policy-map DNA-dscp#QUEUEING_OUT class DNA-EZQOS_12C#VOICE police rate percent 10 priority class DNA-EZQOS_12C#BROADCAST police rate percent 10 priority class DNA-EZQOS_12C#REALTIME police rate percent 13 priority class DNA-EZQOS_12C#MM_CONF bandwidth remaining percent 15 fair-queue random-detect dscp-based class DNA-EZQOS_12C#MM_STREAM bandwidth remaining percent 15 fair-queue random-detect dscp-based class DNA-EZQOS_12C#CONTROL bandwidth remaining percent 4 class DNA-EZQOS_12C#SIGNALING bandwidth remaining percent 3 class DNA-EZQOS_12C#OAM bandwidth remaining percent 3 class DNA-EZQOS_12C#TRANS_DATA bandwidth remaining percent 15 fair-queue random-detect dscp-based class DNA-EZQOS_12C#BULK_DATA bandwidth remaining percent 6 fair-queue random-detect dscp-based class DNA-EZQOS_12C#SCAVENGER bandwidth remaining percent 1 class class-default bandwidth remaining percent 38 fair-queue random-detect dscp-based</pre>	<pre>policy-map DNA-MARKING_IN class DNA-MARKING_IN#TUNNELED-NBAR class DNA-MARKING_IN#VOICE_CUSTOM set dscp ef class DNA-MARKING_IN#BROADCAST_CUSTOM set dscp cs5 class DNA-MARKING_IN#REALTIME_CUSTOM set dscp cs4 class DNA-MARKING_IN#MM_CONF_CUSTOM set dscp af41 class DNA-MARKING_IN#MM_STREAM_CUSTOM set dscp af31 class DNA-MARKING_IN#CONTROL_CUSTOM set dscp cs6 class DNA-MARKING_IN#SIGNALING_CUSTOM set dscp cs3 class DNA-MARKING_IN#OAM_CUSTOM set dscp cs2 class DNA-MARKING_IN#TRANS_DATA_CUSTOM set dscp af21 class DNA-MARKING_IN#BULK_DATA_CUSTOM set dscp af11 class DNA-MARKING_IN#SCAVENGER_CUSTOM set dscp cs1 class DNA-MARKING_IN#VOICE set dscp ef class DNA-MARKING_IN#BROADCAST set dscp cs5 class DNA-MARKING_IN#REALTIME set dscp cs4 class DNA-MARKING_IN#MM_CONF set dscp af41 class DNA-MARKING_IN#MM_STREAM set dscp af31 class DNA-MARKING_IN#CONTROL set dscp cs6 class DNA-MARKING_IN#SIGNALING set dscp cs3 class DNA-MARKING_IN#OAM set dscp cs2 class DNA-MARKING_IN#TRANS_DATA set dscp af21 class DNA-MARKING_IN#BULK_DATA set dscp af11 class DNA-MARKING_IN#SCAVENGER set dscp cs1 class class-default set dscp default interface GigabitEthernet0/0/0 service-policy output DNA-dscp#EQ_Internet-Provider#shape#100.0 service-policy input DNA-MARKING_IN interface GigabitEthernet0/0/1 service-policy input DNA-MARKING_IN service-policy output DNA-dscp#QUEUEING_OUT</pre>
--	---	--	---	--

QoS on Wireless Network

- Marking Policy applied to the specified SSID in both directions



Deploying Wireless Application QoS Policy

- Add new wireless policy under [Policy -> Application QoS -> Application Policies](#)

Application Policies

Queuing Profiles

☐ Deploy by default on wired devices ⓘ

As of: Feb 8, 2026 8:08 PM

+ Add

1 Selected

Filter

Actions ▾

Policy Name ▴▾	Version	Policy Status	Deployment Status	Scope	Queuing Profile
⦿ CVD-QoS-Wired	1	Deployed	3/3 Devices Provisioned	3 Sites	CVD_QUEUING_PROFILE

Showing 1 of 1

Deploying Wireless Application QoS Policy

- Provide policy name; select Wireless as intent
- Select Wireless as intent, along with target SSID

Application Policies

Queuing Profiles

Application QoS Policy Name*

CVD-QoS-Wireless

☐ Wired ☒ Wireless

SSID

Pod46-1x

+ Application Registry

Site Scope 0 Sites

Queuing Profiles CVD_QUEUING_PROFILE

Wireless Applications Versions

Find Application / Application Set

Business Relevant (16)	Default (6)	Business Irrelevant (6)
> authentication-services 39 applications ×	> file-sharing 32 applications ×	> consumer-browsing 226 applications ×
> backup-and-storage 14 applications ×	> general-browsing 13 applications ×	> consumer-file-sharing 40 applications ×
> collaboration-apps 70 applications ×	> general-media 12 applications ×	> consumer-gaming 15 applications ×
> database-apps 34 applications ×	> general-misc 498 applications ×	> consumer-media 107 applications ×

Deploying Wireless Application QoS Policy

- Select and edit site scope to deploy policy

Application Policies

Queuing Profiles

Application QoS Policy Name*

CVD-QoS-Wireless

☐ Wired

Site Scope 0 Sites

Queuing Profiles CVD_QUEUING_PROFILE

Wired

Business Relevant (16)

> authentication-services

39 applications

×

> backup-and-storage

14 applications

×

> collaboration-apps

70 applications

×

> database-apps

34 applications

×

Site Scope

Once you have selected sites, you must assign a Service Provider Profile to an interface of any WAN facing devices to ensure your policy is configured correctly.

Selecting a site (Area/Building/Floor) which is a managed AP location, will deploy the wireless application QoS policy to the associated wireless controller along with it's other managed AP locations.

QSearch Hierarchy

☐ Global

☐ Bay Area

☐ San_Francisco-1

☒ San_Jose-13

Cancel

Save

Deploying Wireless Application QoS Policy

- Modify Queuing Profile or App Set as needed
- Deploy with option to preview and schedule changes

Application Policies

Queuing Profiles

Application QoS Policy Name*

CVD-QoS-Wireless

☐ Wired

☒ Wireless

SSID

Pod46-1x

+ Application Registry

Site Scope 3 Sites

Queuing Profiles CVD_QUEUING_PROFILE

Wireless Applications Versions

Find Application / Application Set

Business Relevant (16)	Default (6)	Business Irrelevant (6)
> authentication-services 39 applications ×	> file-sharing 32 applications ×	> consumer-browsing 226 applications ×
> backup-and-storage 14 applications ×	> general-browsing 13 applications ×	> consumer-file-sharing 40 applications ×
> collaboration-apps 70 applications ×	> general-media 12 applications ×	> consumer-gaming 15 applications ×
> database-apps 34 applications ×	> general-misc 498 applications ×	> consumer-media 107 applications ×
> desktop-virtualization-apps ×	> software-updates ×	> consumer-misc ×

Close

Deploy

Deploying Wireless Application QoS Policy

- Verify deployment status on devices

Application Policies

Queuing Profiles

☐ Deploy by default on wired devices ⓘ

1 Selected Filter Actions

Policy Name	Version	Policy Status	Deployment Status
☐ CVD-QoS-Wired	1	Deployed	3/3 Devices Provisioned
☒ CVD-QoS-Wireless	1	Deployed	1/1 Devices Provisioned

Showing 2 of 2

CVD-QoS-Wireless

×

1

0

1

0

0

0

Total devices

Failed devices

Successful devices

Terminated devices

New devices

Devices being configured

FilterAs of: Feb 8, 2026 8:21 PM ⓘ

Device Name	Site	Status	Status Details	Device Type	Network Role	Device IP Address
C9800-CL	Global/Bay Area/San_Jose-13	✔ Success ⓘ	Protocol/Attribute based policy is configured on the device. This policy supports all default NBAR applications.	Cisco Catalyst 9800-CL Wireless Controller for Cloud	ACCESS	100.64.0.103

Showing 1 of 1

Application QoS Policy Deployed to WLC



```
class-map match-all <WLAN-ProfileName>_TRANS_DATA_438a864c
match protocol attribute business-relevance business-relevant
match protocol attribute traffic-class transactional-data
class-map match-all <WLAN-ProfileName>_REALTIME_438a864c
match protocol attribute business-relevance business-relevant
match protocol attribute traffic-class real-time-interactive
class-map match-all <WLAN-ProfileName>_MM_CONF_438a864c
match protocol attribute business-relevance business-relevant
match protocol attribute traffic-class multimedia-conferencing
class-map match-all <WLAN-ProfileName>_SIGNALING_438a864c
match protocol attribute business-relevance business-relevant
match protocol attribute traffic-class signaling
class-map match-all <WLAN-ProfileName>_BROADCAST_438a864c
match protocol attribute business-relevance business-relevant
match protocol attribute traffic-class broadcast-video
class-map match-all <WLAN-ProfileName>_BULK_DATA_438a864c
match protocol attribute business-relevance business-relevant
match protocol attribute traffic-class bulk-data
class-map match-all <WLAN-ProfileName>_SCAVENGER_438a864c
match protocol attribute business-relevance business-irrelevant
class-map match-all <WLAN-ProfileName>_VOICE_438a864c
match protocol attribute business-relevance business-relevant
match protocol attribute traffic-class voip-telephony
class-map match-all <WLAN-ProfileName>_MM_STREAM_438a864c
match protocol attribute business-relevance business-relevant
match protocol attribute traffic-class multimedia-streaming
class-map match-all <WLAN-ProfileName>_OAM_438a864c
match protocol attribute business-relevance business-relevant
match protocol attribute traffic-class ops-admin-mgmt.
class-map match-all <WLAN-ProfileName>_CONTROL_438a864c
match protocol attribute business-relevance business-relevant
match protocol attribute traffic-class network-control
```

```
policy-map <WLAN-ProfileName>_DNA-MARKING_438a864c
class <WLAN-ProfileName>_VOICE_438a864c
set dscp 46
class <WLAN-ProfileName>_TRANS_DATA_438a864c
set dscp 18
class <WLAN-ProfileName>_SCAVENGER_438a864c
set dscp 8
class <WLAN-ProfileName>_REALTIME_438a864c
set dscp 32
class <WLAN-ProfileName>_MM_STREAM_438a864c
set dscp 26
class <WLAN-ProfileName>_BROADCAST_438a864c
set dscp 40
class <WLAN-ProfileName>_OAM_438a864c
set dscp 16
class <WLAN-ProfileName>_SIGNALING_438a864c
set dscp 24
class <WLAN-ProfileName>_MM_CONF_438a864c
set dscp 34
class <WLAN-ProfileName>_CONTROL_438a864c
set dscp 48
class <WLAN-ProfileName>_BULK_DATA_438a864c
set dscp 10
class class-default
set dscp 0

wireless profile policy <WLAN-ProfileName>_profile
service-policy input <WLAN-ProfileName>_DNA-MARKING_438a864c
service-policy output <WLAN-ProfileName>_DNA-MARKING_438a864c
```

Application QoS Policy Verification on Device



```
Cat9300-2#show policy-map interface G1/0/10
```

```
GigabitEthernet1/0/10
```

```
Service-policy input: DNA-MARKING_IN
```

```
Class-map: DNA-MARKING_IN#OAM (match-all)
```

```
3864 packets
```

```
Match: protocol attribute traffic-class ops-admin-mgmt.
```

```
Match: protocol attribute business-relevance business-  
relevant
```

```
QoS Set
```

```
dscp cs2
```

```
Class-map: DNA-MARKING_IN#SCAVENGER (match-all)
```

```
1040 packets
```

```
Match: protocol attribute business-relevance business-  
irrelevant
```

```
QoS Set
```

```
dscp cs1
```

```
Class-map: class-default (match-any)
```

```
3374 packets
```

```
Match: any
```

```
QoS Set
```

```
dscp default
```

```
Service-policy output: DNA-dscp#APIC_QOS_Q_OUT
```

```
queue stats for all priority classes:
```

```
Queueing
```

```
priority level 1
```

```
(total drops) 0
```

```
(bytes output) 2089815
```

```
queue stats for all priority classes:
```

```
Queueing
```

```
priority level 2
```

```
(total drops) 0
```

```
(bytes output) 0
```

```
Class-map: class-default (match-any)
```

```
58822 packets
```

```
Match: any
```

```
Queueing
```

```
(total drops) 0
```

```
(bytes output) 340871
```

```
bandwidth remaining 38%
```

```
queue-buffers ratio 25
```

Wrap Up

Wrap Up

- NBAR can classify 1500+ applications natively on device, including encrypted apps
- CBAR enhances NBAR capabilities through automatic protocol pack and application rules update without needing device reboot
- Application Health on Catalyst Center gained through info from NBAR/CBAR allows for monitoring and management of application issues to reduce Mean Time to Resolution for users
- Application QoS Policy provides simplified QoS management to ensure end-to-end optimal forwarding of applications based on business relevance through the network

Continue your Learning

Visit Capture the Flag Booth

World of Solutions, Hall 3

Challenge yourself with gamified hands-on labs and activities within a variety of Cisco Solutions

What's New:

**Experience New
Products through
CTF Missions**

Hear at Sessions →

See Demo at Showcase →

Try hands-on at CTF

AI for Everyone Theme:

Cisco and non-Cisco
AI Innovations

Understand AI
Fundamentals

Real-world AI Use-
cases

CTF Mission Areas:

Networking

Security

Data Center and Cloud

Collaboration

Observability

Offensive Security and
Forensics

CTF Activities and Theater:

Design Clinic

AI Hacking

Secure AI Coding - Project
CodeGuard

Splunk Arcade

Squid Trials - Securing AI

CTF Theater (hourly)

Bonus: Earn Cisco Continuing Education (CE) Credits by playing CTF Missions. Redeem to renew your Cisco Certifications

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Engineer meeting

Visit the Technical Solutions Clinics to discuss your technical questions



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

Thank you

CISCO Live !

