SS IOT: Implement WiFi Coexistence with ESL

- Feature history for WiFi-IoT radio coexistence, on page 1
- WiFi-IoT radio coexistence, on page 1

Feature history for WiFi-IoT radio coexistence

- This table provides release and related information for the feature explained in this module.
- This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 1: Feature history for WiFi-IoT radio coexistence

Feature Name	Release Information	Feature Description
WiFi-IoT radio coexistence	Cisco IOS XE 26.1.1	WiFi-IoT radio coexistence is a collaborative interference-reduction mechanism that minimizes signal interference between WiFi and IoT radios operating on the 2.4 GHz ISM band. It utilizes Packet Traffic Arbitration (PTA) to coordinate airtime sharing between collocated radios, improving the performance and reliability of wireless networks in environments with high IoT device density.

WiFi-IoT radio coexistence

WiFi-IoT radio coexistence is a collaborative interference-reduction mechanism that

- minimizes signal interference between WiFi and IoT radios operating on the 2.4 GHz ISM band
- utilizes Packet Traffic Arbitration (PTA) to coordinate airtime sharing between collocated radios, and
- improves the performance and reliability of wireless networks in environments with high IoT device density.

Packet Traffic Arbitration (PTA)

Packet Traffic Arbitration (PTA) is a coordination entity that provides per-packet authorization for transmissions. It dynamically manages the wireless medium based on traffic load, ensuring that high priority packets from either radio are granted access while preventing simultaneous transmissions that would cause collisions.

Collaborative and Non-collaborative Mechanisms

- Non-collaborative: Radios do not exchange information.
- Collaborative: Radios exchange real-time state information to negotiate medium access.

Difference between collaborative and non-collaborative mode

In non-collaborative mode, the IoT radio and the WiFi radio each transmit whenever they have data, regardless of whether the other radio is currently in use. As a result, if a collision occurs when the WiFi radio is busy because it is being used by the WiFi chipset, the IoT radio cannot send its packet. In collaborative mode, the IoT radio asks the WiFi radio for permission to transmit. Once permission is granted, the IoT radio transmits over the radio.

Best practices for WiFi-IoT coexistence

- IOx application dependency: For Electronic Shelf Labeling (ESL) use cases, the coexistence feature requires an active IOx application. The IOx application must be installed and running on the AP to manage the IoT radio firmware.
- Use supported 6E platforms: During initial deployment, use the Cisco Catalyst 9162, 9164, or 9166 series APs.
- Controller priority: The controller’s configuration commands take precedence over requests from local IOx applications.

How WiFi-IoT coexistence works with IOx applications

WiFi-IoT coexistence enables the controller, the AP, and collocated third-party applications to manage radio airtime by facilitating a synchronized communication flow. The key components involved in the process are:

- The controller defines the global administrative state (enable or disable) using RF profiles.
- The AP manages communication between the WiFi chip, the IoT chip, and the IOx application.
- The IOx application, such as those for ESL, requests IoT radio access and provides specific IoT performance counters.

Summary

The process involves these stages:

- Administrative Configuration: The controller sends the desired coexistence state to the AP.
- Application Subscription: After installation, the IOx application establishes gRPC connection to the AP and subscribes to the coexistence service.

- Enablement Request: The IOx application asks the AP to enable coexistence on the IoT chip.
- Priority Verification: The AP checks the administrative state from the controller and, if enabled, activates coexistence on the WiFi and IoT chips.
- Status Synchronization: The IOx application confirms coexistence is enabled on the IoT chip, and the AP reports the 'Enabled' state to the controller.
- Periodic Reporting: The AP collects and forwards IoT statistics from the IOx application to the controller.

Workflow

When the administrative and application states are aligned, the system reliably transmits both WiFi and IoT data without requiring manual intervention.

Configuration priority for WiFi-IoT coexistence

Controller configuration has higher priority than IOx application requests.

- If you disable coexistence on the controller, the AP disables the feature on the WiFi chip and instructs the IOx application to disable the feature on the IoT chip, regardless of the IOx application's requirements.
- The IOx application can only enable coexistence if the administrative state in the AP's RF profile is set to Enabled.

Create an RF profile for WiFi-IoT coexistence (CLI)

Provide a consistent RF environment that supports both WiFi and IoT devices by defining an appropriate RF profile using commands.

RF profiles allow you to manage and tune radio parameters for different deployment needs, such as ensuring reliable operation of WiFi and IoT devices in the 2.4 GHz band.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure Cisco AP and 802.11 parameters.

Example:

```
Device(config)# ap dot11
```

Step 3 Configure 802.11b parameters.

Example:

```
Device(config)# ap dot11 24ghz
```

Step 4 Set the RF-profile name and specify the name of the RF profile to configure.

Example:

```
Device(config)# ap dot11 24ghz rf-profile default-rf-profile
```

Step 5 Specify and enter the description of the RF profile.

Example:

```
Device(config-rf-profile)# description description-detail
```

Step 6 Negate a command. Shut down the profile and disable network.

Example:

```
Device(config-rf-profile)# no shutdown
```

Step 7 Exit the sub-mode.

Example:

```
Device(config-rf-profile)# exit
```

Configure WiFi-IoT coexistence (CLI)

Enable coexistence between WiFi and IoT radios to ensure reliable operation and minimize interference on supported Cisco APs using commands.

WiFi-IoT coexistence allows the AP to support both WiFi and IoT devices simultaneously on the 2.4 GHz band.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure Cisco AP and 802.11 parameters.

Example:

```
Device(config)# ap dot11
```

Step 3 Configure 802.11b parameters.

Example:

```
Device(config)# ap dot11 24ghz
```

Step 4 Set the RF-profile name and specify the name of the RF profile to configure.

Example:

```
Device(config)# ap dot11 24ghz rf-profile default-rf-profile
```

Step 5 Configure the RF Profile IoT settings.

Example:

```
Device(config-rf-profile)# iot
```

Step 6 Configure WiFi-IoT radio coexistence.

Example:

```
Device(config-rf-profile)# iot coexistence
```

Step 7 Exit the sub-mode.

Example:

```
Device(config-rf-profile)# exit
```

Tag the RF profile to an AP (CLI)

Assign a specific RF profile to customize the radio configuration of an AP using commands.

Perform this task when you need to apply a distinct RF profile to a particular AP for more granular wireless control.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure wireless and tag parameters.

Example:

```
Device(config)# wireless tag
```

Step 3 Configure and enter the name of the RF tag.

Example:

```
Device(config)# wireless tag rf default-rf-tag
```

Step 4 Configure and name the dot11b policy.

Example:

```
Device(config-wireless-rf-tag)# 24ghz-rf-policy default-dot11b-policy
```

Step 5 Exit the sub-mode.

Example:

```
Device(config-wireless-rf-tag)# exit
```

Step 6 Configure Cisco AP and enter the ethernet MAC address of the AP.

Example:

```
Device(config)# ap 9.12.15
```

Step 7 Map a RF tag to the AP and enter the name of the RF tag

Example:

```
Device(config-ap-tag)# rf-tag default-rf-tag
```

Step 8 Exit the sub-mode.

Example:

```
Device(config-ap-tag)# exit
```

Verify Admin state on RF profile

Use this command to verify the Admin state on RF profile.

- **show ap rf-profile name <RF_PROFILE> detail**

To verify the Admin state on RF profile, enter this command from the console:

```
Device# show ap rf-profile name iot-coex-custom-test-profile detail

Description                          : custom RF profile for IoT COEX testing
RF Profile Name                      : iot-coex-custom-test-profile
Band                                 : 2.4 GHz
Transmit Power Threshold v1          : -70 dBm
Min Transmit Power                   : -10 dBm
Max Transmit Power                   : 30 dBm
Operational Rates
  802.11b 1M Rate                    : Mandatory
  802.11b 2M Rate                    : Mandatory
  802.11b 5_5M Rate                  : Mandatory
  802.11b 11M Rate                   : Mandatory
  802.11g 6M Rate                    : Supported
  802.11g 9M Rate                    : Supported
  802.11g 12M Rate                   : Supported
  802.11g 18M Rate                   : Supported
  802.11g 24M Rate                   : Supported
  802.11g 36M Rate                   : Supported
  802.11g 48M Rate                   : Supported
  802.11g 54M Rate                   : Supported
Max Clients                          : 200
Trap Threshold
  Clients                            : 12 clients
  Interference                       : 10%
  Noise                              : -70 dBm
  Utilization                        : 80%
Multicast Data Rate                  : auto
Rx SOP Threshold                     : auto
Band Select
  Probe Response                     :  Disabled
  Cycle Count                        :  2 cycles
  Cycle Threshold                    :  200 milliseconds
  Expire Suppression                 :  20 seconds
  Expire Dual Band                   :  60 seconds
  Client RSSI                        :  -80 dBm
  Client Mid RSSI                    :  -80 dBm
High Speed Roam
  hsr mode                           :  Disabled
Load Balancing
  Window                             :  5 clients
  Denial                             :  3 count
Coverage Data
  Data                               : -80 dBm
  Voice                              : -80 dBm
  Minimum Client Level               : 3 clients
  Exception Level                    : 25%
RSSI Settings
```

```
  RSSI Low Check                  : Disabled
  RSSI Threshold                  : -127 dbm
DCA Channel List                  : 1,6,11
Unused Channel List               : 2,3,4,5,7,8,9,10
DCA Foreign AP Contribution       : Enabled
802.11n MCS Rates
  MCS  0                          : Enabled
  MCS  1                          : Enabled
  MCS  2                          : Enabled
  MCS  3                          : Enabled
  MCS  4                          : Enabled
  MCS  5                          : Enabled
  MCS  6                          : Enabled
  MCS  7                          : Enabled
  MCS  8                          : Enabled
  MCS  9                          : Enabled
  MCS 10                          : Enabled
  MCS 11                          : Enabled
  MCS 12                          : Enabled
  MCS 13                          : Enabled
  MCS 14                          : Enabled
  MCS 15                          : Enabled
  MCS 16                          : Enabled
  MCS 17                          : Enabled
  MCS 18                          : Enabled
  MCS 19                          : Enabled
  MCS 20                          : Enabled
  MCS 21                          : Enabled
  MCS 22                          : Enabled
  MCS 23                          : Enabled
  MCS 24                          : Enabled
  MCS 25                          : Enabled
  MCS 26                          : Enabled
  MCS 27                          : Enabled
  MCS 28                          : Enabled
  MCS 29                          : Enabled
  MCS 30                          : Enabled
  MCS 31                          : Enabled
State                             : Up
Client Aware FRA                  : Disabled
FRA Action                        : 2.4GHz/5GHz/Monitor
Client Network Preference         : default
Airtime Fairness Mode             : Disable
Airtime Stealing                  : N/A
Mesh Client Access Airtime Alloc  : Disabled
802.11ax
  OBSS PD                         : Disabled
  Non-SRG OBSS PD Maximum         : -62 dBm
  SRG OBSS PD                     : Disabled
  SRG OBSS PD Minimum             : -82 dBm
  SRG OBSS PD Maximum             : -62 dBm
NDP mode                          : Auto
Guard Interval                    : 800ns
A-MPDU Window                     : 255
Packets Retries Settings:
  Management Retries              : -1
  Aggregate Retries               : -1
  Non_Aggregate Retries           : -1
IOT Coexistence Admin State       : Enabled
```

Verify coexistence configuration applied to an AP on controller

Use this command to verify coexistence configuration applied to an AP on controller.

- **show ap name <AP_NAME>config general | include IOT**

To verify the coexistence configuration applied to an AP on controller, enter this command from the console:

```
Device# show ap name AP8C88.8152.CEE0 config general
Cisco AP Name   : AP8C88.8152.CEE0
================================================

Cisco AP Identifier                              : 940d.4b9c.24e0
Country Code                                     : US
Regulatory Domain Allowed by Country            : 802.11bg:-A   802.11a:-AB   802.11 6GHz:-B
Radio Authority IDs                              : None
AP Country Code                                  : US  - United States
Country Code Resolution Method                   : Proximity
AP Regulatory Domain
  802.11bg                                       : -A
  802.11a                                        : -B
  802.11 6GHz                                    : -B
License Type                                     : CW
License State                                    : Non Compliant
Non Compliance Reason                            : Never Licensed
MAC Address                                      : 8c88.8152.cee0
IP Address Configuration                         : DHCP
IP Address                                       : 100.12.99.185
IP Netmask                                       : 255.255.0.0
Gateway IP Address                               : 100.12.0.1
CAPWAP Path MTU                                  : 1485
Capwap Active Window Size                        : 1
Telnet State                                     : Disabled
CPU Type                                         :  ARMv8 Processor rev 4 (v8l)
Memory Type                                      : DDR4
Memory Size                                      : 1771520 KB
SSH State                                        : Enabled
Serial Console State                             : Enabled
Cisco AP Location                                : default location
AP Floor ID                                      : 0
AP Location Mode                                 : Unknown
Site Tag Name                                    : default-site-tag
RF Tag Name                                      : iot-coex-custom-test-tag
Policy Tag Name                                  : default-policy-tag
AP join Profile                                  : default-ap-profile
Flex Profile                                     : default-flex-profile
Tag Source                                       : Static
Static name                                      : FALSE
Primary Cisco Controller Name                    : katar
Primary Cisco Controller IP Address              : 100.12.45.46
Secondary Cisco Controller Name                  : Not Configured
Secondary Cisco Controller IP Address            : 0.0.0.0
Tertiary Cisco Controller Name                   : Not Configured
Tertiary Cisco Controller IP Address             : 0.0.0.0
Administrative State                             : Enabled
Operation State                                  : Registered
NAT External IP Address                          : 100.12.99.185
AP Certificate type                              : Manufacturer Installed Certificate
AP Certificate Expiry-time                       : 08/09/2099 22:58:26
AP Certificate issuer common-name                : High Assurance SUDI CA
AP Certificate Policy                            : Default
AP CAPWAP-DTLS LSC Status
    Certificate status        : Not Available
AP 802.1x LSC Status
    Certificate status        : Not Available
AP LSC authentication state                      : CAPWAP-DTLS
AP Mode                                          : Local
AP VLAN tagging state                            : Disabled
```

```
AP VLAN tag                                     : 0
CAPWAP Preferred mode                           : IPv4
CAPWAP UDP-Lite                                 : Not Configured
AP Submode                                      : Not Configured
Office Extend Mode                              : Disabled
Link-Encryption                                 : Disabled
Dhcp Server                                     : Disabled
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : information
Logging Syslog facility                         : kern
Software Version                                : 26.2.0.4
Boot Version                                    : 1.1.2.4
Mini IOS Version                                : 0.0.0.0
Stats Reporting Period                          : 180
LED State                                       : Enabled
MDNS Group Id                                   : 0
MDNS Rule Name                                  :
MDNS Group Method                               : None
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : DC/Full Power
Number of Slots                                 : 3
AP Model                                        : CW9174I
IOS Version                                     : 26.2.0.4
Reset Button                                    : Disabled
AP Serial Number                                : FVH2849A988
Management Frame Validation                     : Capable
Management Frame Protection                     : Not capable
AP User Name                                    : lab
AP 802.1X User Mode                             : Global
AP 802.1X User Name                             : Not Configured
Cisco AP System Logging Host                    : 255.255.255.255
Cisco AP Secured Logging TLS mode               : Disabled
AP Up Time                                      : 6 hours 3 minutes 37 seconds
AP CAPWAP Up Time                               : 6 minutes 16 seconds
Join Date and Time                              : 12/04/2025 12:04:53
Join Taken Time                                 : 3 seconds
Join Priority                                   : 1
AP Link Latency                                 : Disable
AP Lag Configuration Status                     : Disabled
Lag Support for AP                              : No
AP runs Dot11k/v LocalMAC                       : Yes
Rogue Detection                                 : Enabled
Rogue Containment auto-rate                     : Disabled
Rogue PMF Denial                              : Disabled
Rogue Containment of standalone flexconnect APs : Disabled
Rogue Detection Report Interval                 : 10
Rogue AP minimum RSSI                           : -90
Rogue AP minimum transient time                 : 0
AP TCP MSS Adjust                               : Enabled
AP TCP MSS Size                                 : 1250
AP IPv6 TCP MSS Adjust                          : Enabled
AP IPv6 TCP MSS Size                            : 1250
Hyperlocation Admin Status                      : Disabled
Retransmit count                                : 5
Retransmit interval                             : 3
Kernel core dump :
  Fulldump capable                              : No
  Minidump capable                              : Yes
Macsec Capability                               : Capable
  Port 0
    Macsec Status                               : NA
    Macsec Ciphersuite                          : NA
  Port 1
```

```
    Macsec Status                                 : NA
    Macsec Ciphersuite                            : NA
MLO Capability                                    : Capable
MLD Base MAC                                      : 960d.4b9c.24f0
Fabric status                                     : Disabled
FIPS status                                       : Disabled
WLANCC status                                     : Disabled
USB Module Type                                   : USB Module
USB Module State                                  : Disabled
USB Module Connected                              : No
USB Override                                      : Disabled
GAS rate limit Admin status                       : Disabled
WPA3 Capability                                   : Enabled
EWC-AP Capability                                 : Disabled
AWIPS Capability                                  : Enabled
AID Management Capability                         : Enabled
Proxy Hostname                                    : Not Configured
Proxy Port                                        : Not Configured
Proxy NO_PROXY list                               : Not Configured
Proxy Username                                    : Not Configured
GRPC server status                                : Disabled
Unencrypted Data Keep Alive                       : Enabled
Local DHCP Server                                 : Disabled
Traffic Distribution Statistics Capability        : Enabled
Dual DFS Statistics                               : Disabled
AP Upgrade Out-Of-Band Capability                 : Enabled
AP statistics                                     : Disabled
AP power derate Capability                        : Enabled
AP PMK Propagation Capability                     : Enabled
AP FTM Responder Capability                       : Enabled
AP FTM Initiator Capability                       : Enabled
AP UWB Responder Capability                       : Disabled
AP UWB Initiator Capability                       : Disabled
AP Client FTM capability                          : Enabled
URWB Capability                                   : Not Capable
6GHz Standard-Power mode                          : Not Allowed
Mesh DCA Run Status                               : N/A
Last Mesh DCA Run                                 :
Meraki Capable AP                                 : Yes
AP Console Speed                                  : 115200
Tilt Angle                                        : 176 Degree(s)
Radio Reset Reason Statistics
Slot 0
  Unknown Reason                                                  : 1
Slot 1
  Unknown Reason                                                  : 1
Slot 2
  Unknown Reason                                                  : 1
Slot 3

Radio Failure Reason Statistics
Slot 0
Slot 1
Slot 2
Slot 3
AP image integrity
  Time                                            : 12/28/2024 02:00:01
  Alterative image loaded                         : No
  Backup image status
    Version                                       : 26.1.0.40
    Partition                                     : part2
    Kernel                                        : Good
    Root FS                                       : Good
    IOX                                           : Good
```

```
  Primary image status
    Version                                         : 26.2.0.4
    Partition                                       : part1
    Kernel                                          : Good
    Root FS                                         : Good
    IOX                                             : Good
IOT Coexistence Admin State                         : Enabled
IOT Coexistence Operational State                   : Enabled
```

Verify coexistence summary of all the APs

Use this command to verify coexistence summary of all the APs.

- **show wireless iot-coexistence summary**

To verify the coexistence summary of all the APs, enter this command from the console:

```
Device# show wireless iot-coexistence summary
```

```
                                                                          |
                       IOT COUNTERS
AP Name                           Radio MAC       Coex Admin  Coex Oper    |   Tx pkts
Rx pkts        CRC     Low Pri   High Pri     Low Pri  High Pri    Low Pri   High Pri
                                                  State       State        |
           errors    requests   requests     denied     denied    Tx abort   Tx abort
-----------------------------------------------------------------------------------------
AP8C88.8152.CEE0                  940d.4b9c.24e0  Enabled     Enabled             359
   344         0         72         72          7          3           1          0
AP24D7.9CBD.F290                  c828.e526.a1c0  Disabled    Not supported
```

Verify coexistence WiFi statistics

Use this command to verify coexistence WiFi statistics.

- **show ap name <AP_NAME> iot coexistence statistics**

To verify the coexistence WiFi statistics, enter this command from the console:

```
Device# show ap name AP8C88.8152.CEE0 iot coexistence statistics

AP name                    : AP8C88.8152.CEE0
AP MAC Address             : 940d.4b9c.24e0
IOT Coex Admin state       : Enabled
IOT Coex Oper state        : Enabled
Last AP response code      : SUCCESS
IOT get stats err cnt      : 0
IOT Tx packets             : 580
IOT Rx packets             : 561
IOT CRC errors             : 0
IOT low pri requests       : 116
IOT high pri requests      : 116
IOT low pri denied         : 11
IOT high pri denied        : 5
IOT low pri tx aborted     : 3
IOT high pri tx aborted    : 0
WiFi get stats err cnt     : 0
WiFi Tx packets            : 0
WiFi Rx packets            : 0
WiFi CRC errors            : 0
```

```
WiFi low pri requests     : 0
WiFi high pri requests    : 0
WiFi low pri denied       : 0
WiFi high pri denied      : 0
WiFi low pri tx aborted   : 0
WiFi high pri tx aborted  : 0
Last Rcvd Time            : 12/04/2025 12:15:01
```