New Features for Cisco IOS XE 17.11.1a

This chapter contains the following sections:

LoRaWAN Pluggable Interface Module Support

These release adds support for the LoRaWAN Pluggable Interface Module which was first available on the IR1101.

Note This is a software parity release only. The LoRaWAN Pluggable Interface Module is neither orderable or hardware deployment ready for the IR1800 until the product is announced. Please reach out to your Cisco contact for any additional info.

The Cisco LoRaWAN Pluggable Interface Module supports eight channels of LoRa connectivity.

There are two different P-LPWA modules:

- The P-LPWA-900 is designed for RF regional profile US915, AS923 and AU915 as defined by the LoRa Alliance RF regional profile specifications.
- The P-LPWA-800 is designed for the EU868, IND865 and RU864 RF regional profile as defined by the LoRa Alliance RF regional profile specifications.

The Cisco LoRaWAN pluggable modules can be managed by command line interface (CLI), or the Cisco IOS XE Web User Interface (WebUI).

Details on installation, configuration, and regulatory information are found in the Cisco LoRaWAN Pluggable Interface Module Installation and Configuration Guide.

GNSS Support on the GPS/Dead Reckoning Module (IRM-GNSS-ADR)

Prior to the Cisco IOS XE 17.11.1a release, the only GNSS constellation supported was GPS. This release introduces support for GPS and Galileo.

Note Only ONE constellation can be enabled at a time.

There are new CLI options available to support the new constellation:

Configuration Commands:

```
(config-controller)# controller gps
<no> dead-reckoning constellation <gps | galileo |gnss >
```

Note The default setting is gps mode. The new galileo and gnss options in the above CLI example is used to configure Galileo and Multiple/Simultaneous GNSS (GPS + Galileo etc) respectively.

Show Commands

```
show platform hardware gps <mode | status | details>
....
Current Constellation Configured =  gps | galileo | gnss
....
```

Any changes made to the configuration will require the router to be rebooted.

More information is available in the Configuring GPS chapter of the IR1800 Software Configuration Guide.

Galileo Support on the LTE Pluggable Modules

With Cisco IOS XE 17.11.1a and earlier, the only GNSS constellation supported was GPS. This release introduces support for Galileo.

Note Only ONE constellation can be enabled at a time.

There are new CLI options available to support the new constellation:

Configuration Commands

```
config# controller cellular <slot/port>
(config-controller)# <no> lte gps constellation <gps | galileo | gnss >
```

Example:

```
(config-controller)#lte gps constellation ?
  galileo  select Galileo as active constellation
  gps      select GPS as active constellation
  gnss      select multiple GNSS as active constellation
```

Note The default setting is gps mode.

The new galileo and gnss options in the above CLI are used to configure Galileo and Multiple/Simultaneous GNSS (GPS + Galileo etc) respectively.

If you disable the GPS configuration, ensure there is no constellation configured, consistent with GPS mode configuration. For example:

```
config# controller Cellular 0/1/0
(config-controller)# no lte gps constellation gps
```

Show Commands

The following example shows the current GNSS constellation as Galileo:

```
#show cellular 0/1/0 gps detail
GPS Feature =  enabled
GPS Mode Configured =  standalone
Current Constellation Configured =  galileo | gps | gnss
GPS Port Selected =  Dedicated GPS port
GPS Status =  GPS acquiring
```

Any changes made to the configuration will require the router to be rebooted.

More information is available in the Cellular Pluggable Interface Module Configuration Guide.

Change to Smart Licensing Packaging

This release brings the IoT routing products inline with other Integrated Service Routers (ISR).

Smart Licensing Overview

Cisco Smart Licensing is a flexible licensing model that provides users with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across their organization. And it's secure. With Smart Licensing users get:

- Easy Activation: Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more Product Activation Keys (PAKs).
- Unified Management: My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- License Flexibility: Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

Smart Licensing Using Policy (SLP), was previously referred to as Smart Licensing Enhanced (SLE), and is the default mode starting with Cisco IOS-XE release 17.3.2. SLE replaced Smart Software Licensing. This feature change for Cisco IOS XE release 17.11.1a focuses on the licensing packaging.

License Levels

The following are the license levels available for all Cisco IR devices.

Base Licenses

- Network Essentials
- Network Advantage (includes Network Essentials)

Note These licenses are ordered through Cisco Commerce Workspace (CCW), and are permanent.

Add-on Licenses — These can be subscribed for a fixed term of three, five, or seven years.

- Digital Networking Architecture (DNA) Essentials
- DNA Advantage (includes DNA Essentials)

Note These licenses are ordered through Cisco Commerce Workspace (CCW), and relate to DNA-C and SDWAN. For further information, see the Cisco SD-WAN and Cisco DNA Center web pages.

The following tables provide details on the licensing levels:

Table 1: Network Essentials (Perpetual License)

Essential Switch Capabilities	Layer 2, Routed Access(RIP, EIGRP Stub, OSPF (1000 routes)), PBR, PIM Stub Multicast (1000 routes) PVLAN, VRRP, PBR, CDP, QoS, FHS, 802.1x, Macsec-128, CoPP, SXP, IP SLA Responder SSO **Note** For the device to be compliant with the DNA Essential License it must not exceed 1000 routes in the routing table regardless of how the routes were learned.
DevOps Integration	• Netconf, Restconf, gRPC • Yang Data Models • GuestShell (On-Box Python) • PnP Agent, ZTP

Table 2: Network Advantage (Perpetual License) Contains all of the Network Essentials plus the following:

IoT & Mobility	CoAP
Full Routing Functionality	BGP, HSRP, OSPF, ISIS,GLBP
Flexible Network Segmentation	VRF, VXLAN, LISP, SGT, MPLS
High Availability & Resiliency	NSF, GIR, Stackwise Virtual*, ISSU/eFSU, Patching (CLI)

Optimize Bandwidth Utilization with Multicast	MSDP, mVPN, AutoRP, PIM-BIDIR

Table 3: DNA Essentials (3,5,7 year terms)

Basic Automation	• PnP Application • LAN Automation • Embedded Event Manager
Basic Assurance	• Health Dashboards – Network and Client • Basic Device & Wired Client Health Monitoring

Table 4: DNA Advantage (3,5,7 year terms) Contains all of the DNA Essentials plus the following:

Advanced Automation	• Encrypted Traffic Analytics • DNA Service for Bonjour
Assurance & Analytics	• Compliance, Custom Reports • Switch 360 & Wired Client 360

Licensing Throughput Levels

In addition to configuring the license level, it is also possible to configure the throughput level on the device. The throughput level determines the bandwidth limit which is applied to encrypted traffic. There is no limit applied to the non-encrypted (clear) traffic going through a device.

Important To comply with global export regulations, if more than 250Mbs of encrypted traffic is required, then an "uncapped" – platform dependent – selection must be done on CCW, as well as an HSEC license.

This limit is imposed bidirectionally. This means that if the throughput limit is set to 250Mbps then up to 250Mbps of encrypted traffic can flow through the device in either direction. For example, the device can both receive and transmit up to 250Mbps of encrypted traffic. There is no limit applied on unencrypted traffic.

When the throughput level on the device is set to 'uncapped' there are no limits imposed on both encrypted and unencrypted traffic flowing through it.

Note To avoid confusion on throughput limits and IOS XE software releases, please note the following:

Cisco IOS XE release 17.11.1a and earlier running on the ESR6300, IR1800, and IR8140 platforms support boost, uncapped, and unlimited licenses. These are configured using the **platform hardware throughput level 2G** CLI.

Future Cisco IOS XE release 17.12.1 and later running on the ESR6300, IR1800, and IR8140 support the same licenses, but will be configured using the **platform hardware throughput level uncapped** CLI.

With future Cisco IOS XE release 17.12.1 and later, the **platform hardware throughput level 2G** and the **platform hardware throughput level uncapped** CLIs will both provide the same throughput as the uncapped license.

The following table shows the throughput limits (also referred to as Tier license) supported on IoT devices as of Cisco IOS XE 17.11.1a release.

Platform	25 Mbps bidirectional (Tier 0)	50 Mbps bidirectional	Up to 200 Mbps bidirectional (Tier 1)	250 Mbps bidirectional	2 Gbps	Uncapped (Tier 2)
ESR 6300	N/A	Yes	N/A	Yes	Yes	To be supported starting with 17.12.1
ESR-6300-LIC-K9	N/A	Yes	N/A	N/A	N/A	Yes
IR1101	N/A	N/A	N/A	Yes	N/A	Supported starting with 17.10.1.
IR1800	N/A	Yes	N/A	Yes	Yes	To be supported starting with 17.12.1
IR8100	N/A	Yes	Yes	Yes	Yes	To be supported starting with 17.12.1
IR8300	Yes	N/A	Yes	N/A	N/A	Yes

Command Line Interface

The following commands are available:

license boot level *<network-essentials/network-advantage>*

The throughput level can be configured using the following CLI on all IR devices except IR8300:

platform hardware throughput level *<limit>*

On the IR8300, the throughput level can be configured using the following CLI:

platform hardware throughput crypto *<limit>*

To see the throughput configured on the device, use the following CLI:

```
show version | include throughput
The current crypto throughput level is: 50000 kbps
```

Cisco IoT Operations Dashboard (OD) Support to Configure and Manage the WP-WIFI6-x Module

Cisco IOS XE release 17.11.1a provides additional capabilities to the Cisco Wi-Fi Interface Module (WIM).

This section contains the following:

WGB Concurrent Radio

Cisco IOS XE 17.11.1a supports the Cisco Wi-Fi Interface Module (WIM) configuration of concurrent radio in Workgroup Bridge (WGB) mode. This feature applies to the WIM that already has the CAPWAP image on Cisco IOS XE 17.11.1a and the unified client image.

The following table lists the Cisco Operational Dashboard use case and corresponding CLIs:

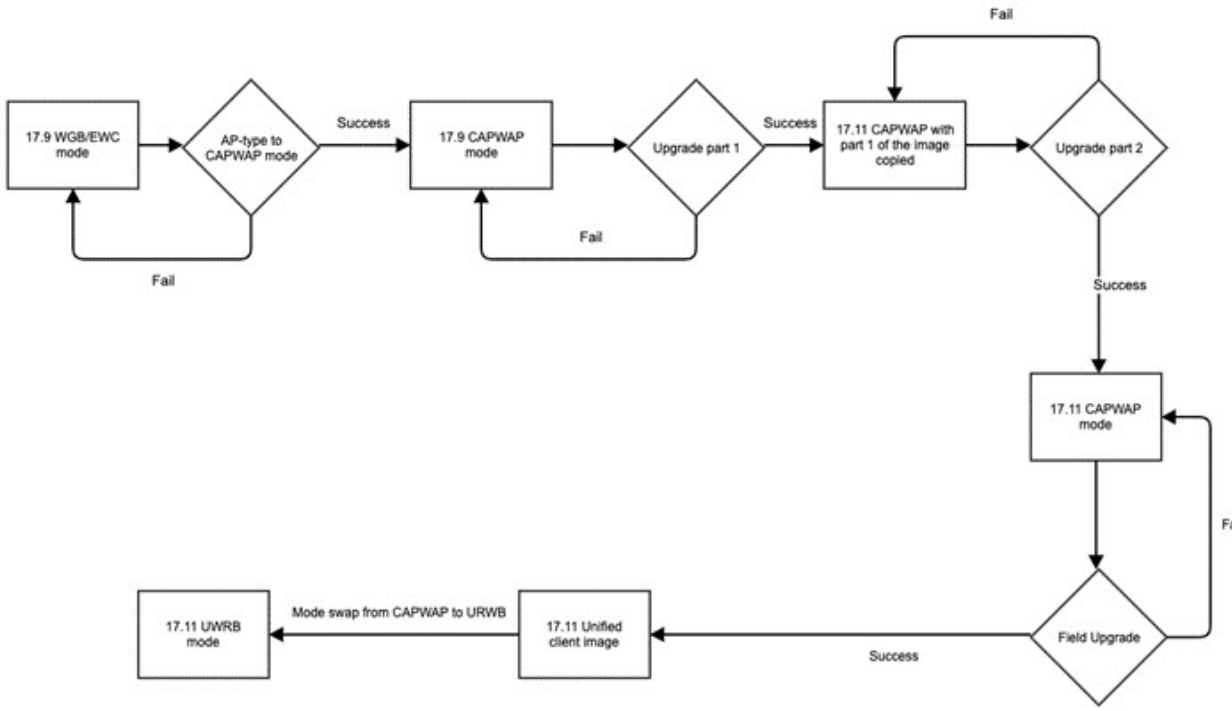
Use Case	CLI
Choose 2.4GHz or 5GHz frequency for the WiFi access or WiFi uplink.	show platform hardware subslot 0/3 module device "config start" show platform hardware subslot 0/3 module device “send_cmd configure dot11Radio <0|1> mode root-ap” show platform hardware subslot 0/3 module device “config end”
Enable Concurrent Radio.	N/A If root-radio is configured, it will be enabled. There is no additional CLI for it. On the Router, configure a unique MAC address for WGB uplink VLAN interface: `interface Vlan <WGB uplink VLAN number> mac-address <unique mac addr>` **Note** <unique mac address> - Derived from GigabitEthernet0/0/0 interface mac address + 4
Configure the SSID profile with a customer-defined name.	show platform hardware subslot 0/3 module device “config start”

Use Case	CLI
Configure SSID (in the profile) with a customer-defined name. Configure the Authentication type (in the profile).	show platform hardware subslot 0/3 module device "config start" show platform hardware subslot 0/3 module device "send_cmd configure ssid-profile <profile-name> ssid <ssid-name> authentication <auth-type> key-management <key-mgmt>" show platform hardware subslot 0/3 module device "config end"
Choose between WGB or uWGB (universal) options.	show platform hardware subslot 0/3 module device "config start" show platform hardware subslot 0/3 module device "send_cmd configure dot11Radio <0/1> mode uwgb <client mac> ssid-profile <ssid>" show platform hardware subslot 0/3 module device "config end" **Note** <client mac> - Wired client mac connected to the IR1800.
Get running configuration. Get Wi-Fi Mode. Get Radio allocated to WGB vs Wi-Fi.	show platform hardware subslot 0/3 module device "show running-config"
Get list of Wi-Fi clients.	show platform hardware subslot 0/3 module device "show controllers dot11 0 client" show platform hardware subslot 0/3 module device " show client summary"
Get hardware status. Get AP status after firmware bootup.	show hw status
Get WGB connection status.	show platform hardware subslot 0/3 module device "show wgb dot11 associations" show platform hardware subslot 0/3 module device "show run"
Get AP Firmware version.	show platform hardware subslot 0/3 module device "show ver"
Radio traffic monitoring for 2.4 & 5Ghz radio.	show platform hardware subslot 0/3 module device "show interface dot11 <0/1>"

Firmware Upgrade

The firmware on the Cisco Wi-Fi Interface Module (WIM) needs to be upgraded from Cisco IOS XE release 17.9.1 to 17.11.1a. In order to perform the upgrade, the WIM needs to be in CAPWAP mode.

The following figure illustrates the work-flow to upgrade the module:



Prerequisites

The following prerequisites exist:

- There must be a network connection between the IR1800 and the AP.
- The IR1800 will need a tftp server enabled for the AP to obtain the images.

Upgrade Steps

This section provides the steps to upgrade the AP Firmware.

Procedure

Step 1 If not already in CAPWAP mode, convert from your existing mode to CAPWAP.

Example:

```
# ap-type capwap
AP serving in WGB mode, system will reboot when ap type is changed to CAPWAP.
Do you want to proceed? (y/n): Y
```

a) Reload the device.
b) Log back in with Username/Password.

Step 2 Upgrade the CAPWAP 17.11.1a images.

a) **archive download-sw /reload tftp://***<IP of IR1800 TFTP>***/ap1g8-k9w8-tar.***<version>**
b) The device will reload automatically.
c) Log back in with Username/Password.

Step 3 Upgrade the second image.

a) **archive download-sw /reload tftp://***<IP of IR1800 TFTP>***/ap1g8t-k9c1-tar.***<version>**
b) Allow the image to upgrade.

```
*****************************************************
Detected field upgrading URWB by CAPWAP image...
New URWB image will be added into flash, but EWC will be removed.
Are you sure to proceed? (y/n) Y
```

c) The device will reload automatically.
d) Log back in with Username/Password.

Step 4 Once the upgrade is completed, the **configure boot mode** command can be used to swap from CAPWAP to URWB mode.

```
#configure boot mode urwb
Image swapping will restore the device to factory settings.
Are you sure to proceed? (y/n) Y
```

Step 5 You can verify the AP version with the **show version** command.

```
#show version
Cisco AP Software, (ap1g8t), [build-info]
Processor board ID FOC251943PG
AP Running Image     : 11.4.8.87
Primary Boot Image   : 11.4.8.87
Backup Boot Image    : 11.4.8.87
```

What to do next

If you want to perform a downgrade from Cisco IOS XE release 17.11.1a back to 17.9.1, perform the following:

```
#archive download-sw /reload tftp://<IP of IR1800 TFTP> /ap1g8
```

The image will download and the device will reload. The device comes back up in CAPWAP mode using Cisco IOS XE 17.9.1

Switch Between CAPWAP and WGB Mode

In Cisco IOS XE 17.11.1a, support has been added for switching the Cisco Wi-Fi Interface Module (WIM) running mode between Control and Provisioning of Wireless Access Points Protocol (CAPWAP) mode and workgroup bridge (WGB) concurrent radio mode. This feature applies to the WIM that already has the CAPWAP image on Cisco IOS XE 17.11.1a and the unified client image.

The following table shows the command and corresponding behaviors to support the switch mode operation:

Current Mode	Target Mode	CLI	Behavior
CAPWAP	WGB concurrent radio	show platform hardware subslot 0/3 module device "config start" show platform hardware subslot 0/3 module device "configure boot mode wgb" show platform hardware subslot 0/3 module device "config end"	Factory reset and the WP-WIFI6-x will run the unified client image
WGB concurrent radio	CAPWAP	show platform hardware subslot 0/3 module device "config start" show platform hardware subslot 0/3 module device "configure boot mode capwap" show platform hardware subslot 0/3 module device "config end"	Factory reset and the WP-WIFI6-x will run the CAPWAP image