

Cisco LoRa WAN Deployment Guide

A Prescriptive Guide for beginners .

Table of Contents

Getting Started	3
<i>Installing IR1101 Router</i>	3
<i>Installing IR1800 Router</i>	3
<i>Connecting to Router Console via Serial Port.....</i>	4
<i>Introduction to the Web User Interface</i>	4
<i>Setting Your Computer to Connect to the Router WebUI.....</i>	4
<i>Understanding Licensing options</i>	4
<i>Image upgrade on IR1101</i>	4
<i>Understanding Application Hosting</i>	4
<i>About Local Manager.....</i>	4
<i>Cisco 4G LTE-Advanced Configuration</i>	4
Sample Deployment Work sheet	5
Few LoRa Deployment Considerations	5
Bringing up Actility Packet forwarder on Routers	8
Actility -Thing Park Network Server Options.....	20
Actility – Packet forwarder as Docker App and naming conventions.....	21
Actility -TPE – OCP step by steps.....	21
Bringing up Common packet forwarder on Routers:	30
ChirpStack – Step by Steps:	38
Sample running configuration with Common packet forwarder:.....	44
Appendix:	48

Getting Started :

Note: The Following indexes has soft links to cisco documents , please use ecopy for the hyperlinks to work, avoid printing.

<i>IR1100 Product Overview</i> <i>Installing IR1101 Router</i> <ul style="list-style-type: none">a. <i>Optional - Antenna Selection and Installation</i>b. <i>Optional - Installing the IRM-1100 Expansion Module</i>c. <i>Optional - IR1101 Technical Specifications Details</i>	IR1101 product Guides
<i>IR1800 Product Overview</i> <i>Cisco IR1800 Series Platform Features</i> <i>Installing IR1800 Router</i> <ul style="list-style-type: none">a. <i>Antennas for the IR1800 Series Router</i>b. <i>Installing Pluggable Interface Modules</i>	IR1800 Product Guides

<p>Connecting to Router Console via Serial Port</p> <ul style="list-style-type: none"> a. <i>Baud rate settings</i> b. <i>Mandatory: Drivers to download</i> 	<p>Connecting to Router Serial Console via Serial cable., cable and reference links console cable (Cisco P/N CAB-CONSOLE-USB, 6ft long)</p> <p>Note: when managing device locally using CLI we tend to use the serial console and connect to router CLI prompt</p>
<p>Introduction to the Web User Interface</p> <ul style="list-style-type: none"> a. <i>WebUI Dashboard</i> b. <i>Day o Cellular Mode</i> c. <i>Configuration Notes</i> 	<p>WebUI introduction, managing the device locally and usage of WebUI in day zero cellular mode</p>
<p>Setting Your Computer to Connect to the Router WebUI</p> <ul style="list-style-type: none"> a. <i>Choosing Basic Mode option on WebUI</i> b. <i>Choosing Advanced Mode WebUI</i> 	<p>Choice of WebUI basic mode and advanced mode</p>
<p>Understanding Licensing options</p> <ul style="list-style-type: none"> a. <i>Cisco Software Licensing</i> b. <i>Consolidated Packages</i> c. <i>Network-Essentials</i> d. <i>Network-Advantage</i> 	<p>Know about licensing options</p> <p>Note: Network advantage is must for LoRa PIM to work</p>
<p>Image upgrade on IR1101</p> <ul style="list-style-type: none"> a. <i>Installing the IOS-XE Software image</i> b. <i>Understanding ROMMON Images</i> c. <i>know about Supported File Systems</i> d. <i>Enabling and Disabling USB access</i> e. <i>Autogenerated File Directories and Files</i> f. <i>Flash Storage</i> g. <i>know about LED Indicators</i> h. <i>Related Documentation</i> 	<p>Know about image upgrade and other details about device filesystem and enabling and disabling usb, led status and other related topics.</p> <p>Note: LoRa PIM is supported from 17.10.1 release on wards. It's important to upgrade your box to latest image</p>
<p>Understanding Application Hosting</p> <ul style="list-style-type: none"> a. <i>Application Hosting</i> b. <i>Information About Application Hosting</i> c. <i>Application Hosting on the IR1101 Router</i> d. <i>How to Configure Application Hosting</i> e. <i>Installing and Uninstalling Apps</i> f. <i>Overriding the App Resource Configuration</i> g. <i>Verifying the Application Hosting Configuration</i> h. <i>Configuration Examples for Application Hosting</i> 	<p>Detail document about application hosting, how to configure and install and manage the apps using CLI and few examples.</p> <p>Note: we are supporting packet forwarders as docker app. How to install and manage app on routers is critical step to learn.</p>
<p>About Local Manager</p> <ul style="list-style-type: none"> a. <i>Overview</i> b. <i>Cisco IOx Local Manager Pages and Options</i> c. <i>Cisco IOx Local Manager Workflows</i> 	<p>Using local manager for app deployment and description of various tabs under local manager. Local manger is specifically designed to help manage app on routers</p> <p>Note: we can manage app life cycle using local manager. Understanding app management via local manager helps.</p>
<p>Cisco 4G LTE-Advanced Configuration</p>	<p>Document links to the cellular provision on IR1101 and IR1800.</p>

Sample Deployment Work sheet

Router	PIM module	Network server + Docker App	WAN choice
	915 815		
IR1101	P-LPWA-900	Chirp Stack + CPF	GE
IR1800	P-LPWA-800	Thingpark + Actility Packet Forwarder	Cellular - select a proper cellular PIM module

Few LoRa Deployment Considerations

a. Platform Choice: IR1101 vs IR1800

Refer to platform documentation for hardware and technical specifications to see which device meets your requirements.

b. PIM choice: 915 PIM vs 815 PIM module

Currently we support two different pluggable interface modules

- P-LPWA-900 for 915 MHz
- P-LPWA-800 for 868 MHz

c. PIM slot choice: LORA PIM module in Base slot vs Expansion slot on IR1101

For IR1101 and existing deployment where the Base PIM slot is being used for cellular, we recommend using expansion slot for lora PIM. For the IR1800 we recommend using whichever PIM slot is available.

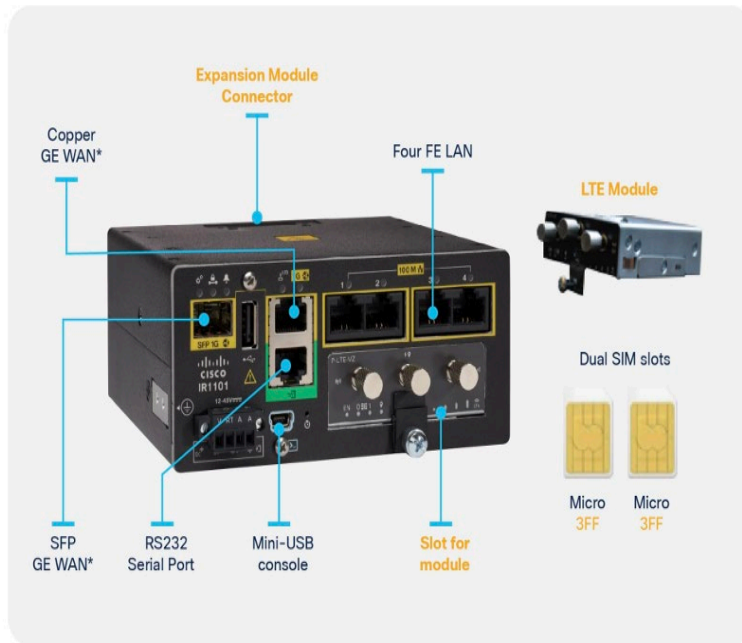


Figure 1.
Cisco IR1101 base platform front view



Figure 2.
Expansion Modules

Supported Scenario's with IR1101

- ✓ IR1101 Base Module + LoRa PIM (lorawan_tty0)
- ✓ IR1101 Base Module + IRM1100 SPMI Expansion Module with PIM module
- ✓ IR1101 Base Module + IRM1100SP EM with PIM module

As a standalone indoors with ethernet backhaul



PIM in base slot will show as lorawan 0/1/0
 PIM in EM slot will show as lorawan 0/3/0
lorawan_tty1,lorawan_tty3 will be interchangely used

d. LORA PIM module support in all the IR1800 pids

PIM slots are available on IR1812, IR1831, IR1833, IR1835 , any choice of PIM slot can work across all SKUs.



IR1821-K9

- 1 cellular slot, 1 Wi-Fi slot
- 4 GB memory
- CAN bus



IR1831-K9

- 2 cellular slots, 1 Wi-Fi slot
- 4 GB memory
- CAN bus



IR1833-K9

- 2 cellular slots, 1 Wi-Fi slot
- 4 GB memory
- CAN bus, PoE/PoE+, ADR GNSS slot, SSD slot



IR1835-K9

- 2 cellular slots, 1 Wi-Fi slot
- 8 GB memory
- CAN bus, PoE/PoE+, ADR GNSS slot, SSD slot
- 4 digital I/O ports, advanced security features, 1 RS232/485 combo port

Cisco Catalyst IR1800 Portfolio

IR1821-K9



Pluggable Side

IR1831-K9



Pluggable Side

IR1833-K9



Pluggable Side

IR1835-K9



Pluggable Side

e. WAN Choice: GE or Cellular

Typical enterprise deployments vs field deployment, a GE o/o/o can be used as WAN for enterprise and extended enterprise cases where we have cable reach.

For outdoor deployments we can choose cellular as WAN as well. Please make sure to have a valid Cellular module and working SIM card and proper cellular data plan in place before making the cellular as WAN.

f. Packet forwarder choice: “Common packet forwarder (CPF)” vs “Activity packet forwarder” (APF)

We support two packet forwarders based on your choice of network server we can use common packet forwarder or Activity packet forwarder.

g. CPF authentication choice: Choice of authentication with CPF deployment

Common packet forwarder supports various kinds of authentication.

```
IR1101 (config-if-lorawan-cpf)#auth-mode ?
  client-server  client and server authentication mode
  server         authentication mode
  sudi           cisco sudi authentication mode
```

h. Choice of security with Activity deployment

Public key and then IPsec tunnel with strong swan server.

i. Choice of Sensor support class A/B/C

Currently we support Class A and Class C sensors only. Class B will be supported in the next release on CPF.

j. Choice of Network server: chirp stack vs Thingpark.

Open-source network server vs engineered Thingpark solution is a customer choice.

Bringing up Activity Packet forwarder on Routers

Bringing up Cellular WAN interface , please refer to the following guide.

[Cisco 4G LTE-Advanced Configuration](#)

Important Notes:

- Actility packet forwarder need some prerequisite setting for the app to ssh to the Router CLI prompt and provision the authentication keys between iox app and the host CLI.
- Use the following on Router config cli /HOST:
 - add a new username:password , which is specific to Actility only.
 - config terminal
 - username actility privilege 15 password 0 actilityPassword
 - exit
 - add/run docker container with the following options (here you can see the default ip addr, user and password but you'll need to change them according to your config):
 - --device /dev/ttyACM0:/dev/ttyACM0
 - --env HOST_IP_ADDR=192.168.42.11
 - --env HOST_USER=actility
 - --env HOST_SETUP_PASSWORD=actilityPassword
 - Once the app is activated and working You'll see that the provisioned password is deleted and new one is created by app it self .Notice that we do not have a password for the actility user anymore (username actility privilege 15).
 - If you want to reinstall the lrr packet forwarder app again in future, you'll have to set again username actility privilege 15 password 0 actilityPassword
 - An APP upgrade won't erase these credentials.
 - Latest packages include other docker run time options to support the LRR.ini file configuration for TPE - OCP deployments

To configure application hosting, enable IOx and configure a VirtualPortGroup to a Layer 3 data port as described in the following sections.

Step 1: Enable IOx

Perform the following steps to enable access to Cisco IOx Local Manager. IOx Local Manager provides a web-based user interface that you can use to manage, administer, monitor, and troubleshoot apps on the host system, and to perform a variety of related activities

1. Enter the following command to enable privileged EXEC mode:
Device> enable
2. Enter this command to enter global configuration mode:
Device# configure terminal
3. Enter this command to enable Cisco IOx:
Device(config)# iox
4. Enter this command to enable the HTTP server on your IPv4 or IPv6 system:
Device(config)# ip http server
5. Enter this command to enable a secure HTTP (HTTPS) server:
Device(config)# ip http secure-server
6. Use the following command to establish a username-based authentication system and privilege level. The username privilege level must be configured as 15.
Command format:
`username name privilege level password {0 | 7 | user-password } encrypted-password`
Command example:
Device(config)# username cisco privilege 15 password 0 cisco
7. Enter this command to exit the interface configuration mode and return to the privileged EXEC mode:
Device(config-if)# end

Step 2 : Configure a VirtualPortGroup to a Layer 3 Data Port

Multiple Layer 3 data ports can be routed to one or more VirtualPortGroups or containers. A VirtualPortGroup interface is a virtual interface that connects the application hosting network to the IOS routing domain. VirtualPortGroups and Layer 3 data ports must be on different subnets.

To configure a VirtualPortGroup to a Layer 3 data port, follow these steps:

1. Enter the following command to enable privileged EXEC mode. Enter your password if prompted.
Device> **enable**
2. Enter the following command to enter global configuration mode:
Device# **configure terminal**
3. Enter the following command to enable IP routing. The ip routing command must be enabled to allow external routing on Layer 3 data ports.
Device(config)# **ip routing**
4. Use the following command to configure an interface and enter interface configuration mode.
Command format: *interface type number*
Command example: Device(config)# **interface gigabitethernet 0/0/0**
5. Enter the following command to place the interface in Layer 3 mode and make it operate more like a router interface than a switch port:
Device(config-if)# **no switchport**
6. Use the following command to configure an IP address for the interface.
Command format: *ip address ip-address mask*
Command example: Device(config)# **ip address dhcp**
7. Enter the following command to exit interface configuration mode and return to global configuration mode:
Device(config-if)# **exit**
8. Use the following command to configure an interface and enter interface configuration mode.
Command format: *interface type number*
Command example: Device(config)# **interface virtualportgroup 0**
9. Use the following command to configure an IP address for the interface.
Command format: *ip address ip-address mask*
Command example: Device(config-if)# **ip address 192.168.2.1 255.255.255.0**
10. Enter the following command to exit interface configuration mode and return to privileged EXEC mode:
Device(config-if)# **end**

Step 3 : Configure Application Networking

Application vNIC interface is the standard Ethernet interface inside the container that connects to the platform data plane for application to send and receive packets.

1. Use the following command to enter global configuration mode, and then enter configuration commands, one per line. Press CTRL-Z when you are finished entering configuration commands.
Device# **configure terminal**

2. Use the following command to configure the application and enter the application configuration mode.

Command format:

Step 4:

```
app-hosting appid app1
```

Command example:

```
Device(config)# app-hosting appid app1
```

1. Use the `app-vnic` command to configure the application interface and the gateway of the application. For example:
Device(config-app-hosting)# **app-vnic gateway0 virtualportgroup 0 guest-interface 0**
2. Use the `guest-ipaddress` command to configure the application Ethernet interface IP address. For example:
Device(config-app-hosting-gateway0)# **guest-ipaddress 192.168.2.9 netmask 255.255.255.0**
3. Use the `app-default-gateway` command to configure the default gateway for the application. For example:
Device(config-app-hosting-gateway0)# **app-default-gateway 192.168.2.1 guest-interface 0**
4. Enter the following command to exit global configuration mode and return to privileged EXEC configuration mode:
Device# **end**

Application Lifecycle Management

This section describes how to install and uninstall apps.

Use the following command to enable privileged EXEC mode:

```
Device> enable
```

Use the following command to install an app from the specified location. The app can be installed from any local storage location such as, flash, bootflash, and usbflasho.

```
Command format:app-hosting install appid application-name package package-path
Command example:
Device(config)# app-hosting install appid APFAPP package flash:actility_tar_gz.tar
```

Use the following command to activate the application. This command validates all application resource requests, and if all resources are available, activates the application. If all resources are not available, the activation fails.

```
Command format:app-hosting activate appid application-name
Command example:Device# app-hosting activate appid APFAPP
```

Use the following command to start the application. This command activates the application start-up scripts.

```
Command format:app-hosting start appid application-name
Command example: Device# app-hosting start appid APFAPP
```

Use the following command to stop the application.

```
Command format:app-hosting stop appid application-name
Command example:Device# app-hosting stop appid APFAPP
```

Use the following command to deactivate all resources that are allocated for the application.

```
Command format:app-hosting deactivate appid application-name
Command example: Device# app-hosting deactivate appid APFAPP
```

Use the following command to uninstall the application. This command uninstalls all packaging and images that are stored and removes all changes and updates to the application.

```
Command format: app-hosting uninstall appid application-name
Command example: Device# app-hosting uninstall appid APFAPP
```

Step 5: Verifying the Application Hosting Configuration

This section describes how to verify the application hosting configuration.

1. Use the following command to enable privileged EXEC mode:
Device> enable
2. Use the following command to display the status of all IOx services:
Device# show iox-service
Router#show iox-service

IOx Infrastructure Summary

IOx service (CAF) Running
IOx service (HA) Not Supported
IOx service (IOxman) Running
IOx service (Sec storage) Running
Libvirt 5.5.0 Running
Dockerd v19.03.13-ce Running
3. Use the following command to display detailed information about the application:
Device# show app-hosting detail
4. Use the following command to display the list of applications and their statuses:
Device# show app-hosting list
App id State

APFAPP RUNNING
5. Use the Console command to connect to the application, as shown in the following example:
iox-ir1101-02# app-hosting app-hosting connect appid APFAPP session

/home/actility/var/log/lrr
/var/volatile/log/_LRRLOG # pwd
/home/actility/var/log/lrr
/var/volatile/log/_LRRLOG # ls -lrt
-rw-r--r-- 1 root root 19 Jul 7 0646 SHELL.log
-rw-r--r-- 1 root support 53 Jul 7 0647 suplog.log
-rw-r--r-- 1 root support 99 Jul 7 0648 pkiconfig.txt
-rw-r--r-- 1 root root 430 Jul 7 0720 lrr_startup_service.log
-rw-r--r-- 2 root root 1620 Jul 7 0721 gwmgr_04.log
-rw-r--r-- 2 root root 1620 Jul 7 0721 gwmgr.log
-rw-r--r-- 1 root root 1657 Jul 7 0721 radioparams.txt
-rw-r--r-- 1 root root 2227 Jul 7 0721 logicchan.txt
-rw-r--r-- 1 root root 1118 Jul 7 1721 stat.html
-rw-r--r-- 2 root root 50515 Jul 7 1721 TRACE_04.log
-rw-r--r-- 2 root root 50515 Jul 7 1721 TRACE.log
-rw-r--r-- 1 root root 64 Jul 7 1723 lrcstatuslink.txt
/var/volatile/log/_LRRLOG #


```

!
!
!
!
!
crypto pki trustpoint TP-self-signed-1150468717
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-1150468717
  revocation-check none
  rsakeypair TP-self-signed-1150468717
!
crypto pki trustpoint SLA-TrustPoint
  enrollment pkcs12
  revocation-check crl
!
crypto pki trustpoint ActilityTP-slrc
  enrollment terminal
  revocation-check none
!
crypto pki trustpoint ActilityTP
  enrollment pkcs12
  revocation-check crl
  rsakeypair ActilityTP
!
crypto pki trustpoint ActilityTP-rrr1
  revocation-check crl
!
!
!
crypto pki certificate map FlexVPN_Cert_Map 1
  subject-name co slrc1_prod-us_actility-tpe-ope
!
crypto pki certificate map FlexVPN_Cert_Map 2
  subject-name co slrc2_prod-us_actility-tpe-ope
!
crypto pki certificate chain TP-self-signed-1150468717
  certificate self-signed 01
crypto pki certificate chain SLA-TrustPoint
  certificate ca 01
crypto pki certificate chain ActilityTP-slrc
  certificate ca 61A845069BBFF60B
crypto pki certificate chain ActilityTP
  certificate 06BF5FDCF5EBD17C
  certificate ca 3A96CABF858AAD9A
crypto pki certificate chain ActilityTP-rrr1
  certificate ca 00F35AC229699BABA8
!
!
!
!
!
!
!
!
!
no license feature hseck9
license udi pid IR1101-K9 sn FCW24160HQ7
license boot level network-advantage
memory free low-watermark processor 45069
!
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
!
!
username admin privilege 15 password 0 cisco
username iox privilege 15 password 0 iox
username dockeruser

```



```

username actility privilege 15
!
!
redundancy
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
!
!
!
!
crypto ikev2 profile FlexVPN_IKEv2_Profile
match certificate FlexVPN_Cert_Map
identity local dn
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint ActilityTP sign
pki trustpoint ActilityTP-rrr1 verify
pki trustpoint ActilityTP-slrc verify
dpd 30 3 periodic
aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy
!
crypto ikev2 dpd 30 3 periodic
crypto ikev2 fragmentation mtu 1260
!
controller Cellular 0/3/0
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
!
!
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes 256 esp-sha256-hmac
mode tunnel
!
crypto ipsec profile FlexVPN_IPsec_Profile
set transform-set FlexVPN_IPsec_Transform_Set
set ikev2-profile FlexVPN_IKEv2_Profile
!
!
!
!
!
!
!
!
!
!
!
interface Tunnel201
ip address negotiated
ip nat outside
ipv6 enable
tunnel source GigabitEthernet0/0/0
tunnel mode ipsec dual-overlay
tunnel destination 52.200.161.236
tunnel path-mtu-discovery
tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Tunnel202
ip address negotiated
ip nat outside
ipv6 enable
tunnel source GigabitEthernet0/0/0

```

```

tunnel mode ipsec dual-overlay
tunnel destination 54.226.90.83
tunnel path-mtu-discovery
tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface VirtualPortGroup0
 ip address 192.168.2.1 255.255.255.0
 ip nat inside
 no mop enabled
 no mop sysid
!
interface GigabitEthernet0/0/0
 ip dhcp client client-id ascii cisco-ac4a.67f9.ae00-Gi0/0/0
 ip address dhcp
 ip nat outside
 ipv6 dhcp client request vendor
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
interface FastEthernet0/0/1
!
interface FastEthernet0/0/2
!
interface FastEthernet0/0/3
!
interface FastEthernet0/0/4
!
interface GigabitEthernet0/0/5
!
interface Cellular0/3/0
 description backup_WAN
 ip address negotiated
 ip nat outside
 ip tcp adjust-mss 1460
 load-interval 30
 shutdown
 dialer in-band
 dialer idle-timeout 0
 dialer-group 1
 ipv6 enable
 pulse-time 1
!
interface Cellular0/3/1
 no ip address
!
interface Vlan1
 no ip address
!
interface Async0/2/0
 no ip address
 encapsulation scada
!
interface LORAWAN0/1/0
 no ip address
 shutdown
 arp timeout 0
 no mop enabled
 no mop sysid
!
iox
 ip forward-protocol nd
 ip tcp selective-ack
 ip tcp mss 1460
 ip tcp window-size 131072
 ip http server
 ip http auth-retry 3 time-window 1
 ip http authentication local
 ip http secure-server

```

```

ip http client source-interface GigabitEthernet0/0/0
ip tftp source-interface GigabitEthernet0/0/0
ip nat inside source list Tunnel201 interface Tunnel201 overload
ip nat inside source list Tunnel202 interface Tunnel202 overload
ip nat inside source list internetacces_Fromdocker interface GigabitEthernet0/0/0 overload
ip nat inside source list internetacces_Fromdocker_cell interface Cellular0/3/0 overload
ip route 10.102.12.0 255.255.255.0 Tunnel201
ip route 10.102.22.0 255.255.255.0 Tunnel202
ip ssh bulk-mode 131072
ip ssh version 2
ip ssh pubkey-chain
    username actility
    key-hash ecdsa-sha2-nistp256 FA249B09C77A121A9759A0FC724F58A8 root@a89e080e0c1e
ip ssh server algorithm publickey ecdsa-sha2-nistp256
ip scp server enable
!
!
ip access-list extended Tunnel201
    10 permit ip host 192.168.2.9 host 10.102.12.10
ip access-list extended Tunnel202
    10 permit ip host 192.168.2.9 host 10.102.22.10
ip access-list extended internetacces_Fromdocker
    10 permit ip 192.168.2.0 0.0.0.255 host 8.8.8.8
    11 permit ip 192.168.2.0 0.0.0.255 host 52.200.161.236
ip access-list extended internetacces_Fromdocker_cell
    10 permit ip host 192.168.2.9 host 8.8.8.8
!
!
ip sla 1
    icmp-echo 8.8.8.8 source-interface GigabitEthernet0/0/0
ip sla schedule 1 life forever start-time now
ip sla 2
    icmp-echo 8.8.8.8 source-interface Cellular0/3/0
ip sla schedule 2 life forever start-time now
ip access-list standard 1
    11 permit any
dialer-list 1 protocol ip permit
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
line con 0
    stopbits 1
line 0/0/0
line 0/2/0
line vty 0 4
    transport input ssh
line vty 5 14
    transport input ssh
!
call-home
    ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
    ! the email address configured in Cisco Smart License Portal will be used as contact email address to
    send SCH notifications.
    contact-email-addr sch-smart-licensing@cisco.com
    profile "CiscoTAC-1"
    active
    destination transport-method http
ntp server 0.pool.ntp.org

```

```

ntp server 1.pool.ntp.org
ntp server 2.pool.ntp.org
!
!
!
!
!
!
!
!
!
!
!
!
!
!
event manager applet restart_actility_lrr
  event none sync yes maxrun 60
  action 1 cli command "enable"
  action 2 cli command "app-hosting stop appid APFC1"
  action 3 wait 5
  action 4 cli command "app-hosting start appid APFC1"
event manager applet Cellular_Activate
  event track 1 state down
  action 1 cli command "enable"
  action 2 cli command "configure terminal"
  action 3 cli command "interface Cellular 0/3/0"
  action 4 cli command "no shut"
  action 5 cli command "end"
event manager applet Cellular_Deactivate
  event track 1 state up
  action 1 cli command "enable"
  action 2 cli command "config terminal"
  action 3 cli command "interface Cellular 0/3/0"
  action 4 cli command "shutdown"
  action 5 cli command "end"
!
end
Router#

```

Activity -Thing Park Network Server Options

a. About Activity Thingpark -Enterprise On Premise Platform / TPE – OCP

This deployment is an enterprise based on prem deployment and it considered as most secured and the **Thingpark server is deployed in the local site enterprise network** and is reachable via IR1101 or IR1800 GE o/o/o port.

Once the app is installed the LRR packet forwarder will contact the TPE-OCP via WAN port and forwards the sensor traffic to TPE dashboard.

b. About Activity Thingpark Community / TPE – Community

A self-service Device and Application makers portal to build their solutions with Thingpark.

Please refer to following URL <https://community.thingpark.org/iot-solutions-catalog/> for more details and login , the navigation should be same as that of TPE – OCP.

c. About Actility Thingpark SaaS / TPE – SaaS

The Cloud deployment of Thingpark dashboard for enterprises as SaaS. Based on the location of the customer and the geography we use various cloud url for connecting to TPE-SaaS. Please make a note that this deployment is not secure, and you need tunnels / certs / and have a make a choice of WAN if your device is remotely deployed, unlike TPE-OCP (on prem).

- <https://thingparkenterprise.us.actility.com/tpe/#/login>
- <https://thingparkenterprise.eu.actility.com/tpe/#/login>
- <https://thingparkenterprise.au.actility.com/tpe/#/login>





Actility – Packet forwarder as Docker App and naming conventions

Actility packet forwarders are docker apps that are sharing with various labels. We use the following label conventions to describe the app type accordingly.

- a. Label **TPE_OCP** – *designated for enterprise reach.*
- b. Label **TPCP** – *designated community portal reach.*
- c. Label **TPE_SaaS EU** -*designated for Europe server reach*
- d. Label **TPE_SaaS US** -*designated for US server reach*

Note : Please refer to the sample screen shot on how the packages are designated with label. You must make a right choice of selection as per your choice if Thingpark deployment.

Sample Screen shot:

NAME
 Cisco_iox_lrr_build_ThingPark_Tpe_OCP.nfr920_2022-10-07.tar.gz
 Cisco_iox_lrr_build_ThingPark_Tpe_SAAS_TPCP.nfr920_2022-10-0...
 Cisco_iox_lrr_build_ThingPark_Tpe_SAAS_EU.nfr920_2022-10-07.t...
 Cisco_iox_lrr_build_ThingPark_Tpe_SAAS_US.nfr920_2022-10-07.t...

Actility -TPE – OCP step by steps

a. TPE OCP/CP/SaaS login

Please use the following url for TPE SaaS login, and make sure either you have required credentials to login or register if you need one. Your IT admin should be a provide you required credentials for you to login.

TPE SaaS Portal Access

Direct your browser to the appropriate TPE SaaS URL:
<https://thingparkenterprise.eu.actility.com/>
<https://thingparkenterprise.au.actility.com/>
<https://thingparkenterprise.us.actility.com/>

Enter credentials for your TPE SaaS account.

Activity

Email

Password

Forgotten password?

LOG IN

b. Understanding Dashboard Page

TPE Portal Dashboard

Display the TPE version when pointing the mouse

Gateways status

Devices status

Dashboard menu

Applications status

BASE STATIONS

DEVICES

RECENT ALARMS

NEWS

APPLICATIONS

Application Name	Application ID	Devices
No data found.		

c. Adding a Base station

Get the LRR UID from Actility support tool

Once the app is installed and running fine, we have a way to console the app session using app-hosting connect app-id APFx session and use su support account to get to the actility support tool.

```
Router#app-hosting connect appid APFC1 session
/ #
/ # su support
```

Get the LRR ID and public keys required.

The support tool is a command utility tool. Please use tab and escape up down arrows on the keyboard to control and highlight the button and press enter to get the next prompt.



Click here to configure status bar
Actility support tool 2.8.17

```
-----BEGIN PUBLIC KEY-----
MIGFMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDFdjkHUsF/P1REDFPpMBmko70
F8tV3oZTL1z+q76yqwnBKz1y91FNsDeN4RAPaVG+2wmjB81wp4RQsBqF92B+/-BJ
iRrzVGARTvmArs1vnJ9uYNIPICHIZa4/ymuxrzDtyHqEUhPvCDUTXh3RAzzHF7X
VcvcaadNYXFSQS/29QIDAQAB
-----END PUBLIC KEY-----
```


Note: You can generate a public key if there is none ,use generate public key option from identifiers

Add GW to the TPE: We return to the TPE screen that we left a few steps ago.

- Complete the fields appropriately
- Use the LRRUID that you captured in a previous step
- Make sure” IPsec for base station to TPE connection” is enabled

- Make sure “Disable public key authentication” is unchecked, and paste public key gathered in previous step
- Press “Save” and check for confirmation

Base Station Manufacturer*



Cisco
A leading company in wireless communication technologies including network equipments and IoT solutions.
[Change manufacturer?](#)

Enter Your Base Station Information*

Model* ⓘ

IR1101 (with LoRa module) ▼

Download the base station documentation

Download the base station image

Name* ⓘ

Test ✔

LRR UUID* ⓘ

005FB6-024B06644473F ✔

RF Region* ⓘ

US 915MHz (72 channels) ▼

IPsec (X.509) for base station to TPE connection ⓘ

Enabled ▼

Additional Information ⓘ

Write here....

Disable public key authentication

Public key ⓘ

MlQGMADGCSqGSIIB3DQEBRQJAAKGNADCBQK5gQDfDjRkN08f7PpREDFpMBMk070
 fBY5ozTL1z476yewNBK2iy9ITNsDeNARApaVG+2wmjBB7wp4RQsBafX92B+1BJ
 iRrzVGARtvmArslvnJ9uYNIPICHIZa4/jmuxrzdDtyHqEUhPvCDUTXh3RAz2HF7X
 VcvcaaNYVXf5QS/29QIDAQAB
 -----END PUBLIC KEY-----

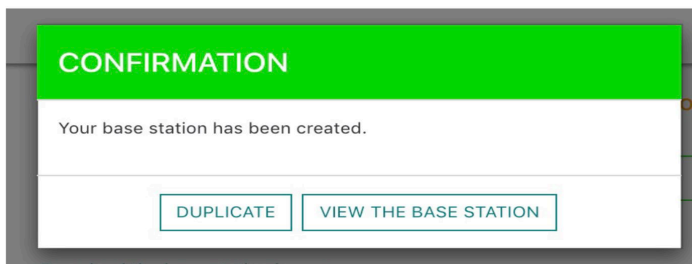
Set Your Base Station Location

To display the base station on the map, enter the coordinates where it will be located.

Mode ⓘ

Onboard GNSS position ▼

CANCEL
SAVE

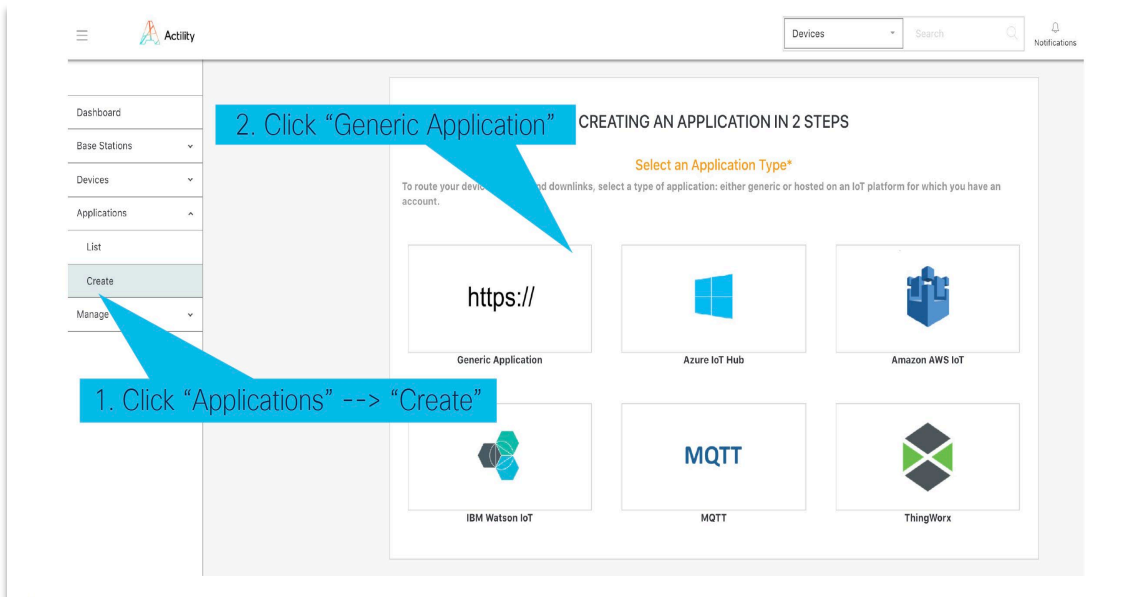


d. Add TPE application

- Before adding a sensor device, we must first define application(s) to which the sensor data will flow.
- POSThere.io is a useful tool for viewing and debugging HTTP POSTs.
- As an example, we will set-up TPE to send sensor data to POSThere.io.
- Please navigate to <https://posthere.io>



1. Copy this link into your clipboard, then click the link



Set Your Application*

Enter the values corresponding to your generic application parameters.

- Populate the fields as shown to the right. Note, your POSThere URL will be unique (from the previous step).
- Please leave the tunnel interface key, as is; it isn't used when interfacing to POSThere.
- Click "save"

Name*

URL*

Content Type*

Tunnel Interface Authentication Key*

Additional Information

CONFIRMATION

Your application has been created.

e. Adding a sensor

Please make sure you have the Sensor related info as DEVEUI, APPKEY, JoinEUI etc.

Dashboard

Base Stations <

Devices ^

List

Create

Import


Applications <

Manage


CREATING A DEVICE IN 3 STEPS

about your device to create and register it in your IoT network.


Select Your Device Manufacturer*




Generic




NKE-Wattec




Adeunis RF



Finsecur



Multitech



View More Manufacturers

1. Click "Devices" → "Create"

2. Click "Generic"

Enter Your Device Information*

Model*

Name*

DevEUI*

Activation mode*

JoinEUI (AppEUI)*

AppKey*

Additional Information

Associate Your Device With Your Application*

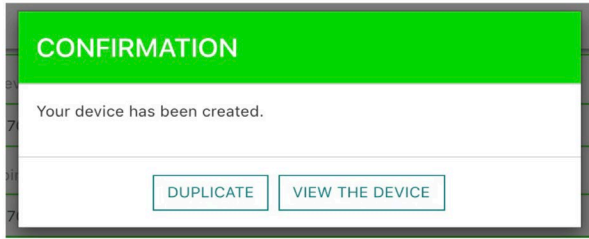
Select the application you want to associate with your device in order to use its data.

Application*

Set Your Device Location

To display the device on the map, enter the coordinates where it will be located.

Mode*

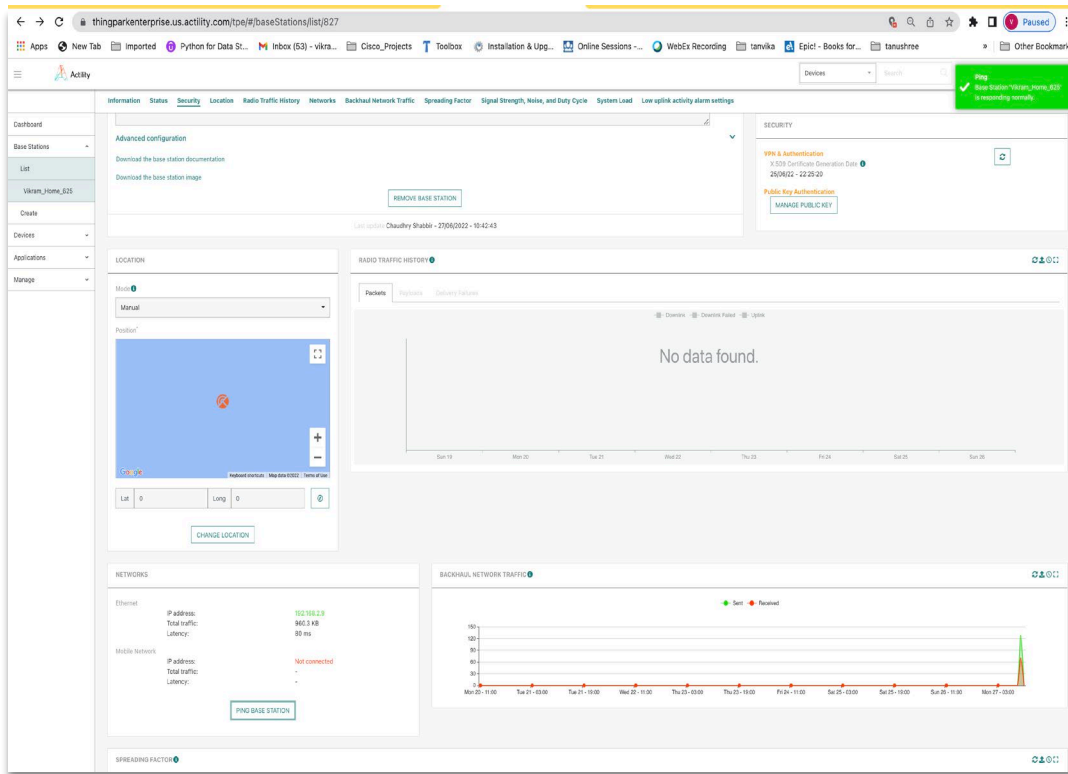


f. Active status

A screenshot of the Cisco Prime Network Manager web interface. The browser's address bar shows the URL "https://10.10.10.10/". The interface is divided into several sections. On the left is a navigation sidebar with options like "Dashboard", "Base Stations", "List", "Create", "Devices", "Applications", and "Manage". The main content area is titled "BASE STATION INFORMATION" and shows the configuration for a device named "Vikram_Home_625". The configuration includes fields for Manufacturer (Cisco), Mode (IR101 (with LoRa module)), LRR ID (10-00-01-14), LRR UUID (000F96-024806644473F), LRR Software Version (2.8.17), and RF Region (US 915MHz (8 channels: CHD-CH7)). There is also a text area for "Additional Information" and a "REMOVE BASE STATION" button at the bottom. On the right side, the "BASE STATION STATUS" section shows the connection status as "CONNECTED" (ACTIVE), LoRaWAN Radio Status as "ON AIR", and Clock Synchronization as "OK". It also displays the Base Station Restart Time as "23/06/22 - 23:34:58" and various performance metrics like "List Uplink", "List Downlink", "Average Uplink Packets", "Average Downlink Packets", and "Last Backup". A "SECURITY" section at the bottom right shows "VPN & Authentication" with a "X.509 Certificate Generation Date" of "25/06/22 - 22:29:20".

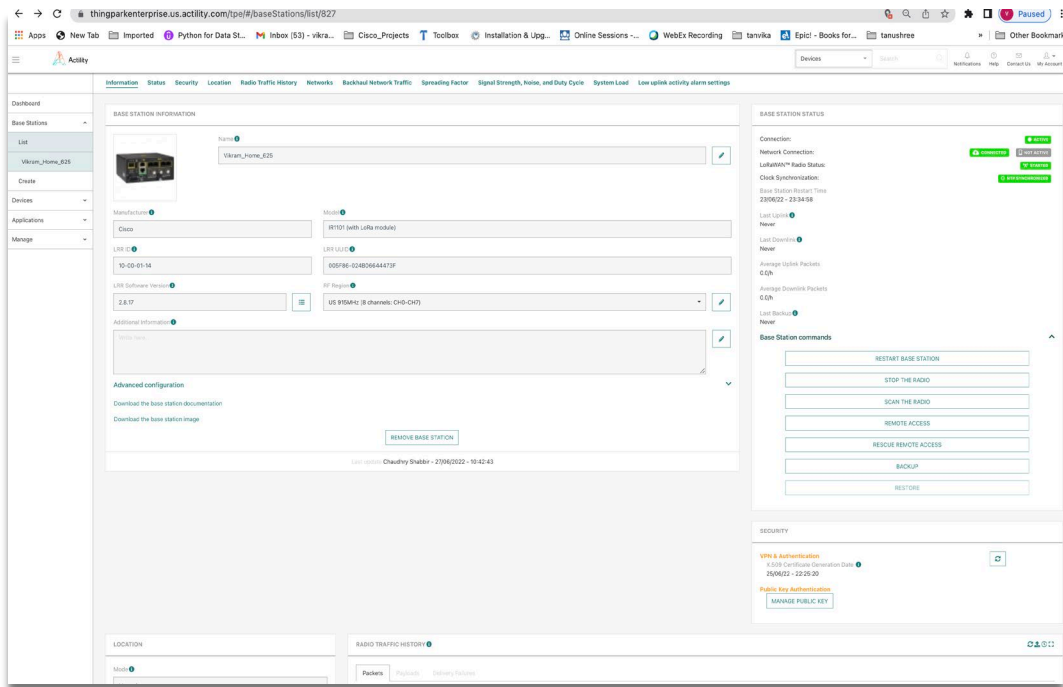
a. Ping check

Performing a ping check will show that the ping is successful to the GW.



i. Base Station command view

Once the device is up, you should be able to see the device connection status showing as green on the right side.



Bringing up Common packet forwarder on Routers:

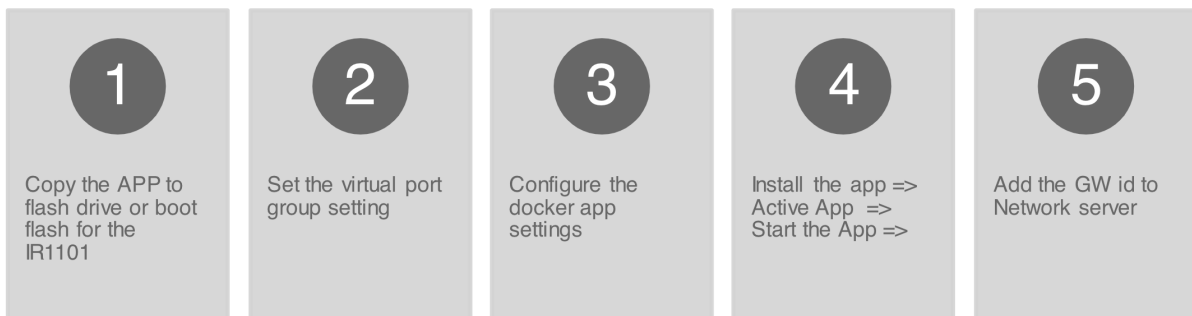
Prerequisites:

- You have a LoRa Network installed – open-source network server
- You have the signed CPF app downloaded from cisco site
- You have the required IR1101 or IR1800 and PIM-LPWA-800|900 module
- Validate license – network advantage license is needed
- GPS connectivity is mandatory for this deployment

Steps to bring up CPF app on IR1101

Before you begin with Common Packet Forwarder:

Order of steps for CPF Docker APP installation



To configure application hosting, enable IOx and configure a VirtualPortGroup to a Layer 3 data port as described in the following sections.

Step 1: Enable IOx

Perform the following steps to enable access to Cisco IOx Local Manager. IOx Local Manager provides a web-based user interface that you can use to manage, administer, monitor, and troubleshoot apps on the host system, and to perform a variety of related activities

8. Enter the following command to enable privileged EXEC mode:
Device> enable
9. Enter this command to enter global configuration mode:
Device# configure terminal
10. Enter this command to enable Cisco IOx:
Device(config)# iox
11. Enter this command to enable the HTTP server on your IPv4 or IPv6 system:
Device(config)# ip http server
12. Enter this command to enable a secure HTTP (HTTPS) server:
Device(config)# ip http secure-server
13. Use the following command to establish a username-based authentication system and privilege level. The username privilege level must be configured as 15.
Command format:
`username name privilege level password {0 | 7 | user-
password } encrypted-password`
Command example:
Device(config)# username cisco privilege 15 password 0 cisco
14. Enter this command to exit the interface configuration mode and return to the privileged EXEC mode:
Device(config-if)# end

Step 2 : Configure a VirtualPortGroup to a Layer 3 Data Port

Multiple Layer 3 data ports can be routed to one or more VirtualPortGroups or containers. A VirtualPortGroup interface is a virtual interface that connects the application hosting network to the IOS routing domain. VirtualPortGroups and Layer 3 data ports must be on different subnets.

To configure a VirtualPortGroup to a Layer 3 data port, follow these steps:

11. Enter the following command to enable privileged EXEC mode. Enter your password if prompted.
Device> **enable**
12. Enter the following command to enter global configuration mode:
Device# **configure terminal**
13. Enter the following command to enable IP routing. The ip routing command must be enabled to allow external routing on Layer 3 data ports.
Device(config)# **ip routing**
14. Use the following command to configure an interface and enter interface configuration mode.
Command format: *interface type number*
Command example: Device(config)# **interface gigabitethernet 0/0/0**
15. Enter the following command to place the interface in Layer 3 mode and make it operate more like a router interface than a switch port:
Device(config-if)# **no switchport**
16. Use the following command to configure an IP address for the interface.
Command format: *ip address ip-address mask*
Command example: Device(config)# **ip address dhcp**
17. Enter the following command to exit interface configuration mode and return to global configuration mode:
Device(config-if)# **exit**
18. Use the following command to configure an interface and enter interface configuration mode.
Command format: *interface type number*
Command example: Device(config)# **interface virtualportgroup 0**
19. Use the following command to configure an IP address for the interface.
Command format: *ip address ip-address mask*
Command example: Device(config-if)# **ip address 192.168.2.1 255.255.255.0**
20. Enter the following command to exit interface configuration mode and return to privileged EXEC mode:
Device(config-if)# **end**

Step 3 : Configure Application Networking

Application vNIC interface is the standard Ethernet interface inside the container that connects to the platform data plane for application to send and receive packets.

1. Use the following command to enter global configuration mode, and then enter configuration commands, one per line. Press CTRL-Z when you are finished entering configuration commands.
Device# **configure terminal**

2. Use the following command to configure the application and enter the application configuration mode.

Command format:

Step 4:

```
app-hosting appid app1
Command example:
Device(config)# app-hosting appid app1
    5. Use the app-vnic command to configure the
        application interface and the gateway of the
        application. For example:
        Device(config-app-hosting)# app-vnic gateway0
        virtualportgroup 0 guest-interface 0
    6. Use the guest-ipaddress command to configure the
        application Ethernet interface IP address. For
        example:
        Device(config-app-hosting-gateway0)# guest-ipaddress
        192.168.2.9 netmask 255.255.255.0
    7. Use the app-default-gateway command to configure the
        default gateway for the application. For example:
        Device(config-app-hosting-gateway0)# app-default-
        gateway 192.168.2.1 guest-interface 0
    8. Enter the following command to exit global
        configuration mode and return to privileged EXEC
        configuration mode:
        Device# end
```

Application Lifecycle Management

This section describes how to install and uninstall apps.

Use the following command to enable privileged EXEC mode:

Device> **enable**

Use the following command to install an app from the specified location. The app can be installed from any local storage location such as, flash, bootflash, and usbflasho.

```
Command format:app-hosting install appid application-name package package-path
Command example:
Device(config)# app-hosting install appid cp package flash:cpf.tar
```

Use the following command to activate the application. This command validates all application resource requests, and if all resources are available, activates the application. If all resources are not available, the activation fails.

```
Command format:app-hosting activate appid application-name
Command example:Device# app-hosting activate appid cp
```

Use the following command to start the application. This command activates the application start-up scripts.

```
Command format:app-hosting start appid application-name
Command example: Device# app-hosting start appid cp
```

Use the following command to stop the application.

```
Command format:app-hosting stop appid application-name
Command example:Device# app-hosting stop appid cp
```

Use the following command to deactivate all resources that are allocated for the application.

```
Command format:app-hosting deactivate appid application-name
Command example: Device# app-hosting deactivate appid cp
```

Use the following command to uninstall the application. This command uninstalls all packaging and images that are stored and removes all changes and updates to the application.

```
Command format: app-hosting uninstall appid application-name
Command example: Device# app-hosting uninstall appid cp
```

Step 5: Verifying the Application Hosting Configuration

This section describes how to verify the application hosting configuration.

1. Use the following command to display detailed information about the application:

```
Router#show app-hosting detail
App id           : cp
Owner            : iox
State            : RUNNING
Application
  Type           : docker
  Name           : cpf
  Version        : v1
  Description     : buildkit.dockerfile.v0
  Author         :
  Path           : bootflash:cpfv5.tar
  URL Path       :
  Multicast      : yes
Activated profile name : custom

Resource reservation
  Memory         : 128 MB
  Disk           : 10 MB
  CPU            : 400 units
  CPU-percent    : 35 %
  VCPU           : 1

Platform resource profiles
  Profile Name   CPU(unit)  Memory(MB)  Disk(MB)
-----
Attached devices
  Type          Name          Alias
-----
serial/shell    iox_console_shell  serial0
serial/aux      iox_console_aux    serial1
serial/syslog   iox_syslog         serial2
serial/trace    iox_trace          serial3

Network interfaces
-----
eth0:
  MAC address    : 52:54:dd:f2:f4:87
  IPv4 address   : 192.168.0.9
  IPv6 address   : ::
  Network name   : VPG0

Docker
-----
Run-time information
  Command        :
  Entry-point    : /station/cpf
  Run options in use : --device /dev/lorawan_tty1:/dev/ttyACM0 -v /bootflash/lorawan_0:/cpf/
  Package run options :
Application health information
  Status         : 0
  Last probe error :
  Last probe output :
```

Use the following command to display the list of applications and their statuses:

Device# show app-hosting list
App id State

CP RUNNING

2. Sample app settings:

```
!
interface VirtualPortGroup0
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 no mop enabled
 no mop sysid
```

lorawan_tty1 as its plugged into slot 1

```
app-hosting appid cp
 app-vnic gateway0 virtualportgroup 0 guest-interface 0
 guest-ipaddress 192.168.0.9 netmask 255.255.255.0
 app-default-gateway 192.168.0.1 guest-interface 0
 app-resource docker
 run-opts 1 "--device /dev/lorawan_tty1:/dev/ttyACM0"
 run-opts 3 "-v /bootflash/lorawan_0:/cpf/"
Router#
```

```
Router#sh iox-service

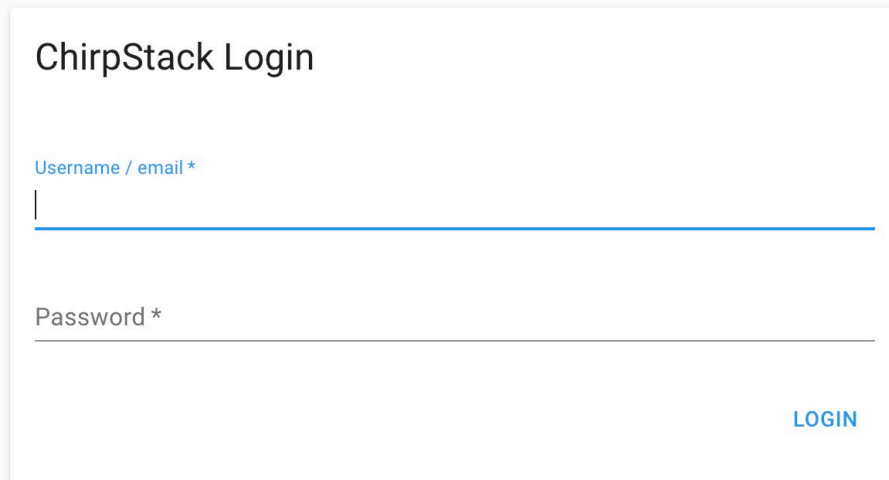
IOx Infrastructure Summary:
-----
IOx service (CAF)           : Running
IOx service (HA)           : Not Supported
IOx service (IOxman)       : Running
IOx service (Sec storage)  : Running
Libvirt 5.5.0              : Running
Dockerd v19.03.13-ce      : Running

Router#
Router#
Router#app-hosting install appid cp package bootflash:cpfv5.tar
Installing package 'bootflash:cpfv5.tar' for 'cp'. Use 'show app-hosting list' for progress.
```

ChirpStack – Step by Steps:

Please refer the appendix for the ChirpStack installation:

1.ChirpStack server login



The image shows a login form titled "ChirpStack Login". It contains two input fields: "Username / email *" and "Password *". The "Username / email *" field has a blue underline and a vertical cursor. The "Password *" field has a grey underline. A blue "LOGIN" button is located at the bottom right of the form.

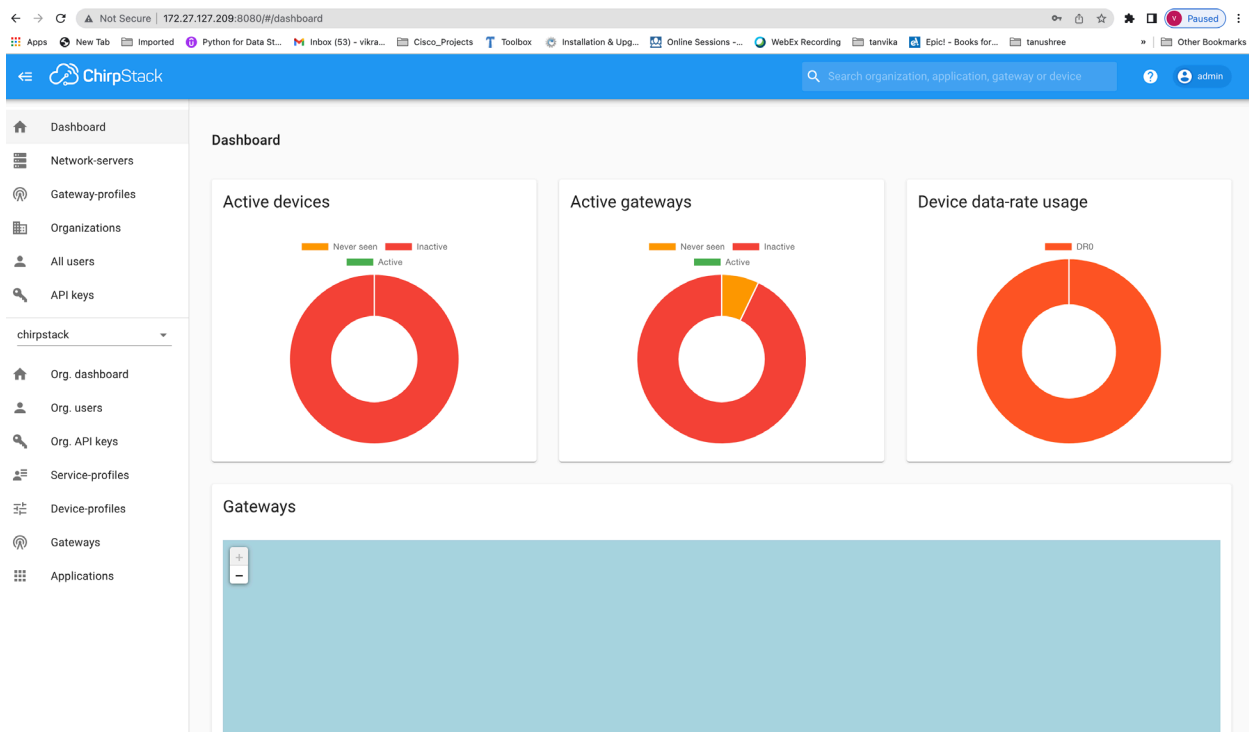
ChirpStack Login

Username / email *

Password *

LOGIN

2.ChirpStack dashboard overview screen:



3. Create Gateway Step:

The 'Gateways' page features a table with the following columns: Last seen, Name, Gateway ID, Network server, and Gateway activity (30d). A '+ CREATE' button is visible in the top right corner.

Last seen	Name	Gateway ID	Network server	Gateway activity (30d)
3 months ago	Aventus	0000000000000033	Ins	
a month ago	Aventus-76	0000000000000076	Ins	█
Never	Aventus-800	0000000000000069	Ins	
8 months ago	Compliance-IR1101	000000ffe000012	Ins	
3 months ago	Compliance-IR1101-2	0000000000000012	Ins	
2 hours ago	EDVT-1101	0000000000000099	Ins	█
2 months ago	EDVT-1101-2	0000000000000089	Ins	
6 months ago	Ir1101	0000000000000039	Ins	
a month ago	Ir1101-33	0000000000000079	Ins	
22 days ago	Ir1101-michael	0000000000000066	Ins	█

Rows per page: 10 | 1-10 of 14

4. Adding a GW Step:

ChirpStack

Search organization, application, gateway or device

admin

- Dashboard
- Network-servers
- Gateway-profiles
- Organizations
- All users
- API keys

chirpstack

- Org. dashboard
- Org. users
- Org. API keys
- Service-profiles
- Device-profiles
- Gateways
- Applications

GENERAL TAGS METADATA

Gateway name *
Test
The name may only contain words, numbers and dashes.

Gateway description *
Testing GW

Gateway ID *
00 00 00 00 00 00 00 19 MSB

Network-server *
Ins
Select the network-server to which the gateway will connect. When no network-servers are available in the dropdown, make sure a service-profile exists for this organization.

Service-profile *
service
Select the service-profile under which the gateway must be added. The available service-profiles depend on the selected network-server, which must be selected first.

Gateway-profile *
gateway
Optional. When assigning a gateway-profile to the gateway, ChirpStack Network Server will attempt to update the gateway according to the gateway-profile. Note that this does require a gateway with ChirpStack Concentrator.

Gateway discovery enabled
When enabled (and ChirpStack Network Server is configured with the gateway discover feature enabled), the gateway will send out periodical pings to test its coverage by other gateways in the same network.

Gateway altitude (meters) *
0
When the gateway has an on-board GPS, this value will be set automatically when the network has received statistics from the gateway.

Gateway location (set to current location)

5. Adding Sensor steps:

ChirpStack

Search organization, application, gateway or device

admin

- Dashboard
- Network-servers
- Gateway-profiles
- Organizations
- All users
- API keys

chirpstack

- Org. dashboard
- Org. users
- Org. API keys
- Service-profiles
- Device-profiles
- Gateways
- Applications

Applications / BAC-Adeunis / Devices / Create

GENERAL VARIABLES TAGS

Device name *
The name may only contain words, numbers and dashes. Please fill out this field.

Device description *

Device EUI * MSB

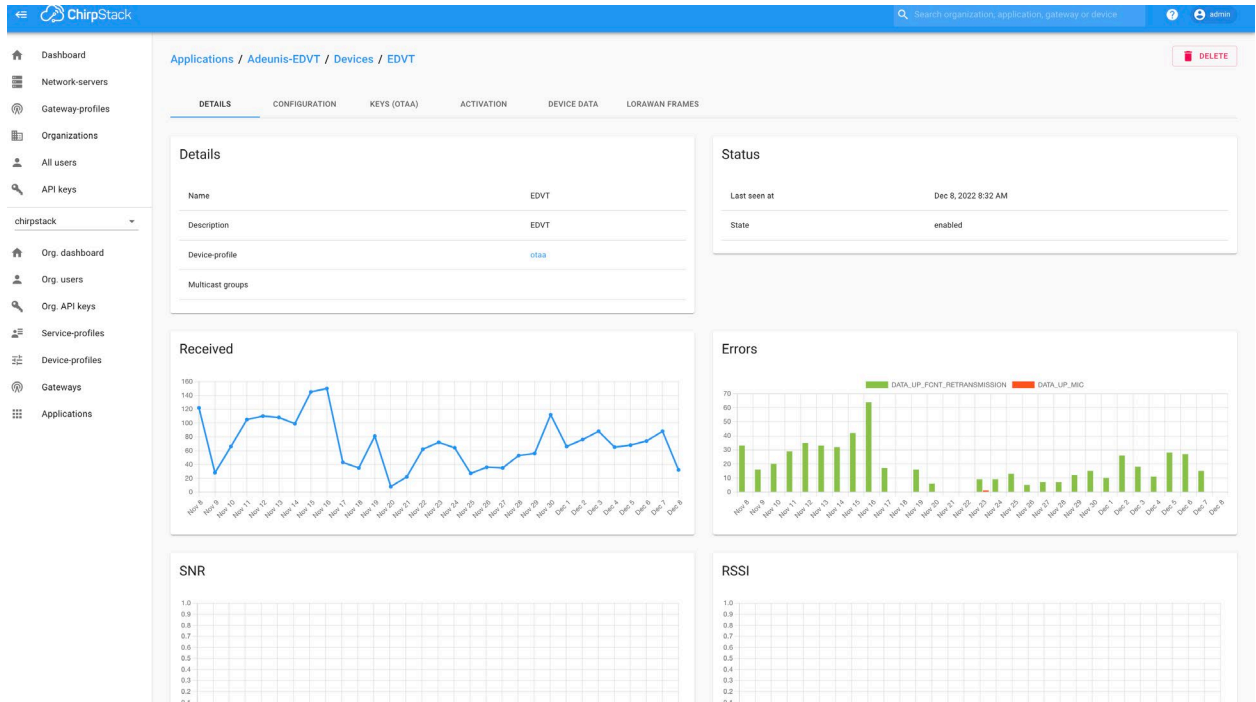
Device-profile *
Device-profile

Disable frame-counter validation
Note that disabling the frame-counter validation will compromise security as it enables people to perform replay-attacks.

Device is disabled
ChirpStack Network Server will ignore received uplink frames and join-requests from disabled devices.

CREATE DEVICE

6. Monitoring the Sensor details :



7. Check the Device DATA frames :

Time	Status	Freq	SF	BW	FCnt	FPort	Confirmed
Dec 08 8:32:43 AM	up	903.1 MHz	SF10	8W125	FCnt: 21869	FPort: 1	Confirmed
Dec 08 8:32:28 AM	up	902.9 MHz	SF10	8W125	FCnt: 21868	FPort: 1	Confirmed
Dec 08 7:52:05 AM	up	903.3 MHz	SF10	8W125	FCnt: 21861	FPort: 1	Confirmed
Dec 08 7:52:01 AM	up	903.1 MHz	SF10	8W125	FCnt: 21860	FPort: 1	Confirmed
Dec 08 7:12:24 AM	up	902.5 MHz	SF10	8W125	FCnt: 21853	FPort: 1	Confirmed
Dec 08 7:12:06 AM	up	902.5 MHz	SF10	8W125	FCnt: 21852	FPort: 1	Confirmed
Dec 08 6:32:40 AM	up	902.9 MHz	SF10	8W125	FCnt: 21845	FPort: 1	Confirmed
Dec 08 6:32:19 AM	up	903.5 MHz	SF10	8W125	FCnt: 21844	FPort: 1	Confirmed
Dec 08 5:52:14 AM	up	902.9 MHz	SF10	8W125	FCnt: 21837	FPort: 1	Confirmed
Dec 08 5:52:06 AM	up	903.5 MHz	SF10	8W125	FCnt: 21836	FPort: 1	Confirmed

8. Checking Live LoRaWAN Frames:

The screenshot shows the ChirpStack interface for the 'Adeunis-EDVT' device. The 'LORAWAN FRAMES' tab is active, displaying a list of frames with their status, frequency, and other parameters.

Time	Status	Freq	SF	BW	CR	FCnt	DevAddr	GW
Dec 08 8:32:44 AM	UnconfirmedDataDown	925.7 MHz	SF10	BW500	FCnt: 7352	DevAddr: 011f4666	GW: 0000000000000099	
Dec 08 8:32:43 AM	ConfirmedDataUp	903.1 MHz	SF10	BW125	FPort: 1	FCnt: 21869	DevAddr: 011f4666	
Dec 08 8:32:28 AM	UnconfirmedDataDown	923.3 MHz	SF10	BW500	FCnt: 7351	DevAddr: 011f4666	GW: 0000000000000099	
Dec 08 8:32:28 AM	ConfirmedDataUp	902.3 MHz	SF10	BW125	FPort: 1	FCnt: 21868	DevAddr: 011f4666	
Dec 08 7:52:06 AM	UnconfirmedDataDown	926.3 MHz	SF10	BW500	FCnt: 7350	DevAddr: 011f4666	GW: 0000000000000099	
Dec 08 7:52:05 AM	ConfirmedDataUp	903.3 MHz	SF10	BW125	FPort: 1	FCnt: 21861	DevAddr: 011f4666	
Dec 08 7:52:02 AM	UnconfirmedDataDown	925.7 MHz	SF10	BW500	FCnt: 7349	DevAddr: 011f4666	GW: 0000000000000099	
Dec 08 7:52:01 AM	ConfirmedDataUp	903.1 MHz	SF10	BW125	FPort: 1	FCnt: 21860	DevAddr: 011f4666	
Dec 08 7:12:25 AM	UnconfirmedDataDown	923.9 MHz	SF10	BW500	FCnt: 7348	DevAddr: 011f4666	GW: 0000000000000099	
Dec 08 7:12:24 AM	ConfirmedDataUp	902.5 MHz	SF10	BW125	FPort: 1	FCnt: 21853	DevAddr: 011f4666	

9. Checking the app keys

The screenshot shows the ChirpStack interface for the 'Adeunis-EDVT' device. The 'KEYS (OTAA)' tab is active, displaying the application key and a note about LoRaWAN 1.0 devices.

Application key *

9b ed e5 3e 82 67 48 7b 8f b6 3e f7 82 e9 e5 77

MSB

For LoRaWAN 1.0 devices. In case your device supports LoRaWAN 1.1, update the device profile first.

SET DEVICE KEYS

10. Check the app session keys and network session keys

The screenshot shows the ChirpStack web interface. The top navigation bar includes the ChirpStack logo, a search bar, and a user profile icon labeled 'admin'. The left sidebar contains a menu with items: Dashboard, Network-servers, Gateway-profiles, Organizations, All users, API keys, chirpstack (selected), Org dashboard, Org users, Org API keys, Service-profiles, Device-profiles, Gateways, and Applications. The main content area is titled 'Applications / Adeunis-EDVT / Devices / EDVT' and has a 'DELETE' button. Below the title are tabs for DETAILS, CONFIGURATION, KEYS (OTAA), ACTIVATION (selected), DEVICE DATA, and LORAWAN FRAMES. The ACTIVATION tab displays the following information:

- Device address*: 01 1f c4 56 (MSB)
- Network session key (LoRaWAN 1.0)*: 73 56 e2 65 13 70 15 38 0e d2 dc 6f e5 e7 b0 a9 (MSB)
- Application session key (LoRaWAN 1.0)*: c8 89 fc 2b 6b 63 d1 13 f9 26 33 62 59 7e f2 97 (MSB)
- Uplink frame-counter*: 21870
- Downlink frame-counter (network)*: 7353

Sample running configuration with Common packet forwarder:

Building configuration...

Current configuration : 7256 bytes

!

! Last configuration change at 20:05:01 UTC Tue Jun 28 2022

!

version 17.9

service timestamps debug datetime msec

service timestamps log datetime msec

service internal

service call-home

platform qfp utilization monitor load 80

platform punt-keepalive disable-kernel-core

!

hostname Sparrow_Artic_900

!

boot-start-marker

boot system bootflash:ir1101-

universalk9.BLD_V179_THROTTLE_LATEST_20220616_072420.SSA.bin

boot-end-marker

!

!

no aaa new-model

!

!

login block-for 60 attempts 3 within 30

login delay 3

login on-success log

ipv6 unicast-routing

!

!

subscriber templating

!

multilink bundle-name authenticated

!

crypto pki trustpoint TP-self-signed-1417813608

enrollment selfsigned

subject-name cn=IOS-Self-Signed-Certificate-1417813608

revocation-check none

```
rsa-keypair TP-self-signed-1417813608
!
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
!
no license feature hsec9
license udi pid IR1101-K9 sn FCW2510PMVK
license boot level network-advantage
memory free low-watermark processor 45131
!
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
username iox privilege 15 password 0 iox
!
redundancy
!
vlan internal allocation policy ascending
!
interface VirtualPortGroup0
ip address 192.168.0.1 255.255.255.0
ip nat inside
no mop enabled
no mop sysid
!
interface GigabitEthernet0/0/0
ip address 172.27.127.134 255.255.255.0
ip nat outside
!
interface FastEthernet0/0/1
!
interface FastEthernet0/0/2
!
interface FastEthernet0/0/3
!
interface FastEthernet0/0/4
!
interface Vlan1
no ip address
!
```

```
interface Async0/2/0
no ip address
encapsulation scada
!
interface LORAWAN0/1/0
no ip address
common-packet-forwarder profile
country UNITEDSTATES
region-channel-plan US915
gateway-id 54
lns-ip 172.27.127.209
lns-port 6080
log-level debug lines 255
cpf enable
arp timeout 0
no mop enabled
no mop sysid
!
iox
ip forward-protocol nd
ip http server
ip http auth-retry 3 time-window 1
ip http authentication local
ip http secure-server
ip http client source-interface GigabitEthernet0/0/0
ip tftp source-interface GigabitEthernet0/0/0
ip nat inside source list NAT_ACL interface GigabitEthernet0/0/0
overload
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/0 172.27.127.1
!
!
ip access-list standard NAT_ACL
10 permit any
!
!
control-plane
!
line con 0
stopbits 1
speed 115200
line 0/0/0
line 0/2/0
```

```
line vty 0 4
login
transport input ssh
line vty 5 14
login
transport input ssh
!
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be
used as contact email address to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
active
destination transport-method http
!
app-hosting appid cp
app-vnic gateway0 virtualportgroup 0 guest-interface 0
guest-ipaddress 192.168.0.9 netmask 255.255.255.0
app-default-gateway 192.168.0.1 guest-interface 0
app-resource docker
run-opts 1 "--device /dev/lorawan_tty1:/dev/ttyACM0"
run-opts 3 "-v /bootflash/lorawan_0:/cpf/"
end
```

Appendix:

- About LoRaWAN: <https://www.youtube.com/watch?v=Qd7kMGaQ5vI>
- ChirpStack installation:
<https://www.youtube.com/watch?v=5CCrpgPZBwY>
- To know more about Actility : <https://www.actility.com/>
- About cisco LPWA PIM module : cisco LoRa PIM module