THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS DESCRIBED IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. THIS DOCUMENT IS PROVIDED “AS IS.” ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED, OR STATUTORY INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, PUNITIVE, EXEMPLARY, OR INCIDENTAL DAMAGES UNDER ANY THEORY OF LIABILITY, INCLUDING WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OF OR INABILITY TO USE THIS DOCUMENT, EVEN IF CISCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

©2023 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED
## Contents

Introduction .......................................................................................................................................4  
Cisco IR1800 managed by IoT OD .....................................................................................................5  
  CAPWAP mode for IoT OD IR1800 Wi-Fi .....................................................................................25  
Cisco IR1800 managed by SD-WAN Manager .................................................................................25  
WAN Failover Operation ..................................................................................................................26  
CURWB Backhaul Managed with IoT OD ..........................................................................................29  
C9800 WLC Configuration for IR1800 Wi-Fi in CAPWAP Mode with Captive Portal .........................42  
  Configure WLAN ..........................................................................................................................42  
  WLAN General ..........................................................................................................................43  
  WLAN Security ..........................................................................................................................44  
  Configure Profiles .......................................................................................................................47  
  Configure Tags .............................................................................................................................50  
  Verify ...........................................................................................................................................52  
Secure Equipment Access to Onboard Equipment ...........................................................................53  
IOx Applications ..............................................................................................................................61  
  Example Vehicle CANBUS Data Application .................................................................................61  
Bus Services ...................................................................................................................................64  
  Automatic Passenger Counting with DILAX ..................................................................................65  
  Emissions Monitoring with SensorComm Wi-NOx ..........................................................................67  
  Video Surveillance with AXIS and Milestone .................................................................................70  
  Voice Communication with InstantConnect ..................................................................................75  
Additional Resources .......................................................................................................................77  
  Cisco References ..........................................................................................................................77  
  Third-party References ................................................................................................................77
Introduction

The configurations in this implementation guide are based on the topology shown below. The IR1835 router and subtended IE3300 switch are used to connect the various devices on the bus. Some sections, like the example vehicle CANBUS IOX application, and the third-party bus services components are only covered at a high level to show what is possible in a Mass Transit deployment, not to document specific configuration steps.

Multiple VLANs are used to provide segmentation between different devices connected behind the IR1800 router as depicted in the color-coded key in the diagram that follows.

Figure 1. IR1835 Mass Transit Equipment Physical Topology
Cisco IR1800 managed by IoT OD

This section documents the configuration for the IR1835 router, managed by IoT Operations Dashboard, using an eCVD Standard Template. The screenshots show the configuration of the various features available in the eCVD template. Some features needed to support the mass transit solution were added as CLI configuration on top of the graphical based eCVD template.

This section shows two different options for configuring the Wi-Fi access point module on the IR1835 with IoT OD – first as a WGB with Hotspot functionality, and secondly as a CAPWAP access point managed by a C9800 wireless LAN controller.

In the Base Configuration section, the interface numbering options are left as default. If the default values conflict with the desired interface naming scheme, they can be changed.

Figure 2. Cisco IR1800 managed by IoT OD – eCVD Template – Base Configuration
The **WAN Uplink** section determines which interfaces are used as WAN interfaces, along with details for cellular APN, IP SLA destination, and so on. In the IR1800 for a transit vehicle, the “Ethernet” interface refers to Gigabit 0/0/0, which will be connected to the CURWB radio and get a DHCP IP address. WGB refers to the 5 GHz Wi-Fi uplink from the WP-WIFI6 module, to be used when the vehicle enters the yard. Cellular 1 is the Cellular 0/4/0 interface in the first PIM slot, and Cellular 2 is the Cellular 0/5/0 interface in the second PIM slot, regardless of which specific hardware modules are used.
Figure 3. Cisco IR1800 managed by IoT OD – eCVD Template – WAN Uplink

<table>
<thead>
<tr>
<th>Edit MT standard I</th>
<th>Configurations</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Base Form</td>
<td>Extended Form</td>
</tr>
<tr>
<td><strong>Base Configuration</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>WAN Uplink</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethernet Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS/NTP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wi-Fi</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>WAN Uplink 1</strong></td>
<td>Interface*</td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td>Ethernet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP Address for IP SLA Test*</td>
<td>208.67.220.222</td>
</tr>
<tr>
<td><strong>WAN Uplink 2</strong></td>
<td>Interface*</td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td>WGB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP Address for IP SLA Test*</td>
<td>208.67.222.220</td>
</tr>
<tr>
<td><strong>WAN Uplink 3</strong></td>
<td>Interface*</td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td>Cellular 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP Address for IP SLA Test*</td>
<td>8.8.4.4</td>
</tr>
<tr>
<td></td>
<td>Cellular APN Username (if Applicable)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cellular APN Password (if Applicable)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cellular SIM PIN (if Applicable)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cellular Access Point Name (if Applicable)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enable Second SIM (if Applicable)</td>
<td>Not Installed</td>
</tr>
<tr>
<td><strong>WAN Uplink 4</strong></td>
<td>Interface*</td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td>Cellular 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP Address for IP SLA Test*</td>
<td>9.9.9.11</td>
</tr>
<tr>
<td></td>
<td>Cellular Access Point Name (if Applicable)</td>
<td></td>
</tr>
</tbody>
</table>
The **Ethernet Settings** section simply enables the four LAN interfaces on the IR1800, to be used to connect to downstream devices. By default, all interfaces are put in VLAN 948. Additional configuration to put the interfaces in different VLANs (for Passenger, Worker, Devices1, and so on), enable 802.1x, apply ZBFW, and more is added later in the CLI at the end of this section.

**Figure 4. Cisco IR1800 managed by IoT OD – eCVD Template – Ethernet Settings**
The **DHCP** section is used to configure a DHCP pool for VLAN 948. DHCP Pools for the other VLANs are added automatically. The various VLANs are used to provide separation for different types of devices on the network. Refer to Figure 1 to better understand how the VLANs are used.

**Figure 5. Cisco IR1800 managed by IoT OD – eCVD Template – DHCP**
The **DNS / NTP** section can be left as default unless specific configuration is required.

**Figure 6. Cisco IR1800 managed by IoT OD – eCVD Template – DNS/NTP**

### Edit MT Standard 1

<table>
<thead>
<tr>
<th>Group Details</th>
<th>Devices</th>
<th>Configurations</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base Form</strong></td>
<td><strong>Extended Form</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Base Configuration**
- **WAN Uplink**
- **Ethernet Settings**
- **DHCP**

**DNS/NT**
- **VPN**
- **Network**
- **Security**
- **Device Management**
- **Wi-Fi**

**DNS Settings**
- **Primary LAN DNS IP Address**
  - 208.67.222.222

**NTP Settings**
- **Primary Network Time Server**
  - time.nist.gov

- **Secondary Network Time Server**
- **Router Local Timezone**
The **VPN** section creates the FlexVPN tunnel (Tunnel 949) to the enterprise headend, based on PSK authentication. In this example, the tunnel is enabled for the CURWB and Cellular interfaces, but not the WGB interface. Depending on the existing enterprise routing and security policies, it may be desirable to disable the VPN over CURWB as well, or potentially if the Cellular interface is using a private APN with direct connectivity to the enterprise.

**Figure 7. Cisco IR1800 managed by IoT OD – eCVD Template – VPN**
In the **Network** section, a QoS policy can be enabled based on various traffic classes.

**Figure 8. Cisco IR1800 managed by IoT OD – eCVD Template – Network**

<table>
<thead>
<tr>
<th>Edit MT Standard 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group Details</strong></td>
</tr>
<tr>
<td><strong>Devices</strong></td>
</tr>
<tr>
<td><strong>Configurations</strong></td>
</tr>
<tr>
<td><strong>Properties</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Base Configuration</th>
<th><strong>QoS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Settings</td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td></td>
</tr>
<tr>
<td>DNS/FTP</td>
<td></td>
</tr>
<tr>
<td>VPN</td>
<td></td>
</tr>
</tbody>
</table>

**Network**

**Security**

**Device Management**

**Wi-Fi**

**Enable Network QoS rules**

<table>
<thead>
<tr>
<th>Max 5 QoS rules</th>
<th>Select Traffic Type</th>
<th>Enter QoS Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice telephony traffic</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Port Forwarding**

<table>
<thead>
<tr>
<th>Max 6 Port Forwarding rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Static Routes</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Max 6 Static Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Network</td>
</tr>
</tbody>
</table>
In the **Security** section, a NetFlow collector can be configured to receive exports, and basic Umbrella functionality can be enabled. Simple firewall rules can be added. An example of a ZBFW for the multiple VLANs is included in the CLI at the end of this section.

Figure 9. Cisco IR1800 managed by IoT OD – eCVD Template – Security
In the Device Management section, ignition sense is enabled to automatically power down the router five minutes after the vehicle is turned off. This works by configuring the router to monitor the input voltage on the power supply to the router, which should be connected to the vehicle’s battery and alternator. When the vehicle is running, the alternator will be charging the battery at a slightly higher voltage than the battery will have at rest, when the vehicle is turned off. This input voltage is used to infer ignition status of the vehicle. In the example below, the voltage threshold is set to 13.2 volts. If the voltage exceeds this – the vehicle is presumed to be running and the router will power up (if previously off) or continue to stay powered up. If the detected voltage drops below this value for the configured time of 300 seconds, the router will power itself down, thus preventing it from draining the vehicle battery unnecessarily.

Auto recovery is also enabled to allow the router to attempt to recover from misconfiguration and other issues, to help prevent sending a technician to troubleshoot a device that is down.
Figure 10. Cisco IR1800 managed by IoT OD – eCVD Template – Device Management

Edit MT Standard 1

<table>
<thead>
<tr>
<th>Group Details</th>
<th>Devices</th>
<th>Configurations</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Base Form</td>
<td>Extended Form</td>
</tr>
</tbody>
</table>

**Base Configuration**

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Vehicle</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**WAN Uplink**

**Ethernet Settings**

<table>
<thead>
<tr>
<th>Enable Ignition Sense</th>
<th>Ignition Off Timer (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>True</td>
<td>300</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ignition Sense Threshold Volts</th>
<th>Ignition Sense Threshold Millivolts</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>500</td>
</tr>
</tbody>
</table>

**Auto Recovery**

- if recovery and hardware reset are enabled and the device has no internet connectivity, then when the hardware reset timer expires, all device configurations will be cleared and it will re-register to IoT OD.

<table>
<thead>
<tr>
<th>Enable Auto Recovery</th>
<th>Enable Router Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>True</td>
<td>True</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Primary Tracking IP Address*</th>
<th>Secondary Tracking IP Address*</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0.1</td>
<td>8.8.4.4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enable Hardware Reset</th>
<th>Hardware Reset Timer</th>
</tr>
</thead>
<tbody>
<tr>
<td>True</td>
<td>12 hours</td>
</tr>
</tbody>
</table>

**Users**

<table>
<thead>
<tr>
<th>User Name</th>
<th>User Password</th>
<th>Privilege Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisco</td>
<td>******</td>
<td>Admin</td>
</tr>
</tbody>
</table>
In the Wi-Fi section the onboard access point is enabled in Workgroup Bridge with Hotspot mode. The Wi-Fi Uplink (WGB) is enabled on the 5GHz radio interface.

To have both an uplink and a hotspot, the Wi-Fi module minimum software version is 17.11 and the IR1800 minimum version is 17.10.1a. Also, the Wi-Fi module must be capable of WGB Concurrent radio, more details about this can be found in the link below, as well as steps to upgrade your module and convert it so that it has the ability for concurrent radio. If during the upgrade procedure any issues are encountered with TFTP, we recommend using HTTP to upgrade the Wi-Fi module through the CLI if there is an HTTP file server available.
Figure 11. Cisco IR1800 managed by IoT OD – eCVD Template – Wi-Fi (WGB with Hotspot)

Edit MT Standard 1

<table>
<thead>
<tr>
<th>Group Details</th>
<th>Devices</th>
<th>Configurations</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Base Form</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Extended Form</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Wi-Fi**

- **WAN Uplink**
- **Ethernet Settings**
- **DHCP**
- **DNS/NTP**
- **VPN**
- **Network**
- **Security**

**Device Management**

- **Wi-Fi**

**Wi-Fi Uplink Settings**

- **Wi-Fi Uplink**
- **Frequency for WGB (Wi-Fi Uplink)**
  - 5GHz

**SSID Profile for Wi-Fi Uplink**

- **SSID Name**
  - RaMA-Enterprise

To login to the CLI of a Wi-Fi module in WGB mode past 17.9.1 the login credentials are the following:

- **Username:** Cisco1
- **Password:** GigabitEth01!
- **Enable Password:** AppleTree01@
Links to the following modules are:

**Wi-Fi Module Overview**

**Wi-Fi Module Concurrent Radio**

A total of four SSIDs are created here for passengers, workers, and devices (two of them, for different types of devices).

**Figure 12. Cisco IR1800 managed by IoT OD – eCVD Template – Wi-Fi (WGB with Hotspot continued)**

Edit MT Standard 1

<table>
<thead>
<tr>
<th>Group Details</th>
<th>Devices</th>
<th>Configurations</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SSID Profile for Wi-Fi Uplink**

- **SSID Name**: RadMA-Enterprise
- **Security (Authentication Type)**: WPA2-PSK
- **SSID Profiles for Wi-Fi Hotspot**
  - **SSID Name**: MT-Device2
  - **Security (Authentication Type)**: WPA2-PSK
  - **Quality of Service Profile**: Silver
  - **SSID Name**: MT-Device
  - **Security (Authentication Type)**: WPA2-PSK
  - **Quality of Service Profile**: Platinum
  - **SSID Name**: MT-Worker
  - **Security (Authentication Type)**: WPA2-PSK
  - **Quality of Service Profile**: Gold
  - **SSID Name**: MT-Passenger
  - **Security (Authentication Type)**: WPA2-PSK
  - **Quality of Service Profile**: Bronze

Each SSID will automatically create the necessary VLANs, DHCP pools, and related configuration, with the exceptions noted.

Finally, the **Extended Form** section of the configuration is used to apply additional CLI as needed, for features that are not supported in the GUI based eCVD template.
Figure 13. Cisco IR1800 managed by IoT OD – eCVD Template – Extended Form CLI

**Edit MT Standard 1**

<table>
<thead>
<tr>
<th>Group Details</th>
<th>Devices</th>
<th>Configurations</th>
<th>Properties</th>
</tr>
</thead>
</table>

**Extended Form Command Line Interface 🔍**

Leverage user property types to parameterize CLI configurations only when Form View is enabled.

```plaintext
1 2
3 interface Wlan-GigabitEthernet0/1/4
4 switchport trunk native vlan 948
5 switchport mode trunk
6 7
8 vlan 955
9 vlan 956
10 vlan 957
11 vlan 958
12 13
14 zone security PASSENGER
15 16 zone security WORKER
17 18 zone security DEVICES1
19 20 zone security DEVICES2
21 22 interface GigabitEthernet0/1/3
23 description trunk to subtended IE switch
24 switchport trunk allowed vlan 948,955–958
25 switchport mode trunk
```

The internal interface connecting the router to the access point module is set as a trunk, with the default VLAN (948) set as native.

```plaintext
interface Wlan-GigabitEthernet0/1/4
switchport trunk native vlan 948
switchport mode trunk
```
Next the four VLANs for Passenger, Worker, Devices1, and Devices2 are created.

```plaintext
vlan 955
vlan 956
vlan 957
vlan 958
```

Four security zones are created, one for each VLAN.

```plaintext
zone security PASSENGER
zone security WORKER
zone security DEVICES1
zone security DEVICES2
```

One of the switch ports is configured as a trunk to connect to the subtended IE switch.

```plaintext
interface GigabitEthernet0/1/3
  description trunk to subtended IE switch
  switchport trunk allowed vlan 948,955-958
  switchport mode trunk
```

A VLAN SVI is created for the Passenger VLAN.

```plaintext
interface Vlan955
  ip address 192.168.110.1 255.255.255.0
  ip nat inside
  zone-member security PASSENGER
```

A VLAN SVI is created for the Worker VLAN.

```plaintext
interface Vlan956
  ip address 192.168.111.1 255.255.255.0
  ip nat inside
  zone-member security WORKER
```

A VLAN SVI is created for the first Devices VLAN.

```plaintext
interface Vlan957
  ip address 192.168.112.1 255.255.255.0
  ip nat inside
  zone-member security DEVICES1
```

A VLAN SVI is created for the second Devices VLAN.

```plaintext
interface Vlan958
  ip address 192.168.113.1 255.255.255.0
```
The Zone Based Firewall uses access lists to match on the subnets for each of the four VLANs.

```
ip access-list extended PASSENGER
    permit ip 192.168.110.0 0.0.0.255 any
ip access-list extended WORKER
    permit ip 192.168.111.0 0.0.0.255 any
ip access-list extended DEVICES1
    permit ip 192.168.112.0 0.0.0.255 any
ip access-list extended DEVICES2
    permit ip 192.168.113.0 0.0.0.255 any
```

The access lists are referenced in class maps for each zone pair.

```
class-map type inspect match-all PASSENGER-TO-INTERNET-CLASS
    match access-group name PASSENGER
class-map type inspect match-all WORKER-TO-INTERNET-CLASS
    match access-group name WORKER
class-map type inspect match-all DEVICES1-TO-INTERNET-CLASS
    match access-group name DEVICES1
class-map type inspect match-all DEVICES2-TO-INTERNET-CLASS
    match access-group name DEVICES2
class-map type inspect match-all WORKER-TO-default-CLASS
    match access-group name WORKER
class-map type inspect match-all DEVICES1-TO-default-CLASS
    match access-group name DEVICES1
class-map type inspect match-all DEVICES2-TO-default-CLASS
    match access-group name DEVICES2
class-map type inspect match-all default-to-DEVICES2-CLASS
    match access-group name DEVICES2
```

Policy maps are then created to inspect each class of traffic based on the zone pairs. In this example the action is just to inspect the traffic, but depending on requirements, other actions (like drop) could be taken.

```
policy-map type inspect PASSENGER-TO-INTERNET-POLICY
    class PASSENGER-TO-INTERNET-CLASS
        inspect
    class class-default
```
drop log

policy-map type inspect WORKER-TO-INTERNET-POLICY
   class WORKER-TO-INTERNET-CLASS
      inspect
      class class-default
      drop log

policy-map type inspect DEVICES1-TO-INTERNET-POLICY
   class DEVICES1-TO-INTERNET-CLASS
      inspect
      class class-default
      drop log

policy-map type inspect DEVICES2-TO-INTERNET-POLICY
   class DEVICES2-TO-INTERNET-CLASS
      inspect
      class class-default
      drop log

policy-map type inspect WORKER-TO-default-POLICY
   class WORKER-TO-default-CLASS
      inspect
      class class-default
      drop log

policy-map type inspect DEVICES1-TO-default-POLICY
   class DEVICES1-TO-default-CLASS
      inspect
      class class-default
      drop log

policy-map type inspect DEVICES2-TO-default-POLICY
   class DEVICES2-TO-default-CLASS
      inspect
      class class-default
      drop log

policy-map type inspect default-TO-DEVICES2-POLICY
   class default-TO-DEVICES2-CLASS
      inspect
class class-default
drop log

Finally, the ZBFW configuration is completed by defining the zone pairs.

zone-pair security PASSENGER-TO-INTERNET source PASSENGER destination INTERNET
    service-policy type inspect PASSENGER-TO-INTERNET-POLICY
zone-pair security WORKER-TO-INTERNET source WORKER destination INTERNET
    service-policy type inspect WORKER-TO-INTERNET-POLICY
zone-pair security DEVICES1-TO-INTERNET source DEVICES1 destination INTERNET
    service-policy type inspect DEVICES1-TO-INTERNET-POLICY
zone-pair security DEVICES2-TO-INTERNET source DEVICES2 destination INTERNET
    service-policy type inspect DEVICES2-TO-INTERNET-POLICY
zone-pair security WORKER-TO-default source WORKER destination default
    service-policy type inspect WORKER-TO-default-POLICY
zone-pair security DEVICES1-TO-default source DEVICES1 destination default
    service-policy type inspect DEVICES1-TO-default-POLICY
zone-pair security DEVICES2-TO-default source DEVICES2 destination default
    service-policy type inspect DEVICES2-TO-default-POLICY
zone-pair security default-TO-DEVICES2 source default destination DEVICES2
    service-policy type inspect default-TO-DEVICES2-POLICY

Note: The “default-TO-DEVICES2” configuration elements were added to enable SEA access from the IOX app to the devices in the 192.168.113.0/24 subnet. Similar configuration will be required if SEA needs to access other subnets.

In the following section 802.1x for wired clients connected to port GigabitEthernet0/1/2 is enabled. When a device connects, it will need to be authenticated by the configured ISE server via RADIUS.

    aaa new-model
    !
    !
    aaa group server radius ISE-RADIUS-GROUP
    server name DatacenterISE
    ip radius source-interface Tunnel949
    !
    aaa authentication dot1x default group ISE-RADIUS-GROUP
    aaa authorization network AUTH_LIST group ISE-RADIUS-GROUP
    aaa accounting update newinfo periodic 2880
aaa accounting dot1x default start-stop group ISE-RADIUS-GROUP
!
epm logging
!
authentication mac-move permit
!
dot1x system-auth-control
!
interface GigabitEthernet0/1/2
  switchport mode access
  authentication port-control auto
  dot1x pae authenticator
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail mac-only
radius-server dead-criteria time 10 tries 3
!
radius server DatacenterISE
  address ipv4 10.3.21.50 auth-port 1645 acct-port 1646
  timeout 3
  key 7 104D000A06185E5A5E57
!
CAPWAP mode for IoT OD IR1800 Wi-Fi

The following figure shows the alternate Wi-Fi configuration in an eCVD template in which the IR1800 access point is managed by a Cisco Catalyst 9800 Wireless LAN Controller.

**Figure 14. Cisco IR1800 managed by IoT OD – eCVD Template – Wi-Fi (Controller/CAPWAP mode)**

Cisco IR1800 managed by SD-WAN Manager

Refer to the *SD-WAN for Industrial Markets Design Guide* for detailed information on configuring the Cisco IR1835 for use in a Mass Transit scenario.

WAN Failover Operation

Failover between WAN interfaces is critical for mass transit buses and similar deployments where the environmental conditions are constantly changing as the vehicle moves. Reducing the failover delay is important to maintaining the best experience for connected devices and users. This interruption in connectivity must be balanced with preventing rapid flapping back-and-forth between interfaces in the case that the vehicle enters an area with poor coverage for all cellular carriers (for example).

The SDWAN CVD provides details about how failovers are handled using BFD monitoring within the service VPNs, as well as other options like “last-resort-circuit” for active-standby scenarios.


This Implementation Guide focuses on how failovers are implemented using the eCVD templates in Cisco IoT Operations Dashboard.

Figure 15. IoT Operations Dashboard – WAN Interface Priorities
The eCVD template allows the WAN uplinks to be selected in prioritized order. Meaning that Uplink 1 will be the default route for all traffic until it is not viable, after which Uplink 2 will be the default route, and so on for Uplink 3 and 4. In the example above, the Ethernet interface (connected to an external CURWB radio) is used as uplink 1, followed by WGB as uplink 2, Cellular 0/4/0 as uplink 3, and Cellular 0/5/0 as uplink 4. The template configures the routing to only have a single default route active at any one time, therefore no load balancing is used for user traffic.

Each of the WAN interfaces is monitored with an ICMP echo based IP SLA and associated track statement. These IP SLA monitoring sessions are always active. A “delay down” statement is added to the IP SLA based track statements to prevent flapping of up/down state in the case that a single ICMP echo is missed.

```
track 12 interface Cellular0/4/0 line-protocol
track 13 interface Cellular0/5/0 line-protocol
track 40 ip sla 40 reachability
delay down 25
!
track 41 ip sla 41 reachability
delay down 25
!
track 42 ip sla 42 reachability
delay down 65
!
track 43 ip sla 43 reachability
delay down 65
!
track 237 ip sla 237 reachability
!
track 238 ip sla 238 reachability
!
track 239 interface Tunnel950 line-protocol
!
track 980 interface GigabitEthernet0/0/0 ip routing
!
track 981 interface Cellular0/4/0 ip routing
!
track 982 interface Cellular0/5/0 ip routing
!
track 983 interface Tunnel950 ip routing
!
```

The IP SLA statements are configured to ping an IP address that is reachable over the associated interface. By default in the eCVD, and as shown in this example, various public DNS server addresses are chosen as the destinations as they are assumed to be highly available and reachable over any internet connection. Different frequencies are configured by default depending on the interface type – 10 seconds for high bandwidth Ethernet uplink, and 30 seconds for Cellular. A lower frequency will potentially reduce the failover time, but at the expense of more data being sent over the interface which can be undesirable for a usage-based Cellular bill.

```
ip sla 40
icmp-echo 208.67.220.222 source-interface GigabitEthernet0/0/0
frequency 10
```
ip sla schedule 40 life forever start-time now
ip sla 41
icmp-echo 208.67.222.220 source-interface Vlan950
frequency 10
ip sla schedule 41 life forever start-time now
ip sla 42
icmp-echo 8.8.4.4
frequency 30
ip sla schedule 42 life forever start-time now
ip sla 43
icmp-echo 9.9.9.11
frequency 30
ip sla schedule 43 life forever start-time now
ip sla 237
icmp-echo 208.67.222.222
frequency 30
ip sla 238
icmp-echo 208.67.220.220
frequency 30

All WAN interfaces are configured to be up and connected at all times. Weighted default routes are used to prioritize one interface over another. Host routes to the IP SLA destinations are added to force the ICMP packets out a specific interface. Host routes to the IP SLA destinations out “Null0” are also added to prevent reachability to these destinations over one of the default routes, in the event the host route out the WAN interface is removed from the routing table.

ip route 8.8.4.4 255.255.255.255 Cellular0/4/0 track 12
ip route 9.9.9.11 255.255.255.255 Cellular0/5/0 track 13
ip route 0.0.0.0 0.0.0.0 Cellular0/4/0 72 track 42
ip route 69.172.234.159 255.255.255.255 Cellular0/4/0 42 track 42
ip route 0.0.0.0 0.0.0.0 Cellular0/5/0 73 track 43
ip route 69.172.234.159 255.255.255.255 Cellular0/5/0 43 track 43
ip route 0.0.0.0 0.0.0.0 Cellular0/4/0 82
ip route 0.0.0.0 0.0.0.0 Cellular0/5/0 83
ip route 8.8.4.4 255.255.255.255 Null0 3
ip route 9.9.9.11 255.255.255.255 Null0 3
ip route 44.230.145.83 255.255.255.255 Cellular0/4/0 90
ip route 44.230.145.83 255.255.255.255 Cellular0/5/0 92
ip route 208.67.220.222 255.255.255.255 Null0 3
ip route 208.67.222.220 255.255.255.255 Null0 3
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/0 dhcp 70
ip route 44.230.145.83 255.255.255.255 GigabitEthernet0/0/0 dhcp
ip route 208.67.220.222 255.255.255.255 GigabitEthernet0/0/0 dhcp
ip route 69.172.234.159 255.255.255.255 GigabitEthernet0/0/0 dhcp 40
ip route 0.0.0.0 0.0.0.0 Vlan950 dhcp 71
ip route 208.67.222.220 255.255.255.255 Vlan950 dhcp
CURWB Backhaul Managed with IoT OD

The Cisco CURWB radios, such as the IW916x series can be managed with the Industrial Wireless service in IoT Operations Dashboard. To onboard the IW radio used as an uplink for the IR1800 router, it is recommended that the initial provisioning is performed in a staging environment before installing in a vehicle.

This section summarizes the steps required to deploy an IW9167 device. For detailed steps and more information refer to the official documentation:

Cisco Catalyst IW9167 Heavy Duty Series Configuration Guides

Industrial Wireless service for IoT Operations Dashboard

1. Create a CSV file containing the serial number and MAC addresses of the IW devices that need to be onboarded into IoT OD:
   
   KWC272109QD,24:16:1B:F9:2B:C0
   KWC272109U3,24:16:1B:F9:2D:B8
   KWC272109TY,24:16:1B:F9:2D:A4
   KWC272109TK,24:16:1B:F9:2D:70

2. Log into IoT Operations Dashboard, and navigate to the Industrial Wireless service. From the Inventory page, click Add Devices and upload the CSV file created above.

3. Either using Configuration Groups, or individual device configuration, setup the device as required. See detailed steps at the end of this section.

4. Next, connect the IW device to a switch that can provide a DHCP address, power over ethernet, and internet access (to IoT OD). From a computer connected to the same switch, identify the DHCP assigned address that was given to the IW access point. From the computer web browser, connect to the IW access point local GUI, or CLI and configure the device to be managed with IoT OD:

   configure iotod-iw online

   The IW access point contacts the IoT OD and attempts to download the configuration parameters. The IW can now be disconnected from the staging switch and installed in the vehicle. The IW connects to the IR1800 routed Gig 0/0/0 port, with an inline power injector to provide power. The IR1800 Gig 0/0/0 interface is assigned a DHCP address, and work “out of the box” with a configuration based on an eCVD template with Ethernet WAN enabled.
Detailed CURWB configuration from the Industrial Wireless service in IoT Operations Dashboard are shown below. This is an example of a possible configuration that was verified in a lab environment. Real-world deployments may require modification.
Figure 18. Cisco URWB managed by IoT OD – Device Configuration - General
Figure 19. Cisco URWB managed by IoT OD – Device Configuration – Wireless Radio

<table>
<thead>
<tr>
<th>Wireless Radio</th>
<th>IOTOD</th>
<th>Last Heard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passphrase</td>
<td>CiscoURWB</td>
<td>CiscoURWB</td>
</tr>
<tr>
<td>Radio 1 enabled</td>
<td>on</td>
<td>on</td>
</tr>
<tr>
<td>Radio 2 enabled</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>Radio 1 role</td>
<td>Fluidity</td>
<td>Fluidity</td>
</tr>
<tr>
<td>Radio 1 Frequency (MHz)</td>
<td>5180 MHz</td>
<td>5180 MHz</td>
</tr>
<tr>
<td>Radio 1 Channel width</td>
<td>40</td>
<td>40</td>
</tr>
</tbody>
</table>
Figure 20. Cisco URWB managed by IoT OD – Device Configuration – Advanced Radio Settings
Figure 21. Cisco URWB managed by IoT OD – Device Configuration – Key Control

<table>
<thead>
<tr>
<th>Inventory</th>
<th>Key Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
</tr>
<tr>
<td>Wireless Radio</td>
<td></td>
</tr>
<tr>
<td>Advanced Radio Settings</td>
<td></td>
</tr>
<tr>
<td>Key Control</td>
<td>IOTOD</td>
</tr>
<tr>
<td>FluidMAX</td>
<td>off</td>
</tr>
<tr>
<td>Multicast</td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td></td>
</tr>
<tr>
<td>Radius</td>
<td></td>
</tr>
<tr>
<td>NTP</td>
<td></td>
</tr>
<tr>
<td>L2TP</td>
<td></td>
</tr>
<tr>
<td>Vlan</td>
<td></td>
</tr>
<tr>
<td>Fluidity</td>
<td></td>
</tr>
<tr>
<td>Fluidity Advanced</td>
<td></td>
</tr>
<tr>
<td>Fast Failover (TITAN)</td>
<td></td>
</tr>
<tr>
<td>Misc</td>
<td></td>
</tr>
<tr>
<td>Spanning Tree</td>
<td></td>
</tr>
<tr>
<td>MPLS</td>
<td></td>
</tr>
<tr>
<td>Asp</td>
<td></td>
</tr>
<tr>
<td>OoS</td>
<td></td>
</tr>
</tbody>
</table>

Last heard and IoT OD Configuration match.
Figure 22. Cisco URWB managed by IoT OD – Device Configuration – Fluidity
Figure 23. Cisco URWB managed by IoT OD – Device Configuration – Fluidity Advanced

<table>
<thead>
<tr>
<th>Fluidity Advanced</th>
<th>IOTOD</th>
<th>Last Heard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large Network Optimization</td>
<td>on</td>
<td>on</td>
</tr>
<tr>
<td>Max Clients Number</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Backhaul Check</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Mesh End Backhaul Check</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Routes</td>
<td>Backhaul</td>
<td>Backhaul</td>
</tr>
<tr>
<td>Degree of Preference Limit</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Degree of Preference Bias</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Per-Client DoP overhead</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Warm Up Time</td>
<td>30000</td>
<td>30000</td>
</tr>
<tr>
<td>Infra. Timeout</td>
<td>800</td>
<td>800</td>
</tr>
<tr>
<td>Fastdrop count</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Figure 24. Cisco URWB managed by IoT OD – Device Configuration – Misc
### Figure 25. Cisco URWB managed by IoT OD – Device Configuration - MPLS

<table>
<thead>
<tr>
<th>SERVICES</th>
<th>ITOD</th>
<th>Last Heard</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless Radio</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced Radio Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FluidMAX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multicast</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Radius</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L2TP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fluidity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fluidity Advanced</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fast Failover (TITAN)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Misc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spanning Tree</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>MPLS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unicast flooding</td>
<td>Disable</td>
<td>Disable</td>
</tr>
<tr>
<td>Arp Unicast</td>
<td>Disable</td>
<td>Disable</td>
</tr>
<tr>
<td>Broadcast packets reduction</td>
<td>Enable</td>
<td>Enable</td>
</tr>
<tr>
<td>Pseudo-wires set</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Cluster ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPLS ARP limit grace (ms)</td>
<td>30000</td>
<td>30000</td>
</tr>
<tr>
<td>MPLS ARP limit block</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>MPLS ARP limit rate</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Figure 26. Cisco URWB managed by IoT OD – Device Configuration - ARP
Figure 27. Cisco URWB managed by IoT OD – Device Configuration - Wi-Fi Multimedia Queues

<table>
<thead>
<tr>
<th>Service</th>
<th>IoTOD</th>
<th>Last Heard</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2TP</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Vlan</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Fluidity</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Fluidity Advanced</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>Fast Failover (TITAN)</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>Misc</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Spanning Tree</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>MPLS</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>Arp</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>QoS</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Wi-Fi Multimedia Queues</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ampdu</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>TFTP</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>Static Routes</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>Allowlist/Blocklist</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Static MACs</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>VLAN Subnets</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

ID 11
Saved - 2023-08-11 12:00:56 pm
Last heard - 2023-08-11 12:20:15 pm

Last heard and IoT OD Configuration match.
Figure 28. Cisco URWB managed by IoT OD – Device Configuration – Ampdu
C9800 WLC Configuration for IR1800 Wi-Fi in CAPWAP Mode with Captive Portal

The screenshots in this section summarize the Catalyst 9800 configuration used to implement Captive Portal authentication for mass transit passengers connected to either the IR1800 onboard AP, or a fixed AP in the transit station. The access points in both cases are managed by the Catalyst 9800 wireless LAN controller over a CAPWAP tunnel.

The access points are configured with FlexConnect Local Switching to optimize the data path from passenger wireless clients to the Internet.

The configuration of the C9800 for CAPWAP and Captive Portal is divided into the following parts:

- Configure WLAN
  - WAN General
  - WAN Security
- Configure Profiles
- Configure Tags
- Verification

Configure WLAN

The first screenshot shows multiple WLANs have been created, all starting with “MT-” in this example. All of these SSIDs will be extended to the IR1800 built in APs. The “MT_Passenger_CAPWAP” SSID is the focus of this section. Notice how it is using Web Auth, versus WPA2-PSK for the other SSIDs.

Figure 29. Cisco Catalyst 9800 – WLANs list
WLAN General

The WLAN is **Enabled** for both 2.4 GHz and 5 GHz bands.

**Figure 30. Cisco Catalyst 9800 – Edit WLAN - General**
WLAN Security
The security configuration for the Passenger SSID is where the captive portal authentication method is defined. In the Layer2 tab, None is selected as the security mechanism.

Figure 31. Cisco Catalyst 9800 – Edit WLAN – Security – Layer2
The WLAN Layer3 Security settings enable Web authentication (also known as Captive Portal). The Web Auth Parameter Map is set to **global**.

**Figure 32. Cisco Catalyst 9800 – Edit WLAN – Security – Layer3**

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device
The **global** web auth parameter is set to type **consent** so that when users attempt to connect, they are presented with a web page on which they need to click **Accept** to acknowledge the terms before being allowed access to the network. This option is set under **Configuration > Security > Web Auth**.

**Figure 34. Cisco Catalyst 9800 – Edit Web Auth Parameter**
**Configure Profiles**

Edit the **Policy Profile** to associate the WLAN to the correct VLAN, which is **VLAN0955** in this case, and is reserved for passenger data.

*Figure 34. Cisco Catalyst 9800 – Edit Policy Profile – Access Policies*
Also configure the profile for **Central Authentication Enabled**, as shown in the screenshot that follows. Note that **Central Switching is Disabled** – resulting in FlexConnect local switching being used so that passenger traffic does not need to be backhauled to the enterprise datacenter. Additional FlexConnect settings are defined later.

**Figure 35. Cisco Catalyst 9800 – Edit Policy Profile – General**

Edit the **Flex Profile** to identify the VLANs that will be locally switched. In the **General** tab, **VLAN 948** is specified as the **Native VLAN**. This is the default LAN subnet that is created by the eCVD template and is used for AP management communication to the WLC. Passenger and other SSID traffic will each have their own separate VLAN to provide segmentation.
Passenger clients will connect on VLAN955. Other VLANs for other SSIDs are also defined here.

Figure 37. Cisco Catalyst 9800 – Edit Flex Profile - VLAN
Configure Tags

Use a **Policy Tag** to associate a WLAN Profile and Policy Profile.

**Figure 38. Cisco Catalyst 9800 – Edit Policy Tag – MT_Passenger_CAPWAP**
Use the **Site Tag** to associate the **Flex Profile**.

**Figure 39. Cisco Catalyst 9800 – Edit Site Tag**
Verify

Verify that the access points are registered with the Catalyst 9800 wireless LAN controller.

*Figure 40. Cisco Catalyst 9800 – Monitoring – AP Statistics*

Verify that wireless clients can connect to the **MT_Passenger_CAPWAP** SSID.

*Figure 41. Cisco Catalyst 9800 – Monitoring – Wireless Clients in MT_Passenger_CAPWAP*
Secure Equipment Access to Onboard Equipment

Cisco Secure Equipment Access (SEA) is a service available in the IoT Operations Dashboard that enables remote connectivity to applications and devices connected behind the industrial router. In this example, the SEA service is used to deploy the SEA agent on the IR1800 and enable remote connectivity to a Windows server running on the bus which hosts the Milestone XProtect application for video recording.

1. Install the SEA agent application from the IoT Operations Dashboard by navigating to the Secure Equipment Access > System Management > Network Devices, and then clicking Add Network Device.

Figure 42. SEA System Management
2. Select the network device that will host the SEA agent. In this example, an **IR1835** router is selected.

**Figure 43. SEA – Add Network Device**
3. The agent is then deployed on the router. During the deployment (or later), click **Add Connected Client**.

Figure 44. SEA Network Device Details and Connected Clients list
4. Enter a descriptive name and IP address for the client device. In this case, **192.168.113.100** is the address of the Windows server running the Milestone XProtect application on bus #1.

Figure 45. SEA – Add Connected Client

**Add Connected Client**

<table>
<thead>
<tr>
<th>Selection Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual entry</td>
</tr>
</tbody>
</table>

Enter the following information to enable Secure Equipment Access to the Connected Clients

<table>
<thead>
<tr>
<th>Client Name*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Milestone-XProtect-Bus1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Address/Host Name*</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.113.100</td>
</tr>
</tbody>
</table>
5. After the connected client is added, one or more access methods can be added to connect to the client device. Click **Add Access Method**.

Figure 46. SEA – Connected Client Details
6. In this example, the Windows server is accessed using Remote Desktop Protocol (RDP). For other types of devices, access methods like SSH or HTTPS, or even product specific native protocols could be configured here.

Figure 47. SEA – Add Access Method
7. Click **Remote Sessions**. All the available access methods for all connected client devices are displayed. Use the search box to narrow down the list of items you want to view. In this example, the IR1835 on Bus1 is configured to access the Milestone Windows server with RDP and an AXIS video camera with HTTPS.

**Figure 48. SEA – Remote Sessions**
8. Clicking **Open Session** for the RDP remote session opens up a new window in the browser with an RDP session to the Windows server. Other access methods (except for SEA Plus) have a similar experience. SEA Plus enables the use of other applications on the local user's computer to connect to remote devices.

**Figure 49. SEA – Remote Desktop Session**
IOx Applications

Example Vehicle CANBUS Data Application

This section shows an example IOx application written by Cisco to demonstrate some of the capabilities of the IR1800 router in conjunction with IOx edge computing. The application is available in Github, but is not supported by Cisco: https://github.com/keholcom/vehicle-obd2

The app is installed and managed through IoT Operations Dashboard. After installed and configured, it pulls data from the IR1800 GPS receiver (on Cellular 0/4/0 in this case) and polls the CANBUS for vehicle information. The type of information available on the CANBUS is vehicle dependent. On the test vehicle (2017 Chevrolet Silverado), the following metrics were available: speed, engine RPM, fuel level, trip time, coolant temperature, and intake air temperature.
Figure 50. IOx Application “vehicle-obd2” Details in IOT OD

In the screenshot above, the application configuration details are visible. This is where the application is set to point to an external MQTT broker which will receive the formatted vehicle telemetry messages.
The Device Configuration section is used to bind the \texttt{gps0} data source to the application. In this case, \texttt{gps0} refers to the GPS receiver on the first cellular modem (interface Cellular 0/4/0).

**Figure 51. IOx Application “vehicle-obd2” Device Configuration**

The MQTT broker receives the formatted vehicle telemetry messages from the IOx application. Subsequently, the data is written into a database for historical records and summarized in a dashboard view using Grafana. The dashboard shows a map of the historical geo-location of the vehicle, vehicle speed, engine RPM, altitude, and coolant temperature.

**Figure 52. IOx Application “vehicle-obd2” MQTT Messages**
The screenshots of the MQTT broker and dashboard are just for illustrative purposes, showing what is possible to do with data extracted using the IR1800 and IOX. This is not publicly available.

**Figure 53. IOx Application "vehicle-obd2" Dashboard**

---

**Bus Services**

A mass transit bus will typically have a variety of services provided by different vendors. These services include automatic passenger counting, emissions monitoring, video surveillance, and voice communications. The subsections that follow illustrate what these systems can look like for a bus deployment and are not meant to document how to configure or operate these services. Please refer to the vendor documentation for more information.
**Automatic Passenger Counting with DILAX**

DILAX provides the automatic passenger counting functionality as validated in the Cisco IoT solutions lab. The PRT-400 sensor is mounted above the equipment racks in the lab and calibrated for the actual height above the floor. An orange box was drawn to identify the floor as a zone. A green line was also drawn across the floor in the PRT-400 interface to simulate a doorway on a transit vehicle. The arrow on the green line identifies the exit direction. Each time a person walked from left to right in the photo, across the green line, the PRT-400 counted the movement as an exit. When a person walked from right to left across the green line, the sensor counted it as an entrance.

*Figure 54. DILAX PRT-400 passenger counter view of “doorway” and floor*
The DILAX SLS-1000 was then similarly setup in the lab and used stereoscopic vision to monitor the scene, identifying entrances and exits.

Figure 55. DILAX SLS-1000 passenger counter sensor 3D view
Emissions Monitoring with SensorComm Wi-NOx

SensorComm provides the Wi-NOx emissions monitoring system as validated for this Converged Public Transport solution. The Wi-NOx system comprises a sensor mounted in the exhaust pipe of the vehicle, and a readout electronics and interface board to convert the sensor signal into a serial data stream. The serial data is input into the IR1835 RS232 serial port which is mapped to an IOx app developed by SensorComm. The IOx app was installed using IoT OD App Management capability as shown in the figure that follows.

Figure 56. SensorComm Wi-NOx emissions monitoring IOX app upload with IoT OD
After the app is uploaded to IoT OD App Manager service, it can be installed to the IR1800.

**Figure 57. SensorComm Wi-NOx emissions monitoring IOX app installed on an IR1800**

To get the Wi-NOx serial data into IOX, some simple router configuration is required. This can be added to the IoT OD eCVD template Extended Form section for CLI.

```
interface Async0/2/0
  no ip address
  encapsulation relay-line
  line 0/2/0
  speed 115200
  relay line 0/2/0 0/0/0
```

After configuration, the serial data from the Wi-NOx interface board is received by the IR1800 and relayed to the IOX app. The text below shows an example of the raw serial data coming from Wi-NOx.

```
[IR1800_FC2649YWYT_RP_0:/]$ cat /dev/ttySerial
8183a6af8|18f00f52|8|c00fb0f1541f1f1f
8183a6b2a|18f00f52|8|c00fb0f1541f1f1f
8183a6b5c|18f00f52|8|c00fb0f1541f1f1f
8183a6bc0|18f00f52|8|c00fb0f1541f1f1f
8183a6bf2|18f00f52|8|c00fb0f1541f1f1f
8183a6c24|18f00f52|8|c00fb0f1541f1f1f
8183a6c56|18f00f52|8|c00fb0f1541f1f1f
8183a6c88|18f00f52|8|c00fb0f1541f1f1f
DEWPOINT
8183a6c8a|18f00f52|8|c00fb0f1541f1f1f
8183a6cede|18f00f52|8|c00fb0f1541f1f1f
8183a6d1e|18f00f52|8|c00fb0f1541f1f1f
```
The Docker logs from the IOX app show how the serial data has been received and decoded into a format that can then be sent over IP to a dashboard, database, or other application in the cloud.
Video surveillance on the transit vehicle is provided by two vendors, AXIS and Milestone. AXIS provides a range of ruggedized video cameras that are suitable for installation on bus or similar vehicle – either inside or out. Milestone provides the X-Protect software suite that provides the camera management, recording, rules, events, and monitoring capability for the video coming off the bus cameras.

The AXIS cameras are connected to a PoE ethernet port, either on the IR1800 directly, or on the subtended IE3x00 switch. The cameras can be configured through a locally hosted GUI, but more typically a centralized solution like Milestone X-Protect provides a more scalable solution. Once the recording servers are installed in the bus (on ruggedized compute running Windows) and in the datacenter/SOC (also running Windows) – the cameras can be discovered automatically by scanning an IP subnet as shown in the figure that follows.
Figure 58. Milestone XProtect – Add Cameras

After the cameras are configured to record to the recording server on the bus, rules can be configured to achieve the desired behavior. For example, a digital input on the AXIS camera can be connected to a panic button at the driver seat. When the panic button is pressed, the digital input causes the rule shown in the figure that follows to be activated and the camera to record video for 5 minutes. Alternatively, the digital input could be connected to a door open/close sensor.
Figure 59. Milestone XProtect – Rule for panic button with digital input
An additional rule to monitor the availability of the recording server (or cameras) on the bus can be added. At the end of a shift, when the bus pulls into the yard and connectivity is restored over the WGB link, the rule could trigger and retrieve all recorded video for the day. Refer to the figure that follows.

Figure 60. Milestone XProtect – Rule for video recording upload after connectivity is restored
The Milestone X-Protect Smart Client can also be used to monitor the video streams from all the managed cameras and recording servers. Refer to the figure that follows.

**Figure 61. Milestone XProtect Smart Client**
Voice Communication with InstantConnect

Voice communication between drivers, security personnel, and others can be implemented using the Instant Connect solution. This push-to-talk capability and advanced bridging of IP and LMR voice channels allows the agent at the central operations center to monitor multiple channels and speak on one or more channels simultaneously. The agent can use a desktop client as shown in the figure that follows.

Figure 62. Instant Connect desktop client
Drivers or other field personnel could similarly use a mobile client to participate in voice communications as well.

**Figure 63. Instant Connect app on RugGear 750 Android phone**
Additional Resources

Cisco References
Cisco IOx product documentation - https://developer.cisco.com/docs/iox/

Third-party References
SensorComm Technologies - https://www.sensorcommtech.com
Milestone XProtect - https://www.milestonesys.com/products/software/xprotect/
InstantConnect - https://www.instantconnectnow.com