# Configure a Fully Transparent Layer 2 Bridge Using URWB

© 2026 Cisco and/or its affiliates. All rights reserved.

Configure a Fully Transparent Layer 2 Bridge Using URWB ..... 3
Key capabilities ..... 3
Guidelines and limitations ..... 3
Configure Layer 2 transparency ..... 3
Layer 2 transparency commands and parameters ..... 6
Legal information ..... 7

© 2026 Cisco and/or its affiliates. All rights reserved.

## Configure a Fully Transparent Layer 2 Bridge Using URWB

This document describes Layer 2 transparency in an Ultra-Reliable Wireless Backhaul (URWB) network and explains how to configure and verify it. Layer 2 transparency forwards selected generic Layer 2 traffic across VLANs, supporting industrial protocols that do not use standard IP headers. The procedures apply to devices running UIW release 17.12.1 or later.

## Key capabilities

Layer 2 transparency provides the following capabilities:

- The system detects EtherTypes at the ingress and egress nodes of MPLS tunnels.
- Administrators can allow specific EtherTypes or enable Allow All to forward all detected EtherTypes.
- Ethernet-I frame forwarding can be controlled independently.
- PROFINET (0x8892) and QNX Qnet (0x8204) are allowed by default.

## Guidelines and limitations

Review these conditions before configuring the feature:

- Reload the device for changes to the Layer 2 transparency allow-list and Ethernet-I settings to take effect.
- The system reserves EtherTypes 0x0900–0x09FF and 0x8847. You cannot add these types to the allow-list manually.
- Filtering occurs at the ingress and egress nodes of MPLS tunnels within the URWB mesh network.

## Configure Layer 2 transparency

Enable VLANs, set the Native and Management VLAN IDs, and configure EtherType and Ethernet-I forwarding. You can perform the configuration through the CLI or Web UI.

### Before you begin

Confirm that the following prerequisites are met:

- The device is running UIW release 17.12.1 or later.
- The Native and Management VLAN IDs (VIDs) for the network are identified.
- The VLAN environment is established.

### Context

Perform this task to configure Layer 2 transparency using the CLI commands.

Establish an SSH session or a direct console connection to the device.

1. Use the **configure vlan status [enabled | disabled]** command to globally enable VLAN functionality on the device.

   ```
   Device# configure vlan enabled
   ```

2. Use the **configure vlan native vlan-id** command to assign the desired Native VLAN ID.

   ```
   Device# configure vlan native <VID>
   ```

© 2026 Cisco and/or its affiliates. All rights reserved.

The supported native VLAN range is 0 to 4094.

3. Use the **configure vlan management vlan-id** command to assign the desired Management VLAN ID.

```
Device# configure vlan management 100
```

The supported Management VLAN range is 1 to 4094.

**Note**: Configure the native VID and management VID according to your network design requirements.

4. Use the **configure mpls ether-filter allow-list add all** command to add all detected EtherTypes to the allow-list.

```
Device# configure mpls ether-filter allow-list add all
```

5. Use the configure mpls ether-filter ethernet-I forward command to configure the system to forward Ethernet-I frames.

```
Device# configure mpls ether-filter ethernet-I forward
```

6. Use the write command to write the changes to system memory.

```
Device# write
```

7. Use the reload command to reload the device and apply the new transparency settings.

```
Device# reload
```

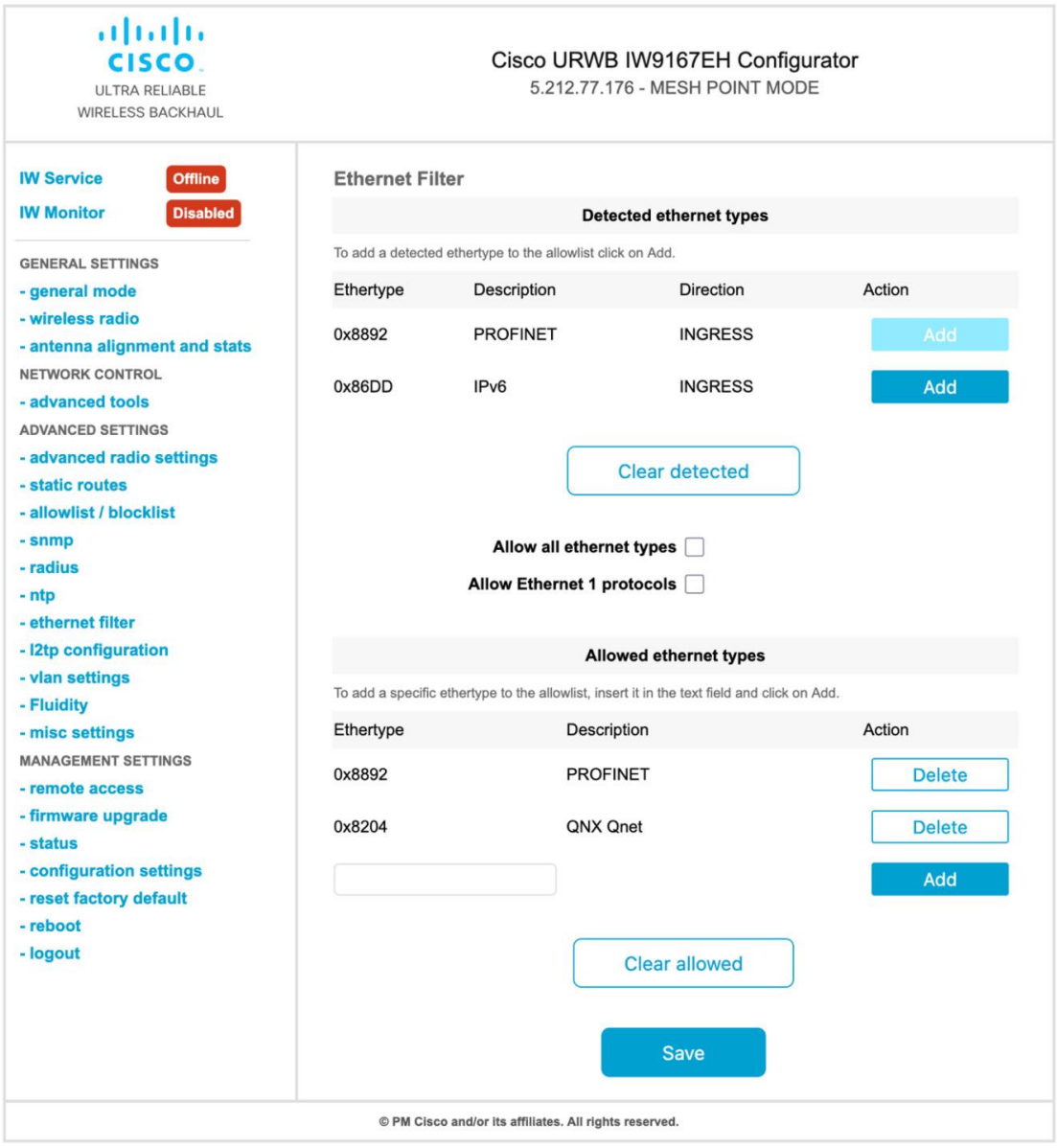
**Note**: The device will now forward all detected Layer 2 EtherTypes and Ethernet-I frames across the URWB network.

## Configure Layer 2 transparency using GUI

Perform this task to configure Layer 2 transparency on the Web UI.

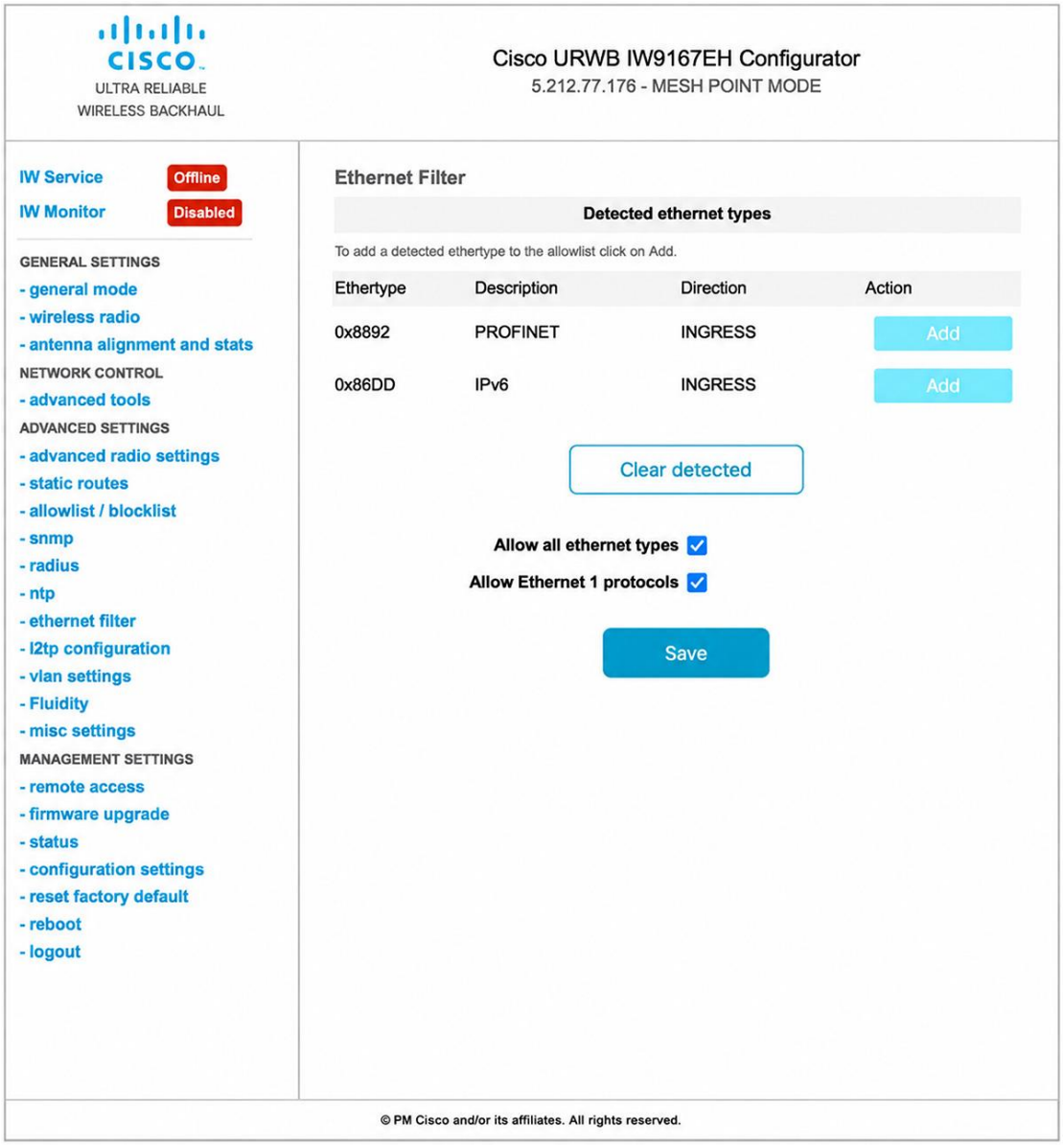
1. Choose **Advanced settings** > **Ethernet Filter**.

© 2026 Cisco and/or its affiliates. All rights reserved.




2. In the **Ethernet Filter** window, check the checkbox for **Allow all ethernet types**. This setting ensures that all detected Layer 2 traffic is forwarded without requiring manual entry of individual hex codes.

© 2026 Cisco and/or its affiliates. All rights reserved.




3. Check the checkbox for **Allow Ethernet 1 protocols** to permit Ethernet-I protocol frames.

4. Click **Save**.

5. Perform a **Reload or Reboot** of the device to apply the changes.

## Layer 2 transparency commands and parameters

### Verification commands

Use these CLI commands to monitor and verify Layer 2 transparency:

| Command | Description |
|---|---|
| show mpls config | Displays the current allow-list status and Ethernet-I forwarding state. |
| show mpls ether-filter | Lists EtherTypes currently detected by ingress nodes. |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Command | Description |
| --- | --- |
| configure mpls ether-filter table clear | Clears the table of detected EtherTypes that are not yet allowed. |

## Configuration parameters

The following parameters govern Layer 2 transparency:

- Allow-list range: 0x0 to 0xFFFF (hexadecimal).
- Reserved EtherTypes: 0x0900–0x09FF and 0x8847 cannot be added to the allow-list.
- MTU: When forwarding additional Layer 2 headers, ensure the wired interface MTU is sufficient to avoid fragmentation. The default MTU is 1600.

## Common EtherTypes

The following EtherTypes are used in URWB networks. PROFINET and QNX Qnet are allowed by default.

| EtherType | Protocol |
| --- | --- |
| 0x8892 | PROFINET (allowed by default) |
| 0x8204 | QNX Qnet (allowed by default) |
| 0x86DD | IPv6 |

## Legal information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html.

Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Examples, command output, network topology diagrams, and other figures are illustrative. Any use of actual IP addresses or phone numbers is unintentional and coincidental.

© 2026 Cisco Systems, Inc. All rights reserved.