Introduction

This document provides information on the theory of operation and configuration for the Cisco Unified Wireless LAN solution as it pertains to supporting Multicast applications such as Apple’s Bonjour protocol. This protocol enables Apple devices to query and announce specific services such as AirPlay which allows audio and video to be shared between devices dynamically.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used
This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

**Conventions**

Refer to Cisco Technical Tips Conventions for more information on document conventions.

**Deployment Considerations**

The Bonjour protocol operates on service announcements and service queries which allow devices to ask and advertise specific applications, such as:

- Printing services
- File sharing services
- Remote desktop services
- iTunes file sharing
- iTunes Wireless iDevice Syncing (in Apple iOS v5.0+)
- AirPlay, which offers these streaming services: Music broadcasting in iOS v4.2+ Video broadcasting in iOS v4.3+ Full screen mirroring in iOS v5.0+ (iPad2, iPhone4S or later)

Each query or advertisement is sent to the Bonjour multicast address for delivery to all clients on the subnet. Apple’s Bonjour protocol relies on Multicast DNS (mDNS) operating at UDP port 5353 and sends to these reserved group addresses:

- IPv4 Group Address - 224.0.0.251
- IPv6 Group Address - FF02::FB

The addresses used by the Bonjour protocol are link-local multicast addresses and thus are only forwarded on the local L2 domain. Routers cannot use multicast routing to redirect the traffic because the time to live (TTL) is set to one, and link-local multicast is meant to stay local by design.

**Configure the Controller to Support Bonjour**

**Deploy Bonjour Devices on a Single VLAN**

When deploying Bonjour over network, it is important that both the client and device offering the service are on the same VLAN. For the wireless network, this means ensuring each client is on the same backend interface in the controller.

**Note:** Apple TV (release v5.0) does not support WPA2-Enterprise authentication. For 802.1x networks, a workaround is to create a WPA2-PSK WLAN using the same wired interface.

For a large scale deployment, using a single VLAN may be impossible. The Apple TV Deployment Using VLAN Select section of this document details how it is possible to have clients on one VLAN while the Apple TV devices are on another.
**Enable Multicast Support**

Go to the Controller tab and then the Multicast link on the left-hand menu. Enable Global Multicast Mode and IGMP Snooping. In the v7.2 release, you should also enable MLD Snooping in order to deal with Bonjour over IPv6.

Multicast and snooping mechanisms are outside the scope of this document. For more background information on these topics, refer to IP Multicast Technology Overview.

**Configure the Multicast Distribution Mode to Access Points**

The Cisco Unified Wireless Network (CUWN) supports two methods of multicast distribution to access points (APs) associated with the controller. In both modes, the original multicast packet from the wired network is encapsulated inside a Layer 3 CAPWAP packet sent via either CAPWAP Unicast or Multicast to the AP. Since the traffic is CAPWAP encapsulated, APs do not have to be on the same VLAN as the client Bonjour traffic. The two methods of Multicast distribution are compared here:

<table>
<thead>
<tr>
<th>Delivery Mechanism</th>
<th>Multicast-Unicast Mode</th>
<th>Multicast-Multicast Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The controller replicates the multicast packet and sends it to each Access Point in a Unicast CAPWAP Tunnel</td>
<td>The controller sends one copy of the multicast packet</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supported Access Point Modes</th>
<th>FlexConnect and Local</th>
<th>Local Mode Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires L3 Multicast Routing on Wired Network</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Controller Loading</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Wired Network Loading</td>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>

**Multicast-Multicast Distribution Mode**

Multicast-multicast mode is the recommended option for scalability and wired bandwidth efficiency reasons.

**Note:** Multicast-multicast mode is required for the 2500-Series Wireless LAN Controller.

Go to the Controller tab under the General page and make sure AP Multicast Mode is configured
to use **Multicast** mode and that a valid group address is configured. The group address is an IPv4 multicast group and is recommended to be in the 239.x.x.x-239.255.255.255 range which is scoped for private multicast applications. Do not use the 224.x.x.x, 239.0.0.x or the 239.128.0.x address ranges for the multicast group address. Addresses in these ranges overlap with the link local MAC addresses and flood all switch ports, even with IGMP snooping enabled.

**Multicast-Unicast Distribution Mode**

If the wired network is not properly configured to deliver the CAPWAP multicast between the controller and AP or FlexConnect mode and APs will be used for centrally switched WLANs supporting multicast, then unicast-multicast mode is required.

Go to the **Controller** tab on the General page and make sure the AP Multicast Mode is configured to use **Unicast** mode.

**Verify Bonjour Is Being Snooped**

In order to verify that Bonjour is being forwarded correctly, browse to the **Monitor** tab and click the **Multicast** left-hand menu. The address of 224.0.0.251 should be visible from the list. Click on the MGID number in order to view the clients which are joined to the Bonjour group.

**Tune Multicast Data Rates**

Multicast applications such as Bonjour require special consideration when being deployed over a wireless network since a multicast in 802.11 is essentially sent out as a broadcast so all clients can hear it. The actual data rate used by the AP in order to transmit the Bonjour frames is the highest mandatory rate configured within that band. For 2.4GHz, this is a default of 11Mbps, and for 5GHz, this is a default of 24Mbps.

In order to optimize the delivery of these frames, it is important to tune the 802.11 data rates within the controller to allow multicast to be delivered at the highest rate that the coverage model of the network can support. For networks with a low density of APs, it may be necessary to keep the data rates at the default. For a network that does not have any requirement to support 802.11b clients, tuning the data rate to 12Mbps Mandatory and lower rates disabled will help to reduce multicast airtime utilization. This is configured under the Wireless tab and the 802.11b/g/n > Network menu.

**Note:** The RF Profiles feature available in v7.2 allows per AP-Group customization of data rates which allows tuning multicast transmission rates for different coverage areas.

**Ensure Peer-to-Peer Blocking Is Disabled**

Peer-to-peer blocking is configured on a per-WLAN basis and prevents clients on the wireless network from communicating with one another. By default, it is disabled for new WLANs, but if enabled, it can cause issues for services like AirPlay when the AppleTV is on the wireless network. Any Bonjour service that relies on communication between wireless clients can be broken by peer-to-peer blocking.

Under the **WLANs** tab > **Advanced** section of the WLAN configuration, make sure P2P Blocking Action is set to **Disabled**.

**Block Bonjour**
In some cases, it is desirable to filter out Bonjour in order to prevent discovery between two nodes while still enabling other multicast applications.

Complete these steps:

1. Create ACLs on the wireless LAN controller in order to filter out IPv6 Bonjour traffic.
2. **(Version 7.2 and above only)** - Create ACLs on the wireless LAN controller in order to filter out IPv6 Bonjour traffic. **Note:** The Bonjour ACL will only filter inbound multicast traffic from wireless clients to the wired network. The ACL does not filter multicast packets coming into the controller.
3. **(Version 7.2 and below)** - Browse to the Controller tab > Interfaces on the left-hand menu in order to apply the ACL. The ACL Name should be changed to the ACL specified in Step 1.
4. **(Version 7.2 and above)** - Apply the IPv4 and IPv6 ACL in order to filter out Bonjour traffic before it can be forwarded to other clients.

**Bonjour Application - Using Apple TV AirPlay**

Apple AirPlay allows the entire screen of an Apple iPad 2 or iPhone 4S to be displayed on the Apple TV (Generation 2). The discovery of the AirPlay service is done via Bonjour, and the subsequent connection is TCP-based uncasting the screen from the device to the Apple TV.

1. Check the Settings > AirPlay menu from the home screen in order to make sure the Apple TV has AirPlay enabled. An optional passcode can be set for security. This is advised in order to prevent screen stealing during a presentation.
2. On the Apple iOS device, double-click the home button in order to reveal the multi-tasking view.
3. Swipe left to right (twice for iPhone, once for iPad) in order to reveal a menu with the AirPlay icon as depicted here:
4. Choose Apple TV from the list, and enable Mirroring.
5. The status bar at the top of the Apple device will turn blue along with adding an icon for AirPlay, signifying that you are broadcasting your screen on the Apple TV.

**Apple TV Deployment Using VLAN Select**

The limitation of using Bonjour on a single VLAN is difficult to scale for large campus networks such as a university or enterprise. If a large subnet is created for all wireless clients, the multicast Bonjour messages would quickly consume up valuable airtime across the network. The VLAN Select feature can be used to assign clients to an array of VLANs on the backend, essentially breaking up the multicast domain. An option of the VLAN Select feature is the Multicast VLAN which allows a specific interface to be selected for downstream multicast traffic.

For more information on VLAN Select, refer to [VLAN Select and Multicast Optimization Features Deployment Guide](#).

Using VLAN Select with the multicast VLAN feature allows a separate subnet to be used for Apple TV devices, while still enabling AirPlay for use by all clients on a separate WLAN.

**Note:** The use of VLAN Select with other Bonjour applications (like messaging, or iTunes sharing) is limited because they are dependent on end user devices being able to send out announcements.
Complete these steps:

1. Go to the Controller tab > Interfaces on the left-hand menu. Create the necessary interfaces for the client VLANs (client-a1 and client-a2 in this example) and also an interface for the Apple TV subnet (client-mcast in this example). **Note:** The Apple TV could also be deployed using the Ethernet interface on the wired network. Make sure that their VLAN is the same as the multicast VLAN used. In this example, VLAN 40.

2. Go to the Controller tab > Interface Groups on the left-hand menu. Create a new interface group, and add in the previously created client interfaces (client-a1 and client-a2, in this example).

3. Go to the WLANs tab and create the client SSID. Select the interface group previously created in Step 2. Enable the Multicast VLAN feature and select the multicast interface created in Step 1. **Note:** The multicast interface feature is one-way, meaning Bonjour advertisements are sent down to clients, but the Bonjour discovery requests are not sent upstream to the Apple TV interface. This means the Apple TV should be forced to announce itself by being put to sleep, and then woken up. For more information, see the [Steps for Users of the VLAN Select - Apple TV Deployment](#) section of this document.

4. (Optional if Apple TVs are wired.) Create a new SSID for the Apple TVs. The security policy should be WPA2-PSK, and the interface should be the multicast VLAN created in Step 1. It is also advisable to configure the WLAN radio policy to 802.11a only, thereby keeping the Apple TV devices on 5GHz.

**Steps for Users of the VLAN Select - Apple TV Deployment**

In order to make sure that the Apple TV list is updated properly on the client, complete these steps:

1. Go to Settings > Sleep Now in order to put the Apple TV to sleep.
2. Make sure the iPad or iPhone used for presenting is connected to the clients wireless network.
3. Press any button on the remote in order to wake up the Apple TV.
4. Complete the steps in the [Bonjour Application - Using Apple TV AirPlay](#) section of this document.

**Bonjour Gateway Deployment**

The Apple Bonjour gateway solves the problem of Bonjour devices being unable to discover one another in a multi-subnet environment. The Bonjour gateway runs the open source Avahi ([http://avahi.org](http://avahi.org)) mDNS software which enables the device to cache and respond to Bonjour queries on other network interfaces.

The Apple Bonjour gateway is designed to sit on multiple network subnets and “reflect” the Bonjour requests across L3 boundaries. The Bonjour gateway should be installed on a PC or in a Virtual Machine which is connected to a trunk port on the network. Alternatively, the Gateway can have multiple physical Ethernet uplinks in order to connect to multiple subnets.
Cisco Switch Configuration for the Bonjour Gateway

The switch uplink configuration should use a trunk port with a native VLAN in order to provide management access to the device. The other tagged VLANs on the port are other subnets which require Bonjour Gateway functions.

interface GigabitEthernet4/14
  description Apple-Bonjour-Gateway
  switchport
  switchport trunk native vlan 20
  switchport trunk allowed vlan 20,21,25,26,40
  switchport mode trunk
end

Bonjour Gateway Deployment Steps

Complete these steps:

2. Boot the Laptop/Desktop/Server machine from ISO image. Complete the on-screen instructions in order to install the Ubuntu software onto your device. **Note:** For the purposes of this document, we will be using Ubuntu Desktop as the example OS.
3. In order to open the Terminal application, click the top icon in the toolbar and enter **Terminal** in the field.
4. Issue the `ifconfig` command in order to confirm the device has Ethernet connectivity access.
   ubuntu@ubuntu:~$ ifconfig
   eth0      Link encap:Ethernet  HWaddr 00:50:56:b3:5e:e2
         inet6 addr: fe80::250:56ff:feb3:5ee2/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:46 errors:0 dropped:0 overruns:0 frame:0
       TX packets:82 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
       RX bytes:4186 (4.1 KB)  TX bytes:8613 (8.6 KB)
          Interrupt:18 Base address:0x2000
5. Add the Avahi daemon and VLAN packages to the OS via the `sudo apt-get install vlan avahi-daemon` commands.
6. Edit the Avahi configuration file and enable the reflector functionality in the Avahi Daemon.
   ubuntu@ubuntu:~$ sudo nano /etc/avahi/avahi-daemon.conf
7. Within the configuration file, change the “enable-reflector” option to *yes* and make sure that no # symbol is before the line.
   #publish-domain=yes
   #publish-dns-servers=192.168.50.1, 192.168.50.2
   #publish-resolv-conf-dns-servers=yes
   #publish-aaaa-on-ipv4=yes
   #publish-a-on-ipv6=no
   [reflector]
   enable-reflector=yes
   #reflect-ipv=no
8. Issue the `sudo vconfig add eth0 <VLAN ID>` command in order to add a VLAN:
#publish-domain=yes
#publish-dns-servers=192.168.50.1, 192.168.50.2
#publish-resolv-conf-dns-servers=yes
#publish-aaaa-on-ipv4=yes
#publish-a-on-ipv6=no

[reflector]
enable-reflector=yes
#reflect-ipv=no

Note: This command may output additional text containing “WARNING: Could not open /proc/net/vlan/config.” This does not affect the capabilities of the Bonjour Gateway.

9. A new Ethernet interface in Linux will be created under the nomenclature of `eth.<VLAN ID>`. This new interface can be statically assigned an IP address or run DHCP. In order to run DHCP on the interface, issue the `sudo dhclient eth0.<VLAN ID>` command.

#publish-domain=yes
#publish-dns-servers=192.168.50.1, 192.168.50.2
#publish-resolv-conf-dns-servers=yes
#publish-aaaa-on-ipv4=yes
#publish-a-on-ipv6=no

[reflector]
enable-reflector=yes
#reflect-ipv=no

10. Issue the `ifconfig` command again in order to confirm that the newly created interface has an IP address:

    ubuntu@ubuntu:~$ ifconfig
    eth0    Link encap:Ethernet  HWaddr 00:50:56:b3:5e:e2
            inet6 addr: fe80::250:56ff:feb3:5ee2/64 Scope:Link
            inet6 addr: 2001:db8:0:10:250:56ff:feb3:5ee2/64 Scope:Global
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:123 errors:0 dropped:26 overruns:0 frame:0
            TX packets:126 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:123111 (12.3 KB)  TX bytes:14712 (14.7 KB)
            Interrupt:18 Base address:0x2000

    eth0.20   Link encap:Ethernet  HWaddr 00:50:56:b3:5e:e2
            inet addr:192.168.20.20  Bcast:192.168.20.255  Mask:255.255.255.0
            inet6 addr: fe80::250:56ff:feb3:5ee2/64 Scope:Link
            inet6 addr: 2001:db8:0:20:250:56ff:feb3:5ee2/64 Scope:Global
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:3 errors:0 dropped:0 overruns:0 frame:0
            TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:762 (762.0 B)  TX bytes:5508 (5.5 KB)

11. Repeat steps 8 through 9 for as many VLANs needed on the Bonjour gateway. Note: The Avahi Bonjour software on the gateway will automatically listen on the new interfaces with IP addresses.

12. List the current Bonjour-capable devices on all subnets connected to the gateway using the `avahi-browse --all -t` command:

    ubuntu@ubuntu:~$ avahi-browse --all -t
    + eth0.26 IPv4 admin@MBP-250 (2) iChat Presence local
    + eth0.26 IPv4 admin@MBP-130 iChat Presence local
    + eth0.25 IPv4 admin@MBP-250 (2) iChat Presence local
    + eth0.25 IPv4 admin@MBP-130 iChat Presence local
    + eth0.30 IPv4 admin@MBP-250 (2) iChat Presence local
    + eth0.30 IPv4 admin@MBP-130 iChat Presence local
    + eth0.20 IPv4 admin@MBP-250 (2) iChat Presence local
    + eth0.20 IPv4 admin@MBP-130 iChat Presence local
Troubleshoot Bonjour Applications

View Available Bonjour Services

In order to troubleshoot Bonjour connectivity issues, the free Mac OS X utility, Bonjour Browser, is useful in viewing available devices. A remote printer on an Apple AirPort Express is shown here:

Related Information

- Technical Support & Documentation - Cisco Systems