Air Time Fairness(ATF) Deployment Guide Rel 8.4

Revised: October 10, 2017,

Introduction

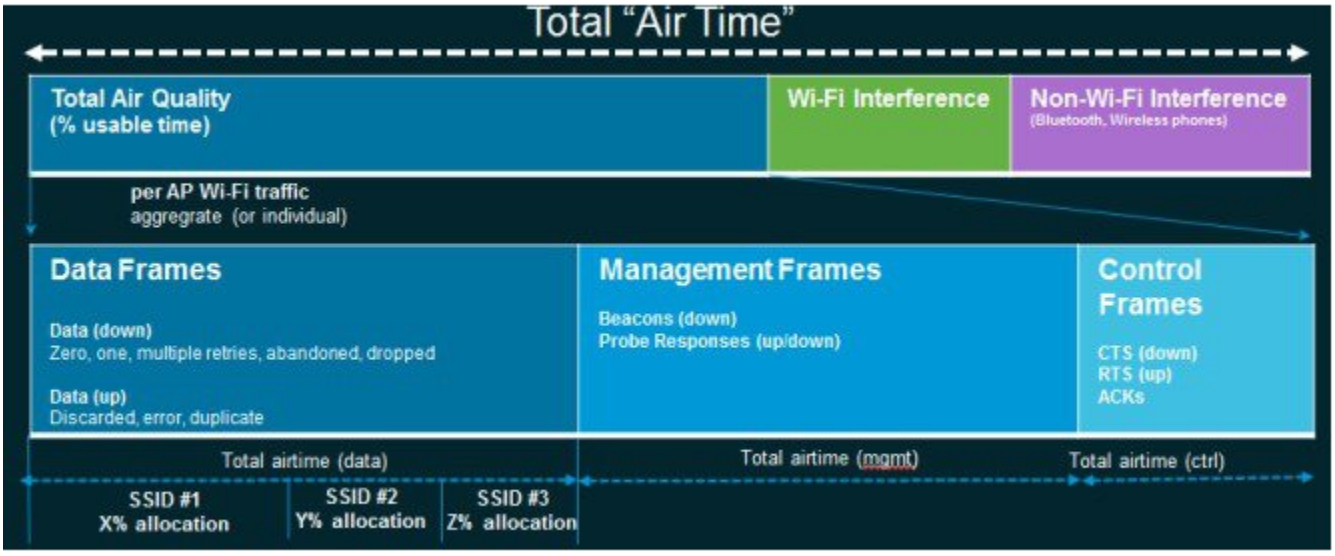
This document introduces ATF (Air Time Fairness) feature, and provides general guidelines for its deployment. The purpose of this document is to:

- Provide an overview of ATF feature, and its deployment within the Cisco Unified Architecture.
- Highlight key Service Provider features

Introduction to Air Time Fairness (ATF) Phase 1

Traditional (wired) implementations of QOS regulate egress bandwidth. With wireless networking, the transmission medium is via radio waves that transmit data at varying rates. Instead of regulating egress bandwidth, it makes more sense to regulate the amount of airtime needed to transmit frames. Air Time Fairness (ATF) is a form of wireless QOS that regulates downlink airtime (as opposed to egress bandwidth). Large scale, high density Wi-Fi deployments are driving this feature. Wireless Network owners are mandating that their applications be allocated some fixed percentage of the total bandwidth of the Wi-Fi network. At the same time, with capital sharing being considered with multiple cellular providers, ATF is needed to ensure fairness of usage across operators.

Before a frame is transmitted, the ATF budget for that SSID is checked to ensure that there is sufficient airtime budget to transmit the frame. Each SSID can be thought of as having a token bucket (1 token = 1 microsecond of airtime). If the token bucket contains enough airtime to transmit the frame, it is transmitted over the air. Otherwise, the frame can either be dropped or deferred. While the concept of dropping a frame is obvious, deferring a frame deserves further explanation. Deferring a frame means that the frame is not admitted into the Access Category Queue (ACQ) . Instead, it remains in the Client Priority Queue (CPQ) and may be transmitted at a later time when the corresponding token bucket contains a sufficient number of tokens (unless the CPQ reaches capacity, at which point the frame will be dropped regardless). The majority of the work involved for ATF takes place on the access points. The wireless controller is used simply to configure the feature and display results.



Cisco Air Time Fairness (ATF) Use Cases

Public Hotspots (Stadium/Airport/Convention Center/Other)

In this instance a public network is sharing a WLAN between two (or more) service providers and the venue. Subscribers to each service provider can be grouped and each group can be allocated a certain percentage of airtime.

Education

In this instance, a university is sharing a WLAN between students, faculty, and guests. The guest network can be further partitioned by service provider. Each group can be assigned a certain percentage of airtime.

Enterprise or Hospitality or Retail

In this instance, the venue is sharing a WLAN between employees and guests. The guest network can be further partitioned by service provider. The guests could be sub-grouped by tier of service type with each subgroup being assigned a certain percentage of airtime, for example a paid group is entitled to more airtime than the free group.

Time Shared Managed Hotspot

In this instance, the business entity managing the hotspot, such as a service provider or an enterprise, can allocate and subsequently lease airtime to other business entities.

ATF Functionality and Capabilities

- ATF policies are applied only in the downlink direction (AP transmitting frames to client). Only airtime in the downlink direction, that is AP to client, can be controlled accurately by the AP. Although airtime in the uplink direction, that is client to AP, can be measured, it cannot be strictly controlled. Although the AP can constrain airtime for packets that it sends to clients, the AP can only measure airtime for packets that it 'hears' from clients because it cannot strictly limit their airtime.
- ATF policies are applied only on wireless data frames; management and control frames gets ignored.
- When ATF is configured per-SSID, each SSID is granted airtime according to the configured policy.
- ATF can be configured to either drop or defer frames that exceed their airtime policies. If the frame is deferred, it will be buffered and transmit at some point in the future when the offending SSID has a sufficient airtime budget. Of course, there is a limit as to how many frames can be buffered. If this limit is crossed, frames will be dropped regardless.
- ATF can be globally enabled or disabled
- ATF can be enabled or disabled on an individual access point, AP group or entire network
- ATF is supported in release 8.4 on the **1260, 1700, 2600, 2700, 3600, 3500, 3700, 1550-128mb,** and **1570** series access points in **local** and **FlexConnect** mode.
- ATF on Mesh is supported in release **8.4** on **1550-128mb, 1560, 1570** and **3700** series MAPs.
- ATF results and statistics are available on the wireless controller.

ATF Modes of Operation

The Framework behind the ATF monitor mode is to allow the user to view and get the stats of overall Air Time being used i.e. to report the Air Time usage for all the AP transmissions. The ATF in monitor mode can be enabled on following levels.

- Disable Mode: By default ATF is disabled on the WLC
- Monitor Mode: To monitor airtime usage on your network

- Enforce—Policy Mode: Assigning ATF policies on your network
    - Strict Enforcement
    - Optimized

Monitor Mode Configuration

The Framework behind the ATF monitor mode is to allow the user to view and get the stats of overall Air Time being used i.e. to report the Air Time usage for all the AP transmissions. The ATF in monitor mode can be enabled on following levels:

- Per AP
- Per AP Group
- Network (all APs)

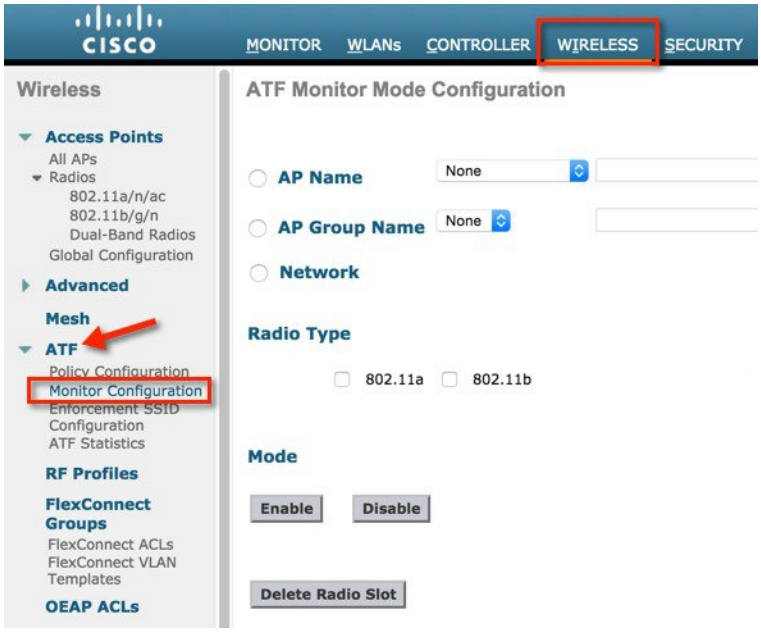
To configure ATF in monitor mode, perform the following steps:

Procedure

Step 1 Choose **WIRELESS > ATF > Monitor Configuration** from WLC's main menu bar.

Step 2 Select **AP Name** or **AP Group Name** or **Network** (all the APs on that particular WLC).

Step 3 Select radio type **802.11a** (5 GHz) or **802.11b** (2.4 GHz) or both.

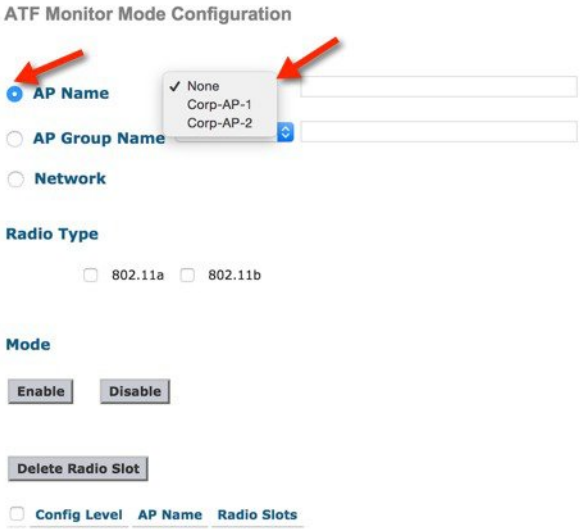


Per AP Monitoring Configuration

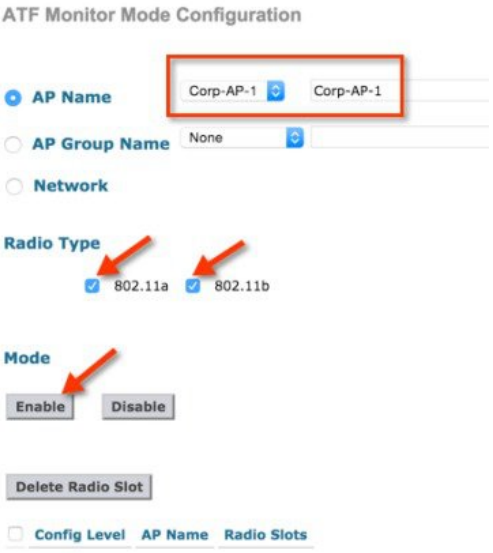
For AP monitoring configuration, perform the following steps

Procedure

Step 1 Click **AP Name** and from the drop down menu choose the AP.



Step 2 Choose the **Radio Type** by checking the 802.11a or 802.11b or both radio boxes and click **Enable** under the **Mode** option.



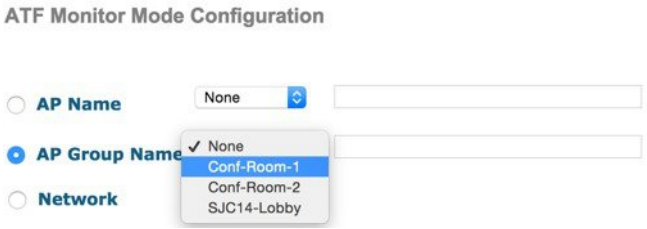
Once configuration is done it displays the config level, AP name and radio slots (**Slot 0 is 802.11b Radio and Slot 1 is 802.11a Radio**) on which monitoring is enabled.

Per AP Group Monitoring Configuration

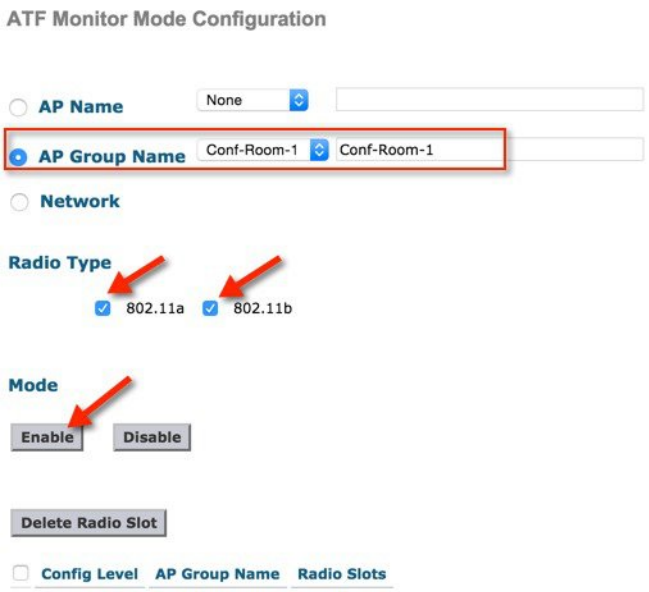
For per AP group monitoring configuration, perform the following steps:

Procedure

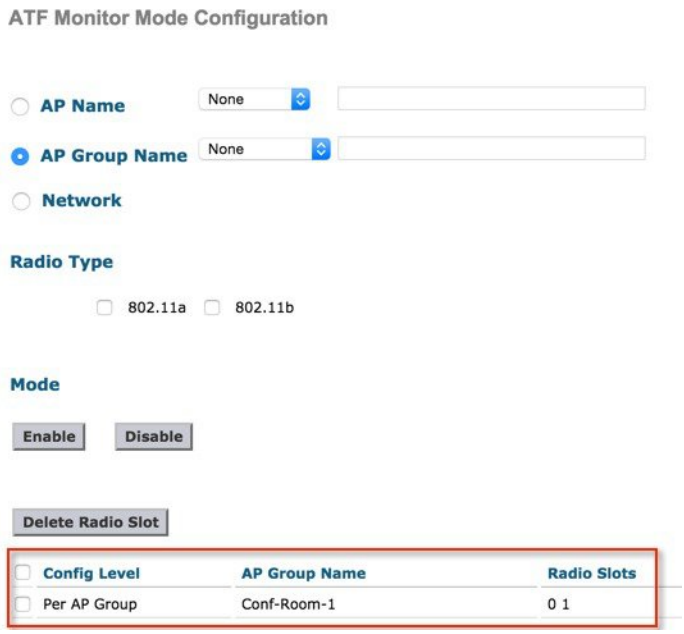
Step 1 Click **AP Group Name** and from the drop down menu choose the AP Group.



Step 2 Choose the **Radio Type** by checking the 802.11a or 802.11b or both radio boxes and click **Enable** under the **Mode** option.



Once configuration is done it displays the config level, AP name and radio slots (**Slot 0 is 802.11b Radio and Slot 1 is 802.11a Radio**) on which monitoring is enabled.



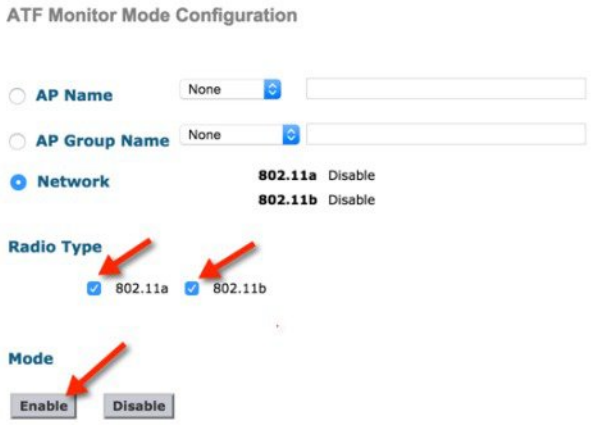
ATF Network Monitoring Configuration

To monitor Air Time on the network, perform the following steps:

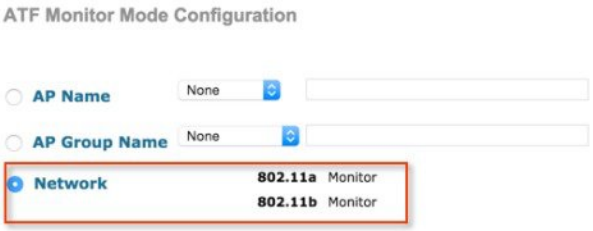
Procedure

Step 1 Click **Network** and this displays the monitor is disabled on the network.

Step 2 Choose the **Radio Type** by checking the 802.11a or 802.11b or both radio boxes then click **Enable** under the **Mode** option



When ATF network monitoring is configured user can see that Radio status change to Monitor from Disable state.



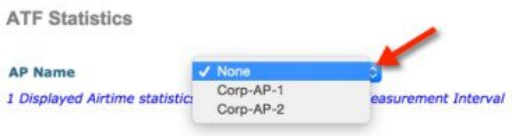
Monitoring ATF Statistics

Procedure

Step 1 To view the ATF statistics from WLC main menu go to **WIRELESS > ATF > ATF Statistics**.

Note Currently in this release ATF statistics are only available per AP.

Step 2 Choose the AP from the AP Name dropdown list.



The ATF statistics will show under two following values:

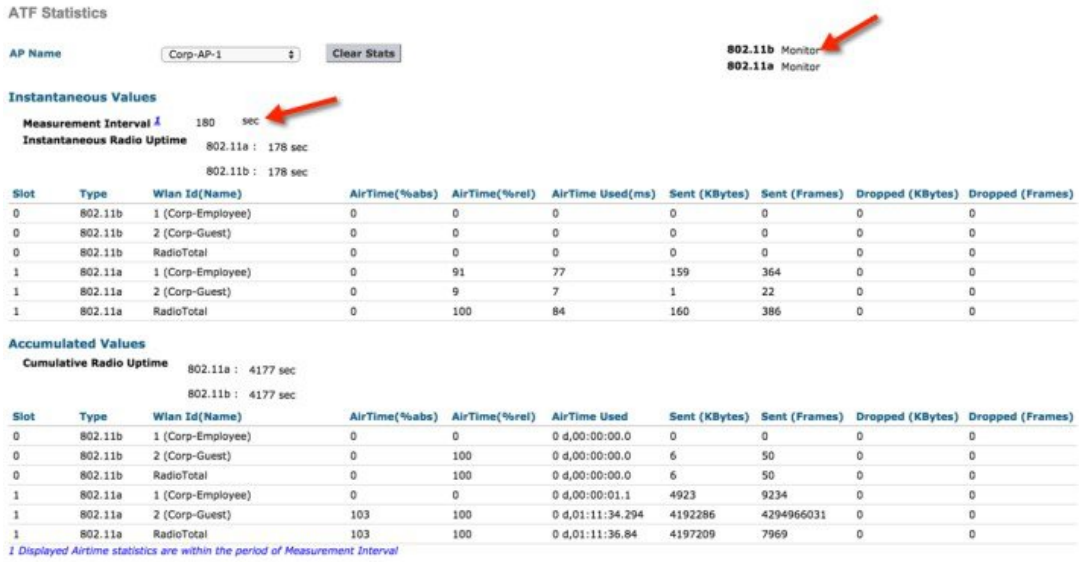
- Instantaneous Values
- Accumulated Values

The Instantaneous values reflect the ATF stats through the measurement interval and Instantaneous Radio uptime. By default the measurement interval is set to180 sec. This is configurable in the range 0 to 65535 on the AP.

User can view the atf stats per WLAN for both 802.11a and 802.11b radios which shows the percentage of AirTime (%abs), percentage of Realtive AirTime(%rel), AirTime used value in miliseconds (ms)

- AirTime (%abs)—Number of airtime units being used per SSID
- Relative AirTime (%rel)—Percentage of time used per SSID
- Airtime Used(ms)—Total airtime used per SSID

The Accumulative Values are the instantaneous ATF statistics which were accumulated over the measurement interval.

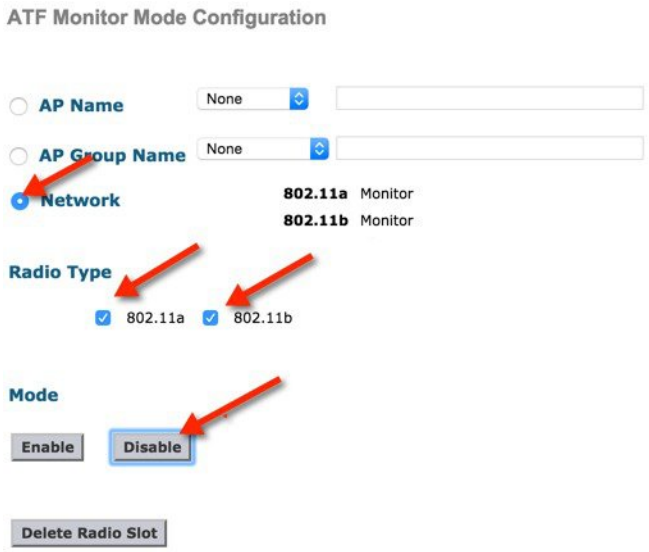


Disabling ATF Monitor Mode

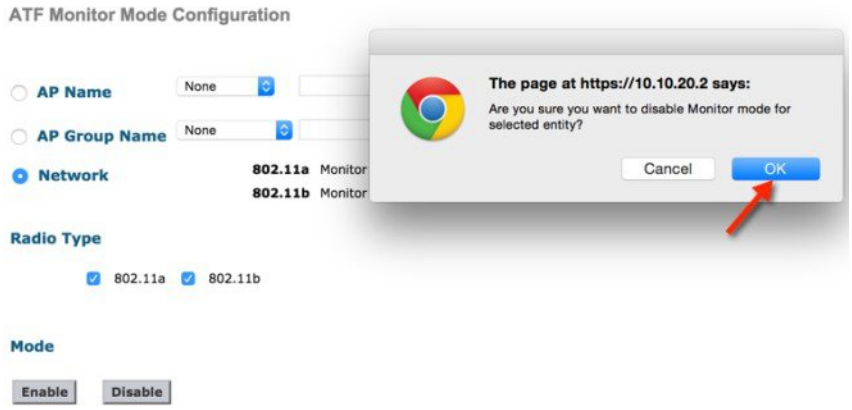
Procedure

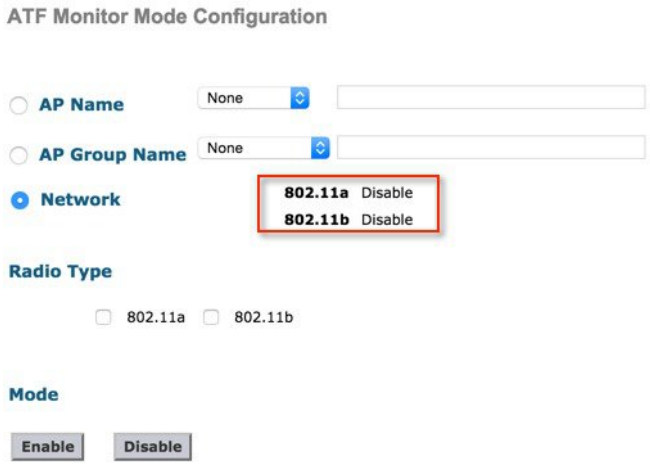
Step 1 To disable the ATF monitoring navigate to **WIRELESS > ATF > Monitor Configuration**.

Step 2 Choose the options **AP Name, AP group and Network** from the drop down menu, whichever the user has previously enabled. Select the **Radio Type** the user want to disable and click **Disable**.



Step 3 Click **OK** on the pop up conformation to disable the ATF.





ATF Enforce-Policy Mode

The Enforcement of Air Time is based on the configured Policy. The ATF Policy/Policies are set by user according to the network requirements.

Air-Time can be Enforced on following parameters:

- WLAN and on all APs connected within a WLC's network
- Per AP group
- On an individual AP

Strict Enforcement per WLAN—Air-Time used by the WLANs on a Radio will be strictly enforced up to the configured limits in the Policies

Optimal Enforcement per WLAN—Share unused air-time from other SSIDs

Steps to Configure ATF

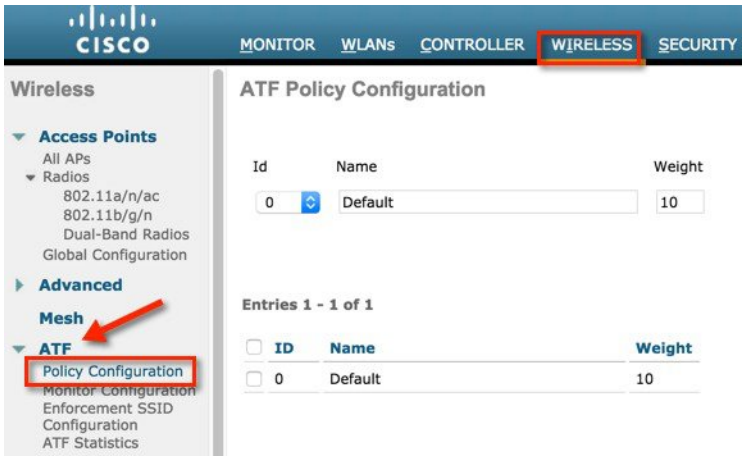
Create Policy

To configure ATF first the user need to create or configure ATF policy.

Procedure

Step 1 Navigate **WIRELESS > ATF > Policy Configuration.**

Step 2 The **Default** policy is 10 and the user has to assign weight from 5 to 100.



Step 3 To create user own policy select the policy Id from the drop down menu and assign a name and weight. Here Weight is the percentage of Air Time which user want to assign to a policy.

Step 4 Click **Create**.

In the example we have created multiple policies with the name **atf-80** and **atf-20** with the Weights 80 and 20 respectively.

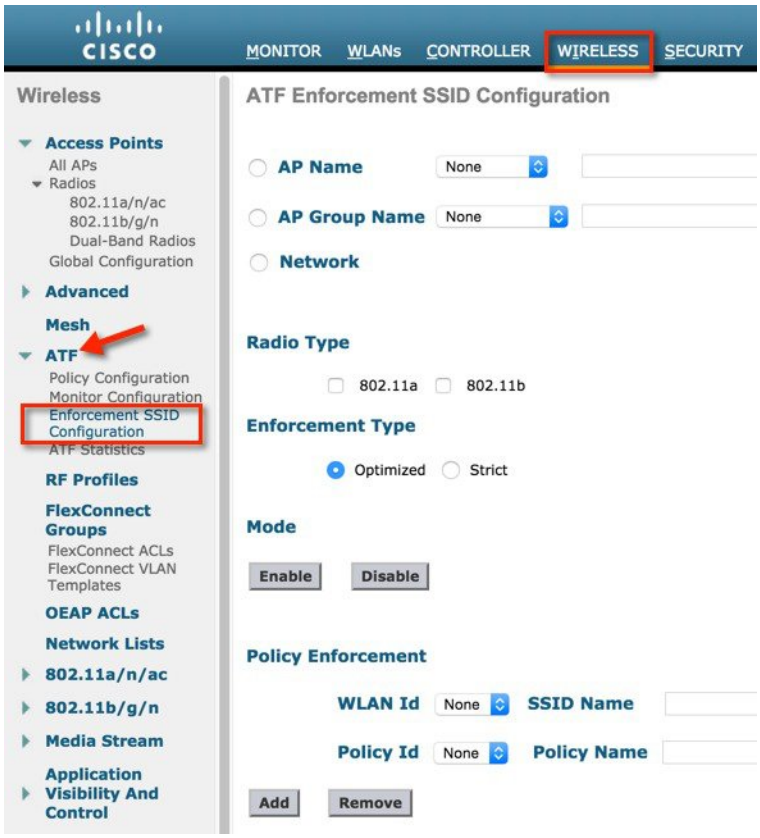
Policy Enforcement on SSID

Note First disable the WLANs on which you want to enable policy enforcement.

Once the policy is configured user can apply the policy to a particular WLAN or on all WLANs per AP group or on an individual AP.

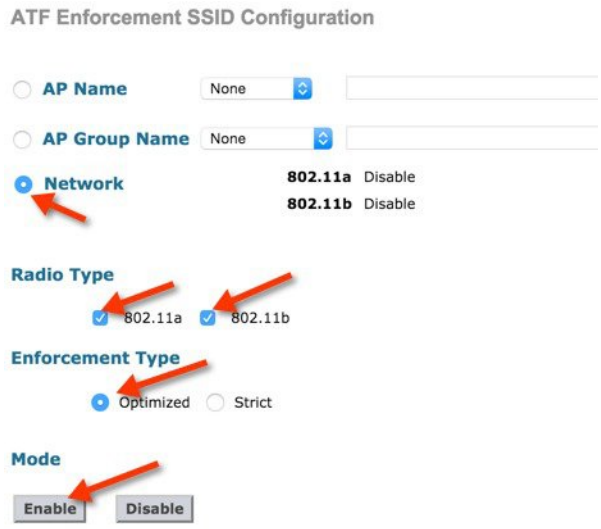
Procedure

Step 1 Naviage to the WLC main menu **WIRELESS > ATF > Enforcement SSID Configuration**.



Step 2 To configure it on the network Select the parameters **Radio Type**, **Enforcement Type** (can select either Optimized or Strict; by default **Optimized** is selected.

Step 3 Click **Enable** under the **Mode**.



When applied, the webpage gives the popup warning to disable the WLAN id before configuring policy enforcement. Click **Ok**, if the WLAN is disabled the enforcement gets applied.

The policy Enforcement shows on Radios and also the Optimization shows Enabled.

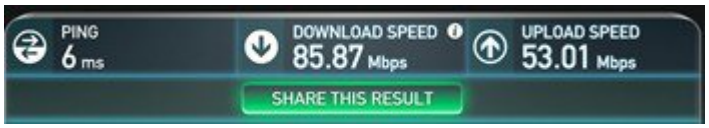
Step 4 To enable strict enforcement policy then select **Strict** option under Enforcement type.
Strict option does not allow sharing of its weighted ratio slot with other WLANs (SSIDs).

When the ATF configuration is done, then **Enable the WLANs** on which ATF was applied. Once the clients are associated to these WLANs user can view the ATF statistics under the ATF statistics page as previously shown in **Monitoring ATF Statistics** section.

The user can also run a speed test to verify the ATF by configuring two WLANs with different ATF policies.

In the example we have configured two ATF policies, one with weight 80 and other with weight 20.

1 We connected a wireless client to SSID with ATF policy with weight 80 configured and observe the effect of the ATF on this WLAN by run http://www.speedtest.net/



2 Connected the same wireless client to SSID with ATF policy with configured as 20 and observed the affects of the ATF on that WLAN. You should see speedtest performance on the download side is much slower. The test results might vary due to the air time availablity, interefrence and so on.

Air Time Fairness–Client Fair Sharing (ATF—Phase 2 Rel 8.2)

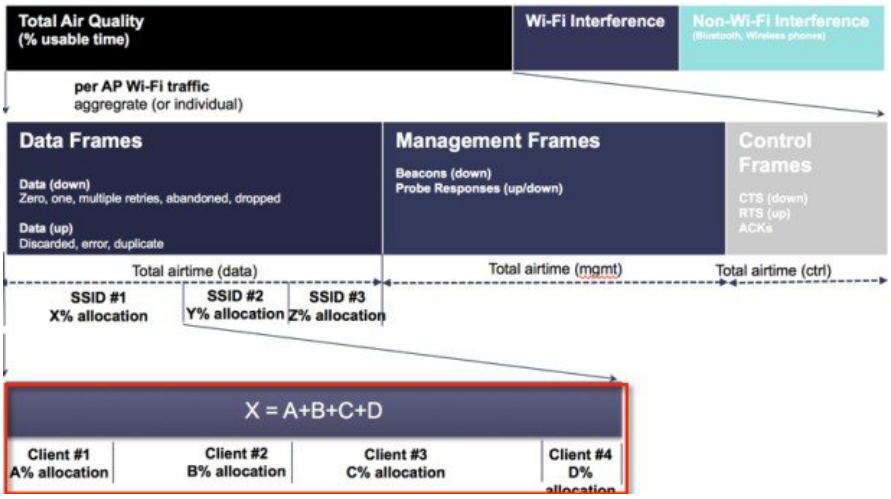
Feature Description

ATF Client Fair Sharing/per client entitlement is introduced in 8.2 release. Client fair share ensures the clients within a SSID/WLAN are treated equally based on their utilization of the radio bandwidth.

Benefit

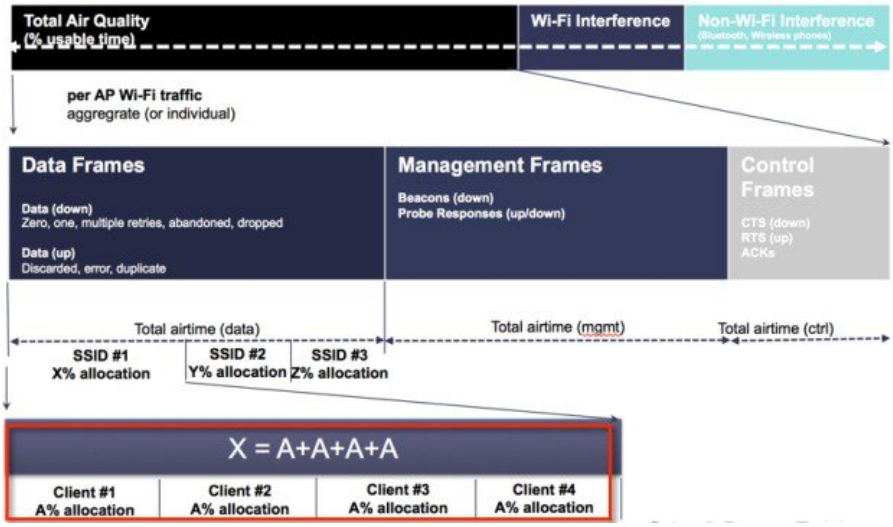
Currently, as part of 8.1 MR2 and MR3 release, SSID based Airtime entitlement is accomplished. However, with SSID based Airtime Fairness, there is no guarantee for the clients within the SSID to be treated equally based on their utilization of the radio bandwidth. There is a potential risk where one or few clients shall end up utilizing the complete airtime allocated for a SSID/WLAN by ruining the opportunity of Wi-Fi experience for rest of the clients within the same SSID.

ATF Phase 1 (Without Client Fair Sharing)



To overcome this problem, in 8.2 release each ATF policy have a new option to turn on or off client fair sharing among clients associated to a policy. This option can be executed while creating, modifying the policy in the Wireless LAN Controller. Customer can use this option or feature to provide fair sharing of Airtime between clients associated to a SSID. As shown below all the clients associated to SSID gets equal air time.

ATF Phase 2 (With Client Fair Sharing)



ATF Configuration Overview

Procedure

Step 1 First configure WLANs on the controller.

Step 2 Configure ATF Policies and enable ATF assign those policies to the WLANs.

Step 3 Connect clients to the ATF enabled WLAN and use media stream applications such as YouTube or www.speedtest.net and observe throughput performance with different ATF policies and weights for downstream data traffic.

Configuration for ATF Phase 2

Procedure

Create WLANs on the controller in our setup we created two WLANs PODX-atf20 and PODX-atf80.

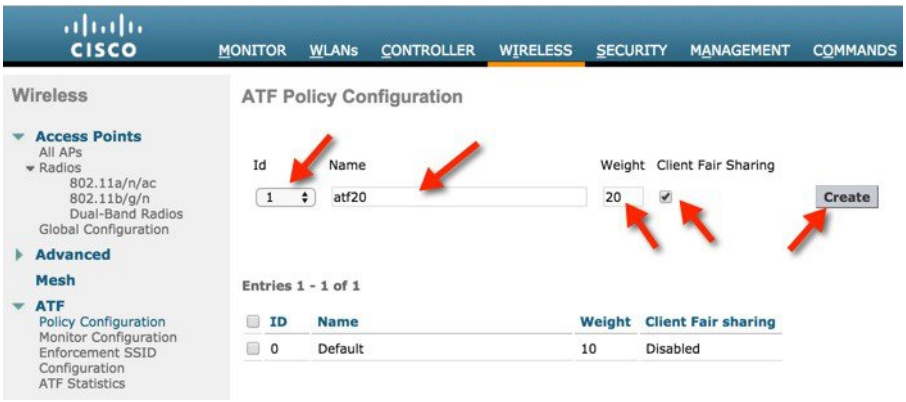
Creating ATF Client Fair Sharing Policies

Procedure

Step 1 On the Controller GUI under **WIRELESS > ATF** click **Policy Configuration** and configure **Id Name**.
Id Name can be any intuitive name, in our example we are configuring the name **atf20** and **atf80**) for weights of 20 and 80 respectively.

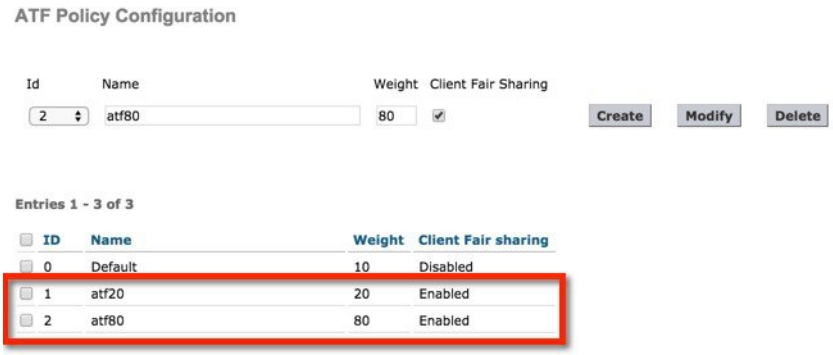
Step 2 Check the **Client Fair Sharing** box and hit **Create** to Create two policies.
User can assign there own ATF policy weights in example below we are using 20 and 80.

- For ATF Policy1: Id=1 Name=atf20 weight=20
- For ATF Policy2: Id=2 Name=atf80 weight=80



The configuration sets the policy, which can be applied per radio.

The two Policy IDs and Weights define policy Id **1 with weight 20** and the second policy Id **2 with weight 80** and **Client Fair Sharing** shows Enabled.



Note Please note these policies have weighted ratios and not percentages, so the total can exceed 100. The minimum weight can be set to 10.

Configure and Enable ATF policy on the Network and per specific Radio Type

Procedure

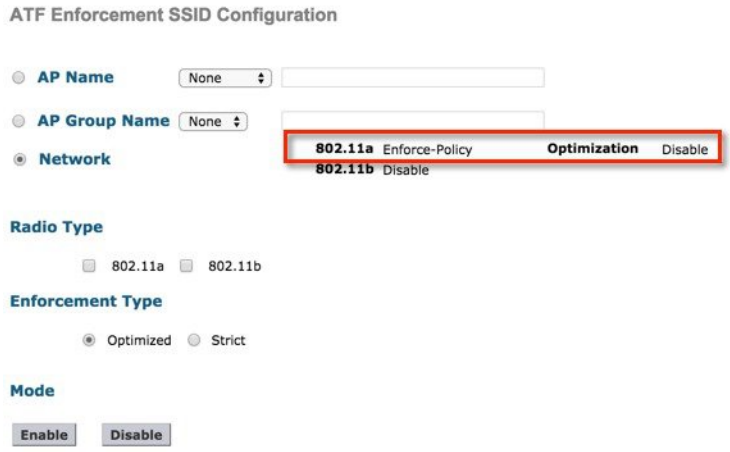
Step 1 Navigate **Wireless > ATF > Enforce SSID configuration**.

Step 2 Select **Network** and select **Radio Type** as 802.11a/b.

Step 3 Choose the policy Enforcement Type as**Optimized** or **Strict**. Apply policy as **Strict** in the setup.

Note When policy configured as **optimized** then WLAN with that option applied to it can share its weighted slot with other WLANs if its own slot is not being used in the given time. **Strict** option does not allow sharing of its weighted ratio slot.

The policy displays that it has been enabled on 5GHz radio and is not Optimized but in Strict mode.



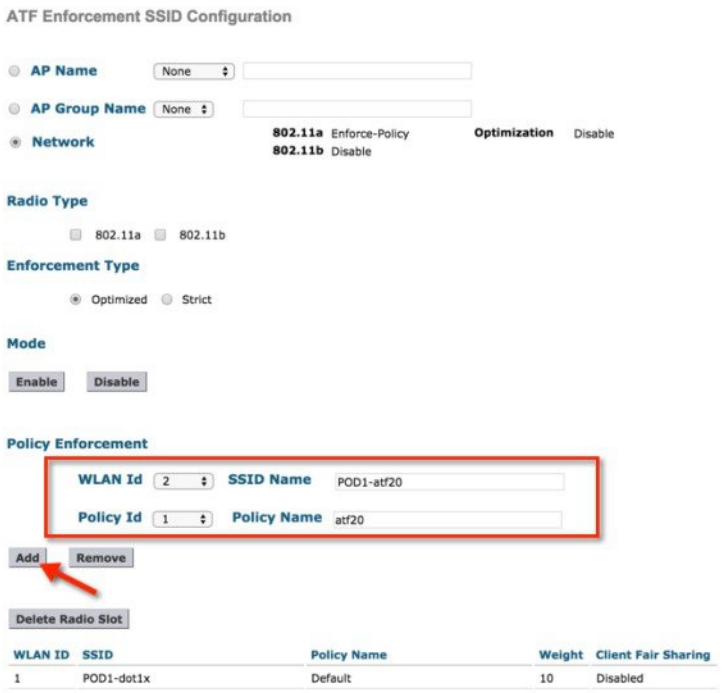
Apply ATF Policy on WLANs

Procedure

Step 1 Navigate **Wireless > ATF > Policy Enforcement**.

Step 2 Select the **WLAN Id** and **Policy Id**.

Step 3 Click **Apply**.
We use ATF policy (atf20) for one WLAN and policy (atf80) for another WLAN as shown.



Once the policies are created and applied to the WLANs, users can check this by running **show atf config wlan** command from WLC CLI and also on the GUI.

You can see from the output that ATF policy configured WLANs are set with configured weights of 20 and 80 and the WLAN on which we did not apply the policy is set to default weight of 10. Also check that Client Fair Sharing shows Enabled for ATF polices we created.

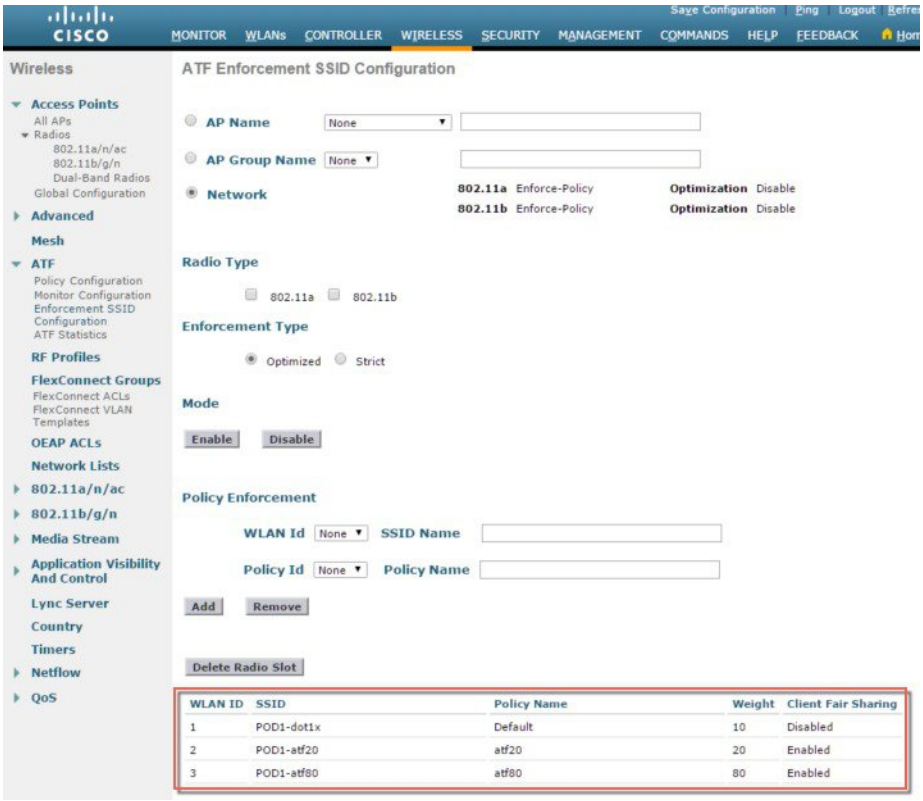
Here is an example is from CLI to confirm the policies have been applied

```
(POD1-WLC) >show atf config wlan

WLAN ID  SSID                 Policy-Name                      Weight  Client Sharing
-------  -------------------  -------------------------------  ------  --------------
1        POD1-dot1x           Default                          10      Disabled
2        POD1-atf20           atf20                            20      Enabled
3        POD1-atf80           atf80                            80      Enabled
```

Enable WLANs in Disabled State

Procedure

Step 1 Navigate to**ATF > Enforcement SSID Configuration** settings.



Step 2 Connect two wireless clients to SSID that is configured with policy 80 and observe the effect of the ATF on this WLAN.

Step 3 Run www.speedtest.net simultaneously on the clients at the same time.
The test results might vary due to the clients capability, interference and other factors.

Step 4 Connect a wireless Client to SSID configured with ATF policy and observe the effects of the ATF on that WLAN.
You should see speedtest performance on the download the test results might vary due to the clients capability, interference and other factors.

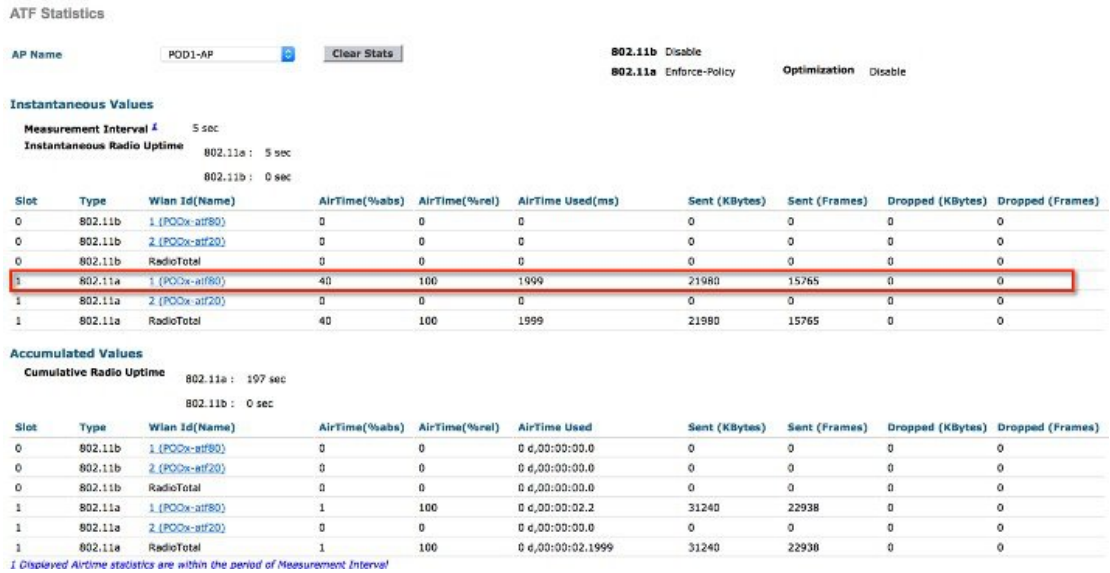
Client ATF Statistics

Procedure

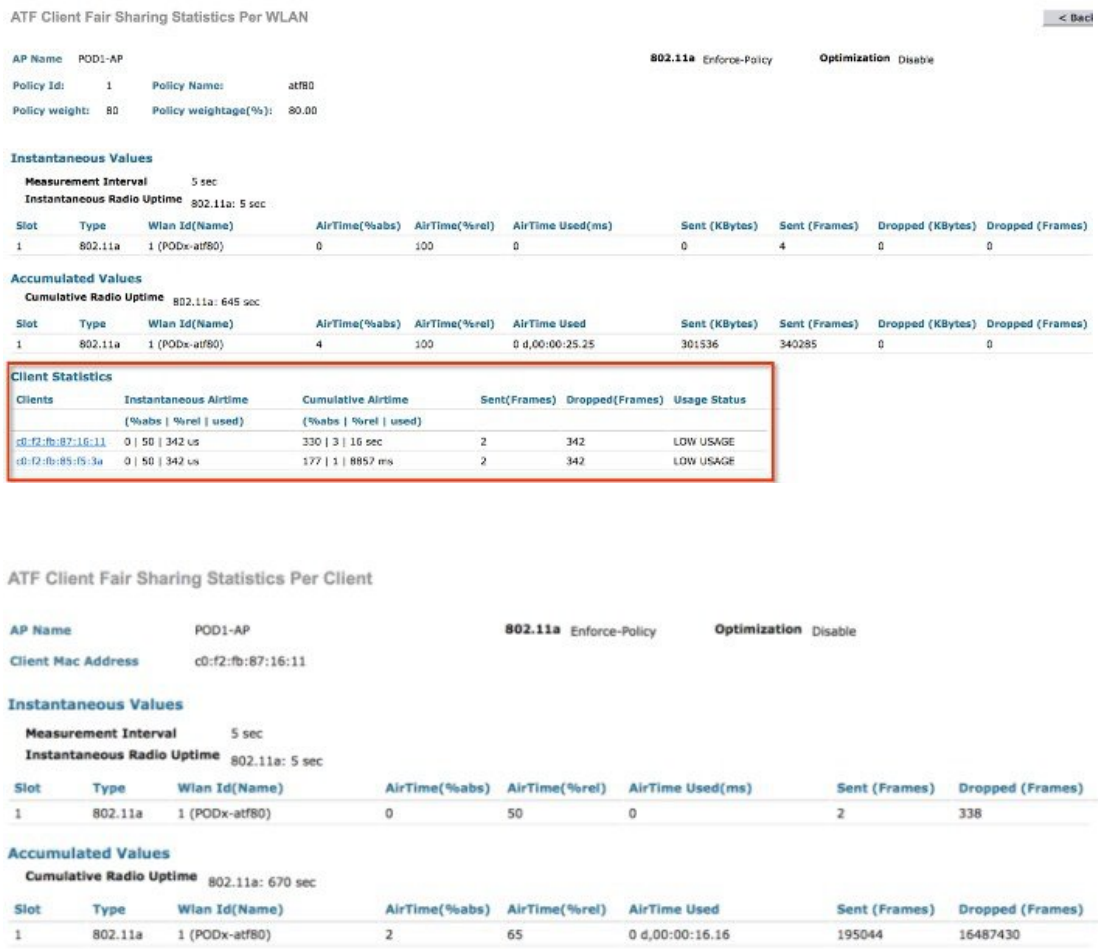
Step 1 Navigate **WIRELESS > ATF > ATF Statistics** and then select the **AP Name** from the drop down menu to which the clients are connected.

ATF Statistics page appears where user can view all the ATF enabled WLAN statistics.

Step 2 To have a granular view of ATF client fair sharing statistics click **WLAN id** which has client fair sharing enabled as shown.



Step 3 Clicking the client MAC address, users can view the WLAN ATF stats as well as client ATF statistics for all the clients associated with that particular WLAN.



ATF Client Fair Sharing Statistics Per WLAN

< Back

AP Name POD1-AP 802.11a Enforce-Policy Optimization Disable

Policy Id: 1 Policy Name: atf80

Policy weight: 80 Policy weightage(%): 80.00

Instantaneous Values

Measurement Interval 5 sec

Instantaneous Radio Uptime 802.11a: 5 sec

Slot	Type	Wlan Id(Name)	AirTime(%abs)	AirTime(%rel)	AirTime Used(ms)	Sent (KBytes)	Sent (Frames)	Dropped (KBytes)	Dropped (Frames)
1	802.11a	1 (PODx-atf80)	0	100	0	0	4	0	0

Accumulated Values

Cumulative Radio Uptime 802.11a: 645 sec

Slot	Type	Wlan Id(Name)	AirTime(%abs)	AirTime(%rel)	AirTime Used	Sent (KBytes)	Sent (Frames)	Dropped (KBytes)	Dropped (Frames)
1	802.11a	1 (PODx-atf80)	4	100	0 d,00:00:25.25	301536	340285	0	0

Client Statistics

Clients	Instantaneous Airtime (%abs | %rel | used)	Cumulative Airtime (%abs | %rel | used)	Sent(Frames)	Dropped(Frames)	Usage Status
c0:f2:fb:87:16:11	0 | 50 | 342 us	330 | 3 | 16 sec	2	342	LOW USAGE
c0:f2:fb:85:f5:3a	0 | 50 | 342 us	177 | 1 | 8857 ms	2	342	LOW USAGE

ATF Client Fair Sharing Statistics Per Client

AP Name POD1-AP 802.11a Enforce-Policy Optimization Disable

Client Mac Address c0:f2:fb:87:16:11

Instantaneous Values

Measurement Interval 5 sec

Instantaneous Radio Uptime 802.11a: 5 sec

Slot	Type	Wlan Id(Name)	AirTime(%abs)	AirTime(%rel)	AirTime Used(ms)	Sent (Frames)	Dropped (Frames)
1	802.11a	1 (PODx-atf80)	0	50	0	2	338

Accumulated Values

Cumulative Radio Uptime 802.11a: 670 sec

Slot	Type	Wlan Id(Name)	AirTime(%abs)	AirTime(%rel)	AirTime Used	Sent (Frames)	Dropped (Frames)
1	802.11a	1 (PODx-atf80)	2	65	0 d,00:00:16.16	195044	16487430

Air Time Fairness in Mesh Deployments Rel 8.4

This section of the document introduces the ATF on Mesh APs and provides guidelines for its deployment. The purpose of this section is to:

- Provide an overview of ATF on Mesh APs
- Highlight supported Key Features
- Provide details on deploying and managing the ATF on Mesh APs

Pre-requisite and Supported Features in 8.4 release

Mesh ATF is supported on AireOS 8.4 or higher release on a Wireless LAN Controller . Mesh ATF is supported on 1550-128Mb, 1570, 1700, 2600, 2700, 3500, 3600 and 3700

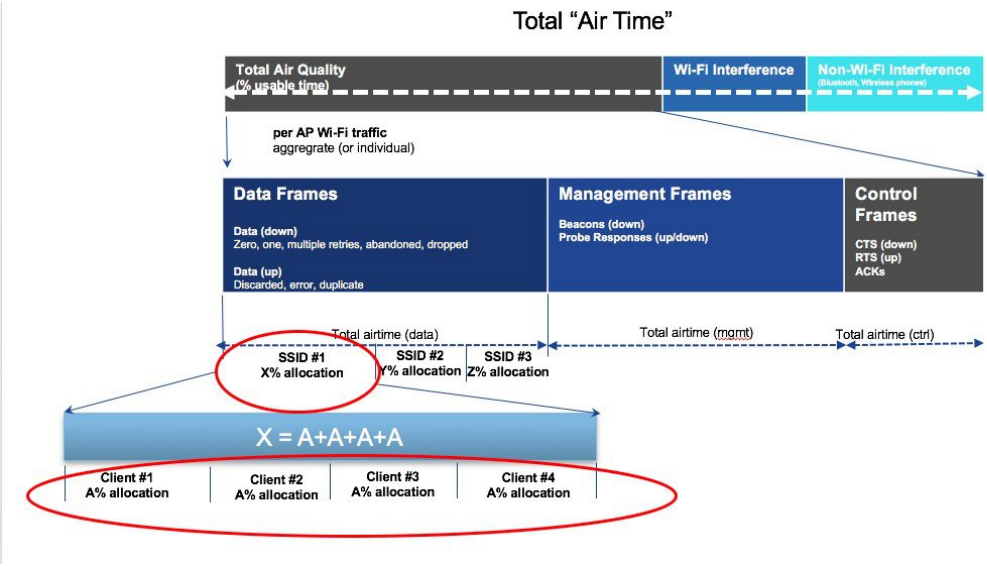
AP	1550 (64 MB)	1550 (128 MB)	1570	3700	1530	1560
Feature	–	–	—	–	–	–
Basic Mesh	Yes	Yes	Yes	Yes	Yes	8.4
Flex+Mesh	Yes	Yes	Yes	Yes	Yes	No
Fast Convergence (background scanning)	No	8.3	8.3	Yes	8.3	8.4
Wired Clients on RAP	Yes	Yes	Yes	No	Yes	No
Wired Clients on MAP	Yes	Yes	Yes	No	Yes	8.4
Daisy Chain	7.6	7.6	7.6	No	7.6	No
LSC	Yes	Yes	Yes	Yes	Yes	No
PSK provisioning: MAP-RAP authentication	8.2	8.2	8.2	8.2	8.2	8.4
ATF on Mesh	No	8.4	8.4	8.4	No	No

ATF Functionality and Capabilities

ATF Functionality and Capabilities:

- ATF policies are applied only in the downlink direction (AP transmitting frames to client). Only airtime in the downlink direction, that is AP to client, can be controlled accurately by the AP. Although airtime in the uplink direction, that is client to AP, can be measured, it cannot be strictly controlled. Although the AP can constrain airtime for packets that it sends to clients, the AP can only measure airtime for packets that it 'hears' from clients because it cannot strictly limit their airtime
- ATF policies are applied only on wireless data frames; management and control frames gets ignored
- When ATF is configured per-SSID, each SSID is granted airtime according to the configured policy
- ATF can be configured to either drop or defer frames that exceed their airtime policies. If the frame is deferred, it will be buffered and transmit at some point in the future when the offending SSID has a sufficient airtime budget. Of course, there is a limit as to how many frames can be buffered. If this limit is crossed, frames will be dropped regardless
- ATF can be globally enabled or disabled
- ATF can be enabled or disabled on an individual access point, AP group or entire network
- Allocation is applied Per SSID and Per Client
- Applies to Downstream only
- Can be configured in WLC GUI/CLI and PI

- Can be applied to all APs on a Network to AP Group or one AP
- Supported on APs in Local mode: **AP 1550-128Mb, 1570, 1700, 2600, 2700, 3500, 3600 and 3700**



ATF on Mesh Feature Overview

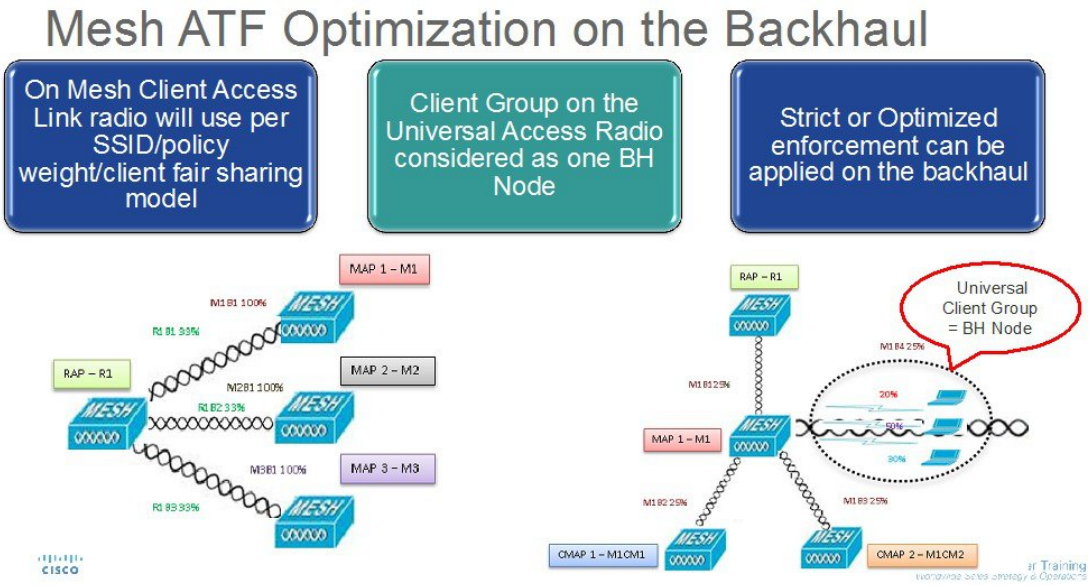
At the present time, enterprise class, high density stadium and other major Wi-Fi deployments with Cisco IOS 11n, 11ac Indoor APs are benefited by "per SSID" based Airtime Fairness and "per Client within a SSID" based Airtime Fairness through 8.1 MR1 and 8.2 releases.

In a same way, currently, there is a demand from the Customers with large scale Outdoor wireless mesh deployments to serve their users by providing fairness among the Wi-Fi users across the Outdoor wireless mesh network in utilizing the AP radio Airtime downstream and also provide administrators the key control to enforce SLA (implied on multiple cellular operator through Wi-Fi hotspot) on the Wi-Fi users across the Outdoor wireless mesh network. However, since all Wi-Fi users traffic is bridged between MAPs and RAPs through the wireless backhaul radio and there is no SSID concept on wireless backhaul radio for backhaul nodes to enforce policies through SSID's for each backhaul node, there is no easy solution for Wi-Fi users across the Outdoor wireless mesh network to get treated fairly in terms of utilizing the Wi-Fi airtime through their Outdoor Wireless Mesh Aps. As far as the clients on client access radios are concerned, it's fairly simple to regulate the airtime fairness through SSIDs (w/ or w/o client fair sharing) in a similar way how it is done for Cisco unified local mode APs.

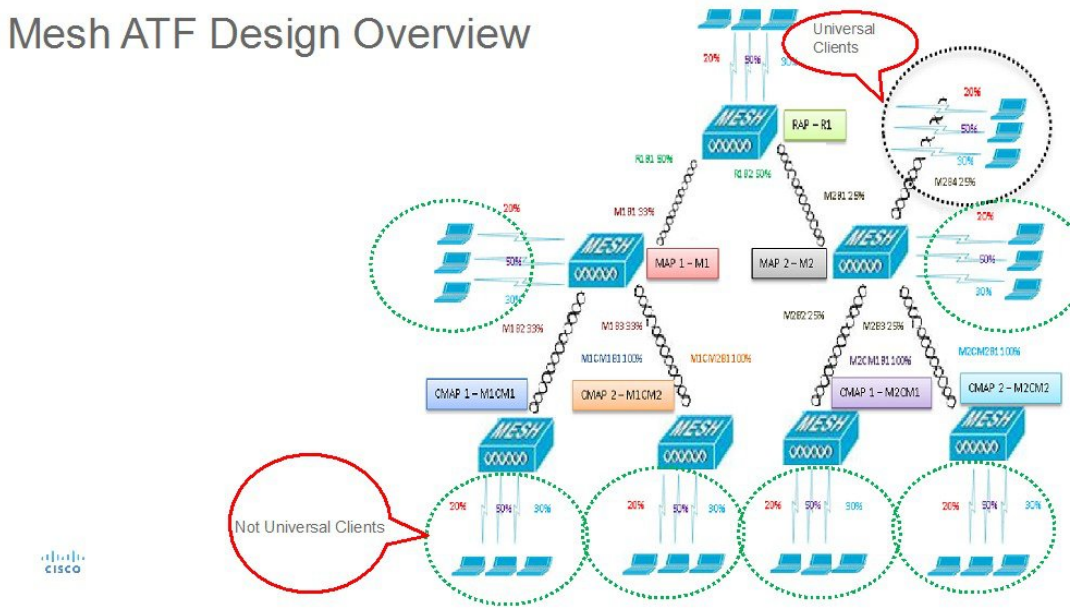
Before the solution overview of supporting ATF on mesh, lets quickly recap ATF - Airtime Fairness (ATF) is basically a concept which provides an ability to regulate/enforce the AP radio airtime in downstream direction for the clients associated through the SSID's. As a result, the Wi-Fi users on wireless network are fairly treated in terms of utilizing the radio WiFi radio airtime. This basically provides the key control either to enforce SLA additionally or simply to avoid certain group or individual from occupying an unfair amount of WiFi airtime on a particular or on a given AP radio. A service level agreement (SLA) is a contract between a service provider (either internal or external) and the end user that defines the level of service expected from the service provider. SLAs are output-based in that their purpose is specifically to define what the customer will receive.

In general, in the Mesh architecture, the Mesh Aps (Parents, child MAPs) in a Mesh Tree will be accessing the same channel (let's forget about extended sub-backhaul radios for a minute) on backhaul radio for mesh connectivity between Parents and child Maps. Whereas, the Root AP will be connected wired to the controller and MAPs will be connected wireless to the controller. Hence all the CAPWAP, Wi-Fi traffic will be bridged to the controller through the wireless backhaul radio and through RAP. In terms of the physical locations, normally the RAPs will be placed at roof top and the MAPs in multiple hops will be placed some distance apart

within each other based on the Mesh network segmentation guidelines. Hence each MAP in a Mesh tree can provide 100% of their own radio airtime downstream to their users though each MAP accessing the same medium. To compare this in non-mesh scenario, where there can be neighboring local mode unified Aps in the arena next to each other in different rooms serving to their respective clients on the same channel with each providing 100% radio airtime downstream. Therefore, ATF has no control over enforcing clients in two different neighboring AP's accessing the same medium. Similarly, it's applicable for MAPs in a Mesh tree. For Outdoor/Indoor Mesh Aps, Airtime fairness must be supported on client access radios which serve regular clients as same as how we currently support ATF on non-mesh unified local mode Aps to serve the clients and additionally it must also be supported on backhaul radios which bridge the traffic to/from the clients on client access radios to RAPs (one hop) or through MAPs to RAPs (multiple hops). Its bit tricky to support ATF on backhaul radio's using the same SSID/Policy/Weight/Client fair sharing model. Since backhaul radio's doesn't have SSIDs and it always bridges traffic through their hidden backhaul nodes. Henceforth, on the backhaul radios either in RAP or MAP, the radio airtime downstream will be fair shared equally based on the number of backhaul nodes. This approach eliminates the problem and provides fairness to users across wireless mesh network in the case where the clients associated to 2nd hop MAP can stall the clients associated to 1st hop MAP where 2nd hop MAP is connected wireless to 1st hop MAP through backhaul radio though the Wi-Fi users in the MAPs are separated by a physical location. In the scenario, when a backhaul radio has an option to serve normal clients through universal client access feature, ATF considers the regular clients into single node and group them into it. It enforces the Airtime by equally fair sharing the radio airtime downstream based on the number of nodes (backhaul nodes + single node for regular clients). We will see more details how this solution is turned into design in the next sections.



A bigger mesh design will looks like this:



ATF Modes of Operation

The Framework behind the ATF monitor mode is to allow the user to view and get the stats of overall Air Time being used i.e. to report the Air Time usage for all the AP transmissions. The ATF in monitor mode can be enabled on following levels.

- Disable Mode: By default ATF is disabled on the WLC
- Monitor Mode: To monitor airtime usage on your network
- Enforce—Policy Mode: Assigning ATF policies on your network
- Strict Enforcement
- Optimized

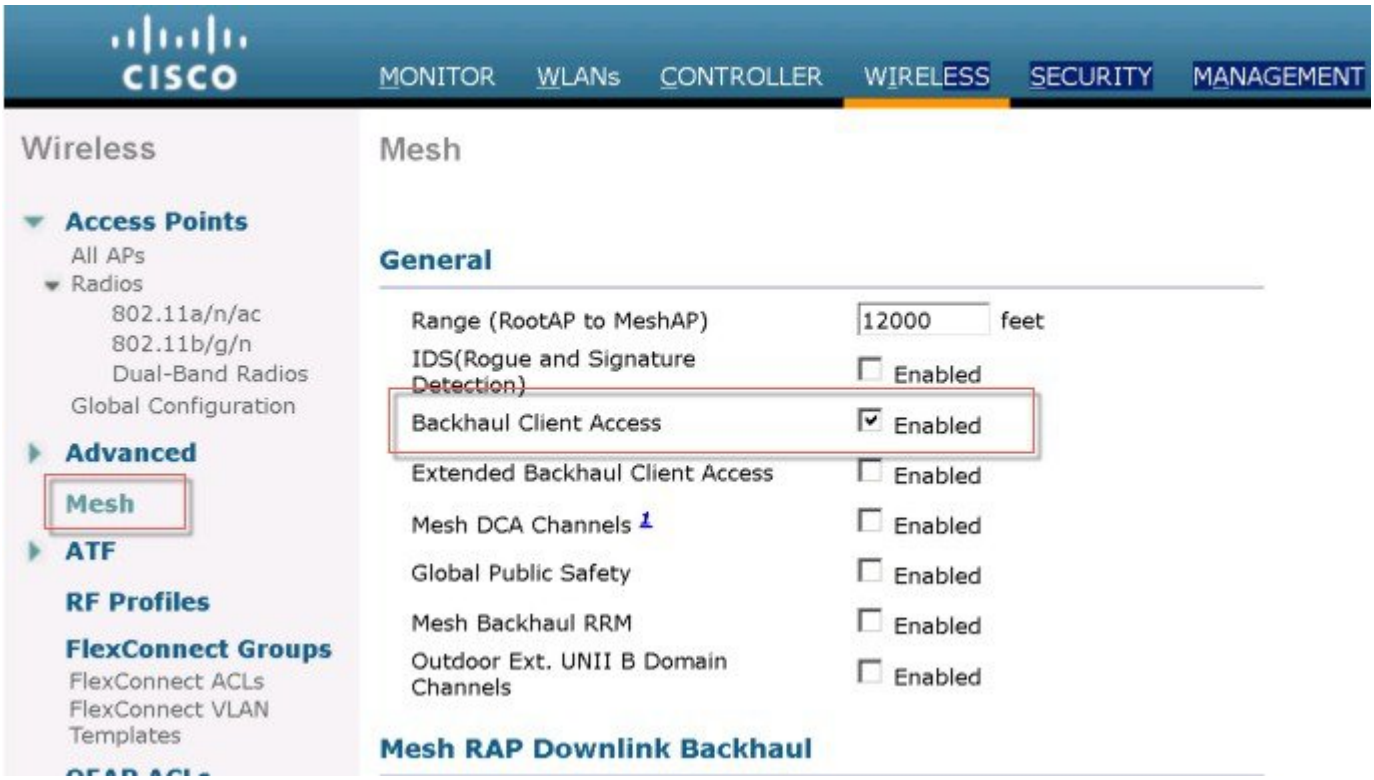
Configuring ATF on Mesh

To configure, ATF on mesh, perform the following steps:

Procedure

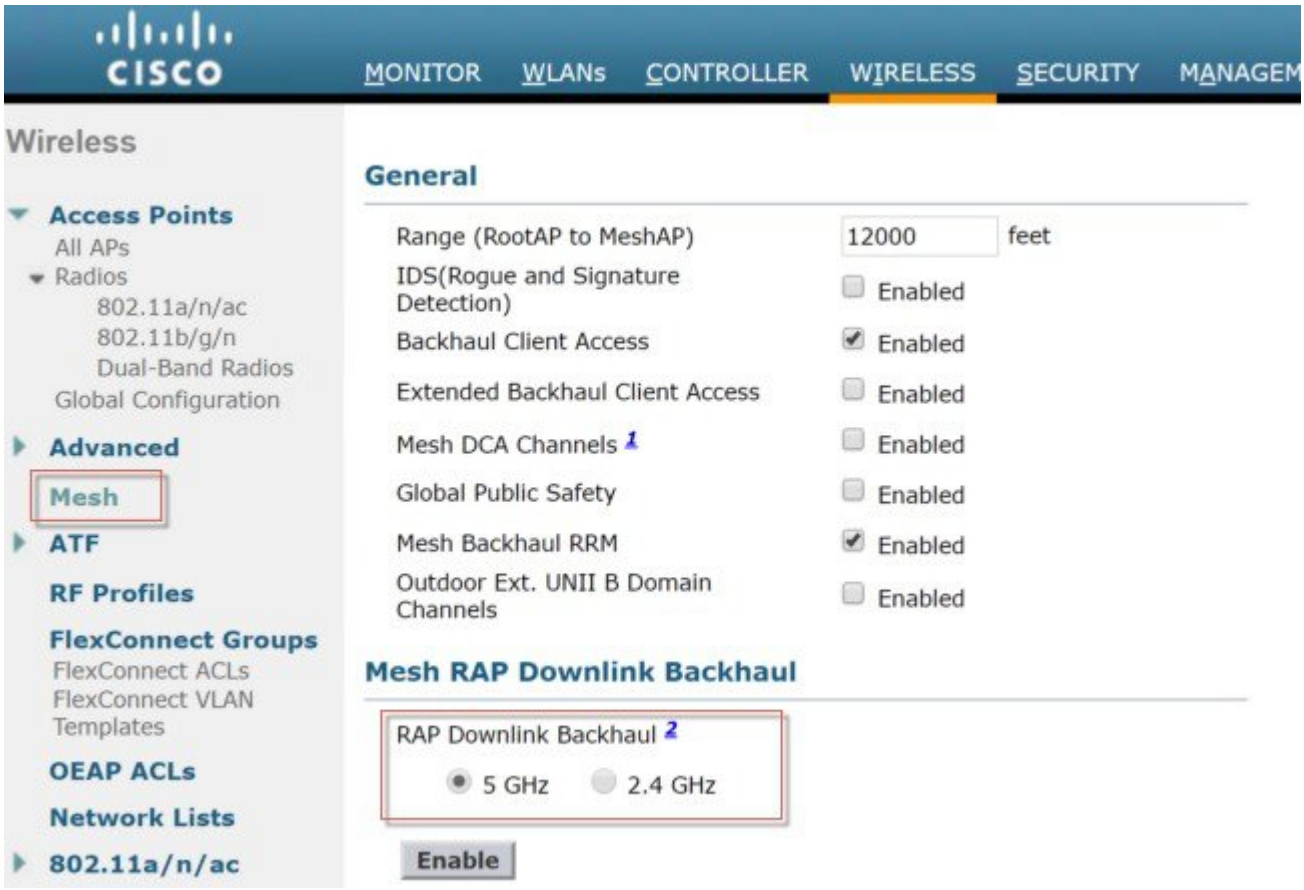
Step 1 Backhaul Client Access- enable/disable.

```
(5520-MA1) >config mesh client-access enable
```



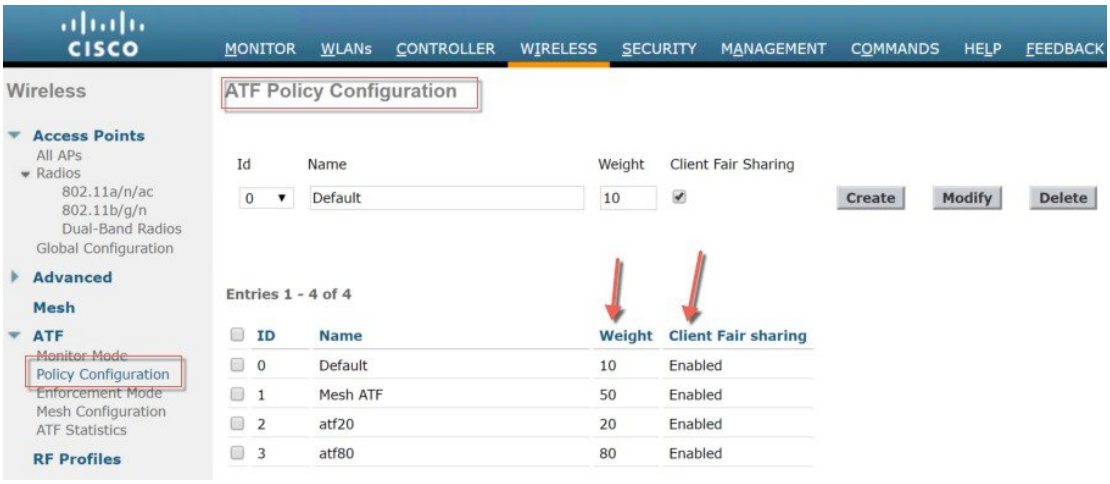
Step 2 RAP Downlink Backhaul configure 5 or 2.4 GHz

```
(5520-MA1) >config mesh backhaul slot <0/1> all
```



Step 3 Create ATF Policy with Weight and Client Sharing

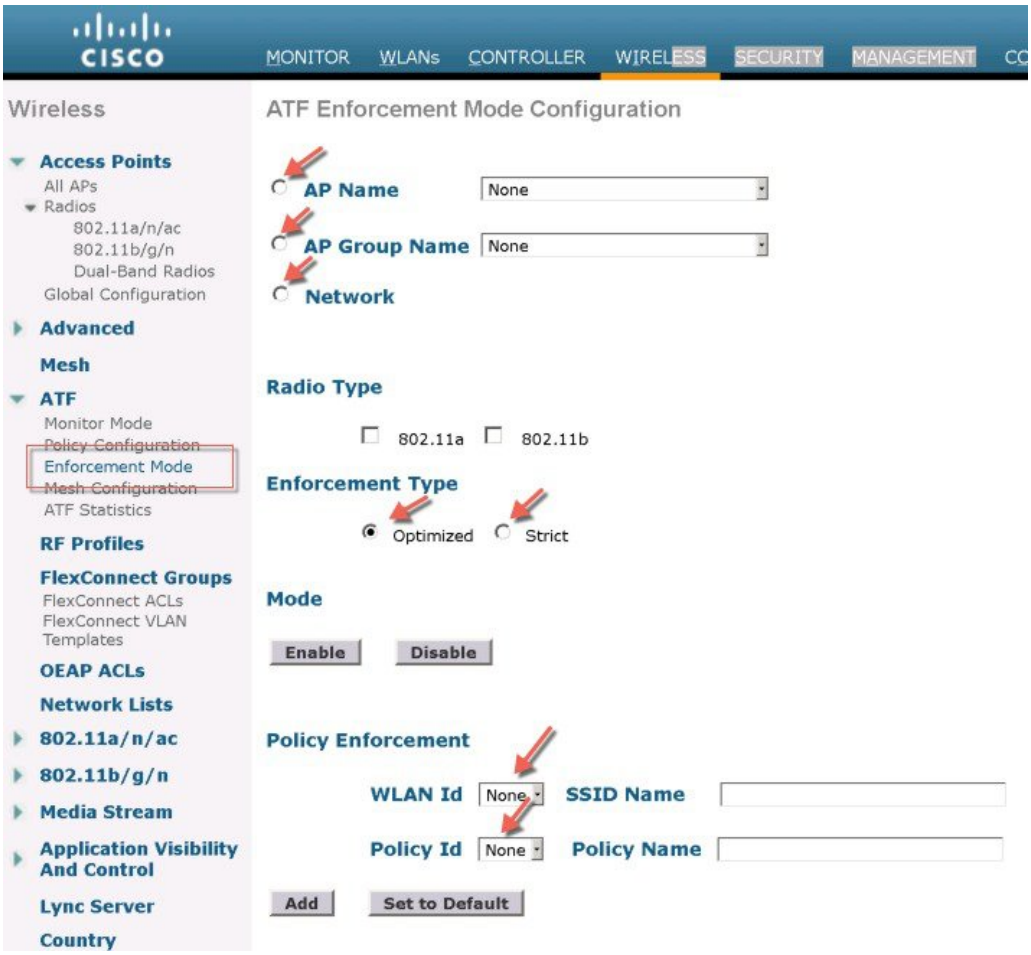
```
(5520-MA1) >config atf 802.11a mode ?

disable         Disables ATF
enforce-policy Configures ATF in enforcement mode
monitor         Configures ATF in monitor mode

(5520-MA1) >config atf 802.11a mode enforce-policy


(5520-MA1) >config atf policy create 1 mesh 25 client-sharing enable
```



Step 4 Configure Enforcement mode per AP/AP Group/Network with Enforcement type and WLAN and Policy applied.

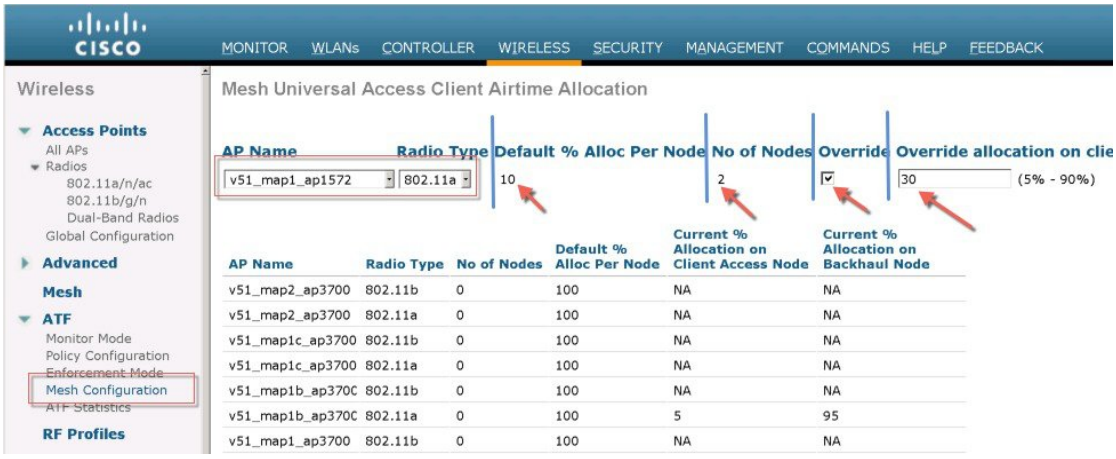
Figure 1:

```
(5520-MA1) >config atf 802.11a optimization enable
```



Step 5 Configure Mesh Universal Access Client Airtime Allocation.

```
> config ap atf 802.11a client-access airtime-allocation <5 - 90> <ap-name> override enable
/disable
> config ap atf 802.11b client-access airtime-allocation <5 - 90> <ap-name> override enable/disable
```



ATF Client Statistics from WLC CLI

From CLI user can also run the following command to see the atf statistics per client on the WLC

```
(WLC)> show atf statistics client <MAC addr>
```

```
(POD1-WLC) >show atf statistics client c0:f2:fb:85:f5:3a

Client MAC Address.............................. c0:f2:fb:85:f5:3a
Client Username ................................ N/A
AP MAC Address.................................. 74:a0:2f:30:1c:40
AP Name......................................... POD1-AP
AP radio slot Id................................ 1
Wireless LAN Id................................. 1
ATF Policy ID................................... 1
Wireless LAN Profile Name....................... PODx-atf80
  Radio Uptime [ Instantaneous | Total ]......... 5 sec | 2460 sec
  Total Radio Air Time........................... 26sec
  Airtime Used .................................. 342us              | 211ms
  Relative Airtime % ............................ 50               | 1
  Absolute Airtime % ............................ 0                | 0

  Frames Sent ................................... 2                |  897
  Frames Dropped ................................ 342              |  211830
```

Client Statistics on AP

If required user can login to AP CLI to see that Clients stats as well by running the following command

```
AP# show controller dot11Radio <0/1> atf
AP # show controller d0/d1 atf cfs client
```

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands