



8.0 AP Features

Indoor APs, Flex, Outdoor

Jerome Henry
Technical Marketing Engineer
Enterprise Networking Market Strategy

August 2014

Agenda

- CleanAir Express for AP 1600
- OEAP GUI Enhancements
- OEAP Link Test
- OEAP Voice QoS Enhancements
- OEAP Firewall
- OEAP Split Tunneling
- 702W VLAN Support
- FlexConnect Features
 - FlexConnect VideoStream
 - FlexConnect Faster Time to Deploy
 - FlexConnect Proxy ARP
- Mesh Enhancements
 - Flex on Mesh
 - Mesh Fast Convergence

Agenda

- FlexConnect VideoStream
- FlexConnect Faster Time to Deploy
- FlexConnect Proxy ARP

Agenda

- Flex on Mesh
- Mesh Fast Convergence

Support for a new -F Domain (Indonesia) on 702i and 3700

Support for a new -F Domain (Indonesia) on 702i and 3700

- Indonesia increased their allowed transmit power in 2.4 GHz to 20 dBm (from 17 dBm), dropping from the CN domain, and getting the F domain
- Code 7.6 reflected that new domain, but AP702i and AP3700 code did not recognize this new domain
- Issue is fixed on 8.0. -F domain is recognized also for 702i and 3700 APs

CleanAir Express for AP 1600

CleanAir Express for AP 1600

- CleanAir Express (*aka*, SI Lite) is a fully functional version of CleanAir, but with limitations compared to CleanAir running on higher grade APs:
 - Interferer detection: AP 1600 recognizes all of the interferers that the other models can recognize. However, AP 1600 can track only 3 devices per radio.
 - System-level features: AP 1600 supports several of the same features as higher-end APs (location, severity list, alert correlation, Air Quality Index, Zone of Impact) and supports the same modes (local, monitor, spectrum analyzer)

CleanAir Express for AP 1600 – Channel Width Impact

- AP 1600 radio channel is 20-MHz wide:
 - When scanning in monitor mode, other APs scan by chunks of 40-MHz. The AP 1600 scans 20-MHz, and therefore needs a higher proportion of the scan cycle to look for interferers.
 - This may lightly impact system throughput in high density environments, especially as SI scan is sent to AP memory (instead of radio memory)

OEAP GUI Enhancements

OEAP GUI Enhancements

The screenshot shows the OEAP GUI interface. The top navigation bar includes 'HOME', 'CONFIGURATION', and 'EVENT_LOG'. The main content area is titled 'Home: Summary' and contains three sections: 'General Information', 'AP Statistics', and 'Association'. In the 'General Information' table, the 'AP Software Version' row is highlighted with a red box, showing the value '7.6.110.18'.

General Information	
Ap Name	APECC8.82B8.81B8
AP IP Address	172.31.255.117
AP Mode	Local
AP MAC Address	EC:C8:82:B8:81:B8
AP Uptime	47 seconds
AP Software Version	7.6.110.18

AP Statistics		
Radio	Admin Status	Freq/Cl
Radio-802.11G	up	2.4 GHz
Radio-802.11A	up	5 GHz/

Association	
Client MAC	Association Time
24:77:03:75:79:70	00:00:31

The screenshot shows the OEAP GUI interface with a new 'AP Info' sidebar on the left. The sidebar contains 'AP Info', 'SSID', and 'Client' sections, with 'AP Info' highlighted by a red box. The main content area is titled 'Home: Summary' and contains 'General Information' and 'AP Statistics' sections. In the 'General Information' table, the 'AP Software Version' row is highlighted with a red box, showing the value '8.0.72.211'.

General Information	
AP Name	APECC8.82B8.81B8
AP IP Address	172.31.255.122
AP Mode	Local
AP MAC Address	EC:C8:82:B8:81:B8
AP Uptime	24 minutes, 22 seconds
AP Software Version	8.0.72.211
CAPWAP Status	Connected
WAN Gateway Status	Reachable

AP Statistics	
---------------	--

OEAP GUI Enhancements



AP Info

SSID

Client

Local SSID

SSID Name	Security Policy	Radio Type
AIR-602	[WPA2][AES][PSK]	2.4 Ghz
AIR-602	None	5.0 Ghz



AP Info

SSID

Client

Association

Local Clients

Client MAC	WLAN SSID	Association Time	Bytes In/Out	Duplicate/Retries	Decrypt Failed
24:77:03:75:79:70	AIR-602	00:28:15	268288/2236416	0/1	0

Corporate Clients

Client MAC	WLAN SSID	Association Time	Bytes In/Out	Duplicate/Retries	Decrypt Failed
------------	-----------	------------------	--------------	-------------------	----------------

©2010 - 2014 Cisco Systems Inc. All rights reserved.

OEAP Link Test

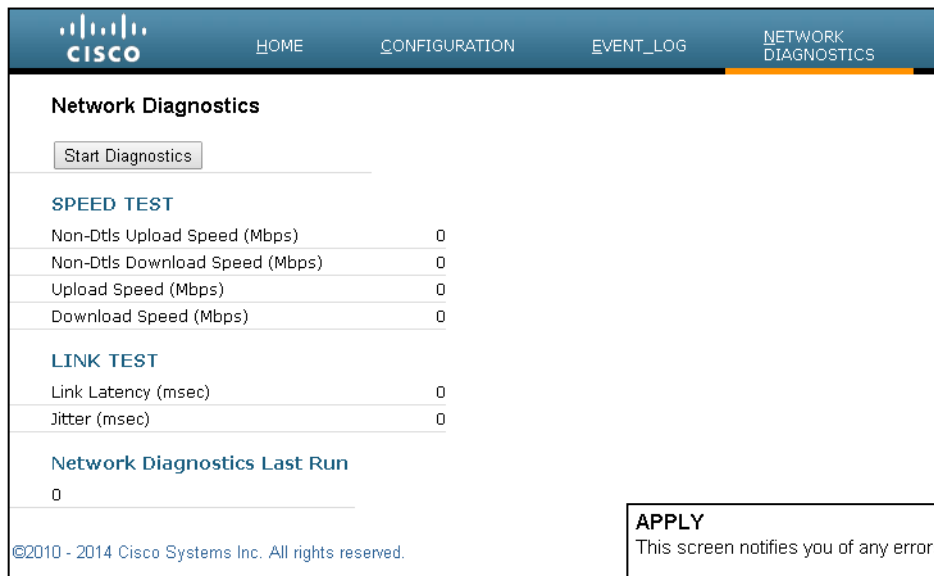
OEAP Link Test

- Allows the end user to determine the non-DTLS throughput of the system by running a speed test on demand, and to determine the link latency and jitter by running a test on demand or periodically.
- The tests may be initiated from the AP GUI, controller GUI, or controller CLI. The results of the speed and link tests will be displayed to the user on the AP GUI, controller GUI, or controller CLI.
- Speed: 1Mb file (speedTest_upload file) is present on the AP, in memory. This file will be uploaded to the controller when the user initiates the test. The file transfer start time and finish time will be noted down, and the file size divided by the elapsed time provides the upload speeds. The speedTest_upload file is downloaded back to the AP from the controller.
- RTT: CAPWAP keepalives are used (1 keepalive per 30 seconds, saved [by 3] every 90 seconds; RTT shows last 5 measurements)
- Jitter is the average difference between the 5 RTTs

OEAP Link Test

- Speed: 1Mb file (speedTest_upload file) is present on the AP, in memory. This file will be uploaded to the controller when the user initiates the test. The file transfer start time and finish time will be noted down, and the file size divided by the elapsed time will give us the upload speeds. The speedTest_upload file is downloaded back to the AP from the controller.
- RTT: CAPWAP keepalives are used (1 keepalive per 30 second, saved [by 3] every 90 seconds, RTT shows last 5 measurements)
- Jitter is the average difference between the 5 RTTs

OEAP Link Test



Network Diagnostics

Start Diagnostics

SPEED TEST

Non-Dtls Upload Speed (Mbps)	0
Non-Dtls Download Speed (Mbps)	0
Upload Speed (Mbps)	0
Download Speed (Mbps)	0

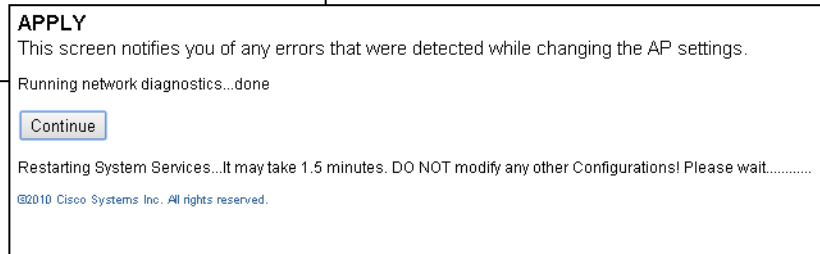
LINK TEST

Link Latency (msec)	0
Jitter (msec)	0

Network Diagnostics Last Run

0

©2010 - 2014 Cisco Systems Inc. All rights reserved.



APPLY

This screen notifies you of any errors that were detected while changing the AP settings.

Running network diagnostics...done

Continue

Restarting System Services...It may take 1.5 minutes. DO NOT modify any other Configurations! Please wait.....

©2010 Cisco Systems Inc. All rights reserved.

OEAP Link Test

The image displays two screenshots of the Cisco Wireless LAN Controller (WLC) Network Diagnostics interface for AP APECC8.82B8.81B8. The left screenshot shows the 'Start Network Diagnostics' button and a table of metrics with zero values. The right screenshot shows the same interface after the test is completed, with the 'Start Network Diagnostics' button disabled and the table populated with performance data. A 'Message from webpage' dialog box is overlaid on the left screenshot, asking for confirmation to proceed with the test.

Left Screenshot (Before Test):

Metric	Value
Dtls Upload Speed (Mbps)	0.00
Dtls Download Speed (Mbps)	0.00
Non-Dtls Upload Speed (Mbps)	0.00
Non-Dtls Download Speed (Mbps)	0.00
Latency (mSec)	0
Jitter (mSec)	0
Network Diagnostics Last Run	

Right Screenshot (After Test):

Metric	Value
Dtls Upload Speed (Mbps)	10.98
Dtls Download Speed (Mbps)	10.27
Non-Dtls Upload Speed (Mbps)	22.70
Non-Dtls Download Speed (Mbps)	26.06
Latency (mSec)	1
Jitter (mSec)	0
Network Diagnostics Last Run	Tue Jun 17 12:03:51 2014

Message from webpage:

Controller will send out a request to the AP to get latency and jitter values. Are you sure you want to continue?

Buttons: OK, Cancel

OEAP Link Test

```
(Cisco Controller) >show ap network-diagnostics ?  
<Cisco AP>      Enter the name of the Cisco AP.
```

```
(Cisco Controller) >show ap network-diagnostics APECC8.82B8.81B8  
AP network diagnostics has been initiated  
Waiting for network diagnostics to complete
```

← Wait a few seconds (2 or 3)

```
===== AP Network Diagnostics =====
```

Speed Test Results:

DTLS Upload Speed	10.98 Mbps
DTLS Download Speed	9.93 Mbps
Non-DTLS Upload Speed	22.69 Mbps
Non-DTLS Download Speed	25.46 Mbps

Link Test Results:

Latency	2 mSec
Jitter	0 mSec

OEAP Voice QoS Enhancements

OEAP Voice QoS Enhancements

- Designed for remote offices, OEAP did not have a voice prioritization feature. However, more and more customers use VoIP over their OEAP.
- In 8.0, OEAP is enhanced to offer high priority for the voice packets compared to other traffic streams:
 - Downstream: SSID is checked to verify if WME is enabled. If WME is enabled, frame UP is checked and applied. If no UP present, L3 TOS is used to derive the priority queue. If no L3 ToS, we use DCF.
 - Upstream: Received frames have their UP checked and capped to WLAN maximum. The value is placed as TOS in L3 CAPWAP header.
 - In both directions, behavior is similar to other APs' QoS tagging principles.

OEAP Voice QoS Enhancements

- No configuration needed. You can check the queues from the WLC, with Monitor > AP > radio

```
(Cisco Controller) >show ap stats 802.11b APECC8.82B8.81B8
.../...
OEAP WMM Stats :
  Best Effort:
    Tx Frame Count..... 0
    Tx Failed Frame Count..... 0
    Tx Expired Count..... 0
    Tx Overflow Count..... 0
    Tx Queue Count..... 0
    Tx Queue Max Count..... 0
```

The screenshot shows the Cisco WLC Monitor interface. The left sidebar contains a navigation tree with 'Monitor' selected. The main content area is divided into two sections: '802.11 MAC Counters' and 'OEAP Queues Stats'. The '802.11 MAC Counters' section displays a table of statistics for the selected radio (802.11a/n/ac and 802.11b/g/n Dual-Band Radios). The 'OEAP Queues Stats' section displays a table of statistics for Voice, Video, Background, and Besteffort queues.

802.11 MAC Counters			
Tx Fragment Count	0	Multicast Tx Frame Count	0
Tx Failed Count	0	Retry Count	0
Multiple Retry Count	0	Frame Duplicate Count	0
RTS Success Count	0	RTS Failure Count	0
ACK Failure Count	0	Rx Fragment Count	0
Multicast Rx Frame Count	0	FCS Error Count	0
Tx Frame Count	0	WEP Undecryptable Count	0

OEAP Queues Stats			
Voice			
Tx Frame Count	0	Tx Failed Frame Count	0
Tx Expired Frame Count	0	Tx Overflow Frame Count	0
Rx Frame Count	0	Rx Failed Frame Count	0
Queue Max Count	0	Queue Current Count	0
Video			
Tx Frame Count	0	Tx Failed Frame Count	0
Tx Expired Frame Count	0	Tx Overflow Frame Count	0
Rx Frame Count	0	Rx Failed Frame Count	0
Queue Max Count	0	Queue Current Count	0
Background			
Tx Frame Count	0	Tx Failed Frame Count	0
Tx Expired Frame Count	0	Tx Overflow Frame Count	0
Rx Frame Count	0	Rx Failed Frame Count	0
Queue Max Count	0	Queue Current Count	0
Besteffort			
Tx Frame Count	0	Tx Failed Frame Count	0
Tx Expired Frame Count	0	Tx Overflow Frame Count	0
Rx Frame Count	0	Rx Failed Frame Count	0
Queue Max Count	0	Queue Current Count	0

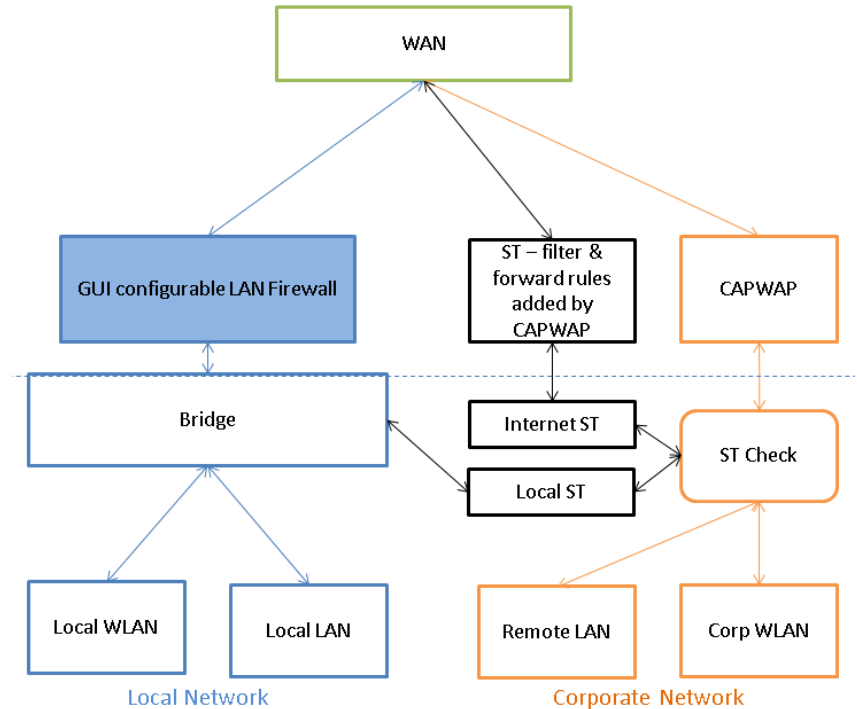
OEAP Firewall

OEAP Firewall

- In 8.0, the OEAP basic firewall feature provides basic firewall protection capability on the OEAP platform that can be enabled or disabled by the end user using the user accessible GUI interface.
- The scope of this feature is limited to the following specific firewall settings:
 1. All ports blocked by default (TCP and UDP)
 2. Some selective unblocking based on application type (i.e., HTTP, HTTPS, SSH, FTP)
 3. More fine-grained but controlled unblocking based on protocol/port
 4. Port forwarding (less than 10 total entries for separate port numbers)
 5. DMZ

OEAP Firewall

- The firewall is applied to the WAN port, but not to CAPWAP traffic coming from the WLC. It is assumed that firewall protection for the CAPWAP traffic will be handled by the controller and no special processing is needed for that traffic.



OEAP Firewall Notes

- OEAP Firewall ‘inside’ interface is LAN ports/local WLANs, and ‘outside’ interface is WAN port. If the firewall is enabled, by default all traffic from local to internet is denied (Application DNS, HTTP and HTTPS are enabled in configuration and will be allowed, to give user default browsing – This can be removed by unchecking in Application access). All rules are ‘allow’ rules in firewall configuration, and no implicit rules are applied.
- Application access provides an easy way of access granting. LAN Application access is for internet access from Local clients (Local LAN and Local WLAN). These rules are not applied on any of split tunnel traffic. LAN IP based access with Port range provide more fine-grain control

OEAP Firewall

- The precedence of the firewall rules are as follows:
 1. Enabled/Disabled
 2. Port forwarding
 3. DMZ
 4. LAN application access
 5. LAN Access Client - Fine grained LAN IP based access with port range

OEAP Firewall Configuration

The screenshot displays the OEAP (One-Click Easy Setup) interface for configuring a firewall. The top navigation bar includes the Cisco logo and links for HOME, CONFIGURATION (highlighted), EVENT_LOG, NETWORK DIAGNOSTICS, and HELP. There are also 'Refresh' and 'Close Window' buttons. The left sidebar lists various configuration categories: System, SSID, DHCP, WAN, Firewall (selected), and Download/Upload. Under the Firewall section, there are links for Filtering, Forwarding, and DMZ. The main content area is titled 'Configuration' and shows 'Firewall Mode' set to 'Firewall Enabled' with a 'Disabled' dropdown menu. An 'Apply' button is visible in the top right of the configuration area. A modal dialog box titled 'APPLY' is open, displaying the following text: 'This screen notifies you of any errors that were detected while changing the AP settings. Validating values...done. Committing values...done.' Below this text is a 'Continue' button. At the bottom of the dialog, it says 'Restarting System Services...It may take 1.5 minutes. DO NOT modify any other Configurations! Please wait.....' and includes a copyright notice: '©2010 Cisco Systems Inc. All rights reserved.'

OEAP Firewall Configuration

System

SSID

DHCP

WAN

Firewall

Filtering

Forwarding

DMZ

Download/Upload

Configuration

Filters

LAN Application Access

Protocol Allow

FTP

TELNET

SMTP

DNS

TFTP

HTTP

POP3

NNTP

SNMP

HTTPS

LAN Access Client

LAN IP Address Range	Protocol	Destination Port Range	Allow
<input type="text"/> - <input type="text"/>	TCP	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>
<input type="text"/> - <input type="text"/>	TCP	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>
<input type="text"/> - <input type="text"/>	TCP	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>
<input type="text"/> - <input type="text"/>	TCP	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>
<input type="text"/> - <input type="text"/>	TCP	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>
<input type="text"/> - <input type="text"/>	TCP	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>
<input type="text"/> - <input type="text"/>	TCP	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>
<input type="text"/> - <input type="text"/>	TCP	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>
<input type="text"/> - <input type="text"/>	TCP	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>
<input type="text"/> - <input type="text"/>	TCP	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>

©2010 - 2014 Cisco Systems Inc. All rights reserved.

OEAP Firewall Configuration

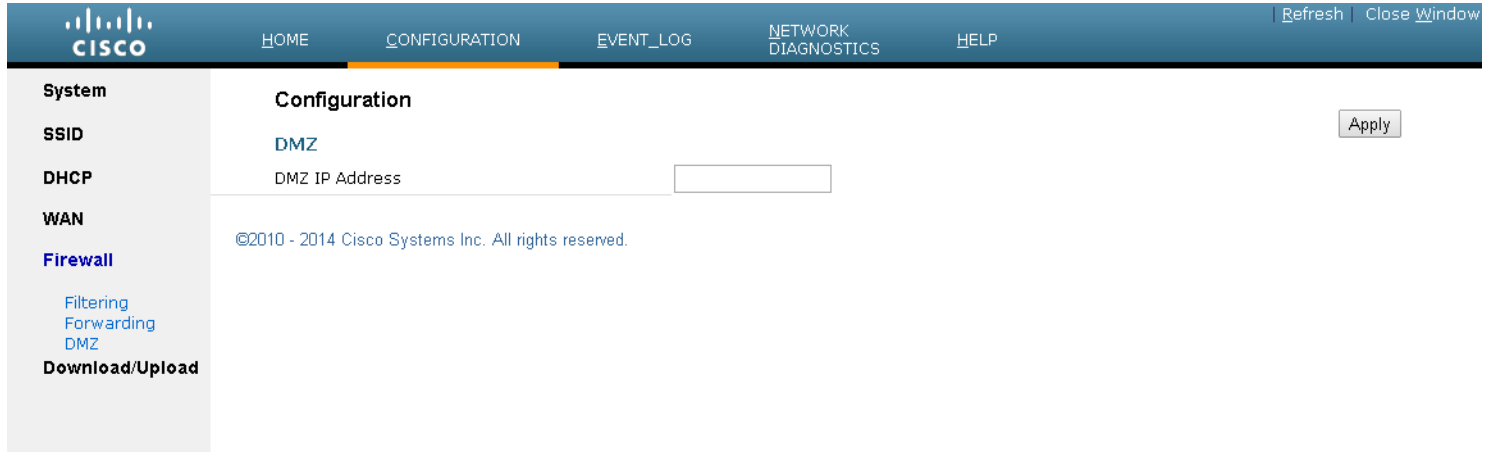
The screenshot shows the OEAP configuration interface. The top navigation bar includes 'HOME', 'CONFIGURATION', 'EVENT_LOG', 'NETWORK DIAGNOSTICS', and 'HELP'. The left sidebar lists 'System', 'SSID', 'DHCP', 'WAN', 'Firewall', and 'Download/Upload'. The 'Firewall' section is expanded to show 'Filtering', 'Forwarding', and 'DMZ'. The main content area is titled 'Configuration' and 'Forward', with a sub-section 'Port Forwards'. An 'Apply' button is visible in the top right. Below the title is a table for configuring port forwards.

Protocol	WAN Port Start	WAN Port End	LAN IP Address	LAN Port Start	LAN Port End	Enabled
TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

©2010 - 2014 Cisco Systems Inc. All rights reserved.

- Port forward allows you to forward to LAN machines' specific WAN ports, without firewall filtering

OEAP Firewall Configuration



The screenshot displays the Cisco OEAP configuration interface. At the top, there is a navigation bar with the Cisco logo and menu items: HOME, CONFIGURATION (highlighted), EVENT_LOG, NETWORK DIAGNOSTICS, and HELP. On the right of the navigation bar are links for Refresh and Close Window. A left-hand sidebar contains a tree view of configuration categories: System, SSID, DHCP, WAN, Firewall (selected), Filtering, Forwarding, DMZ, and Download/Upload. The main content area is titled 'Configuration' and shows the 'DMZ' section. It includes a label 'DMZ IP Address' followed by an empty text input field. An 'Apply' button is located in the top right corner of the configuration area. At the bottom of the main content area, the copyright notice reads: '©2010 - 2014 Cisco Systems Inc. All rights reserved.'

- Traffic to the DMZ address will be forwarded untouched through the firewall

OEAP Split Tunneling

OEAP Split Tunneling

- The split tunneling capability for internet traffic supports routing of internet traffic from corporate clients (associated to corporate SSID or dedicated Ethernet ports) through the local WAN port.
- This allows the OEAP clients on the corporate WLAN to reach the internet directly through the WAN instead of going via the corporate network (i.e., through CAPWAP tunnel). Only the traffic destined to corporate subnets (as configured on controller) go through the CAPWAP tunnel.

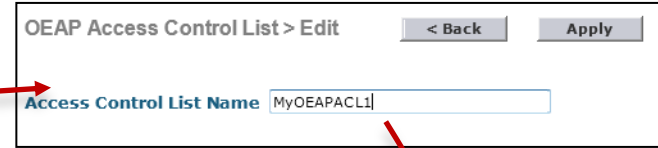
OEAP Split Tunneling

- For enabling/disabling the split tunneling feature, for the WAN or RLAN you have three options:
 - No split tunnel (default value). No split tunnel support enabled, all traffic goes through the controller.
 - Partial split tunnel. Ability to access local resources but internet traffic still goes through controller. This is the existing functionality implemented in Phase-1.
 - Full split tunnel. All traffic except intra-WAN traffic and traffic directed towards some user-configured networks is split tunneled.

OEAP Split Tunneling Configuration



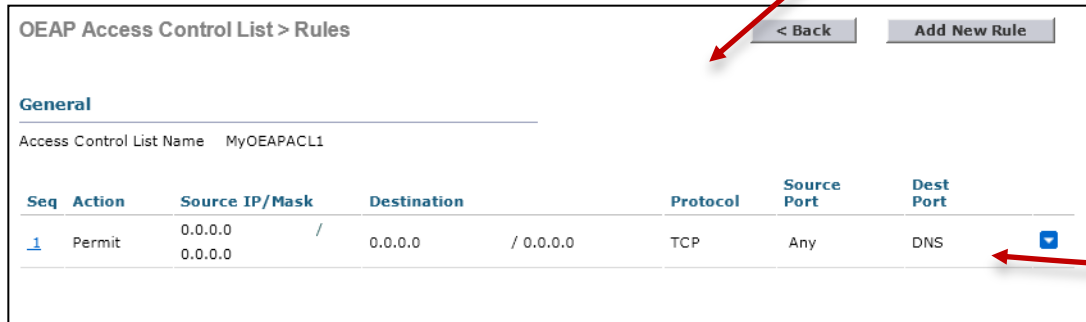
The screenshot shows the Cisco Wireless Management Console interface. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', and 'COMM'. The 'WIRELESS' tab is selected. On the left, a sidebar lists 'Wireless' categories: 'Access Points', 'Advanced', 'Mesh', 'RF Profiles', 'FlexConnect Groups', and 'OEAP ACLs'. The main content area is titled 'OEAP Access Control Lists' and shows 'Entries 0 - 0 of 0'. A 'New...' button is visible in the top right of this section.



This screenshot shows the 'OEAP Access Control List > Edit' configuration page. It features a '< Back' button and an 'Apply' button. The 'Access Control List Name' field is populated with 'MyOEAPACL1'.



This screenshot shows the 'OEAP Access Control Lists' list view. It displays 'Entries 1 - 1 of 1'. The 'Acl Name' field is populated with 'MyOEAPACL1' and has a dropdown arrow on the right.



This screenshot shows the 'OEAP Access Control List > Rules' configuration page. It includes a '< Back' button and an 'Add New Rule' button. The 'Access Control List Name' is 'MyOEAPACL1'. Below is a table with one rule entry:

Seq	Action	Source IP/Mask	Destination	Protocol	Source Port	Dest Port
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	TCP	Any	DNS

Here by default

OEAP Split Tunneling Configuration

OEAP Access Control List > Rules > New

Sequence	<input type="text" value="1"/>		
Source	IP Address <input type="text" value="Any"/> <input type="text" value="IP Address"/>	IP Address <input type="text" value="172.31.255.0"/>	Netmask <input type="text" value="255.255.255.0"/>
Destination	IP Address <input type="text"/>	IP Address <input type="text" value="10.10.10.0"/>	Netmask <input type="text" value="255.255.255.0"/>
Protocol	<input type="text" value="Any"/>		
Action	<input type="text" value="Permit"/>		

- Source can be “any” or a specific subnet. That subnet is in the home LANs, but can also be the subnet of the corporate WLAN clients.

OEAP Split Tunneling Configuration

OEAP Access Control List > Rules > New

Sequence	<input type="text" value="1"/>		
Source	<input type="text" value="IP Address"/> ▼	IP Address <input type="text" value="172.31.255.0"/>	Netmask <input type="text" value="255.255.255.0"/>
Destination	<input type="text" value="IP Address"/> ▼	IP Address <input type="text" value="0.10.10.0"/>	Netmask <input type="text" value="255.255.255.0"/>
Protocol	<input type="text" value="Any"/> ▼		
Action	<input type="text" value="Permit"/> ▼		

Any
IP Address
Local
Network List

- Destination can be “any”, a specific subnet, the local network (OEAP non-corporate, home subnet), or a list of subnets (“network list”)

OEAP Split Tunneling Configuration – Network List

The screenshot displays the Cisco Wireless configuration interface. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', 'FEEDBACK', and 'Home'. The left sidebar shows the 'Wireless' menu with options like 'Access Points', 'Advanced', 'Mesh', 'RF Profiles', 'FlexConnect Groups', 'OEAP ACLs', and 'Network Lists'. The main content area is titled 'Split Tunnel Network Lists' and features a 'New...' button and an 'Apply' button. A red arrow points from the 'New...' button to a 'New' configuration form. This form includes a 'List Index' dropdown set to 'Index0', a 'List Name' text box containing 'lab1', a 'Gateway IP' text box containing '192.168.1.10', and a 'Subnet Mask' text box containing '255.255.255.0'. The form also has '< Back' and 'Apply' buttons.

- Network List has its own menu in Wireless, and configures a list of subnets with the matching gateway (and gateway mask)

OEAP Split Tunneling Configuration – Network List

- The “gateway” is the expected gateway for the return traffic (the gateway of the remote, target network)
 - It does not need to be accurate (if you do not know the return traffic gateway, any IP in the destination subnet is ok)
 - The AP simply applies the mask to the gateway to deduce the network address and the subnet

Split Tunnel Network Lists > New

< Back Apply

List Index Index0 ▾

List Name lab1

Gateway IP 192.168.1.10

Subnet Mask 255.255.255.0

OEAP Split Tunneling Configuration

OEAP Access Control List > Rules > New

Sequence	<input type="text" value="1"/>		
Source	<input type="text" value="IP Address"/> ▼	IP Address <input type="text" value="172.31.255.0"/>	Netmask <input type="text" value="255.255.255.0"/>
Destination	<input type="text" value="IP Address"/> ▼	IP Address <input type="text" value="10.10.10.0"/>	Netmask <input type="text" value="255.255.255.0"/>
Protocol	<input type="text" value="Any"/> ▼	<div style="border: 2px solid red; padding: 2px;"><input type="text" value="Any"/> <input type="text" value="TCP"/> <input type="text" value="UDP"/> <input type="text" value="Other"/></div>	<div style="border: 2px solid red; padding: 2px;"><input type="text" value="Other"/> ▼ <input type="text" value="0"/></div>
Action	<input type="text" value="Permit"/> ▼		

- Protocol can be “any”, TCP, UDP, or “other”.

OEAP Split Tunneling Configuration

OEAP Access Control List > Rules > New

Sequence	<input type="text" value="1"/>	IP Address	<input type="text" value="172.31.255.0"/>	Netmask	<input type="text" value="255.255.255.0"/>
Source	<input type="text" value="IP Address"/>				
Destination	<input type="text" value="IP Address"/>	IP Address	<input type="text" value="10.10.10.0"/>	Netmask	<input type="text" value="255.255.255.0"/>
Protocol	<input type="text" value="Any"/>				
Action	<input type="text" value="Permit"/> <input type="text" value="Deny"/> <input type="text" value="Nat-Route"/>				

- Action can be “permit” (traffic is sent to the corporate network), “deny” (traffic is dumped, not sent to corporate and not sent to the local network), or Nat-Route (route all traffic matching the rule to the local network or NAT the traffic matching the rule to the internet)

OEAP Split Tunneling Configuration Examples

- All traffic to corporate network:
 - All DNS traffic is sent through CAPWAP to corporate
 - Other traffic is not mentioned, and therefore sent to corporate

OEAP Access Control List > Rules [< Back](#) [Add New Rule](#)

General

Access Control List Name MyOEAPACL1

Seq	Action	Source IP/Mask	Destination	Protocol	Source Port	Dest Port	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	<input checked="" type="checkbox"/>
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	TCP	Any	DNS	<input checked="" type="checkbox"/>

OEAP Split Tunneling Configuration Examples

- Local traffic split:
 - The first rule allows the traffic, for which the destination is “local subnet”, to be routed locally by the OEAP
 - The second rule ensures all other traffic is sent through CAPWAP

OEAP Access Control List > Rules [< Back](#) [Add New Rule](#)

General

Access Control List Name MyOEAPACL1

Seq	Action	Source IP/Mask	Destination	Protocol	Source Port	Dest Port	
1	Nat-Route	0.0.0.0 / 0.0.0.0	Local	Any	Any	Any	<input type="checkbox"/>
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	<input type="checkbox"/>

702W VLAN Support

702W VLAN Support

- In 7.6MR2, AP 702W comes with ports disabled, with one CLI command to enable them
- All ports are non-managed, in AP subnet
- In 8.0, you can control the ports individually, to enable/disable, and configure VLAN.



702W VLAN Support

- Default is still disabled

Enabled, define VLAN number

Enable	<input checked="" type="checkbox"/>	None
Enable	<input type="checkbox"/>	None

Enabled, in AP subnet

Wireless

- Access Points
 - All APs
 - Radios
 - 802.11a/n/ac
 - 802.11b/g/n
 - Dual-Band Radios
 - Global Configuration
- Advanced
 - Mesh
 - RF Profiles
 - FlexConnect Groups
 - FlexConnect ACLs
 - OEAP ACLs
 - Network Lists
 - 802.11a/n/ac
 - 802.11b/g/n
 - Media Stream
 - Application Visibility And Control
 - Country
 - Timers
 - Netflow
 - QoS

All APs > Details for AP7c69.f647.50a8

General Credentials Interfaces High Availability Inventory Advanced

Ethernet Interfaces

CDP Configuration

Ethernet Interface#	CDP State
0	<input checked="" type="checkbox"/>

Interface	Operational Status	Tx Unicast Packets	Rx Unicast Packets
GigabitEthernet0	UP	1507	797

Radio Interfaces

Number of Radio Interfaces 2

CDP Configuration

Radio Slot#	CDP State
0	<input type="checkbox"/>
1	<input type="checkbox"/>

Radio Slot#	Radio Interface Type	Sub Band	Admin Status	Oper Status
0	802.11b/g/n	-	Enable	UP
1	802.11a/n	-	Enable	UP

LAN Ports

Number of Ports 4

Port	State	VLAN	VLAN ID
1	Disable	<input type="checkbox"/>	None
2	Disable	<input type="checkbox"/>	None
3	Disable	<input type="checkbox"/>	None
4	Disable	<input type="checkbox"/>	None

702W VLAN Support

```
(Cisco Controller) >config ap lan ?
port-id      Port Id range (1 - 4)
enable       Enables VLAN support on LAN ports.
disable      Disables VLAN support on LAN ports.

(Cisco Controller) >config ap lan port-id ?
<port-id>    Enter the LAN port (1-4)

(Cisco Controller) >config ap lan port-id 3 ?
enable       Enable LAN port.
disable      Disable LAN port.

(Cisco Controller) >config ap lan port-id 3 enable AP7c69.f647.50a8

(Cisco Controller) >config ap lan enable ?
access       Enable/Disable Access VLAN support on LAN ports

(Cisco Controller) >config ap lan enable access ?
vlan         Enable/Disable Access VLAN support on LAN ports

(Cisco Controller) >config ap lan enable access vlan ?
<vlan-id>    Vlan Id range (2 - 4094)

(Cisco Controller) >config ap lan enable access vlan 21 ?
<port-id>    Port Id range (1 - 4)

(Cisco Controller) >config ap lan enable access vlan 21 3 ?
<Cisco AP>   Enter the name of the Cisco AP.

(Cisco Controller) >config ap lan enable access vlan 23 3 AP7c69.f647.50a8
```

702W VLAN Support

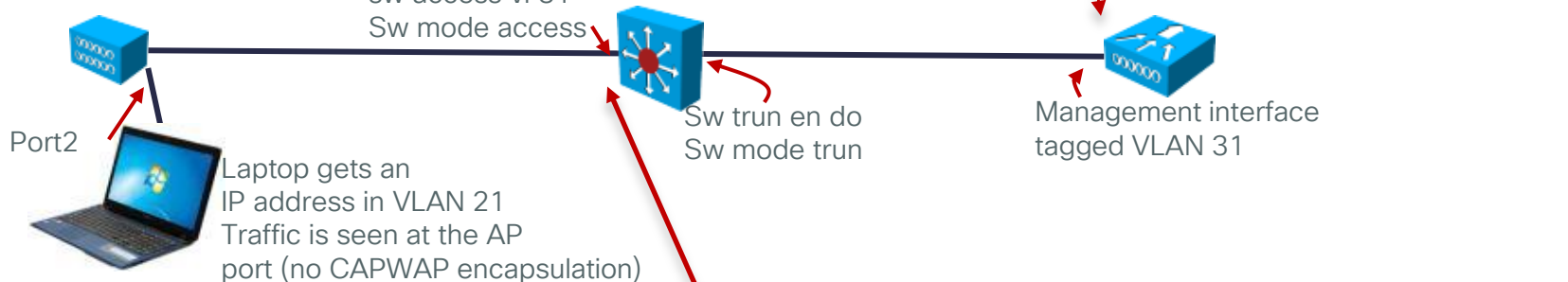
- VLANs do not need to exist on the WLC, just need to exist on AP switch
- Traffic is still bridged on AP switch
 - Only CAPWAP control and CAPWAP data (traffic to and from radio) is exchanged between AP IP address and WLC

Example

- Traffic from the ports is locally switched:

```
Sw trun en do
Sw trun nat vla 31
Sw mode trun
Or
sw access vl 31
Sw mode access
```

Port	State	VLAN	VLAN ID
1	Enable	<input type="checkbox"/>	None
2	Enable	<input checked="" type="checkbox"/>	21



258	16.274904000	0.0.0.0	255.255.255.255	DHCP	346	0	DHCP Discover	- Transaction ID 0xb170c51f
272	16.917418000	0.0.0.0	255.255.255.255	DHCP	594	0	DHCP Discover	- Transaction ID 0x1df87f18
309	18.288095000	10.10.21.4	10.10.21.202	DHCP	346	0	DHCP Offer	- Transaction ID 0xb170c51f
310	18.289313000	0.0.0.0	255.255.255.255	DHCP	358	0	DHCP Request	- Transaction ID 0xb170c51f
311	18.293015000	10.10.21.4	10.10.21.202	DHCP	346	0	DHCP ACK	- Transaction ID 0xb170c51f
414	19.923430000	0.0.0.0	255.255.255.255	DHCP	594	0	DHCP Discover	- Transaction ID 0x1df87f18
477	21.444278000	10.10.21.202	255.255.255.255	DHCP	346	0	DHCP Inform	- Transaction ID 0x744f7ccc
478	21.445382000	10.10.21.4	10.10.21.202	DHCP	346	0	DHCP ACK	- Transaction ID 0x744f7ccc
524	22.929549000	0.0.0.0	255.255.255.255	DHCP	594	0	DHCP Discover	- Transaction ID 0x1df87f18

```

# Frame 310: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits) on interface 0
# Ethernet II, Src: CiscoCon_62:88:db (c8:d7:19:62:88:db), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
# 802.1q Virtual LAN, PRI: 0, CFI: 0, ID: 21
# Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
# User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
# Bootstrap Protocol
    
```


702W VLAN Support

```
AP7c69.f647.50a8#dir
Directory of flash:/
.../...
 53 drwx      2048   Mar 1 1993 00:00:47 +00:00  configs
 59 -rwx       394   Jul 1 2014 00:27:27 +00:00  lan_port_cfg.txt
 60 -rwx     95008   Mar 1 1993 00:02:54 +00:00  lwapp_reap.cfg
.../...
131334144 bytes total (110434304 bytes free)

AP7c69.f647.50a8#more lan_port_cfg.txt
# Sardinia LAN port stored config
# Port  Enable
1      TRUE
2      FALSE
3      FALSE
4      FALSE
# Sardinia vlan stored config
# Port  vlanId  valid
1      0      FALSE
2      0      FALSE
3      0      FALSE
4      0      FALSE
# Don't update any thing in the above for backward compatibility
# Future configurations should be below the above configurations
```

702W VLAN Support

```
(Cisco Controller) >show ap lan ?  
<port id>      Enter the LAN port-Id range (1 - 4)  
port-summary  Displays all port info of an AP  
  
(Cisco Controller) >show ap lan port-summary ?  
<Cisco AP>     For specific AP  
(Cisco Controller) >show ap lan port-summary AP7c69.f647.50a8
```

LAN Port configuration for AP AP7c69.f647.50a8

Port	Status	VlanId
LAN1	ENABLED	19
LAN2	DISABLED	None
LAN3	ENABLED	23
LAN4	DISABLED	None

```
(Cisco Controller) >show ap lan 3 ?  
<Cisco AP>     For specific AP  
(Cisco Controller) >show ap lan 3 AP7c69.f647.50a8
```

LAN Port configuration for AP AP7c69.f647.50a8

Port	Status	VlanId
LAN3	ENABLED	23

Does not mean the port is "up", this is just the config



FlexConnect Features

Agenda

- FlexConnect VideoStream
- FlexConnect Faster Time to Deploy
- FlexConnect Proxy ARP

H/W Platforms Supported in 8.0

Product	H/W Platforms Supported
AP	WSSI module, 11ac module, 3G Module 1260, 3500, 600,1600, 3600, 2600, 3700, 2700, 702, 702W, 802,1530, 1552WU, 1550** 1040, 1140,*#1130, *#1240, **1520
WLC	2500, WLCM2, 5500, WiSM2, 7500 , 8500, vWLC, HA-SKU, UCS-E platforms
MSE	3355, Virtual Appliance

***# feature parity with 7.3 sw release; 8.0 features not supported**

**** 1520 and 1550 with 64-MB will not support PPPoE and PMIPv6**

Flex – 7.2

- Smart AP Image Upgrade
- ACLs on FlexConnect AP
- AAA Override of VLAN - dynamic VLAN assignment for locally switched clients
- FlexConnect Re-branding
- Fast Roaming for Voice Clients
- Peer-to-Peer Blocking

Flex – 7.3 & 7.4

- Flex 7500 Scale Update
- VLAN Based Central Switching
- Split Tunneling
- Central DHCP Processing
- WGB/uWGB Support with local switching
- Bidirectional Rate Limiting
- Support for ISE BYOD Registration & Provisioning

Flex – 7.5, 7.6, 8.0

- PEAP and EAP-TLS Support (7.5)
- FlexConnect Group specific WLAN-VLAN mapping(7.5)
- AAA Client ACL(7.5)
- Ethernet Fallback (7.6)
- **VideoStream for local switching (8.0)**
- **Faster time to deploy (8.0)**
- **Flex with Mesh deployment support (8.0)**

FlexConnect VideoStream

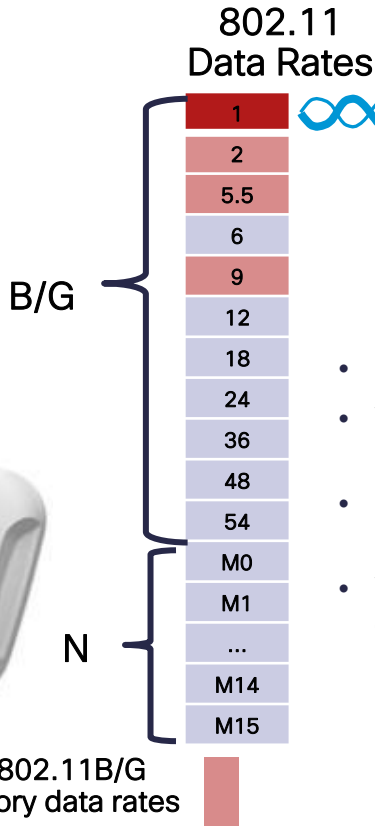
Video Multicast Delivery Challenges

Technical Challenges

- Multicast packets (UDP) are sent as broadcast packets over the air per 802.11 standard
- Broadcast packets do not use error correction: “fire and forget”
- Broadcast packets are sent at lowest supported mandatory data rate:

1 Mb for B/G (400K actual)
6 Mb for A (2.7 Mb actual)

Video Server



Video Impact

- Choppy, unreliable video
- VideoStream does not utilize 802.11n/ac high throughput data rates
- Heavy utilization of channel due to high rate of very slow packets
- Video delivery is not reliable, causing poor quality of experience



Flex Enhancements: Support for VideoStream in Local Switching

- Today, VideoStream can only be done on FlexConnect central switching (while the AP is in connected mode)
- Admission Control is used to protect the system from excessive multicast client bandwidth usage and over-subscription
- Admission control runs on the WLC (the AP just forwards the IGMP join/report from the client; the WLC then makes the admission decision)
- This may not always be desirable because:
 - The admission process over WAN links can add considerable delays (~3.5x the Round Trip Time)
 - Video traffic can quickly fill up a WAN link which could otherwise be capacity-planned to meet the CAPWAP control traffic requirements

Flex Enhancements: Support for VideoStream in Local Switching (Cont.)

- VideoStream for local switching is available on code 8.0. However, because of the local switching aspect, the controller is unable to perform admission control in real-time for that locally switched incoming multicast traffic.
- To keep configuration simple across all modes of APs (non-Flex and FlexLocal, FlexCentral), the same current media stream group configurations will also be used for Flex locally-switched WLANs (no new GUI or CLI)
- Design considerations:
 - Since we do not use the centralized admission control from the WLC, the displayed media stream clients monitored on the controller's GUI or CLI will not include the FLEXCONNECT locally-switched ones
 - FLEXCONNECT local switching WLAN will not be part of the video admission control; hence, there is risk that from the controller side it could over-subscribe video clients with centrally-switched WLANs on the same FLEXCONNECT AP, without taking into account the local video clients.

Advantages of FlexConnect VideoStream



Cisco's *VideoStream* Technology

Transmission adapts to individual client data rate

Reliable retransmission minimizes loss

Better channel utilization

Ensures QoS priority and quality

FlexConnect VideoStream Client Data

Version 8.0.72.149	Channel Width	1.5 Mbps	5 Mbps	10 Mbps
1600 AP	40 MHz	43	21	9
2600 AP	40 MHz	42	23	12
3600 AP	40 MHz	47	24	9
3600 AP + 11ac	40 MHz	32	17	8
3600 AP + 11ac	80 MHz	38	32	20
3700 AP	40 MHz	47	23	12
3700 AP	80 MHz	53	29	19

FlexConnect VideoStream Support

Controllers

5508, 7510, 8510, 2504, vWLC, WiSM2

Access Points

1140, 1260, 3500, 1600, 2600, 3600, 3700, 2700, 1530

Software Support

CUWN Release 8.0

FlexConnect VideoStream Configuration

Enable VideoStream - Global

The screenshot shows the Cisco Wireless configuration page. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar has a 'Wireless' section with a tree view containing 'Access Points', 'Advanced', 'Mesh', 'RF Profiles', 'Network Lists', 'FlexConnect Groups', and 'Media Stream'. The 'Media Stream' section is expanded to show 'General' and 'Streams'. The 'General' page is titled 'Media Stream > General'. A red box highlights the 'Multicast Direct feature' which is checked and labeled 'Enabled'. Below this is the 'Session Message Config' section with several input fields and a text area. A red arrow points to the 'WIRELESS' tab in the top navigation bar, and another red arrow points to the 'General' link in the left sidebar.

```
(Cisco Controller) >config media-stream multicast-direct ?  
enable      Enable Global Multicast to Unicast Conversion  
disable     Disable Global Multicast to Unicast Conversion
```

FlexConnect VideoStream Configuration

Add Stream Configuration

The screenshot shows the Cisco Wireless configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'Wireless' tab is selected. The left sidebar shows a tree view with 'Media Stream' selected. The main content area is titled 'Media Stream > New' and contains the following configuration fields:

Stream Name	Media2
Multicast Destination Start IP Address(ipv4/ipv6)	229.77.77.28
Multicast Destination End IP Address(ipv4/ipv6)	229.77.77.28
Maximum Expected Bandwidth(1 to 35000 Kbps)	500

Below these fields is the 'Resource Reservation Control(RRC) Parameters' section:

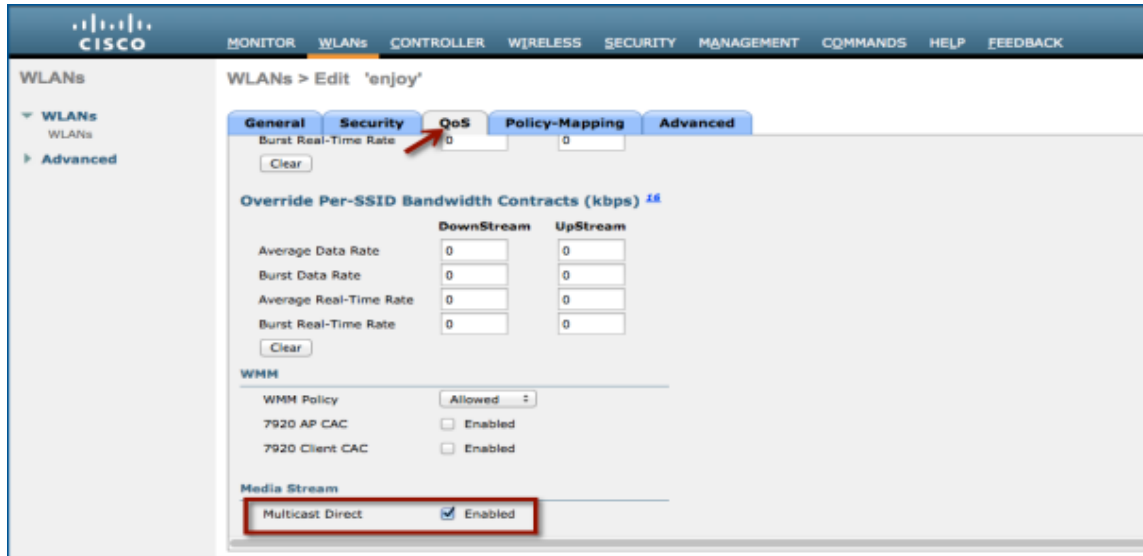
Select from predefined templates	Select
Average Packet Size (100-1500 bytes)	1200
RRC Periodic update	<input checked="" type="checkbox"/>
RRC Priority (1-8)	1
Traffic Profile Violation	best-effort

Buttons for '< Back' and 'Apply' are visible at the top right of the configuration area.

```
(Cisco Controller) >configure media-stream add multicast-direct <media-stream-name> <start-IP> <end-IP> [template | detail <bandwidth> <packet-size> <Re-evaluation> video <priority> <drop|fallback>]'
```

FlexConnect VideoStream Configuration

Enable VideoStream - WLAN



```
(Cisco Controller) >config wlan media-stream multicast-direct 1 ?  
enable          Enables Multicast-direct on the WLAN  
disable        Disables Multicast-direct on the WLAN.
```


FlexConnect VideoStream Monitoring Controller

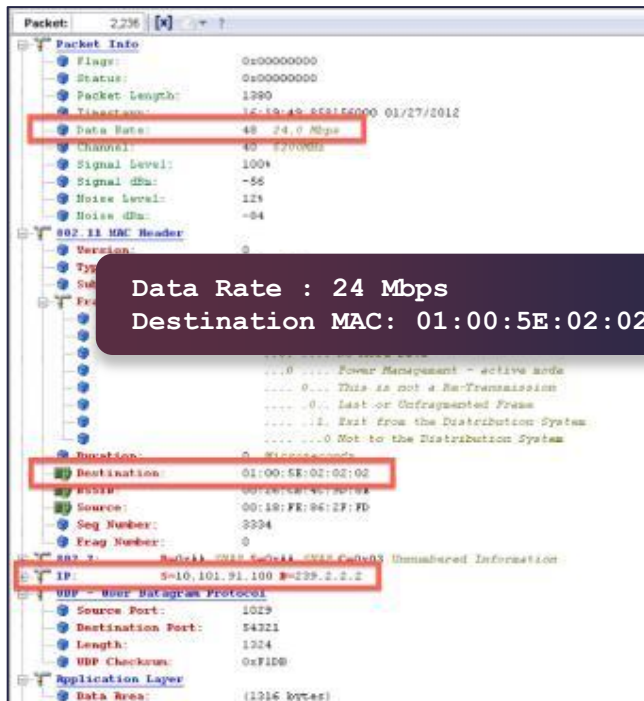
The screenshot shows the Cisco FlexConnect monitoring interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, FEEDBACK. The left sidebar lists various monitoring categories: Monitor, Summary, Access Points, Cisco CleanAir, Statistics, CDP, Rogues, Redundancy, Clients, Sleeping Clients, Multicast, Applications, and Local Profiling. The main content area displays 'Multicast Groups' with two mapping tables: 'Layer3 MGID(Multicast Group ID) Mapping' and 'Layer2 MGID(Multicast Group ID) Mapping'. A red box highlights the 'FlexConnect Multicast Media Stream Clients' table.

Client-Mac	Stream-Name	Multicast-IP	Ap-Name	Vlan	Type
7c:d1:c3:86:7e:dc	Media2	229.77.77.28	AP_1600	0	Multicast Direct
88:cb:87:bd:0c:ab	Media2	229.77.77.28	AP_1600	0	Multicast Direct
d8:96:95:02:7e:b4	Media2	229.77.77.28	AP_1600	0	Multicast Direct

```
(Cisco Controller) >show flexconnect media-stream client summary
```

Client Mac	Stream Name	Multicast IP	AP-Name	VLAN	Type
7c:d1:c3:86:7e:dc	Media2	229.77.77.28	AP_1600	0	Multicast Direct
88:cb:87:bd:0c:ab	Media2	229.77.77.28	AP_1600	0	Multicast Direct
d8:96:95:02:7e:b4	Media2	229.77.77.28	AP_1600	0	Multicast Direct

FlexConnect VideoStream Monitoring WireShark



Packet: 2,236 [x] ?

Packet Info

- Flags: 0x00000000
- Status: 0x00000000
- Packet Length: 1380
- Timestamp: 15-19:49:55.15000 01/27/2012
- Data Rate: 48 24.0 Mbps**
- Channel: 40 22000Hz
- Signal Level: 100%
- Signal dBm: -56
- Noise Level: 12%
- Noise dBm: -84

802.11 MAC Header

- Version: 0
- Type: 0
- Subtype: 0
- Duration: 0 microseconds
- Destination: 01:00:5E:02:02:02**
- Source: 00:18:8E:96:2F:FD
- Seq Number: 3334
- Frag Number: 0

802.2: 802.2.1.5-10.101.91.100 B=239.2.2.2 Unnumbered Information

- IP: 5-10.101.91.100 B=239.2.2.2

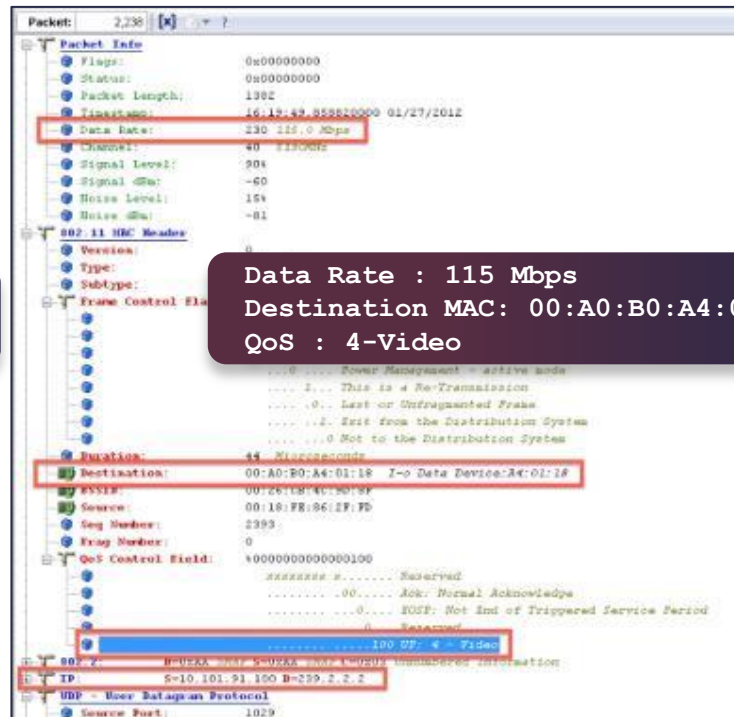
UDP - User Datagram Protocol

- Source Port: 1029
- Destination Port: 54321
- Length: 1324
- UDP Checksum: 0xF1D0

Application Layer

- Data Area: (1316 bytes)

Data Rate : 24 Mbps
Destination MAC: 01:00:5E:02:02:02



Packet: 2,238 [x] ?

Packet Info

- Flags: 0x00000000
- Status: 0x00000000
- Packet Length: 1382
- Timestamp: 16-19:49:55.820000 01/27/2012
- Data Rate: 230 115.0 Mbps**
- Channel: 40 22000Hz
- Signal Level: 90%
- Signal dBm: -60
- Noise Level: 15%
- Noise dBm: -81

802.11 MAC Header

- Version: 0
- Type: 0
- Subtype: 0
- Duration: 0 microseconds
- Destination: 00:A0:B0:A4:01:18 I-o Data Device: A4:01:18**
- Source: 00:18:8E:96:2F:FD
- Seq Number: 3393
- Frag Number: 0

802.2: 802.2.1.5-10.101.91.100 B=239.2.2.2 Unnumbered Information

- IP: 5-10.101.91.100 B=239.2.2.2

UDP - User Datagram Protocol

- Source Port: 1029

Data Rate : 115 Mbps
Destination MAC: 00:A0:B0:A4:01:18
QoS : 4-Video

Legacy Multicast

Multicast Direct

FlexConnect VideoStream Monitoring Access Point

```
AP_1600#show capwap mcast flexconnect clients
=====
Bridge Group: 1
=====
Multicast Group Address 229.77.77.28::
MCUC List:
Number of MCUC Client: 3
88cb.87bd.0cab(Bridge Group = 1 Vlan = 0)
7cd1.c386.7edc(Bridge Group = 1 Vlan = 0)
d896.9502.7eb4(Bridge Group = 1 Vlan = 0)
-----
MC Only List:
Number of MC Only Client: 0
-----
```

FlexConnect VideoStream Limitations

- No admission control for locally-switched clients' multicast video requests
- Due to CAPWAP payload length, only the first 100 media streams will be pushed from WLC to AP
 - e.g., *config media-stream add multicast-direct stream1 225.0.0.1 225.0.0.10 template coarse:* is one entry
- Roaming in standalone mode of FlexConnect AP will not be supported for this feature
- Only IPv4 support
- Session Message Config is not supported

FlexConnect Faster Time to Deploy

Flex Enhancements: Faster Time to Deployment

- 95% of indoor APs ship in local mode
- After a local mode AP joins the WLC, the customer can then change its mode to FlexConnect mode, but prior to 8.0 that would require the AP to reload and rejoin one more time
- New in 8.0: If you change an AP's mode from local to FlexConnect, you can skip the one extra reload, and you can start configuring your FlexConnect parameters without having to wait for the AP to rejoin!
- 8.0 also supports changing the AP's sub mode to wIPS without having to reboot the AP.
- Only Local mode -> Flexconnect mode conversion is supported. Any other mode change will cause the AP to reboot. Similarly, changing the AP sub mode to wIPS does not require a reboot, but the rest of the sub mode configuration does require and AP reboot.

FlexConnect AP Mode Conversion

The screenshot shows the configuration page for AP_2600. The 'FlexConnect' tab is active. The 'AP Mode' dropdown menu is open, and 'FlexConnect' is selected. A red arrow points to the 'FlexConnect' option. The 'Apply' button is highlighted with a red box.

General		Versions	
AP Name	AP_2600	Primary Software Version	8.0.72.114
Location	default location	Backup Software Version	0.0.0.0
AP MAC Address	fc:99:47:d9:86:90	Predownload Status	None
Base Radio MAC	54:78:1a:70:04:70	Predownload Version	None
Admin Status	Enable	Predownload Next Retry Time	NA
AP Mode	FlexConnect	Predownload Retry Count	NA
AP Sub Mode	local	Boot Version	12.4.25.1
Operational Status	monitor	IOS Version	15.3(20140203:113124)S
Port Number		Mini IOS Version	0.0.0.0
Venue Group		IP Config	
Venue Type		IP Address	9.5.56.110
Venue Name		IPv6 Address	
Language		Static IP	<input type="checkbox"/>

Eliminates reboot when AP is converted to FlexConnect mode

Changing to any other mode/sub mode requires reboot

FlexConnect Proxy ARP

FlexConnect Proxy ARP

- Proxy ARP allows the AP to answer ARP requests for the wireless clients (no need to forward the request to the air)
- This feature is useful for the following reasons:
 - More reliable ARP responses on behalf of wireless clients
 - Less load on the wireless channel
 - Reduced power consumption for mobile clients
 - 792x phones can monitor whether proxy ARP is in use on the WLAN (CCX S47), and if it is, can spend more time sleeping; hence, longer battery life
- Proxy ARP is supported with LAP mode Cisco Unified Wireless Network APs and with aIOS APs. Only with locally switched H-REAP WLANs is proxy ARP not supported today.

FlexConnect Proxy ARP

- In 8.0, you can enable ARP caching for locally switched Flex APs. Default is disabled.
- It is a global config and applies only to Flex APs in local switching mode

```
(Cisco Controller) >show flexconnect summary
Fallback Radio Shut configuration:
Fallback Radio Shut: Disabled
Arp-caching: Disabled

(Cisco Controller) >config flexconnect arp-caching ?
enable          Enable Arp Caching for flexconnect
disable         Disable Arp Caching for flexconnect
```

FlexConnect Proxy ARP

- Verification / Troubleshooting:

```
AP7c69.f647.50a8#show derived-config | inc arp  
capwap ap arp-cache
```

Received request, 172.31.255.113 is one of our wireless clients

```
AP7c69.f647.50a8#debug arp
```

```
*Jul 1 02:33:39.311: IP ARP: rcvd req src 172.31.255.24 0018.8bbf.5f63, dst  
172.31.255.113 BVI1
```

AP records ARP of wired requestor (172.31.255.24)

```
*Jul 1 02:33:39.311: IP ARP: creating entry for IP address: 172.31.255.24, hw:  
0018.8bbf.5f63
```

AP responds, source IP is the wireless client IP (AP proxies)

```
*Jul 1 02:33:39.311: IP ARP: sent rep src 172.31.255.113 e0b9.bacc.e62e,  
dst 172.31.255.24 0018.8bbf.5f63 GigabitEthernet0
```

Mesh Enhancements

Agenda

- Flex on Mesh
- Mesh Fast Convergence
- No MAC Authentication
- Daisy Chaining Performance Numbers

Outdoor AP Software Evolution

2014

7.6
CY13

- 1530 support
- “-F” domain for Indonesia on 1530
- Mesh Convergence – Phase 1

Autonomous

- 1530 support

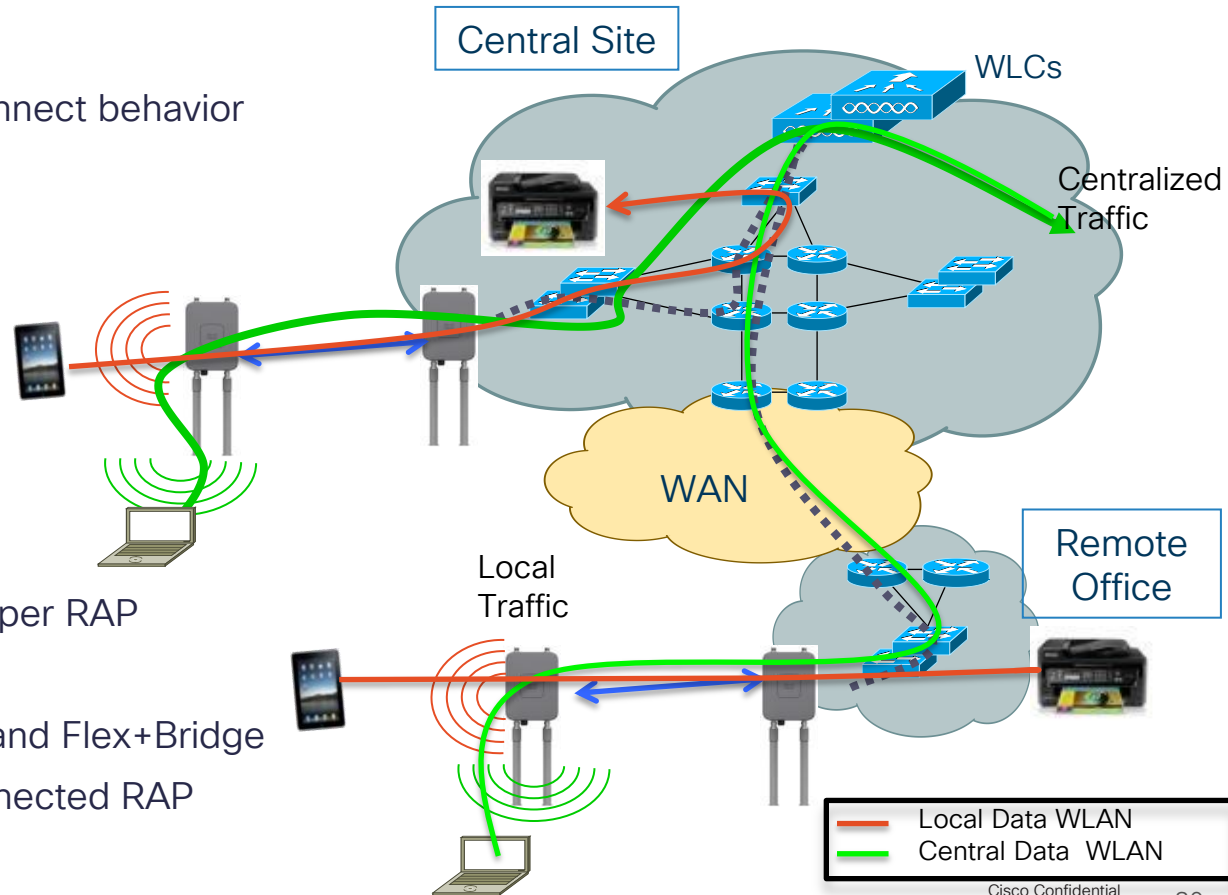
8.0
CY14

- Flex+Bridge mode
- Mesh Convergence – Phase 2 (<1 min, 3rd hop)
- Mesh without MAC filter list
- Support for SFP & PoE-Out port on 1550

Flex on Mesh (Flex+Bridge)

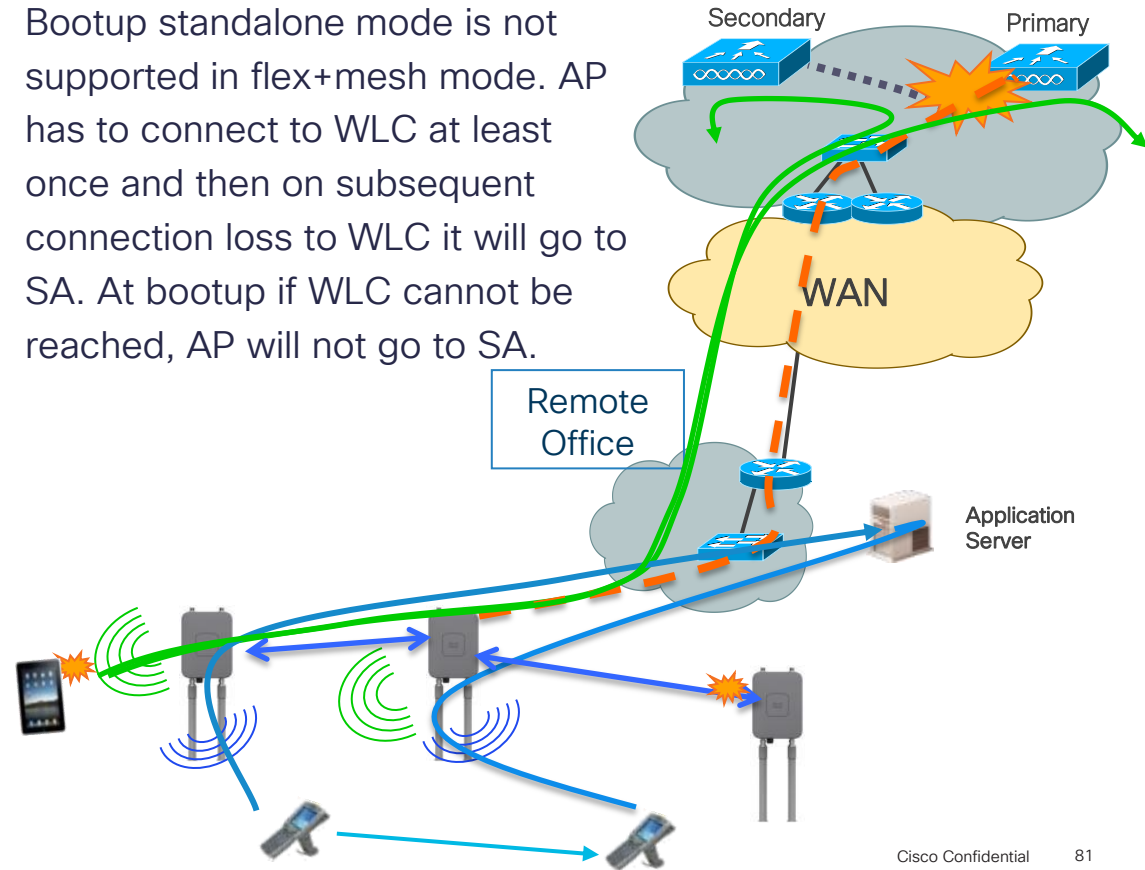
Flex on Mesh (Flex+Bridge)

- New AP mode that allows FlexConnect behavior across mesh-enabled AP
- Control plane supports:
 - Connected (WLC is reachable)
 - Standalone (WLC not reachable)
- Data Plane supports:
 - Centralized (split MAC)
 - Local (local MAC)
- Flexconnect Groups
- Max 8 mesh hops, max 32 MAPs per RAP
- Local AAA support
- A WLC can have a mix of Bridge and Flex+Bridge
- MAPs inherit VLANs from the connected RAP



Flex+Bridge Failover

- AP SSO is supported for RAP only
- Flex+Bridge deployments should be implemented with N+1 redundancy
- Multi-sector RAP deployments can be used for redundancy
- RAP to standalone mode when WLC is not reachable
- MAPs to standalone mode when WLC is not reachable but gateway is
- When in standalone mode no new mesh AP can join the mesh tree
- Bootup standalone mode is not supported in flex+mesh mode. AP has to connect to WLC at least once and then on subsequent connection loss to WLC it will go to SA. At bootup if WLC cannot be reached, AP will not go to SA.



Flex+Bridge Feature Comparison

Feature\AP Mode	Local Mode	Bridge Mode	FlexConnect Mode
Central Switching	Yes	Yes	Yes
Root Ethernet VLAN Bridging	No	Yes (secondary Ethernet hosts)	Yes
Secondary Ethernet Access Ports	No	Yes	No
Secondary Ethernet VLAN Trunk Ports	No	Yes	No
Local VLAN Inheritance by MAPs from RAPs	No	Yes - Secondary Ethernet "access" ports only	No
Wireless Child Mesh APs	No	Yes	No
Fault Tolerant Resilient Mode	No	No	Yes
Security ACLs per VLAN on Ethernet Root Ports	No	No	Yes
Integrated IP Routing (PPP/PPPoE/NAT)	No	No	Yes
VLAN Transparent Bridging	No	No	No
Path Control Protocol	No	Yes	No

Flex+Bridge Mode
Yes
Yes
Yes
Yes
Yes – both bridged 802.11 WLANs and Ethernet "access" ports
Yes
Yes
Yes (on RAPs)
No*
No
Yes

*PPPoE is not supported in Flex+Mesh in 8.0 (even on RAPs)

Flex on Mesh (Flex+Bridge) Feature Support

- **Fault Tolerant Resilient Mode** – enables an AP to continue bridging traffic when the connection to the CAPWAP controller is lost.
 - Both mesh and non-mesh “root APs” continue to bridge traffic.
 - A child mesh AP (MAP) maintains its link to a parent AP and continues to bridge traffic (until its parent link is lost). A child mesh AP can select a new parent (if primary parent is lost), but cannot establish a child link until it reconnects to the CAPWAP controller.
 - Existing wireless clients on the locally switching WLAN can stay connected with their AP in this mode. Their traffic will continue to flow through the mesh and wired network. New wireless clients can connect to the AP on a locally switched WLAN if it is locally authenticated and the radius server is reachable.

Flex on Mesh (Flex+Bridge) Feature Support, Cont.

- **Security ACLs per VLAN on Ethernet Root Ports** – The user can configure a separate set of security ACLs for each VLAN that is configured for an Ethernet root port. In a mesh network, only “root APs” (RAPs) have an Ethernet root port.
- **Integrated IP Routing** – If integrated IP routing is enabled on an AP, then the AP routes IPv4 traffic over a PPP/PPPoE/NAT link to an IP network. IP routing is always disabled on a child mesh AP (MAP).
- **VLAN Transparent Bridging** – Previously, if VLAN transparent bridging was enabled, mesh APs transparently bridged VLAN-tagged frames, between primary and secondary Ethernet LANs, without removing or processing the VLAN tags. VLAN transparent bridging is not supported in the 8.0 release. Instead, the user must explicitly enter a set of allowed VLAN IDs for each secondary Ethernet trunk port. (Note that no function is lost.)

Flex on Mesh (Flex+Bridge) Configuration

MONITOR WLANs CONTROLLER WIRELESS SECURITY MA

All APs > Details for Class3

General Credentials Interfaces High Availability

General

AP Name: Class3
Location: Bldg1
AP MAC Address: 44:2b:03:9a:88:96
Base Radio MAC: 3c:ce:73:1a:09:60
Admin Status: Enable
AP Mode: local
AP Sub Mode: local
Operational Status: monitor
Port Number: Rogue Detector
Venue Group: Bridge
Venue Type: Flex+Bridge
Venue Name: Unspecified

```
(Cisco Controller) >config ap mode ?
```

```
Local          Local mode for the Cisco AP.  
bridge         Bridge mode for the Cisco AP.  
flex+bridge    Flex+Bridge mode for the Cisco AP.  
flexconnect    flexconnect mode for the Cisco AP.  
.../...
```

```
(Cisco Controller) >config ap mode flex+bridge ?  
submode        Configures an Cisco AP submode of operation.
```

```
(Cisco Controller) >config ap mode flex+bridge submode ?  
none           No submode active for the Cisco AP.  
pppoe-only     WIPS submode for the Cisco AP.  
pppoe-wips     WIPS submode for the Cisco AP.  
wips           WIPS submode for the Cisco AP.
```

```
(Cisco Controller) >config ap mode flex+bridge submode none ?  
<Cisco AP>    Enter the name of the Cisco AP.
```

```
(Cisco Controller) >config ap mode flex+bridge submode none Class3
```

```
Changing the AP's mode or submode will cause the AP to reboot.  
Are you sure you want to continue? (y/n) y
```

Flex on Mesh (Flex+Bridge) Configuration

The screenshot displays the configuration page for a Cisco AP Class3. The 'FlexConnect' tab is selected, and the 'Resilient Mode(Standalone mode support)' checkbox is checked. A red box highlights this checkbox, with a red arrow pointing to it from a text annotation: "Enabled by default (switches locally if WLC is lost)".

Navigation tabs: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, FEEDBACK

Page Title: All APs > Details for Class3

Configuration Tabs: General, Credentials, Interfaces, High Availability, Inventory, Mesh, FlexConnect, Advanced

Configuration Fields:

- AP Role: MeshAP
- Bridge Type: Indoor
- Bridge Group Name: [Empty]
- Strict Matching BGN:
- Ethernet Bridging:
- Preferred Parent: none
- Backhaul Interface: 802.11a
- Bridge Data Rate (Mbps): AP's Default
- Ethernet Link Status: UP
- Heater Status: N/A
- Internal Temperature: N/A

FlexConnect Settings:

- Resilient Mode(Standalone mode support):
- Install mapping on radio backhaul:
- VLAN Support:
- FlexConnect Group Name: Not Configured

PreAuthentication Access Control Lists:

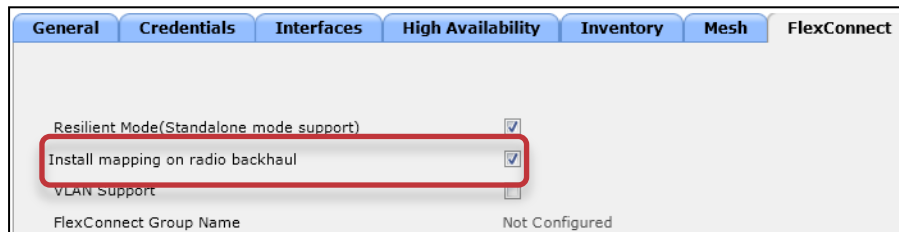
- [External WebAuthentication ACLs](#)
- [Local Split ACLs](#)
- [Central DHCP Processing](#)
- [Layer2 ACLs](#)

```
(Cisco Controller) >config ap flexconnect bridge resilient ?
<Cisco AP>      Enter the name of the Cisco AP.

(Cisco Controller) >config ap flexconnect bridge resilient Clas3 ?
enable          Enable standalone mode
disable         Disable standalone mode
```

Flex on Mesh (Flex+Bridge) Configuration

- FlexConnect APs can have specific WLAN to VLAN mapping
- You can push the RAP/Flex WLAN to VLAN mapping through the radio to the other MAPs using the “Install mapping on radio” option (disabled by default, individual Flex AP config expected):

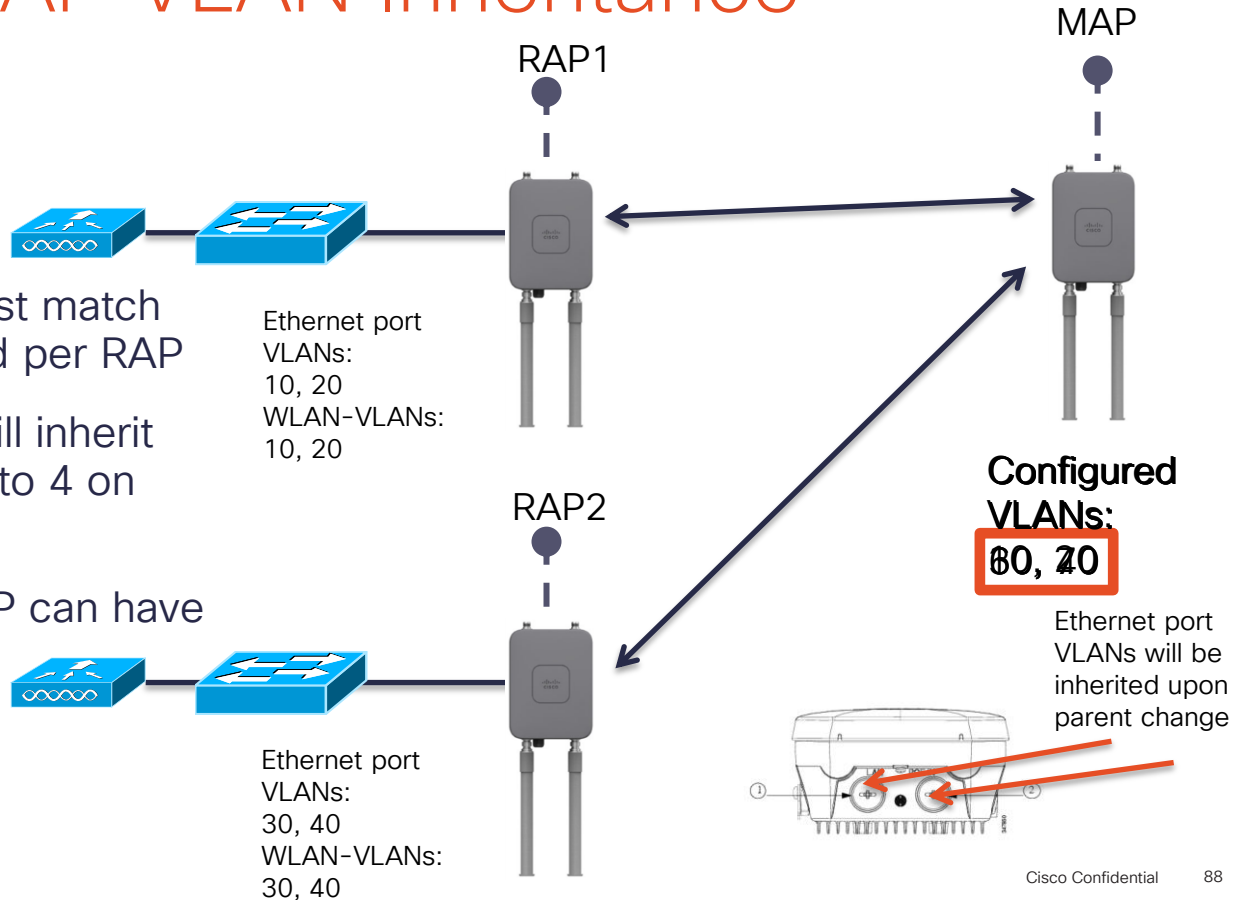


General	Credentials	Interfaces	High Availability	Inventory	Mesh	FlexConnect
Resilient Mode(Standalone mode support) <input checked="" type="checkbox"/>						
Install mapping on radio backhaul <input checked="" type="checkbox"/>						
VLAN Support <input type="checkbox"/>						
FlexConnect Group Name						Not Configured

```
(Cisco Controller) >config ap flexconnect bridge backhaul-wlan ?  
  
<Cisco AP>      Enter the name of the Cisco AP.  
  
(Cisco Controller) >config ap flexconnect bridge backhaul-wlan Class3 ?  
  
enable          Enable the WLAN.  
disable         Disable the WLAN.
```

Flex+Bridge MAP VLAN Inheritance

- The Ethernet port VLANs must match the WLAN-VLANs configured per RAP
- To avoid stranding, a MAP will inherit the Ethernet port VLANs (up to 4 on the 1552) from its parent
- Each parent change, the MAP can have different VLANs configured



Mesh Fast Convergence

8.0 Mesh Fast Convergence

	Parent Loss Detection / Keep-Alive Timers	Channel Scan / Seek	DHCP / CAPWAP Information	Time per Hop (sec)**
Standard	21 / 3 sec	Scan/Seek all 5-GHz channels	Renew/Restart CAPWAP	48.6*
Fast	7 / 3 sec	Scan/Seek only channels found in same bridge group	Maintain DHCP and CAPWAP	20.5*
Very Fast	4 / 1.5	Scan/Seek only channels found in same bridge group	Maintain DHCP and CAPWAP	15.9*

*Numbers are shown for same WLC, same channel, and same subnet. Times are longer if these variables are changed.

**Numbers are part of early feature tests, and are subject to change as of 8.0 CCO

WLC CLI Configuration only (Warning: Decreasing convergence time can lead to more parent changes)

```
(Cisco Controller) >config mesh convergence ?  
  
fast          Set fast convergence method  
standard     Set standard convergence method  
very-fast    Set very fast convergence method
```

8.0 Mesh Fast Convergence

- Verification: WLC side:

```
(Cisco Controller) >show mesh config
.../...
Mesh Convergence Method..... standard
```

- Verification: AP side:

```
Class3#sh mesh convergence
show MESH Convergence

Convergence method: standard
Subset channels:
Num.of Subset channels: 0

Mesh Convergence Global Data
old_conv_method: standard
updated_subset: 0 subset_chan_seek: 0
```

```
Class3#debug mesh convergence
mesh convergence debugging is on
Class3#
*Jun 11 01:40:14.767: ADJEVENT:adjTimerMN: Current
parent 442b.039a.8896, NEEDUP 0, UPDATED 0
*Jun 11 01:40:14.767: MESH_CONVERGENCE:adjacency
442b.039a.8896 stickyEase 43448576
```

No MAC Authentication

New MAC Authentication, Problem

- Deployment Model:
 - Mining customers quickly build up and tear down mining sites, and then move to the next location
 - Mesh APs end up joining many different WLCs
- Problem:
 - It is very difficult to add the AP's MAC address to each WLC across different sites
 - Locally Signed Certs (LSC) are the solution of choice
 - Mesh APs with LSC still need to be added to the MAC Authentication Filter



Mesh AP – Joining Without MAC Filter

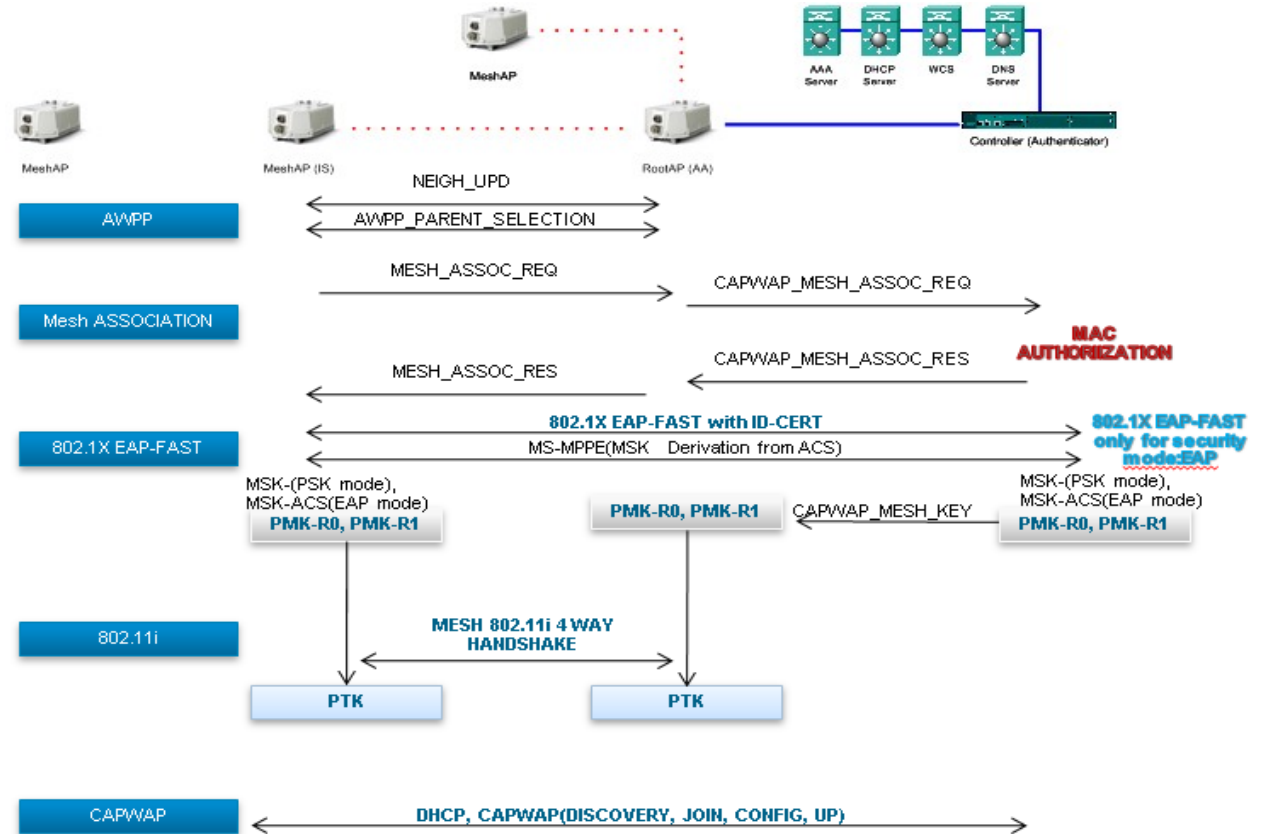
- In 8.0, you can use LSC-Only MAP Authentication (wild card MAC), which effectively disables the MAC filter
- In order to ensure only authorized RAP/MAPs authenticate, WLC must be able to force the EAP with LSC authentication:

SL No	Operation	MAC FILTER	LSC-Only MAP Authentication
1	LSC-Only MAP Authentication enabled	disabled	enabled
2	LSC-Only MAP Authentication disabled	enabled	disabled
3	Security mode: EAP & PSK	EAP or PSK can be used	Only EAP with LSC should be used.
4	Certificates: MIC & LSC	MIC or LSC can be used	Only EAP with LSC should be used

Note: When we enable wildcard MAC then we need to use EAP with LSC to have valid security.

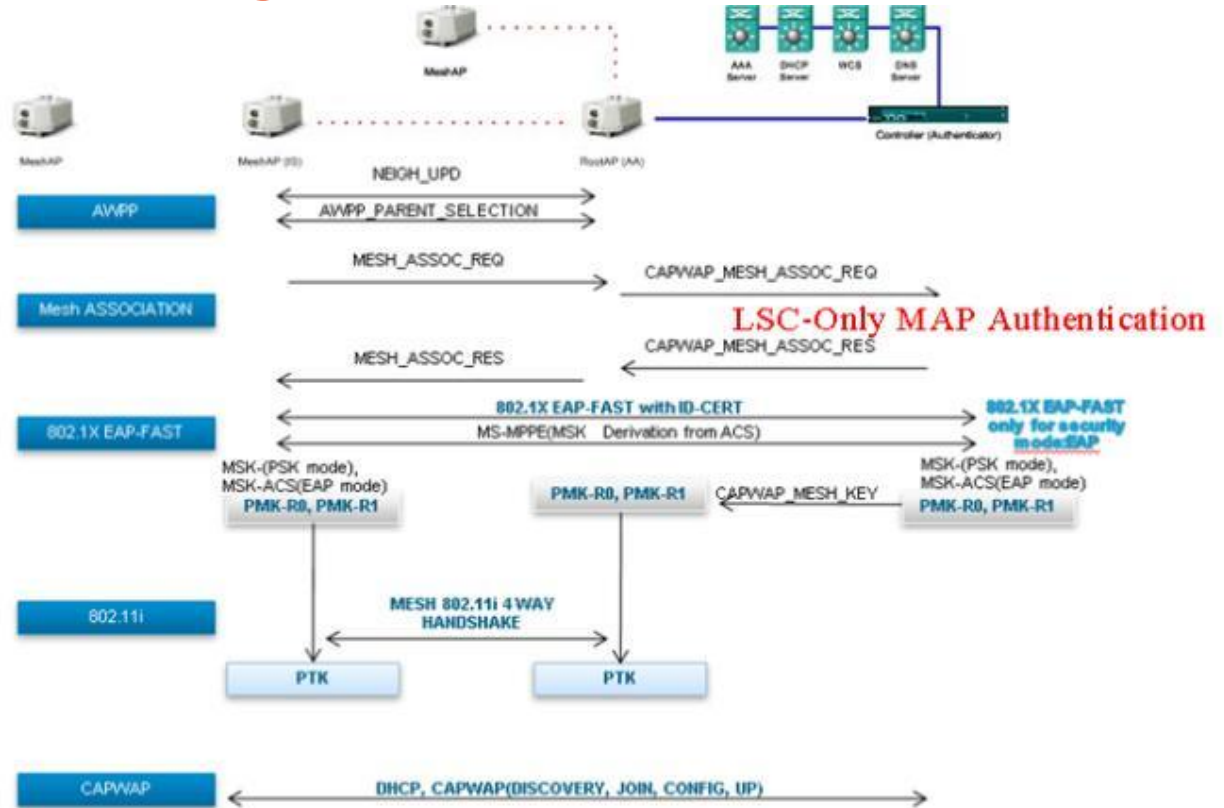
Mesh AP – Joining Without MAC Filter

- Current (7.6 & before) choreography, with MAC authentication:



Mesh AP – Joining Without MAC Filter

- New choreography, with LSC-Only authentication:



Mesh AP – Joining Without MAC Filter

- Choreography notes:
 - With MAC authentication, PSK does not require EAP-FAST because it has MSK key hardcoded inside the code of AP and WLC. Only during EAP security mode we require EAP-FAST. EAP-FAST authenticates the client using the default factory certificate or LSC if MAP is already provisioned with LSC and generates the key and sends the key to MAP. Using these keys it undergoes message handshake and generates the PTK key. Now, in capwap Mesh AP joins the WLC using MIC or LSC.

Mesh AP – Joining Without MAC Filter

- Choreography notes:
 - With LSC Only authentication, WLC allows wildcard mac address in mac filter list and allows all RAP/MAPs to join the WLC, i.e., MAC authorization is disabled.
 - PSK security mode does not provide the valid security. If PSK is chosen as the security mode then it leads to security threat, and any MAP, even a (Cisco) rogue MAP, can join the WLC. For this reason, PSK should not be used in combination with wildcard MAC and is not supported.
 - EAP security mode provides the valid security with LSC. During EAP-FAST MAP gets authenticated using LSC and gets the MSK key from WLC. If there are any rogue MAPs, they get filter over here. Using these keys it undergoes message handshake and generates the PTK key. Now in capwap, Mesh AP joins the WLC using LSC only.

Mesh AP – Joining Without MAC Filter

- Configuration: First, connect your MAPs over Ethernet (no over-the-air provisioning):

The screenshot shows the Cisco Wireless LAN Controller configuration interface. The 'Mesh' configuration page is active, with the 'Security' section expanded. In the 'Security' section, 'LSC Only MAP Authentication' is checked and set to 'Enabled'. Other security options like 'External MAC Filter Authorization' and 'Force External Authentication' are also present but unchecked. The 'General' section shows 'Range (RootAP to MeshAP)' set to 12000 feet. The 'Ethernet Bridging' section has 'VLAN Transparent' checked and enabled. The 'Server ID' table is empty. A red box highlights the 'LSC Only MAP Authentication' checkbox and its 'Enabled' status.

A warning dialog box titled 'Message from webpage' with a question mark icon. The text reads: 'Warning: Enabling LSC Only MAP Authentication will not provision LSC Certificate into MAP over the air. Please make sure MAP is connected to WLC using Ethernet cable to provision LSC. Are you sure you want to continue?'. There are 'OK' and 'Cancel' buttons at the bottom.

An error dialog box titled 'Message from webpage' with a warning triangle icon. The text reads: 'LSC Only MAP Authentication could not be enabled without enabling LSC Provisioning'. There is an 'OK' button at the bottom.

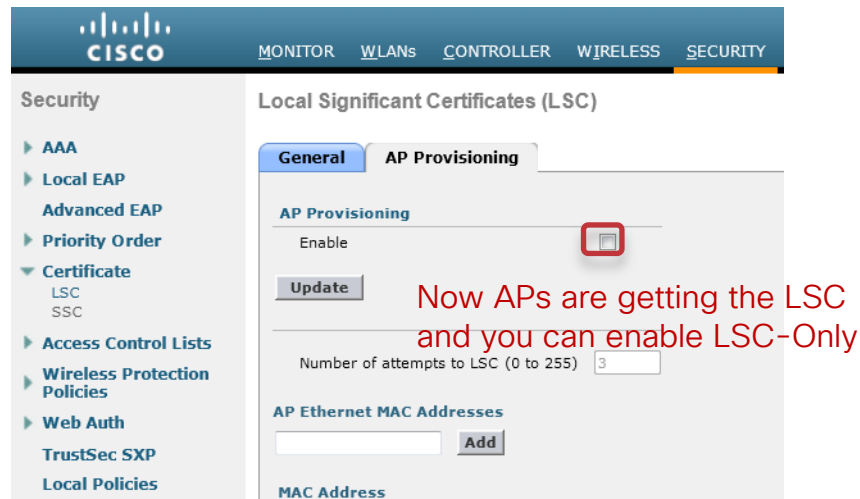
Uh oh, you forgot something

Mesh AP – Joining Without MAC Filter

- Configuration: First, connect your MAPs over Ethernet (no over-the-air provisioning)
- You must also enable LSC provisioning:



The screenshot shows the Cisco configuration interface for Local Significant Certificates (LSC). The 'AP Provisioning' tab is selected, and the 'Enable LSC on Controller' checkbox is checked and highlighted with a red box. The 'Certificate Type' is set to 'CA' and the 'Status' is 'Not Present'. The 'CA Server' section shows the 'CA server URL' as 'https://172.31.255.34/ca'.



The screenshot shows the Cisco configuration interface for Local Significant Certificates (LSC). The 'AP Provisioning' tab is selected, and the 'AP Provisioning' checkbox is checked and highlighted with a red box. The 'Update' button is visible. The 'Number of attempts to LSC (0 to 255)' is set to 3. The 'AP Ethernet MAC Addresses' section has an 'Add' button. A red text annotation reads: 'Now APs are getting the LSC and you can enable LSC-Only'.

Mesh No MAC Authentication

- Configuration:

```
(8500-1) >config mesh security ?
```

```
eap          Enable mesh security EAP for Mesh AP.
```

```
psk          Enable mesh security PSK for Mesh AP.
```

```
rad-mac-filter Configure Mesh security radius mac-filter for Mesh AP.
```

```
lsc-only-auth Configure Mesh security to LSC only MAP Authentication.
```

```
force-ext-auth Configure Mesh security to force external authentication.
```

<-Here is the added option in CLI

Similarly, in CLI you will receive similar warnings if applicable:

```
(8500-1) >config mesh security lsc-only-auth enable
```

```
Warning: Enabling LSC Only MAP Authentication will not provision LSC Certificate into MAP over the air. Please make sure MAP is connected to WLC using Ethernet cable to provision LSC.
```

```
Are you sure you want to continue? (y/N)y
```

```
Enable LSC provisioning before disabling MAC Filter
```



15.3 (8.0) Autonomous Release

Jerome Henry
Technical Marketing Engineer
Enterprise Networking Market Strategy

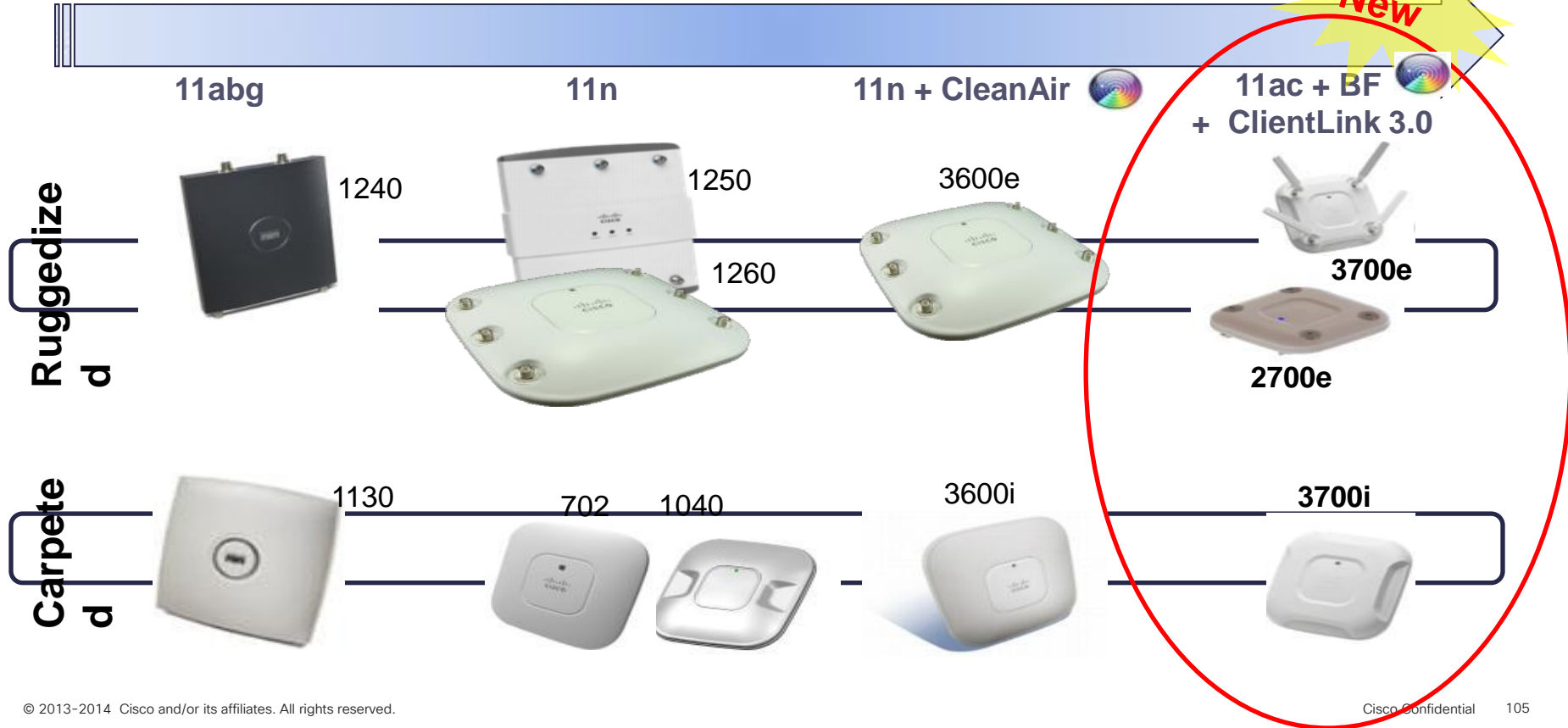
August 2014

What is New in 8.0 aIOS

- AP 3700 & AP 2700 Support
- L2TPv3
- Autoconfig

AP 3700 & AP 2700

aIOS Support for New APs 3700 & 2700



L2TPv3 Over UDP/IP

L2TPv3

- L2TPv3 is a tunneling protocol that enables tunneling of Layer 2 packets over IP core networks
- Secures (encrypts) the wired part of the traffic between the AP and a VPN gateway
 - If you do not implement L2TPv3, anyone can read your client traffic on the wired side, even if traffic is encrypted on the wireless side (encryption stops at the AP)
- L2TPv3 tunnel is a control connection between the end points
- One L2TPv3 tunnel can have multiple data connections
 - Each data connection is termed an L2TPv3 “session”
- The control connection is used to establish, maintain, and release sessions. Each session is identified by a unique session ID.

Configuring L2TP

- Prep work:
 - IP routing has to be enabled before configuring L2TP-class
 - IP CEF has to be enabled
 - Sub-interfaces for VLANs have to be created on the AP
- High-level configuration process:
 1. Define the L2TP-class
 2. Define the pseudo-wire class
 3. Create the VDT and VDT-MNGT interfaces
 4. Map SSID to the tunnel/x-connect
 5. Verify the tunnel is established by using the show commands
 6. Verify the tunnel has an IP address

Using L2TP Show & Debug Commands

How to check counters/statistics:

Ex: 1600-89-time#**show l2tp tunnel packets**

```
L2TP Tunnel Information Total tunnels 1 sessions 1
```

```
LocTunID Pkts-In Pkts-Out Bytes-In Bytes-Out  
517656642 184348 16189 37070708 1056041
```

1600-89-time#

1600-89-time#show l2tp tunnel all

```
L2TP Tunnel Information Total tunnels 1 sessions 1
```

```
Tunnel id 517656642 is up, remote id is 1027082052, 1 active  
sessions
```

```
Locally initiated tunnel
```

```
Tunnel state is established, time since change 01:07:42
```

```
Tunnel transport is UDP (17)
```

```
Remote tunnel name is debian
```

```
Internet Address 99.99.99.10, port 60236
```

```
Local tunnel name is 1600-89
```

```
Internet Address 192.168.29.151, port 1701
```

```
L2TP class for tunnel is l2tp-jag
```

```
Counters, taking last clear into account:
```

```
16194 packets sent, 184532 received
```

```
1056431 bytes sent, 37085867 received
```

```
<Truncated>
```

Debug commands:

- **How to check control channel exchanges**

```
debug l2tp packet error
```

```
debug l2tp packet event
```

- **How to debug data packets via tunnel**

```
debug vpdn packet errors
```

```
debug vpdn packet
```

Defining the L2TP-Class

Define the L2TP- class parameters at the config mode. This mode allows to set the L2TPv3 hello interval, hostname, Cookie length, enabling digest, retransmit and retries for the L2TPv3 control packets.

```
l2tp-class l2tp-jag
  digest secret 7 030752180500
  hello 100
  hostname 1600-89
  retransmit retries 5
  retransmit timeout max 5
  retransmit initial retries 3
  retransmit initial timeout max 6
  retransmit initial timeout min 3
```

Defining Pseudo-Wire Class

Now define the Pseudo-wire class name and configure the parameters. The command “*encapsulation l2tpv3*” has to be entered for other CLIs to be enabled in the pseudowire class section.

The L2TP-class created earlier has to be mapped under the pseudo-wire class created here. L2TPv3IETF is specified for interop with thirdparty L2TPv3 peers.

pseudowire-class pw-jag

encapsulation l2tpv3

protocol l2tpv3ietf l2tp-jag

ip protocol udp

ip local interface BVI1

Used to specify the protocol to be used by L2TPv3.

Default protocol is IP.

Other parameters like Data Sequencing, DF bit , PMTU, TTL, TOS for tunnel can also be configured here.


Creating VDT and VDT-MGMT Interfaces

VDT – Virtual Dot11 Tunnel interface

This interface is used to configure the xconnect to the remote LNS and also map the previously configured Pseudowire-class to it.

```
interface VDT0
no ip address
xconnect 99.99.99.10 1 pw-class pw-jag
End
```

This → the LNS/NMD IP address



VDT-MGMT – Tunnel interface which gets IP address through the tunnel.

Once into the VDT-Mgmt interface below command has to be entered.

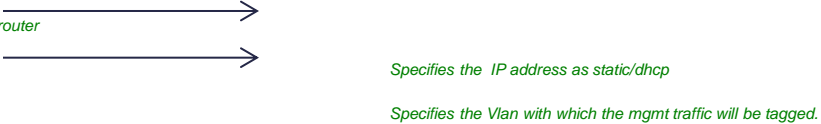
```
"no ip dhcp client request router"
```

Otherwise there will be 2 default routes installed leading to data traffic drop completely.

```
interface VDT-Mgmt0
no ip dhcp client request router
ip address dhcp
vdt-mgmt vlan 10
End
```

Specifies the IP address as static/dhcp

Specifies the Vlan with which the mgmt traffic will be tagged.



Mapping SSID to the Tunnel/Xconnect

Mapping tunnel to the WLAN is done by adding xconnect under the ssid configuration.

```
dot11 ssid test-l2tp →
```

```
  vlan 11
```

```
  xconnect 0           Under SSID xconnect has to be configured.
```

```
  authentication open
```

```
  authentication key-management wpa version 2
```

```
  guest-mode
```

```
  wpa-psk ascii 7 101F5B4A5142445C545D7A
```

```
!
```

```
dot11 ssid test-l2tp1
```

```
  vlan 10
```

```
  xconnect 0
```

```
  authentication open eap eap_methods
```

```
  authentication network-eap eap_methods
```

```
  authentication key-management wpa version 2
```

Show Commands to Check Tunnel

Show command to verify the tunnel is established

```
1600-89-time#sh l2tun
```

```
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
```

```
LocTunID  RemTunID  Remote Name  State  Remote Address  Sessn  L2TP Class/  
Count VPDN Group  
517656642 1027082052  debian      est   99.99.99.10   1   l2tp-jag
```

```
LocID   RemID   TunID   Username, Intf/   State  Last Chg  Uniq ID  
Vcid, Circuit  
2092093504 1418290271 517656642 1, VD0          est   00:58:08 1
```

```
1600-89-time#
```

Show Commands to Check Tunnel Interface IP

Show command to verify the tunnel interface has IP address

```
1600-89-time#sh ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
BVI1	192.168.29.151	YES	DHCP	up	up
Dot11Radio0	unassigned	YES	unset	up	up
Dot11Radio0.1	unassigned	YES	unset	up	up
Dot11Radio0.10	unassigned	YES	unset	up	up
Dot11Radio0.11	unassigned	YES	unset	up	up
Dot11Radio1	unassigned	YES	unset	up	up
Dot11Radio1.1	unassigned	YES	unset	up	up
Dot11Radio1.10	unassigned	YES	unset	up	up
Dot11Radio1.11	unassigned	YES	unset	up	up
GigabitEthernet0	unassigned	YES	unset	up	up
GigabitEthernet0.1	unassigned	YES	unset	up	up
GigabitEthernet0.10	unassigned	YES	unset	up	up
GigabitEthernet0.11	unassigned	YES	unset	up	up
VDT0	unassigned	YES	unset	up	up
VDT-Mgmt0	30.30.10.13	YES	DHCP	up	up

© 2013-2014 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Show Command for Counters/Statistics

```
1600-89-time#show l2tp tunnel packets
```

```
L2TP Tunnel Information Total tunnels 1 sessions 1
```

LocTunID	Pkts-In	Pkts-Out	Bytes-In	Bytes-Out
517656642	184348	16189	37070708	1056041

```
1600-89-time#
```

Show Command for Counter/Statistics

```
1600-89-time#show l2tp tunnel packets
```

```
L2TP Tunnel Information Total tunnels 1 sessions 1
```

```
LocTunID  Pkts-In  Pkts-Out  Bytes-In  Bytes-Out
517656642 184348   16189     37070708 1056041
1600-89-time#show l2tp tunnel all
```

```
L2TP Tunnel Information Total tunnels 1 sessions 1
```

```
Tunnel id 517656642 is up, remote id is 1027082052, 1 active sessions
```

```
  Locally initiated tunnel
```

```
  Tunnel state is established, time since change 01:07:42
```

```
  Tunnel transport is UDP (17)
```

```
  Remote tunnel name is debian
```

```
    Internet Address 99.99.99.10, port 60236
```

```
  Local tunnel name is 1600-89
```

```
    Internet Address 192.168.29.151, port 1701
```

```
  L2TP class for tunnel is l2tp-jag
```

```
  Counters, taking last clear into account:
```

```
    16194 packets sent, 184532 received
```

```
    1056431 bytes sent, 37085867 received
```

```
<Truncated>
```

Debug Commands

Debug commands to be used to check control channel exchanges:

debug l2tp packet error

debug l2tp packet event

Debug commands to be used to debug data packets via tunnel:

debug vpdn packet errors

debug vpdn packet

Not Supported

- Tunnel establishment using IPv6 address
- SNMP and GUI support for this L2TPv3 feature
- Multiple tunnels to same LNS
- Configuring xconnect on physical interfaces (Gig/Dot11) is not supported

Autoconfig

What is Autoconfig?

- When enabled, the Autoconfig feature allows an AP to download its configuration file periodically from an SCP server
- The download is at a pre-determined time, and once downloaded and applied on the AP, it schedules the next configuration download
- The username, password, server-name, and configuration filename are preconfigured on the AP

Enabling Autoconfig, Cont.

Autoconfig can be enabled on an AP by providing the following commands in a boot file as part of the DHCP ip configuration.

Example boot file

```
dot11 autoconfig add env var AUTO_CONFIG_AP_FUNCTIONALITY val YES
dot11 autoconfig add env var AUTO_CONFIG_USER val someuser
dot11 autoconfig add env var AUTO_CONFIG_PASSWD val someonespasswd
dot11 autoconfig add env var AUTO_CONFIG_SERVER val scp.someserver.com
dot11 autoconfig add env var AUTO_CONFIG_INF_FILE val some_inf_file.xml
ntp server 208.210.12.199
clock timezone IST 5 30
dot11 autoconfig download retry interval min 100 max 400
end
```

Configuration File

Autoconfig-enabled AP downloads an information file from SCP server. The information file has the following contents.

- An absolute time and a range value: AP schedules next information file download at this absolute time plus a random value between 0 to range value.
- New startup-configuration

Information File Format

The information file is an XML file and has the following format.

```
<?xml version=" 1.0" encoding=" UTF-8" ?>
<l2tp_cfg>
  <cfg_fetch_start_time><Absolute Time></cfg_fetch_start_time>
  <cfg_fetch_time_range><Random Jitter></cfg_fetch_time_range>
  <cfg_fetch_config>
    <![CDATA[
      <Startup config>
    ]]>
  </cfg_fetch_config>
</l2tp_cfg>
```

Tags Explained

- `cfg_fetch_start_time`: This tag contains an absolute time in the following format.

DAY HH:MM

Here *DAY* must be any of following.

{Sun, Mon, Tue, Wed, Thu, Fri, Sat, All},

HH must be a number from 0 to 23.

MM must be a number from 0 to 59.

Example: "SUN 10:30", "Thu 00:00", "ALL 12:40"

- `cfg_fetch_time_range`: A random number of seconds between 0 to this value is added to the start time to randomize the time when the next information file is downloaded.
- `cfg_fetch_config`: This tag contains the AP's next startup configuration.

Tags Explained, Cont.

- `cfg_fetch_config`: This tag contains AP's next startup configuration

Time Configurations

For the AP to be able to schedule the information file download from the configuration server, the AP clock time must be in sync with a time server. To achieve this, the following must be configured.

An sntp client:

```
sntp server <sntp server ip>
```

For the AP to have the correct time, the correct time zone must be configured as follows:

```
clock timezone <TIMEZONE> <HH> <MM>
```

TIMEZONE is name of time zone like IST, UTC (it could be just any string)

HH is Hours offset from UTC

MM Minutes offset from UTC

Time Configurations, Cont.

For AP to have correct time, correct time zone must be configured as follows

```
clock timezone <TIMEZONE> <HH> <MM>
```

In above configuration -

TIMEZONE is name of timezone like IST, UTC (it could be just any string)

HH is Hours offset from UTC

MM Minutes offset from UTC

Autoconfig Retry Interval

If information file download from SCP server fails, AP tries to download it again after a configured retry interval.

It can be configured as follows:

```
dot11 autoconfig download retry interval min <MIN> max <MAX>
```

MIN is minimum number of seconds between retries

MAX is maximum number of seconds between retries

After every failed download, retry interval doubles, until it becomes larger than *MAX*.

Show Command to Check Autoconfig Status

```
AP1600-ATT#show dot11 autoconfig status
```

```
Dot11 I2tp auto config is disabled
```

```
1600-89-absim#show dot11 autoconfig status
```

```
Auto configuration download will occur after
```

```
45 seconds
```

```
1600-89-absim#show dot11 autoconfig status
```

```
Trying to download information file from server
```

Debug Commands

Debug commands to see autoconfig event and state machine transition.

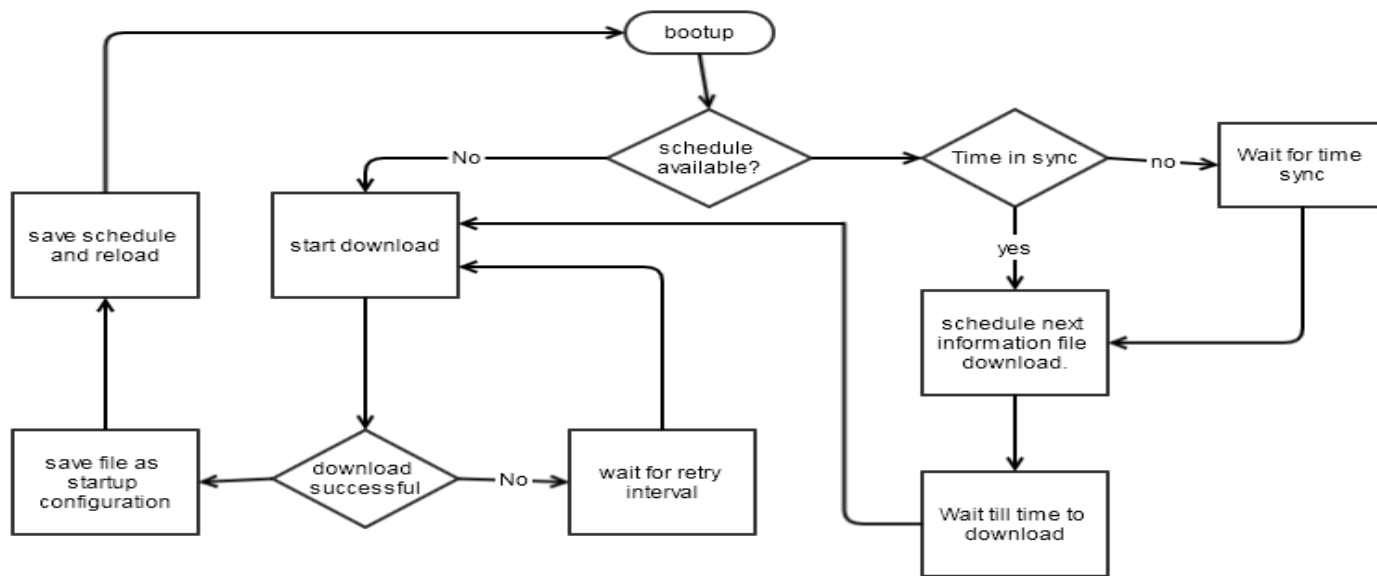
Deb dot11 autoconfigsm

Deb dot11 autoconfigev

Summary of Changes

- AP does not apply a configuration if it is the same as the last downloaded configuration
- A retransmit interval can be configured
- Time to download can be absolute
- A day of week can be chosen on which information file is downloaded

Autoconfig Flow



Thank you.

