Architecting Network for Branch Offices with Cisco Unified Wireless

BRKEWN-2016

Karan Sheth - Sr. Technical Marketing Engineer
Objective

Design & Deploy Branch Network That Increases Business Resiliency
Agenda

- Learn Cisco Unified Wireless LAN Principles *(Reminder)*
- Understand Wireless Branch Deployment Options
- Evaluate FlexConnect Architectural Requirements
- Identify the need for FlexConnect & AP Groups
- Design a Resilient Branch Network
- Design Secure & BYOD enabled Branch Network
- How to operate Wireless Branch efficiently over WAN
- FlexConnect Resiliency DEMO
Cisco Unified Wireless LAN Principles
Cisco One Network: Wireless Deployment Modes

One Policy, One Management, One Network

Unified Access Wireless

- Autonomous
- FlexConnect
- Centralized
- Converged Access

Unparalleled Deployment Flexibility
Cisco Unified Wireless Principles

- Components
  - Wireless LAN Controllers
  - Aironet Access Points
  - Management (Prime Infrastructure)
  - Mobility Services Engine (MSE)

- Principles
  - AP must have CAPWAP connectivity with WLC
  - Configuration downloaded to AP by WLC
  - All Wi-Fi traffic is forwarded to the WLC
Wireless Branch Deployment Options
Branch Office with Local WLAN Controller

Overview

- Branches can also have local remote controllers
- Small or Mid-size Branch WLCs
  - CT-2504,
  - Integrated controller modules in ISR/ISR-G2
  - Converged Access Cat-3850
- High-availability design with central backup controller is supported; WAN limitations may apply
Branch Office with Local WLAN Controller

Advantages

- Cookie cutter configuration for every branch site
- Layer-3 roaming within the branch
- WGB support
- Reliable Multicast (filtering)
- IPv6 L3 Mobility

**Note:** If you have ISR/ISR G2 at branch site then it is recommended to use the IOS Firewall at edge for unified access policies.
Branch Office Deployment

**FlexConnect (HREAP)**

- Hybrid architecture
- Single management and control point
- Data Traffic Switching
  - Centralized traffic (split MAC)
  - or
  - Local traffic (local MAC)
- HA will preserve local traffic only
- Traffic Switching is configured per AP and per WLAN (SSID)
FlexConnect Glossary

- **Connected Mode** – When FlexConnect can reach Controller (connected state), it gets help from controller to complete client authentication.

- **Standalone mode** – When controller is not reachable by FlexConnect, it goes into standalone state and does client authentication by itself.

- **Local Switching** – Data traffic switched onto local VLANs for an SSID

- **Central Switching** – Data traffic tunneled back to WLC for an SSID
Configure FlexConnect Mode

Step 1: Configure Access Point Mode

- Enable FlexConnect mode per AP
- Supported AP: AP-1130, AP-1240, AP-1040, AP-1140, AP-1260, AP-1250, AP-3500, AP-1600, AP-2600, AP-3600
Configure FlexConnect Local Switching

Step 2: Enable Local Switching per WLAN

- Only WLAN with “FlexConnect Local Switching” enabled will allow local switching on the FlexConnect AP
Configure FlexConnect VLAN Mapping

Step 3: FlexConnect Specific Configuration

- FlexConnect AP can be connected on an access port or connected to a 802.1Q trunk port (using the native VLAN)
- VLAN mapping can be performed per AP configuration on WLC and/or by AP groups using Cisco Prime Infrastructure templates
Configure FlexConnect VLAN Mapping

Step 4: FlexConnect Specific Configuration – Native VLAN

- When connecting with Native VLAN on AP, L2 switchport must also match with corresponding Native VLAN configuration.
- Each corresponding SSID that is allowed to be locally switch should be allowed on the corresponding switchport.

```plaintext
interface GigabitEthernet0/1
switchport access vlan 52
switchport trunk encapsulation dot1q
switchport trunk native vlan 52
switchport trunk allowed vlan 52,154,155
switchport mode trunk
spanning-tree portfast
```
Configure FlexConnect SSID-VLAN Mapping

Step 5: Per AP SSID to VLAN Mapping

- Mapping of SSID to 802.1Q VLAN is done per FlexConnect AP

- Or use Cisco Prime Infrastructure (NCS) via configuration templates
Configure FlexConnect VLAN Mapping

Using Cisco Prime Infrastructure

- Prime Infrastructure provides simplified configuration to all FlexConnect APs with one Lightweight AP Template
Evaluate FlexConnect Architectural Requirements
FlexConnect Design Considerations

WAN Limitations Apply

<table>
<thead>
<tr>
<th>Deployment Type</th>
<th>WAN Bandwidth (Min)</th>
<th>WAN RTT Latency (Max)</th>
<th>Max APs per Branch</th>
<th>Max Clients per Branch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>64 kbps</td>
<td>300 ms</td>
<td>5</td>
<td>25</td>
</tr>
<tr>
<td>Data</td>
<td>640 kbps</td>
<td>300 ms</td>
<td>50</td>
<td>1000</td>
</tr>
<tr>
<td>Data</td>
<td>1.44 Mbps</td>
<td>1 sec</td>
<td>50</td>
<td>1000</td>
</tr>
<tr>
<td>Data+Voice</td>
<td>128 kbps</td>
<td>100 ms</td>
<td>5</td>
<td>25</td>
</tr>
<tr>
<td>Data+Voice</td>
<td>1.44 Mbps</td>
<td>100 ms</td>
<td>50</td>
<td>1000</td>
</tr>
<tr>
<td>Monitor</td>
<td>64 kbps</td>
<td>2 sec</td>
<td>5</td>
<td>N/A</td>
</tr>
<tr>
<td>Monitor</td>
<td>640 kbps</td>
<td>2 sec</td>
<td>50</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Feature Limitations Apply

- Some features are not available in standalone mode or in local switching mode
  - MAC/Web Auth in Standalone Mode
  - VideoStream
  - IPv6 L3 Mobility
  - SXP TrustSec
  - See full list in « FlexConnect Feature Matrix »

Economies of Scale For Lean Branches

Flex 7500 Wireless Controller

Key Differentiation

- **WAN Tolerance**
  - High Latency Networks
  - WAN Survivability

- **Security**
  802.1x based port authentication

- **Voice support**
  - Voice CAC
  - OKC/CCKM

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Points</td>
<td>300-6,000</td>
</tr>
<tr>
<td>Clients</td>
<td>64,000</td>
</tr>
<tr>
<td>Branches</td>
<td>2000</td>
</tr>
<tr>
<td>Access Points / Branch</td>
<td>100</td>
</tr>
<tr>
<td>Deployment Model</td>
<td>FlexConnect</td>
</tr>
<tr>
<td>Form Factor</td>
<td>1 RU</td>
</tr>
<tr>
<td>IO Interface</td>
<td>2 x 10GE</td>
</tr>
<tr>
<td>Upgrade Licenses</td>
<td>100, 200, 500, 1K RTU Licenses</td>
</tr>
</tbody>
</table>
### Flex 7500 Scale & Feature Update - 7.0.116.0 vs. 7.4

<table>
<thead>
<tr>
<th>Scalability</th>
<th>7.0.116.0</th>
<th>7.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total APs</td>
<td>2000</td>
<td>6000</td>
</tr>
<tr>
<td>Total Clients</td>
<td>20,000</td>
<td>64,000</td>
</tr>
<tr>
<td>Total FlexConnect Group</td>
<td>500</td>
<td>2000</td>
</tr>
<tr>
<td>Support for OEAPs</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Central Switching BW Limit</td>
<td>~250 Mb</td>
<td>~1 Gb</td>
</tr>
<tr>
<td>Data DTLS Support</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Central Switching 802.1x</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
# FlexConnect Feature Introduction

<table>
<thead>
<tr>
<th>FlexConnect Features</th>
<th>Release Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA-VLAN Override, ALCs &amp; P2P Blocking</td>
<td>7.2</td>
</tr>
<tr>
<td>Smart AP Image Upgrade</td>
<td>7.2</td>
</tr>
<tr>
<td>External Web-Auth &amp; Mobile Device On-boarding</td>
<td>7.2</td>
</tr>
<tr>
<td>Flex 7500 Scale Update</td>
<td>7.3</td>
</tr>
<tr>
<td>VLAN Based Central Switching</td>
<td>7.3</td>
</tr>
<tr>
<td>Split-tunneling</td>
<td>7.3</td>
</tr>
<tr>
<td>Work Group Bridge (WGB) Support</td>
<td>7.3</td>
</tr>
<tr>
<td>Bi-Directional Rate Limiting</td>
<td>7.4</td>
</tr>
<tr>
<td>ISE BYOD Registration &amp; Provisioning</td>
<td>7.4</td>
</tr>
<tr>
<td>AAA-ACL &amp; AAA-QoS Override</td>
<td>7.5</td>
</tr>
<tr>
<td>EAP-TLS &amp; PEAP Support for Local Authentication</td>
<td>7.5</td>
</tr>
</tbody>
</table>
Why do we need FlexConnect & AP Groups?
Understanding AP Groups

Overview

- AP Groups is a logical concept of grouping AP’s which deliver similar Wi-Fi services; these services can be:
  - By physical location, and/or
  - By functional services (data, voice, guest, …)

- Same AP groups need to be defined in all WLC’s of a mobility group

<table>
<thead>
<tr>
<th>Scaling</th>
<th>Flex 7500</th>
<th>CT-5508</th>
<th>WiSM-2</th>
<th>CT-2504</th>
</tr>
</thead>
<tbody>
<tr>
<td># AP Groups</td>
<td>6000</td>
<td>500</td>
<td>1000</td>
<td>50</td>
</tr>
<tr>
<td># WLAN (SSID)</td>
<td>512</td>
<td>512</td>
<td>512</td>
<td>16</td>
</tr>
<tr>
<td># VLAN (Interfaces)</td>
<td>4095</td>
<td>512</td>
<td>512</td>
<td>16</td>
</tr>
</tbody>
</table>
AP Groups
Configuration: Create a New Group

Add New AP Group
- AP Group Name: AP-Group-1
- Description: AP Group for Site 1

Add Cancel
AP Groups Usage
Per Location SSID

- AP groups give the ability to enable Wi-Fi Services (WLAN) based on physical location

- Example
  - Central Site
    - Corporate-Voice, Corporate-Data, Guest-Access
  - Manufacturing Site
    - Corporate-Voice, Corporate-Data, Scanners
  - Store
    - Corporate-Data, Guest-Access
AP Groups Usage
Per AP Group SSID to VLAN Mapping

- AP groups give the ability to statically map Wi-Fi service (WLAN) to VLAN based on physical location.
- Users see the same Wi-Fi service on all sites.
- Admin can monitor and filter based on different IP@ each site.
- Can also be used to have smaller Wi-Fi subnets
  - For example per floor subnets in a building.
Ap Groups
Configuration/VLAN Mapping

Ap Groups > Edit 'AP-Group-1'

Add New

WLAN SSID
Interface /Interface Group(G)
SNMP NAC State

Add Cancel

Ap Groups > Edit 'AP-Group-1'

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>WLAN SSID</th>
<th>Interface /Interface Group(G)</th>
<th>SNMP NA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RackMobility</td>
<td>partenaires</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Understanding FlexConnect Groups

Overview

- FlexConnect groups allow sharing of:
  - CCKM/OKC fast roaming keys
  - Local/backup RADIUS servers IP/keys
  - Local user authentication
  - Local EAP authentication
  - AAA-Override for Local Switching
  - Smart Image Upgrade

- Scaling information

<table>
<thead>
<tr>
<th>Scaling</th>
<th>Flex 7500</th>
<th>CT-5508</th>
<th>WISM2</th>
<th>CT-2504</th>
</tr>
</thead>
<tbody>
<tr>
<td>FlexConnect Groups</td>
<td>2000</td>
<td>100</td>
<td>100</td>
<td>30</td>
</tr>
<tr>
<td>AP per Group</td>
<td>100</td>
<td>25</td>
<td>25</td>
<td>25</td>
</tr>
</tbody>
</table>
FlexConnect Groups and CCKM/OKC Keys

- CCKM/OKC keys are stored on FlexConnect APs for Layer 2 fast roaming
- The FlexConnect APs will receive the CCKM/OKC keys from the WLC
- If a FlexConnect AP boots up in standalone mode, it will not get the OKC/CCKM keys from the WLC and fast roaming will not be supported
- FlexConnect supports 802.11r Fast Transition with local key caching.
**Step 1:** Add a New FlexConnect Group

**Step 2:** Add APs to the FlexConnect Group
Designing a Resilient Wireless Branch Network
FlexConnect Backup Scenario
WAN Failure

- FlexConnect will backup on local switched mode
  - No impact for locally switched SSIDs
  - Disconnection of centrally switched SSIDs clients
- Static authentication keys are locally stored in FlexConnect AP
- Lost features
  - RRM, WIDS, location, other AP modes
  - Web authentication, NAC
FlexConnect Backup Scenario - WLC Failure

- FlexConnect will first backup on local switched mode
  - No impact for locally switched SSIDs
  - Disconnection of centrally switched SSIDs clients
- CCKM roaming allowed in FlexConnect group
- FlexConnect AP will then search for backup WLC; when backup WLC is found, FlexConnect AP will resync with WLC and resume client sessions with central traffic.
- Client sessions with Local Traffic are not impacted during resync with Backup WLC.
FlexConnect Group: Local Backup RADIUS

- Normal authentication is done centrally
- On WAN failure, AP authenticates new clients with locally defined RADIUS server
- Existing connected clients stay connected
- Clients can roam with
  - CCKM fast roaming, or
  - Reauthentication
- Define primary and secondary local backup RADIUS server per FlexConnect group
Local Authentication

- By default FlexConnect AP authenticates clients through central controller
- Local Authentication allow use of local RADIUS server directly from the FlexConnect AP
Local Authentication Configuration

FlexConnect Group: Local Backup Authentication

- Normal authentication is done centrally
- On WAN failure, AP authenticates new clients with its local database
- Each FlexConnect AP has a copy of the local user DB
- Existing authenticated clients stay connected
- Clients can roam with:
  - CCKM fast roaming, or
  - Local re-authentication

<table>
<thead>
<tr>
<th>Supported Security Types</th>
<th>Release Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEAP</td>
<td>6.0</td>
</tr>
<tr>
<td>EAP-FAST</td>
<td>6.0</td>
</tr>
<tr>
<td>PEAP</td>
<td>7.5</td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>7.5</td>
</tr>
</tbody>
</table>
FlexConnect Group: Local Backup Authentication Configuration

- Define users (max 100) and passwords
- Select supported Security protocols i.e. LEAP, EAP-FAST, PEAP or EAP-TLS

1. Define users (max 100) and passwords
2. Select supported Security protocols i.e. LEAP, EAP-FAST, PEAP or EAP-TLS
Designing Secure & BYOD Enabled Branch Network
FlexConnect Peer-to-peer Blocking
Local Switching Peer-to-peer Blocking

- Support for Peer-to-Peer blocking in FlexConnect AP
- Apply for clients on same FlexConnect AP
- P2P blocking modes: disable or drop
- For P2P blocking inter-AP use ACL or Private VLAN function
Both modes of operation will drop the packet @ AP for Local Switching enabled WLAN

* Central Switching WLAN will support “Forward - UpStream” and will send the packet to the next upstream node connected to WLC
FlexConnect AAA VLAN & QoS Override
FlexConnect AAA VLAN Override

Description

- AAA VLAN Override with local or central authentication
- Up to 16 VLANs per FlexConnect AP
- VLAN ID must be enabled per AP or FlexConnect Group
- If VLAN ID does not exist, default VLAN is used, unless « VLAN Based Central Switching » enabled
- **Starting from 7.5** AAA override for QoS is also supported.
FlexConnect AAA VLAN Override Configuration

IETF 65
Tunnel-Medium-Type
Tagged Enum
[T:1] 802

IETF 64
Tunnel-Type
Tagged Enum
[T:1] VLAN

IETF 81
Tunnel-Private-Group-ID
Tagged String
[T:1] 3

WLANs > Edit "FlexDemo"

FlexConnect Groups > Edit "SanJose"

Create Sub-Interface on FlexConnect AP

interface GigabitEthernet1/0/4
description AP-3600-1
switchport trunk encapsulation dot1q
switchport trunk native vlan 109
switchport trunk allowed vlan 3,109
switchport mode trunk
VLAN Based Central Switching

Overview

- While doing AAA VLAN Override with local switching:
- If VLAN ID does not exist at the AP, the traffic is central switched to the central VLAN ID
- If the central VLAN ID does not exist, the traffic is centrally switched to the default VLAN ID of the WLAN
FlexConnect ACL VLAN Mapping & AAA-Override
FlexConnect ACL – VLAN Mapping

Overview

- FlexConnect ACL are applied per VLAN
- FlexConnect ACL are Ingress / Egress oriented
- **Starting from 7.5** FlexConnect ACLs support AAA override

Scale

512 FlexConnect ACL per WLC
- 16 ingress ACL & 16 egress ACL per AP
- 64 ACL rules per ACL
- No IPv6 ACL
FlexConnect Access Lists

- FlexConnect ACL rule creation is similar to rule creation for Local Mode AP
FlexConnect ACL – VLAN Mapping

Configuration – FlexConnect ACL per AP

- FlexConnect ACL can be applied per AP using VLAN Mappings configuration
- FlexConnect ACL can be applied per FlexConnect Groups per VLAN in the ACL Mapping tab.
FlexConnect Split Tunneling
(Using FlexConnect Split ACL)
- Split tunneling allow some traffic to be locally switched although the WLAN is defined as centrally switched
- Split tunneling is using a NAT/PAT feature with ACL to perform the local switching
- Split tunneling is using the AP IP@ for the NAT/PAT feature
FlexConnect ACL – Split Tunneling Configuration

- Create a centrally switched WLAN
  - Flex Local switching should not be checked

- Define Flex ACL to match traffic to be locally switched
  - Central subnet
  - Local subnet
FlexConnect ACL – Split Tunneling
Configuration – Per Access Point

All APs > Details for AP-3600-A

- VLAN Support: ON
- Native VLAN ID: 52
- FlexConnect Group Name: FlexConnect-Site-1

PreAuthentication Access Control Lists
- External WebAuthentication ACLs
- Local Split ACL
- Central DHCP Processing

All APs > AP-3600-A > ACL Mappings

- AP Name: AP-3600-A

WLAN ACL Mapping
- WLAN Id: 1
- Local-Split ACL: Flex_Split_ACL

WLAN Id | WLAN Profile Name | Local-Split ACL
---------|------------------|------------------
1        | RackMobility     | Flex_Split_ACL   

© 2013 Cisco and/or its affiliates. All rights reserved. Cisco Public
### FlexConnect ACL – Split Tunneling

#### Configuration – Per FlexConnect Group

**FlexConnect Groups > Edit “FlexConnect-Site-1”**

<table>
<thead>
<tr>
<th>General</th>
<th>Local Authentication</th>
<th>Image Upgrade</th>
<th>ACL Mapping</th>
<th>Central DHCP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>AAA VLAN-ACL mapping</td>
<td>WLAN-ACL mapping</td>
</tr>
</tbody>
</table>

#### Web Auth ACL Mapping

<table>
<thead>
<tr>
<th>WLAN Id</th>
<th>WLAN Profile Name</th>
<th>WebAuth ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>FlexConnect-Acl-1</td>
</tr>
</tbody>
</table>

#### Local Split ACL Mapping

<table>
<thead>
<tr>
<th>WLAN Id</th>
<th>WLAN Profile Name</th>
<th>LocalSplit ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RackMobility</td>
<td>Flex_Split_ACL</td>
</tr>
</tbody>
</table>

© 2013 Cisco and/or its affiliates. All rights reserved.
Cisco Public
Deploying External WebAuth with FlexConnect Local Switching

(Using FlexConnect WebAuth ACL)
External WebAuth with Local Switching

Description

- Provides L3 Web Redirect from locally switched vlan
- Reduces WAN traffic by locally switching guest traffic
- Flexible and centralized web portal creation for multiple sites
- Provides flexible use of Conditional and Splash Page Web Redirect
- FlexConnect AP must be in Connected state with Centralized Controller for this functionality to work

Starting from 7.2.110
Step 1: Configure Pre-Auth ACL that will be applied to FlexConnect Group, AP or WLAN

FlexConnect Access Control Lists

Acl Name
- FlexConnect
- Flex AAA Overide ACL
- Pre-WebAuthPolicy-ACL
- WebAuth ACL

Access Control Lists > Edit

General

Access List Name: Pre-WebAuthPolicy-ACL

<table>
<thead>
<tr>
<th>Seq</th>
<th>Action</th>
<th>Source IP/Mask</th>
<th>Destination IP/Mask</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Dest Port</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Permit</td>
<td>0.0.0.0/0</td>
<td>192.168.1.11/24</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.0.0.0/0</td>
<td>255.255.255.255</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>

External Web-Server IP
Step 2: Apply Pre-Auth ACL to WLAN

Apply Pre-Auth ACL to WLAN
Step 3: Apply Pre-Auth ACL to FlexConnect AP

External WebAuth with Local Switching Configuration – Per AP

- Map WLAN-Id to Pre-Auth ACL

---

External WebAuthentication ACLs
- Local Split ACLs
- Central DHCP Processing

PreAuthentification Access Control Lists

WLAN ACL Mapping

<table>
<thead>
<tr>
<th>WLAN Id</th>
<th>WLAN Profile Name</th>
<th>WebAuth ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>WebAuth</td>
<td>Pre-WebAuthPolicy-ACL</td>
</tr>
</tbody>
</table>

WebPolicies

WebPolicy ACL FlexConnect-Acl-1
- Add
External WebAuth with Local Switching
Configuration – Per FlexConnect Group

Or Step 3: Apply Pre-Auth ACL to FlexConnect Group

Map WLAN-Id to Pre-Auth ACL
Step 4: Configure External Web Server

External Web-Server IP
Deploying BYOD with FlexConnect Local Switching
(Using FlexConnect WebPolicies ACL)
BYOD Device On-Boarding in FlexConnect
Example: Apple iOS Device Provisioning

1. Initial Connection Using PEAP
2. Device Provisioning Wizard
3. Future Connections Using EAP-TLS

ISE - CA-Server

Starting from 7.4
FlexConnect Access Lists for BYOD

Create FlexConnect ACL to allow access to Cisco ISE

1. Create FlexConnect ACL
2. Select FlexConnect Access Control Lists
3. Add new rule

Access Control List Name: FlexConnect-ACL

<table>
<thead>
<tr>
<th>Seq</th>
<th>Action</th>
<th>Source IP/Mask</th>
<th>Destination IP/Mask</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Dest Port</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Deny</td>
<td>0.0.0.0 / 255.255.255.255</td>
<td>10.150.5.0 / 255.255.255.255</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>2</td>
<td>Deny</td>
<td>0.0.0.0 / 255.255.255.255</td>
<td>0.0.0.0 / 255.255.255.255</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>3</td>
<td>Permit</td>
<td>0.0.0.0 / 255.255.255.255</td>
<td>0.0.0.0 / 255.255.255.255</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>
FlexConnect Web Policy ACL

Configure Web Policy ACL per FlexConnect AP

- ACL Mapping can be configured per FlexConnect AP

Detailed configuration interface showing VLAN and Access Control List (ACL) settings.
- Use ACL Mapping tab in FlexConnect Group configuration
- WebPolicies ACL are not the same as VLAN ACL or WebAuthentication ACL.
To support DHCP Profiling Probe with FlexConnect, DHCP request must be sent to WLC. This is done by the « Central DHCP Processing » configuration.
Deploying BYOD with FlexConnect Wireless
Summary – 802.1x/EAP Authentication

FlexConnect AP

CAPWAP

WLC

ISE

DHCP Server

Web Server

Unknown Device, Redirect to registration

Web Traffic

WiFi Association

802.1x/EAP Request

Inside CAPWAP

Radius Access-Request

Radius Access-Response

- Access-Type: Access-Accept
- URL-Redirect-ACL=FlexACLWebPolicy
- URL-Redirect=http://……)

URL + ACL Redirect

Inside CAPWAP

802.1x/EAP Response

Inside CAPWAP
Deploying BYOD with FlexConnect Wireless

Summary – DHCP Request

- DHCP Request
- RADIUS-Accounting
  - host-name=MyiPad
  - dhcp-class-identifier=APPLE
- DHCP Lease
  - Inside CAPWAP
- Device is an Apple iPad

Web Traffic
- FlexConnect AP
- CAPWAP
- WLC
- ISE
- DHCP Server
- Web Server

Inside CAPWAP
Deploying BYOD with FlexConnect Wireless

Summary – URL-Redirect

HTTP Request Redirected to WLC by AP

Inside CAPWAP

URL-Redirect

© 2013 Cisco and/or its affiliates. All rights reserved. Cisco Public
Deploying BYOD with FlexConnect Wireless
Summary – Registration & Provisioning

Device Registration & Provisioning

- EAP Authentication
- RADIUS Change-of-Authorization

EAP DeAuthentication

ISE

DHCP Server

Web Server

Device is Registered

Trigger Change-of-Auth
Deploying BYOD with FlexConnect Wireless

Summary – Device Access

Device is Registered And Provisioned

Allow Access

DHCP Request/Response

Inside CAPWAP

802.1x/EAP Request/Response

Inside CAPWAP

Radius Access-Request

Radius Access-Response

802.1x Authentication

RADIUS Accept

Web Traffic
Operating Wireless Branch
Smart Upgrade over WAN
Upgrading a FlexConnect Deployment

Concerns

- Sites using FlexConnect AP are usually sites with low WAN bandwidth
- Each site may have small number of AP, but an enterprise may have a lot of branches
- Upgrading ~2000 AP through a low bandwidth WAN is a challenge:
  - Time needed to download all the AP firmware
  - Exhaust of the WAN link
  - Risk of failures during the download
Smart AP Image Upgrade use a « master » AP in each FlexConnect Group to download the code.

Other FlexConnect AP download the code from the master locally

1. Download WLC upgraded firmware (will become primary)
2. Force the « boot image » to be the secondary (and not the newly upgraded one) to avoid parallel download of all AP in case of unexpected WLC reboot
3. WLC elect a master AP in each FlexConnect Group (can be also set manually)
4. Master AP « Pre-download » the AP firmware in the secondary « boot image » (will not disrupt the actual service)—Can be started group per group to limit WAN exhaust

5. Slave AP « Pre-download » the AP firmware from the Master AP

6. Change the « boot image » of the WLC to the new image

7. Reboot the controller
FlexConnect Smart AP Image Upgrade Configuration

- "FlexConnect AP Upgrade" checkbox has to be enabled for each FlexConnect Group.
- By default, Master AP for each FlexConnect Group is selected using Lower-MAC algorithm.
- One Master select per AP type.

Enable Efficient AP Image Upgrade
Random Backoff Interval (100-300sec) between each retry
Master AP Selection is Optional

Valid Range is 1-63
FlexConnect Smart AP Image Upgrade
Configuration (Cont)

Per Branch or FlexConnect Group Upgrade

Upgrade across all Branches or FlexConnect Groups whose “FlexConnect AP Upgrade” checkbox is set
FlexConnect Resiliency Demo
FlexConnect Fault-Tolerance Demo

1. Associate Wireless Clients to SSID FlexDemo
2. Confirm AP is reachable from WLC or in FlexConnect Connected mode.
3. Start Ping from Laptop: 10.10.10.20 to iPad: 10.10.10.10
4. Kill the CAPWAP tunnel between AP & WLC i.e. unplug WLC from the Switch.
5. Check the AP switching from Connected to Standalone due to loss of reachability with WLC.
6. Notice the Ping packets are still running.

Fault-Tolerance is Integrated in FlexConnect architecture & requires No Configuration.
Summary
Summary

- Cisco Unified Wireless Network based on Controllers deliver Wireless Branch Solution
- FlexConnect is the feature designed to solve remote connectivity and WAN constraints
- Several Failover Scenario are targeted to offer Survivability of Small Remote Sites
Deploying Cisco’s FlexConnect in Branches Increases Business Resiliency
Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Cisco Daily Challenge points for each session evaluation you complete.
- Complete your session evaluation online now through either the mobile app or internet kiosk stations.

Maximize your Cisco Live experience with your free Cisco Live 365 account. Download session PDFs, view sessions on-demand and participate in live activities throughout the year. Click the Enter Cisco Live 365 button in your Cisco Live portal to log in.

Note: This slide is now a Layout choice