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
Cisco Unified Wireless LAN Principles
Cisco One Network: Wireless Deployment Modes

One Policy, One Management, One Network

Unified Access Wireless

Autonomous | FlexConnect | Centralised | Converged Access

Unparalleled Deployment Flexibility

New
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
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
- 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
  - Centralised 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
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.

```
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
```

<table>
<thead>
<tr>
<th>VLAN Support</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Native VLAN ID</td>
<td>52</td>
<td></td>
</tr>
</tbody>
</table>

FlexConnect Group Name: FlexConnect-Site-1
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
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>
FlexConnect Design Considerations

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>
## FlexConnect Improvements in 7.2 – 7.5

<table>
<thead>
<tr>
<th>7.2</th>
<th>7.3 &amp; 7.4</th>
<th>7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart AP Image Upgrade</td>
<td>Flex 7500 Scale Update</td>
<td>PEAP and EAP-TLS Support</td>
</tr>
<tr>
<td>ACL’s on FlexConnect AP</td>
<td>VLAN Based Central Switching</td>
<td>FlexConnect Group</td>
</tr>
<tr>
<td>AAA Over-ride of VLAN -</td>
<td>Split Tunnelling</td>
<td>specific WLAN-VLAN</td>
</tr>
<tr>
<td>dynamic VLAN assignment for locally switched clients</td>
<td>Central DHCP Processing</td>
<td>mapping</td>
</tr>
<tr>
<td>FlexConnect Re-branding</td>
<td>WGB/uWGB Support with local switching</td>
<td>AAA Client ACL</td>
</tr>
<tr>
<td>Fast Roaming for Voice Clients</td>
<td>Bidirectional Rate Limiting</td>
<td></td>
</tr>
<tr>
<td>Peer to Peer Blocking</td>
<td>Support for ISE BYOD Registration &amp; Provisioning</td>
<td></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 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'

General WLANs RF Profile APs 802.11u

Add New

WLAN SSID: RackMobility
Interface Group(G): partenaires

Ap Groups > Edit 'AP-Group-1'

General WLANs RF Profile APs 802.11u

WLAN ID  WLAN SSID  Interface/Interface Group(G)  SNMP NA
1  RackMobility  partenaires  Disabled

© 2014 Cisco and/or its affiliates. All rights reserved.
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.
FlexConnect Groups Creation

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

Backup Scenario

- 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

WLANs > Edit 'RackMobility'

**General**
- Maximum Allowed Clients: 8
- Static IP Tunneling: 11
- Wi-Fi Direct Clients Policy:
- Maximum Allowed Clients Per AP Radio: 200

**Security**
- 802.11b/g/n (1-255): 1
  - NAC State: None

**QoS**
- Off Channel Scanning Defer
  - Scan Defer Priority: 0, 1, 2, 3, 5, 6, 7
  - Scan Defer Time (msecs): 100

**Advanced**
- FlexConnect Local Switching: 2
- FlexConnect Local Auth: 12
- Learn Client IP Address: 5

FlexConnect
- FlexConnect Local Switching: Enabled
- FlexConnect Local Auth: Enabled
- Learn Client IP Address: Enabled
FlexConnect Group: Local Backup Authentication

Backup Scenario

- 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
Designing Secure & BYOD Enabled Branch Network
FlexConnect Peer-to-peer Blocking
Local Switching Peer-to-peer Blocking

Description

- 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
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

For Your Reference

CREATE SUB-INTERFACE ON FLEXCONNECT AP

WLANs > Edit 'FlexDemo'

General       Security       QoS       Advanced
Allow AAA Override

FlexConnect Groups > Edit 'SanJose'

VLAN ACL Mapping

Vlan Id: 3
Ingress ACL: none
Egress ACL: none
Add

Attribute | Type          | Value         |
----------|---------------|---------------|
IETF 65   | Tunnel-Medium-Type | Tagged Enum   |
IETF 64   | Tunnel-Type     | Tagged Enum   |
IETF 81   | Tunnel-Private-Group-ID | Tagged String |

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 AAA QoS Override

Description

- Dynamically assign QoS levels and/or bandwidth contracts for local switching, centrally authenticated WLANs
- Web-authenticated WLANs and 802.1X-authenticated WLANs supported
- Order of precedence for Rate Limiting parameters
  - AAA override
  - QoS Profile of AAA override
  - Local WLAN configuration
  - QoS Profile of local WLAN configuration

<table>
<thead>
<tr>
<th>Vendor ID/Vendor Type</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>[14179\002]</td>
<td>Aire-QoS-Level</td>
</tr>
<tr>
<td>[14179\004]</td>
<td>Aire-802.1P-Tag</td>
</tr>
<tr>
<td>[14179\007]</td>
<td>Aire-Data-Bandwidth-Average-Contract</td>
</tr>
<tr>
<td>[14179\008]</td>
<td>Aire-Real-Time-Bandwidth-Average-Contract</td>
</tr>
<tr>
<td>[14179\009]</td>
<td>Aire-Data-Bandwidth-Burst-Contract</td>
</tr>
<tr>
<td>[14179\0010]</td>
<td>Aire-Real-Time-Bandwidth-Burst-Contract</td>
</tr>
</tbody>
</table>

Supported on 802.11n non-mesh access points 1040, 1140, 1250, 1260, 1600, 2600, 3500, 3600, 3700
FlexConnect ACL VLAN Mapping & Per-Client ACL
FlexConnect ACL – VLAN Mapping
Overview

- FlexConnects ACL are applied per VLAN
- FlexConnect ACL are Ingress / Egress oriented
- **Starting from 7.5** FlexConnect ACL support AAA-returned Client ACL

Scale

512 FlexConnect ACL per WLC

- 16 ingress ACL & 16 egress ACL per AP
- 64 ACL rules per ACL
- No IPv6 ACL
FlexConnect Split Tunnelling
(Using FlexConnect Split ACL)
FlexConnect ACL – Split Tunnelling

Overview

- Split tunnelling allow some traffic to be locally switched although the WLAN is defined as centrally switched
- Split tunnelling is using a NAT/PAT feature with ACL to perform the local switching
- Split tunnelling is using the AP IP@ for the NAT/PAT feature

Starting from 7.3
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 centralised web portal creation for multiple sites
- Provides flexible use of Conditional and Splash Page Web Redirect
- FlexConnect AP must be in Connected state with Centralised Controller for this functionality to work
External WebAuth with Local Switching Configuration

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

**Access Control Lists > Edit**

<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
External WebAuth with Local Switching
Configuration – Per AP

Step 3: Apply Pre-Auth ACL to FlexConnect AP

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

Map WLAN-Id to Pre-Auth ACL
External WebAuth with Local Switching Configuration

Step 4: Configure External Web Server

![Web Login Page Configuration](image)
Deploying BYOD with FlexConnect Local Switching (Using FlexConnect WebPolicies ACL)
BYOD Device On-Boarding in FlexConnect
Example: Apple iOS Device Provisioning

Starting from 7.4

1. Initial Connection Using PEAP
2. Device Provisioning Wizard
3. Future Connections Using EAP-TLS
Deploying BYOD with FlexConnect Wireless
Summary – 802.1x/EAP Authentication

- 802.1x/EAP Request
  - Inside CAPWAP
- 802.1x/EAP Response
  - Inside CAPWAP
- Radius Access-Request
  - Inside CAPWAP
- Radius Access-Response
  - Access-Type: Access-Accept
  - URL-Redirect-ACL=FlexACLWeb
  - URL-Redirect=http://……
- URL + ACL Redirect
  - Inside CAPWAP
- WiFi Association
- 802.1x Authentication

ISE
DHCP Server
Web Server
Unknown Device, Redirect to registration

FlexConnect AP
CAPWAP
WLC
DHCP Server
Web Server
Unknown Device, Redirect to registration
Deploying BYOD with FlexConnect Wireless

Summary – DHCP Request

DHCP Request

Inside CAPWAP

RADIUS-Accounting
- host-name=MyiPad
- dhcp-class-identifier=APPLE

Device is an Apple iPad

WAN

DHCP Lease

Inside CAPWAP

DHCP Request

FlexConnect AP

WLC

ISE

DHCP Server

Web Server
Deploying BYOD with FlexConnect Wireless
Summary – URL-Redirect

HTTP Request
Redirected to WLC by AP

Inside CAPWAP

URL-Redirect
Deploying BYOD with FlexConnect Wireless

Summary – Registration & Provisioning

Device Registration & Provisioning

EAP DeAuthentication

RADIUS Change-of-Authorisation

EAP Authentication

ISE

DHCP Server

Web Server

Device is Registered

Trigger Change-of-Auth
Deploying BYOD with FlexConnect Wireless

Summary – Device Access

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

**802.1x/EAP Request/Response**

- Inside CAPWAP

**DHCP Request/Response**

- Inside CAPWAP

**Web Traffic**

**Device is Registered and Provisioned**

**Allow Access**

**Radius Access-Request**

**Radius Access-Response**

**802.1x Authentication**

**RADIUS Accept**

**DHCP Request**

**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 ~6000 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)
FlexConnect Smart AP Image Upgrade

Description (Cont…)

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
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 receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.
- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.
www.CiscoLiveAPAC.com