Desing a nasazení tradičních Cisco WLAN sítí s centralizovanými kontrolery

T-NET4 / L2
Jaroslav Čížek - Cisco
Agenda

- Wireless Deployment Models
- Cisco Wireless Portfolio Update
- DFS Regulation Changes, Migration Path
- Unified Wireless New SW Features
- Cisco Mobile Experience
- Cisco's Meraki Acquisition
- Cisco Expo 2012 Wireless Infrastructure
- Summary
Cisco One Network: Wireless Deployment Modes

One Policy, One Management, One Network

Unified Access Wireless

Autonomous
FlexConnect (Private Cloud)
Centralized
Converged Access

N.A.A.S.
Unified Network
Public Cloud

Unparalleled Deployment Flexibility
Ease of Use

New
Unified Access—Wireless Deployment Modes

<table>
<thead>
<tr>
<th>Target Positioning</th>
<th>Small Wireless Network</th>
<th>Branch</th>
<th>Campus</th>
<th>Branch and Campus</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purchase Decision</strong></td>
<td>Wireless only</td>
<td>Wireless only</td>
<td>Wireless only</td>
<td>Wired and Wireless</td>
</tr>
<tr>
<td><strong>Benefits</strong></td>
<td>• Simple and cost-effective for small networks</td>
<td>• Highly scalable for large number of remote branches • Simple wireless operations with DC hosted controller</td>
<td>• Simplified operations with centralized control for Wireless • Wireless Traffic visibility at the controller</td>
<td>• Wired and Wireless common operations • One Enforcement Point • One OS (IOS) • Traffic visibility at every network layer • Performance optimized for 11ac</td>
</tr>
<tr>
<td><strong>Key Considerations</strong></td>
<td>• Limited RRM, no Rogue detection</td>
<td>• L2 roaming only • WAN BW and latency requirements</td>
<td>• System throughput</td>
<td>• Catalyst 3850 in the access layer</td>
</tr>
</tbody>
</table>
One Network, with Converged Access
A New Deployment Option for Wired / Wireless

**IOS Based WLAN Controller**
- Consistent IOS and ASIC w/ Catalyst 3850
- Required to scale beyond 250 AP or 16K client domains

**Converged Access Mode**
- Integrated wireless controller
- Distributed wired/wireless data plane (CAPWAP termination on switch)
Cisco Wireless Portfolio Update
Cisco Aironet 802.11n G2 Series Access Point Portfolio

**With CleanAir Technology**

**ENTERPRISE READY**
- Coming Soon
- Basic Enterprise AP
- Value optimized
- Enterprise-class Performance
- Voice/Video/Multimedia
- RF Interference Mitigation

**TELEWORKER**
- 600
- Basic Connectivity
- Deployment Flexibility

**1600**
- Any Device / BYOD Optimized
- Client Scalability
- 11ac Migration

**2600**
- High Client Density
- HD Video/VDI
- Investment Protection
- Comprehensive Security

**3600**
- 802.11ac Module
- Security Monitor Module
- 3G Small Cell Module

**INVESTMENT PROTECTION**
- Coming Soon

**BEST IN CLASS**
AP3600 – Security Monitor Module

No requirement to deploy a separate and dedicated overlay of AP’s in monitor mode for full spectrum monitoring

A field-upgradable 3rd Radio module add-on to the AP3600
  Dedicated 2.4 GHz & 5 GHz XOR radio – **both bands supported in the single module**

Enables the AP3600 to be the only AP to concurrently:
  Serve clients on both 2.4 and 5 GHz – with the internal integrated radios and antennas 4x4:3
  Perform wIDS/wIPS scanning on both 2.4 & 5 GHz bands on all channels
  Perform CleanAir spectrum analysis on both 2.4 and 5 GHz bands on all channels

---

**ELM**
Single Data and WIPS AP

**Monitor Mode AP**
Data Serving AP  
Monitor Mode AP

**Security Module**
AP 3600 with Security Module
AP3600 – Investment Protection
802.11ac Wave 1 Module

A field-upgradable 802.11ac module add-on to the AP3600

802.11ac Wave 1 – 5 GHz AP3600 Module
- 5 GHz radio module
- Supporting 802.11a and n clients along with ac clients
- 1.3 Gbps PHY / ~1 Gbps MAC (throughput)
- 3 Spatial Streams, 80 MHz, 256 QAM
- Explicit Beamforming support as per the 802.11ac standard

AP3600 maintains dual-band support 2.4 and 5 GHz
- Supporting b/g/n on 2.4 GHz and a/ac/n on 5 GHz

Power requirement with the 802.11ac Module installed
- Power draw with 802.11ac Module exceeds 15.4 Watts (802.3af), and will require either:
  - Enhanced PoE, 802.3at PoE+, Local Supply or Power Injector 4

Universal Mounting Brackets (Bracket-2) required, or Ceiling Mounting Brackets (Bracket-3)
### 802.11ac: The Next Step in Wi-Fi

**Next gen multi-gigabit Wi-Fi – spec’d up to 6.9 Gbps**
- 5 GHz only (not 2.4 GHz)
- 80 MHz, optional 160 MHz, 80+80MHz
- Optional 256 QAM
- Up to 8 space time streams
- Optional MU-MIMO

<table>
<thead>
<tr>
<th>Year</th>
<th>Standard</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>1997</td>
<td>802.11</td>
<td></td>
</tr>
<tr>
<td>1999</td>
<td>802.11b</td>
<td></td>
</tr>
<tr>
<td>2003</td>
<td>802.11a/g</td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td>HT 802.11n</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>VHT 802.11ac Wave1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VHT 802.11ac Wave2</td>
<td></td>
</tr>
</tbody>
</table>

* - Assuming 160 MHz is available and suitable

1. - Assuming 80 MHz with 4 spatial streams
## Dual band antennas for AP1600e/2600e/3600e

<table>
<thead>
<tr>
<th>Product ID</th>
<th>Description</th>
<th>Gain</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIR-ANT2524DB-R</td>
<td>2.4 GHz 2 dBi / 5 GHz 4 dBi Dipole Ant., Black, RP-TNC connectors</td>
<td>2 dBi (2.4 GHz), 4 dBi (5 GHz)</td>
</tr>
<tr>
<td>AIR-ANT2524DG-R</td>
<td>2.4 GHz 2 dBi / 5 GHz 4 dBi Dipole Ant., Gray, RP-TNC connectors</td>
<td>2 dBi (2.4 GHz), 4 dBi (5 GHz)</td>
</tr>
<tr>
<td>AIR-ANT2524DW-R</td>
<td>2.4 GHz 2 dBi / 5 GHz 4 dBi Dipole Ant., White, RP-TNC connectors</td>
<td>2 dBi (2.4 GHz), 4 dBi (5 GHz)</td>
</tr>
<tr>
<td>AIR-ANT2566P4W-R</td>
<td>2.4 GHz 6 dBi 5 GHz 6 dBi Directional Ant., 4-port, RP-TNC connectors</td>
<td>6 dBi (2.4 GHz), 6 dBi (5 GHz)</td>
</tr>
<tr>
<td>AIR-ANT2524V4C-R</td>
<td>2.4GHz 2 dBi 5GHz 4 dBi Ceiling Mount Omni Ant., 4-port, RP-TNC connectors</td>
<td>2 dBi (2.4 GHz), 4 dBi (5 GHz)</td>
</tr>
<tr>
<td>AIR-ANT2544V4M-R</td>
<td>2.4GHz 4 dBi 5GHz 4 dBi Wall Mount Omni Ant., 4-port, RP-TNC connectors</td>
<td>4 dBi (2.4 GHz), 6 dBi (5 GHz)</td>
</tr>
</tbody>
</table>

*Note for AP1600e: 2566,2524 & 2544 have 4 antenna leads just leave one unused*
Access Point Portfolio

CAMPUS and BRANCH

Enterprise Class
1600

Mission Critical
2600

Best in Class
3600

OUTDOOR

MSO / Cable

Versatile
1552C

1552EU

Industrial
1552H

1552S

1552I

1552EU

M2M
Ruggedized Mobility

Small Branch
819

TELEWORKER

OfficeExtend
600

CiFi
Micro Branch
812

819

881
Controller Product Portfolio
Unified + Converged + Cloud

Features and Functionality

Scale (# of clients and # of APs)

2500
75 APs
1,000 Clients

5500
500 APs
7,000 Clients

WiSM2
1,000 APs
15,000 Clients

WiSM2
1,000 APs
64,000 Clients

Virtual Controller
200 APs
3,000 Clients

FlexConnect
6,000 APs
64,000 Clients

3850
50 APs
2,000 Clients

8500
6,000 APs
64,000 Clients

Cloud
Optimized for Teleworker, Branch, and Distributed Enterprises

5760
1,000 APs
12,000 Clients

Flex7500
6,000 APs
64,000 Clients

Converged Access
Virtual Wireless LAN Controller (vWLC)

Deployment Flexibility

Product Scope

- 5 to 200 AP support, 3000 clients
- 1 AP adder license

**FlexConnect Mode Only**

Support on VMWare ESX/ESXi 4.x/5.x

Support on Cisco UCS B-/C-Series and UCS Express and equivalent servers

The resource requirements:
- CPU: 1 virtual
- CPU Memory: 2 GB
- Disk Space: 8 GB
- Network Interfaces: 2 or more virtual Network Interface cards (vNICs)

Pricing:
- Base SKU: AIR-CTVM-5-K9 - $750 (includes 5 AP license)
- 1 AP Adder License – L-LIC-VM-1A - $150

Target Market

- Price Sensitive Mid-Market
- Alternative to Flex 7500 for customers with fewer branches
- Partner/MSP hosted WiFi service
- NOT for large campus

![Diagram of Cisco CUWN in a BOX with vWLC, vNCS, and vMSE]
Cisco Prime Infrastructure 1.3 (former NCS / WCS)
Single Pane of Glass Management

A Single Solution for Converged Wired and Wireless Management

Lifecycle
- Discovery, inventory, configuration, fault, troubleshooting, remediation

Assurance
- Application performance visibility
- End-user experience

Compliance
- Regulatory compliance
- and best practices

WCS -> Prime Infrastructure - Accelerate Migration from WCS to Cisco Prime

WCS to NCS, and WCS to CPI Migration SKUs ($2k GPL) is extended until June 2013
Mobility Services Engine (MSE) Overview

**Advanced Spectrum Capability**
- System wide Interferer details
- Interferer event correlation
- Visualization of interferer zone of impact & Interferer notification

**Location Services**
- Track & Trace interferers & Layer 1 threats, Rogues, Wi-Fi clients and RF tags
- Geo fencing / Zone based alerts
- Presence detection

**Wireless Intrusion Prevention**
- Detection & Mitigation of security penetration & DOS attacks
- Capability supported in Monitor Mode & data serving AP (Enhanced Local Mode - ELM)

**Advanced Location Services**
- Mobile Concierge
- Thinksmart Location Analytics
- AP3600 Wireless Security & Spectrum Intelligence Module

Available as Physical & Virtual Appliance
MSE tracks up to 50,000 endpoints & supports 10,000 Monitor Mode or ELM AP

Available Q1 CY2013
Cisco Unified Access Portfolio
Deliver an Uncompromised User Experience on Any Workspace

Unified Wireless
- 30% faster
- CleanAir
- VideoStream
- OfficeExtend

Catalyst Switching
- Converged Access
- Advanced QoS
- Self-config for switches/APs
- Dynamic config based on device/policy
- Secure Group Access

Prime Management
- Converged management - wired/wireless/policy
- One-click troubleshooting
- Real-time xperience monitoring

Identity Services Engine
- Single source of policy for wired/wireless/MDM

One Network
Converged Architecture Strategy Assessment

One Management
Services:
- Remote Management
- Network Optimization
- Smart Net Total Care

One Policy
Cisco TrustSec Service
DFS Regulation Changes, Migration Path
European DFS Regulation Changes

New DFS regulation in Europe effective on Jan. 1, 2013 requires more granular DFS pulse detection at the rate of 0.5 µs (vs. current 0.8 µs)

→ Driven by new military/weather radar in EU that pulses at 0.5 µs rate

Impacted AP’s

• AP1042, AP1142, and AP1252

Access Points shipped before Jan. 1, 2013 are not affected by this change

AP platforms deployed can continue to upgrade software post Jan. 1, 2013

=> AP1142(1042) –E domain End of Sale date: November 30, 2012
Access Point Transition – Global View
Case 1: AP not supported in 7.4

Prime Infrastructure 1.2

5508 Controllers in 7.4 with HA

5508 Controllers Cluster in 7.0

Mobility Group

New AP2600, AP1600
Case 2: WLC not supported in 7.3

Prime Infrastructure 1.2

5508 Controllers in 7.3 with HA

4400 Controller Cluster in 7.0

Mobility Group

New AP-2600

Current AP supporting 7.3: Start migration for better feature support
Unified Wireless
New SW Features
Cisco Wireless Redundancy
Better Resiliency, Better TCO

5500, WiSM2, 7500, 8500 Series

L2 Redundant Link
Active WLC
Hot-Standby WLC

- 1:1 wireless stateful failover capability in appliance and integrated controllers
- SSID is always beaconing (even after primary controller is down)
- Subsecond WLAN network convergence
- No duplicate licensing around HA: New HA SKU for 5508, WiSM2, Flex7500, WLC8500
- Clients re-associate after that and sessions need re-establishment

Version 7.2 and older:
500 APs fail-over in approx 90 sec (5500) or in approx 60 sec (WiSM2), clients reassociate time is in addition
Full license count needed on backup controller
High Availability Configuration

By default HA is disabled.

Configure Redundant Management and Peer Redundant Management IP first before enabling AP SSO
HA-SKU as secondary WLC - configuration

**CLI Secondary:** `config redundancy unit secondary`

**CLI Primary:** `config ap primary-base <Switch Name> <Cisco AP> <Switch IP Addr>`

```
(Cisco Controller) > show redundancy summary

Redundancy Mode = SS0 DISABLED
Local State = ACTIVE
Peer State = N/A

Unit = Secondary - HA SKU
Unit ID = 70:81:05:CE:8:40
Redundancy State = N/A
Mobility MAC = 70:01:05:CE:6:40

Redundancy Management IP Address............. 0.0.0.0
Peer Redundancy Management IP Address............. 0.0.0.0
Redundancy Port IP Address...................... 0.0.0.0
Peer Redundancy Port IP Address.................. 169.254.0.0
```

GUI configuration:
Cisco’s Application Visibility & Control
Identify, Analyze, and Optimize Application Traffic

BEFORE
Application View & Control based on Firewall sessions
Visibility to the port level interaction but not the applications running within the port

First Generation Firewall

FW L4 Session Visibility and Control

HTTP = 75%
SMTP = 15%
FTP = 2%
Telnet = 1%
SNMP = 3%

AFTER
Network Based Application Recognition - NBAR2
Deep Packet Inspection and App ID

Improved Visibility & Control

Wireless LAN Controller

Traffic

 Netflix = 50%
 YouTube = 15%
 WebEx = 10%
 Citrix = 9%
 exchange= 8%

NBAR2 LIBRARY
Deep Packet Inspection

POLICY
Packet Mark and Drop

View, Control and Troubleshoot - End User Application Experience

HTTP = 75%
SMTP = 15%
FTP = 2%
Telnet = 1%
SNMP = 3%
Enabling AVC
AVC enabled on per WLAN basis

- Global summary of top applications on Controller Monitor screen
**AVC Summary**

Application Statistics per WLAN with more details UP/Down Streams

### WLANs > Application Statistics

<table>
<thead>
<tr>
<th>Aggregate</th>
<th>Upstream</th>
<th>Downstream</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Name</td>
<td>Packet Count</td>
<td>Byte Count</td>
</tr>
<tr>
<td>ms-lync</td>
<td>35970</td>
<td>19368158</td>
</tr>
<tr>
<td>ssl</td>
<td>5482</td>
<td>4840784</td>
</tr>
<tr>
<td>rtp</td>
<td>6830</td>
<td>1806702</td>
</tr>
<tr>
<td>rtcp</td>
<td>578</td>
<td>362678</td>
</tr>
<tr>
<td>http</td>
<td>296</td>
<td>328084</td>
</tr>
<tr>
<td>bittorrent</td>
<td>457</td>
<td>57236</td>
</tr>
<tr>
<td>citrix</td>
<td>345</td>
<td>30003</td>
</tr>
<tr>
<td>dns</td>
<td>61</td>
<td>12831</td>
</tr>
<tr>
<td>webex-meeting</td>
<td>15</td>
<td>5525</td>
</tr>
<tr>
<td>skype</td>
<td>65</td>
<td>5449</td>
</tr>
</tbody>
</table>

**Application Last 90 Secs Usage(%)**

- ms-lync (72.22%)
- ssl (16.05%)
- rtp (6.74%)
- rtcp (1.35%)
- http (1.22%)
- bittorrent (0.21%)
- citrix (0.11%)
- dns (0.05%)
- webex-meeting (0.02%)
- skype (0.02%)

**Application Cumulative Usage(%)**

- citrix (36.49%)
- ms-ocx-file-transfer (14.76%)
- binary-over-http (12.23%)
- bittorrent (11.88%)
- http (10.10%)
- ms-lync (5.33%)
- rtp (3.47%)
- ssl (3.19%)
- youtube (1.76%)
- itunes (0.81%)
Why Bonjour services need modifications?

- Bonjour is link local multicast and thus forwarded on Local L2 domain
- AirPlay (Apple TV) and AirPrint supported only on a single VLAN
- mDNS operates at UDP port 5353 and sent to the reserved group addresses:
  - IPv4 Group Address – 224.0.0.251
  - IPv6 Group Address – FF02::FB
• In 7.4 Bonjour Services with mDNS gateway on the controller don’t require multicast services to be enabled.
# Configuring mDNS Snooping

Enable mDNS snooping globally and add services

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Service String</th>
<th>Query Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirPrint</td>
<td>_ipp_tcp.local</td>
<td>✓</td>
</tr>
<tr>
<td>AppleTV</td>
<td>_airplay_tcp.local</td>
<td>✓</td>
</tr>
<tr>
<td>Printer</td>
<td>_printer_tcp.local</td>
<td>✓</td>
</tr>
</tbody>
</table>
Configure mDNS profile per WLAN
Create custom profile per WLAN

Enable mDNS snooping profile on the desired VLAN or WLAN
Summary of Bonjour enabled devices

Bonjour enabled devices advertising service is shown as Domain Name

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>MAC Address</th>
<th>IP Address</th>
<th>Vlan Id</th>
<th>Type</th>
<th>TTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple-TV.local.</td>
<td>00:10:4f:03:e7:08:04</td>
<td>10.10.20.101</td>
<td>20</td>
<td>Wireless</td>
<td>4725</td>
</tr>
</tbody>
</table>
802.11K support for Apple iOS 6.0 devices

• Apple and Cisco collaborating on 802.11k
• Existing 7.4 release will support only a subset of features
• Apple WiFi iOS 6.0 devices optimized for roaming and power consumption performance.
• 802.11k neighbor list reduces the need for active and passive scanning.
• Based on our RRM neighbor table an Intelligent and Optimized list created
• Assisted Roaming feature based on the optimized list introduced
• CLI controller configuration support only and no GUI or PI support yet
Management Frames e.g. dis-associate/de-authenticate transmitted in the open
Vulnerable to man-in-the-middle or DOS attacks
Cisco Innovation MFP supported in autonomous release 12.3(8)JA starting 2006 and Unified starting 2008 in version 4.0.155.5 avoids these issues by adding integrity into the management frames

802.11w Local mode support for this feature in 7.4, Flex locally switched support in 7.5
Due to differences between Cisco’s implementation and 11w we had a bug CSCua29504: addressed in 7.3.101.0, 7.2.111.3, 7.0.235.3
Group Management Cypher Suite

The presence of this element indicates the use of 802.11w.
11w GUI Configuration

802.11w MFP is enabled on a per-WLAN basis

Navigate to WLANs and select the WLAN ID for the one you want to enable 802.11w on

The 802.11w IGTK Key is derived using the 4-way handshake which means it can only be used on WLANS configured for WPA or WPA2 security at Layer 2

Disabled = Not in use
Optional = Used if the client supports
Required = Non 11w capable clients can not associate to this WLAN

Time which an associated client must wait before the association may be tried again when first denied with a status code 30

If no response is received from the client SA Query within this time, the client association is deleted from the controller
11w is NOT Cisco MFP

Please do not confuse 802.11w MFP with Cisco’s legacy MFP which can be disabled even when 11w is active.

Cisco MFP is enabled from the drop down menu under AP Authentication Policy.

These settings reflect the Cisco MFP configuration settings on the WLAN Advanced Tab and NOT the 11w status.

Management Frame Protection Settings > General

Management Frame Protection: Disabled (all infrastructure settings are overridden)
Controller Time Source Valid: True

This represents the status of Cisco MFP and NOT the status of 802.11w.
CUWN SW Releases
7.0, 7.3, 7.4? Which Version Should I Use?

Download Software

Recommended releases:
- **7.4** – all NEW HW and features (AVC, HA, …), supported on new WLCs (5508. WiSM2, 2504, Flex 7500, vWLC), AP1600/2600/3600, WSSI module
- **7.3.112** – new mobility / converged access with Cat3850
- **7.5** – future release, target fcs May 2013, support for AP700, 802.11ac module
- **7.0.220** – MD release, last 7.0.240 release recommended, supported on all current (5508. WiSM2, 2504, Flex 7500) and older WLCs (440x, WiSM1, 2106, WLCM)

AssureWave (client compatibility)
https://www.cisco.com/go/assurewave
# 5760 in Centralized deployment mode

## Features comparison to 5508 at FCS

<table>
<thead>
<tr>
<th>Features</th>
<th>5760</th>
<th>5508</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Throughput</strong></td>
<td>60 Gbps</td>
<td>8 Gbps</td>
</tr>
<tr>
<td><strong>Scale</strong></td>
<td>1000 APs 12000 Clients</td>
<td>500 APs 7000 Clients</td>
</tr>
<tr>
<td><strong>Modes</strong></td>
<td>Converged Access</td>
<td>Converged Access</td>
</tr>
<tr>
<td></td>
<td>Centralized (local-mode)</td>
<td>Flex, Mesh, Outdoor, OEAP</td>
</tr>
<tr>
<td><strong>Resiliency</strong></td>
<td>1+1 and N+1 HA SKU AP SSO*</td>
<td>1+1 and N+1 HA SKU AP SSO*</td>
</tr>
<tr>
<td><strong>Application-awareness</strong></td>
<td>Flexible Netflow v9, NBAR2*, Downloadable ACL</td>
<td>NBAR2, Netflow</td>
</tr>
<tr>
<td><strong>QoS</strong></td>
<td>Granular QoS (MQC): Hardware based Queues can be mapped per SSID, per radio, per client Approximate Fair Drop</td>
<td>4 queues – Platinum, Gold, Silver, Bronze Can be applied per WLAN/SSID Bi-directional rate limiting</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Downloadable ACLs SGA(SXP, SGT)*</td>
<td>Dynamic ACLs SGA (SXP)</td>
</tr>
<tr>
<td><strong>IPv6</strong></td>
<td>IPv6 addressing on interfaces, IPv6 ACLs First Hop Security*</td>
<td>IPv6 Client Mobility First Hop Security</td>
</tr>
<tr>
<td><strong>BYOD</strong></td>
<td>ISE 1.1MR, Single SSID*, Device Sensor*</td>
<td>ISE 1.1MR, Single SSID, Device Sensor</td>
</tr>
<tr>
<td><strong>Federal Certs</strong></td>
<td>FIPS, CC, DOD in evaluation* with UCAPL*</td>
<td>FIPS, CC, UCACPL, DOD</td>
</tr>
<tr>
<td><strong>Licensing</strong></td>
<td>Right To Use(RTU)</td>
<td>Tied to serial number</td>
</tr>
<tr>
<td><strong>User Interface</strong></td>
<td>IOS CLI, CPI 2.0 June 2013, Device GUI*</td>
<td>Telnet, Device GUI</td>
</tr>
</tbody>
</table>

IOS Controllers are based on AireOS features 7.0.230.0

* Roadmap (Q3 CY13) • Roadmap (Q2 CY14)
Cisco Mobile Experience
The customer’s personal mobile device detected as they enter the venue.

The customer is seamlessly and securely connected to the Wi-Fi network.

The customer receives highly relevant content and services based on their preferences, profile and location.

**Customer:** Presence in the venue.

**IT:** understand network utilization, peak usage, number and types of devices on the network.

**Business:** insights into customer online and onsite behavior, most traffic paths, dwell times, location density etc.
MSE Key Portfolio Updates
Built on Unified Access Infrastructure
Cisco Connect 2013 – Visitor App

LIVE APP WITH MSE

Created using Meridian App
Includes rich content, indoor navigation, …. 
Enable Mobile App Integration

Location Name: Cisco
Email Addresses: saihankar.c@gmail.com

Get the most from your MSE.

Provide indoor location and way-finding to your users on their wireless devices. Create location-based notifications and offers.

Powered by meridian
Thinksmart Location Analytics

Improving Customer Experience Through Location Analytics

- Detects presence, locates & tracks

Thinksmart
Aggregates and enhances location data for Analytics and Reporting
- Classifies, groups into representative areas (cluster points) based on specified criteria
- Provides dwell time, crowding and other parameters in these representative areas
- Shows typical paths
- Shows breakouts of devices along alternative paths
- Threshold & Policy based alerting
- Reporting (rules engine)
Autonomous AP (aiOS) – new features

- **Full aiOS functionality** for 1550, 1600, 3500, 3600 & ISR812/819
- **Spectrum Expert Mode** - An SE Connect autonomous AP is configured as a dedicated Spectrum Sensor that allows connection to the Cisco Spectrum Expert application currently available
- **Easy GUI setup** - Update the GUI to have a single screen for Easy/Quick Setup
- **BandSelect**
- **L2TPv3** - A Tunneling mechanism for the Access Points that is compatible with Dynamic IP (Public/Private). An Auto configuration (Dropship) solution for the Access Points.
- **802.11r Roaming Support**
Cisco Wi-Fi Carrier-Grade Solution

Cisco Advanced Services – PDI to Solution Assurance to BOT

Home

Office

Community

Retail

Wi-Fi

Cisco Access Points

Indoor

Outdoor

Residential

Intelligent Services Cloud

Cisco Prime Portal & Policy

Cisco WLC

Cisco ASR9K

Cisco ISG

3G/4G Mobile Packet Core

Internet

Management & Provisioning

Cisco Prime

Cisco Wi-Fi Carrier-Grade Solution

Cisco Advanced Services – PDI to Solution Assurance to BOT

Home

Office

Community

Retail

Wi-Fi

Cisco Access Points

Indoor

Outdoor

Residential

Intelligent Services Cloud

Cisco Prime Portal & Policy

Cisco WLC

Cisco ASR9K

Cisco ISG

3G/4G Mobile Packet Core

Internet

Management & Provisioning

Cisco Prime
Cisco's Meraki Acquisition
Mega Trends

By 2014, 90% of organizations will allow personal devices for work use.

100% of IT is struggling to keep up with mobility trends.

- Gartner

MOBILITY  CLOUD  DATA
Meraki: 100% Cloud Managed Network Edge

Meraki MR
Wireless LAN

Meraki MX
Security Appliances

Meraki MS
Ethernet Switches

Meraki SM
Mobile Device Management
Building on the Success of Meraki Customers

Mid-Market
- ZGF
- Needham
- Foster Pepper PLLC
- Bilzin Sumberg
- dcm
- Nordson

Hospitality
- Caravelle Hotell
- Holiday Inn
- Comfort Suites
- Sandman
- Viceroy Hotels & Resorts
- Accor
- Radisson

K-12
- Staunton
- Rainbow Schools
- Exeter
- LPSD
- Regis High School

Retail
- Design Within Reach
- piggy piggy
- Burger King
- United Colors of Benetton
- Caribou Coffee
- Starbucks
- Westfield
Cisco Enterprise and Cloud-Managed Networking Primary Positioning

Cisco Enterprise Portfolio
On-Premise Managed
- Deployment Flexibility

Cisco Cloud Networking Portfolio
Cloud Managed (Meraki)
- Lean, Generalist IT
- Distributed small sites

Features / Network Services

Cisco Small Business Solutions

Network Size (Sites, Density)

Small Business  Mid-Market / Commercial  Enterprise
Cisco Connect 2013 Wireless Infrastructure
Cisco Connect 2013 - wireless infrastrukturna

- Voice
- Connected Mobile Experience
- Security
- Guest Access
- CleanAir
- ClientLink
- BandSelect
- VideoStream
- Switched/Routed Network
- 2x Wireless LAN Controller 5508
- ~35x AP3600
- AP2600
- AP1600
- Client Devices
- Interference
- Spectrum Expert
- Fluke OptiView
- Prime Infra 1.3 + MSE 7.4
- Local analytics, Meridian
- AVC - Appl. visibility
Connect 2013 - Maps
Connect 2013 - Clients

The image shows the interface of a network management tool for Cisco Connect 2013, focusing on clients. The interface is divided into sections for overview, incidents, performance, detail dashboards, and more. It includes charts for client troubleshooting, client distribution, and alarms and events summary. The charts display data on MAC addresses, EAP type, authentication type, and network speed distribution. The interface also shows statistics on the top 5 SSIDs and switches by client count.
Connect 2013 - Interferers
Connect 2013 – Spectrum Expert
Connect 2013 - AVC
Connect 2013 - Meridian

This is a Trial version of Meridian for Cisco MBE customers. For more information, see our MBE Integration Tutorial.
Connect 2013 – Location Analytics
Otázky a odpovědi
Prosíme, ohodnotíte tuto přednášku.
Děkujeme za pozornost.