
TOMORROW
starts here.
CISCO
Cisco live!

Troubleshooting Converged Access Wireless Deployments

BRKEWN-3021

Surendra BG

Senior Technical Services Engineer

#clmel

Cisco live!

Troubleshooting Converged Access Wireless Deployments

BRKEWN-3021 Session Overview and Objectives

This session discusses troubleshooting techniques and best practices for the Cisco Converged Access Mobility Architecture.

We will cover how to troubleshoot mobility and client connectivity issues under the various deployment models.

We will cover common information, tools, and debugs used by TAC to resolve issues. We will also review key issues to watch out for.

© 2015 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Agenda

- Converged Access (CA) Architecture
- Troubleshooting
- Common issues
- Summary

© 2015 Cisco and/or its affiliates. All rights reserved.

Converged Access Architecture

Agenda

Converged Access Architecture

- Hardware platforms
- Internal architecture
- Mobility overview

© 2015 Cisco and/or its affiliates. All rights reserved.
Cisco Public

CA Architecture

Hardware Platforms

Catalyst WS-C3850

Directly connected APs
Up to 50 APs / 2000 users

Catalyst WS-C3650

Directly connected APs
Up to 25 APs / 1000 users

WLC CT-5760

Up to 1000 APs / 12000 clients

Catalyst 4500E SUP 8E

Directly connected APs
Up to 50 APs / 2000 users

Note: the above values are max supported scalability

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

CA Architecture

Access Points

- AP 1040 / 1140
- AP 1260 / 3500
- AP 1600 / 2600 /2700
- AP 3600 + 11ac module
- AP 3700
- AP 1532 / 1570 (Outdoor)
- AP 700 / 702w

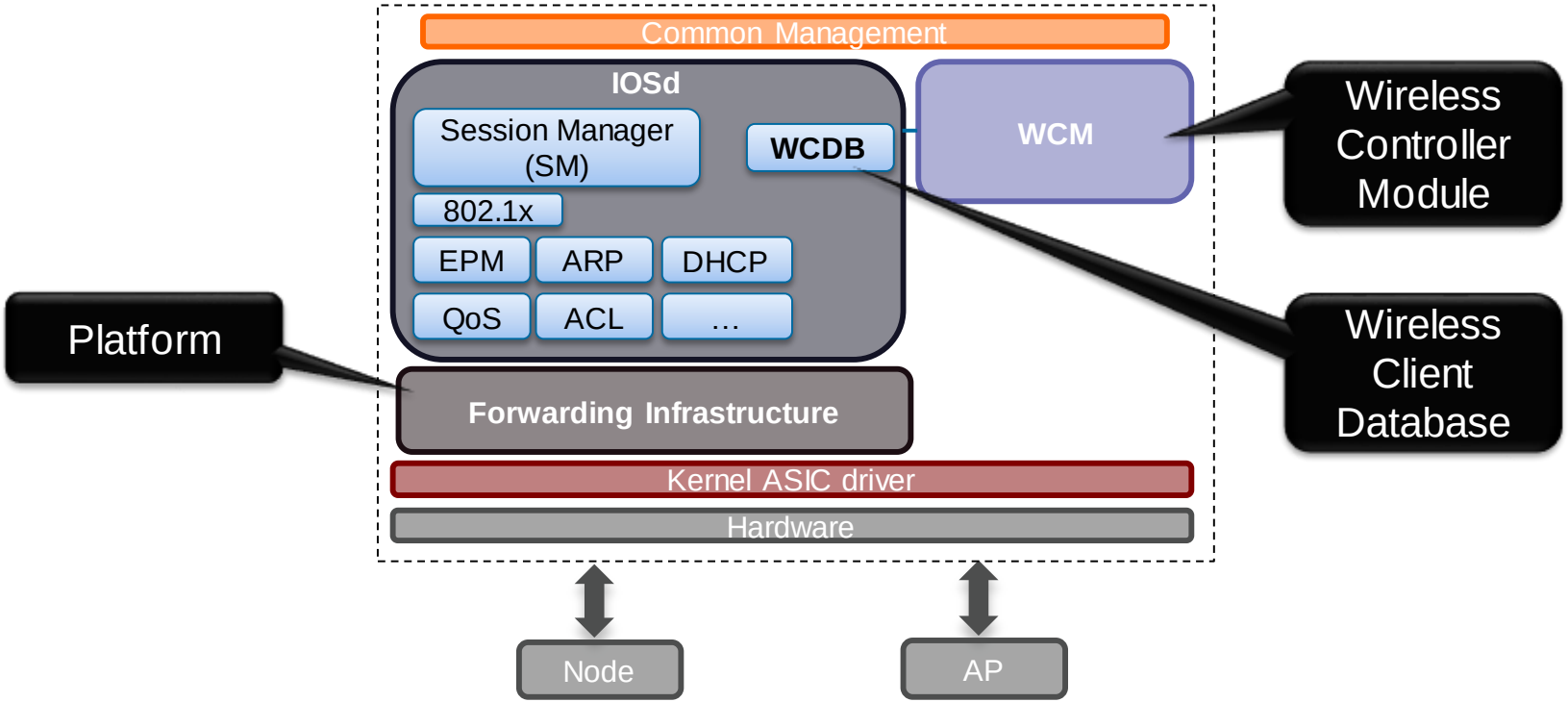
AP modes

- Local
- Monitor, SE-Connect, Sniffer
- Universal AP Support

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

CA Architecture

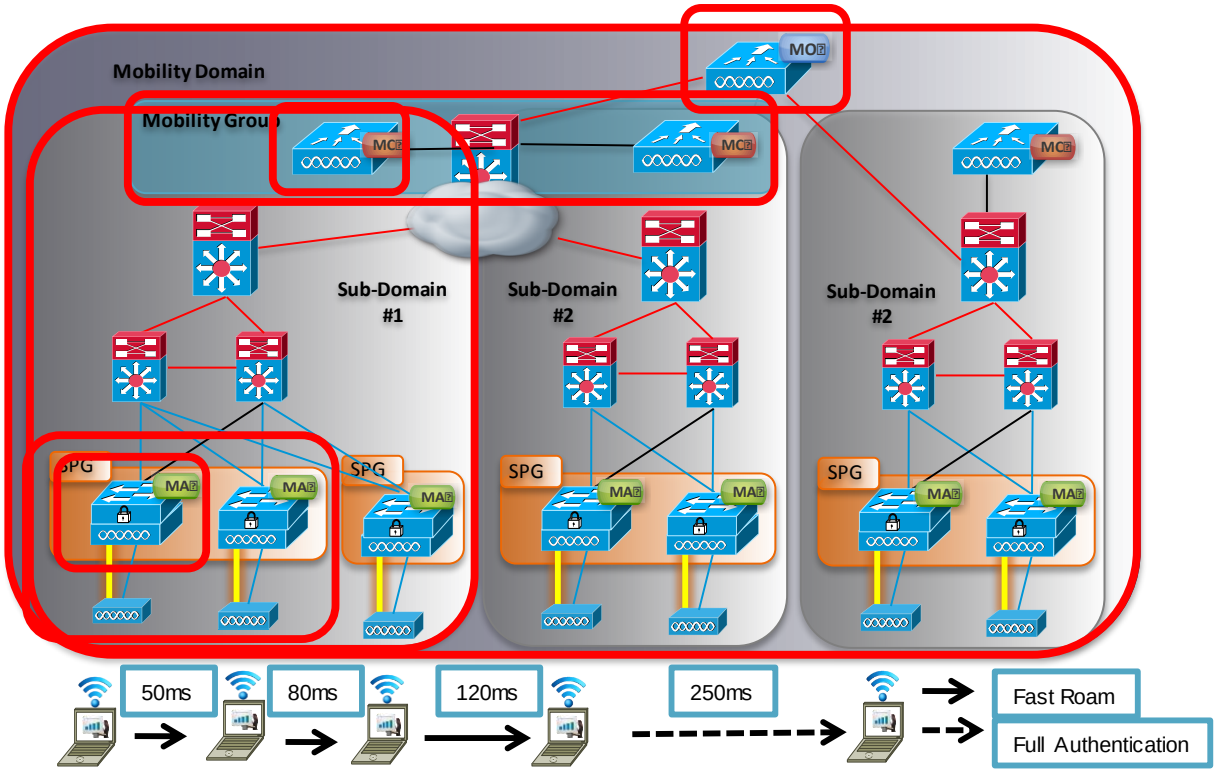
Internal Components (Simplified Schema)



© 2015 Cisco and/or its affiliates. All rights reserved.

CA Architecture – Hierarchical Mobility

Components, Roles and Roaming



Physical Entities

- MC — Mobility Controller
- MA — Mobility Agent
- MO — Mobility Oracle

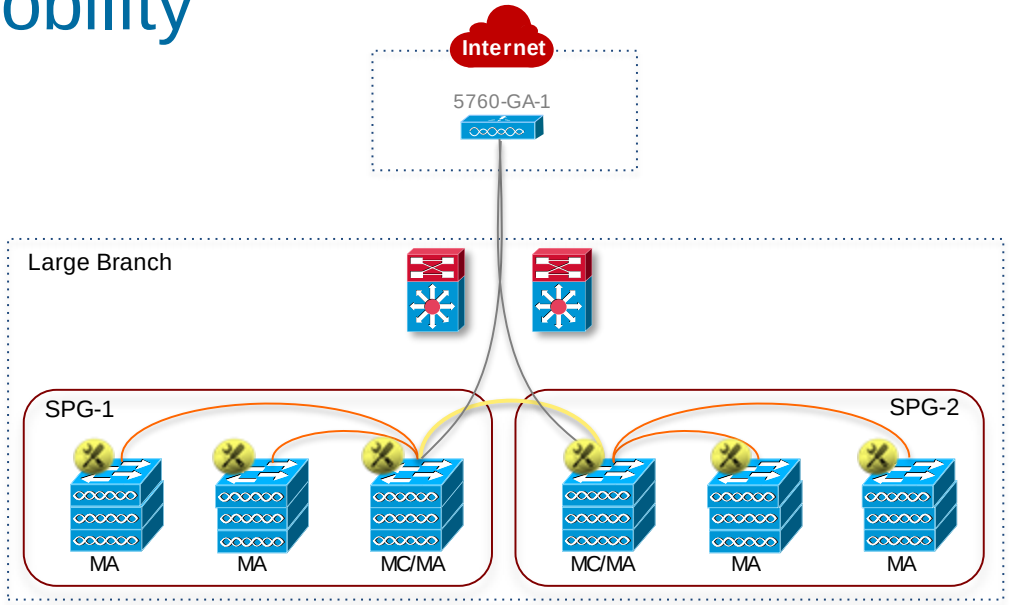
Logical Entities

- SPG — Switch Peer Group
- Mobility Group
- Mobility Domain

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Hierarchical Mobility

MC Managing MA



Default Mode (Distributed)

- Fully Distributed Control / Mgmt / Data Plane architecture
- Complex operation from Unified network design
- Too many touch points for common configurations
- Challenging to deploy Converged Access without Cisco Prime Infra.

Centralise Mobility Agent Management Mode

- Centralised MA provisioning and monitoring from MC
- Single device to deploy common configuration. Automate to paired MA's
- Simplified Management plane. No change in distributed control and data plane architecture
- Alternative solution to deploy Converged Access without Cisco Prime Infra.

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Troubleshooting

Agenda
Troubleshooting

- Troubleshooting Tools
- System level sanity check
- Traces vs. Debugs
- Licensing
- Mobility
- AP Join
- Client flow
- HA AP-SSO

© 2015 Cisco and/or its affiliates. All rights reserved.

Troubleshooting Tools

What is needed…

- Problem definition
  - Identify the issue(s)
  - Reduce the scope of investigation
- Capture
  - L1: Spectrum Expert
  - L2/L3: Wireless sniffer trace (Omnipeek, AirPcap, Sniffer mode AP, Netmon etc..)
- Configuration check
  - Configuration analysis: WLC Config Analyser (WLCCA) – Coming soon!
- Debugging
  - Proper traces/debugs
  - Custom made tool
  - Editor tools (text processing)

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

System Level Sanity Check

- Memory utilisation
- CPU utilisation
- SUP8E Wireless Requirements

- Just an overview, for more details refer to:
  BRKCRS-3146 - Troubleshooting Cisco Catalyst 3850 Series Switches

© 2015 Cisco and/or its affiliates. All rights reserved.

Memory Utilisation

Show Commands

```
3850-1#show processes memory sorted

System memory   : 1941580K total, 1109004K used, 832576K free, 118584K kernel reserved
Lowest(b)       : 215392912
PID      Text          Data       Stack      Heap       RSS        Total      Process
9136     56944         33900      92         3872       192152     323428     iosd
5542     15040         307580     92         3648       122832     595900     fed
9132     21980         557376     88         10544      105796     721672     wcm
6035     4             94196      116        88484      95508      113168     idope.py
5544     836           159180     88         4088       55092      330104     stack-mgr
10083    4             144128     236        18136      46260      240788
wnweb_paster.py
6203     3532          132904     88         872        45868      339972     ffm
6219     112           153364     88         7420       44208      225500     cli_agent
6204     1232          256752     88         9060       33124      363320     eicored
6195     52            113340     88         1188       24820      206348     pdsd
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Memory Utilisation

Show Commands

```
3850-1#show processes memory detailed process iosd sorted

Processor Pool Total:  268435456 Used:  133113932 Free:  135321524
IOS Proce Pool Total:   16777216 Used:    9425820 Free:    7351396
 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
   0   0  169226784   33615104  125812548          0          0 *Init*
 163   0    1534944          0    1558112     907264          0 NGWC DOT1X Proce
   0   0          0          0     918996          0          0 *MallocLite*
   0   0    7235404    5923276     618844   40708507    1348801 *Dead*
 275   0     933472     297340     572084          0          0 os_info_p provid
   1   0     524640       1544     547808          0          0 Chunk Manager
 342   0     270484          0     296652     102676          0 EEM ED Syslog
  33   0   48903984   39285468     292800          0          0 SPI PL client ap
 352   0     223176          0     246344          0          0 EEM Server
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Memory Utilisation

Common Causes

Common Cause	Recommended Solution
Extensive config	Reduce the configuration to supported scale
Excessive memory allocated to trace buffers	Reset trace buffers to default sizes
DoS Attack/Punted traffic causing buffer depletion	Identify packets and block them using an ACL
Protocol flaps/re-convergence causing high transient memory utilisation	Identify reason for network instability
Memory leak caused by software bug	Open a TAC Service Request

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

CPU Utilisation

Show Commands

```
3850-1#show processes cpu sorted

Core 0: CPU utilization for five seconds: 3%; one minute: 5%;  five minutes: 5%
Core 1: CPU utilization for five seconds: 0%; one minute: 1%;  five minutes: 0%
Core 2: CPU utilization for five seconds: 0%; one minute: 0%;  five minutes: 0%
Core 3: CPU utilization for five seconds: 1%; one minute: 1%;  five minutes: 1%
PID    Runtime(ms) Invoked  uSecs  5Sec     1Min     5Min     TTY   Process
5542   1452240     25452052 57     0.63     0.59     0.56     1088  fed
9136   2528710     47631614 53     0.49     0.48     0.48     0     iosd
6206   918720      801369   1146   0.15     0.14     0.15     0     cpumemd
6200   75900       786850   96     0.05     0.01     0.03     0     mem_mgmt
6228   17950       2228827  8      0.05     0.05     0.01     0     snmp_subagent
9132   984350      37970483 25     0.05     0.12     0.11     0     wcm
1      1850        1066     1735   0.00     0.00     0.00     0     init
2      0           122      0      0.00     0.00     0.00     0     kthreadd
3      40          3323     12     0.00     0.00     0.00     0     migration/0
4      0           3        0      0.00     0.00     0.00     0     sirq-high/0
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

CPU Utilisation

Show Commands

```
3850-1#show processes cpu detailed process iosd sorted

Core 0: CPU utilization for five seconds: 8%; one minute: 4%; five minutes: 4%
Core 1: CPU utilization for five seconds: 0%; one minute: 5%; five minutes: 2%
Core 2: CPU utilization for five seconds: 0%; one minute: 0%; five minutes: 0%
Core 3: CPU utilization for five seconds: 1%; one minute: 3%; five minutes: 1%
PID    T C  TID    Runtime(ms) Invoked uSecs  5Sec      1Min      5Min     TTY   Process
                                             (%)       (%)       (%)
9136   L          2531310     4767539 53     1.16      0.62      0.52     0     iosd
9136   L 1  9136   2331260     4667549 0      1.06      0.52      0.43     0     iosd
9136   L 0  9919   200000      997609  0      0.10      0.10      0.08     0     iosd.fastpath
9136   L 1  9920   50          2282    0      0.00      0.00      0.00     0     iosd.aux
6      I          419250      38598   0      3.33      0.44      0.22     0       Check heaps
2      I          610         30677   0      0.00      0.00      0.00     0       Load Meter
3      I          0           9       0      0.00      0.00      0.00     0       SpanTree 4
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

SUP8E Requirements

What is needed…

- Main Release 3.7+ and Rommon Version 15.1(1r)SG4
- VSS is not supported in Wireless mode
- Wireless is supported only in UniversalK9 (crypto) image, Install Boot (Recommended for Wireless)
- Enterprise Services/ IP Base license
- Daughter card failures are considered as SUP failures and triggers SSO switchover in wireless mode

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Traces vs Debugs

- Traces are not displayed on console/terminal, but stored in a circular buffer
- Traces are “always-on”, you can change the level and filtering options
- Traces are less impactful on system performance

- **Traces are preferred for troubleshooting wireless issues!**

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Using Traces

- Set the trace level to debug for the trace we want to collect

```
3850-1#set trace capwap ap event level debug
  debug   Debug-level messages (7)
  default Unset Trace Level Value
  err     Error conditions (3)
  info    Informational (6)
  warning Warning conditions (4)
```

  - To turn off the trace debugging, set the level back to default

- Set and remove the filter for the MAC address

```
3850-1#set trace capwap ap event filter mac xxxx.xxxx.xxxx
3850-1#set trace capwap ap event filter mac yyyy.yyyy.yyyy
3850-1#set trace capwap ap event filter none
```

Adding multiple addresses to the filter list

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Using Traces

- To view unfiltered output:
  - **show trace message <feature>**
- To view filtered output:
  - **show trace sys-filtered-traces**
  - **show trace messages <feature> filtered**
- Several macros are available to enable sets of traces, example:
  - **set trace group-wireless-secure level debug**
- Clear a trace
  - **set trace control <feature> clear**
- Redirect the output to a file for easier offline analysis:
  - **show trace message <feature> | redirect tftp:…**
  - **show trace message <feature> | tee tftp:…**

Feature list:
show trace all-buffer settings

3.3+

File only

Console + File

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Getting Started

Before a client can join, basics must be covered:

- Licensing setup
- Establish mobility relationships
- Have APs to join the controllers

© 2015 Cisco and/or its affiliates. All rights reserved.

Licensing
What is Needed..

- Must run ipservices or ipbase license to enable wireless services on 3850 / 3650

```
3850-2#show license right-to-use
 Slot#  License name    Type       Count    Period left
--------------------------------------------------------
 1      ipservices      permanent      N/A    Lifetime
 1      ipbase          permanent      N/A    Lifetime
 1      apcount         adder          50     Lifetime

License Level on Reboot: ipservices
```

- The 5760 does not have activated license levels, the image is already ipservices

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Count Licenses

- AP count licenses are applied at the MC and are automatically provisioned and enforced at the MA
  - 3650 acting as MC can support up to 25 APs
  - 3850 acting as MC can support up to 50 APs
  - 5760 acting as MC can support up to 1000 APs
  - SUP8E acting as MC can support up to 50 APs

```
c5760-1#show license right-to-use summary
  License Name    Type      Count    Period left
------------------------------------------------
  apcount       base        0         Lifetime
  apcount       adder       25        Lifetime

------------------------------------------------

Evaluation AP-Count: Disabled
Total AP Count Licenses: 25
AP Count Licenses In-use: 4
AP Count Licenses Remaining: 21
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mobility Configuration

Mobility Agent and Mobility Controller

- The **3850 / SUP8E and 3650 are Mobility Agent** (MA) by default
- **AP licensing** is handled by the **Mobility Controller** (MC)
- Must either set a 3850/3650/SUP8E as mobility controller or point it to another device acting as MC

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mobility Configuration

Mobility Agent and Mobility Controller

- To configure a 3850 as a MC:

```
MC(config)# wireless mobility controller
```

  - NOTE: This configuration change will require a reboot!

- To point the 3850 to a different MC:

```
MA(config)# wireless mobility controller ip a.b.c.d
```

- And on the MC (define the SPG and add an MA to it):

```
MC(config)#wireless mobility controller peer-group <SPG1>
MC(config)#wireless mobility controller peer-group <SPG1> member ip w.x.y.z
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mobility Troubleshooting

Show Commands

```
c5760-1#show wireless mobility summary

Mobility Role                                    : Mobility Controller
~cut~

Controllers configured in the Mobility Domain:

IP               Public IP        Group Name       Multicast IP     Link Status
------------------------------------------------------------------------------
192.168.151.21   -                5760             0.0.0.0          UP   : UP

Switch Peer Group Name           : group1
~cut~

IP               Public IP             Link Status
-----------------------------------------------
192.168.151.11   192.168.151.11        UP   : UP
192.168.151.12   192.168.151.12        UP   : UP
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mobility Troubleshooting

Protocols

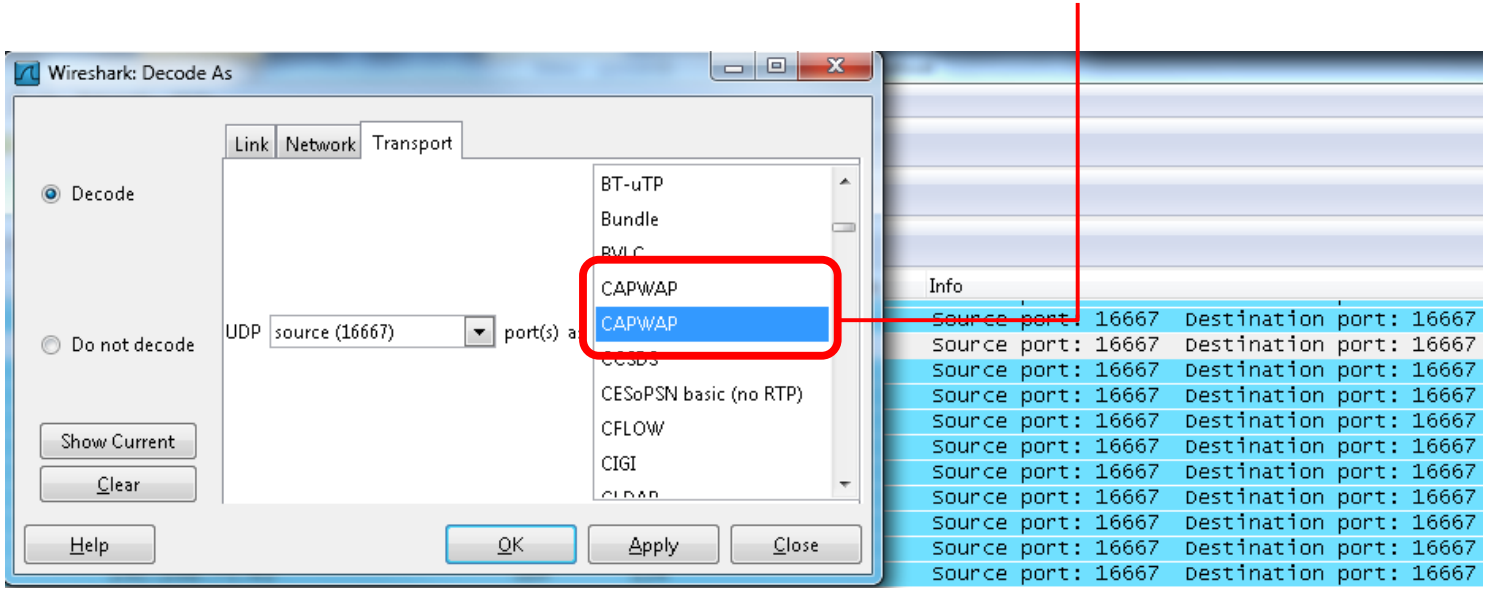
- Control Path
  - UDP port 16666
  - CAPWAP (control) encapsulated
  - DTLS Encrypted
- Data Path
  - UDP port 16667
  - CAPWAP (data) encapsulated
- Mobility Oracle
  - UDP port 16668
  - CAPWAP (control) encapsulated
  - DTLS Encrypted

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mobility Troubleshooting

Capturing Data

- In wireshark, you can click on a UDP port 16667 (data) packet
  - Right click -> Decode as -> CAPWAP Data (will be the 2nd CAPWAP entry in the list)



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mobility Troubleshooting

Capturing Data

- Now the traffic will be properly decoded and viewable:

192.168.75.1	192.168.75.116	ICMP	128	Echo (ping) reply
192.168.75.116	192.168.75.1	ICMP	124	Echo (ping) request
192.168.75.1	192.168.75.116	ICMP	128	Echo (ping) reply
192.168.75.116	192.168.75.1	ICMP	124	Echo (ping) request
192.168.75.1	192.168.75.116	ICMP	128	Echo (ping) reply

0.0.0.0	255.255.255.255	DHCP	411	DHCP Request
192.168.75.1	192.168.75.116	DHCP	396	DHCP ACK

- Allowing you to view communications such as ICMP or DHCP, to assist in packet loss diagnosis

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mobility Troubleshooting

Traces and Debugs

Traces

- set trace mobility handoff level debug
- set trace mobility keepalive level debug

Debugs

- debug mobility keep-alive
- debug mobility handoff
- debug mobility peer-ip w.x.y.z
- debug capwap ios event
- debug capwap ios error

MC-MA, or MA-MA troubleshooting

WLC internal capwap (WLC to WLC, etc)

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mobility Troubleshooting

MA Disconnected

```
5760# debug mobility peer-ip 10.10.20.6

*Oct  9 20:27:43.564: %IOSXE-7-PLATFORM: 1 process wcm: A unsolicited configdownload
response with subtype 2 sent to MA 10.10.20.6.^M
*Oct  9 20:27:43.564: %IOSXE-7-PLATFORM: 1 process wcm: [679: Configdownload
response MC->MA] to 10.10.20.6:16666
*Oct  9 20:27:43.564: %IOSXE-3-PLATFORM: 1 process wcm: *eicore_ipc: %MM-3-end
CONFIGDOWNLOAD_FAILED: Failed to send a config download response packet sending
packet to 10.10.20.6.
*Oct  9 20:27:44.014: %IOSXE-7-PLATFORM: 1 process wcm: Received keepalive status
change message type:1 ,peer Ip 10.10.20.6
*Oct  9 20:27:44.411: %IOSXE-7-PLATFORM: 1 process wcm: [679: Configdownload
response MC->MA] to 10.10.20.6:16666
*Oct  9 20:27:44.998: %SYS-5-CONFIG_I: Co
*Oct  9 20:27:45.403: %IOSXE-7-PLATFORM: 1 process wcm: [679: Configdownload
response MC->MA] to 10.10.20.6:16666
```

No ACK from MA

Retry

Keepalive status change... To “not responding”

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mobility Troubleshooting

MC Managing MA – Centralised Monitoring

- You can see MA states from the MC:

```
Cat3850-DEMO-MC# show wireless mobility summary  (snippet)
Mobility Controller Summary:

Mobility Role                                   : Mobility Controller
Mobility Protocol Port                          : 16666
Mobility Group Name                             : default
Mobility Oracle IP Address                      : 0.0.0.0
DTLS Mode                                       : Enabled
Mobility Domain ID for 802.11r                  : 0xac34
Mobility Keepalive Interval                     : 10
Mobility Keepalive Count                        : 3
Mobility Control Message DSCP Value             : 48
Mobility Domain Member Count                    : 1

IP                Public IP         Link Status     Centralized (Cfgd : Running)
------------------------------------------------------------------------------
1.1.1.1           1.1.1.1           UP    : UP      Enabled         Enabled
3.3.3.1           3.3.3.1           DOWN  : DOWN    Enabled         Enabled
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mobility Troubleshooting

MC Managing MA – Centralised Monitoring

- Main issue you will face comes from Hybrid models, where local config is done on MA, then config is pushed from MC for the same
  - System is built to show you mismatches from MC console
  - If all members fail with the same error, the error message is summarised

```
MC(config-wlan)#client vlan VLAN0100
All: % switch-1:wcm:Request failed - WLAN in the enabled state.
```

  - If errors are not same, the error messages will be displayed individually

```
MC(config-wlan)#client vlan VLAN0100
MA1: % switch-1:wcm:Request failed - WLAN in the enabled state.
MA2: % switch-1:wcm:Request failed - Invalid WLAN.
```

Seen from MC CLI

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Join

Config on 3850

- Enable wireless management

```
3850a(config)# wireless management interface vlan <1-4095>
```

What if “no…”?

- Directly connected APs must be configured as **access** port in the wireless management vlan!

```
3850a(config)#interface gigabit1/0/10
3850a(config-if)#switchport mode access
3850a(config-if)#switchport access vlan 151
```

```
3850(config-if)#switchport mode trunk
Command rejected: Conflict with Capwap

3850(config-if)#switchport mode trunk
3850(config-if)#
```

If AP exists on this port, WLC will reject switch to trunk port

However, if no AP is detected...

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Join

Verify Directly Joined APs (MA and MC)

- show ap summary

```
3850-2#show ap summary
Number of APs: 2

Global AP User Name: Not configured
Global AP Dot1x User Name: Not configured

AP Name                          AP Model  Ethernet MAC    Radio MAC       State
-------------------------------------------------------------------------------
ap1140-sw3850-2-2                1142N     0022.bd1a.d42b  0026.cbd2.6750  Registered
ap1140-sw3850-2-1                1142N     c84c.75f3.e788  18ef.639b.f9d0  Registered
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Join

Verify (sub-)domain Joined APs (MC)

- show wireless mobility ap-list

```
c5760-1#show wireless mobility ap-list
Number of AP entries in the mobility group : 3
Number of AP entries in the sub-domain     : 3

AP name                                  AP radio MAC      Controller IP     Learnt from
-----------------------------------------------------------------------------------------
ap1140-sw3850-2-2                        0026.cbd2.6750    192.168.151.12    Mobility Agent
ap2600-sw3850-3-11                       04da.d24f.f1e0    192.168.151.21    Self
ap1140-sw3850-2-1                        18ef.639b.f9d0    192.168.151.12    Mobility Agent

Controller IP      AP Count
----------------------------
192.168.151.12     2
192.168.151.21     1
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Join Troubleshooting

Typical Issues

- Licensing
- Regulatory domain mismatch
- AP not on wireless management VLAN (3850)
- Certificate validation (time)

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Join

Traces and Debugs

Traces

- set trace group-ap level debug
- set trace group-ap filter mac xxxx.xxxx.xxxx

Debugs

- debug capwap **ap** events
- debug capwap **ap** error

Note: No filter functionality

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Join Troubleshooting

Licensing

- Is the MA configured to talk with an MC?

```
[12/30/13 03:17:36.802 UTC f0e9 8531] 0026.cbd2.6750 License is denied for the AP,
calling the AP reset

[12/30/13 03:17:36.802 UTC f0ea 8531] 0026.cbd2.6750 Reset request sent to
192.168.151.13:44356

[12/30/13 03:17:36.802 UTC f0eb 8531] 0026.cbd2.6750 License check failed: License
is denied for the AP, calling the AP reset
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Join Troubleshooting

Licensing

- Verify: 3850-2#show wireless mobility summary

```
Mobility Agent Summary:

Mobility Role                                          : Mobility Agent

Link Status is Control Link Status : Data Link Status

The status of Mobility Controller:

IP              Public IP             Link Status
-----------------------------------------------
0.0.0.0         0.0.0.0               -    : -
```

- Fix: 3850-2(config)#wireless mobility controller ip …

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Join Troubleshooting

Invalid Country Code

```
*Dec 16 08:33:12.790: *%LWAPP-3-RD_ERR8: 1 wcm:  Country code (ES ) not configured
for AP 18:ef:63:9b:f9:d0
*Dec 16 08:33:12.791: *%LOG-3-Q_IND: 1 wcm:  Country code (ES ) not configured for
AP 18:ef:63:9b:f9:d0
*Dec 16 08:33:12.792: *%LWAPP-3-VALIDATE_ERR: 1 wcm:  Validation of SPAM Vendor
Specific Payload failed - AP  18:ef:63:9b:f9:d0
*Dec 16 08:33:12.793: *%LOG-3-Q_IND: 1 wcm:  Validation of SPAM Vendor Specific
Payload failed - AP  18:ef:63:9b:f9:d0
*Dec 16 08:33:12.793: *%LWAPP-3-RD_ERR8: 1 wcm:  Country code (ES ) not configured
for AP 18:ef:63:9b:f9:d0
*Dec 16 08:33:12.793: *%LWAPP-3-RD_ERR4: 1 wcm:  Invalid regulatory domain
802.11bg:-A     802.11a:-A for AP 18:ef:63:9b:f9:d0
```

- Verify: `3850-2#show wireless country configured`

```
Configured Country.............................: US  - United States
```

- Fix: `3850-2(config)#ap country ?`

```
  WORD  Enter the country code (e.g. US,MX,IN) up to a maximum of 20 countries
```

Must shutdown 2.4 and 5

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Join Troubleshooting - 3850

APs must be in Wireless Management VLAN

```
Oct  9 12:57:45.362: %IOSXE-7-PLATFORM: 1 process wcm: 64D9.8946.CA30 Received a
Discovery Request from 64:d9:89:46:ca:30 on an unsupported VLAN 1.
srcIp(172.29.129.178) dstIp(10.10.20.2) Dropping the discovery request. AP will not
be able to join as it is on a different vlan than management or AP manager vlan
Oct  9 12:57:45.362: %IOSXE-7-PLATFORM: 1 process wcm: 64D9.8946.CA30 Unable to
process Discovery Request from 64d9.8946.ca30 due to missing AP Manager interface,
discovery request received on interface 65535 vlanId 1 srcIp(172.29.129.178)
dstIp(255.255.255.255)
Oct  9 12:57:45.363: %IOSXE-3-PLATFORM: 1 process wcm: *spamApTask0: %CAPWAP-3-
DISC_WIRELESS_INTERFACE_ERR1: Unable to process discovery request from AP
64d9.8946.ca30 , VLAN (1) scrIp (172.29.129.178) dstIp(255.255.255.255), could not
get wireless interface belonging to this network
```

- Verify:

```
3850-2#show wireless interface summary
Interface Name  Interface Type  VLAN ID  IP Address      IP Netmask      MAC Address
-----------------------------------------------------------------------------------
Vlan151         Management      151      192.168.151.12  255.255.255.0   44ad.d96c.77cd
```

- Fix:

```
3850-2(config)#interface gi1/0/1
3850-2(config-if)#switchport access vlan 151
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Join Troubleshooting - 5760

Certificate Validation

```
Jan  1 12:14:04.539: %IOSXE-7-PLATFORM: 1 process wcm: 64D9.8946.B640 Discovery
Request from 10.10.22.31:9618
Jan  1 12:14:04.539: %IOSXE-7-PLATFORM: 1 process wcm: 64D9.8946.B640 Join Priority
Processing status = 0, Incoming Ap's Priority 0, MaxLrads = 1000, joined Aps =0
Jan  1 12:14:04.539: %IOSXE-7-PLATFORM: 1 process wcm: 64D9.8946.B640 Validated
Discovery request with dest ip : 10.10.21.3 from AP  10.10.22.31. Response to be
sent using ip : 10.10.21.3


Jan  1 12:14:14.551: %IOSXE-3-PLATFORM: 1 process wcm: *spamApTask1: %DTLS-3-
HANDSHAKE_FAILURE: Failed to complete DTLS handshake with peer 10.10.22.31  Reason:
sslv3 alert bad certificate

5760#show clock
12:20:27.298 UTC Mon Jan 1 2001
```

AP on different subnet, no problem so far...

- Fix: `3850-2#clock set …`
  `3850-2(config)#ntp server …`

NTP!

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

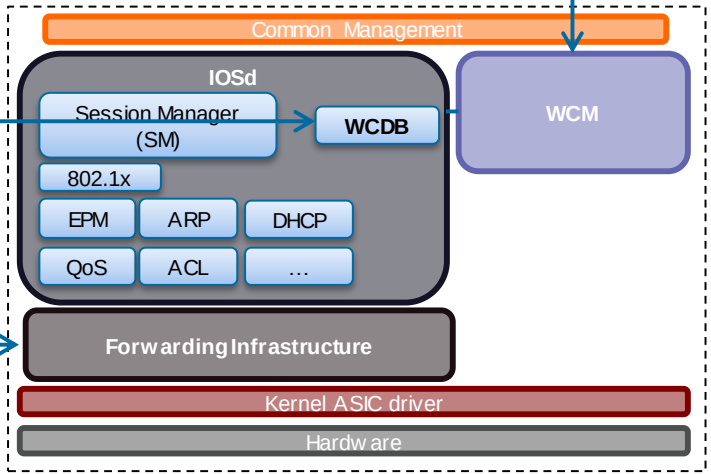
Client Troubleshooting

- 802.11 Authentication
- 802.11 (Re-)Association
- L2 Authentication (802.1x/PSK)
- Mobility discovery
- Client address learning
- L3 Authentication (Web-auth)
- Forwarding
- Roaming

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

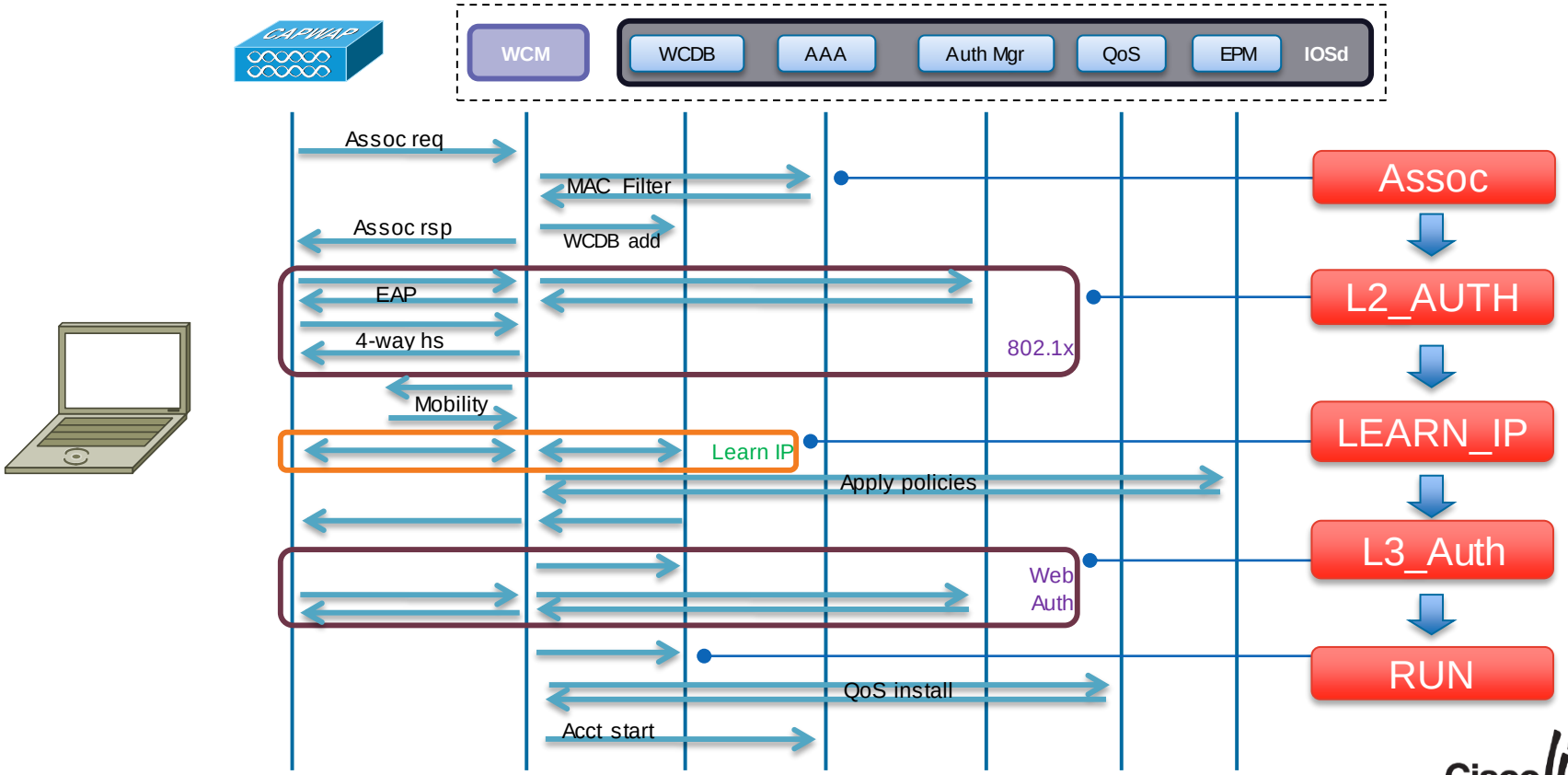
Wireless Client Details

- Client information maintained in 3 main processes
- **WCM**
  - **show wireless client mac-address xxxx.xxxx.xxxx detail**
  - **show wireless client username <username>**
- **IOSd WCDB**
  - **show wcdb database all**
  - **show wcdb database xxxx.xxxx.xxxx**
- **Platform (FED)**
  - **show platform wcdb summary**
  - **show platform wcdb clientIndex <client-index> summary**



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Flow and States



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Troubleshooting

Traces and Debugs

Traces

- set trace group-wireless-client filter mac xxxx.xxxx.xxxx
- set trace group-wireless-client level debug

Open auth

- set trace group-wireless-secure filter mac xxxx.xxxx.xxxx
- set trace group-wireless-secure level debug

L2 auth (3.3SE+)

Debugs

- debug client mac-address xxxx.xxxx.xxxx
- debug wcm-dot1x trace
- debug wcm-dot1x event
- debug wcm-dot1x error

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

802.11 Authentication

- Handled by the Access Point
- Not visible at WLC logs/debugs
- Debugging has to be done at radio driver level (AP):

```
ap# debug dot11 dot11radio0 monitor addr xxxx.xxxx.xxxx
ap# debug dot11 dot11radio0 trace print client mgmt
```

Radio slot:
0 = 2.4 GHz
1 = 5 GHz

MAC filter

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Flow

The Route Toward the RUN State!

© 2015 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Client Association

Success!

Assoc

```
[04/27/13 14:38:47.659 CST 350c 9120] 6896.7B0D.F3BB Association received from mobile on
AP  10BD.186D.9A40
~cut~
for station  6896.7B0D.F3BB  - vapId 1, site 'default-group', interface 'VLAN0079'
[04/27/13 14:38:47.660 CST 3513 9120] 6896.7B0D.F3BB Applying local bridging Interface
Policy for station  6896.7B0D.F3BB  - vlan 79, interface 'VLAN0079'
[04/27/13 14:38:47.660 CST 3514 9120] 6896.7B0D.F3BB STA - rates (8): 130 132 139 150 36
48 72 108 0 0 0 0 0 0 0 0
[04/27/13 14:38:47.660 CST 3515 9120] 6896.7B0D.F3BB STA - rates (12): 130 132 139 150 36
48 72 108 12 18 24 96 0 0 0 0
[04/27/13 14:38:47.660 CST 3518 9120] 6896.7B0D.F3BB WCDB_ADD: ssid ciscolive bssid
10BD.186D.9A40 vlan 79 auth=ASSOCIATION(0) wlan(ap-group/global) 1/1 client 0 assoc 1
mob=Unassoc(0) radio 0 m_vlan 79 ip 0.0.0.0 src 0xcf3d4000000006 dst 0x0 cid
0xd3ae0000000079 glob rsc id 111dhcpsrv  14.
~cut~
Changing state for mobile  6896.7B0D.F3BB  on AP  10BD.186D.9A40  from Idle to Associated
[04/27/13 14:38:47.660 CST 351c 9120] 6896.7B0D.F3BB Ms Timeout = 0, Session Timeout = 0
[04/27/13 14:38:47.661 CST 351d 9120] 6896.7B0D.F3BB Sending Assoc Response to station on
BSSID  10BD.186D.9A40  (status 0) ApVapId 1 Slot 0
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless PCAP

IntelCor_89:51:ca	Broadcast	802.11	78	Probe Request, SN=3659, FN=0, Fla
Cisco_83:42:6e	IntelCor_89:51:ca	802.11	268	Probe Response, SN=2825, FN=0, Fl
IntelCor_89:51:ca	Cisco_83:42:6e	802.11	78	Probe Request, SN=3672, FN=0, Fla
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	802.11	268	Probe Response, SN=2826, FN=0, Fl
IntelCor_89:51:ca	Cisco_83:42:6e	802.11	34	Authentication, SN=3673, FN=0, Fl
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	802.11	34	Authentication, SN=1859, FN=0, Fl
IntelCor_89:51:ca	Cisco_83:42:6e	802.11	161	Association Request, SN=3674, FN=
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	802.11	180	Association Response, SN=1860, FN=

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Association

Assoc

IE Processing

```
STA - rates (12): 130 132 139 150 12 18 24 36 48 72 96 108 0 0 0 0
Processing RSN IE type 48, length 22 for mobile 00:16:ea:b2:04:36
```

- STA - rates
  Mandatory Rates (>128) = (#-128)/2
  Supported Rates (<128) = #/2
  1m,2m,5.5m,11m,6s,9s,12s,18s,24s,36s,48s,54s
- Processing **RSN IE type 48** WPA2-AES
  Processing WPA IE type 221 WPA-TKIP

For more info:
IEEE 802.11-2012
8.4.2.27 RSNE

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Association

Association Response

Assoc

```
Sending Assoc Response to station on BSSID 00:26:cb:94:44:c0 (status 0) ApVapId 1
Slot 0
```

- **Slot 0** = B/G(2.4) Radio
  Slot 1 = A(5) Radio
- Sending Assoc Response **Status 0** = Success
  Anything other than Status 0 is Failure

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Association

Assoc

Typical Issues

- Configuration related
  - Radio/WLAN shutdown
  - Data rate config mismatch
  - WMM policy mismatch
  - MAC filtering failure
- Scaling related
  - Max number of clients on radio interface
  - Call Admission Control (CAC)
- Client in exclusion list
- Client Idle

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Association

Assoc

Excluded Client

- Client in exclusion list

```
*Dec 23 17:31:08.089: %IOSXE-7-PLATFORM: 1 process wcm: 0023.6907.e218 Ignoring
assoc request due to mobile in exclusion list or marked for deletion
```

- Check client exclusion

```
c5760-1# show wireless exclusionlist
```

- Remove a client from exclusion list (deauth)

```
c5760-1# wireless client mac-address xxxx.xxxx.xxxx deauthenticate
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Idle

- Client state as Idle

```
3850-2# show wireless client summary
Number of Local Clients : 1

MAC Address    AP Name                                  WLAN State                 Protocol
-------------------------------------------------------------------------------------------
0023.6907.e218 ap1140-sw3850-2-2                        2    Idle                  11n(2.4)
```

- Upon client association traces usually show…

```
Ignoring 802.11 assoc request from mobile pending deletion
```

- Different causes may lead to this state

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Idle

- Examples of reasons for client idle:
  - CSCug75799 – fixed in 3.2.3SE+
  - Incorrect QoS config
    For more info see BRKCRS-2890 - Converged Access Quality of Service

Available at CiscoLive365!

- Collect client idle troubleshooting info:

```
show tech-support platform wireless client mac-address xxxx.xxxx.xxxx
```

- Force deauth to recover the client:

```
wireless client mac-address xxxx.xxxx.xxxx deauthenticate forced
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Flow

The Route Toward the RUN State!

© 2015 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Layer 2 Authentication

L2_AUTH

Show Client Status

- WCM

```
3850-2#show wireless client summary
Number of Local Clients : 1

MAC Address    AP Name                                  WLAN State                 Protocol
-------------------------------------------------------------------------------------------
0023.6907.e218 ap1140-sw3850-2-2                        2    AUTHENTICATING        11g
```

- WCDB

```
3850-2#show wcdb database all

Mac Address    VlanId IP Address      Src If              Auth     Mob
-------------- ------ --------------- ------------------ -------- -------
0023.6907.e218    153 0.0.0.0         0x00C99740000006BC ASSOCIAT INIT
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco live!

Layer 2 Authentication

L2_AUTH

802.1x Successful Authentication

```
0021.6a89.51ca Association received from mobile on AP  c8f9.f983.4260
0021.6a89.51ca Sending Assoc Response to station on BSSID  c8f9.f983.4260  (status 0)
ApVapId 2 Slot 1
0021.6a89.51ca 1XA: Session Start from wireless client
ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0021.6a89.51ca, Ca2] Session start request from
Client[1] for 0021.6a89.51ca (method: Dot1X, method list: ACS, aaa id: 0x0000037C)
ACCESS-METHOD-DOT1X-DEB: [0021.6a89.51ca, Ca2] Posting !EAP_RESTART on Client 0x2000000E
ACCESS-METHOD-DOT1X-NOTF: [0021.6a89.51ca, Ca2] Sending EAPOL packet
ACCESS-METHOD-DOT1X-INFO: [0021.6a89.51ca, Ca2] EAPOL packet sent to client 0x2000000E
ACCESS-METHOD-DOT1X-NOTF: [0021.6a89.51ca, Ca2] Response sent to the server from
0x2000000E
ACCESS-METHOD-DOT1X-DEB: [0021.6a89.51ca, Ca2] 0x2000000E:request response action
AAA SRV(00000000): process authen req
AAA SRV(00000000): Authen method=SERVER_GROUP ACS
AAA SRV(00000000): protocol reply GET_CHALLENGE_RESPONSE for Authentication
AAA SRV(00000000): Return Authentication status=PASS
ACCESS-METHOD-DOT1X-INFO: [0021.6a89.51ca, Ca2] Received an EAP Success
ACCESS-METHOD-DOT1X-NOTF: [0021.6a89.51ca, Ca2] Received Authz Success for the client
0x2000000E (0021.6a89.51ca)
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 2 Authentication

AP Radio Debugs

*Jan 15 02:50:07.804: A6504097 t 1 3 - B008 2800 2FB698 6F9E11 6F9E11 CFC0 auth l 6

*Jan 15 02:50:07.807: A6504BC0 r 1 69/67 14- B008 13A 6F9E11 2FB698 6F9E11 65C0 auth l 6

*Jan 15 02:50:07.809: A6505313 r 1 69/67 19- 0000 13A 6F9E11 2FB698 6F9E11 65D0 assreq l 139

*Jan 15 02:50:07.827: A6509A92 t 1 2 - 1008 000 2FB698 6F9E11 6F9E11 CFE0 assrsp l 151

*Jan 15 02:50:07.829: A650A056 t 1 0 - 8802 000 2FB698 6F9E11 6F9E11 0290 q7 l87

EAPOL3 EAP id 93 req ident 0 "networkid=peapradius,nasid=SURBG-5760,portid=0"

*Jan 15 02:50:07.879: A6516524 r 1 68/67 19- 8801 13A 6F9E11 2FB698 6F9E11 0010 q7 l22

EAP id 93 resp ident "surbg"

|

Rest of the EAP Transaction

|

*Jan 15 02:50:08.247: A6570622 t 1 0 - 8802 000 2FB698 6F9E11 6F9E11 0330 q7 l54

EAPOL3 EAP id 237 success

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless PCAP

IntelCor_89:51:ca	Cisco_83:42:6e	EAPOL	43	Start
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	EAP	117	Request, Identity
IntelCor_89:51:ca	Cisco_83:42:6e	EAP	52	Response, Identity
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	EAP	84	Request, TLS EAP (EAP-TLS)
IntelCor_89:51:ca	Cisco_83:42:6e	EAP	48	Response, Legacy Nak (Response Only)
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	EAP	84	Request, Protected EAP (EAP-PEAP)
IntelCor_89:51:ca	Cisco_83:42:6e	TLSv1	188	Client Hello
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	TLSv1	543	Server Hello, Certificate, Server Hel
IntelCor_89:51:ca	Cisco_83:42:6e	TLSv1	186	Client Key Exchange, Change Cipher Sp
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	TLSv1	107	Change Cipher Spec, Encrypted Handsha
IntelCor_89:51:ca	Cisco_83:42:6e	EAP	48	Response, Protected EAP (EAP-PEAP)
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	TLSv1	85	Application Data
IntelCor_89:51:ca	Cisco_83:42:6e	TLSv1	85	Application Data
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	TLSv1	117	Application Data
IntelCor_89:51:ca	Cisco_83:42:6e	TLSv1	149	Application Data
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	TLSv1	133	Application Data
IntelCor_89:51:ca	Cisco_83:42:6e	TLSv1	85	Application Data
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	TLSv1	85	Application Data
IntelCor_89:51:ca	Cisco_83:42:6e	TLSv1	85	Application Data
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	EAP	84	Success

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 2 Authentication

L2_AUTH

Typical Issues

- RADIUS server reachability
- Reject from RADIUS server
  - invalid credentials, certificate validation, max sessions…
- EAP timeout
- AAA override
- Incorrect Pre-Shared Key

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 2 Authentication

L2_AUTH

802.1x Auth Fail – RADIUS Timeout

```
ACCESS-METHOD-DOT1X-DEB: [0021.6a89.51ca, Ca3] Posting EAPOL_EAP for 0x1A000001
ACCESS-METHOD-DOT1X-DEB: [0021.6a89.51ca, Ca3] 0x1A000001:entering response state
ACCESS-METHOD-DOT1X-NOTF: [0021.6a89.51ca, Ca3] Response sent to the server from
0x1A000001
ACCESS-METHOD-DOT1X-NOTF: [0021.6a89.51ca, Ca3] Received an EAP Fail
ACCESS-METHOD-DOT1X-DEB: [0021.6a89.51ca, Ca3] Posting EAP FAIL for 0x1A000001
ACCESS-CORE-SM-NOTF: [0021.6a89.51ca, Ca3] Authc failure from Dot1X (1), status AAA
Server Down (2) / event server dead (2)
ACCESS-CORE-SM-NOTF: [0021.6a89.51ca, Ca3] Highest prio method: INVALID, Authz method:
INVALID, Conn hdl: dot1x
ACCESS-CORE-SM-NOTF: [0021.6a89.51ca, Ca3] Client 0021.6a89.51ca, Method dot1x changing
state from 'Running' to 'Authc Failed'
0021.6a89.51ca 1XA: Authentication failed
0021.6a89.51ca 1XA: Sending deauth msg, Reason Code = 23
```

- Network connectivity issues?
- RADIUS server process running?

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco live!

Layer 2 Authentication

AP Radio Debugs

*Jan 15 07:21:36.347: 5BCB7C8F t 1 0 - 8802 000 2FB698 6F9E11 6F9E11 1890 q7 l87
EAPOL3 EAP id 2 req ident 0 "networkid=peapradius ,nasid=SURBG-5760,portid=0"

*Jan 15 07:21:36.374: 5BCBEDBF r 1 72/68 15- 8801 17A 6F9E11 2FB698 6F9E11 0000 q7 l13
EAPOL start
*Jan 15 07:21:36.379: 5BCC00E4 t 1 0 - 8802 000 2FB698 6F9E11 6F9E11 18A0 q7 l87
EAPOL3 EAP id 2 req ident 0 "networkid=peapradius,nasid=SURBG-5760,portid=0"
*Jan 15 07:21:38.515: 5BECA39F-0 2FB698 - pak flags 1
*Jan 15 07:21:38.515: 5BECA397 r 1 67/63 22- 8801 17A 6F9E11 2FB698 6F9E11 0010 q7 l22
EAP id 2 resp ident "surbg"

*Jan 15 07:22:17.159: 5E3AFECD r 1 67/63 22- A000 13A 6F9E11 2FB698 6F9E11 C1D0 disass l 2
reason 8

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless PCAP

Cisco_83:42:6e	IntelCor_89:51:ca	EAP	117	Request, Identity
IntelCor_89:51:ca	Cisco_83:42:6e	EAPOL	43	Start
Cisco_83:42:6e	IntelCor_89:51:ca	EAP	117	Request, Identity
IntelCor_89:51:ca	Cisco_83:42:6e	EAP	52	Response, Identity
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
IntelCor_89:51:ca	Cisco_83:42:6e	802.11	30	QoS Null function (No data), SN=2, FN=0, F
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
IntelCor_89:51:ca	Cisco_83:42:6e	EAPOL	43	Start
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	EAP	117	Request, Identity
IntelCor_89:51:ca	Cisco_83:42:6e	EAP	52	Response, Identity
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
IntelCor_89:51:ca	Cisco_83:42:6e	802.11	30	QoS Null function (No data), SN=5, FN=0, F
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
IntelCor_89:51:ca	Cisco_83:42:6e	802.11	40	Deauthentication, SN=2502, FN=0, Flags=....
Cisco_83:42:6e	IntelCor_89:51:ca	802.11	30	Deauthentication, SN=2132, FN=0,
Cisco_83:42:6e	IntelCor_89:51:ca	EAP	84	Failure
Cisco_83:42:6e	IntelCor_89:51:ca	EAP	84	Failure
Cisco_83:42:6e	IntelCor_89:51:ca	EAP	84	Failure

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 2 Authentication

L2_AUTH

EAP Timeout

```
[13:36:29.668] ACCESS-METHOD-DOT1X-INFO: [001a.7035.84d6, Ca2] EAPOL packet sent to
client 0x270001BD
[13:36:39.907] ACCESS-METHOD-DOT1X-NOTF: [001a.7035.84d6, Ca2] Received an EAP Timeout
[13:36:39.907] ACCESS-METHOD-DOT1X-DEB: [001a.7035.84d6, Ca2] Posting EAP_TIMEOUT for
0x270001BD
[13:36:39.907] ACCESS-METHOD-DOT1X-DEB: [001a.7035.84d6, Ca2] 0x270001BD:entering
timeout state
[13:36:39.907] ACCESS-METHOD-DOT1X-DEB: [001a.7035.84d6, Ca2] 0x270001BD:request timeout
action
[13:36:39.907] ACCESS-METHOD-DOT1X-DEB: [001a.7035.84d6, Ca2] 0x270001BD:entering idle
state
[13:36:39.907] ACCESS-METHOD-DOT1X-DEB: [001a.7035.84d6, Ca2] Posting AUTH_TIMEOUT on
Client 0x270001BD
[13:36:39.907] ACCESS-METHOD-DOT1X-DEB: [001a.7035.84d6, Ca2] 0x270001BD:exiting
authenticating state
[13:36:43.175] ACCESS-METHOD-DOT1X-NOTF: [001a.7035.84d6, Ca2] Override cfg -
SuppTimeout 10s ReAuthMax 3, MaxReq 2, TxPeriod 30s
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 2 Authentication

AP Radio Debugs

*Jan 15 06:57:07.757: 64DA85C t 1 0 - 8802 000 2FB698 6F9E11 6F9E11 1250 q7 l87
EAPOL3 EAP id 1 req ident 0 "networkid=peapradius,nasid=SURBG-5760,portid=0“

*Jan 15 06:57:07.786: 64E197E r 1 65/64 20- 8801 17A 6F9E11 2FB698 6F9E11 0000 q7 l13
EAPOL start
*Jan 15 06:57:07.789: 64E26BA t 1 0 - 8802 000 2FB698 6F9E11 6F9E11 1260 q7 l87
EAPOL3 EAP id 1 req ident 0 "networkid=peapradius ,nasid=SURBG-5760,portid=0"

*Jan 15 06:57:07.878: 64F80BE t 1 0 - 8802 000 2FB698 6F9E11 6F9E11 12A0 q7 l54
EAPOL3 EAP id 80 fail
*Jan 15 06:57:07.879: 64F8657 t 1 0 - 8802 000 2FB698 6F9E11 6F9E11 12B0 q7 l87
EAPOL3 EAP id 81 req ident 0 "networkid=peapradius,nasid=SURBG-5760,portid=0"
*Jan 15 06:57:07.924: 65035E3-0 2FB698 - pak flags 0

*Jan 15 06:57:07.924: 65035DD r 1 66/64 19- A000 13A 6F9E11 2FB698 6F9E11 A000 disass l 2
reason 8

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless PCAP

```
Cisco_83:42:6e     IntelCor_89:51:ca            802.11      268 Probe Response, SN=2868, FN=0, Flags=.
IntelCor_89:51:ca  Broadcast                    802.11       78 Probe Request, SN=51, FN=0, Flags=....
Cisco_83:42:6e     IntelCor_89:51:ca            802.11      268 Probe Response, SN=2869, FN=0, Flags=.
IntelCor_89:51:ca  Cisco_83:42:6e               802.11       78 Probe Request, SN=58, FN=0, Flags=....
                   IntelCor_89:51:ca (RA)       802.11       14 Acknowledgement, Flags=.........
Cisco_83:42:6e     IntelCor_89:51:ca            802.11      268 Probe Response, SN=2870, FN=0, Flags=.
IntelCor_89:51:ca  Cisco_83:42:6e               802.11       34 Authentication, SN=59, FN=0, Flags=...
                   IntelCor_89:51:ca (RA)       802.11       14 Acknowledgement, Flags=.........
Cisco_83:42:6e     IntelCor_89:51:ca            802.11       34 Authentication, SN=395, FN=0, Flags=..
IntelCor_89:51:ca  Cisco_83:42:6e               802.11      161 Association Request, SN=60, FN=0, Flag
                   IntelCor_89:51:ca (RA)       802.11       14 Acknowledgement, Flags=.........
Cisco_83:42:6e     IntelCor_89:51:ca            802.11      180 Association Response, SN=396, FN=0, Fl
Cisco_83:42:6e     IntelCor_89:51:ca            EAP         117 Request, Identity
IntelCor_89:51:ca  Cisco_83:42:6e               EAPOL        43 Start
                   IntelCor_89:51:ca (RA)       802.11       14 Acknowledgement, Flags=.........
Cisco_83:42:6e     IntelCor_89:51:ca            EAP         117 Request, Identity
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 2 Authentication

L2_AUTH

EAP Timers

- show run all | i wireless security dot1x

```
wireless security dot1x eapol-key retries 2
wireless security dot1x eapol-key timeout 1000
wireless security dot1x group-key interval 3600

wireless security dot1x identity-request retries 2
wireless security dot1x identity-request timeout 30
wireless security dot1x request retries 2
wireless security dot1x request timeout 30
```

- Trace output

```
ACCESS-METHOD-DOT1X-NOTF: [001a.7035.84d6, Ca2] Override cfg
- SuppTimeout 30s, ReAuthMax 2  MaxReq 2, TxPeriod 30s
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 2 Authentication

L2_AUTH

802.1x Auth Fail – Reject From AAA

```
0021.6a89.51ca Association received from mobile on AP  c8f9.f983.4260
0021.6a89.51ca Change state to AUTHCHECK (2) last state START (0)
0021.6a89.51ca Change state to 8021X_REQD (3) last state AUTHCHECK (2)
0021.6a89.51ca Session Manager Call Client 5bc3800000003b, uid 41, capwap id
4cd14000000012,Flag 4, Audit-Session ID 0a6987b252838f4b00000029, method list ACS
ACCESS-METHOD-DOT1X-DEB: [0021.6a89.51ca, Ca3] 0xD1000017:entering request state
ACCESS-METHOD-DOT1X-NOTF: [0021.6a89.51ca, Ca3] Sending EAPOL packet
0021.6a89.51ca 1XA: Received 802.11 EAPOL message (len 5) from mobile
0021.6a89.51ca 1XA: Received EAPOL-Start from mobile
ACCESS-METHOD-DOT1X-DEB: [0021.6a89.51ca, Ca3] Posting AUTH_ABORT for 0xD1000017
ACCESS-METHOD-DOT1X-NOTF: [0021.6a89.51ca, Ca3] Received an EAP Fail
ACCESS-CORE-SM-NOTF: [0021.6a89.51ca, Ca3] Authc failure from Dot1X (1), status Cred
Fail (1) / event fail (1)
```

- Incorrect credentials?
- User not found?
- Max sessions?
- Incorrect EAP method?

AAA Server Logs

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 2 Authentication

AP Radio Debug

*Jan 15 04:32:48.475: D7C337E r 1 68/62 20- B000 13A 6F9E11 2FB698 6F9E11 78A0 auth l 6

*Jan 15 04:32:48.475: D7C340C-0 2FB698 - newauth

*Jan 15 04:32:48.476: D7C38C3 t 1 0 - B000 001 2FB698 6F9E11 6F9E11 0000 auth l 6

*Jan 15 04:32:48.479: D7C43F8 r 1 69/62 14- 0000 13A 6F9E11 2FB698 6F9E11 78B0 assreq l 139

*Jan 15 04:32:48.495: D7C8598 t 1 0 - 1000 000 2FB698 6F9E11 6F9E11 0000 assrsp l 151

*Jan 15 04:32:48.497: D7C8B78 t 1 0 - 8802 000 2FB698 6F9E11 6F9E11 0710 q7 l87

EAPOL3 EAP id 1 req ident 0 "networkid=peapradius,nasid=SURBG-5760,portid=0"

*Jan 15 04:32:48.529: D7D09A4 r 1 69/62 21- 8801 17A 6F9E11 2FB698 6F9E11 0000 q7 l13

EAPOL start

*Jan 15 04:32:48.533: D7D170A t 1 0 - 8802 000 2FB698 6F9E11 6F9E11 0720 q7 l87

EAPOL3 EAP id 1 req ident 0 "networkid=peapradius ,nasid=SURBG-5760,portid=0"

*Jan 15 04:32:53.643: DCB28C0 r 1 69/62 20- 8801 17A 6F9E11 2FB698 6F9E11 0010 q7 l22

EAP id 1 resp ident "surbg"

*Jan 15 04:32:53.649: DCB3734 t 1 0 - C000 000 2FB698 6F9E11 6F9E11 0000 deauth l 2

reason 23

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless PCAP

IntelCor_89:51:ca	Cisco_83:42:6e	EAPOL	43	Start
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	EAP	117	Request, Identity
IntelCor_89:51:ca	Cisco_83:42:6e	EAP	50	Response, Identity
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	EAP	84	Request, TLS EAP (EAP-TLS)
IntelCor_89:51:ca	Cisco_83:42:6e	EAP	48	Response, Legacy Nak (Response Only)
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	EAP	84	Request, Protected EAP (EAP-PEAP)
IntelCor_89:51:ca	Cisco_83:42:6e	TLSv1	154	Client Hello
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	TLSv1	543	Server Hello, Certificate, Server H
IntelCor_89:51:ca	Cisco_83:42:6e	TLSv1	186	Client Key Exchange, Change Cipher
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	TLSv1	107	Change Cipher Spec, Encrypted Handsl
IntelCor_89:51:ca	Cisco_83:42:6e	EAP	48	Response, Protected EAP (EAP-PEAP)
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	TLSv1	85	Application Data
IntelCor_89:51:ca	Cisco_83:42:6e	TLSv1	85	Application Data
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	TLSv1	117	Application Data
IntelCor_89:51:ca	Cisco_83:42:6e	TLSv1	133	Application Data
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	TLSv1	85	Application Data
IntelCor_89:51:ca	Cisco_83:42:6e	TLSv1	85	Application Data
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6e	IntelCor_89:51:ca	EAP	84	Failure

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 2 Authentication

L2_AUTH

802.1x Auth Fail – AAA Override

```
[12/23/13 17:30:49.480 UTC a 8531] 0023.6907.e218 misconfiguration: client vlan not
enable, therefore blacklist the client
[12/23/13 17:30:49.480 UTC b 8531] 0023.6907.e218 apfBlacklistMobileStationEntry2
(apf_ms.c:6241) Changing state for mobile  0023.6907.e218  on AP  0026.cbd2.6750  from
Idle to Exclusion-list (1)
[12/23/13 17:30:49.480 UTC c 8531] 0023.6907.e218 Reason code 0, Preset 1, AAA cause 1
[12/23/13 17:30:49.480 UTC d 8531] 0023.6907.e218 Scheduling deletion of Mobile Station:
(callerId: 44) in 10 seconds
[12/23/13 17:30:49.480 UTC e 8531] 0023.6907.e218 client is added to the exclusion list,
reason 6
```

- Incorrect VLAN pushed by AAA?
- VLAN not defined or disabled locally?

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 2 Authentication

L2_AUTH

EAPOL Key Exchange

```
[05/15/13 16:21:45.430 CST 36e7 9120] 6896.7B0D.F3BB Starting key exchange with mobile -
data forwarding is disabled
[05/15/13 16:21:45.430 CST 36e8 9120] 6896.7B0D.F3BB 1XA: Sending EAPOL message to
mobile, WLAN=1 AP WLAN=1
~cut~
[05/15/13 16:21:45.443 CST 36eb 9120] 6896.7B0D.F3BB 1XK: Received EAPOL-key in
PTK_START state (msg 2) from mobile
[05/15/13 16:21:45.443 CST 36ec 9120] 6896.7B0D.F3BB 1XK: Stopping retransmission timer
[05/15/13 16:21:45.443 CST 36ed 9120] 6896.7B0D.F3BB 1XA: Sending EAPOL message to
mobile, WLAN=1 AP WLAN=1
~cut~
[05/15/13 16:21:45.461 CST 36f0 9120] 6896.7B0D.F3BB 1XK: Received EAPOL-key in
PTKINITNEGOTIATING state (msg 4) from mobile
[05/15/13 16:21:45.461 CST 36f1 9120] 6896.7B0D.F3BB 1XK: Set Link Secure: 1
[05/15/13 16:21:45.461 CST 36f2 9120] 6896.7B0D.F3BB 1XK: Key exchange complete -
updating PEM
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco live!

Layer 2 Authentication

AP Radio Debugs

*Feb 2 04:52:12.597: 97CD4D42 t 1 0 - 8802 000 2FB69A 6F9E10 6F9E10 6390 q7 l129

EAPOL2 EAPOL key desc 02 008A 0010 0000 0000 0000 0000 6468 F741 147D

*Feb 2 04:52:12.602: 97CD5BD6 r 1 63/65 19- 8801 13A 6F9E10 2FB69A 6F9E10 0000 q7 l129

EAPOL key desc 02 010A 0000 0000 0000 0000 0000 C715 1678 75D6 1A0A 2A2E

*Feb 2 04:52:12.605: 97CD6F4A t 1 0 - 8802 000 2FB69A 6F9E10 6F9E10 63A0 q7 l163

EAPOL2 EAPOL key desc 02 13CA 0010 0000 0000 0000 0001 6468 F741 147D

*Feb 2 04:52:12.611: 97CD813D r 1 63/67 16- 8801 13A 6F9E10 2FB69A 6F9E10 0010 q7 l107

EAPOL key desc 02 030A 0000 0000 0000 0000 0001 0000 0000 0000 0000 0000

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless PCAP

Cisco_83:42:6f	IntelCor_89:51:ca		802.11	265 Probe Response, SN=2900, FN=0, Flags
IntelCor_89:51:ca	Cisco_83:42:6f		802.11	75 Probe Request, SN=295, FN=0, Flags=.
	IntelCor_89:51:ca (RA)		802.11	14 Acknowledgement, Flags=.....
Cisco_83:42:6f	IntelCor_89:51:ca		802.11	265 Probe Response, SN=2901, FN=0, Flags
IntelCor_89:51:ca	Cisco_83:42:6f		802.11	34 Authentication, SN=296, FN=0, Flags=
	IntelCor_89:51:ca (RA)		802.11	14 Acknowledgement, Flags=.....
Cisco_83:42:6f	IntelCor_89:51:ca		802.11	34 Authentication, SN=2200, FN=0, Flags
IntelCor_89:51:ca	Cisco_83:42:6f		802.11	158 Association Request, SN=297, FN=0, F
	IntelCor_89:51:ca (RA)		802.11	14 Acknowledgement, Flags=.....
Cisco_83:42:6f	IntelCor_89:51:ca		802.11	180 Association Response, SN=2201, FN=0,
Cisco_83:42:6f	IntelCor_89:51:ca		EAPOL	159 Key (Message 1 of 4)
IntelCor_89:51:ca	Cisco_83:42:6f		EAPOL	161 Key (Message 2 of 4)
	IntelCor_89:51:ca (RA)		802.11	14 Acknowledgement, Flags=.....
Cisco_83:42:6f	IntelCor_89:51:ca		EAPOL	193 Key (Message 3 of 4)
IntelCor_89:51:ca	Cisco_83:42:6f		EAPOL	137 Key (Message 4 of 4)
	IntelCor_89:51:ca (RA)		802.11	14 Acknowledgement, Flags=.....

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 2 Authentication

L2_AUTH

EAPOL Key Exchange – Wrong PSK

```
0021.6a89.51ca 1XA: Using PSK
0021.6a89.51ca 1XK: Creating a PKC PMKID Cache entry (RSN 1)
0021.6a89.51ca 1XA: Initiating RSN PSK
0021.6a89.51ca Starting key exchange with mobile - data forwarding is disabled
0021.6a89.51ca 1XA: Sending EAPOL message to mobile, WLAN=1 AP WLAN=1
0021.6a89.51ca 1XA: Received EAPOL-Key from mobile
0021.6a89.51ca 1XK: Received EAPOL-key in PTK_START state (msg 2) from mobile
0021.6a89.51ca 1XA: 'key-response' timer expired
0021.6a89.51ca 1XA: Retransmit 1 of EAPOL-Key M1 (length 121)
0021.6a89.51ca Client authentication failed because the client did not respond to an
EAPOL-key message.SessionID().KeyMsg(1)
0021.6a89.51ca 1XA: Sending deauth msg, Reason Code = 15
0021.6a89.51ca Sent Deauthenticate to mobile with deauth reason code 15 on BSSID
1caa.076f.9e10  slot 1(caller dot1xapi_api.c:1576)
0021.6a89.51ca 1XA: Cleaning up dot1x
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco live!

Layer 2 Authentication

AP Radio Debug

```
*Jan 27 05:07:41.606: C92542A3 r  1      71/69 17- 8801 13A 6F9E10 2FB69A 6F9E10 0000 q7
l129
  EAPOL key desc 02  010A 0000 0000 0000 0000 0000 2888 5356 F66C 4026 1CFB
*Jan 27 05:07:42.456: C9323EDD t  1     0  - 8802 000 2FB69A 6F9E10 6F9E10 50C0 q7 l129
  EAPOL2 EAPOL key desc 02  008A 0010 0000 0000 0000 0000 6468 F741 147D
*Jan 27 05:07:42.460: C9324C8A r  1      69/70 15- 8801 13A 6F9E10 2FB69A 6F9E10 0010 q7
l129
  EAPOL key desc 02  010A 0000 0000 0000 0000 0000 533F 3E2F 198C 7C8C B070
*Jan 27 05:07:43.425: C9410B12 t  1     0  - 8802 000 2FB69A 6F9E10 6F9E10 50D0 q7 l129
  EAPOL2 EAPOL key desc 02  008A 0010 0000 0000 0000 0000 6468 F741 147D
*Jan 27 05:07:43.429: C941199E-0 2FB69A - pak flags 1
*Jan 27 05:07:43.429: C9411996 r  1      70/68 19- 8801 13A 6F9E10 2FB69A 6F9E10 0020 q7
l129
  EAPOL key desc 02  010A 0000 0000 0000 0000 0000 22C1 DC16 84C9 77EE 8ED2
*Jan 27 05:07:44.394: C94FD7B6 t  1     0  - C000 000 2FB69A 6F9E10 6F9E10 0000 deauth l 2
        reason 15
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless PCAP

IntelCor_89:51:ca	Broadcast	802.11	75	Probe Request, SN=837, FN=0, Flags=.....
Cisco_83:42:6f	IntelCor_89:51:ca	802.11	265	Probe Response, SN=2948, FN=0, Flags=....R..
IntelCor_89:51:ca	Cisco_83:42:6f	802.11	75	Probe Request, SN=850, FN=0, Flags=.....
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6f	IntelCor_89:51:ca	802.11	265	Probe Response, SN=2949, FN=0, Flags=....R..
IntelCor_89:51:ca	Cisco_83:42:6f	802.11	34	Authentication, SN=851, FN=0, Flags=.....
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
IntelCor_89:51:ca	Cisco_83:42:6f	802.11	158	Association Request, SN=852, FN=0, Flags=...
	IntelCor_89:51:ca (RA)	802.11	14	Acknowledgement, Flags=.....
Cisco_83:42:6f	IntelCor_89:51:ca	802.11	180	Association Response, SN=3719, FN=0, Flags=.
Cisco_83:42:6f	IntelCor_89:51:ca	EAPOL	159	Key (Message 1 of 4)
IntelCor_89:51:ca	Cisco_83:42:6f	EAPOL	161	Key (Message 2 of 4)
Cisco_83:42:6f	IntelCor_89:51:ca	EAPOL	159	Key (Message 1 of 4)
IntelCor_89:51:ca	Cisco_83:42:6f	EAPOL	161	Key (Message 2 of 4)
Cisco_83:42:6f	IntelCor_89:51:ca	802.11	30	Deauthentication, SN=3844, FN=0,
Cisco_83:42:6f	IntelCor_89:51:ca	802.11	30	Deauthentication, SN=3844, FN=0,

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Flow

The Route Toward the RUN State!

© 2015 Cisco and/or its affiliates. All rights reserved.
Cisco Public

IP Address Learning

LEARN_IP

- IP learning via IOSd modules
  - ARP

```
0023.6907.e218 WCDB_IP_BIND: w/ IPv4 192.168.40.108
ip_learn_type ARP add_delete 1,options_length 0
```

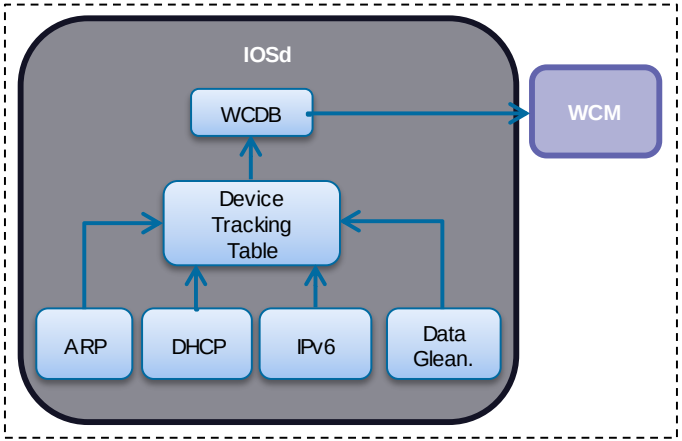
  - DHCP

```
0023.6907.e218 WCDB_IP_BIND: w/ IPv4 192.168.40.108
ip_learn_type DHCP add_delete 1,options_length 0
```

  - IPv6 NDP

```
0023.6907.e218 WCDB_CHANGE: auth=RUN(4) vlan 40
radio 0 client_id 0xe5cd800000068a
mobility=Local(1) src_int 0xfbb30000000671 dst_int
0x0 ackflag 2 reassoc_client 0 llm_notif 0 ip
0.0.0.0 ip_learn_type IPV6_NDP
```

  - Data Gleaning (1st IP packet)



- If roaming, IP info exchanged via mobility

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

IP Address Learning

LEARN_IP

Show Client Status

- WCM

```
3850-2#show wireless client summary
Number of Local Clients : 1

MAC Address    AP Name                                  WLAN State                Protocol
-------------------------------------------------------------------------------------
0023.6907.e218 ap1140-sw3850-2-2                        2    IPLEARN              11g
```

- WCDB

```
3850-2#show wcdb database all

Mac Address    VlanId IP Address       Src If              Auth      Mob
-------------- ------ --------------- ------------------ -------- -------
0023.6907.e218     40 0.0.0.0         0x00C99740000006BC LEARN_IP LOCAL
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

DHCP Snooping

LEARN_IP

Basic Config

- Must enable DHCP snooping if “DHCP Required” is set on the WLAN
- Enable globally

```
3850a(config)# ip dhcp snooping
```

- Enable on client VLAN(s)

```
3850a(config)# ip dhcp snooping vlan X,Y,…
```

- Apply trust on the interface(s) to the DHCP server

```
3850(config)#int gigabitEthernet 1/0/22
3850(config-if)#ip dhcp snooping trust
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco live!

DHCP Snooping

Relay and DHCP Override

LEARN_IP

- If using an ip-helper, need to modify option 82 behaviour
  - "no ip dhcp snooping information option" on the DHCP snooping device
  - or
  - "ip dhcp relay information trusted" (per interface) on the DHCP relay device
  - "ip dhcp relay information trust-all" (global configuration) on the relay device
- Need Layer 3 VLAN interface IP address for WLAN DHCP server override

```
3850a(config-wlan)# ip dhcp server ?
  A.B.C.D  Enter the override DHCP server's IP Address
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

DHCP Snooping

Traces and Debugs

Traces

- set trace dhcp filter mac xxxx.xxxx.xxxx
- set trace dhcp level debug

Debugs

- debug client mac-address xxxx.xxxx.xxxx
- debug ip dhcp snooping events,packet
- debug ip dhcp server events, packet
- debug wcdb error
- debug wcdb event
- debug ip device tracking

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Viewing Client DHCP Handshake

LEARN_IP

Trace

```
dhcp pkt processing routine is called for pak with SMAC = 0021.6a89.51ca and SRC_ADDR = 0.0.0.0
sending dhcp packet outafter processing with SMAC = 0021.6a89.51ca and SRC_ADDR = 0.0.0.0
DHCPD: Got overriding information from client db
DHCPD: Reload workspace interface Vlan30 tableid 0.
DHCPD: tableid for 0.0.0.0 on Vlan30 is 0
DHCPD: DHCPREQUEST received from client 0100.216a.8951.ca.
DHCPD: address 30.30.30.2 mask 255.255.255.0
DHCPD: Sending DHCPACK to client 0100.216a.8951.ca (30.30.30.2).
DHCPD: no option 125
0021.6a89.51ca MS got the IP, resetting the Reassociation Count 0 for client
[WCDB] wcdb_ffcp_cb: client (0021.6a89.51ca) client (0x724680000005ae): FFCP operation (UPDATE)
return code (0)
dhcp pkt processing routine is called for pak with SMAC = 0021.6a89.51ca and SRC_ADDR =
30.30.30.2
sending dhcp packet outafter processing with SMAC = 0021.6a89.51ca and SRC_ADDR = 30.30.30.2
DHCPD: Got overriding information from client db
DHCPD: Reload workspace interface Vlan30 tableid 0.
DHCPD: tableid for 0.0.0.0 on Vlan30 is 0
DHCPD: DHCPINFORM received from client 0100.216a.8951.ca (30.30.30.2).
DHCPD: Sending DHCPACK to client 0100.216a.8951.ca (30.30.30.2).
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless PCAP

IntelCor_89:51:ca	Broadcast	ARP	66 Who has 30.30.30.251? Tell 30.30.30.15
Cisco_fc:96:a8	IntelCor_89:51:ca	ARP	84 30.30.30.251 is at f0:f7:55:fc:96:a8
Cisco_fc:96:a8	IntelCor_89:51:ca	ARP	84 30.30.30.251 is at f0:f7:55:fc:96:a8
Cisco_fc:96:a8	IntelCor_89:51:ca	ARP	84 30.30.30.251 is at f0:f7:55:fc:96:a8
Cisco_fc:96:a8	IntelCor_89:51:ca	ARP	84 30.30.30.251 is at f0:f7:55:fc:96:a8
Cisco_fc:96:a8	IntelCor_89:51:ca	ARP	84 30.30.30.251 is at f0:f7:55:fc:96:a8
0.0.0.0	255.255.255.255	DHCP	370 DHCP Request - Transaction ID 0xae9dacba
0.0.0.0	255.255.255.255	DHCP	370 DHCP Request - Transaction ID 0xae9dacba
30.30.30.1	30.30.30.15	DHCP	372 DHCP ACK - Transaction ID 0xae9dacba

 © 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

DHCP Snooping

Not Getting an IP Address

LEARN_IP

```
0021.6a89.51ca Adding mobile on LWAPP AP  1caa.076f.9e10 (1)
0021.6a89.51ca Association received from mobile on AP  1caa.076f.9e10
0021.6a89.51ca WCDB_ADD: ssid Webauth bssid c8f9.f983.4260 vlan 12 auth=ASSOCIATION(0)
0021.6a89.51ca Change state to L2AUTHCOMPLETE (4) last state AUTHCHECK (2)
 0021.6a89.51ca Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)
 dhcp pkt processing routine is called for pak with SMAC = 0021.6a89.51ca and SRC_ADDR =
0.0.0.0
DHCPD: Sending notification of DISCOVER:
 DHCPD: DHCPDISCOVER received from client 0100.216a.8951.ca on interface Vlan12.
 DHCPD: there is no address pool for 10.105.135.178.
dhcp pkt processing routine is called for pak with SMAC = 0021.6a89.51ca and SRC_ADDR =
0.0.0.0
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Flow

The Route Toward the RUN State!

© 2015 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Web Authentication

L3_Auth

Basic Config

```
ip http server
ip http authentication local
ip http secure-server
!
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
!
parameter-map type webauth ciscolive-webauth
 type webauth | consent | both
```

HTTPS redirect + login

HTTP server

Global Parameter Map

Named Param Map

AAA

Named Map → WLAN

- Local Web-Auth (LWA)
  - Web-Auth vs. Consent
  - Local users vs. RADIUS
  - Custom pages
- Central Web-Auth (CWA)
  - External pages
  - ISE

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Web Authentication

L3_Auth

Captive Portal Bypass

- Apple feature to detect a captive portal (“Captive Network Assistant”)
- Blank page shown if using self-signed SSL certificate on the WLC for Web-Auth
  - When the CNA browser is closed the device disconnects, hence Web-Auth cannot be completed

- Force to use full feature browser instead of CNA, using captive portal bypass on WLC:

```
3850-1(config)# captive-portal-bypass
```

- iOS 7 support as of IOS-XE 3.2.3

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Web Authentication

L3_Auth

Show Client Status

- WCM

```
3850-2#show wireless client summary
Number of Local Clients : 1

MAC Address    AP Name                                  WLAN State                 Protocol
-------------------------------------------------------------------------------------------
0023.6907.e218 ap1140-sw3850-2-2                        1    WEBAUTH_PEND          11g
```

- WCDB

```
3850-2#show wcdb database all

Mac Address    VlanId IP Address      Src If              Auth      Mob
-------------- ------ --------------- ------------------ -------- -------
0023.6907.e218    153 192.168.153.2   0x00C99740000006BC L3_AUTH   LOCAL
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Web Authentication

L3_Auth

Traces and Debugs

Traces

- set trace group-wireless-client level debug
  set trace group-wireless-client filter mac xxxx.xxxx.xxxx
- set trace dhcp level debug
  set trace dhcp filter mac xxxx.xxxx.xxxx
- set trace access-session level debug
  set trace access-session filter mac xxxx.xxxx.xxxx
- set trace mobility handoff level debug
  set trace mobility handoff filter mac xxxx.xxxx.xxxx

Roam / Guest anchor

Debugs

- debug client mac-address xxxx.xxxx.xxxx
- debug ip http all
- debug ip admission all
- debug access-session all
- debug ip tcp socket error
- debug ip http url

Captive bypass

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Web Authentication

L3_Auth

Successful Auth

```
0021.6a89.51ca Association received from mobile on AP  1caa.076f.9e10
0021.6a89.51ca Change state to L2AUTHCOMPLETE (4) last state AUTHCHECK (2)
0021.6a89.51ca WEBAUTH: Using method list local_webauth
[WCDB] ==Update event: client (0021.6a89.51ca) client id:(0x5e200000000026) vlan (30-
>30) global_wlan (9->9) auth_state (L2_AUTH_DONE->LEARN_IP) mob_state (INIT->LOCAL)
DHCPD: DHCPREQUEST received from client 0100.216a.8951.ca.
DHCPD: address 30.30.30.4 mask 255.255.255.0
DHCPD: creating ARP entry (30.30.30.4, 0021.6a89.51ca).
ACCESS-CORE-SM-NOTF: [0021.6a89.51ca, Ca2] Authc success from WebAuth (3), status OK (0)
/ event success (0)
[0021.6a89.51ca, Ca2] Queued AUTHC SUCCESS from WebAuth for session 0x43000017
(0021.6a89.51ca)
0021.6a89.51ca WEBAUTH: IOS Auth Event - Authentication Success!
0021.6a89.51ca Change state to WEBAUTH_NOL3SEC (14) last state WEBAUTH_REQD (8)
0021.6a89.51ca Change state to AUTHZ_WAIT (19) last state WEBAUTH_NOL3SEC (14)
0021.6a89.51ca Client in AUTHZ_WAIT state, advance to RUN
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless PCAP

IntelCor_89:51:ca	Broadcast	ARP	66 Who has 30.30.30.251? Tell 30.30.30.15
Cisco_fc:96:a8	IntelCor_89:51:ca	ARP	84 30.30.30.251 is at f0:f7:55:fc:96:a8
Cisco_fc:96:a8	IntelCor_89:51:ca	ARP	84 30.30.30.251 is at f0:f7:55:fc:96:a8
Cisco_fc:96:a8	IntelCor_89:51:ca	ARP	84 30.30.30.251 is at f0:f7:55:fc:96:a8
Cisco_fc:96:a8	IntelCor_89:51:ca	ARP	84 30.30.30.251 is at f0:f7:55:fc:96:a8
Cisco_fc:96:a8	IntelCor_89:51:ca	ARP	84 30.30.30.251 is at f0:f7:55:fc:96:a8
0.0.0.0	255.255.255.255	DHCP	370 DHCP Request - Transaction ID 0xae9dacba
0.0.0.0	255.255.255.255	DHCP	370 DHCP Request - Transaction ID 0xae9dacba
30.30.30.1	30.30.30.15	DHCP	372 DHCP ACK - Transaction ID 0xae9dacba
30.30.30.15	20.20.20.251	DNS	100 Standard query 0x716e
20.20.20.251	30.30.30.15	DNS	114 Standard query response 0xd1a0 A 55.55.55.55
55.55.55.55	30.30.30.15	TCP	477 http > 64385 [FIN, RST, PSH, ACK, CWR, NS,
30.30.30.15	192.168.200.1	TCP	78 64391 > https [ACK] Seq=1 Ack=1 Win=64240 L

```
⊞ Frame 7606: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
⊞ 802.11 radio information
⊞ IEEE 802.11 QoS Data, Flags: .......T.
⊞ Logical-Link Control
⊟ Internet Protocol Version 4, Src: 30.30.30.15 (30.30.30.15), Dst: 192.168.200.1 (192.168.200.1)
    Version: 4
    Header length: 20 bytes
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Web Authentication

L3_Auth

Typical Issues

- No redirect to login page
- Unable to submit login page
- Logout pop-up
- Success redirect

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Web Authentication

L3_Auth

No Redirect to Login Page

- DNS resolution
  - Check DHCP pool
  - Check client config
- Incorrect Pre-auth ACL
  - Allowed traffic doesn't trigger a redirect
- Max connections (per client / global)

Test: point the browser to an IP addr: http://1.2.3.4/

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco live!

Web Authentication

L3_Auth

Unable to Submit Login Page

- Incorrect login page path
  - All pages (login, success, failure, expired) must be provided
    - Custom pages:

```
c5760-1(config)# parameter-map type webauth ciscolive-webauth
   custom-page login device flash:login.html
   custom-page login expired device flash:loginexpired.html
   custom-page failure device flash:loginfail.html
   custom-page success device flash:loginsuccess.html
```

    - External pages

```
c5760-1(config-params-parameter-map)# redirect ?
  for-login   Redirect for login
  on-failure  Redirect On-Failure
  on-success  Redirect On-Success
  portal      External Portal
```

- Code errors in customised/external login page

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Flow

The Route Toward the RUN State!

© 2015 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Run!

RUN

Show Client Status

- WCM

```
3850-2#show wireless client summary
Number of Local Clients : 1

MAC Address    AP Name                                  WLAN State                 Protocol
-------------------------------------------------------------------------------------------
0023.6907.e218 ap1140-sw3850-2-2                        2    UP                    11g
```

- WCDB

```
3850-2#show wcdb database all

Mac Address    VlanId IP Address       Src If              Auth     Mob
-------------- ------ --------------- ------------------ -------- -------
0023.6907.e218    153 192.168.153.2    0x00C99740000006BC RUN      LOCAL
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Traffic Forwarding Path

RUN

First Association – Mobility state: Local

```
c5760-1#show wcdb database 6c20.568c.dade
mac:                6c20.568c.dade
ssid:               ciscolive
client_type:        Regular Wireless
client_id:          0x00A0AC00000000C1
client_index:       129
user_id:            vlan40
src_interface:      0x00B01DC000000032
dst_interface:      0x0000000000000000
bssid:              04da.d24f.f1e0
radio_id:           0
wlan_id:            2
global_wlan_id:     2
assoc_id:           3
vlan_id:            40
mcast_vlan_id:      153
mobility_state:     LOCAL
auth_state:         RUN
auth_state_wcm:     RUN
```

```
c5760-1#show capwap detail

Name    APName                                  Type
PhyPortIf Mode       McastIf
------ -------------------------------- ---- -----
---- --------- -------
Ca2     ap2600-sw3850-3-11                      data


Name    SrcIP             SrcPort DestIP
DstPort DtlsEn MTU   Xact
------ --------------- ------- -------------- ---
---- ------ ----- ----
Ca2     192.168.151.21   5247    192.168.30.132
7412     No     1449  0

Name    IfId                 McastRef
------ -------------------- --------
Ca2     0x00B01DC000000032 0
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Traffic Forwarding Path

RUN

Handoff – Sticky Anchoring - Mobility State: Anchor

```
c5760-1#show wcdb database 6c20.568c.dade
mac:                6c20.568c.dade
ssid:               ciscolive
client_type:        Regular Wireless
client_id:          0x00A0AC00000000C1
client_index:       129
user_id:            vlan40
src_interface:      0x0092780000000030
dst_interface:      0x0000000000000000
bssid:              0000.0000.0000
radio_id:           0
wlan_id:            2
global_wlan_id:     2
assoc_id:           3
vlan_id:            40
mcast_vlan_id:      153
mobility_state:     ANCHOR
auth_state:         RUN
auth_state_wcm:     RUN
```

```
c5760-1#show capwap detail

Name    APName                                  Type
PhyPortIf Mode       McastIf
------ -------------------------------- ---- -----
---- --------- -------
Ca1     -                                       mob   -
unicast    -

Name    SrcIP             SrcPort DestIP
DstPort DtlsEn MTU   Xact
------ --------------- ------- --------------- ---
---- ------ ----- ----
Ca1     192.168.151.21  16667   192.168.151.12
16667    No     1464  1

Name    IfId                 McastRef
------ -------------------- --------
Ca1     0x0092780000000030 0
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Traffic Forwarding Path

RUN

Handoff – Sticky Anchoring - Mobility State: Foreign

```
3850-2#show wcdb database 6c20.568c.dade
mac:                6c20.568c.dade
ssid:               ciscolive
client_type:        Regular Wireless
client_id:          0x00CF9B0000000707
client_index:       95
user_id:            vlan40
src_interface:      0x00C99740000006BC
dst_interface:      0x00F2ED80000006A9
bssid:              0026.cbd2.6750
radio_id:           0
wlan_id:            2
global_wlan_id:     2
assoc_id:           1
vlan_id:            40
mcast_vlan_id:      153
mobility_state:     FOREIGN
auth_state:         RUN
auth_state_wcm:     RUN
```

```
3850-2#show capwap detail

Name    APName                                  Type
PhyPortIf Mode       McastIf
------  ------------------------------- ---- -----
Ca0     -                                       mob
Ca3     ap1140-sw3850-2-2                       data

Name    SrcIP            SrcPort DestIP
---  --------------- ------- --------------- ---
Ca0     192.168.151.12   16667   192.168.151.21
Ca3     192.168.151.12   5247    192.168.151.16

Name    IfId                 McastRef
------  ------------------ --------
Ca0     0x00F2ED80000006A9 0
Ca3     0x00C99740000006BC 0
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco live!

When Traces Aren't Enough

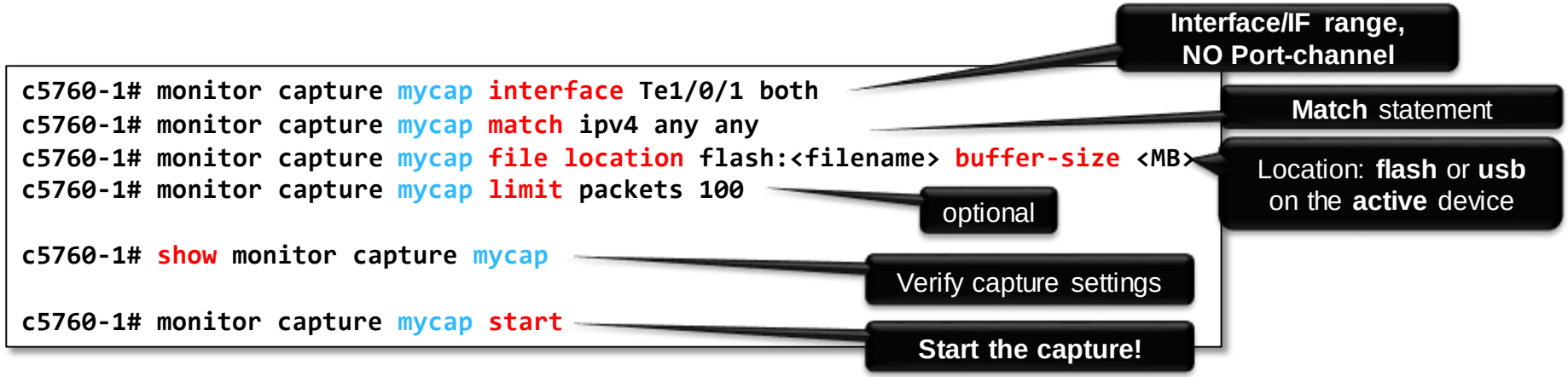
Wireshark Support

- Version 3.3 introduced the ability to capture traffic on a switch port and store it in a buffer:
  - Remote packet capture capability
  - Traffic can be uploaded off of flash and decoded in Wireshark!

```
c5760-1# monitor capture mycap interface Te1/0/1 both
c5760-1# monitor capture mycap match ipv4 any any
c5760-1# monitor capture mycap file location flash:<filename> buffer-size <MB>
c5760-1# monitor capture mycap limit packets 100

c5760-1# show monitor capture mycap

c5760-1# monitor capture mycap start
```



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

When Traces Aren't Enough

Wireless Capture

- Many times, traces/debugs will indicate the point of failure, but the root cause requires a wireless packet capture
- Mac OS X 10.6 and above
- Windows 7 with Netmon 3.4
- Omnipeek
- AP in Sniffer Mode
- For more information, see this supportforum article:
  - https://supportforums.cisco.com/docs/DOC-24502

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

5760 AP SSO

Basic Config

- 3.3SE+ Required
- HA via switch stack
  - StackWise-480
  - max 2 units (1 active, 1 standby)
- AP SSO

- Adding/Removing a powered-on WLC causes both WLCs to reload
  - Power down the WLC to be paired before plugging/removing the stack cables

© 2015 Cisco and/or its affiliates. All rights reserved.

5760 AP SSO

Check Failover Reason

- Failover reasons
  - Process failure
  - Power-fail
  - Manual
- NOTE: a switch port failure will not induce a switchover
- Switchover history

```
c5760-1# show redundancy switchover history
Index   Previous   Current   Switchover              Switchover
        active     active    reason                  time
-----   --------   -------   ----------              ----------
   1        0          2     active unit failed      14:33:24 UTC Wed Jan 1 2014
   2        0          1     user forced             14:48:27 UTC Wed Jan 1 2014
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

5760 AP SSO

Typical Issues

- Incorrect stack cables
- Incorrect LAG/Etherchannel config
- APs fail to join after switchover - Licensing

```
Jan  1 14:33:54.652: *%MM-3-AP_LICENSE_USAGE_EXCEEDED: 2 wcm:  AP usage exceeded licenses
available by 2-Limit AP usage to match license availability
Jan  1 14:35:52.254: *%LWAPP-3-AP_LICENSE_REQUEST_ERR: 2 wcm:  License request failed for AP
04:da:d2:4f:f1:e0 - Check for Controller Licenses
Jan  1 14:35:52.254: *%CAPWAP-3-AP_DB_ALLOC: 2 wcm:  Unable to alloc AP entry in database for
192.168.30.132:7413
```

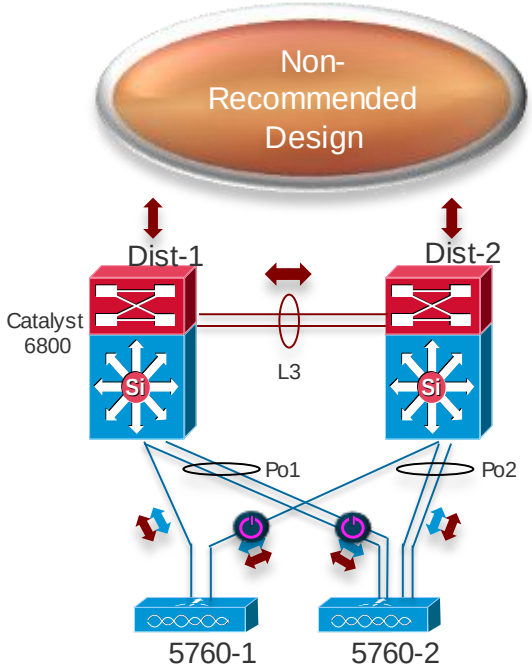

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

5760 AP SSO

Flexlink Facts..

Flexlink unknown facts :

- L2 wireless user roam challenges MAC Add Table-Move-Update (MMU)
- Overall network performance in aggregation block terminating corporate-wide wireless devices



Flexlink known facts :

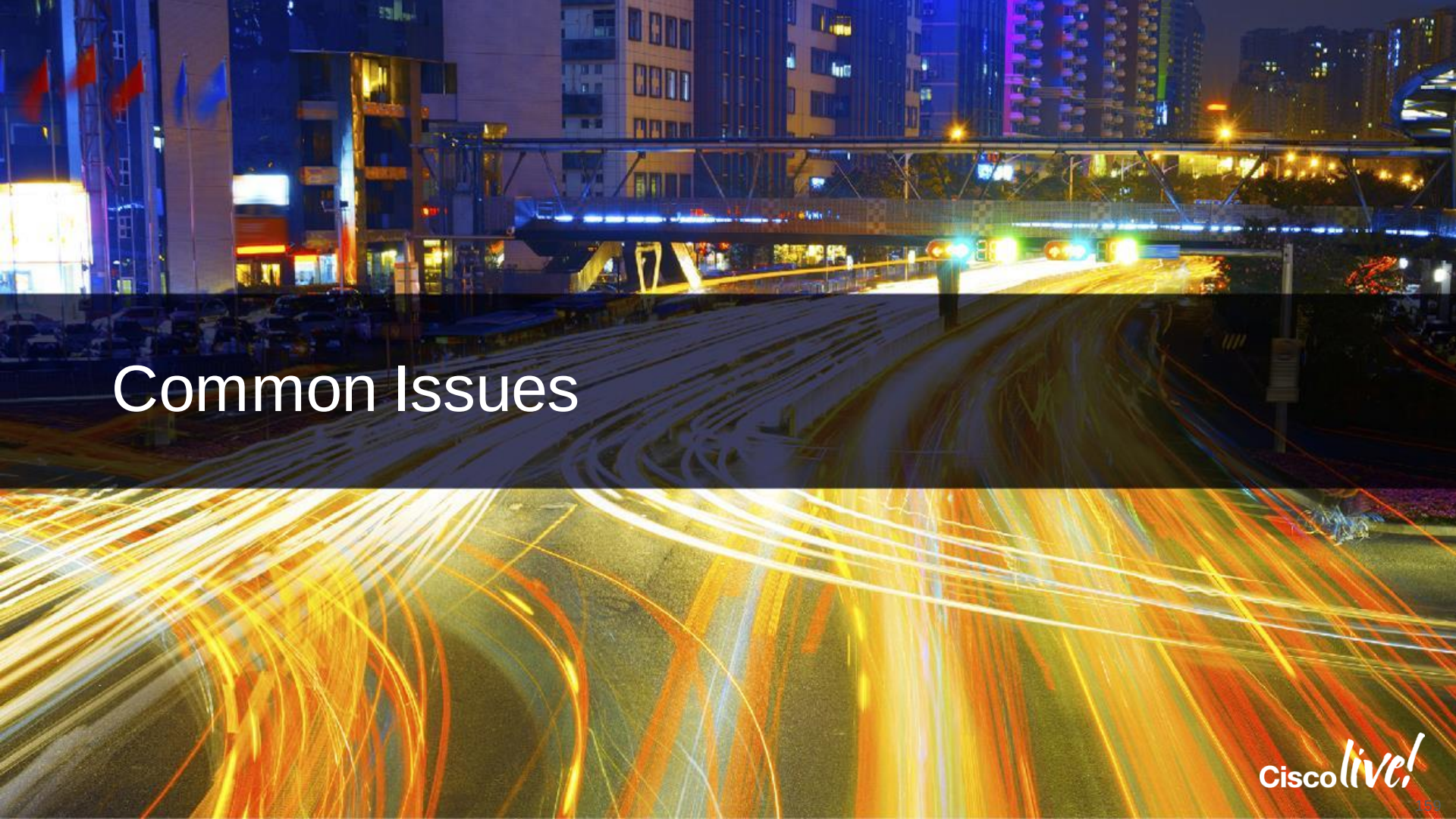
- Flexlink disables STP. Do not replace STP
- Prone to STP loop may cause severe network outage
- Unbalance forwarding paths keeps network resource under/over-utilize
- Unsupported technology on Nexus switching portfolio

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Useful Commands

- show tech-support wireless
  - To be provided when opening a TAC Case, equivalent to a “show run-config” from CUWN
- show run all | section <>
  - Useful for viewing default settings
  - Recommended to use with output modifier
- show wireless client summary
  - Shows all clients connected on the current MA/MC, it will list the AP name and frequency, or the IP address of the anchor location
- show wcdb database all
  - This will output all of the clients, along with the VLAN, IP address, and mobility state

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public


Common Issues

Bugs to Watch Out For

- CSCue76684 – 3850 switch or 5760 controller fails boot after configuration is saved
  - Fixed in 3.2(1)SE

- Copying & pasting multiple commands through SSH can cause character drops, rendering some of the commands ineffective
  - This does not occur when connecting via Telnet
  - Workaround is to add leading spaces to your commands so that the spaces are dropped and the commands are entered properly

- CSCui40588 - GUI is not accessible after AAA authentication for http/s
- - Work around is to use Local username/Password for HTTP/S

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Key Takeaways

- Understand the CA components and client flow
- Understand the mobility hierarchy and design your network accordingly for proper roaming behaviour
- Watch out for the simple stuff!
  - Mobility Config
  - Licensing
  - AP Join
  - DHCP Snooping
- We can use a combination of show commands, debugs and traces to collect information
- Always collect “show tech wireless” for TAC Cases

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public


Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2015 T-Shirt!

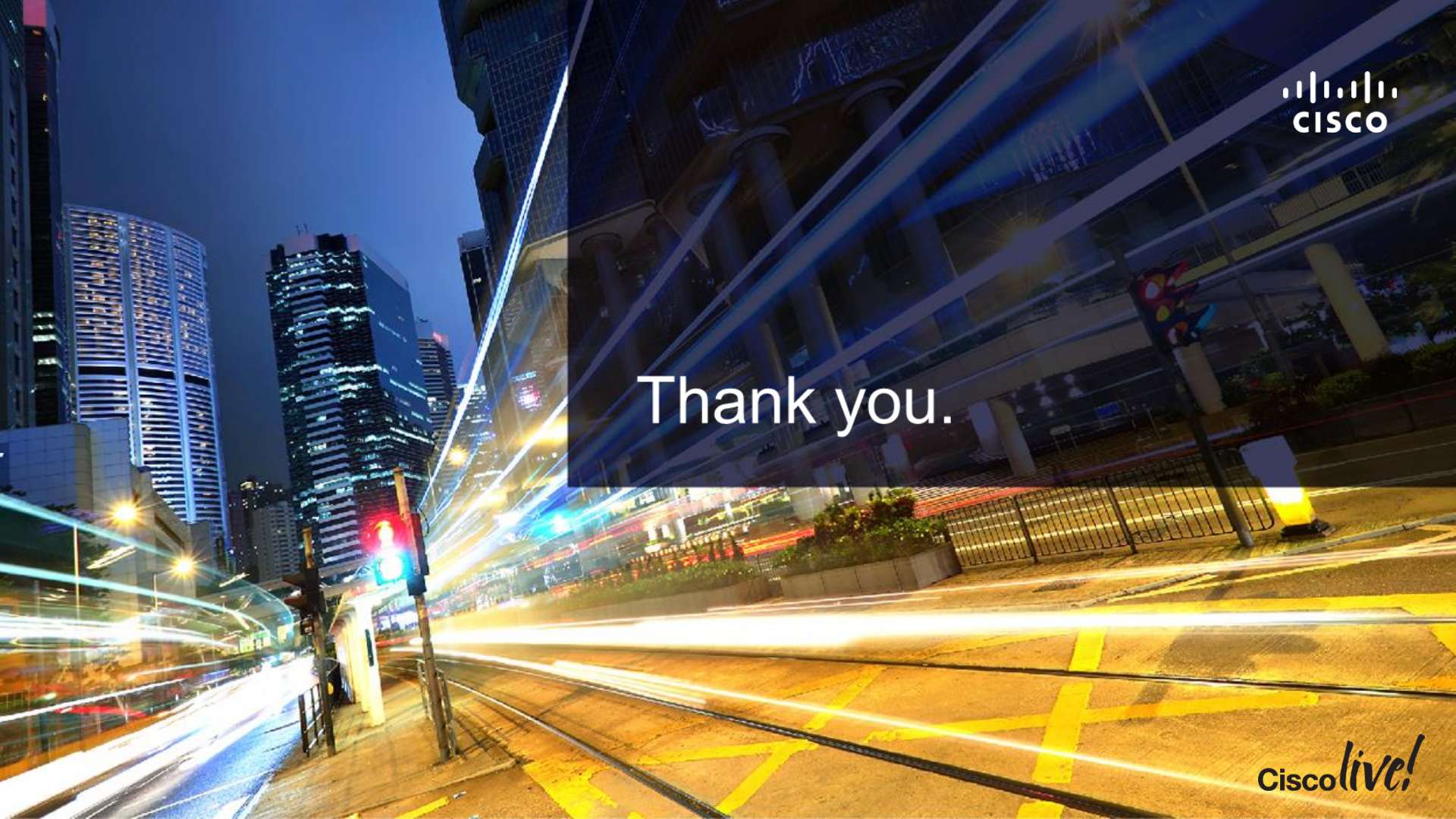
Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public


Thank you.


CISCO