
TOMORROW starts here.
cisco
Cisco live!

Best Practices to Deploy High-Availability in Wireless LAN Architectures

BRKEWN-3014

Brian Levin

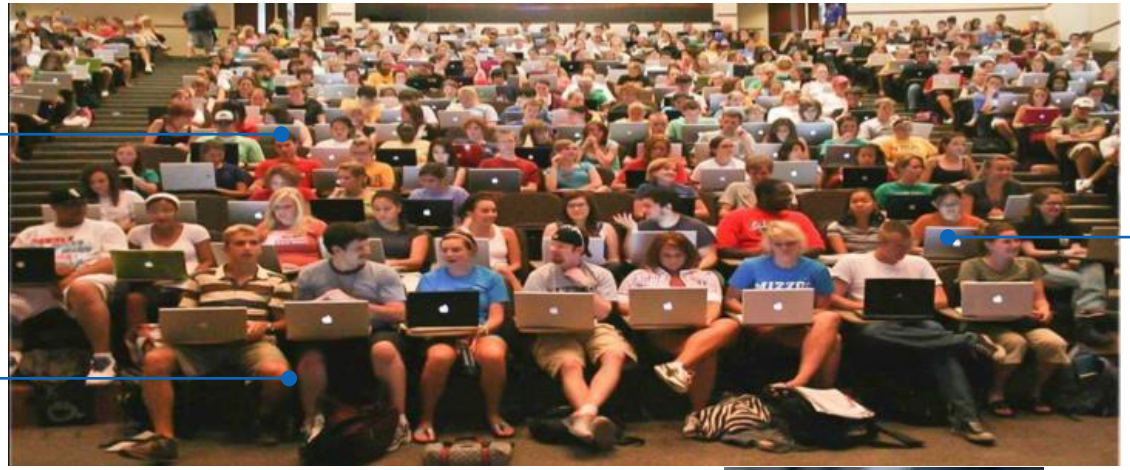
ENG, Technical Marketing Engineer

Cisco live!

The New Normal

High Density

How many devices have you got today?



High Quality

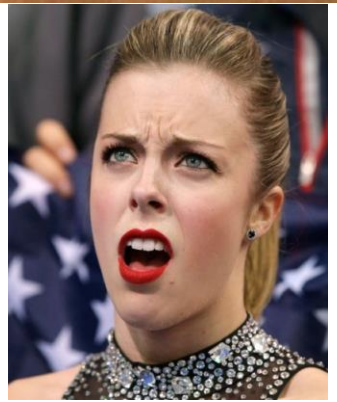
No coverage holes

High Performance

Who wants GE over WiFi?

What about Highly Available?

What if the network goes down??



Planned downtime

Failover

End-to-end access

RF Redundancy

Clustering/Pooling

Application Survivability

Performance

Cost $$$$

Productivity

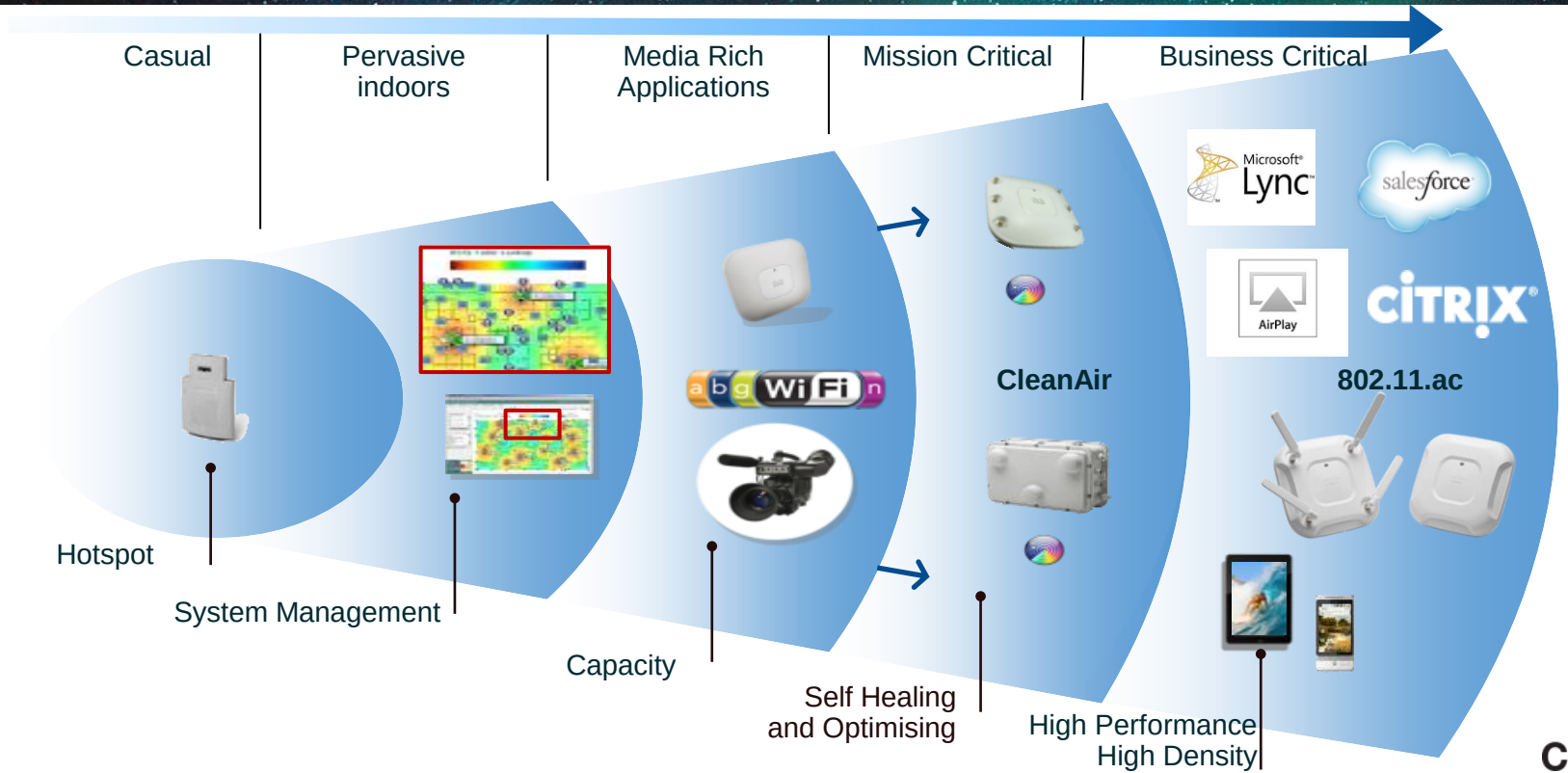
High Availability

Session Objectives:

Provide design guidance and best practices around building reliable and highly available Wireless LAN networks to support your business critical applications

Enterprise Wireless Evolution

From Best-Effort to Business Critical



Cisco live!

Agenda

So what are we really talking about?

- Radio Frequency (RF) High Availability (HA)
  - Site Survey, RRM, CleanAir, etc.
- Network Infrastructure HA
  - Centralised Mode
  - FlexConnect Mode
  - Converged Access Mode
- Management and Mobility Services HA

Radio Frequency (RF) High Availability

- RF HA is the ability to have redundancy in the physical layer
- What does it translates to in practice?
  - Creating a pervasive, stable, predictable RF environment (Proper Design, Site Survey, Radio Planning)
  - Dealing with coverage holes if an AP goes down (RF Management)
  - Improving client (all clients!) received signal (Beamforming)
  - Identifying, Classifying, Mitigating an interference source (Spectrum Intelligence Solution)
- BTW..for all these, Cisco have differentiating features/functionalities

Radio Frequency (RF) High Availability

Recommendations: Site Survey

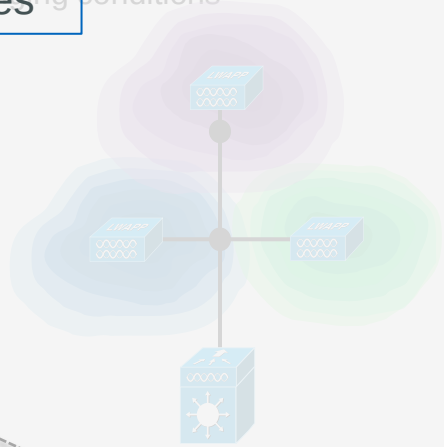
- Site Survey:
  - Use “Active Survey”
  - Use professional tools. Examples: AirMagnet , Ekahau, Veriwave
  - Rule of thumb: design for AP at mid power level, for example level 3
- Get to know the area:
  - Consider three dimensional radio propagation in multi-story buildings
  - Be aware of perimeter and corner areas
- AP positioning is Key
  - Use common sense
  - Internal antennas are designed to be mounted in the ceiling
  - Access Points like light sources should be in the clear and near the users
- Survey for lowest common client type and technology supported
  - 802.11b/g, 802.11a, 802.11n
  - Average Power: iPhone 16 dBm vs. MacBook Pro 20 dBm
  - Antenna gain: 2.4 GHz, iPhone -1.4 dBi vs. MacBook Pro 4.6 dBi

Radio Frequency (RF) High Availability

Radio Resource Management (RRM)

- What are Radio Resource Manager's objectives?
  - Provide a system wide RF view of the network at the Controller (only Cisco!!)
  - Dynamically balance the network and mitigate changes
  - Manage Spectrum Efficiency to constantly provide the optimal throughput under changing conditions
- What's RRM
  - DCA—Dynamic Channel Assignment
  - TPC—Transmit Power Control
  - CHDM—Coverage Hole Detection and Mitigation
- RRM best practices
  - RRM settings to auto for most deployments (High Density is a special case)
  - Design for most radios set at mid power level (lever 3 for example)
  - Survey for lowest common client type and technology supported
  - RRM doesn't replace the site survey and doesn't create spectrum

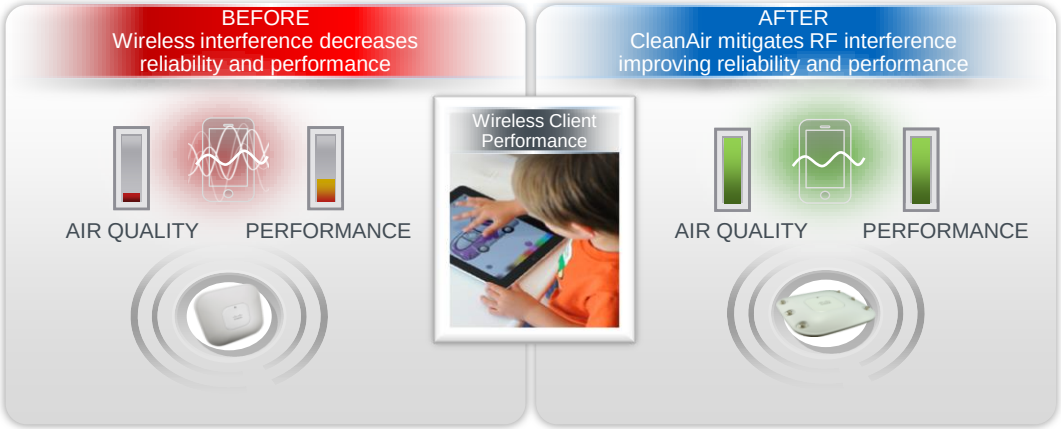
Look out for information at the bottom of the key pages



For more info: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a008072c759.shtml

Radio Frequency (RF) High Availability

Spectrum Intelligence Solution - Cisco CleanAir

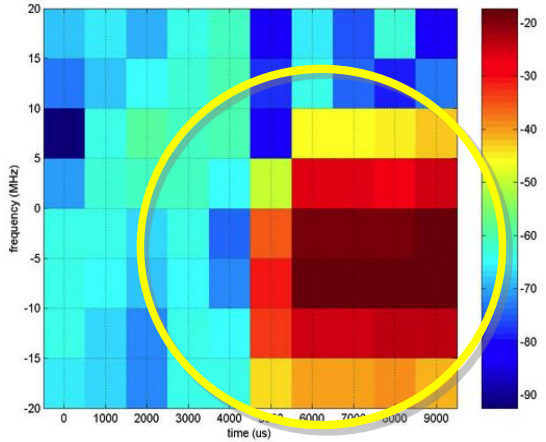


- Spectrum intelligence solution designed to proactively manage the challenges of a shared spectrum
- Assess impact to Wi-Fi performance; proactively change channels when needed
- CleanAir Radio ASIC: Only ASIC based solution can reliably detect interference sources
- Best Practice: turn it on if supported by your APs (3500, 2600, 3600, 3700 and from 8.0 also 1600)

For more info: http://www.cisco.com/en/US/netsol/ns1070

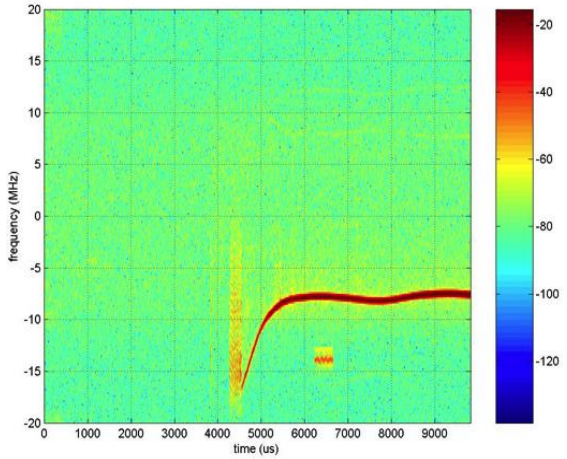
Radio Frequency (RF) High Availability

Spectrum Intelligence Solution - Cisco CleanAir



CleanAir
Hardware based Solution

32 times WiFi chip's visibility
Accurate classification
Multiple device recognition



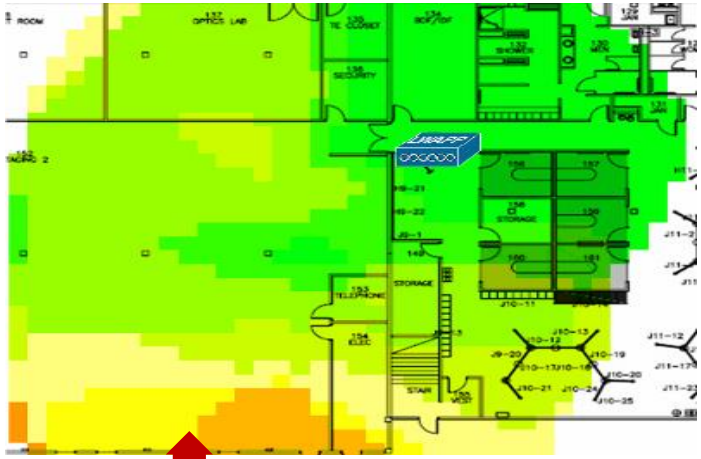
- Spectrum intelligence solution designed to proactively manage the challenges of a shared spectrum
- Assess impact to Wi-Fi performance; proactively change channels when needed
- CleanAir Radio ASIC: Only ASIC based solution can reliably detect interference sources
- Best Practice: turn it on if supported by your APs (3500, 2600, 3600, 3700 and from 8.0 also 1600)

For more info: http://www.cisco.com/en/US/netsol/ns1070

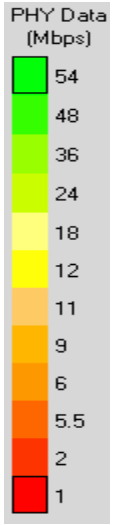
Radio Frequency (RF) High Availability

Client Beamforming – Cisco ClientLink

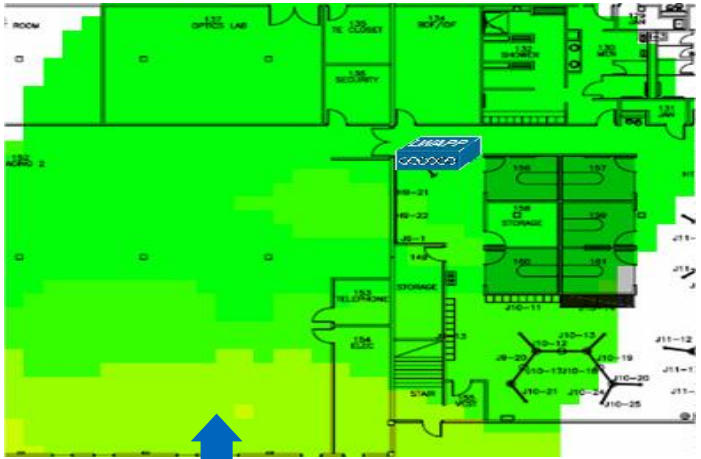
ClientLink Disabled



Lower Data Rates



ClientLink Enabled



Higher Data Rates

Source: Miercom with Fluke Iperf Survey

- Cisco ClientLink a.k.a. Beamforming: reduced Coverage Holes for all clients
- Best practice: on by default

For more info: http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps11983/at_a_glance_c45-691984.pdf

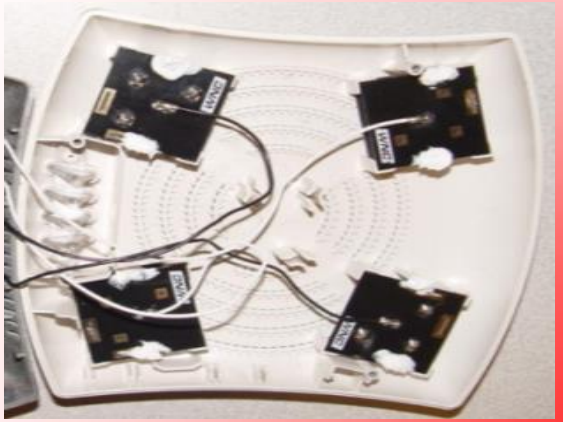
Radio Frequency (RF) High Availability

Recommendations - RF Profiles

- RF Profiles allow the administrator to tune groups of AP's sharing a common coverage zone together.
  - Selectively changing how RRM will operate the AP's within that coverage zone
- RF Profiles are created for either the 2.4 GHz radio or 5GHz radio
  - Profiles are applied to groups of AP's belonging to an AP Group, in which all AP's in the group will have the same Profile Settings
- There are two components to this feature:
  - RF Groups – Existing capability – No impact on channel selection algorithms
  - RF Profile – New from 7.2, providing administrative control over:
    - Min/Max TPC values
    - TPCv1 Threshold
    - TPCv2 Threshold
    - Data Rates

Radio Frequency (RF) High Availability

Everything Starts from the Quality of the AP

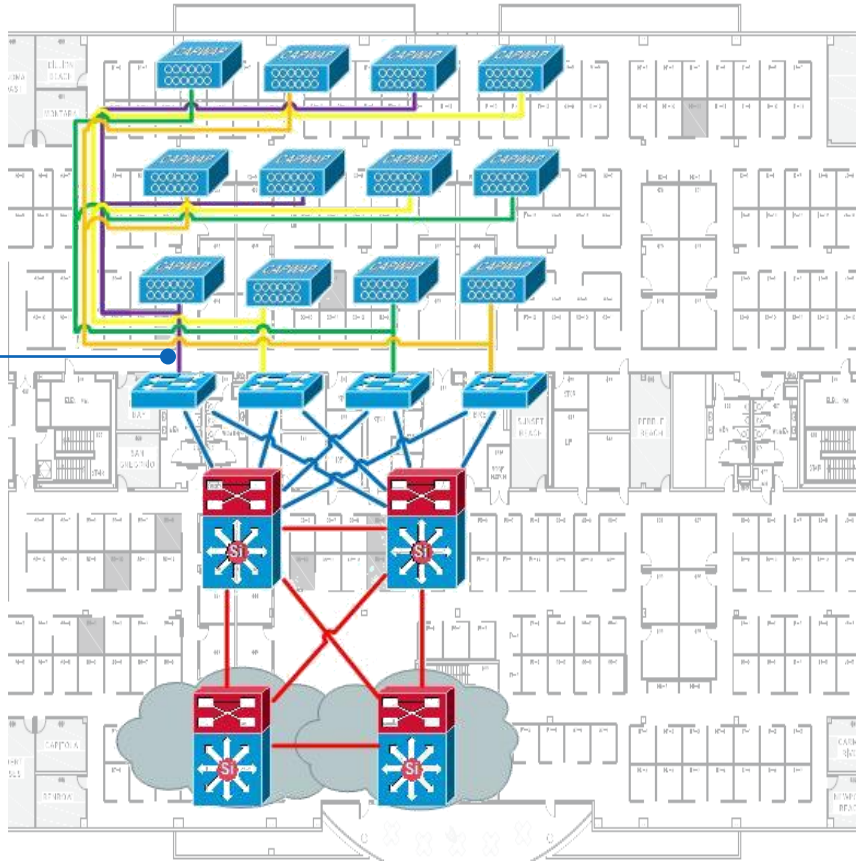
Competitor	Cisco AP
	
Off-the-Shelf plastic designs. Open air vent cooling. Poor Performance AP made with Consumer-grade Materials.	Sealed metal shell for heat-dissipation and durability. No air flow. High Performance Enterprise-Class AP with Reliable Coverage.

Network Infrastructure HA

Network Infrastructure HA

How to physically connect AP

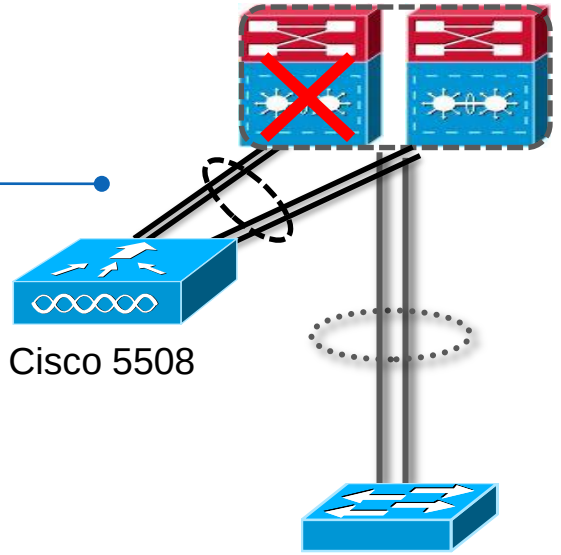
- Create redundancy throughout the access layer by homing APs into different switches
- If the AP is in Local mode, configure the port as access with SPT Portfast
- If the AP is in Flex mode and Local Switching, configure the port as trunk and allow only the VLANs you need



Network Infrastructure HA

How to physically connect 5508 WLC

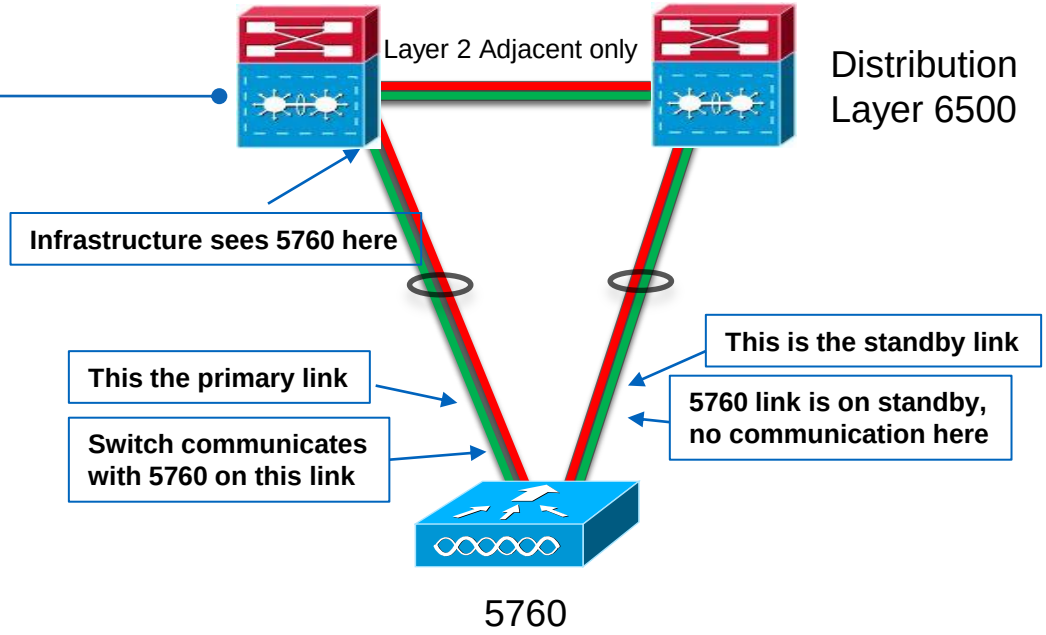
- Use LAG (EtherChannel)
- AireOS based WLC do not support multiple LAGs
- Cisco 5508 WLC can be attached to a Cisco Catalyst VSS switch pair:
  - 4 ports of Cisco 5508 are connected to active VSS switch
  - 2nd set of 4 ports of Cisco 5508 is connected to standby VSS switch
  - In case of failure of primary switch traffic continues to flow through secondary switch in the VSS pair



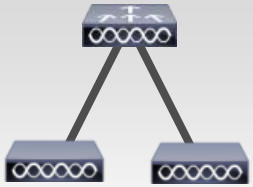
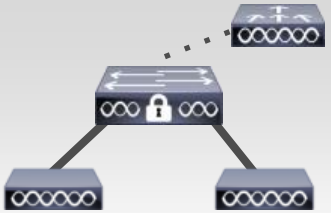
Network Infrastructure HA

How to physically connect 5760

- 5760 supports multiple LAGs
- Don't need to have VSS
- FlexLink is one of the options to connect the 5760 to Distribution
- With FlexLink one link is active and the other Standby



Network Level HA

	Autonomous	FlexConnect	Centralised	Converged Access
				
	Standalone APs	Traffic Distributed at AP	Traffic Centralised at Controller	Traffic Distributed at Switch

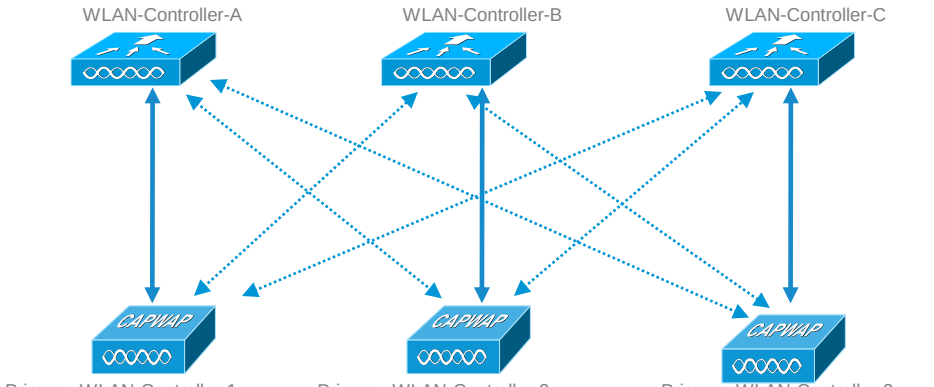
Target Positioning	Small Wireless Network	Branch	Campus	Branch and Campus
Purchase Decision	Wireless only	Wireless only	Wireless only	Wired and Wireless
High Availability	• Can only claim AP quality • No RF HA • No Network layer HA • No services	• Full RF HA • Client SSO when Local Switching	• Most complete solution	• Exploits HA in IOS switches
Key Considerations	• Limited features. Upgradable to controller based	• Branch with WAN BW and latency requirements	• Full features	• Catalyst 3650/3850 in the access layer

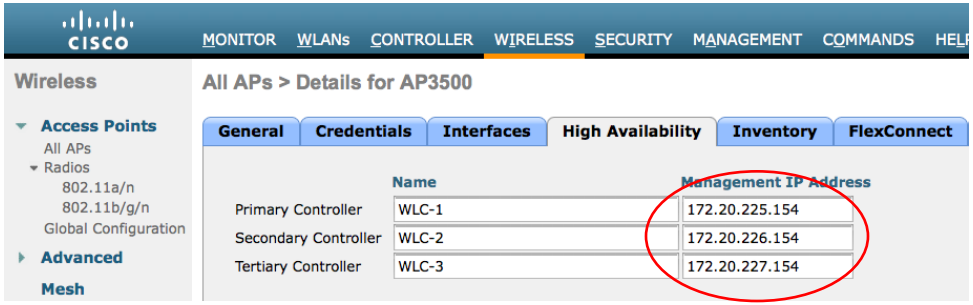
Network Infrastructure HA – Centralised Mode

Centralised Mode HA

	Requirements	Benefits
Client SSO	Minimum release: 7.5 WLC: 5508, WiSM2, 7500, 8510 L2 connection Same HW and software 1:1 box redundancy	Active Client State is synched AP state is synched No Application downtime HA-SKU available
AP SSO (SSID stateful switchover)	Release: 7.3 and 7.4 WLC: 5508, WiSM2, 7500, 8510 Direct physical connection Same HW and SW 1:1 box redundancy	AP state is synched No SSID downtime HA-SKU available (> 7.4)
N+1 Redundancy (Deterministic/Stateless HA, a.k.a.: primary/secondary/tertiary)	Each Controller has to be configured separately	Available on all controllers Crosses L3 boundaries Flexible: 1:1, N:1, N:N HA-SKU available (> 7.4)

N+1 Redundancy

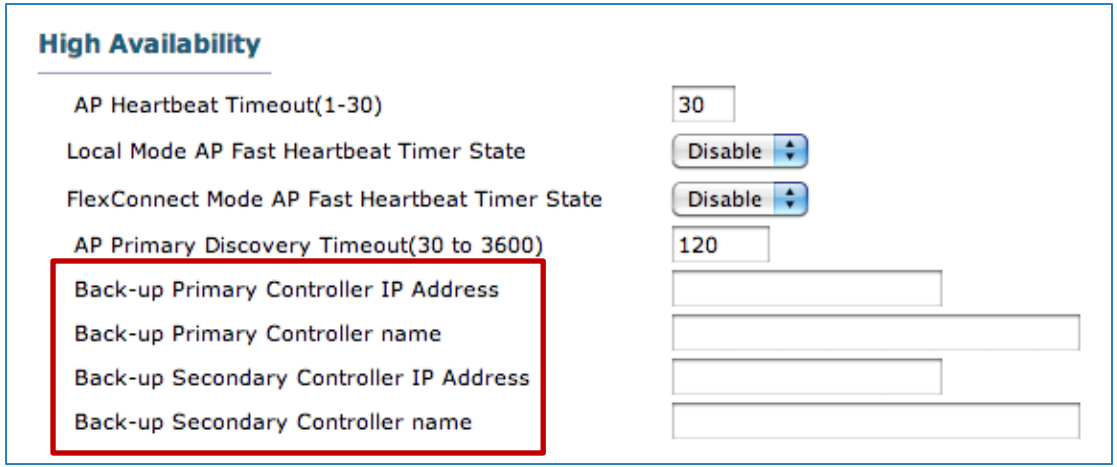




- Administrator statically assigns APs a primary, secondary, and/or tertiary controller
  - Assigned from controller interface (per AP) or Prime Infrastructure (template-based)
  - You need to specify Name and IP if WLCs are not in the same Mobility Group
- Pros:
  - Support for L3 network between WLCs
  - Flexible redundancy design options (1:1, N:1, N:N:1)
  - WLCs can be of different HW and SW
  - Predictability: easier operational management
  - Faster failover times configurable
  - “Fallback” option in the case of failover
- Cons:
  - Stateless redundancy
  - More upfront planning and configuration

N+1 Redundancy

Global backup Controllers

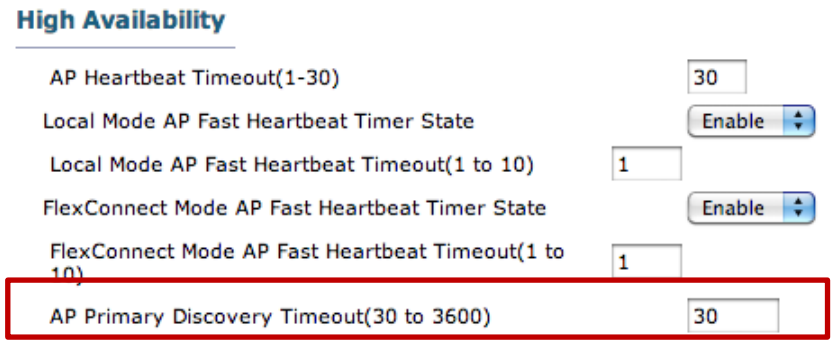


- Backup controllers configured for all APs under Wireless > High Availability
- Used if there are no primary/secondary/tertiary WLCs configured on the AP
- The backup controllers are added to the primary discovery request message recipient list of the AP.

N+1 Redundancy

AP Primary Discovery Request Timer

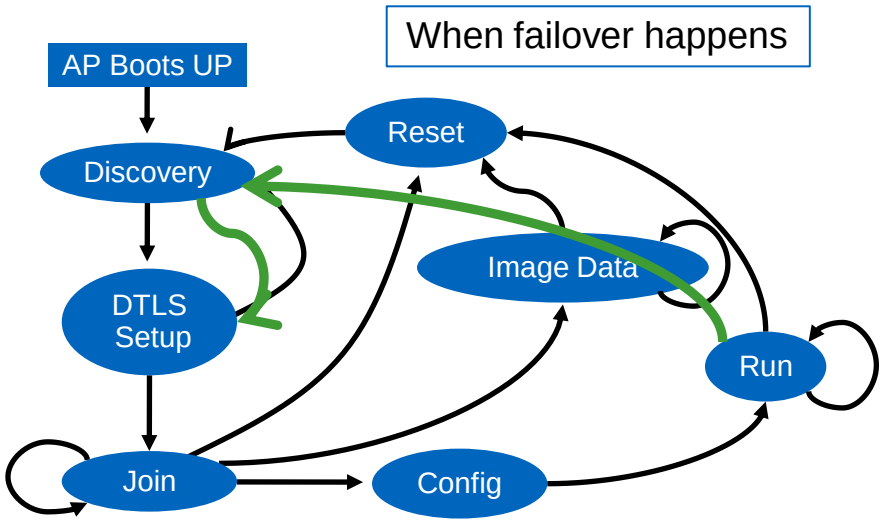
- The access point maintains a list of backup controllers and periodically sends primary discovery requests to each entry on the list.
- Configure a primary discovery request timer to specify the amount of time that a controller has to respond to the discovery request



N+1 Redundancy

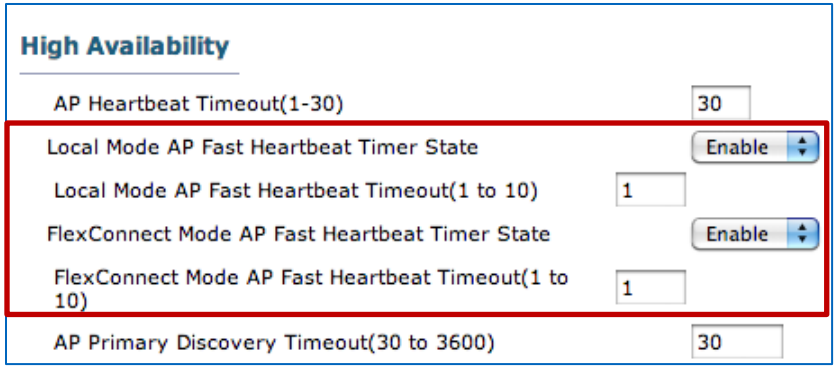
AP Failover Mechanism

- When configured with Primary and backup Controller:
  - AP uses heartbeats to validate current WLC connectivity
  - AP uses Primary Discovery message to validate backup WLC list (every 30 sec)
  - When AP looses 5 heartbeats it start join process to first backup WLC candidate
  - Candidate Backup WLC is the first alive WLC in this order : primary, secondary, tertiary, global primary, global secondary.
  - Failover is faster than Dynamic mode because AP goes back to discovery state just to make sure the backup WLC is UP and then immediately starts the JOIN process



AP Failover

Fast Heartbeat

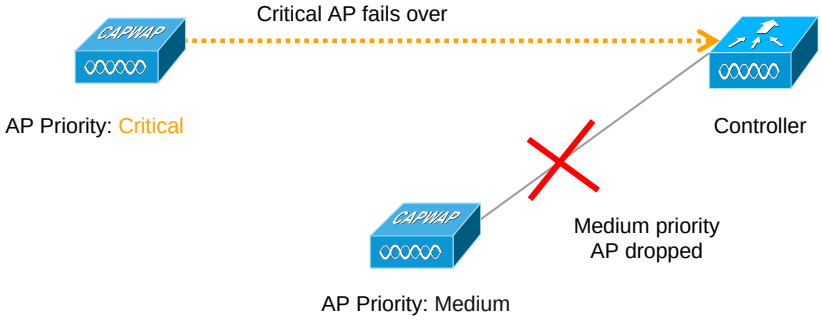


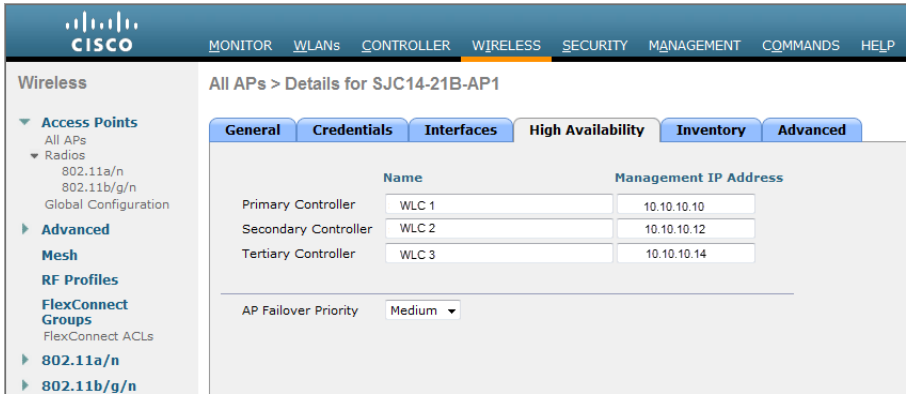
- AP sends HA heartbeat packets, by default every 1 sec
- Fast Heartbeats reduce the amount of time it takes to detect a controller failure
- When the fast heartbeat timer expires, the AP sends a 3 fast echo requests to the WLC for 3 times
- If no response primary is considered dead and the AP selects an available controller from its “backup controller” list in the order of primary, secondary, tertiary, primary backup controller, and secondary backup controller.
- Fast Heartbeat only supported for Local and Flex mode

AP Failover

AP Failover Priority

- Assign priorities to APs: Critical, High, Medium, Low
- Critical priority APs get precedence over all other APs when joining a controller
- In a failover situation, a higher priority AP will be allowed in ahead of all other APs
- If controller is full, existing lower priority APs will be dropped to accommodate higher priority APs

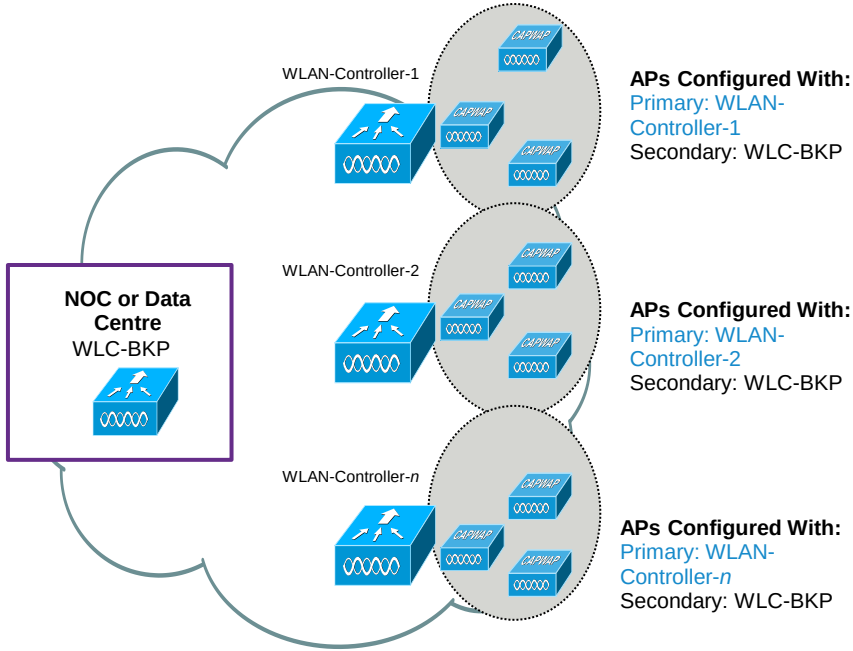




N+1 Redundancy

Best Practices

- Most common Design is N+1 with Redundant WLC in a geographically separate location
- Configure high availability parameters to detect failure and faster failover (min 30 sec)
- Use AP priority in case of over subscription of redundant WLC, or
- Use HA SKU available for 5508, 7500, 8500 and 2500 (from 7.5) controllers

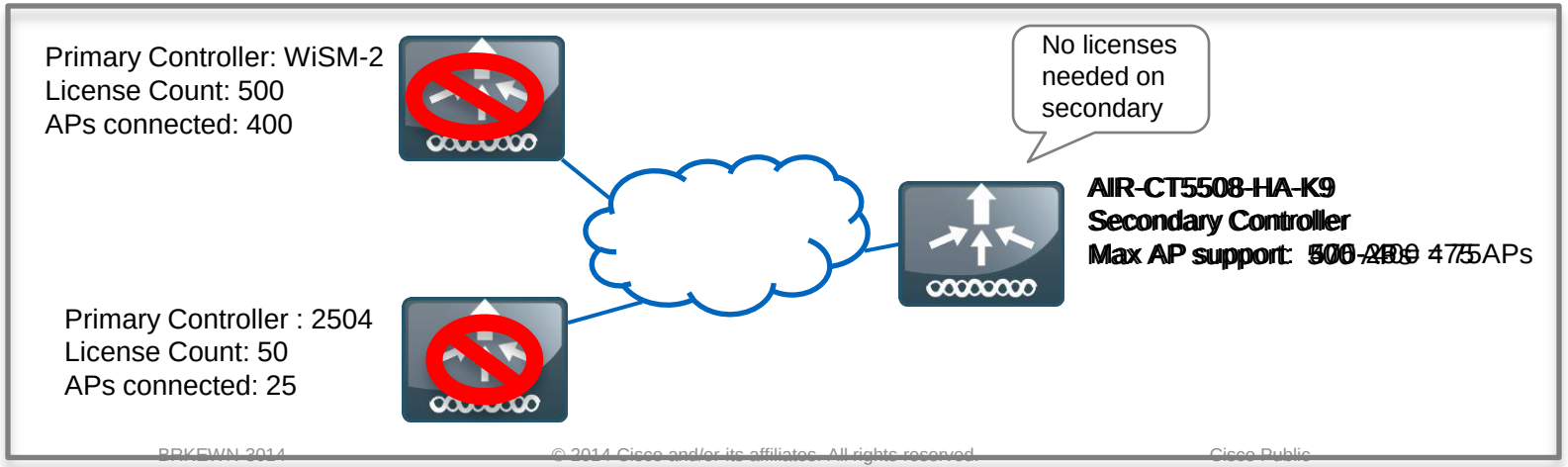


For more info: http://www.cisco.com/en/US/docs/wireless/technology/hi_avail/N1_HA_Overview.html or http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps10315/qa_c67-714540.html

N+1 Redundancy

HA-SKU

- No need to purchase licenses on backup WLC. When backup takes over, 90-days counter is started
- HA-SKU Controller needs to be configured normally as you would do with the secondary controller (no auto synch).
- Supported on 5508, WiSM2, Flex7500, 8510 and 2504
- The HA-SKU provides the capability of the maximum number of APs supported on that hardware
- From 7.6 you can add licenses to HA SKU and use it as Active controller



Centralised Mode: Stateful Switchover

Quick Recap…

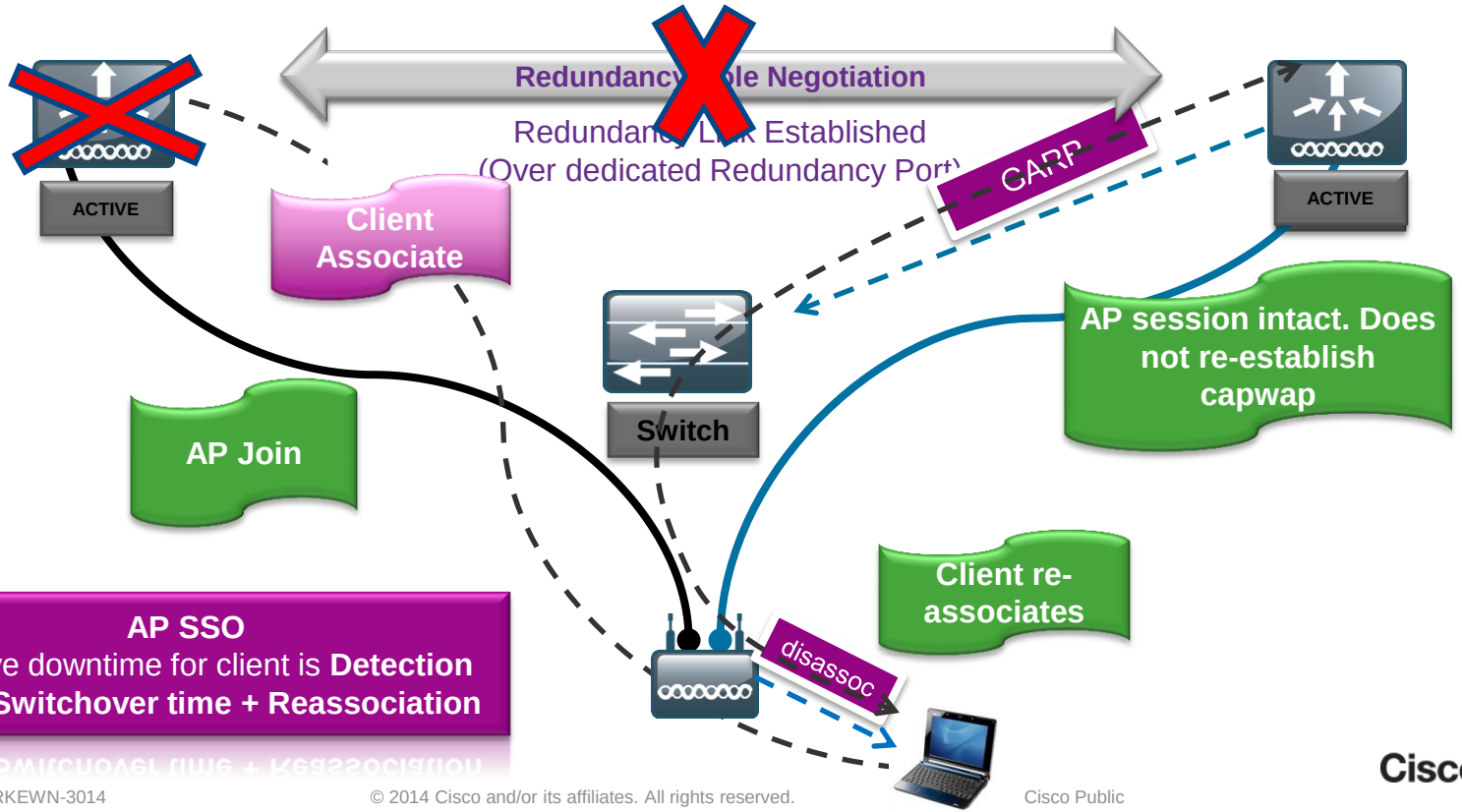
- Primary/Secondary/Tertiary WLC need to be defined on each AP
  - Each WLC configured separately and have their own unique IP Address
- Primary and Secondary Backup are configured Globally
- Fast Heartbeat can be used to speed up failover
- With Failover detection AP goes in Discovery State and CAPWAP State Machine is restarted
- Downtime between Failover may go up to 1.5 minutes depending upon number of APs
- Each WLC is managed and monitored separately by Prime Infrastructure

Stateful Switchover (SSO)

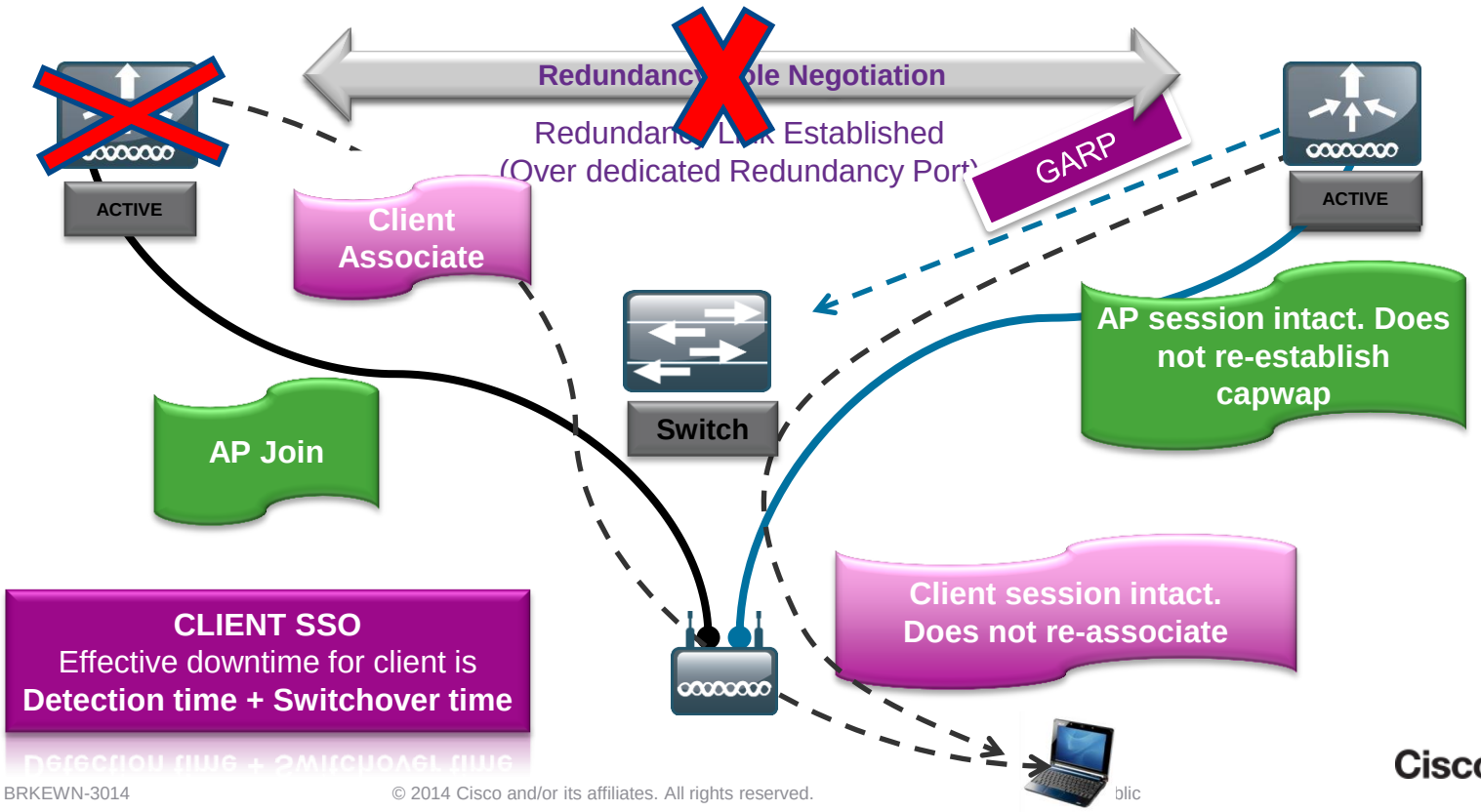
- True Box to Box High Availability i.e. 1:1
  - One WLC in Active state and second WLC in Hot Standby state
  - Secondary continuously monitors the health of Active WLC via dedicated link
- Configuration on Active is synched to Standby WLC
  - This happens at startup and incrementally at each configuration change on the Active
- What else is synched between Active and Standby?
  - AP CAPWAP state in 7.3 and 7.4: APs will not restart upon failover, SSID stays UP – **AP SSO**
  - Active Client State in 7.5: client will not disconnect – **Client SSO**
- Downtime during failover reduced to 5 - 1000 msec depending on Failover
  - In the case of power failure on the Active WLC it may take 350-500 msec
  - In case of network failover it can take up to few seconds
- SSO is supported on 5500 / 7500 / 8500 and WiSM-2 WLC

For more info: http://www.cisco.com/en/US/docs/wireless/controller/technotes/7.5/High_Availability_DG.html

AP SSO Failover Sequence



Client SSO Failover Sequence



Stateful Switch Over (SSO)

Redundancy Management Interface

- Redundancy Management Interface (RMI)
  - To check gateway reachability sending ICMP packets every 1 sec
  - To verify peer reachability via the network once the Active does not respond to keepalives on the Redundant Port
  - Notification to standby in event of box failure or manual reset
  - Communication with Syslog, NTP, TFTP server for uploading configurations
  - Should be in same subnet as Management Interface

```
(5508) >show interface summary


 Number of Interfaces..... 5

Interface Name                   Port Vlan Id  IP Address      Type    Ap Mgr Guest
-------------------------------- ---- -------- --------------- ------- ------ -----
management                       1    61       9.6.61.2        Static  Yes    No
redundancy-management            1    61       9.6.61.22       Static  No     No
redundancy-port                  N/A  N/A      169.254.61.22   Static  No     No
service-port                     N/A  N/A      0.0.0.0         Static  No     No
virtual                          N/A  N/A      1.1.1.1         Static  No     No
```

Stateful Switchover (SSO)

Redundancy Port

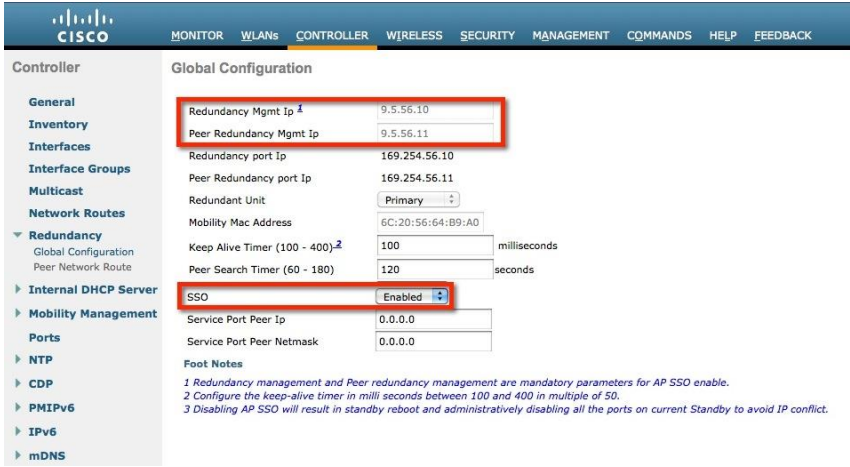
- Redundancy Port (RP):
  - To check peer reachability sending udp keep alive messages every 100 msec
  - Notification to standby in event of box failure
  - Configuration synch from Active to Standby (Bulk and Incremental Config)
  - Auto generated IP Address where last 2 octets are picked from the last 2 octets of Redundancy Management Interface (First 2 octets are always 169.254)
  - If NTP is not configured manual time synch is done from Active to Standby

```
(5508) >show interface summary


 Number of Interfaces..................... 5

Interface Name                   Port Vlan Id  IP Address      Type    Ap Mgr Guest
-------------------------------- ---- -------- --------------- ------- ------ -----
management                       1    61       9.6.61.2        Static  Yes    No
redundancy-management            1    61       9.6.61.22       Static  No     No
redundancy-port                  N/A  N/A      169.254.61.22   Static  No     No
service-port                     N/A  N/A      0.0.0.0         Static  No     No
virtual                          N/A  N/A      1.1.1.1         Static  No     No
```

Stateful Switchover (SSO)

Configuration

- Before configuring HA, Management interfaces on both WLCs must be on the same subnet
- Mandatory Configuration for HA setup:
  - Redundant Management IP Address
  - Peer Redundant Management IP Address
  - Redundancy Mode set to SSO enable (7.3 and 7.4 would show AP SSO)
  - Primary/Secondary Configuration – Required if peer WLC's UDI is not HA SKU
  - The Primary HA must have valid AP licenses
  - Unit can be secondary if it has at least 50 AP permanent licenses



Optional Configuration:
- Service Port Peer IP
- Mobility MAC Address
- Keep Alive and Peer Search Timer

All can be configured on same page

Stateful Switchover (SSO)

HA Pairing

For Your Reference

- Pairing is possible only between same type of hardware and software version.
- Reboot of WLC is required after HA is enabled. Pairing happens when WLC is booting.
- WLC looks for peer (120 sec), the role is determined, configuration is synched from the Active WLC to the Standby WLC via the Redundant Port.
- Initially, the WLC configured as Secondary will report XML mismatch and will download the configuration from Active and reboot again

```
Starting certificate database: ok
Starting VPN Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
Starting LWAPP: ok
Starting CAPWAP: ok
Starting LOCP: ok
Starting Security Services: ok
Starting Policy Manager: ok
Starting Authentication Engine: ok
Starting Mobility Management: ok
Starting Virtual AP Services: ok
```


Cisco live!

Stateful Switchover (SSO)

HA Pairing

For Your Reference

- During the second reboot, after role determination, Secondary WLC will validate the configuration again, report no XML mismatch, and process further in order to establish itself as the Standby WLC

```
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
Standby started downloading configurations from Active...

Standby comparing its own configurations with the configurations downloaded from Active...


Startup XMLs are different, reboot required
New XML downloaded Category: rsyncmgrXferTrasport.
```

Stateful Switchover (SSO)

HA Pairing

For Your Reference

- While config is synching from Active to Standby WLC or Standby WLC is booting no config operation is possible on Active WLC.

```
(5508) >config network webmode enable
AAA_AuthorizeUser:Configurations blocked as standby WLC is still booting up, try after few moments.
```

- Active and Standby election is not an automated process:
  - Active/Standby WLC is decided based on HA SKU. HA SKU is always the Standby
  - If no HA SKU present, Active/Standby is configurable
- No configuration is possible on Standby WLC once paired:

```
(5508-Standby) >?

debug           Manages system debug options.
help            Help
logout          Exit this session. Any unsaved changes are lost.
ping            Send ICMP echo packets to a specified IP address.
reset           Reset options.
show            Display switch options and settings.
```


Cisco live!

Stateful Switchover (SSO)

Configuration Validation

- Main command is “show redundancy summary”

```
(POD1-WLC) >show redundancy summary
            Redundancy Mode = SSO ENABLED
                Local State = ACTIVE
                 Peer State = STANDBY HOT
                       Unit = Primary
                    Unit ID = E0:2F:6D:5C:F0:4
          Redundancy State = SSO (Both AP and
                Mobility MAC = E0:2F:6D:5C:F0:4
Management Gateway Failover = ENABLED (Managem
          Link Encryption = DISABLED

Redundancy Management IP Address.....
Peer Redundancy Management IP Address.....
Redundancy Port IP Address.....
Peer Redundancy Port IP Address.....
Peer Service Port IP Address.....
```

```
(POD1-WLC-Standby) >show redundancy summary
            Redundancy Mode = SSO ENABLED
                Local State = STANDBY HOT
                 Peer State = ACTIVE
                       Unit = Secondary - HA SKU (Inherited AP License Count = 62)
                    Unit ID = E0:2F:6D:5C:EE:A0
          Redundancy State = SSO (Both AP and Client SSO)
                Mobility MAC = E0:2F:6D:5C:F0:40

Average Redundancy Peer Reachability Latency = 1452 usecs
Average Management Gateway Reachability Latency = 750 usecs

Redundancy Management IP Address..... 10.10.10.11
Peer Redundancy Management IP Address..... 10.10.10.10
Redundancy Port IP Address..... 169.254.10.11
Peer Redundancy Port IP Address..... 169.254.10.10
```

Stateful Switchover (SSO)

Connectivity to the boxes

- Only Console and Service Port is available to connect to Standby WLC
- TFTP, NTP and Syslog traffic use the Redundant Management Interface on the Standby WLC
- Telnet / SSH / SNMP / Web Access is not available on Management and Dynamic interface on Standby WLC
- When SSO is enabled, there is no SNMP/GUI access on the service port for both the WLCs in the HA setup

Stateful Switchover (SSO)

Maintenance Mode

- Standby WLC may transition to Maintenance Mode if:
  - Gateway not reachable via Redundant Management Interface
  - Software mismatch
  - WLC with HA SKU have never discovered its peer
  - Redundant Port is down

```
(5508-Standby) >show redundancy summary
 Redundancy Mode = SSO ENABLED
      Local State = NEGOTIATION
       Peer State = DISABLED
             Unit = Secondary - HA SKU
          Unit ID = 00:24:97:69:78:20
Redundancy State = Non Redundant
    Mobility MAC = 00:24:97:69:D2:20

Maintenance Mode = Enabled
Maintenance cause= Negotiation Timeout

Redundancy Management IP Address.............. 9.6.61.23
Peer Redundancy Management IP Address.......... 9.6.61.21
Redundancy Port IP Address..................... 169.254.61.23
Peer Redundancy Port IP Address................ 169.254.61.21
```

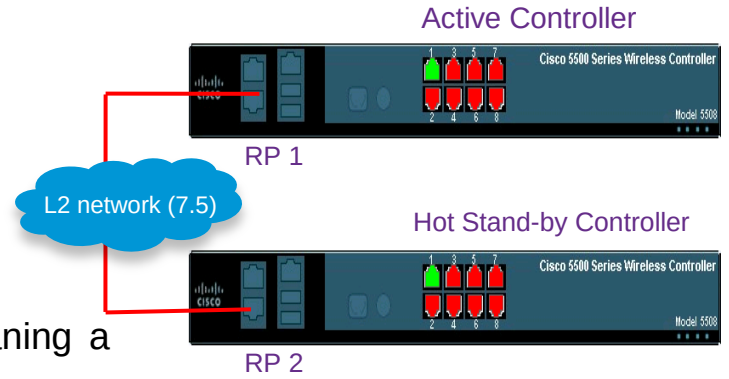
- In Maintenance mode same rule to connect to standby box apply
- WLC should be rebooted to bring it out of Maintenance Mode
  - From 7.6 it will recover automatically after the network converges again

Stateful Switchover (SSO)

Design & Deployment Considerations

How shall I connect the HA Controllers?

- 5500/7500/8500 have dedicated Redundancy Ports
  - Direct connection supported in 7.3 and 7.4
  - L2 connection supported in 7.5 and above
- WiSM-2 has dedicated Redundancy VLAN
  - Redundancy VLAN should be a non-routable VLAN, meaning a Layer 3 interface should not be created for this VLAN
  - WISM-2 can be deployed in single chassis OR multiple chassis
  - WISM-2 in multiple chassis needs to use VSS (7.3, 7.4)
  - WISM-2 in multiple chassis can be L2 connected in 7.5 and above
- Requirements for L2 connection: RTT Latency: < 80 ms; Bandwidth: > 60 Mbps; MTU: 1500



Stateful Switchover (SSO)

Design & Deployment Considerations

- HA Pairing is possible only between the same type of hardware and software versions
- Physical connection between Redundant Ports should be done first before HA configuration
- Keepalive and Peer Discovery timers should be left at default values for better performance
- Internal DHCP is not supported when HA configuration is enabled
- Location, Rogue information, Device and root certificates are not auto synched
- When HA is disabled on Active it will be pushed to Standby and after reboot all the ports will come up on Active and will be disabled on Standby
- SSO and MESH APs: only RAP are supported from 7.5, for MAPs the state is not synched
- In Service Software Upgrade (ISSU) is not supported: plan for down time when upgrading software

Stateful Switchover (SSO)

Design & Deployment Considerations: Software Upgrade Procedure

For Your Reference

After the WLCs are configured in the HA setup, the Standby WLC cannot be upgraded directly from the TFTP/FTP server.

1. Initiate upgrade on the Active WLC in the HA setup via CLI/GUI, and wait for the upgrade to finish.
2. Once the Active WLC executes all the upgrade scripts, it will transfer the entire image to the Standby WLC via the Redundant Port.
3. When the Standby WLC receives the image from the Active WLC, it will start executing the upgrade scripts.
4. Issue the show boot command on the Active WLC in order to make sure the new image is set as the primary image.
5. Once verified, optionally initiate primary image pre-download on the Active WLC in order to transfer the new image to all the APs in the network.
6. It is recommended to reboot both the WLCs almost together after upgrade so that there is no software version mismatch. The Standby WLC can be rebooted from the Active WLC using the reset peer-system command if a scheduled reset is not planned.
7. Schedule Reset applies to both the WLCs in the HA setup. The peer WLC reboots one minute before the scheduled timer expiry on the Active WLC.

Stateful Switchover (SSO)

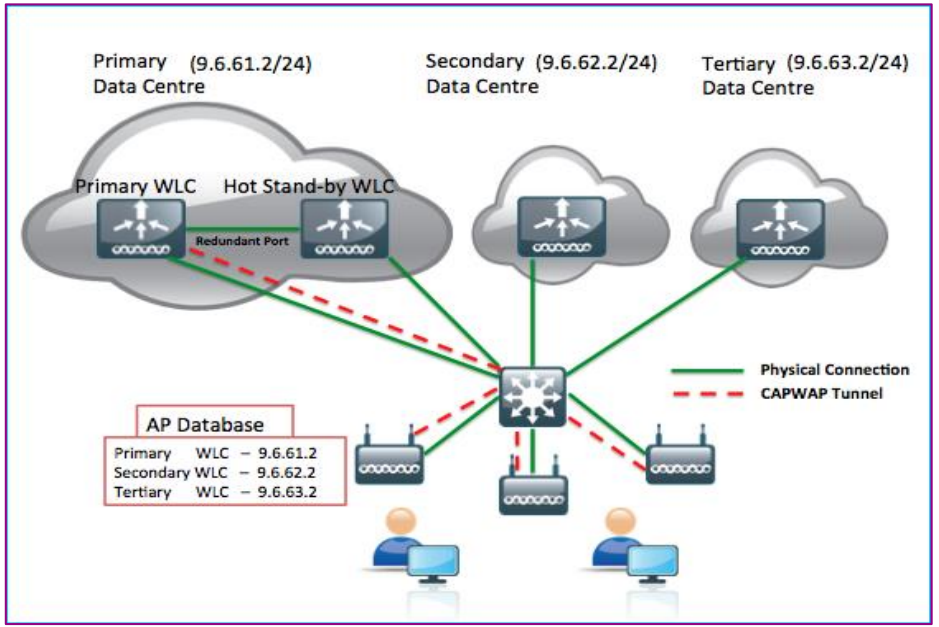
Design & Deployment Considerations Specific to 7.5 (Client SSO)

- ONLY Clients in RUN state are maintained during failover
  - Transient list is deleted
  - Clients in transitions like roaming, dot1x key regeneration, webauth logout, etc. are disassociated
  - Posture and NAC OOB are not supported, since client is not in RUN state
- Some clients and related information are not synced between Active and Standby
  - CCX Based apps - need to be re-started post Switch-over
  - Client Statistics are not synced
  - PMIPv6, NBAR, SIP static CAC info need to be re-learned after SSO
  - WGB and clients associated to it are not synced
  - OEAP(600) clients are not synced
  - Passive clients are not synced
- New mobility is NOT supported with SSO

Stateful Switchover (SSO)

Design: Integration with N+1 Deployments

- Hybrid Design: SSO HA can work together with N+1 failover
- SSO pair can act as the Primary Controller and be deployed with Secondary and Tertiary
- On failure of both Active and Standby WLC in SSO setup, APs will fall back to secondary and further to configured tertiary controller
- Useful to reduce downtime for SSO pair software upgrade



Stateful Switchover (SSO)

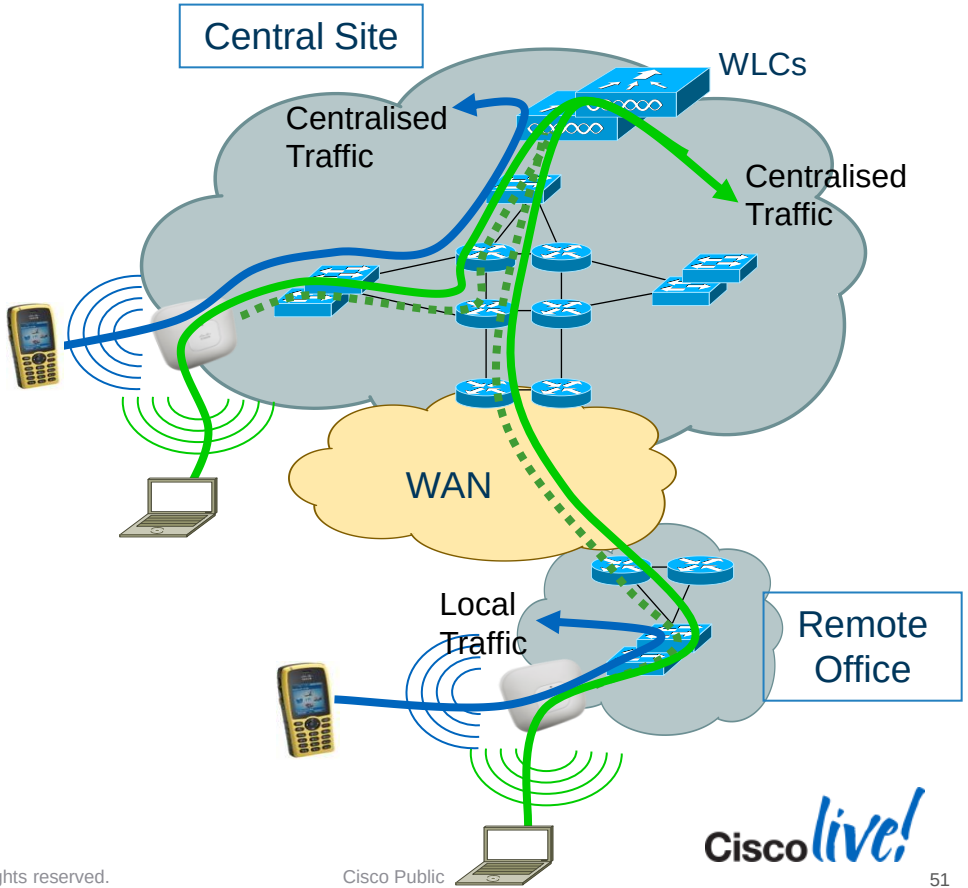
Licensing

- HA Pair with HA-SKU License on one WLC:
  - HA-SKU is a new SKU with Zero AP Count License
  - The device with HA-SKU becomes Standby first time it pairs up
  - AP-count license info will be pushed from Active to Standby
  - On event of Active failure HA-SKU will let APs join with AP-count obtained and will start 90-day count-down. The granularity of the same is in days.
  - After 90-days, HA-SKU WLC starts nagging messages but won't disconnect connected APs
  - With new WLC coming up HA SKU, at the time of paring, the Standby will get the AP Count:
    - If new WLC has higher AP count than previous, 90 days counter is reset.
    - If new WLC has lower AP count than previous, 90 days counter is not reset.
    - Elapsed time and AP-count are remembered on reboot

Network Infrastructure HA – FlexConnect

FlexConnect Quick Recap....

- Control plane, two modes of operation:
  - Connected (when WLC is reachable)
  - Standalone (when WLC is not reachable)
- Data Plane can be:
  - Centralised (split MAC architecture)
  - Local (local MAC architecture)
- Traffic Switching is configured per AP and per WLAN (SSID)
  - From 7.3 split tunnelling is supported on a WLAN basis
- FlexConnect Group:
  - Defines the Key caching domain for Fast Roaming, allows backup Radius scenarios
- WAN recommendations:
  - Minimum bandwidth 12.8 kbps per AP
  - Round trip latency no greater than 300 ms for data deployments and 100 ms for data + voice deployments



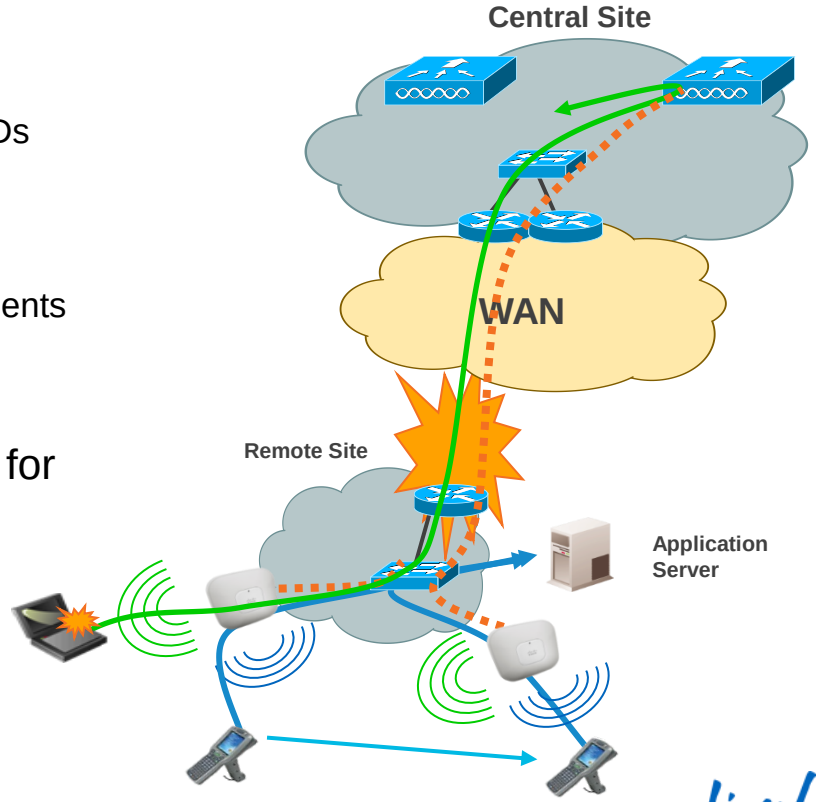
Network HA: FlexConnect Deployment Mode

	Requirements	Benefits
FlexConnect Local Switching	L2 roaming Flex Groups for AAA Local Auth. Fault Tolerance: Identical configuration on N+1 controllers	Upon WLC failure AP stays up and clients are not disconnected Equivalent to Client SSO AAA survivability available
FlexConnect Central Switching	Same as Centralised mode	Same as Centralised mode

For more info: http://www.cisco.com/en/US/products/ps11635/products_tech_note09186a0080b7f141.shtml

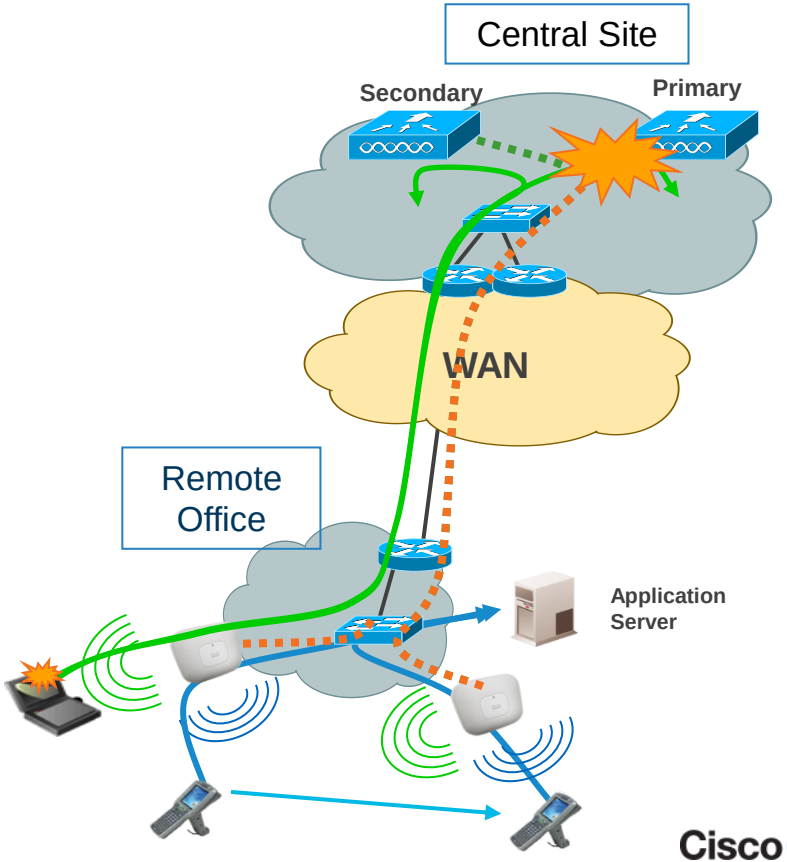
FlexConnect
WAN Failure (or Single Central WLC Failure)

- HA considerations:
  - No impact for connected clients on locally switched SSIDs
  - Disconnection for centrally switched SSIDs clients
- What about new clients?
  - Static keys are locally stored in FlexConnect AP: new clients can join if authentication is PSK
  - Can design for AAA survivability (see next slides)
- Fast roaming allowed within FlexConnect group for already connected clients
- Lost features
  - RRM, CleanAir, WIDS, Location, other AP modes
  - Web authentication, NAC



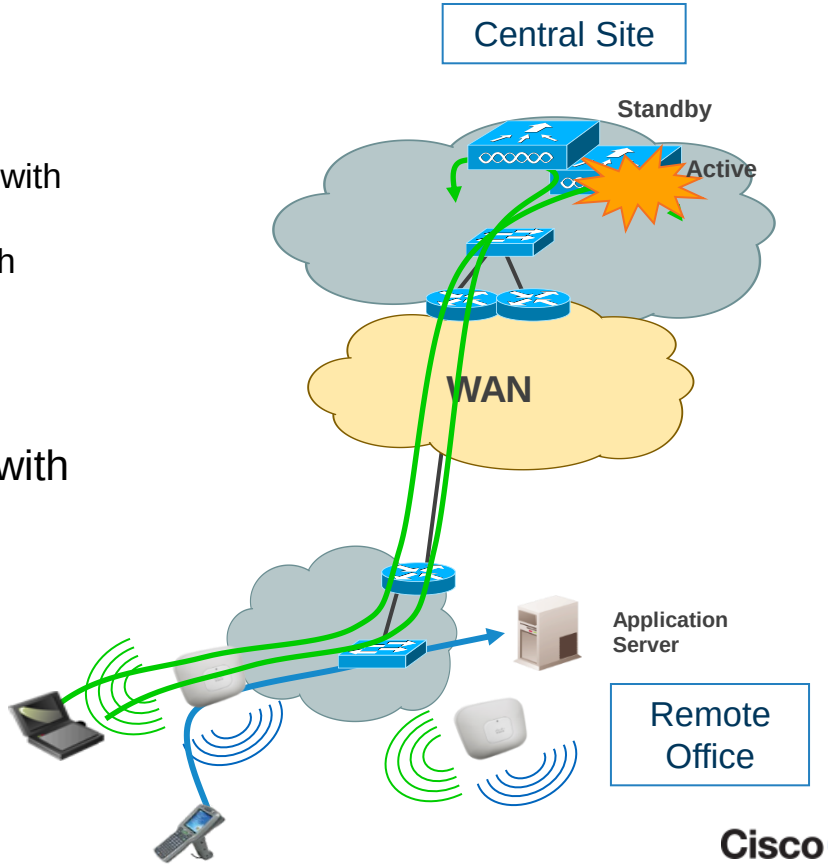
FlexConnect
WLC Failure with Deterministic N+1 HA

- HA considerations:
  - No impact for locally switched SSIDs
  - Disconnection of centrally switched SSIDs clients
- FlexConnect AP transitions to Standalone and then to Connected when joins the Secondary
- When in Standalone mode, Fast roaming is allowed within the FlexConnect Group
- Fault Tolerant: upon re-syncing with Secondary, client sessions for local traffic are not impacted, provided that the configuration on the WLCs are identical



FlexConnect
WLC Failure Scenario with SSO

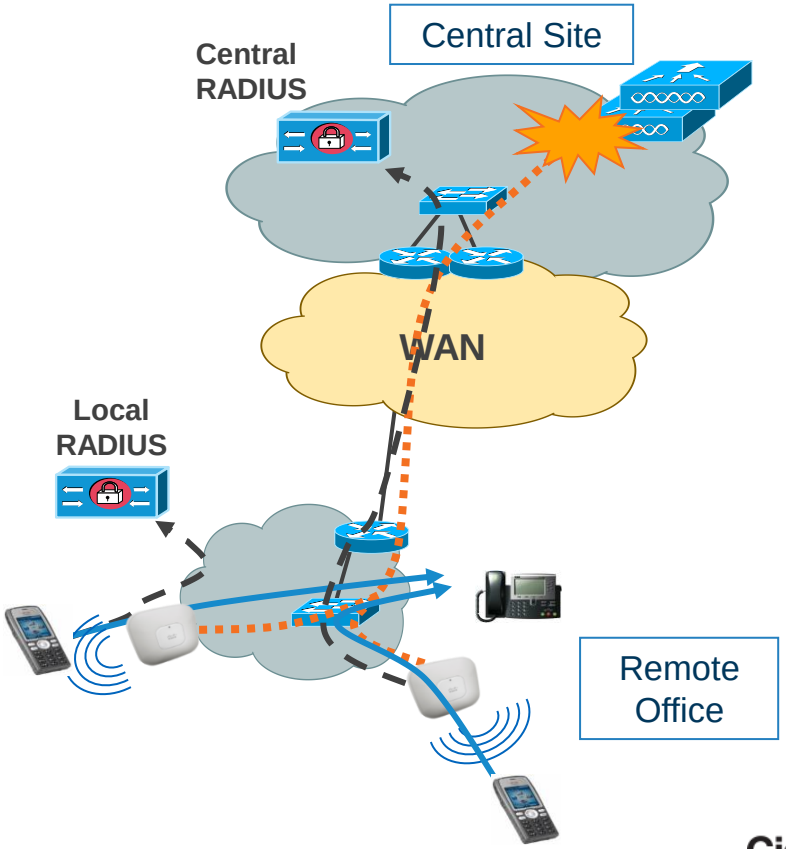
- HA considerations:
  - No impact for locally switched SSIDs
  - Disconnection of centrally switched SSIDs clients with AP SSO
  - No/minimal impact for centrally switched client with Client SSO (7.5 and above)
- FlexConnect AP will NOT transition to Standalone because SSO kicks in
- AP will continue to be in Connected mode with the Standby (now Active) WLC



FlexConnect AAA Survivability

FlexConnect Local Auth

- By default FlexConnect AP authenticates clients through central controller when in Connected mode
- This feature allows AP to act as an Authenticator even in Connected mode
- AAA servers are defined at the FlexGroup level
- Useful HA scenarios:
  - Independent branch: AAA is local at the branch, no AAA traffic goes through WAN
  - WLC goes down but WAN is up. Local users are authenticated from AP to Central site AAA



FlexConnect AAA Survivability

FlexConnect Local Auth: Configuration

For Your Reference

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK

WLANs > Edit 'RackMobility'

< Back | Apply

General | Security | QoS | Advanced

Maximum Allowed Clients [8]: 0

Static IP Tunneling [11]: Enabled

Wi-Fi Direct Clients Policy: Disabled

Maximum Allowed Clients Per AP Radio: 200

Off Channel Scanning Defer

Scan Defer Priority: 0 1 2 3 4 5 6 7 (5, 6, 7 checked)

Scan Defer Time(msecs): 100

FlexConnect

FlexConnect Local Switching [2]: Enabled

FlexConnect Local Auth [12]: Enabled

Learn Client IP Address [5]: Enabled

802.11b/g/n (1 - 255): 1

NAC

NAC State: None

Load Balancing and Band Select

Client Load Balancing

Client Band Select [7]

Passive Client

Passive Client

Voice

Media Session Snooping: Enabled

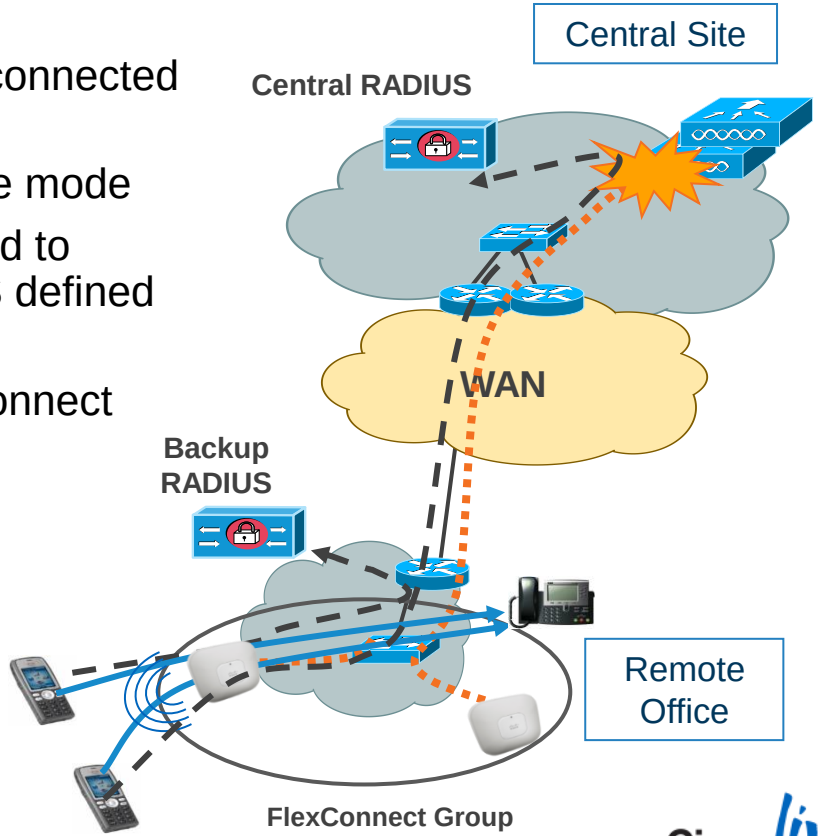
Re-anchor Roamed Voice Clients: Enabled

KTS based CAC Policy: Enabled

FlexConnect AAA Survivability

AAA Server Backup

- By default authentication is done centrally in connected mode
- When WLC/WAN fails, AP goes in Standalone mode
- In Standalone mode, the AP can be configured to authenticate new clients with backup RADIUS defined locally at the AP
- Backup AAA servers are configured at FlexConnect Group level
- Upon WAN/WLC failure:
  - Existing connected clients stay connected
  - New clients are authenticated to the locally defined AAA



FlexConnect AAA Survivability

AAA Server Backup Configuration

For Your Reference

- Define primary and secondary local backup RADIUS server under FlexConnect Group configuration

AAA

Server IP Address	
Server Type	Primary
Shared Secret	
Confirm Shared Secret	
Port Number	1812

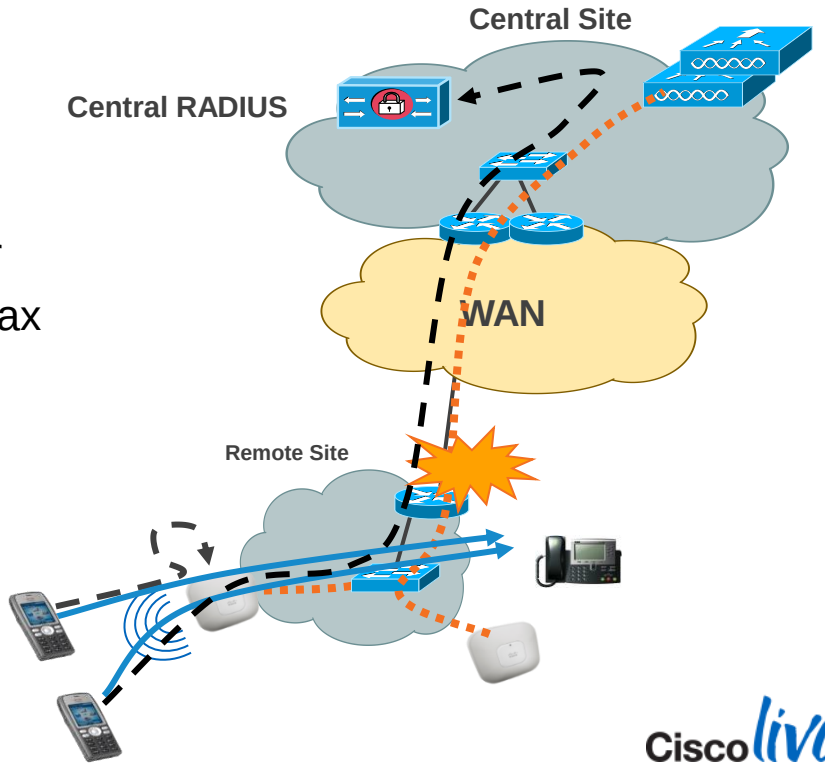
Add

Server Type	Address	Port
Primary	172.16.1.60	1812
Secondary	10.10.5.70	1812

FlexConnect AAA Survivability

AAA Server on AP

- By default authentication is done centrally in connected mode
- When WLC/WAN fails AP goes in Standalone mode
- In Standalone, the AP can act as a AAA server
- EAP-FAST, LEAP, PEAP*, EAP-TLS* and a max of 100 clients supported
- Upon WAN/WLC failure:
  - Existing connected clients stay connected
  - New clients are authenticated to the locally defined AAA

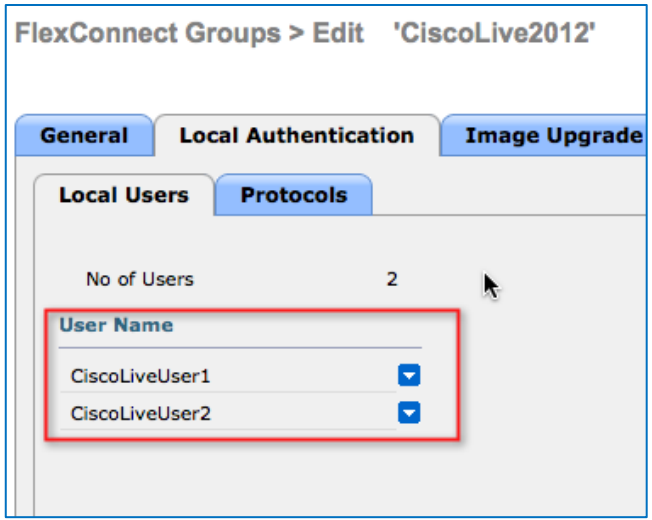


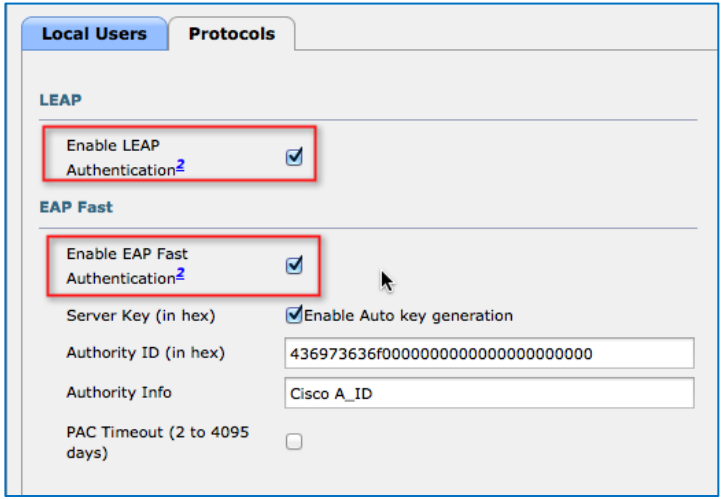
* 7.5 Code and above

FlexConnect
AAA Server on AP - Configuration

For Your Reference

- Define users (max 100) and passwords
- Define EAP parameters (LEAP, EAP-FAST, PEAP, EAP-TLS)

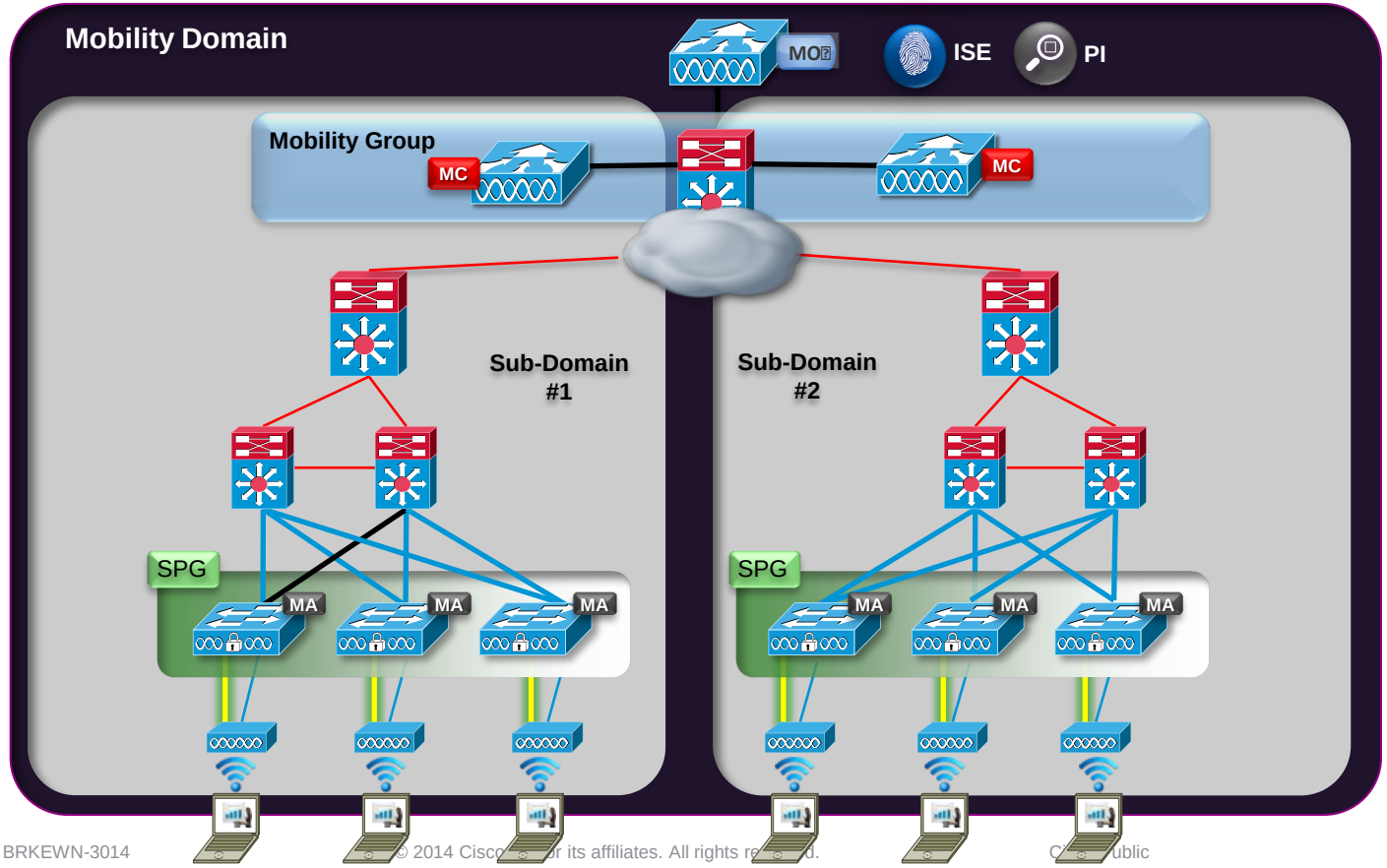




Network Infrastructure HA – Converged Access

Converged Access

Quick recap..



Converged Access: Quick Recap..

- Wireless Controller function in IOS on the Access switch

- Mobility Agent (MA): MA

  Terminates CAPWAP tunnels for locally connected Aps. Handles local clients Database

- Mobility Controller (MC): MC

  Control Plane functions: Handles RRM, Roaming, Switch Peer Groups, etc.

- Switch Peer Group (SPG): SPG

  Group of geographically adjacent switches (MAs) to optimise roaming

- A distributed wireless and wired data plane brings:
  - Scalability, as wireless is terminated at access switch, no hair pinning to a central location
  - Optimised roaming
  - Traffic Visibility as traffic is not CAPWAP tunneled to a central WLC
  - Same tools for troubleshooting that are available for wired
  - Single Point of Ingress for wired and wireless traffic. Common Policy enforcement point for wired and wireless
  - Rich media optimisation: support mission critical application with Qos applied closest to the source

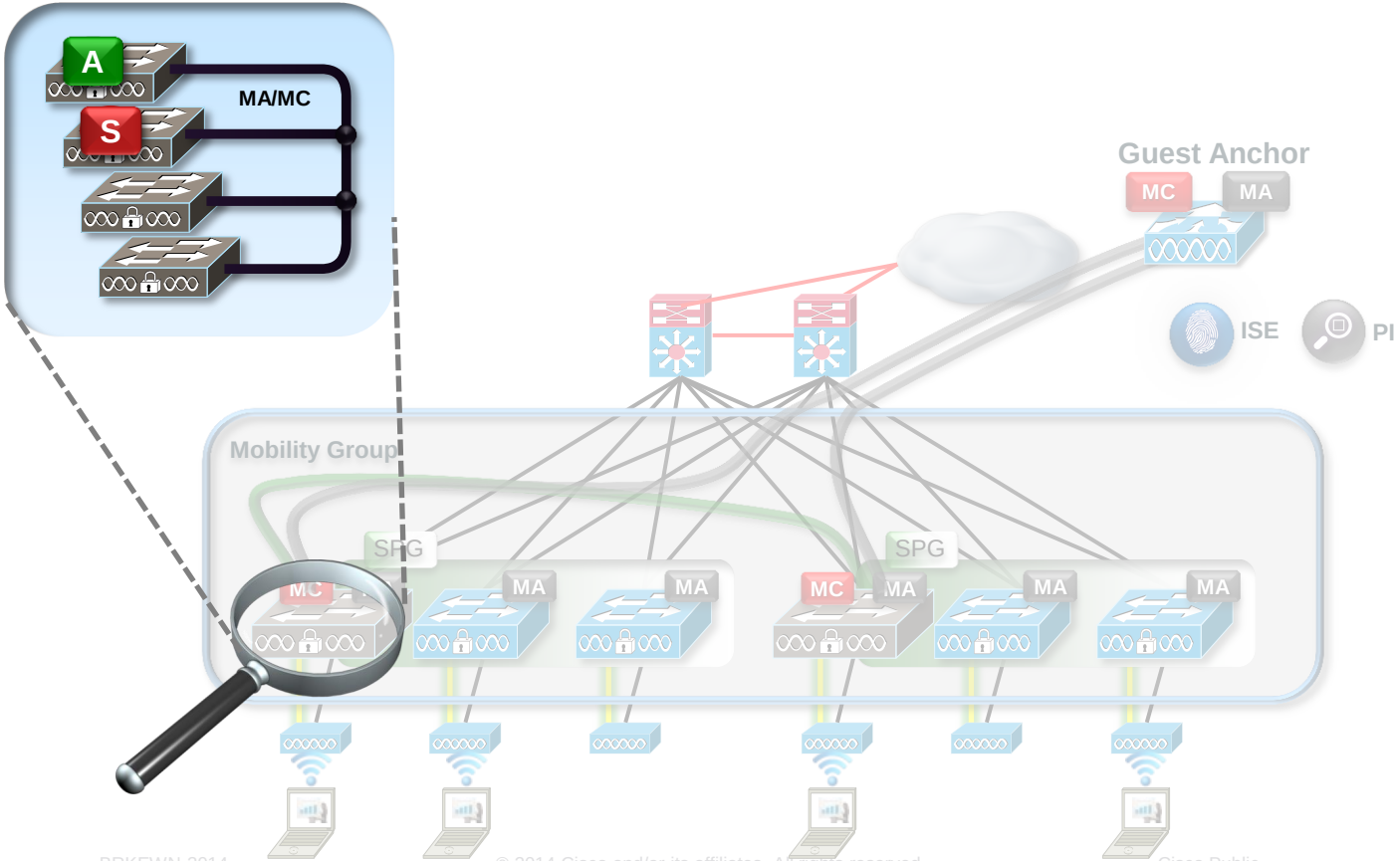
Converged Access Mode HA

	Requirements	Benefits
HA on 5760 (a.k.a. Tunnel SSO)	Release IOS-XE 3.3.0SE Only 2 members stack Stack cables needed Same software	Dynamic Active/Standby election AP CAPWAP information synced Configuration synced Reduced network downtime
HA on 3650/3850 (a.k.a. Tunnel SSO)	Up to 9 members stack in 3.3.0SE Stack cables needed Additional module for 3560	1+1 Stateful redundancy (SSO) Dynamic Active/Standby election Distributed L2/L3 Forwarding Redundancy IOS HA for L3 protocol

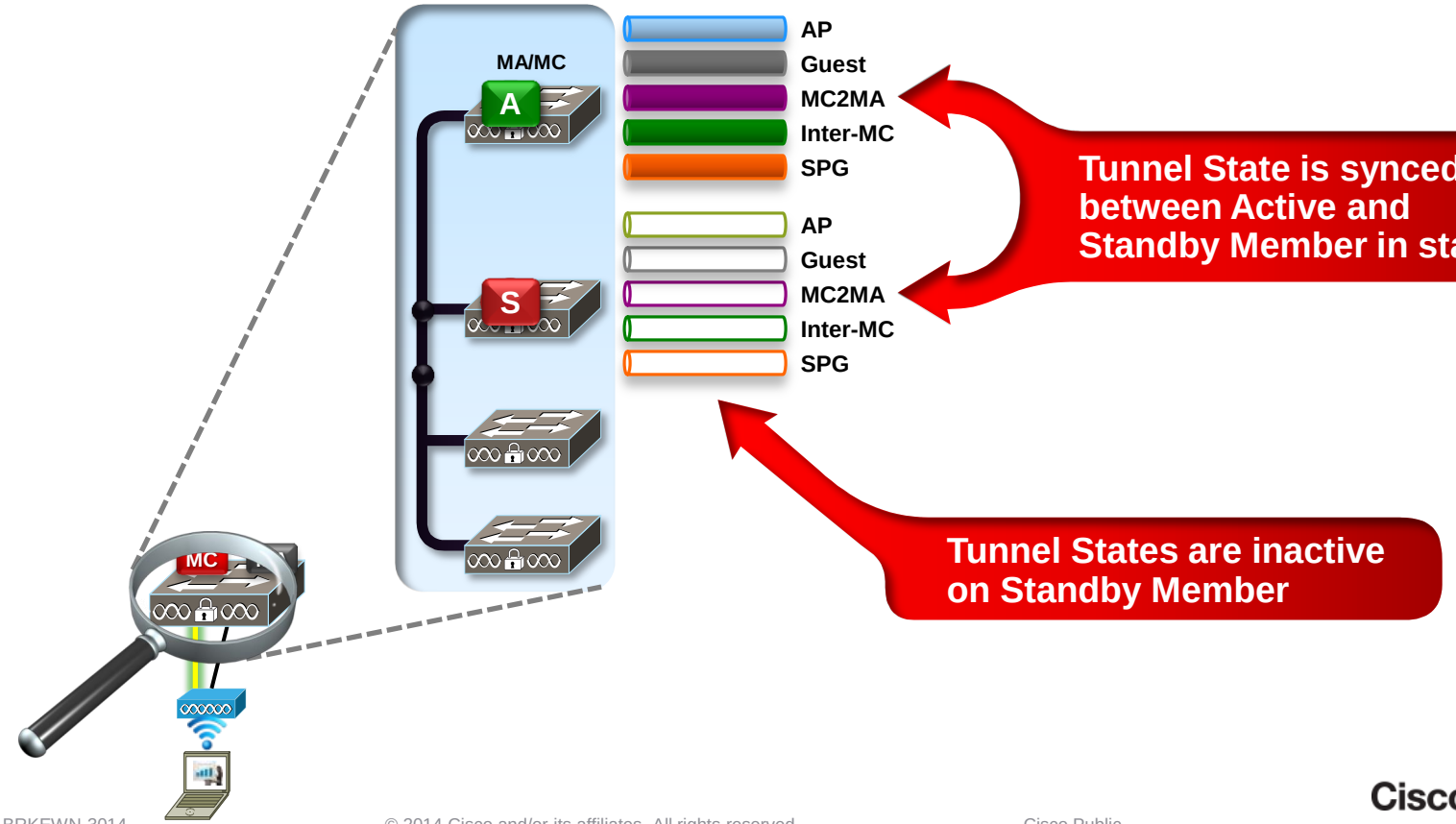
High Availability on the 3850/3650

- Wireless Controller fault is isolated (for example to a single switch/floor)
- HA is available on a per stack basis not between stacks
- There is no HA setup for master-active and master-standby. They are elected automatically by the stack.
  - However, user can set priority level to the members and this is used in the master-active/standby election. Currently, this can be done from CLI
- Licenses are enforced at the MC Level. Licensing best practices:
  - Each switch member in the stack can be licensed independently, up to 25 total AP licenses on 3650 and 50 total on 3850.
  - For best redundancy, it is ideal to enable the proper license count for each stack member, based on the number of APs that will be connected.
  - If the master fails, the remaining switch licenses will still be available to support the other APs.

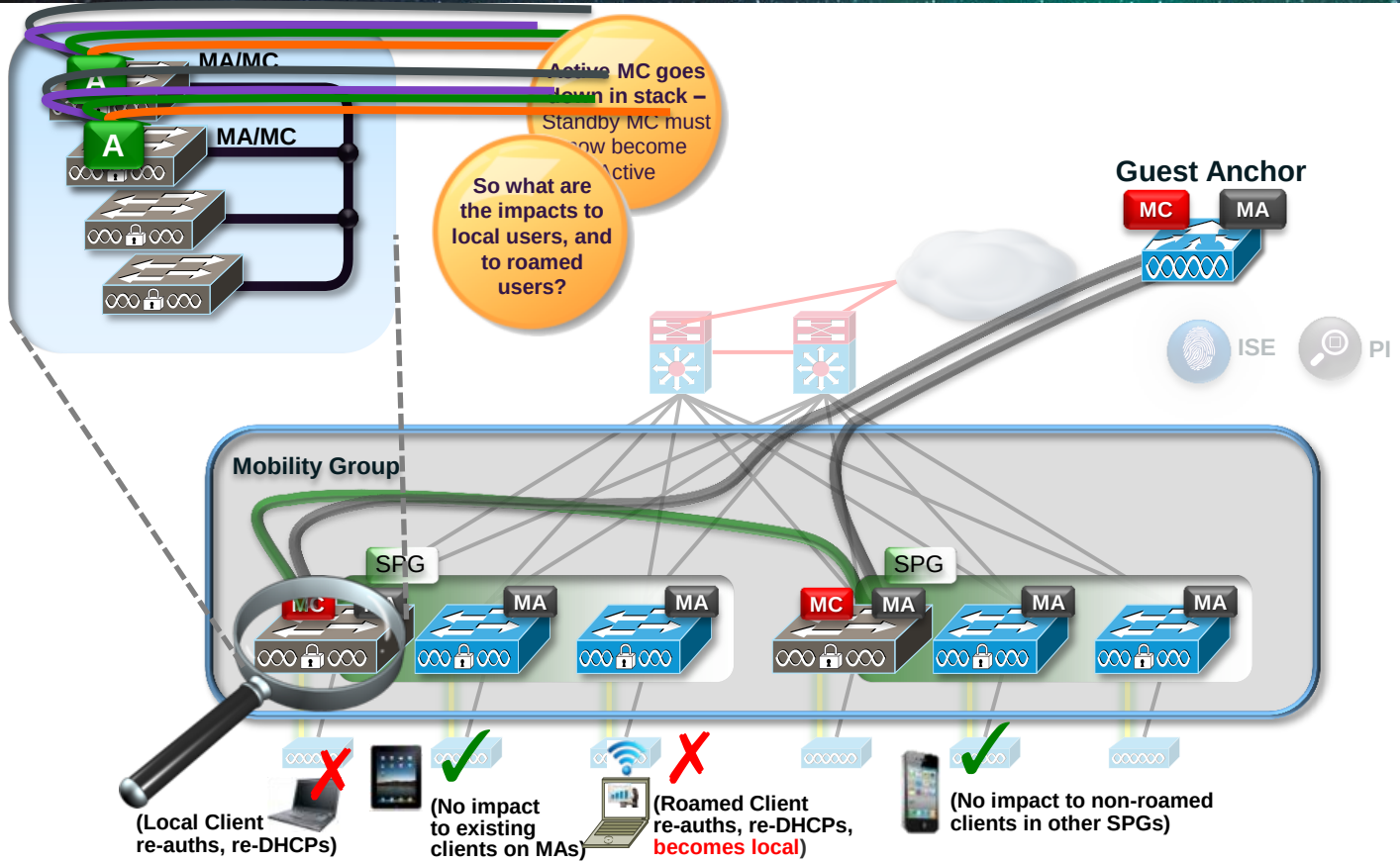
Catalyst 3650/3850 – Tunnel SSO



Catalyst 3650/3850 – Tunnel SSO



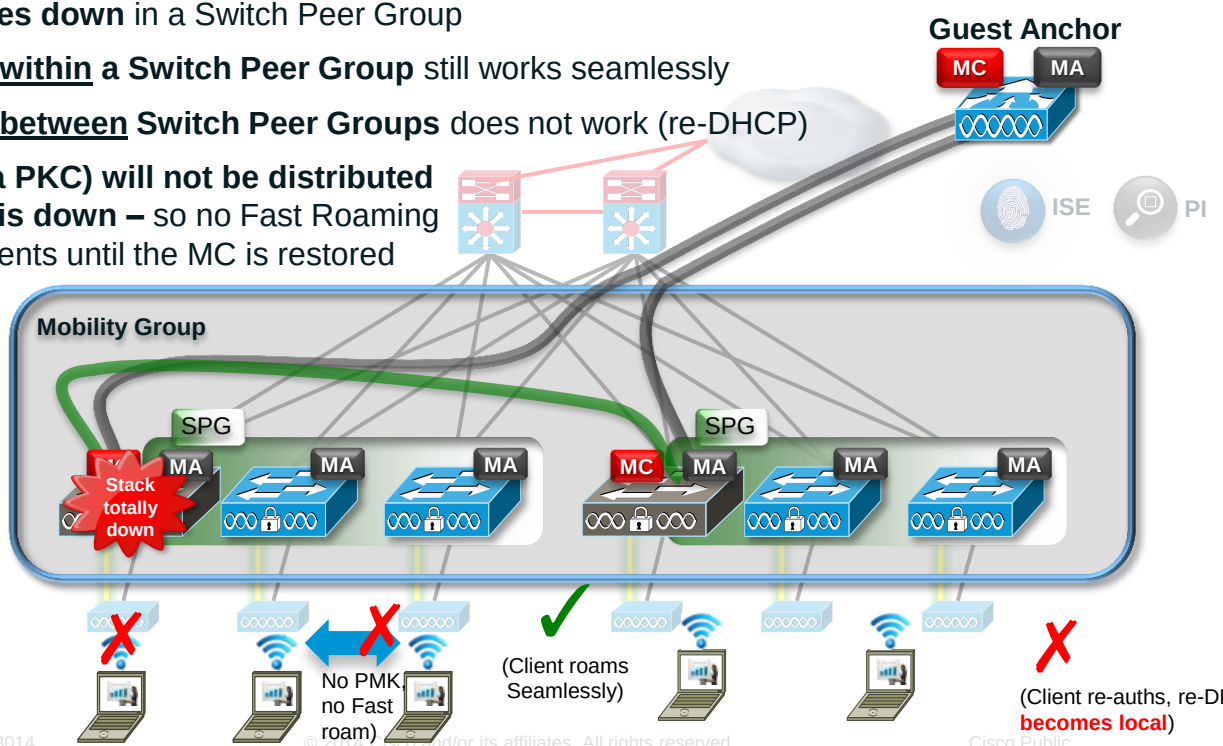
Catalyst 3x50-based MCs – Fault Tolerance in Stack



Catalyst 3x50-based MCs – Fault Tolerance across Stacks

Switch Peer Group Fault Tolerance with Catalyst 3x50

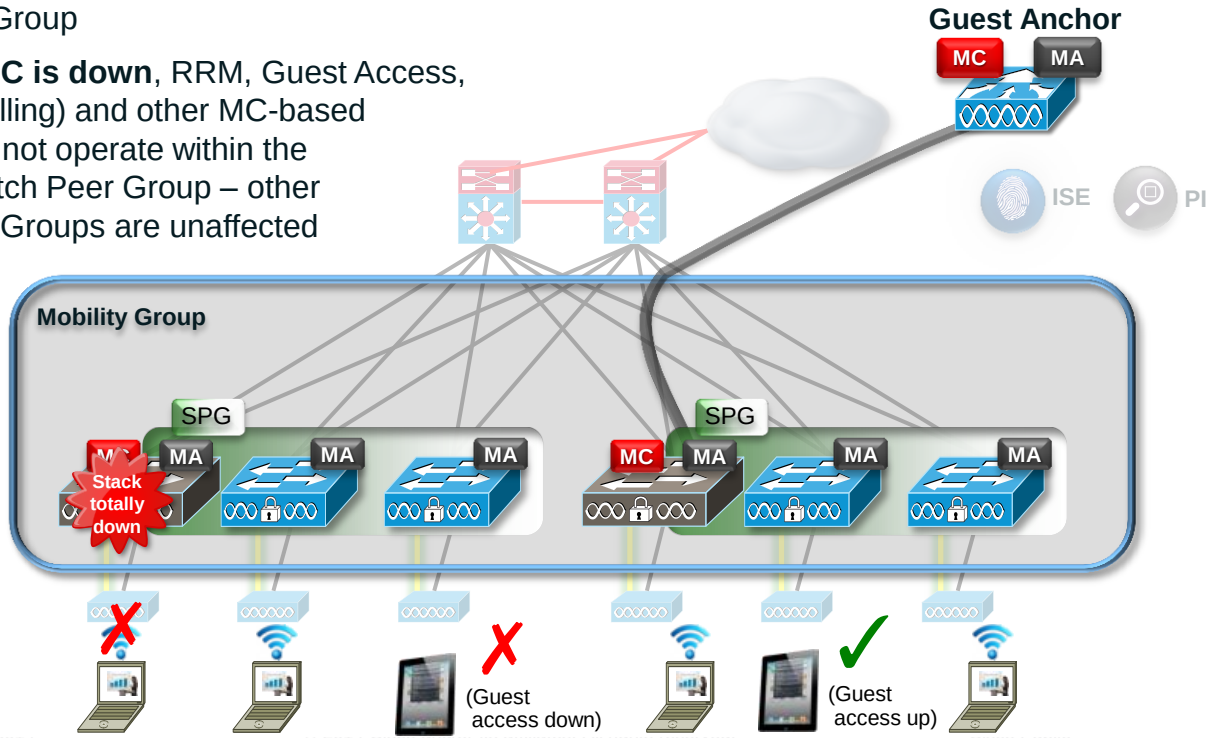
- **If a Catalyst 3x50-based stack, operating as MC, completely goes down** in a Switch Peer Group
  - **Roaming within a Switch Peer Group** still works seamlessly
  - **Roaming between Switch Peer Groups** does not work (re-DHCP)
  - **PMKs (via PKC) will not be distributed if the MC is down –** so no Fast Roaming for new clients until the MC is restored



Catalyst 3x50-based MCs – Fault Tolerance across Stacks

Switch Peer Group Fault Tolerance with Catalyst 3x50

- **If a Catalyst 3x50-based MC is completely down** in a Switch Peer Group
  - **When the MC is down**, RRM, Guest Access, (guest tunnelling) and other MC-based functions do not operate within the affected Switch Peer Group – other Switch Peer Groups are unaffected

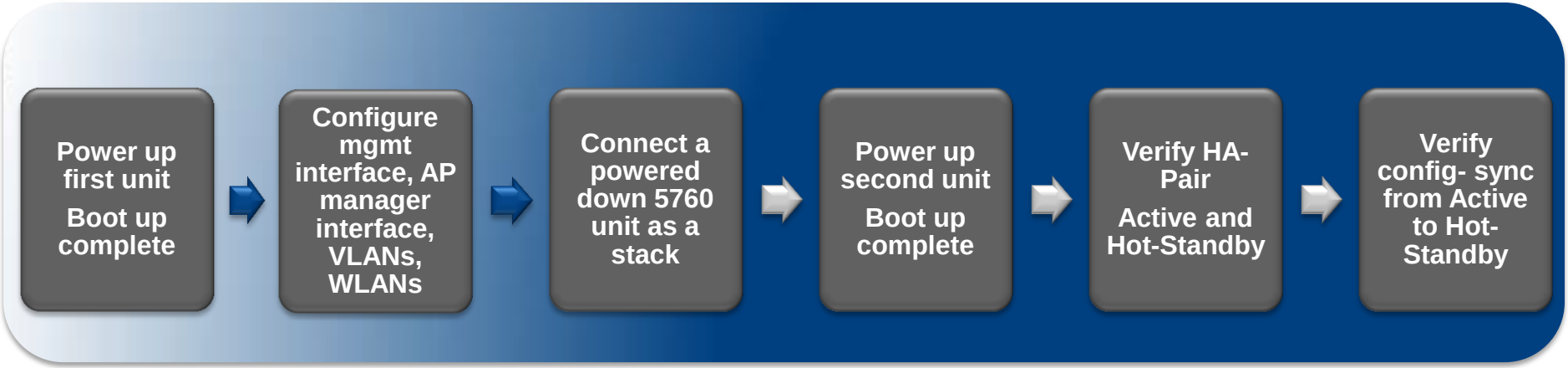


5760 High Availability

- Two 5760 units can be stacked for 1:1 redundancy, using stack cables
- One 5760 elected as Active and the other becomes Hot-Standby
- Bulk and Incremental Configuration sync
- Redundancy supported both at Port level and System level
- AP CAPWAP information sync. APs will not disconnect and continue to be associated to the controller
- Significantly reduces network downtime

5760 High Availability: How to Pair the Boxes

- Recommended: power up the second unit with existing an existing deployed 5760



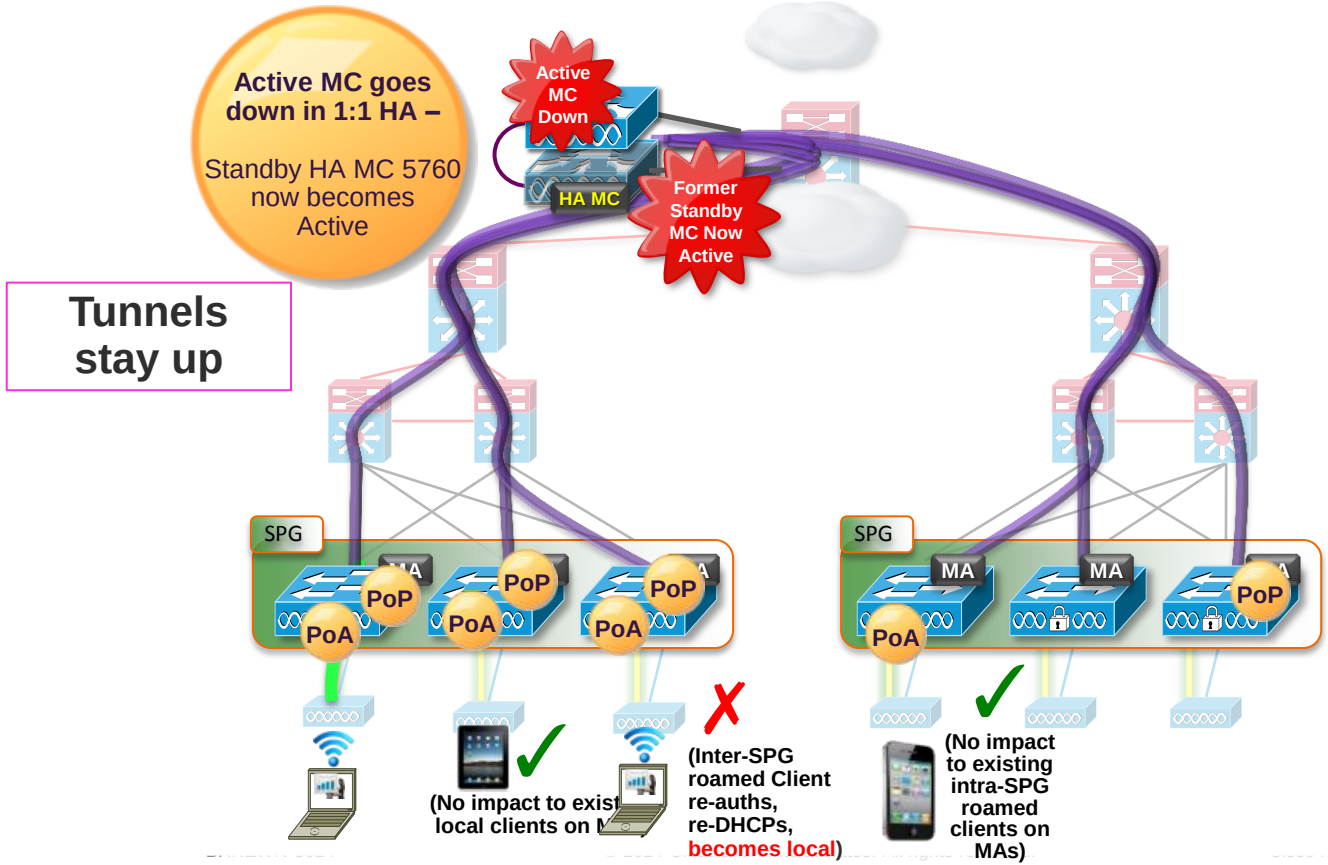
- Adding powered-on 5760 Unit (merging) causes stack to reload and elect a new Active from among themselves. Config on first 5760 may get wiped out
- Use `Controller# switch 1 priority 15` on the first unit to prevent having the second unit become active and wipe out your config …

5760 High Availability: What Happens to Features?

For Your Reference

- **AP Pre-Image Download**: No AP SSO while AP pre-Image download in progress
- **Rogue APs and clients:** NOT synchronised to Standby. Re-learnt upon switchover
- **Security**: Management Frame Protection (MFP) key is NOT synchronised to Standby. Re-learnt upon switchover
- **WiPS:** NOT synchronised to Standby. Re-learnt upon switchover
- **CleanAir:** Interferer devices are re-learnt after switchover
- **NetFlow:** NetFlow records are cleared and collection starts fresh upon switchover
- **RRM:** RRM related configurations and the AP neighbour list in the Leader HA pair is synced to the Standby

WLC 5760-Based MCs – Impact on Clients



Roamed and Local users, High Availability Considerations

- **Local users on their MAs** have no impact following a HA MC failover event
- **Intra-SPG roamed users** also have no impact following the MC HA failover
- **All previously-roamed clients (inter-SPG) will result in a "hard roam" after MC failover** (re-auth, re-DHCP, change of client IP address, known as "becoming local")
- **Any new intra-SPG or inter-SPG roaming happening after MC HA failover** from local MA clients will be handled normally

Cisco live!

Prime and MSE HA

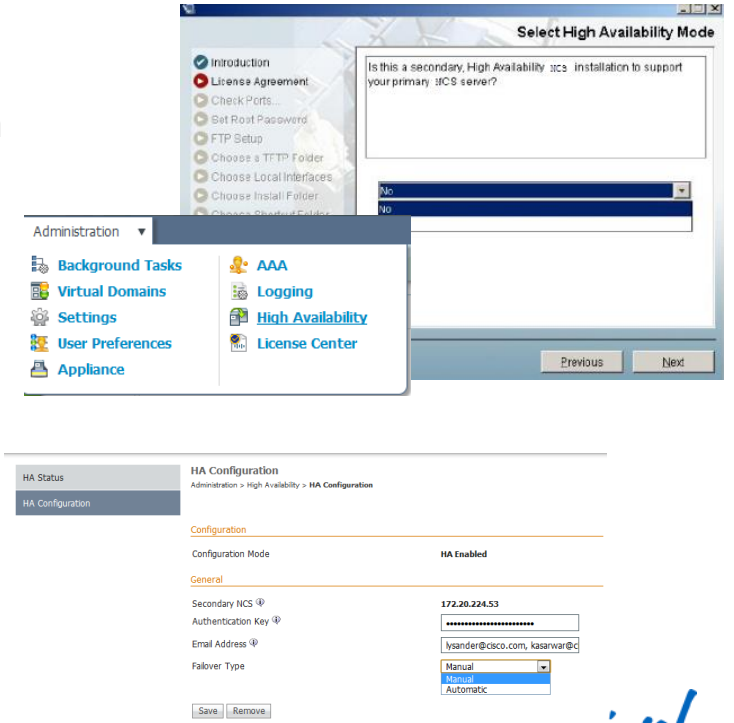
Prime and MSE HA

	Requirements	Benefits
Prime HA	An active / standby (1:1) mode Same software / hardware 3 heartbeats (timeout 2 seconds) missing to failover to standby PI RTU Standby SKU (2.0 and later)	No database loss upon failover Failover Automatic or Manual Failback is always manual No AP licenses needed on Standby Unit Support across L3 link
MSE HA	1:1 & 2:1 configuration (2:1 only with same type of appliance) Direct or L2 Network connection Same software version	HA for all services supported Failover times < 1 min No HA licenses needed Failover Automatic or Manual

Prime Infrastructure HA

Configuration

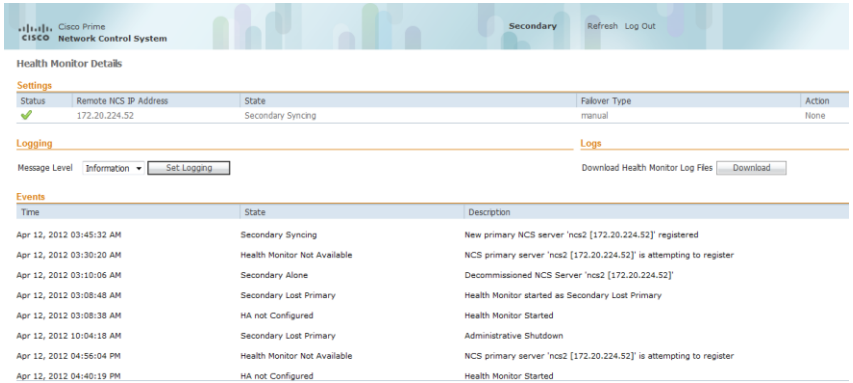
- The first step is to install and configure the Secondary PI. When configuring the Primary PI for HA, the Secondary PI needs to be installed and reachable by the Primary PI
- The following parameters must be configured on the primary PI:
  - name/IP address of secondary PI
  - email address of network administrator for system notification
  - manual or automatic failover option
  - Secondary PI must always be a new installation and this option must be selected during PI install process, i.e. standalone or primary PI cannot be converted to secondary PI. Standalone PI can be converted to HA Primary.



Prime Infrastructure HA

Health Monitor

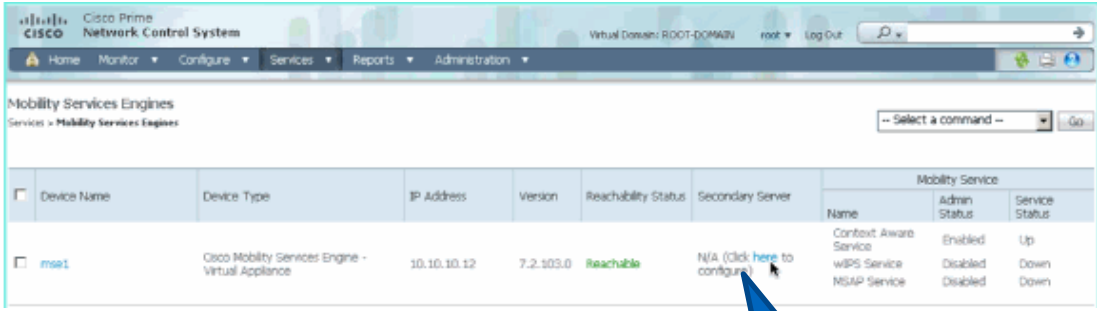
- The Health Monitor (HM) is a process implemented in PI and is the primary component that manages the high availability operation of the system.
- It displays valuable logging and troubleshooting information
- To get to the Health Monitor direct the secondary PI to the 8082 port
  - https://< secondary PI ip address>:8082
  - Note – if you navigate to the primary's port 8082 you will not be able to login as it is only available on the secondary PI

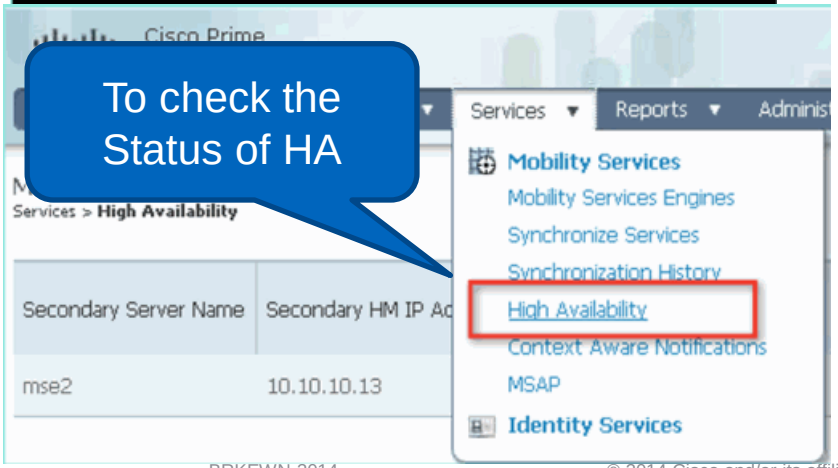


MSE HA

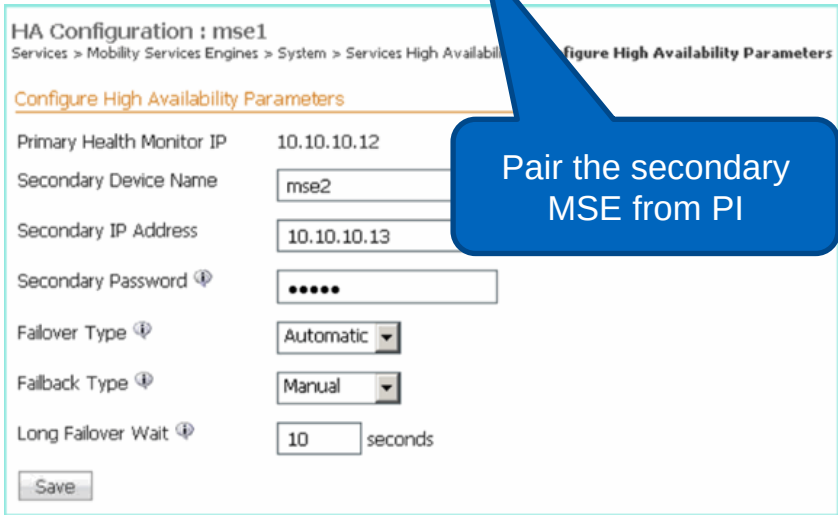
Configuration

1) Set HA mode in startup script





To check the Status of HA



Pair the secondary MSE from PI

Related Sessions and Links

- BRKEWN-2017 - Understanding RF Fundamentals and the Radio Design of Wireless Networks
- BRKCRS-2889 - Converged Access System Architecture – Diving into the “One Network”
- BRKEWN-2022 - Converged Access Mobility Design & Architecture
- BRKEWN-2010 - Design and Deployment of Enterprise WLANs
- WOS HA Demo
- Useful docs:
  - FAQ: http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps10315/qa_c67-714540.html
  - AireOS WLC HA Deployment Guide: http://www.cisco.com/en/US/docs/wireless/controller/technotes/7.5/High_Availability_DG.pdf
  - IOS WLC HA Deployment Guide http://www.cisco.com/en/US/docs/wireless/controller/technotes/5700/software/release/ios_xe_33/5760_HA_DG_iosXE33.html#wp43179




Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

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

Learn online with Cisco Live!

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


CISCO
TM