H3C Wireless
A Technical Overview

Rob Haviland – Technical Marketing Engineer
rob_haviland@3com.com
508.323.1458

GPLM:

- **Jeff Schwartz (jeff_schwartz@3com.com)**
- **Scott Lindsay (scott_lindsay@3com.com)**
- **Tony Bi (tony_bi@3com.com)**

H3C 3COM TippingPoint

H3C Mobility Portfolio

IMC / Comware

Basic Management | Resource Management | User Management | Service Management | Security Management

Wireless Application

IMC WSM Mobility Module

Wireless controller

Unified Switches

WX3010

WX3024

WLAN Controllers

WX5002

WX5004

WLAN Controller Modules

S7500E Module

S9500E Module
*H209

S5800 Module
*H209

Access Points

Indoor APs

WA2110-AG
Single Radio

WA 2612-AGN
Single Radio
*Sept 09

WA2220-AG
Dual Radio

WA 2620-AGN
Dual Radio
*Sept 09

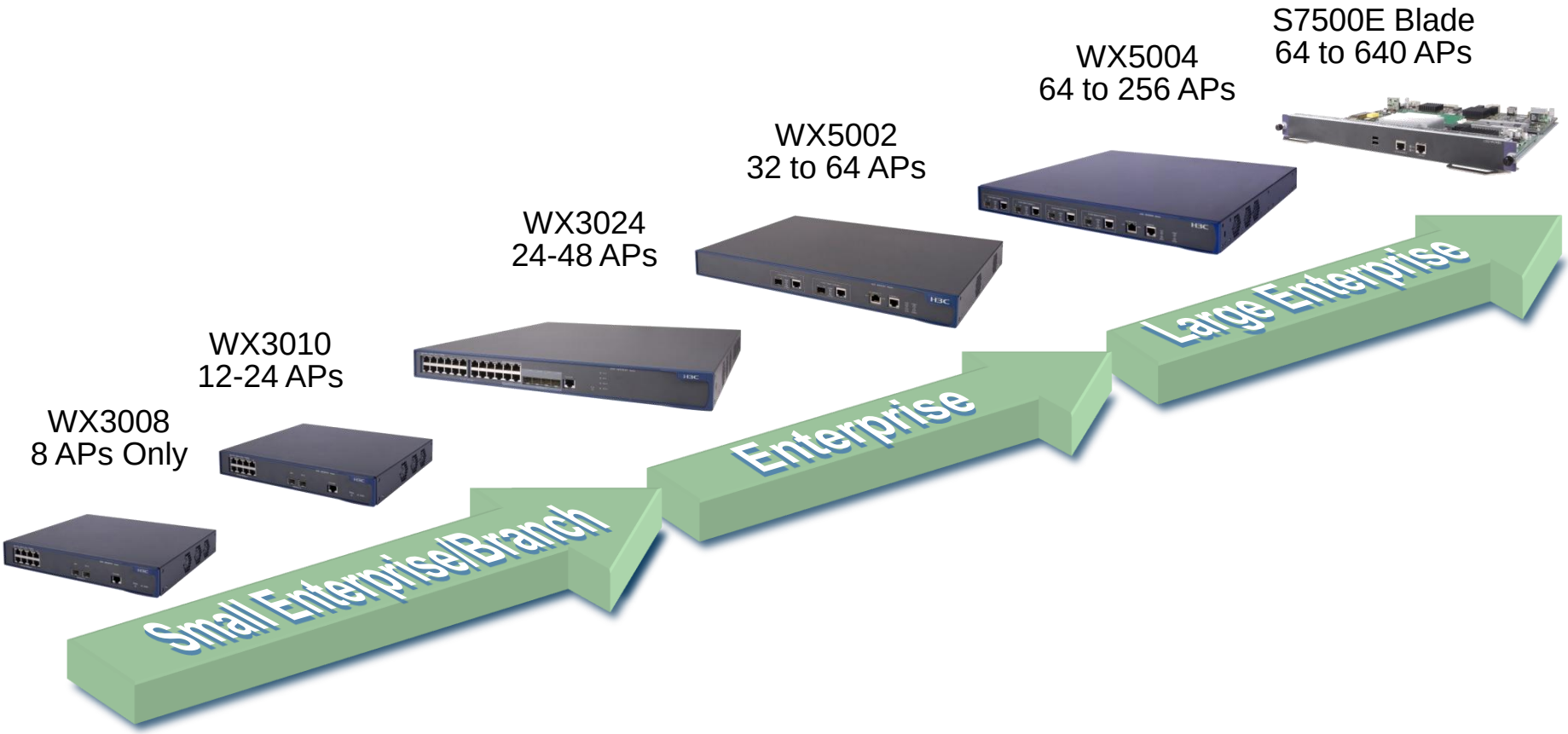
Ruggedized APs

WA 2610E-AGN
Single Radio

WA 2620X-AGN
Outdoor AP
*H110

WA 2620E-AGN
Dual Radio

H3C AP Capacity



Coming soon:
Q4CY09 S5800 (32/64 & 64/256 APs)
Q4CY09 S9500E (128/640 APs)

H3C Access Controller Physical Interfaces

WX3008:
8 * 10/100/1000
PoE and PoE+ Support (Ports 1-4 Only)
125W Total Power Budget
1Gbps Wireless Throughput

WX3010:
8 * 10/100/1000 + 2 * SFP
PoE (All Ports) and PoE+ (Any 5 Ports) Support
125W Total Power Budget
1 Gbps Wireless Throughput

WX3024:
24 * 10/100/1000 + 4 * SFP (dual personality)
2 * 10 Gigabit Slots (back)
PoE (All Ports) and PoE+ (Any 14 Ports) Support
370W Total Power Budget
1 Gbps Wireless Throughput

WX5002:
2 * SFP or 10/100/1000 (dual personality)
1.8 Gbps Wireless Throughput

WX5004:
4 * SFP or 10/100/1000 (dual personality)
4 Gbps Wireless Throughput

S7900E Wireless Access Controller Module:
1 * Higig+ Channel (10 Gig)
10 Gbps Wireless Throughput

Summary: H3C AC Products and Positioning

Product Model	Number of Managed APs	Positioning
H3C WX3008(Future)	**4**	Unified Switch, For SMB and remote office networks. 8*GE-port (PoE+) Unified Wireless Switch
H3C WX3010	**24**	Unified Switch, For small-sized enterprise and remote office networks. 10*GE-port (PoE+) Unified Wireless Switch
H3C WX3024	**48**	Unified Switch, For small-sized enterprise and remote office networks. 24*GE-port (PoE+) Unified Wireless Switch
H3C WX5002	**64**	For medium and small-sized enterprise networks and branch offices. 2*GE-port Wireless Access Controller
H3C WX5004	**256**	For large and medium-sized enterprise networks. 4*GE-port Wireless Access Controller
H3C LSQM1WCMB0	**640**	For large enterprise networks. 10G Blade for the H3C S7510E, H3C S7506V, H3C S7506E, H3C S7503E, and H3C S7502E Chassis

Summary: H3C AP Products and Positioning

Product Model	AP Type	Positioning
H3C WA2110-AG	**FIT AP**	Indoor model 802.11a/b/g (single frequency) For small radius indoor areas and low environment requirements.
H3C WA2220-AG	**FIT AP or FAT AP**	Indoor model 802.11a/b/g (dual frequencies) For small radius indoor areas and low environment requirements.
H3C WA2612-AGN (Future)	**FIT AP or FAT AP**	Cost effective Indoor model 802.11a/b/g/n (single frequency) For medium to larger radius indoor areas and high throughput demands. 2 x 3 MIMO. 802.3af PoE. 3 Imbedded antennas only.
H3C WA2620-AGN (Future)	**FIT AP or FAT AP**	Cost effective Indoor model 802.11a/b/g/n (dual frequencies) For medium to larger radius indoor areas and highest throughput demands. 2 X 3 MIMO. 802.3af PoE. 6 internal antennas and 3 external antennas for a single band.
H3C WA2610E-AGN	**FIT AP or FAT AP**	Indoor model 802.11a/b/g/n (single frequency) For larger radius indoor areas and high throughput demands. 3 X 3 MIMO. 802.3af PoE. 3 external antennas.
H3C WA2620E-AGN	**FIT AP or FAT AP**	Indoor model 802.11a/b/g/n (dual frequencies) For larger radius indoor areas and highest throughput demands. 3 X 3 MIMO. 802.at PoE+. 6 external antennas.

Note:
H3C AP ship as FIT and a simple CLI command changes to FAT.

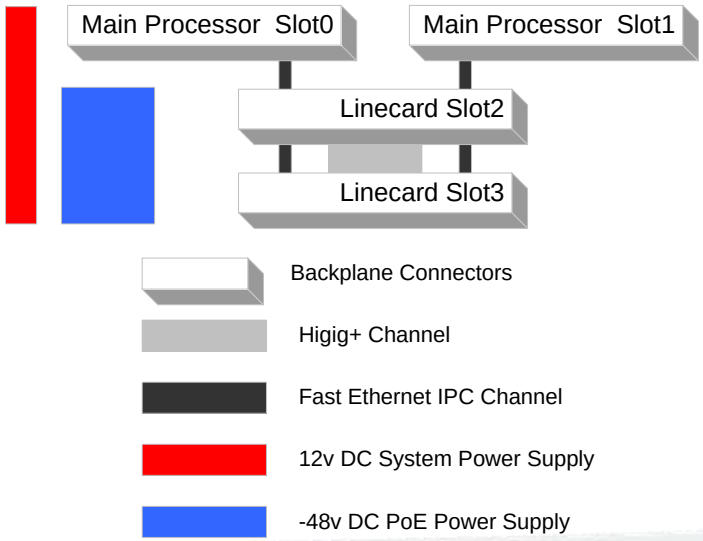
S7500E Wireless AC Module – Hardware Configuration Example

-S7502E

-S7503E

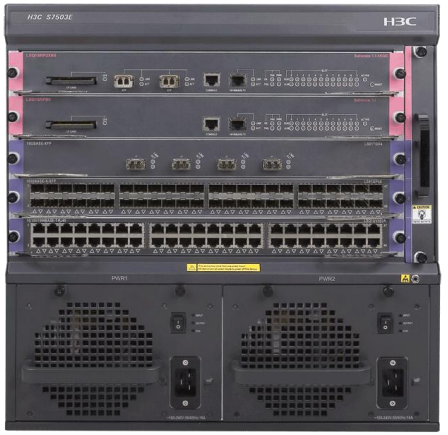
S7502E – Wireless Access Controller Configuration Example (Non-Redundant Solution)

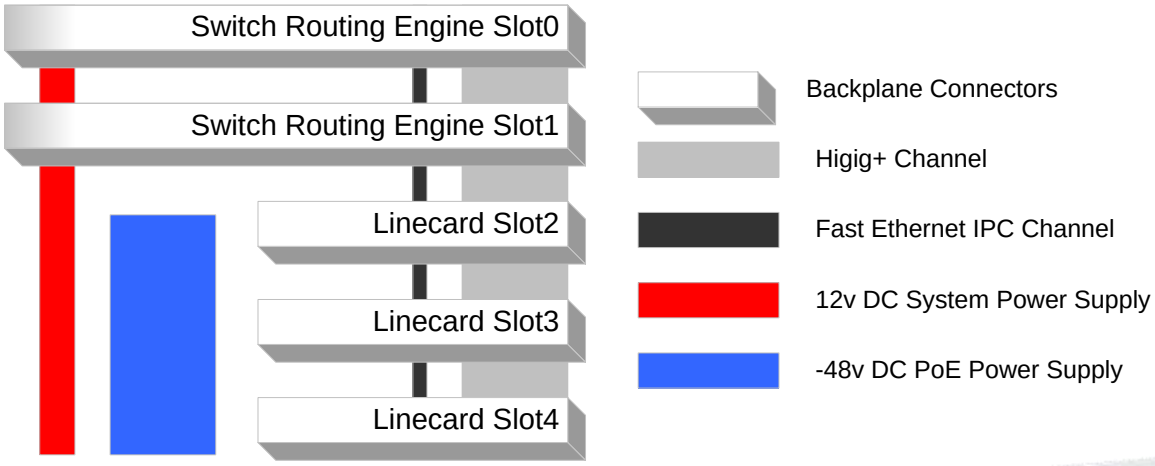
- Typical S7502E Configuration
  - **S7502E Chassis /w Fan (1)**
  - **S7502E 650W AC Power Supply (1 or 2)**
  - **S7502E Management Module (1 or 2)**
  - **S7500E 24 Port 10/100/1000 Base-T Module (1)**
  - **S7500E Wireless Access Controller Module (1)**



S7503E– Wireless Access Controller Configuration Example (Fully Redundant Solution)

- Typical S7503E Configuration
  - **S7503E Chassis /w Fan (1)**
  - **S7500E 1400W AC Power Supply (2)**
  - **S7500E LSQM1SRPB0-Salience VI FRU Pre Rel (2)**
  - **S7500E 24 Port 10/100/1000 Base-T Module (1)**
  - **S7500E Wireless Access Controller Module (2)**

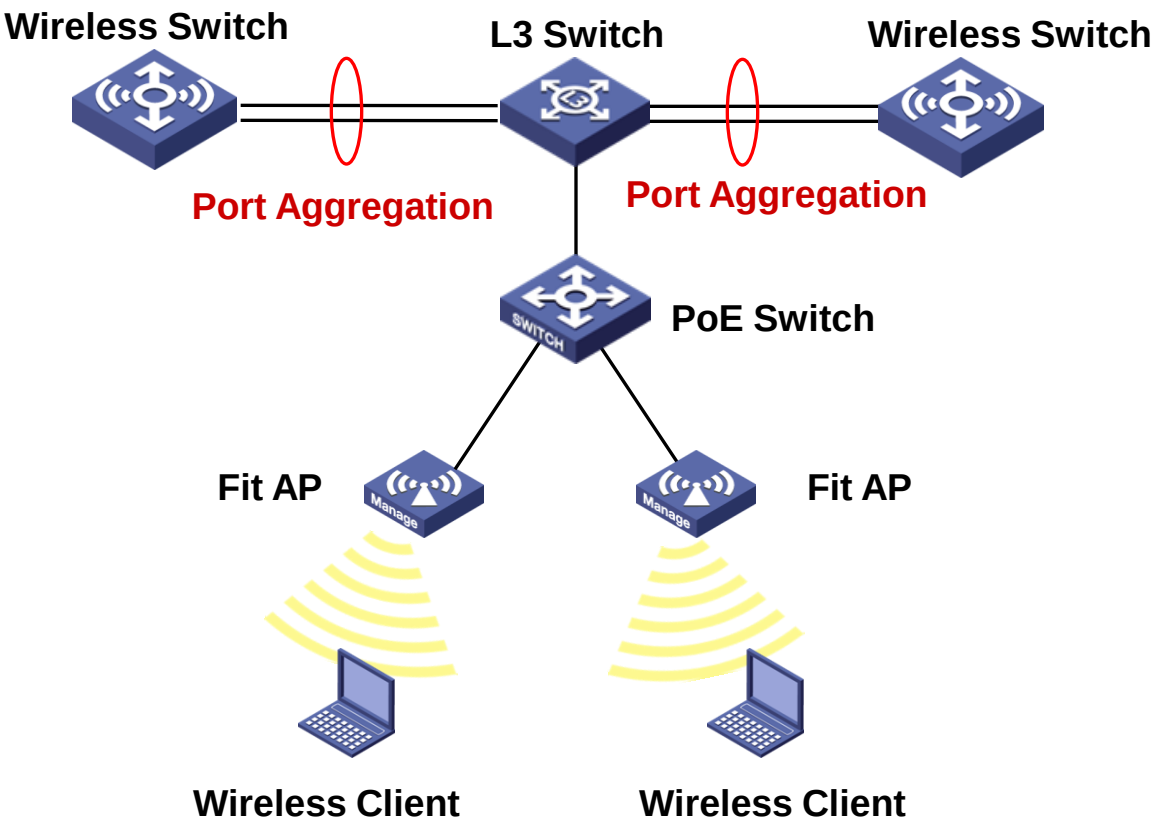




AP Boot Options

- AC to AC / AC to AP Communications
- L2 Option
- L3 Option /w DHCP option 43
- L3 Option /w DNS

AC to AC / AC to AP Communications

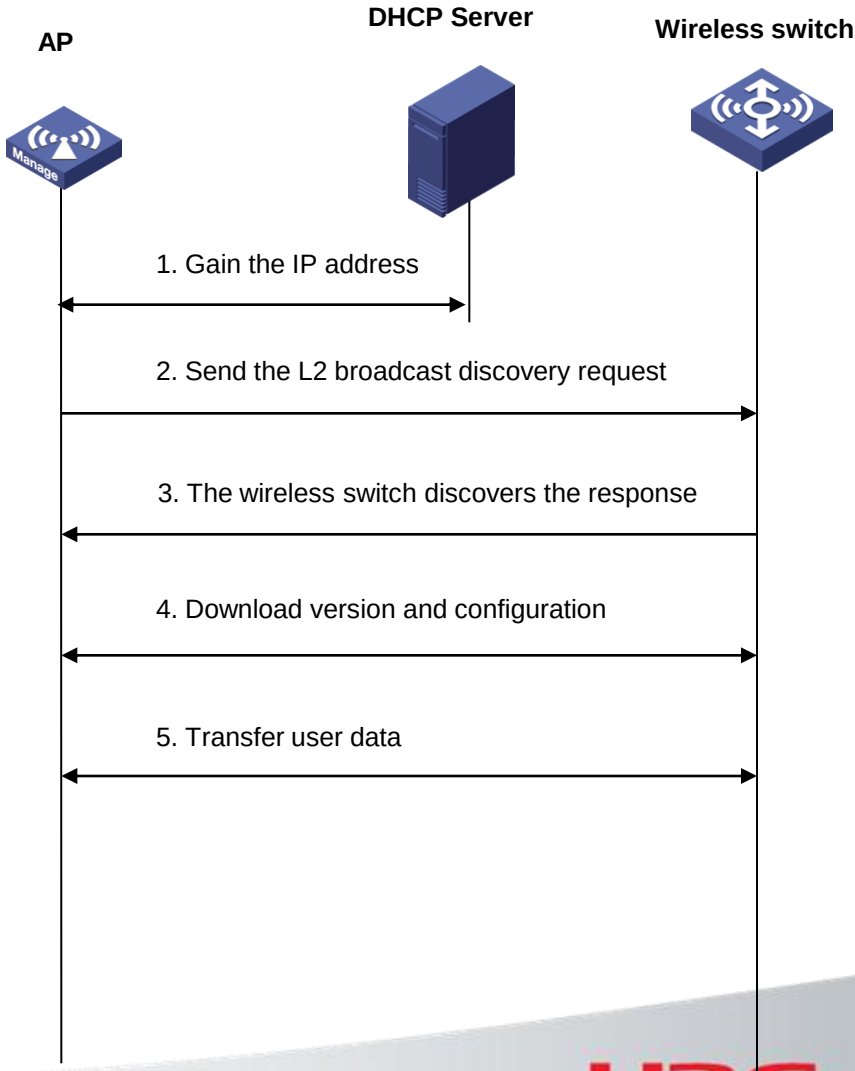


- AC to AC - Proprietary IACTP (Inter Access Controller Tunneling Protocol)
- AC to AP – Really LWAPP - The Draft Standard of CAPWAP. (AC to AP will be CAPWAP in the Q32010)
- H3C Engineer (Yang Shi – Richard Young) is the Author of the CAPWAP Standard

Registration Procedure of AP - Direct Connection or Connection Through L2 Network

AP connects to the wireless switch directly or through the L2 network:

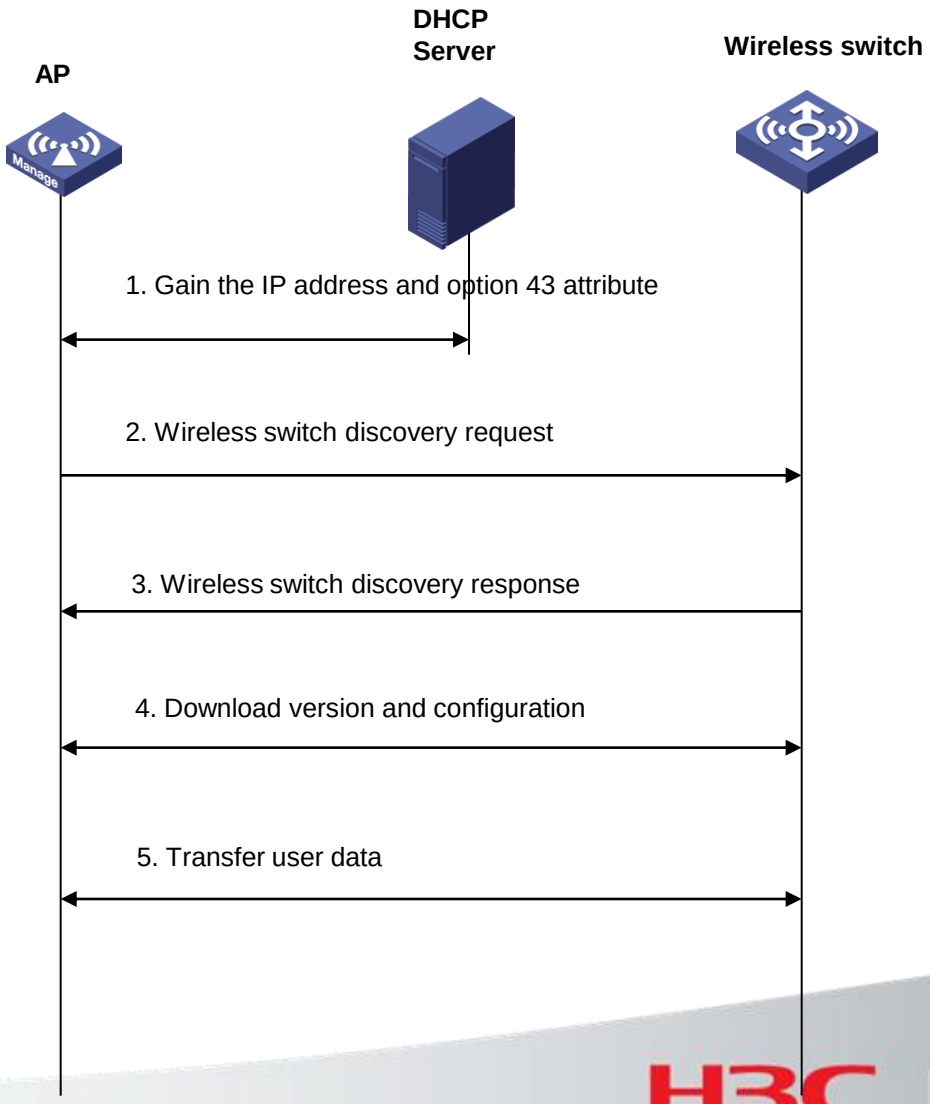
1. AP gains the IP address through the DHCP server.
2. AP sends a L2 broadcast discovery request packet, trying to contact a wireless switch.
3. Upon reception of the request packet, the wireless switch will check whether the AP has the right to connect to the switch. if yes, the switch returns a discovery response.
4. AP downloads the latest software version and configuration from the wireless switch.
5. AP starts to work normally, and exchange user data packets with the wireless switch.



Registration Procedure of AP - L3 Network DHCP Option 43 Mode

AP connects with the wireless switch through L3 network connection:

1. AP gains the IP address and option 43 attribute (with the IP address information of the wireless switch) through the DHCP server.
2. AP gains the IP address of the wireless switch from the option 43 attribute, and then sends a unicast discovery request to the wireless controller.
3. Upon reception of the discovery request packet, the wireless switch will check whether the AP has the right to access the switch. If yes, it returns a discovery response.
4. AP downloads the latest software version and configuration from the wireless switch.
5. AP starts to work normally, and exchange user data packets with the wireless switch.



Example of Option 43 Attribute Configuration

- **H3C equipment has built-in DHCP Server.**

```
[S3600-dhcp-pool-0]dis th
#
dhcp server ip-pool 0
 network 18.0.0.0 mask 255.0.0.0
 option 43 hex  80 0B 00 00 02 12 01 07 01 12 01 07 02
#
```

- Description of Option 43

→ **80: Option type. It is a fixed value, 80, 1 byte.**

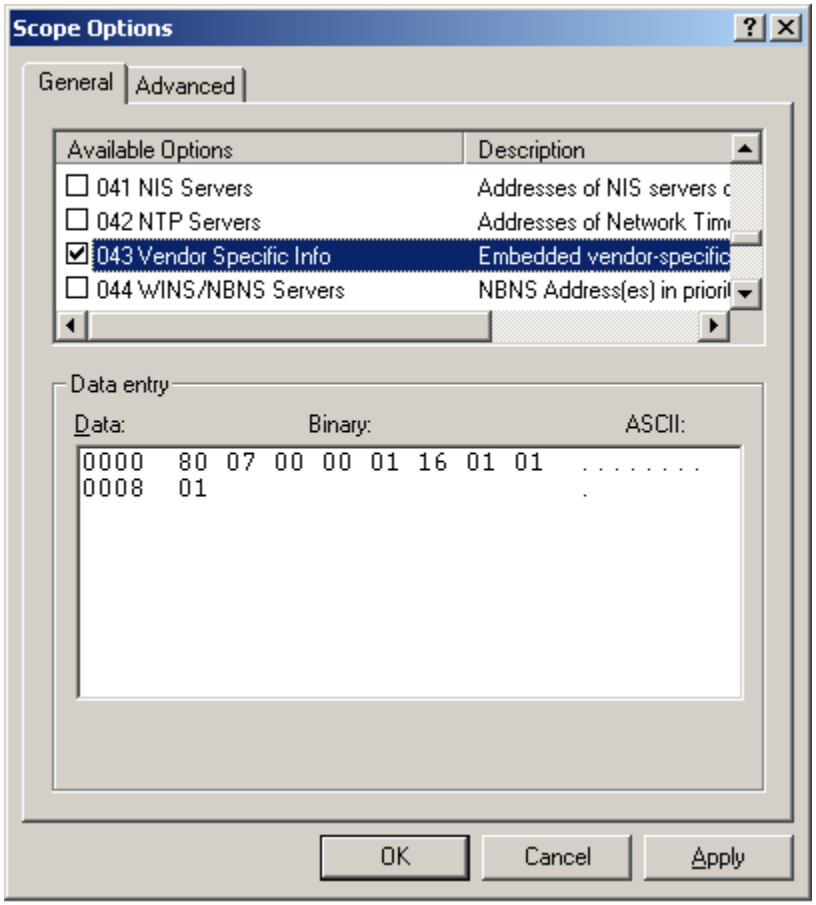
→ **0B: Option length, indicating the length of the following content (number of hex numbers; here it indicates that the following part has 11 hex numbers), 1 byte.**

→ **0000: Server type. It is a fixed value, 0000, two bytes.**

→ **02: The number of the following IP addresses, 1 byte.**

→ **12010701,12010702: Hex expressions of the IP addresses of the two ACs, 18.1.7.1 and 18.1.7.2. Of them, 18.1.7.1 is the address of the main AC.**

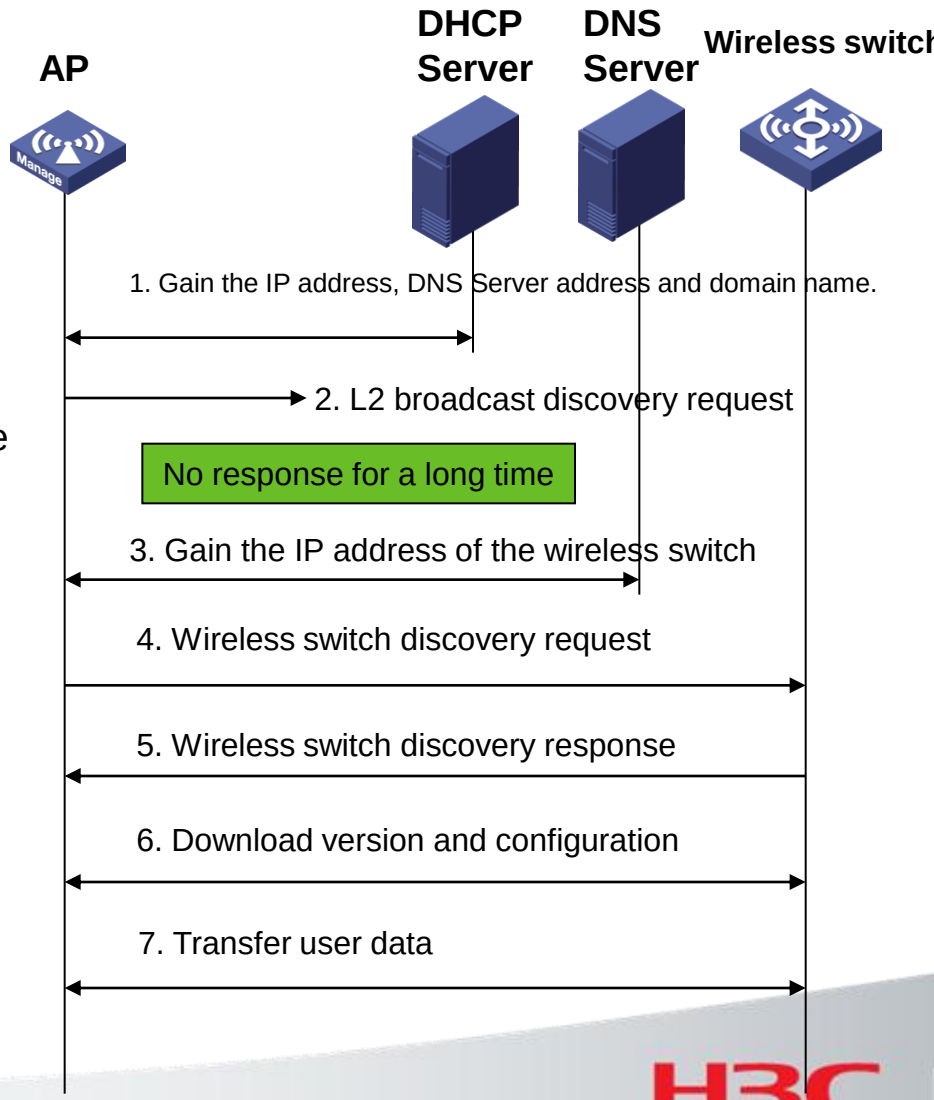
- **Microsoft DHCP Server**



Registration Procedure of AP - L3 Network DNS Mode

AP connects with the wireless switch through L3 network:

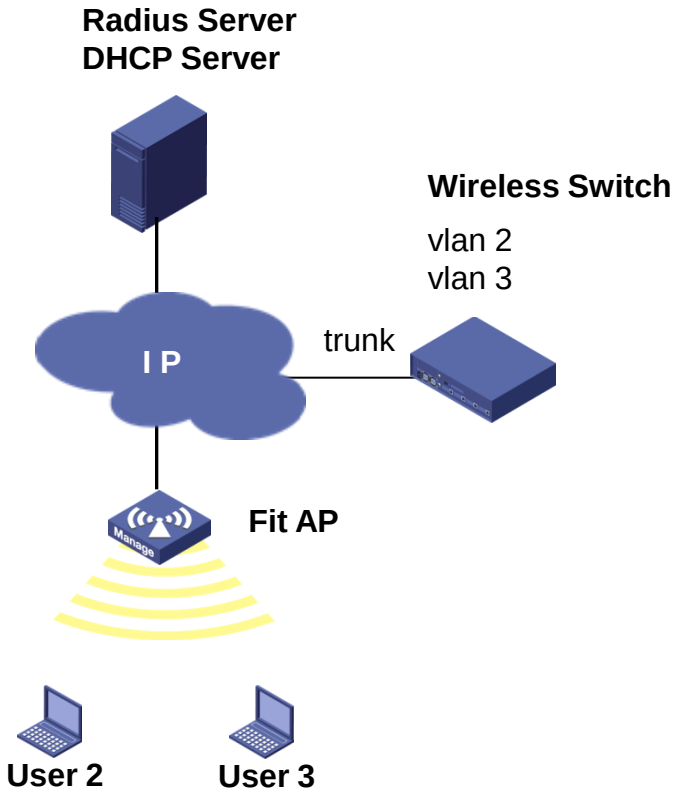
1. AP gains the IP address, DNS server address and domain name through the DHCP server.
2. AP sends the L2 broadcast discovery request packet, trying to contact a wireless switch.
3. AP has no response after repeated discovery requests.
   - AP will gain the IP address of H3C.xxxx.xxx from the DNS server. The IP address is the IP address of the wireless switch. In particular, xxxx.xxx is the domain name learned from the DHCP server.
4. AP sends a unicast discovery request to the wireless switch.
5. Upon reception of the discovery request packet, the wireless switch will check whether the AP has the right to connect to the switch. If yes, it returns a discovery response.
6. AP downloads the latest software version and configuration from the wireless switch.
7. AP starts to work normally, and exchange user data packets with the wireless switch.



Main Features

- User Based Authorization
- Roaming
- Port Aggregation
- Load Balancing
- Encryption
- Local Switching
- Web Portal
- Rogue Detection

Wireless Switch System – User-based Authorization



User 2 MAC: 0000-0000-0002
User 3 MAC: 0000-0000-0003

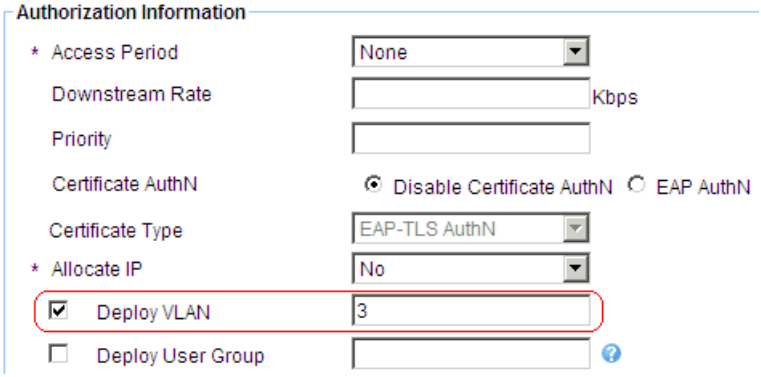
Enable mac-vlan on the WLAN-ESS interface

port link-type hybrid
port hybrid vlan 1 to 3 untagged
mac-vlan enable

Method 1: Set on the wireless switch itself

mac-vlan mac-address 0000-0000-0002 vlan 2
mac-vlan mac-address 0000-0000-0003 vlan 3

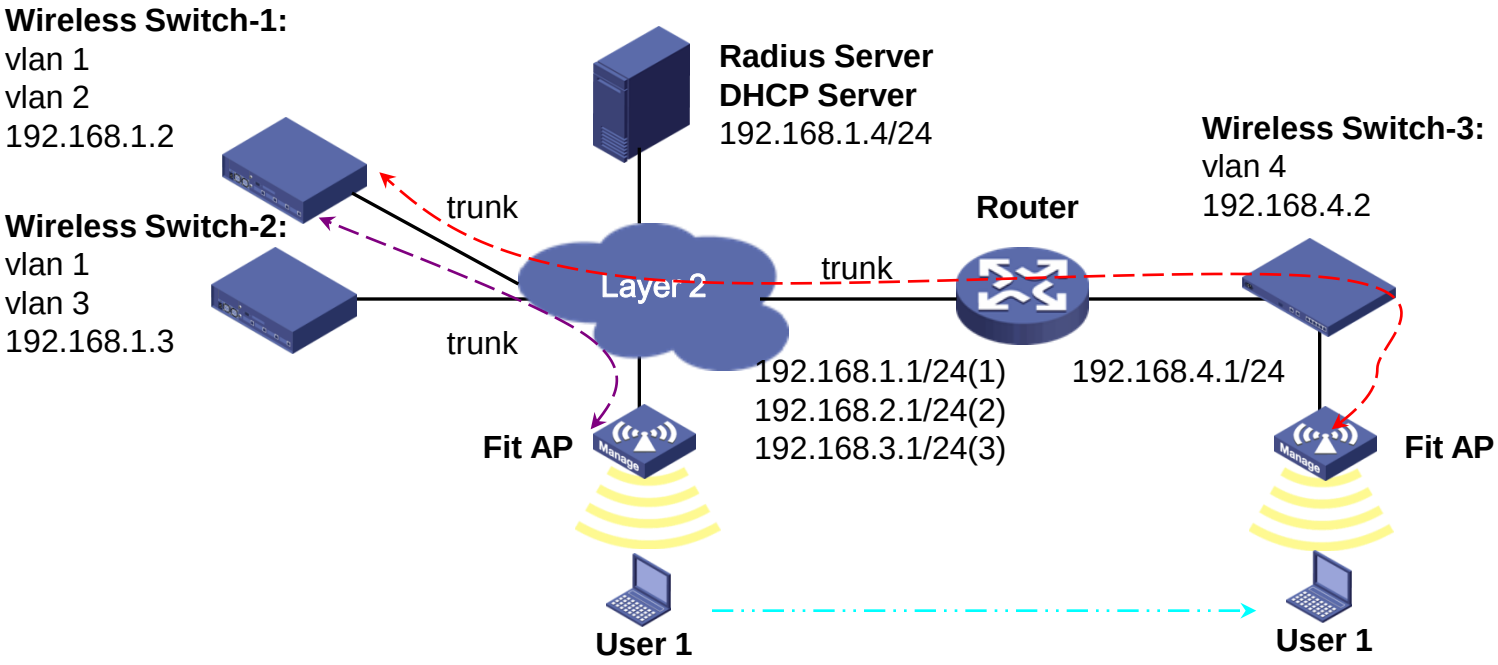
Method 2: Authorize through the Radius Server




```
AVP: l=6  t=Tunnel-Private-Group-Id(81) Tag=0x00: \000\000\003
    [Length: 4]
    Tag: 0x00
    Tunnel-Private-Group-Id:
```

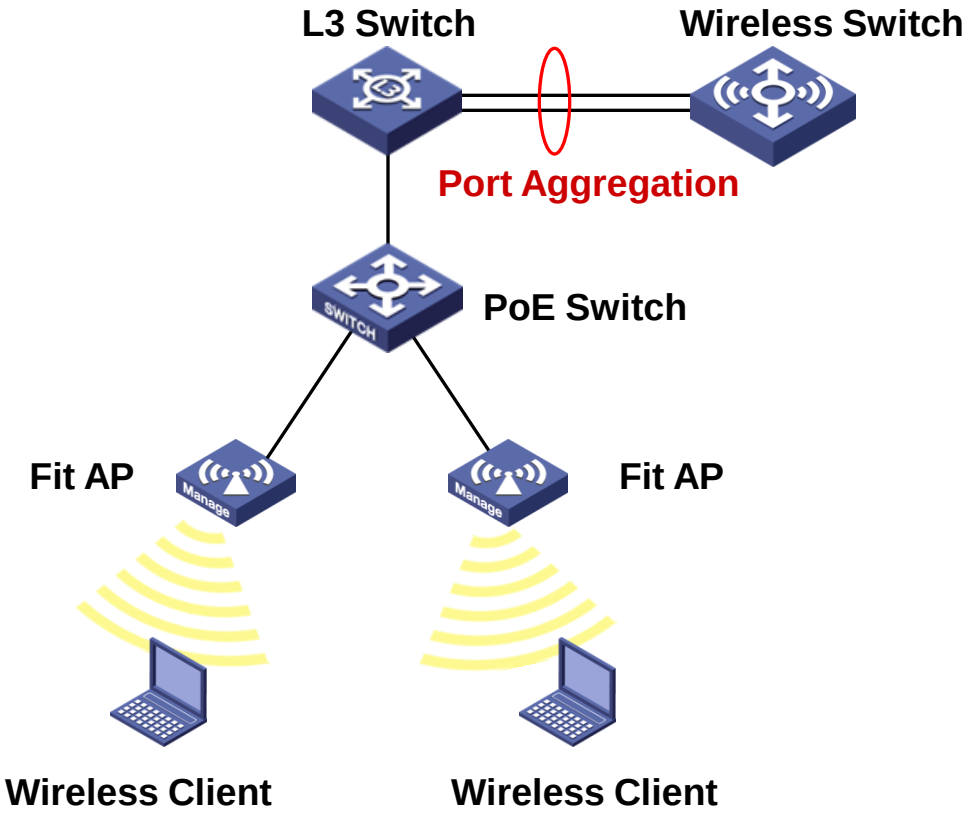
- **The wireless switch can authorize wireless access users (for example, distributing VLAN attributes to users) by setting locally or through the Radius Server, to implement user-based authorization.**

Wireless Switch System – Wireless User Roaming



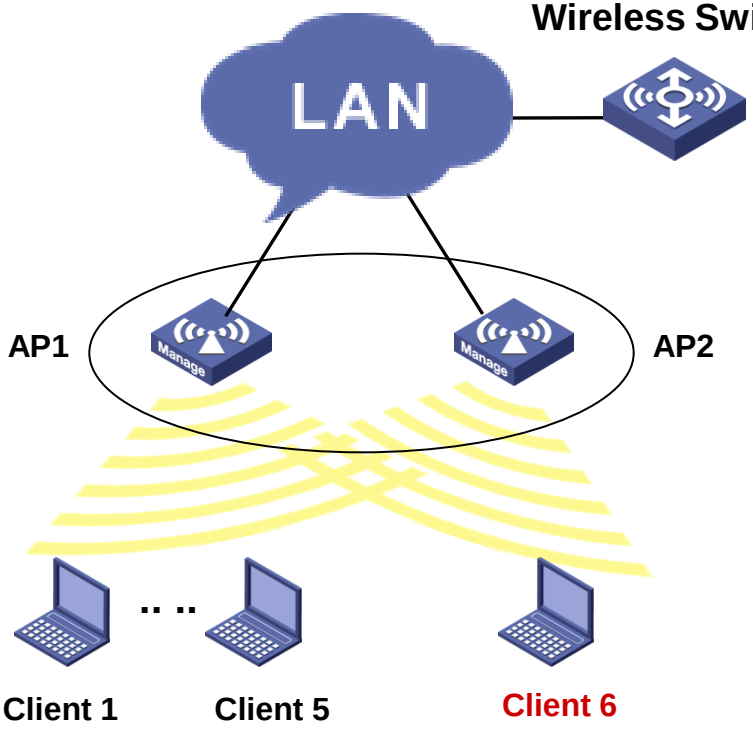
- **Roaming: Users cannot feel the change of networks when they are moving, because their session connections (including IP address, VLAN, and connected services) remain unchanged.**
- **Mobility Domain: Is a wireless network system consisting of multiple wireless switches and APs and supporting wireless client roaming.**
- **8 AC maximum supporting 50 ms roaming times**

Port Aggregation



- **The wireless switch supports port aggregation for load sharing between ports and dynamic port backup.**

Load Balancing Between Fit APs



User access status of two APs before Client 6 accesses the wireless network:

AP1 Session:	AP2 Session:
* client 1 * client 2 * client 3 * client 4 * client 5	Total: 0
Total: 5	

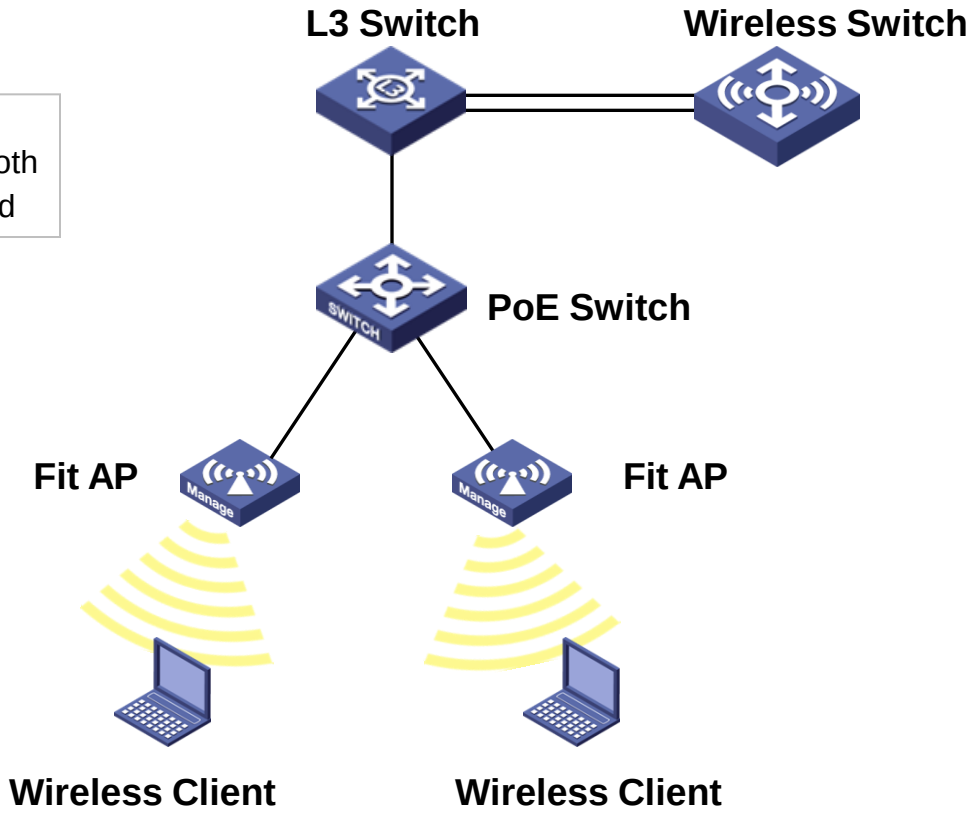
User access status of two APs after Client 6 accesses the wireless network:

AP1 Session:	AP2 Session:
* client 1 * client 2 * client 3 * client 4 * client 5	* client 6 Total: 1
Total: 5	

- **When multiple APs cover the same area, load balancing can be used to control the access session of each AP, so as to guarantee the user bandwidth performance in the areas with high user density.**
- **H3C FIT AP can implement load balancing in two modes: session and traffic. For the session load balancing, the threshold is in the range of 5 to 40, 20 by default. For the traffic load balancing, the threshold is in the range of 10% to 80%, 30% by default.**

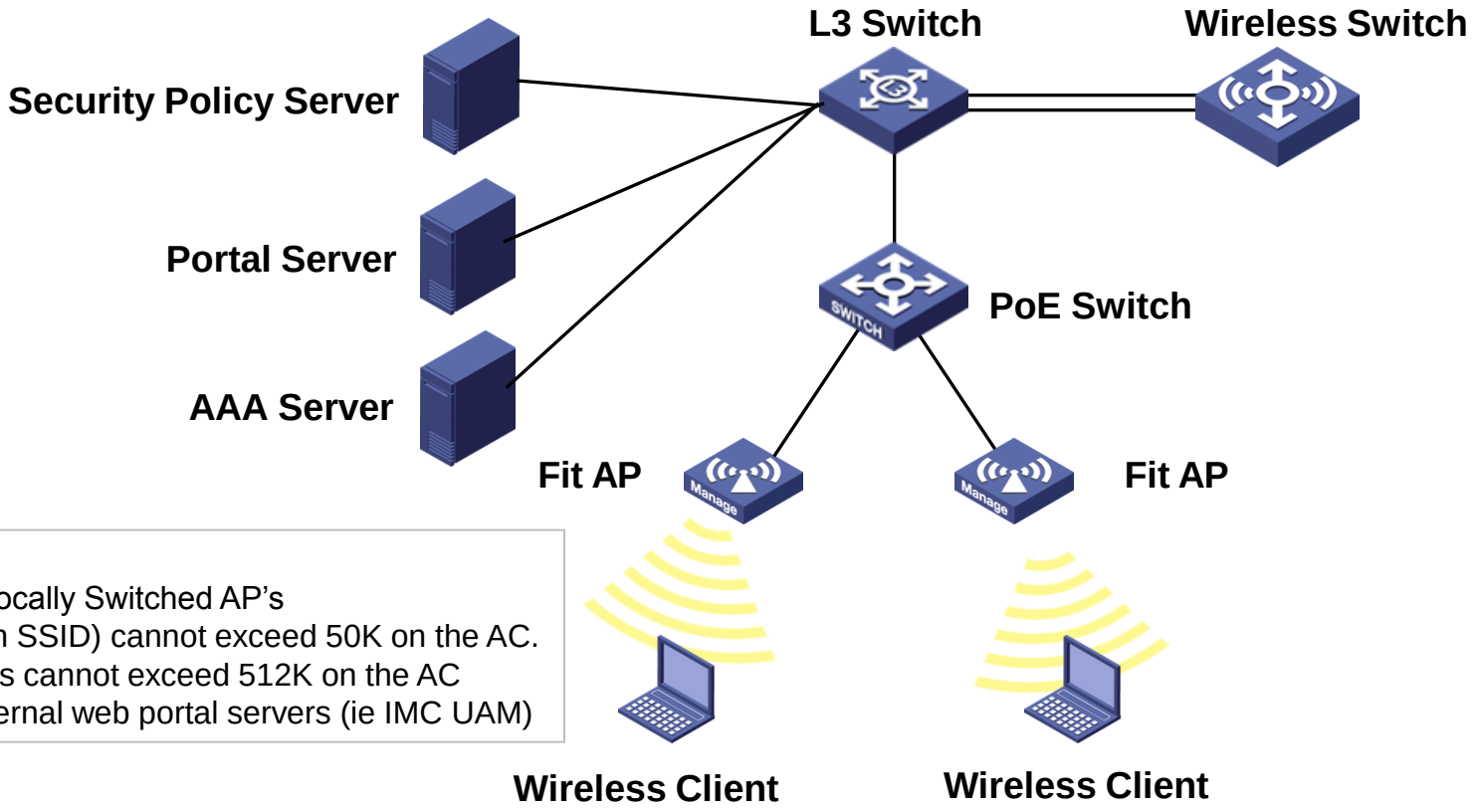
Local Switching

Note:
•Supports SSID, VLAN or Both
•WEB Portal is not supported



- **The local switching feature of the AC is a forwarding mode in which data exchange between clients is performed at the AP**
- **The AC does not take part in the data forwarding any more, which greatly reduces the load on the AC**

Web Portal – Local and External



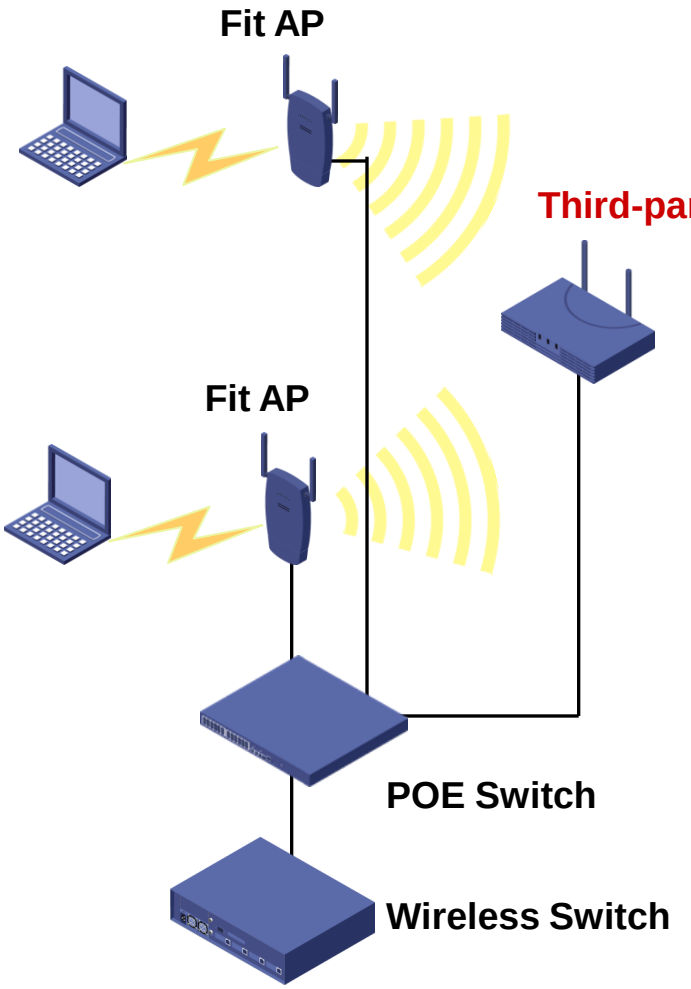
Note:
- Not Supported with Locally Switched AP's
- Web page size (for an SSID) cannot exceed 50K on the AC.
- Combined Web Pages cannot exceed 512K on the AC
- No limitations on external web portal servers (ie IMC UAM)

- **AC forces all users to log into the portal website**
- **Users can access the free services provided on the portal website; but to access the Internet, a user must pass portal authentication on the portal website**

Wireless Switch System – Authentication Encryption Mode

- **Wireless users can be authenticated through the Radius Server or the local database of wireless switch. The wireless switch supports the following authentication modes:**
  - 802.1X authentication
  - MAC authentication
  - Portal authentication
  - PPPoE authentication
- **The wireless switch supports the following encryption modes:**
  - Wired Equivalent Privacy (WEP)
  - Wi-Fi Protected Access (WPA)
  - WPA2

ROGUE Detection

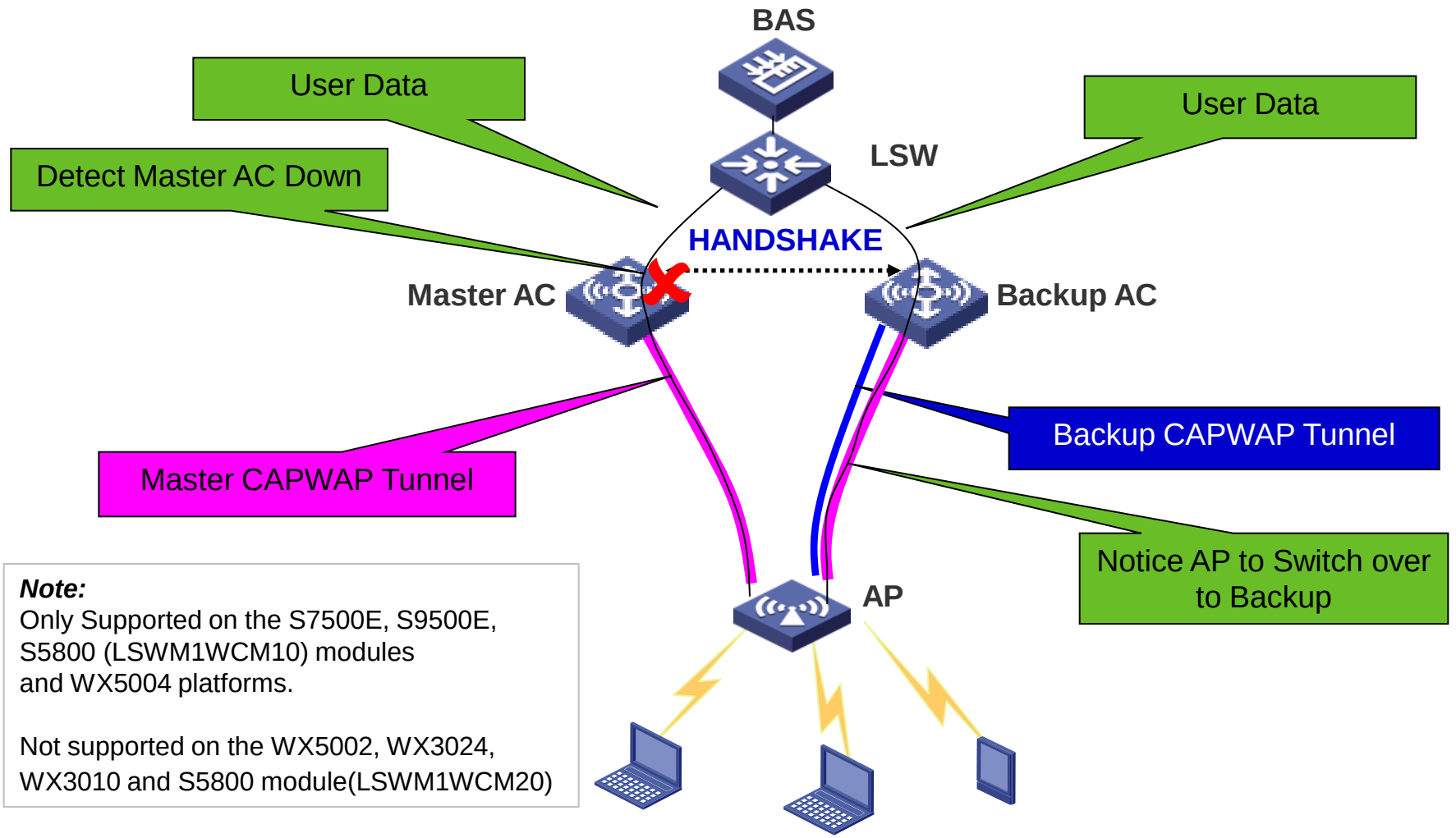


- **Rogue AP means an unauthorized AP running in the network. It and its users may bring threats to network security.**
- **With the Rogue AP detection function, the wireless switch can check Rogue devices and take countermeasures.**
- **APs can work in the following modes:**
  - Normal
  - Monitor
  - Hybrid

Redundancy Options

- 1 + 1 Fast Backup
- N + N Backup
- N + 1 Backup

1+1 Fast Backup

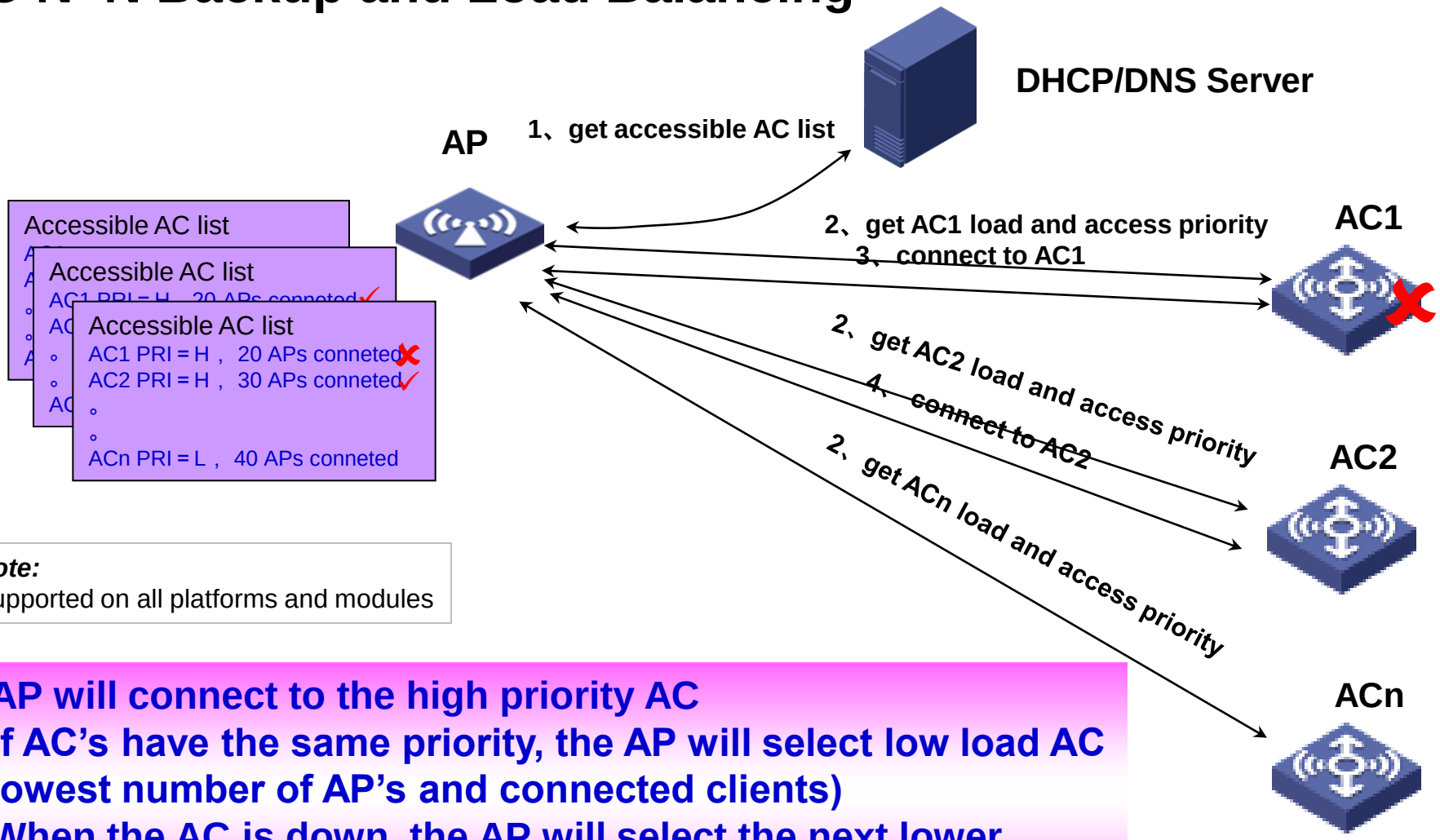


Note:
Only Supported on the S7500E, S9500E, S5800 (LSWM1WCM10) modules and WX5004 platforms.

Not supported on the WX5002, WX3024, WX3010 and S5800 module(LSWM1WCM20)

Backup AC will detect the master AC is down (S7500E, S9500E and S5800 (LSWM1WCM10) modules 100ms, WX5004 300ms) and the AP will switch over to the Backup AC. Master AC and Backup AC must be in the same subnet.

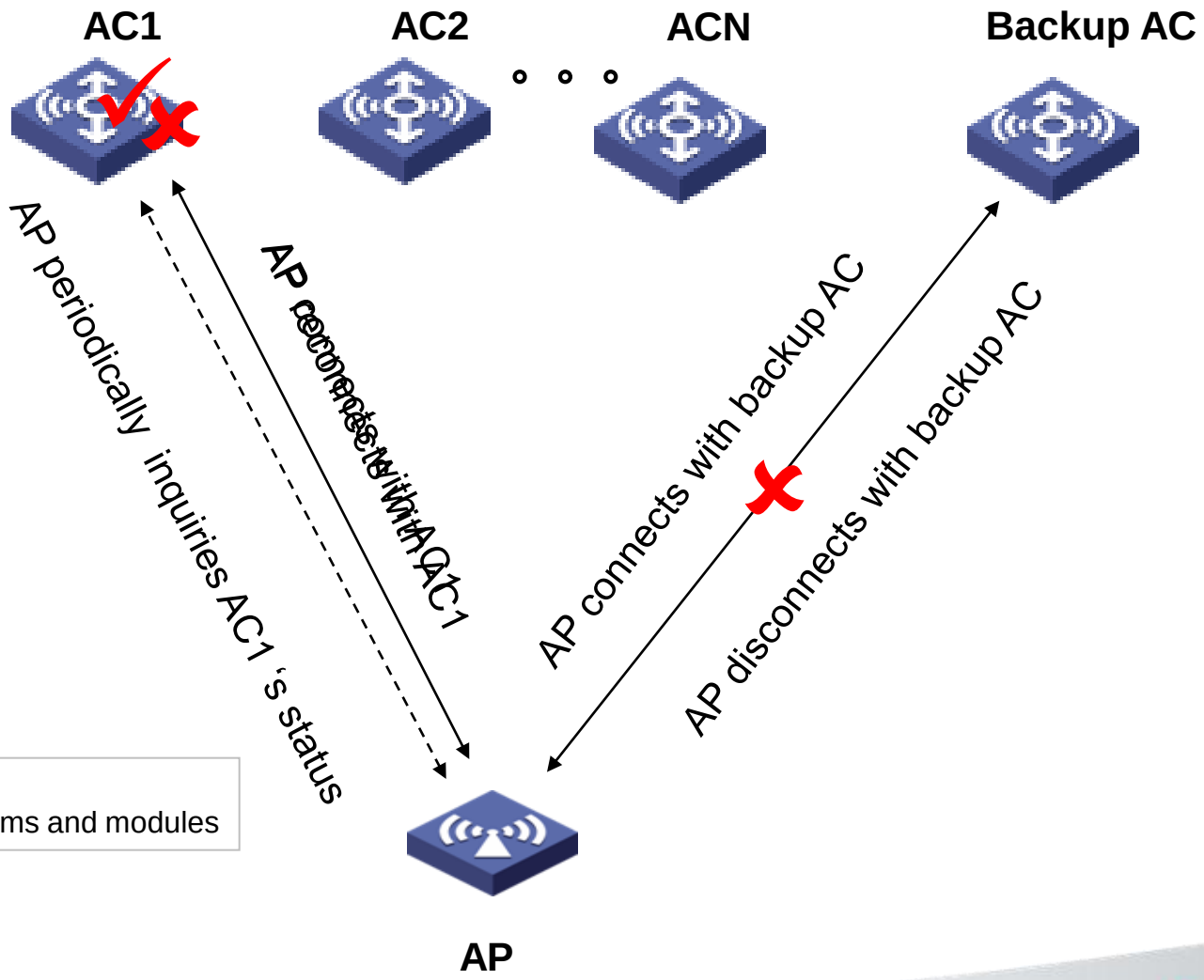
AC N+N Backup and Load Balancing



Note:
Supported on all platforms and modules

- **AP will connect to the high priority AC**
- **If AC's have the same priority, the AP will select low load AC (lowest number of AP's and connected clients)**
- **When the AC is down, the AP will select the next lower priority AC to connect to**

AC N+1 Backup



Note:
Supported on all platforms and modules

CLI Configuration Examples

- WLAN Service
- WLAN Security
- OAP Communications
- Load Balancing
- Roaming
- IDS

Configuring WLAN Service

- Enable WLAN Service
  - WLAN service is a part of COMWARE system. WLAN service can be enabled or disabled by this feature at runtime (WLAN service is enabled by default).
  - Enable WLAN Service (system view):
  - **wlan enable**
- Specify the country code
  - Country code identifies the country in which you want to operate the radio. It determines characteristics such as operating power level and total number of channels available for the transmission of frames. You must set the valid country code or area code before configuring an AP (country code is CN by default) .
  - Specify the country code (system view):
  - **wlan country-code** *code*

Configuring WLAN Service

- Create Wireless Interface
  - H3C wireless controllers support WLAN-ESS and WLAN-DBSS virtual interfaces. WLAN module dynamically creates a WLAN-DBSS virtual interface for each wireless access service;
  - A WLAN-ESS interface is a logical Layer 2 interface created manually, operates like Layer 2 Ethernet ports and has Layer 2 attributes such VLAN, 802.1x and so on;
  - A WLAN-ESS interface is used as a template for configuring WLAN-DBSS interfaces, WLAN-DBSS interfaces inherit the configuration of the corresponding WLAN-ESS interface.
  - Create a WLAN-ESS interface (system view):
  - **interface** *wlan-ess interface-number*

Configuring WLAN Service

- Configure Service Template
  - WLAN service template includes the attributes such as SSID, binding wireless interface, authentication algorithm (open-system or shared key) information. Service template can be **clear** or **crypto** type. You cannot change one type from another directly! To change the service template type, you must delete the existing service template, and configure a new service template again with type as you want.
  - Create a WLAN service template (system view):
  - **wlan service-template** *service-template-number { clear | crypto }*
  - Specify the service set identifier (service template view):
  - **ssid** *ssid-name*
  - Disable the advertising of SSID in beacon frames (service template view):
  - **beacon ssid-hide**
  - Enable authentication method, open system by default (service template view):
  - **authentication-method** *{ open system | shared key }*
  - Bind the WLAN-ESS to the service template (service template view):
  - **bind** *wlan-ess interface-number*
  - Enable local forwarding, disabled by default (service template view):
  - **client forwarding-mode local** [**vlan** *vlan-id-list*]
  - Enable or disable the service template, disable by default (service template view):
  - **service-template** *{ enable | disable }*

Configuring WLAN Service

- Display and Maintain WLAN Service
  - Display the information about a wireless interface:
  - **display interface** *wlan-ess interface-number*
  - Clear the statistics of a wireless interface:
  - **reset counters interface** *wlan-ess interface-number*
  - View the specified service template information:
  - **display wlan service-template** [*service-template-number*]

Configuring WLAN Security

- Enable an Authentication Method
  - Enter WLAN service template view (system view):
  - **wlan service-template** *service-template-number* **crypto**
  - Enable the authentication method (service template view):
  - **authentication-method** { **open-system** | **shared-key** }

📖 Notes:

  - By default, open system authentication is enabled;
  - Shared key authentication is usable only when WEP encryption is adopted;
  - Open system authentication is required for WPA and RSN.

- Configure Security IE
  - The security Information Element (IE) configuration includes WPA or/and RSN configuration.
  - Enable the WPA or/and RSN security IE (service template view):
  - **security-ie** {**wpa | rsn** }

Configuring WLAN Security

- Configure Cipher Suite
  - A cipher suite is used for data encapsulation and decapsulation, it uses one of encryption methods: WEP40, WEP104, TKIP or CCMP.
  - Enable the WEP cipher suite (service template view):
  - **cipher-suite { wep40 | wep104 }**
  - Configure the WEP default key (service template view):
  - **wep default-key { 1 | 2 | 3 | 4 } { wep40 | wep104 } { pass-phrase | raw-key }** *key*
  - Specify a key index number, 1 by default (service template view):
  - **wep key-id { 1 | 2 | 3 | 4 }**
  - Enable the TKIP cipher suite (service template view):
  - **cipher-suite tkip**
  - Enable the CCMP cipher suite (service template view):
  - **cipher-suite ccmp**

📖 Notes:

  - Regarding WEP key, pass-phrase option uses a string of alphanumeric characters as the key: 5 characters for WEP40, 13 characters for WEP104;
  - Raw-key option uses a hexadecimal number as the key: 10-digit number for WEP40, 26-digit number for WEP104.

Configuring WLAN Security

- Configure Port Security
  - Port security is a MAC address-based security mechanism for network access controlling, it controls the access of unauthorized devices to the network by checking the source MAC address of an inbound frame;
  - Four port security modes are added to support Wireless ports: psk, 802.1x (userlogin-secure-ext), mac-authentication, mac-and-psk, all these port security modes implement a link-layer security mechanism for wireless access devices
  - Enable port security, disabled by default (system view):
  - **port-security enable**
  - Specify a security mode for one wireless port (WLAN-ESS interface view):
  - **port-security port-mode** *{ psk | userlogin-secure-ext | mac-authentication |mac-and-psk}*
  - Enable 802.11 key negotiation, not for mac-authentication mode (WLAN-ESS interface view):
  - **port-security tx-key-type 11key**
  - Configure the key for psk or mac-and-psk modes (WLAN-ESS interface view):
  - **port-security preshared-key** { **pass-phrase** | **raw-key** } *key*

📖 Notes:

  - Regarding preshared key, pass-phrase option uses a string of 8 to 63 displayable characters, raw-key option uses a hexadecimal number of the length of 64;
  - AAA-related configurations may be required for 802.1x or mac-authentication.

Configuring WLAN Security

- Configure User Isolation
  - User isolation is designed to isolate clients in the same VLAN from one other while allowing them to access outside network;
  - To achieve this purpose, an AC maintains a user isolation table containing a list of permitted MAC addresses for each VLAN. When the AC receives a unicast sent from a station (wireless or wired station) to another station in the same VLAN, it allows the packet to pass or drops the packet depending on the user isolation table;
  - Even after being isolated, a station can communicate with its gateway so long as the MAC address of the gateway is permitted;
  - User isolation does not apply to the broadcasts and multicasts in a VLAN.
  - Enable user isolation (system view):
  - **user-isolation vlan *vlan-list* enable**
  - Add permitted MAC address entries (system view):
  - **user-isolation vlan *vlan-list* permit-mac *mac-list***

Note:

- The maximum number of permitted MAC addresses that can be configured for a VLAN is 16.

Configuring WLAN Security

- Display and Maintain WLAN Security
  - View the specified service template information:
  - **display wlan service-template** [*service-template-number*]
  - Display the configuration information, running state and statistics of port security:
  - **display port-security** [**interface** *interface-list*]
  - Display 802.1x session information or statistics:
  - **display dot1x** [**sessions | statistics**] [**interface** *interface-list*]
  - Display MAC authentication information:
  - **display mac-authentication** [**interface** *interface-list*]
  - Display user isolation statistics
  - **display user-isolation statistics** [**vlan** *vlan-id*]
  - Clear user isolation statistics
  - **reset user-isolation statistics** [**vlan** *vlan-id*]

Configuring OAP-related Communication

- OAP-related configurations are only required for WX3000 Series and S7500E Wireless Access Control Module (LSQM1WCMB0).
- Configuring OAP-related Communication for WX3024:
- **Configurations on WX3024 AC side:**
  - Login to WX3024 AC via console;
  - Create multiple VLANs as needed (system view):
  - **vlan** *{ vlan-id1* [to *vlan-id2*] | all *}*
  - Enter the internal GigabitEthernet1/0/1 port view (system view):
  - **interface** *GigabitEthernet1/0/1*
  - Configure the port link type as Trunk (GE port view):
  - **port link-type** *trunk*
  - Allow a specified VLAN to pass through the current Trunk port (GE port view):
  - **port trunk permit vlan** *{ vlan-id-list | all }*
  - Configure the default VLAN for the Trunk port (GE port view):
  - **port trunk pvid vlan** *vlan-id*

Configuring OAP-related Communication

- Configuring OAP-related Communication for WX3024:
- **Configurations on WX3024 switch side:**
  - Login to WX3024 switch via OAP command through AC's user view (press **Ctrl+K** to return);
  - **oap connect slot 0**
  - Create multiple VLANs as needed (system view):
  - **vlan** *{ vlan-id1 [to vlan-id2] | all }*
  - Enter the internal GigabitEthernet1/0/29 port view (system view):
  - **interface** *GigabitEthernet1/0/29*
  - Configure the port link type as Trunk (GE port view):
  - **port link-type** *trunk*
  - Allow a specified VLAN to pass through the current Trunk port (GE port view):
  - **port trunk permit vlan** *{ vlan-id-list | all }*
  - Configure the default VLAN for the Trunk port (GE port view):
  - **port trunk pvid vlan** *vlan-id*

Configuring OAP-related Communication

- Configuring OAP-related Communication for LSQM1WCMB0:
- **Configurations on Wireless Access Controller Module (LSQM1WCMB0) side:**
  - Login to LSQM1WCMB0 via console;
  - Create multiple VLANs as needed (system view):
  - **vlan** *{ vlan-id1 [to vlan-id2] | all }*
  - Enter the internal Ten-gigabitEthernet1/0/1 port view (system view):
  - **interface** *Ten-gigabitEthernet1/0/1*
  - Configure the port link type as Trunk (10GE port view):
  - **port link-type** *trunk*
  - Allow a specified VLAN to pass through the current Trunk port (10GE port view):
  - **port trunk permit vlan** *{ vlan-id-list | all }*
  - Configure the default VLAN for the Trunk port (10GE port view):
  - **port trunk pvid vlan** *vlan-id*

Configuring OAP-related Communication

- Configuring OAP-related Communication for LSQM1WCMB0:
- **Configurations on S7500E side:**
  - Login to S7500E via console;
  - Create multiple VLANs as needed (system view):
  - **vlan** *{ vlan-id1 [to vlan-id2] | all }*
  - Enter the internal Ten-gigabitEthernetx/0/1 port view (system view): where x means LSQM1WCMB0 slot number!
  - **interface** *Ten-gigabitEthernetx/0/1*
  - Configure the port link type as Trunk (10GE port view):
  - **port link-type** *trunk*
  - Allow a specified VLAN to pass through the current Trunk port (10GE port view):
  - **port trunk permit vlan** *{ vlan-id-list | all }*
  - Configure the default VLAN for the Trunk port (10GE port view):
  - **port trunk pvid vlan** *vlan-id*

Configuring WLAN Load Balancing

- Configure WLAN Load Balancing
  - AC manages client associations and disassociations. The load balancing parameters configured on the AC are used to determine whether the AC should accept or reject an association;
  - AC does load balancing during the association of a client;
  - AC supports two modes of load balancing:
    - Session mode: load balancing is done based on the number of clients associated with the APs;
    - Traffic mode: load balancing is done based on the amount of traffic going through the APs.
  - Configure session-mode load balancing (RRM view):
  - **load-balance session** *value* [**gap** *gap-value*]
  - Configure traffic-mode load balancing (RRM view):
  - **load-balance traffic *value* [gap *gap-value*]**

📖 Notes:

  - Session threshold is the number of maximum sessions, in the range 5 to 50. Session gap is in the range 1 to 8, 4 by default;
  - Traffic threshold is in the range 10 to 80 percentage. Traffic gap is in the range 10 to 40 percentage, 30 percentage by default.

Configuring WLAN Load Balancing

- Display and Maintain WLAN Load Balancing
  - Display WLAN RRM configuration information:
  - **display wlan rrm**
  - Display the WLAN RRM status of the AP(s):
  - **display wlan ap { all | name *apname* } rrm-status**
  - Display WLAN RRM information of the AP(s):
  - **display wlan ap** { **all** | **name** *ap-name* } [**verbose**]

Configuring WLAN Roaming

- Introduction to IACTP
  - Inter AC Tunneling Protocol (IACTP) is a proprietary protocol of H3C which defines how ACs communicate with each other;
  - IACTP provides a generic encapsulation and transport mechanism between ACs to provide secure AC-AC communications;
  - A mobility group is a group of ACs which communicate with each other using the IACTP protocol.
    - Establishment and maintenance of a mobility group is done using IACTP;
    - Every AC can and only can belong to one mobility group;
    - A maximum of 8 ACs can be present in a mobility group in current version.
  - The AC to which one wireless client associates for the first time is called as the Home-AC (HA) for this client. Another AC in the same mobility group to which this client roams is called as Foreign-AC (FA) for this client;
  - ACTP provides a control tunnel over TCP to exchange and synchronize roaming client database among ACs in the same mobility group prior to and during the roaming;
  - IACTP provides a data tunnel over UDP to transport data packets to or from the roaming client between HA and FA;
  - When 802.1X authentication is enabled on both HA and FA, re-authentication is not required to facilitate seamless roaming within the mobility group.

Configuring WLAN Roaming

- Configure an IACTP Mobility Group
  - An IACTP mobility group includes attributes such as the mobility tunnel protocol type, source IP address, authentication mode, and member IP addresses;
  - Create a mobility group with the specified name (system-view):
  - **wlan mobility-group** *name*
  - Specify the mobility tunnel protocol type, IPv4 type by default (mobility group view):
  - **mobility-tunnel** { **iactp** | **iactp6** }
  - Specify the tunnel source IP address (mobility group view):
  - **source** { **ip** *IPv4-address* | **ipv6** *IPv6-address* }
  - Specify a member IP address(mobility group view):
  - **member** { **ip** *IPv4-address* | **ipv6** *IPv6-address* }
  - Specify the authentication mode, no authentication by default (mobility group view):
  - **authentication-mode** *authentication-method authentication-key*
  - Enable the IACTP service for the group (mobility group view):
  - **mobility-group enable**

📖 Note:

  - Regarding authentication mode, only 128-bit MD5 authentication method is supported at present, authentication key is a string of 1 to 16 characters.

Configuring WLAN Roaming

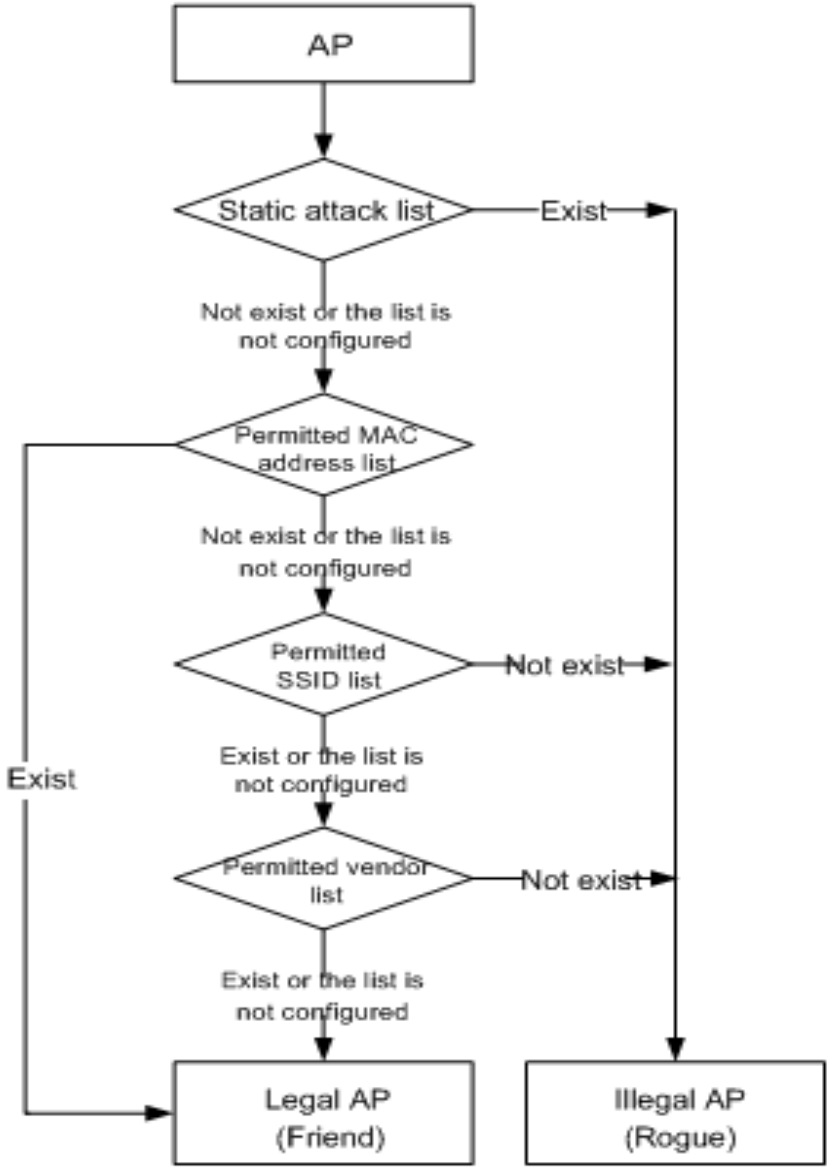
- Display and Maintain WLAN Roaming
  - Display mobility group information:
  - **display wlan mobility-group [member { ip *IPv4-address* | ipv6 *IPv6-address* }]**
  - Display the roam-track information of a client on the HA:
  - **display wlan client roam-track mac-address *mac-address***
  - Display the WLAN client roaming information:
  - **display wlan client** { **roam-in** | **roam-out** } [**member** { **ip** *IPv4-address* | **ipv6** *IPv6-address* }] [**verbose**]

Configuring WLAN IDS

- Introduction to WLAN IDS
  - WLAN Intrusion Detection System (WIDS) is used for the early detection of malicious attacks and intrusions on a wireless network.
  - Detecting rogue devices:
    - Rogue detection is applicable to large wireless networks. It detects the presence of rogue devices in a WLAN network based on the pre-configured rules.
    - Rogue detection can detect different types of devices in a WLAN network: rogue APs, rogue clients, rogue wireless bridges, and ad-hoc terminals.
  - Taking coutermeasures against rogue device attacks:
    - You can enable the countermeasures function on a monitor AP. The monitor AP downloads an attack list from the AC and takes countermeasures against the rogue devices based on the configured countermeasures mode.
    - For example, if the countermeasures mode is **config**, the monitor AP takes countermeasures against only rogue devices in the static attack list. It sends fake de-authentication frames by using the MAC addresses of the rogue devices to remove them from the network.

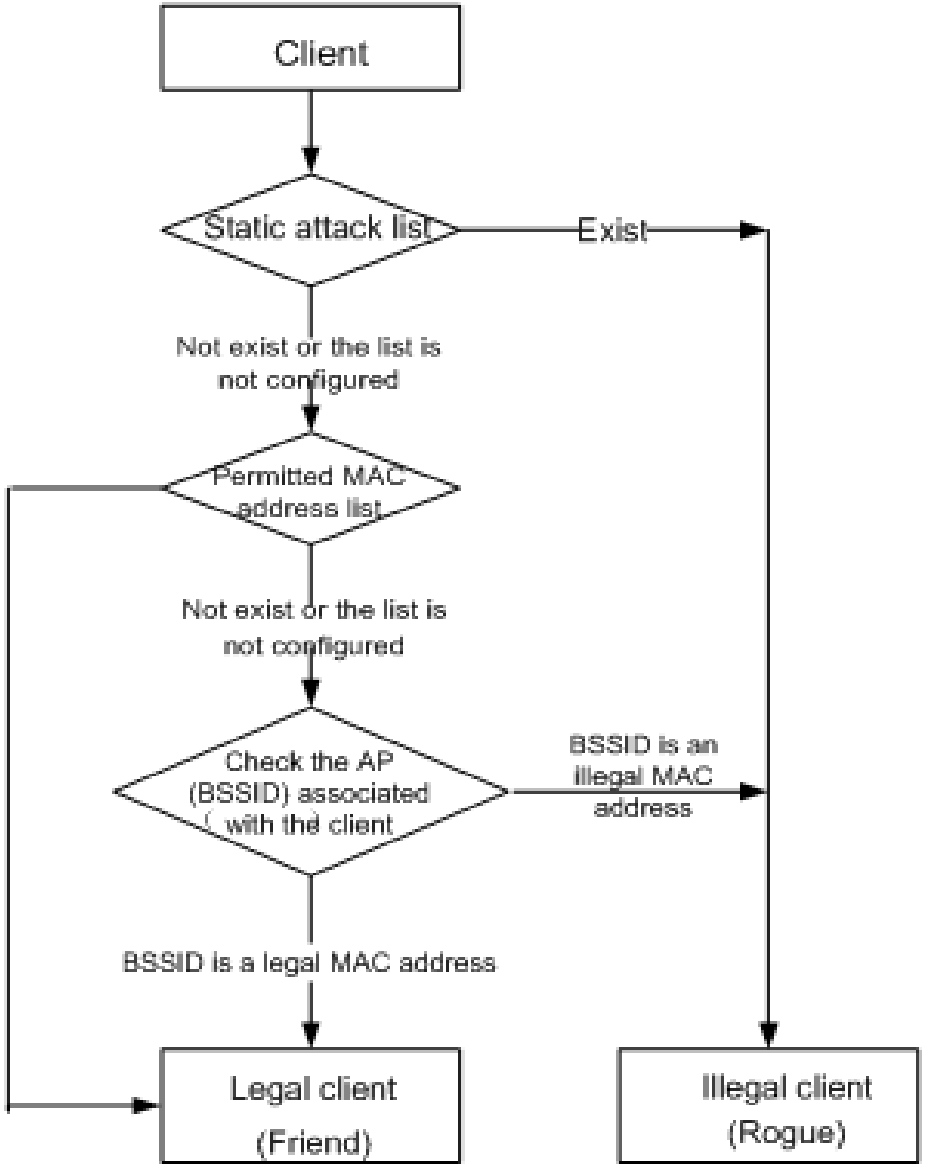
Configuring WLAN IDS

- Check whether an AP is a rogue



Configuring WLAN IDS

- Check whether a client is a rogue



Configuring WLAN IDS

- Configure AP Operating Mode
  - Configure the AP operating mode as monitor (AP template view):
  - **work-mode monitor**
  - Configure the AP operating mode as hybrid (AP template view):
  - **device-detection enable**

📖 Notes:

- By default, the AP operating mode is **normal**;
- When an AP has its operating mode changed from normal to monitor, it does not restart.
- But when an AP has its operating mode changed from monitor to normal, it restarts.

Configuring WLAN IDS

- Configure Detection of Rogue Devices
  - Enter WLAN IDS view (system view):
  - **wlan ids**
  - Add the MAC address of a client or AP to the static attack list (WIDS view):
  - **device attack mac-address *mac-address***
  - Add the MAC address of a client or AP to the permitted MAC address list (WIDS view):
  - **device permit mac-address *mac-address***
  - Add an SSID to the permitted SSID list (WIDS view):
  - **device permit ssid *ssid***
  - Add a vendor ID to the permitted vendor list (WIDS view):
  - **device permit vendor *vendor-oui***
  - Configure the device expiry timer, 600s by default (WIDS view):
  - **device aging-duration *duration***

Configuring WLAN IDS

- Configure Countermeasures Function
  - Based on the configuration, monitor APs can take countermeasures against devices present in its static attack list, all rogue devices, only rogue APs, or only ad hoc clients;
  - Countermeasures will not be taken against wireless bridges even if they are classified as rogues..
  - Configure the countermeasures mode (WIDS view):
  - **countermeasures mode** { **all** | **rogue** | **adhoc** | **config** }
  - Enable the countermeasures function (WIDS view):
  - **countermeasures enable**
- Configure IDS Attack Detection
  - Enable IDS attack detection (WIDS view):
  - **attack-detection enable** { **all** | **flood** | **weak-iv** | **spoof** }

Configuring WLAN IDS

- Configure WLAN IDS Frame Filtering
  - AC can be configured to maintain three types of lists: a static white list, a static blacklist, and a dynamic blacklist added when WLAN IDS detects flood attacks; is a MAC address-based security mechanism for network access controlling, it controls the access of unauthorized devices to the network by checking the source MAC address of an inbound frame;
  - White list and all blacklists entries in the AC will be distributed to all the registered APs;
  - Frame filtering will be carried out on APs as follows:
    - Whenever a frame is received by an AP, the source MAC address is checked;
    - If the source MAC address does not match any entry in the white list, it is dropped;
    - If no white list entries exist, the static and dynamic blacklist entries are searched;
    - If the source MAC address does not match any of the entries in the lists, the frame is further processed. Otherwise, it is dropped.
    - When no entries are present in the frame filter lists, all frames will be permitted.
  - Add an entry into the white list (WIDS view):
  - **whitelist mac-address *mac-address***
  - Add an entry into the static blacklist (WIDS view):
  - **static-blacklist mac-address *mac-address***
  - Enable the dynamic blacklist feature (WIDS view):
  - **dynamic-blacklist enable**
  - Configure the lifetime for dynamic blacklist entries, 300s by default (WIDS view):
  - **dynamic-blacklist lifetime** *lifetime*

Configuring WLAN IDS

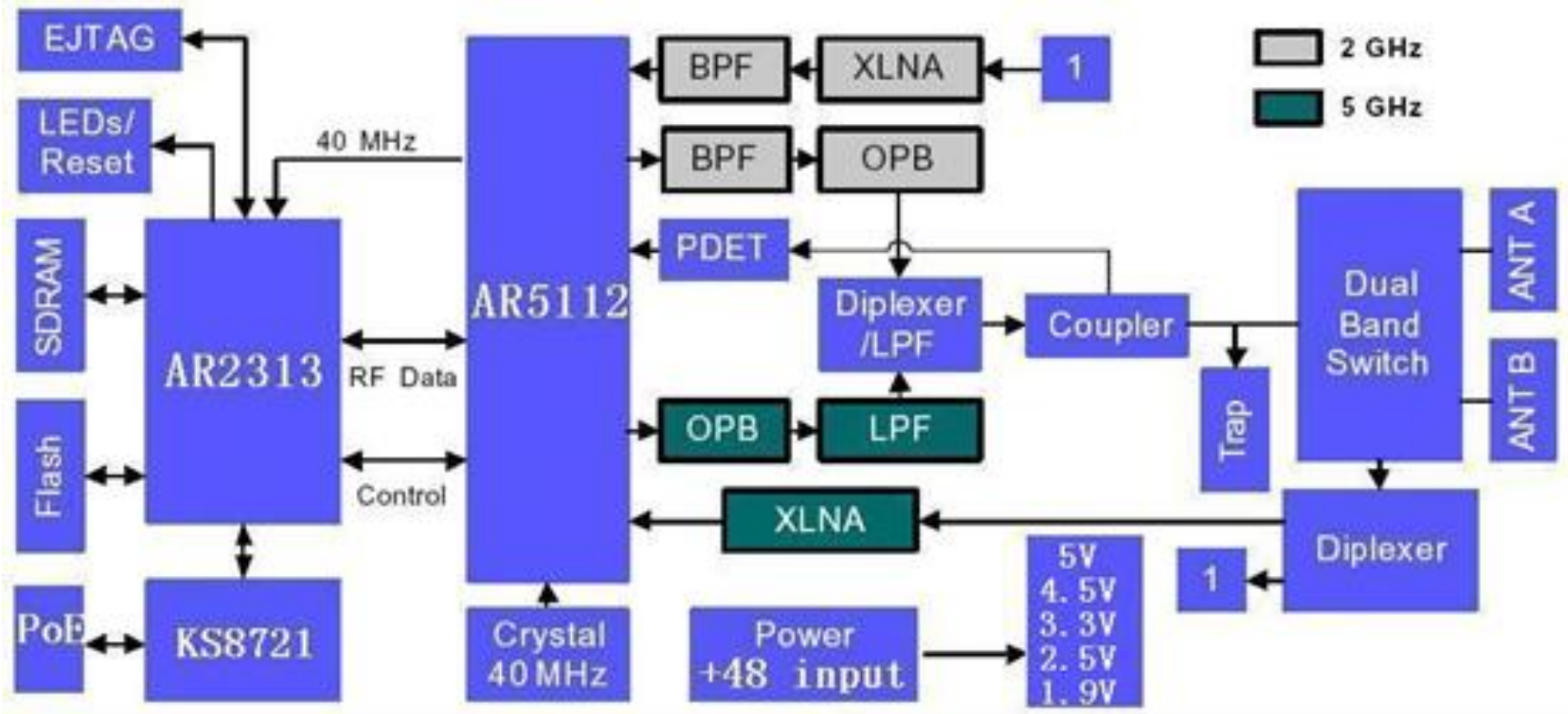
- Display and Maintain WLAN IDS
  - Display attack list information:
  - **display wlan ids attack-list** { **config** | **all** | **ap** *ap-name* }
  - Display detected entities:
  - **display wlan ids detected** { **all** | **rogue** { **ap** | **client** } | **adhoc** | **ssid** | **mac-address** *mac-address* }
  - Display the history of attacks detected in the WLAN system:
  - **display wlan ids rogue-history**
  - Display all the attacks detected by WLAN IDS:
  - **display wlan ids history**
  - Display the list of permitted MAC addresses, the list of permitted SSIDs, or the list of permitted vendor OUIs:
  - **display wlan ids permitted** { **mac-address** | **ssid** | **vendor** }
  - Display the count of attacks detected by WLAN IDS:
  - **display wlan ids statistics**
  - Display white list entries:
  - **display wlan whitelist**
  - Display blacklist entries:
  - **display wlan blacklist** { static | dynamic }
  - Clear the list of detected entities in WLAN:
  - **reset wlan ids detected** { **all** | **rogue** { **ap** | **client** } | **adhoc** | **ssid** | **mac-address** *mac-address* }
  - Clear all entries from the rogue-history list:
  - **reset wlan ids rogue-history**
  - Clear the statistics of attacks detected in the WLAN system:
  - **reset wlan ids statistics**
  - Clear dynamic blacklist entries:
  - **reset wlan dynamic-blacklist** { **mac-address** *mac-address* | **all** }

Thank you

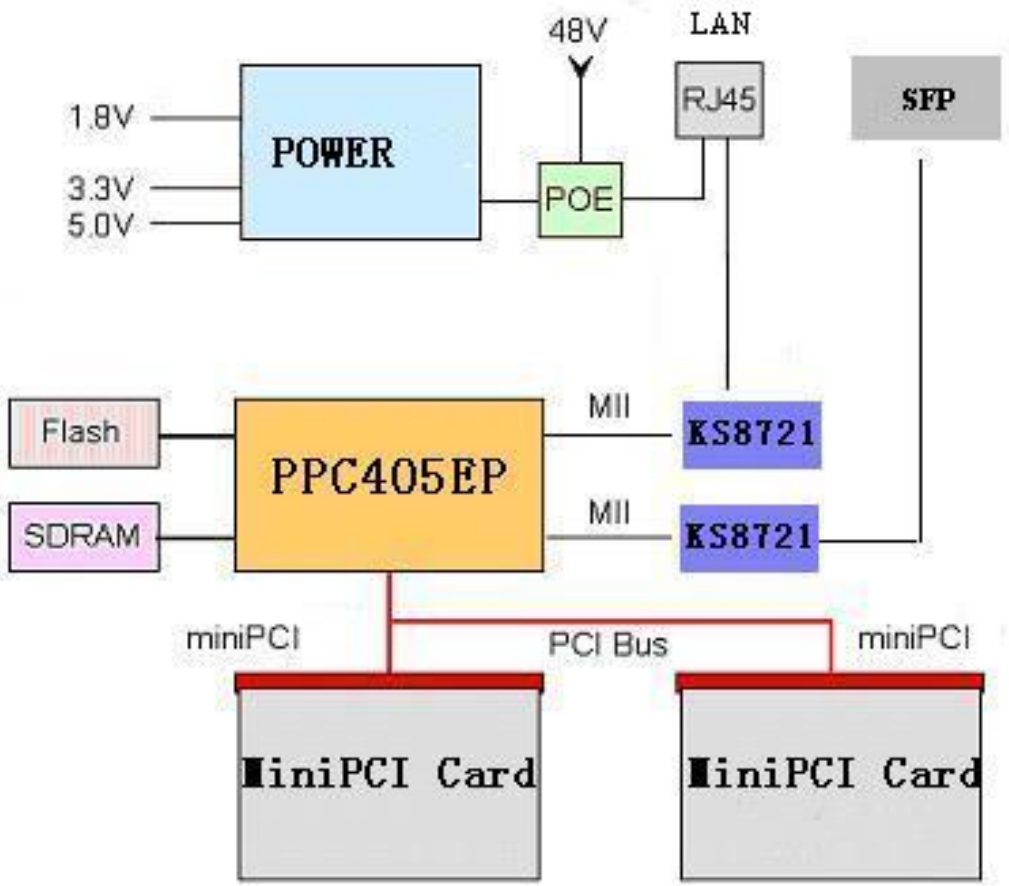
H3C 3Com TippingPoint

AP Functional Block Diagrams

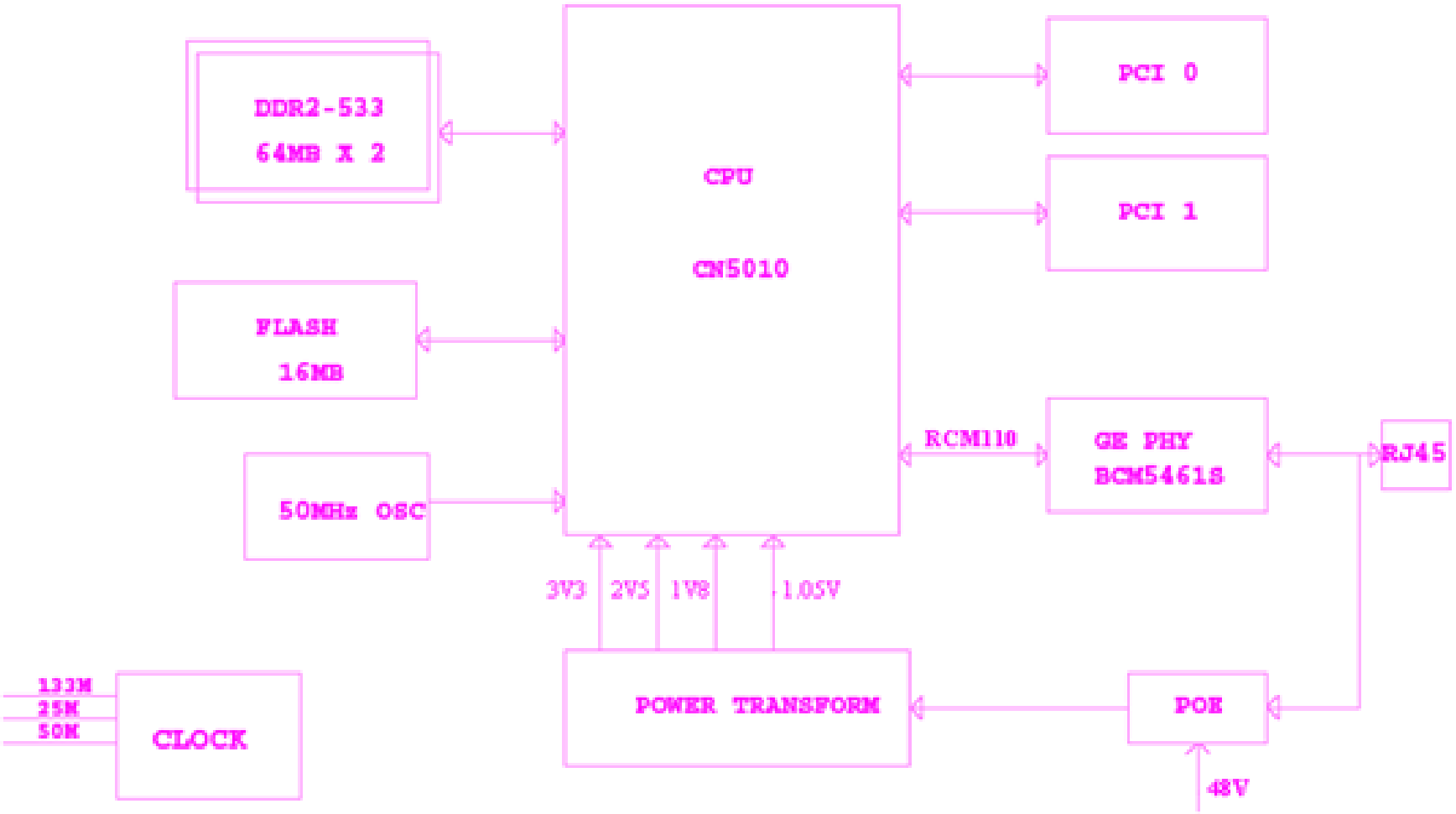
WA2110-AG Functional Block Diagram



WA2200 Functional Block Diagram

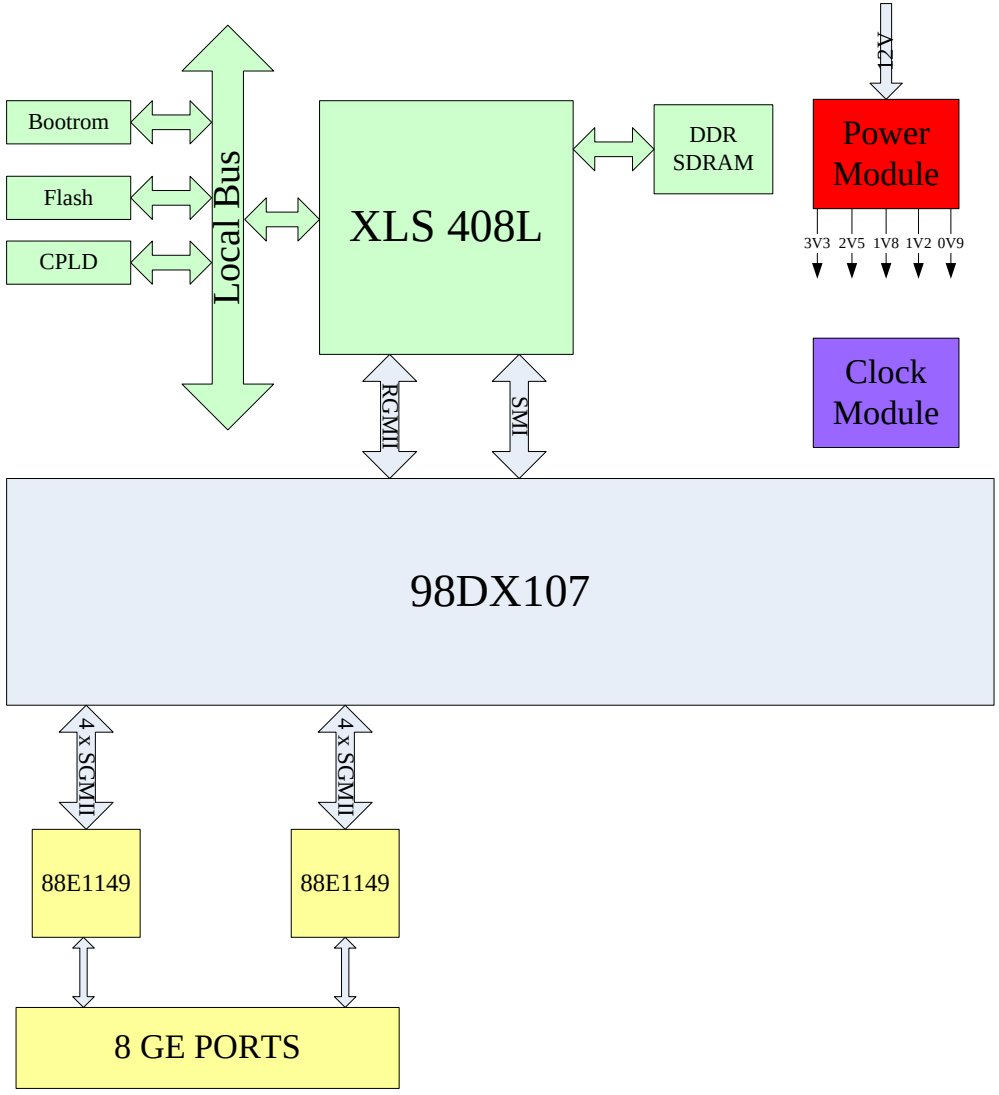


WA2600E Functional Block Diagram

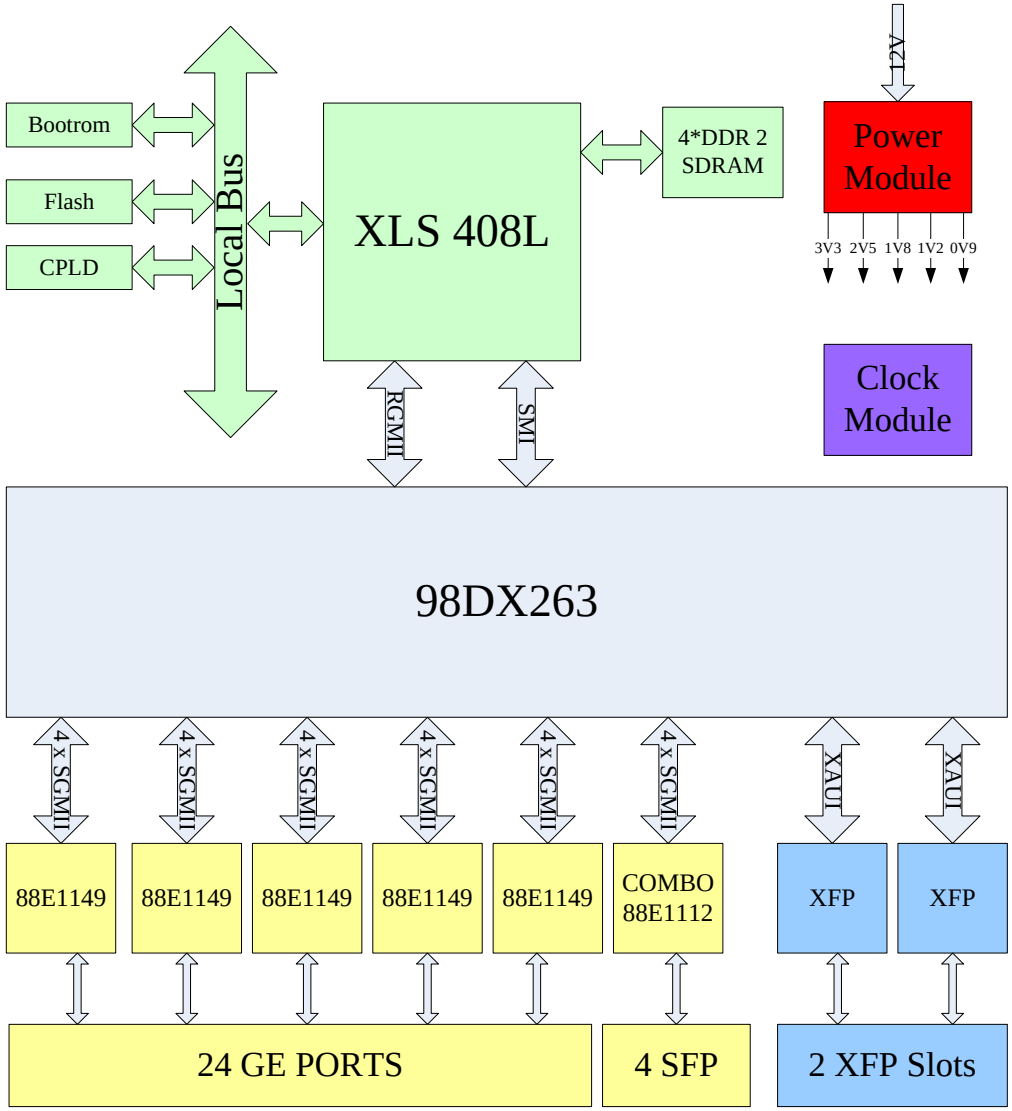


AC Functional Block Diagrams

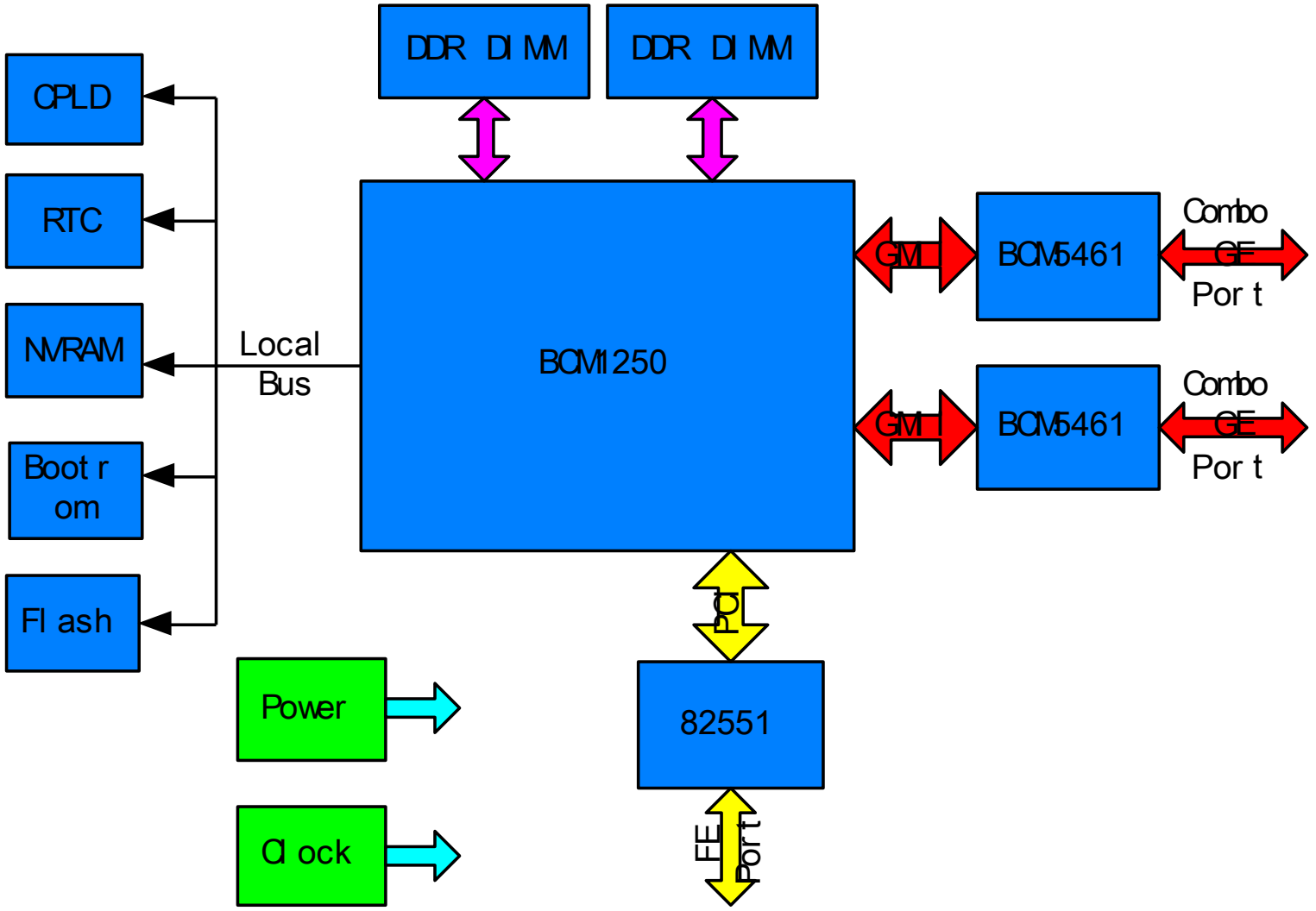
WX3008 Functional Block Diagram



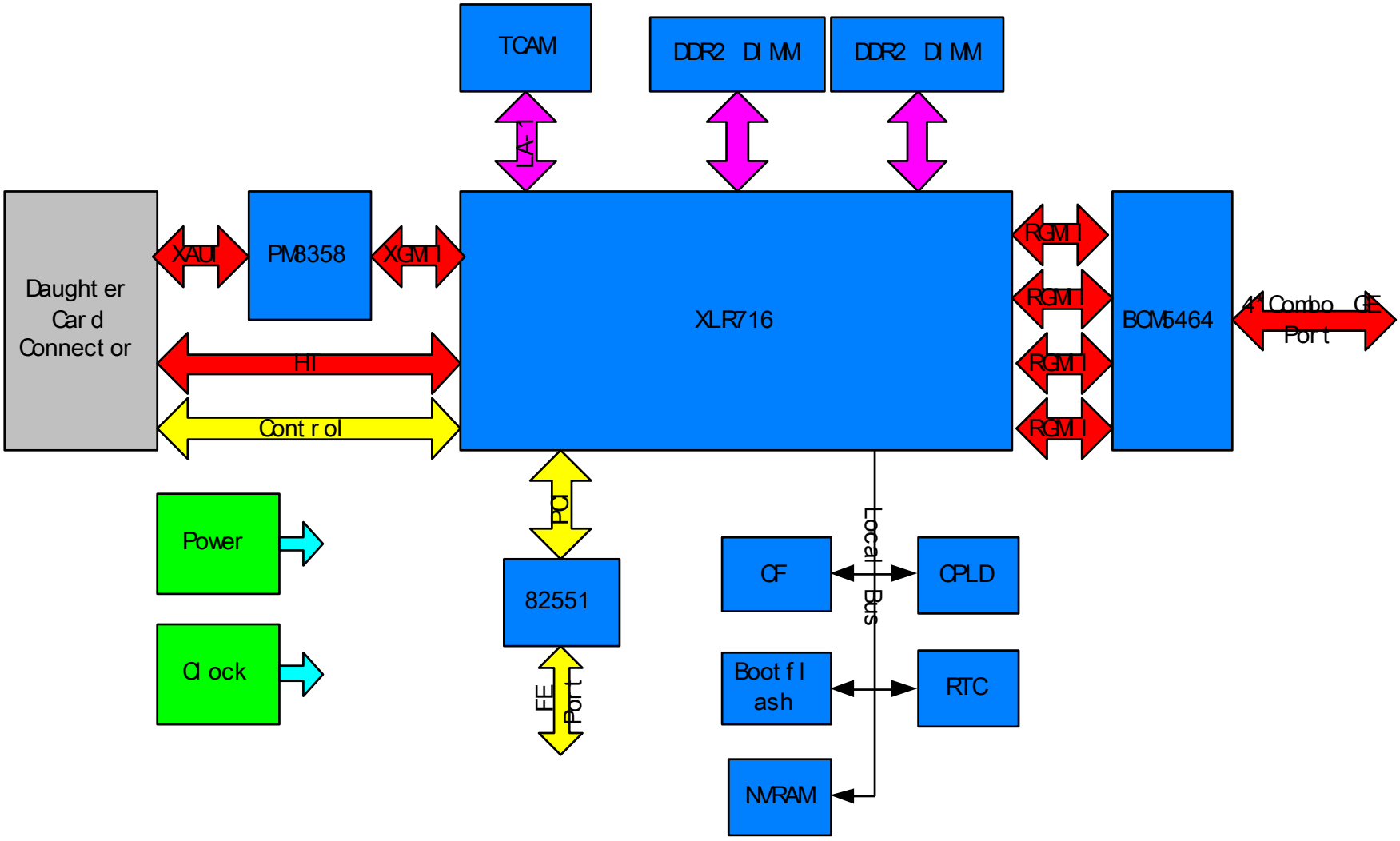
WX3024 Functional Block Diagram



WX5002 Functional Block Diagram



WX5004 Functional Block Diagram



S7500E Wireless Access Controller Module Functional Block Diagram