

Roaming

IAPP and WLCCP
Fast Secure L2 Roaming
Mobile IP
Proxy Mobile IP
Fast Secure L3 Roaming

Why Roaming?



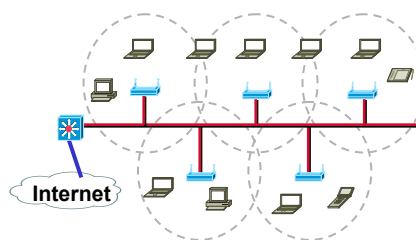
- **Reasons to roam:**
 - ♦ Too much retransmission
 - ♦ Miss too many beacons
- **Special roaming protocol is necessary because:**
 - ♦ Switching tables are not modified as quick as users move
 - ♦ Association and authentication process should not be repeated unnecessarily
 - ♦ Security context (unicast encryption keys, sequence numbers, etc) should also be propagated
- **How long does it take?**
 - ♦ Open Authentication
 - 2 messages only => 2 ms (802.11b)
 - ♦ Shared-Authentication: 4-6 ms
 - ♦ With EAP-TLS under Windows: > 100 ms (!)
 - ♦ Delay to *find* an AP: > 0.3 seconds
 - Probe request / probe response mechanism is performed on all channels
 - ♦ Total delay: > 0.5 seconds
 - ♦ Total delay if 802.1x is involved: up to several seconds

IAPP and WLCCP



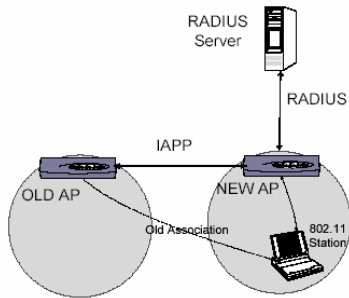
- IEEE 802.11 does NOT specify inter-AP communication
 - ♦ Reason: any LAN technology should be used as infrastructure
- 802.11f: IAPP—draft only!
 - ♦ Draft 6.0 is a *recommended practice*
 - ♦ Problem: context transfer mostly proprietary solved
- Cisco's SWAN's Wireless LAN Context Control Protocol (WLCCP)
 - ♦ Manages the SWAN network topology and the "operational context" for mobile stations in a SWAN network
 - ♦ SWAN has a well defined client context to support security, QoS, etc.

Inter Access Point Protocol



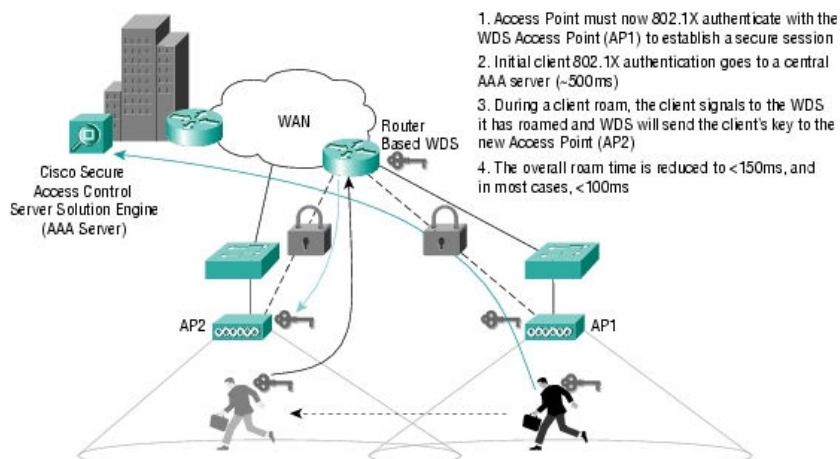
- 802.11 does not specify ANY roaming method
- L2 roaming method for IEEE 802.11 WLANs
 - ♦ Multi-vendor AP interoperability
 - ♦ Relies upon IP environment
- IAPP is result of a cooperation between
 - ♦ Aironet (before Cisco)
 - ♦ Lucent Technologies (before they spun off Agere)
 - ♦ Digital Ocean (before they disappeared from the scene)
- IEEE 802.11 is working on standardizing IAPP in [IEEE 802.11f](#)

IAPP Principles



- Transmits station *security* context between APs
 - Also used by 802.1x authentication
- Uses RADIUS to obtain preconfigured station information
- Proactive caching
 - Current access point distributes the security context of the mobile station to neighboring access points *before* the station actually handoffs
- Requires mobile station to send a *re-association request*
- No need for re-authentication
 - "Seamless handover"
- Protocols used:
 - TCP for Inter-AP communication (context blocks)
 - UDP for IAPP notify packets (224.0.1.178)
 - UDP for RADIUS request/responses
 - Layer 2 frames to update the forwarding tables

Cisco: Fast Secure Roaming



1. Access Point must now 802.1X authenticate with the WDS Access Point (AP1) to establish a secure session
2. Initial client 802.1X authentication goes to a central AAA server (~500ms)
3. During a client roam, the client signals to the WDS it has roamed and WDS will send the client's key to the new Access Point (AP2)
4. The overall roam time is reduced to <150ms, and in most cases, <100ms

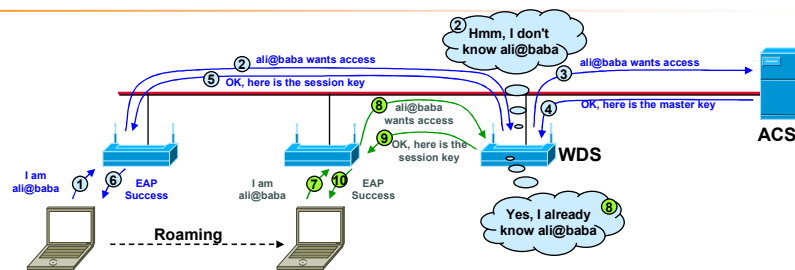
Note: Because the WDS handles roaming and reauthentication, the WAN link is not used

Note



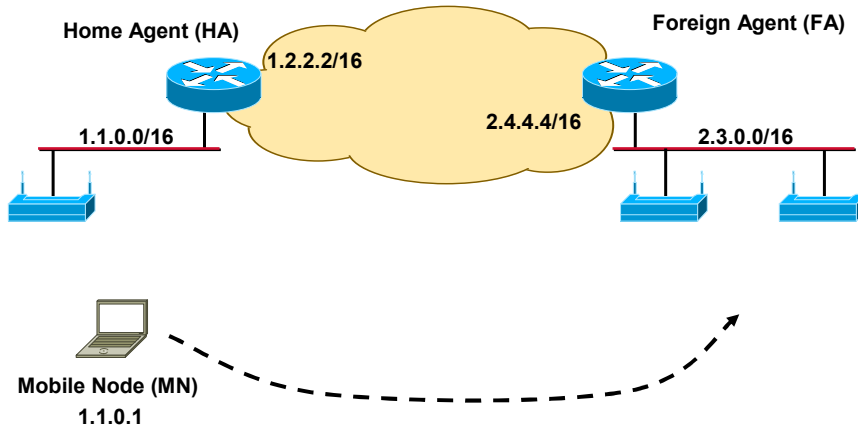
- Configure same SSID on all APs to support seamless roaming without user interaction
 - ♦ Aka Extended SSID (ESSID)
- Hot standby AP associates with the monitored AP as a client and sends IAPP/WLCCP queries to the monitored AP
 - ♦ Through both the Ethernet and the radio ports
 - ♦ If the monitored AP fails to respond, the standby AP comes online and takes the monitored AP's place in the network.

Fast Secure Roaming

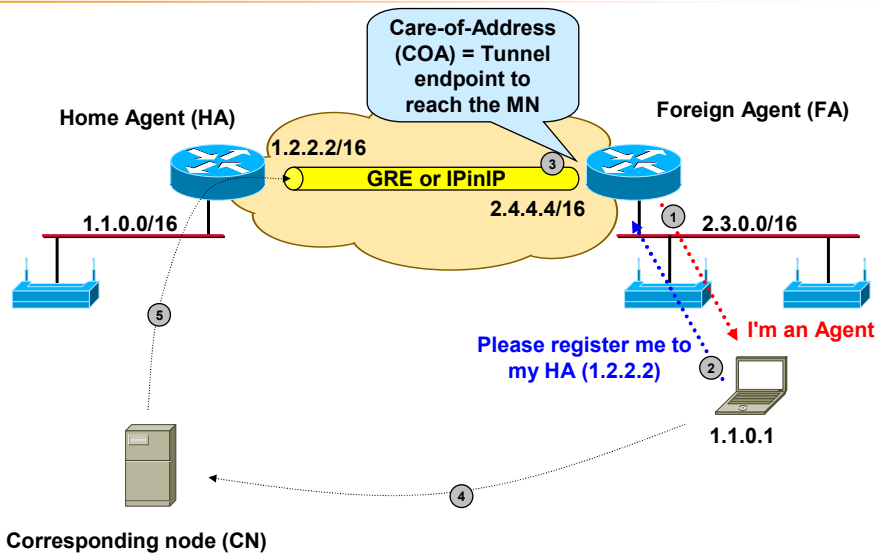


- Using LEAP, one (or more) AP(s) can be configured to provide Wireless Domain Services (WDS)
 - ♦ Cisco Centralized Key Management (CCKM) is supported
 - ♦ **Clients must also enable CCKM**
 - ♦ Also backup WDS can be configured (via priorities)
 - ♦ WDS maintains cache with user credentials for CCKM-capable clients
- Pre-registration request/reply between AP and WDS
 - ♦ WDS forwards auth-request to ACS if client not already in local auth-list
 - ♦ ACS sends master key = MD5(user-ID, credentials) to WDS
 - ♦ WDS (and client) calculate session key from master key
 - ♦ WDS forwards client's session key to new AP
 - ♦ WLCCP protocol used as control traffic between APs and WDS

Mobile IP – Basic Concept (1)



Mobile IP – Basic Concept (2)

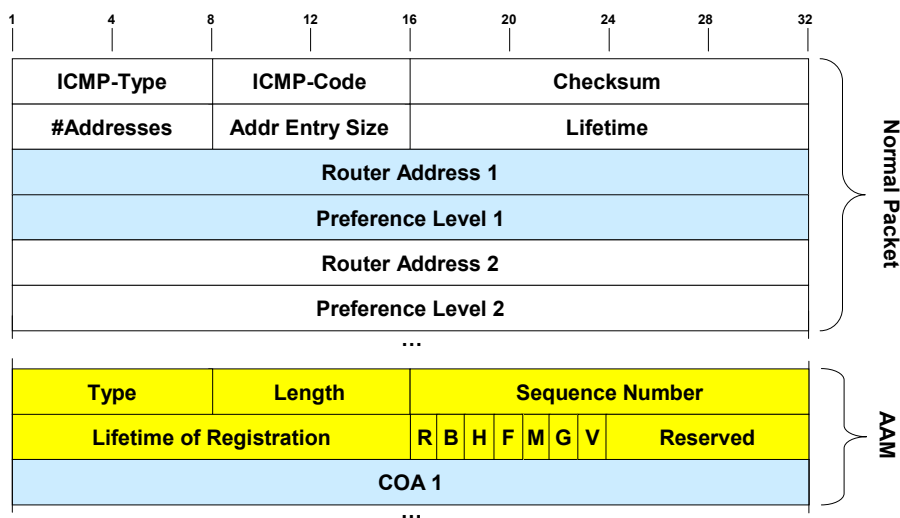


Note

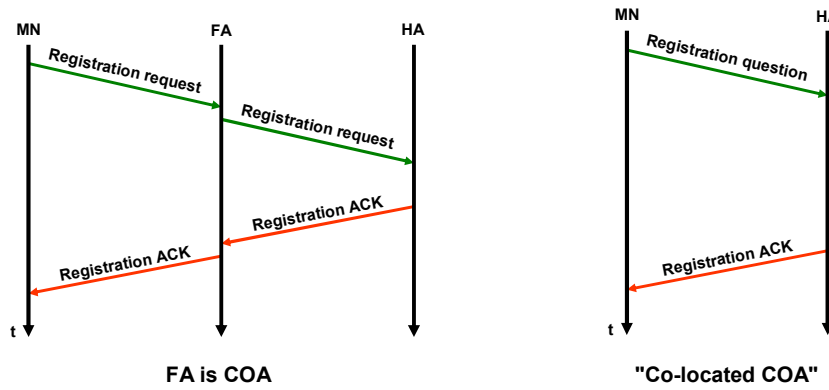


- In the previous example the FA relays the registration process of the MN to the HA
 - ♦ And therefore the COA is associated with the FA
 - ♦ And therefore the tunnel endpoint is at the FA
- But the COA can also be dynamically assigned from the FA to the MN
 - ♦ Then the MN can directly send the registration to the HA
 - ♦ And therefore the tunnel endpoint is at the MN
- In any case, the MN needs Mobile-IP software
 - ♦ Obviously also the HA and FA
- Protocols used
 - ♦ Agent discovery via ICMP Router Discovery Protocol (IRDP)
 - Extensions to the Router Advertisement and Router Solicitation messages already defined for ICMP
 - Sent every 3 seconds
 - ♦ Registration via UDP Port 434
- Lots of extensions available
 - ♦ Regarding efficiency, reliability, security

Agent Advertisement Message



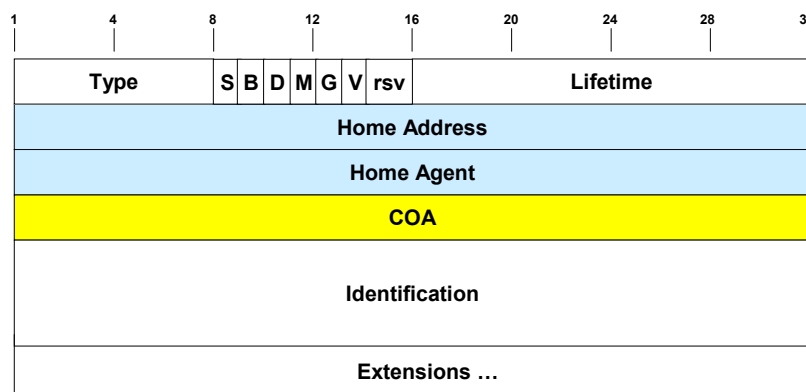
Registration Modes



Registration Message (1)



(Carried in UDP Payload)



Registration Message (2)



- **Type** field set to 1 (=Registration Request)
- **Simultaneous bindings** (S-Bit)
 - Mobile node requests HA to retain its prior mobility bindings
- **Broadcast datagrams** (B-Bit)
 - HA should tunnel any broadcast datagrams that it receives on the home network
- **Decapsulation by mobile node** (D-Bit)
 - MN decapsulates datagrams by itself (using a co-located COA)
- **Rsv**
 - Reserved bits; set to zero
- **Home Address**
 - IP address of the MN
- **Home Agent**
 - IP address of the MN's HA
- **Care-of Address**
 - IP address of tunnel endpoint
- **Identification**
 - 64-bit number used to match registration requests and replies
 - Mitigates replay attacks of registration messages
- **Extensions**
 - E. g. Authentication Extension to be included in all registration Requests

Optimization (1)



To optimize Mobile IP, CN needs to know **current position** of MN (=> maintain a Binding Cache)

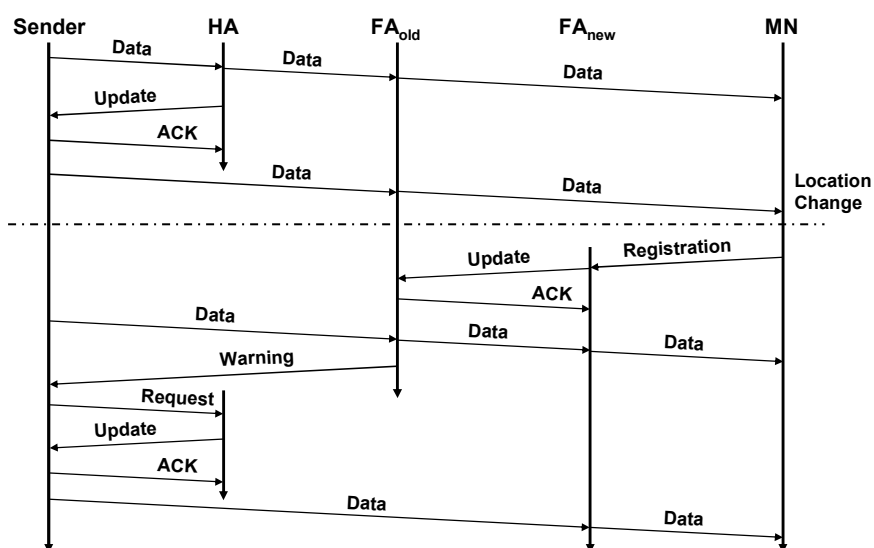


Optimization (2)



- HA may inform CN – but 4 new messages necessary:
 - ♦ **Binding Request**
 - Every CN who wants to know MN's current location can send this message
 - If MN allowed publication of current location, HA can send a Binding Update
 - ♦ **Binding Update**
 - Includes fixed IP address of the MN and COA address
 - ♦ **Binding Acknowledgement**
 - Acknowledgement of Binding Update
 - ♦ **Binding Warning**
 - If a FA receives a packet but this FA isn't the current FA anymore, this FA can send a Binding Warning (smooth handover)
 - Send to HA

Optimization (3)



Proxy Mobile IP (PMIP)

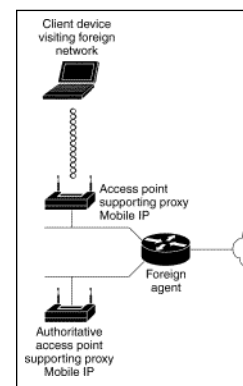


- With PMIP, the Mobile Node does not need a Mobile IP stack
- The AP
 - ♦ Cares for agent discovery
 - ♦ Generates registrations to the HA in behalf of the MN
- Three steps to perform:
 - ♦ Agent discovery
 - ♦ Updating the subnet map table
 - ♦ Device registration
- Tunnel types: GRE or IPinIP

PMIP Phases (1)



- AP boots up or PMIP is enabled
 - ♦ Agent Discovery is performed
 - ♦ HA and FA advertise their services on the network by using the IRDP
 - ♦ AP learns
 - Whether an agent is a HA, a FA, or both
 - The COA
 - The Subnet Map Table, containing a list of HA IP addresses and subnet masks
 - Capabilities (GRE and reverse tunneling, registration lifetime, roaming period)
 - ♦ AP can also enforce these advertisements by sending agent solicitation messages
- Subnet Map Table is sent to Authoritative AP (AAP)
 - ♦ AAP is responsible to keep the latest Subnet Map Table
 - ♦ AAP adds new (PMIP-) AP to a list
 - ♦ AAP also adds learned HA to the Subnet Map Table
 - ♦ Finally, the AAP informs all other APs
 - ♦ You can designate up to three AAPs on your wireless LAN.



PMIP Phases (2)



- When AP detects that client is connected to a foreign network
 - ♦ The AP obtains a COA from the FA
 - ♦ This COA can be shared for multiple client devices
 - ♦ The AP notices that the client belongs to another network and begins the registration
 - ♦ The AP now determines the client's HA address from the subnet map table
- Registration
 - ♦ Each AP is configured with the **mobility security association** (shared key) of all potential visiting clients with their corresponding HA
 - Can be provided by a Radius server
 - ♦ AP sends registration request (mobile-SA shared key, client's IP) to the HA of the client
- Agents check this request
 - ♦ FA checks validity of the registration request (requested lifetime must not exceed its limitations and requested tunnel encapsulation must be available)
 - ♦ HA checks if authentication valid

PMIP Phases (3)



- HA
 - ♦ Creates a mobility binding (client to COA association)
 - ♦ Creates a tunnel to the COA
 - ♦ Creates a routing entry to the client's home IP address through the tunnel
 - ♦ Sends a registration reply
- FA
 - ♦ Checks if registration reply is valid (is registration request still pending?)
 - ♦ Add visiting client to visitor list
 - ♦ Establishes a tunnel to the HA
 - ♦ Creates routing entry to HA
 - ♦ Relays registration reply to client
- AP
 - ♦ Checks validity of registration reply
 - ♦ Forwards client packets to FA
 - ♦ Re-registers on behalf of the visiting client before its registration lifetime expires

Note



- Proxy Mobile IP does not support VLANs (currently?)
- Use NTP:
 - ◆ Registration requests may fail if the timestamps generated by the requestor are outside the window expected by the receiver
- Be sure to enable proxy Mobile IP on each SSID that requires it
 - ◆ None of the proxy Mobile IP configuration commands take effect until proxy Mobile IP is set on the SSID
- AP requires a default gateway entry
- No IP multicast support
- Make sure that UDP port 6500 is not blocked between the authoritative AP and other APs
 - ◆ Used for subnet table updates

PMIP Configuration



```
ap1200# configure terminal
ap1200(config)# ip proxy-mobile enable
ap1200(config)# ip proxy-mobile aap 192.168.15.22 192.168.15.24 192.168.15.28
ap1200(config)# ip proxy-mobile secure node 10.91.7.151 10.91.7.176 spi 102 key ascii 0987654
ap1200(config)# interface fastethernet 0
ap1200(config-if)# ip proxy-mobile
ap1200(config-if)# interface dot11radio 0
ap1200(config-if)# ip proxy-mobile
ap1200(config-if)# ssid tsunami
ap1200(config-if-ssid)# ip proxy-mobile
ap1200(config-if-ssid)# exit
ap1200(config-if)# exit
ap1200(config)# interface bv11
ap1200(config-if)# ip proxy-mobile
ap1200(config-if-ssid)# end
```

PMIP Security



- **Mobile IP**
 - ◆ Uses a strong authentication scheme to protect communications to and from visiting clients
 - ◆ All registration messages between a visiting client and the home agent must contain the mobile-home authentication extension (MHAE).
- **Proxy Mobile IP**
 - ◆ Also implements this requirement in the registration messages sent by the AP on behalf of the visiting clients to the home agent

Fast Secure L3 Roaming



- **WLSM needed**
 - ◆ Only for Cat 6500 switches with Supervisor 720 Module (\$\$\$)
 - ◆ Runs WDS which is responsible for coordination
- **APs can be installed anywhere in L3 network – no VLAN configuration needed**
 - ◆ Traffic confined in tunnels
- **Overlay of multipoint GRE (mGRE) tunnels**
 - ◆ Each tunnel is terminated by the Supervisor Module (that hosts the WLSM)
 - ◆ APs are on the other tunnel endpoints
- **SSID is mapped to a mobility network**
- **Supervisor 720 maintains a database of the clients and the corresponding APs**
 - ◆ Roaming between APs requires updating the database and changing the forwarding information for that client
 - ◆ APs providing Layer 3 mobility must register with the WDS
- **Each AP has configured**
 - ◆ The address of the WDS
 - ◆ LEAP credentials to authenticate AP to the WDS (via AAA server)
 - ◆ AP must be configured to be part of the same mobility group
 - `command mobility network-ID`
 - Also enable CCKM for this mobility group

Fast Secure L3 Roaming – Config

