AP Management
and Handover support

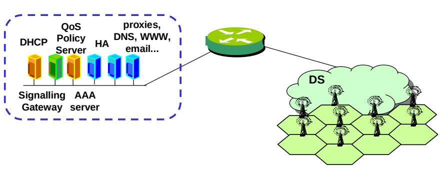
CapWap and 802.11f

Renato Lo Cigno – Alessandro Villani
www.disi.unitn.it/locigno/didattica/NC/

...Copyright

ESS and Micro-mobility

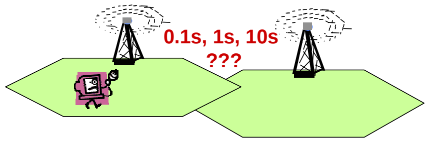
- A collection of coordinated IBSS forms an ESS
- The APs in the same ISS can broadcast the same SSID



- As far as they are on the same LAN mobility between APs is allowed seamlessly (nearly)

AP Coordination (1)

- How to position APs?
- How to assign them channels and power level?
- What happens if I add/remove and AP
- How fast is the re-association to an new AP if I'm roaming the area?



AP Coordination (2)

- Centralized management?
- Distributed coordination?
- What layer (Ethernet or IP)?
- What functionalities
- Integration with user management?
- What about resources?
- Can we balance their use?

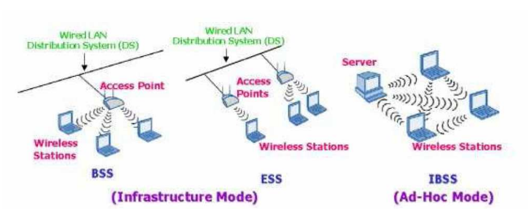
IEEE vs. IETF

- Two main proposal for standardization of an Inter Access Points Protocol – IAPP
- One in IEEE: 802.11f (already standard ... not much implemented ☹) mainly supports coordinated handovers, 802.11r (resource management), 802.11k (fast handover for vehicular applications)
- One in IETF: capwap (Control And Provisioning of Wireless Access Points), not yet definitive (RFCs 4118, 4565, 4564, 3990, plus drafts), omni-comprehensive, not much focused on handovers
- Proprietary solutions (Cisco, Avaya, ...)

802.11f

Scope & Goals

- Main (unique??) goal is enabling and simplifying the mobility between APs within the same ESS



IEEE 802.11f

- Recommendation to implement an Inter-Access Point Protocol (IAPP) over a Distribution System (DS) possibly wireless
- Not much used, also because of limited functionalities
- Standard available @ http://standards.ieee.org/getieee802/download/802.11F-2003.pdf

Realization & Implementation

- IAPP is an application level protocol
- Runs directly on ethernet multicast or on IP multicast, obviously enclosed within the DS
- The standard provides primitives for handover only
- Requires the presence of a Radius server for management purposes
- APs should be registered on the Radius server
- Uses standard MIBs for accessing managing the AP data

Some more stuff ...

- IAPP is not a routing protocol, and assumes a 802-based DS
- IAPP is not concerned with user data delivery
- No address management is considered, STA must have/obtain valid addresses
- May keep a table of physically adjacent APs to support handovers and to do load balancing
- If IAPP is used all APs with the same SSID on the same DS are part of the same ES

IEEE 802.11f: primitives (examples)

- **IAPP-INITIATE/ADD/TERMINATE:** create an ESS, add a node (1 AP) to it, terminate one node
- **IAPP-MOVE.request/indication(STA,AP1):** indicates on the multicast group that STA re-associated with AP1
- **APP-MOVE.response/confirm(STA,AP1,AP2):** transmit all information relevant to STA from the old association AP2 to the new association AP1

Example: IEEE 802.11f on AP Avaya

```
Frame 8706 (87 bytes on wire, 87 bytes captured)
    Ethernet II, Src: 00:02:2d:48:4d:47, Dst:
      01:00:5e:00:01:4c
    Internet Protocol, Src Addr: 172.31.194.21
      (172.31.194.21), Dst Addr: 224.0.1.76 (224.0.1.76)
    User Datagram Protocol, Src Port: 2313 (2313), Dst Port:
      2313 (2313)
    Inter-Access-Point Protocol
        Version: 1
        Type: Announce Request(0)
        Protocol data units
            BSSID(1) Value: 00:02:2d:8a:44:fe
            Capabilities(4) Value: bf (WEP)
            PHY Type(16) Value: DSSS
            Regulatory Domain(17) Value: ETSI (Europe)
            Regulatory Domain(17) Value: Spain
            Radio Channel(18) Value: 7
            Beacon Interval(19) Value: 100 Kus
            Network Name(0) Value: "WILMA\000"
```


Example: IEEE 802.11f on AP Avaya

```
Frame 607 (83 bytes on wire, 83 bytes captured)
    Ethernet II, Src: 00:02:2d:47:4a:c5, Dst:
      01:00:5e:00:01:4c
    Internet Protocol, Src Addr: 172.31.194.25
      (172.31.194.25), Dst Addr: 224.0.1.76 (224.0.1.76)
    User Datagram Protocol, Src Port: 2313 (2313), Dst Port:
      2313 (2313)
    Inter-Access-Point Protocol
        Version: 1
        Type: Announce Request(0)
        Protocol data units
            BSSID(1) Value: 00:20:a6:50:da:ca
            Capabilities(4) Value: 66 (ForwardingWEP)
            PHY Type(16) Value: Unknown
            Regulatory Domain(17) Value: ETSI (Europe)
            Radio Channel(18) Value: 13
            Beacon Interval(19) Value: 100 Kus
            Network Name(0) Value: "WILMA\000"
```


CapWap

capwap basics

- Not alternative to any 802.11 standard/proposal
- Takes a “wide-network (or network-wide?)” perspective w.r.t. the “local-network” perspective of 802
- Indeed, in the end, it is alternative to 802.11f
- Starts providing an interesting classification of different WLAN solutions all supported by 802.11

capwap taxonomy

- AP used as a generic, legacy term
- WTP - Wireless Termination Point: A point of wireless access to the network
  - may or may not implement all APs functionalities
  - if not is also known as “thin-AP”
- AC – Access Controller: centralized point of control if many WTPs are jointly controlled by a back-end unit

capwap functions

- RF monitoring
  - radar detection
  - noise and interference detection
  - measurement.
- RF configuration
  - for retransmission
  - channel selection/assignment
  - transmission power adjustment
- WTP configuration
- WTP firmware loading (e.g. granting network wide consistency)
- Network-wide STA state information
  - information for value-added services
  - mobility and load balancing.
  - ...
- Mutual authentication between network entities

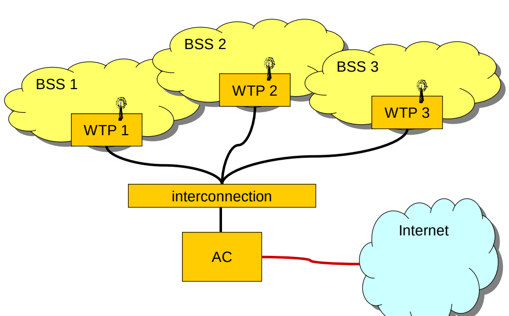
WLAN arch: autonomous

- Traditional WLAN architecture (a WTP is an AP as we know and use every day)
- Each WTP is a single physical device
- Implements all the 802.11 services,
- Configured and controlled individually
- Can be monitored and managed via typical network management protocols like SNMP
- Such WTPs are sometimes referred to as "Fat APs" or "Standalone APs"

capwap WLAN arch: centralized

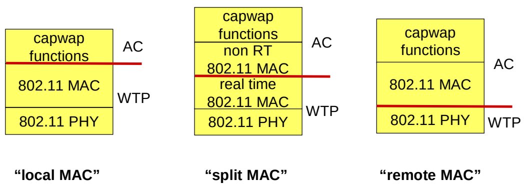
- Hierarchical architecture
- One or more Access Controllers (ACs) manage a large number of WTPs
- AC can be the aggregation point for the data plane
- AC is often co- located with an L2 bridge (Access Bridge), a switch, or an L3 router (Access Router)
- Much better manageability for large scale networks
- IEEE 802.11 functions and CAPWAP control functions are provided by the WTP devices and the AC together
- The WTPs may no longer fully implement 802.11 functions
- WTPs are sometimes called “light weight” or “thin APs”

capwap WLAN arch: centralized



capwap centralized: protocol view

- Interconnection can be L3, L2 or even direct physical connection
- AC can be distributed over several physical devices
- Can support 3 different protocol architectures



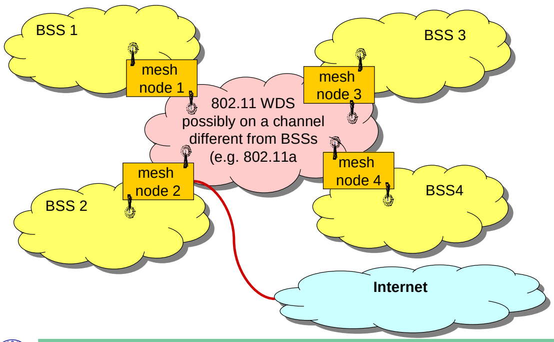
capwap centralized: AC-WTP Interface

- Discovery: The WTPs discover the AC with which they will be bound to and controlled by
- Authentication: WTPs must authenticate with AC (and possibly vice-versa)
- WTP Association: WTP registers with the AC
- Firmware Download: WTP pull or AC push the WTPs firmware
- Control Channel Establishment: The WTP establishes an IP- tunnel with the AC
- Configuration Download: AC push configuration parameters to the WTP

capwap WLAN arch: distributed

- Wireless nodes can form a distributed network among themselves, via wired or wireless media
- A wireless mesh network is one example
- Some of these nodes may have wired Ethernet connections acting as gateways to the external network
- Mesh Networks are a "chapter" by themselves in our course, due to the interesting applications and routing problems

capwap WLAN arch: distributed



capwap WLAN arch: distributed

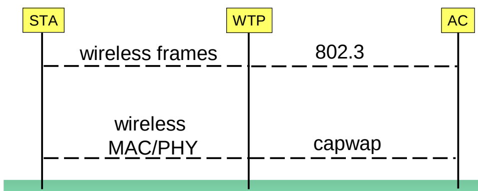
- APs or mesh nodes are peers
- No centralized management
- Service support model??
- Interesting IAPP protocol issues and interesting distributed algorithms issues
- Wireless Meshes
  - Can solve problems of remote area coverage
  - Can extend, improve, make resilient Internet Access

Capwap Protocol (1)

- Conceived for the centralized architecture
  - "local" and "split" MAC only
- Runs on top of IP
  - independent from radio technology
  - "bindings" required for technology mapping
- Deals with both Data and Control communications
  - WTP are not independent
  - All traffic is centralized on the AC

Capwap Protocol (2)

- Its definition for 802.11 includes STAs, though they don't need to implement capwap
- Wireless frames are managed by the AC
  - Local MAC implied bridging at WTP
  - Split MAC details still undefined

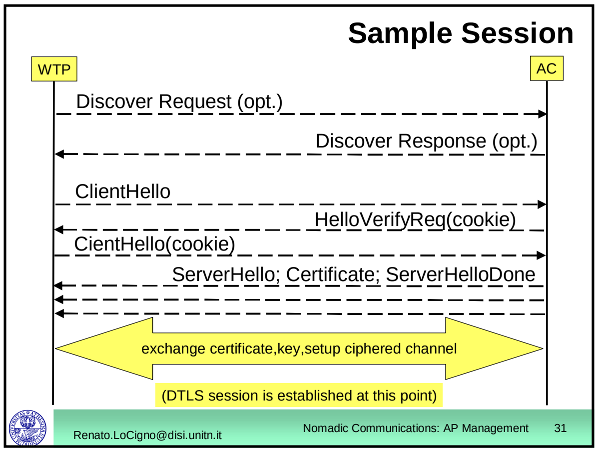


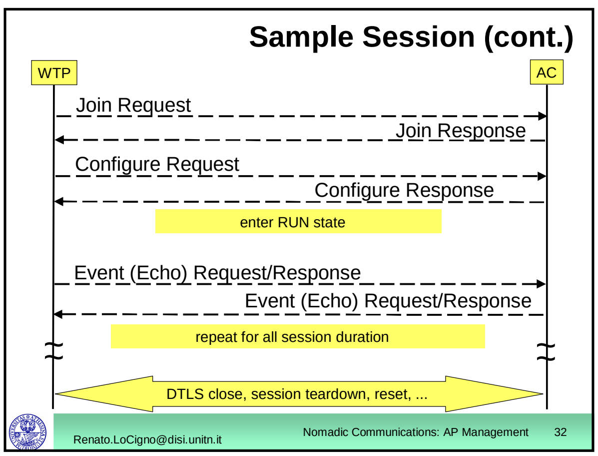
Capwap Protocol Goals

- Centralize authentication and policy enforcement
  - AC does bridging, forwarding, encryption
  - Reduced costs for WTP and higher efficiency
  - WTP can be easily substituted for technology improvements
- Relieve WTP from higher protocol processing
  - Light, low cost WTPs
- Define a generic encapsulation and transport mechanism independent from technology
  - can be applied to 802.15, 802.16, etc.

Capwap Transport

- UDP-like encapsulation
- Builds on top of DTLS (Datagram Transport Layer Security)
  - Not yet widely deployed
  - Cryptographic layer for connectionless services
- Establish a session on WTP connection to the AC
  - Authentication
  - Connection
  - Operation (indefinite, until the WTP is on)


Sample Session
WTP
AC
Discover Request (opt.)
Discover Response (opt.)
ClientHello
HelloVerifyReq(cookie)
CientHello(cookie)
ServerHello; Certificate; ServerHelloDone
exchange certificate,key,setup ciphered channel
(DTLS session is established at this point)
Renato.LoCigno@disi.unitn.it
Nomadic Communications: AP Management
31


Sample Session (cont.)
WTP
AC
Join Request
Join Response
Configure Request
Configure Response
enter RUN state
Event (Echo) Request/Response
Event (Echo) Request/Response
repeat for all session duration
DTLS close, session teardown, reset, ...
Renato.LoCigno@disi.unitn.it
Nomadic Communications: AP Management
32