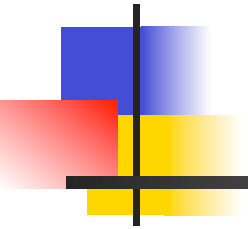
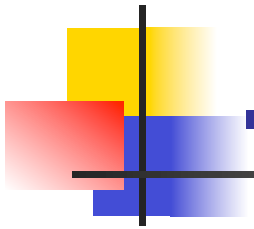


AP Management and Handover support (CAPWAP - 802.11f)

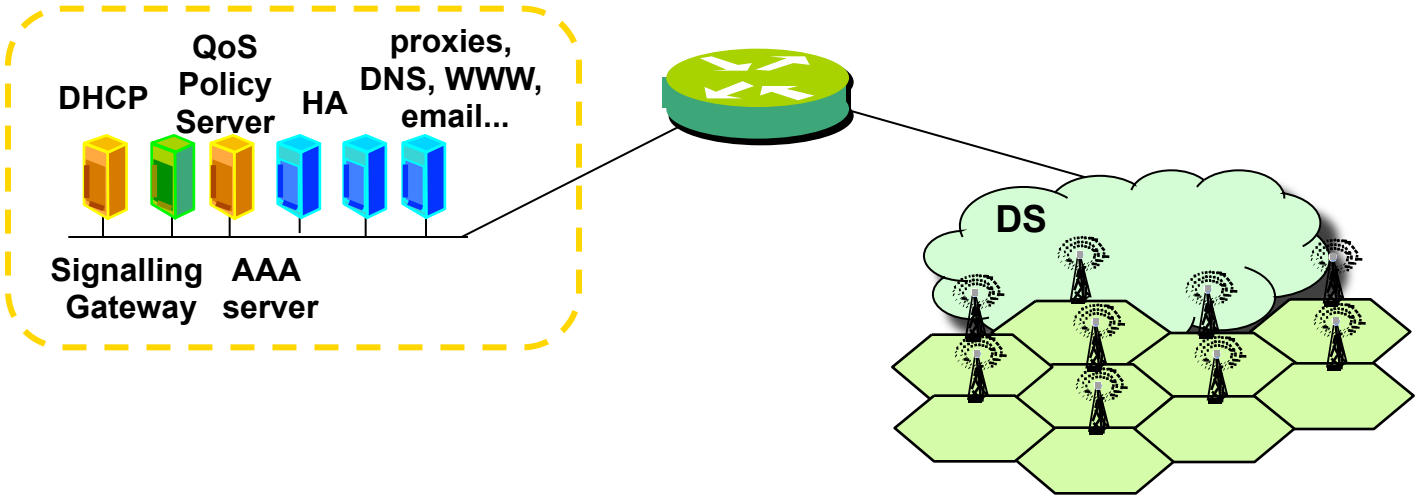
Renato Lo Cigno
http://disi.unitn.it/locigno/index.php/teaching-duties/nomadic-communications



...Copyright

ESS and Micro-mobility

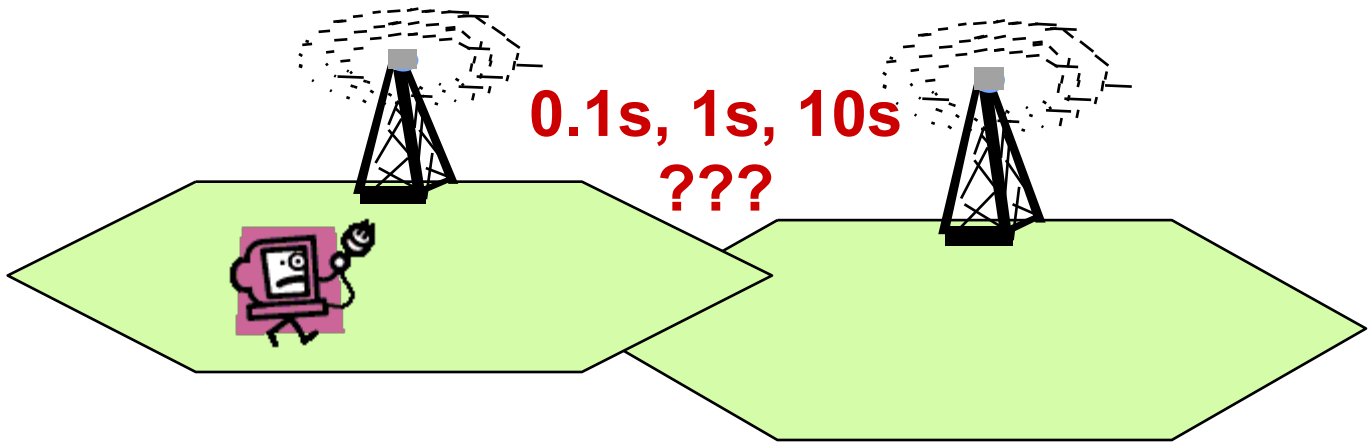
- A collection of coordinated IBSS forms an ESS
- The APs in the same ISS can broadcast the same SSID



- 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?

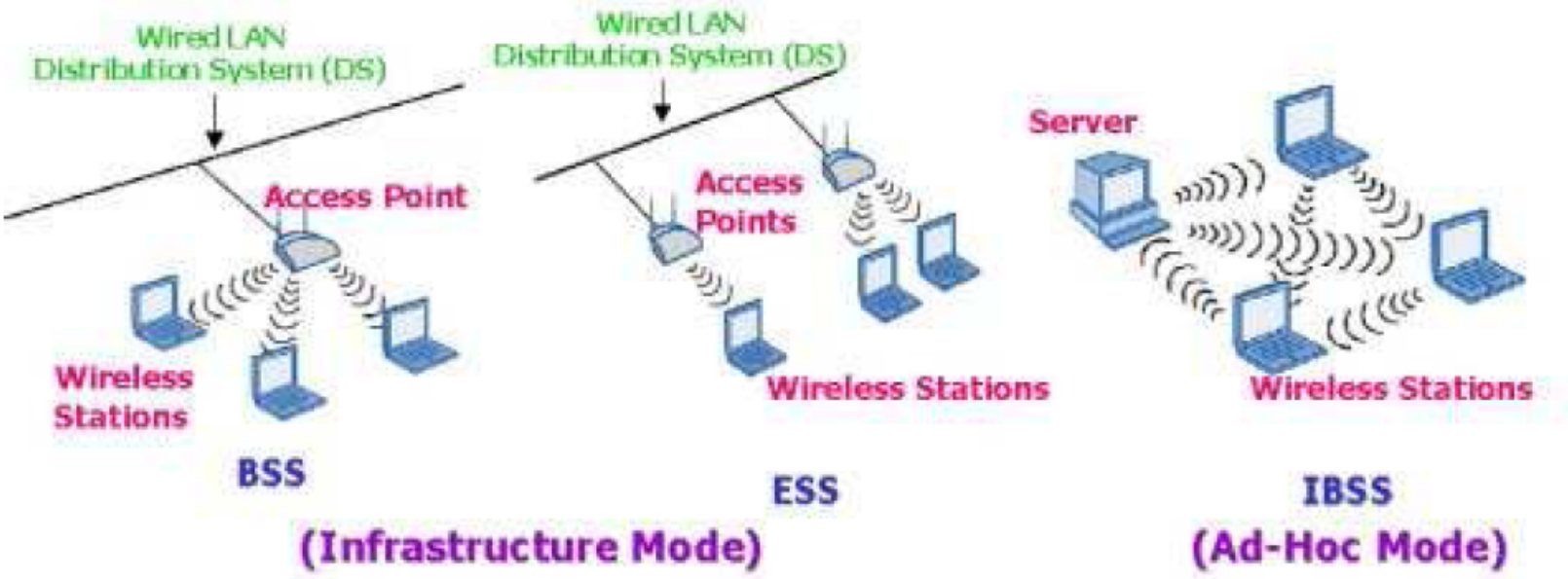
IEEE vs. IETF

- 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), (RFCs 4118, 4564, 4565, 5415 and others), omni-comprehensive, not focused on handovers
- Proprietary solutions based on CAPWAP (Cisco, Juniper, ...)

802.11f

Scope & Goals

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



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

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

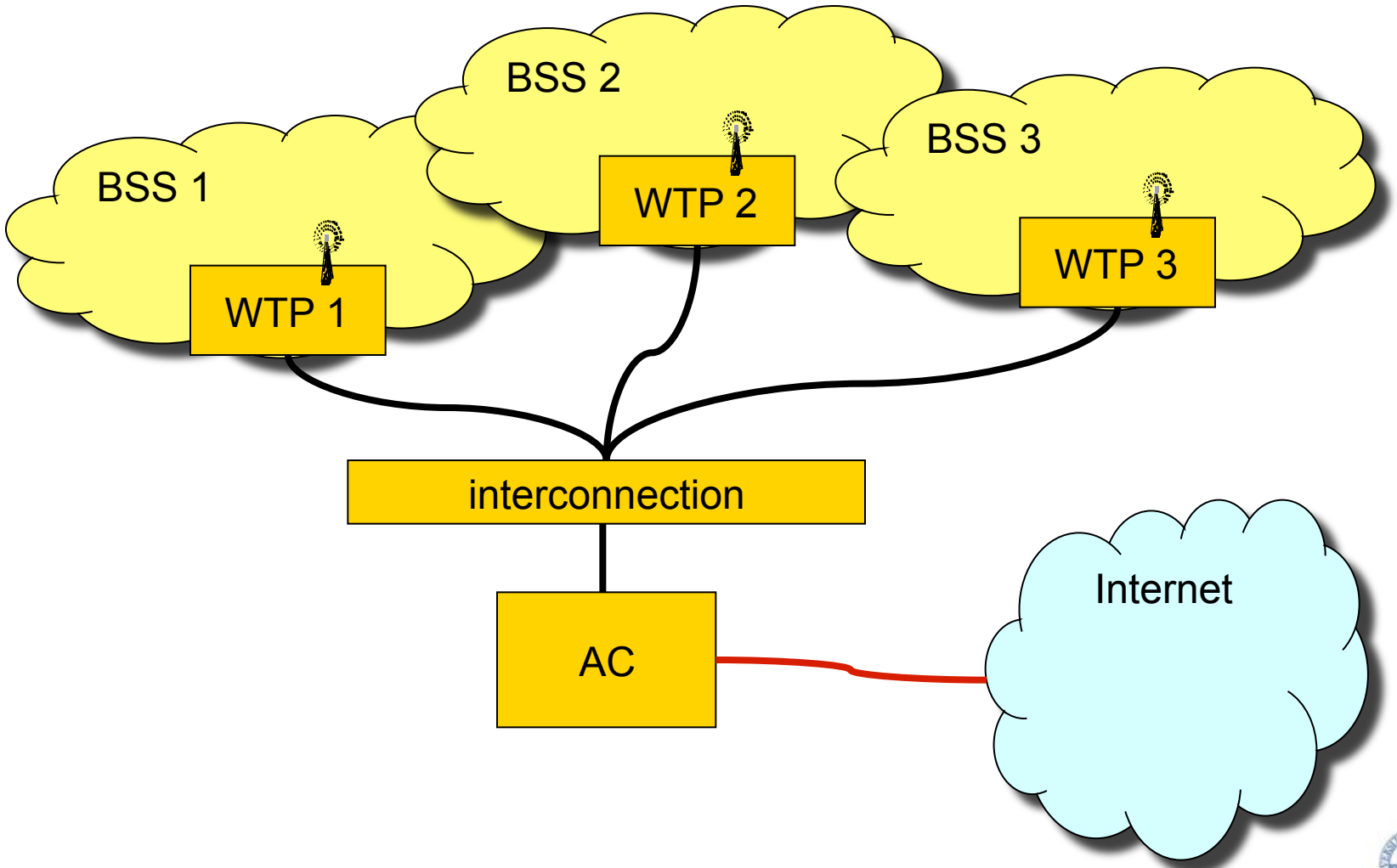
WLAN arch: autonomous

- 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

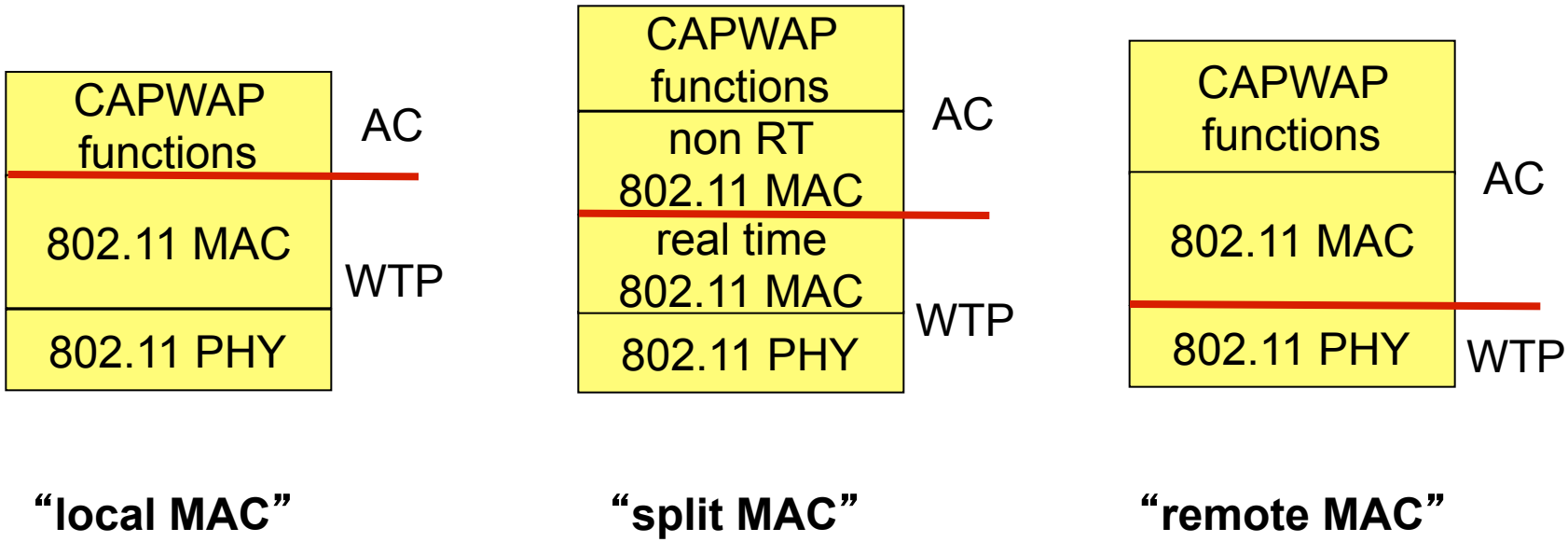
- Hierarchical architecture
- One or more Access Controllers (ACs) manage a large number of WTPs
- AC can be the aggregation point for the data plane
- AC is often co- located with an L2 bridge (Access Bridge), a switch, or an L3 router (Access Router)
- Much better manageability for large scale networks
- 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



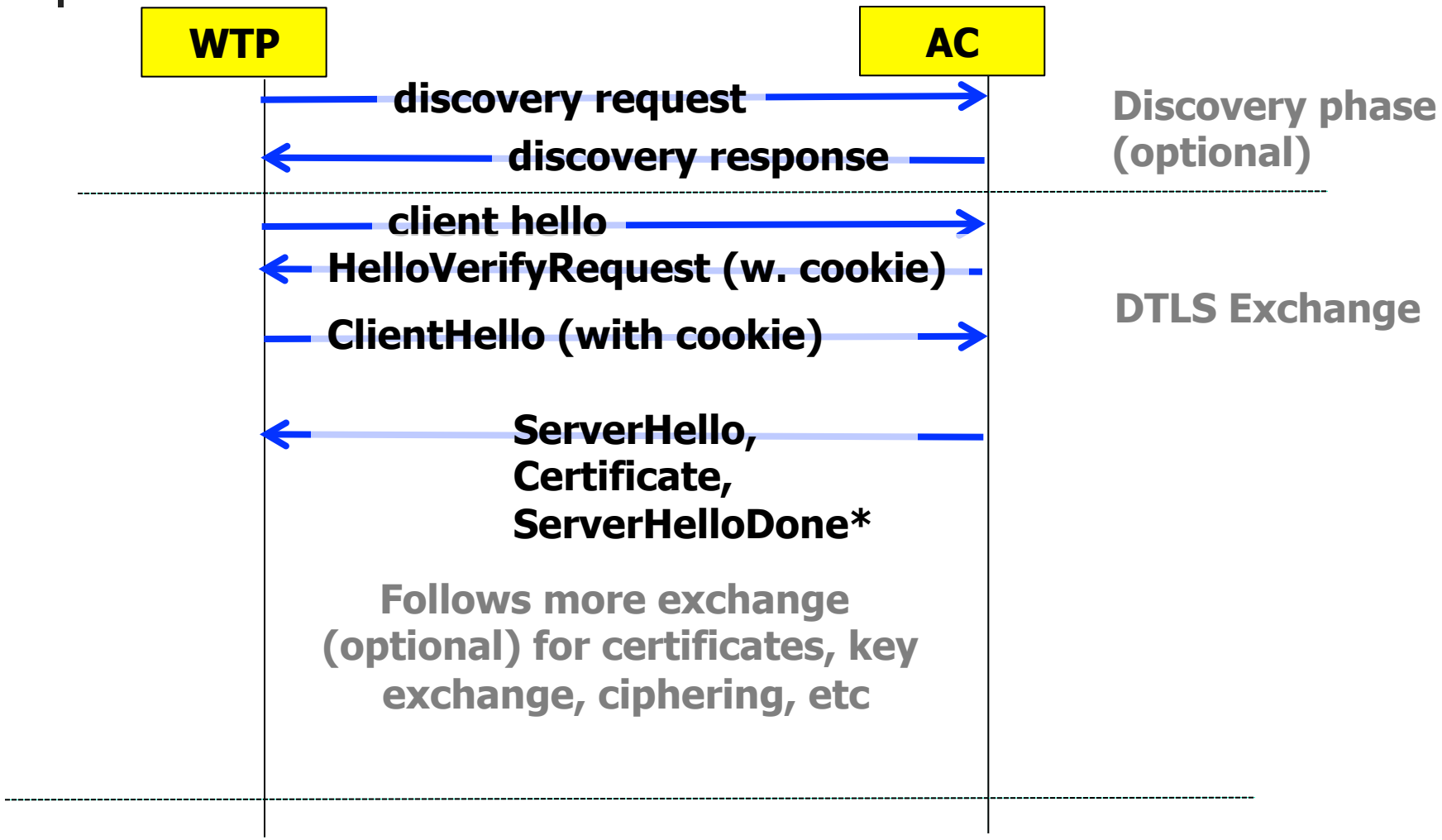
CAPWAP centralized: AC-WTP Interface

- 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 implementations

- Mostly based on the local MAC model
- Tailored for 802.11
- Not-so-much standard, as so far it is not easy to find interoperable devices
- Use DTLS for tunneling, including traffic, which generates high overheads in some configurations
- DTLS is not much implemented, and this makes it already not-so-standard
  - Fundamental if the back-haul is wireless to protect data
- WTPs and AC follow a dialogue split between "initialization" and "run"

CAPWAP initialization



CAPWAP initialization (cont.)