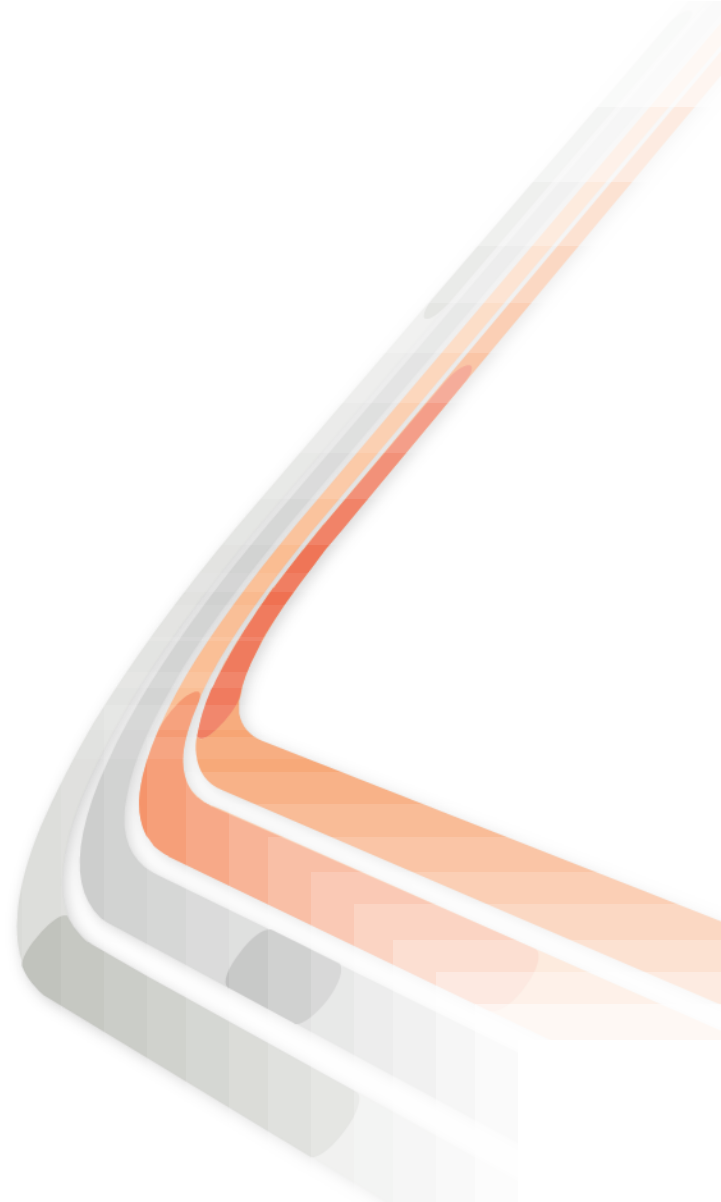




Secure Mobility in Cisco Unified WLAN Networks

BRKEWN-2018

Follow us on Twitter for real time updates of the event:
@ciscoliveeurope, #CLEUR



Housekeeping

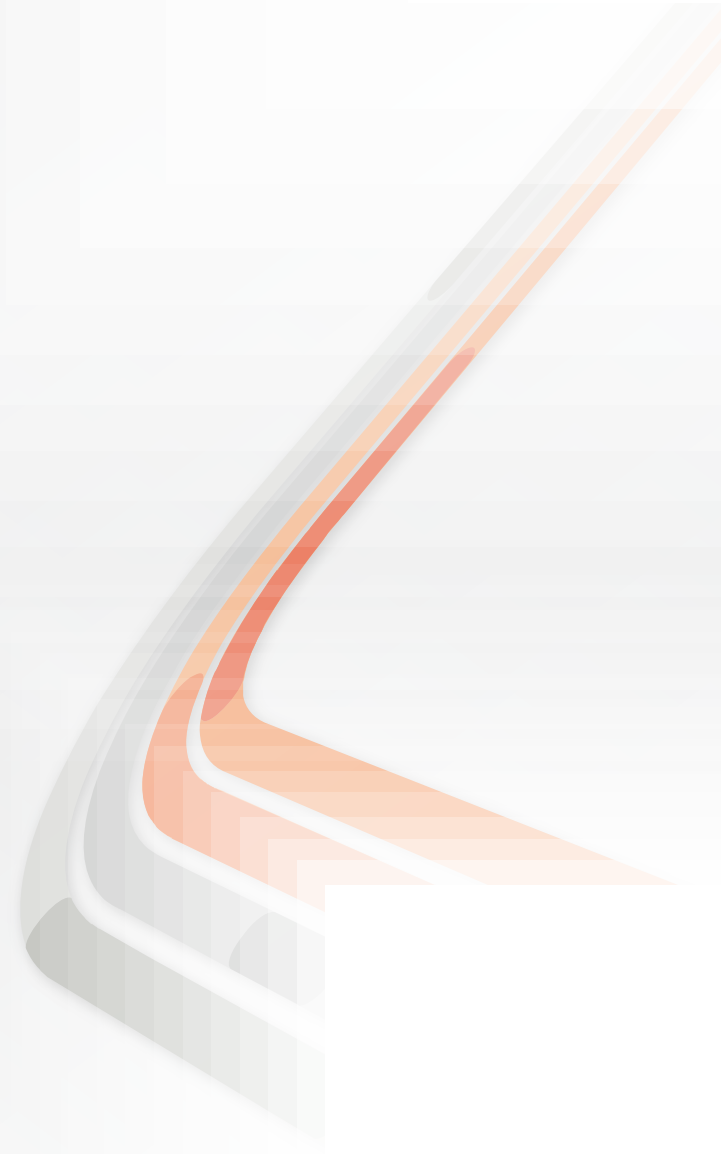
- We value your feedback- don't forget to complete your online session evaluations after each session & the Overall Conference Evaluation which will be available online from Thursday
- Visit the World of Solutions and Meet the Engineer
- Visit the Cisco Store to purchase your recommended readings
- Please switch off your mobile phones
- After the event don't forget to visit Cisco Live Virtual:
www.ciscolivevirtual.com
- Follow us on Twitter for real time updates of the event:
@ciscoliveeurope, #CLEUR

Session Agenda

- Anatomy of a Device Connection
- Anatomy of a Device Roam
- Design and Deployment Considerations

Learn. Connect.
Collaborate. *together.*

Anatomy of a Device Connection

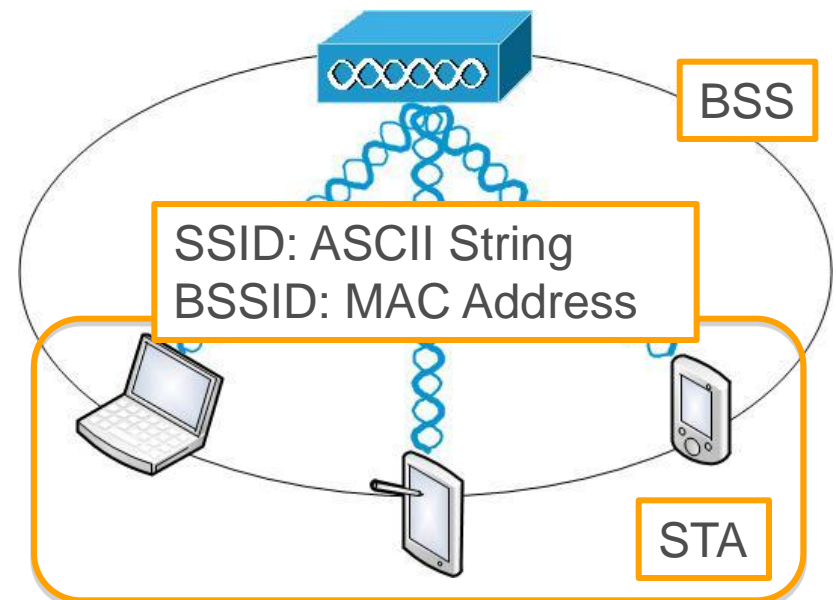
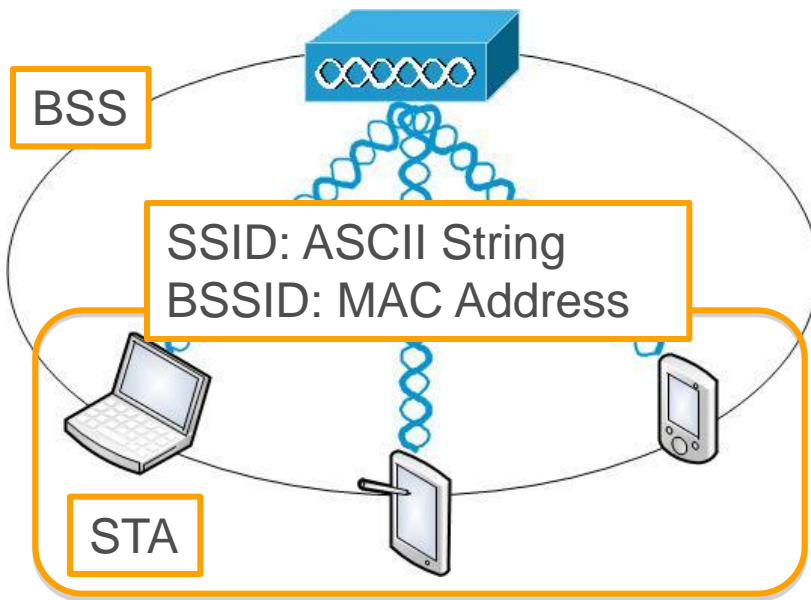


Section Agenda

- 802.11 Architecture and Services Basics
- 802.11i Addendum
- EAP Types and Key Management
- Device Mobility Problem Statement

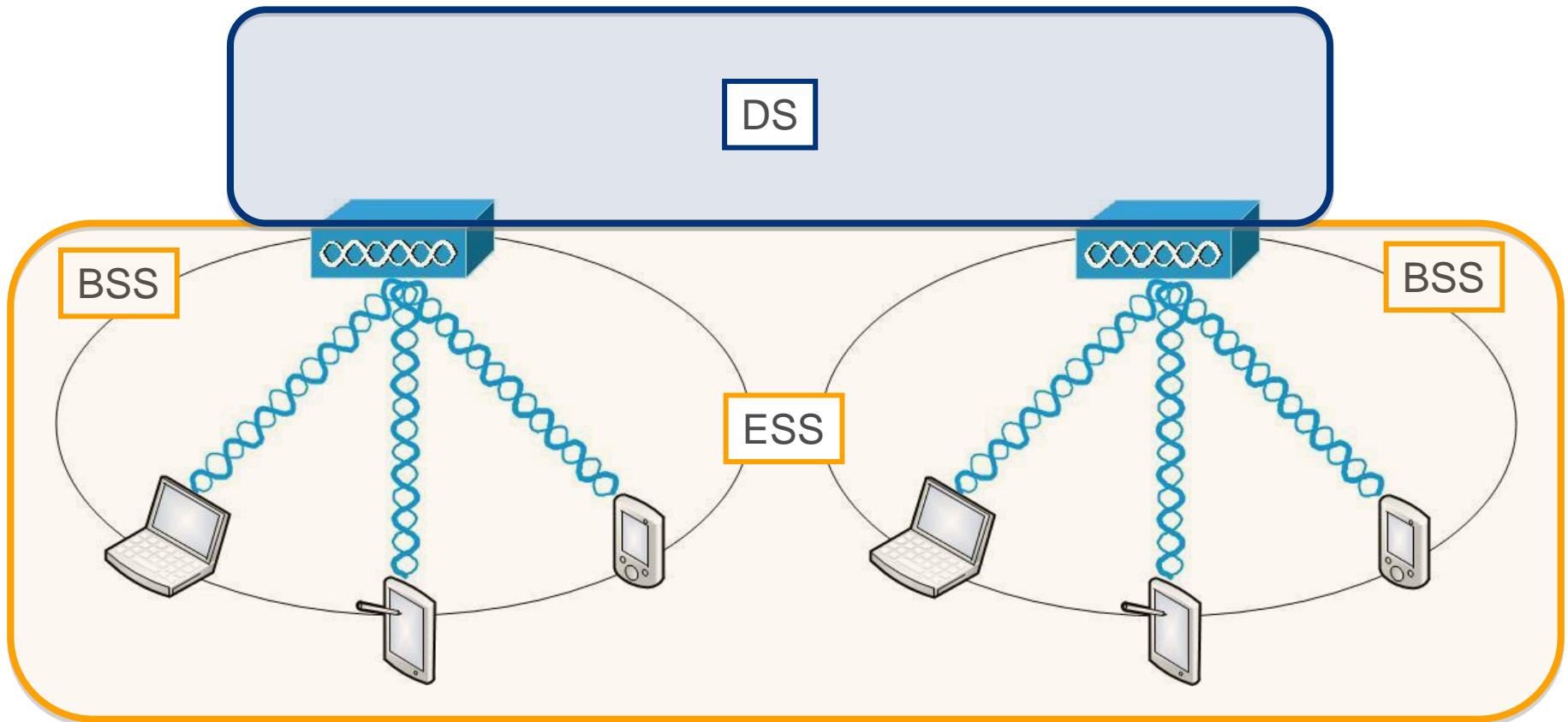
802.11 Architecture Basics

- BSS – Basic Service Set
- SSID – Service Set Identifier
- BSSID – Basic Service Set Identifier
- STA – Station (AKA Client)



802.11 Architecture Basics

- ESS – Extended Service Set
- DS – Distribution System



802.11 Services

Service	Description	Implementation
Distribution Services		
STA Services		

802.11 Services

Service	Description	Implementation
Distribution Services		
Association		
Reassociation		
Disassociation		
STA Services		

802.11 Services

Service	Description	Implementation
Distribution Services		
Association	Used to create a logical connection between a mobile STA and an AP	802.11
Reassociation		
Disassociation		
STA Services		

802.11 Services

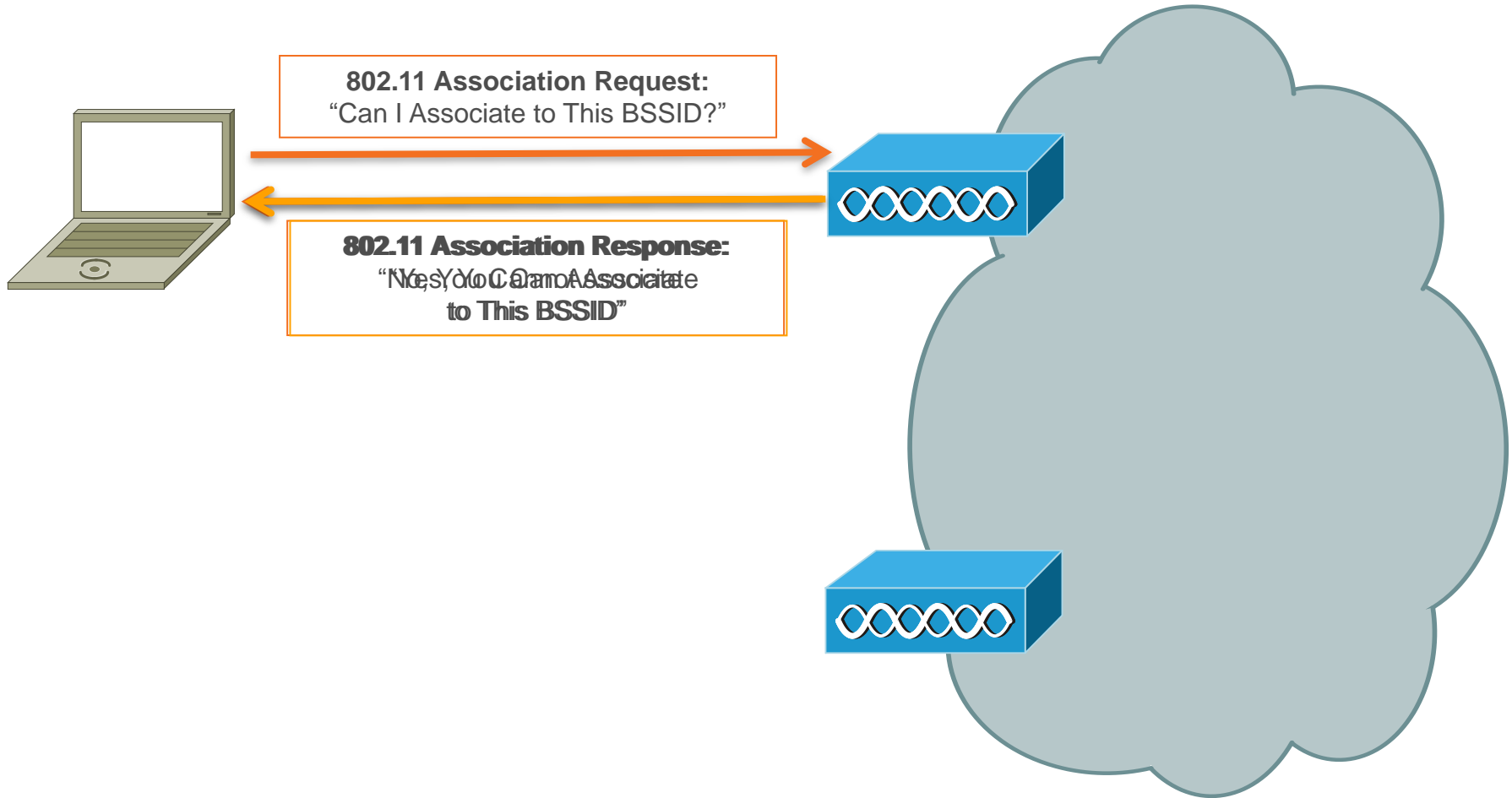
Service	Description	Implementation
Distribution Services		
Association	Used to create a logical connection between a mobile STA and an AP	802.11
Reassociation	Similar to association service, except information about a mobile STA's previous AP may be included; used as a STA moves across an ESS	802.11
Disassociation		
STA Services		

802.11 Services

Service	Description	Implementation
Distribution Services		
Association	Used to create a logical connection between a mobile STA and an AP	802.11
Reassociation	Similar to association service, except information about a mobile STA's previous AP may be included; used as a STA moves across an ESS	802.11
Disassociation	Used by AP to force mobile STA off the BSS or by mobile STA to inform AP it doesn't need service anymore	802.11
STA Services		

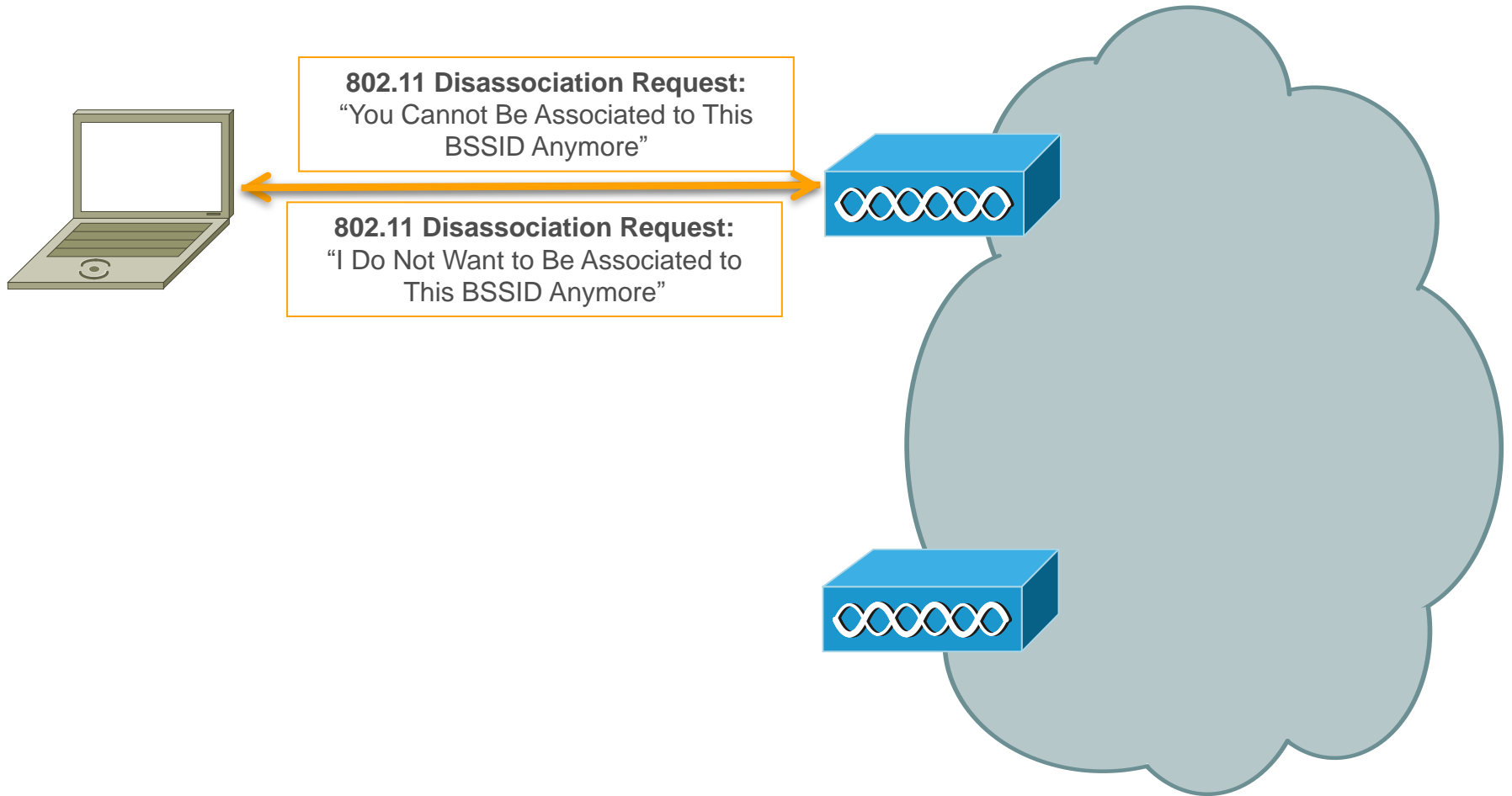
802.11 Distribution Services

Association Service



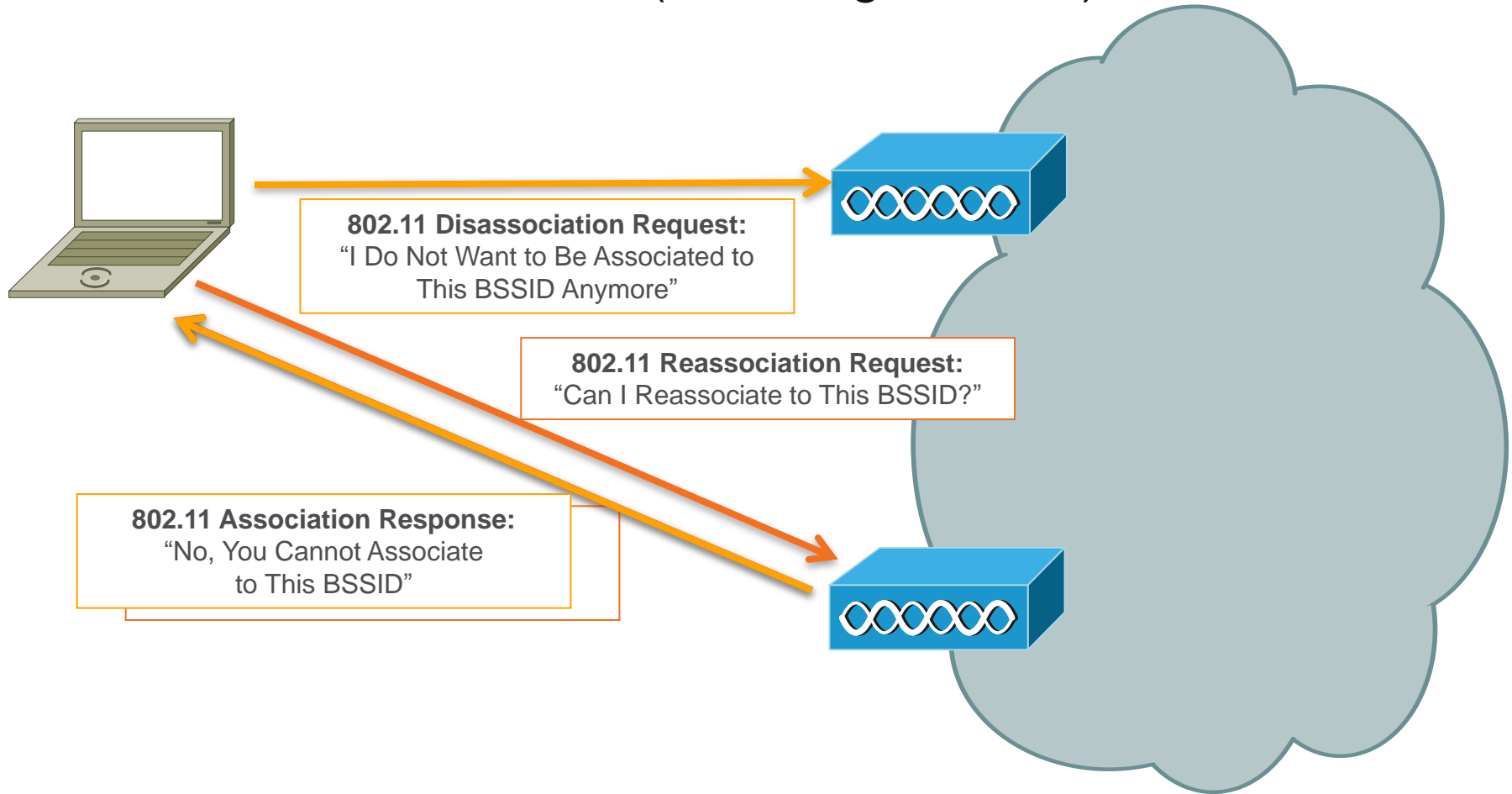
802.11 Distribution Services

Disassociation Service



802.11 Distribution Services

Reassociation Service (Roaming Context)



802.11 Services

Service	Description	Implementation
Distribution Services		
Association	Used to create a logical connection between a mobile STA and an AP	802.11
Reassociation	Similar to association service, except information about a mobile STA's previous AP may be included; used as a STA moves across an ESS	802.11
Disassociation	Used by AP to force mobile STA off the BSS or by mobile STA to inform AP it doesn't need service anymore	802.11
STA Services		

So, What Do These Three Services Accomplish?

What's Missing?

802.11 Services

Service	Description	Implementation
Distribution Services		
Association	Used to create a logical connection between a mobile STA and an AP	802.11
Reassociation	Similar to association service, except information about a mobile STA's previous AP may be included; used as a STA moves across an ESS	802.11
Disassociation	Used by AP to force mobile STA off the BSS or by mobile STA to inform AP it doesn't need service anymore	802.11
STA Services		
Authentication	Used to prove the identity of the STA and AP	WPA/WPAv2 (802.11I), CAPWAP
Deauthentication	Used to eliminate a previously authenticated user from further use of the network	
Privacy	Used to protect frames in transit over wireless medium	

How STAs Connect to a WLAN Securely

STA Services

- 802.11 spec defines authentication, deauthentication, and privacy services, but...
- 802.11 spec provides extremely weak (useless for 2011 requirements) mechanisms for these services:
 - Authentication/Deauthentication: Shared-Key Auth
 - Privacy: Wired Equivalent Privacy (WEP)
- 802.11i addendum adds strong(er) mechanisms for implementing STA security-related services:
 - Authentication/Deauthentication: PSK, 802.1X/EAP
 - Privacy: TKIP & CCMP

WPA/WPA2

WPA

- A snapshot of the 802.11i Standard
- Commonly used with TKIP encryption

WPA2

- Final version of 802.11i
- Commonly used with AES encryption

Authentication Mechanisms

- Personal (PSK) – Home Use
- Enterprise (802.1X/EAP) – Office Use

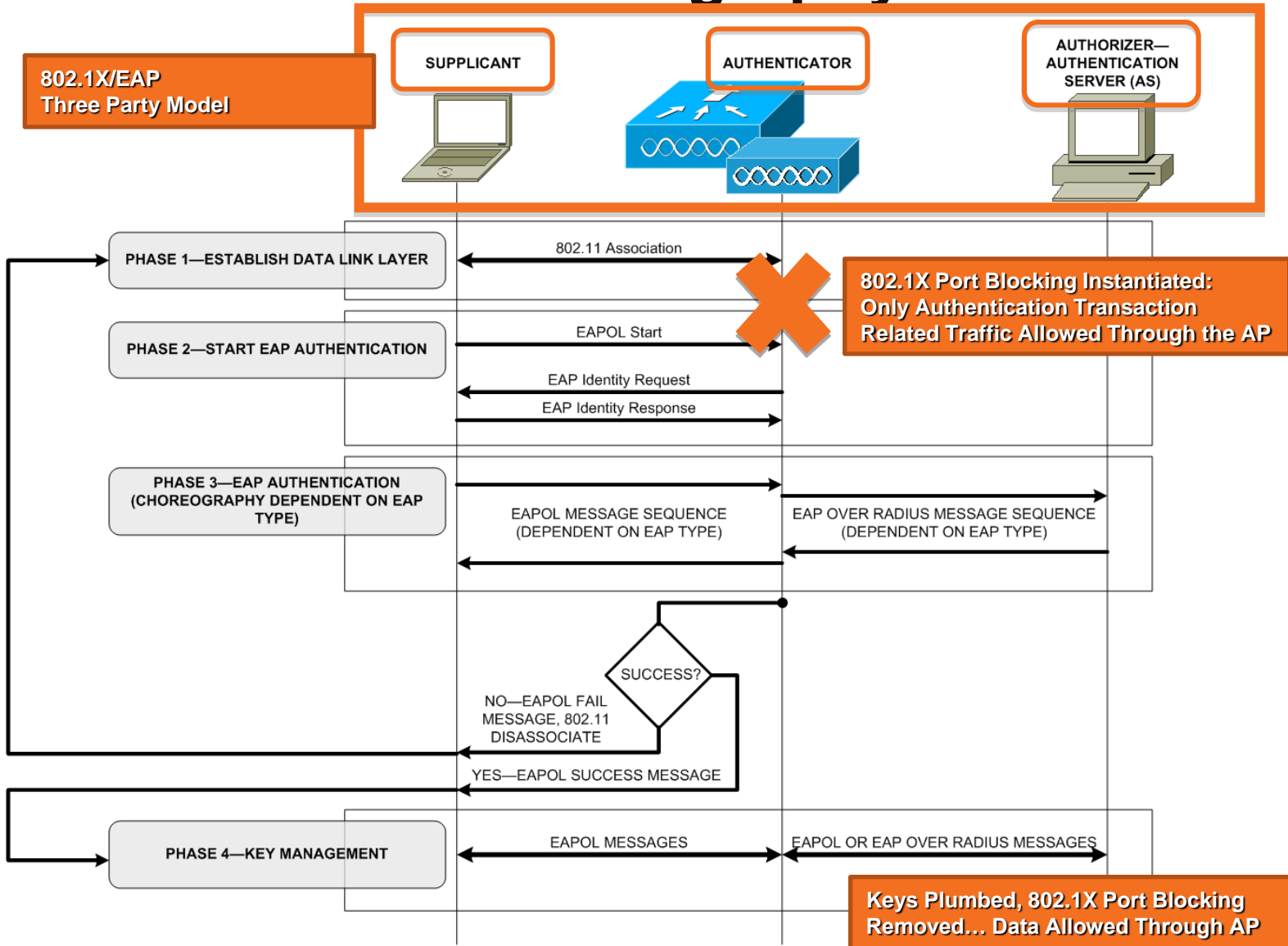
Authentication Best Practices:

WPA2-Enterprise

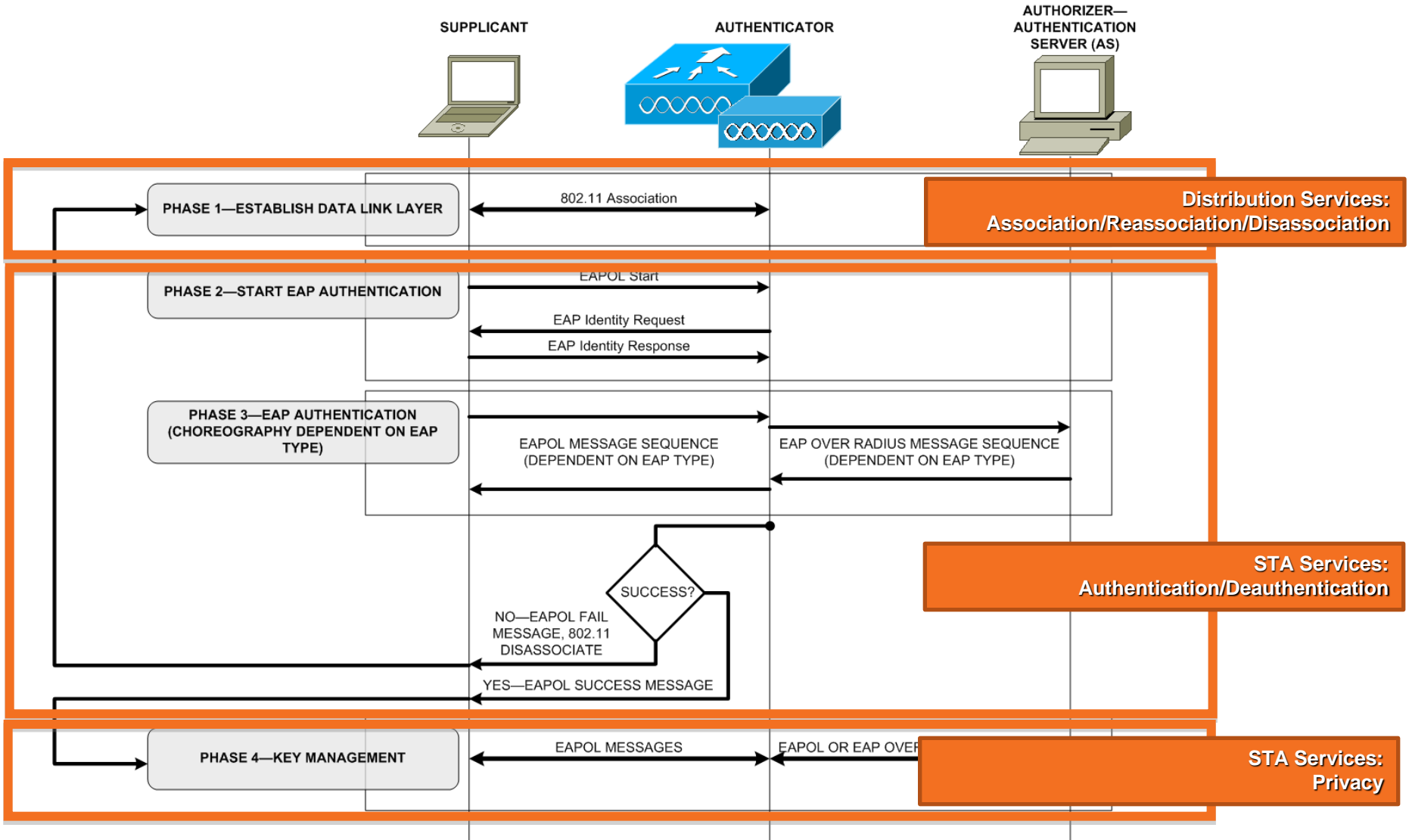
Strong Authentication

- Extensible Authentication Protocol (EAP)
- Outside Methods (Protective Tunnel):
 - PEAP
 - EAP-FAST
 - TLS
- Inside Methods (Authentication Credentials):
 - EAP-MSCHAPv2
 - EAP-GTC

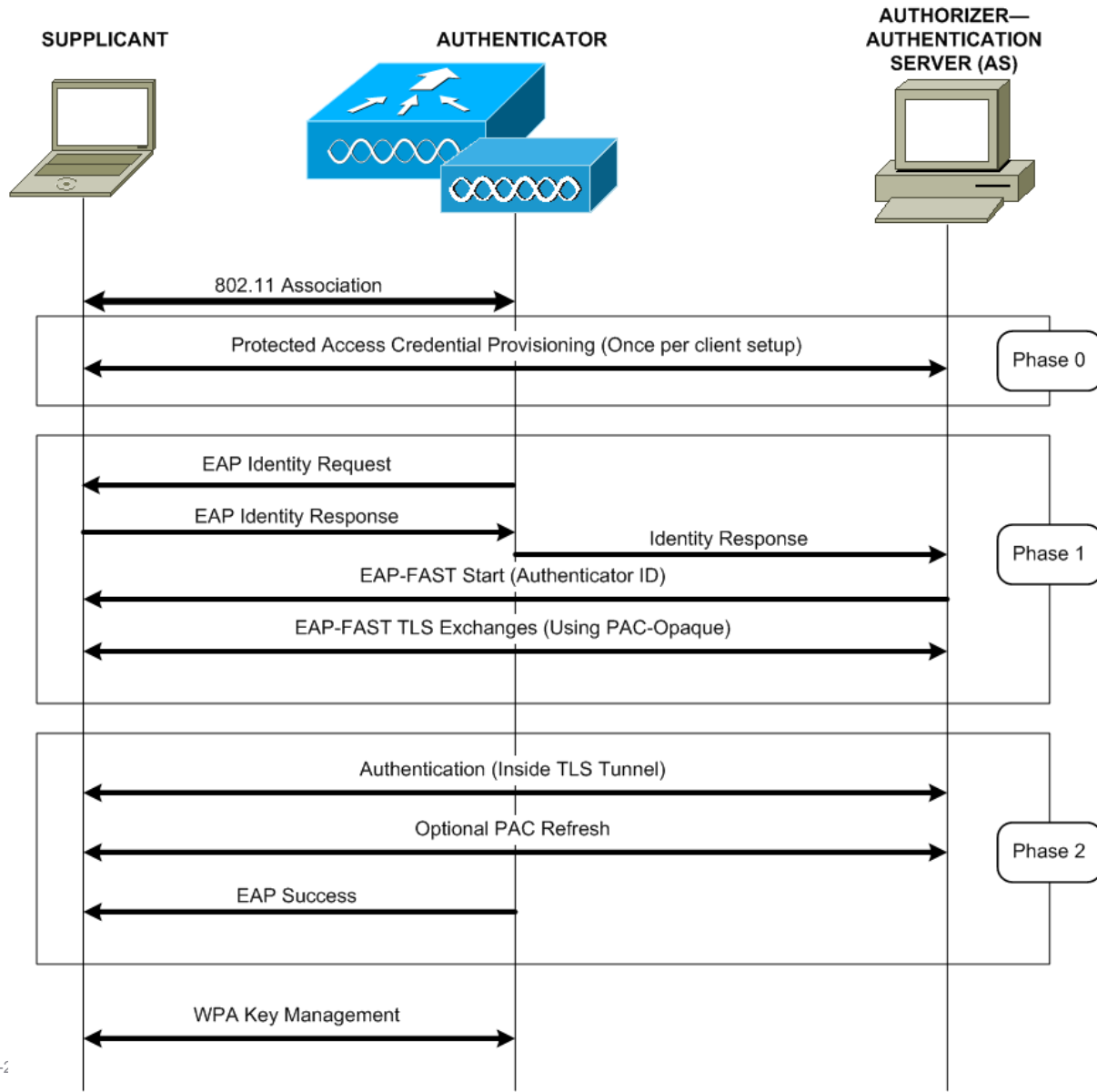
802.1X/EAP Choreography



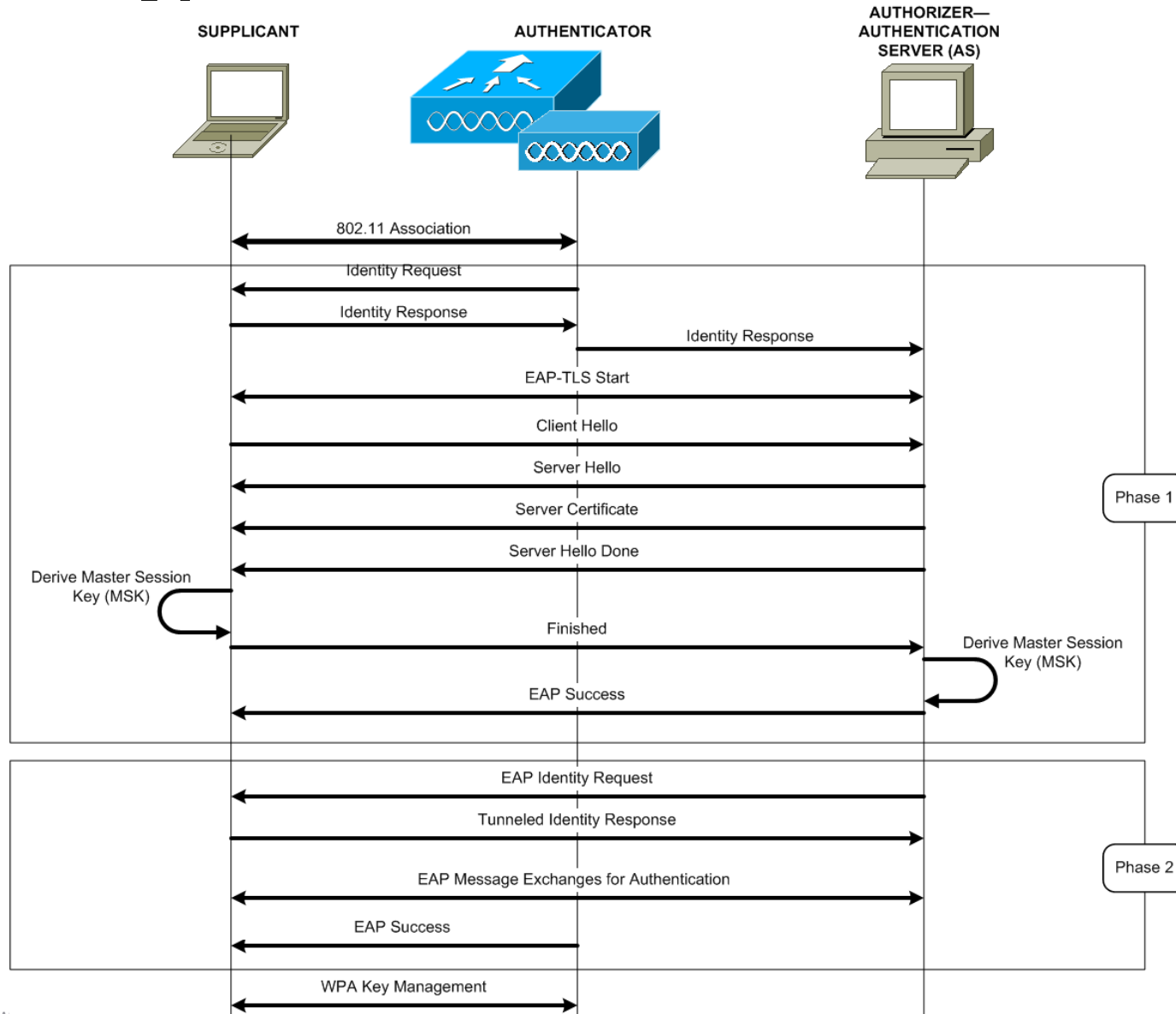
802.1X/EAP Choreography



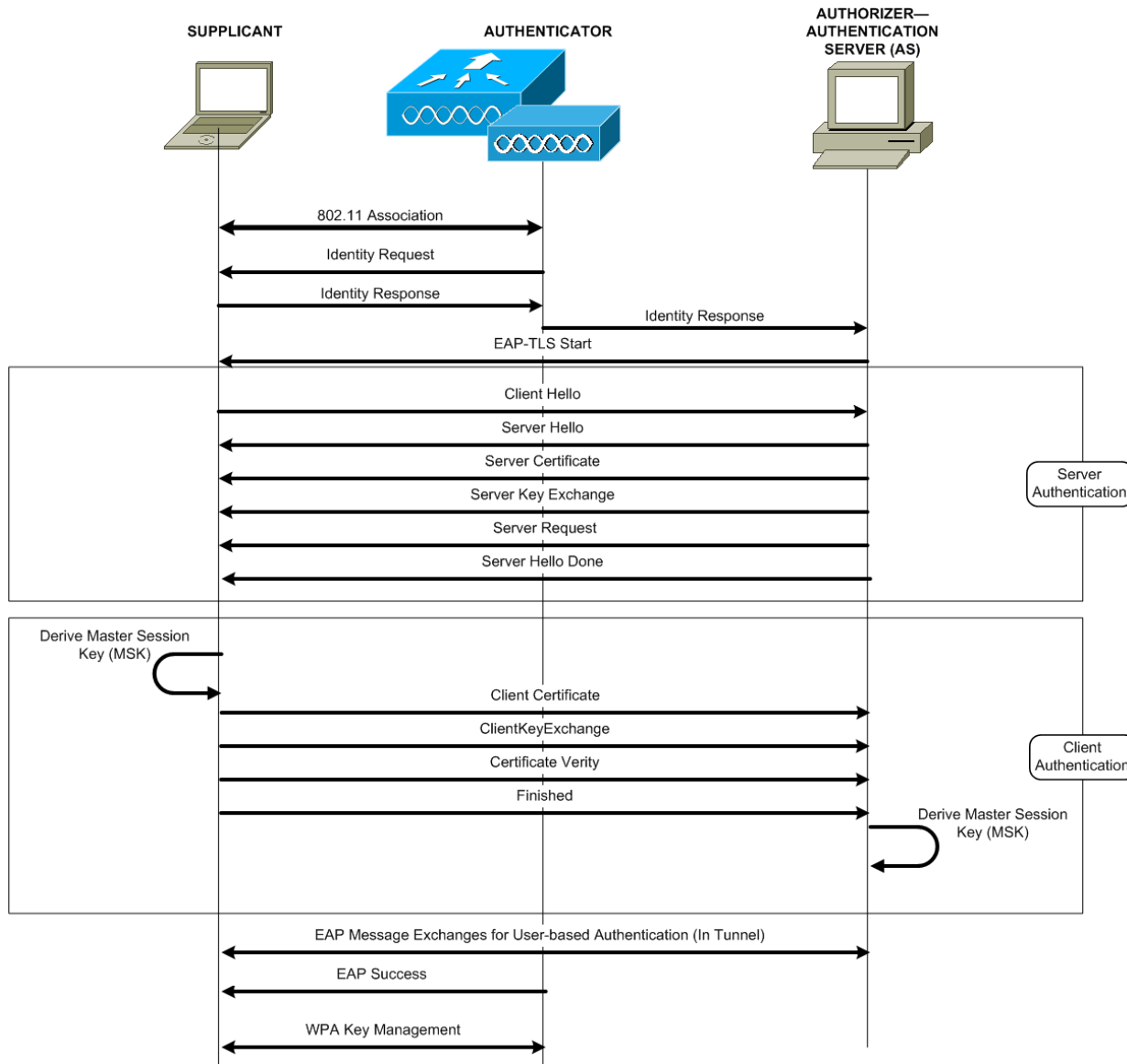
EAP Types: EAP-FAST



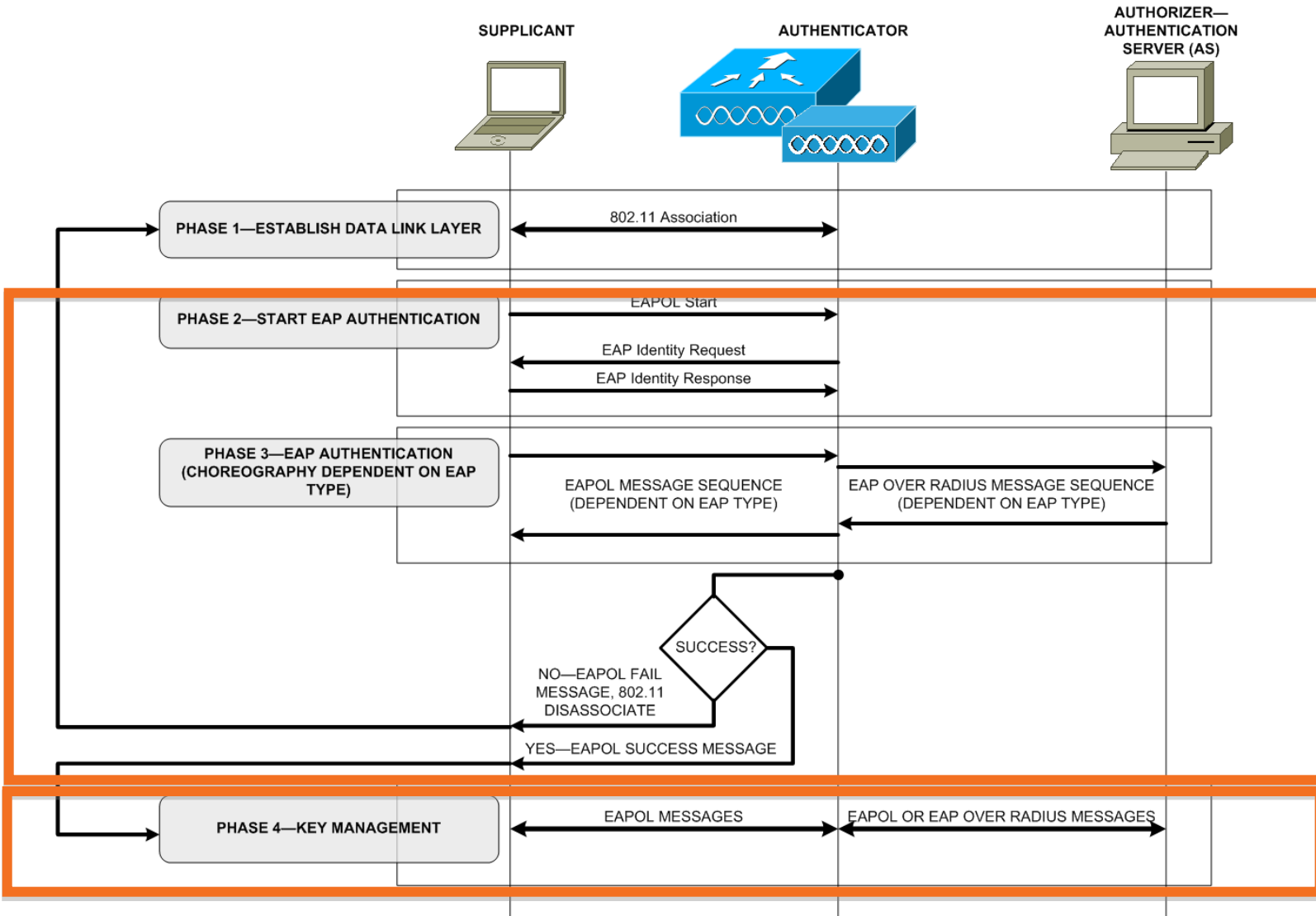
EAP Types: PEAP



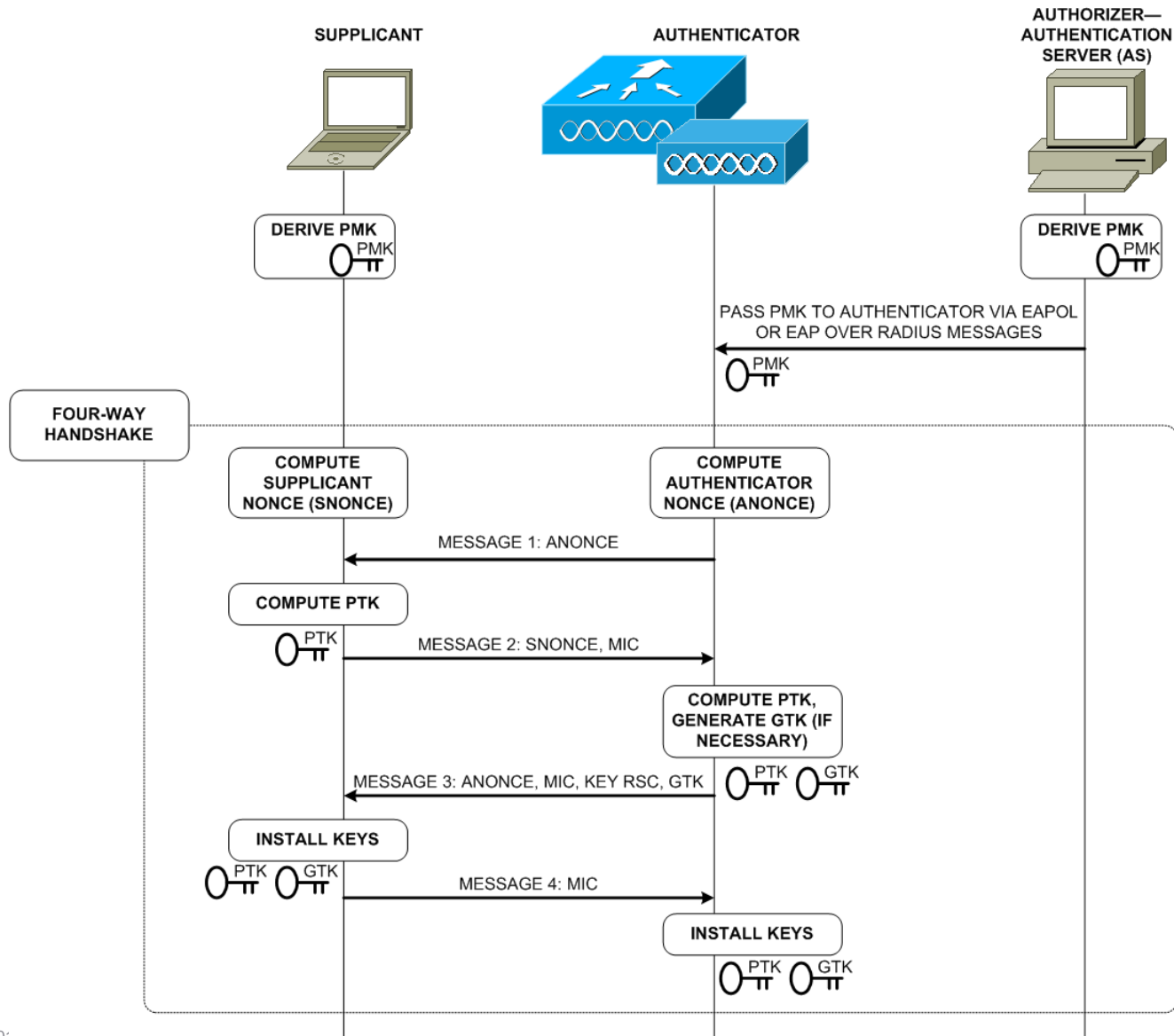
EAP Types: EAP-TLS



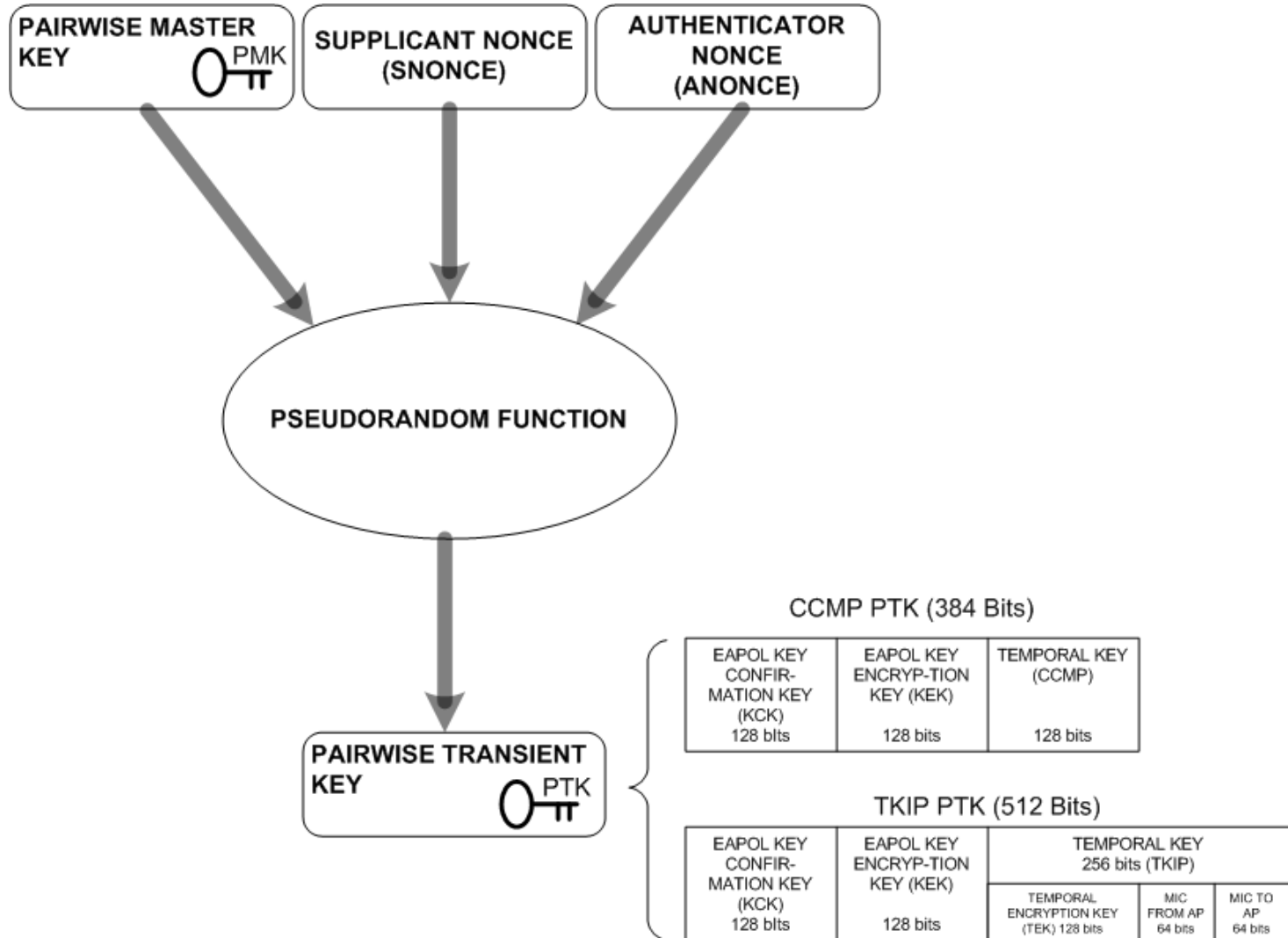
802.1X/EAP Choreography



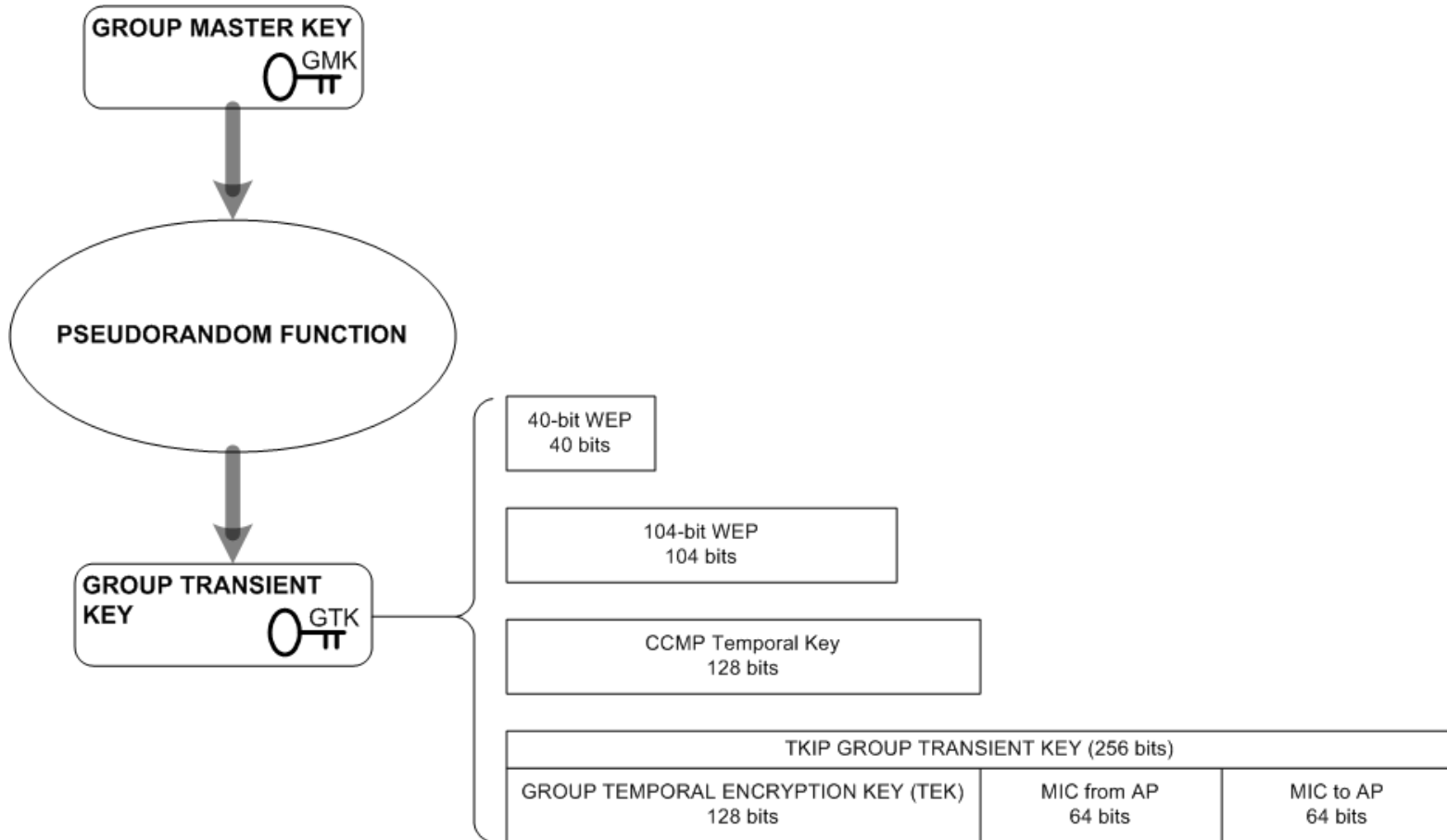
Key Management – Four-Way Handshake



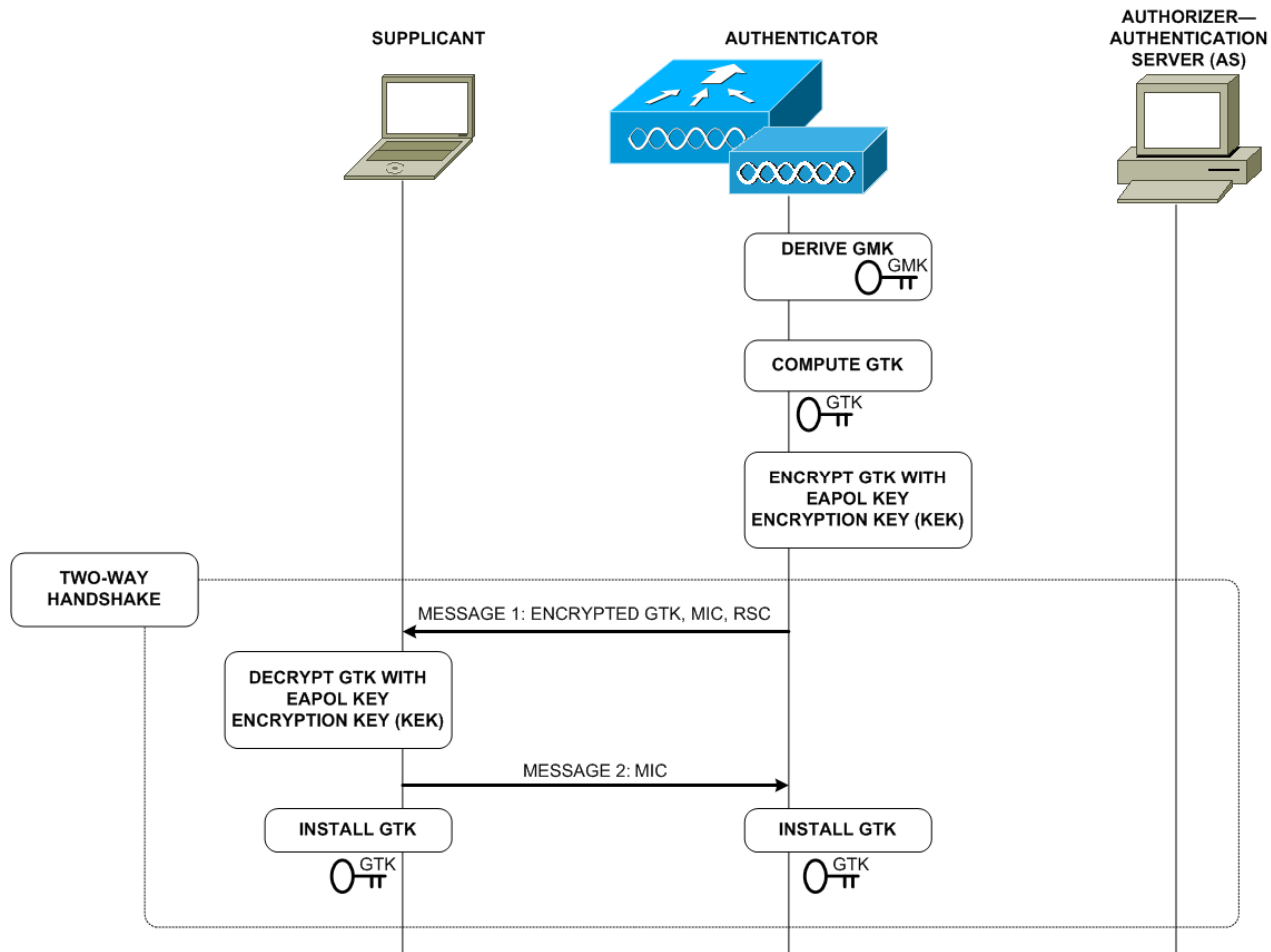
Key Management – Pairwise Transient Key (PTK)



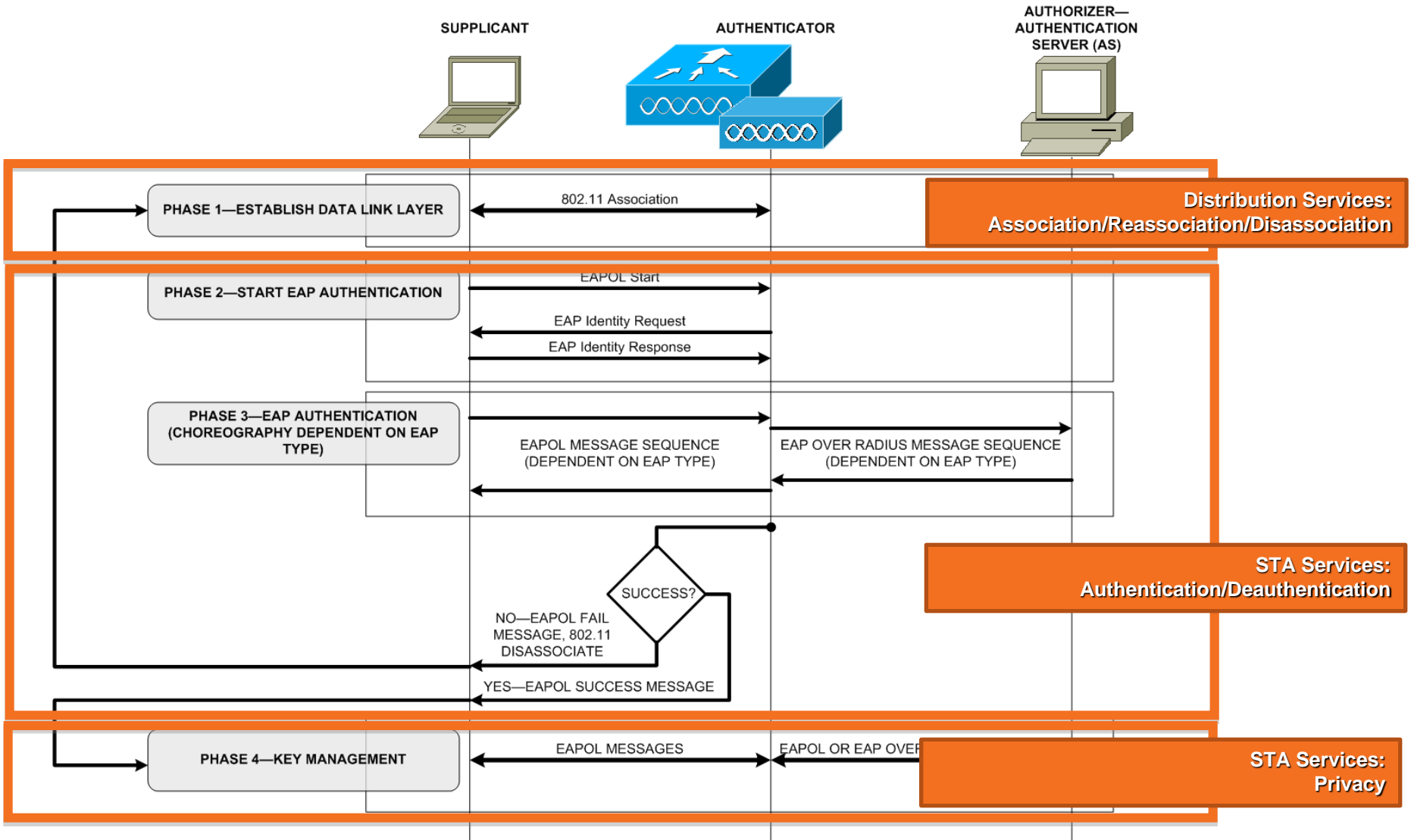
Key Management – Group Transient Key (GTK)



Key Management – GTK Distribution



802.1X/EAP Choreography



802.11 Services

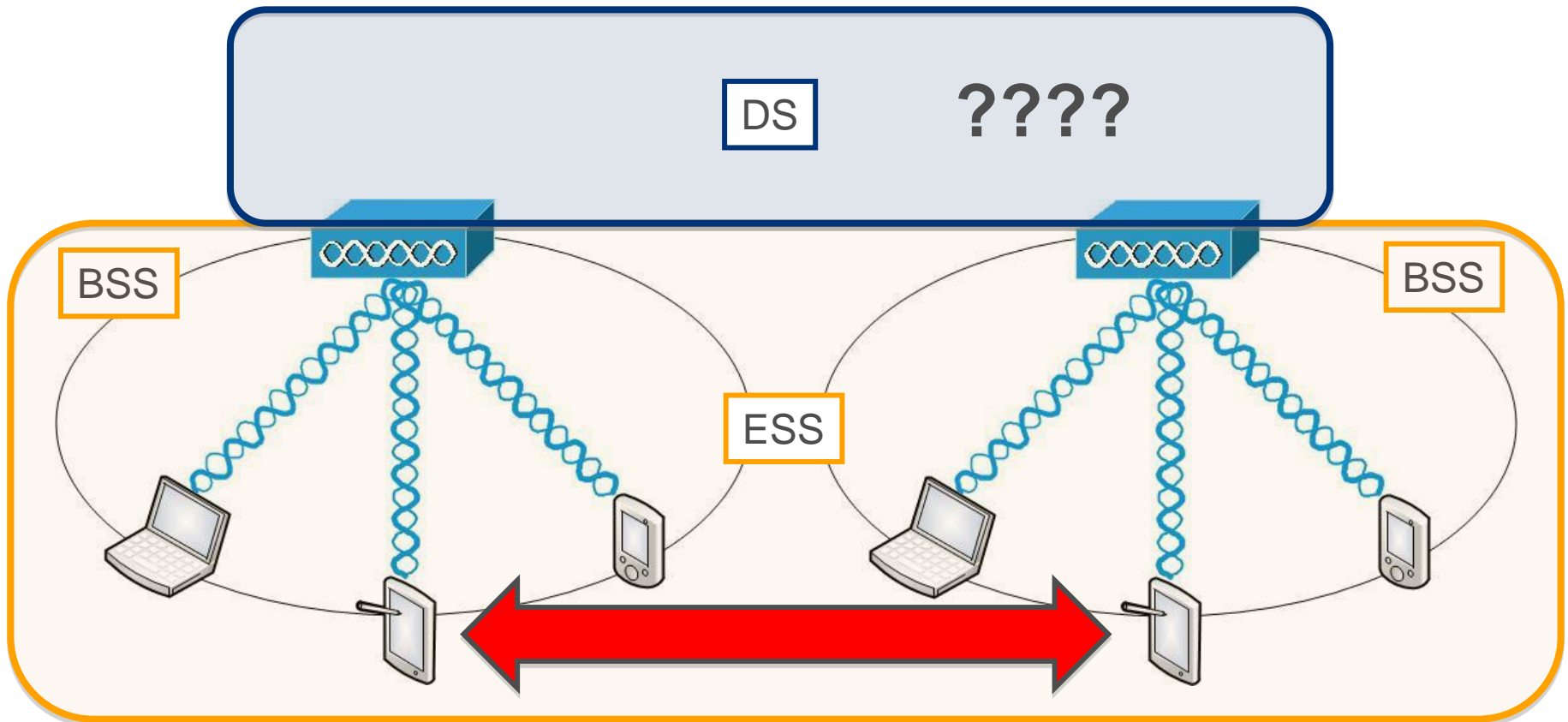
Service	Description	Implementation
Distribution Services		
Association	Used to create a logical connection between a mobile STA and an AP	802.11
Reassociation	Similar to association service, except information about a mobile STA's previous AP may be included; used as a STA moves across an ESS	802.11
Disassociation	Used by AP to force mobile STA off the BSS or by mobile STA to inform AP it doesn't need service anymore	802.11
Distribution	Service to determine how to deliver frames	802.11, CAPWAP
Integration	Service to determine how WLAN connects to other LANs	
STA Services		
Authentication	Used to prove the identity of the STA & AP	

So, What Do These Nine Services Accomplish?

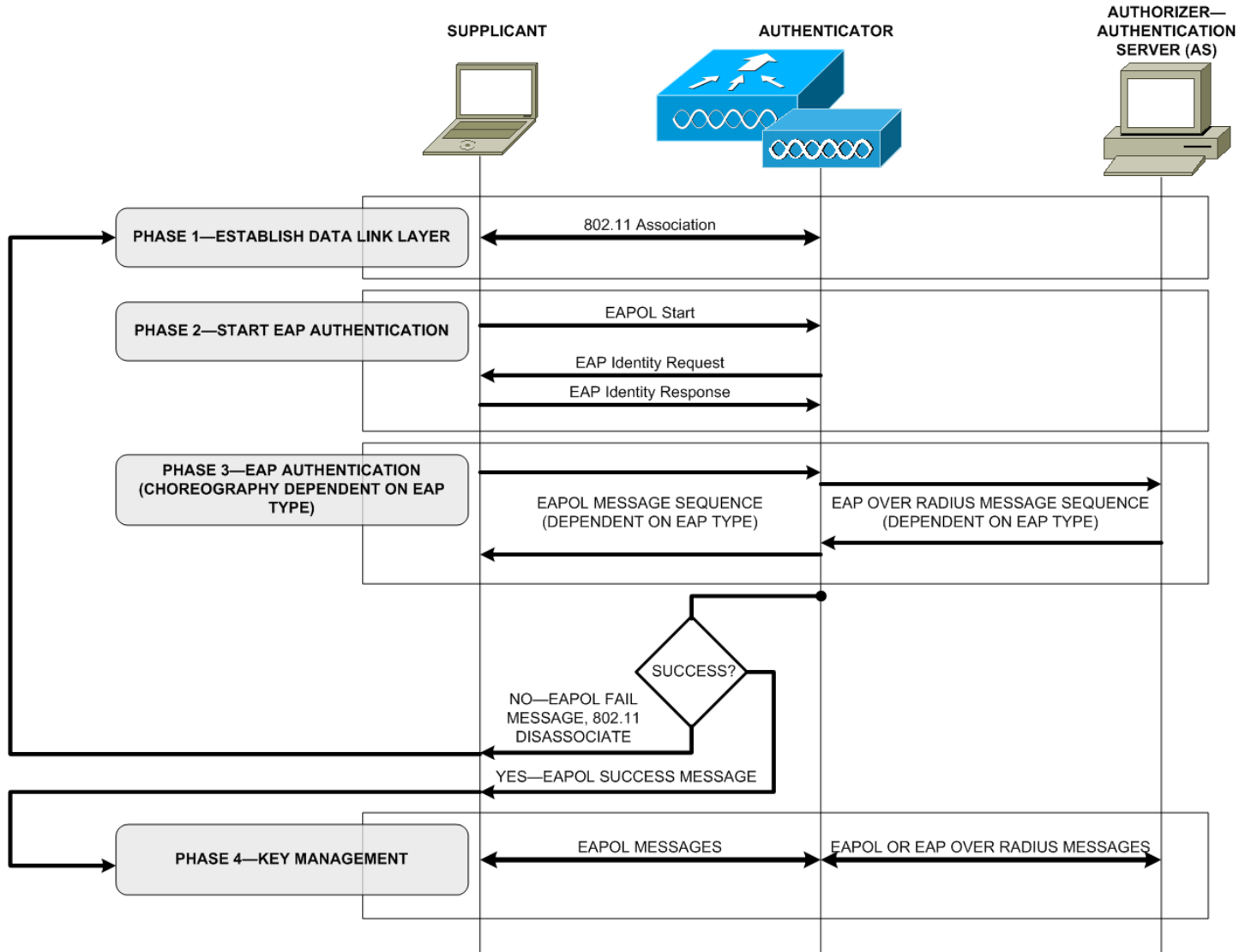
What's Missing?

802.11 Architecture Basics

- ESS – Extended Service Set
- DS – Distribution System



802.1X/EAP Choreography



Device Mobility Problem Statement:

- Specification for how STAs association, authenticate, and protect data privacy defined in context of a single AP (mostly...)
- Specifications for how STAs transition securely in an ESS – hazy
- Specifics of DS/Integration services not well defined for Enterprise

Device Mobility Problem Statement:

- Wireless devices move by definition
- Applications require session persistence, while maintaining security and other services

**Requirement: Facilitate Fast
Secure Roaming for Enterprise
Class Devices in an Efficient and
Scalable Way...**

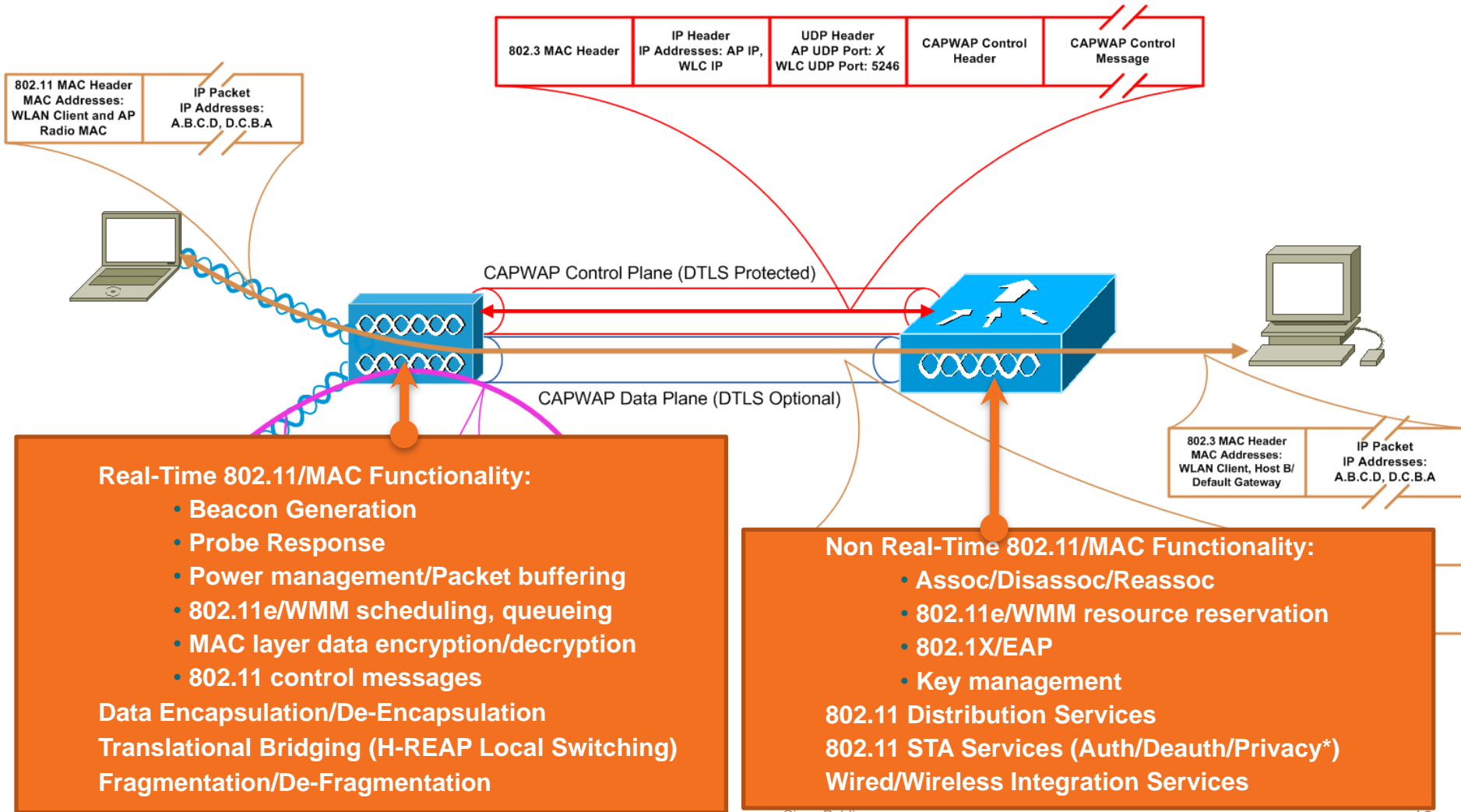
Learn. Connect.
Collaborate. *together.*

Anatomy of a Device Roam

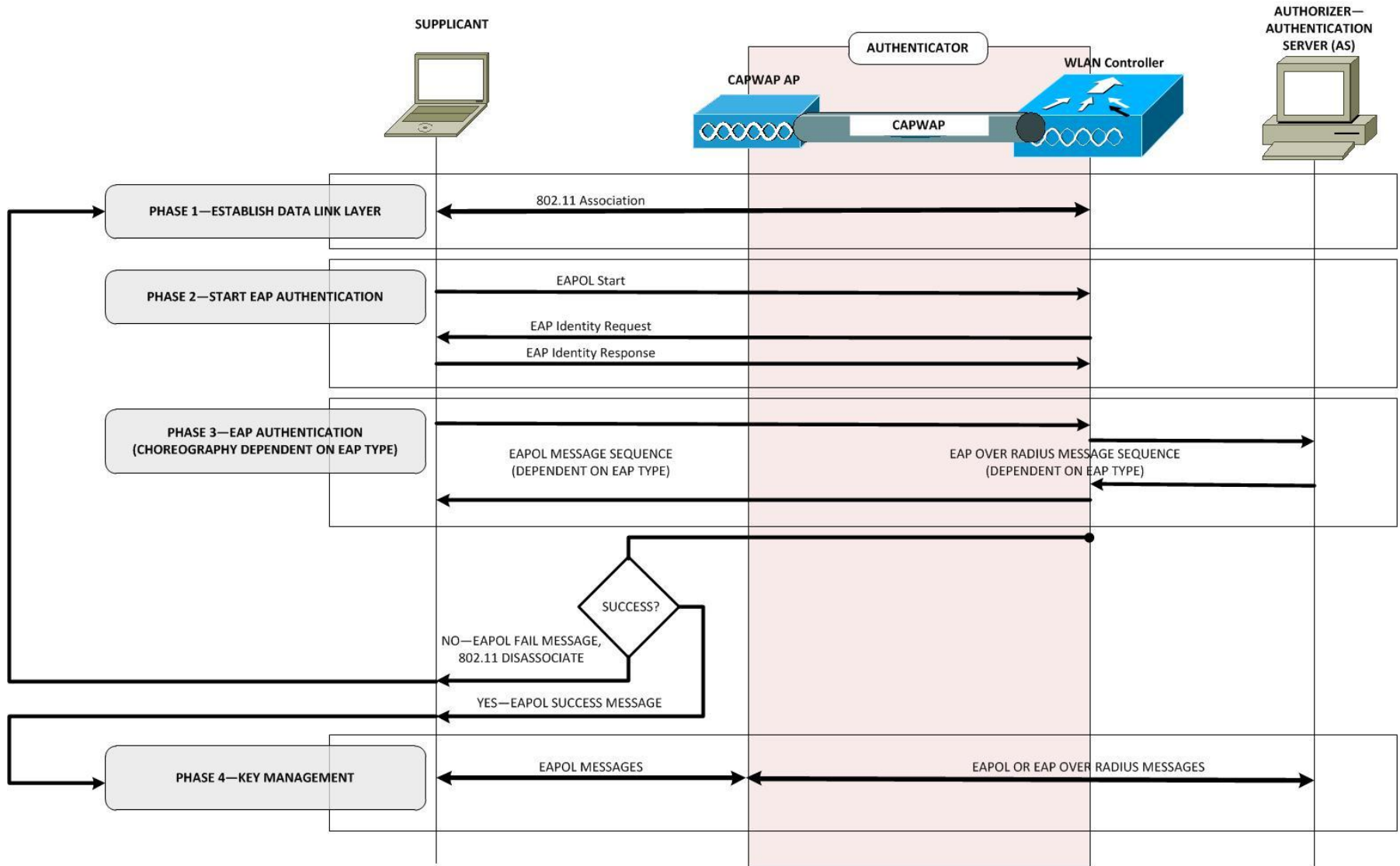
Section Agenda

- CUWN Architecture Review
- Basic Roaming Walkthrough
- Fast Secure Roaming Technologies

CUWN Architecture Review

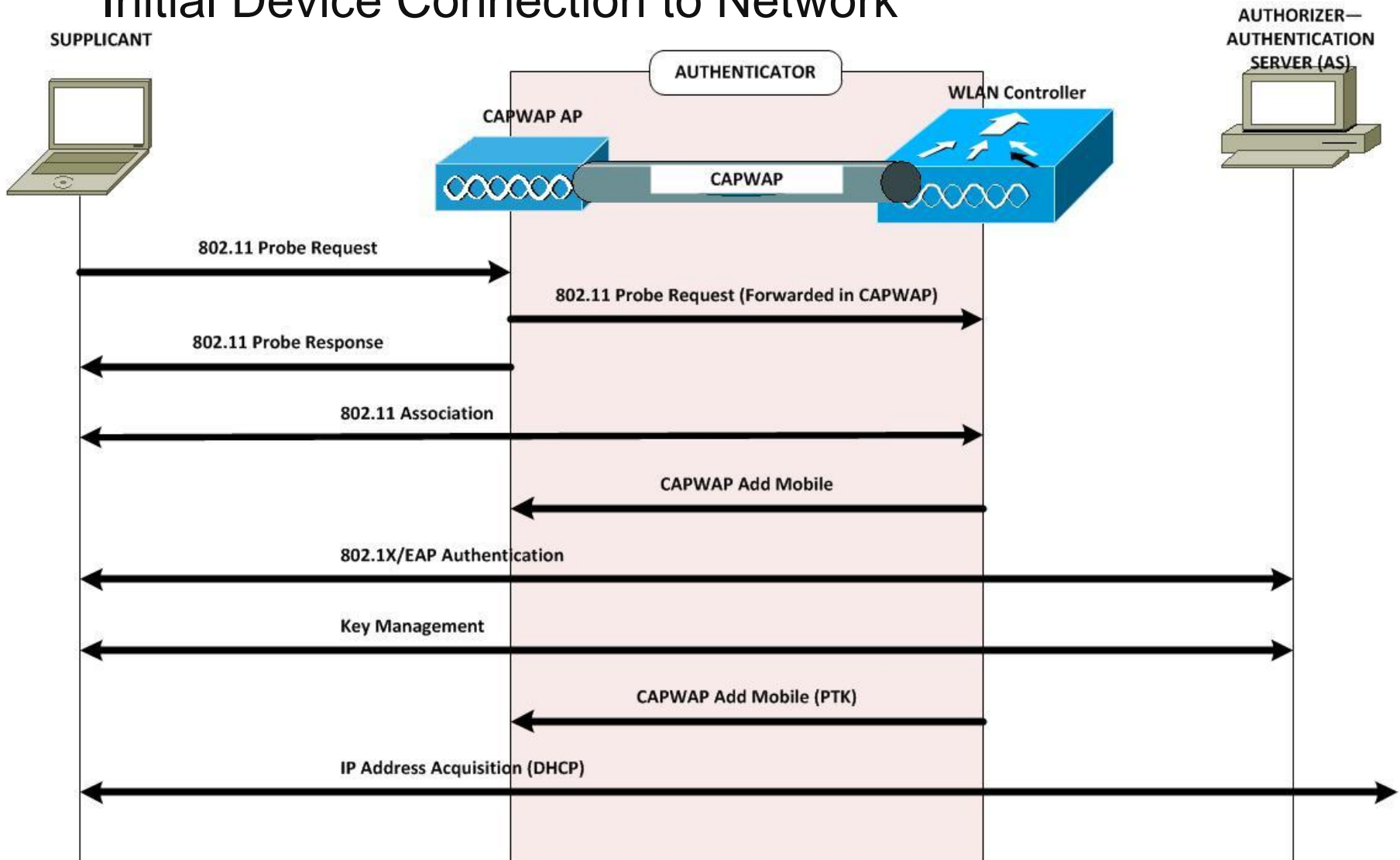


802.1X/EAP Choreography Revisited



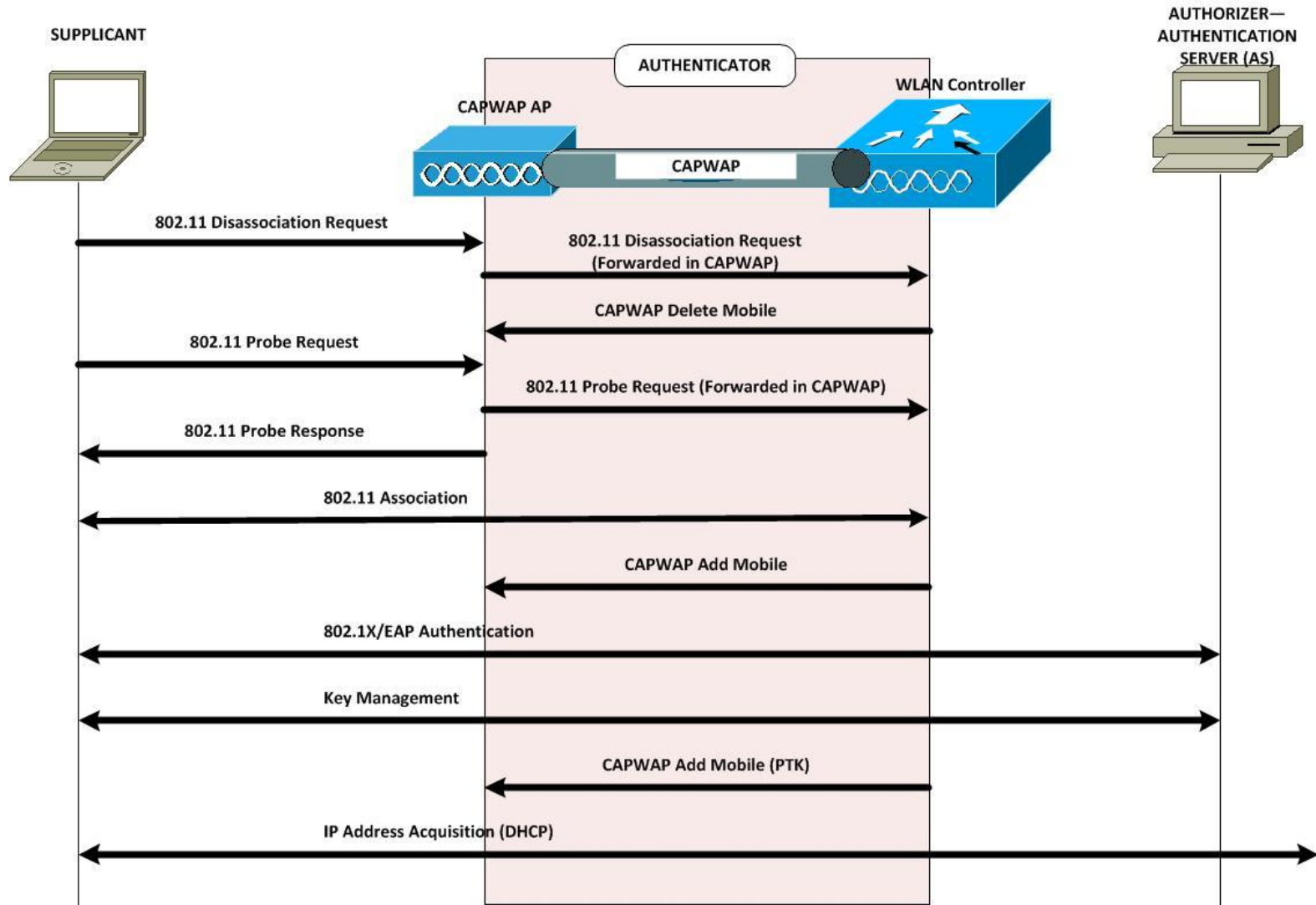
Anatomy of a STA Roam

Initial Device Connection to Network



Anatomy of a STA Roam

Client Roam



Anatomy of a STA Roam

Summary of Important Points

- The STA chooses when to roam
- Each time the STA connects to a new BSSID, it must fully reauthenticate and rekey
- IP Addresses get refreshed on roams (usually)
- How long does a roam take?

How Long Does an STA Roam Take?

- Time it takes for:
 - Client to disassociate +
 - Probe for and select a new AP +
 - 802.11 Association +
 - 802.1X/EAP Authentication +
 - Rekeying +
 - IP address (re) acquisition
- All this can be on the order of seconds... Can we make this faster?

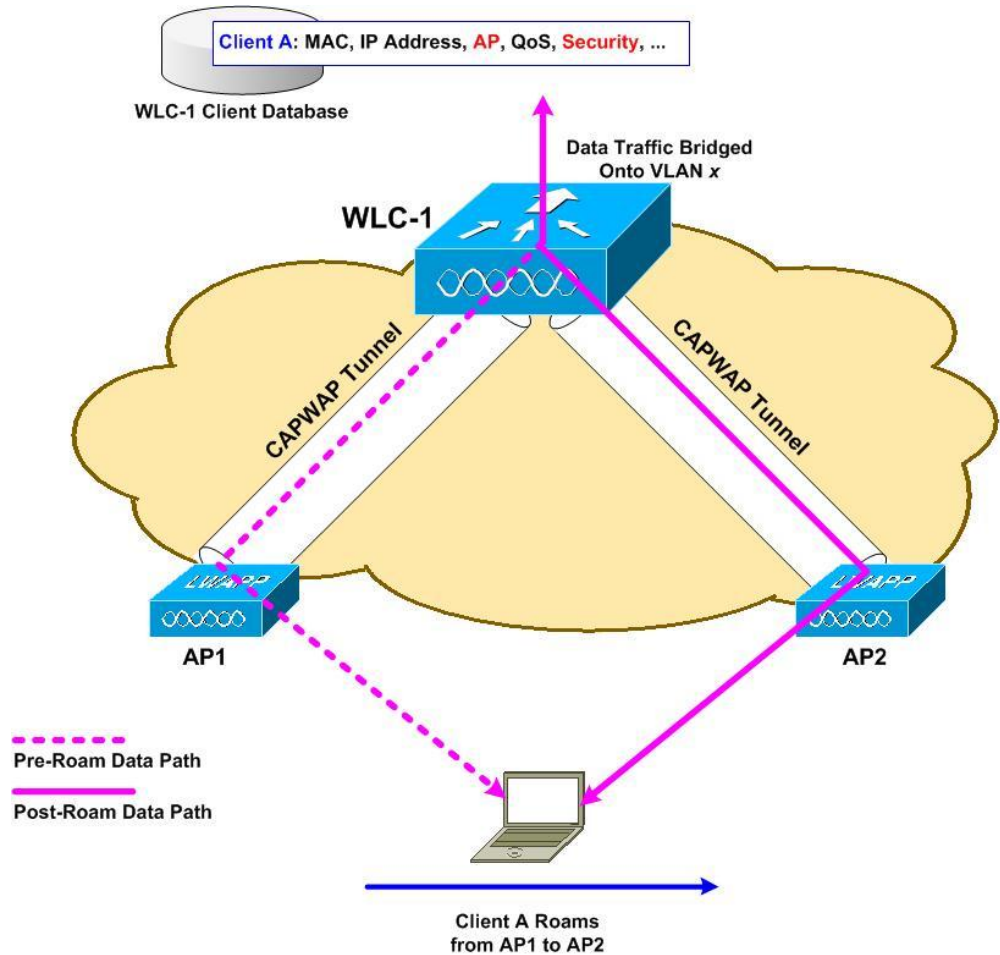
How Are We Going to Make Roaming Faster?

Focus on Where We Can Have the Biggest Impact...

- ❑ Eliminating the (re)IP address acquisition challenge
- ❑ Eliminating full 802.1X/EAP reauthentication

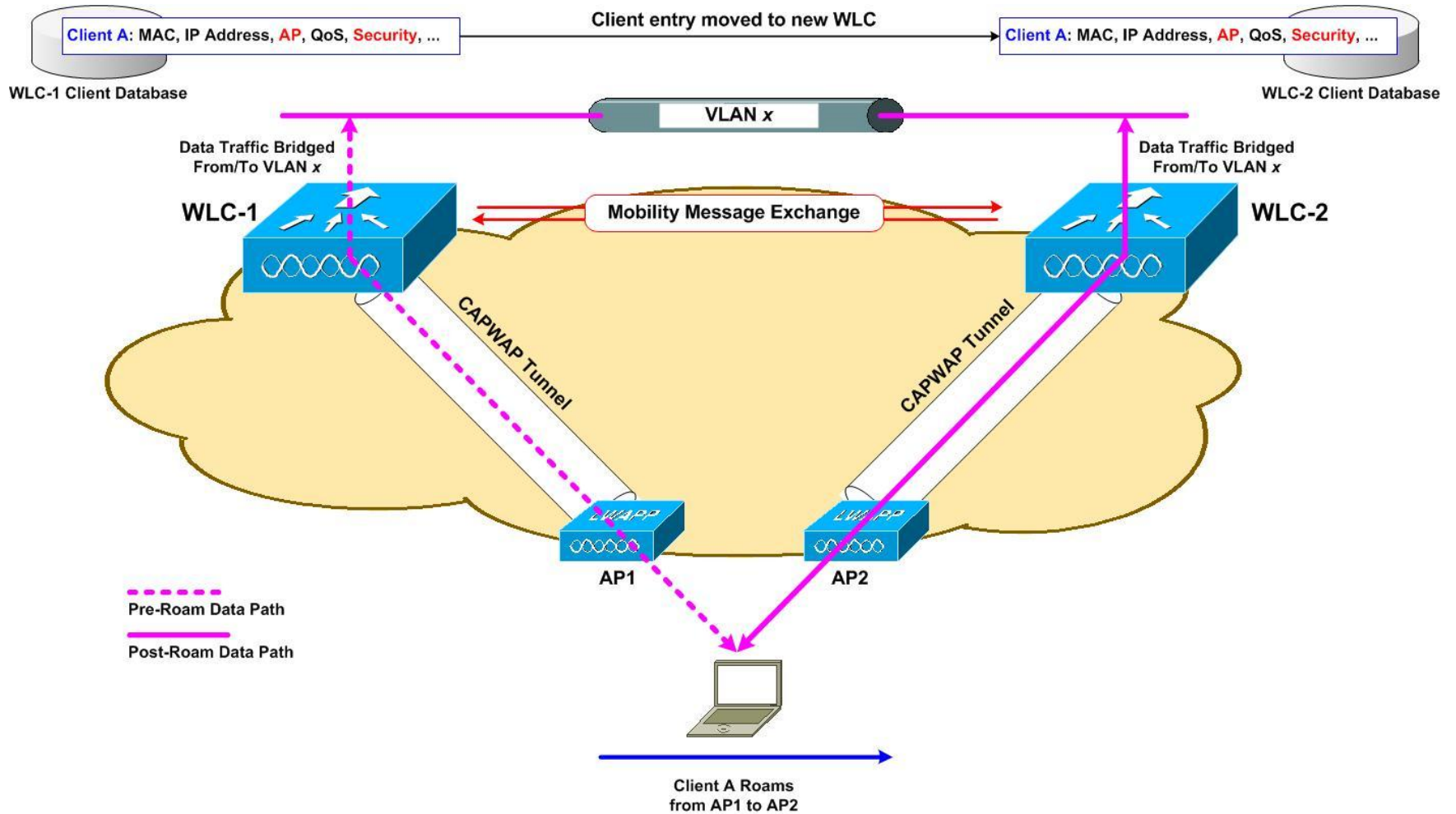
Roaming: Intra-Controller

- Intra-controller roam happens when a STA moves association between APs joined to the same controller
- Client must be re-authenticated and new security session established
- Controller updates client database entry with new AP and appropriate security context
- No IP address refresh needed



Roaming: Inter-Controller

Layer 2

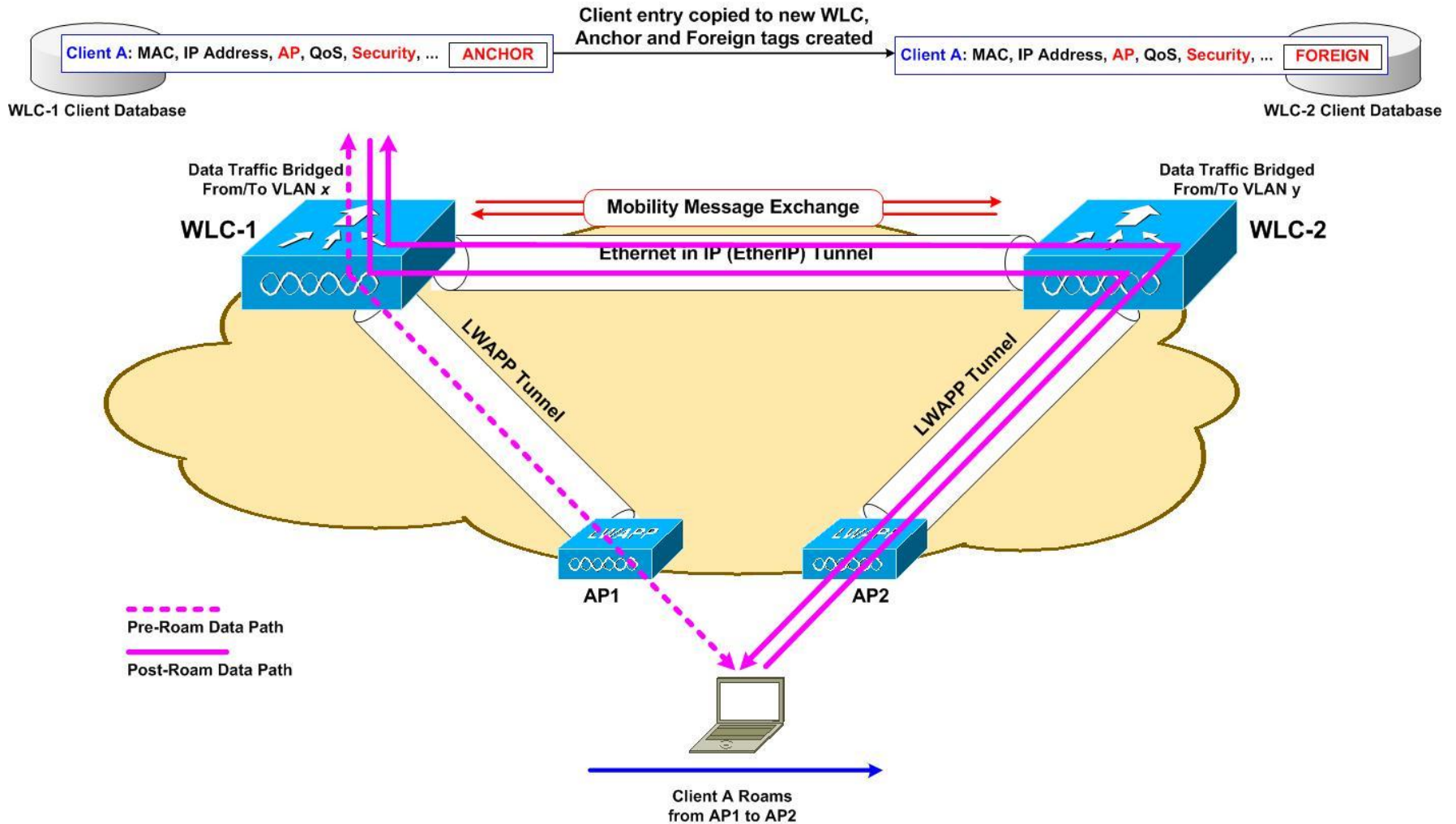


Roaming: Inter-Controller

Layer 2

- L2 inter-controller roam: STA moves association between APs joined to the different controllers but client traffic bridged onto the same subnet
- Client must be re-authenticated and new security session established
- Client database entry **moved** to new controller
- WLCs must be in same mobility group or domain
- No IP address refresh needed
- Account for mobility message exchange in network design

Roaming: Inter-Controller Layer 3



Roaming: Inter-Controller

Layer 3

- L3 inter-controller roam: STA moves association between APs joined to the different controllers but client traffic bridged onto different subnets
 - Client must be re-authenticated and new security session established
 - Client database entry **copied** to new controller – entry exists in both WLC client DBs
 - Original controller tagged as the “anchor”, new controller tagged as the “foreign”
 - WLCs must be in same mobility group or domain
 - No IP address refresh needed
 - Symmetric traffic path established -- asymmetric option has been eliminated as of 6.0 release
 - Account for mobility message exchange in network design
 - Account for asymmetric traffic path (EtherIP)

How Are We Going to Make Roaming Faster?

Focus on Where We Can Have the Biggest Impact...

- ✓ Eliminating the (re)IP address acquisition challenge
- ❑ Eliminating full 802.1X/EAP reauthentication

Cisco Centralized Key Management (CCKM)

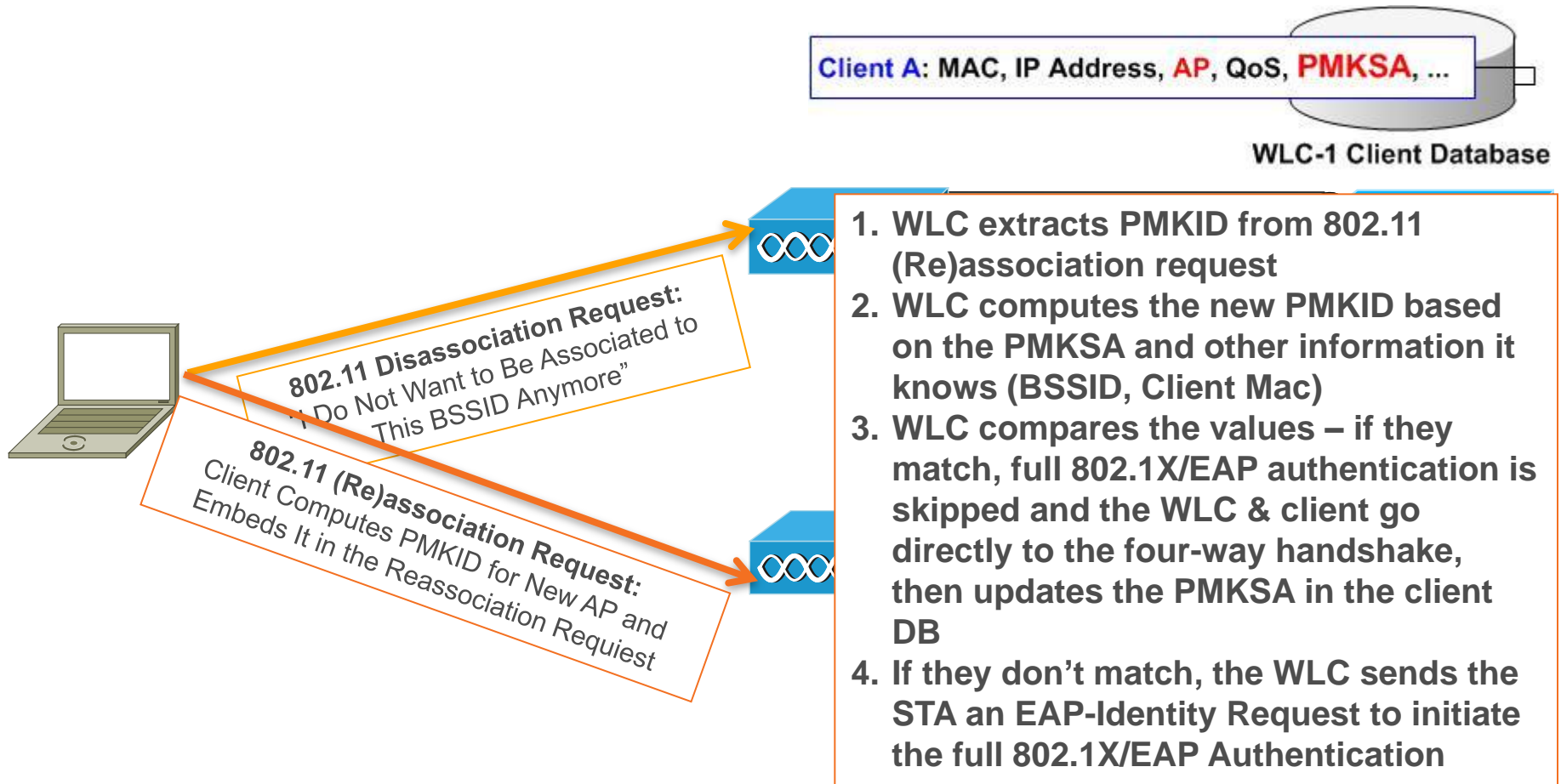
- Cisco introduced CCKM in CCXv2 (pre-802.11I), so widely available, especially with application specific devices (ASDs)
- CCKM originally a core feature of the “Structured Wireless Aware Network” (SWAN) architecture
- CCKM ported to CUWN architecture in 3.2 release
- In highly controlled test environments, CCKM roam times consistently measure in the 5-8 msec range!
- CCKM is most widely implemented in ASDs, especially VoWLAN devices
- To work across WLCs, WLCs must be in the same mobility group
- CCX-based laptops may not fully support CCKM – depends on supplicant capabilities

PMKID Caching

- Optional component of 802.11i specification
- Defines a “PMK Security Association” (PMKSA) that gets stored by authenticator
- PMKSA includes:
 - PMKID
 - Lifetime
 - PMK (32 bytes)
 - BSSID (6 bytes)
 - Client's MAC (6 bytes)
 - AKM (Authentication and Key Management)
- PMKID =
HMAC-SHA1-128 (PMK,
“PMK Name” || BSSID || STA Mac)

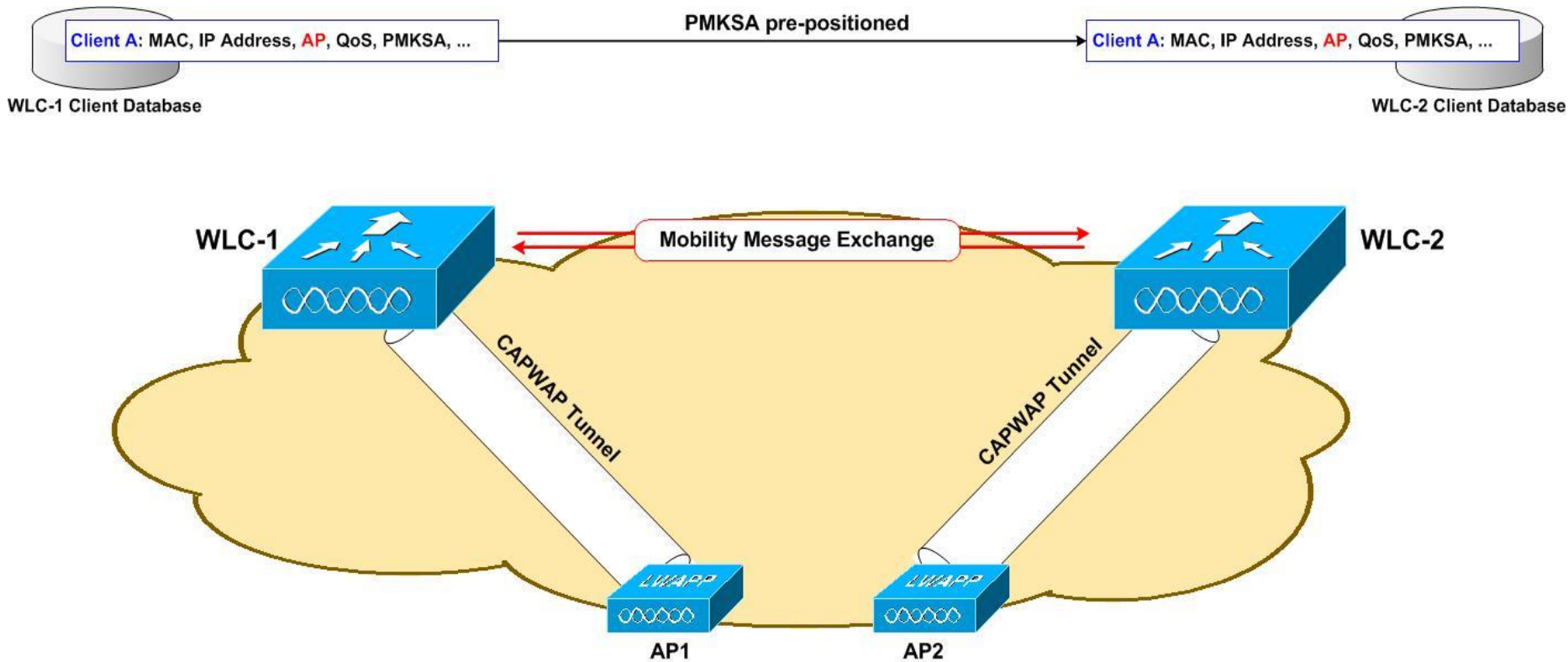
Opportunistic/Proactive Key Caching

Basic Mechanics



Proactive Key Caching

Basic Mechanics



OKC/PKC

Key Data Points

- Requires client/supplicant support
- Supported in Windows since XP SP2
- Many ASDs support OKC and/or PKC
- Check on client support for TKIP vs. CCMP – mostly CCMP only
- Enabled by default on WLCs with WPAv2
- Requires WLCs to be in the same mobility group
- Important design note: pre-positioning of roaming clients consumes spots in client DB
- In *highly controlled test environments*, OKC/PKC roam times consistently measure in the 10-20 msec range!

Standardization! 802.11R

- 802.11R is a ratified IEEE standard, based in large part on CCKM
- 802.11R: “Fast (Basic Service Set) BSS Transition”
- Also includes dynamic QoS capabilities
- No commercially available clients at this point
- WiFi Alliance is planning/implementing 802.11R plugfests in the Voice/Enterprise certification
- Cisco WLCs have implemented 802.11R (unsupported) since 5.2 – Official support will be in 7.2MR1
- In *highly controlled OTA test environments*, 802.11R roam times are comparable to CCKM OTA times

How Are We Going to Make Roaming Faster?

Focus on Where We Can Have the Biggest Impact...

- ✓ Eliminating the (re)IP address acquisition challenge
- ✓ Eliminating full 802.1X/EAP reauthentication

Learn. Connect.
Collaborate. *together.*

Design and Deployment Considerations



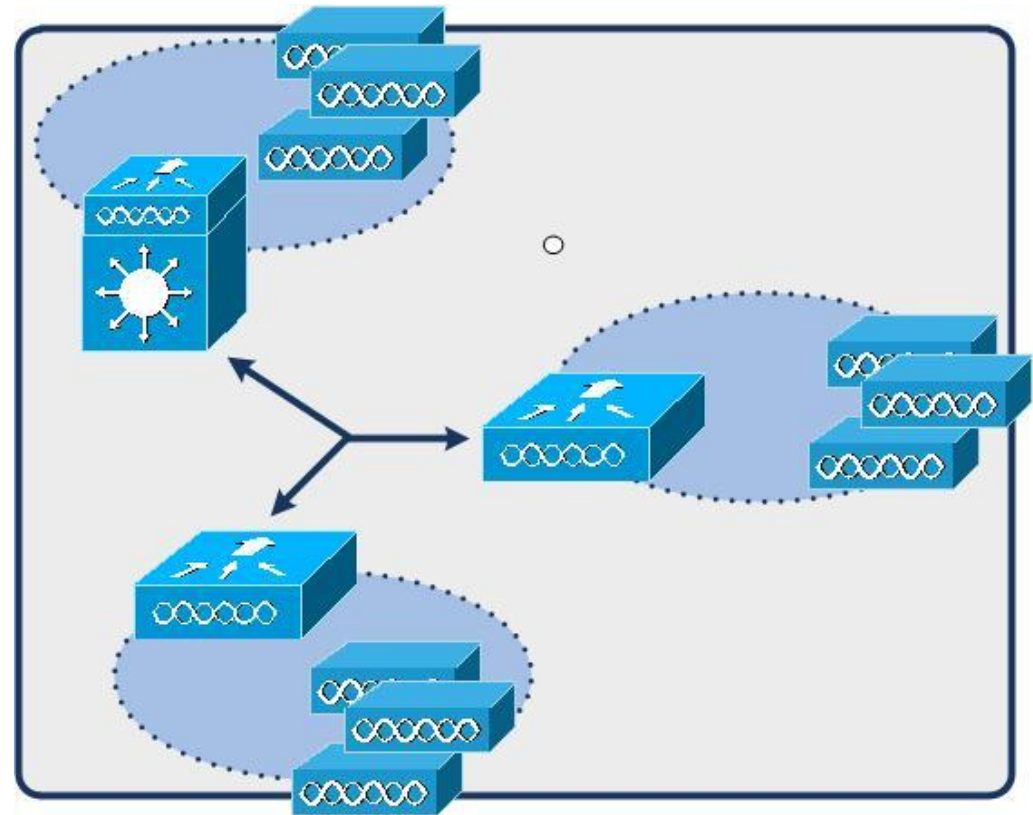
Section Agenda

- Roaming Domains
- Design Considerations for Roaming
- Client Roaming Behavior
- Special Case: H-REAP Groups

Roaming Domains

Mobility Group

- Mobility Group – cluster of up to 24 controllers (regardless of type) that create a seamless roaming domain
- Fast secure roaming technologies work across controllers within a roaming domain
- Mobility messages exchanged either unicast or multicast depending on configuration

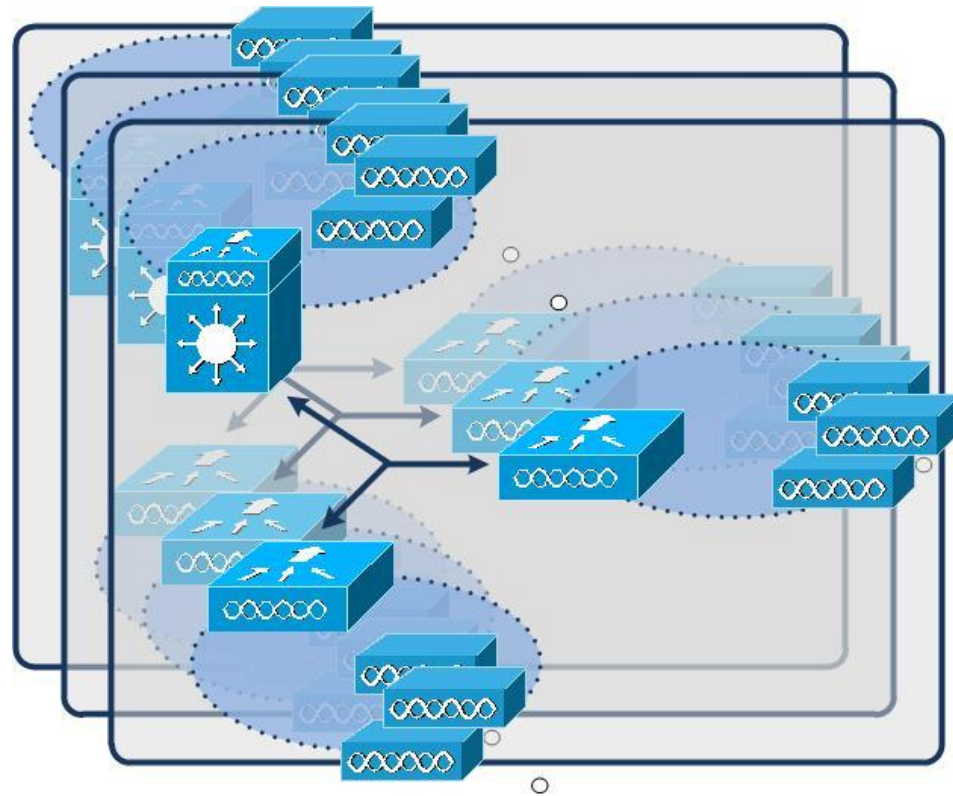


<http://www.cisco.com/en/US/docs/wireless/controller/7.0/configuration/guide/c70mobil.html#wpmkr1100509>

Roaming Domains

Mobility Domain

- Mobility Domain is a seamless roaming domain of up to 3 Mobility Groups
- Max of 72 WLCs
- Seamless roaming == IP addressing is maintained
- Fast secure roaming does work not across Mobility Group – clients crossing these boundaries will have to go through a full reauth, but will retain their IP address



<http://www.cisco.com/en/US/docs/wireless/controller/7.0/configuration/guide/c70mobil.html#wpmkr1100509>

How Long Does a Client Really Take to Roam?

- Time to roam =
 - Client to disassociate +
 - Probe for and select a new AP +
 - 802.11 Association +
 - Mobility message exchange between WLCs +
 - Reauthentication +
 - Rekeying +
 - IP address (re) acquisition
- Network latency will have an impact on these times – consideration for controller placement
- With a fast secure roaming technology, roam times under 150 msec are consistently achievable, though mileage may vary

How Often Do Clients Roam?

- It depends... types of clients and applications
- Most client devices are designed to be “nomadic” rather than “mobile”, though proliferation of small form factor, “smart” devices will probably change this...
- Nomadic clients usually are programmed to try to avoid roaming... so set your expectations accordingly
- “SWAG” design rule of thumb: 10-20 roams per second for every 5000 clients

Designing a Mobility Group/Domain

Design Considerations

- Less roaming is better – clients and apps are happier
- While clients are authenticating/roaming, WLC CPU is doing the processing – not as much of a big deal for 5508 which has dedicated management/control processor
- L3 roaming & fast roaming clients consume client DB slots on multiple controllers – consider “worst case” scenarios in designing roaming domain size
- Leverage natural roaming domain boundaries
- Mobility Message transport selection: multicast vs. unicast
- Make sure the right ports and protocols are allowed

Special Case: FlexConnect Groups

- Support for up to 100 FlexConnect Groups in 5508, 500 in 7500
 - 25 FlexConnect APs per group with 5508, 50 with 7500 controller
 - APs in an FlexConnect share common configuration parameters like RADIUS servers
 - Fast Secure Roaming via CCKM, PKC (for locally switched clients is supported for all clients in an FlexConnect Group (L2 roaming only)... PKC requires 7.0.116.x + code
 - CCKM/PKC keying material is provisioned locally – allows CCKM/PKC to work in standalone mode (existing clients when AP transitioned from connected mode)
- * Note: FlexConnect is new branding for Hybrid REAP (H-REAP)

<http://www.cisco.com/en/US/docs/wireless/controller/7.0/configuration/guide/c70hreap.html#wp1133688>

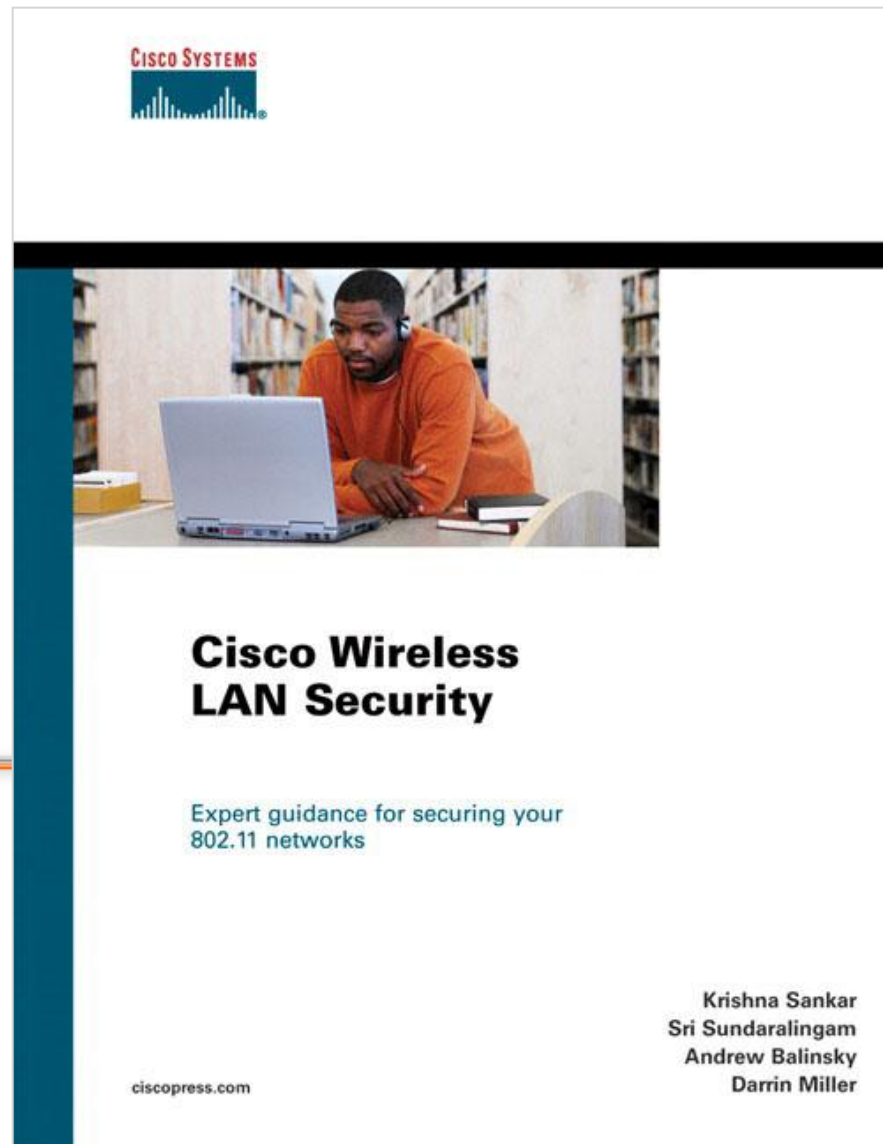
Learn. Connect.
Collaborate. *together.*

Questions?

Recommended Reading

BRKEWN- 2018

Learn. Connect.
Collaborate. *together.*

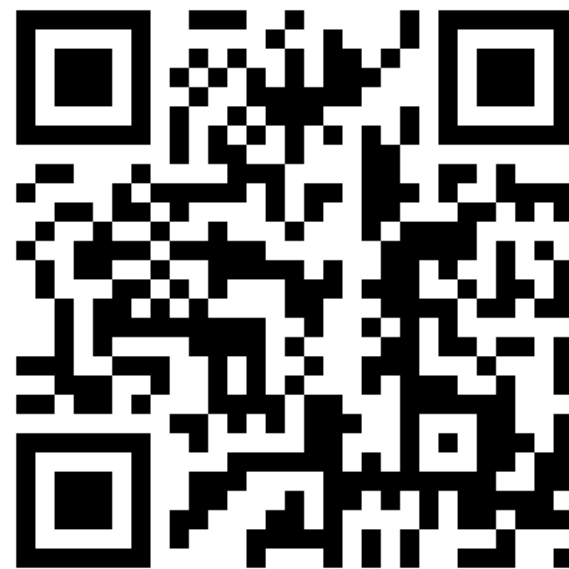


Please complete your Session Survey

We value your feedback

- Don't forget to complete your online session evaluations after each session. Complete 4 session evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt
- Surveys can be found on the Attendee Website at www.ciscoliveLondon.com/onsite which can also be accessed through the screens at the Communication Stations
- Or use the Cisco Live Mobile App to complete the surveys from your phone, download the app at www.ciscoliveLondon.com/connect/mobile/app.html

1. Scan the QR code
(Go to <http://tinyurl.com/qrmelist> for QR code reader software, alternatively type in the access URL above)
2. Download the app or access the mobile site
3. Log in to complete and submit the evaluations



<http://m.cisco.com/mat/cleu12/>



Cisco *live!*

Thank you.

