Emerging IEEE 802.11 Protocols for WLAN Mobility

Sunghyun Choi and Seongkwan Kim

Contents

1. Introduction
2. Background
3. IEEE 802.11 handoff support
4. IEEE 802.11f Inter-Access Point Protocol (IAPP)
5. Emerging standards for fast handoff support
6. Conclusion

1 Introduction

IEEE 802.11 Wireless LANs (WLANs) have been widely deployed and popularized as a dominant means for the broadband wireless access network in the recent years. It is being deployed in many different environments such as home, enterprise, and hot-spot areas. In the enterprise networks as well as hot spots, it is typical to have multiple access points (APs) to cover the geographical area in service. In such environments, providing a seamless service to the users, e.g., Voice over WLAN (VoWLAN) users, even during the movement via handoff, i.e., changing its association from an AP to another as it moves around, is considered a very crucial service requirement. In this paper, we present the mechanisms to enable a smooth WLAN mobility in the context of the emerging IEEE 802.11 protocols.

2 Background

We first present the background information, which is needed to understand the mobility support mechanism in the IEEE 802.11 WLAN. The very basic form of the IEEE 802.11 WLAN is called a basic service set (BSS). There are two types of BSS: infrastructure BSS and independent BSS (IBSS). The former is composed of an AP, which works as the bridge between the (wireline) infrastructure and the wireless link, and a number of stations, which are associated with the AP. On the other hand, the latter is composed of a number of stations, which are communicating directly one another. This type of BSS is also referred to as an *ad-hoc*[†] mode. It is straightforward that for the handoff discussion we are interested in the infrastructure BSS.

[†] This ad-hoc mode of IEEE 802.11 should be differentiated from the ad-hoc networking, for which the protocols are

	802.11a [3]	802.11b [4]	802.11g [7]
Frequency bands	5 GHz	2.4 GHz	2.4 GHz
Number of available channels (in the US)	12 (of 20 MHz width)	11 (of 22 MHz width, overlapping)	
Supported transmission rates (Mbps)	6, 9, 12, 18, 24, 36, 48, 54	1, 2, 5.5, 11	1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54

Table 2.1 Summery of different 802.11 physical (PHY) layers

While a single AP may be enough to cover a small geographical area including a home or a small hot spot, multiple APs are usually deployed to cover large hot spots or enterprise networks. In the latter case, the multiple APs are typically connected to one another via the wireline, e.g., the Ethernet link. A frequency channel planning can be an issue for multiple AP deployment in a given geographical area. To reduce co-channel interference, it is desired to use non-overlapping frequency channels for immediately neighboring APs. However, as found in Table 2.1, there may not be enough non-overlapping channels available (e.g., only three for the 802.11b/g). Although one can avoid co-channel interference by allocating three non-overlapping channels to neighboring APs in a two-dimensional structure, it becomes problematic in the three-dimensional environments such as multiple-story buildings. Therefore, it could be practically impossible to avoid the co-channel interference at least in the 802.11b/g WLANs. Fortunately, the 802.11 distributed coordination function (DCF), which is based on carrier-sense multiple access with collision avoidance (CSMA/CA) protocol [‡], medium access control (MAC) allows APs (or BSSs) in the same frequency channel to share the channel rather smoothly thanks to its carrier sense-based access mechanism.

being defined by the Internet Engineering Task Force (IETF) Mobile Ad Hoc Networking (MANET) Working Group [12].

[‡] In DCF, a station basically transmits its pending frame only when no other stations transmit frames into the channel.

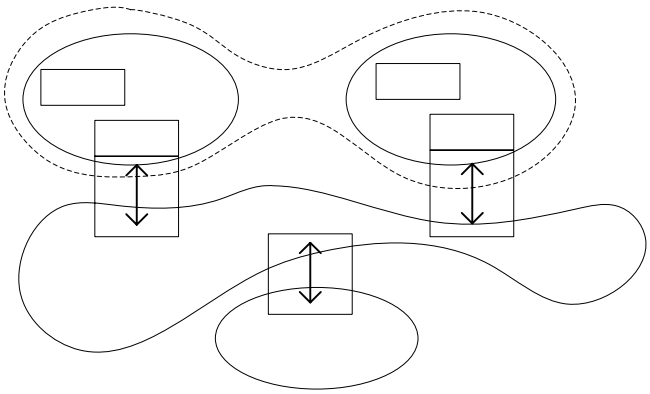


Fig. 1 Conceptual architecture of IEEE 802.11 WLAN

A set of BSSs forms an extended service set (ESS) as shown in Fig. 1. An ESS is identified by a service set identification (SSID), which is often referred to as the "Network Name" in the commercial 802.11 WLAN devices. The APs periodically broadcast a management frame§, called beacon frame, in which a field indicates the SSID so that the stations can identify the APs belonging to the same ESS. The beacon includes many other information fields crucial for the 802.11 WLAN operations, such as the time synchronization, power save support and handoff. The network system, which connects all the APs belonging to the same ESS, is called a distribution system (DS).

In the later part of this chapter, we will discuss how the APs communicate across the DS in order to support the mobility of the stations within the ESS.

3 IEEE 802.11 handoff support

3.1 (Re)-association procedure

In an infrastructure BSS, a station communicates via its AP only. That is, all the frames are either transmitted by an AP (i.e., downlink) or destined to an AP (i.e., uplink).

In order to communicate via an AP, a station should associate with the AP first. However, before the association can be made, the following two steps should be preceded, i.e., scanning and authentication processes. We briefly explain the procedures needed until the association.

- **Scanning:** this is a process for a station to search surrounding APs. There are two different types of scanning: *passive* and *active*. With the passive scanning, the station detects the surrounding APs by receiving the beacon frames transmitted by these surrounding APs. This can be a slow process since the beacon

§ A frame is referred to as the unit of a transfer or a packet in the layer-2 protocols.

transmission interval is typically about 100 ms (or 102.4 ms more exactly). The faster scanning process is the active scanning. With this type of scanning, the station broadcasts a probe request frame, then APs receiving this probe request responds with a probe response frame. The probe response includes virtually the same information as the beacon frame, and hence the station receiving a probe response acquires all the necessary information to associate with the AP. When there are multiple APs found in the neighborhood, the station chooses one of them based on its implementation-dependent decision criteria.

- Authentication: this process is for the station to be authenticated with the AP by proving itself a valid station. There are two types of authentication as defined in the current 802.11 standard: open system and shared key. With the open system, the station sends an authentication request frame, and the requested AP responds with an authentication response frame. There is no specific security information conveyed in the authentication request frame in this case. With the shared key method, a four-way handshake is used for the AP to check whether the requesting station has the same security key or not.
- Association: finally, the station can be associated with the AP by exchanging an association request and an association response frame. Through this exchange, the station is assigned an association identification, and the AP is informed some information required for the proper communication, e.g., the transmission rates supported by the newly-associated station.

Fig. 2 illustrates the association procedure assuming the active scanning and the open system authentication. Even though only a single AP is shown in the figure, there could be multiple APs, which receive the probe request, and respond with a probe response.

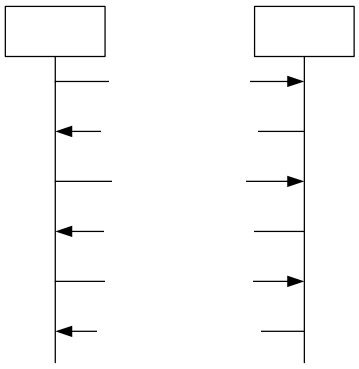


Fig. 2 IEEE 802.11 association procedure

Basically the same procedure should be followed for the handoff of a station. However, in order for the AP accepting a station's association to differentiate between a new association and a handoff, the 802.11 defines two different frame types for the association request. The request for the handoff is called *reassociation* request, where the corresponding frame includes the MAC address of the old AP so that the new AP can communicate with the old AP to support the handoff process more efficiently.

It should be noted that a station can be associated with a single AP at a given time. It is natural since a simultaneous communication with multiple APs, i.e., soft handoff of code-division multiple access (CDMA) systems, is not supported in the 802.11 WLAN. Therefore, the 802.11 handoff is a *hard* handoff naturally. On the other hand, a station can be authenticated with multiple APs. Note that this can reduce the handoff time. However, this requires a station to search surrounding APs, and get authenticated (i.e., 802.11 authentication) in advance. This is often referred to as "pre-authentication" [2]. As will be further mentioned later, there is another pre-authentication in 802.11i [8], which is not 802.11 authentication, but 802.1X-based authentication.

3.2 Layer-2 vs. layer-3 mobility

Fig. 3 illustrates two different types of handoff events within a WLAN depending on whether the two APs involved in the handoff are in the same subnet or not. All the APs and stations in an ESS can be in the same subnet, i.e., all the APs are connected via IEEE 802.1d MAC bridges [10] (e.g., Ethernet switches), and the APs work in the bridge mode. When the two APs involved in a station handoff are in the same subnet, the handoff only involves a layer-2 mobility support without any intervention from the layer 3. See the handoff event labeled as "layer-2 handoff" in Fig. 3. However, when the two APs are in different subnets, or the APs are in the router mode, a handoff involves layer-3 operations since the station cannot use the same IP address after reassociating with the new AP. This should be handled by mobile IP [15][16] or dynamic host configuration protocol (DHCP), which is beyond the scope of this paper.

After reassociating with a new AP, a broadcast frame (originating from the handed off station) should be transmitted to the same subnet so that the layer-2 route tables in the MAC bridges including the APs can be updated. This operation basically completes the layer-2 handoff procedure thanks to the IEEE 802.1d's self-learning process of the routing table [10].

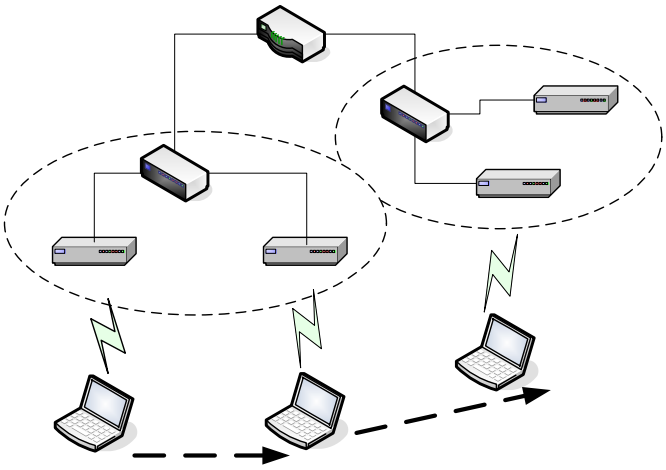


Fig. 3 Layer-2 vs. layer-3 handoffs

4 IEEE 802.11f Inter-Access Point Protocol (IAPP)

The handoff involves the communication between the APs, which relies on the DS. While the 802.11 defines the concept of the DS, it does not define how to implement the DS for the following reasons: (1) the DS involves the higher layer protocols above MAC hence is out of scope of the 802.11, which deals with the MAC and PHY only, and (2) it could be desirable to have the flexibility for the DS construction. Note that the DS can be constructed with any network link, e.g., even with the WLAN link, which is referred to as wireless distribution system (WDS). However, the lack of the standardized DS construction causes interoperability issues among APs from different vendors, especially, in the context of the handoff support. In the 802.11 WLAN (or more specifically, ESS), a station should have only a single association, i.e., the association with a single AP. However, the enforcement of this restriction is unlikely to be achieved due to the lack of the communication among the APs within the ESS.

The 802.11f [6] is a recommended practice for Inter-Access Point Protocol (IAPP), which specifies the information to be exchanged between APs amongst themselves and higher layer management entities to support the 802.11 DS functions. According to the IEEE standards terms, the recommended practice is defined as a document, in which procedures and positions preferred by the IEEE are presented. It should be noted that the 802.11f does not define anything related to the station operation for the handoff.

4.1 Inter-AP communication

The IAPP uses TCP/IP or UDP/IP to carry IAPP packets between APs, and also relies on Remote Authentication Dial In User Service (RADIUS) protocol [13] for APs to

obtain information about one another. A proactive caching mechanism is also defined in order to provide faster roaming by sending the station context to neighboring APs before the actual handoff event.

Fig. 4 shows the architecture of the AP with IAPP. Loaded with venders' proprietary features and algorithms, the AP management entity (APME) is a function external to the IAPP and is typically the main operational program of the AP. The 802.11-1999 defines an entity called station management entity (SME), as shown in Fig. 4, and the APME of the AP incorporates the SME functions. As shown in the figure, the APME can manage/control the IAPP, 802.11 MAC, and 802.11 PHY via the IAPP Service Access Point (SAP), MAC Layer Management Entity (MLME) SAP, and PHY Layer Management Entity (PLME) SAP, respectively.

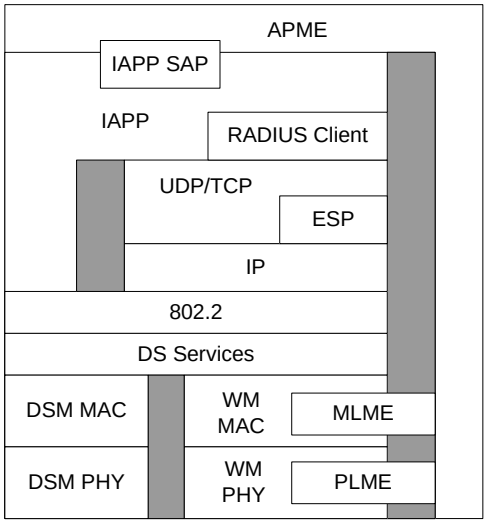


Fig. 4 IEEE 802.11 AP architecture with IAPP

Some functions of the IAPP rely on the RADIUS protocol for the proper and secure operation. In particular, the IAPP entity, i.e., the AP, should be able to find and use a RADIUS server (1) to look up the IP addresses of other APs in the ESS when given the BSS Identifications (BSSIDs)** of those APs, and (2) to obtain security information to protect the content of certain IAPP packets. Actually, the RADIUS server must provide extensions for IAPP-specific operations, which are currently being defined by IETF [14].

The IAPP supports (1) DS services, (2) address mapping between AP's MAC and IP addresses, (3) formation of DS, (4) maintenance of DS, (5) enforcement of a single

** The BSSID of a BSS is determined by the MAC address of the corresponding AP.

association of a station at a given time, and (6) transfer of station context information between APs.

4.2 IAPP operations.

There are three basic IAPP operations: (1) station ADD operation; (2) station MOVE operation; and (3) proactive caching. These operations are briefly explained below.

First, the station ADD operation is triggered when a station is newly associated with an AP. When a station is associated, the AP transmits two packets to the DS: layer-2 update frame and IAPP ADD-notify packet. The layer-2 update frame is addressed at the broadcast address. Upon the reception of this frame, any layer-2 bridge devices, e.g., Ethernet switches connecting multiple APs within the ESS, update the routing table for the associating station according to the IEEE 802.1d bridge table self-learning procedure [10]. The IAPP ADD-notify packet is an IP packet with a destination IP address of the IAPP IP multicast address so that any receiving APs within the ESS remove a stale association with the associating station.

Second, the station MOVE operation is triggered by a station's reassociation when the station hands off from an AP to another AP. The station handing off from an AP transmits a reassociation request frame to the new AP, where the reassocaition request frame includes the MAC address of the old AP as mentioned before. The new AP transmits two packets in this case as well: layer-2 update frame and IAPP MOVE-notify packet. The IAPP MOVE-notify packet is transmitted to the old AP, which in turn transmits an IAPP MOVE-response packet. The response packet carries the context block[††] for the station's association from the old AP to the new AP. Since the reassociation request frame from the station contains only the old AP's MAC address, the new AP needs to look up the IP address of the old AP with the help of a RADIUS server within the ESS. The purpose of the layer-2 update frame is the same as with the station ADD operation. One important fact is that the layer-2 update frame is broadcasted only after the IAPP MOVE-response packet is received from the old AP, as the final step of the hand-off procedure.

Third, the proactive caching is triggered when a station (re)associates with an AP or the context of the station changes. Basically, when the proactive caching is triggered by the APME of an AP, the AP (or the AP's IAPP entity more specifically) transmits the IAPP CACHE-notify packets to its neighboring APs. The notify packet includes the context of the corresponding station. This proactive caching can significant reduce the

[††] The 802.11f does not define what the context block could contain. The examples of the context include security and accounting information of the corresponding station.

handoff delay by broadcasting the layer-2 update frame without waiting for the IAPP MOVE-response packet upon a reassociation, since the new AP has already received the context of the handing-off station from the old AP via the IAPP CACHE-notify packet earlier.

5 IEEE 802.11i for Security Enhancement

IEEE 802.11i [8] provides an enhanced security specification, which defines a Robust Security Network Association (RSNA). An RSNA between a station and its AP can be made after the 802.11 authentication and (re)association are completed, where an open system authentication shall be used under the 802.11i specification. Establishing an RSNA consists of mainly two operations: (1) IEEE 802.1X-based authentication [11], and (2) temporal key establishment. Fig. 5 illustrates the 802.1X authentication, where a station (referred to as a supplicant in the 802.1X terms) and an authentication server authenticate each other, and the mutual authentication results in a pairwise master key (PMK) assignment to the station and its AP. Then, using the PMK, the station and AP perform a 4-way handshake in order to establish the pairwise transient key (PTK), which is used for the encryption of the frames upon an RSNA establishment. When the PTK is generated, an RSNA is established.

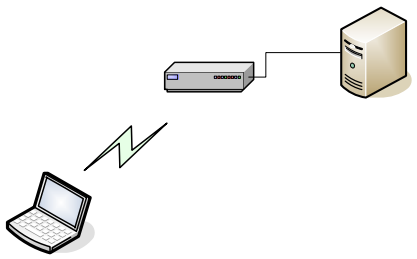


Fig. 5 IEEE 802.1X authentication

The time-consuming four-way handshake has been a controversial topic in TGi discussion and finally triggered the spin-off of a new study group, which we will discuss in a later subsection. In the following, we will discuss the pre-authentication mechanism provided by 802.11i to facilitate fast handoff [8][17].

The 802.11i allows a supplicant station authenticated and associated with an AP to pre-authenticate (based on the 802.1X) with target APs via the current AP and the DS. To initiate the pre-authentication, the station transmits an IEEE 802.1X EAPOL-Start frame with the Destination Address (DA) being the BSSID of the target AP and the

Receiver Address (RA) being the BSSID of the current AP. The current AP receives the Start frame from its Wireless Medium (WM) port and forwards it to the DS via its DS port. The DS delivers the Start frame to the DS port of the target AP. Since the frame is destined to the target AP's BSSID, i.e., the MAC address of the AP's WM port, it is forwarded to the WM port, which then creates a logical WM port with an authenticator Port Access Entity (PAE). The Authenticator PAE responds by sending an EAP-Request destined to the MAC address of the supplicant station, encapsulated in an IEEE 802 frame using the pre-authentication EtherType. The frame is forwarded to the DS port, and the DS delivers it to the current AP, which finally forwards it to the station.

The conversation between the pre-authenticating supplicant station and the target AP continues via the current AP and the DS, until the EAP authentication succeeds or fails. A successful authentication results in Pairwise Master Key Security Association (PMKSA), which the station uses to complete the 4-way and group-key handshakes after a reassociation with the target AP.

6 Emerging standards for fast handoff support

In this section, we discuss handoff-related efforts in various task and study groups within the IEEE 802.11 standardization working group [1].[#] Note that, at the time of writing this paper, all of the task groups being discussed are still active. The following content reflects not only the current drafts but also proposals under discussion in the task groups. It should be understood that even the content in the current drafts may be changed in the final standard.

6.1 Task Group K (TGk) for Radio Resource Measurements

IEEE 802.11 Task Group k defines mechanisms for radio resource measurement [9]. Some of the measurement results and measurement mechanisms can facilitate fast handoff.

Several independent empirical studies on 802.11 handoff showed that the most significant part of handoff latency goes to the scanning process [18][19]. To search for target APs, the station scan one channel at a time, using either passive or active scanning, and wait on that channel for a preset timeout before moving on to the next channel. Scanning all the 11 (or 13 depending on the particular regulatory domain) channels of the 802.11b can take a couple of hundreds milliseconds using active

[#] For the standardization of a new protocol, a study group (SG) is formed first in order to determine the goal and scope of the new standard, then a task group (TG) is formed out of the study group. A new standard specification is generated by a task group, e.g., IEEE 802.11f is generated by Task Group F (TGf).

scanning. If passive scanning is used, or if there are more channels to scan, the scanning process can take even longer. There can be basically two ways to shorten the scanning process: reducing the number of channels to scan and/or reducing the scanning time on each channel.

6.1.1 Limiting scanning channels

Under a normal deployment, there are only a handful of neighboring APs around. To avoid wasting time in scanning channels on which no neighboring AP operates, the 802.11k will provide the Neighbor Report, which contains pertinent information on a collection of neighboring APs known to the AP that sends it. An AP compiles its Neighbor Report, and sends it to the stations in its BSS upon Neighbor Report request frame or Association request frame with a Request information element for the Neighbor Report. The details of how AP compiles the Neighbor Report are outside of the scope of this standard. An AP may get the information of neighboring APs from measurement reports received from the stations within the BSS, from management interface such as Simple Network Management Protocol (SNMP), or from DS via IAPP. The information provided in the Neighbor Report includes each neighboring AP's operating channel, BSSID, capability, and supported PHY type, etc. This information therefore can be used by the station to limit the set of channels to scan for a possible handoff. However, since the information in the Neighbor Report may be stale, the usage of it should considered advisory.

6.1.2 Fast active scanning

To scan for APs using active scanning as defined in the base line 802.11 specification [2], a station broadcasts a probe request on the channel of interest and waits for probe response(s) from the AP(s). The station moves on to another channel after a pre-set timeout timer expires.

Without prior knowledge about the identity of the neighboring APs, the probe request has to be sent to the broadcast address, which may result in simultaneous responses from multiple APs. To avoid collision, probe responses follow the same DCF rule to contend for accessing the medium as data frames from any other station do. As a result, the probe response from an AP could potentially be delayed by data frames from any station. Due to this reason, the timeout cannot be too short, as the station may otherwise miss a delayed probe response. Another reason to keep the timeout long is that the station has no prior knowledge on the number of probe responses to expect and may want to get as many probe responses back as possible. Accordingly to our own

measurements, a typical timeout for active scanning is about 100ms per a single channel even though the timeout value should be implementation dependent.

The analysis above points out that it is the broadcast probe request that makes it difficult to shorten the active scanning timeout. Thanks to the Neighbor Report, a station will have prior knowledge of the identities (i.e., BSSIDs) of the neighboring APs. The station may, therefore, choose to send a unicast probe request destined to a particular AP instead. Two benefits arise from using unicast probe request. First, there is no potential collision from multiple simultaneous probe responses. Second, there is no need to wait for more than one response.

To take advantage of these benefits, [20] proposed the following fast active scanning scheme. Nevertheless the advantage of [20] for reducing scanning overhead, it is not included in the current draft [9] due to the usage of unicast probe request, which is not standard compliant.

6.1.3 Fast passive scanning

Passive scanning is attractive since it causes no additional network traffic loads. Furthermore, in certain regulatory domains, active scanning is banned under certain conditions so that passive scanning may be the only choice. Despite its attractiveness, passive scanning usually takes longer than active scanning, as the scanning station needs to wait up to a beacon interval (typically 100 ms) to receive a beacon. It has been pointed out in [21] that passive scanning can be very efficient if the station knows the Target Beacon Transmission Time (TBTT) of the neighbor APs. The proposal [22] therefore proposes to add the neighbor AP's TBTT information in the Neighbor Report. Knowing when to expect a beacon from a particular AP on a particular channel, a station can switch to the channel right before the TBTT and switch back to the original channel right after receiving a beacon, or after a relatively short timeout should it miss the beacon. In [9], Neighbor TSF (Timing Synchronization Function) information can be notified to the station which sends a Neighbor Report request or Association request frame with Request information element.

6.2 Task Group R (TGr) for Fast Roaming

The enhanced security mechanism introduced in the 802.11i creates some challenges for fast handoff. The 802.11i uses the four-way handshake to setup the Pairwise Transient Key Security Association (PTKSA) upon a reassociation as described earlier. There has been some concern that the 4-way handshake process may be too slow to satisfy the needs of real-time low-latency applications such as

Voice over WLAN (VoWLAN).

Based on current and proposed amendments to the 802.11 standard, i.e., the 802.11e/i, the general roaming process consists of maximum five stages: scanning, 802.11 authentication, re-association, PTK derivation (four-way handshake), and QoS admission control. The main objective of TGr is to optimize the 802.11 protocol to allow a TGr-enabled station to establish security and QoS state at a new TGr-enabled AP with minimal connectivity loss to the DS.

To address the fast roaming issues without jeopardizing the progress of the rest of TGi work, the group decided to spin off a separate new task group to provide solutions for fast roaming while TGi wraps up its current draft. As of early 2005, two proposals, which are Transition Acceleration Protocol (TAP) [23] and Just-In-Time 2 Phase Association (JIT) [24], are being considered the candidates for the first 802.11r draft. It should be noted that these two proposals are not competing, but rather complementary. In the following, we discuss TAP and JIT mechanisms briefly.

6.2.1 Transition Acceleration Protocol (TAP)

Even though the latency introduced by 802.1X authentication under the 802.11i can be reduced via pre-authentication and PMKSA caching as described in Section 5, it is still required to perform a 4-way handshake in order to establish a session key for data communication, which can lead to a notable amount of the roaming gap. To shorten the roaming gap to a minimum, three mechanisms are introduced in TAP, namely, *two-tier PMK distribution hierarchy*, *pre-keying*, and *resource pre-allocation*, respectively.

As shown in Fig. 6, two new levels of key hierarchy between PMK and PTK are introduced in TAP. D-PMK (Derived PMK) and DA-PMK (Derived AP PMK) are derived from PMK and D-PMK, respectively, while PMK is acquired via 802.1X or is pre-shared key, as usual. Before explaining the hierarchical key distribution, the concept of *key circle* (KC) should be addressed. A key circle is a collection of one or more APs sharing a common PMK store. In addition, there is an additional key circle, i.e., *extended key circle* (EKC), which is a group of KCs capable of sharing PMK information.

As mentioned earlier, D-PMK is derived from PMK and may be transmitted by the original KC to a foreign KC when a station roams between KCs within a common EKC. DA-PMK is also derived from D-PMK, and may be transmitted by a KC to a AP when a station roams between APs in a single KC. D-PMK and DA-PMK are always unique to a target KC or AP. Stations can compute D-PMK and DA-PMK using KCID which is a unique identification of a KC.

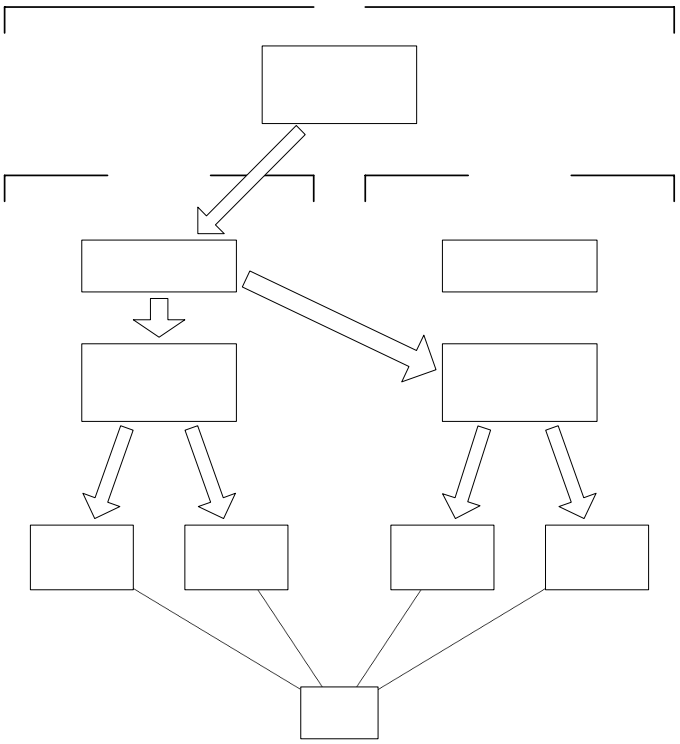


Fig. 6 TAP key hierarchy[§§]

In order for the pre-keying mechanism to be used, TAP PMKSA[***] should exist with the AP's KC or the EKC of which the AP's KC is a member. If a station has no cached PMKSA, or if the pre-key sequence was attempted but has failed, the station associates normally, adding its own TAP advertisement to its association request. During a 4-way handshake, the AP confirms the TAP association with a PMK lifetime. After that, the station creates a new TAP PMKSA, including the lifetime to determine how long the new PMK can be used, and the KCID to determine with whom the new PMK can be used.

If the station already has a cached PMKSA, PTK, which is used for the encryption of the frame between the station and the new AP, is established (i.e., generated from D-PMK or DA-PMK) prior to (re)association at the station side. In another word, the result of the pre-key sequence is the establishment of a new PTK. Moreover, the allocation of resources can be done when the pre-key sequence proceeds, if the station requests this explicitly (i.e., the usage of it is optional).

[§§] In Fig. 6, AAA means authentication, authorization, and accounting, so that an AAA server means a server which can control the three contexts between AAA clients and itself appropriately.

[***] The PMKSA that results from the 802.1X is potentially a TAP PMKSA when the AP has advertised pre-keying capability in its beacon and probe response and the station has advertised pre-keying capability in its (re)association request.

6.2.2 Just-In-Time 2 phase association (JIT)

The JIT seeks to address a large spectrum of network configurations and conditions by offering flexible mechanisms through which mobile stations can quickly adapt to the current environment. For the purpose, three kinds of mechanisms are proposed, i.e., JIT, Query(+JIT), Reservation(+JIT) in JIT.

Basically, JIT is the basic mechanism for performing fast BSS transitions. To address various network conditions, JIT involves using existing IEEE 802.11e (for QoS) and IEEE 802.11k components to discover the next AP for roaming, and follow this up with a reassociation exchange [5][9].

In properly engineered networks, most APs are not fully loaded and if the station acts promptly, resources will not disappear before it commits its connection to the new AP. In this service type, a fast and cheap transition mechanism can be provided with only JIT. JIT allows the station to commit to the new AP and establish a state using the reassociation frames. JIT relies on the next AP to establish new state for the station in a timely manner, without having to rely on DS communications.

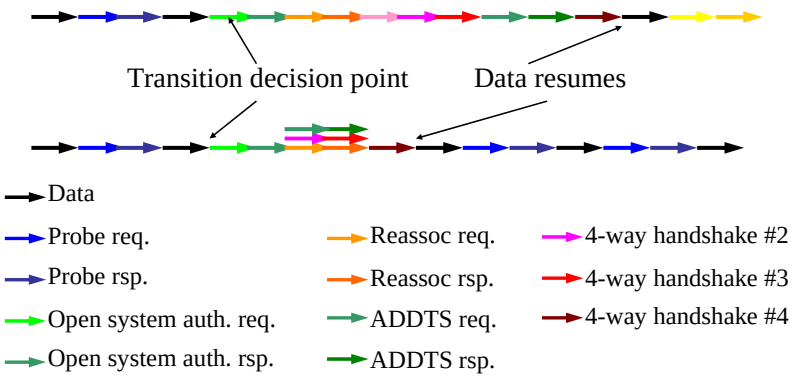


Fig. 7 AP-transition timeline for JIT

Fig. 7 shows the AP-transition timelines for both the traditional (i.e., upper one) and JIT (i.e., lower one) mechanism. We basically observe that with the same transition decision point, the data transmission can resume faster with JIT. As shown in Fig. 7, JIT-enabled station can send reassociation request frame including QoS action information element (IE), such as traffic specification (TSPEC) information [5], which is used in old AP, and optimized 802.11i 4-way handshake message #2, which includes pre-computed PTK[†††]. Upon the reception of the reassociation request frame, a new

[†††] Instead of addressing the new key distribution mechanism proposed in JIT, we just use the term, "pre-computed PTK", because pre-keying scheme (TAP) is considered as a dominant part for the first TGr draft with JIT as *a priori* context transferring scheme. Therefore, you can assume "pre-computed PTK" as the PTK established by pre-keying of TAP, considering the

JIT-enabled AP replies to it with a reassociation response frame with TSPEC information and optimized 802.11i 4-way handshake message #3, which includes GTK. Finally, the station sends optimized 802.11i 4-way handshake message #4.

In Query mechanism, JIT is preceded by a Query phase, which can be enabled with 802.11 authentication frame exchange. With Query, the station transition can be improved under high network load conditions. When the network policy or infrastructure dictates a guaranteed availability of resources, Reservation mechanism can be applied. For a strict guarantee of resource, JIT is preceded with a Reservation phase, which is done over the DS (wireline).

7 Conclusion

In this paper, we have overviewed the mobility support mechanisms of the IEEE 802.11 WLAN. The functions defined in the current standard specifications as well as the emerging recommended practice IEEE 802.11f IAPP. Finally, the current efforts within IEEE 802.11 standardization working group to make the 802.11 handoff faster and more reliable without sacrificing security were briefly summarized.

Reference

[1] IEEE 802.11 Working Group, http://www.ieee802.org/11, on-line.

[2] IEEE Std. 802.11-1999, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*, Reference number ISO/IEC 8802-11:1999(E), IEEE Std 802.11, 1999 edition, 1999.

[3] IEEE Std. 802.11a-1999, *Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHZ Band*, 1999.

[4] IEEE Std. 802.11b-1999, *Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-speed Physical Layer Extension in the 2.4* GHz Band, 1999.

[5] IEEE 802.11e/D13.0, *Draft Supplement to Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Medium Access Control (MAC) Enhancements for Quality of Service (QoS)*, January 2005.

[6] IEEE Std. 802.11f-2003, *Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution System Supporting IEEE 802.11 Operation*, June 2003.

---

coming draft.

[7] IEEE Std. 802.11g-2003, *Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band*, June 2003.

[8] IEEE 802.11g-2003, *Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Control (MAC) Security Enhancements*, 2003.

[9] IEEE 802.11k/D2.0, *Draft Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Specification for Radio Resource Measurement*, February 2005.

[10] IEEE Std. 802.1D-1998, *Part 3: Media Access Control (MAC) bridges*, ANSI/IEEE Std. 802.1D, IEEE 802.1d-1998, 1998 edition, 1998.

[11] IEEE Std. 802.1X-2001, *Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control*, 2001.

[12] RFC 2501, *Mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations*, January 1999.

[13] RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*, June 2000.

[14] R. Moskowitz, *RADIUS Client Kickstart*, draft-moskowitz-radius-client-kickstart-00.txt

[15] C. E. Perkins, *Mobile IP*, IEEE Communications Magazine, May 2002, pp. 66-82.

[16] RFC 3220, *IP mobility support for IPv4*, January 2002.

[17] B. Aboba, *Pre-authentication architecture*, IEEE 802.11-03-0647-00, July 2003.

[18] A. Mishra *et al.*, An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process, *ACM Computer Communication Review*, vol. 33, pp. 93-102, Apr. 2003.

[19] A. Mishra *et al., Fast handoffs using fixed channel probing*, IEEE 802.11-03-0540-00, July 2003.

[20] M. Ryong, F. Watannabe, T. Kawahara and Z. Zhong, *Fast active scan proposals*, IEEE 802.11-03-0623-00, July 2003.

[21] C. R. Wright, *A technique for fast passive scanning*, IEEE 802.11-03-0768-00, September 2003.

[22] M. Lefkowitz, *Neighbor TBTT offset*, IEEE 802.11-03-0860-01, November 2003.

[23] P. Calhoun *et al., Transition Acceleration Protocol (TAP)*, IEEE 802.11-04/1183r1.

[24] N. Cam-Winget *et al., Just-In-Time 2 Phase Association (JIT)*, IEEE 802.11-04/1170-00.

[25] T. S. Rappaport, *Wireless Communications: Principles and Practice*, Second Ed., Prentice Hall, 2002.