802.11i RSN Fast, Secure Roaming

White Paper

Feb 2006
Version 1.00

Author:
Devin Akin, CTO
The CWNP Program
Devin@cwnp.com

Technical Editor:
David Coleman
AirSpy Networks, Inc.
David@AirSpy.com

Introduction

The 802.11i amendment describes the generic process for 802.1X/EAP authentication and key management processes, which includes both generation and distribution of AAA, pairwise, and group keys. For a detailed description of 802.11i Authentication and Key Management (AKM), refer to a whitepaper by the same name by Devin Akin, May 2005 at the CWNP Learning Center at www.cwnp.com.

This whitepaper describes specific features found in the 802.11i amendment that are designed to aid clients in fast roaming while maintaining a secure operating environment. Applications such as VoWLAN are being deployed at a surprising rate, and interoperable fast/secure roaming mechanisms should be deployed by all vendors as a benefit to end users. Most vendors, with some exceptions, are using proprietary fast/secure roaming mechanisms – locking end users into a one-vendor solution throughout the enterprise.

Some useful definitions at this point are:

Pairwise Master Key (PMK) – The highest order key used within the 802.11i amendment. The PMK may be derived from an Extensible Authentication Protocol (EAP) method or may be obtained directly from a Preshared key (PSK).

Pairwise Master Key Security Association (PMKSA) - The context resulting from a successful IEEE 802.1X authentication exchange between the peer and Authentication Server (AS) or from a preshared key (PSK).

PMK Identifier (PMKID) – A number referring to 1) a cached PMKSA that has been obtained through preauthentication with the target AP or 2) a cached PMKSA from an EAP authentication

Pairwise Transient Key (PTK) - A value that is derived from the pairwise master key (PMK), Authenticator address (AA), Supplicant address (SPA), Authenticator nonce (ANonce), and Supplicant nonce (SNonce) using the pseudo-random function (PRF) and that is split up into as many as five keys, i.e., temporal encryption key, two temporal message integrity code (MIC) keys, EAPOL-Key encryption key (KEK), EAPOL-Key confirmation key (KCK).

Pairwise Transient Key Security Association (PTKSA) - The context resulting from a successful 4-Way Handshake exchange between the peer and Authenticator.

Preauthentication – The act of authenticating with an AP to which the STA is currently not associated while the STA is already associated with an AP. If the authentication is left until reassociation time, this may impact the speed with which a STA can reassociate between APs, limiting BSS-transition mobility performance. The use of preauthentication takes the overhead of the authentication service out of the time-critical reassociation process.

Robust Security Network (RSN) – A security network that allows only the creation of robust security network associations (RSNAs). An RSN can be identified by the indication in the RSN Information Element (IE) of Beacon frames that the group cipher suite specified is not wired equivalent privacy (WEP).

4-Way Handshake – A pairwise key management protocol defined by 802.11i-2004. It confirms mutual possession of a pairwise master key (PMK) by two parties and distributes a group temporal key (GTK).

It is purely by coincidence that all relevant definitions start with the letter P. In today's WLAN market, many, even most, vendors implement proprietary fast roaming mechanisms, while the 802.11i amendment offers the same thing as part of its Authentication and Key Management (AKM) scheme. It is the goal of this whitepaper to explain how fast roaming is possible in an 802.11i-compliant ESS without use of additional key management mechanisms or proprietary AKM schemes.

In this document, we will insert an italicized 802.11i amendment section, and then discuss the relevant parts immediately below it. We often highlight parts of the italicized sections in green for emphasis. Our discussions will include screenshots of WLAN protocol analyzer traces.

How PMKSAs and PMKIDs are formed and used

When an RSN-enabled client station successfully authenticates to an RSN-enabled AP (whether autonomous or lightweight with a WLAN switch/controller), a PMKSA is formed and held by both nodes. This PMKSA may be cached for later use or deleted when the station leaves the BSS. Each PMKSA has a unique identifier called a PMKID. The following 802.11i section outlines when and where the PMKID is used.

7.3.2.25.4 PMKID

The PMKID Count and List fields shall be used only in the RSN information element in the (Re)Association Request frame to an AP. The PMKID Count specifies the number of PMKIDs in the PMKID List field. The PMKID list contains 0 or more PMKIDs that the STA believes to be valid for the destination AP. The PMKID can refer to

a) A cached PMKSA that has been obtained through preauthentication with the target AP
b) A cached PMKSA from an EAP authentication
c) A PMKSA derived from a PSK for the target AP

NOTE - A STA can choose not to insert a PMKID in the PMKID List field if the STA does not want to use that PMKSA.

The section above specifies that Association Request and Reassociation Request frames may carry the PMKID in their RSN Information Element (IE). Information Elements are parts of certain types of 802.11 frames that carry relevant information for a specific situation. The RSN IE carries security information about the BSS. From reading this section, we also find out:

- EAP authentications produce PMKSAs
- PMKSAs can be derived from a Preshared Key (PSK)
- STAs and APs may both cache PMKSAs (along with their identifier)
- STAs can choose not to use the PMKID in the (Re)Association Request frame.

If you're wondering what is in a PMKSA, section 8.4.1.1.1below is your answer.

8.4.1.1.1 PMKSA

When the PMKSA is the result of a successful IEEE 802.1X authentication, it is derived from the EAP authentication and authorization parameters provided by the AS. This security association is bidirectional. In other words, both parties use the information in the security association for both sending and receiving.

The PMKSA is created by the Supplicant's SME when the EAP authentication completes successfully or the PSK is configured. The PMKSA is created by the Authenticator's SME when the PMK is created from the keying information transferred from the AS or the PSK is configured. The PMKSA is used to create the PTKSA. PMKSAs are cached for up to their lifetimes. The PMKSA consists of the following elements:
— PMKID, as defined in 8.5.1.2. The PMKID identifies the security association.
— Authenticator MAC address.
— PMK
— Lifetime, as defined in 8.5.1.2.
— AKMP.
— All authorization parameters specified by the AS or local configuration. This can include parameters such as the STA's authorized SSID.

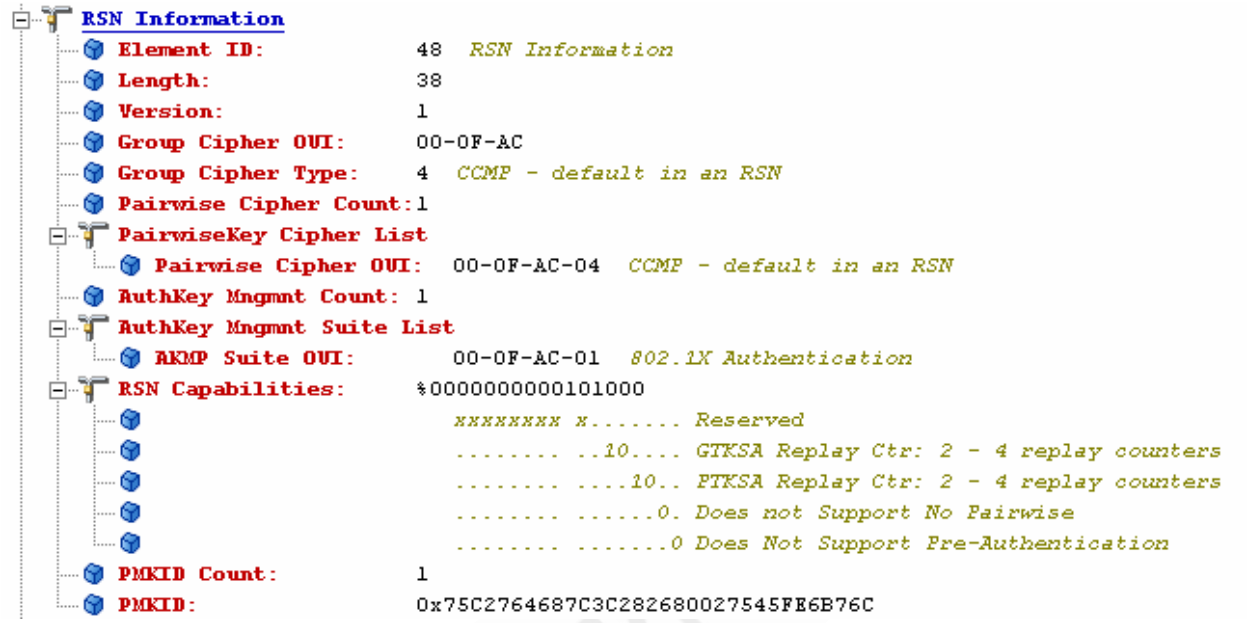
Definition: SME, 802.11-1999 (R2003), Section 10.1

> *In order to provide correct MAC operation, a station management entity (SME) shall be present within each STA. The SME is a layer-independent entity that may be viewed as residing in a separate management plane or as residing "off to the side." The exact functions of the SME are not specified in this standard, but in general this entity may be viewed as being responsible for such functions as the gathering of layer-dependent status from the various layer management entities, and similarly setting the value of layer-specific parameters. SME would typically perform such functions on behalf of general system management entities and would implement standard management protocols.*

Notice the items highlighted in green in this section. It is of particular importance to understand that the PMKSA contains the PMK and the PMKID. Sometimes "PMK" and "PMKSA" are referred to interchangeably by vendors and various documentation, but they are actually different entities within the 802.11i amendment.

In the following figure, you see the RSN IE of an Association Request frame, which includes the PMKID Count and PMKID List (called just "PMKID" in this analyzer). You can see in this Association Request frame that only one PMKID is in the list. In the next section, 8.4.1.2.1, you will see that 1 more PMKIDs may be in the PMKID List, but from practical experience, we can tell you that there's almost always just one in the list. The PMKID listed in the PMKID List is the one cached at the client station specifically for the access point radio (BSSID) to which it wishes to authenticate in the (Re)Association Request frame.

FIGURE 1 (AiroPeek NX)



Let's take a look at 8.4.1.2.1 now. Notice in the second section, it says, "it can include one or more PMKIDs in the RSN information element of its (Re)Association Request frame." This is exactly what we have seen in figure 1.

8.4.1.2.1 Security association in an ESS

A STA roaming within an ESS establishes a new PMKSA by one of three schemes:

— In the case of (re)association followed by IEEE 802.1X or PSK authentication, the STA repeats the same actions as for an initial contact association, but its Supplicant also deletes the PTKSA when it roams from the old AP. The STA's Supplicant also deletes the PTKSA when it disassociates/deauthenticates from all basic service set identifiers (BSSIDs) in the ESS.

— A STA (AP) can retain PMKs for APs (STAs) in the ESS to which it has previously performed a full IEEE 802.1X authentication. If a STA wishes to roam to an AP for which it has cached one or more PMKSAs, it can include one or more PMKIDs in the RSN information element of its (Re)Association Request frame. An AP whose Authenticator has retained the PMK for one or more of the PMKIDs can skip the 802.1X authentication and proceed with the 4-Way Handshake. The AP shall include the PMKID of the selected PMK in Message 1 of the 4-Way Handshake. If none of the PMKIDs of the cached PMKSAs matches any of the supplied PMKIDs, then the Authenticator shall perform another IEEE 802.1X authentication. Similarly, if the STA fails to send a PMKID, the STA and AP must perform a full IEEE 802.1X authentication

— A STA already associated with the ESS can request its IEEE 802.1X Supplicant to authenticate with a new AP before associating to that new AP. The normal operation of the DS via the old AP provides the communication between the STA and the new AP. The STA's IEEE 802.11 management entity delays reassociation with the new AP until IEEE 802.1X authentication completes via the DS. If IEEE 802.1X authentication completes successfully, then PMKSAs shared between the new AP and the STA will be cached, thereby enabling the possible usage of reassociation without requiring a subsequent full IEEE 802.1X authentication procedure.

NOTE: *It is possible for more than one PMKSA to exist. As an example, a second PMKSA may come into existence through PMKSA caching. A STA might leave the ESS and flush its cache. Before its PMKSA expires in the AP's cache, the STA returns to the ESS and establishes a second PMKSA from the AP's perspective.*

Section 8.4.1.2.1 above tells us that a STA roaming within an ESS may establish a new PMKSA by any one of three methods:

1) Full 802.1X/EAP authentication
2) PMK caching
3) Preauthentication via network infrastructure or over the wireless medium

Each of the main points are highlighted in green in the section above. Let's address all three scenarios. First, when a STA first authenticates to an ESS, it must perform a full 802.1X/EAP authentication. This process can be very time-consuming depending on the EAP type and network load conditions. Some EAP authentication exchanges may take over 1 full second to complete. Figure 2 illustrates a full 802.1X/LEAP reassociation that takes 79.8 ms under optimal lab conditions where only one client device is present and the RADIUS authentication server is integrated into the AP (which is under zero data load). Notice the quoted EAP processing time from Cisco Systems' application note Cisco Fast Secure Roaming under Figure 2.

FIGURE 2 (AiroPeek NX)

Packet	Source	Destination	BSSID	Relative Time	Protocol
82	Aironet Wireless C...	Cisco:A5:4F:70	Cisco:A5:4F:70	-0.005157	802.11 Probe Req
83	Cisco:A5:4F:70	Aironet Wireless C...		-0.004843	802.11 Ack
84	Cisco:A5:4F:70	Aironet Wireless C...	Cisco:A5:4F:70	-0.003351	802.11 Probe Rsp
85	Aironet Wireless C...	Cisco:A5:4F:70		-0.003036	802.11 Ack
86	Aironet Wireless C...	Cisco:A5:4F:70	Cisco:A5:4F:70	-0.002350	802.11 Auth
87	Cisco:A5:4F:70	Aironet Wireless C...		-0.002039	802.11 Ack
88	Cisco:A5:4F:70	Aironet Wireless C...	Cisco:A5:4F:70	-0.001781	802.11 Auth
89	Aironet Wireless C...	Cisco:A5:4F:70		-0.001568	802.11 Ack
90	Aironet Wireless C...	Cisco:A5:4F:70	Cisco:A5:4F:70	0.000000	802.11 Reassoc Req
91	Cisco:A5:4F:70	Aironet Wireless C...		0.000314	802.11 Ack
92	Cisco:A5:4F:70	Aironet Wireless C...	Cisco:A5:4F:70	0.000778	802.11 Reassoc Rsp
93	Aironet Wireless C...	Cisco:A5:4F:70		0.000819	802.11 Ack
94	Cisco:A5:4F:70	Aironet Wireless C...	Cisco:A5:4F:70	0.001401	EAP Request
95	Aironet Wireless C...	Cisco:A5:4F:70		0.001444	802.11 Ack
96	Aironet Wireless C...	Cisco:A5:4F:70	Cisco:A5:4F:70	0.053385	EAP Response
97	Cisco:A5:4F:70	Aironet Wireless C...		0.053699	802.11 Ack
98	Cisco:A5:4F:70	Aironet Wireless C...	Cisco:A5:4F:70	0.058302	EAP Request
99	Aironet Wireless C...	Cisco:A5:4F:70		0.058346	802.11 Ack
100	Aironet Wireless C...	Cisco:A5:4F:70	Cisco:A5:4F:70	0.061623	EAP Response
101	Cisco:A5:4F:70	Aironet Wireless C...		0.061937	802.11 Ack
102	Cisco:A5:4F:70	Aironet Wireless C...	Cisco:A5:4F:70	0.065280	EAP Success
103	Aironet Wireless C...	Cisco:A5:4F:70		0.065323	802.11 Ack
104	Aironet Wireless C...	Cisco:A5:4F:70	Cisco:A5:4F:70	0.068301	EAP Request
105	Cisco:A5:4F:70	Aironet Wireless C...		0.068614	802.11 Ack
106	Cisco:A5:4F:70	Aironet Wireless C...	Cisco:A5:4F:70	0.073096	EAP Response
107	Aironet Wireless C...	Cisco:A5:4F:70		0.073139	802.11 Ack
108	Cisco:A5:4F:70	Aironet Wireless C...	Cisco:A5:4F:70	0.073371	802.1x
109	Aironet Wireless C...	Cisco:A5:4F:70		0.073412	802.11 Ack
110	Aironet Wireless C...	Cisco:A5:4F:70	Cisco:A5:4F:70	0.076024	EAPOL-Key
111	Cisco:A5:4F:70	Aironet Wireless C...		0.076338	802.11 Ack
112	Cisco:A5:4F:70	Aironet Wireless C...	Cisco:A5:4F:70	0.077693	802.1x
113	Aironet Wireless C...	Cisco:A5:4F:70		0.077736	802.11 Ack
114	Aironet Wireless C...	Cisco:A5:4F:70	Cisco:A5:4F:70	0.079541	EAPOL-Key
115	Cisco:A5:4F:70	Aironet Wireless C...		0.079855	802.11 Ack

Cisco LEAP Authentication Prior to Fast Secure Roaming
A Cisco LEAP client using Cisco IOS Software version 12.2(8)JA or earlier needs to perform a full Cisco LEAP reauthentication each time it roams. A Cisco LEAP reauthentication requires:

- *A minimum of 100ms*
- *An average of ~600ms*
- *Up to 1.2seconds +*

The timeframes above are in addition to the channel-scanning portion of the L2 roam. Cisco LEAP authentication takes this much time because it requires three roundtrips to a Remote Authentication Dial-In User Service (RADIUS) server using the following process:

- *Client sends identity, Cisco Secure Access Control Server (ACS) or RADIUS Server sends challenge*
- *Client sends challenge response, Cisco Secure ACS sends success*
- *Client sends challenge, Cisco Secure ACS sends challenge response*

In addition to network transit times, each of these roundtrip transactions requires time-consuming cryptographic calculations, hence the total times quoted above.

Cisco Fast Secure Roaming
Application Note, Page 12
Bruce McMurdo, Author
©2004 Cisco Systems

Second, PMK caching is the process of keeping a PMKSA for a period of time after successfully forming an authentication. When a station wishes to roam to another AP, it looks up the BSSID of that AP in its cache hoping to find a PMKID associated with it. If it finds a cached PMKID, then by definition it has a cached PMKSA because the PMKID is part of the PMKSA. If the station wishes to include the PMKID in the (Re)Association Request frame, then it may place it in the RSN IE PMKID List field. Using this feature is optional and up to the discretion of the client station manufacturer. The point of placing the PMKID into the RSN IE of the (Re)Association Request frame is that if the AP also has that particular PMKSA cached, an 802.1X/EAP authentication may be skipped and the authentication may proceed directly to the 4-Way Handshake. Going only through the 4-Way Handshake is many times faster than a full 802.1X/EAP authentication. Reassociations with 4-Way Handshakes are together typically below 100 ms, fast enough for VoWLAN and other time-sensitive applications. Figure 3 illustrates an 802.11i 4-Way Handshake following a reassociation that takes place in 67.88ms (measured from the beginning of the Reassociation Request frame to the ACK following the final EAPoL-Key frame.

FIGURE 3 (AiroPeek NX)

Packet	Source	Destination	BSSID	Relative Time	Protocol
327	Aironet Wireless C...	Cisco:A5:4F:70	Cisco:A5:4F:70	-0.007230	802.11 Probe Req
328	Cisco:A5:4F:70	Aironet Wireless C...		-0.006916	802.11 Ack
329	Cisco:A5:4F:70	Aironet Wireless C...	Cisco:A5:4F:70	-0.005423	802.11 Probe Rsp
330	Aironet Wireless C...	Cisco:A5:4F:70		-0.005108	802.11 Ack
331	Aironet Wireless C...	Cisco:A5:4F:70	Cisco:A5:4F:70	-0.004020	802.11 Auth
332	Cisco:A5:4F:70	Aironet Wireless C...		-0.003709	802.11 Ack
333	Cisco:A5:4F:70	Aironet Wireless C...	Cisco:A5:4F:70	-0.003469	802.11 Auth
334	Aironet Wireless C...	Cisco:A5:4F:70		-0.003256	802.11 Ack
335	Aironet Wireless C...	Cisco:A5:4F:70	Cisco:A5:4F:70	0.000000	802.11 Reassoc Req
336	Cisco:A5:4F:70	Aironet Wireless C...		0.000314	802.11 Ack
337	Cisco:A5:4F:70	Aironet Wireless C...	Cisco:A5:4F:70	0.000821	802.11 Reassoc Rsp
338	Aironet Wireless C...	Cisco:A5:4F:70		0.000862	802.11 Ack
339	Cisco:A5:4F:70	Aironet Wireless C...	Cisco:A5:4F:70	0.001391	802.1x
340	Aironet Wireless C...	Cisco:A5:4F:70		0.001432	802.11 Ack
341	Aironet Wireless C...	Cisco:A5:4F:70	Cisco:A5:4F:70	0.064007	EAPOL-Key
342	Cisco:A5:4F:70	Aironet Wireless C...		0.064321	802.11 Ack
343	Cisco:A5:4F:70	Aironet Wireless C...	Cisco:A5:4F:70	0.065675	802.1x
344	Aironet Wireless C...	Cisco:A5:4F:70		0.065718	802.11 Ack
345	Aironet Wireless C...	Cisco:A5:4F:70	Cisco:A5:4F:70	0.067566	EAPOL-Key
346	Cisco:A5:4F:70	Aironet Wireless C...		0.067881	802.11 Ack
347	Cisco:BF:76:93	Aironet Wireless C...	Cisco:A5:4F:70	0.069596	802.11 TKIP Data

Third, preauthentication with an AP via the network infrastructure enables a STA to stay on-channel while authenticating with nearby APs through the AP to which it is currently connected. Preauthentication via the network infrastructure is also addressed in other 802.11i sections, such as 8.4.6 below. The note found in section 8.4.6 clearly shows us that a STA can preauthenticate over the wired network infrastructure through its current AP.

8.4.6 RSNA authentication in an ESS

NOTE: *A roaming STA's IEEE 802.1X Supplicant may initiate preauthentication by sending an EAPOL-Start message via its old AP, through the DS, to a new AP.*

Preauthentication for Fast Roaming

Let's take a look at the details of how Preauthentication works in 802.11i. The original 802.11-1999 (R2003) standard defined Preauthentication, but gave no details on how it is supposed to work. The 802.11i amendment gives plenty of detail in section 8.4.6.1.

8.4.6.1 Preauthentication and RSNA key management

A STA shall not use preauthentication except when pairwise keys are employed. Preauthentication shall not be used unless the new AP advertises the preauthentication capability in the RSN information element.. When preauthentication is used, then

a) Authentication is independent of roaming.
b) The STA's Supplicant may authenticate with multiple APs at a time.

NOTE: *Preauthentication can be useful as a performance enhancement, as reassociation will not include the protocol overhead of a full reauthentication when it is used.*

Preauthentication uses the IEEE 802.1X protocol and state machines with EtherType 88-C7, rather than the EtherType 88-8E. Only IEEE 802.1X frame types EAP-Packet and EAPOL-Start are valid for preauthentication.

NOTE: *Some IEEE 802.1X Authenticators may not bridge IEEE 802.1X frames, as suggested in C.1.1 of IEEE P802.1X-REV. Preauthentication uses a distinct EtherType to enable such devices to bridge preauthentication frames.*

A STA's Supplicant can initiate preauthentication when it has completed the 4-Way Handshake and configured the required temporal keys. To effect preauthentication, the STA's Supplicant sends an IEEE 802.1X EAPOL-Start message with the DA being the BSSID of a targeted AP and the RA being the BSSID of the AP with which it is associated. The target AP shall use a BSSID equal to the MAC address of its Authenticator.

As preauthentication frames do not use the IEEE 802.1X EAPOL EtherType field, the AP with which the STA is currently associated need not apply any special handling. The AP and the MAC in the STA shall handle these frames in the same way as other frames with arbitrary EtherType field values that require distribution via the DS.

An AP's Authenticator that receives an EAPOL-Start message via the DS may initiate IEEE 802.1X authentication to the STA via the DS. The DS will forward this message to the AP with which the STA is associated. The result of preauthentication may be a PMKSA, if the IEEE 802.1X authentication completes successfully. If preauthentication produces a PMKSA, then, when the Supplicant's STA associates with the preauthenticated AP, the Supplicant can use the PMKSA with the 4-Way Handshake.

Successful completion of EAP authentication over IEEE 802.1X establishes a PMKSA at the Supplicant. The Authenticator has the PMKSA when the AS completes the authentication, passes the keying information (the authentication, authorization, and accounting [AAA] key, a portion of which is the PMK) to the Authenticator, and the Authenticator creates a PMKSA using the PMK. The PMKSA is inserted into the PMKSA cache. Therefore, if the Supplicant and Authenticator lose synchronization with respect to the PMKSA, the 4-Way Handshake will fail. In such circumstances, the MIB variable dot11RSNAStats-4WayHandshakeFailures shall be incremented.

A STA's Supplicant may initiate preauthentication with any AP within its present ESS with preauthentication enabled regardless of whether the targeted AP is within radio range. Even if a STA has preauthenticated, it is still possible that it may have to undergo a full IEEE 802.1X authentication, as the AP's Authenticator may have purged its PMKSA due to, for example, unavailability of resources, delay in the STA associating, etc.

While this text in this section is very straight forward, it would be helpful to have graphics representing some of these steps. The next section will provide the graphics.

Preauthentication over the Network Infrastructure

Figure 4 attempts to illustrate details outlined in section 8.4.6.1 above regarding preauthentication via the network infrastructure.

FIGURE 4

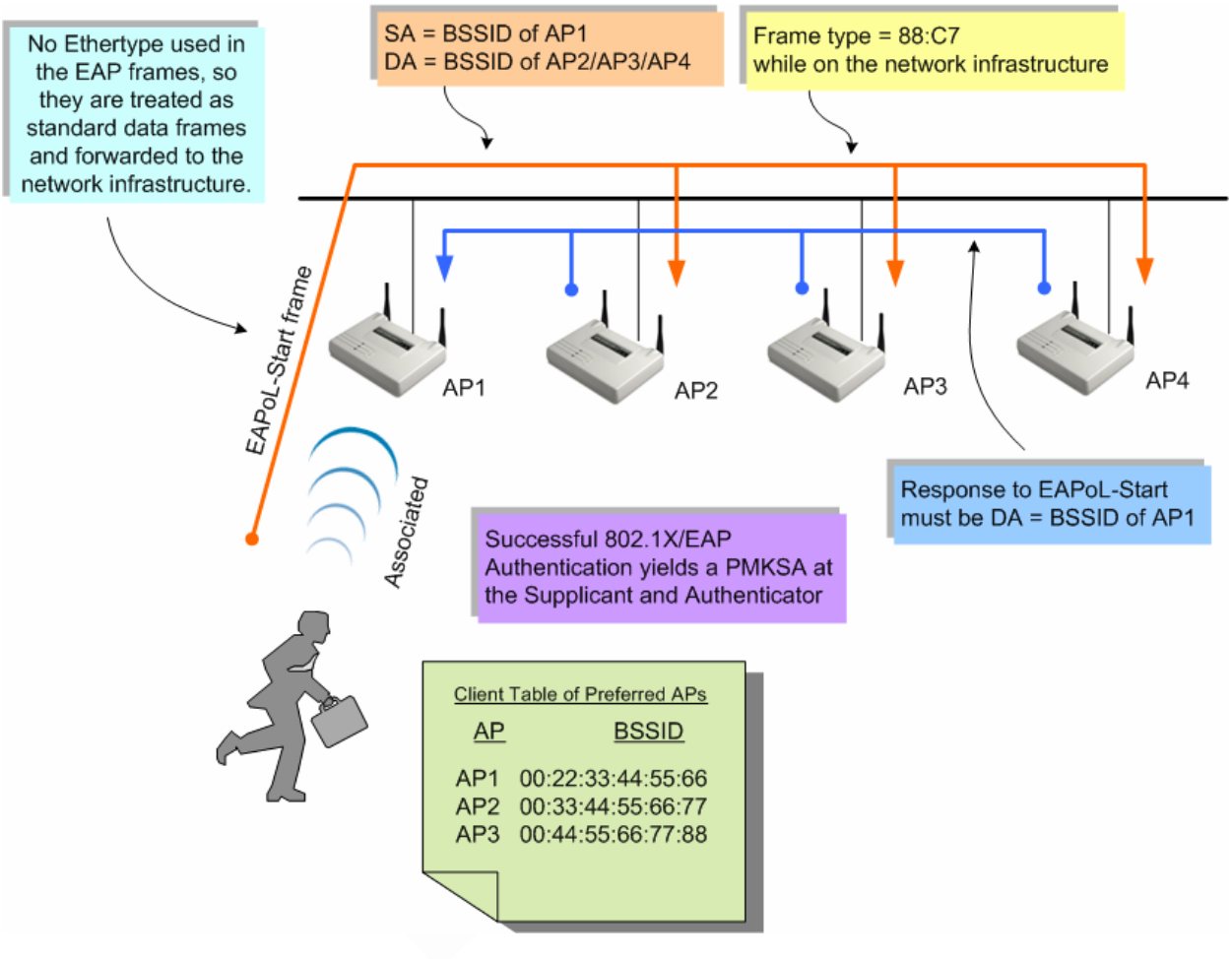


Figure 5 shows preauthentication while it's happening on an Ethernet protocol analyzer over the Ethernet. Not all frames in the exchange are shown in this screenshot.

FIGURE 5 (EtherPeek NX)

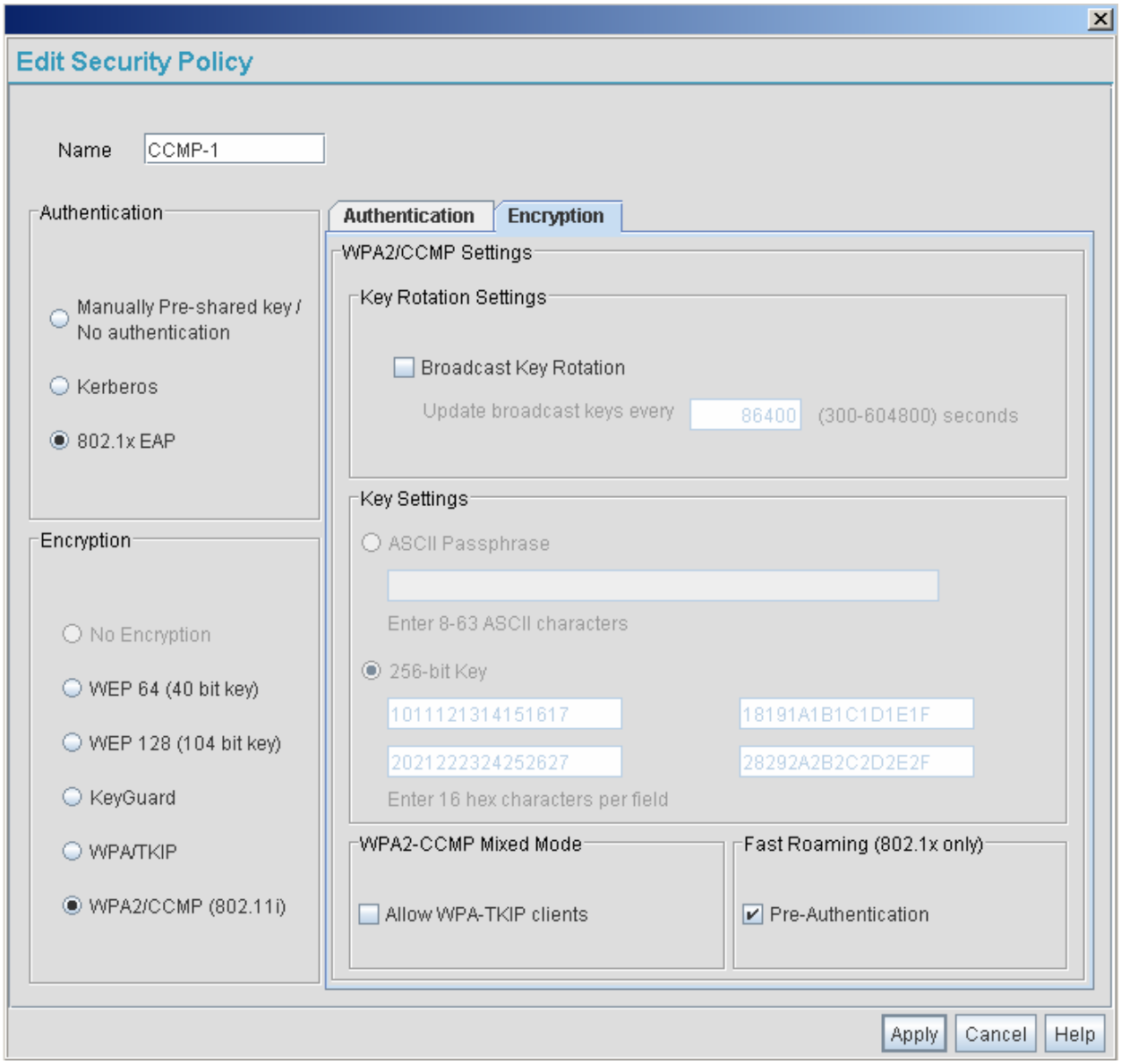
Source	Destination	Protocol	Summary
IP-192.168.100.90	IP-192.168.100.200	RADIUS	C Access Request User:Bo...
IP-192.168.100.200	IP-192.168.100.90	RADIUS	C Access Challenge
Symbol:72:20:D4	Intel Corp:D0:DB:EF	ETHER-88-C7	
Intel Corp:D0:DB:EF	Symbol:72:20:D4	ETHER-88-C7	
IP-192.168.100.90	IP-192.168.100.200	RADIUS	C Access Request User:Bo...
IP-192.168.100.200	IP-192.168.100.90	RADIUS	C Access Challenge
Symbol:72:20:D4	Intel Corp:D0:DB:EF	ETHER-88-C7	
Intel Corp:D0:DB:EF	Symbol:72:20:D4	ETHER-88-C7	
IP-192.168.100.90	IP-192.168.100.200	RADIUS	C Access Request User:Bo...
IP-192.168.100.200	IP-192.168.100.90	RADIUS	C Access Challenge
Symbol:72:20:D4	Intel Corp:D0:DB:EF	ETHER-88-C7	
Intel Corp:D0:DB:EF	Symbol:72:20:D4	ETHER-88-C7	
IP-192.168.100.90	IP-192.168.100.200	RADIUS	C Access Request User:Bo...
IP-192.168.100.200	IP-192.168.100.90	RADIUS	C Access Challenge
Symbol:72:20:D4	Intel Corp:D0:DB:EF	ETHER-88-C7	
Intel Corp:D0:DB:EF	Symbol:72:20:D4	ETHER-88-C7	
IP-192.168.100.90	IP-192.168.100.200	RADIUS	C Access Request User:Bo...
IP-192.168.100.200	IP-192.168.100.90	RADIUS	C Access Challenge
Symbol:72:20:D4	Intel Corp:D0:DB:EF	ETHER-88-C7	
Intel Corp:D0:DB:EF	Symbol:72:20:D4	ETHER-88-C7	
IP-192.168.100.90	IP-192.168.100.200	RADIUS	C Access Request User:Bo...
IP-192.168.100.200	IP-192.168.100.90	RADIUS	C Access Challenge
Symbol:72:20:D4	Intel Corp:D0:DB:EF	ETHER-88-C7	
Intel Corp:D0:DB:EF	Symbol:72:20:D4	ETHER-88-C7	
IP-192.168.100.90	IP-192.168.100.200	RADIUS	C Access Request User:Bo...
IP-192.168.100.200	IP-192.168.100.90	RADIUS	C Access Challenge
Symbol:72:20:D4	Intel Corp:D0:DB:EF	ETHER-88-C7	
Intel Corp:D0:DB:EF	Symbol:72:20:D4	ETHER-88-C7	
IP-192.168.100.90	IP-192.168.100.200	RADIUS	C Access Request User:Bo...
IP-192.168.100.200	IP-192.168.100.90	RADIUS	C Access Challenge
Symbol:72:20:D4	Intel Corp:D0:DB:EF	ETHER-88-C7	
Intel Corp:D0:DB:EF	Symbol:72:20:D4	ETHER-88-C7	
IP-192.168.100.90	IP-192.168.100.200	RADIUS	C Access Request User:Bo...
IP-192.168.100.200	IP-192.168.100.90	RADIUS	C Access Challenge
Symbol:72:20:D4	Intel Corp:D0:DB:EF	ETHER-88-C7	
Intel Corp:D0:DB:EF	Symbol:72:20:D4	ETHER-88-C7	

When a STA has previously performed a full 802.1X/EAP authentication with an AP (whether during association, reassociation, or preauthentication), a PMKSA exists both in the STA and the AP (provided the cache in each has not been dumped). This is true for each STA/AP authentication that has taken place in the ESS. There are rules regarding use of cached PMKSAs, and these are found in 802.11i section 8.4.6.2, discussed in a later section.

Preauthentication Configuration on Infrastructure Devices

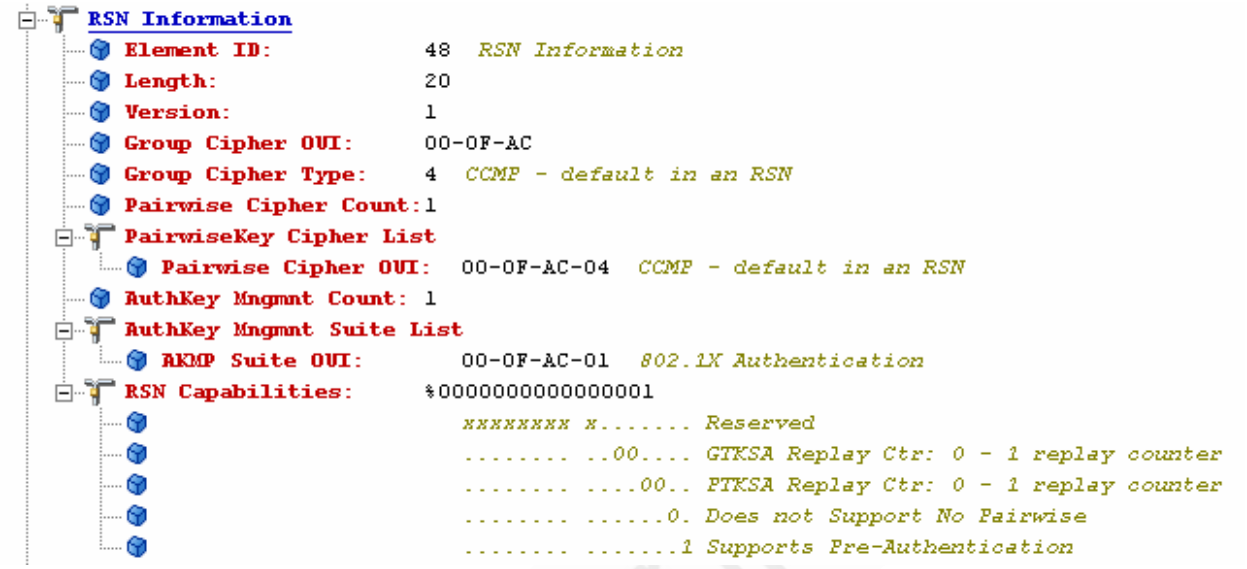
Let's take a look at an autonomous access point that supports preauthentication. Notice the checkbox at the bottom right enabling/disabling preauthentication.

FIGURE 6 (Symbol AP-5131)



Let's take a look at this configuration with a WLAN protocol analyzer. In the RSN Capabilities portion of the RSN IE, Preauthentication is supported, as is illustrated with the 1.

FIGURE 7 (AiroPeek NX)



7.3.2.25.3 RSN capabilities

The length of the RSN Capabilities field is 2 octets. The format of the RSN Capabilities field is as illustrated in Figure 46tc and described after the figure.

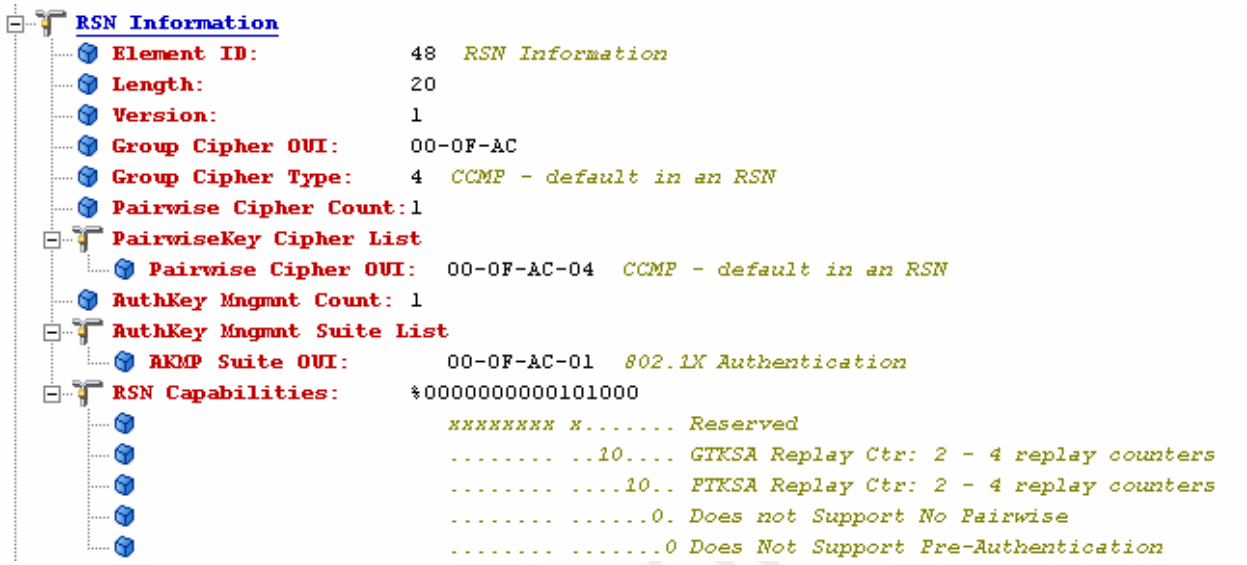
B0	B1	B2 B3	B4 B5	B6 B15
Pre-Auth	No Pairwise	PTKSA Replay Counter	GTKSA Replay Counter	Reserved

Figure 46tc—RSN Capabilities field format

— Bit 0: Pre-Authentication. An AP sets the Pre-Authentication subfield of the RSN Capabilities to 1 to signal it supports preauthentication (see 8.4.6.1) and sets the subfield to 0 when support preauthentication. A non-AP STA sets the Pre-Authentication subfield to 0.

In contrast, figure 8 shows an RSN IE from an AP that has preauthentication disabled.

FIGURE 8 (AiroPeek NX)



Some preauthentication details

First, understand that preauthentication is optional. Some vendors support it, others do not. Preauthentication must be both supported and enabled on the APs and client devices in order to use it in the ESS.

Another important point is focused around the last paragraph in 8.4.6.1 above which says, "*A STA's Supplicant may initiate preauthentication with any AP within its present ESS with preauthentication enabled regardless of whether the targeted AP is within radio range.*" This logically raises the following questions:

1. "How would my client device know of APs outside its radio range?"
2. "How would it benefit my client device to know about radios outside of its radio range?"

Let's start with an example of a vendor who has implemented a feature to address this question in both autonomous APs and WLAN controllers with lightweight APs. Cisco Systems, a leader in Enterprise WLAN systems, offers a proprietary key management scheme called "Cisco Fast Secure Roaming (CFSR)." As part of CFSR when used with autonomous APs, wireless domains (think of a domain as a group) of ≤30 APs are formed. APs to which clients associate send a list of all APs in the domain (which should be the APs in the immediate physical area) to each authenticated client device as they authenticate. See below for the reference.

- *Access points store a maximum list of 30 adjacent access points. This list is aged out over a one-day period.*
- *When a client associates to an access point, the associated access point sends the adjacent access point list to the client as a directed unicast packet.*

Cisco Fast Secure Roaming
Application Note, Page 12
Bruce McMurdo, Author
©2004 Cisco Systems

Since the 802.11i amendment gives the implementer broad (vague) latitude in implementing this feature, Cisco's method of having the authenticator inform the client devices of its surrounding APs is as good as any other method. Any vendor can choose to have their autonomous APs or WLAN switch/controller push such a list of nearby APs to client devices as they authenticate. This feature is simply an addition to the standard that enhances the functionality without negating interoperability. When this feature is present, in whatever form, it is a good thing. Why? Well, that leads to the second question we asked above.

By preauthenticating to all nearby APs over the network infrastructure (through its current wireless connection to an AP), it can assure fast roaming to any number of nearby APs. The primary scenario where the value of this feature breaks down is in high-speed client roaming between autonomous RSN APs. For example, suppose a forklift was moving through a warehouse at 20 mph (32 km/h) where the network was designed with small cells using autonomous APs.

In a case like this, you must remember that preauthentication is up to the client to initiate, each AP (whether autonomous or lightweight) is viewed as a separate AP, and each "preauthentication" is a full 802.1X/EAP authentication. The 802.1X/EAP process can take as much as one full second (depending on the EAP type) and therefore the process of preauthentication simply is not fast enough, even when handled in advanced of a roam, to keep the client device reauthenticating via only the 4-Way Handshake.

PMKSA Caching Rules

8.4.6.2 Cached PMKSAs and RSNA key management

A STA can retain PMKSAs it establishes as a result of previous authentication. The PMKSA cannot be changed while cached. The PMK in the PMKSA is used with the 4-Way Handshake to establish fresh PTKs.

If a non-AP STA in an ESS has determined it has a valid PMKSA with an AP to which it is about to (re)associate, it includes the PMKID for the PMKSA in the RSN information element in the (Re)Association Request. Upon receipt of a (Re)Association Request with one or more PMKIDs, an AP checks whether its Authenticator has retained a PMK for the PMKIDs and whether the PMK is still valid. If so, it asserts possession of that PMK by beginning the 4-Way Handshake after association has completed; otherwise it begins a full IEEE 802.1X authentication after association has completed.

If both sides assert possession of a cached PMKSA, but the 4-Way Handshake fails, both sides may delete the cached PMKSA for the selected PMKID. If a STA roams to an AP with which it is preauthenticating and the STA does not have a PMKSA for that AP, the STA must initiate a full IEEE 802.1X EAP authentication.

The section highlighted in green above is worth paying particular attention to. This shows that it is the client station's decision as to whether or not it initiates fast roaming. The decision is based on whether the client station has a PMKSA corresponding to the BSSID (the MAC address of the AP's radio). For this reason, with 802.11i PMKSA caching, there's no way to pass the PMKSA around from AP to AP or within a WLAN switch/controller because each AP likely has multiple radios, each with their own BSSID. The client would never know to initiate fast roaming in this fashion unless all AP radios had the same BSSID.

Section 8.4.1.2.1 (page 4 above) says, "*An AP whose Authenticator has retained the PMK for one or more of the PMKIDs can skip the 802.1X authentication and proceed with the 4-Way Handshake. The AP shall include the PMKID of the selected PMK in Message 1 of the 4-Way Handshake.*" Section 8.5.3.1.4 (shown below) illustrates the contents of Message 1 in the 4-Way Handshake with the PMKID highlighted in green. Figure 9 illustrates a frame decode of Message 1 in the 4-Way Handshake with the same information highlighted in blue.

8.5.3.1 4-Way Handshake Message 1

Message 1 uses the following values for each of the EAPOL-Key frame fields:
Descriptor Type = N – see 8.5.2
Key Information:
Key Descriptor Version = 1 (RC4 encryption with HMAC-MD5) or 2 (NIST AES key wrap with HMAC-SHA1-128)
Key Type = 1 (Pairwise)
Install = 0
Key Ack = 1
Key MIC = 0
Secure = 0
Error = 0
Request = 0
Encrypted Key Data = 0
Reserved = 0 – unused by this protocol version
Key Length = Cipher-suite-specific; see Table 20f
Key Replay Counter = n – to allow Authenticator to match the right Message 2 from Supplicant
Key Nonce = ANonce
EAPOL-Key IV = 0
Key RSC = 0
Key MIC = 0
Key Data Length = 22
Key Data = PMKID for the PMK being used during this exchange

The Authenticator sends Message 1 to the Supplicant at the end of a successful IEEE 802.1X authentication, after PSK authentication is negotiated, when a cached PMKSA is used, or after a STA requests a new key. On reception of Message 1, the Supplicant determines whether the Key Replay Counter field value has been used before with the current PMKSA. If the Key Replay Counter field value is less than or equal to the current local value, the Supplicant discards the message. Otherwise, the Supplicant

a) Generates a new nonce SNonce.
b) Derives PTK.
c) Constructs Message 2.

FIGURE 9 (AiroPeek NX)

Client Configuration of PMK Caching and Preauthentication

The latest generation of vendor client utilities range greatly in their configuration parameters for PMK (or PMKSA) caching and preauthentication, and some have none at all. In cases like that, it's sometimes advantageous to let the operating system's integrated client utilities handle these matters. Let's look at Microsoft's WPA2-compliant Wireless Zero Configuration (WZC) Service as part of the Windows XP operating system with service pack 2 and the WPA2/WPS IE update. Figure 10 illustrates WZC's configuration parameters for:

- **PMKCacheMode** - PMK Cache enable/disable
- **PMKCacheTTL** - How long the PMK will be cached
- **PMKCacheSize** - How many PMKs can be stored in the PMK cache
- **PreAuthMode** - Preauthentication enable/disable
- **PreAuthThrottle** - To how many candidate APs the client will attempt to preauthenticate

Many client adapter drivers allows WZC to control the wireless radio's operation. In cases where the vendor's client utilities do not have adequate PMK Caching and Preauthentication configuration parameters, and they are needed, then letting the WZC client utility control the radio card would be beneficial. It should noted, however, that many published security risks exist with the WZC therefore many government agencies and corporations maintain security policies restricting the use of the WZC.

FIGURE 10 (Microsoft, Article ID 893357)

Registry values that control preauthentication and PMK caching

The following registry entries in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EAPOL\Parameters\General\Global subkey control the behavior of preauthentication and PMK caching for the WPA2/WPS IE Update:

- PMKCacheMode
- PMKCacheTTL
- PMKCacheSize
- PreAuthMode
- PreAuthThrottle

PMKCacheMode

Value type: REG_DWORD - Boolean
Valid range: 0 (disabled), 1 (enabled)
Default value: 1
Present by default: No
Description: Specifies whether a Windows XP-based wireless client will perform PMK caching. By default, PMKCacheMode is enabled.

PMKCacheTTL

Value type: REG_DWORD
Valid range: 5-1440
Default value: 720
Present by default: No
Description: Specifies the number of minutes that an entry in the PMK cache can exist before being removed. The maximum value is 1440 (24 hours). The default value is 720 (12 hours).

PMKCacheSize

Value type: REG_DWORD
Valid range: 1-255
Default value: 100
Present by default: No
Description: Specifies the maximum number of entries that can be stored in the PMK cache. By default, the PMK cache has 16 entries.

PreAuthMode

Value type: REG_DWORD - Boolean
Valid range: 0 (disabled), 1 (enabled)
Default value: 0
Present by default: No
Description: Specifies whether a Windows XP-based wireless client will try preauthentication. By default, PreAuthMode is disabled.

PreAuthThrottle

Value type: REG_DWORD
Valid range: 1-16
Default value: 3
Present by default: No
Description: Specifies the number of top candidate wireless access points with which the Windows XP-based computer will try preauthentication. The value is based on the ordered list of the most favored wireless access points, as reported by the wireless network adaptor driver. By default, PreAuthThrottle has a value of 3.

Note Changes to any one or more of these registry entry values do not take effect until the next time that you restart the wireless service or the next time that you restart the computer.

Opportunistic PMK Caching

Microsoft has recently released a feature in Windows XP (with service pack 2 and the WPA2/WPS IE update) called Opportunistic PMK Caching. This feature is also supported by some WLAN infrastructure vendors such as Colubris and Symbol in their WLAN switch products and by Funk Software (now part of Juniper Networks). In this section, we will discuss what happens in an autonomous AP architecture when Opportunistic PMK Caching is used, and then we will proceed with how it is used in a WLAN switching architecture.

Autonomous AP Scenario:

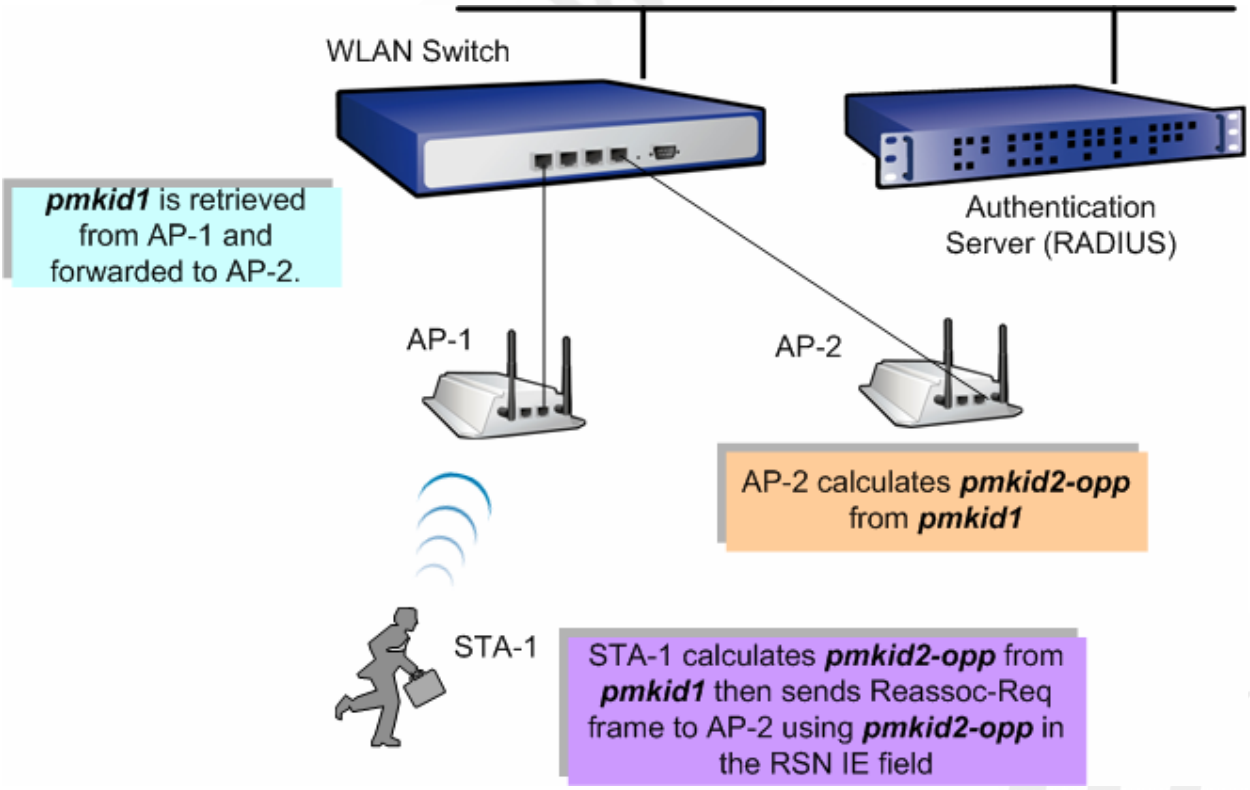
When authenticating to the network for the first time, STA-1 performs a full 802.1X/EAP authentication which yields a PMK on STA-1 and AP-1. The Pairwise Master Key Identifier (PMKID) is a hash generated from part of the PMK, the MAC address of the STA and the BSSID of the AP. When STA-1 wishes to roam from AP-1 to AP-2, it calculates an Opportunistic PMKID, ***pmkid2-opp***, based on the first PMK, its own MAC, and the BSSID of AP-2, and sends this in its Reassociation Request frame to AP-2. Since none of the APs are connected to a centralized control point (like a WLAN switch), AP-2 doesn't know the PMK from STA-1's first association. It therefore has no way to compute ***pmkid2-opp***, so it

ignores the fast reauthentication request from STA-1 and forces the client to perform a full 802.1X/EAP authentication. **Conclusion**: Opportunistic PMK Caching does not work in the autonomous AP architecture.

WLAN Switch Scenario:

Refer to figure 11 for this scenario. When authenticating to the network for the first time, STA-1 performs a full 802.1X/EAP authentication which yields a PMK (let's call it ***pmkid1***) on STA-1 and AP-1. When STA-1 wishes to roam from AP-1 to AP-2, it calculates an Opportunistic PMKID, ***pmkid2-opp***, based on the ***pmkid1***, its own MAC, and the BSSID of AP-2. In a wireless switch environment, the switch has access to all PMKs from all connected access points. The WLAN switch immediately retrieves ***pmkid1*** from AP-1 and forwards it to access points in the area around AP-1. When STA-1 sends a Reassociation Request frame to AP-2 with ***pmkid2-opp*** in the RSN IE, AP-2 calculates ***pmkid2-opp*** from ***pmkid1***. Both STA-1 and AP-2 could then proceed with the 4-Way Handshake. This practice of building all future PMKs based on the first PMK allows fast, secure roaming throughout the ESS almost indefinitely provided the first PMKSA expires neither on the AP nor the client station. **Conclusion**: Opportunistic PMK Caching is the most widely implemented fast BSS transition method available and should be widely deployed by WLAN switch vendors at least until the 802.11r amendment is ratified.

FIGURE 11



NOTE: WZC with the WPA2/WPS IE update may not always behave predictably. Even if a station has a PMKSA cached for a particular AP to which it wants to roam does not mean it has to use a PMKID in the Reassociation Request frame – it's optional. As an added security advantage, a STA or an AP can, ***at any time***, decide to invalidate a cached PMKSA. This forces a STA to perform a new full 802.1X/EAP authentication.

I feel that it's important for large volume, enterprise-class client radio vendors such as Intel, Broadcom, and Atheros to offer additional configuration parameters such as those found in WZC so that the consumer has a choice of client utilities for environments that cannot tolerate authentication latency during roaming.

Summary

The 802.11i amendment gives equipment manufacturers an arsenal of tools with which to allow fast, secure roaming of client stations between APs – regardless of whether autonomous APs or WLAN switches are in use. Using PMKSA caching with preauthentication and opportunistic PMK caching (when WLAN switches are available), handoff speeds are easily fast enough for demanding VoWLAN and other time-sensitive applications. There are many proprietary key management schemes currently on the market, but I can see no valid advantages over the standards-based solution described in this whitepaper. For the WLAN market to continue with steady growth, standardized, fast, secure roaming mechanisms must be industry-developed and implemented by the majority of vendors. Today, most vendors think their proprietary technology is not only better, but easily justified even in the face of standards-based, fast, secure roaming solutions. I firmly disagree with their stance.