

SECURING ENTERPRISE AIR: UNDERSTANDING AND ACHIEVING NEXT-GENERATION WIRELESS SECURITY WITH SYMBOL TECHNOLOGIES AND 802.11i

TECHNICAL WHITE PAPER

February 2005

Wireless networking is quickly becoming a defacto standard in the enterprise, streamlining business processes to deliver increased productivity, reduced costs and increased profitability. Security has remained one of the largest issues as companies struggle with how to ensure that data is protected during transmission and the network itself is secure. Wi-Fi Protected Access (WPA) offered an interim security solution, but was not without constraints that resulted in increased security risks. The new WPA2 (802.11i) standards eliminate these vulnerabilities and offer truly robust security for wireless networks. As a global leader in wireless networking, Symbol not only offers this next-generation of wireless security—but also builds on the new standard with value-added features that further increase performance and the mobility experience for all users.

OVERVIEW

Corporations are increasingly being asked to allow wireless network access to increase business productivity, and corporate security officers must provide assurance that corporate data is protected, security risks are mitigated and regulatory compliance is achieved. This whitepaper will discuss:

- The risks of wireless insecurity
- The progression of security standards and capabilities pertaining to Wi-Fi security
- How the 802.11i standard provides robust security for demanding wireless environments
- How Symbol Technologies incorporates 802.11i in its switching products in a way that optimizes scalability, performance and investment protection

Many of the terms used in this whitepaper are defined in the glossary in Appendix A.

RISKS OF WIRELESS INSECURITY

The advent of wireless computing and the massive processing power available within portable devices provides organizations with an unprecedented ability to provide flexible computing services on-demand to enable business initiatives. While functionality is being rapidly adopted, the process complicates the ability of IT departments to control their own Intranets and enforce their own standards. Where the high performance computers of yesterday required a dedicated room and special environmental controls, today's computers arrive via a visitor's pocket or traveling employee's notebook, and require no hard-wired connections to reach the corporate Intranet.

With this great mobile computing power and flexibility comes major risk. War driving can enable hackers to obtain unauthorized access to corporate resources and proprietary intellectual property. The login credentials of legitimate wireless users can be sniffed or cracked. Malicious insiders can move throughout an enterprise network with impunity via sessions with insecure wireless access points.

The consequences of these risks are significant. We have seen spammers and phishers leverage open access points to send unsolicited and malicious electronic mail in stealth mode. Worms are introduced through a new infection vector. Customer lists and account numbers are routinely downloaded to portable devices. Enterprise databases are accessed and modified by unauthorized users.

The bottom line is that wireless insecurity, as long as it is unaddressed, enables the theft of data, lowers productivity, and causes quantifiable financial losses.

UNDERSTANDING WI-FI PROTECTED ACCESS (WPA)

Created by Symbol and other Wi-Fi Alliance vendors, WPA was based on an early draft of IEEE 802.11i to address critical flaws in WEP. These security shortcomings required an interim solution that would not require hardware upgrades or replacements for existing consumer devices. A series of compromises was made in order to “fix” WEP through software-based firmware upgrades. The majority of existing WEP devices had extremely minimal CPU resources, often based on sub-40 MHz chips based on older hardware such as the 80486. As these devices are typically incapable of encryption work, the implementation of RC4 for WEP was often offloaded onto secondary chips. This is a primary consideration. The replacement for WEP must still use RC4 and RC4 primitives for any and all encryption. The main problems with WEP are:

- WEP does not prevent forgery of packets.
- WEP does not prevent replay attacks. An attacker can simply record and replay packets as desired and they will be accepted as legitimate.
- WEP uses RC4 improperly. The keys used are very weak, and can be brute-forced on standard computers in hours to minutes, using freely available software.
- WEP reuses initialization vectors. A variety of available cryptanalytic methods can decrypt data without knowing the encryption key.
- WEP allows an attacker to undetectably modify a message without knowing the encryption key.

WPA TKIP

The IEEE’s primary response to the problems of WEP was Temporal Key Integrity Protocol (TKIP). TKIP acts as a wrapper for WEP, adding a layer of security around WEP’s otherwise weak encryption.

One of the first problems TKIP solves is that of key length. WEP uses small keys, and their effective length is shorter due to several design flaws. TKIP uniformly uses a 128-bit encryption key, and while WEP can support 128-bit encryption keys, maintaining compatibility with older WEP devices inevitable leads to standardization upon 64-bit encryption keys within a wireless network. However, TKIP still makes use of RC4, a relatively weak encryption algorithm that was used due to hardware constraints on most of the devices originally designed to provide WEP.

TKIP also reduces the chance of replay attackers. TKIP expands the initialization vector (IV) to 48 bits from 24 bits, and combines this IV with the fixed key in a more cryptographically secure manner. Using a 48-bit IV means that any particular value of the IV can not be duplicated with a

particular key. Thus, packets cannot be replayed. Guaranteeing that a particular key-IV pair is never reused also denies an attacker the ability to capture multiple packets that are identically encrypted, which would lead to the ability to extract the plain text messages.

Further, TKIP addresses WEP’s use of a single key by all clients. To create a base key, TKIP uses either a passphrase or a master key derived from the authentication process, and several other pieces of information, such as a client’s MAC address. This base key in turn is used with the IV to create per-packet keys. So in theory, every packet sent over WPA is encrypted by a separate and unique key.

Finally, TKIP takes on weaknesses in key deployment by creating a base key that is different for each client. A client provides a shared secret for authentication and various other pieces of information. On wireless networks secured using WEP, all clients constantly use the same key, providing a large amount of cipher text for attackers to analyze. This also increases the probability of reuse of the 24-bit IV, exposing encrypted messages to attackers.

One fundamental problem continues for networks that have switched from WEP to WPA, or deployed WPA directly, yet do not use authentication. The initial passphrase or secret deployed on clients and access points is often weaker than needed, since it usually must be human-readable and entered by a human. This immediately limits the passphrase or secret to a subset of readable characters that can easily be entered from the keyboard. Furthermore, the length is often limited to 20 characters or less due to the difficulties associated with remembering or entering long strings of seemingly random text.

It is important to note that if robust authentication methods are not used with WPA, it must rely upon Pre-Shared Keys (PSK). The same secret phrase must be entered on all clients and all access points. This carries forward the key management issues inherent in WEP. In addition, it is virtually impossible to securely distribute the key or passphrase, as the secret information must be provided to all clients. A single malicious client can use this data to compromise other client sessions. Unfortunately, WPA-PSK is relatively common due to the lack of a need for a separate authentication system.

802.1X – User Authentication and Network Access

In an attempt to address the lack of user authentication in WEP, support for the 802.1X protocol was added to WPA. The 802.1X

protocol was originally designed for wired networks and only facilitates authentication, therefore it cannot guarantee secure authentication on wireless networks.

The first problem with 802.1X in a wireless network is that an attacker has access to the authentication packets sent and received by clients. If weak authentication methods are used (several are supported) or weak encryption is used (such as RC4), it may be possible for an attacker to discover the authentication credentials.

The second problem is that an attacker can execute a man-in-the-middle attack on the 802.1X authentication sequence. On a wired network this attack would be far more difficult, as an attacker would need physical access to the cable in between the client and the switch being accessed. On a wireless network, anyone within broadcast range has the ability to access. An attacker could be several hundred feet away with directional antennas. We will discuss in the later section “WPA2: Under the Covers” how implementation of Extensible Authentication Protocol (EAP) methods such as TLS can mitigate against possible man-in-the-middle attacks.

The third problem is that an attacker can execute denial-of-service attacks against clients by sending packets to the wireless access point, telling it to drop the client connection. On a wired network, this would again require access to the physical cable between the client and the switch.

The fourth problem is that with hard-wired devices, 802.1X will drop the port if the interface goes down — that is, if the cable is unplugged, or the device at the endpoint is not responsive. However, on wireless networks the status of the physical link condition cannot be trusted. An attacker can access the physical medium used to transmit the signal — the air, for example. Thus anyone within broadcast range could execute a denial-of-service attack against a client system and then take the client’s place before the wireless access point notices.

Additionally, attackers can send disassociation messages to wireless clients, preventing them from disconnecting properly from the access point by sending an 802.1X EAPOL Logoff message.

WPA Cracking Tools

There are a number of WPA cracking tools which attempt to determine the initial shared secret when WPA-PSK is used. Once this secret is known, the base key and session keys can be recreated, and traffic to and from clients and the access point can be decrypted on the fly. Alternatively, attackers can record traffic and then mount an offline attack at a later time, allowing use of greater computational resources.

For the majority of these tools to work, the attacker must be able to monitor the entire initial key exchange. An attacker who starts monitoring wireless traffic while clients are already connected will not be able to gather the proper data to crack the WPA encryption. However, it is relatively simple for an attacker to create a denial-of-service condition by sending disassociation packets to the clients. The clients then disconnect and reconnect, re-authenticating in the process and enabling attackers to view the needed data.

WPA Summary

WPA is generally accepted as an interim step to provide incrementally improved security until WPA2 is available. Most devices that were upgraded to WPA capability are not capable of further upgrades. These devices are generally hardware-constrained, with minimal processing power and with RC4 as the only onboard encryption option.

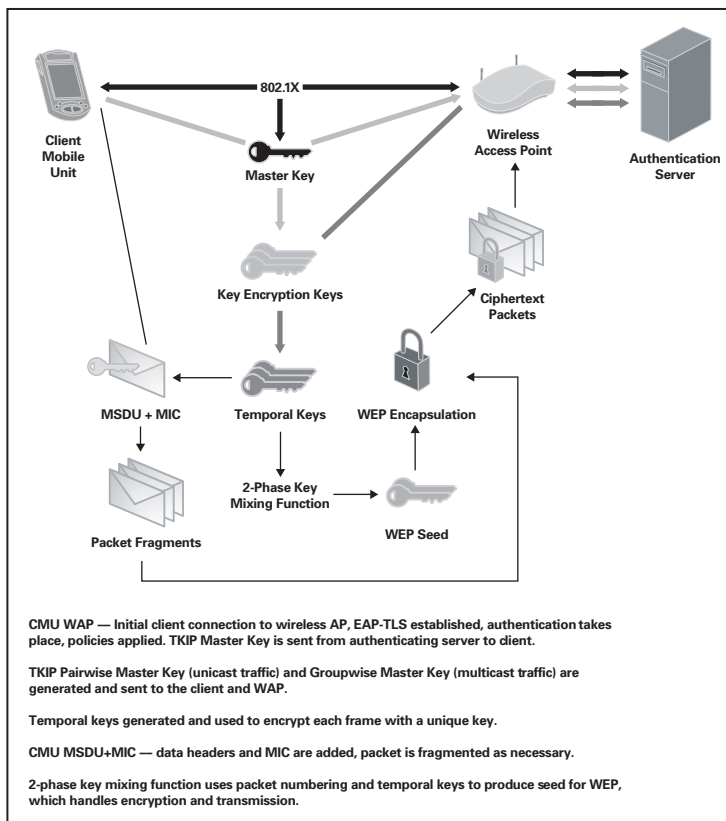


Figure 1 — WPA TKIP

THE WAY FORWARD

Wi-Fi Protected Access 2 (WPA2) and 802.11i

The 802.11i standard is virtually identical to WPA2, and the terms are often used interchangeably. 802.11i and WPA2 are not just the future of wireless access authentication — they are the future of wireless access. Wireless access is still in its infancy, in spite of the purchase and deployment of several million access points and wireless clients. The majority of these access points and clients are relatively immobile. Users sit down with their laptops at a conference table and connect, or a clerk stays within a relatively small area such as a warehouse, using wireless equipment to track inventory.

Increased Density of Access Points

Wireless access in the future will feature increased density of access points. There are several reasons for this, including a greater need for bandwidth. An area covered by a single access point will not be able to provide as much bandwidth to clients as two access points. Also, in office buildings and other areas with stores located near each other, access points are typically not shared, but deployed separately within each location. Some residential areas already have multiple access points on each block. Finally, increased density benefits availability. If two or more access points cover an area and one of the access points fail, the area retains some degree of coverage.

Considering these factors, organizations will likely use more than one access point to cover a given area. But increasing the number of access points without a strategy for centralized management creates additional security risks. Robust management of access points is a key design requirement for Symbol Technologies in the implementation of 802.11i-based products.

Roaming Wireless Clients

Critical to 802.11i is the addition of fast secure roaming support for clients. This assists Voice-over-IP (VoIP) and other mobile applications that require continuous access. While some wireless 802.11 equipment currently supports fast secure roaming, it is usually vendor-specific, as no official standard existed prior to 802.11i that supported this function.

Currently, most wireless clients are relatively immobile, as few truly portable devices have come into use. Laptop users generally sit down at fixed locations to use their systems. However, in the future, more wireless devices (such as phones and PDAs) will support 802.11—and these devices must roam. Also, due to the data types such portable roaming devices will likely carry, such as live voice and video, users will immediately notice any interruptions in service. And if such interruptions are common, the viability and use of live voice and video services becomes untenable. For network providers, access must be smooth and seamless while clients are roaming.

Failover Requirements

Robustness and availability are commonly forgotten yet important aspects of wireless networks. The majority of wireless networks have no failover or redundancy capabilities other than manual connection to a new access point when the one in use fails. As more wireless networks are deployed to carry critical traffic such as phone calls via the VoIP protocols, reliability and robustness will become more important. One benefit of 802.11i roaming support is that a client has de facto support to connect seamlessly to a new access point should the one in use fail. Of course, this will require service coverage of areas by one or more access points, but with costs falling, this is not a serious issue.

WPA2: UNDER THE COVERS

WPA was provided as an interim solution, and it had a number of major constraints. WPA2 was designed as a future-proof solution based on lessons learned by WEP implementers. Symbol Technologies is a key contributor and proponent of the WPA2 standard, and provides next-generation products based on this standard.

WPA2 will be a durable standard for many reasons. One of the most important choices was that of the encryption algorithm. In October 2000, the National Institute of Standards and Technology (NIST) designated the Advanced Encryption Standard (AES) as a robust successor to the aging Data Encryption Standard. AES is an extremely well-documented international encryption algorithm free of royalty or patent, with extensive public review.

WPA2, like WPA, supports two modes of security, sometimes referred to as “home user” and “corporate.” In “home user” mode a pre-shared secret is used, much like WEP or WAP. Access points and clients are all manually configured to use the same secret of up to 64 ASCII characters, such as “this_is_our_secret_password.” An actual 256-bit randomly generated number may also be used, but this is difficult to enter manually into client configurations.

The “corporate” security is based on 802.1X, the EAP authentication framework (including Radius), one of several EAP types (such as EAP/TLS, which provides a much stronger authentication system), and secure key distribution. This paper discusses “corporate” security. “Home user” security introduces the same security problems present in WEP and WPA-PSK.

WPA2 and 802.1X

While 802.1X as a standard preceded 802.11i, it is proving to be a key enabler for secure and flexible wireless networks, allowing for client authentication, wireless network authentication, key distribution and the pre-authentication necessary for roaming. In using 802.1X in conjunction with 802.11i, it is strongly suggested to use EAP as a framework for authentication, and use an EAP type for the actual authentication that provides the optimal balance between cost, manageability and risk mitigation. Most often an 802.1X setup uses EAP-TLS for authentication between the wireless client (supplicant) and the access point (authenticator). In theory, several options may replace EAP-TLS, but in practice this is rare.

The 802.1X authentication protocol as deployed with 802.11i provides a number of services:

- Capabilities negotiation between the client and wireless network provider
- Client authentication to the wireless network provider
- Authentication of the wireless network provider to the client
- A key distribution mechanism for encryption of wireless traffic
- Pre-authentication for roaming clients

In wired 802.1X, the network port is in a controlled state prior to authentication. But on wireless networks no such port exists until the client connects and associates to the wireless access point. This immediately poses a problem, since beacon packets and probe request/response packets

cannot be protected or authenticated. Fortunately, access to this data is not very useful for attackers, other than for potentially causing denial-of-service attacks, and for identifying wireless clients and access points by their hardware MAC addresses.

An 802.1X wireless setup consists of three main components:

- Supplicant (the wireless client)
- Authenticator (the access point)
- Authentication server (usually a Radius server)

The supplicant initially connects to the authenticator, as it would to a WEP- or WPA-protected network. Once this connection is established, the supplicant has in effect a network link to the authenticator (access point). The supplicant can then use this link to authenticate and gain further network access. The supplicant and authenticator first negotiate capabilities. These consist of three items:

- The pairwise cipher suite, used to encrypt unicast (point-to-point) traffic
- The group cipher suite, used to encrypt multicast and broadcast (point-to-multiple-points) traffic
- The use of either a pre-shared key (PSK, or “home user” security, using a shared secret) or 802.1X authentication

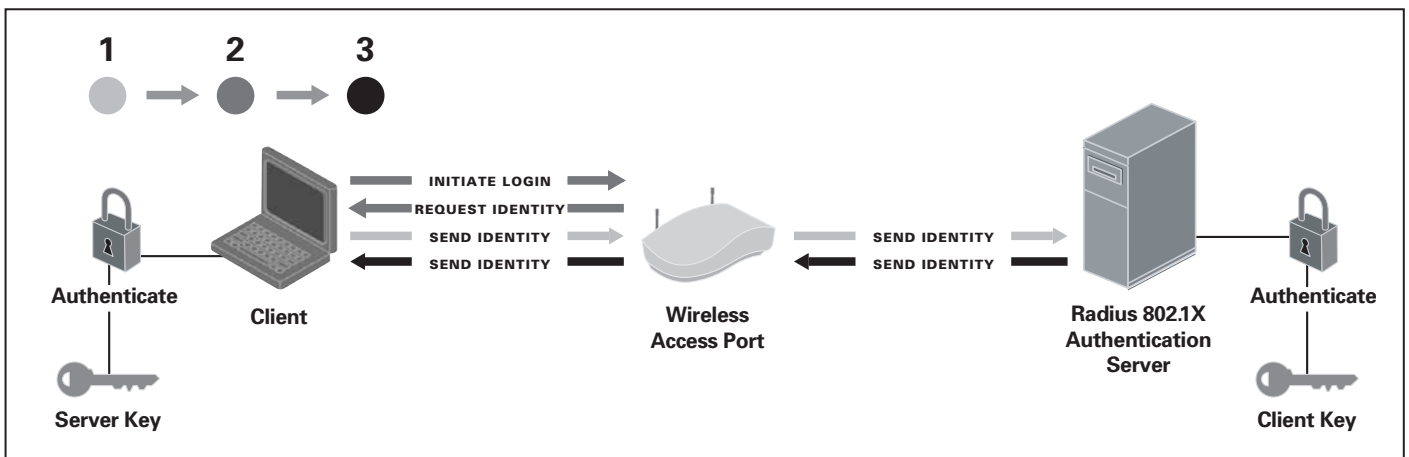


Figure 2 — 802.1X

Once a common set of capabilities is agreed upon — and assuming the network uses 802.1X — the supplicant and the authenticator begin the authentication process. At this point, wireless encryption keys have not been exchanged and the exchange is in the clear. It is EAP-TLS that comes into play to protect this data, providing the essential SSL encryption. Signable X.509 certificates add the benefit of allowing the supplicant to prove its identity to the authenticator, and vice versa.

Several problems arise from the constraints of wireless networking. First, the supplicant must have local copies of the root certificates used by the certificate authority to sign the authenticator's certificate. Because the authenticator (the wireless access point) fully controls the supplicant's access to the network, a hostile authenticator can modify or redirect traffic in any way, and could point the user to fake certificate authority sites. Even if the supplicant has a local copy of the root certificate used to sign the authenticator's certificate, a compromised certificate placed in a certificate revocation list (CRL) may not be detected if the authenticator provides the supplicant with false or old CRL data. Therefore, any compromised authenticator certificates pose a significant risk to wireless network clients, especially since many will not check for certificate revocation.

The key exchange consists of a Master Key (MK) generated on the authentication server and in the supplicant. The MK is sent to the authenticator. The Pairwise Master Key (PMK) is generated from the MK and the Group Master Key (GMK) is generated by the authenticator. The PMK and GMK keys are then used as needed to generate temporal keys, used to encrypt individual frames sent on the wireless network. These keys are known as Pairwise Transient Keys (PTK) and Groupwise Transient Keys (GTK).

The PTK is used to encrypt traffic to and from the supplicant and the authenticator. The GTK is used to encrypt broadcast or multicast traffic sent to all hosts on a particular wireless network.

The actual connection, authentication and key exchange for a system using EAP-TLS appears in Appendix B.

WPA2 and TKIP

WPA2 supports the use of the TKIP encryption scheme to provide backward compatibility with WPA equipment. As 802.11i equipment becomes ubiquitous, networks will drop support for TKIP and WPA, removing a number of potential security vulnerabilities.

TKIP uses a new key for each frame that is encrypted; the keys used to encrypt these frames are called either the Pairwise Temporal Key (for unicast traffic) or Groupwise Temporal Key (for multicast and broadcast traffic). These keys are generated from the Pairwise Master Key (PMK) and Groupwise Master Key (GMK).

The majority of weaknesses in TKIP under WPA are due to a weak encryption algorithm. This problem is securely addressed with TKIP under WPA2. By using 802.1X and EAP-TLS to handle key distribution, keys are transferred securely and are not as prone to attack. The use of an extremely strong cipher, AES, addresses the weaknesses of RC4. Finally, the use of strong key lengths, 128 bits, significantly reduces the chance of a successful brute force attack against AES-encrypted wireless traffic.

WPA2 and CCMP

Moving forward, the 802.11i (and by extension WPA2) standards call for the use of Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), which specifies use of CCM with the AES block cipher. CCM is a general-purpose cipher mode that does not specify the block cipher to use. The CBC-MAC portion provides data integrity and authentication while the counter mode does the actual encryption, protecting the data from eavesdroppers. It is expected that TKIP (using RC4) will be phased out in favor of CCMP as networks transition to pure WPA2 configurations, removing security risks present in support for WPA.

When a packet is encrypted using CCMP, a number of data fields are added. The first field is the message integrity code (MIC), which is appended to the data. The MIC includes the hardware MAC addresses of the source and destination; this data essentially acts as a very strong cryptographically secure hashing function, which prevents man-in-the-middle attacks and other risks. The data and the MIC are then encrypted using the appropriate encryption key.

The packet is then modified with a data header. The first portion of data contained in the packet is the IV and key ID (4 bytes), which is needed to identify the encryption key used to encrypt the packet. At this point an extended IV (4 bytes) is attached to the packet. This field and the IV with key ID field are not encrypted, as the remote end must identify which key was used to encrypt a packet and the packet's sequence number. The first IV ensures that data is ordered properly. The rest of the packet contains the encrypted payload of data and MIC. The resulting packet is shown in Figure 3.

As with TKIP, the addition of MIC to packet data does not prevent replay attacks. MIC only ensures the data is not tampered or modified in transit. In order to prevent replay attacks, the IV included with the packet is referenced to ensure that sequential packets have increasing IV numbers; if an out-of-order IV is received, the client knows something is not right.

The data encrypted in the data payload and MIC field use the temporal key. This key changes for each frame and is generated from the master key, which is in turn generated from the 802.1X authentication performed by the user.

The MIC calculation and encryption of the data payload are done at the same time. This greatly speeds up encryption of packets and reduces the latency introduced by encryption.

WPA2 and Fast Roaming

WPA2 neatly solves the problem of roaming (and failover) in two ways: through the use of Pre-Authentication and PMK Caching.

PMK Caching. When a client re-associates with an access point, it uses a PMK from an older 802.1X authentication executed on the same access point. On this new association, no 802.1X exchange happens; the client immediately carries out the 802.11i handshake and is ready to send/receive data.

When the client loses the connection with the first access point — or otherwise decides to move to the second access point (because of signal strength, for example), it must only change radio frequencies and establish a base 802.11 connection with a second access point that it associated

with previously. Once this is completed, the client only needs to perform the 802.11i handshakes to establish the PTK and the Groupwise Master Key before beginning communication, since authentication has already taken place.

Pre-Authentication. When a client is associated with an access point and hears a beacon from another access point with the same SSID and security policy, it carries out an 802.1X authentication with that access point over the wire. The client and access point derive the PMK and keep it cached. Now if the client roams over to the new access point, it already has a PMK — the 802.1X authentication phase is skipped.

SYMBOL TECHNOLOGIES: LEADING THE WPA2 CHARGE

The industry leadership and award-winning wireless products from Symbol Technologies result from our rapid support of industry standards, scalable architectures, highly manageable platforms, and unmatched availability. This leadership in next-generation wireless networking is embodied by the support of WPA2 within our product line, including the first two 802.11i offerings: Symbol Wireless Switch WS2000 and Symbol Wireless Switch WS5100. It is our commitment to stay at the forefront of wireless standards and to keep these changes transparent to our customers with the industry's most flexible and upgradeable architecture.

In addition to providing comprehensive WPA2 support, Symbol is focused on providing value-added extensions to our wireless networking switches, solving business problems and differentiating ourselves from the competition.

WS2000 and WS5100

The WS2000 and WS5100 from Symbol Technologies provide enterprise-class wireless networking. The centralization of the intelligence that is traditionally distributed to access points into a robust switching architecture delivers unprecedented availability, functionality, manageability and scalability. The WS2000 and WS5100 can coordinate communications between all downstream access points, creating unprecedented opportunities for load balancing, fault tolerance, quality of service (QoS) and roaming performance.

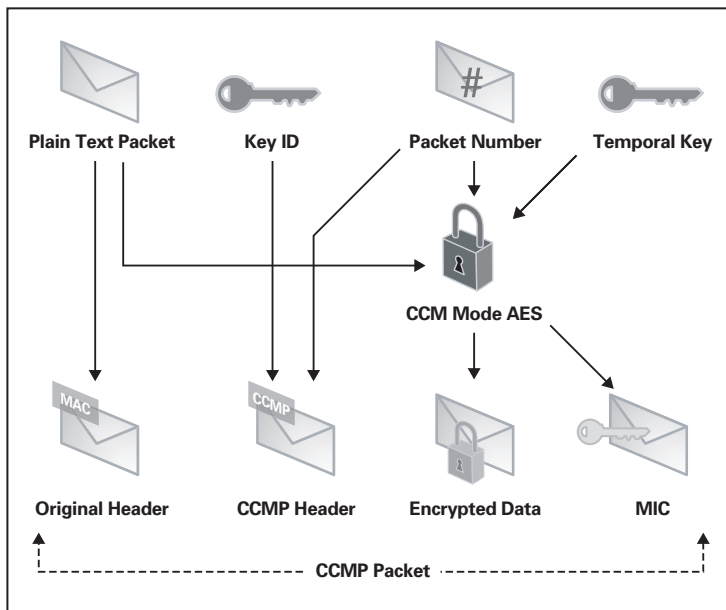


Figure 3 — WPA2 AES-CCMP

Opportunistic PMK Caching: Fast Roaming at Its Fastest

As described in an earlier section, roaming is a key technical advantage of WPA2. However, even the “fast roaming” options included in the standard cause the client a brief disruption of service, which is too lengthy for some time-sensitive applications.

Currently, establishing a connection to an 802.11 access point, authenticating to it, and establishing encryption keys can take anywhere from 150 to 350 milliseconds — and in extreme cases, 800 milliseconds or more. Long delays in establishing connections for clients occur when, due to the need for access points to communicate with back-end authentication servers, network equipment is spread out over a wide area.

While PMK Caching and Pre-Authentication within WPA2 help reduce this latency by reducing redundant instances of 802.1X authentication, experts recognize that this does not close the “disruption gap” that impacts quality of service. Not only does the standard not address intensive applications, but several implementation and architecture specific factors can exacerbate

the problem in wireless networks. In many standard fast roaming scenarios, establishing communications with the network can take 100 to 150 milliseconds, which is an acceptable delay for some activities such as web browsing, but which can result in a very noticeable interruption in service during a Wi-Fi VoIP phone call or video conference.

In July 2004, the IEEE formed a Fast Roaming Task Force to begin work on the 802.11r fast roaming standard for wireless networking. The goal of 802.11r is to improve handoff times between access points. The final product will be known as Fast BSS Transition. Symbol will extend its support to include this new standard, as it does for all other key standards. However, optimized roaming must be enabled today.

To meet this need now, Symbol has employed a unique fast roaming capability in its WPA2-compatible products that improves the roaming latency of WPA2. This feature, Opportunistic PMK Caching, has gained the support of such leading supplicant providers as Microsoft and Funk Software. While PMK Caching and pre-authentication enable fast roaming within the WPA2 standard and are supported by Symbol, Opportunistic PMK Caching takes a big step beyond these techniques. Opportunistic PMK Caching improves fast roaming in order to create a transparent environment for users of latency-sensitive wireless applications.

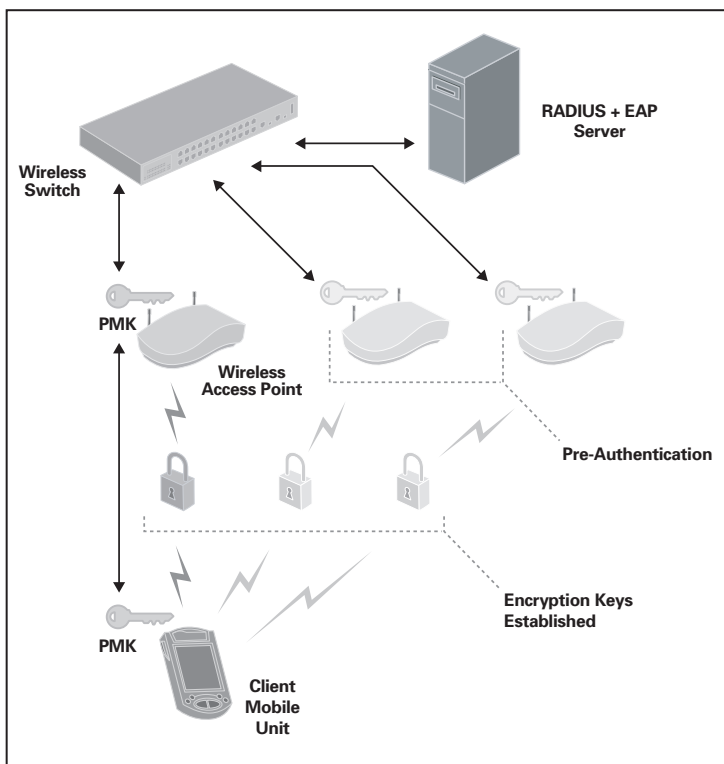


Figure 4 — Opportunistic PMK Caching

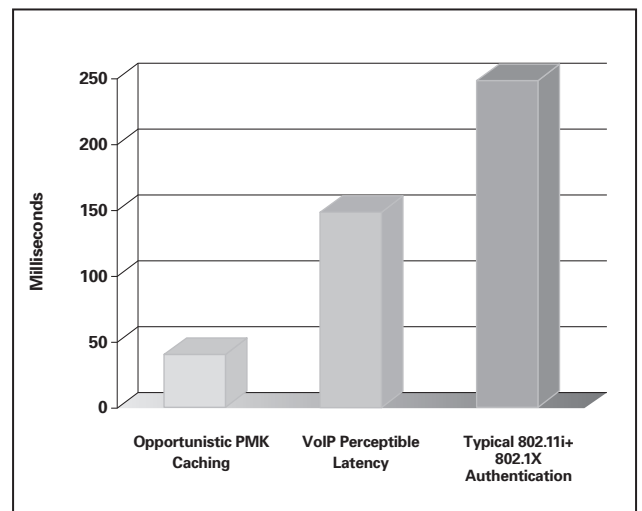


Figure 5 — WLAN Roaming Metrics

In a wireless switch environment, the switch has access to all PMKs from all connected access points. Depending upon the switch policy configuration, it is possible for a PMK from any one of the access points to be used for all connected access points. Therefore, a client may perform PMK caching with any other PMK that is available, bypassing the 4-way CCMP authentication handshake. This can greatly speed up the roaming process between access points, and in some cases will lead to virtually no disruption in service – critical to wireless VoIP and other devices.

Symbol's own testing has shown that the access point handoff can occur in less than 40 milliseconds — far below the 150 milliseconds time considered the threshold of VoIP latency as perceptible to humans. Symbol achieved this key breakthrough with its switch-based architecture, making possible seamless interoperation with several third-party clients and transparent wireless roaming for demanding user applications.

SUMMARY

There is no disputing the benefits that wireless local area networks provide to enterprises. Information technology departments have a mandate to provide wireless services in support of business initiatives, as well as a responsibility to provide these services securely. The history of 802.11-based WLANs has been a legacy of insecurity and significant risk to early adopters. Both WEP and its interim successor WPA have provided only minor obstacles to determined hackers and should be deployed with caution.

The ratification of IEEE 802.11i laid the foundation for drastic improvements in wireless security. WPA2 offers more formidable encryption, better key management, and robust authentication, as well as access point roaming. Symbol Technologies has implemented 802.11i compliance within a next-generation family of upgradeable wireless switches, the WS2000 and WS5100, providing centralized management of access points and a highly scalable architecture.

Symbol Technologies also surpasses a key shortcoming within WPA2 — insufficient access point roaming speeds. The current specification permits a credentials negotiation process, which can cause lengthy disruptions in the connections, a fatal problem for time-sensitive applications such as wireless-based Voice over IP (VoIP). Symbol Technologies developed Opportunistic PMK Caching to overcome this issue, a technique that leverages the centralized wireless switch architecture and provides the highest-speed Wi-Fi roaming available on the market. Symbol Technologies is solving tomorrow's wireless problems today.

REFERENCES

802.11 Standards Committees and Working Groups
<http://grouper.ieee.org/groups/802/11/>

802.1x Standards Committees and Working Groups
<http://www.ieee802.org/1/pages/802.1x.html>

IOMetrix, "Wireless LAN Metrics Liftoff", 2004
<http://www.iometrix.com/whitepapers/whitepaper-azimuth.pdf>

Network World, "VoWiFi Standards Situation", May 3, 2004
<http://www.nwfusion.com/research/2004/0503vowifiside.html>

Symbol Technologies Wireless Switch Data Sheets, 2004
<http://www.symbol.com/products/wireless/security.html>

The Unofficial 802.11 Security Web Page, 2004
<http://www.drizzle.com/~aboba/IEEE/>

ABOUT SYMBOL TECHNOLOGIES

Symbol Technologies, Inc., The Enterprise Mobility Company™, delivers solutions that capture, move and manage information in real time, from the point of activity to the point of decision. Symbol solutions integrate advanced data capture technology, ruggedized mobile computers, wireless infrastructure, enabling software and high-ROI applications from our business partners and Symbol Enterprise Mobility Services. Symbol enterprise mobility solutions increase business productivity and velocity, reduce costs and realize competitive advantage for the world's leading retailers, transportation and logistics companies and manufacturers as well as government agencies and providers of healthcare, hospitality and security. More information is available at www.symbol.com.

APPENDIX A

Glossary

Term	Definition	Notes
802.11	Wireless networking standard that uses 2.4 GHz or IR and provides 1 or 2 megabits/second	Original wireless specification with broad support
802.11a	Wireless networking standard that uses 5 GHz and provides up to 54 megabits/second	An extension of 802.11 (third)
802.11b	Wireless networking standard that uses 2.4 GHz and provides up to 11 megabits/second	An extension of 802.11 (first)
802.11g	Wireless networking standard that uses 2.4 GHz and provides 54 megabits/second	An extension of 802.11 (second)
802.11i	A security protocol that provides strong authentication and encryption of wireless traffic and additional capabilities	
802.1X	A security protocol that supplies a framework for authentication of end devices	
AES	Advanced Encryption Standard	Designated by NIST in 2004
CCM	Counter with CBC-MAC	RFC 3610
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol; uses CCM and specifies AES as the block cypher	
RC4	Stream cipher designed by Ron Rivest for RSA Security	
TKIP	Temporal Key Integrity Protocol, used by WPA, WPA2, 802.11i	
VoIP	Voice over Internet Protocol	
WEP	Wired Equivalent Privacy—A security protocol that provides weak authentication and encryption of wireless traffic	
WPA	Wi-Fi Protected Access—A security protocol that provides authentication and encryption of wireless traffic; based on an early draft of IEEE 802.11i	An enhanced version of WEP that provides slightly stronger security
WPA2	Wi-Fi Protected Access 2—A security protocol that provides strong authentication and encryption of wireless traffic; it is roughly IEEE 802.11i	

APPENDIX B

Supplicant/Authenticator Traffic flow in EAP/TLS

The “<” and “>” represents the direction of the message. A description of the communication and an example of data is in the brackets.

Supplicant	Authenticator	Authentication Server
< Initial association with access point >		
< Security discover capabilities >		
SDC Probe request >		
SDC < Probe response [access point supports]		
SDC 802.11 Open System Authentication >		
SDC < 802.11 Open auth [success]		
SDC Association request [client supports ...] >		
SDC < Association response [success]		
At this point, a port is “Assigned” but traffic is blocked (authentication phase required)		
< 802.1x authentication >		
802.1x < 802.1x [EAP Request Identity]		
802.1x 802.1x [EAP Identity response “my identity”] >		
	Radius access request [EAP response identity “my identity”] >	
	< Radius access Challenge [EAP request]	
< 802.1x [EAP Request, TLS encrypted]		
802.1x [EAP Response, TLS encrypted message] >		
	Radius Access Request [EAP Response, TLS encrypted message] >	
	< Radius Access challenge [EAP request]	
< 802.1x [EAP request, TLS encrypted server response with server key, etc.]		
		Master Key generated
EAP [MK sent, TLS encrypted]		
802.1x [EAP response, TLS encrypted certificate, client key, etc.] >		
	Radius request response [EAP response, TLS encrypted certificate, client key, etc.] >	
	< Radius access challenge [EAP request]	
< 802.1x [EAP request, TLS encrypted message]		
802.1x [EAP response] >		
	Radius Access request [EAP response identity] >	
		Pairwise Master Key generated
EAP [PMK sent, TLS encrypted]		
	< Radius Accept [EAP success, PMK]	
< 802.1x [EAP success]		
< Data protection via PTK and GTK's >		

About Symbol Technologies

Symbol Technologies, Inc., The Enterprise Mobility Company™, manufactures and services enterprise mobility systems, delivering products and solutions that capture, move and manage information in real time to and from the point of business activity. Symbol enterprise mobility solutions integrate advanced data capture products, radio frequency identification technology, mobile computing platforms, wireless infrastructure, mobility software and services programs under the Symbol Enterprise Mobility Services brand. Symbol enterprise mobility products and solutions are designed to increase workforce productivity, reduce operating costs, drive operational efficiencies and realize competitive advantages for the world's leading companies.



Corporate Headquarters

Symbol Technologies, Inc.

One Symbol Plaza
Holtsville, NY 11742-1300
TEL: +1.800.722.6234/+1.631.738.2400
FAX: +1.631.738.5990

For Asia Pacific Area

Symbol Technologies Asia, Inc.

(Singapore Branch)
Asia Pacific Division
230 Victoria Street #05-07/09
Bugis Junction Office Tower
Singapore 188024
TEL: +65.6796.9600
FAX: +65.6337.6488

For Europe, Middle East and Africa

Symbol Technologies

EMEA Division
Symbol Place, Winnersh Triangle
Berkshire, England RG41 5TP
TEL: +44.118.9457000
FAX: +44.118.9457500

For North America, Latin America and Canada

Symbol Technologies

The Americas
One Symbol Plaza
Holtsville, NY 11742-1300
TEL: +1.800.722.6234/+1.631.738.2400
FAX: +1.631.738.5990

Symbol Website

For a complete list of Symbol subsidiaries and business partners worldwide contact us at:

www.symbol.com

Or contact our pre-sales team at:

www.symbol.com/sales



SECENTAIRWP 02/05

Part No. SECENTAIRWP Printed in USA 2/05 © Copyright 2005 Symbol Technologies, Inc. All rights reserved. Symbol is an ISO 9001 and ISO 9002 UKAS, RVC, and RAB Registered company, as scope definitions apply. Specifications are subject to change without notice. Symbol® is a registered trademark, and The Enterprise Mobility Company is a trademark of Symbol Technologies, Inc. All other trademarks and service marks are proprietary to their respective owners. For system, product or services availability and specific information within your country, please contact your local Symbol Technologies office or Business Partner.