Appendix B
Wireless Networking Basics

This chapter provides an overview of wireless networking and security.

Wireless Networking Overview

The WG511U Wireless PC Card conforms to the Institute of Electrical and Electronics Engineers (IEEE) 802.11b standard for wireless LANs (WLANs) and a product update will bring the WG511U into conformance to the 802.11g standard when it is ratified. On an 802.11b or g wireless link, data is encoded using direct-sequence spread-spectrum (DSSS) technology and is transmitted in the unlicensed radio spectrum at 2.5GHz. The maximum data rate for the 802.11b wireless link is 11 Mbps, but it will automatically back down from 11 Mbps to 5.5, 2, and 1 Mbps when the radio signal is weak or when interference is detected. The 802.11g auto rate sensing rates are 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps. Likewise, the 802.11a wireless link offers a maximum data rate of 54 Mbps, but will automatically back down to rates 48, 36, 24, 18, 12, 9, and 6 Mbps.

The 802.11 standard is also called Wireless Ethernet or Wi-Fi by the Wireless Ethernet Compatibility Alliance (WECA, see *http://www.wi-fi.net*), an industry standard group promoting interoperability among 802.11 devices. The 802.11 standard offers two methods for configuring a wireless network - ad hoc and infrastructure.

Infrastructure Mode

With a wireless access point, you can operate the wireless LAN in the infrastructure mode. This mode provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage, interacting with wireless nodes via an antenna.

In the infrastructure mode, the wireless access point converts airwave data into wired Ethernet data, acting as a bridge between the wired LAN and wireless clients. Connecting multiple access points via a wired Ethernet backbone can further extend the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one access point domain to another and still maintain seamless network connection.

Ad Hoc Mode (Peer-to-Peer Workgroup)

In an ad hoc network, computers are brought together as needed; thus, there is no structure or fixed points to the network - each node can generally communicate with any other node. There is no access point involved in this configuration. This mode enables you to quickly set up a small wireless workgroup and allows workgroup members to exchange data or share printers as supported by Microsoft networking in the various Windows operating systems. Some vendors also refer to ad hoc networking as peer-to-peer group networking.

In this configuration, network packets are directly sent and received by the intended transmitting and receiving stations. As long as the stations are within range of one another, this is the easiest and least expensive way to set up a wireless network.

Network Name: Extended Service Set Identification (ESSID)

The Extended Service Set Identification (ESSID) is one of two types of Service Set Identification (SSID). In an ad hoc wireless network with no access points, the Basic Service Set Identification (BSSID) is used. In an infrastructure wireless network that includes an access point, the ESSID is used, but may still be referred to as SSID.

An SSID is a thirty-two character (maximum) alphanumeric key identifying the name of the wireless local area network. Some vendors refer to the SSID as network name. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.

Wireless Channels

IEEE 802.11g/b wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4 GHz and 2.5 GHz. Neighboring channels are 5 MHz apart. However, due to spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum 12.5 MHz above and below the center channel frequency. As a result, two separate wireless networks using neighboring channels (for example, channel 1 and channel 2) in the same general vicinity will interfere with each other. Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk, and provide a noticeable performance increase over networks with minimal channel separation.

The wireless frequencies used by 802.11a and 802.11b/g networks are different. These channel frequency options are discussed below.

802.11b/g Wireless Channels

IEEE 802.11b/g wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4 GHz and 2.5 GHz. Neighboring channels are 5 MHz apart. However, due to spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum 12.5 MHz above and below the center channel frequency. As a result, two separate wireless networks using neighboring channels (for example, channel 1 and channel 2) in the same general vicinity will interfere with each other. Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk, and provide a noticeable performance increase over networks with minimal channel separation.

The radio frequency channels used in 802.11b/g networks are listed in Table B-1:

Table B-1: 802.11b/g Radio Frequency Channels

Channel	Center Frequency	Frequency Spread
1	2412 MHz	2399.5 MHz - 2424.5 MHz
2	2417 MHz	2404.5 MHz - 2429.5 MHz
3	2422 MHz	2409.5 MHz - 2434.5 MHz
4	2427 MHz	2414.5 MHz - 2439.5 MHz
5	2432 MHz	2419.5 MHz - 2444.5 MHz
6	2437 MHz	2424.5 MHz - 2449.5 MHz
7	2442 MHz	2429.5 MHz - 2454.5 MHz
8	2447 MHz	2434.5 MHz - 2459.5 MHz
9	2452 MHz	2439.5 MHz - 2464.5 MHz
10	2457 MHz	2444.5 MHz - 2469.5 MHz
11	2462 MHz	2449.5 MHz - 2474.5 MHz
12	2467 MHz	2454.5 MHz - 2479.5 MHz
13	2472 MHz	2459.5 MHz - 2484.5 MHz

Note: The available channels supported by the wireless products in various countries are different. For example, Channels 1 to 11 are supported in the U.S. and Canada, and Channels 1 to 13 are supported in Europe and Australia.

The preferred channel separation between the channels in neighboring wireless networks is 25 MHz (5 channels). This means that you can apply up to three different channels within your wireless network. There are only 11 usable wireless channels in the United States. It is recommended that you start using channel 1 and grow to use channel 6, and 11 when necessary, as these three channels do not overlap.

802.11a Legal Power Output and Wireless Channels

IEEE 802.11a utilizes 300 MHz of bandwidth in the 5 GHz Unlicensed National Information Infrastructure (U-NII) band. Though the lower 200 MHz is physically contiguous, the FCC has divided the total 300 MHz into three distinct domains, each with a different legal maximum power output. Below is a table of summary for different regulatory domains.

Table B-2: 802.11a Radio Frequency Channels

U-NII Band	Low	Middle	High
Frequency (GHz)	5.15 – 5.25	5.25 – 5.35	5.725 – 5.825
Max. Power Output	• 50 mW for US • 200 mW for Canada, Europe, and Australia	• 250 mW for US • 200 mW for Europe and Australia • 1 W for Canada	• 1 W for US and Australia • 4 W for Canada • 25 mW for Europe

Note: Please check your local Authority for updated information on the available frequency and maximum power output.

IEEE 802.11a uses Orthogonal Frequency Division Multiplexing (OFDM), a new encoding scheme that offers certain benefits over a spread spectrum in channel availability and data rate. The 802.11a uses OFDM to define a total of 8 non-overlapping 200 MHz channels across the 2 lower bands; each of these is divided into 52 sub carriers and each carrier is approximately 300 KHz wide.

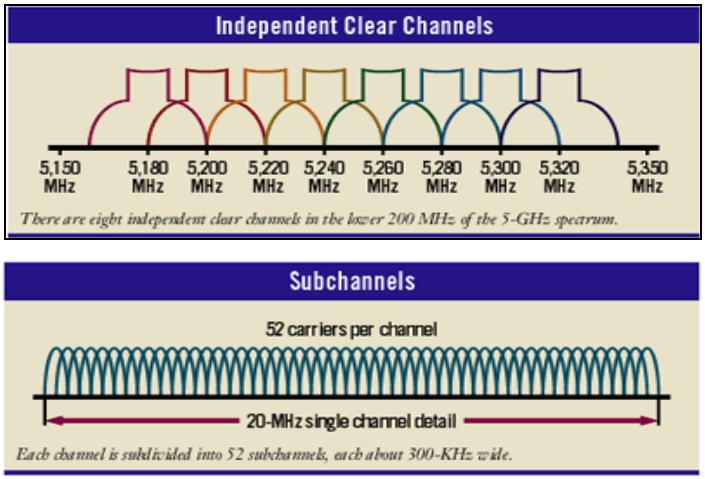

Figure B-1: IEEE 802.11a Channel Allocations

The WG511U user can use thirteen channels in **non-turbo** mode.

Table B-3: 802.11a Turbo Mode Off Radio Frequency Channels

Turbo Mode OFF	
Channel	**Frequency**
36	5.180 GHz
40	5.200 GHz
44	5.220 GHz
48	5.240 GHz
52	5.260 GHz
56	5.280 GHz
60	5.300 GHz
64	5.320 GHz
149	5.745 GHz
153	5.765 GHz
157	5.785 GHz
161	5.805 GHz
165	5.825 GHz

The WG511U user can use five channels in turbo mode.

Turbo Mode ON	
Channel	**Frequency**
42	5.21 GHz
50	5.25 GHz
58	5.29 GHz
152	5.76 GHz
160	5.8 GHz

The available channels supported by the wireless products in various countries are different.

Wireless Security Overview

Wireless technology is evolving rapidly to accommodate the need for stronger security. The following security schemes are supported in Netgear products:

- **WEP**

  Wired Equivalent Privacy is an existing, widely implemented and supported, data encryption protocol for 802.11 wireless networks. All wireless nodes on the network are configured with a static 64-bit or 128-bit Shared Key for data encryption but authentication is optional.

- **WPA**

  Wi-Fi Protected Access (WPA) is a new specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for wireless networks. WPA requires authentication and features strong data encryption that includes dynamic key generation. WPA uses the Extensible Authentication Protocol (EAP) via WPA enables wireless access points using a modified version of the 802.1x protocols to access RADIUS and certificate servers which enable various authentication schemes such as Transport Layer Security (TLS) and Protected EAP (PEAP).

- **WPA-PSK**

  WPA-Pre-Shared Key (WPA-PSK) performs authentication and encryption with a only a wireless access point based on a preshared key without needing to access RADIUS or certificate servers via the 802.1x protocols.

- **802.1x**

  802.1x defines port-based, network access control used to provide authenticated network access and automated data encryption key management.

- **Cisco LEAP**

  Light Extensible Authentication Protocol (LEAP) is a proprietary 802.1x EAP method developed by Cisco for use on wireless networks that use Cisco 802.11 wireless devices. It features dynamic per user per session WEP keys.

These security technologies are discussed below.

WEP Overview

The absence of a physical connection between nodes makes the wireless links vulnerable to eavesdropping and information theft. To provide a certain level of security, the IEEE 802.11 standard has defined two types of authentication methods, Open System and Shared Key. With Open System authentication, a wireless PC can join any network and receive any messages that are not encrypted. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network. By default, IEEE 802.11 wireless devices operate in an Open System network. Recently, Wi-Fi, the Wireless Ethernet Compatibility Alliance (*http://www.wi-fi.net*) developed the Wi-Fi Protected Access (WPA), a new strongly enhanced Wi-Fi security. WPA will soon be incorporated into the IEEE 802.11 standard. WEP and WPA are discussed below.

WEP Authentication

An access point must authenticate a station before the station can associate with the access point or communicate with the network. The IEEE 802.11 standard defines two types of WEP authentication: Open System and Shared Key.

- Open System Authentication allows any device to join the network, assuming that the device SSID matches the access point SSID. Alternatively, the device can use the "ANY" SSID option to associate with any available access point within range, regardless of its SSID.
- Shared Key Authentication requires that the station and the access point have the same WEP Key to authenticate. These two authentication procedures are described below.

The WEP Open System authentication process is illustrated in below.

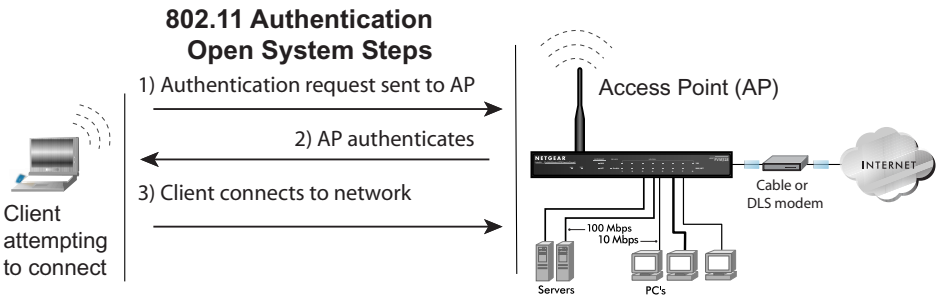

Figure B-2: 802.11 open system authentication

The following steps occur when two devices use Open System Authentication:

1. The station sends an authentication request to the access point.
2. The access point authenticates the station.
3. The station associates with the access point and joins the network.

The WEP Shared Key authentication process is illustrated in below.

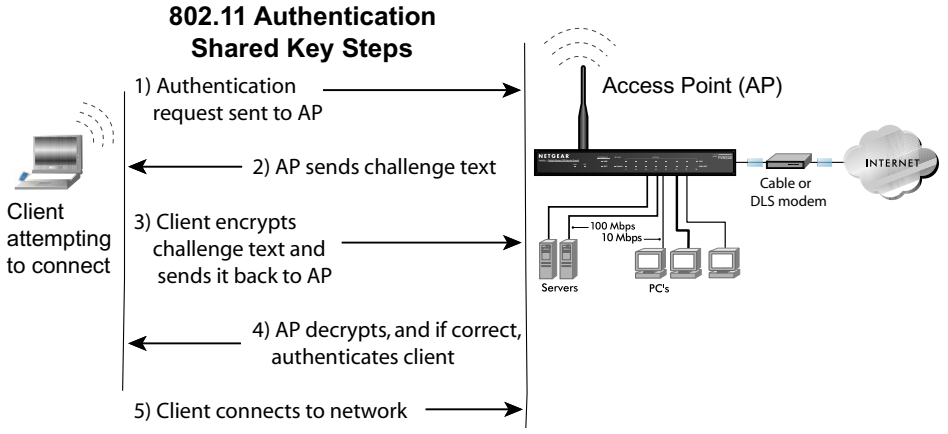

Figure B-3: 802.11 shared key authentication

The following steps occur when two devices use Shared Key Authentication:

1. The station sends an authentication request to the access point.

2. The access point sends challenge text to the station.
3. The station uses its configured 64-bit or 128-bit default key to encrypt the challenge text, and sends the encrypted text to the access point.
4. The access point decrypts the encrypted text using its configured WEP Key that corresponds to the station's default key. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, then the access point and the station share the same WEP Key and the access point authenticates the station.
5. The station connects to the network.

If the decrypted text does not match the original challenge text (i.e., the access point and station do not share the same WEP Key), then the access point will refuse to authenticate the station and the station will be unable to communicate with either the 802.11 network or Ethernet network.

WEP Keys

The IEEE 802.11 standard supports two types of WEP encryption: 64-bit and 128-bit. 128-bit encryption is stronger than 64-bit encryption, but 128-bit encryption may not be available outside of the United States due to U.S. export regulations.

- **64-bit WEP**

The 64-bit WEP data encryption method, allows for a five-character (40-bit) input. Additionally, 24 factory-set bits are added to the forty-bit input to generate a 64-bit encryption key. (The 24 factory-set bits are not user-configurable). This encryption key will be used to encrypt/decrypt all data transmitted via the wireless interface. Some vendors refer to the 64-bit WEP data encryption as 40-bit WEP data encryption since the user-configurable portion of the encryption key is 40 bits wide.

When configured for 64-bit encryption, 802.11 products typically support up to four WEP Keys. Each 64-bit WEP Key is expressed as 5 sets of two hexadecimal digits (0-9 and A-F). For example, "12 34 56 78 90" is a 40-bit WEP Key.

- **128-bit WEP**

The 128-bit WEP data encryption method consists of 104 user-configurable bits. Similar to the forty-bit WEP data encryption method, the remaining 24 bits are factory set and not user configurable. Some vendors allow passphrases to be entered instead of the cryptic hexadecimal characters to ease encryption key entry.

When configured for 128-bit encryption, 802.11 products typically support four WEP Keys but some manufacturers support only one 128-bit key. The 128-bit WEP Key is expressed as 13 sets of two hexadecimal digits (0-9 and A-F). For example, "12 34 56 78 90 AB CD EF 12 34 56 78 90" is a 128-bit WEP Key.

Typically, 802.11 access points can store up to four 128-bit WEP Keys but some 802.11 client adapters can only store one. Therefore, make sure that your 802.11 access and client adapters configurations match.

- **WEP Key Configuration**

Whatever keys you enter for an AP, you must also enter the same keys for the client adapter in the same order. In other words, WEP key 1 on the AP must match WEP key 1 on the client adapter, WEP key 2 on the AP must match WEP key 2 on the client adapter, etc.

Note: The AP and the client adapters can have different default WEP Keys as long as the keys are in the same order. In other words, the AP can use WEP key 2 as its default key to transmit while a client adapter can use WEP key 3 as its default key to transmit. The two devices will communicate as long as the AP's WEP key 2 is the same as the client's WEP key 2 and the AP's WEP key 3 is the same as the client's WEP key 3.

How to Use WEP Parameters

Wired Equivalent Privacy (WEP) data encryption is used when the wireless devices are configured to operate in Shared Key authentication mode. There are two shared key methods implemented in most commercially available products, 64-bit and 128-bit WEP data encryption.

Before enabling WEP on an 802.11 network, you must first consider what type of encryption you require and the key size you want to use. Typically, there are three WEP Encryption options available for 802.11 products:

1. **Does Not Use WEP:** The 802.11 network does not encrypt data. For authentication purposes, the network uses Open System Authentication.

2. **Uses WEP for Encryption:** A transmitting device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving device decrypts the data using the same WEP Key. For authentication purposes, the network uses Open System Authentication.

3. **Uses WEP for Authentication and Encryption:** A transmitting device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving device decrypts the data using the same WEP Key. For authentication purposes, the network uses Shared Key Authentication.

Note: Some 802.11 access points also support **Use WEP for Authentication Only** (Shared Key Authentication without data encryption). However, the WG511U does not offer this option.

802.1x Port Based Network Access Control

Securing any kind of network involves allowing authorized parties to access traffic and networked resources (e.g., servers, hosts) while blocking outsiders. One essential ingredient in this recipe: permitting or denying physical attachment to the underlying communications medium.

In Ethernet LANs, this has long been accomplished by disabling unused RJ-45 jacks and controlling access to Ethernet switch ports according to the Media Access Control (MAC) addresses of the attached device. Early wireless LANs followed suit by using access control lists (ACLs) to permit associations by known MAC addresses while rejecting all others. MAC ACLs are quite easy to understand and configure. However, ACLs become difficult to manage in large dynamic networks and are easily circumvented by network interface cards (NICs) with programmable addresses.

The LAN Port Access Control framework defined by the IEEE 802.1X standard addresses these needs.

With 802.11 WEP, all wireless access points and client wireless adapters on a particular wireless LAN must use the same encryption key. Each sending station encrypts data with a WEP key before transmission, and the receiving station decrypts it using an identical key. This process reduces the risk of someone passively monitoring the transmission and gaining access to the data transmitted over the wireless connections.

However, a major problem with the 802.11 wireless standard is that the keys are cumbersome to change. If you don't update the WEP keys often, an unauthorized person with a sniffing tool can monitor your network for less than a day and decode the encrypted messages. In order to use different keys, you must manually configure each access point and wireless adapter with new keys.

Products based on the 802.11 standard alone offer system administrators no effective method to update the keys. This might not be too much of concern with a few users, but the job of renewing keys on larger networks can be a monumental task. As a result, companies either don't use WEP at all or maintain the same keys for weeks, months, and even years. Both cases significantly heighten the wireless LAN's vulnerability to eavesdroppers.

IEEE 802.1x offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1x ties a protocol called EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication. For details on EAP specifically, refer to IETF's RFC 2284.

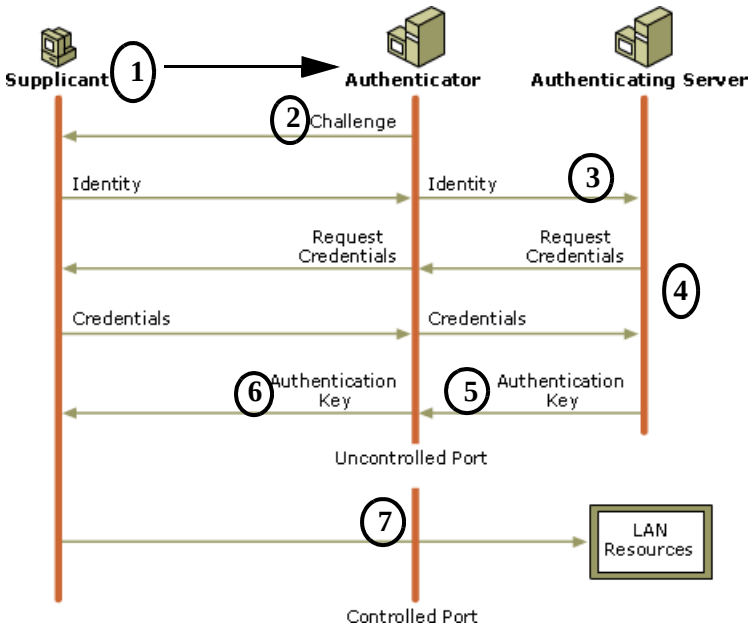

Figure B-4: 802.1x authentication

1. After associating with a wireless access point, the client sends an EAP-start message. This begins a series of message exchanges to authenticate the client.
2. The access point replies with an EAP-request identity message.
3. The client sends an EAP-response packet containing the identity to the authentication server.
4. The authentication server uses a specific authentication algorithm to verify the client's identity. This could be through the use of digital certificates or other EAP authentication type.
5. The authentication server will either send an accept or reject message to the access point.
6. The access point sends an EAP-success packet (or reject packet) to the client.

7. If the authentication server accepts the client, then the access point will transition the client's port to an authorized state and forward additional traffic.

Initial 802.1x communications begin with an unauthenticated supplicant (i.e., client device) attempting to connect with an authenticator (i.e., 802.11 access point). The access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the access point can verify the client's identity using an authentication server (e.g., RADIUS). Once authenticated, the access point opens the client's port for other types of traffic.

The basic 802.1x protocol provides effective authentication and can offering dynamic key management using 802.1x as a delivery mechanism. If configured to implement dynamic key exchange, the 802.1x authentication server can return session keys to the access point along with the accept message. The access point uses the session keys to build, sign and encrypt an EAP key message that is sent to the client immediately after sending the success message. The client can then use contents of the key message to define applicable encryption keys. In typical 802.1x implementations, the client can automatically change encryption keys as often as necessary to minimize the possibility of eavesdroppers having enough time to crack the key in current use.

It's important to note that 802.1x doesn't provide the actual authentication mechanisms. When using 802.1x, you need to choose an EAP type, such as Transport Layer Security (EAP-TLS) or Protected EAP (PEAP), which defines how the authentication takes place.

The important part to know at this point is that the software supporting the specific EAP type resides on the authentication server and within the operating system or application software on the client devices. The wireless access point acts as a “pass through” for 802.1x messages. As a result, you can update the EAP authentication type as newer types become available and your requirements for security change.

802.1x is well on its way to becoming an industry standard, and provides an effective wired and wireless LAN security solution. Windows XP implements 802.1x natively, and the NETGEAR Double 108 Mbps Wireless PC Card 32-bit CardBus WG511U supports 802.1x. The 802.11i committee is specifying the use of 802.1x to eventually become part of the 802.11 standard.

WPA Wireless Security

Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for existing and future wireless LAN systems.

The IEEE introduced the WEP as an optional security measure to secure 802.11 (Wi-Fi) WLANs, but inherent weaknesses in the standard soon became obvious. In response to this situation, the Wi-Fi Alliance announced a new security architecture that remedies the short comings of WEP. This standard, formerly known as Safe Secure Network (SSN), is designed to work with existing 802.11 products and offers forward compatibility with 802.11i, the new wireless security architecture being defined in the IEEE.

WPA offers the following benefits:

- Enhanced data privacy
- Robust key management
- Data origin authentication
- Data integrity protection

Starting August of 2003, all new Wi-Fi certified products had to support WPA. NETGEAR has implemented WPA on its client and access point products. Existing Wi-Fi certified products had until August of 2004 to add WPA support or they would loose their Wi-Fi certification.

While the new IEEE 802.11i standard is being ratified, wireless vendors have agreed on WPA as an interoperable interim standard.

How Does WPA Compare to WEP?

WEP is a data encryption method and is not intended as a user authentication mechanism. WPA user authentication is implemented using 802.1x and the Extensible Authentication Protocol (EAP). Support for 802.1x authentication is required in WPA. In the 802.11 standard, 802.1x authentication was optional. For details on EAP specifically, refer to IETF's RFC 2284.

With 802.11 WEP, all access points and client wireless adapters on a particular wireless LAN must use the same encryption key. A major problem with the 802.11 standard is that the keys are cumbersome to change. If you don't update the WEP keys often, an unauthorized person with a sniffing tool can monitor your network for less than a day and decode the encrypted messages. Products based on the 802.11 standard alone offer system administrators no effective method to update the keys.

For 802.11, WEP encryption is optional. For WPA, encryption using Temporal Key Integrity Protocol (TKIP) is required. TKIP replaces WEP with a new encryption algorithm that is stronger than the WEP algorithm, but that uses the calculation facilities present on existing wireless devices to perform encryption operations. TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. Through these enhancements, TKIP addresses all of known WEP vulnerabilities.

How Does WPA Compare to IEEE 802.11i?

WPA will be forward compatible with the IEEE 802.11i security specification currently under development. WPA is a subset of the current 802.11i draft and uses certain pieces of the 802.11i draft that are ready to bring to market today, such as 802.1x and TKIP. The main pieces of the 802.11i draft that are not included in WPA are secure IBSS (Ad-Hoc mode), secure fast handoff (for specialized 802.11 VoIP phones), as well as enhanced encryption protocols such as AES-CCMP. These features are either not yet ready for market or will require hardware upgrades to implement.

What are the Key Features of WPA Security?

The following security features are included in the WPA standard:

- WPA Authentication
- WPA Encryption Key Management
  - Temporal Key Integrity Protocol (TKIP)
  - Michael *message integrity code* (MIC)
  - AES Support
- Support for a Mixture of WPA and WEP Wireless Clients

These features are discussed below.

WPA addresses most of the known WEP vulnerabilities and is primarily intended for wireless infrastructure networks as found in the enterprise. This infrastructure includes stations, access points, and authentication servers (typically RADIUS servers). The RADIUS server holds (or has access to) user credentials (e.g., user names and passwords) and authenticates wireless users before they gain access to the network.

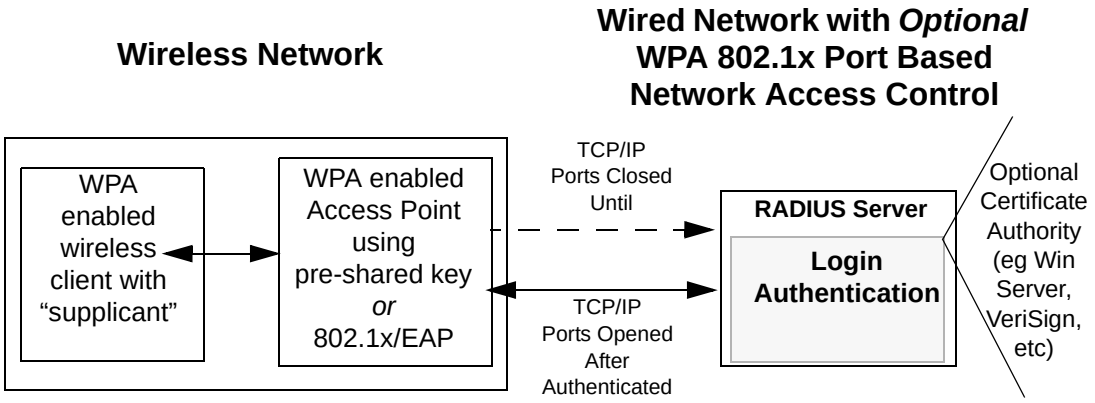

Figure B-5: WPA Overview

The strength WPA comes from an integrated sequence of operations that encompass 802.1X/EAP authentication and sophisticated key management and encryption techniques. Its major operations include:

- **Network security capability determination**. This occurs at the 802.11 level and is communicated through WPA information elements in Beacon, Probe Response, and (Re) Association Requests. Information in these elements includes the authentication method (802.1X or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES).

  The primary information conveyed in the Beacon frames is the authentication method and the cipher suite. Possible authentication methods include 802.1X and Pre-shared key. Pre-shared key is an authentication method that uses a statically configured pass phrase on both the stations and the access point. This eliminates the need for an authentication server, which in many home and small office environments will not be available nor desirable. Possible data encryption options include: WEP, TKIP, and AES (Advanced Encryption Standard). We'll talk more TKIP and AES when addressing data privacy below.

- **Authentication**. EAP over 802.1X is used for authentication. Mutual authentication is gained by choosing an EAP type supporting this feature and is required by WPA. 802.1X port access control prevents full access to the network until authentication completes. 802.1X EAPOL-Key packets are used by WPA to distribute per-session keys to those stations successfully authenticated.

The supplicant in the station uses the authentication and cipher suite information contained in the information elements to decide which authentication method and cipher suite to use. For example, if the access point is using the Pre-shared key method then the supplicant need not authenticate using full-blown 802.1X. Rather, the supplicant must simply prove to the access point that it is in possession of the pre-shared key. If the supplicant detects that the service set does not contain a WPA information element then it knows it must use pre-WPA 802.1X authentication and key management in order to access the network.

- **Key management**. WPA features a robust key generation/management system that integrates the authentication and data privacy functions. Keys are generated after successful authentication and through a subsequent 4-way handshake between the station and Access Point (AP).
- **Data Privacy (Encryption)**. Temporal Key Integrity Protocol (TKIP) is used to wrap WEP in sophisticated cryptographic and security techniques to overcome most of its weaknesses.
- **Data integrity**. TKIP includes a message integrity code (MIC) at the end of each plaintext message to ensure messages are not being spoofed.

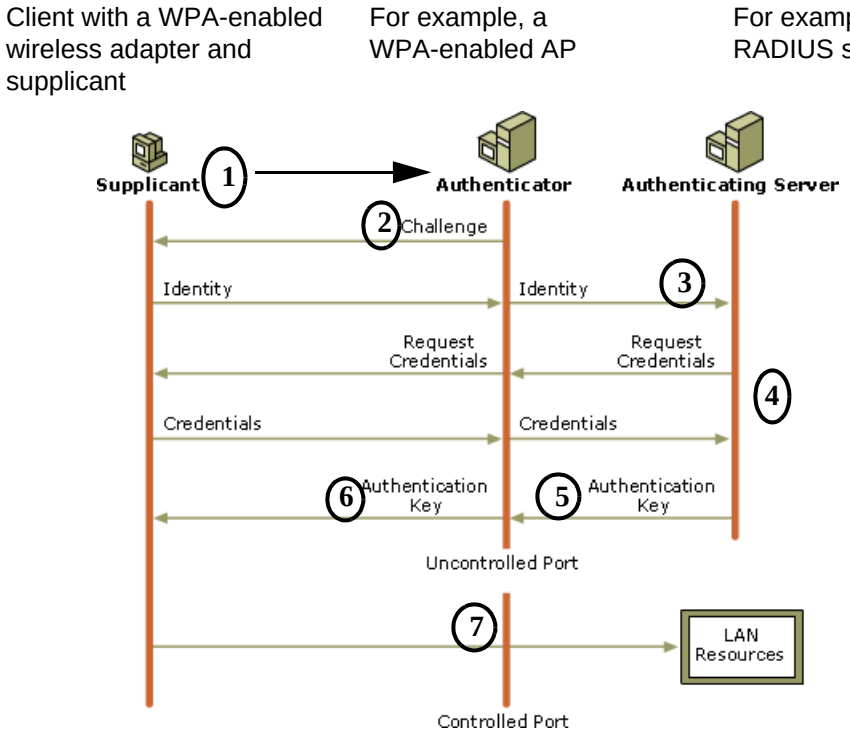

Figure B-6: WPA/802.1x Authentication Sequence

The AP sends Beacon Frames with WPA information element to the stations in the service set. Information elements include the required authentication method (802.1x or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES). Probe Responses (AP to station) and Association Requests (station to AP) also contain WPA information elements.

1. Initial 802.1x communications begin with an unauthenticated supplicant (i.e., client device) attempting to connect with an authenticator (i.e., 802.11 access point). The client sends an EAP-start message. This begins a series of message exchanges to authenticate the client.
2. The access point replies with an EAP-request identity message.
3. The client sends an EAP-response packet containing the identity to the authentication server. The access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the access point can verify the client's identity using an authentication server (e.g., RADIUS).
4. The authentication server uses a specific authentication algorithm to verify the client's identity. This could be through the use of digital certificates or some other EAP authentication type.
5. The authentication server will either send an accept or reject message to the access point.
6. The access point sends an EAP-success packet (or reject packet) to the client.
7. If the authentication server accepts the client, then the access point will transition the client's port to an authorized state and forward additional traffic.

The important part to know at this point is that the software supporting the specific EAP type resides on the authentication server and within the operating system or application "supplicant" software on the client devices. The access point acts as a "pass through" for 802.1x messages, which means that you can specify any EAP type without needing to upgrade an 802.1x-compliant access point. As a result, you can update the EAP authentication type to such devices as token cards (Smart Cards), Kerberos, one-time passwords, certificates, and public key authentication or as newer types become available and your requirements for security change.

IEEE 802.1x offers an effective framework for authenticating and controlling user traffic to a protected network, as well as providing a vehicle for dynamically varying data encryption keys via EAP from a RADIUS server, for example. This framework enables using a central authentication server, which employs mutual authentication so that a rogue wireless user does not join the network.

It's important to note that 802.1x doesn't provide the actual authentication mechanisms. When using 802.1x, the EAP type, such as Transport Layer Security (EAP-TLS) or EAP Tunneled Transport Layer Security (EAP-TTLS) defines how the authentication takes place.

Note: For environments with a Remote Authentication Dial-In User Service (RADIUS) infrastructure, WPA supports Extensible Authentication Protocol (EAP). For environments without a RADIUS infrastructure, WPA supports the use of a preshared key.

Together, these technologies provide a framework for strong user authentication.

WPA Data Encryption Key Management

With 802.1x, the rekeying of unicast encryption keys is optional. Additionally, 802.11 and 802.1x provide no mechanism to change the global encryption key used for multicast and broadcast traffic. With WPA, rekeying of both unicast and global encryption keys is required.

For the unicast encryption key, the Temporal Key Integrity Protocol (TKIP) changes the key for every frame, and the change is synchronized between the wireless client and the wireless access point (AP). For the global encryption key, WPA includes a facility (the Information Element) for the wireless AP to advertise the changed key to the connected wireless clients.

If configured to implement dynamic key exchange, the 802.1x authentication server can return session keys to the access point along with the accept message. The access point uses the session keys to build, sign and encrypt an EAP key message that is sent to the client immediately after sending the success message. The client can then use contents of the key message to define applicable encryption keys. In typical 802.1x implementations, the client can automatically change encryption keys as often as necessary to minimize the possibility of eavesdroppers having enough time to crack the key in current use.

- **Temporal Key Integrity Protocol (TKIP)**

WPA uses TKIP to provide important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. TKIP also provides for the following:

- The verification of the security configuration after the encryption keys are determined.
- The synchronized changing of the unicast encryption key for each frame.
- The determination of a unique starting unicast encryption key for each preshared key authentication.
- **Michael**

With 802.11 and WEP, data integrity is provided by a 32-bit *integrity check value* (ICV) that is appended to the 802.11 payload and encrypted with WEP. Although the ICV is encrypted, you can use cryptanalysis to change bits in the encrypted payload and update the encrypted ICV without being detected by the receiver.

With WPA, a method known as *Michael* specifies a new algorithm that calculates an 8-byte *message integrity code* (MIC) using the calculation facilities available on existing wireless devices. The MIC is placed between the data portion of the IEEE 802.11 frame and the 4-byte ICV. The MIC field is encrypted together with the frame data and the ICV. Michael also provides replay protection. A new frame counter in the IEEE 802.11 frame is used to prevent replay attacks.

- **AES Support**

One of the encryption methods supported by WPA beside TKIP is the advanced encryption standard (AES), although AES support will not be required initially for Wi-Fi certification. This is viewed as the optimal choice for security conscience organizations, but the problem with AES is that it requires a fundamental redesign of the NIC's hardware in both the station and the access point. TKIP was a pragmatic compromise that allows organizations to deploy better security while AES capable equipment is being designed, manufactured, and incrementally deployed.

Is WPA Perfect?

WPA is not without its vulnerabilities. Specifically, it is susceptible to denial of service (DoS) attacks. If the access point receives two data packets that fail the Message Integrity Code (MIC) check within 60 seconds of each other then the network is under an active attack, and as a result, the access point employs counter measures, which includes disassociating each station using the access point. This prevents an attacker from gleaning information about the encryption key and alerts administrators, but it also causes users to lose network connectivity for 60 seconds. More than anything else, this may just prove that no single security tactic is completely invulnerable. WPA is a definite step forward in WLAN security over WEP and has to be thought of as a single part of an end-to-end network security strategy.

Product Support for WPA

Starting in August, 2003, new NETGEAR, Inc. Wi-Fi certified products will support the WPA standard. Existing NETGEAR, Inc. wireless products that had their Wi-Fi certification approved before August, 2003 will have one year to add WPA so as to maintain their Wi-Fi certification.

WPA requires software changes to the following:

- Wireless access points

- Wireless network adapters
- Wireless client programs

Check the NETGEAR web site for WPA-enabled updates to NETGEAR products. For wireless devices in your network from other vendors, check with the vendor regarding WPA support.