# Wireless Networking Basics

NETGEAR

**NETGEAR**, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

n/a
October 2005

## Trademarks

NETGEAR and Auto Uplink are trademarks or registered trademarks of NETGEAR, Inc..

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders. Portions of this document are copyright Intoto, Inc.

## Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

## Product and Publication Details

| | |
|---|---|
| **Model Number:** | n/a |
| **Publication Date:** | October 2005 |
| **Product Family:** | Product Family |
| **Product Name:** | n/a |
| **Home or Business Product:** | n/a |
| **Language:** | English |
| **Publication Version Number:** | 1.0 |

# Contents

## Wireless Networking Basics

### Chapter 1
### About This Manual

### Chapter 2
### Wireless Networking Basics

# Chapter 1
# About This Manual

This chapter describes the intended audience, scope, conventions, and formats of this manual.

## Audience, Scope, Conventions, and Formats

This manual assumes that the reader has basic to intermediate computer and Internet skills. However, basic computer network, Internet, and firewall technologies tutorial information is provided on the NETGEAR Web site.

This manual uses the following typographical conventions:

**Table 1-1. Typographical Conventions**

| | |
|---|---|
| *italics* | Emphasis, books, CDs, URL names |
| **bold** | User input |
| `fixed font` | Screen text, file and server names, extensions, commands, IP addresses |

This manual uses the following formats to highlight special messages:

➡ **Note:** This format is used to highlight information of importance or special interest.

➡ **Tip:** This format is used to highlight a procedure that will save time or resources.

## How to Use this Manual

The HTML version of this manual includes the following:

- Buttons, > and <, for browsing forwards or backwards through the manual one page at a time
- A ☰ button that displays the table of contents. Double-click on a link in the table of contents to navigate directly to where the topic is described in the manual.
- A button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

## How to Print this Manual

To print this manual you can choose one of the following several options, according to your needs.

- **Printing a Page in the HTML View**.

  Each page in the HTML version of the manual is dedicated to a major topic. Use the *Print* button on the browser toolbar to print the page contents.

- **Printing a Chapter**.

  Use the *PDF of This Chapter* link at the top left of any page.

  — Click the "*PDF of This Chapter*" link at the top right of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.

  — Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.

  — Click the print icon in the upper left of the window.

> **Tip:** If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

- **Printing the Full Manual**.

  Use the *Complete PDF Manual* link at the top left of any page.

  — Click the *Complete PDF Manual* link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.

  — Click the print icon in the upper left of the window.

| | |
|---|---|
| ➡ | **Tip:** If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature. |

# Chapter 2
# Wireless Networking Basics

## Wireless Networking Overview

Some NETGEAR products conform to the Institute of Electrical and Electronics Engineers (IEEE) 802.11g standard for wireless LANs (WLANs). On an 802.11 wireless link, data is encoded using direct-sequence spread-spectrum (DSSS) technology and is transmitted in the unlicensed radio spectrum at 2.5 GHz. The maximum data rate for the 802.11g wireless link is 54 Mbps, but it will automatically back down from 54 Mbps when the radio signal is weak or when interference is detected.

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, the wireless LAN can operate in the infrastructure mode. This mode lets you connect wirelessly to wireless network devices within a fixed range or area of coverage. The access point has one or more antennas that allow you to interact with wireless nodes.

In 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, the network has no structure or fixed points—each node can be set up to communicate with any other node. No access point is 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 32-character (maximum) alphanumeric key identifying the name of the wireless local area network. Some vendors refer to the SSID as the 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 the 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 are listed in Table 2-1:

**Table 2-1. 802.11g 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 wireless products in various countries are different.

- Regulations in the United States prohibit using channels greater than channel 11.
- For NETGEAR products sold outside the United States, the wireless region selection determines which channels are available for use in the product.

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

# WEP Wireless Security

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 computer can join any network and receive any messages that are not encrypted. With Shared Key authentication, only those computers 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 (Wired Equivalent Privacy) is discussed below, and WPA is discussed on page 2-8.

## WEP Authentication

The 802.11 standard defines several services that govern how two 802.11 devices communicate. The following events must occur before an 802.11 station can communicate with an Ethernet network through an access point such as the one built in to the NETGEAR product:

1. Turn on the wireless station.
2. The station listens for messages from any access points that are in range.
3. The station finds a message from an access point that has a matching SSID.
4. The station sends an authentication request to the access point.
5. The access point authenticates the station.
6. The station sends an association request to the access point.
7. The access point associates with the station.
8. The station can now communicate with the Ethernet network through the access point.

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.

## WEP Open System Authentication

This process is illustrated below.

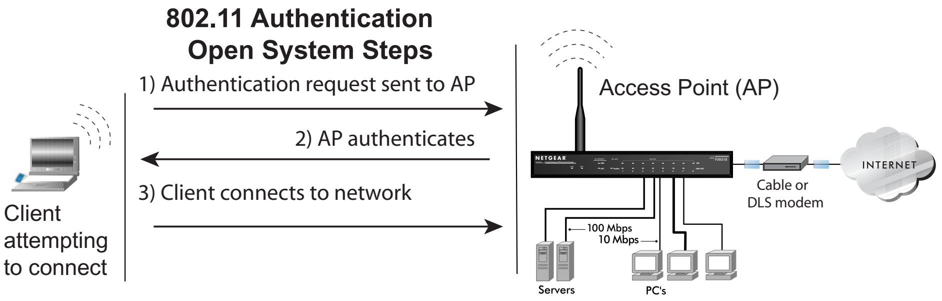

**Figure 2-1**

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.

## WEP Shared Key Authentication

This process is illustrated below.

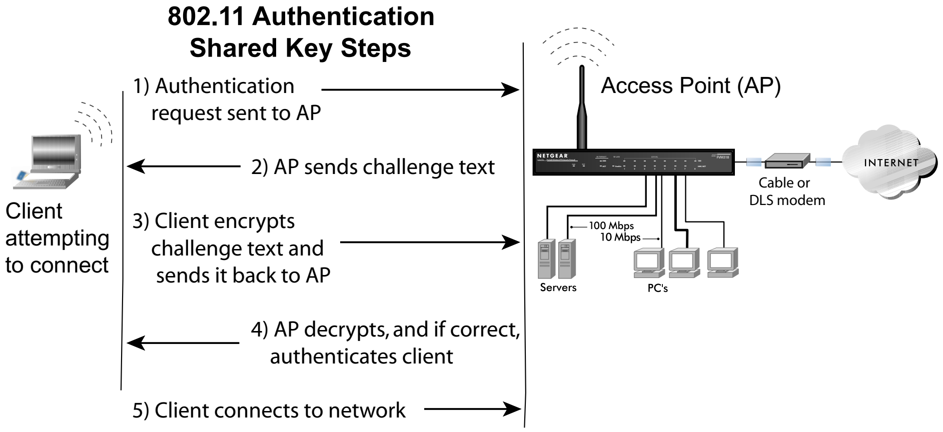
802.11 Authentication
Shared Key Steps
1) Authentication request sent to AP
2) AP sends challenge text
3) Client encrypts challenge text and sends it back to AP
4) AP decrypts, and if correct, authenticates client
5) Client connects to network
Client attempting to connect
Access Point (AP)
NETGEAR
Cable or DLS modem
INTERNET
100 Mbps
10 Mbps
Servers
PC's

**Figure 2-2**

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 it 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 (that is, 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.

## Key Size and Configuration

The IEEE 802.11 standard supports two types of WEP encryption: 40-bit and 128-bit.

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 because the user-configurable portion of the encryption key is 40 bits wide.

The 128-bit WEP data encryption method consists of 104 user-configurable bits. Similar to the 40-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.

The 128-bit encryption is stronger than 40-bit encryption, but 128-bit encryption may not be available outside the United States due to U.S. export regulations.

When configured for 40-bit encryption, 802.11 products typically support up to four WEP keys. Each 40-bit WEP key is expressed as five sets of two hexadecimal digits (0–9 and A–F). For example, “12 34 56 78 90” is a 40-bit WEP key.

When configured for 128-bit encryption, 802.11g 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.

Whatever keys you enter for an access point, 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 access point 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 access point’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

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:

- **Do Not Use WEP:** The 802.11 network does not encrypt data. For authentication purposes, the network uses Open System Authentication.
- **Use WEP for Encryption:** A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP key. The receiving 802.11g device decrypts the data using the same WEP key. For authentication purposes, the 802.11g network uses Open System Authentication.
- **Use WEP for Authentication and Encryption:** A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP key. The receiving 802.11 device decrypts the data using the same WEP key. For authentication purposes, the 802.11 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, some NETGEAR products do not offer this option.

## 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 802.11g (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 in October 2002 that remedies the shortcomings 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 in August of 2003, all new Wi-Fi certified products had to support WPA, and all existing Wi-Fi certified products had one year to comply with the new standard or lose their Wi-Fi certification. NETGEAR has implemented WPA on client and access point products. As of August 2004, all Wi-Fi certified products must support WPA.

## 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 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 do not 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 known WEP vulnerabilities.

## How Does WPA Compare to IEEE 802.11i?

WPA is 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 were ready to bring to market in 2003, 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 Remote Authentication Dial-In User Service servers, called RADIUS servers). The RADIUS server holds (or has access to) user credentials (for example, user names and passwords) and authenticates wireless users before they gain access to the network.

The strength of 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, which is Advanced Encryption Standard).

  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 passphrase on both the stations and the access point. This removes the need for an authentication server, which in many home and small office environments is neither available nor desirable. Possible cipher suites include: WEP, TKIP, and AES. We say more about 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. The 802.1X port access control prevents full access to the network until authentication completes. The 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 four-way handshake between the station and access point.
- **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 plain text message to ensure messages are not being spoofed.

### WPA Authentication:
### Enterprise-level User Authentication via 802.1x/EAP and RADIUS

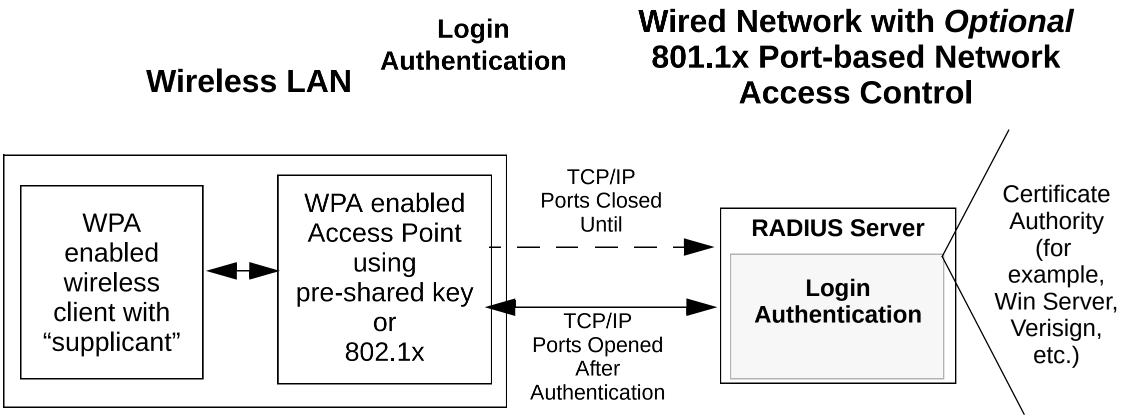
Wireless LAN
Login Authentication
Wired Network with *Optional* 801.1x Port-based Network Access Control
WPA enabled wireless client with "supplicant"
WPA enabled Access Point using pre-shared key or 802.1x
TCP/IP Ports Closed Until
TCP/IP Ports Opened After Authentication
RADIUS Server
Login Authentication
Certificate Authority (for example, Win Server, Verisign, etc.)

**Figure 2-3**

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.

Note that 802.1x does not 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 RADIUS infrastructure, WPA supports Extensible Authentication Protocol (EAP). For environments without a RADIUS infrastructure, WPA supports the use of a pre-shared key.

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

Windows XP implements 802.1x natively, and several NETGEAR switch and wireless access point products support 802.1x.

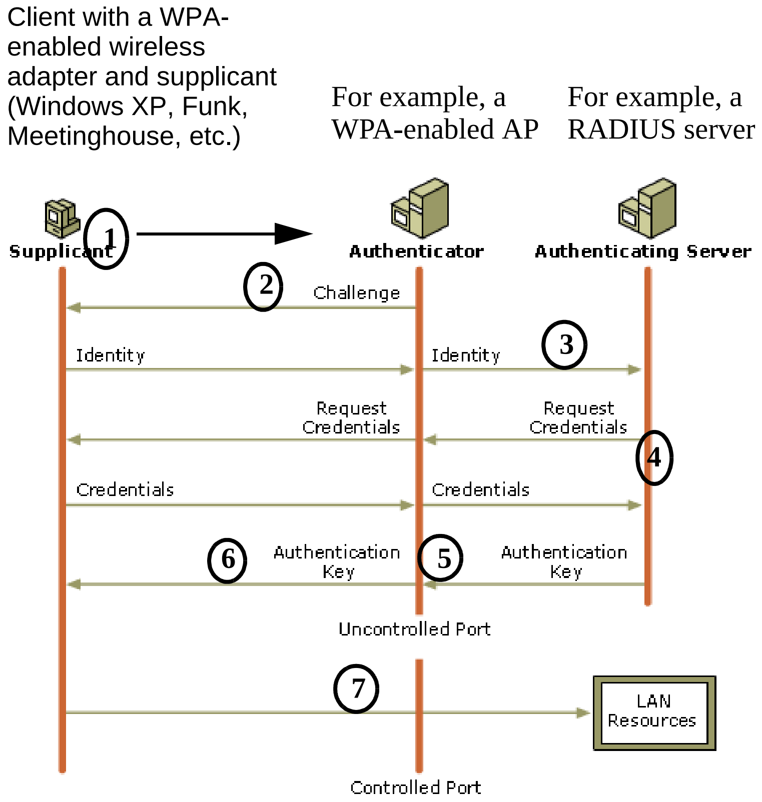

**Figure 2-4**

The access point (AP) sends Beacon Frames with WPA information elements 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 (that is, client device) attempting to connect with an authenticator (that is, 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 (for example, 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.

### WPA Data Encryption Key Management

With 802.1x, the re-keying 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, re-keying 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 pre-shared 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, besides 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-conscious 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 include 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

Some NETGEAR wireless Wi-Fi certified products support the WPA standard.

WPA requires software changes to the following:

- Wireless access points
- Wireless network adapters
- Wireless client programs

### Supporting a Mixture of WPA and WEP Wireless Clients

To support the gradual transition of WEP-based wireless networks to WPA, a wireless AP can support both WEP and WPA clients at the same time. During the association, the wireless AP determines which clients use WEP and which clients use WPA. The disadvantage to supporting a mixture of WEP and WPA clients is that the global encryption key is not dynamic. This is because WEP-based clients cannot support it. All other benefits to the WPA clients, such as integrity, are maintained.

However, a mixed mode supporting WPA and non-WPA clients offers network security that is no better than that obtained with a non-WPA network, and thus this mode of operation is discouraged.

### Changes to Wireless Access Points

Wireless access points must have their firmware updated to support the following:

- **The new WPA information element**
  To advertise their support of WPA, wireless APs send the Beacon frame with a new 802.11 WPA information element that contains the wireless AP's security configuration (encryption algorithms and wireless security configuration information).
- **The WPA two-phase authentication**
  Open system, then 802.1x (EAP with RADIUS or Pre-shared key).
- **TKIP**
- **Michael**
- **AES** (optional)

To upgrade your wireless access points to support WPA, obtain a WPA firmware update from your wireless AP vendor and upload it to your wireless AP.

### Changes to Wireless Network Adapters

Wireless network adapters must have their firmware updated to support the following:

- **The new WPA information element**
  Wireless clients must be able to process the WPA information element and respond with a specific security configuration.
- **The WPA two-phase authentication**
  Open system, then 802.1x (EAP or Pre-shared key).
- **TKIP**
- **Michael**
- **AES** (optional)

To upgrade your wireless network adapters to support WPA, obtain a WPA update from your wireless network adapter vendor, and update the wireless network adapter driver.

For Windows wireless clients, you must obtain an updated network adapter driver that supports WPA. For wireless network adapter drivers that are compatible with Windows XP (Service Pack 1) and Windows Server 2003, the updated network adapter driver must be able to pass the adapter's WPA capabilities and security configuration to the Wireless Zero Configuration service.

Microsoft has worked with many wireless vendors to embed the WPA firmware update in the wireless adapter driver. So, to update you Windows wireless client, all you have to do is obtain the new WPA-compatible driver and install the driver. The firmware is automatically updated when the wireless network adapter driver is loaded in Windows.

### Changes to Wireless Client Programs

Wireless client programs must be updated to permit the configuration of WPA authentication (and Pre-shared key) and the new WPA encryption algorithms (TKIP and the optional AES component).

To obtain the Microsoft WPA client program, visit the Microsoft Web site.