User's Manual for the Wireless Digital Media Player MP115

NETGEAR

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

Version 1.0
November 2004

Trademarks

NETGEAR is a trademark of Netgear, Inc.

Microsoft, Windows, and Windows Media Player are trademarks or registered trademarks of Microsoft Corporation.

RHAPSODY is a registered trademark of Listen.com.

Other brand and product names are registered trademarks or trademarks of their respective holders.

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.

Certificate of the Manufacturer/Importer

It is hereby certified that the Wireless Digital Media Player MP115 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

Customer Support

Refer to the Support Information Card that shipped with your Wireless Digital Media Player MP115.

World Wide Web

NETGEAR maintains a World Wide Web home page that you can access at the universal resource locator (URL) *http://www.netgear.com*. A direct connection to the Internet and a Web browser such as Internet Explorer or Netscape are required.

SOFTWARE LICENSE AGREEMENT

1. This Software License Agreement (the "Agreement") is a legal agreement between you (either an individual or an entity) ("You") and NETGEAR, Inc. ("NETGEAR") regarding the use of NETGEAR's software provided with the Wireless Digital Media Player MP115 (inside the Wireless Digital Media Player MP115, any accompanying CDs, and any accompanying documentation; together, the "Software"). BEFORE YOU USE THIS SOFTWARE, CAREFULLY READ THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU ARE NOT AUTHORIZED TO SIGN, THEN DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, BECAUSE BY DOING SO, YOU ARE AGREEING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT DOWNLOAD, INSTALL OR USE THIS SOFTWARE, AND DESTROY OR RETURN ALL COPIES IN YOUR POSSESSION.

2. Subject to the restrictions set forth below, NETGEAR grants You a nonexclusive, personal, nontransferable, perpetual (subject to Section 5) license to install and use 1 copy of the provided version of the Software in object code format, for internal and personal purposes only, on 1 computer. The Software is "in use" on a computer when it is loaded into the temporary memory or installed into the permanent memory of a computer. The license granted hereunder shall not be effective until You have paid all fees in full. Except for the license rights granted above, NETGEAR and NETGEAR's licensors retain all right, title and interest in and to the Software, including all intellectual property rights therein. YOU MAY NOT (AND MAY NOT ALLOW A THIRD PARTY TO) (a) RENT, LEASE, SUBLICENSE, SELL, ASSIGN, LOAN, USE FOR TIMESHARING OR SERVICE BUREAU PURPOSES OR OTHERWISE TRANSFER THE SOFTWARE OR ANY OF YOUR RIGHTS AND OBLIGATIONS UNDER THIS AGREEMENT; (b) reverse engineer, decompile, disassemble or attempt to reconstruct, identify or discover any source code, underlying ideas, underlying user interface techniques or algorithms of the Software by any means whatsoever, except to the extent the foregoing restrictions are expressly prohibited by applicable law; (c) remove or destroy any copyright notices or other proprietary markings; (d) attempt to circumvent any use restrictions; (e) modify or adapt the Software, merge the Software into another program or create derivative works based on the Software; (f) use, copy or distribute the Software without NETGEAR's written authorization, excepting 1 copy for archival or backup purposes only; or (g) use the Software or the Wireless Digital Media Player MP115 for commercial use. YOU MAY NOT (AND MAY NOT ALLOW A THIRD PARTY TO) COPY, REPRODUCE, CAPTURE, STORE, RETRANSMIT, DISTRIBUTE, OR BURN TO CD (OR ANY OTHER FORMAT) ANY COPYRIGHTED CONTENT (INCLUDING BUT NOT LIMITED TO MUSICAL AND MUSIC-RELATED) THAT YOU ACCESS OR RECEIVE THROUGH USE OF THE SOFTWARE. YOU ASSUME ALL RISK AND LIABILITY, CIVIL AND CRIMINAL, FOR ANY SUCH PROHIBITED USE OF COPYRIGHTED CONTENT.

3. THIS AGREEMENT SHALL BE EFFECTIVE UPON INSTALLATION OF THE SOFTWARE AND SHALL TERMINATE UPON THE EARLIER OF: (A) YOUR FAILURE TO COMPLY WITH ANY TERM OF THIS AGREEMENT OR (B) RETURN, DESTRUCTION OR DELETION OF ALL COPIES OF THE SOFTWARE IN YOUR POSSESSION. NETGEAR's rights and your obligations shall survive any termination of this Agreement. Upon termination of this Agreement, You shall certify in writing to NETGEAR or such NETGEAR licensor that all copies of the Software have been destroyed or deleted from any of your computer libraries or storage devices.

4. NETGEAR warrants that the Software will perform substantially in accordance with the documentation accompanying the Software for a period of 90 days after your initial receipt of the Software. NETGEAR's entire liability and your exclusive remedy for breach of this warranty shall be repair or replacement of the Software. This limited warranty shall be void if failure of the Software has resulted from any accident, abuse, misuse or misapplication by You. EXCEPT AS SET FORTH ABOVE, THE SOFTWARE IS PROVIDED ON AN "AS IS" BASIS. YOU ASSUME ALL RESPONSIBILITY FOR SELECTION OF THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE INSTALLATION OF, USE OF AND RESULTS OBTAINED FROM THE SOFTWARE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NETGEAR DISCLAIMS ALL WARRANTIES, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, QUALITY, ACCURACY, FITNESS FOR A PARTICULAR PURPOSE, AND FITNESS FOR YOUR PURPOSE WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING WRITTEN MATERIALS. THERE IS NO WARRANTY AGAINST INTERFERENCE WITH THE ENJOYMENT OF THE SOFTWARE OR AGAINST

INFRINGEMENT. NETGEAR DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS, BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL DEFECTS IN THE SOFTWARE WILL OR CAN BE CORRECTED.

5. In the event that a claim alleging infringement or misappropriation of an intellectual property right arises concerning the Software, NETGEAR in its sole discretion may elect to defend or settle such claim. NETGEAR, in the event of such claim, may also in its sole discretion, elect to terminate this Agreement and all rights to use the Software and require the return and/or destruction of the Software, with a refund of the fees paid for use of the Software less a reasonable allowance for use and shipping. THE FOREGOING ARE NETGEAR'S SOLE EXCLUSIVE OBLIGATIONS, AND YOUR SOLE AND EXCLUSIVE REMEDIES, WITH RESPECT TO INFRINGEMENT AND/OR MISAPPROPRIATION OF ANY INTELLECTUAL PROPERTY RIGHT.
6. UNDER NO CIRCUMSTANCES WILL NETGEAR OR ITS LICENSORS BE LIABLE FOR ANY CONSEQUENTIAL, SPECIAL, INDIRECT, INCIDENTAL OR PUNITIVE DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF DATA OR OTHER SUCH PECUNIARY LOSS), WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, PRODUCT LIABILITY OR OTHERWISE, ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF NETGEAR AND/OR ITS LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL NETGEAR'S AND ITS LICENSORS' AGGREGATE LIABILITY FOR DAMAGES ARISING OUT OF THIS AGREEMENT EXCEED THE FEES PAID BY YOU FOR THE SOFTWARE. THE FOREGOING LIMITATIONS ARE INDEPENDENT OF THE EXCLUSIVE REMEDY PROVIDED IN SECTION 6 ABOVE AND SHALL APPLY NOTWITHSTANDING ANY FAILURE OF SUCH EXCLUSIVE REMEDY OR OF ITS ESSENTIAL PURPOSE. THE FOREGOING EXCLUSIONS AND LIMITATIONS OF LIABILITY AND DAMAGES SHALL NOT APPLY TO CONSEQUENTIAL DAMAGES FOR PERSONAL INJURY.
7. You may not export or re-export the Software without: (a) the prior written consent of NETGEAR, (b) complying with applicable export control laws, including, but not limited to, restrictions and regulations of the Department of Commerce or other United States agency or authority, and (c) obtaining any necessary permits and licenses. In any event, You may not transfer or authorize the transfer of the Software to a prohibited territory or country or otherwise in violation of any applicable restrictions or regulations.
8. The Software and documentation are considered "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Use, duplication or disclosure of the Software and documentation by the U.S. Government is subject to the restrictions set forth in DFAR Section 227.7202 for military agencies and FAR Section 12.212 for civilian agencies. THIS AGREEMENT IS GOVERNED BY THE LAWS OF THE STATE OF CALIFORNIA, U.S.A., WITHOUT REFERENCE TO ITS CONFLICT OF LAWS PRINCIPLES. THIS AGREEMENT WILL NOT BE GOVERNED BY THE U.N. CONVENTION ON CONTRACTS FOR THE INTERNATIONAL SALES OF GOODS. ANY DISPUTE BETWEEN YOU AND NETGEAR ARISING UNDER THIS AGREEMENT SHALL BE SUBJECT TO THE EXCLUSIVE JURISDICTION OF THE COURTS OF THE STATE OF CALIFORNIA. This Agreement is the entire agreement between You and NETGEAR regarding the subject matter herein and supersedes any other communications with respect to the Software. If any provision of this Agreement is held invalid or unenforceable, the remainder of this Agreement will continue in full force and effect. Failure to prosecute a party's rights with respect to a default hereunder will not constitute a waiver of the right to enforce rights with respect to the same or any other breach.
9. Should you have any questions relating to this Agreement, or if you desire to contact NETGEAR for any reason, please call 1-888-NETGEAR.

Contents

Chapter 1
About This Manual

This chapter describes the intended audience, scope, conventions, and formats of this manual. This manual provides information about using the NETGEAR Wireless Digital Media Player MP115. See the online help for information about how to use the NETGEAR Media Server software. The *MP115 Installation Guide* provides basic setup and installation instructions.

Audience, Scope, Conventions, and Formats

This manual provides information about using the NETGEAR Wireless Digital Media Player MP115. For information about how to use the NETGEAR Media Server software, run the software and click *Help*. See the *MP115 Installation Guide* for information about installing the software.

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

This guide uses the following typographical conventions:

Table 1-1. Typographical Conventions

italics	Emphasis, books, CDs, URL names
bold	User input

This guide uses the following formats to highlight special messages:

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

This manual is written for the MP115 Player according to these specifications:

Table 1-2. Manual Scope

Product Version	Wireless Digital Media Player MP115
Manual Publication Date	November 2004

	Note: Product updates are available on the NETGEAR Web site at *http://www.netgear.com/support/main.asp*.

How to Use This Manual

The HTML version of this manual includes a variety of navigation features as well as links to PDF versions of the full manual and individual chapters.

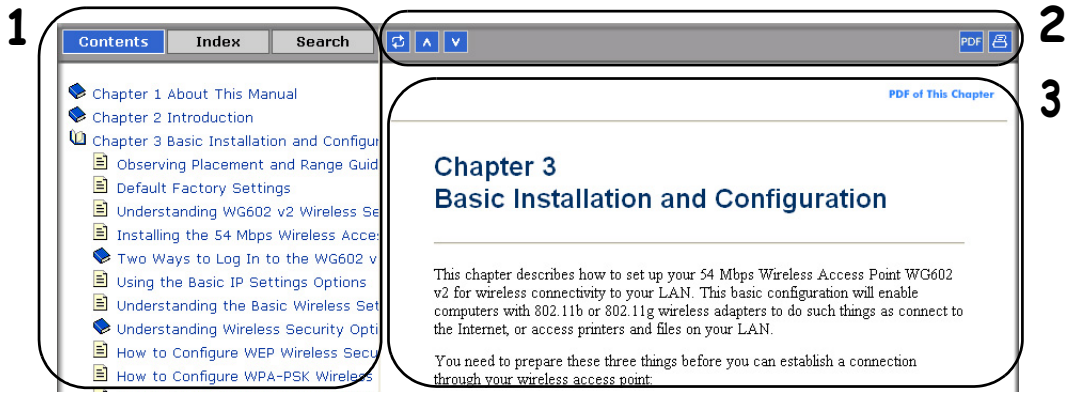


Figure 1-1: HTML version of this manual

1. **Left pane**. Use the left pane to view the Contents, Index, Search, and Favorites tabs.

   To view the HTML version of the manual, you must have a version 4 or later browser with JavaScript enabled.

2. **Toolbar buttons**. Use the toolbar buttons across the top to navigate, print pages, and more.

   The Show in Contents button locates the current topic in the Contents tab.

   Previous/Next buttons display the previous or next topic.

   The PDF button links to a PDF version of the full manual.

   The Print button prints the current topic. Click this button when a step-by-step procedure is displayed to send the entire procedure to your printer. You do not have to worry about specifying the correct range of pages.

3. **Right pane**. Use the right pane to view the contents of the manual. Also, each page of the manual includes a PDF of This Chapter link at the top right which links to a PDF file containing just the currently selected chapter of the manual.

How to Print this Manual

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

- **Printing a "How To" Sequence of Steps in the HTML View**.

  Use the *Print* button  on the upper right of the toolbar to print the currently displayed topic. Using this button when a step-by-step procedure is displayed will send the entire procedure to your printer--you do not have to worry about specifying the correct range of pages.

- **Printing a Chapter**.

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

  – Click "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.

    Note: 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 PDF button in the toolbar at the top right of the browser window.

  – Click the PDF button  on the upper right of the toolbar. The PDF version of the chapter you were viewing 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
Introduction

Congratulations on your purchase of the NETGEAR® Wireless Digital Media Player MP115. The Wireless Digital Media Player MP115 brings the media capabilities of your personal computer to the comfortable confines of your living room. Now, all the pictures, movies, and music stored in your computer, as well as streaming Internet radio content can be accessed right from your television. You can opt for the convenience of current wireless networking standards or the security and reliability of good old-fashioned wires. NETGEAR's friendly user interface and intuitive navigation puts all of your digital content at your fingertips.

The MP115 works with your computer in a client-server system. The MP115 is the client that lets you browse and play media on your television. The media files are stored on your computer (the media server) and "served" to the MP115. A network lets the two devices communicate. The network can either be wired (using the 802.3 Ethernet standard) or wireless (using the 802.11g or 802.11b standard).

Key Features

Note: This manual provides information on the complete features as of the date of publication. Go to *http://kbserver.netgear.com/products/MP115.asp* to find product firmware updates for your MP115.

The MP115 Player provides the following features:

- Wireless networking 802.11g or 802.11b, or wired LAN Ethernet.
- Easy Media server installation with online help.
- Simple menus displayed on your television for MP115 installation and management.
- Use the remote to browse selections displayed on your television screen and to listen to music, watch videos, or view pictures.
- Flash memory for firmware upgrades.

Remote Control

Use the remote control to navigate menus in the Wireless Digital Media Player MP115 and to select and view pictures or videos, or listen to music on your television. When using the remote, aim it at the logo on the right side of the MP115 front panel.

Button	Description
Power Icon	Power
Navigation	
▶	Play
■	Stop
◀◀	Rewind
⏮	Previous
⏸	Pause
▶▶	Fast forward
⏭	Next
OK	Select/Play
Home Icon	Main menu
i	Display media information
Vol +/–	Increase or decrease volume
Page +/–	Scroll up or down
arrow	Mute
Music	Music menu
Video	Video (Movies) menu
Pics	Picture menu
Settings	Settings menu
0-9	Numeric entry, presets and search
Disp Sel	Display Select: troubleshoot by cycling through all eight options for display output.
Shuffle	Play the selected media in random order
Repeat	Repeat a track or the entire media selection

Front Panel

The front of the Wireless Digital Media Player MP115 has a light that shows when it is turned on. The **digita**l logo on the right side shows where to aim the remote when you push buttons.

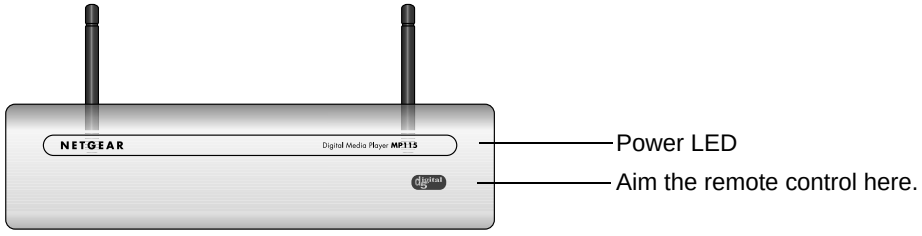


Figure 2-1: MP115 Front Panel

Rear Panel

The rear panel of the MP115 contains the connectors.

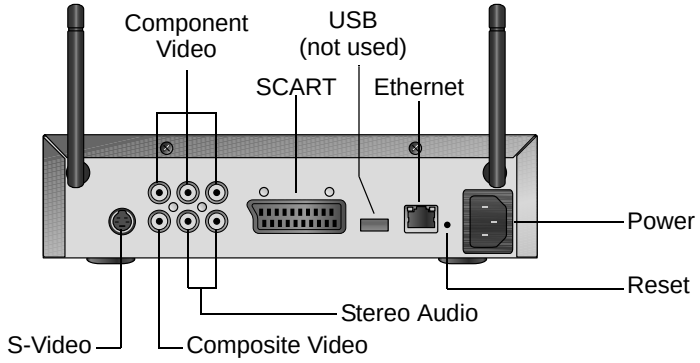


Figure 2-2: MP115 Rear Panel

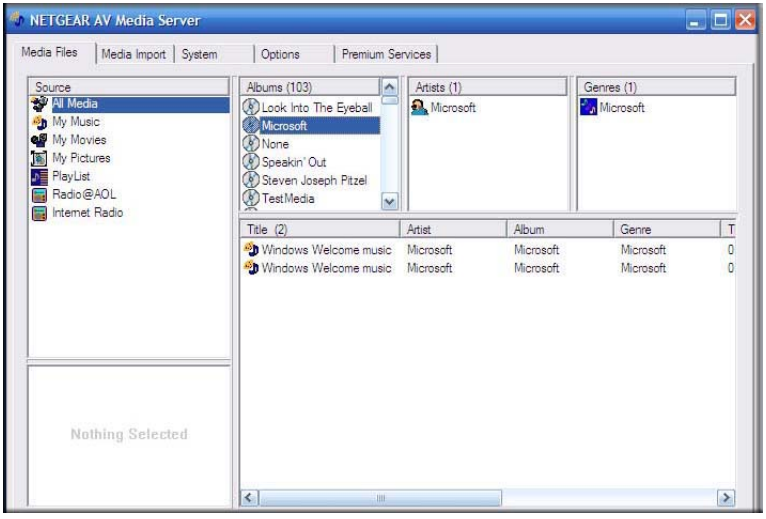
Viewed from left to right, the rear panel contains the following features:

- **S-Video port:** This type of cable does not ship with the product, and you will need to change the MP115 settings in order to use it.
- **Component Video ports:** This type of cable is not included, but the MP115 is compatible with this cable.

- **Composite Video and L/R Audio:** This type of cable is included, and is compatible with most televisions in the United States.
- **SCART:** This cable is widely used in Europe and Australia. Though this cable is not included in the package, the MP115 is set up to be compatible with this cable.
- **USB:** Reserved for future use.
- **Ethernet:** 10/100 Mbps Ethernet port for connecting the media player to a wired LAN (local area network).
- **Reset:** This button resets the MP115.
- **Power:** The MP115 includes an internal power supply and universal power adapter.

Media Server Software

The Wireless Digital Media Player MP115 comes with Media Server software that runs on a computer on your home network. The Media Server software is easily installed from the Resource CD. During installation, the Media Server scans the network for media files, which are then available for MP115 to play. After installation, it automatically starts when that computer is powered on. You may use the Media Server to scan for additional media at any time.



Media Server Software Tabs

The Media Server software includes detailed online help, which is not included in this manual. The Media Server software includes five tabs:

- **Media Files tab:** Scan computers on the network to locate media files, which you can then play on the MP115 Player.
- **Media Import tab:** Import Plugins and scan for media files, which you can then play on the MP115 Player.
- **Options tab:** Specify file types to scan. Display media files.
- **System tab:** Manage network settings such as the Server Name. View Media Server status, and statistics.
- **Premium Services tab:** Manage Internet radio.

Package Contents

The product package should contain the following items:

- Wireless Digital Media Player MP115.
- Remote control (2AA batteries included).
- Power cable, localized to country of sale.
- Category 5 (CAT5) Ethernet cable.
- Composite Video cable and Audio cable.
- *NETGEAR Wireless Digital Media Player MP115 Resource CD* , including:
  - This guide.
  - The Installation Guide.
  - Application Notes and other helpful information.
- *Wireless Media Player MP115 Installation Guide.*
- Warranty/Support Information card.

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the router for repair.

Maintenance and Support

NETGEAR offers the following features to help you maximize your use of the MP115 Player:

- Flash memory for firmware upgrades.
- Free technical support seven days a week, 24 hours a day, for 90 days from the date of purchase.

Chapter 3
Connecting Your Media Player

This chapter describes how to set up the Wireless Digital Media Player MP115 on your local area network (LAN).

Verifying That Basic Requirements Are Met

- Make sure that you have the following:
  - A wireless (802.11b or 802.11g) or Ethernet network
  - One or more computers running Windows 98SE, 2000, ME or XP
  - Television set
  - Broadband Internet service (recommended)
- Have your Network Name (SSID) and security settings handy.
- Firewalls can interfere with or block MP115 performance. If you are running Windows XP Service Pack 2, then during installation the *NETGEAR Wireless Digital Media Player MP115 Resource CD* sets the firewall up to be compatible. If you use other firewalls, such as ZoneAlarm, set the following ports to be open:
  - UDP Ports: 1360, 1900
  - TCP Ports: 1025 – 1035, 3640, 3641, 4000, 4001, 7000 – 7010, 49200 – 49210

  Also see the Media Server software online Firewall topic.

First, Install the Media Server Software

1. Power on your computer and log in as needed.
2. Insert the *Resource CD* into the CD drive on the computer. The CD main page loads.
3. Follow the InstallShield Wizard steps and click Finish when done.

   Note: Depending on your location, complimentary 30-day trials for Internet radio stations may be available for vTuner and Rhapsody. The *Resource CD* automatically installs vTuner. To use the trial for Rhapsody, you must also select INSTALL RHAPSODY Digital Music Service and complete that installation.

4. Restart your computer and the NETGEAR Media Server software automatically runs. The Media Server software icon appears on the Windows System Tray.
5. Use the Media Server software to scan your hard drive to locate your video, picture, and music files. For more information, see "Media Server Software Tabs" on page 4-2, Chapter 4.

   Note: You can use the Options tab on the Media Server to specify which types of files you want to include, as described in the Media Server online help.

Then, Install the MP115 Player

1. Determine which type of cable your television uses:
   - **Video cable and Audio cable:** These two cables are included, and are compatible with most televisions in the U.S.
   - **SCART:** This cable is often used in Europe and Australia, and is not included in the package. However, if you have a SCART cable the MP115 will recognize it, and you can continue to use these instructions.
   - **S-Video, or Component Video:** These cables are not included in the package. If you use this type of cabling you will be prompted to select video output settings when the MP115 first starts up.

2. For composite video, connect the supplied video cable and audio cable to the Composite Video and Stereo Audio ports on the back of the MP115.

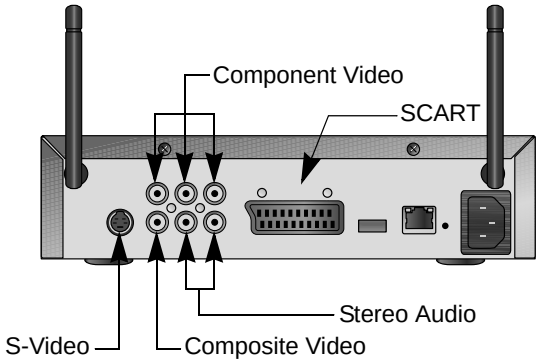


Figure 3-1: MP115 rear view, cable connections

If you are supplying your own SCART, S-Video, or Component Video cable, connect it (and the audio cable if applicable) to the corresponding port on the back of the MP115.

3. Connect the other end of the cables to the corresponding ports on your television.

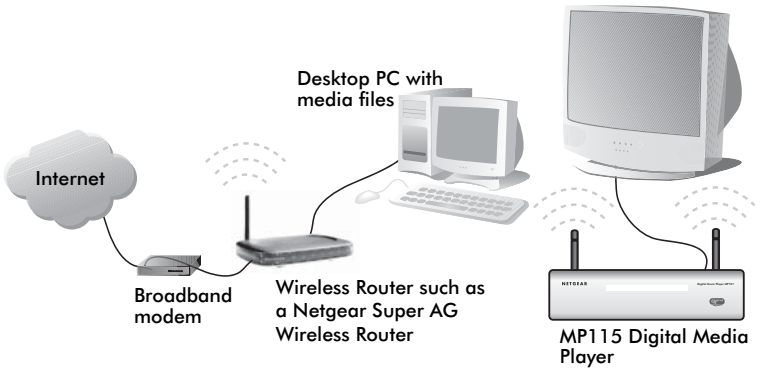


Figure 3-2: Wireless home network with MP115 and television

4. If you have a wired LAN network (not wireless), use an Ethernet cable such as the one provided in the package to connect the MP115 to your router.
5. Install the two AA batteries into the remote control that shipped with the product.

Next, Select the Network and Server for the MP115

Warning: The MP115 includes an internal power supply and universal power adapter. NETGEAR strongly recommends that you confirm the power requirements for your local jurisdiction before you utilize the power cord supplied with the product.

1. Make sure that the MP115 Media Server software is running.

   Note: The Media Server software automatically runs when you restart your computer, and this icon appears on the Windows System Tray.

2. Turn on the television.

3. Connect the MP115 power cord and plug it into an outlet.

   The LED on the front of the MP115 lights up to show that it is powered on. The logo on the lower right corner of the MP115 shows where to aim the remote control.

   The MP115 start-up screen appears on the television screen as shown below:

Figure 3-3: Start-up screen shown on the television

The MP115 automatically performs the following tasks:

- Checking Hardware
- Finding Network
- Getting IP Address
- Finding Server
- Accessing Media

Note: If you have connected an S-Video or Component Video cable, and if the MP115 is not configured to generate output to its S-Video or Component Video ports, then you may see a flickering image or no image on your television screen. The MP115 executes its power on routine in the background.

To fix this problem, push **Disp Sel** on the remote control to cycle through all video output options and select the correct one.

4. If your network is wireless and/or uses security settings, the MP115 stops at Finding Network, and goes to the Settings: Available Networks screen.
    - The MP115 is set from the factory to get its IP Address from a DHCP server. If your network does not use DHCP, you must set up the MP115 with a Static IP Address in the range of addresses on your network.
    - If the MP115 is set to use DHCP and fails to obtain an IP Address from the server, it will resort to an auto IP Address in the range of 169.254.x.x. You can use a Static IP Address if there is a problem connecting the MP115 to the server.
5. Use the remote control to enter your wireless and security settings.

    Then the main menu appears as shown below:

Figure 3-4: Main menu displayed on the television screen

All the files that you scanned with the Media Server software are now available to play on the Wireless Digital Media Player MP115. Use the remote control to select the desired media.

Note: If the MP115 does not connect to the network, it displays the Settings: Network menu. Use the remote to browse and select an Available Network from the onscreen display. For more information, see "Connecting to the MP115" on page 6-1, Chapter 4.

Chapter 4
Videos, Pictures, and Music

Media Formats

To play media, the MP115 must be connected to the network, and the Media Server software must be running. To scan for digital files, go to the computer running the Media Server software and use the Media tab and Media Import tab. The files may be stored on any computer on the network, or on a CD in the computer's CD drive.

The Wireless Digital Media Player MP115 is compatible with the following media file formats:

- MPEG 1, 2, 4 compressed audio and video files
- JPEG and GIF compressed image files
- BMP and TIFF image files
- MP3s up to 320 Kbps or variable bit rate (VBR)
- WMA8 and WMA9 files up to 192Kbps or variable bit rate (VBR)
- WAV audio files
- Internet Radio (streaming MP3)
- Playlist Formats:
  - M3U
  - PLS

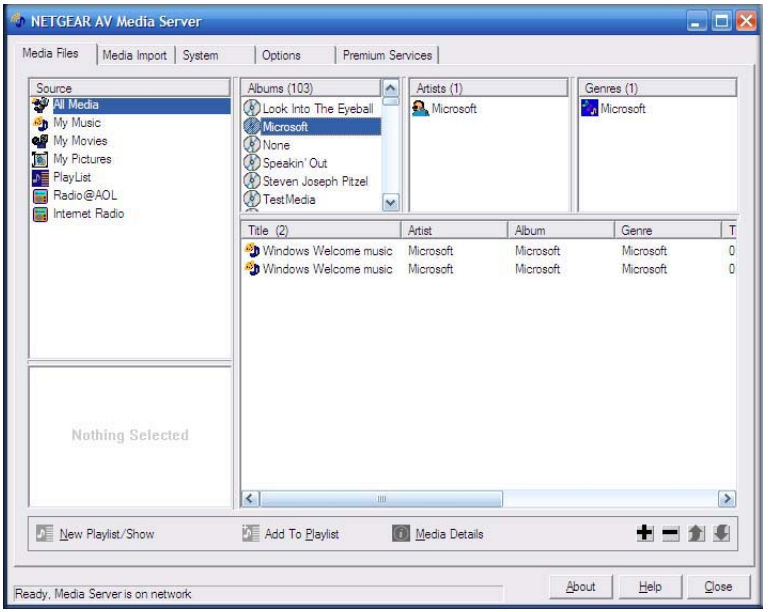
Media Server Software

The Media Server software is easily installed from the Resource CD as described in Chapter 3, "First, Install the Media Server Software " on page 3-2. After installation, it automatically starts when that computer is powered on. The Media Server software icon  appears on the Windows System Tray.

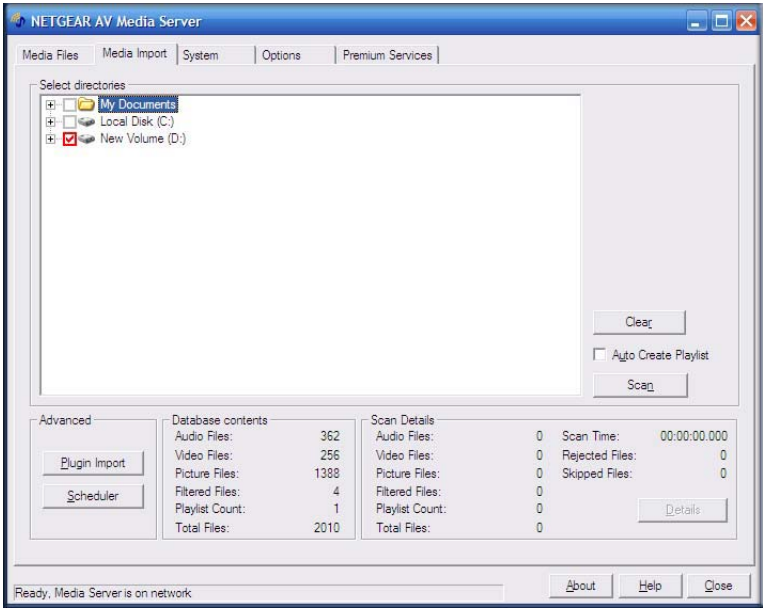
Media Server Software Tabs

The Media Server software has detailed online help, which is not included in this manual. The Media Server software features are grouped onto five tabs:

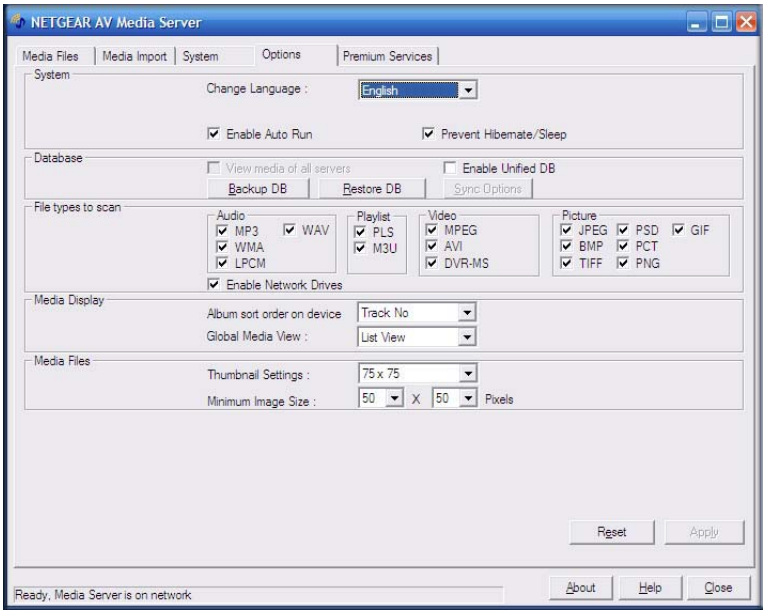
- **Media Files tab:** Scan computers on the network to locate media files, which you can then play on the MP115 Player.



- **Media Import tab:** Import Plugins and scan for media files to play on the MP115 Player.



- **Options tab:** Specify file types to scan. Display media files.



- **System tab:** Manage network settings such as the Server Name. View Media Server status, and statistics.
- **Premium Services tab:** Manage Internet radio.

Watching Videos on Your Television

Before the MP115 can play videos, you must use the Media server software running on your computer to scan and locate your media files. If you want to include media files that are stored on other computers, external hard drives, or other storage devices on the network, make sure to select them when you scan.

Note: You can use the Video Settings menu to set the TV Aspect Ratio, Video Mode, or Video Output. See "Setting the TV Aspect Ratio" on page 5-4.

Use the remote control to select My Video from the Main menu displayed on the television. The Video menu displays the following options:

- **All**: List all available video files in alphabetical order.
- **Albums**: List video files by album.
- **Video Show:** The video show allows you to combine two or more video files into a single show. This is useful when you have a movie that is stored on your computer as several files.

Note: To display information about the video, push **i** on the remote control. This option is only available when a movie is listed or playing:

Searching Alphabetically with the MP115 Remote Control

Any list of content can be searched alphabetically using the alphanumeric keypad on the remote control. This technique is useful for quickly finding an desired selection in a long list of items.

To search a listing alphabetically:

1. Navigate to the directory that contains the desired item.
2. Press the button on the alphanumeric keypad that corresponds to the first letter of the desired item. Pressing each button will cycle through the letters and number printed on the button. For example, pressing 5 will cycle through J-K-L-5.
3. Continue entering additional letters or numbers. Use the ◀◀ or |◀◀ button to backspace. The alphabetic search is *not* case sensitive.
4. Press **OK** to execute the search. The window will scroll to the first item that matches the search criteria.

Viewing Pictures

Before you can view pictures with the MP115, you must use the Media server software running on your computer to scan and locate your media files. If you want to include media files that are stored on other computers, external hard drives, or other storage devices on the network, make sure to select them when you scan.

Use the **Pics** button on the remote control, or select My Pictures from the Main menu to go to the Pictures menu. The Pictures menu shows the following selections:

- **All:** Show all the digital photographs in alphabetical order, by file name. Select the desired photographs to view.
- **Albums:** View photographs by albums.
- **Slideshow:** View all photographs in a selected directory. The MP115 automatically displays one photo after the other. To adjust the length of time each picture is shown for a Slideshow, see "Setting the Slideshow Time" on page 5-2.

Note: You can browse photos by List View or by Thumbnail View; and with or without Previews. To customize these settings, see "Changing the Display" on page 5-1.

Working with Music Files

Before the MP115 can play music, you must use the Media server software running on your computer to scan and locate your media files. If you want to include media files that are stored on other computers, external hard drives, or other storage devices on the network, make sure to select them when you scan.

Some audio files may be stored without information in some fields, such as album or genre. If this is the case, these tracks are listed in a category called "Unknown". Internet Radio selections are listed under the Premium Content selection on the main menu. See "Playing Music from the Internet" on page 4-8.

My Music Menu

You can use the **Music** button on the remote to go to the Music menu, or select My Music from the main menu displayed on your television. The Music menu appears as shown below:

Figure 4-1: Music menu displayed on the television screen

The Music menu offers the following selections:

- All
- Albums
- Artists
- Genres
- Music Playlist

Playing All

1. Select **All** from the Music menu.

   The tracks are listed in alphabetical order.

2. Scroll to the desired album. To *fast scroll*, hold down the Up or Down arrows for three seconds. The Left or Right arrows also *fast scroll* at a faster rate. To perform an alphabetic search see "Shuffle and Repeat" on page 4-7.

3. Push the **Repeat** button on the remote and an icon appears on the lower right of the television screen. Use this button to cycle through three options: all tracks (arrow), one track (1), or play and repeat all (two curved arrows).

Playing Albums

You can play an entire album, or a specific song in the album.

1. Select **Albums** from the Music menu.

   The albums are listed in alphabetical order.

2. Scroll to the desired album. To *fast scroll*, hold down the Up or Down arrows for three seconds. The Left or Right arrows also *fast scroll* at a faster rate. To perform an alphabetic search see "Shuffle and Repeat" on page 4-7.

3. Push the **Repeat** button on the remote and an icon appears on the lower right of the television screen. Use this button to cycle through three options: all tracks (arrow), one track (1), or play and repeat all (two curved arrows).

Playing Songs by an Artist

1. Select **Artist** from the Music menu.

   The artists are listed alphabetically.

2. Scroll through the list and select the desired artist. To *fast scroll*, hold down the Up or Down arrows for three seconds. The Left or Right arrows also *fast scroll* at a faster rate. To perform an alphabetic search see "Shuffle and Repeat" on page 4-7.

3. Push the **Repeat** button on the remote and an icon appears on the lower right of the television screen. Use this button to cycle through three options: all tracks (arrow), one track (1), or play and repeat all (two curved arrows).

Playing Songs by Genre

1. Select **Genre** from the Music menu.

   The genres that are listed depend on the media files that are on your media server or Internet music server. Some formats, such as MP3 include genre. If a music file does not contain a genre, it is listed as Unknown, at the end of the list of genres.

2. Scroll to the desired genre. To *fast scroll*, hold down the Up or Down arrow for three seconds. The Left or Right arrows also *fast scroll* at a faster rate. To perform an alphabetic search see "Shuffle and Repeat" on page 4-7.

3. Push the **Repeat** button on the remote and an icon appears on the lower right of the television screen. Use this button to cycle through four options: genre (musical note), all tracks (arrow), one track (1), or play and repeat all (two curved arrows).

Playing a Music Playlist

1. Select **Music Playlist** from the Music menu.

2. Scroll to the desired playlist and select it.

3. Push the **Repeat** button on the remote and an icon appears on the lower right of the television screen. Use this button to cycle through the options: music playlist (musical note), all tracks (arrow), or one track (1).

Shuffle and Repeat

Shuffle mode plays the selected songs in random order. Repeat lets you repeat a track or the entire selection that you are playing.

Press the **Shuffle** button on the remote control to toggle Shuffle mode on and off. When Shuffle is on, an icon appears on the lower right corner of the television.

Press the **Repeat** button on the remote control to cycle through Repeat modes.

Playing Music from the Internet

vTuner

vTuner lists thousands of Internet Radio stations from over 100 countries around the globe. You can use the Wireless Digital Media Player MP115 to play Internet Radio from vTuner. The vTuner Basic Internet Radio Guide includes a limited number of stations and is included at no charge with your MP115. vTuner Super Guide includes a much larger list of stations and is available for an additional charge. You can sign up for vTuner Super Guide at *http://www.radio1234.com*. You can go to this Web site by clicking the **Radio1234.com** button on the Options tab of the NETGEAR Media Server software.

The Radio1234.com station list is customized for the MP115 and contains only stations that are broadcast in formats it can support.

To play a vTuner Internet Radio station:

1. Select **Premium Content** from the Main menu.
2. Select I**nternet Radio**.

   You can use the options displayed on the television screen to search for radio stations by Genre, Countries, New Stations or Popular Stations.

   Note: You can also select from stations in the My Favorites list. The My Favorites selection will not appear until you have selected radio stations at *http://www.radio1234.com*. This URL can be accessed by clicking the **Radio1234.com** button under the Options tab of the NETGEAR Media Server software.
3. Select an option, and then scroll and select the tracks you would like to play.

Rhapsody

Note: Rhapsody Digital Music Service is available only in the United States.

The Wireless Digital Media Player MP115 can play music over the Internet from Rhapsody Digital Music Service. The Rhapsody service runs on its own server software, which must be installed on your computer in addition to the NETGEAR Media Server Software. After installation you can use the MP115 to select the Rhapsody server. You will have access to all the tracks, albums, playlists and digital radio stations on the My Library tab in your Rhapsody account.

To play Rhapsody Internet radio station:

1. If you do not already have a Rhapsody account, use the *Resource CD* to install the free 30-day trial account on a computer that is on your home network.
2. Access your Rhapsody account.

   Note: Be sure that UPnP Server is enabled in the Rhapsody application. This setting can be found in the Options, User Settings menu item, under the UPnP tab. The UPnP Server will be enabled by default if Rhapsody is installed from the *Resource CD*.
3. Go to the MP115 and push the **Settings** button on the remote control.

   The Settings menu displays on the television.
4. Select **Servers**.
5. Select the **Rhapsody** server. You will receive a message confirming the connection.

   All the music from the *My Library* folder on the Rhapsody server is now accessible from the Wireless Digital Media Player MP115. You can access this music by artist, album, tracks, playlists or radio stations.
6. Select **Premium Service** from the main menu displayed on your television.
7. Select **Rhapsody**.
8. Scroll and select the tracks you would like to play.

Note: The Rhapsody server may not support all of the features that are available on the NETGEAR Media Server software.

Chapter 5
Settings and Maintenance

This chapter describes how to use the configuration and maintenance features of your Wireless Digital Media Player MP115.

Note: If you want to change network settings or options for the Media Server software, use the Media Server Options tab and Media Server System tab as described in the Media Server online help.

Settings

Press the **Settings** button on the remote control. The Settings menu offers the following selections:

- **Servers:** Select an available media server or music server.
- **Network:** Configure your wired or wireless network connection.
- **Video:** Set your preferred video display format, video outputs and aspect ratio.
- **Display:** Set your language preferences, list view settings, Slideshow timing, and screen saver.
- **Maintenance:** Search for and install the latest firmware.
- **Help:** Basic network and player help.

Changing Servers

1. From the Settings menu, select **Servers**.
2. The MP115 searches for servers. You can use the Refresh button at the bottom of the television screen to update the display.
3. Select the server that you want to use.

IP Address

The Wireless Digital Media Player MP115 is set by default to get its IP Address via DHCP. With this setting, the DHCP server on your network assigns the IP Address to the MP115, which is a is a client. If your network does not use DHCP, then you must set the IP Address for the MP115 to be in the correct subnet range for your network.

1. Push the **Settings** button on the remote.
2. Select **Network**, and then select **IP Address**.

   The screen shows DCHP and Static. The MP115 ships set up to use DCHP.
3. Select an option and view the IP Address, Subnet Mask, Network Type, and Network Name.

Available Wireless Networks

1. Push the **Settings** button on the remote.
2. Select **Network**, and then select **Wireless**.
3. Select **Available Networks**.

   The screen shows the following information about the available networks:

   - **Name:** The Network Name (SSID)
   - **Channel:** The channel that the wireless access point is using.
   - **Mode:** AP (Access Point) is the normal setting.
   - **Security:** The default is Disabled.
   - **Signal:** Good, fair, or poor.
4. If you want to change to another network, select the network.

   Note: Networks that do not broadcast their SSID may not appear on this screen. For information about working with hidden networks see "Hidden Networks" on page 5-3. Also see "Wireless Link" on page 6-2.
5. Select Apply and push OK.

Adding a New Network

1. Push the **Settings** button on the remote.
2. From the Settings menu, select **Wireless**.
3. Select **New/Hidden Networks**.

   You are prompted to enter your wireless network SSID (up to 32 characters).
4. Enter the network name (SSID), select **Next** and push **OK**
5. Select **New** for the network type.
6. Select the security level.

The default setting is Disabled. To accept this setting, select NEXT; or press the UP arrow to select WEP mode and specify the key size.

Hidden Networks

Use this option if you want the MP115 to look for a network that does not broadcast its SSID.

1. Push the **Settings** button on the remote.
2. From the Settings menu, select **Wireless**.
3. Select **New/Hidden Networks**.

   The MP115 sends a message to check for hidden networks and also looks for new networks.
4. Check the display on the television screen to see if the network is now listed on the Available Networks screen.

Manually Setting Wireless Configuration for Hidden Networks

Note: Detailed background information about wireless networking can be found in Appendix B, "Wireless Networking Basics".

In order to configure the MP115 to work in a network where the SSID broadcast is disabled, you must manually configure the wireless settings. Also, it may be necessary to manually configure an Ad Hoc network.

To configure wireless settings manually:

1. Push the **Settings** button on the remote.
2. Select **Network**, and then select **Wireless**.
3. From the Wireless menu, select **New/Hidden Network**.

   The current wireless settings, if any, are displayed in the second row for your reference.
4. Press **OK** to accept the setting or press ▶ to change the setting. Enter a value of up to 32 alphanumeric characters for the SSID. After entering the new SSID, press **OK** to save.

   The Wireless Mode is displayed.
5. Press **OK** to accept the setting or press ▶ to change the setting. Options for wireless mode are Infrastructure and Ad/Hoc. If Ad/Hoc is chosen, you will also need to choose a location along with a wireless channel.

6. The WEP Security screen will now be displayed. Detailed instructions for configuring WEP can be found in Appendix B, "Wireless Networking Basics".
7. The system reboots and connects to the selected wireless network.

Specifying the Wireless Location

You can specify the country where your wireless network operates.

1. Push **Settings** on the remote control to go to the Settings menu.
2. From the Settings menu, select **Network**, and then select **Wireless**.
3. Select **Location**, and choose the correct location for your network.
4. Click **Apply** to save the setting.

Setting a Static IP Address

The MP115 is set up to use DHCP. With DHCP, the MP115 get its IP address from a DHCP server on the network. If your network does not use DHCP, then you need to change the MP115 settings to a Static IP Address, and set the IP Address to a subnet within the correct range for your network.

1. Push **Settings** on the remote control to go to the Settings menu.
2. From the Settings menu, select **Network**, and then select **IP Address**.

   The Settings: Network:IP Address screen appears.
3. Select **Static**.
4. Use the number buttons on the remote control to enter the IP Address. Use the **OK** button to save each number and move to the next field.
5. After the IP address is set, enter the subnet mask.

Video Settings

Use the Video Settings menu to set the TV Aspect Ratio, Video Mode, or Video Output.

Setting the TV Aspect Ratio

You can set the Aspect Ratio to Letter Box, Full Screen, or 4:3.

1. Push the **Settings** button on the remote to go to the Settings menu.

2. Select **Video**.
3. Select **TV Aspect Ratio**.
4. Use the navigation buttons on the remote control to display the desired setting.
5. Select **Apply**, and push **OK** on the remote control.

Setting the Video Mode

Set the Video Mode to NTSC, or PAL.

1. Push the **Settings** button on the remote to go to the Settings menu.
2. Select **Video**.
3. Select **Video Mode**.
4. Use the navigation buttons on the remote control to display the desired setting.
5. Select **Apply**, and push **OK** on the remote control.

Video Output

Note: If you select the wrong Video Output, then you may not be able to see the menus on the television. To correct this problem, push the **Disp Sel** button on the remote control. You can cycle through each of the eight possible video modes to find and select the correct one.

You can choose S-Video, SCART, Component Progressive, or Component Interlaced.

- **S-Video:** This cable is not included in the package. If your television uses S-Video, you must provide your own cable and set the Video Output to S-Video.
- **SCART:** This cable is often used in Europe and Australia, and is not included in the package. However, if you have a SCART cable the MP115 will recognize it.
- **Component Progressive and Component Interlaced:** The MP115 is set by default to work with component video cables. To use component progressive you must have a television that supports this technology.

Changing the Video Output Settings

1. Push the **Settings** button on the remote to go to the Settings menu.
2. Select **Video**.
3. Select **Video Output**.
4. Use the navigation buttons on the remote control to display the desired setting.

5. Select **Apply,** and push **OK** on the remote control.

Changing the Display

1. Push the **Settings** button on the remote to go to the Settings menu.
2. From the Settings menu, select **Display**.
3. The Display menu offers the following selections:
   - **Photo/Video Browsing:** Choose List View or Thumbnail View.
   - **Previews:** On or Off.
   - **Language on Screen:** Choose English, German, or French.
   - **Setting the Slideshow Time:** Set the length of time that each picture is displayed during a Slideshow. The Slideshow time may be set to 5 seconds, 8 seconds, or 10 seconds, as explained below.
   - **Selecting the Screen Saver:** Toggle between Floating Logo and Blank Screen.

Setting the Slideshow Time

Set the length of time that each picture is displayed during a Slideshow. The Slideshow time can be set to 5 seconds, 8 seconds, or 10 seconds.

1. Push the **Settings** button on the remote to go to the Settings menu.
2. From the Settings menu, select **Display**.
3. Select **Slideshow Time**.
4. Use the navigation buttons on the remote control to display the desired setting.
5. Select **Apply**, and push **OK** on the remote control.

Upgrading the Wireless Digital Media Player MP115

Warning: Do not play media on the Wireless Digital Media Player MP115 during the upgrade.

1. On the computer that runs the Media Server software, download new firmware from the *http://www.NETGEAR.com* support site.
2. Run the firmware installer program, as described in the firmware release notes.
3. Go to the MP115 and push the **Settings** button on the remote to display the Settings menu.
4. Select **Upgrade Firmware**.

   The television screen shows the Current Firmware Version and lists Available Upgrades.

5. If there is an upgrade available, select it.
6. Select **Apply Upgrade** and push **OK** on the remote control.

   The unit reboots and reconnects to the last network used.

Chapter 6
Troubleshooting

This chapter gives information about troubleshooting your Wireless Digital Media Player MP115. After each problem description, instructions are provided to help you diagnose and solve the problem.

No Television Display

If the wrong video output is set on the MP115 then the television display will not work. Push the **Disp Sel** button on the remote control to cycle through the video output settings. When you have reached the correct setting, the television display will work. Select that setting and push OK on the remote control.

Connecting to the MP115

Here are some tips for correcting simple problems that may prevent you from connecting to the media player.

Problem	Recommended Action
MP115 does not respond to the remote control.	• Check the LED on the front panel of the MP115 to make sure the power is on. • Make sure the television is turned on. • Aim the remote control at the logo on the upper right of the MP115. • The LED on the remote control should flash when you push a button. — If the LED does not flash, and the batteries are working, then the remote may be faulty. — If the LED does flash, reset the MP115
MP115 does not find my network.	• Make sure the Wireless Network Name (SSID) and WEP settings of the MP115 and media server match exactly. • Restart the media server software, then power cycle the MP115.

MP115 does not find the server.	• Make sure your computer is running the media server software. • If you wish to use Rhapsody, make sure that the media server is running Rhapsody, and that Rhapsody is the selected server for the MP115. • Computer firewall software can prevent the media server from communicating with theMP115. See the Firewall topic in the media server online help. • If you do not use DHCP on your network, you must set the IP address of the MP115 in the range of addresses on your network. See IP Address on page 6-3.

Physical Connectivity

Ethernet Link

Because the MP115 incorporates Auto Uplink technology (also called Auto MDI/MDI-X), it is capable of automatically sensing the polarity of the Ethernet connection. You can therefore connect using either a standard or crossover Ethernet cable. The Ethernet port of your MP115 will automatically configure itself properly.

If connecting to your network using Ethernet, the link LED on the back of your MP115 and on your hub or router should both be on. If not, try the following:

- Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.

Wireless Link

Please be aware that wireless data rate and throughput decreases as the distance increases between the Access Point (AP) and the MP115 Player. If you are unable to detect any wireless networks, try the following:

- Your wireless AP (access point) may be too far from the MP115. It may be necessary to move either the AP or the MP115 so that they are closer together.
- If you are using a wireless connection between the AP (or wireless router) and the computer that serves the media content, you might also need to move the computer and the AP closer together.

- If your access point is configured to disable broadcast of SSID, the MP115 will not be able to detect it. You will need to manually configure your wireless settings as described in "Manually Setting Wireless Configuration for Hidden Networks" on page 5-6.
- The MP115 cannot connect to the wireless network while it is connected to the Ethernet network. Disconnect your Ethernet cable.

IP Address

If the MP115 is unable to receive a valid IP address, try the following:

- Verify that a working DHCP server is on your network. PCs on the network should get IP addresses in the correct range.
- If you are using a wireless network, verify that the MP115 is associated with the correct SSID. The SSID that is being used can be displayed by following instructions in "Manually Setting Wireless Configuration for Hidden Networks" on page 5-6.
- If you are using a wireless network, verify that the WEP settings on the MP115 match the settings on your access point. Instructions for setting WEP can be found in Appendix B, "Wireless Networking Basics. If you are using a passphrase, note that it is case-sensitive. Using the WEP Wizard you can view the hex key generated by the passphrase algorithm directly. This must match the setting on your access point.

Connecting to the Server

If the MP115 cannot find the correct server, try the following:

- Verify that the NETGEAR Media Server is running on your PC. You should be able to see the icon in the system tray. If it is not on the network, there will be a red bar through the icon.
- Verify that the MP115 and the PC running the Media Server software are on the same subnet and that they can communicate with each other. In most cases, this means that the first three fields of the two IP address should be the same. Communication can be verified using the Windows Ping utility.

  1. From the Windows toolbar, click on the **Start** button and select **Run**.
  2. In the field provided, type ping followed by the IP address of the MP115. Displaying the IP address is described in IP Address on page 5-2.

     PING 192.168.0.2

3. Click **OK**. You should see a message like this one:

   PINGING <IP ADDRESS> WITH 32 BYTES OF DATA

   If the path is working, you see this message:

   REPLY FROM < IP ADDRESS >: BYTES=32 TIME=NN MS TTL=XXX

   If the path is not working, you see this message:

   REQUEST TIMED OUT

4. If you cannot ping the MP115 your network may not be working correctly.

- The Status Bar of the NETGEAR Media Server, which can be found at the bottom of the window, should show "Media Player is on the network." If the Status Bar shows "Media Server is not on network!", verify that your PC has a valid IP address and that the correct adapter is chosen. The adapter is chosen using the Change Adapter button under the System tab.
- If multiple adapters are installed in your PC, the Media Server software can only monitor one of them at a time. Verify that the correct adapter is chosen. The adapter is chosen using the Change Adapter button under the System tab.

Connecting to the Rhapsody Server

If the MP115 cannot find your Rhapsody server, try the following:

- The Rhapsody application must be running on your PC. This application is different from the NETGEAR Media Server.
- Verify that the version of the Rhapsody server installed supports UPnP and that the UPnP server is running. The Rhapsody application shipped on the *NETGEAR Wireless Digital Media Player MP115 Resource CD* supports UPnP and has the server running by default after installation. The status of the Rhapsody UPnP server can be displayed in the Options menu, User Settings selection under the UPnP tab. The **Start UPnP Server once logged in** box should be selected and the **Status** should indicate **Running**.

Playing Media

If the MP115 cannot play media or music from the NETGEAR Media Server; or music from the Rhapsody server, try the following:

- Check to see if the file is protected. The MP115 cannot play protected files.

- Verify that the file is not corrupt by double-clicking it in the Media Files tab on the Media Server.
- If you are running personal firewall software it may block access to music on your PC. See Firewalls on page 6-5.
- If you are playing from a Rhapsody server, verify that the **My Library** folder is not empty. The MP115 can only play music from the **My Library** folder.

Firewalls

If you are using a firewall, it is best if all of your devices are behind the firewall. If this is not possible, then the next best alternative is to open the ports required for NETGEAR Streaming Media to work. Please note that the latter alternative will reduce some of the protection afforded by the firewall, but is necessary for streaming media devices to work. The ports that must be open include:

UDP Ports: 1360, 1900.

TCP Ports: 1025 – 1035, 3640, 3641, 4000, 4001, 7000 – 7010, 49200 – 49210.

Personal Firewall products can also interfere with the MP115 operation. Detailed instructions for configuring personal firewall products can be found by clicking Help in the NETGEAR Media Server software under the Troubleshooting section.

Glossary

Use the list below to find definitions for technical terms used in this manual.

List of Glossary Terms

10BASE-T
IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.

100BASE-Tx
IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.

802.1x
802.1x defines port-based, network access control used to provide authenticated network access and automated data encryption key management.
The IEEE 802.1x draft standard offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1x uses a protocol called EAP (Extensible Authentication Protocol) 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.

802.11a
IEEE specification for wireless networking at 54 Mbps operating in unlicensed radio bands over 5GHz.

802.11b
IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz.

802.11g
A soon to be ratified IEEE specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz. 802.11g is backwards compatible with 802.11b.

ADSL
Short for asymmetric digital subscriber line, a technology that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).

ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

AES

Advanced Encryption Standard, a symmetric 128-bit block data encryption technique.
It is an iterated block cipher with a variable block length and a variable key length. The block length and the key length can be independently specified to 128, 192 or 256 bits.The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously.

ARP

Address Resolution Protocol, a TCP/IP protocol used to convert an IP address into a physical address (called a DLC address), such as an Ethernet address.
A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address. There is also Reverse ARP (RARP) which can be used by a host to discover its IP address. In this case, the host broadcasts its physical address and a RARP server replies with the host's IP address.

Auto Uplink

Auto Uplink™ technology (also called MDI/MDIX) eliminates the need to worry about crossover vs. straight-through Ethernet cables. Auto Uplink™ will accommodate either type of cable to make the right connection.

Cat 5

Category 5 unshielded twisted pair (UTP) cabling. An Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or Cat 5 or Cat V, by the Electronic Industry Association (EIA).
This rating will be printed on the cable jacket. Cat 5 cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

Denial of Service attack

DoS. A hacker attack designed to prevent your computer or network from operating or communicating.

DHCP

An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.
The DMZ sits between the Internet and an internal network's line of defense, usually some combination of firewalls and bastion hosts. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DNS

Short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses.

Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Domain Name

A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.

DSL

Short for digital subscriber line, but is commonly used in reference to the asymmetric version of this technology (ADSL) that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).

ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

DSLAM

DSL Access Multiplexor. The piece of equipment at the telephone company central office that provides the ADSL signal.

Dynamic Host Configuration Protocol

DHCP. An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.

EAP

Extensible Authentication Protocol is a general protocol for authentication that supports multiple authentication methods.

EAP, an extension to PPP, supports such authentication methods as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards. In wireless communications using EAP, a user requests connection to a WLAN through an AP, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the AP for proof of identity, which the AP gets from the user and then sends back to the server to complete the authentication. EAP is defined by RFC 2284.

ESSID

The Extended Service Set Identification (ESSID) is a thirty-two character (maximum) alphanumeric key identifying the wireless local area network.

Gateway
A local device, usually a router, that connects hosts on a local network to other networks.

IETF
Internet Engineering Task Force. Working groups of the IETF propose standard protocols and procedures for the Internet, which are published as RFCs (Request for Comment) at *www.ietf.org*.
An open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

IP
Internet Protocol is the main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

IP Address
A four-byte number uniquely defining each host on the Internet, usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).
Ranges of addresses are assigned by Internic, an organization formed for this purpose.

ISP
Internet service provider.

Internet Protocol
The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

LAN
A communications network serving users within a limited area, such as one floor of a building.

local area network
LAN. A communications network serving users within a limited area, such as one floor of a building.
A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers.

MAC address
The Media Access Control address is a unique 48-bit hardware address assigned to every network interface card. Usually written in the form 01:23:45:67:89:ab.

Mbps
Megabits per second.

MDI/MDIX
In cable wiring, the concept of transmit and receive are from the perspective of the PC, which is wired as a Media Dependant Interface (MDI). In MDI wiring, a PC transmits on pins 1 and 2. At the hub, switch,

router, or access point, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X). See also AES.

NAT
A technique by which several hosts share a single IP address for access to the Internet.

Network Address Translation
NAT. A technique by which several hosts share a single IP address for access to the Internet.

NIC
Network Interface Card. An adapter in a computer which provides connectivity to a network.

packet
A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

RFC
Request For Comment. Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFCs can be found at *www.ietf.org*.

router
A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

SSID
A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.
This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name. *See also* Wireless Network Name and ESSID.

Subnet Mask
A mask used to determine what subnet an IP address belongs to. Subnetting enables a network administrator to further divide an IP address into two or more subnets.
An IP address has two components, the network address and the host address. For example, consider the IP address 150.215.017.009. Assuming this is part of a Class B network, the first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host on this network.
Subnetting enables the network administrator to further divide the host part of the address into two or more subnets. In this case, a part of the host address is reserved to identify the particular subnet. This is easier to see if we show the IP address in binary format. The full address is: 10010110.11010111.00010001.00001001
The Class B network part is: 10010110.11010111
and the host address is 00010001.00001001

If this network is divided into 14 subnets, however, then the first 4 bits of the host address (0001) are reserved for identifying the subnet.

The subnet mask is the network address plus the bits reserved for identifying the subnetwork. (By convention, the bits for the network address are all set to 1, though it would also work if the bits were set exactly as in the network address.) In this case, therefore, the subnet mask would be 11111111.11111111.11110000.00000000. It's called a mask because it can be used to identify the subnet to which an IP address belongs by performing a bitwise AND operation on the mask and the IP address. The result is the subnetwork address: Subnet Mask 255.255.240.000 11111111.11111111.11110000.00000000
IP Address 150.215.017.009 10010110.11010111.00010001.00001001
Subnet Address 150.215.016.000 10010110.11010111.00010000.00000000

The subnet address, therefore, is 150.215.016.000.

TCP/IP

The main internetworking protocols used in the Internet. The Internet Protocol (IP) used in conjunction with the Transfer Control Protocol (TCP) form TCP/IP.

Universal Plug and Play

UPnP. A networking architecture that provides compatibility among networking technology. UPnP compliant routers provide broadband users at home and small businesses with a seamless way to participate in online games, videoconferencing and other peer-to-peer services.

UTP

Unshielded twisted pair is the cable used by 10BASE-T and 100BASE-Tx Ethernet networks.

WAN

A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.

WEB Proxy Server

A Web proxy server is a specialized HTTP server that allows clients access to the Internet from behind a firewall.
The proxy server listens for requests from clients within the firewall and forwards these requests to remote Internet servers outside the firewall. The proxy server reads responses from the external servers and then sends them to internal client clients.

WEP

Wired Equivalent Privacy is a data encryption protocol for 802.11b wireless networks.
All wireless nodes and access points on the network are configured with a 64-bit or 128-bit Shared Key for data encryption.

wide area network

WAN. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.

Wi-Fi

A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.

Windows Internet Naming Service

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using the Windows Network Neighborhood feature.

WINS

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

Wireless Network Name (SSID)

Wireless Network Name (SSID) is the name assigned to a wireless network. This is the same as the SSID or ESSID configuration parameter.

Appendix A
Technical Specifications

This appendix provides technical specifications for the Wireless Digital Media Player MP115.

Network Protocol and Standards Compatibility	
Data and Routing Protocols:	TCP/IP, DHCP
Power Adapter	
North America:	120V, 60 Hz, input
United Kingdom, Australia:	240V, 50 Hz, input
Europe:	230V, 50 Hz, input
Japan:	100V, 50/60 Hz, input
All regions (output):	12 V DC @ 1A output, 22W maximum
Physical Specifications	
Dimensions:	(H x W x D): 244 x 271 x 221 mm (1.4 x 10.7 x 8.7 in.)
Weight:	1.2 kg (2.6 lbs)
Environmental Specifications	
Operating temperature:	0° to 40° C (32º to 104º F)
Operating humidity:	90% maximum relative humidity, noncondensing
Electromagnetic Emissions	
Meets requirements of:	FCC Part 15 Class B VCCI Class B EN 55 022 (CISPR 22), Class B C-Tick N10947
Interface Specifications	
LAN:	10BASE-T or 100BASE-Tx, RJ-45
WAN:	10BASE-T or 100BASE-Tx, RJ-45

Wireless

Radio Data Rates	1, 2, 5.5, 6, 9, 12, 18, 24, 36, 48, and 54 Mbps Auto Rate Sensing
Frequency	2.4-2.5Ghz
Data Encoding:	802.11b: Direct Sequence Spread Spectrum (DSSS) 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)
Maximum Computers Per Wireless Network:	Limited by the amount of wireless network traffic generated by each node. Typically 30-70 nodes.
Operating Frequency Ranges:	2.412~2.462 GHz (US) 2.457~2.462 GHz (Spain) 2.412~2.484 GHz (Japan)2.457~2.472 GHz (France) 2.412~2.472 GHz (Europe ETSI)
802.11 Security:	40-bit (also called 64-bit) and 128-bit WEP and WPA-PSK[1]

[1] WPA-PSK may not be supported in the orginal product release.

Appendix B
Wireless Networking Basics

Wireless Networking Overview

The MP115 Player conforms 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 2.5GHz. 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, 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 radio frequency channels used are listed in Table B-1:

Table B-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 the wireless products in various countries are different.

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.

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 and WPA are discussed below.

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 MP115:

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.

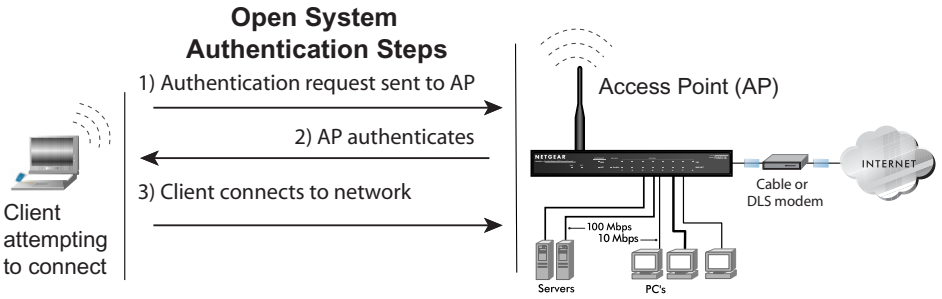


Figure B-1: 802.11 open system authentication

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.

WEP Shared Key Authentication

This process is illustrated below.

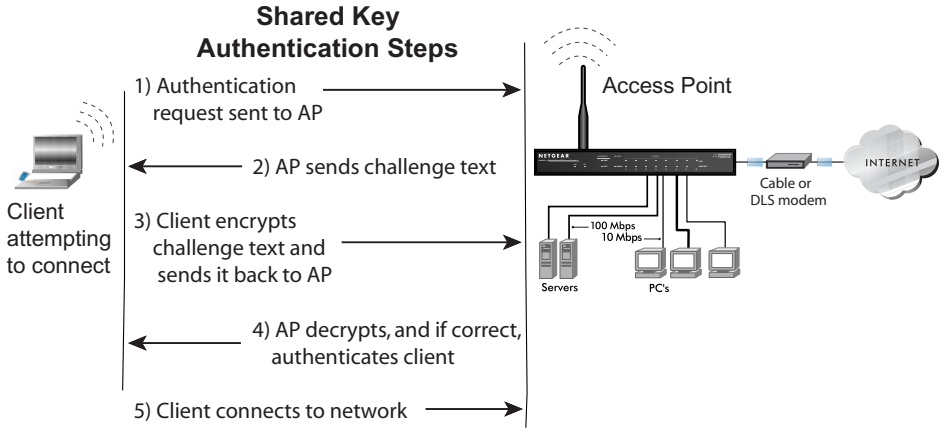


Figure B-2: 802.11 shared key authentication

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.

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 since 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 of 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

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

2. **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.

3. **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, the MP115 does 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 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 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'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 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 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.

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 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 will not be available nor desirable. Possible cipher suites 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. 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 (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 plain text message to ensure messages are not being spoofed.

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

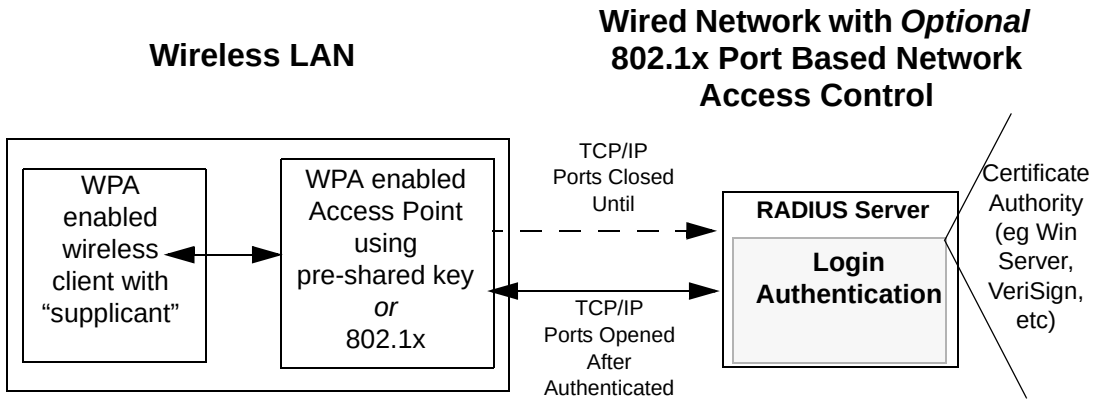


Figure B-3: WPA Overview

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.

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

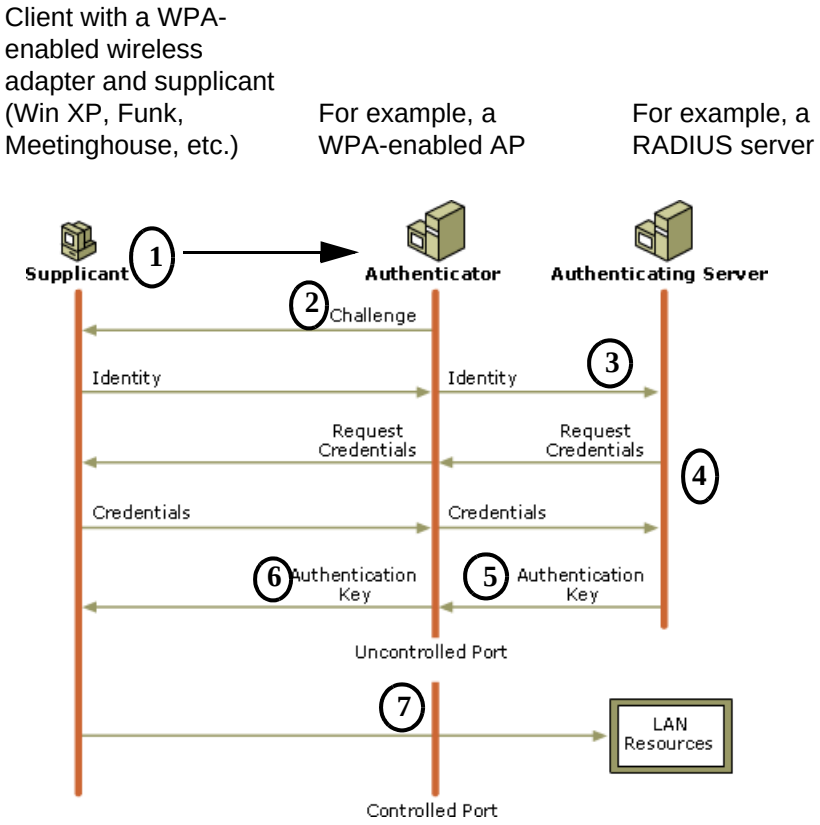


Figure B-4: 802.1x Authentication Sequence

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 (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.

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, NETGEAR, Inc. wireless Wi-Fi certified products will support the WPA standard. 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

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 would offer 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 preshared 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 preshared 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 preshared 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.

Index

O

P

R

S

T

V

W