Over the past few years, the use of wireless LANs has evolved from a curiosity to a necessity. When we travel to many Starbucks or McDonalds, visit an airport or check into a hotel or motel the chances are high that we are able to access the Internet via a wireless LAN connection. Unfortunately, wireless LANs have a finite transmission range which results in service areas resembling the topology of a few patches in a quilt, resulting in transmission dead zones being encountered just when we usually need a communications capability.

One of the most innovative technologies to appear on the horizon since the beginning of the new millennium provides the mechanism to considerably extend the reach of wireless LANs. Referred to as wireless mesh networking, most implementations in currently released products are built upon IEEE 802.11a, b or g wireless LAN protocols. By adding an appropriate routing protocol to 802.11 technology it becomes possible to obtain an automatically configurable, self-healing mesh consisting of a series of platforms using 802.11 technology. This action in effect permits wireless LANs to be extended over a campus, industrial park, suburban neighborhood, or even a city.

Currently there are two primary methods being used to create wireless mesh networks. One method involves adding software to laptops, notebooks, desktops, and even PDAs, enabling those devices to participate as ad hoc members of a mesh network. As long as each device has a wireless LAN adapter. The second method involves the use of routing devices that transmit data using wireless LAN technology and include Ethernet ports in their hardware, enabling any computer with an Ethernet port to become a participant on a mesh network formed by the routers. In this column we will focus our attention on Firetide HotPoint wireless mesh routers which can be considered as supporting the second method used to form a wireless mesh network. That is, HotPoint routers include either two or three Ethernet 10/100 auto sensing ports. By simply plugging your computer or the port of a LAN switch into a HotPoint router you can take advantage of the self-forming, self-healing routing capability of the mesh network formed by the use of the routers.

Overview

Currently Firetide manufactures two versions of their HotPoint router. The HotPoint 1000S is designed for indoor applications and includes three Ethernet 10/100Mbps ports. In comparison, the HotPoint 1000R wireless mesh router has two built-in Ethernet 10/100Mbps ports and represents a rugged device designed for outdoor mounting on utility poles or buildings. The use of the 1000R can extend the range of a mesh by approximately two miles. Both indoor and outdoor routers use the IEEE 802.11b protocol for transmission, with routing at layer 3 based upon a Firetide enhanced version of the Topology Broadcast based on Reverse-Path Forwarding (TBRPF) routing protocol.
Operation

Because it would be difficult for this author to extend power to outdoor locations and coordinate the attachment of computers to routers distributed over a wide geographic area, indoor routers have been used to examine the operation of a HotPoint based wireless mesh network. Three HotPoint routers were used to create a wireless mesh network inside the author’s home. One HotPoint router was connected via one of its Ethernet ports to a combined wireless router and access point that in turn was connected to a cable modem, providing a broadband connection to the Internet. The remaining two HotPoint routers were placed on the second floor of the author’s home. Because the author’s home has a two story stone fireplace, some rooms on the second floor previously could not make a wireless connection with the wireless router/access point located on the first floor. However, once computers were cabled to selectively positioned HotPoint routers it became possible to obtain Internet access from rooms that previously were in effect dead zones with respect to RF signaling.

HotPoint routers are packaged in a cardboard box slightly smaller than the boxes used for pizza delivery. Inside each box is the router, an abbreviated user’s manual and power supply. As we will shortly note, the simplicity of the router makes it a plug and play device with only minor changes to its default configuration needed to better secure the resulting mesh network formed by the use of the equipment.

HotPoint routers are self-configuring, self-healing devices, so there is actually a minimum amount of effort that the end user needs to expend beyond position and providing power to each router and cabling applicable Ethernet devices to one or more ports built into each router. For testing purposes, this author periodically disconnected one HotPoint router from its power source to simulate a mesh network node failure and used a laptop running WildPackets AiroPeek packet capture and decoding program to observe the reconfiguration of the remaining routers in the network. Similar to the wording in Firetide brochures, the HotPoint routers remaining in operation supported the automatic rerouting of data. Because the operation of HotPoint routers is in effect hidden from view, in the remainder of this column we will focus our attention on the use of the HotPoint Manager program which provides a browser-based mechanism for monitoring the activity of other HotPoint routers in your mesh network. In addition, this program provides you with the ability to change certain default settings as a mechanism to enhance the security of the mesh.

HotPoint Manager

HotPoint Manager software is available for Windows, MacOSX, Linux and other Java enabled platforms. The installation of the program is relatively simple, providing you with the ability to create an icon in one of several areas on your computer if you so desire. In a Windows environment HotPoint Manager required approximately 43Mbytes of data storage which included the program as well as a User Guide and two warranty documents, each in PDF format.

The actual use of HotPoint Manager requires an Ethernet crossover cable connection to tie a computer to an Ethernet port on the router. Once this connection is accomplished you would activate the HotPoint Manager program and enter the default password, IP address and subnet mask of the router. Figure 1 illustrates the initial Firetide HotPoint Manager screen display, showing the default settings required to access the router and in effect observe the operation of the mesh network. Because HotPoint routers use a default RFC 1918 address you need to remember to configure the computer accessing the router to be a participant on the default IP network. Although the user manual suggests using the IP address 192.168.224.200 for your computer, you can use any address on that network other than the default address of the router.

Upon access to one HotPoint router you can view all routers in the mesh on a single screen.

Figure 1. The HotPoint Manager initial access screen indicating the default settings required to access the router.
This is illustrated in Figure 2 which shows the default 'Inventory' view of the network. In this example information about the three routers used to form the mesh network are shown. In addition, through the use of this network management program, you can make global changes that affect all routers in the mesh. For example, you can download new firmware from the Firetide website and update all routers via a single connection to one router.

In examining the Inventory View of the mesh network note that by default the HotPoint Name column entries are assigned the serial number of each device. By simply right clicking on an entry you can change the router’s name to something more meaningful, such as ‘KFC Roof’ or ‘Oxford Rd. Pole’. Returning our attention to Figure 2, you can at a glance visually note the status of routers in the mesh by a green upward arrow that indicates each router is operational. In the event that a router disconnects from the mesh the status indicator would change to a red X.

In addition to an inventory view you can also obtain a graphical view of the network. This is accomplished by selecting the Mesh entry from the View menu. The result of that action is a graphical representation of the routers in the mesh as well as a series of tabs that provide you with the ability to view and change certain configuration parameters.

**The Mesh View**

Figure 3 illustrates the HotPoint Manager Mesh View.
screen display. The top window illustrates a graphical representation of the mesh network. In the lower window you will note five tabs, with the Setup tab displayed in the foreground. Through the use of the Setup tab you can change one or more of the three key router access settings. Once you click on the Save button the new settings will be distributed to other routers in the mesh, blocking data traffic until all routers are rebooted. Depending upon the number of routers in the mesh, this action can take a few seconds to several minutes.

**Security Settings**

One of the more interesting aspects of the wireless mesh formed through the use of HotPoint routers is its security capability. HotPoint routers support both WEP and the much more secure Advanced Encryption Standard (AES). Figure 4 illustrates the HotPoint Manager’s default Security tab settings. Note that by default both settings are disabled.

**Other Settings**

The wireless tab permits you the ability to set the SSID used by the routers as well as the 802.11b channel they operate on. Concerning the latter, HotPoint routers by default use Channel 1. You can set a Firetide mesh to any channel from 1 to 10, however, Channel 11 is reserved for your future use.

The Update tab provides you with the ability to update firmware for all routers in the mesh, while the Monitor tab returns you to the Inventory View which provides statistical information and the status of routers in the mesh.

**Observing the Mesh**

Through the use of the WildPacket’s AiroPeek packet capture and decoding program it became possible to observe the flow of HotPoint data. Because space does not permit a detailed description of packet decodes we focus our attention upon the main AiroPeek capture screen as a mechanism to describe how the routers operate hidden from the end user.

Figure 5 shows the AiroPeek program at a point in time when 833 packets were captured, with preliminary details of the first 14 captured packets shown in the top window of the display.

If you examine the Source and Destination columns shown in Figure 5 you will note four IP...
addresses even though only three routers were in operation. The Firetide approach results in the mesh appearing as a layer 2 switch with a single IP address that uses the IEEE 802.11b transmission scheme and operates on a single channel. Concerning the latter, the Channel 1 default was maintained which indicates why all transmissions captured occurred on that channel. The single mesh IP address is 224.0.0.2, while the three routers individually have IP addresses 1.0.100, 1.0.1.131 and 1.0.1.141. Inside the mesh, Firetide HotPoint routers operate as a layer 3 network, routing data using the TBRPF routing protocol. This was easily verified by packet decodes that showed a protocol field value of 17 (UDP) in the IP header and the use of port 712 in the UDP header.

In operation in the author’s home the existing wireless LAN router connected to the cable modem operated on Channel 6 while the HotPoint routers operated on their default Channel 1 setting. Owing to this, any potential interference was negligible. In fact, connecting a laptop to one HotPoint router to access the Internet through two additional HotPoint routers and the previously mentioned switch port on a wireless LAN router showed a near insignificant delay in browsing Web pages that could be the result of many things beside router delay through the mesh. If you’re looking to create a mesh networking environment for your office park, campus or another area you certainly want to consider the use of HotPoint routers.

Firetide
Honolulu Office:
928 Nuuanu Ave., Suite 200
Honolulu, HI 96817, USA
Silicon Valley Office:
16795 Lark Ave.,
Los Gatos, CA 95032, USA
Tel: 877-347-3843
808-528-0007
Web: Firetide.com
E-mail: info@firetide.com

If you wish to order reprints for this or any other articles in the International Journal of Network Management, please see the Special Reprint instructions inside the front cover.