Operating System

Wireless LAN Technologies and Windows XP

By Tom Fout
Microsoft Corporation
Published: July 2001

Abstract

This paper provides an introduction to the Wireless local area network (LAN) technologies being deployed today. It includes an overview of wireless network topologies and general terminology needed to understand the issues. This is followed by a section discussing the various challenges associated with deploying Wireless LAN technologies. Finally a set of solutions to these problems are discussed, featuring how they are implemented/solved by the Windows® XP operating system.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

7/2001

Contents

Tom Fout – Microsoft Corporation

Warren Barkley – Microsoft Corporation

Mark Lee - Microsoft Corporation

An Introduction to Wireless LAN

The availability of wireless networking and wireless LANs can extend the freedom of a network user, solve various problems associated with hard-wired networks and even reduce network deployment costs in some cases. But, along with this freedom, wireless LANs bring a new set of challenges.

There are several wireless LAN solutions available today, with varying levels of standardization and interoperability. Two solutions that currently lead the industry are, HomeRF and Wi-Fi™ (IEEE 802.11b). Of these two, 802.11 technologies enjoy wider industry support and are targeted to solve Enterprise, Home and even public “hot spot” wireless LAN needs. The Wireless Ethernet Compatibility Alliance is working to provide certification of compliance with the 802.11 standards, helping to ensure multi-vendor interoperability.

Wide industry support for interoperability and operating system support address some of the deployment questions for wireless LANs. Still, wireless LANs present us with new challenges around security, roaming and configuration. The rest of this paper discusses these challenges and presents some possible solutions, focusing on how the Windows® XP operating system will play an important role in providing those solutions with support for zero configuration, 802.1x security and other innovations.

Wireless LAN Overview

High-speed wireless LANs can provide the benefits of network connectivity without the restrictions of being tied to a location or tethered by wires. There are many scenarios where this becomes interesting, including the following.

Wireless connections can extend or replace a wired infrastructure in situations where it is costly or prohibitive to lay cables. Temporary installations represent one example of when a wireless network might make sense or even be required. Some types of buildings or building codes may prohibit the use of wiring, making wireless networking an important alternative.

And of course the “no new wires” phenomenon involving wireless, along with phone line networking and even electrical power line networking, has become a major catalyst for home networking and the connected home experience.

The increasingly mobile user becomes a clear candidate for a wireless LAN. Portable access to wireless networks can be achieved using laptop computers and wireless NICs. This enables the user to travel to various locations – meeting rooms, hallways, lobbies, cafeterias, classrooms, etc. – and still have access to their networked data. Without wireless access, the user would have to carry clumsy cabling and find a network tap to plug into.

Beyond the corporate campus, access to the Internet and even corporate sites could be made available through public wireless “hot spots.” networks. Airports, restaurants, rail stations, and common areas throughout cities can be provisioned to provide this service. When the traveling worker reaches his or her destination, perhaps meeting a client at their corporate office, limited access could be provided to the user through the local wireless network. The network can recognize the user from another corporation and create a connection that is isolated from local corporate network but provides Internet access to the visiting user.

In all these scenarios it is worth highlighting that today’s standards-based wireless LANs operate at high speeds – the same speeds that were considered state of the art for wired networks just a few years ago. The access the user has is typically more than 11 megabits per second (Mbps) or about 30 to 100 times faster than standard dial up or Wireless WAN technologies. This bandwidth is certainly adequate to deliver a great user experience for a number of applications or services via the PC or mobile device. In addition, ongoing advancements with these wireless standards continue to increase bandwidth, with speeds of 22 Mbps.

Many infrastructure providers are wiring public areas across the world. Within the next 12 months most airports, conference centers and many hotels will provide 802.11b access for their visitors.

Comparison of Wireless LAN technologies

There are currently two prevalent wireless LAN solutions being deployed. These solutions are the IEEE 802.11standards, primarily 802.11b, and the solution proposed by the HomeRF working group. These two solutions are not interoperable with each other or with other wireless LAN solutions. While HomeRF is designed exclusively for the home environment, 802.11b is designed and is being deployed in homes, small and medium businesses, and large enterprises and in a growing number of public wireless networking hot spots. Several major laptop vendors are shipping or have plans to ship laptops with internal 802.11b NICs. A comparison of these two solutions is given here:

	IEEE 802.11b	**HomeRF**
Major Industry Support	Apple, Cisco, Lucent, 3Com WECA	Compaq, HomeRF Working Group
Status	Shipping	Shipping (Low Speed)
Range	50-300 feet	150 feet
Speed	11 Mbps	1, 2, 10 Mbps
Use	Home, Small Office,	Home

	Campus, Enterprise	
Cost	$75-$150 per card	$85-$129
Security	WEP/802.1x	NWID/encryption
Vendors	Over 75	Under 30
Public Access Points	Over 350	None
Market share of Wireless NICs	72%	21%

Microsoft considers 802.11 to be the most promising and robust solution for use in multiple environments. The rest of this paper focuses on 802.11 technology.

Wireless LAN Topologies

Wireless LANs are built using two basic topologies. These topologies are variously termed; including managed and unmanaged, hosted and peer to peer, and infrastructure and ad-hoc. I will use the terms “infrastructure” and “ad-hoc” in this document. These terms relate to essentially the same basic distinctions in topology.

An infrastructure topology is one that extends an existing wired LAN to wireless devices by providing a base station (called an access point). The access point bridges the wireless and wired LAN and acts as a central controller for the wireless LAN. The access point coordinates transmission and reception from multiple wireless devices within a specific range; the range and number of devices depend on the wireless standard being used and vendor’s product. In infrastructure mode there may be multiple access points to cover a large area or only a single access point for a small area such as a single home or small building.

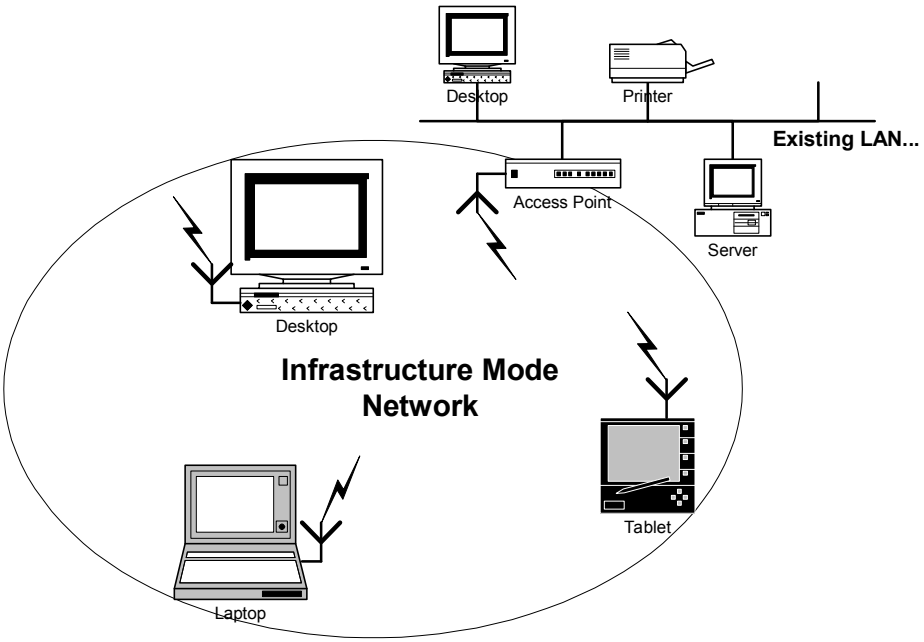

Figure 1: An Infrastructure Mode Network

An ad-hoc topology is one in which a LAN is created solely by the wireless devices themselves, with no central controller or access point. Each device communicates directly with other devices in the network rather than through a central controller. This is useful in places where small groups of computers might congregate and not need access to another network. For example, a home without a wired network, or a conference room where teams meet regularly to exchange ideas, are examples of where ad-hoc wireless networks might be useful.

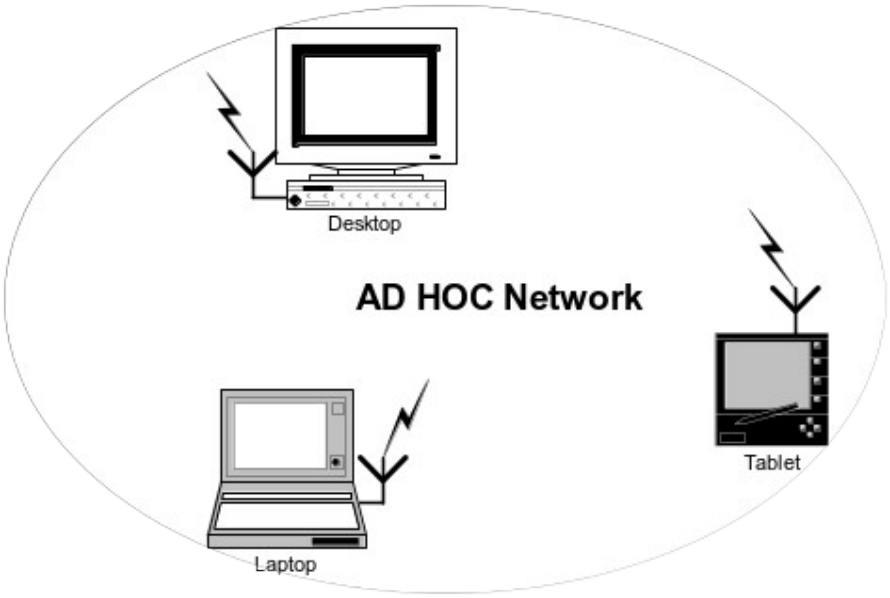

Figure 2: An Ad Hoc Network

For example, when combined with today's new generation of smart peer-to-peer software and and solutions, these ad hoc wireless networks can enable traveling users to collaborate, play multiplayer games, transfer files or otherwise communicate with one another using their PCs or smart devices wirelessly.

How it Works Overview – Infrastructure Mode

The laptop or smart device, which is characterized as a "station" in wireless LAN parlance, first has to identify the available access points and networks. This is done through monitoring for 'beacon' frames from access points announcing themselves, or actively probing for a particular network by using probe frames.

The station chooses a network from those available and goes through an authentication process with the access point. Once the access point and station have verified each other, the association process is started.

Association allows the access point and station to exchange information and capabilities. The access point can use this information and share it with other access points in the network to disseminate knowledge of the station's current location on the network. Only after association is complete can the station transmit or receive frames on the network.

In infrastructure mode, all network traffic from wireless stations on the network goes through an access point to reach the destination on either the wired or wireless LAN.

Current Wireless LAN Challenges

Access to the network is managed using a carrier sense and collision avoidance protocol. The stations will listen for data transmissions for a specified period of time before attempting to transmit – this is the carrier sense portion of the protocol. The station must wait a specific period of time after the network becomes clear before transmitting. This delay, plus the receiving station transmitting an acknowledgement indicating a successful reception form the collision avoidance portion of the protocol. Note that in infrastructure mode, either the sender or receiver is always the access point.

Because some stations may not be able to hear each other, yet both still be in range of the access point, special considerations are made to avoid collisions. This includes a kind of reservation exchange that can take place before a packet is transmitted using a request to send and clear to send frame exchange, and a network allocation vector maintained at each station on the network. Even if a station cannot hear the transmission from the other station, it will hear the clear to send transmission from the access point and can avoid transmitting during that interval.

The process of roaming from one access point to another is not completely defined by the standard. But, the beaconing and probing used to locate access points and a re-association process that allows the station to associate with a different access point, in combination with other vendor specific protocols between access points provides for a smooth transition.

Synchronization between stations on the network is handled by the periodic beacon frames sent by the access point. These frames contain the access point's clock value at the time of transmission so can be used to check for drift at the receiving station. Synchronization is required for various reasons having to do with the wireless protocols and modulation schemes.

How it Works Overview – Ad-hoc Mode

Having explained the basic operation for infrastructure mode, ad-hoc mode can be explained by simply saying there is no access point. Only wireless devices are present in this network. Many of the responsibilities previously handled by the access point, such as beaconing and synchronization, are handled by a station. Some enhancements are not available to the ad-hoc network, such as relaying frames between two stations that cannot hear each other.

There are always new challenges that arise when a new networking medium is introduced into a new environment. With wireless LANs this holds true. Some challenges arise from the differences between wired LANs and wireless LANs. For example, there is a measure of security inherent in a cabled network where the data is contained by the cable plant. Wireless networks present new challenges, since data is traveling thru the air on radio waves.

Other challenges arise out of the unique capabilities of wireless networking. With the freedom of movement gained by removing the tether (wire), users are free to roam from room to room, building to building, city to city and so on, expecting uninterrupted connectivity all the while.

Some challenges have always existed in networking, but are compounded when complexity is added such as with wireless networks. For example, as network configuration continues to become easier, wireless networks add features (sometimes to solve other challenges) and metrics that add to the configuration parameters.

Security Challenges

With a wired network there is an inherent security in that a potential data thief has to gain access to the network through a wired connection, usually meaning physical access to the network cable plant. On top of this physical access, other security mechanisms can be layered.

When the network is no longer contained by wires, the freedom gained by the users of the network can also be extended to the potential data thief. The network now may become available in the hallways, insecure waiting areas, even outside of the building. In a home environment, your network could extend to your neighbors houses if the proper security mechanisms aren't adopted by the networking gear or used properly.

Since its inception, 802.11 has provided some basic security mechanisms to make this enhanced freedom less of a potential threat. For example, 802.11 access points (or sets of access points) can be configured with a service set identifier (SSID). This SSID must also be known by the NIC in order to associate with the AP and thus proceed with data transmission and reception on the network. This is very weak security if at all because:

- The SSID is well known by all NICs and APs
- The SSID is sent through the air in the clear (even beaconed by the AP)
- Whether the association is allowed if the SSID is not known can be controlled by the NIC/Driver locally
- No encryption is provided through this scheme

While there may be other problems with this scheme, already this is enough to stop none but the most casual of hacker.

Additional security is provided through the 802.11 specifications through the Wired Equivalent Privacy (WEP) algorithm. WEP provides 802.11 with authentication and encryption services. The WEP algorithm defines the use of a 40-bit secret key for authentication and encryption and many IEEE 802.11

implementations also allow 104-bit secret keys. This algorithm provides mostly protection against eavesdropping and physical security attributes comparable to a wired network.

A principal limitation to this security mechanism is that the standard does not define a key management protocol for distribution of the keys. This presumes that the secret, shared keys are delivered to the IEEE 802.11 wireless station via a secure channel independent of IEEE 802.11. This becomes even more challenging when a large number of stations are involved such as on a corporate campus.

To provide a better mechanism for access control and security the inclusion of a key management protocol in the specification is required. The 802.1x standard, which is described later in this paper, was developed specifically to address this issue.

Roaming User Challenges

As a user or station roams from access point to access point, an association must be maintained between the NIC and an access point for network connectivity to be maintained. This can present an especially difficult problem if the network is large and the user must cross subnet boundaries or realms of administrative control.

If the user crosses a subnet boundary, the IP address originally assigned to the station may no longer be appropriate for the new subnet. If the transition involves a crossing of administrative domains, it is possible that the station may no longer be allowed to access the network in the new domain based on their credentials.

Beyond simply roaming within a corporate campus, several other roaming user scenarios are very real. With airports and restaurants adding wireless connectivity to the Internet and wireless networks becoming popular networking solutions for the home.

Now it becomes more likely the user could leave the office to meet with someone from another company that also has a compatible wireless network. On the way to this meeting the user could find himself in a train station, restaurant or airport with wireless access and need to retrieve files from the home office. It would be useful for this user to be authenticated and use this connection to access their corporate network. When the user arrives at their his destination they he may not be allowed access to the local corporate network he is visiting. It would be fortuitous however, if the user could be provided access to the Internet in this foreign environment. This access could then be used to create a virtual private network connection to his corporate network. The user might then leave for home and wish to connect to his home network to upload or print files to work on that evening. The user has now roamed into a new wireless network, possibly even running in ad hoc mode.

Solutions to Wireless LAN Challenges

For the example above, roaming is a situation that must be carefully thought through. Configuration becomes an issue for the roaming user as multiple different network configurations could cause a challenge if the user's wireless station is not somewhat self-configuring.

Configuration Challenges

Now that we have a wireless network connection and the added complexity, there are potentially many more things to configure. For example we might need to configure the SSID of the network we are connecting to. Or, we might need to configure a set of WEP keys for security; possibly multiple sets if we have multiple networks to connect to. We might need to have a configuration for work where we have a network operating in infrastructure mode and a configuration for home where we are operating in ad hoc mode. Then we might need to choose which of these configurations to use based on where we are at this time.

Security – 802.1X

To provide security beyond that provided by WEP, the Windows XP networking team worked with the IEEE, Networking vendors and others to define IEEE 802.1X. 802.1X is a draft standard for port-based, network access control used to provide authenticated network access for Ethernet networks. This port-based network access control uses the physical characteristics of the switched LAN infrastructure to authenticate devices attached to a LAN port. Access to the port can be prevented if the authentication process fails. While this standard is designed for wired Ethernet networks, it is applicable to 802.11 Wireless LANs.

Specifically for the wireless case, the access point will act as an authenticator for access to the network, using a Remote Authentication Dial-In User Service (RADIUS) server for authenticating client credentials. Communication is allowed through a logical "uncontrolled port" or channel on the access point for the purpose of validating credentials and obtaining keys to access the network through a logical "controlled port." The keys that are available to the access point and client as a result of this exchange allow the client's data to be

encrypted and be identified by the access point. We have thus added key management protocol to the security of 802.11.

The following steps outline the generic approach that would be used to authenticate a user's machine for wireless access to the network.

- Without a valid authentication key, an access point prohibits all traffic flow through it. When a wireless station comes into range of the access point, the access point issues the station a challenge.
- When the station receives the challenge, it responds with its identity. The access point forwards the station's identity to a RADIUS server for authentication services.
- The RADIUS server then requests the credentials for the station, specifying the type of credentials required to confirm the station's identity. The station sends its credentials to the RADIUS server (through the access point's "uncontrolled port").
- The RADIUS server validates the station's credentials (assuming validity), and transmits an authentication key to the access point. The authentication key is encrypted so that only the access point can interpret it.
- The access point uses the authentication key to securely transmit appropriate keys to the station, including a unicast session key for that station and a global session key for multicasts.
- The station can be asked to re-authenticate periodically to maintain a level of security.

Using RADIUS Further Eases the Burden

This 802.1x approach capitalizes on the widespread and growing use of RADIUS for authentication. A RADIUS server can query a local authentication database if that is appropriate for the scenario. Or, the request could be passed to another server for validation. When RADIUS decides that the machine can be authorized on this network to sends the message back to the access point and the access point then allows the data traffic to flow into the network. A real world example might look like this:

- A user starts his laptop, containing his 802.11 card, in an airport.
- The machine finds there are wireless networks available, chooses a preferred network and associates with it.
- The machine sends the users credentials to the access point to verify that he is allowed on this network.
- The user is ErikB@bigco.com. BigCo has bought wireless access for all their users in airports across the world.
- The RADIUS server, which receives the request from the access point, looks at the packet and sees that it is from a BigCo user.

- The RADIUS server then asks a BigCo server to establish whether this person a real user and if they allowed access.
- If the BigCo server says “yes” the access point is then told to allow the traffic to flow.

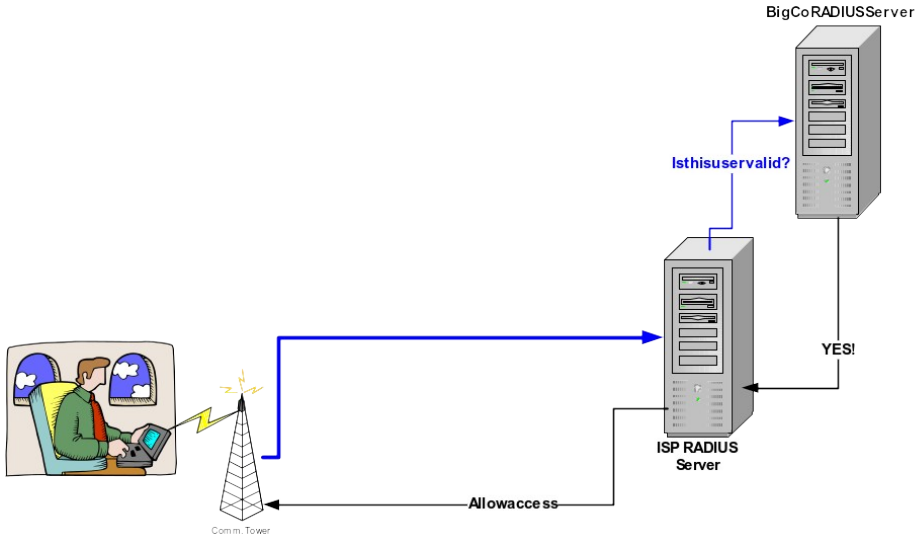

Figure 3: An Example Public Access Scenario

To provide this level of security, Microsoft is providing an 802.1X client implementation in Windows XP and enhancing the Windows RADIUS server, Internet Authentication Server (IAS) to support wireless device authentication. Microsoft has also worked with many 802.11 device vendors to support these mechanisms in their NIC drivers and access point software. Currently many top vendors are either close to shipping or are shipping 802.1x support in their devices.

Roaming – Seamless Roaming

Windows 2000 included enhancements for detecting the availability of a network and acting appropriately. These enhancements have been extended and supplemented in Windows XP to support the transitional nature of a wireless network.

In Windows 2000, media sense capability (detecting an attached network) was used to control the configuration of the network stack and inform the user when the network was unavailable. With Windows XP this feature is used to enhance the wireless roaming experience by detecting a move to a new access point, forcing re-authentication to ensure appropriate network access and detecting changes in IP subnet so an appropriate address can be used to get optimum resource access.

Multiple IP address configurations (DHCP assigned or Static address) can be available on a Windows XP system and the appropriate configuration automatically chosen. When an IP address change occurs, Windows XP allows for additional reconfiguration to occur if appropriate. For example, quality of

service (QoS) reservations can be updated and IE proxy settings re-detected. Through Windows Sockets extensions, applications that want to be network aware (firewalls, browsers, etc.) can be notified of changes in network connectivity and update their behavior based on the changes. The auto-sensing and reconfiguration effectively negates the need for mobile IP to act as a mediator and solves most user issues when roaming between networks.

When roaming from access point to access point there is state and other information about the station that must be moved along with the station. This includes station location information for message delivery and other attributes of the association. Rather than re-create this information upon each transition, one access point can pass this information to the new access point. The protocols to transfer this information are not defined in the standard, but several wireless LAN vendors have jointly developed an Inter-Access Point Protocol (IAPP) for this purpose, further enhancing multi-vendor interoperability.

Configuration – Zero Configuration for Wireless

Microsoft also partnered with 802.11 NIC vendors to improve the roaming experience by automating the process of configuring the NIC to associate with an available network.

The wireless NIC and its NDIS driver need to do very little beyond supporting a few new NDIS Object Identifiers (OIDs) used for the querying and setting of device and driver behavior. The NIC will scan for available networks and pass those to Windows XP. Windows XP has a Wireless Zero Configuration service that then takes care of configuring the NIC with an available network. In the case where there are two networks covering the same area. The user can configure a preferred network order and the machine will try each network in order until it finds an active one. It is even possible to limit association to only the configured, preferred networks.

If no 802.11 networks are found nearby, Windows XP will configure the NIC to use ad hoc networking mode. It is possible for the user to configure the wireless NIC to either disable or be forced into ad hoc mode.

These zero configuration enhancements are integrated with the security enhancements such that if authentication fails, another network will be located to attempt association with.

Wireless LAN is an exciting technology that is just being realized as a solution for enterprise, public and residential deployments. To support these

For More Information

deployments, several key challenges must be met. Microsoft and 802.11 vendors are partnering to meet these challenges head-on with Windows XP.

For the latest information on Windows XP, check out our Web site at http://www.microsoft.com/windowsxp.

For the most current information about the IEEE standards and in particular the 802.11 standards, please see:

http://standards.ieee.org/wireless/