IBM High Rate Wireless LAN Technical Report 102 / A June, 2000

IBM High Rate Wireless LAN/IEEE 802.11b Security Layers[1]

One of the primary concerns of users of Wireless LANs is the assumed reduction in privacy and security. This report addresses that concern and describes the various levels of protection that are available with the IBM High Rate Wireless LAN product family.

In addition to all of the standard LAN access control mechanisms offered by Network Operating Systems, the IBM Wireless LAN uses multiple levels of security to prevent unauthorized access to network resources. These security provisions are available in the standard product offering.

Five Security Layers

The IBM Wireless LAN product family offers five layers of added protection. The combination of these layers provides network security that is at least as good as that available on wired LAN networks. The following elements enhance the basic system security:

1. Spread Spectrum technology
2. The IBMWirelessLAN network name used in combination with the "Closed Wireless System" option
3. Station Authentication
4. Wired Equivalent Privacy (WEP), which includes hardware encryption using a 40-bit or 104-bit user-defined key (WEP)
5. Access point availability control

Spread Spectrum

The IBM Wireless LAN uses low-power Spread Spectrum technology to transmit data. By doing so, each data bit is converted from digital to analog and its digital bit frequency is multiplied from one to eleven times over the allocated frequency band. The signal remains at the center frequency of the channel as long as the original bit stream is composed of a stream of alternating ones and zeroes. When it deviates from this balanced stream, the frequency of the transmitted signal spreads away from the center frequency.

This spreading is done using a unique code, which is built into the transmission unit. Physical access to the LAN does not yield intelligible results unless the IBM Wireless LAN product (or another wireless system that implements the same technology and conversion coding) is used to decode the signal in a reverse sequence to the transmission encoding.

Due to the low power and the spread of the signal, it is very difficult to differentiate IBM Wireless LAN signals from naturally occurring noise. Simply using spectrum analysis for sensing the original signal yields very poor results.

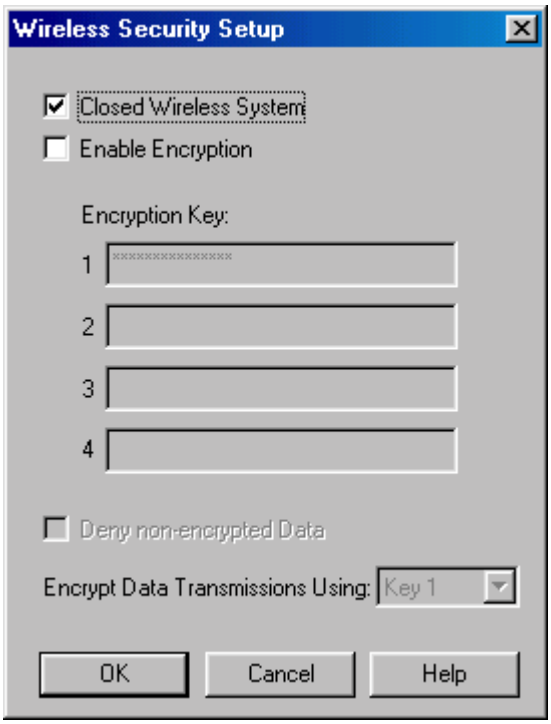
"Closed Wireless System" option

The IBM Wireless LAN complies with the IEEE 802.11b standard. That means that IBM Wireless LAN stations can interact with IEEE 802.11b-compliant access points without having to know the value of the SSID (i.e., the network name) that is used to identify the infrastructure network. Thus, IBM Wireless LAN systems

allow other manufacturers' IEEE 802.11b-compliant systems that implement Direct Sequence Spread Spectrum technology to interact with the IBM access point without knowledge of the SSID. In both these cases, a value of "ANY" for the SSID is sufficient to access the access point and its associated network. This complies with the open nature of the IEEE 802.11b standard.

However, IBM Wireless LAN systems include the so-called "Closed Wireless System" option, which will prevent wireless stations from associating with an IBM access point if the SSID (i.e., Network Name) is not provided. If the option is activated, an SSID-value of "ANY" will not allow a successful association with the Access Point.

The option is activated by clicking a check box on one of the screens of the IBM Wireless LAN AP Manager, which is used to configure IBM Wireless LAN systems. The screen capture below illustrates this.



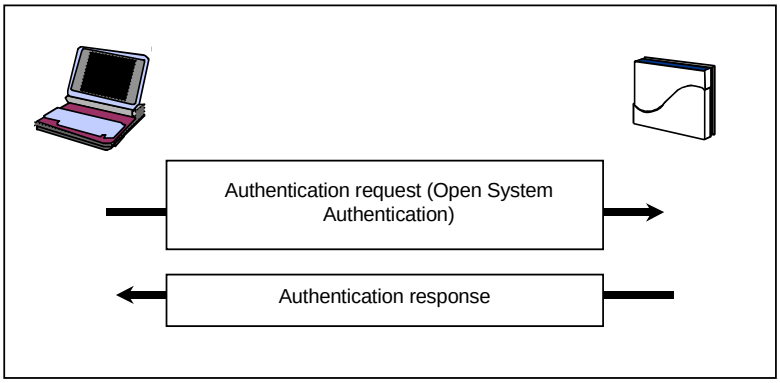
Authentication

IEEE 802.11 describes two mechanisms for authentication:

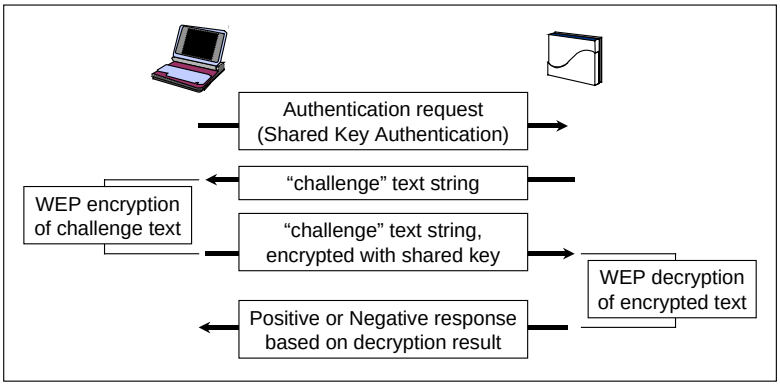
- Open System Authentication
- Shared Key Authentication

If Shared Key Authentication is used, it is considered to be part of the total security plan for the network.

Open System Authentication, is merely a mechanism to identify the station to the Access Point. Its use always results in a positive response, so it is not considered secure. The following diagram illustrates the sequence:



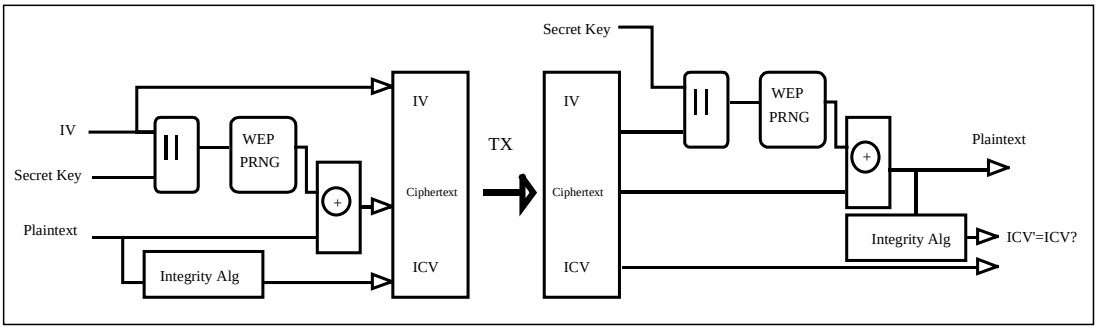
Shared Key Authentication allows access points to verify the user as being authorized to interact with the Access Point. Its use requires WEP (Wired Equivalent Privacy) to be present and active in both the client station and the access point. The actual authentication procedure consists of an exchange of four messages between the client station and the access point. This allows the access point to verify that the station has the proper key (the same key the access point is using). The following diagram illustrates the procedure.



Hardware Encryption using 40-bit or 104-bit Encryption Keys (WEP)

IBM Wireless LAN components can use hardware encryption to increase the privacy of transmitted data. This level of security is known as "Wired Equivalent Privacy" (WEP). With this option enabled, traffic between IBM Wireless LAN client stations will be encrypted to prevent privacy intrusions. All IBM Wireless LAN components can use encryption, but some components by other manufacturers cannot. This must be taken into consideration when a system is configured. Encryption is enabled by setting one or more user-specified encryption keys. The IBM Wireless LAN system allows a user to configure up to four keys, one of which is the active key. The technical report "WEP Encryption" describes how these four keys can be used to apply key rollover schemes. That document also includes background information on configuring WEP. Screenshots show how to configure both the access point and the client station.

The use of WEP is defined in the IEEE 802.11 standard, and it can be used with encryption keys of 64 bits or 128 bits. For either key length, 24 of the bits are called the "Initialization Vector" (IV), and are transmitted in clear text along with the encrypted data. The remaining bits (40 or 104) are termed "the secret key," which is provided by the user during configuration. The encryption algorithm uses this key. The following diagram illustrates the encryption mechanism.



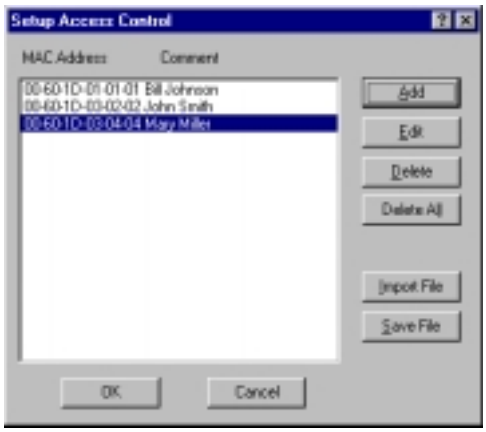
The IV and the secret key are used by the WEP "Pseudo-Random Number Generator" (PRNG) to produce a bit string that is eXclusive-ORed with the data that is to be transmitted. The IV is incremented for each successive transmission and is transmitted in clear text along with the data. At the receiver, the IV is fed to the WEP PRNG (together with the key), where the decipher string is produced. The decipher string is used in another eXclusive-OR operation to reproduce the original data. If this scheme is used, it is not possible for an intruder to obtain the secret key even if the intruder captures an encrypted message with known content (such as standard messages that are generated by some protocol stacks during system startup). The only thing the intruder could obtain in such a case would be the cipher string, but the secret key would remain secure and would continue to protect messages with unknown content.

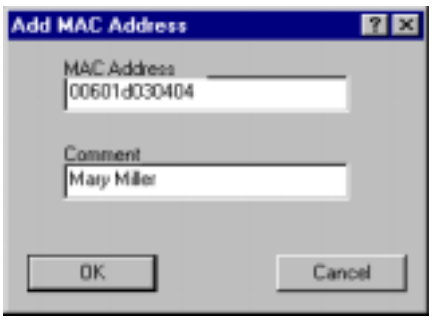
WEP encryption is based on the RC4 algorithm, which is licensed from a company called RSA. This algorithm is used in the Pseudo-Random Number Generator to produce the cipher string.

Access Point Backbone LAN Availability Control

IBM Wireless LAN systems can restrict infrastructure network access to those stations with (hardware) MAC addresses that are included in a pre-loaded filter table. The filtering process is a function of the bridging functionality that the access point implements. To deploy this capability, a user will create a table of MAC addresses for wireless stations that are allowed to have access to the backbone. Stations with MAC addresses that do not appear in this table are not granted access, and the traffic generated by these stations will be filtered out. This mechanism is known as "Access Control" and the specific table mentioned is called the Access Control table.

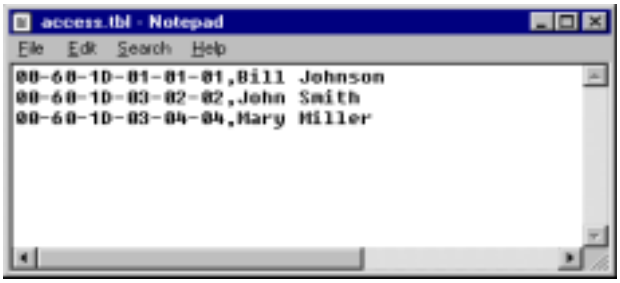
The function is enabled using the IBM Wireless LAN AP Manager software, using screens similar to the ones shown here.





A system administrator will need to create a file of MAC addresses, using the IBM Wireless LAN AP Manager tool, and save the file for subsequent uploading (importing) on all Access Points that are part of the infrastructure.

A file could also be created using a simple editor such as Notepad, as illustrated below. This file can be imported into Access Points that require access control. The MAC addresses must be specified as shown below (i.e., with the format, xx-xx-xx-xx-xx-xx, and separated by a comma from the comment field). The comment field can be up to twenty characters long.



The maximum number of MAC addresses that can be included in the Access Control Table is 497. If more addresses are desired, a RADIUS server and backup can be implemented.

Access Control can protect against unauthorized access only when traffic passes through the "bridging function". This means that if wireless stations A and B both are associated to the same Access Point, Access Control is not effective to protect station B from unauthorized access by station A. The traffic flow from A to B is handled by the firmware in the Access Point electronics and therefore cannot be filtered by the bridge.

Conclusion

The facilities discussed here are included in the IBM High Rate Wireless LAN product family to enhance security. Other user-defined mechanisms, such as passwords on network servers, can be added for even more security. When the included security provisions are enabled, IBM Wireless LAN Systems will have an equal or higher level of privacy than can be expected from wired stations.

[1]Original content from Lucent Orinoco™

