IBM High Rate Wireless LAN: WEP Encryption[1]

June, 2000

This report provides information on various system considerations when using the Wired Equivalent Privacy (WEP) functions of the IBM Wireless LAN System. The WEP configuration parameters are introduced, suggestions are made on how to set up encryption on an IBM Wireless LAN System, and notes are provided to assist you in dealing with frequent encryption key changes. It also describes some special aspects of distributing encryption keys throughout the system.

General Principles and Guidelines

The WEP funct ion uses the IEEE-defined encryption method for data transmissions. This establishes privacy on the LAN network's wireless paths, which is equivalent to that on the networks wired Ethernet paths. When you plan for the configuration and use of WEP on your IBM Wireless System, the following general guidelines apply:

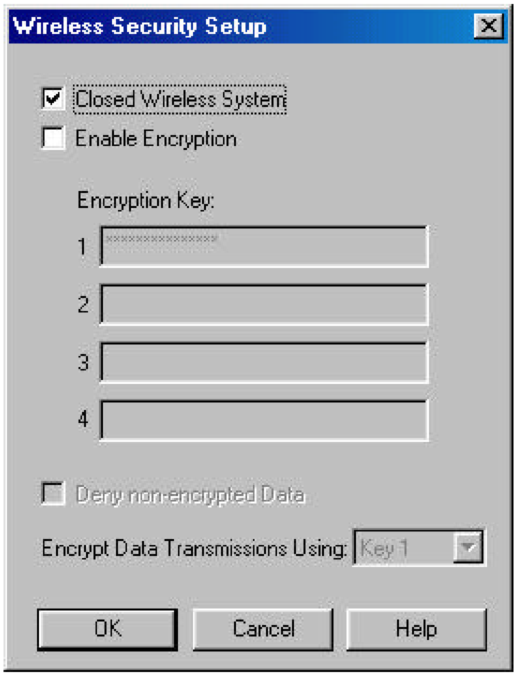
- It is recommended that you set up the system to only allow encrypted data transmissions. This system requires that all client stations and all access points have adapters that support encryption, and that all adapters be set up with the same set of keys.
- It is possible to allow users who cannot support encryption to use the network. To support users with and without encryption capability, all access points must have encryption enabled.
- As is common in network security practices, the distribution of the initial encryption keys requires special considerations; subsequent changes to the encryption keys can be performed under the protection of the operational key.
- Changing encryption keys will require manual reconfiguration of the IBM access points and of the IBM Wireless LAN drivers in the Client Stations; in most cases, the reconfiguration of the client station must be done at the station itself.

Configuration of WEP

When WEP is deployed, all IBMWireless LAN elements in the network must be configured to run with WEP enabled.

Configuring WEP in IBM Access Points

The configuration of the access point will determine the restrictions of the network; here the user must decide whether or not to support non-encrypted transmissions and which keys are valid to use. The configuration screen of IBM AP Manager tool for security setup is shown below.



Wireless Security Setup

☑ Closed Wireless System

□ Enable Encryption

Encryption Key:

1 ***************

2

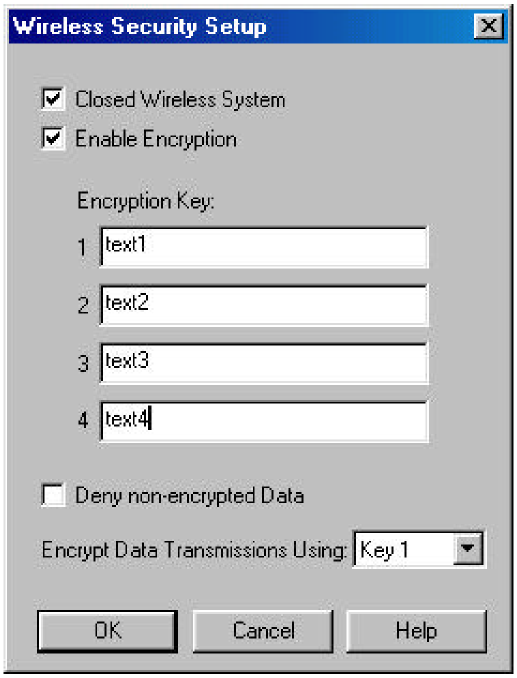
3

4

□ Deny non-encrypted Data

Encrypt Data Transmissions Using: Key 1

The check box "Close Wireless System" is not related to WEP encryption. The check box "Enable Encryption" defines whether encryption is to be used or not. When this box is checked, the additional WEP-related configuration items will be made available, as shown below.



Wireless Security Setup

☑ Closed Wireless System

☑ Enable Encryption

Encryption Key:

1 text1

2 text2

3 text3

4 text4

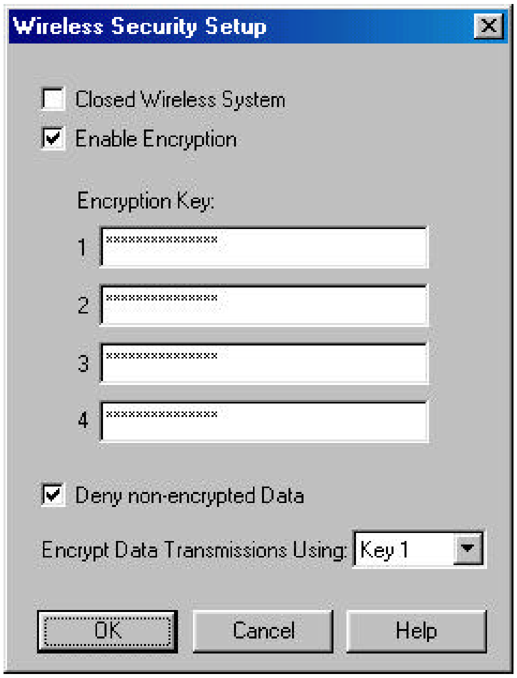
□ Deny non-encrypted Data

Encrypt Data Transmissions Using: Key 1

Up to four encryption keys may be entered when the Enable Encryption selection is made. These keys will be used to encrypt and decrypt data transmissions. The key values are entered in either textual (ASCII) format or hexadecimal format (an entry starting with "0x" will be interpreted as hexadecimal). A text string is translated into the ASCII values associated with the characters.

The user must assign one of the entered keys as the encryption key for all access point transmissions. This assignment is made by selecting the appropriate number from the pull-down-list beside "Encrypt Data Transmissions Using." The final configuration choice is "Deny non-encrypted Data." When this box is checked, the access point will not accept messages from stations that are transmitting data in the clear (without encryption).

After a key value is entered and the OK button is selected, reading it back at a later time will result in all asterisk characters. Changing one or more keys will require full re-entry of the new value at the appropriate "Encryption Key" entry-line. This is illustrated in the next figure.



☐ Closed Wireless System

☑ Enable Encryption

Encryption Key:

1 ***************

2 ***************

3 ***************

4 ***************

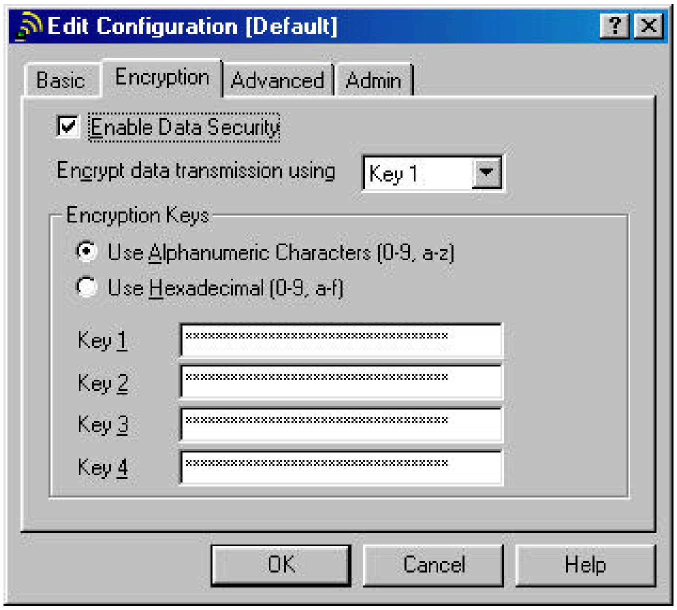
☑ Deny non-encrypted Data

Encrypt Data Transmissions Using: Key 1

This figure shows how the read-back screen will appear after four keys have been entered and Key 1 has been selected as the transmission encryption key.

Configuring WEP in IBM Wireless LAN Client Station Drivers

The figure below shows the properties menu for the Windows-based NDIS Miniport driver. The "Encryption" tab is used to enter the WEP -related parameters.



☑ Enable Data Security

Encrypt data transmission using Key 1

Encryption Keys

● Use Alphanumeric Characters (0-9, a-z)

○ Use Hexadecimal (0-9, a-f)

Key 1 **************************************

Key 2 **************************************

Key 3 **************************************

Key 4 **************************************

Client Station and Access Point configuration use similar parameters, with the exception of the "Deny Non-encrypted Data" check box. Client Stations can always receive non-encrypted data. In a mixed system, reception of non-encrypted multicast messages will be required.

Regular Windows methods are used to configure the Wireless LAN drivers. The configuration is performed at the Client Station and causes a change to that machine's Registry. The WEP keys are not stored in clear-text in the Windows registry. The driver includes the information necessary for interpreting the stored values and for translating them into the required key values.

Encryption Key Considerations

Both access point and client station drivers allow the system to support up to four different encryption keys simultaneously. This conforms to the 802.11 standard, which defines four so-called "default keys." These keys can smooth the transition from the use of one key to the use of a new key. For two PC Card adapters to interact using encrypted data, they must share a common key value having the same key-index number at the moment of transmission. The key-index number of the key used for encryption is transmitted in clear-text in the header of the message, and the receiving station will use it to determine which of the four available keys must be used for decryption.

So, it is not necessary for both sides (typically, an access point and a client station) to have the same set of 4 keys. As long as there is one key in common, they can communicate if they both use that common key. **NOTE:** The 802.11 standard allows a unique key per station, which is related to the station's MAC Address. The IBM Wireless LAN system currently does not support that feature.

Key Rollover

When multiple keys will be used over a period of time, the following must be considered:

- The length of time each key remains in use.

There is a direct correlation between security level (the chance someone will find out what the key value is) and operational overhead (the effort required to reconfigure access points and client stations).

- Requirements for smooth transition from one key to another

- Minimization of end user exposure to key values

The key rollover possibilities built into the 802.11 standard and offered by the IBM Wireless LAN system allow for a number of scenarios, each with different answers to the above considerations.

The sequence of key configuration settings at the access point (shown as AP) and at the client station (shown as STA) over time is shown in the tables below. Each table reflects a certain key rollover strategy. The column "Outward Key" shows which key is used to encrypt traffic from the AP to the STA, and the column "Inward Key(s)" indicates the key(s) that are allowed and can be used to encrypt traffic from the STA to the AP. The configured WEP Keys are shown in order of the index numbers 1-2-3-4; the column "Tx" is the index number configured for transmission. Key values in capital letters are real keys. A key value of zero indicates a non-configured index.

The column "Keys 1-2-3-4" shows an equal sign (=) when the value does not change from the previous period. This is particularly important when the STA keys are involved, since the user usually has no knowledge of the key values. Therefore, the user will have to return their Client Station equipment to an IP department to get the key values changed. However, the user can change the Txkey Index, since that does not reveal secret information.

Single Key – No Transition

Table 1 shows a system where only a single key is used at any point in time. The active key is dictated by AP settings, which show only one valid key during each period. This requires a change to the keys at all STAs simultaneously with changes to the AP configuration.

Period		AP Configuration		Out-ward Key	STA Configuration(s)		In-ward Key
#	Description	Keys 1-2-3-4	Tx		Keys 1-2-3-4	Tx	
0	Main life key A	A-0-0-0	1	A	A-B-C-D	1	A
1	Main life key B	0-B-0-0	2	B	=	2	B
2	Main life key C	0-0-C-0	3	C	=	3	C
3	Main life key D	0-0-0-D	4	D	=	4	D
4	Main life key E	E-0-0-0	1	E	E-F-G-H	1	E
5	Main life key F	0-F-0-0	2	F	=	2	F
..							

Table 1

By initially configuring all STAs with the keys for the first 4 periods, only the Txkey index needs to be changed at all STAs for the first three steps. At the step from period 3 to period 4, the keys have to be changed at all STAs as well.

Single Key – Transition Period

When a transition period is introduced between the main lives of the successive keys, the scheme is changed as shown in Table 2.

Period		AP Configuration		Out-ward	STA Configuration(s)		In-ward
#	Description	Keys 1-2-3-4	Tx	Key	Keys 1-2-3-4	Tx	Key
0	Main life key A	A-0-0-0	1	A	A-B-C-D	1	A
1	Transition A-B	A-B-0-0	2	B	=	1|2	A | B
2	Main life key B	0-B-0-0	2	B	=	2	B
3	Transition B-C	0-B-C-0	3	C	=	2|3	B | C
4	Main life key C	0-0-C-0	3	C	=	3	C
5	Transition C-D	0-0-C-D	4	D	=	3|4	C | D
6	Main life key D	0-0-0-D	4	D	=	4	D
7	Transition D-E	E-0-0-D	1	E	A-B-C-D E-F-G-H	4 1	D E
8	Main life key E	E-0-0-0	1	E	E-F-G-H	1	E
9	Transition E-F	E-F-0-0	2	F	=	1|2	E | F
..							

Table 2

In the transition periods 1, 3 and 5, the Client Station users can switch from one Txkey index to the next. At the end of this period, all stations must have changed to the new key index. Transition period 7 includes the transition to a new set of keys, as well. The total time a key is used consists of the main life time period and two transition periods. Assuming that the main life is much longer than the transition, this can be considered to be a single key scheme, because most of the time only a single key is in use.

Alternative Schemes

Some schemes include main life periods with two or more active keys. An example is shown in Table 3.

Period		AP Configuration		Out-ward	STA Configuration(s)		In-ward
#	Description	Keys 1-2-3-4	Tx	Key	Keys 1-2-3-4	Tx	Key
0	Main life key A	A-0-0-0	1	A	A-B-C-D	1	A
1	Main life A+B	A-B-0-0	2	B	=	1|2	A | B
2	Main life B+C	0-B-C-0	3	C	=	2|3	B | C
3	Main life C+D	0-0-C-D	4	D	=	3|4	C | D
4	Main life D+E	E-0-0-D	1	E	A-B-C-D E-F-G-H	4 1	D E
5	Main life E+F	E-F-0-0	2	F	E-F-G-H	1|2	E | F
..							

Table 3

Table 3 illustrates a scheme where two keys are in use at each period; at the end of each period, the oldest key is invalid and must be replaced at all STAs. The advantage of this scheme over the scheme in Table 2 is that it requires less frequent configuration changes at all APs.

Mixed Systems (WEP / Non-WEP)

Usage of WEP encryption for all data transmissions dictates that all access points in the system must have the parameter "**Deny non-encrypted Data**" set to **O N** (checked in the check-box). This insures that only stations with WEP encryption enabled can connect to the network. In such a system, all data transmissions including multicasts are encrypted with the specified key(s).

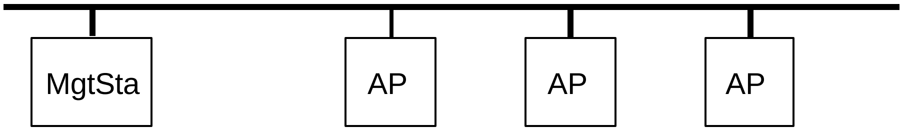
A mixed system can also be set up, where non-WEP client stations can connect to access points and can communicate in clear-text. A mixed system requires that the parameter "**Deny non-encrypted Data**" be set **OFF** (not checked in the check-box) for all access points or for some access points. Those access points will accept transmissions from non-encrypting Client Stations. To allow those client stations to receive network information, multicasts transmitted by the access point are not encrypted.

Initial versus Subsequent Key Distribution

Initial key distribution requires special attention. There is no secure path using the IBM Wireless LAN System for initial key distribution. Any remote initial configuration needs to be done using wired Ethernet connections to avoid exposure of key information as it is transmitted through the air unencrypted. Even this method is exposed. Maximum security can only be attained by going on-site for initial key installation.

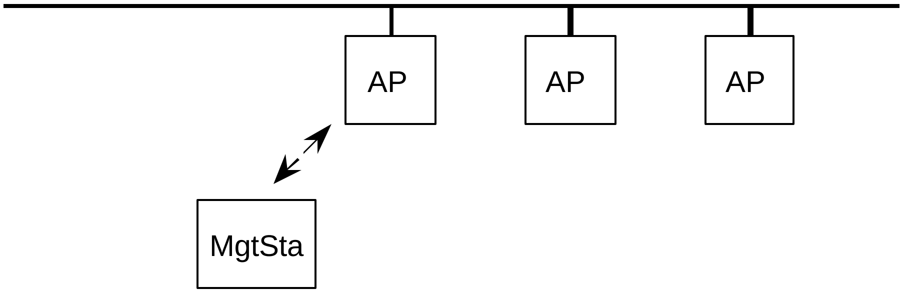
Access Points

The required setup to attain minimal security for initial configuration of Access Points is illustrated in the next figure. A management station (MgtSta) on which IBM Wireless LAN AP Manager is run connects to the Ethernet backbone to which the Access Point (AP) units are connected.



Setting up the keys (and other parameters) in this configuration performed with only minimal disclosure risk. For subsequent key changes, there will not be a security risk in using a wirelessly connected management station, as long as it uses encryption.

For complete security, a security administrator, who will configure the AP, including installation of the encryption keys, must physically visit each AP.



[1]Original content from Lucent Orinoco™