WaveLAN®

Lucent Technologies
Bell Labs Innovations

... WEP Encryption

WaveLAN Technical Bulletin 027 / A **September 1999**

General

Purpose

This bulletin provides additional information on various system aspects of the usage of the Wired Equivalent Privacy (WEP) function of WaveLAN/IEEE. Besides introducing the WEP configuration parameters, it offers suggestions on how to set-up a WaveLAN system with encryption and how to deal with regular changes to the encryption keys. It further addresses the special aspects of initial and subsequent distribution of encryption keys throughout the system.

Scope

WaveLAN System Release 4.0 adds support for the IEEE 802.11 WEP encryption function for those WaveLAN cards that are capable of hardware encryption. The cards with a silver label and annotation “Silver” support encryption; the “Bronze” cards and the original “white-label” cards are not capable to do WEP encryption.

In order to use the WEP function the Silver cards must be loaded with the firmware version 4.08 or higher. A program to load this version of firmware is available on the WaveLAN website; it runs as a Windows application called WSU10408.EXE.

General Principles and Guidelines

The WEP function offers encryption of data transmissions, using a method specified in the IEEE 802.11 standard. This will create on the wireless paths in a LAN network the equivalent privacy as is present on the wired (Ethernet) paths in the network.

When planning to setup a WaveLAN network using WEP, the following general guidelines apply:

- It is recommended to setup the system such that it only allows encrypted data transmissions; such a system requires Silver cards in all participating stations and in all WavePOINTs, as well as knowledge of the encryption key(s) at all participating stations.

- It is possible to allow users who cannot support encryption to use the network; in such a system, non-Silver cards can be used. To support users who do have encryption capability, it is required that all WavePOINTs have encryption enabled and are equipped with Silver cards.

- As is common for security aspects in networking, the distribution of the initial encryption keys requires special considerations; subsequent changes to the encryption keys can be done under the protection of the operational key.

- Changing of encryption keys over time will require manual reconfiguration of WavePOINTs and of the WaveLAN drivers in the user stations; in most cases, the reconfiguration of the user stations needs to be done at the station itself.

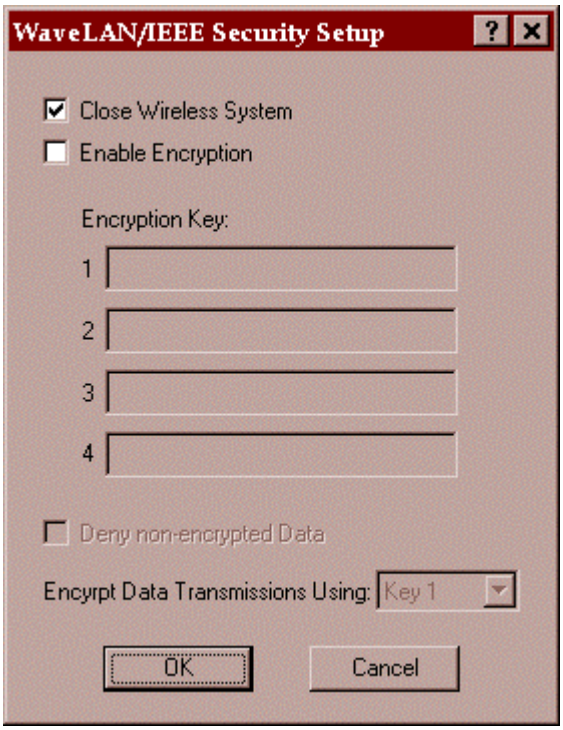
Configuration of WEP

When WEP is to be deployed in a network, all WaveLAN elements in the network need to be configured to run with WEP enabled.

Configuring WEP in WavePOINTs

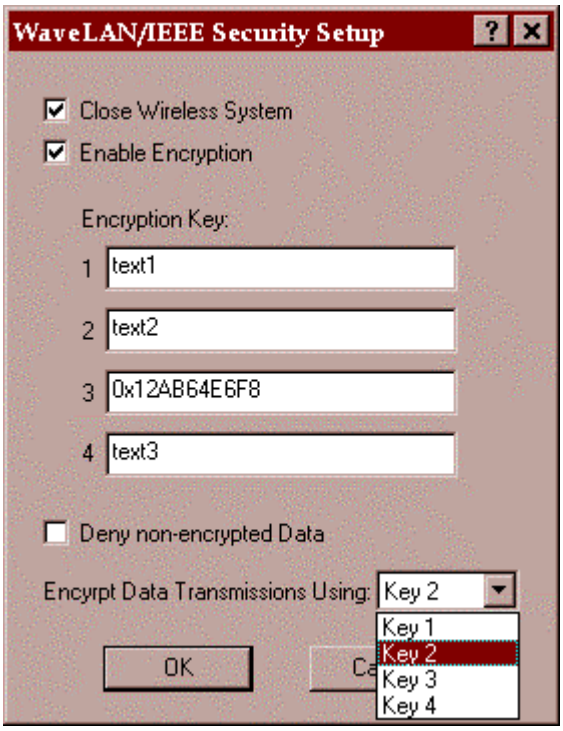
The WavePOINT configuration will determine the restrictions of the network; here the user must decide whether or not to support non-encrypted transmissions and which keys are valid to use.

The configuration screen of the WaveMANAGER/AP tool for security setup is shown below. Notice that this screen will only be presented when the socket in the WavePOINT contains a Silver card; for all other cards, only the “Close Wireless System” option will be offered.



The tick-box “Close Wireless System” is not related to WEP encryption and is not further covered.

The tick-box “Enable Encryption” defines if encryption is to be used or not. When this tick-box is checked, the further WEP related configuration items will be made available, as shown below.



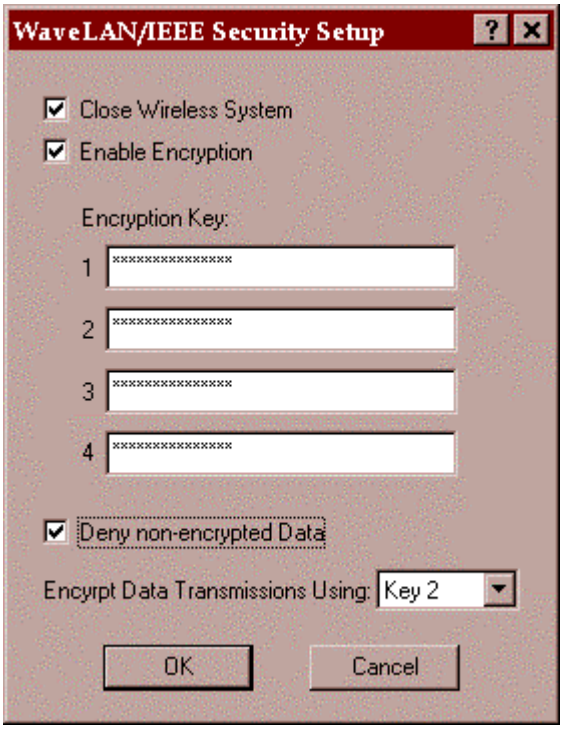
One to four encryption keys must be entered when the Enable Encryption selection is done. These keys will be used to encrypt or decrypt data transmissions. The format of entering the key values is either in textual format or in hexadecimal format (an entry starting with “0x” will be interpreted as hexadecimal). A text string is translated in the ASCII values associated with each character.

The user must assign one of the entered keys as the designated key for encrypting all transmissions by the WavePOINT; this is done by selecting the appropriate number from the pull-down-list “Encrypt Data Transmissions Using”.

The final configuration choice is the tick-box “Deny non-encrypted Data”. When this is checked, the WavePOINT will be configured not to accept stations that are transmitting data in the clear.

When a selection is entered (OK button), and read back at a later time, the key value information will be hidden by asterisk characters. Changing one or more keys will require full re-entry of the new required value at the appropriate “Encryption Key” entry-line.

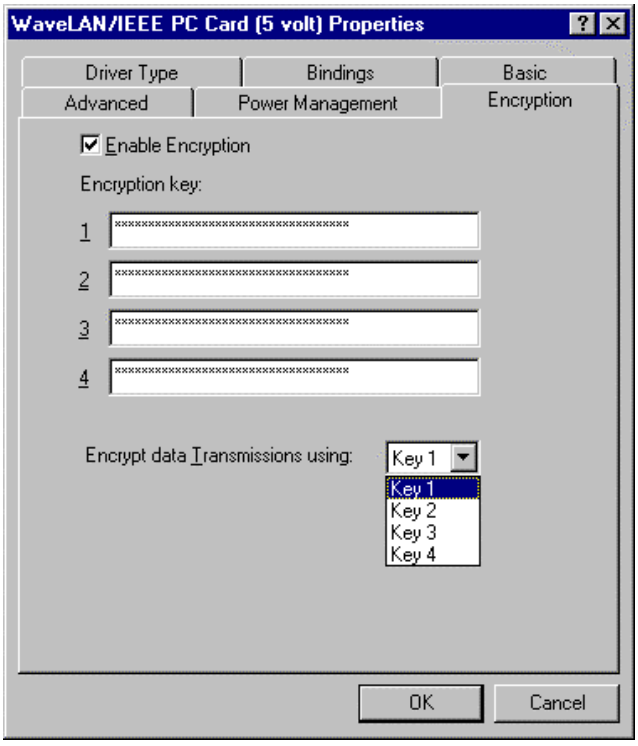
This is illustrated in the next figure.



This figure shows how the read-back screen would appear when four keys were entered and Key2 selected as transmit key.

Configuring WEP in WaveLAN Station Drivers

The figure below gives the format for the Windows based NDIS Miniport driver. A separate tab ”Encryption” is defined for the entry of the WEP related parameters.



The configuration at the station side has similar parameters as for the WavePOINT, with the exception of the “Deny Non-encrypted Data” tick-box. In a station it will always be possible to receive non-encrypted data. The primary example where this is useful is for the reception of non-encrypted multicast messages as will be required in a mixed system.

The (re)configuration has to be done in the regular Windows fashion for WaveLAN drivers. This is carried out at the station, and will result in a change of the registry on that machine. Notice that the WEP keys are not stored in clear-text in the Windows registry. The driver contains the information to interpret the stored values and translate them into the required key values.

Configuring WEP in Ethernet Converters

The (re)configuration of the WaveLAN Ethernet Converter will be very similar to the station driver configuration. The same parameters can be specified.

The key difference is that the configuration will be done from the WaveMANAGER/EC utility, running at a remote machine from the Ethernet Converter that is under configuration. From one WaveMANAGER/EC station, it will be possible to (re)configure all Ethernet Converters in the network.

Encryption Key Considerations

The configuration possibilities of both WavePOINTs and Station drivers described above makes it clear that the system can support up to four different keys simultaneously. This is in accordance with the 802.11 standard, which defines four so-called “default keys”. These keys can be used to smooth the transition from the usage of one key to usage of a next key. The general requirement for two cards to transmit encrypted between each other is that they share a common key value at the same key-index number in the 4-key area at the moment of transmission. The key-index of the key that was used for encryption is transmitted in clear-text in the header of the message, and will be used at the receiving side to determine which of the 4 keys to use for decryption.

So it is not mandatory that both sides (typically WavePOINT and End Station) have the same active set of 4 keys. As long as there is one key in common, they can communicate, provided they both use that common key.

NB: The 802.11 standard also defines the possibility for having a unique key per Station, tied to the station’s MAC Address. WaveLAN currently does not support that feature of the standard WEP function.

Key Roll-Over

When planning the usage of different keys over time a number of aspects have to be considered:

- the length of time one key stays in use;
  this is a direct trade-off between security level (= the chance of someone finding out what the key value is) and operational overhead (= the efforts to reconfigure WavePOINTs and Stations)

- the requirements for smooth transition from one key to another
- the minimization of end user exposure to key values

The key roll-over possibilities built in the 802.11 standard and offered by WaveLAN allow for a number of scenarios, each with different values for the above aspects.

The sequence of key configuration settings at WavePOINT (shown as AP=Access Point) and Station (shown as STA) over time is shown in a number of tables below. Each table reflects a certain key roll-over strategy. Notice that the column "Outward Key" shows which key is used to encrypt traffic from AP to STA and the column "Inward Key(s)" indicates the key(s) that are allowed and possibly used to encrypt traffic from STA to AP. The WEP Keys that are configured are shown in order of index number 1-2-3-4; the column "Tx" is the index number configured for transmission. The key values are shown by capital letters to indicate a real key or by zero to indicate 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 relevant when it concerns the STA keys, since it is envisaged that knowledge of the key values is typically not transferred to the end users, so they have to return their STA equipment to an IP department to get the key values changed. It is envisaged that changing the Txkey Index is an action that can be done by end users, since it does not reveal secret information.

Single Key – No Transition

Table 1 shows a system, where at each point in time only one single key is used. The key to be used is dictated by the AP settings, showing only one valid key at each period. This requires a change over of keys at all STAs more or less synchronous with the AP configuration changes.

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

To introduce a transition period between the main life of the successive keys, the scheme has to be 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

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

Alternative Schemes

Alternative schemes can be envisaged, which have main life periods in which two or more keys are active. An example is given 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 gives a scheme where at each period two keys are in use; at the end of each period, the oldest key is no longer valid and needs to be replaced at all STAs. Advantage of this scheme versus the scheme in table 2 is that it requires less frequent configuration changes at all APs.

Mixed System (WEP / No-WEP)

When setting up a system which strictly demands the usage of WEP encryption for all data transmissions, all the WavePOINTs in the system must be configured to have the parameter "**Deny non-encrypted Data**" set to **ON** (checked in the tick-box). This will assure that only stations with WEP encryption enabled can connect to the network. In a system configured this way, all data transmissions, including multicasts are encrypted with the specified key(s).

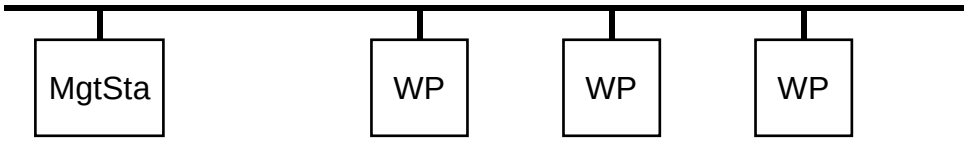
It is also possible to setup a mixed system, where non-WEP stations are allowed to connect to the WavePOINTs and to communicate in clear-text. To create that situation, the parameter "**Deny non-encrypted Data**" must be set **OFF** (not checked in the tick-box) for all WavePOINTs or for a selection of WavePOINTs. Such WavePOINTs will accept non-encrypting stations. To allow such stations to receive network information, the multicasts sent by the WavePOINT are not encrypted.

Initial versus Subsequent Key Distribution

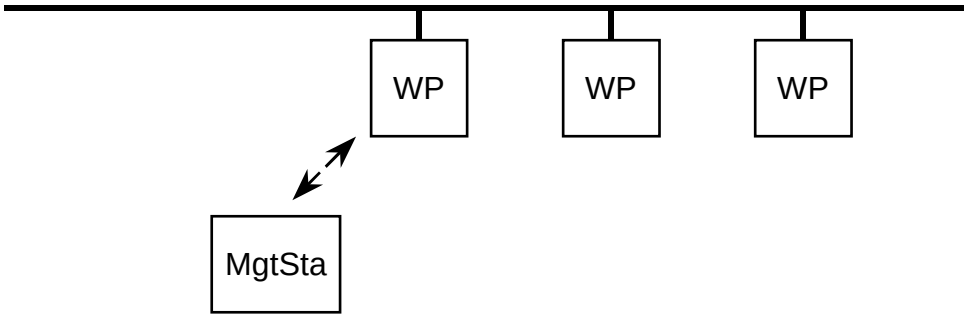
The initial key distribution is always a situation requiring special attention. At the initial distribution, there is by definition not a secure path via the WaveLAN interface. Any remote configuration needs to be done strictly via wired Ethernet connections to avoid exposure of key information being transmitted through the air unencrypted.

WavePOINT

The required setup for initial configuration of WavePOINTs is illustrated in the next figure. A management station (MgtSta) on which WaveMANAGER/AP is run connects to the Ethernet backbone where also the WavePOINT (WP) units are connected.

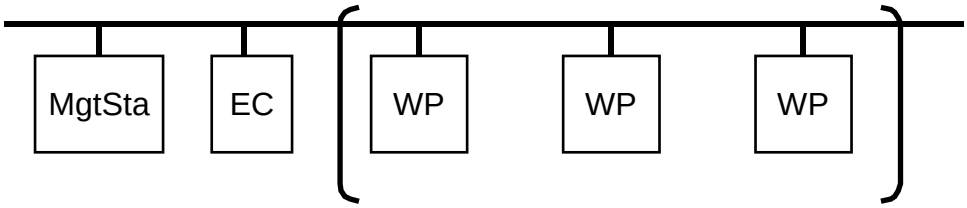


Setting up the keys (and other WEP parameters) and transfer between the management station and the WavePOINT units can be done without disclosure risk. For subsequent changes, it will not pose a security risk to use a wirelessly connected management station, as long as it uses encryption.

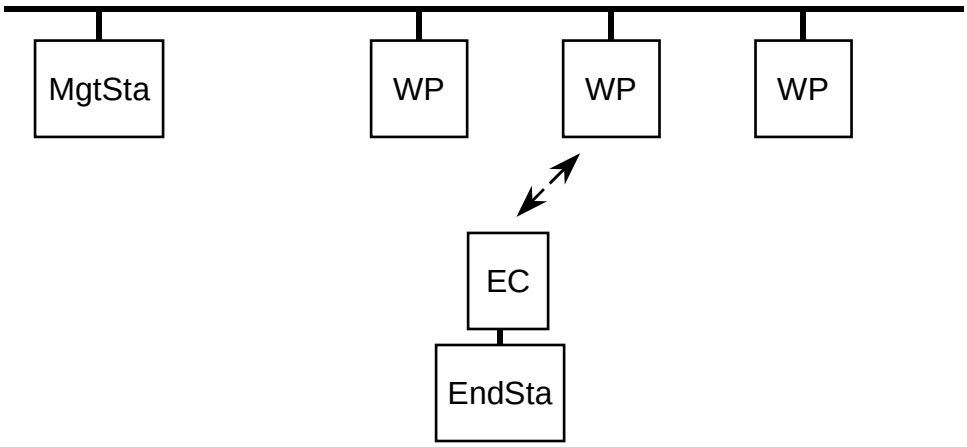


WaveLAN Ethernet Converter

The required setup for initial configuration of WaveLAN Ethernet Converters is illustrated in the next figure. A management station (MgtSta) on which WaveMANAGER/EC is run connects to the Ethernet backbone where also the Ethernet Converter (EC) units are connected. The WP units are shown for reference only and are not relevant in this EC configuration step.



In this setup, the EC units are not operational, since they are intended to be hooked up to an end station via their Ethernet connection. For subsequent re-configuration, the EC units can be kept in their target physical configuration, as illustrated below.



As long as the network is WEP protected, the reconfiguration information (including new keys) can be transmitted over the ethernet and the wireless path via the WP units that connect the EC units. This way, the EC units can be reconfigured from a central location.

