
# Fixed Wireless Security

WHITE PAPER

## Introduction

As wireless has become more integrated into our lives, especially in the mobile space, people have tagged the term "wireless" with the misperception that it is fundamentally incapable of being secure. But in most cases, fixed wireless, and certainly for Skyriver fixed wireless service, security should not be a concern. Although the nature of fixed wireless communications presents security demands not inherent in wired or fiber communications, you can deploy a fixed wireless network that is just as secure, if not more secure than traditional wired networks.

In this paper, we describe the methods and protocols that can be used in fixed wireless networks to make them secure. We also discuss how Skyriver thoughtfully engineered and deployed a fixed wireless network that incorporates a multi-level security solution, based on state of the art security protocols for the protection of Skyriver customers.

## Fixed Wireless Network Security General Concept

The two master elements of wireless security are:

- Encryption and Data Privacy
- Authentication and Access Control

### Encryption and Data Privacy

The aim of encryption is to provide a mechanism to deliver data privacy and integrity. The data should not be decrypted by any unauthorized means. All transmitted packets should originate from senders. The security mechanism should enforce the integrity of data under any circumstances. This requires different techniques to encrypt the actual information so that in the case of access to data, intruders are not able to access the actual information.

### Authentication and Access Control

In fixed wireless networks, the first phase of network security is blocking unauthorized users to access your network before they can create any harm. Authentication should be mutual, enabling wireless device clients and the access network to authenticate each other. A framework should be introduced in order to facilitate the transmission of authentication messages between clients, base stations and authentication servers. From the perspective of the access network, a mechanism should be introduced to validate client credentials in order to grant the right level of access to the requested clients.

In the following sections, the general concepts for encryption and authentication are discussed, followed by specific cases used in fixed wireless systems, and most importantly, in the Skyriver network.

## Encryption and Data Privacy

The main concept of encryption in information theory is to encrypt the information in such a way that only trusted parties can decrypt and gain access. This procedure is accomplished by using a "key". A key is a large set of information that is only known to trusted parties.

### Symmetric Key Encryption

To perform encryption and decryption in secret-key cryptosystems, the same secret key shared between a sender and a receiver is used to encrypt and decrypt messages. With such cryptosystems, the decryption algorithm is simply the reverse of the encryption algorithm (a symmetric cipher). Although this encryption method is easy to implement, it is also easily broken by rogue users because of its simplicity.

### Public Key Encryption

In public key cryptosystems, operation is based on a pair of keys - one key is used to encrypt messages and the other key (different from the first one) is used to decrypt them (see Figure 1). The encryption key is a public key because it need not be secret, i.e. can be made public, but still used for authenticated users in the system. The decryption key is a private key and must be kept secret. In order for public key encryption and decryption to work, the public and private key pair must be selected to satisfy certain mathematical properties. To see how public key encryption operates, suppose that parties A and B wish to communicate to each other using public-key encryption. Let us denote party A's public and private key pair as (Pua, Pra), and party B's public and private key pair (Pub, Prb). In order for party A to send a message to party B, A fetches B's public key Pub (which is not secret and is publicly available), encrypts the message with it and transfers it to B. On receipt of the encrypted message, B decrypts it using his private key Prb. Similarly, if B wishes to send a confidential message to A, B encrypts it with A's public key Pua, and upon receipt, A decrypts it using his private key Pra.

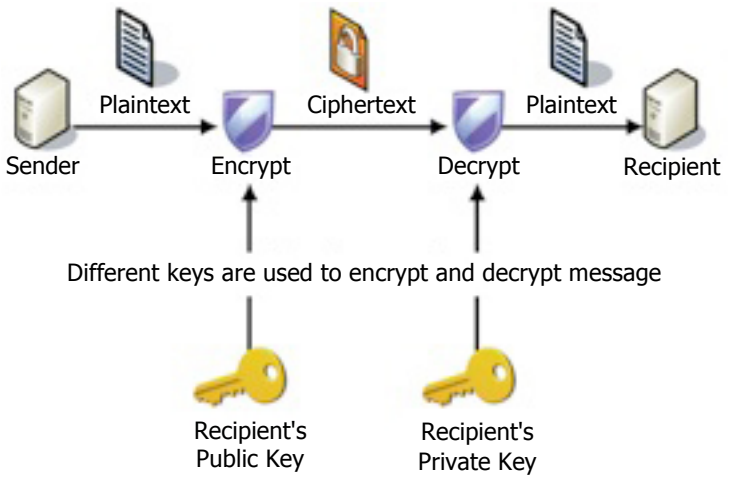


**Figure 1**

## Fixed Wireless Encryption

Fixed Wireless LAN and MAN technologies use the "stream cipher" concept, which is a public key encryption variety. Typically, in stream cipher, a stream of bytes (data packets) will be coded individually. A key (K) is used as a seed generator to create a sequence of pseudorandom bytes (key streams) to encrypt a stream of packets as shown in Figure 2. The pseudorandom generated patterns are only known to trusted parties.

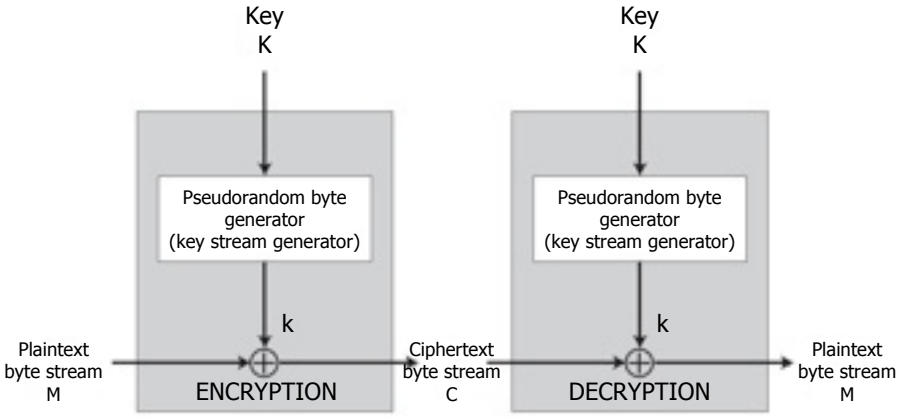


**Figure 2**

Figure 3 shows a general encryption concept at the frame level for fixed wireless networks. All packets are encrypted before transmitting over the air using a RC4 key. Each packet is encrypted with a different RC4 key to increase the overall security of the network. Even if an intruder can recover one RC4 key, only one of the packets will be recoverable, not the whole string of packets. The length of the keys is 64 or 128 bits depending on vendors.

As shown in Figure 3, a 24 bits Initialization Vector (IV) is used to create the 64 or 128 bits key. Only trusted parties are aware of generating patterns. Therefore, for each packet, the transmitter creates a random key and encrypts data packets using generated 64 or 128 bits key. Before transmitting the frame, the transmitter encapsulates the encrypted data in a frame with IV used for its encryption, and sends it to the receiver. The receiver will use received IV and generate the key to decrypt the data packet. There is also an Integrity Check Value (ICV), which is a 32 bit Cycle Redundancy Check (CRC) for data integrity, and a Frame Check Sequence (FCS) to protect the transmitted frame during transmission. As mentioned before, since each packet is encrypted separately with a random IV, the chance that hackers will be able to decrypt the total message is virtually impossible.

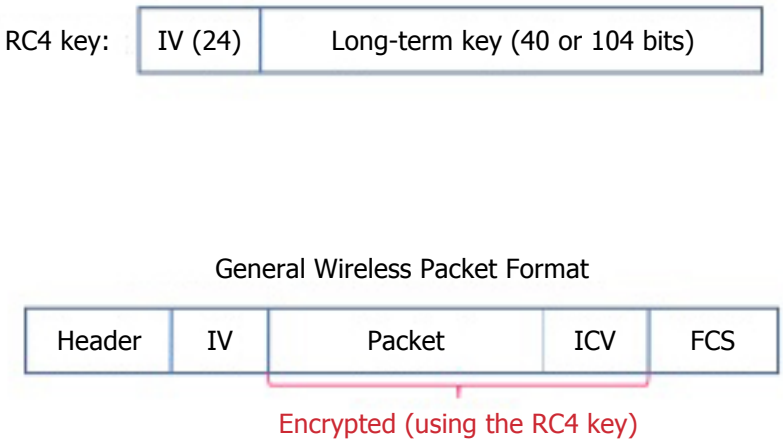


**Figure 3**

The Skyriver access network is enabled by different levels of stream cipher encryptions. This multi-level approach guarantees the security of subscribers in the case of data interception by unknown agents.

## Authentication and Access Control

In general, the Skyriver access network infrastructure uses the following mechanisms for Authentication and Access Control:

1. The client gains access to the wireless medium via multiple access protocol and makes an association with the Base Station.
2. The Base Station accepts the association but places the client in an unauthenticated "holding area". For the unauthenticated client, the access port to the network is blocked and there is no possibility for data communications. The Base Station sends an identification request to the client for further evaluations.
3. The client provides an identification response that contains a specific identifier. Upon receipt of the identification response, the accesses point forwards this response across the core network to the RADIUS server.
4. The RADIUS server looks up the user ID from a database for identification. Once it is identified, it begins a process of challenging the client. The client responds to those challenges until such time as the RADIUS server determines that the client is indeed the client that it claims to be. None of these communications are in the form of plain text over the RF, since plain text can be intercepted by hackers. Different levels of coding and scrambling secure all authentication messages.
5. In wireless LAN/MAN networks, not only must the client be authenticated, but the access point also needs to be authenticated for the client in order to prevent the rogue access points to gain control of users and sniff information.

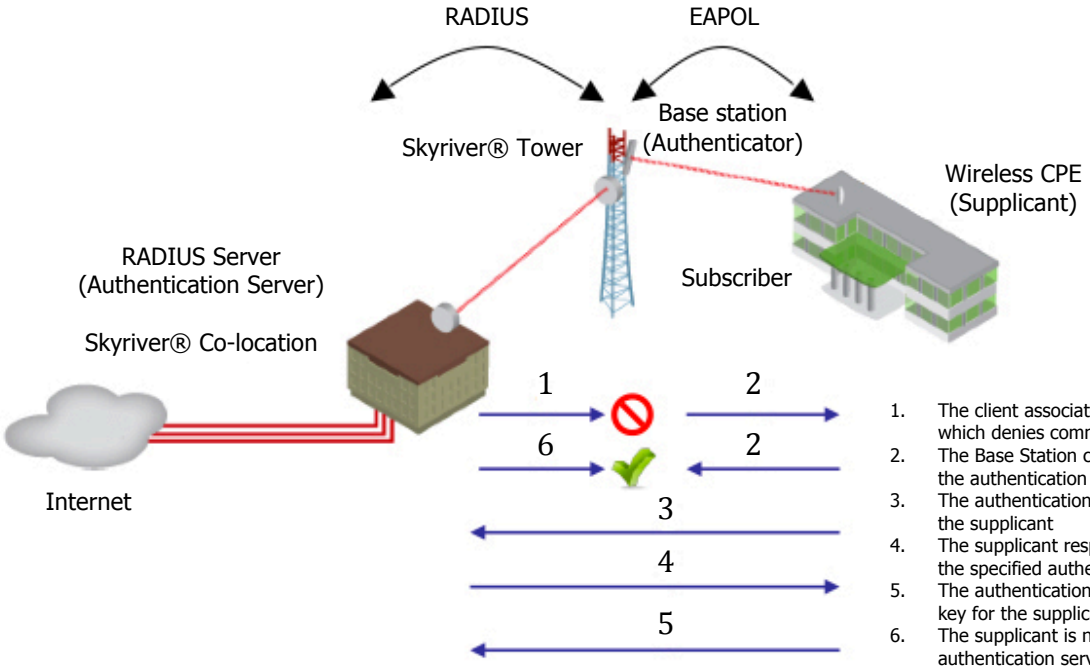


**Figure 4**

1. The client associates with the Base Station which denies communications
2. The Base Station completes a handshake with the authentication server
3. The authentication server sends a challenge to the supplicant
4. The supplicant responds to the challenge using the specified authentication method
5. The authentication server provides a session key for the supplicant
6. The supplicant is now synced with the authentication server and Base Station and can now communicate on the wireless network

**Extensible Authentication Protocol over LAN (EAPOL)**

Vendors leverage the advantage of flexibility in Wireless LAN/MAN technology to deliver a variety of authentication types. However, most of them are based on Extensible Authentication Protocol over LANs (EAPOL). As shown in Figure 4, the authentication exchange is logically carried out between the supplicant and the authentication server, with the authenticator acting only as a bridge.

Network access is controlled by the authenticator, which serves the same role as an access server in a traditional dial-up network. This is the first barrier to protect the network from unauthorized users. The authenticator only terminates the link layer authentication exchange and consequently does not maintain any user information. All incoming requests will pass to the RADIUS server for all higher level authentications including password, username, billing, etc.

The basic format of an EAPOL frame is shown in Figure 5. These frames will be exchanged during the authentication process only. Based on MAC addresses, the authenticator will provide access to a specific user. There are different types of packets in EAPOL negotiations with different lengths, which is why the packet body length is variable.

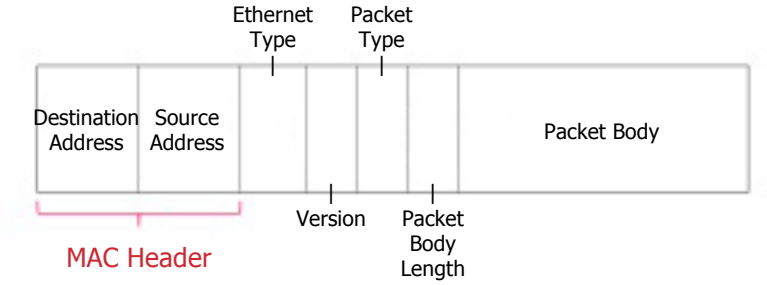


**Figure 5**

Skyriver utilizes RADIUS/EAPOL to protect its subscribers from intruders. Utilization of EAPOL at all base stations guarantees that no rogue subscribers will gain access. In the case of EAPOL failure, the second level of protection, provided by the Skyriver RADIUS server will vet all subscribers with specific authentication to make sure that all of them are permitted users. It also verifies the right set of service level (bit-rate, delay, etc) is allocated to the individual subscriber.

## Conclusion

As demonstrated, the fixed wireless industry has developed a number of security features to secure data transmission over the air, thereby making fixed wireless as secure, if not more secure that wired or cabled networks. Skyriver protects its customers by implementing a multi-level security solution based on state of the art security protocols.