



WIRELESS STANDARDS UPDATE Issue 1/2002

As you are well aware, wireless security is a primary pain point for enterprises moving forward with WLAN deployments. It has been well documented that the basic IEEE 802.11b standards, which specify an option to provide privacy on par with unsecured wireline networks, don't go far enough in securing real-world implementations.

Within this technical update, we will give a first insight into the new 802.1x standard that is designed to enhance the security of wireless local area networks.

We also give an overview of three basic modulation-techniques for transmitting data over the airwaves.

CONTENT

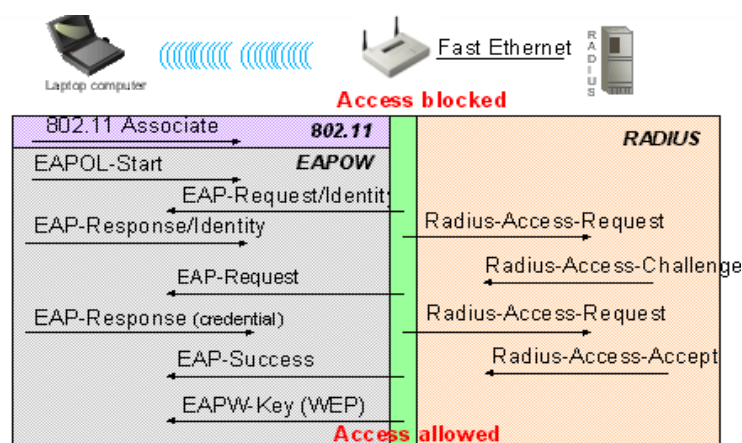
Page	Title
1	802.1x A short overview
3	Data Transmission using Wireless LAN's

✓ 802.1x: A short overview.

IEEE 802.1X is a standard for port-based network access control, to provide authenticated network access for Ethernet networks. Port-based network access control utilises the physical characteristics of the switched LAN infrastructure in order to provide a means of authenticating devices attached to a LAN port, and for preventing access to that port in cases where the authentication process fails. On the next page the successive steps are covered when a wireless client wants to logon to a network through an 802.1x enabled access-point.

When a wireless STA (Station) comes in range of a wireless AP, the following occurs:

1. The wireless AP issues a challenge to the wireless STA.
2. Upon receiving the challenge from AP, the STA sends its identity to the AP.
3. The AP forwards the STA's identity to the RADIUS server (authentication server) to initiate authentication services.
4. The RADIUS server then requests the credentials for the STA, specifying the type of credentials required, to confirm identity.
Requests passing between the STA and the RADIUS server pass through the uncontrolled port on the AP; the STA cannot directly reach the RADIUS server. The AP does not allow communication via the controlled port because the STA does not possess an authentication key.
5. The STA sends the credentials to the RADIUS server.



6. Upon validating the credentials, the RADIUS server transmits an authentication key to the AP. The authentication key is encrypted so that only the AP can access it.
7. The AP uses the authentication key received from the RADIUS server to securely transmit a per-STA unicast session key.

Following authentication, the IEEE 802.1X protocol should be configured to request the STA to re-authenticate periodically, at a configurable time interval!

Summary: With the implementation of the 802.1x security technology, enhanced means for network security is enforced. Wireless clients are denied all direct communication over the wired backbone until they are properly authenticated and granted access by the RADIUS server.

Regular re-authentication of wireless users eliminates further unauthorised access to valuable enterprise content via the wireless links. ♦

✓ Data- Transmission using Wireless LAN

Unlike radio and TV broadcasting, which still widely use analogue broadcasting to transfer data, digital data transmission is used for wireless LAN systems. These techniques were first used in military applications to provide safe radio transmission, however, these technologies have now found their widespread entrance in commercial applications.

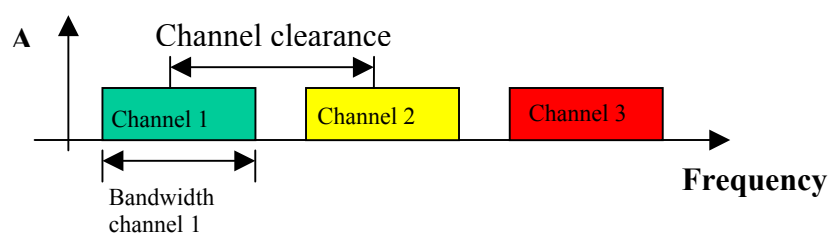
These techniques allow the available airspace to be utilised efficiently by various users at the same time without, interfering with each other.

Generally we can distinguish three transmission technologies, which we will briefly discuss below.

1) Frequency Division Multiple Access. (FDMA)

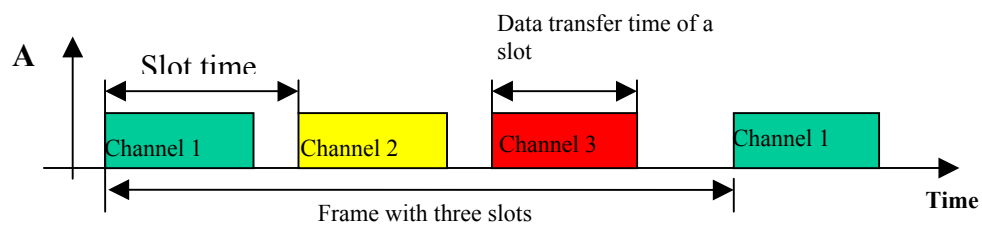
With this technique, every station has its own frequency band for data transmission. This principle is generally known from wireless broadcasting, where each radio transmitter has its own frequency channel.

Bluetooth and older systems like 802.11, use frequency hopping to transmit from one station to the other. Within the 2.4Ghz ISM band 79 channels are defined; these channels have a bandwidth of 1Mhz each, and the system permanently toggles between these channels. Therefore, essentially involving the FDMA technique.



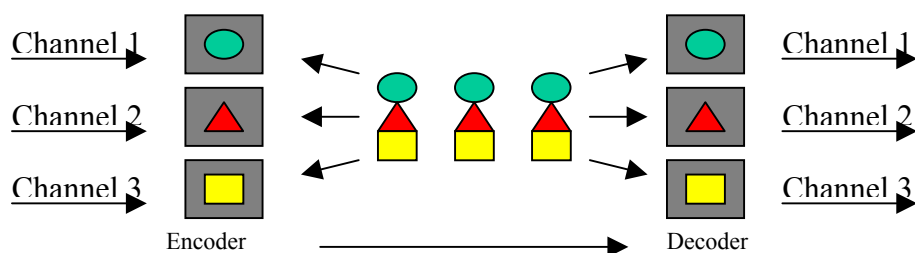
2) Time Division Multiple Access (TDMA).

Using this technique, each station can access the full bandwidth using specific timeslots. Transmission of data is so fast that it appears as if all stations are permanently connected. A widespread example of this technique is DECT (Digital Enhanced Cordless Telecommunication).



3) Code Division Multiple Access (CDMA)

Using CDMA, every station uses a specific code for data transmission, which is only understood by the partner station with an identical code (PC-card \times Access Point). This technique is the primary access technique used in DSSS (Direct Sequence Spread Spectrum), the modulation scheme utilised in the 802.11b standard. The advantage of using this technique is that a substantially higher bit-rate can be obtained in comparison with the FDMA technique (2Mbps \times 11Mbps).



However, networks similar to 802.11b use the same coding, so in order to create a disturbance-free operation in a certain area, a dedicated non-overlapping frequency band must be selected for each radio cell. In most European countries 13 channels are defined, each is taking up 22Mhz, with a 5Mhz clearance between two channels. This means that in the 2.4Ghz ISM band there are only three non-overlapping channels. This is why only three independent DSSS systems can be operated disturbance-free in one area ex. Channels 1,6,11 or 2,7,12 or 3,8,13. ♦

