



ANIXTER Technology Group

WIRELESS STANDARDS UPDATE Issue 9/2002

As wireless equipment based on the new 802.11a standard will start shipping, we provide a brief overview of the benefits and issues related to this new standard. We also take another closer look at the 802.1x port-based authentication method in relation to wireless networks.

CONTENT

<u>Page</u>	<u>Title</u>
1	802.11a Benefits and Implications
3	802.1x: Authentication and key-management

✓ 802.11a Benefits and Implications

The following are benefits of 802.11a:

- **Higher performance.** By far the top reason for choosing 802.11a is the need to support higher end applications involving video, voice, and the transmission of large images and files. In addition, 802.11a does a superior job of supporting densely populated areas of users having lower bandwidth needs, such as surfing the Internet. 802.11a can deliver data rates up to 54Mbps and there's enough room in the 5GHz spectrum to support up to 12 access points operating in the same area without causing interference between access points. This equates to 432Mbps (12 X 54Mbps) total data rate performance. Even the upcoming 802.11g standard, which will deliver 54Mbps data rates in the 2.4GHz band doesn't come close to the performance of 802.11a. With 802.11g, the same problem exists as with 802.11b: You have only three non-overlapping channels for setting access point frequencies, which severely limits capacity.
- **Less RF interference.** The growing use of 2.4GHz cordless phones and Bluetooth devices is crowding the radio spectrum within many facilities. This significantly decreases the performance of 802.11b wireless LANs. Cordless phones wreak enough havoc to cause companies to either ban the use of the



phones or not install wireless LANs. The use of 802.11a operating in the relatively un-crowded 5GHz band avoids this interference. Of course non-802.11 devices will eventually occupy the 5GHz band as well; however, there's much more room with 12 non-overlapping channels to limit interference with the other devices.

The following are drawbacks of 802.11a:

- **Less range.** The superior performance of 802.11a offers excellent support for bandwidth hungry applications, but the higher operating frequency equates to relatively shorter range. Even with this limitation, however, 802.11a can sometimes deliver better performance than 802.11b at similar ranges from the access point. For example at ranges of 100 feet, 802.11a may deliver 24Mbps, but 802.11b devices at the same range are operating at 5.5Mbps. If you're planning to deploy 802.11b networks for 11Mbps throughout the facility, it's very likely that you can install 802.11 access points at the same locations and still achieve 6 to 12Mbps data rates. As a result, you can install approximately the same number of 802.11a access points as 802.11b and likely have similar performance. When needs for higher performance occur in the future, you can add more access points to increase the coverage to 54Mbps throughout the facility. This approach enables you to grow into a longer term, higher performing solution while spreading the costs over time.
- **Limited interoperability.** 802.11a doesn't talk to 802.11b. For example, an end user equipped with an 802.11a NIC will not be able to connect with an 802.11b access point. The 802.11 standard offers no provisions for interoperability between the different physical layers. The solution to this problem is multimode radio cards that support multiple 802.11 PHYs, such as 802.11a/b, 802.11a/g, etc. These cards should be available on the market by the end of 2002 (US market). As a result, an 802.11a/b radio within an end user device will automatically sense whether the access point is 802.11a or 802.11b and then communicate accordingly. Likewise, an access point can also deploy a dual 802.11a/b solution, enabling interoperability with end user devices equipped with either an 802.11a or 802.11b radio. In the meantime, however, you can still install 802.11a wireless LANs. This assumes, however, that you're able to implement 802.11a radios in the user devices. Some devices today, such as bar code scanners, come equipped with 802.11b cards that you can't easily change.
- **Higher prices.** The current list prices of 802.11a products are approximately 30 percent higher than 802.11b, but the price gap should close over the next couple years. The higher price today, nevertheless, causes some companies to install 802.11b in order to lower initial costs. The problem is that the primary migration path for these companies to deliver higher data rates in the future will be to upgrade their 802.11b access points to 802.11g. It's not clear when 802.11g products will be available. 802.11a is widespread available



today in the United States and operates in a much less crowded part of the spectrum that includes higher capacity. 802.11a is clearly a better long-term solution, especially when future performance needs are not very well known. It's better to pay a little more now for a better solution rather than a lot more later to replace hardware.

Of course the decision on which 802.11 PHY to support depends on the requirements of your specific wireless LAN application. Based on the benefits, it is highly recommend using 802.11a unless requirements dictate otherwise. It's always better to have too much performance rather than not enough, especially for large numbers of users and higher end applications.

Source : www.802.11planet.com

✓ 802.1X : Authentication and Key Management

With 802.11's optional WEP (Wired Equivalent Privacy), all access points and client radio NICs on a particular wireless LAN must use the same encryption key. Each sending station encrypts the body of each frame with a WEP key before transmission, and the receiving station decrypts it using an identical key upon reception. This process reduces the risk of someone passively monitoring the transmission and gaining access to the information that the frames are carrying.

A major underlying problem with the existing 802.11 standard is that the keys are cumbersome to change. If you don't update the WEP keys often, an unauthorized person with a sniffing tool, such as AirSnort or WEPcrack, can monitor your network for less than a day and decode the encrypted messages. In order to use different keys, you must manually configure each access point and radio NIC with new common keys.

Products based on the 802.11 standard alone offer system administrators no effective method to update the keys. This might not be too much of concern with a few users, but the job of renewing keys on larger networks can be a monumental task. As a result, companies either don't use WEP at all or maintain the same keys for weeks, months, and even years. Both cases significantly heightens the wireless LAN's vulnerability to eavesdroppers.

The use of IEEE 802.1X offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1X ties a protocol called EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media and supports multiple authentication methods.

Initial 802.1X communications begins with an unauthenticated supplicant (i.e., client device) attempting to connect with an authenticator (i.e., 802.11 access point). The access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point.



The access point blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the access point can verify the client's identity using an authentication server (e.g., RADIUS). Once authenticated, the access point opens the client's port for other types of traffic.

To get a better idea of how 802.1X operates, the following are specific interactions that take place among the various 802.1X elements:

1. The client sends an EAP-start message. This begins a series of message exchanges to authenticate the client; think of this as a group of visitors entering the front gate of a theme park and the group's leader (i.e., client) asking the gatekeeper (i.e., access point) whether they can enter.
2. The access point replies with an EAP-request identity message. In the case of the theme park, the gatekeeper will ask the leader for their name and drivers license.
3. The client sends an EAP-response packet containing the identity to the authentication server. The leader in our example will provide their name and drivers license, and the gatekeeper forwards this information to the group tour manager (i.e., authentication server) who determines whether the group has rights to enter the park.
4. The authentication server uses a specific authentication algorithm to verify the client's identity. This could be through the use of digital certificates or other EAP authentication type. In the case of our example, this process simply involves verifying the validity of the leader's drivers' license and ensuring that the picture on the license matches the leader. In our example, we'll assume the leader is authorized.
5. The authentication server will either send an *accept* or *reject* message to the access point. So the group tour manager at the theme park tells the gatekeeper to let the group enter.
6. The access point sends an EAP-success packet (or reject packet) to the client. The gatekeeper informs the leader that the group can enter the park. Of course the gatekeeper would not let the group in if the group tour manager had rejected the group's admittance.
7. If the authentication server accepts the client, then the access point will transition the client's port to an authorized state and forward additional traffic. This is similar to the gatekeeper automatically opening the gate to let in only people belonging to the group cleared for entry.

The basic 802.1X protocol provides effective authentication regardless of whether you implement 802.11 WEP keys or no encryption at all. Most of major wireless LAN vendors, however, are offering proprietary versions of dynamic key management using 802.1X as a delivery mechanism. If configured to implement dynamic key exchange, the 802.1X authentication server can return session keys to the access point along with the accept message. The access point uses the session keys to build, sign and encrypt an EAP key message that is sent to the client immediately after sending the success message. The client can then use contents of the key message to define applicable encryption keys. In typical 802.1X implementations, the client can automatically change encryption keys as often as necessary to minimize the possibility of eavesdroppers having enough time to crack the key in current use.



802.1X not the whole solution

It's important to note that 802.1X doesn't provide the actual authentication mechanisms. When utilising 802.1X, you need to choose an EAP type, such as Transport Layer Security (EAP-TLS) or EAP Tunneled Transport Layer Security (EAP-TTLS), which defines how the authentication takes place.

The important part to know at this point is that the software supporting the specific EAP type resides on the authentication server and within the operating system or application software on the client devices. The access point acts as a "pass through" for 802.1X messages, which means that you can specify any EAP type without needing to upgrade an 802.1X-compliant access point. As a result, you can update the EAP authentication type as newer types become available and your requirements for security change.

802.1X is the way to go

The use of 802.1X is well on its way to becoming an industry standard, and you would be wise to include it as the basis for your wireless LAN security solution. Windows XP implements 802.1X natively, and some vendors support 802.1X in their 802.11 access points. Wireless LAN implementations of 802.1X fall outside the scope of the 802.11 standard; however, the 802.11i committee is specifying the use of 802.1X to eventually become part of the 802.11 standard.

Source: 80211-planet.com