

AirGuard™ Wireless Applications

3e-525A-3 Wireless Mesh Access Point

Wireless Government Solutions

Security is Paramount

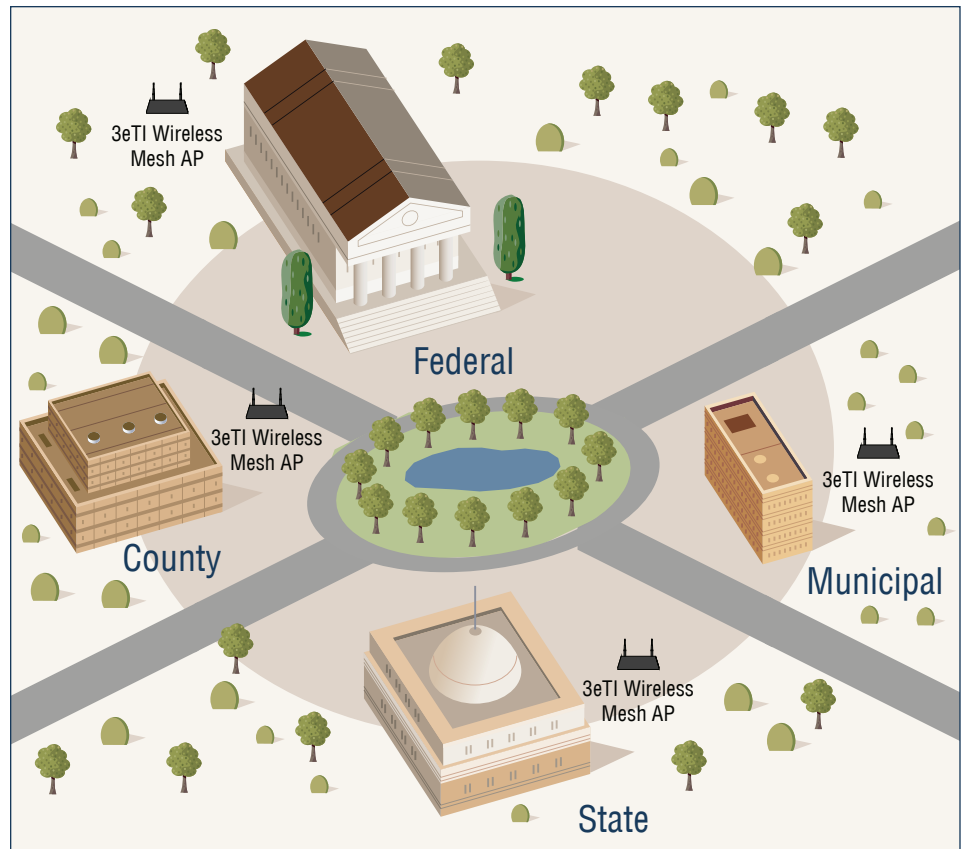
As with commercial and civilian sectors, federal, state and local government agencies see wireless networks as a way to improve mobile workforce efficiencies and enhance productivity. However, due to the sensitive nature of the data and information, wireless LAN (WLAN) security is of the utmost importance — especially when national security interests are at stake.

For U.S. government use of WLANs, stringent, layered security is required. Issued in DoD Directive 8100.2, these requirements mandate strong encryption, user authentication, key management, digital signature, and personal identification based on Federal Information Processing Standards (FIPS) 140-2. Because of the directive, all DoD, Department of Homeland Security and associated civilian agencies must incorporate FIPS validated security to protect WLAN infrastructures.

Proven Platform

Based upon a platform proven in the U.S. military, the AirGuard 3e-525A-3 wireless access point (AP) is a robustly secure, 802.11a/b/g WLAN solution providing encrypted local access, wireless bridging and repeating, and mesh networking.

The AirGuard 3e-525A-3 AP also provides load balancing, adjustable transmit (Tx) power, IPv6 protocol, data rates up to 108 Mbps, and rogue AP detection. These features make it a perfect fit for use in government wireless infrastructures.



The AirGuard 3e-525A-3 wireless mesh access point provides point-to-point, point-to-multipoint or mesh networking solutions.

Most importantly, the 3e-525A-3 AP is FIPS 140-2 Validated™ Level 2 by the National Institute of Standards and Technology (NIST), Common Criteria certified at EAL2+, and certified by the Wi-Fi Alliance.

Practical Applications — Challenging Environments

The AirGuard 3e-525A-3 AP provides 802.11a/b/g connectivity on both its access and bridging ports. In addition,

Turbo A and Super G data rates of 108 Mbps are available for access, bridging / repeating, and mesh networking.

The 3e-525A-3 AP offers practical solutions to some of government's toughest infrastructure communication challenges — easily and cost-effectively. For example, installing LAN infrastructure in landmark government and court buildings can be both difficult and costly using wired LANs. Wired

(continued on back)

AirGuard™ Wireless Applications

3e-525A-3 Wireless Mesh Access Point

Wireless Government Solutions

networks are an obtrusive and risky addition to historic government structures. Furthermore, government staff, administrators and officials require seamless connectivity throughout numerous locations — offices, meeting rooms, courtrooms and legislative chambers — places in which wired networks can't be easily installed.

3eTI AirGuard WLANs eliminate the need for extensive design, labor and materials associated with cabling, enabling high-speed connectivity without costly and risky renovation. AirGuard solutions link employees to critical network resources regardless of their locations — in their offices, legislative chambers, courtrooms and remote meeting facilities.

Cost-Effective Solutions

Unexpected situations also demand that federal, state and local government agencies often have to occupy temporary facilities. This is true for emergency situations, heavy work periods such as tax season, and rapidly expanding schools.

Staff and students housed in these areas require standard network connectivity to nearby main offices and information facilities. Yet budgets often do not permit investing in expensive hard-wired build-outs for short-term space, and

running leased lines between permanent and temporary facilities can be an expensive proposition.

Using AirGuard LAN-to-LAN bridging solutions, temporary work spaces, buildings and classrooms can be networked without costly permanent infrastructure.

Furthermore, when it comes to constant staff moves and rearrangements, 3e-525A-3 WLANs deliver flexibility that wired networks cannot provide. AirGuard solutions allow government organizations to instantly accommodate expanding staff or relocate employees without the high cost of wired additions.

Tangible Benefits

AirGuard infrastructure solutions are simple and inexpensive to implement and provide quick return on investment compared with wired networking additions. Government agencies can save hundreds of dollars per user each time they add or move staff within an AirGuard wireless network. Wireless networking studies also indicate increased employee connect time of two hours longer a day, with an average productivity increase of 22 percent.



AirGuard 3e-525A-3 wireless mesh access point

Benefits

- DoD-proven, FIPS 140-2 Validated™ security
- Increased staff productivity and connectivity time
- Lower total ownership cost than cable
- Extended network with point-to-point, point-to-multipoint or mesh connectivity
- Up to 108 Mbps hot spot / access, bridging and repeating
- Self-configuring, self-healing mesh networks — up to 40 nodes
- Total WLAN solution

FIPS 140-2 Validated™ is a Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian government.