

Secure Wireless Mesh Networks

Wireless Mesh Networks (WMNs) represent a rapidly evolving technology that delivers a seamlessly connected world. These networks are able to effectively connect deployed military units using a flexible and cost-effective existing technology without the burdens of cable management.

The WMN spreads the network connection across dozens or even hundreds of wireless mesh nodes that “talk” to each other to share the connection across a large area. WMNs are anticipated to resolve the limitations and to significantly improve the performance of ad-hoc networks, wireless local area networks (WLANs), wireless personal area networks (WPANs), and wireless metropolitan area networks (WMANs).

WMNs address the market requirements for networks that are highly scalable and offer end users secure, seamless roaming beyond traditional WLAN boundaries. Mesh networks are very reliable, offering considerable network redundancy. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes, whether they are fixed or mobile. In this way, the wireless mesh networks can self-form and self-heal dynamically even where the end points are moving.

Implementation Scenarios for WMNs

AEP Networks pioneered the use of Meshed Networks, originally developed to give soldiers easy deployable, reliable voice, data communications anywhere in the battlefield. The solution creates a wireless network which concentrates all the traffic from any remote nodes/devices in range. The network operates up to 40km in radius. Once the network has been created, any remote node/device can attach to the network using the applications auto roaming functionality. The remote node use the wireless network to securely transmit the user services to the central site, data packets received are then prioritised and aggregated onto the available backhaul, to be delivered to the user services.

The solution can be implemented across a fixed infrastructure for long term use or can be rapidly deployed - within as little as 30 minutes - for event or emergency related applications.

However, the application of WMNs is not limited to military operations or to rugged, isolated regions. They are also being more widely deployed to provide and protect communications across and between military installations (large camps, airfields etc) to



AEP Networks' Deployable Communications Solutions securely handle many-to-many connections in rugged environments, and are capable of dynamically updating and optimising these connections.

provide resilient communications without the need to bury cables. WMNs can ensure that everyone is connected at all times and they are able to link into public networks where required.

Temporary venues also represent a justification WMNs because they can be set up, augmented and moved as necessary while projects progress. This might include military exercises, coalition deployments and homeland defence operations. The deployed forces may well set up a mesh network to cater for an incident that needs to be dealt with quickly and effectively with secure communications as an absolute necessity.

Benefits of AEP Networks WMN implementation at-a-glance

Rapid Implementation: WMNs can be rapidly installed; their architecture is inherently self-organising and does not require manual configuration.

Ease of Management: Centralised control, management and configuration for all satellite/terrestrial networks either at the hub or at the edge/remote location.

Scalability and Redundancy: Nodes can be added for uninterrupted communications; node density also insures redundancy through multiple available paths.

Cost-Effectiveness: Deploying and supporting WMNs does not require extensive planning, installation and administration. Site employees can make changes without having technical expertise.

Disaster Recovery: Ease of implementation in any environment insures continuity of communications during an emergency or disaster.

Multi-Service Communications: Blends Inmarsat, VSAT, 3G, Wifi/WiMax into one service offering.

Uninterrupted Service: End users maintain the same IP address and original phone numbers irrespective of backhaul or service provider used.

AEP Networks Solution

Designed to support a wide range of protocols over many types of physical interfaces

Designed to support a wide range of protocols over many types of physical interfaces

Fully converged and secure packet switch wireless network capable of transmitting video, voice, fax and data over AEP Network's own government approved encryption devices (or other encryptors sourced by the end user where required) using a combination of fixed, mobile, wireless and satellite technologies.

The architecture provides a highly scalable, flexible and secure infrastructure that can operate automatically over different fixed, mobile and satellite networks.

The technology supports a wide range of protocols over many different types of physical interfaces. It is possible to connect the system to 3G mobile networks, Leased Lines, PSTN, ISDN lines, DSL, cable and satellite interfaces, automatically without the need for user configuration. This ability to carry all services across so many different interfaces, and its ability to auto detect the available circuits makes it flexible, resilient and extremely user friendly. The software is configurable to provide user-mandated prioritisation

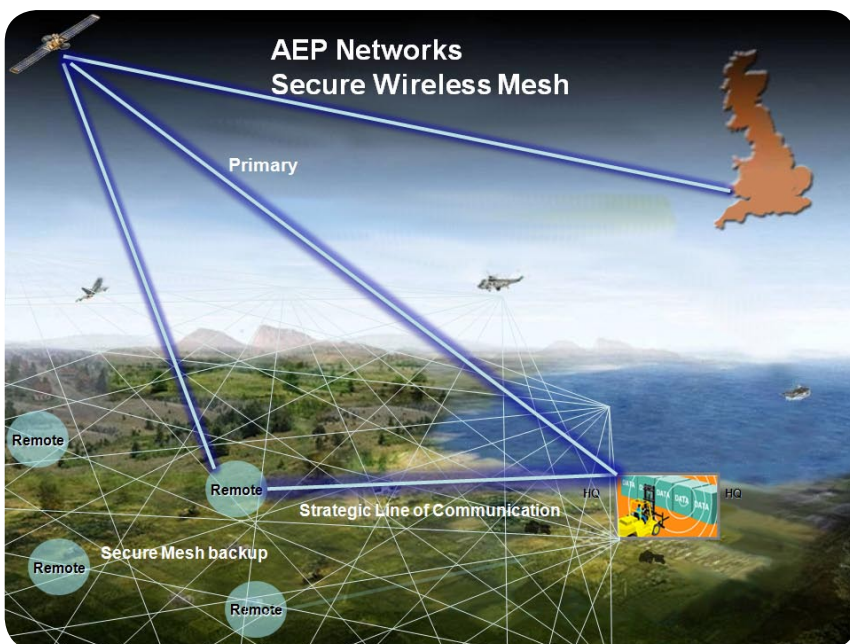
for video, voice and data to control the delays on critical access links.

The functionality includes IP routing and bridging as well as support for a wide range of legacy protocols and terminal emulations. A combination of Sync, Async, Ethernet switch and voice ports all in one unit provides a highly configurable and flexible communications configuration, which supports both legacy and today's sophisticated communications needs.

WMNs in Operation

AEP Networks' WMN solution creates a wireless envelope which concentrates all the traffic from any remote nodes in range. The wireless envelope operates up to 25km in radius. Once the envelope has been created, any remote node can attach to the network using the auto roaming functionality. The remote node uses the wireless network to securely transmit the user services to the central site. Data packets received are then prioritised and aggregated onto the available bearer, to be delivered to the user services.

The solution can be implemented across a fixed infrastructure for long term use or can be rapidly deployed – within as little as 30 minutes – for event or emergency-related applications.



AEP Networks offers secure, multi-bearer communication solutions that are assured to CAPS, CCTM, EU Council and FIPS standards. AEP Networks support a wide range of communications protocols, capable of integrating into a multitude of fixed and mobile network topologies and physical interfaces, enabling access to core voice and data services from the most extreme remote locations, where conventional communications may not be available, or where it is uneconomical to supply fixed telecom infrastructures.

United States

Toll-Free: +1-877-638-4552
 Tel: +1-732-652-5200

Europe

Tel: +44 1442 458 600

Greater China

Tel: +86-13382388860

Japan, SE Asia, Singapore

Tel: +60 3 2166 2260

Australia/New Zealand

Tel: +61 29924 4855

Email: sales@aepnetworks.com Web: www.aepnetworks.com