Sierra Wireless® AirLink Connection Manager (ACM)

FEATURES
- Supports all AirLink gateways
- Integrated Mobile VPN
- Sub-second switching[1]
- Multi-network support
- Meets industry standard security requirements, including FIPS 140-2[1]

BENEFITS
- **Simplified Architecture/ Administration:** enables the enterprise to retain management control over network access and connected mobile assets

- **Simplified deployment at lower cost:** eliminates the need for VPN software clients for individual devices and applications

- **Secures all devices:** securely connects all in-field applications and mobile assets in and around the vehicle to the enterprise

Mobile, Multi-Network Security

Sierra Wireless delivers a complete networking solution that connects mission critical workforces. Ensuring reliable and secure communications for your field workforce is much more complex than it is for office workers. The field workforce is mobile, working across multiple networks as coverage dictates. The hand-off between networks must happen quickly, transparently and securely. Furthermore, the number of devices and applications being used in vehicles is increasing. The IT team requires a solution that secures the myriad devices and applications over any wireless network and one that switches traffic quickly enough that new higher bandwidth applications like voice and video operate without interruption.

FAST NETWORK SWITCHING

The AirLink® Connection Manager (ACM) is a mobile-optimized VPN server that securely extends the enterprise network to the vehicle. Designed to work with AirLink® gateways and routers, the ACM consolidates security onto a single platform for all connected devices and applications in the vehicle area network.

Enterprise applications that require a stable connection and/or static IP address can now be fully mobilized and operate in the vehicle over multiple networks, including data networks from different service providers, public and depot Wi-Fi infrastructures. Static IP plans from the network operator are no longer required. Secure connectivity of devices without VPN client support can be realized. FIPS compliance can now be met. Management of the network is now within the full control of the enterprise.

MULTI-NETWORK SUPPORT

The use of multiple wireless networks highlights the need for a new approach to security. An in-vehicle communications device must be aware of the network environment and know when to switch. The MG90/oMG is constantly monitoring all available networks to determine if connections can be made and if data can be successfully transmitted. It then applies a wide range of user-defined policies to determine which network can be used and immediately switches the traffic. This awareness of the multi-network environment coupled with the ability to keep secure tunnels active over multiple paths allows the switching to happen quickly and securely.

SIMPLIFIES DEPLOYMENT

The ACM server works with AirLink routers and gateways and the AMM to simplify deployment of secure mobile communications across your fleet. Once installed in the DMZ and connected to the corporate firewall, the mobile environment can be set up independently. The mobile-optimized VPN software running on the AirLink oMG/MG90 secures all vehicle area network traffic in and around the vehicle without the need for special software on client devices, and works with the ACM to secure traffic over multiple wide area wireless links. ACM uses standards-based protocols, ensuring organizations are not locked into proprietary security solutions.

COST EFFECTIVE

Since security is provided in both the LAN and WAN environments, and licensing is per router/gateway, ACM is a cost effective VPN security solution. Specialized client software is not required on devices such as laptops, tablets or Smartphones. New applications and devices can be deployed without incurring the additional cost of client licenses, and the reduction in reconfiguration and maintenance effort will result in significant savings for IT departments.

TECHNICAL SPECIFICATIONS

FEATURE	SPECIFICATION
ROUTING	• IPv4 routing - BGPv4, OSPFv2, Custom Static Routes
IP ADDRESS MANAGEMENT	• Static
ENCAPSULATION	• Ethernet, 802.1Q VLANs
FIREWALL	• Stateful Inspection Firewall • ICMP Type Filtering
VPN	• IPsec using Internet Key Exchange (IKEv1/IKEv2) • Mobility and Multi-Homing Extension (MOBIKE)
ENCRYPTION	• 3DES, AES-128 and AES-256 • FIPS-140-2 compliant[1] (optional)
HASHING	• MD5/SHA1/SHA256/SHA512
KEY EXCHANGE	• DH Group 2/5/14/15/16/17/18/19(FIPS)
AUTHENTICATION	• PSK, Certificate(RSA,ECDSA), EAP
HIGH AVAILABILITY	• VRRP • DNS Load Balancing
MANAGEMENT	• Integrated CLI • SSHv2/SSH Public Key
SUPPORTED ROUTERS/GATEWAYS AND CLIENTS	• AirLink Routers/Gateways: oMG2000/500, MG90, MP70, RV50, GX/ES450, LS300 • Mobile VPN Clients: NCP Secure Entry Client
LOGGING	• Syslog • SNMPv2c
HARDWARE	• 19" 1RU rack-mount server appliance • Redundant configuration highly recommended