SIERRA WIRELESS
A SEMTECH COMPANY

DATASHEET

AirLink® Connection Manager (ACM)

KEY FEATURES

- Certified end-to-end solution for all AirLink routers and gateways
- Easy to deploy and manage
- Purpose-built VPN appliance for in-vehicle use cases
- Sub-second switching between multiple networks[1]
- Meets industry standard security requirements, including FIPS 140-2[1]

VPN Virtual Appliance for AirLink Routers and Gateways

AirLink® Connection Manager (ACM) is a VPN appliance that securely extends the enterprise network to the mobile workforce. Optimized for mobility applications, ACM delivers a complete end-to-end solution to securely connect people and mission critical applications. ACM is deployed as a virtual appliance.

Ensuring reliable and secure communications for the mobile workforce is much more complex than it is for office workers:

- Mobile workforces work across multiple networks as coverage dictates, and require uninterrupted connections; a challenge with standard VPN solutions
- First responders, and law enforcement in particular, need to comply with strict encryption guidelines for their communications
- IT teams need an solution that is easy to deploy and manage, and which secures a myriad of devices and applications present in the organization's vehicles

Designed and certified on all AirLink routers and gateways, ACM leverages technologies such as MOBIKE (fast switching), FIPS 140-2 (encryption) and Vehicle Area Networks (VANs) to provide a fast, secure and reliable connection between your routers and your networks.

FAST NETWORK SWITCHING

An in-vehicle communications solution must be aware of the network environment and know when to switch between available networks. AirLink gateways and routers, such as the AirLink XR90 and MG90 multi-network vehicle routers, are 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 all the time over multiple paths, allows the switching to happen quickly and securely.

Traditional LAN-to-LAN VPN solutions will drop the VPN connection if there is a change in the network connection, causing delays of up to 1 minute or more to rebuild the secure VPN tunnel. Software VPN clients may also require login credentials further interrupting connectivity. ACM is optimized for use in a mobile, multi-network environment to seamlessly maintain the VPN as users roam between networks and ensure zero downtime and no loss of communications. This is particularly important for first responders where even a short interruption in communications can make the difference between life and death.

---

1. *Available on AirLink® MG90, XR80 and XR90*

FIPS 140-2 COMPLIANT

While traditional VPN appliances use strong encryption modules, ACM is one of the few that is FIPS 140-2 compliant, ensuring CJIS requirements are met and data from any of the devices connected to the AirLink router is transmitted with the same security level.

VEHICLE AREA NETWORK

Devices connected to the AirLink vehicle router are part of the vehicle area network (VAN).

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 public carrier networks and depot Wi-Fi infrastructures. Static IP plans from the network operator are no longer required and data from devices without VPN client support can finally be secured.

SIMPLIFIES DEPLOYMENT

Once ACM is installed in the DMZ and connected to the corporate firewall, the mobile environment can be set up independently. The mobile-optimized ACM VPN software running on the AirLink devices secures all vehicle area network traffic in and around the vehicle without the need for special software on client devices.

ACM uses standards-based protocols, ensuring organizations are not locked into proprietary security solutions.

COST EFFECTIVE

Since security is provided in both the VAN and WAN environments, and licensing is per router/gateway, ACM is a cost effective VPN solution. Specialized client software is not required on devices such as laptops, tablets or smartphones. New applications and devices can be easily deployed or removed without changing the underlying security infrastructure or incurring the additional cost of client licenses or static IP plans from the carrier. As a result, the reduction in reconfiguration and maintenance effort provides significant savings for IT departments.

Benefits

- **Always on connectivity:** No downtime or loss of communications, even when roaming between networks (cellular and/or Wi-Fi)
- **Simplified deployment and management:** Built for and pre-tested with all AirLink® devices, it makes set up and on-going management easy
- **Low Total Cost of Ownership (TCO):** Provides a carrier agnostic solution, which doesn't require specific service (e.g static public IP), and eliminates the need for VPN software clients for individual devices
- **FIPS 140-2 Compliant:** Securely connects all in-field applications and mobile assets in and around the vehicle to the enterprise with FIPS 140-2 or AES 256

AirLink® Connection Manager (ACM) – Specifications

KEY FEATURES	
Routing	IPv4 Dynamic - BGPv4, OSPFv2 Static - Custom Static Routes support for corporate connected resources
IP Address Management	Static
Encapsulation	Ethernet, 802.1Q VLANs for Quality Service
Firewall	Stateful Inspection Firewall ICMP Type Filtering
LAYER 3 Ipsec VPN	Mobility and Multi-Homing Extension (MOBIKE) IPsec using Internet Key Exchange (IKEv1/IKEv2)
VPN Performance	Support 1,000 concurrent tunnels per ACM appliance Throughput 900 Mbps
FIPS Support	FIPS-140-2 (optional)
Encryption Algorithms[2]	FIPS: AES-256 NON-FIPS: 3DES, AES-128, AES-256
Hashing[2]	FIPS: SHA256, SHA512 NON-FIPS: MDS, SHAI, SHA256, SHA5I2
Key Exchange[2]	FIPS: DHGROUP 14/15/16/17/18/19 NON-FIRS: DHGROUP 2/5/14/15/16/17/18/19
Authentication	PSK, Certificate (RSA,ECDSA), EAP
High Availability	VRRP DNS Load Balancing
Management	Support SSHv2/SSH Public Key Integrated CLI available
Supported Routers/ Gateways and Clients	AirLink Routers/Gateways: XR80, XR90, MG90, MP70, RV50, GX450, ES450 NCP Secure Entry Client for Windows machines (for access outside VAN)
Logging	Syslog SNMPv2c
Deployment	Virtual appliance compatible with vSphere 6.5 or later

[2] *Sierra Wireless does not recommend the use of 3DES, AES-128, MDS, SHAI or DH GROUPS 2 or 5. More secure options should be selected.*

About Sierra Wireless

Sierra Wireless (a subsidiary of Semtech Corporation) is a world leading IoT solutions provider that combines devices, network services, and software to unlock value in the connected economy. Companies globally are adopting 4G, 5G, and LPWA solutions to improve operational efficiency, create better customer experiences, improve their business models, and create new revenue streams. Sierra Wireless works with its customers to develop the right industry-specific solution for their IoT deployments, whether this is an integrated solution to help connect edge devices to the cloud, a software/API service to manage processes with billions of connected assets, or a platform to extract real-time data to improve business decisions. With more than 25 years of cellular IoT experience, Sierra Wireless is the global partner customers trust to deliver them their next IoT solution.

For more information, visit www.sierrawireless.com.

Connect with Sierra Wireless on the IoT Blog at http://www.sierrawireless.com/iot-blog, on Twitter at @SierraWireless, on LinkedIn at https://www.linkedin.com/company/sierra-wireless and on YouTube at https://www.youtube.com/SierraWireless.