onBoard™ CONNECTION MANAGER

MULTI-NETWORK, SECURE IP MOBILITY

oCM

THE CHALLENGE

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 onBoard™ Connection Manager (oCM) is a mobile-optimized VPN appliance, providing secure IP mobility and sub-second switching in a multi-network environment. oCM is designed to work with In Motion Technology's onBoard Mobile Gateway (oMG) and onBoard Mobility Manager (oMM). oCM provides security for all connected devices and applications in the oMG's "vehicle area network". Based on IKEv2 Mobile Internet Key Exchange (MOBIKE) standards, oCM eliminates session interruptions when secure IP traffic is switched from one wireless network to another. MOBIKE enables the oMG to establish a secure tunnel over any available wireless network, and as the vehicle moves and network access changes, the oMG can "move the tunnel" to the next best available network. This happens automatically, transparently, and without disruption to the end-user's applications.

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 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.

SIMPLIFY DEPLOYMENT

oCM works with oMGs and oMM and simplifies 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 MOBIKE software running on the oMG secures all vehicle area network traffic in and around the vehicle without the need for special software on client devices, and works with oCM to secure traffic over multiple wide area wireless links. oCM 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 oMG, oCM is a cost effective 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.

KEY FEATURES

Integrated Mobile VPN

Sub-second switching

Multi-network support

Simple to deploy

Client licenses not required

INMOTION
TECHNOLOGY

A **SIERRA** COMPANY
WIRELESS

FEATURE	SPECIFICATION
ROUTING	• IPv4 routing - BGPv4, OSPFv2, RIPv2, Custom Static Routes
IP ADDRESS MANAGEMENT	• Static, DHCP Server, DHCP Client, DHCP Relay, Dynamic DNS, DNS Forwarding
ENCAPSULATION	• Ethernet, 802.1Q VLANs, PPP, IP in IP, GRE
FIREWALL	• Stateful Inspection Firewall • Zone-based Firewall • P2P Filtering • IPv6 Firewalling • Time-based Firewall Rules • ICMP Type Filtering
SECURITY PROTOCOL	• IPsec using Internet Key Exchange (IKEv2) with Mobility and Multi-Homing Extension (MOBIKE)
VPN	• Site to Site (IPsec) • Remote VPN (IPsec)
ENCRYPTION	• DES, 3DES, AES Encryption - 128- and 256-bit • MD5 and SHA-1 Authentication • RSA • Diffie Helman Key Management
QoS POLICIES	• Priority Queuing • Round Robin • Random/Weighted Random • Classful Queuing
HIGH AVAILABILITY	• VRRP • IPsec VPN Clustering • RAID 1
ADMINISTRATION & AUTHENTICATION	• Integrated CLI • SSHv2/SSH Public Key
LOGGING	• Netflow • Syslog • SNMPv2c
HARDWARE	• 19" 1RU rack-mount server appliance. Redundant configuration highly recommended.

DuraTech USA Inc.
A Certified 8(a), SDB, DBE, SBE, MBE, WBE firm.
Phone: (714) 898-2171   Fax: 866-704-9132
Email: sales@DuraTechUSA.com   www.DuraTechUSA.com