

# 4.9 GHz VIDA broadband network delivers guaranteed quality of service with standard protocols to support real-time public safety data applications

Those in public safety have long sought the ability to quickly access real-time data in the wireless environment. Over the past few years, the introduction of broadband distribution technologies that allow the use of greater bandwidth has kindled hope that the day of fast access to real-time data was finally here.

Until now however, those in public safety have had only a limited set of technology choices for broadband data networks. They could choose 802.11/WiFi networks, which work well for non-critical applications such as routine data downloads/uploads and e-mail, but lack the guaranteed quality of service required for any mission critical or real-time applications. Or they could choose proprietary broadband or hybrid mesh-type networks which offer the access and bandwidth they need, but which rely on proprietary protocols, thereby limiting their choices for third-party applications and increasing costs. Broadband networks using proprietary protocols also tend to lock users into a narrow range of future enhancements, with little or no provision for migration.

**“Our solution uses a scheduled protocol and is therefore contention free. Additionally, calls can be prioritized and a specific bandwidth reserved.”**

Gregory Henderson

However, M/A-COM’s 4.9 GHz network means that a new, open-standards solution to critical broadband video, data and VoIP, with data throughput ranging from 4-19 Mbps, is finally available to those in public safety.

“We’ve taken the time to pursue a more flexible, cost-effective path to the still-evolving, standards-based approach to broadband data,” said M/A-COM’s Gregory Henderson, manager, broadband technology. “It’s more cost effective because it’s based on open standards for both the wireless portion of the distribution process and the IP network portion. We strongly believe that the dollars invested in infrastructure today must provide public safety entities with an assured migration path to broadband solutions that are still in the development stage. Specifically, these solutions include full mobility and multimode operation in a standards-based environment.”

## The problem with WiFi for Public Safety

The reason the often-touted WiFi solution isn’t good for public safety applications can best be summed up by a term prevalent in computer networking circles: quality of service (QoS).

As every law enforcement officer knows, some communications must take precedence over others. It makes no difference whether that communication is in the form of voice, data or streaming video from a surveillance camera. For public safety, wireless data requires the ability to prioritize messages and a guaranteed QoS.

Meeting these two primary requirements are what drove the design of M/A-COM’s new wireless broadband distribution network.

M/A-COM’s solution is based on the IEEE 802.16 series of airlink protocols and provides seamless integration of wireless data on a VIDA – or other – IP Network. This solution also operates as a standalone wireless data network

## Why M/A-COM’s solution is better than WiFi and proprietary mesh technologies for public safety

- Guaranteed quality of service and higher security
- Licensed protection of 4.9 GHz public safety band
- Over-the-air throughput from 4 to 19 Mbps
- Based on open, non-proprietary IEEE 802.16 protocol
- Assured migration to future technologies
- Standalone or fully integrated into a VIDA Network

M/A-COM is a principal member of the IEEE WiMAX Forum



WiMAX  
FORUM

for those who have a dedicated application in mind, such as closed-circuit video surveillance.

### New technology but a familiar ring

Interestingly enough, although today's wireless data solutions are based on digital technology, the problems encountered by some of these solutions are achingly familiar.

"It's a bit like voice communications before the days of trunked radio systems," said product manager Craig Moore. "In the old days, when two or more police officers tried to speak at the same time on the same frequency, they couldn't get through. Trunking technology solved that problem by assigning calls to the first available channel. It also allowed for calls to be prioritized, so an emergency call always went to the front of the line."

Now, however, WiFi and some data networks based on proprietary mesh technologies have a problem similar to those old conventional radio systems. These systems use an unscheduled protocol to determine when a client accesses the network. In these wireless unscheduled protocols, as long as the client

does not hear traffic on the channel, it will attempt to transmit its data - there is no way to schedule/coordinate traffic on the channel. When two or more wireless users try to establish a connection with a base station at the same time, they can block each other. In addition, there is no way to reserve or guarantee access for a high priority application/user.

In contrast, M/A-COM's solution uses a scheduled protocol and is therefore contention free. "Every call is scheduled by the base station, eliminating contention. Additionally, calls can be prioritized and a specific bandwidth reserved. When streaming video is required, for example, the wireless 'client' is assigned a specific time slot and bandwidth. This eliminates contention and provides a guaranteed QoS," said Henderson.

In addition to a scheduled protocol, M/A-COM's 4.9 GHz broadband relies on point-to-multipoint distribution architecture rather than a mesh network. "Mesh networks are very flexible and can be set up *ad hoc* as the situation demands. They work fine for general, non-

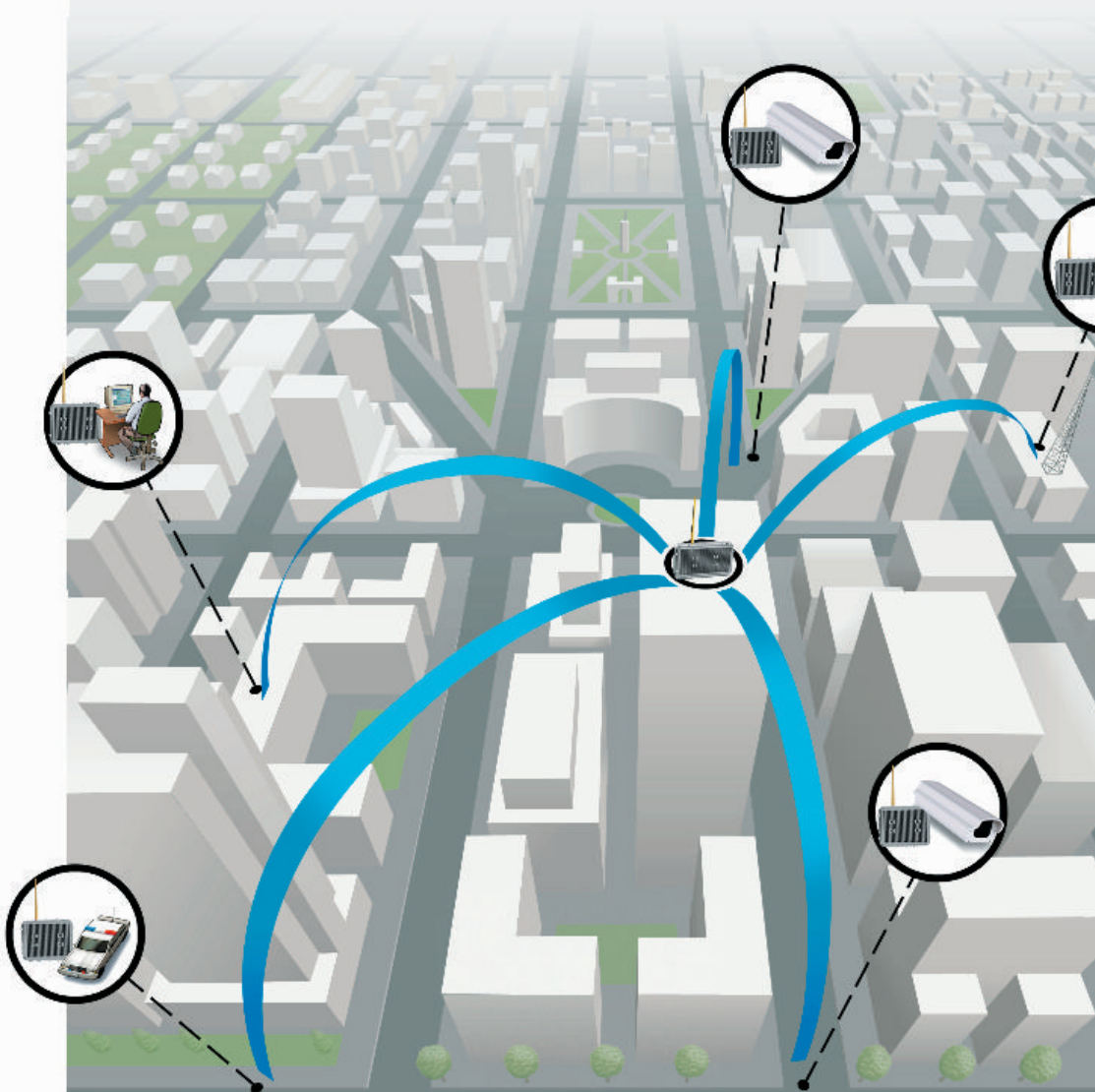
continued →

**"Critical communications... simply must deliver a guaranteed QoS in difficult situations because that is often the times when they are needed most."**

Gregory Henderson

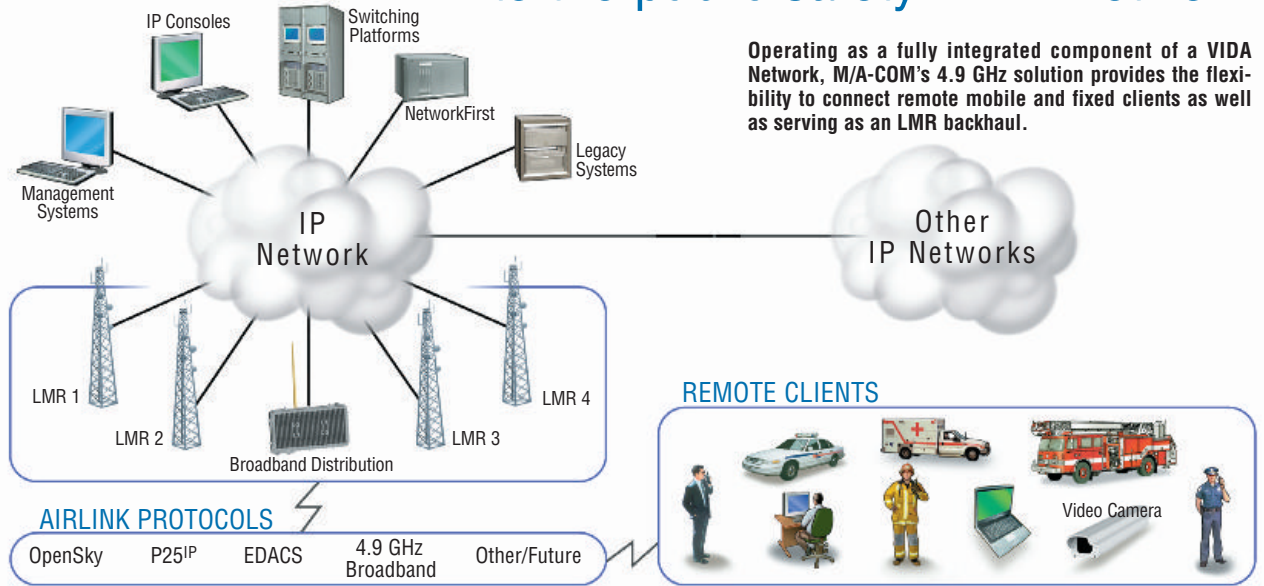
## 4.9 GHz broadband Deployment

A typical M/A-COM 4.9 GHz distribution system deployed in a metro area can employ a mix of both fixed and nomadic clients. In addition to remote data distribution, it provides dedicated and backup LMR backhaul service in place of T1 lines or microwave. The network is easily scalable across a city or region.



-  BASE STATION
-  FIXED CLIENT  
(ex., Video Camera)
-  NOMADIC CLIENT  
(Police Car)
-  FIXED CLIENT  
(Precinct)
-  FIXED CLIENT  
(LMR Backhaul)

# M/A-COM's solution adds broadband data services to the public safety VIDA Network



Operating as a fully integrated component of a VIDA Network, M/A-COM's 4.9 GHz solution provides the flexibility to connect remote mobile and fixed clients as well as serving as an LMR backhaul.

**"It's much harder to sabotage our wireless network because unauthorized users are blocked from being scheduled on the network."**

Gregory Henderson

critical applications. But they compound the contention problem because the data flow must compete for a connection at each 'hop' along the way," said Henderson. "As public safety organizations have learned over the past decade, critical communications are useless if they are rendered inoperable in an emergency. They simply must deliver a guaranteed QoS in difficult situations because that is often the times when they are needed most."

### Less interference, higher security level

Because most of the available wireless data protocols and systems use unlicensed bands (typically 2.4 and 5.8 GHz), every user competes with every other user. In addition, each call is subject to interference caused by other

electronic devices such as wireless phones and home or business wireless networks, which are often prevalent in the urban environments where wireless hotspots are used.

In addition to the guaranteed quality of service, M/ACOM's solution uses the 4.9 GHz band because it is reserved for public safety use and suffers less interference while allowing increased range due to the higher power levels allowed by the FCC. Qualified public safety users don't have to pay to use this band and because it is licensed, there is far less chance of interference from competing wireless devices.

It's important to remember that wireless protocols such as 802.11 (WiFi), and 802-16 (WiMAX), are not frequency dependent. This independence provides greater flexibility, but it

can also be a source of confusion because the same protocol can be used on either licensed or unlicensed bands.

M/ACOM's solution also offers higher security and less susceptibility to what is termed "denial of service" attacks. "An unscheduled protocol is subject to interference caused by too many users. But unscheduled protocols are also vulnerable to a simple denial of service attack, which can be perpetrated by continuously transmitting a weak beacon signal, causing all other clients on

## Video surveillance ideal application

According to Craig Moore, M/A-COM product manager, the 4.9 GHz broadband distribution network is ideal for video surveillance systems deployed for law enforcement and security applications such as at airports, power stations and military installations.

Typically, such systems include a control center application to provide real-time viewing and recording and a number of fixed and controllable video cameras. "We use IP video cameras with embedded MPEG-4 compression from major security camera vendors," says Moore. "The compressed video is then sent back over the 4.9 GHz wireless backhaul to a Network Video Recorder. This is typically located at a 'security center', where the video can be monitored by security personnel and controls used to direct the cameras."

Once a surveillance video system is in place, users with network connectivity, including first responders, can 'see' what is happening in real time simultaneously with security personnel at the security center. The mobile clients can also access the recorded video from the security center.

the network to think the network is busy. It's much harder to sabotage our wireless network because unauthorized users are blocked from being scheduled on the network," Henderson said.

In addition to the inherent resistance to denial of service attacks, the airlink protocol offers "best in class" security, including AES, DES, and/or 3-DES encryption with over-air key management.

### WiMAX Forum helps ensure interoperability

Ensuring interoperability among different manufacturers of the 802.16 protocol is the function of the WiMAX Forum, a non-profit industry group comprised of more than 350 member companies, including M/A-COM.

"Like many technical standards, IEEE 802.16 is broadly written and designed to ensure flexibility without placing undue constraints on technical development. The down-side of this approach is that there is no guarantee that compliant equipment from one manufacturer will interoperate with equipment from another compliant vendor," said Moore.

To correct this, the WiMAX Forum was independently established to promote and certify compatibility and interoperability of broadband wireless products developed in accordance with the 802.16 standard. It's an ongoing process, with the initial profile release (802.16-2004) being optimized for fixed and nomadic applications.

A nomadic client differs from a mobile client in that for the data transfer to take place with a guaranteed quality of service, the client has only limited mobility during the transfer.

"The basic mobile protocol is in development now and scheduled for release in 2007-8," Moore said. "All of our 4.9 GHz systems will be upgradeable to mobile as it becomes available. The advantages of open standards - choice of applications, cost and migration - are vitally important."

### Video a key application

"The current version offering fixed and nomadic service is especially suited for

## Wireless Broadband Terminology

**Airlink protocol:** The data coding and format that allows a connection between elements of a wireless network (WiFi, WiMAX for data; OpenSky, P25<sup>IP</sup>, EDACS voice & data).

**Base Station:** The "server" or host receiver/transmitter in client/server wireless architecture.

**Client:** Remote fixed, mobile or nomadic receiver/transmitter

**Contention:** When two or more unscheduled data calls interfere with each other while attempting to establish a connection with the base station.

**Denial of service:** The act of blocking access to a contention protocol network by continuously transmitting a beacon signal.

**Guaranteed Quality of Service:** Guaranteed bandwidth and connection between client and server.

**LMR backhaul:** Wireline or wireless connection carrying voice & data traffic between LMR sites and dispatch centers (typically microwave or T1).

**Network Administration and Management:** Network management is provided by a browser interface to M/A-COM's Unified Administration System (UAS) or, for limited site deployments, by the base station.

**Scheduled connection:** The recognition and scheduling by a base station of authorized client connections to prevent contention, allow prioritization and guarantee bandwidth.

video surveillance, perimeter control, and mobile command," said Moore. Airports, seaports, railway terminals, military installations and many of the utility distribution and power generation plants are obvious applications for this technology.

"Streaming video, smart cameras and associated control equipment can significantly enhance security through improved video surveillance. Since our solution is based on IP network standards, it is readily scalable across a wide area and is easy to integrate with other elements of the IP network, such as alarm and dispatch functions," notes Moore.

### Guaranteed migration to the future

Users need have no fear that M/A-COM's fixed and nomadic equipment purchased now will in any way limit their ability to add capabilities to their network in the future.

"M/A-COM's long experience in the design and implementation of mobile data - including packet-switched data used in OpenSky and P25<sup>IP</sup> - and the use of M/A-COM's Data Lab to test and optimize applications assures users of the optimum performance and choice of third-party applications. Our solution provides the integrated public safety-grade wireless broadband video and data services required by critical communications users today," Moore said. ■

**"Streaming video, smart cameras and associated control equipment can significantly enhance security through improved video surveillance."**

Craig Moore