SatCom For Net-Centric Warfare June 2011

# MilsatMagazine

## Now published monthly

**Lt. Gen. Tom Sheridan**
**Space & Missile Center**
**Celebrating A Successful Career**

**MILSATMAGAZINE**
**VOL. 4, NO. 4 — JUNE 2011**



## Authors

Darrel Beach
Richard Hart
Hartley Lesser
Rick Lober
Jaime Rubscha
Pattie Waldt

Published monthly by
Satnews Publishers
800 Siesta Way
Sonoma, CA 95476 USA
Phone: (707) 939-9306
Fax: (707) 838-9235


We reserve the right to edit all submitted materials to meet our content guidelines, as well as for grammar and spelling consistency. Articles may be moved to an alternative issue to accommodate publication space requirements or removed due to space restrictions. Submission of content does not constitute acceptance of said material by SatNews Publishers. Edited materials may, or may not, be returned to author and/or company for review prior to publication. The views expressed in our various publications do not necessarily reflect the views or opinions of SatNews Publishers.

# P.SIGS

SPACENET INTEGRATED GOVERNMENT SOLUTIONS

## Mission Critical Communications

Anytime, All-the-Time.

### WARFIGHTER OPERATIONS

Support for voice, video and data applications via fixed or mobile solutions to enable communications among soldiers and commanders on land, at sea or in the air

### COMMS ON THE MOVE (COTM)

Antennas designed to meet the needs of Satcom-On-The-Move (SOTM), military mobile communications, homeland security, search & rescue, asset tracking and other government applications

### CONTINUITY OF OPERATIONS

Satellite-based and other telecom solutions to ensure continuity of operations and help maintain communications in the event of a service disruption

### EMERGENCY RESPONSE

Affordable and flexible emergency communications solutions that deliver assured communications via satellite and other mediums to virtually any location

**Call 866.480.2263 or visit www.spacenetgovernment.com for more information.**

Spacenet Integrated Government Solutions
1750 Old Meadow Road | McLean, VA 22102

# MILSATMAGAZINE — JUNE 2011 — PAYLOAD



A ***United Launch Alliance Atlas V*** rocket carrying the ***Space-Based Infrared System*** (**SBIRS**) satellite for the **United States Air Force** lifted off from **Space Launch Complex-41** at **Cape Canaveral Air Force Station** at 2:10 p.m. EDT on May the 8th. This marked the 50th successful launch for ULA since the company's formation in December of 2006.

This mission was launched aboard an ***Atlas V 401*** vehicle configuration, which includes a 4-meter diameter payload fairing. The booster for this mission was powered by the ***RD AMROSS RD-180*** engine and the ***Centaur*** upper stage was powered by a single **Pratt & Whitney Rocketdyne *RL-10A*** engine.

***SBIRS*** is a consolidated system intended to meet United States infrared space surveillance needs for decades to come. The SBIRS program addresses critical warfighter needs in the areas of missile warning, missile defense and battlespace characterization.

"...departments and agencies shall work jointly to acquire space launch services and hosted payload arrangements that are reliable, responsive to United States Government needs, and cost-effective."

**NATIONAL SPACE POLICY**
June 28, 2010

# OUR POLICY: SPACE DELIVERED

**HOSTING GOVERNMENT PAYLOADS ON COMMERCIAL SATELLITES**

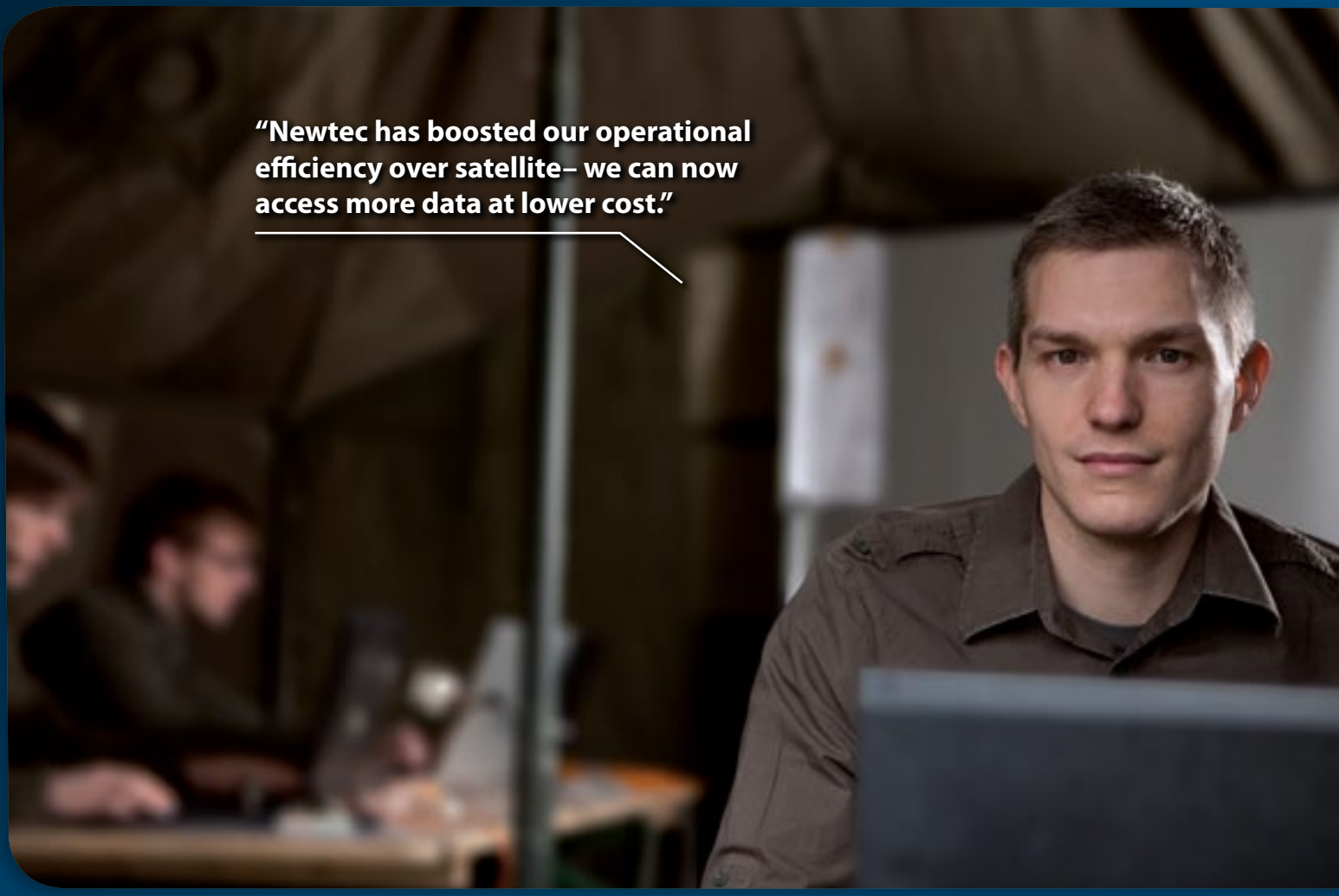
With federal spending cuts hitting, it's never been more important to have an experienced partner who can provide reliable and cost-effective access to space. With a proven track record, regularly scheduled launches and the largest fleet in the satellite industry, Intelsat General is that partner.

Learn how we can put your agency's payloads into geosynchronous orbit while helping you bridge budget and mission gaps. Learn more about our program at www.spacedelivered.com. Join the hosted payload discussion at www.hostedpayload.com

**INTELSAT GENERAL HOSTED PAYLOAD PROGRAM.**
**SPACE DELIVERED.**

INTELSAT.
General Corporation

# MILSATMAGAZINE — JUNE 2011 — ADVERTISER INDEX




# BE READY FOR MORE DATA

The need for failsafe technology. A commitment to uncompromised trust. And above all, ever-increasing bandwidth requirements. If these challenges are driving your organisation forward, then we can help. At Newtec, we firmly believe that more data simply means more opportunity. We design solutions that allow you to get more out of the same bandwidth, increasing your efficiency over satellite. We back this with the proven experience and support you need to cope with the data demands of today...and tomorrow.

***www.newtec.eu***

Newtec

SHAPING THE FUTURE OF SATELLITE COMMUNICATIONS

Belgium | USA | Singapore | Dubai | China | Brazil

www.newtec.eu

# COMMAND CENTER

## LIEUTENANT GENERAL JOHN T. "TOM" SHERIDAN


**Lt. Gen. Sheridan is the Commander of Space and Missile Systems Center, Air Force Space Command, Los Angeles Air Force Base, California. He also manages the research, design, development, acquisition, and sustainment of space and missile systems, launch, command and control, and operational satellite systems.**

**General Sheridan is the *Air Force Program Executive Officer for Space* and oversees the *Air Force Satellite Control Network*; space launch and range programs; the *Space-Based Infrared System Program*; military satellite communication programs; the *Global Positioning System*; intercontinental ballistic missile programs; *Defense Meteorological Satellite Program*; the space superiority system programs; and other emerging transformational space programs. Space and Missile Systems Center was the presitigious *2009 SpotBeam Award* recipient of the *National Security Space Award* for their *Defense Meterological Satellite Program*.**

**General Sheridan graduated from the University of Connecticut in 1973 with a Bachelor of Science in mechanical engineering. He completed the university's Air Force ROTC program as a distinguished graduate. Following an educational delay to earn a Master of Business Administration degree from Bryant College in Rhode Island, he entered active duty in August 1975. His wealth of experience includes acquisition leadership of aircraft, simulator and classified space programs; requirements development across all Air Force space programs; and operational leadership in four different national space programs. He has served as military assistant to the *Assistant Secretary of the Air Force for Space*, Commandant of *Air Command and Staff College*, Director of Requirements at *Headquarters Air Force Space Command*, and as the Deputy Director of the *National Reconnaissance Office*.**

# COMMAND CENTER

## MilsatMagazine (MSM)

***Good day, General. First of all, thank you for your dedicated service to your nation. What led you to seek a career in the U.S.A.F. and into MILSATCOM?***

## General Sheridan

Thanks very much — I'll tell you, it has been an amazing 38 years. It occurred to me the other day that I've been in uniform for more than half of the Air Force's existence. I started my military career as an ROTC cadet at the University of Connecticut. I was looking for a way to serve my country and the Air Force was willing to give me a college scholarship to study engineering — it was a perfect fit. After ROTC, I entered active duty in 1975 when I finished an MBA at Bryant University in Rhode Island. My first seven years of service was in the aircraft development field as an R&D engineer on the AWACS and NATO AWACS programs, both at Hanscom AFB and at NAPMA in Brunssum, Netherlands. Then in October 1982, I was assigned to work for the Secretary of the Air Force - Special Projects at Sunnyvale AFS, which was then the primary satellite ops center for the Air Force. I quickly fell in love with the mission and found my life's passion — MILSATCOM has been a part of it ever since.

## MSM

***You are about to retire from the U.S. Air Force with the distinguished honor of having led the Space and Missile Systems Center, Air Force Space Command, at Los Angeles Air Force Base. Would you please describe your duties to our readers?***

## General Sheridan

I've been very fortunate to lead some of the most talented, dedicated folks in the world. The center has some 5,000 men and women comprised of uniformed military, Air Force civilian, FFRDC personnel, and direct support contractors.

**Lt. Gen. Tom Sheridan, Space and Missile Systems Center commander, checks out a Rose Parade float topped by a GPS satellite model, December 31. (Photo by Lou Hernandez)**

Together we manage an annual budget of $10 billion, where we direct the research, design, development, acquisition, and sustainment of most of our military's satellite, launch, and space command and control systems. This includes mission areas in military satellite communication, missile warning, navigation and timing, space-based weather, space launch and range, space superiority, responsive space, and other emerging evolutionary space programs.

## MSM

***When you where the Deputy Director of the National Reconnaissance Office, what were your responsibilities with that agency?***

## General Sheridan

My role was to assist the Director in managing the critical NRO mission of designing, building, launching, and maintaining America's intelligence and reconnaissance space systems. I was the first military officer to serve as the Deputy Director. This was my fourth assignment to the NRO and a great honor to pave this path for the future. I also served as the commander of the NRO's Air Force Element.

## MSM

***An important aspect of protecting our nation is through the application of resource strategy, especially in regard to spatial resources and MILSATCOM technologies. Do you see such as remaining a high priority mission for our government? At SMC? What other areas do you feel are of crucial importance to safeguarding our warfighters and our citizens?***

## General Sheridan

MILSATCOM has been, and will continue to be, critical to our national security. The recent National Space Policy and the National Security Space Strategy highlighted the importance of space to the interests of our country. The requirements for MILSATCOM capability continue to grow.

Our future space architectures will need to be mission-resilient through many means, such as disaggregated systems providing more affordable satellites and avoiding constellation fragility either due to technical failures or potential hostile actions.

SMC has been developing and fielding space systems for over half a century and will continue to serve as the military space development center of technical excellence. It may sound cliché, but if you look at the big picture, every military space mission area is vital to our national security.

## MSM

***Two areas of concern for both the military/government and commercial arenas revolve around capacity and an educated workforce. How do you see the dire need for capacity being resolved? Are hosted payloads the answer? And how can the U.S.A.F., as well as the other services, encourage young students to follow careers within the STEM environs?***

## General Sheridan

Over the past year, SMC has been actively preparing options for addressing capability gaps to support future decisions. The DoD will undertake studies in FY11 to address capability gaps shortfalls in the mid-term and far-term. The capacity shortfalls will need to be addressed with appropriate investments across the SATCOM enterprise — terminals, ground, and space — and take into account resiliency, affordability, and other factors.

SMC is also currently conducting commercial SATCOM studies with six contractors, including non-traditional suppliers, who are investigating approaches to better utilize commercial SATCOM capabilities, services, and business practices in the future. The study is examining the feasibility and benefits of hosted payloads and commercial type solutions to meet the growing warfighter demand for satellite communications.

Our military and industrial base workforce make up the most talented and dedicated individuals in the world. We need to make sure that the following generations have the skills necessary to meet our future technological demands. I believe the trick to getting our youth excited about science and technology is in the presentation. We have to compete for their attention so we have to make it interesting, motivating and challenging.

# COMMAND CENTER

**Photo to the right...**

**A United Launch Alliance Atlas V rocket with the Air Force's Space Based Infrared Systems (SBIRS) spacecraft at the Space Launch Complex-41 launch pad. SBIRS is designed to provide global, persistent, infrared surveillance capability to meet 21st century demands in mission areas that include missile warning and defense, technical intelligence, and battlespace awareness. (Photo by Pat Corkery, United Launch Alliance.)**

**The SBIRS team is led by the United States Air Force Space and Missile Systems Center's Infrared Space Systems Directorate, located at Los Angeles Air Force Base, California. Lockheed Martin is the SBIRS prime contractor, with Northrop Grumman as the payload integrator. U.S. Air Force Space Command operates the SBIRS system.**

# COMMAND CENTER

## MSM

***What SMC projects are you most proud of commanding and why?***

## General Sheridan

I'm very proud of the work our team is accomplishing in all of our mission areas — they complement each other very well. SMC has had several new programs in work for many years. Over the past two years we have succeeded in completing development and launching four new first-of-a-kind systems into orbit — GPS IIF, AEHF, SBSS, and on 7 May, SBIRS GEO-1. All newly developed systems now have a spacecraft in orbit except for ORS-1, which I expect will launch in late June. The team has worked tremendously hard to achieve this result.

## MSM

***Where do you see MILSATCOM technologies for the military and the government leading over the next couple of years? What are your major concerns regarding our nation's ability to continue the delivery crucial MILSATCOM collected data to commands and warfighters as drawdowns continue and budgets are slashed?***

## General Sheridan

Our dependence upon space has never been greater and that might just go double for MILSATCOM. Our nation simply doesn't go to war in the 21st Century without our space capabilities. AEHF and WGS will each provide 10-times the protected and wideband capabilities of their predecessor programs. They are our workhorses for the near term.

**Team Vandenberg launched a Minotaur IV rocket at 9:41 p.m. Saturday, September 25, 2010, from Space Launch Complex-8 here. The Minotaur IV launched the Space-Based Space Surveillance (SBSS) satellite, a first-of-its-kind satellite that can detect and track orbiting space objects from space.**
**(U.S. Air Force photo/Senior Airman Andrew Lee)**

**Advanced Extremely High Frequency (AEHF) System, image courtesy of Space & Missile Center, L.A.F.B.**

Right now, SMC is actively looking at SATCOM technologies that will address our long-term future needs. We're looking to see what we can do to better and more rapidly deliver capabilities to specific users or geographical areas, thus granting protected connectivity instantaneously to greater segments of users at lower echelons of the force structure.

I believe part of the solution is going to be in developing superior technology that delivers more throughput, but we're also going to need to be efficient in using our available resources and capabilities. We're being asked to do our ever expanding mission with fewer resources. So, we're looking hard at efficiencies; we have to achieve many of these as we proceed. The bottom line is that a system that we cannot afford is not much better than a system that we cannot technologically achieve.

## MSM

***What are your plans after you leave the U.S.A.F. and SMC? Will you be entering the world of commercial SATCOM?***

## General Sheridan

First off, I'll be taking a few months off to just unwind. I owe my wife and family a little more "quality time." After that we'll be starting a new chapter in our lives in Washington, D.C. As I said, Space is my passion, so I wouldn't be surprised if SATCOM becomes some part of my future.

# INTEL

## KEYS TO IMPROVING ON-THE-MOVE COMMUNICATIONS FOR THE WARFIGHTER

**author: Rick Lober, Vice Presdient + General Manager, Defense & Intelligence Systems, Hughes**

Communications-on-the-move (COTM) is vital to U.S. military and intelligence missions at home, abroad, and in theater. Even in a time of leaner budgets, the current threat landscape requires the military to continue advancement of net-centric communications, together with intelligence, surveillance, and reconnaissance (ISR) capabilities. Increased use of satellites is essential to maintain over-the-horizon communications for command and control (C2) and ISR missions, requiring ever more efficient use of high-capacity bandwidth in theater. Faced with these challenges and the reality of tight budget constraints, the military needs to reexamine how to provide the highest quality COTM solutions to troops, while limiting operational costs.

## Bandwidth Efficiency

Many of today's **C2** and **ISR** missions employ COTM solutions with very high data rates. Although appropriate for some missions, C2 functions often only have need for limited data rates, and current technologies may not utilize the excess bandwidth efficiently. By deploying commercial products designed with managed bandwidth technologies, the military can significantly improve its bandwidth efficiency for **COTM** (*Communications-On-The-Move*) terminals. At Hughes, our latest generation commercially developed modems employ technologies to deliver the highest bandwidth efficiency available, while promoting secure and robust networks that meet the unique needs of the military community.

## Antenna Size

Though antenna technology and designs are advancing, today's land mobile COTM versions are still expensive and often cumbersome in the field. As a result, COTM deployments will not see large scale use until antenna cost and size are significantly reduced. Modem technologies that employ advanced modulation and coding schemes can be key to achieving compact and cost-efficient antenna designs. As a case in point, **Hughes** has recently developed several commercial small antenna prototypes currently in field testing that operate with modems employing advanced modulation and forward error correction codes, resulting in greater mobility and much lower cost for both Ku-band and Ka-band COTM solutions.

## Resource Management

The networking needs of warfighters are complex and ever-changing. An operation may begin with an aerial campaign and rapidly switch to a ground attack, requiring different satellite resources. Satellite communications (SatCom) networks must therefore be nimble and responsive to meet these rapidly-changing needs, which requires integrated situational awareness (SA) and dynamic allocation of resources. Many current DoD networks are provisioned based on anticipated demand, meaning commanders must predict the capacity well in advance of operations.

Commercial satellite platforms can provide a model for more efficient capacity management. For example, our commercially successful ***SPACEWAY® 3*** switch-in-the-sky satellite and ground-based *Network Operations Control Center* (**NOCC**) provides Hughes with dynamic resource allocation of 10 Gbps of Ka-band traffic capacity, which can also be combined with terrestrial fixed and/or wireless networking as required to deliver the most bandwidth efficient, combined ground/satellite solutions. Simplified network set-up in tactical situations is powered by the Hughes ***ExpertNMS*** network management software and its highly interactive, user friendly GUI interface, available with our latest VSAT systems. Such a consolidated, end-to-end network management system will transform warfighter COTM whether at home or abroad.

## The Future

Hughes is committed to developing the most advanced and cost efficient COTM solutions to help our military customers maintain over-the-horizon communications anywhere in the world — delivering innovative solutions that stay within budget constraints. The Company looks forward to continuing to work with military partners to enable effective and critical net-centric communications in any mission location or setting.

*About the author*

Rick Lober joined Hughes in late 2008 as the Vice President and General Manager of the Defense and Intelligence Systems Division. He has over 25 years experience with both COTS-based and full MIL communications and intelligence systems starting as a design engineer and progressing to a P&L executive. He has previously worked at Cubic Communications, Inc. and Watkins-Johnson Company and received his BS and MSEE degrees from the University of Illinois,

# FOCUS

# ADVANCEMENTS IN TACTICAL RADIO ACCESSORIES

author: Jaime Rubscha, Product Development Technologies

**Just as in any line of work, effective communication is a *must* within the military. However, unlike most work scenarios, soldiers' ability to communicate effectively can be a matter of life and death. They must be able to relay timely messages through a secure network in order to ensure safety and success.**

While consumer technologies such as cell phones and computers seemingly advance every day, military communication has been moving at a much slower pace. With a more drawn out design cycle and approval process, not to mention information security concerns, military radios and accessories are still evolving, at a pace that is much slower than smart phones and tablet PCs. However, recent advancements in information security and the adaptation of a more commercial business model within the U.S. ***Department of Defense*** (**DoD**), procurement has allowed advanced technologies to be received into the hands of soldiers faster than ever before.

As smart phones and tablet PCs continue to impact the next generation of tech-savvy soldiers, the DoD is working to bring these new technologies into their missions. In previous years, narrow-band radios limited the effectiveness of voice and data sharing — new wideband networks are now allowing all military personnel to see and hear the same information, giving them a clearer picture of what is going on around them. Advanced tactical radios, such as the **Harris *AN/PRC-117G***, provide mobile ad-hoc networked data capabilities down to the soldier level, delivering mission-critical data in the field.

Photo courtesy of Harris Corporation

As these smarter technologies develop, radio accessories are playing an important role in how networked data is shared by various types of military personnel. Different branches and units within the military have their own user-specific needs, creating a wide-variety of accessory options for use with tactical radios. This allows each solider to carry what they need, leaving unnecessary tools aside.

The range of add-ons can be vast — from GPS and soldier-worn cameras to more advanced accessories such as biometric sensors that monitor a soldier's health, or a live UAV feed, viewable via a pair of glasses or even on a wristwatch. With the proper additions, these radios essentially become "wearable computers", allowing for even easier, lighter and more mobile access to information.

When can we expect these ideas to become reality? It is closer than you think. Accessories such as **Android**-based tablets are making their way into units throughout the military. The adoption of more consumer-like accessories has the potential to keep soldiers more informed as well as safer. As soldiers will be familiar with how to operate these devices, such as smart phones, there is a smaller learning curve and less risk for user error. Prototypes are now being unveiled and we could see these more advanced communication methods being tested in the field as early as late summer.

One major concern in recent years has been the exposure of such fragile components to extreme weather environments and terrain — two consistent realities of military life. Designing for rugged environments while keeping up with the latest in technology and user interface simplicity can often be a challenge for defense product development teams. With the recent introduction of the first Android based handsets that match military specifications, such worry is a thing of the past. Newer devices that conform to rigorous government standards combine the tough materials that soldiers rely on with the sleek form factor that they've never experienced before with DoD procured equipment.

Leveraging the Android based platform to bring these capabilities to fruition results in an extremely powerful, technologically advanced system. The U.S. military's embrace of Android has given developers the tools necessary to make applications useful for soldiers, intuitive in stressful situations, and inventive when compared with previous approaches. In the past, most soldiers were stuck with a multitude of devices, each for a separate function. Now they can combine them all into a single unit that fits neatly into their uniforms. The open-standard interface facilitates customizable options and future upgradability through the use of applications and functionality. The result: ***Information dominance on the battlefield***.

Often, accessories are device specific due to the complexity and engineering integration efforts. As development progresses, and more open standard platforms such as Android are used, these information enhancing accessories will continue to enable future capabilities. The military radio will continue to lead the way in in-field defense communications. It's now up to product designers to find ways to expand the radio's capabilities, making the life of a soldier not only easier, but safer.

*About the author*

Jaime Rubscha is Practice Lead for Defense Programs at Product Development Technologies (PDT). Jaime joined the PDT Defense Programs team in November 2010. Most of Jaime's career was spent as a Product Manager for Harris RF Communications, where she was responsible for product line management of the Falcon III manpack software defined tactical radios for both the U.S. Department of Defense and International Government customers. Prior to working in product management, Jaime worked on the Joint Tactical Radio System (JTRS) programs as an electrical engineer. Jaime also gained valuable systems integration experience at TeleCommunication Systems. Jaime was selected for an Engineering Student Internship at BMW in Germany where she generated code and test simulations for the BMW 7 series integration of a fuel cell auxiliary power unit. She holds a Master of Business Administration from the University of Rochester with concentrations in Marketing, Competitive & Organizational Strategy, and Entrepreneurship, and a Bachelor of Science in Electrical Engineering from The Pennsylvania State University.

# INTEL

# CREATING ROBUST MILITARY NETWORKS

author: Darrel Beach, Systems Engineer/Architect, Cisco Systems

**Military organizations need reliable, versatile tactical networks for data, voice, and video communications. However, that goal presents considerable obstacles:**

- ***New software-defined radios allow a single radio to operate with multiple waveforms to provide a wide range of capabilities, depending on frequency, waveform characteristics, and bandwidth, which makes it difficult to establish and maintain IP connectivity***
- ***Radio-based communications can be unreliable, and if routers are not aware of the current condition of each radio, they cannot make effective routing decisions***
- ***Different radios used in military networks use dissimilar connection methods, making it time-consuming to create a network and complex to add new radios to it***
- ***Radios and routers must be able to form ad hoc networks with minimal configuration or changes***

To address these challenges, **Cisco** has introduced the concept of ***Radio Aware Routing*** (**RAR**). Radio Aware Routing optimizes IP routing over diverse radio networks to give users real-time access to critical information while on the move. It provides a standardized way of connecting routers and radios so that using multiple types of radios in a network can potentially be as simple and effective as using off-the-shelf components for wired networks, and video is not disrupted. By abstracting the physical and logical interface of a radio into a form applicable for virtually any type of radio, RAR offers a modular building-block approach for using IP routers over radio networks. Such an approach overcomes many of the underlying problems encountered when using radio-based technologies with IP.

This article describes certain underlying aspects of the Internet's infrastructure, and how the linkage of many diverse networks evolved into what today we know as the Internet. It also discusses advances in mobile networking technologies that build on those fundamentals to make tactical military networks more modular, flexible, and robust.

## Internet Fundamentals

Military data networks are a specialized application of today's enterprise networks. To understand the best way to create a radio-based military network, it is important to review the basics of the Internet and how it was built from many different individual networks. However, there are also important differences between enterprise networks and tactical military networks, which will be discussed later in this article.

Though it did not come into prominence until the 1990s, the Internet has actually existed since the 1970s, arising from **DARPA's** packet-switched ***ARPANET*** military network. From the beginning, these networks were based on a few simple, yet powerful, concepts that are still imperative today.

### — *IP Addresses*

The most fundamental concept within the IP suite is the simple fact that everything that connects to the Internet gets an IP address. It is a simple idea, but one whose power cannot be overstated. Today, the Internet has become so ubiquitous that virtually any device — from cell phones and PDAs to high-tech refrigerators — can be assigned an IP address and then connect to it.

The concept of endpoint addresses did not originate with the Internet. Such addresses, using a variety of formats, are found in many of the underlying networks that form the Internet, such as **SONET**, **ATM**, **Ethernet**, **X.25**, and so on. Each of those technologies was designed to address a specific communications need, so they vary in speed, physical connection methods, and how two endpoints communicate with each other. But the concept of endpoints (computers or other devices) having addresses is consistent across these technologies.

Because the address format used by any of these network technologies is unique to that specific technology, complications arose when you wanted to connect multiple types of networks. For example, how could a computer using an Ethernet address share information with one using an ATM address? The disparate addressing schemes of those standalone network technologies therefore limited their communications ability.

This was the underlying problem that the Internet Protocol was designed to solve. It provides a universal address format, along with a method for allocating addresses to all endpoints on all networks that are connected together using this protocol. The overlay of IP addresses allows these diverse networks to participate in the global Internet. The Internet Protocol ensures that all addresses on a given network are related — an essential aspect of how the Internet operates. For example, imagine two network devices with IP addresses of 10.1.249.10 and 10.1.249.13. Of the four octets of their 32-bit addresses, the first three are identical. From that, we can tell that these two devices are on the same subnet.

This structure of IP addresses is a critical point, as it tells us to which individual network — among the many hundreds of thousands that form the Internet — a certain device is connected, simply by looking at the beginning of its IP address. This architecture is analogous to getting an idea of where a telephone number is located by reading its area code.

***—Internet Routers***

So far, we have seen how the Internet Protocol established the ability to form large Internetworks from smaller diverse networks by assigning a unique address to any device on any of the component networks. This mechanism formed an overlay of IP addresses, and IP became the protocol that connected these diverse networks. But how do devices actually communicate across an Internetwork?

The fundamental building block of the "*network of networks*" now known as the Internet, is a device called an IP router. Essentially, a router connects two or more individual networks so that they can exchange data packets using the Internet Protocol. Multiply this basic architecture hundreds of thousands of times, and you get the Internet as it exists today. Routers are devices that support many different network protocols. They can therefore be used to connect different types of networks, using IP and a common language.

The basic concept of IP routing is depicted in *Figure 1*. Computers, or other endpoint devices, connected to one of the individual networks communicate with other endpoints by transmitting and receiving packets of data formatted according to the Internet Protocol. Each packet of data contains the IP addresses of both its source and destination, so the packet can find its way independently through the connected networks to reach its destination. This is a tremendously powerful concept with great benefits for radio-based networks, with their unpredictable connectivity.

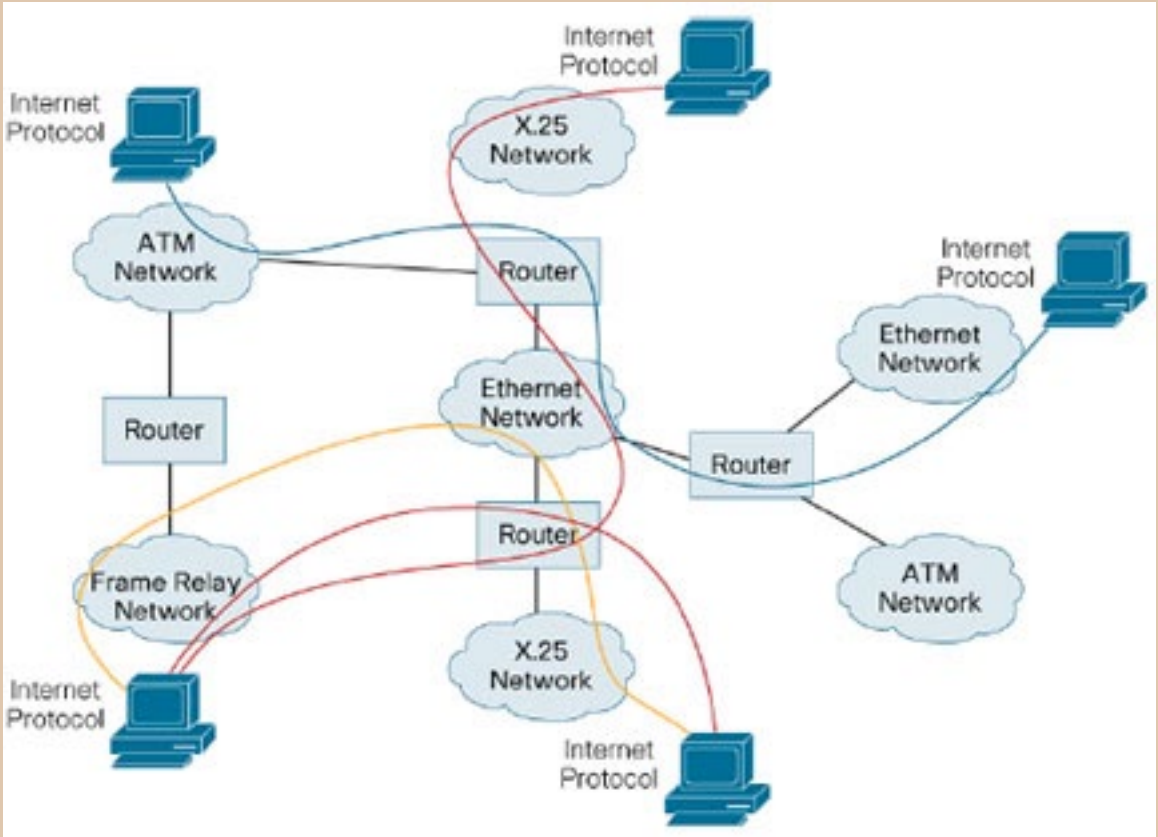



**Figure 1. Internet Structure**

Of course, how a packet finds its way is not a simple matter. Most aspects of its journey are relatively straightforward, but the number of different factors that must work properly, and the sheer number of devices involved, make the total picture more complicated. Suffice it to say that the Internet operates because routers know how to route IP packets from their source to their destination across all of the intervening individual networks. The key technology, and hence, the heart of the Internet is IP routing.

| Computer | IP Addres | Local Network Address |
|---|---|---|
| Computer 2 | 171.1.1.12 | MAC-C |
| Computer 3 | 171.1.1.13 | MAC-D |
| Computer 4 | 171.1.1.14 | MAC-E |
| Computer 5 | 171.1.1.15 | MAC-F |
| Router | 171.1.1.1 | MAC-A |

**Table 1.**

At this point, it is helpful to review what happens in an endpoint that is attempting to communicate using the Internet Protocol. First, the computer (or other device) has to establish its own IP address. As mentioned earlier, an IP address is a 32-bit binary value; it is typically written in "dotted decimal" notation (such as 172.1.1.1) for easier understanding by humans. Remember that one benefit of the IP addressing scheme is the ability to determine on which specific network (among the hundreds of thousands that exist) any given IP address is located. This is accomplished by giving all the computers connected to a single physical network the same IP address prefix. It becomes the function of the routers to understand where all the prefixes are located within the structure of the Internetwork.

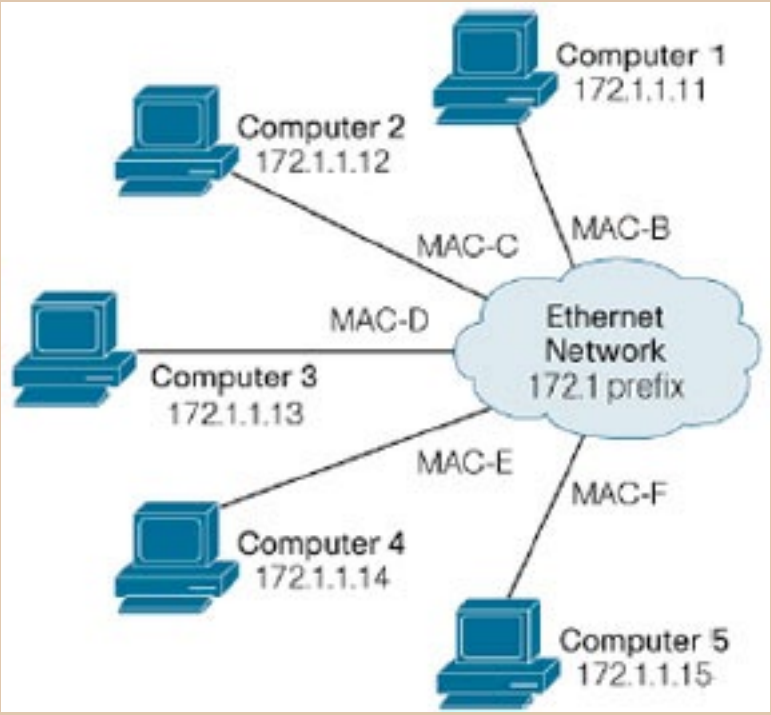



**Figure 2. A Simple Individual IP Network**

*Figure 2* shows the simple example of a single physical Ethernet network with five computers and a router. These days, even many homes have similar networks, with a couple of home computers, a network-attached printer, and a cable modem that acts as a router to the rest of the Internet. In our example, everything connected to this small network has a prefix of 171.1.1.x, with the fourth value in the address being the unique identifier for each endpoint device.

In order for everything to work properly, there are three pieces of information that absolutely must be configured into each computer connected to this network: its own IP address, a number known as a network mask, and the IP address of the "default router" that connects this network to other networks.

Every IP packet has a source address and a destination address that allows each packet of information to be routed individually from the source to the destination. Recall that for any given type of physical network (such as Ethernet, ATM, or X.25), there is some form of address that is usually very different from an IP address. Figure 2 shows a small Ethernet as an example, so every attached computer has a 48-bit Ethernet MAC address. MAC addresses are quite lengthy, so for simplicity, they are shown in *Figure 2* as simply MAC-A through MAC-F.

The local addressing mechanism is an attribute of each type of network, so the form and specifics are different across different network technologies. Therefore, there needs to be a way of correlating a computer's IP address to its local network address. Each type of network has a different way of doing this. In the case of Ethernet, each computer keeps an internal table that lists both the MAC address and the associated IP address. In the

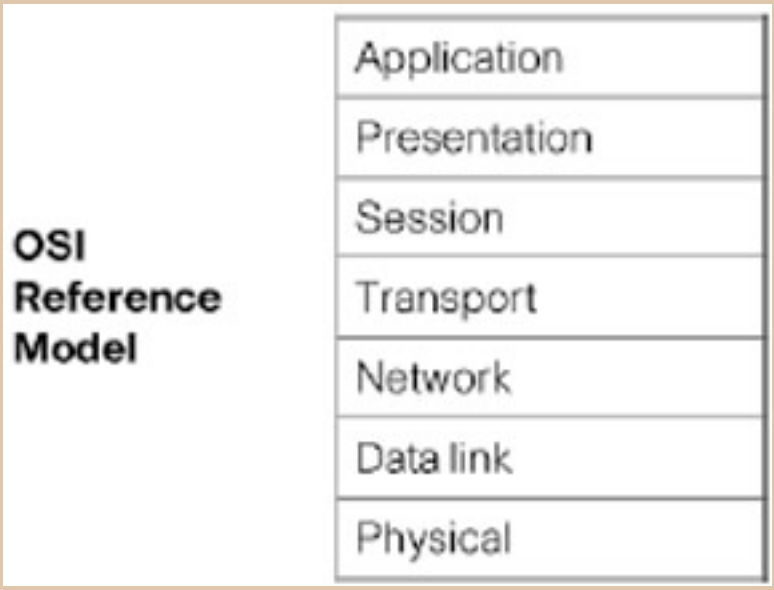



**Figure 3. The OSI Reference Model**

simple example shown in *Figure 2*, Computer 1 would have a table something similar to the one show at the top of the next column.

With that information, Computer 1 can communicate directly with any other computer on its local Ethernet network. However, it must communicate with computers on other networks only by sending packets through the router.

This is where the network mask and default router configurations come into play. The network mask is a number that helps network devices determine whether a destination IP address is on the local network, or whether it is only reachable via a router. If the latter, then the device must know the address of its default router. With these pieces of information, network devices can properly send their traffic either directly to other local devices, or to the appropriate router for remote delivery.

***—Network Layers***

The concepts of mapping addresses (IP to local network) and routing between networks are as fundamental to running the Internet as electricity is to running the appliances in your home. Yet mapping and routing are invisible when you use the Internet, just as the flow of electricity is invisible when you plug in your alarm clock. Nonetheless, those underlying details have vital implications for how devices interconnect to construct an internetwork, which applications can run on those devices, and how well those applications perform.

The interface between a physical network device (such as a computer) and a network consists of special software protocols. The protocols that carry the actual data are implemented on top of the physical interface protocols required for the specific type of network being used. A formal breakdown of these virtual layers can be seen in a protocol reference model, such as the OSI Reference Model shown in *Figure 3*.

The ***ARPANET Reference Model*** (**ARM**), sometimes called the ***DoD Reference Model***, is the forerunner of the OSI Model — and the protocol reference model that bears directly on the formation of the Internet. ARM is described in *Figure 4*.

The OSI Reference Model did not contain a separate layer for Internetworking, which led to the confusion of using the term "network" for both standalone and interconnected networks. When looking at the ARM, "network" and "Internetwork" are clearly two separate layers, and therefore there must be a defined relationship between them. The Internetwork layer was, in fact, meant to be the Internet Protocol. So, for example, an Internet-connected Ethernet network would map IP (Internetwork) addresses to MAC (network) addresses.

There are other details of any underlying network technology that can affect the way things need to happen at the IP layer. For instance, some network technologies (including Ethernet) can send a single packet and have every connected computer receive it; this is called "broadcast" or "multicast" networking. Other networks, such as those using X.25 protocols, might require a packet to be sent individually to every attached computer.

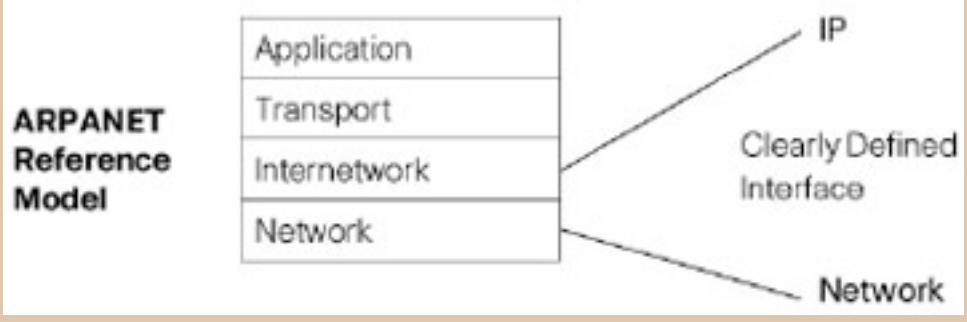



**Figure 4. The ARPANET Reference Model**

These underlying attributes for any given network are important when it comes to configuring routers to talk with each other — and keeping routers working is essential to keeping the Internet running. In radio-based networks, the underlying characteristics and capabilities of the radio network can have a tremendous impact on how the Internet Protocol should operate.

***—Radio-Based IP Networks***

What do those essential aspects of the Internet — diverse underlying networks, unique IP addresses, routers, and network layers — have to do with tactical military networks?

In the ARPANET Reference Model, the details of the relationship between IP and the underlying network are defined in what are termed "Requests for Comment." RFCs are essentially the designated standards for how things must operate and behave when using the Internet protocols. Today, these Internet standards are so well defined that you can purchase practically any commercial, off-the-shelf router and use it to connect almost any combination of networks.

All of the different implementations of IP, as well as many of the underlying routing protocols, have been vigorously tested throughout the decades of the Internet's existence. We now take it for granted that routers and other devices can be purchased from a number of companies, connect to the same type of network the same way, and exchange information correctly. This compatibility was certainly not the case in the early days of the Internet build-out, and it is still a challenge in creating radio-based networks today.

The protocols used by Internet routers to exchange information about the connections between networks are also well defined. Routers understand the specific attributes of each network, such as its bandwidth, its delay times, and whether it is multicast/broadcast capable. They take that information into consideration when deciding how to route each packet to its destination, because being able to accurately and efficiently get packets to their destinations is what has made the Internet a staple of everyday life.

Now, we want to extend that proven architecture to a more challenging environment: **Tactical military networks**. That means we must deal with the vagaries of wireless (radio-based) networks. Range, signal strength, type of antenna, and other attributes of radio systems can vary widely. To make the situation even more difficult, military radios are constantly changing their location. They may go in and out of a network because they are in a vehicle that goes behind a building, or in an aircraft that changes heading. All of these factors add complexity at the Internetwork layer, because the routers must be able to account for the problems introduced by the underlying radio networks.

Even so, all of the previous concepts still apply. A network can be built around a common set of radios using the same waveform. There can be many simultaneous radio networks of different types that must be interconnected. The Internet Protocol is still the unifying force being used to build an internetwork from the underlying radio networks. In effect, tactical networks form an Internet built over radio networks in much the same way the original Internetwork was built over wired network technologies. The key differences are in the underlying operation of the radio networks, which must be taken in account within IP routing functions.

***—MANETs***

One of the most common terms in the realm of radio-based and mobile networking is *mobile ad hoc network*, or **MANET**. Recall that the term "network" can refer to a single instance of a network, or to a broader Internetwork. In mobile radio networking, it has both meanings. A single MANET consists of radios that can exchange data over a certain geographic area. They could be relatively short-range radios, or **BLOS** (*beyond line-of-sight*) radios with ranges of hundreds of miles. They could even use satellites to relay their signals. The details of each type of radio network may vary, but many of the underlying concepts are the same.

The underlying radio network must support an ad hoc capability in which radios can change in relation to each other, and can enter or leave the radio network. This is, in fact, a form of MANET that is operating at the radio network layer. This is a separate function from the idea of ad hoc IP routing, which also must occur. In fact, once a given radio comes into a radio network and stabilizes, the router using the radio must become part of the interconnected set of IP routers. Both functions will have to operate in an ad hoc manner.

The focus of Radio Aware Routing is to provide a mechanism for routers to connect and exchange information over radio paths and be able to obtain information about the radio links. Such detailed information about the links between radios will allow the IP routing

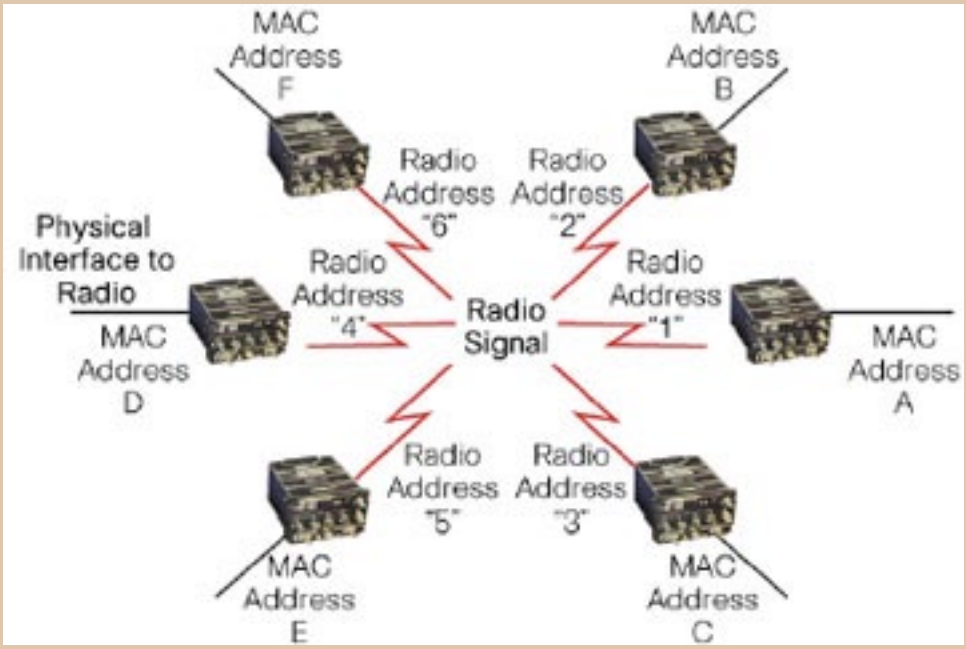



**Figure 5. A Simple Radio Network**

to select the optimal paths, and enable more rapid convergence of IP routing due to any changes in the underlying radio network.

Radio Aware Routing is a broad concept that includes a number of areas. Foremost, is the development of the capability for routers to exchange crucial information with radios. This includes having standards for both the physical interface between a router and a radio, as well as the information to exchange and how it should be exchanged. It also includes a capability for a router to understand at least some minimal information about the underlying radio links even if a particular type of radio doesn't cooperate in the exchange of RAR information. From a modularity standpoint, it is beneficial to have as few physical interface types as possible. It is also desirable to have a set of information-exchange protocols that enable a router to discover information about the underlying radio network. By having such standardized mechanisms in place, it becomes possible to take almost any type of radio, connect it to a router, and have the router optimize the relationship between the radio network and the IP routing layer.

The addressing schemes used in different radio networks will vary, just as they do across different wired networking technologies such as X.25, ATM, and Ethernet. For example, a radio with a broadcast (omnidirectional) antenna may simply use an existing addressing method, such as Ethernet MAC addresses. Other types of radio networks may use something as simple as an 8-bit identifier for each radio terminal. One can also layer addressing schemes on top of each other, which already happens with most networks that transport IP traffic.

An example will help illustrate these concepts. If each radio gets a unique 8-bit address, you could have up to 255 radios on a single network. Let's assume that the radios are omnidirectional and can therefore broadcast information to all other radios in range. A simple representation of this notional radio network is shown in *Figure 5*.

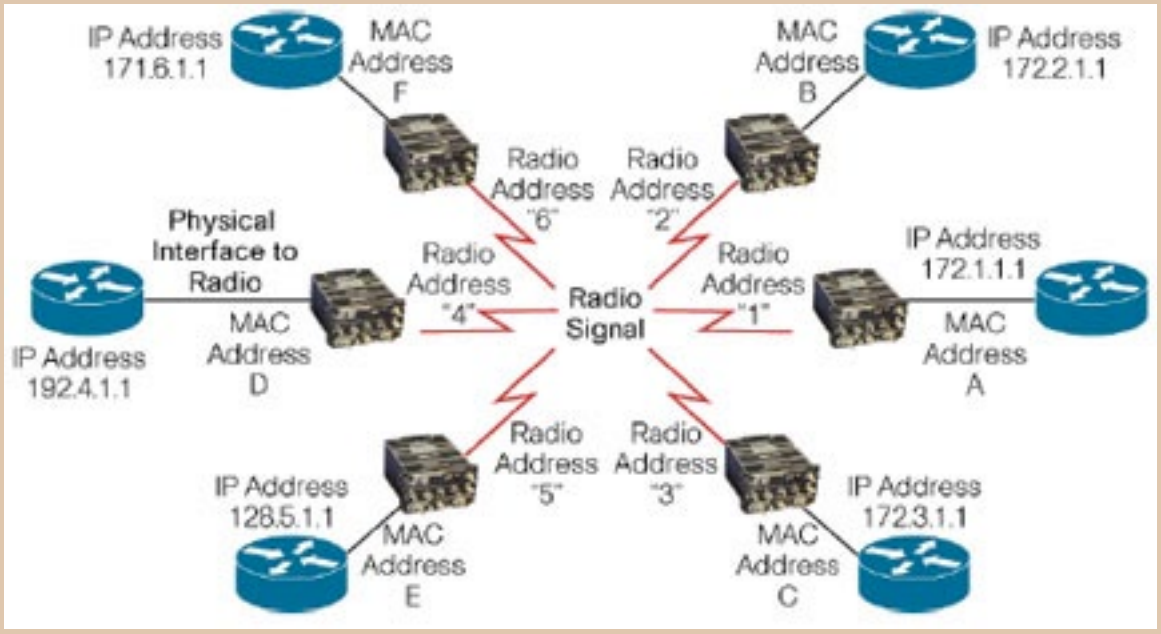



**Figure 6. Radio Network with Internet Routers**

In this example, every radio has an individual address, numbered 1 through 6. The diagram also shows that there must be some type of physical interface to the computers (or other endpoint devices) that will use the radios to exchange data. If a new radio comes into range of this group, it must be able to join the network and begin exchanging data with the

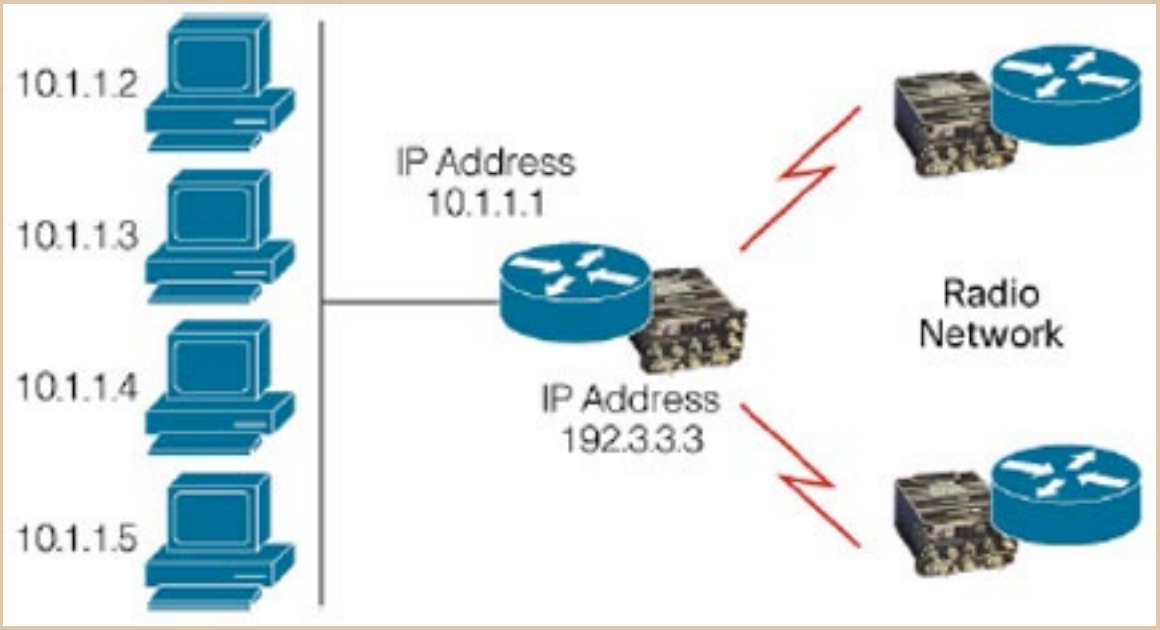



**Figure 7. Multiple End Devices Sharing A Radio/Router**

other radios. Having this occur without manual intervention or reconfiguration of the radios is a form of MANET operating at the network layer of the ARPANET Reference Model.

In this example, the physical interface is Ethernet, and as we know, every Ethernet device must have a 48-bit MAC address. In essence, this example makes the radio network look like a single Ethernet segment. The radios would keep track of the MAC addresses that are reachable through each 8-bit radio address. To add the Internet Protocol to this example, let's connect a router to each radio, as shown in *Figure 6*.

***—Radio Aware Routing***

Now that we have a router behind each radio, we can expand this network to a MANET that uses the Internetwork layer of the ARPANET Reference Model. In the example in *Figure 6*, only routers are connected to the radio network; individual computer systems are on other networks behind the routers. All of the end systems connecting through the routers operate just as they would over any IP network; they are not aware that their communications are being carried over radios. However, the routers need to take into consideration the aspects of radio networks that are different from wired network technologies. In other words, we need to implement Radio Aware Routing.

We mentioned earlier that all IP devices on a single network typically have the same IP address prefix. That organization allows any device on the internetwork to determine whether it is directly connected to a specific destination device, or whether it must use a router to reach that destination. However, the IP addresses assigned to the routers in *Figure 6* do not have a common prefix. This is an attribute necessary for having ad hoc networking capability at the Internetwork layer — the ability for radio-connected devices to join and leave networks without manual intervention.

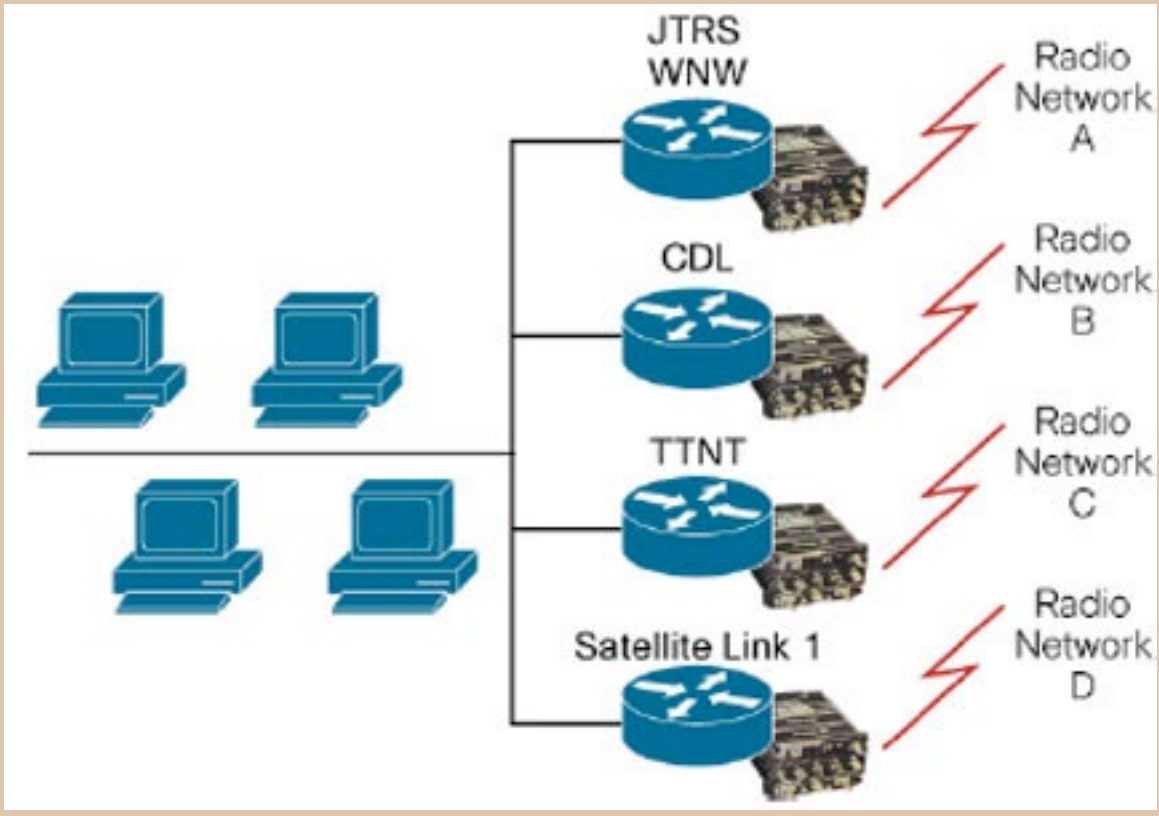



**Figure 8. End Systems With Multiple Radio Types**

Therefore, routers have to operate differently when they are on a radio network than when they are on a traditional network. The specifics of the underlying network will determine exactly what accommodations the routers must make, but there will also be commonalities among radio networks that allow for some degree of standardization.

The diagram in *Figure 6* shows several layers of address mapping that must occur, as well as two layers of MANET. Each radio must recognize other radios that have MAC addresses. When a new radio enters the network or leaves the network (perhaps because its antenna has become obscured), it is beneficial for the radio to notify the router. This allows the IP-layer MANET (or routing protocol in use by the router) to operate on nearly the same timescale as the radio-layer MANET being used in the underlying radio network.

This optimized information exchange along with standardized interfaces is the key functionality provided by RAR. By abstracting the details of the underlying radio networks to a standard set of interfaces, it makes it possible to change the routing and radio functions independently of each other.

There are many other issues to resolve in building radio networks: transiting multiple radios between endpoints, multicast distribution, disruption-tolerant networking paradigms, and long-delay paths, to name a few. But the importance of RAR is in laying the foundation to integrate the two key building blocks: Radios and IP routers.

The trend in radio networking is to actually embed the router within the radio. Whether the router is implemented in software or via a card inside the radio, the result is the same as far as external devices are concerned. The details of how the router interacts with the radio network are completely hidden to them. However, difficulties can arise if communications between the router and the radio are proprietary or nonstandard, as we will discuss shortly.

## End Systems + Routers

As mentioned earlier, each end device on an IP network requires three pieces of information to function: Its own IP address, a network mask, and a default router. In *Figure 7*, all of the computers connect to each other and to the radio via Ethernet. This physical interface and network type is very well understood,

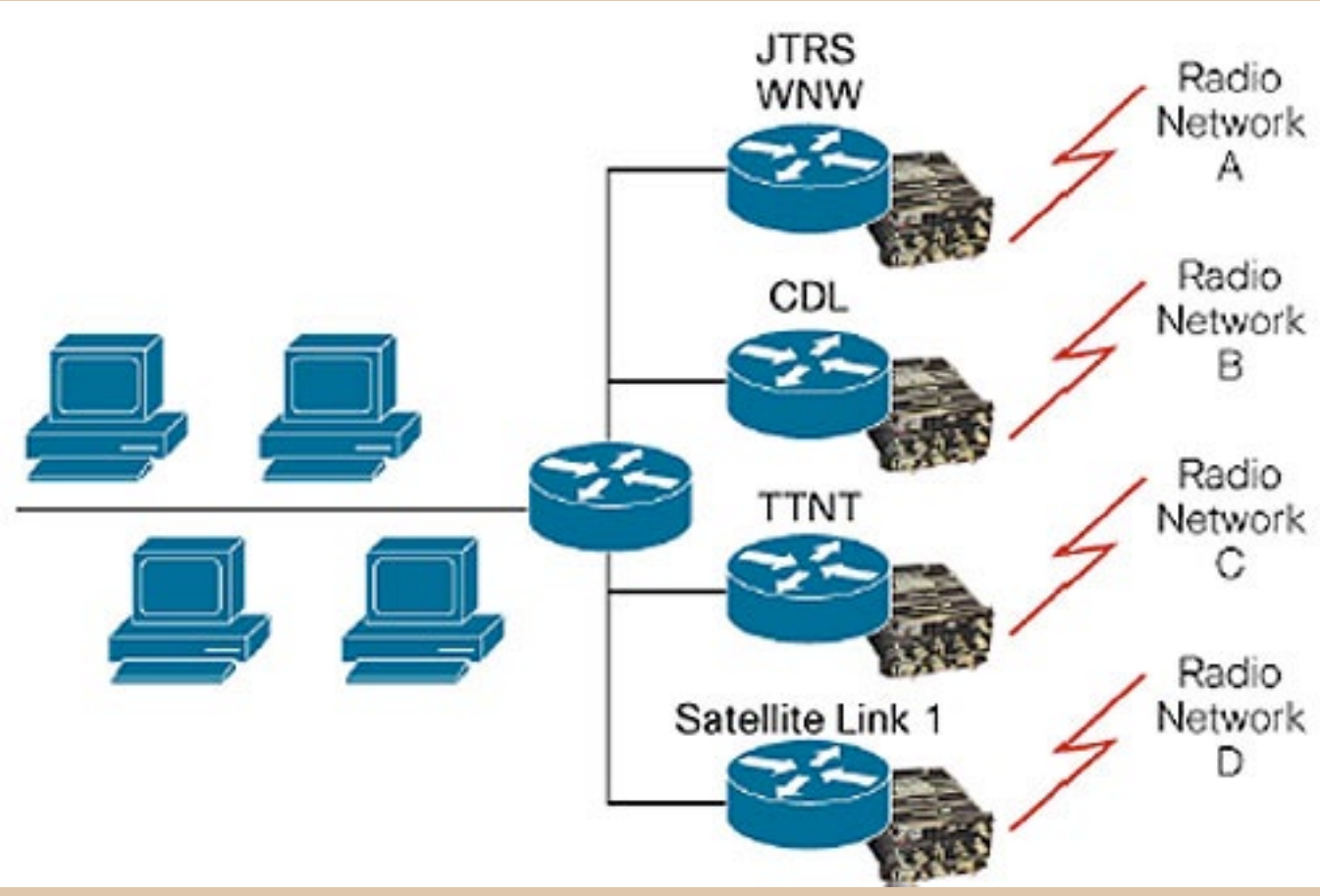



**Figure 9. End Systems With Dedicated Aggregation Router**

is inexpensive, and supports data transfer speeds of a gigabit per second and beyond, all of which makes Ethernet a popular choice.

In *Figure 7*, all of the computers use the router embedded in the radio as their default router. As long as the routers using the radio network implement the necessary ad hoc routing, this example can work just fine. However, in a typical tactical scenario, such a simple topology with a single type of radio will rarely exist. More commonly, a tactical network would require the use of multiple types of radios, as demonstrated in *Figure 8*.

To add to the complexity of this scenario, a vehicle, aircraft, or ship would typically have several different radio paths, all differing in bandwidth, delay, range, and the attributes they present to connected routers. In such a dynamic situation, how do attached devices determine which of the available routers should be their default path to the internetwork? And how do the routers — which may be from different manufacturers and employ different types of both network and internetwork MANETs on their radio networks — communicate with each other across their Ethernet connection? Both issues must be addressed to create an IP-based tactical internetwork. The most straightforward method currently used is to add another router just for the endpoint devices, as shown in *Figure 9*.

Adding this one router simplifies the configuration of the network attached computers. They now use the aggregation router's IP address as their default router, and send all non-local traffic to it for forwarding. This router can also be configured to exchange routing information with each of the radio routers, creating a single overall view of the tactical network's topology. However, we still need to establish a way for the aggregation router and the radio routers to exchange routing information.

This exchange of routing information is dependent on the capabilities and features in each connected radio and router. A specific configuration is usually required for each device. This design also isolates the aggregation router — which is being used by all of the attached devices — from any direct information about the underlying radio networks. This approach causes delay between the

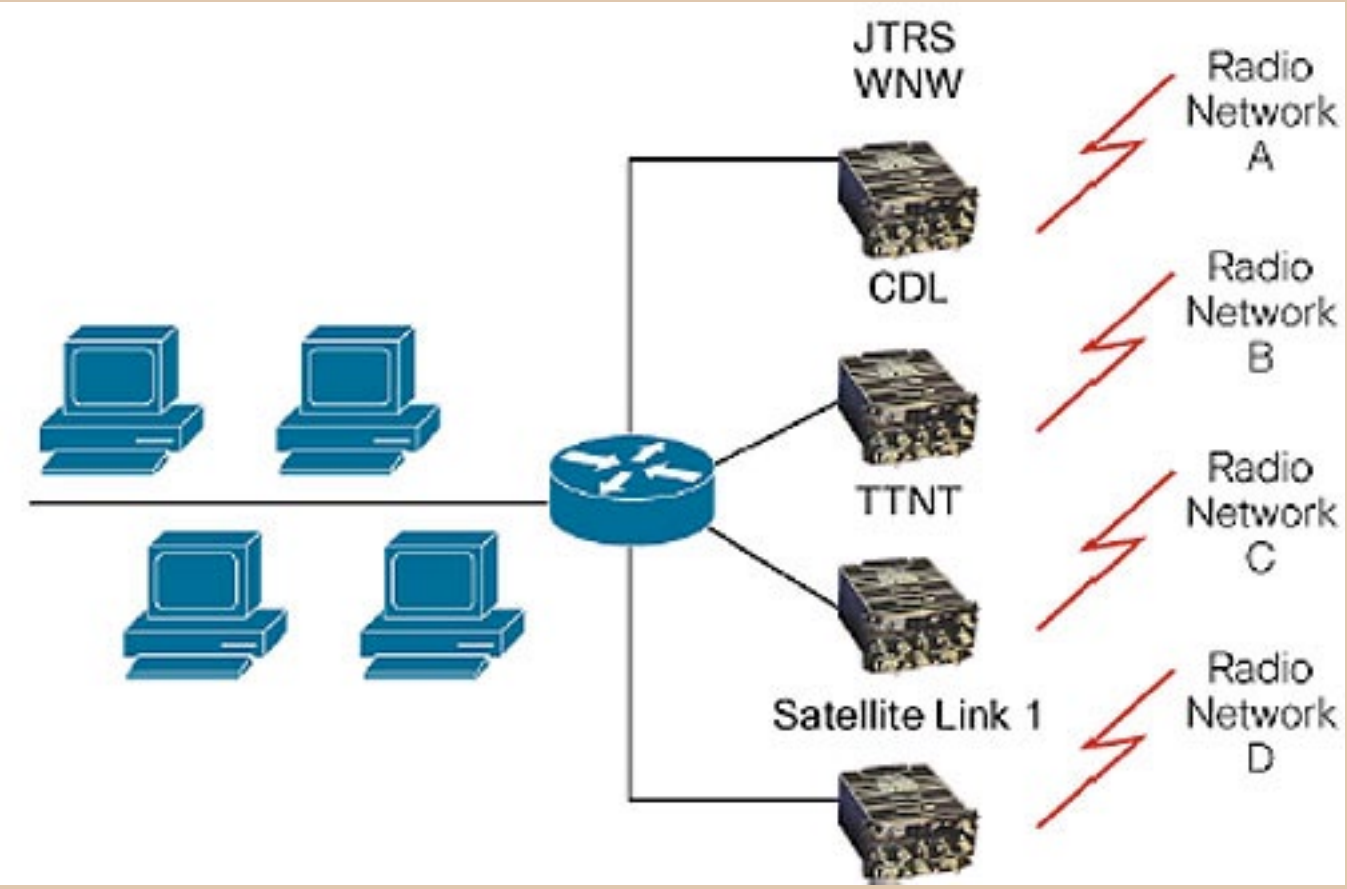



**Figure 10. Standard Router To Radio Interfaces**

loss of a router in an underlying radio network and the ability of the aggregation router to reroute the IP traffic. Additionally, there will be delays in the aggregation router discovering changes in bandwidth or other radio network attributes.

## The Promise of Radio Aware Routing

Whether routers are external to or embedded in radios, they still need some method of interacting with the underlying radio network. With current technologies, the method used depends on the kind of router and radio being used. Suppose, however, that we were to define a standard method for the radios and routers to interact. Information from the radio network (such as bandwidth, delay, and even whether a new radio has joined the network) could then be communicated to the router using a protocol designed for that exact purpose. Due to the very wide range of radios available and their underlying capabilities, there is, in fact, a need for a family or least a range of protocols for such information exchange. Having this set of standards, the network pictured in *Figure 9* would be transformed into the one shown in *Figure 10*.

At first glance, this may seem like a simple change, but its effects would be profound. All attached computers would operate just as they do on the Internet today, unaware that some of their traffic is being carried over a radio network. On the radio side, it would become easy to add additional radio networks. As a result, such a system would offer both the robustness and versatility that tactical military networks demand.

To make such an integrated system feasible, new types of radios would have to support the selected method of exchanging information between the radio network and the router. Any new radio could then immediately connect to any router, without the need for developing yet more proprietary communications software. Reaching a point where building tactical Internetworks based on military or commercially available data radio systems becomes as straightforward as creating new segments of the Internet will ultimately depend on two factors:

- Standardizing on a single physical interface (or at least, a limited set of interfaces) between routers and radios
- Having a standardized protocol for exchanging information between routers and radios

What sorts of information would need to be included in those standards? Consider Ethernet being chosen as the physical interconnection. Ethernet is prevalent, it is inexpensive, and it can cover almost any range of bandwidth. But if the router connects to a radio via a 100-Mbps Ethernet connection, and the radio is only capable of transmitting at 3 Mbps, then there needs to be a way for the radio to inform the router that the actual bandwidth of the link is only 3 Mbps.

Another example occurs in the case of a radio network where each radio can keep track of every other radio on the network, such as with TDMA networks. When a new radio-based router joins the network, it's vital to have a method of notifying every other router about its availability, so that they can immediately begin exchanging routing information with it. This one simple step of proactive notification can have a tremendous impact on how quickly end devices are able to take advantage of the new router.

## Conclusion

Only by choosing which underlying mechanisms to standardize and taking action on that decision can we create a level of connectivity within tactical military Internetworks that we take for granted in the public Internet. Standardization is the core of the Radio Aware Routing concept. It will make it possible to build radio-based networks modularly, just as the Internet is built from a standard set of wired devices and protocols. Any approach that does not include such standardization could actually push the complexity of building a tactical network beyond what is attainable.

All of the underlying principles discussed in this article are being used at this very moment on the Internet. The goal for mobile military networks must be to find the best way to leverage those existing technologies, while adding the necessary radio and satellite wireless capabilities.

To that end, **Cisco** has published **RFC 5578**, which sets out an extension to the *Point-to-Point over Ethernet* (**PPPoE**) protocol that will improve the performance of PPPoE over media that have variable bandwidth and limited buffering, such as mobile radio links. Essentially, the extension allows a radio to tell a router what it sees in the RF environment around it, allowing the router to make more intelligent decisions about how to keep network traffic flowing quickly and efficiently. In addition, changes to IP routing protocols, such as Open Shortest Path First Version 3 (OSPFv3), are being made to use information about underlying radio networks more effectively, and to operate in ad-hoc fashion, thus forming an IP MANET over the radio networks.

The advent of software-defined radios marks a key milestone in the evolution of radio networks. A single radio hardware implementation can, by virtue of software, function as many different types of radios. It may operate in some situations where there is only the one radio, or in other circumstances where there are many radios being used to build a complex radio-based internetwork. Implementing Radio Aware Routing as part of the software-defined radio enables a building-block approach with a well-defined set of standards for building IP-based networks over radio systems. With RAR, changing the functionality of the software-based radio will automatically modify the functionality of IP routing.

Cisco continues to research networking technologies that will make Radio Aware Routing a reality. Working with vendors who are willing to implement the necessary hardware interfaces and software protocols, we foresee solutions that will benefit not only military users, but any group that needs reliable, versatile mobile networks. For More Information Learn more about Radio Aware Routing and other Cisco® solutions for military networks by visiting the following websites:

*Cisco Government Solutions*

*Cisco Defense Solutions*

*Cisco Mobile Government Solutions Radio Aware Routing demonstration video*

*The Future of Ad Hoc Mobility*

*About the author*

Darrel Beach is an Electrical Engineer who has been a Systems Engineer/Architect with Cisco Systems for the last 15 years. He has worked within the DoD on a wide variety of network technology deployments, including Enterprise, Wireless, ATM, Optical, Base Area and Wide Area networks, including Tactical Networks. Prior to joining Cisco Systems, he served 5 years Active Duty in the Air Force where he was involved in designing and deploying the original Defense Data Network and the initial phases of the DISN/AFIN. After active duty service he worked for 5 years as an Air Force Civilian employee continuing work on the DISN and the Air Force deployment of the Air Force Internet (AFIN). He joined Cisco in 1996. He has over 25 years of experience in designing and deploying IP based networks and service delivery technologies.

# FOCUS

## BRINGING FAMILY + STAR INTERACTIONS TO SOLDIERS

**For MTN Government Services (MTNGS), this is a task that inspires mega-wattage star appeal: The company has launched a communications system for a cause that connects soldiers to a top-tier lineup of pro jock athletes who include future NBA Hall-of-Famer *Shaquille O'Neal*; Indy 500 winner and IRL champion *Dan Weldon,* and boxing legend *Evander Holyfield*. As a result, MTNGS is supplying its tech know-how at the nation's top arenas and stadiums, for marquee events such as the *Indy 500*, the *Super Bowl,* and the *MLB/NBA* all-star games.**

The cause itself? ***Pro vs. GI Joe***, a Fairfax, Virginia-based non-profit, connects the men and women serving in the Armed Forces to professional athletes to take part in online video game competitions. So far, Pro vs. GI Joe has connected troops serving in Kuwait, Dubai, Iraq, Afghanistan, Korea, Japan and Germany, among other global hot spots. The foundation's efforts amount to far more than simply bragging rights over a ***Call of Duty*** face-off: It often arranges for troops' family members to attend the competition and get precious, online "face time" with soldiers.

This grassroots effort was launched by the husband-and-wife team of *Greg* and *Addie Zinone* who share the bulk of responsibilities, along with Pro vs. GI Joe staff member *Joe Oneto* and 10 wounded warrior volunteers. They handle all of the athlete/celebrity bookings, engage in military outreach, handle event planning/coordination/logistics as well as website content — and the organization gets by on more than just a little help from its friends. (*Addie* is a staff sergeant in the U.S. Army Reserve and has served two tours of duty in support of *Operation Iraqi Freedom*, most recently from 2007 to 2008.) For the tech connectivity, that's where **MTNGS** comes in.

"When we first met the good people behind Pro vs. GI Joe, they had a 45-foot trailer that was perfect for their mission, save in one respect — they didn't have the needed communications systems installed," said *Jim Ramsey*, a military veteran who is now president of **MTN Government Services**, an **MTN Satellite Communications** subsidiary. Ramsey is a retired U.S. Army lieutenant colonel with 26 years of military service, having commanded and served as the operations officer for the **82nd Airborne Division**, among other units. "There weren't any tables or kitchen-type fixtures in the entire vehicle. It was designed strictly for the foundation's operations. So they turned to us to get the technology up and running."

*Greg Zinone* feels that the continued support from MTNGS has allowed the non-profit to expand its reach and profile in ways that previously were out-of-range. "They came to us with such a rich, deep knowledge of communications systems," *Zinone* says. "For them, installing what to us seemed like the most complex of

satellite operations seemed as familiar as turning on a light switch. And this particular 'light switch' is allowing us to make such a positive impact on the lives of soldiers and their families."

## Chance Contact Leads To A Rewarding Partnership

All of this essentially started off randomly. In 2010, *Ramsey* and other MTNGS executives heard about Pro vs. GI Joe from a local Best Buy manager they knew in the greater Washington, D.C. area. The manager praised the *Zinones* effusively, explaining how they built their entire non-profit from virtually nothing, digging deep into their own pockets to make it work. And nearly every one of those dollars went directly toward the cause, to benefit the soldiers, as opposed to the steep administrative costs that foundations often report.

"When you meet Greg and Addie, you fall in love with their vision," *Ramsey* says. "They've committed to this like no two people I've ever seen. For an hour or whatever, these soldiers get to play games with a big-time athlete, re-connect with their families and forget about whatever troubles they've encountered whether it's the conflict or their wounds or post-traumatic stress disorder (PTSD)."

However, Pro vs. GI Joe wanted to take their operation to the next level, to broaden its profile on a national and even global level. To do so, that trailer would need work. So MTNGS supplied a host of resources to equip it for Very Small Aperture Terminal (VSAT) communications access.

The dish antennas operate in Ku- and C-Band frequencies and are often as small as 75 cm to 2.4 meters in diameter. A *Network Management System* (**NMS**) server allows network operators to monitor and control all operations, sending outbound information from the hub to the VSATs at remote locations. MTNGS has already established itself as an industry leader in VSAT technology, supplying this connectivity to military and government customers for mission-critical transportation units at sea and on land. Communications services delivered include networked headsets and hand units, interactive video conferencing and Wi-Fi Internet connectivity.

## Launching Connectivity Around The World

Now, MTNGS has successfully integrated that same technology in the Pro vs. GI Joe trailer, which must connect seamlessly anywhere that it travels to in the U.S., including professional football stadiums and ballparks, as well as **USO Centers** stationed around the world. The USO is a partner of Pro vs. GI Joe, helping the group put on events from its locations worldwide. In other cases, the soldiers taking part are recuperating in hospitals such as **Walter Reed Army Medical Center**. (Many participants for Pro vs. GI Joe are referred from another partnering foundation, the **Wounded Warrior Project**, which helps combat veterans transition to private life.)

The trailer boasts a half-dozen 55-inch, HD TVs running on six networks with bandwidth capacity of more than 512 CIR. Mounted and dismounted easily on the roof on the road, a 1.2

Ku-band antenna sends and receives the signals. Similar to a classic M*A*S*H unit, the trailer is now technically mobile enough to go anywhere, to any venue, without experiencing any hiccups on the needed communications deployment.

"We need to get out to a lot of big-time events, obviously, and we'll also put on quite a tailgate 'show' along with the video games," *Zinone* says. "I'm constantly putting dogs and burgers on the grill out in the front and it can get crowded and hectic out there. But nothing we do ever disrupts the satellite feed that we need."

There are two cameras in the trailer as well. That's because the whole morale-pumping "thrill' of the Pro vs. GI Joe experience is allowing the soldier and athlete to interact visually and audibly while playing. "If you're playing Madden Football with a couple of NFL players, it makes it so much more of a memorable experience to see and talk to them on streaming video," *Ramsey* says. "This also — if their family members are available — allows the soldiers to take advantage of the experience to get to see and talk to their loved ones again in real-time."

Next on the "to do" list for MTNGS: To wire three more of these trailers for Pro vs. GI Joe so the foundation can take its show on the road to all parts of the nation at the same time. Pro vs. GI Joe also seeks to allow some medically retired wounded veterans to own their own trailer, so they can stage events and help fellow Armed Services members in the process.

"And there's no reason why we can't do that," *Ramsey* says. "We're using the exact same technology that we have used on our customer's cruise ships, and have been aggressively expanding to the yachting and airline industries — as well as ground/air/sea support for military troops in the thick of combat. If we can take our communications systems and expertise to help Pro vs. GI Joe connect wounded veterans to these athletes and even their family members, there's no question that it's something we want to do."


*About the author*

Jim Ramsey is president of MTN Government Services (MTNGS), a subsidiary of MTN Satellite Communications, and is a military veteran with more than 35 years of communications and leadership experience, 26 years of which was spent in the U.S. military. Prior to joining MTNGS, Ramsey held executive positions with Protections Strategies Incorporated, Verizon Federal Network Systems, PRIME LLC, and MorganFranklin Corporation. In each company, he was the vice president of government and federal services responsible for the management of sales, customer service, technical operations, and maintenance. Prior to entering the corporate environment, Ramsey served 26 years in the U.S. Army and retired as a lieutenant colonel. He started his military career in 1979 as a private infantry soldier and ended his career as a signal corps officer. During his career, he commanded and served as the operations officer at various levels within the U.S. Army, including the 5th Infantry Division, the 82nd Airborne Division, the 2nd Infantry Division, and the 18th Airborne Corps, and with the White House Communications Agency (WHCA). While serving at WHCA, Ramsey served as a presidential communications officer for both President Bill Clinton and President George W. Bush. He also commanded four units within WHCA and ended his tour as the unit's operations officer. Ramsey was responsible for planning, installing, and maintaining communications requirements for more than 1,000 presidential trips for Presidents Clinton and Bush during his service at WHCA. He was inducted into the WHCA Hall of Fame in 2005. An alumnus of Bowling Green State University in Ohio, Ramsey graduated with a Bachelor of Business Administration degree. He currently resides in Winchester, Virginia.
For more information, visit www.mtnsat.com.

# INTEL

## TRANSEC IN AN IP-BASED VSAT ARCHITECTURE

**As the ability to monitor satellite transmissions grows more sophisticated, the need to implement increased levels of security becomes more critical. In combatant situations, where even a small spike in traffic can be a critical piece of intelligence, the need to mask any communications activity becomes apparent. The *National Security Agency* (NSA) in the United States has outlined the following vulnerabilities inherent in an IP-based TDMA transmission that must be addressed in order to provide true Transmission Security, or TRANSEC:**

- ***Channel Activity – The ability to secure transmission energy to conceal traffic volumes.***
- ***Control Channel Information – Disguise traffic volumes to secure traffic source and destination.***
- ***Hub and Remote Unit Validation – Ensure remote terminals connected to the network are authorized users.***
- ***Anti-Jam and Low Probability of Intercept – While a consideration, this is not a mandate by the NSA or any other organization.***

**This article discusses elements and considerations of providing a TRANSEC-compliant IP-based VSAT network and the approach iDirect has taken to implement TRANSEC.**

**TRANSEC** requires all network control channels and *Management & Control* (**M&C**) data to be encrypted and that any and all traffic engineering information be obfuscated from an adversary. For example, TRANSEC requires a communications channel to appear completely full to an adversary even if little or no actual data is flowing. This is contrasted with communications security, where the actual communication (*e.g.,* voice, video or data stream) is encrypted but certain header information is sent in the clear. While the encryption is virtually impenetrable, the information in the IP header including the source address, destination address and, most importantly, the **ToS** field are in the clear. With the IP header of an encrypted packet in the clear an adversary can determine how much of the traffic stream is voice, video or data. More significantly, an adversary could determine when high-priority flash-override traffic has been initiated and from which location.

In an **SCPC** (*single channel per carrier*) satellite network topology, achieving TRANSEC compliance is relatively straight forward. For SCPC connections, a bulk encryptor is employed to encrypt any data and control information traversing the network. The IP header of the packet would be encrypted by the bulk encryptor prior to being transmitted to the satellite. In addition, since an SCPC link is static and always on and no control information needs to be exchanged between the SCPC modems, all of the TRANSEC requirements are met.

In a TDMA network, TRANSEC compliance is more difficult. A TDMA network dynamically allocates bandwidth to remotes; therefore, there must be some type of control information transmitted to each device in the network. This control data, containing traffic engineering information, as well as information available from an encrypted IP packet header, can be exploited by an adversary. For example, anomalous traffic volume to a specific remote can indicate new activity in that area while varying ratios of voice-to-data traffic can denote the distribution of intelligence

(data) compared to lower priority voice traffic. **iDirect** has implemented the following solutions in response to the security vulnerabilities of a TDMA VSAT network.

## Channel Activity

***—Challenge***

The first vulnerability that exists in a TDMA network is the availability of traffic engineering information. In an SCPC network, the link is static with no variation in transmission characteristics based on end user communications. An adversary looking at a satellite transponder with a spectrum analyzer will see a constant RF signal. This is contrasted with a TDMA network. A TDMA in-route carrier energizes and de-energizes as traffic flows and stops. The on and off nature of a TDMA in-route is the natural extension of the ability to allocate satellite transponder space to remotes that have transient demands. While this characteristic makes TDMA networks much more bandwidth efficient, it allows an adversary to determine peak periods of activity, identify unusual or unexpected activity spikes, and identify locations of remotes that have remained quiet for a period of time and suddenly experience increased traffic volumes. The obvious risk in having this information in the hands of an adversary is the potential to extrapolate timing and location of scale of strategic activity.

***—Solution***

iDirect has implemented free slot allocation in its TDMA bandwidth distribution algorithm. With free slot allocation, an adversary snooping satellite transponder energies will see a constant "wall of data" regardless of traffic profiles. As the name implies, free slot allocation keeps the in-routes active regardless of actual traffic flows. Free slot allocation preserves the efficiencies of a TDMA system while obfuscating actual traffic volumes, negating the risk of using transmission activity as an intelligence gathering mechanism.

## Acquisition Activity

***—Challenge***

The rate at which remotes acquire into a network can provide critical information to an adversary about troop activities. All TDMA networks provide a dedicated channel for remote acquisition activity. If adversaries monitor the activity in this channel they will be alerted to troop movements by a flurry of acquisition activity.

***—Solution***

iDirect has exceeded the TRANSEC requirements by addressing the acquisition activity vulnerability. The iDirect acquisition algorithm inserts dummy bursts from remotes already in the network and intentionally skips acquisition bursts at times of high activity. The algorithm ensures an adversary sees only a random distribution of acquisition activity. The iDirect acquisition algorithm goes a step further by randomly varying the dummy burst's frequency, timing and power. This randomization ensures an adversary cannot distinguish between a dummy burst and actual acquisition activity.

## Control Channel Information

***—Challenge***

A great deal of traffic volume and priority information can be gleaned by examining the in-band or out-of-band control information within an encrypted TDMA network. As previously discussed, the IP header of a packet contains source, destination and priority information. In order for a TDMA network to provide the quality of service needed to support real time traffic, data quantities and prioritization information must be gathered. This information could be more useful to an adversary than channel activity data because it is specific enough to delineate

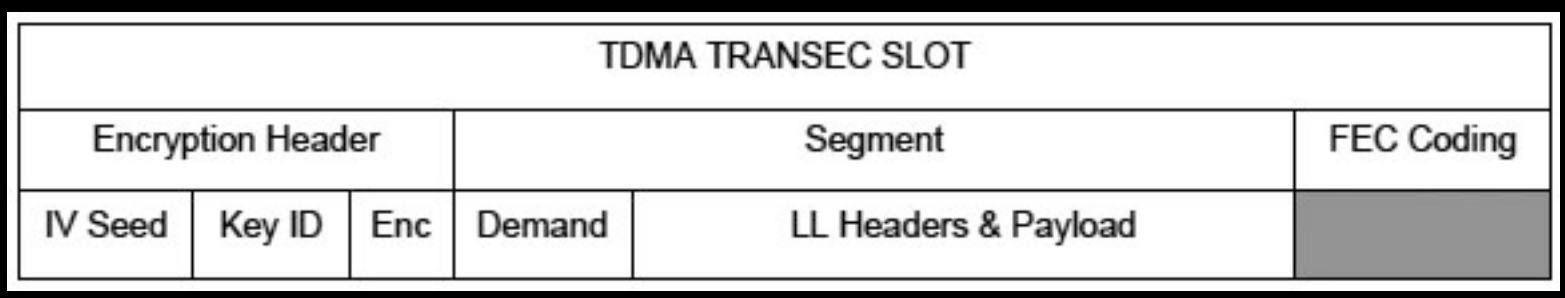



**Figure 1**

between general communications like email and web traffic, versus tactical communications like voice and video.

—***Solution***

The only solution for this vulnerability is to completely encrypt all Layer 2 information as well as any control information disseminated to the remotes. The encryption methodology must be secure enough to thwart an adversary long enough that the data becomes old and unusable. iDirect has implemented FIPS 140-2 certified 256 bit keyed AES encryption for all Layer 2 and control information. The encryption of the Layer 2 frames has a side benefit of re-encrypting the data payload. Therefore, the transmitted IP header itself is AES-encrypted. Additionally, the iDirect TRANSEC TDMA slot is a fixed size, again to obfuscate any traffic characteristics. This Layer 2 encryption solution solves all existing control channel vulnerabilities.

The iDirect Layer 2 encryption method goes a step beyond to feature over-the-air key updates and a unique Layer 2 frame format including an Initialization Vector that ensures randomization of repetitive data streams. The net result is that adversaries are precluded from detecting any repetitive pattern, which can aid in deciphering encryption algorithms.

## Hub and Remote Unit Validation

—***Challenge***

Another vulnerability of a TDMA VSAT system is the concept of Hub and Remote Unit validation. In traditional SCPC architectures, when a link is established, it remains active for very long periods of time. Because these connections are fixed, and there is a significant level of coordination between personnel commissioning the SCPC, a high degree of confidence exists that an adversary is not trying to assume the identity of a trusted entity. In TDMA networks, remotes are routinely coming into and dropping out of the network. This is especially true of networks with **COTM** (*Communications On The Move*) terminals where vehicles are traveling under bridges and behind buildings. This type of

dynamic environment gives an adversary a greater opportunity to obtain a VSAT remote through licit or illicit channels, spoof the device ID and insert a rogue remote into a secure network. Equally feasible is an adversary acquiring a VSAT hub terminal and coaxing a blue force remote into the adversary's network.

***—Solution***

To mitigate this risk, iDirect has implemented **X.509** digital certificates on TRANSEC remotes. An X.509 certificate utilizes RSA public key encryption. With public key encryption two related keys are generated: One private key and one public key. The functionality of these keys is such that anything encrypted with the public key can only be decrypted with the private key and anything encrypted with the private key can only be decrypted with the public key.

In the iDirect system, X.509 certificates can be generated via the NMS server or provided by a third party. Certificates are placed on all TRANSEC line cards and Protocol Processors as well as on the remotes. The hub system keeps the public keys of each remote configured to operate on the hub and the remotes have the public keys of each hub device. During network acquisition, the remote encrypts its X.509 certificate with its private key and the hub verifies by decrypting the certificate with the remote's public key and vice versa. This process ensures a remote is not only authorized to operate in the network but that the hub is a trusted entity.

## Operational Implementation

***—Challenge***

Implementing security and ensuring all security policies are followed can be a burden to the soldier in the field. Implementing TRANSEC and performing key management is no exception. A robust TRANSEC network requires the use of at least two network-wide keys. One key, commonly known as the passphrase, is typically long-lived and is used to encrypt acquisition activity, and one key that is used to encrypt frame header information. The use of front panel displays to enter a passphrase and external key fill mechanisms places an undue burden on the warfighter and introduces security vulnerabilities.

***—Solution***

iDirect has implemented a FIPS-approved software method of key generation and automatic, over-the-air key distribution protocol. Not only does the software-based key generation and key distribution mechanism make TRANSEC operation simpler and more convenient for the warfighter, it makes the system much more secure by removing a human from key distribution.

Another advantage of automatic key generation and distribution is that it seamlessly enables a global COTM TRANSEC network. By automatically generating and distributing new acquisition passphrases a single, dynamic passphrase can be used across global networks.

## DVB-S2 Considerations

For increased bandwidth efficiencies, DVB-S2 offers faster data throughput and better coding capability. DVB-S2 uses the industry's leading forward error coding technology, *Low-Density Parity-check Codes* (**LDPC**) coupled with **BCH** coding. This concatenated LDPC-BCH coding scheme provides performance very close to the theoretical Shannon limit resulting in a 30-40 percent bandwidth efficiency increase over existing DVB-S systems. iDirect's latest release ***iDX 2.3*** enables TRANSEC over DVB-S2/ACM. This allows for additional bandwidth efficiencies stemming from *Adaptive Coding and Modulation* (**ACM**) as well as providing for an extra level of security by creating a continuous wall of strongly encrypted traffic that remains constant. With ***iDX 2.3*** iDirect also introduces **FIPS 140-2 Level 1** certified software as well as **FIPS 140-2 Level 2** compliant* TRANSEC-capable IP modems.

## Conclusion

There are inherent benefits to the IP-based DVB-S2/TDMA platform that iDirect utilizes, with respect to bandwidth efficiency, scalability and the scope of applications that it enables. There are also inherent security risks with a TDMA platform. The iDirect TRANSEC over DVB-S2 architecture is able to provide the highest levels of network security while maintaining the efficiencies and benefits of the TDMA architecture. iDirect has implemented the most efficient TRANSEC-compliant network architecture in the VSAT industry today, which ensures the QoS characteristics of the network are preserved.

# A CASE IN POINT

## MISSION CRITICAL COMMUNICATIONS VIA AUSTRALIA

**Some may wonder why the U.S. military looked all the way to Australia to find a Teleport to provide them with their highly sensitive, mission critical satellite communications. However, this came as no surprise to Australian Teleport providers, who know they are in a unique position to be able to deliver secure, reliable, undisrupted satellite communications, thanks to their rare and stable landscape.**

**As a politically and geologically stable country, with low rainfall and mild temperatures, Australia provides the perfect location to house Teleports and satellite infrastructure. Australia is a geographically remote country, ensuring minimal frequency interference. Plus, the country shares a border, albeit at some distance, with the USA via the Pacific Ocean, providing direct cable access (via the Southern Cross Cable Network) to the USA.**

NewSat's Military Accredited Global Access Point Teleport in Adelaide, Australia

NewSat

Global Satellite Solutions

# 100% up-time from Australia

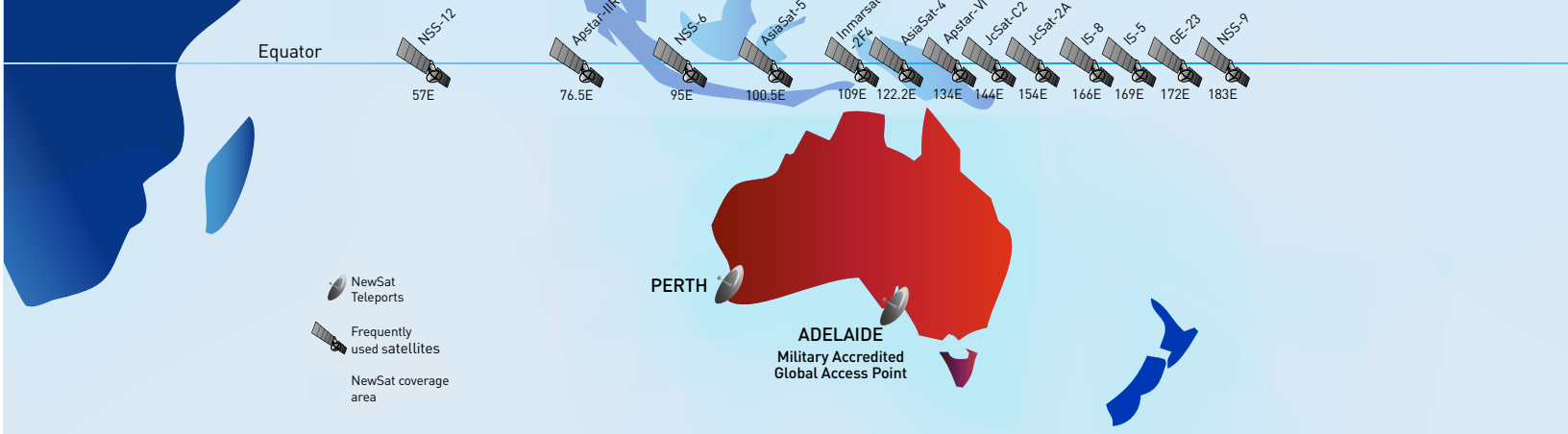
## In 2010, NewSat delivered 100% Teleport availability to customers, providing secure, reliable, uninterrupted connectivity.

As Australia's leading independent satellite service provider, NewSat provides secure, efficient and cost-effective solutions throughout Asia-Pacific, the Middle East, Europe and Africa. NewSat's two Australian Teleports provide access to an extensive range of satellites, a greater choice of tailored solutions and increased redundancy. NewSat adopts the latest technology and provides 24 x 7 x 365 days support ensuring optimal up-time and efficient throughput.

DEFENCE RECOGNISED SUPPLIER – Department of Defence

WORLD TELEPORT ASSOCIATION – FINALIST – 2010 AWARD FOR EXCELLENCE

GLOBAL ACCESS POINT – MILITARY ACCREDITED




**To learn more about NewSat's satellite communication solutions contact us today**

Telephone
**+61 3 9674 4688**

Email
**sales@newsat.com**

# A CASE IN POINT

**Proactive Communications, Inc.** (**PCI**) of the United States required a Teleport operator to provide satellite communications to the U.S. military in Afghanistan and they decided to use an Australian Teleport which could provide the bandwidth required as well as a guarantee of fast, secure, undisrupted connectivity.

## Background

**PCI** is a SatCom provider that delivers reliable and secure enterprise-class communication capabilities to government agencies, military and corporate entities around the world. PCI has become a proven and trusted resource for satellite communications in the most demanding situations and within the harshest of environments.

## Objective

PCI is contracted by the U.S. Government to provide vital communications support to the U.S. military in war zones in the Middle East. Mission critical communications in war zones requires constant transmission and delivery of highly sensitive and secure information. A lack of satellite telecommunications bandwidth over Afghanistan and previous attempts to reach Afghanistan through Europe, caused PCI to consider Australia to solve their demanding communication requirements. PCI required a partner who could provide effective breadth of coverage in challenging and remote locations, as well as being able to provide significant depth in satellite and engineering expertise for the ongoing project.

## Solution

A custom made system that fitted with PCI's requirements securely and cost effectively was designed. This enabled PCI to provide critical communication needs in the deployment of rapid tracking terminals, VoIP, unified communication and private secure networks, using state-of-the-art platforms such as **ComtechEF Data** modems, **Teledyne Paradise** modems and **iDirect** DVB-S2 hub technology. C- and Ku- band coverage from **NewSat**'s **Adelaide Teleport** and fibre backhaul technology was provided.

The stringent security criteria required for U.S. military operations were met through NewSat's Australian Adelaide Teleport, one of only a few U.S. *Military Accredited Global Access Points,* providing unrivaled service coverage in the Middle East. "Our customers are completely reliant on us for satellite communications and meeting their needs in their difficult and dangerous environment is of paramount consideration." - *Marc LeGare*, CEO, Proactive Communications.

From a business point of view, as much as from an operational one, aftermarket support was essential to PCI — partnering with an experienced and qualified company eliminated the need for third party consultants and associated costs. Such dramatically improving PCI's return on investment.

*LeGare* added, "I can directly attribute a sizable impact on our business having NewSat as our business partner. They have provided the capacity for our growth and I'm able to do about $10M because of their solutions."

**The U.S. military receive fast, secure and undisrupted satellite communications through NewSat's Australian Teleport.**

# SatFinder

Satellite Database & Calculation Software

## DATABASE

Information on over 500 satellites (orbital location, frequencies, EIRP, G/T, SFD, bandwidth, programming etc.)

Information on 9,000 companies (address, tel, fax, web, products, services and contact names etc.)

Information on 19,000 executives in the commercial satellite industry.

800 hundred EIRP, G/T & SFD maps in color not published anywhere else.

## CALCULATION

Has full up-down digital link budget calculators with input provision for uplink power control (UPC), ALC, various interferences and multiple carriers.

Finds HPA size, uplink power requirements, bandwidth and power usage per carrier.

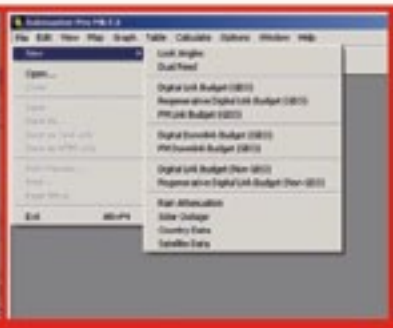
Calculates atmospheric losses and rain fade margins for any desired availability on uplink and downlink.

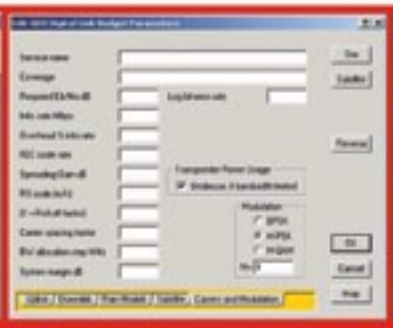
Handles BPSK, QPSK, M-PSK or M-QAM with any FEC code rate.

Determines power or bandwidth limited modes and calculates the power equivalent bandwidth, if appropriate.

Provision for RS codes or 'Turbo' modems. Option for rain up AND rain down scenarios where uplink and downlink are from/to the same city.


**UPDATED QUARTERLY!**




http://www.satnews.com/satfinder

# FOCUS

## RAPID DEPLOYMENT OF CELLULAR OVER SATCOM

author: Richard Hart, Senior Product Line Manager — Mobile Platforms, Powerwave Technoloiges, Inc.

**Planning to restore communications in the event of a natural or man made disaster can be a daunting task to say the least. One must consider a multitude of scenarios and plan for the worst. One such option to consider would be a *rapid mobile deployment unit* (RMDU). Generally speaking an RMDU has the following features: rapidly deployable, telescoping mast, off-grid power solution, equipment enclosure, communications capacity and coverage solution, backhaul solution and command and control elements. In selecting a partner for such a solution one should consider a vendor with a breadth of knowledge and experience in all the technical disciplines that make up an RMDU.**


**An example of the satellite/celluar marriage is the Terrestar Genus phone, which is available to AT&T customers.**

**Powerwave Technologies**' award winning **RMDU** has been designed from the ground up with this in mind. The RMDU integrates all the above technologies in a ruggedized commercial platform for domestic or international use by first responders and government entities. Integration of auto deployable, very small aperture terminals (VSAT) for backhaul of cellular, Wi-Fi and public safety communications coupled with an active-array antenna coverage solution make it a one-stop destination for agencies looking for complete coverage solutions for applications such as disaster recovery, nation building, border security and remote training sites that lack communications coverage. Easy to deploy and reliable backhaul of voice and data when traditional landline backhaul is unavailable make cellular-over-satellite a viable option. When considering cellular-over-satellite considerations such as quality of service techniques, service type, hardware and cellular technologies such as LTE need to be planned carefully.

Today, most major satellite service providers only offer dedicated space segment bandwidth versus that for on-demand bandwidth. Currently, second-tier satellite providers fill this on-demand niche. The reasoning is that the tier 1 service provider assumes the day-to-day cost for maintaining the infrastructure that provides the bandwidth as well as the resources that manage the infrastructure. On-demand bandwidth is typically marketed by oversubscribing the amount of bandwidth by a factor of two or more, which provides the foundation to capture the revenue to support the costs associated with maintaining the infrastructure and those resources. The problem with on-demand is that the bandwidth is shared, meaning that there are multiple subscribers who have the potential of leveraging the same bandwidth, resulting in dropped data on that space segment bandwidth.

Dedicated bandwidth offers the guarantee that the bandwidth will be available when it is required and needed by the customer. For customers with high usage needs and critical data to transport, dedicated bandwidth is most likely the preferred choice. However, this choice typically carries higher monthly fees and charges. The advantages of dedicated bandwidth may outweigh the higher costs and include the following benefits: the bandwidth and the data that rides the bandwidth is only for that customer's traffic. The customer traffic may have bandwidth conflicts/constraints internally, but are not the result of external traffic usage/patterns. Dedicated bandwidth allows for the customer to segment their higher priority traffic over lower priority traffic by the use of a *quality-of-service* (**QoS**) strategy that they own and manage. This QoS strategy can be simplistic or complex, depending on the makeup of the traffic and the critical transport requirements for the traffic types being transmitted.

As the traffic types evolve with newer technologies such as LTE, the QoS strategies become more important to manage and build correctly to ensure streaming video and low-latency apps such as on-line gaming sessions are carried across that bandwidth transport in a timely manner where latency, jitter, and wander can be intrinsically determined and managed for higher data transport performance. As IP is the mainstay for LTE, a QoS strategy that leverages the IP protocol stack becomes more important to manage efficiently. With the advent of newer and faster mobile devices consuming more and more data, the customer will need to properly size the bandwidth pipe to effectively support the various traffic types.

Shared bandwidth is more economically feasible. Shared bandwidth is where two or more customers use and compete for the same bandwidth capacity. This is usually referred to as oversubscription and allows the bandwidth service provider to break apart the total pricing into smaller chunks for each customer utilizing that bandwidth segment. The service provider has the opportunity to get additional revenue with the oversubscription by selling the bandwidth for more than the sum of the segment while the customers only pay for a portion of the overall total bandwidth cost. Shared bandwidth makes sense financially when the customer infrequently transmits or receives data, allowing them to "smooth" the usage over time for that lower cost. Typically, the shared bandwidth approach is good for non-critical data that can handle additional jitter, latency and/or wander if the data encounters delays during the transmission. Those delays most likely will be the result of other customers performing data transmission at the same instance in time.

QoS strategies are more difficult to implement into a shared bandwidth environment due to competing customer traffic profiles/types. For example, Customer A and Customer B both have voice over IP (VoIP), but who gets "first" crack at the bandwidth queue needs to be addressed in the QoS strategy. Other factors, such as *time-of-day* (**ToD**), seasonal, and level of guaranteed service contracts will help formulate the QoS strategies in a shared environment

The expansion of satellite communications from C-to Ku-band and now Ka-band has allowed manufacturers and vendors to develop smaller satcom terminals that more readily support communications-on-the-go. Ku-band satcom vendors are now building terminals that weigh less than 40 lbs. and can be carried in a backpack. Newer satellites have been outfitted with Ka-band transponders and are now offering Ka-band services. Ku-band space segment is fairly weather tolerant. However, the smaller satcom aperture dishes are challenged during inclement weather periods, increasing the difficulty with closing the link loop.

*Block upconverter* (**BUC**) vendors are also able to leverage smaller amplifier electronics to reduce the size of these devices, which allows for higher powered BUCs to be packaged into smaller housing units. C-band is mainly used in maritime applications to better close the communications loop while ocean-going vessels are in-motion. Ku-Band has gained substantial footholds in the US, Europe, Latin America and Africa. Ka-band is now being offered in the U.S. and Europe, but due to the higher frequency is more susceptible to weather conditions. However, pricing for Ka-band satellite links are more economical that C- or Ku–band links.

Service providers are taking advantage of the smaller Ku- and Ka-band satcom terminals and bundling these terminals with Wi-Fi and cellular. This opens new avenues of revenue and sales to entities that require communications in rural or isolated locals. One large entity that counts on extremely reliable communications is the first responders and emergency response group, which requires flexible communications during a disaster to assist with coordination between entities.

The smaller, more portable satcom terminals coupled with greater availability of satellite services and the coupling of Wi-Fi, VoIP, and cellular to the satcom system affords a higher level of flexible and reliable communications to this user segment. Auto-deploy satcom systems allow for set-up to service-ready in a matter of

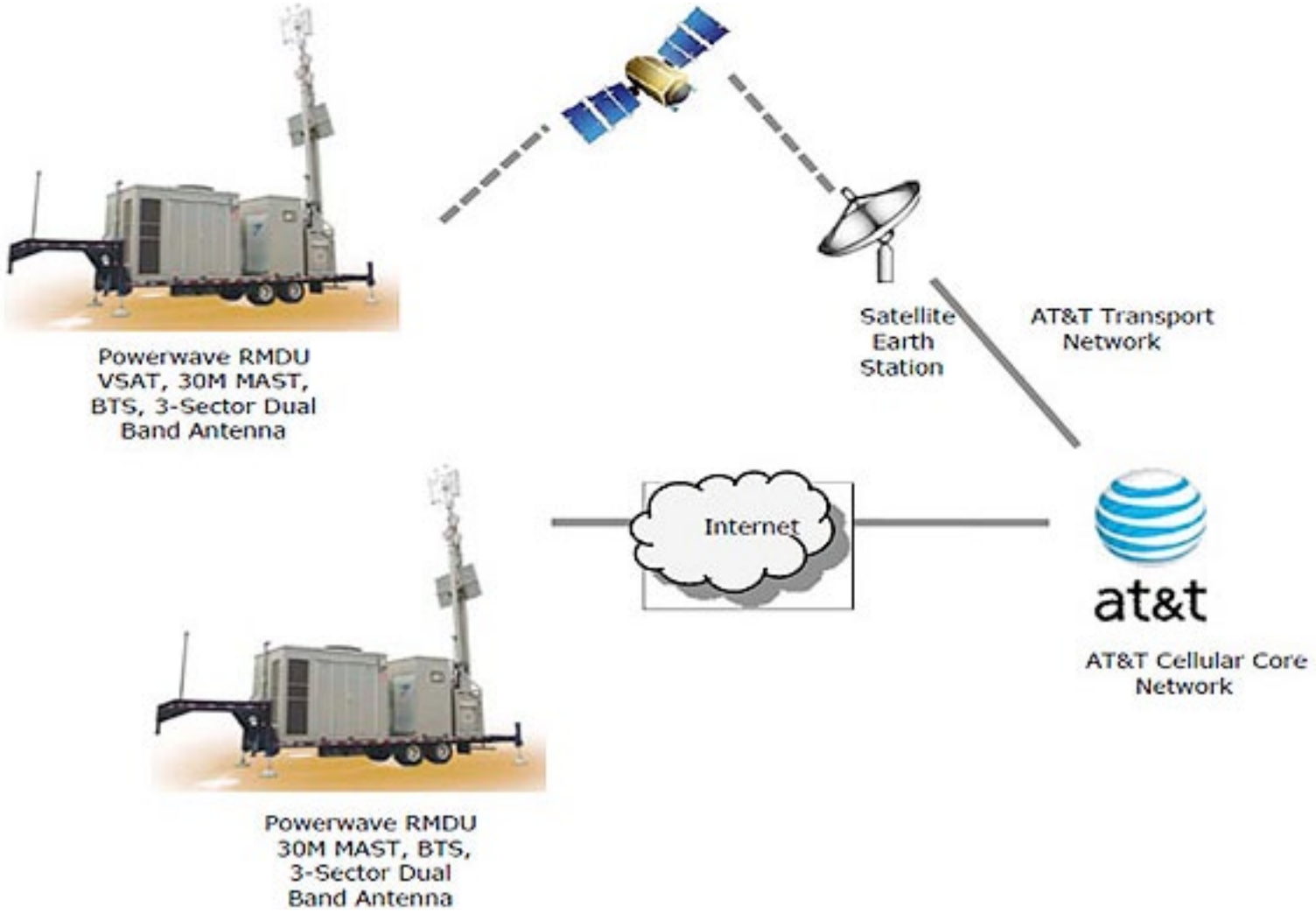



**Figure 1.**
**Tier 1 service providers like AT&T now provide integrated cellular service bundled with satellite.**

minutes, with full system operation in less than 10 minutes. This is vastly quicker than terrestrial-based communication links that require hours, if not days, of coordination to align signal paths to establish a level of reliable communications. Use of satellite auto-deploy SatComs with embedded Wi-Fi, VoIP, and cellular offer a true "plug-n-play" solution when instant communications are needed or warranted. New products in this area are now available from Tier 1 service providers like AT&T. AT&T's integrated cellular service bundled with satellite is called **ARMZ** (*AT&T Remote Mobility Zone*). (*See Figure 1 on the preceding page.*)

To protect the customer traffic, the data should be encrypted using security measures such as *Internet protocol security* (**IPSec**), *generic routing encapsulation* (**GRE**) and *secure sockets layer* (**SSL**) protocols. Use of these types of protocols allow for end-to-end security of the traffic, which is critical for sensitive data that could be received by anyone tuned into a customer's receive signal over a satellite link. By encrypting the traffic across the link, the use of a pre-shared keys embedded into the *public key infrastructure* (**PKI**) will allow for a secure communications link/path. Unless the user receiving the data has the proper PKI key or certificate, the data will be difficult to interpret.

A recommended approach would be to establish a VPN between the customer's remote site and the corporate data center. This would also protect the customer traffic across the backhaul from the Earth station to the customer data center, even allowing the use of the public Internet to support the backhaul. Dynamic IP routing protocols can be implemented that also support a secure, diverse and resilient communications backhaul path between the remote site and the core network. As IPV6 begins to be implemented both by the hardware vendors and by the service providers, this too will afford better, more secure communications between end-points.

Use of satellite backhaul for LTE may be very advantageous in that the topology could be widely distributed, meaning that rural eNodeB base stations could hone back to one of the centralized serving gateways and mobility management entity where the data and call authentication and signaling would occur to support the data/voice session connectivity.

Vendors such as Powerwave Technologies who build small LTE picocells may be able to offer a key service differentiator to wireless operators pushing into the rural areas, which are typically underserved by wireless and broadband operators.

Even though satellite backhaul has significant delays over terrestrial backhaul technologies, the delay can be managed effectively with proper QoS strategies that keep transmission attributes like wander, jitter, and error rates constant to support the high bandwidth, low latency applications being pursued by the LTE forums and operators. By keeping the transmission quality constant, these attributes can be mitigated to help minimize latency related issues for all but the most extreme applications operating within establish parameters.

There are wireless service providers who have embraced satellite transport for their 2G and 3G cell backhaul needs while offering comparable service that support over terrestrial backhaul technologies. The use of satellite is especially receptive to the first responder and emergency response organizations who work in harsh conditions that include no or low signal strength wireless environments. This market segment understands the value of reliable communications, especially across inter-agencies where speedy exchanges of information could be the difference between life and death. LTE will continue this evolution by enhancing inter-agency communications and exchanges as more data applications requiring streaming video and other high demand bandwidth traffic push the envelope of what can be attained in these situations.

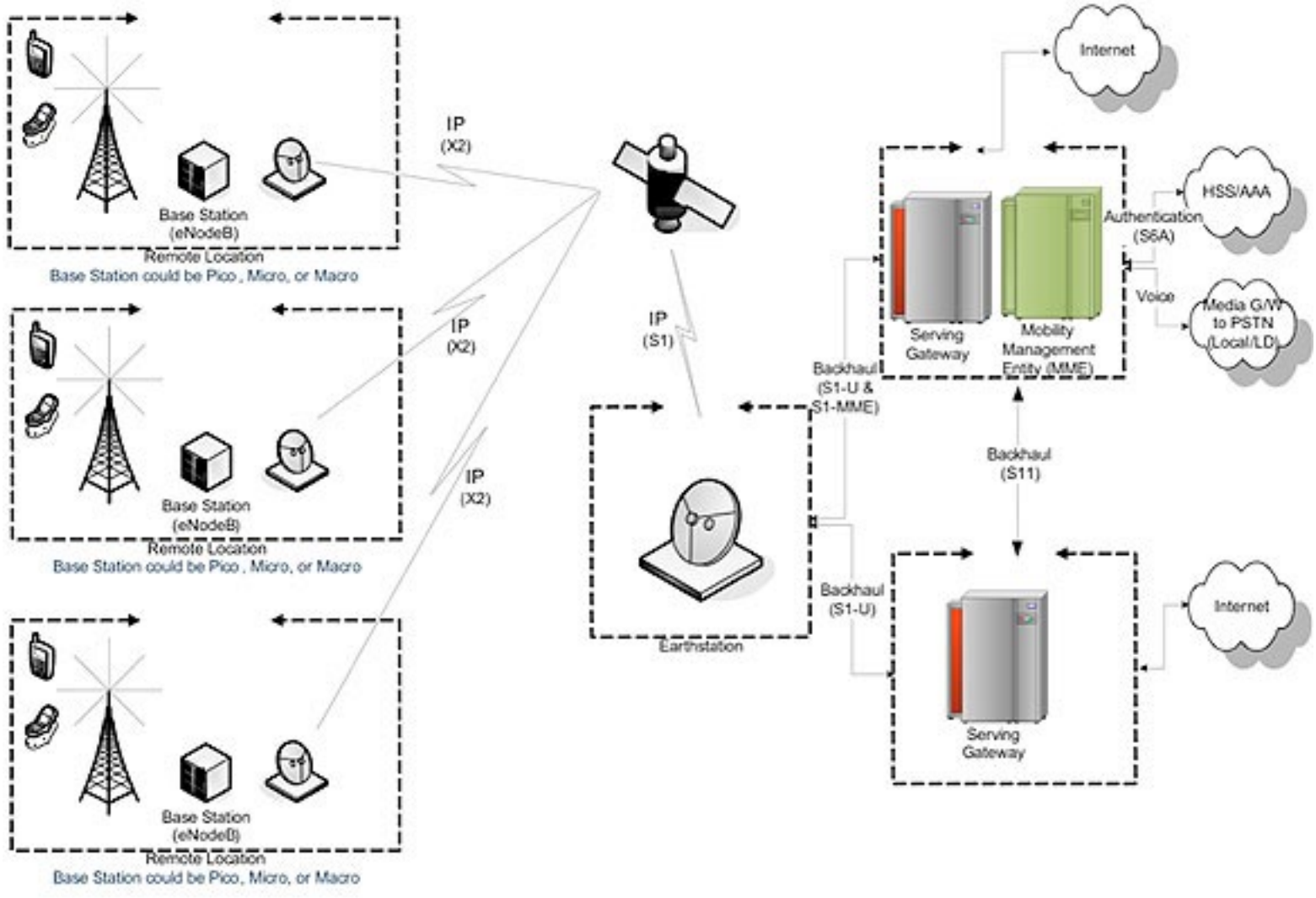



**Figure 2. Dynamic IP routing protocols can be implemented that also support a secure, diverse and resilient communications backhaul path between the remote site and the core network.**

As mentioned previously, the use of IP transport has become the protocol of choice, as it allows the user equipment to send "packets" at pre-defined *maximum transmission unit* (**MTU**) sizes for greatest efficiency and network performance increases. New equipment manufacturers are developing products that incorporate the best of the IP protocol to allow for constant connectivity in diverse and challenging environments.

These vendors have been successful with implementing IP into a satellite RF environment that allows customers to focus on bandwidth efficiency in *very small aperture terminal* (**VSAT**) via the *time-division multiplexing/time-division multiple access* (**TDM/TDMA**) access scheme. One vendor has bypassed the conventional contention schema and devised a method to allocate a specific amount of bandwidth per remote continuously, while dynamically reassessing the allocation based upon queue depth, the configuration-in-run (CIR) configuration, the QoS and prioritization settings, and the rate limits at each remote. This scheme allows for rapid reaction to changing traffic demands to provide adequate CIR and *equipment identity register* (**EIR**) service levels.

Determining the amount of satellite bandwidth a customer requires can be challenging, especially if the majority of the traffic is nondeterministic. The QoS strategy should be based upon differentiated services and use mechanisms such as traffic shaping, (leaky bucket) scheduled algorithms, *weighted fair queuing* (**WFQ**) and/or congestion avoidance (*weighted random early detection* [**WRED**]). These schemes are critical to be implemented for shared bandwidth and are highly suggested for dedicated bandwidth.

## Leveraging The Links

Many articles and subject matter experts have been touting the benefits of satellite for disaster response communications — the true power is when newer communication technologies, such as cellular, leverage satellite links for backhaul due to the availability of space segment and the ease of setting up portable, auto-deploy satcom antenna systems to leverage those links. The quick setup and deployment cycles for on-air are in minutes, which is crucial for prompt response efforts. The satellite systems become an invaluable tool to use during a disaster event to help establish necessary communications, especially for larger mobilization camps and staging areas and promote better inter-agency coordination during the event. Use of cellular-over-satellite allows these staging areas to be closer to the disaster area, helping expedite response and recovery activity. Smaller cellular base stations deployed with the latest cellular technologies, such as LTE, allow for a more standardized communications network that can support voice and high speed data needs and demands.

Powerwave Technologies, Inc. displayed and demonstrated the RMDU capability at AGAUS in Indianapolis, Indiana, June 6th -12th, 2011.

*Acknowledgements*

Richard Hart, Senior Product Line Manager – Mobile Platforms Powerwave Technologies, Inc.

Wayne Berthold, Principle Product Development Engineer, AT&T Mobility Services – Vanguard Services, International Alliances & Integration

# COMMAND CENTER

## ANDY BEEGAN, CTO + SR. V.P., SEGOVIA, INC.

**In his current role, Mr. Beegan is responsible for *Segovia Core Engineering*, *Network Operations*, and *Solutions Delivery*. He has commercial and government experience in engineering management, strategy, business development, satellite RF and IP network design, and program management. Mr. Beegan joined Segovia in its infancy and has played an integral role in the company's network design, product development, and government contracting activities.**

**Mr. Beegan returned to the Segovia team from Booz Allen Hamilton where he supported satellite-related projects for multiple U.S. government agencies. Prior to Segovia, Mr. Beegan served as a Senior Satellite Applications Engineer for PanAmSat (now Intelsat).**

**Mr. Beegan has a Bachelor of Science degree in electrical engineering from the University of Notre Dame and a Master of Science degree, also in electrical engineering, from Virginia Tech. In addition, Mr. Beegan has an MBA from the University of Maryland Smith School of Business.**

## MilsatMagazine (MSM)

***Good day, Mr. Beegan. You have been professionally involved in our industry for many years. What do you see as among the most significant advances for our industry over the past couple of years in the commercial and military/government segments?***

## Andy Beegan

Historically, government acquisition was focused on the space segment of the solution. Segovia's customers understand that satellite, terrestrial, and other managed components should be purchased as a bundle. They get a greater level of service from the providers, and delivery of service is much more cost-effective.

Over the past few years, what we have seen is government changing its approach to contracting to match with the right solution. They understand that increasingly the right solution for their needs is a managed service. Their acquisition approach is beginning to align with that. We see that in particular with the Future COMSATCOM Services Acquisition (FCSA).

Segovia is front and center with what's described under FCSA, and in a position to deliver the same types of services — with the government having an easier path to get these services than it has had in the past.

## MSM

***What is Segovia's charter and what military and government organizations/agencies do you work with?***

## Andy Beegan

Segovia's charter is to deliver network solutions on a global basis for government customers, primarily. That includes a combination of satellite space segment, teleport services, terrestrial connectivity, network operations support, and all other lifecycle managed services associated with such a solution.

We work with all U.S. government and allied nations users. While we do some work with commercial clients, ultimately our main customer is government. Within the U.S. government, one of the primary users is the Department of Defense, and we operate DoD's largest VSAT network by terminal count.

## MSM

***Please explain Segovia's core businesses and how such are implemented across the globe.***

## Andy Beegan

Segovia seamlessly bridges the satellite-to-fiber divide in the global terrestrial communications market. We leverage our satellite and terrestrial communication network expertise to solve our clients' end-to-end global telecommunication needs, delivering flexible, interoperable, custom-fit communication solutions that meet their objectives. Our private Multi-Protocol Label Switched (MPLS) network, and our close working relationships with every major satellite system operator, allow us to deliver solutions with greater speed and reliability.

## MSM

***Given your work with governmental agencies, how do you ensure your firm, given its commercial roots, can address the issues of importance to various government entities? As you worked on many projects while at Booz Allen Hamilton, did this give you the impetus to know how to address government business?***

## Andy Beegan

I started my career as a Senior Satellite Applications Engineer for PanAmSat (now Intelsat). I actually joined Segovia in its infancy, helping in the company's network design, product development, and government contracting activities. For a short time I worked with Booz Allen Hamilton, supporting satellite-related projects for multiple U.S. government agencies.

The government is realizing that in the satellite space set, commercial industry has the capability to deliver services faster and more cost-effectively than the government can on its own. Over the last 10 years or so, Segovia has seen that the U.S. government is relying on commercial industry to deliver these services.

Booz Allen has a very disciplined and structured approach to how they support a government customer. Within Segovia, from a service perspective, a similar disciplined approach applies. We make sure we are very detail-oriented in how we respond to the government customer. Every inquiry from a Segovia customer takes priority over any other internal projects we may be handling. Ours is a real-time network service environment, and we deal

directly with users who are in remote locations, calling into our network operations center. It demands a sense of urgency that is different than you might see in most other companies.

## MSM

***How did you become interested in the satellite industry and how do you see the industry evolving, given the stagnant global financial climate? Exactly what is your background?***

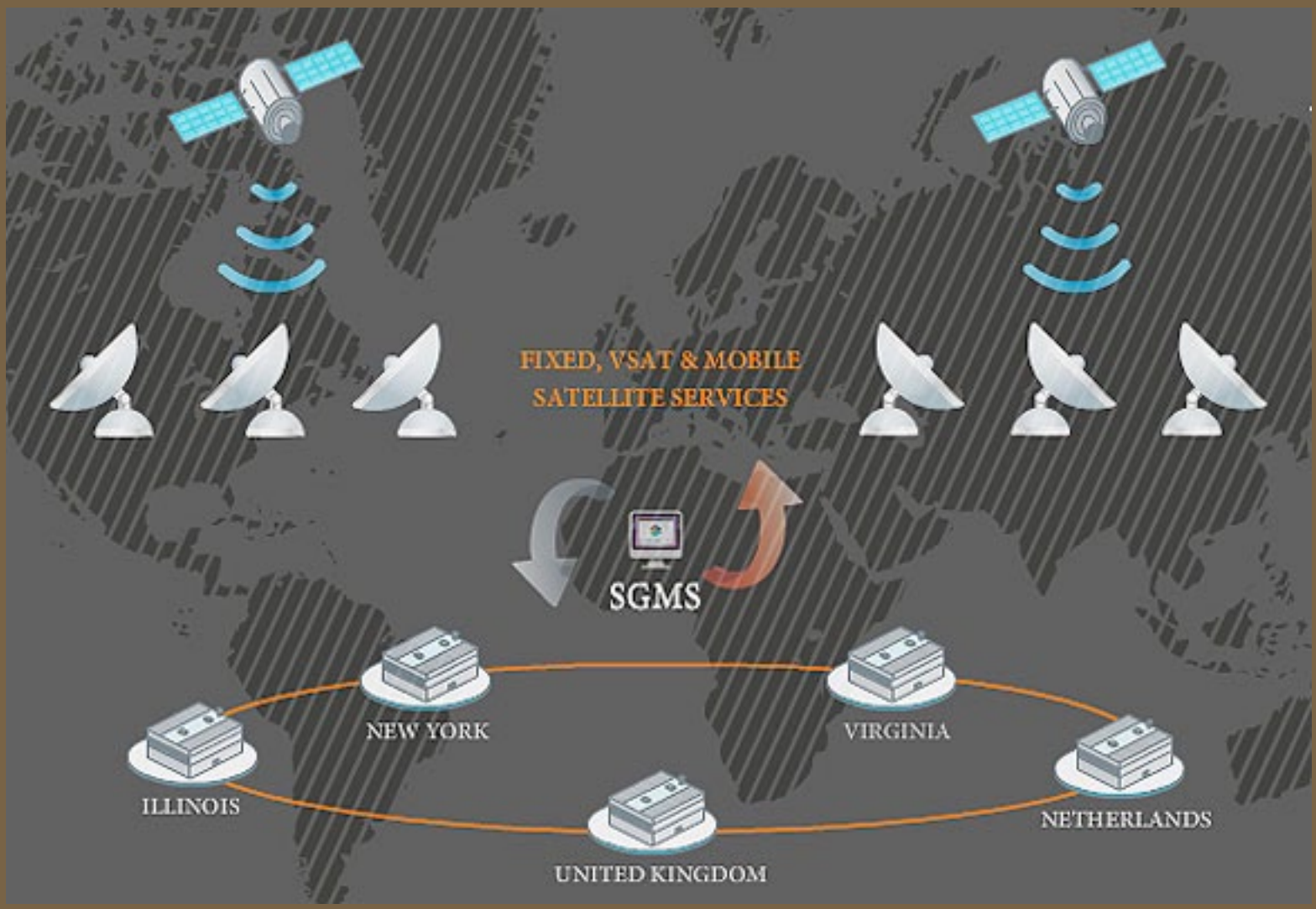
## Andy Beegan

I studied electrical engineering in college at the University of Notre Dame. Directly after, I went into the full-time program at Virginia Tech for Masters degree in electrical engineering. Coming out of Virginia Tech, I knew I wanted to be in a technical field, but also in a field where I had exposure to the business side. The satellite industry was a place where I felt I could exercise my engineering discipline, but would have the opportunity to be involved in the business component as well.

The satellite industry is unique, because it is very difficult to separate the engineer from business. When the engineer is doing his work, he or she has to be very aware of the ramifications on the business side. A very small change to a design can translate into very significant dollars; I think that is something that is very unique to our industry.

Given the economic climate, one of the things that the satellite industry has to do is to provide service as cost-effectively as possible. This goes to the root of how Segovia delivers service. We've often said that when the government procures space segment only, the contractor is incentivized to sell as much space segment as possible. When purchased as a managed service, the provider is incentivized by nothing else but delivering excellent service. The onus is on us to be as efficient with the satellite spectrum as we possibly can.

That goes to the heart of how the industry is evolving. That is why the government is changing the way it is buying such services.



## MSM

***Given your expertise in the more technical side of this business, many involved in uplinking and downlinking data are genuinely concerned about network security. What concerns have been imparted to you, and what are your solutions to such challenges? What advice do you have for users of combo networks and what products and/or services can assist in addressing such needs?***

## Andy Beegan

With our U.S. government clients, the main network security concern is meeting the established network certification and accreditation (C&A) guidelines for compliance with government standards.

The primary process is called the Defense Information Assurance Certification and Accreditation Process (DIACAP). Within DIACAP, there are three different mission assurance category (MAC) levels — from the most secure at Level 1 to the least secure at Level 3. There is an established process in which government auditors visit Segovia's facilities to make sure they live up to the standards that DIACAP lays out.

Segovia's track record of achieving C&A through numerous engagements has allowed us to streamline the experience for our clients. When a customer comes to Segovia, we work with their approval authorities in the leadership team, to enable them to achieve the appropriate certifications quickly to operate on Segovia's network.

Providing specific advice openly on how to secure a network offers insight into how to defeat that security. In general, however, it's important to remember that you are passing traffic from a remote location to a secure location. At every layer of the network—from the space segment to the teleport to the terrestrial backbone—certain measures must be put in place to ensure security.

All devices in the network—from modems at the teleport, to routers and switchers at the backbone, to the servers managing those components—have different security measures associated with them. DIACAP sets standards for configuration of the devices based on the MAC level of the user agency.

Encryption on the network, operational security, personnel security, and personnel and physical security measures all come together to meet the standards as dictated by DIACAP, and each element should be given equal weight in securing the network.

Segovia simplifies the certification and accreditation process for its users by ensuring that those security measures are in place for all devices at every segment of the network.

## MSM

***With governments aching for additional capacity, how do you see the hosted payload business as a solution, or as a wishful thought? Hybrid networks seem to be a workable solution for many applications. Can you reveal some of the examples of Segovia successes in this regard? And, given the mixed nature of hybrid networks, does such increase security concerns?***

## Andy Beegan

Hosted payload is a solution to arrive at volume discounts for space segment with a long-term commitment. Segovia finds more compelling the notion of a hosted network—including hosted satellite spectrum, with flexibility to procure capacity with assured access over the 15-year life of the satellite. This is coupled with ground infrastructure that is delivered as part of our services today. It provides an end-to-end solution within the hosted concept and gives users additional cost efficiencies, because of their up-front commitment to that type of solution.

In fact, hybrid solutions are the solution for any application. No application runs with just satellite space segment—you also need a place to land that space segment, and some terrestrial connectivity for that application to traverse end to end. Segovia has been in a position to deliver those types of services since its inception.

When procuring space segment alone, ultimately there is very little that the provider can do to ensure security. The provider is offering frequency assignments, and their hands are off from there. When procuring a hybrid terrestrial/satellite solution with all the associated components, virtually every provision of DIACAP comes into play, because DIACAP is much more focused on the other pieces outside of the space segment than it is on the space segment itself.

Segovia's track record of success in providing hybrid satellite/terrestrial networks has grown to the point that our managed services include all of the provisions that our customers require to meet their C&A requirements. When users buy service from Segovia, our network architecture, facilities, personnel standards, and security are all designed to move rapidly through the C&A process.

## MSM

***How difficult was it to obtain GSA Schedule 70 approval under the FCSA program? Can you describe to our readers what this award means and how it differs from previous regulations?***

## Andy Beegan

In general, the satellite industry hasn't leveraged the GSA contracts very often in the past. Segovia and the other early players were able to get through the process relatively quickly because we had demonstrated past performance and we understood the requirements of the process to activate the schedule.

Once the schedule is in place, customers can very quickly procure services from the industry. We all have line items on our schedule that can be used in combination to deliver the managed services our customers require. It streamlines the procurement process for customers and gives access to the industry in a way government has not had before.

Segovia was one of the very first companies to go through the FCSA/Schedule 70 award process. In Segovia's case, it took a few months to get through the process. There was a learning curve on both sides to ensure that expectations were met in terms of what was required and what could be provided.

## MSM

***One area where more and more industry involvement is becoming necessary is for first responders and NGOs and their need for crucial communications when confronting disasters, whether natural or manmade. How does Segovia address their communications challenges?***

## Andy Beegan

Segovia has been delivering services to first responder users since the very beginning. Those users are at the core of our business. We meet those challenges in several ways—with pre-positioned, always-on networks and with quick-turn activation of private networks with customer design features. Segovia has an always-on network in place globally; when a disaster happens, users can access the network with their existing remote satellite terminals already in place.

We have other customers with the larger charter to support disaster recovery, domestically or internationally. Those users typically leverage private network services from Segovia, dedicated to that customer's requirements. They use that network for exercise support and real-time disaster recovery missions when they need it.

## MSM

***The growth of companies within our various industries truly depends upon the ability to call upon an educated workforce to develop product. Is Segovia involved in any STEM projects to help drive interest among today's students to enter the satellite communications industry? How important do you see STEM being for the growth of your company?***

## Andy Beegan

From Segovia's earliest, most entrepreneurial days, we've had an intern program every summer for high school and college students. They take on real tasks at the company. We work with the local high schools and universities to provide those opportunities – and by doing so, we are constantly bringing new ideas into the company, rather than just resting on the ideas that have made us successful to date. University students get exposure to developing technology before it becomes commercialized, and Segovia benefits by bringing new ideas into the organization.

## MSM

***Given the technical nature of Segovia product, QoS is important, as is customer training — how is such accomplished by your Company?***

## Andy Beegan

Segovia is only successful if the customer is content with the quality of service they receive. We accomplish quality of service through careful design at space segment, teleport, and terrestrial layers, making sure that our users' applications run optimally from end-to-end. From an application perspective, quality of service can't be guaranteed from space segment alone.

Our service is successful provided we've done all we can to teach the customer how to use it. We do what we can to make it as intuitive as possible. Once they are on board, we provide instruction on how to use the remote satellite terminal, and how to interface with Segovia. Calling into the network operations center, getting information on open tickets, understanding network performance reports — all those things are critical to ensuring that their experience is as positive as it can be.

## MSM

***What is the future for satellite-based content delivery for government and military applications, especially in the latter regard, where timeliness and efficacy offset loss of life?***

## Andy Beegan

Military satellite and commercial satellite architectures are beginning to merge, which is a benefit to government users. Video, voice, and data applications are becoming more sophisticated, and the bandwidth requirements for those same applications today continue to increase. Demand for that bandwidth will not be able to be accommodated on the Ku-band available today. Those needs can be met easily on the Ka-band, delivering an order of magnitude bandwidth increase to very small terminals. Going forward based on our success in the Ku- and C-band world, Segovia will be taking a leadership position in the Ka-band through the Inmarsat Global Xpress offering. We are making certain that our network is architected from the ground up with the same security measures in mind.

In particular, the efficiency of video delivery to airborne users is an application in which Global Xpress will be able to differentiate itself. High-quality video to and from airborne users, at multi-megabit speeds, is something that's impossible on other platforms today.

The cross-pollination between commercial and military satellite will allow organizations to use their remote networks for traffic directly into Department of Defense and commercial facilities alike. We're seeing those discussions taking place right now. Global Xpress is the catalyst for many of those discussions with most of the service elements and Department of Defense leadership community. Segovia is making sure that the Global Xpress architecture meets their requirements, both as they exist now and as they are forecasted to be for the next 15 to 20 years.

## MSM

Looking over your professional career, what products or projects bring a smile to your face and a true sense of satisfaction?

## Andy Beegan

In the government market, we are only successful if we are able to effectively match our customers' requirements with a viable contract vehicle and a repeatable execution plan. Given this dynamic, an extraordinary amount of effort is spent on the proposal process. It's the one place where each side gets an idea of exactly what's needed, and exactly what can be provided to meet those needs.

The proposal process brings a lot of satisfaction in the end. When Segovia executes effective capture management and proposal generation, and we receive an award at the other end, it could be the result of years of work. And when we start activating terminals after contract award, that's very satisfying. This is what makes Segovia successful.

# RECONNECTING VICTIMS IN DISASTER ZONES

author: Thierry Schott, Aid and NGO Head Account Manager, Vizada

**Planning to restore communications in the event of a natural or man made disaster can be a daunting task, to say the least. One must consider a multitude of scenarios and plan for the worst. One such option to consider would be a *rapid mobile deployment unit* (RMDU).**


**Generally speaking, an RMDU has the following features: rapidly deployable, telescoping mast, off-grid power solution, equipment enclosure, communications capacity and coverage solution, backhaul solution and command and control elements. In selecting a partner for such a solution one should consider a vendor with a breadth of knowledge and experience in all the technical disciplines that make up an RMDU.**

With the correct satellite communications services, emergency respondents can exchange vital information with their head offices so that they can better understand the situation on the ground, and ground troops can better understand the global context. With quick and reliable communications the affected populations will also be able to communicate with the outside world, and find food, other vital supplies and emergency housing.

For 13 years, **Télécoms Sans Frontières** (**TSF**) has been at the forefront of emergency disaster relief. Their mission is to set up emergency satellite communications provisions, both voice and Internet, for the local population and also to aid other NGOs (such as **Médecins Sans Frontières** and **Oxfam**) with their work. These partner NGOs are given a data connection, technical assistance, access to free calls, and trouble-shooting equipment, as required.

*Jean-François Cazenave*, co-founder and President of TSF, explained, "You have to understand that even when the pre-existing network is working in an emergency situation, everything is saturated and the network ceases to function. The network cannot tell the difference between a non-emergency call, and the head of an aid agency calling his Government. This is why we need to use satellite communications in every single crisis situation."

**Transit Camp on the Libyan/Tunisian Border**

TSF has been supported by **Vizada** since 1998. Vizada provides TSF with funding and also hardware to be used on the ground. *Thierry Schott*, Aid and NGO Head Account Manager at Vizada, said, "The sponsorship between Vizada and TSF allows us to share our experience and benefit from each others' knowledge. Speed is always essential in our missions with TSF, and this is a lesson which carries over to our commercial customers. TSF are also able to benefit from Vizada's experience of satellite communication needs at the highest level."

TSF is a partner of the **European Commission**'s *Humanitarian Aid* department (**ECHO**) and has been designated *First Emergency Telecoms Responder* within the *United Nations Emergency Telecommunications Cluster* (**ETC**), meaning that TSF is among the first to arrive at the heart of an emergency. Jean-François said, "We have to be there quickly. In the aftermath of an earthquake, you only save lives within the first few hours. For example, the earthquake in Haiti occurred on the 12th January 2010 at 5:00 p.m.; we opened the first telephone line for their Prime Minister on the morning of 14th January."

When working with TSF, Vizada learned that finding the right hardware is essential — there is no time for the TSF team's equipment to be delayed in customs. Any hardware that the TSF team takes with them must be small enough to carry as hand luggage on the plane or helicopter; for example, handheld satellite phones.


**Transit Camp on the Libyan/Tunisian Border**

The importance of having Vizada customer care on-hand at all times cannot be understated. Throughout every mission Vizada provides 24/7 customer care support and advice on telecommunications to TSF, including advice on money-saving through using the right equipment, airtime packages and solutions and settings configurations. For example, Vizada might advise which portable satellite terminals will receive the best signal in a particular area. TSF will also have constant access to Vizada online traffic tools and services, so that their managers can directly activate their airtime account and act independently in an emergency, if needed.

The current situation in Libya is a classic example of the importance of having a fully functioning satellite communications network set up quickly on the ground. Since February 2011, TSF has been conducting humanitarian calling operations at the entrance to the transit camp on the Libyan/Tunisian border. Jean-François said, "We decided to go to Libya because we had heard reports of displaced people. We contacted Vizada and requested some voice terminals to be ready for very quick deployment; we had satellite mobile phones within 24 hours, and they also provided us with advice on networks, funding and other hardware.

"We arrived on the 23rd of February, with thousands of refugees already waiting for us. We were the first to arrive along with the Tunisian government, the European Commission, the UN, IOM (International Organization for Migration), ICRC (International Committee of the Red Cross) and Red Crescent (a humanitarian NGO). We set up a portable satellite terminal network in Tunisia, just 25 metres from Libya."

There are just 20 TSF staff in Libya, and tens of thousands of displaced families. The team work a minimum of 14 hour days, seven days per week. To date, more than 38,000 3-minute international phone calls (76,700 minutes) have been made from the camp on the Tunisia/Libya border by 28,500 displaced people. On March 20th, for 70 percent of the refugees who benefited from TSF's humanitarian calling operations, the call was the first one they made since the beginning of the uprising.

These calls allow the agencies to assess the nature of the crisis. For example, TSF is able to track which countries the calls are made to, which allows them to identify the nationality of the refugees and request support from their respective Governments. These reports are transferred automatically via email through the satellite terminal back to TSF's headquarters in Pau, France.

TSF and Vizada have learned to be flexible when dealing with crises such as Libya, and Jean-François describes every mission as a learning curve. Mid-mission in Libya, TSF were forced to request more data terminals be sent to them, due to the sheer volume of displaced refugees arriving at the camp. For this reason, *Thierry* believes that flexibility and speed of response is absolutely vital in the NGO environment. He said, "By working closely with TSF we are able to tailor our communications advice to enable them to respond quickly to the complex needs of their team, and of the teams for the other NGOs. My team has had to be just as efficient in order to provide TSF with the best service possible."

No-one can predict when the conflict in Libya will end, and the refugees will be able to return home. Vizada is pleased to have been able to make a difference in a conflict affecting so many. Thierry said, "It has been great to see how satellite communications can make a real and tangible difference to people living in the more dire situations. I think it is safe to say that we will be happy to work with TSF for as long as they need us to provide communications and data assistance."

*About the authors*

Thierry Schott is a Key Account Manager with Vizada, managing sales and business development for the Humanitarian and NGO Markets in EMEA & Asia. He has been with Vizada since 2007 and has managed accounts in a number of key vertical markets worldwide.

# The BIG Book of Satellite Communications

*Still at Your Finger Tips After 26 Years.*

## The 2011 International Satellite Directory


Visit: www.satnews.com/directory

The Directory is a comprehensive guide to the people, companies, products, services and the market of the booming satellite industry. With changes of all kinds affecting this dynamic industry, the Directory remains a powerful tool, mapping in detail an otherwise uncharted and complex segment of modern communications.

**NO RISK GUARANTEE!**
We firmly believe that the International Satellite Directory will be so invaluable to you that we guarantee it. Use the Directory and if you are not totally satisfied, simply return it to us within 21 days of receipt for a full prompt refund.

**Directory Contents Includes:**

- International Agencies
- Manufacturers of Satellites and Space Equipment
- Manufacturers of Satellite Ground Equipment
- Network Systems
- PC-Satellite Connectivity
- Users of Satellite Systems
- Providers of Satellite Services
- General Services
- Satellite Operators
- Geosynchronous Satellites
- EIRP Maps
- Uplink Facilities
- Buyer's Guide and Index