COTS Journal

Mobile Ad Hoc Networking Revamps Military Communications

By: Chris O'Rourke, Technical Marketing Manager Cisco Systems Stephen B. Johnson, Customer Support Engineer Extreme Engineering Solutions

With massive amounts of real-time military ISR data to disseminate, traditional networking schemes can't keep up. What's needed are mobile net technologies that deliver the reliability and flexibility required on the deployed edge.

Driven by technologies such as data networking, GPS, real-time video feeds from UAVs, and satellite intelligence, today's modern military has access to a plethora of real-time data. However, getting this information to the warfighter at the "edge of the network" is still problematic. Getting real-time voice, data and streaming video to the warfighter at the edge is no easy task. Networking infrastructure might be in place on the battlefield, though typically it cannot support the heavier requirements of new, feature-rich applications. Soldiers are mobile and need high-performance, high-bandwidth networks that move with them to deliver the information they need.

The U.S. DoD has standardized on IP networks to achieve the goals set out in the high-level Global Information Grid (GIG) and Network Operations (formerly Network Centric Warfare) doctrines. The goal for Network Operations is to provide seamless access to timely information to all warfighters and decision makers at every level in the military hierarchy. This enables soldiers, ground vehicles, aircraft and command centers to shape collected information into a coherent, accurate view of the battlefield.

Mobile Network Building Blocks

A portion of a military IP network can be based on fixed wired infrastructure, utilizing satellites and networking equipment in operations and command centers. But it isn't practical or even possible to create a fixed, wired network infrastructure on a battlefield; the only practical way to provide a networking infrastructure is to create a mobile wireless network. Since most soldiers are typically in or near some sort of vehicle, an effective way to create a mobile wireless network is to make use of vehicles such as Humvees, Strykers and Bradley Fighting Vehicles to carry the infrastructure necessary to build and maintain these networks on the move (Figure 1).

Mobile wireless networks are built using a variety of IP-enabled radios and specialized embedded network routers. Network infrastructure radios are called backhaul radios, which can communicate with other backhaul radios or with satellites. Each backhaul radio is connected to an IP-router to create a network node.

At the "edge of the network" are a variety of clients. Dismounted soldiers carry some, such as handheld radios, man-pack radios, laptops, cameras and PDAs; multiple clients can connect wirelessly to the same IP network node. There are also a variety of clients that reside inside vehicles. Often an Ethernet switch is interfaced to the router in a vehicle, providing a vehicle local area network (LAN), for clients such as radios, laptops, battlefield display systems and mission-control computers. This enables the same IP-networking system in a vehicle to support both internal vehicle and external vehicle communications simultaneously. For example, externally mounted cameras will stream video feeds to the dashboard utilizing the vehicle LAN, while in-vehicle and dismounted soldiers communicate with each other and with remote C2 installations utilizing the mobile wireless network.

Unique Challenges of Mobile Wireless Networks

The Internet was built on a fixed, static, wired infrastructure. More recently, there have been great strides in wireless and mobile connectivity. However, in the consumer and commercial world, wireless and mobile users still rely on a fixed, static, wired infrastructure. Cellular and Wi-Fi base stations and wireless routers are tied into the core networks with routing infrastructure, known gateways and Quality of Service. As a wireless or mobile user, you have to play within the rules; wireless connectivity works great in highly populated areas because that is where the infrastructure investment has been made. But as you move away from population centers, your wireless connection will be less likely to work because of the lack of infrastructure and radio coverage.

With fixed wired networks, the network nodes are fixed, and the only components that move are clients that are not used to route other traffic, such as cellular and Wi-Fi-enabled devices. On the battlefield, not only are the clients mobile, but so are the basic building blocks of a mobile wireless network, for example the radios and specialized embedded routers. This creates a fluid and ever-changing network with dynamic nodes and frequent routing table changes. These are referred to as mobile ad hoc networks.

Mobile Ad Hoc Networks

A Mobile Ad hoc NETwork (MANET, pronounced m?-n?) provides a means for delivering the benefits of IP networking to users operating beyond the reach of a fixed network. It is a self-configuring, infrastructure-less network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and therefore, will change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore participate in the routing of traffic. The primary challenge in building a MANET is equipping each network node to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to a larger network. In ad hoc networks, mobile nodes associate on an extemporaneous or ad hoc basis. Ad hoc networks have numerous distinguishing characteristics when compared with conventional networking solutions. Figure 2 lists those characteristics.

Ad hoc networks deliver a compelling advantage wherever highly mobile warfighters, unsupported by fixed infrastructure, need to share IP-based information. They offer superior information-sharing at all levels, enabling improved situational awareness, a clearer understanding of leader’s intent, and the ability for remote users to self-synchronize. The fact that they’re self-forming and self-healing facilitates deployment and minimizes the need for manual configuration and intervention. Meanwhile, their multi-hop networking nature extends network coverage and provides redundant paths for increased resilience. With ad hoc networks you also have the ability to operate with or without connectivity to a centralized network. Such networks are a key enabler for new applications such as vehicle-to-vehicle networking, intelligent transportation systems, sensor networking, telemetry monitoring and more.

Specialized Embedded Routers Are Key

Traditional network infrastructure routers are designed to work with fixed, mostly static networks with known neighbors. When there is a change to the network infrastructure requiring a change to the way packets are routed, routing tables have to be updated and propagated. Network operators in the fixed networks know the paths available and can engineer the routing changes using costing in the rare cases where neighbors change. There is typically the luxury of having monitoring points alarm to a network operations center (NOC) in the event of such network events. There can be months of planning for network or routing changes within known maintenance windows. A traditional network router would not cope with dynamic routing table changes that can occur with nodes participating in a MANET.

Weather, terrain and mobility make radio-based communications dynamic; therefore, routers must be aware of each radio’s condition in order to make effective routing decisions with built-in mechanisms to prevent constant re-routing and human intervention. Mobile networks delivering real-time services, such as video and data, cannot

tolerate prolonged network disruptions as the network changes due to radio dynamics. To address this challenge, IP routers are deployed with technology to minimize network disruption due to network reconvergence. These routers support features such as radio-aware routing, traffic optimization, firewall/network security and voice services.

Dynamic Link Exchange Protocol

The Dynamic Link Exchange Protocol (DLEP) is the latest protocol in the Radio Aware Routing (RAR) family of protocols that enable communications between a router and a radio in a mobile ad hoc network (Figure 3). It enables a radio to provide a router with information about the quality of links between radios and can report on the presence or loss of potential routing neighbors. Key to the concept of RAR protocols is that a router may connect to a radio using standard Ethernet, but the radio can convey information about the true characteristics of the over-the-air radio links to the router, including the actual available bandwidth, delay, or link quality. This functionality is especially critical with today's dynamic radio waveforms, which can vary frequencies and power based on current conditions in real time. The resulting changes in bandwidth or other characteristics must be communicated to a router using the radio channels in order to apply QoS or to communicate metric information within routing protocols.

The actual available bandwidth to any given radio neighbor may in fact be different from any other neighbor, and certainly may be different from the bandwidth of the physical connection between a radio and a router. The bandwidth to any specific neighbor can also change and such changes need to be taken into account for both IP routing and Quality of Service. Neighbor up/down signaling enables routers to provide faster network convergence by reacting to link status signals generated by the radio, rather than waiting for protocol timers to expire. Routers can factor link quality metrics reported by radios into their OSPFv3- or EIGRP-based route cost calculations. Utilizing bandwidth metrics, routers can provide flow control for data to minimize the need to queue and buffer data in radios, allow voice to be prioritized over video when radio links are degraded, and provide consistent QoS for networks with multiple radios.

SWaP and Ruggedization

Mobile ad hoc networks for military applications pose hardware and platform challenges because many of today's networking devices must be optimized from a Size, Weight and Power (SWaP) perspective and also be made to work reliably in harsh environments. In the peer-to-peer world, anybody or anything that moves can potentially be a wireless networking node. Military ad hoc networking requires a variety of platforms, ranging from vehicle-based to hand-carried or wearable, and all offering equivalent network services.

Whether a router and a Gbit Ethernet switch are deployed in a small two-slot box to provide network connectivity and an in-vehicle LAN, or a router is being integrated into a vehicle's existing mission control computer, such as solutions based on the Extreme Engineering Solutions (X-ES) XPand5200 ½-ATR enclosure (Figure 4), space and power are at a premium. And the hardware needs to be able to survive the harsh environment in a vehicle on the battlefield. Size, weight and power are even more critical for clients carried by dismounted soldiers. Astonishingly, today's infantryman carries approximately 130 pounds of gear.

The ability to integrate the router technology into existing deployed systems and the ability to easily upgrade the equipment as technology changes are important factors. Many systems deployed in vehicles are based on the industry standard VME, 3U CompactPCI, 3U VPX, or PC/104 form factors. These form factors offer excellent ruggedized, conduction-cooled implementations. Choosing an industry-standard, COTS-based router, such as the 3U CompactPCI Cisco 5940 Embedded Services Router, makes it easy to add functionality to existing systems. It also provides flexibility for future upgrades, and it makes it much less likely that the user will get locked into a proprietary design.

Network Solutions for the Dynamic Environment

While the challenges presented by tactical networks are unique, COTS routing technologies are available to deliver network services optimized for dynamic environments. These embedded routers are key to deploying the rich set of applications and service that today's warfighters require. When these ruggedized, embedded routers are coupled with today's high-performance, IP-enabled radios, they do much more than just create mobile ad hoc networks. They help ensure that the networks and the data are highly secure, critical applications are prioritized, and bandwidth is optimized. They deliver vital data to dismounted soldiers, such as live streaming video from UAVs overhead. They allow commanders to get a total, integrated view of the battlespace. They have even allowed the President of the United States to view Navy SEAL operations in real time, half a world away in Pakistan.

What the Future Holds

It is easy to predict what will happen in the future for mobile, ad hoc military networks simply by looking at what is happening in the commercial world. There will be increasing bandwidth demands from an ever-growing list of rich services and applications, as has happened as a result of the explosion of smartphones. There will be a proliferation of connected nodes as the technology is integrated into more clients. This will be driven by the need to continually reduce the SWaP of the radios, routers and embedded systems used to create the communication systems and tactical networks. We will see a variety of industry-standard COTS form factors to support clients and nodes, ranging from dismount to ground vehicle to airframe solutions. Likely form factors will be 3U VPX, XMC, and other emerging small form factors (SFFs).

The demand for smartphones, laptops and tablets is driving the tremendous growth in commercial wireless networks. These same technologies are helping to create mobile, wireless, ad hoc networks for the military. Key to creating these military networks is router technology taken from the commercial world and modified to support the mobility of these networks and the harsh environment of the battlefield. Ruggedized, embedded routers with Radio Aware Routing are helping achieve the goals set out in the Network Operations doctrine.

Cisco Systems

San Jose, CA.

(408) 526-4000.

[www.cisco.com]. (http://www.cisco.com)

Extreme Engineering Solutions

Middleton, WI.

(608) 833-1155.

[www.xes-inc.com]. (http://www.xes-inc.com)