Mobile Networking – Enabling Homeland Security via Rapidly Deployable, Secure Communications

The Challenge

One of the major requirements for homeland security is the ability to rapidly deploy secure communications networks in a variety of environments. Such environments range from deployment in urban areas that already have extensive existing public infrastructure to remote areas with little or no existing communications infrastructure and formidable terrain. The former is likely to be the case for terrorist attacks within the borders. The latter is the case often encountered by the military. The communications networks should enable various sections of the local, state, and federal first response units, as well as the federal and international defense agencies to communicate with each other securely. The use of Internet technology, in particular, mobile-IP, can fulfill many of these requirements today. However, a few issues need to be investigated related to sharing network resources, namely: security over public networks, mixing of public and private networks, and network scalability.

The Importance of Shared Infrastructure

The events of September 11, 2001 showed the importance of communication between agencies, and that this capability is currently lacking. In addition, the ability to exploit a multitude of communication networks, both private and public, came through loud and clear. It is well documented that the phone systems became overloaded, as certain infrastructure was destroyed and other infrastructure overwhelmed. However, other communication networks that deployed Internet technologies were still operational. These systems proved invaluable to security and rescue personnel. ***The ability to utilize any available communications links for <u>mobile networks</u> will provide an even greater benefit.***

The following are two such examples of the utility of the Internet in times of crisis:

> "New York city rescue leaders had been using conference calls on traditional telephone lines to plan their days, but some had to wait up to two days to get a conference together, because of extensive damage to telephone networks in the New York City area.
>
> The Ricochet network, a wireless Internet service provided my Metricom provided Internet access in the area surrounding where the World Trade Center towers once stood." [1]

> "On Sept. 11, the SANS (System Administration, Networking and Security) Institute of Bethesda, Md., was holding an information security training conference at Boston's Park Plaza Hotel.
>
> "At the very end of the hall there was a federal conference," SANS' Steven Northcutt recalled. There were no signs advertising it, but the attendees were clearly law enforcement types, said Northcutt, himself a former government worker.
>
> The feds were asking to use the SANS access points, Northcutt said. By a combination of e-mail and America Online Instant Messenger software, the federal agents managed to communicate with their offices and went on their way." [2]

A significant problem with emergency systems is that they are only used during times of crisis. When the system breaks or degrades, often it is not discovered until the system is needed. This problem can be combated with routine maintenance checks, but due to the time required and tedium of the job this is frequently ineffective. As budgets become constrained, routine maintenance suffers. ***Experience with Public Safety communication systems has shown that the most reliable systems are the ones that are exercised daily. The problems are found and fixed on a regular basis and there are no surprises when an actual emergency arises.***

A shared infrastructure will be exercised every day. Thus, it is more dependable and more cost effective to maintain than fully closed communications system. The public users have the system under a constant test. This is especially valuable in remote areas, as an emergency might not occur for months or years.

Outline

This white paper provides a brief description of mobile networking using Internet technologies as well as issues that need to be addressed before full deployment is possible in an operational network. The topics that will be discussed include:

- The mobile-IP protocol;
- The benefits that mobile networking will provide;
- The various issues associated with deploying these protocols in a manageable, scalable and secure manner;
- Ongoing USCG network deployment to systematically address these issues;
- Remaining work, and,
- Related activities within the IETF

Mobile-IP

What Is It?

Mobile-IP was developed to address wireless networks, but can work equally well in a wired environment. Mobile-IP is an Internet protocol that permits Internet nodes (hosts and routers) to seamlessly "roam" among IP subnetworks and media types. Transport layer connections are maintained across network moves. Mobile IP allows a mobile node to be reachable at a fixed IP address, its identity, (called its *home address*) irrespective of its current point of attachment to the Internet. This is extremely useful for security and as well as authentication, authorization and accounting (AAA). In addition, by maintaining your network identity, real-time "peer-to-peer" networking is possible.

For the past few years, Mobile-IP implementations have been available that address mobile hosts, but not mobile networks. Cisco Systems has recently developed a ***mobile router*** implementation that has been commercially available since October of 2001.

Mobile host implementations of mobile-IP require each host, whether laptop computers, Internet-enabled video cameras, or IP telephones to run their own client software. This makes mobile-IP deployment problematic – particularly if an entire network is mobile. Mobile router technology solves this problem as the router takes care of all the mobile issues and all machines connected to the router can run their conventional software with their conventional configurations. No user intervention is necessary.

How It Works

Mobile-IP works by having the mobile nodes keep a designated system (called its *home agent*) abreast of their current address, in much the same manner that you may leave a forwarding address at the post office so your letters immediately get re-sent to your current location. A good way to think about it is by analogy to the concept of universal phone numbers. Mobile-IP gives you a universal IP address via which your system is always reachable regardless of its current point of attachment to the Internet.

To offer Mobile IP services, service providers or enterprises need a home agent (router or Layer 3 switch) that serves as the anchor point for communications, and either a mobile router (or routers) or mobile devices such as personal digital assistants (PDAs), laptops, and cellular phones equipped with Mobile IP client software. ***Note that any device attached to mobile router does not have to have special client software.*** Foreign agents[i] (router or Layer 3 switch) are required in various locations that deliver packets from the home agent to the mobile device. These foreign agent routers can be provided by a third party and shared among various enterprises. The only requirement is that the foreign agent router can provide connectivity back to the enterprise's home agent
[Fig. 1].

Benefits and Applications

The advantage of mobile-IP technology is the mobile network configurations do not require reconfiguration when changing network attachment points.

Mobile IP maintains control and authentication at the IP level instead of at the physical layer in the radio link,

[i] Foreign agents are simply normal routers with mobile-IP capability and foreign agents service enabled.

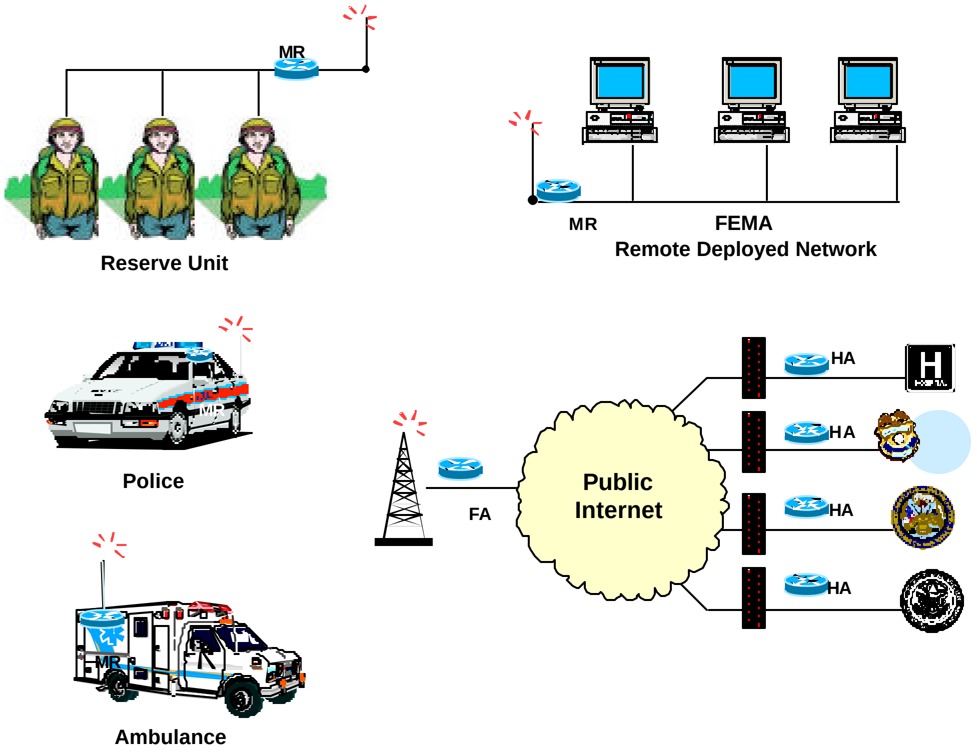

Figure 1: Shared Network

making the hand-over process between ISPs, or foreign agents, transparent to the user.

As you move from one foreign agent to another, your previous connection is removed and a new connection is set up. It works across wireless LANs, CDMA, GSM, and satellite, so it is unaware of link type. Thus, mobile-IP enables communication between various factions over shared infrastructure in a secure manner.

Now we can have EMS, local security forces, the FBI, the National Guard, the Federal Emergency Management Agency (FEMA), and trucking companies all using the same infrastructure (and paying their shared cost to the infrastructure provider).

Paramedics can transmit a patient's vital signs to awaiting doctors continuously, right from the ambulance even while it is moving from the disaster site to the hospital. Hospitals can notify the ambulance as to availability or if the patient should be transported to a better equipped or less busy hospital. Treatments can be initiated while in transit, saving precious minutes.

A police cruiser can be in constant contact with headquarters. A mobile router onboard the cruiser enables voice, video and data transmission simultaneously. Video of the onsite situation can be remotely viewed. Also, video can be transmitted while the cruiser is in transit. Images can be sent to or received from HQ. Documents and pictures are now available to the law enforcement officers wherever they may be.

Emergency agencies can rapidly deploy remote offices without the need for networking and communication experts. Agencies such as FEMA can be connected instantaneously upon arrival at a disaster site.

The National Guard can set up remote communications using the same infrastructure. They can be sharing information with the FBI, the local authorities, and disaster relief agencies in real time over the same shared network.

If for some reason, the public infrastructure is not available, other communication networks can be used. Satellites networks that offer foreign agent services at their ground stations are equally suited to address this emergency situation.

So, who pays for this communications infrastructure? Everybody that uses it, but mostly private companies and local governments – companies such as local trucking and freight delivery, and local public safety. These groups will utilize the network on a daily basis for voice communications, tracking information and inventory. In addition, the wireless ISP would most likely offer services to individuals and public transportation so people can be connected to their corporate Intranets reading email and sharing documents during their daily commute.

Issues

Mobile-IP technology, in particular mobile router is being deployed today by various defense agencies, both U.S. DoD and foreign defense agencies. These deployments currently ensure secure networks by utilizing closed networks.

To take full advantage of mobile-IP technologies during emergencies and disaster relief situations one should utilize all available communication paths possible. One must be able to utilize both their private Intranets and the public Internet in a secure manner. This will drastically reduce communication costs while simultaneously improving reliability, redundancy and ensure a robust communication capability during times of National and International emergencies and disasters. In order to fulfill this, the issues that need to be researched include:

- Development of scalable and manageable architectures;
- Mixing of public and private addressing;
- Interoperability of mobile protocols with corporate or agency proxy servers;
- Crossing corporate or agency firewalls securely;
- Encryption, key distribution and key management; and,
- Authentication, Authorization and Accounting for access to various communication infrastructures.

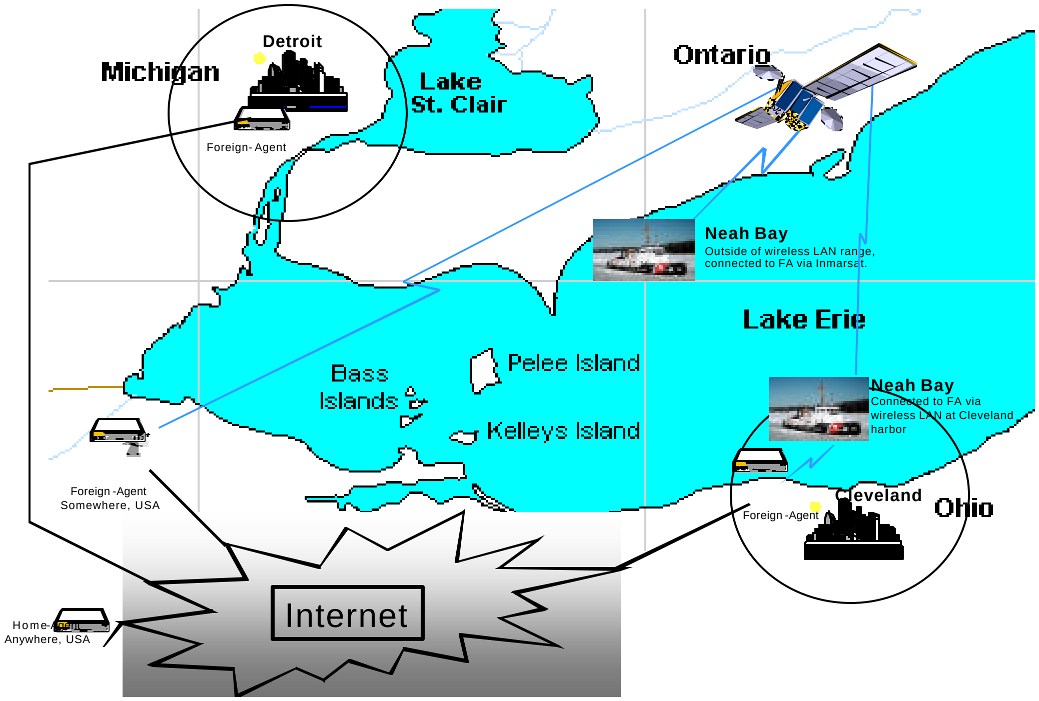

Figure 2: Neah Bay Mobile Router Project

United States Coast Guard Mobile Network Deployment

The Coast Guard Trial

The United State Coast Guard (USCG), NASA and Cisco Systems are working on a project to deploy mobile router technology in the USCG network. The main purpose of this project is to deploy mobile IP and mobile router technology in a real network in order to identify and address issues relate to real network deployment. Issues of particular interests include: operation in mixed private and public address space, sharing of network resources (antennas, wireless connections, etc…) wireless security, crossing firewalls and proxies, scalability and efficiency of operation due to multiple tunnels over low bandwidth satellite links.

The project team is equipping the icebreaker Neah Bay with a mobile router [Fig. 2, Ref. 3]. When the ship is at or near its home port on Lake Erie, it would access the network via Cisco Aironet wireless 802.11b Ethernet antennas on the Federal Building in downtown Cleveland[ii]. As the ship moves about the Great Lakes, it will access the network via foreign agents deployed along the main shipping channels. Detroit will be one of the initial deployments. When the ship is out of range of the terrestrial links, it will access the Internet via satellite links that cover the Great Lakes. Routers serving as foreign agents will be located at satellite ground terminals in places

[ii] In recent tests in November of 2001, we were able to obtain 1 Mbps transmission over 16 nautical miles using 802.11b commercial-off-the-shelf (COTS) equipment.

such as Southbury, Connecticut or Smith Falls, Canada. Both INMARSAT and Globalstar satellite systems are being considered for use.

The Neah Bay is designed primarily for icebreaking, but it also carries out secondary missions in law enforcement, environmental protection, search and rescue, and navigational aid. In the law enforcement mission's drug-interdiction role, Coast Guard units need to exchange information about persons intercepted at sea as a result of antidrug and terrorist operations. With mobile router technology and by deploying a combination of terrestrial wireless and satellite links, the Coast Guard can access information any time, anywhere to fulfill this need.

The Coast Guard increasingly is moving to electronic transmission of many of its paper forms. That's great on the shore side but currently it is hard for ships if you do not have that connectivity at sea. Being connected at sea would be especially helpful here.

By deploying mobile router technology over shared networks, the USCG will reap numerous benefits. There will be substantial saving in communication infrastructure cost as they will be able share the infrastructure costs with other government agencies (both local and foreign), the shipping industry and pleasure boaters [Fig 3]. The USCG will have the ability to be connected even while at sea. In addition, the USCG will not have to deploy information technology experts onboard their ships since mobile router only has to be configure once and then operates autonomously, a truly “set and forget” technology.

Remaining Work

Although the initial infrastructure deployment allows for transmission over the public Internet as well as the USCG private intranet, many of the issues with sharing the wireless links in a secure manner and authorization, authentication and accounting need to be solved and demonstrated. By deploying additional antennas around strategic positions in the Great Lakes, such as on Pelee Island,

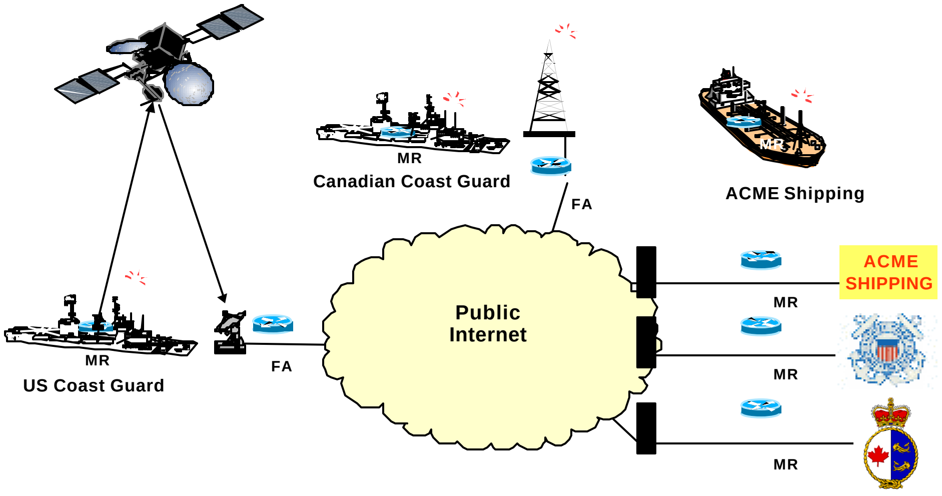

Figure 3: Shared Maritime Network

we can have a system in place that can be shared by the shipping industry, the USCG and the Canadian Coast Guard. This would allow any remaining issues related to shared, secure networks to be worked out collaboratively and cooperatively in an operational environment.

Related Industry Activities

There is a large amount of activity occurring in the commercial communication industry via the Internet Engineering Task Force (IETF) to provide communications over shared networks in a secure manner as well as addressing mobile communications. The cellular phone industry is one prime example. Some of the pertinent working groups include: Mobile-IP (mobile-ip), Mobile Ad hoc Networks (manet), Mobile Networks (monet), IP Security (ipsec) and Secure Internet Key Distribution (siked).

Because of the events of September 11, 2001 and the effectiveness of the Internet to provide communication services, a new group, Internet Emergency Preparedness (ieprep) has been created. Its mission is to provide recommendations for the Emergency Telecommunications Service using existing protocols. This group will determine what can be done with existing protocols and what can not be done.

Conclusion

The ability to utilize all forms of communication while mobile or in a rapid deployment situation greatly enhances the ability of the Government to provide a safe secure environment and to respond to emergency situations. The ability to share networks ensures a reliable, robust communications network and creates an environment for collaborative infrastructure cost sharing. Although the pieces are in place to allow for shared networks, additional work needs to be performed to ensure the security of such networks – particularly when those networks are mobile.

For further information, contact:
William D. Ivancic
NASA Glenn Research Center
(216) 433-3494
wivancic@grc.nasa.gov

[1] Ben Charny: Ricochet rebounds at WTC ground zero, CNET News.com, October 1, 2001, 1:00 PM PT

2 William Jackson: Attacks Show Net's Strength, Weakness, GCN, September 24, 2001; Vol. 20 No. 29

[3] D. Stewart, W. Ivancic, T. Bell, B. Kachmar, D. Shell, K. Leung: Application of Mobile Router to Military Communications, Milcom 2001, October 2001