Network Working Group
Request for Comments: 1677
Category: Informational

B. Adamson
Naval Research Laboratory

August 1994

Tactical Radio Frequency Communication Requirements for IPng

Status of this Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

This document was submitted to the IETF IPng area in response to RFC 1550. Publication of this document does not imply acceptance by the IPng area of any ideas expressed within. Comments should be submitted to the big-internet@munnari.oz.au mailing list.

Executive Summary

The U.S. Navy has several efforts exploring the applicability of commercial internetworking technology to tactical RF networks. Some these include the NATO Communication System Network Interoperability (CSNI) project, the Naval Research Laboratory Data/Voice Integration Advanced Technology Demonstration (D/V ATD), and the Navy Communication Support System (CSS) architecture development.

Critical requirements have been identified for security, mobility, real-time data delivery applications, multicast, and quality-of-service and policy based routing. Address scaling for Navy application of internet technology will include potentially very large numbers of local (intra-platform) distributed information and weapons systems and a smaller number of nodes requiring global connectivity. The flexibility of the current Internet Protocol (IP) for supporting widely different communication media should be preserved to meet the needs of the highly heterogeneous networks of the tactical environment. Compact protocol headers are necessary for efficient data transfer on the relatively-low throughput RF systems. Mechanisms which can enhance the effectiveness of an internet datagram protocol to provide resource reservation, priority, and service quality guarantees are also very important. The broadcast nature of many RF networks and the need for broad dissemination of information to warfighting participants makes multicast the general case for information flow in the tactical environment.

Background

This paper describes requirements for Internet Protocol next generation (IPng) candidates with respect to their application to military tactical radio frequency (RF) communication networks. The foundation for these requirements are experiences in the NATO Communication System Network Interoperability (CSNI) project, the Naval Research Laboratory Data/Voice Integration Advanced Technology Demonstration (D/V ATD), and the Navy Communication Support System (CSS) architecture development.

The goal of the CSNI project is to apply internetworking technology to facilitate multi-national interoperability for typical military communication applications (e.g., electronic messaging, tactical data exchange, and digital voice) on typical tactical RF communication links and networks. The International Standard Organization (ISO) Open Systems Interconnect (OSI) protocol suite, including the Connectionless Network Protocol (CLNP), was selected for this project for policy reasons. This paper will address design issues encountered in meeting the project goals with this particular protocol stack.

The D/V ATD is focused on demonstrating a survivable, self-configuring, self-recovering RF subnetwork technology capable of simultaneously supporting data delivery, including message transfer, imagery, and tactical data, and real-time digital voice applications. Support for real-time interactive communication applications was extended to include a "white board" and other similar applications. IP datagram delivery is also planned as part of this demonstration system.

The CSS architecture will provide U.S. Navy tactical platforms with a broad array of user-transparent voice and data information exchange services. This will include support for sharing and management of limited platform communication resources among multiple warfighting communities. Emphasis is placed on attaining interoperability with other military services and foreign allies. Utilization of commercial off-the-shelf communications products to take advantage of existing economies of scale is important to make any resulting system design affordable. It is anticipated that open, voluntary standards, and flexible communication protocols, such as IP, will play a key role in meeting the goals of this architecture.

Introduction

Before addressing any IPng requirements as applied to tactical RF communications, it is necessary to define what this paper means by "IPng requirements". To maintain brevity, this paper will focus on

criteria related specifically to the design of an OSI model's Layer 3 protocol format and a few other areas suggested by RFC 1550. There are several additional areas of concern in applying internetwork protocols to the military tactical RF setting including routing protocol design, address assignment, network management, and resource management. While these areas are equally important, this paper will attempt to satisfy the purpose of RFC 1550 and address issues more directly applicable to selection of an IPng candidate.

Scaling

The projection given in RFC 1550 that IPng should be able to deal with 10 to the 12th nodes is more than adequate in the face of military requirements. More important is that it is possible to assign addresses efficiently. For example, although a military platform may have a relatively small number of nodes with requirements to communicate with a larger, global infrastructure, there will likely be applications of IPng to management and control of distributed systems (e.g., specific radio communications equipment and processors, weapons systems, etc.) within the platform. This local expansion of address space requirements may not necessarily need to be solved by "sheer numbers" of globally-unique addresses but perhaps by alternate delimitation of addressing to differentiate between globally-unique and locally-unique addressing. The advantages of a compact internet address header are clear for relatively low capacity RF networks.

Timescale, Transition and Deployment

The U.S. Navy and other services are only recently (the last few years) beginning to design and deploy systems utilizing open systems internetworking technology. From this point of view, the time scale for selection of IPng must be somewhat rapid. Otherwise, two transition phases will need to be suffered, 1) the move from unique, "stove pipe" systems to open, internetworked (e.g., IP) systems, and then 2) a transition from deployed IP-based systems to IPng. In some sense, if an IPng is quickly accepted and widely implemented, the transition for tactical military systems will be somewhat easier than the enterprise Internet where a large investment in current IP already exists. However, having said this, the Department of Defense as a whole already deploys a large number of IP-capable systems, and the issue of transition from IP to IPng remains significant.

Security

As with any military system, information security, including confidentiality and authenticity of data, is of paramount importance. With regards to IPng, network layer security mechanisms for tactical

RF networks generally important for authentication purposes, including routing protocol authentication, source authentication, and user network access control. Concerns for denial of service attacks, traffic analysis monitoring, etc., usually dictate that tactical RF communication networks provide link layer security mechanisms. Compartmentalization and multiple levels of security for different users of common communication resources call for additional security mechanisms at the transport layer or above. In the typical tactical RF environment, network layer confidentiality and, in some cases, even authentication becomes redundant with these other security mechanisms.

The need for network layer security mechanisms becomes more critical when the military utilizes commercial telecommunications systems or has tactical systems inter-connected with commercial internets. While the Network Encryption Server (NES) works in this role today, there is a desire for a more integrated, higher performance solution in the future. Thus, to meet the military requirement for confidentiality and authentication, an IPng candidate must be capable of operating in a secure manner when necessary, but also allow for efficient operation on low-throughput RF links when other security mechanisms are already in place.

In either of these cases, key management is extremely important. Ideally, a common key management system could be used to provide key distribution for security mechanisms at any layer from the application to the link layer. As a result, it is anticipated, however, that key distribution is a function of management, and should not dependent upon a particular IPng protocol format.

Mobility

The definition of most tactical systems include mobility in some form. Many tactical RF network designs provide means for members to join and leave particular RF subnets as their position changes. For example, as a platform moves out of the RF line-of-sight (LOS) range, it may switch from a typical LOS RF media such as the ultra-high frequency (UHF) band to a long-haul RF media such as high frequency (HF) or satellite communication (SATCOM).

In some cases, such as the D/V ATD network, the RF subnet will perform its own routing and management of this dynamic topology. This will be invisible to the internet protocol except for (hopefully) subtle changes to some routing metrics (e.g., more or less delay to reach a host). In this instance, the RF subnetwork protocols serve as a buffer to the internet routing protocols and IPng will not need to be too concerned with mobility.

In other cases, however, the platform may make a dramatic change in position and require a major change in internet routing. IPng must be able to support this situation. It is recognized that an internet protocol may not be able to cope with large, rapid changes in topology. Efforts will be made to minimize the frequency of this in a tactical RF communication architecture, but there are instances when a major change in topology is required.

Furthermore, it should be realized that mobility in the tactical setting is not limited to individual nodes moving about, but that, in some cases, entire subnetworks may be moving. An example of this is a Navy ship with multiple LANs on board, moving through the domains of different RF networks. In some cases, the RF subnet will be moving, as in the case of an aircraft strike force, or Navy battlegroup.

Flows and Resource Reservation

The tactical military has very real requirements for multi-media services across its shared and inter-connected RF networks. This includes applications from digital secure voice integrated with applications such as "white boards" and position reporting for mission planning purposes to low-latency, high priority tactical data messages (target detection, identification, location and heading information). Because of the limited capacity of tactical RF networks, resource reservation is extremely important to control access to these valuable resources. Resource reservation can play a role in "congestion avoidance" for these limited resources as well as ensuring that quality-of-service data delivery requirements are met for multi-media communication.

Note there is more required here than can be met by simple quality-of-service (QoS) based path selection and subsequent source-routing to get real-time data such as voice delivered. For example, to support digital voice in the CSNI project, a call setup and resource reservation protocol was designed. It was determined that the QoS mechanisms provided by the CLNP specification were not sufficient for our voice application path selection. Voice calls could not be routed and resources reserved based on any single QoS parameter (e.g., delay, capacity, etc.) alone. Some RF subnets in the CSNI test bed simply did not have the capability to support voice calls. To perform resource reservation for the voice calls, the CLNP cost metric was "hijacked" as essentially a Type of Service identifier to let the router know which datagrams were associated with a voice call. The cost metric, concatenated with the source and destination addresses were used to form a unique identifier for voice calls in the router and subnet state tables. Voice call paths were to be selected by the router (i.e. the "cost" metric was calculated) as a

rule-based function of each subnet's capability to support voice, its delay, and its capacity. While source routing provided a possible means for voice datagrams to find their way from router to router, the network address alone was not explicit enough to direct the data to the correct interface, particularly in cases where there were multiple communication media interconnecting two routers along the path. Fortunately, exclusive use of the cost QoS indicator for voice in CSNI was able to serve as a flag to the router for packets requiring special handling.

While a simple Type of Service field as part of an IPng protocol can serve this purpose where there are a limited number of well known services (CSNI has a single special service - 2400 bps digital voice), a more general technique such as RSVP's Flow Specification can support a larger set of such services. And a field, such as the one sometimes referred to as a Flow Identification (Flow ID), can play an important role in facilitating inter-networked data communication over these limited capacity networks.

For example, the D/V ATD RF sub-network provides support for both connectionless datagram delivery and virtual circuit connectivity. To utilize this capability, an IPng could establish a virtual circuit connection across this RF subnetwork which meets the requirements of an RSVP Flow Specification. By creating an association between a particular Flow ID and the subnetwork header identifying the established virtual circuit, an IPng gateway could forward data across the low-capacity while removing most, if not all, of the IPng packet header information. The receiving gateway could re- construct these fields based on the Flow Specification of the particular Flow ID/virtual circuit association.

In summary, a field such as a Flow Identification can serve at least two important purposes:

1) It can be used by routers (or gateways) to identify packets with special, or pre-arranged delivery requirements. It is important to realize that it may not always be possible to "peek" at internet packet content for this information if certain security considerations are met (e.g., an encrypted transport layer).

2) It can aid mapping datagram services to different types of communication services provided by specialized subnet/data link layer protocols.

Multicast

Tactical military communication has a very clear requirement for multicast. Efficient dissemination of information to distributed warfighting participants can be the key to success in a battle. In modern warfare, this information includes imagery, the "tactical scene" via tactical data messages, messaging information, and real-time interactive applications such as digital secure voice. Many of the tactical RF communication media are broadcast by nature, and multicast routing can take advantage of this topology to distribute critical data to a large number of participants. The throughput limitations imposed by these RF media and the physics of potential electronic counter measures (ECM) dictate that this information be distributed efficiently. A multicast architecture is the general case for information flow in a tactical internetwork.

Quality of Service and Policy-Based Routing

Quality of service and policy based routing are of particular importance in a tactical environment with limited communication resources, limited bandwidth, and possible degradation and/or denial of service. Priority is a very important criteria in the tactical setting. In the tactical RF world of limited resources (limited bandwidth, radio assets, etc.) there will be instances when there is not sufficient capacity to provide all users with their perception of required communication capability. It is extremely important for a shared, automated communication system to delegate capacity higher priority users. Unlike the commercial world, where everyone has a more equal footing, it is possible in the military environment to assign priority to users or even individual datagrams. An example of this is the tactical data exchange. Tactical data messages are generally single-datagram messages containing information on the location, bearing, identification, etc., of entities detected by sensors. In CSNI, tactical data messages were assigned 15 different levels of CLNP priority. This ensured that important messages, such as a rapidly approaching enemy missile’s trajectory, were given priority over less important messages, such as a friendly, slow-moving tanker’s heading.

Applicability

There will be a significant amount of applicability to tactical RF networks. The current IP and CLNP protocols are being given considerable attention in the tactical RF community as a means to provide communication interoperability across a large set of heterogeneous RF networks in use by different services and countries. The applicability of IPng can only improve with the inclusion of features critical to supporting QoS and Policy based routing,

security, real-time multi-media data delivery, and extended addressing. It must be noted that it is very important that the IPng protocol headers not grow overly large. There is a sharp tradeoff between the value added by these headers (interoperability, global addressing, etc.) and the degree of communication performance attainable on limited capacity RF networks. Regardless of the data rate that future RF networks will be capable of supporting, there is always a tactical advantage in utilizing your resources more efficiently.

Datagram Service

The datagram service paradigm provides many useful features for tactical communication networks. The "memory" provided by datagram headers, provides an inherent amount of survivability essential to the dynamics of the tactical communication environment. The availability of platforms for routing and relaying is never 100% certain in a tactical scenario. The efficiency with which multi-cast can be implemented in a connectionless network is highly critical in the tactical environment where rapid, efficient information dissemination can be a deciding factor. And, as has been proven, with several different Internet applications and experiments, a datagram service is capable of providing useful connection-oriented and real-time communication services.

Consideration should be given in IPng to how it can co-exist with other architectures such as switching fabrics which offer demand-based control over topology and connectivity. The military owns many of its own communication resources and one of the large problems in managing the military communication infrastructure is directing those underlying resources to where they are needed. Traditional management (SNMP, etc.) is of course useful here, but RF communication media can be somewhat dynamically allocated. Circuit switching designs offer some advantages here. Dial-up IP routing is an example of an integrated solution. The IPng should be capable of supporting a similar type of operation.

Support of Communication Media

The tactical communication environment includes a very broad spectrum of communication media from shipboard fiber-optic LANs to very low data rate (<2400 bps) RF links. Many of the RF links, even higher speed ones, can exhibit error statistics not necessarily well-serviced by higher layer reliable protocols (i.e., TCP). In these cases, efficient lower layer protocols can be implemented to provide reliable datagram delivery at the link layer, but at the cost of highly variable delay performance.

It is also important to recognize that RF communication cannot be viewed from the IPng designer as simple point-to-point links. Often, highly complex, unique subnetwork protocols are utilized to meet requirements of survivability, communications performance with limited bandwidth, anti- jam and/or low probability of detection requirements. In some of these cases IPng will be one of several Layer 3 protocols sharing the subnetwork.

It is understood that IPng cannot be the panacea of Layer 3 protocols, particularly when it comes to providing special mechanisms to support the endangered-specie low data rate user. However, note that there are many valuable low data rate applications useful to the tactical user. And low user data rates, coupled with efficient networking protocols can allow many more users share limited RF bandwidth. As a result, any mechanisms which facilitate compression of network headers can be considered highly valuable in an IPng candidate.

Security Considerations

Security issues are discussed throughout this memo.

Author's Address

R. Brian Adamson
Communication Systems Branch
Information Technology Division
Naval Research Laboratory
NRL Code 5523
Washington, DC 20375

EMail: adamson@itd.nrl.navy.mil