INTERNETWORKING FOR COALITION INTEROPERABILITY

Sherman Gee
Consultant
25699 Crestfield Circle
Castro Valley, CA 94552
gees@onr.navy.mil

Abstract

This paper describes the architectural features of a global IP (Internet Protocol) network-of-networks created to investigate technical issues related to the transformation of military networks from IPv4 (IPversion4) to IPv6(IPversion 6). The paper reports on the major results achieved to date from this ongoing collaborative R&D investigation. The work provided practical experience and valuable insights on migrating from IPv4 to IPv6 in the design of future global coalition networks built upon multiple, heterogeneous networks. One of the more important aspects of the work was the progress made in integrating disparate building block network technologies and performing local and system-wide interoperability testing that led to demonstrations over a complex global military network-of-networks. By drawing on best-of-breed products and standards from the commercial world and adapting them for military use, the resulting military-civilian dual-use technology base will enable interoperable, manageable, and secure coalition-wide internetworking over both military and civil networks.

Introduction

Recent guidance from the United States (US) Department of Defense (DOD) mandates the use of IPv6 (Internet Protocol version 6) in DOD networks by Fiscal Year 2008.[1] Furthermore, to support the transformation from IPv4 in current defense networks, DOD procurements starting in Fiscal Year 2004 need to be IPv6 compatible.[2] Hence, in a relatively brief period of time, DOD networks are to be transformed from IPv4- to IPv6-based network technologies. This four-year transformation period will undoubtedly be one where both IPv4 and IPv6 will need to co-exist before the transition to IPv6 is complete. Other nations are similarly moving in the direction of IPv6. Germany has issued a directive from the Information Technology Agency of the Federal Armed Forces to migrate from IPv4 to IPv6.[3] Significantly, this directive has been fully harmonized with the German Armaments Department. France has also committed towards IPv6 as has other European nations.

The Internet Protocol (IP), being a product of the Internet Engineering Task Force (IETF), comes primarily from the commercial sector. The protocol was mainly intended for use on the public internet and not in defense networks. Defense networks are designed to satisfy military requirements that are very different from that of the public internet. For example, the military employs narrow-band radios for air, sea and land vehicles that typically comprise a mobile tactical network, while in general the public internet makes use of broadband fiber-optic lines that make up a fixed network infrastructure. For tactical networks part of the network infrastructure itself as well as the end users are mobile, while in contrast public networks provide data services over a fixed network infrastructure to users some of whom could be on the move. Mobility is important in defense networks, and it introduces added complexity to the network design. Bandwidth and mobility are only some of the features that make defense networks distinct from the public internet. Because of these differences, IPv6 cannot be expected to be simply inserted into defense networks. There needs to be a period of investigation, testing, demonstration and integration to ensure that IPv6 will work effectively with other network technologies essential in large, complex defense networks designed to meet military needs.

IP networks are becoming widely deployed and are increasingly made part of military strategy. In the United States, Network-Centric Warfare (NCW) is a fundamental concept unifying geographically distributed air, sea and land units into an effective fighting force by means of tactical networks that provide the needed force connectivity to achieve various military missions, not the least of which is command and control (C2). Timely transmission of multimedia data (e.g. voice, messages, imagery and video) over the tactical networks supports the C2 mission by enabling critical operations such as real-time surveillance, timely command decision-making, consistent tactical picture, and time-critical weapons targeting and control.

However, IP in defense networks by itself is insufficient. It must work effectively with a host of other building block network technologies in order to make the networks sufficiently capable to provide the needed information services to meet military needs in network management, security, routing, quality-of-service, mobility, multicasting, and directory service. Successful integration of the building block technologies in IP networks---drawn principally from best-of-breed developments and standards from the commercial world and adapted to military needs---would provide a powerful enabler for achieving interoperability among dissimilar networks and systems, not only for joint operations, but also for achieving coalition interoperability.

A collaborative R&D project was launched in February 2001 under a multilateral MOU involving eight NATO nations---Canada, France, Germany, the Netherlands, Norway, Italy, the UK, the US---and the NATO C3 Agency (NC3A) to address the technical challenges to coalition interoperability imposed by the highly mobile, regional/littoral warfare environment involving allied/coalition air, sea and land forces. This project, known as Interoperable Networks for Secure Communications (INSC), created a global IP network-of-networks consisting of some 38 secure coalition LANs (Local Area Networks) connected by Virtual Private Networks (VPNs) across national and coalition WANs (Wide Area Networks) carrying mixed media traffic over heterogeneous networks (ISDN, Internet, 6-Bone, HF radio, wireless LAN). This global network, made up of some 15 different sites in eight nations connected via roughly 100 routers, was the primary platform for investigating, testing and demonstrating various IP networking technologies and issues central to coalition interoperability. While both IPv4 and IPv6 were considered, the focus was on the emerging role of IPv6 in tactical networks. Some of the technical challenges addressed were the hierarchical management of a global network of heterogeneous networks, adequacy of emerging Internet security protocols and standards for military networks, end-to-end routing and quality-of-service across multiple autonomous systems, connectivity across dynamic networks-on-the-move reaching to mobile end users, and voice-over-IP (VOIP) with HF radios. A comprehensive program of testing and demonstration was also undertaken to show proof-of-concept of results in a practical military environment. Additional information about this work can be found on the Web at http://insc.nodeca.mil.no. Published technical documents and reports are listed for easy access on this website.

Recognizing that achieving coalition interoperability is beyond the reach of any one nation alone, this collaborative multinational approach makes possible substantive leveraging of technical skills, facilities and resources found in partner nations. This multinational approach is absolutely essential if coalition interoperability is to become reality

Fundamental Precepts

There are several underlying precepts that are important. The approach is to develop interoperability among existing dissimilar systems through collaborative R&D, and not to develop new stand-alone systems. In this way, the considerable past investments in the presently fielded communications equipments can be put to better use. Recognizing that tremendous advances have occurred in the commercial world in the way of new products, services and standards that relate to the Internet, there is no intention to duplicate these developments. Instead, new developments are initiated only where available technology, products and services are inadequate or unavailable. Another important precept is the recognition that military needs are very different from those in the civilian sector. For example, military communications typically employ narrow band radio frequency bearers exhibiting moderate-to-high error rates, while civilian telecommunications typically use broad band fiber-optic lines that have low error rates. Finally, but by no means least important, the nature of collaborative R&D is in itself a substantial contributing factor to realizing the high level of cooperation that is essential for achieving network interoperability among coalition forces.

Objective

The objective is to perform collaborative R&D leading to a practical demonstration of a military internet architecture that is (1) interoperable, manageable, secure, mobile, with quality-of-service over military and civil networks, (2) based on existing and emerging standards, commercial services and products, and (3) provides evolutionary transition from IPv4 to IPv6 for future coalition networks.

In the process of achieving this objective, valuable knowledge and insights will be developed on adopting and implementing best-of-breed developments and standards from the commercial world for military use. Because commercial networking developments and standards are generally individual developments without other network design considerations that normally are important in the design of complex military networks, the work provides a unique platform for investigating the impact and implications of commercial standards-track networking developments on future military network architectures and design. Developing a better understanding of the technical issues derived from the interrelation and integration of individual protocols and standards into a complex overall system design is especially important for coalition networks of the future where coexistence and transformation from IPv4 to IPv6 are essential.

Work Breakdown

Due to the complexity and diversity of the work, the following eight major tasks were defined, led by one of the participating nations as shown below.

- System Architecture (Canada)
- Information Service (Netherlands)
- Network Management (United Kingdom)
- Security (Germany)
- Routing and QoS (France)
- Mobility (United States)
- Sub-networks (Italy)
- Directory Service (Norway)

The lead nation for each task area nominates a task leader for that particular task. The task leader is responsible for seeing that the work on his or her respective task is well coordinated among the nations performing the work. Different nations participating in a specific task also have their own national task leader as a working member of the task. Each task prepares its own work elements and schedule in coordination with other tasks. The task leaders are members of the System Architecture task, where the task plans were discussed, negotiated, agreed and made part of the overall Project Plan.[4]

Operational Scenario

The operational scenario is one that involves air, land and sea forces in a littoral warfare environment, where the deployed forces are highly mobile, constituting a dynamic network topology consisting of multiple autonomous systems (domains) that support dynamic routing, security, manageability, and QoS. This scenario, illustrated in Figure 1, would be typical of a regional conflict or crisis response operation involving coalition forces under a Joint Task Force Commander.

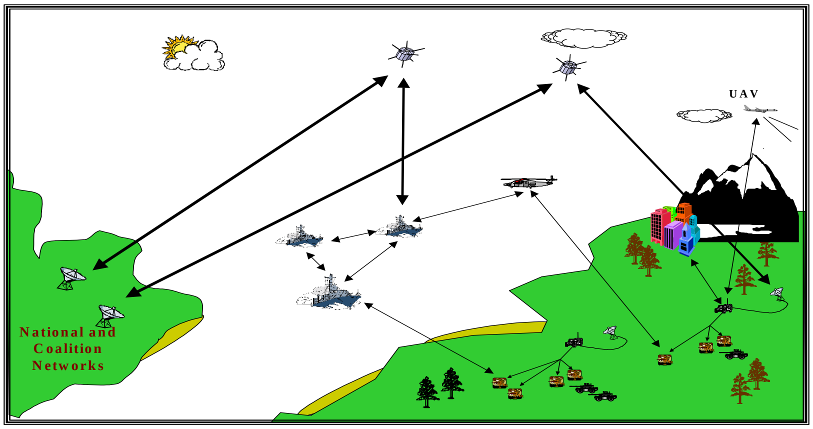

Figure 1 – Operational Scenario

In terms of the NATO STANAG 5048, which provides the draft standard for the minimum scale of connectivity for NATO land forces, this operational scenario extends between the tactical WANs (Wide Area Networks) and the theatre operational WAN.

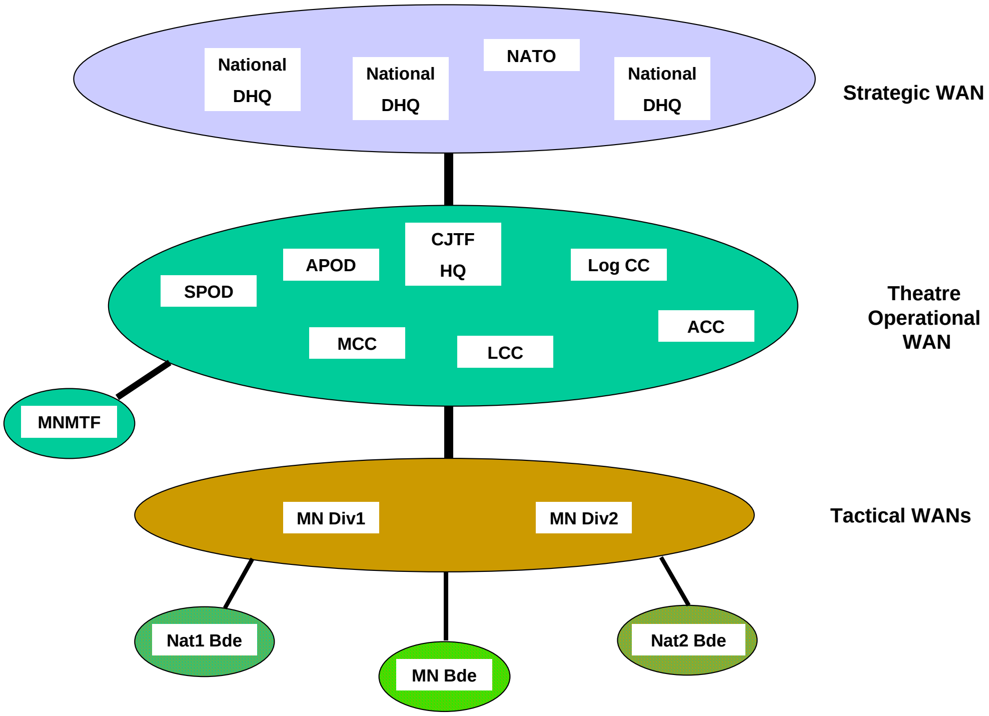

Figure 2 – NATO STANAG 5048, Communications Connectivity

Architectural Features

The network architecture has been built upon a set of design principles that were chosen to support a coherent security service and to provide clear guidance for the design of secure coalition networks.[5] The high-level network architecture is depicted by Figure 3. It is composed of coalition LANs (CLANs) of the Participants (i.e. the participating nations) and NC3A connected via national and coalition wide-area-networks (WANs). The coalition WANs make up the coalition transit network represented by the VPN cloud in the figure. In particular, the coalition WANs are the JCWAN (Joint Command WAN), the LWAN (Land WAN) and the MWAN (Maritime WAN). The coalition WANs are derived from NATO doctrine, where the JCWAN represents coalition theatre WAN, the LWAN represents coalition tactical WAN, and the MWAN represents the coalition maritime tactical WAN. The WANs are composed of mixed media, such as the Internet, the 6 Bone, ISDN and HF radio. From a security standpoint, the WANs are black networks, providing transit services to the users at the CLANs. Virtual private networks

(VPNs) are established that connect the CLANs by means of IPSec tunnels across the WANs.

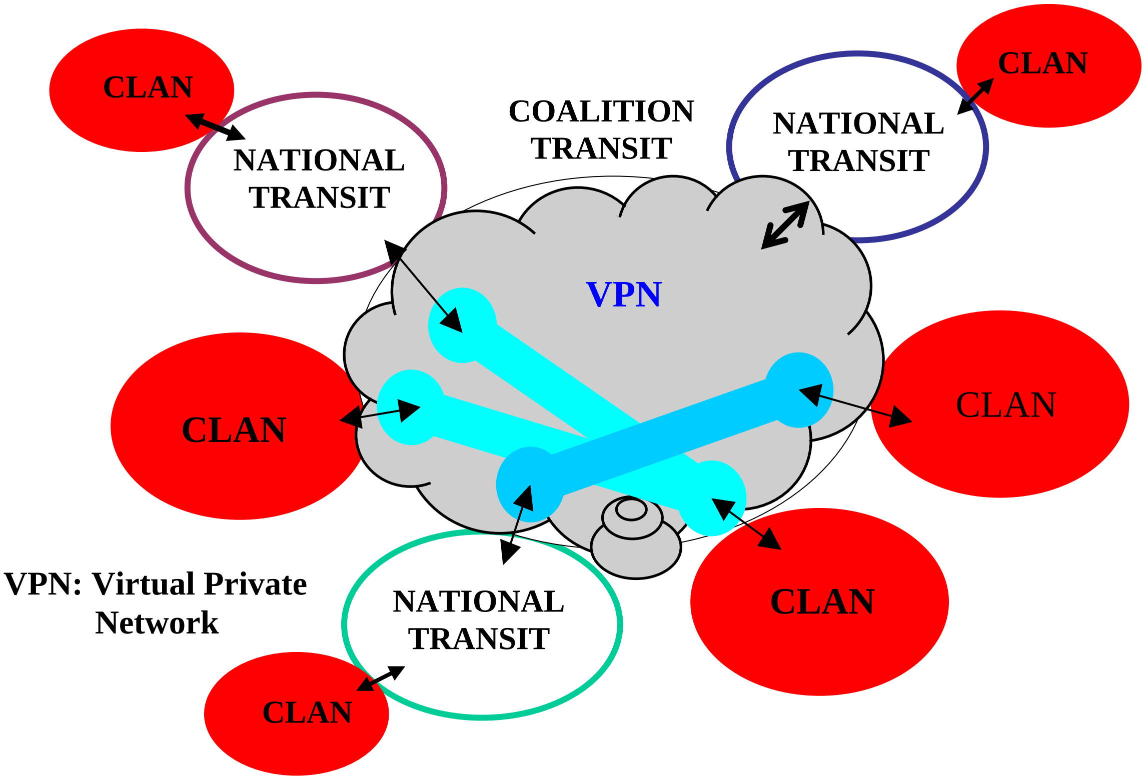

Figure 3 – High Level Network Architecture

The CLANs are red networks that are all in the same coalition and at the same security level. They contain the user workstations and could be located on land, ships or airborne vehicles. CLANs may also be mobile stub networks employing wireless devices that connect through stub gateways to the WAN transit networks. The generic architecture for a typical CLAN is shown in Figure 4. The red CLANs are separated from the black WANs by IP Crypto Devices (ICDs) that implement IPSec. Both IPv4 and IPv6 are supported in the CLANs, but transit services in the WANs are IPv6 only. This dual-stack approach for CLANs is employed as a practical measure because many applications and software tools presently support only IPv4. The CLAN router creates a 4/6 tunnel for IPv4 traffic across the IPv6 WANs as well as provides IPSec security tunnels that enables red CLAN traffic across the black transit WANs. The CLANs are intended to support reliable multicast service also.

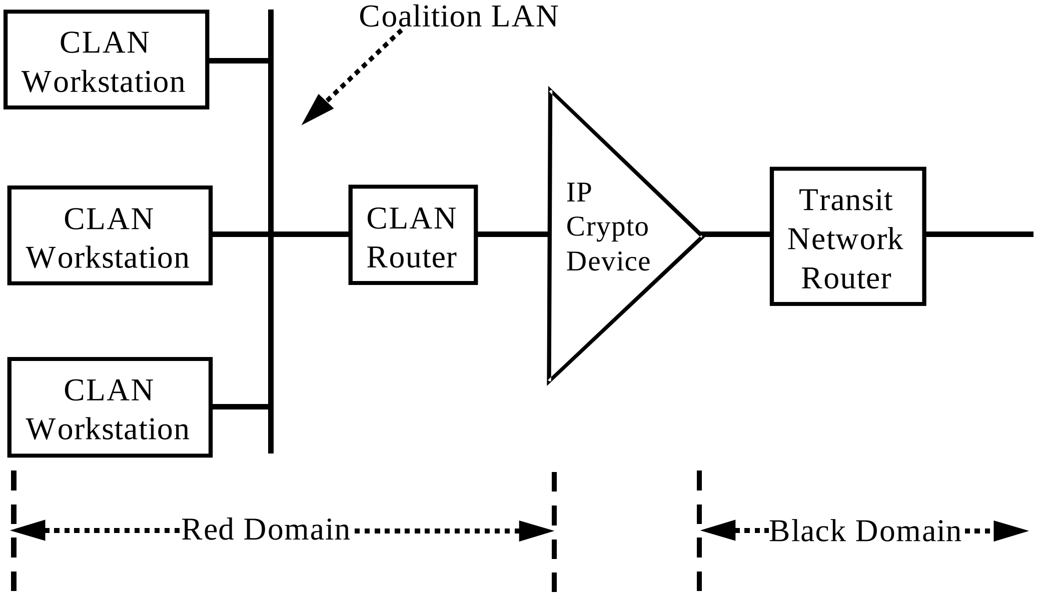

Figure 4 – Generic CLAN Architecture

Dynamic routing was implemented with IPv6 compatible OSPFv3 (Open Shortest Path First) within an autonomous domain, while BGP (Border Gateway Protocol) was used for inter-domain routing. Differentiated Services (DiffServ) was employed to support different service classes required to achieve several levels of QoS across the networks. To support a dynamic network topology, the OLSR (Optimum Link State Routing) MANET (Mobile Ad-hoc Network) protocol from the IETF (Internet Engineering Task Force) was extended to IPv6 and tested with mobile IPv6 (MIPv6) for mobile users with wireless devices. A distributed, hierarchical network management architecture was employed where SNMPc was implemented for IPv4 CLAN management, and netSNMP was used for IPv6 WAN management. A directory service using OpenLDAP, open source implementation of LDAP (Lightweight Directory Access Protocol), provided DNS (Domain Name Service) in the red and black networks, and a repository for PKI (Public Key Infrastructure) data.

The overall architecture provides a practical representation of expected future NATO operations involving coalition air, land and sea forces engaged in limited regional conflicts. The principal architectural features were chosen to represent as realistically as possible anticipated future network-centric warfare involving coalition forces. While it is recognized that the network architecture has been built on mostly commercial products and services instead of actual military equipments (such as ISDN/Internet/6bone instead of military bearers, ICDs instead of military cryptos, and private INSC names and addresses instead of Internet addresses), there has not been any conscious violation of known security policies, Internet rules, NATO architectural principles or established policies of the participating nations. Moreover, the network architecture is in keeping with the R&D nature of the effort, which investigates more the functionality and interoperability of diverse building block technologies, products and services in future military networks rather than the performance of actual networks that might be deployed in a theater of operations today.

Highlights

The test and demonstration results provided valuable practical experience, insights and lessons learned for moving from IPv4 to IPv6 in the design and development of a future global coalition network that is built from multiple diverse heterogeneous sub-networks. The effort was unique in that it was the pioneering investigation into the technical and architectural issues associated with the migration from IPv4 to IPv6 in a military context. It tested and demonstrated technical solutions in conjunction with doctrinal and operational considerations in a practical environment. In the process many technical issues of a practical nature were investigated, such as the impact of IPSec on routing and QoS, or the interplay of OLSRv6 MANET routing with MobileIPv6 (MIPv6).

A primary consideration in developing the overall architecture was the impact of security constraints on the routing and QoS architecture. The routing policies adopted must be consistent with security policies, and still meet other operational needs. The move from static routing to dynamic routing employing OSPF was made for good reasons. It avoided the need to have a full mesh of security associations, which is an important consideration in global networks with large numbers of nodes. In addition, the WANs are typically not static networks, as ISDN service is not needed continually even if for no more than affordability reasons. Moreover, in actual operations, satellite and HF radio would also be used in the WANs where connectivity would be affected by environmental factors and propagation conditions. Hence, dynamic routing using OSPF that can adapt to the best path in a dynamic network topology was the reasonable choice. OSPF also supports multicast, but the ICDs do not. To address this problem, the use of security tunnels was adopted to enable multicast traffic by wrapping the multicast packet in a unicast header and allowing it to transit the ICD. The VPNs established therefore allowed CLAN multicast traffic across the WANs.

Differentiated Services was chosen because it provides scalability and the ability to pass QoS information through security devices by means of the DSCP (Differentiated Services Code Point). Hence, the DSCP feature enabled end-to-end QoS across red and black domains in accordance with established Service Level Specifications. End-to-end QoS also needs to be maintained across mobile stub networks. As a result, QoS testing was performed over wireless MANET networks.

The MANET protocols are being considered within the IETF as potential candidates for industry standards. These protocols apply to networks where the nodes are moving independently, producing a highly dynamic network infrastructure. This aspect of mobility is distinguished from edge device mobility supported by MIPv6. The MANET protocols are especially appropriate for military networks where air, land and sea platforms are constantly on the move. The MANET protocol experimented widely in INSC was OLSR. In addition, MIPv6 experiments and local performance tests were conducted. Extensions to OLSR were also developed to better support signaling with MIPv6, and an experimental prototype was built to support integrated tests. Results from testing of OLSR and other MANET protocols in INSC can then be fed back into the IETF standards process in order that eventual IETF standards for network mobility might also satisfy military needs.

Aside from architectural considerations, a number of individual technical accomplishments can be identified that are particularly significant in terms of being either a significant technical advance or having high promise for an improvement in operational capability.

- Distributed network management of multiple CLANs employing IPv4 SNMPc for management information transfer via v4/v6 tunnels across the WANs
- First prototype IPv6/IPSec implemented for FreeS/WAN Linux
- IPSec header compression for narrowband military networks
- Porting OLSR IPv4 code to IPv6
- Defining new MIPv6 and OLSR routing extensions to enable MIPv6 support with OLSR
- directory service supporting DNS (Domain Name Service) in the red and black networks, and a repository service for PKI

Although they by no means represent a complete listing of accomplishments, they nevertheless are indicative of the breadth and scope of the problem domain.

Perhaps the biggest challenge addressed in the project is the integration of the many building-block technical developments into a practical architecture and network design applicable for military use---and the subsequent test and demonstrations that were carried out. This accomplishment in itself contributes in a major way towards a better understanding of how to design military networks of the future.

Exploitation of Results

Despite the collaborative R&D nature of the work, a major focus has been, and continues to be, to expedite the transition of results into military networks in NATO as well as in the participating nations. For example, the directory service has been considered by NATO Air Force command and control for operational use. Needless to say, several avenues for transition can be pursued.

An important avenue is through the introduction of results into the NATO STANAG process. Maintaining close ties with the NATO SC/5 and SC/6 community, the continuing liaison with the NATO TACOMS Post 2000 project and the SC/6-WG/1 Tactical Communications working group, and having NC3A as a prominent contributor all help immeasurably to achieve this goal. It is also important not to neglect the commercial standards process because dual-use technologies and standards will continue to be needed if the high fixed and operating costs associated with non-interoperable, balkanized networks are to be reduced. A notable example is the strong association established over the course of the work with the IETF MANET working group.

Field demonstrations are another important avenue for exploitation of results. For this reason, multinational testing and demonstrations have been emphasized from the outset. International demonstrations were conducted. Member nations have also conducted special demonstrations for national audiences, and participated in external demonstrations, such as the Joint Warrior Interoperability Demonstrations (JWID) held annually. These demonstrations help to make more visible to military decision-makers and field personnel the new or improved operational capabilities possible. Participants also are positioned to promote the wide deployment and exploitation of results within their own nation's systems and networks.

Finally, presentation of results in symposia such as this 9th ICCRTS provides another avenue by which the transition of results to wider use in both the commercial and military worlds can take place.

Concluding Remarks

An investigation into internetworking of the scale and diversity of a global IP network of heterogeneous networks is by its very nature beyond the capabilities of any one nation. The work is possible only in a multinational setting where diverse people, know-how, facilities and funding can be brought together to work towards mutual benefits. The global network that was created is in itself an important resource for investigating technical issues in network interoperability. For this reason, the participating nations are planning to continue the work during the remaining two years of the MOU. The technical areas are in system architecture, security, network and traffic management, mobility, and IPv4/IPv6 interworking—areas that are highly challenging but also have high-payoff potential. The major thrust is to develop further insights on how different IPv6-based network technologies can be integrated to work together effectively in a practical military context.

References

[1] DoD CIO Memorandum "Internet Protocol Version 6 (IPv6)", dated 9 June 2003.

[2] DoD CIO Memorandum " IPv6 Interim Transition Guidance", dated 29 September 2003.

[3] Bundesministerium der Verteidigung, Memorandum on Migration from IPv4 to IPv6, dated 16 September 2003.

[4] INSC Project Plan, INSC/SC/DU/003, 21 November 2003.

[5] P. Fasano et. al., “Design Principles For A Coalition Network Architecture”, NATO RTA SCI Symposium, Athens, Greece, 21-24 October 2003.

Acknowledgments

The work reported in this paper was performed under the INSC project. Thanks go to the many people from the participating nations and NC3A who contributed to this work. The author serves as chairman of the project steering committee. United States participation in the project was sponsored by the Navy International Programs Office, and the Office of Naval Research in Arlington, Virginia. The work in the United States was principally performed at the Space and Naval Warfare Systems Center, San Diego, California, and at the Naval Research Laboratory, Washington, DC.