Paper

Planning the introduction of IPv6 in NATO

Robert Goode

Abstract— The NATO wide area network provides secure IP services to NATO commands and agencies, and offers information exchange gateways to nations and coalition operations. The IP services support the NATO-wide deployment of core automated information systems (AIS), and the placement of specific functional area services (e.g., intelligence, logistics, C2IS for the services, etc.) at commands. To maintain and improve interoperability within NATO and with partners, NATO will transition from version four of the Internet Protocol (IPv4) to version six (IPv6). The transition to IPv6 will involve the IP network, the information exchange gateways, the core AIS, the functional area services, and the supporting CIS infrastructure. The IPv6 naming and addressing plan being developed supports the NATO command structure and interoperability with NATO partners. The critical issue in the planning process is to support the incremental introduction of IPv6 whilst maintaining network security and reliable interworking with existing IPv4 systems and limiting increases in operations and maintenance costs. To minimise costs and maximise effectiveness NATO is planning the transition in a timescale that is commensurate with commercial adoption in NATO countries, the technology refreshment points for major systems, and the availability of IPv6 security components. New NATO projects will prepare for the transition by detailing their IPv6 upgrade path and procuring dual stack (IPv4 and IPv6) equipment. NATO will develop and adopt standardised approaches for IPv6 protocols and network design.

Keywords— Internet Protocol, IPv6, transition, NATO, CIS.

1. Introduction

The NATO operates a broad range of communications and information systems (CIS) at NATO headquarters (HQ), organizations and agencies. The sites are linked by the NATO secret wide area network (NSWAN), which provides a NATO-wide, cost-effective, interoperable and secure capability. NATO also operates the NATO unclassified WAN (NUWAN) and a number of mission/theatre classified WANs (MSWAN). The NATO WANs provide cryptographically protected virtual private networks (VPN). The traffic on the plaintext (high side) side of the encryption device is referred to as "red", whilst the enciphered traffic (on the low side) is referred to as "black". The terms "red" and "black" are used in this paper to refer to these two cryptographically separated routing domains as shown in Fig. 1.

The NATO CIS are divided into core area services (CAS), which are used by all NATO users, and the functional area services (FAS), which are role-based applications. The CAS provides NATO-wide automated information applications such as electronic mail, web services and document preparation tools. The FAS support specific functions such as logistics, ground, maritime and air operations, intelligence services, etc. The NATO CIS interfaces to national fixed and mobile networks to cover the whole NATO area to support high level political consultation and command and control of military forces. NATO CIS is being transformed to achieve the NATO network enabled capability (NNEC) with a seamless flow of information, and to support the NATO response force (NRF). The NATO response force will be a coherent, high readiness, joint, multinational force package, technologically advanced, flexible, deployable, interoperable and sustainable. As part of the ongoing CIS transformation NATO is planning for a transition of the packet switched NATO VPN (NVPN) from version four of the Internet Protocol (IPv4) to version six (IPv6) [1].

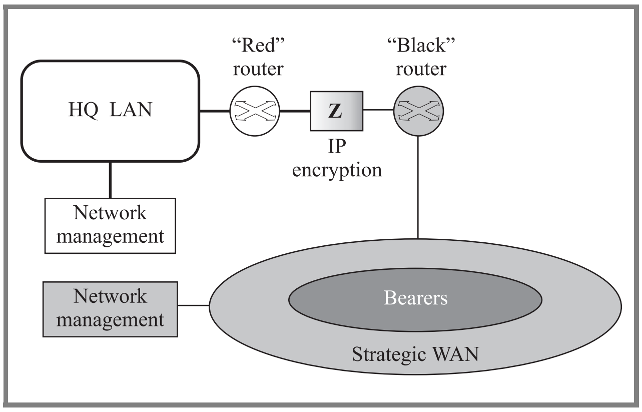

Fig. 1. "Red" and "black" routing domains.

At the time of writing three NATO nations (FR, GE, US [2]) have issued directives relating to the use of IPv6 in their national defence infrastructure, and the US has directed the use of IPv6 in other government departments [3, 4]. The Commission of the European Communities issued a communication to the Council and the European parliament in 2002 [5] which called upon member states to encourage transition towards IPv6. All major vendors of network routers support IPv6, and the vendor of the dominant operating system for PCs (Microsoft) has stated that the next major update to the Windows platform, due out in 2006, will use IPv6 as the preferred transport [6].

The main goals for the NATO IPv6 transition are to:

- support the NNEC seamless flow of information;
- maintain and improve interoperability;

- take advantage of new capabilities to increase functionality and reduce cost;
- stay in line with commercial developments.

This paper considers the planning necessary to achieve the NATO IPv6 transition goals, which involves a pervasive change across the whole of NATO CIS and interfaces to NATO nations and NATO partners. The aims and objectives of the transition planning are presented, and an outline is given of the technical areas being considered. This paper focuses on the transition planning for the communications systems, and discusses planning guidance to NATO and national users at the strategic and tactical level on using the IPv6 NATO WANs.

2. The IPv6 transition planning – outline

The NATO IPv6 transition planning will:

- Develop an evolutionary IPv6 transition plan for NATO CIS infrastructure:
  - specify the IPv6-support to be built into the NATO WANs;
  - specify the approach for naming, addressing, routing, network management, security and transition mechanisms in the NATO WANs.
- Determine the manner in which interoperability will be maintained with NATO partners during the transition:
  - develop guidance to NATO partners on interworking with NATO during the transition.
- Provide NATO with the concepts and know-how to migrate the CIS across strategic and deployed systems to work on a single virtual IPv6 network:
  - develop guidance to core and functional area services to become IPv6-ready;
  - identify the standards which must be supported in specific functional elements.
- Identify new capabilities in IPv6 of which NATO can take advantage:
  - examine: multicast, anycast, multiple address plans, radically increased address space, auto configuration, mobility support, flow labelling, etc.
- Determine the timelines and approaches which achieve the best cost-benefit for the transition in a timescale commensurate with the commercial adoption in NATO countries:
  - work with NATO nations, partners, and industry on timeline planning.
- The transition planning is broad in scope to introduce the system, technical and operational views which need to be considered due to the pervasive nature of an IP transition. In order to support the broad nature of the planning process, the follow methods are used:
  - technical studies;
  - NATO working groups with representation from all NATO stakeholders;
  - in-house test-beds and multinational experimentation;
  - participation in IPv6-related forums and events;
  - IPv6-related training.

3. IPv6-support in the NATO WANs

The NATO WANs must maintain full support for existing IPv4 services during the transition period, to avoid breaks in operational service. This means that the IPv6-support must be in parallel to the IPv4 support, and must not negatively impact it. A second requirement is that the IPv6 access must be ubiquitous, rather than constrained to specific network access points. The transition to IPv6 is envisaged as evolutionary, with an initial low level of IPv6 traffic, which increases over the lifetime of the transition. The transition period is expected to be measured in decades because of the need to maintain IPv4 support to inter-work with legacy systems. The IPv6 support must thus scale from minimal usage to being the dominant traffic type, and should do so in a manner that is cost-effective over the lifetime of the transition.

The NATO WANs need to support routing of IPv6 traffic in an efficient manner, and name resolution through an IPv6-enabled domain name service (DNS), which needs to operate effectively in parallel to an IPv4-enabled DNS. The whole network must be operated securely with guard technology to protect against external network attacks, and intrusion detection to monitor the internal integrity of the environment.

3.1. Naming structure

The fully qualified domain names applied to network devices are frequently visible to users (for example in uniform resource locators – URLs) and so need to make sense to non-technical staff, as well as supporting the needs of network managers. The naming structure is often driven by organizational structure, and uses a standardized format for naming devices types (routers, switches, workstations) and usage (mail server, firewall, administrator, etc.).

The transition from IPv4 to IPv6 does not intrinsically alter the organizational structure or application usage; therefore the existing IPv4 naming structure will be applied to IPv6. The approach clearly simplifies the network manager's task of identifying a specific device in both the IPv4 and IPv6 network. The approach also means that the user does not need to know whether an application is being accessed via IPv4 or IPv6, as the same name can be used in both cases. De-conflicting the resolving of DNS queries which may result in an IPv4 or an IPv6 address (or both) places some constraints on the deployment of the IPv6.

3.2. Addressing plan

Numerical representations of IPv4 addresses are usually hidden from end users, who use the human-readable names instead. The addressing plan can thus be divorced from organizational structure and the use to which a network element is put; and be driven by the network structure to improve operating efficiency and easy maintenance. Two significant considerations for the addressing plan are aggregation to reduce routing table size and frequency of routing advertisements, and scalability to support growth (both planned and exceptional). An addressing plan therefore tends to be hierarchically constructed along geographic (or connectivity) lines, and have reservations for future growth. The transition from IPv4 to IPv6 does not intrinsically alter the network structure or growth forecast, therefore the existing IPv4 addressing plan format will be applied to IPv6. This may mean that a simple mapping function can be used to map hierarchical elements of the IPv4 address onto equivalent elements of the IPv6 address. Clearly there are differences between the IPv4 and IPv6 address formats defined by the Internet Engineering Task Force (IETF), such as the number of bits and the manner in which the addressing mode (unicast, multicast, globally routable versus private/link-local, etc.) is encoded in the bits, and these must be taken into account. Some new capabilities in IPv6 which must be assessed are the option to have multiple addresses plans (with multiple addresses per network interface), the use of anycast, and renumbering.

3.3. Routing

The NATO WANs require an interior gateway protocol (IGP) for distributing routing information internally. An exterior gateway protocol is required for exchanging routing information with peer networks. NATO currently has a limited requirement for IP multicast, which seems likely to increase to achieve the NNEC vision of seamless information exchange. The "red" routing domain is separated from the "black" routing domain by IP-based encryption devices, but both routing domains must be co-operatively managed to achieve a stable and robust network that can support the required network quality of service.

3.4. Network management

A critical element of a reliable CIS infrastructure is the network management system. The network manager needs to view the traffic load and health of the distributed network elements in order to perform problem identification and resolution, and to plan provisioning schedules. The network management system will need to be dual-stacked to provide the monitor and control interface for both the IPv4 and the IPv6 components. An approach is required that will achieve harmonized network management of both the "red" and "black" domains for the NATO WANs. A sample of the requirements is given below:

- Automated address space management for both IPv4 and IPv6.
- Network monitoring and visualisation for both IPv4 and IPv6.
- Scaleable element management.
- Extensible for QoS, transition mechanisms, gateways, applications.
- Manage multiple inter-dependent networks:
    - IPv4 and IPv6 networks,
    - Enciphered virtual private networks ("red") over range of bearers ("black").

3.5. Security

Security is a strong requirement for NATO classified systems. In addition to the confidentiality requirements which can be met by a high-grade IPv4 and IPv6-capable encryption device, there are requirements for integrity, authentication, non-repudiation, reliability, auditing, intrusion detection, and physical security. The full range of high-grade security devices must be available in IPv6-capable form to work in concert with the existing IPv4 devices without significantly increasing the total cost of ownership of the secure networks.

3.6. Transition mechanisms

The IETF has issued a number of request for comment (RFC) documents, e.g. [7–9], which describe a range of transition mechanisms that meet the identified requirements for IPv6 support in the NATO WANs. The simplest initial approach is to transport IPv6 packets encapsulated in IPv4 packets (tunnelling) over the existing IPv4 infrastructure. This works well when the IPv6 traffic is sparse, as was demonstrated by the success of the 6bone [10, 11], but as an approach its suitability is inversely proportional to the quantity of IPv6 traffic. Given that the IPv6 traffic will eventually be dominant, a more suitable approach is to support native IPv4 and IPv6 traffic simultaneously by using dual-stack network elements. Consideration must also be given to converting the network cores from IPv4 to IPv6, and tunnelling IPv4 over IPv6 in the core. The cost-benefit analysis is a significant part of determining the best approach.

There are also requirements to gateway traffic between IPv4 and IPv6 systems, i.e., to interconnect them rather than just enable them to operate in parallel. The IETF has documented a number of application-level transition mechanisms [7].

There is a body of work on the advantages and disadvantages of each transition mechanism in specific circumstances, which includes guidance on transition planning [12–15]. This experience will form a valuable input to NATO.

4. New capabilities in IPv6

The design of IPv6 has benefited from decades of experience with IPv4 networks. The most visible change is that the address space has been drastically increased, from 32-bits to 128-bits. Other improvements have also been made, in the areas of multicast, anycast, mobility, and autoconfiguration. There is also a field which traffic sources can use to label flows through the network which may offer practical benefits to NATO networks by enabling a richer support for network quality of service than is possible for IPv4 (see for example [16] for the issues, [17] and [18] for a possible way forward).

5. Guidance to information services

The purpose of enabling IPv6 support in the NATO WANs is to facilitate IPv6 applications. One obvious part of the guidance to the information service developers is to port their networked applications to an IPv6 stack. It is additionally necessary to provide guidance on inter-working IPv4 with IPv6, including information on when to use specific approaches out of the range on transition mechanisms available. One example of such guidance is [15].

6. Guidance to NATO partners

Maintaining and improving interoperability with NATO nations and partners is a key driver for the transition to IPv6 by NATO. The exchange of information between NATO and a nation or organization is achieved through information exchange gateways (IEGs) [19, 20] as shown in Fig. 2.

The IEGs implement application-level proxies and guard functions for web and electronic-mail, thereby enabling controlled release of data. Applications which require additional services through the IEG can develop the necessary application-level proxies and accredited guard functions. The IEGs do not provide a general packet routing service, but instead form an IP break. This means that routing information does not flow between NATO and nations or partners through an IEG.

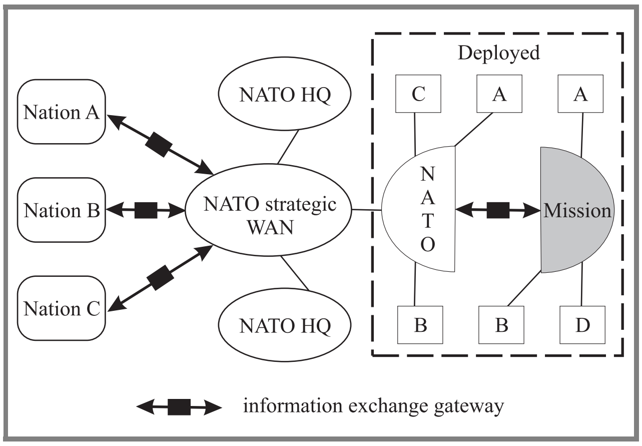

Fig. 2. Use of information exchange gateways.

7. The IPv6 compliance

A common definition of IPv6 compliant that can be uniformly applied in procurement of NATO common-funded equipment is a pre-requisite to achieving a fully functional IPv6 network, and a vital part of defining a standardized interconnection point for NATO and national systems. Work on this topic has been performed in a number of fora, including the IPv6 ready program [21], the European Community [22], and the US DoD [23]. NATO will build on this body of work to develop a common NATO definition in consultation with the nations.

8. Experimentation

NATO actively utilizes testing, experimentation and exercises to support interoperability testing of NATO and national systems. Relevant activities include the NATO interoperability environment testing infrastructure (NIETI), the annual coalition warrior interoperability demonstration, combined endeavour, the *Interoperable Networks for Secure Communications* (INSC) project, and the Combined Federated Battle Laboratories Network (CFBLNet). INSC [24] is an eight-nation project to develop the future communications architecture for combined joint out-of-area operations, and it has an IPv6-focus [25]. The CFBLNet [26] is an arrangement between the US, Combined Communications-Electronics Board (CCEB) and NATO to provide the network of choice for test and evaluation experimentation. The charter nations/organisations are the US, the CCEB nations (AUS, CAN, NZ, UK, US), the NATO nations, and NATO as an organisation. The CFBLNet is currently running a multinational IPv6 initiative.

In order to achieve increased interoperability experimentation will be used to validate the operation of selected transition mechanisms, naming and addressing plans, security devices, routing approaches, etc. Such experimentation is already underway and will need to be continued for the duration of the transition, which is likely to continue for many years.

9. Training

Training of the network designers, network operators, security experts, and application developers will be required to achieve a successful transition. This will ensure that the appropriate transition mechanisms are applied in each case, and with the necessary security configurations.

10. Conclusion

This paper has introduced the areas which must be covered by the NATO IPv6 transition planning process in order to successfully manage the introduction and migration to IPv6 whilst maintaining the interoperability with existing IPv4 systems over a prolonged transition period.

References

[1] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) specification", RFC 2460, Dec. 1998

[2] J. Stenbit, "Memorandum Establishing DoD Policy for Transition to Internet Protocol Version 6 (IPv6)", US Department of Defense, ASD NII-DoD CIO, 9 June 2003.

[3] "IPv6: Federal Agencies need to plan for transition and manage security risks", Rep. GAO-05-471, http://www.gao.gov/new.items/d05471.pdf

[4] "Transition planning for Internet Protocol Version 6 (IPv6)", in Executive Office of the President, Office of Management and Budget as OMB M-05-22 Memorandum for the Chief Information Officers number M-05-22, on Aug., 2005, http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf

[5] "Next generation Internet – priorities for action in migrating to the new Internet Protocol IPv6", in COM(2002) 96 final by the Commission of the European Communities on 21.02.2002 as a communication from the Commission to the Council and the European parliament, http://europa.eu.int/eur-lex/en/com/cnc/2002/com2002_0096en01.pdf

[6] L. Huang, "Microsoft IPv6 Update", in *North Amer. IPv6 Summit*, 2005, http://usipv6.unixprogram.com/North_American_IPv6_Summit_2004/052005/tue/Leigh_Huang.pdf

[7] R. Gilligan and E. Nordmark, "Transition mechanisms for IPv6 hosts and routers", RFC 2893, Aug. 2000.

[8] D. Haskin and R. Callon, "Routing aspects of IPv6 transition", RFC 2185, Sept. 1997.

[9] B. Carpenter and K. Moore, "Connection of IPv6 domains via IPv4 clouds without explicit tunnels", RFC 3056 , Febr. 2001.

[10] 6bone, http://www.6bone.net/

[11] I. Guardini, P. Fasano, and G. Girardi, "IPv6 operational experience within the 6bone", http://carmen.cselt.it/papers/inet2000/index.htm

[12] J. Dočkal and T. Fiala, "Research of the migration from IPv4 to IPv6 in the Czech Army", in *Proc. 6th NATO Reg. Conf. Milit. Commun. Inform. Syst.*, Zegrze, Poland, 2004, pp. 357–362.

[13] T. Chown, "IPv6 campus transition experiences", in *Proc. Int. Symp. Appl. Internet SAINT 2005*, Trento, Italy, 2005.

[14] M. Brig, "Integration techniques – a technical brief on the methods of transitioning to IPv6", in *US IPv6 Summit*, Reston, USA, 2004, http://usipv6.unixprogram.com/usipv6_reston_2004/tue/Brig.pdf

[15] V. Pecus, "DoD IPv6 applications transition planning guidelines", in *US IPv6 Summit*, Reston, USA, 2004, http://usipv6.unixprogram.com/usipv6_reston_2004/thu/Pecus.pdf

[16] R. Goode, P. Guivarch, and M. Stell, "Quality of service in an IP crypto partitioned network", in *Proc. MILCOM 2002*, Anaheim, USA, 2002, vol. 2, pp. 1154–1159.

[17] P. Sevenich and C. Reichmann, "Multiplexing time-critical and conventional data over tactical IPv6 networks of low bandwidth", in *INSC Symp.*, The Hague, The Netherlands, 2003, http://insc.nodeca.mil.no/ifs/files/public/Symposium/Symposium

[18] M. Amanowicz, P. Sevenich, J. Jarmakiewicz, and M. Pilz, "Quality of service support in IPv6-based military networks with limited bandwidth", in *Proc. RTO IST-054 Symp. Milit. Commun.*, Rome, Italy, 2005.

[19] M. Diepstraten and R. Parker, "NATO AIS cooperative zone technologies", in *Proc. 4th NATO Reg. Conf. Milit. Commun. Inform. Syst. RCMCIS*, Zegrze, Poland, 2002, pp. 207–216.

[20] S. Cresdee, M. Diepstraten, E. Frambach, W. Hoogeveen, F. Nolden, L. Schenkels, and D. Stanley, "NATO AIS information exchange gateway evolution", in *Proc. 5th NATO Reg. Conf. Milit. Commun. Inform. Syst. RCMCIS*, Zegrze, Poland, 2003.

[21] "IPv6 ready at URL", http://www.ipv6ready.org/frames.html

[22] "IPv6 standardisation report", IST-2001-34056, M. Ford, Ed., 2005, in European Commission as deliverable D5.1.10 under WP5 as part of the EC Information Society Technologies 6LINK programme; PDF version available via the homepage of the European Commission IST IPv6 cluster, http://www.ist-ipv6.org

[23] D. Coe and A. Sekelsky, "IPv6 capable – DoD definition", in *US IPv6 Summit*, Reston, USA, 2004, http://usipv6.unixprogram.com/usipv6_reston_2004/thu/Coe-Sekelsky.pdf

[24] "Interoperable networks for secure communications (INSC)", http://insc.nodeca.mil.no/

[25] S. Gee, "Internetworking for coalition interoperability", in *9th Int. Comm. Contr. Res. Technol. Symp.*, Copenhagen, Denmark, http://www.dodccrp.org/events/2004/ICCRTS_Denmark/CD/papers/013.pdf

[26] "Combined Federated Battle Laboratories Network (CFBLNet)", http://cfbl.nc3a.nato.int

Robert Goode has been working in the area of network communications for defence systems for twenty years, split between commercial and NATO positions. He has worked on a variety of technology areas including X.25, X.400, trusted computer base, mobility, IP quality of service, and IPv6. He is a Principal Scientist at the NATO Consultation, Command and Control Agency (NC3A) where he is leading the team drafting the NATO IPv6 transition plan. He is actively involved in multinational activities examining IPv6 such as the INSC project and CFBLNet, for which he is the NATO "national" lead.
e-mail: Rob.Goode@nc3a.nato.int
NATO C3 Agency (NC3A)
Oude Waalsdorperweg 61
2597 AK The Hague, The Netherlands