IPv6 Coexistence Mechanisms For Global Air Space System

March 2005 - Version 1.0

This document is Hexago response to NASA Request for Information on Global Air Space System Requirements in the context of the Network Centric Operations for aeronautical networks. The document primary focus is the use of coexistence (transition) mechanisms to help deploy IPv6 in aeronautical telecommunications networks.

Overview

The deployment of the next generation Global Air Space System will take advantage of a widespread usage of IPv6. The use of coexistence mechanisms will facilitate a network-wide deployment of IPv6 by ensuring network reachability of every single node and interoperability between different components of the network.

Hexago suggests a solution based on tunneling, such as Hexago's Migration Broker, as a way to deploy IPv6 rapidly over existing network infrastructures, maximizing ROI on existing networking equipment. This solution offers a seamless path of integration on a wide range of networks and platforms and also provides a scalable and controlled way to deploy while ensuring security. This is an economical and technically tested approach to integrate existing and foreign networks with IPv6.

Coexistence Mechanisms Background

Deploying IPv6 natively involves either a completely independent IPv6-only network or equipment supporting both IPv4 and IPv6. The latter option is usually called 'dual-stack' approach because it involves running both IPv4 and IPv6 software stacks on the same equipment.

However not every network equipment supports IPv6. Some equipment are limited in hardware while some others do not have the resources required to run two network stacks at the same time. IPv6-aware software for these equipment is often not available, either because the manufacturer hasn't developed it yet or do not support the equipment anymore. In order to deploy IPv6 in networks while using the existing equipment's, coexistence mechanisms are required.

Coexistence mechanisms are roughly classified between translation and tunneling protocols. Translation protocols transform outgoing IPv4 packets into their IPv6 equivalent and do the inverse process for incoming packets. Tunneling techniques encapsulate IPv6 packets in IPv4 to make them transit the legacy part of the network. Tunneling requires the end node to support both IPv4 and IPv6, which is the case for most modern operating systems.

Shortcomings Of Translation Technologies

Using translation as a coexistence mechanism presents several shortcomings, making this approach unsuitable for most deployments. These shortcomings are caused mostly by protocols with embedded IP information in the protocol payload. Translation also prevents IPsec to be used since it changes the content of packets. An IETF draft document explains these shortcomings in details (see draft-ietf-v6ops-natpt-to-exprmntl) and suggests that NAT-PT, a standard translation protocol, should not to be deployed anymore.

Some networking protocols, such as DNS and FTP for example, include IP-related information such as IP addresses and ports in the data content of packets. Translating these packets therefore requires special handling for each protocol. This special handling is done by Application Layer Gateways (ALG) or application proxies.

In order to deploy a translation gateway, an application proxy must also be deployed for each protocol containing IP data in its payload, making this approach very unpractical. Also, the mapping not being perfect between the data field in IPv6 and IPv4 packets, some information may be lost in the translation.

Using translation also breaks the end-to-end model of the IPv6 network, introducing additional delays and states. A status for each ongoing connection must be kept in the translation device in order to map correctly incoming packets. If no packets are exchanged for some amount of time, the connection information will be flushed from the translation device, preventing new incoming connections.

Manual, automatic and configured tunneling

Provisioning tunnels manually is an interesting solution for topologies that are not expected to change often. However, as soon as the number of tunnels to manage increases or the related IPv4 addresses are not permanent, managing this type of tunnels becomes both cumbersome and time-consuming. Manual tunnels cannot be used in the case where a NAT device is in the path, since manual tunnels lack a mechanism to keep the associations alive in the NAT devices.

Using automatic tunneling protocols such as 6to4, Teredo or Isatap might be an interesting option, since this type of tunnels requires very little provisioning and can be used even if the network topology and IPv4 addresses change. However these protocols do not provide a permanent IPv6 address. Each time the IPv4 address changes, the related IPv6 addresses or prefix will change as well. Controlling access and network usage (AAA) is also impossible for the protocols using an open relay architecture (see RFC 3964 for a detailed discussion).

A tunnel configuration protocol combines the simplicity of manual tunneling without the problems related to automatic tunneling. The most widely used of these protocols, the Tunnel Setup Protocol (TSP), is used in Hexago's solution. TSP configures a manual tunnel after authenticating to a central server (the tunnel broker) and negotiating the tunnel parameters. AAA functions are available, a permanent IPv6 address and prefix can be assigned to a user and the provisioning of tunnels scales to several thousands for a single broker.

Hexago's Configured Tunnels Solution

This section describes how a solution based on configured tunnels, such as Hexago's Migration Broker, makes IPv6 available network-wide while respecting the specified design requirements.

From an economical perspective, using IPv6 transition mechanisms makes a lot of sense since it increases the return on investment of existing networking equipment. Equipment supporting IPv4 but for which IPv6 support is not possible, either because of unsupported software or limited hardware, can be used for network centric operation. This approach adds value to existing infrastructure at a low cost of acquisition.

Standards and Interoperability

The Migration Broker solution is based on the tunnel broker standard, RFC 3053. It provides a standard IPv6 network access using IPv4 as transport using the Tunnel Setup Protocol (TSP). It is therefore independent of the type of link, as long as IPv4 is available, in a way similar to a VPN.

A wide range of platforms is supported. Most operating systems supporting standard IPv6 in IPv4 encapsulation (protocol 41) can use TSP to create a tunnel and get IPv6 connectivity where or when it isn't natively available. This allows equipment worldwide to interoperate using IPv6.

Security and AAA

The Migration Broker has authentication, authorization and accounting (AAA) capabilities when coupled with an authentication server, for example a Radius server. Each user of the service is authenticated, preventing access from unauthorized clients. Network usage and session times can also be monitored in details.

Making IPv6 available to end nodes makes possible the deployment of IPSec on a wide scale. Negotiating transport mode security associations over IPv6 in IPv4 tunnels makes secure end-to-end connections.

Scalability

A configured tunnel solution scales to support up to several thousands of connections at each service node. Scalability can be increased by stacking up several units working together, also providing redundancy and load-balancing capabilities.

Mobility

Mobile IPv6 provides a way to smoothly move from a network to another while keeping all connections active. However, two conditions must be true to be able to use Mobile IPv6: the network must support IPv6 and the correspondent node (CN) must also support Mobile IPv6. Using TSP allows a node to use IPv6 mobility in any situation, even if the two conditions above are not respected. TSP is therefore a perfect complement to Mobile IPv6, providing mobility for nodes where Mobile IPv6 cannot.

Conclusion

Hexago's Migration Broker is a reliable, proven and economically sound solution to the deployment of IPv6 for Network Centric Operations. It provides an easy way to provision IPv6 tunnels while ensuring interoperability, security and mobility in the network.

About Hexago

Hexago is a firm specializing in the deployment of IPv6-based solutions. It is dedicated to make available simple and efficient ways to deploy IPv6 rapidly in today's networks. Hexago also runs Freenet6, which has been since 1999 the worldwide leader in providing IPv6 access for internet-based users.

Point of contact

Business development

Name: Duane Barry
Title: Director of Business Development
Phone: (613) 270-8384
Fax: (418) 266-5539
Email: duane.barry@hexago.com

Technical

Name: Jean-Francois Tremblay
Title: Sales Engineer
Phone: (418) 266-5533
Fax: (418) 266-5539
Email: jean-francois.tremblay@hexago.com