


IST-2001-32603	Deliverable D4.3.3	
----------------	--------------------	--

Project Number:	IST-2001-32603
Project Title:	6NET
CEC Deliverable Number:	32603/UCL/DS/4.3.3./A1
Contractual Date of Delivery to the CEC:	February 2005
Actual Date of Delivery to the CEC:	May 2005
Title of Deliverable:	Evaluation report on the advantages demonstrated from use of IPv6 dynamic VPNs over different technologies
	FINAL
Work package contributing to Deliverable:	WP4
Type of Deliverable*:	R
Deliverable Security Class**:	PU
Editors:	Manish Lad, Piers O’Hanlon (UCL)
Contributors:	Peter Kirstein (UCL)
Reviewers:	Martin Dunmore (ULANC)

* Type: P - Prototype, R - Report, D - Demonstrator, O - Other

** Security Class: PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

Abstract:

This deliverable outlines the final stages of the 6NET Work Package 4 Activity 4.3 efforts into the deployment of a dynamic IPv6-enabled VPN infrastructure across the 6NET network. It also provides an evaluation of the benefits demonstrated by such a deployment.

Keywords:

VPN, Dynamic IPv6, X-Bone, DVC

Executive Summary

The 6NET Activity 4.3 focuses upon the analysis of IPv6-enabled Dynamic VPN technologies and the subsequent deployment of such technologies across 6NET.

The first Deliverable submitted as part of this activity provided details of the analyses carried out on a number of such activities, while the second Deliverable provided an outline the ongoing efforts made during the second year of the project, to carry out the deployment.

This deliverable provides details on the various deployments undertaken and the applications that have been run over the deployed VPN infrastructures. In addition, it also provides an evaluation of the benefits demonstrated by the deployments and identifies potential future scenarios where such dynamic VPN infrastructures may be valuable tools within the investigations being undertaken during the remainder of the project.

Table of Contents

1. INTRODUCTION.....	4
1.1. PURPOSE & SCOPE.....	4
1.2. STRUCTURE	4
2. DEPLOYMENT STATUS.....	4
2.1. DYNAMIC VPN SYSTEMS DEPLOYED	4
2.1.1. The ISI X-Bone.....	4
2.1.2. The DRDC DVC System	6
2.2. INITIAL APPLICATION DEPLOYMENT	8
2.3. SIP VOIP DEMONSTRATIONS OVER DVC.....	8
3. EVALUATION OF DEPLOYMENT RESULTS.....	10
4. CONCLUSIONS	11
5. REFERENCES.....	12

1. Introduction

1.1. Purpose & Scope

This deliverable outlines the final stages of the 6NET Work Package 4 Activity 4.3 efforts to achieve the goal of full-scale deployment of a dynamic IPv6-enabled VPN infrastructure across the 6NET network. It also provides an evaluation of the benefits demonstrated by such a deployment.

1.2. Structure

The document is structured as follows:

Section 2 outlines the current status of deployment including successfully deployed and tested infrastructure topologies and details of applications run across the infrastructure. Section 3 details the results and opinions on the deployment thus far, and Section 4 provides some conclusions on the success of the dynamic VPN infrastructure deployment and identifies future work to be undertaken.

2. Deployment Status

We outlined in the deliverable D4.3.2 [2] that, “as it stands, a fully deployed IPv6-enabled VPN infrastructure does not provide on its own any benefits for the project. What will be important is the set of applications running over the VPN infrastructure. Essentially any 6NET project-related activity involving multi-site communication and interaction that requires a level of security over and above that provided by running directly over the underlying network, could be undertaken across the VPN infrastructure.”

Both the VPN infrastructures we deployed are able to provide a base network over which project activities can take place in a secure manner. Additionally multiple “overlays” or “coalitions” can be set-up in parallel between different sets of project partners, providing multiple base networks over which different sets of applications could be run.

2.1. Dynamic VPN Systems Deployed

We have successfully deployed two dynamic VPN technologies: the ISI X-Bone [4], and the DRDC Dynamic VPN Controller (DVC) [5]. Both deployments have involved long-distance connections and both have been part of the ongoing objective for 6NET/Euro6IX collaboration via the Universidad de Murcia (UMU) [6].

2.1.1. The ISI X-Bone

The University of Southern California (USC) Information Sciences Institute (ISI) X-Bone system for automated deployment, management, co-ordination and monitoring of overlay networks essentially consists of two component elements:

- **Overlay Managers (OM)** responsible for deploying and coordinating the overlays
- **Resource Daemons (RD)** responsible for coordinating the resources of individual network components

A web-based CGI-implemented graphical user interface (the OM GUI) is provided for communicating with the OM in order to carry out the construction, management and dismantling of overlays.

For completeness, we provide here information on the X-Bone overlay deployment mechanism, which has been provided in previous deliverables.

In order to establish an overlay, an OM sends out an overlay invitation. This is carried out either in the form of an expanding multicast ring search, or through unicast to a pre-defined set of hosts provided to the OM GUI. RDs listen on a pre-defined port for invitation messages. On receipt of an invitation, an RD may respond to the invitation indicating that it is available for inclusion into the overlay. The response sent by the RD is optional and so the RD has a degree of control as to which overlays it will participate in.

The OM waits for a specified period of time and once the timeout has been reached, the OM proceeds with the overlay creation process. This involves first checking that enough RDs have responded, otherwise the overlay creation fails. If it has received more responses to the invitation than required, the OM selects arbitrarily the required number of nodes. In order to establish the overlay, the OM determines first the tunnel endpoint addressing and routing table entries that need to be set-up at the RDs. These determinations are based upon a number of parameters obtained from the OM GUI which provide including details of the topology to be used (star, ring, linear or user-specified using a special definition language), and details of encryption and authentication algorithms for tunnelling. The OM then sets up X.509 encrypted TCP/SSL connections to each of the selected RDs in order to transmit the relevant configuration information. Upon receiving the relevant configuration information, the respective RDs activate their tunnel interfaces.

The creation of overlays within the X-Bone is carried out using a two-layer tunnelling mechanism for each level of overlay. The first layer provides a virtual link layer on top of which the network layer overlay is built. This enables the use of multicast, dynamic routing and IPSec within the overlay since these are intrinsically network layer mechanisms. This method results in three IP headers in the case of an overlay constructed on top of the base network where the innermost header represents the end points within the overlay, the next header acting as a link layer and the outermost header representing the tunnel endpoints within the base network.

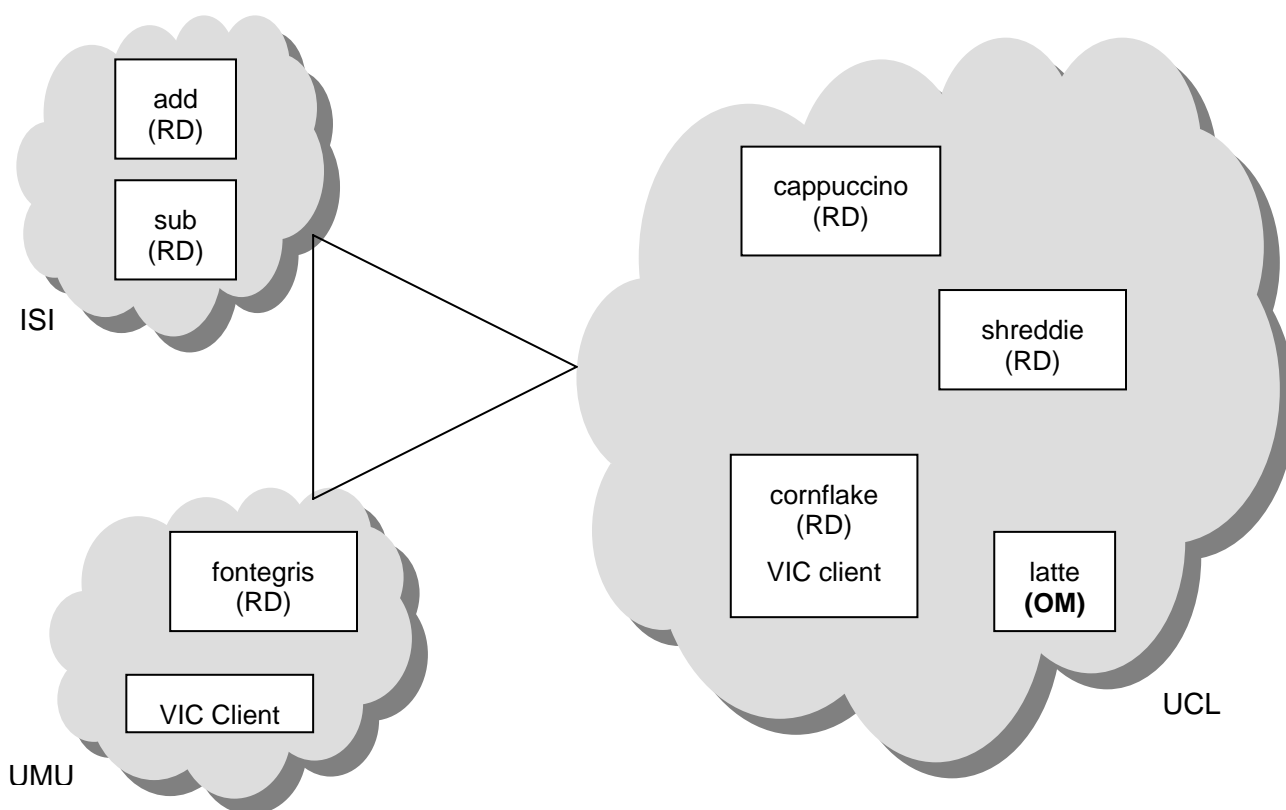


Figure 1: ISI X-Bone Network Set-up

Figure 1 illustrates the various components and network set-up for the X-Bone deployment. The deployment involved multiple Resource Daemons (RD), operating at each site. UCL deployed three RDs, one of which (`cornflake.cs.ucl.ac.uk`) also acted as a VIC application client transmitting video data from an attached webcam.

The Overlay Manager (OM) was also deployed by and located at UCL. This was able to communicate with all the available RDs, and it provided the OM graphical user interface via a web page allowing any of the project partners to deploy overlays involving any number of the available RDs.

As detailed in the previous deliverables of this activity ([1][2]), the X-Bone provides a great deal of flexibility for deployment of overlays with different topologies. The network set-up illustrated in Figure 1 was used to establish multiple different overlays via the UCL OM (`latte.cs.ucl.ac.uk`). These overlays were deployed as Star, Ring and Linear topologies between multiple different sets of the deployed RDs. In addition, a new feature of the X-Bone overlay management system also allowed the specification of custom topologies involving specific, administrator-defined RD nodes.

2.1.2. The DRDC DVC System

The Defence Research and Development Canada (DRDC) agency's Dynamic VPN Controller (DVC) system provides an entirely distributed VPN infrastructure established in the form of "coalitions", with each DVC site maintaining its own set of security and access policies to its local "participating network resources".

For completeness, we provide here information on the DVC system, which has been provided in previous deliverables.

Each coalition partner site runs a local DVC, which is connected to a common wide area network. Coalition partners make their "participating network resources" available through their respective local DVC. Each DVC maintains a local XML-based policy database, constructed via a Java-based policy editor tool, to dictate access to local resources. A web-based CGI-implemented user interface is provided for initiating and disabling coalition connections. In order to establish a connection when a partner makes a request to join a coalition, the local DVC initiates a connection to a remote DVC via SSL. The initiating DVC provides its security policies, which may be passed up to the DVC Operators at the remote sites. If the remote DVC Operator acknowledges the initiating DVC security policies, the remote DVC's security policies are sent to the initiating DVC Operator. Upon acknowledging the remote DVC's security policies, each DVC configures its local system in order to establish the required IPsec VPN tunnel. When a coalition partner's access policies are modified within the local policy database, the DVC is notified and must re-negotiate the VPN connection terms with each of its current coalition partners. Similarly, if a coalition partner's access is terminated, the remote DVC is notified and the relevant VPN link is dismantled. In this way, a coalition connection is established between pair of coalition partner sites wishing to communicate and thus, a fully-meshed topology is formed.

The DVC succeeds in examining the use of policy enforcement in a very thorough manner. This helps to move policy management decisions to an autonomous level. It provides dynamism in establishing and dismantling VPN connections through the use of the security policy negotiation system. However this is at the cost of some level of static information required to know where other coalition partners are within the network.

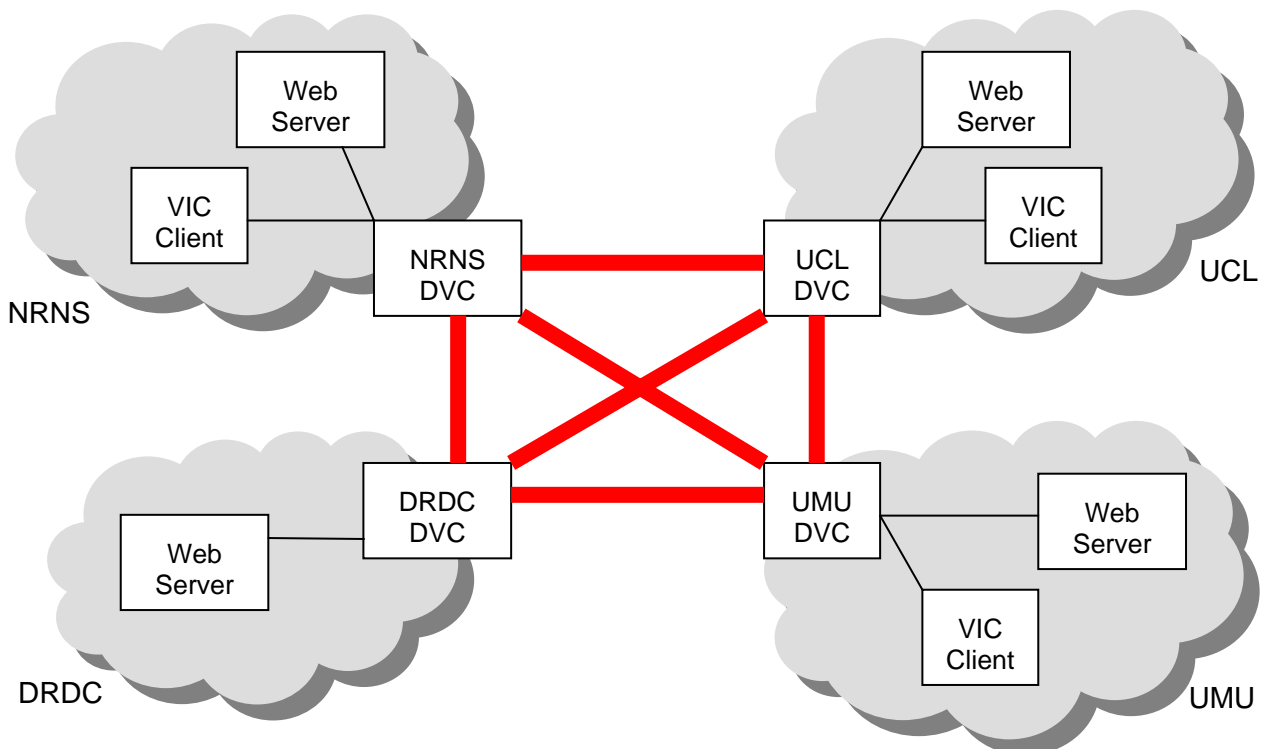


Figure 2: DRDC DVC Network Set-up

Figure 2 illustrates the various components and network set-up of the DVC deployment. Each of the sites had a DVC gateway located at their edge, behind which their network resources are secured. Web servers were installed within each of the private networks in order to provide a basic web resource to partners across the established coalition VPNs. The policies were configured to allow access to this private web server within a coalition.

For video transmission, the VIC application was used and the relevant server/service address/port pair were also activated within the respective policies of each of the participating DVC nodes in order to allow the service to be accessed through the DVC gateways.

As detailed in the previous deliverables of this activity ([1][2]), the topology created by a DVC-deployed infrastructure is a full mesh between the coalition partners involved. This is illustrated in Figure 2 by the red mesh connected between the DVC gateways.

2.2. Initial Application Deployment

The applications run over the two deployments have diversified from the initial testing stages to the more advanced stages. Initially upon establishing the various infrastructures, connectivity was tested through the use of pings run across the overlays. These were then advanced to the provision of web servers used to serve web pages across the VPN infrastructures.

The next stage was to deploy conferencing applications over the dynamic VPN infrastructures. Video (using the VIC application) was transmitted successfully across both X-Bone and DVC infrastructures.

Following the video application deployment, UCL participated in a project demonstration undertaken by the DVC system developers. The demonstration was presented by the DVC system developers to members of another arm of the Canadian defence department and involved the continued secure transmission of video from UCL over the DVC coalition VPN.

The relative ease of set-up of the DVC system then enabled it to be used to further demonstrate Voice over IPv6 scenarios. These are explained in detail in Section 2.3 below.

2.3. SIP VoIP Demonstrations over DVC

We have successfully demonstrated Voice over IPv6 applications running over a DVC-deployed dynamic VPN infrastructure. The scenario was first outlined at the Belgian IPv6 Event held in May 2004 [3]. Subsequently the scenario was demonstrated two weeks later during the 6NET review held in Brussels during June 2004.

The scenario consisted of two separate VoIP demonstrations (illustrated in Figure 3 and Figure 4 below):

- Point-to-point communication – involving communication between a combination of IPv6 and IPv4 SIP user agents, making use of SIP Express Routers (SER) for SIP call set-up and the Mini SIP Proxy (MSP) gateway to handle translation between IPv6 and IPv4.
- Multi-party communication – involving simultaneous group communication between a combination of IPv6 and IPv4 SIP user agents, making use of SIP Express Routers (SER) for SIP call set-up, the Mini SIP Proxy (MSP) gateway to handle translation between IPv6 and IPv4, and the Asterisk multi-party communication server.

Both these demonstrations were run with the first hop (from the IPv6 SIP user agent located at the demonstration site out to the SER located at UCL) secured running over a DVC-established VPN.

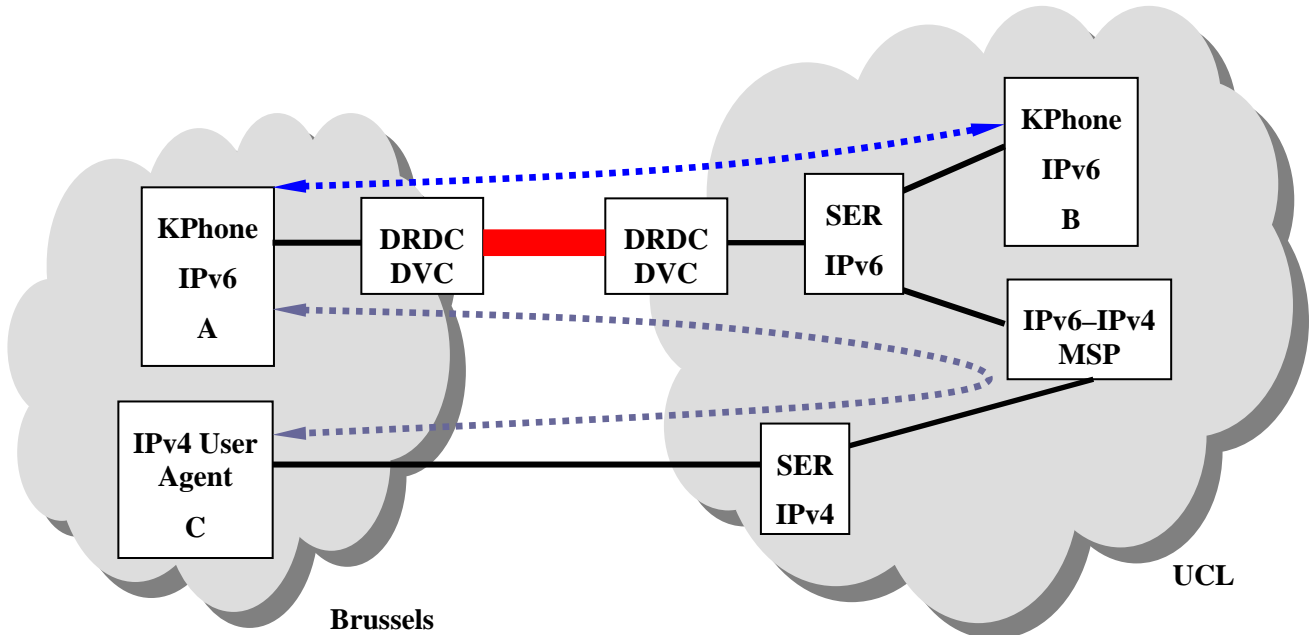


Figure 3: Point-to-point communication

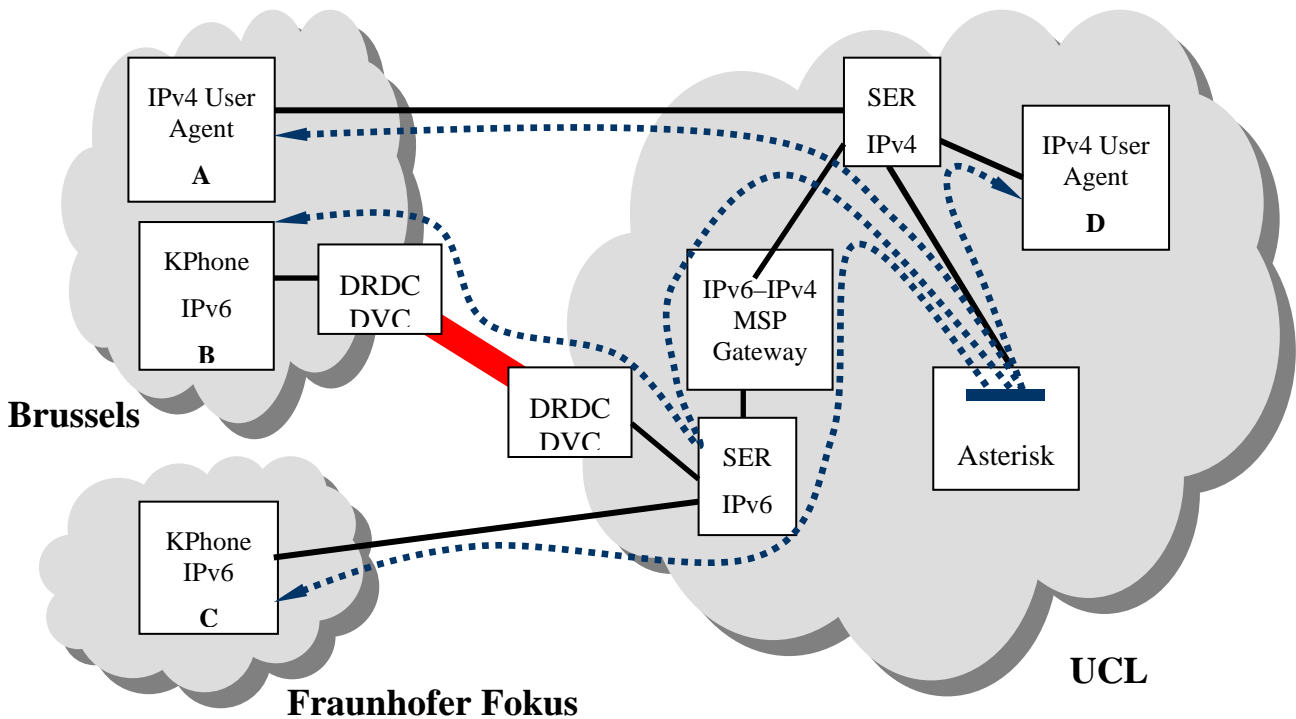


Figure 4: Multi-party communication

3. Evaluation of Deployment Results

As previously mentioned, a fully deployed IPv6-enabled VPN infrastructure does not provide, on its own, direct benefits for the project. What is important is the set of applications running over such an infrastructure.

From the perspective of the individual dynamic VPN infrastructures themselves, both deployments have been successful. Both systems have been successfully installed, configured and used in order to deploy a range of different overlays and VPN infrastructures both locally and across the wide-area involving multiple partner sites.

From the application perspective too, both deployments have been successful. We have demonstrated the use of the dynamic VPN infrastructures to secure traffic for both data (e.g. Web) and communication (e.g. video and audio) applications. One important factor is the steps taken beyond simple local testing. The applications that have been run successfully across the wide-area include a number of separate live project demonstrations. All live demonstrations involved wide-area links. The first of these was run between London and Canada (described in Section 2.2) and demonstrated the long-term stability of the DVC VPN infrastructure during which Video data was continuously transmitted over the secure infrastructure. Additionally a similar experiment was carried out with the X-Bone where video was transmitted between UCL and the ISI site, in the USA. Secondly the DVC system was operated between Brussels and London during the 6NET June 2004 review (described in Section 2.3), demonstrating SIP based VoIP operating over the dynamic VPN.

Once established, the VPN infrastructures simply provide mechanisms for securing of traffic between end-points. Delay and jitter are dependent on network and wide-area Internet conditions thus, audio and video quality remain the same as for non-VPN-secured audio and video transmission. Earlier tests highlighted certain issues, such as the need for improved error feedback; these were fed back to the system developers. Additionally as a result of reviewer feedback, during the June 2004 review, work on improvement of the quality of the audio was carried out under 6NET. This work involved the development of the SIPSet+RAT tool [9], which provided for SIP based higher quality, error tolerant, audio communication.

The dynamic nature of both VPN systems' configuration and deployment greatly reduces the time and effort required in order to secure traffic. Both the DVC and the X-Bone systems are able to establish and manage IPv6 VPNs as well as the respective IPv4-only versions available when we first began these investigations at the start of the project. Once pre-configuration is completed (with the definition of endpoints and policies in DVC and the provision of relevant parameters in X-Bone), establishment of the VPN infrastructures takes a matter of seconds following initiation. With the DVC system, new nodes can be added to a coalition through simple additions to the policy, while with the X-Bone system, new overlays may be rapidly established to as often as necessary. These techniques provide for far simpler deployment than the manual methods of IPsec configuration which are slow and prone to error, and thus greatly benefit any administrator placed in charge of VPN infrastructure deployment and management. Both systems also provide graphical user interfaces to ease further the configuration and management process.

The two systems provide complementary security services, with the X-Bone providing a rapidly configurable private network, whilst the DVC provides an edge-based, policy driven system. Both systems use IPsec at the lowest level to provide secured transport, and employ SSL to secure control communications. The X-Bone is best suited for rapid deployment of arbitrary basic network topologies for application deployment and testing, providing a secured private network overlay. The

DVC allows for policy-based finer grained control over inter-site-based connectivity for controlled deployment of specific services.

There would be considerable scope to use much richer facilities in both systems. For the X-Bone these could allow for much more control of security parameters and hierarchical overlays. Whilst with the DVC much richer policy controlled deployments would be possible. However there was too little practical demand within 6Net for these services to justify substantial investigations into either of these developments.

4. Conclusions

We have run both conferencing and telephony applications across the dynamic VPN infrastructures deployed as part of this activity. Deployment of the VPNs themselves and the applications on top of them has provided valuable operational experience of running such systems. Both X-Bone and DVC were initially developed on IPv4 and have been extended to support IPv6. Whilst the differences in performance and functionality are largely similar, between IPv4 and IPv6, it is important to have such VPN system available for IPv6.

The existing solutions have only provided support for unicast over the VPN. The extension of the range of applications to include multicast-based conference applications, as suggested in previous deliverables, requires multicast routing software. Xorp [7] has been identified as a possible platform to provide a means for enabling this capability in the future.

The collaboration between UMU and DRDC detailed in the deliverable D4.3.2 [2] has continued and UCL continues to follow closely the integration efforts.

In addition, the concepts of the coalition-based approach provided by the DVC system may be useful within the mountain rescue scenario of the mobile router demonstrators (to be described in D4.6.1 [8]), in which confidential communication and data transfer is required between a number of parties. As any particular emergency situation develops and evolves over a period of time, so too will the number of parties involved in the operation. At each step of communication, highly sensitive and personal information will be vulnerable within the wireless environment and thus must be secured. We intend to investigate further the benefits of the coalition-based network approach within this scenario.

5. References

- [1] O’Hanlon. P, Kirstein. P, Lad. M. “First set of IPv6-enabled Dynamic VPNs running”. 6NET Project Deliverable D4.3.1, March 2003. <http://www.6net.org/publications/deliverables/D4.3.1.pdf>
- [2] Lad. M, Kirstein. P. “Upgraded X-Bone Facilities running over the full network”. 6NET Project Deliverable D4.3.2, February 2004. <http://www.6net.org/publications/deliverables/D4.3.2.pdf>
- [3] Belgian IPv6 Event. <http://www.ipv6event.be/>
- [4] ISI X-Bone Overlay Management System. <http://www.isi.edu/xbone/>
- [5] DRDC Dynamic VPN Controller (DVC). <http://nrns.ca/DRDC.htm>
- [6] Universidad de Murcia (UMU). <http://www.um.es/>
- [7] Xorp – eXtensible Open Router Platform. <http://www.xorp.org/>
- [8] 6NET consortium planned Deliverable D4.6.1: “Descriptions of the Mobility demonstrators from WP4”. 6NET Project, June 2005.
- [9] O’Hanlon. P, Varakliotis. S, Ruppelt. R, Fiedler. J, “Realisation of IPv6/IPv4 VoIP Integration Scenarios”. 6NET Project Deliverable D5.11, February 2005. <http://www.6net.org/publications/deliverables/D5.11.pdf>