Naval Research Laboratory

Washington, DC 20375-5320

NRL/MR/5590--06-8979

How to Use FASTLANEs to Protect IP Networks

CHRISTOPHER L. ROBSON

Center for Computational Science
Information Technology Division

August 18, 2006

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
18-08-2006	Memorandum Report	2003-2006

4. TITLE AND SUBTITLE

How to Use FASTLANEs to Protect IP Networks

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Christopher L. Robson

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Research Laboratory, Code 5590
4555 Overlook Avenue, SW
Washington, DC 20375-5320

8. PERFORMING ORGANIZATION REPORT NUMBER

NRL/MR/5590--06-8979

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR / MONITOR'S ACRONYM(S)

11. SPONSOR / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Although ATM is widely deployed by the DoD and the Intelligence Community (IC), there are many IP-based networks being deployed and many ATM networks are being converted to IP converged topologies. These networks will be based on a Multi-Protocol Label Switched infrastructure. Further, the protection of these converged networks is still a formidable task without a clearly defined solution. By using appropriate configuration and taking full advantage of new IP technologies and successful network encryption FASTLANE devices, interconnecting individual agency networks into a common backbone infrastructure can take place successfully. Further, through the use of existing and new IETF standards, these networks can provide Quality of Service (QoS) to traffic flows between protected enclaves. This report details a hybrid architecture consisting of IPv4 and IPv6 network devices interconnected over a common IP backbone supporting protected information and IP QoS in a new IPv4/IPv6 Interim Transitional Hybrid Network (IPITHN) architecture.

15. SUBJECT TERMS

Information assurance within Internet Protocol networks by incorporating KGI-75A technology as the data protection device

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Christopher Robson
Unclassified	Unclassified	Unclassified	UL	26	**19b. TELEPHONE NUMBER** *(include area code)* (202) 404-3138

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

CONTENTS

How to Use FASTLANEs to Protect IP Networks

By Christopher Robson
Naval Research Laboratory
Chris.Robson@nrl.navy.mil
202-404-3138

1. Introduction

While ATM networks are widely deployed by the DoD and the Intelligence Community (IC), IP-based networks are beginning to be deployed and many ATM networks are being converted to IP converged topologies. Further, due to DoD Directive 8000.1, IPv6 will most likely be deployed in at least some DoD/IC locations. However, the convergence to an all IP network will not be completed until well into the 2008-2010 timeframe. And the Intelligence Community most likely will not replace the existing IC backbone until 2012. Even then, these networks will likely be based on a Multi-Protocol Label Switched infrastructure. Further, the protection of these converged networks is still a formidable task without a clearly defined solution. It is the position of this paper that with the proper guidance and standards, all these network topologies can be deployed successfully on one converged network. Furthermore, this convergence can be accomplished today. By using appropriate configurations and taking full advantage of new IP technologies, interconnecting individual agency networks into a common backbone infrastructure can take place successfully. Additionally, it is possible to use existing highly successful network encryption technology, the FASTLANE, while development proceeds with the High Assurance IP Encryptor (HAIPE). Further, through the use of existing Internet Engineering Task Force (IETF) Internet Protocol (IP) standards these networks can provide Quality of Service (QoS) to traffic flows between protected enclaves. If the DoD/IC wants to effectively interconnect diverse systems, a common approach for deploying network segments is required. This paper demonstrates this is achievable with full success. It will detail a hybrid architecture consisting of IPv4 and IPv6 network devices interconnected over a common IP backbone supporting protected information and IP QoS in a new IPv4/IPv6 Interim Transitional Hybrid Network[1] (IPITHN) architecture.

This specification will promulgate a minimum set of rules for the creation of a modified DoD/IC Internetworking infrastructure. Using acceptable IETF network element standards, this new IPITHN DoD/IC standard will promote the seamless interconnection of independently controlled autonomous agency networks; networks that are currently concatenated into an interoperable

[1] Historic note: Prior to the publications of this paper IPITHN was referred to as the FASTLANE Encrypting Optical Networks (FEON) architecture. The name was changed to better reflect the broader scope of the architecture. Therefore any continual reference to FEON will denote the IPITHN.

Manuscript approved June 5, 2006.

inter-network with assured traffic flows such as constant-bit-rate (CBR), unspecified-bit-rate (UBR), near real-time variable-bit-rate (NRT-VBR) and real-time variable-bit-rate (RT-VBR)[2].

IP encryptors cannot currently provide protection that meets current DoD/IC DCID IA policy standards. This is mostly because current IP encryption specifications are based on the IPSec standard. Further, to date, no currently-deliverable IP-based encryptors have been either certified or accredited to the protection standards set by many of the communities of interest. However, combining an ATM encryptor, notably the FASTLANE, with various IP standards the IPITHN can overcome exiting limits of today's IP encryptors. This paper will clearly demonstrate how this can be achieved using the concept of the IPv4/IPv6 Interim Transitional Hybrid Network architecture.

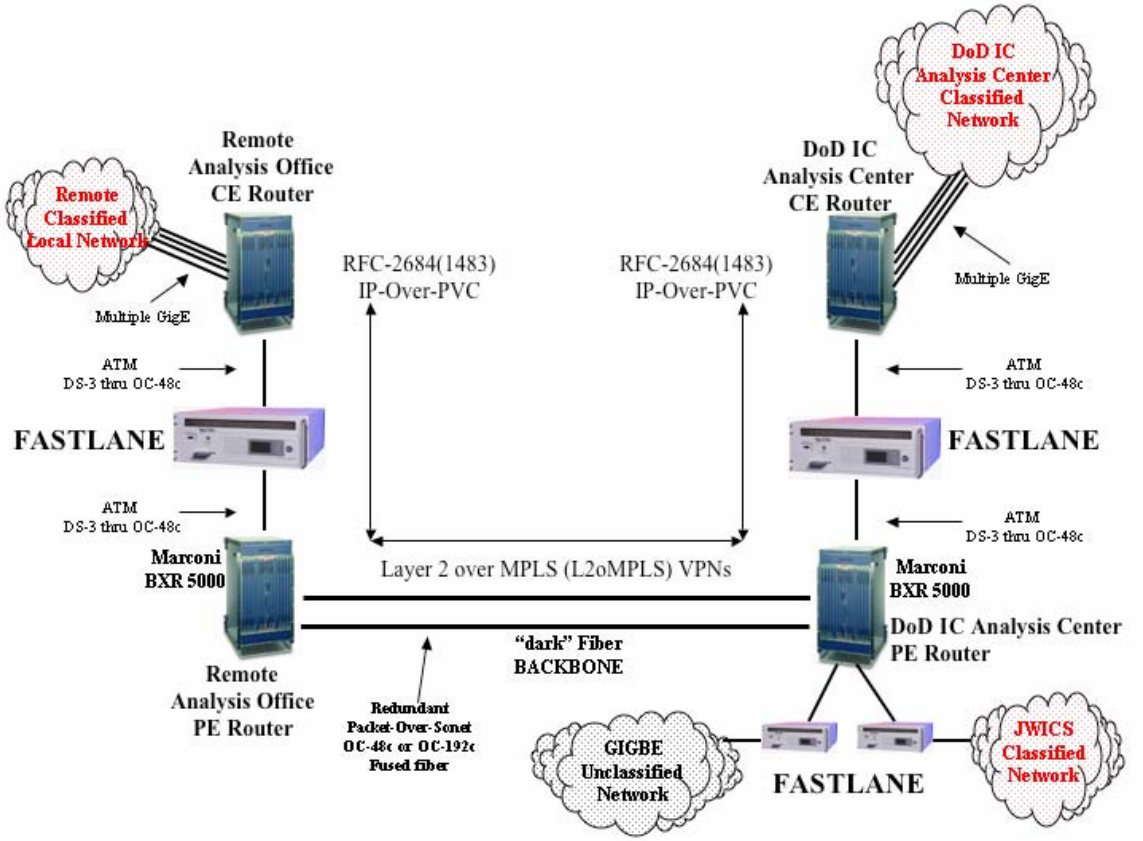


Figure 1: FASTLANE Protected IPv4/IPv6 Interim Transitional Hybrid Network (IPITHN)

This document will detail how the DoD/ICI implementation of an IPv4/IPv6 Interim Transitional Hybrid Network using FASTLANEs, can successfully and fully integrate protected converged networks. The document proposes to demonstrate the feasibility of deploying an IP-based architecture within the DoD/IC that supports traffic flows with service guarantees and data protection. Therefore the DoD/IC can dramatically reduce network build out costs, continue to make efficient use of current ATM high speed network encryptors and be in an excellent

[2] References to Quality-of-Service (QoS) within this document are solely based on IETF standards for QoS for IP traffic flows. It is not within the scope of this document to determine or promote comparison of competing definitions of QoS standards.

position to transition these existing network encryptors with newer IP and Optical based technologies without significantly changing the IP architecture. Figure 1 illustrates a hybrid mix of technology engineered by this specification. Specifically, it shows how to connect remote analysis facilities, command centers and deployed units to a headquarter analysis center by configuring CE routers[3] connected to a local PE routers[4] to an IP backbone. Like the remote facilities, the analysis center has a PE router connected to the WAN IP backbone interconnect and a local connection to the local HQ CE router. Further this illustrated path is protected through a secure encrypted IP interconnect with FASTLANEs. By incorporating multiple logical and physical interfaces within the CE and multiple interfaces to the PE router, priority based, far weighted queuing, as an example, can be applied to each of the individual interfaces. Thus, this interface can be used to control traffic between remote facilities and the parent facility and given interfaced controlled QoS based on requirements associated with the remote facilities policy.

Figure 2 illustrates how this architecture can support legacy networks such as ATM yet grow to support any future encryptors such as the HAIPE. This can be seen by the interconnections of the DISN and JWICS networks through the pair of FASTLANE and HAIPE encryptors at each site.

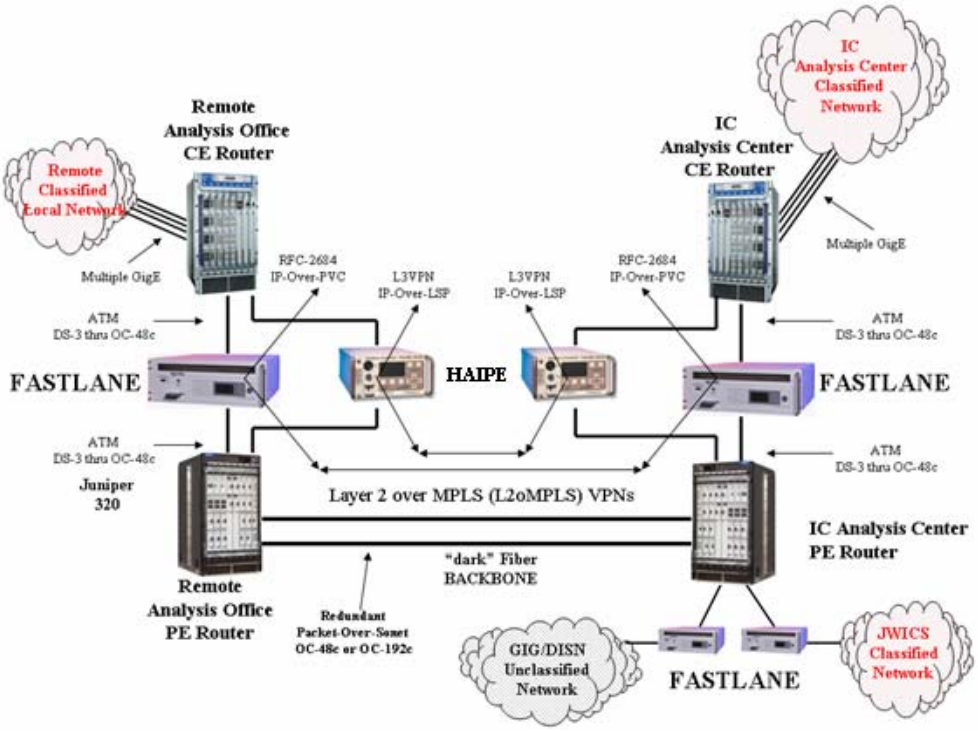


Figure 2: IPITHN transition to a MPLS enabled HAIPE

[3] A CE (Customer Edge) router is a device, which is attached via some sort of data link (e.g., PPP, ATM, ethernet, Frame Relay, GRE tunnel, etc.) to one or more Provider Edge (PE) routers as defined in RFC- 2547, "BGP/MPLS VPNs".

[4] A PE (Provider Edge) router is a device, which is attached via some sort of data link (e.g., PPP, ATM, ethernet, Frame Relay, GRE tunnel, etc.) to one or more Customer Edge (CE) routers and or more Provider (P) routers as defined in RFC- 2547, "BGP/MPLS VPNs".

2. Typical DoD or Intelligence Community protected network.

Typically, network engineers have used two types of encryption devices, the link encryptor to protect point-to-point networks and/or the network encryptor to protect networks. The major advantages with the network encryptor are scalability and lower overall cost. Typically, higher speed link encryptors such as the KG-189 are deployed on aggregated trunk lines and not at all network sites. This is primarily because, like the older KG-95 link encryptor, one encryptor is required for each path between sites. For example, if site "A" wished to interconnect to two other sites, site "A" would require 2 encryptors (Figure 4). A network encryptor such as the KG-75 FASTLANE, KG-175 TACLANE or HAIPEs, allows site "A" to connect to one or more remote sites through a single site/enclave encryptor (see Figure 5). Thus a network encryptor dramatically reduces the cost of network deployment and increases the scalability of the network. Unfortunately and prior to this proposal, non-ATM backboned networks were limited to backbone speeds under OC-3c due to the interface limits of other network encryptors such as the NES or TACLANE. The currently accredited FASTLANE provides the ability for networks to achieve network speeds up to OC-192c. The FASTLANE provides all the advantages of cost and scalability because it is a network encryptor. However, it has always been assumed that only ATM networks could make use of the FASTLANE encryptors. As Figure 1 demonstrates, this assumption is false. This paper references tested prototypes which demonstrate the feasibility of this concept of protecting IP networks. The prototypes, shown in figures 10 and 11, were successfully built and tested to demonstrate how to deploy IP networks using FASTLANEs. Additionally, with proper configuration, a high level of security can be achieved using the FASTLANE in conjunction with IPv4/IPv6 routers and firewalls. Importantly, this design will allow network engineers to protect IP networks today - far in advance of scheduled deployments of the High Assurance IP Encryptor (HAIPE). In fact, by combining new IETF network standards and IPv4/IPv6 L2oMPLS, BGP/MPLS L3VPNs (RFC-2547) along with BGP-MPLS IP VPN extensions for IPv6 VPN (6VPN) integrated with legacy IPv4 and ATM, any network architecture, with protection, can be achieved, producing a highly secure and fully functional network architecture for the DoD/IC. Figure 3 shows how this is accomplished.

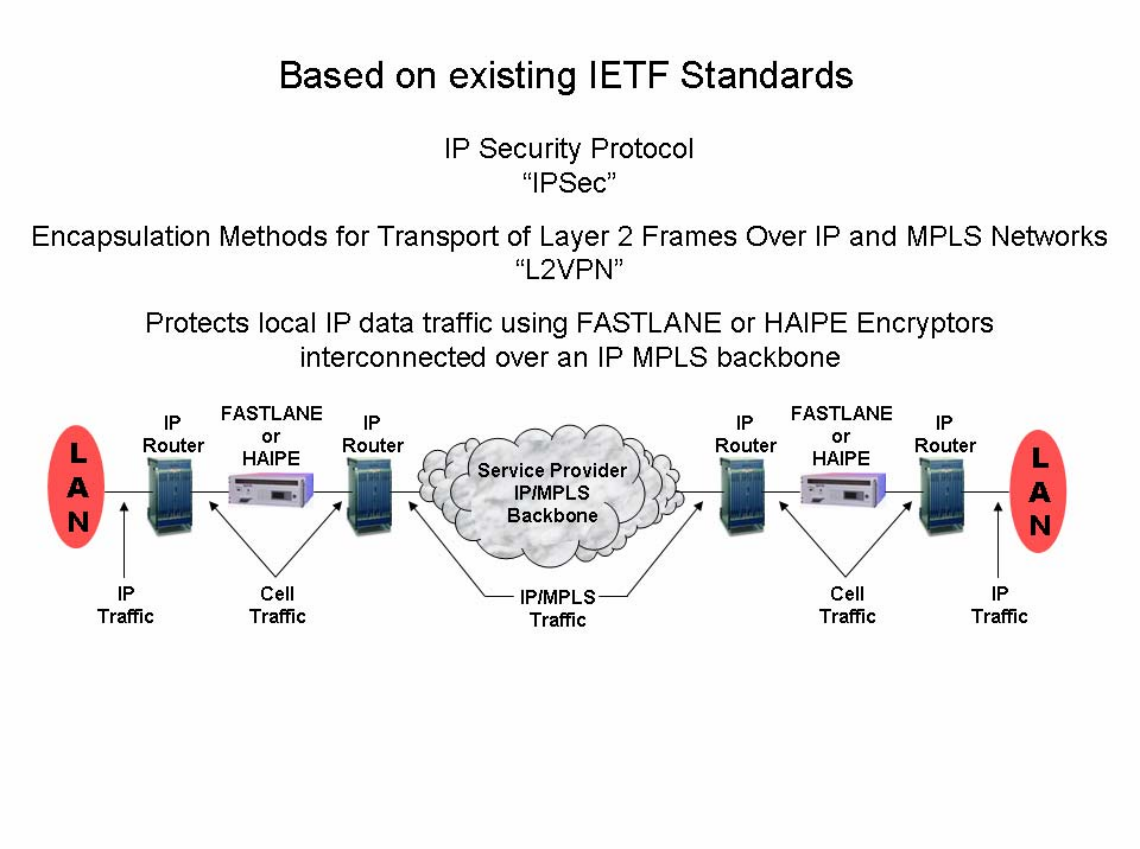


Figure 3: IPITHN FASTLANE Configuration

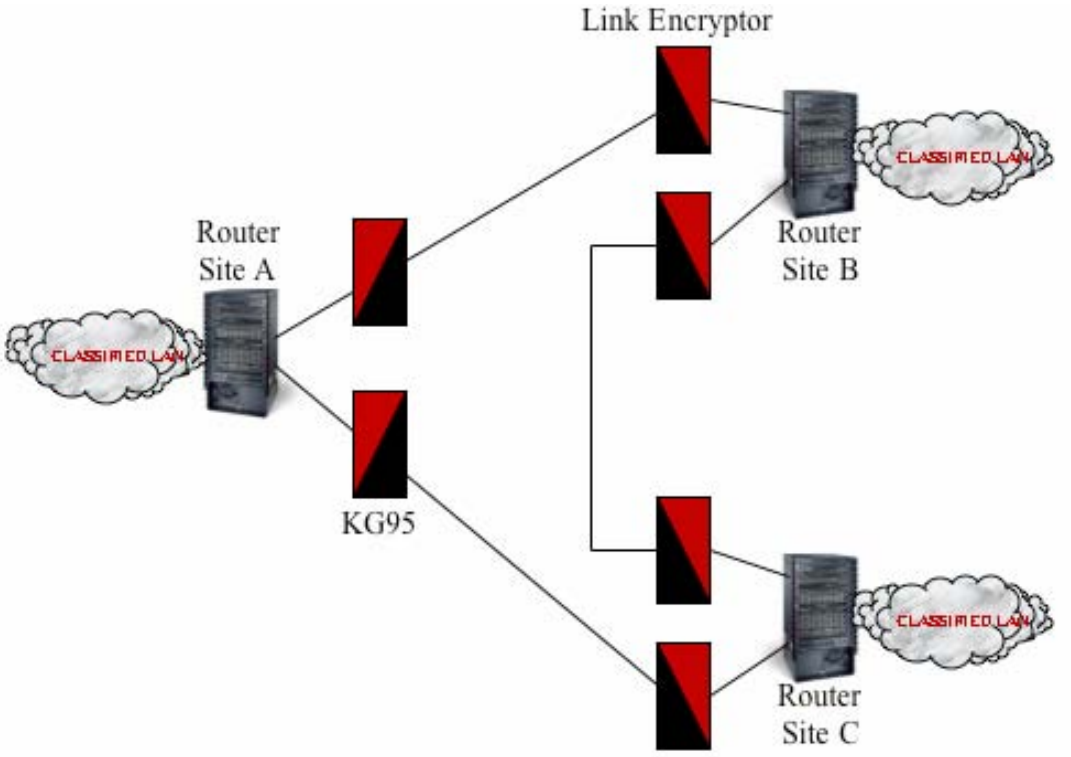


Figure 4: Link Encryptor Configuration

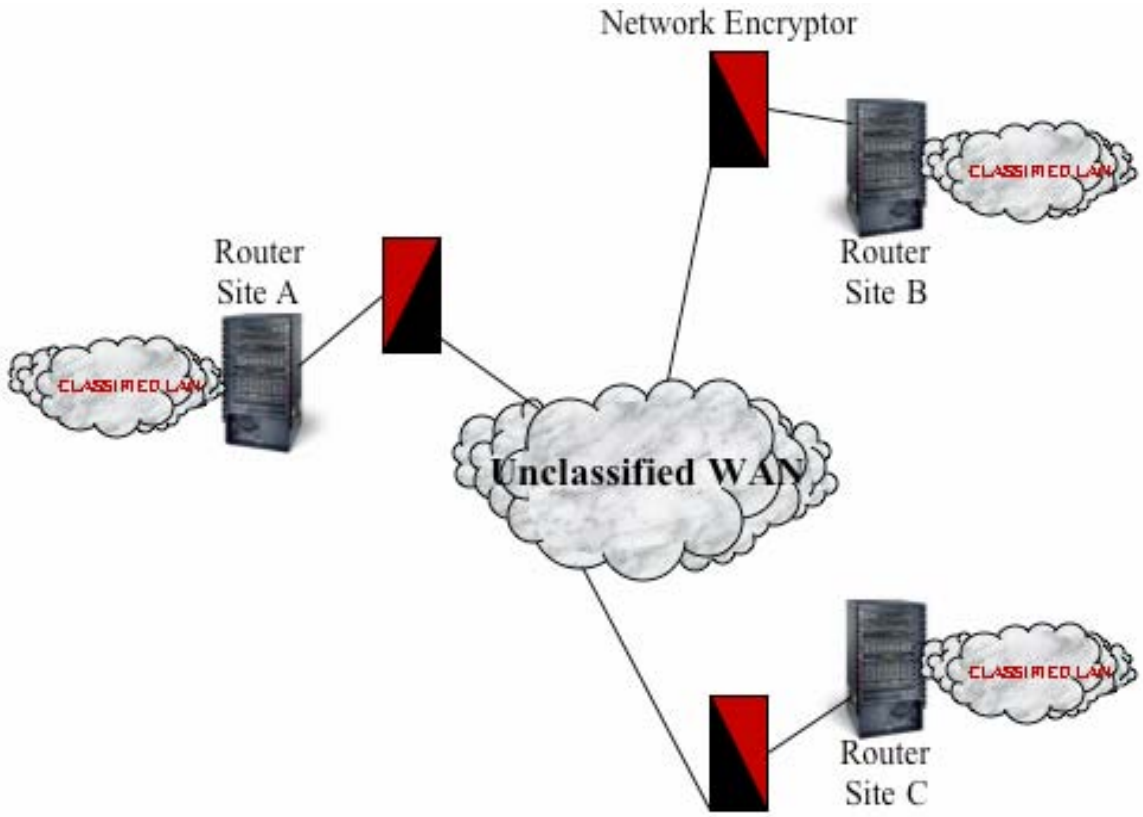


Figure 5: Network Encryptor Configuration

3. Common DoD/IC network path configuration.

In order to provide the best security for FASTLANE encrypted ATM networks, network engineers and security policy makers usually deploy PVP and PVC[5] meshed configurations. The typical configuration of networks secured by FASTLANEs start with a "BLACK" unclassified ATM switch interconnected to the FASTLANE's cipher port. Then the FASTLANE's Plain Text port is connected to a "RED" classified ATM switch. Using this configuration, engineers will configure the FASTLANEs with pass-through PVCs or PVPs, commonly called "RED" PVPs. They then connect and configure a "RED" side IP router with an IP-Over-PVC bridge (RFC-2684) between site RED routers on the network. Although this configuration does not take advantage of the FASTLANE's ability to support on-demand, dynamically switched traffic flows, most administrators require the added security that a PVC provides. Additionally, the "RED" IP router will be configured with IP firewall security for the local site. At most DoD/IC sites that connect to a community ATM backbone, it is common to restrict or disallow the use of directly attached "RED" ATM connections. This restriction allows sites to achieve the maximum level of network security and control. Figure 6 illustrates the today's typical JWICS or DISN site configuration used to connect to a common unclassified backbone.

[5] A PVC network by definition is a permit, manually configured path between ingress and egress network access points.

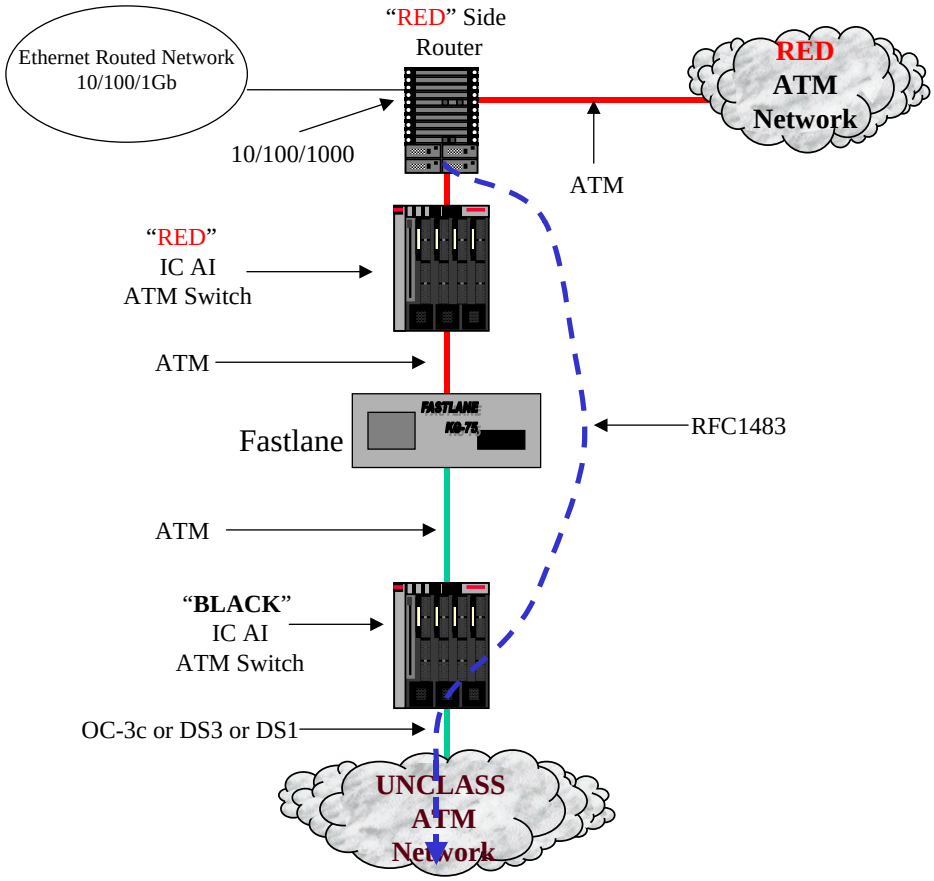


Figure 6: Existing FASTLANE DoD/IC Site Configuration

4. Current ATM QoS control plane.

In today's DoD/IC networks secured by FASTLANEs, QoS is achieved by associating a PVC QoS policy to a manually configured "BLACK" network PVC. Engineers will typically associate several preconfigured PVCs to several CBR circuits for high priority traffic and several PVCs to several UBR circuits for all other traffic. Although this doesn't take full advantage of all the QoS capabilities an ATM network can provide, this is generally done to assure better security control and to simplify network deployment and life-cycle maintenance. Therefore, this common configuration allows minimally trained personnel to maintain the circuits. By using the IPv4/IPv6 Interim Transitional Hybrid Network suggested in this paper, this same QoS can be achieved over DoD/IC core IP/MPLS infrastructures. This paper demonstrates that by associating infrastructure QoS policy to L2VPN and L3VPN "RED" and "BLACK" services, equivalent ATM QoS services can be offered within DoD/IC IP infrastructures.

5. IP QoS control plane.

The simplest approach to associating QoS Service Classes to a L3VPN Virtual Routing and Forwarding (VRF) infrastructure is to statically configure Label Switched Paths (LSP) with

appropriate QoS policies. Obviously scaling and survivability becomes an issue with engineering this type of configuration. Another approach would be to engineer LSP RSVP configurations[6]. This lends itself to a more dynamically controlled network. This configuration emulates "BLACK" switch circuits in DoD/IC ATM networks. Detailing the DoD EF/AF Service Classes are not within the scope of this paper but Figure 7 illustrates how these services classes will be engineered into four VRF-to-QoS table associations.

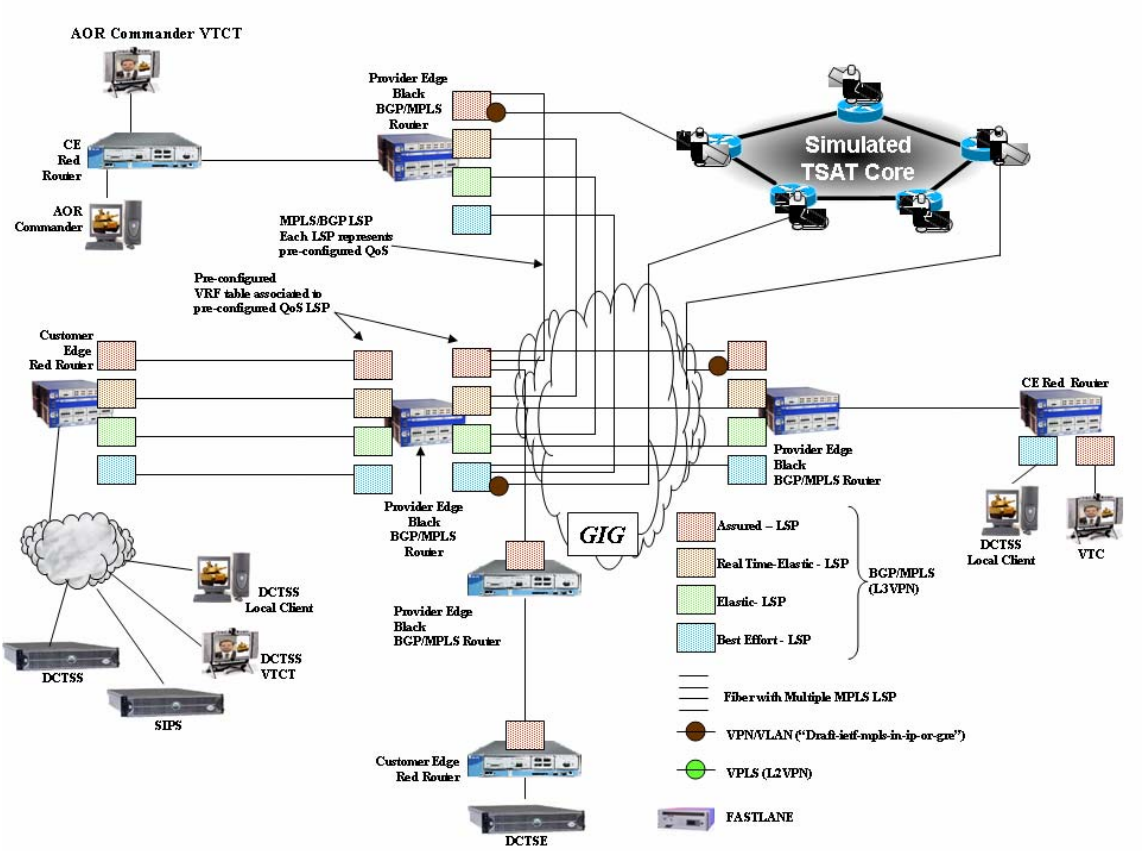


Figure 7. L3VPN QoS LSPs and VPNs

As depicted in the drawing, what is normally a CE router by L3VPN definition, would be a router with both CE and PE functions. This router would function as a CE when exchanging traffic with the local network. Further, each of the associated VRF table instances within this router would be assigned a pre-programmed site Security Association (SA) and QoS policy. By definition these pre-programmed VRF associates would be aligned to specific VLAN paths to the site PE, passing through the site Encryptor (either a FASTLANE via PVC or HAIPE via an IP VLAN). Likewise by definition, because the local CE-PE router functions as a CE router to the site GIG[7] PE router, each of the VLAN paths would be associated to a VRF instance within

[6] It is not within the scope of this plan to propose IP QoS Control Plane alternatives undergoing research and development. This paper will only focus on existing IP QoS control plane technologies such as Resource Reservation Protocol.

[7] The Global Information Grid (GIG) will be a net-centric system operating in a global context to provide processing, storage, management, and transport of information to support all Department of Defense (DoD),

the PE. Since packets passing from the CE through the encryptor will be encrypted, each PE L3VPN VRF instance to a CE interface will be assigned by an interface route within the PE. L3VPN VRF routing, security and QoS associations within the PE for subsequent forwarding through a GIG LSP will be pre-programmed and function as the PE router to the site GIG P. That is each GIG LSP connected to the site PE VRF instance has a pre-programmed site Security Association (SA) and QoS policy applied to the LSP. Additionally, figure 7 illustrates how MPLS in IP or GRE can successfully interconnect MPLS with non-MPLS infrastructures such as the GIG to TSAT interconnect. Simply put, each BGP/MPLS VRF table is mapped to a Virtual Private Network at the ingress PE router traversing through a non-MPLS network to its associated egress PE router. In this way, MPLS LSPs can be mapped across TSAT networks which will not support MPLS LSPs. Since the TSAT core will support PHB Service Classes, networks such as the GIG will not experience any loss of QoS. Figure 8, illustrates the slight modification required to enhance the concept when protection networks using FASTLANEs. Specifically, it is believed the same VPN scheme used to traverse the TSAT Core can be employed to traverse through any encryption devices.

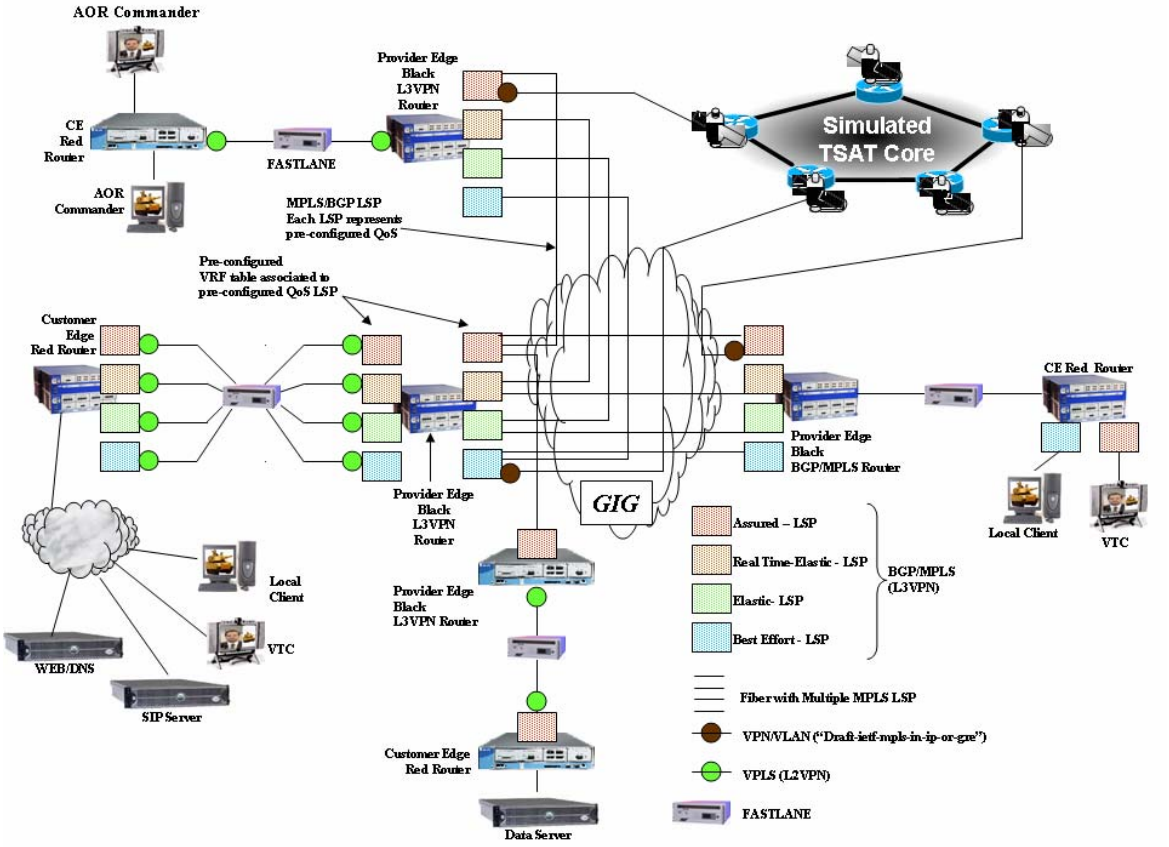


Figure 8. L3VPN QoS LSPs and VPNs with FASTLANE

6. IP traffic bandwidth solutions.

national security, and related Intelligence Community missions and functions-strategic, operational, tactical, and business-in war, in crisis, and in peace.

Today's accredited FASTLANEs support throughput rates up to OC-192c. However, there are limited offerings in IP routers available supporting 10Gbps ATM interfaces compatible with the FASTLANE. This limits the ability to make use of the OC-192c FASTLANE. There are, however, several possible alternatives. One is to deploy a Multi-Service Switch that supports OC-192c POS and OC-192c ATM. Figure 9 illustrates this configuration. The criticism to this configuration is the additional cost and continual requirement for ATM network equipment. A second solution is to deploy new technologies that are still under development. Another interim solution which can be deployed today, is to configure sites with multiple OC-48c interfaces. Although the cost can be of concern, it affords two key advantages to the other configurations. First, site survivability is enhanced with multiple access points. Second, higher bandwidth can be achieved though bandwidth aggregation. It is this last configuration that this paper will focus on since it is the most to be deployed within the DoD/IC.

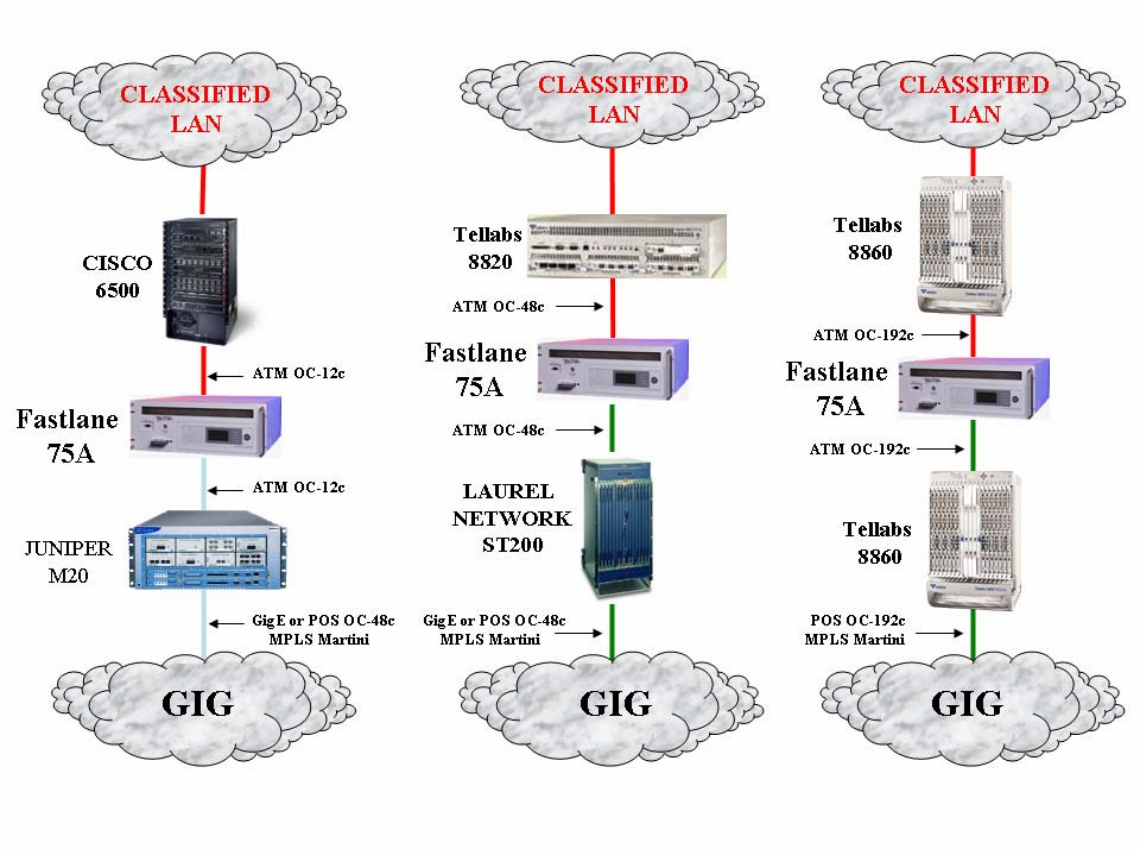
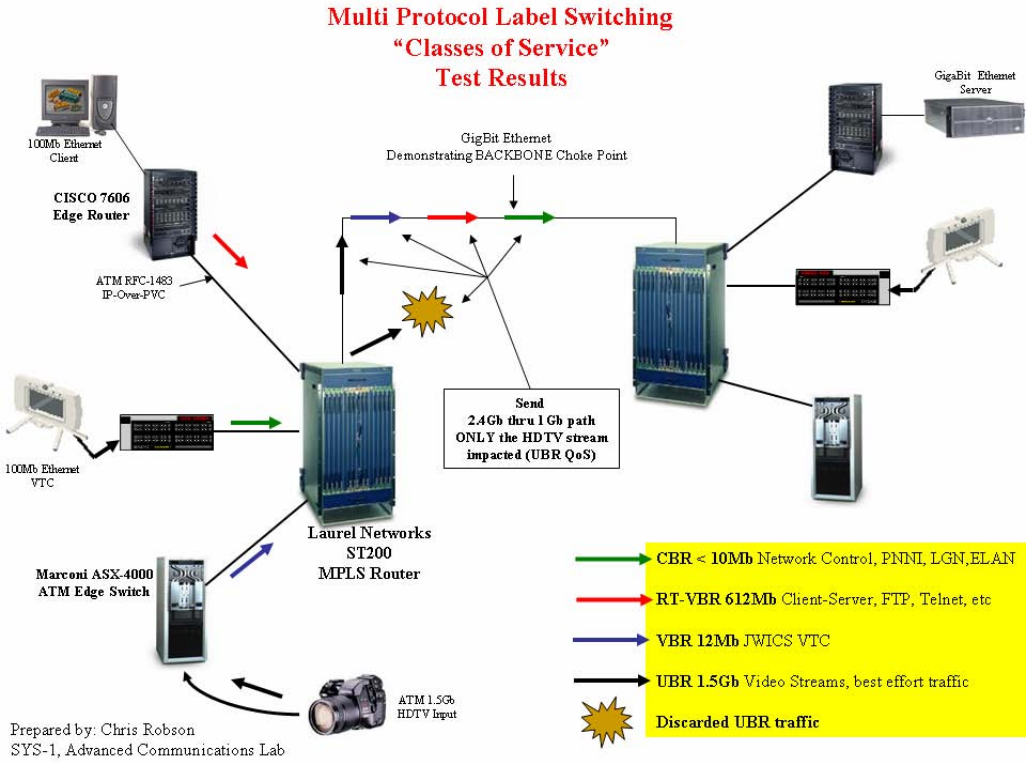


Figure 9: Example IPITHN Node Configurations

7. Successfully tested L2VPN prototype.

To prove that this architecture is a viable solution, the network in Figure 10 was constructed and successfully tested. This configuration consisted of two typically configured DISN Service Delivery Node (SDN) Provider Edge (PE) routers. To simulate a Wide Area Network (WAN) connection, the two simulated PE routers were connected via Gigabit Ethernet (GigE) interfaces. Three local interfaces were configured. The first local interface was configured as an ATM

SONET interface and was programmed to be a DoD/IC ICI compliant network interface[8]. Then this interface was attached to a local ATM switch, simulating a DISN DOD/IC connection. The local ATM switch was then connected to a typical DoD/IC application such as a JWICS VTC system[9]. A second interface on the PE was also connected to another ATM switch. This connection simulated a high speed (1 Gbps or higher) interface. This allowed a video stream which exceeds the configured bandwidth of the port to be introduced into the core network. A video stream, sourced from the high speed connection, was then transmitted through the PE router for QoS saturation testing. The video stream source for this test was an uncompressed HDTV pre-recorded playback at 1.5 Gbps. The third and final interface simulated typical DoD/IC IP data traffic such as a JWICS Portal. This interface incorporated a typical JWICS complaint IP router with an ATM uplink to the PE router. As the figure illustrates, all traffic flows traversed the backbone connection between the two PE routers over the GigE connection. Obviously, the uncompressed HDTV traffic failed in this configuration because the HDTV traffic exceeded the available bandwidth of the PE router WAN interface. However, despite the ability to over tax the WAN connection, the lower bandwidth traffic successfully passed between end-systems with no recorded loss, delay or jitter. This was accomplished by programming the PE routers with priority queuing QoS parameters detailed in figure 10. To further test the concept presented here, FASTLANEs where introduced into the configuration as detailed in figure 11. The simulated JWICS VTC devices were reconfigured as IP devices and attached to the CE routers. In so doing, this test successfully proved the IPITHN could support KG-75 FASTLANE encryptors.



[8] Based on the IC CIO and JWICS as defined in the "Intelligence Community ATM Interface (IC AI) Logical Group Node Hierarchy." specification.
[9] In this prototype two Marconi Virtual Presence Terminals (ViPr) where used to simulate the JWICS VTC equipment.

Figure 10: Completed Simulated GIG CE and PE Prototype Testing

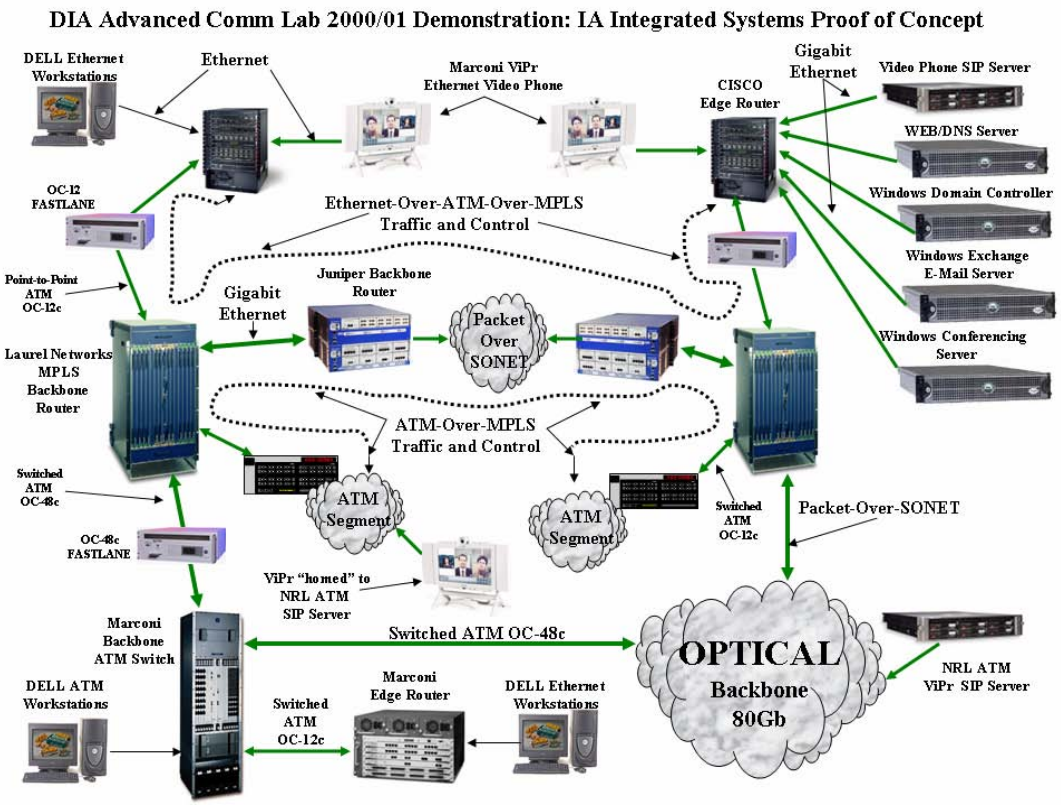


Figure 11: Completed Test Simulating DISN CE and PE Prototype with FASTLANE

8. Successfully completed L3VPN prototype.

To prove the benefits and deployment feasibility of L3VPN service within the IPITHN another prototype network configuration was built on the GIG Evaluation Facilities testbed. Using a combination of GIG compliant Juniper routers and open source Linux routers a successful prototype clearly demonstrated that L3VPN within the IPITHN can benefit the DOD/IC. As figure 12 illustrates traffic separation and communities of interest were successfully constructed using L3VPN technology. To accomplish this three Juniper routers were interconnected over an IS-IS routed backbone. Then MPLS label switched paths where established between the PE routers creating a meshed backbone to simulate a GIG Service Delivery Node (SDN) Provider Edge (PE) router interconnect between typical DoD enclaves. Linux routers built upon Red Hat Fedora Core 4 open source kernel and the Quagga TCP/IP protocol routing stack function as local DISN Customer Edge (CE) routers. Further, to simulate an IC community of interest an additional virtual private network (VPN) was established. This VPN can be viewed as a dedicated direct connection between SSC-SD CE214 and NRL TestDev2 (see figure 12). Specifically, this connection is an IP bidirectional routed path beginning at CE214 through NRL TestDev3. From TestDev3, traffic is directed by local BGP and OSPF routes through NRL TestDev4. This traffic then returns to SD via the NRL Juniper M10i PE because of L3VPN virtual routing and forwarding table (VRFT) VRF-212 routes. From the SD PE, this traffic is

directed to CE212 which is the local CE for VRF-212. CE212 forwards this traffic to CE213 via the Ethernet link between CE212 and CE213. CE213, the CE router associated to SSC-SD M7i PE VRFT VRF-213, will forward the traffic through the GIG-EF to the NRL PE VRFT VRF-213. This traffic is then forward by the NRL PE to the NRL CE VLN 213, TestDev2. Finally, TestDev2 forwards this traffic to the end system via NRL edge router, TestDev6. Traffic distended for the CE214 LAN for any TestDev2 local networks will return through the same path just described. The purpose of this path was to demonstrate the ability to keep separate system views and routing table updates which exist within the VLN 214 LAN from routes in the backbone domains. Typically in today's ATM networks this is accomplished with site local end-to-end PVCs. Clearly this successful configuration demonstrates the ability to accomplish similar separation when using IP MPLS LSP L3VPNs.

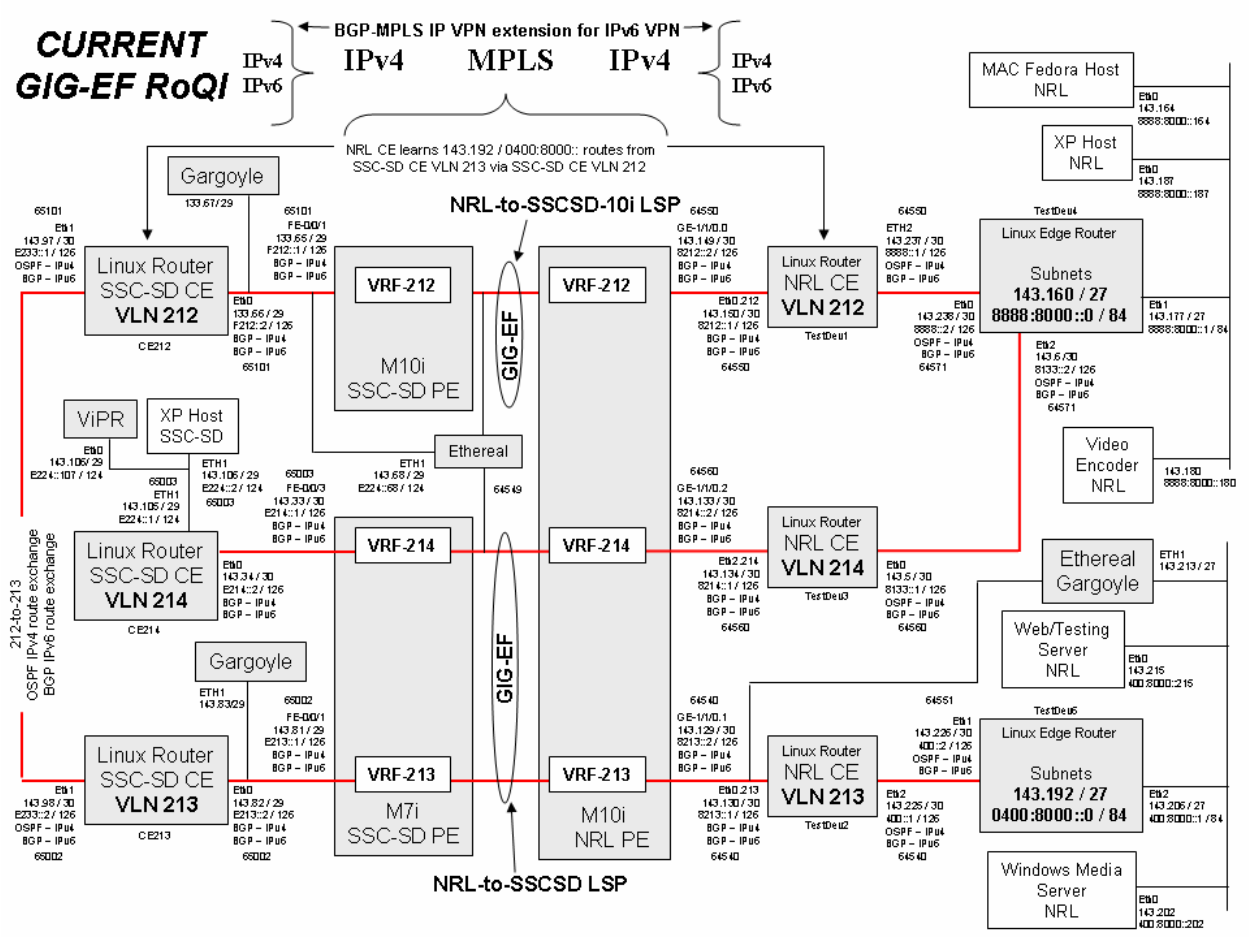


Figure 12: Successful L2VPN, L3VPN and 6VPN Testing

9. Evaluation of cost benefits of an IPv4/IPv6 Interim Transitional Hybrid Network architecture.

The following figures outline a brief look at the cost comparisons of typical DoD/IC configurations. To keep the focus of the comparison as simple as possible the following assumptions set the ground rules for the analysis:

- End user routers are required.
- Highest level of protection must be assured ("Red PVC" equivalence with Traffic Flow Security).
- FASTLANEs are used.
- Line rates above 0C-12c must be supported.
- Cost assumptions include:
    - CORE sites must support high capacity.
    - Direct connections between sites.
    - FASTLANE costs: $50K per unit.
    - Red IP Router costs (with OC-12c): $50K per unit.
    - Red ATM Switch cost (with OC-12c): $50K per unit.
    - Black ATM Switch cost (with OC-48c): $150K per unit.
    - Black IP MPLS Router cost (with OC-48c): $150K per unit.

The following figures detail the four basic node configurations used as a basis for this cost comparison.

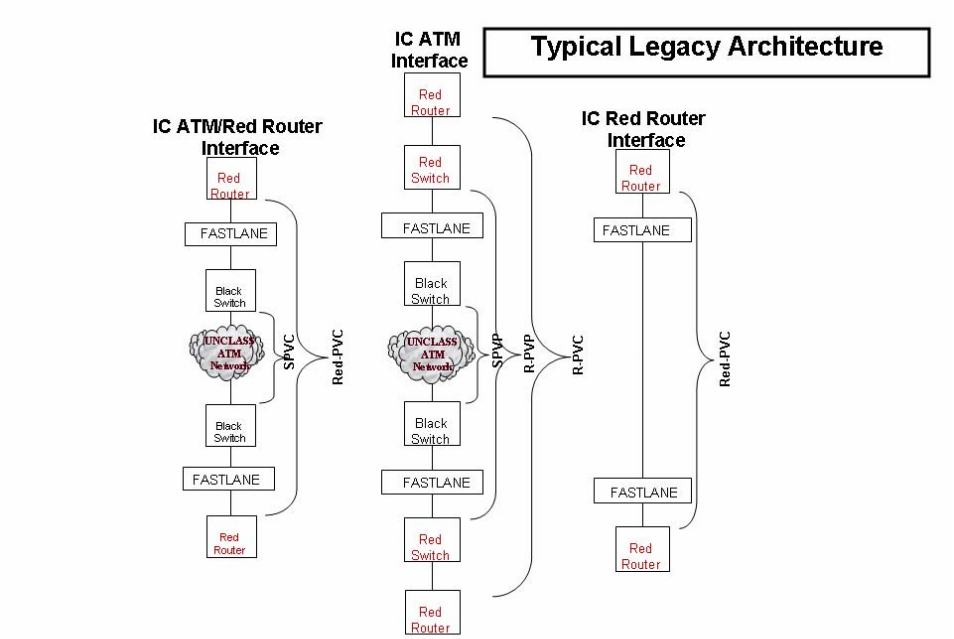


Figure 13: Typical Legacy Node Configuration

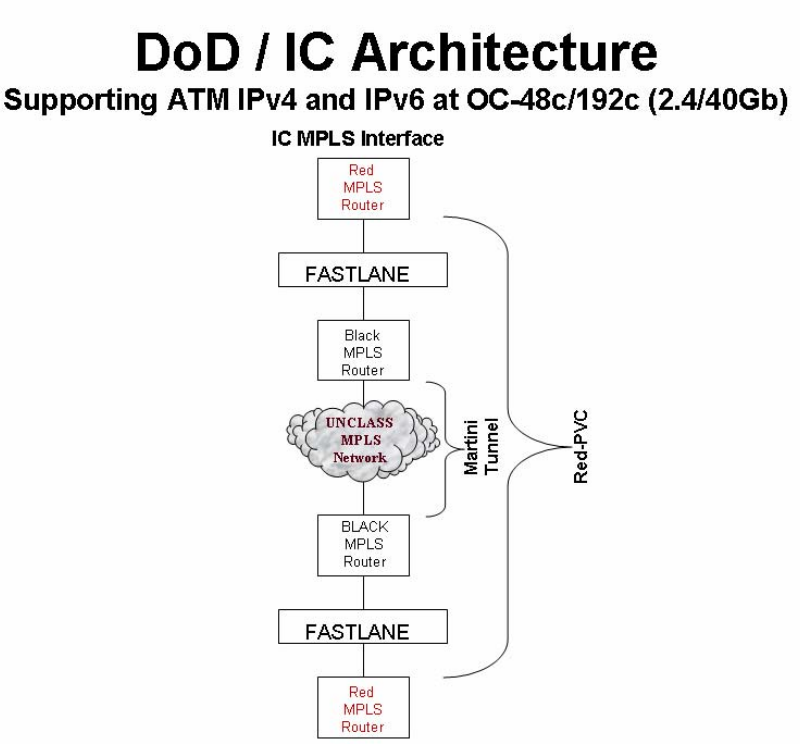


Figure 14: Optimal Node Configuration

The following chart details the costs for deploying the various node configurations detailed above. Although the chart clearly demonstrates the red router with FASTLANEs directly connected to each other (Figure 13, option 3) has a cost savings, logistics and configuration management has proven this type of deployment unmanageable. Because of the logistics benefits, to include access control, network management and point-of-presence management, figure 14 illustrates the most optimal cost benefit deployment configuration.

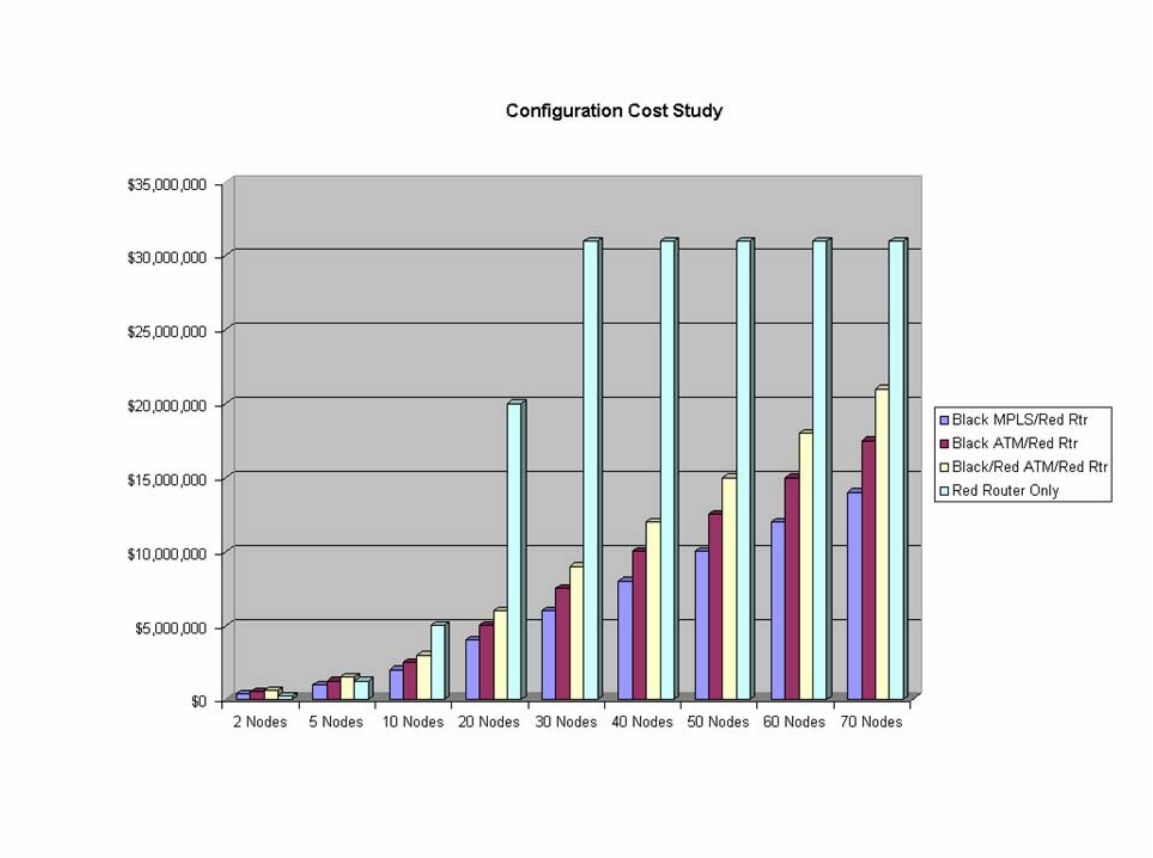


Chart: Configuration Cost Study

10. What the IPv4/IPv6 Interim Transitional Hybrid Network will look like.

The core of the IPv4/IPv6 ITHN will consist of DISN SDN Provider (P) routers interconnected through either GigE or POS interfaces. The P routers will use Intermediate System-to-Intermediate System (IS-IS) routing and interface addressing between peer P routers as well as the PE routers. The IS-IS NSAP address will adhere to the current DISN GIG specification. Further the P router will act as a Label Switch Router (LSR) for MPLS traffic. This is an important point to understand. By functioning strictly as LSRs, the P routers have no need or knowledge of PE router routing information. Thus, it provides a functional level of separation between the core network and the various edge communities of interests. The PE routers will use IS-IS NSAP addressing and routing when interfacing to P routers and exchanging MPLS LSP routing information with the P routers. The PE router will also function as a Label Edge Router (LER) for all MPLS traffic when routing traffic from the CE. Further the PE router will provide the BGP/MPLS VRF L3VPN functions, thus completely compatible with the current GIG SDN standard. To interface to the CE router, the PE will establish a VLAN. The CE router will interface to the PE router using either IPv4 or IPv6 addresses to connect to this VLAN. The CE router will function as a BGP/MPLS L3VPN and L2oVPN edge router to all routers on the CE local network interfaces and receive IGP routes from the LAN for updating the PE VRF tables. Figure 15 illustrates the network configuration.

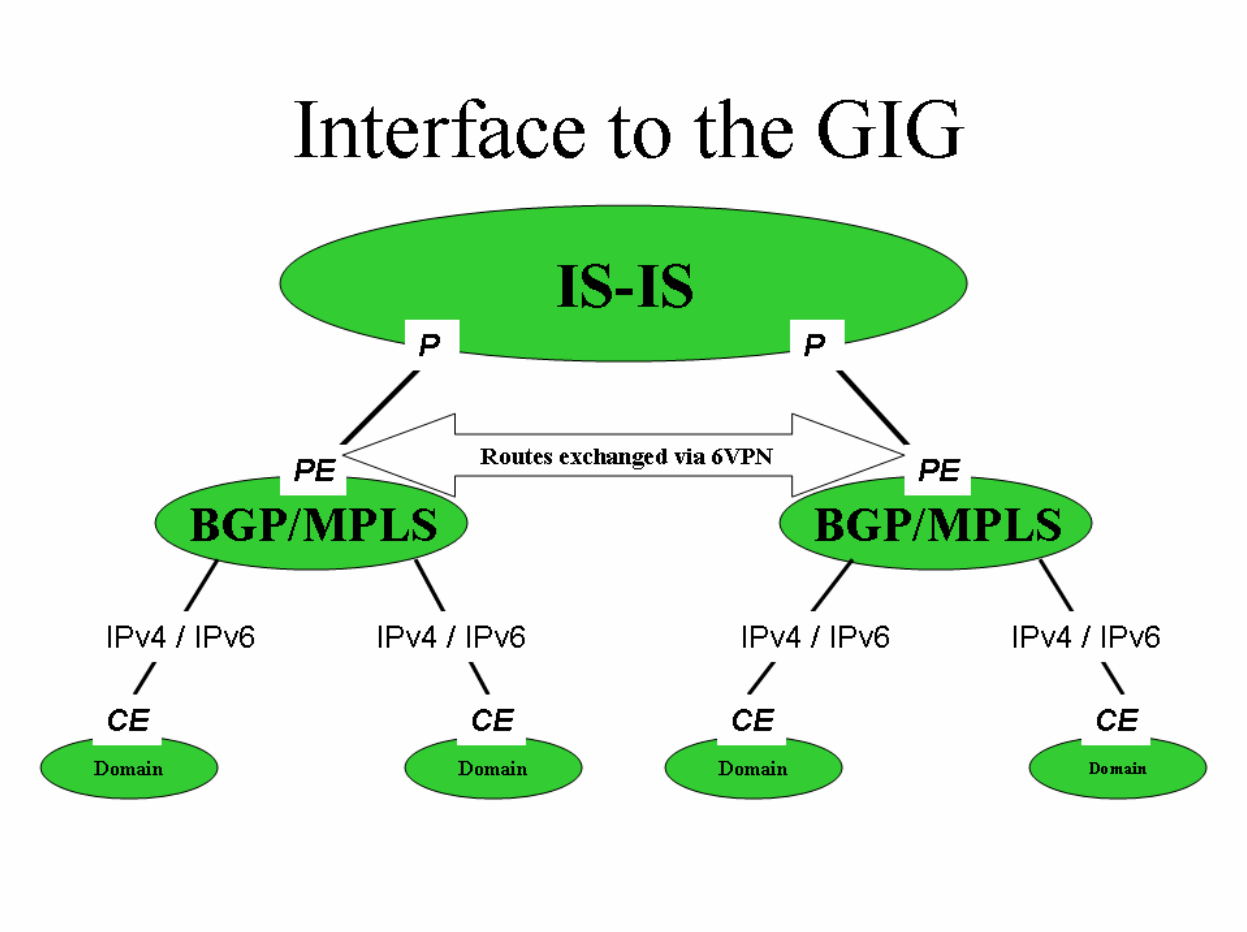


Figure 15: Interfacing to the GIG

11. How the IP QoS traffic flow control plane will function with the IPITHN.

This section will briefly describe how this QoS IPv4/IPv6 Interim Transitional Hybrid Network concept focuses on integrating IETF L2oVPN, L3VPN, 6VPN and RSVP into a seamless QoS capable architecture. Each CE and PE router will be preprogrammed with a set of Service Level Agreement predefined QoS parameters established by the various Executive Agencies. When a RSVP QoS request is received, the requested router will first determine if one of the preprogrammed parameters exists in its QoS database, then determine which VRF table is assigned to the QoS request. Once an association between the requested QoS and a VRF table has been established the router will then direct all traffic from the requesting source through the associated VRF table MPLS path. If no associated VFR table is found, then a new RSVP path can be requested. Figure 16 demonstrates the relationship between traffic flows and VRF tables. To provide the communities-of-interest protection, each PE router configures the L3VPN over a Virtual Private LAN Service (VPLS) L2oVPN using IETF L2VPN VPLS LDP.

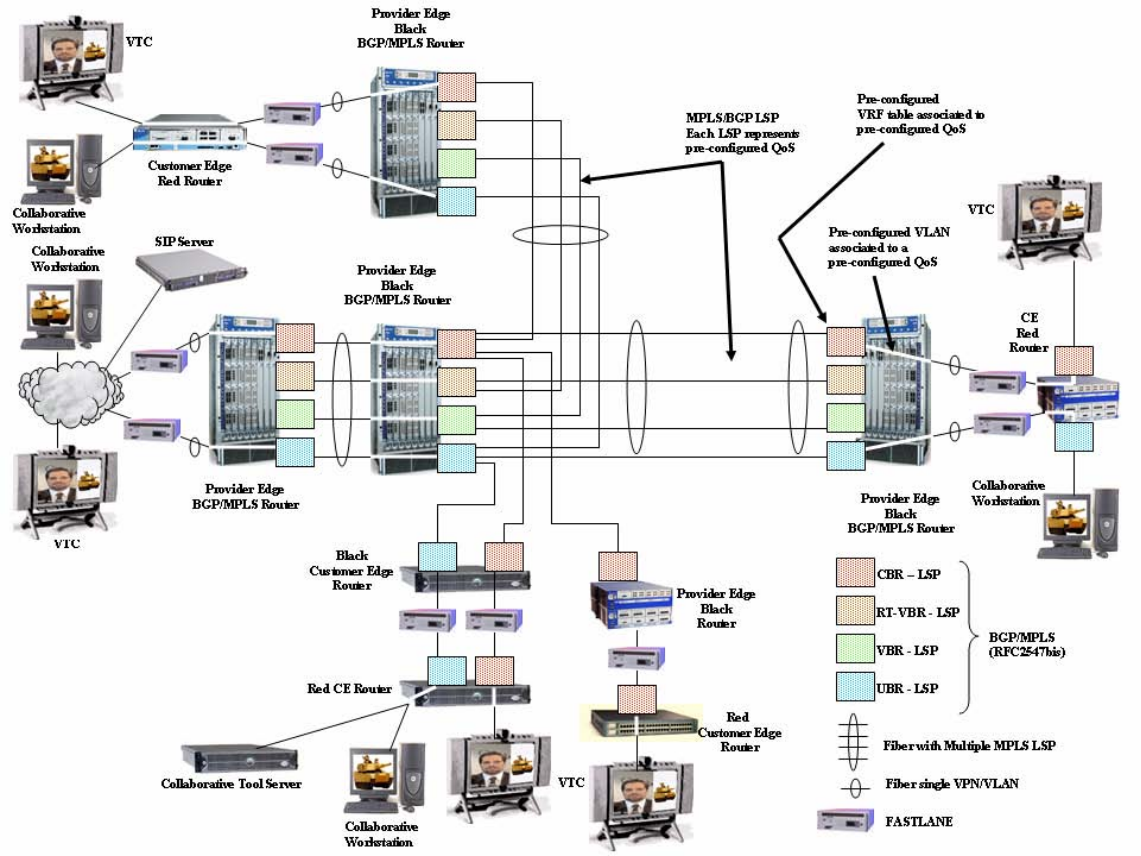


Figure 16. L3VPN VFR Table QoS LSPs

12. Deployed meshed paths.

The IPv4/IPv6 Interim Transitional Hybrid Network can be successfully deployed by building an RFC-2684 edge mesh over an MPLS LSP mapped over an IP POS core mesh. This configuration is similar to the configuration in today's DoD/IC ATM PVC meshed networks. This is accomplished by configuring MPLS routers using BPG-MPLS Layer 3 VPNs within each site Provider Edge Router (PE). In so doing each site PE router is interconnected to each other site PE router through a MPLS Label-Switched-Path (LSP). Then each IP-Over-PVC is associated to a Virtual Routing and Forwarding (VRF) table LSP. Each PVC is bridged to the PE MPLS LSP tunnel using IETF L2oVPN services. Figures 1 and 17 illustrate this configuration.

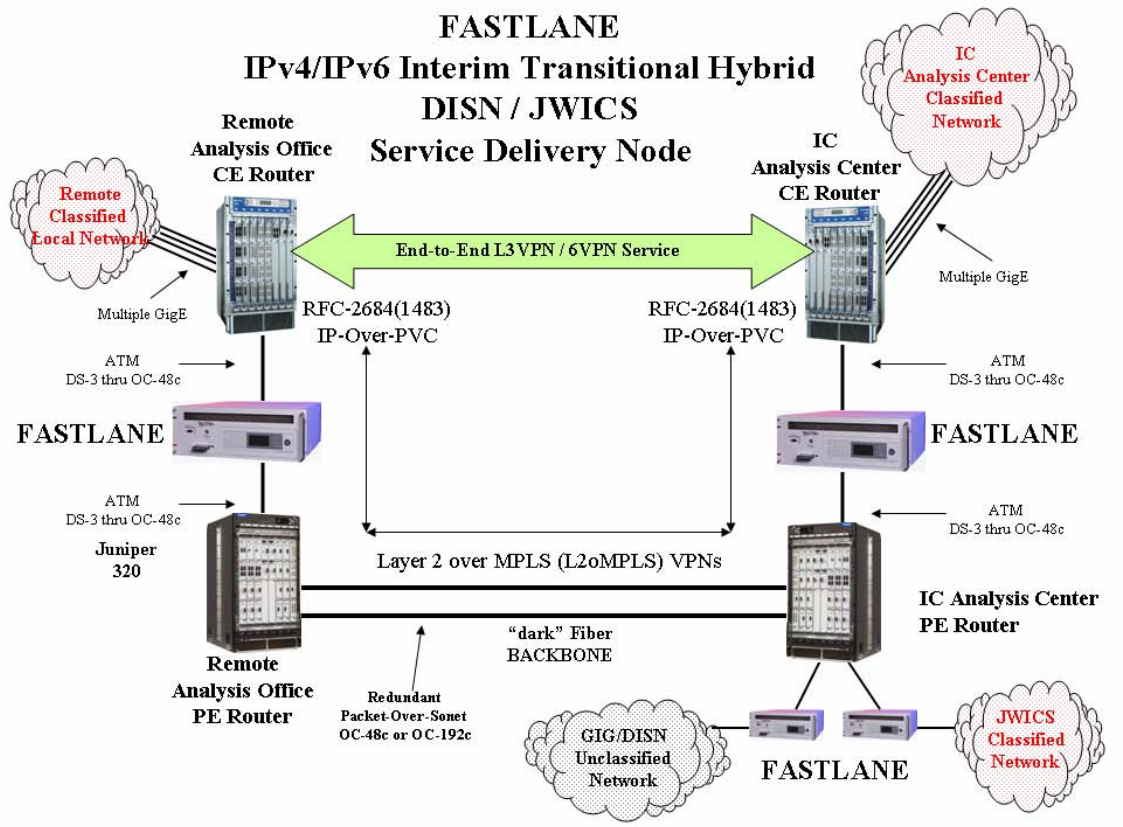


Figure 17: IPITHN Configuration.

13. Conclusion: Policy and security benefits to the IPITHN design.

As proposed, the IPv4/6 Interim Transitional Hybrid Network established for the DoD/IC will provide an architecture that fully maintains each DoD/IC member's autonomy and each member's security. The IPv4/v6 Interim Transitional Hybrid Network will readily support topology aggregation, which has the benefit of hiding the topology internals of peering networks in the interest of security. A global network architecture using secure local ATM PVC connections through FASTLANE encryptors which are switched over to wide-area MPLS LSPs can bring autonomous groups together securely while still supporting individual control. Further, by using an MPLS LSP meshed IP network core, network outages can be dramatically reduced. With an LSP meshed network, any underlying network technology can be deployed without affecting existing security policy and, in fact, will enhance security in the network.

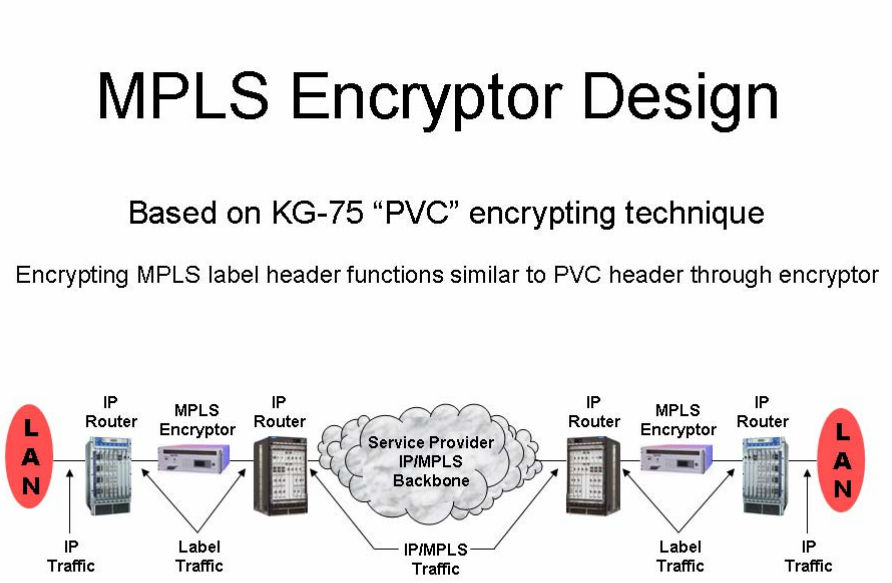
A network based on this IPv4/6 Interim Transitional Hybrid Network configuration will greatly improve internetworking within the DoD/IC. It will simplify routing data between agency networks while maintaining both intra-agency autonomy and security. This hybrid network architecture will not interfere with an agency's internal architecture for its intranets; rather, it defines an architecture which promotes seamless, secure and stability for inter-agency interconnectivity. The architecture is flexible enough to incorporate existing intra-agency addressing because the agency Point-Of-presence (POP) to DoD/IC network backbone summarizes the address of downstream networks before broadcasting them to other DoD/IC

POPs. It also adds additional security by not advertising local routes to the core networks, a key feature of L3VPN service. L3VPNs shortens the routing data, which increases network throughput, as well as promotes a more secure environment by limiting the exposure of an agency's full internal addresses.

This is an IP-centric architecture that minimizes the dependence on any one type of network encryptor. The first iteration incorporates existing, accredited high-performance ATM encryptors. As newer encryption technologies, such as the HAIPE, become mature and attain critical throughput speeds, they can replace the ATM encryptor without changing the architecture. In fact, if a new type of encryptor, such as an MPLS encryptor, were to be developed, it can also replace the ATM encryptor without requiring an architectural change.

14. Future: Proposed MPLS Encryptor design.

We can envision an MPLS Encryptor replacing the FASTLANE encryptor as illustrated below and will be the subject of a follow on work closely associated to the design presented within this paper.

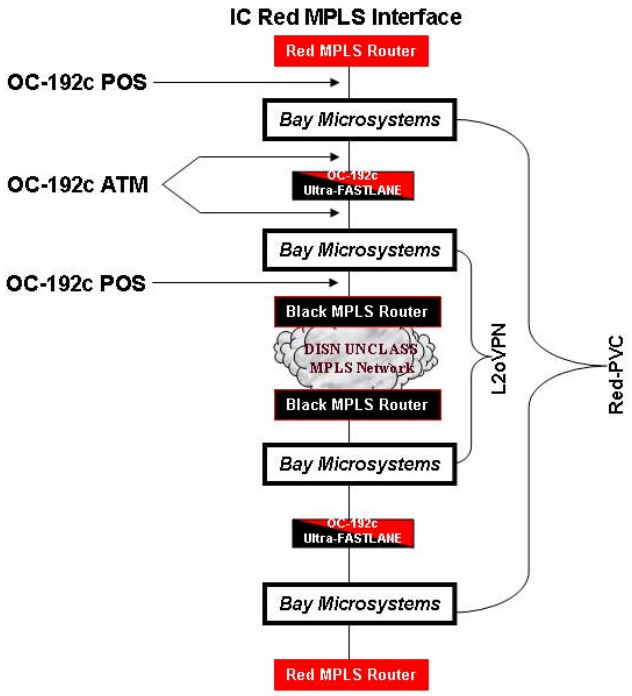


15. Future: Enhanced IPITHN design.

An enhancement to the IPITHN design will be achieved by inserting into the architecture a device under development (at the time of this writing) by Bay Microsystems which is equipped with both OC-192c POS and OC-192c ATM interfaces. The following figure illustrated how this enhancement to the IPITHN would be deployed in a typical DoD network such as the DISN.

DoD / IC Architecture

Supporting ATM, IPv4 and IPv6 at OC-192c



References.

[1] JWICS, IC CIO: Intelligence Community ATM Interface (IC AI) Logical Group Node Hierarchy.
[2] DoD, SPAWAR System Center San Diego: Interoperability Specification for High Assurance Internet Protocol Encryptor (HAIPE) Devices.
[3] DISA/GBE23 (network Engineering): CoS/QoS DESIGN PLAN for DISN IP NETWORKS (FY'05 Update)
[4] DISA/GBE23 (Network Engineering Branch): GIG-BE IP Router Addressing Plan (U) Version 1.2, 21 Mar 2005.
[5] DISA/Global Information Grid: BGP Layer 3 VPN Network Management (Final Draft) Version 1.0.
[6] Juniper, Semeria, Chuck: RFC 2547bis: BGP/MPLS VPN Fundamentals.
[7] Juniper, Semeria, Chuck: RFC 2547bis: BGP/MPLS VPN Hierarchical and Recursive Applications.
[8] Juniper JUNOS 7.0: Configuring Ipv6 Tunnels Over MPLS.
[9] Juniper JUNOS 7.0: VPN Routing and Forwarding Tables.
[10] Juniper JUNOS 7.0: VPN-Ipv4 Addresses and Route Distinguishers.
[11] Juniper JUNOS 7.0: Ipv6 Layer 3 VPNs.
[12] Juniper JUNOS 7.0: Routing Instances for VPNs.
[13] Juniper JUNOS 7.0: Forwarding Across the Provider's Core Network.
[14] Juniper JUNOS 7.0: Distribution of Routes from PE to CE Routers.
[15] Juniper JUNOS 7.0: Using RSVP for VPN Signaling.
[16] Juniper JUNOS 7.0: Layer 3 VPN Configuration Examples.
[17] HP, Technical Documentation: Encapsulating Security Payload (ESP).
[18] IETF: Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering, RFC-3564.
[20] IETF: Requirements for Inter-Area MPLS Traffic Engineering, RFC-4105
[21] IETF: Multi-Protocol Label Switching (MPLS) Support of Differentiated Services, RFC-3270.
[22] IETF: Virtual Private LAN Services over MPLS, draft-ietf-l2vpn-vpls-ldp-08.txt.
[23] IETF: Use of PE-to-PE IPSec i n RFC2547 VPNs, dratf-ietf-l3vpn-ipsec-2547-01.txt.
[24] IETF: Security Architecture for the Internet Protocol, RFC-2401.
[25] IETF: Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE), RFC-4023.
[26] CISCO: Multiprotocol Label Switching Virtual Private Networks, Q&A MPLS MPLS Basics, 2003.
[27] ATRICA: Delivering Hard QoS In Carrier Ethernet Networks, 2005.
[28] River Stone Networking: An Overview of Virtual Private LAN Service A new approach to LAN to LAN Communication, vpls_overview.pdf.
[29] Werner Almesberger: Linux Traffic Control – Next Generation, 18 Oct 2002
[30] TMOK: mistvan, MPLS for Linux How-To, 2001.
[31] Italy (Telecom Italia Lab S.p.A.) and UK (CCSR, University of Surrey): Internetworking between Multi-Layer IPSEC and secure multicast services over GEO satellites, 20 June 2002.
[32] NSA: http://www.nsa.gov/ia/industry/gigscope.cfm