MODEL ARCHITECTURE FOR IPV4 TO IPV6 MIGRATION

Jesus Piña-Saldaña
Telecommunications and Networking Department.
ITESM, Campus Monterrey
Av. E. Garza Sada 2501, 64849,
Monterrey, Nuevo León, México
Jesus.pina@itesm.mx

Raul Ramirez-Velarde
Computer Science Department
ITESM, Campus Monterrey
Av. E. Garza Sada 2501, 64849,
Monterrey, Nuevo León, México
rramirez@itesm.mx

Raul Perez-Cazares
Computer Science Department
ITESM, Campus Monterrey
Av. E. Garza Sada 2501, 64849,
Monterrey, Nuevo León, México
raul.perez@itesm.mx

Abstract
This paper discusses migrating from IPv4 to IPv6 by creating an architectonic transition model and protocol configuration. We believe that IPv6 is the next logical step in the future of the Internet. We show a recommendation for transition that consists of two phases and also show all the necessary equipment configuration to ease the transition.

Keywords
Security, Networking, IPv6, Interoperability, Real-time, Enterprise Architecture.

1. INTRODUCTION

A large number of organizations have found that network architectures are valuable tools in today's competitive, fast-envolvig world. However, their implementation requires several considerations:

Architectural requirements: determine how to integrate business strategy, business objectives and business context, including market and technology trends, to match competitor moves.

Architecture specification: determine how to use architectural patterns, how to create architecture principles, how to model the architecture and document the system using different views, what views are appropriate to what kinds of architectures, what level of detail/specificity should the architecture go into, given its scope, how to manage architecture risk, how to make architecture tradeoffs.

Evaluation: how to assess the system in terms of system requirements.

We propose an architecture that will enable an easy migration from IPv4 to IPv6 which offers many desirable characteristics like: hierarchic architecture of addresses, self-configuration of devices, mobile computing, security and integrity of data, quality of service, support for multimedia traffic, and multicast and unicast real-time applications, etc.

One reason for choosing IPv6 as transport protocol, is that in a few years, the corporate migration from IPv4 to IPv6 is expected to be completed. Hence, compatibility issues will arise sooner or later. Therefore there is a great incentive for having techniques and tools to help enterprises achieve a more easy and transparent migration without affecting business strategy and objectives.

We will instantiate the proposed architecture by referring to ITESM's (Instituto Tecnologico y de Estudios Superiores de Monterrey) own path for migration from IPv4 to IPv6. The architecture proposed consists of a two phase migration. The first phase consists of IPv6 tunneling between ITESM's Internet routers connected to the IPv6 backbone. In this phase, a tool will be created to provide automatically a tunnel 6to4 (that is, tunnel IPv6 traffic through an IPv4 network). The tool will send a script that can be executed in the computer host (operating system specific); this being completely transparent to the user. In the second phase pure islands of IPv6 will be created, migrating little by little all subnetworks without the need to buy new equipment. Although the model is designed to have all services migrated to IPv6, we assume that there will be support for IPv4 in case that some devices have not upgraded to IPv6.

This paper has the following structure: First, IPv6 concepts are discussed followed by the proposed architecture model. Secondly, we discuss the impact of each phase followed by the configuration procedure. Finally, we close discussing the advantages and disadvantages of the proposed scheme and other tasks that have been carried out that benefit the migration process.

2. IPv6 CONCEPTS

Without doubt, IP is a basic layer of the networking stack and IP address are a fundamental identifier for any entity on the Internet. The main problem that is being addressed by moving to IPv6 is the lack of IPv4 addresses that result from the current addressing scheme. IPv6 offers 128 bit addresses which are foreseen to be large enough for future purposes. Whereas upgrading the address bit-length is one of the main benefits, various other features are being built into the new IP protocol to easily enable features like security, QoS, mobility and others [1].

A change in the IP address structure impacts the whole networking stack. First, the IP layer needs to be completely replaced and the new IP layer has to be tuned to run over the various L2 (link layer) mechanisms that are prevalent today. Then, transport protocols have to be built which will take advantage of the new IP layer such as TCP, UDP and other new transport mechanisms like SCTP. Most of today's applications are built on top of a socket layer and

hence they have to be updated to use the new socket mechanisms.

Since this task is fairly complex, it is not possible to throw away the existing IPv4 network and adopt IPv6 immediately. It is foreseen that the transition will happen in stages with a few IPv6 nodes introduced into an IPv4 network and the number gradually increasing over time till some time in the distant future when the entire network becomes IPv6.

It is fairly evident that it would be impossible for the entire Internet to work only on IPv6 since the existing backbone IPv4 networks would pose great difficulty towards complete adoption of IPv6. Therefore, there is a requirement for co-existence of the two networking technologies and Internetworking requirements have emerged.

2.1. NETWORK MANAGEMENT

SNMP is the de-facto management protocol used in the current Internet. As new standards are being defined for the IPv6 protocol and all other related technologies, the corresponding SNMP-MIB (Simple Network Management Protocol-Management Information Base) definitions for these are also being made [10]. However, vendor adoption of these MIBs has been slow but recently vendors have started implementing some of the MIBs. The standard transport mechanism for SNMP is over UDP which could run either over IPv4 or IPv6 with appropriate changes to the socket layer. Standard SNMP management platforms like HP-OV are also indicating roadmaps with support for IPv6.

Unless sufficient management tools are available, the commercial deployment of IPv6 would be doubtful since ISPs (Internet Service Providers) and enterprise network managers require the tools to configure and monitor IPv6 networks. The tools become very important especially in a mixed network scenario where the network manager will have to keep track of tunnels, routing issues, DNS configurations and other important data across both IPv4 and IPv6 networks.

2.2. HEADERS

One of the deficiencies of IPv4 identified by the committees that developed IPv6 was the complexity of its headers. If these were allowed to grow by the same factor as the address space was to be enlarged, then things would start to get rather unwieldy. The IPv4 header has a total of 10 fields, including the two 32-bit address fields (one for the source, one for the destination), and an options field which is padded to bring the whole header up to the correct length. Even with nothing in the options field, an IPv4 header is 20 bytes long, so clearly an 80 byte header for IPv6 was not a desirable thing. So the IPv6 header is simplified by allowing headers to be chained together [12].

On the contrary, in IPv6 there are now only six fields including the two 128 byte addresses for source and destination, and no options. Variations in the header that would have been contained within the IPv4 header, or its options field, are now identified using a new field which specifies that another header is included after the current one but before the data itself. The first header defines the minimum data needed for an IPv6 packet, including the version, priority, flow label, pay-load length and hop limit, and includes a field to say “and there’s another header after this one” (see Fig. 1). There is no limit to the number of headers that can be chained together in this way. As the next header field is an 8-bit number, there can be 255 different types of header. Only six different types are defined at present [12].

- Hop-by-hop options
- Routing header
- Fragment header
- Authentication header
- Encapsulating security
- Payload header
- Destination options header

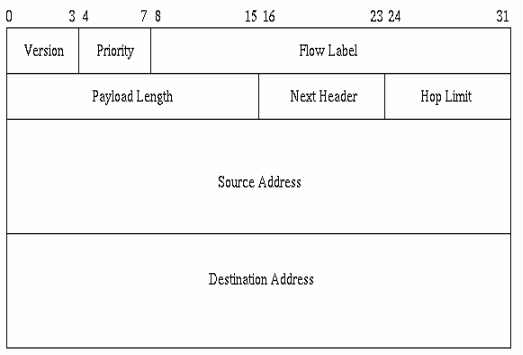

Figure 1 . IPv6 Header Format

The result of this simplification, and improved flexibility, is that the simplest IPv6 header is still only 40 bytes long (or double the size of the IPv4 header without options) despite the fact that the two addresses it incorporates are four times the size of the IPv4 header. Of course, if you decide to have all the trimmings, the header could get quite large, although this is not possible at present as only six header types have been defined. The new solution is much more elegant, in that straightforward tasks need only produce simple and lightweight headers, while allowing more complicated applications or systems to add whatever intricacy they need. The reduced complexity of the default IPv6 header clearly makes the task of the average router much easier than it otherwise might be.

2.3REPRESENTATION OF ADDRESSES

There are three conventional forms for representing IPv6 addresses as text strings [13]:

1. The preferred form is x:x:x:x:x:x:x:x, where the 'x's are the hexadecimal values of the eight 16-bit pieces of the address. Examples:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
1080:0:0:0:8:800:200C:417A

Note that it is not necessary to write the leading zeros in an individual field, but there must be at least one numeral in every field (except for the case described in 2.).

2. Due to the method of allocating certain styles of IPv6 addresses, it will be common for addresses to contain long strings of zero bits. In order to make writing addresses containing zero bits easier a special syntax is available to compress the zeros. The use of "::" indicates multiple groups of 16-bits of zeros. The "::" can only appear once in an address. The "::" can also be used to compress the leading and/or trailing zeros in an address.

For example the following addresses:

1080:0:0:0:8:800:200C:417A a unicast address
FF01:0:0:0:0:0:0:43 a multicast address
0:0:0:0:0:0:0:1 the loopback address
0:0:0:0:0:0:0:0 the unspecified addresses

may be represented as:

1080::8:800:200C:417A a unicast address
FF01::43 a multicast address
::1 the loopback address
:: the unspecified addresses

3. An alternative form that is sometimes more convenient when dealing with a mixed environment of IPv4 and IPv6 nodes is x:x:x:x:x:x:d.d.d.d, where the 'x's are the hexadecimal values of the six high-order 16-bit pieces of the address, and the 'd's are the decimal values of the four low-order 8-bit pieces of the address (standard IPv4 representation).

Examples:

0:0:0:0:0:0:13.1.68.3
0:0:0:0:0:FFFF:129.144.52.38

or in compressed form:

::13.1.68.3
::FFFF:129.144.52.38

2.4. IP FLOWS

IP flows are part of the IPV6 standard [13]. Their aim is to support real-time multimedia traffic in the wired network. The *flow_label* field in the header can be assigned to particular streams of traffic with special quality-of-service requirements (see Fig. 2). The flow label is used by the routers in a way that it resembles the setup path in ATM (Asynchronous Transfer Mode). The flow label can serve as a key in the router cache to reduce the amount of processing. When a datagram comes to a router for the first time it can save the flow label in the cache. The next time a datagram arrives from the same flow (with the same flow label) the router can recognize the flow label in its cache table and find the next hop without having to look in the routing table (which usually is very large). Applying flow labels to real-time connections the processing time in the router can be reduced considerably.

A flow specification is a data structure used by internetworking hosts to request special services. The flow specification can be used as part of the negotiation to describe the type of service that the hosts need from the network. The specification indicates requirements for a single direction. Multidirectional flows are required to request services in both directions using two flow specifications [2].

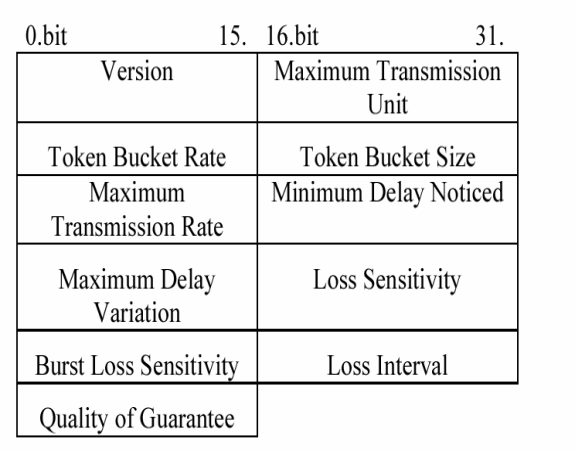

Figure 2 . Format of the flow specification

2.5. SETTING UP A FLOW

There are two possible ways to setup a flow. First, the internetwork can find a route to the receiver. In this case the key problem is to determine if one or more routes from the source to the destination(s) exist, which might be able to support the quality of service requested. Some basic information about the flow needs to be provided to the routing system. This information is:

- How much bandwidth the flow may require
- How delay sensitive the application is
- How much error can be tolerated
- How firm the guarantees need to be
- How much delay variation is tolerated

The flow specification provides all of this information. So it seems plausible to assume it provides enough information to make routing decisions at set-up time.

Second, some researchers have suggested that the negotiation to setup a flow might be an extended negotiation. In this process the requesting host initially requests the best possible flow it could desire and then negotiates with the network until an agreement on a flow is reached with properties that

the network can actually provide and the application still finds useful.

3. NETWORK ARCHITECTURE

The term "network architecture" is commonly used to describe a set of abstract principles for the technical design of protocols and mechanisms for computer communication. Network architecture represents a set of deliberate choices out of many design alternatives, where these choices are informed by an understanding of the requirements [18, 19].

Network architecture is a set of high-level design principles that guide the technical design of a network, especially the engineering of its protocols and algorithms. To flesh out this simple definition, we have examples of the constituents of an architecture and how they are applied. A network architecture must typically specify

- Where and how connection state is maintained and how it is removed
- What entities are named
- How naming, addressing, and routing functions related and how they are performed
- How communication functions are shaped into layers to form a protocol stack
- How network resources are divided between flows and how end-systems react to this division, i.e., fairness and congestion control
- Where security boundaries are drawn and how they are enforced
- How management boundaries are drawn and selectively pierced
- How differing QoS is requested and achieved.

Based on these considerations the proposed architecture will have the following points (see Fig. 3)

- **Network**: The network will work under Ethernet with a star topology which will be divided in two networks: Real-Time-IPv6 (RTV6) and Real-Time-V4 (RTV4). They will coexist by IPv4 tunnels.

- **Clients**: Clients in this model will be Laptops with Linux operating system that will be connected to the RTV6 network by a 1000 Mb switch (half duplex). These clients will have IPv6 addresses and clearance to access server information.

- **Tunneling**: Basically it will be an IPv4 tunnel which will connect our RTV6 router to the Campus' IPV6 router.

- **Application Software**: Software will consist of an application that will be monitoring in real-time device activity via the SNMP protocol.

- **Security**: In this model a firewall will be used in the RTV6 router to control network access, also the IPSEC protocol could be used, for which IPv6 has special headers [9].

- **QoS**: One IPv6 advantage is that broadcast doesn't exist (rather multicasting is used). This avoids unnecessary traffic. Another advantage is that the use of label flow will considerably increase QoS [8].

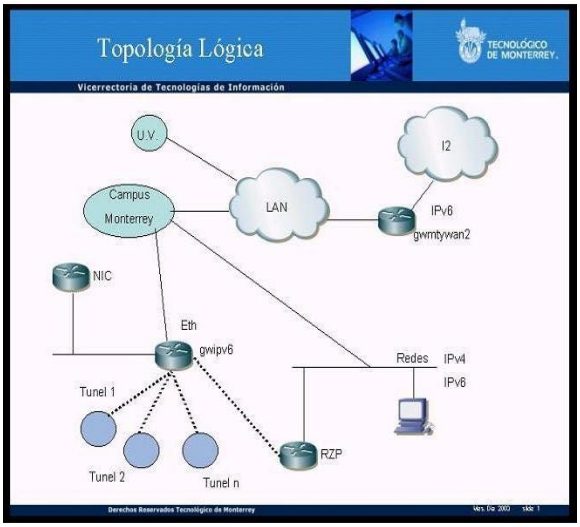

Figure 3. Network Architecture

4. MIGRATION FROM IPV4 TO IPV6

Migration must be seen as an evolutionary process. It will start with the implementation of a new protocol in the communications infrastructure. Then, it will continue with applications, services and management systems modifications, ending with most of the extended-protocol networked devices.

Until full IPv6 migration is achieved, systems would experience little impact. This allows network-layer migration to proceed steered by enterprise requirements. Only in the last phase, the possibility to vanish IPv4 from the current network is finally contemplated. Nevertheless, as this could never take place, both technologies can coexist without any problem. Fig. 4 shows transition architecture:

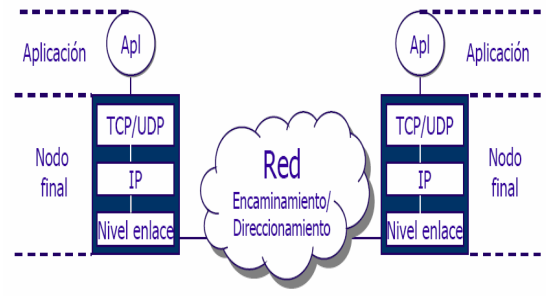

Figure 4.Transition Architecture (taken from [17])

4.1. PREREQUISITES

The requirements that we need to contemplate in the migration process include at least the following points

1. Access to the new network even if the old network access infrastructure must be used. It means, creating a standard for new network protocol access.
2. Access to basic services on the network necessary to use the new protocol.
3. Access to IPv6 information services which are necessary to use the data processing resources of the organization.
4. Documentation and technical support to help users migrate to new levels and documentation of performance advantages.
5. Service support for migration problems that could arise.
6. An address Space Management Service assigned to the new protocol.
7. A Security Management Service in the corporative network (filter, audit, access control, backup, etc).

4.2. NEW NETWORK ARCHITECTURE

To introduce the new network protocol, it is necessary to modify the structure and the architecture of the communications infrastructure. This should be done in the data-link and network levels without affecting other levels.

One of the most desirable solutions for a corporate network migrating from IPv4 to IPv6 is to have the possibility of accessing segments of the IPv6 network from any access point. It is important to realize that many systems and computers working on IPv4 will have to acquire an IPv6 address, therefore the easier the access to the network is, the smaller will the investment be.

For that, if the local access network is based on Ethernet technology, there are two technical solutions:

- Both the IPv4 and IPv6 networks are on the same segment (double stack): That means that the physical level (therefore the same broadcast domain and the same VLAN) and all network devices are to be shared, independently the version of IP to be used.

- IPv4 and IPv6 applications use different network segments (parallel networks): That is to say, a division of the broadcast domains (also called network segments) by means of label techniques VLAN.

4.3. NETWORK WITH DOUBLE-STACKED PROTOCOLS

This is the easiest technique to implement. It doesn't require duplicating the network or network interfaces so the systems can access IPv4 or IPv6. It is only necessary that the computer and routers operating systems be able to use both parallel protocol stacks to distinguish the packages by means of the network-level header, that is, by the version field.

The biggest disadvantage of this method is that both networks could get in each other's way, mainly in cases when network resources have been consumed before introducing IPv6, or when the implicated routers do not have the appropriate capacity to direct the packages for both network levels. This problem, which is rather rare in corporate networks, has to be solved through third party service providers as in the cases a strict quality service level is demanded. A network example is shown in Figs. 5 and 6.

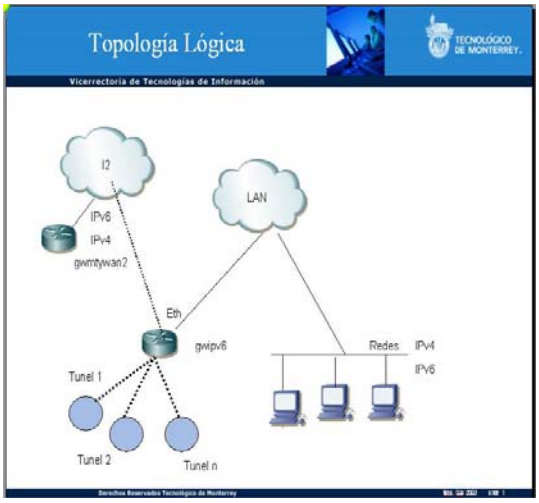

Figure 5. Network with double-stack protocols.

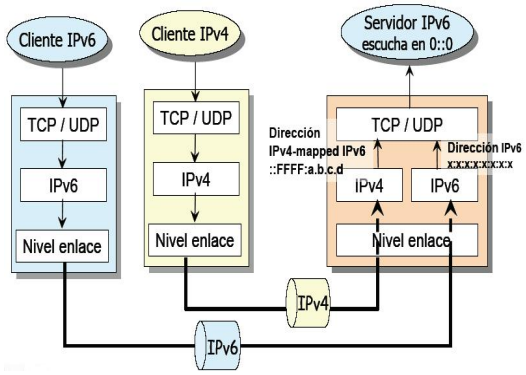

Figure 6 Application Server dual node. [12]

4.4. IPv6 PARALLEL NETWORK

In this technique we separate the physical network segments for the packages of IPv6 from those that circulate on IPv4. This implies that also the routers have to be different.

This solution is the best one for networks with high QoS and stability demands, because it avoids the

possible interferences between both protocols. Today, thanks to Ethernet Networks Segmentation using VLAN techniques, a IPv6 parallel network, would not be so expensive. However, it is likely that there will be high configuration costs, mainly if taking the two networks to the final user station is considered. Fig. 7 shows an example of this network.

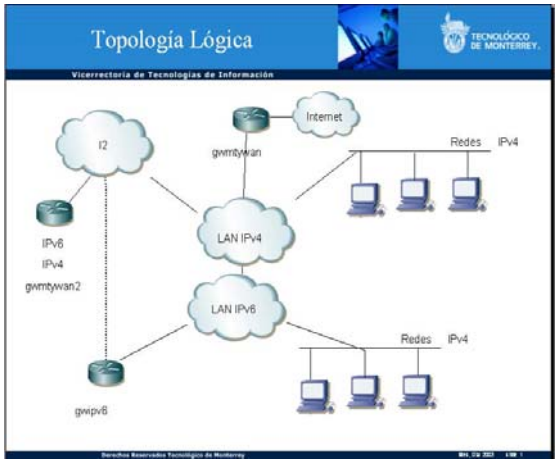

Figure 7. IPv4 and IPv6 parallel networks.

4.5. CONSIDERATIONS FOR THE NEW NETWORK ARCHITECTURE

From the user-side point of view, the double stack technique is the simplest solution to use in corporative scenarios where is impossible to know in advance who could be an IPv6 potential users, as users could be spread all over the organization. But then again, the dual network scenario is the most comfortable and simple to manage, because it allows reducing the maximum networking management workload and only needs a minimum hardware investment.

4.6 MIGRATION MECHANISMS PROBLEMS

We have introduced IPv4 to IPv6 migration mechanisms. However every mechanism has its application scenarios and limitations.

4.6.1. FIST PHASE

It is very important to study the characteristics of each environment to choose the transition mechanisms. We will now study a case in which double protocol stack is used [16].

In its first stage, the most suitable solutions for this transition were the IP tunnels used by the application mentioned [16], which has the following advantages and disadvantages.

Advantages

- Method commonly used 6-bone access.
- Available in a multitude of platforms (Cisco, Telebit, Linux, Lots, Windows NT, etc).
- It is a totally transparent method with respect to IPv6 level and superior levels. It does not affect enterprise applications.
- Does not consume excessive resources. For example MTU (Maximum Transmit Unit) is reduced in 20 bytes (Cab. typical IPv4).
- Main Application: Connection with IPv6 ISP (Internet Service Provider) through the Internet.

Disadvantages

- Procedures are not automatic, but rather manual or semiautomatic.
- If N islands are united and the topology does not consider central node or central interchange, the number of tunnels to establish in this kind of network can go up to N-1. At present there are thousands of IPv6 islands distributed throughout the present Internet, thus this method is very hard to scale.

4.6.2. SECOND PHASE

The second phase, which consists of extending the migration process to other network layers and to applications must follow the following steps at ITESM (At the time of the writing of this paper, this phase is still a work in progress at ITESM)

- Finish migrating the new network provided by LANIC.
- Change to parallel Networks for IPv6 and IPv4 as mentioned in section 3.
- To evolve the entire network to Stateful Configuration (DHCP6).
- To document and establish multi-homing devices so that other campuses can use the Internet 2 network.
- Acquire new and more powerful routers to increase network throughput as by the time this phase is over, networking devices will be obsolete.

4.7 BARRIERS FOR IPv6 AT ITESM

- The problem of multi-homing network devices.
- Patches to IPv4 like NAT that discourage the migration process.
- The lack of real support from manufacturers of routers and software.
- The complexity of migration/transition.
- The users need commercial reasons to be forced to move to IPv6.

4.8. ENUMERATION PLAN

A typical network of an organization has a wide range of IPv4 addresses. In many cases, it has one portion of private addresses (IP addresses that can't be routed to the Internet) and another portion of public addresses (IP addresses that can be routed to the Internet).

The enumeration plan is in charge of address designation for each network in order to give them

connectivity in IPv6. The enumeration plan also affects the routers that have to announce the adequate prefixes to each network, depending on the specified configuration and also the configuration of the routes to take the packages through the intranet.

4.9. CONNECTIVITY MANAGEMENT

Depending basically on the size of the internal network, it is important to make a decision about the route updating procedure. Usually there are two options,

1. Use Interior Gateway Protocols (IGPs). These are normally used when the devices have the network topology and use it to guide the traffic through the most efficient route. The protocol that is traditionally used at ITESM is EIGRP, so this is the one that we will use.

2. Use semiautomatic-configuration static routes. Those are useful when network topology doesn't vary frequently. They are automatically activated once they are configured. This solution is adequate for small networks or ones with great stability as for example, when there are no redundant communication links.

In the case we are using for as demonstration, the solution that we considered the most adequate, is to manage static routes, for tunnels and pure IPv6 routing protocols.

Furthermore for double-stack network devices there are two solutions to be considered. The first and simplest consists of making IPv4 routers go through the new IPv6-capable routers. The second solution is somewhat more complicated, but it is a better solution when enterprise routers cannot support some IPv6 companion protocols. It consists of making the new routers be different from the computers in the network. In our case, the solution that we suggest to adopt for the migration is a mixed solution. There will be two firewall/routers (see Fig. 8).

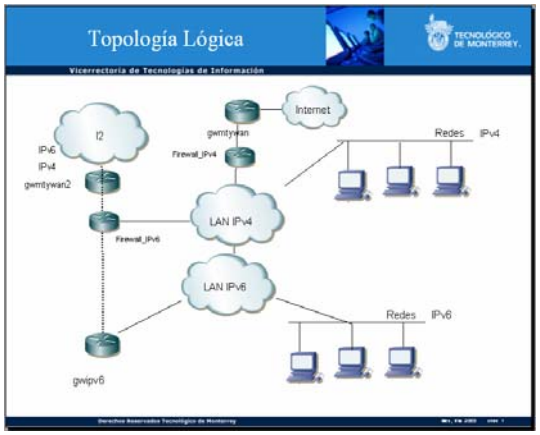

Figure 8. Integrated Network Security

4.10. IMPORTANT CONSIDERATIONS

If we want to have two network protocols sharing a common infrastructure, we should consider many aspects that characterize and differentiae them mainly

1. **Cero Configuration.** While the IPv6 problem is solved in this simple way, auto-configuration (without a network-configuration device) at start time continues to be unresolved. Automatic configuration with a host state (also called zero-configuration process) might be solved by using a modified IPv6 DHCP protocol which is still in development [3].
2. **Broadcast.** IPv4 protocol has and uses broadcast capabilities (such as ARP protocol) to get physical addresses for every host in the network, to construct datagram heathers. The broadcast definition itself implies that all packages of that kind arrive to all devices connected to a one broadcast domain. In IPv6 broadcast is not necessary. Furthermore, its effect is to compromise bandwidth available to all segments of the network shared by IPv4 clients as well as IPv6 clients. But if it is needed, IPv6 multicast is a better solution since its effect on bandwidth is negligible [16].
3. **Security.** While security protocols and mechanisms (IPsec) for IPv4 are optional, in IPv6 all the devices that want to belong to the network should be capable of manage them. Also, it is necessary to have in mind IPv6 nodes use Neighbor Discovery (ND) for many network functions which is susceptible to attacks if it is not used with the security mechanisms offered by the IPsec Authentication Header (AH). Like the automatic methods password management (e.g. Internet Key Exchange, IKE) that is now in development, network membership requires manual password authentication management, which could introduce a large load of administrative work if the number of devices to configure is big. That is why solutions based on IPsec (Secure Neighbor Discovery, SEND [32]) and in cryptographically generated addresses (CGA [33]) are being developed that allow package source identification to know if it was modified in route [34].
4. **Performance.** Commercial switching devices depend on network level. IPv6 capable switches are just now being available. This could be a problem when trying to deploy services in a production environment with IPv6.

4.11. COST

To make a smooth migration, it is necessary to have at least the following basic costs considerations

- Training of non technical personnel (users) for changes in network devices and procedures.
- Training of technical personnel for IPv6 management.
- Necessary software update, including S.O (Operating System).

- Devices configuration at S.O. level to use IPv6 addresses.
- Software configuration of devices that are going to manage VLANs.
- S.O. configuration to manage coexistence between IPv4 and IPv6 in cases where hosts have both address spaces.
- Configuration of network applications to support both types of addressing.

5. TUNNELING IPv6

We have already discussed that some IPv6 characteristics are explicitly designed to simplify migration. For example IPv6 addresses can be automatically derived from IPv4 addresses, IPv6 tunnels can be built on IPv4 networks at least in the initial phase, etc.

IPv6 tunneling is a technique for establishing a "virtual link" between two IPv6 nodes for transmitting data packets as payloads of IPv6 packets. From the point of view of the two nodes, this "virtual link", called an IPv6 tunnel, appears as a point-to-point link on which IPv6 acts like a link-layer protocol. The two IPv6 nodes play specific roles. One node encapsulates original packets received from other nodes or from itself and forwards the resulting tunnel packets through the tunnel. The other node decapsulates the received tunnel packets and forwards the resulting original packets towards their destinations, possibly itself. The encapsulator node is called the tunnel entry-point node, and it is the source of the tunnel packets. The decapsulator node is called the tunnel exit-point, and it is the destination of the tunnel packets.

There are four types of tunneling techniques can be used in the following ways [5]

Router-to-Router: IPv6/IPv4 routers interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves.

Host-to-Router: IPv6/IPv4 hosts can tunnel IPv6 packets to an intermediary IPv6/IPv4 router that can be reached via an IPv4 infrastructure.

Host-to-Host: IPv6/IPv4 host interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves.

Routers-to-Host: IPv6/IPv4 routers can use tunnels to reach an IPv6 host via an IPv4 infrastructure.

In our demonstration case we used Router-to-Router model which shown in the next figure (Fig. 9)

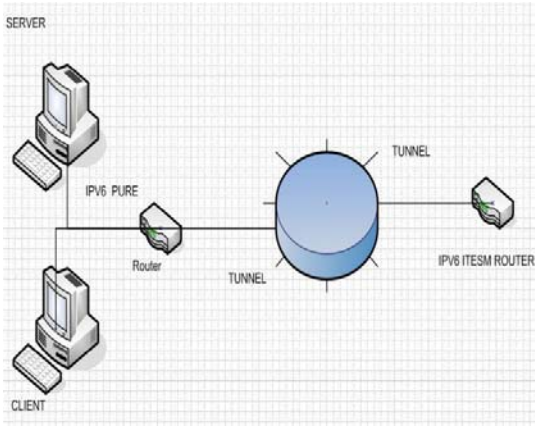

Figure 9. Model Router-to-Router

6 NETWORK ELEMENTS CONFIGURATION

At ITESM, there is a single border router with an uplink to the 6bone and the global IPv6 network. The same router is internally connected via a trunked Gigabit Ethernet interface to a Catalyst 6500 and the Layer 2 infrastructure. The Cisco router now acts as an IPv6 router. It is a simple task to add a VLAN interface with the VLAN-ID of the already existing IPv4 VLANs. Via this interface our IPv6 router sends router advertisements to the VLAN clients and becomes the default router for IPv6 traffic. Standard IPv4 traffic still is routed over the default IPv4-only routers. Since VLANs are spread throughout the entire campus, it is possible to give IPv6 access to various areas.

Linux Host Configuration

The easiest way to set up a tunnel on a Linux host is using the “ip” command [15]. To set up an IPv6-in-IPv4 tunnel a “sit” interface is created as follows

ip tunnel add sit1 remote <IPv4 address of remote tunnel endpoint> \ local <local IPv4 address>

Note that “sit1” is the name of the sit interface. The label “local IPv4 address” is the address of the network interface to be used for the incoming IPv4 traffic which contains encapsulated IPv6 datagrams. After configuring the interface it has to be brought up

ip link set sit1 up

To setup interface sit1 with an IPv6 address other than the self-configured local address we can use the following command

ip add addr <IPv6 address>/<subnet-length> dev sit1

After these commands are issued the output from “ifconfig sit1” should look somewhat like follows

sit1 Link encap: IPv6-in-IPv4

inet6 addr: 3ffe:401:1::fff0:2/112 Scope:Global
inet6 addr: fe80::80b0:b807/128 Scope:Link
UP POINTOPOINTRUNNING NOARP MTU:1480 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors: 0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0

Creating tunnels and adding IPv6 addresses can also be achieved with the command "ifconfig", but this is an old-fashioned style and should not be used in newer Linux distributions.

Cisco Router Configuration

Manually configuring an IPv6-in-IPv4 tunnel on a Cisco IOS platform is not much different from setting up an IP-over-IP tunnel [14]. One creates the interface by simply changing to the configuration mode by typing

configure terminal

Now the interface can be created

(config)# interface Tunnel 0

Note that the tunnel number can be any number from 0 up to about 65000. To configure the interface with an IPv6 address we have two possibilities

(config-if)# IPv6 address <full IPv6-address>/<subnet-length>

or

(config-if)# IPv6 address <prefix>/<prefix-length> eui-64

The first possibility will result in the interface being configured with the exact address one has specified. Note that the subnet length can be set as 128. Using the second possibility we specify a prefix, which may be up to 64 bits long. The full interface IPv6 address be configured with the MAC address of the hardware in the interface identifier as specified in the EUI-64 standard [5]. The tunnel source can either be specified with the name of the IPv4 source or by directly stating the IPv4 address of the local tunnel endpoint

(config-if)# tunnel source 128.176.191.82

or

(config-if)# tunnel source FastEthernet0/0

The tunnel destination is simply set up by

(config-if)# tunnel destination <IPv4 address of remote tunnel endpoint>

Finally we have to set the tunnel mode to "IPv6ip" to specify the correct encapsulation and decapsulation.

(config-if)# tunnel mode IPv6ip

With the "IPv6 route" command we can configure routes for tunnel interfaces just like with any other interface.

7. REMOTE NETWORK MONITORING

Before considering the design of a network-monitoring system, it is best to consider the type of information that is interesting to a network monitor. Then we can look the alternatives for configuring the network-monitoring function.

The information that should be available for network monitoring can be classified as follows

Static. This is information that characterizes the current configuration, such as the number and identification of ports on a router. This information will change only infrequently.

Dynamic. This information is related to network events, such as state change of a protocol machine or the transmission of a packet network.

Statistical. This is information that may be derived from dynamic information, such as the average number of packets transmitted per unit time by an end system.

7.1. REMOTE NETWORK MANAGEMENT REQUIREMENTS

As with any network design, it is best to begin with a definition of the users requirements. This is certainly true of an area as complex as network management. One way to do this is by considering the features that are most important to the user. These list the following as the principal driving forces for justifying an investment in network management

Controlling corporate strategic assets: Networks and distributed computing resources are increasingly vital resources for most organizations. Without effective control, these resources do not provide the throughput that corporate management requires.

Improving service: End users will expect the same improved service as organization information and computing resources grow.

Balancing out various needs: Information and computing resources in an organization must provide end users with various applications at given levels of support with specific requirements in the areas of performance, availability, and security. The network manager must assign and control resources to balance these various needs.

Controlling cost: Resource utilization must be monitored and controlled to enable essential end-user needs to be satisfied with a reasonable cost.

8. IPv6 TODAY

There are a number of standard setting efforts underway today to deal with issues such as: IPv6 architecture, applications, mobility, discovery, routing, security, transition, name service, management, and addressing. Some are complete but many are actively being discussed and worked upon. The IPv6 forum has well over 100 companies involved (www.IPv6forum.com).

Their mission is to promote IPv6, but not to force its deployment or its specifications. A number of active IPv6 testbeds are also underway [12]. The 6BONE is an IPv6 testbed that is designed to assist in the evolution and deployment of the IPv6 Internet. Basically it is a set of IPv6 "islands" with tunnels over the IPv4 Internet. More than 50 countries are involved (www.6bone.net). NTT has one of the largest experimental, commercial IPv6 networks deployed. This is a worldwide IPv6 backbone that is completely IPv6 end-to-end.

9. CONCLUSIONS

Migration to the new IP protocol in present networks is a work which is non-free of risks and costs. Some will be hidden until the moment of making the switch. Planning and discussion are the only tools that can help obtain smoothest migration possible. The risks are related to the possible loss of efficiency in the networks in which IPv6 transition periods is implanted. Costs will depend on the quantity of needed changes, the speed of change and economic and human effort that is dedicated to the task.

What's more, we have to be conscious that network and services migration will only be a part of the migration, and if we want to take advantage of the new protocol characteristics, we will have to make more efforts in extending the network with applications that support quality of service, management of security keys, mobility, etc.

Also it is important to emphasize that migration success will depend, in addition in a great extent to the availability of software adapted to the new technology, that not only allows to extract all the benefits this IPv4 based technology can provide, but that allows the enterprise to take advantage of all positive characteristics while at the same time avoiding in greater or smaller measurement, its possible disadvantages.

10. ACKNOWLEDGEMENTS

This work was funded under two grants from the Department of Telecommunications and Networking Department and Computer Science Department at ITESM, Campus Monterrey.

We would like to thank the other members of the Telecommunications department such as Arturo Servin, Montse Martinez, Elaine Islas and Patricia Medino for arguing and challenging every step of the way, and our reviewers for their insightful comments.

11. REFERENCES

[1] RFC 2460, "Internet Protocol, Version 6 (IPv6). Specification", www.ietf.org, 2000.

[2] S. Schenker, C. Partridge, R. Guerin. "Specification of Guaranteed Quality of Service". http://www.ietf.org/rfc/rfc2212.txt

[3] S. Thomson and T.ÜNarten. "RFC 2462: IPv6 stateless address autoconfiguration". December 1998. Obsoletes RFC1971. Status: DRAFT STANDARD.

[4] R. Callon, D. Haskin. "Routing Aspects of IPv6 Transition". RFC 2185, September 1997.

[5] R. Gilligan and E. Nordmark. "Transition Mechanisms for IPv6 Hosts and Routers". RFC 2893, August 2000.

[6] J. Hagino, K. Yamamoto. "An IPv6-to-IPv4 transport relay translator". RFC3142, June 2001.

[7] G. Cristallo. "Connecting IPv6 islands within a same IPv4 AS". Draft-many ngtrans-connect-IPv6-igp-01, March 2002 (work in progress).

[8] W. Biemolt, "An overview of the Introduction of IPv6 in the Internet". Draft-ietf-ngtrans-introduction-to-IPv6-transition-08, March 2002 (work in progress).

[9] P. Savola. "Security Considerations for 6to4". Internet Draft, draft-ietfv6ops-6to4 security-02.txt; March 2004.

[10] J. Bound. "IPv6 Enterprise Network Scenarios". Internet Draft, draft-ietfv6ops-ent-scenarios-01; November 2003.

[11] Y. Inoue, J. Itojun. "Translating IPv4 and IPv6 connections". http://www.kame.net/newsletter/19981001/; January 17th 2003.

[12] J. P. Martínez. "Tutorial de IPv6". Publicación del Foro IPv6.

[13] M. A. Miller. "Implementing IPv6 Supporting the Next Generation Internet Protocols". Second Edition, M&T Books, U.S.A.

[14] L. Chappell. "Advanced Cisco Router Configuration". Cisco Systems Cisco Press, U.S.A, 1999.

[15] P. Bieringer. "IPv6-HOWTO". http://www.bieringer.de/linux/IPv6/.

[16] Mark A. "Implemeting IPv6 Migrating to the next generation Internet protocol". 1997, U.S.A.

[17] E. M. Castro. "Porte de aplicaciones y servicios a IPv6", http://www.6sos.org/documentos.php

[19] V. Cerf and R. Kahn. "A Protocol for Packet Network Intercommunication". IEEE Trans on Comm, COM-22, No. 5, May 1974, pp. 637-648.

[18] D. Clark, "The Design Philosophy of the DARPA Internet Protocols". Proc SIGCOMM 1988, Sept 1988.