Capstone Project Report for

MPLS/IPv6 Gap Analysis

UNIVERSITY OF ALBERTA

Advisor: Noonari Juned

Name: Yu Yiqiao

Faculty: Master of Science in Internetworking

Date: 2014.12.10

Abstract

With the development of the IPv6 technology globally, an increasing number of companies have dramatically participated in deployment of IPv6 to replace IPv4 network. However, what technologies can be utilized properly in terms of different scenarios has become controversial.

The aim of this report is to investigate,identify and evaluate the present technologies that are applied to the process of network migration from IPv4 to IPv6 network in which primarily based on MPLS environment by means of lab demos and authoritative documents.

The project report includes analysis, comparison and evaluation of seventeen prevailing technologies, respectively for Service Provider, Enterprise as well as Broadband Customer; In particular, analysis of gap between MPLS and IPv6 is intensively discussed; Additionally, the discussion of future trends is displayed on account of each technology.

Keywords: IPv4, IPv6, MPLS

Table of Contents

1. Introduction

Since IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion, the substantial number of organization, enterprise and personal user has updated their equipment in the aspects of both hardware and software, especially for developing countries with limited IPv4 addresses.The US ARMY had completely transited to IPv6 network by 2008; and the biggest American cable system Comcast has deployed 31.63% network to IPv6 until July 2014 [1]. However, along with popularization of IPv6 in global,sorts of technological and economy problems have arisen as well, such as equipment incompatibility, costly implement and so forth.

Also, the need for professional IPv6 engineers is growing dramatically accompanying with IPv6 deployment and update in real industry. It is required for network engineers not only to skillfully implement IPv6 migration techniques in different hardware devices and operating system for service provider, enterprise and broadband customer, but to precisely make a determination that which technique should be adopted in accordance with principles of both cost-effectiveness and efficiency. Relied on that, the report provides them with technique guidance.

Furthermore, in order to avoid essential problems caused by the laws of “Network Hitless Upgrade”, consider to utilize either transitory or permanent techniques would be well-advised to remain cautious. Truly, IPv6 technology adopts entirely different approach of design compared with IPv4, therefore, the spread of IPv6 is at the cost of overthrowing current IPv4 principles. Consequently, on the one hand, costs of upgrading and rebuilding would be immense whether for payment or time, on the other hand, it is not absolutely alarming that if a more concise and effective technique got proliferated and popularized in a short span of time, values of most investment in IPv6 market would turn into nothing. For instance, Chinese governments invested a large amount of money in research and development of ISDN and ATM, more than 20 millions of ISDN lines had been established, but only 2 millions of lines were used, and even more users are turning to utilize other competitive technologies instead of ISDN [2]. Hence, this project also gives suggestions to properly and appropriately upgrade IPv6 network to balance the problem of rules violation in the part of “Case Analysis”.

Project Equipment Used:
Cisco WEB-IOU
GNS3
VMware Workstation

2. Project

2.1. Use Case#01 Service Provider

2.1.1. Dual Stack

(1) **Background:**The technique of Dual Stack (also known as Dual IP layer) is for providing complete support for both IPv4 and IPv6 in hosts and routers standardized in RFC4213. The Dual Stack plays a pivotal role in IPv6 transition and maintaining compatibility with IPv4 network, or so to speak, other techniques applied to IPv6 transition process are based on it. The fundamental principle of Dual Stack is to run both IPv4 and IPv6 on devices; the first IP field -- ***Version segment***-- of the packet can be dealt with respectively without being influenced by each other in terms of *Version 4 or 6.*

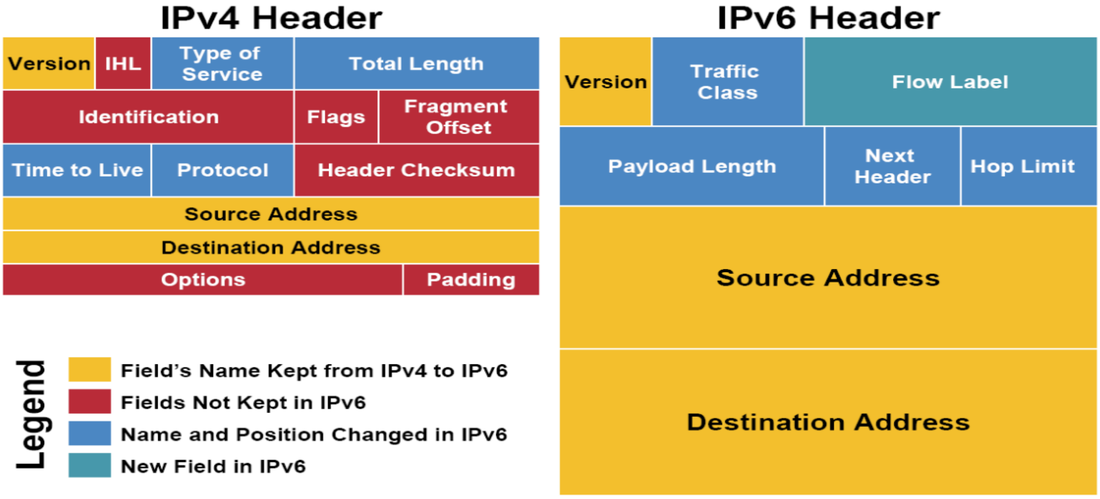


Diagram 1 -- IPv4 VS IPv6 Header [3]

(2) Lab Demos:

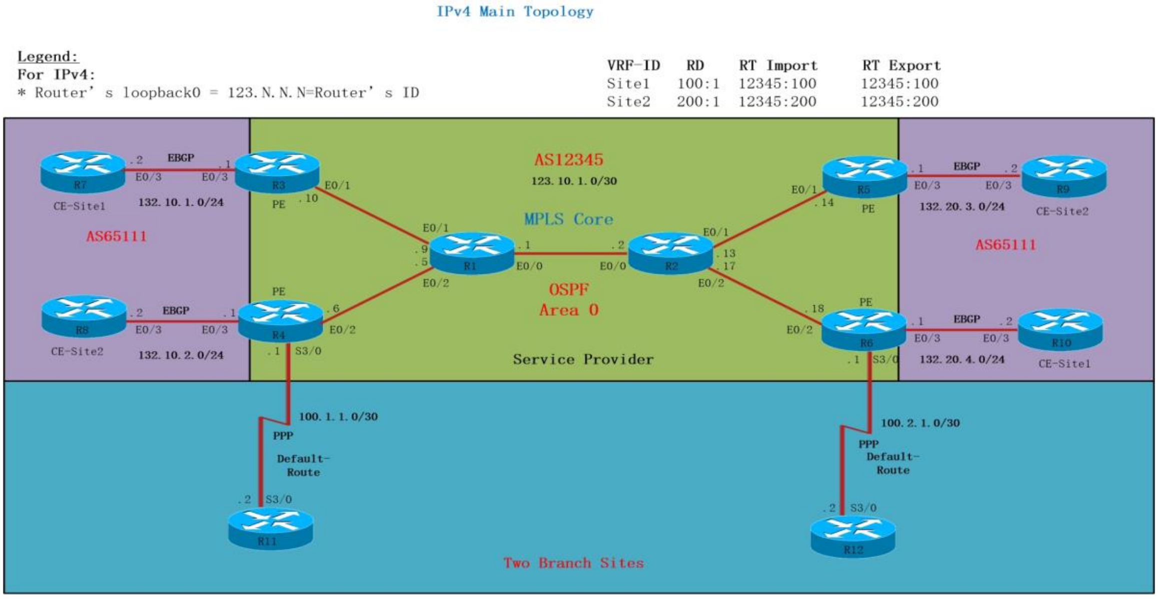
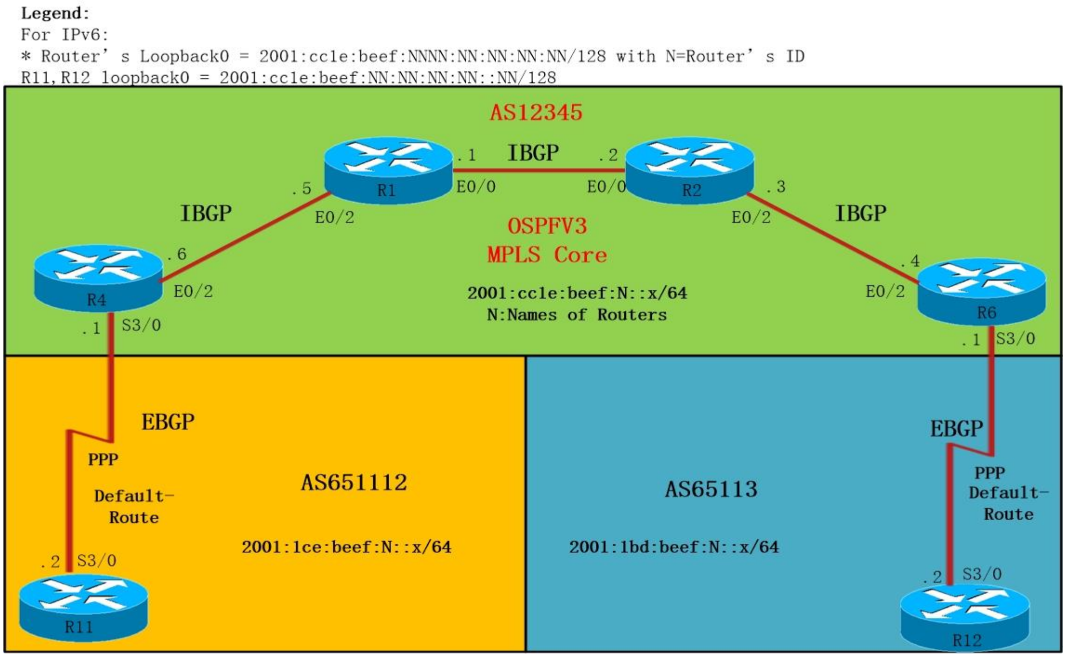


Diagram 2 -- Service Provider Main Topology

Description:

This is an original IPv4 topology used to implement and upgrade IPv6 transition technologies. The core area of Service Provider AS 12345 is operating OSPFv2 and MPLS, R1 and R2 are P Routers, R3,R4,R5,R6 are PE Routers. There are also two CE-Sites-- Site1 and Site2 and two remote branch sites. All IPv4 addresses allocation have been written as shown on the diagram. The pre-configuration is shown on the file of “Service Provider 1”.



Legend:
For IPv6:
* Router’ s Loopback0 = 2001:cc1e:beef:NNNN:NN:NN:NN:NN/128 with N=Router’ s ID
R11,R12 loopback0 = 2001:cc1e:beef:NN:NN:NN:NN::NN/128

Diagram 3 -- IPv6 Local Topology

Lab Purpose	By means of deployment Dual Stack technique, allowing two branch sites to communicate with each other
Lab Implementation	As shown on the file of “Service Provider2_dual stack”
Lab Results	**R12#ping 2001:CC1E:BEEF:11:11:11:11:11 source lo0** Type escape sequence to abort. !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 17/25/37 ms **R12#ping 100.1.1.2** Type escape sequence to abort. !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 15/17/18 ms

(3) Evaluation and Comparison:

Pros	Cons
i. Simple deployment and understanding; this is only required to configure IPv6 addresses and protocols based on original IPv4 environment directly. By default, router first initiates IPv6 connection,if IPv6 is not responding, then it can switchover to IPv4 stack and use it to exchange data that keeps network stability and redundancy. **ii.** Whether for Windows or Linux servers in SP, most of them have built-in IPv6 stack, thus, it would less affect internet service providing. **iii.** Dual Stack has addressed all communication problems of IPv6 compared with tunnel technique.	**i.** For Service Providers, it is required to upgrade all hardware&software that can support both protocol stacks,hence, during this process, service provide would have to invest much money in equipment changing. **ii.** All routers have to maintain both IPv4 and IPv6 tables,such as routing tables which lead router's efficiency decreased, and synchronization of tables is necessary that also consumes router's resources. **iii.** Dual Stack is not able to tackle the problem of IPv4 address crunch. **iv.** Dual Stack increases expenses of equipment maintenance, since it is running two stacks simultaneously.

(4) Conclusion and Future Trend:

According to four principles of SIT (Simple Internet Transition) standardized in RFC1752 [4]:

1) Gradual transition

Introduction: All sorts of organizations have dedicated huge capital to IPv4 network, so investment in IPv4 devices should be protected, ensuring that IPv4 network can be independently and normally running.

Comments: Dual Stack can guarantee existence of current IPv4 network, therefore, it should be a good solution for the rule of gradual transition.

2) Lowest dependency

Introduction: New IPv6 hosts can participate in the network at any time without being dependent on other hosts or routers.

Comments: In terms of Dual Stack,IPv4 and IPv6 stack remains completely independent, therefore, it should be good for the rule of lowest dependency.

3) Convenience for address management

Introduction: When IPv4 hosts and routers are updated to IPv6, they can continue to utilize IPv4 addresses.

Comments: Obviously, Dual Stack is convenient way of managing IPv4/IPv6 addresses.

4) Lower upgrade fees

Introduction: When network is updating from IPv4 to IPv6 or deployment of new IPv6 nodes, all the charges must be seriously considered.

Comments: Compared with tunnel, Dual Stack technique would be costly. However, as for most service providers that own high-end devices which could support IPv6, this kind of impact is not a big deal for Service Providers.

Conclusion: Based on above discussion, Dual Stack is an ideal approach to transit IPv6 network. MPLS also supports to distribute labels for IPv6 message, and the principle is almost same.

Future Trend: In fact, Dual Stack technique has been widely used in Service Provider. For instance,China Telecom” backbone network had commenced to upgrade IPv6 network based on the technique of Dual Stack after long-time research and technical reserve in June, 2012 [5]. Moreover, Dual Stack has been widely deployed in metropolitan area network by organizations and broadband customers in some big China cities like Beijing and Shanghai. In a word, Dual Stack is a mainstream IPv6 transition technology that is being applied by Internet Service Providers.

2.1.2. IPv6 over IPv4 GRE Tunnel

(1) Background:GRE tunnel technique was developed by Cisco and Net-Smiths companies and submitted to IETF in 1994, and was standardized by RFC1701 and 1702 [6]. Currently, almost all Network Equipment Manufacturers support GRE Tunnel.

(2) Introduction: Generic Routing Encapsulation(GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols,such as IP, IPX and AppleTalk, and support all routing protocols,such as OSPF, EIGRP,etc.

(3) Lab Demo: The topology is ‘diagram 2 -- Service Provider Main Topology’, assume that two branch sites are only running IPv6 stack

Lab Purpose	By means of deploying GRE Tunnel, allowing two branch sites to communicate with each other
Lab Implementation	As shown on the file of “Service Provider 3_GRE”
Lab Results	**R11# ping 2001:CC1E:BEEF:12:12:12:12:12** Type escape sequence to abort. !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 18/30/46 ms
Work Process	A GRE header is encapsulated in IPv6 Packet with an IPv4 address,so packet can traverse IPv4 area; when packet leaves IPv4 area, GRE header will be unpacked, and inside packet

	can arrive at destination.
Suggested Usage	Simple P2P tunnels that can be used within a site or between sites

(4) Evaluation and Comparison:

Pros	Cons
i. Easy to implement and deploy. **ii.** GRE is a standard protocol. **iii.** GRE tunnel is popular, since it supports all protocols. **iv.** GRE tunnel technique is mature enough so that anyone can use it. **v.** GRE supports to create elastic VPN. **vi.** GRE tunnel can carry on QoS.	**i.** The minimum length of GRE header is 4 bytes, so it will increase the length of packet so as to increase CPU consumption. **ii.** It is possible to produce the problem of address conflicts when service provider provides multiple users with GRE-based VPN. **iii.** IPv6 over IPv4 GRE tunneling is lack of encryption mechanism.

(5) Conclusion and Future Trend:

Generally, applying GRE Tunnel to IPv6 transition is not a good idea, this is because that GRE Header can enormously increase the consumption of device resources. For other applications, like Site-to-Site IPsec VPN, it can be combined with GRE Tunnel which raises efficiency; however, allowing GRE Tunnel to load layer-3 IPv6 packets is not a good choice.

GRE Tunnel is not a mainstream technology for IPv6 transition; although it supports all protocols, question of high consumption still remains unconvincing.

Further, a type of dynamic routing protocol must be operating, if a router is establishing a large number of GRE Tunnels simultaneously, it must increase the burden on the router and reduce the router performance.

2.1.3. Overlay Tunnel

(1) Background: Overlay tunneling encapsulates IPv6 packets in IPv4 packets for delivery across an IPv4 infrastructure. Between users, they can communicate with isolated IPv6 networks without upgrading IPv4 infrastructure via overlay tunnels.

(2) Lab Demo:

The topology is ‘diagram 2 -- Service Provider Main Topology ’, assume that two branch sites are only running IPv6.

Lab Purpose	By means of deploying Overlay Tunnel, allowing two branch sites to communicate with each other
Lab Implementation	As shown on the file of “Service Provider4_Overlay”
Lab Results	**R11# ping 2001:CC1E:BEEF:12:12:12:12:12**

<table>
<tr><td></td><td>Type escape sequence to abort.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 18/30/46 ms = 15/17/18 ms</td></tr>
<tr><td><b>Work Process</b></td><td>When R11 or R12 sends IPv6 packets to across Edge Routers(R4 or R6), an IPv4 header is encapsulated:<table><tr><td><b>IPv4</b></td><td>IPv6</td><td>TCP</td></tr></table>By this IPv4 header, the packet can successfully traverse IPv4 area in Service Provider. Eventually, when the packet reaches another IPv6 area, IPv4 header will be unpacked, and inside packet can arrive at destination.</td></tr>
<tr><td><b>Suggested Usage</b></td><td>Simple P2P tunnels that can be used within a site or between sites</td></tr>
</table>

(3) Evaluation and Comparison:

Pros	**Cons**
i. Easy to configure and deploy. **ii.** Header consumption is much less than IPv6 over IPv4 GRE Tunnel.	**i.** It is required to use dynamic routing protocols to support,so router has to maintain large routing tables. **ii.** Manually tunnel configuration, which increases the burden on engineers.

(4) Conclusion and Future Trend:

Overlay and GRE tunnels belong to manual tunnels, but they have slight difference. Compared with GRE Tunnel, overlay tunnel’s overhead is lower; however, overlay tunnel could only encapsulate IP header, whereas, GRE tunnel can carry other protocols that is more flexible. This overlay tunnel can be only used in simple environment,thereby generalization performance in Service Providers would not be satisfactory.

2.1.4. 6to4 Tunnel

(1) Background:6to4 allows isolated IPv6 sites or hosts, attached to a wide area network which has no native IPv6 support, to communicate with other such IPv6 domains or hosts with minimal amount of configuration that was standardized in RFC3056 [7].

(2) Introduction: The 6to4 tunnel uses the field of IPv6 address -- ‘2002::/16’ -- allocated by IANA, and maps IPv4 address to IPv6 and plus EUI-64, the specific 6to4 tunnel address can be produced. By means of this mechanism, branch sites are able to configure IPv6 addresses, and no need to apply for IPv6 address space from the Registration Organization.

(3) Lab Demo:

The topology is ‘diagram 2 -- Service Provider Main Topology ’, assume that two branch sites are only running IPv6.

Lab Purpose	By means of deploying 6to4 Tunnel, allowing two branch sites to communicate with each other
Lab Implementation	As shown on the file of “Service Provider 5_6to4”
Lab Results	**R11#ping ipv6 2002:7B06:606:1:A8BB:CCFF:FE00:C00** Type escape sequence to abort. !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/31 ms
Work Process	When R11 sends an IPv6 packet to R4, R4 can produce the IPv4 route path arriving at R6 calculated by that special address.
Suggested Usage	Point-to-multipoint tunnels that can be used to connect isolated IPv6 sites

(4) Evaluation and Comparison:

Pros	Cons
i. Automatic tunneling; No longer need to specific destination, and can calculate route path automatically. **ii.**The router almost does not need maintain routing table, since only the default route is generally used instead of dynamic routing protocol. **iii.**Since 6to4 has no impact on IPv4 routing, it cannot induce routing loops in IPv4. **iv.**Once a site gets an global IPv4 address, all hosts can get IPv6 network connection.	**i.** IPv6 addresses must be special designed according to regulation defined by RFC,therefore, the IPv6 addresses cannot be flexible designed. **ii.** Coupling is a problem when hosts from 6to4 area to communication with hosts from IPv6 area merely, so the repeater might have to be used and make the network complicated. **iii.** Since 6to4 tunnel is established automatically, so it would cause security problems.

(5) Conclusion and future trend:

IETF attaches great importance to development in 6to4 technique that can be widely applied to network transition mechanism. Currently, 6to4 is quite widely deployed in end systems, especially desktop and laptop computers Also, 6to4 is supported in a number of popular models of CPE routers, some of which have it enabled by default, leading to quite widespread unintentional deployment by end users [8]. Compared with static tunnels,such as GRE or overlay tunnel discussed above, the 6to4 apparently performances better whether in the aspects of easy deployment, good router’s performance or IPv6 addresses assignment. Additionally, 6to4 tunnel is able to carry many routing protocols, so its has wide range of application scenarios.

2.1.5. 6rd Tunnel

(1) Background: At present, the backbone network in Service Providers primarily takes IPv4 as main infrastructure, and to upgrade to IPv6 network requires a certain amount of time and capital, therefore, engineering and technical personnel need to find out an urgent technology to provide IPv6 service between IPv6 sites.The concept of 6RD tunnel was proposed and developed. The description of 6rd principles was standardized in RFC5569 [9], and the detailed 6rd standardization is available at RFC5969 expended by Cisco Systems, Inc. According to RFC5569, the Service Provider "FREE" used this mechanism to supply IPv6 service with more than 1,500,000 residential sites in five weeks.

(2) Introduction: As being a type of technology which enables a Service Provider to rapidly deploy IPv6 UNICAST service to IPv4 sites, it utilizes stateless IPv6 in IPv4 encapsulation to transit IPv4-only network infrastructure. Also, 6rd is substantially based on 6to4, but 6rd suppresses 6to4 limitations, such as allowing ISPs from using it to offer full IPv6 UNICAST connectivity to their customers.

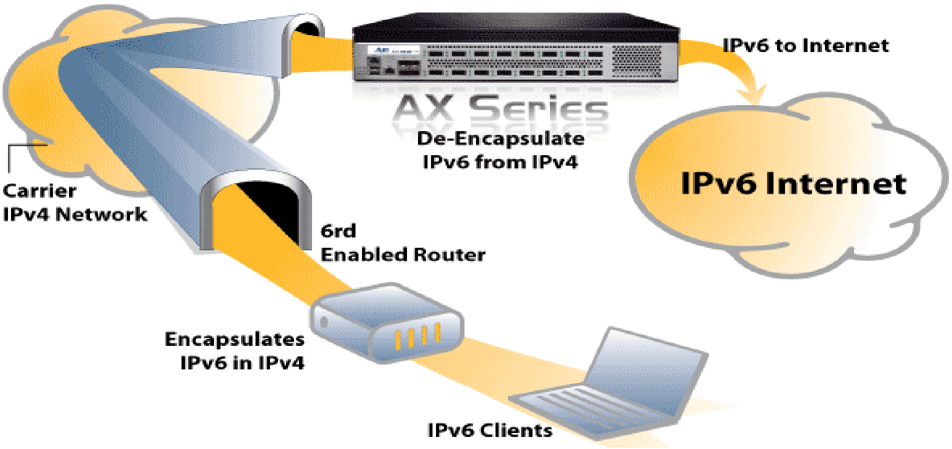


Diagram 4 -- 6rd Example [10]

By comparing with 6to4 tunnel, 6rd tunnel does not require addresses to have a 2002::/16 prefix, therefore, the Service Provider can plan its own address block for the perspective of customer sites which is more flexible. Besides, 6rd needs to carry 32-bit IPv4 destination in IPv6 payload header as it is in 6to4 that effectively reduces the cost of message transferring via paths, and also for a part of customers that are not at a fixed location, 6rd technique is able to provide services,too.
6rd experiment cannot be displayed here, because 6rd requires ASR 1000+, Series IOS-XE support.

(3) Evaluation and Comparison:

Pros	Cons
i. It is allowed for IPv4 and IPv6 users to coexist. **ii.** 6rd provides IPv6 services to users	**i.** This mechanism requires to provide both IPv4 private and public address with IPv6 prefix, hence, it cannot reduce

with fast and flexible approaches that less affects backbone network in Service Provider. **iii.** Stateless 6rd control devices do not require maintain active flow-state tables which can reduce the use of system resources.	consumption of IPv4 address space. **ii.** IPv6 prefix assignment is influenced by IPv4 address which would cause IPv6 spoofing. **iii.** This technology needs long lease time that allocated IPv4 addresses to CE.

(4) Conclusion and Future Trends:

In conclusion, 6rd performs more reliably and leads less burden to the Service Provider than 6to4. According to some successful cases -- Canadian ISP Videotron has deployed 6rd for customers with 6rd-ready routers, and Norwegian ISP Altobox announced that they offer IPv6 to 70,000 customers based on 6rd, all customers who bypass the ISP’s “home central” were able to use 6rd in March 2013 [11]. However, on the basis of authoritative statistic from data collected by Eric Vyncke, they involve tens of thousands of connections to a site since 2008 [12], as shown on the table below:

Year	Native	Teredo	6to4	6rd	ISATAP
2008	21.75	35.75	21.89	18.29	2.50
2009	23.78	46.68	18.07	9.99	1.48
2010	25.53	48.37	19.80	5.70	0.60
2011	27.06	53.92	16.78	1.94	0.30
2012	24.07	60.48	14.14	1.12	0.19
2013	37.86	48.50	12.16	1.40	0.08

The table shows the changes in the rate of five mainstream IPv6 transition technologies from 2008 to 2013. It is clear from the chart that 6rd was developed on the large-scale at the beginning but has not grown at all since then.

Here is a particular case which shows potential issues on 6rd technique: Canadian ISP Rogers Communications deployed 6rd for customers with 6rd-ready routers, but the service was not supported officially and suffered from extremely poor performance [11]. Although Rogers did not disclose its overall IPv6 deployment strategy, except essential deployment issues, 6rd itself would be also problematic. Hence, configuring 6rd in the Service Provider should be more discreet or conduct deep research before deployment.

2.1.6. Teredo Tunnel

(1) Background: Teredo technique was developed by Microsoft and was standardized by RFC 4380 in the IETF [13].

(2) Introduction: Teredo is a transition technology that gives full IPv6 connectivity for IPv6-capable hosts which are on the IPv4 Internet but which have no direct native connection to an IPv6 network. Consider technologies that have just introduced above,either manual tunneling(GRE,Overlay) or automatic tunneling(6to4) cannot solve the problem that when IPv6 candidate node is isolated behind a Network Address Translator (NAT) device. Even "tunnel brokers" is a possible approach to tackle this question that will be analyzed later, however, there are limits existing such as QoS,etc. Also, in the real network environment, almost all border gateways enable NAT for security as well as address space. In order to transport IPv6 packets via one-layer or multi-layer NAT, IPv6 packets must be encapsulated into the data format of IPv4 UDP including IPv4 and UDP Headers, since UDP can be generally unpacked by NAT. Teredo uses independent tunneling protocol to provide IPv6 connectivity by encapsulating IPv6 packets within IPv4 UDP packets with port 3544 that can support NAT traversing. And the Teredo prefix is registered unique routing IPv6 address 2001:0::/32 globally.

(3) Teredo work process:

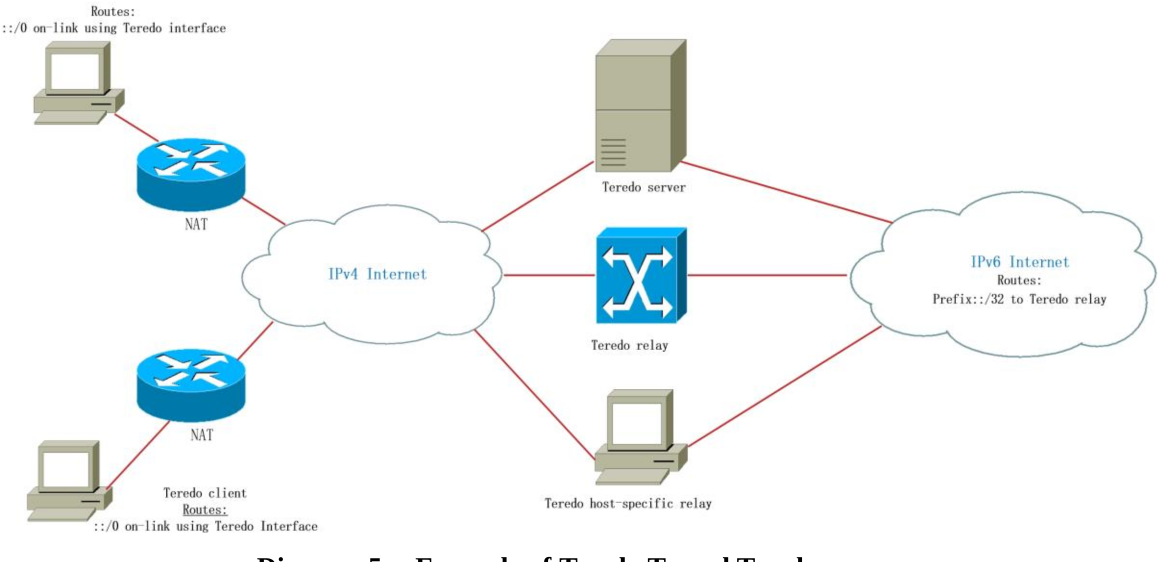

Routes:
::/0 on-link using Teredo interface
NAT
IPv4 Internet
Teredo server
Teredo relay
IPv6 Internet
Routes:
Prefix::/32 to Teredo relay
NAT
Teredo client
Routes:
::/0 on-link using Teredo Interface
Teredo host-specific relay

Diagram 5 -- Example of Teredo Tunnel Topology

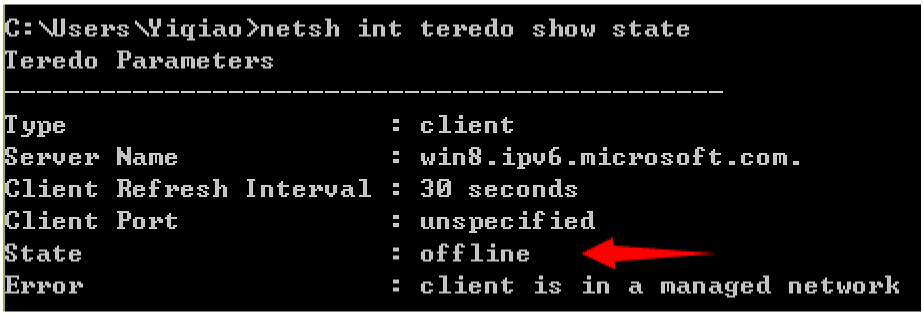
Teredo Process:

- Initialize Teredo clients
- Maintain NAT mapping
- Communications initialization between Teredo clients/sites
- Communications initialization between Teredo clients to Teredo relay
- Communications initialization between IPv6 hosts and Teredo clients

Note that the whole process is automatically supported by Teredo clients in Windows

Operating System without external control.

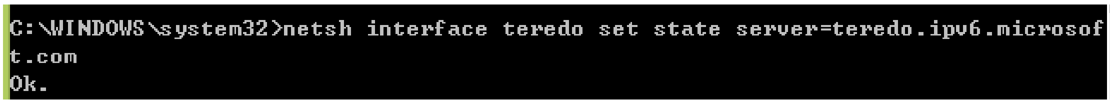
An example of Teredo Tunnel configuration in client -- Windows 7:
Step 1: Check if Tunnel Teredo adapter connects to the Internet:



```
C:\Users\Yiqiao>netsh int teredo show state
Teredo Parameters
---------------------------------------------
Type                    : client
Server Name             : win8.ipv6.microsoft.com.
Client Refresh Interval : 30 seconds
Client Port             : unspecified
State                   : offline
Error                   : client is in a managed network
```

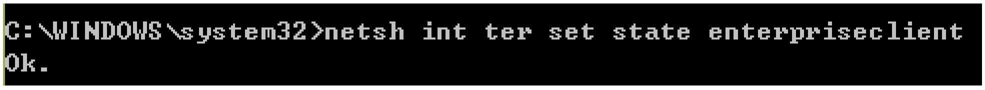
The state is “offline” which means that host has not connected to the server.

Step 2: Run ‘cmd.exe’as administrator and appoint address of Teredo Server:



```
C:\WINDOWS\system32>netsh interface teredo set state server=teredo.ipv6.microsof
t.com
Ok.
```

Step 3: Change parameter of Teredo type from client to enterpriseclient:



```
C:\WINDOWS\system32>netsh int ter set state enterpriseclient
Ok.
```

Then Client State changes to be “qualified”

Step 4: If personal computer would like to access to the Internet websites by IPv6, like Google, we need change files of OS: **C:\Windows\System32\drivers\etc\hosts.**

(4) Evaluation and Comparison:

Pros	Cons
i. Easily traverse NAT devices and provide a rich set of services. **ii**. Endpoints do not require public IPv4 addresses,and packets that can traverse NAT equipment and IPv6 network.	**i.** Teredo can only provide a single IPv6 address per tunnel endpoint. As such, it is impossible to use a single Teredo tunnel to connect multiple hosts, contrary to 6to4, etc. **ii.** The bandwidth available is limited by the Teredo relays to Teredo clients.

(5) Conclusion and Future Trend:
In conclusion, Teredo Tunnel allows automatic IPv6 tunneling between hosts that are located across one or more IPv4 NATs. Since NAT devices supports UDP port translation, so NAT supports Teredo. In reality, NAT is being widely taken by edge devices of Service Provider, Enterprises,Campus or Personal Network, so as for a type of IPv6 transition technology, Teredo Tunnel can be perfectly working.
However, Teredo will be used less and less in the future, this is because Teredo always utilizes relays which break contingency of network structure and more IPv4

edge devices are upgraded to support 6to4 technology.

2.1.7. 6PE, 6VPE

(1) Background: To interconnect IPv6 islands over MPLS areas -- enabled IPv4 cloud, IPv6 Provider Edge Routers (6PE) was standardized by IETF in RFC4798 [14].

To provide Virtual Private Network (VPN) services for its IPv6 customers through its packet-switched backbone MPLS area, IPv6 VPN provider edge(6VPE) was standardize by IETF in RFC4659 [15].

(2) Introduction:MPLS -- as a kind of mature routing&switching technology -- has been widely used on IPv4-based network. MPLS itself combines layer-2 switching with layer-3 routing technologies (L2/L2 integrated data transmission technology), not only has great compatibility with sorts of link-layer technique, also support multiple network-layer protocols including IPv4 and IPv6. Moreover, MPLS relatively simplifies the complexity of the network layer and reduces costs of network upgrading.

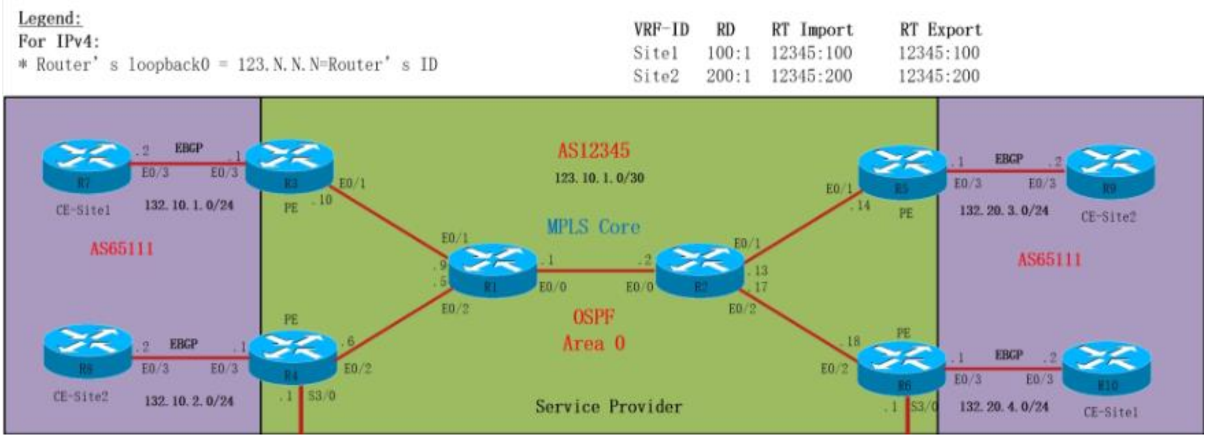
IPv6 is a network layer protocol of the next generation which has got much attention by the industry. The new technologies combined MPLS with IPv6 have arose at the historic moment. Recently, 6PE and 6VPE, being as two mainstream technologies have got widespread support.

6PE:6PE is a transition technology that allows CE routers at IPv6 isolated islands to communicate with other routers located at other IPv6 areas traversing from existing IPv4 PE routers. ISP can take advantage of current IPv4 backbone network to provide IPv6 access capability. The main idea of 6PE is that users' IPv6 information can be transferred to IPv6 routing information attached by MPLS labels, and spread them to IPv4 backbone network via IBGP sessions. The Service Provider can operate OSPF or IS-IS; and between CE and 6PE, static routing, IGP or EBGP can be utilized.

6VPE: Although IPv6 has solved the shortage of address space, for security and privacy, there is still significantly demand for IPv6VPN requirements. 6VPE -- as a type of VPN technology -- can support MPLS/BGP-VPN infrastructure. The functional components contain PE, CE and P router. VRF is responsible for dealing with VPN-IPv6 routes on PE router; CE loads different users and connect them to PE by unique physical/logical interfaces; P router belongs to backbone equipment that is responsible for MPLS transmitting.

Both 6PE and 6VPE can be applied to MPLS+IPv6 network environment, but they are obviously distinct. The goal of 6PE is to connect IPv6 isolated islands, multiple IPv6 sites for 6PE can belong to one VPN (IPv6 public network) and address space is disallowed to overlap. Inversely, 6VPE is a type of IPv6-VPN technology, multiple IPv6 sites can completely belong to different VPNs that is much likely to IPv4-VPN work principles.

(3) Lab Demo:



Legend:
For IPv4:
* Router' s loopback0 = 123.N.N.N=Router' s ID

VRF-ID	RD	RT Import	RT Export
Site1	100:1	12345:100	12345:100
Site2	200:1	12345:200	12345:200

Diagram 6 -- MPLS-VPN

IPv6 Address Allocation:

Router	Port	IPv6 address
PE(R3)	E0/3	2001:1eee:1234::1/64
PE(R4)	E0/3	2001:1eee:1243::1/64
PE(R5)	E0/3	2001:1eee:1324::1/64
PE(R6)	E0/3	2001:1eee:1342::1/64
CE-Site1(R7)	E0/3	2001:1eee:1234::2/64
	Loopback0	2001:1::7/128
CE-Site2(R8)	E0/3	2001:1eee:1243::2/64
	Loopback0	2001:1::8/128
CE-Site1(R9)	E0/3	2001:1eee:1324::2/64
	Loopback0	2001:1::9/128
CE-site2(R10)	E0/3	2001:1eee:1342::2/64
	Loopback0	2001:1::10/128

Preconditions:

Sites can communicate with each other by IPv4 MPLS VPN.

Requirements:

Assume site1 and site2 have upgraded their network to IPv6 based,and they have to utilize MPLS VPN to transit IPv6 messages, but the Service Provider has not deployed IPv6 network now. As to CE Site1 routers R7 and R10, they are required to communicate by 6PE, but for CE Site2 routers R8 and R9, they need 6VPE as solution.

Lab Purpose	**6PE for CE-Site1**

Lab Implementation	As shown on the file of “Service Provider 6_6PE”
Lab Results	**R10#ping 2001:1::7 source lo0** Type escape sequence to abort. Packet sent with a source address of 2001:1::10 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 3/7/19 ms **R10#trace 2001:1::7** Type escape sequence to abort. Tracing the route to 2001:1::7 1 2001:1EEE:1342::1 7 msec 189 msec 11 msec 2 ::FFFF:123.10.1.17 [MPLS: Labels 19/16 Exp 0] 5 msec 9 msec 10 msec 3 ::FFFF:123.10.1.1 [MPLS: Labels 19/16 Exp 0] 7 msec 14 msec 3 msec 4 2001:1EEE:1234::1 [AS 65111] [MPLS: Label 16 Exp 0] 4 msec 6 msec 2 msec 5 2001:1EEE:1234::2 [AS 65111] 17 msec 6 msec 9 msec
Work Process	When CE R10 sends the IPv6 packet to 6PE router, 6PE router will check its IPv6 routing table and tag two-layer labels according to matched next-hop address by mapping 6PE router’s outbound IPv4 address to another IPv4 address, and add prefix “::FFFF:” in front of that, such as “::FFFF:123.10.1.17”. The inner MPLS label is distributed for IPv6 prefix to transmit packets via MP-BGP, and outer MPLS label is distributed for 6PE router’s IPv4 address, and send this packet to next P router via LSP; eventually, this label is popped on R2 (P router) in accordance with the rule of “Penultimate Hop Popping” and bare IPv6 data packets arrive at R3. Note that because of EBGP split-horizon, packets coming from the same AS are not allowed to enter another AS area, so to break split-horizon is necessary.
Suggested Usage	IPv6 - MPLS

.

Lab Purpose	**6VPE for CE-Site2**
Lab Implementation	As shown on the file of “Service Provider 7_6VPE”
Lab Results	**R8#ping ipv6 2001:1::9 source lo0** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 2001:1::9, timeout is 2 seconds:

	Packet sent with a source address of 2001:1::8 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 4/13/28 ms **R8#traceroute ipv6 2001:1::9** Type escape sequence to abort. Tracing the route to 2001:1::9 1 2001:1EEE:1243::1 1 msec 13 msec 1 msec 2 ::FFFF:123.10.1.5 [MPLS: Labels 24/31 Exp 0] 50 msec 10 msec 9 msec 3 ::FFFF:123.10.1.2 [MPLS: Labels 24/31 Exp 0] 9 msec 87 msec 57 msec 4 2001:1EEE:1324::1 [AS 12345] [MPLS: Label 31 Exp 0] 14 msec 11 msec 4 msec 5 2001:1EEE:1324::2 [AS 12345] 3 msec 27 msec 60 msec
Work Process	When CE R8 sends IPv6 packets to CE R9 via IPv6 VPN, the traffic flow should be transmitted inside IPv6 tunnel. When they come to 6VPE router's VRF interface, the 6VPE router will forward them to inside Service Provider's IPv4 core in AS12345 by inner VPN label. Also, outer label(IGP label) for iBGP next-hop distributed by LDP, and inner label(VPN label) for the IPv6 prefix, distributed by MP-BGP. Once packets arrive at Penultimate P router, the inner label will be popped and packets can arrive at destination R9 via VPN. Note that because of EBGP split-horizon, packets coming from the same AS are not allowed to enter another AS area, so to break split-horizon is necessary.
Suggested Usage	IPv6 -- MPLS VPN

(4) Evaluation and Comparison:

6PE and 6VPE	
Pros	**Cons** [16]
i. Enable IPv6 sites to communicate with each other over an MPLS/IPv4 core networking using LSPs. **ii.** Only provider edge routers require upgrade. **iii.** Minimal operational cost and risk, since 6PE and 6VPE cannot impact on existing IPv4 and MPLS services. **iv.** Production services ready, as ISP can delegate IPv6 prefixes.	**i.** Be supported only by SVI interfaces. **ii.** The number of IPv6 VRFs supported is restricted to 113. **iii.** The scale is limited by the number of labels available (4000 labels) for the single label per prefix mode allocation. **iv.** Supports only static routes and BGP for IPv6 in VRF context. **v.** Since P routers are not ipv6 enable, so MPLS core does not support ICMPv6

v. Flexibility and convenience, since 6PE and 6VPE routers can be added at any time	that are necessary to IPv6 ICMP response and PMTU Discovery.

(5) Conclusion and Future Trend:

Cisco made 6PE plans in 2001 conforms to draft standards [IPv6--BGP] issued by IETF which is “By taking BGP protocol to connect IPv6 areas crossing multiple IPv4 clouds”. In terms of some services providers that are unwilling to invest hardware equipment to extend their MPLS based business, 6PE and 6VPE can be an ideal option. Not only 6PE and 6VPE are able to smoothly inject IPv6 services to MPLS backbone network without adversely affecting MPLS itself, but also can avoid revenue risk. Additionally, 6PE and 6VPE have same functional ability, scalability as well as elasticity for IPv4 and IPv6. Eventually, even though sites have both run IPv4 and IPv6, the transmission process of them is not impacted with each other, since they are completely unique and isolated.

Yet, 6PE and 6VPE have their own apparent demerits as well. One of the most obvious example is that PE router would save both IPv4 and IPv6 routes information in VRFs and transport IPv4 and IPv6 packets, therefore, requirement of PE router performance is very high.

In conclusion, these two transition technologies can be widely utilized in the real industry. With traditional Frame-Relay, ATM technologies step down from the stage of history, IPv6,MPLS and various VPNs have occupied the market,obviously it is impossible to upgrade Dual Stack for all devices overnight, so based on MPLS-VPN businesses, a transition technique must be applied, so numerous Service Providers have deployed some 6VPE, like Telus, Rogers, etc. As time goes by, more and more enterprises, personal users have migrated to IPv6, in order for bearer service, Service Provider may have to use these two technologies before all equipment have completed upgrading.

2.1.8. Multicast VPNv6

(1) Background: In order to transmit IPv4/IPv6 multicast traffic between VPN sites within a BGP/MPLS IP VPN, RFC6513 [17] and RFC6516 [18] standardized Multicast (v4/v6).

(2) Introduction: As we know that forwarding mode of multicast message is different from unicast in which requires to do RPF check according to source of multicast packets and incoming interface, and only for packets that are from RPF incoming interface can be forwarded. Also, each router has to know the unicast routing where is route to the source of multicast. However, in BGP/MPLS IP VPN network, P routers have no ideas about what are the private IPv4 or IPv6 network routes. Based on that, Multicast-VPN concept was created that can help both IPv4 and IPv6 multicast packets exchange from isolated areas. The primary thing will be concentrating on IPv6 Multicast-VPN.

As MPLS outstanding performance to be compatible with different protocols, it has extended to serve for IPv4 and IPv6 multicast VPN based on 6VPE as well. The MVPN mainly includes four parts: **(1)** ***Multicast domains:*** composed of a set of interconnected MVRF collections,each multicast domain only corresponds to a multicast-VPN. **(2)** ***MVRF:*** Enable layer-3 multicast instances to maintain unicast and multicast route forwarding tables. **(3)** ***Multicast Tunnel:*** Connect to each MVRF to transmit private data inside multicast domains. **(4)** ***Multicast distribution tree:*** establish multicast distribution tree between PEs belonging to the same VPN, including Share-MDT and Switch-MDT.

(3) Lab Demo:

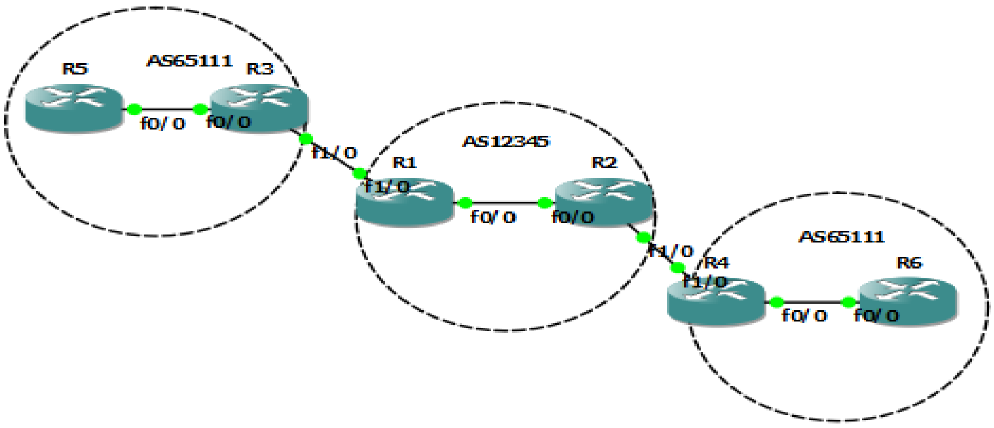


Diagram 7 -- IPv6 MVPN Lab Topology

Pre-lab:

Pre-lab Purpose	**Enable MPLS VPN for CEs (R5,R6) to communicate with each other by IPv6 packets.**
Pre-lab Results	(1) **R5#ping 2001:1::10 source lo0** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 2001:1::10, timeout is 2 seconds: Packet sent with a source address of 2001:1::7 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 64/111/180 ms IPv4 Multicast-VPN configuration is shown on the file of “Service Provider 9_MVPN1”

Lab Purpose	**R6 is able to access to a multicast source R5**
Lab Implementation	As shown on the file of “Service Provider 9_MVPN2”

Lab Results	**R6#ping FF04::1** Output Interface: loopback0 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to FF04::1, timeout is 2 seco nds: Packet sent with a source address of 2001:1::10 Reply to request 0 received from 2001:1::7, 280 ms Reply to request 1 received from 2001:1::7, 184 ms **R6#show ipv6 pim group-map ff04::** IP PIM Group Mapping Table (* indicates group mappings being used) FF00::/8* SM, RP: 2001:1EEE:1234::2 RPF: ,:: Info source: Static Uptime: 00:00:41, Groups: 0
Work Process	When receiver R6 sends IGMP to a multicast source R5,R5 creates (*, FF04::1); After that, PE R4 gets "Join Message" and creates (*, FF04::1) and point f0/0 as MTI interface. PE R4 uses GRE to encapsulate packets and forward it to R5. When R5 receives this message,it should create (*, FF04::1) and send join message for R5. Once R5 gets this message, RPT has successfully created.
Suggested Usage	IPv6 MVPN

(5) Evaluation and Comparison: [19]

Pros	Cons
i. Only upgrade PE routers to support 6VPE that can support IPv6 multicast messages transition. **ii.** Can be able to send IPv6 multicast messages to multiple locations. **iii.** Provides high-speed information delivery. **iv.** IPv6 MVPN support multiple instances at the same time; in other words, it can support multiple IPv6 multicast services.	**i.** IPv6 MVPN adds burden to the PE routers in the Service Provider and results in wasted bandwidth. **ii.** The update source does not support Multiple BGP, and configuring them can break Multicast VPN RPF checking. **iii.** Extranet multicast is not supported, as multicast routes are not allowed to be exported or imported between VRFs. **iv.** Multicast-VPN is immature and still developing.

(6) Conclusion and Future Trend:

With the continuous improvement of living standards, the information consumption for public is growing rapidly, all kinds of IP broadband network applications such as TC, video conference, network audio and video application and multimedia distance education have broad market prospects.At the same time, a lot of bandwidth consumption of Service Provider is challenging to provide more efficient and stable internet services on the basis of the existing network resources, especially in which IPv4 and IPv6 environment. Combined with MPLS VPN, IPv6 multicast technology can be effectively extended and provide an unprecedented business development prospects. Also, the Service Provider does not need improve too many devices to support IPv6 multicast for independent IPv6 areas which is economic. However, defects should not be avoided. Actually, implementing MVPNv6 for IPv6 multicast routes looks tough because of complex configurations; further, MVPNv6 would not currently support all multicast functions, such as bidirectional multicast-routing,etc, so this technique has yet to be improved.

2.2. Use Case#02 Enterprise

2.2.1. Dual Stack

The principles of Dual Stack have been analyzed in Case#01 Service Provider, and its pros and cons have discussed above as well. Here, to compare difference for Dual Stack applied in Service Provider and Enterprise is needed.

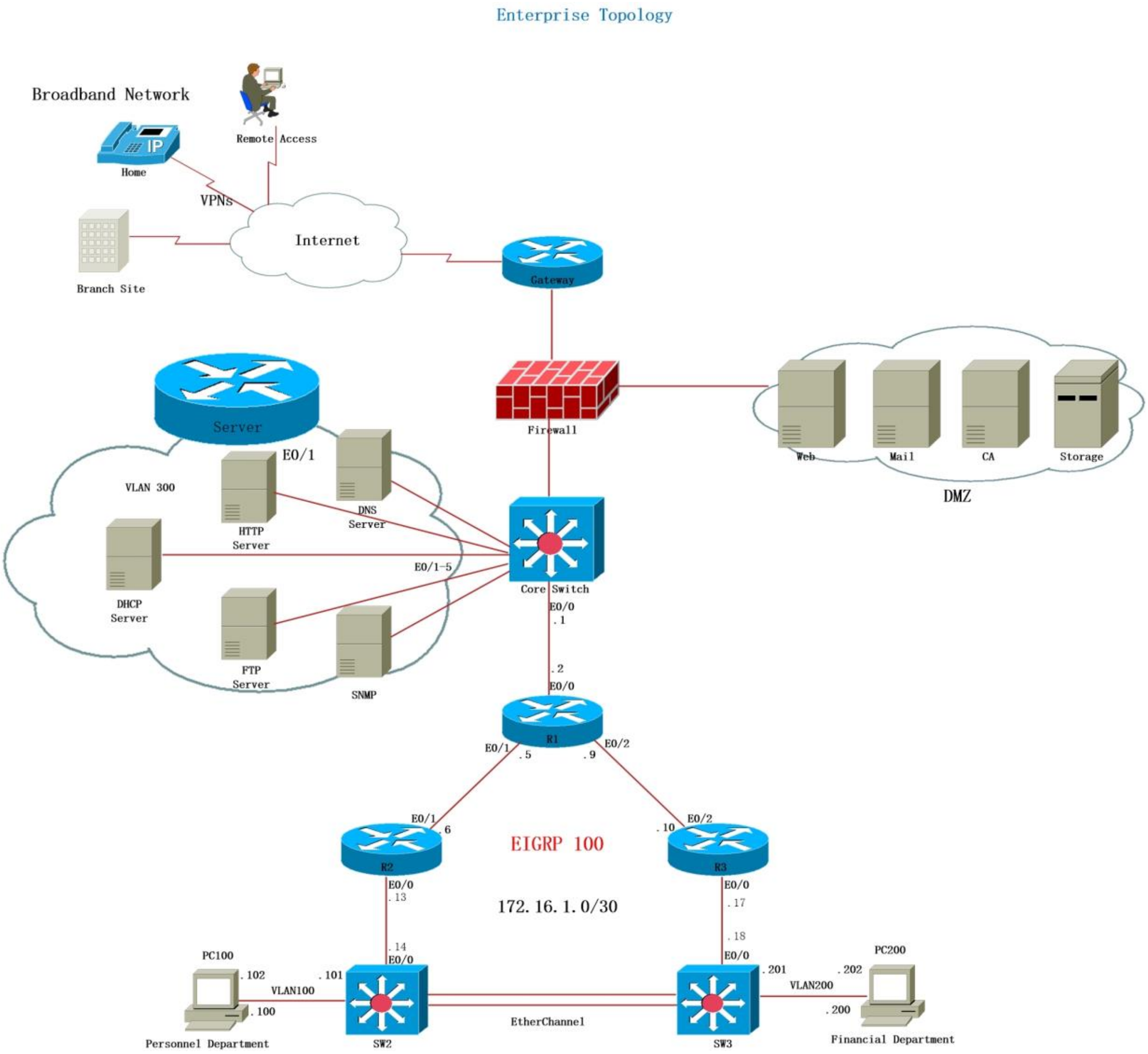


Diagram 8 -- Main Enterprise Topology

This is a typical enterprise inside network topology; a gateway router access to the Internet, and a Firewall protects inside servers and users. Personal users connect to access-layer switches, servers and enterprises are isolated by VLANs. Routers run one or more kinds of dynamic routing protocol (IGP),such as OSPF, EIGRP. Note that wire and device redundancy is necessary for internal network.

Lab Demo:

The topology is ‘diagram 8 -- Main Enterprise Topology ’

IPv6 Address Allocation:

Device	Port	IPv6 address
SW1	VLAN300	2001:DB8:10::2/64
	E0/0	2001:1CE:10::1/64
SW2	VLAN100	2001:CC1E:8BAD:1234::2/64
	E0/0	2001:1FE:10::14/64
SW3	VLAN200	2001:DB8:11::201/64
	E0/0	2001:1AE:10::18/64
R1	E0/0	2001:1CE:10::2/64
	E0/1	2001:1EE:10::5/64
	E0/2	2001:1DE:10::9/64
R2	E0/1	2001:1EE:10::6/64
	E0/0	2001:1FE:10::13/64
R3	E0/0	2001:1AE:10::17/64
	E0/2	2001:1DE:10::10/64
Server	E0/1	2001:DB8:10::1/64
PC100	E0/1	2001:CC1E:8BAD:1234:A8BB:CCFF:FE00:810(auto-conf)
PC200	E0/1	**2001:DB8:11::202/64**

Lab Purpose	**PC100 communicates with PC200**
Lab Implementation	As shown on the file of “Enterprise 1_Dual-Stack”
Lab Results	**PC200#ping 2001:CC1E:8BAD:1234:A8BB:CCFF:FE00:810** Type escape sequence to abort. !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/12 ms
Work Process	Use IPv6-Stack to transmit IPv6 packets

Conclusion and Comparison:

As discussed earlier, Dual Stack technique performs greatly in Service Provider. For enterprises, Dual Stack is worth to utilize as well, and even work better in some scenarios.

First, in almost all enterprises and organizations, the number of network device is significantly less than Service Provider, thereby upgrading hardware equipment must be relatively inexpensive and time-saving.

Second, renew and upgrade devices in Service Provider is at high risk, once a mistake occurs, a large number of customers would be adversely impacted.

Thirdly, planning IPv6 addresses in the enterprise is relatively easy, one reason is that the number of users is much less Service Provider, another reason is that SLAAC mechanism can assign IPv6 addresses easily, even if when any users are authenticated to access to enterprise network, they can obtain an IPv6 address automatically.

2.2.2. ISATAP Tunnel

(1) Background:ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) was originally specified as *experimental* in RFC 4214 and was then completely replaced by a new version, as *informational* in RFC5214 [20].

(2) Introduction:ISATAP is an IPv6 transition mechanism meant to connects IPv6 hosts/routers over IPv4 networks. ISATAP views the IPv4 network as a link layer for IPv6 and views other nodes on the network as potential IPv6 hosts/routers. The fundamental of ISATAP is that before a Dual Stack host is trying to communicate with another host or router, the host must get an ISATAP address. Firstly, Dual Stack host send a request to ISATAP server, and then it can get a 64-bit IPv6 prefix, and add 64-bit "::0:5EFE:x.x.x.x" (x.x.x.x is IPv4 address) which is the final ISATAP address. Once host gets ISATAP address, it becomes ISATAP client that can communicate with others; in other words, ISTAP regards IPv4 network as a host platform, and establishes an IPv6-in-IPv4 automatic tunnel to accomplish IPv6 communications. ISATAP can be implemented in Microsoft Windows Operating Systems(Windows XP, Vista, 7, 8, Server 2008, 2012), Linux, Android, and in some versions of Cisco IOS.

(3) Lab Demo:

The topology is 'diagram 2 -- Service Provider Main Topology ',assume that two branch sites are only running IPv6

Lab Purpose	**By means of deploying ISATAP tunnel, allowing two branch sites to communicate with each other**
Lab Implementation	As shown on the file of "Enterprise 2_ISATAP"
Lab Results	**R11#ping 2001::6402:102** Type escape sequence to abort. !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 23/25/28 ms
Suggested Usage	Point-to-multipoint tunnels that can be used to connect systems within a site

(4) Evaluation and Comparison:

Pros	**Cons**
i.The usage of IPv6 prefix for ISATAP can be any legal IPv6 64-bit prefix, thus, ISATAP can be used in combination with other transition	**i.** Since ISATAP is a tunnel technique, so ISATAP is facing with security issue. If no any measures are put into tunnel protection, attacker can inject many false packets with

technologies, especially when it combines with 6to4, inside dual stack hosts can easily access to IPv6 backbone network. **ii.**ISATAP does not require tunnel nodes to have an unique IPv4 address, only if dual stack hosts own an IPv4 Uncast public or private address, so it can avoid the problem of insufficient IPv4 address. **iii.**ISATAP does not require sites to provide special IPv4 service(i.e. multicast) which is easy to implement.	“protocol 41” into ISATAP tunnel. Also ISATAP is using neighbor discovery protocol,so it can be infected by DoS attack,etc. **ii.** ISATAP builds its PRL by consulting the DNS, which does not rely on lower-layer protocol (IPv6), so this is a violation of network design principles. **iii.** ISATAP requires much higher CPU utilization compared with other tunnel technologies. [21]

(5) Conclusion and Future Trend:

ISATAP tunnel was designed for enterprise networks, and ISATAP provides automatic encapsulation by using a virtual IPv6 overlay. Recently, ISATAP was enhanced to allow automatic IPv4-in-IPv4 encapsulation, so it would be used for enterprise networks with IPv4 and IPv6 co-existence.

2.2.3. SLAAC

(1)Background: Stateless address autoconfiguration (SLAAC) is one of auto-configuration protocols for IPv6 address allocation that was standardized in RFC4862 [22].

(2)Introduction:SLAAC mechanism requires no manual configuration of hosts, minimal configuration of routers and no additional servers. Specifically, SLAAC can allow hosts to generate its own IPv6 addresses using a combination of locally available information and information advertised by routers. Routers advertise IPv6 prefix and the length of prefix by RA message, plus an Interface ID created by EUI-64 progress, then the final IPv6 address can be formed by combining the two. If there is no routers in the real environment, hosts can only generate link-local addresses that are sufficient for communication among nodes.

(3) Lab Demo:

The topology is ‘diagram 8 -- Main Enterprise Topology ’

Lab Purpose	**PC100 obtains IPv6 address automatically when enabling interface; and eventually PC100 can communicate with PC200**
Lab Implementation	As shown on the file of “Enterprise 3_SLAAC”
Lab Results	**PC200#ping 2001:CC1E:8BAD:1234:A8BB:CCFF:FE00:810**

	Type escape sequence to abort. !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/12 ms
Work Process	After SLAAC is enabled on PC100’s direct interface, PC100 starts sending RS message to inform SW2 that “I need RA message”; then SW2 will reply RA message as responding which includes link prefix and the length of prefix, and act as ‘default gateway’ that advertise link-local address; once PC100 receives RA message, PC100 will automatically gain a complete IPv6 address by adding EUI-64 manually or automatically. Note that NS and NA messages play a vital role in duplicate address detection (DAD) which is similar as ARP function for IPv4.
Suggested Usage	Stateless auto-configuration of IPv6 address

(4) Evaluation and Comparison:

Pros	Cons
i.It is pretty simple for hosts/routers to obtain IPv6 addresses. **ii.**“Plug and Play”.	**i.** It is bad for network management, since stateless protocol is hard to keep track of assigned addresses.

(5) Conclusion and Future Trend:

The biggest merit for SLAAC is about “Plug and Play” which means that any users can simply obtain proper IPv6 addresses without conflicts or reputation. The most promising aspect for SLAAC is based on “Internet of Things”.

As we know that IPv6 is in order to solve the problem of insufficient address,while the target of “Internet of Things” technique is to make interconnection between different machines through network and communication technologies,such as sensors,controller,etc. However, traditional IPv4 is obviously not able to support such vast number of devices, so IPv6 is leading the development of “Internet of Things”. Consider that an “intelligent room” is designed with intelligent household appliances, such as fridge, air-conditioner, etc, and you can speak to them to switch them on and off. However, each appliance should have own IPv6 address, therefore, SLAAC can perfectly let them obtain IPv6 address once they plug in power cord and connect to house router.

In conclusion,SLAAC is well suitable for large networks of simple and undifferentiated nodes. That would be the irreplaceable technique in the future.

2.2.4. DHCPv6

(1) Background: Dynamic Host Configuration Protocol (DHCPv6) is a mechanism to auto-configure IPv6 addresses, IPv6 prefixes and other configuration data to IPv6 devices, such as hosts, routers and other devices. DHCPv6 was first standardized in RFC3315 [23], and RFC3319, 3633,5007,6221 extended its functionality.

(2) Introduction: DHCPv6 can automatically allocate reusable IPv6 network addresses to IPv6 nodes by DHCP servers and other configuration information. DHCPv6 can be stateful or stateless. With Stateful DHCPv6, the address assignment and DNS resolvers are both supplied by DHCPv6, but with Stateless DHCPv6, it is really SLAAC with DHCPv6 stepping in to provide the DNS resolver. IPv6 hosts automatically carry on stateless address auto-configuration and send messages tagged by ‘M’ or ‘O’ marks:

M:0 O:0	**Stateless auto-configuration**
M:1 O:1	**Stateful auto-configuration(DHCPv6)**
M:0 O:1	**Stateless auto-configuration and Prefix requires to be obtained by RA**

// M: ipv6 nd managed-config-flag

// O: ipv6 nd other-config-flag

DHCPv6 clients and servers use UDP 546 and 547 ports to exchange messages. DHCPv6 Clients make use of link-local addressing to send and receive DHCPv6 messages, and DHCPv6 servers make use of the reserved link-local “ff02::1:2” and site-local “ff05::1:3”multicast addresses.

(3) Lab Demo:

The topology is ‘diagram 8 -- Main Enterprise Topology ’

Lab Purpose	**PC200 obtains IPv6 address by DHCPv6 server when enabling interface; and eventually PC200 can communicate with PC100**
Lab Implementation	As shown on the file of “Enterprise 4_DHCPv6”
Lab Results	**PC200#ping 2001:DB8:10::1** Type escape sequence to abort. !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/7 ms **Server#show ipv6 dhcp binding** Client: FE80::A8BB:CCFF:FE00:910 DUID: 00030001AABBCC000900 Username : unassigned IA NA: IA ID 0x00040001, T1 43200, T2 69120 Address: 2001:DB8:11:0:E1BE:CEFE:6365:EAF0 preferred lifetime 86400, valid lifetime 172800

	expires at Oct 16 2014 03:01 AM (172612 seconds)
	
	Server#show ipv6 dhcp pool
	DHCPv6 pool: IPv6-Provider
	  Address allocation prefix: 2001:DB8:11::/64 valid 172800 preferred 86400 (1 in use, 0 conflicts)
	  DNS server: 2001:DB8::1
	  Domain name: example.com
	  Active clients: 1

Suggested Usage	Stateful auto-configuration of IPv6 address

(4) Evaluation and Comparison:

Pros	Cons
i. Easy to manage. **ii.** Stateful DHCPv6 can control over how addresses are allocated. **iii.** Provide other services, like NTP **iv.** Stateful DHCPv6 sends Dynamic DNS updates from a central point which is more secure and effective than permitting individuals to update the DNS. **v.** Stateful DHCPv6 can block legal users to access to unknown/insecure DHCPv6 clients. **vi.** Stateless DHCPv6 is much easier to deploy.	**i.** Some platforms are limited to or cannot support DHCPv6 yet, such as Android. **ii.** It is relatively hard to configure and deploy compared with SLAAC. **iii.** For stateless DHCPv6, it still cannot control over how addresses are allocated. **iv.** Stateless DHCPv6 requires each client to have a correct TSIG key to keep DNS for the network updated. **v.** Stateless DHCPv6 does not produce accounting logs which is useful for forensic purposes.

(5) Conclusion and Future Trend:

Unlike SLAAC auto-configuration technique that is more likely to be applied to home network, DHCPv6 tends to be used to centralized management of the host sites,such as big enterprises or Service Providers, since IPv6 addresses assignment for network equipment and hosts require to be under manual intervention and centralized management. On top of that, DHCPv6 server providers various services which can assist network administrator to flexibly allocate IPv6 address, such as DHCP-Relay, re-configuration, etc. Hence, DHCPv6 is an irreplaceable solution for IPv6 address assignment.

2.2.5. DNS

(1) Background:RFC3596 [24] and 3901 [25] defines “DNS Extensions to Support IP Version 6” and “DNS IPv6 Operational Guidelines” to guarantee DNS service continuity across a mixture of IPv4/v6 networks.

(2) Introduction: The Service Provider provides all sorts of services, such as WEB, Email, FTP, etc. The prerequisite of these services requires to be endorsed by Domain Name System (DNS) to do conversion of domain-name and IP address. To provide these services to IPv6 hosts, IPv6 DNS must be installed. IPv6 DNS architecture maintains the layer principles of IPv4 DNS, using “Tree Structure” as picture “Diagram 8 -- DNS Tree Structure” shown below. Overall, the work principle of IPv6 DNS is very similar with IPv4 DNS,

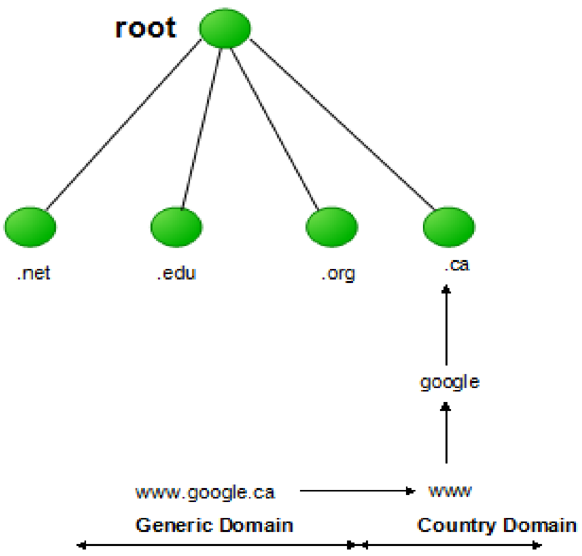


Diagram 9 -- DNS Tree Structure

From this picture we can see that DNS root is unique; the root of the next level is called “the top-level domain” which includes arpa, generic and country domain; the top-level domain of the next level is called “second-level domain”, and by parity of reasoning. Note that each domain is the superior domain’s sub-domain.

DNSv6 contains two methods for Domain Resolution:

1) Forward DNS:

The function of Forward Domain Resolution is to check corresponding IP address by domain-name. IPv6 DNS includes two kinds of resource record in DNS system: “AAAA” and “A6”.

“AAAA”: IPv4 DNS uses “A” to record resources, since the length of IP address is extended from 32 bits to 128 bits, resources record was proposed by RFC1886 and changed from “A” to “AAAA”, but “AAAA” does not support address hierarchy.

“A6”: This was standardized by RFC2874 which supports address hierarchy, aggregation.

2) Reverse DNS:

The function of Reverse Domain Resolution is opposite to Forward DNS, this is to check corresponding Domain-name by IP address. Reverse DNS includes two types of address format: "*Nibble Format*" and "*Bit-string*".

(3) Evaluation and Comparison:

IPv6 DNS can do domain-name resolution for IPv6 address that is irreplaceable for Internet Services. However, the IPv6 DNS has some problems. As report goes, when IPv4 and IPv6 DNS are working together, IPv6 resolution would be slowly.

2.2.6. NAT

NAT-PT

(1) Background: Network Address Translation/Protocol Translation is defined in RFC2766 [27] and has been obsoleted by RFC 4966 .

(2) Introduction:NAT-PT is a mechanism that allows IPv6-node hosts to communicate with IPv4-node hosts. NAT-PT router has an IPv4 address pool, when packets are sent from IPv6 to IPv4 area, the address pool is used to transfer the source of IPv6 addresses. NAT-PT includes three types that are Static, Dynamic and NAPT-PT.Besides, gateway router must support DNS-AGL and FTP-AGL.

The working process of NAT-PT can be displayed by a simple lab as shown below, the objective of this lab is to allow IPv4 host (R1) to access to IPv6 host (R2).

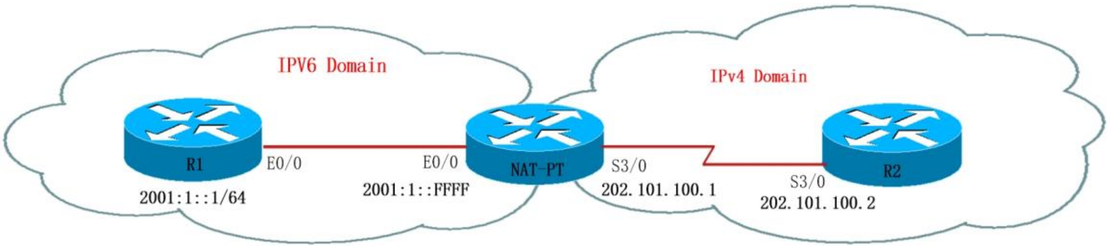


Diagram 10 -- NAT-PT

The lab implementation is on the file of "Enterprise 5_NAT-PT"

<u>Lab Results:</u>

1) When IPv6 side initiates session:

```
R1#ping 2001:2::2
Type escape sequence to abort.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/9/11 ms
```

When IPv6 packets arrive at NAT-PT device, NAT-PT will judge if they should be transferred to IPv4 destination R2 by static NAT mapping -- then NAT device will do address translation from IPv6 to IPv4 by covert IPv6 source address to IPv4 address.

After translation succeeds, then NAT-PT device will save mapping relation tables.

2) When IPv4 side initiates session:

```
R2#ping 202.101.100.100
Type escape sequence to abort.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/9/11 ms
```

When IPv4 packets arrive at NAT-PT device, NAT-PT will judge if they should be transferred to IPv6 network by static NAT mapping configured on NAT-PT router.Then router can transfer destination IPv4 address to IPv6 address by mapping relations. After successful translation, mapping relation tables will be stored on the database on NAT-PT router.

(3) Evaluation and Comparison:

Pros	Cons
i. NAT-PT does not require to upgrade IPv4 and IPv6 nodes that saves time and funds.	**i.** NAT-PT is complex to implement; big overhead processing of protocol and address converting.

(4) Conclusion and future trend:

Actually, as IETF noted that NAT-PT technique has been out of use in the real industry, the main reason is that NAT-PT can consume too much router resources and hardly implement. Only if there is no other communication approaches that can be selected, then NAT-PT would be considered, otherwise, try to avoid using this technology.

NAT64 & DNS64

(1) Background:NAT64 is a mechanism for translating IPv6 packets to IPv4 packets and vice-versa. NAT64 and DNS64 are now in the IETF draft stage, has not yet formed a formal RFC document.

(2) Introduction: In order to solve all kinds of NAT-PT defects, and achieve transformation of network address and protocol between IPv4 and IPv6, IETF redesigned a new solution: NAT64 and DNS64. NAT64 is a stateful transformation technique which generally only supports that IPv6 sites access to IPv4-site resources,but NAT64 as supported by manually configuration of static mapping relation to archive that IPv4 network forwardly can establish connection to access IPv6 network. Also, NAT64 can be working for TCP,UDP and ICMP protocols.

DNS64 always cooperates with NAT64 to work. The function of DNS64 is to check DNS information and combine A record (IPv4 address) from DNS information with AAAA records (IPv6 address), and return combined AAAA records to IPv6 users. Hence, NAT64 also solves the defects of DNS-ALG in NAT-PT [27].

Furthermore, since DNS64 and NAT64 work together, so it is not necessary to make any changes on IPv4 server side or IPv6 client side.

(3) Application scenario:

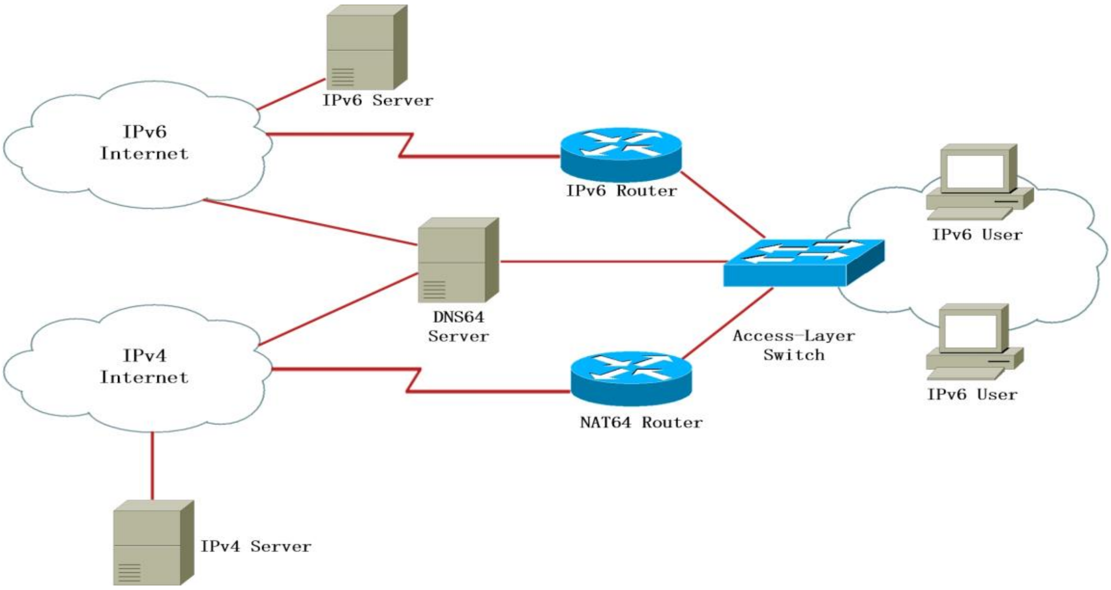


Diagram 11 -- NAT64&DNS64 Example

When IPv6 only users initialize connection to IPv6 website, traffic flow will match IPv6 default route and come to IPv6 router to process. If users are going to access to IPv4 Server, then correlative traffic flow will go through DNS64 Server to form address prefix, Pref64::/n network traffic flow will be forwarded to IPv6 router to process.

Overall, NAT64 & DNS64 can archive IPv4 and IPv6 conversion and allows users to access to IPv4 network resources as well.

(4) Evaluation and Comparison:

Pros	Cons
i. It can solve the problems of traditional NAT-PT.	**i.** At present, it is difficult to support commercial deployment, only suitable for research.

(5) Conclusion and Future Trend:

Although NAT64&DNS64 is able to tackle some NAT problems in IPv6 transition, it does not have the value of commercial deployment, this is because a lot of businesses contain address information required to establish a connection in the data section of the packet, but until now, there is no application that can traverse NAT64. Hence, NAT64, at this stage, is more to demonstrate, and deployment of this scheme needs the accumulation of a certain period of time.

2.2.7. IPsec VPN

(1) Background:IP Security (IPsec) , a framework of open standards from IETF which is a set of protocols for securing IP communications by encrypting and authenticating each IP packet of a communication session.

(2) Introduction:IPsec is comprised of the following sub-protocols: ESP, AH, IPComp and IKE. IPsec. By using IPsec, machines can achieve data confidentiality, data integrity and authentication at the network layer. IPsec offers various security services not only at IPv4 stack, but also for IPv6 protection. Fixed or mobile stations/users can access to Internet via IPsec Site-to-Site or Easy VPN. IPSEC is required to access to the IP source node and applies to both hosts. The basic work process of IPsec VPN is: Send packets-> VPN match-> VPN tunnel negotiation if necessary-> authentication between sites-> establish tunnel-> encrypt data-> re-encapsulate IP header-> packets transmission->packets arrive at the destination of VPN tunnel-> do IP header decapsulation->authenticate integrity->decode->obtain inside information->forward to destination site.

(3) Lab Demo:

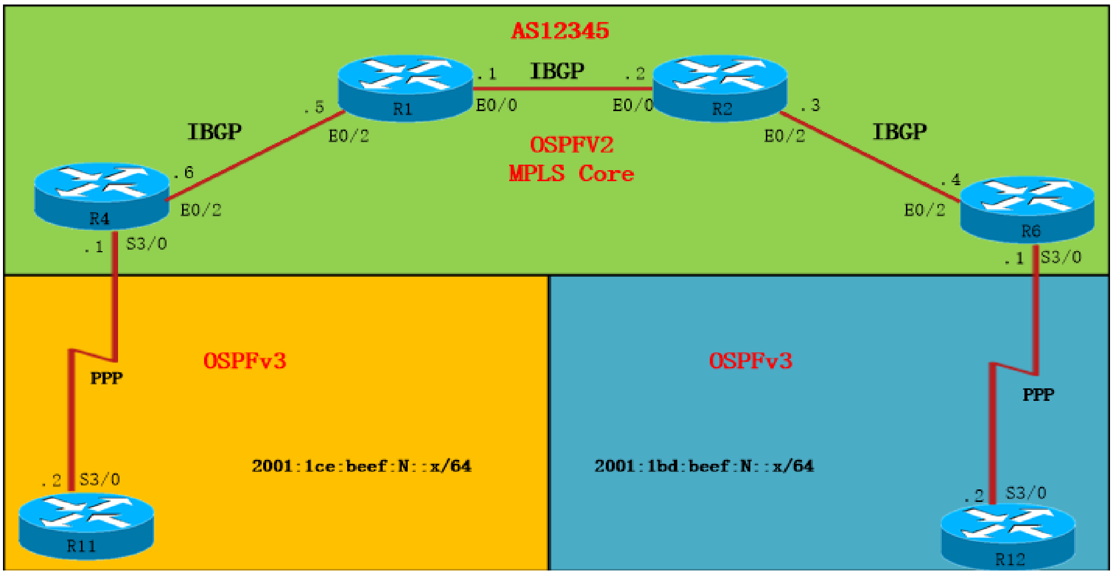


Diagram 12 -- Security VPN Topology

Lab Purpose	**R11 and R12 belong to two different enterprise networks, they should communicate with each other via IPsec VPN**
Lab Implementation	As shown on the file of “Enterprise 6_IPsec VPN for IPv6”
Lab Results	**R11#ping 2001:CC1E:BEEF:12:12:12:12:12 source lo0** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 2001:CC1E:BEEF:12:12:12:12:12, timeout is 2 seconds: Packet sent with a source address of 2001:CC1E:BEEF:11:11:11:11:11

	!!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 21/28/32 ms **R11#show crypto isakmp sa** IPv4 Crypto ISAKMP SA dst src state conn-id status IPv6 Crypto ISAKMP SA dst: 2001:1CE:BEEF:411:A8BB:CCFF:FE00:B00 src: 2001:1BD:BEEF:612:A8BB:CCFF:FE00:C00 state: QM_IDLE conn-id: 1005 status: ACTIVE **R11#show crypto engine connections active** **Crypto Engine Connections** ID Type Algorithm Encrypt Decrypt LastSeqN IP-Address 5 IPsec AES 0 0 0 2001:1CE:BEEF:411:A8BB:CCFF:FE00:B00 6 IPsec AES 0 0 0 2001:1CE:BEEF:411:A8BB:CCFF:FE00:B00 1005 IKE SHA+AES 0 0 0 2001:1CE:BEEF:411:A8BB:CCFF:FE00:B00 **R11#show crypto ipsec sa** outbound esp sas: spi: 0x6E10F27(115412775)
Suggested Usage	Encrypted IPv6 transmission for point-to-point network

(4) Evaluation and Comparison:

Pros	Cons
i. Encrypt IPv6 traffic flow. **ii.**IPsec VPN gateway typically integrates the function of the network firewall. **iii.**IPsec VPN clients support all layer-3 protocols.	**i.** Require to install IPsec VPN clients application program, whereas,not all operating systems support that. **ii.** NAT would block IPsec VPN connectivity. **iii.** Complex configurations.

(5) Conclusion and Future Trend:

As for secret file transferring, IPsec is definitely necessary, in particular for governmental agencies and military industrial enterprises. For instance,the importance of IPsec in IPv6 has grown rapidly as U.S. Department of Defense and federal government have mandates to purchase IPv6-capable systems within a few years [28].

2.2.8. DMVPN

(1) Background: Dynamic Multipoint Virtual Private Network (DMVPN) is a dynamic tunneling form of VPN.

(2) Introduction: The main solution for communications and data transferring between enterprise headquarter and branch sites is based on IPsec Tunnels with hub-and-spoke or full-mesh structures. In reality, the data flow is chiefly distributed to links between centralized and branch sites, nevertheless,only little traffic flow is distributed between branch sites. Since hub-and-spoke network structure requires less point-to-point links, therefore, this is a cost-effective structure module. However, connections between spoke sites do not require extra cost, but in terms of hub-and-spoke module, when spoke site sends traffic to other spokes,extra consumption of centralized resources happens and delay increases especially when data messages are encrypted by IPsec. DMVPN can make spokes to communicate with each other easily. Since GRE header supports all layer-3 protocols, DMVPN applied to IPv6 packets transmission can be accomplished as well.

DMVPN is comprised with four standard sub-protocols: GRE, NHRP, Dynamic Routing Protocols and IPsec.

1) **mGRE:**Support NBMA network

2) **NHRP:**Map logical addresses to physical addresses; only use logical addresses (Tunnel Addresses) that cannot send packets properly so that sites are not able to register.

3) **Dynamic Routing Protocols:**Establish routing neighbors between sites via tunnel’s logical address.

4) **IPsec:**mGRE over IPsec VPN; encrypt mGRE data flow.

Assume that ‘x’ is the source and ‘y’ is destination,and the format of encrypted data packet should be:

IP Header	ESP	GRE	IP Header	IP Payload

Source: x’s public address   Source: x’s private address
Destination: y’s public address   Destination: y’s private address

(3) Lab Demo:

The topology is ‘diagram 12 -- Security VPN Topology ’

Lab Purpose	**R11 is the hub role as the enterprise headquarter, R12 is the spoke as a enterprise branch site; R11 and R12’s loopback0 are simulated as two users, and then can access with each other**
Lab Implementation	As shown on the file of “Enterprise 7_DMVPN”
Lab Results	**R12#ping 2001:CC1E:BEEF:11:11:11:11:11 source lo0** Type escape sequence to abort. 2001:CC1E:BEEF:12:12:12:12:12 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 23/30/41

	ms **Spoke:** **R12#show ipv6 nhrp** 2012::/64 via 2012::1 Tunnel10 created 00:00:15, never expire Type: static, Flags: used NBMA address: 2001:1CE:BEEF:411:A8BB:CCFF:FE00:B00 FE80::A8BB:CCFF:FE00:B00/128 via FE80::A8BB:CCFF:FE00:B00 Tunnel10 created 00:00:04, never expire Type: static, Flags: NBMA address: 2001:1CE:BEEF:411:A8BB:CCFF:FE00:B00 **Hub:** **R11#show ipv6 nhrp multi** I/F NBMA address Tunnel10 2001:1BD:BEEF:6 Flags: dynamic
Suggested Usage	Encrypted IPv6 transmission for point-to-multipoint network

(4) Evaluation and Comparison:

Pros	Cons
i. No need to configure the fixed IPv6 address. **ii.** Much less configurations for central hub. **iii.** No need to change configurations for central hub when adding branch sites. **iv.** Easy the bandwidth pressure of central site.	**i.** DMVPN can produces more protocol overhead, such as adding GRE, IPsec protocols, the grand costs are 80 bits around. **ii.** IPv6 VRFs are not fully supported by IPv6 routing protocols, such as OSPF. **iii.** IPv6 can be only configured on a protected network. **iv.** IKEv1 and NAT66 are not supported. **v.** Hard to traverse NAT device.

(5) Conclusion and Future Trend:

Currently, VPN technology has mostly replaced traditional Frame-relay and ATM as the preferred application in WAN. Whether in the Service Provider or Enterprise, DMVPN technique would account for a large proportion in the market, as this technique is reliable, flexible and efficient.

2.3. Use Case#03 Broadband Customer

2.3.1. Dual Stack

The principles of Dual Stack have been analyzed in Case#01 Service Provider, and its pros and cons have discussed above as well.

For broadband network environment, like home-based customers, Dual Stack has been widely utilized in reality. For one thing, most operating systems support Dual Stack where build-in both IPv4 and IPv6 stack modules, such as Windows, Mac, Linux, Android, etc. As long as broadband network gateway routers offer IPv6 services, then once personal devices turn IPv6 functions on and connect to the Internet, they can automatically obtain IPv6 addresses by SLAAC or DHCPv6 and gain IPv6 services.

2.3.2. Native IPv6

(1) Background: At present, backbone IPv6 transition schemes have tended to be mature which can fulfill the need of present requirements, but evolution of metropolitan area network solution has yet to reach the level of scale deployment. The main problem is about immature user’s access scheme.

(2) Introduction: There are two access schemes to address this problem: Dual Stack and Native IPv6. As discussed early, Dual Stack technique can guarantee to satisfy ample customer services, but it still requires to consume public IPv4 addresses,thereby failing to fundamentally solve the problem of IPv4 address exhaustion. But for Native IPv6 scheme, users can take usage of PPPoEv6/IPoEv6 to obtain IPv6 addresses and relevant information from ***IPv6 BRAS*** and access to IPv6 Internet. Users can use PPPoE to obtain IPv4/IPv6 configuration information, or use IPoEv4/IPoEv6 to obtain and access to Dual Stack network.

(3) Conclusion and Future Trend:

Native IPv6 can solve the problem of IP depletion, but currently, numerous applications cannot run at absolute IPv6 hosts, therefore, this scheme restricts the richness of customer services and unable to adapt to the present IPv6 network transition characteristics at current stage, but it can be utilized in the final phase of network evolution when a large proportion of hosts have supported.

2.3.3. DS-Lite

(1) Background: Dual-Stack Lite experimental test was launched by Comcast in 2008, and adopted by IETF software documents (RFC6333) in 2009 [29].

(2) Introduction: Due to limitations of application-layer software or terminal hardware, it is impossible to upgrading IPv4 to IPv6 network on a large scale in the short period of time, and still not all ***Internet Content Provider (ICP)*** is willing to upgrade to IPv6. Hence, in quite a long time, the main flow in the network will still be “IPv4-IPv4”. Based on the rational view to look upon the gap between IPv4 and IPv6, to archive IPv4 business contingency and smoothly promote IPv6 network deployment, the DS-Lite scheme was proposed, and this concept also conforms to the principle of standard model that aligns the costs and benefits of deploying IPv6 in Service Provider Networks.

The essence of DS-Lite is to deploy IPv4-in-IPv6 Tunnel to accomplish IPv4 data transmission in IPv6 network, and IPv6 data transferring can be completed directly through IPv6 network.

DS-Lite combines IPv4-in-IPv6 tunnel with IPv4 Network Address Translation (NAT) protocol, and co-operate with AFTR (Address Family Translation Router) and Base Bridge Broadband Element (B4) to work out.

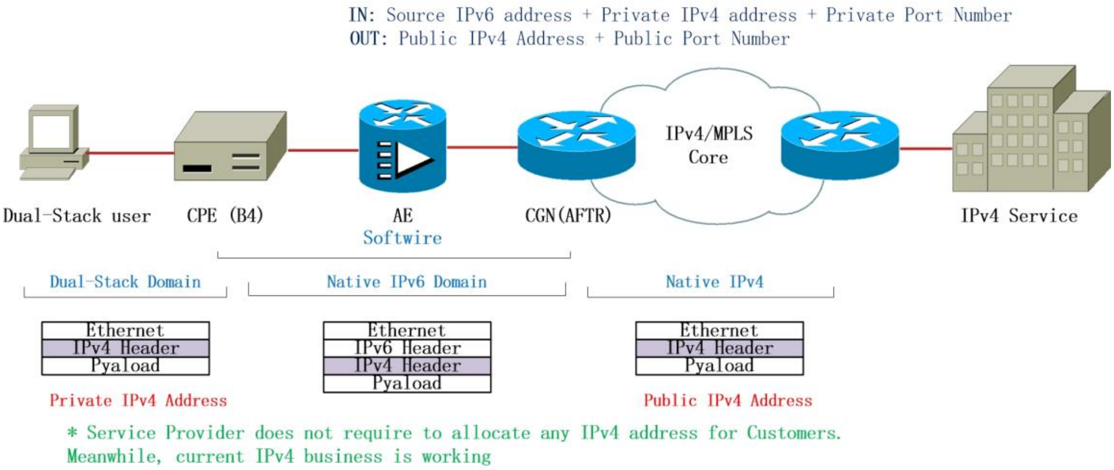


Diagram 13 -- DS-Lite Model Example [30]

Course of work:

1) B4 (Family Gateway) enables DHCPv4 Server to allocate private IPv4 address to inside user.

2) Service Provider advertises location information of AFRT (IPv6 address) by static configuration or DHCPv6.

3) B4 issues connection establishment to AFTR’s IPv4-in-IPv6 tunnel (Softwire), encapsulates IPv4 data flow, the source address is B4 WAN interface’s IPv6 address, the destination should be IPv6 address of AFTR loopback interface, then do de-encapsulation IPv6 packets. Softwire enables NAT which means to translate build-in IPv4 packets (IPv4-IPv4 NAT), and transfer IPv4 messages based on NAT session table.

4) Eventually, CGN device provided by Service Provider can connect to family gateway by single-stack, and Service Provider will not participate in IPv4 address allocation work. When IPv4 packets come, family gateway intercept them and

encapsulate them into inside IPv6 packets. After that, packets are sent to CGN, CGN unpack packets and carry on NAT44 transferring private IPv4 address to public IPv4 address and send them to Service Provider.

(3) Evaluation and Comparison:

Pros	Cons
i. No need to allocate private IPv4 address to users by Service Provider. **ii.** Allows coexistence of IPv4 and IPv6. **iii.** DS-Lite can be ultimate solution for IPv6 transition which helps service provider save money. **iv.** DS-Lite is able to resolve the problem of IPv4 address scarcity issue. **v.** Tunnel Establishment does not need negotiation.	**i.** By means of DS-Lite, IPv4 cannot talk to IPv6 hosts. **ii.** DS-Lite increases the size of traffic because of extra tunnel headers which requires MTU management. **iii.** Need to manage and maintain a mass of NAT tables on AFTR device and upgrade CPE equipment. **iv.** Cannot support end-to-end connection communications.

(4) Conclusion and Future Trend:

Insiders of IPv6 network transition have reached a consensus that DS-Lite can be the ultimate model for IPv6 evolution. If we select DS-Lite as IPv6 transition project, the network will not face up to the problem of “second-time upgrading”, as DS-Lite directly adopts IPv6 Stack, but like 6RD which adopts original IPv4 Stack that has to do second-time upgrading, resulting in costs increased.

Many Service Provides have been researching and deploying DS-Lite. For example, France Telecom and HuaWei are testing DS-Lite and developing relevant hardware equipment together. Also, Comcast is the driving force behind DS Lite.

In conclusion, DS-Lite scheme conforms to the development trend of the future. However, some indicate that DS-Lite is a type of radical policy,because the Service Provider is able to quickly recoup the costs that are invested in IPv6 transition, but the results might be counterproductive.

3. **Case Analysis**

In this part, we will discuss usage of different technologies introduced above in the designed topology which is able to simulate a real network environment [31].

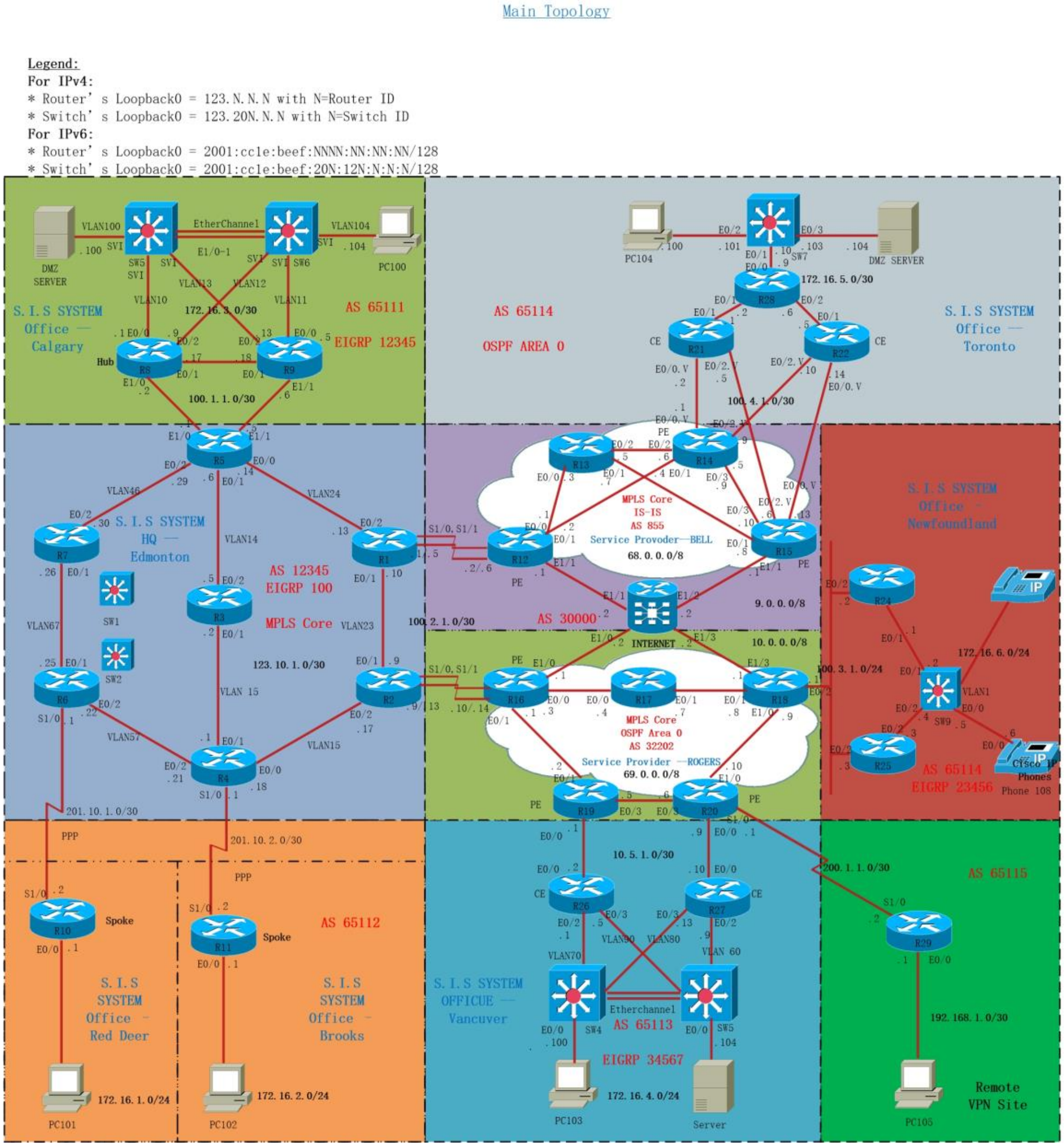


Diagram 14 -- Case Analysis

Brief introduction of the topology:

A big IT company -- S.I.S SYSTEM -- is providing solutions of IP problems for customers. Recently, due to a surge of business expansion, it requires to upgrade devices from IPv4 to IPv6. S.I.S SYSTEM headquarter is located at Edmonton and branch sites are in Calgary, Vancouver, Toronto, Newfoundland, Red Deer, Brooks. Plus, enterprise headquarter also requires to provide services for remote-access users. In order for redundancy, the headquarter applies "Dual-Homed" approach to connect two Service Providers -- Bell and Rogers. Branch sites can communicate with each other via headquarter; in other words, traffic flow must first gather in the place of headquarter, and headquarter will forward traffic flow to specified sites. Besides, Toronto and Vancouver sites are planning to change all devices which will only support IPv6.

Currently, two Service Providers have not completely upgraded to IPv6, and they can only provide IPv4 services for the enterprise now, but the they are also planning to upgrade IPv6 devices. All current protocols and addresses have been marked in the topology.

As being a network designer who is responsible for amongst Service Provider, Enterprise and broadband customers, which technology should be considered?

Consider#01 Service Provider: [32]

(1) Dual Stack: If two Service Providers are deploying Dual Stack, then they can certainly support both IPv4 and IPv6 services. Actually, this is a good solution, since service providers can easily complete deployment only if then enable IPv6 stack on each router. If all Service Provider equipment support dual-stack, then all IPv6 traffic flow can easily traverse Service Provider without affecting IPv4 services. However, if some routers cannot work for IPv6, like R12, R16 those edge routers are disable to support IPv6, then they have be upgraded, since they do not support IPv6 transition tunnel technologies as well, since edge routers have to support IPv6 at lease so that tunnel cannot come into play. If inside routers do not support IPv6 stack, then Service Providers would take a lot of time and money to upgrade device that would not necessarily. Also, if all IPv4 equipment are required to upgrade, original IPv4 service must be adversely impacted, after all, they provide services to most IPv4 customers.Lastly, when IPv6 traffic flow surges to a certain amount, it must scramble for bandwidth with IPv4 and complete with router resources,such as CPU, Cache and Routing tables memory,etc. Consequently, it must be a severe impact on the IPv4 network performance.

(2) GRE/Overlay Tunnel: Obviously, manual tunnels are not suitable for Service Providers as IPv6 transition technologies. Geoff Huston,a Chief Scientist at APNIC, noted that the 90% of IPv6 traffic was native, while 10% was using a tunneling mechanism to carry IPv6 traffic over IPv4 links.The biggest problem is that manual tunnels are hard to maintain. Beyond doubt, there are a lot of customers request IPv6 services, such as 200,000 customers, it is impossible to manually establish and maintain such number of tunnel. If only few customers want to utilize IPv6 manual tunnels to access, then they can be considered. For instance for PC105 that has to utilize GRE over IPsec VPN to access to the Internet, then basic GRE tunnel has to be established. Further, since overhead of GRE header is big, so it could consume limited bandwidth. Eventually, overlay tunnel is not able to support some critical services, like QoS, so it is also not a proper choice for Service Provider.

(3) 6to4 Tunnel:6to4 tunnel can be considered to utilize. First, 6to4 is an automatic tunnel, and network administrator does not need assign tunnel destination address and maintain a lot of tables,since it can automatically calculate route paths. For example, If Toronto and Vancouver sites have changed their devices and could only support IPv6, then in order for IPv6 packets transmission, we need enable R14, R15, R19 and R20 to operate IPv6 stack and establish 6to4 tunnel, like between R14 and R19, while 6to4 tunnel establishment does not require advanced equipment. Plus, since IPv6 traffic does not influence IPv4, so once tunnel is established, then two sites can communicate with each other which is very simple. The only thing is that network analyst has to carefully design 6to4 tunnel addresses. Overall, 6to4 tunnel can be widely used.

(4) 6rd:6rd tunnel can be a rapid option for IPv6 deployment, but it is more expensive than 6to4 tunnel, since it requires ASR Series to support for Ed-Encapsulate IPv6 packets. For instance, if 6rd tunnel is considered to be utilized for connections between Toronto and Vancouver instead of 6to4 tunnel, 6rd tunnel can be established between R19 and R21, and allows clients to use both IPv4 and IPv6. Besides, 6rd controller devices do not require to maintain active flow states, so it can decline the usage of system resources which is better than 6to4 tunnel applied in Service Provider.

(5) Teredo Tunnel: From my perspective, Teredo Tunnel could be a bad idea. First, Teredo tunnel requires Relay, and Teredo address format does not conform to the ideas of IPv6 routing classification. Then, since almost all current hosts have supported IPv6 stack like windows, Mac or Linux systems, so hosts are not necessary to play a role in Teredo client. Hence, compare with 6to4 or 6rd, Teredo tunnel would be a worse solution for this design. For example, if Toronto and Vancouver new equipment has upgraded to support IPv6, Teredo tunnel should be not considered. However, for small branch sites where are in Brooks and Red Deer, and R10 and R11 just enable IPv4 NAT which is unable to support 6to4, in this scenario, Teredo Tunnel can be considered.

(6) 6PE and 6VPE: Assume that all critical IPv6 traffic flow from headquarter and branches should be transmitted via MPLS-VPN configured at edge routers of two Service Providers.

In the first place, consider that Vancouver host PC103 is going to access to the Toronto host PC104 via AS 32202, headquarter and AS 65114 by BGP and MPLS VPN,respectively. How this design can be accomplished in such Dual-Homed environment? Given an advice below, but note that there might be multiple options.

1) Design RD, RT values for assigned traffic source.
2) Put relevant data into designed VRFs.
3) R16 and R19 enable IPv6 stack.
4) R16 and R19 enable 6PE or 6VPE, and test if PC103 can access to the

headquarter.
5) Headquarter routers have gained this message now, then R1 advertise it to the Router R12's VRF in the Service Provider Bell
6) R12 establishes IPv6 MPLS VPN with R14
7) R14 advertise information into AS65114, then PC104 can get PC103's IPv6 address. Eventually, they can communicate with each other.

Pros: To sum up, above approach is a very good solution for connectivity between each sites, only edge routers of Service Provider enable IPv6 MPLS VPN, and process of deployment is relatively easy. Plus, due to VPN technology, the data can be secure.

Cons: However, to archive this process is not simple. First, the enterprise must negotiate with two Service Providers that they would like to serve as the same VRF routes with RD/RT. Second, VPN is not consistent, since traffic flow has to be put into enterprise and reload into another VPN, hence, the process efficiency would be lower. Third, the way of renting two service providers to serve for MPLS-VPN in special lines must be costly.

(7) Multicast-VPNv6: The prerequisite of Multicast-VPNv6 is based on IPv6 VPN which guarantee that Unicast packets can arrive at destinations. However, if Calgary and Newfoundland sites have upgraded to Dual Stack, and Multicast services have to be provided by IPv6 stack. Assume that PC100 is the multicast source,RP is R9 for example, and an user in Newfoundland joins this group, how user can receive multicast messages from Calgary?
1) Service Provider -- ROGERS has to provide Multicast-VPNv6 service between enterprise headquarter and Newfoundland site.
2) When multicast packets arrive at enterprise headquarter, then they are going to look for RP location by Dual Stack which has been deployed in enterprise and Calgary branch.

Consider#02 Enterprise:

(1) Dual Stack: Compare to deploy Dual Stack in Service Provider, Dual Stack is a better way for the enterprise to use Dual Stack inside. Enterprise headquarter should enable IPv6 stack first, since all traffic flow has to run across the headquarter and then is forwarded to other branches. If branches upgrade devices to IPv6 stack first, then packets cannot traverse the headquarter by Dual Stack, the reason is very simple that AS12345 devices do not identify IPv6. Even now branches still send IPv4 messages, then IPv4 packets transmission will not be affected without doubt, since IPv4 and IPv6 are completely isolated.
Also, since the enterprise network environment is different from Service Provider,

enterprise inside devices do not require to carry such a big amount of data, but on the contrary, Service Provider has to assist customers to forward millions of packets at all times, so Dual Stack technique will not give rise low efficiency to routers. Plus, the number of device in enterprise is significantly less than Service Provider, hence enterprise would not need spend too much money and time.

Eventually, Dual Stack technique can fully exploit features of IPv6, therefore, IPv6 services can be guaranteed. And the whole network structure can be flexible and easy to understand. However, Dual Stack technique could not solve the problem of address exhaustion, and enterprise has to maintain some public and private IPv4 addresses.

(2) ISATAP Tunnel:ISATAP, as being a transition technology, is a good choice for enterprise to deploy. For example, the Toronto sites have upgraded to support only IPv6, and Calgary branch and headquarter just support IPv4. Now, PC100 is going to access to Toronto's Server to get files. This time,only if R21 enables R21 as ISATAP router, and PC100 enables IPv6 stack, then PC100 import IPv6 traffic flow into ISATAP tunnel so as to access to Toronto's branch server and get files. This is the cheapest one that can allow IPv4 hosts to access to IPv6 node resources. But this is the approach that can significantly consume equipment's resources.

(3) SLAAC: Generally, SLAAC is not recommended to use in enterprise for IPv6 address allocation. First, it will lead to severe security problem. Consider that once an attacker connects to the switch's interface in the enterprise, and he or she can get an IPv6 address automatically and can be as a legal user working, then messages or packets would be intercepted or captured which would bring about very dangerous results. On top of that, in the enterprise, users' information should be unified managing,and all IPv6 addresses allocation should be unified schemed by engineers,so that only authenticated users have privileges to access to internal servers in the enterprise.

(4) DHCPv6:DHCPv6 is the best choice for enterprise to allocate IPv6 address for users. Actually, in the real industry, the enterprise always applies the way of DHCP server for IPv4 and IPv6 address assignment. For example, in Calgary branch, R8 or R9 can be DHCP servers, and they can maintain both IPv4 and IPv6 DHCP work, and allocate addresses to DHCP Server and PC100. If new users would like to join the network, they have to get permission from network administrator, therefore, address can be orderly distributed without being wasted. Besides, DHCPv6 provides two approaches to allocate address -- stateful and stateless mechanism -- which can be flexible. Also, DHCPv6 server provides Relay function that can allocate IPv6 address for remote users.

However, DHCPv6 is more difficultly to deploy than SLAAC, since network administrator requires to maintain DHCP server. But DHCPv6 is still the first choice for enterprise.

(5) NAT: For this technique, edge routers in Service Provider or Enterprise should support NAT64 or NAT-PT. For example, if Newfoundland staff is going to access to headquarter by NAT. First of all, R25 or R26 should enable NAT64 or NAT-PT, translating IPv6 to IPv4 addresses. Then Service Provider should agree to help to forward these IPv4 packets. When packets arrive at another edge router R16, R16 has to translate IPv4 to IPv6 addresses according to mapping information predefined. After that, headquarter needs to return packets to Newfoundland sites, this process also requires to define NAT policies in two routers. Apparently, NAT is worse than other technologies. First, NAT devices have to maintain a large number of NAT items if there are numerous addresses required to be translated that degrade the performance of routers, Second, the Service Provider requires to design translated addresses for enterprise and agree to assist branch sites to transmit those addresses.

(6) IPsec VPN & DMVPN: These two kinds of Security VPNs has been widely utilized in this topology. In this topology, only enterprise upgrades devices to support IPv6, then VPNs can be working with no need for Service Provider support comparing with MPLS VPN which is much cheaper and in low requirements and conditions.Also, compare with MPLS VPN, IPsec and DMVPN are much more secure which answer needs of requirements for most of customers that data transferring should be encrypted. For example, a R1 can be as a hub, and each branch can have a spoke, like R21 in Toronto, R26 in Vancouver, R24 in Newfoundland and R9 in Calgary. Only if branches can communicate with each other by IPv6 unicast packets, then tunnel can be successfully established. However, the precondition is that each site can intercommunicate by layer-3 IPv6 packets, and then VPNs can be implemented based on that.

Consider#3 Broadband Customers:

One enterprise staff is on vacation and using PC105 in AS 65115. He wants to communicate with other staff in order to deal with some work. In this scenario, in which technology is better to use?

(1) Dual Stack: Dual Stack can be applied to broadband customers. R29 enables IPv6 stack, and when PC105 plugs into gateway router R29, then PC105 will get an IPv6 address by DHCPv6 or SLAAC, then by means of gateway, IPv6 packets can be sent outside. Of course, Dual Stack is suitable for both wired and wireless customers.

(2) Native IPv6: Native IPv6 can be used here, since most users access to Internet through the way of dial-up by PPPoE, especially for home network. PC105 does not require to provide IPv4 address, since it uses only-IPv6 stack. However, PC105 could not use IPv4 stack at this time which prohibit many IPv4 services. Hence, this approach is not recommended.

(3) DS-Lite:DS-Lite combines the benefits of both Dual Stack and Native IPv6; on the one hand, DS-Lite does not need request Service Provider to allocate addresses to users, on the other hand, DS-Lite allows coexistence of IPv4 and IPv6 stack. DS-Lite should be the best approach for broadband customers to access to the Internet.

4. Conclusion

Technique	Dual Stack	Tunnel	NAT
Core idea	• Run IPv4 and IPv6	• One protocol encapsulates another protocol	• Translate a protocol to another protocol
Application	• Coexistence IPv4 with IPv6	• IPv6 hosts/network communications	• Intercommunication between IPv4 and IPv6 nodes
Pros	• High processing efficiency • Network plan is simple • Can fully exploit features of IPv6 • It is easy to understand • No information loss	• It is Easy to configure and deploy • Can fully take pros of current network resources • No information loss	• Only need configure at the edge routers of IPv4 or IPv6 domains • No need to upgrade existing IPv4 and IPv6 devices • Can solve the problem of address exhaustion
Cons	• Take up more resources • Complicated operation and maintenance • Cannot archive intercommunication between IPv4 and IPv6 nodes • Cannot solve the problem of address shortage • Have to maintain a lot of protocols and data • Take more funds and time	• Low efficiency • Cannot archive intercommunication between IPv4 and IPv6 nodes • Support less services • Low scalability • Not adapt to deploy on large scale • Be not compatible with NAT equipment.	• Require to revise DNS server • High protocol and IP overhead • Lead to information loss • Some certain flow cannot traverse NAT device, such as encrypted flow • Some protocols require ALG when being translated which cause a large performance cost

5. References:

[1] John Brzozowski, "*COMCAST REACHES KEY MILESTONE IN LAUNCH OF IPV6 BROADBAND NETWORK*". http://corporate.comcast.com/comcast-voices/comcast-reaches-key-milestone-in-launch-of-ipv6-broadband-network

[2] Tao Wang, "*One of the major defects, breaking the principle of hitless network upgrade* ", blog, 19 Dec. 2007. http://blog.sina.com.cn/s/blog_4fc5407c010085dg.html

[3] Abdullah AI-Shaeya, "*(IPv4 VS IPv6) Header*", ICS343 (KFUPM).

[4] S. Bradner, *The Recommendation for the IP Next Generation Protocol*, IETF RFC 1752, January 1995. https://tools.ietf.org/rfc/rfc1752.txt

[5] Jiping,Zhang, vice-general manager of China Telecom, *Global IPv6&Next Generation Internet Summit 2012, Beijing*.

[6] D. Farinacci and P. Traina, *Generic Routing Encapsulation (GRE)*, IETF RFC 1701 and 1702, October 1994. https://tools.ietf.org/rfc/rfc1701.txt https://tools.ietf.org/rfc/rfc1702.txt

[7] B. Carpenter and K. Moore, *Connection of IPv6 Domains via IPv4 Clouds*, IETF RFC 3056, February 2001. https://www.ietf.org/rfc/rfc3056.txt

[8] B. Carpenter, Advisory Guidelines for 6to4 Deployment, IETF RFC 6343, August 2011. http://tools.ietf.org/html/rfc6343

[9] R. Despres, IPv6 Rapid Deployment on IPv4 Infrastructures (6rd), January 2010. https://tools.ietf.org/html/rfc5569

[10] Google, A10 Networks Authorized Reseller, *IPv6 Rapid Deployment (6rd) for IPv6 Content Access*. http://www.loadbalanceworks.com/ipv6-rapid-deployment.asp

[11] Google, "Wikileaks," http://en.wikipedia.org/wiki/IPv6_rapid_deployment

[12] Lawrence Hughes, *ISATAP - Intra-Site Automatic Tunnel Addressing Protocol*. http://www.sixscape.com/joomla/sixscape/index.php/

[13] C. Huitema, Teredo: *Tunneling IPv6 over UDP through Network Address Translations (NATs)*, IETF RFC 4380. http://www.ietf.org/rfc/rfc4380.txt

[14] J. De Clercq, D. Ooms, S. Prevost and F. Le Faucheur, *Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers(6PE)*, IETF RFC 4798. https://tools.ietf.org/rfc/rfc4798.txt

[15] J. De Clercq, D. Ooms, M. Carugi and F. Le Faucheur, *BGP-MPLS IP Virtual Private Network(VPN) Extension for IPv6 VPN*, IETF RFC 4659. https://tools.ietf.org/rfc/rfc4659.txt

[16] Cisco Systems, Inc. *Cisco ASR 901 Series Aggregation Services Router Software Configuration Guide*, Page 700.

[17] E. Rosen, And R. Aggarwal, *Multicast in MPLS/BGP IP VPNs*, IETF RFC 6513. https://tools.ietf.org/rfc/rfc6513.txt

[18] E. Rosen, IJ. Wijnands, IPv6 Multicast VPN(MVPN) Support Using PIM Control Plane and Selective Provider Multicast Service Interface(S-PMSI), IETF RFC6516. https://tools.ietf.org/rfc/rfc6516.txt

[19] Cisco Systems, Inc. *IP Multicast: MVPN Configuration Guide, Cisco IOS Release 15MT*, Page 21.

[20] F. Templin, T. Gleeson and D. Thaler, *Intra-Site Automatic Tunnel Addressing Protocol(ISATAP)*, IETF RFC5214. https://tools.ietf.org/rfc/rfc5214.txt

[21] Se-Joon Yoon, Jong-Tak Park, Dae-In Choi and Hyun K. Kahng, "*Performance Comparison of 6to4, 6RD, and ISATAP Tunnelling Methods on Real Testbeds*", (IJIDCS) International Journal on Internet and Distributed Computing Systems. Vol: 2 No: 2, 2012.

[22] S. Thomson, T. Narten and T. Jinmei, *IPv6 Stateless Address Autoconfiguration*, IETF RFC 4862. https://tools.ietf.org/rfc/rfc4862.txt

[23] R. Droms, J. Bound, B. Volz, T, Lemon, C. Perkins and M. Carney, *Dynamic Host Configuration Protocol for IPv6(DHCPv6)*, IETF RFC 3315. https://www.ietf.org/rfc/rfc3315.txt

[24] S. Thomson, C. Huitema, V. Ksinant and M. Souissi, *DNS Extensions to Support IP Version 6*, IETF RFC 3596. https://www.ietf.org/rfc/rfc3596.txt

[25] A. Durand and J. Ihren, *DNS IPv6 Transport Operational Guidelines*, IETF RFC 3901. https://tools.ietf.org/rfc/rfc3901.txt

[26] G. Tsirtsis and P. Srisuresh, *Network Address Translation - Protocol Translation(NAT-PT)*, IETF RFC 2766. https://www.ietf.org/rfc/rfc2766.txt

[27] Cisco Systems, Inc. NAT64 Technology: *Connecting IPv6 and IPv4 Networks*, April 2012. http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html

[28] Kaushik Das, *IPSec&IPv6 - Securing the NextGen Internet*. http://ipv6.com/articles/security/IPsec.htm

[29] A. Durand, R. Droms, J. Woodyatt and Y. Lee, *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*, IETF RFC 6333. https://www.ietf.org/rfc/rfc6333.txt

[30] Chunlin Liu, *DS-Lite pushes to the evaluation of IPv6 network*, May 20, 2011. http://www.zte.com.cn/cndata/magazine/zte_technologies/2011/5_11/magazine/201105/t20110520_235209.html

[31] Ciprian Popoviciu, <*Eric Levy-Abegnoli and Patrick Grossetete, Deploying IPv6 Networks*>, ciscopress.com.

[32] Carolyn Duffy Marsan, *IPv6 tunnel basics, Mechanisms aid IPv4 to IPv6 transition for network operators.* http://www.networkworld.com/article/2208835/lan-wan/ipv6-tunnel-basics.html