Migration from IPV4 to IPV6 in Republic of Yemen

Ali M. Alsaih[1,*]
Ghada M. Al-Asadi[1,*]
Ahlam Al-Muafa[1]
Thuraia Al-Washaly[1]
Aisha Althorasi[1]

[1] Communication and Electronics Engineering, Faculty of Engineering, Sana'a University, Sana'a, Yemen.

* Corresponding author: alimanea@gmail.com, g.alasadi@eng-su.edu.ye

https://doi.org/10.20428/JST.24.2.1

Migration from IPV4 to IPV6 in Republic of Yemen

Abstract:

Due to the great features IPv6 has over IPv4, many countries have adopted IPv6 in their networks, and many websites are planning to complete their migration to IPv6. In Yemen, the process of deploying IPv6 is still very slow, and if it continued in the same pace, in few years Internet users in Yemen won't be able to reach some websites or even communicate with IPv6-only users in other countries. In this paper, not only did we investigate the details of the IPv6 transition process in Yemen, but we also suggested, implemented and tested solutions to one of the most important problems that prevent Yemen's ISP from deploying IPv6 in their network, which is the fact that many users still have IPv4-only devices and can't change them or upgrade their software to support IPv6. In our work, we used a combination of software and hardware to implement IPv6 migration techniques, and focused on many important theoretical concepts such as IP addresses planning and OSPF routing in order to make sure that these solutions are applicable in reality.

Keywords: IPv6 deployment, dual-stack, NAT-PT, tunneling, ISP.

https://doi.org/10.20428/JST.24.2.1

الإنتقال من IPV4 إلى IPV6 في الجمهورية اليمنية

الملخص:

نظـرًا للميزات الرائعة التي يتمتع بهـا الإصدار IPv6 على الإصدار IPv4، اعتمدت العديد من الدول الإصدار IPv6 في شبكاتهـا، وتخطـط العديـد من مواقع الويـب لإكمال انتقالهـا إلى الإصـدار IPv6 في اليمن، لا تـزال عمليـة الانتقـال الى IPv6 بطيئـة للغايـة، وإذا استمرت بنفس الوتـيرة، فلن يتمكن مستخدمـو الإنترنت في اليمن في بضع سنوات من الوصول إلى بعض مواقع الويب أو حتى التواصل مع مستخدمي IPv6 فقط في بلدان أخرى. في هذه الورقة، لم نتحقق فقط من تفاصيل عملية انتقال IPv6 في اليمن، ولكننا اقترحنا أيضًا ونفذنا واختبرنـا حلـولًا لإحدى أهم المشـكلات التي تمنع مزود خدمـة الإنترنت في اليمن من نشـر IPv6 في شبكتهم، وهـذا هـو الواقع الذي لا يزال لدى العديد من المستخدمين لأجهـزة IPv4 فقط ولا يمكنهم تغييرها أو تـرقية برامجهم لدعم IPv6. في عملنا، استخدمنا مجموعة من البرامج والأجهزة لتنفيذ تقنيات الانتقال الى IPv6، وركزنـا علـى العديد من المفاهيـم النظرية الهامة مثل تخطيـط عنـاوين IP والتوجيـه باستخدام بـروتوكول OSPF للتأكد من أن هذه الحلول قابلة للتطبيق في الواقع.

الكلمات الرئيسية : الانتقال الى IPv6، مكدس مزدوج، NAT-PT، نفق، مزود خدمة الإنترنت.

1. Introduction:

In the past few years, the number of Internet users in the world has rapidly increased because of the significant technological evolution in handheld devices such as smart cell phones and tablets, which allow getting an access to the Internet at any time and any place. IPv4 won't be able to handle such growth because the number of IPv4 addresses is nearly exhausted [2]. Therefore, it's only a matter of time before Migration to IPv6 becomes mandatory to every ISP even to those who once thought that IPv4 is still adequate. However, a seamless migration to IPv6 can't happen over a night. It requires planning, collecting information, testing, analyzing and many calculations [1,5,7]. The ISP of Yemen, Yemen Net, has been working on the IPv6 migration project since 2011. Until now, they have not deployed IPv6 in their network and they still have a lot of steps to go through. This paper first reviews the IPv6 deployment different strategies, then investigates the current progress Yemen's ISP has made toward an IPv6 deployment, and finally provides the details and results of an implementation of IPv6 deployment techniques that we've made to help pushing the IPv6 transition process in Yemen one step forward [2,5,7,9,10].

2. Migration Technologies Overview:

IPv6 Deployment occurs gradually. Initially, IPv6 is to be deployed within isolated islands with interconnectivity among the islands achieved by the existing IPv4 infrastructure [1- 3]. IPv4 cannot communicate directly with IPv6 due to the huge difference between them. Therefore, the Internet Engineering Task Force (IETF) has defined a number of specific techniques to assist in transitioning to IPv6. These technologies, shown in Fig.1, are the dual-stack, tunneling, and translation.

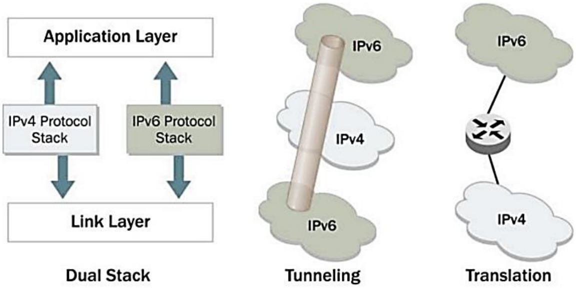

Figure 1: IPv6 deployment techniques

https://doi.org/10.20428/JST.24.2.1

A. Dual-Stack Approach:

The dual-stack approach, shown in Fig.2 is based on implementing both IPv4 and IPv6 protocol stacks on devices requiring access to both network-layer technologies, including routers, any other infrastructure devices and end-user devices. Such devices would be configured with both IPv4 and IPv6 addresses, and they may obtain these addresses via methods defined for the respective protocols as enabled by administrators [1]. This involves enabling two TCP/IP protocol stacks on the WAN core routers, then perimeter routers and firewalls, then the server-farm routers and finally the desktop access routers[9]. Ideally, only the network layer would be dualized, using a common application, transport and data link layer. The dual-stack is the better technique to migrate in IPv6 network in compare to tunneling and NAT techniques as proposed by [2] and [6].

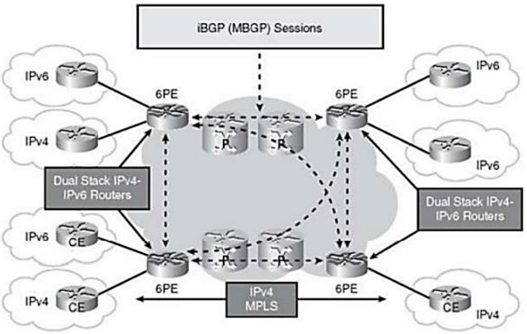

Figure 2: Dual-stack approach

B.Tunneling Approach:

The main usage of tunnelling is to enable a non-IPv6 device to communicate with other devices in IPv6 network. For example, a packet may be passed through an IPv6 network and suddenly reached one of the devices in its rout which was not upgraded to work with IPv6 packet. In this case the tunnelling is used [10]. Tunneling, as shown in Fig.3, is an encapsulation of an IPv6 packet within an IPv4 packet for transmission over an IPv4 network. In general, tunneling of IPv6 packets through an IPv4 network entails prefixing each IPv6 packet with an IPv4 header. This enables the tunneled packet to be routed over an IPv4 routing infrastructure. The entry node of the tunnel, a router or a host, performs the encapsulation. The exit node or tunnel endpoint performs decapsulation to strip off the IPv4 header and route the packet as appropriate to the ultimate destination [1]. Tunneling can be either manual or automatic. An automatic tunnel does not require pre-configuration; it is created based on information contained in the IPv6 packet.

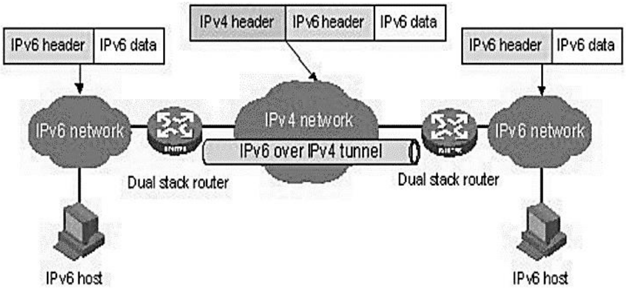

Figure 3: Tunneling approach

C.Translation Approach:

Translation is a technique that allows direct communication between hosts that use different network protocols using a protocol translator between IPv6 and IPv4. Dual- Stack networks (networks that have IPv4 and IPv6) can have some IPv6-only hosts configured to take advantage of the IPv6 autoconfiguration, global addressing, and simpler management features, and these hosts can use NAT-PT (Network Address Translation - Port Translation) to communicate with existing IPv4-only networks in the same organization. One of the benefits of NAT-PT is that no changes are required to existing hosts if NAT-PT is configured, because all NAT-PT configurations are performed at the NAT-PT device. This is shown in Fig.4.

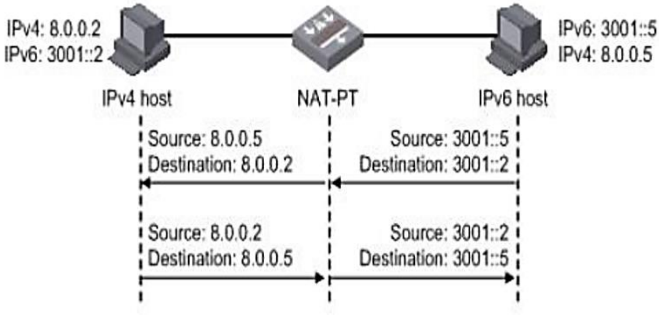

Figure 4: NAT-PT deployment example

https://doi.org/10.20428/JST.24.2.1

3. Yemen's ISP Network overview:

Yemen National Telecommunications Network is used in Yemen as a national backbone network to provide both voice and data communication services. Yemen Net is the main ISP in Yemen. Their network consists of a number of routers and switches including Juniper, Cisco, ZTE, and Huawei, distributed over the whole country, transmission lines, mainly fiber optics links are used, in some areas microwave links are used instead. The core of the network uses Multiprotocol Label Switching (MPLS). The network contains other essential components such as Broadband Remote Access Server (BRA) which routes traffic to and from broadband remote access devices, digital subscriber line access multiplexers (DSLAMs) which are used as access, Authentication, authorization, and accounting (AAA) server, and Domain Name System (DNS). The whole network is connected to the global Internet through only one gateway located in the capital city Sana'a. Fig.5 shows a diagram of the general components of Yemen Net's network.

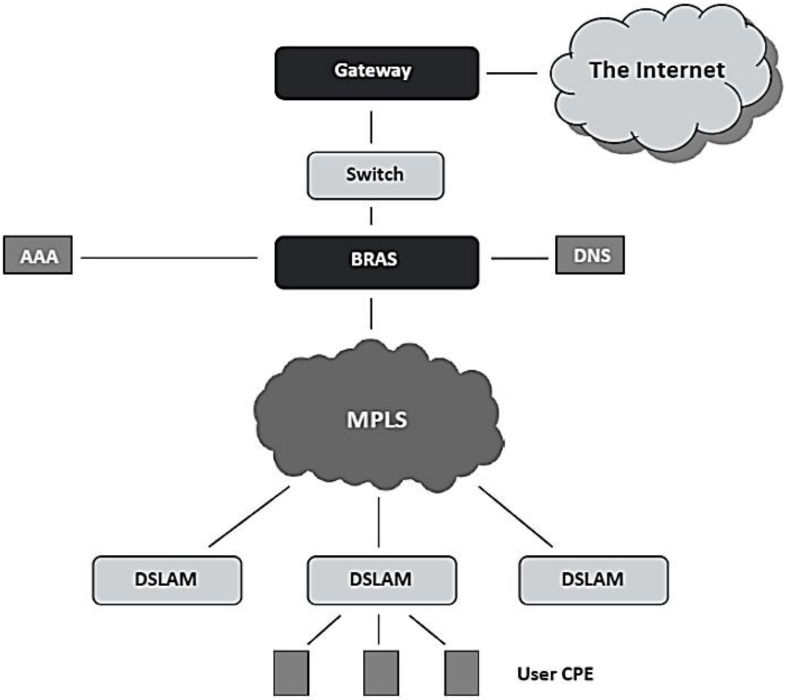

Figure 5: Yemen Net network general diagram

https://doi.org/10.20428/JST.24.2.1

4. Preparation for the transition from IPv4 to IPv6 in Yemen:

Yemen ISP (Yemen Net) is still using IPv4 and has not implemented IPv6 yet. In addition to all the advantages of IPv6 over IPv4, there is a great need for the transition from IPv4 to IPv6 in Yemen due to the following reasons:

1. The number of IPv4 addresses allocated by Yemen’s ISP is very small, and these IP addresses are now completely exhausted.
2. As a solution to the addresses depletion problem, network address translation (NAT) has been used by Yemen net. However, this technique turned to be a problem itself. It caused a great pressure on routers, and if a router goes out of service a very large number of users will lose connection at the same time.

A. Planning:

In 2011 Yemen Net started discussing the need for migrating from IPv4 to IPv6, and in 2012 they made a plan, shown in Fig.6, to conclude the most essential steps to be taken in order for them to be completely ready for the transition.

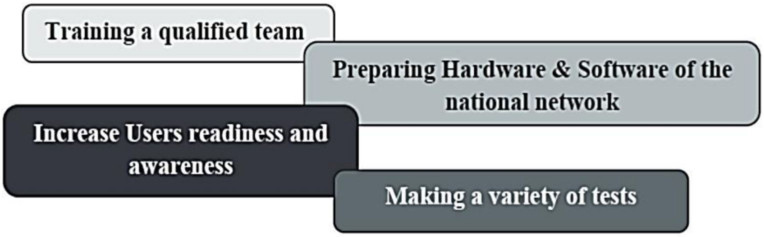
Training a qualified team
Preparing Hardware & Software of the national network
Increase Users readiness and awareness
Making a variety of tests

Figure 6: Yemen Net IPv4/IPv6 transition plan

B. Challenges:

Political and economic situation of Yemen: The conflict between different parties and groups in addition to the resent war on Yemen, have made it extremely difficult to stick to any development plans.

Absence of foreign experts: Experts who provide training and consultation to the Yemeni team had to leave the country because it is not safe anymore for them to stay.

Addressing: Yemeni engineers are still facing IPv6 addressing issues due to the complexity of the network and the lack of experience.

https://doi.org/10.20428/JST.24.2.1

Security: Before moving to IPv6, the national network still needs more work to be fully protected from serious threats such as denial-of-service attack (DOSattack) and Rogue IPv6 Routers [6].

Some end users' devices don't support IPv6.

C. Progress:

1. According to Yemen Net team.
2. The core network hardware and software now fully support both IPv4 and IPv6.
3. About 60% of users are ready for the IPv4/IPv6 transition.
4. An IPv6 lap is almost complete.
5. (2A02:2718::/29) IPv6 addresses range is allocated for Yemen.
6. An IPv6 DNS server (2a02:2718:4::33) is now ready.
7. The First Yemeni IPv6 website has been established recently (Yemen.net.ye).

Fig.7 shows the overall IPv6 and IPv4 support in Yemen.

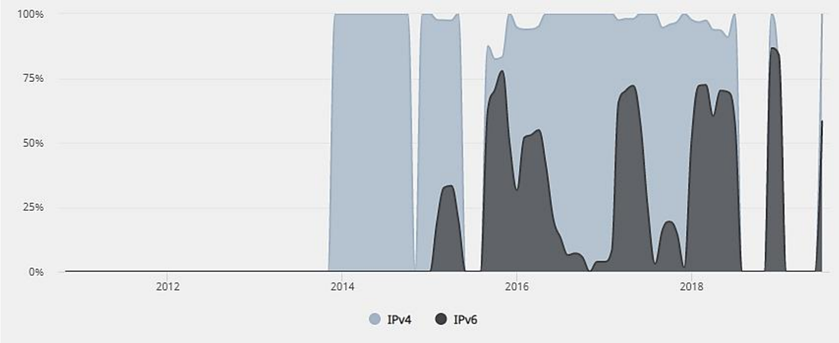

Figure 7: IPv6 and IPv4 support in Yemen [11]

5. Implementation of Possible Solutions:

As previously discussed, Yemen ISP's core network is completely ready for transition to the next generation protocol. However, one of the problems preventing transmission is the fact that some end users' devises (Servers, Routers, or PCs) still support IPv4 only which makes it not possible for the Yemeni ISP to use the dual-stack technique alone. Henceforth, we tried in this paper to introduce temporary methods to be used by users to enable them to communicate normally using Yemen net dual-stack network, until they change their devices to be able to support IPv6.

5.1 Network Design:

Our design and implementation is divided into two parts to overcome two situations that usually prevent a smooth IPv6 transition process (when end users have IPv4-only middle devices or when they have IPv4-only terminal devices). We designed a network that closely represents our national network in Yemen assuming two possible scenarios:

a. We assumed that an IPv6-only user wants to reach an IPv6-only web server with an IPv4-only multi-layer switch positioned in between using tunneling, as shown in Fig.8.

b. We assumed that an IPv6-only user needs to reach an IPv4-only DNS server (secondary DNS server) or vice versa using NAT-PT, as shown in Fig.9.

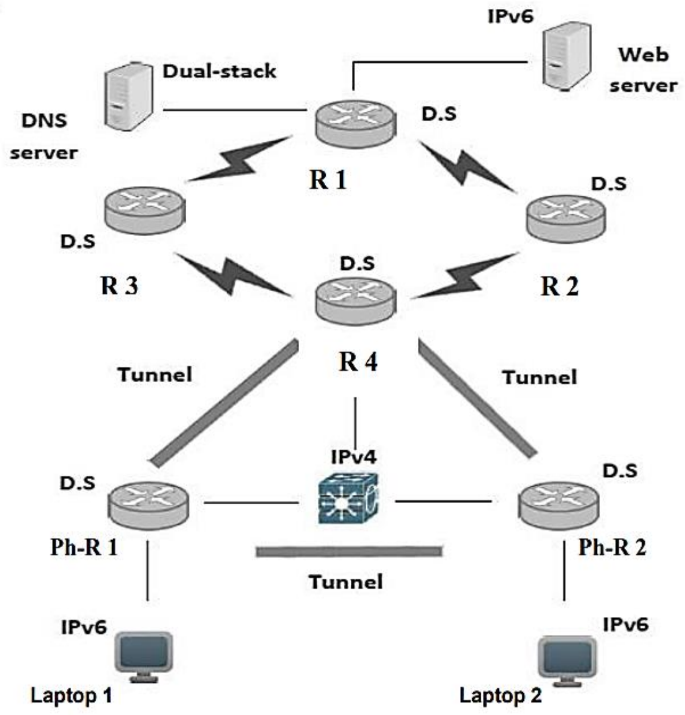

Figure 8: Network 1 topology

https://doi.org/10.20428/JST.24.2.1

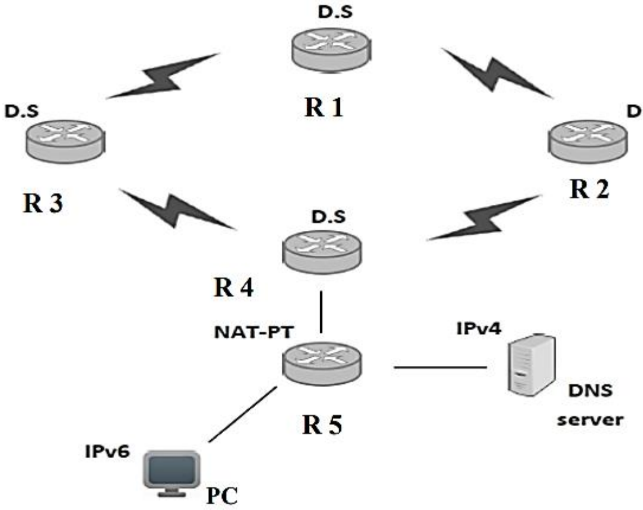

Figure 9: Network 2 topology

5.2 Implementation:

To build both networks we used:

Hardware (physical equipment):

- Cisco Router 1841.
- Cisco Router 2811.
- Cisco Multi-layer Switch.
- Four laptops.
- Ethernet connection wires.
- Serial connection wire.

Software:

- Packet tracer version 6.2 (IP planning and tests). GNS3 version 1.4.
- Oracle virtual box.
- Windows server 2008.
- Router IOS (c1841-adventerprisek9-mz.124-24.t6) and (c2800nm-adventerprisek9-mz.124-11.t1).
- HyperTerminal (real routers configuration).
- Cisco TFTP (real routers IOS upgrading).

https://doi.org/10.20428/JST.24.2.1

- Secure CRT (Terminal emulator).
- Wireshark version 1.12.

Fig.10 shows the hardware we used in our implementation.

Figure 10: Our laboratory

5.3 IP Addresses Planning:

Table 1: Network 1 IPv4 addressing scheme

Device	Interface	IPv4 address
R1	Fast Ethernet 1/0	-
	Fast Ethernet 2/0	172.16.1.1/24
	Serial 0/2	10.10.10.1/30
	Serial 0/3	10.10.10.14/30
R2	Serial 0/1	10.10.10.2/30
	Serial 0/3	10.10.10.5/30
R4	Fast Ethernet 1/0	192.168.20.1/24
	Serial 0/2	10.10.10.6/30
	Serial 0/3	10.10.10.9/30
R3	Serial 0/1	10.10.10.13/30
	Serial 3/0	10.10.10.10/30
Laptop 1	-	-
Laptop 2	-	-
Multilayer switch	Fast Ethernet 0/0	192.168.20.2/24
	Fast Ethernet 0/1	192.168.21.1/24
	Fast Ethernet 0/2	192.168.22.1/24
Ph-R 1	Fast Ethernet 0/1	192.168.21.2/24
	Fast Ethernet 0/0	192.168.24.1/24
Ph-R2	Fast Ethernet 0/1	192.168.22.3/24
	Fast Ethernet 0/0	192.168.23.3/24
Web server	-	-
DNS server	-	172.16.1.2/24

https://doi.org/10.20428/JST.24.2.1

Table 2: Network 2 IPv4 addressing scheme

Device	Interface	IPv4 address	Device	Interface	IPv4 address
R1	Serial 0/2	10.10.10.1/30	R3	Serial 0/1	10.10.10.13/30
	Serial 0/3	10.10.10.14/30		Serial 0/3	10.10.10.10/30
R2	Serial 0/1	10.10.10.2/30	R5	Fast Ethernet 0/1	192.168.20.2/24
	Serial 0/3	10.10.10.5/30		Fast Ethernet 0/2	-
R4	Fast Ethernet 0/0	192.168.20.1/24		Fast Ethernet 0/3	172.16.1.1/24
	Serial 0/2	10.10.10.6/30	PC	-	-
	Serial 0/3	10.10.10.9/30	DNS server	-	172.16.1.2/24

Table 3: Network 1 IPv6 addressing scheme

Device	Interface	IPv4 address
R1	Fast Ethernet 1/0	2a03:2880:2130:cf05::1/64
	Fast Ethernet 2/0	2A02:2718:4:25::1/64
	Serial 0/2	2A02:2718:4:1::1/64
	Serial 0/3	2A02:2718:4:12::14/64
R2	Serial 0/1	2A02:2718:4:1::2/64
	Serial 0/3	2A02:2718:4:4::5/64
R4	Fast Ethernet 1/0	-
	Serial 0/2	2A02:2718:4:4::6/64
	Serial 0/3	2A02:2718:4:8::9/64
R3	Serial 0/1	2A02:2718:4:12::13/64
	Serial 3/0	2A02:2718:4:8::10/64
Laptop 1	-	2A02:2718:4:24::2/64
Laptop 2	-	2A02:2718:4:23::2/64
Multilayer switch	Fast Ethernet 0/0	-
	Fast Ethernet 0/1	-
	Fast Ethernet 0/2	-
Ph-R1	Fast Ethernet 0/1	-
	Fast Ethernet 0/0	2A02:2718:4:24::1/64
Ph-R2	Fast Ethernet 0/1	-
	Fast Ethernet 0/0	2A02:2718:4:23::3/64

Table 2: Continued

Device	Interface	IPv4 address
Web server	-	2a03:2880:2130:cf05::2/64
DNS server	-	2A02:2718:4:25::2/64

Table 4: Network 2 IPv6 addressing scheme

Device	Interface	IPv4 address	Device	Interface	IPv4 address
R1	Serial 0/2	2a02:2718:4:1::1/64	R3	Serial 0/2	2a02:2718:4:12::14/64
	Serial 0/3	2a02:2718:4:12::14/64		Serial 0/3	2a02:2718:4:8::10/64
R2	Serial 0/2	2a02:2718:4:1::2/64	R5	Fast Ethernet 0/0	2a02:2718:4:16::2/64
	Serial 0/3	2a02:2718:4:4::5/64		Fast Ethernet 0/1	2a02:2718:4:20::2/64
R4	Fast Ethernet 0/0	2a02:2718:4:16::1/64		Fast Ethernet 0/2	-
	Serial 0/2	2a02:2718:4:4::6/64	PC	-	2a02:2718:4:20::2/64
	Serial 0/3	2a02:2718:4:8::9/64	DNS server	-	-

5.4 Routing Protocol:

The routing protocol used in our networks is OSPF, because it allows the use of both IPv4 and IPv6. In addition, it has fast convergence, it is loop free and secure, and it takes very low bandwidth. Unlike EIGPR, OSPF is open standard. Also unlike IS-IS, it supports point-to-multipoint links and OSPF routers can belong to multiple areas [8]

5.5 Configuration overview:

Fig.11 shows the simulated part of network 1. There are four routers R1, R2, R3, and R4. Routers configuration included adding IP addresses to each interface, activating OSPF routing protocol, and adding the tunnel commands in R4[9] . We, also, used the.

Virtual box software to create and configure two Windows Servers 2008. One of which is a web server, while the other is a DNS server.

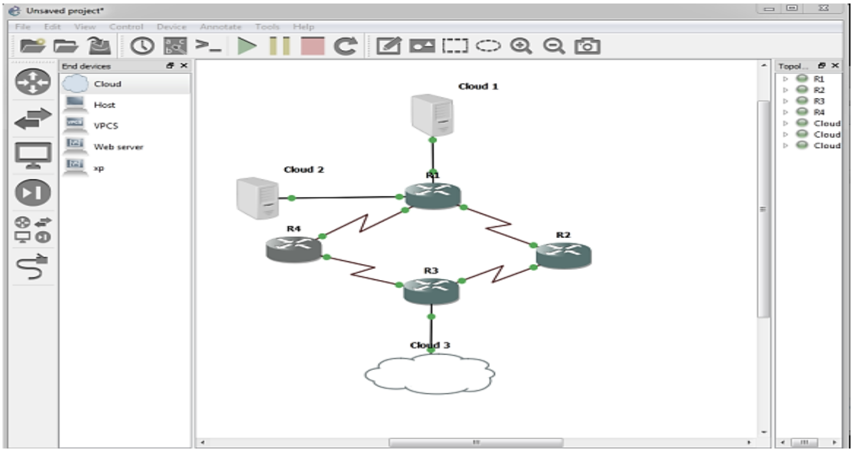

Figure 11: Network 1 GNS3 part

In network 2, shown in Fig.12, routers R1, R2, R3, and R4 have exactly the same configuration as in network 1 (except the tunnel configuration) because they represent the ISP network part. R5 configuration includes the NAT-PT commands.

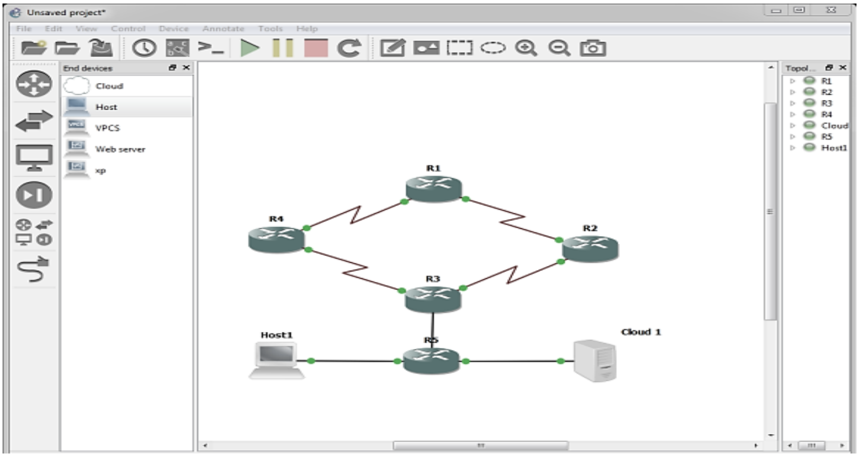

Figure 12: Network 2 in GNS

Before configuring any of the physical devises, we used a serial connection to connect each physical device to a PC with (HyperTerminal) software installed in it is order to add (telnet) commands to each of them. Both physical routers configuration included adding IP addresses to each interface, activating OSPF, and adding the manual tunneling commands. The switch configuration is the same except that its interfaces have IPv4 only addresses and no tunneling.

6. Analysis and Results:

In order to analyze the two networks general performance, we measured the delay and throughput of each network using Wireshark simulator.

A. Delay:

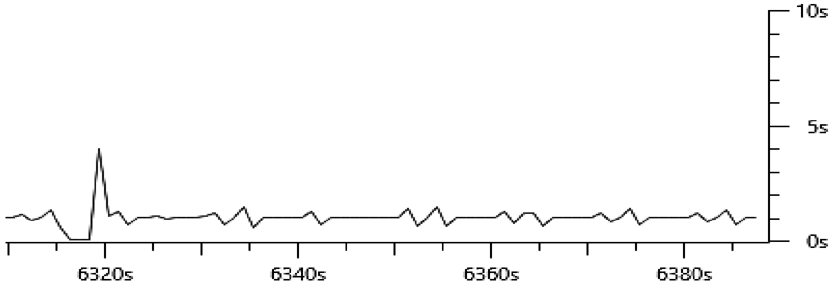

Figure 13: Manual tunnel ping delay analysis

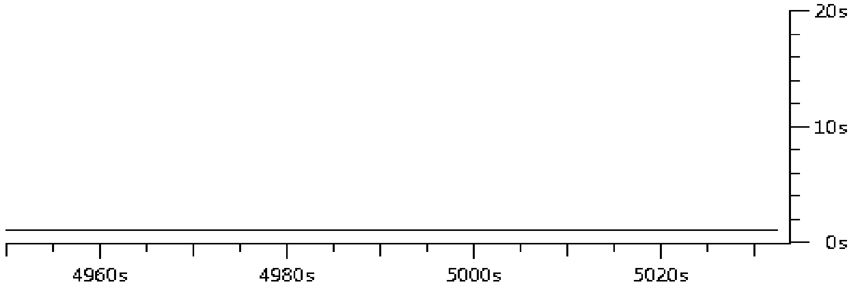

Figure 14: NAT-PT ping delay analysis

As shown in Fig.14, the average delay when using the ping command in network 1 from one of the PCs to the web server through the tunnel is about 2 sec. Fig.15 shows the average delay when using the ping command in network 2 through the NAT-PT router is about 1 sec.

https://doi.org/10.20428/JST.24.2.1

B. Throughput:

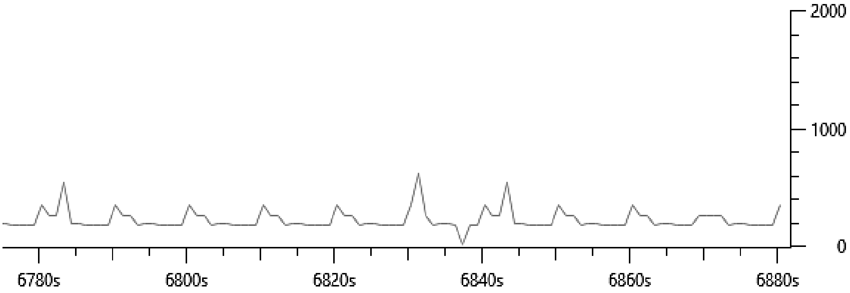

Figure 15: Manual tunnel ping throughput analysis

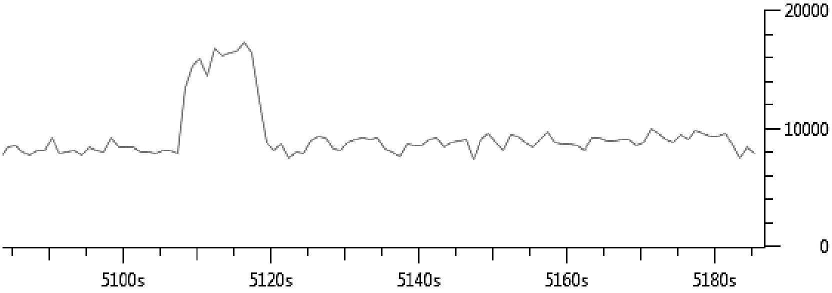

Figure 16: NAT-PT ping throughput analysis

As shown in Fig.16, the average throughput when using the ping command in network 1 from one of the PCs to the web server through the tunnel is about 4000 bits/tick. Fig.17 shows the average throughput when using the ping command in network 2 through the NAT-PT router is about 9000 bits/tick.

7. Results and Deductions:

Both networks have responded successfully to our analyzing and testing and have shown acceptable results meaning that the techniques Both networks have responded successfully to our analyzing and testing and have shown acceptable results meaning that the techniques we've used can, with no doubt, be used as temporary solutions for the end users who still have IPv4-only devices in their internal networks. However, we would like to emphasis on the fact that not both scenarios (manual tunnel and NAT-PT) have the same deployment requirements. Despite the longer configuration

https://doi.org/10.20428/JST.24.2.1

used for the tunneling solution, its implementation is way smoother than that of the NAT-PT. NAT-PT still has many limitations and problems. Even when implemented in GNS3. Many routers (physical or virtual) don't fully support this technique. Only Cisco IOS-XE/XR hardware can work smoothly when applying NAT-PT.

8. Conclusion:

IPv6 deployment strategies can be chosen depending on the current situation of the network. Although all the devices in Yemen ISP's (Yemen Net) network support IPv6, transition from IPv4 to IPv6 in Yemen can't be performed using the dual-stack technique only due to the fact that many Internet users in Yemen are still using IPv4-only devices and won't be able to communicate with users who use IPv6-only devices. We implemented manual tunneling and NAT-PT using GNS3 simulator and real devices to clearly show the conditions, requirements and results of using each technique, and we proved their functionality. Henceforth, we suggest using both tunneling and translation techniques in addition to the dual-stack technique in Yemen as temporary solutions instead of delaying the transition process until all users have devices that support IPv6.

References:

[1]. (IPv4-to-IPv6 Transition and Co-Existence Strategies) Tim Rooney 2011

[2]. Muhammad Yeasir Arafat, Feroz Ahmed and M Abdus Sobhan, "On the Migration of a Large Scale Network from IPv4 to IPv6 Environment", International Journal of Computer Networks & Communications (IJCNC) Vol.6, No.2, March 2014

[3]. IPv6 for Enterprise Networks, Copyright © 2011 Cisco Systems, Inc.

[4]. http://cbspulse.com/2016/02/29/ipv6-smart-persons-guide/

[5]. Nusiba Osman Mohamed Alkhalefa, Amin Babiker A/Nabi Mustafa, "Analysis of Transition Techniques from IPv4 to IPv6", International Journal of Science and Research (IJSR) ISSN 2013.

[6]. IPv6 Transition and Security -Threat Report, NATO.2014.

[7]. Henry Chukwuemeka Paul, Kinn Abass Bakon, " A STUDY ON IPv4 and IPv6: THE IMPORTANCE OF THEIR CO-EXISTENCE", International Journal of Information System and Engineering, Vol. 4 (No.2), November, 2016.

[8]. Manal M. Alhassoun, Sara R. Alghunaim, "A Survey of IPv6 Deployment", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 9, 2016

https://doi.org/10.20428/JST.24.2.1

[9]. S. Gurha, “IPv6 Deployment – Benefit & Opportunities in India with World-wide Experiences”, International Journal of Advanced Technology in Engineering and Science (IJATES), Vol. 03, No. 02, Feb. 2015

[10].E. Agbaraji, F. Opara, and M. Aririguzo, “IPv6 Deployment Status, the Situation in Africa and Way Out,” International Journal of Advances in Engineering & Technology (IJAET), Vol. 1, Issue 6, p. 315, Jan. 2012

[11].https://ipv6-test.com/stats/country/YE.