PES UNIVERSITY
Department of Computer Science & Engineering

UE22CS252B – COMPUTER NETWORKS
Mini Project Report
“IPv6 Transition Mechanisms and Performance Evaluation”
Team Number - 10

Submitted by:

Name: Shravan Jain

SRN: PES2UG22CS528

IV semester section: ‘I’

Name: Sanjiv Raghunandan

SRN: PES2UG22CS504

IV semester section: ‘I’

Submitted to:

Dr. Geetha Dayalan

Associate Professor

Table of Contents

Abstract

As the exhaustion of IPv4 addresses accelerates, the migration towards IPv6 is essential to sustain the demands of internet-connected devices. This project delves into the practical implementation of IPv6 to IPv4 transition methods, focusing on dual-stack deployment, 6to4 tunneling, and NAT-PT (Network Address Translation - Protocol Translation) using Packet Tracer simulation software. Through simulated scenarios, this study examines the operational aspects and efficiency of each transition method. Dual-stack implementation allows coexistence of IPv4 and IPv6 protocols, allowing seamless communication between the two. 6to4 tunneling provides a mechanism for encapsulating IPv6 packets within IPv4 packets, enabling communication between IPv6 hosts across an IPv4 network. NAT-PT facilitates the translation of IPv6 addresses to IPv4 addresses and vice versa, ensuring inter-operability between IPv6 and IPv4 devices. By analyzing the performance, advantages, and limitations of these transition methods, this project offers insights on best methods for IPV4/IPV6 transitions based on various scenarios.

Introduction

Every end device and node needs an IP (internet protocol) address to communicate between the hosts. Address number of currently used IP version 4 is too limited to handle the new demand of IP addresses.

Due to the limitation of IPv4 addresses, another technology raised:

Internet Protocol Version 6 (IPv6). IPv6 was designed for sufficient address space for the present and the future demand for the increased growth of internet. IPv6 increases IP address scheme size from IPv4-32 bits to 128 bits. IPv6 address is cooperated with IPv4 address; this means IPv6 networks is able to merge with IPv4 networks for the future networks. But, anyhow IPv4 does not support new upcoming network criteria. The present IPv4 network is huge and complex, so IPv4 could not be replaced by IPv6 suddenly. Migration from one technology to another technology is absolutely difficult, because of IPv4 and IPv6 are not same assemblage for communication. The three prominent transition mechanisms are widely known as Dual Stack, Tunneling and Network address translation.

Scope of the project

1. Dual-Stack Deployment: Configuration and simulation of dual-stack networks to enable coexistence of IPv6 and IPv4 protocols within the same infrastructure.
2. 6to4 Tunneling: Implementation and analysis of 6to4 tunneling techniques to facilitate communication between IPv6 islands over an IPv4 network.
3. NAT-PT (Network Address Translation - Protocol Translation): Setup and evaluation of NAT-PT mechanisms for translating IPv6 addresses to IPv4 addresses and vice versa, ensuring interoperability between IPv6 and IPv4 devices.

4. Utilization of Packet Tracer software to design, configure, and simulate network environments representative of real-world scenarios for each transition method.
5. Comparative analysis of the performance, advantages, and limitations of dual-stack deployment, 6to4 tunneling, and NAT-PT, aiming to provide insights into their suitability for different network architectures and requirements.
6. Documentation of configuration procedures, simulation results, and analysis findings, culminating in a report.

Hardware and Software requirements

A personal computer or a laptop which is capable of running the latest packet tracer is all that is needed.

Implementation Details

We are using around 35 nodes for each protocol. We have also implemented Clientless SSL VPN in each protocol through ASA-5505 device.

DUAL STACK:

For a simple implementation of the dual stack topology, all the networking devices in the topology should simultaneously support both ipv4 and ipv6 protocols. The hosts/end systems are connected to a dual stack router which in turn is connected to a server. If the server has both IPV4 and IPV6 configured, all the hosts can communicate with it. We configure the respective routes, gateways and enable the DHCP setting in the router.

6to4 TUNNELING:

In a simple implementation of the 6to4 tunneling topology, the IPv6 site has to be connected with another IPv6 site through an IPv4 infrastructure by creating a tunnel interface between two IPv6 networks. The gateway routers should support both protocols. The tunnel interface in the gateway routers should be an IPv6 address. We configure the routes, gateways and enable the DHCP setting in the router. The IPv6 hosts can communicate with the IPv6 server through the IPv4 only router by encapsulating the IPv6 packets inside the IPv4 packets.

NAT-PT:

In a NAT-PT (Network Address Translation – Protocol Translation) topology, the transition changes the header format from IPv6 to IPv4. We are incorporating stateful translation. We take an IPv6 network with only IPv6 hosts and similarly a IPv4 network with only IPv4 hosts. We enable the DHCP setting on the routers in the respective networks to configure the IP addresses. In the middle is a NAT-PT router which has a NAT ipv4 address pool which enables us to communicate between any two hosts of the networks.

Source Code

https://github.com/sanjiv-raghunandan/IPV6-transition-methods.git

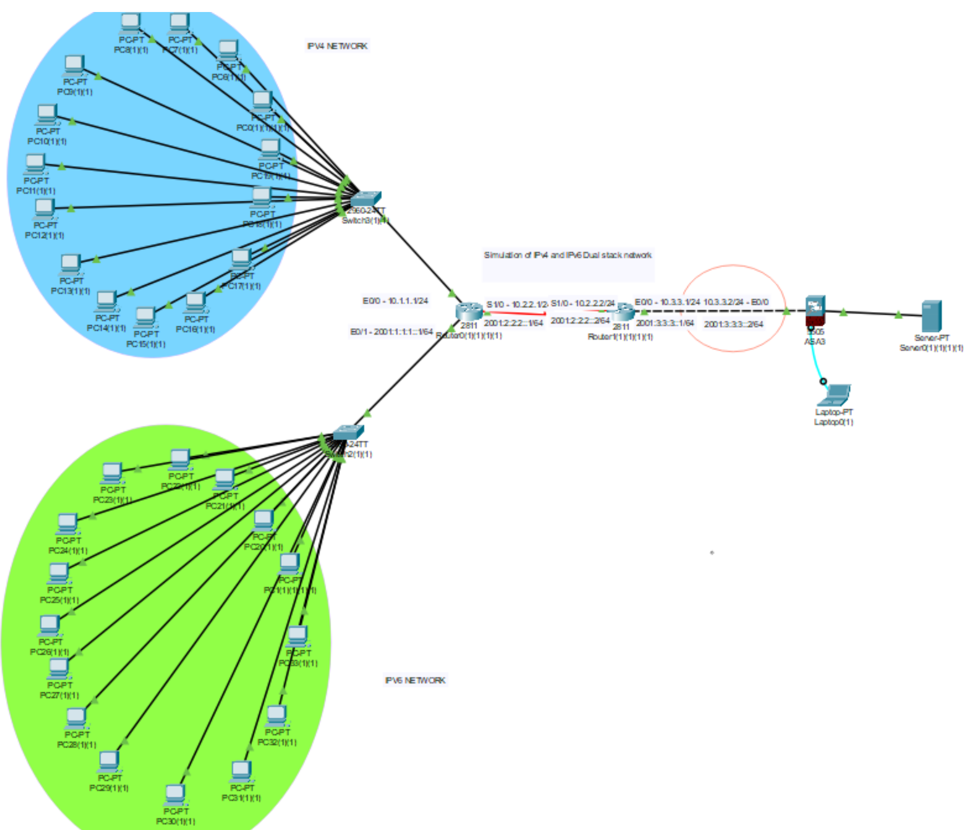
Results and Discussion

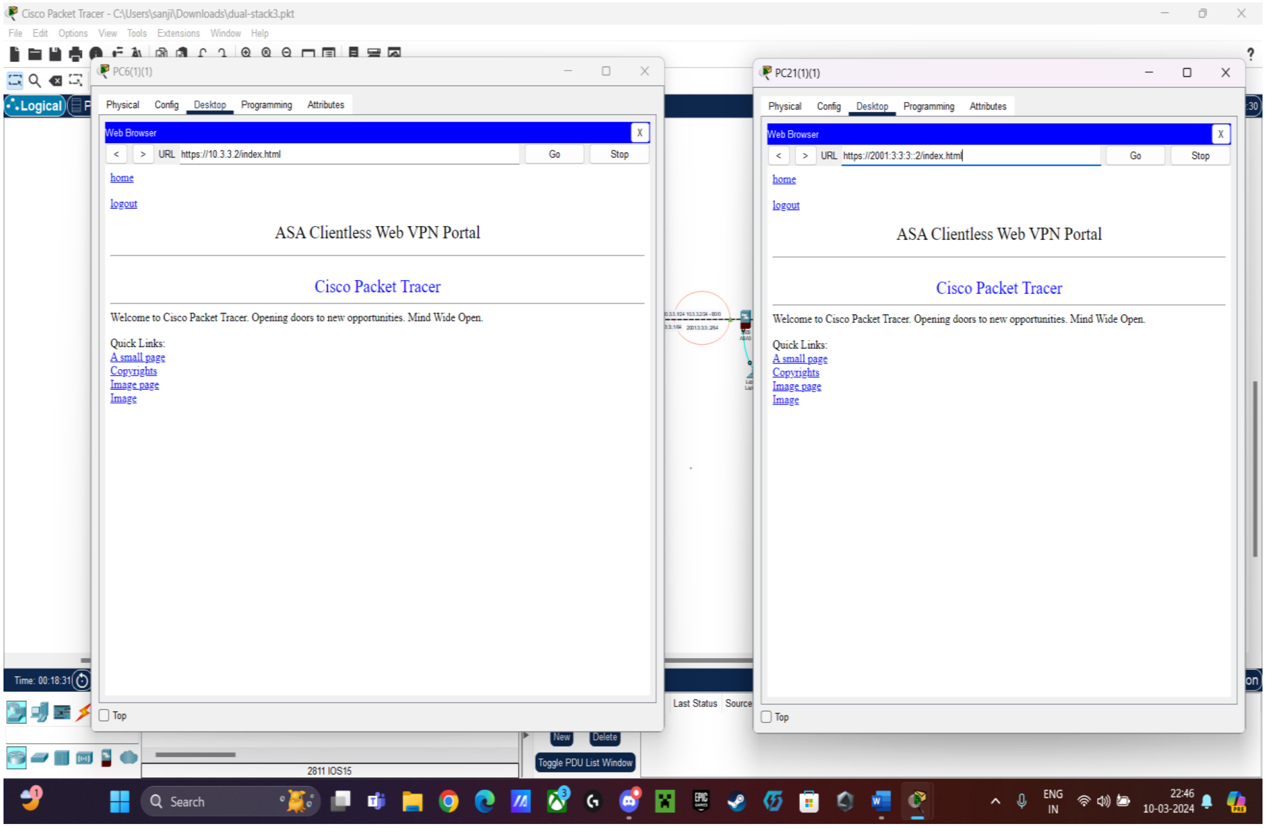
Latency, throughput and packet loss analysis have been done in this report. After observing the packet transmissions, the following results have been found: it has been found that the NAT-PT transition gives the highest latency, while Dual stack provides the moderate and the Tunneling mechanism provides the lowest latency. It is found that tunneling gives the highest throughput rate than the other transition mechanism and the NAT-PT method provides the lowest because of its extra time consuming for the header translation. it is found that NAT-PT transition mechanism experiences highest percentages of packet loss due to its time-consuming limitation. On the other hand, tunneling has the lowest packet lost experience. Summarized below:

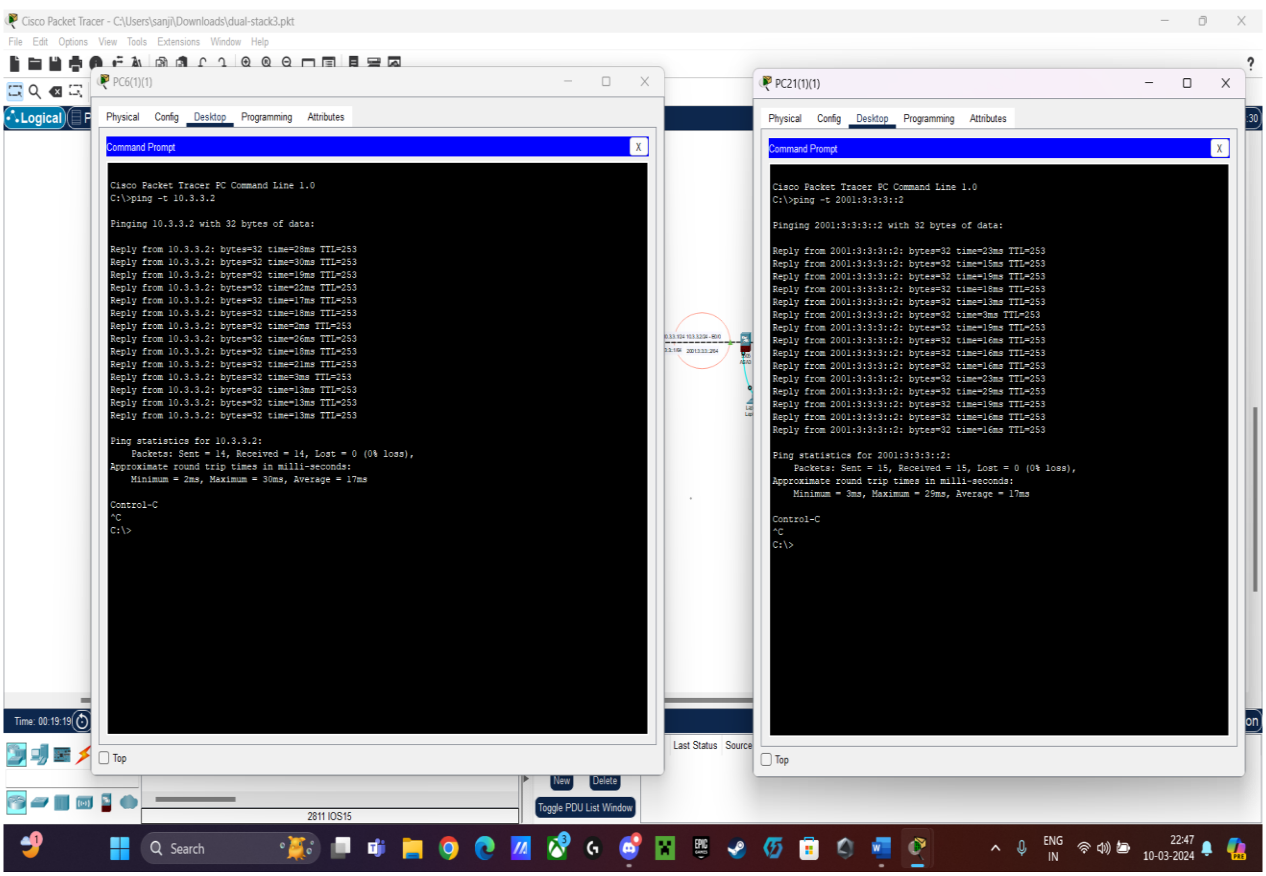
Features	Tunneling	Dual Stack	NAT-PT
Latency	Low	Medium	High
Throughput	Highest	Moderate	Lowest
Packet Loss	Low	Higher compare to tunneling	High

Topology screenshots:

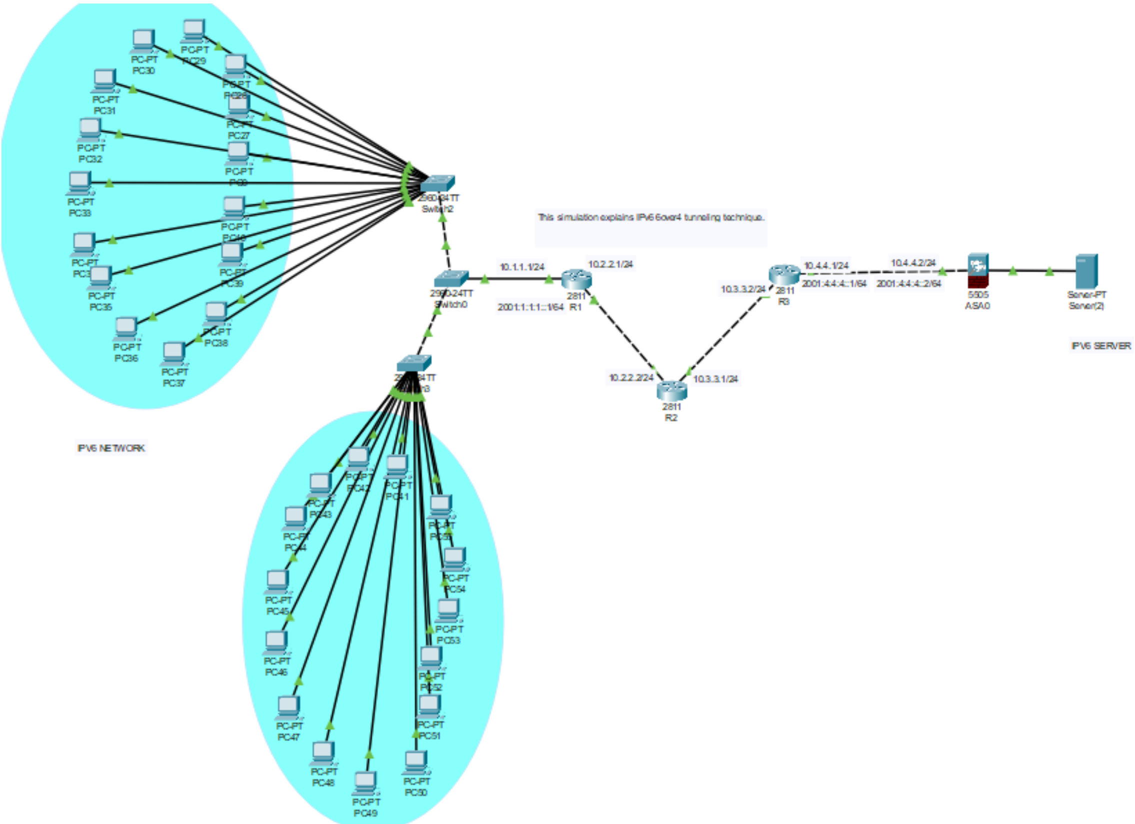
DUAL STACK:



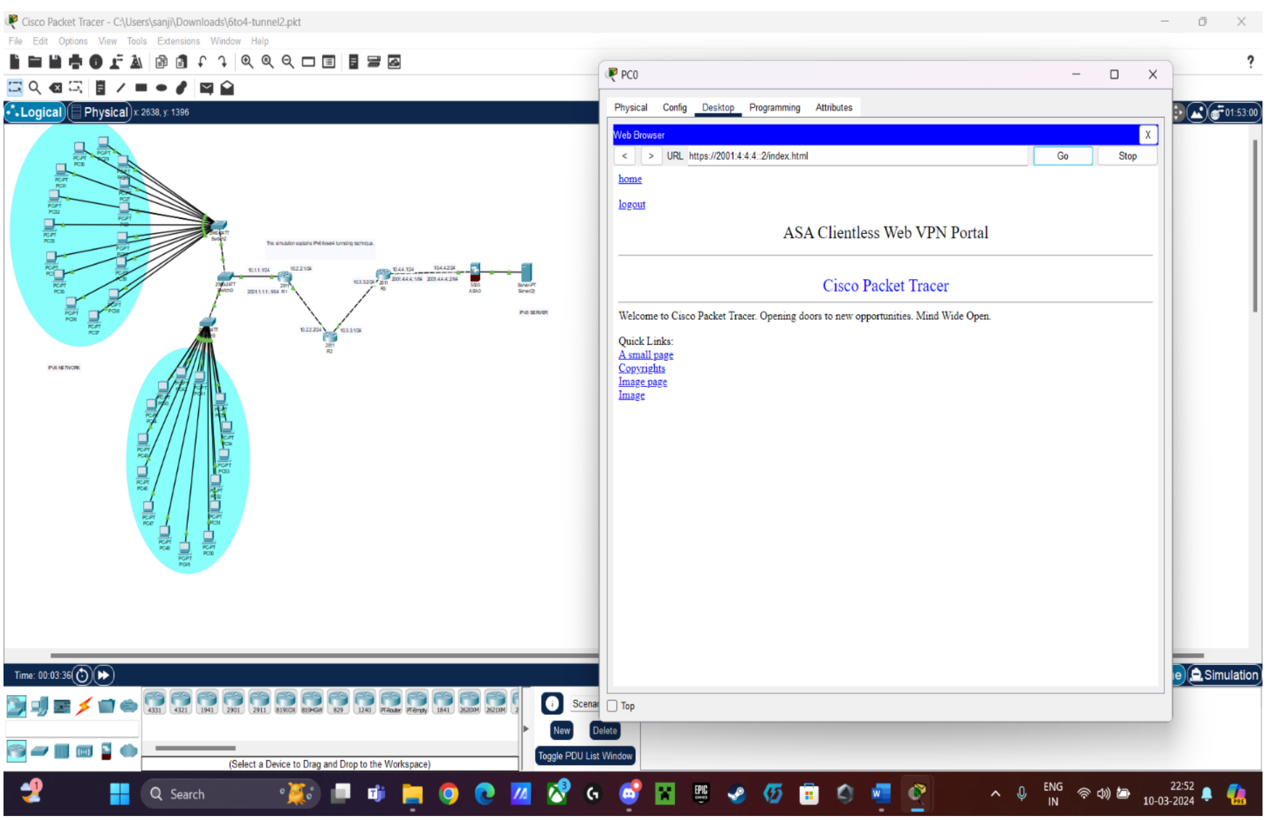

Cisco Packet Tracer - C:\Users\sanji\Downloads\dual-stack3.pkt
PC6(1)(1)
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://10.3.3.2/index.html
Go
Stop
home
logout
ASA Clientless Web VPN Portal
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image
PC21(1)(1)
Web Browser
URL https://2001:3:3:3::2/index.html
Go
Stop
home
logout
ASA Clientless Web VPN Portal
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image
Top
Time: 00:18:31
Last Status
Source
New
Delete
Toggle PDU List Window
2811 IOS15
Search
ENG
IN
22:46
10-03-2024


Cisco Packet Tracer - C:\Users\sanji\Downloads\dual-stack3.pkt
PC6(1)(1)
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping -t 10.3.3.2
Pinging 10.3.3.2 with 32 bytes of data:
Reply from 10.3.3.2: bytes=32 time=28ms TTL=253
Reply from 10.3.3.2: bytes=32 time=30ms TTL=253
Reply from 10.3.3.2: bytes=32 time=19ms TTL=253
Reply from 10.3.3.2: bytes=32 time=22ms TTL=253
Reply from 10.3.3.2: bytes=32 time=17ms TTL=253
Reply from 10.3.3.2: bytes=32 time=18ms TTL=253
Reply from 10.3.3.2: bytes=32 time=2ms TTL=253
Reply from 10.3.3.2: bytes=32 time=26ms TTL=253
Reply from 10.3.3.2: bytes=32 time=18ms TTL=253
Reply from 10.3.3.2: bytes=32 time=21ms TTL=253
Reply from 10.3.3.2: bytes=32 time=3ms TTL=253
Reply from 10.3.3.2: bytes=32 time=13ms TTL=253
Reply from 10.3.3.2: bytes=32 time=13ms TTL=253
Reply from 10.3.3.2: bytes=32 time=13ms TTL=253
Ping statistics for 10.3.3.2:
Packets: Sent = 14, Received = 14, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 30ms, Average = 17ms
Control-C
^C
C:\>
PC21(1)(1)
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping -t 2001:3:3:3::2
Pinging 2001:3:3:3::2 with 32 bytes of data:
Reply from 2001:3:3:3::2: bytes=32 time=23ms TTL=253
Reply from 2001:3:3:3::2: bytes=32 time=15ms TTL=253
Reply from 2001:3:3:3::2: bytes=32 time=19ms TTL=253
Reply from 2001:3:3:3::2: bytes=32 time=18ms TTL=253
Reply from 2001:3:3:3::2: bytes=32 time=13ms TTL=253
Reply from 2001:3:3:3::2: bytes=32 time=3ms TTL=253
Reply from 2001:3:3:3::2: bytes=32 time=19ms TTL=253
Reply from 2001:3:3:3::2: bytes=32 time=16ms TTL=253
Reply from 2001:3:3:3::2: bytes=32 time=16ms TTL=253
Reply from 2001:3:3:3::2: bytes=32 time=16ms TTL=253
Reply from 2001:3:3:3::2: bytes=32 time=23ms TTL=253
Reply from 2001:3:3:3::2: bytes=32 time=29ms TTL=253
Reply from 2001:3:3:3::2: bytes=32 time=19ms TTL=253
Reply from 2001:3:3:3::2: bytes=32 time=16ms TTL=253
Reply from 2001:3:3:3::2: bytes=32 time=16ms TTL=253
Ping statistics for 2001:3:3:3::2:
Packets: Sent = 15, Received = 15, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 29ms, Average = 17ms
Control-C
^C
C:\>
Top
Time: 00:19:19
Last Status
Source
New
Delete
Toggle PDU List Window
2811 IOS15
Search
ENG
IN
22:47
10-03-2024

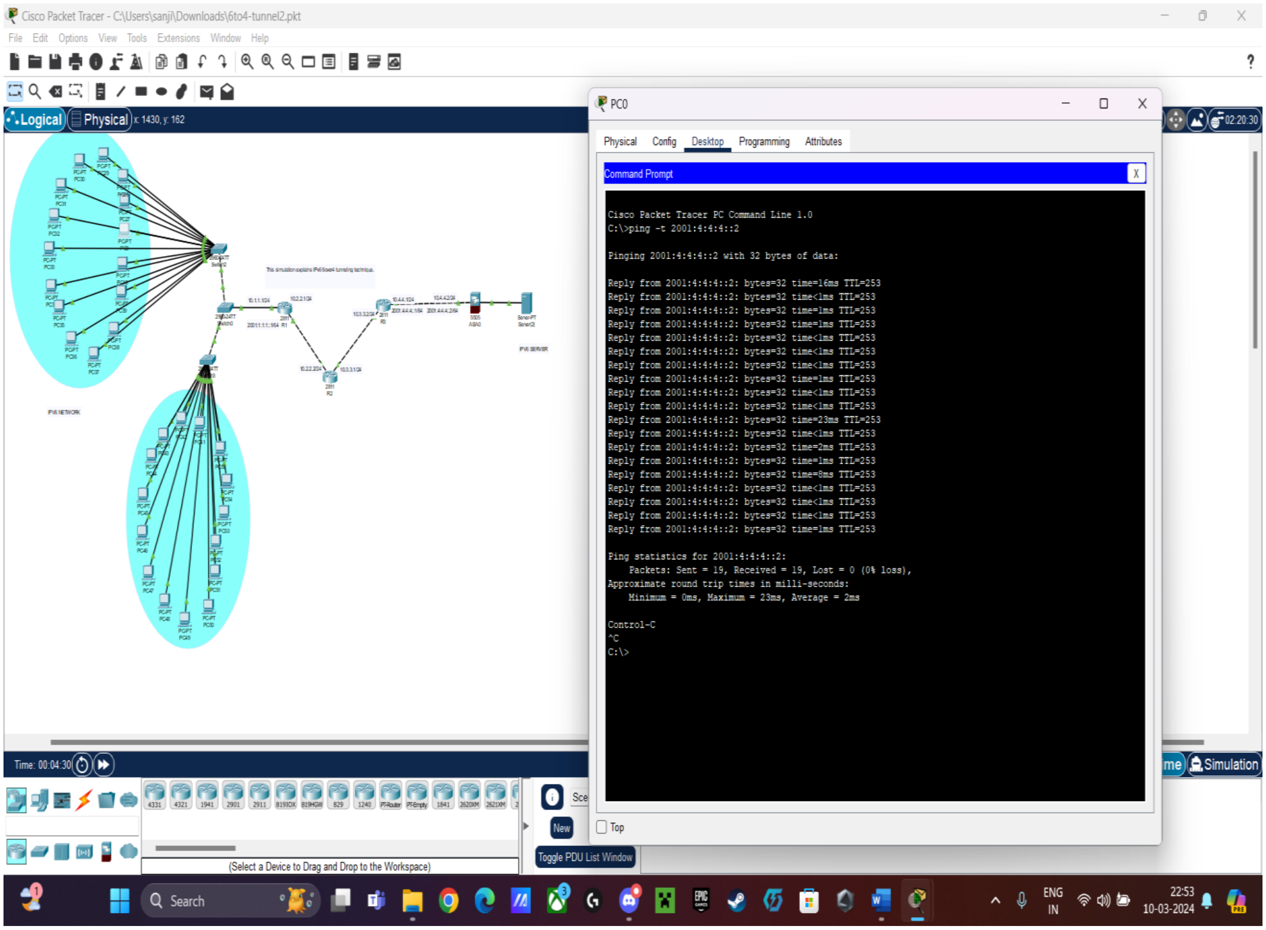
TUNNELING:



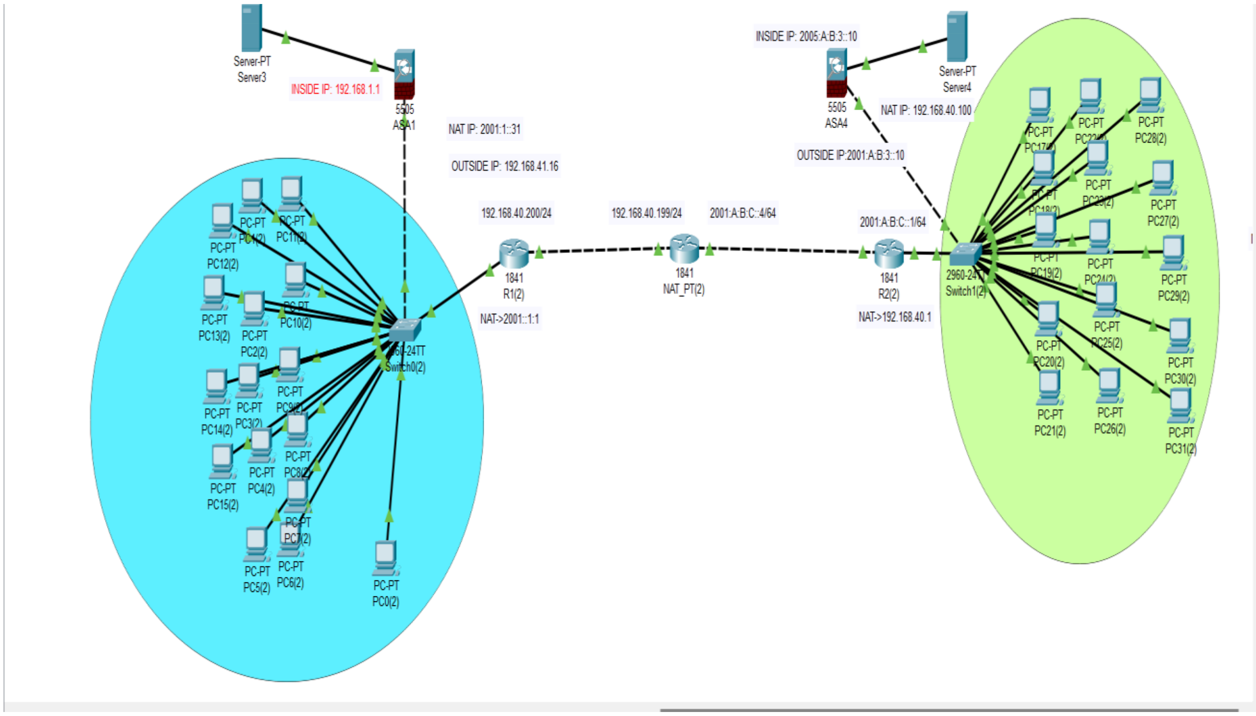
This simulation explains IPv6 6over4 tunneling technique.
10.1.1.1/24
10.2.2.1/24
2001:1:1:1::1/64 R1
10.3.3.2/24
10.4.4.1/24
10.4.4.2/24
2001:4:4:4::1/64
2001:4:4:4::2/64
5505
ASA0
Server-PT
Server(2)
IPV6 SERVER
10.2.2.2/24
10.3.3.1/24
2811
R2
IPV6 NETWORK

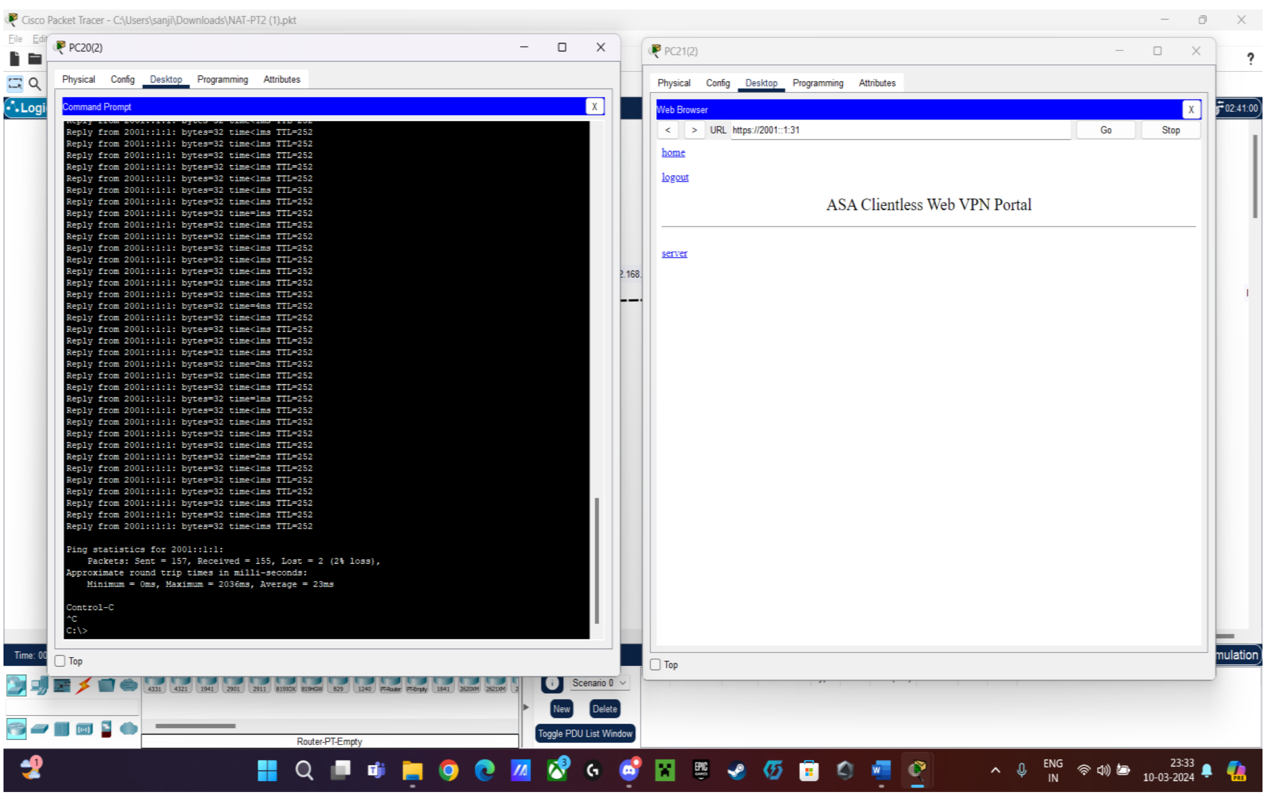


Cisco Packet Tracer - C:\Users\sanji\Downloads\6to4-tunnel2.pkt
PC0
Physical Config Desktop Programming Attributes
Web Browser
URL https://2001:4:4:4::2/index.html
Go
Stop
home
logout
ASA Clientless Web VPN Portal
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image


Cisco Packet Tracer - C:\Users\sanji\Downloads\6to4-tunnel2.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping -t 2001:4:4:4::2
Pinging 2001:4:4:4::2 with 32 bytes of data:
Reply from 2001:4:4:4::2: bytes=32 time=16ms TTL=253
Reply from 2001:4:4:4::2: bytes=32 time<1ms TTL=253
Reply from 2001:4:4:4::2: bytes=32 time=1ms TTL=253
Reply from 2001:4:4:4::2: bytes=32 time=1ms TTL=253
Reply from 2001:4:4:4::2: bytes=32 time<1ms TTL=253
Reply from 2001:4:4:4::2: bytes=32 time<1ms TTL=253
Reply from 2001:4:4:4::2: bytes=32 time<1ms TTL=253
Reply from 2001:4:4:4::2: bytes=32 time=1ms TTL=253
Reply from 2001:4:4:4::2: bytes=32 time<1ms TTL=253
Reply from 2001:4:4:4::2: bytes=32 time<1ms TTL=253
Reply from 2001:4:4:4::2: bytes=32 time=23ms TTL=253
Reply from 2001:4:4:4::2: bytes=32 time<1ms TTL=253
Reply from 2001:4:4:4::2: bytes=32 time=2ms TTL=253
Reply from 2001:4:4:4::2: bytes=32 time=1ms TTL=253
Reply from 2001:4:4:4::2: bytes=32 time=8ms TTL=253
Reply from 2001:4:4:4::2: bytes=32 time<1ms TTL=253
Reply from 2001:4:4:4::2: bytes=32 time<1ms TTL=253
Reply from 2001:4:4:4::2: bytes=32 time<1ms TTL=253
Reply from 2001:4:4:4::2: bytes=32 time=1ms TTL=253
Ping statistics for 2001:4:4:4::2:
Packets: Sent = 19, Received = 19, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 23ms, Average = 2ms
Control-C
^C
C:\>
Top
Simulation
Toggle PDU List Window
(Select a Device to Drag and Drop to the Workspace)

NAT-PT:


Server-PT
Server3
INSIDE IP: 192.168.1.1
5505
ASA1
NAT IP: 2001:1::31
OUTSIDE IP: 192.168.41.16
192.168.40.200/24
1841
R1(2)
NAT->2001::1:1
192.168.40.199/24
2001:A:B:C::4/64
1841
NAT_PT(2)
2001:A:B:C::1/64
1841
R2(2)
NAT->192.168.40.1
INSIDE IP: 2005:A:B:3::10
Server-PT
Server4
5505
ASA4
NAT IP: 192.168.40.100
OUTSIDE IP:2001:A:B:3::10
2960-24TT
Switch1(2)
PC-PT
PC0(2)
PC-PT
PC5(2)
PC-PT
PC6(2)
PC-PT
PC15(2)
PC-PT
PC4(2)
PC-PT
PC14(2)
PC-PT
PC3(2)
PC-PT
PC13(2)
PC-PT
PC2(2)
PC-PT
PC12(2)
PC-PT
PC10(2)
PC-PT
PC20(2)
PC-PT
PC21(2)
PC-PT
PC26(2)
PC-PT
PC25(2)
PC-PT
PC30(2)
PC-PT
PC31(2)
PC-PT
PC27(2)
PC-PT
PC28(2)
PC-PT
PC29(2)

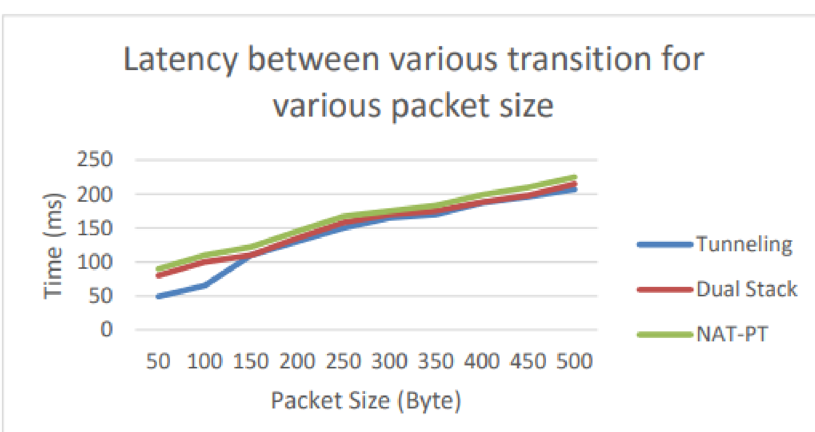

Cisco Packet Tracer - C:\Users\sanji\Downloads\NAT-PT2 (1).pkt
PC20(2)
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Reply from 2001::1:1: bytes=32 time<1ms TTL=252
Ping statistics for 2001::1:1:
Packets: Sent = 157, Received = 155, Lost = 2 (2% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2036ms, Average = 23ms
Control-C
^C
C:\>
PC21(2)
Web Browser
URL https://2001::1:31
Go
Stop
home
logout
ASA Clientless Web VPN Portal
server
Top
Scenario 0
New
Delete
Toggle PDU List Window
Router-PT-Empty
ENG
IN
23:33
10-03-2024

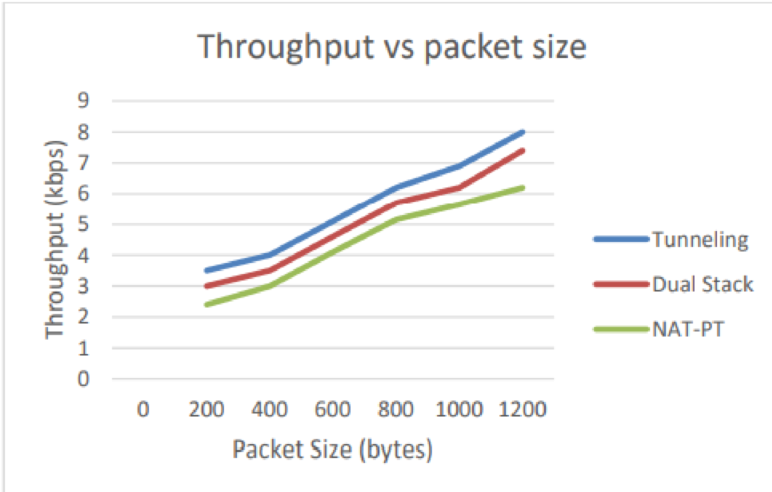
Conclusion

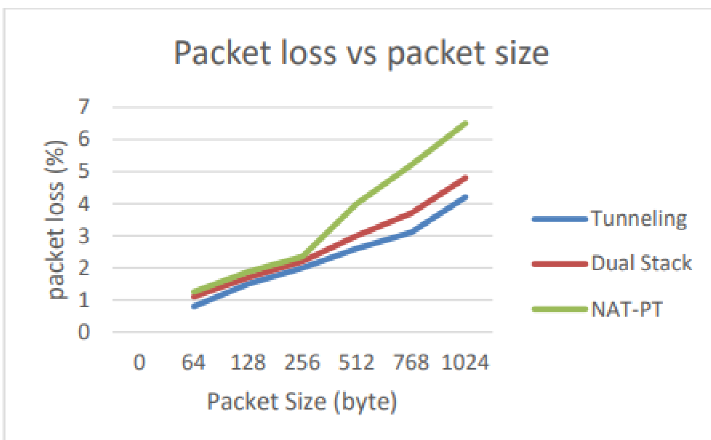
The three mechanisms of the IPv6 to IPv4 transition have been discussed, deployed and analyzed.

It has been found that three mechanisms have distinct advantages and features with some disadvantages. The appropriate transition mechanism will be chosen for the network based on various parameters like the size of the network, the availability of the latest devices, the cost, the security concern and so on. If latency, throughput and packet loss are considered then tunneling method is the best choice while the NAT-PT is the worst. Dual stack is moderate in all the three parameters considered. Tunneling would the best go-to protocol but has some security issues (spoofing, bypass security measures, lack of visibility, encapsulation vulnerabilities) which need to be configured. By taking security, scalability, cost effectiveness and simplicity of implementation, dual stack would be the best approach.

STATISTICS:







Learning Outcome

From the following experimentation, we understand how the implementation of different protocols in real life scenarios work. The approach to be taken in future scenarios and implementing it in different simulation software. The different security implications to cover and to mitigate the risks effectively. All of this together will help us smoothly transition into an IPv6 worldwide network.