2020

National IPv6 Transition Plan

Implementation Guidelines

Oman IPv6 Task Force

Acknowledgements

This document was produced within the National IPv6 transition plan Project. Oman IPv6 Task Force (OTFv6) would like to express its gratitude to Mr. Sina Ghane (Huawei Oman) and Dr. Shubair Abdullah (Sultan Qaboos University) for their substantial contributions in the development of this document.

Table of Contents

Key contributors

Project Manager and Executive Editor:
Yahya Nasser Al Hajri
Editors:
Zainab Khalfan Salim Al-Farsi
Saif Said Ali Al Ghafri
Al-Wahida Majid Khalifa Al-Harthy
Nasser Mohammed Khalifah Al Jabri
Abdulrahman Al-Hajri

Mohammed Al Wahaibi
Nuzha Mohammed Ali Al Maharbi
Shaima Nasser Hamed Al Mukhaini

The content of this document is based on a number of theoretical dependencies and assumptions. TRA shall not be bound by or liable for any statement, representation, undertaking or omission made in this document. Furthermore, the TRA may change at any time the contents of this document at its sole discretion and shall not be liable for the consequences of such changes.

1. Introduction

The Sultanate of Oman is economically and socially developing nation that is always eager to apply and deploy modern technologies in the public and private sectors. The telecommunications ecosystem in Sultanate of Oman consists of many stakeholders like the Government organizations, service providers, content and application providers, equipment manufacturers, cloud computing/data centers providers etc. The Telecommunications Regulatory Authority (TRA) comes across all of these stakeholders to be the linkage that sets out standardized policies. It is responsible for formulating various standards and specifications for equipment used by the licensees for providing telecom and Internet services.

Since the advent of IPv6, the Government of Sultanate of Oman has recognized the importance of deploying IPv6 in the country, and has taken an important step by forming the Oman IPv6 Task Force (OTFv6) to work with the TRA in the Sultanate. The main goal of OTFv6 is to give the initial push required by the industry to move on the road to IPv6 adoption. It was tasked to bring all the industry stakeholders to a common IPv6 platform countrywide. To increase awareness of IPv6 deployment, the OTFv6 publishes this document, the national IPv6 transition plan for transiting from IPv4 to IPv6. The OTFv6 carried out a number of activities under the umbrella of the TRA such as visiting entities from Public and the private sectors, conducting training programs on IPv6, sharing IPv6 best practices to the Government organizations, and releasing IPv6 monthly newsletters. As for IPv6 testing of equipment, and to ensure that all stakeholders perform the IPv6 journey in a coordinated and standardized manner, TRA has started developing an IPv6 test lab that is contributed by the telecom vendors for the benefit of stakeholders for getting their networking equipment tested for IPv6 readiness.

2. Rationale

The national IPv6 transition plan initiated due to the fact that Internet acts as a catalyst for socio-economic development of a country and serves as an effective medium for delivery of various citizen centric services even in remote and rural areas. Since the current version of the Internet Protocol (IPv4) has run out of addresses in our region in the third week of November 2019, the broadband revolution that is on the verge of sweeping the country is sure to ride on next generation Internet Protocol version 6 (IPv6) which has many inherent advantages as well.

The TRA recognizes the futuristic role of IPv6 and aims to achieve substantial transition to IPv6 in the country in a phased and time bound manner. The adoption of IPv6 based innovative applications in areas like rural emergency healthcare, tele-education; smart metering, smart grid, smart building, smart city etc. have enormous potential to boost the socio- economic development of the country thereby improving the quality of life of people in Oman. By releasing this document, the OTFv6 hopes that it will be an important milestone in the journey of transition from IPv4 to IPv6.

3. Content

The content of this document is divided into two parts, guidelines and recommendations. The guidelines part covers everything related to the transition process such as human resources, training courses, equipment, etc. in order to achieve a coordinated transition from IPv4 to IPv6. The recommendations, some of which are mandatory in nature, have been formulated and firmed up after extensive discussions with all stakeholders including Government organizations and industry associations and adopting the pragmatic approach while incorporating the relevant viewpoints. Efforts have been made to incorporate all relevant inputs, material and experience gained during the last two and a half years since the release of earlier Roadmap. In addition, the content provides details of challenges faced and strategies and draws the timelines to be adopted by the different stakeholders in the IPv6 ecosystem in the Sultanate.

4. Objectives

The objectives of the national IPv6 transition plan are summarized in the following:

- Drive IPv6 adoption in Oman through initiatives.
- Facilitate the IPv6 deployment for government entities that are connected to the Oman Government Network (OGN)
- Direct government entities, banks, oil & gas companies, and others to enable IPv6 aiming towards end of 2020.
- Address issues for nationwide implementation of IPv6, including address allocation, migration process, equipment, Human Capacity, and policy assistance.

The OTFv6 sincerely hopes that with this initiative and the support of all stakeholders, the above-mentioned objectives will be timely achieved.

5. OTFv6 Role & Responsibility

5.1. Objectives

The main goal of the OTFv6 is to plan, administer, and monitor the national initiative with the following objectives:

1. Obtain a broad understanding of IPv6 and develop the national transition roadmap
2. Carefully study other countries' migration documents and/or manuals, if any in order to prevent any unforeseen issues that might occur during or after the transition
3. well understand the different transition mechanisms and network architectures
4. List the readiness of the equipment and services

5.2. Members

The OTFv6 consists of members from Telecommunications Regulatory Authority (TRA), Ministry of Technology & Communications (MTC) and Internet Service Providers (ISPs). The OTFv6 also receives support from the vendors and academia.

5.3. Roles and Responsibilities

The work of OTFv6 team is a very important part of the project. The OTFv6 team will be responsible for the following duties:

1- Studying and choosing the IPv4-IPv6 transition mechanism that is aligned with what the telecommunication ecosystems adopt in the Sultanate.
2- Assessing the readiness of ISPs operating the Sultanate in providing.
3- Encouraging and implementing capacity-building projects in IPv6 in order to facilitate human and infrastructure capacity development in Oman.
4- Cooperating with and helping partner organizations and stakeholders in spreading the awareness of IPv6.

5- Carrying out frequent meetings with the transition teams at different entities and stakeholders to follow up the process of deploying IPv6.

6. Entities Roles and Responsibilities

6.1. Public and Private sector

The roles and responsibilities of the public and private sector entities are as follows:

1. The corporate organizations are mandated to prepare a detailed transition plan, for deploying the IPv6 in their networks to work along with the IPv4 stack. The due date of plan submission is December 2018.
2. Equipment that are procured by any organization should support IPv4 stack as well as IPv6 stack (dual stack). They should be deployed with IPv6 supported applications through a technology that helps to migrate to an IPv6 network without changing the currently operating end-user applications with immediate effects.
3. All new IP based services such as cloud computing, data centers, etc. being provisioned for/by the corporate should support and run IPv4 and IPv6 protocols with immediate effect.
4. Starting from 1/1/2019, all services/applications/systems that provide services to the public are required to support dual stack traffic regardless of whether these services/applications/systems are existing or will be developed in the future.
5. All corporate organizations were mandated to implement the IPv6 stack to work along with the IPv4 stack (dual stack) before or by December 2020. The corporate organizations may choose an appropriate date before December 2020 to complete the implementation based on the complexity of the network and the equipment/technological life cycles.

6.2. Internet Service Providers (ISP)

The role and responsibilities of ISP are described below:

I. Enterprise/corporate customers:

   a. All new wireless or wireline connections of enterprise /corporate customers provided by ISPs in or after the first quarter of 2018 should be capable of carrying IPv6 traffic.

b. Regarding the existing enterprise customers, who are not IPv6 ready, the ISP should educate and encourage their customers to switch over to IPv6.

II. Retail wireline customers:

c. All new retail wireline customer connections provided by ISPs in or after the first quarter of 2018 should be capable of carrying IPv6 traffic either on dual stack or on native IPv6.

d. The ISP shall endeavor to progressively replace/upgrade their owned Customer Premises Equipment (CPE) which are not IPv6 ready as per the following timelines:

i. Replace/upgrade 25% of CPE by December 2018
ii. Replace/upgrade 50% of CPE by June 2019
iii. Replace/upgrade 75% of CPE by December 2019
iv. Replace/upgrade 100% of CPE by June 2020

e. Regarding the customers, own CPE, which are not IPv6 ready, the ISP should educate and encourage them to replace/upgrade their CPE to IPv6 ready CPE.

III. Retail wireless customers:

f. Starting from the third quarter of 2018, all new Long-Term Evolution (LTE) customer connections provided by ISPs should be capable of carrying IPv6 traffic either on dual stack or on native IPv6.

6.3. Content and Applications Providers

The role and responsibilities of contents and applications providers are mainly represented by:

- All Content and Application providers were required to adopt both IPv4 and IPv6 (Dual Stack) for content and applications starting by the first quarter of 2018.

6.4. Equipment's Dealers/Importers

The role and responsibilities of equipment's dealers/importers are mainly represented by:

- All IP-based Equipment's submitted to TRA for Type Approval certificate, should support IPv6 effective since June 2018.

The TRA has taken some regulatory measures towards some IP-based equipment. These measures were taken in coordination with the importers of these equipment. These regulatory measures are applicable only to some of the IP-based equipment mentioned in the following list:

1. Switches
2. Routers
3. Servers
4. Firewalls
5. Terminal cards
6. xDSL modems
7. Telephone set
8. Core network equipment
9. IoT equipment

7. Steps to Enable IPv6 in Public and Private Sector Networks

Public and private sector entities are recommended to follow a phased transition approach spread over a period of time depending on the complexity and the IPv6 readiness of the current networks. A typical phased transition approach is depicted in Figure 1.

Figure 1. Typical phased IPv4 to IPv6 transition approach

In the following, a description is provided for the necessary steps of the typical phased transition approach during an IPv6 deployment project:

Appointment of transition team:

The transition team is appointed to drive the IPv6 implementation within the organization during the project period. The transition team will be responsible for the following duties:

- Identify internal stakeholders (Contract & Procurement, Network, Application & Systems, etc.)
- Identify external stakeholders, if any.
- Identify scope (assets such as devices, systems, services using IP protocol)
- Gap analysis (current technologies, services, skills, etc.)
- Identify transition requirements
- Assign team to develop and implement the overall transition plan
- Identify associated cost (time and effort, resources, tools, testing, network and systems re-engineering/updating, etc.)

Training:

In order to have a seamless transition with minimum disruption due to human error or lack of knowledge, it is of utmost importance to develop skilled IPv6 trained human resources within the organization. The required persons are to be identified for IPv6 training and arrangements for their training to be made. This can go on as a parallel and continuous activity.

Assessment:

The transition plan should be discussed with all stakeholders and a detailed assessment across the following should be conducted:

i) Network Assessment
ii) Application Assessment
iii) Services Assessment
iv) Security Assessment

Every project should start with an audit of the current and future planned changes in infrastructure, from client devices, operating systems, applications, network services, servers, security equipment and, of course, all the equipment that supports the network itself (switches, routers, wireless, and so forth).

It is essential to test from various points on the Internet, to confirm that your network is not just accessible from its immediate environment, economy or region.

Applications and Services Tests:

Examining applications and services helps to identify several challenges and problems, including, applications that use literal addresses, the applications that use old libraries without IPv6 support, and the applications that store 32-bit fields in databases. The test stage should preferably include classifying and studying these applications in order to take appropriate actions against the challenges created by them. Involving the application and services vendors is important in this stage. The vendors are able to confirm the IPv6 compatibility of these application and services.

Plan and Strategy Formulation:

This stage involves detailed planning and formulation of a transition strategy based on assessment gaps identified in the existing network. The plan should consider the future networks and services to ensure that the network and its applications and services comply with future developments, such as the Internet of Things (IoT) and Smart Cities. The plan and strategy formation stage may involve the following technical aspects:

i) Development of IPv6 addressing plan: It is recommended to start from scratch and not relying on the current IPv4 addressing plan since the IPv4 address plans are most likely based on private addresses that may be duplicated in different parts of the network.

ii) The use of Border Gateway Protocol (BGP): In IPv6 there is no need for NAT, therefore the use of BGP is good practice. Furthermore, to avoid renumbering when changing ISP. It is essential to use BGP and provider independent addressing.

iii) The operation of Domain Name System (DNS): The transition to IPv6 is based on the fact that the operating system and/or applications are able to choose properly if they must use IPv4 or IPv6. This implies an intensive use of the DNS for the entire network, which is not common when using only IPv4.

iv) The assignment of IPv6 addresses: One of the most important aspects when deploying IPv6 is to understand the differences between the different mechanisms of address assignment, such as auto configuration with Stateless Address Auto configuration

(SLAAC), with Dynamic Host Configuration Protocol (DHCPv6), or with the combination of both and even the use of multiple addresses on each interface. It is also necessary to understand what devices or operating systems can use either one and in what circumstances.

Obtain Internet Number Resources:

For government entities members of OGN, the required IPv6 address blocks are to be acquired as per the IPv6 address plan firmed up by MTC. The addresses may be obtained from MTC directly. For non-governmental entities, the Internet Number Resources Autonomous System Numbers (ASN) and IP addresses may be obtained from RIPE NCC. This ASN is required to avoid renumbering and to be able to have your own addresses with BGP. The organization can qualify for a minimum of one /48 for each 'site' of the network. This allows addressing for up to 65,536 subnets (/64) within each site. If it is a larger network, which may need to sub-assign addresses to third parties, even to other institutions in the case of a government network, then it will qualify for a minimum of one /32 (allowing 65,536 sites, each with its own /48). Large networks of governments will often require shorter prefixes, for example, /25 or /26.

Pilot Testing:

A pilot test of network either centrally or in one of the organizations has to be set up for the purpose of detailed testing of the networks, applications and services before transition to IPv6. The process should cover testing of the IPv6 readiness across hardware, applications, services and their capability to interoperate with IPv4 for a seamless transition. The security audit should also be included in this process.

Implementation:

On successful completion of testing, it is required that organizations implement its transition plan. This involves deployment of equipment in the network and transition of applications and systems. The implementation stage is often involve checking contracts with ISP and connections with other organizations. Deploying IPv6 will require discuss the IPv6 support including BGP support. Its good practice to announce your own addressing space via your own ASN. If the direct connection with other entities in the Sultanate. It is important to coordinate with these entities about your plans. In addition, since the IPv6 address space in very huge,

it is easier to use specific IP addressing management tools (IP Address Management (IPAM)), which can be open source. Often these solutions allow coordination with the DNS and even with DHCPv4 and DHCPv6.

Auditing & Commissioning:

During the implementation stage, it is important to audit the network and applications to be able to run all the services seamlessly. Auditing the networks and applications is important to complete IPv6 readiness. Post successful audit the networks and applications will be certified as IPv6 ready for the services checked in audit. These audits will have to be conducted on a regular basis as and when any changes in network/application take place.

Network Management:

Since IPv6 is a new protocol, the IPv6 network management is important to take care of any issues arising post implementation.

8. Security

Just like the early deployment of many technologies, security is often left to the final stages of implementation which introduces many challenges and also complicates the security deployment at later stage. While IPv6 is not directly compatible with its predecessor, it possesses many of the same risks associated with IPv4. However, if implemented properly, IPv6 has the potential to provide a foundation for creating a secure infrastructure for an organization as well as the Internet as a whole. IPv6 provides many additional security features over IPv4 like extension header based, IPsec support, and Secure Neighbor Discovery Protocol (SeND), etc.

8.1. Challenges

IPv6 is likely to follow the same course as the number of deployments increase. The attacker community is gaining interest in IPv6, as it is an easy route for them with lack of IPv6 expertise in organizations. It is therefore important for organizations to improve the security of IPv6 deployments from day one. IPv6 has some advantages over IPv4 but also have few unique security vulnerabilities. The transition to IPv6 is inevitable; therefore organizations should understand the challenges that appear during

the deployment of IPv6 protocols and the operations of the IPv6 services. Organizations are most likely to face the below mentioned security challenges during the deployment process:

1. Setting up the IPv6 Access-list (ACL)
2. Configuring the authentication and encryption of IPv6 routing protocols
3. Configuring IPv6 source guard, router advertisement guard, and DHCPv6 guard
4. Setting up IPv6 neighbor discovery inspection

If organizations elect to deploy IPv6 without overcoming the above challenges, it is like running a backdoor protocol to the network systems that could potentially be exploited. Security vulnerabilities that exist for IPv4 also generally apply to IPv6; however, there are additional vulnerabilities that exist for IPv6. Some instances of these issues are described as follows:

1. IPv6 reconnaissance attacks
2. Attacks due to IPv6 auto-configuration
3. Man-in-the-middle attack (as in IPv4)
4. Type 0 routing header attack
5. Dual-stack related issues
6. ICMPv6 and Multicast addressing

8.2. Proposed Approach for Secure IPv6 Deployment

Organizations should understand the security risks of deploying IPv6, as well as strategies to mitigate such risks. Figure 2 depicts a recommended approach for secure IPv6 deployment.

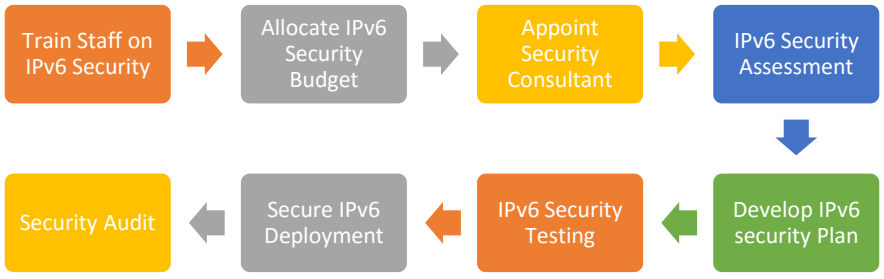

Figure 2. Approach for secure IPv6 deployment

Step-1: Train Staff on IPv6 security:

Organizations must understand the differences between IPv4 and IPv6 and know how those differences have security implications. IPv6 is going to coexist with IPv4 for a near future, which means the network is as secure as the least secure protocol; organizations should have the security architecture in place for both protocols. Since both protocols do not inter-operate, it requires a transition technique such as dual-stack and IPv6 network address translation (NAT64). Organizations need to ensure a secure transition deployment.
As a first step, organizations should look to build IPv6 security skill sets equaling to IPv4 security skill sets. Organizations should provide IPv6 security training for key operational personnel and policy makers. The individuals should have enough information to be able to formulate IPv6 policy and guidance for the organization, and to implement enough security safeguards to enforce the policies.

Step-2: Allocate IPv6 Security Budget:

Organizations should do the budget allocation for IPv6 security in addition to IPv4. Budget calculation should be based on efforts required for security assessment, design, testing and deployment. Organizations should allocate additional budget if any hardware upgrade is required to meet the security requirements.

Step-3: Appoint Security Consultant: (Optional)

Organizations may choose to appoint external security consultants or internal staff for conducting IPv6 security posture analysis, build IPv6 security plan, testing and deployment. Based on organizations' IPv6 security skill sets and the business needs, some or all of these activities can be outsourced to experienced consultants.

Step-4: IPv6 Security Assessment:

IPv6 security assessment helps to understand the risks posed to an organization by vulnerabilities present in the organization's IP-networked systems including IPv6 and IPv4. Security assessment should capture network, applications and services security posture and highlight the vulnerabilities with possible mitigation techniques.

Step-5: Develop IPv6 Security Plan:

While IPv6 provides the foundation for the development and implementation of a more secure network, organizations must be

concerned with potential issues the new protocol may create. Examples of these issues are:

- Poorly implemented IPv6 protocols
- Few network protection devices/tools support IPv6
- Improperly configured network elements like firewalls, Intrusion detection systems (IDS), intrusion prevention systems (IPS), etc.
- Poorly implemented IPv6 routing protocols
- Inconsistent IPv4 security features with those of IPv6
- Few IPv4 network management tools ported to IPv6
- New or existing applications unable to leverage new IPv6 features

The development of the IPv6 security plan should include a core understanding of all of the components necessary to secure the organization's networks. Organizations should build the security plan by giving due consideration to all the above points. Figure 3 shows some major components of an IPv6 security plan.

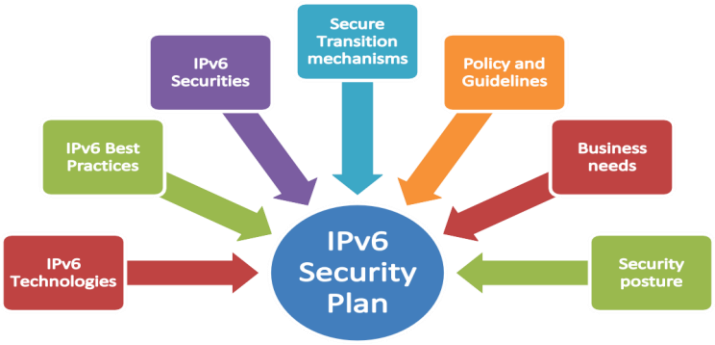

Figure 3. Major components of IPv6 security plan

Step-6: IPv6 Security Testing:

Validation of IPv6 features, interoperability, and performance issues become critical factors for organizations for smooth transition to IPv6. Since IPv6 is a new protocol stack, it becomes important to test the protocol implementations in vendor hardware and software as this could become critical. Below are the suggested tests, organizations should perform before deployment:

- IPv6 security conformance testing
- IPv6 security inter-op testing
- IPv6 security performance testing
- IPv6 security design validation testing

Step-7: Secure IPv6 Deployment:

On successful completion of testing, it is required that organizations implement the transition plan.

Step-8: IPv6 Security Audit:

Organizations should have a regular audit policy to ensure that new vulnerabilities are adequately addressed in the network. It is recommended to have periodic security audits (e.g. at least one security audit every year) to assess the security state of the network so that appropriate actions can be taken proactively.

8.3. IPv6 Security Recommendations

In order to achieve security parity with IPv4 networks, the emerging IPv6 networks should be protected against all attacks for which IPv4 networks are currently protected. They should additionally be protected against new attacks that are specific to new features. Below are a list of recommendations in this regard:

- Encourage staff to increase their knowledge of IPv6 to a level comparable with their current understanding of IPv4.
- Plan a phased IPv6 deployment utilizing appropriate transition mechanisms to support business needs.
- Use automated address management tools to avoid manual entry of IPv6 addresses, as they are prone to error because of their length and form of notation.
- Develop a proper ICMPv6 (Internet Control Protocol for IPv6) filtering policy to ensure that only ICMPv6 essential IPv6 operation messages are allowed. Security firewalls will have to be configured accordingly for IPv6.
- Be aware of extension header threats and filter extension headers appropriately
- Drop packets containing Routing Header Type 0 and unknown option headers whenever possible.
- Deny packets that do not follow the rules for extension headers. Perform Unicast RPF filtering to prevent spoofed source addresses.
- Deploy the Domain Name System Security Extensions (DNSSEC)
- Restrict who can send messages to multicast group addresses

- Use Internet Protocol Security (IPsec) to authenticate and provide confidentiality to assets that can be tied to a scalable trust model.
- Enable controls that might not have been used in IPv4 due to a lower threat level during initial deployment (implementing default deny access control policies, implementing routing protocol security, etc.).
- Use Control Plane Policing for granular control over the router's processes.
- Use Quality of Service (QoS) policy to control misbehaving IPv6 applications and ICMPv6 flooding
- Use Access Control Lists (ACL) to selectively filter IPv6 traffic.
- Follow the vendor offering, which should include protection against RA, ND, and DHCPv6 attacks.
- Deploy SeND to secure the IPv6 ND protocol operation.
- Harden your computers against malicious IPv6 packets.
- Check on what ports your computer is listening for connections. Review your neighbor cache for unauthorized systems.
- Make sure that your IPv6 hosts are not unintentionally forwarding IPv6 packets. Leverage IPv6-capable stateful firewall.

9. Equipment Standards and Testbed

9.1. Requirements for IPv6 in ICT Equipment

Lists of required RFC/3GPP standards for different types of hardware. The ICT hardware equipment can be divided into seven functional groups:

- Host: client or server
- Layer 2 switch
- Router or Layer 3 switch
- Network security equipment (firewalls, IDS, IPS...)
- CPE
- Mobile device
- Load balancer

The details of the mandatory and optional RFCs available in RIPE-554 document through the following link:

https://www.ripe.net/publications/docs/ripe-554/at_download/pdf

9.2. IPv6 Test Lab

This section provides information about how you can use the equipment listed below to create a test lab to configure and test the IPv6 protocol. These instructions take you through setting up a test lab based on the Base Configuration test lab and deploying IPv6 on these equipment. The resulting IPv6 test lab demonstrates default and configured IPv6 connectivity across an intranet and a simulated IPv4-only Internet. Beyond the set of tasks described in this section, these instructions allow you to create a functioning IPv6-capable network. You can use this network to:

- Learn more and experiment IPv6 features and functionality
- Explore network protocol and process specifics by capturing network traffic with a packet analyzer (e.g. Network Monitor)
- Improve applications development for IPv6 or modifying existing applications to support both IPv4 and IPv6.

9.2.1.Hardware and Software Requirements

The following are required components of the test lab:

- Router
- IP Phone
- Switch 24-port
- Server that meet the minimum hardware requirements for Windows Server 2012
- Clients that meet the minimum hardware requirements for Windows 10
- Firewall

9.2.2.Steps for Configuring the IPv6 Test Lab

You can get the Base Configuration Test Lab Guide for Windows from https://social.technet.microsoft.com/wiki/contents/articles/1262.test-lab-guides.aspx

10. FAQ

Below you can find answers to the most asked questions about the national IPv6 transition plan

10.1. Compatibility

The OTFv6 do not wish entities to put additional investments in changing their systems. The majority of the IP based systems, applications, or equipment available in the market are compatible with IPv6. The dual stack transition mechanism can allow the IPv4 and IPv6 devices to operate with each other in the same network. Therefore, TRA communicated to all entities clearly that systems, applications, and equipment that are incompatible with IPv6 can be exempted temporary from this project requirements, and it can operate with IPv4 during their current lifecycle, and to enable IPv6 once it is time to change these systems, applications or equipment.

10.2. The lack of knowledge

The lack of knowledge in IPv6 is considered one of the main challenges in IPv6 transition projects around the world. Therefore, OTFv6 worked to overcome this challenge through several initiatives and provided training to hundreds of personnel from public and private sectors free of charge. However, this should not stop the entities from implementing the project and building the required capacity during the project implementation.

10.3. Insufficient support at ISPs and vendors

Before issuing the national IPv6 transition plan, the TRA worked with ISPs in Oman to insure their readiness to offer their IP-based services over IPv6. The OTFv6 meets the ISPs regularly to discuss their role in this project. On other side, the vendors support can be insured only through the services contract between these entities and the vendor.

10.4. Cost

Several case studies mentioned that adopting IPv6 at an early stage and doing it gradually reduces the cost of the transition. Planning early allows aligning the deployment of IPv6 with regular refresh cycles and other IT initiatives. The legacy system that do not support IPv6 is not required to be changed immediately. Excluding such costly components from the project shall allow these entities to implement the project without financial burdens.

10.5. Complexity

The proper planning and gradual transition allows the entities to deploy the IPv6. The guidelines developed to help the organization in gradual implementation of the IPv6 protocol into the network.

10.6. Legacy system

As explained above, the legacy systems that do not support IPv6 can be exempted temporary and IPv6 deployment can be postponed until the changing of the systems with new IPv6-compatible systems.

10.7. Cleaning current IPv4 inventory

The national IPv6 transition plan specifies that the authorities should implement IPv6 to operate side by side with the existing IPv4 in their network using the dual stack IP implementations. It is not mandatory to get rid of IPv4 in neither short nor long term but entities should bear in mind the cost involved in running two networks in parallel especially the maintenance wise.

10.8. Scope

The scope of the national IPv6 transition plan includes the entire network including the public phasing services and the internal network (LAN).

10.9. Timeframe and Milestones

TRA circulated the timeframe and milestones with all entities, which remains unchanged.

11. Glossary of Terms and Acronyms

TRA	Telecommunication Regulatory Authority
MTC	Ministry of Technology & Communications
OGN	Oman Government Network
IPv6	Internet Protocol version 6
IPv4	Internet Protocol version 4
IPsec	Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs).
NAT	Network Address Translation is a method of remapping one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.
RIPE NCC	(Rйseaux IP Europйens Network Coordination Centre) the regional Internet registry (RIR) for Europe, West Asia, and the former USSR
CPE	Customer Premises Equipment
ISP	Internet Service Provider
Dual-Stack	A dual stack network is a network in which all of the nodes are both IPv4 and IPv6 enabled
IPv6 DS-lite	Dual Stack Lite (DS-Lite) is an IPv6 transition solution for ISPs with IPv6 infrastructure to connect their IPv4 subscribers to the Internet. DS-Lite uses IPv4-in-IPv6 tunneling to send a subscriber's IPv4 packet through a tunnel on the IPv6 access network to the ISP. The IPv6 packet is decapsulated to recover the subscriber's IPv4 packet and is then sent to the Internet after NAT address and port translation and other LSN related processing. The response packets traverse through the same path to the subscriber.

Annexure A, IPv6 Implementation Activity Sheet

Sr. No.	Activity	Proposed Target Date	Status
1.	Appointment of Nodal Officer		
2.	Circulation of letters, guidelines, checklist etc. to all organizations under the organization and orders on appointment of organizational nodal officers		
3.	Appointment of Organizational Nodal Officers		
4.	Form a "Transition Team" consisting of concerned officers & experts from stakeholders like service provider, vendors, software developers etc.) for giving technical advice and look into issues concerned with transition to IPv6		
5.	Call a meeting of all organizations under the ministry and discuss the following issues – a) Instructions issued by TRA b) Checklists issued by TRA c) Annexure 'A' & 'B' of Roadmap d) Preparation of equipment reports		
6.	Reports preparations based on activities		
7.	Audit of Equipment Reports by other Agency		
8.	**(optional)** Based on the Equipment Audit Reports, prepare an Equipment replacement plan to phase out non-compliant hardware and software. Assistance may be taken from "Transition Team" Please read (10.1.Compatibility and 10.6. Legacy system)		
9.	Prepare a procurement plan for the organization		
10.	Identify persons for IPv6 training and send them on training (Parallel Activity)		
11.	Float tenders for procurement of hardware and software as per the plans		
12.	IPv6 Address Allocation Policy		
13.	Set up a pilot test network either centrally or in one of the organization for testing and training		
14.	Equipment procurement and deployment in the network		
15.	Testing of hardware and software and transition of applications		
16.	Launch of IPv6 Services		

Annexure B, Transitioning Mechanism Practice Sample

Touch Points	Area	Component	Transition Mechanism	Protocol
Network	WAN	Routers	Dual Stack	OSPv3, ISISv6, BGP4 for IPv6, 6PE, 6VPE, ICMPv6
	LAN	L3 SW	Dual Stack	OSPv3, ISISv6, BGP4 for IPv6, ICMPv6
	Security	Firewall	Dual Stack	OSPv3, IPv6 ACL, NAT44, NAT64, ICMPv6
		IDS	Dual Stack,	ICMPv6
		Servers	Dual Stack	
		Desktops	Dual Stack	
		Video Conf. MCU	Dual Stack	
		IP Phones	Dual Stack	
Website		Website	Dual Stack	All services to support IPv6
Applications		DNS	Dual Stack	Support AAAA records
		AAA	Dual Stack	Support RFC 3162
		DHCP	Dual Stack	DHCPv6
		EMS/NMS	Dual Stack	ICMPv6
		e-Gov. Apps	Dual Stack	ICMPv6
Services		Data	Dual Stack	All services to support IPv6
		Voice	Dual Stack	All services to support IPv6
		Video	Dual Stack	All services to support IPv6